Cisco Secure Firewall ASA Series Command Reference, I - R Commands

First Published: 2005-05-31

Last Modified: 2023-12-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

PART I

I Commands

ia – inr

icmp

To configure access rules for ICMP traffic that terminates at the Secure Firewall ASA interface, use the **icmp** command. To remove the configuration, use the **no** form of this command.

icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*
no icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

deny	Deny access if the conditions are matched.
icmp_type	(Optional) ICMP message type (see Table 1-1).
if_name	The interface name.
ip_address	The IP address of the host sending ICMP messages to the interface.
net_mask	The network mask to be applied to the IP address of the host.
permit	Permit access if the conditions are matched.

Command Default

The default behavior of the ASA is to allow all ICMP traffic to the ASA interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any ASA interface. If no ICMP control list is configured, then the ASA accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the ASA does not respond to ICMP echo requests directed to a broadcast address.

The ASA only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

VPN access to an interface other than the one from which you entered the ASA is not supported. For example, if your VPN access is located on the outside interface, you can only initiate a connection directly to the outside interface. You should enable VPN on the directly accessible interface of the ASA and use name resolution so that you don't have to remember multiple addresses.

The icmp deny command disables pinging to an interface, and the icmp permit command enables pinging to an interface. With pinging disabled, the ASA cannot be detected on the network. This is also referred to as configurable proxy pinging.

Use the access-list extended or access-group command for ICMP traffic that is routed through the ASA for destinations on a protected interface.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about path MTU discovery.

If an ICMP control list is configured for an interface, then the ASA first matches the specified ICMP traffic and then applies an implicit deny for all other ICMP traffic on that interface. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the ASA discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a permit statement is assumed.

The following table lists the supported ICMP type values.

Table 1: ICMP Types and Literals

ICMP Type	Literal	Description
0	echo-reply	The echo reply is the response to an echo request to indicate successful communication.
3	unreachable	The device could not deliver a package to the final desination.
8	echo	The echo message that carries the address of the source. This address is the destination for the echo-reply message.
11	time-exceeded	During processing of a package, the device identifies the Time-To-Live value equal to zero and therefore the package is discarded.

Examples

The following example denies all ping requests and all incoming ICMP connections in general, except for unreachable messages, at the outside interface:

```
ciscoasa(config)# icmp permit any unreachable outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

The following example permits host 172.16.2.15 or hosts on subnet 172.22.1.0/16 to ping the outside interface:

```
ciscoasa(config)# icmp permit host 172.16.2.15 echo outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo outside
ciscoasa(config)# icmp permit any unreachable outside
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.

Commands	Description
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

icmp-object

To add ICMP types to an ICMP object group, use the icmp-object command in icmp-type configuration mode. To remove ICMP types, use the **no** form of this command.

icmp-object*icmp_type*
no icmp-object *icmp_type*

Syntax Description

icmp_type	Specifies an ICMP type name or number (0-255).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Icmp-type configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **icmp-object** command is used with the **object-group icmp-type** command to define an ICMP object. It is used in icmp-type configuration mode.

Instead of using this command, use **object-group service** and **service-group** commands to create a service group that contains ICMP types. Service groups can include ICMP6 and ICMP codes, whereas ICMP objects cannot.

ICMP type numbers and names include:

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**

Number	ICMP Type Name
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

Examples

The following example shows how to use the **icmp-object** command in icmp-type configuration mode:

```
ciscoasa(config)# object-group icmp-type icmp_allowed
ciscoasa(config-icmp-type)# icmp-object echo
ciscoasa(config-icmp-type)# icmp-object time-exceeded
ciscoasa(config-icmp-type)# exit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

icmp unreachable

To configure the unreachable ICMP message rate limit for ICMP traffic that terminates at an ASA interface, use the **icmp unreachable** command. To remove the configuration, use the **no** form of this command.

icmp unreachable rate-limit *rate* **burst-size** *size*
no icmp unreachable rate-limit *rate* **burst-size** *size*

Syntax Description

rate-limit *rate*	Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
burst-size *size*	Sets the burst rate, between 1 and 10. The burst size number of reponses are sent, but subsequent replies are not sent until the rate limit is reached.

Command Default

The default rate limit is 1 message per second.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(2)	This command was added.

Usage Guidelines

If you allow ICMP messages, including unreachable messages, to be sent to an ASA interface (see the **icmp** command), then you can control the rate of unreachable messages.

This command, along with the **set connection decrement-ttl** command, is required to allow a traceroute through the ASA that shows the ASA as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 10
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
set connection decrement-ttl	Decrements the time to live value for a packet.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

id-cert-issuer

To indicate whether the system accepts peer certificates issued by the CA associated with this trustpoint, use the **id-cert-issuer** command in crypto ca-trustpoint configuration mode. To disallow certificates that were issued by the CA associated with the trustpoint, use the **no** form of this command. This is useful for trustpoints that represent widely used root CAs.

id-cert-issuer
no id-cert-issuer

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is enabled (identity certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command to limit certificate acceptance to those issued by the subordinate certificate of a widely used root certificate. If you do not allow this feature, the ASA rejects any IKE peer certificate signed by this issuer.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and lets an administrator accept identity certificates signed by the issuer for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# id-cert-issuer
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

id-mismatch

To enable logging for excessive DNS ID mismatches, use the **id-mismatch** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-mismatch [**count** *number* **duration** *seconds*] **action log**
id-mismatch [**count** *number* **duration** *seconds*] **action log**]

Syntax Description

count number	The maximum number of mismatch instances before a system message log is sent.
duration seconds	The period, in seconds, to monitor.

Command Default

This command is disabled by default. The default rate is 30 in the a period of 3 seconds if the options are not specified when the command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

A high rate of DNS ID mismatches may indicate a cache poisoning attack. This command can be enabled to monitor and alert such attempts. A summarized system message log will be printed if the mismatch rate exceeds the configured value. The **id-mismatch** command provides the system administrator with additional information to the regular event-based system message log.

Examples

The following example shows how to enable ID mismatch in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-mismatch action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-randomization

To randomize the DNS identifier for a DNS query, use the **id-randomization** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-randomization
no id-randomization

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled by default. The DNS identifier from the DNS query does not get modified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

ID randomization helps protect against cache poisening attacks.

Examples

The following example shows how to enable ID randomization in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-randomization
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-usage

To specify how the enrolled identity of a certificate can be used, use the **id-usage** command in crypto ca trustpoint configuration mode. To set the usage of the certificate to the default, use the **no** form of this command.

id-usage { **ssl-ipsec** | **code-signer** }
no id-usage { **ssl-ipsec code-signer** }

Syntax Description

code-signer	The device identity represented by this certificate is used as a Java code signer to verify applets provided to remote users.
ssl-ipsec	(Default) The device identity represented by this certificate can be used as the server-side identity for SSL or IPsec-encrypted connections.

Command Default

The **id-usage** command default is **ssl-ipsec**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Remote-access VPNs can use SSL, IPsec, or both protocols, depending on deployment requirements, to permit access to virtually any network application or resource. The **id-usage** command allows you to specify the type of access to various certificate-protected resources.

A CA identity and in some cases, a device identity, is based on a certificate issued by the CA. All of the commands within the crypto ca trustpoint configuration mode control CA-specific configuration parameters, which specify how the ASA obtains the CA certificate, how the ASA obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Only a single instance of the **id-usage** command can be present in a trustpoint configuration. To enable the trustpoint for the **code-signer** and/or **ssl-ipsec** options, use a single instance which can specify either or both options.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and designates it as a code-signer certificate:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for the trustpoint general, and designates it as both a code-signer certificate and as a server side identity for SSL or IPsec connections:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for the trustpoint checkin1, and resets it to limit its use to SSL or IPsec connections:

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# no
 id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
java-trustpoint	Configures the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location.
ssl trust-point	Specifies the certificate that represents the SSL certificate for an interface.
trust-point (tunnel-group ipsec-attributes mode)	Specifies the name that identifies the certificate to be sent to the IKE peer,
validation-policy	Specifies conditions for validating certificates associated with user connections.

igmp

To reinstate IGMP processing on an interface, use the **igmp** command in interface configuration mode. To disable IGMP processing on an interface, use the **no** form of this command.

igmp
no igmp

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
ciscoasa(config-if)# no igmp
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the ASA and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **igmp access-group** command in interface configuration mode. To disable groups on the interface, use the **no** form of this command.

igmp access-group *acl*
no igmp access-group *acl*

Syntax Description

acl	Name of an IP access list. You can specify a standard or and extended access list. However, if you specify an extended access list, only the destination address is matched; you should specify **any** for the source.

Command Default

All groups are allowed to join on an interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp access-group 1
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp forward interface

To enable forwarding of all IGMP host reports and leave messages received to the interface specified, use the **igmp forward interface** command in interface configuration mode. To remove the forwarding, use the **no** form of this command.

igmp forward interface *if-name*
no igmp forward interface *if-name*

Syntax Description

if-name	Logical name of the interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Enter this command on the input interface. This command is used for stub multicast routing and cannot be configured concurrently with PIM.

Examples

The following example forwards IGMP host reports from the current interface to the specified interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp forward interface outside
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp join-group

To configure an interface to be a locally connected member of the specified group, use the **igmp join-group** command in interface configuration mode. To cancel membership in the group, use the **no** form of this command.

igmp join-group *group-address*
no igmp join-group *group-address*

Syntax Description

group-address	IP address of the multicast group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command configures an ASA interface to be a member of a multicast group. The **igmp join-group** command causes the ASA to both accept and forward multicast packets destined for the specified multicast group.

To configure the ASA to forward the multicast traffic without being a member of the multicast group, use the **igmp static-group** command.

Examples

The following example configures the selected interface to join the IGMP group 255.2.2.2:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp join-group 225.2.2.2
```

Related Commands

Command	Description
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp limit

To limit the number of IGMP states on a per-interface basis, use the **igmp limit** command in interface configuration mode. To restore the default limit, use the **no** form of this command.

igmp limit *number*
no igmp limit [*number*]

Syntax Description

number	Number of IGMP states allowed on the interface. Valid values range from 0 to 5000. The default value is 500. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the **igmp join-group** and **igmp static-group** commands) are still permitted.

Command Default

The default is 500.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **igmp max-groups** command.
9.15(1) *Also in 9.12(4)*	The igmp limit was increased from 500 to 5000.

Usage Guidelines

This command configures the limit of IGMP states. Membership reports exceeding the configured limits are not entered in the IGMP cache, and traffic for the excess membership reports is not forwarded.

When you change the IGMP limit on the interface with active joins on it, the new limit is not applicable to the existing groups. ASA validates the limit only when a new group is added to the interface or when the IGMP join timers expire. To apply the new limit with immediate effect, you must disenable and re-enable IGMP on the interface.

Examples

The following example limits the number of IGMP states on the interface to 250:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp limit 250
```

Related Commands

Command	Description
igmp	Reinstates IGMP processing on an interface.
igmp join-group	Configure an interface to be a locally connected member of the specified group.
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

To configure the frequency at which IGMP host query messages are sent by the interface, use the **igmp query-interval** command in interface configuration mode. To restore the default frequency, use the **no** form of this command.

igmp query-interval *seconds*
no igmp query-interval *seconds*

Syntax Description

seconds	Frequency, in seconds, at which to send IGMP host query messages. Valid values range from 1 to 3600. The default is 125 seconds.

Command Default

The default query interval is 125 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Multicast routers send host query messages to discover which multicast groups have members on the networks attached to the interface. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Host query messages are addressed to the all-hosts multicast group, which has an address of 224.0.0.1 TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages:

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Version 2, the designated router is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the **igmp query-timeout** command), it becomes the querier.

Caution Changing this value may severely impact multicast forwarding.

Examples

The following example changes the IGMP query interval to 120 seconds:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-interval 120
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-max-response-time

To specify the maximum response time advertised in IGMP queries, use the **igmp query-max-response-time** command in interface configuration mode. To restore the default response time value, use the **no** form of this command.

igmpquery-max-response-time*seconds*
no igmp query-max-response-time *seconds*

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Valid values are from 1 to 25. The default value is 10 seconds.

Command Default

10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command is valid only when IGMP Version 2 or 3 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example changes the maximum query response time to 8 seconds:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-max-response-time 8
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-timeout

To configure the timeout period before the interface takes over as the querier after the previous querier has stopped querying, use the **igmp query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

igmpquery-timeout*seconds*
no igmp query-timeout *seconds*

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. Valid values are from 60 to 300 seconds. The default value is 255 seconds.

Command Default

The default query interval is 255 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command requires IGMP Version 2 or 3.

Examples

The following example configures the router to wait 200 seconds from the time it received the last query before it takes over as the querier for the interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-timeout 200
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

igmp static-group

To configure the interface to be a statically connected member of the specified multicast group, use the **igmp static-group** command in interface configuration mode. To remove the static group entry, use the **no** form of this command.

igmp static-group *group*
no igmp static-group *group*

Syntax Description

group	IP multicast group address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When configured with the **igmp static-group** command, the ASA interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the ASA to both accept and forward multicast packets for a specific multicast group, use the **igmp join-group** command. If the **igmp join-group** command is configured for the same group address as the **igmp static-group** command, the **igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Examples

The following example adds the selected interface to the multicast group 239.100.100.101:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp static-group 239.100.100.101
```

Related Commands

Command	Description
igmp join-group	Configures an interface to be a locally connected member of the specified group.

igmp version

To configure which version of IGMP the interface uses, use the **igmp version** command in interface configuration mode. To restore version to the default, use the **no** form of this command.

igmp version { **1** | **2** }
no igmp version [**1** | **2**]

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.

Command Default

IGMP Version 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

All routers on the subnet must support the same version of IGMP. Hosts can have any IGMP version (1 or 2), and the ASA will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2, including as the **igmp query-max-response-time** and **igmp query-timeout** commands.

Examples

The following example configures the selected interface to use IGMP Version 1:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp version 1
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

Command	Description
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

ignore-ipsec-keyusage (Deprecated)

To suppress key usage checking on IPsec client certificates, use the **ignore-ipsec-keyusage** command in ca-trustpoint configuration mode. To resume key usage checking, use the **no** form of this command.

ignore-ipsec-keyusage
no ignore-ipsec-keyusage

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added as a safety measure and was deprecated at the same time. Note that future releases might not offer suppression of key usage checking.

Usage Guidelines

Use of this command indicates that the values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates are not to be validated. This command ignores key usage checking and is useful for non-compliant deployments.

Examples

The following example shows how to ignore the results of key usage checking:

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

ignore lsa mospf

To suppress the sending of syslog messages when the router receives LSA Type 6 MOSPF packets, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of the syslog messages, use the **no** form of this command.

ignore lsa mospf
no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Type 6 MOSPF packets are unsupported.

Examples

The following example causes LSA Type 6 MOSPF packets to be ignored:

```
ciscoasa(config-router)# ignore lsa mospf
```

Related Commands

Command	Description
show running-config router ospf	Displays the OSPF router configuration.

ignore-lsp-errors

To allow the ASA to ignore IS-IS link-state packets that are received with internal checksum errors rather than purging the link-state packets, use the **ignore-lsp-errors** command in router isis configuration mode. To disable this function, use the **no** form of this command.

ignore-lsp-errors
no ignore-lsp-errors

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default, that is, corrupted LSPs are dropped instead of purged for network stability.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The IS-IS protocol definition requires that a received link-state packet with an incorrect data-link checksum be purged by the receiver, which causes the initiator of the packet to regenerate it. However, if a network has a link that causes data corruption while still delivering link-state packets with correct data link checksums, a continuous cycle of purging and regenerating large numbers of packets can occur.

Because this could render the network nonfunctional, use the **ignore-lsp-errors** command to ignore these link-state packets rather than purge the packets. Link-state packets are used by the receiving routers to maintain their routing tables.

If you want to explicitly purge the corrupted LSPs, issue the **no ignore-lsp-errors** command.

Examples

The following example instructs the router to ignore link-state packets that have internal checksum errors:

ciscoasa(config)# **router isis**

```
ciscoasa(config-router)# ignore-lsp-errors
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

ignore-ssl-keyusage (Deprecated)

To suppress key usage checking on SSL client certificates, use the **ignore-ssl-keyusage** command in ca-trustpoint configuration mode. To resume key usage checking, use the **no** form of this command.

ignore-ssl-keyusage
no ignore-ssl-keyusage

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added as a safety measure and was deprecated at the same time. Note that future releases might not offer suppression of key usage checking.

Usage Guidelines

Use of this command indicates that the values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates are not to be validated. This command ignores key usage checking and is useful for noncompliant deployments.

Examples

The following example shows how to ignore the results of key usage checking:

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ssl-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

ike-retry-count

To configure the maximum number of connection retry attempts a Cisco AnyConnect VPN Client using IKE should make before falling back to SSL to attempt the connection, use the **ike-retry-count** command in group-policy webvpn configuration mode or username webvpn configuration mode. To remove this command from the configuration and reset the maximum number of retry attempts to the default value, use the **no** form of this command.

ike-retry-count { **none** | *value* }
no ike-retry-count { **none** | *value* }

Syntax Description

none	Specifies that no retry attempts are allowed.
value	Specify the maximum number of connection retry atttempts (1-10) for the Cisco AnyConnect VPN Client to perform after an initial connection failure.

Command Default

The default number of allowed retry attempts is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added

Usage Guidelines

Use the **ike-retry-count** command to control the number of times that the Cisco AnyConnect VPN Client should attempt to connect using IKE. If the client fails to connect using IKE after the number of retries specified in this command, it falls back to SSL to attempt the connection. This value overrides any value that exists in the Cisco AnyConnect VPN Client.

Note To support fallback from IPsec to SSL, the **vpn-tunnel-protocol** command must be have with both the **svc** and **ipsec** arguments configured.

Examples

The following example sets the IKE retry count to 7 for the group policy named FirstGroup:

```
ciscoasa
(config)# group-policy FirstGroup attributes
ciscoasa
(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)# ike-retry-count 7
ciscoasa
(config-group-webvpn)#
```

The following example sets the IKE retry count to 9 for the username Finance:

```
ciscoasa
(config)#
username
Finance attributes
ciscoasa
(config-username)# webvpn
ciscoasa
(config-username-webvpn)# ike-retry-count 9
ciscoasa
(config-group-webvpn)#
```

Related Commands

Command	Description
group-policy	Creates or edits a group policy.
ike-retry-timeout	Specifies the number of seconds between IKE retry attempts.
username	Adds a user to the ASA database.
vpn-tunnel-protocol	Configures a VPN tunnel type (IPsec, L2TP over IPsec, or WebVPN).
webvpn	Enters group-policy webvpn configuration mode or username webvpn configuration mode.

ikev1 pre-shared-key

To specify a preshared key to support IKEv1 connections based on preshared keys, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

pre-shared-key*key*
no pre-shared-key

Syntax Description

key	Specifies an alphanumeric key between 1 and 128 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The command name was changed from pre-shared-key to ikev1 pre-shared-key.

Usage Guidelines

You can apply this attribute to all IPsec tunnel-group types.

Examples

The following command entered in config-ipsec configuration mode, specifies the preshared key XYZX to support IKE connections for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key xyzx
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev1 trust-point

To specify the name of a trustpoint that identifies the certificate to be sent to the IKEv1 peer, use the **trust-point** command in tunnel-group ipsec-attributes mode. To eliminate a trustpoint specification, use the **no** form of this command.

trust-point*trust-point-name*
no trust-point *trust-point-name*

Syntax Description

trust-point-name	Specifies the name of the trustpoint to use.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec attributes	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The command name was changed from trust-point to ikev1 trust-point.

Usage Guidelines

You can apply this attribute to all IPsec tunnel group types.

Examples

The following example entered in tunnel-ipsec configuration mode, configures a trustpoint for identifying the certificate to be sent to the IKEv1 peer for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 trust-point mytrustpoint
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev1 user-authentication

To configure hybrid authentication during IKE, use the **ikev1 user-authentication** command in tunnel-group ipsec-attributes configuration mode. To disable hybrid authentication, use the **no** form of this command.

ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }
no ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }

Syntax Description

hybrid	Specifies hybrid XAUTH authentication during IKE.
interface	(Optional) Specifies the interface on which the user authentication method is configured.
none	Disables user authentication during IKE.
xauth	Specifies XAUTH, also called extended user authentication.

Command Default

The default authentication method is XAUTH or extended user authentication. The default is all interfaces.

Note You must leave the value at the XAUTH default to avoid breaking any established L2TP over IPsec sessions. If the tunnel-group is set to any other value (such as isakmp ikev1-user-authentication none), then you cannot establish an L2TP over IPsec session.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.4(1)	The command name was changed from isakmp **ikev1-user-authentication** to **ikev1 user-authentication.**

Usage Guidelines

You use this command when you need to use digital certificates for ASA authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+, or SecurID. This command breaks Phase 1 of IKE down into the following two steps, together called hybrid authentication:

1. The ASA authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
2. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

Note Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

An IPsec hybrid RSA authentication type is rejected when the exchange type is main mode.

When you omit the optional *interface* argument, the command applies to all the interfaces and serves as a backup when the per-interface command is not specified. When there are two **ikev1 user-authentication** commands specified for a tunnel group, and one uses the *interface* argument and one does not, the one specifying the interface takes precedence for that particular interface.

Examples

The following example commands enable hybrid XAUTH on the inside interface for a tunnel group called example-group:

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 user-authentication (inside) hybrid
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
aaa-server	Defines a AAA server.
pre-shared-key	Creates a preshared key for supporting IKE connections.
tunnel-group	Creates and manages the database of connection specific records for IPsec, L2TP/IPsec, and WebVPN connections.

ikev2 local-authentication

To specify local authentication for IKEv2 LAN-to-LAN connections, use the **ikev2 local-authentication** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**
no ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**

Syntax Description

certificate	Specifies certificate authentication.
hex	Configures a hex pre-shared key.
key_value	The key value, from 1 to 128 characters.
pre-shared-key	Specifies a local preshared key that is used to authenticate the remote peer.
string	Enter a hex pre-shared key between 2 and 256 with an even number of characters.
trustpoint	Specifies the trustpoint that identifies the certificate to send to the remote peer.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(2)	Remote authentication using EAP was added.
9.4(1)	The hex and hex string keywords were added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

You may configure only one authentication option for local authentication.

You must configure this command using the **certificate** option before you may use the **ikev2 remote-authentication** command to enable EAP authentication.

For IKEv2 connections, the tunnel group mapping must know which authentication methods to allow for remote authentication (PSK, certificate, and EAP) and local authentication (PSK and certificate), and which trust point to use for local authentication.

Examples

The following command specifies the preshared key XYZX to support IKE connections for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

The following commands configure the remote access tunnel group to authenticate the ASA to the peer using its identity certificate, which is associated with the trustpoint, myIDcert. The peer may also be authenticated using a preshared key, certificate, or EAP.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key XYZX
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 mobike-rrc

To enable return routability checking during mobile IKE (mobike) communications for IPsec IKEv2 RA VPN connections, use the **ikev2 mobike-rrc** command in tunnel-group ipsec-attributes configuration mode. To disable return routability checking, use the **no** form of this command.

ikev2 mobike-rrc
no ikev2 mobike-rrc

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Mobike is “always on.” This command is used to enable RRC for mobike connections.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.8(1)	This command was added.

Usage Guidelines

This command applies to IPsec IKEv2 RA VPN tunnel groups only.

Examples

The following example commands enable the return routability check for mobike for a tunnel group called example-group:

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 mobike-rrc
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

Command	Description
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 remote-authentication

To specify remote authentication for IPsec IKEv2 LAN-to-LAN connections, use the **ikev2 remote-authentication** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }
no ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }

Syntax Description

certificate	Specifies certificate authentication.
eap	Specifies the Extensible Authentication Protocol (EAP) is the method that supports user authentication with generic, third-party IKEv2 remote access clients (in addition to AnyConnect).
hex	Configure a hex pre-shared key.
key_value	The key value, from 1 to 128 characters.
pre-shared-key	Specifies a local preshared key that is used to authenticate the remote peer.
query-identity	Requests the EAP identity from the peer.
string	Enter a hex pre-shared key between 2 and 256 with an even number of characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(2)	The **eap** and **query-identity** keywords were added.
9.4(1)	The hex and hex-string keywords were added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

Before you can enable EAP for remote authentication, you must configure local authentication using a certificate and a valid trustpoint using the **ikev2 local-authentication pre-shared-key** *key-value* | **certificate** *trustpoint* command. Otherwise, an error occurs and the EAP authentication request is rejected.

You may configure multiple authentication options for remote authentication.

Note For IKEv2 connections, the tunnel group mapping must know which authentication methods to allow for remote authentication (PSK, certificate, and EAP) and local authentication (PSK and certificate), and which trust point to use for local authentication. Currently, mapping is performed using the IKE ID, which is taken from the peer or peer certificate field value (using the certificate map). If both options fail, then the in-coming connection is mapped to the default remote access tunnel group. A certificate map is an applicable option only when the remote peer is authenticated via a certificate. This map allows mapping to different tunnel groups. For certificate authentication only, the tunnel group lookup is performed using rules or using the default setting. For EAP and PSK authentication, the tunnel group lookup is performed using the IKE ID on the client (it matches the tunnel group name) or using the default setting.

Examples

The following commands specify the preshared key XYZX to support IKEv2 connections for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key xyzx
```

The following commands show an EAP request for authentication being denied:

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

ikev2 rsa-sig-hash

To configure the IKEv2 RSA signature hash, use the **ikev2 rsa-sig-hash** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

ikev2rsa-sig-hashsha1
no ikev2 rsa-sig-hash sha1

Syntax Description

sha1	Signs the IKEv2 authentication payload with the SHA-1 hash function.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

This command applies to IPsec IKEv2 LAN-to-LAN tunnel groups only.

Examples

The following commands sign the IKEv2 authentication payload with the SHA-1 function:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 rsa-sig-hash sha
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

im

To enable instant messaging over SIP, use the **im** command in parameters configuration mode, which is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

im
noim

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enable instant messaging over SIP in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# im
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

imap4s (Deprecated)

Note The last supported release for this command was 9.5(1).

To enter IMAP4S configuration mode, use the **imap4s** command in global configuration mode. To remove any commands entered in IMAP4S command mode, use the **no** form of this command.

imap4s
no imap4s

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

IMAP4 is a client/server protocol in which your Internet server receives and holds e-mail for you. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. IMAP4S lets you receive e-mail over an SSL connection.

Examples

The following example shows how to enter IMAP4S configuration mode:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)#
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
show running-config imap4s	Displays the running configuration for IMAP4S.

imi-traffic-descriptor

To define an action when the IMI Traffic Descriptor (IMITD) option occurs in a packet header with IP Options inspection, use the **imi-traffic-descriptor** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

imi-traffic-descriptor action { **allow** | **clear** }
no imi-traffic-descriptor action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the IMI Traffic Descriptor IP option.
clear	Remove the IMI Traffic Descriptor option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the IMI Traffic Descriptor IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# imi-traffic-descriptor action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

import

To provide one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface to StateLess Address Auto Configuration (SLAAC) clients, use the **import** command in ipv6 dhcp pool configuration mode. To remove the parameters, use the **no** form of this command.

import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }
no import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }

Syntax Description

dns-server	Imports the domain name server (DNS) server IP address.
domain-name	Imports the domain name.
nis address	Imports the Network Information Service (NIS) server IP address.
nis domain-name	Imports the NIS domain name.
nisp address	Imports the Network Information Service Plus (NIS+) server IP address.
nisp domain-name	Imports the NIS+ domain name.
sip address	Imports the Session Initiation Protocol (SIP) server IP address.
sip domain-name	Imports the SIP domain name.
sntp address	Imports the Simple Network Time Protocol (SNTP) server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the DNS server or domain name, when they send

Information Request (IR) packets to the ASA. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and in the **import** command. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.

Command	Description
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

import webvpn AnyConnect-customization

To load an AnyConnect customization object onto the flash device of the ASA, enter the **import webvpn AnyConnect-customization** command in privileged EXEC mode.

import webvpn AnyConnect-customization type { **binary** | **resource** | **transform** } **platform** { **linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile** } **name** *name* { *URL* | **stdin** { *num_chars* | *data* **quit** } }

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
platform {**linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile**}	Client platform to which the object applies.
stdin {*num_chars data* | *data* **quit**}	Specifies that the data will be provided from stdin. If the number of characters is not specified then the data read from standard input is expected to be base64-encoded followed by "\nquit\n".
type {**binary** | **resource** | **transform**}	Type of customization object being imported.
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure WebVPN is enabled on an ASA interface before you enter the **import customization** command. To do so, enter the **show running-config** command.

The ASA copies the customization object from the URLor stdin to the ASA file system disk0:/csco_config/customization.AnyConnect customizations may include custom AnyConnect GUI resources, a binary custom help file and binary VPN scripts, and installer transforms.

Related Commands

Command	Description
revert webvpn AnyConnect-customization	Removes the specified customization object from the flash device of the ASA.
show import webvpn AnyConnect-customization	Lists the customization objects present on the flash device of the ASA.

import webvpn customization

To load a customization object onto the flash device of the ASA, enter the **import webvpn customization** command in privileged EXEC mode.

import webvpn customization *name URL*

Syntax Description

name	The name that identifies the customization object. The maximum number is 64 characters.
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure WebVPN is enabled on an ASA interface before you enter the **import customization** command. To do so, enter the **show running-config** command.

The ASA does the following when you import a customization object:

- Copies the customization object from the URL to the ASA file system disk0:/csco_config/customization as MD5*name*.
- Performs a basic XML syntax check on the file. If it is invalid, the ASA deletes the file.
- Checks that the file in index.ini contains the record MD5*name*. If not, the ASA adds MD5*name* to the file.
- Copies the MD5*name* file to RAMFS /csco_config/customization/ with as ramfs *name*.

Examples

The following example imports to the ASA a customization object, *General.xml*, from the URL 209.165.201.22/customization and names it *custom1*.

```
ciscoasa# import webvpn customization custom1 tftp://209.165.201.22/customization /General.xml
```

```
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn customization	Removes the specified customization object from the flash device of the ASA.
show import webvpn customization	Lists the customization objects present on the flash device of the ASA.

import webvpn mst-translation

To load an MST (Microsoft Transform) object onto the flash device of the ASA, enter the **import webvpn mst-translation** command in privileged EXEC mode.

import webvpn mst-transation AnyConnect language *language URL* | **stdin** { *num_chars data* | *data* **quit** } }

Syntax Description

language *language*	The translation language.
stdin {*num_chars data* | *data* **quit**}	Specifies that the data will be provided from stdin. If the number of characters is not specified then the data read from standard input is expected to be base64-encoded followed by "\nquit\n".
URL	Remote path to the source of the XML customization object. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This file translates the AnyConnect installer.

Related Commands

Command	Description
show import webvpn mst-translation	Lists the customization objects present on the flash device of the ASA.

import webvpn plug-in protocol

To install a plug-in onto the flash device of the ASA, enter the **import webvpn plug-in protocol** command in privileged EXEC mode.

import webvpn plug-in protocol *protocol URL*

Syntax Description

protocol

- **rdp—**The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The website containing the original is http://properjavardp.sourceforge.net/ .
- **ssh,telnet—**The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The website containing the original is http://javassh.org/ .

Caution The **import webvpn plug-in protocol ssh,telnet** *URL* command installs *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When typing the **ssh,telnet** string, do *not* insert a space. Use the **revert webvpn plug-in protocol** command to remove any **import webvpn plug-in protocol** commands that deviate from these requirements.

- **vnc—**The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The website containing the original is http://www.tightvnc.com/ .

URL	Remote path to the source of the plug-in.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Before installing a plug-in, do the following:

- Make sure Clientless SSL VPN ("webvpn") is enabled on an interface on the ASA. To do so, enter the **show running-config** command.
- Create a temporary directory named "plugins" on a local TFTP server (for example, with the hostname "local_tftp_server"), and download the plug-ins from the Cisco website to the "plugins" directory. Enter the hostname or address of the TFTP server and the path to the plug-in that you need into the URL field of the **import webvpn plug-in protocol** command.

The ASA does the following when you import a plug-in:

- Unpacks the .jar file specified in the *URL*.
- Writes the file to the csco-config/97/plugin directory on the ASA file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future Clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page. The following table shows the changes to the main menu and address field of the portal page.

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
citrix	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

The ASA does not retain the **import webvpn plug-in protocol** command in the configuration. Instead, it loads the contents of the csco-config/97/plugin directory automatically. A secondary ASA obtains the plug-ins from the primary ASA.

When the user in a Clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

Note Support has been added for SSH V2 in addition to previous SSH V1 and Telnet. The plug-in protocol is still the same (ssh and telnet), and the URL formats are as follows:ssh://<target> — uses SSH V2ssh://<target>/?version=1 — uses SSH V1telnet://<target> — uses telnet

To remove the respective **import webvpn plug-in protocol** command and disable support for the protocol, use the **revert webvpn plug-in protocol** command.

Examples

The following command adds Clientless SSL VPN support for RDP:

```
ciscoasa# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
```

```
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

The following command adds Clientless SSL VPN support for SSH and Telnet:

```
ciscoasa# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar
Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

The following command adds Clientless SSL VPN support for VNC:

```
ciscoasa# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar
Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

Related Commands

Command	Description
revert webvpn plug-in protocol	Removes the specified plug-in from the flash device of the ASA.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

import webvpn translation-table

To import a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **import webvpn translation-table** command in privileged EXEC mode.

import webvpn translation-table *translation_domain* **language** *language url*

Syntax Description

language	Specifies a language for the translation table. Enter the value for *language* in the manner expressed by your browser language options.
translation_domain	Specifies the functional area and associated messages visible to remote users.
url	Specifies the URL of the XML file used to create the customization object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that is visible to remote users has its own translation domain and is specified by the *translation_domain argument*. The following table shows the translation domains and the functional areas translated.

Translation Domain	Functional Areas Translated
AnyConnect	*Messages displayed on the user interface of the Cisco AnyConnect VPN Client.*
banners	Banners displayed to remote users and messages when VPN access is denied.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	*Messages on the login and logout pages, portal page, and all the messages customizable by the user.*

Translation Domain	Functional Areas Translated
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
PortForwarder	Messages displayed to port forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA, and portal messages that are not customizable.

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the ASA includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the *login and logout pages, portal page, and URL bookmarks for clientless users,* the ASA **generates the customization** and **url-list** translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

Download the template for the translation domain using the **export webvpn translation-table** command, make changes to the messages, and use the **import webvpn translation-table** command to create the object. You can view available objects with the **show import webvpn translation-table** command.

Be sure to specify language in the manner expressed by your browser language options. For example, Microsoft Internet Explorer uses the abbreviation >*zh* for the Chinese language. The translation table imported to the ASA must also be named >*zh* .

With the exception of the AnyConnect translation domain, a translation table has no affect, and messages are not translated until you create a customization object, identify a translation table to use in that object, and specify the customization for the group policy or user. Changes to the translation table for the AnyConnect domain are immediately visible to Secure Client users. See the **import webvpn customization** command for more information.

Examples

The following example imports a translation-table for the translation domain affecting the Secure Client user interface, and specifies the translation table is for the Chinese language. The **show import webvpn translation-table** command displays the new object:

```
ciscoasa# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
```

```
Translation Tables:
zh AnyConnect
```

Related Commands

Command	Description
export webvpn translation-table	Exports a translation table.
import webvpn customization	Imports a customization object that references the translation table.
revert	Removes translation tables from flash.
show import webvpn translation-table	Displays available translation table templates and translation tables.

import webvpn url-list

To load a URL list onto the flash device of the ASA, enter the **import webvpn url-list** command in privileged EXEC mode.

import webvpn url-list *name URL*

Syntax Description

name	The name that identifies the URL list. The maximum number is 64 characters.
URL	Remote path to the source of the URL list. The maximum number is 255 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Make sure that WebVPN is enabled on a ASA interface before you enter the **import url-list** command. To do so, enter the **show running-config** command.

The ASA does the following when you import a URL list:

- Copies the URL list from the URL to the ASA file system disk0:/csco_config/url-lists as *name on flash* = base 64*name*.
- Performs a basic XML syntax check on the file. If the syntax is invalid, the ASA deletes the file.
- Checks that the file in index.ini contains the record base 64*name*. If not, the ASA adds base 64*name* to the file.
- Copies the *name* file to RAMFS /csco_config/url-lists/ with ramfs name = *name*.

Examples

The following example imports a URL list, *NewList.xml*, from the URL 209.165.201.22/url-lists to the ASA and names it *ABCList*.

```
ciscoasa# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
```

```
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn url-list	Removes the specified URL list from the flash device of the ASA.
show import webvpn url-list	Lists the URL lists present on the flash device of the ASA.

import webvpn webcontent

To import content to flash memory that is visible to remote Clientless SSL VPN users, use the **import webvpn webcontent** command in privileged EXEC mode.

import webvpn webcontent *destination url source url*

Syntax Description

destination url	**The URL to export to**. The maximum number is 255 characters.
source url	The URL in the ASA flash memory in which the content resides. The maximum number is 64 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Content imported with the **webcontent** option is visible to remote Clientless users. This includes help content visible on the Clientless portal and logos used by customization objects that customize user screens.

Content imported to URLs with the path /+CSCOE+/ is visible only to authorized users.

Content imported to URLs with the path /+CSCOU+/ is visible to both unauthorized and authorized users.

For example, a corporate logo imported as /+CSCOU+/logo.gif could be used in a portal customization object and be visible on the logon page and the portal page. The same logo.gif file imported as /+CSCOE+/logo.gif would only be visible to remote users after they have logged in successfully.

Help content that appears on the various application screens must be imported to specific URLs. The following table shows the URLs and screen areas for the help content displayed for standard Clientless applications:

URL	Clientless Screen Area
/+CSCOE+/help/*language* /app-access-hlp.inc	Application Access

URL	Clientless Screen Area
/+CSCOE+/help/*language* /file-access-hlp.inc	Browse Networks
/+CSCOE+/help/*language* /net_access_hlp.html	Secure Client
/+CSCOE+/help/*language* /web-access-help.inc	Web Access

The following table shows the URLs and screen areas for the help content displayed for optional plug-in Clientless applications:

URL	Clientless Screen Area
/+CSCOE+/help/*language* /ica-hlp.inc	MetaFrame Access
/+CSCOE+/help/*language* /rdp-hlp.inc	Terminal Servers
/+CSCOE+/help/*language* /ssh,telnet-hlp.inc	Telnet/SSH Servers
/+CSCOE+/help/*language* /vnc-hlp.inc	VNC Connections

The *language* entry in the URL path is the language abbreviation that you designate for the help content. The ASA does not actually translate the file into the language you specify, but labels the file with the language abbreviation.

Examples

The following example imports the HTML file *application_access_help.html,* from a TFTP server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

The following example imports the HTML file *application_access_help.html,* from a tftp server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

Related Commands

Command	Description
export webvpn webcontent	Exports previously imported content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

inspect a – inspect z

inspect ctiqbe

To enable CTIQBE protocol inspection, use the **inspect ctiqbe** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable inspection, use the **no** form of this command.

inspect ctiqbe
no inspect ctiqbe

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added and replaces the previously existing **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect ctiqbe** command enables CTIQBE protocol inspection, which supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the ASA .

The Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI) are used by many Cisco VoIP applications. Computer Telephony Interface Quick Buffer Encoding (CTIQBE) is used by Cisco TAPI Service Provider (TSP) to communicate with Cisco CallManager.

The following summarizes limitations that apply when using CTIQBE application inspection:

- Stateful failover of CTIQBE calls is not supported.
- Using the **debug ctiqbe** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the ASA, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.
- CTIQBE application inspection does not support CTIQBE messages fragmented in multiple TCP packets.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the ASA, calls between these two phones will fail.

- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the same port of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect** ctiqbe command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect** ctiqbe command does not use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect** ctiqbe command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the CTIQBE inspection engine, which creates a class map to match CTIQBE traffic on the default port (2748). The service policy is then applied to the outside interface.

```
ciscoasa(config)# class-map ctiqbe-port
ciscoasa(config-cmap)# match port tcp eq 2748
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ctiqbe_policy

ciscoasa(config-pmap)# class ctiqbe-port
ciscoasa(config-pmap-c)# inspect ctiqbe
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ctiqbe_policy interface outside
```

To enable CTIQBE inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show conn	Displays the connection state for different connection types.
show ctiqbe	Displays information regarding the CTIQBE sessions established across the ASA and the media connections allocated by the CTIQBE inspection engine.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect dcerpc

To enable inspection of DCERPC traffic destined for the endpoint-mapper, use the inspect dcerpc command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect dcerpc [*map_name*]
no inspect dceprc [*map_name*]

Syntax Description

map_name	(Optional) The name of the DCERPC inspection map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **inspect dcerpc** command enables or disables application inspection for the DCERPC protocol.

Examples

The following example shows how to define a DCERPC inspection policy map with the timeout configured for DCERPC pinholes.

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
ciscoasa(config)# class-map dcerpc
ciscoasa(config-cmap)# match port tcp eq 135
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class dcerpc
ciscoasa(config-pmap-c)# inspect dcerpc dcerpc_map
ciscoasa(config)# service-policy global-policy global
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.

Commands	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.
timeout pinhole	Configures the timeout for DCERPC pinholes and overrides the global system pinhole timeout.

inspect diameter

To enable Diameter application inspection, use the inspect **diameter** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect diameter [*diameter_map*] [**tls-proxy** *proxy_name*]
no inspect diameter [*diameter_map*] [**tls-proxy** *proxy_name*]

Note Diameter inspection requires the Carrier license.

Syntax Description

diameter_map	Specifies a Diameter policy map name.
tls-proxy *proxy_name*	Uses the specified TLS proxy so that encrypted connections can be inspected.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.
9.6(1)	The **tls-proxy** keyword was added.

Usage Guidelines

Diameter is an Authentication, Authorization, and Accounting (AAA) protocol used in next-generation mobile and fixed telecom networks such as EPS (Evolved Packet System) for LTE (Long Term Evolution) and IMS (IP Multimedia Subsystem). It replaces RADIUS and TACACS in these networks.

Diameter uses TCP and SCTP as the transport layer, and secures communications using TCP/TLS and SCTP/DTLS. It can optionally provide data object encryption as well. For detailed information on Diameter, see RFC 6733.

Diameter applications perform service management tasks such as deciding user access, service authorization, quality of service, and rate of charging. Although Diameter applications can appear on many different control-plane interfaces in the LTE architecture, the ASA inspects Diameter command codes and attribute-value pairs (AVP) for the following interfaces only:

- S6a: Mobility Management Entity (MME) - Home Subscription Service (HSS).
- S9: PDN Gateway (PDG) - 3GPP AAA Proxy/Server.
- Rx: Policy Charging Rules Function (PCRF) - Call Session Control Function (CSCF).

Diameter inspection opens pinholes for Diameter endpoints to allow communication. The inspection supports 3GPP version 12 and is RFC 6733 compliant. You can use it for TCP/TLS (by specifying a TLS proxy when you enable inspection) and SCTP, but not SCTP/DTLS. Use IPsec to provide security to SCTP Diameter sessions.

You can optionally use a Diameter inspection policy map to filter traffic based on application ID, command codes, and AVP, to apply special actions such as dropping packets or connections, or logging them. You can create custom AVP for newly-registered Diameter applications. Filtering let's you fine-tune the traffic you allow on your network.

Note Diameter messages for applications that run on other interfaces will be allowed and passed through by default. However, you can configure a Diameter inspection policy map to drop these applications by application ID, although you cannot specify actions based on the command codes or AVP for these unsupported applications.

Examples

The following example applies Diameter inspection globally on the default ports, which are TCP/3868, TCP/5868, and SCTP/3868.

```
ciscoasa(config)# policy-map global_policy

ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect diameter
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy global_policy global
```

Related Commands

Commands	Description
class	Defines the traffic class to which to apply security actions.
inspect sctp	Enables SCTP inspection.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect diameter	Shows the status and statistics of the inspect diameter policy.
tls-proxy	Defines a TLS proxy.

inspect dns

To enable DNS inspection (if it has been previously disabled) or to configure DNS inspection parameters, use the **inspect dns** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable DNS inspection, use the **no** form of this command.

inspect dns [*map_name*] [**dynamic-filter-snoop**]
no inspect dns [*map_name*] [**dynamic-filter-snoop**]

Syntax Description

dynamic-filter-snoop	(Optional) Enables dynamic filter snooping, which is used exclusively by the Botnet Traffic Filter. Include this keyword only if you use Botnet Traffic Filtering. We suggest that you enable DNS snooping only on interfaces where external DNS requests are going. Enabling DNS snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the ASA.
map_name	(Optional) Specifies the name of the DNS map.

Command Default

This command is enabled by default. Botnet Traffic Filter snooping is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.
7.2(1)	This command was modified to allow configuration of additional DNS inspection parameters.
8.2(1)	The **dynamic-filter-snoop** keyword was added.

Usage Guidelines

DNS inspection is enabled by default, using the preset_dns_map inspection class map:

- The maximum DNS message length is 512 bytes.
- The maximum client DNS message length is automatically set to match the Resource Record.
- DNS Guard is enabled, so the ASA tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the ASA. The ASA also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.
- Translation of the DNS record based on the NAT configuration is enabled.

- Protocol enforcement is enabled, which enables DNS message format check, including domain name length of no more than 255 characters, label length of 63 characters, compression, and looped pointer check.

DNS Inspection Required for DNS Rewrite

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

DNS rewrite performs two functions:

- Translating a public address (the routable or "mapped" address) in a *>DNS reply* to a private address (the "real" address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

As long as DNS inspection remains enabled, you can configure DNS rewrite for NAT.

Examples

The following example shows how to set the maximum DNS message length:

```
ciscoasa(config)# policy-map type inspect dns dns-inspect
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 1024
```

The following example creates a class map for all UDP DNS traffic, enables DNS inspection and Botnet Traffic Filter snooping with the default DNS inspection policy map, and applies it to the outside interface:

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
policy-map	Associates a class map with specific security actions.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.

inspect esmtp

To enable SMTP/ESMTP application inspection or to change the ports to which the ASA listens, use the **inspect esmtp** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect esmtp [*map_name*]
no inspect esmtp [*map_name*]

Syntax Description

map_name (Optional) The name of the ESMTP map.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

ESMTP inspection is enabled by default, using the _default_esmtp_map inspection policy map.

- The server banner is masked.
- Encrypted traffic is inspected.
- Special characters in sender and receiver address are not noticed, no action is taken.
- Connections with command line length greater than 512 are dropped and logged.
- Connections with more than 100 recipients are dropped and logged.
- Messages with body length greater than 998 bytes are logged.
- Connections with header line length greater than 998 are dropped and logged.
- Messages with MIME filenames greater than 255 characters are dropped and logged.
- EHLO reply parameters matching “others” are masked.

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the ASA and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar is most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

Extended SMTP application inspection adds support for these extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS, and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the ASA supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, ONEX, VERB, CHUNKING, and private extensions and are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “0” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP may hang if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human-readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character (|) is deleted (changed to a blank space) and “<” ,”>” are only allowed if they are used to define a mail address (“>” must be preceded by “<”).
- Unexpected transition by the SMTP server.
- For unknown commands, the ASA changes all the characters in the packet to X. In this case, the server generates an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

Examples

The following example enables the SMTP inspection engine, which creates a class map to match SMTP traffic on the default port (25). The service policy is then applied to the outside interface.

```
ciscoasa(config)# class-map smtp-port
ciscoasa(config-cmap)# match port tcp eq 25
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map smtp_policy

ciscoasa(config-pmap)# class smtp-port
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy smtp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

inspect ftp

To configure the port for FTP inspection or to enable enhanced inspection, use the **inspect ftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ftp [**strict** [*map_name*]]
no inspect ftp [**strict** [*map_name*]]

Syntax Description

map_name	The name of an FTP inspection map.
strict	(Optional) Enables enhanced inspection of FTP traffic and forces compliance with RFC standards.

Command Default

FTP inspection is enabled by default, and the ASA listens to port 21 for FTP.

Use caution when moving FTP to a higher port. For example, if you set the FTP port to 2021, all connections that initiate to port 2021 will have their data payload interpreted as FTP commands.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated. The *map_name* option was added.

Usage Guidelines

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address

FTP application inspection prepares secondary channels for FTP data transfer. Ports for these channels are negotiated through PORT or PASV commands. The channels are allocated in response to a file upload, a file download, or a directory listing event.

Note Apply inspection only to the port for the FTP control connection and not the data connection. The ASA stateful inspection engine dynamically prepares the data connection as necessary.

If you disable FTP inspection engines with the **no inspect ftp** command, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

Strict FTP

Strict FTP increases the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. To enable strict FTP, include the strict option with the **inspect ftp** command.

When you use strict FTP, you can optionally specify an FTP inspection policy map to specify FTP commands that are not permitted to pass through the ASA.

After you enable the **strict** option on an interface, FTP inspection enforces the following behavior:

- An FTP command must be acknowledged before the ASA allows a new command.
- The ASA drops connections that send embedded commands.
- The 227 and PORT commands are checked to ensure they do not appear in an error string.

Caution Using the **strict** option may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

If the **strict** option is enabled, each FTP command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the PORT and PASV reply command is checked to see if it is five. If it is not five, then the PORT command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the FTP command to see if it ends with <CR><LF> characters, as required by the RFC. If it does not, the connection is closed.
- Size of RETR and STOR commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The PORT command should always be sent from the client. The TCP connection is denied if a PORT command is sent from the server.
- Reply spoofing—PASV reply command (227) should always be sent from the server. The TCP connection is denied if a PASV reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing—The ASA closes the connection if it detects TCP stream editing.
- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. As port numbers in the range from 1 to 1024 are reserved for well-known connections, if the negotiated port falls in this range, then the TCP connection is freed.
- Command pipelining—The number of characters present after the port numbers in the PORT and PASV reply command is cross checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.

- The ASA replaces the FTP server response to the SYST command with a series of Xs. to prevent the server from revealing its system type to FTP clients. To override this default behavior, use the **no mask-syst-reply** command in the FTP map.

FTP Log Messages

FTP application inspection generates the following log messages:

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

Examples

Before submitting a username and password, all FTP users are presented with a greeting banner. By default, this banner includes version information useful to hackers trying to identify weaknesses in a system. The following example shows how to mask this banner:

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.
policy-map type inspect	Creates an inspection policy map.
request-command deny	Specifies FTP commands to disallow.
service-policy	Applies a policy map to one or more interfaces.

inspect gtp

To enable GTP inspection, use the **inspect gtp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to disable GTP inspection.

inspect gtp [*map_name*]
no inspect gtp [*map_name*]

Note GTP inspection requires the GTP/GPRS or Carrier license.

Syntax Description

map_name (Optional) Name for the GTP inspection policy map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	Support was added for GTPv2 and IPv6 addresses.

Usage Guidelines

GPRS Tunneling Protocol is used in GSM, UMTS and LTE networks for general packet radio service (GPRS) traffic. GTP provides a tunnel control and management protocol to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP also uses a tunneling mechanism for carrying user data packets. Service provider networks use GTP to tunnel multi-protocol packets through the GPRS backbone between endpoints.

GTP inspection is not enabled by default. However, if you enable it without specifying your own inspection map, a default map is used which provides the following processing. You need to configure a map only if you want different values.

- Errors are not permitted.
- The maximum number of requests is 200.
- The maximum number of tunnels is 500.

- The GSN/endpoint timeout is 30 minutes.
- The PDP context timeout is 30 minutes. In GTPv2, this is the bearer context timeout.
- The request timeout is 1 minute.
- The signaling timeout is 30 minutes.
- The tunneling timeout is 1 hour.
- The T3 response timeout is 20 seconds.
- Unknown message IDs are dropped and logged. This behavior is confined to messages the 3GPP defines for the S5S8 interface. Messages defined for other GPRS interfaces might be allowed with minimal inspection.

Use the **policy-map type inspect gtp** command to define the parameters for GTP. After defining the GTP map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the inspect command to the class, and to apply the policy to one or more interfaces.

The well-known ports for GTP are UDP 3386, 2123, and 2152.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect gtp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect gtp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect gtp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example shows how to limit the number of tunnels in the network:

```
ciscoasa(config)# policy-map type inspect gtp
 gmap

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default

ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

Related Commands

Commands	Description
class	Defines the traffic class to which to apply security actions.

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect gtp	Shows that status and statistics of the inspect gtp policy.

inspect h323

To enable H.323 application inspection or to change the ports to which the ASA listens, use the **inspect h323** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect h323 { **h225** | **ras** } [*map_name*]
no inspect h323 { **h225** | **ras** } [*map_name*]

Syntax Description

h225	Enables H.225 signaling inspection.
map_name	(Optional) The name of the H.323 map.
ras	Enables RAS inspection.

Command Default

The default port assignments are as follows:

- h323 h225 1720
- h323 ras 1718-1719

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The inspect h323 command provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. The ASA supports H.323 through Version 6, including the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the ASA supports multiple calls on the same call signaling channel, a feature added with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the ASA.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the ASA uses an ASN.1 decoder to decode the H.323 messages.
- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect h323** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect h323** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect h323** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the H.323 inspection engine, which creates a class map to match H.323 traffic on the default port (1720). The service policy is then applied to the outside interface.

```
ciscoasa(config)# class-map h323-port
ciscoasa(config-cmap)# match port tcp eq 1720
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map h323_policy

ciscoasa(config-pmap)# class h323-port
ciscoasa(config-pmap-c)# inspect h323
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy h323_policy interface outside
```

Related Commands

Commands	Description
policy-map type inspect	Creates an inspection policy map.
show h225	Displays information for H.225 sessions established across the ASA.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the ASA.
timeout {**h225** | **h323**}	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

inspect http

To enable HTTP application inspection or to change the ports to which the ASA listens, use the **inspect http command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect http [*map_name*]
no inspect http [*map_name*]

Syntax Description

map_name (Optional) The name of the HTTP inspection map.

Command Default

The default port for HTTP is 80.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

Tip You can install a service module that performs application and URL filtering, which includes HTTP inspection, such as ASA CX or ASA FirePOWER. The HTTP inspection running on the ASA is not compatible with these modules. Note that it is far easier to configure application filtering using a purpose-built module rather than trying to manually configure it on the ASA using an HTTP inspection policy map.

Use the HTTP inspection engine to protect against specific attacks and other threats that are associated with HTTP traffic.

HTTP application inspection scans HTTP headers and body, and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the security appliance.

The enhanced HTTP inspection feature, which is also known as an application firewall and is available when you configure an HTTP inspection policy map, can help prevent attackers from using HTTP messages for circumventing network security policy.

HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements

in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.

Enhanced HTTP inspection verifies the following for all HTTP messages:

- Conformance to RFC 2616
- Use of RFC-defined methods only.
- Compliance with the additional criteria.

Examples

In this example, any HTTP connection (TCP traffic on port 80) that enters the ASA through any interface is classified for HTTP inspection. Because the policy is a global policy, inspection occurs only as the traffic enters each interface.

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
policy-map type inspect	Creates an inspection policy map.

inspect icmp

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect icmp
no inspect icmp

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The ICMP inspection engine allows ICMP traffic to be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the ASA in an ACL. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct

When ICMP inspection is disabled, which is the default configuration, ICMP echo reply messages are denied from a lower security interface to a higher security interface, even if it is in response to an ICMP echo request.

Examples

You enable the ICMP application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface. To enable ICMP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect icmp error

To enable application inspection for ICMP error messages, use the **inspect icmp** error command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect icmp error
no inspect icmp error

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

When ICMP Error inspection is enabled, the ASA creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The ASA overwrites the packet with the translated IP addresses.

When disabled, the ASA does not create translation sessions for intermediate nodes that generate ICMP error messages. ICMP error messages generated by the intermediate nodes between the inside host and the ASA reach the outside host without consuming any additional NAT resource. This is undesirable when an outside host uses the traceroute command to trace the hops to the destination on the inside of the ASA. When the ASA does not translate the intermediate hops, all the intermediate hops appear with the mapped destination IP address.

The ICMP payload is scanned to retrieve the five-tuple from the original packet. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. The ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the mapped IP is changed to the real IP (Destination Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet mapped IP is changed to the real IP
  - Original packet mapped port is changed to the real Port

- Original packet IP checksum is recalculated

Examples

The following example enables the ICMP error application inspection engine, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface. To enable ICMP error inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
inspect icmp	Enables or disables the ICMP inspection engine.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect ils

To enable ILS application inspection, use the inspect **ils command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ils
no inspect ils

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect ils** command provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The ASA supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the ASA border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the **timeout** command.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH

RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions.
- Parses the LDAP packet.
- Extracts IP addresses.
- Translates IP addresses as necessary.
- Encodes the PDU with translated addresses using BER encode functions.
- Copies the newly encoded PDU back to the TCP packet.
- Performs incremental TCP checksum and sequence number adjustment.

ILS inspection has the following limitations:

- Referral requests and responses are not supported.
- Users in multiple directories are not unified.
- Single users having multiple identities in multiple directories cannot be recognized by NAT.

Note Because H.225 call signaling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP **timeout** command. By default, this interval is set at 60 minutes.

Examples

You enable the ILS inspection engine as shown in the following example, which creates a class map to match ILS traffic on the default port (389). The service policy is then applied to the outside interface. To enable ILS inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map ils-port
ciscoasa(config-cmap)# match port tcp eq 389
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ils_policy

ciscoasa(config-pmap)# class ils-port
ciscoasa(config-pmap-c)# inspect ils
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ils_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.

Commands	Description
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.

inspect im

To enable inspection of Instant Messenger traffic, use the inspect im command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect im *map_name*
no inspect im *map_name*

Syntax Description

map_name	The name of the IM map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **inspect im** command enables or disables application inspection for the IM protocol. The Instant Messaging (IM) inspect engine lets you control the network usage of IM and stop leakage of confidential data, propagation of worms, and other threats to the corporate network.

Examples

The following example shows how to define an IM inspection policy map:

```
ciscoasa(config)# regex loginname1 "user1\@example.com"
ciscoasa(config)# regex loginname2 "user2\@example.com"
ciscoasa(config)# regex loginname3 "user3\@example.com"
ciscoasa(config)# regex loginname4 "user4\@example.com"
ciscoasa(config)# regex yahoo_version_regex "1\.0"
ciscoasa(config)# regex gif_files ".*\.gif"
ciscoasa(config)# regex exe_files ".*\.exe"
ciscoasa(config)# class-map type regex match-any yahoo_src_login_name_regex
ciscoasa(config-cmap)# match regex loginname1
ciscoasa(config-cmap)# match regex loginname2
ciscoasa(config)# class-map type regex match-any yahoo_dst_login_name_regex
ciscoasa(config-cmap)# match regex loginname3
ciscoasa(config-cmap)# match regex loginname4
ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
```

```
ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex
ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy2
ciscoasa(config-cmap)# match version regex yahoo_version_regex
ciscoasa(config)# class-map im_inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect ip-options

To enable inspection of IP options in a packet header, use the inspect ip-options command in class or policy map type inspect configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ip-options [*map_name*]
no inspect ip-options *map_name*

Syntax Description

map_name (Optional.) The name of the IP Options map.

Command Default

This command is enabled by default in the global policy. The default inspection map allows packets with the router-alert option, but drops packets that have any other options.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy or class map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added. Supported options are **eool**, **nop**, and **router-alert** options. If an IP header contains additional options other than EOOL, NOP, or RTRALT, regardless of whether the ASA is configured to allow these options, the ASA will drop the packet.
9.5(1)	Support for all IP options was added.

Usage Guidelines

In a packet, the IP header contains the Options field. The Options field, commonly referred to as IP Options, provides for control functions that are required in some situations but unnecessary for most common communications. In particular, IP Options include provisions for time stamps, security, and special routing. Use of IP Options is optional and the field can contain zero, one, or more options.

You can configure IP Options inspection to control which IP packets are allowed based on the contents of the IP Options field in the packet header. You can drop packets that have unwanted options, clear the options (and allow the packet), or allow the packet without change.

If you want non-default processing, create an IP Options inspection policy map, enter the **parameter** command, and specify the actions to take for the various options. You can inspect the following options. In all cases, the allow action allows packets that contain the option without modification; the clear action allows the packets but removes the option from the header.

Use the **no** form of the command to remove the option from the map. Any packet that contains an option that you do not include in the map is dropped, even if the packet contains otherwise allowed or cleared options.

For a list of IP options, with references to the relevant RFCs, see the IANA page, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml .

- **default action** {**allow** | **clear**}—Sets the default action for any option not explicitly included in the map. If you do not set a default action of allow or clear, packets that contain non-allowed options are dropped.
- **basic-security action** {**allow** | **clear**}—Allows or clears the Security (SEC) option.
- **commercial-security action** {**allow** | **clear**}—Allows or clears the Commercial Security (CIPSO) option.
- **eool action** {**allow** | **clear**}—Allows or clears the End of Options List option. This option, which contains just a single zero byte, appears at the end of all options to mark the end of a list of options. This might not coincide with the end of the header according to the header length.
- **exp-flow-control action** {**allow** | **clear**}—Allows or clears the Experimental Flow Control (FINN) option.
- **exp-measurement action** {**allow** | **clear**}—Allows or clears the Experimental Measurement (ZSU) option.
- **extended-security action** {**allow** | **clear**}—Allows or clears the Extended Security (E-SEC) option.
- **imi-traffic-descriptor action** {**allow** | **clear**}—Allows or clears the IMI Traffic Descriptor (IMITD) option.
- **nop action** {**allow** | **clear**}—Allows or clears the No Operation option. The Options field in the IP header can contain zero, one, or more options, which makes the total length of the field variable. However, the IP header must be a multiple of 32 bits. If the number of bits of all options is not a multiple of 32 bits, the NOP option is used as “internal padding” to align the options on a 32-bit boundary.
- **quick-start action** {**allow** | **clear**}—Allows or clears the Quick-Start (QS) option.
- **record-route action** {**allow** | **clear**}—Allows or clears the Record Route (RR) option.
- **router-alert action** {**allow** | **clear**}.—Allows or clears the Router Alert (RTRALT) option. This option is allowed in the default IP Options inspection policy map. This option notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols that require relatively complex processing from the routers along the packets delivery path. Dropping RSVP packets containing the Router Alert option can cause problems in VoIP implementations.
- **timestamp action** {**allow** | **clear**}—Allows or clears the Time Stamp (TS) option.
- {**0-255**} **action** {**allow** | **clear**}—Allows or clears the option identified by the option type number. The number is the whole option type octet (copy, class, and option number), not just the option number portion of the octet. These option types might not represent real options. Non-standard options must be in the expected type-length-value format defined in the Internet Protocol RFC 791, http://tools.ietf.org/html/rfc791 .

Examples

The following example shows how to define an IP Options inspection policy map that allows the ASA to pass packets that contain the EOOL, NOP, and RTRALT options in the packet header.

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow

ciscoasa(config-pmap-p)# nop action allow

ciscoasa(config-pmap-p)# router-alert action allow
```

The following example shows how to set a new default action to allow packets with any IP options.

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action allow
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Creates an inspection policy map.

inspect ipsec-pass-thru

To enable IPsec pass-through inspection, use the inspect ipsec-pass-thru command in class map configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ipsec-pass-thru [*map_name*]
no inspect ipsec-pass-thru [*map_name*]

Syntax Description

map_name (Optional) The name of the IPsec pass-through map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **inspect ipsec-pass-thru** command enables or disables application inspection. IPsec pass-through application inspection provides convenient traversal of ESP (IP protocol 50) and/or AH (IP protocol 51) traffic associated with an IKE UDP port 500 connection. It avoids lengthy access list configuration to permit ESP and AH traffic and also provides security using timeout and maximum connections.

Use the IPsec pass-through parameter map to identify a specific map to use for defining the parameters for the inspection. Use the policy-map type inspect command to access the parameters configuration, which lets you specify the restrictions for ESP or AH traffic. You can set the per-client maximum connections and the idle timeout in parameters configuration mode.

Use the class-map, policy-map, and service-policy commands to define a class of traffic, to apply the inspect command to the class, and to apply the policy to one or more interfaces. The parameter map defined is enabled when used with the inspect ipsec-pass-thru command.

NAT and non-NAT traffic is permitted. However, PAT is not supported.

Note In ASA 7.0(1), the **inspect ipsec-pass-thru** command allowed only ESP traffic to pass through. To retain the same behavior in later versions, a default map that permits ESP is created and attached if the **inspect ipsec-pass-thru** command is specified without any arguments. This map can be seen in the output of the show running-config all command.

Examples

The following example shows how to use access lists to identify IKE traffic, define an IPsec pass-through parameter map, define a policy, and apply the policy to the outside interface:

```
ciscoasa(config)# access-list ipsecpassthruacl permit udp any any eq 500
ciscoasa(config)# class-map ipsecpassthru-traffic
ciscoasa(config-cmap)# match access-list ipsecpassthruacl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru iptmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
ciscoasa(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
ciscoasa(config)# policy-map inspection_policy
ciscoasa(config-pmap)# class ipsecpassthru-traffic
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru iptmap
ciscoasa(config)# service-policy inspection_policy interface outside
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect ipv6

To enable IPv6 inspection, use the inspect ipv6 command in class configuration mode. Class configuration mode is accessible from policy-map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ipv6 [*map_name*]
no inspect ipv6 [*map_name*]

Syntax Description

map_name	(Optional.) The name of the IPv6 inspection policy map.

Command Default

IPv6 inspection is disabled by default.

If you enable IPv6 inspection and do not specify an inspection policy map, then the default IPv6 inspection policy map is used, and the following actions are taken:

- Allows only known IPv6 extension headers. Non-conforming packets are dropped and logged.
- Enforces the order of IPv6 extension headers as defined in the RFC 2460 specification. Non-conforming packets are dropped and logged.
- Drops any packet with a routing type header.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

IPv6 inspection lets you selectively log or drop IPv6 traffic based on the extension header. In addition, IPv6 inspection can check conformance to RFC 2460 for type and order of extension headers in IPv6 packets.

Examples

The following example drops all IPv6 traffic with the hop-by-hop, destination-option, routing-address, and routing type 0 headers:

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop
 match header destination-option
```

```
  drop
 match header routing-address count gt 0
  drop
 match header routing-type eq 0
  drop
policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
match header	Matches IPv6 headers in an IPv6 inspection policy map.
policy-map type inspect ipv6	Creates an inspection policy map for IPv6.
policy-map	Creates a Layer 3/4 policy map.
verify-header	Configures IPv6 inspection parameters.

inspect lisp

To enable LISP inspection, use the **inspect lisp** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. To disable LISP inspection, use the **no** form of this command.

inspect lisp [*inspect_map_name*]
no inspect lisp [*inspect_map_name*]

Syntax Description

inspect_map_name	Specify the LISP inspection map name (**policy-map type inspect lisp**) if you want to limit the EIDs or if you need to specify the pre-shared key for LISP messages.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	We added this command.

Usage Guidelines

The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example Inspects LISP traffic (UDP 4342) between a LISP router at 192.168.50.89 (on inside) and an ITR or ETR router (on another ASA interface) at 192.168.10.8:

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

inspect m3ua

To enable M3UA inspection, use the **inspect m3ua** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to disable M3UA inspection.

inspect m3ua [*map_name*]
no inspect m3ua [*map_name*]

Note M3UA inspection requires the Carrier license.

Syntax Description

map_name (Optional) Name for the M3UA inspection policy map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

MTP3 User Adaptation (M3UA) is a client/server protocol that provides a gateway to the SS7 network for IP-based applications that interface with the SS7 Message Transfer Part 3 (MTP3) layer. M3UA makes it possible to run the SS7 User Parts (such as ISUP) over an IP network. M3UA is defined in RFC 4666.

M3UA uses SCTP as the transport layer. SCTP port 2905 is the expected port, although you can configure the signaling gateways to use a different port.

The MTP3 layer provides networking functions such as routing and node addressing, but uses point codes to identify nodes. The M3UA layer exchanges Originating Point Codes (OPC) and Destination Point Codes (DPC). This is similar to how IP uses IP addresses to identify nodes.

M3UA inspection provides limited protocol conformance.

You can optionally create an M3UA inspection policy map to apply access policy based on point codes or Service Indicators (SI). You can also apply rate limiting based on message class and type.

Examples

The following example shows an M3UA inspection policy map and inspection policy.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasahostname(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect m3ua m3ua-map
ciscoasa(config)# service-policy global_policy global
```

Related Commands

Commands	Description
class	Defines the traffic class to which to apply security actions.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect m3ua	Shows that status and statistics of the inspect m3ua policy.

inspect mgcp

To enable MGCP application inspection or to change the ports to which the ASA listens, use the inspect **mgcp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect mgcp [*map_name*]
no inspect mgcp [*map_name*]

Syntax Description

map_name	(Optional) The name of the MGCP map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

To use MGCP, you usually need to configure at least two **inspect** commands: one for the port on which the gateway receives commands, and one for the port on which the Call Agent receives commands. Normally, a Call Agent sends commands to the default MGCP port for gateways, 2427, and a gateway sends commands to the default MGCP port for Call Agents, 2727.

MGCP is used for controlling media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses.

Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, and broad-band wireless devices.
- Business gateways, that provide a traditional digital PBX interface or an integrated >*soft PBX* interface to a Voice over IP network.

MGCP messages are transmitted over UDP. A response is sent back to the source address (IP address and UDP port number) of the command, but the response may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response.

Note MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the ASA and allows MGCP end points to register with the call agent.

Use the **call-agent** and **gateway** commands in MGCP map configuration mode to configure the IP addresses of one or more call agents and gateways. Use the **command-queue** command in MGCP map configuration mode to specify the maximum number of MGCP commands that will be allowed in the command queue at one time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect mgcp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect mgcp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect mgcp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

The maximum number of MGCP commands that can be queued is 150.

Examples

The following example shows how to identify MGCP traffic, define a MGCP inspection map, define a policy, and apply the policy to the outside interface. This creates a class map to match MGCP traffic on the default ports (2427 and 2727). The service policy is then applied to the outside interface. This configuration allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117. To enable MGCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2427

ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2727
ciscoasa(config)# class-map mgcp_port
ciscoasa(config-cmap)# match access-list mgcp_acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect mgcp inbound_mgcp
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-agent 10.10.11.5 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.6 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.7 102
ciscoasa(config-pmap-p)# call-agent 10.10.11.8 102
ciscoasa(config-pmap-p)# gateway 10.10.10.115 101
ciscoasa(config-pmap-p)# gateway 10.10.10.116 102
ciscoasa(config-pmap-p)# gateway 10.10.10.117 102
ciscoasa(config-pmap-p)# command-queue 150
ciscoasa(config-mgcp-map)# exit
```

```
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class mgcp_port
ciscoasa(config-pmap-c)# inspect mgcp
mgcp-map inbound_mgcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map type inspect mgcp	Creates an inspection policy map for MGCP.
show mgcp	Displays information about MGCP sessions established through the ASA.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect mmp

To configure the MMP inspection engine, use the **inspect mmp** command in class configuration mode. To remove MMP inspection, use the **no** form of this command.

inspect mmp tls-proxy [*name*]
no inspect mmp tls-proxy [*name*]

Syntax Description

name	Species the TLS proxy instance name.
tls-proxy	Enables the TLS proxy for MMP inspection. The MMP protocol can additionally use the TCP transport; however, the CUMA client only supports the TLS transport. Therefore, the **tls-proxy** keyword is required to enable MMP inspection.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(4)	The command was added.

Usage Guidelines

The ASA includes an inspection engine to validate the CUMA Mobile Multiplexing Protocol (MMP). MMP is a data transport protocol for transmitting data entities between CUMA clients and servers. Use the **inspect mmp** command when the ASA is deployed between CUMA clients and servers and inspection of MMP packets is required.

MMP inspection must be enabled with the TLS proxy because MMP traffic is transported only over a TLS connection.

Note While configuring the MMP inspection engine, please note that it can only be added under a non-default inspection class.

Examples

The following example shows the use of the **inspect mmp** command to inspect MMP traffic:

```
ciscoasa
```

```
(config)#
class-map mmp
ciscoasa
(config-cmap)#
match port tcp eq 5443
ciscoasa
(config-cmap)#
exit
ciscoasa
(config)#
policy-map mmp-policy
ciscoasa
(config-pmap)#
class mmp
ciscoasa(config-pmap-c)# inspect mmp tls-proxy myproxy
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa
(config)#
service-policy mmp-policy interface outside
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.

inspect netbios

To enable NetBIOS application inspection or to change the ports to which the ASA listens, use the inspect netbios **command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect netbios [*map_name*]
no inspect netbios [*map_name*]

Syntax Description

map_name	(Optional) The name of the NetBIOS map.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect netbios** command enables or disables application inspection for the NetBIOS protocol. NetBIOS inspection is enabled by default. The NetBIOS inspection engine translates IP addresses in the NetBIOS name service (NBNS) packets according to the ASA NAT configuration. You can optionally create a policy map to drop or log NetBIOS protocol violations.

Examples

The following example shows how to define a NetBIOS inspection policy map:

```
ciscoasa(config)# policy-map type inspect netbios netbios_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation drop
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
policy-map type inspect netbios	Creates an inspection policy map for NetBIOS.

Commands	Description
service-policy	Applies a policy map to one or more interfaces.

inspect pptp

To enable PPTP application inspection or to change the ports to which the ASA listens, use the inspect **pptp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect pptp
no inspect pptp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The Point-to-Point Tunneling Protocol (PPTP) is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE [RFC 2637] when negotiated over the PPTP TCP control channel. Port Address Translation is not performed for the unmodified version of GRE [RFC 1701, RFC 1702].

Specifically, the ASA inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network.

To enable PPTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

You enable the PPTP inspection engine as shown in the following example, which creates a class map to match PPTP traffic on the default port (1723). The service policy is then applied to the outside interface.

```
ciscoasa(config)# class-map pptp-port
ciscoasa(config-cmap)# match port tcp eq 1723
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pptp_policy
ciscoasa(config-pmap)# class pptp-port
ciscoasa(config-pmap-c)# inspect pptp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy pptp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect radius-accounting

To enable or disable RADIUS accounting inspection or to define a map for controlling traffic or tunnels, use the **inspect radius-accounting** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect radius-accounting *map_name*
no inspect radius-accounting [*map_name*]

Syntax Description

map_name	Name for the RADIUS accounting map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The purpose of RADIUS accounting inspection is to prevent over-billing attacks on GPRS networks that use RADIUS servers. Although you do not need the GTP/GPRS or Carrier license to implement RADIUS accounting inspection, it has no purpose unless you are implementing GTP inspection and you have a GPRS setup.

Use the **policy-map type inspect radius-accounting** command to create an inspection map to use for defining the parameters for RADIUS accounting. After entering the parameters command, you can define the inspection characteristics and behavior using the **send response**, **host**, **validate-attribute**, **enable gprs**, and **timeout users** commands.

Then you use the **class-map type management**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the inspect radius-accounting command to the class, and to apply the policy to one or more interfaces.

Note The **inspect radius-accounting** command can only be used with the **class-map type management** command.

Examples

The following example shows how to configure a RADIUS accounting inspection map and enable inspection globally.

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

Related Commands

Commands	Description
parameters	Defines the traffic class to which to apply security actions.
class-map type management	Lets you identify Layer 3 or 4 management traffic destined for the ASA to which you want to apply actions.
policy-map type inspect radius-accounting	Creates an inspection policy map for RADIUS accounting.
show and **clear service-policy**	Lets you view and clear service policy settings.
service-policy	Applies a policy map to one or more interfaces.

inspect rsh

To enable RSH application inspection or to change the ports to which the ASA listens, use the inspect **rsh** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rsh
no inspect rsh

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

Examples

The following example enables the RSH inspection engine, which creates a class map to match RSH traffic on the default port (514). The service policy is then applied to the outside interface. To enable RSH inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy

ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect rtsp

To enable RTSP application inspection or to change the ports to which the ASA listens, use the inspect **rtsp** command in class configuration mode. Class configuration mode is accessible from policy-map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rtsp [*map_name*]
no inspect rtsp [*map_name*]

Syntax Description

map_name	(Optional) The name of the RTSP map.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect rtsp** command lets the ASA pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

Note For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The ASA only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that will be used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The ASA parses setup response messages with a status code of 200. If the response message is traveling inbound, the server is outside relative to the ASA and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the ASA does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the setup response message, the ASA will need to keep state and remember the client ports in the setup message. QuickTime places the client ports in the setup message and then the server responds with only the server ports.

Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the ASA, add an **access-list** command statement from the server to the client or vice versa. For RealPlayer, change transport mode by choosing **Options** > **Preferences** > **Transport** > **RTSP Settings**.

If using TCP mode on the RealPlayer, check the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the ASA, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, check the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the ASA, add a **inspect rtsp** *port* command statement.

Restrictions and Limitations

The following restrictions apply to the RSTP inspection.

- The ASA does not support multicast RTSP or RTSP messages over UDP.
- The ASA does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The ASA cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and the ASA cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of translates the ASA performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.

Examples

The following example enables the RTSP inspection engine, which creates a class map to match RTSP traffic on the default ports (554 and 8554). The service policy is then applied to the outside interface.

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554

ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic

ciscoasa(config-cmap)# match access-list rtsp-acl

ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy

ciscoasa(config-pmap)# class rtsp-traffic
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect scansafe

To enable Cloud Web Security inspection on the traffic in a class, use the **inspect scansafe** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. To remove the inspect action, use the **no** form of this command.

inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]
no inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

Syntax Description

scansafe_policy_name	Specifies the inspection class map name defined by the **policy-map type inspect scansafe** command.
fail-open	(Optional) Allows traffic to pass through the ASA if the Cloud Web Security servers are unavailable.
fail-close	(Optional) Drops all traffic if the Cloud Web Security servers are unavailable. **fail-close** is the default.

Command Default

fail-close is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Cisco Cloud Web Security provides web security and web filtering services through the Software-as-a-Service (SaaS) model. Enterprises with the ASA in their network can use Cloud Web Security services without having to install additional hardware.

Note This feature is also called “ScanSafe,” so the ScanSafe name appears in some commands.

Configure this command using Modular Policy Framework:

1. Create inspection policy maps using the **policy-map type inspect scansafe** command, at least one for HTTP and one for HTTPS (assuming you want to inspect both types of traffic).
2. (Optional) Configure a whitelist using the **class-map type inspect scansafe** command.

3. Define the traffic that you want to inspect using the **class-map** command. You must configure separate class maps for HTTP and HTTPS traffic.
4. Enter the **policy-map** command to define the policy.
5. For HTTP, enter the **class** command to reference the HTTP class map.
6. Enter the **inspect scansafe** command, referencing the HTTP inspection policy map.
7. For HTTPS, enter the **class** command to reference the HTTPS class map.
8. Enter the **inspect scansafe** command, referencing the HTTPS inspection policy map.
9. Finally, apply the policy map to an interface using the **service-policy** command.

Examples

The following example configures two classes: one for HTTP and one for HTTPS. Each ACL exempts traffic to www.cisco.com and to tools.cisco.com, and to the DMZ network, for both HTTP and HTTPS. All other traffic is sent to Cloud Web Security, except for traffic from several whitelisted users and groups. The policy is then applied to the inside interface.

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443
ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS
```

```
ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

inspect sctp

To enable or disable Stream Control Transmission Protocol (SCTP) inspection, use the **inspect sctp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to disable SCTP inspection.

inspect sctp [*map_name*]
no inspect sctp [*map_name*]

Note SCTP inspection requires the Carrier license.

Syntax Description

map_name (Optional) Name for the SCTP inspection policy map.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

SCTP (Stream Control Transmission Protocol) supports the telephony signaling protocol SS7 and is also a transport protocol for several interfaces in the 4G LTE mobile network architecture. You would use SCTP inspection along with GTP and Diameter inspection if you have mobile network traffic going through the device.

You can optionally specify an SCTP policy map if you want to filter on SCTP applications to provide variable services. You can selectively drop, log, or rate limit SCTP traffic classes based on the payload protocol identifier (PPID). Use the **policy-map type inspect sctp** command to create the policy map.

Examples

The following example creates an inspection policy map that will drop unassigned PPIDs (unassigned at the time this example was written), rate limit PPIDs 32-40, and log the Diameter PPID. The service policy applies the inspection to the inspection_default class, which matches all SCTP traffic.

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
```

```
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
policy-map global_policy
 class inspection_default
  inspect sctp sctp-pmap
!
service-policy global_policy global
```

Related Commands

Commands	Description
class	Defines the traffic class to which to apply security actions.
clear service-policy inspect sctp	Clears global SCTP statistics.
policy-map type inspect	Creates an inspection policy map.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect sctp	Shows that status and statistics of the inspect sctp policy.

inspect sip

To enable SIP application inspection or to change the ports to which the ASA listens, use the inspect **sip** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]
no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the specified inspection session.
sip_map	Specifies a SIP policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the specified inspection session. The keyword **tls-proxy** cannot be used as a Layer 7 policy map name.
uc-ime *proxy_name*	Enable the Cisco Intercompany Media Engine Proxy for SIP inspection.

Command Default

SIP inspection is enabled by default using the default inspection map, which includes the following:

- SIP instant messaging (IM) extensions: Enabled.
- Non-SIP traffic on SIP port: Permitted.
- Hide server's and endpoint's IP addresses: Disabled.
- Mask software version and non-SIP URIs: Disabled.
- Ensure that the number of hops to destination is greater than 0: Enabled.
- RTP conformance: Not enforced.
- SIP conformance: Do not perform state checking and header validation.

Also note that inspection of encrypted traffic is not enabled. You must configure a TLS proxy to inspect encrypted traffic.

The default port assignment for SIP is 5060.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.
8.0(2)	The tls-proxy keyword was added.
9.4(1)	The **phone-proxy** and **uc-ime** keywords were removed.

Usage Guidelines

SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.

SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks. It also supports application security and protocol conformance, which enforce the sanity of the SIP messages, as well as detect SIP-based attacks.

SIP inspection is enabled by default. You need to configure it only if you want non-default processing, or if you want to identify a TLS proxy to enable encrypted traffic inspection.

To support SIP calls through the ASA, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

Limitations for SIP Inspection

SIP inspection applies NAT for embedded IP addresses. However, if you configure NAT to translate both source and destination addresses, the external address ("from" in the SIP header for the "trying" response message) is not rewritten. Thus, you should use object NAT when working with SIP traffic so that you avoid translating the destination address.

The following limitations and restrictions apply when using PAT with SIP:

- If a remote endpoint tries to register with a SIP proxy on a network protected by the ASA, the registration fails under very specific conditions, as follows:
  - PAT is configured for the remote endpoint.
  - The SIP registrar server is on the outside network.
  - The port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.
- If a SIP device transmits a packet in which the SDP portion has an IP address in the owner/creator field (o=) that is different than the IP address in the connection field (c=), the IP address in the o= field may not be properly translated. This is due to a limitation in the SIP protocol, which does not provide a port value in the o= field.
- When using PAT, any SIP header field which contains an internal IP address without a port might not be translated and hence the internal IP address will be leaked outside. If you want to avoid this leakage, configure NAT instead of PAT.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect sip** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect sip** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect sip** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the SIP inspection engine, which creates a class map to match SIP traffic on the default port (5060). The service policy is then applied to the outside interface. To enable SIP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map sip-port
ciscoasa(config-cmap)# match port tcp eq 5060
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sip_policy

ciscoasa(config-pmap)# class sip-port
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sip_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map type inspect sip	Creates an inspection policy map for SIP.
show sip	Displays information about SIP sessions established through the ASA.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect skinny

To enable SCCP (Skinny) application inspection, use the inspect **skinny** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]
no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the inspection session.
skinny_map	Specifies a skinny policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the inspection session.

Command Default

SCCP inspection is enabled by default using these defaults:

- Registration: Not enforced.
- Maximum message ID: 0x181.
- Minimum prefix length: 4
- Media timeout: 00:05:00
- Signaling timeout: 01:00:00.
- RTP conformance: Not enforced.

Also note that inspection of encrypted traffic is not enabled. You must configure a TLS proxy to inspect encrypted traffic.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.
8.0(2)	The keyword **tls-proxy** was added.
9.4(1)	The **phone-proxy** keyword was deprecated.

Release	Modification
9.13(1)	The **tls-proxy** keyword was deprecated. The keyword will be removed in a future release.
9.14(1)	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was removed.

Usage Guidelines

Skinny (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323 compliant terminals.

The ASA supports PAT and NAT for SCCP. PAT is necessary if you have more IP phones than global IP addresses for the IP phones to use. By supporting NAT and PAT of SCCP Signaling packets, Skinny application inspection ensures that all SCCP signaling and media packets can traverse the ASA.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The ASA also supports DHCP options 150 and 66, which it accomplishes by sending the location of a TFTP server to Cisco IP Phones and other DHCP clients. Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

Note The ASA supports inspection of traffic from Cisco IP Phones running SCCP protocol version 22 and earlier.

Supporting Cisco IP Phones

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be static as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An static identity entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an ACL to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an identity static entry. When using NAT, an identity static entry maps to the same IP address. When using PAT, it maps to the same IP address and port.

When the Cisco IP Phones are on a higher security interface compared to the TFTP server and Cisco CallManager, no ACL or static entry is required to allow the Cisco IP Phones to initiate the connection.

Restrictions and Limitations

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones fail because the ASA currently does not support NAT or PAT for the file content transferred over TFTP. Although the ASA supports NAT of TFTP messages and opens a pinhole for the TFTP file, the ASA cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone configuration files that are transferred by TFTP during phone registration.

Note The ASA supports stateful failover of SCCP calls except for calls that are in the middle of call setup.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect skinny** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect skinny** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect skinny** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the SCCP inspection engine, which creates a class map to match SCCP traffic on the default port (2000). The service policy is then applied to the outside interface. To enable SCCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map skinny-port
ciscoasa(config-cmap)# match port tcp eq 2000
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map skinny_policy

ciscoasa(config-pmap)# class skinny-port
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy skinny_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map type inspect skinny	Creates an inspection policy map for SCCP.
show skinny	Displays information about SCCP sessions established through the ASA.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect snmp

To enable SNMP application inspection or to change the ports to which the ASA listens, use the inspect **snmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect snmp [*map_name*]
no inspect snmp [*map_name*]

Syntax Description

map_name	The name of the SNMP map.

Command Default

This command is enabled by default starting in 9.14(1). It is disabled by default in previous releases.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.14(1)	The command enabled by default, and the SNMP map was made optional.

Usage Guidelines

Starting with 9.14(1), SNMP application inspection is applied to both to-the-device and through-the-device traffic. This inspection is necessary if you configure SNMP v3 where users are limited to specific SNMP hosts. Without the inspection, a defined v3 user can poll the device from any allowed host. SNMP inspection is enabled by default for the default ports, so you need to configure it only if you use non-default ports. The default ports are UDP/161, 162 (for all device types) and UDP/4161 for devices that also run Secure Firewall eXtensible Operating System (FXOS), as FXOS listens on UDP/161.

In releases previous to 9.14(1), SNMP inspection is not enabled by default, and it applies to through-the-box traffic only.

SNMP application inspection also lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The system can deny SNMP versions 1, 2, 2c, or 3. To deny a specific version of SNMP, use the **deny version** command within an SNMP map, which you create using the **snmp-map** command. After configuring the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

Starting with 9.14(1), if you do not need to control the versions, simply enable SNMP inspection without a map. In previous versions, a map is required.

Examples

The following example identifies SNMP traffic, defines an SNMP map, defines a policy, enables SNMP inspection, and applies the policy to the outside interface:

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sqlnet

To enable Oracle SQL*Net application inspection, use the inspect **sqlnet** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sqlnet
no inspect sqlnet

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

The default port assignment is 1521.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The SQL*Net protocol consists of different packet types that the ASA handles to make the data stream appear consistent to the Oracle applications on either side of the ASA.

The default port assignment for SQL*Net is 1521. This is the value used by Oracle for SQL*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL*Net inspection to a range of port numbers.

Note Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The ASA acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

The ASA NATs all addresses and looks in the packets for all embedded ports to open for SQL*Net Version 1.

For SQL*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the ASA, a flag will be set in the connection data structure to expect the Data or Redirect message that follows to be NATed and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be NATed and port connections will be opened.

Examples

The following example enables the SQL*Net inspection engine, which creates a class map to match SQL*Net traffic on the default port (1521). The service policy is then applied to the outside interface. To enable SQL*Net inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map sqlnet-port
ciscoasa(config-cmap)# match port tcp eq 1521
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sqlnet_policy

ciscoasa(config-pmap)# class sqlnet-port
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sqlnet_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*net.

inspect stun

To enable Session Traversal Utilities for NAT (STUN) application inspection, use the inspect **stun** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect stun
no inspect stun

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

The default port assignment is TCP/3478 and UDP/3478.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Session Traversal Utilities for NAT (STUN), defined in RFC 5389, is used by WebRTC clients for browser-based real-time communications so that plug-ins are not necessary. WebRTC clients often use cloud STUN servers to learn their public IP addresses and ports. WebRTC uses Interactive Connectivity Establishment (ICE, RFC 5245) to verify connectivity between clients. These clients typically use UDP, although they can also use TCP or other protocols.

Because firewalls often block outgoing UDP traffic, WebRTC products such as Cisco Spark can have problems completing connections. STUN inspection opens pinholes for STUN endpoints, and enforces basic STUN and ICE compliance, to allow communications for clients if the connectivity check is acknowledged by both sides. Thus, you can avoid opening new ports in your access rules to enable these applications.

When you enable STUN inspection on the default inspection class, TCP/UDP port 3478 is watched for STUN traffic. The inspection supports IPv4 addresses and TCP/UDP only.

There are some NAT limitations for STUN inspection. For WebRTC traffic, static NAT/PAT44 are supported. Cisco Spark can support additional types of NAT, because Spark does not require pinholes. You can also use NAT/PAT64, including dynamic NAT/PAT with Cisco Spark.

STUN inspection is supported in failover and cluster modes, as pinholes are replicated. However, the transaction ID is not replicated among units. In the case where a unit fails after receiving a STUN Request and another unit received the STUN Response, the STUN Response will be dropped.

Examples

The following example enables STUN inspection as part of the default global inspection rule.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect stun
ciscoasa(config)# service-policy global_policy global
```

Related Commands

Commands	Description
class	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including STUN.
show service-policy inspect diameter	Shows the status and statistics of the inspect diameter policy.

inspect sunrpc

To enable Sun RPC application inspection or to change the ports to which the ASA listens, use the inspect sunrpc command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sunrpc
no inspect sunrpc

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

To enable Sun RPC application inspection or to change the ports to which the ASA listens, use the inspect sunrpc command in policy map class configuration mode, which is accessible by using the **class** command within policy map configuration mode. To remove the configuration, use the **no** form of this command.

The **inspect sunrpc** command enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port on the system. When a client attempts to access an Sun RPC service on a server, it must find out which port that service is running on. It does this by querying the portmapper process on the well-known port of 111.

The client sends the Sun RPC program number of the service, and gets back the port number. From this point on, the client program sends its Sun RPC queries to that new port. When a server sends out a reply, the ASA intercepts this packet and opens both embryonic TCP and UDP connections on that port.

Note NAT or PAT of Sun RPC payload information is not supported.

Examples

The following example enables the RPC inspection engine, which creates a class map to match RPC traffic on the default port (111). The service policy is then applied to the outside interface. To enable RPC inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map sunrpc-port
ciscoasa(config-cmap)# match port tcp eq 111
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sample_policy
ciscoasa(config-pmap)# class sunrpc-port
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sample_policy interface outside
```

Related Commands

Commands	Description
clear configure sunrpc_server	Removes the configuration performed using the **sunrpc-server** command.
clear sunrpc-server active	Clears the pinholes that are opened by Sun RPC application inspection for specific services, such as NFS or NIS.
show running-config sunrpc-server	Displays the information about the Sun RPC service table configuration.
sunrpc-server	Allows pinholes to be created with a specified timeout for Sun RPC services, such as NFS or NIS.
show sunrpc-server active	Displays the pinholes open for Sun RPC services.

inspect tftp

To disable TFTP application inspection, or to enable it if it has been previously disabled, use the inspect **tftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect tftp
no inspect tftp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

The default port assignment is 69.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

Trivial File Transfer Protocol (TFTP), described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The ASA inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

Examples

The following example enables the TFTP inspection engine, which creates a class map to match TFTP traffic on the default port (69). The service policy is then applied to the outside interface. To enable TFTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map tftp-port
ciscoasa(config-cmap)# match port udp eq 69
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map tftp_policy

ciscoasa(config-pmap)# class tftp-port
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy tftp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect vxlan

To enable Virtual Extensible Local Area Network (VXLAN) application inspection, use the **inspect vxlan** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect vxlan
no inspect vxlan

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

The default port assignment is UDP/4789.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Virtual Extensible Local Area Network (VXLAN) inspection works on VXLAN encapsulated traffic that passes through the ASA. It ensures that the VXLAN header format conforms to standards, dropping any malformed packets. VXLAN inspection is not done on traffic for which the ASA acts as a VXLAN Tunnel End Point (VTEP) or a VXLAN gateway, as those checks are done as a normal part of decapsulating VXLAN packets.

VXLAN packets are UDP, normally on port 4789. This port is part of the default-inspection-traffic class, so you can simply add VXLAN inspection to the inspection_default global service policy rule. Alternatively, you can create a class for it using port or ACL matching.

Examples

The following example enables VXLAN inspection as part of the global inspection default rule.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect vxlan
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect waas

To enable WAAS application inspection, use the **inspect waas** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect waas
no inspect waas

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enable WAAS application inspection on the default inspection class.

```
policy-map global_policy
 class inspection_default
  inspect waas
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect xdmcp

To enable XDMCP application inspection or to change the ports to which the ASA listens, use the **inspect xdmcp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect xdmcp
no inspect xdmcp

Syntax Description

This command has no arguments or keywords.

Command Default

Starting with 9.16, this command is disabled by default. In prior releases, it was enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added. It replaced the **fixup** command, which has been deprecated.

Usage Guidelines

The inspect **xdmcp** command enables or disables application inspection for the XDMCP protocol.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the ASA must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the ASA. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting:

```
setenv DISPLAY Xserver:n
```

where *n* is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the ASA can NAT if needed. XDCMP inspection does not support PAT.

Examples

The following example enables the XDMCP inspection engine, which creates a class map to match XDMCP traffic on the default port (177). The service policy is then applied to the outside interface.

To enable XDMCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

```
ciscoasa(config)# class-map xdmcp-port
ciscoasa(config-cmap)# match port tcp eq 177
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map xdmcp_policy

ciscoasa(config-pmap)# class xdmcp-port
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy xdmcp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

int – ipu

integrity

To specify the ESP integrity algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the integrity command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

integrity { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }
no integrity { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }

Syntax Description

md5	Specifies the MD5 algorithm for the ESP integrity protection.
null	Allows an administrator to choose null as the IKEv2 integrity algorithm when AES-GCM is specified as the encryption algorithm.
sha	(Default) Specifies the Secure Hash Algorithm (SHA) SHA 1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection.
sha256	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Command Default

The default is **sha (**SHA 1 algorithm).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **integrity** command to set the integrity algorithm for the ESP protocol.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
8.4(2)	The sha256, sha384, and sha512 keywords were added for SHA 2 support.
9.0(1)	The null option as an IKEv2 integrity algorithm was added.

Examples

The following example enters IKEv2 policy configuration mode and sets the integrity algorithm to MD5:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.

intercept-dhcp

To enable DHCP Intercept, use the **intercept-dhcp enable** command in group-policy configuration mode. To remove the **intercept-dhcp** attribute from the running configuration and allow the users to inherit a DHCP Intercept configuration from the default or other group policy, use the **no** form of this command.

intercept-dhcp *netmask* { **enable** | **disable** }
no intercept-dhcp

Syntax Description

disable	Disables DHCP Intercept.
enable	Enables DHCP Intercept.
netmask	Provides the subnet mask for the tunnel IP address.

Command Default

DHCP Intercept is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To disable DHCP Intercept, use the **intercept-dhcp disable** command.

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the ASA limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

DHCP Intercept lets Microsoft XP clients use split-tunneling with the ASA. The ASA replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.

Examples

The following example shows how to set DHCP Intercepts for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# intercept-dhcp enable
```

interface (global)

To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode. To remove a subinterface, use the **no** form of this command; you cannot remove a physical interface or a mapped interface.

For physical interfaces (for all models except the ASASM):

interface *physical_interface*
For subinterfaces (not available for the ASA 5505 or the ASASM, or for the Management interface on the ASA 5506-X through ASA 5555-X):

interface { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*
no interface { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*

For multiple context mode when a mapped name is assigned:

interface *mapped_name*

Syntax Description

mapped_name	In multiple context mode, specifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Specifies the physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional. The physical interface types include the following: • **ethernet** • gigabitethernet • **tengigabitethernet** • **management** Enter the type followed by slot/port, for example, **gigabitethernet 0/1**. The management interface is meant for management traffic only. You can, however, use it for through traffic if desired, depending on your model (see the **management-only** command). See the hardware documentation that came with your model to identify the interface type, slot, and port number.
subinterface	Specifies an integer between 1 and 4294967293 designating a logical subinterface. The maximum number of subinterfaces varies depending on your ASA model. Subinterfaces are not available for the ASA 5505, ASASM, or for the management interface on the ASA 5512-X through ASA 5555-X. See the configuration guide for the maximum subinterfaces (or VLANs) per platform. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk.

Command Default

By default, the ASA automatically generates **interface** commands for all physical interfaces.

In multiple context mode, the ASA automatically generates **interface** commands for all interfaces allocated to the context using the **allocate-interface** command.

The default state of an interface depends on the type and the context mode:

- Multiple context mode, context—All allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.
- Single mode or multiple context mode, system—Interfaces have the following default states:
  - Physical interfaces—Disabled.
  - Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to allow for new subinterface naming conventions and to change arguments to be separate commands under interface configuration mode.

Usage Guidelines

In interface configuration mode, you can configure hardware settings (for physical interfaces), assign a name, assign a VLAN, assign an IP address, and configure many other settings, depending on the type of interface and the security context mode.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For subinterfaces, also configure the **vlan** command.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

The Management 0/0 interface on the ASA 5512-X through ASA 5555-X has the following characteristics:

- No through traffic support
- No subinterface support
- No priority queue support
- No multicast MAC support
- The IPS SSP software module shares the Management 0/0 interface. Separate MAC addresses and IP addresses are supported for the ASA and IPS module. You must perform configuration of the IPS IP

address within the IPS operating system. However, physical characteristics (such as enabling the interface) are configured on the ASA.

