Cisco Secure Firewall ASA Series Command Reference, T - Z Commands and IOS Commands for ASASM

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

T-Z Commands

ta – tk

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family configuration mode. To disable this function, use the **no** form of the command.

table-map *map_name* [**filter**]
no table-map *map_name* [**filter**]

Syntax Description

map_name	The name of the route map that should control what gets put into the BGP routing table (RIB).
filter	(Optional) Specifies that the route map controls not only the metrics on a BGP route, but also whether the route is downloaded into the RIB. A BGP route is not downloaded to the RIB if it is denied by the route 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
Address family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

A table map references a route map that sets metrics and a tag value for routes that are updated in the BGP routing table, or controls whether routes are downloaded to the RIB.

When the table-map command:

- Does not include the **filter** keyword, the route map referenced is used to set certain properties of a route before the route is installed (downloaded) into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- Includes the **filter** keyword, the route map referenced also controls whether the BGP route is downloaded to the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

You can use match clauses in the route map that the table map references to match routes based on IP access list, autonomous system paths, and next hop.

Examples

In the following address family configuration mode example, the Secure Firewall ASA software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
ciscoasa(config)# route-map tag
ciscoasa(config-route-map)# match as path 10
ciscoasa(config-route-map)# set automatic-tag
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# table-map tag
```

Related Commands

Command	Description
address-family	Enters the address-family configuration mode.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

tcp-inspection

To enable DNS over TCP inspection, use the **tcp-inspection** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

tcp-inspection
no tcp-inspection

Syntax Description

This command has no arguments or keywords.

Command Default

DNS over TCP inspection 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
9.6(2)	This command was added.

Usage Guidelines

Add this command to a DNS inspection policy map to include DNS/TCP port 53 traffic in the inspection. Without this command, UDP/53 DNS traffic only is inspected. Ensure that DNS/TCP port 53 traffic is part of the class to which you apply DNS inspection. The inspection default class includes TCP/53.

Examples

The following example shows how to enable DNS over TCP inspection a DNS inspection policy map:

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

Related Commands

Command	Description
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
show running-config policy-map	Display all current policy map configurations.

tcp-map

To define a set of TCP normalization actions, use the **tcp-map** command in global configuration mode. The TCP normalization feature lets you specify criteria that identify abnormal packets, which the ASA drops when they are detected. To remove the TCP map, use the **no** form of this command.

tcp-map *map_name*
no tcp-map *map_name*

Syntax Description

map_name	Specifies the TCP map 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
7.0(1)	This command was added.
7.2(4)/8.0(4)	The **invalid-ack**, **seq-past-window**, and **synack-data** subcommands were added.

Usage Guidelines

This feature uses Modular Policy Framework. First define the TCP normalization actions you want to take using the **tcp-map** command. The **tcp-map** command enters tcp-map configuration mode, where you can enter one or more commands to define the TCP normalization actions. Then define the traffic to which you want to apply the TCP map using the **class-map** command. Enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, enter the **set connection advanced-options** command to reference the TCP map. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the CLI configuration guide.

The following commands are available in tcp-map configuration mode:

check-retransmission	Enables and disables the retransmit data checks.
checksum-verification	Enables and disable checksum verification.
exceed-mss	Allows or drops packets that exceed MSS set by peer.
invalid-ack	Sets the action for packets with an invalid ACK.

queue-limit	Configures the maximum number of out-of-order packets that can be queued for a TCP connection. This command is only available on the ASA 5500 series adaptive ASA. On the PIX 500 series ASA, the queue limit is 3 and cannot be changed.
reserved-bits	Sets the reserved flags policy in the ASA.
seq-past-window	Sets the action for packets that have past-window sequence numbers, namely the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window.
synack-data	Sets the action for TCP SYNACK packets that contain data.
syn-data	Allows or drops SYN packets with data.
tcp-options	Sets the action for packets based on the contents of the TCP options field in the TCP header.
ttl-evasion-protection	Enables or disables the TTL evasion protection offered by the ASA.
urgent-flag	Allows or clears the URG pointer through the ASA.
window-variation	Drops a connection that has changed its window size unexpectedly.

Examples

For example, to allow urgent flag and urgent offset packets for all traffic sent to the range of TCP ports between the well known FTP data port and the Telnet port, enter the following commands:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config-tcp-map)# class-map urg-class
ciscoasa(config-cmap)# match port tcp range ftp-data telnet
ciscoasa(config-cmap)# policy-map pmap
ciscoasa(config-pmap)# class urg-class
ciscoasa(config-pmap-c)# set connection advanced-options tmap
ciscoasa(config-pmap-c)# service-policy pmap global
```

Related Commands

Command	Description
class (policy-map)	Specifies a class map to use for traffic classification.
clear configure tcp-map	Clears the TCP map configuration.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config tcp-map	Displays the information about the TCP map configuration.
tcp-options	Allows or clears the selective-ack, timestamps, or window-scale TCP options.

tcp-options

To allow or clear the TCP options in a TCP header, use the **tcp-options** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

tcp-options { **md5 | mss | selective-ack | timestamp | window-scale | range** *lower upper* } *action*
no tcp-options { **md5 | mss | selective-ack | timestamp | window-scale | range** *lower upper* } *action*

Syntax Description

action	The action to perform for the option. Actions are: • **allow** [**multiple**]—Allow packets that contain the option. Starting with 9.6(2), **allow** means to allow packets that contain a single option of this type. This is the default for all of the named options. If you want to allow packets even if they contain more than one instance of the option, add the **multiple** keyword. The **multiple** keyword is not available with **range**. • **maximum** *limit*—For **mss** only. Set the maximum segment size to the indicated limit, from 68-65535. The default TCP MSS is defined on the **sysopt connection tcpmss** command. • **clear**—Remove the options of this type from the header and allow the packet. This is the default for all of the numbered options you can configure on the **range** keyword. Note that clearing the timestamp option disables PAWS and RTT. • **drop**—Drop packets that contain this option. This action is available for **md5** and **range** only.
md5	Sets the action for the MD5 option.
mss	Sets the action for the maximum segment size option.
range *lower upper*	Sets with action for the numbered options within the lower and upper bounds of the range. To set the action for a single numbered option, enter the same number for the lower and upper range. (9.6(2) and later.) The valid ranges are within 6-7, 9-18, and 20-255. (9.6(1) and earlier.) The valid ranges are within 6-7 and 9-255.
selective-ack	Sets the action for the selective acknowledgment mechanism (SACK) option.
timestamp	Sets the action for the timestamp option. Clearing the timestamp option will disable PAWS and RTT.
window-scale	Sets the action for the window scale mechanism option.

Command Default

(9.6(1) and earlier.) The default is to allow all of the named options, and clear options 6-7 and 9-255.

(9.6(2) and later.) The default is to allow a single instance of each of the named options, drop packets with more than one of a given named option, and clear options 6-7, 9-18, and 20-155.

Command Modes

The 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.
9.6(2)	Default handling of the named options was changed to allow a packet if it contains a single option of a given type, and drop the packet if there are more than one option of that type. Also, the **md5**, **mss**, **allow multiple**, and **mss maximum** keywords were added. The default for the MD5 option was changed from clear to allow.

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 **tcp-options** command in tcp-map configuration mode to define how the various TCP options should be handled.

Examples

The following example shows how to drop all packets with TCP options in the ranges of 6-7 and 9-255:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# tcp-options range 6 7 drop
ciscoasa(config-tcp-map)# tcp-options range 9 18 drop
ciscoasa(config-tcp-map)# tcp-options range 20 255 drop
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.

telnet

To allow Telnet access to an interface, use the **telnet** command in global configuration mode. To remove Telnet access, use the **no** form of this command.

telnet { *ipv4_address mask* | *ipv6_address/prefix* } *interface_name*
no telnet { *ipv4_address mask* | *ipv6_address/prefix* } *interface_name*

Syntax Description

interface_name	Specifies the name of the interface on which to allow Telnet. You cannot enable Telnet on the lowest security interface unless you use Telnet in a VPN tunnel. A physical or virtual interface can be specified.
ipv4_address mask	Specifies the IPv4 address of a host or network authorized to Telnet to the ASA, and the subnet mask.
ipv6_address/prefix	Specifies the IPv6 address/prefix authorized to Telnet to the ASA.

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(2), 9.1(2)	The default password, “cisco” has been removed; you must actively set a login password using the **password** command.
9.9.(2)	Virtual interfaces can now be specified.

Usage Guidelines

The **telnet** command lets you specify which hosts can access the ASA CLI with Telnet. You can enable Telnet to the ASA on all interfaces. However, You cannot use Telnet to the lowest security interface unless you use Telnet inside a VPN tunnel. Also, if a BVI interface is specified, managenent-access must be configured on that interface.

Use the password command to set a password for Telnet access to the console. Use the who command to view which IP addresses are currently accessing the ASA console. Use the kill command to terminate an active Telnet console session.

If you use the aaa **authentication telnet con**sole command, Telnet console access must be authenticated with an authentication server.

Examples

This example shows how to permit hosts 192.168.1.3 and 192.168.1.4 to access the ASA CLI through Telnet. In addition, all the hosts on the 192.168.2.0 network are given access.

```
ciscoasa(config)# telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.1.4 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.2.0 255.255.255.0 inside
ciscoasa(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

This example shows a Telnet console login session (the password does not display when entered):

```
ciscoasa# passwd: cisco
Welcome to the XXX
…
Type help or '?' for a list of available commands.
ciscoasa>
```

You can remove individual entries with the **no telnet** command or all telnet command statements with the **clear configure telnet** command:

```
ciscoasa(config)# no telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

ciscoasa(config)# clear configure telnet
```

Related Commands

Command	Description
clear configure telnet	Removes a Telnet connection from the configuration.
kill	Terminates a Telnet session.
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the ASA.
telnet timeout	Sets the Telnet timeout.
who	Displays active Telnet administration sessions on the ASA.

telnet timeout

To set the Telnet idle timeout, use the **telnet timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

telnet timeout *minutes*
no telnet timeout *minutes*

Syntax Description

minutes	Number of minutes that a Telnet session can be idle before being closed by the ASA. Valid values are from 1 to 1440 minutes. The default is 5 minutes.

Command Default

By default, Telnet sessions left idle for five minutes are closed by the ASA.

Command Modes

The 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 the telnet timeout command to set the maximum time that a console Telnet session can be idle before being logged off by the ASA.

Examples

This example shows how to change the maximum session idle duration:

```
ciscoasa(config)# telnet timeout 10
ciscoasa(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

Related Commands

Command	Description
clear configure telnet	Removes a Telnet connection from the configuration.
kill	Terminates a Telnet session.
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the ASA.
telnet	Enables Telnet access to the ASA.

Command	Description
who	Displays active Telnet administration sessions on the ASA.

terminal interactive

To enable help in the current CLI session when you enter **?** at the CLI, use the **terminal interactive** command in privileged EXEC mode. To disable CLI help, use the **no** form of this command.

terminal interactive
no terminal interactive

Syntax Description

This command has no arguments or keywords.

Command Default

Interactive CLI help 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Normally, when you enter **?** at the ASA CLI, you see command help. To be able to enter **?** as text within a command (for example, to include a **?** as part of a URL), you can disable interactive help using the **no terminal interactive** command.

Examples

The following example shows how to turn the console into a non-interactive mode, then into an interactive mode:

```
ciscoasa# no
 terminal interactive
ciscoasa# terminal interactive
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the “---more---” prompt. This command is saved to the configuration.
show running-config terminal	Displays the current terminal settings.
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.

Command	Description
terminal width	Sets the terminal display width in global configuration mode.

terminal monitor

To allow syslog messages to show in the current CLI session, use the **terminal monitor** command in privileged EXEC mode. To disable syslog messages, use the **no** form of this command.

terminal { **monitor | no monitor** }

Syntax Description

monitor	Enables the display of syslog messages in the current CLI session.
no monitor	Disables the display of syslog messages in the current CLI session.

Command Default

Syslog messages are disabled by default. This command is interactive 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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to display and disable syslog messages in the current session:

```
ciscoasa# terminal monitor
ciscoasa# terminal no monitor
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is saved to the configuration.
show running-config terminal	Displays the current terminal settings.
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.

terminal pager

To set the number of lines on a page before the "---More---" prompt appears for Telnet sessions, use the **terminal pager** command in privileged EXEC mode.

terminal 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		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.

Usage Guidelines

This command changes the pager line setting only for the current Telnet session. However, the ASA re-initiates the pager value in the current session from the running-config only when you enter the **login** command in user EXEC mode or enter the **enable** command to enter privileged EXEC mode. This is as-designed.

Note An unexpected "--- More---" prompt occurs before the ASA redisplays the user prompt, which may have suppressed the output of the **banner exec** command. Use the **banner motd** command or **banner login** command instead.

To save a new default pager setting to the configuration, do the following:

1. Access the user EXEC mode by entering the **login** command or access the privileged EXEC mode by entering the **enable** command.

2. Enter the **pager** command.

If you use Telnet to access 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# terminal pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the “---More---” prompt. This command is saved to the configuration.
show running-config terminal	Displays the current terminal settings.
terminal	Allows syslog messages to display in the Telnet session.
terminal width	Sets the terminal display width in global configuration mode.

terminal width

To set the width for displaying information during console sessions, use the **terminal width** command in global configuration mode. To disable, use the **no** form of this command.

terminal width *columns*
no terminal width *columns*

Syntax Description

columns	Specifies the terminal width in columns. The default is 80. The range is 40 to 511.

Command Default

The default display width is 80 columns.

Command Modes

The 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.

Examples

This example shows how to terminal display width to 100 columns:

```
ciscoasa# terminal width 100
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Sets the terminal line parameters in privileged EXEC mode.

test aaa-server

To check whether the ASA can authenticate or authorize users with a particular AAA server, use the **test aaa-server** command in privileged EXEC mode. Failure to reach the AAA server may be due to incorrect configuration on the ASA, or the AAA server may be unreachable for other reasons, such as restrictive network configurations or server downtime.

test aaa-server { **authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*] [**ad-agent**] }

Syntax Description

ad-agent	Tests connectivity to the AAA AD agent server.
authentication	Tests a AAA server for authentication capability.
authorization	Tests a AAA server for legacy VPN authorization capability.
host *ip_address*	Specifies the server IP address. If you do not specify the IP address in the command, you are prompted for it.
password *password*	Specifies the user password. If you do not specify the password in the command, you are prompted for it.
server_tag	Specifies the AAA server tag as set by the **aaa-server** command.
username *username*	Specifies the username of the account used to test the AAA server settings. Make sure the username exists on the AAA server; otherwise, the test will fail. If you do not specify the username in the command, you are prompted for it.

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(4)	This command was added.
8.4(2)	The **ad-agent** keyword was added.

Usage Guidelines

The **test aaa-server** command lets you verify that the ASA can authenticate users with a particular AAA server, and for legacy VPN authorization, if you can authorize a user. This command lets you test the AAA server without having an actual user who attempts to authenticate or authorize. It also helps you isolate whether

AAA failures are due to misconfiguration of AAA server parameters, a connection problem to the AAA server, or other configuration errors on the ASA.

Examples

The following example configures a RADIUS AAA server named srvgrp1 on host 192.168.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650. The **test aaa-server** command following the setup of the AAA server parameters indicates that the authentication test failed to reach the server.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
test aaa-server authentication svrgrp1
Server IP Address or name:
192.168.3.4
Username:
bogus
Password:
mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

The following is sample output from the **test aaa-server** command with a successful outcome:

```
ciscoasa# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

Related Commands

Command	Description
aaa authentication console	Configures authentication for management traffic.
aaa authentication match	Configures authentication for through traffic.
aaa-server	Creates a AAA server group.
aaa-server host	Adds a AAA server to a server group.

test aaa-server ad-agent

To test the Active Directory Agent configuration after you configure, use the **test aaa-server ad-agent** command in AAA Server Group configuration mode.

test aaa-server ad-agent

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
Aaa server group configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

To configure the Active Directory Agent for the Identity Firewall, you must enter the **ad-agent-mode** command, which is a submode of the **aaa-server** command. Entering the **ad-agent-mode** command enters the AAA Server Group configuration mode.

After configuring the Active Directory Agent, enter the **test aaa-server ad-agent** command to verify that the ASA has a functional connection to the Active Directory Agent.

Periodically or on-demand, the AD Agent monitors the Active Directory server security event log file via WMI for user login and logoff events. The AD Agent maintains a cache of user ID and IP address mappings. and notifies the ASA of changes.

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between ASA and AD Agent.

Examples

The following example shows how to enable **ad-agent-mode** while configuring the Active Directory Agent for the Identity Firewall and then test the connection:

```
hostname(config)# aaa-server adagent protocol radius
hostname(config)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
hostname(config-aaa-server-host)# key mysecret
hostname(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
hostname(config-aaa-server-host)# test aaa-server ad-agent
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

test dynamic-access-policy attributes

To enter the dap attributes mode, from Privileged EXEC mode, enter the **test dynamic-access-policy attributes** command. Doing so lets you specify user and endpoint attribute value pairs.

dynamic-access-policy attributes

Command Default

No default value or behaviors.

Command Modes

The 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
8.0(2)	This command was added.

Usage Guidelines

Normally the ASA retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The ASA writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record.

This feature lets you experiment with creating a DAP record.

Examples

The following example shows how to use the **attributes** command.

```
ciscoasa
 #
test dynamic-access-policy attributes
ciscoasa
(config-dap-test-attr)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
attributes	Enters attributes mode, in which you can specify user attribute value pairs.
display	Displays current attribute list.

test dynamic-access-policy execute

To test already configured DAP records, use the test dynamic-access-policy execute command in privileged EXEC mode:

test dynamic-access-policy execute

Syntax Description

AAA attribute value	The DAP subsystem on the device references these values when evaluating the AAA and endpoint selection attributes for each record. • AAA Attribute—Identifies the AAA attribute. • Operation Value—Identifies the attribute as =/!= to the given value.
endpoint attribute value	Identifies the endpoint attribute. • Endpoint ID—Provides the endpoint attribute ID. • Name/Operation/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
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(4)	This command was added.

Usage Guidelines

This command lets you test the retrieval of the set of DAP records configured on the device by specifying authorization attribute value pairs.

test regex

To test a regular expression, use the **test regex** command in privileged EXEC mode.

test regex *input_text regular_expression*

Syntax Description

input_text	Specifies the text that you want to match with the regular expression.
regular_expression	Specifies the regular expression up to 100 characters in length. See the **regex** command 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **test regex** command tests a regular expression to make sure it matches what you think it will match.

If the regular expression matches the input text, you see the following message:

```
INFO: Regular expression match succeeded.
```

If the regular expression does not match the input text, you see the following message:

```
INFO: Regular expression match failed.
```

Examples

The following example tests input text against a regular expression:

```
ciscoasa# test
 regex farscape scape
INFO: Regular expression match succeeded.
ciscoasa# test
 regex farscape scaper
INFO: Regular expression match failed.
```

Related Commands

Command	Description
class-map type inspect	Creates an 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.
regex	Creates a regular expression.

test sso-server (Deprecated)

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

To test an SSO server with a trial authentication request, use the **test sso-server** command in privileged EXEC mode.

test sso-server *server-name* **username** *user-name*

Syntax Description

server-name	Specifies the name of the SSO server being tested.
user-name	Specifies the name of a user on the SSO server being tested.

Command Default

No default values 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
Config-webvpn	• Yes	—	• Yes	—	—
Config-webvpn-sso-saml	• Yes	—	• Yes	—	—
Config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—
Global configuration mode	• Yes	—	• Yes	—	—
Privileged EXEC	• 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 **test sso-server** command tests whether an SSO server is recognized and responding to authentication requests.

If the SSO server specified by the *server-name* argument is not found, the following error appears:

ERROR: sso-server *server-name* does not exist

If the SSO server is found but the user specified by the *user-name* argument is not found, the authentication is rejected.

In the authentication, the ASA acts as a proxy for the WebVPN user to the SSO server. The ASA currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. This command applies to both types of SSO Servers.

Examples

The following example, entered in privileged EXEC mode, successfully tests an SSO server named my-sso-server using a username of Anyuser:

```
ciscoasa# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
ciscoasa#
```

The following example shows a test of the same server, but the user, Anotheruser, is not recognized and the authentication fails:

```
ciscoasa# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
ciscoasa#
```

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.
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.

text-color

To set a color for text in the WebVPN title bar on the login, home page, and file access page, use the **text-color** command in webvpn mode. To remove a text color from the configuration and reset the default, use the no form of this command.

text-color [*black* | *white* | *auto*]
no text-color

Syntax Description

auto	Chooses black or white based on the settings for the secondary-color command. That is, if the secondary color is black, this value is white.
black	The default text color for title bars is white.
white	You can change the color to black.

Command Default

The default text color for the title bars is 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
config-webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set the text color for title bars to black:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# text-color black
```

Related Commands

Command	Description
secondary-text-color	Sets the secondary text color for the WebVPN login, home page, and file access page.

tftp blocksize

To configure the TFTP blocksize value, use **tftp blocksize** command in global configuration mode. To remove the blocksize configuration, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

tftp blocksize *number*
no tftp blocksize

Syntax Description

number	Specifies the blocksize value to be configured. This value can be between 513 and 8192 octets. A new default value is set for the blocksize—1456 octets.

Command Default

The new default value is 1456 octets. If the server does not supported this negotiation, the old default value—512 octets size prevail.

Command Modes

The 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
9.13(1)	This command was added.

Usage Guidelines

The **tftp blocksize** command allows you to configure a larger blocksize to enhance the tftp file transfer speed. This configurable blocksize value option is appended to tftp read/write request and sent to tftp server for acknowledgement. On receiving the Option Acknowledgment (OACK), the file transfer is initiated with the configured blocksize value. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets.

The **show running-configuration** command displays the configured blocksize value, except the default value.

Examples

The following example shows how to specify a TFTP blocksize value:

```
ciscoasa(config)# tftp blocksize 2048
ciscoasa(config)#
```

Related Commands

Command	Description
show running-config tftp blocksize	Displays the configured blocksize value, except the default value.

tftp-server

To specify the default TFTP server and path and filename for use with **configure net** or **write net** commands, use the **tftp-server** command in global configuration mode. To remove the server configuration, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

tftp-server *interface_name server filename*
no tftp-server [*interface_name server filename*]

Syntax Description

filename	Specifies the path and filename.
interface_name	Specifies the gateway interface name. If you specify an interface other than the highest security interface, a warning message informs you that the interface is unsecure.
server	Sets the TFTP server IP address or name. You can enter an IPv4 or 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
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	The gateway interface is now required.

Usage Guidelines

The **tftp-server** command simplifies entering the **configure net** and **write net** commands. When you enter the **configure net** or **write net** commands, you can either inherit the TFTP server specified by the **tftp-server** command, or provide your own value. You can also inherit the path in the **tftp-server** command as-is, add a path and filename to the end of the **tftp-server** command value, or override the **tftp-server** command value.

The ASA supports only one **tftp-server** command.

Examples

The following example shows how to specify a TFTP server and then read the configuration from the /temp/config/test_config directory:

```
ciscoasa(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
ciscoasa(config)# configure net
```

Related Commands

Command	Description
configure net	Loads the configuration from the TFTP server and path that you specify.
show running-config tftp-server	Displays the default TFTP server address and the directory of the configuration file.

tftp-server address (Deprecated)

To specify the TFTP servers in the cluster, use the **tftp-server address** command in phone-proxy configuration mode. To remove the TFTP server from the Phone Proxy configuration, use the **no** form of this command.

tftp-server address *ip_address* [*port*] **interface** *interface*
no tftp-server address *ip_address* [*port*] **interface** *interface*

Syntax Description

ip_address	Specifies the address of the TFTP server.
interface *interface*	Specifies the interface on which the TFTP server resides. This must be the real address of the TFTP server.
port	(Optional) This is the port the TFTP server is listening in on for the TFTP requests. This should be configured if it is not the default TFTP port 69.

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
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

The Phone Proxy must have at least one CUCM TFTP server configured. Up to five TFTP servers can be configured for the Phone Proxy.

The TFTP server is assumed to be behind the firewall on the trusted network; therefore, the Phone Proxy intercepts the requests between the IP phones and TFTP server. The TFTP server must reside on the same interface as the CUCM.

Create the TFTP server using the internal IP address and specify the interface on which the TFTP server resides.

On the IP phones, the IP address of the TFTP server must be configured as follows:

- If NAT is configured for the TFTP server, use the TFTP server's global IP address.
- If NAT is not configured for the TFTP server, use the TFTP server's internal IP address.

If the service-policy is applied globally, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on all ingress interfaces, except for the interface on which the TFTP server resides. When the service-policy is applied on a specific interface, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on that specified interface to the phone-proxy module.

If a NAT rule is configured for the TFTP server, it must be configured prior to applying the service-policy so that the global address of the TFTP server is used when installing the classification rule.

Examples

The following example shows the use of the **tftp-server address** command to configure two TFTP servers for the Phone Proxy:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.2 in interface outside
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.3 in interface outside
ciscoasa
(config-phone-proxy)#
media-termination address
192.168.1.4
 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address
192.168.1.25
 interface outside
ciscoasa
(config-phone-proxy)#
tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
ctl-file asactl
ciscoasa
(config-phone-proxy)#
cluster-mode nonsecure
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

threat-detection basic-threat

To enable basic threat detection, use the **threat-detection basic-threat** command in global configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection basic-threat
no threat-detection basic-threat

Syntax Description

This command has no arguments or keywords.

Basic threat detection is enabled by default. The following default rate limits are used:

Table 1: Basic Threat Detection Default Settings

Packet Drop Reason	Trigger Settings	
Average Rate	Burst Rate	
• DoS attack detected • Bad packet format • Connection limits exceeded • Suspicious ICMP packets detected	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 20 second period.
	80 drops/sec over the last 3600 seconds.	320 drops/sec over the last 120 second period.
Scanning attack detected	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
	4 drops/sec over the last 3600 seconds.	8 drops/sec over the last 120 second period.
Incomplete session detected such as TCP SYN attack detected or UDP session with no return data attack detected (combined)	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 20 second period.
	80 drops/sec over the last 3600 seconds.	160 drops/sec over the last 120 second period.
Denial by access lists	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	640 drops/sec over the last 120 second period.
• Basic firewall checks failed • Packets failed application inspection	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	1280 drops/sec over the last 120 second period.

Packet Drop Reason	Trigger Settings	
Interface overload	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 20 second period.
	1600 drops/sec over the last 3600 seconds.	6400 drops/sec over the last 120 second period.

Command Modes

The 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.
8.2(1)	The burst rate interval was changed from 1/60th to 1/30th of the average rate.

Usage Guidelines

When you enable basic threat detection, the ASA monitors the rate of dropped packets and security events due to the following reasons:

- Denial by access lists
- Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length)
- Connection limits exceeded (both system-wide resource limits, and limits set in the configuration)
- DoS attack detected (such as an invalid SPI, Stateful Firewall check failure)
- Basic firewall checks failed (This option is a combined rate that includes all firewall-related packet drops in this bulleted list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.)
- Suspicious ICMP packets detected
- Packets failed application inspection
- Interface overload
- Scanning attack detected (This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.)
- Incomplete session detection such as TCP SYN attack detected or UDP session with no return data attack detected

When the ASA detects a threat, it immediately sends a system log message (733100) and alerts Adaptive Security Device Manager (ASDM).

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 1.1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command. You can override the default settings for each type of event by using the **threat-detection rate** command.

If an event rate is exceeded, then the ASA sends a system message. The ASA tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst event rate is 1/30th of the average rate interval or 10 seconds, whichever is higher. For each event received, the ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate
 60 burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can change the default rate limits for each event type using the **threat-detection rate** command in global configuration mode. If you enable scanning threat detection using the **threat-detection scanning-threat** command, then this command with the **scanning-threat** keyword also sets the when a host is considered to be an attacker or a target; otherwise the default **scanning-threat** value is used for both basic and scanning threat detection. To return to the default setting, use the **no** form of this command.

threat-detection rate { **acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack** } **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*
no threat-detection rate { **acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack** } **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

Syntax Description

acl-drop	Sets the rate limit for dropped packets caused by denial by access lists.
average-rate *av_rate*	Sets the average rate limit between 0 and 2147483647 in drops/sec.
bad-packet-drop	Sets the rate limit for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
burst-rate *burst_rate*	Sets the burst rate limit between 0 and 2147483647 in drops/sec. The burst rate is calculated as the average rate every *N* seconds, where *N* is the burst rate interval. The burst rate interval is 1/30th of the **rate-interval** *rate_interval* value or 10 seconds, whichever is larger.
conn-limit-drop	Sets the rate limit for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	Sets the rate limit for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	Sets the rate limit for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop** , **inspect-drop** , and **scanning-threat** .
icmp-drop	Sets the rate limit for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	Sets the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	Sets the rate limit for dropped packets caused by an interface overload.
rate-interval *rate_interval*	Sets the average rate interval between 600 seconds and 2592000 seconds (30 days). The rate interval is used to determine the length of time over which to average the drops. It also determines the burst threshold rate interval.

scanning-threat	Sets the rate limit for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	Sets the rate limit for dropped packets caused by an incomplete session, such as TCP SYN attack or UDP session with no return data attack.

Command Default

When you enable basic threat detection using the **threat-detection basic-threat** command, the following default rate limits are used:

Table 2: Basic Threat Detection Default Settings

Packet Drop Reason	Trigger Settings	
Average Rate	Burst Rate	
• **dos-drop**	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 20 second period.
• **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	100 drops/sec over the last 3600 seconds.	400 drops/sec over the last 120 second period.
scanning-threat	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
	5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 120 second period.
syn-attack	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 20 second period.
	100 drops/sec over the last 3600 seconds.	200 drops/sec over the last 120 second period.
acl-drop	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 20 second period.
	400 drops/sec over the last 3600 seconds.	800 drops/sec over the last 120 second period.
• **fw-drop** • **inspect-drop**	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 20 second period.
	400 drops/sec over the last 3600 seconds.	1600 drops/sec over the last 120 second period.
interface-drop	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 20 second period.
	2000 drops/sec over the last 3600 seconds.	8000 drops/sec over the last 120 second period.

Command Modes

The 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.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.

Usage Guidelines

You can configure up to three different rate intervals for each event type.

When you enable basic threat detection, the ASA monitors the rate of dropped packets and security events due to the event types described in the "Syntax Description" table.

When the ASA detects a threat, it immediately sends a system log message (733100) and alerts ASDM.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 1.1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command.

If an event rate is exceeded, then the ASA sends a system message. The ASA tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event received, the ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate
            60 burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection scanning-threat

To enable scanning threat detection, use the **threat-detection scanning-threat** command in global configuration mode. To disable scanning threat detection, use the **no** form of this command.

threat-detection scanning-threat [**shun** [**except** { **ip-address** *ip_address mask* | **object-group** *network_object_group_id* } | **duration** *seconds*]]
no threat-detection scanning-threat [**shun** [**except** { **ip-address** *ip_address mask* | **object-group** *network_object_group_id* } | **duration** *seconds*]]

Syntax Description

duration *seconds*	Sets the duration of a shun for an attacking host, between 10 and 2592000 seconds. The default length is 3600 seconds (1 hour).
except	Exempts IP addresses from being shunned. Enter this command multiple times to identify multiple IP addresses or network object groups to exempt from shunning.
ip-address *ip_address mask*	Specifies the IP address you want to exempt from shunning.
object-group *network_object_group_id*	Specifies the network object group that you want to exempt from shunning. See the **object-group network** command to create the object group.
shun	Automatically terminates a host connection when the ASA identifies the host as an attacker, in addition to sending syslog message 733101.

Command Default

The default shun duration is 3600 seconds (1 hour).

The following default rate limits are used for scanning attack events:

Table 3: Default Rate Limits for Scanning Threat Detection

Average Rate	Burst Rate
5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 120 second period.

Command Modes

The 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.
8.0(4)	The **duration** keyword was added.

Usage Guidelines

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the ASA scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

Caution The scanning threat detection feature can affect the ASA performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

You can configure the ASA to send system log messages about an attacker or you can automatically shun the host. By default, the system log message 730101 is generated when a host is identified as an attacker.

The ASA identifies attackers and targets when the scanning threat event rate is exceeded. The ASA tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event detected that is considered to be part of a scanning attack, the ASA checks the average and burst rate limits. If either rate is exceeded for traffic sent from a host, then that host is considered to be an attacker. If either rate is exceeded for traffic received by a host, then that host is considered to be a target. You can change the rate limits for scanning threat events using the **threat-detection rate scanning-threat** command.

To view hosts categorized as attackers or as targets, use the **show threat-detection scanning-threat** command.

To view shunned hosts, use the **show threat-detection shun** command. To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following example enables scanning threat detection and automatically shuns hosts categorized as attackers, except for hosts on the 10.1.1.0 network. The default rate limits for scanning threat detection are also changed.

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
 burst-rate 20
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
 burst-rate 20
```

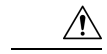
Related Commands

Command	Description
clear threat-detection shun	Releases a host from being shunned.
show threat-detection scanning-threat	Shows the hosts that are categorized as attackers and targets.

Command	Description
show threat-detection shun	Shows hosts that are currently shunned.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.

threat-detection statistics

To enable advanced threat detection statistics, use the **threat-detection statistics** command in global configuration mode. To disable advanced threat detection statistics, use the **no** form of this command.



