思科 ASA 系列命令参考、ASASM 的 T 至 Z 命令和 IOS 命令

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

文本部件号： 不适用，仅在线提供

思科 ASA 系列命令参考、ASASM 的 T 至 Z 命令和 IOS 命令

第 1 部分

T 至 Z 命令

Table-map 至 title

table-map

要在 IP 路由表通过 BGP 获知路由进行更新时修改度量和标记值，请在地址系列配置模式下使用 **table-map** 命令。要禁用此功能，请使用该命令的 **no** 形式。

table-map *map_name*

no table-map *map_name*

语法说明

map_name	来自 **route-map** 命令的路由映射名称。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
地址系列配置	• 是	-	• 是	• 是	-

命令历史记录

版本	**修改**
9.2(1)	添加了此命令。

使用指南

此命令将 **route-map** 命令定义的路由映射名称添加到 IP 路由表。此命令用于设置标记名称和路由度量以实施重分布。

您可在 **table-map** 命令中使用路由映射的 **match** 子句。支持 IP 访问列表、自治系统路径和下一跃点 match 子句。

示例

在以下地址系列配置模式示例中，ASA 软件配置为自动计算 BGP 获知路由的标记值并更新 IP 路由表：

```
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
```

相关命令

命令	描述
address-family	进入 address-family 配置模式。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。

tcp-inspection

要启用通过 TCP 的 DNS 检测，请在参数配置模式下使用 **tcp-inspection** 命令。要禁用协议实施，请使用此命令的 **no** 形式。

tcp-inspection

no tcp-inspection

语法说明

此命令没有任何参数或关键字。

默认值

禁用通过 TCP 的 DNS 检测。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.6(2)	添加了此命令。

使用指南

将此命令添加到 DNS 检测策略映射，以便在检测中包括 DNS/TCP 端口 53 流量。如果不使用此命令，则仅会检测 UDP/53 DNS 流量。确保 DNS/TCP 端口 53 流量是要应用 DNS 检测的类的一部分。该检测的默认类包括 TCP/53。

示例

以下示例展示如何在 DNS 检测策略映射中启用通过 TCP 进行的 DNS 检测：

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

相关命令

命令	描述
inspect dns	启用 DNS 检测。
policy-map type inspect dns	创建 DNS 检测策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

tcp-map

要定义一组 TCP 规范化操作，请在全局配置模式下使用 **tcp-map** 命令。TCP 规范化功能可让您指定识别异常数据包的标准，ASA 在检测到这些数据包时将其丢弃。要删除 TCP 映射，请使用此命令的 **no** 形式。

tcp-map *map_name*

no tcp-map *map_name*

语法说明

map_name	指定 TCP 映射名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
7.2(4)/8.0(4)	添加了 **invalid-ack**、**seq-past-window** 和 **synack-data** 子命令。

使用指南

此功能使用模块化策略框架。首先使用 **tcp-map** 命令定义您想要执行的 TCP 规范化操作。**tcp-map** 命令会进入 tcp-map 配置模式，您可在此模式下输入一条或多条命令来定义 TCP 规范化操作。然后，使用 **class-map** 命令定义您要对其应用 TCP 映射的流量。输入 **policy-map** 命令以定义策略，然后输入 **class** 命令以引用类映射。在类配置模式下，输入 **set connection advanced-options** 命令，以引用 TCP 映射。最后，使用 **service-policy** 命令将策略映射应用到接口。有关模块化策略框架工作原理的详细信息，请参阅 CLI 配置指南。

以下命令在 tcp-map 配置模式下可用：

check-retransmission	启用和禁用重新传输数据检查。
checksum-verification	启用和禁用校验和验证。
exceed-mss	允许或丢弃超出对等设备所设置的 MSS 数据包。
invalid-ack	设置对具有无效 ACK 的数据包的操作。
queue-limit	配置可以排队等待 TCP 连接的无序数据包的最大数量。此命令仅在 ASA 5500 系列自适应 ASA 上可用。在 PIX 500 系列 ASA 上，队列限制为 3 且无法更改。
reserved-bits	在 ASA 中设置保留标志策略。

seq-past-window	设置对具有 past-window 序列号的数据包的操作，即接收的 TCP 数据包序列号大于 TCP 接收窗口的右侧边界。
synack-data	设置对包含数据的 TCP SYNACK 数据包的操作。
syn-data	允许或丢弃具有数据的 SYN 数据包。
tcp-options	基于 TCP 报头中的 TCP 选项字段的内容来设置数据包的操作。
ttl-evasion-protection	启用或禁用 ASA 提供的 TTL 回避保护。
urgent-flag	通过 ASA 允许或清除 URG 指针。
window-variation	丢弃意外更改其窗口大小的连接。

示例

例如，要允许所有流量的紧急标志和紧急偏移数据包发送到众所周知的 FTP 数据端口与 Telnet 端口之间的 TCP 端口范围，请输入以下命令：

```
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
```

相关命令

命令	描述
class (policy-map)	指定要用于流量分类的类映射。
clear configure tcp-map	清除 TCP 映射配置。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config tcp-map	显示关于 TCP 映射配置的信息。
tcp-options	允许或清除 selective-ack、timestamp 或 window-scale TCP 选项。

tcp-options

要在 TCP 报头中允许或清除 TCP 选项，请在 tcp-map 配置模式下使用 **tcp-options** 命令。要删除此指定，请使用此命令的 **no** 形式。

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*

语法说明

action	要为选项执行的操作。操作包括： • **allow** [**multiple**] - 允许包含该选项的数据包。自 9.6(2) 起，**allow** 表示允许包含单个此类型选项的数据包。这是所有已命名选项的默认设置。如果要允许数据包，即便其中包含该选项的多个实例亦不例外，请添加 **multiple** 关键字。**multiple** 关键字不适用于 **range**。 • **maximum** *limit* - 仅限 **mss**。将最大分段大小设置为所示的限制，范围为 68-65535。默认 TCP MSS 在 **sysopt connection tcpmss** 命令中定义。 • **clear** - 从报头中删除此类型的选项并允许该数据包。这是您可以在 **range** 关键字中配置的所有已编号选项的默认设置。请注意，清除时间戳选项将禁用 PAWS 和 RTT。 • **drop** - 丢弃包含此选项的数据包。此操作仅可用于 **md5** 和 **range**。
md5	为 MD5 选项设置操作。
mss	为最大分段大小选项设置操作。
range *lower upper*	为范围下限和上限内的编号选项设置操作。要为单个编号选项设置操作，请对范围下限和上限输入相同的编号。 （9.6(2) 及更高版本。）有效范围为 6-7、9-18 和 20-255。 （9.6(1) 及更低版本。）有效范围为 6-7 和 9-255。
selective-ack	为选择性确认机制 (SACK) 选项设置操作。
timestamp	为时间戳选项设置操作。清除时间戳选项将禁用 PAWS 和 RTT。
window-scale	为窗口缩放机制选项设置操作。

默认值

（9.6(1) 及更低版本。）默认将允许所有已命名选项，并清除选项 6-7 和 9-255。

（9.6(2) 及更高版本。）默认将允许每个已命名选项的一个实例、丢弃具有一个以上给定已命名选项的数据包，并清除 6-7、9-18 和 20-155 选项。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Tcp-map 配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.6(2)	如果对已命名选项的默认处理中包含给定类型的单个选项，则更改为允许数据包；如果有多个该类型的选项，则丢弃数据包。此外，添加了 **md5**、**mss**、**allow multiple** 和 **mss maximum** 关键字。MD5 选项的默认值已从清除更改为允许。

使用指南

将 **tcp-map** 命令与模块化策略框架基础设施结合使用。使用 **class-map** 命令定义流量类并使用 **tcp-map** 命令定制 TCP 检查。应用新 TCP 映射使用 **policy-map** 命令。使用 **service-policy** 命令激活 TCP 检查。

使用 **tcp-map** 命令进入 TCP 映射配置模式。在 tcp-map 配置模式下使用 **tcp-options** 命令定义对各种 TCP 选项的处理方式。

示例

以下示例展示如何丢弃 6-7 和 9-255 范围内具有 TCP 选项的所有数据包：

```
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
```

相关命令

命令	描述
class	指定要用于流量分类的类映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
set connection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 tcp-map 配置模式的访问。

telnet

要允许接口的 Telnet 访问，请在全局配置模式下使用 **telnet** 命令。要删除 Telnet 访问，请使用此命令的 **no** 形式。

telnet {*ipv4_address mask* | *ipv6_address/prefix*} *interface_name*

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

语法说明

interface_name	指定要在其上允许 Telnet 的接口的名称。除非在 VPN 隧道中使用 Telnet，否则无法在最低安全接口上启用 Telnet。可以指定物理或虚拟接口。
ipv4_address mask	指定授权通过 Telnet 登录到 ASA 的主机或网络的 IPv4 地址，以及子网掩码。
ipv6_address/prefix	指定授权通过 Telnet 登录到 ASA 的 IPv6 地址/前缀。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(2)、9.1(2)	默认密码“cisco”已删除；您必须主动使用 **password** 命令设置登录密码。
9.9.(2)	现在，可以指定虚拟接口。

使用指南

telnet 命令可让您指定哪些主机能够通过 Telnet 访问 ASA CLI。您可以启用 Telnet 以登录到所有接口上的 ASA。但是，除非在 VPN 隧道内使用 Telnet，否则无法使用 Telnet 登录到最低安全接口。此外，如果指定了 BVI 接口，则必须在该接口上配置 **managenent-access**。

使用 **password** 命令以设置控制台 Telnet 访问的密码。使用 **who** 命令以查看哪些 IP 地址当前正在访问 ASA 控制台。使用 **kill** 命令以终止活动的 Telnet 控制台会话。

如果您使用 **aaa authentication telnet console** 命令，则 Telnet 控制台访问必须使用身份验证服务器进行验证。

示例

本例显示如何允许主机 192.168.1.3 和 192.168.1.4 通过 Telnet 访问 ASA CLI。此外，位于 192.168.2.0 网络上的所有主机均被赋予访问权限。

```
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
```

本例显示 Telnet 控制台登录会话（输入时未显示密码）：

```
ciscoasa# passwd: cisco

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

您可以使用 **no telnet** 命令删除单独的条目，也可以使用 **clear configure telnet** 命令删除所有 telnet 命令语句：

```
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
```

相关命令

命令	描述
clear configure telnet	从配置中删除 Telnet 连接。
kill	终止 Telnet 会话。
show running-config telnet	显示授权使用 Telnet 连接登录到 ASA 的 IP 地址当前列表。
telnet timeout	设置 Telnet 超时。
who	显示 ASA 上活动的 Telnet 管理会话。

telnet timeout

要设置 Telnet 空闲超时，请在全局配置模式下使用 **telnet timeout** 命令。要恢复默认超时，请使用此命令的 **no** 形式。

telnet timeout *minutes*

no telnet timeout *minutes*

语法说明

minutes	Telnet 会话被 ASA 关闭之前可处于空闲状态的分钟数。有效值为 1 到 1440 分钟。默认值为 5 分钟。

默认值

默认情况下，Telnet 会话空闲五分钟后即被 ASA 关闭。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

使用 **telnet timeout** 命令设置控制台 Telnet 会话被 ASA 注销之前可处于空闲状态的最长时间。

示例

本例显示如何更改最长会话空闲持续时间：

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

相关命令

命令	描述
clear configure telnet	从配置中删除 Telnet 连接。
kill	终止 Telnet 会话。
show running-config telnet	显示授权使用 Telnet 连接登录到 ASA 的 IP 地址当前列表。
telnet	启用对 ASA 的 Telnet 访问。
who	显示 ASA 上活动的 Telnet 管理会话。

terminal interactive

如果要在 CLI 中输入 **?** 时启用当前 CLI 的帮助，请在特权 EXEC 模式下使用 **terminal interactive** 命令。要禁用 CLI 帮助，请使用此命令的 **no** 形式。

terminal interactive

no terminal interactive

语法说明

此命令没有任何参数或关键字。

默认值

默认已启用交互式 CLI 帮助。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
9.4(1)	添加了此命令。

使用指南

通常，在 ASA CLI 中输入 **?** 时，会显示命令帮助。为了能够输入 **?** 作为命令中的文本（例如，将 **?** 加入 URL 中），可以使用 **no terminal interactive** 命令禁用交互式帮助。

示例

以下示例显示如何将控制台转换成非交互模式再转换为交互模式：

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

相关命令

命令	描述
clear configure terminal	清除终端显示宽度设置。
pager	设置在出现“---more---”提示符前要在 Telnet 会话中显示的行数。此命令将保存到配置。
show running-config terminal	显示当前终端设置。
terminal pager	设置在出现“---more---”提示符前要在 Telnet 会话中显示的行数。此命令不会保存到配置中。
terminal width	在全局配置模式中设置终端显示宽度。

terminal monitor

要允许在当前 CLI 会话中显示系统日志消息，请在特权 EXEC 模式下使用 **terminal monitor** 命令。要禁用系统日志消息，请使用此命令的 **no** 形式。

terminal {**monitor** | **no monitor**}

语法说明

监控	允许在当前 CLI 会话中显示系统日志消息。
no monitor	禁止在当前 CLI 会话中显示系统日志消息。

默认值

默认情况下，系统日志消息已禁用。默认情况下此命令为交互式命令。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	**修改**
7.0(1)	添加了此命令。

示例

以下示例显示如何在当前会话中显示和禁用系统日志消息：

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

相关命令

命令	**描述**
clear configure terminal	清除终端显示宽度设置。
pager	设置在出现“---more---”提示符前要在 Telnet 会话中显示的行数。此命令将保存到配置。
show running-config terminal	显示当前终端设置。
terminal pager	设置在出现“---more---”提示符前要在 Telnet 会话中显示的行数。此命令不会保存到配置中。
terminal width	在全局配置模式中设置终端显示宽度。

terminal pager

要设置在出现 Telnet 会话“---More---”提示符前在页面上显示的行数，请在特权 EXEC 模式下使用 **terminal pager** 命令。

terminal pager [lines] *lines*

语法说明

[**lines**] *lines*	设置在出现“---More---”提示符前在页面上显示的行数。默认值是 24 行；0 表明不存在页面限制。行数范围是 0 至 2147483647 行。**lines** 关键字可选，并且无论是否存在关键词，命令都是一样的。

默认值

默认值为 24 行。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令仅更改当前 Telnet 会话的分页程序行设置。但是，仅当您在用户 EXEC 模式下输入 **login** 命令，或输入 **enable** 命令以进入特权 EXEC 模式时，ASA 才会从正在运行配置重新发起当前会话中的分页程序值。这正如原先设计的那样。

注 在 ASA 重新显示用户提示符之前，出现意外的“---More---”提示符，这可能会抑制 **banner exec** 命令的输出。而是使用 **banner motd** 命令或 **banner login** 命令。

要将新的默认分页程序设置保存到配置，请执行以下操作：

1. 通过输入 **login** 命令访问用户 EXEC 模式，或通过输入 **enable** 命令访问特权 EXEC 模式。
2. 输入 **pager** 命令。

如果您使用 Telnet 访问管理情景，则分页程序行设置会在您更改为其他情景时跟随您的会话，即使在给定情景中 **pager** 命令具有不同设置。要更改当前分页程序设置，请使用新设置输入 **terminal pager** 命令，您也可以在当前情景中输入 **pager** 命令。除将新分页程序设置保存到情景配置外，**pager** 命令还可将新设置应用于当前 Telnet 会话中。

示例

以下示例将显示的行数更改为 20：

```
ciscoasa# terminal pager 20
```

相关命令

命令	描述
clear configure terminal	清除终端显示宽度设置。
pager	设置在出现“---More---”提示符前要在 Telnet 会话中显示的行数。此命令将保存到配置。
show running-config terminal	显示当前终端设置。
terminal	允许在 Telnet 会话中显示系统日志消息。
terminal width	在全局配置模式中设置终端显示宽度。

terminal width

要设置控制台会话期间显示信息的宽度，请在全局配置模式下使用 **terminal width** 命令。要禁用，请使用此命令的 **no** 形式。

terminal width *columns*

no terminal width *columns*

语法说明

columns	指定终端宽度（以列为单位）。默认值为 80。范围为 40 到 511。

默认值

默认显示宽度为 80 列。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

示例

本例显示如何将终端显示宽度设为 100 列：

```
ciscoasa# terminal width 100
```

相关命令

命令	描述
clear configure terminal	清除终端显示宽度设置。
show running-config terminal	显示当前终端设置。
terminal	在特权 EXEC 模式下设置终端行参数。

test aaa-server

要检查 ASA 是否能够使用特定 AAA 服务器验证或授权用户，请在特权 EXEC 模式下使用 **test aaa-server** 命令。无法访问 AAA 服务器可能是由于 ASA 中的配置错误，或者 AAA 服务器可能出于其他原因（例如受限的网络配置或服务器停机）无法访问。

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

语法说明

ad-agent	测试与 AAA AD 代理服务器的连接。
authentication	测试 AAA 服务器的身份验证功能。
authorization	测试 AAA 服务器的传统 VPN 授权功能。
host *ip_address*	指定服务器 IP 地址。如果没有在命令中指定 IP 地址，系统将提示您输入地址。
password *password*	指定用户密码。如果没有在命令中指定密码，系统将提示您输入密码。
server_tag	指定通过 **aaa-server** 命令设置的 AAA 服务器标记。
username *username*	指定用于测试 AAA 服务器设置的帐户的用户名。确保 AAA 服务器中存在该用户名；否则，测试将失败。如果没有在命令中指定用户名，系统将提示您输入用户名。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(4)	添加了此命令。
8.4(2)	添加了 **ad-agent** 关键字。

使用指南

test aaa-server 命令可让您验证 ASA 是否能够使用特定 AAA 服务器验证用户，以及对于传统 VPN 授权，您是否能够授权用户。此命令可让您测试 AAA 服务器而无需尝试验证或授权的实际用户。它还可帮助您隔离 AAA 故障是由于 AAA 服务器参数配置错误、AAA 服务器连接问题还是 ASA 中的其他配置错误。

示例

以下示例配置主机 192.168.3.4 上名为 srvgrp1 的 RADIUS AAA 服务器，将超时设置为 9 秒，将重试间隔设置为 7 秒，并配置验证端口 1650。**test aaa-server** 命令跟随 AAA 服务器参数的设置表明身份验证测试无法访问该服务器。

```
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
```

以下是具有成功结果的 **test aaa-server** 命令的输出示例：

```
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
```

相关命令

命令	描述
aaa authentication console	配置管理流量的身份验证。
aaa authentication match	配置通过流量的身份验证。
aaa-server	创建 AAA 服务器组。
aaa-server host	将 AAA 服务器添加到服务器组。

test aaa-server ad-agent

要在配置后测试 Active Directory 代理配置，请在 AAA 服务器组配置模式下使用 **test aaa-server ad-agent** 命令。

test aaa-server ad-agent

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Aaa 服务器组配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

要为身份防火墙配置 Active Directory 代理，必须输入 **ad-agent-mode** 命令，即 **aaa-server** 命令的子模式。输入 **ad-agent-mode** 命令即可进入 AAA 服务器组配置模式。

配置 Active Directory 代理后，输入 **test aaa-server ad-agent** 命令验证 ASA 是否有与 Active Directory 代理的功能性连接。

AD 代理可通过 WMI 定期或按需监控 Active Directory 服务器安全事件日志文件有无用户登录和注销事件。AD 代理维护用户 ID 和 IP 地址映射的缓存并向 ASA 通报更改。

配置 AD 代理服务器组的主 AD 代理和辅助 AD 代理。当 ASA 检测到主要 AD 代理未响应并且辅助代理已指定时，ASA 会切换到辅助 AD 代理。AD 代理的 Active Directory 服务器使用 RADIUS 作为通信协议；因此，应指定 ASA 与 AD 代理之间共享密钥的主要属性。

示例

以下示例展示如何在为身份防火墙配置 Active Directory 代理的同时启用 **ad-agent-mode**，然后测试连接：

```
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
```

相关命令

命令	描述
aaa-server	创建 AAA 服务器组并配置组特定和所有组主机通用的 AAA 服务器参数。
clear configure user-identity	清除身份防火墙功能的配置。

test dynamic-access-policy attributes

要进入 dap 属性模式，请从特权 EXEC 模式输入 **test dynamic-access-policy attributes** 命令。这样可以指定用户和终端属性值对。

dynamic-access-policy attributes

默认值

没有默认值或行为。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

通常，ASA 从 AAA 服务器检索用户授权属性，而从思科安全桌面、主机扫描、CNA 或 NAC 检索终端属性。对于 test 命令，您可在此属性模式下指定用户授权和终端属性。ASA 将其写入评估 DAP 记录的 AAA 选择属性和终端选择属性时 DAP 子系统引用的属性数据库。

此功能可让您尝试创建 DAP 记录。

示例

以下示例展示如何使用 **attributes** 命令。

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

相关命令

命令	描述
dynamic-access-policy-record	创建 DAP 记录。
attributes	进入属性模式，您可在该模式下指定用户属性值对。
display	显示当前属性列表。

test dynamic-access-policy execute

要测试已配置的 DAP 记录，请在特权 EXEC 模式下使用 test dynamic-access-policy execute 命令：

test dynamic-access-policy execute

语法说明

AAA attribute value	评估每个记录的 AAA 和终端选择属性时，设备上的 DAP 子系统会引用这些值。 – AAA 属性 - 标识 AAA 属性。 – 操作值 - 将属性标识为 =/!= 指定的值。
endpoint attribute value	标识终端属性。 – 终端 ID - 提供终端属性 ID。 – 名称/操作/值 -

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(4)	添加了此命令。

使用指南

通过指定授权属性值对，此命令可让您测试检索设备上配置的一组 DAP 记录。

test regex

要测试正则表达式，请在特权 EXEC 模式下使用 **test regex** 命令。

test regex *input_text regular_expression*

语法说明

input_text	指定要匹配正则表达式的文本。
regular_expression	指定正则表达式，最多 100 个字符的长度。有关正则表达式中可使用元字符的列表，请参阅 **regex** 命令。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

test regex 命令测试正则表达式以确保其匹配您认为其将匹配的内容。

如果正则表达式匹配输入文本，您将看到以下消息：

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

如果正则表达式不匹配输入文本，您将看到以下消息：

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

示例

以下示例针对正则表达式测试输入文本：

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

ciscoasa# test regex farscape scaper

INFO: Regular expression match failed.
```

相关命令

命令	描述
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	通过将流量类和一个或多个操作关联，创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
class-map type regex	创建正则表达式类映射。
regex	创建正则表达式。

test sso-server（已弃用）

注 支持此命令的最后一个版本是版本 9.5(1)。

要测试具有试验身份验证请求的 SSO 服务器，请在特权 EXEC 模式下使用 **test sso-server** 命令。

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

语法说明

server-name	指定所测试 SSO 服务器的名称。
user-name	指定所测试 SSO 服务器中用户的名称。

默认值

没有默认值或行为。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Config-webvpn	• 是	-	• 是	-	-
Config-webvpn-sso-saml	• 是	-	• 是	-	-
Config-webvpn-sso-siteminder	• 是	-	• 是	-	-
全局配置模式	• 是	-	• 是	-	-
特权 EXEC	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。
9.5(2)	为了支持 SAML 2.0，此命令已弃用。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。**test sso-server** 命令测试 SSO 服务器是否已识别并响应身份验证请求。

如果未找到通过 *server-name* 参数指定的 SSO 服务器，则出现以下错误：

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

如果已找到 SSO 服务器，但未找到通过 *user-name* 参数指定的用户，则拒绝身份验证。

在身份验证中，ASA 充当 WebVPN 用户登录 SSO 服务器的代理。ASA 当前支持 SiteMinder SSO 服务器（以前称为 Netegrity SiteMinder ）和 SAML POST 类型 SSO 服务器。此命令适用于这两种类型的 SSO 服务器。

示例

以下示例进入特权 EXEC 模式，通过用户名 Anyuser 成功测试名为 my-sso-server 的 SSO 服务器：

```
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#
```

以下示例展示相同服务器的测试，但用户 Anotheruser 无法识别，因此身份验证失败：

```
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#
```

相关命令

命令	描述
max-retry-attempts	配置 ASA SSO 身份验证尝试失败后的重试次数。
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

text-color

要设置登录、主页和文件访问页面上 WebVPN 标题栏中文本的颜色，请在 webvpn 模式下使用 **text-color** 命令。要从配置中删除文本颜色并重置默认值，请使用此命令的 no 形式。

text-color [*black* | *white* | *auto***]**

no text-color

语法说明

auto	根据 secondary-color 命令的设置选择黑色或白色。也就是说，如果辅助颜色为黑色，则该值为白色。
black	标题栏的默认文本颜色为白色。
white	您可以将颜色更改为黑色。

默认值

标题栏的默认文本颜色为白色。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
config-webvpn	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

示例

以下示例展示如何将标题栏的文本颜色设置为黑色：

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

相关命令

命令	描述
secondary-text-color	设置 WebVPN 登录、主页和文件访问页面的辅助文本颜色。

tftp-server

要指定默认 TFTP 服务器以及路径和文件名与 **configure net** 或 **write net** 命令一起使用，请在全局配置模式下使用 **tftp-server** 命令。要删除服务器配置，请使用此命令的 **no** 形式。此命令支持 IPv4 和 IPv6 地址。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

语法说明

filename	指定路径和文件名。
interface_name	指定网关接口名称。如果指定了并非最高安全接口的接口，则显示一条警告消息，通知您该接口不安全。
server	设置 TFTP 服务器的 IP 地址或名称。您可以输入 IPv4 或 IPv6 地址。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	现在需要网关接口。

使用指南

tftp-server 命令可简化输入 **configure net** 和 **write net** 命令。当您输入 **configure net** 或 **write net** 命令时，您可以继承通过 **tftp-server** 命令指定的 TFTP 服务器，也可以提供自己的值。您还可以原样继承 **tftp-server** 命令中的路径，将路径和文件名添加到 **tftp-server** 命令值结尾，或覆盖 **tftp-server** 命令值。

ASA 仅支持一条 **tftp-server** 命令。

示例

以下示例展示如何指定 TFTP 服务器，然后从 /temp/config/test_config 目录读取配置：

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

相关命令

命令	描述
configure net	从您指定的 TFTP 服务器和路径载入配置。
show running-config tftp-server	显示默认 TFTP 服务器地址和配置文件的目录。

tftp-server address（已弃用）

要指定集群中的 TFTP 服务器，请在 phone-proxy 配置模式下使用 **tftp-server address** 命令。要从电话代理配置中删除 TFTP 服务器，请使用此命令的 **no** 形式。

tftp-server address *ip_address* [*port*] **interface** *interface*

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

语法说明

ip_address	指定 TFTP 服务器的地址。
interface *interface*	指定 TFTP 服务器所在的接口。此项必须是 TFTP 服务器的真实地址。
port	（可选）此项是 TFTP 服务器侦听 TFTP 请求的端口。如果不是默认的 TFTP 端口 69，应进行配置。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
电话代理配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(4)	添加了此命令。
9.4(1)	此命令以及所有 **phone-proxy** 模式命令均已弃用。

使用指南

电话代理必须配置至少一台 CUCM TFTP 服务器。最多可为电话代理配置五台 TFTP 服务器。

假设 TFTP 服务器位于防火墙背后受信任的网络上；因此，电话代理会拦截 IP 电话与 TFTP 服务器之间的请求。TFTP 服务器必须位于与 CUCM 相同的接口上。

使用内部 IP 地址创建 TFTP 服务器，并指定 TFTP 服务器所在的接口。

在 IP 电话上，必须配置 TFTP 服务器的 IP 地址如下：

- 如果为 TFTP 服务器配置 NAT，则使用 TFTP 服务器的全局 IP 地址。
- 如果没有为 TFTP 服务器配置 NAT，则使用 TFTP 服务器的内部 IP 地址。

如果服务策略全局应用，将创建分类规则，控制到达所有入口接口（TFTP 服务器所在的接口除外）上 TFTP 服务器的所有 TFTP 流量。当服务策略应用于特定接口时，将创建分类规则，将到达该指定接口上 TFTP 服务器的所有 TFTP 流量指向电话代理模块。

如果为 TFTP 服务器配置 NAT 规则，则必须在应用服务策略之前进行配置，以便在安装分类规则时使用 TFTP 服务器的全局地址。

示例

以下示例展示使用 **tftp-server address** 命令配置电话代理的两台 TFTP 服务器：

```
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
```

相关命令

命令	描述
phone-proxy	配置电话代理实例。

threat-detection basic-threat

要启用基本威胁检测，请在全局配置模式下使用 **threat-detection basic-threat** 命令。要禁用基本威胁检测，请使用此命令的 **no** 形式。

threat-detection basic-threat

no threat-detection basic-threat

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，启用基本威胁检测。使用以下默认速率限制：

表 1-1　基本威胁检测默认设置

	触发器设置	
丢包原因	**平均速率**	**突发速率**
• 检测到 DoS 攻击 • 数据包格式错误 • 超出连接限制 • 检测到可疑的 ICMP 数据包	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 400 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 320 个丢包/秒。
检测到扫描攻击	在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
	在过去 3600 秒内 4 个丢包/秒。	在过去 120 秒内 8 个丢包/秒。
检测不完整会话，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击（组合）	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 200 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 160 个丢包/秒。
被访问列表拒绝	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 800 个丢包/秒。
	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 640 个丢包/秒。
• 基本防火墙检查失败	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 1600 个丢包/秒。
• 数据包未通过应用检查	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 1280 个丢包/秒。
接口过载	在过去 600 秒内 2000 个丢包/秒。	在过去 20 秒内 8000 个丢包/秒。
	在过去 3600 秒内 1600 个丢包/秒。	在过去 120 秒内 6400 个丢包/秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。

使用指南

当您启用基本威胁检测后，ASA 会监控由于以下原因导致的丢包和安全事件速率：

- 被访问列表拒绝
- 不良数据包格式（例如 invalid-ip-header 或 invalid-tcp-hdr-length）
- 超出连接限制（系统范围资源限制和在配置中设置的限制）
- 检测到 DoS 攻击（例如无效 SPI，状态防火墙检查失败）
- 基本防火墙检查失败（此选项是包括此项目符号列表中所有防火墙相关丢包的组合速率。它不包括非防火墙相关丢包（例如接口过载、数据包未通过应用检查以及检测到扫描攻击。）
- 检测到可疑的 ICMP 数据包
- 数据包未通过应用检查
- 接口过载
- 检测到扫描攻击（此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。全面扫描威胁检测（请参阅 **threat-detection scanning-threat** 命令）采用此扫描攻击速率信息，然后通过例如将主机归类为攻击者并自动回避以采取相应措施。）
- 不完整会话检测，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击

当 ASA 检测到威胁时，它会立即发送系统日志消息 (733100) 并提醒 ASDM。

基本威胁检测仅当有丢包或潜在威胁时影响性能；即使在这种情况下，对性能的影响仍然可以忽略。

“默认值”部分中的表 1-1 列出了默认设置。您可以使用 **show running-config all threat-detection** 命令查看所有这些默认设置。您可通过使用 **threat-detection rate** 命令覆盖每种类型事件的默认设置。

如果超出事件速率，则 ASA 将发送系统消息。ASA 跟踪两种类型的速率：在某一间隔内的平均事件率，以及在较短突发间隔内的突发事件率。突发事件率为平均速率间隔的 1/30 或 10 秒，以较高者为准。对于收到的每个事件，ASA 将检查平均速率和突发速率限制；如果两种速率均超出，则 ASA 将发送两条单独的系统消息，最多允许每种速率类型在每个突发期间发送一条消息。

示例

以下示例启用基本威胁检测，然后更改 DoS 攻击的触发器：

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

相关命令

命令	描述
clear threat-detection rate	清除基本威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection rate	显示基本威胁检测统计信息。
threat-detection rate	设置每种事件类型的威胁检测速率限制。
threat-detection scanning-threat	启用扫描威胁检测。

threat-detection rate

使用 **threat-detection basic-threat** 命令启用基本威胁检测后，您可以在全局配置模式下使用 **threat-detection rate** 命令更改每种事件类型的默认速率限制。如果使用 **threat-detection scanning-threat** 命令启用扫描威胁检测，则采用 **scanning-threat** 关键字的此命令还会设置主机何时被视为攻击者或目标；否则，默认的 **scanning-threat** 值将用于基本和扫描威胁检测。要恢复默认设置，请使用此命令的 **no** 形式。

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*

语法说明

acl-drop	设置由于被访问列表拒绝导致丢包的速率限制。
average-rate *av_rate*	设置介于 0 到 2147483647 之间的平均速率限制，以丢包数/秒为单位。
bad-packet-drop	设置由于被不良数据包格式（例如 invalid-ip-header 或 invalid-tcp-hdr-length）拒绝导致丢包的速率限制。
burst-rate *burst_rate*	设置介于 0 到 2147483647 之间的突发速率限制，以丢包数/秒为单位。突发速率计算为每 *N* 秒的平均速率，其中 *N* 是突发速率间隔。突发速率间隔是 **rate-interval** *rate_interval* 值的 1/30 或 10 秒，以较大者为准。
conn-limit-drop	设置由于超出连接限制（系统范围资源限制和在配置中设置的限制）导致丢包的速率限制。
dos-drop	设置由于检测到 DoS 攻击（例如无效 SPI，状态防火墙检查失败）导致丢包的速率限制。
fw-drop	设置由于基本防火墙检查失败导致丢包的速率限制。此选项是包括此命令中所有防火墙相关丢包的组合速率。它不包括非防火墙相关丢包（例如 **interface-drop**、**inspect-drop** 和 **scanning-threat**）。
icmp-drop	设置由于检测到可疑 ICMP 数据包被拒绝导致丢包的速率限制。
inspect-drop	设置由于数据包未通过应用检查导致丢包的速率限制。
interface-drop	设置由于接口过载导致丢包的速率限制。
rate-interval *rate_interval*	将平均速率间隔设置为介于 600 秒到 2592000 秒（30 天）之间的值。速率间隔用于确定平均丢包数的时长。它还可确定突发阈值速率间隔。
scanning-threat	设置由于检测到扫描攻击导致丢包的速率限制。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。全面扫描威胁检测（请参阅 **threat-detection scanning-threat** 命令）采用此扫描攻击速率信息，然后通过将主机归类为攻击者并自动回避等方法，以便采取相应措施。
syn-attack	为不完整会话（例如，TCP SYN 攻击或无返回数据的 UDP 会话攻击）造成的丢包设置速率限制。

默认值

使用 **threat-detection basic-threat** 命令启用基本威胁检测后，请使用以下默认速率限制：

表 1-2　基本威胁检测默认设置

	触发器设置	
丢包原因	**平均速率**	**突发速率**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 400 个丢包/秒。
	在过去 3600 秒内 100 个丢包/秒。	在过去 120 秒内 400 个丢包/秒。
scanning-threat	在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
	在过去 3600 秒内 5 个丢包/秒。	在过去 120 秒内 10 个丢包/秒。
syn-attack	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 200 个丢包/秒。
	在过去 3600 秒内 100 个丢包/秒。	在过去 120 秒内 200 个丢包/秒。
acl-drop	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 800 个丢包/秒。
	在过去 3600 秒内 400 个丢包/秒。	在过去 120 秒内 800 个丢包/秒。
• **fw-drop** • **inspect-drop**	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 1600 个丢包/秒。
	在过去 3600 秒内 400 个丢包/秒。	在过去 120 秒内 1600 个丢包/秒。
interface-drop	在过去 600 秒内 2000 个丢包/秒。	在过去 20 秒内 8000 个丢包/秒。
	在过去 3600 秒内 2000 个丢包/秒。	在过去 120 秒内 8000 个丢包/秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。

使用指南

可以为每种事件类型配置最多三个不同的速率间隔。

当您启用基本威胁检测后，ASA 会监控由于“语法说明”表中所述事件类型导致的丢包率和安全事件：

当 ASA 检测到威胁时，它会立即发送系统日志消息 (733100) 并提醒 ASDM。

基本威胁检测仅当有丢包或潜在威胁时影响性能；即使在这种情况下，对性能的影响仍然可以忽略。

“默认值”部分中的表 1-1 列出了默认设置。您可以使用 **show running-config all threat-detection** 命令查看所有这些默认设置。

如果超出事件速率，则 ASA 将发送系统消息。ASA 跟踪两种类型的速率：在某一间隔内的平均事件率，以及在较短突发间隔内的突发事件率。对于收到的每个事件，ASA 将检查平均速率和突发速率限制；如果两种速率均超出，则 ASA 将发送两条单独的系统消息，最多允许每种速率类型在每个突发期间发送一条消息。

示例

以下示例启用基本威胁检测，然后更改 DoS 攻击的触发器：

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

相关命令

命令	描述
clear threat-detection rate	清除基本威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection rate	显示基本威胁检测统计信息。
threat-detection basic-threat	启用基本威胁检测。
threat-detection scanning-threat	启用扫描威胁检测。

threat-detection scanning-threat

要启用扫描威胁检测，请在全局配置模式下使用 **threat-detection scanning-threat** 命令。要禁用扫描威胁检测，请使用此命令的 **no** 形式。

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*]]

语法说明

duration *seconds*	设置回避攻击主机的持续时间，该值介于 10 到 2592000 秒之间。默认时长为 3600 秒（1 小时）。
except	无需回避的 IP 地址。多次输入此命令以标识无需回避的多个 IP 地址或网络对象组。
ip-address *ip_address mask*	指定无需回避的 IP 地址。
object-group *network_object_group_id*	指定无需回避的网络对象组。请参阅 **object-group network** 命令以创建对象组。
shun	当 ASA 将主机标识为攻击者时，除了发送系统日志消息 733101 以外，自动终止主机连接。

默认值

默认回避持续时间为 3600 秒（1 小时）。

以下默认速率限制用于扫描攻击事件：

表 1-3　　扫描威胁检测的默认速率限制

平均速率	突发速率
在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
在过去 3600 秒内 5 个丢包/秒。	在过去 120 秒内 10 个丢包/秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
8.0(4)	添加了 **duration** 关键字。

使用指南

典型的扫描攻击包含测试子网中每个 IP 地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。与基于流量签名的 IPS 扫描检测不同，ASA 扫描威胁检测功能维护包含可分析扫描活动的主机统计信息的广泛数据库。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机 IPID 等易受攻击的 TCP 行为以及更多行为）。

小心 扫描威胁检测功能可以显著影响 ASA 性能和内存，同时创建和收集基于主机和子网的数据结构和信息。

可以将 ASA 配置为发送关于攻击者的系统日志消息，也可以自动回避该主机。默认情况下，主机被标识为攻击者后，将生成系统日志消息 730101。

超出扫描威胁事件速率后，ASA 会标识攻击者和目标。ASA 跟踪两种类型的速率：在某一间隔内的平均事件率，以及在较短突发间隔内的突发事件率。对于被视为扫描攻击组成部分的检测到的每个事件，ASA 会检查平均和突发速率限制。如果从主机发送的流量超出任一速率，则该主机被视为攻击者。如果主机接收的流量超出任一速率，则该主机被视为目标。您可以使用 **threat-detection rate scanning-threat** 命令更改扫描威胁事件的速率限制。

要查看归类为攻击者或目标的主机，请使用 **show threat-detection scanning-threat** 命令。

要查看回避的主机，请使用 **show threat-detection shun** 命令。要释放回避的主机，请使用 **clear threat-detection shun** 命令。

示例

以下示例启用扫描威胁检测并自动回避归类为攻击者的主机，位于 10.1.1.0 网络上的主机除外。扫描威胁检测的默认速率限制也将更改。

```
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
```

相关命令

命令	描述
clear threat-detection shun	释放回避的主机。
show threat-detection scanning-threat	显示归类为攻击者和目标的主机。
show threat-detection shun	显示当前回避的主机。
threat-detection basic-threat	启用基本威胁检测。
threat-detection rate	设置每种事件类型的威胁检测速率限制。

threat-detection statistics

要启用高级威胁检测统计信息，请在全局配置模式下使用 **threat-detection statistics** 命令。要禁用高级威胁检测统计信息，请使用此命令的 **no** 形式。

小心 启用统计信息可能会影响 ASA 性能，具体取决于所启用统计信息的类型。**threat-detection statistics host** 命令会显著影响性能；如果您有高流量负载，可考虑临时启用此类型的统计信息。不过，**threat-detection statistics port** 命令的影响有限。

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*]]

语法说明

access-list	（可选）启用访问列表拒绝的统计信息。访问列表统计信息仅当使用 **show threat-detection top access-list** 命令时显示。
average-rate *attacks_per_sec*	（可选）对于 TCP 拦截，设置系统日志消息生成的平均速率阈值，该值介于 25 到 2147483647 之间。默认值为每秒 200 条消息。超出平均速率时，将生成系统日志消息 733105。
burst-rate *attacks_per_sec*	（可选）对于 TCP 拦截，设置系统日志消息生成的阈值，该值介于 25 到 2147483647 之间。默认值为每秒 400 条消息。超出突发速率时，将生成系统日志消息 733104。
host	（可选）启用主机统计信息。只要主机处于活动状态并且位于扫描威胁主机数据库中，即可累积主机统计信息。处于非活动状态 10 分钟后，将从数据库中删除主机（并清除统计信息）。
number-of-rate {**1** | **2** | **3**}	（可选）设置为主机、端口或协议统计信息维护的速率间隔数。默认速率间隔数为 **1**，该值将保持较低的内存利用率。要查看更多速率间隔，请将该值设置为 **2** 或 **3**。例如，如果将该值设置为 **3**，则查看过去 1 小时、8 小时和 24 小时的数据。如果将此关键字设置为 **1**（默认值），则仅维护最短速率间隔的统计信息。如果将该值设置为 **2**，则维护最短的两个间隔。
port	（可选）启用端口统计信息。
protocol	（可选）启用协议统计信息。
rate-interval *minutes*	（可选）对于 TCP 拦截，设置历史记录监控时段的大小，该值介于 1 到 1440 分钟之间。默认值为 30 分钟。在此间隔期间，ASA 会采样攻击数量 30 次。
tcp-intercept	（可选）启用 TCP 拦截所拦截攻击的统计信息。请参阅 **set connection embryonic-conn-max** 命令，或者 **nat** 或 **static** 命令，以启用 TCP 拦截。

默认值

默认情况下，访问列表统计信息已启用。如果没有在此命令中指定任何选项，则启用所有选项。

默认 **tcp-intercept rate-interval** 为 30 分钟。默认 **burst-rate** 为每秒 400 次。默认 **average-rate** 为每秒 200 次。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
8.0(4)/8.1(2)	添加了 **tcp-intercept** 关键字。
8.1(2)	添加了 **number-of-rates** 关键字用于主机统计信息，并且默认速率数从 3 更改为 1。
8.2(1)	突发速率间隔从平均速率的 1/60 更改为 1/30。
8.3(1)	添加了 **number-of-rates** 关键字用于端口和协议统计信息，并且默认速率数从 3 更改为 1。

使用指南

如果没有在此命令中指定任何选项，则启用所有统计信息。要仅启用某些统计信息，请对此命令输入每种统计信息类型，不要同时输入不带任何选项的该命令。可以输入 **threat-detection statistics**（不带任何选项），然后通过输入具有统计信息特定选项（例如，**threat-detection statistics host number-of-rate 2**）的命令自定义某些统计信息。如果输入 **threat-detection statistics**（不带任何选项），然后输入特定统计信息的命令，但不带任何统计信息特定选项，则该命令没有任何影响，因为命令已启用。

如果输入此命令的 **no** 形式，它会删除所有 **threat-detection statistics** 命令，包括默认情况下已启用的 **threat-detection statistics access-list** 命令。

使用 **show threat-detection statistics** 命令查看统计信息。

您无需使用 **threat-detection scanning-threat** 命令启用扫描威胁检测；您可以单独配置检测和统计信息。

示例

以下示例启用除主机以外所有类型的扫描威胁检测和扫描威胁统计信息：

```
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
```

相关命令

命令	描述
threat-detection scanning-threat	启用扫描威胁检测。
show threat-detection statistics host	显示主机统计信息。
show threat-detection memory	显示用于高级威胁检测统计信息的内存。
show threat-detection statistics port	显示端口统计信息。

命令	描述
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。

threshold

要为 SLA 监控操作中的超出阈值事件设置阈值，请在 SLA 监控配置模式下使用 **threshold** 命令。要恢复默认值，请使用此命令的 **no** 形式。

threshold *milliseconds*

no threshold

语法说明

milliseconds	指定要声明的上升阀值的毫秒数。有效值为 0 至 2147483647。该值不应大于为超时设置的值。

默认值

默认阈值为 5000 毫秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
SLA 监控配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

