思科 ASA 系列命令参考，A 至 H 命令

更新日期：2014 年 11 月 5 日

Cisco Systems, Inc.
www.cisco.com

思科在全球设有 200 多个办事处。
地址、电话号码和传真号码
在思科网站上列出，网址为：
www.cisco.com/go/offices。

文本部件号：不适用，仅限在线使用

思科 ASA 系列命令参考，A 至 H 命令

第 1 部分

A 至 B 命令

第 1 章

aaa accounting command 至 accounting-server-group 命令

aaa accounting command

要在 CLI 上输入除 **show** 命令外的任何命令时将记账消息发送给 TACACS+ 记账服务器，请在全局配置模式下使用 **aaa accounting command** 命令。要禁用对命令记账的支持，请使用此命令的 **no** 形式。

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

语法说明

privilege *level*	如果您使用 **privilege** 命令定制命令特权级别，您可以通过指定最小特权级别来限制 ASA 包括的命令。ASA 不包括低于最小特权级别的命令。 **注**　如果输入弃用的命令并启用 **privilege** 关键字，则 ASA 不会为弃用的命令发送记账信息。如果要包括弃用的命令，请务必禁用 **privilege** 关键字。许多弃用的命令在 CLI 上仍被接受，且它们通常转换为 CLI 当前接受的命令；它们不包括在 CLI 帮助或本指南中。
tacacs+-server-tag	指定向其发送记账记录的 TACACS+ 服务器或服务器组，如 **aaa-server protocol** 命令所指定。

默认值

默认权限级别为 0。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在配置 **aaa accounting command** 命令时，会记录除管理员输入的 **show** 命令外的每个命令并将其发送给记账服务器或服务器组。

示例

以下示例指定为任何支持的命令生成记账记录，并将这些记录发送给来自名为 adminserver 的组的服务器：

```
ciscoasa(config)# aaa accounting command adminserver
```

相关命令

命令	说明
aaa accounting	启用或禁用 TACACS+ 或 RADIUS 用户记账（在 **aaa-server** 命令指定的服务器上）。
clear configure aaa	删除或重置配置的 AAA 记账值。
show running-config aaa	显示 AAA 配置。

aaa accounting console

要启用对用于管理访问的 AAA 记账的支持，请在全局配置模式下使用 **aaa accounting console** 命令。要禁用对用于管理访问的 AAA 记账的支持，请使用此命令的 **no** 形式。

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

no aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

语法说明

enable	启用记账记录的生成以标记条目并从特权 EXEC 模式退出。
serial	启用记账记录的生成以标记通过串行控制台接口建立的管理会话的建立和终止。
server-tag	指定向其发送记账记录的服务器组（由 **aaa-server protocol** 命令定义）。有效的服务器组协议是 RADIUS 和 TACACS+。
ssh	启用记账记录的生成以标记通过 SSH 创建的管理会话的建立和终止。
telnet	启用记账记录的生成以标记通过 Telnet 创建的管理会话的建立和终止。

默认值

默认情况下，禁用用于管理访问的 AAA 记账。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须指定先前在 **aaa-server** 命令中指定的服务器组的名称。

示例

以下示例指定为启用访问生成记账记录，并将这些记录发送给名为 adminserver 的服务器：

```
ciscoasa(config)# aaa accounting enable console adminserver
```

相关命令

命令	说明
aaa accounting match	启用或禁用 TACACS+ 或 RADIUS 用户记账（在 **aaa-server** 命令指定的服务器上）。
aaa accounting command	指定记录管理员 / 用户输入的具有指定特权级别或更高级别的每个命令或一组命令，并将其发送给记账服务器或服务器组。
clear configure aaa	删除或重置配置的 AAA 记账值。
show running-config aaa	显示 AAA 配置。

aaa accounting include, exclude

要启用对通过 ASA 的 TCP 或 UDP 连接的记账，请在全局配置模式下使用 **aaa accounting include** 命令。要将地址从记账中排除，请使用 **aaa accounting exclude** 命令。要禁用记账，请使用此命令的 **no** 形式。

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

语法说明

exclude	将指定的服务和地址从记账中排除（如果已由 **include** 命令指定）。
include	指定需要记账的服务和 IP 地址。不处理未由 **include** 语句指定的流量。
inside_ip	指定较高安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是目标地址。如果将命令应用于较高安全接口，则此地址是源地址。使用 0 表示所有主机。
inside_mask	指定内部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
interface_name	指定用户需要从中记账的接口名称。
outside_ip	（可选）指定较低安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是源地址。如果将命令应用于较高安全接口，则此地址是目标地址。使用 0 表示所有主机。
outside_mask	（可选）指定外部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
server_tag	指定 **aaa-server host** 命令定义的 AAA 服务器组。
service	指定需要记账的服务。您可以指定以下值之一： • **any** 或 **tcp/0**（指定所有 TCP 流量） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp/***port* • **udp/***port*

默认值

默认情况下，禁用用于管理访问的 AAA 记账。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 可以将关于通过 ASA 的任何 TCP 或 UDP 流量的记账信息发送给 RADIUS 或 TACACS+ 服务器。如果同时对该流量进行身份验证，则 AAA 服务器可以按用户名维护记账信息。如果未对该流量进行身份验证，则 AAA 服务器可以按 IP 地址维护记账信息。记账信息包括会话的开始和停止时间、用户名、会话时通过 ASA 的字节数、使用的服务以及每个会话的持续时间。

使用此命令前，您必须首先使用 **aaa-server** 命令指定一个 AAA 服务器。

要启用对 ACL 指定的流量的记账，请使用 **aaa accounting match** 命令。您无法在与 **include** 和 **exclude** 命令相同的配置中使用 **match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

您无法在具有相同安全性的接口之间使用 **aaa accounting include** 和 **exclude** 命令。对于该情况，您必须使用 **aaa accounting match** 命令。

示例

以下示例对所有 TCP 连接启用记账：

```
ciscoasa(config)# aaa-server mygroup protocol tacacs+
ciscoasa(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

相关命令

命令	说明
aaa accounting match	启用对 ACL 指定的流量的记账。
aaa accounting command	启用管理访问的记账。
aaa-server host	配置 AAA 服务器。
clear configure aaa	清除 AAA 配置。
show running-config aaa	显示 AAA 配置。

aaa accounting match

要启用对通过 ASA 的 TCP 和 UDP 连接的记账，请在全局配置模式下使用 **aaa accounting match** 命令。要禁用对流量的记账，请使用此命令的 **no** 形式。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

语法说明

acl_name	通过与 ACL 名称匹配来指定需要记账的流量。对 ACL 中的 permit 条目记账，但对 deny 条目免予记账。仅对 TCP 和 UDP 流量支持此命令。如果输入此命令，且它引用允许其他协议的 ACL，则会显示警告消息。
interface_name	指定用户需要从中记账的接口名称。
server_tag	指定 **aaa-server** 命令定义的 AAA 服务器组标记。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 可以将关于通过 ASA 的任何 TCP 或 UDP 流量的记账信息发送给 RADIUS 或 TACACS+ 服务器。如果同时对该流量进行身份验证，则 AAA 服务器可以按用户名维护记账信息。如果未对该流量进行身份验证，则 AAA 服务器可以按 IP 地址维护记账信息。记账信息包括会话的开始和停止时间、用户名、会话时通过 ASA 的字节数、使用的服务以及每个会话的持续时间。

使用此命令前，您必须首先使用 **aaa-server** 命令指定一个 AAA 服务器。

仅将记账信息发送给服务器组中的活动服务器，除非您在 AAA 服务器协议配置模式下使用 **accounting-mode** 命令启用同时记账。

您无法在与 **aaa accounting include** 和 **exclude** 命令相同的配置中使用 **aaa accounting match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

示例

以下示例对与特定 ACL acl2 匹配的流量启用记账：

```
ciscoasa(config)# access-list acl12 extended permit tcp any any
ciscoasa(config)# aaa accounting match acl2 outside radserver1
```

相关命令

命令	说明
aaa accounting include, exclude	通过在命令中直接指定 IP 地址来启用记账。
access-list extended	创建 ACL。
clear configure aaa	删除 AAA 配置。
show running-config aaa	显示 AAA 配置。

aaa authentication console

要对通过串行、SSH、HTTPS (ASDM) 或 Telnet 连接访问 ASA CLI 的用户或使用 **enable** 命令进入特权 EXEC 模式的用户进行身份验证，请在全局配置模式下使用 **aaa authentication console** 命令。要禁用身份验证，请使用此命令的 **no** 形式。

aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console {LOCAL** | *server_group* [**LOCAL**]**}**

语法说明

enable	对使用 **enable** 命令进入特权 EXEC 模式的用户进行身份验证。
http	对通过 HTTPS 访问 ASA 的 ASDM 用户进行身份验证。如果要使用 RADIUS 或 TACACS+ 服务器，则您只需配置 HTTPS 身份验证。默认情况下，ASDM 使用本地数据库进行身份验证，即使您未配置此命令。

LOCAL	使用本地数据库进行身份验证。**LOCAL** 关键字**是**区分大小写的。如果本地数据库为空，则会显示以下警告消息：
	`Warning:local database is empty!Use 'username' command to define local users.`
	如果当 **LOCAL** 关键字仍存在于配置中时本地数据库变为空，则会显示以下警告消息：
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	指定 **aaa-server** 命令定义的 AAA 服务器组标记。HTTPS 管理身份验证不支持用于 AAA 服务器组的 SDI 协议。 如果除 *server-tag* 参数外还使用 **LOCAL** 关键字，则您可以将 ASA 配置为将本地数据库用作回退方法（如果 AAA 服务器不可用）。**LOCAL** 关键字是区分大小写的。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示不会对使用何种方法提供任何指示。
serial	对使用串行控制台端口访问 ASA 的用户进行身份验证。
ssh	对使用 SSH 访问 ASA 的用户进行身份验证。
telnet	对使用 Telnet 访问 ASA 的用户进行身份验证。

默认值

默认情况下，禁止回退至本地数据库。

如果未定义 **aaa authentication telnet console** 命令，则您可以使用 ASA 登录密码（使用 **password** 命令设置）访问 ASA CLI。

如果未定义 **aaa authentication http console** 命令，则您可以不使用用户名和 ASA 启用密码（使用 **enable password** 命令设置）访问 ASA（通过 ASDM）。如果定义 **aaa** 命令，但是 HTTPS 身份验证请求超时（意味着 AAA 服务器可能已关闭或不可用），则您可以使用默认的管理员用户名和启用密码访问 ASA。默认情况下，不设置启用密码。

如果未定义 **aaa authentication ssh console** 命令，则您可以使用用户名 **pix** 和 ASA 启用密码（使用 **enable password** 命令设置）访问 ASA CLI。默认情况下，启用密码为空。此行为与您在不配置 AAA 时登录到 ASA 时的行为不同；在后一种情况下，您使用登录密码（通过 **password** 命令设置）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **telnet** 或 **ssh** 命令配置对 ASA 的访问，ASA 才能对 Telnet 或 SSH 用户进行身份验证。这些命令识别允许与 ASA 通信的 IP 地址。

登录到 ASA

连接到 ASA 后，登录并进入用户 EXEC 模式。

- 如果不对 Telnet 启用任何身份验证，则不用输入用户名，而是输入登录密码（使用 **password** 命令设置）。对于 SSH，输入 “pix” 作为用户名，然后输入登录密码。
- 如果使用此命令对 Telnet 或 SSH 启用身份验证，则输入在 AAA 服务器或本地用户数据库上定义的用户名和密码。

进入特权 EXEC 模式

要进入特权 EXEC 模式，请输入 **enable** 命令或 **login** 命令（如果仅使用本地数据库）。

- 如果不配置启用身份验证，则在输入 **enable** 命令时输入系统启用密码（通过 **enable password** 命令设置）。但是，如果不使用启用身份验证，则在输入 **enable** 命令后，您将不再作为特殊用户登录。要维护您的用户名，请使用启用身份验证。
- 如果配置启用身份验证，则 ASA 会提示您输入用户名和密码。

要使用本地数据库进行身份验证，您可以使用 **login** 命令，它可维护用户名，但不需要任何配置即可启用身份验证。

访问 ASDM

默认情况下，您可以使用空的用户名和 **enable password** 命令设置的启用密码登录到 ASDM。但是，如果您在登录屏幕上输入用户名和密码（而非将用户名留空），则 ASDM 会检查本地数据库以进行匹配。

虽然您可以使用此命令配置 HTTPS 身份验证并指定本地数据库，但默认情况下会始终启用该功能。如果要使用 AAA 服务器进行身份验证，则应仅配置 HTTPS 身份验证。HTTPS 身份验证不支持对 AAA 服务器组使用 SDI 协议。HTTPS 身份验证的最大用户名提示符数是 30 个字符。最大密码长度为 16 个字符。

系统执行空间中不支持 AAA 命令

在多情景模式下，您无法在系统配置中配置任何 AAA 命令。

允许的登录尝试次数

如下表所示，对经过身份验证访问 ASA CLI 的提示的操作有所不同，具体取决于您使用 **aaa authentication console** 命令选择的选项。

选项	允许的登录尝试次数
enable	三次尝试失败后会拒绝访问
serial	可持续尝试，直到成功为止
ssh	三次尝试失败后会拒绝访问
telnet	可持续尝试，直到成功为止
http	可持续尝试，直到成功为止

限制用户 CLI 和 ASDM 访问

您可以使用 **aaa authorization exec** 命令配置管理授权以限制本地用户、RADIUS、TACACS+ 或 LDAP 用户（如果将 LDAP 属性映射到 RADIUS 属性）访问 CLI、ASDM 或 **enable** 命令。

注　管理授权中不包括串行访问，因此，如果配置 **aaa authentication serial console**，则进行身份验证的任何用户都可以访问控制台端口。

要为管理授权配置用户，请了解对每个 AAA 服务器类型或本地用户的以下要求：

- RADIUS 或 LDAP（映射的）用户 - 为以下值之一配置服务类型属性。（要映射 LDAP 属性，请参阅 **ldap attribute-map** 命令。）
  - Service-Type 6（管理）- 允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。
  - Service-Type 7（NAS 提示）- 在配置 **aaa authentication {telnet | ssh} console** 命令时允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令配置**启用**身份验证，则用户无法使用 **enable** 命令进入特权 EXEC 模式。
  - Service-Type 5（出站）- 拒绝管理访问。用户无法使用 **aaa authentication console** 命令指定的任何服务（**serial** 关键字除外；允许串行访问）。远程访问（IPSec 和 SSL）用户仍可对其远程访问会话进行身份验证并终止会话。
- TACACS+ 用户 - 使用 “service=shell” 请求授权，然后服务器以 PASS（通过）或 FAIL（失败）予以响应。
  - PASS，特权级别 1 - 允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。
  - PASS，特权级别 2 及更高 - 在配置 **aaa authentication {telnet | ssh} console** 命令时允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令配置启用身份验证，则用户无法使用 **enable** 命令进入特权 EXEC 模式。
  - FAIL - 拒绝管理访问。用户无法使用 **aaa authentication console** 命令指定的任何服务（**serial** 关键字除外；允许串行访问）。
- 本地用户 - 设置 **service-type** 命令。默认情况下，**service-type** 是 **admin**，它允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。

示例

以下示例展示使用 **aaa authentication console** 命令与带有服务器标记 “radius” 的 RADIUS 服务器进行 Telnet 连接。

```
ciscoasa(config)# aaa authentication telnet console radius
```

以下示例识别用于启用身份验证的服务器组 “AuthIn”：

```
ciscoasa(config)# aaa authentication enable console AuthIn
```

以下示例展示当 “svrgrp1” 组中的所有服务器都失败时，**aaa authentication console** 命令与回退至 LOCAL 用户数据库的结合使用：

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs
ciscoasa(config)# aaa authentication ssh console svrgrp1 LOCAL
```

相关命令

命令	说明
aaa authentication	启用或禁用用户身份验证。
aaa-server host	指定要用于用户身份验证的 AAA 服务器。
clear configure aaa	删除或重置配置的 AAA 记账值。
ldap map-attributes	将 LDAP 属性映射到 ASA 可理解的 RADIUS 属性。
service-type	限制本地用户 CLI 访问。
show running-config aaa	显示 AAA 配置。

aaa authentication include, exclude

要启用对通过 ASA 的连接的身份验证，请在全局配置模式下使用 **aaa authentication include** 命令。要禁用身份验证，请使用此命令的 **no** 形式。要将地址从身份验证中排除，请使用 **aaa authentication exclude** 命令。要不将地址从身份验证中排除，请使用此命令的 **no** 形式。

aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL}**

语法说明

exclude	将指定的服务和地址从身份验证中排除（如果已由 **include** 命令指定）。
include	指定需要身份验证的服务和 IP 地址。不处理未由 **include** 语句指定的流量。
inside_ip	指定较高安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是目标地址。如果将命令应用于较高安全接口，则此地址是源地址。使用 0 表示所有主机。
inside_mask	指定内部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
interface_name	指定用户需要从中进行身份验证的接口名称。
LOCAL	指定本地用户数据库。
outside_ip	（可选）指定较低安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是源地址。如果将命令应用于较高安全接口，则此地址是目标地址。使用 0 表示所有主机。
outside_mask	（可选）指定外部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
server_tag	指定 **aaa-server** 命令定义的 AAA 服务器组。
service	指定需要进行身份验证的服务。您可以指定以下值之一： • **any** 或 **tcp/0**（指定所有 TCP 流量） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] 虽然您可以将 ASA 配置为需要针对对任何协议或服务的网络访问进行身份验证，但用户可以直接使用 HTTP、HTTPS、Telnet 或仅使用 FTP 进行身份验证。用户必须首先使用上述服务之一进行身份验证，ASA 才允许其他需要身份验证的流量。有关详细信息请参阅 “ 使用指南 ”。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要启用对 ACL 指定的流量的身份验证，请使用 **aaa authentication match** 命令。您无法在与 **include** 和 **exclude** 命令相同的配置中使用 **match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