Examples

The following example configures parameters for the physical interface in single mode:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

The following example configures parameters for a subinterface in single mode:

```
ciscoasa(config)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# no
shutdown
ciscoasa(config-if)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# no shutdown
ciscoasa(config-subif)# context contextA
ciscoasa(config-ctx)# ...
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
member-interface	Assigns interfaces to a redundant interface.
clear interface	Clears counters for the **show interface** command.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN to a subinterface.

interface (vpn load-balancing)

To specify a non-default public or private interface for VPN load-balancing in the VPN load-balancing virtual cluster, use the **interface** command in vpn load-balancing mode. To remove the interface specification and revert to thte default interface, use the **no** form of this command.

interface { **lbprivate** | **lbpublic** } *interface-name*
interface { **lbprivate** | **lbpublic** }

Syntax Description

interface-name	The name of the interface to be configured as the public or private interface for the VPN load-balancing cluster.
lbprivate	Specifies that this command configures the private interface for VPN load-balancing.
lbpublic	Specifies that this command configures the public interface for VPN load-balancing.

Command Default

If you omit the **interface** command, the **lbprivate** interface defaults to **inside**, and the **lbpublic** interface defaults to **outside**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
vpn load-balancing	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must have first used the **vpn load-balancing** command to enter vpn load-balancing configuration mode.

You must also have previously used the **interface**, **ip address** and **nameif** commands to configure and assign a name to the interface that you are specifying in this command.

Examples

The following is an example of a **vpn load-balancing** command sequence that includes an **interface** command that specifies the public interface of the cluster as “test” one that reverts the private interface of the cluster to the default (inside):

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
```

```
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# no
 interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

ciscoasa(config-load-balancing)# **participate**

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing configuration mode.

interface bvi

To configure the bridge virtual interface (BVI) for a bridge group, use the **interface bvi** command in global configuration mode. To remove the BVI configuration, use the **no** form of this command.

interface bvi *bridge_group_number*
no interface bvi *bridge_group_number*

Syntax Description

bridge_group_number	Specifies the bridge group number as an integer between 1 and 100; for 9.3(1) and later, the range is increased to between 1 and 250.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(1)	The number range was increased to between 1 and 250 to support 250 BVIs.
9.6(2)	The maximum interfaces per bridge group was increased from 4 to 64.

Usage Guidelines

Use this command to enter interface configuration mode so you can configure a management IP address for the bridge group. If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context. At least one bridge group is required per context or in single mode.

Each bridge group requires a management IP address. The ASA uses this IP address as the source address for packets originating from the bridge group. The management IP address must be on the same subnet as the connected network. For IPv4 traffic, the management IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

For another method of management, you can configure the Management interface, separate from any bridge groups.

For 9.2 and earlier, You can configure up to 8 bridge groups in single mode or per context in multiple mode; for 9.3(1) and later, you can configure up to 250 bridge groups. Each bridge group can include up to 4 interfaces. In 9.6(2) and later, you can add up to 64 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.

Note Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group.

Note For a separate management interface, a non-configurable bridge group (ID 301) is automatically added to your configuration. This bridge group is not included in the bridge group limit.

Note The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

Examples

The following example includes two bridge groups of three interfaces each, plus a management-only interface:

```
interface gigabitethernet 0/0
nameif inside
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside
security-level 0
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
nameif inside
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
nameif dmz
```

```
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

Related Commands

Command	Description
ace/bvi	Clears the bridge virtual interface configuration.
bridge-group	Groups transparent firewall interfaces into a bridge group.
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.
show bridge-group	Shows bridge group information, including member interfaces and IP addresses.
show running-config interface bvi	Shows the bridge group interface configuration.

interface loopback

To create a loopback interface, use the **interface loopback** command in the global configuration mode. Use the **no** form of the command to remove the loopback interface.

interface loopback *number*
no interface loopback *number*

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Usage Guidelines

A loopback interface is software-only interface that emulates a physical interface. The loopback interface is reachable through multiple physical interfaces. You can only use a loopback interface for to/from the device traffic.

The following features support the loopback interface:

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- Syslog
- Telnet
- VTI source interface

Command History

Release	Modification
9.18(2)	This command was added.
9.19(1)	Support for VTI was added.

Release	Modification
9.20(1)	Support for DNS, HTTP, and ICMP was added.

Examples

The following example creates a new loopback interface:

```
ciscoasa(config)# interface loopback 10
```

Related Commands

Command	Description
tunnel source interface	Specifies the source interface to create a VTI tunnel.
ssh	Configures SSH for an interface.
logging host	Specifies the syslog host.
neighbor update-source	Configures an interface as the source for a BGP-speaking neighbor.
snmp-server host	Specifies the SNMP server.
telnet	Configures Telnet for an interface.

interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **interface-policy** command in failover group configuration mode. To restore the default values, use the **no** form of this command.

interface-policy *num* [**%**]
no interface-policy *num* [**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Command Default

If the **failover interface-policy** command is configured for the unit, then the default for the **interface-policy failover group** command assumes that value. If not, then *num* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group Configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other ASA is functioning correctly, the ASA will mark itself as failed and a failover may occur (if the active ASA is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Examples

The following partial example shows a possible configuration for a failover group:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover interface-policy	Configures the interface monitoring policy.
monitor-interface	Specifies the interfaces being monitored for failover.

interface port-channel

To configure an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command in global configuration mode. To remove an EtherChannel interface, use the **no** form of this command.

interfaceport-channel*number*
no interface port-channel *number*

Syntax Description

number Specifies the EtherChannel channel group ID, between 1 and 48. This interface was created automatically when you added an interface to the channel group. If you have not yet added an interface, then this command creates the port-channel interface.

Note You need to add at least one member interface to the port-channel interface before you can configure logical parameters for it, such as a name.

Command Default

By default, port-channel interfaces are enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Note This command is not supported on the ASA 5505 or the ASASM. You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel.

For more information about interfaces, see the CLI configuration guide.

Examples

The following example configures three interfaces as part of an EtherChannel. It also sets the system priority to be a higher priority, and GigabitEthernet 0/2 to be a higher priority than the other interfaces in case more than eight interfaces are assigned to the EtherChannel.

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

interface redundant

To configure a redundant interface and enter interface configuration mode, use the **interface redundant** command in global configuration mode. To remove a redundant interface, use the **no** form of this command.

interface redundant *number*
no interface redundant *number*

Syntax Description

number	Specifies a logical redundant interface ID, between 1 and 8. A space between **redundant** and the ID is optional.

Command Default

By default, redundant interfaces are enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

A redundant interface pairs an active and a standby physical interface (see the **member-interface** command). When the active interface fails, the standby interface becomes active and starts passing traffic.

All ASA configuration refers to the logical redundant interface instead of the member physical interfaces.

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Note This command is not supported on the ASA 5505 or the ASASM.

For more information about interfaces, see the CLI configuration guide.

Examples

The following example creates two redundant interfaces:

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
member-interface	Assigns a physical interface to a redundant interface.
redundant-interface	Changes the active member interface.
show interface	Displays the runtime status and statistics of interfaces.

interface tunnel

To create a new VTI tunnel interface, use the **interface tunnel** command in the Global Configuration mode. Use the no form of the command to remove the VTI tunnel interface.

interface tunnel *number*
no interface tunnel *number*

Syntax Description

number	Assigns a number to the tunnel interface. This can be any value between 0-1024.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• No	• Yes	• No	• -

Command History

Release	Modification
9.7(1)	We introduced this command and its submodes.
9.16(1)	The number of tunnel interfaces supported was increased from 100 to 1024 per device.

Examples

The following example creates a new tunnel interface:

```
ciscoasa(config)# interface tunnel 10
```

Related Commands

Command	Description
tunnel source interface	Specifies the source interface to create a VTI tunnel.
tunnel destination	Specifies the IP address of the VTI tunnel's destination.
tunnel mode	Specifies that IPsec is used for tunnel protection.
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

interface vlan

For the ASA 5505 and ASASM, to configure a VLAN interface and enter interface configuration mode, use the **interface vlan** command in global configuration mode. To remove a VLAN interface, use the **no** form of this command.

interface vlan *number*
no interface vlan *number*

Syntax Description

number Specifies a VLAN ID.

For the ASA 5505, use an ID between 1 and 4090. The VLAN interface ID is enabled by default on VLAN 1.

For the ASASM, use an ID between 2 to 1000 and from 1025 to 4094.

Command Default

By default, VLAN interfaces are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
8.4(1)	ASASM support was added.

Usage Guidelines

For the ASASM, you can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the **show vlan** command. If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the **show interface** command for more information about interface states.

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For the ASA 5505 switch physical interfaces, assign the physical interface to the VLAN interface using the **switchport access vlan** command.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

For more information about interfaces, see the CLI configuration guide.

Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

The following example configures five VLAN interfaces, including the failover interface, which is configured separately using the **failover lan** command:

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
show interface	Displays the runtime status and statistics of interfaces.

interface vni

To configure a VXLAN Network Identifier (VNI) interface and enter interface configuration mode, use the **interface vni** command in global configuration mode. To remove a VNI interface, use the **no** form of this command.

interface vni *number*
no interface vni *number*

Syntax Description

number	Sets the ID between 1 and 10000. This ID is only an internal interface identifier.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

You must associate a VNI interface with a VTEP source interface using the **vtep-nve** command. You must also set the VXLAN **segment-id**.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and associates the VNI 1 interface wth it:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

interim-accounting-update

To enable the generation of RADIUS interim-accounting-update messages for the AAA server group, use the **interim-accounting-update** command in aaa-server group configuration mode. To disable interim-accounting-update messages, use the **no** form of this command.

interim-accounting-update [**periodic** [*hours*]]
no interim-accounting-update [**periodic** [*hours*]]

Syntax Description

periodic [*hours*]	(Optional) Enables the periodic generation and transmission of accounting records for every VPN session that is configured to send accounting records to the server group in question. You can optionally include the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120. Use this option for a server group configured for ISE Change of Authentication.

Command Default

By default interim-accounting-update is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	The **periodic** keyword was added.

Usage Guidelines

If you use this command without the **periodic** keyword, the ASA sends interim-accounting-update messages only when a VPN tunnel connection is added to a clientless VPN session. When this happens the accounting update is generated in order to inform the RADIUS server of the newly assigned IP address.

If you are using the server group to configure ISE Change of Authorization for a remote access VPN, add the **periodic** keyword. Period reporting includes AnyConnect connections as well as clientless sessions.

ISE maintains a directory of active sessions based on the accounting records that it receives from NAS devices like the ASA. However, if ISE does not receive any indication that the session is still active accounting message or posture transactions) for a period of 5 days, it will remove the session record from its database. To ensure that long-lived VPN connections are not removed, configure the group to send periodic interim-accounting-update messages to ISE for all active sessions.

Examples

The following example shows how to configure an ISE server group for dynamic authorization (CoA) updates and hourly periodic accounting. Included is the tunnel group configuration that configures password authentication with ISE.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. In this case, you include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

Command	Description
authorize-only	Enables authorize-only mode for the RADIUS server group.
dynamic-authorization	Enables dynamic authorization for the RADIUS server group.

internal-password

To display an additional password field on the clientless SSL VPN portal page, use the **internal-password** command in webvpn configuration mode. This additional password is used by the ASA to authenticate users to file servers for whom SSO is allowed.

To disable the ability to use an internal password, use the **no** version of the command.

internal-passwordenable
no internal password

Syntax Description

enable	Enables use of an internal password.

Command Default

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If enabled, end users type a second password when logging in to a clientless SSL VPN session. The clientless SSL VPN server sends an SSO authentication request, including the username and password, to the authenticating server using HTTPS. If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN server. This cookie is kept on the ASA on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

The internal password feature is useful if you require that the internal password be different from the SSL VPN password. In particular, you can use one-time passwords for authentication to the ASA, and another password for internal sites.

Examples

The following example shows how to enable the internal password:

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 internal password enable
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn configuration mode, which lets you configure attributes for clientless SSL VPN connections.

internal-port

To specify the VXLAN internal port for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **internal-port** command in interface configuration mode. To remove the port, use the **no** form of this command.

internal-port *port*
no internal-port *port*

Syntax Description

port Sets the port between 1024 and 65535.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

internal-segment-id

To specify the VXLAN internal segment ID for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **internal-segment-id** command in interface configuration mode. To remove the ID, use the **no** form of this command.

internal-segment-id *id*
no internal-segment-id *id*

Syntax Description

id	Sets the ID between 1 and 16777215.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
proxy paired	Sets the interface to paired proxy mode.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

interval maximum

To configure the maximum interval between update attempts by a DDNS update method, use the **interval** command in DDNS-update-method mode. To remove an interval for a DDNS update method from the running configuration, use the **no** form of this command.

interval maximum *days hours minutes seconds*
no interval maximum *days hours minutes seconds*

Syntax Description

days	Specifies the number of days between update attempts with a range of 0 to 364.
hours	Specifies the number of hours between update attempts with a range of 0 to 23.
minutes	Specifies the number of minutes between update attempts with a range of 0 to 59.
seconds	Specifies the number of seconds between update attempts with a range of 0 to 59.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ddns-update-method configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The days, hours, minutes, and seconds are added together to arrive at the total interval.

Examples

The following example configures a method called ddns-2 to attempt an update every 3 minutes and 15 seconds:

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.

Command	Description
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.

invalid-ack

To set the action for packets with an invalid ACK, use the **invalid-ack** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

invalid-ack { **allow** | **drop** }
no invalid-ack

Syntax Description

allow	Allows packets with an invalid ACK.
drop	Drops packets with an invalid ACK.

Command Default

The default action is to drop packets with an invalid ACK.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **invalid-ack**—In tcp-map configuration mode, you can enter the **invalid-ack** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the TCP map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

You might see invalid ACKs in the following instances:

- In the TCP connection SYN-ACK-received status, if the ACK number of a received TCP packet is not exactly the same as the sequence number of the next TCP packet sending out, it is an invalid ACK.
- Whenever the ACK number of a received TCP packet is greater than the sequence number of the next TCP packet sending out, it is an invalid ACK.

Note TCP packets with an invalid ACK are automatically allowed for WAAS connections.

Examples

The following example sets the ASA to allow packets with an invalid ACK:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	Identifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

ip address

To set the IP address for an interface (in routed mode) or for the bridge virtual interface (BVI) (routed or transparent mode), use the **ip address** command in interface configuration mode. To remove the IP address, use the **no** form of this command.

ip address *ip_address* [*mask*] **standby** *ip_address* | **cluster-pool** *poolname*]
no ip address [*ip_address*]

Syntax Description

cluster-pool *poolname*	(Optional) For ASA clustering, sets the cluster pool of addresses defined by the **ip local pool** command. The main cluster IP address defined by the *ip_address* argument belongs to the current master unit only. Each cluster member receives a local IP address from this pool. You cannot determine the exact address assigned to each unit in advance; to see the address used on each unit, enter the **show ip local pool** *poolname* command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the local IP used from the pool.
ip_address	The IP address for the interface.
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the ASA uses the default mask for the IP address class.
standby *ip_address*	(Optional) For failover, sets the IP address for the standby unit.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.
8.4(1)	For transparent mode, bridge groups were added. You now set the IP address for the BVI, and not globally.
9.0(1)	The **cluster-pool** keyword was added to support ASA clustering.

Release	Modification
9.7(1)	For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections.

Usage Guidelines

This command also sets the standby address for failover.

Multiple Context Mode Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

Transparent Firewall Guidelines

A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

Failover Guidelines

The standby IP address must be on the same subnet as the main IP address.

ASA Clustering Guidelines

You can only set the cluster pool for an individual interface after you configure the cluster interface mode to be individual (**cluster-interface mode individual** command). The only exception is for the management-only interface(s):

- You can always configure the management-only interface as an individual interface, even in spanned EtherChannel mode. The management interface can be an individual interface even in transparent firewall mode.
- In spanned EtherChannel mode, if you configure the management interface as an individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.

/31 Subnet Guidelines

For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 ASAs only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog.

- 31-Bit Subnet and Clustering—You can use a 31-bit subnet mask for Spanned EtherChannels. Individual interfaces (including the Management IP address in Spanned EtherChannel mode) do not support a 31-bit subnet. You also cannot use the 31-bit subnet for the Cluster Control Link.
- 31-Bit Subnet and Failover—For failover, when you use a 31-bit subnet for the ASA interface IP address, you cannot configure a standby IP address for the interface because there are not enough addresses. Normally, an interface for failover should have a standby IP address so the active unit can perform

interface tests to ensure standby interface health. Without a standby IP address, the ASA cannot perform any network tests; only the link state can be tracked. For the failover and optional separate state link, which are point-to-point connections, you can also use a 31-bit subnet.

- 31-Bit Subnet and Management—If you have a directly-connected management station, you can use a point-to-point connection for SSH or HTTP on the ASA, or for SNMP or Syslog on the management station.
- 31-Bit Subnet Unsupported Features—The following features do not support the 31-Bit subnet:
  - BVI interfaces for bridge groups— The bridge group requires at least 3 host addresses: the BVI, and two hosts connected to two bridge group member interfaces. you must use a /29 subnet or smaller.
  - Multicast Routing

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

The following example sets the management address and standby address of bridge group 1:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
show ip address	Shows the IP address assigned to an interface.

ip address dhcp

To use DHCP to obtain an IP address for an interface, use the **ip address dhcp** command in interface configuration mode. To disable the DHCP client for this interface, use the **no** form of this command.

ip address dhcp [**setroute**]
no ip address dhcp

Syntax Description

setroute	(Optional) Allows the ASA to use the default route supplied by the DHCP server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was changed from a global configuration command to an interface configuration mode command. You can also enable this command on any interface, instead of only the outside interface.

Usage Guidelines

Reenter this command to reset the DHCP lease and request a new lease.

If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

Note The ASA rejects any leases that have a timeout of less than 32 seconds.

Examples

The following example enables DHCP on the Gigabitethernet0/1 interface:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
show ip address dhcp	Shows the IP address obtained from the DHCP server.

ip address pppoe

To enable PPPoE, use the **ip address pppoe** command in interface configuration mode. To disable PPPoE, use the **no** form of this command.

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]
no ip address [*ip_address* [*mask*]] **pppoe**

Syntax Description

ip_address	Manually sets the IP address instead of receiving an address from the PPPoE server.
mask	Specifies the subnet mask for the IP address. If you do not set the mask, the ASA uses the default mask for the IP address class.
setroute	Lets the ASA use the default route supplied by the PPPoE server. If the PPPoE server does not send a default route, the ASA creates a default route with the address of the access concentrator as the gateway.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

PPPoE combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.

Before you set the IP address using PPPoE, configure the **vpdn** commands to set the username, password, and authentication protocol. If you enable this command on more than one interface, for example for a backup link to your ISP, then you can assign each interface to a different VPDN group if necessary using the pppoe client vpdn group command.

The maximum transmission unit (MTU) size is automatically set to 1492 bytes, which is the correct value to allow PPPoE transmission within an Ethernet frame.

Reenter this command to reset and restart the PPPoE session.

You cannot set this command at the same time as the **ip address** command or the **ip address dhcp** command.

Examples

The following example enables PPPoE on the Gigabitethernet 0/1 interface:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

The following example manually sets the IP address for a PPPoE interface:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for an interface.
pppoe client vpdn group	Assigns this interface to a particular VPDN group.
show ip address pppoe	Shows the IP address obtained from the PPPoE server.
vpdn group	Creates a vpdn group and configures PPPoE client settings.

ip-address-privacy

To enable IP address privacy, use the **ip-address-privacy** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

ip-address-privacy
no ip-address-privacy

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enable IP address privacy over SIP in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.

ip audit attack

To set the default actions for packets that match an attack signature, use the **ip audit attack** command in global configuration mode. To restore the default action (to reset the connection), use the **no** form of this command.

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit attack

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the ASA takes no action. If you do not enter the **action** keyword, the ASA assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Command Default

The default action is to send and alarm.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can specify multiple actions, or no actions. You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an attack signature. The audit policy for the inside interface overrides this default to be alarm only, while the policy for the outside interface uses the default setting set with the **ip audit attack** command.

```
ciscoasa(config)# ip audit attack action alarm reset
ciscoasa(config)# ip audit name insidepolicy attack action alarm
```

```
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

ip audit info

To set the default actions for packets that match an informational signature, use the **ip audit info** command in global configuration mode. To restore the default action (to generate an alarm), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit info

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the ASA takes no action. If you do not enter the **action** keyword, the ASA assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Command Default

The default action is to generate an alarm.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an informational signature. The audit policy for the inside interface overrides this default to be alarm and drop, while the policy for the outside interface uses the default setting set with the **ip audit info** command.

```
ciscoasa(config)# ip audit info action alarm reset
```

```
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.
show running-config ip audit info	Shows the configuration for the **ip audit info** command.

ip audit interface

To assign an audit policy to an interface, use the **ip audit interface** command in global configuration mode. To remove the policy from the interface, use the **no** form of this command.

ip audit interface *interface_name policy_name*
no ip audit interface *interface_name policy_name*

Syntax Description

interface_name	Specifies the interface name.
policy_name	The name of the policy you added with the **ip audit name** command. You can assign an info policy and an attack policy to each interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example applies audit policies to the inside and outside interfaces:

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.
show running-config ip audit interface	Shows the configuration for the **ip audit interface** command.

ip audit name

To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the **ip audit name** command in global configuration mode. To remove the policy, use the **no** form of this command.

ip audit name *name* { **info** | **attack** } [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit name *name* { **info** | **attack** } [**action** [**alarm**] [**drop**] [**reset**]]

Syntax Description

action	(Optional) Specifies that you are defining a set of actions. If you do not follow this keyword with any actions, then the ASA takes no action. If you do not enter the **action** keyword, then the ASA uses the default action set by the **ip audit attack** and **ip audit info** commands.
alarm	(Optional) Generates a system message showing that a packet matched a signature.
attack	Creates an audit policy for attack signatures; the packet might be part of an attack on your network, such as a DoS attack or illegal FTP commands.
drop	(Optional) Drops the packet.
info	Creates an audit policy for informational signatures; the packet is not currently attacking your network, but could be part of an information-gathering activity, such as a port sweep.
name	Sets the name of the policy.
reset	(Optional) Drops the packet and closes the connection.

Command Default

If you do not change the default actions using the **ip audit attack** and **ip audit info** commands, then the default action for attack signatures and informational signatures is to generate an alarm.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. To apply the policy, assign it to an interface using the **ip audit interface** command. You can assign an info policy and an attack policy to each interface.

For a list of signatures, see the **ip audit signature** command.

If traffic matches a signature, and you want to take action against that traffic, use the **shun** command to prevent new connections from the offending host and to disallow packets from any existing connection.

Examples

The following example sets an audit policy for the inside interface to generate an alarm for attack and informational signatures, while the policy for the outside interface resets the connection for attacks:

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
shun	Blocks packets with a specific source and destination address.

ip audit signature

To disable a signature for an audit policy, use the **ip audit signature** command in global configuration mode. To reenable the signature, use the **no** form of this command.

ip audit signature *signature_number* **disable**
no ip audit signature *signature_number*

Syntax Description

disable	Disables the signature.
signature_number	Specifies the signature number to disable. See Table 2: Signature IDs and System Message Numbers for a list of supported signatures.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms. Table 2: Signature IDs and System Message Numbers lists supported signatures and system message numbers.

Table 2: Signature IDs and System Message Numbers

Signature ID	Message Number	Signature Title	Signature Type	Description
1000	400000	IP options-Bad Option List	Informational	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001	400001	IP options-Record Packet Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).

Signature ID	Message Number	Signature Title	Signature Type	Description
1002	400002	IP options-Timestamp	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003	400003	IP options-Security	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004	400004	IP options-Loose Source Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005	400005	IP options-SATNET ID	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006	400006	IP options-Strict Source Route	Informational	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100	400007	IP Fragment Attack	Attack	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
1102	400008	IP Impossible Packet	Attack	Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1103	400009	IP Overlapping Fragments (Teardrop)	Attack	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.
2000	400010	ICMP Echo Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
2001	400011	ICMP Host Unreachable	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).
2002	400012	ICMP Source Quench	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).

Signature ID	Message Number	Signature Title	Signature Type	Description
2003	400013	ICMP Redirect	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004	400014	ICMP Echo Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005	400015	ICMP Time Exceeded for a Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006	400016	ICMP Parameter Problem on Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
2007	400017	ICMP Timestamp Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
2008	400018	ICMP Timestamp Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009	400019	ICMP Information Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010	400020	ICMP Information Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011	400021	ICMP Address Mask Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012	400022	ICMP Address Mask Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).
2150	400023	Fragmented ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.
2151	400024	Large ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.

Signature ID	Message Number	Signature Title	Signature Type	Description
2154	400025	Ping of Death Attack	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3040	400026	TCP NULL flags	Attack	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3041	400027	TCP SYN+FIN flags	Attack	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3042	400028	TCP FIN only flags	Attack	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3153	400029	FTP Improper Address Specified	Informational	Triggers if a port command is issued with an address that is not the same as the requesting host.
3154	400030	FTP Improper Port Specified	Informational	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
4050	400031	UDP Bomb attack	Attack	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
4051	400032	UDP Snork attack	Attack	Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052	400033	UDP Chargen DoS attack	Attack	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
6050	400034	DNS HINFO Request	Informational	Triggers on an attempt to access HINFO records from a DNS server.
6051	400035	DNS Zone Transfer	Informational	Triggers on normal DNS zone transfers, in which the source port is 53.
6052	400036	DNS Zone Transfer from High Port	Informational	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053	400037	DNS Request for All Records	Informational	Triggers on a DNS request for all records.
6100	400038	RPC Port Registration	Informational	Triggers when attempts are made to register new RPC services on a target host.
6101	400039	RPC Port Unregistration	Informational	Triggers when attempts are made to unregister existing RPC services on a target host.

Signature ID	Message Number	Signature Title	Signature Type	Description
6102	400040	RPC Dump	Informational	Triggers when an RPC dump request is issued to a target host.
6103	400041	Proxied RPC Request	Attack	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155	400047	mountd (mount daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.
6180	400049	rexd (remote execution daemon) Attempt	Informational	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
6190	400050	statd Buffer Overflow	Attack	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Examples

The following example disables signature 6100:

```
ciscoasa(config)# ip audit signature 6100 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit signature	Shows the configuration for the **ip audit signature** command.

ip-client

To allow FXOS to initiate management traffic and send it out of a Firepower 2100 ASA data interface, use the **ip-client** command in global configuration mode. To disable traffic initiation, use the **no** form of this command.

ip-client*interface_name*
no ip-client *interface_name*

Syntax Description

interface_name	Specifies the interface name through which FXOS can send management traffic.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.8(2)	We added this command.

Usage Guidelines

You can enable FXOS management traffic initiation on ASA data interfaces, which is required for SNMP traps, or NTP and DNS server access, for example. For incoming management traffic, see the **fxos permit** command.

In the FXOS configuration, make sure the default gateway is set to 0.0.0.0, which sets the ASA as the gateway. See the FXOS **set out-of-band** command.

Examples

The following allows FXOS traffic initiation through the outside interface:

```
ciscoasa(config)# ip-client outside
```

Related Commands

Command	Description
connect fxos	From the ASA CLI, connects to the FXOS CLI.
fxos permit	Allows FXOS management access on ASA data interfaces.
fxos port	Sets the FXOS management access port.

ip-comp

To enable LZS IP compression, use the **ip-comp enable** command in group-policy configuration mode. To disable IP compression, use the **ip-comp disable** command.To remove the **ip-comp** attribute from the running configuration, use the **no** form of this command.

ip-comp { **enable** | **disable** }
no ip-comp

Syntax Description

disable	Disables IP compression.
enable	Enables IP compression.

Command Default

IP compression is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuratio	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **no** form of this command enables inheritance of a value from another group policy. Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.

Caution Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the ASA. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

If the endpoints generate IP compression traffic, you should disable IP compression to prevent improper decompression of the packets. If IP compression is enabled on a particular LAN to LAN tunnel, host A cannot communicate with host B when trying to pass IP compression data from one side of the tunnel to other side.

Note When the **ip-comp** command is enabled and IPsec fragmentation is configured for "before-encryption," you cannot have IPsec compression (ip-comp_option and pre-encryption). The IP header sent to the crypto chip becomes obfuscated (because of the compression), causing the crypto chip to generate an error when processing the supplied outbound packet. You might also check your MTU level to ensure that it is a small amount (such as 600 bytes).

Examples

The following example shows how to enable IP compression for the group policy named "FirstGroup":

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```

ip local pool

To configure IP address pools, use the **ip local pool** command in global configuration mode. To delete the address pool, use the **no** form of this command.

ip local pool *poolname first-address-last-address* [**mask** *mask*]
no ip local pool *poolname*

Syntax Description

first-address	Specifies the starting address in the range of IP addresses.
last-address	Specifies the final address in the range of IP addresses.
mask *mask*	(Optional) Specifies a subnet mask for the pool of addresses. You cannot use a 255.255.255.254 (/31) or 255.255.255.255 (/32) subnet mask.
poolname	Specifies the name of the IP address pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	IP local pool for the cluster pool in the **ip address** command to support ASA clustering was added.

Usage Guidelines

You must supply the mask value when the IP addresses assigned to VPN clients belonging to a non-standard network and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets fall under the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

Examples

The following example configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

Command	Description
clear configure ip local pool	Removes all IP local pools.
show running-config ip local pool	Displays the IP pool configuration. To specify a specific IP address pool, include the name in the command.

ip unnumbered

To borrow or inherit an IP address from an interface (for example, a loopback interface), use the **ip unnumbered** command in the interface configuration mode. To stop inheriting an ip address from an interface, use the **no** form of this command.

ip unnumbered *interface-name*
no ip unnumbered

Syntax Description

interface-name	Specifies the name of an interface to inherit the IP address..

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

The **ip unnumbered** command is used to inherit the IP address of the selected interface as the address for the current interface.

Examples

The following example borrows the IP address from the loopback interface:

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ip unnumbered loopback1
```

Related Commands

Command	Description
ipv6 unnumbered *interface-name*	Inherits the IPv6 address of the specified interface.
interface loopback *loopback-number*	Creates a loopback interface.

ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode.To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command.

ip-phone-bypass { **enable** | **disable** }
no ip-phone-bypass

Syntax Description

disable	Disables IP Phone Bypass.
enable	Enables IP Phone Bypass.

Command Default

IP Phone Bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. The **no** form of this command option allows inheritance of a value for IP Phone Bypass from another group policy.

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. If enabled, secure unit authentication remains in effect.

You need to configure IP Phone Bypass only if you have enabled user authentication.

You also need to configure the **mac-exempt** option to exempt the clients from authentication. See the **vpnclient mac-exempt** command for more information.

Examples

The following example shows how to enable IP Phone Bypass for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

Related Commands

Command	Description
user-authentication	Requires users behind a hardware client to identify themselves to the ASA before connecting.

ips

To divert traffic from the ASA to the AIP SSM for inspection, use the **ips** command in class configuration mode. To remove this command, use the **no** form of this command.

ips { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [**sensor** { *sensor_name* | *mapped_name* }]
no ips { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [**sensor** { *sensor_name* | *mapped_name* }]

Syntax Description

fail-close	Blocks traffic if the AIP SSM fails.
fail-open	Permits traffic if the AIP SSM fails.
inline	Directs packets to the AIP SSM; the packet might be dropped as a result of IPS operation.
promiscuous	Duplicates packets for the AIP SSM; the original packet cannot be dropped by the AIP SSM.
sensor {*sensor_name* | *mapped_name* }	Sets the virtual sensor name for this traffic. If you use virtual sensors on the AIP SSM (using Version 6.0 or above), you can specify a sensor name using this argument. To see available sensor names, enter the **ips ... sensor ?** command. Available sensors are listed. You can also use the **show ips** command. If you use multiple context mode on the ASA, you can only specify sensors that you assigned to the context (see the **allocate-ips** command). Use the *mapped_name* argument if configured in the context. If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM. If you enter a name that does not yet exist on the AIP SSM, you get an error, and the command is rejected.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Virtual sensor support was added.

Usage Guidelines

The ASA 5500 series supports the AIP SSM, which runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. Before or after you configure the **ips** command on the ASA, configure the security policy on the AIP SSM. You can either session to the AIP SSM from the ASA (the **session** command) or you can connect directly to the AIP SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM. For more information about configuring the AIP SSM, see Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface.

To configure the **ips** command, you must first configure the **class-map** command, **policy-map** command, and the **class** command.

The AIP SSM runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you apply the **ips** command for a class of traffic on the ASA, traffic flows through the ASA and the AIP SSM in the following way:

1. Traffic enters the ASA.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane (using the **inline** keyword; See the **promiscuous** keyword for information about only sending a copy of the traffic to the AIP SSM).
4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the ASA over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the ASA.

Examples

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic if the AIP SSM card fails for any reason:

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM card fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
```

```
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

Related Commands

Command	Description
allocate-ips	Assigns a virtual sensor to a security context.
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy map configurations.

ipsec-udp

To enable IPsec over UDP, use the **ipsec-udp enable** command in group-policy configuration mode. To remove the IPsec over UDP attribute from the current group policy, use the **no** form of this command.

ipsec-udp { **enable** | **disable** }
no ipsec-udp

Syntax Description

disable	Disables IPsec over UDP.
enable	Enables IPsec over UDP.

Command Default

IPsec over UDP is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **no** form of this command enables inheritance of a value for IPsec over UDP from another group policy.

IPsec over UDP, sometimes called IPsec through NAT, lets a Cisco VPN Client or hardware client connect via UDP to an ASA that is running NAT.

To disable IPsec over UDP, use the **ipsec-udp disable** command.

To use IPsec over UDP, you must also configure the **ipsec-udp-port** command.

The Cisco VPN Client must also be configured to use IPsec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPsec over UDP.

IPsec over UDP is proprietary, applies only to remote access connections, and requires mode configuration, which means that the ASA exchanges configuration parameters with the client while negotiating SAs.

Using IPsec over UDP may slightly degrade system performance.

The ipsec-udp-port command is not supported on an ASA5505 operating as a VPN client. The ASA 5505 in client mode can initiate IPsec sessions on UDP ports 500 and/or 4500.

Examples

The following example shows how to configure IPsec over UDP for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

Related Commands

Command	Description
ipsec-udp-port	Specifies the port on which the ASA listens for UDP traffic.

ipsec-udp-port

To set a UDP port number for IPsec over UDP, use the **ipsec-udp-port** command in group-policy configuration mode. To disable the UDP port, use the **no** form of this command.

ipsec-udp-port*port*
noipsec-udp-port

Syntax Description

port	Identifies the UDP port number using an integer in the range of 4001 through 49151.

Command Default

The default port is 10000.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuratio	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **no** form of this command enables inheritance of a value for the IPsec over UDP port from another group policy.

In IPsec negotiations. the ASA listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic.

You can configure multiple group policies with this feature enabled, and each group policy can use a different port number.

Examples

The following example shows how to set an IPsec UDP port to port 4025 for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

Command	Description
ipsec-udp	Lets a Cisco VPN Client or hardware client connect via UDP to an ASA that is running NAT.

ipv – ir

ipv4-prefix

To configure the IPv4 prefix for the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **ipv4-prefix** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the prefix.

ipv4-prefix*ipv4_network_addressnetmask*
no ipv4-prefix *ipv4_network_address netmask*

Syntax Description

ipv4_network_address netmask	The IPv4 prefix that defines the IPv4 address pool for the customer edge (CE) device. Specify a network address and subnet mask, for example, 192.168.3.0 255.255.255.0. You cannot use the same IPv4 prefix in different MAP domains.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The IPv4 prefix defines the IPv4 address pool for the customer edge (CE) device. The CE device first translates its IPv4 address to an address (and port number) in the pool defined by the IPv4 prefix. MAP then translates this new address to an IPv6 address using the prefix in the default mapping rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
```

```
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

ipv6 address

To enable IPv6 and configure the IPv6 addresses on an interface (in routed mode) or for the bridge group or management interface address (transparent mode), use the **ipv6 address** command. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }
no ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }

Syntax Description

autoconfig	Enables stateless autoconfiguration on the interface. Enabling stateless autoconfiguration on the interface configures IPv6 addresses based on prefixes received in router advertisement messages. A link-local address, based on the modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled. Not supported for transparent firewall mode. **Note** Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send router advertisement messages, the ASA does send router advertisement messages in this case. See the **ipv6 nd suppress-ra** command to suppress messages.
cluster-pool *poolname*	(Optional) For ASA clustering, sets the cluster pool of addresses defined by the **ipv6 local pool** command. The main cluster IP address defined by the argument belongs to the current master unit only. Each cluster member receives a local IP address from this pool. You cannot determine the exact address assigned to each unit in advance; to see the address used on each unit, enter the **show ipv6 local pool** *poolname* command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the local IP used from the pool.
default	(Optional) Obtains a default route from Router Advertisements.
default trust	(Optional) Installs a default route from Router Advertisements.
dhcp (autoconfig)	(Optional) Specifies the ASA only uses a default route from Router Advertisements that come from a trusted source (in other words, from the same server that provided the IPv6 address).
dhcp	Obtains the IPv6 address from a DHCPv6 server.
ignore	(Optional) Specifies that Router Advertisements can be sourced from another network, which can be a riskier method.
ipv6_address/prefix_length	Assigns a global address to the interface. When you assign a global address, the link-local address is automatically created for the interface.

ipv6_prefix/prefix_length **eui-64**	Assigns a global address to the interface by combining the specified prefix with an interface ID generated from the interface MAC address using the modified EUI-64 format. When you assign a global address, the link-local address is automatically created for the interface. If the value specified for the >*prefix_length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID. An error message will be displayed if another host is using the specified address. You do not need to specify the standby address; the interface ID will be generated automatically. The modified EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower three bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.
ipv6_address **link-local**	Manually configures the link-local address only. The *ipv6_address* specified with this command overrides the link-local address that is automatically generated for the interface. The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in modified EUI-64 format. An interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error message will be displayed if another host is using the specified address.
prefix_name ipv6_address/prefix_length	Uses a delegated prefix. This feature requires an ASA interface to have the DHCPv6 Prefix Delegation client enabled (**ipv6 dhcp client pd**). Typically, the delegated prefix will be /60 or smaller so you can subnet to multiple /64 networks. /64 is the supported subnet length if you want to support SLAAC for connected clients. You should specify an address that completes the /60 subnet, for example ::1:0:0:0:1. Enter :: before the address in case the prefix is smaller than /60. For example, if the delegated prefix is 2001:DB8:1234:5670::/60, then the global IP address assigned to this interface is 2001:DB8:1234:5671::1/64. The prefix that is advertised in router advertisements is 2001:DB8:1234:5671::/64. In this example, if the prefix is smaller than /60, the remaining bits of the prefix will be 0's as indicated by the leading ::. For example, if the prefix is 2001:DB8:1234::/48, then the IPv6 address will be 2001:DB8:1234::1:0:0:0:1/64.
standby *ipv6_address*	(Optional) Specifies the interface address used by the secondary unit or failover group in a failover pair.

Command Default

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.
8.2(2)	Support for a standby address was added.
8.4(1)	For transparent mode, bridge groups were added. You set the IP address for the BVI, and not globally.
9.0(1)	The **cluster-pool** keyword was added to support ASA clustering.
9.6(2)	We added the following options: • **autoconfig default trust** {**dhcp** | **ignore**} • **dhcp** [**default**] • *prefix_name ipv6_address/prefix_length*

Usage Guidelines

Configuring an IPv6 address on an interface enables IPv6 on that interface; you do not need to use the **ipv6 enable** command after specifying an IPv6 address.

Multiple Context Mode Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

DHCPv6 and prefix delegation options are not supported with multiple context mode.

Transparent Firewall Guidelines

Transparent mode only supports manually setting the IPv6 address. A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

Failover Guidelines

The standby IP address must be on the same subnet as the main IP address.

ASA Clustering Guidelines

You can only set the cluster pool for an individual interface after you configure the cluster interface mode to be individual (**cluster-interface mode individual**). The only exception is for the management-only interface(s):

- You can always configure the management-only interface as an individual interface, even in spanned EtherChannel mode. The management interface can be an individual interface even in transparent firewall mode.
- In spanned EtherChannel mode, if you configure the management interface as an individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.

DHCPv6 and prefix delegation options are not supported with clustering.

Examples

The following example assigns 2001:0DB8:BA98::3210/64 as the global address for the selected interface and 2001:0DB8:BA98::3211 as the address for the corresponding interface on the standby unit:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

The following example assigns an IPv6 address automatically for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

The following example assigns IPv6 prefix 2001:0DB8:BA98::/64 to the selected interface and specifies an EUI-64 interface ID in the low order 64 bits of the address. If this device is part of a failover pair, you do not need to specify the **standby** keyword; the standby address will be automatically created using the modified EUI-64 interface ID.

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface on the primary unit in a failover pair, and FE80::260:3EFF:FE11:6671 as the link-level address for the corresponding interface on the secondary unit.

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

The following example assigns ::1:0:0:0:1/64 as the address to complete the Deligated Prefix:

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

Related Commands

Command	Description
debug ipv6 interface	Displays debugging information for IPv6 interfaces.
show ipv6 interface	Displays the status of interfaces configured for IPv6.

ipv6-address-pool

To specify a list of IPv6 address pools for allocating addresses to remote clients, use the **ipv6-address-pool** command in tunnel-group general-attributes configuration mode. To eliminate IPv6 address pools, use the **no** form of this command.

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [*...ipv6_address_pool6*]
no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [*...ipv6_address_pool6*]

Syntax Description

interface_name	(Optional) Specifies the interface to be used for the address pool.
ipv6_address_pool	Specifies the name of the address pool configured with the **ipv6 local pool** command. You can specify up to six local address pools.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The IPv6 address-pool settings in the group-policy **ipv6-address-pools** command override the IPv6 address pool settings in the tunnel group **ipv6-address-pool** command.

The order in which you specify the pools is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in tunnel-group general-attributes configuration mode, specifies a list of IPv6 address pools for allocating addresses to remote clients for an IPsec remote access tunnel group test:

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
```

```
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
ipv6-address-pools	Configures the IPv6 address pools settings for the group policy, which override those settings for the tunnel group.
ipv6 local pool	Configures IP address pools to be used for VPN remote access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group	Configures a tunnel group.

ipv6-address-pools

To specify a list of up to six IPv6 address pools from which to allocate addresses to remote clients, use the **ipv6-address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

ipv6-address-pools value *ipv6_address_poll1* [*...ipv6_address_pool6*]
no ipv6-address-pools value *ipv6_address_poll1* [*...ipv6_address_pool6*]
ipv6-address-poolsnone
noipv6-address-poolsnone

Syntax Description

ipv6_address_pool	Specifies the names of the up to six IPv6 address pools configured with the **ipv6 local pool** command. Use spaces to separate the IPv6 address pool names.
none	Specifies that no IPv6 address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to six IPv6 address pools from which to assign addresses.

Command Default

By default, the IPv6 address pools attribute is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To configure IPv6 address pools, use the **ipv6 local pool** command.

The order in which you specify the pools in the **ipv6-address-pools** command is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

The **ipv6-address-pools none** command disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The **no ipv6-address-pools none** command removes the **ipv6-address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example, entered in group-policy attributes configuration mode, configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients, then associates that pool with GroupPolicy1:

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-
address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group policies or for a particular group policy.

ipv6 dhcp client pd

To enable the DHCPv6 Prefix Delegation client, and name the prefix(es) obtained on an interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable the client, use the **no** form of this command.

ipv6 dhcp client pd *name*
no ipv6 dhcp client pd *name*

Syntax Description

name Sets the name for this prefix. The name can be up to 200 characters. You will use this name when assigning an IP address to an interface using the prefix (**ipv6 address** *prefix_name*).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Enable the DHCPv6 Prefix Delegation client on one or more interfaces. The ASA obtains one or more IPv6 prefixes that it can subnet and assign to inside networks. Typically, the interface on which you enable the prefix delegation client obtains its IP address using the DHCPv6 address client; only other ASA interfaces use addresses derived from the delegated prefix.

This feature is not supported in clustering.

You cannot configure this feature on a management-only interface.

Examples

The following example configures the DHCPv6 address client and prefix delegation client on GigabitEthernet 0/0, then assigns addresses with the prefix on GigabitEthernet 0/1 and 0/2:

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcp client pd hint

To provide one or more hints about the delegated prefix you want to receive, use the **ipv6 dhcp client pd hint** command in interface configuration mode. To disable the client, use the **no** form of this command.

ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*
no ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	Specifies the IPv6 prefix and length that you want to receive.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Typically you want to request a particular prefix length, such as ::/60, or if you have received a particular prefix before and want to ensure you get it again when the lease expires, you can enter the whole prefix as the hint. If you enter multiple hints (different prefixes or lengths), then it is up to the DHCP server which hint to honor, or whether to honor the hint at all.

Examples

The following example configures the DHCPv6 address client and prefix delegation client on GigabitEthernet 0/0, then assigns addresses with the prefix on GigabitEthernet 0/1 and 0/2:

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcp pool

To configure the IPv6 DHCP pool that contains the information you want the DHCPv6 server to provide to StateLess Address Auto Configuration (SLAAC) clients, use the **ipv6 dhcp pool** command in global configuration mode. To remove the pool, use the **no** form of this command.

ipv6 dhcp pool *pool_name*
no ipv6 dhcp pool *pool_name*

Syntax Description

pool_name	Specifies a name for the pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify this pool name when you enable the server. You can configure separate pools for each interface if you want, or you can use the same pool on multiple interfaces. After you enter the **ipv6 dhcp pool** command, you can configure one or more parameters to provide to the clients.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcprelay enable

To enable DHCPv6 relay service on an interface, use the **ipv6 dhcprelay enable** command in global configuration mode. To disable the DHCPv6 relay service, use the **no** form of this command.

ipv6 dhcprelay enable *interface*
no ipv6 dhcprelay enable *interface*

Syntax Description

interface	Specifies the output interface for a destination.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command allows you to enable DHCPv6 relay service on an interface.When the service is enabled, incoming DHCPv6 messages from a client on the interface, which may have been relayed by another relay agent, are forwarded to all configured relay destinations through all configured outgoing links. For multiple context mode, you cannot enable DHCP relay service on an interface that is used by more than one context (that is, a shared interface).

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay server	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.

Command	Description
ipv6 dhcprelay timeout	Sets the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

ipv6 dhcprelay server

To specify the IPv6 DHCP server destination address to which client messages are forwarded, use the **ipv6 dhcprelay server** command in global configuration mode. To remove the IPv6 DHCP server destination address, use the **no** form of this command.

ipv6 dhcprelay server *ipv6-address* [*interface*]
no ipv6 dhcprelay server *ipv6-address* [*interface*]

Syntax Description

interface	(Optional) Specifies the output interface for a destination.
ipv6-address	Can be a link-scoped unicast, multicast, site-scoped unicast, or global IPV6 address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command enables you to specify the IPv6 DHCP server destination address to which client messages are forwarded. Client messages are forwarded to the destination address through the link to which the output interface is connected. If the specified address is a link-scoped address, then you must specify the interface. Unspecified, loopback, and node-local multicast addresses are not allowed as the relay destination. You can specify a maximum of ten servers per context.

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay enable	Enables IPv6 DHCP relay service on an interface.

Command	Description
ipv6 dhcprelay timeout	Sets the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

ipv6 dhcprelay timeout

To set the amount of time in seconds that are allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure, use the **ipv6 dhcprelay timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6dhcprelaytimeout*seconds*
noipv6dhcprelaytimeout*seconds*

Syntax Description

seconds	Sets the number of seconds that are allowed for DHCPv6 relay address negotiation. Valid values range from 1 to 3600.

Command Default

The default is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command allows you to set the amount of time in seconds that are allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay server	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.
ipv6 dhcprelay enable	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.

ipv6 dhcp server

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature, configure the DHCPv6 stateless server using the **ipv6 dhcp server** command in interface configuration mode. To disable the DHCP server, use the **no** form of this command.

ipv6 dhcp server *pool_name*
no ipv6 dhcp server *pool_name*

Syntax Description

pool_name	Sets the name of the IPv6 pool configured with the **ipv6 dhcp pool** command. This pool includes information that you want to provide to clients on a given interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
```

```
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.

Command	Description
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 enable

To enable IPv6 processing and you have not already configured an explicit IPv6 address, use the **ipv6 enable** command in global configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—
Global configuration	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface, while also enabling the interface for IPv6 processing.

The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address for an interface and enables IPv6 processing on the interface.

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 enforce-eui64

To enforce the use of modified EUI-64 format interface identifiers in IPv6 addresses on a local link, use the **ipv6 enforce-eui64** command in global configuration mode. To disable modified EUI-64 address format enforcement, use the **no** form of this command.

ipv6 enforce-eui64 *if_name*
no ipv6 enforce-eui64 *if_name*

Syntax Description

if_name	Specifies the name of the interface, as designated by the **nameif** command, for which you are enabling modified EUI-64 address format enforcement.

Command Default

Modified EUI-64 format enforcement is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

When this command is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the modified EUI-64 format. If the IPv6 packets do not use the modified EUI-64 format for the interface identifier, the packets are dropped and the following syslog message is generated:

```
%ASA-3-325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

The modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower three bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.

Examples

The following example enables modified EUI-64 format enforcement for IPv6 addresses received on the inside interface:

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address on an interface.
ipv6 enable	Enables IPv6 on an interface.

ipv6 icmp

To configure ICMP access rules for an interface, use the **ipv6 icmp** command in global configuration mode. To remove an ICMP access rule, use the **no** form of this command.

ipv6 icmp { **permit** | **deny** } { *ipv6-prefix / prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*
no ipv6 icmp { **permit** | **deny** } { *ipv6-prefix / prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*

Syntax Description

any	Keyword specifying any IPv6 address. An abbreviation for the IPv6 prefix ::/0.
deny	Prevents the specified ICMP traffic on the selected interface.
host	Indicates that the address refers to a specific host.
icmp-type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	The name of the interface, as designated by the **nameif** command, to which the access rule applies.
ipv6-address	The IPv6 address of the host sending ICMPv6 messages to the interface.
ipv6-prefix	The IPv6 network that is sending ICMPv6 messages to the interface.

permit	Allows the specified ICMP traffic on the selected interface.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Command Default

If no ICMP access rules are defined, all ICMP traffic is permitted.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

If there are no ICMP rules defined for an interface, all IPv6 ICMP traffic is permitted.

If there are ICMP rules defined for an interface, then the rules are processed in order on a first-match basis followed by an implicit deny all rule. For example, if the first matched rule is a permit rule, the ICMP packet is processed. If the first matched rule is a deny rule, or if the ICMP packet did not match any rule on that interface, then the ASA discards the ICMP packet and generates a syslog message.

For this reason, the order that you enter the ICMP rules is important. If you enter a rule denying all ICMP traffic from a specific network, and then follow it with a rule permitting ICMP traffic from a particular host on that network, the host rule will never be processed. The ICMP traffic is blocked by the network rule. However, if you enter the host rule first, followed by the network rule, the host ICMP traffic will be allowed, while all other ICMP traffic from that network is blocked.

The **ipv6 icmp** command configures access rules for ICMP traffic that terminates at the ASA interfaces. To configure access rules for pass-through ICMP traffic, see the **ipv6 access-list** command.

Examples

The following example denies all ping requests and permits all packet-too-big messages (to support path MTU discovery) at the outside interface:

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

ipv6 local pool

To configure an IPv6 address pool, use the **ipv6 local pool** command in global configuration mode. To delete the pool, use the **no** form of this command.

ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*
no ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*

Syntax Description

ipv6_address	Specifies the starting IPv6 address for the pool.
number_of_addresses	Range: 1-16384.
pool_name	Specifies the name to assign to this IPv6 address pool.
prefix_length	Range: 0-128.

Command Default

By default, the IPv6 local address pool is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	IPv6 local pool for the cluster pool in the **ipv6 address** command to support ASA clustering was added.

Usage Guidelines

For VPN, to assign IPv6 local pools, use either the **ipv6-local-pool** command in the tunnel group or the **ipv6-address-pools** command (note the "s" on this command) in the group policy. The ipv6-address-pools setting in the group policy overrides the ipv6-address-pools setting in the tunnel group.

Examples

The following example configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients:

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

Related Commands

Command	Description
ipv6-address-pool	Associates IPv6 address pools with a VPN tunnel group policy.
ipv6-address-pools	Associates IPv6 address pools with a VPN group policy.
clear configure ipv6 local pool	Clears all configured IPv6 local pools.
show running-config ipv6	Shows the configuration for IPv6.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection, use the **ipv6 nd dad attempts** command in interface configuration mode. To return to the default number of duplicate address detection messages sent, use the **no** form of this command.

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

Syntax Description

value	A number from 0 to 600. Entering 0 disables duplicate address detection on the specified interface. Entering 1 configures a single transmission without follow-up transmissions. The default value is 1 message.

Command Default

The default number of attempts is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. The frequency at which the neighbor solicitation messages are sent is configured using the **ipv6 nd ns-interval** command.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state.

Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up. An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

Note While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Examples

The following example configures 5 consecutive neighbor solicitation messages to be sent when duplicate address detection is being performed on the tentative unicast IPv6 address of the interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd managed-config-flag

To configure the ASA to set the managed address config flag in the IPv6 router advertisement packet, use the **ipv6 nd managed config-flag** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The IPv6 autoconfiguration client host can use this flag to indicate that it must use the stateful address configuration protocol (DHCPv6) to obtain addresses in addition to the derived stateless autoconfiguration address.

Examples

The following example sets the managed address config flag in the IPv6 router advertisement packet for the interface GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

Related Commands

Command	Description
ipv6 nd other-config-flag	Configures the ASA to set the other config flag in the IPv6 router advertisement packet.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ns-interval *value*
no ipv6 nd ns-interval [*value*]

Syntax Description

value The interval between IPv6 neighbor solicitation transmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds.

Command Default

The default is 1000 milliseconds between neighbor solicitation transmissions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd other-config-flag

To configure the ASA to set the other config flag in the IPv6 router advertisement packet, use the **ipv6 nd other-config-flag** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The IPv6 autoconfiguration client host can use this flag to indicate that it must use the stateful address configuration protocol (DHCPv6) to obtain non-address configuration information such as DNS server information.

Examples

The following example sets the other config flag in the IPv6 router advertisement packet for the interface GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Configures the ASA to set the managed address config flag in the IPv6 router advertisement packet.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]
no ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

Syntax Description

at *valid-date preferred-date*	The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* .
default	Default values are used.
infinite	(Optional) The valid lifetime does not expire.
ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
no-advertise	(Optional) Indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is not used for on-link determination.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with the **infinite** keyword. The default is 604800 (7 days).
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
valid-lifetime	The amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with the **infinite** keyword. The default is 2592000 (30 days).

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds in router advertisements sent out on the specified interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval [**msec**] *value*
no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	(Optional) indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is seconds.
value	The interval between IPv6 router advertisement transmissions. Valid values range from 3 to 1800 seconds, or from 500 to 1800000 milliseconds if the **msec** keyword is provided. The default is 200 seconds.

Command Default

200 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

To configure the “router lifetime” value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*
no ipv6 nd ra-lifetime [*seconds*]

Syntax Description

seconds	The validity of the ASA as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the ASA should not be considered a default router on the selected interface.

Command Default

1800 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The “router lifetime” value is included in all IPv6 router advertisements sent out an interface. The value indicates the usefulness of the ASA as a default router on this interface.

Setting the value to a non-zero value to indicates that the ASA should be considered a default router on this interface. The non-zero value for the “router lifetime” value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the ASA should not be considered a default router on this interface.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *value*
no ipv6 nd reachable-time [*value*]

Syntax Description

value The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default value is 0.

When 0 is used for the *value* argument, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

Command Default

Zero milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

To see the reachable time used by the ASA, including the actual value when this command is set to 0, use the **show ipv6 interface** command to display information about the IPv6 interface, including the ND reachable time being used.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Command Default

Router advertisements are automatically sent on LAN interfaces if IPv6 unicast routing is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static entry from the neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6_address if_name mac_address*
no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

Syntax Description

if_name	The internal or external interface name designated by the **nameif** command.
ipv6_address	The IPv6 address that corresponds to the local data link address.
mac_address	The local data line (hardware MAC) address.

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the **copy** command is used to store the configuration.

Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example adds a static entry for the an inside host with an IPv6 address of 3001:1::45A and a MAC address of 0002.7D1A.9472 to the neighbor discovery cache:

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

ipv6 ospf

To enable the OSPFv3 interface configuration for IPv6, use the **ipv6 ospf** command in global configuration mode. To disable the OSPFv3 interface configuration for IPv6, use the **no** form of this command.

ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]
no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

Syntax Description

cost	Explicitly specifies the cost of sending a packet on an interface.
database-filter	Filters outgoing LSAs to an OSPFv3 interface.
dead-interval *seconds*	Sets the time period in seconds for which hello packets must not be seen before neighbors indicate that the router is down. The value must be the same for all nodes on the network and can range from 1 to 65535. The default is four times the interval set by the **ipv6 ospf hello-interval** command.
flood-reduction	Specifies the flood reduction of LSAs to the interface.
hello-interval *seconds*	Specifies the interval in seconds between hello packets sent on the interface. The value must be the same for all nodes on a specific network and can range from 1 to 65535. The default interval is 10 seconds for Ethernet interfaces and 30 seconds for non-broadcast interfaces.
mtu-ignore	Disables the OSPF MTU mismatch detection when DBD packets are received. OSPF MTU mismatch detection is enabled by default.
neighbor	Configures OSPFv3 router interconnections to non-broadcast networks.
network	Sets the OSPF network type to a type other than the default, which depends on the network type.
priority	Sets the router priority, which helps determine the designated router for a network. Valid values range from 0 to 255.
process-id	Specifies the OSPFv3 process to be enabled. Valid values range from 1 to 65535.
retransmit-interval *seconds*	Specifies the time in seconds between LSA retransmissions for adjacencies that belong to the interface. The time must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds. The default is 5 seconds.
transmit-delay *seconds*	Sets the estimated time in seconds to send a link-state update packet on the interface. Valid values range from 1 to 65535 seconds. The default is 1 second.

Command Default

All IPv6 addresses are included by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must enable an OSPFv3 routing process before you can create an OSPFv3 area.

Examples

The following example enables OSPFv3 interface configuration:

```
ciscoasa(config)# ipv6 ospf 3
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf area

To create an OSPFv3 area for IPv6, use the **ipv6 ospf area** command in global configuration mode. To disable the OSPFv3 area configuration for IPv6, use the **no** form of this command.

ipv6 ospf area [*area-num*] [**instance**]
no ipv6 ospf area [*area-num*] [**instance**]

Syntax Description

area-num	Specifies the OSPFv3 area to be enabled.
instance	Specifies the area instance ID that is to be assigned to an interface.

Command Default

All IPv6 addresses are included by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must configure OSPFv3 routing on each interface separately. An interface can have only one OSPFv3 area, and OSPFv3 for the ASA supports only one instance per interface. Each interface uses a different area instance ID. The area instance ID only affects the receipt of OSPF packets, and applies to normal OSPF interfaces and virtual links.

Examples

The following example enables OSPFv3 interface configuration:

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the cost of sending a packet on an interface to the default value, use the **no** form of this command.

ipv6 ospf cost *interface-cost*
no ipv6 ospf cost *interface-cost*

Syntax Description

interface-cost	Specifies an unsigned integer value expressed as the link-state metric, which can range from 1 to 65535.

Command Default

The default cost is based on the bandwidth.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to explicitly specify the packet cost for an interface.

Examples

The following example sets the packet cost to 65:

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf database-filter all out

To filter outgoing LSAs to an OSPFv3 interface, use the **ipv6 ospf databse-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to filter outgoing LSAs to an OSPFv3 interface.

Examples

The following example filters outgoing LSAs to the specified interface:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare that the router is down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

Syntax Description

seconds	Specifies the interval in seconds. The value must be the same for all nodes in the network. Valid values range from 1 to 65535.

Command Default

The default is four times the interval that is set by the **ipv6 ospf hello-interval** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the interval during which hello packets are not seen before neighbors notify that the router is down.

Examples

The following example sets the dead interval to 60:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf encryption

To specify the encryption type for an interface, use the **ipv6 ospf encryption** command in interface configuration mode. To remove the encryption type for an interface, use the **no** form of this command.

ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }
no ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }

Syntax Description

authentication-algorithm	Specifies the encryption algorithm to be used. Valid values are one of the following: • **md5**—Enables message digest 5 (MD5). • **sha1**—Enables SHA-1.
encryption-algorithm	Specifies the encryption algorithm to be used with ESP . . Valid values are the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—Specifies ESP with no encryption.
esp	Specifies the encapsulating security payload (ESP).
ipsec	Specifies the IP security protocol.
key	Specifies the number used in the calculation of the message digest. When MD5 authentication is used, the key must be 32 hexadecimal digits (16 bytes) long. When SHA-1 authentication is used, the key must be 40 hexadecimal digits (20 bytes) long.
key-encryption-type	(Optional) Specifies the key encryption type, which can be one of the following values: • **0**—The key is not encrypted. • **7**—The key is encrypted.
null	Overrides area authentication.
spi *spi*	Specifies the security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the encryption type for an interface.

Examples

The following example enables SHA-1 encryption on the interface:

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf flood-reduction

To specify the flood reduction of LSAs to the interface, use the **ipv6 ospf flood-reduction** command in interface configuration mode. To remove the flood reduction of LSAs to the interface, use the **no** form of this command.

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the flood reduction of LSAs to an interface.

Examples

The following example enables flood reduction of LSAs to the interface:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.

Command	Description
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf hello-interval

To set the time period for which hello packets must not be seen before neighbors declare that the router is down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

Syntax Description

seconds	Specifies the interval in seconds. The value must be the same for all nodes in the network. Valid values range from 1 to 65535.

Command Default

The default interval is 10 seconds if you are using Ethernet and 30 seconds if you are using non-broadcast.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the interval during which hello packets are not seen before neighbors notify that the router is down.

Examples

The following example sets the dead interval to 60:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf mtu-ignore

To disable OSPFv3 maximum transmission unit (MTU) mismatch detection when the ASA receives database descriptor (DBD) packets, use the **ipv6 ospf mtu-ignore** command in interface configuration mode. To reset the MTU mismatch detection when the ASA receives DBD packets to the default, use the **no** form of this command.

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to disable OSPFv3 MTU mismatch detection when the ASA receives DBD packets.

Examples

The following example disables OSPFv3 MTU mismatch detection when the ASA receives DBD packets:

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf neighbor

To configure OSPFv3 router interconnections to nonbroadcast networks, use the **ipv6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]
no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

Syntax Description

cost *number*	(Optional) Assigns a cost to the neighbor in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assume the cost of the interface, based on the **ipv6 ospf cost** command.
database-filter	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.
ipv6-address	Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
poll-interval *seconds*	(Optional) A number value that represents the poll interval time in seconds. RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (two minutes). This keyword does not apply to point-to-multipoint interfaces.
priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified. The default is 0.

Command Default

The default depends on the network type.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	•	•		—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure OSPFv3 router interconnections to nonbroadcast networks.

Examples

The following example configures an OSPFv3 neighboring router:

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf network

To configure the OSPFv3 network type to a type other than the default, use the **ipv6 ospf network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }
no ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }

Syntax Description

broadcast	Sets the network type to broadcast.
point-to-point non-broadcast	Sets the network type to point-to-point non-broadcast.

Command Default

The default depends on the network type.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure the OSPFv3 network type to a type that is different from the default.

Examples

The following example sets the OSPFv3 network to a broadcast network:

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf priority

To set the router priority, which helps determine the designated router for a specified network, use the **ipv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*
no ipv6 ospf priority *number-value*

Syntax Description

number-value	Sets the number value that specifies the priority of the router. Valid values range from 0 to 255.

Command Default

The default priority is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the priority of the router.

Examples

The following example sets the priority of the router to 4:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf retransmit-interval	Specifies the time between LSA retransmissions for adjacencies that belong to the interface.

ipv6 ospf retransmit-interval

To specify the time between LSA retransmissions for adjacencies that belong to the interface, use the **ipv6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*
no ipv6 ospf retransmit-interval *seconds*

Syntax Description

seconds	Specifies the time in seconds between retransmissions. The interval must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds.

Command Default

The default is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the time between LSA retransmissions for adjacencies that belong to the interface.

Examples

The following example sets the retransmission interval to 8 seconds:

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

Related Commands

Command	Description
ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf transmit-delay

To set the estimated time that is required to send a link-state update packet on the interface, use the **ipv6 ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*
no ipv6 ospf transmit-delay *seconds*

Syntax Description

seconds	Specifies the time in seconds that is required to send a link-state update. Valid values range from 1 to 65535 seconds.

Command Default

The default is 1 second.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the estimated time that is required to send a link-state update packet on the interface.

Examples

The following example sets the transmission delay to 3 seconds:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6-prefix

To configure the IPv6 prefix for the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **ipv6-prefix** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the prefix.

ipv6-prefix *ipv6_prefix / prefix_length*
no ipv6-prefix *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	The IPv6 prefix defines the address pool for the customer edge (CE) device's IPv6 address. Specify an IPv6 prefix and prefix length, which is normally 64, but cannot be less than 8. You cannot use the same IPv6 prefix in different MAP domains.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The IPv6 prefix defines the address pool for the CE device's IPv6 address. MAP translates IPv6 packets back to IPv4 only if the packets have a destination address with this prefix and a source address with the IPv6 prefix defined in the default mapping rule, and is within the right port range. Any IPv6 packets sent to the CE device from other addresses are simply processed as IPv6 traffic without MAP translation. Packets from the MAP source/destination pools, but with out-of-range ports, are simply dropped.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule
```

```
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ipv6 prefix-list *list-name* [**seq** *seq-number*] { **deny** *ipv6-prefix* | *prefix-length* | **description** *text* } [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. Cannot be the same name as an existing access list. **Note** The name cannot be ‘detail’ or ‘summary’, because they are keywords.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that match the condition.
permit	Permits networks that match the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the length (the "from" portion of the length range).
le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the highest value of a range of the length (the "to" portion of the length range).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Related Commands

Command	Description
show ipv6 prefix-list	Displays IPv6 prefix lists.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 route

To add an IPv6 route to the IPv6 routing table, use the **ipv6 route** command in global configuration mode. To remove an IPv6 default route, use the **no** form of this command.

ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]
no ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

Syntax Description

administrative-distance	(Optional) The administrative distance of the route. The default value is 1, which gives static routes precedence over any other type of routes except connected routes.
if_name	The name of the interface for which the route is being configured.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network.
ipv6-prefix	The IPv6 network that is the destination of the static route. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
tunneled	(Optional) Specifies the route as the default tunnel gateway for VPN traffic.

Command Default

By default, the administrative distance is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

Use the **show ipv6 route** command to view the contents of the IPv6 routing table.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the ASA that cannot

be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled**option:

- Do not enable unicast RPF (**ip verify reverse-path** command) on the egress interface of the tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route. Doing so causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, or SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the **tunneled**option; ECMP for tunneled traffic is not supported.

Examples

The following example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 with an administrative distance of 110:

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

Command	Description
debug ipv6 route	Displays debugging messages for IPv6 routing table updates and route cache updates.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 router ospf

To create an OSPFv3 routing process and enter IPv6 router configuration mode, use the **ipv6 router ospf** command in global configuration mode.

ipv6 router ospf *process-id*

Syntax Description

process-id	Specifies the internal identification, which is locally assigned and can be a positive integer from 1 to 65535. The number used is the number that is assigned administratively when you enable the OSPFv3 for IPv6 routing process.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **ipv6 router ospf** command is the global configuration command for OSPFv3 routing processes running on the ASA. After you enter the **ipv6 router ospf** command, the command prompt appears as (config-rtr)#, indicating that you are in IPv6 router configuration mode.

When using the **no ipv6 router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no ipv6 router ospf** command terminates the OSPFv3 routing process specified by its *process-id* argument**.** You assign the *process-id* value locally on the ASA. You must assign a unique value for each OSPFv3 routing process. You can use a maximum of two processes.

Use the **ipv6 router ospf** command in IPv6 router configuration mode to configure OSPFv3 routing processes with the following OSPFv3-specific options:

- **area**—Configures OSPFv3 area parameters. Supported parameters include the area ID as a decimal value from 0 to 4294967295 and the area ID in the IP address format of **A.B.C.D**.
- **default**—Sets a command to its default value. The **originate** parameter distributes the default route.
- **default-information**—Controls distribution of default information.
- **distance**—Defines the OSPFv3 route administrative distance based on the route type. Supported parameters include the administrative distance with values from 1 to 254 and **ospf** for the OSPF distance.

- **exit—**Exits IPv6 router configuration mode.
- **ignore**—Suppresses the sending of syslog messages with the **lsa** parameter when the router receives a link-state advertisement (LSA) for Type 6 Multicast OSPF (MOSPF) packets.
- **log-adjacency-changes**—Configures the router to send a syslog message when an OSPFv3 neighbor goes up or down. With the **detail** parameter, all state changes are logged.
- **passive-interface**—Suppresses routing updates on an interface with the following parameters:
  - **GigabitEthernet**—Specifies the GigabitEthernet IEEE 802.3z interface.
  - **Management**—Specifies the management interface.
  - **Port-channel**—Specifies the Ethernet channel of an interface.
  - **Redundant**—Specifies the redundant interface.
  - **default**—Suppresses routing updates on all interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain into another according to the following parameters:
  - **connected**—Specifies connected routes.
  - **ospf**—Specifies OSPF routes.
  - **static**—Specifies static routes.
- **router-id**—Creates a fixed router ID for a specified process with the following parameters:
  - **A.B.C.D**—Specifies the OSPF router ID in IP address format.
  - **cluster-pool**—Configures an IP address pool when Layer 3 clustering is configured.
- **summary-prefix**—Configures IPv6 address summaries with valid values from 0 to 128. The **X:X:X:X::X/** parameter specifies the IPv6 prefix.
- **timers—**Adjusts routing timers with the following parameters:
  - **lsa**—Specifies OSPF LSA timers.
  - **pacing**—Specifies OSPF pacing timers.
  - **throttle**—Specifies OSPF throttle timers.

Examples

The following example enables an OSPFv3 routing process and enters IPv6 router configuration mode:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
clear ipv6 ospf	Removes all IPv6 settings in the OSPFv3 routing process.

Command	Description
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6-split-tunnel-policy

To set a IPv6 split tunneling policy, use the **ipv6-split-tunnel-policy** command in group-policy configuration mode. To remove the ipv6-split-tunnel-policy attribute from the running configuration, use the **no** form of this command.

ipv6-split-tunnel-policy { **tunnelall** | **tunnelspecified** | **excludespecified** }
no ipv6-split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.
ipv6-split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the ASA. Remote users reach Internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's Internet service provider.

Command Default

IPv6 split tunneling is disabled by default, which is **tunnelall**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

IPv6 split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable IPv6 split tunneling.

This enables inheritance of a value for IPv6 split tunneling from another group policy.

IPv6 split tunneling lets a remote-access VPN client conditionally direct packets over an IPsec or SSL IPv6 tunnel in encrypted form, or to a network interface in cleartext form. With IPv6 split-tunneling enabled, packets

not bound for destinations on the other side of the IPsec or SSL VPN tunnel endpoint do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies IPv6 split tunneling policy to a specific network.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-split-
tunnel-policy tunnelspecified
```

Related Commands

Command	Description
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.

ipv6-vpn-address-assign

To specify a method for assigning IPv6 addresses to remote access clients, use the **ipv6-vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured VPN address assignment methods from the ASA, user the **no** version of this command. without arguments.

ipv6-vpn-addr-assign { **aaa** | **local** }
no ipv6-vpn-addr-assign { **aaa** | **local** }

Syntax Description

aaa	The ASA retrieves addresses from an external or internal (LOCAL) AAA (authentication, authorization, and accounting) server on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method.
local	The ASA distributes IPv6 addresses from internally configured address pools.

Command Default

Both the AAA and local VPN address assignment options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(2)	Support for multiple context mode was added.

Usage Guidelines

The ASA can use either the AAA or local methods for assigning IPv6 addresses to remote access clients. If you configure more than one address assignment method, the ASA searches each of the options until it finds an IPv6 address.

Examples

The following example shows how to configure AAA as the address assignment method.

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

The following example shows how to configure the use of a local address pool for the address assignment method.

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool to be used for VPN group policies.
show running-config group-policy	Shows the configuration for all group policies or for a particular group policy.
vpn-addr-assign	Specifies a method for assigning IPv4 addresses to remote access clients.

ipv6-vpn-filter

To specify the name of the IPv6 ACL to use for VPN connections, use the **ipv6-vpn-filter** command in group-policy configuration or username configuration mode. To remove the ACL, including a null value created by issuing the **ipv6-vpn-filter none** command, use the **no** form of this command.

ipv6-vpn-filter { **value** *IPV6-ACL-NAME* | **none** }
no ipv6-vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *IPV6-ACL-NAME*	Provides the name of the previously configured access list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	The **ipv6-vpn-filter** command was deprecated. Use the **vpn-filter** command to configure unified filters with either IPv4 and IPv6 entries. This IPv6 filter is only used if there are no IPv6 entries in the access list specified by the **vpn-filter** command.
9.1(4)	The **ipv6-vpn-filter** command has been disabled, only the "no" form of the command is allowed. Use **vpn-filter** command to configure unified filters for IPv4 and IPv6 entries. If this command is mistakenly used to specify IPv6 ACLs the connection is terminated.

Usage Guidelines

Clientless SSL VPN does not use the ACL defined in the **ipv6-vpn-filter** command.

The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **ipv6-vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **ipv6-vpn-filter** command to apply those ACLs.

Examples

The following example shows how to set a filter that invokes an access list named ipv6_acl_vpn for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-vpn-filter value ipv6_acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
vpn-filter	Specifies the names of an IPv4 or IPv6 ACL to use for VPN connections.

ip verify reverse-path

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip verify reverse-path interface *interface_name*
no ip verify reverse-path interface *interface_name*

Syntax Description

interface_name	The interface on which you want to enable Unicast RPF.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

Normally, the ASA only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the ASA to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the ASA, the ASA routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the ASA can use the default route to satisfy Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the ASA uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the ASA drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the ASA drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.

- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure that they arrived on the same interface used by the initial packet.

Examples

The following example enables Unicast RPF on the outside interface:

```
ciscoasa(config)# ip verify reverse-path interface outside
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the configuration set using the **ip verify reverse-path** command.
clear ip verify statistics	Clears the Unicast RPF statistics.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the configuration set using the **ip verify reverse-path** command.

ipv6 unnumbered

To borrow or inherit an IPv6 address from an interface (for example, a loopback interface), use the **ipv6 unnumbered** command in the interface configuration mode. To stop inheriting an ip address from an interface, use the **no** form of this command.

ipv6 unnumbered *interface-name*
no ipv6 unnumbered

Syntax Description

interface-name	Specifies the name of an interface to inherit the IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

The `ipv6 unnumbered` command is used to inherit the IPv6 address of the selected *`interface`* as the address for the current interface.

Examples

The following example borrows the IPv6 address from the loopback interface and uses it for the VTI tunnel interface:

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ipv6 unnumbered loopback1
```

Related Commands

Command	Description
ip unnumbered *interface-name*	Inherits the IP address of the specified interface.
interface loopback *loopback-number*	Creates a loopback interface.

is – iz

isakmp am-disable (Deprecated)

To disable inbound aggressive mode connections, use the **isakmp am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

isakmp am-disable
no isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp am-disable** command replaced it.

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
ciscoasa(config)# isakmp am-disable
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp disconnect-notify (Deprecated)

To enable disconnect notification to peers, use the **isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

isakmp disconnect-notify
no isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp disconnect-notify** command replaced it.

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
ciscoasa(config)# isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp enable (Deprecated)

To enable ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA, use the **isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

isakmp enable *interface-name*
no isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp enable** command replaced it.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
ciscoasa(config)# no isakmp enable
 inside
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp identity (Deprecated)

To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }
no isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISKMP negotiation by connection type; IP address for the preshared key or certificate DN for certificate authentication.
hostname	Uses the fully qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Command Default

The default ISAKMP identity is the **isakmp identity hostname** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp identity** command replaced it.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPsec peer, depending on connection type:

```
ciscoasa(config)# isakmp identity auto
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.

Command	Description
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp ipsec-over-tcp (Deprecated)

To enable IPsec over TCP, use the **isakmp ipsec-over-tcp** command in global configuration mode. To disable IPsec over TCP, use the **no** form of this command.

isakmp ipsec-over-tcp [**port** *port1...port10*]
no isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPsec over TCP connections. You can list up to 10 ports. Port numbers can be in the range of 1-65535. The default port number is 10000.

Command Default

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp ipsec-over-tcp** command replaces it.

Examples

This example, entered in global configuration mode, enables IPsec over TCP on port 45:

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp keepalive

To configure IKE keepalives, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]
no isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]

Syntax Description

disable	Disables IKE keepalive processing, which is enabled by default.
infinite	The ASA never initiates keepalive monitoring.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds that the peer can idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10 seconds for a LAN-to-LAN group, and 300 second for a remote access group.

Command Default

The default for a remote access group is a threshold of 300 seconds and a retry of 2 seconds.

For a LAN-to-LAN group, the default is a threshold of 10 seconds and a retry of 2 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. You can apply this attribute only to IPsec remote access and IPsec LAN-to-LAN tunnel group types.

Examples

The following example entered in tunnel-group ipsec-attributes configuration mode, configures IKE DPD, establishes a threshold of 15, and specifies a retry interval of 10 for the IPsec LAN-to-LAN tunnel group with the IP address 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
```

```
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel group IPsec attributes for this group.

isakmp nat-traversal (Deprecated)

To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **isakmp enable** command) in global configuration mode and then use the **isakmp nat-traversal** command. If you have enabled NAT traversal, you can disable it with the **no** form of this command.

isakmp nat-traversal *natkeepalive*
no isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keepalive interval, from 10 to 3600 seconds. The default is 20 seconds.

Command Default

By default, NAT traversal (**isakmp nat-traversal** command) is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp nat-traversal** command replaced it.

Usage Guidelines

Network Address Translation (NAT), including Port Address Translation (PAT), is used in many networks where IPsec is also used, but there are a number of incompatibilities that prevent IPsec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The ASA supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html , and NAT traversal is supported for both dynamic and static crypto maps.

This command enables NAT-T globally on the ASA. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then enables NAT traversal with an interval of 30 seconds:

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy authentication

To specify an authentication method within an IKE policy, use the **isakmp policy authentication** command in global configuration mode. To remove the ISAKMP authentication method, use the **clear configure** command.

isakmp policy *priority* **authentication** { **crack** | **pre-share** | **rsa-sig** }

Syntax Description

crack	Specifies IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This means you can prove to a third party whether or not you had an IKE negotiation with the peer.

Command Default

The default ISAKMP policy authentication is the **pre-share** option.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

IKE policies define a set of parameters for IKE negotiation. If you specify RSA signatures, you must configure the ASA and its peer to obtain certificates from a certification authority (CA). If you specify preshared keys, you must separately configure these preshared keys within the ASA and its peer.

Examples

The following example, entered in global configuration mode, sets the authentication method of RSA signatures to be used within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy encryption (Deprecated)

To specify the encryption algorithm to use within an IKE policy, use the **isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, use the **no** form of this command.

isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }
no isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }

Syntax Description

3des	Specifies that the triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default ISAKMP policy encryption is **3des**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy encryption** command replaced it.

Examples

The following example, entered in global configuration mode, sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25:

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy group (Deprecated)

To specify the Diffie-Hellman group for an IKE policy, use the **isakmp policy group** command in global configuration mode.To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

isakmp policy *priority* **group** { **1** | **2** | **5** }
no isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Command Default

The default is group 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added. Group 7 was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy group** command replaced it.

Usage Guidelines

IKE policies define a set of parameters to use during IKE negotiation.

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires ISAKMP policy to have DH group 2 configured. (If you have DH group 1 configured, the Cisco VPN Client cannot connect.)AES support is available on ASAs licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) group 5 instead of group 1 or group 2. This is done with the **isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 group   2
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy hash (Deprecated)

To specify the hash algorithm for an IKE policy, use the **isakmp policy hash** command in global configuration mode.To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

isakmp policy *priority* **hash** { **md5** | **sha** }
no isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) be used as the hash algorithm in the IKE policy.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies that SHA-1 (HMAC variant) be used as the hash algorithm in the IKE policy.

Command Default

The default hash algorithm is SHA-1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy hash** command replaces it.

Usage Guidelines

IKE policies define a set of parameters to be used during IKE negotiation.

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, specifies that the MD5 hash algorithm be used within the IKE policy, with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 hash    md5
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.

Command	Description
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy lifetime (Deprecated)

To specify the lifetime of an IKE security association before it expires, use the **isakmp policy lifetime** command in global configuration mode. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

isakmp policy *priority* **lifetime** *seconds*
no isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime.

Command Default

The default value is 86,400 seconds (one day).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy lifetime** command replaced it.

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPsec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default, but you can specify an infinite lifetime if the peer does not propose a lifetime.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) within the IKE policy with the priority number of 40:

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

Related Commands

clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp reload-wait (Deprecated)

To enable waiting for all active sessions to voluntarily terminate before rebooting the ASA, use the **isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the ASA, use the **no** form of this command.

isakmp reload-wait
no isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was deprecated. The **crypto isakmp reload-wait** command replaced it.

Examples

The following example, entered in global configuration mode, tells the ASA to wait until all active sessions have terminated before rebooting:

```
ciscoasa(config)# isakmp reload-wait
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isis priority

To configure the priority of designated ASAs on an interface, use the **isis priority** command in interface isis configuration mode. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]
no isis priority [**level-1** | **level-2**]

Syntax Description

number-value	Sets the priority of a router. The range is 0 to 127.
level-1	(Optional) Sets the priority for Level 1 independently.
level-2	(Optional) Sets the priority for Level 2 independently.

Command Default

The default is 64.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface isis Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command sets the priority that is used to determine which ASA on a LAN will be the designated router or DIS. The priorities are advertised in the hello packets. The ASA with the highest priority becomes the DIS.

Note In IS-IS there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If an ASA with a higher priority comes on line, it takes over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

Examples

The following example shows Level 1 routing given priority by setting the priority level to 80. This ASA is now more likely to become the DIS:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis priority 80 level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

isis protocol shutdown

To disable the IS-IS protocol so that it cannot form adjacencies on a specified interface and place the IP address of the interface into the LSP that is generated by the ASA, use the **isis protocol shutdown** command in interface isis configuration mode. To reenable the IS-IS protocol, use the **no** form of this command.

isis protocol shutdown
no isis protocol shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command lets you disable the IS-IS protocol for a specified interface without removing the configuration parameters. The IS-IS protocol does not form any adjacencies for the interface for which this command has been configured, and the IP address of the interface is put into the LSP that is generated by the ASA. Use the **protocol shutdown** command if you do not want IS-IS to form any adjacency on any interface and to clear the IS-IS LSP database.

Examples

The following example disables the IS-IS protocol on GigabitEthernet 0/0:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis protocol shutdown
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

isis retransmit-interval

To configure the amount of time between retransmission of each IS-IS LSP, use the **isis retransmit-interval** command in interface isis configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-interval *seconds*
no isis retransmit-interval *seconds*

Syntax Description

seconds	(Optional) The time between retransmission of each LSP. The number should be greater than the expected round-trip delay between any two routers on the attached network. The range is 0 to 65535.

Command Default

The default is 5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

Make sure the *seconds* argument is conservative, otherwise needless retransmission results. This command has no effect on LAN (multi-point) interfaces.

Examples

The following example configures GigabitEthernet 0/0 for retransmission of each IS-IS LSP every 60 seconds for a large serial line:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-interval 60
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

isis retransmit-throttle-interval

To configure the amount of time between retransmissions of each IS-IS LSP on an interface, use the **isis retransmit-throttle-interval** command in interface isis configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-throttle-interval *milliseconds*
no isis retransmit-throttle-interval

Syntax Description

milliseconds	(Optional) The minimum delay between LSP retransmission on the interface. The range is 0 to 65535.

Command Default

The delay is determined by the **isis lsp-interval** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command can be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be resent on the interface.

This command is distinct from the rate at which LSPs are sent on the interface (controlled by the **isis lsp-interval** command) and the period between retransmissions of a single LSP (controlled by the **isis retransmit-interval** command). You can use these commands in combination to control the offered load of routing traffic from one ASA to its neighbors.

Examples

The following example configures GigabitEthernet 0/0 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-throttle-interval 300
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

isis tag

To set a tag on the IP address configured for an interface when this IP prefix is put into an IS-IS LSP, use the **isis tag** command in interface isis configuration mode. To stop tagging the IP address, use the **no** form of this command.

isis tag *tag-number*
no isis tag *tag-number*

Syntax Description

tag-number	The number that serves as a tag on an IS-IS route. The range is 1 to 4294967295.

Command Default

No route tag is associated for IP addresses configured for the interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface isis configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes. Configuring this command triggers the ASA to generate new LSPs because the tag is a new piece of information in the packet.

Examples

The following example configures GigabitEthernet 0/0 to have a tag of 100:

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis tag 100
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

is-type

To configure the routing level for an instance of the IS-IS routing process, use the **is-type** command in router isis configuration mode. To reset the default value, use the **no** form of this command.

isis type [**level-1** | **level 1-2** | **level-2-only**
no isis type [**level-1** | **level 1-2** | **level-2-only**

Syntax Description

level-1	(Optional) Indicates intra-area routing. This ASA only learns about destinations inside its area. Level 2 (inter-area) routing is performed by the closest Level 1-2 ASA.
level-1-2	(Optional) The ASA performs both Level 1 and Level 2 routing. This ASA runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
level-2-only	(Optional) Indicates inter-area routing. This ASA is part of the backbone and does not communicate with Level 1-only ASAs in its own area.

Command Default

In conventional IS-IS configurations, the ASA acts as both a Level 1 (intra-area) and a Level 2 (inter-area) router.

In multi-area IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and inter-area) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

We highly recommend that you configure the type of IS-IS routing process. If you are configuring multi-area IS-IS, you must configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If only one area is in the network, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must

be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are by default Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process), you can remove Level 2 (inter-area) routing for the area using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area.

Examples

The following example specifies an area router:

```
ciscoasa#
router isis
ciscoasa(config-router)#
is-type level-2-only
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.

Command	Description
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.

Command	Description
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

issuer (Deprecated)

Note The last supported release of this command was Version 9.5(1).

To specify the security device that is sending assertions to a SAML-type SSO server, use the **issuer** command in webvpn-sso-saml configuration mode for that specific SAML type. To remove the issuer name, use the **no** form of this command.

issuer*identifier*
no issuer [*identifier*]

Syntax Description

identifier	Specifies a security device name, usually the hostname of the device. An identifier must be less than 65 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn-sso-saml configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

SSO support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

Examples

The following example specifies the issuer name for a security device named asa1.example.com:

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

Related Commands

Command	Description
assertion-consumer-url	Specifies the URL that the security device uses to contact the SAML-type SSO server assertion consumer service.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

issuer-name

To specify the issuer name DN of all issued certificates, use the **issuer-name** command in local certificate authority (CA) server configuration mode. To remove the subject DN from the certificate authority certificate, use the **no** form of this command.

issuer-name*DN-string*
no issuer-name *DN-string*

Syntax Description

DN-string	Specifies the distinguished name of the certificate, which is also the subject name DN of the self-signed CA certificate. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. An issuer name must be less than 500 alphanumeric characters.

Command Default

The default issuer name is cn=*hostame.domain-name*, for example cn=asa.example.com.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.3(1)	This command was added.
8.0(2)	Support for quotation marks was added to retain commas in *DN-string* values.

Usage Guidelines

This command specifies the issuer name that appears on any certificate created by the local CA server. Use this optional command if you want the issuer name to be different from the default CA name.

Note This issuer name configuration cannot be changed after you have enabled the CA server and generated the certificate by issuing the **no shutdown** command.

Examples

The following example configures certificate authentication:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc.”
```

```
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca server configuration mode commands, which allow you to configure and manage the local CA.
keysize	Specifies the size of the public and private keys generated at certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate and issued certificates.
show crypto ca server	Displays the characteristics of the local CA.
show crypto ca server cert-db	Displays local CA server certificates.

PART II

J - M Commands

j – k

java-trustpoint(Deprecated)

To configure the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location, use the **java-trustpoint** command in webvpn configuration mode.To remove a trustpoint for Java object signing, use the **no** form of this command.

java-trustpoint*trustpoint*
no java-trustpoint

Syntax Description

trustpoint	Specifies the trustpoint location configured by the **crypto ca import** command.

Command Default

By default, a trustpoint for Java object signing is set to none.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(2)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

A trustpoint is a representation of a certificate authority (CA) or identity key pair. For the **java-trustpoint** command, the given trustpoint must contain the X.509 certificate of the application signing entity, the RSA private key corresponding to that certificate, and a certificate authority chain extending up to a root CA. This is typically achieved by using the **crypto ca import** command to import a PKCS12 formatted bundle. You can obtain a PKCS12 bundle from a trusted CA authority or you can manually create one from an existing X.509 certificate and an RSA private key using open source tools such as openssl.

Note An uploaded certificate cannot be used to sign Java objects that are embedded with packages (for example, the CSD package).

Examples

The following example first configures a new trustpoint, then configures it for WebVPN Java object signing:

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
```

```
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

The following example configures the new trustpoint for signing WebVPN Java objects:

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca import	Imports the certificate and key pair for a trustpoint using PKCS12 data.

join-failover-group

To assign a context to a failover group, use the **join-failover-group** command in context configuration mode. To restore the default setting, use the **no** form of this command.

join-failover-group*group_num*
no join-failover-group *group_num*

Syntax Description

group_num	Specifies the failover group number.

Command Default

Failover group 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	• Yes	• Yes	—	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The admin context is always assigned to failover group 1. You can use the **show context detail** command to display the failover group and context association.

Before you can assign a context to a failover group, you must create the failover group with the **failover group** command in the system context. Enter this command on the unit where the context is in the active state. By default, unassigned contexts are members of failover group 1, so if the context had not been previously assigned to a failover group, you should enter this command on the unit that has failover group 1 in the active state.

You must remove all contexts from a failover group, using the **no join-failover-group** command, before you can remove a failover group from the system.

Examples

The following example assigns a context named ctx1 to failover group 2:

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

Related Commands

Command	Description
context	Enters context configuration mode for the specified context.

Command	Description
failover group	Defines a failover group for Active/Active failover.
show context detail	Displays context detail information, including name, class, interfaces, failover group association, and configuration file URL.

jumbo-frame reservation

To enable jumbo frames for supported models, use the **jumbo-frame reservation** command in global configuration mode. To disable jumbo frames, use the **no** form of this command.

Note Changes in this setting require you to reboot the ASA.

jumbo-frame reservation
no jumbo-frame reservation

Syntax Description

This command has no arguments or keywords.

Command Default

Jumbo frame reservation is disabled by default on ASA hardware, ASA virtual, and ISA 3000.

Jumbo frames are supported by default on other models.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	This command was added for the ASA 5580.
8.2(5)/8.4(1)	Support for the ASA 5585-X was added.
8.6(1)	Support for the ASA 5512-X through ASA 5555-X was added.
9.3(2)	Support for the ASA 5506-X was added.
9.3(3)	Support for the ASA 5508-X and 5516-X was added.

Usage Guidelines

This procedure only applies to ASA hardware models, the ISA 3000 and the ASA virtual. Other models support jumbo frames by default.

Jumbo frames are not supported on the ASAv5 and ASAv10 with less than 8GB RAM.

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and VLAN tagging, 18 bytes), up to 9216 bytes. Note that the **mtu** command specifies the *payload* value only, so for a 9216 byte jumbo frame, set the MTU to be 9198 (9216-18 bytes for the header)

Jumbo frame support requires extra memory, which might limit the maximum use of other features, such as access lists.

Jumbo frames are not supported on the Management *n* /*n* interface.

Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9198 using the **mtu** command. For the ASASM, you do not need to set the **jumbo-frame** reservation command; it supports jumbo frames by default. Just set the MTU to the desired value.

Also, be sure to configure the MSS (maximum segment size) value for TCP when using jumbo frames. The MSS should be 120 bytes less than the MTU. For example, if you configure the MTU to be 9000, then the MSS should be configured to 8880. You can configure the MSS with the **sysopt connection tcpmss** command.

Both the primary and the secondary units require a reboot so that the failover pair supports jumbo frames. To avoid downtime, do the following:

- Issue the command on the active unit.
- Save the running configuration on the active unit.
- Reboot the primary and secondary units, one at a time.

Examples

The following example enables jumbo frame reservation, saves the configuration, and reloads the ASA:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5
70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

Related Commands

Command	Description
mtu	Specifies the maximum transmission unit for an interface.
show jumbo-frame reservation	Shows the current configuration of the **jumbo-frame reservation** command.

kcd-server

To configure Kerberos Constrained Delegation (KCD) for clientless SSL remote access VPN, use the **kcd-server** command in webvpn configuration mode. To disable KCD, use the **no** form of this command.

kcd-server *aaa-server-group_name* **username** *user_id* **password** *password* [**validate-server-certificate**]
no kcd-server

Syntax Description

username	Specifies the Active Directory user with administrator or service level privileges to add devices to the domain.
password	Specifies the password for the user.
validate-server-certificate	(Optional.) Instructs the ASA to validate the server certificate and thus the identity of the server when joining the domain. If you omit this option, the system assumes the domain controller is valid.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.15(1)	The **validate-server-certificate** keyword was added.

Usage Guidelines

Use the **kcd-server** command in webvpn configuration mode to allow the ASA to join an Active Directory domain. The domain controller name and realm are specified in the **aaa-server-groupname** command. The AAA server group has to be a Kerberos server type. The **username** and **password** options do not correspond to a user with Administrator privileges, but they should correspond to a user with service-level privileges on the domain controller. To view the existing configuration, use the **show webvpn kcd** command.

Kerberos Constrained Delegation, or KCD, in the ASA environment provides clientless SSL remote access VPN users Single Sign-on (SSO) access to all web services that are protected by Kerberos. The ASA maintains a credential on behalf of the user (a service ticket) and uses this ticket to authenticate the user to the services.

In order for the **kcd-server** command to function, the ASA must establish a trust relationship between the *source* domain (the domain where the ASA resides) and the *target* or *resource* domain (the domain where

the web services reside). The ASA crosses the certification path from the source to the destination domain and acquires the necessary tickets on behalf of the remote access user to access the services.

This path is called cross-realm authentication. During each phase of cross-realm authentication, the ASA relies on the credentials at a particular domain and the trust relationship with the subsequent domain.

The KCD configuration also requires that you configure the domain controller as a DNS server (for example, in the DefaultDNS group), and enable DNS lookup on the interface through which the domain controller can be reached.

Examples

The following is a configuration example of KCD, where the Domain Controller is 10.1.1.10 (reachable via inside interface) and the domain name is PRIVATE.NET. Additionally, the Service Account username and password on the domain controller is dcuser and dcuser123! .

```
----Enable a DNS lookup by configuring the DNS server and Domain name --------------
ciscoasa
(config)#
dns domain-lookup inside
ciscoasa
(config)#
dns server-group DefaultDNS
ciscoasa
(config-dns-server-group)#
name-server 10.1.1.10
ciscoasa
(config-dns-server-group)#
domain-name
private.net
----Configure the AAA server group with Server and Realm-------------------------------
ciscoasa
(config)#
aaa-server KerberosGroup protocol Kerberos
ciscoasa
(config-asa-server-group)#
aaa-server KerberosGroup (inside) host 10.1.1.10
ciscoasa
(config-asa-server-group)#
kerberos-realm PRIVATE.NET
----Enable KCD-----------------------------
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
kcd-server KerberosGroup username dcuser password dcuser123!
validate-server-certificate
```

Related Commands

Command	Description
aaa-server	Enters aaa-server configuration mode, so you can configure AAA server parameters.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
show aaa kerberos	Displays Kerberos tickets.
show webvpn kcd	Displays the KCD configuration.

keepout

To present an administrator-defined message rather than a login page for new user sessions (when the ASA undergoes a maintenance or troubleshooting period), use the **keepout** command in webvpn configuration mode. To remove a previously set keepout page, use the **no** version of the command.

keepout
no keepout *string*

Syntax Description

string	An alphanumeric string in double quotation marks.

Command Default

No keepout page.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

When this command is enabled, the clientless WebVPN portal page becomes unavailable. You receive an administrator-defined message stating the unavailability of the portal rather than a login page for the portal. Use the **keepout** command to disable clientless access, but still allow AnyConnect access. You can also use this command to indicate portal unavailability when maintenance is occurring.

Note If HostScan is installed, the keepout feature does not stop the ASA from opening pages like Cisco Secure Desktop portal. To avoid the Cisco Secure Desktop port, HostScan needs to be uninstalled.

Examples

The following example shows how to configure a keepout page:

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 keepout "The system is unavailable until 7:00 a.m. EST."
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn configuration mode, which lets you configure attributes for clientless SSL VPN connections.

kerberos-realm

To specify the realm name for this Kerberos server, use the **kerberos-realm** command in aaa-server host configuration mode. To remove the realm name, use the **no** form of this command:

kerberos-realm*string*
no kerberos-realm

Syntax Description

string A case-sensitive, alphanumeric string, up to 64 characters long. Spaces are not permitted in the string.

Note Kerberos realm names use numbers and upper case letters only. Although the ASA accepts lower case letters in the *string* argument, it does not translate lower case letters to upper case letters. Be sure to use upper case letters only.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for Kerberos servers.

The value of the *string* argument should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Windows 2000 Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

The *string* argument must use numbers and upper case letters only. The **kerberos-realm** command is case sensitive, and the ASA does not translate lower case letters to upper case letters.

Examples

The following sequence shows the **kerberos-realm** command to set the kerberos realm to "EXAMPLE.COM" in the context of configuring a AAA server host:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration submode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

key (aaa-server host)

To specify the server secret value used to authenticate the NAS to the AAA server, use the **key** command in aaa-server host configuration mode. The aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove the key, use the **no** form of this command.

key [**0** | **8**] *key*
no key

Syntax Description

key An alphanumeric keyword, which can be up to 127 characters long. You can optionally precede the key with a number to indicate encryption:

- 0 means the key is not encrypted. This is the default.
- 8 means the key is an AES encrypted base64 hash.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The *key* value is a case-sensitive, alphanumeric keyword of up to 127 characters, which is the same value as the key on the TACACS+ server. Any characters over 127 are ignored. The key is used between the client and the server for encrypting data between them. The key must be the same on both the client and server systems.The key cannot contain spaces, but other special characters are allowed. The key (server secret) value authenticates the ASA to the AAA server.