阈值仅用于指示超出阈值事件，这不会影响可达性，但可用于评估 **timeout** 命令是否正确设置。

示例

以下示例配置 ID 为 123 的 SLA 操作并创建 ID 为 1 的跟踪条目以跟踪 SLA 的可达性。SLA 操作频率设置为 10 秒，阈值设置为 2500 毫秒而超时值设置为 4000 毫秒。

```
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
```

相关命令

命令	描述
sla monitor	定义 SLA 监控操作。
timeout	定义 SLA 操作等待响应的时间量。

throughput level

要设置智能许可授权请求的吞吐量级别，请在许可证智能配置模式下使用 **throughput level** 命令。要删除吞吐量级别和取消许可您的设备，请使用此命令的 **no** 形式。

注 此功能仅适用于 ASAv。

throughput level {100M | 1G | 2G}

no throughput level [100M | 1G | 2G]

语法说明

100M	将吞吐量级别设置为 100 Mbps。
1G	将吞吐量级别设置为 1 Gbps。
2G	将吞吐量级别设置为 2 Gbps。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
许可证智能配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
9.3(2)	添加了此命令。

使用指南

当您请求或更改吞吐量级别时，必须先退出许可证智能配置模式，更改才能生效。

示例

以下示例将功能级别设置为“标准”，并将吞吐量级别设置为 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)#
```

相关命令

命令	描述
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clear configure license	清除智能许可配置。
feature tier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
license smart	让您为智能许可请求许可证授权。
license smart deregister	从许可证颁发机构注销设备。
license smart register	向许可证颁发机构注册设备。
license smart renew	续订注册或许可证授权。
service call-home	启用 Smart Call Home。
show license	显示智能许可状态。
show running-config license	显示智能许可配置。

ticket（已弃用）

要配置思科公司间媒体引擎代理的票证纪元和密码，请在 UC-IME 配置模式下使用 **ticket** 命令。要从代理中删除配置，请使用此命令的 **no** 形式。

ticket epoch *n* **password** *password*

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

语法说明

n	指定两次密码完整性检查之间的时长。请输入 1-255 的整数。
password	设置思科公司间媒体引擎票证的密码。输入至少 10 个、最多 64 个来自 US-ASCII 字符集的可打印字符。允许使用的字符包括 0x21 到 0x73（包含边界），不包含空格字符。 一次只能配置一个密码。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
UC-IME 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.3(1)	添加了此命令。
9.4(1)	此命令以及所有 **uc-ime** 模式命令均已弃用。

使用指南

配置思科公司间媒体引擎的票证纪元和密码。

纪元包含一个整数，在每次更改密码时更新。初次配置代理和初次输入密码时，输入 1 用于纪元整数。每次更改密码时，增加纪元以指示新密码。您必须在每次更改密码时递增纪元值。

通常，您可以按顺序递增纪元；但 ASA 允许您在更新纪元时选择任意值。

如果您更改纪元值，则当前密码失效，并且您必须输入新密码。

我们建议密码至少为 20 个字符。一次只能配置一个密码。

票证密码存储在闪存中。**show running-config uc-ime** 命令的输出显示 ***** 而不是密码字符串。

注 您在 ASA 中配置的纪元和密码必须匹配思科公司间媒体引擎服务器上配置的纪元和密码。有关信息，请参阅思科公司间媒体引擎服务器文档。

示例

以下示例展示在思科公司间媒体引擎代理中指定票证和纪元：

```
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
```

相关命令

命令	描述
show running-config uc-ime	显示思科公司间媒体引擎代理的运行中配置。
uc-ime	在 ASA 上创建思科公司间媒体引擎代理实例。

timeout (aaa-server host)

要配置与 AAA 服务器建立连接时放弃之前允许的主机特定最长响应时间（以秒为单位），请在 aaa-server 主机模式下使用 **timeout** 命令。要删除超时值并将超时重置为默认值 10 秒，请使用此命令的 **no** 形式。

timeout *seconds*

no timeout

语法说明

seconds	指定请求的超时间隔（1-60 秒）。这是 ASA 放弃对主要 AAA 服务器的请求之前经过的时间。如果有备用 AAA 服务器，则 ASA 会将请求发送到备用服务器。

默认值

默认超时值为 10 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
aaa-server 主机配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令对所有 AAA 服务器协议类型均有效。

使用 **timeout** 命令指定的时间长度 ASA 尝试与 AAA 服务器进行连接。使用 **retry-interval** 命令指定 ASA 在两次连接尝试之间等待的时间量。

超时是 ASA 尝试完成与服务器的事务时花费的总时间量。重试间隔确定超时时段内通信重试的频率。因此，如果重试间隔大于或等于超时值，您将不会看到重试。如果要查看重试，重试间隔必须小于超时值。

示例

以下示例在主机 1.2.3.4 上将名为“svrgrp1”的 RADIUS AAA 服务器配置为使用超时值 30 秒，重试间隔 10 秒。因此，ASA 在 30 秒之后放弃前会尝试通信尝试三次。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 30
ciscoasa(config-aaa-server-host)# retry-interval 10
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	描述
aaa-server host	进入 aaa server 主机配置模式，以便能够配置主机特定的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa	显示当前 AAA 配置值。

timeout (dns server-group)

要指定尝试下一个 DNS 服务器之前等待的时间量，请在 dns-server-group 配置模式下使用 **timeout** 命令。要恢复默认超时，请使用此命令的 **no** 形式。

timeout *seconds*

no timeout [*seconds*]

语法说明

seconds	指定介于 1 到 30 之间的超时（以秒为单位）。默认值为 2 秒。每次 ASA 重试服务器列表，此超时将加倍。在 dns-server-group 配置模式下使用 **retries** 命令以配置重试次数。

默认值

默认的超时时间为 2 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
DNS 服务器组配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

示例

以下示例将 DNS 服务器组“dnsgroup1”的超时设置为 1 秒：

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

相关命令

命令	描述
clear configure dns	删除所有用户创建的 DNS 服务器组并将默认服务器组的属性重置为默认值。
domain-name	设置默认域名。
retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
show running-config dns server-group	显示当前运行的 DNS 服务器组配置。

timeout (global)

要设置各项功能的全局最长空闲时间的持续时间，请在全局配置模式下使用 **timeout** 命令。要将所有超时设置为默认值，请使用此命令的 **no** 形式。要将一项功能重置为其默认值，请重新输入 **timeout** 命令及默认值。

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

语法说明

absolute	（对于 **uauth** 可选）需要在 uauth 超时过期后重新验证。默认情况下，**absolute** 关键字已启用。要将 uauth 计时器设置为在经过非活动时段后超时，请输入 **inactivity** 关键字代替。
conn	指定连接关闭之前经过的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 1 小时 (1:0:0)。使用 **0** 表示连接永不超时。
conn-holddown	系统应在该连接使用的路由不再存在或处于非活动状态时维持连接的时间长度。如果在此等待期间内路由未处于活动状态，系统将释放该连接。配置连接等待计时器的目的是为了降低路由摆动的影响，其中路由可能会快速显示和断开。您可以减小等待计时器，以便更快地进行路由融合。默认值为 15 秒，范围介于 00:00:00 到 00:00:15 秒之间。
floating-conn	当多个路由共存于一个具有不同性能的网络时，ASA 在创建连接时使用性能最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。
hh:*mm*:*ss*	以小时、分钟和秒钟为单位指定超时。如果可用，使用 **0** 表示连接永不超时。
h225	指定 H.225 信令连接关闭之前经过的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 1 小时 (1:0:0)。超时值 0:0:1 会在清除所有呼叫后立即禁用计时器并关闭 TCP 连接。
h323	指定 H.245 (TCP) 和 H.323 (UDP) 媒体连接关闭之前经过的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323（RTP 和 RTCP）媒体连接共享空闲超时。
half-closed	指定释放 TCP 半关闭连接之前经过的空闲时间，该值介于 0:5:0（适用于 9.1(1) 及更早版本）或 0:0:30（适用于 9.1(2) 及更高版本）到 1193:0:0 之间。默认值为 10 分钟 (0:10:0)。使用 **0** 表示连接永不超时。
icmp	指定 ICMP 的空闲时间，该值介于 0:0:2 到 1193:0:0 之间。默认值为 2 秒 (0:0:2)。
icmp-error	指定 ASA 在收到 ICMP 回应应答数据包后删除 ICMP 连接之前的空闲时间，该值介于 0:0:0 到 0:1:0 之间；或者为 **timeout icmp** 值，以较低者为准。默认为 **0**（禁用）。如果禁用此超时并启用 ICMP 检测，ASA 将在收到回应应答后立即删除 ICMP 连接；因此，针对该（现已关闭）连接生成的任何 ICMP 错误都将被丢弃。此超时可以延迟删除 ICMP 连接，使您能够接收重要的 ICMP 错误。

igp stale-route	指定闲置时间，也就是将过时的路由从路由器信息库中删除前将它保存多长时间。这些路由供内部网关协议（例如 OSPF）使用。默认值为 70 秒 (00:01:10)，范围介于 00:00:10 到 00:01:40 之间。
inactivity	（对于 **uauth** 可选）需要在非活动超时过期后重新验证 uauth。
mgcp	设置删除 MGCP 媒体连接之前经过的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)
mgcp-pat	设置删除 MGCP PAT 转换之前经过的绝对间隔，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。
pat-xlate	指定释放 PAT 转换插槽之前经过的空闲时间，该值介于 0:0:30 到 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。
sctp	指定流控制传输协议 (SCTP) 连接关闭之前允许的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。
sip	指定 SIP 控制连接关闭之前经过的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 30 分钟 (0:30:0)。使用 **0** 表示连接永不超时。
sip-disconnect	指定 CANCEL 或 BYE 消息未收到 200 OK 时，删除 SIP 会话之前经过的空闲时间，该值介于 0:0:1 到 00:10:0 之间。默认值为 2 分钟 (0:2:0)。
sip-invite	（可选）指定 PROVISIONAL 响应和媒体 xlate 的针孔关闭之前经过的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 3 分钟 (0:3:0)。
sip_media	指定 SIP 媒体连接关闭之前经过的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。使用 **0** 表示连接永不超时。 SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
sip-provisional-media	指定 SIP 临时媒体连接的超时值，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。
sunrpc	指定 SUNRPC 插槽关闭之前经过的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 10 分钟 (0:10:0)。使用 **0** 表示连接永不超时。
tcp-proxy-reassembly	配置丢弃等待重组的缓冲数据包之前经过的空闲超时，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
uauth	指定身份验证和授权缓存超时并且用户必须重新验证下一连接之前经过的持续时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。默认计时器为 **absolute**；可以通过输入 **inactivity** 关键字将超时设置为经过非活动时段后发生。**uauth** 持续时间必须比 **xlate** 持续时间短。设置为 **0** 表示禁用缓存。如果连接使用被动 FTP 或使用 **virtual http** 命令进行网络身份验证，请勿使用 **0**。
udp	指定释放 UDP 插槽之前经过的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。使用 **0** 表示连接永不超时。
xlate	指定释放转换插槽之前经过的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 3 小时 (3:0:0)。

默认值

默认值如下：

- **conn** 为 1 小时 (**1:0:0**)。
- **conn-holddown** 为 15 秒 (**0:0:15**) 。
- **floating-conn** 永不超时 (**0**)。

- **h225** 为 1 小时 (**1:0:0**)。
- **h323** 为 5 分钟 (**0:5:0**)。
- **half-closed** 为 10 分钟 (**0:10:0**)。
- **icmp** 为 2 秒 (**0:0:2**)。
- **icmp-error** 永不超时 (**0**)。
- **igp stale-route** 为 70 秒 (**00:01:10**)。
- **mgcp** 为 5 分钟 (**0:5:0**)。
- **mgcp-pat** 为 5 分钟 (**0:5:0**)。
- **rpc** 为 5 分钟 (**0:5:0**)。
- **sctp** 为 2 分钟 (**0:2:0**)。
- **sip** 为 30 分钟 (**0:30:0**)。
- **sip-disconnect** 为 2 分钟 (**0:2:0**)。
- **sip-invite** 为 3 分钟 (**0:3:0**)。
- **sip_media** 为 2 分钟 (**0:2:0**)。
- **sip-provisional-media** 为 2 分钟 (**0:2:0**)。
- **sunrpc** 为 10 分钟 (**0:10:0**)。
- **tcp-proxy-reassembly** 为 1 分钟 (**0:1:0**)。
- **uauth** 为 5 分钟 (**0:5:0**) **绝对值**。
- **udp** 为 2 分钟 (**0:02:0**)。
- **xlate** 为 3 小时 (**3:0:0**)。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置模式	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	已添加 **mgcp-pat**、**sip-disconnect** 和 **sip-invite** 关键字。
7.2(4)/8.0(4)	添加了 **sip-provisional-media** 关键字。
7.2(5)/8.0(5)/8.1(2)/8.2(1)	添加了 **tcp-proxy-reassembly** 关键字。
8.2(5)/8.4(2)	添加了 **floating-conn** 关键字。
8.4(3)	添加了 **pat-xlate** 关键字。
9.1(2)	**half-closed** 最小值已降至 30 秒 (0:0:30)。
9.4(3)/9.6(2)	已添加 **conn-holddown** 关键字。
9.5(2)	已添加 **sctp** 关键字。

版本	修改
9.7(1)	已添加 **igp stale-route** 关键字。
9.8(1)	已添加 **icmp-error** 关键字。

使用指南

timeout 命令可让您设置全局超时。对于某些功能，**set connection timeout** 命令优先使用该命令中标识的流量。

您可以在 **timeout** 命令后输入多个关键字和值。

连接计时器 (**conn**) 优先于转换计时器 (**xlate**)；转换计时器仅当所有连接均已超时后有效。

示例

以下示例展示如何配置最长空闲时间的持续时间：

```
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
```

相关命令

命令	描述
clear configure timeout	清除超时配置并将其重置为默认值。
set connection timeout	使用模块化策略框架设置连接超时。
show running-config timeout	显示指定协议的超时值。

timeout (policy-map type inspect gtp > parameters)

要更改 GTP 会话的非活动计时器，请在参数配置模式下使用 **timeout** 命令。您可以通过先输入 **policy-map type inspect gtp** 命令来访问参数配置模式。使用此命令的 **no** 形式将这些间隔设置为其默认值。

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*

语法说明

hh:*mm*:*ss*	指定服务的空闲超时（以“小时:分钟:秒”格式）。如果不想设置超时，请指定数字 0。
endpoint	删除 GTP 终端之前允许处于非活动状态的最长时间。
gsn	删除 GSN 之前允许处于非活动状态的最长时间。 从 9.5(1) 开始，此关键字已移除，且替换为 **endpoint** 关键字。
pdp-context	删除 GTP 会话的 PDP 情景前允许处于非活动状态的最长时间。在 GTPv2 中，这属于承载情景。
request	从请求队列中删除某个请求之前允许处于非活动状态的最长时间。对丢弃请求的任何后续响应也将被丢弃。
signaling	删除 GTP 信令之前允许处于非活动状态的最长时间。
t3-response	删除连接前等待响应的最长时间。
tunnel	终止 GTP 隧道之前允许处于非活动状态的最长时间。

默认值

endpoint、**gsn**、**pdp-context** 和 **signaling** 的默认值为 30 分钟。

request 的默认值为 1 分钟。

tunnel 的默认值为 1 小时（如果没有收到删除 PDP 情景请求）。

t3-response 的默认值为 20 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.5(1)	**gsn** 关键字已替换为 **endpoint**。

使用指南

使用此命令更改 GTP 检测中所用的默认超时。

示例

以下示例将请求队列的超时值设置为 2 分钟：

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

相关命令

命令	描述
clear service-policy inspect gtp	将清除全局 GTP 统计数据。
inspect gtp	适用于特定的 GTP 映射，以用于应用检查。
show service-policy inspect gtp	显示 GTP 配置。

timeout (policy-map type inspect m3ua > parameters)

要更改 M3UA 会话的非活动计时器，请在参数配置模式使用 **timeout** 命令。您可以通过先输入 **policy-map type inspect m3ua** 命令来访问参数配置模式。使用此命令的 **no** 形式将这些间隔设置为其默认值。

timeout {**endpoint** | **session**} *hh*:*mm*:*ss*

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

语法说明

hh:*mm*:*ss*	指定服务的空闲超时（以“小时:分钟:秒”格式）。如果不想设置超时，请指定数字 0。
endpoint	删除 M3UA 终端统计信息之前允许处于非活动状态的最长时间。默认值为 30 分钟。
session	如果启用严格 ASP 状态验证，则表示删除 M3UA 会话之前的空闲超时，该值的格式为 hh:mm:ss。默认值为 30 分钟 (00:30:00)。禁用此超时可防止系统删除过时的会话。

默认值

endpoint 和 **session** 的默认值为 30 分钟。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.6(2)	添加了此命令。
9.7(1)	已添加了 **session** 关键字。

使用指南

使用此命令更改在 M3UA 检测中使用的默认超时。

示例

以下示例为终端设置 45 分钟的超时。

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

相关命令

命令	描述
inspect m3ua	启用 M3UA 检测。
policy-map type inspect	创建检查策略映射。
show service-policy inspect m3ua	显示 M3UA 统计信息。
strict-asp-state	启用严格 M3UA ASP 状态验证。

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

要更改 RADIUS 记帐用户的非活动计时器，请在参数配置模式下使用 **timeout** 命令。您可以通过先输入 **policy-map type inspect radius-accounting** 命令来访问参数配置模式。使用此命令的 **no** 形式将这些间隔设置为其默认值。

timeout users *hh*:*mm*:*ss*

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

语法说明

hh:*mm*:*ss*	此项为超时，其中 *hh* 指定小时，*mm* 指定分钟，*ss* 指定秒钟，而冒号 (:) 分隔这三个组成部分。值 0 表示永不立即关闭。默认值为一小时。
users	指定用户的超时。

默认值

用户的默认超时为一小时。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例将用户的超时值设置为 10 分钟：

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

相关命令

命令	描述
inspect radius-accounting	设置 RADIUS 记账的检查。
parameters	设置检查策略映射的参数。

timeout (type echo)

要设置 SLA 操作等待请求数据包响应的时间量，请在 type echo 配置模式下使用 **timeout** 命令。您可以通过首先输入 **sla monitor** 命令来访问 type echo 配置模式。要恢复默认值，请使用此命令的 **no** 形式。

timeout *milliseconds*

no timeout

语法说明

毫秒	0 到 604800000。

默认值

默认超时值为 5000 毫秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Type echo 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

使用 **frequency** 命令设置 SLA 操作发出请求数据包的频率，使用 **timeout** 命令设置 SLA 操作等待接收这些请求响应的时长。为 **timeout** 命令指定的值不能大于为 **frequency** 命令指定的值。

示例

以下示例配置 ID 为 123 的 SLA 操作并创建 ID 为 1 的跟踪条目以跟踪 SLA 的可达性。SLA 操作频率设置为 10 秒，阈值设置为 2500 毫秒而超时值设置为 4000 毫秒。

```
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
```

相关命令

命令	描述
frequency	指定 SLA 操作重复的速率。
sla monitor	定义 SLA 监控操作。

timeout assertion

要配置 SAML 超时，请在 webvpn 配置模式下使用 **timeout assertion** 命令：

timeout assertion *number of seconds*

语法说明

number of seconds	SAML IdP 超时（以秒为单位）。

默认值

默认值为 none，这意味着断言中的 NotBefore 和 NotOnOrAfter 确定有效性。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
config webVPN	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.5.2	添加了此命令。

使用指南

如果指定，则在 NotBefore 和超时秒数之和早于 NotOnOrAfter 的情况下，此配置会覆盖 NotOnOrAfter。如果不指定，则断言中的 NotBefore 和 NotOnOrAfter 用于确定有效性。在 config-webvpn-saml-idp 下面输入超时值时，断言和秒数值均为必填。

示例

以下示例配置基于无客户端 VPN 的 URL、SAML 请求签名和 SAML 断言超时：

```
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 pinhole

要配置 DCERPC 针孔的超时并覆盖两分钟的全局系统针孔超时，请在参数配置模式下使用 **timeout pinhole** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

timeout pinhole *hh:mm:ss*

no timeout pinhole

语法说明

hh:mm:ss	针孔连接的超时。该值介于 0:0:1 到 1193:0:0 之间。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例展示如何在 DCERPC 检查策略映射中配置针孔连接的针孔超时：

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

相关命令

命令	描述
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

timeout secure-phones（已弃用）

要配置从电话代理数据库删除 secure-phone 条目之前经过的空闲超时，请在 phone-proxy 配置模式下使用 **timeout secure-phones** 命令。要将超时值恢复为默认值 5 分钟，请使用此命令的 **no** 形式。

timeout secure-phones *hh:mm:ss*

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

语法说明

hh:mm:ss	指定删除对象之前经过的空闲超时。默认值为 5 分钟。

默认值

安全电话超时的默认值为 5 分钟。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(4)	添加了此命令。
9.4(1)	此命令以及所有 **phone-proxy** 模式命令均已弃用。

使用指南

由于安全电话始终在启动时请求 CTL 文件，因此电话代理会创建将电话标记为安全的数据库。安全电话数据库中的条目在经过指定的配置超时后将被删除（通过 **timeout secure-phones** 命令）。条目的时间戳在每次注册时更新以刷新 SIP 电话接收的电话代理和 SCCP 电话的 Keepalive。

timeout secure-phones 命令的默认值为 5 分钟。指定大于 SCCP Keepalive 和 SIP 注册刷新最大超时值的值。例如，如果 SCCP Keepalive 配置为 1 分钟的间隔，而 SIP 注册刷新配置为 3 分钟，请将此超时值配置为大于 3 分钟。

示例

以下示例展示使用 **timeout secure-phones** 命令在 3 分钟后将电话代理配置为安全电话数据库中的超时条目：

```
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
```

相关命令

命令	描述
phone-proxy	配置电话代理实例。

time-range

要进入 time-range 配置模式并定义可附加到流量规则或操作的时间范围，请在全局配置模式下使用 **time-range** 命令。要禁用，请使用此命令的 **no** 形式。

time-range *name*

no time-range *name*

语法说明

name	时间范围的名称。名称不得超过 64 个字符。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

创建时间范围并不会限制对设备的访问。**time-range** 命令仅定义时间范围。定义时间范围之后，您可以将其附加到流量规则或操作。

要实施基于时间的 ACL，请使用 **time-range** 命令定义某日和周的特定时间。然后，使用 **access-list extended time-range** 命令将时间范围与 ACL 绑定。

时间范围依赖于 ASA 的系统时钟；但是，该功能与 NTP 同步配合使用效果最佳。

示例

以下示例创建一个名为“New_York_Minute”的时间范围，然后进入 time range 配置模式：

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

创建时间范围并进入 time-range 配置模式后，您可以使用 **absolute** 和 **periodic** 命令定义时间范围参数。要恢复 **time-range** 命令 **absolute** 和 **periodic** 关键字的默认设置，请在 time-range 配置模式下使用 **default** 命令。

要实施基于时间的 ACL，请使用 **time-range** 命令定义某日和周的特定时间。然后，使用 **access-list extended** 命令将时间范围与 ACL 绑定。以下示例将名为“Sales”的 ACL 与名为“New_York_Minute”的时间范围绑定：

```
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)#
```

有关 ACL 的详细信息，请参阅 **access-list extended** 命令。

相关命令

命令	描述
absolute	定义时间范围生效时的绝对时间。
access-list extended	配置允许或拒绝 IP 流量通过 ASA 的策略。
default	恢复 **time-range** 命令 **absolute** 和 **periodic** 关键字的默认设置。
periodic	指定支持 time-range 功能的各功能的重复（每周）时间范围。

timers bgp

要调整 BGP 网络计时器，请在路由器 bgp 配置模式下使用 **timers bgp** 命令。要重置 BGP 计时默认值，请使用此命令的 **no** 形式。

timers bgp *keepalive holdtime* [*min-holdtime*]

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

语法说明

keepalive	思科 IOS 软件将 *keepalive* 消息发送到其对等设备的频率（以秒为单位）。默认值为 60 秒。范围是从 0 到 65535。
holdtime	时间间隔（以秒为单位），若经过该时间后未收到 *keepalive* 消息，软件声明对等设备失效。默认值为 180 秒。范围是从 0 到 65535。
min-holdtime	（可选）指定来自 BGP 邻居的最短可接受保持时间的时间间隔（以秒为单位）。最短可接受保持时间必须小于或等于在 *holdtime* 参数中指定的时间间隔。范围是从 0 到 65535。

默认值

keepalive：60 秒
holdtime：180 秒

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
路由器 bgp 配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
9.2(1)	添加了此命令。

使用指南

当 *holdtime* 参数配置的值小于 20 秒时，将显示以下警告：A hold time of less than 20 seconds increases the chances of peer flapping（保持时间小于 20 秒会增加对等设备摆动的几率）

如果最短可接受保持时间的时间间隔大于指定的保持时间，将显示一条通知：Minimum acceptable hold time should be less than or equal to the configured hold time（最短可接受保持时间应小于或等于配置的保持时间）

注 如果在 BGP 路由器上配置最短可接受保持时间，则仅当远程对等设备通告的保持时间等于或大于最短可接受保持时间的时间间隔时，才建立远程 BGP 对等会话。如果最短可接受保持时间的时间间隔大于配置的保持时间，则下次尝试建立远程会话将失败，并且本地路由器将发送通知表明“不可接受的保持时间”。

示例

以下示例将 keepalive 计时器更改为 70 秒、hold-time 计时器更改为 130 秒，并将最短可接受保持时间的时间间隔更改为 100 秒：

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

timers lsa arrival

要设置 ASA 接受来自 OSPFv3 邻居的相同 LSA 的最短间隔，请在 IPv6 路由器配置模式下使用 **timers lsa arrival** 命令。要恢复默认值，请使用此命令的 **no** 形式。

timers lsa arrival *milliseconds*

no timers lsa arrival *milliseconds*

语法说明

milliseconds	指定两次接受到达邻居之间相同 LSA 必须经过的最短延迟（以毫秒为单位）。有效值为 0 到 600,000 毫秒。

默认值

默认值为 1000 毫秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
IPv6 路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令指示两次接受从邻居到达的相同 LSA 必须经过的最短间隔。

示例

以下示例将接受相同 LSA 的最短间隔设置为 2000 毫秒：

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

相关命令

命令	描述
ipv6 router ospf	OSPFv3 进入路由器配置模式。
show ipv6 ospf	显示关于 OSPFv3 路由过程的一般信息。
timers pacing flood	配置 OSPFv3 路由过程的 LSA 泛洪数据包定步。

timers lsa-group-pacing

要指定将 OSPF 链路状态通告 (LSA) 收集到组中以及刷新、验证校验和或老化的间隔，请在路由器配置模式下使用 **timers lsa-group-pacing** 命令。要恢复默认值，请使用此命令的 **no** 形式。

timers lsa-group-pacing *seconds*

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

语法说明

seconds	将 OSPF 链路状态通告 (LSA) 收集到组中以及刷新、验证校验和或老化的间隔。有效值范围为 10 到 1800 秒。

默认值

默认间隔为 240 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

要更改将 OSPF 链路状态通告 (LSA) 收集到组中以及刷新、验证校验和或老化的间隔，请使用 **timers lsa-group-pacing** *seconds* 命令。要恢复计时器默认值，请使用 **no timers lsa-group-pacing** 命令。

示例

以下示例将 LSA 的组处理间隔设置为 500 秒：

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

相关命令

命令	描述
router ospf	进入路由器配置模式。
show ospf	显示关于 OSPF 路由过程的一般信息。
timers spf	指定最短路径优先 (SPF) 计算延迟和保持时间

timers pacing flood

要配置 LSA 泛洪数据包定步，请在 IPv6 路由器配置模式下使用 **timers pacing flood** 命令。要恢复默认泛洪数据包定步值，请使用此命令的 **no** 形式。

timers pacing flood *milliseconds*

no timers pacing flood *milliseconds*

语法说明

milliseconds	指定泛洪队列中的 LSA 在两次更新之间定步的时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。

默认值

默认值为 33 毫秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
IPv6 路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令以配置 LSA 泛洪数据包定步。

示例

以下示例将 LSA 泛洪数据包定步更新配置为以 20 毫秒的间隔对 OSPFv3 进行：

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

相关命令

命令	描述
ipv6 router ospf	进入 IPv6 路由器配置模式。
timers pacing lsa-group	指定将 OSPFv3 LSA 收集到组中以及刷新、验证校验和或老化的间隔。

timers pacing lsa-group

要指定将 OSPFv3 LSA 收集到组中以及刷新、验证校验和或老化的间隔，请在 IPv6 路由器配置模式下使用 **timers pacing lsa-group** 命令。要恢复默认值，请使用此命令的 **no** 形式。

timers pacing lsa-group *seconds*

no timers pacing lsa-group [*seconds*]

语法说明

seconds	指定将 LSA 收集到组中以及刷新、验证校验和或老化的间隔秒数。有效值范围为 10 到 1800 秒。

默认值

默认间隔为 240 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
IPv6 路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令指示将 OSPFv3 LSA 收集到组中以及刷新、验证校验和或老化的间隔。

示例

以下示例将 LSA 组之间的 OSPFv3 组数据包定步更新配置为以 300 秒的间隔对 OSPFv3 路由过程 1 进行：

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

相关命令

命令	描述
ipv6 router ospf	进入 IPv6 路由器配置模式。
show ipv6 ospf	显示关于 OSPFv3 路由过程的一般信息。
timers pacing flood	配置 OSPFv3 路由过程的 LSA 泛洪数据包定步。
timers pacing retransmission	配置 LSA 重新传输数据包定步。

timers pacing retransmission

要配置链路状态通告 (LSA) 重新传输数据包定步，请在路由器配置模式下使用 **timers pacing retransmission** 命令。要恢复默认重新传输数据包定步值，请使用此命令的 **no** 形式。

timers pacing retransmission *milliseconds*

no timers pacing retransmission

语法说明

milliseconds	指定重新传输队列中的 LSA 定步的时间间隔（以毫秒为单位）。有效值为 5 毫秒到 200 毫秒。

默认值

默认间隔为 66 毫秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
IPv6 路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.2(1)	添加了此命令。

使用指南

配置开放最短路径优先 (OSPF) 重新传输定步计时器，以便控制 OSPF 重新传输队列中后续链路状态更新数据包之间的数据包间间隔。此命令可用于控制进行 LSA 更新的速率，以便区域泛洪大量 LSA 时能够降低可能出现的高 CPU 或缓冲区利用率。OSPF 数据包重新传输定步计时器的默认设置适合大多数 OSPF 部署。

注 除非满足 OSPF 数据包泛洪要求的所有其他选项均已用尽，否则请勿更改数据包重新传输定步计时器。具体而言，网络运营商应首选使用汇总、末节区域使用、队列调整和缓冲区调整，然后再更改默认泛洪计时器。

此外，更改计时器值没有任何指导；每个 OSPF 部署都是唯一的，因此应依据个案而定。网络运营商应承担与更改默认数据包重新传输定步计时器值有关的风险。

示例

以下示例将 LSA 泛洪定步更新配置为以 55 毫秒的间隔对 OSPF 路由过程 1 进行：

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

相关命令

命令	描述
ipv6 router ospf	进入 IPv6 路由器配置模式。
show ipv6 ospf	显示关于 OSPFv3 路由过程的一般信息。
timers pacing flood	配置 OSPFv3 路由过程的 LSA 泛洪数据包定步。

timers spf

要指定最短路径优先 (SPF) 计算延迟和保持时间，请在路由器配置模式下使用 **timers spf** 命令。要恢复默认值，请使用此命令的 **no** 形式。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

语法说明

delay	指定 OSPF 收到拓扑更改与启动最短路径优先 (SPF) 计算之间的延迟时间（以秒为单位），该值为 1 到 65535。
holdtime	两个连续 SPF 计算之间的保持时间（以秒为单位）；有效值为 1 到 65535。

默认值

默认值如下：

- *delay* 为 5 秒。
- *holdtime* 为 10 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
路由器配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

要配置 OSPF 协议收到拓扑更改与启动计算之间的延迟时间，以及两个连续 SPF 计算之间的保持时间，请使用 **timers spf** 命令。要恢复计时器默认值，请使用 **no timers spf** 命令。

示例

以下示例将 SPF 计算延迟设置为 10 秒，将 SPF 计算保持时间设置为 20 秒：

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

相关命令

命令	描述
router ospf	进入路由器配置模式。
show ospf	显示关于 OSPF 路由过程的一般信息。
timers lsa-group-pacing	指定收集以及刷新、验证校验和或老化 OSPF 链路状态通告 (LSA) 的间隔。

timers throttle

要为“开放最短路径优先”(OSPF) 链路状态通告 (LSA) 生成过程或 SPF 生成过程设置速率限制值，请在路由器 ospf 或 ipv6 路由器 ospf 配置模式下使用 **timers throttle** 命令。要恢复默认值，请使用此命令的 **no** 形式。

timers throttle {**lsa** | **spf**} *start-interval hold-interval max-interval*

no timers throttle {**lsa** | **spf**}

语法说明

lsa	配置 LSA 调速。
start-interval	指定生成第一次出现的 LSA 时的延迟（以毫秒为单位）。指定接收 SPF 计算更改的延迟（以毫秒为单位）。 指定生成第一次出现的 LSA 时的最短延迟（以毫秒为单位）。 **注** 本地 OSPF 拓扑更改后立即生成 LSA 的第一个实例。仅当经过 *start-interval* 后才会生成下一 LSA。 有效值介于 0 到 600,000 毫秒之间。默认值为 0 毫秒；LSA 将立即发送。
hold-interval	指定发起相同 LSA 的最长延迟（以毫秒为单位）。指定第一个和第二个 SPF 计算之间的延迟（以毫秒为单位）。 指定再次生成 LSA 的最短延迟（以毫秒为单位）。该值用于计算 LSA 生成的后续速率限制时间。有效值介于 1 到 600,000 毫秒之间。默认值为 5000 毫秒。
max-interval	指定发起相同 LSA 的最短延迟（以毫秒为单位）。指定 SPF 计算的最长等待时间（以毫秒为单位）。 指定再次生成 LSA 的最长延迟（以毫秒为单位）。有效值介于 1 到 600,000 毫秒之间。默认值为 5000 毫秒。
spf	配置 SPF 调速。

默认值

LSA 限制：

- 对于 *start-interval*，默认值为 0 毫秒。
- 对于 *hold-interval*，默认值为 5000 毫秒。
- 对于 *max-interval*，默认值为 5000 毫秒。

SPF 限制：

- 对于 *start-interval*，默认值为 5000 毫秒。
- 对于 *hold-interval*，默认值为 10000 毫秒。
- 对于 *max-interval*，默认值为 10000 毫秒。

命令模式

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个 情景	系统
Ipv6 路由器 ospf 配置	• 是	-	• 是	• 是	-
路由器 ospf 配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。
9.2(1)	添加对 IPv6 的支持。

使用指南

LSA 和 SPF 限制提供一种动态机制，在网络不稳定时减慢 OSPF 中的 LSA 更新的速度，通过提供 LSA 速率限制（以毫秒为单位）允许更快的 OSPF 融合。

对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPF 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPF 会自动更正为最小延迟值。

对于 SPF 限制，如果 *hold-interval* 或 *max-interval* 小于 *start-interval*，则 OSPF 会自动更正为 *start-interval* 值。同样地，如果 *max-interval* 小于 *hold-interval*，则 OSPF 会自动更正为 *hold-interval* 值。

示例

以下示例配置 OSPFv3 LSA 限制（以毫秒为单位）：

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

对于 LSA 限制，以下示例展示指定的最长延迟值小于最短延迟值时进行自动更正：

```
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
```

以下示例配置 OSPFv3 SPF 限制（以毫秒为单位）：

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

对于 SPF 限制，以下示例展示指定的最长延迟值小于最短延迟值时进行自动更正：

```
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
```

相关命令

命令	描述
ipv6 router ospf	进入 IPv6 路由器配置模式。
show ipv6 ospf	显示关于 OSPFv3 路由过程的一般信息。
timers lsa-group-pacing	指定收集以及刷新、验证校验和或老化 OSPFv3 LSA 的间隔。

timestamp

要在带有 IP 选项检测的数据包报头中出现时间戳 (TS) 选项时定义操作，请在参数配置模式下使用 **timestamp** 命令。要禁用此功能，请使用此命令的 **no** 形式。

timestamp action {allow | clear}

no timestamp action {allow | clear}

语法说明

allow	允许其中包含时间戳 IP 选项的数据包。
clear	从数据包报头中删除时间戳选项，然后允许数据包。

默认值

默认情况下，IP 选项检测会丢弃包含时间戳 IP 选项的数据包。

您可以在 IP 选项检测策略映射中使用 **default** 命令更改默认值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.5(1)	添加了此命令。

使用指南

此命令可配置的 IP 选项检查策略映射中。

可以配置 IP 选项检测来控制具有特定 IP 选项的哪些 IP 数据包可以通过 ASA。您可以允许数据包通过，而无需更改或清除指定的 IP 选项，然后允许数据包通过。

示例

以下示例展示如何在策略映射中设置 IP 选项检查的操作：

```
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
```

相关命令

命令	描述
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。

命令	描述
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

title

要定制 WebVPN 用户连接到安全设备时所显示 WebVPN 页面的标题，请在 webvpn 定制模式下使用 **title** 命令：

title {**text** | **style**} *value*

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

要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

语法说明

text	指示您正在更改文本。
style	指示您正在更改样式。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

默认值

默认标题文本为“WebVPN Service”。

默认标题样式如下：

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

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
WebVPN 定制	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

使用指南

要使其没有标题，请使用 **title text** 命令而不带 *value* 参数。

style 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查询位于 www.w3.org 的万维网联盟 (W3C) 网站上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

示例

在以下示例中，标题使用文本“Cisco WebVPN Service”定制：

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

相关命令

命令	描述
徽标	定制 WebVPN 页面上的徽标。
page style	定制使用层叠样式表 (CSS) 参数的 WebVPN 页面。

tls-proxy 至 type echo 命令

tls-proxy

要在 TLS 配置模式下配置 TLS 代理实例或者设置最大会话数，请在全局配置模式下使用 **tls-proxy** 命令。要删除配置，请使用此命令的 **no** 形式。

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

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

语法说明

max_sessions *max_sessions*	指定平台上支持的最大 TLS 代理会话数。
noconfirm	运行 **tls-proxy** 命令而不需要确认。
proxy_name	指定 TLS 代理实例的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **tls-proxy** 命令进入 TLS 代理配置模式以创建 TLS 代理实例，或者设置平台上支持的最大会话数。

示例

以下示例展示如何创建 TLS 代理实例：

```
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
```

相关命令

命令	描述
客户端	定义密码套件以及设置本地动态证书颁发者或密钥对。
ctl-provider	定义 CTL 提供程序实例，然后进入提供程序配置模式。
server trust-point	指定要在 TLS 握手期间呈现的代理信任点证书。
show tls-proxy	显示 TLS 代理。

tos

要定义 SLA 操作请求数据包的 IP 报头中的服务字节类型，请在 SLA 监控协议配置模式下使用 **tos** 命令。要恢复默认值，请使用此命令的 **no** 形式。

tos *number*

no tos

语法说明

number	要用于 IP 报头中的服务类型值。有效值为 0 至 255。

默认值

默认服务类型值为 0。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
SLA 监控协议配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此字段包含延迟、优先级、可靠性等信息。可供网络上其他路由器用于策略路由和承诺接入速率等功能。

示例

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求/响应时间探测操作。它将回应请求数据包的有效负载大小设为 48 字节、SLA 操作期间发送的回应请求数设为 5、服务类型字节设为 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
```

相关命令

命令	描述
num-packets	指定要在 SLA 操作期间发送的请求数据包数。
request-data-size	指定请求数据包负载的大小。
sla monitor	定义 SLA 监控操作。
type echo	将 SLA 操作配置为回应响应时间探测操作。

traceroute

要确定将传送至其目标的路由数据包，请使用 **traceroute** 命令。

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**]

语法说明

destination_ip	指定 traceroute 的目标 IP 地址。支持 IPv4 和 IPv6 地址。
hostname	必须跟踪其路由的主机的主机名。主机目标地址可以是 IPv4 或 IPv6 地址。如果指定了主机，请使用 **name** 命令定义它，或者配置 DNS 服务器以启用 traceroute 将主机名解析为 IP 地址。支持 DNS 域名，例如 www.example.com。
max-ttl	可以使用的最大 TTL 值。默认值为 30。此命令在跟踪路由数据包到达目标或达到该值时终止。
min_ttl	第一次探测的 TTL 值。默认值为 1，但也可以设置为更高的值来抑制已知跃点的显示。
numeric	指定只输出打印中间网关的 IP 地址。如果未指定此关键字，跟踪路由会尝试查找跟踪时到达的网关主机名。
port *port_value*	用户数据报协议 (UDP) 探测消息使用的目标端口。默认值为 33434。
probe *probe_num*	在每个 TTL 级别要发送的探测次数。默认计数为 3。
source	指定 IP 地址或接口用作跟踪数据包的源。IPv6 将仅接受 IPv6 源地址。
source_interface	指定数据包跟踪的源接口。指定后，将使用源接口的 IP 地址。
source_ip	指定数据包跟踪的源 IP 地址。此 IP 地址必须是其中一个接口的 IP 地址。在透明模式下，它必须是 ASA 的管理 IP 地址。
timeout	指定使用超时值
timeout_value	指定在连接超时前等待响应的时间（秒）。默认值为 3 秒。
ttl	用于指定探测中要使用的“生存时间”值范围的关键字。
use-icmp	指定使用 ICMP 探测数据包而不是 UDP 探测数据包。

默认值

此命令没有默认设置。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.2(1)	添加了此命令。
9.7.(1)	已将此命令更新为接受 IPv6 地址。

使用指南

traceroute 命令可打印发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。以下是 **traceroute** 命令打印的输出符号：

输出符号	描述
*	在超时期限内未收到对探测的响应。
U	没有通往目标的路由。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。对于 ICMPv6，地址超出范围。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。对于 ICMPv6，端口不可访问。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

示例

以下示例展示指定了目标 IP 地址时产生的跟踪路由输出：

```
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
```

相关命令

命令	描述
捕捉	捕捉数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕捉配置。
packet-tracer	启用数据包跟踪功能。

track rtr

要跟踪 SLA 操作的可达性，请在全局配置模式下使用 **track rtr** 命令。要删除 SLA 跟踪，则使用此命令的 **no** 形式。

track *track-id* **rtr** *sla-id* **reachability**

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

语法说明

可访问性	指定跟踪对象的可达性。
sla-id	跟踪条目所用 SLA 的 ID。
track-id	创建跟踪条目对象 ID。有效值为从 1 到 500。

默认值

禁用 SLA 跟踪。

命令模式

下表展示可输入命令的模式：

	防火墙模式		**安全情景**		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	**修改**
7.2(1)	添加了此命令。

使用指南

track rtr 命令创建跟踪条目对象 ID 并指定该跟踪条目使用的 SLA。

每项 SLA 操作保持操作返回代码值，该代码值通过跟踪过程解译。返回代码可能正常、超过阈值或者有多个其他返回代码。表 2-1 显示涉及这些返回代码的对象可达性状态。

表 2-1　SLA 跟踪返回代码

Tracking	**返还码**	**跟踪状态**
可访问性	正常或超过阈值	Up
	任何其他代码	关闭

示例

以下示例配置 ID 为 123 的 SLA 操作，并且创建 ID 为 1 的跟踪条目来跟踪 SLA 的可访问性：