您无法在具有相同安全性的接口之间使用 **aaa authentication include** 和 **exclude** 命令。对于该情况，您必须使用 **aaa authentication match** 命令。

即使您禁用序列随机化，TCP 会话仍可能将其序列号随机排列。当 AAA 服务器代理 TCP 会话以在允许访问前对用户进行身份验证时会发生这种情况。

One-Time 身份验证

给定 IP 地址上的用户仅需对所有规则和类型进行一次身份验证，直到身份验证会话到期为止。（请参阅 **timeout uauth** 命令了解超时值。）例如，如果您将 ASA 配置为对 Telnet 和 FTP 进行身份验证，且用户首先成功对 Telnet 进行身份验证，则只要身份验证会话存在，该用户就不必也对 FTP 进行身份验证。

对于 HTTP 或 HTTPS 身份验证，无论将 **timeout uauth** 命令设置得如何低，经过身份验证后，用户都无需重新进行身份验证，因为浏览器在每个到该特定站点的后续连接中缓存字符串“Basic=Uuhjksdkfhk==”。仅当用户退出 Web 浏览器的*所有*实例并重启时才可清除它。清空缓存是无用的。

接收身份验证质询所需的应用

虽然您可以将 ASA 配置为需要针对对任何协议或服务的网络访问进行身份验证，但用户可以直接使用 HTTP、HTTPS、Telnet 或仅使用 FTP 进行身份验证。用户必须首先使用上述服务之一进行身份验证，ASA 才允许其他需要身份验证的流量。

ASA 支持 AAA 的身份验证端口是固定的：

- 端口 21 用于 FTP
- 端口 23 用于 Telnet
- 端口 80 用于 HTTP
- 端口 443 用于 HTTPS

ASA 身份验证提示

对于 Telnet 和 FTP，ASA 生成身份验证提示。

对于 HTTP，ASA 默认情况下使用基本 HTTP 身份验证，并提供身份验证提示。您可以选择将 ASA 配置为将用户重定向到他们可以输入自己的用户名和密码的内部网页（使用 **aaa authentication listener** 命令配置）。

对于 HTTPS，ASA 生成定制登录屏幕。您可以选择将 ASA 配置为将用户重定向到他们可以输入自己的用户名和密码的内部网页（使用 **aaa authentication listener** 命令配置）。

重定向是在基本方法上进行的改进，因为它提供进行身份验证时的改进用户体验，以及在 Easy VPN 和防火墙模式下对 HTTP 和 HTTPS 的相同用户体验。它还支持直接通过 ASA 进行身份验证。

在下列情况下，您可能希望继续使用基本 HTTP 身份验证：不想 ASA 打开侦听端口；在路由器上使用 NAT，且不想为 ASA 提供的网页创建转换规则；基本 HTTP 身份验证更适用于您的网络。例如，非浏览器应用（例如，当将 URL 嵌入到邮件中时）可能更适合基本身份验证。

正确进行身份验证后，ASA 将您重定向到原始目标。如果目标服务器也有自己的身份验证，则用户输入另一个用户名和密码。如果使用基本 HTTP 身份验证，且需要输入目标服务器的另一个用户名和密码，则需要配置 **virtual http** 命令。

注　如果在不使用 **aaa authentication secure-http-client** 命令时使用 HTTP 身份验证，则以明文形式将用户名和密码从客户端发送到 ASA。我们建议，无论何时启用 HTTP 身份验证，请使用 **aaa authentication secure-http-client** 命令。

对于 FTP，用户可以选择输入 ASA 用户名（符号 (@) 紧随其后），然后输入 FTP 用户名 (name1@name2)。对于密码，用户输入 ASA 密码（符号 (@) 紧随其后），然后输入 FTP 密码 (password1@password2)。例如，输入以下文本。

```
name> asa1@partreq
password> letmein@he110
```

此功能在您具有需要多次登录的级联防火墙时有用。您可以通过多个符号 (@) 隔开几个名称和密码。

允许的登录尝试次数因支持的协议不同而存在差异：

协议	允许的登录尝试次数
FTP	不正确的密码立即导致连接丢弃。
HTTP HTTPS	连续重新提示，直到成功登录为止。
Telnet	四次尝试失败后丢弃连接。

静态 PAT 和 HTTP

对于 HTTP 身份验证，ASA 在配置静态 PAT 时检查实际端口。如果它检测到以实际端口 80 为目标的流量，则不论映射的端口如何，ASA 都会拦截 HTTP 连接并实施身份验证。

例如，假设将外部 TCP 端口 889 转换为端口 80 (www) 且任何相关的 ACL 均允许流量：

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

当用户尝试访问端口 889 上的 10.48.66.155 时，ASA 拦截流量并实施 HTTP 身份验证。在 ASA 允许 HTTP 连接完成前，用户会在其 Web 浏览器中看到 HTTP 身份验证页面。

如果本地端口与端口 80 不同，如以下示例中所示：

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

用户将无法看到身份验证页面。相反，ASA 将一条错误消息发送给 Web 浏览器，指示在使用请求的服务前必须对用户进行身份验证。

直接通过 ASA 进行身份验证

如果不想允许 HTTP、HTTPS、Telnet 或 FTP 通过 ASA，但要对其他类型的流量进行身份验证，则您可以通过配置 **aaa authentication listener** 命令来使用 HTTP 或 HTTPS 直接通过 ASA 进行身份验证。

当为接口启用 AAA 时，您可以直接通过位于以下 URL 的 ASA 进行身份验证：

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

或者，您可以配置虚拟 Telnet（使用 **virtual telnet** 命令）。使用虚拟 Telnet，用户远程登录到一个在 ASA 上配置的给定 IP 地址，且 ASA 提供 Telnet 提示。

示例

以下示例在外部接口上包括身份验证 TCP 流量，其中包含内部 IP 地址 192.168.0.0、网络掩码 255.255.0.0 和所有主机的外部 IP 地址，且使用名为 TACACS+ 的服务器组。第二个命令行在外部接口上排除 Telnet 流量，其中包括内部地址 192.168.38.0 和所有主机的外部 IP 地址：

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
ciscoasa(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

以下示例展示使用 *interface-name* 参数的方式。ASA 具有内部网络 192.168.1.0、外部网络 209.165.201.0（子网掩码 255.255.255.224）和外围网络 209.165.202.128（子网掩码 255.255.255.224）。

此示例启用对从内部网络向外部网络发起的连接的身份验证：

```
ciscoasa(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

此示例启用对从内部网络向外围网络发起的连接的身份验证：

```
ciscoasa(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

此示例启用对从外部网络向内部网络发起的连接的身份验证：

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

此示例启用对从外部网络向外围网络发起的连接的身份验证：

```
ciscoasa(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

此示例启用对从外围网络向外部网络发起的连接的身份验证：

```
ciscoasa(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

相关命令

命令	说明
aaa authentication console	为管理访问启用身份验证。
aaa authentication match	为通过流量启用用户身份验证。
aaa authentication secure-http-client	提供在允许 HTTP 请求穿越 ASA 前向 ASA 进行用户身份验证的安全方法。
aaa-server	配置与组相关的服务器属性。
aaa-server host	配置与主机相关的属性。

aaa authentication listener

要启用 HTTP(S) 侦听端口以对网络用户进行身份验证，请在全局配置模式下使用 **aaa authentication listener** 命令。在启用侦听端口时，ASA 提供用于直接连接和通过流量（可选）的身份验证页面。要禁用侦听程序，请使用此命令的 **no** 形式。

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

语法说明

http[**s**]	指定要侦听的协议，即 HTTP 或 HTTPS。分别为每个协议输入此命令。
interface_name	指定要启用侦听程序的接口。
port *portnum*	指定 ASA 用于对定向或重定向的流量进行侦听的端口号；默认端口为 80 (HTTP) 和 443 (HTTPS)。您可以使用任何端口号并保留相同的功能，但是请确保您的直接身份验证用户知道该端口号；重定向的流量会自动发送到正确的端口号，但是直接验证器必须手动指定端口号。
redirect	将通过流量重定向到 ASA 提供的身份验证网页。若没有此关键字，则仅流向 ASA 接口的流量可以访问身份验证网页。

默认值

默认情况下，未启用任何侦听程序服务，且 HTTP 连接使用基本 HTTP 身份验证。如果启用侦听程序，则默认端口为 80 (HTTP) 和 443 (HTTPS)。

如果从 7.2(1) 升级，则在端口 1080 (HTTP) 和 1443 (HTTPS) 上启用侦听程序。同时启用 **redirect** 选项。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(2)	引入了此命令。

使用指南

在没有 **aaa authentication listener** 命令的情况下，当 HTTP(S) 用户需要在配置 **aaa authentication match** 或 **aaa authentication include** 命令后通过 ASA 进行身份验证时，ASA 使用基本 HTTP 身份验证。对于 HTTPS，ASA 生成定制登录屏幕。

如果您使用 **redirect** 关键字配置 **aaa authentication listener** 命令，则 ASA 将所有 HTTP(S) 身份验证请求重定向到 ASA 提供的网页。

重定向是在基本方法上进行的改进，因为它提供进行身份验证时的改进用户体验，以及在 Easy VPN 和防火墙模式下对 HTTP 和 HTTPS 的相同用户体验。它还支持直接通过 ASA 进行身份验证。

在下列情况下，您可能希望继续使用基本 HTTP 身份验证：不想 ASA 打开侦听端口；在路由器上使用 NAT，且不想为 ASA 提供的网页创建转换规则；基本 HTTP 身份验证更适用于您的网络。例如，非浏览器应用（例如，当将 URL 嵌入到邮件中时）可能更适合基本身份验证。

如果输入*不带* **redirect** 选项的 **aaa authentication listener** 命令，则仅启用通过 ASA 的直接身份验证，同时允许通过流量使用基本 HTTP 身份验证。**redirect** 选项同时启用直接身份验证和通过流量身份验证。当要对不支持身份验证质询的流量类型进行身份验证时，直接身份验证是有用的；您可以在使用任何其他服务前直接通过 ASA 对每个用户进行身份验证。

注　如果启用 **redirect** 选项，则您无法也为用于转换接口 IP 地址的同一接口和用于侦听程序的同一端口配置静态 PAT； NAT 会成功，但身份验证会失败。例如，不支持以下配置：

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside redirect
```

支持以下配置；侦听程序使用端口 1080 而非默认端口 80：

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside port 1080 redirect
```

示例

以下示例将 ASA 配置为将 HTTP 和 HTTPS 连接重定向到默认端口：

```
ciscoasa(config)# aaa authentication http redirect
ciscoasa(config)# aaa authentication https redirect
```

以下示例允许身份验证请求直接到达 ASA；通过流量使用基本 HTTP 身份验证：

```
ciscoasa(config)# aaa authentication http
ciscoasa(config)# aaa authentication https
```

以下示例将 ASA 配置为将 HTTP 和 HTTPS 连接重定向到非默认端口：

```
ciscoasa(config)# aaa authentication http port 1100 redirect
ciscoasa(config)# aaa authentication https port 1400 redirect
```

相关命令

命令	说明
aaa authentication match	为通过流量配置用户身份验证。
aaa authentication secure-http-client	启用 SSL 并保护 HTTP 客户端与 ASA 之间用户名和密码交换的安全。
clear configure aaa	删除配置的 AAA 配置。
show running-config aaa	显示 AAA 配置。
virtual http	支持带有基本 HTTP 身份验证的级联 HTTP 身份验证。

aaa authentication match

要启用对通过 ASA 的连接的身份验证，请在全局配置模式下使用 **aaa authentication match** 命令。要禁用身份验证，请使用此命令的 **no** 形式。

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

语法说明

acl_name	指定扩展的 ACL 名称。
interface_name	指定从中对用户进行身份验证的接口名称。
LOCAL	指定本地用户数据库。
server_tag	指定 **aaa-server** 命令定义的 AAA 服务器组标记。
user-identity	指定映射到身份防火墙的用户身份。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	添加了 **user-identity** 关键字。

使用指南

您无法在与 **include** 和 **exclude** 命令相同的配置中使用 **aaa authentication match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

即使您禁用序列随机化，TCP 会话仍可能将其序列号随机排列。当 AAA 服务器代理 TCP 会话以在允许访问前对用户进行身份验证时会发生这种情况。

One-Time 身份验证

给定 IP 地址上的用户仅需对所有规则和类型进行一次身份验证，直到身份验证会话到期为止。（请参阅 **timeout uauth** 命令了解超时值。）例如，如果您将 ASA 配置为对 Telnet 和 FTP 进行身份验证，且用户首先成功对 Telnet 进行身份验证，则只要身份验证会话存在，该用户就不必也对 FTP 进行身份验证。

对于 HTTP 或 HTTPS 身份验证，无论将 **timeout uauth** 命令设置得如何低，经过身份验证后，用户都无需重新进行身份验证，因为浏览器在每个到该特定站点的后续连接中缓存字符串“Basic=Uuhjksdkfhk==”。仅当用户退出 Web 浏览器的*所有*实例并重启时才可清除它。清空缓存是无用的。

接收身份验证质询所需的应用

虽然您可以将 ASA 配置为需要针对对任何协议或服务的网络访问进行身份验证，但用户可以直接使用 HTTP、HTTPS、Telnet 或仅使用 FTP 进行身份验证。用户必须首先使用上述服务之一进行身份验证，ASA 才允许其他需要身份验证的流量。

ASA 支持 AAA 的身份验证端口是固定的：

- 端口 21 用于 FTP
- 端口 23 用于 Telnet
- 端口 80 用于 HTTP
- 端口 443 用于 HTTPS（需要 **aaa authentication listener** 命令）

ASA 身份验证提示

对于 Telnet 和 FTP，ASA 生成身份验证提示。

对于 HTTP，ASA 默认情况下使用基本 HTTP 身份验证，并提供身份验证提示。您可以选择将 ASA 配置为将用户重定向到他们可以输入自己的用户名和密码的内部网页（使用 **aaa authentication listener** 命令配置）。

对于 HTTPS，ASA 生成定制登录屏幕。您可以选择将 ASA 配置为将用户重定向到他们可以输入自己的用户名和密码的内部网页（使用 **aaa authentication listener** 命令配置）。

重定向是在基本方法上进行的改进，因为它提供进行身份验证时的改进用户体验，以及在 Easy VPN 和防火墙模式下对 HTTP 和 HTTPS 的相同用户体验。它还支持直接通过 ASA 进行身份验证。

在下列情况下，您可能希望继续使用基本 HTTP 身份验证：不想 ASA 打开侦听端口；在路由器上使用 NAT，且不想为 ASA 提供的网页创建转换规则；基本 HTTP 身份验证更适用于您的网络。例如，非浏览器应用（例如，当将 URL 嵌入到邮件中时）可能更适合基本身份验证。

正确进行身份验证后，ASA 将您重定向到原始目标。如果目标服务器也有自己的身份验证，则用户输入另一个用户名和密码。如果使用基本 HTTP 身份验证，且需要输入目标服务器的另一个用户名和密码，则需要配置 **virtual http** 命令。

注　如果在不使用 **aaa authentication secure-http-client** 命令时使用 HTTP 身份验证，则以明文形式将用户名和密码从客户端发送到 ASA。我们建议，无论何时启用 HTTP 身份验证，请使用 **aaa authentication secure-http-client** 命令。

对于 FTP，用户可以选择输入 ASA 用户名（符号 (@) 紧随其后），然后输入 FTP 用户名 (name1@name2)。对于密码，用户输入 ASA 密码（符号 (@) 紧随其后），然后输入 FTP 密码 (password1@password2)。例如，输入以下文本。

```
name> asa1@partreq
password> letmein@he110
```

此功能在您具有需要多次登录的级联防火墙时有用。您可以通过多个符号 (@) 隔开几个名称和密码。

允许的登录尝试次数因支持的协议不同而存在差异：

协议	允许的登录尝试次数
FTP	不正确的密码立即导致连接丢弃。
HTTP HTTPS	连续重新提示，直到成功登录为止。
Telnet	四次尝试失败后丢弃连接。

静态 PAT 和 HTTP

对于 HTTP 身份验证，ASA 在配置静态 PAT 时检查实际端口。如果它检测到以实际端口 80 为目标的流量，则不论映射的端口如何，ASA 都会拦截 HTTP 连接并实施身份验证。

例如，假设将外部 TCP 端口 889 转换为端口 80 (www) 且任何相关的 ACL 均允许流量：

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

当用户尝试访问端口 889 上的 10.48.66.155 时，ASA 拦截流量并实施 HTTP 身份验证。在 ASA 允许 HTTP 连接完成前，用户会在其 Web 浏览器中看到 HTTP 身份验证页面。

如果本地端口与端口 80 不同，如以下示例中所示：

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

用户将无法看到身份验证页面。相反，ASA 将一条错误消息发送给 Web 浏览器，指示必须在使用请求的服务前对用户进行身份验证。

直接通过 ASA 进行身份验证

如果不想允许 HTTP、HTTPS、Telnet 或 FTP 通过 ASA，但要对其他类型的流量进行身份验证，则您可以通过配置 **aaa authentication listener** 命令来使用 HTTP 或 HTTPS 直接通过 ASA 进行身份验证。

当为接口启用 AAA 时，您可以直接通过位于以下 URL 的 ASA 进行身份验证：

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

或者，您可以配置虚拟 Telnet（使用 **virtual telnet** 命令）。使用虚拟 Telnet，用户远程登录到一个在 ASA 上配置的给定 IP 地址，且 ASA 提供 Telnet 提示。