This command is valid only for RADIUS and TACACS+ servers.

Examples

The following example configures a TACACS+ AAA server named “srvgrp1” on host “1.2.3.4,” sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the key as “myexclusivemumblekey.”

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure host-specific AAA server parameters.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays the AAA server configuration.

key (cluster group)

To set an authentication key for control traffic on the cluster control link, use the **key** command in cluster group configuration mode. To remove the key, use the **no** form of this command.

key *shared_secret*
no key [*shared_secret*]

Syntax Description

shared_secret	Sets the shared secret to an ASCII string from 1 to 63 characters. The shared secret is used to generate the key.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

Examples

The following example sets a shared secret:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.

Command	Description
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

key chain

To configure rotating keys for authenticating IGP peers, use the **key chain** command in the global configuration mode. To remove the configuration, use the **no** form of the command.

key chain *key-chain-name* **key** *key-id* **key-string** { **0** | **8** } *key-string-text* **cryptographic-algorithm md5** [**accept-lifetime** [*local* | *start-time*] [**duration** { *duration value* | *infinite* | *end-time* }]

no key chain *key-chain-name* **key** *key-id* **key-string** { **0** | **8** } *key-string-text* **cryptographic-algorithm md5** [**accept-lifetime** [*local* | *start-time*] [**duration** { *duration value* | *infinite* | *end-time* }]

Syntax Description

key-chain-name	The name for the key chain to be configured for OSPFv2 authentication.
key-id	The unique identifier in the key chain; the valid range being 1 to 255.
0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
key-string-text	The password for the key id. The string can be a plain text or an encrypted value.
md5	The supported cryptographic algorithm. Only md5 is supported.
accept-lifetime	(Optional) The time interval within which the device accepts the key during key exchange with another device.
send-lifetime	(Optional) The time interval within which the device sends the key during key exchange with another device.

Command Default

The accept or send lifetimes, if not specified, is always active by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• No

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

Use **key chain** command to configure the key chain to be used in OSPFv2 authentication for an interface. You must enter the **key id**, **key string,** and the **cryptographic-algorithm** command. Enter **accept and send lifetimes** to schedule the rotation of keys. The lifetime variables helps to handle secured key rollover. The

device uses the lifetimes of keys to determine which keys in a key chain are active at any given point in time. When the lifetimes are not specified, the key chain authentication functions similar to that of MD5 authentication without time lines. Use the **no key chain** to remove the configuration of the key chain.

Examples

The following example shows the key chain configuration commands:

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite

ciscoasa(config-keychain-key)#
```

Examples

The following example provides the output of the running key chain configuration:

```
ciscoasa# show running key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# show runing key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Related Commands

Command	Description
show key chain	Displays the configured key chains
show running key chain	Displays the key chain details that is currently active
clear configure key chain	Removes the key chains configured

key config-key password-encryption

To set the master passphrase used for generating the encryption key to securely store plain text passwords in encrypted format, use the **key config-key password-encryption** command in global configuration mode. To decrypt passwords encrypted with the passphrase, use the no form of this command.

key config-key password-encryption *passphrase* [*old_passphrase*]
no key config-key password-encryption *passphrase*

Syntax Description

passphrase	The passphrase must be between 8 and 128 character long. All characters except the backspace and double quote will be accepted for the passphrase. If you do not enter the passphrase in the command, you are prompted for it. Use the interactive prompts to enter passwords to avoid having the passwords logged in the command history buffer.
old_passphrase	If you are changing the passphrase, enter the old passphrase.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

Features that use the master passphrase include the following:

- OSPF
- EIGRP
- VPN load balancing
- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses

You must enter both the **key config-key password-encrypt** command and the **password encryption aes** command in any order to trigger password encryption. Enter **write memory** to save the encrypted passwords to the startup configuration. Otherwise, passwords in the startup configuration may still be visible. In multiple context mode, use **write memory all** in the system execution space to save all context configurations.

This command will only be accepted in a secure session, for example by console, SSH, or ASDM via HTTPS.

Use the **no key config-key password-encrypt** command with caution, because it changes the encrypted passwords into plain text passwords. You might use the **no** form of this command when downgrading to a software version that does not support password encryption.

If failover is enabled but no failover shared key is set, an error message appears if you change the master passphrase, informing you that you must enter a failover shared key to protect the master passphrase changes from being sent as plain text.

Enabling or changing password encryption in Active/Standby failover causes a **write standby**, which replicates the active configuration to the standby unit. Without this replication, the encrypted passwords on the standby unit will differ even though they use the same passphrase; configuration replication ensures that the configurations are the same. For Active/Active failover, you must manually enter **write standby**. A **write standby** can cause traffic interruption in Active/Active mode, because the configuration is cleared on the secondary unit before the new configuration is synced. You should make all contexts active on the primary ASA using the **failover active group 1** and **failover active group 2** commands, enter **write standby**, and then restore the group 2 contexts to the secondary unit using the **no failover active group 2** command.

The write erase command when followed by the reload command will remove the master passphrase and all configuration if it is lost.

Examples

The following example sets the passphrase used for generating the encryption key, and enables password encryption:

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

Command	Description
password encryption aes	Enables password encryption.
write erase	Removes the master passphrase if it is lost when followed by the reload command.

key-hash

To manually add a hashed SSH host key for a server for the on-board Secure Copy (SCP) client, use the **key-hash** command in server configuration mode. You can access the server configuration mode by first entering the **ssh pubkey-chain** command. To remove the key, use the **no** form of this command.

key-hash { **md5** | **sha256** } *fingerprint*
no key-hash { **md5** | **sha256** } *fingerprint*

Syntax Description

fingerprint	Enters the hashed key.
{md5 | sha256}	Sets the type of hash used, either MD5 or SHA-256. The ASA always uses SHA-256 in its configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Server configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

You can copy files to and from the ASA using the on-board SCP client. The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.

For each server, you can specify the **key-string** (public key) or **key-hash** (hashed value) of the SSH host. The **key-hash** enters the already hashed key (using an MD5 or SHA-256 key); for example, a key that you copied from **show** command output.

Examples

The following example adds an already hashed host key for the server at 10.86.94.170:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

Command	Description
copy	Copies a file to or from the ASA.
key-hash	Enters a hashed SSH host key.
key-string	Enters a public SSH host key.
ssh pubkey-chain	Manually adds or deletes servers and their keys from the ASA database.
ssh stricthostkeycheck	Enables SSH host key checking for the on-board Secure Copy (SCP) client.

keypair

To specify the key pair whose public key is to be certified, use the **keypair** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

[no] keypair *name* | [**rsa modulus** | **2048** | **4096**] | [**ecdsa elliptic-curve 256** | **384** | **521**] | [**eddsa edwards-curve Ed25519**]

Syntax Description

name	Specifies the name of the key pair for non-CMP enrollments.
rsa	Generate RSA keys for any CMP manual and automatic enrollments.
ecdsa	Generate ECDSA keys for any CMP manual and automatic enrollments.
eddsa	Generate EdDSA keys for any CMP manual and automatic enrollments.

Command Default

The default setting is not to include the key pair.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	New EDCSA and RSA keypairs were added.
9.16(1)	• Support to certificates with RSA key sizes smaller than 2048 bits was removed. Hence the rsa modulus options were modified to display 2048 bits and bigger values. • New EdDSA keypair was added.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint central, and specifies a key pair to be certified for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.
crypto key generate dsa	Generates DSA keys.
crypto key generate rsa	Generates RSA keys.
default enrollment	Returns enrollment parameters to their defaults.

keysize

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server at user certificate enrollment, use the **keysize** command in ca-server configuration mode. To reset the keysize to the default length of 1024 bits, use the **no** form of this command.

keysize*size*
no keysize

Syntax Description

size The size of the key, in bits. The size can be one of the following:

- 512
- 768
- 1024
- 2048
- 4096

Command Default

By default, each key in the key pair is 1024 bits long.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.13(1)	This command was removed.

Examples

The following example specifies a key size of 2048 bits for all public and private key pairs generated for users by the local CA server:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize 2048
ciscoasa
```

```
(config-ca-server)
#
```

The following example resets the key size to the default length of 1024 bits for all public and private key pairs generated for users by the local CA server:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca-server configuration mode command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject name DN of the certificate authority certificate.
subject-name-default	Specifies a generic subject name DN to be used along with the username in all user certificates issued by a CA server.

keysize server

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server for configuring the size of the CA keypair, use the **keysize server** command in ca-server configuration mode. To reset the keysize to the default length of 1024 bits, use the **no** form of this command.

keysize server *size*
no keysize server

Syntax Description

size The size of the key, in bits. The size can be one of the following:

- 512
- 768
- 1024
- 2048
- 4096

Command Default

By default, each key in the key pair is 1024 bits long.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.13(1)	This command was removed.

Examples

The following example specifies a key size of 2048 bits for the CA certificate:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize server 2048
ciscoasa
(config-ca-server)
#
```

The following example resets the key size to the default length of 1024 bits for the CA certificate:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize server
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca-server configuration mode command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject name DN of the certificate authority certificate.
keysize	Specifies the key pair size for the user certificate.
subject-name-default	Specifies a generic subject name DN to be used along with the username in all user certificates issued by a CA server.

key-string

To manually add a public SSH host key for a server for the on-board Secure Copy (SCP) client, use the **key-string** command in server configuration mode. You can access the server configuration mode by first entering the **ssh pubkey-chain** command. This command prompts you to enter a key string. When the string is saved to the configuration, it is hashed using SHA-256, and stored as the **key-hash** command. Therefore, to remove the string, use the **no key-hash** command.

key-string *key_string*

Syntax Description

key_string	Enters the public key.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Server configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

You can copy files to and from the ASA using the on-board SCP client. The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.

For each server, you can specify the **key-string** (public key) or **key-hash** (hashed value) of the SSH host. The *key_string* is the Base64 encoded RSA public key of the remote peer. You can obtain the public key value from an open SSH client; that is, from the .ssh/id_rsa.pub file. After you submit the Base64 encoded public key, that key is then hashed via SHA-256.

Examples

The following example adds a host string key for the server at 10.7.8.9:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

The following example shows the saved hashed key:

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

Command	Description
copy	Copies a file to or from the ASA.
key-hash	Enters a hashed SSH host key.
key-string	Enters a public SSH host key.
ssh pubkey-chain	Manually adds or deletes servers and their keys from the ASA database.
ssh stricthostkeycheck	Enables SSH host key checking for the on-board Secure Copy (SCP) client.

kill

To terminate a Telnet session, use the **kill** command in privileged EXEC mode.

kill*telnet_id*

Syntax Description

telnet_id	Specifies the Telnet session ID.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **kill** command lets you terminate a Telnet session. Use the who command to see the Telnet session ID. When you kill a Telnet session, the ASA lets any active commands terminate and then drops the connection without warning.

Examples

The following example shows how to terminate a Telnet session with the ID “2”. First, the who command is entered to display the list of active Telnet sessions. Then the **kill 2** command is entered to terminate the Telnet session with the ID “2”.

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

Related Commands

Command	Description
telnet	Configures Telnet access to the ASA.
who	Displays a list of active Telnet sessions.

l2 – lof

l2tp tunnel hello

To specify the interval between hello messages on L2TP over IPsec connections, use the **l2tp tunnel hello** command in global configuration mode. To reset the interval to the default, use the **no** form of the command:

l2tp tunnel hello *interval*
no l2tp tunnel hello *interval*

Syntax Description

interval	Interval between hello messages in seconds. The Default is 60 seconds. The range is 10 to 300 seconds.

Command Default

The default is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **l2tp tunnel hello** command enables the ASA to detect problems with the physical layer of the L2TP connection. The default is 60 secs. With the default setting in place, you can expect the L2TP tunnel to disconnect after 180 seconds. If you configure it to a lower value, connections that are experiencing problems are disconnected earlier. The maximum retry of L2TP is 3.

Examples

The following example configures the interval between hello messages to 30 seconds:

```
ciscoasa(config)# l2tp tunnel hello 30
```

Related Commands

Command	Description
show vpn-sessiondb detail remote filter protocol L2TPOverIPsec	Displays the details of L2TP connections.
vpn-tunnel-protocol l2tp-ipsec	Enables L2TP as a tunneling protocol for a specific tunnel group.

lacp max-bundle

To specify the maximum number of active interfaces allowed in the EtherChannel channel group, use the **lacp max-bundle** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp max-bundle *number*
no lacp max-bundle

Syntax Description

number	Specifies the maximum number of active interfaces allowed in the channel group, between 1 and 8; for 9.2(1) and later, the maximum is rasied to 16. If your switch does not support 16 active interfaces, be sure to set this command to 8 or fewer.

Command Default

(9.1 and earlier) The default is 8.

(9.2(1) and later) The default is 16.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.2(1)	The number of active interfaces was raised from 8 to 16.

Usage Guidelines

Enter this command for a port-channel interface. The maximum number of active interfaces per channel group is eight; to decrease the number, use this command.

Examples

The following example sets the maximum number of interfaces in the EtherChannel to four:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

lacp port-priority

To set the priority for a physical interface in an EtherChannel, use the **lacp port-priority** command in interface configuration mode. To set the priority to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp port-priority *number*
no lacp port-priority

Syntax Description

number	Sets the priority between 1 and 65535. The higher the number, the lower the priority.

Command Default

The default is 32768.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

Enter this command for a physical interface. The ASA uses this setting to decide which interfaces are active and which are standby if you assign more interfaces than can be used. If the port priority setting is the same for all interfaces, then the priority is determined by the interface ID (slot/port). The lowest interface ID is the highest priority. For example, GigabitEthernet 0/0 is a higher priority than GigabitEthernet 0/1.

If you want to prioritize an interface to be active even though it has a higher interface ID, then set this command to have a lower value. For example, to make GigabitEthernet 1/3 active before GigabitEthernet 0/7, then make the **lacp port-priority** value be 12345 on the 1/3 interface vs. the default 32768 on the 0/7 interface.

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. See the **lacp system-priority** command.

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group.

Examples

The following example sets a lower port priority for GigabitEthernet 0/2 so it will be used as part of the EtherChannel ahead of GigabitEthernet 0/0 and 0/1:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

lacp system-priority

For EtherChannels, to set the LACP system priority globally for the ASA, use the **lacp system-priority** command in global configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp system-priority *number*
no lacp system-priority

Syntax Description

number	Sets the LACP system priority, from 1 to 65535. The default is 32768. The higher the number, the lower the priority. This command is global for the ASA.

Command Default

The default is 32768.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. For interface priorities within an EtherChannel, see the **lacp port-priority** command.

Examples

The following example sets the system priority to be higher than the default (a lower number):

```
ciscoasa(config)# lacp system-priority 12345
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.

Command	Description
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

ldap-attribute-map

To bind an existing mapping configuration to an LDAP host, use the **ldap-attribute-map** command in aaa-server host configuration mode. To remove the binding, use the **no** form of this command.

ldap-attribute-map *map-name*
no ldap-attribute-map *map-name*

Syntax Description

map-name	Specifies an LDAP attribute mapping configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

If the Cisco-defined LDAP attribute names do not meet your ease-of-use or other requirements, you can create your own attribute names, map them to Cisco attributes, and then bind the resulting attribute configuration to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This command enters ldap-attribute-map configuration mode. Note that there is no hyphen after "ldap" in this command.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map configuration mode to populate the attribute mapping configuration.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map configuration to an LDAP server.

Examples

The following example commands, entered in aaa-server host configuration mode, bind an existing attribute map named myldapmap to an LDAP server named ldapsvr1:

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running ldap attribute mapping configuration or all running attribute mapping configurations.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

ldap-base-dn

To specify the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request, use the **ldap-base-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this specification, thus resetting the search to start at the top of the list, use the **no** form of this command.

ldap-base-dn*string*
no ldap-base-dn

Syntax Description

string A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request; for example, OU=Cisco.

Command Default

Start the search at the top of the list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP base DN as starthere.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-base-dn starthere
ciscoasa
(config-aaa-server-host)#
exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN.

ldap-defaults

To define LDAP default values, use the **ldap-defaults** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These default values are used only when the LDAP server requires them. To specify no LDAP defaults, use the **no** form of this command.

ldap-defaults *server* [*port*]
no ldap-defaults

Syntax Description

port	(Optional) Specifies the LDAP server port. If this parameter is not specified, the ASA uses the standard LDAP port (389).
server	Specifies the IP address or domain name of the LDAP server. If one exists within the CRL distribution point, it overrides this value.

Command Default

The default setting is not set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configure configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example defines LDAP default values on the default port (389):

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

ldap-dn

To pass a X.500 distinguished name and password to an LDAP server that requires authentication for CRL retrieval, use the **ldap-dn** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them. To specify no LDAP DN, use the **no** form of this command.

ldap-dn *x.500-name password*
no ldap-dn

Syntax Description

password	Defines a password for this distinguished name. The maximum field length is 128 characters.
x.500-name	Defines the directory path to access this CRL database, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum field length is 128 characters.

Command Default

The default setting is not on.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configure configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example specifies an X.500 name CN=admin,OU=devtest,O=engineering and a password xxzzyy for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

Related Commands

Command	Description
crl configure	Enters crl configure configuration mode.
crypto ca trustpoint	Enters ca trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

ldap-group-base-dn

To specify the base group in the Active Directory hierarchy used by dynamic access policies for group searches, use the **ldap-group-base-dn** command in aaa-server host configuration mode. To remove the command from the running configuration, use the no form of the command:

ldap-group-base-dn [*string*]
no ldap-group-base-dn [*string*]

Syntax Description

string A case-sensitive string of up to 128 characters that specifies the location in the Active Directory hierarchy where the server should begin searching. For example, ou=Employees. Spaces are not permitted in the string, but other special characters are allowed.

Command Default

No default behavior or values. If you do not specify a group search DN, the search begins at the base DN.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server host configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

The **ldap-group-base-dn** command applies only to Active Directory servers using LDAP, and specifies an Active Directory hierarchy level that the **show ad-groups** command uses to begin its group search. The groups retrieved from the search are used by dynamic group policies as selection criteria for a specific policy.

Examples

The following example sets the group base DN to begin the search at the organization unit (ou) level Employees:

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

Related Commands

Command	Description
group-search-timeout	Adjusts the time the ASA waits for a response from an Active Directory server for a list of groups.
show ad-groups	Displays groups that are listed on an Active Directory server.

ldap-login-dn

To specify the name of the directory object that the system should bind this as, use the **ldap-login-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-login-dn*string*
no ldap-login-dn

Syntax Description

string A case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Some LDAP servers, including the Microsoft Active Directory server, require that the ASAestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The ASA identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the ASA. These characteristics should correspond to those of a user with administrator privileges.

For the *string* variable, enter the name of the directory object for VPN Concentrator authenticated binding, for example: cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com. For anonymous access, leave this field blank.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login DN as myobjectname.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host)
# ldap-login-dn myobjectname
ciscoasa(config-aaa-server
-host)
#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-login-password

To specify the login password for the LDAP server, use the **ldap-login-password** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this password specification, use the **no** form of this command:

ldap-login-password*string*
no ldap-login-password

Syntax Description

string A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for LDAP servers. The maximum password string length is 64 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login password as obscurepassword.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server)# timeout 9
ciscoasa
(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa
(config-aaa-server)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-naming-attribute

To specify the Relative Distinguished Name attribute, use the **ldap-naming-attribute** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-naming-attribute*string*
no ldap-naming-attribute

Syntax Description

string The case-sensitive, alphanumeric Relative Distinguished Name attribute, consisting of up to 128 characters, that uniquely identifies an entry on the LDAP server. Spaces are not permitted in the string, but other special characters are allowed.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP naming attribute as cn.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
```

```
)# ldap-naming-attribute cn
ciscoasa
(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-over-ssl

To establish a secure SSL connection between the ASA and the LDAP server, use the **ldap-over-ssl** command in aaa-server host configuration mode. To disable SSL for the connection, use the **no** form of this command.

ldap-over-ssl [**enable** | **reference-identity** *ref_id_name*]

no ldap-over-ssl [**enable** | **reference-identity** *ref_id_name*]

Syntax Description

enable	Specifies that SSL secures a connection to an LDAP server.
reference-identity *ref_id_name*	Specifies reference-identity name to validate LDAP server identity.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
9.18(1)	This command was enhanced to validate the LDAP server identity.

Usage Guidelines

Use this command to specify that SSL secures a connection between the ASA and an LDAP server.

Note We recommend enabling this feature if you are using plain text authentication. See the **sasl-mechanism command.**

Examples

The following commands, entered in aaa-server host configuration mode, enable SSL for a connection between the ASA and the LDAP server named ldapsvr1 at IP address 10.10.0.1. They also configure the plain SASL authentication mechanism.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)#
```

To validate the LDAP server identity by specifying the reference identity name, use **reference-identity** *ref_id_name*. A reference-identity object is created using **crypto ca reference-identity refidname** with a matching criteria. When you configure reference-identity under ldap aaa-server configuration, ASA tries to find a hostname match with ldap server certificate. Failure to resolve the host or when no match is found, the connection is terminated with an error message.

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
  enable              Require an SSL connection to the LDAP server
  reference-identity  Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
  WORD < 65 char  Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
  <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

The show running-config aaa server displays the configured reference-identity name as one of the options:

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

Related Commands

Command	Description
sasl-mechanism	Specifies SASL authentication between the LDAP client and server.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ssl-client-certificate	Specifies the certificate that the ASA should present to the LDAP server as the client certificate when using LDAPS.
crypto ca reference-identity refidname	To configure a reference-identity object.

ldap-scope

To specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request, use the **ldap-scope** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-scope*scope*
no ldap-scope

Syntax Description

scope The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values are:

- **onelevel**—Search only one level beneath the Base DN
- **subtree**—Search all levels beneath the Base DN

Command Default

The default value is **onelevel**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Specifying the scope as **onelevel** results in a faster search, because only one level beneath the Base DN is searched. Specifying **subtree** is slower, because all levels beneath the Base DN are searched.

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP scope to include the subtree levels.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
```

```
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa
(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.

leap-bypass

To enable LEAP Bypass, use the **leap-bypass enable** command in group-policy configuration mode. To disable LEAP Bypass, use the **leap-bypass disable** command. To remove the LEAP Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for LEAP Bypass from another group policy.

leap-bypass { **enable** | **disable** }
no leap-bypass

Syntax Description

disable	Disables LEAP Bypass.
enable	Enables LEAP Bypass.

Command Default

LEAP Bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When enabled, LEAP Bypass allows LEAP packets from wireless devices behind a VPN hardware client to travel across a VPN tunnel prior to user authentication. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Devices are then able to authenticate again, per user authentication.

This feature does not work as intended if you enable interactive hardware client authentication.

For further information, see the CLI configuration guide.

Note There may be security risks in allowing any unauthenticated traffic to traverse the tunnel.

Examples

The following example shows how to set LEAP Bypass for the group policy named “FirstGroup”:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# leap-bypass enable
```

Related Commands

Command	Description
secure-unit-authentication	Requires VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel.
user-authentication	Requires users behind VPN hardware clients to identify themselves to the ASA before connecting.

license

To configure the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes, use the **license** command in scansafe general-options configuration mode. To remove the license, use the **no** form of this command.

license*hex_key*
no license [*hex_key*]

Syntax Description

hex_key	Specifies the authentication key as a 16-byte hexadecimal number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Each ASA must use an authentication key that you obtain from Cloud Web Security. The authentication key lets Cloud Web Security identify the company associated with web requests and ensures that the ASA is associated with valid customer.

You can use one of two types of authentication keys for your ASA: the company key or the group key.

Company Authentication Key

A Company authentication key can be used on multiple ASAs within the same company. This key simply enables the Cloud Web Security service for your ASAs. The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter. For more information, see the Cloud Web Security documentation: http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html .

Group Authentication Key

A Group authentication key is a special key unique to each ASA that performs two functions:

- Enables the Cloud Web Security service for one ASA.
- Identifies all traffic from the ASA so you can create ScanCenter policy per ASA.

The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter. For more information, see the Cloud Web Security documentation: http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html .

Examples

The following example configures a primary server only:

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.

Command	Description
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

license-server address

To identify the shared licensing server IP address and shared secret for use by a participant, use the **license-server address** command in global configuration mode. To disable participation in shared licensing, use the **no** form of this command. A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed amongst a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

license-server address *address* **secret** *secret* [**port port**]
no license-server address [*address* **secret** *secret* [**port port**]]

Syntax Description

address	Identifies the shared licensing server IP address.
port *port*	(Optional) If you changed the default port in the server configuration using the **license-server port** command, set the port for the backup server to match, between 1 and 65535. The default port is 50554.
secret *secret*	Identifies the shared secret. The secret must match the secret set on the server using the **license-server secret** command.

Command Default

The default port is 50554.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The shared licensing participant must have a shared licensing participant key. Use the **show activation-key** command to check your installed licenses.

You can only specify one shared license server for each participant.

The following steps describe how shared licenses operate:

1. Decide which ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.

2. Decide which ASAs should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.
3. (Optional) Designate a second ASA as a shared licensing backup server. You can only specify one backup server.

Note The shared licensing backup server only needs a participant license.

1. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
2. When you configure the ASA as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

Note The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

1. The shared licensing server responds with information about how often the participant should poll the server.
2. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
3. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

Note The shared licensing server can also participate in the shared license pool if it runs out of local sessions. It does not need a participant license as well as the server license to participate.

1. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
2. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
3. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The ASA uses SSL between the server and participant to encrypt all communications.

Communication Issues Between Participant and Server

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.

- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.
- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

Examples

The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup address

To identify the shared licensing backup server IP address for use by a participant, use the **license-server backup address** command in global configuration mode. To disable use of the backup server, use the **no** form of this command.

license-server backup address *address*
no license-server address [**address**]

Syntax Description

address	Identifies the shared licensing backup server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The shared licensing backup server must have the **license-server backup enable** command configured.

Examples

The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.

Command	Description
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup backup-id

To identify the shared licensing backup server in the main shared licensing server configuration, use the **license-server backup backup-id** command in global configuration mode. To remove the backup server configuration, use the **no** form of this command.

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]
no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

Syntax Description

address	Identifies the shared licensing backup server IP address.
backup-id *serial_number*	Identifies the shared licensing backup server serial number.
ha-backup-id *ha_serial_number*	If you use failover for the backup server, identifies the secondary shared licensing backup server serial number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can only identify 1 backup server and its optional standby unit.

To view the backup server serial number, enter the **show activation-key** command.

To enable a participant to be the backup server, use the **license-server backup enable** command.

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing

sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

Note When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server "recharges" up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.

Command	Description
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup enable

To enable this unit to be the shared licensing backup server, use the **license-server backup enable** command in global configuration mode. To disable the backup server, use the **no** form of this command.

license-server backup enable *interface_name*
no license-server enable *interface_name*

Syntax Description

interface_name	Specifies the interface on which participants contact the backup server. You can repeat this command for as many interfaces as desired.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The backup server must have a shared licensing participant key.

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

Note When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server "recharges" up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.

Examples

The following example identifies the license server and shared secret, and enables this unit as the backup shared license server on the inside interface and dmz interface.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server enable

To identify this unit as a shared licensing server, use the **license-server enable** command in global configuration mode. To disable the shared licensing server, use the **no** form of this command. A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed amongst a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

license-server enable *interface_name*
no license-server enable *interface_name*

Syntax Description

interface_name	Specifies the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The shared licensing server must have a shared licensing server key. Use the **show activation-key** command to check your installed licenses.

The following steps describe how shared licenses operate:

1. Decide which ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which ASAs should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.
3. (Optional) Designate a second ASA as a shared licensing backup server. You can only specify one backup server.

Note The shared licensing backup server only needs a participant license.

1. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
2. When you configure the ASA as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

Note The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

1. The shared licensing server responds with information about how often the participant should poll the server.
2. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
3. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

Note The shared licensing server can also participate in the shared license pool if it runs out of local sessions. It does not need a participant license as well as the server license to participate.

1. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
2. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
3. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The ASA uses SSL between the server and participant to encrypt all communications.

Communication Issues Between Participant and Server

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.
- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.
- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and DMZ interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server port

To set the port on which the shared licensing server listens for SSL connections from participants, use the **license-server port** command in global configuration mode. To restore the default port, use the **no** form of this command.

license-server port *port*
no license-server port [*port*]

Syntax Description

seconds	Sets the port on which the server listens for SSL connections from participants, between 1 and 65535. The default is TCP port 50554.

Command Default

The default port is 50554.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If you change the port from the default, be sure to set the same port for each participant using the **license-server address** command.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and DMZ interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server refresh-interval

To set the refresh interval provided to participants to set how often they should communicate with the shared licensing server, use the **license-server refresh-interval** command in global configuration mode. To restore the default refresh interval, use the **no** form of this command.

license-server refresh-interval *seconds*
no license-server refresh-interval [*seconds*]

Syntax Description

seconds	Sets the refresh interval between 10 and 300 seconds. The default is 30 seconds.

Command Default

The default is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Each participant regularly communicates with the shared licensing server using SSL so the shared licensing server can keep track of current license usage and receive and respond to license requests.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server secret

To set the shared secret on the shared licensing server, use the **license-server secret** command in global configuration mode. To remove the secret, use the **no** form of this command.

license-server secret *secret*
no license-server secret *secret*

Syntax Description

secret	Sets the shared secret, a string between 4 and 128 ASCII characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Any participant with this secret identified in the **license-server address** command can use the licensing server.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.

Command	Description
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license smart

To set the smart licensing entitlement request, use the **license smart** command in global configuration mode. To remove the entitlement and unlicense your device, use the **no** form of this command.

Note This feature is supported on the ASA virtual and Chassis only.

license smart
no license smart

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.4(1.152)	Support for the Firepower 9300 was added.
9.6(1)	Support for the Firepower 4100 series was added.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

This command enters license smart configuration mode, where you can set the feature tier and other license entitlements. For the ASA virtual, when you request the entitlements for the first time, you must exit license smart configuration mode for your changes to take effect.

Examples

The following example sets the feature tier to standard, and the throughput level to 2G:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart deregister

To deregister the device from the Cisco License Authority for smart licensing, use the **license smart deregister** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart deregister

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

Deregistering the ASA removes the ASA from your account. All license entitlements and certificates on the ASA are removed. You might want to deregister to free up a license for a new ASA. This command causes the ASA to reload.

Examples

The following example deregisters the device:

```
ciscoasa# license smart deregister
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.

Command	Description
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart register

To register the device with the Cisco License Authority for smart licensing, use the **license smart register** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart register idtoken *id_token* [**force**]

Syntax Description

idtoken *id_token*	In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this ASA.
force	Registers an ASA that is already registered, but that might be out of sync with the License Authority.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

When you register the ASA, the License Authority issues an ID certificate for communication between the ASA and the License Authority. It also assigns the ASA to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the ASA if the ID certificate expires because of a communication problem, for example.

Examples

The following example registers with an registration token:

```
ciscoasa# license smart register idtoken
YjE3NjctMzYtMGQzMi00OTA4LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NWk2bzV3SDE0ZkgwQkdMRmZlNlNCNGlvRnBHUFpjcm02WlB4TU4w%0Ac2NrMD0%3D%0A
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart renew

To renew the registration or license entitlement authorization for smart licensing, use the **license smart renew** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart renew { **id** | **auth** }

Syntax Description

id	Renews the device registration.
auth	Renews the license entitlement.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for internet access, or if you make any licensing changes in the Smart Software Manager, for example.

Examples

The following example renews both the registration and license authorization:

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart reservation

To enable permanent license reservation, use the **license smart reservation** command in global configuration mode. To disable permanent license reservation, use the **no** form of this command.

license smart reservation
no license smart reservation

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory). The permanent license enables all features to their maximum levels.

For the ASA virtual, when you enter the **license smart reservation** command, the following commands are removed:

```
license smart
feature tier standard
throughput level {100M | 1G | 2G}
```

To use regular smart licensing, use the **no** form of this command, and re-enter the above commands. Other Smart Call Home configuration remains intact but unused, so you do not need to re-enter those commands.

For Chassis, you must enter the **license smart**/**feature** commands for any non-default licenses; for example, for the context license. These commands are required so the ASA knows to allow configuration of the feature.

Note For permanent license reservation, you must return the license before you decommission the ASA. If you do not officially return the license, the license remains in a used state and cannot be reused for a new ASA. See the **license smart reservation return** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation cancel

To cancel a permanent license reservation request if you have not yet entered the code in the Smart Software Manager, use the **license smart reservation cancel** command in privileged EXEC mode.

license smart reservation cancel

Note This feature applies only to the ASA virtual and the Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

If you requested a license code to enter in the Smart Software Manager using the **license smart reservation request universal** command, and have not yet entered this code into the Smart Software Manager, you can cancel the request using the **license smart reservation cancel** command.

If you disable permanent license reservation (**no license smart reservation**), then any pending requests are canceled.

If you already entered the code into the Smart Software Manager, then you must finish applying the license to the ASA, after which point you can return the license using the **license smart reservation return** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then cancels the request:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation install

To enter a permanent license reservation authorization code received from the Smart Software Manager, use the **license smart reservation install** command in privileged EXEC mode.

license smart reservation install *code*

Note This feature applies only to the ASA virtual and the Firepower 2100.

Syntax Description

code The permanent license reservation authorization code received from the Smart Software Manager.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory). Request a code to enter into the Smart Software Manager using the **license smart reservation request universal** command. When you enter the code into the Smart Software Manager, copy the resulting authorization code and enter it on the ASA using the **license smart reservation install** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation universal

To request the license code to enter in the Smart Software Manager, use the **license smart reservation universal** command in privileged EXEC mode.

license smart reservation universal

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager. Request a code to enter into the Smart Software Manager using the **license smart reservation request universal** command.

The ASA virtual deployment determines which license (ASAv5/ASAv10/ASAv30) is requested.

If you re-enter this command, then the same code is displayed, even after a reload. If you have not yet entered this code into the Smart Software Manager and want to cancel the request, enter the **license smart reservation cancel** command.

If you disable permanent license reservation, then any pending requests are canceled. If you already entered the code into the Smart Software Manager, then you must complete this procedure to apply the license to the ASA, after which point you can return the license if desired. See the **license smart reservation return** command.

To request the authorization code, go to the Smart Software Manager Inventory screen (https://software.cisco.com/#SmartLicensing-Inventory), and click the **Licenses** tab. The **Licenses** tab displays all existing licenses related to your account, both regular and permanent. Click **License Reservation**, and

type the ASA code into the box. Click **Reserve License**. The Smart Software Manager generates an authorization code. You can download the code or copy it to the clipboard. At this point, the license is now in use according to the Smart Software Manager.

If you do not see the **License Reservation** button, then your account is not authorized for permanent license reservation. In this case, you should disable permanent license reservation and re-enter the regular smart license commands.

Enter the authorization code on the ASA using the **license smart reservation install** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation return

To generate a return code to return the license to the Smart Software Manager, use the **license smart reservation return** command in privileged EXEC mode.

license smart reservation return

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager. If you no longer need a permanent license (for example, you are retiring an ASA or changing the ASA virtual model level so it needs a new license), you must officially return the license to the Smart Software Manager. If you do not return the license, then the license stays in a used state and cannot easily be freed up for use elsewhere.

When you enter the **license smart reservation return** command, the ASA immediately becomes unlicensed and moves to the Evaluation state. If you need to view this code again, re-enter this command. Note that if you request a new permanent license (**license smart reservation request universal**) or change the ASA virtual model level (by powering down and changing the vCPUs/RAM), then you cannot re-display this code. Be sure to capture the code to complete the return.

Before you enter the code in the Smart Software Manager, view the ASA universal device identifier (UDI) using the **show license udi** command so you can find this ASA instance in the Smart Software Manager. Go to the Smart Software Manager Inventory screen (https://software.cisco.com/#SmartLicensing-Inventory), and click the **Product Instances** tab. The **Product Instances** tab displays all licensed products by the UDI.

Find the ASA virtual you want to unlicense, choose **Actions > Remove**, and type the ASA return code into the box. Click **Remove Product Instance**. The permanent license is returned to the available pool.

Examples

The following example generates the return code on the ASA virtual, and views the ASA virtual UDI:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

lifetime (ca server mode)

To specify the length of time that the Local Certificate Authority (CA) certificate, each issued user certificates, or the Certificate Revocation List (CRL) is valid, use the **lifetime** command in ca server configuration mode. To reset the lifetime to the default setting, use the **no** form of this command.

lifetime { **ca-certificate** | **certificate** | **crl** } *time*
lifetime { **ca-certificate** | **certificate** | **crl** }

Syntax Description

ca-certificate	Specifies the lifetime of the local CA server certificate.
certificate	Specifies the lifetime of all user certificates issued by the CA server.
crl	Specifies the lifetime of the CRL.
time	For the CA certificate and all issued certificates, *time* specifies the number of days the certificate is valid. The valid range is from 5 to 30 years. The default lifetime value is 15 years. For all the issued user certificates, the valid range is from one day to four years. The default lifetime value is 2 years. For the CRL, *time* specifies the number of hours the CRL is valid. The valid range for the CRL is from 1 to 720 hours.

Command Default

The default lifetimes are:

- CA certificate—15 years
- Issued certificates— Two years
- CRL—Six hours

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.12(1)	The allowed values for lifetime ca-certificate is changed to 5 to 30 years with a default of 15 years. The allowed values for lifetime certificate is changed to 1 day to 4 years with a default of 2 years.

Usage Guidelines

By specifying the number of days or hours that a certificate or CRL is valid, this command determines the expiration date included in the certificate or the CRL.

The **lifetime ca-certificate** command takes effect when the local CA server certificate is first generated (that is, when you initially configure the local CA server and issue the **no shutdown** command). When the CA certificate expires, the configured lifetime value is used to generate the new CA certificate. You cannot change the lifetime value for existing CA certificates.

Examples

The following example configures the CA to issue certificates that are valid for three months:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime certificate 90
ciscoasa
(config-ca-server)
)#
```

The following example configures the CA to issue a CRL that is valid for two days:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime crl 48
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point (CDP) to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
show crypto ca server	Displays the local CA configuration details in ASCII text.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server crl	Displays the current CRL of the local CA.

lifetime (ikev2 policy mode)

To specify the encryption algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the encryption command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

lifetime { { **seconds** *seconds* } | **none** }

Syntax Description

seconds	The lifetime in seconds, from 120 to 2,147,483,647 seconds. The default is 86,400 seconds (24 hours).

Command Default

The default is 86,400 seconds (24 hours).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **lifetime** command to set the SA lifetime.

The lifetime sets the interval for IKEv2 SA rekeys. Using the none keyword disables rekeying the SA. However, the Secure Client can still rekey the SA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.

Examples

The following example enters IKEv2 policy configuration mode and sets the lifetime to 43,200 seconds (12 hours):

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.

Command	Description
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.

limit-resource

To specify a resource limit for a class in multiple context mode, use the **limit-resource** command in class configuration mode. To restore the limit to the default, use the **no** form of this command. The ASA manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

limit-resource [**rate**] { **all** | *resource_name* } *number* [**%**] }
no limit-resource [**rate**] { **all** | *resource_name* }

Syntax Description

all	Sets the limit for all resources.
number [**%**]	Specifies the resource limit as a fixed number greater than or equal to 1, or as a percentage of the system limit between 1 and 100 (when used with the percent sign (%)). Set the limit to **0** to indicate an unlimited resource, or for VPN resource types, to set the limit to none. For resources that do not have a system limit, you cannot set the percentage (%); you can only set an absolute value.
rate	Specifies that you want to set the rate per second for a resource. See Table 3: Resource Names and Limits for resources for which you can set the rate per second.
resource_name	Specifies the resource name for which you want to set a limit. This limit overrides the limit set for **all**.

Command Default

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

For most resources, the default class provides unlimited access to resources for all contexts, except for the following limits:

- Telnet sessions—5 sessions. (The maximum per context.)
- SSH sessions—5 sessions. (The maximum per context.)
- ASDM sessions—5 sessions. (The maximum per context.)
- IPsec sessions—5 sessions. (The maximum per context.)
- MAC addresses—(varies per model). (The maximum per context.)
- AnyConnect peers—0 sessions. (You must manually configure the class to allow any AnyConnect peers.)
- VPN site-to-site tunnels—0 sessions. (You must manually configure the class to allow any VPN sessions.)
- HTTPS sessions—6 sessions. (The maximum per context.)

Note If you also set the **quota management-session** command within a context to set the maximum administrative sessions (SSH, etc.), then the lower value will be used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	A new resource type, **routes**, was created to set the maximum number of routing table entries in each context. New resource types, **vpn other** and **vpn burst other**, were created to set the maximum number of site-to-site VPN tunnels in each context.
9.5(2)	New resource types, **vpn anyconnect** and **vpn burst anyconnect**, were created to set the maximum number of AnyConnect VPN peers in each context.
9.6(2)	New resource type, **storage**, was created to set the maximum storage.
9.12(1)	New resource type, **http**, was added to control HTTPS connections.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced; the only exception is VPN resources, which are disabled by default. If you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context. For VPN resources, you must configure resource management to allow any VPN tunnels.

Table 3: Resource Names and Limits lists the resource types and the limits. See also the **show resource types** command.

Table 3: Resource Names and Limits

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
asdm	Concurrent	1 minimum 5 maximum	200	ASDM management sessions. **Note** ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 200 ASDM sessions represents a limit of 400 HTTPS sessions.

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
conns	Concurrent or Rate	N/A	Concurrent connections: See the CLI configuration guide for the connection limit for your platform. Rate: N/A	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
hosts	Concurrent	N/A	N/A	Hosts that can connect through the ASA.
http	Concurrent	1 minimum 6 maximum	100	Non-ASDM HTTPS sessions
inspects	Rate	N/A	N/A	Application inspections.
mac-addresses	Concurrent	N/A	(varies per model)	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
routes	Concurrent	N/A	N/A	Dynamic routes.
ssh	Concurrent	1 minimum 5 maximum	100	SSH sessions.
storage	MB	The maximum depends on your specified flash memory drive	The maximum depends on your specified flash memory drive	Storage limit of context directory in MB. Specify the drive using the **storage-url** command.
syslogs	Rate	N/A	N/A	System log messages.
telnet	Concurrent	1 minimum 5 maximum	100	Telnet sessions.
vpn burst anyconnect	Concurrent	N/A	The AnyConnect Premium Peers for your model minus the sum of the sessions assigned to all contexts for vpn anyconnect.	The number of AnyConnect sessions allowed beyond the amount assigned to a context with **vpn anyconnect**. For example, if your model supports 5000 peers, and you assign 4000 peers across all contexts with **vpn anyconnect**, then the remaining 1000 sessions are available for **vpn burst anyconnect**. Unlike **vpn anyconnect**, which guarantees the sessions to the context, **vpn burst anyconnect** can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
vpn anyconnect	Concurrent	N/A	See the "Supported Feature Licenses Per Model" section in the CLI configuration guide for the AnyConnect VPN peers available for your model.	AnyConnect peers. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The peers you assign for this resource are guaranteed to the context.
vpn burst other	Concurrent	N/A	The Other VPN session amount for your model minus the sum of the sessions assigned to all contexts for **vpn other**.	The number of site-to-site VPN sessions allowed beyond the amount assigned to a context with **vpn other**. For example, if your model supports 5000 sessions, and you assign 4000 sessions across all contexts with **vpn other**, then the remaining 1000 sessions are available for **vpn burst other**. Unlike **vpn other**, which guarantees the sessions to the context, **vpn burst other** can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.
vpn other	Concurrent	N/A	See the "Supported Feature Licenses Per Model" section in the CLI configuration guide for the Other VPN sessions available for your model.	Site-to-site VPN sessions. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The sessions you assign for this resource are guaranteed to the context.
xlates	Concurrent	N/A	N/A	Address translations.

[1] If this column value is N/A, then you cannot set a percentage of the resource because there is no hard system limit for the resource.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold, enter the following commands:

```
ciscoasa(config)# class gold
ciscoasa(config-class)#
limit-resource mac-addresses 10000
ciscoasa(config-class)#
limit-resource conns 15%
ciscoasa(config-class)#
limit-resource rate conns 1000
ciscoasa(config-class)#
limit-resource rate inspects 500
```

```
ciscoasa(config-class)#
limit-resource hosts 9000
ciscoasa(config-class)#
limit-resource asdm 5
ciscoasa(config-class)#
limit-resource ssh 5
ciscoasa(config-class)#
limit-resource rate syslogs 5000
ciscoasa(config-class)#
limit-resource telnet 5
ciscoasa(config-class)#
limit-resource xlates 36000
ciscoasa(config-class)#
limit-resource routes 700
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
member	Assigns a context to a resource class.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

lmfactor

To set a revalidation policy for caching objects that have only the last-modified timestamp, and no other server-set expiration values, use the **lmfactor** command in cache configuration mode. To set a new policy for revalidating such objects, use the command again. To reset the attribute to the default value of 20, enter the **no** version of the command.

lmfactor*value*
nolmfactor

Syntax Description

value	An integer in the range of 0 to 100.

Command Default

The default value is 20.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The ASA uses the value of the lmfactor to estimate the length of time for which it considers a cached object to be unchanged. This is known as the expiration time. The ASA estimates th expiration time by the time elapsed since the last modification multiplied by the lmfactor.

Setting the lmfactor to zero is equivalent to forcing an immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

Examples

The following example shows how to set an lmfactor of 30:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

load-monitor

To configure cluster traffic load monitoring, use the **load-monitor** command in cluster configuration mode. To disable this feature, use the **no** form of this command.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]
no load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

Syntax Description

frequency *seconds*	(Optional) Sets the time in seconds between monitoring messages, between 10 and 360 seconds. The default is 20 seconds.
intervals *intervals*	(Optional) Sets the number of intervals for which the ASA maintains data, between 1 and 60. The default is 30.

Command Default

This command is enabled by default. The default frequency is 20 seconds. The default interval is 30.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

You can monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default. For example, for inter-chassis clustering on the Firepower 9300 with 3 security modules in each chassis, if 2 security modules in a chassis leave the cluster, then the same amount of traffic to the chassis will be sent to the remaining module and potentially overwhelm it. You can periodically monitor the traffic load. If the load is too high, you can choose to manually disable clustering on the unit.

Use the **show cluster info load-monitor** command to view the traffic load.

Examples

The following example sets the frequency to 50 seconds, and the interval to 25:

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

Related Commands

Command	Description
cluster	Enters cluster configuration mode

local-base-url

(Optional) Configures the local base URL of the SAML service provider for VPN authentication. In a DNS load balancing cluster, when you configure SAML authentication on ASAs, you can specify this URL to uniquely resolve to the device on which the configuration is applied.

To disable this feature, use the **no** form of this command

local base-url { **url** }
no local base-url

Syntax Description

url	Local base URL of the SAML service provider for VPN authentication.

Command Default

None.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(3)	This command was added.
9.19(1)5	This command was added.

Usage Guidelines

You must use this command in conjunction with the **base-url** command.

Examples

The following example sets up a local base-url:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp https://idp.com/<app-specific>
ciscoasa(config-webvpn-saml-idp)# base url https://asa-dns-group.vpn.customer.com
ciscoasa(config-webvpn-saml-idp)# local-base-url https://this-asa.vpn.customer.com
```

Related Commands

Command	Description
signature	Enable or disable signature in SAML request. By default, the signature is disabled.
timeout	Configures the SAML IdP timeout.
trustpoint	Configures the trustpoint in saml-idp sub-mode.

Command	Description
url	Configures the SAML IdP URL.
base-url	Configures the base URL of the SAML service provider for VPN authentication.

local-domain-bypass

To configure local domains for which DNS requests should bypass Cisco Umbrella, use the **local-domain-bypass** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }
no local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }

Syntax Description

regular_expression	A regular expression that identifies the local domain to bypass. This can be as simple as the local domain, for example, example.com. The expression can be up to 100 characters. If you use this option, you can enter the **local-domain-bypass** command multiple times to define more than one local domain.
regex class *regex_classmap*	The name of the regular expression class that defines the local domain names to bypass. Any DNS requests for fully-qualified domain names that match the regular expressions in the class are sent directly to the configured DNS servers, not to the Umbrella servers.

Command Default

The default is that DNS requests for all domains are sent to Cisco Umbrella.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Umbrella configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

Following are the guidelines for using this command:

- You can enter this command multiple times to define regular expressions for domain names directly.
- You can enter this command only once when using a regular expression class. However, you can combine both a single regular expression class version of the command with multiple instances where you use a regular expression directly.

Examples

The following example defines example.com as the local domain to bypass.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass example.com
```

The following example creates a regular expression to match example.com, which would match any fully-qualified domain name on *example.com. Then, the example creates the required regular expression class map and uses it as the local domain bypass for Umbrella.

```
ciscoasa(config)# regex example-com example.com

ciscoasa(config)# class-map type regex match-any umbrella-bypass

ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

Related Commands

Commands	Description
umbrella-global	Configures the Cisco Umbrella global parameters.

local-unit

To provide a name for this cluster member, use the **local-unit** command in cluster group configuration mode. To remove the name, use the **no** form of this command.

local-unit *unit_name*
no local-unit [*unit_name*]

Syntax Description

unit_name	Names this member of the cluster with a unique ASCII string from 1 to 38 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Each unit must have a unique name. A unit with a duplicated name will be not be allowed in the cluster.

Examples

The following example names this unit as unit1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.

Command	Description
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

location-logging

To have GTP inspection log the location and change of location for mobile stations, use the **location-logging** command in GTP inspection policy map parameters configuration mode. Use the **no** form of this command to disable location logging.

location-logging [**cell-id**]
no location-logging [**cell-id**]

Syntax Description

cell-id	Whether to include the cell ID where the user currently is registered. The cell ID is extracted from the Cell Global Identification (CGI) or E-UTRAN Cell Global Identifier (ECGI).

Command Default

By default, location logging is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

You can use GTP inspection to track location changes for mobile stations. Tracking location changes might help you identify fraudulent roaming charges, for example, if you see a mobile station move from one location to another within an unlikely time window, such as moving from a cell in the United States to one in Europe within 30 minutes.

When you enable location logging, the system generates syslog messages for new or changed locations for each International Mobile Subscriber Identity (IMSI):

- 324010 indicates the creation of a new PDP context, and includes the Mobile Country Code (MCC), Mobile Network Code (MNC), the information elements, and optionally the cell ID where the user currently is registered. The cell ID is extracted from the Cell Global Identification (CGI) or E-UTRAN Cell Global Identifier (ECGI).
- 324011 indicates that the IMSI has moved from the one stored during the PDP context creation. The message shows the previous and current MCC/MNC and optionally, cell ID.

By default, syslog messages do not include timestamp information. If you plan to analyze these messages to identify improbable roaming, you must also enable timestamps. Timestamp logging is not part of the GTP inspection map. Use the **logging timestamp** command.

Examples

The following example adds the timestamp to syslog messages and then enables location logging with the cell ID.

```
ciscoasa(config)# logging timestamp

ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# location-logging cell-id
```

Related Commands

Commands	Description
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.
show service-policy inspect gtp	Displays the GTP configuration and statistics.

log – lz

log

When using the Modular Policy Framework, log packets that match a **match** command or class map by using the **log** command in match or class configuration mode. This log action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic. To disable this action, use the no form of this command.

log
nolog

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **log** command to log all packets that match the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example sends a log when packets match the http-traffic class map.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.

Commands	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

log-adjacency-changes

To enable the IS-IS to send a syslog message when an NLSP IS-IS adjacency changes states (up or down), use the **log-adjacency-changes** command in router isis configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**all**]
no log-adjacency-changes [**all**]

Syntax Description

all	(Optional) Includes changes generated by non_IIH events.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command allows the monitoring of IS-IS adjacency state changes. This may be very useful when monitoring large networks. Messages are logged using the system error message facility. Messages are of the form:

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

Examples

The following example instructs the router to log adjacency changes:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

log-adj-changes

To configure the router to send a syslog message when an OSPF neighbor goes up or down, use the **log-adj-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]
no log-adj-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **log-adj-changes** command is enabled by default; it appears in the running configuration unless removed with the **no** form of the command.

Examples

The following example disables the sending of a syslog message when an OSPF neighbor goes up or down:

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.

log-adjacency-changes

To configure the router to send a syslog message when an OSPFv3 neighbor goes up or down, use the **log-adjacency-changes** command in IPv6 router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**detail**]
no log-adjacency-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **log-adjacency-changes** command is enabled by default; it appears in the running configuration unless removed with the **no** form of the command.

Examples

The following example disables the sending of a syslog message when an OSPFv3 neighbor goes up or down:

```
ciscoasa(config)# ipv6
 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.

logging asdm

To send syslog messages to the ASDM log buffer, use the **logging asdm** command in global configuration mode. To disable logging to the ASDM log buffer, use the **no** form of this command.

logging asdm [*logging_list* | *level*]
no logging asdm [*logging_list* | *level*]

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the ASDM log buffer. For information about creating lists, see the **logging list** command.

Command Default

ASDM logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Before any messages are sent to the ASDM log buffer, you must enable logging using the **logging enable** command.

When the ASDM log buffer is full, the ASA deletes the oldest message to make room in the buffer for new messages. To control the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

The following example shows how to enable logging, send log buffer messages of severity levels 0, 1, and 2 to the ASDM, and how to set the ASDM log buffer size to 200 messages:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages that it contains.
logging asdm-buffer-size	Specifies the number of ASDM messages retained in the ASDM log buffer
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging configuration.

logging asdm-buffer-size

To specify the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command in global configuration mode. To reset the ASDM log buffer to its default size of 100 messages, use the **no** form of this command.

loggingasdm-buffer-size*num_of_msgs*
no logging asdm-buffer-size *num_of_msgs*

Syntax Description

num_of_msgs	Specifies the number of syslog messages that the ASA retains in the ASDM log buffer.

Command Default

The default ASDM syslog buffer size is 100 messages.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When the ASDM log buffer is full, the ASA deletes the oldest message to make room in the buffer for new messages. To control whether logging to the ASDM log buffer is enabled or to control the kind of syslog messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

The following example shows how to enable logging, send messages of severity levels 0, 1, and 2 to the ASDM log buffer, and how to set the ASDM log buffer size to 200 messages:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages that it contains.
logging asdm	Enables logging to the ASDM log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffered

To enable the ASA to send syslog messages to the log buffer, use the **logging buffered** command in global configuration mode. To disable logging to the log buffer, use the **no** form of this command.

logging buffered [*logging_list* | *level*]
no logging buffered [*logging_list* | *level*]

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the log buffer. For information about creating lists, see the **logging list** command.

Command Default

The defaults are as follows:

- Logging to the buffer is disabled.
- The buffer size is 4 KB.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Before any messages are sent to the log buffer, you must enable logging using the **logging enable** command.

New messages append to the end of the buffer. When the buffer fills up, the ASA clears the buffer and continues adding messages to it. When the log buffer is full, the ASA deletes the oldest message to make room in the buffer for new messages. You can have buffer contents automatically saved each time the contents of the buffer have "wrapped," which means that all the messages since the last save have been replaced by new messages. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

At any time, you can save the contents of the buffer to flash memory. For more information, see the **logging savelog** command.

You can view syslog messages that have been sent to the buffer with the **show logging** command.

Examples

The following example configures logging to the buffer for severity level 0 and level 1 events:

```
ciscoasa(config)# logging buffered alerts
ciscoasa(config)#
```

The following example creates a list named" notif-list" with a maximum severity level of 7 and configures logging to the buffer for syslog messages identified by the "notif-list" list:

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
logging savelog	Saves the contents of the log buffer to flash memory.

logging buffer-size

To specify the size of the log buffer, use the **logging buffer-size** command in global configuration mode. To reset the log buffer to its default size of 4 KB of memory, use the **no** form of this command.

loggingbuffer-size*bytes*
no logging buffer-size *bytes*

Syntax Description

bytes	Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the ASA uses 8 KB of memory for the log buffer.

Command Default

The default log buffer size is 4 KB of memory.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To see whether the ASA is using a log buffer of a size other than the default buffer size, use the **show running-config logging** command. If the **logging buffer-size** command is not shown, then the ASA uses a log buffer of 4 KB.

For more information about how the ASA uses the buffer, see the **logging buffered** command.

Examples

The following example enables logging, enables the logging buffer, and specifies that the ASA uses 16 KB of memory for the log buffer:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.

Command	Description
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging savelog	Saves the contents of the log buffer to flash memory.

logging class

To configure the maximum severity level per logging destination for a message class, use the **logging class** command in global configuration mode. To remove a message class severity level configuration, use the **no** form of this command.

logging class *class destination level* [*destination level* . . .]
no logging class *class*

Syntax Description

class	Specifies the message class whose maximum severity levels are configured per destination. For valid values of *class* , see the "Usage Guidelines" section.
destination	Specifies a logging destination for *class*. For the destination, the *level* determines the maximum severity level sent to *destination*. For valid values of *destination*, see the "Usage Guidelines" section that follows.
level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action is needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages. **Note** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

Command Default

By default, the ASA does not apply severity levels on a logging destination and message class basis. Instead, each enabled logging destination receives messages for all classes at the severity level determined by the logging list or severity level specified when you enabled the logging destination.

Command Modes

The following table shows the modes in which you may enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The **eigrp** option was added to valid class values.
8.2(1)	The **dap** option was added to valid class values.
9.12(1)	The **bfd, bgp, idb, ipv6, multicast, routing, object-group-search, pbr, sla** options was added to valid class values

Usage Guidelines

Valid values for *class* include the following:

- **auth**—User authentication.
- **bfd**—BFD Routing
- **bgp**—BGP Routing
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **dap—**Dynamic Access Policies.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **eigrp**—EIGRP routing.
- **email**—Email proxy.
- **ha**—Failover.
- **idb**—Interface
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **ipaa—**IP address assignment
- **ipv6**—IPv6 Stack

- **multicast**—Multicast Routing
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.
- **object-group-search**—Object group search
- **ospf**—OSPF routing.
- **pbr**—Policy Based Routing
- **rip**—RIP routing.
- **rm**—Resource Manager.
- **routing**—All Routing
- **session**—User session.
- **sla**—SLA Object-tracking
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPsec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Valid logging destinations are as follows:

- **asdm**—To learn about this destination, see the **logging asdm** command.
- **buffered**—To learn about this destination, see the **logging buffered** command.
- **console**—To learn about this destination, see the **logging console** command.
- **history**—To learn about this destination, see the **logging history** command.
- **mail**—To learn about this destination, see the **logging mail** command.
- **monitor**—To learn about this destination, see the **logging monitor** command.
- **trap**—To learn about this destination, see the **logging trap** command.

Examples

The following example specifies that, for failover-related messages, the maximum severity level for the ASDM log buffer is 2 and the maximum severity level for the syslog buffer is 7:

```
ciscoasa(config)# logging class ha asdm 2 buffered 7
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging console

To enable the ASA to display syslog messages in console sessions, use the **logging console** command in global configuration mode. To disable the display of syslog messages in console sessions, use the **no** form of this command.

logging console [*logging_list* | *level*]
nologgingconsole

Note We recommend that you do not use this command, because it may cause many syslog messages to be dropped due to buffer overflow. For more information, see the "Usage Guidelines" section.

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

  Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the console session. For information about creating lists, see the **logging list** command.

Command Default

The ASA does not display syslog messages in console sessions by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Before any messages are sent to the console, you must enable logging using the **logging enable** command.

Caution Using the **logging console** command could significantly degrade system performance. Instead, use the logging buffered command to start logging and the show logging command to view the messages. To make viewing the most current messages easier, use the clear logging **buffer** command to clear the buffer.

Examples

The following example shows how to enable syslog messages of severity levels 0, 1, 2, and 3 to appear in console sessions:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging debug-trace

To redirect debugging messages to logs as syslog message 711001 issued at severity level 7, use the **logging debug-trace** command in global configuration mode. To stop sending debugging messages to logs, use the **no** form of this command.

loggingdebug-trace
nologgingdebug-trace

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA does not include debugging output in syslog messages.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Debugging messages are generated as severity level 7 messages. They appear in logs with the syslog message number 711001, but do not appear in any monitoring session.

Examples

The following example shows how to enable logging, send log messages to the system log buffer, redirect debugging output to logs, and turn on debugging of disk activity.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

The following is sample output of a debugging message that could appear in the logs:

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.

Command	Description
show running-config logging	Displays the logging-related portion of the running configuration.

logging debug-trace persistent

To enable debug syslogs active in a particular session to be logged, even after the session ends, use the **logging debug-trace persistent** command in the global configuration mode. To disable a specific persistent debug configuration, use the **no** form of this command. This will clear it from the local session and also from persistent debugs.

loggingdebug-tracepersistent
nologgingdebug-tracepersistent

Syntax Description

This command has no arguments or keywords.

Command Default

By default, when a session ends, all the debug commands enabled in that particular session no longer exist in the configuration and hence are no longer logged on to a syslog server.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

When the logging debug-trace persistent command is enabled, any debug command entered from any session is saved globally and is visible from all sessions. This command gets saved to running configurations and across reboots.

Examples

The following example shows how to enable logging, send log messages to the system log buffer, redirect debugging output to logs, and turn on persistent debugging of disk activity.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace persistent
ciscoasa(config)# debug disk filesystem
```

The following is sample output of a debugging message that could appear in the logs:

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging device-id

To configure the ASA to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the use of a device ID, use the **no** form of this command.

logging device-id { **cluster-id** | **context-name** | **hostname ipaddress** *interface_name* [**system**] | **string** *text* }
no logging device-id { **cluster-id** | **context-name** | **hostname ipaddress** *interface_name* [**system**] | **string** *text* }

Syntax Description

cluster-id	Specifies the unique name of an individual ASA unit in the cluster as the device ID.
hostname	Specifies the hostname of the ASA as the device ID.
ipaddress *interface_name*	Specifies the device ID or the IP address of the interface in *interface_name*. If you use the ipaddress keyword, syslog messages sent to an external server include the IP address of the interface specified, regardless of which interface the ASA uses to send the log data to the external server.
string *text*	Specifies the characters included in *text* as the device ID, which can be up to 16 characters long. You cannot use white space characters or any of the following characters: • &—ampersand • '—single quote • "—double quote • <—less than • >—greater than • ?—question mark
system	(Optional) In the cluster environment, dictates that the device ID becomes the system IP address on the interface.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	The **cluster-id** and **system** keywords have been added.

Usage Guidelines

If you use the ipaddress keyword, the device ID becomes the specified ASA interface IP address, regardless of the interface from which the message is sent. This keyword provides a single, consistent device ID for all messages that are sent from the device. If you use the **system** keyword, the specified ASA uses the system IP address instead of the local IP address of the unit in a cluster. The **cluster-id** and **system** keywords apply to the ASA 5580 and 5585-X only.

Examples

The following example shows how to configure a host named “secappl-1”:

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

The hostname appears at the beginning of syslog messages, as shown in the following message:

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging emblem

To use the EMBLEM format for syslog messages sent to destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of EMBLEM format, use the **no** form of this command.

loggingemblem
nologgingemblem

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA does not use EMBLEM format for syslog messages.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed to be independent of the **logging host** command.

Usage Guidelines

The **logging** emblem command lets you to enable EMBLEM-format logging for all logging destinations other than syslog servers. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

Note The timestamp string for the emblem format does not include the year. To have the year displayed in the eventing syslog, you can enable timestamp as per RFC 5424 using the **logging timestamp rfc5424** command. Following is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

Alternatively, you can use the **logging device-id** command.

Examples

The following example shows how to enable logging and enable the use of EMBLEM-format for logging to all logging destinations except syslog servers:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging emblem
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging enable

To enable logging for all configured output locations, use the **logging enable** command in global configuration mode. To disable logging, use the **no** form of this command.

loggingenable
nologgingenable

Syntax Description

This command has no arguments or keywords.

Command Default

Logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **logging on** command.

Usage Guidelines

The **logging enable** command allows you to enable or disable sending syslog messages to any of the supported logging destinations. You can stop all logging with the no logging enable command.

You can enable logging to individual logging destinations with the following commands:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Examples

The following example shows how to enable logging. The output of the **show logging** command illustrates how each possible logging destination must be enabled separately:

```
ciscoasa
```

```
(config)#
logging enable
ciscoasa
(config)#
show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging facility

To specify the logging facility used for messages sent to syslog servers, use the **logging facility** command in global configuration mode. To reset the logging facility to its default of 20, use the **no** form of this command.

loggingfacility*facility*
nologgingfacility

Syntax Description

facility	Specifies the logging facility; valid values are 16 through 23.

Command Default

The default facility is 20 (LOCAL4).

Command Modes

The following table shows the modes in which you can enter the command, with the exceptions noted in the Syntax Description section.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Syslog servers file messages based on the facility number in the message. There are eight possible facilities: 16 (LOCAL0) through 23 (LOCAL7).

Examples

The following example shows how to specify that the ASA indicate the logging facility as 16 in syslog messages. The output of the **show logging** command includes the facility being used by the ASA:

```
ciscoasa(config)# logging facility 16
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
```

```
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging flash-bufferwrap

To enable the ASA to write the log buffer to flash memory every time the buffer is full of messages that have never been saved, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing of the log buffer to flash memory, use the **no** form of this command.

loggingflash-bufferwrap
nologgingflash-bufferwrap

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- Logging to the buffer is disabled.
- Writing the log buffer to flash memory is disabled.
- The buffer size is 4 KB.
- Minimum free flash memory is 3 MB.
- Maximum flash memory allocation for buffer logging is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

For the ASA to write the log buffer to flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to flash memory. You can enable logging to the buffer, using the **logging buffered** command. However, if the configured logging buffer size is more than 2MB, the internal log buffer will not be written to flash memory.

While the ASA writes log buffer contents to flash memory, it continues storing any new event messages to the log buffer.

The ASA creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY
-MM
-DD
```

-*HHMMSS*
.TXT

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

The availability of flash memory affects how the ASA saves syslog messages using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

Examples

The following example shows how to enable logging, enable the log buffer, and enable the ASA to write the log buffer to flash memory:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.

logging flash-maximum-allocation

To specify the maximum amount of flash memory that the ASA uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. To reset the maximum amount of flash memory used for this purpose to its default size of 1 MB of flash memory, use the **no** form of this command.

loggingflash-maximum-allocation*kbytes*
nologgingflash-maximum-allocation*kbytes*

Syntax Description

kbytes	The largest amount of flash memory, in kilobytes, that the ASA can use to save log buffer data.

Command Default

The default maximum flash memory allocation for log data is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command determines how much flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** causes flash memory use for log files to exceed the maximum amount specified by the **logging flash-maximum-allocation** command, the ASA deletes the oldest log files to free sufficient memory for the new log file. If there are no files to delete or if, after all old files are deleted, free memory is too small for the new log file, the ASA fails to save the new log file.

To see whether the ASA has a maximum flash memory allocation of a size different than the default size, use the **show running-config logging** command. If the **logging flash-maximum-allocation** command is not shown, then the ASA uses a maximum of 1 MB for saved log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the ASA uses the log buffer, see the **logging buffered** command.

Examples

The following example shows how to enable logging, enable the log buffer, enable the ASA to write the log buffer to flash memory, with the maximum amount of flash memory used for writing log files set to approximately 1.2 MB of memory:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-maximum-allocation 1200
ciscoasa(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging flash-minimum-free	Specifies the minimum amount of flash memory that must be available for the ASA to permit writing of the log buffer to flash memory.

logging flash-minimum-free

To specify the minimum amount of free flash memory that must exist before the ASA saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. To reset the minimum required amount of free flash memory to its default size of 3 MB, use the **no** form of this command.

loggingflash-minimum-free*kbytes*
nologgingflash-minimum-free*kbytes*

Syntax Description

kbytes The minimum amount of flash memory, in kilobytes, that must be available before the ASA saves a new log file.

Command Default

The default minimum free flash memory is 3 MB.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The logging flash-minimum-free command specifies how much flash memory the **logging savelog** and **logging flash-bufferwrap** commands must preserve at all times.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** would cause the amount of free flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the ASA deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the ASA fails to save the new log file.

Examples

The following example shows how to enable logging, enable the log buffer, enable the ASA to write the log buffer to flash memory, and specifies that the minimum amount of free flash memory must be 4000 KB:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging flash-maximum-allocation	Specifies the maximum amount of flash memory that can be used for writing log buffer contents.

logging flow-export-syslogs

To enable or disable all of the syslog messages that NetFlow captures, use the **logging flow-export-syslogs** command in global configuration mode.

logging flow-export-syslogs { **enable** | **disable** }

Syntax Description

enable	Enables all of the syslog messages that Netflow captures.
disable	Disables all of the syslog messages that Netflow captures.

Command Default

By default, all syslogs that are captured by NetFlow are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.

Usage Guidelines

If the security appliance is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command. The syslog messages that will be disabled are as follows:

Syslog Message	Description
106015	A TCP flow was denied because the first packet was not a SYN packet.
106023	A flow that is denied by an ingress ACL or an egress ACL that is attached to an interface through the **access-group** command.
106100	A flow that is permitted or denied by an ACL.
302013 and 302014	A TCP connection and deletion.
302015 and 302016	A UDP connection and deletion.
302017 and 302018	A GRE connection and deletion.
302020 and 302021	An ICMP connection and deletion.

Syslog Message	Description
313001	An ICMP packet to the security appliance was denied.
313008	An ICMPv6 packet to the security appliance was denied.
710003	An attempt to connect to the security appliance was denied.

Note Although this is a configuration mode command, it is not stored in the configuration. Only the **no logging message xxxxxx** commands are stored in the configuration.

Examples

The following example shows how to disable redundant syslog messages that NetFlow captures and the sample output that appears:

```
ciscoasa(config)# logging flow-export-syslogs disable
ciscoasa(config)# show running-config logging
no logging message xxxxx1
no logging message xxxxx2
```

where the *xxxxx1* and *xxxxx2* are syslog messages that are redundant because the same information has been captured through NetFlow. This command is like a command alias, and will convert to a batch of no logging message xxxxxx commands. After you have disabled the syslog messages, you can enable them individually with the **logging message xxxxxx** command, where *xxxxxx* is the specific syslog message number.

Related Commands

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
show flow-export counters	Displays a set of runtime counters for NetFlow.

logging from-address

To specify the sender e-mail address for syslog messages sent by the ASA, use the **logging from-address** command in global configuration mode. All sent syslog messages appear to come from the address you specify. To remove the sender e-mail address, use the **no** form of this command.

loggingfrom-address*from-email-address*
no logging from-address *from-email-address*

Syntax Description

from-email-address	Source e-mail address, that is, the e-mail address that syslog messages appear to come from (for example, cdb@example.com).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Sending syslog messages by e-mail is enabled by the **logging mail** command.

The address specified with this command need not correspond to an existing e-mail account.

Examples

To enable logging and set up the ASA to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
ciscoasa
(config)#
logging enable
```

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging mail	Enables the ASA to send syslog messages by e-mail and determines which messages are sent by e-mail.
logging recipient-address	Specifies the e-mail address to which syslog messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.

logging ftp-bufferwrap

To enable the ASA to send the log buffer to an FTP server every time the buffer is full of messages that have never been saved, use the **logging ftp-bufferwrap** command in global configuration mode. To disable sending the log buffer to an FTP server, use the **no** form of this command.

loggingftp-bufferwrap
no logging ftp-bufferwrap

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- Logging to the buffer is disabled.
- Sending the log buffer to an FTP server is disabled.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enable **logging ftp-bufferwrap**, the ASA sends log buffer data to the FTP server that you specify with the **logging ftp-server** command. While the ASA sends log data to the FTP server, it continues storing any new event messages to the log buffer.

For the ASA to send log buffer contents to an FTP server, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to flash memory. To enable logging to the buffer, use the **logging buffered** command.

The ASA creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Examples

The following example shows how to enable logging, enable the log buffer, specify an FTP server, and enable the ASA to write the log buffer to an FTP server. The example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username, logsupervisor and password, 1luvMy10gs. Log files are to be stored in the /syslogs directory:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-server	Specifies FTP server parameters for use with the **logging ftp-bufferwrap** command.

logging ftp-server

To specify details about the FTP server that the ASA sends log buffer data to when **logging ftp-bufferwrap** is enabled, use the **logging ftp-server** command in global configuration mode. To remove all details about an FTP server, use the **no** form of this command.

logging ftp-server *ftp_server path username* [*0* | *8*] *password*
no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) user password will follow.
8	(Optional) Specifies that an encrypted user password will follow.
ftp-server	External FTP server IP address or hostname. **Note** If you specify a hostname, be sure that DNS is operating correctly on your network.
password	The password for the username specified, which can be up to 64 characters long.
path	Directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. For example: `/security_appliances/syslogs/appliance107`
username	A username that is valid for logging in to the FTP server.

Command Default

No FTP server is specified by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	Support for password encryption was added.

Usage Guidelines

You can only specify one FTP server. If a logging FTP server is already specified, using the **logging ftp-server** command replaces this FTP server configuration with the new one that you enter.

The ASA does not verify the FTP server information that you specify. If you misconfigure any of the details, the ASA fails to send log buffer data to the FTP server.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are not supported. For example, 0 pass and 1 are invalid passwords.

Examples

The following example shows how to enable logging, enable the log buffer, specify an FTP server, and enable the ASA to write the log buffer to an FTP server. This example specifies an FTP server whose hostname is logserver. The server can be accessed with the username, user1 and password, pass1. Log files are to be stored in the /path1 directory:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

The following example shows how to enter an encrypted password:

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8
JPAGWzIIFVlheXv2I9nglfytOzHU
```

The following example shows how to enter an unencrypted (clear text) password:

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.

logging hide username

To hide usernames (for example, "*****") in syslogs when the username's validity is unknown, use the **logging hide username** command in global configuration mode. To see these usernames, use the **no** form of this command.

logginghideusername
no logging hide username

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to hide usernames.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(3)	This command was added.

Usage Guidelines

The **logging hide username** command allows you to hide usernames in syslogs until they are verified as valid.

Note This command is not available in Version 9.4(1).

Examples

The following example shows how to hide usernames in syslogs until they are verified as valid:

```
ciscoasa(config)# logging hide username
ciscoasa# show logging
Syslog logging: enabled
...
Hide Username logging: enabled | disabled
...
```

Related Commands

Command	Description
logging enable	Enables logging.

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging history

To enable SNMP logging and specify which messages are to be sent to SNMP servers, use the **logging history** command in global configuration mode. To disable SNMP logging, use the **no** form of this command.

logging history [**rate-limit** *number interval* **level** *level* | *logging_list* | *level*]
no logging history

Syntax Description

interval	Specifies the logging interval in seconds (under **rate-limit**) and thereby limiting the rate at which logs are forwarded to SNMP. If you set the **logging rate-limit** command, it takes precedence over this setting.
level	Specifies the logging level for history rate-limit. The messages that are forwarded to SNMP are limited to the specified syslog level.
level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages. **Note** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.
logging_list	Specifies the list that identifies the messages to send to the SNMP server. For information about creating lists, see the **logging list** command.
number	When using **rate-limit**, specify the *number* of messages to be logged for the *interval* period.
rate-limit	Limits the logs that are forwarded to SNMP. Specify **rate-limit**, in seconds for logging the syslog.

Command Default

The ASA does not log to SNMP servers by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.20(1)	The **rate-limit** keyword was added to rate limit the logs sent to SNMP.

Usage Guidelines

The **logging history** command allows you to enable logging to an SNMP server and to set the SNMP message level or event list.

Examples

The following example shows how to enable SNMP logging and specify that messages of severity levels 0, 1, 2, and 3 are sent to the SNMP server configured:

```
ciscoasa(config)# logging enable
ciscoasa(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
ciscoasa(config)# snmp-server enable traps syslog
ciscoasa(config)# logging history errors
ciscoasa(config)#
```

Examples

The following example rate limits critical syslogs sent to SNMP to 15 messages/15 seconds.

```
ciscoasa(config)# logging history rate-limit 15 15 level critical
```

Use the **no logging history** command to mitigate memory leakage of your device. This command does not impact the regular logging to the syslog server.

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
snmp-server	Specifies SNMP server details.

logging host

To define a syslog server, use the **logging host** command in global configuration mode. To remove a syslog server definition, use the **no** form of this command.

logging host *interface_name syslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*]] [**format emblem**]] [**secure** [**reference-identity** *reference_identity_name*]]
no logging host *interface_name syslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*] [**format emblem**]] [**secure** [**reference-identity** *reference_identity_name*]]

Syntax Description

format emblem	(Optional) Enables EMBLEM format logging for the syslog server. EMBLEM-format logging is available for UDP syslog messages only.
interface_name	Specifies the interface on which the syslog server resides.
port	Indicates the port that the syslog server listens to for messages. Valid port values are 1025–65535 for either protocol. If you enter zero as a port number, or use an invalid character or symbol, an error occurs.
secure	(Optional) Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. **Note** A secure logging connection can only be established with an SSL/TLS-capable syslog server. If an SSL/TLS connection cannot be established, all new connections will be denied. You may change this default behavior by entering the **logging permit-hostdown** command.
syslog_ip	Specifies the IP address (IPv4 or IPv6) of the syslog server.
tcp	Specifies that the ASA should use TCP to send messages to the syslog server.
udp	Specifies that the ASA should use UDP to send messages to the syslog server.
reference_identity_name	Specifies the name of the reference identity object that enables RFC 6125 reference identity checks for additional security. Identity checks on the received server certificate are based on this previously configured reference identity object
timestamp [**legacy** | **rfc5424**]	(Optional) Enables the timestamp format, which can be specified in legacy format or in RFC5424 format (yyyy-MM-THH:mm:ssZ, where the letter Z indicates the UTC time zone) .

Command Default

The default protocol is UDP.

The default setting for the **format emblem** option is false.

The default setting for the **secure** option is false.

The default port numbers are as follows:

- UDP—514
- TCP —1470

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0	This command was added.
8.0(2)	The **secure** keyword was added.
8.4(1)	Connection blocking can be enabled and disabled.
9.6.2	Added **reference-identity** option.
9.7(1)	You can now use IPv6 addresses for syslog servers. If you have a directly-connected syslog server, you can use a /31 subnet on the ASA and syslog server to create a point-to-point connection.

Usage Guidelines

The **logging host** *syslog_ip* format emblem command allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP syslog messages only. If you enable EMBLEM-format logging for a particular syslog server, then the messages are sent to that server. If you use the **logging timestamp** command, the messages with a time stamp are also sent.

You can use multiple logging host commands to specify additional servers that would all receive the syslog messages. However, you can only specify a server to receive either UDP or TCP syslog messages, not both.

If the presented identity in the server certificate cannot be matched against the configured **reference-identity**, the connection is not established and an error is logged.

The default setting for connection blocking is on when the **logging host** command has been configured to use TCP to send messages to a syslog server. If a TCP-based syslog server is configured, you can disable connection blocking with the **logging permit-hostdown** command.

Note When the **tcp** option is used in the **logging host** command, the ASA will drop connections across the firewall if the syslog server is unreachable.

You can display only the *port* and *protocol* values that you previously entered by using the **show running-config logging** command and finding the command in the listing—TCP is listed as 6, and UDP is listed as 17. TCP ports work only with the syslog server. The *port* must be the same port on which the syslog server listens.

Note An error message occurs if you try to use the **logging host** command and the **secure** keyword with UDP.

Sending syslogs over TCP is not supported on a standby ASA.

Examples

The following examples show how to send syslog messages of severity levels 0, 1, 2, and 3 to a syslog server on the inside interface that uses the default protocol and port number:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 2001:192:168:88::111
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging list

To create a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs), use the **logging list** command in global configuration mode. To remove the list, use the **no** form of this command.

logging list *name* { **level** *level* [**class** *event_class*] | **message** *start_id* [*-end_id*] }
no logging list *name*

Syntax Description

class *event_class*	(Optional) Sets the class of events for syslog messages. For the level specified, only syslog messages of the class specified are identified by the command. See the "Usage Guidelines" section for a list of classes.
level *level*	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages. **Note** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.
message *start_id* [*-end_id*]	Specified a message ID or range of IDs. To look up the default level of a message, use the **show logging** command or see the syslog messages guide.
name	Sets the logging list name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Logging commands that can use lists are the following:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *event_class* include the following:

- **auth**—User authentication.
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **email**—Email proxy.
- **ha**—Failover.
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.

- **ospf**—OSPF routing.
- **rip**—RIP routing.
- **session**—User session.
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPSec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Examples

The following example shows how to use the logging list command:

```
ciscoasa(config)# logging list my-list 100100-100110
ciscoasa(config)# logging list my-list level critical
ciscoasa(config)# logging list my-list level warning class vpn
ciscoasa(config)# logging buffered my-list
```

The preceding example states that syslog messages that match the criteria specified will be sent to the logging buffer. The criteria specified in this example are:

- Syslog message IDs that fall in the range of 100100 to 100110
- All syslog messages with critical level or higher (emergency, alert, or critical)
- All VPN class syslog messages with warning level or higher (emergency, alert, critical, error, or warning)

If a syslog message satisfies any one of these conditions, it is logged to the buffer.

Note When you design list criteria, the criteria can specify overlapping sets of messages. Syslog messages matching more than one set of criteria are logged normally.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging mail

To enable the ASA to send syslog messages by e-mail and to determine which messages are sent by e-mail, use the **logging mail** command in global configuration mode. To disable e-mailing of syslog messages, use the **no** form of this command.

logging mail [*logging_list* | *level*]
no logging mail [*logging_list* | *level*]

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the e-mail recipient. For information about creating lists, see the **logging list** command.

Command Default

Logging to e-mail is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

E-mailed syslog messages appear in the subject line of the e-mails sent.

Examples

To set up the ASA to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which e-mailed syslog messages appear to come.
logging list	Creates a reusable list of message selection criteria.
logging recipient-address	Specifies the e-mail address to which e-mailed syslog messages are sent.
smtp-server	Configures an SMTP server.

logging message

To enable logging of a syslog message, or to change the level of a message, use the **logging message** command in global configuration mode. To disable logging of a message, or to set it to its default level, use the **no** form of this command.

logging message *syslog_id* [**level** *level* | **standby**]
no logging message *syslog_id* [**level** *level* | **standby**]

Syntax Description

level *level* (Optional) Sets the severity level for the specified syslog message. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

To look up the default level of a message, use the **show logging** command or see the syslog messages guide.

syslog_id The ID of the syslog message that you want to enable or disable or whose severity level you want to modify.

standby (Optional) Specify the **no** form of the command with the **standby** keyword to block specific syslog messages from being generated on a standby unit.

Command Default

By default, all syslog messages are enabled and the severity levels of all messages are set to their default levels.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.4(1)	The **standby** keyword was added.

Usage Guidelines

You can use the **logging message** command for these purposes:

- To specify whether a message is enabled or disabled.
- To disable generation of a syslog message on the standby unit.
- To set the severity level of a message.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

To prevent the ASA from generating a particular syslog message, use the **no** form of the **logging message** command (without the **level** keyword) in global configuration mode. To let the ASA generate a particular syslog message, use the **logging message** command (without the **level** keyword). You can use these two versions of the **logging message** command in parallel.

Examples

The series of commands in the following example show the use of the **logging message** command to specify both whether a message is enabled and the severity level of the message:

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)
ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled),standby logging (disabled)
ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

Command	Description
clear configure logging	Clears all logging configuration or message configuration only.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging message standby

To unblock a specific syslog message that was previously blocked from being generated on a standby unit, use the **logging message standby** command in global configuration mode. To block a specific syslog message from being generated on a standby unit, use the **no** form of this command.

logging message *syslog_id* **standby**
no logging message *syslog_id* **standby**

Syntax Description

syslog_id	The ID of the syslog message that you want to enable or disable on a standby unit.

Command Default

By default, all syslog messages are generated on the standby unit (only when the logging standby command is enabled).

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

You can use the **[no] logging message** *syslog_id* **standby** command to specify whether or not a syslog message is enabled or disabled on a standby unit.

You can use the **show logging** command to determine whether or not a syslog message has been enabled.

Examples

The series of commands in the following example show how to use the **logging message** *syslog_id* **standby** command to specify whether or not a syslog message has been enabled on the standby unit:

```
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled), standby logging disabled
```

Related Commands

Command	Description
clear configure logging	Clears all logging configuration or syslog message configuration only.
logging enable	Enables logging.

Command	Description
show running-config logging	Displays the logging-related portion of the running configuration.

logging monitor

To enable the ASA to display syslog messages in SSH and Telnet sessions, use the **logging monitor** command in global configuration mode. To disable the display of syslog messages in SSH and Telnet sessions, use the **no** form of this command.

logging monitor [*logging_list* | *level*]
nologgingmonitor

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the SSH or Telnet session. For information about creating lists, see the **logging list** command.

Command Default

The ASA does not display syslog messages in SSH and Telnet sessions by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **logging monitor** command enables syslog messages for all sessions in the current context; however, in each session, the **terminal** command controls whether syslog messages appear in that session.

Examples

The following example shows how to enable the display of syslog messages in console sessions. The use of the **errors** keyword indicates that messages of severity levels 0, 1, 2, and 3 should display in SSH and Telnet sessions. The **terminal** command enables the messages to appear in the current session:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
terminal	Sets terminal line parameters.

logging permit-hostdown

To make the status of a TCP-based syslog server irrelevant to new user sessions, use the **logging permit-hostdown** command in global configuration mode. To cause the ASA to deny new user sessions when a TCP-based syslog server is unavailable, use the **no** form of this command.

loggingpermit-hostdown
nologgingpermit-hostdown

Syntax Description

This command has no arguments or keywords.

Command Default

By default, if you have enabled logging to a syslog server that uses a TCP connection, the ASA does not allow new network access sessions when the syslog server is unavailable for any reason. The default setting is false for the **logging permit-hostdown** command.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you are using TCP as the logging transport protocol for sending messages to a syslog server, the ASA denies new network access sessions as a security measure if the ASA is unable to reach the syslog server. You can use the **logging permit-hostdown** command to remove this restriction.

Examples

The following example makes the status of TCP-based syslog servers irrelevant to whether the ASA permits new sessions. When the **logging permit-hostdown** command includes in its output the **show running-config logging** command, the status of TCP-based syslog servers is irrelevant to new network access sessions.

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging queue

To specify how many syslog messages the ASA may hold in its queue before processing them according to the logging configuration, use the **logging queue** command in global configuration mode. To reset the logging queue size to the default of 512 messages, use the **no** form of this command.

logging queue *queue_size*
no logging queue *queue_size*

Syntax Description

queue_size	The number of syslog messages permitted in the queue used for storing syslog messages before processing them. Valid values are from 0 to 8192 messages, depending on the platform type. If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages), depending on the platform. On the ASA-5505, the maximum queue size is 1024. On the ASA-5510, it is 2048, and on all other platforms, it is 8192.

Command Default

The default queue size is 512 messages.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When traffic is so heavy that the queue fills up, the ASA may discard messages. On the ASA 5505, the maximum queue size is 1024. On the ASA-5510, it is 2048. On all other platforms, it is 8192.

Caution Increasing the logging queue size on low-end platforms can reduce the volume of available DMA memory for other features, such as ASDM, WebVPN, DHCP Server, and so forth. These features can stop functioning if the system runs out of DMA memory. Use the **show memory detail** command to check the volume of free DMA memory in the MEMPOOL_DMA pool.

Examples

The following example shows how to display the output of the logging queue and show logging queue commands:

```
ciscoasa(config)# logging queue 0
ciscoasa(config)# show logging queue
```

```
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the logging queue command is set to 0, which means that the queue is set to the maximum of 8192. The syslog messages in the queue are processed by the ASA in the manner dictated by the logging configuration, such as sending syslog messages to mail recipients, saving them to flash memory, and so forth.

The output of this example show logging queue command shows that 5 messages are queued, 3513 messages was the largest number of messages in the queue at one time since the ASA was last booted, and that 1 message was discarded. Even though the queue was set for unlimited messages, the message was discarded because no block memory was available to add the message to the queue.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging rate-limit

To limit the rate at which syslog messages are generated, use the **logging rate-limit** command in privileged EXEC mode. To disable rate limiting, use the **no** form of this command in privileged EXEC mode.

logging rate-limit { **unlimited** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }
[**no**] **logging rate-limit** { **unlimited** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }

Syntax Description

block*value*	Percentage of the block to act as the threshold for rate limiting.
dynamic	Limits logging rate when block usage of size 256 exceeds a specified threshold value. Disables the rate limiting when the block usage returns to normal value.
interval	(Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for *interval* is 0 through 2147483647.
level *severity_level*	Applies the set rate limits on all syslog messages that belong to a certain severity level. All syslog messages at a specified severity level are rate-limited individually. The valid range for *severity_level* is 1 through 7.
message	Suppresses reporting of this syslog message.
message limit*value*	Number of messages permitted for the dynamic rate-limit.
num	Number of syslog messages that can be generated during the specified time interval. The valid range of values for *num* is 0 through 2147483647.
syslog_id	ID of the syslog message to be suppressed. The valid range of values is 100000-999999.
unlimited	Disables rate limiting, which means that there is no limit on the logging rate.

Command Default

The default setting for *interval* is 1.

The default setting for **message limit***value* is 10.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(4)	This command was added.
9.18(1)	Dynamic option for rate-limit was added.

Usage Guidelines

The syslog message severity levels are as follows:

- 0—System is unusable
- 1—Immediate action needed
- 2—Critical Conditions
- 3—Error Conditions
- 4—Warning Conditions
- 5—Normal but significant conditions
- 6—Informational Messages
- 7—Debugging Messages

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

Examples

To limit the rate of syslog message generation, you can enter a specific message ID. The following example shows how to limit the rate of syslog message generation using a specific message ID and time interval:

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

This example suppresses syslog message 302020 from being sent to the host after the rate limit of 100 is reached in the specified interval of 600 seconds.

To limit the rate of syslog message generation, you can enter a specific severity level. The following example shows how to limit the rate of syslog message generation using a specific severity level and time interval.

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

This example suppresses all syslog messages under severity level 6 to the specified rate limit of 1000 in the specified time interval of 600 seconds. Each syslog message in severity level 6 has a rate limit of 1000.

To enable the dynamic rate limit of messages when the block usage of size 256 is high, use the **dynamic** keyword. You can specify the percentage of free 256 blocks as threshold for triggering the dynamic rate-limit. You can also use the **message limit** keyword to allow number of messages for dynamic rate-limit. Its default value is 10.

```
asa(config)# logging rate-limit ?

configure mode commands/options:
  <1-2147483647>  Specify logging rate-limit number
  dynamic         Specify dynamic option for rate-limit
  unlimited       Specify unlimited option for rate-limit

asa(config)# logging rate-limit dynamic ?

configure mode commands/options:
  block  Dynamic rate-limit for block usage

asa(config)# logging rate-limit dynamic block ?

configure mode commands/options:
  <1-100>  Specify 256 blocks free percentage to trigger dynamic rate-limit
asa(config)# logging rate-limit dynamic block 50 ?

configure mode commands/options:
  messagelimit  Specify the number of messages allowed for dynamic rate-limit

asa(config)# logging rate-limit dynamic block 50 messagelimit ?

configure mode commands/options:
  <1-100>  Specify logging rate-limit interval
```

Related Commands

Command	Description
clear running-config logging rate-limit	Resets the logging rate limit setting to its default.
show logging	Shows the messages currently in the internal buffer or logging configuration settings.
show running-config logging rate-limit	Shows the current logging rate limit setting.

logging recipient-address

To specify the receiving e-mail address for syslog messages sent by the ASA, use the **logging recipient-address** command in global configuration mode. To remove the receiving e-mail address, use the **no** form of this command.

logging recipient-address *address* [**level** *level*]
no logging recipient-address *address* [**level** *level*]

Syntax Description

address	Specifies recipient e-mail address when sending syslog messages by e-mail.
level	Indicates that a severity level follows.
level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages. **Note** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use. **Note** We do not recommend using a severity level greater than 3 with the **logging recipient-address** command. Higher severity levels are likely to cause dropped syslog messages because of buffer overflow. The message severity level specified by a **logging recipient-address** command overrides the message severity level specified by the **logging mail** command. For example, if a **logging recipient-address** command specifies a severity level of 7 but the **logging mail** command specifies a severity level of 3, the ASA sends all messages to the recipient, including those of severity levels 4, 5, 6, and 7.

Command Default

The default value is set to the errors logging level.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can configure up to 5 recipient addresses. If you want, each recipient address can have a different message level than that specified by the **logging mail** command. Sending syslog messages by e-mail is enabled by the **logging mail** command.

Use this command to have more urgent messages sent to a larger number of recipients.

Examples

To set up the ASA to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which syslog messages appear to come.
logging mail	Enables the ASA to send syslog messages by e-mail and determines which messages are sent by e-mail.

Command	Description
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.

logging savelog

To save the log buffer to flash memory, use the **logging savelog** command in privileged EXEC mode.

logging savelog [*savefile*]

Syntax Description

savefile (Optional) Saved flash memory file name. If you do not specify the file name, the ASA saves the log file using a default time-stamp format, as follows:

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Command Default

The defaults are as follows:

- Buffer size is 4 KB.
- Minimum free flash memory is 3 MB.
- Maximum flash memory allocation for buffer logging is 1 MB.
- The default log file name is described in the “Syntax Description” section.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Before you can save the log buffer to flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be saved to flash memory. To enable logging to the buffer, use the **logging buffered** command.

Note The **logging savelog** command does not clear the buffer. To clear the buffer, use the **clear logging buffer** command.

Examples

The following example enables logging and the log buffer, exits global configuration mode, and saves the log buffer to flash memory using the file name, latest-logfile.txt:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# exit
ciscoasa# logging savelog latest-logfile.txt
ciscoasa#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.

logging standby

To enable the failover standby ASA to send syslog messages to logging destinations, use the **logging standby** command in global configuration mode. To disable syslog messaging and SNMP logging, use the **no** form of this command.

loggingstandby
nologgingstandby

Syntax Description

This command has no arguments or keywords.

Command Default

The logging standby command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enable the **logging standby** command to ensure that the syslog messages of the failover standby ASA stay synchronized if failover occurs.

Note Using the **logging standby** command causes twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

Examples

The following example enables the ASA to send syslog messages to the failover standby ASA. The output of the **show logging** command indicates that this feature is enabled:

```
ciscoasa(config)# logging standby
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
failover	Enables the failover feature.
logging enable	Enables logging.
logging host	Defines a syslog server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging timestamp

To specify that syslog messages should include the date and time that the messages was generated, use the **logging timestamp** command in global configuration mode. To remove the date and time from syslog messages, use the **no** form of this command.

logging timestamp [**rfc5424**]
nologgingtimestamp

Syntax Description

rfc5424 (Optional) All timestamp of syslog messages would be displaying the time as per RFC 5424 format:

```
YYYY
-MM
-DD
THH:MM:SS
Z
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Command Default

The ASA does not include the date and time in syslog messages by default.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.10(1)	**The option to enable timestamp as per RFC 5424 format was added**

Usage Guidelines

The logging timestamp command makes the ASA include a timestamp in all syslog messages. Untill version 9.10(1), the timestamp of syslogs was RFC 3164 compliant where the timestamp was displayed in "MM DD YYYY HH:MM:SS" format.

This format is not preferred in SIEMs and hence RFC 5424 option was introduced in 9.10(1).

Use the RFC 5424 option with logging timestamp command to enable syslogs support timezone as per RFC 5424.

Examples

The following example enables the inclusion of timestamp information in all syslog messages:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp
ciscoasa(config)#
```

The following example enables the inclusion of timestamp information in RFC 5424 format in all syslog messages:

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp rfc5424
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging trap

To specify which syslog messages the ASA sends to a syslog server, use the **logging trap** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

logging trap [*logging_list* | *level*]
nologgingtrap

Syntax Description

level Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the ASA generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:

- **0** or **emergencies**—System is unusable.
- **1** or **alerts**—Immediate action needed.
- **2** or **critical**—Critical conditions.
- **3** or **errors**—Error conditions.
- **4** or **warnings**—Warning conditions.
- **5** or **notifications**—Normal but significant conditions.
- **6** or **informational**—Informational messages.
- **7** or **debugging**—Debugging messages.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

logging_list Specifies the list that identifies the messages to send to the syslog server. For information about creating lists, see the **logging list** command.

Command Default

No default syslog message trap is defined.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you are using TCP as the logging transport protocol, the ASA denies new network access sessions as a security measure if the ASA is unable to reach the syslog server, if the syslog server is misconfigured or if the disk is full.

UDP-based logging does not prevent the ASA from passing traffic if the syslog server fails.

Examples

The following example shows how to send syslog messages of severity levels 0, 1, 2, and 3 to a syslog server that resides on the inside interface and uses the default protocol and port number.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

login

To log into privileged EXEC mode using the local user database (see the username command) or to change user names, use the **login** command in user EXEC mode.

login

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

From user EXEC mode, you can log in to privileged EXEC mode as any username in the local database using the **login** command. The **login** command is similar to the **enable** command when you have enable authentication turned on (see the **aaa authentication console** command). Unlike enable authentication, the **login** command can only use the local username database, and authentication is always required with this command. You can also change users using the **login** command from any CLI mode.

To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the **aaa authorization command** for more information.

Caution If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

Examples

The following example shows the prompt after you enter the **login** command:

```
ciscoasa> login
Username:
```

Related Commands

Command	Description
aaa authorization command	Enables command authorization for CLI access.
aaa authentication console	Requires authentication for console, Telnet, HTTP, SSH, or **enable** command access.
logout	Logs out of the CLI.
username	Adds a user to the local database.

login-button

To customize the Login button of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **login-button** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-button { **text** | **style** } *value*

[**no**] **login-button** { **text** | **style** } *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default login button text is “Login”.

The default login button style is:

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the Login button with the text “OK”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

Related Commands

Command	Description
login-title	Customizes the title of the WebVPN page login box.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.

login-message

To customize the login message of the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **login-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-message { **text** | **style** } *value*

[**no**] **login-message** { **text** | **style** } *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default login message is “Please enter your username and password”.

The default login message style is background-color:#CCCCCC;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
WebVPN customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the login message text is set to "username and password":

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

Related Commands

Command	Description
login-title	Customizes the title of the login box on the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page login.
password-prompt	Customizes the password prompt of the WebVPN page login.
group-prompt	Customizes the group prompt of the WebVPN page login.

login-title

To customize the title of the login box on the WebVPN page displayed to WebVPN users, use the **login-title** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-title { **text** | **style** } *value*

[**no**] **login-title** { **text** | **style** } *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default login text is "Login".