Caution Enabling statistics can affect the ASA performance, depending on the type of statistics enabled. The **threat-detection statistics host** command affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. The **threat-detection statistics port** command, however, has modest impact.

threat-detection statistics [**access-list** | [**host | port | protocol** [**number-of-rate** { **1 | 2 | 3** }] | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]
no threat-detection statistics [**access-list | host | port | protocol | tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

Syntax Description

access-list	(Optional) Enables statistics for access list denies. Access list statistics are only displayed using the **show threat-detection top access-list** command.
average-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.
burst-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
host	(Optional) Enables host statistics. The host statistics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
number-of-rate { **1** | **2** | **3** }	(Optional) Sets the number of rate intervals maintained for host, port, or protocol statistics. The default number of rate intervals is **1** , which keeps the memory usage low. To view more rate intervals, set the value to **2** or **3** . For example, if you set the value to **3** , then you view data for the last 1 hour, 8 hours, and 24 hours. If you set this keyword to **1** (the default), then only the shortest rate interval statistics are maintained. If you set the value to **2** , then the two shortest intervals are maintained.
port	(Optional) Enables port statistics.
protocol	(Optional) Enables protocol statistics.
rate-interval *minutes*	(Optional) For TCP Intercept, sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the ASA samples the number of attacks 30 times.

tcp-intercept	(Optional) Enables statistics for attacks intercepted by TCP Intercept. See the **set connection embryonic-conn-max command** , or the **nat** or **static** commands to enable TCP Intercept.

Command Default

Access list statistics are enabled by default. If you do not specify any options in this command, then you enable all options.

The default **tcp-intercept rate-interval** is 30 minutes. The default **burst-rate** is 400 per second. The default **average-rate** is 200 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
8.0(2)	This command was added.
8.0(4)/8.1(2)	The **tcp-intercept** keyword was added.
8.1(2)	The **number-of-rates** keyword was added for host statistics, and the default number of rates was changed from 3 to 1.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.3(1)	The **number-of-rates** keyword was added for port and protocol statistics, and the default number of rates was changed from 3 to 1.

Usage Guidelines

If you do not specify any options in this command, then you enable all statistics. To enable only certain statistics, enter this command for each statistic type, and do not also enter the command without any options. You can enter **threat-detection statistics** (without any options) and then customize certain statistics by entering the command with statistics-specific options (for example, **threat-detection statistics host number-of-rate 2**). If you enter **threat-detection statistics** (without any options) and then enter a command for specific statistics, but without any statistic-specific options, then that command has no effect because it is already enabled.

If you enter the **no** form of this command, it removes all **threat-detection statistics** commands, including the **threat-detection statistics access-list** command, which is enabled by default.

View statistics using the **show threat-detection statistics** commands.

You do not need to enable scanning threat detection using the **threat-detection scanning-threat** command; you can configure detection and statistics separately.

Examples

The following example enables scanning threat detection and scanning threat statistics for all types except host:

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection statistics access-list
ciscoasa(config)# threat-detection statistics port
ciscoasa(config)# threat-detection statistics protocol
ciscoasa(config)# threat-detection statistics tcp-intercept
```

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics host	Shows the host statistics.
show threat-detection memory	Shows the memory use for advanced threat detection statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

threshold

To set the threshold value for over threshold events in SLA monitoring operations, use the **threshold** command in SLA monitor configuration mode. To restore the default value, use the **no** form of this command.

threshold *milliseconds*
no threshold

Syntax Description

milliseconds	Specifies the number of milliseconds for a rising threshold to be declared. Valid values are from 0 to 2147483647. This value should not be larger than the value set for the timeout.

Command Default

The default threshold is 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
SLA monitor configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The threshold value is only used to indicate over threshold events, which do not affect reachability but may be used to evaluate the proper settings for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
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
sla monitor	Defines an SLA monitoring operation.

Command	Description
timeout	Defines the amount of time the SLA operation waits for a response.

throughput level

To set the throughput level for the smart licensing entitlement request, use the **throughput level** command in license smart configuration mode. To remove the throughput level and unlicense your device, use the **no** form of this command.

Note This feature is supported on the ASA virtual only.

throughput level { **100M | 1G | 2G** }
no throughput level [**100M | 1G | 2G**]

Syntax Description

100M	Sets the throughput level to 100 Mbps.
1G	Sets the throughput level to 1 Gbps.
2G	Sets the throughput level to 2 Gbps.

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
License smart configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

When you request or change the throughput level, 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.

ticket (Deprecated)

To configure the ticket epoch and password for the Cisco Intercompany Media Engine proxy, use the **ticket** command in UC-IME configuration mode. To remove the configuration from the proxy, use the **no** form of this command.

ticket epoch *n* **password** *password*
no ticket epoch *n* **password** *password*

Syntax Description

n	Specifies the length of time between password integrity checks. Enter an integer from 1-255.
password	Sets the password for the Cisco Intercompany Media Engine ticket. Enter a minimum of 10 and a maximum of 64 printable character from the US-ASCII character set. The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. Only one password can be configured at a time.

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
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

Configures the ticket epoch and password for Cisco Intercompany Media Engine.

The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password.

Typically, you increment the epoch sequentially; however, the ASA allows you to choose any value when you update the epoch.

If you change the epoch value, the current password is invalidated and you must enter a new password.

We recommend a password of at least 20 characters. Only one password can be configured at a time.

The ticket password is stored onto flash. The output of the **show running-config uc-ime** command displays ***** instead of the password string.

Note The epoch and password that you configure on the ASA must match the epoch and password configured on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

Examples

The following example shows specify the ticket and epoch in the Cisco Intercompany Media Engine Proxy:

```
ciscoasa
(config)# uc-ime local_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
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

Related Commands

Command	Description
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
uc-ime	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

timeout (aaa-server host)

To specify the length of time during which the ASA attempts to make a connection to a AAA server, use the **timeout** command in aaa-server host mode. To remove the timeout value and reset the timeout to the default value of 10 seconds, use the **no** form of this command.

timeout *seconds*
no timeout

Syntax Description

seconds	Specifies the timeout interval (1-300 seconds) for the server. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. If the number of consecutive failed transactions reaches the limit specified on the **max-failed-attempts** command in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Command Default

The default timeout value 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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid for all AAA server protocol types.

Use the **retry-interval** command to specify the amount of time the ASA waits between connection attempts. These intervals happen within the overall timeout, so if you have a long retry interval, the system will be able to make fewer retry attempts within the overall timeout. In practice, the retry interval should be less than the timeout interval.

Use the **max-failed-attempts** command to specify the maximum number of consecutive failed AAA transactions before deactivating a failed server. A AAA transaction is a sequence of an initial request and all retries. For the RADIUS protocol, the initial request and all the retries have same RADIUS packet identifier in the RADIUS protocol header.

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host 10.2.3.4 to use a timeout value of 30 seconds, with a retry interval of 10 seconds.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
```

```
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 10.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 30
ciscoasa
(config-aaa-server-host)# retry-interval 10
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.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa	Displays the current AAA configuration values.

timeout (dns server-group)

To specify the amount of time to wait before trying the next DNS server, use the **timeout** command in dns server-group configuration mode. To restore the default timeout, use the **no** form of this command.

timeout *seconds*
no timeout [*seconds*]

Syntax Description

seconds	Specifies the timeout in seconds between 1 and 30. The default is 2 seconds. Each time the ASA retries the list of servers, this timeout doubles. Use the **retries** command in dns-server-group configuration mode to configure the number of retries.

Command Default

The default timeout is 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
Dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Examples

The following example sets the timeout to 1 second for the DNS server group “dnsgroup1”:

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# timeout 1
```

Related Commands

Command	Description
clear configure dns	Removes all user-created DNS server-groups and resets the default server group’s attributes to the default values.
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.
show running-config dns server-group	Shows the current running DNS server-group configuration.

timeout (global)

To set the global maximum idle time duration for various features, use the **timeout** command in global configuration mode. To set all timeouts to the default, use the **no** form of this command. To reset a single feature to its default, reenter the **timeout** command with the default value.

timeout { **conn | conn-holddown | floating-conn | h225 | h323 | half-closed | icmp | icmp-error | igp stale-route | mgcp | mgcp-pat | pat-xlate | sctp | sip | sip-disconnect | sip-invite | sip_media | sip-provisional-media | sunrpc | tcp-proxy-reassembly | udp | xlate** } *hh:mm:ss*
timeout uauth *hh:mm:ss* [**absolute | inactivity**]
no timeout

Syntax Description

absolute	(Optional for **uauth**) Requires a reauthentication after the uauth timeout expires. The **absolute** keyword is enabled by default. To set the uauth timer to timeout after a period of inactivity, enter the **inactivity** keyword instead.
conn	Specifies the idle time after which a connection closes, between 0:5:0 and 1193:0:0. The default is 1 hour (1:0:0). Use 0 to never time out a connection.
conn-holddown	How long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. The purpose of the connection holddown timer is to reduce the effect of route flapping, where routes might come up and go down quickly. You can reduce the holddown timer to make route convergence happen more quickly. The default is 15 seconds, the range is 00:00:00 to 00:00:15.
floating-conn	When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0.
hh:*mm*:*ss*	Specifies the timeout in hours, minutes, and seconds. Use 0 to never time out a connection, if available.
h225	Specifies the idle time after which an H.225 signaling connection closes, between 0:0:0 and 1193:0:0. The default is 1 hour (1:0:0). A timeout value of 0:0:1 disables the timer and closes the TCP connection immediately after all calls are cleared.
h323	Specifies the idle time after which H.245 (TCP) and H.323 (UDP) media connections close, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.

half-closed	Specifies the idle time after which a TCP half-closed connection will be freed, between 0:5:0 (for 9.1(1) and earlier) or 0:0:30 (for 9.1(2) and later) and 1193:0:0. The default is 10 minutes (0:10:0). Use 0 to never time out a connection. A connection is considered half-closed if both the FIN and FIN-ACK have been seen. If only the FIN has been seen, the regular **conn** timeout applies.
icmp	Specifies the idle time for ICMP, between 0:0:2 and 1193:0:0 The default is 2 seconds (0:0:2).
icmp-error	Specifies the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet, between 0:0:0 and 0:1:0 or the **timeout icmp** value, whichever is lower. The default is **0** (disabled). When this timeout is disabled, and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors.
igp stale-route	Specifies the idle time for how long to keep a stale route before removing it from the router information base. These routes are for interior gateway protocols such as OSPF. The default is 70 seconds (00:01:10), the range is 00:00:10 to 00:01:40.
inactivity	(Optional for **uauth**) Requires uauth reauthentication after the inactivity timeout expires.
mgcp	Sets the idle time after which an MGCP media connection is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0)
mgcp-pat	Sets the absolute interval after which an MGCP PAT translation is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0).
pat-xlate	Specifies the idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.
sctp	Specifies the idle time until a Stream Control Transmission Protocol (SCTP) connection closes, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).
sip	Specifies the idle time after which a SIP control connection will be closed, between 0:5:0 and 1193:0:0. The default is 30 minutes (0:30:0). Use 0 to never time out a connection.
sip-disconnect	Specifies the idle time after which a SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 00:10:0. The default is 2 minutes (0:2:0).
sip-invite	(Optional) Specifies the idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 1193:0:0. The default is 3 minutes (0:3:0).

sip_media	Specifies the idle time after which a SIP media connection will be closed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use 0 to never time out a connection. The SIP media timer is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
sip-provisional-media	Specifies timeout value for SIP provisional media connections, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).
sunrpc	Specifies the idle time after which a SUNRPC slot will be closed, between 0:1:0 and 1193:0:0. The default is 10 minutes (0:10:0). Use 0 to never time out a connection.
tcp-proxy-reassembly	Configures the idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).
uauth	Specifies the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The default timer is **absolute**; you can set the timeout to occur after a period of inactivity by entering the **inactivity** keyword. The **uauth** duration must be shorter than the **xlate** duration. Set to 0 to disable caching. Do not use **0** if passive FTP is used for the connection or if the **virtual http** command is used for web authentication.
udp	Specifies the idle time until a UDP slot is freed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use 0 to never time out a connection.
xlate	Specifies the idle time until a translation slot is freed, between 0:1:0 and 1193:0:0. The default is 3 hours (3:0:0).

Command Default

The defaults are as follows:

conn is 1 hour (**1:0:0**).

- **conn-holddown** is 15 seconds (**0:0:15**)
- **floating-conn** never times out (**0**)
- **h225** is 1 hour (**1:0:0**).
- **h323** is 5 minutes (**0:5:0**).
- **half-closed** is 10 minutes (**0:10:0**).
- **icmp** is 2 seconds (**0:0:2**)
- **icmp-error** never times out (**0**)
- **igp stale-route** is 70 seconds (**00:01:10**)
- **mgcp** is 5 minutes (**0:5:0**).
- **mgcp-pat** is 5 minutes (**0:5:0**).
- **rpc** is 5 minutes (**0:5:0**).
- **sctp** is 2 minutes (**0:2:0**).

- **sip** is 30 minutes (**0:30:0**).
- **sip-disconnect** is 2 minutes (**0:2:0**).
- **sip-invite** s 3 minutes (**0:3:0**).
- **sip_media** is 2 minutes (**0:2:0**).
- **sip-provisional-media** is 2 minutes (**0:2:0**).
- **sunrpc** is 10 minutes (**0:10:0**)
- **tcp-proxy-reassembly** is 1 minute (**0:1:0**)
- **uauth** is 5 minutes (**0:5:0**) **absolute**.
- **udp** is 2 minutes (**0:02:0**).
- **xlate** is 3 hours (**3:0:0**).

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 mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	The **mgcp-pat,** sip-disconnect, and sip-invite keywords were added.
7.2(4)/8.0(4)	The **sip-provisional-media** keyword was added.
7.2(5)/8.0(5)/8.1(2)/8.2(1)	The **tcp-proxy-reassembly** keyword was added.
8.2(5)/8.4(2)	The **floating-conn** keyword was added.
8.4(3)	The **pat-xlate** keyword was added.
9.1(2)	The minimum **half-closed** value was lowered to 30 seconds (0:0:30).
9.4(3)/9.6(2)	The **conn-holddown** keyword was added.
9.5(2)	The **sctp** keyword was added.
9.7(1)	The **igp stale-route** keyword was added.
9.8(1)	The **icmp-error** keyword was added.

Usage Guidelines

The **timeout** command lets you set global timeouts. For some features, the **set connection timeout** command takes precedence for traffic identified in the command.

You can enter multiple keywords and values after the **timeout** command.

The connection timer (**conn**) takes precedence over the translation timer (**xlate**); the translation timer works only after all connections have timed out.

Examples

The following example shows how to configure the maximum idle time durations:

```
ciscoasa(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
ciscoasa(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00
sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

Related Commands

Command	Description
clear configure timeout	Clears the timeout configuration and resets it to the defaults.
set connection timeout	Sets connection timeouts using Modular Policy Framework.
show running-config timeout	Displays the timeout value of the designated protocol.

timeout (policy-map type inspect gtp > parameters)

To change the inactivity timers for a GTP session, use the **timeout** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect gtp** command. Use the **no** form of this command to set these intervals to their default values.

timeout { **endpoint | gsn | pdp-context | request | signaling | t3-response | tunnel** } *hh:mm:ss*
no timeout { **endpoint | gsn | pdp-context | request | signaling | t3-response | tunnel** } *hh:mm:ss*

Syntax Description

hh:*mm*:*ss*	The idle timeout for the specified service (in hour:minute:second format). To have no timeout, specify 0 for the number.
endpoint	The maximum period of inactivity before a GTP endpoint is removed.
gsn	The maximum period of inactivity before a GSN is removed. Starting in 9.5(1), this keyword is removed and replaced by the **endpoint** keyword.
pdp-context	The maximum period of inactivity before removing the PDP context for a GTP session. In GTPv2, this is the bearer context.
request	The maximum period of inactivity after which a request is removed from the request queue. Any subsequent responses to a dropped request will also be dropped.
signaling	The maximum period of inactivity before GTP signaling is removed.
t3-response	The maximum wait time for a response before removing the connection.
tunnel	The maximum period of inactivity for the GTP tunnel before it is torn down.

Command Default

The default is 30 minutes for **endpoint**, **gsn**, **pdp-context**, and **signaling**.

The default for **request** is 1 minute.

The default for **tunnel** is 1 hour (in the case where a Delete PDP Context Request is not received).

The default for **t3-response** is 20 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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Release	Modification
9.5(1)	The **gsn** keyword was replaced by **endpoint**.

Usage Guidelines

Use this command to change the default timeouts used in GTP inspection.

Examples

The following example sets a timeout value for the request queue of 2 minutes:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout request 00:02:00
```

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.

timeout (policy-map type inspect m3ua > parameters)

To change the inactivity timers for an M3UA session, use the **timeout** 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 set these intervals to their default values.

timeout { **endpoint | session** } *hh:mm:ss*
no timeout { **endpoint | session** } *hh:mm:ss*

Syntax Description

hh:mm:ss	The idle timeout for the specified service (in hour:minute:second format). To have no timeout, specify 0 for the number.
endpoint	The maximum period of inactivity before statistics for an M3UA endpoint are removed. The default is 30 minutes.
session	The idle timeout to remove an M3UA session if you enable strict ASP state validation, in hh:mm:ss format. The default is 30 minutes (00:30:00). Disabling this timeout can prevent the system from removing stale sessions.

Command Default

The default is 30 minutes for **endpoint** and **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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.
9.7(1)	The **session** keyword was added.

Usage Guidelines

Use this command to change the default timeouts used in M3UA inspection.

Examples

The following example sets a 45 minute timeout for endpoints.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
```

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.
strict-asp-state	Enables strict M3UA ASP state validation.

timeout (policy-map type inspect radius-accounting > parameters)

To change the inactivity timers for RADIUS accounting users, use the **timeout** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect radius-accounting** command. Use the **no** form of this command to set these intervals to their default values.

timeout users *hh:mm:ss*
no timeout users *hh:mm:ss*

Syntax Description

hh:mm:ss	This is the timeout where hh specifies the hour, mm specifies the minutes, ss specifies the seconds, and a colon (:) separates these three components. The value 0 means never tear down immediately. The default is one hour.
users	Specifies the timeout for users.

Command Default

The default timeout for users is one hour.

Command Modes

The 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 sets a timeout value for the user of ten minutes:

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout user 00:10:00
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

timeout (type echo)

To set the amount of time the SLA operation waits for a response to the request packets, use the **timeout** command in type echo configuration mode. You can access the type echo configuration mode by first entering the **sla monitor** command.To restore the default value, use the **no** form of this command.

timeout *milliseconds*
no timeout

Syntax Description

milliseconds	0 to 604800000.

Command Default

The default timeout value is 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
Type echo configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **frequency** command to set how often the SLA operation sends out the request packets and the **timeout** command to set how long the SLA operation waits to receive a response to those requests. The values specified for the **timeout** command cannot be greater than the value specified for the **frequency** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
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
frequency	Specifies the rate at which the SLA operation repeats.
sla monitor	Defines an SLA monitoring operation.

timeout assertion

To configure the SAML timeout, use the **timeout assertion** command in webvpn configuration mode:

timeout assertion *number of seconds*

Syntax Description

number of seconds	SAML IdP timeout, in seconds.

Command Default

The default is none, which means that NotBefore and NotOnOrAfter in the assertion determines the validity.

Command Modes

The 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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5.2	This command was added.

Usage Guidelines

If specified, this configuration overrides NotOnOrAfter if the sum of NotBefore and timeout-in-seconds is earlier than NotOnOrAfter. If not specified, NotBefore and NotOnOrAfter in the assertion is used to determine the validity. When you input a timeout value under config-webvpn-saml-idp, both assertion and the number of seconds value are mandatory.

Examples

The following example configures the clientless VPN base URL, SAML request signature, and SAML assertion timeout:

```
ciscoasa(config-webvpn-saml-idp)# base url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
```

ciscoasa(config-webvpn-saml-idp)# **timeout assertion 7200**

timeout edns

To configure 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, use the **timeout edns** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

timeout edns *hh:mm:ss*
no timeout edns *hh:mm:ss*

Syntax Description

hh:mm:ss	The idle timeout for a connection from the client to the Umbrella server (in hour:minute:second format), from 0:0:0 to 1193:0:0. The default is 0:02:00 (2 minutes). To have no timeout, specify 0 for the number.

Command Default

The default is 0:02:00 (2 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
Umbrella configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Examples

The following example sets a one minute idle timeout for connections from a client to the Umbrella server.

```
ciscoasa(config)# umbrella-global

ciscoasa(config)# timeout edns 0:1:0
```

Related Commands

Commands	Description
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
umbrella-global	Configures the Cisco Umbrella global parameters.

timeout pinhole

To configure the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes, use the **timeout pinhole** 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.

timeout pinhole *hh:mm:ss*
no timeout pinhole

Syntax Description

hh:mm:ss	The timeout for pinhole connections. Value is between 0:0:1 and 1193:0:0.

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 configure the pinhole timeout for pin hole connections in a DCERPC inspection policy map:

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
```

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.

timeout secure-phones (Deprecated)

To configure the idle timeout after which the secure-phone entry is removed from the Phone Proxy database, use the **timeout secure-phones** command in phone-proxy configuration mode. To set the timeout value back to the default of 5 minutes, use the **no** form of this command.

timeout secure-phones *hh:mm:ss*
no timeout secure-phones *hh:mm:ss*

Syntax Description

hh:mm:ss	Specifies the idle timeout after which the object is removed. The default is 5 minutes.

Command Default

The default value for secure phone 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	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Since secure phones always request a CTL file upon bootup, the Phone Proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). The entry's timestamp is updated for each registration refresh the Phone Proxy receives for SIP phones and KeepAlives for SCCP phones.

The default value for the **timeout secure-phones** command is 5 minutes. Specify a value that is greater than the maximum timeout value for SCCP KeepAlives and SIP Register refresh. For example, if the SCCP Keepalives are configured for 1 minute intervals and the SIP Register Refresh is configured for 3 minutes, configure this timeout value greater than 3 minutes.

Examples

The following example shows the use of the **timeout secure-phones** command to configure the Phone Proxy to timeout entries in the secure phone database after 3 minutes:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.2 in interface outside
ciscoasa
(config-phone-proxy)#
```

```
tftp-server address 192.168.1.3 in interface outside
ciscoasa
(config-phone-proxy)#
media-termination address 192.168.1.4
ciscoasa
(config-phone-proxy)#
tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
ctl-file asactl
ciscoasa(config-phone-proxy)# timeout secure-phones 00:03:00
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

time-range

To enter time-range configuration mode and define a time range that you can attach to traffic rules, or an action, use the **time-range** command in global configuration mode. To disable, use the **no** form of this command.

time-range *name*
no time-range *name*

Syntax Description

name Name of the time range. The name must be 64 characters or less.

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

Creating a time range does not restrict access to the device. The **time-range** command defines the time range only. After a time range is defined, you can attach it to traffic rules or an action.

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 time range relies on the system clock of the ASA; however, the feature works best with NTP synchronization.

Examples

The following example creates a time range named “New_York_Minute” and enters time range configuration mode:

```
ciscoasa(config)# time-range New_York_Minute
ciscoasa(config-time-range)#
```

After you have created a time range and entered time-range configuration mode, you can define time range parameters with the **absolute** and **periodic** commands. To restore default settings for the **time-range** command **absolute** and **periodic** keywords, use the **default** command in time-range configuration mode.

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** command to bind the time range to an ACL. The following example binds an ACL named “Sales” to a time range named “New_York_Minute”:

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
ciscoasa(config)#
```

See the **access-list extended** command for more information about ACLs.

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.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.

timers nsf wait

To adjust nsf wait timer, use the timers nsf wait command in router ospf configuration mode. To reset the OSPF timing defaults, use the no form of this command.

timers nsf wait *interval*
no timers nsf wait *interval*

Syntax Description

interval	Interface wait interval (in seconds) during NSF restart. The default is 20 seconds. The range is from 0 to 65535.

Command Default

The default value of nsf wait timer is 20 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
Router ospf configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known that all neighbors are listed in the packet, but the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. Use the **timer nsf wait** command to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds.

Examples

The following example shows configuration of the nsf wait interval in seconds:

```
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# timers ?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
router mode commands/options:
  wait  Interface wait interval during NSF restart
ciscoasa(config-router)# timers nsf wait ?
router mode commands/options:
  <1-65535>  Seconds
ciscoasa(config-router)# timers nsf wait 35
ciscoasa(config-router)#
```

timers bgp

To adjust BGP network timers, use the timers bgp command in router bgp configuration mode. To reset the BGP timing defaults, use the no form of this command.

timers bgp *keepalive holdtime* [*min-holdtime*]
no timers bgp *keepalive holdtime* [*min-holdtime*]

Syntax Description

keepalive	Frequency (in seconds) with which the Cisco IOS 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: 60 secondsholdtime: 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
Router bgp configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

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, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# timers bgp 70 130 100
```

timers lsa arrival

To set the minimum interval at which the ASA accepts the same LSA from OSPFv3 neighbors, use the **timers lsa arrival** command in IPv6 router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*
no timers lsa arrival *milliseconds*

Syntax Description

milliseconds	Specifies the minimum delay in milliseconds that must pass between acceptance of the same LSA that is arriving between neighbors. Valid values are from 0 to 600,000 milliseconds.

Command Default

The default is 1000 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
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to indicate the minimum interval that must pass between acceptance of the same LSA that is arriving from neighbors.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# timers lsa arrival 2000
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.

timers lsa-group-pacing

To specify the interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa-group-pacing *seconds*
no timers lsa-group-pacing [*seconds*]

Syntax Description

seconds	The interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged. Valid values are from 10 to 1800 seconds.

Command Default

The default interval is 240 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
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To change the interval at which the OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** *seconds* command. To return to the default timer values, use the **no timers lsa-group-pacing** command.

Examples

The following example sets the group processing interval of LSAs to 500 seconds:

```
ciscoasa(config-rtr)# timers lsa-group-pacing 500
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers spf	Specifies the shortest path first (SPF) calculation delay and hold time

timers pacing flood

To configure LSA flood packet pacing, use the **timers pacing flood** command in IPv6 router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*
no timers pacing flood *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds at which LSAs in the flooding queue are paced in-between updates. The configurable range is from 5 to 100 milliseconds.

Command Default

The default is 33 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
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure LSA flood packet pacing.

Examples

The following example configures LSA flood packet pacing updates to occur in 20-millisecond intervals for OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
timers pacing lsa-group	Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

timers pacing flood

To configure LSA flood packet pacing, use the **timers pacing flood** command in IPv6 router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*
no timers pacing flood *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds at which LSAs in the flooding queue are paced in-between updates. The configurable range is from 5 to 100 milliseconds.

Command Default

The default is 33 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
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure LSA flood packet pacing.

Examples

The following example configures LSA flood packet pacing updates to occur in 20-millisecond intervals for OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
timers pacing lsa-group	Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

timers pacing lsa-group

To specify the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged, use the **timers pacing lsa-group** command in IPv6 router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*
no timers pacing lsa-group [*seconds*]

Syntax Description

seconds	Specifies the number of seconds in the interval at which LSAs are collected into a group and refreshed, check summed, or aged. Valid values are from 10 to 1800 seconds.

Command Default

The default interval is 240 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
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to indicate the interval at which the OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

Examples

The following example configures OSPFv3 group packet pacing updates between LSA groups to occur in 300-seconds intervals for OSPFv3 routing process 1:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission

To configure link-state advertisement (LSA) retransmission packet pacing, use the timers pacing retransmission command in router configuration mode. To restore the default retransmission packet pacing value, use the no form of this command.

timers pacing retransmission *milliseconds*
no timers pacing retransmission

Syntax Description

milliseconds	Specifies the time interval in milliseconds at which LSAs in the retransmission queue are paced. Valid values are from 5 milliseconds to 200 milliseconds.

Command Default

The default interval is 66 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
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Configuring Open Shortest Path First (OSPF) retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue. This command allows you to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced. The default settings for OSPF packet retransmission pacing timers are suitable for the majority of OSPF deployments.

Note Do not change the packet retransmission pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers.

Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 55-millisecond intervals for OSPF routing process 1:

```
hostname(config)# router ospf 1
hostname(config-router)# timers pacing retransmission 55
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.

timers spf

To specify the shortest path first (SPF) calculation delay and hold time, use the **timers spf** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers spf *delay holdtime*
no timers spf [*delay holdtime*]

Syntax Description

delay	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds, from 1 to 65535.
holdtime	The hold time between two consecutive SPF calculations in seconds; valid values are from 1 to 65535.

Command Default

The defaults are as follows:

- *delay* is 5 seconds.
- *holdtime* 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
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

To configure the delay time between when the OSPF protocol receives a topology change and when it starts a calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** command. To return to the default timer values, use the **no timers spf** command.

Examples

The following example sets the SPF calculation delay to 10 seconds and the SPF calculation hold time to 20 seconds:

```
ciscoasa(config-router)# timers spf 10 20
ciscoasa(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers lsa-group-pacing	Specifies the interval at which OSPF link-state advertisements (LSAs) are collected and refreshed, checksummed, or aged.

timers throttle

To set rate-limiting values for Open Shortest Path First (OSPF) link-state advertisement (LSA) generation or SPF generation, use the timers throttle command in router ospf or ipv6 router ospf configuration mode. To restore the default values, use the no form of this command.

timers throttle { **lsa | spf** } *start-interval hold-interval max-interval*
no timers throttle { **lsa | spf** }

Syntax Description

lsa	Configures LSA throttling.
start-interval	Specifies the delay in milliseconds to generate the first occurrence of the LSA. Specifies the delay in milliseconds to receive a change to the SPF calculation. Specifies the minimum delay in milliseconds to generate the first occurrence of LSAs. **Note** The first instance of LSA is generated immediately after a local OSPF topology change. The next LSA is generated only after start-interval. Valid values are between 0 and 0 to 600,000 milliseconds. The default value is 0 milliseconds; the LSA is sent immediately.
hold-interval	Specifies the maximum delay in milliseconds to originate the same LSA. Specifies the delay in milliseconds between the first and second SPF calculations. Specifies the minimum delay in milliseconds to generate the LSA again.This value is used to calculate the subsequent rate limiting times for LSA generation. Valid values are between 1 and 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Specifies the minimum delay in milliseconds to originate the same LSA. Specifies the maximum wait time in milliseconds for SPF calculations. Specifies the maximum delay in milliseconds to generate the LSA again. Valid values are between 1 and 600,000 milliseconds. The default value is 5000 milliseconds.
spf	Configures SPF throttling.

Command Default

LSA throttling:

- For *start-interval* , the default value is 0 milliseconds.
- For *hold-interval* , the default value is 5000 milliseconds.
- For *max-interval* , the default value is 5000 milliseconds.

SPF throttling:

- For *start-interval* , the default value is 5000 milliseconds.
- For *hold-interval* , the default value is 10000 milliseconds.
- For *max-interval* , the default value is 10000 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
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—
Router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.2(1)	Added support for IPv6.

Usage Guidelines

LSA and SPF throttling provide a dynamic mechanism to slow down LSA updates in OSPF during times of network instability and allow faster OSPF convergence by providing LSA rate limiting in milliseconds.

For LSA throttling, if the minimum or maximum time is less than the first occurrence value, then OSPF automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPF automatically corrects to the minimum delay value.

For SPF throttling, if *hold-interval* or *max-interval* is less than *start-interval* , then OSPF automatically corrects to the *start-interval* value. Similarly, if *max-interval* is less than *hold-interval* , then OSPF automatically corrects to the *hold-interval* value.

Examples

The following example configures OSPFv3 LSA throttling in milliseconds:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 4000 5000
```

For LSA throttling, the following example shows the automatic correction that occurs if the maximum delay value specified is less than the minimum delay value:

```
ciscoasa(config)# ipv6 router ospf 10

ciscoasa(config-rtr)# timers throttle lsa 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6

ipv6 router ospf 10
 timers throttle lsa 100 100 100
```

The following example configures OSPFv3 SPF throttling in milliseconds:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

For SPF throttling, the following example shows the automatic correction that occurs if the maximum delay value specified is less than the minimum delay value:

```
ciscoasa(config)# ipv6 router ospf 10

ciscoasa(config-rtr)# timers throttle spf 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6

ipv6 router ospf 10
 timers throttle spf 100 100 100
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers lsa-group-pacing	Specifies the interval at which OSPFv3 LSAs are collected and refreshed, checksummed, or aged.

timestamp

To define an action when the Time Stamp (TS) option occurs in a packet header with IP Options inspection, use the **timestamp** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

timestamp action { **allow | clear** }
no timestamp action { **allow | clear** }

Syntax Description

allow	Allow packets containing the Time Stamp IP option.
clear	Remove the Time Stamp option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Time Stamp 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)# timestamp 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.

title

To customize the title of the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **title** command from webvpn customization mode:

title { **text | style** } *value*
[**no**] **title** { **text | style** } *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

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 title text is "WebVPN Service".

The default title style is:

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger;vertical-align:middle;text-align:left;font-weight:bold

Command Modes

The 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	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

To have no title, use the **title text** command without a *value* argument.

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 title is customized with the text “Cisco WebVPN Service”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# title text Cisco WebVPN Service
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

tl – tz

tls-proxy

To configure a TLS proxy instance in TLS configuration mode or to set the maximum sessions, use the tls-proxy command in global configuration mode. To remove the configuration, use the **no** form of this command.

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]
no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

Syntax Description

max_sessions *max_sessions*	Specifies the maximum number of TLS proxy sessions to support on the platform.
noconfirm	Runs the **tls-proxy** command without requiring confirmation.
proxy_name	Specifies the name of the TLS 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	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the tls-proxy command to enter TLS proxy configuration mode to create a TLS proxy instance, or to set the maximum sessions supported on the platform.