示例

以下一组示例说明如何使用 **aaa authentication match** 命令：

```
ciscoasa(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

ciscoasa(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

在此情景下，以下命令：

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

相当于此命令：

```
ciscoasa(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa 命令语句列表根据 **access-list** 命令语句之间的顺序排列。如果您先输入以下命令：

```
ciscoasa(config)# aaa authentication match mylist outbound TACACS+
```

再输入此命令：

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

ASA 会在尝试在 **yourlist access-list** 命令语句组中寻找匹配项前，尝试在 **mylist access-list** 命令语句组中找到一个匹配项。

要启用对通过 ASA 的连接的身份验证并将其与身份防火墙功能匹配，请输入以下命令：

```
ciscoasa(config)# aaa authenticate match access_list_name inside user-identity
```

相关命令

命令	说明
aaa authorization	启用用户授权服务。
access-list extended	创建 ACL。
clear configure aaa	删除配置的 AAA 配置。
show running-config aaa	显示 AAA 配置。

aaa authentication secure-http-client

要启用 SSL 并保护 HTTP 客户端与 ASA 之间用户名和密码交换的安全，请在全局配置模式下使用 **aaa authentication secure-http-client** 命令。要禁用此功能，请使用此命令的 **no** 形式。

aaa authentication secure-http-client

no aaa authentication secure-http-client

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

aaa authentication secure-http-client 命令提供在允许基于用户 HTTP 的 Web 请求穿越 ASA 前向 ASA 进行用户身份验证的安全方法。此命令用于通过 SSL 的 HTTP 直接转发代理身份验证。

aaa authentication secure-http-client 命令有以下限制：

- 在运行时，最多允许 16 个 HTTPS 身份验证进程。如果所有 16 个 HTTPS 身份验证进程都在运行，则不允许需要身份验证的第 17 个新的 HTTPS 连接。
- 当配置 **uauth timeout 0** 时（将 **uauth timeout** 设置为 0），HTTPS 身份验证可能无法工作。如果浏览器在 HTTPS 身份验证后发起多个 TCP 连接以加载网页，则允许第一个连接通过，但是后续连接会触发身份验证。因此，会不断向用户显示身份验证页面，即使每次都输入正确的用户名和密码。要解决此问题，请使用 **timeout uauth 0:0:1** 命令将 **uauth timeout** 设置为 1 秒。但是，此解决方法会打开一个 1 秒的机会窗口，它可允许未经身份验证的用户通过防火墙（如果他们来自同一源 IP 地址）。
- 由于 HTTPS 身份验证在 SSL 端口 443 上进行，用户不得配置 **access-list** 命令语句来拦截从 HTTP 客户端到端口 443 上的 HTTP 服务器的流量。此外，如果在端口 80 上为网络流量配置静态 PAT，则也必须为 SSL 端口配置静态 PAT。在以下示例中，第一行为网络流量配置静态 PAT，且必须添加第二行以支持 HTTPS 身份验证配置：

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

示例

以下示例配置要对其安全地进行身份验证的 HTTP 流量：

```
ciscoasa(config)# aaa authentication secure-http-client
ciscoasa(config)# aaa authentication include http...
```

其中 “...” 代表您的 *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag* 的值。

以下命令配置要对其安全地进行身份验证的 HTTPS 流量：

```
ciscoasa (config)# aaa authentication include https...
```

其中 “...” 代表您的 *authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* 的值。

注　HTTPS 流量不需要 **aaa authentication secure-https-client** 命令。

相关命令

命令	说明
aaa authentication	启用 LOCAL、TACACS+ 或 RADIUS 用户身份验证（在 **aaa-server** 命令指定的服务器上）。
virtual telnet	访问 ASA 虚拟服务器。

aaa authorization command

要启用命令授权，请在全局配置模式下使用 **aaa authorization command** 命令。要禁用命令授权，请使用此命令的 **no** 形式。

aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

no aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

语法说明

LOCAL	启用 **privilege** 命令设置的本地命令特权级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户对 CLI 访问进行身份验证时，ASA 将该用户置于本地数据库、RADIUS 或 LDAP 服务器定义的特权级别中。用户可以访问用户特权级别及该级别以下的命令。 如果您在 TACACS+ 服务器组标记后指定 **LOCAL**，则当 TACACS+ 服务器组不可用时仅将本地用户数据库作为回退用于命令授权。
tacacs+ server_tag	为 TACACS+ 授权服务器指定预定义的服务器组标记。AAA 服务器组标记如 **aaa-server** 命令所定义。

默认值

默认情况下禁用回退至本地数据库用以授权。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	增加了当 TACACS+ 服务器组暂时不可用时对回退至 LOCAL 授权的支持。
8.0(2)	增加了对在 RADIUS 或 LDAP 服务器上定义的特权级别的支持。

使用指南

aaa authorization command 命令指定是否在 CLI 上执行命令有待授权。默认情况下，您在登录时可以进入用户 EXEC 模式，该模式仅提供极少数量的命令。当输入 **enable** 命令时（或当使用本地数据库时输入 **login** 命令），您可以进入特权 EXEC 模式并访问高级命令（包括配置命令）。如果要控制对命令的访问，ASA 允许您配置命令授权，其中您可以确定哪些命令可供用户使用。

支持的命令授权方法

您可以使用两个命令授权方法之一：

- 本地特权级别 - 在 ASA 上配置命令特权级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户对 CLI 访问进行身份验证时，ASA 将该用户置于本地数据库、RADIUS 或 LDAP 服务器定义的特权级别中。用户可以访问用户特权级别及该级别以下的命令。请注意，所有用户首次登录时（命令级别为 0 或 1）都进入用户 EXEC 模式。用户需要使用 **enable** 命令再次进行身份验证才能进入特权 EXEC 模式（命令级别为 2 或更高），或使用 **login** 命令登录（仅限本地数据库）。

注　您可以使用本地命令授权，其中本地数据库中没有任何用户，也不具有 CLI 或启用身份验证。相反，输入 **enable** 命令时，输入系统启用密码，然后 ASA 将您置于级别 15。您可以为每个级别创建启用密码，以便当您输入 **enable** *n*（2 到 15）时，ASA 将您置于级别 *n*。不使用这些级别，除非您启用本地命令授权。（请参阅 **enable** 命令了解更多信息。）

- TACACS+ 服务器特权级别 - 在 TACACS+ 服务器上，配置用户或组可以在其对 CLI 访问进行身份验证后使用的命令。使用 TACACS+ 服务器检查用户在 CLI 上输入的每个命令。

安全情景和命令授权

以下是在使用多个安全情景实施命令授权时要考虑的重点：

- 每个情景中的 AAA 设置都是离散的，不在情景之间共享。

  配置命令授权时，您必须分别配置每个安全情景。这样您可以为不同安全情景实施不同命令授权。

  当在安全情景之间切换时，管理员应知道登录时指定的用户名允许的命令在新情景会话中可能不同，或在新情景中可能根本未配置该命令授权。若不了解命令授权在安全情景之间可能不同，管理员会感到困扰。下一点会让此行为更为复杂。

- 无论在上次情景会话中使用什么用户名，以 **changeto** 命令开始的新情景会话都始终将默认的用户名 “enable_15” 用作管理员身份。如果没有为 enable_15 用户配置命令授权，或对 enable_15 用户的授权不同于对上次情景会话中的用户的授权，则此行为可导致混乱。

  此行为也影响命令记账，命令记账仅在可以准确将每个发出的命令与特定管理员关联时才有用。由于具有使用 **changeto** 命令的权限的所有管理员都可以在其他情景中使用 enable_15 用户名，因此命令记账记录可能不易将登录的用户识别为 enable_15 用户名。如果您为每个情景使用不同的记账服务器，则跟踪使用 enable_15 用户名的用户需要关联多个服务器的数据。

  在配置命令授权时，请考虑以下方面：

  - 若管理员具有有效使用 **changeto** 命令的权限，则该管理员有权限在其他每个情景中使用对 enable_15 用户允许的所有命令。
  - 如果打算根据每个情景进行不同的命令授权，请确保在每个情景中使用对允许使用 **changeto** 命令的管理员拒绝的命令拒绝 enable_15 用户名。

  当在安全情景之间切换时，管理员可以退出特权 EXEC 模式，然后再次输入 **enable** 命令以使用所需的用户名。

注　系统执行空间不支持 **aaa** 命令；因此，命令授权在系统执行空间中不可用。

本地命令授权前提条件

- 使用 **aaa authentication enable console** 命令为本地、RADIUS 或 LDAP 身份验证配置启用身份验证。

  启用身份验证对于在用户访问 **enable** 命令后维护用户名十分重要。

  或者，您可以使用 **login** 命令（与具有身份验证的 **enable** 命令相同），该命令不需要配置。我们不建议使用此选项，因为它不像启用身份验证那样安全。

  您也可以使用 CLI 身份验证 (**aaa authentication** {**ssh | telnet | serial**} **console**)，但是这不是必需的。

- 如果将 RADIUS 用于身份验证，则您可以使用 **aaa authorization exec** 命令从 RADIUS 中启用管理用户特权级别的支持（但是这不是必需的）。此命令也启用对本地、RADIUS、LDAP（映射的）和 TACACS+ 用户的管理授权。
- 请参阅以下每个用户类型的前提条件：
  - 本地数据库用户 - 使用 **username** 命令将本地数据库中的每个用户配置为从 0 到 15 的特权级别。
  - RADIUS 用户 - 使用 0 和 15 之间的值配置具有 Cisco VSA CVPN3000-Privilege-Level 的用户。
  - LDAP 用户 - 配置具有 0 和 15 之间的特权级别的用户，然后使用 **ldap map-attributes** 命令将 LDAP 属性映射到 Cisco VAS CVPN3000-Privilege-Level。
- 请参阅 **privilege** 命令，了解有关设置命令特权级别的信息。

TACACS+ 命令授权

如果启用 TACACS+ 命令授权，且用户在 CLI 上输入命令，则 ASA 将命令和用户名发送到 TACACS+ 服务器以确定命令是否已授权。

在使用 TACACS+ 服务器配置命令授权时，请勿保存配置，直到您确定其按照您期望的方式运行为止。如果您因错误被锁定，通常可以通过重启 ASA 来恢复访问。

请确保您的 TACACS+ 系统完全稳定且可靠。必要的可靠性级别通常需要您具有完全冗余的 TACACS+ 服务器系统和完全冗余的与 ASA 的连接性。例如，在您的 TACACS+ 服务器池中包括一个与接口 1 连接的服务器和另一个与接口 2 连接的服务器。如果 TACACS+ 服务器不可用，则您也可以将本地命令授权配置为回退方法。在这种情况下，您需要配置本地用户和命令特权级别。

请参阅 CLI 配置指南，了解有关配置 TACACS+ 服务器的信息。

TACACS+ 命令授权前提条件

- 使用 **aaa authentication** {**ssh | telnet | serial**} **console** 命令配置 CLI 身份验证。
- 使用 **aaa authentication enable console** 命令配置 **enable** 身份验证。

示例

以下示例展示如何使用名为 tplus1 的 TACACS+ 服务器组启用命令授权：

```
ciscoasa(config)# aaa authorization command tplus1
```

以下示例展示在 tplus1 服务器组中的所有服务器不可用时如何配置管理授权以支持回退至本地用户数据库。

```
ciscoasa(config)# aaa authorization command tplus1 LOCAL
```

相关命令

命令	说明
aaa authentication console	启用 CLI、ASDM 和启用身份验证。
aaa authorization exec	从 RADIUS 中启用管理用户特权级别的支持。
aaa-server host	配置与主机相关的属性。
aaa-server	配置与组相关的服务器属性。
enable	进入特权 EXEC 模式。
ldap map-attributes	将 LDAP 属性映射到 ASA 可使用的 RADIUS 属性。
login	使用用于身份验证的本地数据库进入特权 EXEC 模式。
service-type	限制本地数据库用户 CLI、ASDM 和启用访问。
show running-config aaa	显示 AAA 配置。

aaa authorization exec

要启用管理授权，请在全局配置模式下使用 **aaa authorization exec** 命令。要禁用管理授权，请使用这些命令的 **no** 形式。

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

no aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

语法说明

authentication-server	指示将从用于对用户进行身份验证的服务器中检索授权属性。
auto-enable	使具有足够授权特权的管理员能够通过输入一次自己的身份验证凭证进入特权 EXEC 模式。
LOCAL	指示将从 ASA 的本地用户数据库中检索授权属性，无论身份验证如何完成。

默认值

默认情况下，此命令已禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
8.2(2)	添加了 **LOCAL** 选项。
9.2(1)	添加了 **auto-enable** 选项。

使用指南

使用 **aaa authorization exec** 命令时，检查用户的服务类型凭证后才允许控制台访问。

使用 **no aaa authorization exec** 命令禁用管理授权时，请注意以下方面：

- 检查用户的服务类型凭证后才允许控制台访问。
- 如果配置了命令授权，且在 RADIUS、LDAP 和 TACACS+ 用户的 AAA 服务器上找到特权级别属性，则仍然应用这些属性。

如果在访问 CLI、ASDM 或 **enable** 命令时配置 **aaa authentication console** 命令以对用户进行身份验证，则 **aaa authorization exec** 命令可以根据用户配置限制管理访问。

注　管理授权中不包括串行访问，因此，如果配置 **aaa authentication serial console**，则进行身份验证的任何用户都可以访问控制台端口。

要为管理授权配置用户，请了解对每个 AAA 服务器类型或本地用户的以下要求：

- LDAP 映射的用户 - 要映射 LDAP 属性，请参阅 **ldap attribute-map** 命令。
- RADIUS 用户 - 使用 IETF RADIUS 数字 **service-type** 属性，该属性映射到以下值之一：
  - Service-Type 5（出站）拒绝管理访问。用户无法使用 **aaa authentication console** 命令指定的任何服务（**serial** 关键字除外；允许串行访问）。远程访问（IPsec 和 SSL）用户仍可对其远程访问会话进行身份验证并终止会话。
  - Service-Type 6（管理）允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。
  - 在配置 **aaa authentication {telnet | ssh} console** 命令时，Service-Type 7（NAS 提示）允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令配置**启用**身份验证，则用户无法使用 **enable** 命令进入特权 EXEC 模式。

注　仅识别 Login (1)、Framed (2)、Administrative (6) 和 NAS-Prompt (7) 服务类型。使用任何其他服务类型会导致访问被拒绝。

- TACACS+ 用户 - 使用 “service=shell” 条目请求授权，然后服务器以 PASS（通过）或 FAIL（失败）予以响应，如下所示：
  - PASS，特权级别 1 允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。
  - PASS，在配置 **aaa authentication {telnet | ssh} console** 命令时特权级别 2 及更高允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令配置启用身份验证，则用户无法使用 **enable** 命令进入特权 EXEC 模式。
  - FAIL（失败）拒绝管理访问。用户无法使用 **aaa authentication console** 命令指定的任何服务（**serial** 关键字除外；允许串行访问）。
- 本地用户 - 设置 **service-type** 命令，它在 **username** 命令的用户名配置模式下。默认情况下，**service-type** 是 **admin**，它允许对 **aaa authentication console** 命令指定的任何服务进行完全访问。

示例

以下示例使用本地数据库启用管理授权：

```
ciscoasa(config)# aaa authorization exec LOCAL
```

相关命令

命令	说明
aaa authentication console	启用控制台身份验证。
ldap attribute-map	映射 LDAP 属性。
service-type	限制本地用户的 CLI 访问。
show running-config aaa	显示 AAA 配置。

aaa authorization include, exclude

要启用对通过 ASA 的连接的授权，请在全局配置模式下使用 **aaa authorization include** 命令。要禁用授权，请使用此命令的 **no** 形式。要将地址从授权中排除，请使用 **aaa authorization exclude** 命令。要不将地址从授权中排除，请使用此命令的 **no** 形式。

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

语法说明

exclude	将指定的服务和地址从授权中排除（如果已由 **include** 命令指定）。
include	指定需要授权的服务和 IP 地址。不处理未由 **include** 语句指定的流量。
inside_ip	指定较高安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是目标地址。如果将命令应用于较高安全接口，则此地址是源地址。使用 0 表示所有主机。
inside_mask	指定内部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
interface_name	指定用户需要从中授权的接口名称。
outside_ip	（可选）指定较低安全接口上的 IP 地址。此地址可以是源地址或目标地址，具体取决于要应用此命令的接口。如果将命令应用于较低安全接口，则此地址是源地址。如果将命令应用于较高安全接口，则此地址是目标地址。使用 0 表示所有主机。
outside_mask	（可选）指定外部 IP 地址的网络掩码。如果 IP 地址是 0，请使用 0。对一个主机使用 255.255.255.255。
server_tag	指定 **aaa-server** 命令定义的 AAA 服务器组。
service	指定需要授权的服务。您可以指定以下值之一： • **any** 或 **tcp/0**（指定所有 TCP 流量） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] **注**　指定端口范围可能在授权服务器上生成意外结果。ASA 将端口范围作为字符串发送到服务器，期望服务器将其解析成特定端口。并非所有服务器都执行此操作。此外，您可能想就特定服务对用户进行授权，如果接受范围，则这种情况不会发生。

默认值

IP 地址为 **0** 表示 “all hosts（所有主机）”。将本地 IP 地址设置为 **0** 将允许授权服务器决定对哪些主机进行授权。

默认情况下禁用回退至本地数据库用以授权。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	**exclude** 参数允许用户指定将某端口排除在某个或某些特定主机之外。

使用指南

要为 ACL 指定的流量启用授权，请使用 **aaa authorization match** 命令。您无法在与 **include** 和 **exclude** 命令相同的配置中使用 **match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