The default HTML style of the login title is background-color: #666666; color: white.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the login title style:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

Command	Description
login-message	Customizes the login message of the WebVPN login page.
username-prompt	Customizes the username prompt of the WebVPN login page.
password-prompt	Customizes the password prompt of the WebVPN login page.
group-prompt	Customizes the group prompt of the WebVPN login page.

logo

To customize the logo on the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **logo** command from webvpn customization mode. To remove a logo from the configuration and reset the default (the Cisco logo), use the **no** form of this command.

logo { **none** | **file** { *path value* } }

[**no**] **logo** { **{none** | **file** { *path value* } }

Syntax Description

file	Indicates you are supplying a file containing a logo.
none	Indicates that there is no logo. Sets a null value, thereby disallowing a logo. Prevents inheriting a logo.
path	The path of the filename. The possible paths are disk0:, disk1:, or flash:
value	Specifies the filename of the logo. Maximum length is 255 characters, with no spaces. File type must be JPG, PNG, or GIF, and must be less than 100 KB.

Command Default

The default logo is the Cisco logo.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

If the filename you specify does not exist, an error message displays. If you remove a logo file but the configuration still points to it, no logo displays.

The filename cannot contain spaces.

Examples

In the following example, the file cisco_logo.gif contains a custom logo:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Related Commands

Command	Description
title	Customizes the title of the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

logout

To exit from the CLI, use the **logout** command in user EXEC mode.

logout

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **logout** command lets you log out of the ASA. You can use the **exit** or **quit** commands to go back to unprivileged mode.

Examples

The following example shows how to log out of the ASA:

```
ciscoasa> logout
```

Related Commands

Command	Description
login	Initiates the log-in prompt.
exit	Exits an access mode.
quit	Exits configuration or privileged mode.

logout-message

To customize the logout message of the WebVPN logout screen that is displayed to WebVPN users when they logout from WebVPN service, use the **logout-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

logout-message { **text** | **style** } *value*

[**no**] **logout-message** { **text** | **style** } *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default logout message text is “Goodbye”.

The default logout message style is background-color:#999999;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
WebVPN customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the logout message style:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# logout-message style background-color: rgb(51,51,255);color:
 rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

Command	Description
logout-title	Customizes the logout title of the WebVPN page.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.

lsp-full suppress

To control which routes are suppressed when the link-state protocol data unit (PDU) becomes full, use the **lsp-full suppress** command in router isis configuration mode. To stop suppression of redistributed routes, specify the **no** form of this command.

lsp-full suppress { **external** [**interlevel**] | **interlevel** [**external**] | **none** }
nolsp-fullsuppress

Syntax Description

external	Suppresses any redistributed routes on this ASA.
interlevel	Suppresses any routes coming from the other level. For example, if the Level-2 LSP becomes full, routes from Level 1 are suppressed.
none	Suppresses no routes.

Command Default

Redistributed routes are suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command allows the monitoring of IS-IS adjacency state changes. This may be very useful when monitoring large networks. Messages are logged using the system error message facility. Messages are of the form:

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

Examples

The following example shows how to specify that if the LSP becomes full, both redistributed routes and routes from another level will be suppressed from the LSP:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-full suppress interlevel external
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
pnrotocol shutdow	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

lsp-gen-interval

To customize IS-IS throttling of LSP generation, use the **lsp-gen-interval** command in router isis configuration mode. To restore default values, use the **no** form of this command.

lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*
nolsp-gen-interval

Syntax Description

level-1	(Optional) Applies intervals to Level 1 areas only.
level-2	(Optional) Applies intervals to Level 2 areas only.
lsp-max-wait	Indicates the maximum interval between two consecutive occurrences of an LSP being generated. The range is 1 to 120 seconds.
lsp-initial-wait	(Optional) Indicates the initial LSP generation delay. The range is 1 to 120,000 milliseconds.
lsp-second-wait	(Optional) Indicates the hold time between the first and second LSP generation. The range is 1 to 120,000 milliseconds.

Command Default

lsp-max-wait: 5 seconds

lsp-initial-wait: 50 milliseconds

lsp-second-wait: 5000 milliseconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The following descriptions aid in determining whether to change the default values of this command:

- The *lsp-initial-wait* argument indicates the initial wait time before generating the first LSP.
- The third argument indicates the amount of time to wait between the first and second LSP generation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *lsp-max-wait interval* specified, so this value causes the throttling or slowing down of the LSP generation

after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down

- After the network calms down and there are no triggers for 2 times the *lsp-max-wait* interval, fast behavior is restored (the initial wait time).

Examples

The following example configures the intervals for LSP generation throttling:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface

Command	Description
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.

Command	Description
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

lsp-refresh-interval

To set the LSP refresh interval, use the **lsp-refresh-interval** command in router isis configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds*
no lsp-refresh-interval

Syntax Description

seconds	Interval at which LSPs are refreshed.The range is 1 to 65535 seconds.

Command Default

The default is 900 seconds (15 minutes).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The refresh interval determines the rate at which the software periodically transmits in LSPs the route topology information that it originates. This is done to keep the database information from becoming too old.

Note LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you set the LSP lifetime too low compared to the LSP refresh interval, the software reduces the LSP refresh interval to prevent the LSPs from timing out.

Examples

The following example configures the IS-IS LSP refresh interval to 1080 seconds:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-refresh-interval 1080
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.

Command	Description
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.

Command	Description
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

maa – match d

mac address

To specify the virtual MAC addresses for the active and standby units, use the **mac address** command in failover group configuration mode. To restore the default virtual MAC addresses, use the **no** form of this command.

mac address *phy_if* [*active_mac*] [*standby_mac*]
no mac address *phy_if* [*active_mac*] [*standby_mac*]

Syntax Description

phy_if	The physical name of the interface to set the MAC address.
active_mac	The virtual MAC address for the active unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
standby_mac	The virtual MAC address for the standby unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Command Default

The defaults are as follows:

- Active unit default MAC address: 00a0.c9*physical_port_number* .*failover_group_id* 01.
- Standby unit default MAC address: 00a0.c9*physical_port_number* .*failover_group_id* 02.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the virtual MAC addresses are not defined for the failover group, the default values are used.

If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address.

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

Examples

The following partial example shows a possible configuration for a failover group:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover mac address	Specifies a virtual MAC address for a physical interface.

mac-address

To manually assign a private MAC address to an interface or subinterface, use the **mac-address** command in interface configuration mode. In multiple context mode, this command can assign a different MAC address to the interface in each context. For an individual interface in a cluster, you can assign a cluster pool of MAC addresses. To revert the MAC address to the default, use the **no** form of this command.

mac-address { *mac_address* [**standby** *mac_address* | **site-id** *number* [**site-ip ip_address**]] | **cluster-pool** *pool_name* }
no mac-address { *mac_address* [**standby** *mac_address* | **site-id** *number* [**site-ip ip_address**]] | **cluster-pool** *pool_name* }

Syntax Description

cluster-pool *pool_name*	For a cluster in individual interface mode (see the **cluster interface-mode** command), or for a management interface in any cluster interface mode, sets a pool of MAC addresses to be used for a given interface on each cluster member. Define the pool using the **mac-address pool** command.
mac_address	Sets the MAC address for this interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. If you use failover, this MAC address is the active MAC address. **Note** Because auto-generated addresses (the **mac-address auto** command) start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.
site-id *number*	(Optional; Routed mode only) For inter-site clustering, configures a site-specific MAC address for each site.
site-ip *ip_address*	(Optional; Routed mode only) For inter-site clustering, configures a site-specific IP address for each site. The IP address must be on the same subnet as the global IP address.
standby *mac_address*	(Optional) Sets the standby MAC address for failover. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Command Default

The default MAC address is the burned-in MAC address of the physical interface. Subinterfaces inherit the physical interface MAC address. Some commands set the physical interface MAC address (including this command in single mode), so the inherited address depends on that configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(5)/8.2(2)	The use of A2 to start the MAC address was restricted when also used with the **mac-address auto** command.
9.0(1)	The **cluster-pool** keyword was added to support clustering.
9.5(1)	The **site-id** keyword was added.
9.6(1)	The **site-ip** keyword was added.

Usage Guidelines

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the ASA easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the CLI configuration guide for more information.

You can assign each MAC address manually with this command, or you can automatically generate MAC addresses for shared interfaces in contexts using the **mac-address auto** command. If you automatically generate MAC addresses, you can use the **mac-address** command to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

For clustering, you must configure a global MAC address for a Spanned EtherChannel. With a manually-configured MAC address, the MAC address stays with the current master unit. In multiple context mode, if you share an interface between contexts, you should enable auto-generation of MAC addresses. Note that you must manually configure the MAC address for non-shared interfaces.

For inter-site clustering in routed mode, configure a site-specific MAC address and IP address on the master unit for each site, then use the **site-id** command on each unit to assign it to a site.

Examples

The following example configures the MAC address for GigabitEthernet 0/1.1:

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

The following example configures site-specific MAC addresses for Spanned EtherChannel port-channel 1:

```
ciscoasa(config-if)# interface port-channel 1
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.7.7.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.7.7.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.7.7.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.7.7.4
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address auto	Auto-generates MAC addresses (active and standby) for shared interfaces in multiple context mode.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

mac-address auto

To automatically assign private MAC addresses to each shared context interface, use the **mac-address auto** command in global configuration mode. To disable automatic MAC addresses, use the **no** form of this command.

mac-address auto [**prefix** *prefix*]
no mac-address auto

Syntax Description

prefix *prefix*	(Optional) Sets a user-defined prefix as part of the MAC address. The *prefix* is a decimal value between 0 and 65535. If you do not enter a prefix, then the ASA generates a default prefix. This prefix is converted to a 4-digit hexadecimal number. The prefix ensures that each ASA uses unique MAC addresses (using different prefix values), so you can have multiple ASAs on a network segment, for example.

Command Default

Automatic MAC address generation is disabled by default, except for the ASASM, where it is enabled by default. When enabled, the ASA autogenerates the prefix based on the last two bytes of the interface (ASA 5500-X) or backplane (ASASM) MAC address. You can customize the prefix if desired.

If you disable MAC address generation, see the following default MAC addresses:

- For the ASA 5500-X series appliances—The physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.
- For the ASASM—All VLAN interfaces use the same MAC address, derived from the backplane MAC address.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
8.0(5)/8.2(2)	The **prefix** keyword was added. The MAC address format was changed to use the prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresses are also now persistent across reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.
8.5(1)	Autogeneration is now enabled by default (**mac-address auto**) for the ASASM only.

Release	Modification
8.6(1)	The ASA now converts the automatic MAC address generation configuration to use a default prefix. The ASA auto-generates the prefix based on the last two bytes of the interface (ASA 5500) or backplane (ASASM) MAC address. This conversion happens automatically when you reload, or if you reenable MAC address generation. The legacy method of MAC address generation is no longer available. **Note** To maintain hitless upgrade for failover pairs, the ASA does *not* convert the MAC address method in an existing configuration upon a reload if failover is enabled.

Usage Guidelines

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each shared context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the CLI configuration guide for information about classifying packets.

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the **mac-address** command to manually set the MAC address.

Interaction with Manual MAC Addresses

If you manually assign a MAC address and also enable auto-generation, then the manually assigned MAC address is used. If you later remove the manual MAC address, the auto-generated address is used.

Because auto-generated addresses start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.

Failover MAC Addresses

For use with failover, the ASA generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption. See the <xref> section for more information.

For upgrading failover units with the legacy version of the **mac-address auto** command before the **prefix** keyword was added, see the <xref> section.

MAC Address Format Using a Prefix

The ASA generates the MAC address using the following format:

A2*xx.yyzz.zzzz*

Where *xx.yy* is a user-defined prefix or an autogenerated prefix based on the last two bytes of the interface (ASA 5500) or backplane (ASASM) MAC address, and zz.zzzz is an internal counter generated by the ASA. For the standby MAC address, the address is identical except that the internal counter is increased by 1.

For an example of how the prefix is used, if you set a prefix of 77, then the ASA converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the ASA native form:

A2**4D.00***zz.zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1.03***zz.zzzz*

MAC Address Format Without a Prefix (Legacy Method)

This method may be used if you use failover and you upgraded to Version 8.6 or later; in this case, you have to manually enable the prefix method.

Without a prefix, the MAC address is generated using the following format:

- Active unit MAC address: 12*_slot .port _subid .contextid* .
- Standby unit MAC address: 02*_slot .port _subid .contextid* .

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context, viewable with the **show context detail** command. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

- Active: 1200.0131.0001
- Standby: 0200.0131.0001

This MAC address generation method does not allow for persistent MAC addresses across reloads, does not allow for multiple ASAs on the same network segment (because unique MAC addresses are not guaranteed), and does not prevent overlapping MAC addresses with manually assigned MAC addresses. We recommend using a prefix with the MAC address generation to avoid these issues.

When the MAC Address is Generated

When you configure a **nameif** command for the interface in a context, the new MAC address is generated immediately. If you enable this command after you configure context interfaces, then MAC addresses are generated for all interfaces immediately after you enter the command. If you use the **no mac-address auto** command, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

Setting the MAC Address Using Other Methods

You can also set the MAC address using other commands or methods, but we recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

Viewing MAC Addresses in the System Configuration

To view the assigned MAC addresses from the system execution space, enter the **show running-config all context** command.

The **all** option is required to view the assigned MAC addresses. Although this command is user-configurable in global configuration mode only, the **mac-address auto** command appears as a read-only entry in the configuration for each context along with the assigned MAC address. Only allocated interfaces that are configured with a **nameif** command within the context have a MAC address assigned.

Note If you manually assign a MAC address to an interface, but also have auto-generation enabled, the auto-generated address continues to show in the configuration even though the manual MAC address is the one that is in use. If you later remove the manual MAC address, the auto-generated one shown will be used.

Viewing MAC Addresses Within a Context

To view the MAC address in use by each interface within the context, enter the **show interface | include (Interface)|(MAC)** command.

Note The **show interface** command shows the MAC address in use; if you manually assign a MAC address and also have auto-generation enabled, then you can only view the unused auto-generated address from within the system configuration.

Examples

The following example enables automatic MAC address generation with a prefix of 78:

```
ciscoasa(config)# mac-address auto prefix 78
```

The following output from the **show running-config all context admin** command shows the primary and standby MAC address assigned to the Management0/0 interface:

```
ciscoasa# show running-config all context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

The following output from the **show running-config all context** command shows all the MAC addresses (primary and standby) for all context interfaces. Note that because the GigabitEthernet0/0 and GigabitEthernet0/1 main interfaces are not configured with a **nameif** command inside the contexts, no MAC addresses have been generated for them.

```
ciscoasa# show running-config all context
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!
context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!
context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
```

```
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address	Manually sets the MAC address (active and standby) for a physical interface or subinterface. In multiple context mode, you can set different MAC addresses in each context for the same interface.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

mac-address pool

To add a MAC address pool for use on an individual interface in an ASA cluster, use the **mac-address pool** command in global configuration mode. To remove an unused pool, use the **no** form of this command.

mac-address pool *name start_mac_address - end_mac_address*
no mac-address pool *name* [*start_mac_address - end_mac_address*]

Syntax Description

name	Names the pool up to 63 characters in length.
start_mac_address - end_mac_address	Specifies the first MAC address and the last MAC address. Note to add a space around the dash (-).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You can use the pool in the **mac-address cluster-pool** command in interface configuration mode. It is not common to manually configure MAC addresses for an interface, but if you have special needs to do so, then this pool is used to assign a unique MAC address to each interface.

Examples

The following example adds a MAC address pool with 8 MAC addresses, and assigns it to the GigabitEthernet 0/0 interface:

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

Related Commands

Command	Description
interface	Configures an interface.
mac-address	Configures a MAC address for an interface.

mac-address-table aging-time

To set the timeout for MAC address table entries, use the **mac-address-table aging-time** command in global configuration mode. To restore the default value of 5 minutes, use the **no** form of this command.

mac-address-tableaging-time*timeout_value*
no mac-address-table aging-time

Syntax Description

timeout_value	The time a MAC address entry stays in the MAC address table before timing out, between 5 and 720 minutes (12 hours). 5 minutes is the default.

Command Default

The default timeout is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

No usage guidelines.

Examples

The following example sets the MAC address timeout to 10 minutes:

```
ciscoasa(config)# mac-address-timeout aging time 10
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.

Command	Description
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

mac-address-table static

To add a static entry to the MAC address table, use the **mac-address-table static** command in global configuration mode. To remove a static entry, use the **no** form of this command. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the ASA drops the traffic and generates a system message.

mac-address-table static *interface_name mac_address*
no mac-address-table static *interface_name mac_address*

Syntax Description

interface_name	The source bridge group member interface.
mac_address	The MAC address you want to add to the table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command in routed mode when using Integrated Routing and Bridging.

Examples

The following example adds a static MAC address entry to the MAC address table:

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.

Command	Description
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

mac-learn disable

To disable MAC address learning for an interface, use the **mac-learn** command in global configuration mode. To reenable MAC address learning, use the **no** form of this command. By default, each interface automatically learns the MAC addresses of entering traffic, and the ASA adds corresponding entries to the MAC address table. You can disable MAC address learning if desired.

mac-learn*interface_name***disable**
no mac-learn *interface_name* **disable**

Syntax Description

interface_name	The bridge group member interface on which you want to disable MAC learning.
disable	Disables MAC learning.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	You can now configure this command in routed mode when using Integrated Routing and Bridging.

Examples

The following example disables MAC learning on the outside interface:

```
ciscoasa(config)# mac-learn outside disable
```

Related Commands

Command	Description
clear configure mac-learn	Sets the **mac-learn** configuration to the default.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

Command	Description
show running-config mac-learn	Shows the **mac-learn** configuration.

mac-learn flood

To enable flooding for unknown MAC addresses for non IPv4/IPv6 packets, use the **mac-learn flood** command in global configuration mode. To disable MAC address flooding, use the **no** form of this command.

mac-learn flood
no mac-learn flood

Command Default

Flooding is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was added.

Examples

The following example enables MAC flooding:

```
ciscoasa(config)# mac-learn flood
```

Related Commands

Command	Description
clear configure mac-learn	Sets the **mac-learn** configuration to the default.
mac-address-table static	Adds static MAC address entries to the MAC address table.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.
show running-config mac-learn	Shows the **mac-learn** configuration.

mac-list

To specify a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization, use the **mac-list** command in global configuration mode. To remove a MAC list entry, use the **no** form of this command.

mac-list *id* { **deny** | **permit** } *mac macmask*
no mac-list *id* { **deny** | **permit** } *mac macmask*

Syntax Description

deny	Indicates that traffic matching this MAC address does not match the MAC list and is subject to both authentication and authorization when specified in the **aaa mac-exempt** command. You might need to add a deny entry to the MAC list if you permit a range of MAC addresses using a MAC address mask such as ffff.ffff.0000, and you want to force a MAC address in that range to be authenticated and authorized.
id	Specifies a hexadecimal MAC access list number. To group a set of MAC addresses, enter the **mac-list** command as many times as needed with the same ID value. The order of entries matters, because the packet uses the first entry it matches, as opposed to a best match scenario. If you have a permit entry, and you want to deny an address that is allowed by the permit entry, be sure to enter the deny entry before the permit entry.
mac	Specifies the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn
macmask	Specifies the portion of the MAC address that should be used for matching. For example, ffff.ffff.ffff matches the MAC address exactly. ffff.ffff.0000 matches only the first 8 digits.
permit	Indicates that traffic matching this MAC address matches the MAC list and is exempt from both authentication and authorization when specified in the **aaa mac-exempt** command.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To enable MAC address exemption from authentication and authorization, use the **aaa mac-exempt** command. You can only add one instance of the **aaa mac-exempt** command, so be sure that your MAC list includes all

the MAC addresses you want to exempt. You can create multiple MAC lists, but you can only use one at a time.

Examples

The following example bypasses authentication for a single MAC address:

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2. Enter the deny statement before the permit statement, because 00a0.c95d.02b2 matches the permit statement as well, and if it is first, the deny statement will never be matched.

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
clear configure mac-list	Removes a list of MAC addresses previously specified by the **mac-list** command.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.

mail-relay

To configure a local domain name, use the **mail-relay** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mail-relay domain_name action { **drop-connection** | **log** }
no mail-relay domain_name action { **drop-connection** | **log** }

Syntax Description

domain_name	Specifies the domain name.
drop-connection	Closes the connection.
log	Generates a system log message.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a mail relay for a specific domain:

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

management-access

To allow management access to an interface other than the one from which you entered the ASA when using VPN, use the **management-access** command in global configuration mode. To disable management access, use the **no** form of this command.

management-access*mgmt_if*
no management-access *mgmt_if*

Syntax Description

mgmt_if	Specifies the name of the management interface you want to access when entering the ASA from another interface. A physical or virtual interface can be specified.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.9.(2)	Virtual interfaces can now be specified.
9.14(1)	SNMP is no longer supported.
9.17(1)	If you use the CiscoSSH stack (the **ssh stack ciscossh** command), then this feature is not supported for SSH.

Usage Guidelines

This command allows you to connect to an interface other than the one you entered the ASA from when using a full tunnel IPsec VPN or SSL VPN client (AnyConnect 2.x client, SVC 1.x) or across a site-to-site IPsec tunnel. You can use Telnet, SSH, Ping, or ASDM to connect to an ASA interface. You can also use a management access interface as the source interface for syslog messages sent through the VPN tunnel.

You can define only one management-access interface.

In 9.5(1) and later, due to routing considerations with the separate management and data routing tables, the VPN termination interface and the management access interface need to be the same type: both need to be management-only interfaces or regular data interfaces. Therefore, do not configure management-access on a management-only interface except in the rare instance that the VPN termination interface is management-only.

If you use the CiscoSSH stack (the **ssh stack ciscossh** command), then this feature is not supported for SSH.

This feature is not supported for SNMP in 9.14(1) and later. For SNMP over VPN, we recommend enabling SNMP on a loopback interface in 9.18(2) and later. You don't need the management-access feature enabled to use SNMP on the loopback interface. Loopback also works for SSH.

When using identity NAT between the management-access interface network and VPN networks (a common NAT configuration for VPN traffic), you must specify the **nat** command **route-lookup** keyword. Without route lookup, the ASA sends traffic out the interface specified in the **nat** command, regardless of what the routing table says. For example, you configure **management-access inside**, so a VPN user entering on the outside can manage the inside interface. If the identity **nat** command specifies **(inside,outside)**, then you do not want the ASA to send the management traffic out to the inside network; it will never return to the inside interface IP address. The route lookup option lets the ASA send the traffic directly to the inside interface IP address instead of to the inside network. For traffic from the VPN client to a host on the inside network, the route lookup option will still result in the correct egress interface (inside), so normal traffic flow is not affected.

Examples

The following example shows how to configure a firewall interface named inside as the management access interface:

```
ciscoasa(config)# management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the ASA.
show management-access	Displays the name of the internal interface configured for management access.

management-only

To set an interface to accept management traffic only, use the **management-only** command in interface configuration mode. To allow through traffic, use the **no** form of this command.

management-only [**individual**]
no management-only [**individual**]

Syntax Description

individual	For the Firepower 9300 ASA security module cluster, you must specify the **individual** keyword for a management interface when in Spanned interface mode.

Command Default

The Management *n* /*n* interface, if available for your model, is set to management-only mode by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	The placement of this command in the running configuration has been moved to the top of the interface section to support ASA clustering, which has special exemptions for management interfaces.
9.4(1.152)	The **individual** keyword was added.

Usage Guidelines

Most models include a dedicated management interface called Management *n* /*n* , which is meant to support traffic to the ASA. However, you can configure any interface to be a management-only interface using the **management-only** command.

Note For all models except the ASA 5585-X, you cannot disable management-only mode for the Management interface. By default, this command is always enabled.

In transparent firewall mode, in addition to the maximum allowed through-traffic interfaces, you can also use the Management interface (either the physical interface, a subinterface (if supported for your model), or an EtherChannel interface comprised of Management interfaces (if you have multiple Management interfaces)) as a separate management interface. You cannot use any other interface types as management interfaces.

If your model does not include a Management interface, you must manage the transparent firewall from a data interface.

In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. Note that except for the ASA 5585-X, the management interface does not allow subinterfaces, so for per-context management, you must connect to a data interface.

The management interface is not part of a normal bridge group. Note that for operational purposes, it is part of a non-configurable bridge group.

Examples

The following example disables management-only mode on the Management interface:

```
ciscoasa(config)# interface management0/0
ciscoasa(config-if)# no management-only
```

The following example enables management-only mode on a subinterface:

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# management-only
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

map-domain

To configure a Mapping Address and Port (MAP) domain, use the **map-domain** command in global configuration mode. Use the **no** form of this command to delete the MAP domain.

map-domain*name*
no map-domain *name*

Syntax Description

name	The name of the MAP domain, which is an alphanumeric string up to 48 characters. The name can also include the following special characters: period (.), slash (/), and colon (:).

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

Mapping Address and Port (MAP) is primarily a feature for use in service provider (SP) networks. The service provider can operate an IPv6-only network, the MAP domain, while supporting IPv4-only subscribers and their need to communicate with IPv4-only sites on the public Internet. MAP is defined in RFC7597, RFC7598, and RFC7599.

For the service provider, within the MAP domain, the benefit of MAP over NAT46 is that the substitution of an IPv6 address for the subscriber's IPv4 address (and back again to IPv4 at the SP network edge) is stateless. This provides greater efficiency within the SP network compared to NAT46.

There are two MAP techniques, MAP-Translation (MAP-T) and MAP-Encapsulation (MAP-E). The ASA supports MAP-T; MAP-E is not supported.

To configure MAP-T, you create one or more domains. When you configure MAP-T on customer edge (CE) and border relay (BR) devices, ensure that you use the same parameters for each device that will participate in each domain.

You can configure up to 25 MAP-T domains. In multiple-context mode, you can configure up to 25 domains per context.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

map-name

To map a user-defined attribute name to a Cisco attribute name, use the **map-name** command in ldap-attribute-map configuration mode.

To remove this mapping, use the **no** form of this command.

map-name *user-attribute-name Cisco-attribute-name*
no map-name *user-attribute-name Cisco-attribute-name*

Syntax Description

user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute.
Cisco-attribute-name	Specifies the Cisco attribute name that you are mapping to the user-defined name.

Command Default

By default, no name mappings exist.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ldap-attribute-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

With the **map-name** command, you can map your own attribute names to Cisco attribute names. You can then bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map configuration mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map configuration mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example commands map a user-defined attribute name Hours to the Cisco attribute name cVPN3000-Access-Hours in the LDAP attribute map myldapmap:

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
ciscoasa(config-ldap-attribute-map)#
```

Within ldap-attribute-map configuration mode, you can enter "?" to display the complete list of Cisco LDAP attribute names:

```
ciscoasa(config-ldap-attribute-map)# map-name <name>
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
 :
 :
  cVPN3000-X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

mapping-service (Deprecated)

To configure a mapping service for the Cisco Intercompany Media Engine proxy, use the **mapping-service** command in UC-IME configuration mode. To remove the mapping service from the proxy, use the **no** form of this command.

mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*
no mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

Syntax Description

interface	Specifies the name of the interface to be used for the listening interface or uc-ime interface.
listening-interface	Configures the interface on which the ASA listens for the mapping requests.
listening-port	(Optional) Configures the listening port for the mapping service.
port	(Optional) Specifies the TCP port number on which the ASA listens for the mapping requests. The port number must be 1024 or higher to avoid conflicts with other services on the device, such as Telnet or SSH. By default, the port number is TCP 8060.
uc-ime-interface	Configures the interface that connects to the remote Cisco UCM.

Command Default

By default the mapping-service for off-path deployments of the Cisco Intercompany Media Engine proxy listens on TCP port 8060.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
UC-IME configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.
9.4(1)	This command was deprecated along with all **uc-ime** mode commands.

Usage Guidelines

For an off-path deployment of the Cisco Intercompany Media Engine proxy on the ASA, adds the mapping service to the proxy configuration. To configure the mapping service, you must specify the outside interface (remote enterprise side) on which to listen for mapping requests and the interface that connects to the remote Cisco UCM.

Note You can only configure one mapping server for the Cisco Intercompany Media Engine proxy.

You configure the mapping service when the Cisco Intercompany Media Engine proxy is configured for an off-path deployment.

In an off path deployment, inbound and outbound Cisco Intercompany Media Engine calls pass through an adaptive security appliance enabled with the Cisco Intercompany Media Engine proxy. The adaptive security appliance is located in the DMZ and configured to support primarily Cisco Intercompany Media Engine. Normal Internet-facing traffic does not flow through this ASA.

For all inbound calls, the signaling is directed to the ASA because destined Cisco UCMs are configured with the global IP address on the ASA. For outbound calls, the called party could be any IP address on the Internet; therefore, the ASA is configured with a mapping service that dynamically provides an internal IP address on the ASA for each global IP address of the called party on the Internet.

Cisco UCM sends all outbound calls directly to the mapped internal IP address on the adaptive security appliance instead of the global IP address of the called party on the Internet. The ASA then forwards the calls to the global IP address of the called party.

Examples

The following example shows ...:

```
ciscoasa
(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
uc-ime-interface outside
```

Related Commands

Command	Description
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
show uc-ime	Displays statistical or detailed information about fallback-notifications, mapping-service-sessions, and signaling-sessions.
uc-ime	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

map-value

To map a user-defined value to a Cisco LDAP value, use the **map-value** command in ldap-attribute-map configuration mode. To delete an entry within a map, use the **no** form of this command.

map-value *user-attribute-name user-value-string Cisco-value-string*
no map-value *user-attribute-name user-value-string Cisco-value-string*

Syntax Description

Cisco-value-string	Specifies the Cisco value string for the Cisco attribute.
user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute name.
user-value-string	Specifies the user-defined value string that you are mapping to the Cisco attribute value.

Command Default

By default, there are no user-defined values mapped to Cisco attributes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ldap-attribute-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

With the **map-value** command, you can map your own attribute values to Cisco attribute names and values. You can then bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map configuration mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map configuration mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example, entered in ldap-attribute-map configuration mode, sets the user-defined value of the user attribute Hours to a user-defined time policy named workDay and a Cisco-defined time policy named Daytime:

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP maps.

mask

When using the Modular Policy Framework, mask out part of the packet that matches a **match** command or class map by using the **mask** command in match or class configuration mode. This mask action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. For example, you can you use **mask** command for the DNS application inspection to mask a header flag before allowing the traffic through the ASA. To disable this action, use the no form of this command.

mask [**log**]
no mask [**log**]

Syntax Description

log	Logs the match. The system log message number depends on the application.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **mask** command to mask part of the packet that matches the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

Examples

The following example masks the RD and RA flags in the DNS header before allowing the traffic through the ASA:

```
ciscoasa(config-cmap)# policy-map type inspect dns dns-map1
ciscoasa(config-pmap-c)# match header-flag RD
ciscoasa(config-pmap-c)# mask log
```

```
ciscoasa(config-pmap-c)# match header-flag RA
ciscoasa(config-pmap-c)# mask log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

mask-banner

To obfuscate the server banner, use the **mask-banner** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mask-banner
no mask-banner

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to mask the server banner:

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

mask-syst-reply

To hide the FTP server response from clients, use the **mask-syst-reply** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the no form of this command.

mask-syst-reply
no mask-syst-reply

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
FTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the mask-syst-reply command with strict FTP inspection to protect the FTP server system from clients. After enabling this command, the servers replies to the **syst** command are replaced by a series of Xs.

Examples

The following example causes the ASA to replace the FTP server replies to the syst command with Xs:

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

Commands	Description
request-command deny	Specifies FTP commands to disallow.

match access-list

When using the Modular Policy Framework, use an access list to identify traffic to which you want to apply actions by using the **match access-list** command in class-map configuration mode. To remove the **match access-list** command, use the **no** form of this command.

match access-list *access_list_name*
no match access-list *access_list_name*

Syntax Description

access_list_name	Specifies the name of an access list to be used as match criteria.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

After you enter the **class-map** command, you can enter the **match access-list** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You can only include one **match access-list** command in the class map, and you cannot combine it with other types of **match** commands. The exception is if you define the **matchdefault-inspection-traffic** command which matches the default TCP and UDP ports used by all applications that the ASA can inspect, then you can narrow the traffic to match using a **match access-list** command. Because the **match default-inspection-traffic** command specifies the ports to match, any ports in the access list are ignored.

1. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
2. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
3. Activate the actions on an interface using the **service-policy** command.

Examples

The following example creates three Layer 3/4 class maps that match three access lists:

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp
ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp
ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match any

When using the Modular Policy Framework, match all traffic to which you want to apply actions by using the **match any** command in class-map configuration mode. To remove the **match any** command, use the **no** form of this command.

match any
no match any

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

After you enter the **class-map** command, you can enter the **match any** command to identify all traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You cannot combine the **match any** command with other types of **match** commands.

1. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
2. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
3. Activate the actions on an interface using the **service-policy** command.

Examples

This example shows how to define a traffic class using a class map and the **match any** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 any
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match apn

To configure a match condition for an access point name in GTP messages, use the **match apn** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **apn regex** { *regex_name* | **class** *regex_class_name* }
no match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for an access point name in an GTP inspection policy map:

```
ciscoasa(config-pmap)# match apn class gtp_regex_apn
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.

match application-id

To configure a match condition for the Diameter application identifier of Diameter messages, use the **match application-id** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **application-id** *app_id* [*app_id_2*]
no match [**not**] **application-id** *app_id* [*app_id_2*]

Syntax Description

app_id	The Diameter application name or number (0-4294967295). If there is a range of consecutively-numbered applications that you want to match, you can include a second ID. You can define the range by application name or number, and it applies to all the numbers between the first and second IDs.

Command Default

Diameter inspection allows all applications.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in a Diameter inspection class map or policy map. Use it to filter traffic based on Diameter application ID. You can then drop the packet, drop the connection, or log matching traffic.

These applications are registered with the IANA. Following are the core supported applications, but you can filter on other applications. Use the CLI help for a list of application names.

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0). This is the base Diameter protocol.

The IETF has a list of registered applications, command codes, and attribute-value pairs at http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml , although Diameter inspection does not support all listed items. See the 3GPP web site for their technical specifications.

Examples

The following example shows how to configure a match condition for the 3gpp-s6a and 3gpp-s13 application IDs.

```
ciscoasa(config)# class-map type inspect diameter match-any log_app

ciscoasa(config-cmap)# match application-id 3gpp-s6a

ciscoasa(config-cmap)# match application-id 3gpp-s13
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
inspect diameter	Enables Diameter inspection.
policy-map type inspect	Creates an inspection policy map.

match as-path

To match a BGP autonomous system path access list, use the match as-path command in route-map configuration mode. To remove a path list entry, use the no form of this command.

match as-path *path-list-number*
no match as-path *path-list-number*

Syntax Description

path-list-number	Autonomous system path access list number.

Command Default

No path lists are defined.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The values set by the match as-path and set weight commands override global values. For example, the weights assigned with the match as-path and set weight route-map configuration commands override the weight assigned using the neighbor weight command.

A route map can have several parts. Any route that does not match at least one match clause relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified. It can accept more than one path-list-name.

Examples

The following example sets the autonomous system path to match BGP autonomous system path access list as-path-acl:

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

Related Commands

Command	Description
set-weight	Specifies the BGP weight for the routing table.
neighbor-weight	Assigns a weight to a neighbor connection.

match avp

To configure a match condition for a Diameter attribute-value pair (AVP) in Diameter messages, use the **match avp** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

To match AVP by attribute only:

match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]
no match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]

To match an AVP based on the value of the attribute:

match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*
no match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*

Syntax Description

code	The name or number (1-4294967295) of an attribute-value pair. For the first code, you can specify the name of a custom AVP or one that is registered in RFCs or 3GPP technical specifications and is directly supported in the software. If you want to match a range of AVP, specify the second code by number only. If you want to match an AVP by its value, you cannot specify a second code. See the CLI help for a list of AVP names.
value	The value portion of the AVP. You can configure this only if the data type of the AVP is supported. For example, you can specify an IP address for AVP that have the address data type. For detailed information on how to configure this parameter, see the Usage section below.
vendor-id *id_number*	(Optional.) The ID number of the vendor to also match, from 0-4294967295. For example, the 3GPP vendor ID is 10415, the IETF is 0.

Command Default

Diameter inspection allows all AVP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in a Diameter inspection class map or policy map. Use it to filter traffic based on Diameter AVP. You can then drop the packet, drop the connection, or log matching traffic.

Use the CLI help for a list of AVP names. The IETF has a list of registered applications, command codes, and attribute-value pairs at https://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml , although Diameter inspection does not support all listed items. See the 3GPP web site for their technical specifications.

If you are configuring a value match, following are the specific syntax of the value option for the supported data types:

- Diameter Identity, Diameter URI, Octet String—Use regular expression or regular expression class objects to match these data types.

{**regex** *regex_name* | **class** *regex_class*}

- Address—Specify the IPv4 or IPv6 address to match. For example, 10.100.10.10 or 2001:DB8::0DB8:800:200C:417A.
- Time—Specify the start and end dates and time. Both are required. Time is in 24-hour format.

date *year month day* **time** *hh*:*mm*:*ss* **date** *year month day* **time** *hh*:*mm*:*ss*

For example:

date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00

- Numeric—Specify a range of numbers:

range *number_1 number_2*

The valid number range depends on the data type:

- Integer32: -2147483647 to 2147483647
- Integer64: -9223372036854775807 to 9223372036854775807
- Unsigned32: 0 to 4294967295
- Unsigned64: 0 to 18446744073709551615
- Float32: decimal point representation with 8 digit precision
- Float64: decimal point representation with 16 digit precision

Examples

The following example shows how to configure a match condition for a specific IP address that appears on the host-ip-address AVP on Capability Exchange Request/Answer command messages.

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.

Command	Description
diameter	Creates custom attribute-value pairs.
inspect diameter	Enables Diameter inspection.
policy-map type inspect	Creates an inspection policy map.

match body

To configure a match condition on the length or length of a line of an ESMTP body message, use the **match body** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **body** [**length** | **line length**] **gt** *bytes*
no match [**not**] **body** [**length** | **line length**] **gt** *bytes*

Syntax Description

length	Specifies the length of an ESMTP body message.
line length	Specifies the length of a line of an ESMTP body message.
bytes	Specifies the number to match in bytes.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for a body line length in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match body line length gt 1000**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.

Command	Description
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match called-party

To configure a match condition on the H.323 called party, use the **match called-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **called-party** [**regex** *regex*]
no match [**not**] **match** [**not**] **called-party** [**regex** *regex*]

Syntax Description

regex regex	Specifies to match on the regular expression.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for the called party in an H.323 inspection class map:

```
ciscoasa(config-cmap)# match called-party regex caller1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match calling-party

To configure a match condition on the H.323 calling party, use the **match calling-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **calling-party** [**regex** *regex*]
no match [**not**] **match** [**not**] **calling-party** [**regex** *regex*]

Syntax Description

regex regex	Specifies to match on the regular expression.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for the calling party in an H.323 inspection class map:

```
ciscoasa(config-cmap)# match calling-party regex caller1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match certificate

To configure a certificate match rule, use the **match certificate** command in crypto ca trustpoint configuration mode. To remove the rule from the configuration, use the **no** form of this command.

match certificate *map-name* [**override ocsp** [**trustpoint** *trustpoint-name*] *seq-num* **url** *URL* | **override cdp** *seq-num* **url** *URL*]
no match certificate *map-name* [**override ocsp** [*seq-num* **url** *URL*] | **override cdp** [*seq-num* **url** *URL*]]

Syntax Description

map-name	Specifies the name of the certificate map to match to this rule. You must configure the certificate map before configuring a match rule. The maximum length is 65 characters.
override ocsp	Specifies that the purpose of the rule is to override an OCSP URL in a certificate.
seq-num	Sets the priority for this match rule. The valid range is from 1 to 10000. The ASA evaluates the match rule with the lowest sequence number first, followed by higher numbers until it finds a match.
trustpoint	(Optional) Specifies using a trustpoint for verifying the OCSP responder certificate.
trustpoint-name	(Optional) Identifies the trustpoint to use with the override to validate responder certificates.
url	Specifies accessing a URL for OCSP revocation status.
URL	Identifies the URL to access for OCSP revocation status.
override cdp	Specifies that the purpose of the rule is to override a CRL URL in a certificate.
seq-num	Sets the rank of each URL in the list. Specifies a value from 1 to 5. The ASA tries the URL at lowest rank (1) first.
url	Specifies accessing a URL for CRL revocation status.
URL	The URL to access the CRL revocation status.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Provision to configure cdp override was added.
9.15(1)	Prior to this release, static CDPs can be mapped uniquely to each certificate in a chain that is being validated. However, only one such mapping was supported for each certificate. From this release, the match certificate cdp override command accepts multiple instances for the same map name.

Usage Guidelines

During the PKI certificate validation process, the ASA checks certificate revocation status to maintain security by using either CRL checking or Online Certificate Status Protocol (OCSP). With CRL checking, the ASA retrieves, parses, and caches CRLs, which provide a complete list of revoked certificates. OCSP offers a more scalable method of checking revocation status because OCSP localizes certificate status on a validation authority, which it queries for the status of a specific certificate.

Certificate match rules let you configure OCSP URL overrides, which specify a URL to check for revocation status, rather than the URL in the AIA field of the remote user certificate. Match rules also let you configure trustpoints to use to validate OCSP responder certificates, which let the ASA validate responder certificates from any CA, including self-signed certificates and certificates external to the validation path of the client certificate.

Similar to OCSP, you can use the **match certificate** command to configure CDP URL overrides. This command supports the identification of static CDP URLs through the certificate map. For each certificate that needs CRL validation, CRLs are retrieved based on the CDP extension in the certificate and any URLs that are mapped in this configuration. The **policy** command in the **config-ca-crl** submode can be used to exclude the CDPs from the certificate or the static CDPs.

You can now configure multiple static CDPs to a single map. To remove individual instances, in the **no** form of the command, specify the URL and sequence numbers. Ensure that the specified URL and sequence numbers are the same values that you had configured. If you are not mentioning any specific information, all the entries for the map will be removed. The provision to have or to remove multiple instances for a map is not applicable for OCSP.

When configuring OCSP, be aware of the following requirements:

- You can configure multiple match rules within a trustpoint configuration, but you can have only one match rule for each crypto ca certificate map. You can, however, configure multiple crypto ca certificate maps and associate them with the same trustpoint.
- You must configure the certificate map before configuring a match rule.
- To configure a trustpoint to validate a self-signed OCSP responder certificates, you import the self-signed responder certificate into its own trustpoint as a trusted CA certificate. Then you configure the **match certificate** command in the client certificate validating trustpoint to use the trustpoint that contains the self-signed OCSP responder certificate to validate the responder certificate. The same applies for validating responder certificates external to the validation path of the client certificate.
- A trustpoint can validate both the client certificate and the responder certificate if the same CA issues both of them. But if different CAs issue the client and responder certificates, you need to configure two trustpoints, one trustpoint for each certificate.
- The OCSP server (responder) certificate typically signs the OCSP response. After receiving the response, the ASA tries to verify the responder certificate. The CA normally sets the lifetime of its OCSP responder

certificate to a relatively short period to minimize the chance of it being compromised.The CA typically also includes an ocsp-no-check extension in the responder certificate indicating that this certificate does not need revocation status checking. But if this extension is not present, the ASA tries to check its revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fails. To avoid this possibility, use the **revocation-check none** command when configuring the responder certificate validating trustpoint, and use the **revocation-check ocsp** command when configuring the client certificate.

- If the ASA does not find a match, it uses the URL specified in the **ocsp url** command. If you have not configured the **ocsp url** command, the ASA uses the AIA field of the remote user certificate. If the certificate does not have an AIA extension, revocation status checking fails.

Examples

The following example shows how to create a certificate match rule for a trustpoint called newtrust. The rule has a map name called mymap, a sequence number of 4, a trustpoint called mytrust, and specifies a URL of 10.22.184.22.

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
 url 10.22.184.22
ciscoasa(config-ca-trustpoint)#
```

The following example shows how to configure a crypto ca certificate map, and then a match certificate rule to identify a trustpoint that contains a CA certificate to validate the responder certificate. This certificate is necessary if the CA identified in the newtrust trustpoint does not issue an OCSP responder certificate.

1. Configure the certificate map that identifies the client certificates to which the map rule applies. In this example, the name of the certificate map is mymap and the sequence number is 1. Any client certificate with a subject-name that contains a CN attribute equal to mycert matches the mymap entry.

   ```
   ciscoasa(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
   ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
   ciscoasa(config-ca-cert-map)#
   ```

2. Configure a trustpoint that contains the CA certificate to use to validate the OCSP responder certificate. In the case of self-signed certificates, this is the self-signed certificate itself, which is imported and locally trusted. You can also obtain a certificate for this purpose through external CA enrollment. When prompted to do so, paste in the CA certificate.

   ```
   ciscoasa(config-ca-cert-map)# exit
   ciscoasa(config)# crypto ca trustpoint mytrust
   ciscoasa(config-ca-trustpoint)# enroll terminal
   ciscoasa(config-ca-trustpoint)# crypto ca authenticate mytrust
   Enter the base 64 encoded CA certificate.
   End with the word "quit" on a line by itself

   MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
   NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
   AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
   7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
   v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
   ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
   gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
   tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
   e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
   quit
   ```

```
INFO: Certificate has the following attributes:
Fingerprint: 7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

3. Configure the original trustpoint, newtrust, with OCSP as the revocation checking method. Then set a match rule that includes the certificate map, mymap, and the self-signed trustpoint, mytrust, configured in Step 2.

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint: 9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust
 4 url 10.22.184.22
```

Any connection that uses the newtrust trustpoint for client certificate authentication checks to see if the client certificate matches the attribute rules specified in the mymap certificate map. If so, the ASA accesses the OCSP responder at 10.22.184.22 for certificate revocation status, then uses the mytrust trustpoint to validate the responder certificate.

Note The newtrust trustpoint is configured to perform revocation checking via OCSP for the client certificates. However, the mytrust trustpoint is configured for the default revocation-check method, which is none. As a result, no revocation checking is performed on the OCSP responder certificate.

The following example shows configuring a match certificate rule using CDP. The rule has a map name called test, with 1, 2, and 3 as sequence numbers, and static URLs. While selecting CDPs for a certificate, ASA selects the 3 CDPs for any certificate that matches the certificate map named *test*. If the ASA determines that a CRL is needed while validating the certificate, the URLs are tried in the given sequence until a CRL is successfully retrieved.

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 1 url http://1.1.1.1
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 2 url http://1.1.1.2
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 3 url http://1.1.1.3
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca certificate map	Creates crypto ca certificate maps. Use this command in global configuration mode.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode. Use this command in global configuration mode.
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
revocation-check	Specifies the method(s) to use for revocation checking and the order in which to try them.

match certificate allow expired-certificate (deprecated)

To allow an administrator to exempt certain certificates from expiration checking, use the **match certificate allow expired-certificate** command in ca-trustpool configuration mode. To disable the exemption of certain certificates, use the **no** form of this command.

match certificate < **map** > **allow expired-certificate**
no match certificate < **map** > **allow expired-certificate**

Syntax Description

allow	Allows expired certificate to be accepted.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpool configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.13(1)	This command was removed.

Usage Guidelines

The trustpool match commands leverage the certificate map objects to configure certificate specific exceptions or overrides to the global trustpool policy. The match rules are written relative to the certificate that is being validated.

Related Commands

Command	Description
match certificate skip revocation check	Exempts certain certificates from revocation checking.

match certificate skip revocation-check

To allow an administrator to exempt certain certificates from revocation checking, use the **match certificate skip revocation-check** command in ca-trustpool configuration mode. To disable the exemption from revocation checking, use the **no** form of this command.

matchcertificatemapskiprevocation-check
nomatchcertificatemapskiprevocation-check

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-trustpool configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The trustpool match commands leverage the certificate map objects to configure certificate specific exceptions or overrides to the global trustpool policy. The match rules are written relative to the certificate that is being validated.

Examples

The following example shows skipping the validity check for the certificate with the Subject DN common name of "mycompany123."

```
crypto ca certificate map mycompany 1subject-name attr cn eq mycompany123
crypto ca trustpool policymatch certificate mycompany skip revocation-check
```

Related Commands

Command	Description
match certificate allow expired-certificate	Exempts certain certificates from expiration checking.

match cmd

To configure a match condition on the ESMTP command verb, use the **match cmd** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]
no match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

Syntax Description

verb verb	Specifies the ESMTP command verb.
line length gt bytes	Specifies the length of a line.
RCPT count gt recipients_number	Specifies the number of recipient email addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition in an ESMTP inspection policy map for the verb (method) NOOP exchanged in the ESMTP transaction:

```
ciscoasa(config-pmap)# match cmd verb NOOP
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match command-code

To configure a match condition for the Diameter command code of Diameter messages, use the **match command-code** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **command-code** *code* [*code_2*]
no match [**not**] **command-code** *code* [*code_2*]

Syntax Description

code The Diameter command code name or number (0-4294967295). If there is a range of consecutively-numbered command codes that you want to match, you can include a second code. You can define the range by command code name or number, and it applies to all the numbers between the first and second codes. See the CLI help for a list of command code names.

Command Default

Diameter inspection allows all command codes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in a Diameter inspection class map or policy map. Use it to filter traffic based on Diameter command code. You can then drop the packet, drop the connection, or log matching traffic.

The IETF has a list of registered applications, command codes, and attribute-value pairs athttp://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml , although Diameter inspection does not support all listed items. See the 3GPP web site for their technical specifications.

Examples

The following example shows how to configure a match condition for a specific IP address that appears on the host-ip-address AVP on Capability Exchange Request/Answer command messages.

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip

ciscoasa(config-cmap)# match command-code cer-cea

ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
inspect diameter	Enables Diameter inspection.
policy-map type inspect	Creates an inspection policy map.

match community

To match a Border Gateway Protocol (BGP) community, use the match community command in route-map configuration mode. To remove the match community command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the no form of this command.

match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }
no match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }

Syntax Description

standard-list-number	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.
expanded-list-number	Specifies an expanded community list number from 100 to 500 that identifies one or more permit or deny groups of communities
community-list-name	The community list name.
exact	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.

Command Default

No community list is matched by the route map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

A route map can have several parts. Any route that does not match at least one match command relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Matching based on community list number is one of the types of match commands applicable to BGP.

Examples

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)#  match community 1
ciscoasa(config-route-map)# set weight 100
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

In the following example, the routes that match community list LIST_NAME will have the weight set to 100. Any route that has community 101 alone will have the weight set to 100.

```
ciscoasa(config)#  community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

The following example shows that the routes that match expanded community list 500. Any route that has extended community 1 will have the weight set to 150.

```
ciscoasa(config)#  community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

Related Commands

Command	Description
set-weight	Specifies the BGP weight for the routing table.
community-list	Creates or configures a BGP community list.

match default-inspection-traffic

To specify default traffic for the inspect commands in a class map, use the **match default-inspection-traffic** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchdefault-inspection-traffic
nomatchdefault-inspection-traffic

Syntax Description

This command has no arguments or keywords.

Command Default

See the Usage Guidelines section for the default traffic of each inspection.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.6(2)	TCP/53 was added for DNS over TCP inspection, which is not enabled by default. Default ports for M3UA and STUN were also added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Using the **match default-inspection-traffic** command, you can match default traffic for the individual **inspect** commands. The **match default-inspection-traffic** command can be used in conjunction with one other match command, which is typically an access-list in the form of **permit ip** *src-ip dst-ip* .

The rule for combining a second **match** command with the **match default-inspection-traffic** command is to specify the protocol and port information using the **match default-inspection-traffic** command and specify all other information (such as IP addresses) using the second **match** command. Any protocol or port information specified in the second **match** command is ignored with respect to the **inspect** commands.

For instance, port 65535 specified in the example below is ignored:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 default-inspection-traffic
ciscoasa(config-cmap)# match port 65535
```

Default traffic for inspections are as follows:

Inspection Type	Protocol Type	Source Port	Destination Port
ctiqbe	tcp	N/A	2748
dcerpc	tcp	N/A	135
diameter	tcp, sctp	N/A	3868
dns	udp, tcp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
im	tcp	N/A	1-65539
ip-options	rsvp	N/A	N/A
ipsec-pass-thru	udp	N/A	500
m3ua	sctp	N/A	2905
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
radius-accounting	udp	N/A	1646
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sctp	sctp	any	any
sip	tcp, udp	N/A	5060
skinny	tcp	N/A	2000

smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
stun	tcp, udp	N/A	3478
tftp	udp	N/A	69
waas	tcp	N/A	1-65535
xdmcp	udp	177	177

Examples

The following example shows how to define a traffic class using a class map and the **match default-inspection-traffic** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 default-inspection-traffic
ciscoasa(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match dns-class

To configure a match condition for the Domain System Class in a DNS Resource Record or Question section, use the **match dns-class** command in class-map or policy-map configuration mode. To remove a configured class, use the **no** form of this command.

match [**not**] **dns-class** { **eq** *c_well_known* | *c_val* } { **range** *c_val1 c_val2* }
no match [**not**] **dns-class** { **eq** *c_well_known* | *c_val* } { **range** *c_val1 c_val2* }

Syntax Description

eq	Specifies an exact match.
c_well_known	Specifies DNS class by well-known name, IN.
c_val	Specifies an arbitrary value in the DNS class field (0-65535).
range	Specifies a range.
c_val1 c_val2	Specifies values in a range match. Each value between 0 and 65535.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, this command inspects all fields (questions and RRs) of a DNS message and matches the specified class. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: match not header-flag QR and match question.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS class in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match dns-type

To configure a match condition for a DNS type, including Query type and RR type, use the **match dns-type** command in class-map or policy-map configuration mode. To remove a configured dns type, use the **no** form of this command.

match [**not**] **dns-type** { **eq** *t_well_known* | *t_val* } { **range** *t_val1 t_val2* }
no match [**not**] **dns-type** { **eq** *t_well_known* | *t_val* } { **range** *t_val1 t_val2* }

Syntax Description

eq	Specifies an exact match.
t_well_known	Specifies DNS type by well-known name: A, NS, CNAME, SOA, TSIG, IXFR, or AXFR.
t_val	Specifies an arbitrary value in the DNS type field (0-65535).
range	Specifies a range.
t_val1 t_val2	Specifies values in a range match. Each value between 0 and 65535.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, this command inspects all sections of a DNS message (questions and RRs) and matches the specified type. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: match not header-flag QR and match question.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS type in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match domain-name

To configure a match condition for a DNS message domain name list, use the **match domain-name** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **domain-name regex** *regex_id*
match [**not**] **domain-name regex class** *class_id*
no match [**not**] **domain-name regex** *regex_id*
no match [**not**] **domain-name regex class** *class_id*

Syntax Description

regex	Specifies a regular expression.
regex_id	Specifies the regular expression ID.
class	Specifies the class map that contains multiple regular expression entries.
class_id	Specifies the regular expression class map ID.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command matches domain names in the DNS message against predefined list. Compressed domain names will be expanded before matching. The match condition can be narrowed down to a particular field in conjunction with other DNS match commands.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to match the DNS domain name in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match dpc

To configure a match condition for the destination point code (DPC) of M3UA data messages, use the **match dpc** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **dpc** *code*
no match [**not**] **dpc** *code*

Syntax Description

code	The destination point code in *zone -region -sp* format.

Command Default

M3UA inspection allows all destination point codes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop packets based on the destination point code. Point code is in *zone -region -sp* format, where the possible values for each element depend on the SS7 variant. You define the variant on the **ss7 variant** command in the policy map.

- ITU—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7]. This is the default SS7 variant.
- ANSI—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].
- Japan—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127].
- China—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

Examples

The following example shows how to configure a match condition for a specific destination point code for ITU.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
match opc	Matches the M3UA originating point code.
policy-map type inspect	Creates an inspection policy map.
ss7 variant	Identifies the SS7 variant to use in the policy map.

match dscp

To identify the IETF-defined DSCP value (in an IP header) in a class map, use the **match dscp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match dscp { *values* }
no match dscp { *values* }

Syntax Description

values Specifies up to eight different the IETF-defined DSCP values in the IP header. Range is 0 to 63.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Using the **match dscp** command, you can match the IETF-defined DSCP values in the IP header.

Examples

The following example shows how to define a traffic class using a class map and the **match dscp** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 dscp af43 cs1 ef
ciscoasa(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match port	Specifies the TCP/UDP ports as the comparison criteria for packets received on that interface.
show running-config class-map	Displays the information about the class map configuration.

match e – match q

match ehlo-reply-parameter

To configure a match condition on the ESMTP ehlo reply parameter, use the **match ehlo-reply-parameter** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **ehlo-reply-parameter** *parameter*
no match [**not**] **ehlo-reply-parameter** *parameter*

Syntax Description

parameter	Specifies the ehlo reply parameter.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for an ehlo reply parameter in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match ehlo-reply-parameter auth**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match filename

To configure a match condition for a filename for FTP transfer, use the **match filename** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filename in an FTP inspection class map:

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
ciscoasa(config-cmap)# match username regex class ftp_regex_user
ciscoasa(config-cmap)# match filename regex ftp-file
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match filetype

To configure a match condition for a filetype for FTP transfer, use the **match filetype** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filetype in an FTP inspection policy map:

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match flow ip destination-address

To specify the flow IP destination address in a class map, use the **match flow ip destination-address** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchflowipdestination-address
nomatchflowipdestination-address

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions on a tunnel group, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **match flow ip destination-address** command. Use **match tunnel-group** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
```

```
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for VPN.

match header (policy-map type inspect esmtp)

To configure a match condition on the ESMTP header, use the **match header** command in policy-map type inspect esmtp configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **header** [[**length** | **line length**] **gt** *bytes* | **to-fields count gt** *to_fields_number*]
no match [**not**] **header** [[**length** | **line length**] **gt** *bytes* | **to-fields count gt** *to_fields_number*]

Syntax Description

length gt bytes	Specifies to match on the length of the ESMTP header message.
line length gt bytes	Specifies to match on the length of a line of an ESMTP header message.
to-fields count gt to_fields_number	Specifies to match on the number of To: fields.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map type inspect esmtp configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for a header in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match header length gt 512**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match header (policy-map type inspect ipv6)

To configure a match condition on the IPv6 header, use the **match header** command in policy-map type inspect ipv6 configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }
no match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }

Syntax Description

ah	Matches the IPv6 Authentication extension header
count gt *number*	Specifies the maximum number of IPv6 extension headers, from 0 to 255.
destination-option	Matches the IPv6 destination-option extension header.
esp	Matches the IPv6 Encapsulation Security Payload (ESP) extension header.
fragment	Matches the IPv6 fragment extension header.
hop-by-hop	Matches the IPv6 hop-by-hop extension header.
not	(Optional) Does not match the specified parameter.
routing-address count gt *number*	Sets the maximum number of IPv6 routing header type 0 addresses, greater than a number between 0 and 255.
routing-type {**eq** | **range**} *number*	Matches the IPv6 routing header type, from 0 to 255. For a range, separate values by a space, for example, **30 40**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map type inspect ipv6 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Specifies the headers you want to match. By default, the packet is logged (**log**); if you want to drop (and optionally also log) the packet, enter the **drop** and optional **log** commands in match configuration mode.

Re-enter the **match** command and optional **drop** action for each extension you want to match:

Examples

The following example creates an inspection policy map that will drop and log all IPv6 packets with the hop-by-hop, destination-option, routing-address, and routing type 0 headers:

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match header-flag

To configure a match condition for a DNS header flag, use the **match header-flag** command in class-map or policy-map configuration mode. To remove a configured header flag, use the **no** form of this command.

match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }
no match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }

Syntax Description

eq	Specifies an exact match. If not configured, specifies a match-all bit mask match.
f_well_known	Specifies DNS header flag bits by well-known name. Multiple flag bits may be entered and logically OR'd. QR (Query, note: QR=1, indicating a DNS response) AA (Authoritative Answer) TC (TrunCation) RD (Recursion Desired) RA (Recursion Available)
f_value	Specifies an arbitrary 16-bit value in hexadecimal form.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a DNS class map or policy map. Only one entry can be entered in a DNS class map.

Examples

The following example shows how to configure a match condition for a DNS header flag in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match im-subscriber

To configure a match condition for a SIP IM subscriber, use the **match im-subscriber** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for a SIP IM subscriber in a SIP inspection class map:

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match interface

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. To remove the match interface entry, use the **no** form of this command.

match interface *interface-name*
no match interface *interface-name*

Syntax Description

interface-name	Name of the interface (not the physical interface). Multiple interface names can be specified.

Command Default

No match interfaces are defined.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the interface-type interface-number arguments.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions that are given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria. If there is more than one interface specified in the **match** command. then the **no match interface** interface-name can be used to remove a single interface.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. If you want to modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows that the routes with their next hop outside is distributed:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

Related Commands

Command	Description
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address that is specified by the access lists.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match invalid-recipients

To configure a match condition on the ESMTP invalid recipient address, use the **match invalid-recipients** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **invalid-recipients count gt** *number*
no match [**not**] **invalid-recipients count gt** *number*

Syntax Description

count gt number	Specifies to match on the invalid recipient number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for invalid recipients count in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match invalid-recipients count gt 1000**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match ip address

To redistribute any routes that have a route address or match packet that is passed by one of the access lists specified, use the **match ip address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ip address { *acl_id . . .* | **prefix-list** *prefix_list_id . . .* }
no match ip address { *acl_id . . .* | **prefix-list** *prefix_list_id . . .* }

Syntax Description

acl_id	Specifies the name of an access-list. Multiple access lists can be specified.
prefix-list *prefix_list_id*	Specifies the name of a prefix-list. Multiple prefix lists can be specified. **Note** Not supported for OSPF.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(2)	For OSPF, prefix lists are no longer supported.

Usage Guidelines

The **route-map** command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to redistribute internal routes:

```
ciscoasa(config)# route-map test
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match ipv6 address	Distributes any routes that have an IPv6 route address or match packet that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip next-hop

To redistribute any routes that have a next-hop router address that is passed by one of the access lists specified, use the **match ip next-hop** command in route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*
no match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix-list *prefix_list*	Name of prefix list.

Command Default

Routes are distributed freely, without being required to match a next-hop address.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *acl* argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows how to distribute routes that have a next-hop router address passed by access list acl_dmz1 or acl_dmz2:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip route-source

To redistribute routes that have been advertised by routers and access servers at the address that is specified by the ACLs, use the **match ip route-source** command in the route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip route-source { *acl . . .* } **prefix-list** *prefix_list*
match ip route-source { *acl . . .* }

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix_list	Name of prefix list.

Command Default

No filtering on a route source.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-name argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section

and specify an explicit match. The next-hop and source-router address of the route are not the same in some situations.

Examples

The following example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by ACLs acl_dmz1 and acl_dmz2:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the ACLs specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ipv6 address

To redistribute any routes that have an IPv6 route address or match packet that is passed by one of the access lists specified, use the **match ipv6 address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ipv6 address { *acl . . .* } **prefix-list**
no match ipv6 address { *acl . . .* } **prefix-list**

Syntax Description

acl	Specifies the name of an access list. Multiple access lists can be specified.
prefix-list	Specifies the name of a match prefix list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to redistribute internal routes: access-list acl_dmz1 extended permit ipv6 any <net> <mask>

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,

Command	Description
match ip address	Distributes any routes that have a route address or match packet that is passed by one of the access lists specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match login-name

To configure a match condition for a client login name for instant messaging, use the **match login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for a client login name in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match media-type

To configure a match condition on the H.323 media type, use the **match media-type** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **media-type** [**audio** | **data** | **video**]
no match [**not**] **media-type** [**audio** | **data** | **video**]

Syntax Description

audio	Specifies to match audio media type.
data	Specifies to match data media type.
video	Specifies to match video media type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for audio media type in an H.323 inspection class map:

```
ciscoasa(config-cmap)# match media-type audio
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match message class

To configure a match condition for the message class and type of M3UA messages, use the **match message class** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message class** *class_id* [**id** *message_id*]
no match [**not**] **message class** *class_id* [**id** *message_id*]

Syntax Description

class_id	The message class. See the usage section for a list of supported classes and types.
id *message_id*	The message type within the specified class.

Command Default

M3UA inspection allows all message classes and types without rate limits.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop or rate limit packets based on the message class and type. The following table lists the possible values. Consult M3UA RFCs and documentation for detailed information about these messages.

M3UA Message Class	Message ID Type
0 (Management Messages)	0-1
1 (Transfer Messages)	1
2 (SS7 Signaling Network Management Messages)	1-6
3 (ASP State Maintenance Messages)	1-6
4 (ASP Traffic Maintenance Messages)	1-4
9 (Routing Key Management Messages)	1-4

Examples

The following example shows how to configure a match condition for M3UA messages.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match message class 2 id 6
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.

match message id

To configure a match condition for a GTP message ID, use the **match message id** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }
no match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }

Syntax Description

{**v1** | **v2**}	(Starting with 9.5(1).) Indicates the GTP version. Use **v1** for GTPv0-1, and **v2** for GTPv2.
message_id	The message ID, which can be 1 to 255.
range *lower_range upper_range*	A range of message IDs. Specify the lower and upper boundaries of the range.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.5(1)	The {**v1** | **v2**} keywords were added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for a message ID in a GTP inspection policy map:

```
ciscoasa(config-pmap)# match message id 33
```

Starting with release 9.5(1), you need to add the {**v1** | **v2**} keyword:

```
ciscoasa(config-pmap)# match message v2 id 33
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.

match message length

To configure a match condition for a GTP message ID, use the **match message length** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message length min** *min_length* **max** *max_length*
no match [**not**] **message length min** *min_length* **max** *max_length*

Syntax Description

min *min_length*	Specifies a minimum message ID length. Value is between 1 and 65536.
max *max_length*	Specifies a maximum message ID length. Value is between 1 and 65536.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for a message length in a GTP inspection policy map:

```
ciscoasa(config-pmap)# match message length min 8 max 200
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.
match message id	Matches traffic based on message ID.

match message-path

To configure a match condition for the path taken by a SIP message as specified in the Via header field, use the **match message-path** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match metric

To redistribute routes with the metric specified, use the **match metric** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match metric *number*
no match metric *number*

Syntax Description

number	Route metric, which can be an IGRP five-part metric; valid values are from 0 to 4294967295.

Command Default

No filtering on a metric value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows how to redistribute routes with the metric 5:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match mime

To configure a match condition on the ESMTP mime encoding type, mime filename length, or mime file type, use the **match mime** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]
no match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]

Syntax Description

encoding type	Specifies to match on the encoding type.
filename length gt bytes	Specifies to match on the filename length.
filetype regex	Specifies to match on the file type.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for a mime filename length in an ESMTP inspection policy map:

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match mime filename length gt 255**

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match msisdn

To configure a match condition for a GTP Mobile Station International Subscriber Directory Number (MSISDN) information element in the Create PDP Context request, Create Session request, and Modify Bearer Response messages, use the **match msisdn** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }
no match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }

Syntax Description

regex_name	The name of a regular expression object.
class *class_name*	The name of a regular expression class.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP policy map.

You can filter on the Mobile Station International Subscriber Directory Number (MSISDN) information element in the Create PDP Context request. You can drop and optionally log messages based on a specific MSISDN, or on a range of MSISDNs based on the first x number of digits. You use a regular expression to specify the MSISDN. MSISDN filtering is supported for GTPv1 and GTPv2 only.

Examples

The following example shows how to configure an MSISDN match condition using a regular expression object.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match msisdn regex msisdn1
ciscoasa(config-pmap-c)# drop log
```

The following example shows how to configure an MSISDN match condition using a regular expression class.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# match msisdn regex class msisdn2

ciscoasa(config-pmap-c)# drop log
```

Related Commands

Command	Description
drop	Drop packets that match the criteria.
log	Log packets that match the criteria.
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.

match opc

To configure a match condition for the originating point code (OPC) of M3UA data messages, use the **match opc** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **opc** *code*
no match [**not**] **opc** *code*

Syntax Description

code	The originating point code in *zone -region -sp* format.

Command Default

M3UA inspection allows all originating point codes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop packets based on the originating point code. Point code is in *zone -region -sp* format, where the possible values for each element depend on the SS7 variant. You define the variant on the **ss7 variant** command in the policy map.

- ITU—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7]. This is the default SS7 variant.
- ANSI—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].
- Japan—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127].
- China—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

Examples

The following example shows how to configure a match condition for a specific originating point code for ITU.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match opc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
match dpc	Matches the M3UA destination point code.
policy-map type inspect	Creates an inspection policy map.
ss7 variant	Identifies the SS7 variant to use in the policy map.

match peer-ip-address

To configure a match condition for the peer IP address for instant messaging, use the **match peer-ip-address** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-ip-address** *ip_address ip_address_mask*
no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

Syntax Description

ip_address	Specifies a hostname or IP address of the client or server.
ip_address_mask	Specifies the netmask for the client or server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer IP address in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match peer-login-name

To configure a match condition for the peer login name for instant messaging, use the **match peer-login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class regex_class_name	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer login name in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
show running-config class-map	Displays the information about the class map configuration.

match port

When using the Modular Policy Framework, match the ports to which you want to apply actions by using the **match port** command in class-map configuration mode. To remove the **match port** command, use the **no** form of this command.

match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }
no match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }

Syntax Description

eq *port*	Specifies a single port name or number.
range *beg_port end_port*	Specifies beginning and ending port range values between 1 and 65535.
tcp	Specifies a TCP port.
sctp	Specifies an SCTP port.
udp	Specifies a UDP port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	The **sctp** keyword was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.

After you enter the **class-map** command, you can enter the **match port** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** command (the **class-map type management** command only allows the match port command). You can only include one **match port** command in the class map, and you cannot combine it with other types of **match** commands.

1. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
2. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
3. Activate the actions on an interface using the **service-policy** command.

Examples

The following example shows how to define a traffic class using a class map and the **match port** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match ppid

To configure a match condition for the payload protocol identifier (PPID) for SCTP inspection, use the **match ppid** command in inspection policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **ppid** *ppid_1* [*ppid_2*]
no match [**not**] **ppid** *ppid_1* [*ppid_2*]

Syntax Description

ppid_1 [*ppid_2*]	Specifies an SCTP PPID, either by the PPID number (0-4294967295) or name (see the CLI help for the available names). You can include a second (higher) PPID to specify a range.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Inspection policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in an SCTP inspection policy map. Use it to filter on PPID to apply special actions to those IDs, such as drop, log, or rate limit.

If you decide to filter on PPID, keep the following in mind:

- PPIDs are in data chunks, and a given packet can have multiple data chunks. If a packet includes data chunks with different PPIDs, the packet will not be filtered, and the assigned action will not be applied to the packet.
- If you use PPID filtering to drop or rate-limit packets, be aware that the transmitter will resend any dropped packets. Although a packet for a rate-limited PPID might make it through on the next attempt, a packet for a dropped PPID will again be dropped. You might want to evaluate the eventual consequence of these repeated drops on your network.

Examples

The following example creates an SCTP inspection policy map that will drop unassigned PPIDs (unassigned at the time this example was written), rate limit PPIDs 32-40, and log the Diameter PPID.

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
```

Related Commands

Command	Description
drop	Drops matching traffic.
inspect sctp	Enables SCTP inspection.
log	Logs matching traffic.
policy-map type inspect sctp	Creates an SCTP inspection policy map.
rate-limit	Applies a rate limit to matching traffic.

match precedence

To specify a precedence value in a class map, use the **match precedence** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchprecedence*value*
nomatchprecedence*value*

Syntax Description

value	Specifies up to four precedence values separated by a space. Range is 0 to 7.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match precedence** command to specify the value represented by the TOS byte in the IP header.

Examples

The following example shows how to define a traffic class using a class map and the **match precedence** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 precedence 1
ciscoasa(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match protocol

To configure a match condition for a specific instant messaging protocol, such as MSN or Yahoo, use the **match protocol** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **protocol** { **msn-im** | **yahoo-im** }
no match [**not**] **protocol** { **msn-im** | **yahoo-im** }

Syntax Description

msn-im	Specifies to match the MSN instant messaging protocol.
yahoo-im	Specifies to match the Yahoo instant messaging protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the Yahoo instant messaging protocol in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match protocol yahoo-im
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
show running-config class-map	Displays the information about the class map configuration.

match question

To configure a match condition for a DNS question or resource record, use the **match question** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match { **question** | { **resource-record answer** | **authority** | **additional** } }
no match { **question** | { **resource-record answer** | **authority** | **additional** } }

Syntax Description

question	Specifies the question portion of a DNS message.
resource-record	Specifies the resource record portion of a DNS message.
answer	Specifies the Answer RR section.
authority	Specifies the Authority RR section.
additional	Specifies the Additional RR section.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, this command inspects the DNS header and matches the specified field. It can be used in conjunction with other DNS match commands to define inspection of a particular question or RR type..

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS question in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match question
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
policy-map type inspect	Creates an inspection policy map.

match r – me

match regex

To identify a regular expression in a regular expression class map, use the **match regex** command in class-map type regex configuration mode. To remove the regular expression from the class map, use the **no** form of this command.

match regex *name*
no match regex *name*

Syntax Description

name	The name of the regular expression you added with the **regex** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map type regex configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(2)	This command was added.

Usage Guidelines

The **regex** command can be used for various features that require text matching. You can group regular expressions in a regular expression class map using the **class-map type regex** command and then multiple **match regex** commands.

For example, you can configure special actions for application inspection using an inspection policy map (see the **policy map type inspect** command). In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets.

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
```

```
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
 [a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy test interface outside
```

Related Commands

Command	Description
class-map type regex	Creates a regular expression class map.
regex	Adds a regular expression.
test regex	Tests a regular expression.

match req-resp

To configure a match condition for both HTTP requests and responses, use the **match req-resp** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **req-resp content-type mismatch**
no match [**not**] **req-resp content-type mismatch**

Syntax Description

content-type mismatch	Matches traffic with a content-type field in the HTTP response that does not match the accept field in the corresponding HTTP request message.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command enables the following checks:

- Verifies that the value of the header content-type is in the internal list of supported content types,
- Verifies that the header content-type matches the actual content in the data or entity body portion of the message.
- Verifies the content type field in the HTTP response matches the **accept** field in the corresponding HTTP request message.

If the message fails any of the above checks, the ASA takes the configured action.

The following is the list of supported content types.

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword

application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

Some content-types in this list may not have a corresponding regular expression (magic number) so they cannot be verified in the body portion of the message. When this case occurs, the HTTP message will be allowed.

Examples

The following example shows how to restrict HTTP traffic based on the content type of the HTTP message in an HTTP policy map:

```
ciscoasa
(config)#
 policy-map type inspect http http_map
ciscoasa
(config-pmap)#
 match req-resp content-type mismatch
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match request-command

To restrict specific FTP commands, use the **match request-command** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]
no match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]

Syntax Description

ftp_command	Specifies one or more FTP commands to restrict.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for a specific FTP command in an FTP inspection policy map:

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match request-method

To configure a match condition for the SIP method type, use the **match request-method** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **request-method** *method_type*
no match [**not**] **request-method** *method_type*

Syntax Description

method_type	Specifies a method type according to RFC 3261 and supported extensions. Supported method types include: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
ciscoasa(config-cmap)# match request-method ack
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
show running-config class-map	Displays the information about the class map configuration.

match request method

To configure a match condition for HTTP requests, use the **match request method** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }
no match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }

Syntax Description

built-in-regex	Specifies the built-in regex for content type, method, or transfer encoding.
class *class_map name*	Specifies the name of the class map of regex type.
regex *regex_name*	Specifies the name of the regular expression configured using the **regex** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Table 4: Built-in Regex Values

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search

setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

Examples

The following example shows how to define an HTTP inspection policy map that will allow and log any HTTP connection that attempts to access "www\.example.com/.*\.asp" or "www\example[0-9][0-9]\.com" with methods "GET" or "PUT." All other URL/Method combinations will be silently allowed:

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match route-type

To redistribute routes of the specified type, use the **match route-type** command in route-map configuration mode. To remove the route type entry, use the **no** form of this command.

match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }
no match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }

Syntax Description

external	OSPF external routes or EIGRP external routes.
internal	OSPF intra-area and interarea routes or EIGRP internal routes.
local	Locally generated BGP routes.
nssa-external	Specifies the external NSSA.
type-1	(Optional) Specifies the route type 1.
type-2	(Optional) Specifies the route type 2.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **route-map** global configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

For OSPF, the **external type-1** keywords match only type 1 external routes and the **external type-2** keywords match only type 2 external routes.

Examples

The following example shows how to redistribute internal routes:

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match rtp

To specify a UDP port range of even-number ports in a class map, use the **match rtp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match rtp *starting_port range*
no match rtp *starting_port range*

Syntax Description

starting_port	Specifies lower bound of even-number UDP destination port. Range is 2000-65535
range	Specifies range of RTP ports. Range is 0-16383.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match rtp** command to match RTP ports (even UDP port numbers between the *starting_port* and the *starting_port* plus the *range*).

Examples

The following example shows how to define a traffic class using a class map and the **match rtp** command:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
```

```
 rtp 20000 100
ciscoasa(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match selection-mode

To configure a match for the Selection Mode information element in the Create PDP Context request, use the **match selection-mode** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **selection-mode** *mode_value*
no match [**not**] **selection-mode** *mode_value*

Syntax Description

mode_value The Selection Mode information element in the Create PDP Context request. The selection mode specifies the origin of the Access Point Name (APN) in the message, and can be one of the following.

- 0—Verified. The APN was provided by the mobile station or network, and the subscription is verified.
- 1—Mobile Station. The APN was provided by the mobile station, and the subscription is not verified.
- 2—Network. The APN was provided by the network, and the subscription is not verified.
- 3—Reserved, not used.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP policy map.

You can filter on the Selection Mode information element in the Create PDP Context request. The selection mode specifies the origin of the Access Point Name (APN) in the message. You can drop and optionally log messages based on these modes. Selection Mode filtering is supported for GTPv1 and GTPv2 only.

Examples

The following example shows how to match selection mode 1 and 2 and drop and log the Create PDP Context messages that have those modes.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match selection-mode 1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap)# match selection-mode 2
ciscoasa(config-pmap-c)# drop log
```

Related Commands

Command	Description
drop	Drop packets that match the criteria.
log	Log packets that match the criteria.
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.

match sender-address

To configure a match condition on the ESMTP sender e-mail address, use the **match sender-address** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]
no match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]

Syntax Description

length gt *bytes*	Specifies to match on the sender e-mail address length.
regex *regex*	Specifies to match on the regular expression.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to configure a match condition for the sender email address of length greater than 320 characters in an ESMTP inspection policy map:

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match server

To configure a match condition for an FTP server, use the **match server** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

The ASA matches the server name based using the initial 220 server message that is displayed above the login prompt when connecting to an FTP server. The 220 server message might contain multiple lines. The server match is not based on the FQDN of the server name resolved through DNS.

Examples

The following example shows how to configure a match condition for an FTP server in an FTP inspection policy map:

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match service

To configure a match condition for a specific instant messaging service, use the **match service** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }
no match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }

Syntax Description

chat	Specifies to match the instant messaging chat service.
file-transfer	Specifies to match the instant messaging file transfer service.
games	Specifies to match the instant messaging games service.
voice-chat	Specifies to match the instant messaging voice chat service.
webcam	Specifies to match the instant messaging webcam service.
conference	Specifies to match the instant messaging conference service.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the chat service in an instant messaging class map:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match service-indicator

To configure a match condition for the service indicator of M3UA messages, use the **match service-indicator** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **service-indicator** *number*
no match [**not**] **service-indicator** *number*

Syntax Description

number The service indicator number, 0-15. See the usage section for a list of supported service indicators.

Command Default

M3UA inspection allows all service indicators.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop packets based on the service indicator. Following are the available service indicators. Consult M3UA RFCs and documentation for detailed information about these service indicators.

- 0—Signaling Network Management Messages
- 1—Signaling Network Testing and Maintenance Messages
- 2—Signaling Network Testing and Maintenance Special Messages
- 3—SCCP
- 4—Telephone User Part
- 5—ISDN User Part
- 6—Data User Part (call and circuit-related messages)
- 7—Data User Part (facility registration and cancellation messages)
- 8—Reserved for MTP Testing User Part
- 9—Broadband ISDN User Part
- 10—Satellite ISDN User Part

- 11—Reserved
- 12—AAL type 2 Signaling
- 13—Bearer Independent Call Control
- 14—Gateway Control Protocol
- 15—Reserved

Examples

The following example shows how to configure a match condition for M3UA service indicators.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.

match third-party-registration

To configure a match condition for the requester of a third-party registration, use the **match third-party-registration** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

The third-party registration match command is used to identify the user who can register others with a SIP register or SIP proxy. It is identified by the From header field in the REGISTER message in the case of mismatching From and To values.

Examples

The following example shows how to configure a match condition for third-party registration in a SIP inspection class map:

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.

Command	Description
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match tunnel-group

To match traffic in a class map that belongs to a previously defined tunnel-group, use the **match tunnel-group** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

matchtunnel-group*name*
nomatchtunnel-group*name*

Syntax Description

name	Text for the tunnel group name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **police** command. Use **match tunnel-group** along with **match flow ip destination-address** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
ciscoasa(config)# class-map cmap
```

```
ciscoasa(config-cmap)# match
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and L2TP,

match uri

To configure a match condition for the URI in the SIP headers, use the **match uri** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*
no match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*

Syntax Description

sip	Specifies a SIP URI.
tel	Specifies a TEL URI.
length gt *gt_bytes*	Specifies the maximum length of the URI. Value is between 0 and 65536.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	— • Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the URI in the SIP message:

```
ciscoasa(config-cmap)# match uri sip length gt
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match url-filter

To configure a match condition for URL filtering in an RTSP message, use the **match url-filter** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This command can be configured in an RTSP class map or policy map.

Examples

The following example shows how to configure a match condition for URL filtering in an RTSP inspection policy map:

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match user group

To specify a user or group to whitelist for Cloud Web Security, use the **match user group** command in class-map configuration mode. To remove the match, use the **no** form of this command.

match [**not**] { [**user** *username*] [**group** *groupname*] }
no match [**not**] { [**user** *username*] [**group** *groupname*] }

Syntax Description

not	(Optional) Specifies that the user and/or group should be filtered using Web Cloud Security. For example, if you whitelist the group "cisco," but you want to scan traffic from users "johncrichton" and "aerynsun," you can specify **match not** for those users.
user *username*	Specifies a user to whitelist.
group *groupname*	Specifies a group to whitelist.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class map configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If you use AAA rules or IDFW, you can configure the ASA so that web traffic from specific users or groups that otherwise match the service policy rule is not redirected to the Cloud Web Security proxy server for scanning. When you bypass Cloud Web Security scanning, the ASA retrieves the content directly from the originally requested web server without contacting the proxy server. When it receives the response from the web server, it sends the data to the client. This process is called "whitelisting" traffic.

Although you can achieve the same results of exempting traffic based on user or group when you configure the class of traffic using ACLs to send to Cloud Web Security, you might find it more straightforward to use a whitelist instead. Note that the whitelist feature is only based on user and group, not on IP address.

After creating the whitelist as part of the inspection policy map (**policy-map type inspect scansafe**), you can use this map when you specify the Cloud Web Security action using the **inspect scansafe** command.

Examples

The following example whitelists the same users and groups for the HTTP and HTTPS inspection policy maps:

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
whitelist	Performs the whitelist action on the class of traffic.

match username

To configure a match condition for an FTP username, use the **match username** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP username in an FTP inspection class map:

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match uuid

To configure a match condition for the universally unique identifier (UUID) of DCERPC messages, use the **match uuid** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **uuid** *type*
no match [**not**] **uuid** *type*

Syntax Description

type The UUID type to match. One of the following:

- **ms-rpc-epm**—Matches Microsoft RPC EPM messages.
- **ms-rpc-isystemactivator**—Matches ISystemMapper messages.
- **ms-rpc-oxidresolver**—Matches OxidResolver messages.

Command Default

DCERPC inspection allows all message types.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in a DCERPC inspection class map or policy map. Use it to filter traffic based on DCERPC UUID. You can then reset or log matching traffic.

Examples

The following example shows how to configure a match condition for the ms-rpc-isyustemactivator UUID in the DCERPC message:

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap

ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
policy-map type inspect	Creates an inspection policy map.

match version

To configure a match condition for the GTP version in GTP inspection, use the **match version** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]
no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

Syntax Description

version_id	Specifies a version between 0 and 255.
range *lower_range upper_range*	Specifies a lower and upper range of versions.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

The following example shows how to configure a match condition for a message version in a GTP inspection policy map:

```
ciscoasa(config-pmap)# match version 1
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.

max-area-addresses

To configure additional manual addresses for an IS-IS area, use the **max-area-addresses** command in router isis configuration mode. To disable the manual addresses, use the **no** form of this command.

max-area-addresses *number*
no max-area-addresses *number*

Syntax Description

number	The number of manual addresses to add. The range is 3 to 234.

Command Default

No manual addresses are configured for an IS-IS area.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command lets you maximize the size of an IS-IS area by configuring additional manual addresses. You specify the number of addresses you want to add and assign a NET address to create each manual address.

Examples

The following example configures three addresses:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addreses 3
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.

Command	Description
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.

Command	Description
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.

Command	Description
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

max-failed-attempts

To specify the number of failed AAA transactions allowed for any given server in the server group before that server is deactivated, use the **max-failed-attempts** command in aaa-server group configuration mode. To remove this specification and revert to the default value, use the **no** form of this command.

max-failed-attempts*number*
nomax-failed-attempts

Syntax Description

number	An integer in the range of 1-5, specifying the number of failed AAA transactions allowed for any given server in the server group specified in a previous **aaa-server** command.

Command Default

The default value of *number* is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must have configured the AAA server or group before issuing this command.

Examples

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# max-failed-attempts 4
ciscoasa
(config-aaa-server-group)#
```

Related Commands

Command	Description
aaa-server *server-tag***protocol** *protocol*	Enters aaa-server group configuration mode so that you can configure AAA server parameters that are group-specific and common to all hosts in the group.
clear configure aaa-server	Removes all AAA server configurations.

Command	Description
show running-config aaa	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

max-forwards-validation

To enable check on Max-forwards header field of 0, use the **max-forwards-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log** }
no max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log** }

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection of a violation occurs.
log	Specifies standalone or additional log in case of violation. It can be associated to any of the actions.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command counts the number of hops to destination, which cannot be 0 before reaching the destination.

Examples

The following example shows how to enable max forwards validation in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

max-header-length

To restrict HTTP traffic based on the HTTP header length, use the **max-header-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]
no max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
request	Request message.
reset	Send a TCP reset message to client and server.
response	(Optional) Response message.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After enabling the max-header-length command, the ASA only allows messages having an HTTP header within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and optionally create a syslog entry.

Examples

The following example restricts HTTP requests to those with HTTP headers that do not exceed 100 bytes. If a header is too large, the ASA resets the TCP connection and creates a syslog entry.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

max-lsp-lifetime

To set the maximum time that LSPs can remain in an ASA's database without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default lifetime, use the **no** form of this command.

max-lsp-lifetime *seconds*
nomax-lsp-lifetime

Syntax Description

seconds	The lifetime of the LSP in seconds. The range is 1 to 65535.

Command Default

The default is 1200 seconds (20 minutes).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If the lifetime is exceeded before a refresh LSP arrives, the LSP is dropped from the database.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** command. LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you misconfigure the LSP lifetime to be too low compared to the LSP refresh interval, the software reduces the LSP refresh interval to prevent the LSPs from timing out.

You might prefer higher values for each command to reduce control traffic at the expense of holding stale LSPs from a crashed or unreachable router in the database longer (thus wasting memory) or increasing the risk of undetected bad LSPs staying active (very rare).

Examples

The following example configures an LSP lifetime of 40 minutes:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

maximum-paths (BGP)

To control the maximum number of parallel BGP routes that can be installed in a routing table, use the maximum-paths command in address-family configuration mode. To restore the default value, use the no form of this command.

maximum-paths [**ibgp**] *number-of-paths*
no maximum-paths [**ibgp**] *number-of-paths*

Syntax Description

ibgp	(Optional) This will enable you to control the maximum number of internal BGP routes that can be installed to the routing table.
number-of-paths	Number of routes to install to the routing table.

Command Default

By default, BGP installs only one best path in the routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The maximum-paths command is used to configure equal-cost or unequal-cost multipath load sharing for BGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to BGP peers when BGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path.

To configure BGP equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.

Examples

The following example configuration installs two parallel iBGP paths:

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Related Commands

Commands	Description
show bgp	Displays entries in the BGP routing table.

maximum-paths (IS-IS)

To configure multipath load sharing for IS-IS protocol, use the **maximum-paths** command in router isis configuration mode. To disable multipath load sharing for ISIS routes, use the **no** form of this command.

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

Syntax Description

number-of-paths	The number of routes to install to the routing table. The range is 1 to 8.

Command Default

By default, IS-IS only installs one best path in the routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The **maximum-paths** command is used to configure ISIS multipath load sharing when ECMP is configured in the ASA.

Examples

The following example configures the maximum paths in the routing table at eight:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.

Command	Description
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.

Command	Description
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.

Command	Description
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

max-object-size

To set a maximum size for objects that the ASA can cache for WebVPN sessions, use the max-object-size command in cache mode. To change the size, use the command again.

max-object-size*integerrange*

Syntax Description

integer	0 - 10000
range	KB

Command Default

1000 KB

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The Maximum object size must be larger than the minimum object size. The ASA calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 4000 KB:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# max-object-size
 4000
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
min-object-size	Defines the minimum size of an object to cache.

max-retry-attempts (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To configure the number of times the ASA retries a failed SSO authentication attempt before letting the request time out, use the **max-retry-attempts** command in the webvpn configuration mode for the specific SSO server type.

To return to the default value, use the **no** form of this command.

max-retry-attempts *retries*
nomax-retry-attempts

Syntax Description

retries The number of times the ASA retries a failed SSO authentication attempt. The range is 1 to 5 retries.

Command Default

The default value for this command is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map type regex configuration	• Yes	—	• Yes	—	—
config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

Once you have configured the ASA to support SSO authentication, optionally you can adjust two timeout parameters:

- The number of times the ASA retries a failed SSO authentication attempt using the **max-retry-attempts command.**
- The number of seconds before a failed SSO authentication attempt times out (see the **request-timeout** command).

Examples

The following example, entered in webvpn-sso-siteminder configuration mode, configures four authentication retries for the SiteMinder SSO server named my-sso-server:

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

max-uri-length

To restrict HTTP traffic based on the length of the URI in the HTTP request message, use the **max-uri-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]
no max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
reset	Send a TCP reset message to client and server.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

After enabling the max-uri-length command, the ASA only allows messages having a URI within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and create a syslog entry.

URIs with a length less than or equal to the configured value will be allowed. Otherwise, the specified action will be taken.

Examples

The following example restricts HTTP requests to those with URIs that do not exceed 100 bytes. If a URI is too large, the ASA resets the TCP connection and creates a syslog entry.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

mcast-group

To specify the multicast group for a VXLAN VNI interface, use the **mcast-group** command in interface configuration mode. To remove the group, use the **no** form of this command.

mcast-group *mcast_ip*
nomcast-group

Syntax Description

mcast_ip	Sets the multicast group IP address, IPv4 or IPv6.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.
9.20(1)	This command now supports IPv6.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface with the **mcast-group** command (or on the VTEP as a whole).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

If you do not set the multicast group for the VNI interface, the default group from the VTEP source interface configuration is used, if available (**default-mcast-group** command). If you manually set a VTEP peer IP for the VTEP source interface using the **peer ip** command, you cannot specify a multicast group for the VNI interface. Multicast is not supported in multiple context mode.

Examples

The following example configures the VNI 1 interface and specifies a multicast group of 236.0.0.100:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Command	Description
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

mcc

To identify the mobile country code and the mobile network code for IMSI prefix filtering in GTP inspection, use the **mcc** command in policy map parameters configuration mode. To remove the configuration, use the no form of this command.

[**drop**] **mcc** *country_code* **mnc** *network_code*
no [**drop**] **mcc** *country_code* **mnc** *network_code*

Syntax Description

drop	Specifies that connections that match the prefix combination should be dropped. Thus, your combinations indicate the unwanted prefixes. Without this keyword, connections must match the prefix combinations to be allowed. All prefix filtering within a given map must be consistent, either all drop or all allow.
country_code	A non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prefixed by 0 to create a three-digit value.
network_code	A two or three-digit value identifying the network code.

Command Default

By default, GTP inspection does not check for valid MCC/MNC combinations.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.16(1)	The **drop** keyword was added.

Usage Guidelines

You can enter the command as many times as necessary to specify all targeted MCC/MNC pairs, but all commands within the policy map must be either **mcc** or **drop mcc**. You cannot combine these commands.

By default, GTP inspection does not check for valid Mobile Country Code (MCC)/Mobile Network Code (MNC) combinations. If you configure IMSI prefix filtering, the MCC and MNC in the IMSI of the received packet is compared with the configured MCC/MNC combinations. The system then takes one of the following actions based on the command:

- **mcc** command—The packet is dropped if it does not match.

- **drop mcc** command—The packet is dropped if it does match.

The Mobile Country Code is a non-zero, three-digit value; add zeros as a prefix for one- or two-digit values. The Mobile Network Code is a two- or three-digit value.

Add all MCC and MNC combinations you want to either permit or to drop. By default, the ASA does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Examples

The following example identifies traffic for IMSI Prefix filtering with an MCC of 111 and an MNC of 222:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

media-termination (Deprecated)

To specify the media termination instance to use for media connections to the Phone Proxy feature, use the **media-termination** command in phone proxy configuration mode.

To remove the media-termination address from the Phone Proxy configuration, use the **no** form of this command.

media-terminationinstance_name
nomedia-termination*instance_name*

Syntax Description

instance_name	Specifies the name of the interface for which the media termination address is used. Only one media-termination address can be configured per interface.

Command Default

There are no default settings for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
8.2(1)	This command was updated to allow for using NAT with the media-termination address. The **rtp-min-port** and **rtp-max-ports** keywords were removed from the command syntax and included as a separate command.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

The ASA must have IP addresses for media termination that meet the following criteria:

For the media termination instance, you can configure a global media-termination address for all interfaces or configure a media-termination address for different interfaces. However, you cannot use a global media-termination address and media-termination addresses configured for each interface at the same time.

If you configure a media termination address for multiple interfaces, you must configure an address on each interface that the ASA uses when communicating with IP phones.

The IP addresses are publicly routable addresses that are unused IP addresses within the address range on that interface.

See CLI configuration guide for the complete list of prerequisites that you must follow when creating the media termination instance and configuring the media termination addresses.

Examples

The following example shows the use of the media-termination address command to specify the IP address to use for media connections:

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

media-type

To set the media type to copper or fiber Gigabit Ethernet, use the **media-type** command in interface configuration mode. The fiber SFP connector is available on the 4GE SSM for the ASA 5500 series adaptive security appliance. To restore the media type setting to the default, use the **no** form of this command.

media-type { **rj45** | **sfp** }
no media-type [**rj45** | **sfp**]

Syntax Description

rj45	(Default) Sets the media type to the copper RJ-45 connector.
sfp	Sets the media type to the fiber SFP connector.

Command Default

The default is **rj45**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(4)	This command was added.

Usage Guidelines

The **sfp** setting uses a fixed speed (1000 Mbps), so the **speed** command allows you to set whether the interface negotiates link parameters or not. The **duplex** command is not supported for **sfp**.

Examples

The following example sets the media type to SFP:

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

Command	Description
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

member

To assign a context to a resource class, use the **member** command in context configuration mode. To remove the context from the class, use the **no** form of this command.

member*class_name*
nomember*class_name*

Syntax Description

class_name	Specifies the class name you created with the **class** command.