Examples

The following example shows how to create a TLS proxy instance:

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.

token

To configure the API token needed to register with Cisco Umbrella, use the **token** command in Umbrella configuration mode. Use the **no** form of this command to remove the token.

token *api_token*
no token *api_token*

Syntax Description

api_token	The API token needed to register with Cisco Umbrella. You must obtain the token from the Cisco Umbrella Network Devices Dashboard (https://login.umbrella.com/). A token will be a hexadecimal string, for example, AABBA59A0BDE1485C912AFE.

Command Default

There is no default API token.

Command Modes

The 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

You must configure an API token to successfully register the device with Cisco Umbrella. The token is unique per customer, but not per device.

Registration is for a standalone device, cluster, or failover group. You do not register each device within a cluster or failover group separately. In multiple context mode, each context is a device, whether it is standalone or resides within a cluster or failover group.

Examples

The following example configures an API token for registration with Cisco Umbrella.

```
ciscoasa(config)# umbrella-global

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
```

Related Commands

Commands	Description
public-key	Configures the public key used with Cisco Umbrella.
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.
umbrella-global	Configures the Cisco Umbrella global parameters.

tos

To define a type of service byte in the IP header of an SLA operation request packet, use the **tos** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

tos *number*
no tos

Syntax Description

number	The service type value to be used in the IP header. Valid values are from 0 to 255.

Command Default

The default type of service value 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
Sla monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This field contains information such as delay, precedence, reliability, and so on. This is can be used by other routers on the network for policy routing and features such as Committed Access Rate.

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, the number of echo requests sent during an SLA operation to 5, and the type of service byte to 80.

```
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)# tos 80
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.
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.

traceroute

To determine the route packets will take to their destination, use the **traceroute** command.

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

Syntax Description

destination_ip	Specifies the destination IP address for the traceroute. Supports both IPv4 and IPv6 addresses.
hostname	The hostname of the host to which the route has to be traced. The host destination can be an IPv4 or IPv6 address. If the hostname is specified, define it with the **name** command, or configure a DNS server to enable traceroute to resolve the hostname to an IP address. Supports DNS domain names such as www.example.com.
max-ttl	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
min_ttl	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
numeric	Specifies the output print only the IP addresses of the intermediate gateways. If this keyword is not specified the traceroute attempts to look up the hostnames of the gateways reached during the trace.
port *port_value*	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
probe *probe_num*	The number of probes to be sent at each TTL level. The default count is 3.
source	Specifies an IP address or interface is used as the source for the trace packets. IPv6 will accept only the IPv6 source address.
source_interface	Specifies the source interface for the packet trace. When specified, the IP address of the source interface is used.
source_ip	Specifies the source IP address for the packet trace. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the ASA.
timeout	Specifies a timeout value is used
timeout_value	Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
ttl	Keyword to specify the range of Time To Live values to use in the probes.
use-icmp	Specifies the use of ICMP probe packets instead of UDP probe packets.

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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.7.(1)	This command was updated to accept IPv6 address.

Usage Guidelines

The **traceroute** command prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the **traceroute** command:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
U	No route to the destination.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable. For ICMPv6, address is out of scope.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable. For ICMPv6, port not reachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Examples

The following example shows traceroute output that results when a destination IP address has been specified:

```
ciscoasa# traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
ciscoasa/admin(config)# traceroute 2002::130
```

```
Type escape sequence to abort.
Tracing the route to 2002::130
 1  5000::2 0 msec 0 msec 0 msec
2  2002::130 10 msec 0 msec 0 msec
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.
packet-tracer	Enables packet tracing capabilities.

track rtr

To track the reachability of an SLA operation, use the **track rtr** command in global configuration mode. To remove the SLA tracking, use the **no** form of this command.

track *track-id* **rtr** *sla-id* **reachability**
no track *track-id* **rtr** *sla-id* **reachability**

Syntax Description

reachability	Specifies that the reachability of the object is being tracked.
sla-id	The ID of the SLA used by the tracking entry.
track-id	Creates a tracking entry object ID. Valid values are from 1 to 500.

Command Default

SLA tracking 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 **track rtr** command creates a tracking entry object ID and specifies the SLA used by that tracking entry.

Every SLA operation maintains an operation return-code value, which is interpreted by the tracking process. The return code may be OK, Over Threshold, or several other return codes. Table 2-1 displays the reachability state of an object with respect to these return codes.

Table 4: SLA Tracking Return Codes

Tracking	Return Code	Track State
Reachability	OK or Over Threshold	Up
	Any other code	Down

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
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
```

Related Commands

Command	Description
route	Configures a static route.
sla monitor	Defines an SLA monitoring operation.

traffic-forward

To direct traffic to a module and bypass access control and other processing, use the **traffic-forward** command in interface configuration mode. To disable traffic-forwarding, use the **no** form of this command.

traffic-forward *module_type***monitor-only**
no traffic-forward *module_type* **monitor-only**

Syntax Description

module_type The type of module. Supported modules are:

- **sfr**—ASA FirePOWER module.
- **cxsc**—ASA CX module.

monitor-only Sets the module to monitor-only mode. In monitor-only mode, the module can process traffic, but then drops the traffic. Usage differs by module type:

- ASA FirePOWER—Use this command to configure passive mode. You can use this mode for production purposes.
- ASA CX—This is strictly a demonstration mode. You cannot use the traffic-forwarding interface or the device for production purposes.

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
9.1(2)	This command was added.
9.2(1)	The **sfr** keyword was added.
9.3(2)	Support for production use with the **sfr** keyword was added.

Usage Guidelines

This command is an alternative to using the service policy **sfr** or **cxsc** commands with the **monitor-only** keyword to redirect traffic to the module. With service policies, the traffic is still subject to ASA processing, such as access rules and TCP normalization, that can result in dropped traffic. Additionally, the ASA simply sends a copy of the traffic to the module, and eventually transmits the traffic according to its own policies.

The **traffic-forward** command, on the other hand, bypasses ASA processing completely and simply forwards the traffic to the module. The module then inspects traffic, makes policy decisions, and generates events, showing you what it would have done to the traffic if it was operating in inline mode. Although the module operates on a copy of the traffic, the ASA itself drops the traffic immediately regardless of ASA or module policy decisions. The module acts as a black hole.

Connect the traffic-forwarded interface to a SPAN port on a switch in your network.

Traffic-forwarding interface configuration has these restrictions:

- You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed.
- The ASA must be in single context transparent mode.
- Traffic-forwarding interfaces must be physical interfaces, not VLANs or BVIs. The physical interface also cannot have any VLANs associated with it.
- Traffic-forwarding interfaces cannot be used for ASA traffic; you cannot name them or configure them for ASA features, including failover or management-only.

Examples

The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
cxsc	Service policy command that redirects traffic to an ASA CX module.
sfr	Service policy command that redirects traffic to an ASA FirePOWER module.

traffic-non-sip

To allow non-SIP traffic using the well-known SIP signaling port, use the **traffic-non-sip** 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.

traffic-non-sip
no traffic-non-sip

Syntax Description

This command has no arguments or keywords.

Command Default

Beginning with 9.16, this command is disabled by default. In previous releases, it 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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.16(1)	The default setting was changed to disabled.

Examples

The following example shows how to allow non-SIP traffic using the well-known SIP signaling port in a SIP inspection policy map:

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

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.

transfer-encoding

To restrict HTTP traffic by specifying a transfer encoding type, use the **transfer-encoding** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of this command.

transfer-encoding type { **chunked | compress | deflate | gzip | identity | default** } **action** { **allow | reset | drop** } [**log**]
no transfer-encoding type { **chunked | compress | deflate | gzip | identity | default** } **action** { **allow | reset | drop** } [**log**]

Syntax Description

action	Specifies the action taken when a connection using the specified transfer encoding type is detected.
allow	Allows the message.
chunked	Identifies the transfer encoding type in which the message body is transferred as a series of chunks.
compress	Identifies the transfer encoding type in which the message body is transferred using UNIX file compression.
default	Specifies the default action taken by the ASA when the traffic contains a supported request method that is not on a configured list.
deflate	Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951).
drop	Closes the connection.
gzip	Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952).
identity	Identifies connections in which the message body is no transfer encoding is performed.
log	(Optional) Generates a syslog.
reset	Sends a TCP reset message to client and server.
type	Specifies the type of transfer encoding to be controlled through HTTP application inspection.

Command Default

This command is disabled by default. When the command is enabled and a supported transfer encoding type is not specified, the default action is to allow the connection without logging. To change the default action, use the **default** keyword and specify a different default action.

Command Modes

The 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

When you enable the **transfer-encoding** command, the ASA applies the specified action to HTTP connections for each supported and configured transfer encoding type.

The ASA applies the **default** action to all traffic that does *not* match the transfer encoding types on the configured list. The preconfigured **default** action is to **allow** connections without logging.

For example, given the preconfigured default action, if you specify one or more encoding types with the action of **drop** and **log**, the ASA drops connections containing the configured encoding types, logs each connection, and allows all connections for the other supported encoding types.

If you want to configure a more restrictive policy, change the default action to **drop** (or **reset**) and **log** (if you want to log the event). Then configure each permitted encoding type with the **allow** action.

Enter the **transfer-encoding** command once for each setting you wish to apply. You use one instance of the **transfer-encoding** command to change the default action and one instance to add each encoding type to the list of configured transfer encoding types.

When you use the **no** form of this command to remove an application category from the list of configured application types, any characters in the command line after the application category keyword are ignored.

Examples

The following example provides a permissive policy, using the preconfigured default, which allows all supported application types that are not specifically prohibited.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# transfer-encoding gzip drop log
ciscoasa(config-http-map)#
```

In this case, only connections using GNU zip are dropped and the event is logged.

The following example provides a restrictive policy, with the default action changed to reset the connection and to log the event for any encoding type that is not specifically allowed.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# port-misuse default action reset log
ciscoasa(config-http-map)# port-misuse identity allow
ciscoasa(config-http-map)#
```

In this case, only connections using no transfer encoding are allowed. When HTTP traffic for the other supported encoding types is received, the ASA resets the connection and creates a syslog entry.

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.

trustpoint (saml idp)

To configure a trustpoint that contains the certificates for idp authentication or sp authentication, use the **trustpoint** command in saml idp configuration mode. You can access the saml idp configuration mode by first entering the **webvpn** command. To remove the trustpoint, use the **no** form of this command.

trustpoint { **idp | sp** } *trustpoint-name*
no trustpoint { **idp| sp** } *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the name of the trustpoint to use.
sp	The trustpoint contains the ASA (SP)'s certificate for IdP to verify ASA's signature or encrypt SAML assertion.
idp	The trustpoint contains the IdP certificate for ASA to verify SAML assertions.

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
Saml idp configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

Related Commands

Command	Description
saml idp	Creates a configuration for a third-party Idp, and puts you in saml-idp mode so you can configure SAML attributes.

trustpoint (sso server) (Deprecated)

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

To specify the name of a trustpoint that identifies the certificate to be sent to the SAML POST-type SSO server, use the **trustpoint** command in sso server mode. To eliminate a trustpoint specification, use the **no** form of this command.

trustpoint *trustpoint-name*
no trustpoint *trustpoint-name*

Syntax Description

trustpoint-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
Config webvpn sso saml	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command is 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 SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

Examples

The following example enters config-webvpn-sso-saml mode and names a trustpoint for identifying the certificate to be sent to the SAML POST type SSO Server:

```
ciscoasa(config-webvpn)# sso server
ciscoasa(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

Related Commands

Command	Description
crypto ca trustpoint	Manages trustpoint information.
show webvpn sso server	Displays the operating statistics for all SSO servers configured on the security device.
sso server	Creates, names, and specifies type for an SSO server.

trust-verification-server

To identify Trust Verification Services servers, which enable Cisco Unified IP Phones to authenticate application servers during HTTPS establishment, use the **trust-verification-server** command in parameters configuration mode for SIP inspection. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

trust-verification-server { **ip** *address* | **port** *number* }
no trust-verification-server { **ip** *address* | **port** *number* }

Syntax Description

ip *address*	Specifies the IP address of the Trust Verification Services server. You can enter the command with this argument up to four times in a SIP inspection policy map. SIP inspection opens pinholes to each server for each registered phone, and the phone decides which to use. Configure the Trust Verification Services server on the Cisco Unified Communications Manager (CUCM) server.
port *number*	Specifies the port number used by the server. The allowed port range is 1026 to 32768.

Command Default

The default port is 2445.

Command Modes

The 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
9.3(2)	This command was added.

Examples

The following example shows how to configure four Trust Verification Services servers in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.1

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.2

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.3

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.4
```

```
ciscoasa(config-pmap-p)# trust-verification-server port 2445
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.

tsig enforced

To require a TSIG resource record to be present, use the **tsig enforced** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

tsig enforced action { **drop** [**log**] | **log** }
no tsig enforced [**action** { **drop** [**log**] | **log** }]

Syntax Description

drop	Drops the packet if TSIG is not present.
log	Generates a system message log.

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 enables monitoring and enforcement of TSIG presence in DNS transactions.

Examples

The following example shows how to enable TSIG 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)# tsig enforced 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.
policy-map	Creates a Layer 3/4 policy map.

Command	Description
show running-config policy-map	Display all current policy map configurations.

ttl-evasion-protection

To enable Time-To-Live (TTL) evasion protection, use the **ttl-evasion-protection** command in tcp-map configuration mode. To disable the feature, use the **no** form of this command.

ttl-evasion-protection
no ttl-evasion-protection

Syntax Description

This command has no arguments or keywords.

Command Default

TTL evasion protection offered 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
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 **ttl-evasion-protection** command in tcp-map configuration mode to prevent attacks that attempt to evade security policy. With TTL evasion protect, the maximum TTL for a connection is determined by the TTL in the initial packet. The TTL for subsequent packets can decrease, but it cannot increase. The system will reset the TTL to the lowest previously-seen TTL for that connection.

For instance, an attacker can send a packet that passes policy with a very short TTL. When the TTL goes to zero, a router between the ASA and the endpoint drops the packet. It is at this point that the attacker can send a malicious packet with a long TTL that appears to the ASA to be a retransmission and is passed. To the endpoint host, however, it is the first packet that has been received by the attacker. In this case, an attacker is able to succeed without security preventing the attack. Enabling this feature prevents such attacks.

Examples

The following example shows how to disable TTL evasion protection on flows from network 10.0.0.0 to 20.0.0.0:

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0 255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# no
```

```
 ttl-evasion-protection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
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.

tunnel destination

To specify the IP address (IPv4 or IPv6) of the VTI tunnel's destination, use the tunnel destination command in the interface configuration mode. Use the no form of this command to remove the VTI tunnel's destination IP address.

tunnel destination { *IP address* | *hostname* }
no tunnel destination { *IP address* | *hostname* }

Syntax Description

IP address	Specifies the IP address (IPv4 or IPv6) of the VTI tunnel's destination.
hostname	Specifies the hostname of the VTI tunnel's destination.

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	• No	• Yes	• No	—

Command History

Release	Modification
9.7(1)	We introduced this command.
9.16(1)	We introduced support for IPv6 addresses.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

Examples

The following example specifies the IP address of the VTI tunnel's destination:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel destination 10.2.2.3
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
tunnel source interface	Specifies the source interface to create a VTI tunnel.

Command	Description
tunnel mode	Specifies that IPsec is used for tunnel protection.
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel mode

To specify the tunnel protection mode for a VTI tunnel, use the tunnel mode command in the interface configuration mode. A tunnel can use IPSec over IPv4 or IPv6. Use the no form of this command to remove VTI tunnel protection.

tunnel mode ipsec { **ipv4** | **ipv6** }
no tunnel mode ipsec { **ipv4** | **ipv6** }

Syntax Description

ipsec	Specifies that the tunnel will use IPsec as the tunnel protection standard.
ipv4	Specifies that the tunnel will use IPsec over IPv4.
ipv6	Specifies that the tunnel will use IPsec over 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	• No	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.
9.16(1)	We introduced IPSec over IPv6.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

Examples

The following example specifies IPsec as the protection mode:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel mode ipsec ipv4
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.

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 protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel protection ipsec

To specify the IPsec profile for the VTI tunnel, use the **tunnel protection ipsec** command in the interface configuration mode. Use the no form of this command to remove the IPsec profile for the tunnel.

tunnel protection ipsec { **profile** *IPsec_profile_name* | **policy** *acl_name* }
no tunnel protection ipsec *IPsec_profile_name*
no tunnel protection ipsec policy *acl_name*

Syntax Description

IPsec_profile_name	Specifies the name of the IPsec profile.
acl_name	Specifies the name of the ACL.

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	• No	• Yes	• No	—

Command History

Release	Modification
9.19(1)	Support for configuring specific traffic selectors using ACL for a static VTI.
9.7(1)	We introduced this command.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

The IKEv1 policy is attached to the IPsec profile when using the **tunnel protection ipsec profile** command.

The **tunnel protection ipsec policy** command is an optional command. If an ACL isn't attached to a static VTI, by default any-any traffic selector is chosen for the VTI tunnel.

Examples

In the following example, profile12 is the IPsec profile:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec profile profile12
```

Examples

The following shows how to configure specific traffic selectors using acl10 for a static VTI (Tunnel10):

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec policy acl10
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
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 the tunnel protection mode for a VTI tunnel.

tunnel source interface

To specify the source interface for the VTI tunnel, use the tunnel source interface command in the interface configuration mode. Use the no form of this command to remove the VTI tunnel's source interface.

tunnel source interface *interface_name*
tunnel source interface *interface_name* **ipv6** *ipv6_address*
no tunnel source interface *interface_name*
no tunnel source interface *interface_name* **ipv6** *ipv6_address*

Syntax Description

interface_name	Specifies the source interface to be used to create the VTI tunnel. If the source interface is an IPv6 address, prefix ipv6 to the 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
9.7(1)	We introduced this command.
9.16(1)	We introduced support for IPv6 addresses.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel**command in the Global Configuration mode. The IP address is taken from the selected interface.

Examples

The following example specifies the source interface of the VTI tunnel:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel source interface outside
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
tunnel destination	Specifies the IP address of the VTI tunnel's destination.
tunnel mode	Specifies that IPsec is used for tunnel protection.

Command	Description
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel-group

To create and manage the database of connection-specific records for IPsec and WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

tunnel-group *name* **type** *type*
no tunnel-group *name*

Syntax Description

name Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.

type Specifies the type of tunnel group:

- remote-access—Allows a user to connect using either IPsec remote access or WebVPN (portal or tunnel client).
- ipsec-l2l—Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet.

Note The following tunnel-group types are deprecated in Release 8.0(2):ipsec-ra—IPsec remote access webvpn—WebVPN. The ASA converts these to the remote-access 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
Global configuration	• Yes	See Note.	• Yes	• Yes	—

Note The tunnel-group command is available in transparent firewall mode to allow configuration of a LAN-to-LAN tunnel group, but not a remote-access group or a WebVPN group. All the **tunnel-group** commands that are available for LAN-to-LAN are also available in transparent firewall mode.

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The webvpn type was added.
8.0(2)	The remote-access type was added and the ipsec-ra and webvpn types were deprecated.

Release	Modification
8.3(1)	The *name argument was modified to accept IPv6 addresses.*
9.0(1)	Support for multiple context mode was added.
9.15(1)	The external-browser option is deprecated in the config-tunnel-webvpn mode.
9.17(1)	WebAuthN support was added using AnyConnect external browser. The external-browser option is added in the config-tunnel-webvpn mode.

Usage Guidelines

SSL VPN users (both AnyConnect and clientless) can choose which tunnel group to access using these different methods:

- group-url
- group-alias
- certificate maps, if using certificates

This command and subcommands configures the ASA to allow users to select a group via a drop-down menu when they log in to the webvpn service. The groups that appear in the menu are either aliases or URLs of real connection profiles (tunnel groups) configured on the ASA.

The ASA has the following default tunnel groups:

- DefaultRAGroup, the default IPsec remote-access tunnel group
- DefaultL2LGroup, the default IPsec LAN-to-LAN tunnel group
- DefaultWEBVPNGroup, the default WebVPN tunnel group.

You can change these groups, but not delete them. The ASA uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

After entering the **tunnel-group** command, you enter the appropriate following commands to configure specific attributes for a particular tunnel group. Each of these commands enters a configuration mode for configuring tunnel-group attributes.

- **tunnel-group general-attributes**
- tunnel-group ipsec-attributes
- tunnel-group webvpn-attributes
- tunnel-group ppp-attributes

For LAN-to-LAN connections, the ASA attempts to select a tunnel group for a connection by matching the peer address specified in the crypto map to a tunnel group of the same name. Therefore, for IPv6 peers, you should configure the tunnel group name as the IPv6 address of the peer. You can specify the tunnel group name in short or long notation. The CLI reduces the name to the shortest notation. For example, if you enter this tunnel group command:

```
ciscoasa(config)# tunnel-group 2001:0db8:0000:0000:0000:0000:1428:57ab type ipsec-l2l
```

The tunnel group appears in the configuration as:

```
tunnel-group 2001:0db8::1428:57ab type ipsec-l2l
```

Examples

The following examples are entered in global configuration mode. The first configures a remote access tunnel group. The group name is group1.

```
ciscoasa(config)# tunnel-group group1 type remote-access
ciscoasa(config)#
```

The following example shows the tunnel-group command configuring the webvpn tunnel group named “group1”. You enter this command in global configuration mode:

```
ciscoasa(config)# tunnel-group group1 type webvpn
ciscoasa(config)#
```

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 general-attributes	Enters the config-general mode for configuring general tunnel-group attributes
tunnel-group ipsec-attributes	Enters the config-ipsec mode for configuring IPsec tunnel-group attributes.
tunnel-group ppp-attributes	Enters the config-ppp mode for configuring PPP settings for L2TP connections.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

tunnel-group general-attributes

To enter the general-attribute configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

tunnel-group *name* **general-attributes**
no tunnel-group *name* **general-attributes**

Syntax Description

general-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-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
Tunnel-group general-attributes configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Various attributes from other tunnel-group types migrated to the general tunnel-group attributes list, and the prompt for tunnel-group general-attributes mode changed.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration mode, creates a remote-access tunnel group for a remote-access connection using the IP address of the LAN-to-LAN peer, then enters general-attributes configuration mode for configuring tunnel-group general attributes. The name of the tunnel group is 209.165.200.225.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type remote-access
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
ciscoasa(config-tunnel-general)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for an IPsec remote access connection, and then enters general configuration mode for configuring general attributes for the tunnel group named "remotegrp":

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group ipsec-attributes

To enter the ipsec-attribute configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol.

To remove all IPsec attributes, use the **no** form of this command.

tunnel-group *name* **ipsec-attributes**
no tunnel-group *name* **ipsec-attributes**

Syntax Description

ipsec-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Various IPsec tunnel-group attributes migrated to the general tunnel-group attributes list, and the prompt for tunnel-group ipsec-attributes mode changed.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration, creates a tunnel group for the IPsec remote-access tunnel group named remotegrp, and then specifies IPsec group attributes:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group-list enable

To enable the tunnel-groups defined in tunnel-group group-alias, use the **tunnel-group-list enable** command:

tunnel-group-list enable

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
Webvpn configuration	• Yes	—	• Yes	• Yes	—

Usage Guidelines

This command is used in conjunction with the tunnel-group group-alias and group-url commands for clientless and AnyConnect VPN client sessions. It enables the feature so that the tunnel-group drop-down is displayed on the login page. The group-alias is a text string such as employees, engineering, or consultants defined by the ASA administrator to display to end users.

Command History

Release	Modification
7.0(1)	This command was added.

Examples

```
ciscoasa# configure
 terminal
ciscoasa(config)# tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)# group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
```

Related Commands

Command	Description
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.
group-alias	Configures an alias for a connection profile (tunnel group).
group-url	Matches the URL or IP address specified by the VPN endpoint to the connection profile.

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

tunnel-group-map

When the adaptive security appliance receives an IPsec connection request with client certificate authentication, it assigns a connection profile to the connection according to a policy you configure.

That policy can be to use rules you configure, use the certificate OU field, use the IKE identity (i.e. hostname, IP address, key ID), the client's IP address, or a default connection profile to assign the connection profile. For SSL connections, the adaptive security appliance only uses the rules you configure to assign the connection profile.

The **tunnel-group-map** command assigns a connection profile to the connection based on rules you configure by associating an existing map name with a connection profile.

Use the **no** form of this command to disassociate a connection profile with a map name. The no form of the command does not delete the map name, just its association with a connection profile.

This is the syntax of the command:

tunnel-group-map [*mapname*] [*rule-index*] [*connection-profile*]
no tunnel-group-map [*mapname*] [*rule-index*]

Note

- You create the certificate map name with this command:crypto ca certificate map [mapname] [rule-index]
- A "tunnel group" is old terminology for what we now call a "connection profile." Think of the tunnel-group-map command as creating a connection profile map.

Syntax Description

mapname	Required. Identifies the name of the existing certificate map.
rule-index	Required. Identifies the rule-index associated with the mapname. The rule-index parameter was defined using the **crypto ca certificate map** command. The values are 1 to 65535.
connection-profile	Designates the connection profile name for this certificate map list.

Command Default

If a tunnel-group-map is not defined, and the ASA receives an IPsec connection request with client certificate authentication, the ASA assigns a connection profile by trying to match the certificate authentication request to one of these policies, in this order:

Certificate ou field—Determines connection profile based on the value of the organizational unit (OU) field in the subject distinguished name (DN).

IKE identity—Determines the connection profile based on the content of the phase1 IKE ID.

peer-ipDetermines the connection profile based on the established client IP address.

Default Connection Profile—If the ASA does not match the previous three policies, it assigns the default connection profile. The default profile is DefaultRAGroup. The default connection profile would otherwise be configured using the tunnel-group-map default-group 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	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The map name you specify must already exist before you can associate it with a connection profile. You create a map name using the **crypto ca certificate map** command. Refer to the documentation on the **crypto ca certificate map** command for more information.

Once you have associated map names with connection profiles, you need to enable the tunnel-group-map to use the rules you have configured rather than the default polices described earlier. To do this you must run the tunnel-group-map enable rules command in global configuration mode.

Examples

The following example associates the map name SalesGroup, with rule index 10, to the SalesConnectionProfile connection profile.

```
ciscoasa(config)# tunnel-group-map SalesGroup 10 SalesConnectionProfile
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map [map name]	Enters ca certificate map configuration mode and you can use it to create a certificate map name.
tunnel-group-map enable	Enables certificate-based IKE sessions based on established rules.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-group-map default-group

The tunnel-group-map default-group command specifies the default tunnel-group to use if the name could not be determined using other configured methods.

Use the **no** form of this command to eliminate a tunnel-group-map.

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*
no tunnel-group-map

Syntax Description

default-group *tunnel-group-name*	Specifies a default tunnel group to use when the name cannot be derived by other configured methods. The *tunnel-group name* must already exist.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Command Default

The default value for the **tunnel-group-map default-group** is DefaultRAGroup.

Command Modes

The 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)	Support for multiple context mode was added.

Usage Guidelines

The tunnel-group-map commands configure the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. To associate the certificate map entries, created using the **crypto ca certificate map** command, with tunnel groups, use the **tunnel-group-map** command in global configuration mode. You can invoke this command multiple times as long as each invocation is unique and you do not reference a map index more than once.

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

The processing that derives the tunnel-group name from the certificate ignores entries in the certificate map that are not associated with a tunnel group (any map rule not identified by this command).

Examples

The following example entered in global configuration mode, specifies a default tunnel group to use when the name cannot be derived by other configured methods. The name of the tunnel group to use is group1:

```
ciscoasa(config)# tunnel-group-map default-group group1
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters crypto ca certificate map configuration mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map enable	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups

tunnel-group-map enable

The **tunnel-group-map enable** command configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. Use the **no** form of this command to restore the default values.

tunnel-group-map [*rule-index*] **enable** *policy*
no tunnel-group-map enable [*rule-index*]

Syntax Description

policy	Specifies the policy for deriving the tunnel group name from the certificate. *Policy* can be one of the following: **ike-id**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou, then the certificate-based IKE sessions are mapped to a tunnel group based on the content of the phase1 IKE ID. **ou**—Indicates that if a tunnel-group is not determined based on a rule lookup, then use the value of the organizational unit (OU) in the subject distinguished name (DN). **peer-ip**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou or ike-id methods, then use the established peer IP address. **rules**—Indicates that the certificate-based IKE sessions are mapped to a tunnel group based on the certificate map associations configured by this command.
rule index	(Optional) Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Command Default

The default values for the **tunnel-group-map** command are **enable ou** and **default-group** set to DefaultRAGroup.

Command Modes

The 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)	Support for multiple context mode was added.

Usage Guidelines

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

Examples

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the content of the phase1 IKE ID:

```
ciscoasa(config)# tunnel-group-map enable ike-id
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the established IP address of the peer:

```
ciscoasa(config)# tunnel-group-map enable peer-ip
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions based on the organizational unit (OU) in the subject distinguished name (DN):

```
ciscoasa(config)# tunnel-group-map enable ou
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions based on established rules:

```
ciscoasa(config)# tunnel-group-map enable rules
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-group ppp-attributes

To enter the ppp-attributes configuration mode and configure PPP settings that are used by L2TP over IPsec connections, use the **tunnel-group ppp-attributes** command in global configuration mode.

To remove all PPP attributes, use the **no** form of this command.

tunnel-group *name* **ppp-attributes**
no tunnel-group *name* **ppp-attributes**

Syntax Description

name	Specifies the name of the tunnel-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
Global 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

PPP settings are used by the Layer 2 Tunneling Protocol (L2TP), a VPN tunneling protocol which allows remote clients to use the dialup telephone service public IP network to securely communicate with private corporate network servers. L2TP is based on the client/server model and uses PPP over UDP (port 1701) to tunnel the data. All of the tunnel-group ppp commands are available for the PPPoE tunnel-group type.

Examples

The following example creates the tunnel group *telecommuters* and enters ppp-attributes configuration mode:

```
ciscoasa(config)# tunnel-group telecommuters type pppoe
ciscoasa(config)# tunnel-group telecommuters ppp-attributes
ciscoasa(tunnel-group-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group-preference

To change the VPN preference to a connection profile with a group URL that matches the one specified by the endpoint, use the **tunnel-group-preference** command in webvpn configuration mode. To remove the command from the configuration, use the **no** form.

tunnel-group-preference group-url
no tunnel-group-preference group-url

Syntax Description

This command has no arguments or keywords.

Command Default

By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This command overrides the default 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
Config-webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)/8.4(2)	This command was added.

Usage Guidelines

This command changes the preference of a connection profile during the connection profile selection process. It lets you rely on the group URL preference used by many older ASA software releases. If the endpoint specifies a group URL that is not present in a connection profile, but it specifies a certificate value that matches that of a connection profile, the ASA assigns that connection profile to the VPN session.

Although you enter this command in webvpn configuration mode, it changes the connection profile selection preference for all clientless and AnyConnect VPN connections negotiated by the ASA.

Examples

The following example changes the preference of a connection profile during the connection profile selection process:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-preference group-url
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.
group-url	Matches the URL or IP address specified by the VPN endpoint to the connection profile.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

tunnel-group webvpn-attributes

To enter the webvpn-attribute configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

tunnel-group *name* **webvpn-attributes**
no tunnel-group *name* **webvpn-attributes**

Syntax Description

name	Specifies the name of the tunnel-group. **Note** Ensure that the tunnel group name does not contain the following special characters: &, ", or <.
webvpn-attributes	Specifies WebVPN attributes for this tunnel-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
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.8(1)	Changed the pre-fill-username and secondary-pre-fill-username value from clientless to client.

Usage Guidelines

In addition to the general attributes, you can also configure the following attributes specific to WebVPN connections in webvpn-attribute mode:

- authentication
- customization
- dns-group
- group-alias
- group-url

- without-csd

The pre-fill-username and secondary-pre-fill-username attributes are used to extract a username from a certificate for use in authentication and authorization. The values are client or clientless.

Examples

The following example entered in global configuration mode, creates a tunnel group for a WebVPN connection using the IP address of the LAN-to-LAN peer, then enters webvpn-configuration mode for configuring WebVPN attributes. The name of the tunnel group is 209.165.200.225.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type webvpn
ciscoasa(config)# tunnel-group 209.165.200.225 webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for a WebVPN connection, and then enters webvpn configuration mode for configuring WebVPN attributes for the tunnel group named "remotegrp":

```
ciscoasa(config)# tunnel-group remotegrp type webvpn
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-limit

To specify the maximum number of active GTP tunnels allowed, use the **tunnel limit** command in policy map parameters configuration mode. Use the **no** form of this command to set the tunnel limit back to its default.

tunnel-limit *max_tunnels*
no tunnel-limit *max_tunnels*

Syntax Description

max_tunnels	The maximum number of tunnels allowed. This is equivalent to the number of PDP contexts or endpoints.

Command Default

The default tunnel limit 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
Parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

New requests will be dropped once the number of tunnels specified by this command is reached.

Examples

The following example specifies a maximum of 10,000 tunnels for GTP traffic:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 10000
```

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.

tx-ring-limit

To specify the depth of the priority queues, use the **tx-ring-limit** command in priority-queue 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, the ASA 5512-X through ASA 5555-X Management interface, or the ASA Services Module. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.)

tx-ring-limit *number-of-packets*
no tx-ring-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears. The range 3 through 511.

Command Default

The default is 511.

Command Modes

The 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	• 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.

You must use the **priority-queue** command to create the priority queue for an interface before priority queuing takes effect. 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 mode, as shown by the prompt. In priority-queue 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.