```
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
```

相关命令

命令	描述
route	配置静态路由。
sla monitor	定义 SLA 监控操作。

traffic-forward

要将流量定向到模块并绕过访问控制和其他处理过程，请在接口配置模式下使用 **traffic-forward** 命令。要禁用流量转发，请使用此命令的 **no** 形式。

traffic-forward *module_type* **monitor-only**

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

语法说明

module_type	模块的类型。支持的模块包括： • **sfr**—ASA FirePOWER 模块。 • **cxsc**—ASA CX 模块。
monitor-only	将模块设为只监控模式。在仅监控模式下，模块可以处理流量，但是之后会丢弃流量。根据不同的模块类型，使用情况也会不同： • ASA FirePOWER - 使用此命令配置被动模式。您可以将此模式用于生产用途。 • ASA CX - 这严格来说是演示模式。您无法将流量转发接口或设备用于生产目的。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	-	• 是	• 是	-	-

命令历史记录

版本	修改
9.1(2)	添加了此命令。
9.2(1)	添加了 **sfr** 关键字。
9.3(2)	添加了 **sfr** 关键字，可支持生产使用。

使用指南

此命令可替代对服务策略 **sfr** 或 **cxsc** 命令的使用，其使用 **monitor-only** 关键字将流量重定向至模块。使用服务策略，流量仍会经过 ASA 处理（例如访问规则和 TCP 规范化），这可导致丢弃流量。此外，ASA 仅会将流量的副本发送至模块，并最终根据其自己的策略传输流量。

而 **Traffic-forward** 命令会完全绕过 ASA 处理，只将流量转发到模块。该模块然后会检查流量、制定策略决策并生成事件，显示当流量以内联模式运行时您需要对其执行什么操作。虽然该模块在流量副本上运行，则无论 ASA 或模块化策略决策如何，ASA 自身会立即丢弃流量。该模块充当黑洞。

将流量转发接口连接到您网络中交换机上的 SPAN 端口。

流量转发接口配置有以下限制：

- 在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许使用一种类型的安全策略。
- ASA 必须处于单情景透明模式下。
- 流量转发接口必须是物理接口，而不能是 VLAN 或 BVI。物理接口也不能关联任何 VLAN。
- 流量转发接口不能用于 ASA 流量；不能为这些接口命名或配置接口用于 ASA 功能，包括故障切换或仅管理功能。

示例

以下示例将 GigabitEthernet 0/5 设为流量转发接口：

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

相关命令

命令	描述
Interface	进入接口配置模式。
cxsc	将流量重定向到 ASA CX 模块的服务策略命令。
sfr	将流量重定向到 ASA FirePOWER 模块的服务策略命令。

traffic-non-sip

要允许使用已知 SIP 信令端口的非 SIP 流量，请在参数配置模式使用 **traffic-non-sip** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

traffic-non-sip

no traffic-non-sip

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下会启用此命令。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例展示在 SIP 检查策略映射中如何允许使用已知 SIP 信令端口的非 SIP 流量：

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

相关命令

命令	描述
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

transfer-encoding

要通过指定传输编码类型来限制 HTTP 流量，请在 HTTP 映射配置模式（使用 **http-map** 命令可访问）下使用 **transfer-encoding** 命令：要禁用此功能，请使用此命令的 **no** 形式。

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**]

语法说明

action	指定在检测到连接使用指定的传输编码类型时所执行的操作。
allow	允许消息。
chunked	标识消息正文作为一系列信息块传输的传输编码类型。
compress	标识消息正文使用 UNIX 文件压缩传输的传输编码类型。
default	指定当流量包含不在配置列表中的支持请求方式时 ASA 采取的默认操作。
deflate	标识消息正文使用 zlib 格式 (RFC 1950) 和 deflate 压缩 (RFC 1951) 传输的传输编码类型。
drop	关闭连接。
gzip	标识消息正文使用 GNU zip (RFC 1952) 传输的传输编码类型。
identity	标识消息正文没有传输编码时执行的连接。
log	（可选）生成系统日志。
reset	将 TCP 重置消息发送到客户端和服务器。
type	指定要通过 HTTP 应用检查控制的传输编码类型。

默认值

此命令默认禁用。当启用此命令并且未指定支持的传输编码类型时，默认操作是允许连接但不记录日志。要更改默认操作，请使用 **default** 关键字并指定不同的默认操作。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
HTTP 映射配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

启用 **transfer-encoding** 命令时，ASA 将为每个支持和配置的传输编码类型对 HTTP 连接应用指定的操作。

对于与配置列表中的传输编码类型*不*匹配的所有流量，ASA 将应用**默认**操作。预配置的**默认**操作是**允许**连接而不记录日志。

例如，按照预配置的默认操作，如果您指定一个或多个具有操作**丢弃**和**记录**的编码类型，则 ASA 将丢弃包含已配置编码类型的连接、记录每个连接，并允许其他支持的编码类型的所有连接。

如果要配置更严格的策略，可将默认操作改为**丢弃**（或**重置**）并**记录**（如果要记录事件）。然后使用**允许**操作配置每个允许的编码类型。

为每项要应用的设置输入一次 **transfer-encoding** 命令。使用 **transfer-encoding** 命令的一个实例更改默认操作，一个实例将每个编码类型添加到配置的传输编码类型列表。

使用此命令的 **no** 形式从配置的应用类型列表中删除应用类别时，将会忽略命令行中应用类别关键字后的所有字符。

示例

以下示例提供使用预配置默认值的允许策略，允许未明确禁止的所有支持的应用类型。

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

在这种情况下，只会丢弃使用 GNU zip 的连接，并且会记录事件。

以下示例提供限制策略，此策略更改默认操作来重置连接，并且为未明确允许的任何编码类型记录事件。

```
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)#
```

在这种情况下，只允许不使用传输编码的连接。收到其他支持的编码类型的 HTTP 流量时，ASA 会重置连接并创建系统日志条目。

相关命令

命令	描述
class-map	定义要应用的安全操作的流量类。
debug appfw	显示与增强型 HTTP 检查关联的流量详细信息。
http-map	为配置的增强型 HTTP 检查定义 HTTP 映射。
inspect http	应用要用于应用检查的特定 HTTP 映射。
policy-map	将类映射与特定的安全操作相关联。

trustpoint (saml idp)

要配置包含 idp 身份验证或 sp 身份验证证书的信任点，请在 saml idp 配置模式下使用 **trustpoint** 命令。您可以通过先输入 **webvpn** 命令来访问 saml idp 配置模式。要删除信任点，请使用此命令的 **no** 形式。

trustpoint {**idp** | **sp**} *trustpoint-name*

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

语法说明

trustpoint-name	指定要使用的信任点的名称。
sp	该信任点包含 ASA (SP) 的证书，以便 IdP 可验证 ASA 的签名或加密 SAML 断言。
idp	该信任点包含 IdP 证书，以便 ASA 可验证 SAML 断言。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Saml idp 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.5(2)	添加了此命令。

使用指南

信任点代表证书机构身份，基于无需验证测试即可视为有效的 CA 颁发证书，特别是用于在证书路径中提供第一个公钥的公钥证书。

相关命令

命令	描述
saml idp	为第三方 Idp 创建一个配置，并将您置于 saml-idp 模式下，以便您可以配置 SAML 属性。

trustpoint (sso server)（已弃用）

注 支持此命令的最后一个版本是版本 9.5(1)。

要指定信任点的名称以标识要发送到 SAML POST 类型 SSO 服务器的证书，请在 sso 服务器模式下使用 **trustpoint** 命令。要消除信任点指定，请使用此命令的 **no** 形式。

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

语法说明

trustpoint-name	指定要使用的信任点的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Config webvpn sso saml	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
9.5(2)	为了支持 SAML 2.0，此命令已弃用。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。ASA 当前支持 SAML POST 类型的 SSO 服务器和 SiteMinder 类型的 SSO 服务器。

此命令仅适用于 SAML 类型的 SSO 服务器。

信任点代表证书机构身份，基于无需验证测试即可视为有效的 CA 颁发证书，特别是用于在证书路径中提供第一个公钥的公钥证书。

示例

以下示例进入 config-webvpn-sso-saml 模式，并且命名信任点以标识要发送到 SAML POST 类型 SSO 服务器的证书：

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

相关命令

命令	描述
crypto ca trustpoint	管理信任点信息。
show webvpn sso server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso server	创建、命名并指定 SSO 服务器的类型。

trust-verification-server

要标识 Trust Verification Services 服务器，以使 Cisco Unified IP 电话在 HTTPS 建立期间验证应用服务器身份，请在 SIP 检查的参数配置模式下使用 **trust-verification-server** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

trust-verification-server {**ip** *address* | **port** *number*}

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

语法说明

ip *address*	指定 Trust Verification Services 服务器的 IP 地址。输入此命令时，此参数在 SIP 检查策略映射中最多可以使用四次。SIP 检测会为每个已注册的电话打开用于连接到每台服务器的针孔，由电话确定使用哪个针孔。在思科统一通信管理器 (CUCM) 服务器上配置 Trust Verification Services 服务器。
port *number*	指定服务器使用的端口号。允许的端口范围是 1026 到 32768。

默认值

默认端口为 2445。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.3(2)	添加了此命令。

示例

以下示例展示如何在 SIP 检查策略映射中配置四台 Trust Verification Services 服务器：

```
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
```

相关命令

命令	描述
policy-map type inspect	创建检查策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

tsig enforced

若需要 TSIG 资源记录存在，请在参数配置模式下使用 **tsig enforced** 命令。要禁用此功能，请使用此命令的 **no** 形式。

tsig enforced action {**drop** [**log**] | **log**}

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

语法说明

drop	如果 TSIG 不存在，则丢弃数据包。
log	生成系统消息日志。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	**修改**
7.2(1)	添加了此命令。

使用指南

此命令在 DNS 事务处理中启用 TSIG 在线状态的监控和实施。

示例

以下示例展示如何在 DNS 检查策略映射中启用 TSIG 实施：

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

相关命令

命令	**描述**
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

ttl-evasion-protection

要启用生存时间 (TTL) 规避保护，请在 tcp-map 配置模式下使用 **ttl-evasion-protection** 命令。要禁用该功能，请使用此命令的 **no** 形式。

ttl-evasion-protection

no ttl-evasion-protection

语法说明

此命令没有任何参数或关键字。

默认值

默认将启用所提供的 TTL 规避保护。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
TCP 映射配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

将 **tcp-map** 命令与模块化策略框架基础设施结合使用。使用 **class-map** 命令定义流量类并使用 **tcp-map** 命令定制 TCP 检查。应用新 TCP 映射使用 **policy-map** 命令。使用 **service-policy** 命令激活 TCP 检查。

使用 **tcp-map** 命令进入 TCP 映射配置模式。在 tcp-map 配置模式下使用 **ttl-evasion-protection** 命令防止试图规避安全策略的攻击。利用 TTL 规避保护，对应于连接的最大 TTL 数由初始数据包中的 TTL 确定。后续数据包的 TTL 可以减少，但不能增加。系统会将 TTL 重置为该连接之前看到过的最低 TTL。

例如，攻击者可以发送一个 TTL 很短的通过策略的数据包。当 TTL 变为零时，ASA 与终端之间的路由器就会丢弃数据包。此时攻击者可以发送一个 TTL 很长、似乎 ASA 是重新传输的恶意数据包并获得通过。但到达终端主机时，它是攻击者收到的第一个数据包。在这种情况下，攻击者可以成功绕过防范攻击的安全措施。启用此功能可防止此类攻击。

示例

以下示例展示如何在从网络 10.0.0.0 到 20.0.0.0 的流上禁用 TTL 规避保护。

```
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
```

相关命令

命令	描述
class	指定要用于流量分类的类映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
set connection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

tunnel destination

要指定 VTI 隧道目标的 IP 地址，请在接口配置模式下使用 **tunnel destination** 命令。要删除 VTI 隧道的目标 IP 地址，请使用此命令的 **no** 形式。

tunnel destination {*IP address* | *hostname*}

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

语法说明

IP address	指定 VTI 隧道目标的 IP 地址 (IPv4)。
hostname	指定 VTI 隧道目标的主机名。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 否	• 是	• 否	-

命令历史记录

版本	修改
9.7(1)	我们引入了此命令。

使用指南

在全局配置模式下使用 **interface tunnel** 命令之后，可在接口配置模式下使用此命令。

示例

以下示例指定 VTI 隧道目标的 IP 地址:

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

相关命令

命令	描述
interface tunnel	创建新的 VTI 隧道接口。
tunnel source interface	指定用于创建 VTI 隧道的源接口。
tunnel mode	指定将 IPsec 用于隧道保护。
tunnel protection ipsec	指定将用于隧道保护的 IPsec 配置文件。

tunnel mode

要指定 VTI 隧道的隧道保护模式，请在接口配置模式下使用 **tunnel mode** 命令。要删除 VTI 隧道保护，请使用此命令的 **no** 形式。

tunnel mode *ipsec IPv4*

no tunnel mode *ipsec IPv4*

语法说明

ipsec	指定为隧道将使用 IPsec 作为隧道保护标准。
IPv4	指定为隧道将通过 IPv4 使用 IPsec。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 否	• 是	• 否	-

命令历史记录

版本	修改
9.7(1)	我们引入了此命令。

使用指南

在全局配置模式下使用 **interface tunnel** 命令之后，可在接口配置模式下使用此命令。

示例

以下示例将 IPsec 指定为保护模式：

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

相关命令

命令	描述
interface tunnel	创建新的 VTI 隧道接口。
tunnel source interface	指定用于创建 VTI 隧道的源接口。
tunnel destination	指定 VTI 隧道目标的 IP 地址。
tunnel protection ipsec	指定将用于隧道保护的 IPsec 配置文件。

tunnel protection ipsec

要指定 VTI 隧道的 Ipsec 配置文件，请在接口配置模式下使用 **tunnel protection ipsec** 命令。要删除隧道的 IPsec 配置文件，请使用此命令的 **no** 形式。

tunnel protection ipsec *IPsec profile name*

no tunnel protection ipsec *IPsec profile name*

语法说明

ipsec profile name	指定要使用的 IPsec 配置文件的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 否	• 是	• 否	-

命令历史记录

版本	修改
9.7(1)	我们引入了此命令。

使用指南

在全局配置模式下使用 **interface tunnel** 命令之后，可在接口配置模式下使用此命令。使用此命令时，IKEv1 策略将附加到 IPsec 配置文件。

示例

在以下示例中，profile12 是 IPsec 配置文件：

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

相关命令

命令	描述
interface tunnel	创建新的 VTI 隧道接口。
tunnel source interface	指定用于创建 VTI 隧道的源接口。
tunnel destination	指定 VTI 隧道目标的 IP 地址。
tunnel mode	指定将 IPsec 用于隧道保护。

tunnel source interface

要指定 VTI 隧道的源接口，请在接口配置模式下使用 **tunnel source interface** 命令。要删除 VTI 隧道的源接口，请使用此命令的 **no** 形式。

tunnel source interface *interface name*

no tunnel source interface *interface name*

语法说明

interface name	指定用于创建 VTI 隧道的源接口。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 否	• 是	• 否	-

命令历史记录

版本	修改
9.7(1)	我们引入了此命令。

使用指南

在全局配置模式下使用 **interface tunnel** 命令之后，可在接口配置模式下使用此命令。IP 地址取自所选接口。

示例

以下示例指定 VTI 隧道的源接口：

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

相关命令

命令	描述
interface tunnel	创建新的 VTI 隧道接口。
tunnel destination	指定 VTI 隧道目标的 IP 地址。
tunnel mode	指定将 IPsec 用于隧道保护。
tunnel protection ipsec	指定将用于隧道保护的 IPsec 配置文件。

tunnel-group

要为 IPsec 和 WebVPN 隧道创建和管理连接特定记录的数据库，请在全局配置模式下使用 **tunnel-group** 命令。要删除隧道组，则使用此命令的 **no** 形式。

tunnel-group *name* **type** *type*

no tunnel-group *name*

语法说明

name	指定隧道组的名称。这可以是您选择的任何字符串。如果名称是 IP 地址，通常是对等设备的 IP 地址。
type	指定隧道组类型： • remote-access - 允许用户使用 IPsec 远程接入或 WebVPN（门户或隧道客户端）连接。 • ipsec-l2l - 指定 IPsec 局域网至局域网，允许两个站点或局域网通过 Internet 等公共网络安全地连接。 **注** 以下隧道组类型在 8.0(2) 版本中已弃用： ipsec-ra - IPsec 远程接入 webvpn - WebVPN ASA 会将这些类型转换为 remote-access 类型。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	请参阅注释。	• 是	• 是	-

注 tunnel-group 命令适用于透明防火墙模式，允许局域网至局域网隧道组配置，但不允许 remote-access 组或 WebVPN 组。所有适用于局域网至局域网的 **tunnel-group** 命令也适用于透明防火墙模式。

命令历史记录

版本	修改
7.0(1)	添加了此命令。
7.1(1)	添加了 webvpn 类型。
8.0(2)	添加了 remote-access 类型，并废弃了 ipsec-ra 和 webvpn 类型。
8.3(1)	*name* 参数经过修改，接受 IPv6 地址。
9.0(1)	增加了多情景模式支持。

使用指南

SSL VPN 用户（AnyConnect 和无客户端）可以使用以下不同的方法选择哪个隧道组接入：

- group-url
- group-alias
- 证书映射（如果使用证书）

此命令和子命令用于配置 ASA，使用户在登录到 webvpn 服务时可以通过下拉菜单选择组。菜单中显示的组是 ASA 上配置的实际连接配置文件（隧道组）的别名或 URL。

ASA 具有以下默认隧道组：

- DefaultRAGroup，默认 IPsec 远程接入隧道组
- DefaultL2LGroup，默认 IPsec 局域网至局域网隧道组
- DefaultWEBVPNGroup，默认 WebVPN 隧道组。

您可以更改这些组，但不能删除它们。如果在隧道协商过程中没有标识特定隧道组，ASA 将会使用这两个隧道组来配置远程访问隧道组和 LAN 到 LAN 隧道组的默认隧道参数。

在输入 **tunnel-group** 命令后，输入以下适当的命令为特定隧道组配置特定属性。其中每个命令都可以进入用于配置隧道组属性的配置模式。

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

对于局域网至局域网连接，ASA 会尝试将加密映射中指定的对等地址匹配到相同名称的隧道组，以选择用于连接的隧道组。因此，对于 IPv6 对等设备，您应该将隧道组名称配置为对等设备的 IPv6 地址。您可以使用短记数法或长记数法指定隧道组名称。CLI 会将名称减至最短的记数法。例如，如果您输入以下隧道组命令：

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

隧道组在配置中显示为：

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

示例

以下示例是在全局配置模式下输入的。第一个配置远程接入隧道组。组名是 group1。

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

以下示例展示配置 webvpn 隧道组“group1”的 tunnel-group 命令。在全局配置模式下输入此命令：

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

相关命令

命令	描述
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group general-attributes	进入用于配置常规隧道组属性的 config-general 模式。
tunnel-group ipsec-attributes	进入用于配置 IPsec 隧道组属性的 config-ipsec 模式。
tunnel-group ppp-attributes	进入用于为 L2TP 连接配置 PPP 设置的 config-ppp 模式。
tunnel-group webvpn-attributes	进入用于配置 WebVPN 隧道组属性的 config-webvpn 模式。

tunnel-group general-attributes

要进入常规属性配置模式，请在全局配置模式下使用 **tunnel-group general-attributes** 命令。此模式用于配置所有支持的隧道协议公用的设置。

要删除所有常规属性，请使用此命令的 **no** 形式。

tunnel-group *name* **general-attributes**

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

语法说明

general-attributes	指定此隧道组的 属性。
name	指定隧道组的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
隧道组常规属性配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
7.1(1)	其他隧道组类型的各项属性迁移到了常规隧道组属性列表，并且隧道组常规属性模式的提示已更改。
9.0(1)	增加了多情景模式支持。

示例

以下示例是在全局配置模式下输入的，使用局域网至局域网对等设备的 IP 地址为远程接入连接创建 remote-access 隧道组，然后进入常规属性配置模式，配置隧道组常规属性。隧道组的名称是 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)#
```

以下示例是在全局配置模式下输入的，为 IPsec 远程接入连接创建一个名为“remotegrp”的隧道组，然后进入常规配置模式，为名为“remotegrp”的隧道组配置常规属性。

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

相关命令

命令	描述
clear configure tunnel-group	清除整个隧道组数据库或只清除指定的隧道组。
show running-config tunnel-group	为指定的隧道组或所有隧道组显示当前运行的隧道组配置。
tunnel-group	为 IPsec 和 WebVPN 隧道创建和管理连接特定记录的数据库。

tunnel-group ipsec-attributes

要进入 ipsec 属性配置模式，请在全局配置模式下使用 **tunnel-group ipsec-attributes** 命令。此模式用于配置特定于 IPsec 隧道协议的设置。

要删除所有 IPsec 属性，请使用此命令的 **no** 形式。

tunnel-group *name* **ipsec-attributes**

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

语法说明

ipsec-attributes	指定此隧道组的 属性。
name	指定隧道组的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
7.1(1)	各项 IPsec 隧道组属性迁移到了常规隧道组属性列表，并且隧道组 ipsec 属性模式的提示已更改。
9.0(1)	增加了多情景模式支持。

示例

以下示例是在全局配置中输入的，为名为 remotegrp 的 IPsec 远程接入隧道组创建一个隧道组，然后指定 IPsec 组属性：

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

相关命令

命令	描述
clear configure tunnel-group	清除整个隧道组数据库或只清除指定的隧道组。
show running-config tunnel-group	为指定的隧道组或所有隧道组显示当前运行的隧道组配置。
tunnel-group	为 IPsec 和 WebVPN 隧道创建和管理连接特定记录的数据库。

tunnel-group-list enable

要启用在 tunnel-group group-alias 中定义的隧道组，请使用 **tunnel-group-list enable** 命令：

tunnel-group-list enable

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Webvpn 配置	• 是	-	• 是	• 是	-

使用指南

此命令与 tunnel-group group-alias 及 group-url 命令一起用于无客户端和 AnyConnect VPN 客户端会话。它启用相关功能，使隧道组下拉列表显示在登录页。组别名是 ASA 管理员定义的一个文本字符串，例如员工、工程或顾问，用来显示给最终用户。

命令历史记录

版本	修改
7.0(1)	添加了此命令。

示例

```
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
```

相关命令

命令	描述
tunnel-group	创建 VPN 连接配置文件或访问 VPN 连接配置文件数据库。
group-alias	配置连接配置文件（隧道组）的别名。
group-url	将 VPN 终端指定的 URL 或 IP 地址与连接配置文件进行匹配。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。

tunnel-group-map

当自适应安全设备收到采用客户端证书身份验证的 IPsec 连接请求时，它将根据您配置的策略为连接分配连接配置文件。

该策略可以使用您配置的规则、证书 OU 字段、IKE 身份（如主机名、IP 地址、密钥 ID）、客户端 IP 地址或默认连接配置文件分配连接配置文件。对于 SSL 连接，自适应安全设备只使用您配置的规则分配连接配置文件。

tunnel-group-map 命令根据您配置的规则，通过将现有映射名称与连接配置文件关联向连接分配连接配置文件。

使用此命令的 **no** 形式可取消连接配置文件与映射名称的关联。该命令的 no 形式不删除映射名称，只取消其与连接配置文件的关联。

以下是该命令的语法：

tunnel-group-map [mapname] [rule-index] [connection-profile]

no tunnel-group-map [mapname] [rule-index]

注

- 您可以使用此命令创建证书映射名称：
  crypto ca certificate map [mapname] [rule-index]
- “隧道组”是一个旧术语，现在我们称之为“连接配置文件”。考虑使用 tunnel-group-map 命令来创建连接配置文件映射。

语法说明

mapname	Required.标识**现有**证书映射的名称。
rule-index	Required.标识与映射名称关联的规则索引。rule-index 参数使用 **crypto ca certificate map** 命令定义。有效值为 1 到 65535。
connection-profile	为此证书映射列表指定连接配置文件名称。

默认值

如果未定义隧道组映射，并且 ASA 收到采用客户端证书身份验证的 IPsec 连接请求，ASA 会按以下顺序尝试将证书身份验证请求与其中一个策略进行匹配，以分配连接配置文件：

证书 ou 字段 - 根据主题可分辨名称 (DN) 中的组织单位 (OU) 字段值确定连接配置文件。

IKE 身份 - 根据第 1 阶段 IKE ID 的内容确定连接配置文件。

peer-ip - 根据现有的客户端 IP 地址确定连接配置文件。

默认连接配置文件 - 如果 ASA 与前三个策略不匹配，将会分配默认连接配置文件。默认配置文件为 DefaultRAGroup。否则使用 tunnel-group-map default-group 命令配置默认连接配置文件。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

您指定的映射名称必须已经存在，然后才可将其与连接配置文件关联。可使用 **crypto ca certificate map** 命令创建映射名称。详细信息请参阅有关 **crypto ca certificate map** 命令的文档。

将映射名称与连接配置文件关联后，需要启用 tunnel-group-map 以使用您配置的规则而不是前述默认策略。为此必须在全局配置模式下运行 **tunnel-group-map enable rules** 命令。

示例

以下示例将规则索引为 **10** 的映射名称 **SalesGroup** 关联到 **SalesConnectionProfile** 连接配置文件。

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

相关命令

命令	描述
crypto ca certificate map [map name]	进入 ca 证书映射配置模式，然后可以使用它来创建证书映射名称。
tunnel-group-map enable	根据建立的规则启用基于证书的 IKE 会话。
tunnel-group-map default-group	将现有隧道组名称指定为默认隧道组。

tunnel-group-map default-group

如果使用其他配置的方法无法确定名称，**tunnel-group-map default-group** 命令将指定使用默认隧道组。

使用此命令的 **no** 形式可删除隧道组映射。

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

语法说明

default-group *tunnel-group-name*	指定当其他配置的方法无法推导出名称时使用默认隧道组。*隧道组名称*必须已存在。
rule index	（可选）请参阅 **crypto ca certificate map** 命令指定的参数。有效值为 1 到 65535。

默认值

tunnel-group-map default-group 的默认值为 DefaultRAGroup。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

tunnel-group-map 命令配置基于证书的 IKE 会话用以映射到隧道组的策略和规则。要将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联，请在全局配置模式下使用 **tunnel-group-map** 命令。您可以多次调用此命令，前提是每次调用都是唯一的，并且不多次引用映射索引。

crypto ca certificate map 命令维护证书映射规则的优先级列表。只能有一个映射。但此映射最多可有 65535 个规则。详细信息请参阅有关 **crypto ca certificate map** 命令的文档。

从证书推导隧道组名称的处理会忽略证书映射中未关联隧道组的条目（此命令未识别的任何映射规则）。

示例

以下示例在全局配置模式下输入，指定当其他配置的方法无法推导出名称时使用默认隧道组。要使用的隧道组名称是 group1：

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

相关命令

命令	描述
crypto ca certificate map	进入 crypto ca certificate map 配置模式。
subject-name (crypto ca certificate map)	标识 CA 证书中要与规则条目字符串进行比较的 DN。
tunnel-group-map enable	配置基于证书的 IKE 会话用以映射到隧道组的策略和规则。

tunnel-group-map enable

tunnel-group-map enable 命令配置基于证书的 IKE 会话用以映射到隧道组的策略和规则。使用此命令的 **no** 形式可恢复默认值。

tunnel-group-map [*rule-index*] **enable** *policy*

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

语法说明

policy	指定用于从证书获取隧道组名称的策略。*Policy* 可以是以下某一项： **ike-id** - 指示如果根据规则查找或 ou 无法确定隧道组，则基于证书的 IKE 会话将根据第 1 阶段 IKE ID 的内容映射到隧道组。 **ou** - 指示如果根据规则查找无法确定隧道组，则使用主题可分辨名称 (DN) 中的组织单位 (OU) 值。 **peer-ip** - 指示如果根据规则查找、ou 或 ike-id 方法无法确定隧道组，则使用现有的对等 IP 地址。 **rules** - 指示基于证书的 IKE 会话根据此命令配置的证书映射关联映射到隧道组。
rule index	（可选）指 **crypto ca certificate map** 命令指定的参数。有效值为 1 到 65535。

默认值

tunnel-group-map 命令的默认值是 **enable ou**，并且 **default-group** 设为 DefaultRAGroup。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

crypto ca certificate map 命令维护证书映射规则的优先级列表。只能有一个映射。但此映射最多可有 65535 个规则。详细信息请参阅有关 **crypto ca certificate map** 命令的文档。

示例

以下示例使基于证书的 IKE 会话根据第 1 阶段 IKE ID 的内容映射到隧道组：

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

以下示例使基于证书的 IKE 会话根据对等设备的现有 IP 地址映射到隧道组：

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

以下示例根据主题可分辨名称 (DN) 的组织单位 (OU) 映射基于证书的 IKE 会话：

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

以下示例根据现有的规则映射基于证书的 IKE 会话：

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

相关命令

命令	描述
crypto ca certificate map	进入 CA 证书映射模式。
subject-name (crypto ca certificate map)	标识 CA 证书中要与规则条目字符串进行比较的 DN。
tunnel-group-map default-group	将现有隧道组名称指定为默认隧道组。

tunnel-group ppp-attributes

要进入 PPP 属性配置模式并且配置 L2TP over IPsec 连接使用的 PPP 设置，请在全局配置模式下使用 **tunnel-group ppp-attributes** 命令。

要删除所有 PPP 属性，请使用此命令的 **no** 形式。

tunnel-group *name* **ppp-attributes**

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

语法说明

name	指定隧道组的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

PPP 设置由第 2 层隧道协议 (L2TP) 使用，此协议是一个 VPN 隧道协议，允许远程客户端使用拨号电话服务公共 IP 网络安全地与专用企业网络服务器通信。L2TP 基于客户端/服务器模型，使用 PPP over UDP（端口 1701）传输数据。所有 tunnel-group ppp 命令适用于 PPPoE 隧道组类型。

示例

以下示例创建隧道组 *telecommuters* 并且进入 ppp 属性配置模式：

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

相关命令

命令	描述
clear configure tunnel-group	清除整个隧道组数据库或只清除指定的隧道组。
show running-config tunnel-group	为指定的隧道组或所有隧道组显示当前运行的隧道组配置。
tunnel-group	为 IPsec 和 WebVPN 隧道创建和管理连接特定记录的数据库。

tunnel-group-preference

要使用与终端指定的 URL 匹配的组 URL 更改连接配置文件的 VPN 首选项，请在 webvpn 配置模式下使用 **tunnel-group-preference** 命令。要从配置中删除此命令，则使用 **no** 形式。

tunnel-group-preference group-url

no tunnel-group-preference group-url

语法说明

此命令没有任何参数或关键字。

命令默认

默认情况下，如果 ASA 将连接配置文件中指定的证书字段值与终端所用证书的字段值进行匹配，ASA 会将该配置文件分配到 VPN 连接。此命令会覆盖默认行为。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Config-webvpn	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.2(5)/8.4(2)	添加了此命令。

使用指南

此命令在连接配置文件选择过程中会更改连接配置文件首选项。它可让您采用许多旧版 ASA 软件使用的组 URL 首选项。如果终端指定不在连接配置文件中的组 URL，但指定与连接配置文件匹配的证书值，则 ASA 会将该连接配置文件分配到 VPN 会话。

虽然您是在 webvpn 配置模式下输入此命令，但它会更改 ASA 协商的所有无客户端和 AnyConnect VPN 连接的连接配置文件选择首选项。

示例

以下示例在连接配置文件选择过程中更改连接配置文件首选项：

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

相关命令

命令	描述
tunnel-group	创建 VPN 连接配置文件或访问 VPN 连接配置文件数据库。
group-url	将 VPN 终端指定的 URL 或 IP 地址与连接配置文件进行匹配。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。

tunnel-group webvpn-attributes

要进入 webvpn 属性配置模式，请在全局配置模式下使用 **tunnel-group webvpn-attributes** 命令。此模式配置 WebVPN 隧道公用的设置。

要删除所有 WebVPN 属性，请使用此命令的 **no** 形式。

tunnel-group *name* **webvpn-attributes**

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

语法说明

name	指定隧道组的名称。
webvpn-attributes	指定此隧道组的 WebVPN 属性。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。
9.8(1)	将 pre-fill-username 和 secondary-pre-fill-username 值从 clientless 更改为 client。

使用指南

除了常规属性之外，还可以在 webvpn 属性模式下配置以下特定于 WebVPN 连接的属性：

- authentication
- customization
- dns-group
- group-alias
- group-url
- without-csd

Pre-fill-username 和 secondary-pre-fill-username 属性用于从身份验证和授权中使用的证书提取用户名。值为 client 或 clientless。

示例

以下示例是在全局配置模式下输入的，使用局域网至局域网对等设备的 IP 地址为 WebVPN 连接创建一个隧道组，然后进入 webvpn 配置模式，配置 WebVPN 属性。隧道组的名称是 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)#
```

以下示例是在全局配置模式下输入的，为 WebVPN 远程接入连接创建一个名为“remotegrp”的隧道组，然后进入 webvpn 配置模式，为名为“remotegrp”的隧道组配置 WebVPN 属性。

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

相关命令

命令	描述
clear configure tunnel-group	清除整个隧道组数据库或只清除指定的隧道组。
show running-config tunnel-group	为指定的隧道组或所有隧道组显示当前运行的隧道组配置。
tunnel-group	为 IPsec 和 WebVPN 隧道创建和管理连接特定记录的数据库。

tunnel-limit

要指定允许的最大活跃 GTP 隧道数，请在策略映射参数配置模式下使用 **tunnel limit** 命令。使用此命令的 **no** 形式将隧道限制设置回其默认值。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

语法说明

max_tunnels	允许的最大隧道数。该值相当于 PDP 情景或终端数量。

默认值

默认隧道限制为 500。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

达到此命令指定的隧道数后，新请求将被丢弃。

示例

以下示例为 GTP 流量指定最多 10,000 个隧道：

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

相关命令

命令	描述
clear service-policy inspect gtp	将清除全局 GTP 统计数据。
inspect gtp	适用于特定的 GTP 映射，以用于应用检查。
show service-policy inspect gtp	显示 GTP 配置。

tx-ring-limit

要指定优先级队列的深度，请在优先级队列模式下使用 **tx-ring-limit** 命令。要删除此指定，请使用此命令的 **no** 形式。

注 ASA 5580 万兆位以太网接口、ASA 5512-X 至 ASA 5555-X 管理接口或 ASA 服务模块不支持此命令。（万兆位以太网接口支持 ASA 5585-X 上的优先级队列。）

tx-ring-limit *number-of-packets*

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

语法说明

number-of-packets	指定在以太网传输驱动程序推回接口上的队列以让其缓冲数据包直到拥塞消除为止之前，允许进入该驱动程序的低延迟或正常优先级数据包最大数。范围为 3 至 511。

默认值

默认值为 511。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
优先级队列	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

ASA 允许两类流量：较高优先级的低延迟队列 (LLQ)，对延迟敏感的流量（例如语音和视频）；所有其他尽力而为的流量（默认）。ASA 会识别优先流量并执行适当的服务质量 (QoS) 策略。您可以配置的规模和深度优先级队列，以优化流量。

必须在优先级队列生效之前使用 **priority-queue** 命令为接口创建优先级队列。您可以将 **priority-queue** 命令应用于任何可由 **nameif** 命令定义的接口。

priority-queue 命令将进入优先级队列模式，如提示所示。在优先级队列模式中，可以配置传输队列中在任何指定时间允许的数据包最大数（**tx-ring-limit** 命令），以及在丢弃数据包之前允许缓冲的任一类（优先或尽力而为）数据包数（**queue-limit** 命令）。

Tx 环限制和您指定的队列限制影响较高的优先级低延迟队列和尽力服务队列。Tx 环限制是两种类型的允许进入驱动程序，驱动程序外推到坐在该接口的队列来告诉它们这些缓冲区数据包，直到拥塞清除之前的数据包数。通常情况下，您可以调整这两个参数，以优化低延迟流量的流动。

由于队列大小有限制，队列可以填满和溢出。如果队列已满，任何额外的数据包无法进入队列，并将丢弃。这是*丢弃的尾部*。以避免队列填充起来，您可以使用 **priority-queue** 命令以提高队列缓冲区大小。

注 用于 **queue-limit** 和 **tx-ring-limit** 命令的值范围上限在运行时动态确定。要查看此限制，请在命令行中输入 **help** 或 **?**。关键的决定因素是设备上支持的队列和可用的内存所需的内存。

对于 ASA 型号 5505 （仅限此型号），在一个接口配置优先级队列会覆盖所有其他接口上的相同配置。也就是说，所有接口上只存在上次应用的配置。此外，如果优先级队列配置从一个接口删除，就会从所有接口删除。

要解决此问题，请仅在一个接口上配置 **priority-queue** 命令。如果不同的接口需要 **queue-limit** 和/或 **tx-ring-limit** 命令的不同设置，请在任一接口上使用所有 queue-limit 的最大值和所有 tx-ring-limit 的最小值。

示例

以下示例配置优先级队列名为 test，指定 2048 数据包的队列限制和传输队列限制为 256 数据包的接口。

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

相关命令

命令	描述
clear configure priority-queue	指定接口的当前优先级队列配置中移除。
priority-queue	配置优先级队列。在接口上。
queue-limit	指定在优先级队列丢弃数据前可排入该队列的最大数据包数。
show priority-queue statistics	显示指定接口的优先级队列统计信息。
show running-config priority-queue	显示当前优先级队列配置。如果指定 **all** 关键字，此命令将显示所有当前的 **priority-queue**、**queue-limit** 和 **tx-ring-limit** 命令配置值。

type echo

要将 SLA 操作配置为回应响应时间探测操作，请在 SLA 监控配置模式下使用 **type echo** 命令。要从 SLA 配置删除类型，请使用此命令的 **no** 形式。

type echo protocol ipIcmpEcho *target* **interface** *if-name*

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

语法说明

interface *if-name*	如 **nameif** 命令所示，指定要用于发送回应请求数据包的接口名称。接口源地址用作回应请求数据包中的源地址。
protocol	协议关键字。唯一支持的值是 **ipIcmpEcho**，它指定对回应操作使用 IP/ICMP 回应请求。
target	监控的对象的 IP 地址或主机名。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
SLA 监控配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

ICMP 数据包的有效负载默认大小为 28 字节，会创建一个大小为 64 字节的总 ICMP 数据包。可以使用 **request-data-size** 命令更改有效负载的大小。

示例

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求/响应时间探测操作。它创建 ID 为 1 的跟踪条目来跟踪 SLA 的可达性。SLA 操作频率设置为 10 秒，阈值设置为 2500 毫秒而超时值设置为 4000 毫秒。

```
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
```

相关命令

命令	描述
num-packets	指定要在 SLA 操作期间发送的请求数据包数。
request-data-size	指定 SLA 操作请求数据包的有效负载大小。
sla monitor	定义 SLA 监控操作。

uc-ime 至 username-prompt 命令

uc-ime（已弃用）

要创建思科公司间媒体引擎代理实例，请在全局配置模式下使用 **uc-ime** 命令。要删除代理实例，请使用此命令的 **no** 形式。

uc-ime *uc-ime_name*

no uc-ime *uc-ime_name*

语法说明

uc-ime_name	指定在 ASA 中配置的思科公司间媒体引擎代理的实例名称。*名称*限制为 64 个字符。 ASA 中只能配置一个思科公司间媒体引擎代理。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.3(1)	添加了此命令。
9.4(1)	此命令已弃用。

使用指南

配置思科公司间媒体引擎代理。思科跨企业间媒体引擎支持公司使用 VoIP 技术提供的高级功能按需通过互联网进行互联。通过利用 P2P、安全和 SIP 协议在不同企业之间创建动态 SIP 中继，思科公司间媒体引擎可在不同企业的思科 Unified Communication Manager 集群之间实现企业到企业联盟。许多企业彼此协作，就像一个大型企业一样运作。

您必须创建媒体终端实例，然后才能在思科公司间媒体引擎代理中指定该实例。

ASA 中只能配置一个思科公司间媒体引擎代理。

示例

以下示例展示如何通过使用 **uc-ime** 命令配置思科公司间媒体引擎代理。

```
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
```

相关命令

命令	描述
fallback	配置思科公司间媒体引擎用于在连接完整性降级时从 VoIP 回退到 PSTN 的回退计时器。
show uc-ime	显示有关回退通知、映射服务会话和信令会话的统计数据或详细信息。
ticket	配置思科公司间媒体引擎代理的票证期限和密码。
ucm	配置思科公司间媒体引擎代理连接的思科 UCM。

ucm（已弃用）

要配置思科公司间媒体引擎代理连接哪个思科统一通信管理器 (UCM)，请在全局配置模式下使用 **ucm** 命令。要删除连接到思科公司间媒体引擎代理的思科 UCM，请使用此命令的 **no** 形式。

ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

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

语法说明

address	用于配置 Cisco Unified Communications Manager (UCM) IP 地址的关键字。
ip_address	指定思科 UCM 的 IP 地址。输入 IPv4 格式的 IP 地址。
nonsecure	指定思科 UCM 或思科 UCM 集群在非安全模式下运行。
secure	指定思科 UCM 或思科 UCM 集群在安全模式下运行。
trunk-security-mode	用于配置思科 UCM 或思科 UCM 集群安全模式的关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
UC-IME 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.3(1)	添加了此命令。
9.4(1)	此命令以及所有 **uc-ime** 模式命令均已弃用。

使用指南

指定企业中的思科 UCM 服务器。

您可以为思科公司间媒体引擎代理输入多条 **ucm** 命令。

注 在思科公司间媒体引擎启用了 SIP 中继的情况下，必须包括集群中每个思科 UCM 的条目。

为思科 UCM 或思科 UCM 集群指定 **secure** 表示思科 UCM 或思科 UCM 集群正在启动 TLS；因此，您必须设置为组件配置 TLS。

您可以在此任务中指定 **secure** 选项，也可以在稍后为企业配置 TLS 时进行更新。

企业内的 TLS 是指 ASA 所观测的思科公司间媒体引擎中继的安全状态。

如果思科公司间媒体引擎中继的传输安全在思科 UCM 中发生变化，则必须在自适应安全设备上也进行更改。不匹配将导致呼叫失败。自适应安全设备不支持使用不安全 IME 中继的 SRTP。自适应安全设备假设通过安全中继允许 SRTP。因此，如果使用 TLS，则必须检查允许的 SRTP 有无 IME 中继。ASA 支持 SRTP 回退到 RTP 进行安全 IME 中继呼叫。

代理位于企业边缘并检查在企业之间创建的 SIP 中继之间的 SIP 信令。它终止来自互联网的 TLS 信令，然后启动到思科 UCM 的 TCP 或 TLS。

传输层安全 (TLS) 是一种加密协议，为网络（如互联网）上的通信提供安全保护。TLS 在传输层端到端加密网络连接的网段。

如果内部网络中允许 TCP，则不需要执行此任务。

在本地企业内配置 TLS 的主要步骤如下：

- 在本地 ASA 中，为自签证书创建另一个 RSA 密钥和信任点。
- 在本地思科 UCM 和本地 ASA 之间导出和导入证书。
- 为 ASA 中的本地思科 UCM 创建信任点。

通过 TLS 进行身份验证：要使 ASA 可以充当代表 N 个企业的端口，思科 UCM 必须能够接受来自 ASA 的一个证书。由于思科 UCM 从证书提取主题名称，然后与安全配置文件中配置的名称进行比较，因此可通过将所有 UC-IME SIP 中继与同一 SIP 安全配置文件关联（该配置文件包含与 ASA 所显示相同的主题名称）来完成此操作。

示例

以下示例展示如何连接到 UCM 代理：