您无法在具有相同安全性的接口之间使用 **aaa authorization include** 和 **exclude** 命令。对于该情况，您必须使用 **aaa authorization match** 命令。

您可以使用 TACACS+ 配置 ASA 以执行网络访问授权。身份验证和授权语句无关；但是，会拒绝与授权语句匹配的任何未经身份验证的流量。要使授权成功，用户必须首先通过 ASA 进行身份验证。由于位于给定 IP 地址的用户仅需对所有规则和类型进行一次身份验证，如果身份验证会话未到期，则会发生授权，即使该流量与身份验证语句匹配。

用户进行身份验证后，ASA 检查用于匹配流量的授权规则。如果流量与授权语句匹配，则 ASA 将用户名发送到 TACACS+ 服务器。TACACS+ 服务器根据用户简档以允许或拒绝该流量来对 ASA 予以响应。ASA 在响应中实施授权规则。

请参阅您的 TACACS+ 服务器的文档，了解有关为用户配置网络访问授权的信息。

对于每个 IP 地址，允许一个 **aaa authorization include** 命令。

如果首次尝试授权失败，且第二次尝试导致超时，请使用 **service resetinbound** 命令重置授权失败的客户端，以便其不会重新传输任何连接。在 Telnet 中的示例授权超时消息如下。

```
Unable to connect to remote host: Connection timed out
```

注　指定端口范围可能在授权服务器上生成意外结果。ASA 将端口范围作为字符串发送到服务器，期望服务器将其解析成特定端口。并非所有服务器都执行此操作。此外，您可能想就特定服务对用户进行授权，如果接受范围，则这种情况不会发生。

示例

以下示例使用 TACACS+ 协议：

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
```

```
ciscoasa(config)# aaa authorization include any inside 0 0 0 0
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authentication ssh console tplus1
```

在此示例中，第一条命令语句创建名为 tplus1 的服务器组并指定与此组结合使用 TACACS+ 协议。第二条命令指定具有 IP 地址 10.1.1.10 的身份验证服务器驻留在内部接口上且在 tplus1 服务器组中。接下来的三条命令语句指定会使用 tplus1 服务器组对通过外部接口启动到任何外部主机的连接的任何用户进行身份验证，授权成功通过身份验证的用户使用任何服务，以及会将所有出站连接信息记录在记账数据库中。最后一条命令语句指定对 ASA 控制台的 SSH 访问需要从 tplus1 服务器组的身份验证。

以下示例启用对从外部接口的 DNS 查找的授权：

```
ciscoasa(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

以下示例启用从内部主机到达内部接口的 ICMP 回显数据包的授权：

```
ciscoasa(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

这意味着，如果用户未使用 Telnet、HTTP 或 FTP 对外部主机进行身份验证，则无法对这些主机进行 ping 操作。

以下示例仅对从内部主机到达内部接口的 ICMP 回显 (ping) 启用授权：

```
ciscoasa(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

相关命令

命令	说明
aaa authorization command	指定是否执行命令有待授权，或如果指定服务器组中的所有服务器均已禁用，则将管理授权配置为支持回退至本地用户数据库。
aaa authorization match	为特定访问列表命令名称启用或禁用 LOCAL 或 TACACS+ 用户授权服务。
clear configure aaa	删除或重置配置的 AAA 记账值。
show running-config aaa	显示 AAA 配置。

aaa authorization match

要启用对通过 ASA 的连接的授权，请在全局配置模式下使用 **aaa authorization match** 命令。要禁用授权，请使用此命令的 **no** 形式。

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

语法说明

acl_name	指定扩展的 ACL 名称。请参阅 **access-list extended** 命令。**permit** ACE 将匹配的流量标记为要进行授权，而 **deny** 条目将匹配的流量从授权中排除。
interface_name	指定用户需要从中进行身份验证的接口名称。
server_tag	指定 **aaa-server** 命令定义的 AAA 服务器组标记。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您无法在与 **include** 和 **exclude** 命令相同的配置中使用 **aaa authorization match** 命令。我们建议您使用 **match** 命令而非 **include** 和 **exclude** 命令； ASDM 不支持 **include** 和 **exclude** 命令。

您可以使用 TACACS+ 配置 ASA 以执行网络访问授权。使用 **aaa authorization match** 命令的 RADIUS 授权仅支持到 ASA 的 VPN 管理连接。

身份验证和授权语句无关；但是，会拒绝与授权语句匹配的任何未经身份验证的流量。要使授权成功，用户必须首先通过 ASA 进行身份验证。由于位于给定 IP 地址的用户仅需对所有规则和类型进行一次身份验证，如果身份验证会话未到期，则会发生授权，即使该流量与身份验证语句匹配。

用户进行身份验证后，ASA 检查用于匹配流量的授权规则。如果流量与授权语句匹配，则 ASA 将用户名发送到 TACACS+ 服务器。TACACS+ 服务器根据用户简档以允许或拒绝该流量来对 ASA 予以响应。ASA 在响应中实施授权规则。

请参阅您的 TACACS+ 服务器的文档，了解有关为用户配置网络访问授权的信息。

如果首次尝试授权失败，且第二次尝试导致超时，请使用 **service resetinbound** 命令重置授权失败的客户端，以便其不会重新传输任何连接。在 Telnet 中的示例授权超时消息如下。

```
Unable to connect to remote host: Connection timed out
```

注　指定端口范围可能在授权服务器上生成意外结果。ASA 将端口范围作为字符串发送到服务器，期望服务器将其解析成特定端口。并非所有服务器都执行此操作。此外，您可能想就特定服务对用户进行授权，如果接受范围，则这种情况不会发生。

示例

以下示例将 tplus1 服务器组与 **aaa** 命令结合使用：

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization match myacl inside tplus1
```

在此示例中，第一条命令语句将 tplus1 服务器组定义为 TACACS+ 组。第二条命令指定具有 IP 地址 10.1.1.10 的身份验证服务器驻留在内部接口上且在 tplus1 服务器组中。接下来的两条命令语句指定使用 tplus1 服务器组对穿越内部接口到任何外部主机的任何连接进行身份验证，并将所有这些连接记录在记账数据库中。最后一条命令语句指定与 myacl 中的 ACE 匹配的任何连接由 tplus1 服务器组中的 AAA 服务器授权。

相关命令

命令	说明
aaa authorization	启用或禁用用户授权。
clear configure aaa	将所有 AAA 配置参数重置为默认值。
clear uauth	为一个用户或所有用户删除 AAA 授权和身份验证缓存，强制用户在其下次创建连接时重新进行身份验证。
show running-config aaa	显示 AAA 配置。
show uauth	显示向授权服务器提供用于身份验证和授权目的的用户名、与该用户名绑定的 IP 地址，以及是仅对该用户进行身份验证，还是也对缓存的服务进行身份验证。

aaa local authentication attempts max-fail

要限制 ASA 允许任何给定用户帐户的连续失败的本地登录尝试次数（具有特权级别 15 的用户除外；此功能不影响级别 15 的用户），请在全局配置模式下使用 **aaa local authentication attempts max-fail** 命令。要禁用此功能并允许无限数量的连续失败的本地登录尝试次数，请使用此命令的 **no** 形式。

aaa local authentication attempts max-fail *number*

语法说明

number	在锁定前用户可输入错误密码的最大次数。此数字可以在 1 到 16 的范围内。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅影响使用本地用户数据库进行的身份验证。如果省略此命令，则用户可以输入错误密码的次数不存在任何限制。

用户使用错误密码尝试达到配置的尝试次数后，用户会被锁定，且无法成功登录，直到管理员解锁用户名为止。锁定或解锁用户名会生成系统日志消息。

此命令不影响具有特权级别 15 的用户；无法锁定他们。

当用户成功通过身份验证或 ASA 重启时，失败的尝试次数重置为零，且锁定状态重置为 No。

示例

以下示例展示使用 **aaa local authentication attempts max-limits** 命令将允许的最大尝试失败次数设置为 2：

```
ciscoasa(config)# aaa local authentication attempts max-limits 2
```

相关命令

命令	说明
clear aaa local user lockout	清除指定用户的锁定状态并将其失败尝试次数计数器设置为 0。
clear aaa local user fail-attempts	将失败的用户身份验证尝试次数重置为零，而无需修改用户锁定状态。
show aaa local user	显示当前锁定的用户名的列表。

aaa mac-exempt

要指定使用要免除身份验证和授权的 MAC 地址的预定义列表，请在全局配置模式下使用 **aaa mac-exempt** 命令。要禁止使用 MAC 地址的列表，请使用此命令的 **no** 形式。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

语法说明

id	指定使用 **mac-list** 命令配置的 MAC 列表编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您只能添加一个 **aaa mac-exempt** 命令。在使用 **aaa mac-exempt** 命令前，使用 **mac-list** 命令配置 MAC 列表编号。MAC 列表中的 permit 条目使 MAC 地址免除身份验证和授权，而 deny 条目需要对 MAC 地址进行身份验证和授权（如果已启用）。您只能添加 **aaa mac-exempt** 命令的一个实例，因此请确保 MAC 列表包括要免除的所有 MAC 地址。

示例

以下示例对单个 MAC 地址跳过身份验证：

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

以下条目对所有硬件 ID 为 0003.E3 的思科 IP 电话跳过身份验证：

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

以下示例免除对一组 MAC 地址的身份验证，其中 00a0.c95d.02b2 除外：

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

相关命令

命令	说明
aaa authentication	启用用户身份验证。
aaa authorization	启用用户授权服务。
aaa mac-exempt	免除 MAC 地址列表中地址的身份验证和授权。
show running-config mac-list	显示之前在 **mac-list** 命令中指定的 MAC 地址列表。
mac-list	指定一个 MAC 地址列表，用于使 MAC 地址免除身份验证和 / 或授权。

aaa proxy-limit

要为给定 IP 地址限制并发身份验证尝试次数（同时），请在全局配置模式下使用 **aaa proxy-limit** 命令。要恢复为默认代理限制值，请使用此命令的 **no** 形式。

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

语法说明

disable	指定不允许任何代理。
proxy_limit	指定每个用户允许的并发代理连接数，其范围为 1 到 128。

默认值

默认代理限制值为 16。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果源地址是代理服务器，请考虑将此 IP 地址从身份验证中排除，或增加允许的未完成的 AAA 请求数。

例如，如果两个用户位于同一 IP 地址（可能与终端服务器连接），且他们都打开浏览器或连接并同时尝试开始进行身份验证，则仅允许一个用户通过，第二个用户会被拦截。

来自该 IP 地址的第一个会话将被代理并向其发送身份验证请求，而另一个会话会超时。这与单个用户名具有多少连接无关。

示例

以下示例展示如何为给定 IP 地址设置最大未完成的身份验证尝试（同时）次数：

```
ciscoasa(config)# aaa proxy-limit 6
```

相关命令

命令	说明
aaa authentication	启用、禁用或查看 LOCAL、TACACS+ 或 RADIUS 用户身份验证（在 **aaa-server** 命令指定的服务器上）或 ASDM 用户身份验证。
aaa authorization	启用或禁用 LOCAL 或 TACACS+ 用户授权服务。
aaa-server host	指定 AAA 服务器。
clear configure aaa	删除或重置配置的 AAA 记账值。
show running-config aaa	显示 AAA 配置。

aaa-server

要创建 AAA 服务器组并配置特定于组且为所有组主机共有的 AAA 服务器参数，请在全局配置模式下使用 **aaa-server** 命令。要删除指定的组，请使用此命令的 **no** 形式。

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

语法说明

protocol *server-protocol*	指定组中服务器支持的 AAA 协议： • **http-form** • **kerberos** • **ldap** • **nt**（请注意，此选项自 9.3(1) 版本起不再可用。） • **radius** • **sdi** • **tacacs+**
server-tag	指定与 **aaa-server host** 命令指定的名称匹配的服务器组名称。其他 AAA 命令引用 AAA 服务器组名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	添加了 **http-form** 协议。
8.2(2)	单一模式的最大 AAA 服务器组数从 15 增加至 100。
8.4(2)	添加了 AAA 服务器组配置模式下的 **ad-agent-mode** 选项。
9.3(1)	**nt** 选项不再可用。Windows NT 域身份验证支持已弃用。

使用指南

在单模式下您可以具有最多 100 个服务器组，在多模式下每个情景具有 4 个服务器组。在单模式下每个组可以具有最多 15 个服务器，在多模式下具有 4 个服务器。用户登录时，从您在配置中指定的第一个服务器开始一次访问一个服务器，直到有服务器响应为止。

通过使用 **aaa-server** 命令定义 AAA 服务器组协议来控制 AAA 服务器配置，然后使用 **aaa-server host** 命令将服务器添加到组中。输入 **aaa-server protocol** 命令时，会进入 AAA 服务器组配置模式。

如果使用 RADIUS 协议且在 AAA 服务器组配置模式下，请注意以下方面：

- 要为无客户端 SSL 和 AnyConnect 会话启用多会话记账，请输入 **interim-accounting-update** 选项。如果选择此选项，则除开始和停止记录外还将临时记账记录发送到 RADIUS 服务器。
- 要指定 ASA 和 AD 代理之间的共享密钥，并指示 RADIUS 服务器组包括并非具有完整功能的 RADIUS 服务器的 AD 代理，请输入 **ad-agent-mode** 选项。仅可将使用此选项配置的 RADIUS 服务器组与用户身份关联。因此，当指定未使用 **ad-agent-mode** 选项配置的 RADIUS 服务器组时，**test aaa-server** {**authentication** | **authorization**} *aaa-server-group* 命令不可用。

注　每当在启动期间从配置中输入或读取 **aaa-server protocol nt** 命令时，ASA 向控制台显示一条消息。消息指示此身份验证方法会在 ASA 的下一个主版本中删除。

示例

以下示例展示使用 **aaa-server** 命令修改 TACACS+ 服务器组配置的详细信息：

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# reactivation mode timed
ciscoasa(config-aaa-server-group)# max-failed attempts 2
```

相关命令

命令	说明
accounting-mode	指示是将记账消息发送给单个服务器（单一模式），还是发送给组中的所有服务器（同时模式）。
reactivation-mode	指定重新激活发生故障的服务器的方法。
max-failed-attempts	指定服务器组中的任何给定的服务器之前都会禁用该服务器将容忍的失败的次数。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

aaa-server active, fail

要重新激活标记为发生故障的 AAA 服务器，请在特权 EXEC 模式下使用 **aaa-server active** 命令。要停用活动服务器，请在特权 EXEC 模式下使用 **aaa-server fail** 命令。

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

语法说明

active	将服务器设置为活动状态。
fail	将服务器设置为故障状态。
host	指定主机 IP 地址名称或 IP 地址。
name	用使用 **name** 命令在本地分配的名称或 DNS 名称指定服务器的名称。DNS 名称的最大字符数为 128，使用 **name** 命令分配的名称的最大字符数为 63。
server_ip	指定 AAA 服务器的 IP 地址。
server_tag	指定与 **aaa-server** 命令指定的名称匹配的服务器组的符号名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

若没有此命令，则发生故障的组中的服务器仍处于故障状态，直到该组中的所有服务器发生故障为止，届时重新激活所有服务器。

示例

以下示例展示服务器 192.168.125.60 的状态并手动将其重新激活：

```
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED.Server disabled at 11:10:08 UTC  Fri Aug 22
...
ciscoasa# aaa-server active host 192.168.125.60
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
```

```
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated).Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

相关命令

命令	说明
aaa-server	创建并修改 AAA 服务器组。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

aaa-server host

要将 AAA 服务器配置为 AAA 服务器组的一部分并配置特定于主机的 AAA 服务器参数，请在全局配置模式下使用 **aaa-server host** 命令。要删除主机配置，请使用此命令的 **no** 形式。

aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

语法说明

(*interface-name*)	（可选）指定身份验证服务器所在的网络接口。此参数中的括号是必需的。如果不指定接口，则默认为 **inside**（如果可用）。
key	（可选）指定最多 127 个字符的区分大小写的字母数字关键字，它与 RADIUS 或 TACACS+ 服务器上的密钥具有相同的值。输入的超过 127 的任何字符都会被忽略。在 ASA 和服务器之间使用密钥来对它们之间的数据进行加密。ASA 和服务器系统上的密钥必须相同。密钥中不允许有空格，但是允许有其他特殊字符。您可以在主机模式下使用 **key** 命令添加或修改密钥。
name	用使用 **name** 命令在本地分配的名称或 DNS 名称指定服务器的名称。DNS 名称的最大字符数为 128，使用 **name** 命令分配的名称的最大字符数为 63。
server-ip	指定 AAA 服务器的 IP 地址。
server-tag	指定与 **aaa-server** 命令指定的名称匹配的服务器组的符号名称。
timeout *seconds*	（可选）请求的超时间隔。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。您可以在主机配置模式下使用 **timeout** 命令修改超时间隔。

默认值

默认超时值为 10 秒。

默认接口为内部接口。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	增加了对 DNS 名称的支持。
9.0(1)	已增加对用户身份的支持。

使用指南

通过使用 **aaa-server** 命令定义 AAA 服务器组来控制 AAA 服务器配置，然后使用 **aaa-server host** 命令将服务器添加到组中。使用 **aaa-server host** 命令时，进入 AAA 服务器主机配置模式，您可以从该模式中指定并管理特定于主机的 AAA 服务器连接数据。

在单模式下您可以具有最多 15 个服务器组，在多模式下每个情景具有 4 个服务器组。在单模式下每个组可以具有最多 16 个服务器，在多模式下具有 4 个服务器。用户登录时，从您在配置中指定的第一个服务器开始一次访问一个服务器，直到有服务器响应为止。

示例

以下示例配置名为“watchdogs”的 Kerberos AAA 服务器组，将一个 AAA 服务器添加到该组中，并为该服务器定义 Kerberos 领域：

注　Kerberos 领域名称仅使用数字和大写字母。虽然 ASA 接受小写字母的领域名称，但它不会将小写字母转换为大写字母。请确保仅使用大写字母。