Note The upper limit of the range of values for the **queue-limit** and **tx-ring-limit** commands 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.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, 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.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 2048 packets and a transmit queue limit of 256 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 2048
ciscoasa(priority-queue)# tx-ring-limit 256
```

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.
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config 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** command configuration values.

type echo

To configure the SLA operation as an echo response time probe operation, use the **type echo** command in SLA monitor configuration mode. To remove the type from the SLA configuration, use the **no** form of this command.

type echo protocol ipIcmpEcho *target* **interface** *if-name*
no type echoprotocol ipIcmpEcho *target* **interface** *if-name*

Syntax Description

interface *if-name*	Specifies the interface name, as specified by the **nameif** command, of the interface used to send the echo request packets. The interface source address is used as the source address in the echo request packets.
protocol	The protocol keyword. The only value supported is **ipIcmpEcho**, which specifies using an IP/ICMP echo request for the echo operation.
target	The IP address or host name of the object being monitored.

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
Sla monitor configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The default size of the payload of the ICMP packets is 28 bytes, creating a total ICMP packet size of 64 bytes. The payload size can be changed using the **request-data-size** command.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
```

```
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.
request-data-size	Specifies the size of the payload for the SLA operation request packet.
sla monitor	Defines an SLA monitoring operation.

u

uc-ime (Deprecated)

To create the Cisco Intercompany Media Engine proxy instance, use the **uc-ime** command in global configuration mode. To remove the proxy instance, use the **no** form of this command.

uc-ime *uc-ime_name*
no uc-ime *uc-ime_name*

Syntax Description

uc-ime_name	Specifies the instance name of the Cisco Intercompany Media Engine proxy configured on the ASA. The *name* is limited to 64 characters. Only one Cisco Intercompany Media Engine proxy can be configured on the ASA.

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.
9.4(1)	This command was deprecated.

Usage Guidelines

Configures the Cisco Intercompany Media Engine proxy. Cisco Intercompany Media Engine enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them.

You must create the media termination instance before you specify it in the Cisco Intercompany Media Engine proxy.

Only one Cisco Intercompany Media Engine proxy can be configured on the ASA.

Examples

The following example shows how to configure a Cisco Intercompany Media Engine proxy by using the **uc-ime** command.

```
ciscoasa
(config)# uc-ime local_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
```

Related Commands

Command	Description
fallback	Configures the fallback timers that the Cisco Intercompany Media Engine uses to fallback from VoIP to PSTN when connection integrity degrades.
show uc-ime	Displays statistical or detailed information about fallback-notifications, mapping-service-sessions, and signaling-sessions.
ticket	Configures the ticket epoch and password for the Cisco Intercompany Media Engine proxy.
ucm	Configures the Cisco UCMs that the Cisco Intercompany Media Engine Proxy connects to.

ucm (Deprecated)

To configure which Cisco Unified Communication Managers (UCM) that the Cisco Intercompany Media Engine Proxy connects to, use the **ucm** command in global configuration mode. To remove the Cisco UCMs that are connected to the Cisco Intercompanuy Media Engine Proxy, use the **no** form of this command.

ucm address *ip_address* **trunk-security-mode** { **nonsecure | secure** }
no ucm address *ip_address* **trunk-security-mode** { **nonsecure | secure** }

Syntax Description

address	The keyword to configure the IP address of the Cisco Unified Communications Manager (UCM).
ip_address	Specifies the IP address of the Cisco UCM. Enter the IP address in IPv4 format.
nonsecure	Specifies that the Cisco UCM or Cisco UCM cluster is operating in non-secure mode.
secure	Specifies that the Cisco UCM or Cisco UCM cluster is operating in secure mode.
trunk-security-mode	The keyword to configure the security mode of the Cisco UCM or Cisco UCM cluster.

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
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

Specifies the Cisco UCM server in the enterprise.

You can enter multiple **ucm** commands for the Cisco Intercompany Media Engine proxy.

Note You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled.

Specifying **secure** for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS; therefore, you must set up configure TLS for components.

You can specify the **secure** option in this task or you can update it later while configuring TLS for the enterprise.

TLS within the enterprise refers to the security status of the Cisco Intercompany Media Engine trunk as seen by the ASA.

If the transport security for the Cisco Intercompany Media Engine trunk changes on Cisco UCM, it must be changed on the adaptive security appliance as well. A mismatch will result in call failure. The adaptive security appliance does not support SRTP with non-secure IME trunks. The adaptive security appliance assumes SRTP is allowed with secure trunks. So SRTP Allowed must be checked for IME trunks if TLS is used. The ASA supports SRTP fallback to RTP for secure IME trunk calls.

The proxy sits on the edge of the enterprise and inspects SIP signaling between SIP trunks created between enterprises. It terminates TLS signaling from the Internet and initiates TCP or TLS to Cisco UCM.

Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the Transport Layer end-to-end.

This task is not required if TCP is allowable within the inside network.

Key steps for Configuring TLS within the local enterprise:

- On the local ASA, create another RSA key and trustpoint for the self-signed certificate.
- Exporting and importing the certificates between the local Cisco UCM and local ASA.
- Create a trustpoint for local Cisco UCM on the ASA.

Authentication via TLS: In order for the ASA to act as a port on behalf of N enterprises, the Cisco UCMs must be able to accept the one certificate from the ASA. This can be done by associating all the UC-IME SIP trunks with the same SIP security profile containing the same subject name as that of the one presented by the ASA because the Cisco UCM extracts the subject name from the certificate and compares that with the name configured in the security profile.

Examples

The following example shows how to connect to a UCM proxy:

```
ciscoasa
(config)# uc-ime local_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
```

umbrella

To enable the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella, use the **umbrella** command in DNS inspection policy map parameters configuration mode. To disable Cisco Umbrella, use the **no** form of this command.

umbrella [**tag** *umbrella_policy*] [**fail-open**]
no umbrella [**tag** *umbrella_policy*] [**fail-open**]

Syntax Description

fail-open	If the Cisco Umbrella DNS server is unavailable, have Umbrella disable itself on this policy map and allow DNS requests to go to the other DNS servers configured on the system, if any. When the Umbrella DNS servers are available again, the policy map resumes using them. If you do not include this option, DNS requests continue to go to the unreachable Umbrella resolver, so they will not get a response.
tag *umbrella_policy*	(Optional.) The name of an Enterprise Security policy, which is defined in Cisco Umbrella, to apply to the device. If you do not specify a policy, or the name you enter does not exist in Cisco Umbrella, the default policy is assigned.

Command Default

If you do not specify a tag, the device registration assigns the default Enterprise Security 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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.
9.12(1)	The **fail-open** keyword was added.

Usage Guidelines

Use this command when configuring a DNS inspection policy map.

The presence of this command in an active DNS inspection policy map starts the registration process with the Cisco Umbrella registration server. You need to have installed the registration server's CA certificate to establish the connection and registration, which happens over HTTPS.

You must also configure the global parameters using the **umbrella-global** command in global configuration mode.

Examples

The following example enables Umbrella using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

The following example enables Umbrella to fail open, using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection. If you have already registered with a tag, and just want to add the **fail-open** option, you must include the same tag in the command or you will reregister the device with no tag.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella
 fail-open

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.
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
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.
umbrella-global	Configures the Cisco Umbrella global parameters.

umbrella-global

To enter Umbrella configuration mode so that you can configure the global settings required to connect the device to the Cisco Umbrella portal, use the **umbrella-global** command in global configuration mode. Use the **no** form of this command to remove the global Umbrella configuration.

umbrella-global
no umbrella-global

Syntax Description

This command has no arguments or keywords.

Command Default

There is no default global Umbrella 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
global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

If you subscribe to the Cisco Umbrella service, you can configure the device so that it registers with Cisco Umbrella.

The Umbrella global settings primarily define the API token that is needed to register the device with Cisco Umbrella. You obtain the token from the Cisco Umbrella dashboard.

The global settings are not sufficient to enable Umbrella. You must also enable Umbrella in your DNS inspection policy map using the umbrella command in parameters configuration mode.

Examples

The following example configures the global Umbrella settings and also shows how to enable Umbrella in the default DNS inspection policy map.

```
ciscoasa(config)# umbrella-global

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.
local-domain-bypass	Configures the local domains for which DNS requests should bypass Cisco Umbrella.
public-key	Configures the public key used with Cisco Umbrella.
resolver	Configures the addresses of the Cisco Umbrella DNS servers, which resolve DNS requests.
token	Identifies the API token that is needed to register with Cisco Umbrella.
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.
umbrella	Enables the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella.

undebug

To disable the display of debugging information in the current session, use the **undebug** command in privileged EXEC mode.

undebug { *command* | **all** }

Syntax Description

all	Disables all debug output.
command	Disables debug for the specified command. See the Usage Guidelines for information about the supported commands.

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 modified. It includes additional **debug** keywords.

Usage Guidelines

The following commands can be used with the **undebug** command. For more information about debugging a specific command, or for the associated arguments and keywords for a specific **debug** command, see the entry for the **debug** command.

- aaa—AAA information
- acl—ACL information
- all—All debugging
- appfw—Application firewall information
- arp—ARP including NP operations
- asdm—ASDM information
- auto-update—Auto-update information
- boot-mem—Boot memory calculation and set
- cifs—CIFS information

- cmgr—CMGR information
- context—Context information
- cplane—CP information
- crypto—Crypto information
- ctiqbe—CTIQBE information
- ctl-provider—CTL provider debugging information
- dap—DAP information
- dcerpc—DCERPC information
- ddns—Dynamic DNS information
- dhcpc—DHCP client information
- dhcpd—DHCP server information
- dhcprelay—DHCP Relay information
- disk—Disk information
- dns—DNS information
- eap—EAP information
- eigrp—EIGRP protocol information
- email—Email information
- entity—Entity MIB information
- eou—EAPoUDP information
- esmtp—ESMTP information
- fips—FIPS 140-2 information
- fixup—Fixup information
- fover—Failover information
- fsm—FSM information
- ftp—FTP information
- generic—Miscellaneous information
- gtp—GTP information
- h323—H323 information
- http—HTTP information
- icmp—ICMP information
- igmp—Internet Group Management Protocol
- ils—LDAP information

- im—IM inspection information
- imagemgr—Image Manager information
- inspect—inspect debugging information
- integrityfw—Integrity Firewall information
- ip—IP information
- ipsec-over-tcp—IPsec over TCP information
- ipsec-pass-thru—Inspect ipsec-pass-thru information
- ipv6—IPv6 information
- iua-proxy—IUA proxy information
- kerberos—KERBEROS information
- l2tp—L2TP information
- ldap—LDAP information
- mfib—Multicast forwarding information base
- mgcp—MGCP information
- module-boot—Service module boot information
- mrib—Multicast routing information base
- nac-framework—NAC-FRAMEWORK information
- netbios-inspect—NETBIOS inspect information
- npshim—NPSHIM information
- ntdomain—NT domain information
- ntp—NTP information
- ospf—OSPF information
- p2p—P2P inspection information
- parser—Parser information
- pim—Protocol Independent Multicast
- pix—PIX information
- ppp—PPP information
- pppoe—PPPoE information
- pptp—PPTP information
- radius—RADIUS information
- redundant-interface—redundant interface information
- rip—RIP information

- rtp—RTP information
- rtsp—RTSP information
- sdi—SDI information
- sequence—Add sequence number
- session-command—Session command information
- sip—SIP information
- skinny—Skinny information
- sla—IP SLA Monitor Debug
- smtp-client—Email system log messages
- splitdns—Split DNS information
- sqlnet—SQLNET information
- ssh—SSH information
- sunrpc—SUNRPC information
- tacacs—TACACS information
- tcp—TCP for WebVPN
- tcp-map—TCP map information
- timestamps—Add timestamp
- track—static route tracking
- vlan-mapping—VLAN mapping information
- vpn-sessiondb—VPN session database information
- vpnlb—VPN load balancing information
- wccp—WCCP information
- webvpn—WebVPN information
- xdmcp—XDMCP information
- xml—XML parser information

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The example disables all debugging output:

```
ciscoasa(config)# undebug all
```

Related Commands

Command	Description
debug	Displays debug information for the selected command.

unit join-acceleration

To enable accelerated cluster joining, use the **unit joint-acceleration** command in cluster configuration mode. To disable this feature, use the **no** form of this command.

unit join-acceleration
no unit join-acceleration

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
Cluster configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

When a data node has the same configuration as the control node, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each node, and is not replicated from the control to the data.

Note Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the node, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** command to view incompatible configuration.

Examples

The following example disables accelerated cluster joining:

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no unit join-acceleration
```

Related Commands

Command	Description
cluster	Enters cluster configuration mode

unit parallel-join

To ensure that the security modules in a Firepower 9300 chassis join the cluster simultaneously so that traffic is evenly distributed between the modules, use the **unit parallel-join** command in cluster group configuration mode. To disable parallel joining, use the **no** form of this command.

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*
no unit parallel-join [*num_of_units* **max-bundle-delay** *max_delay_time*]

Syntax Description

num_of_units	Specifies the minimum number of modules in the same chassis required to be ready before a module can join the cluster, between 1 and 3. The default is 1, meaning that a module will not wait for other modules to be ready before it joins the cluster. If you set the value to 3, for example, then each module will wait the *max_delay_time* or until all 3 modules are ready before joining the cluster. All 3 modules will request to join the cluster roughly simultaneously, and will all start receiving traffic around the same time.
max-bundle-delay *max_delay_time*	Specifies the maximum delay time in minutes before a module stops waiting for other modules to be ready before it joins the cluster, between 0 and 30 minutes. The default is 0, meaning the module will not wait for other modules to be ready before it joins the cluster. If you set the *num_of_units* to 1, then this value must be 0. If you set the *num_of_units* to 2 or 3, then this value must be 1 or more. This timer is per module, but when the first module joins the cluster, then all other module timers end, and the remaining modules join the cluster. For example, you set the *num_of_units* to 3, and the *max_delay_time* to 5 minutes. When module 1 comes up, it starts its 5 minute timer. Module 2 comes up 2 minutes later and starts its 5 minute timer. Module 3 comes up 1 minute later, therefore all modules will now join the cluster at the 4 minute mark; they will not wait for the timers to complete. If module 3 never comes up, then Module 1 will join the cluster at the end of its 5 minute timer, and Module 2 will also join, even though its timer still has 2 minutes remaining; it will not wait for its timer to complete.

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
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.10(1)	Command added.

Usage Guidelines

If a module joins very much in advance of other modules, it can receive more traffic than desired, because the other modules cannot yet share the load.

Examples

The following example sets the number of modules to 2, and the maximum delay time to 6 minutes:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# unit parallel-join 2 max-bundle-delay 6
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.

unix-auth-gid

To set the UNIX group ID, use the **unix-auth-gid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid *identifier*
no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Command Default

The default is 65534.

Command Modes

The 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	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX group ID to 4567:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
 unix-auth-gid 4567
```

Related Commands

Command	Description
unix-auth-uid	Sets the UNIX user ID.

unix-auth-uid

To set the UNIX user ID, use the **unix-auth-uid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid *identifier*
no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Command Default

The default is 65534.

Command Modes

The 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	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX user ID to 333:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
 unix-auth-gid 333
```

Related Commands

Command	Description
unix-auth-gid	Sets the UNIX group ID.

unsupported

To log Diameter elements that are not directly supported by the software, use the **unsupported** command in policy map parameters configuration mode. Use the **no** form of this command to remove the setting.

unsupported { **application-id | avp | command-code** } **action log**
no unsupported { **application-id | avp | command-code** } **action log**

Syntax Description

application-id	Log Diameter messages whose application ID is not directly supported.
avp	Log Diameter messages that contain an attribute-value pair (AVP) that is not directly supported.
command-code	Log Diameter messages that contain a command code that is not directly supported.

Command Default

The default is to allow the elements without logging them.

Command Modes

The 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(2)	This command was added.

Usage Guidelines

Use this command when configuring a Diameter inspection policy map.

These options specify application IDs, command codes, and AVP that are not directly supported by the software. The default is to allow the elements without logging them. You can enter the command three times to enable logging for all elements.

Examples

The following example logs all unsupported application IDs, command codes, and AVP:

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# unsupported application-id action log
ciscoasa(config-pmap-p)# unsupported command-code action log
ciscoasa(config-pmap-p)# unsupported avp action log
```

Related Commands

Commands	Description
inspect diameter	Enables Diameter inspection.
policy-map type inspect diameter	Creates a Diameter inspection policy map.

upgrade rommon

To upgrade the ASA 5506-X and ASA 5508-X series security appliances, use the **upgrade rommon** command in privileged EXEC mode.

upgrade rommon { **disk 0 | disk 1 | flash** } **:** / [**path**] **filename**

Syntax Description

disk0:/ [*path* /] *filename*	This option indicates the internal Flash memory. You can also use **flash** instead of **disk0** ; they are aliased.
disk1:/ [*path* /] *filename*	This option indicates the external Flash memory card.
flash:/ [*path* /] *filename*	This option indicates the internal Flash card; **flash** is an alias for **disk0:**

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
9.3(2)	This command was added.

Usage Guidelines

Once you supply a filename to the command, the command verifies the file and asks you to confirm the upgrade. If you have unsaved configuration information, you are prompted to save the information before beginning the reload. If you confirm, the ASA goes to ROMMON and the upgrade procedure begins.

Examples

The following example shows how to upgrade the ASA 5506-X and ASA 5508-X series security appliances:

```
ciscoasa# upgrade rommon disk0:/kenton_rommon_1-0-19_release.SPA

Verifying file integrity of disk0:/kenton_rommon_1-0-19_release.SPA
Computed Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4

Embedded Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
```

```
                        9ef1fa4c3892f04b2e71a6b19ddb64c4

Digital signature successfully validated
File Name                     : disk0:/kenton_rommon_1-0-19_release.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54232BC5
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

upload-max-size

Note The **upload-max-size** command does not work. Do not use it. However, you might see it in the running configuration, and it is available in the CLI.

To specify the maximum size allowed for an object to upload, use the **upload-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

upload-max-size*size*
no upload-max-size

Syntax Description

size	Specifies the maximum size allowed for a uploaded object. The range is 0 through 2147483647.

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	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
download-max-size	Specifies the maximum size of an object to download.
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.

uri-non-sip

To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, use the **uri-non-sip** 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.

uri-non-sip action { **mask | log** } [**log**]
no uri-non-sip action { **mask | log** } [**log**]

Syntax Description

log	Specifies standalone or additional log in case of violation.
mask	Masks the non-SIP URIs.

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 identify the non-SIP URIs present in the Alert-Info and Call-Info header fields in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# uri-non-sip 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.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

url (crl configure) (Deprecated)

To maintain the list of static URLs for retrieving CRLs, use the **url** command in crl configure configuration mode. The crl configure configuration mode is accessible from the **crypto ca trustpoint** configuration mode. To delete an existing URL, use the **no** form of this command.

url*indexurl*
no url *index url*

Syntax Description

index	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The ASA tries the URL at index 1 first.
url	Specifies the URL from which to retrieve the CRL.

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
Crl configure configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	This command was removed. See the **match certificate** command.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

Examples

The following example enters crl configure mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL https://example.com from which to retrieve CRLs:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
policy	Specifies the source for retrieving CRLs.

url (saml idp)

To configure the SAML IdP URL for signing in or signing out, use the **url** command in saml idp configuration mode. You can access the saml idp configuration mode by first entering the **webvpn** command. To remove the URL, use the **no** form of this command.

url { **sign-in | sign-out** } **value** *url*
no url *url*

Syntax Description

url	Specifies the URL from which to retrieve the CRL.

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
Saml idp configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

url-block

To manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server, use the **url-block** command. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer*
no url-block block *block_buffer*
url-block mempool-size *memory_pool_size*
no url-block mempool-size *memory_pool_size*
url-block url-size *long_url_size*
no url-block url-size *long_url_size*

Syntax Description

block *block_buffer*	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks.
mempool-size *memory_pool_size*	Configures the maximum size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
url-size *long_url_size*	Configures the maximum allowed URL size in KB for each long URL being buffered. The permitted values, which specifies a maximum URL size,: for Websense are 2, 3, or 4, representing 2 KB, 3 KB, or 4KB; or for Secure Computing, 2 or 3, representing 2 KB or 3 KB.

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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

For Websense filtering servers, the url-block url-size command allows filtering of long URLs, up to 4 KB. For Secure Computing, the url-block url-size command allows filtering of long URLs, up to 3 KB. For both Websense and N2H2 filtering servers, the url-block block command causes the ASA to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default ASA behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the url-block block command and the filtering server permits the connection, the ASA sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the ASA sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the **url-block block command** to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block** url-size command with the url-block mempool-size command to specify the maximum length of a URL to be filtered and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense or Secure-Computing server. The **url-block** url-size command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense or Secure-Computing server (through a TCP packet stream) so that the Websense or Secure-Computing server can grant or deny access to that URL.

Examples

The following example assigns 56 1550-byte blocks for buffering responses from the URL filtering server:

```
ciscoasa#(config)# url-block block 56
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

url-cache

To enable URL caching for URL responses received from a Websense server and to set the size of the cache, use the url-cache command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-cache { **dst | src_dst** } *kbytes* [**kb**]
no url-cache { **dst | src_dst** } *kbytes* [**kb**]

Syntax Description

dst	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the Websense server.
size *kbytes*	Specifies a value for the cache size within the range 1 to 128 KB.
src_dst	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the Websense server.
statistics	Use the statistics option to display additional URL cache statistics, including the number of cache lookups and hit rate.

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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **url-cache** command provides a configuration option to cache responses from the URL server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Note The N2H2 server application does not support this command for URL filtering.

Caching stores URL access privileges in memory on the ASA. When a host requests a connection, the ASA first looks in the URL cache for matching access privileges instead of forwarding the request to the Websense server. Disable caching with the **no url-cache** command.

Note If you change settings on the Websense server, disable the cache with the no url-cache command and then re-enable the cache with the url-cache command.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 URL filtering while using the **url-cache** command.

Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
ciscoasa(config)# url-cache src_dst 128
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for URL responses received from a Websense filtering server.
url-server	Identifies a Websense server for use with the filter command.

url-entry

To enable or disable the ability to enter any HTTP/HTTPS URL on the portal page, use the **url-entry** command in dap webvpn configuration mode.

url-entry enable | enable

enable | disable	Enables or disables the ability to browse for file servers or shares.

Command Default

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows how to enable URL entry for the DAP record called Finance:

```
ciscoasa
 (config) config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dynamic-access-policy-record)#
 url-entry enable
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

url-length-limit

To configure the maximum length of the URL allowed in the RTSP message, use the **url-length-limit** 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.

url-length-limit *length*
no url-length-limit *length*

Syntax Description

length	The URL length limit in bytes. Range is 0 to 6000.

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 configure the URL length limit in an RTSP inspection policy map:

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

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.

url-list

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a url list, use the **url-list none** command. Using the command a second time overrides the previous setting.

url-list { **value** *name* **|** **none** } [**index**]
no url-list

Syntax Description

index	Indicates the display priority on the home page.
none	Sets a null value for URL lists. Prevents inheriting a list from a default or specified group policy.
value *name*	Specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Command Default

There is no default URL list.

Command Modes

The following table shows the modes in which you enter the commands:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list via an XML object. Use the **import** command in global configuration mode to download a URL list to the security appliance. Then use the url-list command to apply a list to a particular group policy or user.

Examples

The following example applies a URL list called FirstGroupURLs for the group policy named FirstGroup and assigns it first place among the URL lists:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

Related Commands

Command	Description
clear configure url-list	Removes all url-list commands from the configuration. If you include the list name, the ASA removes only the commands for that list.
show running-configuration url-list	Displays the current set of configured **url-list** commands.
webvpn	Lets you enter webvpn mode. This can be webvpn configuration mode, group-policy webvpn configuration mode (to configure webvpn settings for a specific group policy), or username webvpn configuration mode (to configure webvpn settings for a specific user).

url-server

To identify an N2H2 or Websense server for use with the filter command, use the **url-server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

N2H2
url-server [(*if_name*)] **vendor** { **smartfilter | n2h2** } **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** { **TCP** [*connections number*] } | **UDP**]
no url-server [(*if_name*)] **vendor** { **smartfilter | n2h2** } **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** { **TCP** [**connections** *number*] } | **UDP**]

Websense
url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** { **TCP | UDP | connections** *num_conns*] | *version*]
no url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** { **TCP | UDP** [**connections** *num_conns*] | *version*]

Syntax Description

N2H2

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	(Optional) The network interface where the authentication server resides. If not specified, the default is inside.
port *number*	The N2H2 server port. The ASA also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP.
timeout *seconds*	The maximum idle time permitted before the ASA switches to the next server you specified. The default is 30 seconds.
vendor	Indicates URL filtering service, using either ‘smartfilter’ or ‘n2h2’ (for backward compatibility); however, ‘smartfilter’ is saved as the vendor string.

Websense

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.

if_name	The network interface where the authentication server resides. If not specified, the default is inside.
timeout *seconds*	The maximum idle time permitted before the ASA switches to the next server you specified. The default is 30 seconds.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP protocol, Version 1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol Version **1** or **4**. The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

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
7.0(1)	This command was added.

Usage Guidelines

The url-server command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers in single context mode and 4 URL servers in multi mode; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the ASA does not update the configuration on the application server; this must be done separately, according to the vendor instructions.

The **url-server** command must be configured before issuing the **filter** command for HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

Once you designate the server, enable the URL filtering service with the **filter url** command.

Use the **show url-server statistics** command to view server statistic information including unreachable servers.

Follow these steps to filter URLs:

1. Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.
2. Enable URL filtering with the **filter** command.

3. (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.
4. (Optional) Enable long URL and HTTP buffering support using the **url-block** command.
5. Use the **show url-block block statistics**, **show url-cache statistics**, or the **show url-server statistics** commands to view run information.

For more information about filtering by N2H2, visit N2H2's website at:

http://www.n2h2.com

For more information about Websense filtering services, visit the following website:

http://www.websense.com/

Examples

Using N2H2, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP version
 4
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for URL responses received from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

urgent-flag

To allow or clear the URG pointer through the TCP normalizer, use the **urgent-flag** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

urgent-flag { **allow | clear** }
no urgent-flag { **allow clear** }

Syntax Description

allow	Allows the URG pointer through the TCP normalizer.
clear	Clears the URG pointer through the TCP normalizer.

Command Default

The urgent flag and urgent offset are clear 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 **urgent-flag** command in tcp-map configuration mode to allow the urgent flag.

The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore, end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks. The default behavior is to clear the URG flag and offset.

Examples

The following example shows how to allow the urgent flag:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 513
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.

user

To create a user in a user group object that supports the Identity Firewall feature, use the **user** command in the user-group object configuration mode. Use the **no** form of this command to remove the user. from the object.

user [*domain_nickname* \] *user_name*
[**no**] **user** [*domain_nickname* \] *user_name*

Syntax Description

domain_nickname	(Optional) Specifies the domain in which to add the user.
user_name	Specifies the name for the user. The user name can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If the user name contains a space, you must enclose the name in quotation marks. The *user_name* argument that you specify with the **user** keyword contains an ASCII user name and does not specify an IP address.

Command Default

If you do not specify the *domain_nickname argument, the user is created in the LOCAL domain configured for the Identity Firewall feature*.

Command Modes

The 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 user configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for the Identity Firewall feature. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups. A user can belong to local user groups and user groups imported from Active Directory.

The ASA supports up to 256 user groups (including imported user groups and local user groups).

You active user group objects by including them within an access group, capture, or service policy.

Within a user group object, you can define the following object types:

- **User**—adds a single user to the object-group user. The user can be either a LOCAL user or imported user.

The name of an imported user must be the sAMAccountName, which is unique, rather than the common name (cn), which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used for imported users defined by the user object.

- User-group—adds an imported user group, which is defined by an external directory server, such as Microsoft Active Directory server, to the group-object user.

The group name of the user-group must be the sAMAccountName, which is unique, rather than the cn, which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used in the *user_group_name* argument specified with the **user-group** keyword.

Note You can add *domain_nickname\\user_group_name* or *domain_nickname\user_ name* directly within a user group object without specifying them in the object first. If the *domain_nickname* is associated with a AAA server, the ASA imports the detailed nested user groups and the users defined in the external directory server, such as the Microsoft Active Directory server, to the ASA when the user object group is activated.

- **Group-object**—adds a group defined locally on the ASA to the object-group user.

Note When including an object-group within a object-group user object, the ASA does not expand the object-group in access groups even when you enable ACL optimization. The output of the **show object-group** command does not display the hit count, which is available only for regular network object-group when ACL optimization is enabled.

- **Description**—adds a description for the object-group user.

Examples

The following example shows how to use the **user** command with the **user-group object** command to add a user in a user group object for use with the Identity Firewall feature:

```
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 CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\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 CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

Related Commands

Command	Description
description	Adds a description to the group created with the **object-group user** command.
group-object	Adds a locally defined object group to a user object group created with the **object-group user** command for use with the Identity Firewall feature.
object-group user	Creates an user group object for the Identity Firewall feature.
user-group	Adds a user group imported from Microsoft Active Directory to the group created with the **object-group user** command.
user-identity enable	Creates the Cisco Identity Firewall instance.

user-alert

To enable broadcast of an urgent message to all clientless SSL VPN users with currently active session, use the **user-alert** command in privileged EXEC mode. To disable the message, use the **no** form of this command.

user-alert *string cancel*
no user-alert

Syntax Description

cancel	Cancels pop-up browser window launch.
string	An alpha-numeric.

Command Default

No message.

Command Modes

The 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.

Usage Guidelines

When you issue this command, end users see a pop-up browser window with the configured message. This command causes no change in the ASA configuration file.

Examples

The following example shows how to enable DAP trace debugging:

```
ciscoasa
 #
We will reboot the security appliance at 11:00 p.m. EST time. We apologize for any
inconvenience.
ciscoasa
 #
```

user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

user-authentication { **enable | disable** }
no user-authentication

Syntax Description

disable	Disables user authentication.
enable	Enables user authentication.

Command Default

User 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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Individual users authenticate according to the order of authentication servers that you configure.

If you require user authentication on the primary ASA, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable user authentication for the group policy named "FirstGroup":

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 user-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
secure-unit-authentication	Provides additional security by requiring the VPN client to authenticate with a username and password each time the client initiates a tunnel.
user-authentication-idle-timeout	Sets an idle timeout for individual users. If there is no communication activity on a user connection in the idle timeout period, the ASA terminates the connection.

user-authentication-idle-timeout

To set an idle timeout for individual users behind hardware clients, use the **user-authentication-idle-timeout** command in group-policy configuration mode. To delete the idle timeout value, use the **no** form of this command. This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, use the **user-authentication-idle-timeout none** command.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the ASA terminates the connection.

user-authentication-idle-timeout { *minutes* | **none** }
no user-authentication-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the idle timeout period. The range is from 1 through 35791394 minutes
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting an user authentication idle timeout value from a default or specified group policy.

Command Default

30 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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

This timer terminates only the client's access through the VPN tunnel, not the VPN tunnel itself.

The idle timeout indicated in response to the **show uauth** command is always the idle timeout value of the user who authenticated the tunnel on the Cisco Easy VPN remote device.

Examples

The following example shows how to set an idle timeout value of 45 minutes for the group policy named "FirstGroup":

```
ciscoasa
(config)#
```

```
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 user-authentication-idle-timeout 45
```

Related Commands

Command	Description
user-authentication	Requires users behind hardware clients to identify themselves to the ASA before connecting.

user-group

To add a user group imported from Microsoft Active Directory to the group created with the **object-group user** command for use with the Identity Firewall feature, use the **user-group** command in the **user-group object** configuration mode. Use the **no** form of this command to remove the user group from the object.

user-group [*domain_nickname* \] *user_group_name*
[**no**] **user-group** [*domain_nickname* \] *user_group_name*

Syntax Description

domain_nickname	(Optional) Specifies the domain in which to create the user group.
user_group_name	Specifies the name for the user group. The group name can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If the group name contains a space, you must enclose the name in quotation marks.

Command Default

If you do not specify the *domain_nickname argument, the user group is created in the LOCAL domain configured for the Identity Firewall feature*.

Command Modes

The 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 user configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for the Identity Firewall feature. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups. A user can belong to local user groups and user groups imported from Active Directory.

The ASA supports up to 256 user groups (including imported user groups and local user groups).

You activate user group objects by including them within an access group, capture, or service policy.

Within a user group object, you can define the following object types:

- **User**—Adds a single user to the object-group user. The user can be either a LOCAL user or imported user.

The name of an imported user must be the sAMAccountName, which is unique, rather than the common name (cn), which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used for imported users defined by the user object.

- User-group—Adds an imported user group, which is defined by an external directory server, such as Microsoft Active Directory server, to the group-object user.

The group name of the user group must be the sAMAccountName, which is unique, rather than the cn, which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used in the *user_group_name* argument specified with the **user-group** keyword.

Note You can add *domain_nickname**user_group_name* or *domain_nickname**user_ name* directly within a user group object without specifying them in the object first. If the *domain_nickname* is associated with a AAA server, the ASA imports the detailed nested user groups and the users defined in the external directory server, such as the Microsoft Active Directory server, to the ASA when the user object group is activated.

- **Group-object**—Adds a group defined locally on the ASA to the object group user.

Note When including an object group within a object group user object, the ASA does not expand the object group in access groups even when you enable ACL optimization. The output of the **show object-group** command does not display the hit count, which is available only for a regular network object group when ACL optimization is enabled.

- **Description**—Adds a description for the object group user.