```
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
```

undebug

要禁用在当前会话中显示调试信息，请在特权 EXEC 模式下使用 **undebug** 命令。

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

语法说明

all	禁用所有调试输出。
command	禁用指定命令的调试。有关所支持命令的信息，请参阅“使用指南”。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• **是**	• **是**	• 是	• 是	• **是**

命令历史记录

版本	修改
7.0(1)	此命令已修改。包括了额外的 **debug** 关键字。

使用指南

以下命令可以与 **undebug** 命令一起使用。有关调试特定命令的详细信息，或特定 **debug** 命令的关联参数和关键字，请参阅 **debug** 命令的条目。

- aaa - AAA 信息
- acl - ACL 信息
- all - 所有调试
- appfw - 应用防火墙信息
- arp - ARP（包括 NP 运行）
- asdm - ASDM 信息
- auto-update - 自动更新信息
- boot-mem - 引导内存计算和设置
- cifs - CIFS 信息
- cmgr - CMGR 信息
- context - 情景信息
- cplane - CP 信息
- crypto - 加密信息
- ctiqbe - CTIQBE 信息

- ctl-provider - CTL 提供程序调试信息
- dap - DAP 信息
- dcerpc - DCERPC 信息
- ddns - 动态 DNS 信息
- dhcpc - DHCP 客户端信息
- dhcpd - DHCP 服务器信息
- dhcprelay - DHCP 中继信息
- disk - 磁盘信息
- dns - DNS 信息
- eap - EAP 信息
- eigrp - EIGRP 协议信息
- email - 邮件信息
- entity - 实体 MIB 信息
- eou - EAPoUDP 信息
- esmtp - ESMTP 信息
- fips - FIPS 140-2 信息
- fixup - 修复信息
- fover - 故障切换信息
- fsm - FSM 信息
- ftp - FTP 信息
- generic - 其他信息
- gtp - GTP 信息
- h323 - H323 信息
- http - HTTP 信息
- icmp - ICMP 信息
- igmp - 互联网组管理协议
- ils - LDAP 信息
- im - IM 检查信息
- imagemgr - 映像管理器信息
- inspect - 检查调试信息
- integrityfw - 完整性防火墙信息
- ip - IP 信息
- ipsec-over-tcp - IPsec over TCP 信息
- ipsec-pass-thru - 检查 ipsec-pass-thru 信息
- ipv6 - IPv6 信息
- iua-proxy - IUA 代理信息
- kerberos - KERBEROS 信息
- l2tp - L2TP 信息

- ldap - LDAP 信息
- mfib - 组播转发信息库
- mgcp - MGCP 信息
- module-boot - 服务模块引导信息
- mrib - 组播路由信息库
- nac-framework - NAC-FRAMEWORK 信息
- netbios-inspect - NETBIOS 检查信息
- npshim - NPSHIM 信息
- ntdomain - NT 域信息
- ntp - NTP 信息
- ospf - OSPF 信息
- p2p - P2P 检查信息
- parser - 解析器信息
- pim - 协议无关组播
- pix - PIX 信息
- ppp - PPP 信息
- pppoe - PPPoE 信息
- pptp - PPTP 信息
- radius - RADIUS 信息
- redundant-interface - 冗余接口信息
- rip - RIP 信息
- rtp - RTP 信息
- rtsp - RTSP 信息
- sdi - SDI 信息
- sequence - 添加序列号
- session-command - 会话命令信息
- sip - SIP 信息
- skinny - Skinny 信息
- sla - IP SLA 监视器调试
- Smtp-client - 电子邮件系统日志消息
- splitdns - 拆分 DNS 信息
- sqlnet - SQLNET 信息
- ssh - SSH 信息
- sunrpc - SUNRPC 信息
- tacacs - TACACS 信息
- tcp - 适用于 WebVPN 的 TCP
- tcp-map - TCP 映射信息
- timestamps - 添加时间戳

- track - 静态路由跟踪
- vlan-mapping - VLAN 映射信息
- vpn-sessiondb - VPN 会话数据库信息
- vpnlb - VPN 负载平衡信息
- wccp - WCCP 信息
- webvpn - WebVPN 信息
- xdmcp - XDMCP 信息
- xml - XML 解析器信息

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

示例

本示例禁用所有调试输出：

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

相关命令

命令	描述
debug	显示所选命令的调试信息。

unix-auth-gid

要设置 UNIX 组 ID，请在组策略 webvpn 配置模式下使用 **unix-auth-gid** 命令。要从配置中删除此命令，请使用此命令的 **no** 版本。

unix-auth-gid *identifier*

no storage-objects

语法说明

identifier	指定范围为 0 到 4294967294 之间的整数。

默认值

默认值为 65534。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
组策略 webvpn 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

该字符串指定网络文件系统 (NetFS) 位置。仅支持 SMB 和 FTP 协议；例如，smb://（NetFS 位置）或 ftp://（NetFS 位置）。您可在 **storage-objects** 命令中使用此位置的名称。

示例

以下示例将 UNIX 组 ID 设置为 4567：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 4567
```

相关命令

命令	描述
unix-auth-uid	设置 UNIX 用户 ID。

unix-auth-uid

要设置 UNIX 用户 ID，请在组策略 webvpn 配置模式下使用 **unix-auth-uid** 命令。要从配置中删除此命令，请使用此命令的 **no** 版本。

unix-auth-gid *identifier*

no storage-objects

语法说明

identifier	指定范围为 0 到 4294967294 之间的整数。

默认值

默认值为 65534。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
组策略 webvpn 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

该字符串指定网络文件系统 (NetFS) 位置。仅支持 SMB 和 FTP 协议；例如，smb://（NetFS 位置）或 ftp://（NetFS 位置）。您可在 **storage-objects** 命令中使用此位置的名称。

示例

以下示例将 UNIX 用户 ID 设置为 333：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 333
```

相关命令

命令	描述
unix-auth-gid	设置 UNIX 组 ID。

unsupported

要记录不直接受软件支持的 Diameter 元素，请在策略映射参数配置模式下使用 **unsupported** 命令。使用此命令的 **no** 形式删除设置。

unsupported {**application-id** | **avp** | **command-code**} **action log**

no unsupported {**application-id** | **avp** | **command-code**} **action log**

语法说明

application-id	记录其应用程序 ID 不直接受支持的 Diameter 消息。
avp	记录其中包含不直接受支持的“属性-值”对 (AVP) 的 Diameter 消息。
command-code	记录其中包含不直接受支持的命令代码的 Diameter 消息。

默认值

默认设置为允许这些元素而不对它们进行日志记录。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.5(2)	添加了此命令。

使用指南

配置 Diameter 检测策略映射时使用此命令。

这些选项指定该软件不直接支持的应用 ID、命令代码和 AVP。默认设置为允许这些元素而不对它们进行日志记录。您可以输入该命令三次以对所有元素启用日志记录。

示例

以下示例将记录所有不支持的应用 ID、命令代码和 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
```

相关命令

命令	描述
inspect diameter	启用 Diameter 检测。
policy-map type inspect diameter	创建 Diameter 检测策略映射。

upgrade rommon

要升级 ASA 5506-X 和 ASA 5508-X 系列安全设备，请在特权 EXEC 模式下使用 **upgrade rommon** 命令。

upgrade rommon [disk0 | disk1 | flash]:/[*path*] *filename*

语法说明

disk0:/[*path*/]*filename*	此选项表示内部闪存。您还可以使用 **flash** 代替 **disk0**；它们互为别名。
disk1:/[*path*/]*filename*	此选项表示外部闪存卡。
flash:/[*path*/]*filename*	此选项表示内部闪存卡；**flash** 是 **disk0:** 的别名。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.3(2)	添加了此命令。

使用指南

为该命令提供文件名后，该命令将验证文件并要求您确认升级。如果您有未保存的配置信息，系统将提示您在开始重新加载前保存该信息。如果您确认，ASA 将转至 ROMMON 并将开始升级过程。

示例

以下示例展示如何升级 ASA 5506-X 和 ASA 5508-X 系列安全设备：

```
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

注 **upload-max-size** 命令不起作用。不使用它。但是，此命令可能会显示在运行配置中，并可在 CLI 中使用。

要指定对象上传所允许的最大大小，请在组策略 webvpn 配置模式下使用 **upload-max-size** 命令。要从配置中删除该对象，请使用此命令的 **no** 版本。

upload-max-size *size*

no upload-max-size

语法说明

size	指定已上传的对象所允许的最大大小。范围为 0 到 2147483647。

默认值

默认大小为 2147483647。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略 webvpn 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

相关命令

命令	描述
post-max-size	指定要发布对象的最大大小。
webvpn	在组策略配置模式或用户名配置模式下使用。让您可以进入 WebVPN 模式以配置应用于组策略或用户名的参数。
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

srv-id

要在引用标识对象中配置 uri-id，请在 *ca-reference-identity* 模式下使用 **uri-id** 命令。要删除 uri-id in，请使用此命令的 **no** 形式。您可以通过先输入 **crypto ca reference-identity** 命令以配置引用标识对象，来访问 *ca-reference-identity* 模式。

srv-id *value*

no srv-id *value*

语法说明

value	每个引用 ID 的值。
srv-id	otherName 类型的 subjectAltName 条目，根据 RFC 4985 中的定义，其名称形式为 SRVName。SRV-ID 标识符可以同时包含域名和应用服务类型。例如，SRV-ID“_imaps.example.net”可以拆分为 DNS 域名部分“example.net”和应用服务类型部分“imaps”。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
ca-reference-identity	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.6(2)	我们引入了此命令。

使用指南

在创建引用标识后，可向或从引用标识中添加或删除四种类型的标识符及其相关联的值。

引用标识符可以包含标识应用服务的信息，并且必须包含标识 DNS 域名的信息。

示例

以下示例为系统日志服务器创建引用标识：

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

相关命令

命令	描述
crypto ca reference-identity	配置引用标识对象。
cn-id	配置引用标识对象中的通用名称标识符。
dns-id	配置引用标识对象中的 DNS 域名标识符。
uri-id	配置引用标识对象中的 URI 标识符。
logging host	配置可使用引用标识对象进行安全连接的日志记录服务器。
call-home profile destination address http	配置可使用引用标识对象进行安全连接的 Smart Call Home 服务器。

uri-non-sip

要识别 Alert-Info 和 Call-Info 报头字段中存在的非 SIP URI，请在参数配置模式下使用 **uri-non-sip** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

uri-non-sip action {**mask** | **log**} [**log**]

no uri-non-sip action {**mask** | **log**} [**log**]

语法说明

log	指定违规情况下的独立或附加日志。
mask	屏蔽非 SIP URI。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例展示如何识别 SIP 检查策略映射的 Alert-Info 和 Call-Info 报头字段中存在的非 SIP URI：

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

相关命令

命令	描述
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

url (crl configure)

要维护用于检索 CRL 的静态 URL 列表，请在 crl configure 配置模式下使用 **url** 命令。crl configure 配置模式可从 **crypto ca trustpoint** 配置模式进行访问。要删除现有的 URL，请使用此命令的 **no** 形式。

url *index url*

no url *index url*

语法说明

index	指定从 1 到 5 的值以确定列表中每个 URL 的等级。ASA 首先尝试位于索引 1 的 URL。
url	指定从其检索 CRL 的 URL。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Crl configure 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

您无法覆盖现有的 URL。要替换现有的 URL，请首先使用此命令的 **no** 形式删除该 URL。

示例

以下示例进入 crl 配置模式，设置索引 3 用于创建和维护 CRL 检索的 URL 列表，并配置 URL https://example.com 以从其检索 CRL：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

相关命令

命令	描述
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
policy	指定用于检索 CRL 的源。

url (saml idp)

要配置用于登录或注销的 SAML IdP URL，请在 saml idp 配置模式下使用 **url** 命令。您可以通过先输入 **webvpn** 命令来访问 saml idp 配置模式。要删除 URL，请使用此命令的 **no** 形式。

url {**sign-in** | **sign-out**} **value** *url*

no url *url*

语法说明

url	指定从其检索 CRL 的 URL。

默认值

没有默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Saml idp 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.5(2)	添加了此命令。

使用指南

您无法覆盖现有的 URL。要替换现有的 URL，请首先使用此命令的 **no** 形式删除该 URL。

url-block

要管理等待来自过滤服务器的过滤决策时用于网络服务器响应的 URL 缓冲区，请使用 **url-block** 命令。要删除配置，请使用此命令的 **no** 形式。

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*

语法说明

block *block_buffer*	创建 HTTP 响应缓冲区以存储等待来自过滤服务器的过滤决策时的网络服务器响应。允许的值从 1 到 128，该值指定 1550 字节数据块的数量。
mempool-size *memory_pool_size*	配置 URL 缓冲内存池的最大大小，以千字节 (KB) 为单位。允许的值从 2 到 10240，该值指定从 2 KB 到 10240 KB 的 URL 缓冲内存池。
url-size *long_url_size*	为每个缓冲的长 URL 配置允许的最大 URL 大小（以 KB 为单位）。指定最大 URL 大小的允许值：对于 Websense 为 2、3 或 4，表示 2 KB、3 KB 或 4 KB；对于 Secure Computing 为 2 或 3，表示 2 KB 或 3 KB。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

对于 Websense 过滤服务器，**url-block url-size** 命令可以过滤最长 4 KB 的长 URL。对于 Secure Computing，**url-block url-size** 命令可以过滤最长 3 KB 的长 URL。对于 Websense 和 N2H2 过滤服务器，**url-block block** 命令会导致 ASA 缓冲从网络服务器接收的数据包，以响应网络客户端请求，同时等待来自 URL 过滤服务器的响应。与丢弃数据包并且需要网络服务器在连接允许时重新传输数据包的默认 ASA 行为相比，这将提高网络客户端的性能。

如果您使用 **url-block block** 命令并且过滤服务器允许该连接，则 ASA 将数据块从 HTTP 响应缓冲区发送到网络客户端，然后从缓冲区中删除这些数据块。如果过滤服务器拒绝该连接，则 ASA 将拒绝消息发送到网络客户端，并从 HTTP 响应缓冲区中删除这些数据块。

使用 **url-block block** 命令以指定等待来自过滤服务器的过滤决策时用于缓冲网络服务器响应的数据块数量。

将 **url-block url-size** 命令与 **url-block mempool-size** 命令一起使用，以指定要过滤的最大 URL 长度和要分配给 URL 缓冲区的最大内存。使用这些命令可以将长度超过 1159 字节（最大长度可达 4096 字节）的 URL 传递给 Websense 或 Secure-Computing 服务器。**url-block url-size** 命令在缓冲区中存储长度超过 1159 字节的 URL，然后将该 URL 传递给 Websense 或 Secure-Computing 服务器（通过 TCP 数据包流），以便 Websense 或 Secure-Computing 服务器能够授予或拒绝该 URL 的访问权限。

示例

以下示例分配 56 个 1550 字节的数据块，以用于来自 URL 过滤服务器的缓冲响应：

```
ciscoasa#(config)# url-block block 56
```

相关命令

命令	描述
clear url-block block statistics	清除数据块缓冲区使用计数器。
filter url	将流量引导至 URL 过滤服务器。
show url-block	显示关于 URL 缓存的信息，该缓存在等待来自 N2H2 或 Websense 过滤服务器的响应时用于缓冲 URL。
url-cache	在来自 N2H2 或 Websense 服务器的响应挂起时，启用 URL 缓存并设置缓存的大小。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

url-cache

要为从 Websense 服务器接收的 URL 响应启用 URL 缓存和设置缓存的大小，请在全局配置模式下使用 **url-cache** 命令。要删除配置，请使用此命令的 **no** 形式。

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

语法说明

dst	根据 URL 目标地址缓存条目。如果所有用户在 Websense 服务器上共享相同的 URL 过滤策略，请选择此模式。
size *kbytes*	指定缓存大小的值，范围为 1 到 128 KB。
src_dst	基于发起 URL 请求的源地址以及 URL 目标地址缓存条目。如果用户没有在 Websense 服务器上共享相同的 URL 过滤策略，请选择此模式。
statistics	使用 **statistics** 选项以显示更多 URL 缓存统计信息，包括缓存查找数和命中率。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

url-cache 命令提供配置选项用于缓存来自 URL 服务器的响应。

使用 **url-cache** 命令以启用 URL 缓存、设置缓存的大小和显示缓存统计信息。

注 N2H2 服务器应用不支持此命令进行 URL 过滤。

缓存在 ASA 的内存中存储 URL 访问权限。主机请求连接时，ASA 首先在 URL 缓存中查找有无匹配的访问权限，而不是将请求转发到 Websense 服务器。使用 **no url-cache** 命令可禁用缓存。

注 如果您更改 Websense 服务器上的设置，则使用 **no url-cache** 命令禁用缓存，然后使用 **url-cache** 命令重新启用缓存。

使用 URL 缓存不会更新 Websense 协议版本 1 的 Websense 记帐日志。如果使用 Websense 协议版本 1，请运行 Websense 以累积日志，以便您能够查看 Websense 记帐信息。获得满足安全需求的使用配置文件后，启用 **url-cache** 以增加吞吐量。使用 **url-cache** 命令时，Websense 协议版本 4 URL 过滤的记帐日志将会更新。

示例

以下示例基于源和目标地址缓存所有出站 HTTP 连接：

```
ciscoasa(config)# url-cache src_dst 128
```

相关命令

命令	描述
clear url-cache statistics	从配置中删除 **url-cache** 命令语句。
filter url	将流量引导至 URL 过滤服务器。
show url-cache statistics	显示关于 URL 缓存的信息，该缓存用于从 Websense 过滤服务器接收的 URL 响应。
url-server	标识与 **filter** 命令一起使用的 Websense 服务器。

url-entry

要启用或禁用在门户页面上输入任何 HTTP/HTTPS URL 的功能，请在 dap webvpn 配置模式下使用 **url-entry** 命令。

url-entry enable | disable

enable | disable	启用或禁用浏览文件服务器或共享的功能。

默认值

没有默认值或行为。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Dap webvpn 配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

示例

以下示例展示如何为名为 Finance 的 DAP 记录启用 URL 条目：

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# url-entry enable
```

相关命令

命令	描述
dynamic-access-policy-record	创建 DAP 记录。
file-entry	启用或禁用输入要访问的文件服务器名称的功能。

url-length-limit

要配置 RTSP 消息中允许的最大 URL 长度，请在参数配置模式下使用 **url-length-limit** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此命令的 **no** 形式。

url-length-limit *length*

no url-length-limit *length*

语法说明

length	URL 长度限制（以字节为单位）。范围为 0 到 6000。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

示例

以下示例展示如何在 RTSP 检查策略映射中配置 URL 长度限制：

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

相关命令

命令	描述
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

url-list

要将 WebVPN 服务器和 URL 列表应用到特定用户或组策略，请在组策略 webvpn 配置模式下或在 username webvpn 配置模式下使用 **url-list** 命令。要删除列表，包括使用 **url-list none** 命令创建的空值，请使用此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。要阻止继承 url 列表，请使用 **url-list none** 命令。再次使用该命令将覆盖以前的设置。

url-list {**value** *name* | **none**} [*index*]

no url-list

语法说明

index	表示在主页上的显示优先级。
none	为 URL 列表设置一个空值。防止从默认或指定的组策略继承列表。
value *name*	指定以前配置的 URL 列表的名称。要配置此类列表，请在全局配置模式下使用 **url-list** 命令。

默认值

没有默认 URL 列表。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略 webvpn 配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

再次使用该命令将覆盖以前的设置。

您必须通过 XML 对象创建 URL 列表，然后才能在 webvpn 模式下使用 **url-list** 命令识别要在用户或组策略的 WebVPN 主页上显示的列表。在全局配置模式下使用 **import** 命令以将 URL 列表下载到安全设备。然后使用 url-list 命令以将列表应用到特定组策略或用户。

示例

以下示例对名为 FirstGroup 的组策略应用名为 FirstGroupURLs 的 URL 列表，并为其分配 URL 列表中的第一个位置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

相关命令

命令	描述
clear configure url-list	从配置中删除所有 url-list 命令。如果包含列表名称，则 ASA 仅删除该列表的命令。
show running-configuration url-list	显示当前配置的一组 **url-list** 命令。
webvpn	可让您进入 webvpn 模式。这可以是 webvpn 配置模式、组策略 webvpn 配置模式（用于配置特定组策略的 webvpn 设置）或 username webvpn 配置模式（用于配置特定用户的 webvpn 设置）。

url-server

要标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器，请在全局配置模式下使用 **url-server** 命令。要删除配置，请使用此命令的 **no** 形式。

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*]

语法说明

N2H2

connections	限制允许的最大 TCP 连接数。
num_conns	指定从安全设备到 URL 服务器创建的最大 TCP 连接数。由于此数值基于服务器，因此不同服务器可能有不同的连接值。
host *local_ip*	运行 URL 过滤应用的服务器。
if_name	（可选）身份验证服务器所在的网络接口。如果未指定，默认值为 inside。
port *number*	N2H2 服务器端口。ASA 还侦听此端口上的 UDP 回复。默认端口号为 4005。
protocol	协议可以使用 **TCP** 或 **UDP** 关键字进行配置。默认值是“TCP”。
timeout *seconds*	ASA 切换到您指定的下一服务器之前允许的最大空闲时间。默认值为 30 秒。
vendor	表示 URL 过滤服务，使用“smartfilter”或“n2h2”（为实现向后兼容性）；但“smartfilter”保存为供应商字符串。

Websense

connections	限制允许的最大 TCP 连接数。
num_conns	指定从安全设备到 URL 服务器创建的最大 TCP 连接数。由于此数值基于服务器，因此不同服务器可能有不同的连接值。
host *local_ip*	运行 URL 过滤应用的服务器。
if_name	身份验证服务器所在的网络接口。如果未指定，默认值为 inside。
timeout *seconds*	ASA 切换到您指定的下一服务器之前允许的最大空闲时间。默认值为 30 秒。
protocol	协议可以使用 **TCP** 或 **UDP** 关键字进行配置。默认值为 TCP 协议，版本 1。
vendor websense	指示 URL 过滤服务供应商为 Websense。
version	指定协议版本 **1** 或 **4**。默认值为 TCP 协议版本 1。TCP 可以使用版本 1 或版本 4 进行配置。UDP 只能使用版本 4 进行配置。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个 情景	系统
全局配置	• 是	-	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

url-server 命令指定运行 N2H2 或 Websense URL 过滤应用的服务器。限制为单情景模式下 16 台 URL 服务器和多情景模式下 4 台 URL 服务器；但您一次只能使用一种应用（N2H2 或 Websense）。此外，在 ASA 上更改您的配置不会更新应用服务器上的配置；此操作必须按照供应商的说明单独完成。

url-server 命令必须在发出针对 HTTPS 和 FTP 的 **filter** 命令之前进行配置。如果从服务器列表中删除所有 URL 服务器，则也将删除与 URL 过滤有关的所有 **filter** 命令。

指定服务器后，使用 **filter url** 命令启用 URL 过滤服务。

使用 **show url-server statistics** 命令以查看服务器统计信息，包括不可访问的服务器。

按照以下步骤操作以过滤 URL：

步骤 1 使用适当形式的供应商特定 **url-server** 命令，指定 URL 过滤应用服务器。

步骤 2 使用 **filter** 命令启用 URL 过滤。

步骤 3 （可选）使用 **url-cache** 命令启用 URL 缓存以改善已有的响应时间。

步骤 4 （可选）使用 **url-block** 命令启用长 URL 和 HTTP 缓冲支持。

步骤 5 使用 **show url-block block statistics**、**show url-cache statistics** 或 **show url-server statistics** 命令以查看运行信息。

有关通过 N2H2 过滤的详细信息，请访问 N2H2 网站，网址为：

http://www.n2h2.com

有关 Websense 过滤服务的详细信息，请访问以下网站：

http://www.websense.com/

示例

以下示例使用 N2H2 过滤所有出站 HTTP 连接，来自 10.0.2.54 主机的连接除外：

```
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
```

以下示例使用 Websense 过滤所有出站 HTTP 连接，来自 10.0.2.54 主机的连接除外：

```
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
```

相关命令

命令	描述
clear url-server	清除 URL 过滤服务器统计信息。
filter url	将流量引导至 URL 过滤服务器。
show url-block	显示关于 URL 缓存的信息，该缓存用于从 N2H2 或 Websense 过滤服务器接收的 URL 响应。
url-cache	在来自 N2H2 或 Websense 服务器的响应挂起时，启用 URL 缓存并设置缓存的大小。

urgent-flag

要通过 TCP 规范器允许或清除 URG 标志，请在 tcp-map 配置模式下使用 **urgent-flag** 命令。要删除此指定，请使用此命令的 **no** 形式。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

语法说明

allow	通过 TCP 规范器允许 URG 标志。
clear	通过 TCP 规范器清除 URG 标志。

默认值

默认情况下，紧急标志和紧急偏移将被清除。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Tcp-map 配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

将 **tcp-map** 命令与模块化策略框架基础设施结合使用。使用 **class-map** 命令定义流量类并使用 **tcp-map** 命令定制 TCP 检查。应用新 TCP 映射使用 **policy-map** 命令。使用 **service-policy** 命令激活 TCP 检查。

使用 **tcp-map** 命令进入 TCP 映射配置模式。在 tcp-map 配置模式下使用 **urgent-flag** 命令以允许紧急标志。

URG 标志用于指示数据包包含优先级高于流内其他数据的信息。TCP RFC 对 URG 标志的确切解释模糊不清；因此，终端系统以不同的方式处理紧急偏移，从而可能使终端系统易受攻击。默认行为是清除 URG 标志和偏移。

示例

以下示例展示如何允许紧急标志：

```
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
```

相关命令

命令	描述
class	指定要用于流量分类的类映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
set connection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 tcp-map 配置模式的访问。

user

要在支持身份防火墙功能的用户组对象中创建用户，请在 user-group object 配置模式下使用 **user** 命令。使用此命令的 **no** 形式可从对象中删除用户。

user [*domain_nickname*\]*user_name*

[no] user [*domain_nickname*\]*user_name*

语法说明

domain_nickname	（可选）指定要添加用户的域。
user_name	指定用户的名称。用户名可包含任意字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.]。如果用户名包含空格，您必须将名称包含在引号内。 使用 **user** 关键字指定的 *user_name* 参数包含 ASCII 用户名，因此不会指定 IP 地址。

默认值

如果没有指定 *domain_nickname* 参数，则用户在为身份防火墙功能配置的 LOCAL 域中创建。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
对象组用户配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

ASA 将 LDAP 查询发送到在 Active Directory 域控制器中全局定义的用户组的 Active Directory 服务器。ASA 将为身份防火墙功能导入这些组。但是，ASA 可能有未全局定义的本地化网络资源，从而需要采用本地化安全策略的本地用户组。本地用户组可包含从 Active Directory 导入的嵌套组和用户组。ASA 将合并本地和 Active Directory 组。用户可以属于本地用户组和从 Active Directory 导入的用户组。

ASA 最多支持 256 个用户组（包括导入的用户组和本地用户组）。

您可通过将用户组对象包含在访问组、捕获或服务策略中以进行激活。

在用户组对象内，您可以定义以下对象类型：

- **User** - 将单一用户添加到 object-group user。用户可以是 LOCAL 用户或导入的用户。

  导入用户的名称必须是唯一的 sAMAccountName，而不是可能不唯一的公用名称 (cn)。但是，有些 Active Directory 服务器管理员可能要求 sAMAccountName 和 cn 完全相同。在这种情况下，ASA 在 **show user-identity ad-group-member** 命令输出中显示的 cn 可用于通过用户对象定义的导入用户。

- **User-group** - 将通过外部目录服务器（例如 Microsoft Active Directory 服务器）定义的导入用户组添加到 group-object user。

  user-group 的组名称必须是唯一的 sAMAccountName，而不是可能不唯一的 cn。但是，有些 Active Directory 服务器管理员可能要求 sAMAccountName 和 cn 完全相同。在这种情况下，ASA 在 **show user-identity ad-group-member** 命令输出中显示的 cn 可在通过 **user-group** 关键字指定的 *user_group_name* 参数中使用。

  注 您可以在用户组对象中直接添加 *domain_nickname**user_group_name* 或 *domain_nickname**user_ name* 而无需首先在对象中指定它们。如果 *domain_nickname* 与 AAA 服务器关联，则用户对象组激活时，ASA 将外部目录服务器（例如 Microsoft Active Directory 服务器）中定义的详细嵌套用户组和用户导入到 ASA。

- **Group-object** - 将 ASA 上本地定义的组添加到 object-group user。

  注 在 object-group user 对象中包含 object-group 时，ASA 不会在访问组中扩展 object-group，即使您启用了 ACL 优化。**show object-group** 命令的输出不会显示命中数，该项在 ACL 优化启用时仅可用于普通的网络 object-group。

- **Description** - 添加 object-group user 的说明。

示例

以下示例展示如何将 **user** 命令与 **user-group object** 命令一起使用，以添加用户组对象中的用户，从而与身份防火墙功能一起使用：

```
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
```

相关命令

命令	描述
description	将说明添加到使用 **object-group user** 命令创建的组。
group-object	将本地定义的对象组添加到使用 **object-group user** 命令创建的用户对象组，以便与身份防火墙功能一起使用。
object-group user	创建用于身份防火墙功能的用户组对象。
user-group	将从 Microsoft Active Directory 导入的用户组添加到使用 **object-group user** 命令创建的组。
user-identity enable	创建思科身份防火墙实例。

user-alert

要通过当前活动会话启用到所有无客户端 SSL VPN 用户的紧急消息广播，请在特权 EXEC 模式下使用 **user-alert** 命令。要禁用该消息，请使用此命令的 **no** 形式。

user-alert *string cancel*

no user-alert

语法说明

cancel	取消弹出浏览器窗口启动。
string	一个字母数字。

默认值

无消息。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

当您发出此命令后，最终用户会看到弹出浏览器窗口及配置的消息。此命令不会导致 ASA 配置文件发生变化。

示例

以下示例展示如何启用 DAP 跟踪调试：

```
ciscoasa # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
ciscoasa #
```

user-authentication

要启用用户身份验证，请在组策略配置模式下使用 **user-authentication enable** 命令。要禁用用户分身份验证，请使用 **user-authentication disable** 命令。要从运行配置中删除用户身份验证属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承用户身份验证的值。

启用后，用户身份验证要求硬件客户端背后的个人用户进行身份验证，以获取通过隧道访问网络的权限。

user-authentication {**enable** | **disable**}

no user-authentication

语法说明

disable	禁用用户身份验证。
enable	启用用户身份验证。

默认值

用户身份验证已禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

个人用户按照身份验证服务器的配置顺序进行身份验证。

如果要求在主要 ASA 上进行用户身份验证，请务必在所有备用服务器上也进行配置。

示例

以下示例展示如何为名为“FirstGroup”的组策略启用用户身份验证：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication enable
```

相关命令

命令	描述
ip-phone-bypass	无需经过用户身份验证即可让 IP 电话连接。安全设备身份验证仍然有效。
leap-bypass	启用后，可让来自 VPN 客户端背后无线设备的 LEAP 数据包在用户身份验证之前穿越 VPN 隧道。这样就可让使用思科无线接入点设备的工作站建立 LEAP 身份验证。然后，它们将根据用户身份验证再次进行验证。
secure-unit-authentication	通过在客户端每次启动隧道时均要求 VPN 客户端使用用户名和密码进行身份验证，提供额外的安全性。
user-authentication-idle-timeout	设置各用户的空闲超时。如果在空闲超时期限内用户连接上没有通信活动，则 ASA 会终止该连接。

user-authentication-idle-timeout

要设置硬件客户端背后各用户的空闲超时，请在组策略配置模式下使用 **user-authentication-idle-timeout** 命令。要删除空闲超时值，请使用此命令的 **no** 形式。此选项允许从其他组策略继承空闲超时值。要阻止继承空闲超时值，请使用 **user-authentication-idle-timeout none** 命令。

如果在空闲超时期限内硬件客户端背后的用户没有通信活动，则 ASA 会终止该连接。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

语法说明

minutes	指定空闲超时期限的分钟数。范围为 1 到 35791394 分钟
none	允许无限制的空闲超时期限。使用空值设置空闲超时，从而禁止空闲超时。阻止从默认或指定组策略继承用户身份验证空闲超时值。

默认值

30 分钟.

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

最小值为 1 分钟，默认值为 30 秒，最大值为 10,080 分钟。

此计时器仅终止客户端通过 VPN 隧道进行的访问，而非终止 VPN 隧道本身。

响应 **show uauth** 命令所指示的空闲超时始终是思科简易 VPN 远程设备上进行隧道身份验证的用户的空闲超时值。

示例

以下示例展示如何为名为“FirstGroup”的组策略设置 45 分钟的空闲超时值：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication-idle-timeout 45
```

相关命令

命令	描述
user-authentication	要求硬件客户端背后的用户先对 ASA 确定自身身份，然后再进行连接。

user-group

要将从 Microsoft Active Directory 导入的用户组添加到使用 **object-group user** 命令创建的组，以与身份防火墙功能一起使用，请在 **user-group object** 配置模式下使用 **user-group** 命令。使用此命令的 **no** 形式可从对象中删除用户组。

user-group [*domain_nickname*\]*user_group_name*

[no] user-group [*domain_nickname*\]*user_group_name*

语法说明

domain_nickname	（可选）指定要在其中创建用户组的域。
user_group_name	指定用户组的名称。组名称可包含任意字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.]。如果组名称包含空格，您必须将名称包含在引号内。

默认值

如果没有指定 *domain_nickname* 参数，则用户组在为身份防火墙功能配置的 LOCAL 域中创建。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
对象组用户配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

ASA 将 LDAP 查询发送到在 Active Directory 域控制器中全局定义的用户组的 Active Directory 服务器。ASA 将为身份防火墙功能导入这些组。但是，ASA 可能有未全局定义的本地化网络资源，从而需要采用本地化安全策略的本地用户组。本地用户组可包含从 Active Directory 导入的嵌套组和用户组。ASA 将合并本地和 Active Directory 组。用户可以属于本地用户组和从 Active Directory 导入的用户组。

ASA 最多支持 256 个用户组（包括导入的用户组和本地用户组）。

您可通过将用户组对象包含在访问组、捕获或服务策略中以进行激活。

在用户组对象内，您可以定义以下对象类型：

- **User** - 将单一用户添加到 object-group user。用户可以是 LOCAL 用户或导入的用户。

  导入用户的名称必须是唯一的 sAMAccountName，而不是可能不唯一的公用名称 (cn)。但是，有些 Active Directory 服务器管理员可能要求 sAMAccountName 和 cn 完全相同。在这种情况下，ASA 在 **show user-identity ad-group-member** 命令输出中显示的 cn 可用于通过用户对象定义的导入用户。

- **User-group** - 将通过外部目录服务器（例如 Microsoft Active Directory 服务器）定义的导入用户组添加到 group-object user。

  用户组的组名称必须是唯一的 sAMAccountName，而不是可能不唯一的 cn。但是，有些 Active Directory 服务器管理员可能要求 sAMAccountName 和 cn 完全相同。在这种情况下，ASA 在 **show user-identity ad-group-member** 命令输出中显示的 cn 可在通过 **user-group** 关键字指定的 *user_group_name* 参数中使用。

  注 您可以在用户组对象中直接添加 *domain_nickname**user_group_name* 或 *domain_nickname**user_ name* 而无需首先在对象中指定它们。如果 *domain_nickname* 与 AAA 服务器关联，则用户对象组激活时，ASA 将外部目录服务器（例如 Microsoft Active Directory 服务器）中定义的详细嵌套用户组和用户导入到 ASA。

- **Group-object** - 将在 ASA 上本地定义的组添加到对象组用户。

  注 在 object group user 对象中包含对象组时，ASA 不会在访问组中扩展对象组，即使您启用了 ACL 优化。**show object-group** 命令的输出不会显示命中数，该项在 ACL 优化启用时仅可用于普通的网络对象组。

- **Description** - 添加 object group user 的说明。

示例

以下示例展示如何将 **user-group** 命令与 **user-group object** 命令一起使用，以添加用户组对象中的用户组，以便与身份防火墙功能一起使用：

```
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
```

相关命令

命令	描述
description	将说明添加到使用 **object-group user** 命令创建的组。
group-object	将本地定义的对象组添加到使用 **object-group user** 命令创建的用户对象组，以便与身份防火墙功能一起使用。
object-group user	创建用于身份防火墙功能的用户组对象。
user	将用户添加到使用 **object-group user** 命令创建的对象组。
user-identity enable	创建思科身份防火墙实例。

user-identity action ad-agent-down

要设置 Active Directory 代理无响应时思科身份防火墙实例的操作，请在全局配置模式下使用 **user-identity action ad-agent-down** 命令。要删除身份防火墙实例的这一操作，请使用此命令的 **no** 形式。

user-identity action ad-agent-down disable-user-identity-rule

no user-identity action ad-agent-down disable-user-identity-rule

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，此命令已禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

指定当 AD 代理不响应时的操作。

AD 代理关闭并且配置 **user-identity action ad-agent-down** 命令后，ASA 会禁用与该域中用户关联的用户身份规则。此外，该域中所有用户 IP 地址的状态在 **show user-identity user** 命令显示的输出中均标记为已禁用。

示例

以下示例展示如何启用身份防火墙的这一操作：

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity action domain-controller-down

要设置 Active Directory 域控制器关闭时思科身份防火墙实例的操作，请在全局配置模式下使用 **user-identity action domain-controller-down** 命令。要删除该操作，请使用此命令的 **no** 形式。

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**

语法说明

domain_nickname	指定身份防火墙的域名。

默认值

默认情况下，此命令禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

指定域由于 Active Directory 域控制器未响应而关闭时的操作。

域关闭并且配置 **disable-user-identity-rule** 关键字后，ASA 会禁用该域的用户身份-IP 地址映射。此外，该域中所有用户 IP 地址的状态在 **show user-identity user** 命令显示的输出中均标记为已禁用。

示例

以下示例展示如何配置身份防火墙的这一操作：

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity action mac-address-mismatch

要设置发现用户的 MAC 地址与 ASA 设备 IP 地址不一致时思科身份防火墙实例的操作，请在全局配置模式下使用 **user-identity action mac-address mismatch** 命令。要删除该操作，请使用此命令的 **no** 形式。

user-identity action mac-address mismatch remove-user-ip

no user-identity action mac-address mismatch remove-user-ip

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，ASA 在此命令指定时使用 **remove-user-ip**。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

指定当发现用户的 MAC 地址与当前映射到该 MAC 地址的 ASA 设备 IP 地址不一致时的操作。该操作用于禁用用户身份规则的影响。

配置 **user-identity action mac-address-mismatch** 命令后，ASA 会删除该客户端的用户身份-IP 地址映射。

示例

以下示例展示如何配置身份防火墙：

```
ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity action netbios-response-fail

要设置客户端未响应思科身份防火墙实例的 NetBIOS 探测时的操作，请在全局配置模式下使用 **user-identity action netbios-response-fail** 命令。要删除该操作，请使用此命令的 **no** 形式。

user-identity action netbios-response-fail remove-user-ip

no user-identity action netbios-response-fail remove-user-ip

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，此命令禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

指定客户端不响应 NetBIOS 探测时的操作。例如，该客户端的网络连接可能已被阻止或客户端处于不活动状态。

配置 **user-identity action remove-user-ip** 命令后，ASA 会删除该客户端的用户身份-IP 地址映射。

示例

以下示例展示如何配置身份防火墙：

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity aaa-server adagent

要定义用于思科身份防火墙实例的 AD 代理的服务器组，请在 AAA 服务器主机配置模式下使用 **user-identity ad-agent aaa-server** 命令。要删除该操作，请使用此命令的 **no** 形式。

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*

语法说明

aaa_server_group_tag	指定与身份防火墙关联的 AAA 服务器组。

默认值

此命令没有默认值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

aaa_server_group_tag 变量中定义的第一台服务器是主要 AD 代理，而定义的第二台服务器是辅助 AD 代理。

身份防火墙仅支持定义两台 AD 代理主机。

当 ASA 检测到主要 AD 代理关闭并且辅助代理已指定时，它会切换到辅助 AD 代理。AD 代理的 AAA 服务器使用 RADIUS 作为通信协议，并且应指定 ASA 与 AD 代理之间共享密钥的主要属性。

示例

以下示例展示如何定义用于身份防火墙的 AD 代理 AAA 服务器主机：

```
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity ad-agent active-user-database

要定义 ASA 如何从思科身份防火墙实例的 AD 代理检索用户身份-IP 地址映射信息，请在全局配置模式下使用 **user-identity ad-agent active-user-database** 命令。要删除配置，请使用此命令的 **no** 形式。

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

no user-identity ad-agent active-user-database {**on-demand** | **full-download**}

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，ASA 5505 使用 on-demand 选项。其他 ASA 平台使用 full-download 选项。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

定义 ASA 如何从 AD 代理检索用户身份 - IP 地址映射信息：

- **full-download** - 指定 ASA 在 ASA 启动时发送请求到 AD 代理以下载整个 IP-用户映射表，然后在用户登录和注销时接收增量 IP-用户映射。
- **on-demand** - 指定 ASA 在 ASA 接收需要新连接的数据包，并且其源 IP 地址的用户不在用户身份数据库中时，从 AD 代理检索 IP 地址的用户映射信息。

默认情况下，ASA 5505 使用 on-demand 选项。其他 ASA 平台使用 full-download 选项。

完整下载是由事件驱动的，这意味着下载数据库、仅将更新发送到用户身份-IP 地址映射数据库等后续请求。

ASA 向 AD 代理注册变更请求后，AD 代理会将新事件发送到 ASA。

示例

以下示例展示如何配置身份防火墙的这一选项：

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity ad-agent hello-timer

要定义 ASA 与思科身份防火墙实例的 AD 代理之间的计时器，请在全局配置模式下使用 **user-identity ad-agent hello-timer** 命令。要删除配置，请使用此命令的 **no** 形式。

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

no user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

语法说明

number	指定计时器的重试次数。
seconds	指定计时器的时长。

默认值

默认情况下，问候计时器设置为 30 秒和 5 次重试。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

定义 ASA 和 AD 代理之间的问候计时器。

ASA 与 AD 代理之间的问候计时器定义 ASA 交换问候数据包的频率。ASA 使用问候数据包以获得 ASA 复制状态（同步或不同步）和域状态（运行或关闭）。如果 ASA 没有收到来自 AD 代理的响应，它会在指定间隔后重新发送问候数据包。

默认情况下，问候计时器设置为 30 秒和 5 次重试。

示例

以下示例展示如何配置身份防火墙的这一选项：

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity ad-agent event-timestamp-check

要启用 RADIUS 事件时间戳检查以保护 ASA 免于授权重播更改攻击，请在全局配置模式下使用 **user-identity ad-agent event-timestamp-check** 命令。要删除配置，请使用此命令的 **no** 形式。

user-identity ad-agent event-timestamp-check

no user-identity ad-agent event-timestamp-check

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为已禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• **是**	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.1(5)	添加了此命令。

使用指南

此命令允许 ASA 跟踪其接收的每个标识符的上次事件时间戳；并在事件时间戳比 ASA 的时钟早至少 5 分钟，或其时间戳早于上次事件时间戳时丢弃所有消息。

对于新引导的 ASA，由于没有上次事件时间戳，因此 ASA 会将事件时间戳与自己的时钟进行比较。如果事件在至少 5 分钟之前发生，则 ASA 不会接受该消息。

注 我们建议您将 ASA、Active Directory 和 Active Directory 代理配置为使用 NTP 在彼此之间同步时钟。

示例

以下示例展示如何配置身份防火墙的事件时间戳检查：

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

相关命令

命令	描述
user-identity ad-agent hello-timer	定义 ASA 与思科身份防火墙实例的 AD 代理之间的计时器。

user-identity default-domain

要指定思科身份防火墙实例的默认域，请在全局配置模式下使用 **user-identity default-domain** 命令。要删除默认域，请使用此命令的 **no** 形式。

user-identity default-domain *domain_NetBIOS_name*

no user-identity default-domain *domain_NetBIOS_name*

语法说明

domain_NetBIOS_name	指定身份防火墙的默认域。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

对于 *domain_NetBIOS_name*，输入最多 32 个字符的名称，可包含 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.]，第一个字符不能是“.”和“ ”。如果域名包含空格，则将整个名称包含在引号内。域名不区分大小写。

当没有为所有用户或用户组明确配置域时，所有用户和用户组都使用默认域。未指定默认域时，用户和组的默认域为 LOCAL。对于多情景模式，您可以设置每个情景的默认域名，如同在系统执行空间内一样。

注 您指定的默认域名必须匹配 Active Directory 域控制器中配置的 NetBIOS 域名。如果域名不匹配，则 AD 代理将错误地把用户身份-IP 地址映射与配置 ASA 时您输入的域名关联。要查看 NetBIOS 域名，请在任意文本编辑器中打开 Active Directory 用户事件安全日志。

身份防火墙对所有本地定义的用户组或本地定义的用户使用 LOCAL 域。通过网络门户（直通代理）登录的用户被指定为属于其进行身份验证的 Active Directory 域。通过 VPN 登录的用户被指定为属于 LOCAL 域，除非 VPN 通过具有 Active Directory 的 LDAP 进行身份验证，这样身份防火墙便能够将用户与其 Active Directory 域关联。

示例

以下示例展示如何配置身份防火墙的默认域：

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity domain

要关联思科身份防火墙实例的域，请在全局配置模式下使用 **user-identity domain** 命令。要删除域关联，请使用此命令的 **no** 形式。

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

no user-identity *domain_nickname* **aaa-server** *aaa_server_group_tag*

语法说明

aaa_server_group_tag	指定与身份防火墙关联的 AAA 服务器组。
domain_nickname	指定身份防火墙的域名。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• **是**	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

将为导入用户组查询而为 AAA 服务器定义的 LDAP 参数与域名相关联。

对于 *domain_nickname*，输入最多 32 个字符的名称，可包含 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.]，第一个字符不能是“.”和“ ”。如果域名包含空格，您必须将空格字符包含在引号内。域名不区分大小写。