Command Default

By default, the context is assigned to the default class.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context. The ASA manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

Examples

The following example assigns the context test to the gold class:

```
ciscoasa(config-ctx)# context
 test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
limit-resource	Sets the limit for a resource.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

member-interface

To assign a physical interface to a redundant interface, use the **member-interface** command in interface configuration mode. This command is available only for the redundant interface type. You can assign two member interfaces to a redundant interface. To remove a member interface, use the **no** form of this command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.

member-interface*physical_interface*
nomember-interface*physical_interface*

Syntax Description

physical_interface	Identifies the interface ID, such as **gigabitethernet 0/1**. See the **interface** command for accepted values. Both member interfaces must be the same physical type.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Both member interfaces must be of the same physical type. For example, both must be Ethernet.

You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.

⚠

Caution If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters such as **speed** and **duplex** commands, the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.

If you shut down the active interface, then the standby interface becomes active.

To change the active interface, enter the **redundant-interface** command.

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the **mac-address** command or the **mac-address auto** command). When the active interface fails over to the standby, the same MAC address is maintained so traffic is not disrupted.

Examples

The following example creates two redundant interfaces:

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
redundant-interface	Changes the active member interface.
show interface	Displays the runtime status and statistics of interfaces.

memberof

To specify a list of group-names that this user is a member of, use the **memberof** command in username attributes configuration mode. To remove this attribute from the configuration, use the **no** form of this command.

memberof *group_1* [, *group_2* , . . . *group_n*]
no memberof *group_1* [, *group_2* , . . . *group_n*]

Syntax Description

group_1 through group_n	Specifies the groups to which this user belongs.

Command Default

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Enter a comma-separated list of group names to which this user belongs.

Examples

The following example entered in global configuration mode, creates a username called newuser, then specifies that newuser is a member of the DevTest and management groups:

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

Related Commands

Command	Description
clear configure username	Clears the entire username database or just the specified username.
show running-config username	Displays the currently running username configuration for a specified user or for all users.
username	Creates and manages the database of user names.

memory appcache-threshold enable

To enable the memory application cache threshold, use the **memory appcache-threshold enable** command in the configuration mode. To disable the **memory appcache-threshold,** use the **no** form of this command.

memoryappcache-thresholdenable
nomemoryappcache-thresholdenable

Syntax Description

This command has no arguments or keywords.

Command Default

This **memory appcache-threshold enable** command is enabled on ASA 5585-X FirePOWER SSP-60 (5585-60) by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

Enabling memory appcache-threshold restricts application cache allocations after reaching certain memory threshold so that there is a reservation of memory to maintain stability and manageability of the device.

In ASA 9.10.1 release, the memory appcache-threshold feature was implemented on 5585-60 to restrict the application cache allocations for through-the-box connections only.

This command configures the application cache allocation threshold to 85%of the system memory. When the memory usage reaches the threshold level, the new through-the-box connections to the device are dropped.

The **no** form of the command causes all of the memory allocation restriction to be freed for usage without validation. The current statistical counters are retained to maintain the troubleshooting history until the **clear memory appcache-threshold** command is executed.

For 9.10.1 release, only SNP Conn Core 00 application cache type is managed. This name is aligned with the output of “show mem app-cache”.

Examples

The following example enables the appcache-memory threshold:

```
ciscoasa(config)# memory appcache-threshold enable
```

Related Commands

Command	Description
show memory appcache-threshold	Show the status and hit count of memory appcache-threshold
clear memory appcache-threshold	Clear the hit count of memory appcache-threshold

memory delayed-free-poisoner enable

To enable the delayed free-memory poisoner tool, use the **memory delayed-free-poisoner enable** command in privileged EXEC mode. To disable the delayed free-memory poisoner tool, use the **no** form of this command. The delayed free-memory poisoner tool lets you monitor freed memory for changes after it has been released by an application.

memorydelayed-free-poisonerenable
nomemorydelayed-free-poisonerenable

Syntax Description

This command has no arguments or keywords.

Command Default

The **memory delayed-free-poisoner enable** command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Enabling the delayed free-memory poisoner tool has a significant impact on memory usage and system performance. The command should only be used under the supervision of the Cisco TAC. It should not be run in a production environment during heavy system usage.

When you enable this tool, requests to free memory by the applications running on the ASA are written to a FIFO queue. As each request is written to the queue, each associated byte of memory that is not required by lower-level memory management is “poisoned” by being written with the value 0xcc.

The freed memory requests remain in the queue until more memory is required by an application than is in the free memory pool. When memory is needed, the first freed memory request is pulled from the queue and the poisoned memory is validated.

If the memory is unmodified, it is returned to the lower-level memory pool and the tool reissues the memory request from the application that made the initial request. The process continues until enough memory for the requesting application is freed.

If the poisoned memory has been modified, then the system forces a crash and produces diagnostic output to determine the cause of the crash.

The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically. Validation can also be started manually using the **memory delayed-free-poisoner validate** command.

The **no** form of the command causes all of the memory referenced by the requests in the queue to be returned to the free memory pool without validation and any statistical counters to be cleared.

Examples

The following example enables the delayed free-memory poisoner tool:

```
ciscoasa# memory delayed-free-poisoner enable
```

The following is sample output when the delayed free-memory poisoner tool detects illegal memory reuse:

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

<xref> describes the significant portion of the output.

Table 5: Illegal Memory Usage Output Description

Field	Description
heap region	The address region and size of the region of memory available for use by the requesting application. This is not the same as the requested size, which may be smaller given the manner in which the system may parcel out memory at the time the memory request was made.
memory address	The location in memory where the fault was detected.
byte offset	The byte offset is relative to the beginning of the heap region and can be used to find the field that was modified if the result was used to hold a data structure starting at this address. A value of 0 or that is larger than the heap region byte count may indicate that the problem is an unexpected value in the lower level heap package.
allocated by/freed by	Instruction addresses where the last malloc/calloc/realloc and free calls where made involving this particular region of memory.
Dumping...	A dump of one or two regions of memory, depending upon how close the detected fault was to the beginning of the region of heap memory. The next eight bytes after any system heap header is the memory used by this tool to hold a hash of various system header values plus the queue linkage. All other bytes in the region until any system heap trailer is encountered should be set to 0xcc.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory delayed-free-poisoner validate

To force validation of all elements in the **memory delayed-free-poisoner** queue, use the **memory delayed-free-poisoner validate** command in privileged EXEC mode.

memorydelayed-free-poisonervalidate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must enable the delayed free-memory poisoner tool using the **memory delayed-free-poisoner enable** command before issuing the **memory delayed-free-poisoner validate** command.

The **memory delayed-free-poisoner validate** command causes each element of the **memory delayed-free-poisoner** queue to be validated. If an element contains unexpected values, then the system forces a crash and produces diagnostic output to determine the cause of the crash. If no unexpected values are encountered, the elements remain in the queue and are processed normally by the tool; the **memory delayed-free-poisoner validate** command does not cause the memory in the queue to be returned to the system memory pool.

Note The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically.

Examples

The following example causes all elements in the **memory delayed-free-poisoner** queue to be validated:

```
ciscoasa# memory delayed-free-poisoner validate
```

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory caller-address

To configure a specific range of program memory for the call tracing, or caller PC, to help isolate memory problems, use the **memory caller-address** command in privileged EXEC mode. The caller PC is the address of the program that called a memory allocation primitive. To remove an address range, use the **no** form of this command.

memorycaller-address*startPCendPC*
nomemorycaller-address

Syntax Description

endPC	Specifies the end address range of the memory block.
startPC	Specifies the start address range of the memory block.

Command Default

The actual caller PC is recorded for memory tracing.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0	This command was added.

Usage Guidelines

Use the **memory caller-address** command to isolate memory problems to a specific block of memory.

In certain cases the actual caller PC of the memory allocation primitive is a known library function that is used at many places in the program. To isolate individual places in the program, configure the start and end program address of the library function, thereby recording the program address of the caller of the library function.

Note The ASA might experience a temporary reduction in performance when caller-address tracing is enabled.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08

ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
```

```
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory-caller address	Displays the address ranges configured on the ASA.

memory logging

To enable memory logging, use the **memory logging** command in global configuration mode. To disable memory logging, use the **no** form of this command.

memory logging [**1024-4194304**] [**wrap**] [**size** [**1-2147483647**]] [**process** *process-name*] [**context** *context-name*]
nomemorylogging

Syntax Description

1024-4194304	Specifies the number of logging entries in the memory logging buffer. This is the only required argument to specify.
context *context-name*	Specifies the virtual context and context name to monitor.
process *process-name*	Specifies the process and process name to monitor. **Note** The Checkheaps process is completely ignored as a process because it uses the memory allocator in a non-standard way.
size 1-2147483647	Specifies the size and number of entries to monitor.
wrap	Save the buffer when it wraps. It can only be saved once. If it wraps multiple times, it can be overwritten. When the buffer wraps, a trigger is sent to the event manager to enable saving of the data.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

To change memory logging parameters, you must disable it, then reenable it.

Examples

The following example enables memory logging:

```
ciscoasa
```

```
(config)#
memory logging 202980
```

Related Commands

Command	Description
event memory-logging-wrap	Enables response to memory logging wrap events.
show memory logging	Displays memory logging results.

memory profile enable

To enable the monitoring of memory usage (memory profiling), use the **memory profile enable** command in privileged EXEC mode. To disable memory profiling, use the **no** form of this command.

memoryprofileenablepeak*peak_value*
nomemoryprofileenablepeak*peak_value*

Syntax Description

peak_value	Specifies the memory usage threshold at which a snapshot of the memory usage is saved to the peak usage buffer. The contents of this buffer could be analyzed at a later time to determine the peak memory needs of the system.

Command Default

Memory profiling is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0	This command was added.

Usage Guidelines

Before enabling memory profiling, you must first configure a memory text range to profile with the **memory profile text** command.

Some memory is held by the profiling system until you enter the **clear memory profile** command. See the output of the **show memory status** command.

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

The following example enables memory profiling:

```
ciscoasa# memory profile enable
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.

memory profile text

To configure a program text range of memory to profile, use the **memory profile text** command in privileged EXEC mode. To disable, use the **no** form of this command.

memory profile text { *startPC endPC* | **all** *resolution* }
no memory profile text { *startPC endPC* | **all** *resolution* }

Syntax Description

all	Specifies the entire text range of the memory block.
endPC	Specifies the end text range of the memory block.
resolution	Specifies the resolution of tracing for the source text region.
startPC	Specifies the start text range of the memory block.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0	This command was added.

Usage Guidelines

For a small text range, a resolution of "4" normally traces the call to an instruction. For a larger text range, a coarse resolution is probably enough for the first pass and the range could be narrowed down to a set of smaller regions in the next pass.

After entering the text range with the **memory profile text** command, you must then enter the **memory profile enable** command to begin memory profiling. Memory profiling is disabled by default.

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows how to configure a text range of memory to profile, with a resolution of 4:

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

The following example displays the configuration of the text range and the status of memory profiling (OFF):

```
ciscoasa# show memory profile
InUse profiling: OFF Peak profiling: OFF Profile: 0x004018b4-0x004169d0(00000004)
```

Note To begin memory profiling, you must enter the **memory profile enable** command. Memory profiling is disabled by default.

Related Commands

Command	Description
clear memory profile	Clears the buffers held by the memory profiling function.
memory profile enable	Enables the monitoring of memory usage (memory profiling).
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory-caller address	Displays the address ranges configured on the ASA.

memory-size

To configure the amount of memory on the ASA which the various components of WebVPN can access, use the **memory-size** command in webvpn mode. You can configure the amount of memory either as a as a set amount of memory in KB or as a percentage of total memory. To remove a configured memory size, use the **no** form of this command.

Note A reboot is required for the new memory size setting to take effect.

memory-size { **percent** | **kb** } *size*
no memory-size [{ **percent** | **kb** } *size*]

Syntax Description

kb	Specifies the amount of memory in Kilobytes.
percent	Specifies the amount of memory as a percentage of total memory on the ASA.
size	Specifies the amount of memory, either in KB or as a percentage of total memory.

Command Default

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The configured amount of memory will be allocated immediately. Before configuring this command, check the amount of available memory by using show memory. If a percentage of total memory is used for configuration, ensure that the configured value is below the available percentage. If a Kilobyte value is used for configuration, ensure that the configured value is below the available amount of memory in Kilobytes.

Examples

The following example shows how to configure a WebVPN memory size of 30 per cent:

```
ciscoasa
(config)#
 webvpn
ciscoasa
```

```
(config-webvpn)#
 memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

Related Commands

Command	Description
show memory webvpn	Displays WebVPN memory usage statistics.

memory tracking enable

To enable the tracking of heap memory request, use the **memory tracking enable** command in privileged EXEC mode. To disable memory tracking, use the **no** form of this command.

memorytrackingenable
nomemorytrackingenable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(8)	This command was added.

Usage Guidelines

Use the **memory tracking enable** command to track heap memory requests. To disable memory tracking, use the **no** form of this command.

Before you enable memory tracking, ensure to change the default interval and count value in the app-agent heartbeat command to the ones below:

app-agent heartbeat interval 6000 retry-count 6

Examples

The following example enables tracking heap memory requests:

```
ciscoasa# memory tracking enable
```

Related Commands

Command	Description
clear memory tracking	Clears all currently gathered information.
show memory tracking	Shows currently allocated memory.
show memory tracking address	Lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.

Command	Description
show memory tracking dump	This command shows the size, location, partial callstack, and a memory dump of the given memory address.
show memory tracking detail	Shows various internal details to be used in gaining insight into the tool's internal behavior.

memory-utilization

Use the memory utilization command to configure ASA to automatically reboot or crash once the system memory is used up at a pre-defined level. Once the memory usage reaches the configured threshold limit, the system automatically reloads.Threshold value could be in the range of 90-99%.

memory-utilization reload-threshold < **%** >
memory-utilization reload-threshold < **%** > [**crashinfo**]

Syntax Description

reload-threshold	Specifies the system memory threshold limit.
crashinfo	(Optional) Specifies that if used, the crash information is saved before a system reload.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

It is recommended that you DO NOT configure this feature on those systems that are known to experience environments, where very high memory utilization is commonly observed. Use the optional crashinfo argument to generate a crash information file before a system reload.

Examples

The following example displays how to configure memory utilization feature on ASA:

```
ciscoasa# memory-utilization reload-threshold 95
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.
memory profile enable	Enables the monitoring of memory usage (memory profiling).
clear memory profile	Clears the buffers held by the memory profiling function.

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.

merge-dacl

To merge a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet, use the **merge-dacl** command in aaa-server group configuration mode. To disable the merging of a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet, use the **no** form of this command.

merge dacl { **before_avpair** | **after_avpair** }
nomergedacl

Syntax Description

after_avpair	Specifies that the downloadable ACL entries should be placed after the Cisco AV pair entries. This option applies only to VPN connections. For VPN users, ACLs can be in the form of Cisco AV pair ACLs, downloadable ACLs, and an ACL that is configured on the ASA. This option determines whether or not the downloadable ACL and the AV pair ACL are merged, and does not apply to any ACLs configured on the ASA.
before_avpair	Specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries.

Command Default

The default setting is **no merge dacl**, which specifies that downloadable ACLs will not be merged with Cisco AV pair ACLs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
AAA-server group configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

If both an AV pair and a downloadable ACL are received, the AV pair has priority and is used.

Examples

The following example specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries:

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

Related Commands

Command	Description
aaa-server host	Identifies the server and the AAA server group to which it belongs.
aaa-server protocol	Identifies the server group name and the protocol.
max-failed-attempts	Specifies the maximum number of requests sent to a AAA server in the group before trying the next server.

message-length

To filter DNS packets that do not meet the configured maximum length, use the message-length command in parameters configuration mode. Use the **no** form to remove the command.

message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }
no message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }

Syntax Description

length	The maximum number of bytes allowed in a DNS message, from 512 to 65535.
client {*length* | **auto**}	The maximum number of bytes allowed in a client DNS message, from 512 to 65535, or **auto** to set the maximum length to the value in the Resource Record.
server {*length* | **auto**}	The maximum number of bytes allowed in a server DNS message, from 512 to 65535, or **auto** to set the maximum length to the value in the Resource Record.

Command Default

The default inspection sets DNS maximum message length to 512, and client length to **auto**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

You can configure the maximum DNS message length as parameter in a DNS inspection map.

Examples

The following example shows how to configure the maximum DNS message length in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

Related Commands

Commands	Description
parameter	Enters parameter configuration mode while in policy map configuration mode.

Commands	Description
policy-map type inspect dns	Creates a DNS inspection policy map.

message-tag-validation

To validate the content of certain fields in M3UA messages, use the **message-tag-validation** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect m3ua** command. Use the **no** form of this command to remove the setting.

message-tag-validation { **dupu** | **error** | **notify** }
no message-tag-validation { **dupu** | **error** | **notify** }

Syntax Description

dupu	Enable validation for the Destination User Part Unavailable (DUPU) message. The User/Cause field must be present, and it must contain only valid cause and user codes.
error	Enable validation for the Error message. All mandatory fields must be present and contain only allowed values. Each error message must contain the required fields for that error code.
notify	Enable validation for the Notify message. The status type and status information fields must contain allowed values only.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command to ensure that the content of certain fields are checked and validated for the specified M3UA message type. Messages that fail validation are dropped.

Examples

The following example enables message validation for DUPU, Error, and Notify messages in M3UA inspection.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.
show service-policy inspect m3ua	Displays M3UA statistics.

metric

To globally change the metric value for all IS-IS interfaces, use the **metric** command in router isis configuration mode. To disable the metric value and reinstate the default metric value of 10, use the **no** form of this command.

metric *default-value* [**level-1** | **level-2**]
no metric *default-value* [**level-1** | **level-2**]

Syntax Description

default-value	The metric value to be assigned to the link and used to calculate the path cost via the links to destinations. The range is 1 to 63.
level-1	(Optional) Sets IS-IS Level 1 IPv4 or IPv6 metric.
level-2	(Optional) Sets IS-IS Level 2 IPv4 or IPv6 metric.

Command Default

The default is 10.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

When you need to change the default metric value for all IS-IS interfaces, we recommend that you use the **metric** command in to configure all interfaces globally. Globally configuring the metric values prevents user errors, such as unintentionally removing a set metric from an interface without configuring a new value and unintentionally allowing the interface to revert to the default metric of 10, thereby becoming a highly preferred interface in the network.

Once you enter the **metric** command to change the default IS-IS interface metric value, an enabled interface uses the new value instead of the default value of 10. Passive interfaces continue to use the metric value of 0.

Examples

The following example configures the IS-IS interfaces with a global metric of 111:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

metric-style

To configure a router running IS-IS so that it generates and accepts only new-style type, length, value objects (TLVs), use the **metric-style** command in router isis configuration mode. To disable this function, use the **no** form of this command.

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
no metric [**level-1** | **level-2** | **level-1-2**]

Syntax Description

narrow	Instructs the ASA to use the old style of TLVs with the narrow metric.
transition	(Optional) Instructs the ASA to accept both old- and new-style TLVs during transition.
wide	Instructs the ASA to use the new style of TLVs to carry the wider metric.
level-1	(Optional) Enables this command on routing Level 1.
level-2	(Optional) Enables this command on routing Level 2.
level-1-2	(Optional) Instructs the router to accept both old- and new-style TLVs.

Command Default

The default is 10.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If you enter the metric-style wide command, an ASA generates and accepts only new-style TLVs. Therefore, the ASA uses less memory and other resources than it would if it generated both old-style and new-style TLVs.

This style is appropriate for enabling MPLS traffic engineering across an entire network.

Examples

The following example configures the ASA to generate and accept new-style TLVs on Level 1:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

mf – mz

mfib forwarding

To reenable MFIB forwarding on an interface, use the **mfib forwarding** command in interface configuration mode. To disable MFIB forwarding on an interface, use the **no** form of this command.

mfibforwarding
nomfibforwarding

Syntax Description

This command has no arguments or keywords.

Command Default

The **multicast-routing** command enables MFIB forwarding on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

When you enable multicast routing, MFIB forwarding is enabled on all interfaces by default. Use the **no** form of the command to disable MFIB forwarding on a specific interface. Only the **no** form of the command appears in the running configuration.

When MFIB forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when MFIB forwarding is disabled.

Examples

The following example disables MFIB forwarding on the specified interface:

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing.
pim	Enables PIM on an interface.

migrate

To migrate a LAN-to-LAN (IKEv1) or remote access configuration (SSL or IKEv1) to IKEv2, use the migrate command from global configuration mode:

migrate { **l2l** | **remote-access** { **ikev2** | **ssl** } | **overwrite** }

Syntax Description

l2l	Migrates the IKEv1 LAN-to-LAN configuration to IKEv2.
remote-access	Specifies remote access configuration.
ikev2	Migrates the remote access IKEv1 configuration to IKEv2.
ssl	Migrates the remote access SSL configuration to IKEv2.
overwrite	Overwrites existing IKEv2 configuration.

Command Default

There is no default value or behavior.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **migrate l2l** command migrates all LAN-to-LAN IKEv1 configuration to IKEv2.

If you use the **overwrite** keyword, the ASA overwrites any existing IKEv2 configuration with migrated commands instead of merging them.

The **migrate remote-access** command migrates the IKEv1 or SSL settings to IKEv2, but you must still perform these configuration tasks:

- Load the Secure Client package file(s) in webvpn configuration mode.
- Configure the Secure Client profiles and specify them for group policies.
- Associate any customization objects you used for IKEv1 connections with the tunnel group(s) used for IKEv2 connections.

- Specify server authentication identity certificates (trustpoints) using the **crypto ikev2 remote-access trust-point** command. The ASA uses the trustpoint to authenticate itself to remote Secure Clients connecting with IKEv2.
- Specify IKEv2 and/or SSL for any tunnel groups or group policies you may have configured in addition to the default ones (the DefaultWEBVPNGroup tunnel-group and default group-policy are configured to allow IKEv2 or SSL).
- Configure group aliases or group URLs in the tunnel-groups to enable the clients to connect to groups other than the default group.
- Update any external group policies and/or user records.
- Any other global, tunnel group, group policy settings to change client behavior.
- Configure the port to be used by the client to download files and/or perform software upgrades for IKEv2 using the **crypto ikev2 enable** <interface> [client-services [port]] command.

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which the IPsec peers communicate.
show run crypto ikev2	Displays IKEv2 configuration information.

min-object-size

To set a minimum size for objects that the ASA can cache for WebVPN sessions, use the min-object-size command in cache mode. To change the size, use the command again. To set no minimum object size, enter a value of zero (0).

min-object-size*integerrange*

Syntax Description

integer	0 - 10000
range	KB.

Command Default

The default size is 0 KB.

Command Modes

The following table shows the modes in which you enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cache Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The minimum object size must be smaller than the maximum object size. The ASA calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 40 KB:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# min-object-size
 40
ciscoasa(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.

mkdir

To create a new directory, use the **mkdir** command in privileged EXEC mode.

mkdir [/ **noconfirm**] [**disk0:** | **disk1:** | | **flash:**] *path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series adaptive security appliances, the **flash** keyword is aliased to **disk0**.
path	The name and path of the directory to create.

Command Default

If you do not specify a path, the directory is created in the current working directory.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If a directory with the same name already exists, then the new directory is not created.

Examples

The following example shows how to make a new directory called “backup”:

```
ciscoasa# mkdir backup
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
rmdir	Removes the specified directory.

Command	Description
pwd	Display the current working directory.

mobile-device portal

To change the clientless vpn access web portal from the mini-portal to the full-browser portal, for all mobile devices, use the **mobile-device portal** command from webvpn configuration mode. You will only need to make this configuration for smart phones running older operating systems such as Windows CE. You will not need to configure this option using modern smart phones as they use the full-browser portal by default.

mobile-device portal { **full** }
no mobile-device portal { **full** }

Syntax Description

mobile-device portal {full}	Changes the clientless vpn access portal from the mini-portal to the full-browser portal for all mobile devices.

Command Default

Before you run the command, the default behavior is that some mobile devices will get clientless vpn access through the mini-portal and some will use the full portal.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)	This command was added simultaneously in 8.2(5) and 8.4(2).
8.4(2)	This command was added simultaneously in 8.2(5) and 8.4(2).

Usage Guidelines

Use this command only if you are recommended to do so by Cisco Technical Assistance Center (TAC).

Examples

Changes the clientless vpn access portal to a full-browser portal for all mobile devices.

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

Related Commands

Command	Description
show running-config webvpn	Displays the running configuration for webvpn.

mode

To set the security context mode to single or multiple, use the **mode** command in global configuration mode. You can partition a single ASA into multiple virtual devices, known as security contexts. Each context behaves like an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone appliances. In single mode, the ASA has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

mode { **single** | **multiple** } [**noconfirm**]

Syntax Description

multiple	Sets multiple context mode.
noconfirm	(Optional) Sets the mode without prompting you for confirmation. This option is useful for automated scripts.
single	Sets the context mode to single.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In multiple context mode, the ASA includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone device (see the **config-url** command to identify the context configuration location). The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

When you change the context mode using the **mode** command, you are prompted to reboot.

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the ASA converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The ASA automatically adds an entry for the admin context to the system configuration with the name "admin."

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the ASA; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device.

Not all features are supported in multiple context mode. See the CLI configuration guide for more information.

Examples

The following example sets the mode to multiple:

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

The following example sets the mode to single:

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

Related Commands

Command	Description
context	Configures a context in the system configuration and enters context configuration mode.
show mode	Shows the current context mode, either single or multiple.

monitor-interface

To enable health monitoring on a specific interface, use the **monitor-interface** command in global configuration mode. To disable interface monitoring, use the **no** form of this command.

monitor-interface { *if_name* | **service-module** }
no monitor-interface { *if_name* **service-module** }

Syntax Description

if_name	Specifies the name of the interface being monitored.
service-module	Monitors the service module. If you do not want a hardware module failure, such as the ASA FirePOWER module, to trigger failover, you can disable module monitoring using the **no** form of this command.

Command Default

Monitoring of physical interfaces and the service module is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.3(1)	The service-module keyword was added.

Usage Guidelines

The number of interfaces that can be monitored for the ASA is platform dependent and can be determined by viewing the **show failover** command output.

Hello messages are exchanged during every interface poll frequency time period between the ASA failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.

- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

In Active/Active failover, this command is only valid within a context.

Examples

The following example enables monitoring on an interface named “inside”:

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure monitor-interface	Restores the default interface health monitoring for all interfaces.
failover interface-policy	Specifies the number or percentage of monitored interface that must fail for failover to occur.
failover polltime	Specifies the interval between hello messages on an interface (Active/Standby failover).
polltime interface	Specifies the interval between hello messages on an interface (Active/Active failover).
show running-config monitor-interface	Displays the **monitor-interface** commands in the running configuration.

more

To display the contents of a file, use the **more** command in privileged EXEC mode.

more { **/ascii** | **/binary** | **/ebcdic** / **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:** } *filename*

Syntax Description

/**ascii**	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
/**ebcdic**	(Optional) Displays binary files in EBCDIC.
disk0*:*	(Optional) Displays a file on the internal Flash memory.
disk1:	(Optional) Displays a file on the external Flash memory card.
filename	Specifies the name of the file to display.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series adaptive security appliance, the **flash** keyword is aliased to **disk0**.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a website.
https:	(Optional) Displays a file on a secure website.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.

Command Default

ASCII mode

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **more filesystem:** command prompts you to enter the alias of the local directory or file systems.

Note When you view a configuration file that you have saved using the **more** command, tunnel-group passwords in the configuration file appear in clear text.

Examples

The following example shows how to display the contents of a local file named “test.cfg”:

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
```

```
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

Command	Description
cd	Changes to the specified directory.
pwd	Displays the current working directory.

mount type cifs

To make a Common Internet File System (CIFS) accessible to the security appliance, use the **mount type cifs** command in global configuration mode. This command lets you enter mount cifs configuration mode. To un-mount the CIFS network file system, use the **no** form of this command.

mount *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*
[**mount**] **mount** *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*

Syntax Description

domain *domain-name*	(Optional) For CIFS file systems only, this argument specifies the Windows NT domain name. A maximum of 63 characters is permitted.
name	Specifies the name of an existing file system to be assigned to the Local CA.
password password	Identifies the authorized password for file-system mounting.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the CIFS file-system server.
share *sharename*	Explicitly identifies a specific server share (a folder) by name to access file data within a server.
status enable or **disable**	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
user *username*	The authorized username for file-system mounting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **mount** command uses the Installable File System (IFS) to mount the CIFS file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

The **mount** command attaches the CIFS file system on the security appliance to the UNIX file tree. Conversely, the **no mount** command detaches it.

The *mount-name* specified in the **mount** command is used by other CLI commands to refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of an existing mounted file system to save database files to non-flash storage.

The CIFS remote file-access protocol is compatible with the way applications share data on local disks and network file servers. Running over TCP/IP and using the Internet's global DNS, CIFS is an enhanced version of Microsoft's open, cross-platform Server Message Block (SMB) protocol, the native file-sharing protocol in the Windows operating systems.

Always exit from the root shell after using the **mount** command. The **exit** keyword in mount-cifs-config mode returns the user to global configuration mode.

In order to reconnect, remap your connections to storage.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

The following example mounts *cifs://amer;chief:big-boy@myfiler02/my_share* as the label, *cifs_share:*

```
ciscoasa
(config)#
mount cifs_share type CIFS

ciscoasa (config-mount-cifs)#
server myfiler02a
```

Related Commands

Command	Description
debug cifs	Logs CIFS debug messages.
debug ntdomain	Logs Web VPN NT Domain debug messages
debug webvpn cifs	Logs WebVPN CIFS debug messages.
dir all-filesystems	Displays the files of all filesystems mounted on the ASA.

mount type ftp

To make a File Transfer Protocol (FTP) file system accessible to the security appliance, use the **mount type ftp** command in global configuration mode to enter mount FTP configuration mode. The **no mount type ftp** command is used to unmount the FTP network file system.

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* { **status enable** | **status disable** } { **mode active** | **mode passive** } **username** *username* **password** *password*

Syntax Description

mode active or **passive**	Identifies the FTP transfer mode as either active or passive.
no	Removes an already mounted FTP file system, rendering it inaccessible.
password password	Identifies the authorized password for file-system mounting.
path *pathname*	Specifies the directory pathname to the specified FTP file-system server. The pathname cannot contain spaces.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the FTPFS file-system server.
status enable or **disable**	Identifies the state of the file system as mounted or unmounted (available or unavailable).
username *username*	Specifies the authorized username for file-system mounting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **mount** *name* **type ftp** command uses the Installable File System (IFS) to mount the specified network file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

To confirm that the FTP file system actually is mounted, use the **dir all-filesystems** instruction

The mount-name specified in the **mount** command is used when other CLI commands refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage

for the local certificate authority, needs the mount name of a mounted file system to save database files to non-flash storage.

Note Using the **mount** command when you create an FTP-type mount requires that the FTP server must have a UNIX directory listing style. Microsoft FTP servers have the MS-DOS directory listing style as their default.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

This example mounts *ftp://amor;chief:big-kid@myfiler02* as the label, *my ftp:*

```
ciscoasa
(config)#
mount myftp type ftp server myfiler02a path status enable username chief password big-kid
```

Related Commands

Command	Description
debug webvpn	Logs WebVPN debugging messages.
ftp mode passive	Controls interaction between the FTP client on the ASA and the FTP server.

mroute

To configure a static multicast route, use the **mroute** command in global configuration mode. To remove a static multicast route, use the **no** form of this command.

mroute *src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]
no *mroute src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]

Syntax Description

dense *output_if_name*	(Optional) The interface name for dense mode output. The **dense** *output_if_name* keyword and argument pair is only supported for SMR stub multicast routing (igmp forwarding).
distance	(Optional) The administrative distance of the route. Routes with lower distances have preference. The default is 0.
in_if_name	Specifies the incoming interface name for the mroute.
rpf_addr	Specifies the incoming interface for the mroute. If the RPF address PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-addr* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system.
smask	Specifies the multicast source network address mask.
src	Specifies the IP address of the multicast source.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command lets you statically configure where multicast sources are located. The ASA expects to receive multicast packets on the same interface as it would use to send unicast packets to a specific source. In some cases, such as bypassing a route that does not support multicast routing, multicast packets may take a different path than the unicast packets.

Static multicast routes are not advertised or redistributed.

Use the **show mroute** command displays the contents of the multicast route table. Use the **show running-config mroute** command to display the mroute commands in the running configuration.

Examples

The following example shows how configure a static multicast route using the **mroute** command:

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the configuration.
show mroute	Displays the IPv4 multicast routing table.
show running-config mroute	Displays the **mroute** commands in the configuration.

mschapv2-capable

To enable MS-CHAPv2 authentication requests to the RADIUS server, use the **mschapv2-capable** command in aaa-server host configuration mode. To disable MS-CHAPv2, use the **no** form of this command.

mschapv2-capable
nomschapv2-capable

Syntax Description

This command has no arguments or keywords.

Command Default

MS-CHAPv2 is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

To enable MS-CHAPv2 as the protocol used between the ASA and the RADIUS server for a VPN connection, password management must be enabled in the tunnel-group general-attributes. Enabling password management generates an MS-CHAPv2 authentication request from the ASA to the RADIUS server. See the description of the **password-management** command for details.

If you use double authentication and enable password management in the tunnel group, then the primary and secondary authentication requests include MS-CHAPv2 request attributes. If a RADIUS server does not support MS-CHAPv2, then you can configure that server to send a non-MS-CHAPv2 authentication request by using the **no mschapv2-capable** command.

Examples

The following example disables MS-CHAPv2 for the RADIUS server authsrv1.cisco.com:

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server for a AAA server group.
password-management	When you configure the password-management command, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password.
secondary-authentication-server-group	Specifies the secondary AAA server group, which cannot be an SDI server group.

msie-proxy except-list

To configure browser proxy exception list settings for a local bypass on the client device, enter the **msie-proxy except-list** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy except-list { **value** *server* [*:port*] | **none** }
nomsie-proxyexcept-list

Syntax Description

none	Indicates that there is no IP address/hostname or port and prevents inheriting an exception list.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client device. The port number is optional.

Command Default

By default, msie-proxy except-list is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to set a Microsoft Internet Explorer proxy exception list, consisting of the server at IP address 192.168.20.1, using port 880, for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy local-bypass

To configure browser proxy local-bypass settings for a client device, enter the **msie-proxy local-bypass** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy local-bypass { **enable** | **disable** }
no msie-proxy local-bypass { **enable** | **disable** }

Syntax Description

disable	Disables browser proxy local-bypass settings for a client device.
enable	Enables browser proxy local-bypass settings for a client device.

Command Default

By default, msie-proxy local-bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to enable Microsoft Internet Explorer proxy local-bypass for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
```

ciscoasa(config-group-policy)#

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy lockdown

To hide the Connections tab in Microsoft Internet Explorer and the system proxy tab in the Settings app for the duration of an AnyConnect VPN session or to leave it unchanged, use the **msie-proxy lockdown** command in group-policy configuration mode.

msie-proxy lockdown [**enable** | **disable**]

Syntax Description

disable	Leaves the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app unchanged.
enable	Hides the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app for the duration of an AnyConnect VPN session.

Command Default

The default value of this command in the default group policy is enable. Each group policy inherits its default values from the default group policy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.2(3)	This command was added.

Usage Guidelines

Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. In addition, from Windows 10 version 1703 (or later), enabling this feature also hides the system proxy tab in the Settings app for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab in Microsoft Internet Explorer and system proxy tab in the Settings app unchanged.

To use this feature, you must also specify a private-side proxy.

Note Hiding the system proxy tab in the Settings app for the duration of an AnyConnect VPN session needs AnyConnect version 4.7.03052 or later.

This command makes a temporary change to the user registry for the duration of the AnyConnect VPN session. When AnyConnect closes the VPN session, it returns the registry to the state it was in before the session.

You might enable this feature to prevent users from specifying a proxy service and changing LAN settings. Preventing user access to these settings enhances endpoint security during the AnyConnect session.

Refer to the Cisco Secure Client Administrator Guide , or the release notes for your mobile device for further information about proxy settings.

Examples

The following example hides the Connections tab for the duration of the AnyConnect session:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

The following example leaves the Connections tab unchanged:

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

Related Commands

Command	Description
msie-proxy except-list	Specifies an exception list of proxy servers for browser on the client device.
msie-proxy local-bypass	Bypasses the local browser proxy settings configured on the client device.
msie-proxy method	Specifies the browser proxy actions for a client device.
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file that defines the proxy servers.
msie-proxy server	Configures proxy server for browser on the client device.
show running-config group-policy	Shows the group policy settings in the running configuration.

msie-proxy method

To configure the browser proxy actions ("methods") for a client device, enter the **msie-proxy method** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]
no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url** }

Note See the Usage Guidelines section for qualifications that apply to this syntax.

Syntax Description

auto-detect	Enables the use of automatic proxy server detection in the browser for the client device.
no-modify	Leaves the HTTP browser proxy server setting in the browser unchanged for this client device.
no-proxy	Disables the HTTP proxy setting in the browser for the client device.
use-pac-url	Directs the browser to retrieve the HTTP proxy server setting from the proxy auto-configuration file URL specified in the **msie-proxy pac-url** command.
use-server	Sets the HTTP proxy server setting in the browser to use the value configured in the **msie-proxy server** command.

Command Default

The default method is use-server.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The use-pac-url option was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number can contain up to 100 characters.

This command supports the following combinations of options:

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. The .pac file resides on a web server. When you specify **use-pac-url**, the browser uses the .pac file to determine the proxy settings. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure auto-detect as the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

The following example configures the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup to use the server QAserver, port 1001 as the server for the client PC:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file.
msie-proxy server	Configures a browser proxy server and port for a client device.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy pac-url

To tell a browser where to look for proxy information, enter the **msie-proxy pac-url** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy pac-url { **none** | **value** *url* }
nomsie-proxypac-url

Syntax Description

none	Specifies that there is no URL value.
value *url*	Specifies the URL of the website at which the browser can get the proxy auto-configuration file that defines the proxy server or servers to use.

Command Default

The default value is none.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Requirements

To use the proxy auto-configuration feature, the remote user must use the Cisco AnyConnect VPN Client. To enable the use of the proxy auto-configuration URL, you must also configure the **msie-proxy method** command with the **use-pac-url** option.

Why Use This Command

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.

- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

How to Use the Proxy Auto-Configuration Feature

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file. Then, when you specify **use-pac-url** in the **msie-proxy method** command, the browser uses the .pac file to determine the proxy settings.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure a browser to get its proxy setting from the URL www.example.com for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

The following example disables the proxy auto-configuration feature for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy method	Configures the browser proxy actions (“methods”) for a client device.
msie-proxy server	Configures a browser proxy server and port for a client device.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy server

To configure a browser proxy server and port for a client device, enter the **msie-proxy server** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy server { **value** *server* [*:port*] | **none** }
nomsie-proxyserver

Syntax Description

none	Indicates that there is no IP address/hostname or port specified for the proxy server and prevents inheriting a server.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client device. The port number is optional.

Command Default

By default, no msie-proxy server is specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Refer to the Cisco Secure Client Administrator Guide , *Release 3.1* or the release notes for your mobile device for further information about proxy settings.

Examples

The following example shows how to configure the IP address 192.168.10.1 as a Microsoft Internet Explorer proxy server, using port 880, for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

mtu

To specify the maximum transmission unit for an interface, use the **mtu** command in global configuration mode. To reset the MTU block size to 1500 for Ethernet interfaces, use the **no** form of this command. This command supports IPv4 and IPv6 traffic.

mtu*interface_namebytes*
nomtu*interface_namebytes*

Syntax Description

bytes	Number of bytes in the MTU; valid values are from 64 to 9198 bytes (9000 for the Secure Client and Firepower 9300 ASA security module).
interface_name	Internal or external network interface name.

Command Default

The default *bytes* is 1500 for Ethernet interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.1(6)	The maximum MTU was changed from 65535 to 9198 (or 9000, depending on your model).

Usage Guidelines

The **mtu** command lets you to set the payload size (not including Layer 2 headers or VLAN tagging) that is sent on a connection. Data that is larger than the MTU value is fragmented before being sent. The default MTU is 1500 bytes for Ethernet interfaces (which is also the maximum without jumbo frame reservation). In this case, the size of the packet with Layer 2 headers (14 bytes) and VLAN tagging (4 bytes) is 1518 bytes. This value is sufficient for most applications, but you can pick a lower number if network conditions require it.

The ASA supports IP path MTU discovery (as defined in RFC 1191), which allows a host to dynamically discover and cope with the differences in the maximum allowable MTU size of the various links along the path. Sometimes, the ASA cannot forward a datagram because the packet is larger than the MTU that you set for the interface, but the “don’t fragment” (DF) bit is set. The network software sends a message to the sending host, alerting it to the problem. The host has to fragment packets for the destination so that they fit the smallest packet size of all the links along the path.

When using the Layer 2 Tunneling Protocol (L2TP), we recommend that you set the MTU size to 1380 to account for the L2TP header and IPsec header length.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Starting in Version 9.1(6), the maximum MTU that the ASA can use is 9198 bytes. This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems. If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value.

Examples

This example shows how to specify the MTU for an interface:

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
show running-config mtu	Displays the current maximum transmission unit block size.

mtu cluster

To set the maximum transmission unit of the cluster control link, use the **mtu cluster** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mtu cluster *bytes*
no mtu cluster [*bytes*]

Syntax Description

bytes	Specifies the maximum transmission unit for the cluster control link interface, between 64 and 65,535 bytes. The default MTU is 1500 bytes.

Command Default

The default MTU is 1500 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation using the **jumbo-frame reservation** command.

This command is a global configuration command, but is also part of the bootstrap configuration, which is not replicated between units.

Examples

The following example sets the cluster control link MTU to 9000 bytes:

```
ciscoasa(config)# mtu cluster 9000
```

Related Commands

Command	Description
cluster-interface	Identifies the cluster control link interface.
jumbo frame-reservation	Enables use of jumbo Ethernet frames.

multicast boundary

To configure a multicast boundary for administratively-scoped multicast addresses, use the **multicast boundary** command in interface configuration mode. To remove the boundary, use the **no** form of this command. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains.

multicast boundary *acl* [**filter-autorp**]
no multicast boundary *acl* [**filter-autorp**]

Syntax Description

acl	Specifies an access list name or number. The access list defines the range of addresses affected by the boundary. Use only standard ACLs with this command; extended ACLs are not supported.
filter-autorp	Filters Auto-RP messages denied by the boundary ACL. If not specified, all Auto-RP messages are passed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use this command to configure an administratively scoped boundary on an interface to filter multicast group addresses in the range defined by the *acl* argument. A standard access list defines the range of addresses affected. When this command is configured, no multicast data packets are allowed to flow across the boundary in either direction. Restricting multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Examples

The following example sets up a boundary for all administratively scoped addresses and filters the Auto-RP messages:

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

multicast-routing

To enable IP multicast routing on the ASA, use the **multicast routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

multicast-routing
nomulticast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

The **multicast-routing** command enables PIM and IGMP on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **multicast-routing** command enables PIM and IGMP on all interfaces.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.If the security appliance is the PIM RP, use the untranslated outside address of the security appliance as the RP address.

The number of entries in the multicast routing tables are limited by the amount of RAM on the system. <xref> lists the maximum number of entries for specific multicast tables based on the amount of RAM on the security appliance. Once these limits are reached, any new entries are discarded.

Table 6: Entry Limits for Multicast Tables (Combined Static and Dynamic Entries)

Table	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP Groups	1000	3000	5000

Table	16 MB	128 MB	128+ MB
PIM Routes	3000	7000	12000

Examples

The following example enables IP multicast routing on the ASA:

```
ciscoasa(config)# multicast-routing
```

Related Commands

Command	Description
igmp	Enables IGMP on an interface.
pim	Enables PIM on an interface.

mus

To specify the IP range and interface on which the ASA identifies the WSA, use the **mus** command in global configuration mode. To turn the service off, use the **no** form of this command. This command supports IPv4 and IPv6 traffic. Only WSAs found on the specified subnet and interface are registered.

mus *IPv4 address IPv4 mask interface_name*
no mus *IPv4 address IPv4 mask interface_name*

Note To function as expected, this command requires a release of the AsyncOS for Web version 7.0 that provides AnyConnect Secure Mobility licensing support for the Secure Client. It also requires an AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

The following commands are possible:

- A.B.C.D—The IP address of WSA authorized to access ASA.
- host—The client periodically checks connectivity to the Web Security appliance by sending a request to a fictitious host. By default, the fictitious host URL is mus.cisco.com. When AnyConnect Security Mobility is enabled, the Web Security appliance intercepts requests destined for the fictitious host and replies to the client.
- password—Configure WSA password.
- server—Configure WSA server

Examples

The following example allows WSA servers on the 1.2.3.x subnet to access secure mobility solutions on the *inside* interface:

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

Related Commands

Command	Description
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
mus server	Specifies the port on which the ASA listens for WSA communication.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus host

To specify the MUS hostname on the ASA, enter the **mus host** command in global configuration mode. This is the telemetry URL sent from the ASA to the Secure Client. The Secure Clients use this URL to contact the WSA in the private network for MUS-related services. To remove any commands entered with this command, use the **no mus host** command.

mus host *host name*
nomushost

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

You can enable AnyConnect Secure Mobility for a given port. The WSA port values are 1 through 21000. If a port is not specified in the command, port 11999 is used.

You must configure AnyConnect Secure Mobility shared secret before executing this command.

Note To function as expected, this command requires a release of the AsyncOS for Web version 7.0 that provides AnyConnect Secure Mobility licensing support for the Secure Client. It also requires an AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Examples

The following example shows how to enter the AnyConnect Secure Mobility host and WebVPN command submode:

```
ciscoasa(config)# webvpn

ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside

ciscoasa(config-webvpn)# mus password abcdefgh123
```

```
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus password

To set up shared secred for AnyConnect Secure Mobility communications, enter the **mus password** command in global configuration mode. To remove the shared secred, use the **no mus password** command.

muspassword
nomuspassword

Note To function as expected, this command requires a release of the AsyncOS for Web version 7.0 that provides AnyConnect Secure Mobility licensing support for the Secure Client. It also requires an AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Syntax Description

This command has no arguments or keywords.

Command Default

.The valid password is defined by the regular expression [0-9, a-z, A-Z,:;_/-]{8,20}. The overall length of the shared secret password is a minimum of 8 characters and maximum of 20 characters.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

This WebVPN submode lets you configure global settings for WebVPN. You can set up the shared secret for AnyConnect Secure Mobility communications.

Examples

The following example shows how to enter an AnyConnect Secure Mobility password and WebVPN command submode:

```
ciscoasa
(config)#
 mus password <password_string>
ciscoasa
(config-webvpn)#
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus server	Specifies the port on which the ASA listens for WSA communication.
show webvpn mus	Displays information about the active WSA connection security appliance.

mus server

To specify the port on which the ASA listens for WSA communication, enter the **mus server** command in global configuration mode. To remove any commands entered with this command, use the **no mus server** command.

musserverenable
nomusserverenable

Note To function as expected, this command requires a release of the AsyncOS for Web version 7.0 that provides AnyConnect Secure Mobility licensing support for the Secure Client. It also requires an AnyConnect release that supports AnyConnect Secure Mobility, ASA 8.3, and ASDM 6.3.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

You must specify a port the AnyConnect Secure Mobility service uses. The communication between the ASA and the WSA is by a secure SSL connection on a port specified by the administrator with values of 1 through 21000.

You must configure AnyConnect Secure Mobility shared secret before executing this command.

Examples

The following example shows how to enter the AnyConnect Secure Mobility password and WebVPN command submode:

```
ciscoasa
(config-webvpn)#
mus server enable
?
webvpn mode commands/options
```

```
 port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

Related Commands

Command	Description
mus	Specifies the IP range and interface on which the ASA identifies the WSA.
mus password	Sets up shared secret for AnyConnect Secure Mobility communications.
show webvpn mus	Displays information about the active WSA connection security appliance.

PART III

N - R Commands

n

nac-authentication-server-group (Deprecated)

To identify the group of authentication servers to be used for Network Admission Control posture validation, use the **nac-authentication-server-group** command in tunnel-group general-attributes configuration mode. To inherit the authentication server group from the default remote access group, access the alternative group policy from which to inherit it, then use the **no** form of this command.

nac-authentication-server-group *server-group*
no nac-authentication-server-group

Syntax Description

server-group	Name of the posture validation server group, as configured on the ASA using the **aaa-server host** command. The name must match the server-tag variable specified in that command.

Command Default

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(1)	This command was deprecated. The **authentication-server-group** command in nac-policy-nac-framework configuration mode replaced it.

Usage Guidelines

Configure at least one Access Control Server to support NAC. Use the **aaa-server** command to name the ACS group. Then use the **nac-authentication-server-group** command, using the same name for the server group.

Examples

The following example identifies acs-group1 as the authentication server group to be used for NAC posture validation:

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

The following example inherits the authentication server group from the default remote access group.

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
aaa-server	Creates a record of the AAA server or group and sets the host-specific AAA server attributes.
debug eap	Enables logging of EAP events to debug NAC messaging.
debug eou	Enables logging of EAP over UDP (EAPoUDP) events to debug NAC messaging.
debug nac	Enables logging of NAC events.
nac	Enables Network Admission Control on a group policy.

nac-policy (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To create or access a Cisco Network Admission Control (NAC) policy, and specify its type, use the **nac-policy** command in global configuration mode. To remove the NAC policy from the configuration, use the **no** form of this command.

nac-policy *nac-policy-name* **nac-framework**
no nac-policy *nac-policy-name* **nac-framework**

Syntax Description

nac-policy-name	Name of the NAC policy. Enter a string of up to 64 characters to name the NAC policy. The **show running-config nac-policy** command displays the name and configuration of each NAC policy already present on the security appliance.
nac-framework	Specifies the use of a NAC framework to provide a network access policy for remote hosts. A Cisco Access Control Server must be present on the network to provide NAC Framework services for the ASA. If you specify this type, the prompt indicates you are in config--nac-policy-nac-framework configuration mode. This mode lets you configure the NAC Framework policy.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
8.0(2)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use this command once for each NAC Appliance to be assigned to a group policy. Then use the **nac-settings** command to assign the NAC policy to each applicable group policy. Upon the setup of an IPsec or Cisco AnyConnect VPN tunnel, the ASA applies the NAC policy associated with the group policy in use.

You cannot use the **no nac-policy** *name* command to remove a NAC policy if it is already assigned to one or more group policies.

Examples

The following command creates and accesses a NAC Framework policy named nac-framework1:

```
ciscoasa
(config)
# nac-policy nac-framework1 nac-framework
ciscoasa
(config-nac-policy-nac-framework)
```

The following command removes the NAC Framework policy named nac-framework1:

```
ciscoasa
(config)
# no nac-policy nac-framework1
ciscoasa
(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
show running-config nac-policy	Displays the configuration of each NAC policy on the ASA.
show nac-policy	Displays NAC policy usage statistics on the ASA.
clear nac-policy	Resets the NAC policy usage statistics.
nac-settings	Assigns a NAC policy to a group policy.
clear configure nac-policy	Removes all NAC policies from the running configuration except for those that are assigned to group policies.

nac-settings (Deprecated)

Note The last supported release for this command was Version 9.1(1).

To assign a NAC policy to a group policy, use the **nac-settings** command in group-policy configuration mode, as follows:

nac-settings { **value** *nac-policy-name* | **none** }
no nac-settings { **value** *nac-policy-name* | **none** }

Syntax Description

nac-policy-name	NAC policy to be assigned to the group policy. The NAC policy you name must be present in the configuration of the ASA. The **show running-config nac-policy** command displays the name and configuration of each NAC policy.
none	Removes the *nac-policy-name* from the group policy and disables the use of a NAC policy for this group policy. The group policy does not inherit the nac-settings value from the default group policy.
value	Assigns the NAC policy to be named to the group policy.

Command Default

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
8.0(2)	This command was added.
9.1(2)	This command was deprecated.

Usage Guidelines

Use the **nac-policy** command to specify the name and type of the NAC policy, then use this command to assign it to a group policy.

The **show running-config nac-policy** command displays the name and configuration of each NAC policy.

The ASA automatically enables NAC for a group policy when you assign a NAC policy to it.

Examples

The following command removes the *nac-policy-name* from the group policy. The group policy inherits the *nac-settings* value from the default group policy:

```
ciscoasa(config-group-policy)
# no nac-settings
ciscoasa(config-group-policy)
```

The following command removes the *nac-policy-name* from the group policy and disables the use of a NAC policy for this group policy. The group policy does not inherit the nac-settings value from the default group policy.

```
ciscoasa(config-group-policy)
# nac-settings none
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
show running-config nac-policy	Displays the configuration of each NAC policy on the ASA.
show nac-policy	Displays NAC policy usage statistics on the ASA.
show vpn-session_summary.db	Displays the number IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

name (dynamic-filter blacklist or whitelist)

To add a domain name to the Botnet Traffic Filter blacklist or whitelist, use the **name** command in dynamic-filter blacklist or whitelist configuration mode. To remove the name, use the **no** form of this command. The static database lets you augment the dynamic database with domain names or IP addresses that you want to whitelist or blacklist.

name *domain_name*
no name *domain_name*

Syntax Description

domain_name	Adds a name to the blacklist. You can enter this command multiple times for multiple entries. You can add up to 1000 blacklist entries.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-filter blacklist or whitelist configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

After you enter the dynamic-filter whitelist or blacklist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as good names in a whitelist or bad names in a blacklist using the **address** and **name** commands.

You can enter this command multiple times for multiple entries. You can add up to 1000 blacklist and 1000 whitelist entries.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the *DNS host cache* . (This action is a background process, and does not affect your ability to continue configuring the ASA).

If you do not have a domain name server configured for the ASA, or it is unavailable, then you can alternatively enable DNS packet inspection with Botnet Traffic Filter snooping (see the **inspect dns dynamic-filter-snooping** command). With DNS snooping, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache. See the **inspect dns dynamic-filter-snooping** command for information about the DNS reverse lookup cache.

Entries in the DNS host cache have a time to live (TTL) value provided by the DNS server. The largest TTL value allowed is 1 day (24 hours); if the DNS server provides a larger TTL, it is truncated to 1 day maximum.

For the DNS host cache, after an entry times out, the ASA periodically requests a refresh for the entry.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.

Command	Description
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

name (global)

To associate a name with an IP address, use the **name** command in global configuration mode. To disable the use of the text names but not remove them from the configuration, use the **no** form of this command.

name *ip_address* [*name* [**description** *text*]]
no name *ip_address* [*name* [**description** *text*]]

Syntax Description

description	(Optional) Specifies a description for the ip address name.
ip_address	Specifies an IP address of the host that is named.
name	Specifies the name assigned to the IP address. Use characters a to z, A to Z, 0 to 9, a dash, and an underscore. The *name* must be 63 characters or less. Also, the *name* cannot start with a number.
text	Specifies the text for the description.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.0(4)	This command was enhanced to include an optional description.
8.3(1)	You can no longer use a named IP address in a **nat** command or an **access-list** command; you must use **object network** names instead. Although **network-object** commands in an object group accept **object network** names, you can still also use a named IP address identified by the **name** command.

Usage Guidelines

To enable the association of a name with an IP address, use the **names** command. You can associate only one name with an IP address.

You must first use the **names** command before you use the **name** command. Use the name command immediately after you use the names command and before you use the **write memory** command.

The **name** command lets you identify a host by a text name and map text strings to IP addresses. The **no name** command allows you to disable the use of the text names but does not remove them from the configuration. Use the **clear configure name** command to clear the list of names from the configuration.

To disable displaying **name** values, use the **no names** command.

Both the name and names commands are saved in the configuration.

The name command does not support assigning a name to a network mask. For example, this command would be rejected:

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```

Note None of the commands in which a mask is required can process a name as an accepted network mask.

Examples

This example shows that the **names** command allows you to enable use of the **name** command. The **name** command substitutes **sa_inside** for references to 192.168.42.3 and **sa_outside** for 209.165.201.3. You can use these names with the **ip address** commands when assigning IP addresses to the network interfaces. The **no names** command disables the **name** command values from displaying. Subsequent use of the **names** command again restores the **name** command value display.

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
names	Enables the association of a name with an IP address.
show running-config name	Displays the names associated with an IP address.

nameif

To provide a name for an interface, use the **nameif** command in interface configuration mode. To remove the name, use the **no** form of this command. The interface name is used in all configuration commands on the ASA instead of the interface type and ID (such as gigabitethernet0/1), and is therefore required before traffic can pass through the interface.

nameif *name*
no nameif

Syntax Description

name Sets a name up to 48 characters in length. The name is not case-sensitive. Do not use the names "Metrics_History" or "MH"; they cause ASDM to show the interface in a down state.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

For subinterfaces, you must assign a VLAN with the **vlan** command before you enter the **nameif** command.

You can change the name by reentering this command with a new value. Do not enter the **no** form, because that command causes all commands that refer to that name to be deleted.

Examples

The following example configures the names for two interfaces to be "inside" and "outside:"

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.
security-level	Sets the security level for the interface.
vlan	Assigns a VLAN ID to a subinterface.

names

To enable the association of a name with an IP address, use the **names** command in global configuration mode. You can associate only one name with an IP address. To disable displaying **name** values, use the **no names** command.

names
no names

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To enable the association of a name with an IP address, use the **names** command. You can associate only one name with an IP address.

You must first use the **names** command before you use the **name** command. Use the name command immediately after you use the names command and before you use the **write memory** command.

To disable displaying **name** values, use the **no names** command.

Both the name and names commands are saved in the configuration.

Examples

This example shows that the **names** command allows you to enable use of the **name** command. The **name** command substitutes **sa_inside** for references to 192.168.42.3 and **sa_outside** for 209.165.201.3. You can use these names with the **ip address** commands when assigning IP addresses to the network interfaces. The **no names** command disables the **name** command values from displaying. Subsequent use of the **names** command again restores the **name** command value display.

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
```

```
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.
show running-config name	Displays a list of names associated with IP addresses.
show running-config names	Displays the IP address-to-name conversions.

name-separator (pop3s, imap4s, smtps) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify a character as a delimiter between the e-mail and VPN username and password, use the **name-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the **no** version of this command.

name-separator [*symbol*]
no name-separator

Syntax Description

symbol	(Optional) The character that separates the e-mail and VPN usernames and passwords. Choices are "@," (at) "|" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Command Default

The default is ":" (colon).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s	• Yes	• —	• Yes	• —	—
Imap4s	Yes	—	Yes	—	—
Smtps	Yes	—	Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

The name separator must be different from the server separator.

Examples

The following example shows how to set a hash (#) as the name separator for POP3S:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)# name-separator #
```

Related Commands

Command	Description
server-separator	Separates the e-mail and server names.

name-server

To identify one or more DNS servers so that the ASA can resolve hostnames to IP addresses, use the **name-server** command in dns server-group configuration mode. To remove a server or servers, use the **no** form of this command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] [*interface_name*]
no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the interface name through which the ASA communicates with the server. If you do not specify the interface, the ASA checks the data routing table; if there are no matches, it then checks the management-only routing table.
ip_address	Specifies the DNS server IP address. You can specify up to six addresses as separate commands, or for convenience, up to six addresses in one command separated by spaces. If you enter multiple servers in one command, the ASA saves each server in a separate command in the configuration. The ASA tries each DNS server in order until it receives a response.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(1)	The *interface_name* argument was added.

Usage Guidelines

To enable DNS lookup on an interface, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used.

By default, the ASA uses the **dns server-group DefaultDNS** server group for outgoing requests. You can change the default server group using the **dns-group** command. Other server groups can be associated with

specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. Other DNS server groups can be configured for VPN tunnel groups. See the **tunnel-group** command for more information.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

If you do not specify the interface for the **name-server**, the ASA checks the data routing table; if there are no matches, it then checks the management-only routing table. Note that if you have a default route through a data interface, all DNS traffic will match that route and never check the management-only routing table. In this scenario, always specify the interface if you need to access the server through a management interface.

Examples

The following example adds three DNS servers to the group “DefaultDNS”:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

The ASA saves the configuration as separate commands, as follows:

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

To add two additional servers, you can enter them as one command:

```
ciscoasa(config)# dns server-group
DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

To delete multiple servers you can enter them as multiple commands or as one command, as follows:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# no
 name-server 10.5.1.1 10.8.3.8
```

Related Commands

Command	Description
domain-name	Sets the default domain name.
retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
timeout	Specifies the amount of time to wait before trying the next DNS server.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

nat (global)

To configure twice NAT for IPv4, IPv6, or between IPv4 and IPv6 (NAT64), use the **nat** command in global configuration mode. To remove the twice NAT configuration, use the **no** form of this command.

For static NAT:

nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source static** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **any** }] [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *real_src_mapped_dest_svc_obj* | **any** } *mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*

no nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source static** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **any** }] [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *real_src_mapped_dest_svc_obj* | **any** } *mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*

For dynamic NAT:

nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**] } [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *mapped_dest_svc_obj* *real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*

no nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**] } [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *mapped_dest_svc_obj* *real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*

or

no nat { *line* **after-auto** *line* }

Syntax Description

(*real_ifc***,***mapped_ifc***)**	(Optional) Specifies the real and mapped interfaces. If you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword **any** for one or both of the interfaces. For bridge group member interfaces (in transparent or routed mode), you must specify the real and mapped interfaces; you cannot use **any**. Because twice NAT can translate both the source and destination addresses, these interfaces are better understood to be the source and destination interfaces.
after-auto	Inserts the rule at the end of section 3 of the NAT table, after the network object NAT rules. By default, twice NAT rules are added to section 1. You can insert a rule anywhere in section 3 using the *line* argument.

any	(Optional) Specifies a wildcard value. The main uses for **any** are: • Interfaces—You can use **any** for one or both interfaces (**(any,outside)**, for example). If you do not specify the interfaces, then **any** is the default. However, **any** does not apply to bridge group member interfaces, and **any** is not available in transparent mode. • Static NAT source real and mapped IP addresses—You can specify **source static any any** to enable identity NAT for all addresses. • Dynamic NAT or PAT source real addresses—You can translate all addresses on the source interface by specifying **source dynamic any** *mapped_obj* For static NAT, although **any** is also available for the real source port/mapped destination port, or for the source or destination real address (without **any** as the mapped address), these uses might result in unpredictable behavior. **Note** The definition of "any" traffic (IPv4 vs. IPv6) depends on the rule. Before the ASA performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the ASA can determine the value of **any** in a NAT rule. For example, if you configure a rule from "any" to an IPv6 server, and that server was mapped from an IPv4 address, then **any** means "any IPv6 traffic." If you configure a rule from "any" to "any," and you map the source to the interface IPv4 address, then **any** means "any IPv4 traffic" because the mapped interface address implies that the destination is also IPv4.
block-allocation	Enables port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with **round-robin**, but you cannot use the **extended** or **flat** [**include-reserve**] options. You also cannot use interface PAT fallback.
description *desc*	(Optional) Provides a description up to 200 characters.
destination	(Optional) Configures translation for the destination address. Although the main feature of twice NAT is the inclusion of the destination IP address, the destination address is optional. If you do specify the destination address, you can configure static translation for that address or just use identity NAT for it. You might want to configure twice NAT without a destination address to take advantage of some of the other qualities of twice NAT, including the use of network object groups for real addresses, or manually ordering of rules. For more information, see the CLI configuration guide.

dns	(Optional) Translates DNS replies. Be sure DNS inspection is enabled (**inspect dns**) (it is enabled by default). You cannot configure the **dns** keyword if you configure a **destination** address. Do not use this option with PAT rules. See the CLI configuration guide for more information.
dynamic	Configures dynamic NAT or PAT for the source addresses. The destination translation is always static.
extended	(Optional) Enables extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service* , as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.
flat [**include-reserve**] **include-reserve**	(Optional, pre-9.15) Enables use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also specify the **include-reserve** keyword. (9.15+) Starting with 9.15, flat is the default and unconfigurable behavior for a PAT pool. The **include-reserve** keyword is independent from the flat keyword, so you can still elect to include the reserved ports, 1-1023, in the PAT pool.
inactive	(Optional) To make this rule inactive without having to remove the command, use the **inactive** keyword. To reactivate it, reenter the whole command without the **inactive** keyword.
interface [**ipv6**]	(Optional) Uses the interface IP address as the mapped address. If you specify **ipv6**, then the IPv6 address of the interface is used. For the dynamic NAT source mapped address, if you specify a mapped object or group followed by the **interface** keyword, then the IP address of the mapped interface is only used if all other mapped addresses are already allocated. For dynamic PAT, you can specify **interface** alone for the source mapped address. For static NAT with port translation (source or destination), be sure to also configure the **service** keyword. For this option, you must configure a specific interface for the *mapped_ifc* . This option is not available in transparent mode. In routed mode, you cannot use this option if the destination interface is a bridge group member.

line	(Optional) Inserts a rule anywhere in section 1 of the NAT table. By default, the NAT rule is added to the end of section 1 (see the CLI configuration guide for more information). If you want to add the rule into section 3 instead (after the network object NAT rules), then use the **after-auto** *line* option.
mapped_dest_svc_obj	(Optional) For dynamic NAT/PAT, specifies the mapped destination port (the destination translation is always static). See the **service** keyword for more information.
mapped_object	Identifies the mapped network object or object group (**object network** or **object-group network**). For dynamic NAT, you typically configure a larger group of addresses to be mapped to a smaller group. **Note** The mapped object or group cannot contain a subnet.You can share this mapped IP address across different dynamic NAT rules, if desired.You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address. For dynamic PAT, configure a group of addresses to be mapped to a single address. You can either translate the real addresses to a single mapped address of your choosing, or you can translate them to the mapped interface address. If you want to use the interface address, do not configure a network object for the mapped address; instead use the **interface** keyword. For static NAT, the mapping is typically one-to-one, so the real addresses have the same quantity as the mapped addresses. You can, however, have different quantities if desired. For more information, see the CLI configuration guide.
mapped_src_real_dest_svc_obj	(Optional) For static NAT, specifies the either the mapped source port, the real destination port, or both together. See the **service** keyword for more information.
net-to-net	(Optional) For static NAT 46, specify **net-to-net** to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this keyword.
no-proxy-arp	(Optional) For static NAT, disables proxy ARP for incoming packets to the mapped IP addresses.
pat-pool *mapped_obj*	(Optional) Enables a PAT pool of addresses; all addresses in the object are used as PAT addresses. For dynamic NAT, you can configure the PAT pool as a fallback method. You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
real_dest_svc_obj	(Optional) For dynamic NAT/PAT, specifies the real destination port (the destination translation is always static). See the **service** keyword for more information.

real_ifc	(Optional) Specifies the name of the interface where packets may originate. For source option. For the source option, the origin_ifc is the real interface. For the destination option, the real_ifc is the mapped interface.
real_object	Identifies the real network object or object group (**object network** or **object-group network**). You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
real_src_mapped_dest_svc_obj	(Optional) For static NAT, specifies the either the real source port, the mapped destination port, or both together. See the **service** keyword for more information.
round-robin	(Optional) Enables round-robin address allocation for a PAT pool. By default, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns an address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
route-lookup	(Optional) For identity NAT in routed mode, determines the egress interface using a route lookup instead of using the interface specified in the NAT command. If you do not specify interfaces in the NAT command, a route lookup is used by default.
service	(Optional) Specifies the port translation. • Dynamic NAT and PAT—Dynamic NAT and PAT do not support (additional) port translation. However, because the *destination* translation is always static, you can perform port translation for the destination port. A service object (**object service**) can contain both a source and destination port, but only the destination port is used in this case. If you specify the source port, it will be ignored. • Static NAT with port translation—You should specify *either* the source *or* the destination port for both service objects. You should only specify *both* the source and destination ports if your application uses a fixed source port (such as some DNS servers); but fixed source ports are rare. For source port translation, the objects must specify the source service. The order of the service objects in the command in this case is **service** *real_port mapped_port* . For destination port translation, the objects must specify the destination service. The order of the service objects in this case is **service** *mapped_port real_port* . In the rare case where you specify both the source and destination ports in the object, the first service object contains the real source port/mapped destination port; the second service object contains the mapped source port/real destination port. See the "Usage Guidelines" section for more information about "source" and "destination" terminology. For identity port translation, simply use the same service object for both the real and mapped ports (source and/or destination ports, depending on your configuration). The "not equal" (**neq**) operator is not supported. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP).

source	Configures translation for the source address.
static	Configures static NAT or static NAT with port translation.
unidirectional	(Optional) For static NAT, makes the translarion unidirection from the source to the destination; the destination addresses cannot initiate traffic to the source addresses. This option might be useful for testing purposes.

Command Default

- By default, the rule is added to the end of section 1 of the NAT table.
- The default value of *real_ifc* and *mapped_ifc* is **any**, which applies the rule to all interfaces.
- (8.3(1), 8.3(2), and 8.4(1)) The default behavior for identity NAT has proxy ARP disabled. You cannot configure this setting. (8.4(2) and later) The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired.
- If you specify an optional interface, then the ASA uses the NAT configuration to determine the egress interface. (8.3(1) through 8.4(1)) The only exception is for identity NAT, which always uses a route lookup, regardless of the NAT configuration. (8.4(2) and later) For identity NAT, the default behavior is to use the NAT configuration, but you have the option to always use a route lookup instead.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
8.3(2)	When migrating from a pre-8.3 NAT exemption configuration, the keyword **unidirectional** is added for the resulting static identity NAT rule.
8.4(2)/8.5(1)	The **no-proxy-arp**, **route-lookup**, **pat-pool**, and **round-robin** keywords were added. The default behavior for identity NAT was changed to have proxy ARP enabled, matching other static NAT rules. For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed.

Release	Modification
8.4(3)	The **extended**, **flat**, and **include-reserve** keywords were added. When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. *This feature is not available in 8.5(1).*
9.0(1)	NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6. Translating between IPv4 and IPv6 is not supported in transparent mode. We added the **interface ipv6** option and the **net-to-net** option.
9.5(1)	The **block-allocation** keyword was added.
9.15(1)	The **flat** keyword was removed, and the **include-reserve** keyword is no longer a sub-parameter of flat. All PAT pools now use a flat port range, 1024-65535, and you can optionally include the reserved ports, 1-1023.
9.17(1)	You can specify an FQDN network object as the translated (mapped) destination.

Usage Guidelines

Usage Guideline

Twice NAT lets you identify both the source and destination address in a single rule. Specifying both the source and destination addresses lets you specify that a source address should be translated to A when going to destination X, but be translated to B when going to destination Y, for example.

Note For static NAT, the rule is bidirectional, so be aware that "source" and "destination" are used in commands and descriptions throughout this guide even though a given connection might originate at the "destination" address. For example, if you configure static NAT with port translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then in the command, you must specify the *source* ports to be translated (real: 23, mapped: 2323). You specify the source ports because you specified the Telnet server address as the **source** address.

The destination address is optional. If you specify the destination address, you can either map it to itself (identity NAT), or you can map it to a different address. The destination mapping is always a static mapping.

Twice NAT also lets you use service objects for static NAT with port translation; network object NAT only accepts inline definition.

For detailed information about the differences between twice NAT and network object NAT, see the CLI configuration guide.

Twice NAT rules are added to section 1 of the NAT rules table, or if specified, section 3. For more information about NAT ordering, see the CLI configuration guide.

Mapped Address Guidelines

The mapped IP address pool cannot include:

- The mapped interface IP address. If you specify **any** interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), use the **interface** keyword instead of the IP address.
- (Transparent mode) The management IP address.

- (Dynamic NAT) The standby interface IP address when VPN is enabled.
- Existing VPN pool addresses.

Prerequisites

- For both the real and mapped addresses, configure network objects or network object groups (the **object network** or **object-group network** command). Network object groups are particularly useful for creating a mapped address pool with discontinuous IP address ranges or multiple hosts or subnets. You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
- For static NAT with port translation, configure TCP or UDP service objects (the **object service** command).

Objects and object groups used in NAT cannot be undefined; they must include IP addresses.

Clearing Translation Sessions

If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using clear xlate command. However, clearing the translation table disconnects all of the current connections.

PAT Pool Guidelines

- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record, and the PAT rule to use is ambiguous.
- (Pre-9.15) If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. (8.4(3) and later, not including 8.5(1) or 8.6(1)) If you have a lot of traffic that uses the lower port ranges, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.
- (9.15+) Ports are mapped to an available port in the 1024 to 65535 range. You can optionally include the reserved ports, those below 1024, to make the entire port range available for translations.

When operating in a cluster, blocks of 512 ports per address are allocated to the members of the cluster, and mappings are made within these port blocks. If you also enable block allocation, the ports are distributed according to the block allocation size, whose default is also 512.

- If you enable block allocation for a PAT pool, port blocks are allocated in the 1024-65535 range only. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host.
- If you use an object group for the dynamic NAT mapped IP addresses, and the group includes host addresses, then enabling the PAT pool changes the use of those host addresses from PAT fallback to dynamic NAT.
- (8.4(3) and later, not including 8.5(1) or 8.6(1)) If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT and a flat range, then the other rule must also specify extended PAT and a flat range.

Exten ded PAT for a PAT Pool Guidelines

- Many application inspections do not support extended PAT. See the configuration guide for a complete list of unsupported inspections.
- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT-with-port-translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.
- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.
- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.

Round robin for a PAT Pool Guidelines

- (8.4(3) and later, not including 8.5(1) or 8.6(1)) If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. **Note**: This "stickiness" does not survive a failover. If the ASA fails over, then subsequent connections from a host may not use the initial IP address.
- (8.4(2), 8.5(1), and 8.6(1)) If a host has an existing connection, then subsequent connections from that host will likely use *different* PAT addresses for each connection because of the round robin allocation. In this case, you may have problems when accessing two websites that exchange information about the host, for example an e-commerce site and a payment site. When these sites see two different IP addresses for what is supposed to be a single host, the transaction may fail.

NAT and IPv6

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices. Note that you cannot perform NAT64/46 when the interfaces are members of the same bridge group.

- NAT66 (IPv6-to-IPv6)—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only).
- NAT46 (IPv4-to-IPv6)—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.4 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address.
- NAT64 (IPv6-to-IPv4)—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

Examples

The following example includes a host on the 10.1.2.0/24 network that accesses two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129:*port* . When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130:*port* .

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

The following example shows the use of source and destination ports. The host on the 10.1.2.0/24 network accesses a single host for both web services and Telnet services. When the host accesses the server for Telnet services, the real address is translated to 209.165.202.129:*port* . When the host accesses the same server for web services, the real address is translated to 209.165.202.130:*port* .

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# service
 tcp
 destination eq telnet
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1 destination
 static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# service
 tcp
 destination eq http
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2 destination
 static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

The following example shows the use of static interface NAT with port translation. Hosts on the outside access an FTP server on the inside by connecting to the outside interface IP address with destination port 65000 through 65004. The traffic is untranslated to the internal FTP server at 192.168.10.100:6500 through :65004. Note that you specify the source port range in the service object (and not the destination port) because you want to translate the source address and port as identified in the command; the destination port is “any.” Because static NAT is bidirectional, “source” and “destination” refers primarily to the command keywords; the actual source and destination address and port in a packet depends on which host sent the packet. In this example, connections are originated from outside to inside, so the “source” address and port of the FTP server is actually the destination address and port in the originating packet.

```
ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-obvject)# service tcp source range 65000 65004
ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-obvject)# host 192.168.10.100
ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

The following example configures dynamic NAT for an IPv6 inside network 2001:DB8:AAAA::/96 when accessing servers on the IPv4 209.165.201.1/27 network as well as servers on the 203.0.113.0/24 network:

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254
ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158
ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination static
 SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination static
 SERVERS_2 SERVERS_2
```

The following example configures interface PAT for inside network 192.168.1.0/24 when accessing outside IPv6 Telnet server 2001:DB8::23, and Dynamic PAT using a PAT pool when accessing any server on the 2001:DB8:AAAA::/96 network.

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200
ciscoasa(config)# object network TELNET_SVR
ciscoasa(config-network-object)# host 2001:DB8::23
ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23
ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
 static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL destination
 static SERVERS SERVERS
```

Related Commands

Command	Description
clear configure nat	Removes the NAT configuration (both twice NAT and network object NAT).
show nat	Displays NAT policy statistics.
show nat pool	Displays information about NAT pools.
show running-config nat	Shows the NAT configuration.
show xlate	Displays NAT session (xlate) information.
xlate block-allocation	Configures the PAT port block allocation characteristics.

nat (object)

To configure NAT for a network object, use the **nat** command in object network configuration mode. To remove the NAT configuration, use the **no** form of this command.

For dynamic NAT and PAT:

nat [(*real_ifc* , *mapped_ifc*)] **dynamic** { *mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**]] [**interface** [**ipv6**]] } [**dns**]

no nat [(*real_ifc* , *mapped_ifc*)] **dynamic** { *mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**]] [**interface** [**ipv6**]] } [**dns**]

For static NAT and static NAT with port translation:

nat [(*real_ifc* , *mapped_ifc*)] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [**ipv6**] } [**net-to-net**] [**dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

no nat [(*real_ifc* , *mapped_ifc*)] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [**ipv6**] } [**net-to-net**] [**dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

Syntax Description

(*real_ifc***,***mapped_ifc***)**	(Optional) For static NAT, specifies the real and mapped interfaces. If you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword **any** for one or both of the interfaces. Be sure to include the parentheses in your command. For bridge group member interfaces (in transparent or routed mode), you must specify the real and mapped interfaces; you cannot use **any**.
block-allocation	Enables port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with **round-robin**, but you cannot use the **extended** or **flat** [**include-reserve**] options. You also cannot use interface PAT fallback.
dns	(Optional) Translates DNS replies. Be sure DNS inspection (**inspect dns**) is enabled (it is enabled by default). This option is not available if you specify the **service** keyword (for static NAT). Do not use this option with PAT rules. For more information, see the CLI configuration guide.
dynamic	Configures dynamic NAT or PAT.

extended	(Optional) Enables extended PAT for a PAT pool. Extended PAT uses 65535 ports per *service* , as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.
flat [**include-reserve**] **include-reserve**	(Optional, pre-9.15) Enables use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also specify the **include-reserve** keyword. (9.15+) Starting with 9.15, flat is the default and unconfigurable behavior for a PAT pool. The **include-reserve** keyword is independent from the flat keyword, so you can still elect to include the reserved ports, 1-1023, in the PAT pool.
interface [**ipv6**]	(Optional) For dynamic NAT, if you specify a mapped IP address, object, or group followed by the **interface** keyword, then the IP address of the mapped interface is only used if all of the other mapped addresses are already allocated. For dynamic PAT, if you specify the **interface** keyword instead of a mapped IP address, object, or group, then you use the interface IP address for the mapped IP address. You must use this keyword when you want to use the interface IP address; you cannot enter it inline or as an object. If you specify **ipv6**, then the IPv6 address of the interface is used. For static NAT with port translation, you can specify the **interface** keyword if you also configure the **service** keyword. For this option, you must configure a specific interface for the *mapped_ifc* . You cannot specify **interface** in transparent mode. In routed mode, you cannot use this option if the destination interface is a bridge group member.
mapped_inline_host_ip	If you specify **dynamic**, then using a host IP address configures dynamic PAT. If you specify **static**, the netmask or range for the mapped network is the same as that of the real network. For example, if the real network is a host, then this address will be treated as a host address. In the case of a range or subnet, then the mapped addresses include the same number of addresses as the real range or subnet. For example, if the real address is defined as a range from 10.1.1.1 through 10.1.1.6, and you specify 172.20.1.1 as the mapped address, then the mapped range will include 172.20.1.1 through 172.20.1.6. If you want a many-to-one mapping, which we do not recommend, use a host network object instead of an inline address.

mapped_obj	Specifies the mapped IP address(es) as a network object (**object network**) or object group (**object-group network**). You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address. For dynamic NAT, the object or group cannot contain a subnet. You can share this mapped object across different dynamic NAT rules, if desired. See the "Mapped Address Guidelines" for information about disallowed mapped IP addresses. For static NAT, typically you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses. For more information, see the CLI configuration guide.
mapped_port	(Optional) Specifies the mapped TCP/UDP/SCTP port. You can specify ports by either a literal name or a number in the range of 0 to 65535.
net-to-net	(Optional) For NAT 46, specify **net-to-net** to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this keyword.
no-proxy-arp	(Optional) For static NAT, disables proxy ARP for incoming packets to the mapped IP addresses.
pat-pool *mapped_obj*	(Optional) Enables a PAT pool of addresses; all addresses in the object are used as PAT addresses. For dynamic NAT, you can configure the PAT pool as a fallback method. You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
real_port	(Optional) For static NAT, specifies the real TCP/UDP/SCTP port. You can specify ports by either a literal name or a number in the range of 0 to 65535.
round-robin	(Optional) Enables round-robin address allocation for a PAT pool. By default, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns an address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
route-lookup	(Optional) For identity NAT in routed mode, determines the egress interface using a route lookup instead of using the interface specified in the NAT command. If you do not specify interfaces in the NAT command, a route lookup is used by default.
service {**tcp** | **udp** | **sctp**}	(Optional) For static NAT with port translation, specifies the protocol for port translation: TCP, UDP, SCTP.
static	Configures static NAT or static NAT with port translation.

Command Default

- The default value of *real_ifc* and *mapped_ifc* is **any**, which applies the rule to all interfaces.
- (8.3(1), 8.3(2), and 8.4(1)) The default behavior for identity NAT has proxy ARP disabled. You cannot configure this setting. (8.4(2) and later) The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired.
- If you specify an optional interface, then the ASA uses the NAT configuration to determine the egress interface. (8.3(1) through 8.4(1)) The only exception is for identity NAT, which always uses a route

lookup, regardless of the NAT configuration. (8.4(2) and later) For identity NAT, the default behavior is to use the NAT configuration, but you have the option to always use a route lookup instead.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
8.4(2)/8.5(1)	The **no-proxy-arp**, **route-lookup**, **pat-pool**, and **round-robin** keywords were added. The default behavior for identity NAT was changed to have proxy ARP enabled, matching other static NAT rules. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality.
8.4(3)	The **extended**, **flat**, and **include-reserve** keywords were added. When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. *This feature is not available in 8.5(1).*
9.0(1)	NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6. Translating between IPv4 and IPv6 is not supported in transparent mode. We added the **interface ipv6** option and the **net-to-net** option.
9.5(1)	The **block-allocation** keyword was added.
9.5(2)	The **service sctp** keyword was added.
9.15(1)	The **flat** keyword was removed, and the **include-reserve** keyword is no longer a sub-parameter of flat. All PAT pools now use a flat port range, 1024-65535, and you can optionally include the reserved ports, 1-1023.

Usage Guidelines

When a packet enters the ASA, both the source and destination IP addresses are checked against the network object NAT rules. The source and destination address in the packet can be translated by separate rules if separate matches are made. These rules are not tied to each other; different combinations of rules can be used depending on the traffic.

Because the rules are never paired, you cannot specify that a source address should be translated to A when going to destination X, but be translated to B when going to destination Y. Use twice NAT for that kind of functionality (twice NAT lets you identify the source and destination address in a single rule).

For detailed information about the differences between twice NAT and network object NAT, see the CLI configuration guide.

Network object NAT rules are added to section 2 of the NAT rules table. For more information about NAT ordering, see the CLI configuration guide.

Depending on the configuration, you can configure the mapped address inline if desired or you can create a network object or network object group for the mapped address (the **object network** or **object-group network** command). Network object groups are particularly useful for creating a mapped address pool with discontinuous IP address ranges or multiple hosts or subnets. You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.

Objects and object groups used in NAT cannot be undefined; they must include IP addresses.

You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules, you need to create multiple objects that specify the same IP address, for example, **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02**, and so on.

Mapped Address Guidelines

The mapped IP address pool cannot include:

- The mapped interface IP address. If you specify **any** interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), use the **interface** keyword instead of the IP address.
- (Transparent mode) The management IP address.
- (Dynamic NAT) The standby interface IP address when VPN is enabled.
- Existing VPN pool addresses.

Clearing Translation Sessions

If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using clear xlate command. However, clearing the translation table disconnects all of the current connections.

PAT Pool Guidelines

- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record, and the PAT rule to use is ambiguous.
- (Pre-9.15) If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. (8.4(3) and later, not including 8.5(1) or 8.6(1)) If you have a lot of traffic that uses the lower port ranges, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.
- (9.15+) Ports are mapped to an available port in the 1024 to 65535 range. You can optionally include the reserved ports, those below 1024, to make the entire port range available for translations.

When operating in a cluster, blocks of 512 ports per address are allocated to the members of the cluster, and mappings are made within these port blocks. If you also enable block allocation, the ports are distributed according to the block allocation size, whose default is also 512.

- If you enable block allocation for a PAT pool, port blocks are allocated in the 1024-65535 range only. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application

requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host.

If you use an object group for the dynamic NAT mapped IP addresses, and the group includes host addresses, then enabling the PAT pool changes the use of those host addresses from PAT fallback to dynamic NAT.

- (8.4(3) and later, not including 8.5(1) or 8.6(1)) If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT and a flat range, then the other rule must also specify extended PAT and a flat range.

Extended PAT for a PAT Pool Guidelines

- Many application inspections do not support extended PAT. See the configuration guide for a complete list of unsupported inspections.
- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT-with-port-translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.
- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.
- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.

Round robin for a PAT Pool Guidelines

- (8.4(3) and later, not including 8.5(1) or 8.6(1)) If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. **Note**: This “stickiness” does not survive a failover. If the ASA fails over, then subsequent connections from a host may not use the initial IP address.
- (8.4(2), 8.5(1), and 8.6(1)) If a host has an existing connection, then subsequent connections from that host will likely use *different* PAT addresses for each connection because of the round robin allocation. In this case, you may have problems when accessing two websites that exchange information about the host, for example an e-commerce site and a payment site. When these sites see two different IP addresses for what is supposed to be a single host, the transaction may fail.
- Round robin, especially when combined with extended PAT, can consume a large amount of memory.

NAT and IPv6

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices. Note that you cannot perform NAT64/46 when the interfaces are members of the same bridge group.

- NAT66 (IPv6-to-IPv6)—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only).
- NAT46 (IPv4-to-IPv6)—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For

example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.4 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address.

- NAT64 (IPv6-to-IPv4)—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

Examples

Dynamic NAT Examples

The following example configures dynamic NAT that hides 192.168.2.0 network behind a range of outside addresses 2.2.2.1-2.2.2.10:

```
ciscoasa(config)# object network my-range-obj
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

The following example configures dynamic NAT with dynamic PAT backup. Hosts on inside network 10.76.11.0 are mapped first to the nat-range1 pool (10.10.10.10-10.10.10.20). After all addresses in the nat-range1 pool are allocated, dynamic PAT is performed using the pat-ip1 address (10.10.10.21). In the unlikely event that the PAT translations are also use up, dynamic PAT is performed using the outside interface address.

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20
ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21
ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

The following example configures dynamic NAT with dynamic PAT backup to translate IPv6 hosts to IPv4. Hosts on inside network 2001:DB8::/96 are mapped first to the IPv4_NAT_RANGE pool (209.165.201.1 to 209.165.201.30). After all addresses in the IPv4_NAT_RANGE pool are allocated, dynamic PAT is performed using the IPv4_PAT address (209.165.201.31). In the event that the PAT translations are also used up, dynamic PAT is performed using the outside interface address.

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30
ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31
ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

Dynamic PAT Example

The following example configures dynamic PAT that hides the 192.168.2.0 network behind address 2.2.2.2:

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

The following example configures dynamic PAT that hides the 192.168.2.0 network behind the outside interface address:

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

The following example configures dynamic PAT with a PAT pool to translate the inside IPv6 network to an outside IPv4 network:

```
ciscoasa(config)# object network IPv4_POOL
ciscoasa(config-network-object)# range 203.0.113.1 203.0.113.254
ciscoasa(config)# object network IPv6_INSIDE
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

Static NAT Examples

The following example configures static NAT for the real host 1.1.1.1 on the inside to 2.2.2.2 on the outside with DNS rewrite enabled.

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

The following example configures static NAT for the real host 1.1.1.1 on the inside to 2.2.2.2 on the outside using a mapped object.

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

The following example configures static NAT with port translation for 1.1.1.1 at TCP port 21 to the outside interface at port 2121.

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

The following example maps an inside IPv4 network to an outside IPv6 network.

```
ciscoasa(config)# object network inside_v4_v6
```

```
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

The following example maps an inside IPv6 network to an outside IPv6 network.

```
ciscoasa(config)# object network inside_v6
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

Identity NAT Examples

The following example maps a host address to itself using an inline mapped address:

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 10.1.1.1
```

The following example maps a host address to itself using a network object:

```
ciscoasa(config)# object network my-host-obj1-identity
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

Related Commands

Command	Description
clear configure nat	Removes the NAT configuration (both twice NAT and network object NAT).
show nat	Displays NAT policy statistics.
show nat pool	Displays information about NAT pools.
show running-config nat	Displays the NAT configuration.
show xlate	Displays xlate information.
xlate block-allocation	Configures the PAT port block allocation characteristics.

nat (vpn load-balancing)

To set the IP address to which NAT translates the IP address of this device, use the **nat** command in VPN load-balancing configuration mode. To disable this NAT translation, use the **no** form of this command.

nat *ip-address*
no nat [*ip-adddress*]

Syntax Description

ip-address	The IP address to which you want this NAT to translate the IP address of this device.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
VPN load-balancing configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

In the **no nat** form of the command, if you specify the optional *ip-address* value, the IP address must match the existing NAT IP address in the running configuration.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **nat** command that sets the NAT-translated address to 192.168.10.10:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

nat-assigned-to-public-ip

To automatically translate a VPN peer's local IP address back to the peer's real IP address, use the **nat-assigned-to-public-ip** command in tunnel-group general-attributes configuration mode. To disable the NAT rules, use the **no** form of this command.

nat-assigned-to-public-ip *interface*
no nat-assigned-to-public-ip *interface*

Syntax Description

interface	Specifies the interface where you want to apply NAT.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(3)	This command was added.

Usage Guidelines

In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address.

You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the **show nat** command.

Data Flow

The following steps describe the packet flow through the ASA when this feature is enabled:

1.The VPN peer sends a packet to the ASA.

The outer source/destination consists of the peer public IP address/ASA IP address. The encrypted inner source/destination consists of the VPN-assigned IP address/inside server address.

2.The ASA decrypts the packet (removing the outer source/destination).

3.The ASA performs a route lookup for the inside server, and sends the packet to the inside interface.

4.The automatically created VPN NAT policy translates the VPN-assigned source IP address to the peer public IP address.

5.The ASA sends the translated packet to the server.

6.The server responds to the packet, and sends it to the peer's public IP address.

7.The ASA receives the response, and untranslates the destination IP address to the VPN-assigned IP address.

8.The ASA forwards the untranslated packet to the outside interface where it is encrypted, and an outer source/destination is added consisting of the ASA IP address/peer public IP address.

9.The ASA sends the packet back to the peer.

10. The peer decrypts and processes the data.

Limitations

Because of routing issues, we do not recommend using this feature unless you know you need this feature; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations:

- Only supports Cisco IPsec and Secure Client.
- Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied.
- If you enable reverse route injection (see the **set reverse-route** command), only the VPN-assigned IP address is advertised.
- Does not support load-balancing (because of routing issues).
- Does not support roaming (public IP changing).

Examples

The following example enables NAT to the public IP for the "vpnclient" tunnel group:

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

The following is sample output from the **show nat detail** command showing an automatic NAT rule from peer 209.165.201.10 with assigned IP 10.1.226.174:

```
ciscoasa# show nat detail
 Auto NAT Policies (Section 2)
 1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
     translate_hits = 0, untranslate_hits = 0
     Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

Related Commands

Command	Description
show nat	Shows current xlates.
tunnel-group general-attributes	Sets general attributes for a tunnel group.
debug menu webvpn 99	For AnyConnect SSL sessions, the VPN NAT interface is stored in the session.

Command	Description
debug menu ike 2 *peer_ip*	For Cisco IPsec client sessions, the VPN NAT interface is stored in the SA.
debug nat 3	Shows debug messages for NAT.

nat-rewrite

To enable NAT rewrite for IP addresses embedded in the A-record of a DNS response, use the **nat-rewrite** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

nat-rewrite
no nat-rewrite

Syntax Description

This command has no arguments or keywords.

Command Default

NAT rewrite is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no nat-rewrite** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This feature performs NAT translation of A-type Resource Record (RR) in a DNS response.

Examples

The following example shows how to enable NAT rewrite in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# nat-rewrite
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

nbns-server

To configure an NBNS server, use the **nbns-server** command in tunnel-group webvpn-attributes configuration mode. To remove the NBNS server from the configuration, use the **no** form of this command.

The ASA queries NBNS servers to map NetBIOS names to IP addresses. WebVPN requires NetBIOS to access or share files on remote systems.

nbns-server { *ipaddr* | *hostname* } [**master**] [**timeout** *timeout*] [**retry** *retries*]
no nbns-server

Syntax Description

hostname	Specifies the hostname for the NBNS server.
ipaddr	Specifies the IP address for the NBNS server.
master	Indicates that this is a master browser, rather than a WINS server.
retry	Indicates that a retry value follows.
retries	Specifies the number of times to retry queries to NBNS servers. The ASA recycles through the list of servers the number of times you specify here before sending an error message. The default value is 2; the range is 1 through 10.
timeout	Indicates that a timeout value follows.
timeout	Specifies the amount of time the ASA waits before sending the query again, to the same server if there is only one, or another server if there are multiple NBNS servers. The default timeout is 2 seconds; the range is 1 to 30 seconds.

Command Default

No NBNS server is configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn-attributes configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Moved from webvpn mode to tunnel-group webvpn configuration mode.

Usage Guidelines

In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group webvpn-attributes configuration mode.

Maximum of 3 server entries. The first server you configure is the primary server, and the others are backups, for redundancy.

Use the **no** option to remove the matching entry from the configuration.

Examples

The following example shows how to configure the tunnel-group "test" with an NBNS server that is a master browser with an IP address of 10.10.10.19, a timeout value of 10 seconds, and 8 retries. It also shows how to configure an NBNS WINS server with an IP address of 10.10.10.24, a timeout value of 15 seconds, and 8 retries.

```
ciscoasa
(config)#
 tunnel-group test type webvpn
ciscoasa
(config)#
 tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
tunnel-group webvpn-attributes	Specifies the WebVPN attributes for the named tunnel-group.

neighbor (router eigrp)

To define an EIGRP neighbor router with which to exchange routing information, use the **neighbor** command in router eigrp configuration mode. To remove a neighbor entry, use the **no** form of this command.

neighbor *ip_address* **interface** *name*
no neighbor *ip_address* **interface** *name*

Syntax Description

interface *name*	The interface name, as specified by the **nameif** command, through which the neighbor can be reached.
ip_address	IPv4 or IPv6 address of the neighbor router with which routing information is exchanged.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router eigrp configuration	—	•	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.20(1)	Support for IPv6 was added.

Usage Guidelines

You can use multiple neighbor statements to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP exchanges routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

Note Configuring the **passive-interface** command for an interface suppresses all incoming and outgoing routing updates and hello messages on that interface. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

EIGRP hello messages are sent as unicast messages to neighbors defined using the **neighbor** command.

Examples

The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

Examples

The following example configures EIGRP peering sessions with the fe80::250:56ff:feb9:b41b and fe80::250:56ff:fe9f:13f4 neighbors:

```
ciscoasa(config)# rtr eigrp 100
ciscoasa(config-rtr)# neighbor fe80::250:56ff:feb9:b41b interface gig1
ciscoasa(config-rtr)# neighbor fe80::250:56ff:fe9f:13f4 interface branch_office
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debug information for EIGRP neighbor messages.
show eigrp neighbors	Displays the EIGRP neighbor table.

neighbor (router ospf)

To define a static neighbor on a point-to-point, non-broadcast network, use the **neighbor** command in router ospf configuration mode. To remove the statically defined neighbor from the configuration, use the **no** form of this command.

neighbor *ip_address* [**interface** *name*]
no neighbor *ip_address* [**interface** *name*]

Syntax Description

interface *name*	(Optional) Specifies the interface name, as specified by the **nameif** command, through which the neighbor can be reached.
ip_address	Specifies the IP address of the neighbor router.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf configuration	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **neighbor** command is used to advertise OSPF routes over VPN tunnels. One neighbor entry must be included for each known non-broadcast network neighbor. The neighbor address must be on the primary address of the interface.

The **interface** option needs to be specified when the neighbor is not on the same network as any of the directly connected interfaces of the system. Additionally, a static route must be created to reach the neighbor.

Examples

The following example defines a neighbor router with an address of 192.168.1.1:

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.

Command	Description
show running-config router	Displays the commands in the global router configuration.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the neighbor activate command in address-family configuration mode. To disable the exchange of an address with a BGP neighbor, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **activate**
no neighbor { *ip_address* | *ipv6-address* } **activate**

Syntax Description

ip_address	IP address of the BGP router.
ipv6-address	IPv6 address of the BGP router

Command Default

Address exchange with BGP neighbors is enabled by default for the IPv4 address family. You cannot enable address exchange for any other address families.

Note Address exchange for the IPv4 address family is enabled by default for each BGP routing session defined by the neighbor remote-as command; unless you configure the no bgp default ipv4-activate command before configuring the neighbor remote-as command, or you disable address exchange with a specific neighbor by using the no neighbor activate command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument and support for IPv6 address family were added.

Usage Guidelines

You can use this command to advertise address information in the form of an IP prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

Examples

The following example enables address exchange for IPv4 address family unicast for the BGP neighbor 172.16.1.1:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.

neighbor advertise-map

To advertise the routes in the BGP table matching the configured route-map, use the neighbor advertise-map command in router configuration mode. To disable route advertisement, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **advertise-map** *map-name* { **exist-map** *map-name* | **non-exist-map** *map-name* } [**check-all-paths**]
no neighbor { *ip_address* | *ipv6-address* } **advertise-map** *map-name* { **exist-map** *map-name* | **non-exist-map** *map-name* } [**check-all-paths**]

Syntax Description

ipv4_address	Specifies the IPv4 address of the router that should receive conditional advertisements.
ipv6_address	Specifies the IPv6 address of the router that should receive conditional advertisements.
advertise-map map-name	Specifies the name of the route map that will be advertised if the conditions of the exist map or non-exist map are met.
exist-map map-name	Specifies the name of the exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
non-exist-map map-name	Specifies the name of the non-exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
check-all-paths	(Optional) Enables checking of all paths by the exist-map with a prefix in the BGP table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

Use the neighbor advertise-map command to conditionally advertise selected routes. The routes (prefixes) that will be conditionally advertised are defined in two route maps: an advertise map and either an exist map or non-exist map.

The route map associated with the exist map or non-exist map specifies the prefix that the BGP speaker will track.

The route map associated with the advertise map specifies the prefix that will be advertised to the specified neighbor when the condition is met.

If an exist map is configured, the condition is met when the prefix exists in both the advertise map and the exist map.

If a non-exist map is configured, the condition is met when the prefix exists in the advertise map, but does not exist in the non-exist map.

If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.

Examples

The following router configuration example configures BGP to check all :

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a non-exist map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

The following peer group configuration example configures BGP to check all paths against the prefix to the BGP neighbor:

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor route1 send-community both
ciscoasa(config-router-af)# neighbor route1 advertise-map MAP1 exist-map MAP2 check-all-paths
```

Related Commands

Command	Description
address-family ipv4	Enters the address family configuration mode.

neighbor advertisement-interval

To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the neighbor advertisement-interval command in address-family configuration mode. To restore the default value, use the no form of this command

neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*
no neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router
seconds	Minimum time interval between sending BGP routing updates. Valid values are between 0 and 600.

Command Default

eBGP sessions not in a VRF: 30 seconds

eBGP sessions in a VRF: 0 seconds

iBGP sessions: 0 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes.

Examples

The following example sets the minimum time between sending BGP routing updates to 10 seconds:

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

The following example sets the minimum time between sending BGPv6 routing updates to 100 seconds:

```
asa(config-router-af)# neighbor 2001::1 advertisement-interval 100
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
neighbor activate	Enables information exchange with a BGP neighbor.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command in address-family configuration mode. To send no route as a default, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **default-originate** [**route-map** *route-map name*]
no neighbor { *ip_address* | *ipv6-address* } **default-originate** [**route-map** *route-map name*]

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
route-map route-map name	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Command Default

No default route is sent to the neighbor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause and there is a route that matches the IP access list exactly. The route map can also contain other match clauses.

You can use standard or extended access lists with the neighbor default-originate command.