Examples

The following example shows how to use the **user-group** command with the **user-group object** command to add a user group in a user group object for use with the Identity Firewall feature:

```
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 CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\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 CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

Related Commands

Command	Description
description	Adds a description to the group created with the **object-group user** command.

Command	Description
group-object	Adds a locally defined object group to a user object group created with the **object-group user** command for use with the Identity Firewall feature.
object-group user	Creates a user group object for the Identity Firewall feature.
user	Adds a user to the object group created with the **object-group user** command.
user-identity enable	Creates the Cisco Identity Firewall instance.

user-identity action ad-agent-down

To set the action for the Cisco Identity Firewall instance when the Active Directory Agent is unresponsive, use the **user-identity action ad-agent-down** command in global configuration mode. To remove this action for the Identity Firewall instance, use the **no** form of this command.

user-identity action ad-agent-down disable-user-identity-rule
no user-identity action ad-agent-down disable-user-identity-rule

Syntax Description

This command has no arguments or keywords.

Command Default

By default, 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
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when the AD Agent is not responding.

When the AD Agent is down and the **user-identity action ad-agent-down** command is configured, the ASA disables the user identity rules associated with the users in that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa
(config)#
user-identity action ad-agent-down disable-user-identity-rule
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action domain-controller-down

To set the action for the Cisco Identity Firewall instance when the Active Directory domain controller is down, use the **user-identity action domain-controller-down** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**
no user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.

Command Default

By default, 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
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when the domain is down because Active Directory domain controller is not responding.

When the domain is down and the **disable-user-identity-rule** keyword is configured, the ASA disables the user identity-IP address mapping for that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command.

Examples

The following example shows how to configure this action for the Identity Firewall:

```
ciscoasa(config)#
user-identity action domain-controller-down SAMPLE disable-user-identity-rule
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action mac-address-mismatch

To set the action for the Cisco Identity Firewall instance when a user's MAC address is found to be inconsistent with the ASA device IP address, use the **user-identity action mac-address mismatch** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action mac-address mismatch remove-user-ip
no user-identity action mac-address mismatch remove-user-ip

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA uses **remove-user-ip** when this command 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
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when a user's MAC address is found to be inconsistent with the ASA device IP address currently mapped to that MAC address. The action is to disable the effect of user identity rules.

When the **user-identity action mac-address-mismatch** command is configured, the ASA removes the user identity-IP address mapping for that client.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa
(config)#
user-identity action mac-address-mismatch remove-user-ip
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action netbios-response-fail

To set the action when a client does not respond to a NetBIOS probe for the Cisco Identity Firewall instance, use the **user-identity action netbios-response-fail** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action netbios-response-fail remove-user-ip
no user-identity action netbios-response-fail remove-user-ip

Syntax Description

This command has no arguments or keywords.

Command Default

By default, 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
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when a client does not respond to a NetBIOS probe. For example, the network connection might be blocked to that client or the client is not active.

When the **user-identity action remove-user-ip** command is configured, the ASA removed the user identity-IP address mapping for that client.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa
(config)#
user-identity action netbios-response-fail remove-user-ip
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent aaa-server

To define the server group of the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent aaa-server** command in AAA server host configuration mode. To remove the action, use the **no** form of this command.

user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*
no user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

Syntax Description

aaa_server_group_tag	Specifies the AAA server group associated with the Identity Firewall.

Command Default

This command has 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
Aaa server host configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The first server defined in *aaa_server_group_tag* variable is the primary AD Agent and the second server defined is the secondary AD Agent.

The Identity Firewall supports defining only two AD Agent hosts.

When the ASA detects that the primary AD Agent is down and a secondary agent is specified, it switches to secondary AD Agent. The AAA server for the AD agent uses RADIUS as the communication protocol, and should specify the key attribute for the shared secret between the ASA and AD Agent.

Examples

The following example shows how to define the AD Agent AAA server host for the Identity Firewall:

```
ciscoasa(config-aaa-server-hostkey)#
user-identity ad-agent aaa-server adagent
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent active-user-database

To define how the ASA retrieves the user identity-IP address mapping information from the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent active-user-database** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identityuser-identity ad-agent active-user-database { **on-demand | full-download** }
no user-identityuser-identity ad-agent active-user-database { **on-demand | full-download** }

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA 5505 uses the on-demand option. The other ASA platforms use the full-download 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	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Defines how the ASA retrieves the user identity-IP address mapping information from the AD Agent:

- **full-download**—Specifies that the ASA send a request to the AD Agent to download the entire IP-user mapping table when the ASA starts and then to receive incremental IP-user mapping when users log in and log out.
- **on-demand**—Specifies that the ASA retrieve the user mapping information of an IP address from the AD Agent when the ASA receives a packet that requires a new connection, and the user of its source IP address is not in the user-identity database.

By default, the ASA 5505 uses the on-demand option. The other ASA platforms use the full-download option.

Full downloads are event driven, meaning that subsequent requests to download the database, send just the updates to the user identity-IP address mapping database.

When the ASA registers a change request with the AD Agent, the AD Agent sends a new event to the ASA.

Examples

The following example shows how to configure this option for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent active-user-database full-download
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent hello-timer

To define the timer between the ASA and the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent hello-timer** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*
no user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

Syntax Description

number	Specifies the number of times to retry the timer.
seconds	Specifies the length of time for the timer.

Command Default

By default, the hello timer is set to 30 seconds and 5 retries.

Command Modes

The 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(2)	This command was added.

Usage Guidelines

Defines the hello timer between the ASA and the AD Agent.

The hello timer between the ASA and the AD Agent defines how frequently the ASA exchanges hello packets. The ASA uses the hello packet to obtain ASA replication status (in-sync or out-of-sync) and domain status (up or down). If the ASA does not receive a response from the AD Agent, it resends a hello packet after the specified interval.

By default, the hello timer is set to 30 seconds and 5 retries.

Examples

The following example shows how to configure this option for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent hello-timer seconds 20 retry-times 3
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent event-timestamp-check

To enable RADIUS event time stamp checking to protect the ASA from a change of authorization replay attack, use the **user-identity ad-agent event-timestamp-check** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identity ad-agent event-timestamp-check
no user-identity ad-agent event-timestamp-check

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting 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
9.1(5)	This command was added.

Usage Guidelines

This command enables the ASA to keep track of the last event time stamp that it receives for each identifier and to discard any message if the event time stamp is at least 5 minutes older than the ASA's clock, or if its time stamp is earlier than the last event's time stamp.

For a newly booted ASA that does not have knowledge of the last event time stamp, the ASA compares the event time stamp with its own clock. If the event is at least 5 minutes older, the ASA does not accept the message.

Note We recommend that you configure the ASA, Active Directory, and Active Directory agent to synchronize their clocks among themselves using NTP.

Examples

The following example shows how to configure an event time stamp check for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent event-timestamp-check
```

Related Commands

Command	Description
user-identity ad-agent hello-timer	Defines the timer between the ASA and the AD Agent for the Cisco Identity Firewall instance.

user-identity default-domain

To specify the default domain for the Cisco Identity Firewall instance, use the **user-identity default-domain** command in global configuration mode. To remove the default domain, use the **no** form of this command.

user-identity default-domain *domain_NetBIOS_name*
no user-identity default-domain *domain_NetBIOS_name*

Syntax Description

domain_NetBIOS_name	Specifies the default domain for the Identity Firewall.

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(2)	This command was added.

Usage Guidelines

For *domain_NetBIOS_name,* enter a name up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name contains a space, enclose the entire name in quotation marks. The domain name is not case sensitive.

The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. For multiple context mode, you can set a default domain name for each context, as well as within the system execution space.

Note The default domain name you specify must match the NetBIOS domain name configured on the Active Directory domain controller. If the domain name does not match, the AD Agent will incorrectly associate the user identity-IP address mapping with the domain name that you enter when configuring the ASA. To view the NetBIOS domain name, open the Active Directory user event security log in any text editor.

The Identity Firewall uses the LOCAL domain for all locally defined user groups or locally defined users. Users logging in through a web portal (cut-through proxy) are designated as belonging to the Active Directory domain with which they authenticated. Users logging in through a VPN are designated as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with Active Directory, so that the Identity Firewall can associate the users with their Active Directory domain.

Examples

The following example shows how to configure the default domain for the Identity Firewall:

```
ciscoasa(config)#
user-identity default-domain SAMPLE
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity domain

To associate the domain for the Cisco Identity Firewall instance, use the **user-identity domain** command in global configuration mode. To remove the domain association, use the **no** form of this command.

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*
no user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

Syntax Description

aaa_server_group_tag	Specifies the AAA server group associated with the Identity Firewall.
domain_nickname	Specifies the domain name for the Identity Firewall.

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(2)	This command was added.

Usage Guidelines

Associates the LDAP parameters defined for the AAA server for importing user group queries with the domain name.

For *domain_nickname,* enter a name up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name contains a space, you must enclose that space character in quotation marks. The domain name is not case sensitive.

Examples

The following example shows how to associate the domain for the Identity Firewall:

```
ciscoasa(config)#
user-identity domain SAMPLE aaa-server ds
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity enable

To create the Cisco Identity Firewall instance, use the **user-identity enable** command in global configuration mode. To disable the Identity Firewall instance, use the **no** form of this command.

user-identity enable
no user-identity enable

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
8.4(2)	This command was added.

Usage Guidelines

This command enables the Identity Firewall.

Examples

The following example shows how to enable the Identity Firewall:

```
ciscoasa
(config)# user-identity enable
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity inactive-user-timer

To specify the amount of time before a user is considered idle for the Cisco Identity Firewall instance, use the **user-identity inactive-user-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

user-identity inactive-user-timer minutes *minutes*
no user-identity inactive-user-timer minutes *minutes*

Syntax Description

minutes	Specifies the amount of time in minutes before a user is considered idle, meaning the ASA has not received traffic from the user's IP address for the specified amount of time.

Command Default

By default, the idle timeout is set to 60 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	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When the timer expires, the user's IP address is marked as inactive and removed from the local cached user identity-IP address mapping database and the ASA no longer notifies the AD Agent about that IP address removal. Existing traffic is still allowed to pass. When this command is specified, the ASA runs an inactive timer even when the NetBIOS Logout Probe is configured.

Note The Idle Timeout option does not apply to VPN or cut-through-proxy users.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)#
user-identity inactive-user-timer minutes 120
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity logout-probe

To enable NetBIOS probing for the Cisco Identity Firewall instance, use the **user-identity logout-probe** command in global configuration mode. To remove the disable probing, use the **no** form of this command.

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]
no user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

Syntax Description

minutes	Specifies the number of minutes between probes.
seconds	Specifies the length of time for the retry interval.
times	Specifies the number of times to retry the probe.

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(2)	This command was added.

Usage Guidelines

To minimize the NetBIOS packets, the ASA only sends a NetBIOS probe to a client when the user has been idle for more than the specified number of minutes.

Set the NetBIOS probe timer from1 to 65535 minutes and the retry interval from 1 to 256 retries. Specify the number of times to retry the probe:

- **match-any**—As long as the NetBIOS response from the client contains the user name of the user assigned to the IP address, the user identity is be considered valid. Specifying this option requires that the client enabled the Messenger service and configured a WINS server.
- **exact-match**—The user name of the user assigned to the IP address must be the only one in the NetBIOS response. Otherwise, the user identity of that IP address is considered invalid. Specifying this option requires that the client enabled the Messenger service and configured a WINS server.
- **user-not-needed**—As long as the ASA received a NetBIOS response from the client the user identity is considered valid.

The Identity Firewall only performs NetBIOS probing for those users identities that are in the active state and exist in at least one security policy. The ASA does not perform NetBIOS probing for clients where the users logged in through cut-through proxy or by using VPN.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity monitor

For Cloud Web Security, to download the specified user or group information from the AD agent, use the user-identity monitor command in global configuration mode. To stop monitoring, use the **no** form of this command.

user-identity monitor { **user-group** [*domain-name* \\ ] *group-name* | **object-group-user** *object-group-name*
no user-identity monitor { **user-group** [*domain-name* \\ ] *group-name* | **object-group-user** *object-group-name*

Syntax Description

object-group-user *object-group-name*	Specifies an **object-group user** name. This group can include multiple groups.
user-group [*domain-name*\\]*group-name*	Specifies a group name inline. Although you specify 2 backslashes (\\) between the domain and the group, the ASA modifies the name to include only one backslash when it sends it to Cloud Web Security, to comply with Cloud Web Security notation conventions.

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
8.4(2)	This command was added.

Usage Guidelines

When you use the Identity Firewall feature, the ASA only downloads user identity information from the AD server for users and groups included in active ACLs; the ACL must be used in a feature such as an access rule, AAA rule, service policy rule, or other feature to be considered active. Because Cloud Web Security can base its policy on user identity, you may need to download groups that are not part of an active ACL to get full Identity Firewall coverage for all your users. For example, although you can configure your Cloud Web Security service policy rule to use an ACL with users and groups, thus activating any relevant groups, it is not required; you could use an ACL based entirely on IP addresses. The user identity monitor feature lets you download group information directly from the AD Agent.

The ASA can only monitor a maximum of 512 groups, including those configured for the user identity monitor and those monitored through active ACLs.

Examples

The following example monitors the CISCO\\Engineering usergroup:

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

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.

user-identity poll-import-user-group-timer

To specify the amount of time before the ASA queries the Active Directory server for user group information for the Cisco Identity Firewall instance, use the **user-identity poll-import-user-group-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

user-identity poll-import-user-group-timer hours *hours*
no user-identity poll-import-user-group-timer hours *hours*

Syntax Description

hours	Sets the hours for the poll timer.

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(2)	This command was added.

Usage Guidelines

Specifies the amount of time before the ASA queries the Active Directory server for user group information.

If a user is added to or deleted from to an Active Directory group, the ASA received the updated user group after import group timer runs.

By default, the poll timer is 8 hours.

To immediately update user group information, enter the **user-identity update import-user** command:

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)#
user-identity poll-import-user-group-timer hours 1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity static user

To create a new user-IP address mapping or set a user's IP address to inactive for the Cisco Identity Firewall feature, use the **user-identity static user** command in global configuration mode. To remove this configuration for the Identity Firewall, use the **no** form of this command.

user-identity static user [*domain* \] *user_name host_ip*
no user-identity static user [*domain* \] *user_name host_ip*

Syntax Description

domain	Creates a new user-IP address mapping or sets the IP address to inactive for the user in the specified domain.
host_ip	Specifies the IP address of the user for which to create a new user-IP address mapping or to set as inactive.
user_name	Specifies the user name for which to create a new user-IP address mapping or the user or sets the users IP address to inactive.

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)	The command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

The following example shows how to create a static maping for user1.

```
ciscoasa
(config)#
user-identity static user SAMPLE\user1 192.168.1.101
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity update active-user-database

To download the entire active-user database from the Active Directory Agent, use the **user-identity update active-user-database** command in global configuration mode.

user-identity update active-user-database [**timeout minutes** *minutes*]

Syntax Description

minutes	Specifies the number of minutes for the timeout.

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	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command downloads the entire active-user database from Active Directory Agent.

This command starts the update operation, generates a starting update log and returns immediately. When the update operation finishes or is aborted at timer expiration, another syslog message is generated. Only one outstanding update operation is allowed. Rerunning the command displays an error message.

When the command finishes running, the ASA displays [Done] at the command prompt then generates a syslog message.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa# user-identity update active-user-database
ERROR: one update active-user-database operation is already in progress
[Done] user-identity update active-user-database
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity update import-user

To download the entire active user database from the Active Directory Agent, use the **user-identity update active-user-database** command in global configuration mode.

user-identity update import-user [[*domain_nickname* \\ ] *user_group_name* [**timeout seconds** *seconds*]]

Syntax Description

domain_nickname	Specifies the domain of the group to update.
seconds	Specifies the number of seconds for the timeout.
user_group_name	When *user_group_name* is specified, only the specified import-user group is updated. Only activated groups (for example, groups in an access group, access list, capture, or service policy) can be updated. If the given group is not activated, this command rejects the operation. If the specified group has multiple levels of hierarchies, recursive LDAP queries are conducted. If *user_group_name* is not specified, the ASA starts the LDAP update service immediately and tries to periodically update all activated groups.

Command Default

The ASA retries the update up to 5 times and generates warning messages as necessary.

Command Modes

The 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(2)	This command was added.

Usage Guidelines

This command updates the specified import user group database by querying the Active Directory server immediately without waiting for the expiration of the poll import user group timer. There is no command to update the local user group, because the group ID database is updated whenever the local user group has a configuration change.

This command does not block the console to wait for the return of the LDAP query.

This command starts the update operation, generates a starting update log and returns immediately. When the update operation finishes or is aborted at timer expiration, another syslog message is generated. Only one outstanding update operation is allowed. Rerunning the command displays an error message.

If the LDAP query is successful, the ASA stores retrieved user data in the local database and changes the user/group association accordingly. If the update operation is successful, you can run the **show user-identity user-of-group** *domain\\group* command to list all stored users under this group.

The ASA checks after each update for all imported groups. If an activated Active Directory group does not exist in Active Directory, the ASA generates a syslog message.

If *user_group_name* is not specified, the ASA starts the LDAP update service immediately and tries to periodically update all activated groups. The LDAP update service runs in the background and periodically updates import user groups via an LDAP query on the Active Directory server.

At system boot up time, if there are import user groups defined in access groups, the ASA retrieves user/group data via LDAP queries. If errors occur during the update, the ASA retries the update up to 5 times and generates warning messages as necessary.

When the command finishes running, the ASA displays [Done] at the command prompt then generates a syslog message.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa# user-identity update import-user group.sample-group1
ERROR: Update import-user group is already in progress
[Done] user-identity update import-user group.sample-group1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity user-not-found

To enable user-not-found tracking for the Cisco Identity Firewall instance, use the **user-identity user-not-found** command in global configuration mode. To remove this tracking for the Identity Firewall instance, use the **no** form of this command.

user-identity user-not-found enable
no user-identity user-not-found enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, 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
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Only the last 1024 IP addresses are tracked.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa
(config)#
user-identity user-not-found enable
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-message

To specify a text message to display when a DAP record is selected, use the user-message command in dynamic-access-policy-record mode. To remove this message, use the **no** version of the command. If you use the command more than once for the same DAP record, the newer message replaces the previous message.

user-message *message*
no user-message

Syntax Description

message	The message for users assigned to this DAP record. Maximum 128 characters. If the message contains spaces, enclose it 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
Dynamic-access-policy-record	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

For a successful SSL VPN connection, the portal page displays a flashing, clickable icon that lets the user see the message(s) associated with the connection. If the connection is terminated from a DAP policy (action = terminate), and if there is a user message configured in that DAP record, then that message displays on the login screen.

If more than one DAP record applies to a connection, the ASA combines the applicable user messages and displays them as a single string.

Examples

The following example shows how to set a user message of "Hello Money Managers" for the DAP record called Finance.

```
ciscoasa
 (config) config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 user-message "Hello Money Managers"
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

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.

user-parameter

To specify the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication, use the **user-parameter** command in aaa-server-host configuration mode.

user-parameter *name*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string The name of the username parameter included in the HTTP POST request. The maximum name size is 128 characters.

Command Default

There is 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

This is an SSO with HTTP Forms command. The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.

Note At login, the user enters the actual name value which is entered into the HTTP POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies that the username parameter userid be included in the HTTP POST request used for SSO authentication:

```
ciscoasa(config)# aaa-server testgrp1 host example.com
```

```
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(config-aaa-server-host)#
```

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.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.

user-statistics

To activate the collection of user statistics by MPF and match lookup actions for the Identify Firewall, use the **user-statistics** command in policy-map configuration mode. To remove collection of user statistics, use the **no** form of this command.

user-statistics [**accounting | scanning**]
no user-statistics [**accounting | scanning**]

Syntax Description

accounting	(Optional) Specifies that the ASA collect the sent packet count, sent drop count, and received packet count.
scanning	(Optional) Specifies that the ASA collect only the sent drop count.

Command Default

By default, 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
Policy-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When you configure a policy map to collect user statistics, the ASA collects detailed statistics for selected users. When you specify the **user-statistics** command without the **accounting** or **scanning** keywords, the ASA collects both accounting and scanning statistics.

Examples

The following example shows how to activate user statistics for the Identity Firewall:

```
ciscoasa
(config)#
class-map c-identity-example-1
ciscoasa
(config-cmap)#
match access-list identity-example-1
ciscoasa
(config-cmap)#
exit
ciscoasa
(config)#
policy-map p-identity-example-1
```

```
ciscoasa
(config-pmap)#
class c-identity-example-1
ciscoasa
(config-pmap)#
user-statistics accounting
ciscoasa
(config-pmap)#
exit
ciscoasa
(config)#
service-policy p-identity-example-1 interface outside
```

Related Commands

Command	Description
policy-map	Assigns actions to traffic that you identified with a Layer 3/4 class map when using the Modular Policy Framework.
service-policy(**global**)	Activates a policy map globally on all interfaces or on a targeted interface.
show service-policy [**user-statistics**]	Displays user statistics for configured service policies when you enable user-statistics scanning or accounting for the Identity Firewall.
show user-identity ip-of-user [**detail**]	Displays received packets, sent packets, and drops statistics for the IP address for a specified user when you enable user statistics scanning or accounting for the Identity Firewall.
show user-identity user active [**detail**]	Displays received packets, sent packets and drops statistics in the specified time period for active users when you enable user statistics scanning or accounting for the Identity Firewall.
show user-identity user-of-ip [**detail**]	Displays received packets, sent packets, and drops statistics for the user for a specified IP address when you enable user statistics scanning or accounting for the Identity Firewall.
user-identity enable	Creates the Identity Firewall instance.

user-storage

To store personalized user information between clientless SSL VPN sessions, use the **user storage** command in group-policy webvpn configuration mode. To disable user storage, use the **no** form of the command.

user-storage *NETFS-location*
no user-storage

Syntax Description

NETFS-location	Specifies a file system desination in the form proto://user:password@host:port/path If the username and password are embedded in the NETFS-location then the password input is treated as clear.

Command Default

User 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 webvpn mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.4(6)	Prevented the password being shown in clear text during show-run.

Usage Guidelines

User-storage enables you to store cached credentials and cookies at a location other than the ASA flash. This command provides single sign on for personal bookmarks of a clientless SSL VPN user. The user credentials are stored in an encrypted format on the FTP/CIFS/SMB server as a <user_id>.cps file that is not decryptable.

Although the username, password, and preshared key are shown in the configuration, this poses no security risk because the ASA stores this information in encrypted form, using an internal algorithm.

If data is encrypted on an external FTP or SMB server, you can define personal bookmarks within the portal page by selecting add bookmark (for example: user-storage cifs://jdoe:test@10.130.60.49/SharedDocs). You can create personalized URLs for all plugin protocols as well.

Note If you have a cluster of ASAs that all refer to the same FTP/CIFS/SMB server and use the same “storage-key,” you can access the bookmarks through any of the ASAs in the cluster.

Examples

The following example shows how to set user storage for a user called newuser with a password of 12345678 at a file share called anyshare, and a path of anyfiler02a/new_share:

```
ciscoasa
(config)#
wgroup-policy DFLTGrpPolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)#
 user-storage cifs://newuser:12345678@anyfiler02a/new_share
ciscoasa(config-group_webvpn)#
```

Related Commands

Command	Description
storage-key	Specifies a storage key to protect the data stored between sessions.
storage-objects	Configures storage objects for the data stored between sessions.

username

To add a user to the ASA local database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username that you want to remove.

username *name* [**password** *password* [**pbkdf2 | mschap | encrypted | nt-encrypted**] **| nopassword**] [**privilege** *priv_level*]
no username *name* [**password** *password* [**pbkdf2 | mschap | encrypted | nt-encrypted**] **| nopassword**] [**privilege** *priv_level*]

Syntax Description

encrypted	For 9.6 and earlier, indicates that the password is encrypted (if you did not specify **mschap**) for passwords 32 characters and fewer. When you define a password in the **username** command, the ASA creates an MD5 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** command output would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s encrypted` The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password. In 9.7 and later, passwords of all lengths use PBKDF2.
mschap	Specifies that the password will be converted to Unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using MSCHAPv1 or MSCHAPv2.
name	Specifies the name of the user as a string from 3 to 64 characters in length, using any combination of ASCII printable characters with the exception of spaces and the question mark.
nopassword	Indicates that *any* password can be entered for this user. This is an insecure configuration, so use this keyword with caution. (9.6(2) and later) To create a username without a password, do not enter the **password** or **nopassword** keywords. For example the **ssh authentication** command allows you to install a public key on the ASA and use a private key with your SSH client, so you may not want any password configured.

nt-encrypted	Indicates that the password is encrypted for use with MSCHAPv1 or MSCHAPv2. If you specified the **mschap** keyword when you added the user, then this keyword is displayed instead of the **encrypted** keyword when you view the configuration using the **show running-config** command. When you define a password in the **username** command, the ASA encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **nt-encrypted** keyword. For example, if you enter the password "test," the **show running-config** display would appear to be something like the following: `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` The only time you would actually enter the **nt-encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password.

password *password*	Sets the password as a case-sensitive string of 8 to 127 alphanumeric and special characters. You can use any character in the password with the following exceptions:
	
	• No spaces
	• No question marks
	• You cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected:
	  • **abc**user1
	  • user**543**
	  • user**aaaa**
	  • user2**666**

pbkdf2	Indicates that the password is encrypted. For 9.6 and earlier, the PBKDF2 (Password-Based Key Derivation Function 2) hash is used only when the password is more than 32 characters in length. In 9.7 and later, all passwords use PBKDF2. When you define a password in the **username** command, the ASA creates a PBKDF2 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **pbkdf2** keyword. For example, if you enter a long password, the **show running-config** command output would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s pbkdf2` The only time you would actually enter the **pbkdf2** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password. Note that already existing passwords continue to use the MD5-based hash unless you enter a new password.
privilege *priv_level*	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

Command Default

The default privilege level 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
7.0.1	This command was added.
7.2(1)	The **mschap** and **nt-encrypted** keywords were added.
9.6(1)	The password length was increased to 127 characters, and the **pbkdf2** keyword was added.
9.6(2)	You can now create a username without the **password** or **nopassword** keywords.
9.7(1)	Passwords of all lengths are now saved to the configuration using the PBKDF2 hash.
9.17(1)	The minumum password length was changed from 3 to 8 characters. Also you cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666**

Usage Guidelines

The **login** command uses this database for authentication.

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. (See the **aaa authorization command** command.) 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 AAA authentication so the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the **enable** password to access privileged EXEC mode.

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the **username attributes** command.

When password authentication policy is enabled, you can no longer change your own password or delete your own account with the **username** command. You can, however, change your password with the **change-password** command.

To display the username password date, use the **show running-config all username** command.

Examples

The following example shows how to configure a user named “anyuser” with a password of 12345678 and a privilege level of 12:

```
ciscoasa
(config)#
 username anyuser password 12345678 privilege 12
```

Related Commands

Command	Description
aaa authorization command	Configues command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs for a specified user.

username *name***attributes**
no username *name* **attributes**

Syntax Description

name Provides the name of the user.

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 configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **service-type** attribute was added.
9.1(2)	The **ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} attribute was added.

Usage Guidelines

The internal user authentication database consists of the users entered with the **username** command. The **login** command uses this database for authentication. You can configure the username attributes using either the **username** command or the **username attributes** command.

The command syntax in username configuration mode has the following characteristics in common:

- The **no** form removes the attribute from the running configuration.
- The **none** keyword also removes the attribute from the running configuration. But it does so by setting the attribute to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

The **username attributes** command enters username attributes mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Names an existing tunnel group with which the user is required to connect.
password-storage	Enables or disables storage of the login password on the client system.
service-type [**remote-access** | **admin** | **nas-prompt**]	Restricts console login and enables login for users who are assigned the appropriate level. The **remote-access** option specifies basic AAA services for remote access. The **admin** option specifies AAA services, login console privileges, EXEC mode privileges, the enable privilege, and CLI privileges. The **nas-prompt** option specifies AAA services, login console privileges, EXEC mode privileges, but no enable privileges.
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	Enables public key authentication on a per-user basis. The value of the *key* argument can refer to the following: • When the *key* argument is supplied and the hashed tag is not specified, the value of the key must be a base64 encoded public key that is generated by SSH key generation software that can generate SSH-RSA raw keys (that is, with no certificates). After you submit the base64 encoded public key, that key is then hashed via SHA-256 and the corresponding 32-byte hash is used for all further comparisons. • When the *key* argument is supplied and the hashed tag is specified, the value of the key must have been previously hashed with SHA-256 and be 32 bytes long, with each byte separated by a colon (for parsing purposes). The **pkf** option enables you to authenticate using 4096-bit RSA keys as an SSH public key file (PKF). This option is not restricted to 4096-bit RSA keys, but can be used for any size less than or equal to 4096-bit RSA keys. The nointeractive option suppresses all prompts when importing an SSH public key formatted key. This noninteractive data entry mode is only intended for ASDM use. The *key* field and the **hashed** keyword are only available with the **publickey** option, and the **nointeractive** keyword is only available with the **pkf** option. When you save the configuration, the hashed key value is saved to the configuration and used when the ASA is rebooted. **Note** You can use the PKF option when failover is enabled, but the PKF data is not automatically replicated to the standby system. You must enter the **write standby** command to synchronize the PKF setting to the standby system in the failover pair.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL.
vpn-framed-ip-address	Specifies the IP address and the netmask to be assigned to the client.
vpn-group-policy	Specifies the name of a group policy from which to inherit attributes.
vpn-idle-timeout [**alert-interval**]	Specifies the idle timeout period in minutes, or **none** to disable it. Optionally specifies a pre-timeout alert interval.

Attribute	Function
vpn-session-timeout [**alert-interval**]	Specifies the maximum user connection time in minutes, or **none** for unlimited time. Optionally specifies a pre-timeout alert interval.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters username webvpn configuration mode, in which you configure WebVPN attributes.

You configure webvpn-mode attributes for the username by entering the **username attributes** command and then entering the **webvpn** command in username webvpn configuration mode. See the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter username attributes configuration mode for a user named "anyuser":

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
```

Related Commands

Command	Description
clear config username	Clears the username database.
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the ASA database.
webvpn	Enters webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

username-from-certificate

To specify the field in a certificate to use as the username for authorization, use the **username-from-certificate** command in tunnel-group general-attributes mode. The DN of the peer certificate used as username for authorization

To remove the attribute from the configuration and restore default values, use the **no** form of this command.

username-from-certificate { *primary-attr* [*secondary-attr*] | **use-entire-name** }
no username-from-certificate

Syntax Description

primary-attr	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enable, the derived name can also be used in an authentication query.
use-entire-name	Specifies that the ASA must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
use-script	Specifies the use of a script file generated by ASDM to extract the DN fields from a certificate for use as a username.

Command Default

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

Command Modes

The 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(4)	This command was added.

Usage Guidelines

This command selects the field in the certificate to use as the username. It replaces the deprecated **authorization-dn-attributes** command in Release 8.0(4) and following. The **username-from-certificate** command forces the security appliance to use the specified certificate field as the username for username/password authorization.

To use this derived username in the pre-fill username from certificate feature for username/passwordauthentication or authorization, you must also configure the **pre-fill-username** command in tunnel-group webvpn-attributes mode. That is, to use the pre-fill username feature, you must configure both commands.

Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.
use-entire-name	Use entire DN name. Not available as a secondary attribute.
use-script	Use a script file generated by ASDM.