示例

以下示例展示如何关联身份防火墙的域：

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity enable

要创建思科身份防火墙实例，请在全局配置模式下使用 **user-identity enable** 命令。要禁用身份防火墙实例，请使用此命令的 **no** 形式。

user-identity enable

no user-identity enable

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

此命令将启用身份防火墙。

示例

以下示例展示如何启用身份防火墙：

```
ciscoasa(config)# user-identity enable
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity inactive-user-timer

要指定用户被思科身份防火墙实例视为空闲之前经过的时间量，请在全局配置模式下使用 **user-identity inactive-user-timer** 命令。要删除该计时器，请使用此命令的 **no** 形式。

user-identity inactive-user-timer minutes *minutes*

no user-identity inactive-user-timer minutes *minutes*

语法说明

minutes	指定用户被视为空闲之前经过的时间量，表示 ASA 在指定的时间量内未收到来自用户 IP 地址的流量。

默认值

默认情况下，空闲超时设置为 60 分钟。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

计时器过期后，用户的 IP 地址将标记为非活动状态，并将从本地缓存的用户身份-IP 地址映射数据库中删除，而 ASA 不再通知 AD 代理关于该 IP 地址删除的事宜。现有的流量仍允许通过。指定此命令后，ASA 将运行非活动计时器，即使已配置 NetBIOS 注销探测功能。

注 Idle Timeout 选项不适用于 VPN 或直通代理用户。

示例

以下示例展示如何配置身份防火墙：

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity logout-probe

要对思科身份防火墙实例启用 NetBIOS 探测，请在全局配置模式下使用 **user-identity logout-probe** 命令。要删除禁用探测，请使用此命令的 **no** 形式。

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**]

语法说明

minutes	指定两次探测之间的分钟数。
seconds	指定重试间隔的时长。
times	指定探测的重试次数。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

为将 NetBIOS 数据包的数量减至最少，ASA 仅当用户空闲超过指定的分钟数后将 NetBIOS 探测发送到客户端。

设置 NetBIOS 探测计时器（1 到 65535 分钟）和重试间隔（1 到 256 次重试）。指定探测的重试次数：

- **match-any** - 只要 NetBIOS 从包含分配到该 IP 地址的用户之用户名的客户端响应，用户身份即视为有效。指定此选项要求客户端启用 Messenger 服务并配置 WINS 服务器。
- **exact-match** - 分配到 IP 地址的用户之用户名在 NetBIOS 响应中必须唯一。否则，该 IP 地址的用户身份将被视为无效。指定此选项要求客户端启用 Messenger 服务并配置 WINS 服务器。
- **user-not-needed** - 只要 ASA 从客户端收到 NetBIOS 响应，用户身份即视为有效。

身份防火墙仅对用户身份处于活动状态并且位于至少一个安全策略中的用户执行 NetBIOS 探测。ASA 不对用户通过直通代理或使用 VPN 登录的客户端执行 NetBIOS 探测。

示例

以下示例展示如何配置身份防火墙：

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity monitor

对于云网络安全，要从 AD 代理下载指定的用户或组信息，请在全局配置模式下使用 user-identity monitor 命令。要停止监控，请使用此命令的 **no** 形式。

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*}

语法说明

object-group-user *object-group-name*	指定 **object-group user** 名称。该组可包含多个组。
user-group [*domain-name*\\] *group-name*	指定内嵌组名称。尽管您在域和组之间指定了 2 个反斜线 (\\)，但 ASA 会在将其发送到云网络安全时修改该名称以仅包含一个反斜线，从而符合云网络安全表示法约定。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

当您使用身份防火墙功能时，ASA 仅从 AD 服务器下载活动 ACL 中包含的用户和组的用户身份信息；ACL 必须在如访问规则、AAA 规则、服务策略规则等功能或被视为活动的其他功能中使用。由于云网络安全可将其策略基于用户身份，因此您可能需要下载并非活动 ACL 一部分的组，以获得所有用户的完全身份防火墙覆盖。例如，尽管您可以将云网络安全服务策略规则配置为使用具有用户和组的 ACL，从而激活任何相关组，但这并非必需；您可以完全基于 IP 地址使用 ACL。用户身份监控功能可让您从 AD 代理直接下载组信息。

ASA 最多只能监控 512 个组，包括配置用于用户身份监控的组和通过活动 ACL 进行监控的组。

示例

以下示例监控 CISCO\\Engineering 用户组：

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

相关命令

命令	描述
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和/或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置常规云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
show scansafe statistics	显示总计和当前 HTTP 连接数。
白名单	对流量类执行白名单操作。

user-identity poll-import-user-group-timer

要指定 ASA 查询 Active Directory 服务器以获得思科身份防火墙实例的用户组信息之前经过的时间量，请在全局配置模式下使用 **user-identity poll-import-user-group-timer** 命令。要删除该计时器，请使用此命令的 **no** 形式。

user-identity poll-import-user-group-timer hours *hours*

no user-identity poll-import-user-group-timer hours *hours*

语法说明

hours	设置轮询计时器的小时数。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

指定在 ASA 查询 Active Directory 服务器有关用户组信息之前的时间量。

如果在 Active Directory 组添加或删除用户，则 ASA 会在导入组计时器运行后收到更新的用户组。

默认情况下，轮询计时器为 8 小时。

要立即更新用户组信息，请输入 **user-identity update import-user** 命令：

示例

以下示例展示如何配置身份防火墙：

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity static user

要为思科身份防火墙功能创建新用户-IP 地址映射或将用户的 IP 地址设置为非活动状态，请在全局配置模式下使用 **user-identity static user** 命令。要删除身份防火墙的这一配置，请使用此命令的 **no** 形式。

user-identity static user [*domain*\] *user_name host_ip*

no user-identity static user [*domain*\] *user_name host_ip*

语法说明

domain	为指定域中的用户创建新用户-IP 地址映射或将 IP 地址设置为非活动状态。
host_ip	指定为其创建新用户-IP 地址映射或设置为非活动状态的用户的 IP 地址。
user_name	指定为其创建新用户-IP 地址映射或将其用户 IP 地址设置为非活动状态的用户的用户名。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.7(1)	引入了此命令。

使用指南

此命令没有使用指南。

示例

以下示例展示如何为 user1 创建静态映射。

```
ciscoasa(config)# user-identity static user SAMPLE\user1 192.168.1.101
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity update active-user-database

要从 Active Directory 代理下载完整的 active-user 数据库，请在全局配置模式下使用 **user-identity update active-user-database** 命令。

user-identity update active-user-database [**timeout minutes** *minutes*]

语法说明

minutes	指定超时的分钟数。

默认值

默认超时是 5 分钟。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

此命令从 Active Directory 代理下载完整的 active-user 数据库。

此命令将启动更新操作，生成起始更新日志并立即返回。更新操作完成或在计时器到期时中止后，将生成另一个系统日志消息。只允许一个未完成的更新操作。重新运行该命令将显示错误消息。

该命令完成运行后，ASA 将在命令提示符下显示 [已完成]，然后生成系统日志消息。

示例

以下示例展示如何启用身份防火墙的这一操作：

```
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
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity update import-user

要从 Active Directory 代理下载完整的 active-user 数据库，请在全局配置模式下使用 **user-identity update active-user-database** 命令。

user-identity update import-user [[*domain_nickname*\\] *user_group_name* [**timeout seconds** *seconds*]]

语法说明

domain_nickname	指定要更新的组的域。
seconds	指定超时的秒数。
user_group_name	指定 *user_group_name* 后，只更新指定的 import-user 组。只能更新激活的组（例如，访问组、访问列表、捕获或服务策略中的组）。 如果指定的组未激活，则此命令拒绝该操作。如果指定的组有多个级别的层次结构，则执行递归 LDAP 查询。 如果没有指定 *user_group_name*，则 ASA 立即启动 LDAP 更新服务并尝试定期更新所有激活的组。

默认值

ASA 最多重试更新 5 次，并在必要时生成警告消息。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• **是**	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

此命令通过立即查询 Active Directory 服务器而不等待轮询导入用户组计时器过期来更新指定的导入用户组数据库。没有用于更新本地用户组的命令，因为组 ID 数据库在每次本地用户组配置发生变化时都会更新。

此命令不会阻止控制台等待 LDAP 查询返回。

此命令将启动更新操作，生成起始更新日志并立即返回。更新操作完成或在计时器到期时中止后，将生成另一个系统日志消息。只允许一个未完成的更新操作。重新运行该命令将显示错误消息。

如果 LDAP 查询成功，则 ASA 将在本地数据库中存储检索的用户数据并相应地更改用户/组关联。如果更新操作成功，您可以运行 **show user-identity user-of-group** *domain**group* 命令列出该组下所有存储的用户。

ASA 在每次更新后检查所有导入的组。如果 Active Directory 中不存在激活的 Active Directory 组，则 ASA 会生成系统日志消息。

如果没有指定 *user_group_name*，则 ASA 立即启动 LDAP 更新服务并尝试定期更新所有激活的组。LDAP 更新服务在后台运行并通过 Active Directory 服务器上的 LDAP 查询定期更新导入用户组。

在系统启动时，如果访问组中定义了导入用户组，则 ASA 会通过 LDAP 查询检索用户/组数据。如果更新过程中发生错误，则 ASA 最多重试更新 5 次，并在必要时生成警告消息。

该命令完成运行后，ASA 将在命令提示符下显示 [已完成]，然后生成系统日志消息。

示例

以下示例展示如何启用身份防火墙的这一操作：

```
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
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-identity user-not-found

要对思科身份防火墙实例启用 user-not-found 跟踪，请在全局配置模式下使用 **user-identity user-not-found** 命令。要删除身份防火墙实例的这一跟踪，请使用此命令的 **no** 形式。

user-identity user-not-found enable

no user-identity user-not-found enable

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，此命令禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• **是**	• 是	• 是	-	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

只跟踪最后 1024 个 IP 地址。

示例

以下示例展示如何启用身份防火墙的这一操作：

```
ciscoasa(config)# user-identity user-not-found enable
```

相关命令

命令	描述
clear configure user-identity	清除身份防火墙功能的配置。

user-message

要指定选择 DAP 记录时显示的文本消息，请在 dynamic-access-policy-record 模式下使用 user-message 命令。要删除此消息，请使用此命令的 **no** 版本。如果对同一 DAP 记录多次使用该命令，则较新的消息会取代以前的消息。

user-message *message*

no user-message

语法说明

message	分配给此 DAP 记录的用户的消息。最多 128 个字符。如果消息包含空格，请将其包含在双引号内。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Dynamic-access-policy- record	• 是	• 是	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

对于成功的 SSL VPN 连接，门户页面将显示闪烁、可点击的图标，可让用户查看与连接关联的消息。如果连接通过 DAP 策略终止（操作 = 终止），并且该 DAP 记录中配置了用户消息，则该消息在登录屏幕上显示。

如果有多条 DAP 记录适用于一个连接，则 ASA 组合适用的用户消息并将其显示为单一字符串。

示例

以下示例展示如何为名为 Finance 的 DAP 记录设置用户消息“Hello Money Managers”。

```
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)#
```

相关命令

命令	描述
dynamic-access-policy-record	创建 DAP 记录。
show running-config dynamic-access-policy-record [*name*]	显示所有 DAP 记录或指定 DAP 记录正在使用的配置。

user-parameter

要指定 HTTP POST 请求参数（其中必须提交用户名以供 SSO 身份验证）的名称，请在 aaa-server-host 配置模式下使用 **user-parameter** 命令。

user-parameter *name*

注 要正确配置使用 HTTP 协议的 SSO，必须透彻地了解身份验证和 HTTP 协议交换的工作原理。

语法说明

string	HTTP POST 请求中包含的用户名参数的名称。最大名称大小为 128 个字符。

默认值

没有默认值或行为。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Aaa-server-host 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

使用指南

这是带有 HTTP Forms 命令的 SSO。ASA 的 WebVPN 服务器可使用 HTTP POST 请求向 SSO 服务器提交单点登录身份验证请求。所需命令 **user-parameter** 可指定 HTTP POST 请求必须包括用于 SSO 身份验证的用户名参数。

注 登录时，用户可输入实际名称值，该值将输入到 HTTP POST 请求中并传递给身份验证网络服务器。

示例

以下示例在 aaa-server-host 配置模式下输入，指定要将用户名参数 userid 包含在用于 SSO 身份验证的 HTTP POST 请求中：

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	描述
action-uri	指定要接收用于单点登录身份验证的用户名和密码的网络服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建用于与身份验证网络服务器交换的隐藏参数。
password-parameter	指定 HTTP POST 请求参数（其中必须提交用户密码以供 SSO 身份验证）的名称。
start-url	指定用于提取登录前 Cookie 的 URL。

user-statistics

要激活通过 MPF 收集用户统计信息和匹配身份防火墙的查找操作，请在 policy-map 配置模式下使用 **user-statistics** 命令。要删除收集的用户统计信息，请使用此命令的 **no** 形式。

user-statistics [**accounting** | **scanning**]

no user-statistics [**accounting** | **scanning**]

语法说明

accounting	（可选）指定 ASA 收集已发送数据包数、已发送丢包数和已接收数据包数。
scanning	（可选）指定 ASA 仅收集已发送丢包数。

默认值

默认情况下，此命令禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
策略映射配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.4(2)	添加了此命令。

使用指南

当配置策略映射以收集用户统计信息时，ASA 会收集所选用户的详细统计信息。当指定 **user-statistics** 命令而不带 **accounting** 或 **scanning** 关键字时，ASA 会收集记帐和扫描统计信息。

示例

以下示例展示如何激活身份防火墙的用户统计信息：

```
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
```

相关命令

命令	描述
policy-map	使用模块化策略框架时，将操作分配给您使用第 3/4 层类映射标识的流量。
service-policy(**global**)	在所有接口或目标接口上全局激活策略映射。
show service-policy [**user-statistics**]	当您对身份防火墙启用 user-statistics 扫描或记帐时，显示所配置服务策略的用户统计信息。
show user-identity ip-of-user [**detail**]	当您对身份防火墙启用 user-statistics 扫描或记帐时，显示指定用户 IP 地址的已接收数据包数、已发送数据包数和丢包数统计信息。
show user-identity user active [**detail**]	当您对身份防火墙启用 user-statistics 扫描或记帐时，显示指定时间段内活动用户的已接收数据包数、已发送数据包数和丢包数统计信息。
show user-identity user-of-ip [**detail**]	当您对身份防火墙启用 user-statistics 扫描或记帐时，显示指定 IP 地址用户的已接收数据包数、已发送数据包数和丢包数统计信息。
user-identity enable	创建身份防火墙实例。

user-storage

要在无客户端 SSL VPN 会话之间存储个性化的用户信息，请在组策略 webvpn 配置模式下使用 **user storage** 命令。要禁用用户存储，请使用该命令的 **no** 形式。

user-storage *NETFS-location*

no user-storage]

语法说明

NETFS-location	以 proto://user:password@host:port/path 形式指定文件系统目标 如果用户名和密码嵌入到 NETFS-location 中，则密码输入被视为明文。

默认值

用户存储已禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略 webvpn 模式	• 是	-	• **是**	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。
8.4(6)	阻止密码在 **show-run** 过程中以明文显示。

使用指南

User-storage 使您能够在 ASA 闪存以外的位置存储缓存的凭证和 cookie。此命令提供无客户端 SSL VPN 用户个人书签的单点登录。用户凭证以加密的格式在 FTP/CIFS/SMB 服务器中存储为不可解密的 <user_id>.cps 文件。

尽管用户名、密码和预共享密钥在配置中显示，但这不会带来安全风险，因为 ASA 使用内部算法以加密形式存储此信息。

如果数据在外部 FTP 或 SMB 服务器上加密，您可以通过选择添加书签在门户网页内定义个人书签（例如：user-storage cifs://jdoe:test@10.130.60.49/SharedDocs）。您也可以为所有插件协议创建个性化的 URL。

注 如果您有全部指向相同 FTP/CIFS/SMB 服务器并且使用相同“存储密钥”的 ASA 集群，则可以通过集群中的任何 ASA 访问书签。

示例

以下示例展示如何在名为 anyshare、路径为 anyfiler02a/new_share 的文件共享中为名为 newuser、密码为 12345678 的用户设置用户存储：

```
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)#
```

相关命令

命令	描述
storage-key	指定用于保护会话之间所存储数据的存储密钥。
storage-objects	配置两次会话之间所存储的数据的存储对象。

username

如要将用户添加到 ASA 本地数据库，请在全局配置模式下输入 **username** 命令。要删除用户，请将此命令的 **no** 版本与您要删除的用户名一起使用。

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*]

语法说明

encrypted	对于 9.6 及更早版本，表示已对包含 32 个和更少字符的密码进行加密（如果您未指定 **mschap**）。出于安全目的，当您在 **username** 命令中定义密码时，ASA 会在将密码保存到配置时创建 MD5 哈希。输入 **show running-config** 命令后，**username** 命令不会显示实际密码；它将显示加密的密码，后跟 **encrypted** 关键字。例如，如果您输入密码“test”，则 **show running-config** 命令输出将显示为类似以下内容： `username pat password rvEdRh0xPC8bel7s encrypted` 您在 CLI 实际输入 **encrypted** 关键字的唯一情况是您将配置剪切并粘贴到另一个 ASA 并且使用相同的密码。 在 9.7 及更高版本中，所有长度的密码均使用 PBKDF2。
mschap	指定密码在您输入后将转换为 Unicode 并使用 MD4 进行哈希加密。如果用户使用 MSCHAPv1 或 MSCHAPv2 进行身份验证，则使用此关键字。
name	将用户名称指定为长度介于 3 至 64 个字符的字符串（使用 ASCII 可打印字符的任意组合，空格和问号除外）。
nopassword	表示可为此用户输入*任意*密码。这是不安全的配置，因此请谨慎使用此关键字。 （9.6(2) 及更高版本）要创建没有密码的用户名，请不要输入 **password** 或 **nopassword** 关键字。例如，**ssh authentication** 命令允许您在 ASA 上安装公共密钥，并在 SSH 客户端上使用私有密钥，因此您可能不想配置任何密码。
nt-encrypted	表示密码已加密以与 MSCHAPv1 或 MSCHAPv2 一起使用。如果您在添加用户时指定了 **mschap** 关键字，则使用 **show running-config** 命令查看配置时，显示此关键字而不是 **encrypted** 关键字。 如果在 **username** 命令中定义了密码，则 ASA 会在将该密码保存到配置时会对其进行加密，以确保安全。输入 **show running-config** 命令后，**username** 命令不会显示实际密码；它将显示加密的密码，后跟 **nt-encrypted** 关键字。例如，如果您输入密码“test”，则 **show running-config** 显示内容将类似以下内容： `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` 您在 CLI 实际输入 **nt-encrypted** 关键字的唯一情况是您将配置剪切并粘贴到另一个 ASA 并且使用相同的密码。
password *password*	将密码设置为包含 3 至 32 个字符（9.5 及更早版本）或 127 个字符（9.6 及更高版本）的字符串，可以是 ASCII 可打印字符（字符代码 32-126）的任意组合，但是空格和问号除外。

pbkdf2	表示密码已加密。对于 9.6 及更早版本，仅当密码长度超过 32 个字符时，才使用 PBKDF2（基于密码的密钥派生函数 2）哈希。在 9.7 及更高版本中，所有密码均使用 PBKDF2。出于安全目的，当您在 **username** 命令中定义密码时，ASA 会在将密码保存到配置时创建 PBKDF2 哈希。输入 **show running-config** 命令后，**username** 命令不会显示实际密码；它将显示加密的密码，后跟 **pbkdf2** 关键字。例如，如果您输入一个长密码，则 **show running-config** 命令输出将类似以下内容： `username pat password rvEdRh0xPC8bel7s pbkdf2` 您在 CLI 实际输入 **pbkdf2** 关键字的唯一情况是您将配置剪切并粘贴到另一个 ASA 并且使用相同的密码。 请注意，现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。
privilege *priv_level*	将此用途的权限级别设置为 0 到 15（最低到最高）。默认特权级别为 2。此权限级别与命令授权一起使用。

默认值

默认特权级别为 2。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0.1	添加了此命令。
7.2(1)	添加了 **mschap** 和 **nt-encrypted** 关键字。
9.6(1)	密码长度已增加到 127 个字符，并且已添加了 **pbkdf2** 关键字。
9.6(2)	现在，您可以在不使用 **password** 或 **nopassword** 关键字的情况下创建用户名。
9.7(1)	现在，将使用 PBKDF2 哈希值将所有长度的密码保存到配置。

使用指南

login 命令使用此数据库进行身份验证。

如果您将可访问 CLI 的用户，以及您不希望其进入特权模式的用户添加到本地数据库，则您应启用命令授权。（请参阅 **aaa authorization command** 命令。)在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可使用 AAA 身份验证，以使用户无法使用 **login** 命令；也可将所有本地用户设置为 1 级，从而控制可使用 **enable** 密码访问特权 EXEC 模式的用户。

默认情况下，使用此命令添加的 VPN 用户没有属性或组策略关联。您必须使用 **username attributes** 命令显式配置所有值。

密码身份验证策略启用后，您无法再使用 **username** 命令更改自己的密码或删除自己的帐户。不过，您可以使用 **change-password** 命令更改密码。

要显示用户名密码日期，请使用 **show running-config all username** 命令。

示例

以下示例展示如何配置名为“anyuser”、密码为 12345678 且权限级别为 12 的用户：

```
ciscoasa(config)# username anyuser password 12345678 privilege 12
```

相关命令

命令	描述
aaa authorization command	配置命令授权。
clear config username	清除特定用户或所有用户的配置。
show running-config username	显示特定用户或所有用户的运行配置。
username attributes	进入可让您配置特定用户属性的用户名属性模式。
webvpn	进入您可以配置指定组 WebVPN 属性的 config-group-webvpn 模式。

username attributes

要进入用户名属性模式，请在用户名配置模式下使用 **username attributes** 命令。要删除特定用户的所有属性，请使用此命令的 **no** 形式并附加该用户名。要删除所有用户的所有属性，请使用此命令的 **no** 形式而不附加用户名。属性模式可让您配置特定用户的属性-值对。

username *name* **attributes**

no username *name* **attributes**

语法说明

name	提供用户的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
8.0(2)	添加了 **service-type** 属性。
9.1(2)	添加了 **ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} 属性。

使用指南

内部用户身份验证数据库包含使用 **username** 命令输入的用户。**login** 命令使用此数据库进行身份验证。您可以使用 **username** 命令或 **username attributes** 命令配置用户名属性。

用户名配置模式的命令语法有以下共同特征：

- **no** 形式从运行配置中删除属性。
- **none** 关键字也从运行配置中删除属性。但它通过将属性设置为空值，从而阻止继承来实现此功能。
- 布尔型属性有用于启用和禁用设置的显式语法。

username attributes 命令进入用户名属性模式，您可在该模式下配置以下任意属性：

属性	功能
group-lock	命名用户需要连接的现有隧道组。
password-storage	启用或禁用在客户端系统中存储登录密码。

属性	功能
service-type [**remote-access** | **admin** | **nas-prompt**]	限制控制台登录，以及允许分配相应级别的用户登录。**remote-access** 选项指定远程访问的基本 AAA 服务。**admin** 选项指定 AAA 服务、登录控制台权限、EXEC 模式权限、启用权限和 CLI 权限。**nas-prompt** 选项指定 AAA 服务、登录控制台权限、EXEC 模式权限，但没有启用权限。
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	基于每个用户启用公共密钥身份验证。*key* 参数的值可以引用以下内容： • 提供 *key* 参数且未指定哈希标记时，密钥值必须是通过能够生成 SSH-RSA 原始密钥（即无证书）的 SSH 密钥生成软件生成的 base64 编码公共密钥。提交 base64 编码的公共密钥后，该密钥随即通过 SHA-256 进行哈希加密，并将相应的 32 位哈希值用于所有进一步的比较。 • 提供 *key* 参数且哈希标记已指定时，密钥值必须事先采用 SHA-256 进行哈希加密并且长度为 32 字节，每个字节以冒号分隔（用于解析目的）。 **pkf** 选项使您能够使用 4096 位 RSA 密钥作为 SSH 公共密钥文件 (PKF) 进行身份验证。此选项并非限制为 4096 位 RSA 密钥，而是可使用小于或等于 4096 位 RSA 密钥的任何大小。 **nointeractive** 选项在导入 SSH 公共密钥格式的密钥时抑制所有提示。此非交互式数据输入模式仅供 ASDM 使用。 *key* 字段和 **hashed** 关键字仅对 **publickey** 选项可用，而 **nointeractive** 关键字仅对 **pkf** 选项可用。 当您保存配置时，哈希加密的密钥值将保存到该配置并在 ASA 重新引导时使用。 **注** 您可以在故障切换启用时使用 PKF 选项，但 PKF 数据不会自动复制到备用系统。您必须输入 **write standby** 命令以将 PKF 设置同步到故障切换对中的备用系统。
vpn-access-hours	指定配置的 time-range 策略的名称。
vpn-filter	指定用户特定 ACL 的名称。
vpn-framed-ip-address	指定要分配给客户端的 IP 地址和网络掩码。
vpn-group-policy	指定从其继承属性的组策略的名称。
vpn-idle-timeout [**alert-interval**]	指定空闲超时期限（以分钟为单位），或指定 **none** 以禁用。可以选择指定超时前警报间隔。
vpn-session-timeout [**alert-interval**]	指定最长用户连接时间（以分钟为单位），或指定 **none** 表示无限时间。可以选择指定超时前警报间隔。
vpn-simultaneous-logins	指定允许同时登录的最大数量。
vpn-tunnel-protocol	指定允许的隧道协议。
webvpn	进入可在其中配置 WebVPN 属性的用户名 webvpn 配置模式。

您可以通过在用户名 webvpn 配置模式下输入 **username attributes** 命令，然后输入 **webvpn** 命令，配置用户名的 webvpn-mode 属性。有关详细信息，请参阅 **webvpn** 命令（组策略属性和用户名属性模式）。

示例

以下示例展示如何为名为“anyuser”的用户进入用户名属性配置模式：

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)#
```

相关命令

命令	描述
clear config username	清除用户名数据库。
show running-config username	显示特定用户或所有用户的运行配置。
username	将用户添加到 ASA 数据库。
webvpn	进入您可以配置指定组 WebVPN 属性的 webvpn 配置模式。

username-from-certificate

要指定证书中的字段用作授权用户名，请在 tunnel-group general-attributes 模式下使用 **username-from-certificate** 命令。对等证书的 DN 用作授权用户名

要从配置中删除属性并还原默认值，请使用此命令的 **no** 形式。

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

语法说明

primary-attr	指定用于获得从证书进行授权查询的用户名的属性。如果启用了 pre-fill-username，则获得的名称也可在身份验证查询中使用。
secondary-attr	（可选）指定与主要属性一起使用的附加属性，用于得出进行身份验证或从数字证书进行授权查询的用户名。如果启用了 pre-fill-username，则获得的名称也可在身份验证查询中使用。
use-entire-name	指定 ASA 必须使用完整主题 DN (RFC1779) 得出从数字证书进行授权查询的名称。
use-script	指定使用 ASDM 生成的脚本文件从证书提取 DN 字段用作用户名。

默认值

主要属性的默认值为 CN（公用名称）。

辅助属性的默认值为 OU（组织单位）。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
隧道组常规属性配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(4)	添加了此命令。

使用指南

此命令选择证书中的字段用作用户名。它在版本 8.0(4) 和后续版本中取代弃用的 **authorization-dn-attributes** 命令。**username-from-certificate** 命令强制安全设备使用指定的证书字段作为用户名/密码授权的用户名。

要在证书功能的预填充用户名中使用这一得出的用户名进行用户名/密码身份验证或授权，您还必须在 tunnel-group webvpn-attributes 模式下配置 **pre-fill-username** 命令。也就是说，要使用预填充用户名功能，您必须配置两条命令。

主要和辅助属性可能的值包括：

属性	定义
C	国家/地区：两个字母的国家/地区缩写。这些代码符合 ISO 3166 国家/地区缩写。
CN	公用名称：人员、系统或其他实体的名称。不可用作辅助属性。
DNQ	域名限定符。
EA	邮件地址。
GENQ	辈分词。
GN	名字。
I	首字母缩写。
L	区域：组织所在的城市或城镇。
N	名称。
O	组织：公司、机构、办事处、协会或其他实体的名称。
OU	组织单位：组织 (O) 内的子组。
SER	序列号。
SN	姓氏。
SP	省/自治区/直辖市：组织所在的省/自治区/直辖市
T	职位。
UID	用户标识符。
UPN	用户主体名称。
use-entire-name	使用完整 DN 名称。不可用作辅助属性。
use-script	使用 ASDM 生成的脚本文件。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的 IPsec 远程访问隧道组，指定使用 CN（公用名称）作为主要属性和 OU 作为辅助属性，用于得出从数字证书进行授权查询的名称：

```
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)#
```

以下示例展示如何修改隧道组属性以配置预填充用户名。

```
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
```

相关命令

命令	描述
pre-fill-username	启用预填充用户名功能。
show running-config tunnel-group	显示指示的隧道组配置。
tunnel-group general-attributes	指定命名的隧道组的常规属性。

username password-date

要使系统能够在启动时，或将文件复制到运行配置时恢复密码创建日期，请在非交互配置模式下输入 **username pasword-date** 命令；换句话说，仅当启动已包含此命令的配置文件时，此命令才可用；您不能在 CLI 提示符下输入此命令。

username *name* **password-date** *date*

语法说明

name	将用户名称指定为长度介于 3 至 64 个字符的字符串（使用 ASCII 可打印字符的任意组合，空格和问号除外）。
date	使系统能够在引导过程中读取用户名时恢复密码创建日期。如果不存在，则密码日期设置为当前日期。日期为 mmm-dd-yyyy 格式。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
非交互	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.1(2)	添加了此命令。

使用指南

要显示用户名密码日期，请使用 **show running-config all username** 命令。

不能从 CLI 提示符中输入 **username password-date** 值。仅当密码策略生命周期非零时，密码日期才会保存到启动配置。这意味着密码日期仅当配置密码过期后才会保存。您不能使用 **username password-date** 命令来阻止用户更改密码创建日期。

相关命令

命令	描述
aaa authorization command	配置命令授权。
clear config username	清除特定用户或所有用户的配置。
show running-config username	显示特定用户或所有用户的运行配置。
username attributes	进入可让您配置特定用户属性的用户名属性模式。
webvpn	进入您可以配置指定组 WebVPN 属性的 config-group-webvpn 模式。

username-prompt

要定制在 WebVPN 用户连接到安全设备时向其显示的 WebVPN 页面登录框的用户名提示，请在 webvpn 定制模式下使用 **username-prompt** 命令：要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

语法说明

text	指示您正在更改文本。
style	指示您正在更改样式。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

默认值

用户名提示的默认文本是“USERNAME:”。

用户名提示的默认样式为 color:black;font-weight:bold;text-align:right。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
WebVPN 定制	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

使用指南

style 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查询位于 www.w3.org 的万维网联盟 (W3C) 网站上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

示例

在以下示例中，文本更改为“Corporate Username:”，默认样式随字体粗细变粗后更改：

```
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
```

相关命令

命令	描述
group-prompt	定制 WebVPN 页面的组提示。
password-prompt	定制 WebVPN 页面的密码提示信息。

Validate-attribute 至 vxlan port 命令

validate-attribute

要在使用 RADIUS 记账时验证 RADIUS 属性，请使用 **inspect validate attribute** 命令访问 radius-accounting 参数配置模式，然后在该模式下使用 **validate attribute** 命令。

默认情况下该选项处于禁用状态。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

语法说明

attribute_number	使用 RADIUS 记账时要验证的 RADIUS 属性。值范围为 1-191。不支持供应商特定属性。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Radius-accounting 参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

配置此命令后，除了 Framed IP 属性，安全设备还会对这些属性进行匹配。此命令允许有多个实例。

您可以从以下位置找到 RADIUS 属性类型列表：

http://www.iana.org/assignments/radius-types

示例

以下示例展示如何启用用户名 RADIUS 属性的 RADIUS 记账：

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate attribute 1
```

相关命令

命令	描述
inspect radius-accounting	设置 RADIUS 记账的检查。
parameters	设置检查策略映射的参数。

validate-key

要为 LISP 消息指定预共享密钥，请在参数配置模式下使用 **validate-key** 命令。您可以通过先输入 **policy-map type inspect lisp** 命令来访问参数配置模式。要删除密钥，请使用此命令的 **no** 形式。

validate-key *key*

no validate-key *key*

语法说明

key	为 LISP 消息指定预共享密钥。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.5(2)	添加了此命令。

使用指南

指定 LISP 预共享密钥，以便 ASA 可以读取 LISP 消息内容。

关于集群流移动性的 LISP 检测

ASA 检测 LISP 流量是否发生位置更改，然后使用此信息进行无缝集群操作。如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

集群流移动性包含多种相互关联的配置：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。请参阅 **policy-map type inspect lisp**、**allowed-eid** 和 **validate-key** 命令。
2. LISP 流量检查 - ASA 检查 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。请参阅 **inspect lisp** 命令。
3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。请参阅 **cluster flow-mobility lisp** 命令。

4. 站点 ID - ASA 使用每个集群设备的站点 ID 确定新的所有者。请参阅 **site-id** 命令。
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。请参阅 **flow-mobility lisp** 命令。

示例

以下示例将 EID 限制为 10.10.10.0/24 网络上的 EID，并指定预共享密钥：

```
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
```

相关命令

命令	描述
allowed-eids	基于 IP 地址限制检测到的 EID。
clear cluster info flow-mobility counters	清除流移动性计数器。
clear lisp eid	从 ASA EID 表中删除 EID。
cluster flow-mobility lisp	为服务策略启用流移动性。
flow-mobility lisp	为集群启用流移动性。
inspect lisp	检测 LISP 流量。
policy-map type inspect lisp	定制 LISP 检测。
site-id	为集群机箱设置站点 ID。
show asp table classify domain inspect-lisp	显示 LISP 检测的 ASP 表。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show lisp eid	显示 ASA EID 表。
show service-policy	显示服务策略。

validation-policy

要指定在何种条件下可使用信任点验证与传入的用户连接相关联的证书，请在 crypto ca trustpoint 配置模式下使用 **validation-policy 命令**。要指定不能对指定条件使用信任点，请使用此命令的 **no** 形式。

[no] validation-policy {ssl-client | ipsec-client} [no-chain] [subordinate-only]

语法说明

ipsec-client	指定与信任点相关联的证书颁发机构 (CA) 证书和策略可用于验证 IPsec 连接。
no-chain	禁用不在安全设备上的辅助证书链。
ssl-client	指定与信任点相关联的证书颁发机构 (CA) 证书和策略可用于验证 SSL 连接。
subordinate-only	禁用对直接从此信任点代表的 CA 颁发的客户端证书的验证。

默认值

没有默认值或行为。

命令模式

下表展示可输入命令的模式：

命令历史记录

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Crypto ca trustpoint 配置	• 是	• 是	• 是	• 是	-

版本	修改
8.0(2)	添加了此命令。

使用指南

远程访问 VPN 可根据部署要求使用安全套接字层 (SSL) VPN、IP 安全 (IPsec) 或同时使用两者，以允许对几乎所有网络应用或资源的访问。**validation-policy** 命令可指定允许访问自注册 CA 证书的协议类型。

此命令带 **no-chain** 选项时可阻止 ASA 支持未配置为其信任点的辅助 CA 证书。

ASA 可以对同一 CA 有两个信任点，这会造成同一 CA 有两个不同身份证书。如果使用该信任点向已与另一个启用此功能的信任点相关联的 CA 进行验证，则此选项将自动禁用。这样可防止在选择路径验证参数时产生混淆。如果用户尝试在已向与另一个信任点关联的 CA 进行过身份验证且启用了此功能的信任点上激活此功能，则不允许进行该操作。不能有两个信任点都启用此设置并向同一 CA 进行身份验证。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并将其指定为 SSL 信任点：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

以下示例进入 checkin1 信任点的 crypto ca trustpoint 配置模式，并将其设置为接受从属于指定信任点的证书。

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	描述
crypto ca trustpoint	进入 trustpoint 配置模式。
id-usage	指定如何使用信任点的注册身份。
ssl trust-point	指定表示接口的 SSL 证书的证书信任点。

validation-usage

要指定此信任点的验证允许的使用类型，请在 crypto ca trustpoint 配置模式下使用 **validation-usage** 命令。要不指定使用类型，请使用此命令的 **no** 形式。

validation-usage ipsec-client | ssl-client | ssl-server

no validation-usage ipsec-client | ssl-client | ssl-server

语法说明

ipsec-client	表示可使用此信任点验证 IPsec 客户端连接。
ssl-client	表示可使用此信任点验证 SSL 客户端连接。
ssl-server	表示可使用此信任点验证 SSL 服务器证书。

默认值

ipsec-client、ssl-client

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Crypto ca trustpoint 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	已添加此命令以取代 client-types 命令。

使用指南

当同一个 CA 证书关联多个信任点时，只能为某特定客户端类型配置其中一个信任点。但可以为一个客户端类型配置其中一个信任点，而为另一个客户端类型配置其他信任点。

如果有已使用某客户端类型配置的与同一个 CA 证书相关联的信任点，则不允许使用相同的客户端类型设置配置新的信任点。此命令的 **no** 形式会清除设置，使信任点无法用于任何客户端验证。

远程访问 VPN 可根据部署要求使用安全套接字层 (SSL) VPN、IP 安全 (IPsec) 或同时使用两者，以允许访问所有网络应用或资源。

相关命令

命令	描述
crypto ca trustpoint	进入指定信任点的 crypto ca trustpoint 配置模式。

vdi

要使运行在移动设备上的 Citrix Receiver 应用通过 ASA 安全地远程访问 XenApp 和 XenDesktop VDI 服务器，请使用 **vdi** 命令。

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

语法说明

domain *domain*	登录到虚拟化基础设施服务器的域。此值可以是无客户端宏。
password *password*	登录到虚拟化基础设施服务器的密码。此值可以是无客户端宏。
type	VDI 的类型。对 Citrix Receiver 类型，该值必须为 *citrix*。
url *url*	XenApp 或 XenDesktop 服务器的完整 URL 包括 HTTP 或 HTTPS、主机名和端口号，以及 XML 服务的路径。
username *username*	登录到虚拟化基础设施服务器的用户名。此值可以是无客户端宏。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Webvpn 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

在 VDI 模型中，管理员发布预装企业应用的桌面，最终用户可远程访问这些桌面。这些虚拟化资源的呈现和任何其他资源（例如邮件）一样，因此，用户不需要通过 Citrix 访问网关来访问它们。用户使用 Citrix Receiver 移动客户端登录到 ASA，然后 ASA 连接到预定义的 Citrix XenApp 或 XenDesktop 服务器。管理员必须在组策略下配置 Citrix 服务器的地址和登录凭证，这样，当用户连接到其 Citrix 虚拟化资源时，他们输入 ASA 的 SSL VPN IP 地址和凭证，而非指向 Citrix 服务器的地址和凭证。当 ASA 验证凭证后，接收方客户端开始通过 ASA 检索已授权的应用。

支持的移动设备

- iPad - Citrix Receiver 4.x 或更高版本
- iPhone/iTouch - Citrix Receiver 4.x 或更高版本
- Android 2.x 手机 - Citrix Receiver 2.x 或更高版本
- Android 3.x 平板电脑 - Citrix Receiver 2.x 或更高版本
- Android 4.0 手机 - Citrix Receiver 2.x 或更高版本

示例

如果用户名和组策略都已配置，则用户名设置优先于组策略。

```
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>]
```

相关命令

命令	描述
debug webvpn citrix	深入了解启动基于 Citrix 的应用和桌面的过程。

verify

要检验文件的校验和，请在特权 EXEC 模式下使用 **verify** 命令。

verify *path*

verify {**/md5** | **sha-512**} *path* [*expected_value*]

verify /signature running

语法说明

/md5	计算并显示指定软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。
/sha-512	计算并显示指定软件映像的 SHA-512 值。将此值与 Cisco.com 上此映像的可用值进行比较。
/signature running	验证运行中 ASA 映像的签名。
expected_value	（可选）指定的映像的已知哈希值。ASA 将显示一条消息，验证哈希值是否匹配或是否存在不匹配情况。
path	• **disk0:/**[*path*/]*filename* 表示内部闪存。您还可以使用 **flash** 代替 **disk0**；它们互为别名。 • **disk1:/**[*path*/]*filename* 表示外部闪存卡。 • **flash:/**[*path*/]*filename* 此选项表示内部闪存卡。**flash** 是 **disk0:** 的别名。 • **ftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*] **type** 可以是以下关键字之一： – **ap** - ASCII 被动模式 – **an** - ASCII 正常模式 – **ip** -（默认）二进制被动模式 – **in** - 二进制正常模式 • **http**[**s**]**://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename* • **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;int=***interface_name*] 如果要覆盖到服务器地址的路由，请指定接口名称。 路径名不能包含空格。如果路径名有空格，则在 **tftp-server** 命令而不是 **verify** 命令中设置路径。 • **system:running-config** 计算或验证运行中配置的哈希值。 • **system:text** 计算或验证 ASA 进程文本的哈希值。

默认值

当前的闪存设备是默认文件系统。

注 指定 **/md5** 或 **/sha-512** 选项时，您可以使用网络文件（例如来自 FTP、HTTP 或 TFTP 的文件）作为源。不带 **/md5** 或 **/sha-512** 选项的 **verify** 命令仅允许验证闪存中的本地映像。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	-	• 是

命令历史记录

版本	修改
7.2(1)	添加了此命令。
9.3(2)	添加了 **signature** 关键字。
9.6(2)	添加了 **system:text** 选项。

使用指南

使用 **verify** 命令验证文件的校验和，然后再使用文件。

分布在磁盘上的每个软件映像对整个映像使用单个校验和。当映像复制到闪存中时才显示此校验和；当映像文件从一个磁盘复制到另一个磁盘时，不会显示。

在加载或复制新的映像之前，记录映像的校验和与 MD5 信息，以便当您将映像复制到闪存中或服务器上时可验证校验和。Cisco.com 上提供多种映像信息。

要显示闪存的内容，请使用 **show flash** 命令。闪存的内容列表不包含各个文件的校验和。要重新计算和验证映像复制到闪存后的校验和，请使用 **verify** 命令。但请注意，当文件保存到文件系统之后，**verify** 命令才检查其完整性。损坏的映像可能会传输到 ASA 并保存在文件系统中，不进行检测。如果损坏的映像成功传输到 ASA，则软件无法识别映像已损坏，而文件将成功验证。

要使用消息摘要 5 (MD5) 散列算法确保文件验证，请使用带 **/md5** 选项的 **verify** 命令。MD5 是一种通过创建唯一的 128 位消息摘要来验证数据完整性的算法（在 RFC 1321 中定义）。**verify** 命令的 **/md5** 选项通过将映像的 MD5 校验和值与该映像的已知 MD5 校验和值进行比较，检查 ASA 软件映像的完整性。目前 Cisco.com 提供了所有安全设备软件映像的 MD5 值，以供与本地系统映像值进行比较。您也可以指定 SHA-512 (**/sha-512**)。

要执行 MD5 或 SHA-512 完整性检查，请使用 **/md5** 或 **/sha-512** 关键字执行 **verify** 命令。例如，执行 **verify /md5 flash:cdisk.bin** 命令将计算并显示软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。

或者，您可以先从 Cisco.com 获取 MD5 值，然后在命令语法中指定此值。例如，执行 **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** 命令将显示验证 MD5 值匹配或不匹配的消息。MD5 值不匹配表示映像已损坏或输入了错误的 MD5 值。

示例

以下示例展示对名为 cdisk.bin 的映像文件执行 **verify** 命令的情况。为清楚起见，某些文字已删除：

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

以下示例展示对 disk0 中的签名映像执行 **verify** 命令的情况：

```
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:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f0599
7fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

相关命令

命令	描述
copy	复制文件。
dir	列出系统中的文件。

verify-header

要仅允许已知的 IPv6 扩展报头并实施 IPv6 扩展报头的顺序，请在参数配置模式下使用 **verify-header** 命令。您可以通过先输入 **policy-map type inspect ipv6** 命令来访问参数配置模式。要禁用这些参数，请使用此命令的 **no** 形式。

verify-header {**order** | **type**}

no verify-header {**order** | **type**}

语法说明

order	按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。
type	仅允许已知的 IPv6 扩展报头。

命令默认

默认情况下，order 和 type 均启用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
参数配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
8.2(1)	添加了此命令。

使用指南

默认情况下，这些参数均启用。要禁用它们，请输入关键字 no。

示例

以下示例对 IPv6 检查策略映射禁用 order 和 type 参数：