```
ciscoasa(config)# aaa-server watchdogs protocol kerberos
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

以下示例配置名为“svrgrp1”的 SDI AAA 服务器组，然后将一个 AAA 服务器添加到该组中，将超时间隔设置为 6 秒，将重试间隔设置为 7 秒，并将 SDI 版本配置为版本 5：

```
ciscoasa(config)# aaa-server svrgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 6
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# sdi-version sdi-5
```

以下示例展示在将 **aaa-server** *aaa_server_group_tag* 命令用于 LDAP 搜索时，如何缩小目标组的搜索路径：

```
ciscoasa(config)# aaa-server CISCO_AD_SERVER protocol ldap
ciscoasa(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
ciscoasa(config-aaa-server-host)# server-port 636
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password *
ciscoasa(config-aaa-server-host)# ldap-login-dn CISCO\username1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
```

注　指定 **ldap-group-base-dn** 命令时，所有组必须位于 LDAP 目录层次结构中的该命令之下，且任何组不能位于此路径外。

仅当至少存在一个激活的基于用户身份的策略时，**ldap-group-base-dn** 命令才会生效。

必须配置 **server-type microsoft** 命令（并非默认值）。

第一个 **aaa-server** *aaa_server_group_tag* **host** 命令用于 LDAP 操作。

相关命令

命令	说明
aaa-server	创建并修改 AAA 服务器组。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

absolute

要在时间范围生效时定义绝对时间，请在时间范围配置模式下使用 **absolute** 命令。要不为时间范围指定时间，请使用此命令的 **no** 形式。

absolute [**end** *time date*] [**start** *time date*]

no absolute

语法说明

date	（可选）以年月日的格式指定日期；例如，2006 年 1 月 1 日。年份的有效范围为 1993 年到 2035 年。
end	（可选）指定时间范围的结束。
start	（可选）指定时间范围的开始。
time	（可选）以小时分钟的格式指定时间。例如，8:00 是上午 8:00， 20:00 是下午 8:00。

默认值

如果未指定任何开始时间和日期，则 permit 或 deny 语句立即生效且始终有效。同样，最大结束时间是 2035 年 12 月 31 日 23:59。如果未指定任何结束时间和日期，则关联的 permit 或 deny 语句无限期有效。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
时间范围配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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。

示例

以下示例在 2006 年 1 月 1 日上午 8:00 激活 ACL：

```
ciscoasa(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

相关命令

命令	说明
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。
time-range	定义对 ASA 基于时间的访问控制。

accept-subordinates

要在以前未在设备上安装下级 CA 证书时将 ASA 配置为接受这些证书（如果在第一阶段 IKE 交换期间交付），请在 crypto ca trustpoint 配置模式下使用 **accept-subordinates** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

accept-subordinates

no accept-subordinates

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 ON（接受下级证书）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在第 1 阶段处理期间，IKE 对等设备可能通过下级证书和身份证书。下级证书可能尚未在 ASA 上安装。此命令允许管理员支持未在设备上配置为信任点的下级 CA 证书，而不要求所有建立的信任点的所有下级 CA 证书均可接受；换句话说，此命令让设备可以对证书链进行身份验证，而无需在本地安装完整的链。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并允许 ASA 为中心信任点接受下级证书：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# accept-subordinates
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。

access-group

要将扩展的 ACL 与单个接口绑定，请在全局配置模式下使用 **access-group** 命令。要从接口取消绑定 ACL，请使用此命令的 **no** 形式。

access-group *access_list* {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**]

no access-group *access_list* {**in** | **out**} **interface** *interface_name*

要使用单个命令将一组全局规则应用于所有接口，请在全局配置模式下使用 **access-group global** 命令。要从所有配置的接口中删除全局规则，请使用此命令的 **no** 形式。

access-group *access_list* [**global**]

no access-group *access_list* [**global**]

语法说明

access_list	扩展的 ACL *id*。
control-plane	（可选）指定 ACL 是否用于所有传入流量（to-the-box 流量）。例如，您可以使用此选项通过拦截 ISAKMP 来阻止某些远程 IP 地址启动到 ASA 的 VPN 会话。用于所有传入管理流量的访问规则（由 **http**、**ssh** 或 **telnet** 等此类命令定义）的优先级比使用 **control-plane** 选项应用的 ACL 高。因此，允许此类允许的管理流量传入，即使被所有传入 ACL 明确拒绝。此选项仅对 **in** 方向可用。
global	将 ACL 应用于所有接口上的所有流量。
in	过滤指定接口上的入站数据包。
interface *interface_name*	网络接口的名称。
out	过滤指定接口上的出站数据包。
per-user-override	（可选）允许可下载的用户 ACL 覆盖应用于接口的 ACL。此选项仅对 **in** 方向可用。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.3(1)	修改了此命令以支持全局策略。

使用指南

特定于接口的访问组规则的优先级高于全局规则，因此在数据包分类时，先处理特定于接口的规则，再处理全局规则。

特定于接口的规则的使用指南

access-group 命令将扩展的 ACL 与接口绑定。您必须首先使用 **access-list extended** 命令创建 ACL。

您可以将 ACL 应用于向接口传入或从接口传出的流量。如果在 **access-list** 命令语句中输入 **permit** 选项，则 ASA 继续处理数据包。如果在 **access-list** 命令语句中输入 **deny** 选项，则 ASA 丢弃数据包并生成系统日志消息 106023 或 106100（对于使用非默认日志记录的 ACE）。

对于入站 ACL，**per-user-override** 选项允许下载的 ACL 覆盖应用于接口的 ACL。如果 **per-user-override** 选项不存在，则 ASA 保持现有过滤行为。当存在 **per-user-override** 时，ASA 允许与用户关联的每用户访问列表中的 **permit** 或 **deny** 状态（如果已下载一个列表）覆盖与 ACL 关联的 **access-group** 命令中的 permit 或 deny 状态。此外，遵守以下规则：

- 在数据包到达时，如果没有与数据包关联的每用户 ACL，则会应用接口 ACL。
- 每用户 ACL 由 **timeout** 命令的 **uauth** 选项指定的超时值管理，但是 AAA 每用户会话超时值可以将其覆盖。
- 现有 ACL 日志行为是相同的。例如，如果因每用户 ACL 拒绝用户流量，则会记录系统日志消息 109025。如果允许用户流量，则不会生成任何系统日志消息。每用户访问列表中的日志选项将不起作用。

默认情况下，VPN 远程访问流量与接口 ACL 不匹配。但是，如果使用 **no sysopt connection permit-vpn** 命令关闭此旁路，则该行为取决于是否存在应用于组策略的 **vpn-filter**，以及是否设置 **per-user-override** 选项：

- 无 **per-user-override**，无 **vpn-filter** - 流量与接口 ACL 匹配。
- 无 **per-user-override**、**vpn-filter** - 流量首先与接口 ACL 匹配，然后与 VPN 过滤器匹配。
- **per-user-override**、**vpn-filter** - 流量仅与 VPN 过滤器匹配。

注　如果从一个或多个 **access-group** 命令引用的 ACL 中删除所有功能条目（permit 和 deny 语句），则自动从配置中删除 **access-group** 命令。**access-group** 命令无法引用空白 ACL 或仅包含一条注释的 ACL。

全局规则的使用指南

access-group global 命令将一组全局规则应用于所有流量，无论流量到达 ASA 上的哪个接口。

所有全局规则仅应用于入口（入站）方向的流量。全局规则不支持出口（出站）流量。如果结合入站接口访问规则配置全局规则，则先处理特定的接口访问规则，再处理通用的全局访问规则。

示例

以下示例展示如何使用 **access-group global** 命令将 ACL 应用于所有配置的接口：

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any

ciscoasa(config)# access-group acl-2
ciscoasa(config)# access-group acl-1 in interface outside

ciscoasa(config)# show run access-group acl-2
ciscoasa(config)# access-group acl-1 in interface outside

ciscoasa(config)# access-group acl-2 global
```

以上访问组配置在分类表中添加以下规则（从 **show asp table classify** 命令中输出）：

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

以上规则将流量从 10.1.2.2 传递到输出接口上的 10.2.2.2，并因全局拒绝规则丢弃从 10.1.1.10 到输出接口上的 10.2.2.20 的流量。

以下示例允许从任何地方对 DMZ 中的 HTTP 服务器的全局访问（使用 IP 地址 10.2.2.2）：

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

以上规则允许从外部主机 10.1.2.2 到主机 10.2.2.2 的 HTTP 连接，且它允许从内部主机 192.168.0.0 到主机 10.2.2.2 的 HTTP 连接。

以下示例展示如何结合使用全局策略和接口策略。该示例允许从任何内部主机访问服务器（使用 IP 地址 10.2.2.2），但是它拒绝从任何其他主机访问该服务器。接口策略优先。

```
ciscoasa(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
ciscoasa(config)# access-list global_acl deny ip any host 10.2.2.2
ciscoasa(config)# access-group inside_acl in interface inside
ciscoasa(config)# access-group global_acl global
```

以上规则拒绝从外部主机 10.1.2.2 到主机 10.2.2.2 的 SSH 连接，它允许从内部主机 192.168.0.0 到主机 10.2.2.2 的 SSH 连接。

以下示例展示 NAT 和全局访问控制策略如何配合使用。该示例允许一个从外部主机 10.1.2.2 到主机 10.2.2.2 的 HTTP 连接，也允许另一个从内部主机 192.168.0.0 到主机 10.2.2.2 的 HTTP 连接，但拒绝（根据隐式规则）一个从外部主机 10.255.255.255 到主机 172.31.255.255 的 HTTP 连接。

```
ciscoasa(config)# object network dmz-server host 10.1.1.2
ciscoasa(config)# nat (any, any) static 10.2.2.2
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

以下示例展示 NAT 和全局访问控制策略如何配合使用。该示例允许一个从主机 10.1.1.1 到主机 192.168.0.0 的 HTTP 连接，也允许另一个从主机 209.165.200.225 到主机 172.16.0.0 的 HTTP 连接，但拒绝一个从主机 10.1.1.1 到主机 172.16.0.0 的 HTTP 连接。

```
ciscoasa(config)# object network 10.1.1.1 host 10.1.1.1
ciscoasa(config)# object network 172.16.0.0 host 172.16.0.0
ciscoasa(config)# object network 192.168.0.0 host 192.168.0.0
ciscoasa(config)# nat (inside, any) source static 10.1.1.1 10.1.1.1 destination static
                  192.168.0.0 172.16.0.0
```

```
ciscoasa(config)# access-list global_acl permit ip object 10.1.1.1 object 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip host 209.165.200.225 object 172.16.0.0
ciscoasa(config)# access-list global_acl deny ip any 172.16.0.0
ciscoasa(config)# access-group global_acl global
```

相关命令

命令	说明
access-list extended	创建扩展的 ACL。
clear configure access-group	从所有接口删除访问组。
show running-config access-group	显示与接口绑定的当前 ACL。

access-list alert-interval

要指定各拒绝流最大值消息之间的时间间隔，请在全局配置模式下使用 **access-list alert-interval** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

access-list alert-interval *secs*

no access-list alert-interval

语法说明

secs	各拒绝流最大值消息生成之间的时间间隔；有效值为从 1 到 3600 秒。默认值为 300 秒。

默认值

默认值为 300 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果为 ACL deny 语句配置 **log** 选项且流量与 ACL 语句匹配，则设备缓存流信息。为防止缓存过载，为系统日志消息 106100 中显示的统计信息保留的缓存拒绝流具有最大数量。如果在发出 106100 并重置缓存前达到最大值，则发出系统日志消息 106101 以指示超过拒绝流最大值。

access-list alert-interval 命令设置生成系统日志消息 106101 的时间间隔。当达到拒绝流最大值时，如果自生成上一条系统日志消息 106101 至少已经过 *secs* 秒，则生成另一条系统日志消息 106101。

请参阅 **access-list deny-flow-max** 命令，了解有关拒绝流最大值消息生成的信息。

示例

以下示例展示如何指定各拒绝流最大值消息之间的时间间隔：

```
ciscoasa(config)# access-list alert-interval 30
```

相关命令

命令	说明
access-list deny-flow-max	指定可创建的并发拒绝流的最大数量。
access-list extended	将 ACL 添加到配置中并将其用于为通过 ASA 的 IP 流量配置策略。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。

access-list deny-flow-max

要指定可缓存的并发拒绝流的最大数量以计算消息 106100 的统计信息，请在全局配置模式下使用 **access-list deny-flow-max** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

access-list deny-flow-max *number*

no access-list deny-flow-max *number*

语法说明

number	应缓存以计算系统日志消息 106100 的统计信息的拒绝流的最大数量，在 1 和 4096 之间。默认值为 4096。

默认值

默认值为 4096。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当 ASA 达到缓存拒绝流的最大数量时，生成系统日志消息 106101。

示例

以下示例展示如何指定可缓存的并发拒绝流的最大数量：

```
ciscoasa(config)# access-list deny-flow-max 256
```

相关命令

命令	说明
access-list alert-interval	设置发出各 106101 消息之间的时间。
access-list extended	将 ACL 添加到配置中并将其用于为通过 ASA 的 IP 流量配置策略。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list ethertype

要配置控制基于其 EtherType 的流量的 ACL，请在全局配置模式下使用 **access-list ethertype** 命令。要删除 ACL，请使用此命令的 **no** 形式。

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **isis** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **isis** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

语法说明

any	允许或拒绝所有流量。
bpdu	允许或拒绝桥接协议数据单元。
deny	拒绝流量。
hex_number	允许或拒绝具有特定 EtherType（指定为一个大于或等于 0x600 的 16 位十六进制数字）的流量。
id	指定 ACL 的名称或编号。
ipx	允许或拒绝 IPX。
isis	允许或拒绝中间系统到中间系统 (IS-IS)。
mpls-multicast	允许或拒绝 MPLS 组播。
mpls-unicast	允许或拒绝 MPLS 单播。
permit	允许流量。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4 (5)、9.1(2)	我们添加了 **isis** 关键字。

使用指南

EtherType ACL 由一个或多个指定 EtherType 的访问控制项 (ACE) 组成。EtherType 规则控制一个 16 位十六进制数字标识的任何 EtherType，以及选定的流量类型。

注　对于 EtherType ACL，在 ACL 末尾的隐式拒绝不影响 IP 流量或 ARP；例如，如果允许 EtherType 8037，则在 ACL 末尾的隐式拒绝当前不拦截之前使用扩展的 ACL 允许的任何 IP 流量（或从较高安全接口到较低安全接口隐式允许的 IP 流量）。但是，如果明确拒绝具有 EtherType ACE 的所有流量，则拒绝 IP 和 ARP 流量；仍仅允许物理协议流量，例如自动协商。

支持的 EtherType 和其他流量

EtherType 规则控制以下方面：

- 一个 16 位十六进制数字标识的 EtherType，包括常见类型 IPX 和 MPLS 单播或组播。
- 以太网 V2 帧。
- 默认情况下允许的 BPDU。BPDU 为 SNAP 封装，且 ASA 专为处理 BPDU 而设计。
- 中继端口（思科专有）BPDU。中继 BPDU 在负载内包含 VLAN 信息，因此如果允许 BPDU，则 ASA 使用传出 VLAN 修改负载。
- 中间系统到中间系统 (IS-IS)。

不支持以下类型的流量：

- 802.3 格式化帧 - 规则不处理这些帧，因为它们使用不同于类型字段的长度字段。

返回流量的访问规则

由于 EtherType 是无连接的，如果希望流量在两个方向传递，您需要将规则应用于两个接口。

允许 MPLS

如果允许 MPLS，请确保通过配置连接到 ASA 的两个 MPLS 路由器以将 ASA 接口上的 IP 地址用作 LDP 或 TDP 会话的路由器 ID，来通过 ASA 建立标签分发协议和标记分发协议 TCP 连接。（LDP 和 TDP 允许 MPLS 路由器协商用于转发数据包的标签（地址）。）

在思科 IOS 路由器上，输入您的协议、LDP 或 TDP 的相应命令。接口是连接到 ASA 的接口。