Note When multiple DN attributes are configured in a certificate, ASA extracts the username from the last subject DN attribute.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute and OU as the secondary attribute to use to derive a name for an authorization query from a digital certificate:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN OU
ciscoasa(config-tunnel-general)#
```

The following example shows how to modify the tunnel-group attributes to configure the pre-fill username.

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
 secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

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-choice

To select the certificate from where the username should be used for pre-fill username field for primary authentication or authorization, use the **username-from-certificate-choice** command. Use this command in tunnel-group general-attributes mode. To use the username from the default certificate, use the **no** form of the command.

username-from-certificate-choice { **first-certificate | second-certificate** }
no username-from-certificate-choice { **first-certificate | second-certificate** }

Syntax Description

first-certificate	Specifies if the username from the machine certificate sent in SSL or IKE to be used in pre-fill username field for primary authentication.
second-certificate	Specifies if the username from the user certificate from client to be used in pre-fill username field for peimary authentication.

Command Default

The username for prefill is retrieved from the second certificate 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
9.14(1)	This command was added.

Usage Guidelines

The multiple certificates option allows certificate authentication of both the machine and user via certificates. The pre-fill username field allows a field from the certificates to be parsed and used for subsequent (primary and secondary) AAA authentication in a AAA and certificate authenticated connection. The username for prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to choose whether the first certificate (machine certificate) or second certificate (user certificate) should be used to derive the username for the pre-fill username field.

This command is available and can be configured for any tunnel groups irrespective of the authentication type (aaa, certificate, or multiple-certificate). However, the configuration takes effect only for Multiple Certificate Authentication (multiple-certificate or aaa multiple-certificate). When the option is not used for Multiple Certificate Authentication, the second certificate is used by default for authentication or authorization purpose.

Examples

The following example shows how to configure the certificate to be used for prefill username for primary and secondary authentication or authorization:

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>

ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice first-certificate
ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

Related Commands

Command	Description
secondary-username-from-certificate-choice	Specify the certificate option for secondary authentication.

username password-date

To enable the system to restore a password creation date at boot time or when copying a file to the running configuration, enter the **username pasword-date** command in non-interactive configuration mode; in other words, this command is only available when booting up a configuration file with this command already present; you cannot enter this command at the CLI prompt.

username *name* **password-date** *date*

Syntax Description

name	Specifies the name of the user as a string from 3 to 64 characters in length, using any combination of ASCII printable characters with the exception of spaces and the question mark.
date	Enables the system to restore password creation dates for usernames, which are read in during bootup. If not present, the password date is set to the current date. The date is in the format, mmm-dd-yyyy.

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
Non-interactive	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

To display the username password date, use the **show running-config all username** command.

You cannot enter **username password-date** values from a CLI prompt. The password date is saved to the startup configuration only if the password policy lifetime is not zero. This means that password dates are saved only if password expiration is configured. You cannot use the **username password-date** command to prevent users from changing password creation dates.

Related Commands

Command	Description
aaa authorization command	Configues command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.

Command	Description
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username-prompt

To customize the username prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **username-prompt** command from webvpn customization mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

username-prompt { **text | style** } *value*
[**no**] **username-prompt** { **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 is text of the username prompt is "USERNAME:".

The default style of the username prompt is color:black;font-weight:bold;text-align:right.

Command Modes

The 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	• 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 text is changed to "Corporate Username:", and the default style is changed with the font weight increased to bolder:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# username-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page.
password-prompt	Customizes the password prompt of the WebVPN page.

V

validate-attribute

To validate RADIUS attributes when using RADIUS accounting, use the **validate-attribute** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

validate-attribute [*attribute_number*]
no validate-attribute [*attribute_number*]

Syntax Description

attribute_number	The RADIUS attribute to be validated with RADIUS accounting. Values range from 1-191. Vendor Specific Attributes are not supported.

Command Default

This option 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
Radius-accounting parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When this command is configured, the security appliance will also do a match on these attributes in addition to the Framed IP attribute. Multiple instances of this command are allowed.

You can find a list of RADIUS attribute types here:

http://www.iana.org/assignments/radius-types

Examples

The following example shows how to enable RADIUS accounting for the user name RADIUS attribute:

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate-attribute 1
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

validate-kdc

To enable the authentication of the Kerberos Key Distribution Center (KDC) using an uploaded keytab file, use the **validate-kdc** command in aaa-server group mode. To disable KDC authentication, use the **no** form of this command.

validate-kdc
no validate-kdc

Command Default

This option 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
aaa-server group	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.8(4)	This command was added.

Usage Guidelines

You can configure a Kerberos AAA server group to authenticate the servers in the group using the **validate-kdc** command. To accomplish the authentication, you must also import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

When you enable KDC validation, after obtaining the ticket-granting ticket (TGT) and validating the user, the system also requests a service ticket on behalf of the user for **host**/*ASA_hostname*. The system then validates the returned service ticket against the secret key for the KDC, which is stored in a keytab file that you generated from the KDC and then uploaded to the ASA. If KDC authentication fails, the server is considered untrusted and the user is not authenticated.

To accomplish KDC authentication, you must do the following:

1. (On the KDC.) Create a user account in the Microsoft Active Directory for the ASA (go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**). For example, if the fully-qualified domain name (FQDN) of the ASA is asahost.example.com, create a user named asahost.
2. (On the KDC.) Create a host service principal name (SPN) for the ASA using the FQDN and user account:

```
C:> setspn -A HOST/asahost.example.com asahost
```

1. (On the KDC.) Create a keytab file for the ASA (line feeds added for clarity):

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
```

```
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

1. (On the ASA.) Import the keytab (in this example, new.keytab) to the ASA using the **aaa kerberos import-keytab** command.
2. (On the ASA.) Add the **validate-kdc** command to the Kerberos AAA server group configuration. The keytab file is used only by server groups that contain this command.

Note You cannot use KDC validation in conjunction with Kerberos Constrained Delegation (KCD). The **validate-kdc** command will be ignored if the server group is used for KCD.

Examples

The following example shows how to import a keytab named new.keytab that resides on an FTP server, and enable KDC validation in a Kerberos AAA server group.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab

ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

Related Commands

Commands	Description
aaa kerberos import-keytab	Imports a Kerberos keytab file that was exported from a Kerberos Key Distribution Center (KDC)
clear aaa kerberos keytab	Clears the imported Kerberos keytab file.
show aaa kerberos keytab	Shows information about the Kerberos keytab file.

validate-key

To specify the pre-shared key for LISP messages, use the **validate-key** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect lisp** command. To remove the key, use the **no** form of this command.

validate-key *key*
no validate-key *key*

Syntax Description

key	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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Specify the LISP pre-shared key so the ASA can read LISP message contents.

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 limits EIDs to those on the 10.10.10.0/24 network and specifies the pre-shared key:

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

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.

validation-policy

To specify the conditions under which a trustpoint can be used to validate the certificates associated with an incoming user connection, use the **validation-policy command** in crypto ca trustpoint configuration mode. To specify that the trustpoint cannot be used for the named condition, use the **no** form of the command.

[**no**] **validation-policy** { **ssl-client | ipsec-client** } [**no-chain**] [**subordinate-only**]

Syntax Description

ipsec-client	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate IPsec connections.
no-chain	Disables the chaining of subordinate certificates that are not resident on the security device.
ssl-client	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate SSL connections.
subordinate-only	Disables validation of client certificates issued directly from the CA represented by this trustpoint.

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
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Remote-access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to virtually any network application or resource. The **validation-policy** command allows you to specify the protocol type permitted to access on-board CA certificates.

The **no-chain** option with this command prevents an ASA from supporting subordinate CA certificates that are not configured as trustpoints on it.

The ASA can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is disabled automatically if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated

to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint, central, and designates it an SSL trustpoint:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint, checkin1,and sets it to accept certificates that are subordinate to the specified trustpoint.

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

validation-usage

To specify the usage types for which validation with this trustpoint is allowed, use the **validation-usage command** in crypto ca trustpoint configuration mode. To not specify the usage types, use the **no** form of the command.

validation-usage ipsec-client | ssl-client | ssl-server
no validation-usage ipsec-client | ssl-client | ssl-server

Syntax Description

ipsec-client	Indicates that IPsec client connections can be validated using this trustpoint.
ssl-client	Indicates that SSL client connections can be validated using this trustpoint.
ssl-server	Indicates that SSL server certificates can be validated using this trustpoint.

Command Default

ipsec-client, ssl-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
Crypto ca trustpoint configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added to replace the client-types command.

Usage Guidelines

When there are multiple trustpoints associated with the same CA certificate, only one of the trustpoints can be configured for a specific client type. However, one of the trustpoints can be configured for one client type and the other trustpoint with another client type.

If there is a trustpoint associated with the same CA certificate that is already configured with a client type, the new trustpoint is not allowed to be configured with the same client-type setting. The **no** form of the command clears the setting so that a trustpoint cannot be used for any client validation.

Remote access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to any network application or resource.

Related Commands

Command	Description
crypto ca trustpoint	Enters the crypto ca trustpoint configuration mode for the specified trustpoint.

vdi

To provide secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA, use the **vdi** command.

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

Syntax Description

domain *domain*	Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.
password *password*	Password for logging into the virtualization infrastructure server. This value can be a clientless macro.
type	Type of VDI. For a Citrix Receiver type, this value must be *citrix* .
url *url*	Full URL of the XenApp or XenDesktop server including http or https, hostname, and port number, as well as the path to the XML service.
username *username*	Username for logging into the virtualization infrastructure server. This value can be a clientless macro.

Command Modes

The 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
9.0(1)	This command was added.

Usage Guidelines

In a VDI model, administrators publish desktops pre-loaded with enterprise applications, and end users remotely access these desktops. These virtualized resources appear just as any other resources, such as email, so that users do not need to go through a Citrix Access Gateway to access them. Users log onto the ASA using Citrix Receiver mobile client, and the ASA connects to a pre-defined Citrix XenApp or XenDesktop Server. The administrator must configure the Citrix server's address and logon credentials under Group Policy so that when users connect to their Citrix Virtualized resource, they enter the ASA's SSL VPN IP address and credentials instead of pointing to the Citrix Server's address and credentials. When the ASA has verified the credentials, the receiver client starts to retrieve entitled applications through the ASA.

Supported Mobile Devices

- iPad—Citrix Receiver version 4.x or later
- iPhone/iTouch—Citrix Receiver version 4.x or later

- Android 2.x phone—Citrix Receiver version 2.x or later
- Android 3.x tablet—Citrix Receiver version 2.x or later
- Android 4.0 phone—Citrix Receiver version 2.x or later

Examples

If both username and group policy are configured, username settings take precedence over group policy.

```
configure terminal
 group-policy DfltGrpPolicy attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>
configure terminal
 username <username> attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>]
```

Related Commands

Command	Description
debug webvpn citrix	Provides insight into the process of launching Citrix-based applications and desktops.

verify

To verify the checksum of a file, use the **verify** command in privileged EXEC mode.

verify*path*
verify { **/md5 | sha-512** } *path* [*expected_value*]
verify /signature running

Syntax Description

/md5	Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
/sha-512	Calculates and displays the SHA-512 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
/signature running	Verifies the signature of the running ASA image.
expected_value	(Optional) The known hashed value for the specified image. The ASA displays a message verifying that the hashed values match or that there is a mismatch.

path	• **disk0:**/[*path*/]*filename* Indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* Indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This option indicates the internal Flash card. **flash** is an alias for **disk0:**. • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: • **ap**—ASCII passive mode • **an**—ASCII normal mode • **ip**—(Default) Binary passive mode • **in**—Binary normal mode • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **verify** command. • **system:running-config** Calculates or verifies the hash for the running configuration. • **system:text** Calculates or verifies the hash for the text of the ASA process.

Command Default

The current flash device is the default file system.

Note When you specify the **/md5** or **/sha-512** option, you can use a network file, such as from FTP, HTTP or TFTP, as the source. The **verify** command without the **/md5** or **/sha-512** option only lets you verify local images in flash.

Command Modes

The 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
7.2(1)	This command was added.
9.3(2)	The **signature** keyword was added.
9.6(2)	The **system:text** option was added.

Usage Guidelines

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into flash memory or onto a server. A variety of image information is available on Cisco.com.

To display the contents of flash memory, use the **show flash** command. The flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the ASA and saved in the file system without detection. If a corrupt image is transferred successfully to the ASA, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of the ASA software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all security appliance software images for comparison against local system image values. You can also specify SHA-512 (**/sha-512**).

To perform the MD5 or SHA-512 integrity check, issue the **verify** command using the **/md5** or **/sha-512** keyword. For example, issuing the **verify /md5 flash:cdisk.bin** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

The following example shows the **verify** command used on an image file called cdisk.bin. Some of the text was removed for clarity:

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

The following example shows the **verify** command used on a signature image in disk0:

```
ciscoasa(config)# verify lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validate
ciscoasa(config)# verify /signature lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validated
ciscoasa(config)# verify /signature cdisk.smp
Verifying file integrity of disk0:/cdisk.smp
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f05997fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

Related Commands

Command	Description
copy	Copies files.
dir	Lists the files in the system.

verify-header

To allow only known IPv6 extension headers and enforces the order of IPv6 extension headers, use the **verify-header** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect ipv6** command. To disable these parameters, use the **no** form of this command.

verify-header { **order** | **type** }
no verify-header { **order** | **type** }

Syntax Description

order	Enforces the order of IPv6 extension headers as defined in the RFC 2460 specification.
type	Allows only known IPv6 extension headers.

Command Default

Both order and type 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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

These parameters are enabled by default. To disable them, enter the no keyword.

Examples

The following example disables the order and type parameters for an IPv6 inspection policy map:

```
ciscoasa(config)# policy-map type inspect ipv6 ipv6-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# no verify-header order
ciscoasa(config-pmap-p)# no verify-header type
```

Related Commands

Command	Description
inspect ipv6	Enables IPv6 inspection.
parameters	Enters parameters configuration mode for an inspection policy map.

Command	Description
policy-map type inspect ipv6	Creates an IPv6 inspection policy map.

version

To specify the version of RIP used globally by the ASA, use the **version** command in router 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 but sends only 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
Router 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 send version** and **rip receive version** commands 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 Version 2 packets on all interfaces:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.

Command	Description
router rip	Enables the RIP routing process and enter router configuration mode for that process.

virtual http

To configure a virtual HTTP server, use the **virtual http** command in global configuration mode. To disable the virtual server, use the **no** form of this command.

virtual http *ip_address* [**warning**]
no virtual http *ip_address* [**warning**]

Syntax Description

ip_address	Sets the IP address for the virtual HTTP server on the ASA. Make sure this address is an unused address that is routed to the ASA.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the ASA. This keyword applies only for text-based browsers, where the redirect cannot happen automatically.

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
7.2(1)	This command was deprecated because the inline basic HTTP authentication method used in prior releases was replaced by the redirection method; this command was no longer needed.
7.2(2)	This command was revived because you can now choose between using basic HTTP authentication (the default) or using HTTP redirection using the **aaa authentication listener** command. The redirection method does not require an extra command for cascading HTTP authentications.

Usage Guidelines

When you use HTTP authentication on the ASA (see the **aaa authentication match** or the **aaa authentication include** command), the ASA uses basic HTTP authentication by default. You can change the authentication method so that the ASA redirects HTTP connections to web pages generated by the ASA itself using the **aaa authentication listener** command with the **redirect** keyword.

However, if you continue to use basic HTTP authentication, then you might need the **virtual http** command when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the ASA, then the **virtual http** command lets you authenticate separately with the ASA (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the ASA is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the ASA. The ASA prompts for the AAA server username and password. After the AAA server authenticates the user, the ASA redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

For inbound users (from lower security to higher security), you must also include the virtual HTTP address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual HTTP IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual HTTP address. A **static** statement is not required.

Note Do not set the **timeout uauth** command duration to 0 seconds when using the **virtual http** command, because this setting prevents HTTP connections to the real web server.

Examples

The following example shows how to enable virtual HTTP along with AAA authentication:

```
ciscoasa(config)# virtual http 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list ACL-IN remark This is the HTTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list ACL-IN remark This is the virtual HTTP address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list AUTH remark This is the HTTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list AUTH remark This is the virtual HTTP address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
aaa authentication listener http	Sets the method by which the ASA authentica
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the ASA virtual server.
sysopt uauth allow-http-cache	When you enable the **virtual http** command, this command lets you use the username and password in the browser cache to reconnect to the virtual server.
virtual telnet	Provides a virtual Telnet server on the ASA to let users authenticate with the ASA before initiating other types of connections that require authentication.

virtual telnet

To configure a virtual Telnet server on the ASA, use the **virtual telnet** command in global configuration mode. You might need to authenticate users with the virtual Telnet server if you require authentication for other types of traffic for which the ASA does not supply an authentication prompt. To disable the server, use the **no** form of this command.

virtual telnet *ip_address*
no virtual telnet *ip_address*

Syntax Description

ip_address	Sets the IP address for the virtual Telnet server on the ASA. Make sure this address is an unused address that is routed to the ASA.

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

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the ASA, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message "Authentication Successful." Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual Telnet IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual Telnet address. A **static** statement is not required.

To logout from the ASA, reconnect to the virtual Telnet IP address; you are prompted to log out.

Examples

This example shows how to enable virtual Telnet along with AAA authentication for other services:

```
ciscoasa(config)# virtual telnet 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list ACL-IN remark This is the SMTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list ACL-IN remark This is the virtual Telnet address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list AUTH remark This is the SMTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list AUTH remark This is the virtual Telnet address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the ASA virtual server.
virtual http	When you use HTTP authentication on the ASA, and the HTTP server also requires authentication, this command allows you to authenticate separately with the ASA and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the ASA is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

vlan (group-policy)

To assign a VLAN to a group policy, use the **vlan** command in group-policy configuration mode. To remove the VLAN from the configuration of the group policy and replace it with the VLAN setting of the default group policy, use the **no** form of this command.

[**no**] **vlan** { *vlan_id* | **none** }

Syntax Description

none	Disables the assignment of a VLAN to the remote access VPN sessions that match this group policy. The group policy does not inherit the vlan value from the default group policy.
vlan_id	Number of the VLAN, in decimal format, to assign to remote access VPN sessions that use this group policy. The VLAN must be configured on this ASA, using the **vlan** command in interface configuration mode.

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

This command specifies the egress VLAN interface for sessions assigned to this group policy. The ASA forwards all traffic on this group to that VLAN. You can assign a VLAN to each group policy to simplify access control. Applying the VLAN interface configuration disrupts the client-to-client communication. All packets, including packets destined to a second client, are forced to the vlan interface. You must have a device downstream to route packets back to the firewall to maintain client-to-client communication.

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 option. These inspection engines ignore the vlan-mapping setting which could result in packets being incorrectly routed.

Examples

The following command assigns the VLAN 1 to the group policy:

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

The following command removes VLAN mapping from the group policy:

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
show vlan	Shows the VLANs configured on the ASA.
vlan (Interface configuration mode)	Assigns a VLAN ID to a subinterface.
show vpn-session_summary.db	Displays the number IPsec, Cisco AnyConnect, and NAC sessions, and the number of VLANs in use.
show vpn-sessiondb	Displays information about VPN sessions, including VLAN mapping and NAC results.

vlan (interface)

To assign a VLAN ID to a subinterface, use the **vlan** command in interface configuration mode. To remove a VLAN ID, use the **no** form of this command. Subinterfaces require a VLAN ID to pass traffic. VLAN subinterfaces let you configure multiple logical interfaces on a single physical interface. VLANs let you keep traffic separate on a given physical interface, for example, for multiple security contexts.

vlan *id* [**secondary** *vlan_range*]
no vlan [**secondary** *vlan_range*]

Syntax Description

id	Specifies an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.
secondary *vlan_range*	(Optional) Specifies one or more secondary VLANs. The *vlan_id* is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. The secondary VLANs can be separated by spaces, commas, and dashes (for a contiguous range). When the ASA receives traffic on the secondary VLANs, it maps the traffic to the primary VLAN.

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 moved from a keyword of the **interface** command to an interface configuration mode command.
9.5(2)	We added the **secondary** keyword.

Usage Guidelines

You can configure a primary VLAN, as well as one or more secondary VLANs. When the ASA receives traffic on the secondary VLANs, it maps it to the primary VLAN. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the ASA changes the old ID. To remove some secondary VLANs from the list, you can use the **no** command and only list the VLANs to remove. You can only selectively remove listed VLANs; you cannot remove a single VLAN in a range, for example.

You need to enable the physical interface with the **no shutdown** command to let subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual.

The maximum number of subinterfaces varies depending on your platform. See the CLI configuration guide for the maximum subinterfaces per platform.

Examples

The following example assigns VLAN 101 to a subinterface:

```
ciscoasa(config)# interface gigabitethernet0/0.1
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 changes the VLAN to 102:

```
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-interface)# vlan 102
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

The following example maps a set of secondary VLANs to VLAN 200:

```
interface gigabitethernet 0/6.200
vlan 200 secondary 500 503 600-700
```

The following example removes secondary VLAN 503 from the list:

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
vlan 200 secondary 500 600-700
no nameif
no security-level
no ip address
```

The following example shows how VLAN mapping works with the Catalyst 6500. Consult the Catalyst 6500 configuration guide on how to connect nodes to PVLANS.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the current configuration of the interface.

vpdn group

To create or edit a vpdn group and configure PPPoE client settings, use the **vpdn group** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

vpdn group *group_name* { **localname** *username* | **request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }
no vpdn group *group_name* { **localname** *name* | **request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }

Note PPPoE is not supported when failover is configured on the ASA, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

localname *username*	Links the user name to the vpdn group for authentication, and must match the name configured with the **vpdn username** command.
ppp authentication{chap | mschap | pap}}	Specifies the Point-to-Point Protocol (PPP) authentication protocol. The Windows client dial-up networking settings lets you specify what authentication protocol to use (PAP, CHAP, or MS-CHAP). Whatever you specify on the client must match the setting you use on the security appliance. Password Authentication Protocol (PAP) lets PPP peers authenticate each other. PAP passes the host name or username in clear text. Challenge Handshake Authentication Protocol (CHAP) lets PPP peers prevent unauthorized access through interaction with an access server. MS-CHAP is a Microsoft derivation of CHAP. PIX Firewall supports MS-CHAP Version 1 only (not Version 2.0). If an authentication protocol is not specified on the host, do not specify the ppp authentication option in your configuration.
request dialout pppoe	Specifies to allow dial out PPPoE requests.
vpdn group *group_name*	Specifies a name for the vpdn 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
Global configuration	• 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

Virtual Private Dial-up Networking (VPDN) is used to provide long distance, point-to-point connections between remote dial-in users and a private network. VDPN on the security appliance uses the Layer 2 tunneling technology PPPoE to establish dial-up networking connections from the remote user to the private network across a public network.

PPPoE is the Point-to-Point Protocol (PPP) over Ethernet. PPP is designed to work with network layer protocols such as IP, IPX, and ARA. PPP also has CHAP and PAP as built-in security mechanisms.

The **show vpdn session pppoe** command displays session information for PPPOE connections. The **clear configure vpdn group** command removes all **vpdn group** commands from the configuration and stops all the active L2TP and PPPoE tunnels. The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Because PPPoE encapsulates PPP, PPPoE relies on PPP to perform authentication and ECP and CCP functions for client sessions operating within the VPN tunnel. Additionally, PPPoE is not supported in conjunction with DHCP because PPP assigns the IP address for PPPoE.

Note Unless the VPDN group for PPPoE is configured, PPPoE cannot establish a connection.

To define a VPDN group to be used for PPPoE, use the **vpdn group** *group_name* **request dialout pppoe** command. Then use the **pppoe client vpdn group** command from interface configuration mode to associate a VPDN group with a PPPoE client on a particular interface.

If your ISP requires authentication, use the **vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} command to select the authentication protocol used by your ISP.

Use the **vpdn group** *group_name* **localname** *username* command to associate the username assigned by your ISP with the VPDN group.

Use the **vpdn username** *username* password *password* command to create a username and password pair for the PPPoE connection. The username must be a username that is already associated with the VPDN group specified for PPPoE.

Note If your ISP is using CHAP or MS-CHAP, the username may be called the remote system name and the password may be called the CHAP secret.

The PPPoE client functionality is turned off by default, so after VPDN configuration, enable PPPoE with the **ip address** *if_name* **pppoe** [**setroute**] command. The setroute option causes a default route to be created if no default route exists.

As soon as PPPoE is configured, the security appliance attempts to find a PPPoE access concentrator with which to communicate. When a PPPoE connection is terminated, either normally or abnormally, the ASA attempts to find a new access concentrator with which to communicate.

The following **ip address** commands should not be used after a PPPoE session is initiated because they will terminate the PPPoE session:

- **ip address outside pppoe**, because it attempts to initiate a new PPPoE session.
- **ip address outside dhcp**, because it disables the interface until the interface gets its DHCP configuration.
- **ip address outside** *address netmask*, because it brings up the interface as a normally initialized interface.

Examples

The following example creates a vdpn group *telecommuters* and configures the PPPoE client:

```
ciscoasa(config)# vpdn group telecommuters request dialout pppoe
ciscoasa(config)# vpdn group telecommuters localname user1
ciscoasa(config)# vpdn group telecommuters ppp authentication pap
ciscoasa(config)# vpdn username user1 password test1
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-subif)# ip address pppoe setroute
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configurations.
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show vpdn group *group_name*	Displays the vpdn group configuration.
vpdn username	Creates a username and password pair for the PPPoE connection.

vpdn username

To create a username and password pair for PPPoE connections, use the **vpdn username** command in global configuration mode.

vpdn username *username* **password** *password* [**store-local**]
no vpdn username *username* **password** *password* [**store-local**]

Note PPPoE is not supported when failover is configured on the ASA, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

password	Specifies the password.
store-local	Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.
username	Specifies the username.

Command Default

No default behavior or values. See Usage Guidelines.

Command Modes

The 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.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The vpdn username must be a username that is already associated with the VPDN group specified with the **vpdn group** *group_name* **localname** *username* command.

The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Examples

The following example creates the vpdn username *bob_smith* with the password *telecommuter* 9/8:

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

Related Commands

Command	Description
clear configure vpdn group	Removes all **vpdn group** commands from the configurations.
clear configure vpdn username	Removes all **vpdn username** commands from the configuration.
show vpdn group	Displays the VPDN group configuration.
vpdn group	Create a VPDN group and configures PPPoE client settings,

vpn-access-hours

To associate a group policy with a configured time-range policy, use the **vpn-access-hours** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, use the **vpn-access-hours none** command.

vpn-access hours value { *time-range* } **| none**
no vpn-access hours

Syntax Description

none	Sets VPN access hours to a null value, thereby allowing no time-range policy. Prevents inheriting a value from a default or specified group policy.
time-range	Specifies the name of a configured time-range policy.

Command Default

Unrestricted.

Command Modes

The 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.

Examples

The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-access-hours 824
```

Related Commands

Command	Description
time-range	Sets days of the week and hours of the day for access to the network, including start and end dates.

vpn-addr-assign

To specify a method for assigning IPv4 addresses to remote access clients, use the **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.

vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }
no vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }

Syntax Description

aaa	Assigns IPv4 addresses from an external or internal (LOCAL) AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from an IP address pool configured on the ASA and associates them with a tunnel group.
reuse-delay delay	The delay before a released IP address can be reused. The range is 0 to 480 minutes. The default is 0 (disabled).

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.
8.0.3	The reuse-delay option was added.
9.5(2)	Support for multiple context mode was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If you choose DHCP, you should also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use. You must use the dhcp-server command to indicate the IP addresses that the DHCP server uses.

If you choose local, you must also use the **ip-local-pool** command to define the range of IP addresses to use. You then use the **vpn-framed-ip-address** and **vpn-framed-netmask** commands to assign IP addresses and netmasks to individual users.

With the local pool, you can use the reuse-delay delay option to adjust the delay before a released IP address can be reused. Increasing the delay prevents problems firewalls may experience when an IP address is returned to the pool and reassigned quickly.

If you choose AAA, you obtain IP addresses from either a previously configured RADIUS server.

Examples

The following example shows how to configure DHCP as the address assignment method:

```
ciscoasa
(config)#
 vpn-addr-assign dhcp
```

Related Commands

Command	Description
dhcp-network-scope	Specifies the range of IP addresses the ASA DHCP server should use to assign addresses to users of a group policy.
ip-local-pool	Creates a local IP address pool.
ipv6-addr-assign	Specifies a method for assigning IPv6 addresses to remote access clients.
vpn-framed-ip-address	Specifies the IP address to assign to a particular user.
vpn-framed-ip-netmask	Specifies the netmask to assign to a particular user.

vpn-mode

To specify the VPN mode for a cluster, use the **vpn-mode** command in cluster group configuration mode. The clustering vpn-mode command allows the administrator to switch between centralized mode or distributed mode. To reset the VPN mode, use the no form of the command. The backup option of the CLI allows the administrator to configure whether to have VPN session backups created on a different chassis. The no form of this command returns the configuration to default values.

vpn-mode [**centralized | distributed**] [**backup** { **flat | remote-chassis** }]
[**no**] **vpn-mode** [**centralized | distributed** { **flat | remote-chassis** }]

Command Default

The default VPN mode is centralized. The default backup is flat.

Syntax Description

centralized	VPN sessions are centralized, running only on the cluster master unit.
distributed	VPN sessions are distributed across the members of the cluster.
flat	Backup sessions are allocated on any other member of the cluster.
remote-chassis	Backup sessions allocated on another chassis' member.

Command Modes

The 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
9.9(1)	This command was added.

Usage Guidelines

In flat backup mode, standby sessions are established on any other cluster member. This will protect users from blade failures, however, chassis failure protection is not guaranteed.

In remote-chassis backup mode standby sessions are established on a member of another chassis in the cluster. This will protect users from both blade failures and chassis failures.

If remote-chassis is configured in a single chassis environment (intentionally configured or the result of a failure), no backups will be created until another chassis joins.

Examples

```
ciscoasa (cfg-cluster)# vpn-mode distributed
Return the backup strategy of a distributed VPN cluster to default:
no vpn-mode distributed backup
```

Related Commands

Command	Description
cluster group	Configures the cluster group settings.
show cluster vpn-sessiondb distribution	View the distribution of active and backup sessions across cluster members.

vpnclient connect

To attempt to establish an Easy VPN Remote connection to the configured server or servers, use the **vpnclient connect** command in global configuration mode.

vpnclient connect

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	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Examples

The following example shows how to attempt to establish an Easy VPN Remote connection to a configured EasyVPN server:

```
ciscoasa
(config)#
vpnclient connect
ciscoasa
(config)#
```

vpnclient enable

To enable the Easy VPN Remote feature, use the **vpnclient enable** command in global configuration mode. To disable the Easy VPN Remote feature, use the **no** form of this command:

vpnclient enable
no vpnclient enable

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

If you enter the vpnclient enable command, the supported ASA functions as an Easy VPN Remote hardware client.

Examples

The following example shows how to enable the Easy VPN Remote feature:

```
ciscoasa
(config)#
vpnclient enable
ciscoasa
(config)#
```

The following example shows how to disable the Easy VPN Remote feature:

```
ciscoasa
(config)#
no
vpnclient enable
ciscoasa
(config)#
```

vpnclient ipsec-over-tcp

To configure the ASA running as an Easy VPN Remote hardware client to use TCP-encapsulated IPsec, use the **vpnclient ipsec-over-tcp** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient ipsec-over-tcp [**port** *tcp_port*]
no vpnclient ipsec-over-tcp

Syntax Description

port	(Optional) Specifies the use of a particular port.
tcp_port	(Required if you specify the keyword **port**.) Specifies the TCP port number to be used for a TCP-encapsulated IPsec tunnel.

Command Default

The Easy VPN Remote connection uses port 10000 if the command does not specify a port number.

Command Modes

The 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

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

By default, the Easy VPN client and server encapsulate IPsec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate IPsec within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPsec over TCP adds unnecessary overhead.

If you configure an ASA to use TCP-encapsulated IPsec, enter the following command to let it send large packets over the outside interface:

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

This command clears the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether the packet can be fragmented. This command lets the Easy VPN hardware client send packets that are larger than the MTU size.

Examples

The following example shows how to configure the Easy VPN Remote hardware client to use TCP-encapsulated IPsec, using the default port 10000, and to let it send large packets over the outside interface:

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

The next example shows how to configure the Easy VPN Remote hardware client to use TCP-encapsulated IPsec, using the port 10501, and to let it send large packets over the outside interface:

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

vpnclient mac-exempt

To exempt devices behind an Easy VPN Remote connection from individual user authentication requirements, use the **vpnclient mac-exempt** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]
no vpnclient mac-exempt

Syntax Description

mac_addr_1	MAC address, in dotted hexadecimal notation, specifying a manufacturer and serial number of a device for which to exempt individual user authentication. For more than one device, specify each MAC address, separating each with a space and the respective network mask. The first 6 characters of the MAC address identify the device manufacturer, and the last 6 characters are the serial number. The last 24 bits are the unit's serial number in hexadecimal format.
mac_mask_1	Network mask for the corresponding MAC address. Use a space to separate the network mask and any subsequent MAC address and network mask pairs.

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Devices such as Cisco IP phones, wireless access points, and printers are incapable of performing authentication, and therefore do not authenticate when individual unit authentication is enabled. If individual user authentication is enabled, you can use this command to exempt such devices from authentication. The exemption of devices from individual user authentication is also called "device pass-through."

The format for specifying the MAC address and mask in this command uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of

all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.

Note You must have Individual User Authentication and User Bypass configured on the headend device. For example, if you have the ASA as the headend, configure the following under group policy:ciscoasa(config-group-policy)# **user-authentication enable**ciscoasa(config-group-policy)# **ip-phone-bypass enable**

Examples

Cisco IP phones have the Manufacturer ID 00036b, so the following command exempts any Cisco IP phone, including Cisco IP phones, you might add in the future:

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa
(config)#
```

The next example provides greater security but less flexibility because it exempts one specific Cisco IP phone:

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa
(config)#
```

vpnclient management

To generate IPsec tunnels for management access to the Easy VPN Remote hardware client, use the **vpnclient management** command in global configuration mode.

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]
vpnclient management clear

To remove the attribute from the running configuration, use the **no** form of this command, which sets up IPsec tunnels exclusively for management in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

no vpnclient management clear

Syntax Description

clear	Uses normal routing to provide management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client. This option does not create management tunnels. **Note** Use this option if a NAT device is operating between the client and the Internet.
ip_addr	IP address of the host or network for which to build a management tunnel from the Easy VPN hardware client. Use this argument with the **tunnel** keyword. Specify one or more IP addresses, separating each with a space and the respective network mask.
ip_mask	Network mask for the corresponding IP address. Use a space to separate the network mask and any subsequent IP address and network mask pairs.
tunnel	Automates the setup of IPsec tunnels specifically for management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client.

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

It assumes the ASA 5505 configuration contains the following commands:

- **vpnclient server** to specify the peer.
- **vpnclient mode** to specify the client mode (PAT) or network extension mode.

One of the following:

- **vpnclient vpngroup** to name the tunnel group and the IKE pre-shared key used for authentication on the Easy VPN server.
- **vpnclient trustpoint** to name the trustpoint identifying the RSA certificate to use for authentication

Note The public address of an ASA behind a NAT device is inaccessible unless you add static NAT mappings on the NAT device.

Note Regardless of your configuration, DHCP requests (including renew messages) should not flow over IPsec tunnels. Even with a vpnclient management tunnel, DHCP traffic is prohibited.

Examples

The following example shows how to generate an IPsec tunnel from the outside interface of the ASA 5505 to the host with the IP address/mask combination 192.168.10.10 255.255.255.0:

```
ciscoasa
(config)#
vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa
(config)#
```

The following example shows how to provide management access to the outside interface of the ASA 5505 without using IPsec:

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

To configure the Easy VPN Remote connection for either client mode or network extension mode, use the **vpnclient mode** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mode { **client-mode | network-extension-mode** }
no vpnclient mode

Syntax Description

client-mode	Configures the Easy VPN Remote connection to use client mode (PAT).
network-extension-mode	Configures the Easy VPN Remote connection to use network extension mode (NEM).

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

The Easy VPN Client supports one of two modes of operation: client mode or NEM. The mode of operation determines whether the inside hosts, relative to the Easy VPN Client, are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because Easy VPN Client does not have a default mode.

- In client mode, the Easy VPN client performs port address translation (PAT) for all VPN traffic from its inside hosts. This mode requires no IP address management for either the inside address of the hardware client (which has a default RFC 1918 address assigned to it) or the inside hosts. Because of PAT, the inside hosts are not accessible from the enterprise network.
- In NEM, all nodes on the inside network and the inside interface are assigned addresses routable across the enterprise network. The inside hosts are accessible from the enterprise network over a tunnel. Hosts on the inside network are assigned IP addresses from an accessible subnet (statically or through DHCP). PAT is not applied to the VPN traffic when in network extension mode.

Note If the Easy VPN hardware client is using NEM and has connections to secondary servers, use the **crypto map set reverse-route** command on each headend device to configure dynamic announcements of the remote network using Reverse Route Injection (RRI).

Examples

The following example shows how to configure an Easy VPN Remote connection for client mode:

```
ciscoasa
(config)#
vpnclient mode client-mode
ciscoasa
(config)#
```

The following example shows how to configure an Easy VPN Remote connection for NEM:

```
ciscoasa
(config)#
vpnclient mode network-extension-mode
ciscoasa
(config)#
```

vpnclient nem-st-autoconnect

To configure the Easy VPN Remote connection to automatically initiate IPsec data tunnels when NEM and split tunneling are configured, use the **vpnclient nem-st-autoconnect** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient nem-st-autoconnect
no vpnclient nem-st-autoconnect

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Before entering the **vpnclient nem-st-autoconnect** command, ensure that network extension mode is enabled for the hardware client. 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. After the tunnel is up, either side can initiate data exchange.

Note You must also configure the Easy VPN server to enable network extension mode. To do so, use the **nem enable** command in group-policy configuration mode.

IPsec data tunnels are automatically initiated and sustained when in network extension mode, except when split-tunneling is configured.

Examples

The following example shows how to configure an Easy VPN Remote connection to automatically connect in network extension mode with split-tunneling configured. Network extension mode is enabled for the group policy FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
ciscoasa
(config)#
vpnclient nem-st-autoconnect
ciscoasa
(config)#
```

Related Commands

Command	Description
nem	Enables network extension mode for hardware clients.