```
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
```

相关命令

命令	描述
inspect ipv6	启用 IPv6 检查。
parameters	进入检查策略映射的参数配置模式。
policy-map type inspect ipv6-	创建 IPv6 检查策略映射。

版本

要指定 ASA 全局使用的 RIP 版本，请在路由器配置模式下使用 **version** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

version {**1** | **2**}

no version

语法说明

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

默认值

ASA 接受版本 1 和版本 2 数据包，但只发送版本 1 数据包。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
路由器配置	• 是	-	• 是	-	-

命令历史记录

版本	**修改**
7.2(1)	添加了此命令。

使用指南

您可以通过在接口上输入 **rip send version** 和 **rip receive version** 命令，基于每个接口覆盖全局设置。如果您指定 RIP 第 2 版，您可以启用邻居身份验证和使用基于 MD5 加密进行身份验证的 RIP 更新。

示例

以下示例配置 ASA 以发送和接收所有接口上的 RIP 版本 2 数据包：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
```

相关命令

命令	**描述**
rip send version	指定要从特定的接口发送更新时使用的 RIP 版本。
rip receive version	指定要接受时接收更新特定接口上的 RIP 版本。
router rip	启用 RIP 路由过程和路由器配置模式下输入此过程。

virtual http

要配置虚拟 HTTP 服务器，请在全局配置模式下使用 **virtual http** 命令。要禁用虚拟服务器，请使用此命令的 **no** 形式。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

语法说明

ip_address	设置 ASA 上虚拟 HTTP 服务器的 IP 地址。确保此地址是路由到 ASA 且未使用的地址。
warning	（可选）通知用户 HTTP 连接需要重定向到 ASA。此关键字仅适用于基于文本的浏览器，在这些浏览器中无法自动执行重定向。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	此命令已弃用，因为在先前版本中使用的内嵌基本 HTTP 身份验证的方法被重定向方法取代；不再需要此命令。
7.2(2)	重新启用了此命令，因为您现在可以选择使用基本 HTTP 身份验证（默认），或使用利用 **aaa authentication listener** 命令的 HTTP 重定向。重定向方法无需对层叠 HTTP 身份验证使用额外的命令。

使用指南

当您在 ASA 上使用 HTTP 身份验证（请参阅 **aaa authentication match** 或 **aaa authentication include** 命令）时，ASA 默认使用基本 HTTP 身份验证。您可以更改身份验证方法，从而让 ASA 将 HTTP 连接重定向到 ASA 自身使用带 **redirect** 关键字的 **aaa authentication listener** 命令生成的网页。

但是，如果您继续使用基本 HTTP 身份验证，则当您有层叠 HTTP 身份验证时，可能需要执行 **virtual http** 命令。

如果目标 HTTP 服务器除了 ASA 还需要身份验证，则 **virtual http** 命令可以分别使用 ASA（通过 AAA 服务器）和使用 HTTP 服务器进行身份验证。如果没有虚拟 HTTP，则使用 ASA 进行身份验证所用的同一个用户名和密码会发送给 HTTP 服务器；不会单独提示您输入 HTTP 服务器用户名和密码。假设 AAA 和 HTTP 服务器的用户名和密码不同，则 HTTP 身份验证会失败。

此命令将所有要求 AAA 身份验证的 HTTP 连接重定向到 ASA 上的虚拟 HTTP 服务器。ASA 提示输入 AAA 服务器用户名和密码。在 AAA 服务器对用户进行身份验证后，ASA 将 HTTP 连接重定向回原始服务器，但不包含 AAA 服务器用户名和密码。由于 HTTP 数据包中不包含用户名和密码，HTTP 服务器会单独提示用户输入 HTTP 服务器用户名和密码。

对于入站用户（从较低安全性到较高安全性），还必须包括虚拟 HTTP 地址作为应用到源接口的访问列表中的目标接口。此外，必须对虚拟 HTTP IP 地址添加 **static** 命令，即使不需要 NAT（使用 **no nat-control** 命令）。通常使用身份 NAT 命令（将地址转换为本身）。

对于出站用户，对流量有显式许可，但如果将访问列表应用于内部接口，要确保允许访问虚拟 HTTP 地址。不需要 **static** 语句。

注 在使用 **virtual http** 命令时，不要将 **timeout uauth** 命令持续时间设置为 0 秒，因为这会阻止 HTTP 连接到真正的网络服务器。

示例

以下示例展示如何启用虚拟 HTTP 及 AAA 身份验证：

```
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+
```

相关命令

命令	描述
aaa authentication listener http	设置 ASA 进行身份验证的方法
clear configure virtual	从配置中删除 **virtual** 命令语句。
show running-config virtual	显示 ASA 虚拟服务器的 IP 地址。
sysopt uauth allow-http-cache	当您启用 **virtual http** 命令时，此命令可使用浏览器缓存中的用户名和密码重新连接到虚拟服务器。
virtual telnet	提供 ASA 上的虚拟 Telnet 服务器以让用户通过 ASA 进行身份验证，然后再启动要求进行身份验证的其他类型的连接。

virtual telnet

要配置 ASA 上的虚拟 Telnet 服务器，请在全局配置模式下使用 **virtual telnet** 命令。如果您需要对 ASA 不提供身份验证提示的其他类型流量进行身份验证，可能需要使用虚拟 Telnet 服务器对用户进行身份验证。要禁用服务器，请使用此命令的 **no** 形式。

virtual telnet *ip_address*

no virtual telnet *ip_address*

语法说明

ip_address	设置 ASA 上的虚拟 Telnet 服务器的 IP 地址。确保此地址是路由到 ASA 且未使用的地址。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

虽然您可以配置任何协议或服务的网络访问身份验证（请参阅 **aaa authentication match** 或 **aaa authentication include** 命令），但您只能直接使用 HTTP、Telnet 或 FTP 进行身份验证。用户首先必须使用这些服务之一进行身份验证，然后才允许需要身份验证的其他流量通过。如果不想允许 HTTP、Telnet 或 FTP 通过 ASA，但要对其他类型流量进行身份验证，您可以配置虚拟 Telnet；用户通过 Telnet 连接到 ASA 上配置的给定 IP 地址，ASA 提供 Telnet 提示。

您必须配置到虚拟 Telnet 地址的 Telnet 访问以及要使用 **authentication match** 或 **aaa authentication include** 命令进行身份验证的其他服务。

当未经身份验证的用户连接到虚拟 Telnet IP 地址时，将要求用户输入用户名和密码，然后由 AAA 服务器对其进行身份验证。进行身份验证后，用户会看到“身份验证成功”消息。然后，用户可以成功访问要求进行身份验证的其他服务。

对于入站用户（从较低安全性到较高安全性），还必须包括虚拟 Telnet 地址作为应用到源接口的访问列表中的目标接口。此外，必须对虚拟 Telnet IP 地址添加 **static** 命令，即使不需要 NAT（使用 **no nat-control** 命令）。通常使用身份 NAT 命令（将地址转换为本身）。

对于出站用户，对流量有显式许可，但如果将访问列表应用于内部接口，要确保允许访问虚拟 Telnet 地址。不需要 **static** 语句。

要从 ASA 注销，请重新连接到虚拟 Telnet IP 地址；将会提示您注销。

示例

以下示例展示如何启用虚拟 Telnet 以及其他服务的 AAA 身份验证：

```
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+
```

相关命令

命令	描述
clear configure virtual	从配置中删除 **virtual** 命令语句。
show running-config virtual	显示 ASA 虚拟服务器的 IP 地址。
virtual http	当使用 ASA 上的 HTTP 身份验证时，HTTP 服务器还需要进行身份验证，此命令可让您分别使用 ASA 和 HTTP 服务器进行身份验证。如果没有虚拟 HTTP，则使用 ASA 进行身份验证所用的同一个用户名和密码会发送给 HTTP 服务器；不会单独提示您输入 HTTP 服务器用户名和密码。

vlan（组策略）

要将 VLAN 分配给组策略，请在组策略配置模式下使用 **vlan** 命令。要从组策略配置中删除 VLAN 并使用默认组策略的 VLAN 设置替换它，请使用此命令的 **no** 形式。

[**no**] **vlan** {*vlan_id* |**none**}

语法说明

none	禁止将 VLAN 分配到与此组策略匹配的远程访问 VPN 会话。组策略不会从默认组策略继承 vlan 值。
vlan_id	VLAN 编号（十进制格式），分配到使用此组策略的远程访问 VPN 会话。必须在接口配置模式下使用 **vlan** 命令配置在此 ASA 上的 VLAN。

默认值

默认值为 none。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.0(2)	添加了此命令。

使用指南

此命令指定分配给此组策略的会话的传出 VLAN 接口。ASA 将此组上的所有流量转发到该 VLAN。您可以将 VLAN 分配到每个组策略以简化访问控制。使用此命令作为使用 ACL 过滤会话上流量的替代方案。

请勿将 VoIP 检测引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS 检查引擎或 DCE RPC 检查引擎与 vlan mapping 选项一起使用。这些检测引擎将忽略 vlan 映射设置，这可能会导致错误地路由数据包。

示例

以下命令将 VLAN 1 分配给组策略：

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

以下命令从组策略中删除 VLAN 映射：

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

相关命令

命令	描述
show vlan	显示在 ASA 上配置的 VLAN。
vlan（接口配置模式）	将 VLAN ID 分配给子接口。
show vpn-session_summary.db	显示 IPsec、Cisco AnyConnect、NAC 会话数和正在使用的 VLAN 数量。
show vpn-session.db	显示有关 VPN 会话的信息，包括 VLAN 映射和 NAC 结果。

vlan (interface)

要将 VLAN ID 分配给子接口，请在接口配置模式下使用 **vlan** 命令。要删除 VLAN ID，请使用此命令的 **no** 形式。子接口需要 VLAN ID 传递流量。VLAN 子接口允许您在单个物理接口上配置多个逻辑接口。VLAN 可以单独在特定的物理接口上保持流量（例如对于多个安全情景）。

vlan *id* [**secondary** *vlan_range*]

no vlan [**secondary** *vlan_range*]

语法说明

id	指定一个介于 1 和 4094 之间的整数。某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。
secondary *vlan_range*	（可选）指定一个或多个辅助 VLAN。*vlan_id* 是介于 1 和 4094 之间的整数。某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。 可以使用空格、逗号和连字符（适用于连续范围）分隔辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 是	• 是	-	• 是

命令历史记录

版本	修改
7.0(1)	此命令已从 **interface** 命令的关键字转变为接口配置模式命令。
9.5(2)	我们添加了 **secondary** 关键字。

使用指南

可以配置主 VLAN，以及一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 上的流量时，它会将该流量映射到主 VLAN。每个子接口必须有一个 VLAN ID，然后才能传递流量。要更改 VLAN ID，您无需使用 **no** 选项删除旧 VLAN ID；您可以输入带有不同 VLAN ID 的 **vlan** 命令，ASA 会更改旧的 ID。要从列表中删除某些辅助 VLAN，可以使用 **no** 命令，并仅列出要删除的 VLAN。可以仅有选择地删除列出的 VLAN；例如，不能删除某一范围中的单个 VLAN。

您需要使用 **no shutdown** 命令启用物理接口，从而让子接口也启用。如果启用了子接口，您通常不想让物理接口传递流量，因为物理接口会传递未标记的数据包。因此，您无法通过关闭物理接口阻止流量通过物理接口。相反，不加 **nameif** 命令可确保物理接口不传递流量。如果要让物理接口传递未标记的数据包，您可以照常配置 **nameif** 命令。

子接口的最大数量根据具体平台而异。请参阅CLI 配置指南以获取每个平台的子接口最大数量。

示例

以下示例将 VLAN 101 分配给子接口：

```
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
```

以下示例将 VLAN 更改为 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
```

以下示例将一组辅助 VLAN 映射到 VLAN 200：

```
interface gigabitethernet 0/6.200
    vlan 200 secondary 500 503 600-700
```

以下示例将从列表中删除辅助 VLAN 503：

```
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
```

以下示例显示 VLAN 映射如何与 Catalyst 6500 配合使用。请查看 Catalyst 6500 配置指南，了解如何将节点连接到 PVLANS。

ASA 配置

```
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 配置

```
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
!
```

相关命令

命令	描述
allocate-interface	将接口和子接口分配至安全情景。
Interface	配置接口并进入接口配置模式。
show running-config interface	显示接口的当前配置。

vpdn group

要创建或编辑 VPDN 组和配置 PPPoE 客户端设置，请在全局配置模式下使用 **vpdn group** 命令。要从配置中删除组策略，请使用此命令的 **no** 形式。

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**}}

注 如果在 ASA 上配置故障切换，或在多情景模式或透明模式下，则不支持 PPPoE。仅在单个路由模式下没有故障切换时才支持 PPPoE。

语法说明

localname *username*	将用户名链接到 VPDN 组以进行身份验证，且必须匹配使用 **vpdn username** 命令配置的名称。
**ppp authentication {chap | mschap | pap}}	指定点对点协议 (PPP) 身份验证协议。通过 Windows 客户端拨号网络设置，可指定使用哪种身份验证协议（PAP、CHAP 或 MS-CHAP）。您在客户端上指定的所有内容必须匹配您在安全设备上使用的设置。密码身份验证协议 (PAP) 可让 PPP 对等设备相互进行身份验证。PAP 以明文形式传递主机名或用户名。质询握手身份验证协议 (CHAP) 可让 PPP 对等设备通过与访问服务器交互来阻止未授权的访问。MS-CHAP 是 Microsoft 针对 CHAP 的派生项。PIX 防火墙仅支持 MS-CHAP 版本 1（不是版本 2.0）。 如果未指定主机上的身份验证协议，不要在您的配置中指定 **ppp authentication** 选项。
request dialout pppoe	指定为允许拨出 PPPoE 请求。
vpdn group *group_name*	指定 vpdn 组的名称

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是		-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

虚拟专用拨号网络 (VPDN) 用于提供远程拨入用户和专用网络之间的长途点对点连接。安全设备上的 VDPN 使用第 2 层隧道技术 PPPoE 建立从远程用户跨公共网络到专用网络的拨号网络连接。

PPPoE 是基于以太网的点对点协议 (PPP)。PPP 专为配合使用网络层协议（例如 IP、IPX 和 ARA）而设计。PPP 还有 CHAP 和 PAP 作为内置安全机制。

show vpdn session pppoe 命令显示 PPPOE 连接的会话信息。**clear configure vpdn group** 命令从配置中删除所有 **vpdn group** 命令并停止所有活动的 L2TP 和 PPPoE 隧道。**clear configure vpdn username** 命令从配置中删除所有 **vpdn username** 命令。

由于 PPPoE 封装 PPP，PPPoE 依赖于 PPP 对 VPN 隧道中运行的客户端会话执行身份验证以及 ECP 和 CCP 功能。此外，由于 PPP 分配 PPPoE 的 IP 地址，因此 PPPoE 不支持与 DHCP 同时使用。

注 除非配置了 PPPoE 的 VPDN 组，否则 PPPoE 无法建立连接。

要定义用于 PPPoE 的 VPDN 组，请使用 **vpdn group** *group_name* **request dialout pppoe** 命令。然后在接口配置模式下使用 **pppoe client vpdn group** 命令，以将 VPDN 组关联到特定接口上的 PPPoE 客户端。

如果您的 ISP 需要身份验证，请使用 **vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} 命令选择您的 ISP 使用的身份验证协议。

使用 **vpdn group** *group_name* **localname** *username* 将您的 ISP 分配的用户名关联到 VPDN 组。

使用 **vpdn username** *username* password *password* 命令创建 PPPoE 连接的用户名和密码对。用户名必须是已关联到 PPPoE 指定的 VPDN 组的用户名。

注 如果您的 ISP 使用 CHAP 或 MS-CHAP，用户名可以为远程系统名称，密码可以为 CHAP 密钥。

默认情况下 PPPoE 客户端功能关闭，因此配置 VPDN 后，使用 **ip address** *if_name* **pppoe** [**setroute**] 命令启用 PPPoE。如果不存在默认路由，**setroute** 选项会创建一条默认路由。

配置 PPPoE 后，安全设备会尝试查找 PPPoE 接入集中器以进行通信。如果 PPPoE 连接终止，无论是正常还是异常终止，ASA 都会尝试查找新接入集中器进行通信。

PPPoE 会话启动后，不要使用以下 **ip address** 命令，因为它们会终止 PPPoE 会话：

- **ip address outside pppoe**，因为它试图启动一个新的 PPPoE 会话。
- **ip address outside dhcp**，因为它禁用接口，直到接口获取其 DHCP 配置。
- **ip address outside** *address netmask*，因为它将接口启用为正常初始化接口。

示例

以下示例创建一个 vdpn 组 *telecommuters* 并配置 PPPoE 客户端：

```
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
```

相关命令

命令	描述
clear configure vpdn group	从配置中删除所有 vpdn group 命令。
clear configure vpdn username	从配置中删除所有 vpdn username 命令。

命令	描述
show vpdn group *group_name*	显示 VPDN 组配置。
vpdn username	创建 PPPoE 连接的用户名和密码对。

vpdn username

要创建 PPPoE 连接的用户名和密码对，请在全局配置模式下使用 **vpdn username** 命令。

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

注 如果在 ASA 上配置故障切换，或在多情景模式或透明模式下，则不支持 PPPoE。仅在单个路由模式下没有故障切换时才支持 PPPoE。

语法说明

password	指定密码。
store-local	将用户名和密码存储在安全设备上 NVRAM 中的特殊位置。如果自动更新服务器将 clear config 命令发送到安全设备并且连接随后中断，则安全设备可以从 NVRAM 读取用户名和密码，并向访问集中器进行身份验证。
username	指定用户名。

默认值

无默认行为或值。请参阅使用指南。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是		-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

VPDN 用户名必须已关联到使用 **vpdn group** *group_name* **localname** *username* 命令指定的 VPDN 组。

clear configure vpdn username 命令从配置中删除所有 **vpdn username** 命令。

示例

以下示例创建 VPDN 用户名 *bob_smith* 及密码 *telecommuter*9/8：

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

相关命令

命令	描述
clear configure vpdn group	从配置中删除所有 **vpdn group** 命令。
clear configure vpdn username	从配置中删除所有 **vpdn username** 命令。
show vpdn group	显示 VPDN 组配置。
vpdn group	创建 VPDN 组并配置 PPPoE 客户端设置。

vpn-access-hours

要将组策略关联到已配置的时间范围策略，请在组策略配置模式或用户名配置模式下使用 **vpn-access-hours** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承时间范围值。为防止继承值，请使用 **vpn-access-hours none** 命令。

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

语法说明

none	将 VPN 访问时间设置为空值，从而允许无时间范围策略。防止从默认或指定的组策略继承值。
time-range	指定配置的 time-range 策略的名称。

默认值

不受限制。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

示例

以下示例展示如何将名为 FirstGroup 的组策略关联到名为 824 的时间范围策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-access-hours 824
```

相关命令

命令	描述
time-range	设置访问网络的每周天数和每天小时数，包括开始日期和结束日期。

vpn-addr-assign

要指定将 IPv4 地址分配到远程访问客户端的方法，请在全局配置模式下使用 **vpn-addr-assign** 命令。要从配置中删除属性，请使用此命令的 **no** 版本。要从 ASA 中删除所有已配置的 VPN 地址分配方法，请使用此命令的 **no** 版本（不带参数）。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *delay*]}

语法说明

aaa	从外部或内部（本地）AAA 身份验证服务器分配 IPv4 地址。
dhcp	通过 DHCP 获取 IP 地址。
local	从 ASA 上配置的 IP 地址池分配 IP 地址并将其关联到隧道组。
reuse-delay *delay*	已发布的 IP 地址在可重用之前的延迟。范围为 0 至 480 分钟。默认为 0（禁用）。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
8.0.3	添加了 **reuse-delay** 选项。
9.5(2)	增加了多情景模式支持。

使用指南

如果您选择了 DHCP，您还应使用 **dhcp-network-scope** 命令定义 DHCP 服务器可使用的 IP 地址范围。您必须使用 **dhcp-server** 命令指示 DHCP 服务器可使用的 IP 地址。

如果选择 local，还必须使用 **ip-local-pool** 命令定义要使用的 IP 地址范围。然后使用 **vpn-framed-ip-address** 和 **vpn-framed-netmask** 命令将 IP 地址和网络掩码分配给个人用户。

如果使用本地池，您可以使用 **reuse-delay** *delay* 选项以调整延迟，然后才能重用已发布的 IP 地址。增加延迟可防止 IP 地址返回地址池并快速重新分配时防火墙遇到的问题。

如果选择 AAA，您可以从之前配置的 RADIUS 服务器获取 IP 地址。

示例

以下示例展示如何配置 DHCP 作为地址分配方法：

```
ciscoasa(config)# vpn-addr-assign dhcp
```

相关命令

命令	描述
dhcp-network-scope	指定 ASA DHCP 服务器应该用来为组策略用户分配地址的 IP 地址范围。
ip-local-pool	创建本地 IP 地址池。
ipv6-addr-assign	指定为远程访问客户端分配 IPv6 地址的方法。
vpn-framed-ip-address	指定 IP 地址以分配给特定用户。
vpn-framed-ip-netmask	指定网络掩码以分配给特定用户。

vpn-mode

要指定集群的 VPN 模式，请在集群组配置模式下使用 **vpn-mode** 命令。集群的 vpn-mode 命令让管理员可以在集中模式或分布模式之间切换。要重置 VPN 模式，请使用此命令的 no 形式。CLI 的备份选项让管理员可以配置是否在不同机箱上创建 VPN 会话备份。此命令的 no 形式可将配置恢复为默认值。

vpn-mode [centralized | distributed][backup {flat | remote-chassis}]

[no] vpn-mode [centralized | distributed {flat | remote-chassis}]

默认值

默认 VPN 模式为集中模式。默认备份是平面。

语法说明

centralized	VPN 会话为集中式，仅在集群主设备上运行。
distributed	系统将 VPN 会话分布在各集群成员中。
flat	系统在集群的任何其他成员上分配备份会话。
remote-chassis	系统在另一个机箱的成员上分配备份会话。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
集群配置	• 是	• 是	• 是	-	• 是

命令历史记录

版本	修改
9.9(1)	添加了此命令。

使用指南

在平面备份模式下，将在任何其他集群成员上建立备用会话。这将防止用户受到刀片故障的影响，但无法保证机箱故障保护。

在远程机箱备份模式下，将在集群中的另一个机箱的成员上建立备用会话。这将防止用户受到刀片故障和机箱故障的影响。

如果在单机箱环境中配置了远程机箱（有意配置或由于故障而造成），则不会创建任何备份，直到另一个机箱加入。

示例

```
ciscoasa (cfg-cluster)# vpn-mode distributed

Return the backup strategy of a distributed VPN cluster to default:
no vpn-mode distributed backup
```

相关命令

命令	描述
cluster group	配置集群组设置。
show cluster vpn-sessiondb distribution	查看集群成员间的活跃会话和备份会话的分布情况。

vpnclient connect

要尝试建立到已配置的单个或多个服务器的 Easy VPN Remote 连接，请在全局配置模式下使用 **vpnclient connect** 命令。

vpnclient connect

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-
特权 EXEC	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

示例

以下示例展示如何尝试建立到已配置的 Easy VPN 服务器的 Easy VPN Remote 连接。

```
ciscoasa(config)# vpnclient connect
ciscoasa(config)#
```

vpnclient enable

要启用 Easy VPN Remote 功能，请在全局配置模式下使用 **vpnclient enable** 命令。要禁用 Easy VPN Remote 功能，请使用此命令的 **no** 形式：

vpnclient enable

no vpnclient enable

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

如果您输入 **vpnclient enable** 命令，则支持的 ASA 功能作为 Easy VPN Remote 硬件客户端。

示例

以下示例展示如何启用 Easy VPN Remote 功能：

```
ciscoasa(config)# vpnclient enable
ciscoasa(config)#
```

以下示例展示如何禁用 Easy VPN Remote 功能：

```
ciscoasa(config)# no vpnclient enable
ciscoasa(config)#
```

vpnclient ipsec-over-tcp

要配置作为 Easy VPN Remote 硬件客户端运行的 ASA 以使用 TCP 封装的 IPsec，请在全局配置模式下使用 **vpnclient ipsec-over-tcp** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

语法说明

port	（可选）指定使用特定端口。
tcp_port	（如果您指定 **port** 关键字，则为必需。）指定要为 TCP 封装的 IPsec 隧道使用的 TCP 端口号。

默认值

如果此命令未指定端口号，则 Easy VPN Remote 连接使用端口 10000。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

默认情况下，Easy VPN 客户端和服务器将 IPsec 封装在用户数据报协议 (UDP) 数据包中。某些环境（如具有某些防火墙规则或 NAT 和 PAT 设备）禁止 UDP。要在此环境中使用标准封装安全协议（ESP、Protocol 50）或互联网密钥交换（IKE、UDP 500），您必须配置客户端和服务器以将 IPsec 封装在 TCP 数据包内，从而启用安全隧道。但如果您的环境允许 UDP，配置 IPsec over TCP 会添加不必要的开销。

如果配置 ASA 以使用 TCP 封装的 IPsec，请输入以下命令使它通过外部接口发送数据包：

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

此命令可以清除封装报头中的不分段 (DF) 位。DF 位是 IP 报头中确定数据包是否可以分段的位。此命令可让 Easy VPN 硬件客户端发送大于 MTU 大小的数据包。

示例

以下示例展示如何使用默认端口 10000 配置 Easy VPN Remote 硬件客户端以使用 TCP 封装的 IPsec，并使它通过外部接口发送大数据包：

```
ciscoasa(config)# vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

以下示例展示如何使用端口 10501 配置 Easy VPN Remote 硬件客户端以使用 TCP 封装的 IPsec，并使它通过外部接口发送大数据包：

```
ciscoasa(config)# vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

vpnclient mac-exempt

要从个人用户身份验证要求中排除 Easy VPN Remote 连接的设备，请在全局配置模式下使用 **vpnclient mac-exempt** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

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

语法说明

mac_addr_1	MAC 地址，以点号分隔的十六进制数表示，指定免除个人用户身份验证的设备的制造商和序列号。对于多个设备，指定每个 MAC 地址，用空格和各自的网络掩码分隔开来。 MAC 地址的前 6 个字符识别设备制造商，后 6 个字符是序列号。最后 24 位是十六进制格式的设备序列号。
mac_mask_1	对应的 MAC 地址的网络掩码。使用空格分隔网络掩码和所有后续的 MAC 地址和网络掩码对。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

设备（如思科 IP 电话、无线接入点和打印机）无法执行身份验证，因此在启用单个设备验证时不会进行身份验证。如果启用个人用户身份验证，可使用此命令从身份验证中免除此类设备。从个人用户身份验证中免除设备也称为“设备传递”。

此命令中指定的 MAC 地址和掩码的格式为三个十六进制数字（以点号分隔）；例如，MAC 掩码 ffff.ffff.ffff 只匹配指定的 MAC 地址。全零的 MAC 掩码不匹配任何 MAC 地址，而 ffff.ff00.0000 的 MAC 掩码匹配同一制造商生产的所有设备。

注 您必须在头端设备中配置个人用户身份验证和用户旁路。例如，如果您将 ASA 作为头端，请在组策略下配置以下内容：

```
ciscoasa(config-group-policy)# user-authentication enable
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

示例

思科 IP 电话具有制造商 ID 00036b，因此以下命令免除所有思科 IP 电话，包括您以后可能添加的思科 IP 电话：

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa(config)#
```

下一个示例提供了更好的安全性，但降低了灵活性，因为它只免除特定的思科 IP 电话：

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa(config)#
```

vpnclient management

要生成管理访问 Easy VPN Remote 硬件客户端的 IPsec 隧道，请在全局配置模式下使用 **vpnclient management** 命令。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

要从正在运行配置中删除属性，请使用此命令的 **no** 形式，此命令以 **split-tunnel-policy** 和 **split-tunnel-network-list** 命令同样的方式建立管理专用 IPsec 隧道。

no vpnclient management

语法说明

clear	使用普通路由提供从企业网络到作为 Easy VPN 客户端运行的 ASA 5505 的外部接口的管理访问。此选项不创建管理隧道。 **注** 如果 NAT 设备在客户端和互联网之间运行，请使用此选项。
ip_addr	从 Easy VPN 硬件客户端为其建立管理隧道的主机或网络的 IP 地址。使用带有关键字 **tunnel** 的参数。指定一个或多个 IP 地址，用空格和各自的网络掩码分隔开来。
ip_mask	对应的 IP 地址的网络掩码。使用空格分隔网络掩码和所有后续的 IP 地址和网络掩码对。
tunnel	专为从企业网络到作为 Easy VPN 客户端运行的 ASA 5505 的外部接口的管理访问提供 IPsec 隧道自动化设置。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

它假设 ASA 5505 配置包含以下命令：

- **vpnclient server** 指定对等设备。
- **vpnclient mode** 指定客户端模式 (PAT) 或网络扩展模式。

以下项之一：

- **vpnclient vpngroup** 命名用于 Easy VPN 服务器上的隧道组和用于身份验证的 IKE 预共享密钥。
- **vpnclient trustpoint** 命名标识 RSA 证书以用于身份验证的信任点

注 NAT 设备后面的 ASA 的公共地址是无法访问的，除非您在 NAT 设备上添加静态 NAT 映射。

注 无论您如何配置，DHCP 请求（包括更新消息）都不应该流经 IPsec 隧道。即使是 vpnclient 管理隧道，也禁止 DHCP 流量。

示例

以下示例展示如何生成从 ASA 5505 的外部接口到 IP 地址/掩码组合为 192.168.10.10 255.255.255.0 的主机的 IPsec 隧道：

```
ciscoasa(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa(config)#
```

以下示例展示如何提供对不使用 IPsec 的 ASA 5505 外部接口的管理访问：

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

要配置客户端模式或网络扩展模式的 Easy VPN Remote 连接，请在全局配置模式下使用 **vpnclient mode** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

语法说明

client-mode	配置 Easy VPN Remote 连接以使用客户端模式 (PAT)。
network-extension-mode	配置 Easy VPN Remote 连接以使用网络扩展模式 (NEM)。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

Easy VPN 客户端支持两种运行模式：客户端模式或 NEM。运行模式确定了相对于 Easy VPN 客户端的内部主机是否可以通过隧道从企业网络访问。先要强制指定运行模式，然后才能进行连接，因为 Easy VPN 客户端没有默认模式。

- 在客户端模式下，Easy VPN 客户端对来自内部主机的所有流量执行端口地址转换 (PAT)。此模式不需要对硬件客户端的内部地址（分配的默认地址是 RFC 1918）或内部主机进行 IP 地址管理。由于 PAT，无法从企业网络访问内部主机。
- 在 NEM 中，内部网络和内部接口的所有节点都分配了可在整个企业网络路由的地址。内部主机可以从企业网络通过隧道访问。内部网络上的主机从可访问的子网上分配 IP 地址（静态或通过 DHCP）。在网络扩展模式下，PAT 不应用于 VPN 流量。

注 如果 Easy VPN 硬件客户端使用 NEM 并且连接到辅助服务器，请在每个头端设备上使用 **crypto map set reverse-route** 命令以使用反向路由注入 (RRI) 配置远程网络的动态声明。

示例

以下示例展示如何为客户端模式配置 Easy VPN Remote 连接：

```
ciscoasa(config)# vpnclient mode client-mode
ciscoasa(config)#
```

以下示例展示如何为 NEM 配置 Easy VPN Remote 连接：

```
ciscoasa(config)# vpnclient mode network-extension-mode
ciscoasa(config)#
```

vpnclient nem-st-autoconnect

要配置 Easy VPN Remote 连接在 NEM 和拆分隧道配置后自动启动 IPsec 数据隧道，请在全局配置模式下使用 **vpnclient nem-st-autoconnect** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

在输入 **vpnclient nem-st-autoconnect** 命令之前，确保为硬件客户端启用了网络扩展模式。网络扩展模式可让硬件客户端通过 VPN 隧道为远程专用网络提供单一、可路由的网络。IPsec 封装从硬件客户端背后的专用网络到 ASA 背后的网络的所有流量。PAT 不适用。因此，ASA 背后的设备可以通过隧道而且只能通过隧道直接访问硬件客户端背后的专用网络中的设备，反之亦然。硬件客户端必须启动隧道。隧道运行后，任一端均可发起数据交换。

注 您还必须配置 Easy VPN 服务器以启用网络扩展模式。要执行此操作，请在组策略配置模式下使用 **nem enable** 命令。

在网络扩展模式下，IPsec 数据隧道自动启动并保持，除非配置了拆分隧道。

示例

以下示例展示如何配置 Easy VPN Remote 连接以在配置了拆分隧道的情况下自动以网络扩展模式连接。对组策略 FirstGroup 启用网络扩展模式：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# nem enable
ciscoasa(config)# vpnclient nem-st-autoconnect
ciscoasa(config)#
```

相关命令

命令	描述
nem	对硬件客户端启用网络扩展模式。

要从运行配置中删除属性，请使用此命令的 **no** 形式。

no vpnclient sercure interface

vpnclient server

要为 Easy VPN Remote 连接配置主要和辅助 IPsec 服务器，请在全局配置模式下使用 **vpnclient server** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient server *ip_primary_address* [*ip_secondary_address_1...ipsecondary_address_10*]

no vpnclient server

语法说明

ip_primary_address	主要 Easy VPN (IPsec) 服务器的 IP 地址或 DNS 名称。所有 ASA 或 VPN 3000 集中器系列都可以作为 Easy VPN 服务器。
ip_secondary_address_n	（可选）多达十个备用 Easy VPN 服务器的 IP 地址或 DNS 名称的列表。使用空格分隔列表中的项目。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

必须先配置服务器，然后才能建立连接。**vpnclient server** 命令支持 IPv4 地址、名称数据库或 DNS 名称并按照这个顺序解析地址。

您可以使用服务器的 IP 地址或主机名。

示例

以下示例将名称 headend-1 与地址 10.10.10.10 关联并使用 **vpnclient server** 命令指定三台服务器：headend-dns.example.com （主要）、headend-1（辅助）和 192.168.10.10（辅助）：

```
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)#
```

以下示例展示如何配置 IP 地址为 10.10.10.15 的 VPN 客户端 IPsec 主要服务器以及 IP 地址为 10.10.10.30 和 192.168.10.45 的辅助服务器。

```
ciscoasa(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa(config)#
```

vpnclient server-certificate

要配置 Easy VPN Remote 连接以只接受到带有证书映射指定的特定证书的 Easy VPN 服务器的连接，请在全局配置模式下使用 **vpnclient server-certificate** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

语法说明

certmap_name	指定证书映射的名称，该映射指定可接受的 Easy VPN 服务器证书。最大长度为 64 个字符。

默认值

Easy VPN 服务器证书过滤默认为禁用状态。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

使用此命令启用 Easy VPN 服务器证书过滤。使用 crypto ca certificate map 和 crypto ca certificate chain 命令定义证书映射本身。

示例

以下示例展示如何配置 Easy VPN Remote 连接以只支持到带有证书映射名为 homeservers 的 Easy VPN 服务器的连接：

```
ciscoasa(config)# vpnclient server-certificate homeservers
ciscoasa(config)#
```

相关命令

命令	描述
certificate	添加指定的证书。
vpnclient trustpoint	配置将由 Easy VPN Remote 连接使用的 RSA 身份证书。

vpnclient trustpoint

要配置 Easy VPN Remote 连接使用的 RSA 身份证书，请在全局配置模式下使用 **vpnclient trustpoint** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

语法说明

链	发送整个证书链。
trustpoint_name	指定标识 RSA 证书以用于身份验证的信任点。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

使用 **crypto ca trustpoint** 命令定义信任点。一个信任点代表一个 CA 身份，也可能代表一个基于 CA 签发的证书的设备身份。信任点子模式下的命令控制 CA 特定的配置参数，这些参数指定 ASA 如何获取 CA 证书、ASA 如何从 CA 以及由 CA 签发的用户证书的身份验证策略中获取其证书。

示例

以下示例展示如何配置 Easy VPN Remote 连接，以使用名为 central 的特定身份证书和发送整个证书链：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config)# vpnclient trustpoint central chain
ciscoasa(config)#
```

相关命令

命令	描述
crypto ca trustpoint	进入指定信任点的信任点子模式并管理信任点信息。

vpnclient username

要配置 Easy VPN Remote 连接的 VPN 用户名和密码，请在全局配置模式下使用 **vpnclient username** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

语法说明

xauth_password	指定用于 XAUTH 的密码。最大长度为 64 个字符。
xauth_username	指定用于 XAUTH 的用户名。最大长度为 64 个字符。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

当安全设备身份验证禁用且服务器请求 XAUTH 凭证时，会使用 XAUTH 用户名和密码参数。如果安全设备身份验证已启用，这些参数将被忽略，并且 ASA 将提示用户输入用户名和密码。

示例

以下示例展示如何配置 Easy VPN Remote 连接，以使用 XAUTH 用户名 testuser 以及密码 ppurkm1：

```
ciscoasa(config)# vpnclient username testuser password ppurkm1
ciscoasa(config)#
```

vpnclient vpngroup

要配置 Easy VPN Remote 连接的 VPN 隧道组名称和密码，请在全局配置模式下使用 **vpnclient vpngroup** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

语法说明

group_name	指定在 Easy VPN 服务器上配置的 VPN 隧道组的名称。最大长度是 64 个字符，而且不允许使用空格。
preshared_key	Easy VPN 服务器用于身份验证的 IKE 预共享密钥。最大长度为 128 个字符。

默认值

如果作为 Easy VPN Remote 硬件客户端运行的 ASA 的配置未指定隧道组，则客户端将尝试使用 RSA 证书。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令仅适用于作为 Easy VPN Remote 硬件客户端运行的 ASA：运行版本 7.2(1) 至 9.2 的 ASA 5505，或运行版本 9.5(1) 或更高版本的 ASA 5506 或 5508 型号。

使用预共享密钥作为密码。

在建立连接之前，您还必须配置服务器并指定模式。

示例

以下示例展示如何配置 Easy VPN Remote 连接，其中 VPN 隧道组的组名称为 TestGroup1，密码为 my_key123。

```
ciscoasa(config)# vpnclient vpngroup TestGroup1 password my_key123
ciscoasa(config)#
```

相关命令

命令	描述
vpnclient trustpoint	配置 RSA 身份证书，以供 Easy VPN 连接使用。

vpn-filter

要指定用于 VPN 连接的 ACL 名称，请在组策略或用户名模式下使用 **vpn-filter** 命令。要删除 ACL，包括通过执行 **vpn-filter none** 命令创建的空值，请使用此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。为防止继承值，请使用 **vpn-filter none** 命令。

您配置 ACL 来为此用户或组策略允许或拒绝各种类型的流量。然后，使用 **vpn-filter** 命令以应用这些 ACL。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

语法说明

none	指示没有访问列表。设置一个空值，从而禁止访问列表。防止从其他组策略继承访问列表。
value *ACL name*	提供先前配置的访问列表的名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• **是**	-	• **是**	• 是	-
用户名配置	• **是**	-	• **是**	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.0(1)	添加了对 IPv4 和 IPv6 ACL 的支持。增加了多情景模式支持。
9.1.(4)	添加了对 IPv4 和 IPv6 ACL 的支持。如果已弃用的命令 **ipv6-vpn-filter** 被错误地用于指定 IPv6 ACL，则连接将终止。

使用指南

无客户端 SSL VPN 不使用 **vpn-filter** 命令中定义的 ACL。

根据设计，vpn-filter 功能只过滤入站方向的流量。出站规则会自动构建。在创建 ICMP 访问列表时，如果想要定向过滤器，不要以访问列表格式指定 ICMP 类型。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置调用名为 acl_vpn 的访问列表的过滤器：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-filter value acl_vpn
```

相关命令

命令	描述
access-list	创建访问列表，或使用可下载访问列表。
ipv6-vpn-filter	已弃用的命令，之前用于指定 IPv6 ACL。

vpn-framed-ip-address

要指定为个人用户分配的 IPv4 地址，请在用户名模式下使用 **vpn-framed-ip-address** 命令。要删除该 IP 地址，请使用此命令的 **no** 形式。

vpn-framed-ip-address {*ip_address*} {*subnet_mask*}

no vpn-framed-ip-address

语法说明

ip_address	为此用户提供 IP 地址。
subnet_mask	指定子网掩码。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

示例

以下示例显示如何为名为 anyuser 的用户设置 IP 地址 10.92.166.7：

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

在用户名模式下使用 **vpn-framed-ipv6-address** 命令，将专用 IPv6 地址分配给用户。要删除该 IP 地址，请使用此命令的 **no** 形式。

vpn-framed-ipv6-address *ip_address/subnet_mask*

no vpn-framed-ipv6-address *ip_address/subnet_mask*

语法说明

ip_address	为此用户提供 IP 地址。
subnet_mask	指定子网掩码。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

示例

以下示例展示如何为名为 *anyuser* 的用户设置 IP 地址和子网掩码 2001::3000:1000:2000:1/64。此地址表示前缀值为 2001:0000:0000:0000，接口 ID 为 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)
```

相关命令

命令	描述
vpn-framed-ip-address	指定要为个人用户分配的 IPv4 地址。

vpn-group-policy

要使用户从已配置的组策略继承属性，请在用户名配置模式下使用 **vpn-group-policy** 命令。要从用户配置删除组策略，请使用此命令的 **no** 形式。使用此命令可让用户继承尚未在用户名级别配置的属性。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

语法说明

group-policy name	提供组策略的名称。

默认值

默认情况下，VPN 用户没有组策略关联。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

如果特定用户的组策略中的属性在用户名模式下可用，您可以通过在用户名模式下配置该属性以覆盖其值。

示例

以下示例显示如何配置名为 anyuser 的用户使用名为 FirstGroup 的组策略中的属性：

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-group-policy FirstGroup
```

相关命令

命令	描述
group-policy	将组策略添加到 ASA 数据库。
group-policy attributes	进入可让您为组策略配置 AVP 的组策略属性模式。
username	将用户添加到 ASA 数据库。
username attributes	进入可让您为指定用户配置 AVP 的用户名属性模式。

vpn-idle-timeout

要配置用户超时期限，请在组策略配置模式或用户名配置模式下使用 **vpn-idle-timeout** 命令。如果在此期间连接上没有通信活动，则 ASA 将终止此连接。您可以选择延长默认为一分钟的超时前警报间隔。

要从运行配置中删除属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承超时值。要防止继承值，请使用 **vpn-idle-timeout none** 命令。

vpn-idle-timeout {*minutes* **| none} [alert-interval** *minutes***]**

no vpn-idle-timeout

no vpn-idle-timeout alert-interval

语法说明

minutes	指定超时期限的分钟数和超时警报前的分钟数。使用 1 和 35791394 之间的一个整数。
none	AnyConnect (SSL IPsec/IKEv2)：使用以下命令中的全局 WebVPN default-idle-timeout 值（秒）：**ciscoasa(config-webvpn)# default-idle-timeout** 在 WebVPN **default-idle-timeout** 命令中，此值的范围是 60 到 86400 秒；默认全局 WebVPN 空闲超时（秒）- 默认值为 1800 秒（30 分钟）。 **注** 对于所有 AnyConnect 连接，ASA 需要一个非零的空闲超时值。 对于 WebVPN 用户，仅当在组策略/用户名属性中设置了 vpn-idle-timeout none 时，才会实施 **default-idle-timeout** 值。 站点到站点（IKEv1、IKEv2）和 IKEv1 远程访问：禁用超时并允许无限制的空闲期。

默认值

30 分钟。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

AnyConnect 客户端支持 SSL 和 IKEv2 连接的会话恢复。通过此功能，最终用户设备可以进入休眠模式，丢失其 WiFi 或任何其他类似连接，并在返回时恢复同一连接。

示例

以下示例展示如何为名为“FirstGroup”的组策略设置 15 分钟的 VPN 空闲超时：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-idle-timeout 30
```

如果没有为用户定义空闲超时、VPN 空闲超时值为 0 或该值不在有效范围内，则安全设备使用默认空闲超时值。

相关命令

default-idle-timeout	指定全局 WebVPN 默认空闲超时。
group-policy	创建或编辑组策略。
vpn-session-timeout	配置 VPN 连接允许的最大时间量。此时间段结束时，ASA 将终止连接。

vpn load-balancing

要进入可以配置 VPN 负载平衡和相关功能的 VPN 负载平衡模式，请在全局配置模式下使用 **vpn load-balancing** 命令。

vpn load-balancing

注 要使用 VPN 负载平衡，您必须具有带 Plus 许可的 ASA 5510 或 ASA 5520 或更高版本。VPN 负载均衡还需要活动的 3DES/AES 许可证。在启用负载均衡之前，安全设备将检查此加密许可证是否存在。如果没有检测到活动的 3DES 或 AES 许可证，安全设备会阻止启用负载均衡，也会阻止负载均衡系统进行 3DES 的内部配置，除非许可证允许此使用。