Examples

In the following example, the local router injects route 0.0.0.0 to the neighbor 72.16.2.3 unconditionally:

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
In the following example, the local router injects route 0.0.0.0 to the neighbor 2001::1:
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
neighbor activate	Enables information exchange with a BGP neighbor.

neighbor description

To associate a description with a neighbor, use the neighbor description command in address-family configuration mode. To remove the description, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **description** *text*
no neighbor { *ip_address* | *ipv6-address* } **description** *text*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Examples

In the following example, the description of the neighbor is “peer with example.com”:

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the IPv6 neighbor is “peer with example.com”:

```
ciscoasa(config-router-af)#neighbor 2001::1 description peer with example.com
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
neighbor activate	Enables information exchange with a BGP neighbor.

neighbor disable-connected-check

To disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface, use the neighbor disable-connected-check command in address-family configuration mode. To enable connection verification for eBGP peering sessions, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **disable-connected-check**
no neighbor { *ip_address* | *ipv6-address* } **disable-connected-check**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.

Command Default

A BGP routing process will verify the connection of single-hop eBGP peering session (TTL=254) to determine if the eBGP peer is directly connected to the same network segment by default. If the peer is not directly connected to same network segment, connection verification will prevent the peering session from being established.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

The neighbor disable-connected-check command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

This command is required only when the neighbor ebgp-multihop command is configured with a TTL value of 1. The address of the single-hop eBGP peer must be reachable. The neighbor update-source command must be configured to allow the BGP routing process to use the loopback interface for the peering session.

Examples

In the following example, a single-hop eBGP peering session is configured between two BGP peers that are reachable on the same network segment through a local loopback interfaces on each router:

BGP Peer 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
BGP Peer 2
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
BGPv6 Peer
ciscoasa(config-router)# neighbor 2001::1 disable-connected-check
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the neighbor distribute-list command in address-family configuration mode. To remove an entry, use the no form of this command.

neighbor *ip_address* **distribute-list** { **access-list-name** } { **in** | **out** }
no neighbor *ip_address* **distribute-list** { **access-list-name** } { **in** | **out** }

Syntax Description

ip_address	IP address of the neighbor router.
access-list-name	Name of a standard access list.
in	Access list is applied to incoming advertisements to that neighbor
out	Access list is applied to outgoing advertisements to that neighbor

Command Default

No BGP neighbor is specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the ip as-path access-list and neighbor filter-list commands.
- The access-list (IP standard) commands can be used to configure standard access lists for the filtering of advertisement
- The route-map (IP) command can be used to filter advertisements. Route maps may be configured with autonomous system filters, prefix filters, access lists and distribute lists.

Standard access lists may be used to filter routing updates. However, in the case of route filtering when using classless inter-domain routing (CIDR), standard access lists do not provide the level of granularity that is necessary to configure advanced filtering of network addresses and masks.

Examples

In the following example, BGP neighbor information in the standard access-list distribute-list-acl is applied to incoming advertisements to the neighbor 172.16.4.1.

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
network	Specifies the networks to be advertised by BGP.
access-list permit	Specifies packets to forward.
access-list deny	Species packets to deny.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in address-family configuration mode. To return to the default, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop** [**ttl**]
no neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
ttl	(Optional) Time to live. Valid values are between 1 and 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	• —	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff. To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

The following example allows connections to or from neighbor 2001::1, which resides on a network that is not directly connected:

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af) neighbor 12001::1 ebgp-multihop
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.

neighbor fall-over bfd (router bgp)

To configure BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD, use the **fall-over** option when configuring the neighbor.

neighbor *ip_address* | *ipv6_address* **fall-over bfd**

Syntax Description

ip_address/ipv6_address	IP/IPv6 address of the neighbor router A.B.C.D/ X:X:X:X::X format.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router BFD configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

When configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair.

Examples

The following example configures BFD support for the 172.16.10.2 and 1001::2 neighbors:

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.10.2 fall-over bfd
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 1001::2 fall-over bfd
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.

Command	Description
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

neighbor filter-list

To set up a BGP filter, use the neighbor filter-list command in address-family configuration mode. To disable this function, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **filter-list** *access-list-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **filter-list** *access-list-name* { **in** | **out** }

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
access-list-name	Name of an autonomous system path access list. You define this access list with the as-path access-list command.
in	Access list is applied to incoming routes.
out	Access list is applied to outgoing routes.

Command Default

No BGP filter is used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command establishes filters on both inbound and outbound BGP routes.

Note Do not apply both a neighbor distribute-list and a neighbor prefix-list command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (neighbor distribute-list or neighbor prefix-list) can be applied to each inbound or outbound direction.

Examples

In the following address-family configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_
ciscoasa(config)# as-path access-list as-path-acl deny ^123$
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

In the following address-family configuration mode example, the BGPv6 neighbor with IP address 2001::1 is not sent advertisements about any path through or from the adjacent autonomous system:

```
ciscoasa(config-router-af)# neighbor 2001::1 filter-list as-path-acl out
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
network	Specifies the network to be advertised by the BGP routing process.

neighbor ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor, use the neighbor ha-mode graceful-restart command in the address-family configuration mode. To remove from the configuration the BGP graceful restart capability for a neighbor, use the no form of this command.

neighbor *ip_address* **ha-mode graceful-restart** [**disable**]
no neighbor *ip_address* **ha-mode graceful-restart**

Syntax Description

ip_address	IP address of the neighbor.
disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart capability is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

The neighbor ha-mode graceful-restart command is used to enable or disable the graceful restart capability for an individual BGP neighbor. Use the disable keyword to disable the graceful restart capability when graceful restart has been previously enabled for the BGP peer.

The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware ASA. An ASA that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. An ASA that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

Note To enable the BGP graceful restart capability globally for all BGP neighbors, use the bgp graceful-restart command. When the BGP graceful restart capability is configured for an individual neighbor, each method of configuring graceful restart has the same priority, and the last configuration instance is applied to the neighbor.

Use the show bgp neighbors command to verify the BGP graceful restart configuration for BGP neighbors.

Examples

The following example enables the BGP graceful restart capability for the BGP neighbor, 172.21.1.2:

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

Related Commands

Command	Description
bgp graceful-restart	Enables or disables he BGP graceful restart capability globally for all BGP neighbors.
show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

neighbor local-as

To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the neighbor local-as command in address-family configuration mode. To disable AS_PATH attribute customization, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]
no neighbor { *ip_address* | *ipv6-address* } **local-as**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
autonomous-system-number	(Optional) Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. **Note** With this argument, you cannot specify the autonomous system number from the local BGP routing process or from the network of the remote peer. For more details about autonomous system number formats, see the router bgp command.
no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.
replace-as	(Optional) Replaces the real autonomous system number with the local autonomous system number in the eBGP updates. The autonomous system number from the local BGP routing process is not prepended.
dual-as	(Optional) Configures the eBGP neighbor to establish a peering session using the real autonomous system number (from the local BGP routing process) or by using the autonomous system number configured with the autonomous-system-number argument (local-as).

Command Default

The autonomous system number from the local BGP routing process is prepended to all external routes by default.

Command Modes

The following table shows the modes in which you can enter the command:

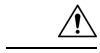
Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

The neighbor local-as command is used to customize the AS_PATH attribute by adding and removing autonomous system numbers for routes received from eBGP neighbors. The configuration of this command allows a router to appear to external peers as a member of another autonomous system for the purpose of autonomous system number migration. This feature simplifies the process of changing the autonomous system number in a BGP network by allowing the network operator to migrate customers to new configurations during normal service windows without disrupting existing peering arrangements.



Caution BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This command should be configured only for autonomous system migration, and should be de-configured after the transition has been completed. This procedure should be attempted only by an experienced network operator. Routing loops can be created through improper configuration.

This command can be used for only true eBGP peering sessions. This command does not work for two peers in different sub-autonomous systems of a confederation.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

Local-AS Example

The following example establishes peering between Router 1 and Router 2 through autonomous system 300, using the local-as feature:

Router 1 (Local router)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300
Router 2 (Remote router)
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

No-prepend keyword configuration Example

The following example configures BGP to not prepend autonomous system 500 to routes received from the 192.168.1.1 neighbor:

```
ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend
```

Replace-as keyword configuration Example

The following example strips private autonomous system 64512 from outbound routing updates for the 172.20.1.1 neighbor and replaces it with autonomous system 600:

```
ciscoasa(config)# router bgp 64512

ciscoasa(config-router)# address-family ipv4

ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as

ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as
```

Dual-as keyword configuration Example

The following examples show the configurations for two provider networks and one customer network. Router 1 belongs to autonomous system 100, and Router 2 belongs to autonomous system 200. Autonomous system 200 is being merged into autonomous system 100. This transition needs to occur without interrupting service to Router 3 in autonomous system 300 (customer network). The neighbor local-as command is configured on router 1 to allow Router 3 to maintain peering with autonomous system 200 during this transition. After the transition is complete, the configuration on Router 3 can be updated to peer with autonomous system 100 during a normal maintenance window or during other scheduled downtime.

Router 1 Configuration (Local Provider Network)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

Router 2 Configuration (Remote Provider Network)

```
ciscoasa(config)# router bgp 200

ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
 ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

Router 3 Configuration (Remote Customer Network)

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

To complete the migration after the two autonomous systems have merged, the peering session is updated on Router 3:

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

BGPv6 configuration

```
ciscoasa(config-router-af)# neighbor 2001::1 local-as 500 no-prepend
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
bgp router-id	Configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process.
neighbor activate	Enables information exchange with a BGP neighbor.
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP neighbor table.
network	Specifies the network to be advertised by the BGP routing process.
synchronization	Enables the synchronization between BGP and your Interior Gateway Protocol (IGP) system

neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the neighbor maximum-prefix command in address-family configuration mode. To disable this function, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
no neighbor { *ip_address* | *ipv6-address* } **maximum-prefix** *maximum*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
maximum	Maximum number of prefixes allowed from this neighbor.
threshold	(Optional) Integer specifying at what percentage of maximum the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
restart	(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The restart timer is configured with the restart-interval argument.
restart-interval	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
warning-only	(Optional) Allows the router to generate a log message when the maximum is exceeded, instead of terminating the peering.

Command Default

This command is disabled by default. There is no limit on the number of prefixes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the warning-only keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the clear bgp command is issued.

Examples

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 1000:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

The following example sets the maximum number of prefixes allowed from the neighbor at 2001::1 to 1000:

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
network	Specifies the network to be advertised by the BGP routing process.

neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor, use the neighbor next-hop-self command in address-family configuration mode. To disable this feature, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **next-hop-self**
no neighbor { *ip_address* | *ipv6-address* } **next-hop-self**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
warning-only	(Optional) Allows the router to generate a log message when the maximum is exceeded, instead of terminating the peering.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

The following example forces all updates destined for 2001::1 to advertise this router as the next hop:

```
ciscoasa(config-router-af)#neighbor 2001::1 next-hop-selfs
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.

neighbor password

To enable message digest5 (MD5) authentication on a TCP connection between two BGP peers, use the neighbor password command in address-family configuration mode. To disable this function, use the no form of this command

neighbor { *ip_address* | *ipv6-address* } **password** [**0-7**] *string*
no neighbor { *ip_address* | *ipv6-address* } **password**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
string	Case-sensitive password of up to 25 characters in length. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.
0-7	(Optional) Encryption type. 0-6 is without encryption. 7 is used for encryption.

Command Default

MD5 is not authenticated on a TCP connection between two BGP peers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the ASA software to generate and check the MD5 digest of every segment sent on the TCP connection.

When configuring you can provide a case-sensitive password of up to 25 characters regardless of whether the service password-encryption command is enabled. If the length of password is more than 25 characters, an error message is displayed and the password is not accepted. The string can contain any alphanumeric characters, including spaces. A password cannot be configured in the number-space-anything format. The space after the

number can cause authentication to fail. You can also use any combination of the following symbolic characters along with alphanumeric characters:

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < . , ?

Caution If the authentication string is configured incorrectly, the BGP peering session will not be established. We recommend that you enter the authentication string carefully and verify that the peering session is established after authentication is configured.

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as the following will appear on the console while the routers attempt to establish a BGP session between them:

%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179

Configuring an MD5 Password in an Established BGP Session

If you configure or change the password or key used for MD5 authentication between two BGP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the BGP hold-down timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the hold-down timer expires, the session will time out.

Note Configuring a new timer value for the hold-down timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the hold-down timer to avoid resetting the BGP session.

Examples

The following example configures MD5 authentication for the peering session with the 10.108.1.1 neighbor. The same password must be configured on the remote peer before the hold-down timer expires:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

The following example configures a password for more than 25 characters when the service password-encryption command is disabled.

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
 ciscoasa(config-router-af)# neighbor 209.165.200.225 password 12345678912345678912345678901

    % BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
 no service password-encryption
  neighbor 209.165.200.225 password 123456789123456789123456
```

In the following example an error message occurs when you configure a password for more than 25 characters when the service password-encryption command is enabled.

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901

% BGP: Password length must be less than or equal to 25.
 Router(config-router)# do show run | i password  service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
bgp router-id	Configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process.
neighbor remote-as	Add an entry to the BGP or multiprotocol BGP neighbor table.

neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, use the neighbor prefix-list command in address-family configuration mode. To remove a filter list, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **prefix-list** *prefix-list-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **prefix-list** *prefix-list-name* { **in** | **out** }

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-adress	IPv6 address of the neighbor router.
prefix-list-name	Name of a prefix list.
in	Filter list is applied to incoming advertisements from that neighbor.
out	Filter list is applied to outgoing advertisements to that neighbor.

Command Default

All external and advertised address prefixes are distributed to BGP neighbors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the ip as-path access-list global configuration command and used in the neighbor filter-list command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the neighbor distribute-list command.

Note Do not apply both a neighbor distribute-list and a neighbor prefix-list command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (neighbor distribute-list or neighbor prefix-list) can be applied to each inbound or outbound direction..

Examples

The following address-family configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 10.23.4.1:

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

The following address family router configuration mode example applies the prefix list named CustomerA to outgoing advertisements to neighbor 10.23.4.3:

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
The following address family router configuration mode example applies the prefix list named
 CustomerA to outgoing advertisements to neighbor 2001::1:
ciscoasa(config-router-af)#neighbor 2001::1 prefix-list CustomerA out
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
network	Specifies the network to be advertised by the BGP routing process.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the neighbor remote-as command in the address-family configuration mode. To remove an entry from the table, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*
no neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. For more details about autonomous system number formats, see the router bgp command. When used with the alternate-as keyword, up to five autonomous system numbers may be entered.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

By default, neighbors that are defined using the neighbor remote-as command in router configuration mode exchange only unicast address prefixes.

Use the alternate-as keyword is used to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range

of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the bgp listen command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second neighbor remote-as command shows an internal BGP neighbor (with the same autonomous system number) at address 10.108.234.2; and the last neighbor remote-as command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31 1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
network	Specifies the network to be advertised by the BGP routing process.

Command	Description
neighbor remove private-as	Removes private autonomous system numbers from the eBGP outbound routing updates.

neighbor remove-private-as

To remove private autonomous system numbers from the eBGP outbound routing updates, use the neighbor remove-private-as command in address-family configuration mode. To disable this function, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **remove-private-as** [**all** [**replace-as**]]
no neighbor { *ip_address* | *ipv6-address* } **remove-private-as** [**all** [**replace-as**]]

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.
replace-as	(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.

Command Default

No private AS numbers are removed from the AS path.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command is available for external BGP (eBGP) neighbors only. The private AS values are 64512 to 65535. When an update is passed to the external neighbor, if the AS path includes private AS numbers, the software will drop the private AS numbers

- The neighbor remove-private-as command removes private AS numbers from the AS path even if the path contains both public and private ASNs
- The neighbor remove-private-as command removes private AS numbers even if the AS path contains only private AS numbers. There is no likelihood of a 0-length AS path because this command can be applied to eBGP peers only, in which case the AS number of the local router is appended to the AS path. The neighbor remove-private-as command removes private AS numbers even if the private ASNs appear before the Confederation segments in the AS path.

- Upon removing private AS numbers from the AS path, the path length of prefixes being sent out will decrease. Because the AS path length is a key element of BGP best path selection, it might be necessary to retain the path length. The replace-as keyword ensures that the path length is retained by replacing all removed AS numbers with the local router's AS number.
- The feature can be applied to neighbors per address family. Therefore, you can apply the feature to a neighbor in one address family and not in another, affecting update messages on the outbound side for only the address family for which the feature is configured.

Examples

The following example shows a configuration that removes the private AS number from the updates sent to 172.16.2.33. The result is that the AS path for the paths advertised by 10.108.1.1 through AS 100 will contain only “100” (as seen by autonomous system 2051).

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer

ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as


Router-in-AS100# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
 Advertised to non peer-group peers:
   172.16.2.33
 65001
    10.108.1.1 from 10.108.1.1
     Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
    172.16.2.32 from 172.16.2.32
     Origin IGP, metric 0, localpref 100, valid, external, best
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor description	Associates a description with a neighbor
neighbor remote-as	Adds a BGP or multi-protocol BGP routing entry to the routing table.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the neighbor route-map command in address-family configuration mode. To remove a route map, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
map-name	Name of a route-map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

When specified in address-family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

Examples

The following example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

The following example applies a route map named internal-map to BGP incoming route from 2001::1:

```
ciscoasa(config-router-af)# neighbor 2001::1 route-map internal-map in
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
match as-path	Matches a BGP autonomous system path that is specified by an access list
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
match as-path	Match a BGP autonomous system path that is specified by an access list.
set local-preference	Specify a preference value for the autonomous system path.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the neighbor send-community command in address-family configuration mode. To remove the entry, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **send-community**
no neighbor { *ip_address* | *ipv6-address* } **send-community**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Examples

In the following address-family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

In the following example, the router is configured to send the communities attribute to its neighbor at IP address 2001::1:

```
ciscoasa(config-router-af)# neighbor 2001::1 send-community
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.

neighbor shutdown

To disable a neighbor, use the neighbor shutdown command in address-family configuration mode. To re-enable the neighbor, use the no form of this command.

neighbor *ip_address* **shutdown**
no neighbor *ip_address* **shutdown**

Syntax Description

ip_address	IP address of the neighbor router.

Command Default

No change is made to the status of any BGP neighbor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The neighbor shutdown command terminates any active session for the specified neighbor and removes all associated routing information .

To display a summary of BGP neighbors, use the show bgp summary command. Those neighbors with an Idle status and the Admin entry have been disabled by the neighbor shutdown command.

'State/PfxRcd' shows the current state of the BGP session or the number of prefixes the router has received from a neighbor. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string 'PfxRcd' appears in the entry, the neighbor is shut down, and the connection is idle.

Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.

Command	Description
show bgp summary	Displays a summary of BGP neighbor status.

neighbor timers

To set the timers for a specific BGP peer, use the neighbor timers command in address-family configuration mode. To clear the timers for a specific BGP peer , use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **timers** *keepalive holdtime* [*min-holdtime*]

no neighbor { *ip_address* | *ipv6-address* } **timers**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
keepalive	Frequency (in seconds) with which the ASA software sends keepalive messages to its peer. The default is 60 seconds.The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the holdtime argument. The range is from 0 to 65535.

Command Default

Keepalive time: 60 seconds

Holdtime: 180 seconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

- The timers configured for a specific neighbor override the timers configured for all BGP neighbors using the timers bgp command.
- When configuring the holdtime argument for a value of less than twenty seconds, the following warning is displayed: A hold time of less than 20 seconds increases the chances of peer flapping.

- If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed: Minimum acceptable hold time should be less than or equal to the configured hold time.

Note When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating "unacceptable hold time."

Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.47.0:

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum hold-time interval to 100 seconds for the BGP peer 192.168.1.2:

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds, for the BGP peer 2001::1:

```
ciscoasa(config-router-af)# neighbor 2001::1 timers 70 210
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables exchange of information with a BGP neighbor.

neighbor transport

To enable a TCP transport session option for a Border Gateway Protocol (BGP) session, use the neighbor transport command in router or address-family configuration mode. To disable a TCP transport session option for a BGP session, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [**disable**] }
no neighbor { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [**disable**] }

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
connection-mode	Specifies the type of connection - active or passive.
active	Specifies an active connection.
passive	Specifies a passive connection.
path-mtu-discovery	Enables TCP transport path maximum transmission unit (MTU) discovery. TCP path MTU discovery is enabled by default.
disable	Disables TCP path MTU discovery.

Command Default

If this command is not configured, TCP path MTU discovery is enabled by default, but no other TCP transport session options are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

This command is used to specify various transport options. An active or passive transport connection can be specified for a BGP session. TCP transport path MTU discovery can be enabled to allow a BGP session to take advantage of larger MTU links. Use the show bgp neighbors command to determine whether TCP path

MTU discovery is enabled.If you use the disable keyword to disable discovery, discovery is also disabled on any peer that inherits the template in which you disabled discovery.

Examples

The following example shows how to configure the TCP transport connection to be active for a single internal BGP (iBGP) neighbor:

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

The following example shows how to configure the TCP transport connection to be passive for a single external BGP (eBGP) neighbor:

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

The following example shows how to disable TCP path MTU discovery for a single BGP neighbor:

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

The following example shows how to configure the TCP transport connection to be active for a single BGPv6 neighbor:

```
ciscoasa(config-router-af)#neighbor 2001::1 transport connection-mode active
```

The following example shows how to enable TCP path MTU discovery for a single BGPv6 neighbor:

```
ciscoasa(config-router-af)#neighbor 2001::1 transport path-mtu-discovery
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables exchange of information with a BGP neighbor.
neighbor remote-as	Adds an entry to the BGP or multi-protocol BGP routing table.
show bgp neighbor	Displays information about BGP neighbors

neighbor ttl-security

To secure a Border Gateway Protocol (BGP) peering session and to configure the maximum number of hops that separate two external BGP (eBGP) peers, use the neighbor ttl-security command in address-family configuration mode. To disable this feature, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*
no neighbor { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
hop-count	Number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured hop-count argument. Valid values are a number between 1 and 254.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

The neighbor ttl-security command provides a lightweight security mechanism to protect BGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses in the packet headers.

This feature leverages designed behavior of IP packets by accepting only IP packets with a TTL count that is equal to or greater than the locally configured value. Accurately forging the TTL count in an IP packet is generally considered to be impossible. Accurately forging a packet to match the TTL count from a trusted peer is not possible without internal access to the source or destination network.

This feature should be configured on each participating router. It secures the BGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router. When this feature is enabled, BGP will establish or maintain a session only if the TTL value in the IP packet header is equal to or greater

than the TTL value configured for the peering session. This feature has no effect on the BGP peering session, and the peering session can still expire if keepalive packets are not received. If the TTL value in a received packet is less than the locally configured value, the packet is silently discarded and no Internet Control Message Protocol (ICMP) message is generated. This is designed behavior; a response to a forged packet is not necessary.

To maximize the effectiveness of this feature, the hop-count value should be strictly configured to match the number of hops between the local and external network. However, you should also take path variation into account when configuring this feature for a multihop peering session.

The following restrictions apply to the configuration of this command:

- This feature is not supported for internal BGP (iBGP) peers.
- The neighbor ttl-security command cannot be configured for a peer that is already configured with the neighbor ebgp-multihop command. The configuration of these commands is mutually exclusive, and only one of these commands is needed to enable a multihop eBGP peering session. An error message will be displayed in the console if you attempt to configure both commands for the same peering session.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside of your network. This restriction also includes peers that are on the network segment between the source and destination network.

Examples

The following example sets the hop count to 2 for a directly connected neighbor. Because the hop-count argument is set to 2, BGP will accept only IP packets with a TTL count in the header that is equal to or greater than 253. If a packet is received with any other TTL value in the IP packet header, the packet will be silently discarded.

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

The following example sets the hop count to 2 for a directly connected BGPv6 neighbor.

```
ciscoasa(config-router-af)#neighbor 2001::1 ttl-security hops 2
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables exchange of information with a BGP neighbor.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected

neighbor update-source

To configure an interface as the source for a BGP-speaking neighbor, use the **neighbor update-source** command in address-family configuration mode. To disable this feature, use the no form of this command.

neighbor { *ipv_address* | *ipv6-address* } **update-source** { *interface name* }

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
interface name	Specifies the name of the interface, as specified by the `nameif` command, that the ASA uses as the source for BGP routing.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode.	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.18(2)	This command is added.

Usage Guidelines

This command is useful to run BGP protocol over the loopback interface and allow the loopback interface to participate in redistribution and prefix advertisement.

Examples

The following example updates loopback interface loop1 as source for BGP neighbor 10.108.1.1:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 109
ciscoasa(config-router-af)# neighbor 10.108.1.1 update-source loop1
```

The following example updates loopback interface loop1 as source for BGP neighbor 2001::1:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 2001::1 remote-as 109
ciscoasa(config-router-af)# neighbor 2001::1 update-source loop1
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables information exchange with a BGP neighbor.
neighbor remote-as	Adds a BGP or multi-protocol BGP routing entry to the routing table.

neighbor version

To configure the ASA software to accept only a particular BGP version, use the neighbor version command in the address-family configuration mode. To use the default version level of a neighbor, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **version** *number*
no neighbor { *ip_address* | *ipv6-address* } **version** *number*

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
number	BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Command Default

BGP version 4.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

Entering this command disables dynamic version negotiation.

Examples

The following example locks down to Version 4 of the BGP protocol:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
ciscoasa(config-router-af)# neighbor 2001::1 version 4
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables exchange of information with a BGP neighbor.

neighbor weight

To assign a weight to a neighbor connection, use the neighbor weight command in address-family configuration mode. To remove a weight assignment, use the no form of this command.

neighbor { *ip_address* | *ipv6-address* } **weight number**
no neighbor { *ip_address* | *ipv6-address* } **weight number**

Syntax Description

ip_address	IP address of the neighbor router.
ipv6-address	IPv6 address of the neighbor router.
number	Weight to assign. Valid values are between 0 and 65535.

Command Default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the set weight route-map command override the weights assigned using the neighbor weight command.

Examples

The following address-family configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

The following address-family configuration mode example sets the weight of all routes learned via 2001::1:

```
ciscoasa(config-router-af)# neighbor 2001::1 weight 50
```

Related Commands

Command	Description
address-family ipv4	Enters address-family configuration mode.
neighbor activate	Enables exchange of information with a BGP neighbor.

nem

To enable network extension mode for hardware clients, use the **nem enable** command in group-policy configuration mode. To disable NEM, use the **nem disable** command. To remove the NEM attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy.

nem { **enable**|**disable** }
no nem

Syntax Description

disable	Disables Network Extension Mode.
enable	Enables Network Extension Mode.

Command Default

Network extension mode is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Usage Guidelines

Network Extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPsec encapsulates all traffic from the private network behind the hardware client to networks behind the ASA. PAT does not apply. Therefore, devices behind the ASA have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set NEM for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
```

netmod

To disable a network module, use the **netmod** command in global configuration mode. To enable a network module, use the **no** form of this command.

Note This command is only supported on the Secure Firewall 3100.

netmod 2 disable
no netmod 2 disable

Syntax Description

2	Specifies the module in slot 2.
disable	Disabled the network module.

Command Default

If the module is installed when you first boot up, then it is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.17(1)	This command was introduced for the Secure Firewall 3100.

Usage Guidelines

If you install a network module before you first power on the firewall, no action is required; the network module is enabled and ready for use. If you need to make changes to your network module installation after initial bootup, then use this command.

Adding a new module or permanently removing a module requires a reload. You can hot swap a network module for a new module of the same type without having to reload. However, you must shut down the current module to remove it safely. If you replace a network module with a different type, then a reload is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present.

Examples

The following example disables the network module.

```
ciscoasa(config)# netmod 2 disable
```

The following example enabled the network module.

```
ciscoasa(config)# no netmod 2 disable
```

network (address-family)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) routing processes, use the network command in address-family configuration mode. To remove an entry from the routing table, use the no form of this command.

network { *ipv4_address* [**mask** *network_mask*] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [*subnet_prefix* | *prefix_length*] } [**route-map** *route_map_name*]
no network { *ipv4_address* [**mask** *network_mask*] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [*subnet_prefix* | *prefix_length*] } [**route-map** *route_map_name*]

Syntax Description

ipv4_address	The IPv4 network that BGP or multiprotocol BGP will advertise.
ipv6_prefix/*prefix_length*	The IPv6 network that BGP or multiprotocol BGP will advertise.
mask network_mask	(Optional) Network or subnetwork mask with mask address.
prefix_delegation_name	If you enable the DHCPv6 Prefix Delegation client (**ipv6 dhcp client pd**), then you can advertise the prefix(es).
subnet_prefix/*prefix_length*	(Optional) To subnet the prefix, specify the subnet_prefix/prefix length.
route-map route_map_name	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

Command Default

No networks are specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.6(2)	We added the *prefix_delegation_name* [*subnet_prefix*/*prefix_length*] arguments.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

Related Commands

Command	Description
show bgp interfaces	Displays entries in the BGP routing table.

network (router eigrp)

To specify a list of networks for the EIGRP routing process, use the **network** command in router configuration mode. To remove a network definition, use the **no** form of this command.

network *ip_addr* [*mask*]
no network *ip_addr* [*mask*]

Syntax Description

ip_addr	The IP address of a directly connected network. The interface connected to the specified network will participate in the EIGRP routing process.
mask	(Optional) The network mask for the IP address.

Command Default

No networks are specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **network** command starts EIGRP on all interfaces with at least one IP address in the specified network. It inserts the connected subnet from the specified network in the EIGRP topology table.

The ASA then establishes neighbors through the matched interfaces. There is no limit to the number of **network** commands that can be configured on the ASA.

Examples

The following example defines EIGRP as the routing protocol to be used on all interfaces connected to networks 10.0.0.0 and 192.168.7.0:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp interfaces	Displays information about interfaces configured for EIGRP.

Command	Description
show eigrp topology	Displays the EIGRP topology table.

network (router rip)

To specify a list of networks for the RIP routing process, use the **network** command in router configuration mode. To remove a network definition, use the **no** form of this command.

network { *ip_addr* | *ipv6-address* } | < *prefix-length* >
no network { *ip_addr* | *ipv6-address* } |< *prefix-length* >[**route-map** *route-map-name*]

Syntax Description

ip_addr	The IP address of a directly connected network. The interface connected to the specified network will participate in the RIP routing process.
ipv6-address	The IPv6 address to be used. The IPv6 address must be entered in the format X:X:X:X::X.
prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Valid values are between 0 and 128.
route-map-name	The route-map whose attributes will be modified.

Command Default

No networks are specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration, Address-family configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.3(2)	The ipv6-address argument was added and support was added for the IPv6 address-family.

Usage Guidelines

The network number specified must not contain any subnet information. There is no limit to the number of network commands you can use on the router. RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

Examples

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.0.0.0 and 192.168.7.0:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
In the following example the attributes of the test-route-map route map connected to the
2001::1 network will be modified.
ciscoasa(config-router)# network 2001:0:0:0::1 route-map test-route-map
```

Related Commands

Command	Description
router rip	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

network-acl

To specify a firewall ACL name that you configured previously using the **access-list** command, use the **network-acl** command in dynamic-access-policy-record configuration mode. To remove an existing network ACL, use the **no** form of this command. To remove all network ACLs, use the command without arguments.

network-acl *name*
no network-acl [*name*]

Syntax Description

name	Specifies the name of the network ACL. The maximum number for a name is 240 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-access-policy-record configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use this command multiple time to assign multiple firewall ACLs to the DAP record.

The ASA verifies each of the ACLs you specify to make sure they contain only permit rules or only deny rules for the access-list entries. If any of the specified ACLs contain mixed permit and deny rules, then the ASA rejects the command.

The following example shows how to apply a network ACL called Finance Restrictions to the DAP record named Finance.

```
ciscoasa
(config)#

dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
 network-acl Finance Restrictions
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
access-policy	Configures a firewall access policy.

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces defined with the address/netmask pair, use the **no** form of this command.

network *addr mask* **area** *area_id*
no network *addr mask* **area** *area_id*

Syntax Description

addr	IP address.
area *area_id*	Specifies the area that is to be associated with the OSPF address range. The *area_id* can be specified in either IP address format or in decimal format. When specified in decimal format, valid values range from 0 to 4294967295.
mask	The network mask.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

For OSPF to operate on the interface, the address of the interface must be covered by the **network area** command. If the **network area** command does not cover the IP address of the interface, it will not enable OSPF over that interface.

There is no limit to the number of **network area** commands you can use on the ASA.

Examples

The following example enables OSPF on the 192.168.1.1 interface and assigns it to area 2:

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.

Command	Description
show running-config router	Displays the commands in the global router configuration.

network-object

To add a host object, a network object, or a subnet object to a network object group, use the network-object command in object-group network configuration mode. To remove network objects, use the **no** form of this command.

network-object { **host** *address* | *IPv4_address mask* | *IPv6_address* | *IPv6_prefix* | **object** *name* }
no network-object { **host** *ip_address* | *ip_address mask* | **object** *name* }

Syntax Description

host *ip_address*	Specifies a host IPv4 or IPv6 address.
IPv4_address mask	Specifies an IPv4 network address and subnet mask.
IPv6_address/IPv6_prefix	Specifies an IPv6 network address and prefix length.
object *name*	Specifies a network object (created by the **object network** command).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object-group network configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	The **object** argument was added to support network objects (**object network** command).
9.0(1)	Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses, although you cannot use a mixed group in NAT.

Usage Guidelines

The **network-object** command is used with the **object-group** command to define a host object, a network object, or a subnet object.

Examples

The following example shows how to use the **network-object** command to create a new host object in a network object group:

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
```

```
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
group-object	Adds network object groups.
object network	Adds a network object.
object-group network	Defines network object groups.
show running-config object-group	Displays the current object groups.

network-service-member

To add a network-service object to a network-service group, use the **network-service-member** command in object group configuration mode. Use to **no** form of the command to remove an object from a group

network-service-member *object_name*
no network-service-member *object_name*

Syntax Description

object_name	The name of a network-service object. If there are spaces in the name, enclose the name in double quotation marks.

Command Default

No default values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Network-service object-group configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was added.

Example

The following example adds three existing network-service objects to a network-service object group.

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

Related Commands

Command	Description
clear object-group	Clears hit counts for object groups.
object-group network-service	Defines network-service object groups.
show object-group network-service	Displays network-service objects and their hit counts.

nis address

To provide the Network Information Service (NIS) address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **nis address** command in ipv6 dhcp pool configuration mode. To remove the NIS server, use the **no** form of this command.

nis address *nis_ipv6_address*
no nis address *nis_ipv6_address*

Syntax Description

nis_ipv6_address	Specifies the NIS IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the NIS address, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

nis domain-name

To provide the Network Information Service (NIS) domain name to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **nis domain-name** command in ipv6 dhcp pool configuration mode. To remove the NIS domain name, use the **no** form of this command.

nis domain-name *nis_domain_name*
no nis domain-name *nis_domain_name*

Syntax Description

nis_domain_name	Specifies the NIS domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the NIS domain name, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

nisp address

To provide the Network Information Service Plus (NIS+) server IP address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **nisp address** command in ipv6 dhcp pool configuration mode. To remove the NIS+ server, use the **no** form of this command.

nisp address *nisp_ipv6_address*
no nisp address *nisp_ipv6_address*

Syntax Description

nisp_ipv6_address	Specifies the NIS+ server IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the NIS+ server, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

nisp domain-name

To provide the Network Information Service Plus (NIS+) domain name to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **nisp domain-name** command in ipv6 dhcp pool configuration mode. To remove the NIS+ somain name, use the **no** form of this command.

nisp domain-name *nisp_domain_name*
no nisp domain-name *nisp_domain_name*

Syntax Description

nisp_domain_name	Specifies the NIS+ domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the NIS+ domain name, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

nop

To define an action when the No Operation IP option occurs in a packet header with IP Options inspection, use the **nop** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

nop action { **allow | clear** }
no nop action { **allow | clear** }

Syntax Description

allow	Allow packets containing the No Operation IP option.
clear	Remove the No Operation option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the No Operation IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

The Options field in the IP header can contain zero, one, or more options, which makes the total length of the field variable. However, the IP header must be a multiple of 32 bits. If the number of bits of all options is not a multiple of 32 bits, the No Operation (NOP) or IP Option 1 is used as “internal padding” to align the options on a 32-bit boundary.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

nsf cisco

To enable Cisco nonstop forwarding (NSF) operations on an ASA that is running Open Shortest Path First (OSPF), use the nsf cisco command in router configuration mode. To return to the default, use the no form of this command.

nsf cisco [**enforce global**]
no nsf cisco [**enforce global**]

Syntax Description

enforce global	(Optional) Cancels NSF restart on all interfaces when neighboring networking devices that are not NSF-aware are detected on any interface during the restart process.

Command Default

Cisco NSF graceful restart is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command enables Cisco NSF on an OSPF router. When NSF is enabled on a router, the router is NSF-capable and will operate in restarting mode.

If a router is expected to cooperate with a neighbor that is doing an NSF graceful restart only, the neighbor router must be running a Cisco software release that supports NSF but NSF need not be configured on the router. When a router is running a Cisco software release that supports NSF, the router is NSF-aware.

By default, neighboring NSF-aware routers will operate in NSF helper mode during a graceful restart.

If neighbors that are not NSF-aware are detected on a network interface during an NSF graceful restart, restart is aborted on that interface only and graceful restart will continue on other interfaces. To cancel restart for the entire OSPF process when neighbors that are not NSF-aware are detected during restart, configure this command with the enforce global keywords.

Note The NSF graceful restart will also be canceled for the entire process when a neighbor adjacency reset is detected on any interface or when an OSPF interface goes down.

Examples

The following example enables Cisco NSF graceful restart with the enforce global option:

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# cisco nsf enforce global
```

Related Commands

Command	Description
nsf cisco helper	Enables Cisco NSF helper mode on ASA.
nsf ietf	Enables IETF NSF

nsf cisco helper

To enable Cisco nonstop forwarding (NSF) helper mode on an ASA that is running Open Shortest Path First (OSPF), use the nsf cisco helper command in the router configuration mode. The Cisco NSF helper mode is enabled by default and can be disabled by issuing the no nsf cisco helper under router configuration mode.

nsf cisco helper
no nsf cisco helper

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco NSF helper mode is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

When an ASA has NSF enabled, the ASA is said to be NSF-capable and will operate in graceful restart mode--the OSPF router process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighboring ASAs of the NSF-capable ASA will be NSF-aware and will operate in NSF helper mode. When the NSF-capable ASA is performing graceful restart, the helper ASAs assist in the nonstop forwarding recovery process. If you do not want the ASA to help the restarting neighbor with nonstop forwarding recovery, enter the no nsf cisco helper command.

Examples

The following example disables the NSF helper mode:

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# no nsf cisco helper
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF on ASA.
nsf ietf	Enables IETF NSF

nsf ietf

To configure Internet Engineering Task Force (IETF) NSF operations on an ASA that is running OSPF, use the nsf ietf command in router configuration mode. To return to the default, use the no form of this command.

nsf ietf [**restart-interval** *seconds*]
no nsf ietf

Syntax Description

restart-interval seconds	(Optional) Specifies the length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default is 120.

Note For a restart interval below 30 seconds, graceful restart will be terminated.

Command Default

IETF NSF graceful restart mode is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command enables IETF NSF on an ASA. When NSF is enabled on an ASA, the ASA is NSF-capable and will operate in restarting mode.

If an ASA is expected to cooperate with a neighbor that is doing an NSF graceful restart only, the neighbor ASA must support NSF but NSF need not be configured on the router. When an ASA is running an application that supports NSF, the ASA is NSF-aware.

Examples

The following example disables the NSF helper mode:

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# nsf ietf restart-interval 240
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF on ASA.

Command	Description
nsf cisco helper	Enables Cisco NSF helper mode on ASA.
nsf ietf helper	Enables IETF NSF helper mode on ASA.

nsf ietf helper

The IETF NSF helper mode is enabled by default. To enable IETF NSF helper mode explicitly, use the nsf ietf helper command in router configuration mode. It can be disabled by using the no form of the command.

Optionally, strict link-state advertisement (LSA) checking can be enabled by using the nsf ietf helper strict-lsa-checking command.

nsf ietf helper [**strict-lsa-checking**]
no nsf ietf helper

Syntax Description

strict-lsa-checking	(Optional) Enables strict link-state advertisement (LSA) checking for helper mode.

Command Default

The IETF NSF helper mode is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

When an ASA has NSF enabled, it is said to be NSF-capable and will operate in graceful restart mode--the OSPF process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighboring ASAs of the NSF-capable ASA will be NSF-aware and will operate in NSF helper mode. When the NSF-capable ASA is performing graceful restart, the helper ASAs assist in the nonstop forwarding recovery process. If you do not want the ASA to help the restarting neighbor with nonstop forwarding recovery, enter the no nsf ietf helper command.

To enable strict LSA checking on both NSF-aware and NSF-capable ASAs, enter the nsf ietf helper strict-lsa-checking command. However, strict LSA checking will not become effective until the ASA becomes a helper ASA during an IETF graceful restart process. With strict LSA checking enabled, the helper ASA will terminate the helping process of the restarting ASA if it detects that there is a change to an LSA that would be flooded to the restarting ASA or if there is a changed LSA on the retransmission list of the restarting ASA when the graceful restart process is initiated.

Examples

The following example enables IETF NSF helper with strict LSA checking:

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa
(config-router)# nsf ietf helper strict-lsa-checking
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF on ASA.
nsf cisco helper	Enables Cisco NSF helper mode on ASA.
nsf ietf	Enables IETF NSF on ASA.

nt-auth-domain-controller

To specify the name of the NT Primary Domain Controller for this server, use the **nt-auth-domain-controller** command in aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

nt-auth-domain-controller *string*
no nt-auth-domain-controller

Syntax Description

string Specifies the name, up to 16 characters long, of the Primary Domain Controller for this server.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for NT Authentication AAA servers. You must have first used the **aaa-server host** command to enter host configuration mode. The name in the *string* variable must match the NT entry on the server itself.

Examples

The following example configures the name of the NT Primary Domain Controller for this server as "primary1":

```
ciscoasa
(config)# aaa-server svrgrp1 protocol nt
ciscoasa
(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa
(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa server host	Enters aaa server host configuration mode so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.

Command	Description
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

ntp authenticate

To enable authentication with an NTP server, use the **ntp authenticate** command in global configuration mode. To disable NTP authentication, use the **no** form of this command.

ntp authenticate
no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• —	Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you enable authentication, the ASA only communicates with an NTP server if it uses the correct trusted key in the packets (see the **ntp trusted-key** command). You must also specify the server key (see the **ntp server key** command), or the ASA will communicate to the server without authentication even when you configure the **ntp authenticate** command. The ASA also uses an authentication key to synchronize with the NTP server (see the **ntp authentication-key** command).

Examples

The following example identifies two NTP servers and enables authentication for the key IDs 1 and 2:

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

Related Commands

Command	Description
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.
show ntp status	Shows the status of the NTP association.

ntp authentication-key

To set a key to authenticate with an NTP server, use the **ntp authentication-key** command in global configuration mode. To remove the key, use the **no** form of this command.

ntp authentication-key *key_id* { **md5 | sha1 | sha256 | sha512 | cmac** } *key*
no ntp authentication-key *key_id* [{ **md5 | sha1 | sha256 | sha512 | cmac** } [**0|8**] *key*]

Syntax Description

0	(optional) Indicates <key_value> is plain text. Format is plain text if 0 or 8 is not present.
8	(optional) Indicates <key_value> is encrypted text. Format is plain text if 0 or 8 is not present.
key	Sets the key value as a string up to 32 characters in length.
key_id	Identifies a key ID between 1 and 4294967295. You must specify this ID as a trusted key using the **ntp trusted-key** command.
md5	Specifies the authentication algorithm as MD5.
sha1	Specifies the authentication algorithm as SHA-1.
sha256	Specifies the authentication algorithm as SHA-256.
sha512	Specifies the authentication algorithm as SHA-512.
cmac	Specifies the authentication algorithm as AES-CMAC.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• —	Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	The **sha1**, **sha256**, **sha512**, and **cmac** keywords were added.

Usage Guidelines

To use NTP authentication, also configure the **ntp authenticate** command and **ntp server key** command.

Examples

The following example identifies two NTP servers and enables authentication for the key IDs 1 and 2:

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.
show ntp status	Shows the status of the NTP association.

ntp server

To identify an NTP server to set the time on the ASA, use the **ntp server** command in global configuration mode. To remove the server, use the **no** form of this command.

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]
no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

Syntax Description

ip_address	Sets the IPv4 or IPv6 IP address of the NTP server.
key *key_id*	If you enable authentication using the **ntp authenticate** command, sets the trusted key ID for this server. See also the **ntp trusted-key** command.
source *interface_name*	Identifies the outgoing interface for NTP packets if you do not want to use the default interface in the routing table. Because the system does not include any interfaces in multiple context mode, specify an interface name defined in the admin context.
prefer	Sets this NTP server as the preferred server if multiple servers have similar accuracy. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the **prefer** keyword specifies which of those servers to use. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one. For example, the ASA uses a server of stratum 2 over a server of stratum 3 that is preferred.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to make the source interface optional.
9.12(1)	We added IPv6 support.
9.14(1)	We added NTPv4 support.

Usage Guidelines

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is. In multiple context mode, set the NTP server in the system configuration only.

Time derived from an NTP server overrides any time set manually.

The ASA supports NTPv4.

Examples

The following example identifies two NTP servers and enables authentication for the key IDs 1 and 2:

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.
show ntp status	Shows the status of the NTP association.

ntp trusted-key

To specify an authentication key ID to be a trusted key, which is required for authentication with an NTP server, use the **ntp trusted-key** command in global configuration mode. To remove the trusted key, use the **no** form of this command. You can enter multiple trusted keys for use with multiple servers.

ntp trusted-key *key_id*
no ntp trusted-key *key_id*

Syntax Description

key_id	Sets a key ID between 1 and 4294967295.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• —	Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To use NTP authentication, also configure the **ntp authenticate** command and **ntp server key** command. To synchronize with a server, set the authentication key for the key ID using the **ntp authentication-key** command.

Examples

The following example identifies two NTP servers and enables authentication for the key IDs 1 and 2:

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.

Command	Description
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.
show ntp status	Shows the status of the NTP association.

num-packets

To specify the number of request packets sent during an SLA operation, use the **num-packets** command in sla monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

num-packets *number*
no num-packets *number*

Syntax Description

number The number of packets sent during an SLA operation. Valid values are from 1 to 100.

Note When all the packets specified as the number argument (in this command) are lost, the tracked route has failed.

Command Default

The default number of packets sent for echo types is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Sla monitor protocol configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Increase the default number of packets sent to prevent incorrect reachability information due to packet loss.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes and the number of echo requests sent during an SLA operation to 5. All 5 packets must be lost before the tracked route is removed

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
request-data-size	Specifies the size of the request packet payload.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

nve

To create the Network Virtualization Endpoint (NVE) instance for VXLAN encapsulation, use the **nve** command in global configuration mode. To remove the NVE instance, use the **no** form of this command.

nve 1
no nve 1

Syntax Description

1	Specifies the NVE instance, which is always 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

You can configure one VTEP source interface per ASA or per security context. You can configure one NVE instance that specifies this VTEP source interface. All VNI interfaces must be associated with this NVE instance.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and associates the VNI 1 interface wth it:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

nve-only

To specify that the VXLAN source interface is NVE-only, use the **nve-only** command in interface configuration mode. To remove the NVE-only restriction, use the **no** form of this command.

nve-only
[**cluster**]
no nve-only

Syntax Description

Syntax Description

cluster	When configuring ASA virtual clustering, you must specify **nev-only cluster** for the cluster control link.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.17(1)	We added the **cluster** keyword to support ASA virtual clustering.

Usage Guidelines

You can configure one VTEP source interface per ASA or per security context. The VTEP is defined as a Network Virtualization Endpoint (NVE); VXLAN VTEP is the only supported NVE at this time.

In transparent mode, the **nve-only** setting is required for the VTEP interface and lets you configure an IP address for the interface. This command is optional for routed mode where this setting restricts traffic to VXLAN and common management traffic only on this interface.

For ASA virtual clustering, you must use a VXLAN interface for the cluster control link; in this case, specify **nev-only cluster**.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and specifies that it is NVE-only:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

nve-only

O

object-group

To define object groups that you can use to optimize your configuration, use the **object-group** command in global configuration mode. Use the **no** form of this command to remove object groups from the configuration.

object-group { **protocol | network | icmp-type | security | user | network-service** } *grp_name*
object-group service *grp_name* [**tcp | udp | tcp-udp**]

Syntax Description

grp_name	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.
icmp-type	(Not recommended, use **service** instead.) Defines a group of ICMP types such as echo and echo-reply. After entering the **object-group icmp-type** command, use the **icmp-object** and the **group-object** commands to add ICMP objects.
network	Defines a group of hosts or subnet IP addresses. After entering the **object-group network** command, use the **network-object** and the **group-object** commands to add network objects. You can create a group with a mix of IPv4 and IPv6 addresses. **Note** You cannot use a mixed object group for NAT.
network-service	Defines a group of subnets or domain names with optional service specifications. After entering this command, use the **network-service-member** command to add network-service objects, or the **domain** and **subnet** commands to add members directly.
protocol	(Not recommended, use **service** instead.) Defines a group of protocols such as TCP and UDP. After entering the **object-group protocol** command, use the **protocol-object** and the **group-object** commands to add protocol objects.
security	Defines a security group object for use with Cisco TrustSec. After entering the **object-group protocol** command, use the **security-group** and the **group-object** commands to add security group objects.
service	Defines a service based on protocol, ICMP types, and TCP/UDP/SCTP ports.
[tcp | udp | tcp-udp	To define a mixed group of services, or SCTP ports, do not specify the protocol type for the object-group. After entering the **object-group service** command, add service objects to the service group with the **service-object** and the **group-object** commands. This is the preferred method, even if the object is meant to include only lists of TCP or UDP (or both) ports. Using the **tcp**, **udp**, and **tcp-udp** keywords directly on the object-group service command is not recommended. Instead, leave these keywords off the command and configure TCP and UDP ports on the **service-object** command. If you do include one of these keywords, use the **port-object** and the **group-object** commands to add port groups.
user	Defines users and user groups that you can use to control access with the identity firewall. After entering the **object-group protocol** command, use the **user**, **user-group**, and the **group-object** commands to add user and user group objects.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	Support for the **user** keyword was added to support identity firewall.
9.0(1)	You can now create network object groups that can support a mix of both IPv4 and IPv6 addresses. Support for the **security** keyword was added to support Cisco TrustSec.
9.14	The **icmp-type** keyword was deprecated. Use the **service** keyword, and specify **service icmp** in the object instead.
9.17(1)	The **network-service** keyword was added.

Usage Guidelines

Objects such as hosts or services can be grouped, and then you can use the object group in features such as ACLs (**access-list**) and NAT (**nat**). This example shows the use of a network object group in an ACL:

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group NWgroup1
```

You can group commands hierarchically; an object group can be a member of another object group.

Examples

The following example shows how to use the **object-group network** command to create a network object group:

```
ciscoasa(config)# object-group network sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.eng.ftp.servcers
ciscoasa(config-network-object-group)# network-object host 172.23.56.194
ciscoasa(config-network-object-group)# network-object 192.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# exit
```

The following example shows how to use the **object-group network** command to create a network object group that includes an existing object-group:

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers

ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224

ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

The following example shows how to use the **group-object** mode to create a new object group that consists of previously defined objects, and then how to use these objects in an ACL:

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)#access-list all permit tcp object-group all_hosts any eq www
```

Without the **group-object** command, you need to define the *all_hosts* group to include all the IP addresses that have already been defined in *host_grp_1* and *host_grp_2*. With the **group-object** command, the duplicated definitions of the hosts are eliminated.

The following example shows how to add both TCP and UDP services to a service object group:

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

The following example shows how to add multiple service objects to a service object group:

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# group-object SSH
ciscoasa(config-service-object-group)# group-object EIGRP
ciscoasa(config-service-object-group)# group-object HTTPS
```

The following example shows how to add a mix of protocol, port, and ICMP specifications in a service object group:

```
ciscoasa(config)# object-group service mixed
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

The following example shows how to use the **service-object** subcommand, which is useful for grouping TCP and UDP services:

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
```

```
ciscoasa(config-network-object-group)# network-object host kqk.suu.pyl.gnl
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group locals
 object-group remote
```

The following example shows how to use the **object-group user** command to create user group objects:

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

(Not recommended, use service objects instead.) The following example shows how to use the **object-group icmp-type** mode to create a ICMP object group:

```
ciscoasa(config)# object-group icmp-type icmp-allowed
ciscoasa(config-icmp-object-group)# icmp-object echo
ciscoasa(config-icmp-object-group)# icmp-object time-exceeded
ciscoasa(config-icmp-object-group)# exit
```

(Not recommended, use service objects instead.) The following example shows how to use the **object-group protocol** mode to create a protocol object group:

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit
ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit
```

(Not recommended, leave off the **tcp** keyword and define the port with the **service-object** command instead.) The following example shows how to use the **object-group service** mode to create a TCP port object group:

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service-object-group)# group-object eng_www_service
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object range 2000 2005
ciscoasa(config-service-object-group)# exit
```

The following examples show how to use object groups to simplify the access list configuration. This grouping enables the access list to be configured in 1 line instead of 24 lines, which would be needed if no grouping is used.

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host
209.165.200.225
ciscoasa(config-network-object-group)# network-object host
209.165.200.230
ciscoasa(config-network-object-group)# network-object host
209.165.200.235
ciscoasa(config-network-object-group)# network-object host
209.165.200.240
ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100
ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```

Note The **show running-config access-list** command displays the access list as configured with the object group names. The **show access-list** command displays this information plus the access list entries that use groups expanded out into individual entries without their object groupings.

The following example configures a set of SaaS applications using previously-defined network-service objects.

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
port-object	Adds a port object to a service object group.
security-group	Adds a security group to a security group object group.
show running-config object-group	Displays the current object groups.
user	Adds a username to a user group object.
user-group	Adds a user group name to a user group object.

object-group-search

To enable ACL optimization, use the **object-group-search** command in global configuration mode. Use the **no** form of this command to disable ACL optimization.

object-group-search { **access-control | threshold** }
no object-group-search { **access-control | threshold** }

Syntax Description

access-control	Enables object group search for access control rules.
threshold	Enables a maximum threshold for object group search processing. See the usage notes for detailed information.

Command Default

(Pre-9.18) Object group search is disabled by default. The threshold is also disabled by default.

Starting with 9.18, object group search is enabled by default for access control for new deployments.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.12(1)	The **threshold** keyword was added. The keyword was also added in interim releases of 9.8, 9.9, and 9.10.
9.18(1)	The default for access control was changed to enabled for new deployments. You must enable it on upgrades if it was not previously enabled.

Usage Guidelines

The **object-group-search** command optimizes all ACLs in the inbound direction.

You can reduce the memory required to search access rules by enabling object group search, but this is at the expense rule of lookup performance and increased CPU utilization. When enabled, object group search does not expand ACLs that use network or service objects in the ASP table, but instead searches access rules for matches based on those group definitions. You will see this in the **show access-list** output.

Object group search is subject to a threshold. For each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. This check is to prevent performance degradation. Configure your rules to prevent an excessive number of matches. Avoid the creation of duplicate objects to prevent reaching the threshold.

Starting in release 9.12(1), and in interim releases back to 9.8(x), this threshold is disabled by default. Use the **show running-config all object-group-search** command to determine whether the threshold option is configured, and if so, the current setting.

When you enable object group search, and you have a significant number of features enabled, a large number of active connections, and large ACLs for your access groups, there will be a connection drop during the operation and a performance drop while establishing new connections. These drops can happen even if you enable transactional commit (**asp rule-engine transactional-commit access-group**).

Note Object group search works with network and service objects only. It does not work with security group or user objects. Do not enable this feature if the ACLs include security groups. The result can be inactive ACLs or other unexpected behavior.

Examples

The following example shows how to use the **object-group-search** command to enable ACL optimization:

```
ciscoasa(config)# object-group-search access-control
```

The following is sample output from the **show access-list** command when **object-group-search** is not enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group BLK-LAN
 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=2) 0xce8596ec
    access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

The following is sample output from the **show access-list** command when **object-group-search** is enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
```

```
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

Related Commands

Command	Description
clear config object-group search	Clears the object-group-search configuration.
show object-group	Shows the hit count if the object group is of the network object-group type.
show running-config object-group	Displays the current object groups.
show running-config object-group-search	Show the object-group-search configuration in the running configuration.

object network

To configure a named network object, use the **object network** command in global configuration mode. Use the **no** form of this command to remove the object from the configuration.

object network *name* [**rename** *new_obj_name*]
no object network *name*

Syntax Description

name	Specifies the name of the network object. The name can be from 1 to 64 characters in length, consisting of letters, numbers, and the following special characters: underscore, hyphen, comma, forward slash, and period. Objects and object groups share the same name space.
rename *new_obj_name*	(Optional) Renames the object to the new object name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
8.4(2)	Support for fully-qualified domain names (FQDN) was added. See the **fqdn** command.

Usage Guidelines

The network object can contain a host, a network, a range IP addresses (IPv4 or IPv6), or an FQDN. After you enter the command, use the **host**, **fqdn**, **subnet**, or **range** command to add one address to the object.

You can also enable NAT rules on this network object using the **nat** command. You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules, you need to create multiple objects that specify the same IP address, for example, **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02**, and so on.

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a network object:

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully-qualified domain name network object.
host	Specifies a host network object.
nat	Enables NAT for the network object.
object-group network	Creates a network object group.
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

object network-service

To configure a named network-service object, use the **object network-service** command in global configuration mode. Use the **no** form of this command to remove the object from the configuration.

object network-service *name* [**dynamic**]
no object network-service *name*

Syntax Description

dynamic	(Optional.) The **dynamic** keyword means that the object will not be saved to the running configuration, it will be shown in the **show object** output only. The **dynamic** keyword is primarily for use by external device managers.
name	The name can be up to 128 characters, and can include spaces. If you include spaces, you must enclose the name in double quotation marks.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(2)	This command was added.

Usage Guidelines

A network-service object defines a single application. It defines the application location either by subnet specification or more commonly, DNS domain name. Optionally, you can include protocol and port to narrow the scope of the application.

You can use these objects in network-service group objects only; you cannot directly use a network-service object in an access control list entry (ACE).

Add one or more application locations and optional services to the object using one of the following commands. Use the **no** form of the command to remove the location. You can enter these commands multiple times.

- **domain** *domain_name* [*service*]—The DNS name, up to 253 characters. This can be fully-qualified (such as www.example.com) or partial (such as example.com), in which case the object matches all subdomains, that is, servers with the partial name (such as www.example.com, www1.example.com, long.server.name.example.com, and so forth). Connections will be matched against the longest name if an exact match is available. The domain name can resolve to multiple IP addresses.

- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

The service specification for these commands is the same. Specify the service only if you want to limit the scope of the connections matched. By default, any connection to the resolved IP addresses matches the object.

protocol [*operator port*]

where:

- *protocol* is the protocol used in the connection, such as tcp, udp, ip, and so forth. Use ? to see the list of protocols.
- (TCP/UDP only.) *operator* is one of the following:
  - **eq** equals the port number specified.
  - **lt** means any port less than the specified port number.
  - **gt** means any port greater than the specified port number.
  - **range** means any port between the two ports specified.
- (TCP/UDP only.) *port* is the port number, 1-65535 or a mnemonic, such as www. Use ? to see the mnemonics. For ranges, you must specify two ports, with the first port being a lower number than the second port.

Example

Following is an example of a network-service object.

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Related Commands

Command	Description
app-id	Specifies an application ID for the object.
clear object	Clears hit counts for network-service objects.
description	Adds a description to the object.
domain	Specifies domain name for the object.
object-group network-service	Creates a network-service object group.
show object	Shows the network-service objects.
subnet	Specifies a subnet for the object.

object service

To configure a service object that is automatically reflected in all configurations in which the object is used, use the **object service** command in global configuration mode. Use the **no** form of this command to remove the object.

object service *name* [**rename** *new_obj_name*]
no object service *object name* [**rename** *new_obj_name*]

Syntax Description

name	Specifies the name of the service object. The name can be from 1 to 64 characters in length, consisting of letters, numbers, and the following special characters: underscore, hyphen, comma, and period. The object name must start with a letter.
rename *new_obj_name*	(Optional) Renames the object to the new object name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

The service object can contain a protocol, ICMP, ICMPv6, or TCP /UDP/SCTP port or port ranges. After you enter the command, use the **service** command to add one service specification to the object.

If you configure an existing service object with a different protocol and port (or ports), the new configuration replaces the existing protocol and port (or ports) with the new ones.

Examples

The following example shows how to create a service object:

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

Related Commands

Command	Description
clear configure object	Clears all objects created.

Command	Description
service	Configures the protocol and port for the service object.

ocsp disable-nonce

To disable the nonce extension, use the ocsp disable-nonce command in crypto ca trustpoint configuration mode. To re-enable the nonce extension, use the **no** form of this command.

ocsp disable-nonce
no ocsp disable-nonce

Syntax Description

This command has no arguments or keywords.

Command Default

By default, OCSP requests include a nonce extension.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When you use this command, the OCSP request does not include the OCSP nonce extension, and the ASA does not check it. By default, OCSP requests include a nonce extension, which cryptographically binds requests with responses to avoid replay attacks. However, some OCSP servers use pre-generated responses that do not contain this matching nonce extension. To use OCSP with these servers, you must disable the nonce extension.

Examples

The following example shows how to disable the nonce extension for a trustpoint called newtrust.

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode. Use this command in global configuration mode.
match certificate	Configures an OCSP override rule.
ocsp interface*nameif*	Specifies the interface that can be used in OCSP revocation check.

Command	Description
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

ocsp interface

To configure the source interface for ASA to reach OCSP, use **interface** *nameif* command in the crypto ca trustpool configuration mode. To remove the interface from the configuration, use the **no** form of this command.

ocsp interface *nameif*
no ocsp interface *nameif*

Syntax Description

interface *nameif*	Specifies the interface that the ASA uses to reach the OCSP server.

Command Default

No defaults for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration.	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

By default, OCSP uses the global routing table that does not include management interface entries. If OCSP is behind a management interface, the OCSP revocation check does not succeed. When you use this command, the OCSP revocation check can be configured to use the interfaces, including management interface as required.

Examples

The following example shows how to configure the source interface for OCSP.

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
```

```
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt  url
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url  ?

crypto-ca-trustpoint mode commands/options:
  LINE < 500 char  URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url http://lal-bagh:8888
```

Related Commands

Command	Description
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
revocation-check	Specifies the methods to use for revocation checking, and the order in which to try them.

ocsp url

To configure an OCSP server for the ASA to use to check all certificates associated with a trustpoint rather than the server specified in the AIA extension of the client certificate, use the **ocsp url** command in crypto ca trustpoint configuration mode. To remove the server from the configuration, use the **no** form of this command.

ocsp url *URL*
no ocsp url

Syntax Description

URL Specifies the HTTP URL for the OCSP server.

Note ASA supports both IPv4 and IPv6 OCSP URLs. Enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.20(1)	Support for IPv6 OCSP URL was added.

Usage Guidelines

The ASA supports only HTTP URLs, and you can specify only one URL per trustpoint.

The ASA provides three ways to define an OCSP server URL, and it attempts to use OCSP servers according to how you define them, in the following order:

- An OCSP server you set using **match certificate** command.
- An OCSP server you set using the **ocsp url** command.
- The OCSP server in the AIA field of the client certificate.

If you do not configure an OCSP URL via the **match certificate** command or the **ocsp url** command, the ASA uses the OCSP server in the AIA extension of the client certificate. If the certificate does not have an AIA extension, revocation status checking fails.

Examples

The following example shows how to configure an OCSP server with the URL http://10.1.124.22.

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

The following example shows how to configure OCSP with the IPv6 URL:

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp url  http://[0:0:0:0:0:ffff:0a01:7c16]
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode. Use this command in global configuration mode.
match certificate	Configures an OCSP override rule,
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
ocsp interface*nameif*	Specifies the interface that can be used in OCSP revocation check.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

onscreen-keyboard(Deprecated)

To insert an onscreen keyboard into the logon pane or all panes with a login/password requirement, use the **onscreen-keyboard** command in webvpn mode. To remove a previously configured onscreen keyboard, use the **no** version of the command.

onscreen-keyboard { **logon** | **all** }
no onscreen-keyboard [**logon** | **all**]

Syntax Description

logon	Inserts the onscreen keyboard for the logon pane.
all	Inserts the onscreen keyboard for the logon pane, and for all other panes with a login/password requirement.

Command Default

No onscreen keyboard.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The onscreen keyboard lets you enter user credentials without keystrokes.

Examples

The following example shows how to enable the onscreen keyboard for the logon page:

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 onscreen-keyboard logon
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn mode, which lets you configure attributes for clientless SSLVPN connections.

ospf authentication

To enable the use of OSPF authentication, use the **ospf authentication** command in interface configuration mode. To restore the default authentication stance, use the **no** form of this command.

ospf authentication { **key-chain key-chain-name** | **message-digest** | **null** }
no ospf authentication

Syntax Description

key-chain *key-chain-name*	(Optional) Specifies a key chain to use for authentication. The key-name argument can be a maximum of 63 alphanumeric characters.
message-digest	(Optional) Specifies to use OSPF message digest authentication.
null	(Optional) Specifies to not use OSPF authentication.

Command Default

By default, OSPF authentication is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.12(1)	Key chain feature was added to support rotating keys for OSPF authentication.

Usage Guidelines

Before using the **ospf authentication** command, configure a password for the interface using the **ospf authentication-key** command. If you use the **message-digest** keyword, configure the message-digest key for the interface with the **ospf message-digest-key** command.

For backward compatibility, authentication type for an area is still supported. If the authentication type is not specified for an interface, the authentication type for the area will be used (the area default is null authentication).

When this command is used without any options, simple password authentication is enabled.

Examples

The following example shows how to enable simple password authentication for OSPF on the selected interface:

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

The following example shows how to enable key-chain password authentication for OSPF on the selected interface:

```
ciscoasa(config)# interface gigabitEthernet 0/0
ciscoasa(config-if)# ospf authentication key-chain CHAIN-INT-OSPFKEYS
```

Related Commands

Command	Description
ospf **authentication-key**	Specifies the password used by neighboring routing devices.
ospf message-digest-key	Enables MD5 authentication and specifies the MD5 key.

ospf authentication-key

To specify the password used by neighboring routing devices, use the **ospf authentication-key** command in interface configuration mode. To remove the password, use the **no** form of this command.

ospf authentication-key [**0** | **8** } *password*
no ospf authentication-key

Syntax Description

0	Specifies an unencrypted password will follow
8	Specifies an encrypted password will follow.
password	Assigns an OSPF authentication password for use by neighboring routing devices. The password must be less than 9 characters. You can include blank space between two characters. Spaces at the beginning or end of the password are ignored.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The password created by this command is used as a key that is inserted directly into the OSPF header when routing protocol packets are originated. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Examples

The following example shows how to specify a password for OSPF authentication:

```
ciscoasa(config-if)# ospf authentication-key 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands

Command	Description
area authentication	Enables OSPF authentication for the specified area.
ospf authentication	Enables the use of OSPF authentication.

ospf cost

To specify the cost of sending a packet through the interface, use the **ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospf cost *interface_cost*
no ospf cost

Syntax Description

interface_cost	The cost (a link-state metric) of sending a packet through an interface. This is an unsigned integer value from 0 to 65535. 0 represents a network that is directly connected to the interface, and the higher the interface bandwidth, the lower the associated cost to send packets across that interface. In other words, a large cost value represents a low bandwidth interface and a small cost value represents a high bandwidth interface. The OSPF interface default cost on the ASA is 10. This default differs from Cisco IOS software, where the default cost is 1 for Fast Ethernet and Gigabit Ethernet and 10 for 10BaseT. This is important to take into account if you are using ECMP in your network.

Command Default

The default *interface_cost* is 10.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **ospf cost** command lets you explicitly specify the cost of sending a packet on an interface. The *interface_cost* parameter is an unsigned integer value from 0 to 65535.

The **no ospf cost** command allows you to reset the path cost to the default value.

Examples

The following example show how to specify the cost of sending a packet on the selected interface:

```
ciscoasa(config-if)# ospf cost 4
```

Related Commands

Command	Description
show running-config interface	Displays the configuration of the specified interface.

ospf database-filter

To filter out all outgoing LSAs to an OSPF interface during synchronization and flooding, use the **ospf database-filter** command in interface configuration mode. To restore the LSAs, use the **no** form of this command.

ospf database-filter all out
no ospf database-filter all out

Syntax Description

all	Filters all outgoing LSAs to an OSPF interface.
out	

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **ospf database-filter** command filters outgoing LSAs to an OSPF interface. The **no ospf database-filter all out** command restores the forwarding of LSAs to the interface.

Examples

The following example shows how to use the **ospf database-filter** command to filter outgoing LSAs:

```
ciscoasa(config-if)# ospf database-filter all out
```

Related Commands

Command	Description
show interface	Displays interface status information.

ospf dead-interval

To specify the interval before neighbors declare a router down, use the **ospf dead-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf dead-interval { *seconds* **minimal** | **hello-multiplier** *multiplier* }
no ospf dead-interval

Syntax Description

seconds	The length of time during which no hello packets are seen. The default for *seconds* is four times the interval set by the **ospf hello-interval** command (which ranges from 1 to 65535).
minimal	Sets the dead interval to 1 second. Using this keyword requires that the hello-multiplier keyword and multiplier argument are also configured.
hello-multiplier multiplier	Integer value in the range from 3 to 20, representing the number of hello packets sent during 1 second.

Command Default

The default value for *seconds* is four times the interval set by the **ospf hello-interval** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.2(1)	Support for Fast Hello packets was added.

Usage Guidelines

The ospf dead-interval command lets you set the dead interval before neighbors to declare the router down (the length of time during which no hello packets are seen). The *seconds* argument specifies the dead interval and must be the same for all nodes on the network. The default for *seconds* is four times the interval set by the **ospf hello-interval** command from 1 to 65535.

The **no** ospf dead-interval command restores the default interval value.

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network.

Specifying a smaller dead interval (seconds) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

OSPF Support for Fast Hello Packets

By specifying the minimal and hello-multiplier keywords with a multiplier argument, you are enabling OSPF fast hello packets. The minimal keyword sets the dead interval to 1 second, and the hello-multiplier value sets the number of hello packets sent during that 1 second, thus providing subsecond or "fast" hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

Use the show ospf interface command to verify the dead interval and fast hello interval.

Examples

In the following example, OSPF Support for Fast Hello Packets is enabled by specifying the minimal keyword and the hello-multiplier keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

Related Commands

Command	Description
ospf hello-interval	Specifies the interval between hello packets sent on an interface.
show ospf interface	Displays OSPF-related interface information.

ospf hello-interval

To specify the interval between hello packets sent on an interface, use the **ospf hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

ospf hello-interval *seconds*
no ospf hello-interval

Syntax Description

seconds	Specifies the interval between hello packets that are sent on the interface; valid values are from 1 to 65535 seconds.

Command Default

The default value for **hello-interval** *seconds* is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the OSPF hello interval to 5 seconds:

```
ciscoasa(config-if)# ospf hello-interval 5
```

Related Commands

Command	Description
ospf dead-interval	Specifies the interval before neighbors declare a router down.
show ospf interface	Displays OSPF-related interface information.

ospf message-digest-key

To enable OSPF MD5 authentication, use the **ospf message-digest-key** command in interface configuration mode. To remove an MD5 key, use the **no** form of this command.

ospf message-digest-key *key-id* **md5** [**0** | **8**] *key*
no ospf message-digest-key

Syntax Description

key-id	Enables MD5 authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
md5 *key*	Alphanumeric password of up to 16 bytes. You can include spaces between key characters. Spaces at the beginning or end of the key are ignored. MD5 authentication verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
0	Specifies an unencrypted password will follow
8	Specifies an encrypted password will follow.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The ospf message-digest-key command lets you enable MD5 authentication. The **no** form of the command let you remove an old MD5 key. *key_id* is a numerical identifier from 1 to 255 for the authentication key. *key* is an alphanumeric password of up to 16 bytes. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Examples

The following example shows how to specify an MD5 key for OSPF authentication:

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication.
ospf authentication	Enables the use of OSPF authentication.

ospf mtu-ignore

To disable OSPF maximum transmission unit (MTU) mismatch detection on receiving database packets, use the **ospf mtu-ignore** command in interface configuration mode. To restore MTU mismatch detection, use the **no** form of this command.

ospf mtu-ignore
no ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

By default, **ospf mtu-ignore** is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange Database Descriptor (DBD) packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.The **ospf mtu-ignore** command disables OSPF MTU mismatch detection on receiving DBD packets. It is enabled by default.

Examples

The following example shows how to disable the **ospf mtu-ignore** command:

```
ciscoasa(config-if)# ospf mtu-ignore
```

Related Commands

Command	Description
show interface	Displays interface status information.

ospf network point-to-point non-broadcast

To configure the OSPF interface as a point-to-point, non-broadcast network, use the **ospf network point-to-point non-broadcast** command in interface configuration mode. To remove this command from the configuration, use the **no** form of this command.

ospf network point-to-point non-broadcast
no ospf network point-to-point non-broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **ospf network point-to-point non-broadcast** command lets you to transmit OSPF routes over VPN tunnels.

When the interface is specified as point-to-point, the OSPF neighbors have to be manually configured; dynamic discovery is not possible. To manually configure OSPF neighbors, use the **neighbor** command in router configuration mode.

When an interface is configured as point-to-point, the following restrictions apply:

- > You can define only one neighbor for the interface.
- You need to define a static route pointing to the crypto endpoint.
- The interface cannot form adjacencies unless neighbors are configured explicitly.
- If OSPF over the tunnel is running on the interface, regular OSPF with an upstream router cannot be run on the same interface.
- You should bind the crypto-map to the interface before specifying the OSPF neighbor to ensure that the OSPF updates are passed through the VPN tunnel. If you bind the crypto-map to the interface after specifying the OSPF neighbor, use the **clear local-host all** command to clear OSPF connections so the OSPF adjacencies can be established over the VPN tunnel.

Examples

The following example shows how to configure the selected interface as a point-to-point, non-broadcast interface:

```
ciscoasa(config-if)# ospf network point-to-point non-broadcast
ciscoasa(config-if)#
```

Related Commands

Command	Description
neighbor	Specifies manually configured OSPF neighbors.
show interface	Displays interface status information.

ospf priority

To change the OSPF router priority, use the **ospf priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

ospf priority *number*
no ospf priority [*number*]

Syntax Description

number	Specifies the priority of the router; valid values are from 0 to 255.

Command Default

The default value for *number* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

In multiple context mode, for shared interfaces, specify 0 to ensure the device does not become the designated router. OSPFv2 instances cannot form adjacencies with each other across shared interfaces.

Examples

The following example shows how to change the OSPF priority on the selected interface:

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

ospf retransmit-interval

To specify the time between LSA retransmissions for adjacencies belonging to the interface, use the **ospf retransmit-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf retransmit-interval [*seconds*]
no ospf retransmit-interval [*seconds*]

Syntax Description

seconds	Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.

Command Default

The default value of **retransmit-interval** *seconds* is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it will re-send the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example shows how to change the retransmit interval for LSAs:

```
ciscoasa(config-if)# ospf retransmit-interval 15
ciscoasa(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ospf transmit-delay** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf transmit-delay [*seconds*]
no ospf transmit-delay [*seconds*]

Syntax Description

seconds	Sets the estimated time required to send a link-state update packet on the interface. The default value is 1 second with a range from 1 to 65535 seconds.

Command Default

The default value of *seconds* is 1 second.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

LSAs in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the transmit delay to 3 seconds for the selected interface:

```
ciscoasa(config-if)# ospf restransmit-delay 3
ciscoasa(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

otp expiration

To specify the duration in hours that an issued One-Time Password (OTP) for the local Certificate Authority (CA) enrollment page is valid, use the **otp expiration** command in ca server configuration mode. To reset the duration to the default number of hours, use the **no** form of this command.

otp expiration *timeout*
no otp expiration

Syntax Description

timeout Specifies the time in hours users have to enroll for a certificate from the local CA before the OTP for the enrollment page expires. Valid values range from 1 to 720 hours (30 days).

Command Default

By default, a OTP expiration for certificate enrollment is 72 hours (3 days).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The OTP expiration period specifies the number of hours that a user has to log in to the enrollment page of the CA server. After the user logs in and enrolls for a certificate, the time period specified by the **enrollment retrieval** command starts.

Note The user OTP for enrolling for a certificate with the enrollment interface page is also used as the password to unlock the PKCS12 file containing the issued certificate and keypair for that user.

Examples

The following example specifies that the OTP for the enrollment page applies for 24 hours:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# otp expiration 24
ciscoasa
(config-ca-server)
#
```

The following example resets the OTP duration to the default of 72 hours:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# no otp expiration
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
enrollment-retrieval	Specifies the time in hours that an enrolled user can retrieve a PKCS12 enrollment file.
show crypto ca server	Displays the certificate authority configuration.

output console

To send the output of the **action** commands to the console, use the **output console** command in event manager applet configuration mode. To remove the console as an output destination, use the **no** form of this command.

output console
no output console

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to send the output of the **action** commands to the console.

Examples

The following example sends the output of the **action** commands to the console:

```
ciscoasa(config-applet)# output console
```

Related Commands

Command	Description
output file append	Writes the **action** command output to a single file, but that file is appended to every time.
output file new	Sends the output of the **action** commands to a new file for each applet that is invoked.
output file overwrite	Writes the **action** command output to a single file, which is truncated every time.
output file rotate	Creates a set of files that are rotated.
output none	Discards any output from the **action** commands.

output file

To redirect the **action** command output to a specified file, use the **output file** command in event manager applet configuration mode. To remove the specified action, use the **no** form of this command.

output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]
no output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

Syntax Description

append *filename*	Continuously appends output to the specified filename, which is a local (to the ASA) filename.
new	Creates a new file for output named eem-*applet* -*timestamp* .log, in which *applet* is the name of the event manager applet and *timestamp* is a dated timestamp in the format of YYYYMMDD-hhmmss.
overwrite *filename*	Writes output to the specified filename, but truncates the output each time an event manager applet is invoked.
rotate *n*	Creates a file for output named eem-*applet* -*x* .log, in which *applet* is the name of the event manager applet, and *x* is the file number. When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written. The newest file is indicated by 0, and the oldest file is indicated by the highest number (*n* -1). The *n* argument specifies the rotate value. Valid values range from 2 - 100.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use the **output file** command to redirect the **action** command output to a specified file.

Examples

The following example appends output to a single file:

```
ciscoasa(config-applet)# output file append examplefile1
```

The following example sends the output of the **action** commands to a new file:

```
ciscoasa(config-applet)# output file new
```

The following example writes output to a single, truncated file:

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

The following example creates a set of files that are rotated:

```
ciscoasa(config-applet)# output file rotate 50
```

Related Commands

Command	Description
output console	Sends the output of the **action** commands to the console.
output none	Discards any output from the **action** commands.

output none

To discard any output from the **action** commands, use the **output none** command in event manager applet configuration mode. To retain output from the **action** commands, use the **no** form of this command.

output none
no output none

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to discard any output from **action** commands.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to discard any output from the **action** commands.

Examples

The following example discards any output from the **action** commands:

```
ciscoasa(config-applet)# output none
```

Related Commands

Command	Description
output console	Sends the output of the **action** commands to the console.
output file append	Writes the **action** command output to a single file, but that file is appended to every time.
output file new	Sends the output of the **action** commands to a new file for each applet that is invoked.
output file overwrite	Writes the **action** command output to a single file, which is truncated every time.
output file rotate	Creates a set of files that are rotated.

outstanding (Deprecated)

Note The last supported release of this command was Version 9.5(1).

To limit the number of unauthenticated e-mail proxy sessions, use the **outstanding** command in the applicable e-mail proxy configuration mode. To remove the attribute from the configuration, use the **no** form of this command.

outstanding { *number* }
no outstanding

Syntax Description

number	The number of unauthenticated sessions permitted. The range is from 1 to 1000.

Command Default

The default is 20.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s	• Yes	—	• Yes	•	—
Imap4s	• Yes	—	• Yes	—	—
Smtps	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

Use the no version of this command to remove the attribute from the configuration, which permits an unlimited number of unauthenticated sessions. This also limit s DOS attacks on the e-mail ports.

E-mail proxy connections have three states:

- **1.**A new e-mail connection enters the “unauthenticated” state.
- **2.**When the connection presents a username, it enters the “authenticating” state.
- **3.**When the ASA authenticates the connection, it enters the “authenticated” state.

If the number of connections in the unauthenticated state exceeds the configured limit, the ASA terminates the oldest unauthenticated connection, preventing overload. It does not terminate authenticated connections.

Examples

The following example shows how to set a limit of 12 unauthenticated sessions for POP3S e-mail proxy.

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)
#
 outstanding 12
```

override-account-disable (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To override an account-disabled indication from a AAA server, use the **override-account-disable** command in tunnel-group general-attributes configuration mode. To disable an override, use the **no** form of this command.

override-account-disable
no override-account-disable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

This command is valid for servers, such as RADIUS with NT LDAP, and Kerberos, that return an "account-disabled" indication.

You can configure this attribute for IPsec RA and WebVPN tunnel-groups.

Examples

The following example allows overriding the "account-disabled" indicator from the AAA server for the WebVPN tunnel group "testgroup":

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

The following example allows overriding the "account-disabled" indicator from the AAA server for the IPsec remote access tunnel group "QAgroup":

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the tunnel-group database or the configuration for a particular tunnel group.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

override-svc-download

To configure the connection profile to override the group policy or username attributes configuration for downloading an AnyConnect or SSL VPN client, use the **override-svc-download** command from tunnel-group webvpn attributes configuration mode. To remove the command from the configuration, use the **no** form of the command:

override-svc-download enable
no override-svc-download enable

Command Default

The default is disabled. The ASA does not override the group policy or username attributes configuration for downloading the client.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The security appliance allows clientless, AnyConnect, or SSL VPN client connections for remote users based on whether clientless and/or SSL VPN is enabled in the group policy or username attributes with the **vpn-tunnel-protocol** command. The **svc ask** command further modifies the client user experience by prompting the user to download the client or return to the WebVPN home page.

However, you may want clientless users logging in under specific tunnel groups to not experience delays waiting for the download prompt to expire before being presented with the clientless SSL VPN home page. You can prevent delays for these users at the connection profile level with the **override-svc-download** command. This command causes users logging through a connection profile to be immediately presented with the clientless SSL VPN home page regardless of the **vpn-tunnel-protocol** or **svc ask** command settings.

Examples

In the following example, the user enters tunnel-group webvpn attributes configuration mode for the connection profile >*engineering* and enables the connection profile to override the group policy and username attribute settings for client download prompts:

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

Related Commands

Command	Description
show webvpn svc	Displays information about installed SSL VPN clients.
svc	Enables or requires the SSL VPN client for a specific group or user.
svc image	Specifies a client package file that the ASA expands in cache memory for downloading to remote PCs.

pa - pn

packet-tracer

The packet-tracer command can be used in privileged EXEC mode to generate a 5-to-6 tuple packet against a firewall's current configurations. For clarity, the packet-tracer syntax is shown separately for ICMP, TCP/UDP/SCTP, and IP packet modeling. You can replay mulitple packets and trace a complete workflow using the **pcap** keyword.

packet-tracer input *ifc_name* [**vlan-id** *vlan_id*] **icmp** [**inline-tag** *tag*] { *src_ip* | **user** *username* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } *icmp_value* [*icmp_code*] [*dmac*] { *dst_ip* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } [**detailed**] [**xml**]

packet-tracer input *ifc_name* [**vlan-id** *vlan_id*] **rawip** [**inline-tag** *tag*] { *src_ip* | **user** *username* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } *protocol* [*dmac*] { *dst_ip* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } [**detailed**] [**xml**]

packet-tracer input *ifc_name* [**vlan-id** *vlan_id*] { **tcp** | **udp** | **sctp** } [**inline-tag** *tag*] { *src_ip* | **user** *username* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } *src_port* [*dmac*] { *dst_ip* | **security-group** { **name** *name* | **tag** *tag* } | **fqdn** *fqdn_string* } *dst_port* [*options*] [**detailed**] [**xml**]

packet-tracer input *ifc_name* **pcap** *pcap_filename* [**bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force**]

Syntax Description

bypass-checks	(Optional) Bypasses the security checks for simulated packets.
decrypted	(Optional) Considers simulated packet as IPsec/SSL VPN decrypted.
detailed	(Optional) Provides detailed trace results information.
dmac	Specifies the destination MAC address. It provides a complete picture of the life of a switched packet by displaying the output interface selection and also the packet drop due to the unknown destination MAC address.
dst_ip	Specifies the destination IPv4 or IPv6 address for the packet trace.
dst_port	Specifies the destination port for a TCP/UDP/SCTP packet trace. Depending on the port, you may have additional options, including for **vxlan** and **geneve** inner packets.
fqdn *fqdn_string*	Specifies the fully qualified domain name of the host, which can be both the source and destination IP address. Supports the FQDN for IPv4 only.
force	Removes existing pcap trace and executes a new pcap file.
icmp	Specifies the protocol to use is ICMP.
icmp_type	Specifies the ICMP type for an ICMP packet trace. Ensure to use V6 type for ICMPv6 packet-tracer.
icmp_code	Specifies the ICMP code corresponding to the type for an ICMP packet tracer. Ensure to use V6 code for ICMPv6 packet-tracer.

input *ifc_name*	Specifies the ingress interface of the packet.
inline-tag *tag*	Specifies the security group tag value being embedded in the Layer 2 CMD header. Valid values range 0–65533.
json	(Optional) Displays the trace results in JSON format.
pcap	Specifies pcap as input.
pcap_filename	The pcap filename that contain the packet for tracing.
protocol	Specifies the protocol number for raw IP packet tracing, 0-255.
persist	(Optional) Enables tracing for a long term and also tracing in cluster.
rawip	Specifies the protocol to use is raw IP.
sctp	Specifies the protocol to use is SCTP.
security-group {**name** *name* | **tag** *tag* }	Specifies the source and destination security groups based on the IP-SGT lookup for Trustsec. You can specify a security group name or a tag number.
src_port	Specifies the source port for a TCP/UDP/SCTP packet trace.
src_ip	Specifies the source IPv4 or IPv6 address for the packet trace.
tcp	Specifies the protocol to use is TCP.
transmit	(Optional) Allows simulated packet to transmit from device.
type	Specifies the ICMP type for an ICMP packet trace.
udp	Specifies the protocol to use is UDP.
user *username*	Specifies the user identity in the format of *domain\user* if you want to specify the user as the source IP address. The most recently mapped address for the user (if any) is used in the trace.
vlan-id *vlan_id*	(Optional) Specifies the VLAN identity for the flow. Values range from 1 - 4096.
xml	(Optional) Displays the trace results in XML format.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
8.4(2)	Two keyword-argument pairs were added: user *username* and fqdn *fqdn_ string* . Renamed and redefined several keywords. Added support for IPv6 source addresses.
9.0(1)	Support for user identity was added. Only IPv4 fully qualified domain names (FQDNs) are supported.
9.3(1)	The **inline-tag** *tag* keyword-argument pair was added to support the security group tag value being embedded in the Layer 2 CMD header.
9.4(1)	Two keyword-argument pairs were added: **vlan-id** *vlan_id* and **vxlan-inner** *vxlan_inner_tag* .
9.5(2)	The sctp keyword was added.
9.7(1)	Support for transparent firewall mode. A new trace module for destination MAC address was introduced.
9.9.(1)	Support for clustering persistent tracing was introduced. Using this feature, it is possible to trace packets on cluster units. New options were added: persist, bypass-checks, decrypted, transmit, id, and origin.
9.14(1)	Enhanced the packet-tracer output to provide specific reasons for packet allow/drop while routing the packets.
9.17(1)	Enhanced the packet-tracer command to allow a pcap file as input for tracing. Also added support for **geneve**.

Usage Guidelines

In addition to capturing packets with the capture command, it is possible to trace the lifespan of a packet through the ASA to see if it is behaving as expected. The packet-tracer command enables you to do the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines that caused the rule addition.
- Show a timeline of packet changes in a datapath.
- Inject tracer packets into the datapath.
- Search for an IPv4 or IPv6 address based on the user identity and the FQDN.
- Debug packets across cluster nodes.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the ASA. **packet-tracer** allows a firewall administrator to inject a virtual packet into the security appliance and track the flow from ingress to egress. Along the way, the packet is evaluated against flow and route lookups, ACLs, protocol inspection, and NAT. The power of the utility comes from the ability to simulate real-world traffic by specifying source and destination addresses with protocol and port information.

The optional **vlan-id** keyword allows packet tracer to enter a parent interface, which is later redirected to a subinterface that matches the VLAN identity. The VLAN identity is an optional entry only for

non-sub-interfaces. Management interface is an exception, where a parent management-only interface can only have the management-only sub-interfaces.

The destination MAC address lookup is available.

In transparent firewall mode, when the input interface is VTEP, Destination MAC address is optionally enabled if you enter a value in VLAN. Whereas in the bridge group member interface, Destination MAC address is a mandatory field but is optional if you enter the vlan-id keyword.

In routed firewall mode, when the input interface is bridge group member interface, the vlan-id keyword and dmac argument are optional.

The following tables provide full information pertaining to the interface-dependent behavior of VLAN identity and Destination MAC address in transparent and routed firewall modes respectively.

Transparent firewall mode:

Interface	VLAN	Destination MAC address
Management	Enabled (Optional)	Disabled
VTEP	Enabled (Optional)	Disabled. When the user enters a value in VLAN, the Destination MAC address is enabled but is optional.
Bridge Virtual Interface (BVI)	Enabled (Optional)	Enabled (Mandatory). When the user enters a value in VLAN, the Destination MAC address is optional.

Routed firewall mode:

Interface	VLAN	Destination MAC address
Management	Enabled (Optional)	Disabled
Routed interface	Enabled (Optional)	Disabled
Bridge Group Member	Enabled (Optional)	Enabled (Optional)

When you run the **packet-tracer** command using the input ingress interface and if the packet does not get dropped, the packet traverses through different phases like UN-NAT, ACLs, NAT, IP-OPTIONS, and FLOW-CREATION. The resultant message is displayed: “ALLOW”.

In a scenario where the firewall configurations could cause live traffic to be dropped, the simulated tracer packet will also be dropped. In some instances, a specific drop reason will be provided. For example, if a packet was dropped because of an invalid header validation, the following message appears: “packet dropped due to bad ip header (reason).” The packet gets dropped in a switching sequence if the Destination MAC address is unknown. It initiates the ASA to search for the Destination MAC address. packet-tracer can be executed again and the L2 lookup is successful if the Destination MAC address was found.

VXLAN and Geneve support in packet-tracer enables you to specify inner packet Layer 2 source and destination MAC addresses, Layer 3 source and destination IP addresses, Layer 4 protocol, Layer 4 source and destination port numbers, and the Virtual Network Interface (VNI) number. Only TCP, SCTP, UDP, raw IP, and ICMP are supported for the inner packet.

You can specify a user identity for the source using domain/user format. The ASA searches for the user's IP address and uses it in packet trace testing. If a user is mapped to multiple IP addresses, the most recent login IP address is used and the output shows that more IP address-user mapping exists. If user identity is specified

in the source part of this command, then the ASA searches for the user's IPv4 or IPv6 address based on the destination address type that the user entered.

You can specify security group name or security group tag as a source. The ASA searches for the IP address based on the security group name or security group tag and uses it in packet trace testing. If a security group tag or security group name is mapped to multiple IP addresses, then one of the IP addresses is used and the output shows that more IP address-to-security group tag mapping exists.

You can also specify a FQDN as both the source and destination address. The ASA performs DNS lookup first, then retrieves the first returned IP address for packet construction.

For traffic scenarios like L3 to Bridge Virtual Interface and Bridge Virtual Interface to Bridge Virtual Interface, where destination IP is the next hop through BVI interface on ASA, then, packet tracer does double ROUTE-LOOKUP. Also, the flow is not created.

With ARP and MAC address table entry cleared, the packet tracer always does double ROUTE-LOOKUP and destination MAC address is resolved and stored in database. Whereas this is not the case for any other traffic scenario. Destination MAC address is never resolved and stored in database, when it is a L3 interface. Since the BVI interface is configured with *nameif* and has L3 properties, the DMAC lookup should not be done.

This behavior is seen only in first attempt when there are no MAC address and ARP entries present. Once the entry is present for DMAC, the packet tracer output is as expected. The flow is created.

With persistent tracing, it is possible to trace a packet when it passes between cluster units. The packet you want to track across cluster units must be injected using the persist option. The persistent tracing for each packet is equipped with a packet-id and a hop count with which it is possible to determine the injected packet origin and packet hop phases through the cluster nodes. The packet-id is a combination of <node name of the device where the packet originated> and an incremental number. The packet-id is unique for each new packet received for the first time on a node. The hop count populates every time the packet moves from one cluster member to another. For example, packets in clustering arrive to a member based on external load-balancing numbered list. The Host-1 sends a packet to Host-2. The injected packet is redirected between the cluster nodes before it is sent to Host-2. The metadata output displays Tracer origin-id B:7 hop 0 , Tracer origin-id B:7 hop 1 , and Tracer origin-id B:7 hop 2 respectively. Where B is the name of the cluster node from which the packet originated. And 7 is an incremental number, representing this is the 7th packet originating from this cluster node. This number increases with each new packet originating from this node. “B” and “7” together forms a unique-id to identify a packet. A cluster unit local name is the same for every packet that is passing through this unit. Each packet is differentiated when the global buffer uses the unique-id and the hop count. Once the packets are traced, the persistent traces are available on each node until the time you manually discard them to free up some memory. The enabled persistent traces in a context are stored in a per-context buffer. Use the origin-owner-ID (two values <origin-owner> <id>), to locate the traces in the set.

It is possible to allow simulated packets to egress the ASA. Using the transmit option via packet-tracer, you can let the packets be transmitted on the network. By default, the packet-tracer discards the packet before transmitting it. A flow is generated in the flow table once the packets are egressed.

By using the bypass-checks option via packet-tracer, it is possible to bypass ACL, VPN filters, uRPF, and IPsec spoof checks. It applies for both ingress and egress conditions and the simulated IPsec packets are not dropped.

It is possible to inject a decrypted packet in a VPN tunnel, which is generic and applicable for both IPSec and TLS. It is also possible to simulate a packet that comes across a VPN tunnel. The simulated ‘decrypted’ packet would be matched against an existing VPN tunnel and the associated tunnel policies would be applied. However, this functionality is not applicable for a route-based VPN tunnel.

While the **packet-tracer** injects and traces a single packet, the **pcap** keyword enables the packet-tracer to replay multiple packets (maximum of 100 packets) and to trace an entire flow. You can provide the pcap file as input and obtain the results in XML or JSON format for further analysis. To clear the trace output, use the **pcap trace** sub command of **clear packet-tracer**. You cannot use the trace output while the trace is in progress.

The following example shows how to run packet-tracer with a pcap file as input:

```
ciscoasa# packet-tracer input inside pcap http_get.pcap detailed xml
```

The following example shows how to run packet-tracer by clearing existing pcap trace buffer and giving a pcap file as input:

```
ciscoasa# packet-tracer input inside pcap http_get.pcap force
```

Examples

The following example traces an ICMP packet from the inside interface. The result indicates that the packet is dropped due to the reverse-path verification failure (RPF). The reason for the failure could be that the traffic entered the outside interface from an address that is known to the routing table, but is associated with the inside interface. Similarly, if traffic enters the inside interface from an unknown source address, the device drops the packet because the matching route (the default route) indicates the outside interface.

```
ciscoasa#  packet-tracer input inside icmp 10.15.200.2 8 0$

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd793b4a0, priority=12, domain=capture, deny=false
        hits=621531641, user_data=0xd7bbe720, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd7dc31d8, priority=1, domain=permit, deny=false
        hits=23451445222, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   10.15.216.0     255.255.252.0   inside

Phase: 4
Type: ROUTE-LOOKUP
Subtype: input
```

```
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         outside


Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (rpf-violated) Reverse-path verify failed
```

The following example traces a TCP packet for the HTTP port from 201.1.1.1 to 202.1.1.1.