To remove the attribute from the running configuration, use the **no** form of this command.

no vpnclient sercure interface

vpnclient server

To configure the primary and secondary IPsec servers, for the Easy VPN Remote connection, use the **vpnclient server** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server *ip_primary_address* [*ip_secondary_address_1 … ipsecondary_address_10*]
no vpnclient server

Syntax Description

ip_primary_address	IP address or DNS name of the primary Easy VPN (IPsec) server. Any ASA or VPN 3000 Concentrator Series can act as an Easy VPN server.
ip_secondary_address_n	(Optional) List of the IP addresses or DNS names of up to ten backup Easy VPN servers. Use a space to separate the items in the 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

A server must be configured before a connection can be established. The **vpnclient server** command supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order.

You can use either the IP address or the hostname of a server.

Examples

The following example associates the name headend-1 with the address 10.10.10.10 and uses the **vpnclient server** command to specify three servers: headend-dns.example.com (primary), headend-1 (secondary), and 192.168.10.10 (secondary):

```
ciscoasa
(config)#
names
ciscoasa(config)# 10.10.10.10 headend-1
```

```
ciscoasa(config)# vpnclient server headend-dns.example.com headend-1 192.168.10.10
ciscoasa(config)#
```

The following example shows how to configure a VPN client primary IPsec server with the IP address 10.10.10.15 and secondary servers with the IP addresses 10.10.10.30 and 192.168.10.45.

```
ciscoasa
(config)#
vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa
(config)#
```

vpnclient server-certificate

To configure the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map, use the **vpnclient server-certificate** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server-certificate *certmap_name*
no vpnclient server-certificate

Syntax Description

certmap_name	Specifies the name of a certificate map that specifies the acceptable Easy VPN server certificate. The maximum length is 64 characters.

Command Default

Easy VPN server certificate filtering 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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Use this command to enable Easy VPN server certificate filtering. You define the certificate map itself using the crypto ca certificate map and crypto ca certificate chain commands.

Examples

The following example shows how to configure an Easy VPN Remote connection to support only connections to Easy VPN servers with the certificate map name homeservers:

```
ciscoasa
(config)#
vpnclient server-certificate homeservers
ciscoasa
(config)#
```

Related Commands

Command	Description
certificate	Adds the indicated certificate.

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN Remote connection.

vpnclient trustpoint

To configure the RSA identity certificate to be used by the Easy VPN Remote connection, use the **vpnclient trustpoint** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient trustpoint *trustpoint_name* [**chain**]
no vpnclient trustpoint

Syntax Description

chain	Sends the entire certificate chain.
trustpoint_name	Specifies the name of a trustpoint identifying the RSA certificate to use for authentication.

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
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Define the trustpoint using the **crypto ca trustpoint** command. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub 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.

Examples

The following example shows how to configure an Easy VPN Remote connection to use the specific identity certificate named central and to send the entire certificate chain:

```
ciscoasa(config)# crypto ca trustpoint
central
ciscoasa
(config)#
vpnclient trustpoint central chain
ciscoasa
```

```
(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint submode for the specified trustpoint and manages trustpoint information.

vpnclient username

To configure the VPN username and password for the Easy VPN Remote connection, use the **vpnclient username** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient username *xauth_username* **password** *xauth password*
no vpnclient username

Syntax Description

xauth_password	Specifies the password to use for XAUTH. The maximum length is 64 characters.
xauth_username	Specifies the username to use for XAUTH. The maximum length 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

The XAUTH username and password parameters are used when secure unit authentication is disabled and the server requests XAUTH credentials. If secure unit authentication is enabled, these parameters are ignored, and the ASA prompts the user for a username and password.

Examples

The following example shows how to configure the Easy VPN Remote connection to use the XAUTH username testuser and the password ppurkm1:

```
ciscoasa
(config)#
vpnclient username testuser password ppurkm1
ciscoasa
(config)#
```

vpnclient vpngroup

To configure the VPN tunnel group name and password for the Easy VPN Remote connection, use the **vpnclient vpngroup** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient vpngroup *group_name* **password** *preshared_key*
no vpnclient vpngroup

Syntax Description

group_name	Specifies the name of the VPN tunnel group configured on the Easy VPN server. The maximum length is 64 characters, and no spaces are allowed.
preshared_key	The IKE pre-shared key used for authentication by the Easy VPN server. The maximum length is 128 characters.

Command Default

If the configuration of the ASA running as an Easy VPN Remote hardware client does not specify a tunnel group, the client attempts to use an RSA certificate.

Command Modes

The 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

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Use the pre-shared key as the password.

You must also configure a server and specify the mode before establishing a connection.

Examples

The following example shows how to configure an Easy VPN Remote connection with a VPN tunnel group with the group name TestGroup1 and the password my_key123.

```
ciscoasa
(config)#
vpnclient vpngroup TestGroup1 password my_key123
ciscoasa
(config)#
```

Related Commands

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN connection.

vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, including a null value created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **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 **vpn-filter** command to apply those ACLs.

vpn-filter { **value** *ACL name* **| none** }
no 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 *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	• Yes	—
Username configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for IPv4 and IPv6 ACLs was added. Support for multiple context mode was added.
9.1.(4)	Support for IPv4 and IPv6 ACLs was added. If the deprecated command **ipv6-vpn-filter** is mistakenly used to specify IPv6 ACLs, the connection will be terminated.

Usage Guidelines

Clientless SSL VPN does not use the ACL defined in the **vpn-filter** command.

By design, the vpn-filter feature allows for traffic to be filtered in inbound direction only. The outbound rule is automatically compiled. When creating an icmp access-list, do not specify icmp type in the access-list formatting if you want directional filters.

The VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection.

Examples

The following example shows how to set a filter that invokes an access list named acl_vpn for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-filter value acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
ipv6-vpn-filter	Deprecated command which was used previously to specify IPv6 ACLs.

vpn-framed-ip-address

To specify the IPv4 address to assign to an individual user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

vpn-framed-ip-address { *ip_address* }{ *subnet_mask* }
no vpn-framed-ip-address

Syntax Description

ip_address	Provides the IP address for this user.
subnet_mask	Specifies the subnetwork 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
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

Use the **vpn-framed-ipv6-address** command in username mode to assign a dedicated IPv6 address to a user. To remove the IP address, use the **no** form of this command.

vpn-framed-ip6-address *ip_address/subnet_mask*
no vpn-framed-ip6-address *ip_address/subnet_mask*

Syntax Description

ip_address	Provides the IP address for this user.
subnet_mask	Specifies the subnetwork 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
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows how to set an IP address and netmask of 2001::3000:1000:2000:1/64 for a user named *anyuser* . This address indicates a prefix value of 2001:0000:0000:0000 and an interface ID of 3000:1000:2000:1.

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ipv6-address
2001::3000:1000:2000:1/64
ciscoasa(config-username)
```

Related Commands

Command	Description
vpn-framed-ip-address	Specifies an IPv4 address to assign to an individual user.

vpn-group-policy

To have a user inherit attributes from a configured group policy, use the vpn-group-policy command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy { *group-policy name* }
no vpn-group-policy { *group-policy name* }

Syntax Description

group-policy name	Provides the name of the group policy.

Command Default

By default, VPN users have no group policy association.

Command Modes

The 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 configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can override the value of an attribute in a group policy for a particular user by configuring it in username mode, if that attribute is available in username mode.

Examples

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)# vpn-group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Adds a group policy to the ASA database.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a group policy.

Command	Description
username	Adds a user to the ASA database.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

vpn-idle-timeout

To configure a user timeout period use the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode. If there is no communication activity on the connection in this period, the ASA terminates the connection. You can optionally extend the timeout alert-interval from the default one minute.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

vpn-idle-timeout { *minutes* | **none** } [**alert-interval** *minutes*]
no vpn-idle-timeout
no vpn-idle-timeout alert-interval

Syntax Description

minutes	Specifies the number of minutes in the timeout period, and the number of minutes before the time-out alert. Use an integer between 1 and 35791394.
none	AnyConnect (SSL IPsec/IKEv2): Use the global WebVPN default-idle-timeout value (seconds) from the command: ciscoasa**(config-webvpn)# default-idle-timeout** The range for this value in the WebVPN **default-idle-timeout** command is 60-86400 seconds; the default Global WebVPN Idle timeout in seconds -- default is 1800 seconds (30 min). **Note** A non-zero idle timeout value is required by ASA for all AnyConnect connections. For a WebVPN user, the **default-idle-timeout** value is enforced only if vpn-idle-timeout none is set in the group policy/username attribute. Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access: Disable timeout and allow for an unlimited idle period.

Command Default

30 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
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The Secure Client supports session resumption for SSL and IKEv2 connection. With this capability, end user devices can go into sleep mode, lose their WiFi, or any of the like and resume the same connection upon return.

Examples

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named “FirstGroup”:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-idle-timeout 30
```

The security appliance uses the default-idle-timeout value if no idle timeout is defined for a user, if the vpn-idle-timeout value is 0, or if the value does not fall into the valid range.

Related Commands

default-idle-timeout	Specifies the global WebVPN default idle timeout.
group-policy	Creates or edits a group policy.
vpn-session-timeout	Configures the maximum amount of time allowed for VPN connections. At the end of this period of time, the ASA terminates the connection.

vpn load-balancing

To enter vpn load-balancing mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

vpn load-balancing

Note To use VPN load balancing, you must have an ASA 5510 with a Plus license or an ASA 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

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.
8.0(2)	Support for the ASA 5510 with a Plus license and models above 5520 was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A load-balancing cluster can include security appliance models 5510 (with a Plus license), or ASA 5520 and above. You can also include VPN 3000 Series Concentrators in the cluster. While mixed configurations are possible, administration is generally simpler if the cluster is homogeneous.

Use the **vpn load-balancing** command to enter vpn load-balancing mode. The following commands are available in vpn load-balancing mode:

- **cluster encryption**
- **cluster ip address**
- **cluster key**

- **cluster port**
- **interface**
- **nat**
- **participate**
- **priority**
- **redirect-fqdn**

See the individual command descriptions for detailed information.

Examples

The following is an example of the **vpn load-balancing** command; note the change in the prompt:

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

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” 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)# **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-sessiondb

To specify the maximum number of VPN sessions or Secure Client VPN sessions, use the vpn-sessiondb command from global configuration mode. To remove the limit from the configuration, use the no form of the command:

vpn-sessiondb { **max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number* }

Syntax Description

max-anyconnect-premium-or-essentials-limit number	Specifies the maximum number of AnyConnect sessions, from 1 to the maximum sessions allowed by the license.
max-other-vpn-limit number	Specifies the maximum number of VPN sessions other than Secure Client sessions, from 1 to the maximum sessions allowed by the license. This includes Cisco VPN client (IPsec IKEv1) and LAN-to-LAN VPN.

Command Default

By default, the ASA does not limit the number of VPN sessions lower than the licensed maximum.

Command Modes

The 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.
8.4(1)	The following keywords were changed: • max-anyconnect-premium-or-essentials-limit replaced max-session-limit • max-other-vpn-limit replaced max-webvpn-session-limit
9.0(1)	Support for multiple context mode was added.

Examples

The following example sets the maximum AnyConnect sessions to 200:

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-webvpn-session-limit	Sets a maximum number of WebVPN sessions.

vpn-sessiondb logoff

To log off all or selected VPN sessions, use the **vpn-sessiondb logoff** command in global configuration mode.

vpn-sessiondb logoff { **all** | **anyconnect** | **email-proxy** | **index index_number** | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *groupname* | **vpn-lb** | **webvpn** } [**noconfirm**]

Syntax Description

all	Logs off all VPN sessions.
anyconnect	Logs of all AnyConnect VPN client sessions.
email-proxy	(Deprecated) Logs off all e-mail proxy sessions.
index *index_number*	Logs off a single session by index number. Specify the index number for the session. You can view index numbers for each session with the show vpn-sessiondb detail command.
ipaddress *IPaddr*	Logs off sessions for the IP address hat you specify.
l2l	Logs off all LAN-to-LAN sessions.
name *username*	Logs off sessions for the username that you specify.
protocol *protocol-name*	Logs off sessions for protocols that you specify. The protocols include:

	• ikev1—Sessions using the Internet Key Exchange version 1 (IKEv1) protocol. • ikev2—Sessions using the Internet Key Exchange version 2 (IKEv2) protocol. • ipsec—IPsec sessions using either IKEv1 or IKEv2. • ipseclan2lan—IPsec LAN-to-LAN sessions. • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T sessions. • ipsecovernatt—IPsec over NAT-T sessions. • ipsecovertcp—IPsec over TCP sessions. • ipsecoverudp—IPsec over UDP sessions. • l2tpOverIpSec—L2TP over IPsec sessions. • l2tpOverIpsecOverNatT—L2TP over IPsec over NAT-T sessions. • webvpn—Clientless SSL VPN sessions. • imap4s—IMAP4 sessions. • pop3s—POP3 sessions. • smtps—SMTP sessions. • anyconnectParent—Secure Client sessions, regardless of the protocol used for the session (terminates AnyConnect IPsec IKEv2 and SSL sessions). • ssltunnel—SSL VPN sessions, including AnyConnect sessions using SSL and clientless SSL VPN sessions. • dtlstunnel—Secure Client sessions with DTLS enabled.
ra-ikev1-ipsec	Logs off all IPsec IKEv1 remote-access sessions.
ra-ikev2-ipsec	Logs off all IPsec IKEv2 remote-access sessions.
tunnel-group *groupname*	Logs off sessions for the tunnel group (connection profile) that you specify.
webvpn	Logs off all clientless SSL VPN sessions.

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.
8.4(1)	The following protocol keywords were changed or added: • remote was changed to ra-ikev1-ipsec. • ike was changed to ikev1. • ikev2 was added. • anyconnectParent was added.
9.0(1)	Support for multiple context mode was added.
9.3(2)	The **ra-ikev2-ipsec** keyword was added.
9.8(1)	The **email-proxy** option was deprecated.

Examples

The following example shows how to log off all Secure Client sessions:

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

The following example shows how to log off all IPsec sessions:

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

To configure a maximum amount of time allowed for VPN connections, use the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode. At the end of this period of time, the ASA terminates the connection. You can optionally extend the timeout alert-interval from the default one minute.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-session-timeout none** command.

vpn-session-timeout { *minutes* | **none** } [**alert-interval** *minutes*]
no vpn-session-timeout
no vpn-session-timeout alert-interval

Syntax Description

minutes	Specifies the number of minutes in the timeout period, and the number of minutes before the time-out alert. Use an integer between 1 and 35791394.
none	Permits an unlimited session timeout period. Sets session timeout with a null value, thereby disallowing a session timeout. Prevents inheriting a value from a default or specified group policy.

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
7.0(1)	This command was added.
9.7(1)	**alert-interval** applied to AnyConnect VPNs

Examples

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-session-timeout 180
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-idle-timeout	Configures the user timeout period. If there is no communication activity on the connection in this period, the ASA terminates the connection.

vpnsetup

To display a list of steps for configuring VPN connections on the ASA, use the **vpnsetup** command from global configuration mode.

vpnsetup { **ipsec-remote-access | l2tp-remote-access | site-to-site | ssl-remote-access** } **steps**

Syntax Description

ipsec-remote-access	Displays steps to configure the ASA to accept IPsec connections.
l2tp-remote-access	Displays steps to configure the ASA to accept L2TP connections.
site-to-site	Displays steps to configure the ASA to accept LAN-to-LAN connections.
ssl-remote-access	Displays steps to configure the ASA to accept SSL connections.
steps	Specifies to display the steps for the connection type.

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	• Yes	—

Command History

Release	Modification
8.0(3)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows the output of the **vpnsetup ssl-remote-access steps command:**

```
ciscoasa(config-t)# vpnsetup ssl-remote-access steps
Steps to configure a remote access SSL VPN remote access connection and AnyConnect with
examples:
1. Configure and enable interface
 interface GigabitEthernet0/0
  ip address 10.10.4.200 255.255.255.0
  nameif outside
  no shutdown
 interface GigabitEthernet0/1
  ip address 192.168.0.20 255.255.255.0
  nameif inside
  no shutdown
```

```
2. Enable WebVPN on the interface
 webvpn
  enable outside
3. Configure default route
 route outside 0.0.0.0 0.0.0.0 10.10.4.200
4. Configure AAA authentication and tunnel group
 tunnel-group DefaultWEBVPNGroup type remote-access
 tunnel-group DefaultWEBVPNGroup general-attributes
  authentication-server-group LOCAL
5. If using LOCAL database, add users to the Database
 username test password t3stP@ssw0rd
 username test attributes
  service-type remote-access
Proceed to configure AnyConnect VPN client:
6. Point the ASA to an AnyConnect image
 webvpn
  svc image anyconnect-win-2.1.0148-k9.pkg
7. enable AnyConnect
 svc enable
8. Add an address pool to assign an ip address to the AnyConnect client
 ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
9. Configure group policy
 group-policy DfltGrpPolicy internal
 group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol svc webvpn
ciscoasa(config-t)#
```

Related Commands

Command	Description
show running-config	Displays the running configuration of the ASA.

vpn-simultaneous-logins

To configure the number of simultaneous logins permitted for a user, use the **vpn-simultaneous-logins** command in group-policy configuration mode or username configuration mode. To remove the attribute and return to the default value, use the **no** form of this command.

vpn-simultaneous-logins *integer*
no vpn-simultaneous-logins

Syntax Description

integer	A number between 0 and 2147483647.

Command Default

The default is 3 simultaneous logins.

Command Modes

The 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

This option allows inheritance of a value from another group policy. Enter 0 to disable login and prevent user access.

Note While the maximum limit for the number of simultaneous logins is very large, allowing several simultaneous logins could compromise security and affect performance.

Stale AnyConnect, IPsec Client, or Clientless sessions (sessions that are terminated abnormally) might remain in the session database, even though a "new" session has been established with the same username.

If the value of vpn-simultaneous-logins is 1, and the same user logs in again after an abnormal termination, then the stale session is removed from the database and the new session is established. If, however, the existing session is still an active connection and the same user logs in again, perhaps from another PC, the first session is logged off and removed from the database, and the new session is established.

If the number of simultaneous logins is a value greater than 1, then, when you have reached that maximum number and try to log in again, the session with the longest idle time is logged off. If all current sessions have

been idle an equally long time, then the oldest session is logged off. This action frees up a session and allows the new login.

Once the maximum session limit is reached, it takes some time for the system to delete the oldest session. Thus, a user might not be able to immediately log on and might have to retry the new connection before it completes successfully. This should not be a problem if users log off their sessions as expected. You can optionally remove the delay by configuring the system to not wait for the deletion to complete and immediately allow the new user connection, using the **vpn-simultaneous-login-delete-no-delay** command.

Examples

The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
ciscoasa(config)#  group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

To configure a VPN tunnel type (IPsec with IKEv1 or IKEv2, L2TP over IPsec, SSL, or clientless SSL), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }
no vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }

Syntax Description

ikev1	Negotiates an IPsec tunnel with IKEv1 between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
ikev2	Negotiates an IPsec tunnel with IKEv2 between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
l2tp-ipsec	Negotiates an IPsec tunnel for an L2TP connection.
ssl-client	Negotiates an SSL VPN tunnel with an SSL VPN client.
ssl-clientless	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

Command Default

The default is 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
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.17(1)	The ssl-clientless keyword was removed due to support removal for clientless web VPN.
8.4(1)	The ipsec keyword was replaced by the ikev1 and ikev2 keywords.
7.3(1)	The **svc** keyword was added.
7.2(1)	The **l2tp-ipsec** keyword was added.

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

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

Examples

The following example shows how to configure WebVPN and IPsec tunneling modes for the group policy named “FirstGroup”:

```
ciscoasa
(config)#

group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol webvpn
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol IPsec
```

Related Commands

Command	Description
address pools	Specifies a list of address pools for allocating addresses to remote clients.
show running-config group-policy	Displays the configuration for all group-policies or for a specific group-policy.

vtep-nve

To associate a VXLAN VNI interface with the VTEP source interface, use the **vtep-nve** command in interface configuration mode. To remove the association, use the **no** form of this command.

vtep-nve 1
no vtep-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
Interface 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 with 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.

vxlan port

To set the VXLAN UDP port, use the **vxlan port** command in global configuration mode. To remove restore the default port, use the **no** form of this command.

vxlan port *udp_port*
no vxlan port *udp_port*

Syntax Description

udp_port	Sets the VXLAN UDP port. The default is 4789.

Command Default

The default port is 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
Nve configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789. If your network uses a non-standard port, you can change it.

Examples

For example:

```
ciscoasa(config)# vxlan port 5678
```

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.

Command	Description
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.

W - Z

wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **wccp** command in global configuration mode. To disable the service group and deallocate space, use the no form of this command.

wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
no wccp { **web-cache** | *service-number* } [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]

Syntax Description

access-list	Specifies the name of the access list.
group-list	(Optional) Access list that determines which web caches are allowed to participate in the service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password	(Optional) Specifies Message Digest 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded.
password	Specifies the password to be used for authentication. The password argument can be up to seven characters in length.
redirect-list	(Optional) Used with an access list that controls traffic redirected to this service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list. The access list should only contain network addresses. Port-specific entries are not supported
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.
web-cache	Specifies the web-cache service. **Note** Web cache counts as one service. The maximum number of services, including those assigned with the service-number argument, are 256.

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
7.2(1)	This command was added.

Examples

The following example shows how to enable WCCP for participation in a service group:

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

wccp redirect

To enable packet redirection on the ingress of an interface using Web Cache Communication Protocol (WCCP), use the **wccp redirect** command. To disable WCCP redirection, use the no form of this command.

wccp interface *interface_name service* **redirect in**
no wccp interface *interface_name service* **redirect in**

Syntax Description

in	Specifies redirection when packet comes into this interface
interface_name	Name of the interface where packets should be redirected..
service	Specifies the service group. You can specify the **web-cache** keyword, or you can specify the identification number (from 0 to 99) of the service.

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
7.2(1)	This command was added.

Examples

The following example shows how to enable WCCP redirection on the inside interface for the web-cache service:

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp	Enables support of WCCP with service groups.

web-agent-url (Deprecated)

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

To specify the SSO server URL to which the ASA makes SiteMinder-type SSO authentication requests, use the **web-agent-url** command in config-webvpn-sso-siteminder mode.

To remove an SSO server authentication URL, use the **no** form of this command.

web-agent-url *url*
no web-agent-url *url*

Note This command is required for SiteMinder-type SSO authentication.

Syntax Description

url	Specifies the authentication URL of the SiteMinder-type SSO server. Must contain http:// or https://.

Command Default

By default, an authentication URL 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
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 SSO server has a URL that handles authentication requests.

This command applies only to the SiteMinder type of SSO server.

Use the **web-agent-url** command to configure the ASA to send authentications to this URL. Before configuring the authentication URL, you must create the SSO server using the **sso-server** command.

For https communication between the security appliance and SSO-server, make sure that the SSL encryption settings match on both sides. On the security appliance, verify this with the **ssl encryption** command.

Examples

The following example, entered in config-webvpn-sso-siteminder mode, specifies an authentication URL of http://www.example.com/webvpn:

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
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.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type 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.
ssl encryption	Specifies the encryption algorithms the SSL/TLS protocol uses.
sso-server	Creates a single sign-on server.

web-applications

To customize the Web Application box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-applications** command from webvpn customization mode:

web-applications { **title | message | dropdown** } { **text | style** } *value*
[**no**] **web-applications** { **title | message | dropdown** } { **text | style** } *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the drop down box.
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 title text is “Web Application”.

The default title style is background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Web Address (URL)”.

The default message style is background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “Web Bookmarks”.

The default dropdown style is border:1px solid black;font-weight:bold;color:black;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	• Yes	—	• Yes	— s	—

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 changes the title to “Applications”, and the color of the text to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-applications title text Applications
ciscoasa(config-webvpn-custom)# web-applications title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

web-bookmarks

To customize the Web Bookmarks title or links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-bookmarks** command from webvpn customization mode:

web-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }
[**no**] { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML 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 link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “Web Bookmarks”.

Command Modes

The 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	• 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 Web Bookmarks title to “Corporate Web Bookmarks”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.

web update-type

To specify the address types (IPv4 or IPv6) that you want to update when using the DDNS Web update method, use the **web update-type** command in ddns update method configuration mode. To restore the default, use the **no** form of this command.

web update-type { **ipv4 | ipv6** [**all**] **| both** [**all**] }
no web update-type [**ipv4 | ipv6** [**all**] **| both** [**all**]]

Syntax Description

ipv4	Updates the IPv4 address.
ipv6	Updates the latest IPv6 address.
all	Updates all IPv6 addresses.
both	Updates the IPv4 address and the latest IPv6 address.

Command Default

The default is **both all** .

Command Modes

The 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
9.15(1)	Command added.

Usage Guidelines

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS) provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates the following RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The ASA supports the following DDNS update methods: Standard DDNS (see the **ddns** command) and Web (using the **web update-url** command). The Web update method uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/). With this method when the IP address or hostname changes, the ASA sends an HTTP request directly to a DNS provider with which you have an account.

Examples

The following example configures the web type method and sets the IP address type to IPv4:

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>

  web update-type ipv4
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Related Commands

Command	Description
ddns update	Associates a DDNS method with an interface.
ddns update hostname	Specifies the hostname for the interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
web update-url	Sets the DDNS update method to Web and sets the update URL.

web update-url

To specify the web update method for DDNS along with the web type URL, use the **web update-url** command in ddns update method configuration mode. To remove the method, use the **no** form of this command.

web update-url https: *//username:password@provider-domain/path* **?hostname=<h>&myip=<a>**
no web update-url https: *//username:password@provider-domain/path* **?hostname=<h>&myip=<a>**

Syntax Description

username	The username at the DDNS provider.
password	The password for this username.
provider-domain	The DDNS provider domain.
path	The path required at the DDNS domain. Check with your DDNS provider for the correct path.
?hostname=<h>&myip=<a>	Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the **?** without the software interpreting the **?** as a help query. Although these keywords look like arguments, you need to enter this text verbatim at the end of the URL. The ASA will automatically replace the <h> and <a> fields with the hostname and IP address when it sends the DDNS 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
Ddns update method configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.15(1)	Command added.

Usage Guidelines

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS)

provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates the following RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The ASA supports the following DDNS update methods: Standard DDNS (see the **ddns** command) and Web (using the **web update-url** command). The Web update method uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/). With this method when the IP address or hostname changes, the ASA sends an HTTP request directly to a DNS provider with which you have an account.

You can also specify the address types (IPv4 or IPv6) that you want to update using the **web update-type** command.

The web method for DDNS also requires you to identify the DDNS server root CA to validate the DDNS server certificate for the HTTPS connection. For example:

```
crypto ca trustpoint DDNS_Trustpoint
   enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

Examples

The following example configures the web type method:

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Related Commands

Command	Description
ddns update	Associates a DDNS method with an interface.
ddns update hostname	Specifies the hostname for the interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
web update-type	Specifies the address types (IPv4 or IPv6) that you want to update.

webvpn (global)

To enter webvpn mode, in global configuration mode, enter the **webvpn** command. To remove any commands entered with this command, use the **no webvpn** command. These **webvpn** commands apply to all WebVPN users.

These **webvpn** commands let you configure AAA servers, default group policies, default idle timeout, http and https proxies, and NBNS servers for WebVPN, as well as the appearance of WebVPN screens that end users see.

webvpn
no webvpn

Syntax Description

This command has no arguments or keywords.

Command Default

WebVPN 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
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

This WebVPN mode lets you configure global settings for WebVPN. WebVPN mode, which you enter from either group-policy mode or username mode, lets you customize a WebVPN configuration for specific users or group policies. The ASA clientless SSL VPN configuration supports only one http-proxy and one https-proxy command each.

Note You must enable browser caching for WebVPN to work.

Examples

The following example shows how to enter WebVPN command mode:

```
ciscoasa
(config)#
 webvpn
```

```
ciscoasa
(config-webvpn)#
```

webvpn (group-policy attributes, username attributes)

To enter this webvpn mode, use the **webvpn** command in group-policy attributes configuration mode or in username attributes configuration mode. To remove all commands entered in webvpn mode, use the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

Webvpn commands for group policies and usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

webvpn
no webvpn

Syntax Description

This command has no arguments or keywords.

Command Default

WebVPN 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
Group-policy attributes configuration	• Yes	—	• Yes	—	—
Username attributes configuration	• 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

Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. The **webvpn** command in group-policy attributes configuration mode or username attributes configuration mode applies the settings specified in the webvpn command to the group or user specified in the parent command. In other words, webvpn mode, described in this section, and which you enter from group-policy or username mode, lets you customize a WebVPN configuration for specific users or group policies.

The webvpn attributes that you apply for a specific group policy in group-policy attributes mode override those specified in the default group policy. The WebVPN attributes that you apply for a specific user in username attributes mode override both those in the default group policy and those in the group policy to which that user belongs. Essentially, these commands let you tweak the settings that would otherwise be

inherited from the default group or the specified group policy. For information about the WebVPN settings, see the description of the **webvpn** command in global configuration mode.

The following table lists the attributes you can configure in webvpn group-policy attributes and username attributes mode. See the individual command descriptions for details.

Attribute	Description
auto-signon	Configures the ASA to automatically pass WebVPN user login credentials on to internal servers, providing a single sign-on method for WebVPN users.
customization	Specifies a preconfigured WebVPN customization to apply.
deny-message	Specifies a message to display to the user when access is denied.
filter	Identifies the access list to be used for WebVPN connections.
functions	Configures file access and file browsing, MAPI Proxy, and URL entry over WebVPN.
homepage	Sets the URL of the web page that displays when WebVPN users log in.
html-content-filter	Identifies Java, ActiveX, images, scripts, and cookies to filter for WebVPN sessions.
http-comp	Specifies the HTTP compression algorithm to use.
keep-alive-ignore	Specifies the maximum object size to ignore for updating the session.
port-forward	Enables WebVPN application access.
port-forward-name	Configures the display name that identifies TCP port forwarding to end users.
sso-server	Configures the SSO server name.
svc	Configures SSL VPN Client attributes.
url-list	Identifies a list of servers and URLs that users can access via WebVPN.

Examples

The following example shows how to enter webvpn mode for the group policy named “FirstGroup”:

```
ciscoasa
(config)#
group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-webvpn)#
```

The following example shows how to enter webvpn mode for the username named “test”:

```
ciscoasa
(config)#
group-policy test attributes
ciscoasa
(config-username)#
 webvpn
ciscoasa(config-webvpn)#
```

Related Commands

clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn mode to configure webvpn attributes for the group.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

whitelist

For Cloud Web Security, to perform the whitelist action on the class of traffic, use the **whitelist** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map type inspect scansafe** command, then the **parameters** command. To disable whitelisting, use the **no** form of this command.

whitelist
no whitelist

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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Identify the traffic you want to whitelist using the **class-map type inspect scansafe** command. Use the inspection class map in the **policy-map type inspect scansafe** command, and specify the **whitelist** action for the class. Call the inspection policy map in 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.
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.

who

To display active Telnet administration sessions on the ASA, use the **who** command in privileged EXEC mode.

who [*local_ip*]

Syntax Description

local_ip (Optional) Specifies to limit the listing to one internal IP address or network address, either 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **who** command allows you to display the TTY_ID and IP address of each Telnet client that is currently logged into the ASA.