```
ciscoasa(config)# mpls ldp router-id interface force
```

或

```
ciscoasa(config)# tag-switching tdp router-id interface force
```

示例

以下示例展示如何添加 EtherType ACL：

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

相关命令

命令	说明
access-group	将 ACL 与接口绑定。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list extended

要将访问控制项 (ACE) 添加到扩展的 ACL，请在全局配置模式下使用 **access-list extended** 命令。要删除 ACE，请使用此命令的 **no** 形式。

对于任何类型的流量，不具有端口：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

对于 TCP 或 UDP 流量，具有端口：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

对于 ICMP 流量，具有 ICMP 类型：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**}[*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

语法说明

access_list_name	将 ACL ID 指定为长度最多 241 个字符的字符串或整数。ID 是区分大小写的。 **提示**　全部使用大写字母可更好地查看配置中的 ACL ID。
deny	如果条件匹配，则拒绝数据包。在网络访问时（**access-group** 命令），此关键字阻止数据包通过 ASA。在将应用检查应用于类映射时（**class-map** 和 **inspect** 命令），此关键字使流量免除检查。某些功能不允许使用拒绝 ACE。请参阅针对使用 ACL 的每个功能的命令文档，了解更多信息。

dest_address_argument	指定数据包要发往的 IP 地址或 FQDN。可用参数包括： • **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。指定网络掩码时，方法与思科 IOS 软件 **access-list** 命令不同。ASA 使用网络掩码（例如，对于 C 类掩码为 255.255.255.0）。思科 IOS 掩码使用通配符位（例如 0.0.0.255）。 • *ipv6-address*/*prefix-length* - 指定 IPv6 主机或网络地址和前缀。 • **any**、**any4** 和 **any6** - **any** 指定 IPv4 和 IPv6 流量； **any4** 仅指定 IPv4 流量； **any6** 仅指定 IPv6 流量。 • **interface** *interface_name* - 指定 ASA 接口的名称。使用接口名称（而非 IP 地址）基于接口是流量的源还是目标来匹配流量。当流量源是设备接口时，您必须指定接口关键字而非在 ACL 中指定实际 IP 地址。例如，您可以使用此选项通过拦截 ISAKMP 来阻止某些远程 IP 地址启动到 ASA 的 VPN 会话。来自或发往 ASA 的任何流量本身需要您使用带有 **control-plane** 关键字的 **access-group** 命令。 • **object** *nw_obj_id* - 指定使用 **object network** 命令创建的网络对象。 • **object-group** *nw_grp_id* - 指定使用 **object-group network** 命令创建的网络对象组。
icmp_argument	（可选）指定 ICMP 类型和代码。 • *icmp_type* [*icmp_code*] - 按名称或编号指定 ICMP 类型，以及用于该类型的可选 ICMP 代码。如果不指定代码，则使用所有代码。 • **object-group** *icmp_grp_id* - 为使用 **object-group service** 或（弃用的）**object-group icmp** 命令创建的 ICMP/ICMP6 指定对象组。
inactive	（可选）禁用 ACE。要重新启用它，请输入不带有 **inactive** 关键字的完整 ACE。通过此功能，您可以在配置中保留非活动 ACE 的记录以使重新启用更轻松。
line *line-num*	（可选）指定要插入 ACE 的行号。如果不指定行号，则将 ACE 添加到 ACL 的末尾。行号不保存在配置中；它仅指定插入 ACE 的位置。
log [[*level*] [**interval** *secs*] | **disable** | **default**]	（可选）当 ACE 与用于网络访问的数据包匹配时，设置日志记录选项（使用 **access-group** 命令应用的 ACL）。如果输入不带有任何参数的 **log** 关键字，则在默认级别 (6) 为默认间隔（300 秒）启用系统日志消息 106100。如果不输入 **log** 关键字，则为拒绝的数据包生成默认系统日志消息 106023。日志选项是： • *level* - 在 0 和 7 之间的严重级别。默认值为 6（信息性）。如果您为活动 ACE 更改此级别，则新级别应用于新连接；现有连接继续记录在原来的级别中。 • **interval** *secs* - 各系统日志消息之间的时间间隔（以秒为单位），从 1 到 600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。 • **disable** - 禁用所有 ACE 日志记录。 • **default** - 对消息 106023 启用日志记录。此设置与不包括 **log** 选项相同。
permit	如果条件匹配，则允许数据包。在网络访问时（**access-group** 命令），此关键字允许数据包通过 ASA。在将应用检查应用于类映射时（**class-map** 和 **inspect** 命令），此关键字将检查应用于数据包。

port_argument	（可选）如果将协议设置为 TCP 或 UDP，则指定源或目标端口。如果不指定端口，则与所有端口匹配。可用参数包括： • *operator port* - *operator* 可以是以下项之一： – **lt** - 小于 – **gt** - 大于 – **eq** - 等于 – **neq** - 不等于 – **range** - 值的范围（含两端）。使用此运算符时，需指定两个端口号，例如： `range 100 200` *port* 可以是表示 TCP 或 UDP 端口号的整数或端口名称。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC 和 Talk 都需要一个对 TCP 的定义和一个对 UDP 的定义。TACACS+ 需要一个对 TCP 上的端口 49 的定义。 • **object** *service_obj_id* - 指定使用 **object service** 命令创建的服务对象。 • **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。
protocol_argument	指定 IP 协议。可用参数包括： • *name* 或 *number* - 指定协议名称或编号。例如，UDP 是 17，TCP 是 6，EGP 是 47。指定 **ip** 以应用于所有协议。请参阅 CLI 帮助，了解可用选项。 • **object-group** *protocol_grp_id* - 指定使用 **object-group protocol** 命令创建的协议对象组。 • **object** *service_obj_id* - 指定使用 **object service** 命令创建的服务对象。TCP、UDP 或 ICMP 服务对象包括一个协议和一个源和 / 或目标端口或 ICMP 类型和代码，用于将流量与 ACE 匹配时；无需在 ACE 中分别配置端口 / 类型。 • **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。
security_group_argument	为与 TrustSec 功能结合使用，除源地址或目标地址外还指定要将流量与其匹配的安全组。可用参数包括： • **object-group-security** *security_obj_grp_id* - 指定使用 **object-group security** 命令创建的安全对象组。 • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} - 指定安全组名称或标记。
source_address_argument	指定发送数据包的 IP 地址或 FQDN。可变参数与为 *dest_address_argument* 描述的相同。
tcp	将协议设置为 TCP。
time-range *time_range_name*	（可选）指定时间范围对象，用于确定一天中 ACE 处于活动状态的时间和一周中保持此状态的天数。如果不包括时间范围，则 ACE 始终为活动状态。请参阅 **time-range** 命令，了解有关定义时间范围的信息。
udp	将协议设置为 UDP。

user_argument	为与身份防火墙功能结合使用，除源地址外还指定要将流量与其匹配的用户或组。可用参数包括： • **object-group-user** *user_obj_grp_id* - 指定使用 **object-group user** 命令创建的用户对象组。 • **user** {[*domain_nickname*\]*name* | **any** | **none**} - 指定用户名。指定 **any** 以将所有用户与用户凭证匹配，或指定 **none** 以匹配未映射到用户名的地址。这些选项对于将 **access-group** 与 **aaa authentication match** 策略结合特别有用。 • **user-group** [*domain_nickname*\\]*user_group_name* - 指定用户组名称。请注意双反斜线 \\ 将域名与组名称隔开。

默认值

- 用于拒绝 ACE 的默认日志记录仅为拒绝的数据包生成系统日志消息 106023。
- 指定 **log** 关键字时，系统日志消息 106100 的默认级别是 6（信息性），且默认间隔为 300 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.3(1)	使用 NAT 或 PAT 时，在用于几种功能的 ACL 中不再需要映射的地址和端口。现在，您应始终将未转换的实际地址和端口用于这些功能。使用实际地址和端口意味着，如果 NAT 配置更改，您无需更改 ACL。有关详细信息，请参阅第 1-67 页上的 “ 使用实际 IP 地址的功能 ” 一节。
8.4(2)	除源 IP 地址或目标 IP 地址外，您现在还可以将身份防火墙用户和组用于源和目标。为源和目标增加了对 **user**、**user-group** 和 **object-group-user** 的支持。
9.0(1)	除源 IP 地址或目标 IP 地址外，您现在还可以将 TrustSec 安全组用于源和目标。为源或目标增加了对 **security-group** 和 **object-group-security** 的支持。
9.0(1)	增加了对 IPv6 的支持。更改了 **any** 关键字以表示 IPv4 和 IPv6 流量。添加了 **any4** 和 **any6** 关键字以分别表示纯 IPv4 和纯 IPv6 流量。您可以为源和目标指定 IPv4 和 IPv6 地址的组合。如果使用 NAT 在 IPv4 和 IPv6 之间转换，则实际数据包不会包括 IPv4 和 IPv6 地址的组合；但是，对于许多功能，ACL 始终使用实际 IP 地址，且不会考虑 NAT 映射的地址。特定于 IPv6 的 ACL 已弃用。将现有 IPv6 ACL 迁移到扩展的 ACL。请参阅版本说明，了解有关迁移的更多信息。有关 ACL 迁移的信息，请参阅 9.0 版本说明。
9.0(1)	增加了对 ICMP 代码的支持。将 **icmp** 指定为协议时，您可以输入 *icmp_type* [*icmp_code*]。

使用指南

ACL 由一个或多个具有相同 ACL ID 的 ACE 组成。将 ACL 用于控制网络访问或指定供许多功能操作的流量。除非在 ACE 中指定行号，否则将您为给定 ACL 名称输入的每个 ACE 附加到 ACL 的末尾。要删除整个 ACL，请使用 **clear configure access-list** 命令。

ACE 的顺序

ACE 的顺序非常重要。当 ASA 决定是转发还是丢弃数据包时，ASA 按条目的列出顺序使用每个 ACE 测试数据包。找到匹配项后，不再检查更多 ACE。例如，如果您在 ACL 的开头创建一个明确允许所有流量的 ACE，则不进一步检查其他语句。

使用实际 IP 地址的功能

以下命令和功能在 ACL 中使用实际 IP 地址：

- **access-group** 命令
- 模块化策略框架 **match access-list** 命令
- 僵尸网络流量过滤器 **dynamic-filter enable classify-list** 命令
- AAA **aaa ... match** 命令
- WCCP **wccp redirect-list group-list** 命令

使用映射的 IP 地址的功能

以下功能使用 ACL，但是这些 ACL 使用接口上可见的映射的值：

- IPsec ACL
- **capture** 命令 ACL
- 每用户 ACL
- 路由协议 ACL
- 所有其他功能 ACL

不支持身份防火墙、FQDN 和 TrustSec ACL 的功能

以下功能使用 ACL，但无法接受带有身份防火墙（指定用户或组名称）、FQDN（完全限定域名）或 TrustSec 值的 ACL：

- **route-map** 命令
- VPN **crypto map** 命令
- VPN **group-policy** 命令，**vpn-filter** 除外
- WCCP
- DAP

示例

以下 ACL 允许所有主机（在应用 ACL 的接口上）通过 ASA：

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

以下示例 ACL 阻止 192.168.1.0/24 上的主机访问 209.165.201.0/27 网络。允许所有其他地址。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

如果要限制为仅可访问某些主机，请输入受限的 **permit ACE**。默认情况下，除非明确允许，否则拒绝所有其他流量。

```
ciscoasa(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

以下 ACL 限制所有主机（在应用 ACL 的接口上）访问位于 209.165.201.29 地址的网站。允许所有其他流量。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

以下 ACL 使用对象组，它限制内部网络上的若干主机访问几台 Web 服务器。允许所有其他流量。

```
ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

以下示例暂时禁用一个 ACL，该 ACL 允许从一组网络对象 (A) 到另一组网络对象 (B) 的流量：

```
ciscoasa(config)# access-list 104 permit ip host object-group A object-group B inactive
```

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
```

请参阅 **time-range** 命令，了解有关如何定义时间范围的更多信息。

以下 ACL 允许任何 ICMP 流量：

```
ciscoasa(config)# access-list abc extended permit icmp any any
```

以下 ACL 允许用于对象组 “obj_icmp_1” 的任何 ICMP 流量：

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

以下 ACL 允许从源主机 10.0.0.0 到目标主机 10.1.1.1、具有 ICMP 类型 3 和 ICMP 代码 4 的 ICMP 流量。不允许所有其他类型的 ICMP 流量。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

以下 ACL 允许从源主机 10.0.0.0 到目标主机 10.1.1.1、具有 ICMP 类型 3 和任何 ICMP 代码的 ICMP 流量。不允许所有其他类型的 ICMP 流量。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

相关命令

命令	说明
access-group	将 ACL 与接口绑定。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACE。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list remark

要在扩展的 EtherType 或标准访问控制条目前后指定要添加的注释的文本，请在全局配置模式下使用 **access-list remark** 命令。要删除注释，请使用此命令的 **no** 形式。

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** *text*

语法说明

id	ACL 的名称。
line *line-num*	（可选）要插入注释的行号。
remark text	注释的文本

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

注释文本必须至少包含一个非空格字符；不允许空的注释。注释文本的长度最多为 100 个字符，包括空格和标点符号。

您无法在仅包括一个注释的 ACL 上使用 **access-group** 命令。

示例

以下示例展示如何指定 ACL 末尾的注释文本。

```
ciscoasa(config)# access-list MY_ACL remark checklist
```

相关命令

命令	说明
access-list extended	将 ACL 添加到配置中并将其用于为通过 ASA 的 IP 流量配置策略。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list rename

要重命名 ACL，请在全局配置模式下使用 **access-list rename** 命令。

access-list *id* **rename** *new_acl_id*

语法说明

id	现有 ACL 的名称。
rename *new_acl_id*	将新的 ACL ID 指定为长度最多 241 个字符的字符串或整数。ID 是区分大小写的。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果将 ACL 重命名为同一名称，则 ASA 会以静默方式忽略该命令。

示例

以下示例展示如何将 ACL 从 TEST 重命名为 OUTSIDE：

```
ciscoasa(config)# access-list TEST rename OUTSIDE
```

相关命令

命令	说明
access-list extended	将 ACL 添加到配置中并将其用于为通过 ASA 的 IP 流量配置策略。
clear access-group	清除 ACL 计数器。
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list standard

要将访问控制项 (ACE) 添加到标准 ACL 中，请在全局配置模式下使用 **access-list standard** 命令。要删除 ACE，请使用此命令的 **no** 形式。

access-list *id* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

语法说明

any4	与任何 IPv4 地址匹配。
deny	如果条件匹配，则拒绝或免除数据包。
host *ip_address*	指定 IPv4 主机地址（即子网掩码为 255.255.255.255）。
id	ACL 的名称或编号。
ip_address subnet_mask	指定 IPv4 网络地址和子网掩码。
permit	如果条件匹配，则允许或包括数据包。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

标准 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。标准 ACL 用于有限数量的功能，例如路由映射或 VPN 过滤器。标准 ACL 仅使用 IPv4 地址，且仅定义目标地址。

示例

以下示例展示如何将规则添加到标准 ACL 中：

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

相关命令

命令	说明
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示当前正在运行的访问列表配置。

access-list webtype

要将访问控制项 (ACE) 添加到过滤无客户端 SSL VPN 连接的 webtype ACL 中，请在全局配置模式下使用 **access-list webtype** 命令。要删除 ACE，请使用此命令的 **no** 形式。

access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

no access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

access-list *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

语法说明

deny	匹配条件时拒绝访问。
dest_address_argument	指定数据包要发往的 IP 地址。目标地址选项是： • **host** *ip_address* - 指定 IPv4 主机地址。 • *dest_ip_address mask* - 指定 IPv4 网络地址和子网掩码，例如 10.100.10.0 和 255.255.255.0。 • *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。 • **any**、**any4** 和 **any6** - **any** 指定 IPv4 和 IPv6 流量； **any4** 仅指定 IPv4 流量； **any6** 仅指定 IPv6 流量。
id	指定 ACL 的名称或编号。
inactive	（可选）禁用 ACE。要重新启用它，请输入不带有 **inactive** 关键字的完整 ACE。通过此功能，您可以在配置中保留非活动 ACE 的记录以使重新启用更轻松。
log [[*level*] [**interval** *secs*] | **disable** | **default**]	（可选）当 ACE 与数据包匹配时，设置日志记录选项。如果输入不带有任何参数的 **log** 关键字，则在默认级别 (6) 为默认间隔（300 秒）启用 VPN 过滤器系统日志消息 106102。如果不输入 **log** 关键字，则生成默认 VPN 过滤器系统日志消息 106103。日志选项是： • *level* - 在 0 和 7 之间的严重级别。默认值为 6（信息性）。 • **interval** *secs* - 各系统日志消息之间的时间间隔（以秒为单位），从 1 到 600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。 • **disable** - 禁用所有 ACE 日志记录。 • **default** - 对消息 106103 启用日志记录。此设置与不包括 **log** 选项相同。

operator port	（可选）如果指定 **tcp**，则为目标端口。如果不指定端口，则与所有端口匹配。*operator* 可以是以下项之一： • **lt** - 小于 • **gt** - 大于 • **eq** - 等于 • **neq** - 不等于 • **range** - 值的范围（含两端）。使用此运算符时，需指定两个端口号，例如： `range 100 200` *port* 可以是表示 TCP 端口号的整数或端口名称。
permit	匹配条件时允许访问。
time_range *name*	（可选）指定时间范围对象，用于确定一天中 ACE 处于活动状态的时间和一周中保持此状态的天数。如果不包括时间范围，则 ACE 始终为活动状态。请参阅 **time-range** 命令，了解有关定义时间范围的信息。
url {*url_string* | **any**}	指定要匹配的 URL。使用 **url any** 与所有基于 URL 的流量匹配。否则，请输入 URL 字符串，它可以包括通配符。有关 URL 字符串的提示，请参阅使用指南。

默认值

默认值如下：

- ACL 日志记录为拒绝的数据包生成系统日志消息 106103。
- 指定 **log** 可选关键字时，系统日志消息 106102 的默认级别是 6（信息性）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

access-list webtype 命令用于配置无客户端 SSL VPN 过滤。

以下是指定 URL 时的一些提示和限制：

选择 **any** 与所有 URL 匹配。

- “Permit url any” 会允许具有格式 protocol://server-ip/path 的所有 URL，并会拦截与此模式不匹配的流量，例如端口转发。应让 ACE 允许到所需端口（思科端口 1494）的连接，以便隐式拒绝不会发生。

- 具有 “permit url any” 的 ACL 不影响智能隧道和 ICA 插件，因为它们仅与 smart-tunnel:// 和 ica:// 类型匹配。
- 您可以使用这些协议：cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel:// 和 smtp://。您也可以在协议中使用通配符；例如，htt* 与 http 和 https 匹配，星号 * 与所有协议匹配。例如，*://*.example.com 与传输到 example.com 网络的基于 URL 的任何类型的流量匹配。
- 如果指定 smart-tunnel:// URL，则您可以仅包括服务器名称。URL 无法包含路径。例如，smart-tunnel://www.example.com 可接受，但是不接受 smart-tunnel://www.example.com/index.html。
- 星号 * 与零个字符或任何数量的字符匹配。要与任何 http URL 匹配，请输入 http://*/*。
- 问号 ? 与任何一个字符准确匹配。
- 方括号 [] 是范围运算符，与范围中的任何字符匹配。例如，要与 http://www.cisco.com:80/ 和 http://www.cisco.com:81/ 匹配，请输入 **http://www.cisco.com:8[01]/**。