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
8.0(2)	增加了对带有 Plus 许可证的 ASA 5510 及 5520 以上型号的支持。

使用指南

负载平衡集群可包括安全设备型号 5510（带 Plus 许可证），或 ASA 5520 及以上型号。您还可以在集群中包括 VPN 3000 系列集中器。虽然混合配置是可行的，但如果集群是同构的，管理通常更为简单。

使用 **vpn load-balancing** 命令进入 VPN 负载平衡模式。以下命令可在 VPN 负载平衡模式下使用：

- **cluster encryption**
- **cluster ip address**
- **cluster key**
- **cluster port**
- **Interface**
- **nat**
- **participate**

- **priority**
- **redirect-fqdn**

有关详细信息，请参阅单个命令说明。

示例

以下是 **vpn load-balancing** 命令的示例；注意提示符的变化：

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

以下是 VPN 负载平衡命令序列的示例，其中包含将集群的公共接口指定为“test”以及将集群的专用接口指定为“foo”的 interface 命令：

```
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
```

相关命令

命令	描述
clear configure vpn load-balancing	删除负载平衡运行时间配置并禁止负载平衡。
show running-config vpn load-balancing	显示当前 VPN 负载平衡虚拟集群配置。
show vpn load-balancing	显示 VPN 负载平衡运行时间统计信息。

vpn-session-db

要指定 VPN 会话或 AnyConnect 客户端 VPN 会话的最大数量，请在全局配置模式下使用 **vpn-session-db** 命令。要从配置中删除限制，请使用此命令的 **no** 形式：

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number*}

语法说明

max-anyconnect-premium-or-essentials-limit *number*	指定 AnyConnect 的最大会话数，从 1 到许可证允许的最大会话数。
max-other-vpn-limit *number*	指定除 AnyConnect 客户端会话以外的 VPN 会话最大数，从 1 到许可证允许的最大会话数。这包括思科 VPN 客户端 (IPsec IKEv1) 和局域网至局域网 VPN。

默认值

默认情况下，ASA 不限制小于许可的最大数量的 VPN 会话数。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
8.4(1)	更改了以下关键字： • **max-anyconnect-premium-or-essentials-limit** 取代了 **max-session-limit** • **max-other-vpn-limit** 取代了 **max-webvpn-session-limit**
9.0(1)	增加了多情景模式支持。

示例

以下示例将 AnyConnect 会话最大数设置为 200：

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

相关命令

命令	描述
vpn-sessiondb logoff	注销所有或特定类型的 IPsec VPN 和 WebVPN 会话。
vpn-sessiondb max-webvpn-session-limit	设置 WebVPN 会话最大数。

vpn-sessiondb logoff

要注销所有或选定 VPN 会话，请在全局配置模式下使用 **vpn-sessiondb logoff** 命令。

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**]

语法说明

all	注销所有 VPN 会话。
anyconnect	注销所有 AnyConnect VPN 客户端会话。
email-proxy	（已弃用）注销所有电邮代理会话。
index *index_number*	按索引编号注销单个会话。指定会话的索引编号。您可以使用 **show vpn-sessiondb detail** 命令查看每个会话的索引编号。
ipaddress *IPaddr*	注销您指定的 IP 地址的会话。
l2l	注销所有 LAN 到 LAN 会话。
name *username*	注销您指定的用户名的会话。
protocol *protocol-name*	注销您指定的协议的会话。这些协议包括： • ikev1 - 使用互联网密钥交换版本 1 (IKEv1) 的会话。 • ikev2 - 使用互联网密钥交换版本 2 (IKEv2) 的会话。 • ipsec - 使用 IKEv1 或 IKEv2 的 IPsec 会话。 • ipseclan2lan—IPsec LAN-to-LAN 会话。 • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T 会话。 • ipsecovernatt - IPsec over NAT-T 会话。 • ipsecovertcp - IPsec over TCP 会话。 • ipsecoverudp - IPsec over UDP 会话。 • l2tpOverIpSec - L2TP over IPsec 会话。 • l2tpOverIpsecOverNatT - L2TP over IPsec over NAT-T 会话。 • webvpn - 无客户端 SSL VPN 会话。 • imap4s - IMAP4 会话。 • pop3s - POP3 会话。 • smtps - SMTP 会话。 • anyconnectParent - AnyConnect 客户端会话，无论对会话采用哪种协议（终止 AnyConnect IPsec IKEv2 和 SSL 会话）。 • ssltunnel - SSL VPN 会话，包括使用 SSL 和无客户端 SSL VPN 会话的 AnyConnect 会话。 • dtlstunnel - 启用 DTLS 的 AnyConnect 客户端会话。
ra-ikev1-ipsec	注销所有 IPsec IKEv1 远程访问会话。
ra-ikev2-ipsec	注销所有 IPsec IKEv2 远程访问会话。
tunnel-group *groupname*	注销您指定的隧道组（连接配置文件）会话。
webvpn	注销所有无客户端 SSL VPN 会话。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
8.4(1)	更改或添加了以下**协议**关键字： • **remote** 已更改为 **ra-ikev1-ipsec**。 • **ike** 已更改为 **ikev1**。 • 添加了 **ikev2**。 • 添加了 **anyconnectParent**。
9.0(1)	增加了多情景模式支持。
9.3(2)	添加了 **ra-ikev2-ipsec** 关键字。
9.8(1)	**email-proxy** 选项已弃用。

示例

以下示例展示如何注销所有 AnyConnect 客户端会话：

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

以下示例展示如何注销所有 IPsec 会话：

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

要配置 VPN 连接允许的最大时间量，请在组策略配置模式或用户名配置模式下使用 **vpn-session-timeout** 命令。此时间段结束时，ASA 将终止连接。您可以选择延长默认为一分钟的超时前警报间隔。

要从运行配置中删除属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承超时值。要阻止继承值，请使用 **vpn-session-timeout none** 命令。

vpn-session-timeout {*minutes* | **none**} [**alert-interval** *minutes*]

no vpn-session-timeout

no vpn-session-timeout alert-interval

语法说明

minutes	指定超时期限的分钟数和超时警报前的分钟数。使用 1 和 35791394 之间的一个整数。
none	允许无限会话超时期限。将会话超时设置为空值，从而禁止使用会话超时。防止从默认或指定的组策略继承值。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。
9.7(1)	**alert-interval** 应用于 AnyConnect VPN

示例

以下示例显示如何将名为 FirstGroup 的组策略的 VPN 会话超时设置为 180 分钟：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-session-timeout 180
```

相关命令

group-policy	创建或编辑组策略。
vpn-idle-timeout	配置用户超时期限。如果在此期间连接上没有通信活动，则 ASA 将终止此连接。

vpnsetup

要显示 ASA 上的配置 VPN 连接的步骤列表，请在全局配置模式下使用 **vpnsetup** 命令。

vpnsetup {**ipsec-remote-access** | **l2tp-remote-access** | **site-to-site** | **ssl-remote-access**} **steps**

语法说明

ipsec-remote-access	显示配置 ASA 以接受 IPsec 连接的步骤。
l2tp-remote-access	显示配置 ASA 以接受 L2TP 连接的步骤。
site-to-site	显示配置 ASA 以接受 LAN 到 LAN 连接的步骤。
ssl-remote-access	显示配置 ASA 以接受 SSL 连接的步骤。
steps	指定显示连接类型的步骤。

默认值

此命令没有默认设置

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
8.0(3)	添加了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例展示 **vpnsetup ssl-remote-access steps** 命令的输出：

```
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)#
```

相关命令

命令	描述
show running-config	显示 ASA 正在运行的配置。

vpn-simultaneous-logins

要配置用户允许的同时登录数，请在组策略配置模式或用户名配置模式下使用 **vpn-simultaneous-logins** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承值。输入 0 则禁用登录并阻止用户访问。

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

语法说明

integer	0 到 2147483647 之间的数字。

默认值

默认值为 3 个同时登录。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

输入 0 则禁用登录并阻止用户访问。

注 尽管同时登录数的上限非常大，但允许多个用户同时登录可能会降低安全性并影响性能。

即使已使用同一用户名建立“新”会话，停滞的 AnyConnect 会话、IPsec 客户端会话或无客户端会话（异常终止的会话）仍然可能保留在会话数据库中。

如果 vpn-simultaneous-logins 的值为 1，并且同一用户在异常终止后再次登录，则会从数据库中删除停滞的会话并建立新会话。但是，如果现有会话仍然是活动连接并且同一用户再次登录（可能从其他 PC），则会注销且从数据库中删除第一个会话并建立新会话。

如果同时登录数的值大于 1，则当达到此最大数并尝试再次登录时，会注销空闲时间最长的会话。如果所有当前会话的空闲时间同样长，则会注销最早的会话。此操作会释放一个会话并允许新用户登录。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置最大同时登录数 4：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

要配置 VPN 隧道类型（使用 IKEv1 或 IKEv2 的 IPsec、L2TP over IPsec、SSL 或无客户端 SSL），请在组策略配置模式或用户名配置模式下使用 **vpn-tunnel-protocol** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

no vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

语法说明

ikev1	在两个对等设备（一个远程访问客户端或另一个安全网关）之间协商使用 IKEv1 的 IPsec 隧道。创建管理身份验证、加密、封装和密钥管理的安全关联。
ikev2	在两个对等设备（一个远程访问客户端或另一个安全网关）之间协商使用 IKEv2 的 IPsec 隧道。创建管理身份验证、加密、封装和密钥管理的安全关联。
l2tp-ipsec	协商 L2TP 连接的 IPsec 隧道。
ssl-client	协商使用 SSL VPN 客户端的 SSL VPN 隧道。
ssl-clientless	通过启用 HTTPS 的 Web 浏览器为远程用户提供 VPN 服务，且不需要客户端。

默认值

默认值为 IPsec。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-
用户名配置	• 是	-	• 是	-	-

命令历史记录

版本	**修改**
7.0(1)	添加了此命令。
7.2(1)	添加了 **l2tp-ipsec** 关键字。
7.3(1)	添加了 **svc** 关键字。
8.4(1)	**ipsec** 关键字已被 **ikev1** 和 **ikev2** 关键字取代。

使用指南

使用此命令配置一个或多个隧道模式。至少必须配置一个隧道模式供用户通过 VPN 隧道进行连接。

注 要支持从 IPsec 回退到 SSL，**vpn-tunnel-protocol** 命令必须配置有 **svc** 和 **ipsec** 参数。

示例

以下示例展示如何为名为 “FirstGroup”的组策略配置 WebVPN 和 IPsec 隧道模式：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn
ciscoasa(config-group-policy)# vpn-tunnel-protocol IPsec
```

相关命令

命令	描述
address pools	指定将地址分配给远程客户端的地址池列表。
show running-config group-policy	显示所有组策略或特定组策略的配置。

vtep-nve

要将 VXLAN VNI 接口与 VTEP 源接口相关联，请在接口配置模式下使用 **vtep-nve** 命令。要删除关联，请使用此命令的 **no** 形式。

vtep-nve 1

no vtep-nve 1

语法说明

1	指定 NVE 实例，它始终为 1。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
接口配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.4(1)	添加了此命令。

使用指南

每个 ASA 或每个安全情景可以配置一个 VTEP 源接口。您可以配置一个用于指定此 VTEP 源接口的 NVE 实例。所有 VNI 接口都必须与此 NVE 实例关联。

示例

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并将 VNI 1 接口与之关联：

```
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
```

相关命令

命令	描述
debug vxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peer ip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
show arp vtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
show interface vni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show mac-address-table vtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
show nve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
show vni vlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

vxlan port

要设置 VXLAN UDP 端口，请在全局配置模式下使用 **vxlan port** 命令。要删除默认端口，请使用此命令的 **no** 形式。

vxlan port *udp_port*

no vxlan port *udp_port*

语法说明

udp_port	设置 VXLAN UDP 端口。默认值为 4789。

命令默认

默认端口为 4789。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Nve 配置	• 是	• 是	• 是	-	• 是

命令历史记录

版本	修改
9.4(1)	添加了此命令。

使用指南

默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。如果网络使用非标准端口，可以对其进行更改。

示例

例如：

```
ciscoasa(config)# vxlan port 5678
```

相关命令

命令	描述
debug vxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。

命令	描述
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peer ip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
show arp vtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
show interface vni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show mac-address-table vtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
show nve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
show vni vlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。

Wccp 至 zone-member 命令

wccp

要分配空间并启用指定网络缓存通信协议 (WCCP) 服务支持以加入服务组，请在全局配置模式下使用 **wccp** 命令。要禁用此服务组并取消分配空间，请使用此命令的 no 形式。

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**]]

语法说明

access-list	指定访问列表的名称。
group-list	（可选）确定允许哪些网络缓存加入服务组的访问列表。access-list 参数应包括一个用于指定访问列表的字符串（名称或编号，不超过 64 个字符）。
password	（可选）指定对从服务组收到的消息进行 Message Digest 5 (MD5) 身份验证。未获身份验证接受的消息将被丢弃。
password	指定用于身份验证的密码。password 参数的最大长度为七个字符。
redirect-list	（可选）与用于控制重定向到此服务组的流量的访问列表一起使用。access-list 参数应包括一个用于指定访问列表的字符串（名称或编号，不超过 64 个字符）。访问列表应只包含网络地址。不支持端口特定条目
service-number	动态服务标识符，表示缓存所指定的服务定义。动态服务编号为 0 到 254，且最高为 255。最多允许 256 个，其中包括使用 **web-cache** 关键字指定的网络缓存服务。
web-cache	指定网络缓存服务。 **注** 网络缓存计为一项服务。最大服务数（包括使用 service-number 参数分配的服务）为 256。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个 情景	系统
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例展示如何让 WCCP 加入服务组：

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

相关命令

命令	描述
show wccp	显示 WCCP 配置。
wccp redirect	启用 WCCP 重定向支持。

wccp redirect

要使用 Web 缓存通信协议 (WCCP) 在接口入口启用数据包重定向，请使用 **wccp redirect** 命令。要禁用 WCCP 重定向，请使用此命令的 no 形式。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

语法说明

in	指定当数据包进入此接口时重定向。
interface_name	应在其中重定向数据包的接口的名称。
service	指定服务组。您可以指定 **web-cache** 关键字，也可以指定服务的标识号（从 0 到 99）。

默认值

此命令默认禁用。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例展示如何在内部接口对网络缓存服务启用 WCCP 重定向：

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

相关命令

命令	描述
show wccp	显示 WCCP 配置。
wccp	对服务组启用 WCCP 支持。

web-agent-url（已弃用）

注 支持此命令的最后一个版本是版本 9.5(1)。

要指定 ASA 向其发出 SiteMinder 类型 SSO 身份验证请求的 SSO 服务器 URL，请在 config-webvpn-sso-siteminder 模式下使用 **web-agent-url** 命令。

要删除 SSO 服务器身份验证 URL，请使用此命令的 **no** 形式。

web-agent-url *url*

no web-agent-url *url*

注 SiteMinder 类型 SSO 身份验证需要执行此命令。

语法说明

url	指定 SiteMinder 类型 SSO 服务器的身份验证 URL。必须包含 http:// 或 https://。

默认值

默认情况下，身份验证 URL 未配置。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
Config-webvpn-sso-siteminder	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。
9.5(2)	为了支持 SAML 2.0，此命令已弃用。

使用指南

单点登录支持，仅适用于 WebVPN，可让用户访问不同服务器上的不同安全服务，而无需重复输入用户名和密码。SSO 服务器具有处理身份验证请求的 URL。

此命令仅适用于 SiteMinder 类型的 SSO 服务器。

使用 **web-agent-url** 命令配置 ASA 将身份验证发送到此 URL。在配置身份验证 URL 之前，必须使用 **sso-server** 命令创建 SSO 服务器。

对于安全设备与 SSO 服务器之间的 https 通信，请确保两端的 SSL 加密设置匹配。在安全设备上，使用 **ssl encryption** 命令对此进行验证。

示例

以下示例在 config-webvpn-sso-siteminder 模式中输入，用于指定 http://www.example.com/webvpn 的身份验证 URL：

```
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)#
```

相关命令

命令	描述
max-retry-attempts	配置 ASA SSO 身份验证尝试失败后的重试次数。
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder-type SSO 服务器。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
ssl encryption	指定 SSL/TLS 协议使用的加密算法。
sso-server	创建单点登录服务器。

web-applications

要定制 WebVPN 主页上向通过验证的 WebVPN 用户显示的 Web Application 框，请从 webvpn 定制模式使用 **web-applications** 命令：

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

语法说明

title	指定您要更改标题。
message	指定您要更改标题下显示的消息。
dropdown	指定您要更改下拉列表框。
text	指示您正在更改文本。
style	指定您正在更改 HTML 样式。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

默认值

默认标题文本为“Web Application”。

默认标题样式为 background-color:#99CCCC;color:black;font-weight:bold;text-transform: uppercase

默认消息文本为“Enter Web Address (URL)”。

默认消息样式为 background-color:#99CCCC;color:maroon;font-size:smaller。

默认下拉列表文本为“Web Bookmarks”。

默认下拉样式为 border:1px solid black;font-weight:bold;color:black;font-size:80%。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
WebVPN 定制	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

使用指南

style 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查询位于 www.w3.org 的万维网联盟 (W3C) 网站上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

示例

以下示例将标题改为“Applications”，将文本颜色改为蓝色：

```
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
```

相关命令

命令	描述
application-access	定制 WebVPN 主页的 Application Access 框。
browse-networks	定制 WebVPN 主页的 Browse Networks 框。
web-bookmarks	定制 WebVPN 主页上的 Web Bookmarks 标题或链接。
file-bookmarks	定制 WebVPN 主页上的 File Bookmarks 标题或链接。

web-bookmarks

要定制 WebVPN 主页上向通过验证的 WebVPN 用户显示的 Web Bookmarks 标题或链接，请从 webvpn 定制模式使用 **web-bookmarks** 命令：

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

语法说明

链接	指定您要更改链接。
title	指定您要更改标题。
style	指定您正在更改 HTML 样式。
text	指示您正在更改文本。
value	要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

默认值

默认链接样式为 color:#669999;border-bottom: 1px solid #669999;text-decoration:none。

默认标题样式为 color:#669999;background-color:#99CCCC;font-weight:bold。

默认标题文本为“Web Bookmarks”。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
WebVPN 定制	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.1(1)	添加了此命令。

使用指南

style 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查询位于 www.w3.org 的万维网联盟 (W3C) 网站上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

示例

以下示例将 Web Bookmarks 标题定制为“Corporate Web Bookmarks”：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

相关命令

命令	描述
application-access	定制 WebVPN 主页的 Application Access 框。
browse-networks	定制 WebVPN 主页的 Browse Networks 框。
file-bookmarks	定制 WebVPN 主页上的 File Bookmarks 标题或链接。
web-applications	定制 WebVPN 主页的 Web Application 框。

webvpn (global)

要进入 webvpn 模式，请在全局配置模式下输入 **webvpn** 命令。要删除使用此命令输入的任何命令，请使用 **no webvpn** 命令。这些 **webvpn** 命令适用于所有 WebVPN 用户。

通过这些 **webvpn** 命令，可配置 AAA 服务器、默认组策略、默认空闲超时、http 和 https 代理、WebVPN 的 NBNS 服务器，以及最终用户看到的 WebVPN 屏幕外观。

webvpn

no webvpn

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用 WebVPN。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是		-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

此 WebVPN 模式可用于配置 WebVPN 的全局设置。WebVPN 模式（从组策略模式或用户名模式进入）可用于为特定用户或组策略定制 WebVPN 配置。ASA 无客户端 SSL VPN 配置仅分别支持一个 http-proxy 命令和一个 https-proxy 命令。

注 必须启用浏览器缓存，WebVPN 才可运行。

示例

以下示例展示如何进入 WebVPN 命令模式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#
```

webvpn (group-policy attributes, username attributes)

要进入此 **webvpn** 模式，请在组策略属性配置模式或用户名属性配置模式下使用 **webvpn** 命令。要删除在 WebVPN 模式中输入的所有命令，请使用此命令的 **no** 形式。这些 webvpn 命令适用于从中配置它们的用户名或组策略。

组策略和用户名的 WebVPN 命令定义通过 WebVPN 对文件、MAPI 代理、URL 和 TCP 应用的访问。它们还标识 ACL 和要过滤的流量类型。

webvpn

no webvpn

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用 WebVPN。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
组策略属性配置	• 是	-	• 是		-
用户名属性配置	• 是	-	• 是		-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

WebVPN 模式（从全局配置模式进入）可用于配置 WebVPN 的全局设置。组策略属性配置模式或用户名属性配置模式中的 **webvpn** 命令将 webvpn 命令中指定的设置应用到父命令中指定的组或用户。换句话说，本节介绍的以及您从组策略或用户名模式进入的 webvpn 模式，可让您为特定用户或组策略定制 WebVPN 配置。

应用于组策略属性模式中特定组策略的 webvpn 属性将覆盖在默认组策略中指定的属性。应用于用户名属性模式中特定用户的 WebVPN 属性将覆盖默认组策略以及该用户所属组策略中的属性。实质上，这些命令可以调整从默认组或指定的组策略继承的设置。有关 WebVPN 设置的信息，请参阅全局配置模式下的 **webvpn** 命令的说明。

下表列出了可在 webvpn 组策略属性和用户名属性模式中配置的属性。有关详细信息，请参阅各个命令的说明。

属性	描述
auto-signon	配置 ASA 自动将 WebVPN 用户登录凭证传递到内部服务器，为 WebVPN 用户提供单点登录方法。
customization	指定要应用的预配置 WebVPN 定制。
deny-message	指定在访问被拒绝时显示给用户的消息。
filter	识别要用于 WebVPN 连接的访问列表。
functions	配置文件访问和文件浏览、MAPI 代理以及 WebVPN 上的 URL 输入。
homepage	设置当 WebVPN 用户登录时显示的网页的 URL。
html-content-filter	识别要为 WebVPN 会话过滤的 Java、ActiveX、图像、脚本和 Cookie。
http-comp	指定要使用的 HTTP 压缩算法。
keep-alive-ignore	指定更新会话时要忽略的最大对象大小。
port-forward	启用 WebVPN 应用访问。
port-forward-name	配置用于识别转发到最终用户的 TCP 端口的显示名称。
sso-server	配置 SSO 服务器名称。
svc	配置 SSL VPN 客户端属性。
url-list	识别用户可通过 WebVPN 访问的服务器和 URL 列表。

示例

以下示例展示如何进入组策略“FirstGroup”的 webvpn 模式：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-webvpn)#
```

以下示例展示如何进入用户名“test”的 webvpn 模式：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-webvpn)#
```

相关命令

clear configure group-policy	删除特定组策略或所有组策略的配置。
group-policy attributes	进入 config-group-policy 模式，在该模式中可以为指定的组策略配置属性和值，或者进入 webvpn 模式配置组的 webvpn 属性。
show running-config group-policy	显示特定组策略或所有组策略正在运行的配置。
webvpn	进入您可以配置指定组 WebVPN 属性的 config-group-webvpn 模式。

白名单

对于云网络安全，要对流量类执行白名单操作，请在类配置模式下使用 **whitelist** 命令。您可以先输入 **policy-map type inspect scansafe** 命令，然后输入 **parameters** 命令，进入类配置模式。要禁用白名单，请使用此命令的 **no** 形式。

whitelist

no whitelist

语法说明

此命令没有任何参数或关键字。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
类配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

使用 **class-map type inspect scansafe** 命令识别要加入白名单的流量。使用 **policy-map type inspect scansafe** 命令中的检查类映射，并且为类指定 **whitelist** 操作。调用 **inspect scansafe** 命令中的检查策略映射。

示例

以下示例将 HTTP 及 HTTPS 检测策略映射的相同用户和组加入白名单：

```
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
```

相关命令

命令	描述
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和/或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置常规云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。

who

要显示 ASA 上活动的 Telnet 管理会话，请在特权 EXEC 模式下使用 **who** 命令。

who [*local_ip*]

语法说明

local_ip	（可选）指定将列表限于一个内部 IP 地址或网络地址（IPv4 或 IPv6）。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

who 命令可显示当前登录到 ASA 的每个 Telnet 客户端的 TTY_ID 和 IP 地址。

示例

此示例显示当客户端通过 Telnet 会话登录到 ASA 时 **who** 命令的输出。

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

相关命令

命令	描述
kill	终止 Telnet 会话。
telnet	添加对 ASA 控制台的 Telnet 访问权限并设置空闲超时。

window-variation

要断开与窗口大小变化的连接，请在 tcp-map 配置模式下使用 **window-variation** 命令。要删除此指定，请使用此命令的 **no** 形式。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

语法说明

allow-connection	允许连接。
drop-connection	断开连接。

默认值

默认操作是允许连接。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
Tcp-map 配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

将 **tcp-map** 命令与模块化策略框架基础设施结合使用。使用 **class-map** 命令定义流量类并使用 **tcp-map** 命令定制 TCP 检查。应用新 TCP 映射使用 **policy-map** 命令。使用 **service-policy** 命令激活 TCP 检查。

使用 **tcp-map** 命令进入 tcp-map 配置模式。在 tcp-map 配置模式下使用 **window-variation** 命令断开与已经缩小的窗口大小的所有连接。

窗口大小机制允许 TCP 通告一个大窗口，随后通告一个不接受过多数据的较小窗口。根据 TCP 规范，强烈反对“缩小窗口”。检测到这种情况时，连接可能会断开。

示例

以下示例展示如何断开与各窗口大小的所有连接：

```
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
```

相关命令

命令	描述
class	指定要用于流量分类的类映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
set connection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 tcp-map 配置模式的访问。

wins-server

要设置主要和辅助 WINS 服务器的 IP 地址，请在组策略配置模式下使用 **wins-server** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。此选项允许从另一个组策略继承 WINS 服务器。要禁止继承服务器，请使用 **wins-server none** 命令。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

语法说明

none	将 wins-servers 设为空值，从而不允许 WINS 服务器。防止从默认或指定的组策略继承值。
value *ip_address*	指定主要和辅助 WINS 服务器的 IP 地址。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
组策略配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

每次发出 **wins-server** 命令时，都会覆盖现有设置。例如，如果配置 WINS 服务器 x.x.x.x，然后配置 WINS 服务器 y.y.y.y，第二条命令会覆盖第一条，并且 y.y.y.y 会成为唯一 WINS 服务器。对于多个服务器也一样。要添加 WINS 服务器而不覆盖以前配置的服务器，请在输入此命令时包含所有 WINS 服务器的 IP 地址。

示例

以下示例展示如何使用 IP 地址 10.10.10.15、10.10.10.30 和 10.10.10.45 为组策略 FirstGroup 配置 WINS 服务器：

```
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

要让特定用户在输入 group-url 表中的一个条目来建立 VPN 会话时无需对每个连接配置文件运行思科安全桌面的 Hostscan 应用程序，请在隧道 webvpn 配置模式下使用 **without-csd** 命令。要从配置中删除此命令，请使用此命令的 **no** 形式。

without-csd [**anyconnect**]

no without-csd [**anyconnect**]

语法说明

anyconnect	（可选）更改命令只会影响 AnyConnect 连接。

默认值

没有默认值。如果已安装，则使用 Hostscan。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
隧道 webvpn 配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
8.2(1)	添加了此命令。
9.2(1)	添加了 **anyconnect** 关键字。

使用指南

此命令可防止当用户输入此连接配置文件（在 CLI 中称为隧道组）上配置的 url-group 列表中的 URL 时，思科安全桌面的 Hostscan 应用程序在终端上运行。输入此命令会阻止检测这些会话的终端状况，因此，您可能需要调整动态访问策略 (DAP) 配置。

示例

以下示例中的第一条命令将创建一个 group-url，其中“example.com”是 ASA 的域，“no-csd”是 URL 的唯一部分。当用户输入此 URL 时，ASA 会将此连接配置文件分配到会话。必须输入 **group-url** 命令，**without-csd** 命令才可生效。**without-csd** 命令让用户无需运行 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)#
```

相关命令

命令	描述
csd enable	对没有 without-csd 命令的所有连接配置文件启用 Cisco Secure Desktop。
csd image	将命令中指定的 Cisco Secure Desktop 映像从路径中指定的闪存驱动器复制到运行配置。
group-url	创建此连接配置文件所独有的 group-url。

write erase

要清除启动配置，请在特权 EXEC 模式下使用 **write erase** 命令。运行配置保持不变。

write erase

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	-	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令在安全情景中不受支持。情景启动配置在系统配置中由 **config-url** 命令识别。如果要删除情景配置，您可以从远程服务器手动删除文件（如果已指定）或者在系统执行空间使用 **delete** 命令清除闪存中的文件。

对于 ASAv，此命令在**重新加载**之后恢复部署配置（初始虚拟部署设置）。要完全擦除配置，请使用 **clear configure all** 命令。要擦除部署配置并应用与 ASA 设备相同的工厂默认值配置，请参阅 **configure factory-default**。

注 ASAv 会启动当前运行的映像，因此，不会恢复到原始启动映像。

在重新加载之前，请不要保存配置。

对于故障切换对中的 ASAv，请先关闭备用设备。为防止备用设备变成主用设备，必须将其关闭。如果让其处于打开状态，则当清除主用设备配置后，备用设备将变为主用设备。当原来的主用设备重新加载并且通过故障切换链路重新连接后，旧配置将从新主用设备同步，并且擦除所需要的部署配置。在主用设备重新加载后，您可以打开备用设备。然后，部署配置将同步到备用设备。

示例

以下示例将清除启动配置：

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

相关命令

命令	描述
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
delete	从闪存中删除文件。
show running-config	显示运行配置。
write memory	将运行配置保存到启动配置。

write memory

要将运行配置保存到启动配置，请在特权 EXEC 模式下使用 **write memory** 命令。

write memory [**all** [**/noconfirm**]]

语法说明

/noconfirm	使用 **all** 关键字时，将消除确认提示。
all	从多情景模式下的系统执行空间，此关键字将保存所有情景配置和系统配置。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.2(1)	现在，您可以使用 **all** 关键字保存所有情景配置。

使用指南

运行配置是内存中当前运行配置，包括您在命令行中所做的所有更改。如果您将更改保存到启动配置（即在启动时加载到运行的内存中的配置），更改只会在两次重新启动之间保留。您可以使用 **boot config** 命令，将单情景模式下及多情景模式下系统的启动配置位置从默认位置（隐藏的文件）更改为您选择的位置。对于多情景模式，情景启动配置位于系统配置中的 **config-url** 命令所指定的位置。

在多情景模式下，您可以在每个情景中输入 **write memory** 命令来保存当前情景配置。要保存所有情景配置，请在系统执行空间中输入 **write memory all** 命令。情景启动配置可驻留在外部服务器上。在这种情况下，ASA 会将配置保存回 **config-url** 命令指定的服务器，但 HTTP 和 HTTPS URL 除外，这些 URL 不允许您将配置保存回服务器。在 ASA 使用 **write memory all** 命令保存每个情景之后，将会出现以下消息：

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

有时，情景因错误而无法保存。请参阅以下错误的相关信息：

- 对于因内存不足而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- 对于因无法到达远程目标而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- 对于因情景被锁定而无法保存的情景，系统将显示以下消息：

```
Unable to save the configuration for the following contexts as these contexts are
locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

  仅当另一位用户已保存配置或正在删除情景时，情景才会锁定。

- 对于因启动配置为只读配置而不能保存的情景（例如，在 HTTP 服务器上），在所有其他消息的末尾将显示以下消息报告：

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- 对于因闪存中有坏扇区而无法保存的情景，会出现以下消息：

```
The context 'context a' could not be saved due to Unknown errors
```

由于系统使用管理情景接口来访问情景启动配置，因此 **write memory** 命令也使用管理情景接口。但 **write net** 命令使用情景接口将配置写入 TFTP 服务器。

write memory 命令与 **copy running-config startup-config** 命令作用相等。

示例

以下示例将运行配置保存到启动配置：

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

相关命令

命令	描述
admin-context	设置管理情景。
configure memory	将启动配置与运行配置合并。
config-url	指定情景配置的位置。
copy running-config startup-config	将运行配置复制到启动配置。
write net	将运行配置复制到 TFTP 服务器。

write net

要将运行配置保存到 TFTP 服务器，请在特权 EXEC 模式下使用 **write net** 命令。

write net [*server*:[*filename*] | :*filename*]

语法说明

:*filename*	指定路径和文件名。如果已使用 **tftp - server** 命令设置文件名，则此参数可选。 如果在此命令以及 **tftp-server** 命令中指定文件名，则 ASA 会将 **tftp-server** 命令中的文件名视为目录，而将 **write net** 命令中的文件名添加为该目录下的文件。 要覆盖 **tftp-server** 命令值，请在路径和文件名前面输入一个斜杠。斜杠表示该路径不是 tftpboot 目录的相对路径，而是绝对路径。为此文件生成的 URL 在文件名路径前面有一个双斜杠 (//)。如果需要的文件在 tftpboot 目录中，您可以在文件名路径中包含 tftpboot 目录的路径。如果您的 TFTP 服务器不支持此类 URL，则改用 **copy running-config tftp** 命令。 如果使用 **tftp-server** 命令指定了 TFTP 服务器地址，您可以输入文件名，只在后面加一个冒号 (:)。
server:	设置 TFTP 服务器的 IP 地址或名称。此地址将覆盖您在 **tftp-server** 命令中设置的地址（如果有）。 默认网关接口是安全性最高的接口；但是，您可以使用 **tftp-server** 命令设置不同的接口名称。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

运行配置是内存中当前运行配置，包括您在命令行中所做的所有更改。

在多情景模式下，此命令仅保存当前配置；您不能使用单个命令保存所有情景，而必须单独为系统及每个情景输入此命令。**write net** 命令使用情景接口将配置写入 TFTP 服务器。但 **write memory** 命令使用管理情景接口保存到启动配置，因为系统使用管理情景接口来访问情景启动配置。

write net 命令与 **copy running-config tftp** 命令作用相等。

示例

以下示例在 **tftp-server** 命令中设置 TFTP 服务器和文件名：

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

以下示例在 **write net** 命令中设置服务器和文件名。**tftp-server** 命令未填充。

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

以下示例在 **write net** 命令中设置服务器和文件名。**tftp-server** 命令提供目录名称，服务器地址被覆盖。

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

相关命令

命令	描述
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
copy running-config tftp	将运行配置复制到 TFTP 服务器。
show running-config	显示运行配置。
tftp-server	设置用于其他命令的默认 TFTP 服务器和路径。
write memory	将运行配置保存到启动配置。

write standby

要将 ASA 或情景运行配置复制到故障切换备用设备，请在特权 EXEC 模式下使用 **write standby** 命令。

write standby

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

仅在备用设备或故障切换组的配置与主用设备或故障切换组的配置不同步时，才应使用此命令。直接在备用设备或故障切换组上输入命令时，通常会发生这种情况。

对于主用/备用故障切换，在主用设备上输入 **write standby** 命令会将主用故障切换设备的运行配置写入备用设备的运行配置。

对于主用/主用故障切换，**write standby** 命令的行为如下：

- 如果在系统执行空间输入 **write standby** 命令，系统配置以及 ASA 上所有安全情景的配置都将写入对等设备。这包括处于备用状态的安全情景的配置信息。您必须在具有处于主用状态的故障切换组 1 的系统执行空间中输入命令。
- 如果您在安全情景中输入 **write standby** 命令，只有安全情景的配置会写入对等设备。您必须在安全情景为主用状态的设备上的安全情景中输入命令。

write standby 命令会将配置复制到对等设备的运行配置；不会将其保存到启动配置。要将配置更改保存到启动配置，请在您输入 **write standby** 命令的设备上使用 **copy running-config startup-config** 命令。该命令将复制到对等设备，而且配置保存到启动配置。

启用状态故障切换后，**write standby** 命令还会在配置复制完成后将状态信息复制到备用设备。在多情景模式中，在复制状态信息的情景中输入 **write standby**。

注 在输入 **write standby** 命令后，故障切换接口会在配置重新同步后立即关闭。这也可能导致要检测的故障切换状态接口暂时失效。

示例

以下示例将当前运行配置写入备用设备：

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

相关命令

命令	描述
failover reload-standby	强制备用设备重新启动。

write terminal

要在终端上显示运行配置，请在特权 EXEC 模式下使用 **write terminal** 命令。

write terminal

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	• 是

命令历史记录

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令与 **show running-config** 命令作用相等。

示例

以下示例将运行配置写入终端：

```
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
...
```

相关命令

命令	描述
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
show running-config	显示运行配置。
write memory	将运行配置保存到启动配置。

xlate block-allocation

要为运营商级或大规模 PAT 配置端口块分配特征，请在全局配置模式下使用 **xlate block-allocation** 命令。要恢复默认值，请使用此命令的 **no** 形式。

xlate block-allocation {**size** *value* | **maximum-per-host** *number*}

no xlate block-allocation {**size** *value* | **maximum-per-host** *number*}

语法说明

size *value*	块分配大小，即每个块中的端口数。 范围为 32-4096。默认值为 512。 如果不使用默认值，请确保 64,512 能被您所选的大小整除（1024-65535 范围中的端口数)。否则，会出现无法分配的端口。例如，如果指定 100，会有 12 个未使用端口。
maximum-per-host *number*	每个主机可分配的最大块数。限制是针对每个协议，因此限制为 4 表示每个主机最多 4 个 UDP 块、4个 TCP 块和 4 个 ICMP 块。 范围为 1-8，默认值为 4。

命令默认

默认分配大小为 512。默认每主机最大数为 4。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.5(1)	添加了此命令。

使用指南

对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。当使用块中端口的最后一个转换被删除时，系统将释放该块。

只能在 1024 - 65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1 - 1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。

xlate block-allocation 命令可配置这些端口块的特征。在 **nat** 命令中使用 block-allocation 关键字，以便在使用 PAT 池时根据 PAT 规则启用端口块分配。

示例

以下示例更改端口块分配特征，并为对象 NAT 规则中的 PAT 池实施端口块分配：

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6

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
```

相关命令

命令	描述
nat (global)	添加一个两倍 NAT 规则。
nat (object)	添加对象 NAT 规则。
show local-host	显示已分配给主机的端口块。
show running-config xlate	显示 **xlate** 配置。

xlate per-session

要使用多会话 PAT，请在全局配置模式下使用 **xlate per-session** 命令。要删除多会话 PAT 规则，请使用此命令的 **no** 形式。

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*

语法说明

deny	创建拒绝规则。
destination_ip	对于目标 IP 地址，可进行以下配置： • **host** *ip_address* - 指定 IPv4 主机地址。 • *ip_address mask* - 指定 IPv4 网络地址和子网掩码。 • *ipv6-address*/*prefix-length* - 指定 IPv6 主机或网络地址和前缀。 • **any4** 和 **any6** - **any4** 指定纯 IPv4 流量；**any6** 则指定 any6 流量。
operator dest_port	*operator* 匹配目标使用的端口号。允许的运算符如下： • lt — 小于 • gt — 大于 • eq — 等于 • neq — 不等于 • range — 值的包含范围。使用此运算符时，需指定两个端口号，例如： `range 100 200`
operator src_port	（可选）*operator* 与源使用的端口号匹配。允许的运算符如下： • lt — 小于 • gt — 大于 • eq — 等于 • neq — 不等于 • range — 值的包含范围。使用此运算符时，需指定两个端口号，例如： `range 100 200`
permit	创建允许规则。
source_ip	对于源 IP 地址，可进行以下配置： • **host** *ip_address* - 指定 IPv4 主机地址。 • *ip_address mask* - 指定 IPv4 网络地址和子网掩码。 • *ipv6-address*/*prefix-length* - 指定 IPv6 主机或网络地址和前缀。 • **any4** 和 **any6** - **any4** 指定纯 IPv4 流量；**any6** 则指定 any6 流量。
tcp	指定 TCP 流量。
udp	指定 UDP 流量。

命令默认

默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT xlate。安装了以下默认规则：

```
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
```

注 这些规则无法删除，无论手动创建什么规则，它们始终存在。因为会按顺序评估规则，所以可以忽略默认规则。例如，要使这些规则完全失效，可以添加以下拒绝规则：

```
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
```

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	• 是	• 是	• 是	-

命令历史记录

版本	修改
9.0(1)	添加了此命令。

使用指南

每会话 PAT 功能可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归主单元所有。在每会话 PAT 会话结束时，ASA 将发送重置并立即删除 xlate。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。对于“命中并运行”的数据流，例如 HTTP 或 HTTPS，每会话功能可以显著提高一个地址支持的连接速度。不使用每会话功能时，一个用于 IP 协议的地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 65535/*average-lifetime*。

默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT xlate。对于可受益于多会话 PAT 的流量，例如 H.323、SIP 或 Skinny，您可以创建每会话拒绝规则来禁用每会话 PAT。

添加的每会话 PAT 规则在默认规则上面，但在任何其他手动创建的规则下面。确保按照所需的应用顺序创建规则。

示例

以下示例为 H.323 流量创建拒绝规则，以便它使用多会话 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
```

相关命令

命令	描述
clear configure xlate	清除 **xlate 每会话**规则。
nat (global)	添加一个两倍 NAT 规则。
nat (object)	添加对象 NAT 规则。
show running-config xlate	显示 **xlate 每会话**规则。

区域

要添加流量区域，请在全局配置模式下使用 **zone** 命令。要删除区域，请使用此命令的 **no** 形式。

zone *name*

no zone *name*

语法说明

name	设置最多 48 个字符的时区名称。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
9.3(2)	添加了此命令。

使用指南

您可以向*流量区域*分配多个接口，让现有流中的流量在该区域内的任何接口流出或流入 ASA。此功能允许 ASA 上的等价多路径 (ECMP) 路由以及多个接口分担流向 ASA 的外部流量负载均衡。

区域允许流量进出区域中的任何接口，但安全策略（访问规则、NAT 等）本身仍然应用于每个接口，而非每个区域。如果为区域中的所有接口配置相同的安全策略，则可对该流量成功实施 ECMP 和负载均衡。

您最多可以创建 256 个区域。

示例

以下示例配置具有 4 个成员接口的外部区域：

```
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
```

相关命令

命令	描述
clear configure zone	清除区域配置。
clear conn zone	清除区域连接。
clear local-host zone	清除区域主机。
show asp table routing	显示用于调试的加速安全路径表，并显示与每个路由关联的区域。
show asp table zone	显示用于调试的加速安全路径表。
show conn long	显示区域的连接信息。
show local-host zone	显示区域内本地主机的网络状态。
show nameif zone	显示接口名称和区域名称。
show route zone	显示区域接口的路由。
show running-config zone	显示区域配置。
show zone	显示区域 ID、情景、安全级别和成员。
zone-member	将接口分配给流量区域。

zonelabs-integrity fail-close

要配置 ASA，使 VPN 客户端连接在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败时关闭，请在全局配置模式下使用 **zonelabs-integrity fail-close** 命令。要恢复默认设置，使 VPN 连接在 Zone Labs 连接失败时保持打开，请使用此命令的 **no** 形式。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

语法说明描述

此命令没有任何参数或关键字。

默认值

默认情况下，连接在失败时保持打开。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

如果主要 Zone Labs Integrity 防火墙服务器不响应 ASA，ASA 在默认情况下仍会建立到专用网络的 VPN 客户端连接。它也会保持现有打开的连接。这可确保企业 VPN 不会因防火墙服务器发生故障而中断。但是，如果您不希望 VPN 连接在 Zone Labs Integrity 防火墙服务器失败时保持运行，请使用 **zonelabs-integrity fail-close** 命令。

要恢复默认状况，使 ASA 在 Zone Labs Integrity 防火墙服务器的连接失败时保持客户端 VPN 连接，请使用 **zonelabs-integrity fail-open** 命令。

示例

以下示例配置 ASA 在 Zone Labs Integrity 防火墙服务器未响应或连接中断时关闭 VPN 客户端连接。

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity fail-open	指定到 ASA 的 VPN 客户端连接在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败后保持打开。
zonelabs-integrity fail-timeout	指定 ASA 宣告无响应的 Zone Labs Integrity 防火墙服务器不可达之前所经过的时间（秒）。
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。

zonelabs-integrity fail-open

为使 ASA 的远程 VPN 客户端连接在 ASA 与 Zone Labs Integrity 防火墙服务之间的连接失败后保持打开，请在全局配置模式下使用 **zonelabs-integrity fail-open** 命令。要在 Zone Labs 服务器连接失败时关闭 VPN 客户端连接，请使用此命令的 **no** 形式。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，如果 ASA 无法建立或保持与 Zone Labs Integrity 防火墙服务器的连接，远程 VPN 连接将保持打开。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