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Result:
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC Address Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC address lookup resulted in egress ifc outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe83542f0, priority=1, domain=permit, deny=false
hits=7313, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbd94026a0, priority=12, domain=permit, deny=false
hits=8, user_data=0x7fdbf07cbd00, cs_id=0x0, use_real_addr,
flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Forward Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=10, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe8363790, priority=0, domain=inspect-ip-options, deny=true
hits=212, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any
Phase: 6
Type: NAT
       Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Reverse Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=12, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x7fdbd93dfc10, priority=0, domain=inspect-ip-options, deny=true
hits=110, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 221, packet dispatched to next module
Module information for forward flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
```

```
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
44# command example
ciscoasa(config)# command example
resulting screen display here
<Text omitted.>
```

The following example traces a TCP packet for the HTTP port from 10.100.10.10 to 10.100.11.11. The result indicates that the packet will be dropped by the implicit deny access rule.

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10  80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

The following example shows how to trace a packet from inside host 10.0.0.2 to outside host 20.0.0.2 with the username of CISCO\abc:

```
ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2
Source: CISCO\abc 10.0.0.2
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

The following example shows how to trace a packet from inside host 20.0.0.2 with the username of CISCO\abc and display the trace results in XML format:

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>
<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>
```

The following example shows how to trace a packet from inside host xyz.example.com to external host abc.example.com.

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)
Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

The following example displays output from the **packet-tracer** command to show security group tag mapping to an IP address:

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

The following example displays output from the **packet-tracer** command to show Layer 2 SGT Imposition:

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

The following example outlines VXLAN support for UDP/TCP and ICMP inner packets

```
packet-tracer in inside udp 30.0.0.2 12345 30.0.0.100 vxlan vxlan-inner 1234 1.1.1.1 11111
 2.2.2.2 22222 aaaa.bbbb.cccc aaaa.bbbb.dddd detailedOuter packet: UDP from 30.0.0.2 to
```

```
30.0.0.100 (vtep/nve source-interface IP) with default vxlan destination port.
Inner packet: VXLAN in-tag 1234, UDP from 1.1.1.1/11111 to 2.2.2.2/22222 with smac
aaaa.bbbb.cccc and dmac aaaa.bbbb.dddd
```

The following example displays output for persistent tracing when it passes between cluster units:

```
ciscoasa# cluster exec show packet-tracer
B(LOCAL):**************************************************************
tracer 10/8 (allocate/freed), handle 10/8 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 0 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 5
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To A(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
=======  Tracer origin-id B:7, hop 2 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From A(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-4: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) have been elected owner by (0).
<Snipping phase 6-16: ACCESS-LIST, NAT, IP-OPTIONS, INSPECT, INSPECT, FLOW-CREATION,
ACCESS-LIST, NAT, IP-OPTIONS, ROUTE-LOOKUP, ADJACENCY-LOOKUP>
A:**************************************************************
tracer 6/5 (allocate/freed), handle 6/5 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 1 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From B(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-7: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP, ACCESS-LIST, NAT, IP-OPTIONS>
Phase: 8
Type: CLUSTER-EVENT
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (0) am director, not creating dir flow for ICMP pkt recvd by (1).
Phase: 9
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To B(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
ciscoasa#
```

The following example displays output when packets are traced using origin and id options from the cluster nodes:

```
cluster2-asa5585a# cluster exec show packet-tracer | i origin-id
b(LOCAL):**************************************************************
=======  Tracer origin-id b:2, hop 0 =======
=======  Tracer origin-id b:2, hop 2 =======
a:**************************************************************
=======  Tracer origin-id a:17, hop 0 =======
=======  Tracer origin-id b:2, hop 1 =======
=======  Tracer origin-id b:2, hop 3 =======
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer ori
cluster2-asa5585a# cluster exec show packet-tracer origin b id 2
b(LOCAL):**************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 4
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
```

```
Additional Information:
To a(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 2 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From a(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
```

```
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: FULL
I (1) am redirecting to (0) due to matching action (1).
Phase: 15
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
a:**********************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 1 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
```

```
Additional Information:
From b(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am director, found static rule to classify owner as (253).
Phase: 7
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To b(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 3 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
```

```
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
```

```
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 70, packet dispatched to next module
Phase: 19
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
Phase: 20
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1730 reference 6
Phase: 21
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
```

```
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside2
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer origin a
b(LOCAL):**************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:**************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
```

```
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
```

```
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer id 17
b(LOCAL):************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 0.0.0.0 using egress ifc  identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
```

The following example outlines clearing persistent traces from the cluster nodes:

```
ciscoasa# cluster exec clear packet-tracer
```

For injecting decrypted packets in an IPSec tunnel, there are some conditions. When the IPSec tunnel is not negotiated, an error message is displayed. Secondly, when the IPSec tunnel is negotiated, the packet goes through.

The following example outlines when IPSec tunnel is **not** negotiated for injecting decrypted packets:

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
decrypted
  ********************************************************************
  WARNING: An existing decryption SA was not found. Please confirm the
  IPsec Phase 2 SA or Anyconnect Tunnel is established.
  ********************************************************************
  Phase: 1
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
```

```
I (0) got initial, attempting ownership.
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect ftp
service-policy global_policy global
Additional Information:
Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: DROP
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
cluster2-asa5585a(config)#
```

The following example outlines when IPSec tunnel is negotiated for injecting decrypted packets:

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 decrypted
  Phase: 1
  Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
```

```
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
```

```
  Type: VPN
  Subtype: encrypt
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 20
  Type: VPN
  Subtype: encrypt
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 21
  Type: FLOW-CREATION
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  New flow created with id 1099, packet dispatched to next module
  Phase: 22
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 23
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  Phase: 24
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  Phase: 25
  Type: FLOW-CREATION
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  New flow created with id 1100, packet dispatched to next module
  Phase: 26
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
  Result:
  input-interface: outside
```

```
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
```

The following example uses the transmit option to allow simulated packets to egress and capture the same on the outgoing interface:

```
cluster2-asa5585a(config)# packet-tracer input outside icmp 211.1.1.10 8 0 213.1.1.10
transmit
  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
  Phase: 5
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:
  Phase: 6
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 7
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
```

```
Additional Information:
Phase: 8
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6449, packet dispatched to next module
Phase: 15
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 16
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
  Phase: 18
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 19
  Type: ADJACENCY-LOOKUP
  Subtype: Resolve Nexthop IP address to MAC
  Result: ALLOW
  Config:
  Additional Information:
  found adjacency entry for next-hop 214.1.1.9 on interface  outside
  adjacency Active
  mac address 4403.a74a.9a32 hits 15 reference 1
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
  cluster2-asa5585a(config)#
```

The following example outlines the ICMP packet being captured on the outgoing interface:

```
cluster2-asa5585a(config)# cluster exec show capture test | i icmp
  a(LOCAL):*******************************************************
    14: 02:18:16.717736      802.1Q vlan#212 P0 211.1.1.10 > 213.1.1.10: icmp: echo request

  cluster2-asa5585a(config)#
```

The examples for the bypass-checks option for packet-tracer is outlined through the following phases as listed. Specific examples are provided for each scenario:

- When the IPSec tunnel between spoke and hub is not created.
- The IPSec tunnel between two boxes must be negotiated and the initial packet triggers tunnel establishment.
- The IPSec negotiation is complete and the tunnel comes up.
- Once the tunnel is up, the packets injected will be sent through the tunnel. The security checks (ACLs, VPN filtering..) that is available along with the packet path will be bypassed or skipped.

The IPSec tunnel is not created:

```
cluster2-asa5585a(config)# sh crypto ipsec sa
  There are no ipsec sas
  cluster2-asa5585a(config)#
```

The tunnel negotiation process commences:

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks
  Phase: 1
```

```
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
```

```
  Config:
  class-map inspection_default
   match default-inspection-traffic
  policy-map global_policy
   class inspection_default
    inspect ftp
  service-policy global_policy global
  Additional Information:
  Phase: 10
  Type: VPN
  Subtype: ipsec-tunnel-flow
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 11
  Type: INSPECT
  Subtype: inspect-ftp
  Result: ALLOW
  Config:
  class-map inspection_default
   match default-inspection-traffic
  policy-map global_policy
   class inspection_default
    inspect ftp
  service-policy global_policy global
  Additional Information:
  Phase: 12
  Type: VPN
  Subtype: ipsec-tunnel-flow
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 13
  Type: VPN
  Subtype: encrypt
  Result: DROP
  Config:
  Additional Information:
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule
  cluster2-asa5585a(config)#
```

Once the IPSec tunnel is negotiated and the tunnel comes up:

```
cluster2-asa5585a#
  cluster2-asa5585a(config)# sh crypto ipsec sa
  interface: outside2
      Crypto map tag: crypto-map-peer4, seq num: 1, local addr: 214.1.1.10
        access-list toPeer4 extended permit ip host 211.1.1.1 host 213.1.1.2
        local ident (addr/mask/prot/port): (211.1.1.1/255.255.255.255/0/0)
        remote ident (addr/mask/prot/port): (213.1.1.2/255.255.255.255/0/0)
        current_peer: 214.1.1.9
        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
```

```
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
        #TFC rcvd: 0, #TFC sent: 0
        #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
        #send errors: 0, #recv errors: 0
        local crypto endpt.: 214.1.1.10/500, remote crypto endpt.: 214.1.1.9/500
        path mtu 1500, ipsec overhead 74(44), media mtu 1500
        PMTU time remaining (sec): 0, DF policy: copy-df
        ICMP error validation: disabled, TFC packets: disabled
        current outbound spi: A642726D
        current inbound spi : CF1E8F90

      inbound esp sas:
        spi: 0xCF1E8F90 (3474886544)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4285440/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
      outbound esp sas:
        spi: 0xA642726D (2789372525)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4239360/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
  cluster2-asa5585a(config)#
```

The packet is allowed to pass through once the tunnel is up and since the bypass-checks option is applied, the security checks are skipped:

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 bypass-checks

  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 2
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
```

```
Flow type: NO FLOW
I (0) am becoming owner
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module
Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
```

The following example traces a TCP packet in a directly connected hosts having the ARP entry for nexthop.

```
ciscoasa# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80 detailed

Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
```

```
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

The following example traces a TCP packet that is dropped due to absence of a valid ARP entry for nexthop. Note that the drop reason provides the tip to check the ARP table.

```
<Displays same phases as in the previous example till Phase 8>
Result:
input-interface: inside(vrfid:0)
input-status: up
```

```
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has entry
 for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

The following example depicts packet tracer for sub-optimal routing with NAT and a reachable nexthop.

```
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
ciscoasa# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
```

```
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
The following example depicts packet tracer for sub-optimal routing with NAT, where, the
packet is dropped due to non-reachable nexthop.
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>
Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.
show packet-tracer	Displays the trace buffer output of the most recently run packet-tracer on a PCAP file.

pager

To set the default number of lines on a page before the " ---More--- " prompt appears for Telnet sessions, use the **pager** command in global configuration mode.

pager [**lines**] *lines*

Syntax Description

[**lines**] *lines*	Sets the number of lines on a page before the " ---More--- " prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Command Default

The default is 24 lines.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from a privileged EXEC mode command to a global configuration mode command. The **terminal pager** command was added as the privileged EXEC mode command.

Usage Guidelines

This command changes the default pager line setting for Telnet sessions. If you want to temporarily change the setting only for the current session, use the **terminal pager** command.

If you Telnet to the admin context, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

Examples

The following example changes the number of lines displayed to 20:

```
ciscoasa(config)# pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.

Command	Description
terminal	Allows system log messages to display on the Telnet session.
terminal pager	Sets the number of lines to display in a Telnet session before the “ ---more--- ” prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

page style

To customize the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **page style** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

page style *value*
[**no**] **page style** *value*

Syntax Description

value	Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default page style is background-color:white;font-family:Arial,Helv,sans-serif

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the page style to large:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
title	Customizes the title of the WebVPN page

parameters

To enter parameters configuration mode to set parameters for an inspection policy map, use the **parameters** command in policy-map configuration mode.

parameters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

An inspection policy map may support one or more **parameters** commands. Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

Examples

The following example shows how to set the maximum message length for DNS packets in the default inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.

Command	Description
show running-config policy-map	Display all current policy map configurations.

participate

To force the device to participate in the virtual load-balancing cluster, use the **participate** command in VPN load-balancing configuration mode. To remove a device from participation in the cluster, use the **no** form of this command.

participate
no participate

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior is that the device does not participate in the vpn load-balancing cluster.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
VPN load-balancing configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first configure the interface using the **interface** and **nameif** commands, and use the **vpn load-balancing** command to enter VPN load-balancing mode. You must also have previously configured the cluster IP address using the **cluster ip** command and configured the interface to which the virtual cluster IP address refers.

This command forces this device to participate in the virtual load-balancing cluster. You must explicitly issue this command to enable participation for a device.

All devices that participate in a cluster must share the same cluster-specific values: ip address, encryption settings, encryption key, and port.

Note When using encryption, you must have previously configured the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If isakmp is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.If isakmp was enabled when you configured the **cluster encryption** command, but was disabled before you configured the **participate** command, you get an error message when you enter the **participate** command, and the local device will not participate in the cluster.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **participate** command that enables the current device to participate in the vpn load-balancing cluster:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

passive-interface (ipv6 router ospf)

To suppress the sending and receiving of routing updates on an interface or across all interfaces that are using an OSPFv3 process, use the **passive-interface** command in ipv6 router ospf configuration mode. To reenable routing updates on an interface or across all intterfaces that are using an OSPFv3 process, use the **no** form of this command.

passive-interface [*interface_name*]
no passive-interface [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the interface name on which the OSPFv3 process is running.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command enables passive routing on an interface.

Examples

The following example suppresses the sending and receiving of routing updates on the inside interface.

```
ciscoasa(config)# ipv6
router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
show running-config router	Displays the router configuration commands in the running configuration.

passive-interface (isis)

To select ISIS hello packets and routing updates on interfaces while still including the interface addresses in the topology database, use the **passive-interface** command in router isis configuration mode. To reenable outgoing hello packets and routing updates, use the **no** form of this command.

passive-interface [**default** | **inside** | **management** | **management2**]
no passive-interface [**default** | **inside** | **management** | **management2**]

Syntax Description

default	Suppresses routing updates on all interfaces.
inside	The name of interface GigabithEthernet0/0.
management	The name of interface Management0/0.
management2	The name of interface Management0/1.

Command Default

The default is to suppress routing updates on all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command enables passive routing on an interface.

Examples

The following example suppresses the sending and receiving of routing updates on the inside interface.

```
ciscoasa(config)# router isis
ciscoasa(config-router)# passive-interface inside
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

passive-interface (router eigrp)

To disable the sending and receiving of EIGRP routing updates on an interface, use the **passive-interface** command in router eigrp configuration mode. To reenable routing updates on an interface, use the **no** form of this command.

passive-interface { **default***if_name* }
no passive-interface { **default***if_name* }

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) The name of the interface, as specified by the **nameif** command, to passive mode.

Command Default

All interfaces are enabled for active routing (sending and receiving routing updates) when routing is enabled for that interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router eigrp configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	Support for EIGRP routing was added.

Usage Guidelines

Enables passive routing on the interface. For EIGRP, this disables the transmission and reception of routing updates on that interface.

You can have more than one **passive-interface** command in the EIGRP configuration. You can use the **passive-interface default** command to disable EIGRP routing on all interfaces, and then use the **no passive-interface** command to enable EIGRP routing on specific interfaces.

Examples

The following example sets the outside interface to passive EIGRP. The other interfaces on the security appliance send and receive EIGRP updates.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

The following example sets all interfaces except the inside interface to passive EIGRP. Only the inside interface will send and receive EIGRP updates.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface default
ciscoasa(config-router)# no passive-interface inside
```

Related Commands

Command	Description
show running-config router	Displays the router configuration commands in the running configuration.

passive-interface (router rip)

To disable the transmission of RIP routing updates on an interface, use the **passive-interface** command in router rip configuration mode. To reenable RIP routing updates on an interface, use the **no** form of this command.

passive-interface { **default** | *if_name* }
no passive-interface { **default** | *if_name* }

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) Sets the specified interface to passive mode.

Command Default

All interfaces are enabled for active RIP when RIP is enabled.

If an interface or the **default** keyword is not specified, the commands defaults to **default** and appears in the configuration as passive-interface default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router rip configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables, but does not broadcast routing updates.

Examples

The following example sets the outside interface to passive RIP. The other interfaces on the security appliance send and receive RIP updates.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.

Command	Description
router rip	Enables the RIP routing process and enters rip router configuration mode.
show running-config rip	Displays the RIP commands in the running configuration.

passwd

To set the login password for Telnet, use the **passwd** command in global configuration mode. To reset the password, use the **no** form of this command.

passwd *password* [**encrypted**]
no passwd *password*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another ASA but do not know the original password, you can enter the **passwd** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.
password	Sets the password as a case-sensitive string of up to 80 characters. The password must not contains spaces.

Command Default

9.1(1): The default password is "cisco."

9.1(2): No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	The aliased **password** command was removed; only **passwd** is supported.
8.4(2)	The SSH default username is no longer supported; you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password.
9.0(2), 9.1(2)	The default password, "cisco," has been removed; you must actively set a login password. Using the **no passwd** or **clear configure passwd** command removes the password; formerly, it reset it to the default of "cisco."

Usage Guidelines

When you enable Telnet with the **telnet** command, you can log in with the password set by the **passwd** comamnd. After you enter the login password, you are in user EXEC mode. If you configure CLI authentication per user for Telnet using the **aaa authentication telnet console** command, then this password is not used.

This password is also used for Telnet sessions from the switch to the ASASM (see the **session** command).

Examples

The following example sets the password to Pa$$w0rd:

```
ciscoasa(config)# passwd
Pa$$w0rd
```

The following example sets the password to an encrypted password that you copied from another ASA:

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

password (crypto ca trustpoint)

To specify a challenge phrase that is registered with the CA during enrollment, use the **password** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

password *string*
no password *string*

Syntax Description

string Specifies the name of the password as a character string. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, "hello 21" is a legal password, but "21 hello" is not. The password checking is case sensitive. For example, the password "Secret" is different from the password "secret".

Command Default

The default setting is to not include a password.

Command Modes

The following table shows the modes in which you can enter thecommand:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command lets you specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the ASA.

The CA typically uses a challenge phrase to authenticate a subsequent revocation request.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes a challenge phrase registered with the CA in the enrollment request for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

password encryption aes

To enable password encryption using a master passphrase, use the **password encryption aes** command in global configuration mode. To disable password encryption, use the **no** form of this command.

password encryption aes
no password encryption aes

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

You must enter both the **key config-key password-encrypt** command and the **password encryption aes** command in any order to trigger password encryption. Enter **write memory** to save the encrypted passwords to the startup configuration. Otherwise, passwords in the startup configuration may still be visible. In multiple context mode, use **write memory all** in the system execution space to save all context configurations. If you later disable password encryption using the **no password encryption aes** command, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted, as required by the application.

This command will only be accepted in a secure session, for example by console, SSH, or ASDM via HTTPS.

Enabling or changing password encryption in Active/Standby failover causes a **write standby**, which replicates the active configuration to the standby unit. Without this replication, the encrypted passwords on the standby unit will differ even though they use the same passphrase; configuration replication ensures that the configurations are the same. For Active/Active failover, you must manually enter **write standby**. A **write standby** can cause traffic interruption in Active/Active mode, because the configuration is cleared on the secondary unit before the new configuration is synced. You should make all contexts active on the primary ASA using the **failover active group 1** and **failover active group 2** commands, enter **write standby**, and then restore the group 2 contexts to the secondary unit using the **no failover active group 2** command.

The write erase command when followed by the reload command will remove the master passphrase and all configuration if it is lost.

Examples

The following example sets the passphrase used for generating the encryption key, and enables password encryption:

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

Command	Description
key config-key password-encryption	Sets the passphrase used for generating the encryption key.
write erase	Removes the master passphrase if it is lost when followed by the reload command.

password-history

This command appears in the configuration for the **username attributes** command when you enable the **password-policy reuse-interval** command and is not user-configurable. It stores previous passwords in an encrypted form.

password-history *hash1,hash2,hash3...*

Syntax Description

hash1,hash2,hash3, ...	Shows previous passwords that have been hashed using PBKDF2 (Password-Based Key Derivation Function 2).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username attributes configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

This command is not user-configurable, and only shows in show output when you enable the **password-policy reuse-interval** command.

Examples

The following example changes a password two times, and then shows the previous hashed passwords:

```
ciscoasa(config)# username test password pw1
ciscoasa(config)# show running-config username test
username test password $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ== pbkdf2
ciscoasa(config)# username test password pw2
ciscoasa(config)# show running-config username test
username test password $sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw== pbkdf2
username test attributes
  password-history $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)# username test password pw3
ciscoasa(config)# show running-config username test
username test password $sha512$5000$o8WLa1qnLdp2Js4OlW+NdQ==$4Be4eHtPmOxdpfH6j+F4qQ== pbkdf2
username test attributes
  password-history
$sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==,$sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)#
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

password-management

To enable password management, use the **password-management** command in tunnel-group general-attributes configuration mode. To disable password management, use the **no** form of this command. To reset the number of days to the default value, use the **no** form of the command with the **password-expire-in-days** keyword specified.

password-management [**password-expire-in-days** *days*]
nopassword-management
no password-management password-expire-in-days [*days*]

Syntax Description

days	Specifies the number of days (0 through 180) before the current password expires. This parameter is required if you specify the **password-expire-in-days** keyword.
password-expire-in-days	(Optional) Indicates that the immediately following parameter specifies the number of days before the current password expires that the ASA starts warning the user about the pending expiration. This option is valid only for LDAP servers. See the Usage Notes section for more information.

Command Default

The default is no password management. If you do not specify the **password-expire-in-days** keyword for an LDAP server, the default length of time to start warning before the current password expires is 14 days.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The ASA supports password management for the RADIUS and LDAP protocols. It supports the "password-expire-in-days" option for LDAP only.

You can configure password management for IPsec remote access and SSL VPN tunnel-groups.

When you configure the password-management command, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This command is valid for AAA servers that support such notification; that is, natively to LDAP servers and RADIUS proxied to an NT 4.0 or Active Directory server. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

Note Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This command requires MSCHAPv2 so please check with your vendor.

The ASA, releases 7.1 and later, generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN Client (ASA software version 8.0 and higher)
- IPsec VPN Client
- Clientless SSL VPN (ASA software version 8.0 and higher) WebVPN (ASA software versions 7.1 through 7.2.x)
- SSL VPN Client full tunneling client

These RADIUS configurations include RADIUS with LOCAL authentication, RADIUS with Active Directory/Kerberos Windows DC, RADIUS with NT/4.0 Domain, and RADIUS with LDAP.

Password management is *not* supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the ASA perspective, it is talking only to a RADIUS server.

Note For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.

Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Note that this command does not change the number of days before the password expires, but rather, the number of days ahead of expiration that the ASA starts warning the user that the password is about to expire.

If you do specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The ASA does not notify the user of the pending expiration, but the user can change the password after it expires.

Note Radius does not provide a password change, or provide a password change prompt.

Examples

The following example sets the days before password expiration to begin warning the user of the pending expiration to 90 for the WebVPN tunnel group “testgroup”:

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

The following example uses the default value of 14 days before password expiration to begin warning the user of the pending expiration for the IPsec remote access tunnel group “QAgroup”:

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
passwd	Sets the login password.
radius-with-expiry	Enables negotiation of password update during RADIUS authentication (Deprecated).
show running-config passwd	Shows the login password in encrypted form.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

password-parameter

To specify the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication, use the **password-parameter** command in aaa-server-host configuration mode. This is an SSO with the HTTP Forms command.

password-parameter *string*

Note To configure SSO with HTTP correctly, you must have a thorough working knowledge of authentication and HTTP exchanges.

Syntax Description

string The name of the password parameter included in the HTTP POST request. The maximum password length is 128 characters.

Command Default

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The required command **password-parameter** specifies that the POST request must include a user password parameter for SSO authentication.

Note At login, the user enters the actual password value, which is entered into the POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies a password parameter named user_password:

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

password-policy authenticate enable

To determine whether users are allowed to modify their own user account, use the **password-policy authenticate enable** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy authenticate enable
no password-policy authenticate enable

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

If authentication is enabled, the **username** command does not allow users to change their own password or delete their own account. In addition, the **clear configure username** command does not allow users to delete their own account.

Examples

The following example shows how to enable users to modify their user account:

```
ciscoasa(config)# password-policy authenticate enable
```

Related Commands

Command	Description
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy lifetime

To set password policy for the current context and the interval in days after which passwords expire, use the **password-policy lifetime** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy lifetime *value*
no password-policy lifetime *value*

Syntax Description

value Specifies the password lifetime. Valid values range from 0 to 65535 days.

Command Default

The default lifetime value is 0 days.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

Passwords have a specified maximum lifetime. A lifetime interval of 0 days specifies that local user passwords never expire. Note that passwords expire at 12:00 a.m. of the day following lifetime expiration.

Examples

The following example specifies a password lifetime value of 10 days:

```
ciscoasa(config)# password-policy lifetime 10
```

Related Commands

Command	Description
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy minimum-changes

To set the minimum number of characters that must be changed between new and old passwords, use the **password-policy minimum-changes** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-changes *value*
no password-policy minimum-changes *value*

Syntax Description

value	Specifies the number of characters that must be changed between new and old passwords. Valid values range from 0 to 64 characters.

Command Default

The default number of changed characters is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

New passwords must include a minimum of 4 character changes from the current password and are considered changed only if they do not appear anywhere in the current password.

Examples

The following example specifies a minimum number of character changes between old and new passwords of 6 characters:

```
ciscoasa(config)# password-policy minimum-changes 6
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime in days after which passwords expire.
password-policy minimum-length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lowercase characters that passwords may have.

password-policy minimum-length

To set the minimum length of passwords, use the **password-policy minimum-length** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-length*value*
no password-policy minimum-length *value*

Syntax Description

value Specifies the minimum length for passwords. Valid values range from 3 to 32 characters.

Command Default

The default minimum length is 3.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

If the minimum length is less than any of the other minimum attributes (changes, lower case, upper case, numeric, and special), an error message appears and the minimum length is not changed. The recommended password length is 8 characters.

Examples

The following example specifies a minimum number of characters for passwords as 8:

```
ciscoasa(config)# password-policy minimum-length 8
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of changed characters allowed between old and new passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy minimum-lowercase

To set the minimum number of lower case characters that passwords may have, use the **password-policy minimum-lowercase** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-lowercase*value*
no password-policy minimum-lowercase*value*

Syntax Description

value	Specifies the minimum number of lower case characters for passwords. Valid values range from 0 to 64 characters.

Command Default

The default number of minimum lower case characters is 0, which means there is no minimum.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command sets the minimum number of lower case characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of lower case characters that passwords may have as 6:

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-numeric

To set the minimum number of numeric characters that passwords may have, use the **password-policy minimum-numeric** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-numeric *value*
no password-policy minimum-numeric *value*

Syntax Description

value Specifies the minimum number of numeric characters for passwords. Valid values range from 0 to 64 characters.

Command Default

The default number of minimum numeric characters is 0, which means there is no minimum.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command sets the minimum number of numeric characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of numeric characters that passwords may have as 8:

```
ciscoasa(config)# password-policy minimum-numeric 8
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-special

To set the minimum number of special characters that passwords may have, use the **password-policy minimum-special** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-special *value*
no password-policy minimum-special *value*

Syntax Description

value	Specifies the minimum number of special characters for passwords. Valid values range from 0 to 64 characters.

Command Default

The default number of minimum special characters is 0, which means there is no minimum.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command sets the minimum number of special characters that passwords may have. Special characters include the following: !, @, #, $, %, ^, &, *, '(‘ and ‘)’.

Examples

The following example specifies the minimum number of special characters that passwords may have as 2:

```
ciscoasa(config)# password-policy minimum-special 2
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-uppercase

To set the minimum number of upper case characters that passwords may have, use the **password-policy minimum-uppercase** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-uppercase *value*
no password-policy minimum-uppercase *value*

Syntax Description

value Specifies the minimum number of upper case characters for passwords. Valid values range from 0 to 64 characters.

Command Default

The default number of minimum upper case characters is 0, which means there is no minimum.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

This command sets the minimum number of upper case characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of upper case characters that passwords may have as 4:

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy reuse-interval

To prohibit the reuse of a password for a local username, use the **password-policy reuse-interval** command in global configuration mode. To remove this restriction, use the **no** form of this command.

password-policy reuse-interval *value*
no password-policy reuse-interval [*value*]

Syntax Description

value Sets the number of previous passwords that you cannot use when creating a new password, between 2 and 7.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

You can prohibit the reuse of a password that matches previously used passwords. The previous passwords are stored in the configuration under each **username** in encrypted form using the **password-history** command; this command is not user-configurable.

Examples

The following example sets the password resuse interval to 5:

```
ciscoasa(config)# password-policy reuse-interval 5
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.

Command	Description
username	Configures a local user.

password-policy username-check

To prohibit a password that matches a username, use the **password-policy username-check** command in global configuration mode. To remove this restriction, use the **no** form of this command.

password-policy username-check
no password-policy username-check

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

You can prohibit a password that matches the name in a **username** command.

Examples

The following example restricts the password from matching the username john_crichton:

```
ciscoasa(config)# password-policy username-check
ciscoasa(config)# username john_crichton password moya privilege 15
ciscoasa(config)# username aeryn_sun password john_crichton privilege 15
ERROR: Password must contain:
ERROR:  a value that complies with the password policy
ERROR: Username addition failed.
ciscoasa(config)#
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.

Command	Description
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

password-storage

To let users store their login passwords on the client system, use the **password-storage enable** command in group-policy configuration mode or username configuration mode. To disable password storage, use the **password-storage disable** command.

To remove the password-storage attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for password-storage from another group policy.

password-storage { **enable** | **disable** }
no password-storage

Syntax Description

disable	Disables password storage.
enable	Enables password storage.

Command Default

Password storage is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Enable password storage only on systems that you know to be in secure sites.

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

Examples

The following example shows how to enable password storage for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

peer-group

To identify the ASA virtual cluster nodes for the VXLAN cluster control link, use the **peer-group** command in nve configuration mode. To remove the peer group, use the **no** form of this command.

peer-group *network_object_name*
no peer-group *network_object_name*

Syntax Description

network_object_name Identifies the network object defined by the **object-group network** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

Identify the VTEP peer IP addresses by creating a network object group using the **object-group network** command.

The underlying IP network between VTEPs is independent of the cluster control link network that the VNI interfaces use. The VTEP network may include other devices, and VTEP peers may not even be on the same subnet.

The VTEP source interface IP address should be included as one of the peers in the network object group.

Examples

The following example creates a network object group with hosts defined inline:

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

The following example creates a network object group that refers to a standalone network object:

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54
```

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

The following example defines interface gigabitethernet 0/7 as the cluster control link VTEP source interface and identifies the cluster-peers network object group as the peer-group:

```
interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

interface vni 1
    segment-id 1000
    vtep-nve 1
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only cluster	Specifies that the NVE is for the cluster control link.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

peer-id-validate

To specify whether to validate the identity of the peer using the peer's certificate, use the **peer-id-validate** command in tunnel-group ipsec-attributes mode. To return to the default value, use the **no** form of this command.

peer-id-validate *option*
no peer-id-validate

Syntax Description

option Specifies one of the following options:

- **req**: required
- **cert**: if supported by certificate
- **nocheck**: do not check

Command Default

The default setting for this command is **req**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec attributes	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can apply this attribute to all IPsec tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, requires validating the peer using the identity of the peer's certificate for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

peer ip

To manually specify the peer VXLAN tunnel endpoint (VTEP) IP address, use the **peer ip** command in nve configuration mode. To remove the peer address, use the **no** form of this command.

peer ip *ip_address*
no peer ip

Syntax Description

ip_address	Sets the peer VTEP IP address, IPv4 or IPv6.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.20(1)	This command now supports IPv6.

Usage Guidelines

If you specify the peer IP address, you cannot use multicast group discovery. Multicast is not supported in multiple context mode, so manual configuration is the only option. You can only specify one peer for the VTEP.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and specifies a peer IP address of 10.1.1.2:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.

Command	Description
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

perfmon

To display performance information, use the **perfmon** command in privileged EXEC mode.

perfmon { **verbose** | **interval** *seconds* | **quiet** | **settings** } [*detail*]

Syntax Description

verbose	Displays performance monitor information at the ASA console.
interval *seconds*	Specifies the number of seconds before the performance display is refreshed on the console.
quiet	Disables the performance monitor displays.
settings	Displays the interval and whether it is quiet or verbose.
detail	Displays detailed information about performance.

Command Default

The *seconds* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0	Support for this command was added on the ASA.
7.2(1)	Support for the **detail** keyword was added.

Usage Guidelines

The perfmon command allows you to monitor the performance of the ASA. Use the show perfmon command to display the information immediately. Use the perfmon verbose command to display the information every 2 minutes continuously. Use the perfmon interval seconds command with the perfmon verbose command to display the information continuously every number of seconds that you specify.

An example of the performance information is displayed as follows:

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s

WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

This information lists the number of translations, connections, Websense requests, address translations (called "fixups"), and AAA transactions that occur each second.

Examples

This example shows how to display the performance monitor statistics every 30 seconds on the ASA console:

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

Command	Description
show perfmon	Displays performance information.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To disable, use the **no** form of this command.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*
no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

Syntax Description

days-of-the-week	(Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Command Default

If a value is not entered with the **periodic** command, access to the ASA as defined with the **time-range** command is in effect immediately and always on.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Time-range configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the ASA; however, the feature works best with NTP synchronization.

Examples

Some examples follow:

If you want:	Enter this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekdays 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight	**periodic weekend 12:00 to 23:59**

The following example shows how to allow access to the ASA on Monday through Friday, 8:00 a.m. to 6:00 p.m. only:

```
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range)#
```

The following example shows how to allow access to the ASA on specific days (Monday, Tuesday, and Friday), 10:30 a.m. to 12:30 p.m.:

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the ASA.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
time-range	Defines access control to the ASA based on time.

periodic-authentication certificate

To enable periodic certificate verification, use the **periodic-authentication certificate** command. To inherit the settings from the default group policy, use the **no** form of this command.

periodic-authentication certificate <*time in hours*> **none**
no periodic-authentication certificate <*time in hours*> **none**

Syntax Description

time in hours	Sets the interval between 1 and 168 hours.
none	Disables periodic authentication.

Command Default

The periodic certificate verification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Default group-policy configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The command by default will be **periodic-authentication certificate none** for the default group-policy. Other groups policies inherit the setting from the default policy unless changed.

Examples

```
100(config-group-policy)# periodic-authentication ?
group-policy mode commands/options:
  certificate  Configure periodic certificate authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
100(config-group-policy)# help periodic-authentication
```

permit-errors

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, use the **permit-errors** command in policy map parameters configuration mode. To return to the default behavior, where all invalid packets or packets that failed parsing are dropped. use the **no** form of this command.

permit-errors
no permit-errors

Syntax Description

This command has no arguments or keywords.

Command Default

By default, all invalid packets or packets that failed parsing are dropped.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **permit-errors** command in a GTP inspection policy map parameters to allow any packets that are invalid or encountered an error during inspection of the message to be sent through the ASA instead of being dropped.

Examples

The following example permits traffic containing invalid packets or packets that failed parsing:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-errors
```

Related Commands

Commands	Description
policy-map type inspect gtp	Defines a GTP inspection policy map.
inspect gtp	Applies a specific GTP map to use for application inspection.

permit-response

To configure GSN or PGW pooling, use the permit-response command in policy map parameters configuration mode. Use the **no** form of this command remove the pooling relationship.

permit-response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*
no permit-response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

Syntax Description

from-object-group *from_obj_group_id*	The network object group that identifies the GSN/PGW endpoints. This must be an object group (**object-group** command). These endpoints are allowed to send requests to and receive responses from the **to-object-group**. Starting with release 9.5(1), the object group can contain IPv6 addresses, not just IPv4.
to-object-group *to_obj_group_id*	The network object group that identifies the SGSN/SGW. This must be an object group (**object-group** command). These addresses are allowed to receive responses from the set of endpoints identified in the **from-object-group**. Starting with release 9.5(1), the object group can contain IPv6 addresses, not just IPv4.

Command Default

The ASA drops GTP responses from GSNs or PGWs that were not specified in the GTP request.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(4)	This command was added. GTP inspection supports IPv4 addresses only.
9.5(1)	Support for IPv6 addresses was added.

Usage Guidelines

When the ASA performs GTP inspection, by default the ASA drops GTP responses from GSNs or PGWs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs or PGWs to provide efficiency and scalability of GPRS.

To configure GSN/PGW pooling and thus support load balancing, create a network object group that specifies the GSN/PGW endpoints and specify this on the from-object-group parameter. Likewise, create a network object group for the SGSN/SGW and select it on the to-object-group parameter. If the GSN/PGW responding belongs to the same object group as the GSN/PGW that the GTP request was sent to and if the SGSN/SGW

is in an object group that the responding GSN/PGW is permitted to send a GTP response to, the ASA permits the response.

The network object group can identify the endpoints by host address or by the subnet that contains them.

Examples

The following example permits GTP responses from any host on the 192.168.32.0 network to the host with the IP address 192.168.112.57:

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1

ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit

ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# permit-response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

Commands	Description
policy-map type inspect gtp	Defines a GTP inspection policy map.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

pfs

To enable PFS, use the **pfs enable** command in group-policy configuration mode. To disable PFS, use the **pfs disable** command. To remove the PFS attribute from the running configuration, use the **no** form of this command.

pfs { **enable** | **disable** }
no pfs

Syntax Description

disable	Disables PFS.
enable	Enables PFS.

Command Default

PFS is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The PFS setting on the VPN Client and the ASA must match.

Use the **no** form of this command to allow the inheritance of a value for PFS from another group policy.

In IPsec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.

Examples

The following example shows how to set PFS for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# pfs enable
```

phone-proxy (Deprecated)

To configure the Phone Proxy instance, use the **phone-proxy** command in global configuration mode.

To remove the Phone Proxy instance, use the **no** form of this command.

phone-proxy*phone_proxy_name*
no phone-proxy *phone_proxy_name*

Syntax Description

phone_proxy_name	Specifies the name of the Phone Proxy instance.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated.

Usage Guidelines

Only one Phone Proxy instance can be configured on the ASA.

If NAT is configured for the HTTP proxy server, the global or mapped IP address of the HTTP proxy server with respect to the IP phones is written to the Phone Proxy configuration file.

Examples

The following example shows the use of the **phone-proxy** command to configure the Phone Proxy instance:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa
(config-phone-proxy)#
media-termination address
192.0.2.25
 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
```

```
ctl-file asactl
ciscoasa
(config-phone-proxy)#
cluster-mode nonsecure
ciscoasa
(config-phone-proxy)#
timeout secure-phones 00:05:00
ciscoasa
(config-phone-proxy)#
disable service-settings
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
tls-proxy	Configures the TLS proxy instance.

pim

To re-enable PIM on an interface, use the **pim** command in interface configuration mode. To disable PIM, use the **no** form of this command.

pim
no pim

Syntax Description

This command has no arguments or keywords.

Command Default

The **multicast-routing** command enables PIM on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **multicast-routing** command enables PIM on all interfaces by default. Only the **no** form of the **pim** command is saved in the configuration.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

Examples

The following example disables PIM on the selected interface:

```
ciscoasa(config-if)# no pim
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim accept-register

To configure the ASA to filter PIM register messages, use the **pim accept-register** command in global configuration mode. To remove the filtering, use the **no** form of this command.

pim accept-register { **list** *acl* | **route-map** *map-name* }
no pim accept-register

Syntax Description

list *acl*	Specifies an access list name or number. Use only extended host ACLs with this command.
route-map *map-name*	Specifies a route-map name. Use extended host ACLs in the referenced route-map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is used to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the ASA will immediately send back a register-stop message.

Examples

The following example restricts PIM register messages to those from sources defined in the access list named “no-ssm-range”:

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim bidir-neighbor-filter

To control which bidir-capable neighbors can participate in the DF election, use the **pim bidir-neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim bidir-neighbor-filter *acl*
no pim bidir-neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. The access list defines the neighbors that can participate in bidir DF elections. Use only standard ACLs with this command; extended ACLs are not supported.

Command Default

All routers are considered to be bidir capable.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The **pim bidir-neighbor-filter** command enables the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in DF election while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When the **pim bidir-neighbor-filter** command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election does not occur.
- If a denied neighbor supports bidir, then DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Examples

The following example allows 10.1.1.1 to become a PIM bidir neighbor:

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
```

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

Command	Description
multicast boundary	Defines a multicast boundary for administratively-scoped multicast addresses.
multicast-routing	Enables multicast routing on the ASA.

pim bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the pim bsr-border command in interface configuration mode.

Note A border interface in a PIM sparse mode (PIM-SM) domain requires special precautions to avoid exchange of certain traffic with a neighboring domain reachable through that interface, especially if that domain is also running PIM-SM.

pim bsr-border
no pim bsr-border

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

When this command is configured on an interface, no PIM Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Examples

The following example configures the interface to be PIM domain border:

```
ciscoasa(config)# interface gigabit 0/0
ciscoasa(config-if)# pim bsr-border
ciscoasa(config)# show runn interface gigabitEthernet 0/0
!
```

```
interface GigabitEthernet0/0
 nameif outsideA
 security-level 0
 ip address 2.2.2.2 255.255.255.0
 pim bsr-border
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.
pim bsr-candidate	Configures ASA as candidate BSR

pim bsr-candidate

To configure the router to announce its candidacy as a bootstrap router (BSR), use the pim bsr-candidate command in global configuration mode. To remove this router as a candidate for being a bootstrap router, use the no form of this command.

pim bsr-candidate *interface-name* [*hash-mask-length* [*priority*]]
no pim bsr-candidate

Syntax Description

interface-name	Interface name on this router from which the BSR address is derived. This address is sent in BSR messages.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The C-BSR with the highest priority value is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default priority is 0.

Command Default

The command is disabled by default.

When a device is configured as a bsr-candidate without hash-length and priority, it assumes a default hash length of 0 and priority as 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command causes the ASA to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is

the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, it drops the bootstrap message.

This ASA continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Examples

The following example configures the ASA as a candidate boot strap router (C-BSR) on the inside interface, with a hash length of 30 and a priority of 10:

```
ciscoasa(config)# pim bsr-candidate inside 30 10
ciscoasa(config)# sh runn pim
pim bsr-candidate inside 30 10
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.
pim bsr-border	Configures ASA as border BSR

pim dr-priority

To configure the neighbor priority on the ASA used for designated router election, use the **pim dr-priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

pim dr-priority *number*
no pim dr-priority

Syntax Description

number	A number from 0 to 4294967294. This number is used to determine the priority of the device when determining the designated router. Specifying 0 prevents the ASA from becoming the designated router.

Command Default

The default value is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The device with the largest priority value on an interface becomes the PIM designated router. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the DR. If a device does not include the DR-Priority Option in hello messages, it is regarded as the highest-priority device and becomes the designated router. If multiple devices do not include this option in their hello messages, then the device with the highest IP address becomes the designated router.

Examples

The following example sets the DR priority for the interface to 5:

```
ciscoasa(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim hello-interval

To configure the frequency of the PIM hello messages, use the **pim hello-interval** command in interface configuration mode. To restore the hello-interval to the default value, use the **no** form of this command.

pim hello-interval *seconds*
no pim hello-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the ASA waits before sending a hello message. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.

Command Default

The interval default is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the PIM hello interval to 1 minute:

```
ciscoasa(config-if)# pim hello-interval 60
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim join-prune-interval

To configure the PIM join/prune interval, use the **pim join-prune-interval** command in interface configuration mode. To restore the interval to the default value, use the **no** form of this command.

pim join-prune-interval *seconds*
no pim join-prune-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the ASA waits before sending a join/prune message. Valid values range from 10 to 600 seconds. 60 seconds is the default.

Command Default

The default interval is 60 seconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the PIM join/prune interval to 2 minutes:

```
ciscoasa(config-if)# pim join-prune-interval 120
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim neighbor-filter

To control which neighbor routers can participate in PIM, use the **pim neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim neighbor-filter *acl*
no pim neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. Use only standard ACLs with this command; extended ACLs are not supported.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command defines which neighbor routers can participate in PIM. If this command is not present in the configuration then there are no restrictions.

Multicast routing and PIM must be enabled for this command to appear in the configuration. If you disable multicast routing, this command is removed from the configuration.

Examples

The following example allows the router with the IP address 10.1.1.1 to become a PIM neighbor on interface GigabitEthernet 0/2:

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim old-register-checksum

To allow backward compatibility on a rendezvous point (RP) that uses old register checksum methodology, use the **pim old-register-checksum** command in global configuration mode. To generate PIM RFC-compliant registers, use the **no** form of this command.

pim old-register-checksum
no pim old-register-checksum

Syntax Description

This command has no arguments or keywords.

Command Default

The ASA generates PIM RFC-compliant registers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA software accepts register messages with checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS method—accepting register messages with the entire PIM message for all PIM message types. The **pim old-register-checksum** command generates registers compatible with Cisco IOS software.

Examples

The following example configures the ASA to use the old checksum calculations:

```
ciscoasa(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim rp-address

To configure the address of a PIM rendezvous point (RP), use the **pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

pim rp-address *ip_address* [*acl*] [**bidir**]
no pim rp-address *ip_address*

Syntax Description

acl	(Optional) The name or number of a standard access list that defines which multicast groups the RP should be used with. Do not use a host ACL with this command.
bidir	(Optional) Indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM sparse mode.
ip_address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.

Command Default

No PIM RP addresses are configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain require knowledge of the well-known PIM RP address. The address is statically configured using this command.

Note The ASA does not support Auto-RP; you must use the **pim rp-address** command to specify the RP address.

You can configure a single RP to serve more than one group. The group range specified in the access list determines the PIM RP group mapping. If the an access list is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

Note The ASA always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Examples

The following example sets the PIM RP address to 10.0.0.1 for all multicast groups:

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

Related Commands

Command	Description
pim accept-register	Configures candidate RPs to filter PIM register messages.

pim spt-threshold infinity

To change the behavior of the last hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

pim spt-threshold infinity [**group-list** *acl*]
no pim spt-threshold

Syntax Description

group-list *acl*	(Optional) Indicates the source groups restricted by the access list. The *acl* argument must specify a standard ACL; extended ACLs are not supported.

Command Default

The last hop PIM router switches to the shortest-path source tree by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the **group-list** keyword is not used, this command applies to all multicast groups.

Examples

The following example causes the last hop PIM router to always use the shared tree instead of switching to the shortest-path source tree:

```
ciscoasa(config)# pim spt-threshold infinity
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

ping

To test connectivity from a specified interface to an IP address, use the **ping** command in privileged EXEC mode. The parameters available differ for regular ICMP-based ping compared to TCP ping. Enter the command without parameters to be prompted for values, including characteristics not available as parameters.

ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes* [**validate**]
ping tcp [*if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]
ping

Note The source and port options are only available with the tcp option; the data, size, and validate options are not available with the tcp option.

Syntax Description

data *pattern*	(Optional, ICMP only.) Specifies the 16-bit data pattern in hexadecimal format, from 0 to FFFF. The default is 0xabcd.
host	Specifies the IPv4 address or name of the host to ping. For ICMP pings, you can specify an IPv6 address (which is not supported for TCP pings). When using host names, the name can be a DNS name or a name assigned with the **name** command. The maximum number of characters for DNS names is 128, and the maximum number of characters for names created with the **name** command is 63. You must configure a DNS server to use DNS names.
if_name	(Optional) Specifies the interface name whose IP address is used for the ping source; however, the actual egress interface is determined by a route lookup using the data routing table.
port	(TCP only.) Specifies the TCP port number for the host you are pinging, 1-65535.
repeat *count*	(Optional) Specifies the number of times to repeat the ping request. The default is 5.
size *bytes*	(Optional, ICMP only.) Specifies the datagram size in bytes. The default is 100.
source *host port*	(Optional, TCP only.) Specifies a certain IP address and port to send the ping from (Use port = 0 for a random port). The source address does not affect how the packet is routed.
tcp	(Optional) Tests a connection over TCP (the default is ICMP). A TCP ping sends SYN packets and considers the ping successful if the destination sends a SYN-ACK packet. You can also have at most 2 concurrent TCP pings running at a time.
timeout *seconds*	(Optional) Specifies the number of seconds of the timeout interval. The default is 2 seconds.
validate	(Optional, ICMP only.) Validates reply data.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Support for DNS names was added.
8.4(1)	The **tcp** option was added.
9.18(2)	If you specify the interface in the command, the source IP address matches the specified interface IP address, but the actual egress interface is determined by a route lookup using the data routing table.

Usage Guidelines

The **ping** command allows you to determine if the ASA has connectivity or if a host is available on the network.

When using regular ICMP-based ping, ensure that you do not have **icmp** rules that prohibit these packets (if you do not use ICMP rules, all ICMP traffic is allowed). If you want internal hosts to ping external hosts over ICMP, you must do one of the following:

- Create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list acl_grp permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.
- Configure the ICMP inspection engine using the **inspect icmp** command. For example, adding the **inspect icmp** command to the **class default_inspection** class for the global service policy allows echo replies through the ASA for echo requests initiated by internal hosts.

When using TCP ping, you must ensure that access policies allow TCP traffic on the ports you specify.

This configuration is required to allow the ASA to respond and accept messages generated from the **ping** command. The **ping** command output shows if the response was received. If a host is not responding after you enter the **ping** command, a message similar to the following appears:

```
ciscoasa(config)# ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

To route ping packets, the ASA uses the data routing table, and falls back to the management routing table only if there is not a matching route in the data table. Specifying the source IP address for TCP ping does not affect how the packet is routed. For example, even if you manually specify the source address to match an interface IP address, then the ping will not be sent out of that interface. The egress interface is only determined by the route lookup.

Use the **show interface** command to ensure that the ASA is connected to the network and is passing traffic. The address of the specified *if_name* is used as the source address of the ping unless you specify a different source address (TCP ping only).

You can also perform an extended ping by entering **ping** without parameters. You are prompted for the parameters, including some characteristics not available as keywords.

Examples

The following example shows how to determine if other IP addresses are visible from the ASA:

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example specifies a host using a DNS name:

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following is an example of an extended ping:

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
The following are examples of the ping tcp command:
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7

Source IP port: [0] 465

Repeat count: [5]
Timeout in seconds: [2] 5

Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms
ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Related Commands

Command	Description
icmp	Configures access rules for ICMP traffic that terminates at an interface.
show interface	Displays information about the VLAN configuration.

po - pq

police

To apply QoS policing to a class map, use the **police** command in class configuration mode. To remove rate limiting, use the **no** form of this command.

police { **output** | **input** } *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]
no police

Syntax Description

conform-rate	Sets the rate limit for this traffic class, from 8000 and 2000000000 bits per second. For the ASA virtual and Firepower 4100/9300, the range is 8000-100000000000. For example, to limit traffic to 5Mbps, enter 5000000.
conform-burst	Specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512000000 bytes. For the ASA virtual and Firepower 4100/9300, the range is 1000-25600000000. If you omit this parameter, the default value is 1/32 of the conform-rate in bytes (that is, with a conform rate of 100,000, the default conform-burst value would be 100,000/32 = 3,125). Note that the conform-rate is in bits/second, whereas the conform-burst is in bytes.
conform-action [**drop** | **transmit**]	Sets the action to take when the traffic is below the policing rate and burst size. You can **drop** or **transmit** the traffic. The default is to transmit the traffic.
exceed-action [**drop** | **transmit**]	Sets the action to take when traffic exceeds the policing rate and burst size. You can **drop** or **transmit** packets that exceed the policing rate and burst size. The default is to drop excess packets.
input	Enables policing of traffic flowing in the input direction.
output	Enables policing of traffic flowing in the output direction.

Command Default

No default behavior or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **input** option was added. Policing traffic in the inbound direction is now supported.

Usage Guidelines

Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the ASA drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

To enable policing, use the Modular Policy Framework:

1.class-map—Identify the traffic on which you want to perform policing.

2.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.police**—Enable policing for the class map.

3.service-policy—Assigns the policy map to an interface or globally.

You can configure each of the QoS features alone if desired for the ASA. Often, though, you configure multiple QoS features on the ASA so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + policing (for the rest of the traffic).

You cannot configure priority queuing and policing for the same set of traffic.

- Traffic shaping (for all traffic on an interface) + hierarchical priority queuing (for a subset of traffic).

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the ASA does not restrict you from configuring this.

See the following guidelines:

- QoS is applied unidirectionally; only traffic that enters the interface to which you apply the policy map is affected (or exits the interface, depending on the whether you specify **input** or **output**).
- If a service policy is applied or removed from an interface that has existing traffic already established, the QoS policy is not applied or removed from the traffic stream. To apply or remove the QoS policy for such connections, you must clear the connections and re-establish them. See the **clear conn** command.
- To-the-box traffic is not supported.
- Traffic to and from a VPN tunnel bypass interface is not supported.
- When you match a tunnel group class map, only outbound policing is supported.

Examples

The following is an example of a **police** command for the output direction that sets the conform rate to 100,000 bits per second, with a burst value of 20,000 bytes.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass

ciscoasa(config-pmap-c)# police output 100000 20000
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

The following example shows how to do rate-limiting on traffic destined to an internal web server:

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

Related Commands

class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

policy

To specify the source for retrieving the CRL, use the **policy** command in ca-crl configuration mode.

policy { **static** | **cdp** | **both** }

Syntax Description

both	Specifies that if obtaining a CRL using the CRL distribution point fails, retry using static CDPs up to a limit of five.
cdp	Uses the CDP extension embedded within the certificate being checked. In this case, the ASA retrieves up to five CRL distributions points from the CDP extension of the certificate being verified and augments their information with the configured default values, if necessary. If the ASA attempt to retrieve a CRL using the primary CDP fails, it retries using the next available CDP in the list. This continues until either the ASA retrieves a CRL or exhausts the list.
static	Uses up to five static CRL distribution points. If you specify this option, specify also the LDAP or HTTP URLs with the **protocol** command.

Command Default

The default setting is **cdp**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and configures CRL retrieval to occur using the CRL distribution point extension in the certificate being checked or if that fails, to use static CDPs:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
url	Creates and maintains a list of static URLs for retrieving CRLs.

policy-list

To create a Border Gateway Protocol (BGP) policy list, use the **policy-list** command in policy-map configuration mode. To remove a policy list, use the **no** form of this command.

policy-list *policy-list-name* { **permit** | **deny** }
no policy-list *policy-list-name*

Syntax Description

policy-list-name	Name of the configured policy list.
permit	Permits access for matching conditions.
deny	Denies access for matching conditions.

Command Default

This command is not enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. Policy- lists configured within a route map are evaluated with AND semantics or OR semantics. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

The policy-list sub-commands are listed here:

Sub-Commands	Details
match as-path [path-list-number]	Matches as-path and it can take multiple as-path path-list numbers
Match community[community-name][exact-match]	Community name is must and exact-match is optional. Multiple names can be given
Match interface [interface-name]	Can take Multiple interface names

Sub-Commands	Details
match metric <0-4294967295>	It can take multiple numbers
Match ip address [acl name prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Match ip next-hop [acl name | prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Match ip route-source [acl name | prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Default match	Default will have all above options under “match”
Help	Helps for the subsequent commands
No	Negation of the commands
Exit	Exit policy-map mode

Examples

In the following example, a policy list is configured that permits all network prefixes that match AS 1 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

In the following example, a policy list is configured that permits traffic that matches community 20 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

In the following example, a policy list is configured that denies traffic that matches community 20 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

When using the Modular Policy Framework, assign actions to traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command) by using the **policy-map** command (without the **type** keyword) in global configuration mode. To remove a Layer 3/4 policy map, use the **no** form of this command.

policy-map*name*
no policy-map *name*

Syntax Description

name	Specifies the name for this policy map up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Command Default

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy for a particular feature.)

The default policy includes the following application inspections:

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

The default policy configuration includes the following commands:

```
class-map inspection_default
 match default-inspection-traffic
```

```
policy-map type inspect dns preset_dns_map
 parameters
message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1.Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.

2.(Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.

3.Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.

4.Activate the actions on an interface using the **service-policy** command.

The maximum number of policy maps is 64, but you can only apply one policy map per interface. You can apply the same policy map to multiple interfaces. You can identify multiple Layer 3/4 class maps in a Layer 3/4 policy map (see the **class** command), and you can assign multiple actions from one or more feature types to each class map.

Examples

The following is an example of a **policy-map** command for connection policy. It limits the number of connections allowed to the web server 10.1.1.1:

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the ASA does not make this match because they previously matched other classes.

NetFlow events are configured through Modular Policy Framework. If Modular Policy Framework is not configured for NetFlow, no events are logged. Traffic is matched based on the order in which classes are configured. After a match is detected, no other classes are checked. For NetFlow events, the configuration requirements are as follows:

- A flow-export destination (that is, a NetFlow collector) is uniquely identified by its IP address.

- Supported event types are flow-create, flow-teardown, flow-denied, flow-update, and all, which include the four previously listed event types.
- Use the **flow-export event-type** {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination** command to configure the address of NetFlow collectors and filters to determine which NetFlow records should be sent to each collector.
- Flow-export actions are not supported in interface policies.
- Flow-export actions are only supported in the **class-default** command and in classes with the **match any** or **match access-list** command.
- If no NetFlow collector has been defined, no configuration actions occur.
- NetFlow Secure Event Logging filtering is order-independent.

The following example exports all NetFlow events between hosts 10.1.1.1 and 20.1.1.1 to destination 15.1.1.1.

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
clear configure policy-map	Removes all policy map configuration. If a policy map is in use in a **service-policy** command, that policy map is not removed.
class-map	Defines a traffic class map.
service-policy	Assigns the policy map to an interface or globally to all interfaces.
show running-config policy-map	Display all current policy map configurations.

policy-map type inspect

When using the Modular Policy Framework, define special actions for inspection application traffic by using the **policy-map type inspect** command in global configuration mode. To remove an inspection policy map, use the **no** form of this command.

policy-map type inspect *application policy_map_name*
no policy-map [**type inspect** *application*] *policy_map_name*

Syntax Description

application Specifies the type of application traffic you want to act upon. Available types include:

- **dcerpc**
- **diameter**
- **dns**
- **esmtp**
- **ftp**
- **gtp**
- **h323**
- **http**
- **im**
- **ip-options**
- **ipsec-pass-thru**
- **ipv6**
- **lisp**
- **m3ua**
- **mgcp**
- **netbios**
- **radius-accounting**
- **rtsp**
- **scansafe**
- **sctp**
- **sip**
- **skinny**
- **snmp**

policy_map_name	Specifies the name for this policy map up to 40 characters in length. Names that begin with "_internal" or "_default" are reserved and cannot be used. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.2(1)	The **ipv6** keyword was added to support IPv6 inspection.
9.0(1)	The **scansafe** keyword was added to support Cloud Web Security.
9.5(2)	The **lisp** keyword was added to support LISP inspection.
9.5(2)	The **diameter** and **sctp** keywords were added.
9.6(2)	The **m3ua** keywords were added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

An inspection policy map consists of one or more of the following commands entered in policy-map configuration mode. The exact commands available for an inspection policy map depends on the application.

- **match** command—You can define a **match** command directly in the inspection policy map to match application traffic to criteria specific to the application, such as a URL string. Then you enable actions in match configuration mode such as **drop**, **reset**, **log**, and so on. The **match** commands available depend on the application.
- **class** command—This command identifies an inspection class map in the policy map (see the **class-map type inspect** command to create the inspection class map). An inspection class map includes **match** commands that match application traffic with criteria specific to the application, such as a URL string, for which you then enable actions in the policy map. The difference between creating a class map and using a **match** command directly in the inspection policy map is that you can group multiple matches, and you can reuse class maps.

- **parameters** command—Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

You can specify multiple **class** or **match** commands in the policy map.

Some **match** commands can specify regular expressions to match text inside a packet. See the **regex** command and the **class-map type regex** command, which groups multiple regular expressions.

The default inspection policy map configuration includes the following commands:

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

If a packet matches multiple different **match** or **class** commands, then the order in which the ASA applies the actions is determined by internal ASA rules, and not by the order they are added to the policy map. The internal rules are determined by the application type and the logical progression of parsing a packet, and are not user-configurable. For example for HTTP traffic, parsing a Request Method field precedes parsing the Header Host Length field; an action for the Request Method field occurs before the action for the Header Host Length field. For example, the following match commands can be entered in any order, but the **match request method get** command is matched first.

```
ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log
```

If an action drops a packet, then no further actions are performed. For example, if the first action is to reset the connection, then it will never match any further **match** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. (You can configure both the **reset** (or **drop-connection**, and so on.) and the **log** action for the same **match** command, in which case the packet is logged before it is reset for a given match.)

If a packet matches multiple **match** or **class** commands that are the same, then they are matched in the order they appear in the policy map. For example, for a packet with the header length of 1001, it will match the first command below, and be logged, and then will match the second command and be reset. If you reverse the order of the two **match** commands, then the packet will be dropped and the connection reset before it can match the second **match** command; it will never be logged.

```
ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset
```

A class map is determined to be the same type as another class map or **match** command based on the lowest priority **match** command in the class map (the priority is based on the internal rules). If a class map has the same type of lowest priority **match** command as another class map, then the class maps are matched according to the order they are added to the policy map. If the lowest priority command for each class map is different, then the class map with the higher priority **match** command is matched first.

If you want to exchange an in-use inspection policy map for a different map name, you must remove the **inspect** *protocol map* command, and enter it again with the new map. For example:

```
ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# no
 inspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2
```

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match
 regex
 example
ciscoasa(config-cmap)# match
 regex
 example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
(a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy inbound_policy interface outside
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
parameters	Enters parameter configuration mode for an inspection policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

policy-route

To configure policy-based routing on an interface, use the **policy-route** command in interface configuration mode.

policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }
no policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }

Syntax Description

cost *value*	Sets the relative cost of the interface for policy-based routing evaluation. The value can be 1-65535. The default is 0, which you can reset by using the **no** version of the command. The lower the number, the higher the priority. For example, 1 has priority over 2.
route-map*route_map_name*	Specifies the name of the route map to use for policy-based routing.
path-monitoring	Set the monitoring type for the interface's peer to collect the flexible metrics.

Command Default

There is no default route map. The default cost is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.17(1)	The **cost** keyword was added.
9.18(1)	This command was enhanced to include path-monitoring feature for PBR to determine the best path for routing traffic.

Usage Guidelines

After configuring the route-map that specifies the match criteria and the resulting action if all of the match clauses are met, use the **policy-route route-map** command to apply it to a particular interface.

If you use **set adaptive-interface cost** as a criteria in the route map, set the cost on the interface using the **policy-route cost** command.

When you set policy-route cost, and use the **set adaptive-interface cost** command in the route map, the egress traffic is round-robin load balanced across any selected interfaces (assuming they are up) that have the same interface cost. If costs are different, higher cost interfaces are used as backups to the lowest cost interface.

For example, by setting the same cost on 2 WAN links, you can load balance the traffic across those links to perhaps improve performance. However, if one WAN link has higher bandwidth than the other, you can set the higher bandwidth link's cost to 1, and the lower bandwidth link to 2, so that the lower bandwidth link is used only if the higher bandwidth link is down.

Examples

The following example applies a route map to an interface for policy-based routing.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmapv4
ciscoasa(config)# show run interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  policy-route route-map testmapv4
!
ciscoasa(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
       ip address (access-lists): testaclv4
   Set clauses:
               ip next-hop 1.1.1.1
```

The following example sets unequal costs, so that output1 is the preferred link, and output2 is used only if output1 is down. To configure load balancing across the interfaces, set equal cost values.

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

The path monitoring feature detects a failure in a route link or path that is no longer forwarding traffic. It enables threat defense to collect performance metrics like RTT, jitter, packet loss, and Mean Opinion Score (MOS) to determine the best path for forwarding the traffic.

To configure path monitoring, use the **policy-route** command. You must specify the monitoring type that the device must use to collect the performance metrics from the peer gateway. For the auto option, the next-hop of the default route is used as the peer to monitor. IPv4 is attempted first, and then IPv6. For VTI interfaces, the auto option is not supported. You must specify the IPv4 or IPv6 address of its peer.

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost             set interface cost
  path-monitoring  Keyword for path monitoring
  route-map        Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config
```

```
ciscoasa(config-if)# policy-route path-monitoring auto
```

policy-server-secret (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To configure a secret key used to encrypt authentication requests to a SiteMinder SSO server, use the **policy-server-secret** command in webvpn-sso-siteminder configuration mode. To remove a secret key, use the **no** form of this command.

policy-server-secret *secret-key*
no policy-server-secret

Note This command is required for SiteMinder SSO authentication.

Syntax Description

secret-key	The character string used as a secret key to encrypt authentication communications. There is no minimum or maximum number of characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config-webvpn-sso-siteminder configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. You first create the SSO server using the **sso-server** command. For SiteMinder SSO servers, the **policy-server-secret** command secures authentication communications between the ASA and the SSO server.

The command argument, *secret-key*, is similar to a password: you create it, save it, and configure it. It is configured on both the ASA using the **policy-server-secret** command and on the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

This command applies only to the SiteMinder type of SSO server.

Examples

The following command, entered in config-webvpn-sso-siteminder mode and including a random character string as an argument, creates a secret key for SiteMinder SSO server authentication communications:

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

policy static sgt

To apply a policy to a manually configured Cisco TrustSec link, use the **policy static sgt** command in cts manual interface configuration mode. To remove a policy to a manually configured CTS link, use the **no** form of this command.

policy static sgt *sgt_number* [**trusted**]
no policy static sgt *sgt_number* [**trusted**]

Syntax Description

sgt *sgt_number*	Specifies the SGT number to apply to incoming traffic from the peer. Valid values are from 2-65519.
static	Specifies an SGT policy to incoming traffic on the link.
trusted	Indicates that ingress traffic on the interface with the SGT specified in the command should not have its SGT overwritten. Untrusted is the default.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cts manual interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command applies a policy to a manually configured CTS link.

Restrictions

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI, TVI, and VNI.

Examples

The following example enables an interface for Layer 2 SGT imposition and defines whether or not the interface is trusted:

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Related Commands

Command	Description
cts manual	Enables Layer 2 SGT Imposition and enters cts manual interface configuration mode.
propagate sgt	Propagates a security group tag (called **sgt**) on an interface. Propagation is enabled by default.

polltime interface

To specify the data interface polltime and holdtime in an Active/Active failover configuration, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface [**msec**] *polltime* [**holdtime** *time*]
no polltime interface [**msec**] *polltime* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time (as a calculation) between the last-received hello message from the peer unit and the commencement of interface tests to determine the health of the interface. It also sets the duration of each interface test as *holdtime* /16. Valid values are from 5 to 75 seconds. The default is 5 times the *polltime* . You cannot enter a holdtime value that is less than five times the *polltime* . To calculate the time before starting interface tests (y): **1.** x = (*holdtime* /*polltime)/2* , rounded to the nearest integer. (.4 and down rounds down; .5 and up rounds up.) **2.** y = x**polltime* For example, if you use the default holdtime of 25 and polltime of 5, then y = 15 seconds.
interface *time*	Specifies how long to wait between sending a hello packet to the peer. Valid values range from 1 to 15 seconds. The default is 5. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Command Default

The poll *time* is 5 seconds.

The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The command was changed to include the optional **holdtime** *time* value and the ability to specify the poll time in milliseconds.

This command is available for Active/Active failover only. Use the **failover polltime interface** command in Active/Standby failover configurations.

With a faster polltime, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

You can include both **polltime unit** and **polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following partial example shows a possible configuration for a failover group. The interface poll time is set to 500 milliseconds and the hold time to 5 seconds for data interfaces in failover group 1.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Specifies the unit failover poll and hold times.
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.

poll-timer

To specify the timer during which the ASA queries the DNS server to resolve fully qualified domain names (FQDN) that are defined in a network object group, use the **poll-timer** command in dns server-group configuration mode for the DefaultDNS server group only. To remove the timer, use the **no** form of this command.

poll-timer minutes *minutes*
no poll-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer in minutes. Valid values are from 1 to 65535 minutes.

Command Default

By default, the DNS timer is 240 minutes or 4 hours.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command is supported for the DefaultDNS server group only.

This command specifies the timer during which the ASA queries the DNS server to resolve the FQDN that was defined in a network object group. A FQDN is resolved periodically when the poll DNS timer has expired or when the TTL of the resolved IP entry has expired, whichever comes first.

This command has effect only when at least one network object group has been activated.

Examples

The following example sets the DNS poll timer to 240 minutes:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# poll-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.

pop3s (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To enter POP3S configuration mode, use the **pop3s** command in global configuration mode. To remove any commands entered in POP3S command mode, use the **no** version of this command.

POP3 is a client/server protocol in which your Internet server receives and holds e-mail for you. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. This standard protocol is built into most popular e-mail products. POP3S lets you receive e-mail over an SSL connection.

pop3s
no pop3

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Examples

The following example shows how to enter POP3S configuration mode:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)#
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.

Command	Description
show running-config pop3s	Displays the running configuration for POP3S.

port (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the port an e-mail proxy listens to, use the **port** command in the applicable e-mail proxy command mode. To revert to the default value, use the **no** version of this command.

port *portnum*
no port

Syntax Description

portnum	The port for the e-mail proxy to use. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Command Default

The default ports for e-mail proxies are as follows:

E-mail Proxy	Default Port
IMAP4S	993
POP3S	995
SMTPS	988

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s	• Yes	—	• Yes	—	—
Imap4s	• Yes	—	• Yes	—	—
Smtps	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Examples

The following example shows how to set port 1066 for the IMAP4S e-mail proxy:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# port 1066
```

portal-access-rule(Deprecated)

This command allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources.

portal-access-rule none
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*] } { **any** | **user-agent match** *string* }
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*] } { **any** | **user-agent match** *string* }]
clear configure webvpn portal-access-rule

Syntax Description

none	Removes all portal access rules. Clientless SSL VPN sessions will not restricted based on HTTP header.
priority	Priority of rule. Range: 1-65535.
permit	Permit access based upon HTTP header.
deny	Deny access based upon HTTP header.
code	Permit or deny access based on a returned HTTP status code. Default: 403.
code	The HTTP status code number based on which you want to permit or deny access. Range: 200-599.
any	Match any HTTP header string.
user-agent match	Enable comparison of strings in HTTP headers.
string	Specify the string to match in the HTTP header. Surround the string you are searching for with wildcards (*) for a match that contains your string or do not use wildcards to specify an exact match of your string. **Note** We recommend using wildcards in your search string. Without them, the rule may not match any strings or many fewer than you expect. If the string you are searching for has a space in it, the string must be enclosed in quotations; for example, "*a string* ". When using both quotations and wild cards, your search string would look like this: "**a string* *".
no portal-access-rule	Use to delete a single portal-access-rule.
clear configure webvpn portal-access-rule	Equivalent to portal-access-rule none command.

Command Default

portal-access-rule none

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)	This command was added simultaneously in ASA 8.2.5 and 8.4(2).
8.4(2)	This command was added simultaneously in ASA 8.2.5 and 8.4(2).
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

This check is performed prior to user authentication.

Examples

The following example creates three portal access rules:

- Portal access rule 1 denies attempted clientless SSL VPN connections when the ASA returns code 403 and Thunderbird is in the HTTP header.
- Portal access rule 10 permits attempted clientless SSL VPN connections when MSIE 8.0 (Microsoft Internet Explorer 8.0) is in the HTTP header.
- Portal access rule 65535 permits all other attempted clientless SSL VPN connections.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```

Note If HostScan is installed, the port-access-rule feature does not stop the ASA from opening pages like Cisco Secure Desktop portal. To avoid the Cisco Secure Desktop port, HostScan needs to be uninstalled.

Related Commands

Command	Description
show run webvpn	Displays webvpn configuration including all portal-access-rules.
show vpn-sessiondb detail webvpn	Display information about VPN sessions. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information.
debug webvpn request *n*	Enables logging of debug messages at a particular level of debugging. Default: 1. Range: 1-255.

port-channel load-balance

For EtherChannels, to specify the load-balancing algorithm, use the **port-channel load-balance** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

port-channel load-balance { **dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port** }
no port-channel load-balance

Syntax Description

dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination IP address
dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination IP address • Destination Port
dst-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination MAC address
dst-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination port
src-dst-ip	(Default) Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Destination IP address

src-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Destination IP address • Source Port • Destination Port
src-dst-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Source MAC address • Destination MAC address
src-dst-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source port • Destination port
src-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address
src-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Source port
src-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Source MAC address
src-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source port
vlan-dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Destination IP address

vlan-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Destination IP address • Destination port
vlan-only	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN
vlan-src-dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Destination IP address
vlan-src-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Destination IP address • Source port • Destination port
vlan-src-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address
vlan-src-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Source port

Command Default

The default is **src-dst-ip**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

The ASA distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (**src-dst-ip**). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a *hash_value* **mod** *active_links* result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

For a spanned EtherChannel in clustering, load balancing occurs on a per ASA basis. For example, if you have 32 active interfaces in the spanned EtherChannel across 8 ASAs, with 4 interfaces per ASA in the EtherChannel, then load balancing only occurs across the 4 interfaces on the ASA.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

Examples

The following example sets the load-balancing algorithm to use the source and destination IP addresses and ports:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

port-channel min-bundle

For EtherChannels, to specify the minimum number of active interfaces required for the port-channel interface to become active, use the **port-channel min-bundle** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

port-channel min-bundle *number*
no port-channel min-bundle

Syntax Description

number	Specifies the minimum number of active interfaces required for the port-channel interface to become active, between 1 and 8; for 9.2(1) and later, the active interfaces can be between 1 and 16.

Command Default

The default is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.
9.2(1)	The number of active interfaces was increased from 8 to 16.

Usage Guidelines

Enter this command for a port-channel interface. If the active interfaces in the channel group falls below this value, then the port-channel interface goes down, and could trigger a device-level failover.

Examples

The following example sets the minimum number of active interfaces required for the port-channel to become active to two:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.

Command	Description
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

port-channel span-cluster

To sets this EtherChannel as a spanned EtherChannel in an ASA cluster, use the **port-channel span-cluster** command in interface configuration mode. To disable spanning, use the **no** form of this command.

Note Supported on ASA hardware models only. Other models implicitly set data EtherChannels to spanned mode.

port-channel span-cluster [**vss-load-balance**]
no port-channel span-cluster [**vss-load-balance**]

Syntax Description

vss-load-balance	(Optional) Enables VSS load balancing. If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the **vss-id** keyword in the **channel-group** command for each member interface before enabling load balancing.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must be in spanned EtherChannel mode (**cluster interface-mode spanned**) to use this feature.

This feature lets you group one or more interfaces per unit into an EtherChannel that spans all units in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the bridge group, not to the interface. The EtherChannel inherently provides load balancing as part of basic operation.

Examples

The following example creates an EtherChannel (port-channel 2) with the tengigabitethernet 0/8 interface as the only member, and then spans the EtherChannel across the cluster. Two subinterfaces are added to port-channel 2.

```
interface tengigabitethernet 0/8
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
cluster interface-mode	Sets the cluster interface mode, for either Spanned EtherChannels or individual interfaces.

port-forward(Deprecated)

To configure the set of applications that users of clientless SSL VPN session can access over forwarded TCP ports, use the **port-forward** command in webvpn configuration mode.

port-forward { *list_name local_port remote_server remote_port description* }

To configure access to multiple applications, use this command with the same *list_name* multiple times, once for each application.

To remove a configured application from a list, use the **no port-forward** *list_name local_port* command (you need not include the *remote_server* and *remote_port* parameters).

no port-forward *listname localport*

To remove an entire configured list, use the **no port-forward** *list_name* command.

no port-forward *list_name*

Syntax Description

description	Provides the application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.
list_name	Groups the set of applications (forwarded TCP ports) users of clientless SSL VPN sessions can access. Maximum 64 characters.
local_port	Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *list_name*. Enter a port number in the range 1-65535. To avoid conflicts with existing services, use a port number greater than 1024.
remote_port	Specifies the port to connect to for this application on the remote server. This is the actual port the application uses. Enter a port number in the range 1-65535 or port name.
remote_server	Provides the DNS name or IP address of the remote server for an application. If you enter the IP address, you may enter it in either IPv4 or IPv6 format. We recommend using a host name so that you do not have to configure the client applications for a specific IP addresses. The dns server-group command **name-server** must resolve the host name to an IP address.

Command Default

There is no default port forwarding list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The command mode was changed to webvpn.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

Port forwarding does not support Microsoft Outlook Exchange (MAPI) proxy. However, you can configure Smart Tunnel support for Microsoft Outlook Exchange 2010.

Examples

The following table shows the values used for example applications.

Application	Local Port	Server DNS Name	Remote Port	Description
IMAP4S e-mail	20143	IMAP4Sserver	143	Get Mail
SMTPS e-mail	20025	SMTPSserver	25	Send Mail
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

The following example shows how to create a port forwarding list called *SalesGroupPorts* that provides access to these applications:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

Related Commands

Command	Description
port-forward auto-start	Entered in group-policy webvpn or username webvpn mode, this command starts port forwarding automatically and assigns the specified port forwarding list when the user logs onto a clientless SSL VPN session.
port-forward enable	Entered in group-policy webvpn or username webvpn mode, this command starts assigns the specified port forwarding list when the user logs on, but requires the user to start port forwarding manually, using the **Application Access** > **Start Applications** button on the clientless SSL VPN portal page.

Command	Description
port-forward disable	Entered in group-policy webvpn or username webvpn mode, this command turns off port forwarding.

port-forward-name(Deprecated)

To configure the display name that identifies TCP port forwarding to end users for a particular user or group policy, use the **port-forward-name** command in webvpn mode, which you enter from group-policy or username mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** use the no form of the command. The **no** option restores the default name, "Application Access." To prevent a display name, use the **port-forward none** command.

port-forward-name { **value** *name* | **none** }
no port-forward-name

Syntax Description

none	Indicates that there is no display name. Sets a null value, thereby disallowing a display name. Prevents inheriting a value.
value *name*	Describes port forwarding to end users. Maximum of 255 characters.

Command Default

The default name is "Application Access."

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Examples

The following example shows how to set the name, "Remote Access TCP Applications," for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

port-object

To add a port object to a service object group of the type TCP, UDP, or TCP-UDP, use the **port-object** command in object-group service configuration mode. To remove port objects, use the **no** form of this command.

port-object { **eq** *port* | **range** *begin_port end_port* }
no port-object { **eq** *port* | **range** *begin_port end_port* }

Syntax Description

range *begin_port end_port*	Specifies a range of ports (inclusive), between 0 and 65535.
eq *port*	Specifies the decimal number (between 0 and 65535) or name of a TCP or UDP port for a service object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object-network service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **port-object** command is used with the **object-group service** *protocol* command to define an object that is either a specific port or a range of ports.

If a name is specified for a TCP or UDP service, it must be one of the supported TCP or/and UDP names, and must be consistent with the protocol type of the object group. For instance, for a protocol types of tcp, udp, and tcp-udp, the names must be a valid TCP service name, a valid UDP service name, or a valid TCP and UDP service name, respectively.

If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object.

The following service names are supported:

TCP	UDP	TCP and UDP
bgp	biff	discard
chargen	bootpc	domain

TCP	UDP	TCP and UDP
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

This example shows how to use the **port-object** command in service configuration mode to create a new port (service) object group:

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

post-max-size

To specify the maximum size allowed for an object to post, use the **post-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

post-max-size *size*
no post-max-size

Syntax Description

size	Specifies the maximum size allowed for a posted object. The range is 0 through 2147483647. Setting the size to 0 effectively disallows object posting.

Command Default

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example sets the maximum size for a posted object to 1500 bytes:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
post-max-size 1500
```

Related Commands

Command	Description
download-max-size	Specifies the maximum size of an object to download.
upload-max-size	Specifies the maximum size of an object to upload.

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

power inline

To enable or disable Power over Ethernet+ (PoE+) on the Firepower 1010 Ethernet 1/7 or 1/8 interface, use the **power inline** command in interface configuration mode. To return to the default state, use the **no** form of this command.

power inline { **auto** | **never** | **consumption wattage** *milliwatts* }

Note Supported for the Firepower 1010 only. Not supported for the Firepower 1010E.

Syntax Description

consumption wattage *milliwatts*	Manually specifies the wattage in milliwatts, from 4000 to 30000. Use this command if you want to set the watts manually and disable LLDP negotiation.
auto	Delivers power automatically to the powered device using a wattage appropriate to the class of the powered device. The Firepower 1010 uses LLDP to further negotiate the correct wattage.
never	Disables PoE.

Command Default

The default is **auto**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 1010 supports both IEEE 802.3af (PoE) and 802.3at (PoE+). PoE+ uses Link Layer Discovery Protocol (LLDP) to negotiate the power level. PoE+ can deliver up to 30 watts to a powered device. Power is only supplied when needed.

If you shut down the interface, then you disable power to the device. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+.

Examples

The following example manually sets the wattage for Ethernet 1/7 and sets the power to auto for Ethernet 1/8:

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

Related Commands

Command	Description
show power inline	Shows PoE status.

power-supply

For dual power supplies in the ISA 3000, to establish dual power supplies as the expected configuration in the ASA OS, use the **power-supply** command in global configuration mode. To disable the dual power supply, use the **no** form of this command.

power-supply dual
no power-supply dual

Syntax Description

dual	Specifies a dual power supply.

Command Default

By default, the dual power supply is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

If one power supply fails, the ASA issues an alarm. By default, the ASA expects a single power supply and won't issue an alarm as long as it includes one working power supply.

Examples

The following example establishes the dual power supply:

```
ciscoasa(config)# power-supply dual
```

pppoe client route distance

To configure an administrative distance for routes learned through PPPoE, use the **pppoe client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

pppoe client route distance *distance*
no pppoe client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through PPPoE. Valid values are from 1 to 255.

Command Default

Routes learned through PPPoE are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client route distance** command is checked only when a route is learned from PPPoE. If the **pppoe client route distance** command is entered after a route is learned from PPPoE, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enablgin PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client route track

To configure the PPPoE client to associate added routes with a specified tracked object number, use the **pppoe client route track** command in interface configuration mode. To remove the PPPoE route tracking, use the **no** form of this command.

pppoe client route track *number*
no pppoe client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client route track** command is checked only when a route is learned from PPPoE. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client secondary

To configure the PPPoE client to register as a client of a tracked object and to be brought up or down based on the tracking state, use the **pppoe client secondary** command in interface configuration mode. To remove the client registration, use the **no** form of this command.

pppoe client secondary track *number*
no pppoe client secondary track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client secondary** command is checked only when PPPoE session starts. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.

prc-interval

To customize IS-IS throttling of partial route calculations (PRC), use the **prc-interval** command in router isis configuration mode. To restore default values, use the **no** form of this command.

prc-interval *prc-max-wait* [*prc-initial-wait prc-second-wait*]
no prc-interval

Syntax Description

prc-max-wait	Indicates the maximum interval between two consecutive PRC calculations. The range is 1 to 120 seconds.
prc-initial-wait	(Optional) Indicates the initial PRC calculation delay after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.
prc-second-wait	(Optional) Indicates the hold time between the first and second PRC calculation (in milliseconds). The range is 1 to 120,000 milliseconds.

Command Default

The default are:

prc-max-wait: 5 seconds

prc-initial-wait: 2000 milliseconds

prc-second-wait: 5000 milliseconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

PRC is the software process of calculating routes without performing a shortest path first (SPF) calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the Routing Information Base (RIB).

The following description helps in determining whether to change the default values of this command:

- The *prc-initial-wait* argument indicates the initial wait time (in milliseconds) before generating the first LSP.
- The *prc-second-wait* argument indicates the amount of time to wait (in milliseconds) between the first and second LSP generation.

- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *prc-max-wait* interval specified, so this value causes the throttling or slowing down of the PRC calculation after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for two times the *prc-max-wait* interval, fast behavior is restored (the initial wait time).

Examples

The following example intervals for PRC.

```
ciscoasa(config)# router isis
ciscoasa(config-router)# prc-interval 2 50 100
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.

Command	Description
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.

Command	Description
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

pr - pz

pre-fill-username

To enable extracting a username from a client certificate for use in authentication and authorization, use the **pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

pre-fill-username { **client** | **clientless** }
no pre-fill-username

Syntax Description

client	Enables this feature for AnyConnect VPN client connections. Use the **client** keyword in 9.8(1)+.
ssl-client	
clientless	Enables this feature for clientless connections.

Command Default

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.8(1)	The **ssl-client** keyword was changed to **client**.

Usage Guidelines

The **pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **username-from-certificate** command as the username for username/password authentication and authorization. To use this pre-fill username from certificate feature, you must configure both commands.

To enable this feature, you must also configure the **username-from-certificate** command in tunnel-group general-attributes mode.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the name for an authentication or authorization query for an SSL VPN client must be derived from a digital certificate:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

preempt

To cause the failover group to become active on the preferred unit, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]
no preempt [*delay*]

Syntax Description

seconds The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Command Default

By default, there is no delay.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Earlier software versions allowed "simultaneous" boot up so that the failover groups did not require the **preempt** command to become active on the preferred unit. However, this functionality has now changed so that both failover groups become active on the first unit to boot up.

Usage Guidelines

Assigning a **primary** or **secondary** preference to a failover group specifies which unit the failover group becomes active on when you set the **preempt** command. Both failover groups become active on the first unit that boots up (even if it seems like they boot simultaneously, one unit becomes active first), despite the **primary** or **secondary** setting for the group. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Note If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured

with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

The OSPFv2, EIGRP and BGP protocols all use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

prefix-list*prefix-list-name* [**seq***seq_num*] { **permit** | **deny** } *network*/*len* [**ge***min_value*] [**le***max_value*]
no prefix-list *prefix-list-name* [**seq** *seq_num*] { **permit** | **deny** } *network* / *len* [**ge** *min_value*] [**le** *max_value*]

Syntax Description

/	A required separator between the *network* and *len* values.
deny	Denies access for a matching condition.
ge *min_value*	(Optional) Specifies the minimum prefix length to be matched. The value of the *min_value* argument must be greater than the value of the *len* argument and less than or equal to the *max_value* argument, if present.
le *max_value*	(Optional) Specifies the maximum prefix length to be matched. The value of the *max_value* argument must be greater than or equal to the value of the *min_value* argument, if present, or greater than the value of the *len* argument if the *min_value* argument is not present.
len	The length of the network mask. Valid values are from 0 to 32.
network	The network address.
permit	Permits access for a matching condition.
prefix-list-name	The name of the prefix list. The prefix-list name cannot contain spaces.
seq *seq_num*	(Optional) Applies the specified sequence number to the prefix list being created.

Command Default

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Release	Modification
9.2(1)	Support for BGP was added.

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The ASA begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a mach is made, the ASA does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network*/*len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified.The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

len < *min_value* <= *max_value* <= 32

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix10.0.0.0/8:

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list*prefix-list-name***description***text*
no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

prefix-list-name	The name of a prefix list.
text	The text of the prefix list description. You can enter a maximum of 80 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Command Default

Prefix list sequence numbering is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Only the **no** form of this command appears in the configuration. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples

The following example disables prefix list sequence numbering:

```
ciscoasa(config)# no prefix-list sequence-number
```

Related Commands

Command	Description
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prf

To specify the pseudo-random function (PRF) in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the prf command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the no form of this command:

prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }
no prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

Syntax Description

md5	Specifies the MD5 algorithm.
sha	(Default) Specifies the Secure Hash Algorithm SHA 1.
sha256	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Command Default

The default is **sha** (SHA 1).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **prf** command to select the pseudo-random function used for the construction of keying material for all of the cryptographic algorithms used in the SA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
8.4(2)	The sha256, sha384, and sha512 keywords were added for SHA 2 support.

Examples

The following example enters IKEv2 policy configuration mode and sets the PRF to MD5:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.

primary

To set the preferred unit for a failover group when using the **preempt** command, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary
no primary

Syntax Description

This command has no arguments or keywords.

Command Default

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Earlier software versions allowed "simultaneous" boot up so that the failover groups did not require the **preempt** command to become active on the preferred unit. However, this functionality has now changed so that both failover groups become active on the first unit to boot up.

Usage Guidelines

Assigning a **primary** or **secondary** preference to a failover group specifies which unit the failover group becomes active on when you set the **preempt** command. Both failover groups become active on the first unit that boots up (even if it seems like they boot simultaneously, one unit becomes active first), despite the **primary** or **secondary** setting for the group. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
```

```
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
secondary	Gives the secondary unit a higher priority than the primary unit.

priority (class)

To enable QoS priority queuing, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queuing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

Note This command is not supported on the ASA Services Module.

priority
no priority

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

LLQ priority queuing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queuing:

- Standard priority queuing—Standard priority queuing uses an LLQ priority queue on an interface (see the **priority-queue** command), while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop* .To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queuing—Hierarchical priority queuing is used on interfaces on which you enable a traffic shaping queue (the **shape** command). A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queuing:

- Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.
- Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
- For IPsec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
- IPsec-over-TCP is not supported for priority traffic classification.

Configuring QoS with Modular Policy Framework

To enable priority queuing, use the Modular Policy Framework. You can use standard priority queuing or hierarchical priority queuing.

For standard priority queuing, perform the following tasks:

1.class-map—Identify the traffic on which you want to perform priority queuing.

2.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.priority**—Enable priority queuing for the class map.

3.service-policy—Assigns the policy map to an interface or globally.

For hierarchical priority-queuing, perform the following tasks:

1.class-map—Identify the traffic on which you want to perform priority queuing.

2.policy-map (for priority queuing)—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.priority**—Enable priority queuing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.

3.policy-map (for traffic shaping)—Identify the actions associated with the **class-default** class map.

- **a.class class-default**—Identify the **class-default** class map on which you want to perform actions.
- **b.shape**—Apply traffic shaping to the class map.
- **c.service-policy**—Call the priority queuing policy map in which you configured the **priority** command so you can apply priority queuing to a subset of shaped traffic.

4.service-policy—Assigns the policy map to an interface or globally.

Examples

The following is an example of the **priority** command in policy-map configuration mode:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

Related Commands

class	Specifies a class map to use for traffic classification.

clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

priority (cluster group)

To set the priority of this unit for master unit elections in an ASA cluster, use the **priority** command in cluster group configuration mode. To remove the priority, use the **no** form of this command.

priority *priority_number*
no priority [*priority_number*]

Syntax Description

priority_number	Sets the priority of this unit for master unit elections, between 1 and 100, where 1 is the highest priority.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Members of the cluster communicate over the cluster control link to elect a master unit, as follows:

1. When you enable clustering for a unit (or when it first starts up with clustering already enabled), it broadcasts an election request every 3 seconds.

2. Any other units with a higher priority respond to the election request; the priority is set between 1 and 100, where 1 is the highest priority.

3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes master.

Note If multiple units tie for the highest priority, the cluster unit name, and then the serial number is used to determine the master.

4. If a unit later joins the cluster with a higher priority, it does not automatically become the master unit; the existing master unit always remains as the master unless it stops responding, at which point a new master unit is elected.

Note You can manually force a unit to become the master using the **cluster master unit** command. For centralized features, if you force a master unit change, then all connections are dropped, and you have to re-establish the connections on the new master unit. See the configuration guide for a list of centralized features.

Examples

The following example sets the priority to 1 (the highest):

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables conn ection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the ma ximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

priority (vpn load balancing)

To set the priority of the local device participating in the virtual load-balancing cluster, use the **priority** command in VPN load-balancing mode. To revert to the default priority specification, use the **no** form of this command.

priority *priority*
no priority

Syntax Description

priority	The priority, in the range of 1 to 10, that you want to assign to this device.

Command Default

The default priority depends on the model number of the device:

Model Number	Default Priority
5520	5
5540	7

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
VPN load-balancing	—	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

This command sets the priority of the local device participating in the virtual load-balancing cluster.

The priority must be an integer in the range of 1 (lowest) to 10 (highest).

The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster. See CLI configuration guide for details about the master-election process.

The **no** form of the command reverts the priority specification to the default value.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **priority** command that sets the priority of the current device to 9:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

Note This command is not supported on ASA 5580 Ten Gigabit Ethernet interfaces. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.) This command is also not supported for the ASA 5512-X through ASA 5555-X Management interface.This command is not supported on the ASA Services Module.

priority-queue *interface-name*
no priority-queue *interface-name*

Syntax Description

interface-name	Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505 or ASASM, the name of the VLAN interface.

Command Default

By default, priority queuing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(3)/8.4(1)	Support for Ten Gigabit Ethernet interfaces was added for the ASA 5585-X.

Usage Guidelines

LLQ priority queuing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queuing:

- Standard priority queuing—Standard priority queuing uses an LLQ priority queue on an interface that yopu create using the **priority-queue** command, while all other traffic goes into the “best effort” queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop* . To avoid having the queue fill up, you can increase the queue buffer size (the **queue-limit** command). You can also fine-tune the maximum number of packets allowed into the transmit queue (the **tx-ring-limit** command). These options

let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.

- Hierarchical priority queuing—Hierarchical priority queuing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used.

Note On the ASA 5505 only, configuring a priority queue on one interface overwrites the same configuration on all other interfaces; only the last applied configuration is present on all interfaces. Also, if the priority queue configuration is removed from one interface, it is removed from all interfaces. To work around this issue, configure the priority-queue command on only one interface. If different interfaces need different settings for the queue-limit and/or tx-ring-limit commands, use the largest of all queue limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

Related Commands

Command	Description
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure priority-queue	Removes the current priority queue configuration.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.

privilege

To configure command privilege levels for use with command authorization (local, RADIUS, and LDAP (mapped) only), use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*
no privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege only for the clear form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
command *command*	Specifies the command you are configuring. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately.
configure	(Optional) Sets the privilege only for the configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
level *level*	Specifies the privilege level; valid values are from 0 to 15. Lower privilege level numbers are lower privilege levels.
mode *cli_mode*	(Optional) If a command can be entered in multiple CLI modes, such as user EXEC/privileged EXEC mode, global configuration mode, or a command configuration mode, then you can set the privilege level for these modes separately. If you do not specify the mode, then all versions of the command use the same level. See the following modes: • **exec**—Specifies both user EXEC mode and privileged EXEC mode. • **configure**—Specifies global configuration mode, accessed using the **configure terminal** command. • *command_config_mode* —Specifies a command configuration mode, accessed using the command name in global or another command configuration mode. For example, the **mac-address** command can be entered in both global and interface configuration mode. The mode keyword lets you set the level separately for each mode. You cannot use this command to set the level for a command
show	(Optional) Sets the privilege only for the show form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.

Command Default

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**
- **enable**

- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

To view all privilege levels, see the **show running-config all privilege all** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	Support for RADIUS users with Cisco VSA CVPN3000-Privilege-Level was added. LDAP users are supported if you map the LDAP attribute to the CVPN3000-Privilege-Level using the **ldap map-attributes** command.

Usage Guidelines

The **privilege** command lets you set privilege levels for ASA commands when you configure the **aaa authorization command LOCAL** command. Even though the command uses the **LOCAL** keyword, this keyword enables local, RADIUS, and LDAP (mapped) authorization.

Examples

For example, the **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. For example, set each form separately as follows:

```
ciscoasa(config)# privilege
 show
 level
 5
 command
 filter
ciscoasa(config)# privilege
 clear
 level
 10
 command
 filter
ciscoasa(config)# privilege
 cmd
 level
 10
 command
 filter
```

Alternatively, you can set all filter commands to the same level:

```
ciscoasa(config)# privilege
 level
 5
 command
 filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level.

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

The following example shows the **mac-address** command in two modes, and different levels for show, clear, and cmd versions :

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

Related Commands

Command	Description
clear configure privilege	Removes privilege command statements from the configuration.
show curpriv	Displays current privilege level.
show running-config privilege	Displays privilege levels for commands.

profile

To create or edit a call-home profile, use the **profile** command in call-home configuration mode. To remove one or all of the configured call-home profiles, use the **no** form of this command specifying one or all of the profiles. You can access the call-home configuration mode by first entering the **call-home** command.

profile *profile-name*
no profile { *profile-name* | **all** }

Syntax Description

profile-name	Name of the profile, up to 20 characters long.
all	Includes all configured profiles.

Command Default

A default profile, **Cisco TAC**, has been provided. The default profile has a predefined set of groups (diagnostic, environment, inventory, configuration, and telemetry) to monitor and predefined destination e-mail and HTTPS URLs. The default profile is created automatically when you initially configure Smart Call Home. The destination e-mail is callhome@cisco.com and the destination URL is https://tools.cisco.com/its/service/oddce/services/DDCEService.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
call-home configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	We introduced this command.
8.2(2)	Added the keyword all.
9.3(2)	We added the **License** profile for Smart Software Licensing.
9.6(2)	Introduced the reference-identity option for **destination address http**.

Usage Guidelines

The following commands are used in profile configuration mode.

Enable or Disable a Profile

To enable a call-home profile, use the **active** command in call-home-profile configuration mode. To disable a call-home profile, use the **no active** command in call-home-profile configuration mode. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command. The default is enabled.

active

no active

Set Profile Commands to Default

To set the call home profile settings to their default values use the default command in call-home-profile configuration mode. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** commands. You can also reset call-home configuration mode settings from this mode. Use command help, **default ?**, to determine and reset all call-home profile and general settings.

default {**activedestinationemail-subjectsubscribe-to-alert-group**}

Destination Type, Address and Settings

To set the destination address, reference identity, message format, and transport method for the Smart Call Home message receiver, use the **destination** command in call-home-profile configuration mode. To remove the destination parameters, or reset them to default, use the **no destination** or **default** command.

The default message format is XM, the default message size is 5MB (0 means unlimited), and the default transport method is e-mail. You must specify a previously configured reference identity. This is used to validate the call-home server's certificate when connecting. It applies to http destinations only.

destination address {**e-mail** *e-mail-address***http** *http-url*}
no destination address {**e-mailhttp** [**all**]}
destination address http *http-url* **reference-identity** *ref-id-name*
no destination address http *http-url* **reference-identity** *ref-id-name*
destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
no destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
destination message-size-limit *max-size*
no destination message-size-limit *max-size*
destination preferred-msg-format {**short-textlong-textxml**}
no destination preferred-msg-format {**short-textlong-textxml**}
destination transport-method {**e-mailhttp**}
no destination transport-method {**e-mailhttp**}

Configure E-mail Subject

To set a prefix or suffix on the email subject for call-home email, use the **email-subject** command in call-home-profile configuration mode. To clear these fields use the **no email-subject** command. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command.

email-subject {**appendprepend**} *chars*
no email-subject {**appendprepend**} *chars*

Subscribe to an alert group

To subscribe to an alert group use the s**ubscribe-to-alert-group** command in call-home-profile configuration mode. To clear these subscriptions use the no s**ubscribe-to-alert-group** command. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command.

- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]—Subscribes to events of a group with a specified severity level.alert-group-name: Syslog, diagnostic, environment, or threat are valid values.
- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]—Subscribes to syslogs

with a severity level or message ID.start-[end]: One syslog message ID or a range of syslog message IDs.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to inventory events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to configuration events.full: Configuration to export the running configuration, startup configuration, feature list, number of elements in an access list, and the context name in multimode.minimum: Configuration to export-only feature list, number of elements in an access list, and the context name in multimode.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]—Subscribes to telemetry periodic events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}—Subscribes to snapshot periodic events.minutes: The interval in minutes.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.

Related Commands

Command	Description
call-home	Puts the user into call home configuration mode
show call-home	Displays Call Home configuration information.
reference-identity	Configures a reference identity object.

prompt

To customize the CLI prompt, use the prompt command in global configuration mode. To revert to the default prompt, use the no form of this command.

prompt { [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]
no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

Syntax Description

cluster-unit	Displays the cluster unit name. Each unit in a cluster can have a unique name.
context	(Multiple mode only) Displays the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
priority	Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the **failover lan unit** command.
state	Displays the traffic-passing state or role of the unit. For failover, the following values are displayed for the **state** keyword: • act—Failover is enabled, and the unit is actively passing traffic. • stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. • actNoFailover—Failover is not enabled, and the unit is actively passing traffic. • stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit. For clustering, the following values are displayed for the **state** keyword: • control node • data node For example, if you set **prompt hostname cluster-unit state**, then in the prompt "ciscoasa/cl2/data node>", the hostname is ciscoasa, the unit name is cl2, and the state name is data node.

Command Default

The default prompt is the hostname. In multiple context mode, the hostname is followed by the current context name (*hostname* /*context*).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	The **cluster-unit** option was added. The **state** keyword was updated for clustering.
9.19(1)	For clustering, the **state** display was changed from **master** and **slave** to **control node** and **data node**.

Usage Guidelines

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/).

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

The ability to add information to a prompt allows you to see at-a-glance which ASA you are logged into when you have multiple modules. During a failover, this feature is useful when both ASAs have the same hostname.

Examples

The following example shows all available elements in the prompt available for failover:

```
ciscoasa(config)# prompt hostname context slot state priority
```

The prompt changes to the following string:

```
ciscoasa/admin/pri/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

propagate sgt

To enable propagation of a security group tag (called **sgt**) on an interface, use the **propagate sgt** command in cts manual interface configuration mode. To disable propagation of a security group tag (called **sgt**) on an interface, use the **no** form of this command.

propagate sgt
no propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

Propagation is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cts manual interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command enables and disables the propagation of a security group tag in CTS Layer 2 SGT Imposition.

Restrictions

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI, TVI, and VNI.

Examples

The following example enables an interface for Layer 2 SGT imposition and indicates that the SGT is not being propagated:

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

Related Commands

Command	Description
cts manual	Enables Layer 2 SGT Imposition and enters cts manual interface configuration mode.