示例

以下示例展示如何拒绝对特定公司 URL 的访问：

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

以下示例展示如何拒绝对特定网页的访问：

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

以下示例展示如何拒绝通过端口 8080 对特定服务器上的任何 URL 的 HTTP 访问：

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

相关命令

命令	说明
clear configure access-list	从正在运行的配置中清除 ACL。
show access-list	按编号显示 ACL 条目。
show running-config access-list	显示正在 ASA 上运行的访问列表配置。

accounting-mode

要指示是将记账消息发送给单个服务器（单一模式），还是发送给组中的所有服务器（同时模式），请在 AAA 服务器配置模式下使用 **accounting-mode** 命令。要删除记账模式指定，请使用此命令的 **no** 形式。

accounting-mode {**simultaneous** | **single**}

语法说明

simultaneous	将记账消息发送给组中的所有服务器。
single	将记账消息发送给单个服务器。

默认值

默认值为单一模式。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
aaa 服务器配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **single** 关键字将记账消息发送给单个服务器。使用 **simultaneous** 关键字将记账消息发送给服务器组中的所有服务器。

仅当服务器组用于记账时此命令才有意义（RADIUS 或 TACACS+）。

示例

以下示例展示使用 **accounting-mode** 命令将记账消息发送给组中的所有服务器：

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

相关命令

命令	说明
aaa accounting	启用或禁用记账服务。
aaa-server protocol	进入 AAA 服务器组配置模式，因此您可以配置特定于组且为组中所有主机共有的 AAA 服务器参数。
clear configure aaa-server	将删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

accounting-port

要为此主机指定用于 RADIUS 记账的端口号，请在 AAA 服务器主机配置模式下使用 **accounting-port** 命令。要删除身份验证端口指定，请使用此命令的 **no** 形式。

accounting-port *port*

no accounting-port

语法说明

port	用于 RADIUS 记账的端口号；有效值范围为 1 到 65535。

默认值

默认情况下，设备侦听端口 1646 上的 RADIUS 以进行记账（符合 RFC 2058）。如果没有指定端口，则使用 RADIUS 记账默认端口号 (1646)。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server host configuration	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令指定要向其发送记账记录的远程 RADIUS 服务器主机的目标 TCP/UDP 端口号。如果您的 RADIUS 记账服务器使用除 1646 外的端口，则您必须在使用 **aaa-server** 命令启动 RADIUS 服务前为相应的端口配置 ASA。

此命令仅对为 RADIUS 配置的服务器组有效。

示例

以下示例在主机 “1.2.3.4” 上配置名为 “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，并配置记账端口 2222。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accountinq-port 2222
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

相关命令

命令	说明
aaa accounting	保留用户访问哪些网络服务的记录。
aaa-server host	进入 AAA 服务器主机配置模式，因此您可以配置特定于主机的 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-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

accounting-server-group

要指定用于发送记账记录的 AAA 服务器组，请在各种模式下使用 **accounting-server-group** 命令。要从配置中删除记账服务器，请使用此命令的 **no** 形式。

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

语法说明

group_tag	识别之前配置的记账服务器或服务器组。使用 **aaa-server** 命令配置记账服务器。

默认值

默认情况下不配置任何记账服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
隧道组常规属性配置	• 是	—	• 是	—	—
config-mdm-proxy 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令在隧道组常规属性配置模式（而非 WebVPN 配置模式）下可用。
9.3(1)	此命令在配置 MDM 代理模式下可用。

使用指南

ASA 使用记账来记录用户访问的网络资源。如果在 WebVPN 配置模式下输入此命令，则它会转换为隧道组常规属性配置模式下的同一命令。

示例

以下示例在隧道组常规属性配置模式下输入，它为 IPSec 局域网到局域网隧道组 “xyz” 配置名为 “aaa-server123” 的记账服务器组：

```
ciscoasa(config)# tunnel-group xyz type IPSec_L2L
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

以下示例展示如何配置 POP3S 邮件代理以使用名为 POP3SSVRS 的记账服务器组：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# accounting-server-group POP3SSVRS
```

以下示例展示如何配置 MDM 代理记账服务器组：

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# accounting-server-group MDMSVRGRP
```

相关命令

命令	说明
aaa-server	配置身份验证、授权和记账服务器。

acl-netmask-convert 至 application-access hide-details 命令

acl-netmask-convert

要指定 ASA 如何处理在来自使用 **aaa-server host** 命令访问的 RADIUS 服务器的可下载 ACL 中接收的网络掩码，请在 aaa-server 主机配置模式下使用 **acl-netmask-convert** 命令。要删除 ASA 的指定行为，请使用此命令的 **no** 形式。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

语法说明

auto-detect	指定 ASA 应尝试确定所使用的网络掩码表达式的类型。如果 ASA 检测到通配符网络掩码表达式，则将其转换为标准的网络掩码表达式。有关此关键字的详细信息，请参阅 “ 使用指南 ”。
standard	指定 ASA 假设从 RADIUS 服务器收到的可下载 ACL 仅包含标准网络掩码表达式。不执行从通配符网络掩码表达式的任何转换。
wildcard	指定 ASA 假设从 RADIUS 服务器收到的可下载 ACL 只包含通配符网络掩码表达式并在下载 ACL 时将其全部转换为标准网络掩码表达式。

默认值

默认情况下，不执行从通配符网络掩码表达式的任何转换。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Aaa-server-host 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

在 RADIUS 服务器提供包含采用通配符格式的网络掩码的可下载 ACL 时，将 **acl-netmask-convert** 命令与 wildcard 或 auto-detect 关键字一起使用。ASA 要求可下载 ACL 包含标准网络掩码表达式，而思科 VPN 3000 系列集中器要求可下载 ACL 包含通配符网络掩码表达式，后者是标准 netmas 表达式的反转形式。通配符掩码在位位置上用 1 表示忽略，用 0 表示匹配。**acl-netmask-convert** 命令可最大限度地减小这些差别对您在 RADIUS 服务器上如何配置可下载 ACL 的影响。

当您不确定 RADIUS 服务器如何配置时，**auto-detect** 关键字非常有用；但无法明确检测和转换带有 “ 洞 ” 的通配符网络掩码表达式。例如，通配符网络掩码 0.0.255.0 允许在第三个八位组中包含任何内容，可在思科 VPN 3000 系列集中器中有效使用，但 ASA 可能不会将此表达式检测为通配符网络掩码。

示例

以下示例在 “192.168.3.4” 主机上配置名为 “srvgrp1” 的 RADIUS AAA 服务器、支持可下载 ACL 网络掩码的转换、设置超时值为 9 秒、设置重试间隔为 7 秒，并且配置身份验证端口 1650：

```
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)# acl-netmask-convert wildcard
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)#
```

相关命令

命令	说明
aaa authentication	在通过 **aaa-server** 命令指定的服务器上启用或禁用 LOCAL、TACACS+ 或 RADIUS 用户身份验证，或者 ASDM 用户身份验证。
aaa-server host	进入 AAA 服务器主机配置模式，在此模式下可以配置特定于主机的 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-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

action

要将访问策略应用到会话或终止会话，请在动态访问策略记录配置模式下使用 **action** 命令。要重置会话以将访问策略应用到会话，请使用此命令的 **no** 形式。

action {continue | terminate}

no action {continue | terminate}

语法说明

continue	将访问策略应用到会话。
terminate	终止连接。

默认值

默认值为 continue。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
动态访问策略记录配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **continue** 关键字以将访问策略应用到所选的全部 DAP 记录。使用 **terminate** 关键字以终止在所选的任何 DAP 记录中的连接。

示例

以下示例展示如何终止 DAP 策略 Finance 的会话：

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# action terminate
ciscoasa(config-dynamic-access-policy-record)#
```

相关命令

命令	说明
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 记录正在运行的配置。

action cli command

要在事件管理器小应用上配置操作，请在事件管理器小应用配置模式下使用 **action cli command** 命令。要删除配置的操作，请输入 **no action** *n* 命令。

action *n* **cli command** "*command*"

no action *n*

语法说明

"*command*"	指定命令的名称。*command* 选项的值必须位于引号中；否则，如果命令由多个单词组成，则会发生错误。命令在全局配置模式下作为权限级别为 15（最高）的用户来运行。因为已禁用，此命令不接受任何输入。如果命令使 **noconfirm** 选项可用，请使用此选项。
n	指定操作 ID。有效 ID 在 0 到 42947295 之间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
事件管理器小应用配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用此命令在事件管理器小应用上配置操作。

示例

以下示例展示如何在事件管理器小应用上配置操作：

```
hostname (config-applet)# action 1 cli command "show version"
```

相关命令

命令	说明
description	描述小应用。
event manager run	运行事件管理器小应用。
show event manager	显示已配置的每个事件管理器小应用的统计信息。
debug event manager	管理事件管理器的调试跟踪记录。

action-uri

要指定 Web 服务器 URI 以为单点登录 (SSO) 身份验证接收用户名和密码，请在 aaa-server-host 配置模式下使用 **action-uri** 命令。要重置 URI 参数值，请使用此命令的 **no** 形式。

action-uri *string*

no action-uri

注　要正确配置带有 HTTP 协议的 SSO，您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	身份验证计划的 URI。您可以在多行中输入此参数。每行的最大字符数为 255。完整 URI 的最大字符数是 2048。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server-host 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

这是带有 HTTP Forms 命令的 SSO。URI（即统一资源标识符）是一个紧凑字符串，用于标识互联网上的一个内容点，无论它是文本页、视频或声音剪辑、静止或活动图像还是软件程序。URI 最常见的形式是网页地址，网页地址是一种名为 URL 的特定形式或 URI 的子集。

ASA 的 WebVPN 服务器可使用 POST 请求以将 SSO 身份验证请求提交到身份验证 Web 服务器。为此，请配置 ASA，以使用 HTTP POST 请求将用户名和密码传递给身份验证 Web 服务器上的操作 URI。**action-uri** 命令指定 ASA 向其发送 POST 请求的 Web 服务器上的身份验证程序的位置和名称。

可以利用浏览器直接连接到 Web 服务器登录页面，以发现身份验证 Web 服务器上的操作 URI。在浏览器中展示的登录网页的 URL 是身份验证 Web 服务器的操作 URI。

为方便输入，您可以在多个连续行中输入 URI。ASA 会将输入的多行内容连接为 URI。尽管每个 action-uri 行最多包含 255 个字符，但您可以在每行输入较少的字符。

注　字符串中问号的前面必须放置 CTRL-v 转义序列。

示例

以下示例指定 www.example.com 上的 URI：

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

注　在操作 URI 中必须包括主机名和协议。在前一个示例中，它们包含在 URI 开始位置的 http://www.example.com 中。

相关命令

命令	说明
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建隐藏参数以供与 SSO 服务器交换。
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-parameter	在必须提交用户名以供 SSO 身份验证时指定 HTTP POST 请求参数的名称。

activation-key

要在 ASA 上输入一个许可激活密钥，请在特权 EXEC 模式下使用 **activation-key** 命令。

activation-key [**noconfirm**] *activation_key* [**activate** | **deactivate**]

语法说明

activate	激活基于时间的激活密钥。**activate** 为默认值。您为给定功能激活的最后一个基于时间的密钥是活动密钥。
activation_key	将激活密钥应用于 ASA。*activation_key* 是一个五元素十六进制字符串，各个元素之间都有一个空格。前导 0x 说明符是可选的；假设任何值均采用十六进制。 您可以安装一个永久密钥和多个基于时间的密钥。如果输入一个新的永久密钥，它会覆盖已安装的永久密钥。
deactivate	停用基于时间的激活密钥。停用的激活密钥仍然安装在 ASA 中，以后您可以使用 **activate** 关键字来激活该密钥。如果是第一次输入密钥，之后指定 **deactivate**，则在 ASA 上安装的密钥处于不活动状态。
noconfirm	（可选）输入激活密钥而不提示您进行确认。

默认值

默认情况下，您的 ASA 在发货时已经安装许可证。此许可证可能是基础许可证，您要向基础许可证添加更多许可证，也可能它已经安装您的所有许可证，具体取决于您的订购以及您的供应商为您安装的许可证。查看 **activation-key** 命令以确定您已经安装的许可证。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(5)	增加了以下限制： • ASA5510 基础许可证连接数从 32000 到 5000； VLAN 数从 0 增至 10。 • ASA5510 Security Plus 许可证连接数从 64000 增至 130000； VLAN 数从 10 增至 25。 • ASA5520 连接数从 130000 增至 280000； VLAN 数从 25 增至 100。 • ASA5540 连接数从 280000 增至 400000； VLAN 数从 100 增至 200。
7.1(1)	引入了 SSL VPN 许可证。
7.2(1)	为 ASA 5550 和更高版本引入了 5000 用户 SSL VPN 许可证。

版本	修改
7.2(2)	• ASA 5505 ASA 上的 Security Plus 许可证的最大 VLAN 数从 5 个（3 个全功能接口； 1 个故障切换接口；一个限制为备用接口）增至 20 个全功能接口。此外，中继端口数量从 1 增至 8。 • 以下产品的 VLAN 限值有所增加：ASA 5510（基础许可证数从 10 增至 50，Security Plus 许可证数从 25 增至 100）、ASA 5520（从 100 增至 150）和 ASA 5550（从 200 增至 250）。
7.2(3)	对于 Security Plus 许可证，ASA 5510 对端口 0 和 1 支持 GE（千兆以太网）。如果将许可证从基础升级到 Security Plus，则外部以太网 0/0 和 0/1 端口的容量从初始的 FE（快速以太网）(100 Mbps) 增至 GE (1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令更改接口上的速度，使用 **show interface** 命令查看为每个接口配置的当前速度。
8.0(2)	• 引入了 Advanced Endpoint Assessment 许可证。 • ASA 5510 Security Plus 许可证支持 VPN 负载平衡。
8.0(3)	引入了 AnyConnect for Mobile 许可证。
8.0(4)/8.1(2)	引入了对基于时间的许可证的支持。
8.1(2)	ASA 5580 上支持的 VLAN 数量从 100 增至 250。
8.0(4)	引入了 UC Proxy 会话许可证。
8.2(1)	• 引入了僵尸网络流量过滤器许可证。 • 引入了 AnyConnect Essentials 许可证。默认情况下，ASA 使用 AnyConnect Essentials 许可证，但您可以使用 **no anyconnect-essentials** 命令来禁用它以使用其他许可证。 • 引入了 SSL VPN 的共享许可证。
8.2(2)	移动代理不再要求 UC Proxy 许可证。
8.3(1)	• 不再要求每个设备上的故障切换许可证相同。来自主设备和辅助设备的组合许可证是同时用于这两种设备的许可证。 • 基于时间的许可证是可叠加的。 • 引入了 IME 许可证。 • 您可以安装多个基于时间的许可证，一次为一个功能激活一个许可证。 • 您可以使用 **activate** 和 **deactivate** 关键字来分别激活和取消激活基于时间的许可证。

版本	修改
8.4(1)	• 对于带 SSP-10 的 ASA 5550 和 ASA 5585-X，最大情景数从 50 增至 100。对于带 SSP-20 和更高版本的 ASA 5580 和 5585-X，最大数量从 50 增至 250。 • 对于 ASA 5580 和 5585-X，VLAN 的最大数量从 250 增至 1024。 • 我们增加了防火墙连接限制： – ASA 5580-20 - 从 1,000 K 增至 2,000 K。 – ASA 5580-40 - 从 2,000 K 增至 4,000 K。 – 带 SSP-10 的 ASA 5585-X：从 750 K 增至 1,000 K – 带 SSP-20 的 ASA 5585-X：从 1,000 K 增至 2,000 K – 带 SSP-40 的 ASA 5585-X：从 2,000 K 增至 4,000 K – 带 SSP-60 的 ASA 5585-X：从 2,000 K 增至 10,000 K • 对于 ASA 5580，AnyConnect VPN 会话限值从 5,000 增至 10,000。 • 对于 ASA 5580，另一个 VPN 会话限值从 5,000 增至 10,000。 • 使用 IKEv2 的 IPsec 远程访问 VPN 添加到了 AnyConnect Essentials 和 AnyConnect Premium 许可证。 • 站点到站点会话添加到了 Other VPN 许可证（之前的 IPsec VPN）。 • 对于无负载加密的型号（例如 ASA 5585-X），ASA 软件禁用统一通信和 VPN 功能，以便 ASA 可以出口到某些国家 / 地区。

使用指南

获取激活密钥

要获取激活密钥，您需要产品授权密钥，可从您的思科客户代表那里购买产品授权密钥。您需要为每个功能许可证购买单独的产品激活密钥。例如，如果您有基础许可证，您可以分别为高级终端评估和额外的 SSL VPN 会话购买单独的密钥。

在获得产品授权密钥后，请在 Cisco.com 的以下某个 URL 上注册密钥。

- 如果您是 Cisco.com 的注册用户，请访问以下网站：

  http://www.cisco.com/go/license

- 如果您不是 Cisco.com 的注册用户，请访问以下网站：

  http://www.cisco.com/go/license/public

情景模式指南

- 在多情景模式下，在系统执行空间中应用激活密钥。
- 在多情景模式下不支持共享许可证。

故障切换指南

- 在主用 / 主用模式不支持共享许可证。
- 故障切换设备不要求每个设备上使用相同的许可证。

  ASA 软件的早期版本要求每个设备上的许可证匹配。从版本 8.3(1) 开始，不再需要安装相同的许可证。通常，您仅为主设备购买许可证；对于主用 / 备用故障切换，辅助设备会在变为主用状态时继承主许可证。如果您在两台设备上都有许可证，则这两个许可证会组合为一个运行故障切换集群许可证。