如果主要 Zone Labs Integrity 防火墙服务器不响应 ASA，ASA 在默认情况下仍会建立到专用网络的 VPN 客户端连接。它还会保持现有打开的连接。这可确保企业 VPN 不会因防火墙服务器发生故障而中断。但是，如果您不希望 VPN 连接在 Zone Labs Integrity 防火墙服务器失败时保持运行，请使用 **zonelabs-integrity fail-close** 命令。然后要恢复默认状况，使 ASA 在 Zone Labs Integrity 防火墙服务器的连接失败时保持客户端 VPN 连接，请使用 **zonelabs-integrity fail-open** 命令或 **no zonelabs-integrity fail-open** 命令。

示例

以下示例恢复默认状况，使 VPN 客户端连接在 Zone Labs Integrity 防火墙服务器的连接失败时保持打开：

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity fail-close	指定 ASA 在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败时关闭 VPN 客户端连接。
zonelabs-integrity fail-timeout	指定 ASA 宣告无响应的 Zone Labs Integrity 防火墙服务器不可达之前所经过的时间（秒）。

zonelabs-integrity fail-timeout

要指定 ASA 在宣告无响应的 Zone Labs Integrity 防火墙服务器不可达之前所经过的时间（秒），请在全局配置模式下使用 **zonelabs-integrity fail-timeout** 命令。要恢复 10 秒的默认超时值，请使用此命令的 **no** 形式，不带任何参数。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

语法说明

timeout	ASA 宣告无响应的 Zone Labs Integrity 防火墙服务器不可达之前所经过的秒数。接受的范围从 5 到 20 秒。

默认值

默认超时值为 10 秒。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

如果 ASA 等待指定的秒数后没有收到 Zone Labs 服务器的响应，便宣告该服务器无响应。VPN 客户端连接默认保持打开，或者使用 **zonelabs-integrity fail-open** 命令配置为保持打开。但是，如果已发出 **zonelabs-integrity fail-close** 命令，该连接将在 ASA 宣告 Integrity 服务器无响应时关闭。

示例

以下示例配置 ASA 在 12 秒后宣告主用 Zone Labs Integrity 服务器不可达：

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity fail-open	指定到 ASA 的 VPN 客户端连接在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败后保持打开。
zonelabs-integrity fail-close	指定 ASA 在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败时关闭 VPN 客户端连接。
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。

zonelabs-integrity interface

要指定 ASA 接口用于与 Zone Labs Integrity 服务器通信，请在全局配置模式下使用 **zonelabs-integrity interface** 命令。要将 Zone Labs Integrity 防火墙服务器接口重置回默认值 none（无），请使用此命令的 **no** 形式。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

语法说明

Interface	指定与 Zone Labs Integrity 防火墙服务器通信的 ASA 接口。这通常是使用 **nameif** 命令创建的接口名称。

默认值

默认情况下，Zone Labs Integrity 防火墙服务器接口设置为 none（无）。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

示例

以下示例使用 10.0.0.5 到 10.0.0.7 范围的 IP 地址配置三个 Zone Labs Integrity 服务器。这些命令也配置 ASA 在端口 300 以及称为 inside 的接口上侦听服务器：

```
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)#
```

相关命令

命令	描述
zonelabs-integrity port	指定 ASA 上用于与 Zone Labs Integrity 防火墙服务器通信的端口。
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。
zonelabs-integrity ssl-certificate-port	指定 Zone Labs Integrity 防火墙服务器在检索 SSL 证书时要连接的 ASA 端口。
zonelabs-integrity ssl-client-authentication	允许 ASA 使用 Zone Labs Integrity 防火墙服务器 SSL 证书进行身份验证。

zonelabs-integrity port

要指定 ASA 用于与 Zone Labs Integrity 防火墙服务器通信的端口，请在全局配置模式下使用 **zonelabs-integrity port** 命令。要为 Zone Labs Integrity 防火墙服务器恢复为默认端口 5054，请使用此命令的 **no** 形式。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

语法说明

port	指定 ASA 上的 Zone Labs Integrity 防火墙服务器端口。
port_number	Zone Labs Integrity 防火墙服务器的端口号。范围为 10 至 10000。

默认值

默认 Zone Labs Integrity 防火墙服务器端口是 5054。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

ASA 在分别使用 **zonelabs-integrity port** 和 **zonelabs-integrity interface** 命令配置的端口和接口上侦听 Zone Labs Integrity 防火墙服务器。

注 ASA 的当前版本每次只支持一个 Integrity 服务器，即使用户接口支持多达五个 Integrity 服务器的配置也一样。如果主用服务器失败，可在 ASA 中配置其他 Integrity Server 并重建客户端 VPN 会话。

示例

以下示例使用 IP 地址 10.0.0.5 配置 Zone Labs Integrity 服务器。这些命令也配置 ASA 在端口 300（而非默认端口 5054）上侦听主用 Zone Labs 服务器：

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity interface	指定 ASA 与主用 Zone Labs Integrity 服务器通信的接口。
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。
zonelabs-integrity ssl-certificate-port	指定 Zone Labs Integrity 防火墙服务器在检索 SSL 证书时要连接的 ASA 端口。
zonelabs-integrity ssl-client-authentication	允许 ASA 使用 Zone Labs Integrity 防火墙服务器 SSL 证书进行身份验证。

zonelabs-integrity server-address

要将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置，请在全局配置模式下使用 **zonelabs-integrity server-address** 命令。通过 IP 地址或主机名指定 Zone Labs 服务器。

要从运行配置删除 Zone Labs Integrity 防火墙服务器，请使用此命令的 **no** 形式，并且不含参数。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

注 尽管用户接口似乎支持多个 Integrity 服务器的配置，但 ASA 在当前版本中每次仅支持一部服务器。

语法说明

hostname	指定 Zone Labs Integrity 防火墙服务器的主机名。有关主机名指导原则，请参阅 **name** 命令。
ip-address	指定 Zone Labs Integrity 防火墙服务器的 IP 地址。

命令默认

默认情况下未配置 Zone Labs Integrity 防火墙服务器。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

使用此版本时，可以配置一个 Zone Labs Integrity 防火墙服务器。如果该服务器失败，则先配置另一个 Integrity 服务器，然后重建客户端 VPN 会话。

要通过主机名指定服务器，必须先使用 **name** 命令配置 Zone Labs 服务器名称。在使用 **name** 命令之前，请先使用 **names** 命令启用它。

注 安全设备的当前版本每次只支持一个 Integrity Server，即使用户接口支持多达五个 Integrity Server 的配置也一样。如果主用服务器失败，可在 ASA 中配置其他 Integrity Server 并重建客户端 VPN 会话。

示例

以下示例将服务器名称 ZL-Integrity-Svr 分配到 IP 地址 10.0.0.5，并且使用该名称配置 Zone Labs Integrity 服务器：

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity fail-close	指定 ASA 在 ASA 与 Zone Labs Integrity 防火墙服务器之间的连接失败时关闭 VPN 客户端连接。
zonelabs-integrity interface	指定 ASA 与主用 Zone Labs Integrity 服务器通信的接口。
zonelabs-integrity port	指定 ASA 上用于与 Zone Labs Integrity 防火墙服务器通信的端口。
zonelabs-integrity ssl-certificate-port	指定 Zone Labs Integrity 防火墙服务器在检索 SSL 证书时要连接的 ASA 端口。
zonelabs-integrity ssl-client-authentication	允许 ASA 使用 Zone Labs Integrity 防火墙服务器 SSL 证书进行身份验证。

zonelabs-integrity ssl-certificate-port

要指定 Zone Labs Integrity 防火墙服务器在检索 SSL 证书时要连接的 ASA 端口，请在全局配置模式下使用 **zonelabs-integrity ssl-certificate-port** 命令。要恢复为默认端口号 (80)，请使用此命令的 **no** 形式且不带参数。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

语法说明

cert-port-number	指定 ASA 预期 Zone Labs Integrity 防火墙服务器在请求 SSL 证书时要连接的端口号。

默认值

默认情况下，ASA 预期 Zone Labs Integrity 防火墙服务器在端口 80 上请求 SSL 证书。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

对于 ASA 与 Zone Labs Integrity 防火墙服务器之间的 SSL 通信，ASA 是 SSL 服务器，Zone Labs 服务器是 SSL 客户端。发起 SSL 连接时，SSL 服务器 (ASA) 的证书必须由客户端（Zone Labs 服务器）进行身份验证。**zonelabs-integrity ssl-certificate-port** 命令指定 Zone Labs 服务器在请求 SSL 服务器证书时连接的端口。

示例

以下示例配置 ASA 上的端口 30 接收来自 Zone Labs Integrity 服务器的 SSL 证书请求：

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity port	指定 ASA 上用于与 Zone Labs Integrity 防火墙服务器通信的端口。
zonelabs-integrity interface	指定 ASA 与主用 Zone Labs Integrity 服务器通信的接口。

命令	描述
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。
zonelabs-integrity ssl-client-authentication	允许 ASA 使用 Zone Labs Integrity 防火墙服务器 SSL 证书进行身份验证。

zonelabs-integrity ssl-client-authentication

要启用 ASA 的 Zone Labs Integrity 防火墙服务器 SSL 证书身份验证，请在全局配置模式下使用 **zonelabs-integrity ssl-client-authentication** 命令，并且带 *enable* 参数。要禁用 Zone Labs SSL 证书身份验证，请使用 *disable* 参数，或者使用此命令的 **no** 形式且不带参数。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

语法说明

disable	指定 Zone Labs Integrity 防火墙服务器的 IP 地址。
enable	指定 ASA 对 Zone Labs Integrity 防火墙服务器的 SSL 证书进行身份验证。

默认值

默认情况下，禁用 ASA 的 Zone Labs Integrity 防火墙服务器 SSL 证书身份验证。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	-	-

命令历史记录

版本	修改
7.2(1)	添加了此命令。

使用指南

对于 ASA 与 Zone Labs Integrity 防火墙服务器之间的 SSL 通信，ASA 是 SSL 服务器，Zone Labs 服务器是 SSL 客户端。发起 SSL 连接时，SSL 服务器 (ASA) 的证书必须由客户端（Zone Labs 服务器）进行身份验证。但客户端证书的身份验证可选。可以使用 **zonelabs-integrity ssl-client-authentication** 命令启用或禁用 ASA 的 Zone Lab 服务器（SSL 客户端）证书身份验证。

示例

以下示例配置 ASA 对 Zone Labs Integrity 防火墙服务器 SSL 证书进行身份验证。

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

相关命令

命令	描述
zonelabs-integrity interface	指定 ASA 与主用 Zone Labs Integrity 服务器通信的接口。
zonelabs-integrity port	指定 ASA 上用于与 Zone Labs Integrity 防火墙服务器通信的端口。

命令	描述
zonelabs-integrity server-address	将 Zone Labs Integrity 防火墙服务器添加到 ASA 配置。
zonelabs-integrity ssl-certificate-port	指定 Zone Labs Integrity 防火墙服务器在检索 SSL 证书时要连接的 ASA 端口。

zone-member

要将接口添加到流量区域，请在接口配置模式下使用 **zone-member** 命令。要删除接口，可使用此命令的 **no** 形式。

zone-member *name*

no zone-member *name*

语法说明

name	标识 **zone** 命令设置的区域名称。

命令默认

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
全局配置	• 是	-	• 是	• 是	-

命令历史记录

版本	修改
9.3(2)	添加了此命令。

使用指南

配置所有接口参数，包括名称、IP 地址和安全级别。添加到区域的第一个接口决定区域的安全级别。所有其他接口必须具有相同的安全级别。要更改区域中接口的安全级别，除了一个接口之外，所有其他接口都必须删除，然后更改安全级别，再重新添加接口。

将接口分配到区域时，该接口上的所有连接都会删除。必须重新建立连接。

如果从区域删除某个接口，以该接口为主接口的连接都会删除。必须重新建立连接。如果该接口是当前接口，ASA 会将连接移回主接口。区域路由表也会刷新。

您可以将以下类型的接口添加到区域：

- 物理
- VLAN
- EtherChannel
- 冗余

您不能添加以下类型的接口：

- 管理专用
- 管理访问
- 故障切换或状态链路

- 集群控制链路
- EtherChannel 或冗余接口中的成员接口

接口只能是一个区域的成员。

每个区域最多可包含 8 个接口。

示例

以下示例配置具有 4 个成员接口的外部区域：

```
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
```

相关命令

命令	描述
clear configure zone	清除区域配置。
clear conn zone	清除区域连接。
clear local-host zone	清除区域主机。
show asp table routing	显示用于调试的加速安全路径表，并显示与每个路由关联的区域。
show asp table zone	显示用于调试的加速安全路径表。
show conn long	显示区域的连接信息。
show local-host zone	显示区域内本地主机的网络状态。
show nameif zone	显示接口名称和区域名称。
show route zone	显示区域接口的路由。
show running-config zone	显示区域配置。
show zone	显示区域 ID、情景、安全级别和成员。
zone	配置流量区域。

第 2 部分

用于 ASA 服务模块的思科 IOS 命令

用于 ASASM 的思科 IOS 命令

clear diagnostics loopback

要清除在线诊断测试配置，请在特权 EXEC 模式下使用 **clear diagnostic loopback** 命令。

clear diagnostics loopback

语法说明

此命令没有任何参数或关键字

默认值

无默认行为或值。

命令模式

特权 EXEC

使用指南

clear diagnostics loopback 命令用于清除在线诊断测试配置。

示例

以下是 **clear diagnostics loopback** 命令的输出示例：

```
ciscoasa# clear diagnostics loopback

Port    Test    Pkts-received  Failures
0       0       0              0
1       0       0              0
```

相关命令

命令	描述
show diagnostics loopback	显示与 PC 环回测试、测试运行数、收到的环回数据包数量及检测到的失败次数相关的信息。

firewall autostate

要启用自动状态消息，请在全局配置模式下使用 **firewall autostate** 命令。要禁用自动状态，则使用此命令的 **no** 形式。

firewall autostate

no firewall autostate

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，禁用自动状态。

命令模式

全局配置

使用指南

自动状态消息可让 ASA 快速检测失败或运行的交换机接口。管理引擎可向 ASA 发送自动状态消息，说明与 ASA VLAN 关联的物理接口状态。例如，当与 VLAN 关联的所有物理接口关闭时，自动状态消息会告知 ASA VLAN 已关闭。此信息可让 ASA 宣告 VLAN 已关闭，避免像平常一样需要通过监测接口来确定链路故障端。自动状态消息大幅缩短了 ASA 检测链路故障的时间（只需要几毫秒，而没有自动状态支持时则需要长达 45 秒）。

交换机管理引擎在以下情况下会向 ASA 发送自动状态消息：

- 属于 VLAN 的最后一个接口关闭。
- 属于 VLAN 的第一个接口打开。

示例

以下示例启用自动状态消息：

```
Router(config)# firewall autostate
```

相关命令

命令	描述
show firewall autostate	显示自动状态功能的设置。

firewall module

要向 ASA 分配防火墙组，请在全局配置模式下输入 **firewall module** 命令。要删除防火墙组，则使用此命令的 **no** 形式。

firewall module *module_number* **vlan-group** *firewall_group*

no firewall module *module_number* **vlan-group** *firewall_group*

语法说明

module_number	指定模块编号。使用 **show module** 命令查看已安装的模块及其编号。
vlan-group *firewall_group*	按照 **firewall vlan-group** 命令的定义指定一个或多个组编号。 • 单一编号 (*n*) • 范围 (*n-x*) 不同的编号或范围用逗号分隔。例如，输入以下编号： `5,7-10`

默认值

无默认行为或值。

命令模式

全局配置

使用指南

- 您可以为每个 ASASM 最多分配 16 个防火墙 VLAN 组。（您可以在思科 IOS 软件中创建超过 16 个 VLAN 组，但每个 ASASM 只可分配 16 个组。）请参阅 **firewall vlan-group** 命令以创建一个组。例如，您可以将所有 VLAN 分配到一个组；也可以创建内部组和外部组；还可以为每位用户创建一个组。
- 每个组的 VLAN 数没有限制，但 ASASM 只能使用 ASASM 系统最大限制范围内的 VLAN（有关详细信息，请参阅 ASASM 许可文档）。
- 您不能将同一个 VLAN 分配到多个防火墙组。
- 可以将单个防火墙组分配到多个 ASASM。例如，您想要分配到多个 ASASM 的 VLAN 可以位于每个 ASASM 独有的 VLAN 中的单独组中。
- 如果在同一交换机机箱内使用 ASASM 故障切换，请勿将为故障切换和状态通信保留的 VLAN 分配到交换机端口。但是，如果在机箱之间使用故障切换，则必须在机箱之间的中继端口中包含 VLAN。
- 如果 VLAN 在分配到 ASASM 之前未添加到交换机，VLAN 将存储在管理引擎数据库中，并且在添加到交换机时发送到 ASASM。
- 在交换机上分配 VLAN 之前，您可以在 ASASM 配置中配置它。请注意，当交换机将 VLAN 发送到 ASASM 时，该 VLAN 默认在 ASASM 上管理性打开，而不管您是否在 ASASM 配置中关闭它们。这种情况下您需要将其再次关闭。

示例

以下示例展示如何创建三个防火墙 VLAN 组：每个 ASA 一个，还有一个包含分配到两个 ASA 的 VLAN。

```
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
```

以下是 **show firewall vlan-group** 命令的输出示例：

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

以下是 **show firewall module** 命令的输出示例，其中显示所有 VLAN 组：

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

相关命令

命令	描述
firewall vlan-group	将 VLAN 分配到 VLAN 组。
show firewall module vlan-group	显示 VLAN 组和分配给它们的 VLAN。
show module	显示所有已安装的模块。

firewall multiple-vlan-interfaces

为了让您将多个 SVI 添加到 ASA，请在全局配置模式下使用 **firewall multiple-vlan-interfaces** 命令。要禁用此功能，请使用此命令的 **no** 形式。

firewall multiple-vlan-interfaces

no firewall multiple-vlan-interfaces

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，不允许多个 SVI。

命令模式

全局配置

使用指南

MSFC 上定义的 VLAN 称为交换虚拟接口。如果将用于 SVI 的 VLAN 分配到 ASA，则 MSFC 将在 ASA 与另一个第 3 层 VLAN 之间路由。出于安全原因，默认情况下 MSFC 与 ASA 之间只能存在一个 SVI。例如，如果您使用多个 SVI 误配置了系统，可能会由于同时将内部和外部 VLAN 分配到 MSFC 而意外允许流量通过 ASA。

但在某些网络情景中可能需要绕过 ASA。例如，如果在与 IP 主机相同的以太网网段中有 IPX 主机，则会需要多个 SVI。由于 ASA 在路由的防火墙模式下只处理 IP 流量，而会丢弃其他协议流量，例如 IPX（透明防火墙模式可选择性允许非 IP 流量），您可能希望为 IPX 流量绕过 ASA。确保使用访问列表配置 MSFC，只允许 IPX 流量通过 VLAN。

对于多情景模式下的透明防火墙，您需要使用多个 SVI，因为每个情景的外部接口上都需要唯一 VLAN。也可以选择在路由模式下使用多个 SVI，这样便无需共享用于外部接口的单一 VLAN。

示例

以下示例展示典型的多 SVI 配置：

```
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#
```

以下是 **show interface** 命令的输出示例：

```
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
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	定义 VLAN 组。

firewall vlan-group

要将 VLAN 分配到防火墙组，请在全局配置模式输入 **firewall vlan-group** 命令。要删除 VLAN，则使用此命令的 **no** 形式。

firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

no firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

语法说明

firewall_group	指定组 ID 为整数。
vlan_range	指定分配到组的 VLAN。*vlan_range* 值可以是通过以下方法之一识别的一个或多个 VLAN（2-1000 和 1025-4094）： • 单一编号 (*n*) • 范围 (*n-x*) 不同的编号或范围用逗号分隔。例如，输入以下编号： `5,7-10,13,45-100` **注** 路由端口和 WAN 端口消耗内部 VLAN，因此，1020-1100 范围内的 VLAN 可能已在使用中。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

全局配置。

使用指南

- 使用 **firewall module** 命令最多可将 16 个防火墙 VLAN 组分配到每个 ASASM。（您可以在思科 IOS 软件中创建超过 16 个 VLAN 组，但每个 ASASM 只可分配 16 个组。）例如，您可以将所有 VLAN 分配到一个组；也可以创建内部组和外部组；还可以为每位用户创建一个组。
- 每个组的 VLAN 数没有限制，但 ASASM 只能使用 ASASM 系统最大限制范围内的 VLAN（有关详细信息，请参阅 ASASM 许可文档）。
- 您不能将同一个 VLAN 分配到多个防火墙组。
- 可以将单个防火墙组分配到多个 ASASM。例如，您想要分配到多个 ASASM 的 VLAN 可以位于每个 ASASM 独有的 VLAN 中的单独组中。
- 使用 2-1000 和 1025-4094 的 VLAN ID。
- 路由端口和 WAN 端口消耗内部 VLAN，因此，1020-1100 范围内的 VLAN 可能已在使用中。
- 不能使用保留的 VLAN。
- 不能使用 VLAN 1。
- 如果在同一交换机机箱内使用 ASASM 故障切换，请勿将为故障切换和状态通信保留的 VLAN 分配到交换机端口。但是，如果在机箱之间使用故障切换，则必须在机箱之间的中继端口中包含 VLAN。

- 如果 VLAN 在分配到 ASASM 之前未添加到交换机，VLAN 将存储在管理引擎数据库中，并且在添加到交换机时发送到 ASASM。
- 在交换机上分配 VLAN 之前，您可以在 ASASM 配置中配置它。请注意，当交换机将 VLAN 发送到 ASASM 时，该 VLAN 默认在 ASASM 上管理性打开，而不管您是否在 ASASM 配置中关闭它们。这种情况下您需要将其再次关闭。

示例

以下示例展示如何创建三个防火墙 VLAN 组：每个 ASA 一个，还有一个包含分配到两个 ASA 的 VLAN。

```
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
```

以下是 **show firewall vlan-group** 命令的输出示例：

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

以下是 **show firewall module** 命令的输出示例，其中显示所有 VLAN 组：

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
show firewall vlan-group	显示 VLAN 组和分配给它们的 VLAN。
show module	显示所有已安装的模块。

service-module session

要从交换机 CLI 获得对 ASASM 的控制台访问，请在特权 EXEC 模式下输入 **service-module session** 命令。

service-module session [**switch** {**1** | **2**}] **slot** *number*

语法说明

slot *number*	指定 ASASM 的插槽编号。要查看模块插槽编号，请在交换机提示符下输入 **show module** 命令。
switch {**1**	**2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

特权 EXEC

使用指南

使用 **service-module session** 命令，创建 ASASM 的虚拟控制台连接，此虚拟连接具有实际控制台连接的所有优点和限制。

可以获得以下优势：

- 在重新加载时连接会保持，不会超时。
- 可以通过 ASASM 重新加载保持连接并查看启动消息。
- 如果 ASASM 无法加载镜像，可以访问 ROMMON。

限制包括：

- 连接缓慢（9600 波特）。
- 每次只能激活一个控制台连接。

注 由于连接的保持性，如果不正常注销 ASASM，连接存在时间可能超过预期。如果其他人希望登录，他们需要先中断现有连接。有关详细信息，请参阅 CLI 配置指南。

示例

以下示例展示如何获得对插槽 3 中 ASASM 的控制台访问：

```
Router# service-module session slot 3
ciscoasa>
```

相关命令

命令	描述
session	通过背板 Telnet 连接 ASASM。

session

要从交换机 CLI 通过背板 Telnet 连接 ASASM，请在特权 EXEC 模式下使用 **session** 命令。

session [**switch** {**1** | **2**}] **slot** *number* **processor 1**

语法说明

processor 1	指定处理器编号，始终为 1。
slot *number*	指定插槽编号。要查看模块插槽编号，请在交换机提示符下输入 **show module** 命令。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

特权 EXEC

使用指南

使用 **session** 命令创建到 ASASM 的 Telnet 连接。

可以获得以下优势：

- 可以同时拥有多个到 ASASM 的会话。
- Telnet 会话是快速连接。

限制包括：

- Telnet 会话在 ASASM 重新加载时终止，并且可能会超时。
- 在 ASASM 完全加载之前无法访问它；不能访问 ROMMON。

注 其他服务模块支持的 **session** *slot* **processor 0** 命令在 ASASM 上不受支持；ASASM 没有处理器 0。

系统将提示您输入登录密码。请输入 ASASM 的登录密码。默认密码为 **cisco**。

您将进入用户 EXEC 模式。

示例

以下示例通过 Telnet 连接到处理器 1 中的 ASASM：

```
Router# session slot number processor 1
ciscoasa passwd: cisco
ciscoasa>
```

相关命令

命令	描述
service-module session	从交换机 CLI 获取对 ASASM 的控制台访问。

show boot device

要查看默认引导分区，请使用 **show boot device** 命令。

show boot device [*mod_num*]

语法说明

mod_num	（可选）指定模块编号。使用 **show module** 命令查看已安装的模块及其编号。

默认值

默认引导分区是 cf:4。

命令模式

特权 EXEC。

示例

以下是 **show boot device** 命令的输出示例，该命令展示安装在思科 IOS 软件上的每个 ASA 的引导分区：

```
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 ]:
```

相关命令

命令	描述
boot device (IOS)	设置默认引导分区。
show module (IOS)	显示所有已安装的模块。

show diagnostic loopback

要显示与 PC 环回测试相关的相关信息，包括测试运行次数、收到的环回数据包数和检测到的失败数，请在特权 EXEC 模式下使用 **show diagnostics loopback** 命令。

show diagnostics loopback

语法说明

此命令没有任何参数或关键字

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	•	•	•	-	•

命令历史记录

版本	修改
12.2(18)SXF5	添加了此命令。

使用指南

show diagnostic loopback 命令提供与 PC 环回测试相关的信息，包括测试次数、收到的环回数据包数和检测到的失败数。

示例

以下是 **show diagnostics loopback** 命令的输出示例：

```
ciscoasa# show diagnostics loopback

Port    Test    Pkts-received  Failures
0       447     447            0
1       447     447            0
```

相关命令

命令	描述
clear diagnostics loopback	清除在线诊断测试配置。
firewall autostate	启用自动状态功能。

show firewall autostate

要查看自动状态功能的设置，请在特权 EXEC 模式下使用 **show firewall autostate** 命令。

show firewall autostate

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，禁用自动状态。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	•	•	•	•	•

使用指南

思科 IOS 软件中的自动状态消息允许 ASA 快速检测失败或运行的交换机接口。交换机管理引擎在以下情况下会向 ASA 发送自动状态消息：

- 属于 VLAN 的最后一个接口关闭。
- 属于 VLAN 的第一个接口打开。

相关命令

命令	描述
clear diagnostics loopback	清除在线诊断测试配置。
firewall autostate	启用自动状态功能。

show firewall module

要查看分配到每个 ASA 的 VLAN 组，请在特权 EXEC 模式下输入 **show firewall module** 命令。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*]

语法说明

module_number	（可选）指定模块编号。使用 **show module** 命令查看已安装的模块及其编号。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	•	•	•	•	•

示例

以下是 **show firewall module** 命令的输出示例，其中显示所有 VLAN 组：

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	将 VLAN 分配到 VLAN 组。
show firewall module vlan-group	显示 VLAN 组和分配给它们的 VLAN。
show module	显示所有已安装的模块。

show firewall module state

要查看每个 ASA 的状态，请在特权 EXEC 模式下输入 **show firewall module state** 命令。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **state**

语法说明

module_number	（可选）指定模块编号。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	•	•	•	•	•

示例

以下是 **show firewall module state** 命令的输出示例：

```
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:
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	将 VLAN 分配到 VLAN 组。
show firewall module vlan-group	显示 VLAN 组和分配给它们的 VLAN。
show module	显示所有已安装的模块。

show firewall module traffic

要查看通过每个 ASA 的流量，请在特权 EXEC 模式下输入 **show firewall module traffic** 命令。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **traffic**

语法说明

module_number	（可选）指定模块编号。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	•	•	•	•	•

示例

以下是 **show firewall module traffic** 命令的输出示例：

```
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
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	将 VLAN 分配到 VLAN 组。
show firewall module vlan-group	显示 VLAN 组和分配给它们的 VLAN。
show module	显示所有已安装的模块。

show firewall module version

要查看 ASA 服务模块的软件版本编号，请在特权 EXEC 模式下输入 **show firewall module version** 命令。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **version**

语法说明

module_number	（可选）指定模块编号。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	• 是	• 是	• 是	• 是	• 是

示例

以下是 **show firewall module version** 命令的输出示例：

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	创建一组 VLAN。
show module	显示所有已安装的模块。

show firewall module vlan-group

要查看可分配到 ASA 的 VLAN 组，请在特权 EXEC 模式下输入 **show firewall module vlan-group** 命令。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **vlan-group** [*firewall_group*]

语法说明

firewall_group	（可选）指定组 ID。
module_number	（可选）指定模块编号。
switch {**1** | **2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	•	•	•	•	•

示例

以下是 **show firewall module vlan-group** 命令的输出示例：

```
Router# show firewall module vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	创建一组 VLAN。
show module	显示所有已安装的模块。

show firewall multiple-vlan-interfaces

要为 ASASM 显示多个防火墙 VLAN 接口的状态，请在特权 EXEC 模式下输入 **show firewall multiple-vlan-interfaces** 命令。

show firewall multiple-vlan-interfaces

语法说明

此命令没有任何参数或关键字。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	一个	情景	系统
特权 EXEC	•	•	•	•	•

示例

以下是 **show firewall multiple-vlan-interfaces** 命令的输出示例：

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	创建一组 VLAN。
show module	显示所有已安装的模块。

show module

为检查交换机是否确认 ASASM 并使其上线，请在特权 EXEC 模式下使用 **show module** 命令。

show module [**switch** {**1** | **2**}] [*mod-num* | **all**]

语法说明

all	（可选）指定所有模块。
mod_num	（可选）指定模块编号。
switch {**1**	**2**}	（可选）对于 VSS 配置，指定交换机编号。

默认值

无默认行为或值。

命令模式

下表展示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**一个**	**情景**	**系统**
特权 EXEC	•	•	•	•	•

示例

以下是 **show module** 命令的输出示例：

```
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
```

相关命令

命令	描述
firewall module	将 VLAN 组分配到 ASA。
firewall vlan-group	创建一组 VLAN。

第 3 部分

参考

使用命令行界面

本章介绍如何在 ASA 中使用 CLI，包括以下部分：

注 CLI 使用类似于思科 IOS CLI 的语法和其他约定，但是 ASA 操作系统不是思科 IOS 软件版本。请勿假定思科 IOS CLI 命令适用于 ASA 或在其之上具有相同功能。

防火墙模式和安全情景模式

ASA 在以下模式的组合中运行：

- 透明防火墙或路由防火墙模式

  防火墙模式确定 ASA 是作为第 2 层还是第 3 层防火墙运行。

- 多情景模式或单情景模式

  安全情景模式确定 ASA 是作为单个设备还是作为多个安全情景（作用类似虚拟设备）运行。

有些命令仅在特定模式下可用。

命令模式和提示符

ASA CLI 包含各种命令模式。有些命令只能在特定模式下输入。例如，要输入显示敏感信息的命令，您需要输入密码并进入具有更多特权的模式。然后，为确保不会意外输入配置更改，必须进入配置模式。所有较低的命令均可在较高模式下输入。例如，可以在全局配置模式下输入特权 EXEC 命令。

注 各种类型的提示全部是默认提示，并且配置后可能会不同。

- 当处于系统配置模式或单情景模式时，提示以主机名开头：

  ```
  ciscoasa
  ```

- 列显提示字符串时，系统会解析提示配置并按照设置 **prompt** 命令的顺序列显已配置的关键字值。关键字参数可以是以下任意项并且可采用任意顺序：主机、域、情景、优先级、状态。

  ```
  asa(config)# prompt hostname context priority state
  ```

- 如果您在某一情景中，则提示符以主机名开头，后跟情景名称：

  ```
  ciscoasa/context
  ```

提示根据访问模式而异：

- 用户执行模式

  通过用户 EXEC 模式可查看最低 ASA 设置。首次访问 ASA 时，用户 EXEC 模式提示显示如下：

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 特权执行模式

  通过特权 EXEC 模式可查看特权级别内的所有当前设置。任何用户 EXEC 模式命令在特权 EXEC 模式下都将适用。在用户 EXEC 模式下输入 **enable** 命令（需要密码）可启动特权 EXEC 模式。提示包含数字符号 (#)：

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- 全局配置模式

  通过全局配置模式可更改 ASA 配置。所有用户 EXEC、特权 EXEC 和全局配置命令在此模式下均可用。在特权 EXEC 模式下输入 **configure terminal** 命令可启动全局配置模式。提示将更改为以下形式：

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 命令特定配置模式

  从全局配置模式下，某些命令可进入命令特定配置模式。所有用户 EXEC、特权 EXEC、全局配置和命令特定配置命令在此模式下均可用。例如，**interface** 命令会进入接口配置模式。提示将更改为以下形式：

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

语法格式

命令语法说明使用表 7-1 中列出的约定。

表 7-1　语法约定

约定	描述
粗体	粗体文本指示按字面显示输入的命令和关键字。
斜体	斜体文本指示由您提供值的参数。
[x]	方括号中包含可选元素（关键字或参数）。
|	竖线指示可选或必需的关键字或参数集中的选项。
[x | y]	将以竖线分隔的关键字或参数括起来的方括号指示可选选项。
{x | y}	将以竖线分隔的关键字或参数括起来的大括号指示必需选项。
[x {y | z}]	方括号或大括号的嵌套集合指示可选或必需元素中的可选或必需选项。方括号中的大括号和竖线指示可选元素中的必需选项。

缩写命令

您可以将大多数命令缩写为最少的命令独有字符；例如，您可以输入 **wr t**（而不是输入完整命令 **write terminal**）查看配置，也可以输入 **en** 启动特权模式以及输入 **conf t** 启动配置模式。此外，还可以输入 **0** 以表示 **0.0.0.0**。

命令行编辑

ASA 使用与思科 IOS 软件相同的命令行编辑约定。您可以使用 **show history** 命令查看所有以前输入的命令，或者使用向上箭头或 **^p** 命令逐个查看以前输入的命令。检查以前输入的命令后，您可以使用向下箭头或 **^n** 命令在列表中前移。到达想要重新使用的命令后，您可以编辑该命令或按 **Enter** 键启动该命令。您也可以使用 **^w** 删除光标左侧的字词，或使用 **^u** 删除该行。

ASA 在一条命令中最多允许 512 个字符；额外字符会被忽略。

命令补全

要在输入部分字符串后补全命令或关键字，请按 **Tab** 键。仅当部分字符串仅与一个命令或关键字匹配时，ASA 才会补全命令或关键字。例如，如果输入 **s** 并按 **Tab** 键，则 ASA 不会补全命令，因为它与多个命令匹配。但是，如果输入 **dis**，则 **Tab** 键会补全 **disable** 命令。

命令帮助

通过输入以下命令，可从命令行获取帮助信息：

- **help** *command_name*

  显示特定命令的帮助。

- *command_name* **?**

  显示可用参数列表。

- *string***?**（无空格）

  列出以字符串开头的可能命令。

- **?** 和 **+?**

  列出所有可用命令。如果输入 **?**，则 ASA 仅显示可用于当前模式的命令。要显示所有可用命令，包括可用于较低模式的命令，请输入 **+?**。

注 如果要在命令字符串中包含问号 (?)，则必须在键入问号之前按 **Ctrl-V**，以便避免意外调用 CLI 帮助。

查看运行配置

要查看运行配置，请使用以下命令之一。

要过滤命令输出，请参阅“过滤 show 和 more 命令输出”一节，第 7-4 页。

命令	目的
show running-config [**all**] [*command*]	显示运行配置。如果指定 **all**，则还会显示所有默认设置。如果指定 *command*，则输出仅包含相关命令。 **注** 许多关键字都显示为 *****。要以明文或加密形式查看密码（如果您启用了主口令），请使用下面的 **more** 命令。
more system:running-config	显示运行配置。如果您启用了主口令，则密码将以明文或加密形式显示。

过滤 show 和 more 命令输出

您可以将竖线 (|) 与任何 **show** 命令配合使用，并包含过滤器选项和筛选表达式。与思科 IOS 软件类似，通过将各输出行与正则表达式匹配来执行筛选。通过选择不同过滤器选项，可以包含或排除与表达式匹配的所有输出。您还可以显示以与表达式匹配的行开头的所有输出。

将筛选选项与 **show** 命令配合使用的语法如下：

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

或

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

注 **more** 命令可以查看任何文件（而不仅仅是运行配置）的内容；有关详细信息，请参阅命令参考。

在此命令字符串中，第一根竖线 (|) 是运算符，并且必须包含在命令中。此运算符将 **show** 命令的输出定向到过滤器。在语法图中，其他竖线 (|) 指示备用选项，并且不是命令的一部分。

include 选项包含与正则表达式匹配的所有输出行。不带 **-v** 的 **grep** 选项具有相同的效果。**exclude** 选项排除匹配正则表达式的所有输出行。带 **-v** 的 **grep** 选项具有相同的效果。**begin** 选项显示以与正则表达式匹配的行开头的所有输出行。

将 *regexp* 替换为任何思科 IOS 正则表达式。正则表达式未括在引号或双引号中，所以请注意后面的空格，它们也会被视为正则表达式的一部分。

创建正则表达式时，可以使用要与之匹配的任何字母或数字。此外，某些关键字字符（称为*元字符*）在正则表达式中使用时具有特殊含义。

使用 **Ctrl+V** 可转义 CLI 中的所有特殊字符，如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

重定向和附加 show 命令输出

您可以将 **show** 命令的输出内容重定向到设备上或远程位置的文件，而不是将其显示在屏幕上。当重定向到设备上的文件时，也可以将该命令输出附加到文件。

Show *command* | {**append** | **redirect**} *url*

- **append** *url* 将输出内容添加到现有文件。使用以下方法之一指定文件：
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*] - **flash** 和 **disk0** 指示 内部闪存。您可以使用任一选项。
  - **disk1:/**[[*path*/]*filename*] - 指示外部内存。
- **redirect** *url* 将创建指定的文件。如果文件已存在，则覆盖它。
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*] - **flash** 和 **disk0** 指示 内部闪存。您可以使用任一选项。
  - **disk1:/**[[*path*/]*filename*] - 指示外部内存。
  - **Smb:/[[path/]filename]/**[[*path*/]*filename*] - 指示服务器消息阻止，UNIX 服务器本地文件系统。
  - **Ftp://[[user[:password]@]server[:port]/[path/]filename[;type=xx]]**[[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*]] - 指示 FTP 服务器。**type** 可以是下列关键字之一：**ap**（ASCII 被动模式）、**an**（ASCII 普通模式）、**ip**（默认 - 二进制被动模式）、**in**（二进制普通模式）。
  - **Scp://[[user[:password]@]server[/path]/filename[;int=interface_name]]**[[*user*[**:***password*]@]*server*[**/***path*]*/filename*[**;int=***interface_name*]] - 指示 SCP 服务器。**;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问安全复制 (SCP) 服务器。
  - **Tftp://[[user[:password]@]server[:port]/[path/]filename[;int=interface_name]]**[[*user*[**:***password*]@]*server*[**:***port*]**/**[*path*/]*filename*[**;int=***interface_name*]] - 指示 TFTP 服务器。

获取 show 命令输出的行数

您可能不想查看实际的 **show** 命令输出，而只想查看输出内容的行数，或查看与正则表达式匹配的行数。然后，您可以轻松将此行数与您上次输入命令时的行数进行比较。当进行配置更改时，可将此当作一项快速检查。可以使用 **count** 关键字，或在 **grep** 关键字中添加 **-c**。

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

将 *regular_expression* 替换为任何思科 IOS 正则表达式。正则表达式未括在引号或双引号中，所以请注意后面的空格，它们也会被视为正则表达式的一部分。正则表达式是可选的；如果您不包含正则表达式，则计数将返回未经过滤的输出中的总行数。

创建正则表达式时，可以使用要与之匹配的任何字母或数字。此外，某些关键字字符（称为元字符）在正则表达式中使用时具有特殊含义。使用 **Ctrl+V** 可转义 CLI 中的所有特殊字符，如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

例如，要在 **show running-config** 输出中显示所有行的总数：

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

以下示例显示了如何快速检查有多少个接口在工作。第一个示例显示如何使用 **grep** 关键字与正则表达式仅过滤显示为正常运行状态的行。下一个示例添加了 **-c** 选项，仅会显示计数而非实际输出的行。

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

命令输出分页

对于如 **help** 或 **?**、**show**、**show xlate** 之类的命令或者提供长列表的其他命令，您可以决定是让信息显示一屏后暂停，还是让命令运行到完成为止。通过 **pager** 命令，您可以选择在 More 提示出现之前要显示的行数。

启用分页后，会出现以下提示：

```
<--- More --->
```

More 提示符使用与 UNIX **more** 命令类似的语法：

- 要查看另一屏信息，请按**空格**键。
- 要查看下一行，请按 **Enter** 键。
- 要返回到命令行，请按 **q** 键。

添加注释

您可以在某一行之前前置冒号 (:) 来创建注释。但是，该注释仅出现在命令历史记录缓冲区中，而不出现在配置中。因此，您可以使用 **show history** 命令或通过按箭头键检索以前的命令来查看注释，但是由于注释不在配置中，**write terminal** 命令不会显示注释。

文本配置文件

本节介绍如何设置可下载至 ASA 的文本配置文件的格式，包括以下主题：

命令如何与文本文件中的行相对应

文本配置文件包含与本指南中所述命令对应的行。

在示例中，命令之前前置有 CLI 提示。以下示例中的提示为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在系统未提示输出命令的文本配置文件中，会因此省略提示：

```
context a
```

命令特定配置模式命令

命令特定配置模式命令在命令行中输入时缩进显示在主命令下。只要这些命令紧跟在主命令后显示，便无需缩进文本行。例如，以下未缩进文本的读取与缩进文本相同：

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
   nameif outside
```

自动文本条目

将配置下载到 ASA 时，它会自动插入一些行。例如，ASA 为默认设置或为配置的修改时间插入行。创建文本文件时，无需输入这些自动条目。

行顺序

大致上，命令可以依照文件中的任何顺序。但是，某些行（例如 ACE）按其显示顺序进行处理，并且顺序可影响访问列表的功能。其他命令也可能具有顺序要求。例如，您必须先为接口输入 **nameif** 命令，因为许多后续命令都使用该接口的名称。此外，命令特定配置模式下的命令必须紧跟在主命令之后。

文本配置中不包括的命令

有些命令不会在配置中插入行。例如，**show running-config** 之类的运行时命令在文本文件中没有对应的行。

密码

登录、启用和用户密码存储在配置中之前会自动加密。例如，密码“cisco”的加密形式可能类似于 jMorNbK0514fadBh。您可以将配置密码以其加密形式复制到另一个 ASA，但是无法自行解密密码。

如果您在文本文件中输入了未加密的密码，则 ASA 不会在您将配置复制到 ASA 时将其自动加密。仅当使用 **copy running-config startup-config** 或 **write memory** 命令从命令行保存运行配置时，ASA 才会将其加密。

多个安全情景文件

对于多个安全情景，整个配置由以下多个部分组成：

- 安全情景配置
- 系统配置，用于确定 ASA 的基本设置，包括情景列表
- 管理情景，用于为系统配置提供网络接口

  系统配置不包含其自己的任何接口或网络设置。相反，当系统需要访问网络资源（例如从服务器下载情景）时，它会使用指定为管理情景的情景。

每个情景都类似于一个单情景模式配置。系统配置与情景配置的不同之处在于，系统配置仅包含系统命令（例如所有情景的列表），而其他典型命令不存在（例如许多接口参数）。

支持的字符集

ASA CLI 当前仅支持 UTF-8 编码。UTF-8 是 Unicode 符号的特定编码方案，并已设计为与符号的 ASCII 子集兼容。ASCII 字符在 UTF-8 中表示为单字节字符。所有其他字符在 UTF-8 中均表示为多字节符号。

完全支持 ASCII 可打印字符（0x20 到 0x7e）。可打印的 ASCII 字符与 ISO 8859-1 相同。UTF-8 是 ISO 8859-1 的超集，因此前 256 个字符 (0-255) 与 ISO 8859-1 相同。ASA CLI 最多支持 255 个 ISO 8859-1 字符（多字节字符）。