Examples

This example shows the output of the **who** command when a client is logged into the ASA through a Telnet session:

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

Related Commands

Command	Description
kill	Terminate a Telnet session.
telnet	Adds Telnet access to the ASA console and sets the idle timeout.

window-variation

To drop a connection with a window size variation, use the **window-variation** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

window variation { **allow-connection | drop-connection** }
no window variation { **allow-connection | drop-connection** }

Syntax Description

allow-connection	Allows the connection.
drop-connection	Drops the connection.

Command Default

The default action is to allow the connection.

Command Modes

The 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 **window-variation** command in tcp-map configuration mode to drop all connections with a window size that has been shrunk.

The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged. When this condition is detected, the connection can be dropped.

Examples

The following example shows how to drop all connections with a varied window size:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# window-variation drop-connection
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.

wins-server

To set the IP address of the primary and secondary WINS servers, use the **wins-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a WINS server from another group policy. To prevent inheriting a server, use the **wins-server none** command.

wins-server value { *ip_address* } [*ip_address*] | **none**
no wins-server

Syntax Description

none	Sets wins-servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary WINS servers.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Every time you issue the **wins-server** command you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same holds true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

Examples

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

without-csd

To exempt certain users from running the Hostscan application of Cisco Secure Desktop on a per connection profile basis if they enter one of the entries in the group-urls table to establish the VPN session, use the **without-csd** command in tunnel webvpn configuration mode. To remove this command from the configuration, use the **no** form of the command.

without-csd [**anyconnect**]
no without-csd [**anyconnect**]

Syntax Description

anyconnect	(Optional) Changes the command to affect only AnyConnect connections.

Command Default

No default values. If installed, Hostscan 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
Tunnel webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.2(1)	The **anyconnect** keyword was added.

Usage Guidelines

This command prevents the Hostscan application of Cisco Secure Desktop from running on the endpoint if the user enters a URL in the url-group list configured on this connection profile (called a tunnel group in the CLI). Entering this command prevents the detection of endpoint conditions for these sessions, so you may need to adjust the dynamic access policy (DAP) configuration.

Examples

The first command in the following example creates a group-url in which “example.com” is the domain of the ASA and “no-csd” is the unique portion of the URL. When the user enters this URL, the ASA assigns this connection profile to the session. The **group-url** command is required for the **without-csd** command to have an effect. The **without-csd** command exempts the user from running Cisco Secure Desktop.

```
ciscoasa(config-tunnel-webvpn)# group-url https://example.com/no-csd enable
ciscoasa(config-tunnel-webvpn)# without-csd
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
csd enable	Enables Cisco Secure Desktop for all connection profiles that do not have a without-csd command.
csd image	Copies the Cisco Secure Desktop image named in the command, from the flash drive specified in the path to the running configuration.
group-url	Creates a group-url unique to this connection profile.

write erase

To erase the startup configuration, use the **write erase** command in privileged EXEC mode. The running configuration remains intact.

write erase

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
7.0(1)	This command was added.

Usage Guidelines

This command is not supported within a security context. Context startup configurations are identified by the config-url command in the system configuration. If you want to delete a context configuration, you can remove the file manually from the remote server (if specified) or clear the file from Flash memory using the **delete** command in the system execution space.

For the ASA virtual, this command restores the deployment configuration (the initial virtual deployment settings) after a **reload**. To erase the configuration completely, use the **clear configure all** command. To erase the deployment configuration and apply the same factory default configuration as for the ASA appliances, see **configure factory-default**.

Note The ASA virtual boots the current running image, so you are not reverted to the original boot image.Do not save the configuration before you reload.

For the ASA virtual in a failover pair, first power off the standby unit. To prevent the standby unit from becoming active, you must power it off. If you leave it on, when you erase the active unit configuration, then the standby unit becomes active. When the former active unit reloads and reconnects over the failover link, the old configuration will sync from the new active unit, wiping out the deployment configuration you wanted. After the active unit reloads, you can power on the standby unit. The deployment configuration will then sync to the standby unit.

Examples

The following example erases the startup configuration:

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
delete	Removes a file from Flash memory.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

write memory

To save the running configuration to the startup configuration, use the **write memory** command in privileged EXEC mode.

write memory [**all** [**/noconfirm**]]

Syntax Description

/noconfirm	Eliminates the confirmation prompt when you use the **all** keyword.
all	From the system execution space in multiple context mode, this keyword saves all context configurations as well as the system 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	You can now save all context configurations with the **all** keyword.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line. Changes are only preserved between reboots if you save them to the startup configuration, which is the configuration loaded into running memory at startup. The location of the startup configuration for single context mode and for the system in multiple context mode can be changed from the default location (a hidden file) to a location of your choosing using the **boot config** command. For multiple context mode, a context startup configuration is at the location specified by the **config-url** command in the system configuration.

In multiple context mode, you can enter the **write memory** command in each context to save the current context configuration. To save all context configurations, enter the **write memory all** command in the system execution space. Context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server specified by the **config-url** command, except for HTTP and HTTPS URLs, which do not allow you to save the configuration back to the server. After the ASA saves each context with the **write memory all** command, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

```
The context 'context a' could not be saved due to Unavailability of resources
```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

```
The context 'context a' could not be saved due to non-reachability of destination
```

- For contexts that are not saved because the context is locked, the following message appears:

```
Unable to save the configuration for the following contexts as these contexts are locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

```
Unable to save the configuration for the following contexts as these contexts have read-only
 config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- For contexts that are not saved because of bad sectors in the Flash memory, the following message appears:

```
The context 'context a' could not be saved due to Unknown errors
```

Because the system uses the admin context interfaces to access context startup configurations, the **write memory** command also uses the admin context interfaces. The **write net** command, however, uses the context interfaces to write a configuration to a TFTP server.

The **write memory** command is equivalent to the **copy running-config startup-config** command.

Examples

The following example saves the running configuration to the startup configuration:

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454
19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

Related Commands

Command	Description
admin-context	Sets the admin context.
configure memory	Merges the startup configuration with the running configuration.
config-url	Specifies the location of the context configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

write net

To save the running configuration to a TFTP server, use the **write net** command in privileged EXEC mode.

write net [*server* **:** [*filename*] **|:** *filename*]

Syntax Description

: *filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the ASA treats the **tftp-server** command filename as a directory, and adds the **write net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If your TFTP server does not support this type of URL, use the **copy running-config tftp** command instead. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
server **:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line.

In multiple context mode, this command saves only the current configuration; you cannot save all contexts with a single command. You must enter this command separately for the system and for each context. The **write net** command uses the context interfaces to write a configuration to a TFTP server. The **write memory** command, however, uses the admin context interfaces to save to the startup configuration because the system uses the admin context interfaces to access context startup configurations.

The **write net** command is equivalent to the **copy running-config tftp** command.

Examples

The following example sets the TFTP server and filename in the **tftp-server** command:

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command is not populated.

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command supplies the directory name, and the server address is overridden.

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
copy running-config tftp	Copies the running configuration to a TFTP server.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write memory	Saves the running configuration to the startup configuration.

write standby

To copy the ASA or context running configuration to the failover standby unit, use the **write standby** command in privileged EXEC mode.

write standby

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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You should only use this command if the configuration on the standby unit or failover group becomes out-of-sync with the configuration of the active unit or failover group. This typically happens when commands are entered on the standby unit or failover group directly.

For Active/Standby failover, the **write standby** command entered on the active unit writes the running configuration of the active failover unit to the running configuration on the standby unit.

For Active/Active failover, the **write standby** command behaves as follows:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the ASA are written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.

The **write standby** command replicates the configuration to the running configuration of the peer unit; it does not save the configuration to the startup configuration. To save the configuration changes to the startup configuration, use the **copy running-config startup-config** command on the same unit that you entered the **write standby** command. The command will be replicated to the peer unit and the configuration saved to the startup configuration.

When Stateful Failover is enabled, the **write standby** command also replicates state information to the standby unit after the configuration replication is complete. In multiple context mode, enter **write standby** within the context to replicate state information.

Note After you enter the write standby command, the failover interfaces will go down momentarily while the configuration becomes re-synchronized. This can also cause a temporary failure of the failover state interface to be detected.

Examples

The following example writes the current running configuration to the standby unit:

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

Related Commands

Command	Description
failover reload-standby	Forces the standby unit to reboot.

write terminal

To show the running configuration on the terminal, use the **write terminal** command in privileged EXEC mode.

write terminal

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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is equivalent to the show running-config command.

Examples

The following example writes the running configuration to the terminal:

```
ciscoasa# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.

Command	Description
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

xlate block-allocation

To configure the port block allocation characteristics for carrier-grade or large-scale PAT, use the **xlate block-allocation** command in global configuration mode. To return to default values, use the **no** form of this command.

xlate block-allocation { **size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds* }
no xlate block-allocation { **size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds* }

Syntax Description

size *value*	The block allocation size, which is the number of ports in each block. The range is 32-4096. The default is 512. If you do not use the default, ensure that the size you choose divides evenly into 64,512 (the number of ports in the 1024-65535 range). Otherwise, there will be ports that cannot be allocated. For example, if you specify 100, there will be 12 unused ports.
maximum-per-host *number*	The maximum blocks that can be allocated per host. The limit is per protocol, so a limit of 4 means at most 4 UDP blocks, 4 TCP blocks, and 4 ICMP blocks per host. The range is 1-8, the default is 4.
pba-interim-logging *seconds*	Enable interim logging. By default, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates message 305017 at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. You can specify an interval from 21600-604800 seconds (6 hours to 7 days).

Command Default

The default allocation size is 512. The default per-host maximum is 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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.
9.12(1)	The **pba-interim-logging** command was added.

Usage Guidelines

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 (see RFC 6888). 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. Blocks are freed when the last xlate that uses a port in the block is removed.

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.

The **xlate block-allocation** command configures the characteristics of these port blocks. Use the block-allocation keyword on the **nat** command to enable port block allocation per PAT rule when using a PAT pool.

Examples

The following example changes the port block allocation characteristics and implements port block allocation for a PAT pool in an object NAT rule:

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6
xlate block-allocation pba-interim-logging 21600
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat dynamic pat-pool mapped-pat-pool block-allocation
```

Related Commands

Command	Description
nat (global)	Adds a twice NAT rule.
nat (object)	Adds an object NAT rule.
show local-host	Shows the port blocks allocated to hosts.
show running-config xlate	Shows the **xlate** configuration.

xlate per-session

To use multi-session PAT, use the **xlate per-session** command in global configuration mode. To remove a multi-session PAT rule, use the **no** form of this command.

xlate per-session { **permit | deny** } { **tcp | udp** } *source_ip* [*operator src_port*] *destination_ip operator dest_port*
no xlate per-session { **permit | deny** } { **tcp | udp** } *source_ip* [*operator src_port*] *destination_ip operator dest_port*

Syntax Description

deny	Creates a deny rule.
destination_ip	For the destination IP address, you can configure the following: • **host** *ip_address* —Specifies an IPv4 host address. • *ip_address mask* —Specifies an IPv4 network address and subnet mask. • *ipv6-address/prefix-length* —Specifies an IPv6 host or network address and prefix. • **any4** and **any6**—**any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic.
operator dest_port	The *operator* matches the port numbers used by the destination. The permitted operators are as follows: • lt—less than • gt—greater than • eq—equal to • neq—not equal to • range—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200`
operator src_port	(Optional) The *operator* matches the port numbers used by the source. The permitted operators are as follows: • lt—less than • gt—greater than • eq—equal to • neq—not equal to • range—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200`

permit	Creates a permit rule.
source_ip	For the source IP address, you can configure the following: • **host** *ip_address* —Specifies an IPv4 host address. • *ip_address mask* —Specifies an IPv4 network address and subnet mask. • *ipv6-address/prefix-length* —Specifies an IPv6 host or network address and prefix. • **any4** and **any6**—**any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic.
tcp	Specifies TCP traffic.
udp	Specifies UDP traffic.

Command Default

By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. The following default rules are installed:

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

You cannot remove these rules, and they always exist after any manually-created rules. Because rules are evaluated in order, you can override the default rules. For example, to completely negate these rules, you could add the following deny rules:

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

Command Modes

The 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

The per-session PAT feature improves the scalability of PAT and, for clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For "hit-and-run" traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is 65535/*average-lifetime* .

By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT be creating a per-session deny rule.

When you add a per-session PAT rule, the rule is placed above the default rules, but below any other manually-created rules. Be sure to create your rules in the order you want them applied.

Examples

The following example creates a deny rule for H.323 traffic, so that it uses multi-session PAT:

```
ciscoasa(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
ciscoasa(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

Related Commands

Command	Description
clear configure xlate	Clears the **xlate per-session** rules.
nat (global)	Adds a twice NAT rule.
nat (object)	Adds an object NAT rule.
show running-config xlate	Shows the **xlate per-session** rules.

zone

To add a traffic zone, use the **zone** command in global configuration mode. To remove the zone, use the **no** form of this command.

zone *name*
no zone *name*

Syntax Description

name	Sets the zone name up to 48 characters in length.

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
9.3(2)	This command was added.

Usage Guidelines

You can assign multiple interfaces to a *traffic zone* , which lets traffic from an existing flow exit or enter the ASA on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the ASA as well as external load balancing of traffic to the ASA across multiple interfaces.

Zones allow traffic to and from any interface in the zone, but the security policy itself (access rules, NAT, and so on) is still applied per interface, not per zone. If you configure the same security policy for all interfaces within the zone, then you can successfully implement ECMP and load balancing for that traffic.

You can create a maximum of 256 zones.

Examples

The following example configures an outside zone with 4 member interfaces:

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.

zonelabs-integrity fail-close

To configure the ASA so that connections to VPN clients close when the connection between the ASA and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command in global configuration mode.To reinstate the default whereby the VPN connections remain open on failure of the Zone Labs connection, use the **no** form of this command.

zonelabs-integrity fail-close
no zonelabs-integrity fail-close

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the connection remains open on failure.

Command Modes

The 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

If the primary Zone Labs Integrity Firewall Server does not respond to the ASA, the ASA still establishes VPN client connections to the private network by default. It also maintains open, existing connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command.

To return to the default condition whereby the ASA maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command.

Examples

The following example configures the ASA to close the VPN client connections if the Zone Labs Integrity Firewall Server fails to respond or if the connection is interrupted:

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the ASA remain open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

zonelabs-integrity fail-open

To keep remote VPN client connections to the ASA open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command in global configuration mode. To close connections to VPN clients upon failure of the Zone Labs server connection, use the **no** form of this command.

zonelabs-integrity fail-open
no zonelabs-integrity fail-open

Syntax Description

This command has no arguments or keywords.

Command Default

By default, remote VPN connections remain open if the ASA does not establish or maintain a connection to the Zone Labs Integrity Firewall 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	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the ASA, the ASA still establishes VPN client connections to the private network by default. It also maintains existing open connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command. To then return to the default condition whereby the ASA maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command or the **no zonelabs-integrity fail-open** command.

Examples

The following example reinstates the default condition whereby the VPN client connections remain open if the connection to the Zone Labs Integrity Firewall Server fails:

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.

zonelabs-integrity fail-timeout

To specify the time in seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Server unreachable, use the **zonelabs-integrity fail-timeout** command in global configuration mode. To restore the default timeout of 10 seconds, use the **no** form of this command without an argument.

zonelabs-integrity fail-timeout *timeout*
no zonelabs-integrity fail-timeout

Syntax Description

timeout	The number of seconds before the ASA declares a nonresponsive Zone Labs Integrity Firewall Servers unreachable. The acceptable range is from 5 to 20 seconds.

Command Default

The default timeout value 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If the ASA waits for the specified number of seconds without a response from the Zone Labs server, the server is declared nonresponsive. Connections to VPN clients either remain open by default or if configured to do so with the **zonelabs-integrity fail-open** command. If, however, the **zonelabs-integrity fail-close** command has been issued, the connections will close when the ASA declares the Integrity server unresponsive.

Examples

The following example configures the ASA to declare the active Zone Labs Integrity Server to be unreachable after 12 seconds:

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the ASA remain open after the connection between the ASA and the Zone Labs Integrity Firewall Server fails.

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

zonelabs-integrity interface

To specify an ASA interface for communication with the Zone Labs Integrity Server, use the **zonelabs-integrity interface** command in global configuration mode. To reset the Zone Labs Integrity Firewall Server interface back to the default of none, use the **no** form of this command.

zonelabs-integrity interface *interface*
no zonelabs-integrity interface

Syntax Description

interface	Specifies the ASA interface on which the Zone Labs Integrity Firewall Server communicates. It is often an interface name created with the **nameif** command.

Command Default

By default, the Zone Labs Integrity Firewall Server interface 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example configures three Zone Labs Integrity Servers using IP addresses ranging from 10.0.0.5 to 10.0.0.7. The commands also configure the ASA to listen to the server on port 300 and on an interface called inside:

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)# zonelabs-integrity interface inside
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.

Command	Description
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity port

To specify a port on the ASA for communicating with a Zone Labs Integrity Firewall Server, use the **zonelabs-integrity port** command in global configuration mode. To revert to the default port of 5054 for the Zone Labs Integrity Firewall Server, use the **no** form of this command.

zonelabs-integrity port *port_number*
no zonelabs-integrity port *port_number*

Syntax Description

port	Specifies a Zone Labs Integrity Firewall Server port on the ASA.
port_number	The number of the Zone Labs Integrity Firewall Server port. It can range from 10 to 10000.

Command Default

The default Zone Labs Integrity Firewall Server port is 5054.

Command Modes

The 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 ASA listens to the Zone Labs Integrity Firewall Server on the port and interface configured with the **zonelabs-integrity port** and **zonelabs-integrity interface** commands respectively.

Note The current release of the ASA supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

Examples

The following example configures a Zone Labs Integrity Servers using the IP address 10.0.0.5. The commands also configure the ASA to listen to the active Zone Labs server on port 300 instead of the default 5054 port:

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity server-address

To add Zone Labs Integrity Firewall Servers to the ASA configuration, use the **zonelabs-integrity server-address** command in global configuration mode. Specify the Zone Labs server by either IP address or hostname.

To remove Zone Labs Integrity Firewall Servers from the running configuration, use the **no** form of this command without arguments.

zonelabs-integrity server-address { *hostname1* | *ip-address1* }
no zonelabs-integrity server-address

Note While the user interfaces appear to support the configuration of multiple Integrity Servers, the ASA only supports one server at a time in the current release.

Syntax Description

hostname	Specifies the hostname of the Zone Labs Integrity Firewall Server. See the **name** command for hostname guidelines.
ip-address	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Command Default

By default, no Zone Labs Integrity Firewall Servers 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
7.2(1)	This command was added.

Usage Guidelines

With this release, you can configure one Zone Labs Integrity Firewall Server. If that server fails, configure another Integrity Server first and then reestablish the client VPN session.

To specify a server by hostname, you must first configure the Zone Labs server name using the **name** command. Before using the **name** command, use the **names** command to enable it.

Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

Examples

The following example assigns the server name ZL-Integrity-Svr to the IP address 10.0.0.5 and configures a Zone Labs Integrity Server using that name:

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the ASA close VPN client connections when the connection between the ASA and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity ssl-certificate-port

To specify an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate, use the **zonelabs-integrity ssl-certificate-port** command in global configuration mode. To revert to the default port number (80), use the **no** form of this command without an argument.

zonelabs-integrity ssl-certificate-port *cert-port-number*
no zonelabs-integrity ssl-certificate-port

Syntax Description

cert-port-number	Specifies a port number on which the ASA expects the Zone Labs Integrity Firewall Server to connect when requesting an SSL certificate.

Command Default

By default, the ASA expects the Zone Labs Integrity Firewall Server to request an SSL certificate on port 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

For SSL communications between the ASA and the Zone Labs Integrity Firewall Server, the ASA is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (ASA) must be authenticated by the client (Zone Labs server). The **zonelabs-integrity ssl-certificate-port** command specifies the port to which the Zone Labs server connects when requesting the SSL server certificate.

Examples

The following example configures port 30 on the ASA to receive SSL certificate requests from the Zone Labs Integrity Server:

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA.

zonelabs-integrity ssl-client-authentication

To enable authentication of the Zone Labs Integrity Firewall Server SSL certificate by the ASA, use the **zonelabs-integrity ssl-client-authentication** command in global configuration mode with the *enable* argument. To disable authentication of the Zone Labs SSL certificate, use the *disable* argument or use the **no** form of this command without an argument.

zonelabs-integrity ssl-client-authentication { *enable* | *disable* }
no zonelabs-integrity ssl-client-authentication

Syntax Description

disable	Specifies the IP address of the Zone Labs Integrity Firewall Server.
enable	Specifies that the ASA authenticates the SSL certificate of the Zone Labs Integrity Firewall Server.

Command Default

By default, ASA authentication of the Zone Labs Integrity Firewall Server SSL certificate 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

For SSL communications between the ASA and the Zone Labs Integrity Firewall Server, the ASA is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (ASA) must be authenticated by the client (Zone Labs server). Authentication of the client certificate is optional, however. You use the **zonelabs-integrity ssl-client-authentication** command to enable or disable ASA authentication of the Zone Lab server (SSL client) certificate.

Examples

The following example configures the ASA to authenticate the SSL certificate of the Zone Labs Integrity Server:

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the ASA interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the ASA for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the ASA configuration.
zonelabs-integrity ssl-certificate-port	Specifies an ASA port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.

zone-member

To add an interface to a traffic zone, use the **zone-member** command in interface configuration mode. To remove the interface, use the **no** form of this command.

zone-member *name*
no zone-member *name*

Syntax Description

name	Identifies the zone name set by the **zone** 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
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Configure all interface parameters including the name, IP address, and security level. The first interface that you add to a zone determines the security level of the zone. All additional interfaces must have the same security level. To change the security level for interfaces in a zone, you must remove all but one interface, and then change the security levels, and re-add the interfaces.

When you assign an interface to a zone, any connections on that interface are deleted. The connections must be reestablished.

If you remove an interface from a zone, any connections that have the interface as the primary interface are deleted. The connections must be reestablished. If the interface is the current interface, the ASA moves the connections back to the primary interface. The zone route table is also refreshed.

You can add the following types of interfaces to a zone:

- Physical
- VLAN
- EtherChannel
- Redundant

You cannot add the following types of interfaces:

- Management-only
- Management-access
- Failover or state link
- Cluster control link
- Member interfaces in an EtherChannel or redundant interface

An interface can be a member of only one zone.

You can include up to 8 interfaces per zone.

Examples

The following example configures an outside zone with 4 member interfaces:

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.

PART II

IOS Commands for ASASM

Cisco IOS Commands for ASASM

clear diagnostics loopback

To clear the online diagnostic test configuration, use the clear diagnostic **loopback** command in privileged EXEC mode.

clear diagnostics loopback

Syntax Description

This command has no arguments or keywords

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

The **clear diagnostics loopback** command clears the online diagnostic test configuration.

Examples

The following is sample output from the **clear diagnostics loopback** command:

```
ciscoasa#
clear diagnostics loopback
Port  Test  Pkts-received    Failures
0  0  0    0
1  0  0    0
```

Related Commands

Command	Description
show diagnostics loopback	Shows the information related to the PC loopback test, the number of tests run, the number of loopback packets received, and the number of failures detected.

firewall autostate

To enable autostate messaging, use the **firewall autostate** command in global configuration mode. To disable autostate, use the **no** form of this command.

firewall autostate
no firewall autostate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, autostate is disabled.

Command Modes

Global configuration

Usage Guidelines

Autostate messaging lets the ASA quickly detect that a switch interface has failed or has come up. The supervisor engine can send autostate messages to the ASA about the status of physical interfaces associated with ASA VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASA that the VLAN is down. This information lets the ASA declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASA takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

The switch supervisor sends an autostate message to the ASA when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

Examples

The following example enables autostate messaging:

```
Router(config)# firewall autostate
```

Related Commands

Command	Description
show firewall autostate	Shows the setting of the autostate feature.

firewall module

To assign firewall groups to the ASA, enter the **firewall module** command in global configuration mode. To remove the groups, use the **no** form of this command.

firewall module *module_number* **vlan-group** *firewall_group*
no firewall module *module_number* **vlan-group** *firewall_group*

Syntax Description

module_number	Specifies the module number. Use the **show module** command to view installed modules and their numbers.
vlan-group *firewall_group*	Specifies one or more group numbers as defined by the **firewall vlan-group** command: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas. For example, enter the following numbers: `5,7-10`

Command Default

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

- You can assign up to 16 firewall VLAN groups to each ASASM. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) See the **firewall vlan-group** command to create a group. For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.
- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

Examples

The following example shows how to create three firewall VLAN groups: one for each ASA, and one that includes VLANs assigned to both ASAs.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the show firewall vlan-group command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

firewall multiple-vlan-interfaces

To allow you to add more than one SVI to the ASA, use the **firewall multiple-vlan-interfaces** command in global configuration mode. To disable this feature, use the **no** form of this command.

firewall multiple-vlan-interfaces
no firewall multiple-vlan-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

By default, multiple SVIs are not allowed.

Command Modes

Global configuration

Usage Guidelines

A VLAN defined on the MSFC is called a switched virtual interface. If you assign the VLAN used for the SVI to the ASA, then the MSFC routes between the ASA and other Layer 3 VLANs. For security reasons, by default, only one SVI can exist between the MSFC and the ASA. For example, if you misconfigure the system with multiple SVIs, you could accidentally allow traffic to pass around the ASA by assigning both the inside and outside VLANs to the MSFC.

However, you might need to bypass the ASA in some network scenarios. For example, if you have an IPX host on the same Ethernet segment as IP hosts, you will need multiple SVIs. Because the ASA in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the ASA for IPX traffic. Make sure to configure the MSFC with an access list that allows only IPX traffic to pass on the VLAN.

For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface. You might also choose to use multiple SVIs in routed mode so you do not have to share a single VLAN for the outside interface.

Examples

The following example shows a typical configuration with multiple SVIs:

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

The following is sample output from the show interface command:

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

```
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type:ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
Queueing strategy:fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
L3 out Switched:ucast:0 pkt, 0 bytes
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   4 packets output, 256 bytes, 0 underruns
   0 output errors, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to the ASA.
firewall vlan-group	Defines a VLAN group.

firewall vlan-group

To assign VLANs to a firewall group, enter the **firewall vlan-group** command in global configuration mode. To remove the VLANs, use the **no** form of this command.

firewall [**switch** { **1** | **2** }] **vlan-group** *firewall_group vlan_range*
no firewall [**switch** { **1** | **2** }] **vlan-group** *firewall_group vlan_range*

Syntax Description

firewall_group	Specifies the group ID as an integer.
vlan_range	Specifies the VLANs assigned to the group. The *vlan_range* value can be one or more VLANs (2 to 1000 and from 1025 to 4094) identified in one of the following ways: • A single number (*n*) • A range (*n*-*x*) Separate numbers or ranges by commas. For example, enter the following numbers: `5,7-10,13,45-100` **Note** Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Global configuration.

Usage Guidelines

- You can assign up to 16 firewall VLAN groups to each ASASM using the **firewall module** command. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- Use VLAN IDs 2 to 1000 and from 1025 to 4094.
- Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.

- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.
- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

Examples

The following example shows how to create three firewall VLAN groups: one for each ASA, and one that includes VLANs assigned to both ASAs.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the show firewall vlan-group command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

service-module session

To gain console access to the ASASM from the switch CLI, enter the **service-module session** command in privileged EXEC mode.

service-module session [**switch** { **1 | 2** }] **slot** *number*

Syntax Description

slot *number*	Specifies the slot number of the ASASM. To view the module slot numbers, enter the **show module** command at the switch prompt.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

Using the **service-module session** command, you create a virtual console connection to the ASASM, with all the benefits and limitations of an actual console connection.

Benefits include:

- The connection is persistent across reloads and does not time out.
- You can stay connected through ASASM reloads and view startup messages.
- You can access ROMMON if the ASASM cannot load the image.

Limitations include:

- The connection is slow (9600 baud).
- You can only have one console connection active at a time.

Note Because of the persistence of the connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection. See the CLI configuration guide for more information.

Examples

The following example shows how to gain console access to an ASASM in slot 3:

```
Router# service-module session slot 3
ciscoasa>
```

Related Commands

Commands	Description
session	Telnets to the ASASM over the backplane.

session

To Telnet from the switch CLI to the ASASM over the backplane, use the **session** command in privileged EXEC mode.

session [**switch** { **1 | 2** }] **slot** *number* **processor 1**

Syntax Description

processor 1	Specifies the processor number, which is always 1.
slot *number*	Specifies the slot number. To view the module slot numbers, enter the **show module** command at the switch prompt.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

Using the **session** command, you create a Telnet connection to the ASASM.

Benefits include:

- You can have multiple sessions to the ASASM at the same time.
- The Telnet session is a fast connection.

Limitations include:

- The Telnet session is terminated when the ASASM reloads, and can time out.
- You cannot access the ASASM until it completely loads; you cannot access ROMMON.

Note The **session** *slot* **processor 0** command, which is supported on other services modules, is not supported on the ASASM; the ASASM does not have a processor 0.

You are prompted for the login password. Enter the login password to the ASASM. By default, the password is **cisco**.

You access user EXEC mode.

Examples

The following example Telnets to an ASASM in processor 1:

```
Router# session slot number processor 1
ciscoasa passwd: cisco
ciscoasa>
```

Related Commands

Command	Description
service-module session	Obtains console access to the ASASM from the switch CLI.

show boot device

To view the default boot partition, use the **show boot device** command.

show boot device [*mod_num*]

Syntax Description

mod_num	(Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers.

Command Default

The default boot partition is cf:4.

Command Modes

Privileged EXEC.

Examples

The following is sample output from the **show boot device** command that shows the boot partitions for each installed ASA on Cisco IOS software:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Related Commands

Command	Description
boot device (IOS)	Sets the default boot partition.
show module (IOS)	Shows all installed modules.

show diagnostic loopback

To display information related to the PC loopback test, including the number of tests run, the number of loopback packets received, and the number of failures detected, use the **show diagnostics loopback** command in privileged EXEC mode.

show diagnostics loopback

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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
12.2(18)SXF5	This command was added.

Usage Guidelines

The **show diagnostics loopback command provides** information related to the PC loopback test, including the number of tests run, the number of loopback packets received, and the number of failures detected.

Examples

The following is sample output from the **show diagnostics loopback** command:

```
ciscoasa#
show diagnostics loopback
Port  Test  Pkts-received    Failures
0  447  447    0
1  447  447    0
```

Related Commands

Command	Description
clear diagnostics loopback	Clears the online diagnostic test configuration.
firewall autostate	Enables the autostate feature.

show firewall autostate

To view the setting of the autostate feature, use the **show firewall autostate** command in privileged EXEC mode.

show firewall autostate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, autostate is disabled.

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
Privileged EXEC	•	•	•	•	•

Usage Guidelines

Autostate messaging in Cisco IOS software allows the ASA to quickly detect that a switch interface has failed or come up. The switch supervisor sends an autostate message to the ASA when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

Related Commands

Command	Description
clear diagnostics loopback	Clears the online diagnostic test configuration.
firewall autostate	Enables the autostate feature.

show firewall module

To view the VLAN groups assigned to each ASA, enter the **show firewall module** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*]

Syntax Description

module_number	(Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

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

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
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

show firewall module state

To view the state of each ASA, enter the **show firewall module state** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*] **state**

Syntax Description

module_number	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module state command:

```
Router# show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.

Command	Description
show module	Shows all installed modules.

show firewall module traffic

To view the traffic flowing through each ASA, enter the **show firewall module traffic** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*] **traffic**

Syntax Description

module_number	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module traffic command:

```
Router# show firewall module 11 traffic
Firewall module 11:
Specified interface is up line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

show firewall module version

To view the software version number of the ASA Services Module, enter the **show firewall module version** command in privileged EXEC mode.

show firewall [**switch** { **1 | 2** }] **module** [*module_number*] **version**

Syntax Description

module_number	(Optional) Specifies the module number.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Examples

The following is sample output from the show firewall module version command:

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:
Sw Version: 100.7(8)19
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show firewall module vlan-group

To view VLAN groups that can be assigned to the ASA, enter the**show firewall module vlan-group** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*] **vlan-group** [*firewall_group*]

Syntax Description

firewall_group	(Optional) Specifies the group ID.
module_number	(Optional) Specifies the module number.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module vlan-group command:

```
Router# show firewall module vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show firewall multiple-vlan-interfaces

To show the state of multiple firewall VLAN interfaces for the ASASM, enter the **show firewall multiple-vlan-interfaces** command in privileged EXEC mode.

show firewall multiple-vlan-interfaces

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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall multiple-vlan-interfaces command:

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show module

To verify that the switch acknowledges the ASASM and has brought it online, use the **show module** command in privileged EXEC mode.

show module [**switch** { **1** | **2** }] [*mod-num* | **all**]

Syntax Description

all	(Optional) Specifies all the modules.
mod_num	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show module command:

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2    3  ASA Service Module                      WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                      WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                     WS-X6716-10GE      SAL1442WZD1
Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok
Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok
Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
```

```
 4 TRIFECTA           SAD135101Z9
Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.