Command	Description
policy static sgt	Applies a policy to a manually configured CTS link.

protocol

To specify the protocol and encryption types for an IPsec proposal for IKEv2 connections, use the **protocol** command from IPsec proposal configuration mode. To remove the protocol and encryption types, use the no form of the command:

protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }
no protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }

Syntax Description

esp	Specifies the Encapsulating Security Payload (ESP) IPsec protocol (currently the only supported protocol for IPsec).
des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
null	Does not use encryption for ESP.
integrity	Specifies the integrity algorithm for the IPsec protocol.
md5	Specifies the md5 algorithm for the ESP integrity protection.
sha-1	(Default) Specifies the Secure Hash Algorithm (SHA) SHA-1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection.
sha-256	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-384	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-512	Specifies which algorithm to use as an IPsec integrity algorithm.

null	Choose if AES-GCM/GMAC is configured as the encryption algorithm.

Command Default

The default settings for an IPsec proposal are the encryption type 3DES and the integrity type SHA-1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec proposal configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for AES-GCM or AES-GMAC algorithm was added. The ability to choose an algorithm to use as an IPsec integrity algorithm was added.

Usage Guidelines

IKEv2 IPsec proposals can have multiple encryption and integrity types. Use this command to specify the types, which allows the peer to pick and choose as desired.

You must choose the null integrity algorithm if AES-GMC/GMAC is configured as the encryption algorithm.

Examples

The following example creates the IPsec proposal proposal_1, configures the ESP encryption types DES and 3DES, and specifies the crypto algorithms MD5 and SHA-1 for integrity protection:

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

Related Commands

Command	Description
crypto ikev2 enable	Enables ISAKMP IKEv2 negotiation on the interface on which the IPsec peer communicates.
crypto ipsec ikev2 ipsec-proposal	Creates an IPsec proposal and enters IPsec proposal configuration mode where you specify multiple encryption and integrity types for the proposal.
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.

Command	Description
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

protocol-enforcement

To enable the domain name, label length, and format check, including compression and looped pointer check, use the **protocol-enforcement** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

protocol-enforcement
no protocol-enforcement

Syntax Description

This command has no arguments or keywords.

Command Default

Protocol enforcement is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no protocol-enforcement** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Under certain conditions, protocol enforcement is performed even if the command is disabled. This occurs when parsing a DNS resource record is required for other purposes, such as DNS resource record classification, NAT or TSIG check.

Examples

The following example shows how to enable protocol enforcement in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-enforcement
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in ca-crl configuration mode. To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

protocol http
no protocol http

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit HTTP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you use this command, be sure to assign HTTP rules to the public interface filter. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

Examples

The following example enters ca-crl configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol ldap
no protocol ldap

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit LDAP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the protocol-object command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*
no protocol-object *protocol*

Syntax Description

protocol	Protocol name or number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Protocol configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.

Command	Description
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in crl configure mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol scep
no protocol scep

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit SCEP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

protocol shutdown

To disable the IS-IS protocol so that it cannot form any adjacency on any interface and will clear the IS-IS LSP database, use the **protocol shutdown** command in router isis configuration mode. To reenable the IS-IS protocol, use the **no** form of this command

protocol shutdown
no protocol shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command allows you to disable the IS-IS protocol for a specific routing instance without removing any existing IS-IS configurations parameters. When you enter the **protocol shutdown** command, the IS-IS protocol continues to run on the ASA, and you can use the current IS-IS configuration, but IS-IS does not form any adjacencies on any interface, and it also clears the IS-IS LSP database.

If you want to disable the IS-IS protocol for a specific interface, use the **isis protocol shutdown** command.

Examples

The following example disables the IS-IS protocol for a specific routing instance:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

Related Commands

protocol-violation

To define actions when a protocol violation occurs with HTTP and NetBIOS inspection, use the **protocol-violation** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

protocol-violation action [**drop** [**log**] | **log**]
no protocol-violation action [**drop** [**log**] | **log**]

Syntax Description

drop	Specifies to drop packets that do not conform to the protocol.
log	Specifies to log the protocol violations.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an HTTP or NetBIOS policy map. A syslog is issued when the HTTP or NetBIOS parser cannot detect a valid HTTP or NetBIOS message in the first few bytes of the message. This occurs, for instance, when a chunked encoding is malformed and the message cannot be parsed.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.

Command	Description
show running-config policy-map	Display all current policy map configurations.

proxy-auth

To flag the tunnel group as a specific proxy authentication tunnel group, use the **proxy-auth** command in webvpn configuration mode.

proxy-auth [**sdi**]

Syntax Description

sdi	Parses RADIUS/TACACS SDI proxy messages into native SDI directives.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Use the **proxy-auth** command for enabling the parsing of aaa-server proxy authentication text messages into native protocol directives.

proxy-auth_map sdi

To map RADIUS challenge messages returned from a RADIUS proxy server to native SDI messages, use the **proxy-auth_map sdi** command in aaa-server configuration mode.

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

Syntax Description

radius_challenge_message	Specifies the RADIUS challenge messages that are used to map specific SDI messages, which can any of the following: • new-pin-meth—New PIN Method, [default] Do you want to enter your own pin • new-pin-reenter—Reenter new PIN, [default] Reenter PIN: • new-pin-req—New PIN requested, [default] Enter your new Alpha-Numerical PIN • new-pin-sup—New PIN supplied, [default] Please remember your new PIN • new-pin-sys-ok—New PIN accepted, [default] New PIN Accepted • next-ccode-and-reauth—Reauthenticate on token change, [default] new PIN with the next card code • next-code—Provide the tokencode without PIN, [default] Enter Next PASSCODE • ready-for-sys-pin—Accept system generated PIN, [default] ACCEPT A SYSTEM GENERATED PIN
sdi_message	Specifies the native SDI messages.

Command Default

The default mapping on the ASA corresponds to default settings on the Cisco ACS (including the system administration, configuration, and RSA SecureID prompts), which also synchronizes with default settings on the RSA Authentication Manager.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

To enable parsing and mapping of RADIUS challenge messages from a RADIUS proxy, you must enable the **proxy-auth** command in tunnel-group configuration mode. Then default mapping values are used. You can change the default mapping values using the **proxy-auth_map** command.

A remote user connects to the ASA with the Secure Client and tries to authenticate using an RSA SecurID token. The ASA can be configured to use a RADIUS proxy server which in turn, communicates with the SDI server about that authentication.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server than when the ASA is communicating through the RADIUS proxy.

Therefore, to appear as a native SDI server to the Secure Client, the ASA must interpret the messages from the RADIUS server. Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The Secure Client might fail to respond, and authentication might fail.

Related Commands

Command	Description
proxy-auth	Enables parsing and mapping of RADIUS challenge messages from a RADIUS proxy.

proxy-bypass

To configure the ASA to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML—use the **proxy-bypass** command in webvpn configuration mode. To disable proxy bypass, use the **no** form of the command.

proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }
no proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }

Syntax Description

host	Identifies the host to forward traffic to. Use either the host IP address or a hostname.
interface	Identifies the ASA interface for proxy bypass.
interface name	Specifies an ASA interface by name.
link	Specifies rewriting of absolute external links.
none	Specifies no rewriting.
path-mask	Specifies the pattern to match.
path-mask	Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 128 bytes.
port	Identifies the port reserved for proxy bypass.
port number	Specifies a high numbered port reserved for proxy bypass. The port range is 20000-21000. You can use a port for one proxy bypass rule only.
rewrite	(Optional) Specifies the additional rules for rewriting: none or a combination of XML and links.
target	Identifies the remote server to forward the traffic to.
url	Enter the URL in the format **http(s)://***fully_qualified_domain_name*[:*port*]. Maximum 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
xml	Specifies rewriting XML content.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
WebVPN configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Use proxy bypass for applications and web resources that work better with minimum content rewriting. The proxy-bypass command determines how to treat specific web applications that travel through the ASA.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.example.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.example.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

Examples

The following example shows how to configure the ASA to use port 20001 for proxy bypass over the webvpn interface, using HTTP and its default port 80, to forward traffic to example.com and to rewrite XML content.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

The next example shows how to configure the ASA to use the path mask mypath/* for proxy bypass on the outside interface, using HTTP and its default port 443 to forward traffic to example.com, and to rewrite XML and link content.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
rewrite	Determines whether traffic travels through the ASA.

proxy-ldc-issuer

To issue TLS proxy local dynamic certificates, use the proxy-ldc-issuer command in crypto ca trustpoint configuration mode. To remove the configuration, use the **no** form of this command.

proxy-ldc-issuer
no proxy-ldc-issuer

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the proxy-ldc-issuer command to issue TLS proxy local dynamic certificates. The proxy-ldc-issuer command grants a crypto trustpoint the role as local CA to issue the LDC and can be accessed from crypto ca trustpoint configuration mode.

The proxy-ldc-issuer command defines the local CA role for the trustpoint to issue dynamic certificates for TLS proxy. This command can only be configured under a trustpoint with “enrollment self.”

Examples

The following example shows how to create an internal local CA to sign the LDC for phones. This local CA is created as a regular self-signed trustpoint with proxy-ldc-issuer enabled.

```
ciscoasa(config)# crypto ca trustpoint ldc_server
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.

Commands	Description
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

proxy paired

To set the VNI interface to paired proxy mode for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **proxy paired** command in interface configuration mode. To remove the proxy, use the **no** form of this command.

proxy paired
no proxy paired

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.

Command	Description
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

proxy-server (Deprecated)

To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, use the **proxy-server** command in phone-proxy configuration mode. To remove the HTTP proxy configuration from the Phone Proxy, use the **no** form of this command.

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*
no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

Syntax Description

interface *ifc*	Specifies the interface on which the HTTP proxy resides on the ASA.
ip_address	Specifies the IP address of the HTTP proxy.
listen_port	Specifies the listening port of the HTTP proxy. If not specified, the default will be 8080.

Command Default

If the listen port is not specified, the port is configured to be 8080 by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.

The *ip_address* you enter should be the global IP address based on where the IP phone and HTTP proxy server is located.

If the proxy server is located in a DMZ and the IP phones are located outside the network, the ASA does a lookup to see if there is a NAT rule and uses the global IP address to write into the configuration file.

You can enter a hostname in the *ip_address* argument when that hostname can be resolved to an IP address by the ASA (for example, DNS lookup is configured) because the ASA will resolve the hostname to an IP address.

By default, the Phone URL Parameters configured under the Enterprise Parameters use an FQDN in the URLs. The parameters might need to be changed to use an IP address if the DNS lookup for the HTTP proxy does not resolve the FQDNs.

To make sure the proxy server URL was written correctly to the IP phones configuration files, check the URL on an IP phone under Settings > Device Configuration > HTTP configuration >Proxy Server URL.

The Phone Proxy does not inspect this HTTP traffic to the proxy server.

If the ASA is in the path of the IP phone and the HTTP proxy server, use existing debugging techniques (such as syslogs and captures) to troubleshoot the proxy server.

You can configure only one proxy server while the Phone Proxy is in use; however, if the IP phones have already downloaded their configuration files after you have configured the proxy server, you must restart the IP phones so that they get the configuration file with the proxy server's address in the file.

Examples

The following example shows the use of the **proxy-server** command to configure the HTTP proxy server for the Phone Proxy:

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

proxy single-arm

To enable single-arm proxy for a VXLAN VNI interface, use the **proxy single-arm** command in interface configuration mode. To disable the proxy, use the **no** form of this command.

proxy single-arm
no proxy single-arm

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
9.17(1)	We added this command.

Usage Guidelines

The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The ASA virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint). This use case requires you to configure the VNI interface as a single-arm proxy. Be sure to also enable **same-security-traffic permit intra-interface** to allow traffic to u-turn out the VTEP source interface.

Examples

The following example configures the VNI interface as a single-arm proxy:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.

Command	Description
encapsulation geneve	Sets the NVE instance to Geneve encapsulation.
interface vni	Creates the VNI interface for VXLAN tagging.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.

ptp domain

To specify the domain number of all PTP ports on the ISA 3000, use the **ptp domain** command in privileged EXEC or global configuration mode. The domain number ranges from 0 to 255; the default value is 0. Packets received on a domain different from the configured domain will be treated like regular multicast packets and will not undergo any PTP processing. To reset the domain number to 0, the default value, use the **no** form of this command.

ptp domain *domain_num*
no ptp domain

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

domain *domain_num*	Specifies the domain number for all PTP-enabled ports on the ISA 3000.

Command Default

The default **ptp domain** number is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The **ptp domain** command is also available in global configuration mode.

Examples

The following example shows the use of the **ptp domain** command to set the PTP domain number to 127:

```
ciscoasa# ptp domain 127
```

Related Commands

Command	Description
show ptp port	Displays PTP interface/port information.

ptp enable

To enable PTP on an interface on the ISA 3000, use the **ptp enable** command in interface configuration mode. The mode in which PTP will be enabled is specified with the **ptp mode** command. To disable PTP on an interface, use the **no** form of this command. PTP packets coming into and going out of the interface will then be treated like regular multicast packets.

ptp enable
no ptp enable

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

This command has no arguments or keywords.

Command Default

PTP is enabled on all ISA 3000 interfaces in transparent mode by default. In routed mode, you must add the necessary configuration to ensure that the PTP packets are allowed to flow through the device.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

This command is entered in interface configuration mode only.

This command is allowed only on physical interfaces. It is not allowed on sub-interfaces, other virtual interfaces, or the management interface.

PTP flows on VLAN sub-interfaces are supported, assuming the appropriate PTP configuration is present on the parent interface.

If PTP is not enabled in any mode, this command will be accepted, but will have no effect. A warning will be issued.

Related Commands

Command	Description
show ptp clock	Displays PTP clock properties.

ptp mode

To specify the PTP clock mode on the ISA 3000, use the **ptp mode** command in privileged EXEC or global configuration mode. To disable PTP on all interfaces, use the **no** form of this command.

ptp mode e2etransparent
no ptp mode

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

e2etranparent	Enables End to End Transparent mode on all PTP-enabled interfaces on the ISA 3000.

Command Default

End to End Transparent mode is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

When End to End Transparent mode is disabled, all PTP packets are treated like any other multicast packets. This is equivalent to forward mode.

The **ptp mode** command is also available in global configuration mode.

Examples

The following example shows the use of the **ptp mode** command to set the PTP clock mode to End to End Transparent:

```
ciscoasa# ptp mode e2etranparent
```

Related Commands

Command	Description
show ptp internal-info	Displays PTP statistics and counter information.

public-key

To specify the DNSCrypt provider public key for certificate verification required by Cisco Umbrella, use the **public-key** command in Umbrella configuration mode. Use the **no** form of this command to remove the key and use the default key.

public-key *dnscrypt_key*
no public-key [*dnscrypt_key*]

Syntax Description

dnscrypt_key	The public key used by the Cisco Umbella server for DNSCrypt. This key is relevant only if you enable dnscrypt in the DNS inspection policy map used for Cisco Umbrella. The key is a 32-byte hexadecimal value. Enter the hex value in ASCII with a colon separator for every 2 bytes. The key is 79 bytes long. Obtain this key from Cisco Umbrella.

Command Default

The default key is used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Umbrella configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

If you intend to enable DNSCrypt in the DNS inspection policy map, you can optionally configure the DNSCrypt provider public key for certificate verification. If you do not configure the key, the default currently distributed public key is used for validation.

Configuring a key is necessary only if Cisco Umbrella changes the public key it uses for DNSCrypt encryption.

Examples

The following example configures a public key for use with Cisco Umbrella. The example also shows how to enable DNSCrypt in the default DNS inspection policy map, which is used in global DNS inspection.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
```

```
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
dnscrypt	Enables DNScrypt encryption for the connection between the device and Cisco Umbrella.
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
token	Identifies the API token that is needed to register with Cisco Umbrella.
umbrella-global	Configures the Cisco Umbrella global parameters.

publish-crl

To allow other ASAs to validate the revocation status of certificates issued by the local CA, use the **publish-crl** command in ca-server configuration mode to allow downloading of the CRL directly from and interface on the ASA. To make the CRL unavailable for downloading, use the **no** form of this command.

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

Syntax Description

interface *interface*	Specifies the *nameif* used for the interface, such as gigabitethernet0/1. See the interface command for details.
port *portnumber*	(Optional) Specifies the port on which the interface device expects to download the CRL. Port numbers can be in the range of 1-65535.

Command Default

The default **publish-crl** status is **no publish**. TCP port 80 is the default for HTTP.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The CRL is inaccessible by default. You must enable access to the CRL file on the interface and port required.

TCP port 80 is the HTTP default port number. If you configure a non-default port (other than port 80), be sure the **cdp-url** configuration includes the new port number so other devices know to access this specific port.

The CRL Distribution Point (CDP) is the location of the CRL on the local CA ASA. The URL you configure with the **cdp-url** command is embedded into any issued certificates. If you do not configure a specific location for the CDP, the default CDP URL is: http://hostname.domain/+CSCOCA+/asa_ca.crl.

An HTTP redirect and a CRL download request are handled by the same HTTP listener, if Clientless SSL VPN is enabled on the same interface. The listener checks for the incoming URL and if it matches the one configured with the **cdp-url** command, the CRL file downloads. If the URL does not match the **cdp-url** command, the connection is redirected to HTTPS (if HTTP redirect is enabled).

Examples

The **publish-crl** command example, entered in ca-server configuration mode, enables port 70 of the outside interface for CRL download:

```
ciscoasa(config)# crypto ca server
```

```
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies a particular location for the automatically generated CRL.
show interface	Displays the runtime status and statistics of interfaces.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Command Default

The root directory (/) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0	This command was added.

Usage Guidelines

This command is similar in functionality to the **dir** command.

Examples

The following example shows how to display the current working directory:

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
more	Displays the contents of a file.

q - res

queue-limit (priority-queue)

To specify the depth of the priority queues, use the **queue-limit** command in priority-queue configuration mode. To remove this specification, use the **no** form of this command.

Note This command is not supported on ASA 5580 Ten Gigabit Ethernet interfaces. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.) This command is also not supported for the ASA 5512-X through ASA 5555-X Management interface.This command is not supported on the ASA Services Module.

queue-limit *number-of-packets*
no queue-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets that can be queued (that is, buffered) before the interface begins dropping packets. The upper limit of the range of values is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device. The queues must not exceed the available memory. The theoretical maximum number of packets is 2147483647.

Command Default

The default queue limit is 1024 packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Priority-queue configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The ASA recognizes priority traffic and enforces appropriate quality of service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.

Note You *must* configure the **priority-queue** command in order to enable priority queueing for the interface.

You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue configuration mode, as shown by the prompt. In priority-queue configuration mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best -effort) allowed to be buffered before dropping packets (**queue-limit** command).

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop* . To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 234 packets and a transmit queue limit of 3 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.

queue-limit (tcp-map)

To configure the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, use the **queue-limit** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

queue-limit *pkt_num* **timeout** *seconds*
no queue-limit

Syntax Description

pkt_num	Specifies the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, between 1 and 250. The default is 0, which means this setting is disabled and the default system queue limit is used depending on the type of traffic. See the "Usage Guidelines" section for more information.
timeout *seconds*	(Optional) Sets the maximum amount of time that out-of-order packets can remain in the buffer, between 1 and 20 seconds. The default is 4 seconds. If packets are not put in order and passed on within the timeout period, then they are dropped. You cannot change the timeout for any traffic if the *pkt_num* argument is set to 0; you need to set the limit to be 1 or above for the **timeout** keyword to take effect.

Command Default

The default setting is 0, which means this command is disabled.

The default timeout is 4 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)/8.0(4)	The **timeout** keyword was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1.tcp-map—Identifies the TCP normalization actions.

- **a.queue-limit**—In tcp-map configuration mode, you can enter the **queue-limit** command and many others.

2.class-map—Identify the traffic on which you want to perform TCP normalization.

3.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.set connection advanced-options**—Identify the tcp-map you created.

4.service-policy—Assigns the policy map to an interface or globally.

If you do not enable TCP normalization, or if the **queue-limit** command is set to the default of 0, which means it is disabled, then the default system queue limit is used depending on the type of traffic:

- Connections for application inspection (the **inspect** command), IPS (the **ips** command), and TCP check-retransmission (the TCP map **check-retransmission** command) have a queue limit of 3 packets. If the ASA receives a TCP packet with a different window size, then the queue limit is dynamically changed to match the advertised setting.
- For other TCP connections, out-of-order packets are passed through untouched.

If you set the **queue-limit** command to be 1 or above, then the number of out-of-order packets allowed for all TCP traffic matches this setting. For example, for application inspection, IPS, and TCP check-retransmission traffic, any advertised settings from TCP packets are ignored in favor of the **queue-limit** setting. For other TCP traffic, out-of-order packets are now buffered and put in order instead of passed through untouched.

Examples

The following example sets the queue limit to 8 packets and the buffer timeout to 6 seconds for all Telnet connections:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	Identifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

quick-start

To define an action when the Quick-Start (QS) option occurs in a packet header with IP Options inspection, use the **quick-start** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

quick-start action { **allow** | **clear** }
no quick-start action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Quick-Start IP option.
clear	Remove the Quick-Start option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Quick-Start IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# quick-start action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

quit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **quit** command.

quit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **quit** command in privileged or user EXEC modes, you log out from the ASA. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **quit** command to exit global configuration mode, and then logout from the session:

```
ciscoasa(config)# quit
ciscoasa# quit
Logoff
```

The following example shows how to use the **quit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
ciscoasa(config)# quit
ciscoasa# disable
ciscoasa>
```

Related Commands

Command	Description
exit	Exits a configuration mode or logs out from privileged or user EXEC modes.

quota management-session

To set the maximum number of aggregate, per user, and per-protocol administrative sessions that are allowed on the ASA, use the **quota management-session** command in global configuration mode. To set the quota to the default value, use the **no** form of this command.

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*
no quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

Syntax Description

number	Specifies the maximum number of simultaneous ASDM, SSH, and Telnet sessions that are allowed. (9.12 and later) When entered without any other keywords, this argument sets the aggregate number of sessions between 1 and 15. The default is 15. (9.10 and earlier) Valid values are from 0 (unlimited) to 10,000.
ssh	Sets the maximum SSH sessions, between 1 and 5. The default is 5.
telnet	Sets the maximum Telnet sessions, between 1 and 5. The default is 5.
http	Sets the maximum HTTPS (ASDM) sessions, between 1 and 5. The default is 5.
user	Sets the maximum sessions per user, between 1 and 5. The default is 5.

Command Default

(9.12 and later) The aggregate default is 15.

The SSH, Telnet, HTTP, and user defaults are 5.

(9.10 and earlier) The default is 0, which means there is no session limit.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.
9.12(1)	You can now enter this command within a context instead of in the system. You can also now set the per user and per-protocol limits, in addition to the aggregate limit. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15.

Usage Guidelines

When the quota is reached, subsequent management session requests are denied, and a syslog message is generated. The console session is never blocked by the management session quota mechanism to prevent device lockout.

Note In multiple context mode, you cannot configure the number of ASDM sessions, where the maximum is fixed at 5 sessions.

Note If you also set a resource limit per context for the maximum administrative sessions (SSH, etc.) using the **limit-resource** command, then the lower value will be used.

Examples

The following example configures the aggregate management session quota to 8, and the individual session limits to various quantities:

```
ciscoasa
(config)#
quota management-session 8
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

Related Commands

Command	Description
show run quota management-session	Displays the current value of the management-session quota.
show quota management-session	Displays statistics for management sessions.

radius-common-pw

To specify a common password to be used for all users who are accessing a RADIUS authorization server through the ASA, use the **radius-common-pw** command in aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

radius-common-pw *string*
no radius-common-pw

Syntax Description

string	A case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server host	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for RADIUS authorization servers.

The RADIUS authorization server requires a password and username for each connecting user. The ASA provides the username automatically. You enter the password here. The RADIUS server administrator must configure the RADIUS server to associate this password with each user authorizing to the server via this ASA. Be sure to provide this information to your RADIUS server administrator.

If you do not specify a common user password, each user password is the username. If you are using usernames for common user passwords, as a security precaution, do not use the RADIUS server for authorization anywhere else on your network.

13-125

Note The *string* argument is essentially a space-filler. The RADIUS server expects and requires it, but does not use it. Users do not need to know it.

Examples

The following example configures a RADIUS AAA server group named “svrgrp1” on host “1.2.3.4,” sets the timeout interval to 9 seconds, sets the retry interval to 7 seconds, and configures the RADIUS commnon password as “allauthpw.”

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)#
radius-common-pw allauthpw
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

radius-reject-message

To enable the display of a RADIUS reject message on the login screen when authentication is rejected, use the **radius-eject-message** command from tunnel-group webvpn attributes configuration mode. To remove the command from the configuration, use the **no** form of the command:

radius-reject-message
no radius-reject-message

Command Default

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Enable this command if you want to display to remote users a RADIUS message about an authentication failure.

Examples

The following example enables the display of a RADIUS rejection message for the connection profile named engineering:

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (Deprecated)

Note The last supported release of this command was Version 8.0(1).

To have the ASA use MS-CHAPv2 to negotiate a password update with the user during authentication, use the **radius-with-expiry** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

radius-with-expiry
no radius-with-expiry

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated. The **password-management** command replaces it. The **no** form of the **radius-with-expiry** command is no longer supported.
8.0(2)	This command was deprecated.

Usage Guidelines

You can apply this attribute only to the IPSec remote-access tunnel-group type. The ASA ignores this command if RADIUS authentication has not been configured.

Examples

The following example entered in config-ipsec configuration mode, configures Radius with Expiry for the remote-access tunnel group named remotegrp:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# radius-with-expiry
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
password-management	Enables password management. This command, in the tunnel-group general-attributes configuration mode, replaces the **radius-with-expiry** command.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

raid

To manage the SSDs in a RAID, use the **raid** command in privileged EXEC mode.

Note This command is only supported on the Secure Firewall 3100.

raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	Adds an SSD to the RAID. It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up.
psid	If you add an SSD that was previously used on another system, and is still locked, enter the *psid*. The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.
remove	Removes the SSD from the RAID and keeps the data intact.
remove-secure	Removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD.
local-disk {**1** | **2**}	Specifies the SSD, disk1 or disk2.

Command Default

If you have two SSDs, they form a RAID when you boot up.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

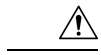
Release	Modification
9.17(1)	This command was introduced for the Secure Firewall 3100.

Usage Guidelines

You can perform the following tasks while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.

- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.



Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Examples

The following example removes disk2 from the RAID and performs a secure erase.

```
ciscoasa# raid remove-secure local-disk 2
```

Related Commands

Command	Description
show raid	Shows the RAID status.
show ssd	Shows the SSD status.

range

To configure a range of addresses for a network object, use the **range** command in object configuration mode. Use the **no** form of this command to remove the object from the configuration.

range *ip_addr_1 ip_addr2*
no range *ip_addr_1 ip_addr2*

Syntax Description

ip_addr_1	Identifies the first IP address in the range, either IPv4 or IPv6.
ip_addr_2	Identifies the last IP address in the range.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.0(1)	We added support for IPv6 addresses.

Usage Guidelines

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a range network object:

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully-qualified domain name network object.
host	Specifies a host network object.

Command	Description
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

ras-rcf-pinholes

To enable call setup between H.323 endpoints when the Gatekeeper is inside the network, use the **ras-rcf-pinholes** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

ras-rcf-pinholes enable
no ras-rcf-pinholes enable

Syntax Description

enable	Enables call setup between H.323 endpoints.

Command Default

By default, this option is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(5)	This command was added.

Usage Guidelines

The ASA includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the ASA opens a pinhole through source IP address/port 0/0.

Examples

The following example shows how to set up an action in a policy map to open pinholes for these calls:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

rate-limit

When using the Modular Policy Framework, limit the rate of messages for packets that match a **match** command or class map by using the **rate-limit** command in match or class configuration mode. This rate limit action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the no form of this command.

rate-limit *rate*
no rate-limit *rate*

Syntax Description

rate	Applies a rate limit to the traffic, 1 - 4294967295. For ESMTP, GTP, RTSP, and SIP, the rate is in packets per second. For SCTP, the rate is in kilobits per second (kbps).

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.5(2)	This command was extended to SCTP inspection, where the rate is in kbps rather than packets per second.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **rate-limit** command to limit the rate of messages.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect sip sip_policy_map** command where sip_policy_map is the name of the inspection policy map.

Examples

The following example limits the invite requests to 100 messages per second:

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(config-pmap-c)# rate-limit 100
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

reactivation-mode

To specify the method by which failed servers in a group are reactivated, use the **reactivation-mode** command in aaa-server protocol mode. To remove this specification, use the **no** form of this command.

reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }
no reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }

Syntax Description

deadtime *minutes*	(Optional) Specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent re-enabling of all servers. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.
depletion	Reactivates failed servers only after all of the servers in the group are inactive.
timed	Reactivates failed servers after 30 seconds of down time.

Command Default

The default reactivation mode is depletion, and the default deadtime value is 10.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server protocol configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Each server group has an attribute that specifies the reactivation policy for its servers.

In **depletion** mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers. When **depletion** mode is in use, you can also specify the **deadtime** parameter. The **deadtime** parameter specifies the amount of time (in minutes) that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. This parameter is meaningful only when the server group is being used in conjunction with the local fallback feature. Additionally, if you also use the group for accounting, where local fallback isn't used, then the deadtime will be canceled. You can avoid this problem by creating a different group (with the same servers) for accounting.

In **timed** mode, failed servers are reactivated after 30 seconds of down time. This is useful when customers use the first server in a server list as the primary server and prefer that it is online whenever possible. This policy breaks down in the case of UDP servers. Since a connection to a UDP server will not fail, even if the

server is not present, UDP servers are put back on line blindly. This could lead to slowed connection times or connection failures if a server list contains multiple servers that are not reachable.

Accounting server groups that have simultaneous accounting enabled are forced to use the **timed** mode. This implies that all servers in a given list are equivalent.

Note This command is ignored for SDI server groups, because SDI server groups contain a single server.

Examples

The following example configures a TACACS+ AAA server named "srvgrp1" to use the depletion reactivation mode, with a deadtime of 15 minutes:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
ciscoasa
(config-aaa-server)#
exit
ciscoasa
(config)#
```

The following example configures a TACACS+ AAA server named "srvgrp1" to use timed reactivation mode:

```
ciscoasa
(config)# aaa-server svrgrp2 protocol tacacs+
ciscoasa
(config-aaa-server)# reactivation-mode timed
ciscoasa
(config-aaa-server)#
```

Related Commands

accounting-mode	Indicates whether accounting messages are sent to a single server or sent to all servers in the group.
aaa-server protocol	Enters aaa-server group configuration mode so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

record-entry

To specify the trustpoints to be used for the creation of the CTL file, use the record-entry command in ctl-file configuration mode. To remove a record entry from a CTL, use the **no** form of this command.

record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]
no record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

Syntax Description

capf	Specifies the role of this trustpoint to be CAPF. Only one CAPF trustpoint can be configured.
cucm	Specifies the role of this trustpoint to be CCM. Multiple CCM trustpoints can be configured.
cucm-tftp	Specifies the role of this trustpoint to be CCM+TFTP. Multiple CCM+TFTP trustpoints can be configured.
domain-name *domain_name*	(Optional) Specifies the domain name of the trustpoint used to create the DNS field for the trustpoint. This is appended to the Common Name field of the Subject DN to create the DNS Name. The domain name should be configured when the FQDN is not configured for the trustpoint.
address *ip_address*	Specifies the IP address of the trustpoint.
tftp	Specifies the role of this trustpoint to be TFTP. Multiple TFTP trustpoints can be configured.
trustpoint *trust_point*	Sets the name of the trustpoint installed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
CTL-file configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.

Usage Guidelines

Only one domain-name can be specified. If the CTL file does not exist, manually export this certificate from CUCM to the ASA.

Use this command only when you have not configured a CTL file for the Phone Proxy. Do not use this command when you have already configured a CTL file.

The IP address you specify in the *ip_address* argument must be the global address or address as seen by the IP phones because it will be the IP address used for the CTL record for the trustpoint.

Add additional record-entry configurations for each entity that is required in the CTL file.

Examples

The following example shows the use of the **record-entry** command to specify the trustpoints to be used for the creation of the CTL file:

```
ciscoasa(config-ctl-file)# record-entry
 cucm-tftp
 trustpoint cucm1 address 192.168.1.2
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

record-route

To define an action when the Record Route (RR) option occurs in a packet header with IP Options inspection, use the **record-route** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

record-route action { **allow** | **clear** }
no record-route action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Record Route IP option.
clear	Remove the Record Route option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Record Route IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# record-route action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

redirect-fqdn

To enable or disable redirection using a fully qualified domain name in vpn load-balancing mode, use the **redirect-fqdn enable** command in global configuration mode.

redirect-fqdn { **enable** | **disable** }
no redirect-fqdn { **enable** | **disable** }

Note To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

disable	Disables redirection with fully qualified domain names.
enable	Enables redirection with fully qualified domain names.

Command Default

This behavior is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a secondary device.

As a VPN cluster master, this ASA can send a fully qualified domain name (FQDN), using reverse DNS lookup, of a cluster device (another ASA in the cluster), instead of its outside IP address, when redirecting VPN client connections to that cluster device.

All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

To do WebVPN load Balancing using FQDNs rather than IP addresses, you must do the following configuration steps:

1. Enable the use of FQDNs for Load Balancing with the **redirect-fqdn enable** command.
2. Add an entry for each of your ASA outside interfaces into your DNS server, if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup.
3. Enable DNS lookups on your ASA with the command - “dns domain-lookup inside” (or whichever interface has a route to your DNS server).
4. Define your DNS server IP address on the ASA; for example: dns name-server 10.2.3.4 (IP address of your DNS server)

Examples

The following is an example of the **redirect-fqdn** command that disables redirection:

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that enables redirection for a fully qualified domain name, specifies the public interface of the cluster as “test” and the private interface of the cluster as “foo”:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

redistribute (ipv6 router ospf)

To redistribute IPv6 routes from one OSPFv3 routing domain into OSPFv3 routing domain, use the **redistribute** command in ipv6 router ospf configuration mode. To disable the redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

as-number	Specifies the autonomous system number of the routing process. Valid values range from 1 to 65535.
external	Specifies the OSPFv3 metric routes that are external to a specified autonomous system, but are imported into OSPFv3 as type 1 or type 2 external routes. Valid values are 1 or 2.
include-connected	(Optional) Allows the target protocol to redistribute routes that have been learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
internal	Specifies OSPFv3 metric routes that are internal to a specified autonomous system.
level-1	Specifies that for Intermediate System-to-Intermediate System (IS-IS), the level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that for IS-IS, both level 1 and level 2 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that for IS-IS, level 2 routes are redistributed into other IP routing protocols independently.
map-tag	Specifies the identifier of a configured route map.
match	(Optional) Redistributes routes into other routing domains.
metric *metric_value*	(Optional) Specifies the OSPFv3 default metric value, which ranges from 0 to 16777214.
metric-type *metric_type*	(Optional) Specifies the external link type that is associated with the default route advertised into the OSPFv3 routing domain. It can be either of the following two values: 1 for type 1 external routes or 2 for type 2 external routes.
nssa-external	Specifies routes that are external to the autonomous system, but are imported into OSPFv3 in a not so stubby area (NSSA) for IPv6 as type 1 or type 2 external routes.
process-id	(Optional) Specifies the number that is assigned administratively when the OSPFv3 routing process is enabled.

route-map *map_name*	(Optional) Specifies the name of the route map that is used to filter the routes that are imported from the source routing protocol to the current OSPFv3 routing protocol. If specified but no route maps tags are listed, no routes are imported. If not specified, all routes are redistributed.
source-protocol	Specifies the source protocol from which routes are being redistributed. Valid values can be one of the following: connected, ospf, or static.
tag *tag_value*	(Optional) Specifies the 32-bit decimal value that is attached to each external route. This value is not used by OSPFv3 itself, but may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero is used. Valid values range from 0 to 4294967295.
transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

Command Default

The following are the command defaults:

- **metric** *metric-value*: **0**
- **metric-type** *type-value*: **2**
- **match**: **internal**, **external 1**, **external 2**
- **tag** *tag-value*: **0**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows how to redistribute static routes into the current OSPFv3 process:

```
ciscoasa(config-if)# ipv6
 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.

Command	Description
show running-config ipv6 router	Displays the commands in the router configuration for OSPFv3.

redistribute (router eigrp)

To redistribute routes from one routing domain into the EIGRP routing process, use the **redistribute** command in router eigrp configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*
no redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*

Syntax Description

bandwidth	EIGRP bandwidth metric in Kilobits per second. Valid values are from 1 to 4294967295.
connected	Specifies redistributing a network connected to an interface into the EIGRP routing process.
delay	EIGRP delay metric, in 10 microsecond units. Valid values are from 0 to 4294967295.
external *type*	Specifies the EIGRP metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies EIGRP metric routes that are internal to a specified autonomous system.
load	EIGRP effective bandwidth (loading) metric. Valid values are from 1 to 255, where 255 indicates 100% loaded.
match	(Optional) Specifies the conditions for redistributing routes from OSPF into EIGRP.
metric	(Optional) Specifies the values for the EIGRP metrics of routes redistributed into the EIGRP routing process.
mtu	The MTU of the path. Valid values are from 1 to 65535.
nssa-external *type*	Specifies the EIGRP metric type for routes that are external to an NSSA; valid values are **1** or **2**.
eigrp *pid*	Used to redistribute an EIGRP routing process into the EIGRP routing process. The *pid* specifies the internally used identification parameter for an EIGRP routing process; valid values are from 1 to 65535.
reliability	EIGRP reliability metric. Valid values are from 0 to 255, where 255 indicates 100% reliability.
rip	Specifies redistributing a network from the RIP routing process into the EIGRP routing process.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the EIGRP routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into the EIGRP routing process.

Command Default

The following are the command defaults:

- **match**: **Internal**, **external 1**, **external 2**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router eigrp configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Redistribute for EIGRP IPv6 route was added.

Usage Guidelines

You must specify the **metric** with the redistribute command if you do not have a **default-metric** command in your EIGRP configuration.

Examples

The following example redistributes static and connected routes into the EIGRP routing process:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redistribute (router ospf)

To redistribute routes from one routing domain into an OSPF routing process, use the **redistribute** command in router ospf configuration mode. To remove the redistribution when no options are included, use the **no** form of this command. The **no** form of the command with an option removes only the configuration for that option.

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

Syntax Description

connected	Specifies redistributing a network connected to an interface into an OSPF routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the OSPF routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type *metric_type*	(Optional) The external link type associated with the default route advertised into the OSPF routing domain. It can be either of the following two values: **1** (Type 1 external route) or **2** (Type 2 external route).
nssa-external *type*	Specifies the OSPF metric type for routes that are external to an NSSA; valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the current OSPF routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
rip	Specifies redistributing a network from the RIP routing process into the current OSPF routing process.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the current OSPF routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into an OSPF process.

subnets	(Optional) For redistributing routes into OSPF, scopes the redistribution for the specified protocol. If not used, only classful routes are redistributed.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Command Default

The following are the command defaults:

- **metric** *metric-value*: 0
- **metric-type** *type-value*: **2**
- **match**: **Internal**, **external 1**, **external 2**
- **tag** *tag-value*: 0

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was modified to include the **rip** keyword.
8.0(2)	This command was modified to include the **eigrp** keyword.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows how to redistribute static routes into the current OSPF process:

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

Command	Description
redistribute (RIP)	Redistributes routes into the RIP routing process.
router ospf	Enters router configuration mode.

Command	Description
show running-config router	Displays the commands in the global router configuration.

redistribute (router rip)

To redistribute routes from another routing domain into the RIP routing process, use the **redistribute** command in router rip configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]

Syntax Description

connected	Specifies redistributing a network connected to an interface into the RIP routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the RIP routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from OSPF to RIP.
metric {*metric_value* | **transparent**}	(Optional) Specifies the RIP metric value for the route being redistributed. Valid values for *metric_value* are from 0 to 16. Setting the metric to **transparent** causes the current route metric to be used.
nssa-external *type*	Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the RIP routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the RIP routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into an OSPF process.

Command Default

The following are the command defaults:

- **metric** *metric-value*: 0
- **match**: **Internal**, **external 1**, **external 2**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router rip configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	This command was modified to include the **eigrp** keyword.
9.0(1)	Multiple context mode is supported.

Examples

The following example shows how to redistribute static routes into the current RIP process:

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# redistribute static metric 2
```

Related Commands

Command	Description
redistribute (router eigrp)	Redistributes routes from other routing domains into EIGRP.
redistribute (router ospf)	Redistributes routes from other routing domains into OSPF.
router rip	Enables the RIP routing process and enters router configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redistribute isis

To redistribute IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1, use the **redistribute isis** command in router isis configuration mode. To disable the redistribution, use the **no** form of this command.

redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]
no redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]

Syntax Description

level-1 | level-2	The level from which and to which you are redistributing IS-IS routes.
into	The keyword that separates the level of routes being redistributed from the level into which you are redistributing routes.
distribute-list *list-number*	(Optional) The number of a distribute list that controls the IS-IS redistribution. You may specify either a distribute list or a route map, but not both.
route-map *map-tag*	(Optional) The name of a route map that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

In IS-IS, all areas are stub areas, which means that no routing information is leaked from the backbone (Level 2) into areas (Level 1). Level 1-only routers use default routing to the closest Level 1-Level 2 router in their area. This command lets you redistribute Level 2 IP routes into Level 1 areas. This redistribution enables Level 1-only routers to pick the best path for an IP prefix to get out of the area. This is an IP-only feature, CLNS routing is still stub routing.

For more control and stability you can configure a distribute list or route map to control which Level 2 IP routes can be redistributed into Level 1. This allows large IS-IS-IP networks to use area for better scalability.

Note You must specify the **metric-style wide** command for the **redistribute isis** command to work.

Examples

In the following example, access list 100 controls the redistribution of IS-IS from Level 1 into Level 2:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 distribute-list 100
ciscoasa(config-router)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

In the following example, the route map named match-tag controls the redistribution of IS-IS from Level 1 into Level 2 so that only routes tagged with 110 are redistributed:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
ciscoasa(config-router)# route-map match-tag permit 10
ciscoasa(config-router)# match tag 11
```

Related Commands

redundant-interface

To set which member interface of a redundant interface is active, use the **redundant-interface** command in privileged EXEC mode.

redundant-interface redundant *number* **active-member** *physical_interface*

Syntax Description

active-member *physical_interface*	Sets the active member. See the **interface** command for accepted values. Both member interfaces must be the same physical type.
redundant *number*	Specifies the redundant interface ID, such as **redundant1**.

Command Default

By default, the active interface is the first member interface listed in the configuration, if it is available.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To view which interface is active, enter the following command:

```
ciscoasa# show interface redundant
number
 detail
 | grep Member
```

For example:

```
ciscoasa# show interface redundant1
 detail
 | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

Examples

The following example creates a redundant interface. By default, gigabitethernet 0/0 is active because it is first in the configuration. The redundant-interface command sets gigabitethernet 0/1 as the active interface.

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
member-interface	Assigns a member interface to a redundant interface pair.
show interface	Displays the runtime status and statistics of interfaces.

regex

To create a regular expression to match text, use the **regex** command in global configuration mode. To delete a regular expression, use the **no** form of this command.

regex *name regular_expression*
regex *name* [*regular_expression*]

Syntax Description

name	Specifies the regular expression name, up to 40 characters in length.
regular_expression	Specifies the regular expression up to 100 characters in length. See the "Usage Guidelines" section for a list of metacharacters you can use in the regular expression.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **regex** command can be used for various features that require text matching. For example, you can configure special actions for application inspection using Modular Policy Framework using an *inspection policy map* (see the **policy map type inspect** command). In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map (see the **class-map type regex** command).

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

Note As an optimization, the ASA searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like "http://", be sure to search for "http:/" instead.

Table 7: regex Metacharacters lists the metacharacters that have special meanings.

Table 7: regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp***)**	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*****	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x***}** or **{***x***,}**	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc***]**	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc***]**	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a-c***]**	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **"test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.

Character	Description	Notes
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
\NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Usage Guidelines

To test a regular expression to make sure it matches what you think it will match, enter the **test regex** command.

The regular expression performance impact is determined by two main factors:

- The length of text that needs to be searched for a regular expression match.

The regular expression engine has only a small impact to the ASA performance when the search length is small.

- The number of regular expression chained tables that need to be searched for a regular expression match.

How the Search Length Impacts Performance

When you configure a regular expression search, every byte of the searched text is usually examined against a regular expression database to find a match. The longer the searched text is, the longer the search time will be. Below is a performance test case which illustrates this phenomenon.

- An HTTP transaction includes one 300-byte long GET request and one 3250-byte long response.
- 445 regular expressions for URI search and 34 regular expressions for request body search.
- 55 regular expressions for response body search.

When a policy is configured to search the URI and the body in the HTTP GET request only, the throughput is:

- 420 Mbps when the corresponding regular expression database is not searched.
- 413 Mbps when the corresponding regular expression database is searched (this demonstrates a relatively small overhead of using regular expression).

But when a policy is configured to also search the whole HTTP response body, the throughput drops down to 145 Mbps because of the long response body (3250 bytes) search.

Following is a list of factors that will increase the length of text for a regular expression search:

- A regular expression search is configured on multiple, different protocol fields. For example, in HTTP inspection, if only URI is configured for a regular expression match, then only the URI field is searched for a regular expression match, and the search length is then limited to the URI length. But if additional

protocol fields are also configured for a regular expression match, such as Headers, Body, and so on, then the search length will increase to include the header length and body length.

- The field to be searched is long. For example, if the URI is configured for a regular expression search, then a long URI in a GET request will have a long search length. Also, currently the HTTP body search length is limited by default to 200 bytes. If, however, a policy is configured to search the body, and the body search length is changed to 5000 bytes, then there will be severe impact on the performance because of the long body search.

How the Number of Chained Regular Expression Tables Impact Performance

Currently, all regular expressions that are configured for the same protocol field, such as all regular expressions for URI, are built into a database consisting of one or more regular expression chained tables. The number of tables is determined by the total memory required and the availability of memory at the time the tables are built. A regular expression database will be split into multiple tables under any of the following conditions:

- When the total memory required is greater than 32 MB since the maximum table size is limited to 32 MB.
- When the size of the largest contiguous memory is not sufficient to build a complete regular expression database, then smaller but multiple tables will be built to accommodate all the regular expressions. Note that the degree of memory fragmentation varies depending on many factors that are interrelated and are almost impossible to predict the level of fragmentation.

With multiple chained tables, each table must be searched for regular expression matches and hence the search time increases in proportion to the number of tables that are searched.

Certain types of regular expressions tend to increase the table size significantly. It is prudent to design regular expressions in a way to avoid wildcard and repeating factors if possible. See Table 7: regex Metacharacters for a description of the following metacharacters:

- Regular expressions with wildcard type of specifications:
- Dot (.)
- Various character classes that match any character in a class:
- [^a-z]
- [a-z]
- [abc]]
- Regular expressions with repeating type of specifications:
- *
- +
- {n,}
- Combination of the wild-card and repeating types of regular expressions can increase the table size dramatically, for examples:
- 123.*xyz
- 123.+xyz
- [^a-z]+

- [^a-z]*
- .*123.* (This should not be done because this is equivalent to matching "123").

The following examples illustrate how memory consumptions are different for regular expressions with and without wildcards and repetition.

- Database size for the following 4 regular expressions is 958,464 bytes.

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- Database size for the following 4 regular expressions is only 10240 bytes.

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

A large number of regular expressions will increase the total memory that is needed for the regular expression database and hence increases the probabilities of more tables if memory is fragmented. Following are examples of memory consumptions for different numbers of regular expressions:

- 100 sample URIs: 3,079,168 bytes
- 200 sample URIs: 7,156,224 bytes
- 500 sample URIs: 11,198,971 bytes

Note The maximum number of regular expressions per context is 2048.The **debug menu regex 40 10** command can be used to display how many chained tables there are in each regex database.

Examples

The following example creates two regular expressions for use in an inspection policy map:

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
```

Related Commands

Command	Description
class-map type inspect	Creates ain inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
class-map type regex	Creates a regular expression class map.
test regex	Tests a regular expression.

reload

To reboot and reload the configuration, use the **reload** command in privileged EXEC mode.

reload [**at** *hh* **:** *mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh* **:**] *mm*] [**max-hold-time** [*hh* **:**] *mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

Syntax Description

at *hh*:*mm*	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 hours.
cancel	(Optional) Cancels a scheduled reload.
day	(Optional) Number of the day in the range from 1 to 31.
in [*hh***:**]*mm*]	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must occur within 24 hours.
max-hold-time [*hh***:***mm*	(Optional) Specifies the maximum hold time the ASA waits to notify other subsystems before a shutdown or reboot. After this time elapses, a quick (forced) shutdown/reboot occurs.
month	(Optional) Specifies the name of the month. Enter enough characters to create a unique string for the name of the month. For example, "Ju" is not unique because it could represent June or July, but "Jul" is unique because no other month beginning with those exact three letters.
noconfirm	(Optional) Permits the ASA to reload without user confirmation.
quick	(Optional) Forces a quick reload, without notifying or correctly shutting down all the subsystems.
reason *text*	(Optional) Specifies the reason for the reload, 1 to 255 characters. The reason text is sent to all open IPsec VPN client, terminal, console, Telnet, SSH, and ASDM connections/sessions. **Note** Some applications, like ISAKMP, require additional configuration to send the reason text to IPsec VPN clients. See the VPN CLI Configuration Guide for more information.
save-config	(Optional) Saves the running configuration to memory before shutting down. If you do not enter the **save-config** keyword, any configuration changes that have not been saved will be lost after the reload.
save-show-tech	(Optional) Saves the output of the **show tech** command to a file before the reload occurs.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to add the following new arguments and keywords: *day*, *hh*, *mm*, *month*, **quick**, **save-config**, and *text*.
9.1(3)	The **save-show-tech** keyword was added.

Usage Guidelines

The command lets you reboot the ASA and reload the configuration from flash memory.

By default, the **reload** command is interactive. The ASA first checks whether the configuration has been modified but not saved. If so, the ASA prompts you to save the configuration. In multiple context mode, the ASA prompts for each context with an unsaved configuration. If you specify the **save-config** keyword, the configuration is saved without prompting you. The ASA then prompts you to confirm that you really want to reload the system. Only a response of **y** or pressing the **Enter** key causes a reload. After confirmation, the ASA starts or schedules the reload process, depending on whether you have specified a delay keyword (**in** or **at**).

By default, the reload process operates in "graceful" mode. All registered subsystems are notified when a reboot is about to occur, allowing these subsystems to shut down properly before the reboot. To avoid waiting until for such a shutdown to occur, specify the **max-hold-time** keyword to specify a maximum time to wait. Alternatively, you can use the **quick** keyword to force the reload process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

You can force the **reload** command to operate noninteractively by specifying the **noconfirm** keyword. In this case, the ASA does not check for an unsaved configuration unless you have specified the **save-config** keyword. The ASA does not prompt you for confirmation before rebooting the system. It starts or schedules the reload process immediately, unless you have specified a delay keyword, although you can specify the **max-hold-time** or **quick** keyword to control the behavior or the reload process.

Use the **reload cancel** command to cancel a scheduled reload. You cannot cancel a reload that is already in progress.

Note Configuration changes that are not written to the flash partition are lost after a reload. Before rebooting, enter the **write memory** command to store the current configuration in the flash partition.

Examples

The following example shows how to reboot and reload a configuration:

```
ciscoasa#
reload
```

```
Proceed with ?  [confirm]
 y
Rebooting...
XXX
Bios VX.X
...
```

Related Commands

Command	Description
show reload	Displays the reload status of the ASA.

remote-access threshold session-threshold-exceeded

To set threshold values, use the **remote-access threshold** command in global configuration mode. To remove threshold values, use the **no** version of this command. This command specifies the number of active remote access sessions, at which point the ASA sends traps.

remote-access threshold session-threshold-exceeded *threshold-value*
no **remote-access threshold session-threshold-exceeded**

Syntax Description

threshold-value	Specifies an integer less than or equal to the session limit the ASA supports.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0 (1)	This command was added.

Examples

The following example shows how to set a threshold value of 1500:

```
ciscoasa# remote-access threshold session-threshold-exceeded 1500
```

Related Commands

Command	Description
snmp-server enable trap remote-access	Enables threshold trapping.

rename (class-map)

To rename a class map, enter the **rename** command in class-map configuration mode.

rename *new_name*

Syntax Description

new_name	Specifies the new name of the class map, up to 40 characters in length. The name "class-default" is reserved.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to rename a class map from test to test2:

```
ciscoasa(config)# class-map test
ciscoasa(config-cmap)# rename test2
```

Related Commands

Command	Description
class-map	Creates a class map.

rename (privileged EXEC)

To rename a file or a directory from the source filename to the destination filename, use the **rename** command in privileged EXEC mode.

rename [**/noconfirm**] [**disk0 :** | **disk1 :** | **flash:**] *source-path* [**disk0 :** | **disk1 :** | **flash:**] *destination-path*

Syntax Description

/**noconfirm**	(Optional) Suppresses the confirmation prompt.
destination-path	Specifies the path of the destination file.
disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
source-path	Specifies the path of the source file.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **rename flash: flash:** command prompts you to enter a source and destination filename.

You cannot rename a file or directory across file systems.

For example:

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

Examples

The following example shows how to rename a file named “test” to “test1”:

```
ciscoasa# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

Related Commands

Command	Description
mkdir	Creates a new directory.
rmdir	Removes a directory.
show file	Displays information about the file system.

renewal-reminder

To specify the number of days before user certificate expiration that an initial reminder to re-enroll is sent to certificate owners, use the **renewal-reminder** command in ca server configuration mode. To reset the time to the default of 14 days, use the **no** form of this command.

renewal-reminder *days*
no renewal-reminder

Syntax Description

days	Specifies the time in days before the expiration of an issued certificate that the certificate owner is first reminded to re-enroll. Valid values range from 1 to 90 days.

Command Default

The default value is 14 days.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

There are three reminders in all. An e-mail is sent automatically to the certificate owner for each of the three reminders if an e-mail address is specified in the user database. If no e-mail address exists, a syslog message is generated to alert the administrator of the renewal.

By default, the CA server sends the following three e-mail messages in the specified order before certificate expiration:

1. Certification Enrollment Invitation

2. Reminder: Certification Enrollment Invitation

3. Last Reminder: Certification Enrollment Invitation

The first e-mail is the invitation, the second e-mail is a reminder, and the third e-mail is a final reminder. The default setting for this notification is 14 days, which means that the initial invitation goes out 14 days before certificate expiration, the reminder e-mail goes out 7 days before certificate expiration, and the final reminder e-mail goes out 3 days before certificate expiration.

You can customize the renewal-reminder interval using the **renewal-reminder** *days* command.

Examples

The following example specifies that the ASA send an expiration notice to users 7 days before certificate expiration:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# renewal-reminder 7
ciscoasa
(config-ca-server)
#
```

The following example resets the expiration notice time to the default of 14 days before certificate expiration:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no renewal-reminder
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
lifetime	Specifies the lifetimes of the CA certificate, all issued certificates, and the CRL.
show crypto ca server	Displays the configuration details of the local CA server.

replication http

To enable HTTP connection replication for the failover group, use the **replication http** command in failover group configuration mode. To disable HTTP connection replication, use the **no** form of this command.

replication http
no replication http

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

This command is available for Active/Active failover only. It provides the same functionality as the **failover replication http** command for Active/Standby failover, except for failover groups in Active/Active failover configurations.

Examples

The following example shows a possible configuration for a failover group:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.

Command	Description
failover replication http	Configures stateful failover to replicate HTTP connections.

request-command deny

To disallow specific commands within FTP requests, use the **request-command deny** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the no form of this command.

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }
no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

Syntax Description

appe	Disallows the command that appends to a file.
cdup	Disallows the command that changes to the parent directory of the current working directory.
dele	Disallows the command that deletes a file on the server.
get	Disallows the client command for retrieving a file from the server.
help	Disallows the command that provides help information.
mkd	Disallows the command that makes a directory on the server.
put	Disallows the client command for sending a file to the server.
rmd	Disallows the command that deletes a directory on the server.
rnfr	Disallows the command that specifies rename-from filename.
rnto	Disallows the command that specifies rename-to filename.
site	Disallows the command that is specific to the server system. Usually used for remote administration.
stou	Disallows the command that stores a file using a unique file name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
FTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is used for controlling the commands allowed within FTP requests traversing the ASA when using strict FTP inspection.

Examples

The following example causes the ASA to drop FTP requests containing **stor**, **stou**, or **appe** commands:

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# request-command deny put stou appe
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.

request-data-size

To set the size of the payload in the SLA operation request packets, use the **request-data-size** command in sla monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

request-data-size *bytes*
no request-data-size

Syntax Description

bytes The size, in bytes, of the request packet payload. Valid values are from 0 to 16384. The minimum value depends upon the protocol used. For echo types, the minimum value is 28 bytes. Do not set this value higher than the maximum allowed by the protocol or the PMTU.

Note The ASA adds an 8-byte timestamp to the payload, so the actual payload is *bytes* + 8.

Command Default

The default *bytes* is 28.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
sla monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

For reachability, it may be necessary to increase the default data size to detect PMTU changes between the source and the target. Low PMTU will likely affect session performance and, if detected, may indicate that the secondary path be used.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes and the number of echo requests sent during an SLA operation to 5.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

request-queue

To specify the maximum number of GTP requests that will be queued waiting for a response, use the request-queue command in policy map parameters configuration mode. Use the **no** form of this command to return this number to the default of 200.

request-queue *max_requests*
no request-queue *max_requests*

Syntax Description

max_requests	The maximum number of GTP requests that will be queued waiting for a response, from 1 to 4294967295.

Command Default

The default is 200.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **request-queue** command specifies the maximum number of GTP requests that are queued waiting for a response. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

Examples

The following example specifies a maximum request queue size of 300:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# request-queue 300
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
inspect gtp	Applies a specific GTP map to use for application inspection.

Commands	Description
show service-policy inspect gtp	Displays the GTP configuration.

request-timeout (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To configure the number of seconds before a failed SSO authentication attempt times out, use the **request-timeout** command in webvpn configuration mode.

To return to the default value, use the **no** form of this command.

request-timeout *seconds*
no request-timeout

Syntax Description

seconds	The number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds. Fractions are not supported.

Command Default

The default value for this command is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1.1	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports SiteMinder and SAML POST type SSO servers.

This command applies to both types of SSO Servers.

Once you have configured the ASA to support SSO authentication, you have the option to adjust two timeout parameters:

- The number of seconds before a failed SSO authentication attempt times out using the **request-timeout** command.
- The number of times the ASA retries a failed SSO authentication attempt. (See the **max-retry-attempts command.)**

Examples

The following example, entered in webvpn-config-sso-siteminder mode, configures an authentication timeout at ten seconds for the SiteMinder type SSO server, “example”:

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# request-timeout 10
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

reserved-bits

To clear reserved bits in the TCP header, or drop packets with reserved bits set, use the **reserved-bits** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

reserved-bits { **allow** | **clear** | **drop** }
no reserved-bits { **allow** | **clear** | **drop** }

Syntax Description

allow	Allows packet with the reserved bits in the TCP header.
clear	Clears the reserved bits in the TCP header and allows the packet.
drop	Drops the packet with the reserved bits in the TCP header.

Command Default

The reserved bits are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **reserved-bits** command in tcp-map configuration mode to remove ambiguity as to how packets with reserved bits are handled by the end host, which may lead to desynchronizing the ASA. You can choose to clear the reserved bits in the TCP header or even drop packets with the reserved bits set.

Examples

The following example shows how to clear packets on all TCP flows with the reserved bit set:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# reserved-bits clear
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

reserve-port-protect

To restrict usage on the reserve port during media negotiation, use the **reserve-port-protect** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

reserve-port-protect
no reserve-port-protect

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows how to protect the reserve port in an RTSP inspection policy map:

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

reset

When using the Modular Policy Framework, drop packets, close the connection, and send a TCP reset for traffic that matches a **match** command or class map by using the **reset** command in match or class configuration mode. This reset action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the no form of this command.

reset [**log**]
no reset [**log**]

Syntax Description

log	Logs the match. The system log message number depends on the application.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **reset** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you reset a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to reset the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. You can configure both the **reset** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is reset for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example resets the connection and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

resolver

To configure the addresses of the Cisco Umbrella DNS servers, which resolve DNS requests, use the **resolver** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

resolver { **ipv4** | **ipv6** } *ip_address*
no resolver { **ipv4** | **ipv6** } *ip_address*

Syntax Description

ipv4 *ip_address*	The IPv4 address of the Umbrella DNS server to use.
ipv6 *ip_address*	The IPv6 address of the Umbrella DNS server to use.

Command Default

The default DNS resolvers are 208.67.220.220 and 2620:119:53::53.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Umbrella configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

You can configure both IPv4 and IPv6 addresses by entering the command twice. You can specify valid Umbrella DNS servers only.

Examples

The following example defines non-default DNS resolvers for Cisco Umbrella. The servers are 208.67.222.222 and 2620:119:35::35.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222

ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

Related Commands

Commands	Description
umbrella-global	Configures the Cisco Umbrella global parameters.

responder-only

To configure one end of the VTI tunnel to act only as a responder, use the responder-only command in the IPsec profile configuration mode. Use the no form of this command to remove the responder-only mode.

responder-only
no responder-only

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

Using this command, one end of the VTI tunnel can be configured to act as a responder only.

The responder-only end will not initiate the tunnel or rekeying.

This option is useful when collision handling is not available, or when both ends of a tunnel try to initiate the tunnel simultaneously in instances when IKEv1 is used. All the rekey configurations for the IKE or IPsec tunnels on the responder-only end would be ignored even if configured.

Examples

The following example adds the responder-only mode to the IPsec profile:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.

Command	Description
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

rest-api (Deprecated)

Use the **agent** keyword to enable an installed REST API Agent from flash. Use the no form of this command to disable the Agent.

Use the image keyword after downloading a REST API package to this ASA (using the **copy** command) to verify and install the package. The version of the REST API Agent must match the ASA version. To uninstall this package, use the no form of this command.]

rest-api [**agent** | **image disk0 :** / *package*]
no rest-api [**agent** | **image disk0 :** / *package*]

Syntax Description

agent	Enable the installed REST API Agent.
image disk0:/*package*	Install the previously downloaded REST API image, identified by *package* .

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Enable/disable REST API Agent	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.
9.17(1)	This command was deprecated.

Usage Guidelines

Issue this command with the **image** keyword to perform compatibility and validation checks on the specified REST API package. If the package passes all checks pass, it will be installed to internal flash.

The REST API configuration is saved in the startup configuration file. Use the **clear configure** command to clear this configuration.

Installing or updating the REST API package will not trigger a reboot of the ASA.

Use this command with the **agent** keyword to enable the installed REST API Agent.

Examples

This example downloads the REST API package from cisco.com, and then installs it:

```
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-9.3.2-32.pkg  disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
```

This example upgrades the existing REST API Agent by disabling the running REST API Agent, and then downloading, installing and starting the new REST API Agent:

```
ciscoasa(config)# no rest-api agent
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-121-lfbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
ciscoasa(config)# rest-api agent
```

Related Commands

Commands	Description
copy	Copy a specified REST API package from a TFTP server to the internal flash memory.
show rest-api agent	Determine if the REST API Agent is running.
clear configure	Clear the running configuration, including the REST API configuration.

restore

To restore an ASA configuration, certificates, keys, and images from a backup file, use the **restore** command in privileged EXEC mode.

restore [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**cert-passphrase** *value*] [**location** *path*]

Syntax Description

cert-passphrase *value*	During the restoration of VPN certificates and preshared keys, a secret key identified by the **cert-passphrase** keyword is required to decode the certificates. You must provide a passphrase to be used for decoding the certificates in PKCS12 format.
context *ctx-name*	In multiple context mode from the system execution space, enter the **context** keyword to restore the specified context. Each backed up context file must be restored individually; that is, re-enter the **restore** command for each.
interface *name*	(Optional) Specifies the interface name through which the backup will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
location *path*	The restore **location** can be a local disk or a remote URL. If you do not provide a location, the following default names are used: • Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz • Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz
/noconfirm	Specifies not to prompt for the **location** and **cert-passphrase** parameters. Allows you to bypass warning and error messages to continue the backup.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

See the following guidelines:

- You should have at least 300 MB of disk space available at the restore location before you start a restore.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one restore at a time.
- You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.
- If you use clustering, you can only restore the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see the CLI configuration guide to learn how to reset it before continuing with the backup.
- If you import PKCS12 data (with the **crypto ca trustpoint** command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.
- If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **restore** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to restore through a data interface.
- You cannot back up using the CLI and restore using ASDM, or vice versa.
- Each backup file includes the following content:
- Running-configuration
- Startup-configuration
- All security images

Cisco Secure Desktop and Host Scan images

Cisco Secure Desktop and Host Scan settings

AnyConnect (SVC) client images and profiles

AnyConnect (SVC) customizations and transforms

- Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
- VPN pre-shared keys
- SSL VPN configurations

- Application Profile Custom Framework (APCF)
- Bookmarks
- Customizations
- Dynamic Access Policy (DAP)
- Plug-ins
- Pre-fill scripts for connection profiles
- Proxy Auto-config
- Translation table
- Web content
- Version information

Examples

The following example shows how to restore a backup:

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
is required to restore running configuration, startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
device, please note them for future reference.
ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the IP
is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the IP
is already used as media-termination address on interface inside.
```

```
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
 configuration file if you want to preserve the old http- and https-proxy configurations.
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
cisco. If the passphrase is not correct, certificates will not be restored.
No passphrase was provided for identity certificates. Using the default value: cisco. If
the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

Related Commands

Command	Description
backup	Backs up an ASA configuration, keys, certificates, and images from a backup file.

ret - rz

retries

To specify the number of times to retry the list of DNS servers when the ASA does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

retries *number*
no retries [*number*]

Syntax Description

number	Specifies the number of retries, from 0 through 10. The default is 2.

Command Default

The default number of retries is 2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Add DNS servers using the **name-server** command.

This command replaces the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The ASA tries each server only once.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# retries 0
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters the dns server-group mode.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

retry-count

To set the value for the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable, enter the **retry-count** command in scansafe general-options configuration mode. To restore the default, use the **no** form of this command.

retry-count *value*
no retry-count [*value*]

Syntax Description

value Enters the retry counter value, from 2 to 100. The default is 5.

Command Default

The default value is 5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Scansafe general-options configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 minutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active.

If a client or the ASA can reach the server at least twice consecutively before the retry count is reached, the polling stops and the tower is determined to be reachable.

The retry count also applies to application health checking if you enable it.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

Examples

The following example configures a retry value of 7:

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
```

```
health-check application
retry-count 7
license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
health-check application	Enables Cloud Web Security application health checking for failover.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the waits before polling the proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

retry-interval

To configure the amount of time between retry attempts for a particular AAA server designated in a previous **aaa-server host** command, use the **retry-interval** command in aaa-server host mode. To reset the retry interval to the default value, use the **no** form of this command.

retry-interval *seconds*
no retry-interval

Syntax Description

seconds	Specify the retry interval (1-10 seconds) for the request. This is the time the ASA waits before retrying a connection request.

Command Default

The default retry interval is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
AAA-server host	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the ASA waits between connection attempts. Use the **timeout** command to specify the length of time during which the ASA attempts to make a connection to a AAA server.

This command does not apply to servers in an RSA SecurID REST API server group.

Note For the RADIUS protocol, if the server responds with an ICMP Port Unreachable message, the retry-interval setting is ignored and the AAA server is immediately moved to the failed state. If this is the only server in the AAA group, it is reactivated and another request is sent to it. This is the intended behavior.

Examples

The following examples show the **retry-interval** command in context.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 7
```

```
ciscoasa
(config-aaa-server-host)# retry-interval 9
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol
timeout	Specifies the length of time during which the ASA attempts to make a connection to a AAA server.

reval-period

To specify the interval between each successful posture validation in a NAC Framework session, use the **reval-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC Framework policy, use the **no** form of this command.

reval-period *seconds*
no reval-period [*seconds*]

Syntax Description

seconds	Number of seconds between each successful posture validation. The range is 300 to 86400.

Command Default

The default value is 36000.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.3(0)	"nac-" was removed from the command name. The command was moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

The ASA starts the revalidation timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The ASA maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation.

Examples

The following example changes the revalidation timer to 86400 seconds:

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes the revalidation timer from the NAC policy:

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

Command	Description

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
debug nac	Enables logging of NAC Framework events.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.

revert webvpn all

To remove all web-related data (customization, plug-in, translation table, URL list, and web content) from the ASA flash memory, enter the **revert webvpn all** command in privileged EXEC mode.

revert webvpn all

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn all** command to disable and remove all web-related information (customization, plug-in, translation table, URL list, and web content) from the flash memory of the ASA. Removal of all web-related data returns default settings when applicable.

Examples

The following command removes all of the web-related configuration data from the ASA:

```
ciscoasa# revert webvpn all
ciscoasa
```

Related Commands

Command	Description
show import webvpn (option)	Displays various imported WebVPN data and plug-ins. currently present in flash memory on the ASA.

revert webvpn AnyConnect-customization

To remove a file from the ASA that *customizes the Secure client GUI*, use the **revert webvpn AnyConnect-customization** command in privileged EXEC mode.

revert webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

Syntax Description

type	The type of customizing file: • binary—An executable that replaces the AnyConnect GUI. • resource—A resource file, such as the corporate logo. • transform—A transform that customizes the MSI.
platform	The OS of the endpoint device running the Secure Client. Specify one of the following: linux, mac-intel, mac-powerpc, win, or win-mobile.
name	The name that identifies the file to remove (maximum 64 characters).

Command Default

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

For detailed procedures for customizing the Secure Client GUI, see the AnyConnect VPN Client Administrator Guide.

Examples

The following example removes the Cisco logo that was previously imported as a resource file to customize the AnyConnect GUI:

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

Related Commands

Command	Description
customization	Specifies the customization object to use for a tunnel-group, group, or user.

Command	Description
export customization	Exports a customization object.
import customization	Installs a customization object.
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn customization	Displays the current customization objects present on the flash device of the ASA.

revert webvpn customization

To remove a customization object from the ASA cache memory, enter the **revert webvpn customization** command in privileged EXEC mode.

revert webvpn customization *name*

Syntax Description

name	Specifies the name of the customization object to be deleted.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn customization** command to remove Clientless SSL VPN support for the specified customization and to remove it from the cache memory on the ASA. Removal of a customization object returns default settings when applicable. A customization object contains the configuration parameters for a specific, named portal page.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.

Note Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file before you upgrade to Version 8.0.

Examples

The following command removes the customization object named GroupB:

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

Related Commands

Command	Description
customization	Specifies the customization object to use for a tunnel-group, group, or user.
export customization	Exports a customization object.
import customization	Installs a customization object.
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn customization	Displays the current customization objects present on the flash device of the ASA.

revert webvpn plug-in protocol

To remove a plug-in from the flash device of the ASA, enter the **revert webvpn plug-in protocol** command in privileged EXEC mode.

revert plug-in protocol *protocol*

Syntax Description

protocol Enter one of the following strings:

- rdp

The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services.

- **ssh**

The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer.

- **vnc**

The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn plug-in protocol** command to disable and remove Clientless SSL VPN support for the specified Java-based client application, as well as to remove it from the flash drive of the ASA.

Examples

The following command removes support for RDP:

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

Related Commands

Command	Description
import webvpn plug-in protocol	Copies the specified plug-in from a URL to the flash device of the ASA. Clientless SSL VPN automatically supports the use of the Java-based client application for future sessions when you issue this command.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

revert webvpn translation-table

To remove a translation table from the ASA flash memory, enter the **revert webvpn translation-table** command in privileged EXEC mode.

revert webvpn translation-table *translationdomain* **language** *language*

Syntax Description

translationdomain	Available translation domains: • **AnyConnect** • **PortForwarder** • **banners** • **csd** • **customization** • **url-list** • **webvpn** • If available, translations of messages from Citrix, RPC, Telnet-SSH, and VNC plug-ins.)
language *language*	Specifies the language to be deleted. Specify the language using the 2-character code. Enter ? to see which languages are installed. Use the **show import webvpn translation-table** command to see which languages in each domain have been installed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn translation-table** command to disable and remove an imported translation table and to remove it from the flash memory. Removal of a translation table returns default settings when applicable.

Examples

The following command removes the AnyConnect translation table for French:

```
ciscoasa# revert webvpn translation-table anyconnect language fr

ciscoasa#
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL-list, and web content) .
show import webvpn translation-table	Displays the current translation tables currently present on the flash device.

revert webvpn url-list

To remove a URL list from the ASA, enter the **revert webvpn url-list** command in privileged EXEC mode.

revert webvpn url-list template *name*

Syntax Description

template *name*	Specifies the name of a URL list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn url-list** command to disable and remove a current URL list from the flash drive of the ASA. Removal of a url-list returns default settings when applicable.

The template argument used with the **revert webvpn url-list** command specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Examples

The following command removes the URL list, servers2:

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show running-configuration url-list	Displays the current set of configured URL list commands.
url-list (WebVPN mode)	Applies a list of WebVPN servers and URLs to a particular user or group policy.

revert webvpn webcontent

To remove a specified web object from a location in the ASA flash memory, enter the **revert webvpn webcontent** command in privileged EXEC mode.

revert webvpn webcontent *filename*

Syntax Description

filename	Specifies the name of the flash memory file with the web content to be deleted.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn content** command to disable and remove a file containing the web content and to remove it from the flash memory of the ASA. Removal of web content returns default settings when applicable.

Examples

The following command removes the web content file, ABCLogo, from the ASA flash memory:

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn webcontent	Displays the web content currently present in flash memory on the ASA.

revocation-check

To define whether revocation checking is needed for the trustpool policy, use the **revocation-check** command in crypto ca trustpool configuration mode. To restore the default revocation checking method, which is *none*, use the **no** form of this command.

revocation-check { [**crl**] [**ocsp**] [**none**] }
no revocation-check { [**crl**] [**ocsp**] [**none**] }

Syntax Description

crl	Specifies that the ASA should use CRL as the revocation checking method.
none	Specifies that the ASA should interpret the certificate status as valid, even if all methods return an error.
ocsp	Specifies that the ASA should use OCSP as the revocation checking method.

Command Default

The default value is *none*.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpool configuration mode	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(1)	Interface keyword to revocation checking using OCSP URL was added.
9.13(1)	The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.
9.15(1)	The option to bypass revocation checking, which was removed in 9.13(1), was restored.

Usage Guidelines

The signer of the OCSP response is usually the OCSP server (responder) certificate. After receiving the response, devices try to verify the responder certificate.

Normally a CA sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of compromising its security. The CA includes an ocsp-no-check extension in the responder certificate that indicates it does not need revocation status checking. But if this extension is not present, the device tries to check the certificate revocation status using the revocation methods you configure for the trustpoint with this **revocation-check** command. The OCSP responder certificate must be verifiable if it does not have an

ocsp-no-check extension since the OCSP revocation check fails unless you also set the *none* option to ignore the status check.

Note With any permutation of the optional arguments, *none* must be the last keyword used.

The ASA tries the methods in the order in which you configure them, trying the second and third methods only if the previous method returns an error (for example, server down), instead of finding the status as revoked.

You can set a revocation checking method in the client certificate validating trustpoint and also configure no revocation checking (**revocation-check none)** in the responder certificate validating trustpoint. See the **match certificate** command for a configuration example.

If you have configured the ASA with the **revocation-check crl none** command, when a client connects to the ASA, it automatically starts downloading the CRL because it has not been cached, then validates the certificate, and finishes downloading the CRL. In this case, if the CRL is not cached, the ASA validates the certificate before downloading the CRL.

The following options for bypassing revocation checking, which was removed in ASA 9.13(1), was later restored:

Option	Action
revocation-check crl none	If CRLs cannot be accessed, bypass revocation checking
revocation-check ocsp none	If OCSP checking cannot be performed, bypass revocation checking
revocation-check crl ocsp none	If CRLs cannot be accessed, try OCSP. If OCSP cannot be performed, bypass revocation checking
revocation-check ocsp crl none	If OCSP cannot be performed, try CRLs, else, bypass revocation checking

When you are assigning OCSP URL for revocation checking, you can specify the management interface from where the OCSP is reachable. This interface value determines the routing decision.

Examples

```
ciscoasa(config-ca-trustpoint)# revocation-chec
k ?
crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)# ocsp
ocsp interface mgmt url http://1.1.1.1:8888
```

Here, mgmt is the name of the management interface

Related Commands

Command	Description
crypto ca trustpool policy	Enters a submode that provides the commands that define the trustpool policy.
match certificate allow expired-certificate	Allows the administrator to exempt certain certificates from expiration checking.

Command	Description
match certificate skip revocation-check	Allows the administrator to exempt certain certificates from revocation checking.

rewrite(Deprecated)

To disable content rewriting a particular application or type of traffic over a WebVPN connection, use the **rewrite** command in webvpn mode. To eliminate a rewrite rule, use the **no** form of this command with the rule number, which uniquely identifies the rule. To eliminate all rewriting rules, use the **no** form of the command without the rule number.

By default, the ASA rewrites, or transforms, all WebVPN traffic.

rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]
no rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]

Syntax Description

disable	Defines this rewrite rule as a rule that disables content rewriting for the specified traffic. When you disable content rewriting, traffic does not go through the security appliance.
enable	Defines this rewrite rule as a rule that enables content rewriting for the specified traffic.
integer	Sets the order of the rule among all of the configured rules. The range is 1-65534.
name	(Optional) Identifies the name of the application or resource to which the rule applies.
order	Defines the order in which the ASA applies the rule.
resource-mask	Identifies the application or resource for the rule.
resource name	(Optional) Specifies the application or resource to which the rule applies. Maximum 128 bytes.
string	Specifies the name of the application or resource to match that can contain a regular expression. You can use the following wildcards: Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 300 bytes.

Command Default

The default is to rewrite everything.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The ASA performs content rewriting for applications to insure that they render correctly over WebVPN connections. Some applications do not require this processing, such as external public websites. For these applications, you might choose to turn off content rewriting.

You can turn off content rewriting selectively by using the rewrite command with the disable option to let users browse specific sites directly without going through the ASA. This is similar to split-tunneling in IPsec VPN connections.

You can use this command multiple times. The order in which you configure entries is important because the ASA searches rewrite rules by order number and applies the first rule that matches.

Examples

The following example shows how to configure a rewrite rule, order number of 1, that turns off content rewriting for URLS from cisco.com domains:

```
ciscoasa
(config-webpn)#
 rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
proxy-bypass	Configures minimal content rewriting for a particular application.

re-xauth

To require that IPsec users reauthenticate on IKE rekey, issue the **re-xauth enable** command in group-policy configuration mode. To disable user reauthentication on IKE rekey, use the **re-xauth disable** command.

To remove the re-xauth attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for reauthentication on IKE rekey from another group policy.

re-xauth { **enable** [**extended**] | **disable** }
no re-xauth

Syntax Description

disable	Disables reauthentication on IKE rekey
enable	Enables reauthentication on IKE rekey
extended	Extends the time allowed for reentering authentication credentials until the maximum lifetime of the configured SA.

Command Default

Reauthentication on IKE rekey is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0.4	The **extended** keyword was added.

Usage Guidelines

Reauthentication on IKE rekey applies only to IPsec connections.

If you enable reauthentication on IKE rekey, the ASA prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates. Use the **extended** keyword to allow users to reenter authentication credentials until the maximum lifetime of the configured SA.

To check the configured rekey interval, in monitoring mode, issue the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data.

Note The reauthentication fails if there is no user at the other end of the connection.

Examples

The following example shows how to enable reauthentication on rekey for the group policy named FirstGroup:

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip authentication mode

To specify the type of authentication used in RIP Version 2 packets, use the **rip authentication mode** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

rip authentication mode { **text** | **md5** }
no rip authentication mode

Syntax Description

md5	Uses MD5 for RIP message authentication.
text	Uses clear text for RIP message authentication (not recommended).

Command Default

Clear text authentication is used by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

Command	Description
rip authentication key	Enables RIP Version 2 authentication and specifies the authentication key.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.

Command	Description
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip authentication key

To enable authentication of RIP Version 2 packets and specify the authentication key, use the **rip authentication key** command in interface configuration mode. To disable RIP Version 2 authentication, use the **no** form of this command.

rip authentication key [**0**|**8**] *string* **key_id** *id*
no rip authentication key

Syntax Description

0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
id	Specifies the key identification value; valid values range from 1 to 255.
key	Specifies the shared key to be used for the authentication key string. The key can contain up to 16 characters.
string	Specifies the unencrypted (cleartext) user password.

Command Default

RIP authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates. When you enable neighbor authentication, you must ensure that the *key* and *key_id* arguments are the same as those used by neighbor devices that provide RIP version 2 updates. The key is a text string of up to 16 characters.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet 0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

Related Commands

Command	Description
rip authentication mode	Specifies the type of authentication used in RIP Version 2 packets.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

version { [**1**] [**2**] }
no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Command Default

The ASA accepts Version 1 and Version 2 packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to receive RIP Versions 1 and 2 packets the specified interface:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
router rip	Enables the RIP routing process and enters router configuration mode for that process.

Command	Description
version	Specifies the version of RIP used globally by the ASA.

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

rip send version { [**1**] [**2**] }
no rip send version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Command Default

The ASA sends RIP Version 1 packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to send and receive RIP Versions 1 and 2 packets on the specified interface:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.

Command	Description
version	Specifies the version of RIP used globally by the ASA.

rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

rmdir [/ **no confirm**] [**disk0:| disk1:| flash:**] *path*

Syntax Description

/noconfirm	(Optional) Suppresses the confirmation prompt.
disk0*:*	(Optional) Specifies the nonremovable internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the removable external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the nonremovable internal flash, followed by a colon. In the ASA 5500 series adaptive security appliances, the **flash** keyword is aliased to **disk0**.
path	(Optional) The absolute or relative path of the directory to remove.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the directory is not empty, the **rmdir** command fails.

Examples

The following example shows how to remove an existing directory named “test”:

```
ciscoasa# rmdir test
```

Related Commands

Command	Description
dir	Displays the directory contents.
mkdir	Creates a new directory.
pwd	Displays the current working directory.
show file	Displays information about the file system.

route

To enter a static or default route for the specified interface, use the **route** command in global configuration mode. To remove routes from the specified interface, use the **no** form of this command.

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]
no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] **tunneled**]

Syntax Description

gateway_ip	Specifies the IP address of the gateway router (the next-hop address for this route). **Note** The *gateway_ip* argument is optional in transparent mode.
interface_name	Specifies the interface name through which the traffic is routed. For transparent mode, specify a bridge group member interface name. For routed mode with bridge groups, specify the BVI name. In routed mode, to "black hole" unwanted traffic, enter the **null0** interface.
ip_address	Specifies the internal or external network IP address.
metric	(Optional) Specifies the administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
netmask	Specifies a network mask to apply to *ip_address*.
track*number*	(Optional) Associates a tracking entry with this route. Valid values are from 1 to 500. **Note** The **track** option is only available in single, routed mode.
tunneled	Specifies the route as the default tunnel gateway for VPN traffic.

Command Default

The *metric* default is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **track** *number* value was added.
9.2(1)	The **null0** interface option was added.
9.7(1)	Support was added for BVI interfaces in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

Use the **route** command to enter a default or static route for an interface. To enter a default route, set *ip_address* and *netmask* to **0.0.0.0,** or use the shortened form of **0**. All routes that are entered using the **route** command are stored in the configuration when it is saved.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the ASA that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled** option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of a tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route, because the session will fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with vlan mapping options or tunneled routes. These inspection engines ignore the vlan-mapping setting which could result in packets being incorrectly routed.

You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

Create static routes to access networks that are connected outside a router on any interface. For example, the ASA sends all packets that are destined to the 192.168.42.0 network through the 192.168.1.5 router with the following static route command.

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

After you enter the IP address for each interface, the ASA creates a CONNECT route in the route table. This entry is not deleted when you use the **clear route** or **clear configure route** commands.

Unlike with ACLs, static **null0** routes do not cause any performance degradation. The **null0** configuration is used to prevent routing loops. BGP leverages the **null0** configuration for Remotely Triggered Black Hole routing.

Examples

The following example shows how to specify one default route command for an outside interface:

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

The following example shows how to add these static route commands to provide access to the networks:

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

The following example uses an SLA operation to install a default route to the 10.1.1.1 gateway on the outside interface. The SLA operation monitors the availability of that gateway. If the SLA operation fails, then the backup route on the DMZ interface is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
```

```
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

The following example shows how to configure a static null0 route:

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

Related Commands

Command	Description
clear configure route	Removes statically configured **route** commands.
clear route	Removes routes learned through dynamic routing protocols such as RIP.
show route	Displays route information.
show running-config route	Displays configured routes.

route-map

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

route-map *name* [**permit | deny**] [*sequence number*]
no route-map *name* [**permit | deny**] [*sequence number*]

Syntax Description

name	Defines a meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same name.
permit	(Optional) If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the permit keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set. The permit keyword is the default.
deny	(Optional) If the match criteria are met for the route map and the deny keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted.

Command Default

There are no defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use route maps to redistribute routes

Use the route-map global configuration command, and the match and set route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The match route-map configuration command has multiple formats. The match commands can be given in any order, and all match commands must "pass" to cause the route to be redistributed according to the set actions given with the set commands. The no forms of the match commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the router global configuration command. The source routing protocol is the one you specify with the redistribute router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

The sequence-number argument works as follows:

1. If no entry is defined with the route-map name, an entry is created with the sequence-number argument set to 10.

2. If only one entry is defined with the route-map name, that entry becomes the default entry for the following route-map command. The sequence-number argument of this entry is unchanged.

3. If more than one entry is defined with the route-map name, an error message is printed to indicate that the sequence-number argument is required.

4. If the no route-map name command is specified (with no sequence-number argument), the whole route map is deleted.

Examples

The following example shows how to redistribute routes with a hop count equal to 1 into OSPF. The ASA redistributes these routes as external LSAs with a metric of 5 and a metric type of Type 1:

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

The following example shows how to redistribute the 10.1.1.0 static route into eigrp process 1 with the configured metric value:

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.
route	Creates a static or default route for an interface.
router	Enters the router configuration mode for a specified protocol.

route priority high

To assign a high priority to an IS-IS IP prefix, use the **route priority high** command in router isis configuration mode. To remove the IP prefix priority, use the **no** form of this command

route priority high *tag-value*
no route priority high *tag-value*

Syntax Description

tag-value Assigns a high priority to IS-IS IP prefixes with a specific route tag. The range is 1 to 4294967295.

Command Default

No IP prefix priority is set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

When you use the **route priority high** command to tag higher priority IS-IS IP prefixes for faster processing and installation in the global routing table, you can achieve faster convergence. For example, you can help Voice over IP (VoIP) gateway addresses get processed first to help VoIP traffic get updated faster than other types of packets.

Examples

The following example uses the **route priority high** command to assign a tag value of 100 to the IS-IS IP prefix:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# route priority high tag 100
```

Related Commands

router-alert

To define an action when the Router Alert IP option occurs in a packet header with IP Options inspection, use the **router-alert** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

router-alert action { **allow | clear** }
no router-alert action { **allow | clear** }

Syntax Description

allow	Allow packets containing the Router Alert IP option.
clear	Remove the Router Alert option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection allows packets containing the Router Alert IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

The Router Alert (RTRALT) or IP Option 20 notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols require relatively complex processing from the routers along the packets delivery path.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the router bgp command in global configuration mode. To remove a BGP routing process, use the no form of this command.

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535.

Command Default

No BGP routing process is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octetnumbers in the range from 1 to 65535 as described in RFC 4271, A Border Gateway Protocol 4 (BGP-4).

Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) allocates four-octet autonomous system numbers in the range from 65536 to 4294967295.

RFC 5396, Textual Representation of Autonomous System (AS) Numbers, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Examples

The following example shows how to configure a BGP process for autonomous system number 100:

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

Related Commands

Command	Description
show route bgp	Displays the routing table.
show bgp summary	Display the status of all Border Gateway Protocol (BGP) connections

router eigrp

To start an EIGRP routing process and configure parameters for that process, use the **router eigrp** command in global configuration mode. To disable EIGRP routing, use the **no** form of this command.

router eigrp *as-number*
no router eigrp *as-number*

Syntax Description

as-number	Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information. Valid values are from 1 to 65535.

Command Default

EIGRP routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **router eigrp** command creates an EIGRP routing process or enters router configuration mode for an existing EIGRP routing process. You can only create a single EIGRP routing process on the ASA.

Use the following router configuration mode commands to configure the EIGRP routing processes:

- **auto-summary**—Enable/disable automatic route summarization.
- **default-information**—Enable/disable the reception and sending of default route information.
- **default-metric**—Define the default metrics for routes redistributed into the EIGRP routing process.
- **distance eigrp**—Configure the administrative distance for internal and external EIGRP routes.
- **distribute-list**—Filter the networks received and sent in routing updates.
- **eigrp log-neighbor-changes**—Enable/disable the logging of neighbor state changes.
- **eigrp log-neighbor-warnings**—Enable/disable the logging of neighbor warning messages.
- **eigrp router-id**—Creates a fixed router ID.
- **eigrp stub**—Configures the ASA for stub EIGRP routing.

- **neighbor**—Statically define an EIGRP neighbor.
- **network**—Configure the networks that participate in the EIGRP routing process.
- **passive-interface**—Configure an interface to act as a passive interface.
- **redistribute**—Redistribute routes from other routing processes into EIGRP.

Use the following interface configuration mode commands to configure interface-specific EIGRP parameters:

- **authentication key eigrp**—Define the authentication key used for EIGRP message authentication.
- **authentication mode eigrp**—Define the authentication algorithm used for EIGRP message authentication.
- **delay**—Configure the delay metric for an interface.
- **hello-interval eigrp**—Change the interval at which EIGRP hello packets are sent out of an interface.
- **hold-time eigrp**—Change the hold time advertised by the ASA.
- **split-horizon eigrp**—Enable/disable EIGRP split-horizon on an interface.
- **summary-address eigrp**—Manually define a summary address.

Examples

The following example shows how to enter the configuration mode for the EIGRP routing process with the autonomous system number 100:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
clear configure eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3. To reset OSPF to use the previous router ID behavior, use the **no** form of this command.

router-id *id*
no router-id [*id*]

Syntax Description

id Specifies the router ID in IP address format.

Command Default

If not specified, the highest-level IP address on the ASA is used as the router ID.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The processing order for this command was changed. The command is now processed before the **network** commands in an OSPFv2 configuration.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

By default, the ASA uses the highest-level IP address on an interface that is covered by a **network** command in the OSPF configuration. If the highest-level IP address is a private address, then that address is sent in hello packets and database definitions. To use a specific router ID, use the **router-id** command to specify a global address for the router ID.

Router IDs must be unique within an OSPF routing domain. If two routers in the same OSPF domain are using the same router ID, routing may not work correctly.

You should enter the **router-id** command before entering **network** commands in an OSPF configuration. This prevents possible conflicts with the default router ID generated by the ASA. If you do have a conflict, you will receive the message:

```
ERROR: router-id id in use by ospf process pid
```

To enter the conflicting ID, remove the **network** command that contains the IP address causing the conflict, enter the **router-id** command, and then re-enter the **network** command.

Clustering

In Layer 2 clustering, you either need to configure the **router-id** *id* command or leave the router ID blank, provided all units receive the same router ID.

Examples

The following example sets the router ID to 192.168.1.1:

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPFv2 routing processes.

router-id cluster-pool

To specify the router ID cluster pool for a Layer 3 clustering deployment, use the **router-id cluster-pool** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3.

router-id cluster-pool hostname | A.B.C.D *ip_pool*

Syntax Description

cluster-pool	Enables configuration of an IP address pool when Layer 3 clustering is configured.
hostname | **A.B.C.D**	Specifies the OSPF router ID for this OSPF process.
ip_pool	Specifies the name of the IP address pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Router IDs must be unique within an OSPFv2 or OSPFv3 routing domain in clustering. If two routers in the same OSPFv2 or OSPFv3 domain are using the same router ID, routing in clustering may not work correctly.

In Layer 2 clustering, you either need to configure the **router-id** *id* command or leave the router ID blank, provided all units receive the same router ID.

When a Layer 3 cluster interface is configured, each unit must have a unique interface IP address. To make sure that each unit has a unique interface IP address, you can configure a local pool of IP addresses for OSPFv2 or OSPFv3 with the **router-id cluster-pool** command.

Examples

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv2:

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
```

```
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv3:

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
router ospf	Enters router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show ospf	Displays general information about the OSPFv2 routing processes.

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis
no router isis

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command is used to enable IS-IS routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the ASA. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible. See the Related Commands table for a list of commands used to configure IS-IS.

Examples

In the following example IS-IS routing is enabled:

```
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Related Commands

router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

router ospf *pid*
no router ospf *pid*

Syntax Description

pid Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The *pid* does not need to match the ID of OSPF processes on other routers.

Command Default

OSPF routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the ASA. Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in router configuration mode.

When using the **no router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no router ospf** command terminates the OSPF routing process specified by its *pid.* You assign the *pid* locally on the ASA. You must assign a unique value for each OSPF routing process.

The **router ospf** command is used with the following OSPF-specific commands to configure OSPF routing processes:

- **area**—Configures a regular OSPF area.
- **compatible rfc1583**—Restores the method used to calculate summary route costs per RFC 1583.
- **default-information originate**—Generates a default external route into an OSPF routing domain.
- **distance**—Defines the OSPF route administrative distances based on the route type.
- **ignore**—Suppresses the sending of syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets.

- **log-adj-changes**—Configures the router to send a syslog message when an OSPF neighbor goes up or down.
- **neighbor**—Specifies a neighbor router. Used to allow adjacency to be established over VPN tunnels.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain to another according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timer lsa arrival**— Defines the minimum interval (in msec) between accepting the same link-state advertisement (LSA) from OSPF neighbors.
- **timer pacing flood**— Defines the minimum interval (in msec) at which LSAs in the flooding queue are paced between updates.
- **timer pacing lsa-group**— Defines the interval (in sec) between groups of LSA being refreshed or managed.
- **timer pacing retransmission**— Defines the minimum interval (in msec) between neighbor retransmissions.
- **timer throttle lsa**— Defines the delay to generate the first occurrence of LSA (in milliseconds).
- **timer throttle spf**— Defines the delay between receiving a change to SPF calculation (in milliseconds).
- **timer nsf wait**—Defines the interface wait interval during NSF restart. The default value is 20 seconds. The permissible range is 1 to 65535 seconds.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

Related Commands

Command	Description
clear configure router	Clears the OSPF router commands from the running configuration.
show running-config router ospf	Displays the OSPF router commands in the running configuration.

router rip

To start a RIP routing process and configure parameters for that process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

router rip
no router rip

Syntax Description

This command has no arguments or keywords.

Command Default

RIP routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **router rip** command is the global configuration command for configuring the RIP routing processes on the ASA. You can only configure one RIP process on the ASA. The **no router rip** command terminates the RIP routing process and removes all router configuration for that process.

When you enter the **router rip** command, the command prompt changes to ciscoasa(config-router)#, indicating that you are in router configuration mode.

The **router rip** command is used with the following router configuration commands to configure RIP routing processes:

- **auto-summary**—Enable/disable automatic summarization of routes.
- **default-information originate**—Distribute a default route.
- **distribute-list in**—Filter networks in incoming routing updates.
- **distribute-list out**—Filter networks in outgoing routing updates.
- **network**—Add/remove interfaces from the routing process.
- **passive-interface**—Set specific interfaces to passive mode.
- **redistribute**—Redistribute routes from other routing processes into the RIP routing process.
- **version**—Set the RIP protocol version used by the ASA.

Additionally, you can use the following commands in interface configuration mode to configure RIP properties on a per-interface basis:

- **rip authentication key**—Set an authentication key.
- **rip authentication mode**—Set the type of authentication used by RIP Version 2.
- **rip send version**—Set the version of RIP used to send updates out of the interface. This overrides the version set in global router configuration mode, if any.
- **rip receive version**—Set the version of RIP accepted by the interface. This overrides the version set in global router configuration mode, if any.

RIP is not supported in transparent mode. By default, the ASA denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through an ASA operating in transparent mode you must define access list entries to permit this traffic. For example, to permit RIP version 2 traffic through the ASA, create an access list entry such as the following:

ciscoasa(config)# **access-list myriplist extended permit ip any host 224.0.0.9**

To permit RIP version 1 broadcasts, create an access list entry such as the following:

ciscoasa(config)# **access-list myriplist extended permit udp any any eq rip**

Apply these access list entries to the appropriate interface using the **access-group** command.

You can enable both RIP and OSPF routing on the ASA at the same time.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

Related Commands

Command	Description
clear configure router rip	Clears the RIP router commands from the running configuration.
show running-config router rip	Displays the RIP router commands in the running configuration.

rtp-conformance

To check RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP, use the **rtp-conformance** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

rtp-conformance [**enforce-payloadtype**]
no rtp-conformance [**enforce-payloadtype**]

Syntax Description

enforce-payloadtype	Enforces payload type to be audio/video based on the signaling exchange.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to check RTP packets flowing on the pinholes for protocol conformance on an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
debug rtp	Displays debug information and error messages for RTP packets associated with H.323 and SIP inspection.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

rtp-min-port rtp-max-port (Deprecated)

To configure the rtp-min-port and rtp-max-port limits for the phone proxy feature, use the **rtp-min-port rtp-max-port** command in phone-proxy configuration mode. To remove the limits from the phone proxy configuration, use the **no** form of this command.

rtp-min-port *port1* **rtp-maxport** *port2*
no rtp-min-port *port1* **rtp-maxport** *port2*

Syntax Description

port1	Specifies the minimum value for the RTP port range for the media termination point, where *port1* can be a value from 1024 to 16384.
port2	Specifies the maximum value for the RTP port range for the media termination point, where *port2* can be a value from 32767 to 65535.

Command Default

By default, the *port1* value for the **rtp-min-port** keyword is 16384 and the *port2* value for the **rtp-max-port** keyword is 32767.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Configure the RTP port range for the media termination point when you need to scale the number of calls that the Phone Proxy supports.

Examples

The following example shows the use of the **rtp-min-port** command to specify the ports to use for media connections:

```
ciscoasa
(config-phone-proxy)#
rtp-min-port 2001 rtp-maxport 32770
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.