- 对于 ASA 5505 和 5510，两个设备都需要 Security Plus 许可证；基础许可证不支持故障切换，因此，您无法在只有基础许可证的备用设备上启用故障切换。

升级和降级指南

如果从任何之前版本升级到最新版本，您的激活密钥仍保持兼容。但如果要维护降级功能，您可能会遇到问题：

- 降级到版本 8.1 或更早版本 - 在升级后，若您激活*在 8.2 之前*引入的其他功能许可证，则您执行降级后激活密钥会继续与早期版本兼容。但是，如果激活在 *8.2 或更高版本*中引入的功能许可证，则激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下指导原则：
  - 如果您之前输入过早期版本的激活密钥，则 ASA 会使用该密钥（没有您在版本 8.2 或更高版本中激活的任何新许可证）。
  - 如果您有新系统且没有早期的激活密钥，则需要请求与早期版本兼容的新激活密钥。
- 降级到版本 8.2 或更早的版本 - 8.3 中引入了更强大的基于时间的密钥使用以及故障切换许可证变更：
  - 如果您有多个基于时间的激活密钥处于活动状态，则在您降级后，只有最近激活的基于时间的密钥可以处于活动状态。所有其他密钥都会变为非活动状态。
  - 如果在故障切换对上有不匹配的许可证，则降级将禁用故障切换。即使密钥匹配，使用的许可证也不再是组合许可证。

其他指导原则和限制

- 激活密钥不存储在您的配置文件中；它作为隐藏文件存储在闪存中。
- 激活密钥被绑定到设备的序列号。功能许可证无法在设备之间转移（除非硬件发生故障）。如果您由于硬件故障而必须更换设备，请与思科许可团队联系以将现有许可证转到新的序列号。思科许可团队将要求您提供产品许可密钥参考编号和现有序列号。
- 一旦购买，您将无法退还许可证来获取退款或升级的许可证。
- 虽然您可以激活所有许可类型，但有些功能互不兼容；例如多情景模式和 VPN。AnyConnect Essentials 许可证与以下许可证不兼容：完整 SSL VPN 许可证、共享 SSL VPN 许可证和高级终端评估许可证。默认情况下，使用 AnyConnect Essentials 许可证而不是上述许可证，但您可以使用 **no anyconnect-essentials** 命令在配置中禁用 AnyConnect Essentials 许可证，以恢复使用其他许可证。
- 有些永久许可证会在激活后要求您重新加载 ASA。表 2-1 列出了需要重新加载的许可证。

表 2-1　永久许可证重新加载要求

型号	要求重新加载的许可证操作
ASA 5505 和 ASA 5510	在基础许可证与 Security Plus 许可证之间切换。
所有型号	更改加密许可证。
所有型号	对任何永久许可证降级（例如，从 10 个情景降低到 2 个情景）。

示例

以下示例展示如何更改 ASA 上的激活密钥：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

以下是 **activation-key** 命令的示例输出，其中展示在新激活密钥不同于旧激活密钥时故障切换的输出：

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada

Validating activation key.This may take a few minutes...
The following features available in the running permanent activation key are NOT available
in the new activation key:
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key?[y]
Flash permanent activation key was updated with the requested key.
```

以下是来自许可证文件的示例输出：

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520

Failover                        : Enabled
VPN-DES                         : Enabled
VPN-3DES-AES                    : Enabled
Security Contexts               : 10
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled

----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.

Platform = asa

123456789JA:yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.

Platform = asa

123456789JA:yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

相关命令

命令	说明
anyconnect-essentials	启用或禁用 AnyConnect Essentials 许可证。
show activation-key	显示激活密钥。
show version	显示软件版本和激活密钥。

activex-relay

要将需要 ActiveX 的应用集成到无客户端门户，请在组策略 webvpn 配置模式或用户名 webvpn 模式下使用 **activex-relay** 命令。要从默认组策略继承 **activex-relay** 命令，请使用此命令的 **no** 形式。

activex-relay {**enable** | **disable**}

no activex-relay

语法说明

enable	在 WebVPN 会话上启用 ActiveX。
disable	在 WebVPN 会话上禁用 ActiveX。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **activex-relay enable** 命令，以允许用户为包含对象标记的任何 HTML 内容（如图像、音频、视频、Java 小应用、ActiveX、PDF 或 Flash）从 WebVPN 浏览器启动 ActiveX。这些应用使用 WebVPN 会话来下载和上传 ActiveX 控件。ActiveX 中继仍然有效，直到 WebVPN 会话关闭。如果您计划使用类似于 Microsoft OWA 2007 之类的工具，则应该禁用 ActiveX。

注　由于它们有相同的功能，**activex-relay enable** 命令会生成智能隧道日志，即使智能隧道已被禁用。

以下示例对与指定组策略关联的 WebVPN 会话启用 ActiveX 控件。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

以下示例对与指定用户名关联的 WebVPN 会话禁用 ActiveX 控件。

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```

ad-agent-mode

要启用 AD 代理模式以便为思科身份防火墙实例配置 Active Directory 代理，请在全局配置模式下使用 **ad-agent-mode** 命令。

ad-agent-mode

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

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** 命令可进入 aaa 服务器组配置模式。

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。并通知 ASA 更改。

配置 AD 代理服务器组的主要和辅助 AD 代理。若 ASA 检测到主 AD 代理不响应且指定了辅助代理，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，您应该为 ASA 和 AD 代理之间的共享密钥指定密钥属性。

示例

以下示例展示如何在为身份防火墙配置 Active Directory 代理时启用 **ad-agent-mode**：

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

相关命令

命令	说明
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。

address（动态过滤器黑名单或白名单）

要将 IP 地址添加到僵尸网络流量过滤器黑名单或白名单，请在动态过滤器黑名单或白名单配置模式下使用 **address** 命令。要删除地址，请使用此命令的 **no** 形式。

address *ip_address mask*

no address *ip_address mask*

语法说明

ip_address	将 IP 地址添加到黑名单。
mask	定义 IP 地址的子网掩码。*掩码*可用于单个主机或者子网。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
动态过滤器黑名单或白名单配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

静态数据库可让您使用要加入白名单或黑名单的域名或 IP 地址扩充动态数据库。进入动态过滤器白名单或黑名单配置模式后，您可以使用 **address** 和 **name** 命令，手动输入要在白名单中标记为好名称或在黑名单中标记为坏名称的域名或 IP 地址（主机或子网）。

您可以多次输入此命令以添加多个条目。最多可以添加 1000 个黑名单条目和 1000 个白名单条目。

示例

以下示例创建黑名单和白名单的条目：

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

相关命令

命令	说明
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；若配合使用 **detail** 关键字，则同时显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

address（媒体终端）

要指定媒体终端实例的地址以用于到电话代理功能的媒体连接，请在媒体终端配置模式下使用 **address** 命令。要从媒体终端配置删除地址，请使用此命令的 **no** 形式。

address *ip_address* [**interface** *intf_name*]

no address *ip_address* [**interface** *intf_name*]

语法说明

interface *intf_name*	指定使用媒体终端地址的接口名称。每个接口只能配置一个媒体终端地址。
ip_address	指定 IP 地址以用于媒体终端实例。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
媒体终端配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

ASA 必须具有符合以下条件的媒体终端的 IP 地址：

- 对于媒体终端实例，您可以为所有接口配置一个全局媒体终端地址，或者为不同的接口分别配置一个媒体终端地址。但不能同时使用全局媒体终端地址以及为每个接口配置的媒体终端地址。
- 如果为多个接口配置一个媒体终端地址，您必须在 ASA 与 IP 电话通信时使用的每个接口上配置一个地址。
- IP 地址是公开路由的地址，也是该接口的地址范围内未使用的 IP 地址。

有关创建媒体终端实例和配置媒体终端地址时必须遵守的前提条件的完整列表，请参阅 CLI 配置指南。

示例

以下示例展示使用媒体终端地址命令指定用于媒体连接的 IP 地址：

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。
media-termination	配置媒体终端实例以用于电话代理实例。

address-family ipv4

要输入地址系列以配置使用标准 IP 版本 4 (IPv4) 地址前缀的路由会话，请在路由器配置模式下使用 **address-family ipv4** 命令。要退出地址系列配置模式并从运行配置中删除 IPv4 地址系列配置，请使用此命令的 **no** 形式。

address-family ipv4

no address-family ipv4

默认值

IPv4 地址前缀未启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
路由器模式配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

address-family ipv4 命令将情景路由器置于地址系列配置模式下，在该模式下您可以配置使用标准 IPv4 地址前缀的路由会话。要退出地址系列配置模式并返回路由器配置模式，请键入 **exit**。

注　默认情况下，为使用 **neighbor remote-as** 命令配置的每个 BGP 路由会话通告地址系列 IPv4 的路由信息，除非您在配置 **neighbor remote-as** 命令之前输入 **no bgp default ipv4-unicast** 命令。

示例

以下示例将路由器置于 IPv4 地址系列的地址系列配置模式：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

相关命令

命令	说明
bgp default ipv4-unicast	将 IP 版本 4 (IPv4) 单播地址系列设置为 BGP 对等会话的默认值。
neighbor remote-as	向 BGP 或多协议 BGP 邻居表添加条目。

address-pool（隧道组常规属性模式）

要指定地址池列表以将地址分配给远程客户端，请在隧道组常规属性配置模式下使用 **address-pool** 命令。要消除地址池，请使用此命令的 **no** 形式。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

语法说明

address_pool	指定使用 **ip local pool** 命令配置的地址池的名称。您可以指定最多 6 个本地地址池。
interface name	（可选）指定要用于地址池的接口。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

可以输入这些命令中的多个，每个接口一个。如果未指定接口，则该命令指定所有未显式引用的接口的默认值。

组策略 **address-pool** 命令中的地址池设置会覆盖隧道组 **address-pool** 命令中的本地池设置。

指定这些池的顺序非常重要。ASA 以这些池在此命令中出现的顺序分配这些池中的地址。

示例

以下示例在隧道组常规配置模式中输入，它指定一个地址池列表以将地址分配给远程客户端用于 IPsec 远程访问隧道组测试：

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

相关命令

命令	说明
ip local pool	配置将用于 VPN 远程访问隧道的 IP 地址池。
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-map default-group	将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联起来。

address-pool（组策略属性配置模式）

要指定地址池列表以将地址分配给远程客户端，请在组策略属性配置模式下使用 **address-pool** 命令。要从组策略中删除属性并允许从组策略的其他来源继承，请使用此命令的 **no** 形式。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

语法说明

address_pool	指定使用 **ip local pool** 命令配置的地址池的名称。您可以指定最多 6 个本地地址池。
none	指定不配置任何地址池并禁止从其他组策略来源继承。
value	指定一个最多包含 6 个地址池的列表（将从这些地址池分配地址）。

默认值

默认情况下地址池属性允许继承。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令中的地址池设置会覆盖组中的本地池设置。您可以指定最多包含六个本地地址池的列表以用于本地地址分配。

指定这些池的顺序非常重要。ASA 以这些池在此命令中出现的顺序分配这些池中的地址。

address-pool none 命令禁止从其他策略来源（如 DefaultGrpPolicy）继承此属性。命令 **no address pools none** 从配置中删除 **address-pools none** 命令，从而恢复默认值；默认值允许继承。

示例

以下示例在配置常规配置模式中输入，它将 pool_1 和 pool_20 地址池配置为地址池列表以将地址分配给 GroupPolicy1 的远程客户端：

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

相关命令

命令	说明
ip local pool	配置将用于 VPN 组策略的 IP 地址池。
clear configure group-policy	清除所有已配置的组策略。
show running-config group-policy	显示所有组策略的配置或特定组策略的配置。

admin-context

要设置系统配置的管理情景，请在全局配置模式下使用 **admin-context** 命令。

admin-context *name*

语法说明

name	将名称设置为最多包含 32 个字符的字符串。如果尚未定义任何情景，则首先使用此命令指定管理情景名称。然后，您使用 **context** 命令添加的第一个情景必须是指定的管理情景名称。 此名称区分大小写，这样，您可以使用名称分别为 “customerA” 和 “CustomerA” 的两个情景。您可以使用字母、数字或连字符，但名称的开头或结尾不能使用连字符。 “System” 或 “Null”（采用大写或小写字母）是保留名称，不得使用。

默认值

对于多情景模式下的新 ASA，管理情景名为 “admin”。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

只要情景配置驻留在 内部闪存 上，您就可以将该情景设置为管理情景。

无法删除当前管理情景，除非您使用 **clear configure context** 命令删除所有情景。

系统配置不会为自身包括任何网络接口或网络设置；相反，当系统需要访问网络资源（例如下载 ASA 软件或允许管理员进行远程管理）时，它使用其中一个被指定为管理情景的情景。

示例

以下示例将管理情景设置为 “administrator”：

```
ciscoasa(config)# admin-context administrator
```

相关命令

命令	说明
clear configure context	从系统配置删除所有情景。
context	在系统配置中配置情景，然后进入情景配置模式。
show admin-context	显示当前管理情景名称。

aggregate-address

要在边界网关协议 (BGP) 数据库中创建聚合条目，请在地址系列配置模式下使用 **aggregate-address** 命令。要禁用此功能，请使用此命令的 **no** 形式。

aggregate-address *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*][**advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*][**advertise-map** *map-name*] [**attribute-map** *map-name*]

语法说明

address	聚合地址。
mask	聚合掩码。
as-set	（可选）生成自主系统设置路径信息。
summary-only	（可选）过滤来自更新的所有更具体的路由。
suppress-map *map-name*	（可选）指定用于选择要禁止的路由的路由映射的名称。
advertise-map *map-name*	（可选）指定用于选择用来创建 AS_SET 原始社区的路由的路由映射的名称。
attribute-map *map-name*	（可选）指定用于设置聚合路由的属性的路由映射的名称。

默认值

在使用此命令创建聚合路由时，原子聚合属性自动设置，除非指定了 **as-set** 关键字。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
情景配置、	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

您可在 BGP 和多协议 BGP (mBGP) 中实施聚合路由，方法有两种：将聚合路由重新分配到 BGP 或 mBGP 中，或者使用条件聚合路由功能。

如果在指定范围内有更具体的 BGP 或 mBGP 路由，将 **aggregate-address** 命令与 no 关键字一起使用可在 BGP 或 mBGP 路由表中创建聚合条目。（路由信息库 (RIB) 中必须存在与聚合匹配的较长前缀。）聚合路由将被通告为来自您的自主系统，并会设置原子路由属性以显示可能缺失的信息。（默认情况下，设置原子聚合属性，除非您指定了 **as-set** 关键字。）

使用 **as-set** 关键字会按照该命令在无此关键字时的规则创建一个聚合条目，但为此路由通告的路径将是一个 AS_SET，其中包含正在进行摘要处理的所有路径中的所有元素。在聚合多条路径时，请勿使用 **aggregate-address** 命令的此形式，因为随着摘要路由的自主系统路径抵达能力信息的变化，必须不断提取和更新此路由。

使用 **summary-only** 关键字不仅会创建聚合路由（例如 192.*.*.*），而且会抑制将更具体的路由通告到所有邻居。如果希望仅抑制到特定邻居的通告，则可以谨慎使用 **neighbor distribute-list** 命令。如果获知更具体的路由泄漏，则所有 BGP 或 mBGP 路由器会选择该路由而不是您正在生成的不太具体的路由（使用最长匹配路由）。

使用 **suppress-map** 关键字可创建聚合路由，但会抑制指定路由的通告。可以使用路由映射的 **match** 子句来选择性地抑制一些更具体的路由，让其他路由保留非抑制状态。支持 IP 访问列表和自主系统路径访问列表 match 子句。

使用 **advertise-map** 关键字可选择将用于构建聚合路由的不同组件，例如 AS_SET 或社区。若聚合的组件位于各单独的自主系统中且您希望使用 AS_SET 创建聚合，然后将它通告给其中某些自主系统，则 **aggregate-address** 命令的此形式很有用。必须牢记从 AS_SET 中省去特定自主系统编号，以防止接收路由器处的 BGP 环路检测机制丢弃聚合。支持 IP 访问列表和自主系统路径访问列表 **match** 子句。

使用 **attribute-map** 关键字可允许对聚合路由的属性进行更改。若构成 AS_SET 的路由之一配置了某个属性（如 community no-export，该属性可防止导出聚合路由），则 **aggregate-address** 命令的此形式很有用。可以创建属性映射路由映射以更改聚合属性。

示例

以下示例创建一个聚合路由并抑制将更具体的路由通告到所有邻居。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式以配置使用标准 IP 版本 4 的路由会话。

allocate-interface

要将接口分配到安全情景，请在情景配置模式下使用 **allocate-interface** 命令。要从情景删除接口，请使用此命令的 **no** 形式。

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

语法说明

invisible	（默认）使情景用户通过 **show interface** 命令只能看到映射名称（如果已配置）。

map_name	（可选）设置映射名称。
	map_name 是可在情景中使用的接口的字母数字别名，而不是接口 ID。如果您没有指定映射名称，则在情景中使用接口 ID。出于安全性考虑，您可能不希望情景管理员知道情景正在使用哪些接口。
	映射名称必须以字母开头，以字母或数字结尾，并且内部字符只能是字母、数字或下划线。例如，可以使用以下名称：
	`int0`
	`inta`
	`int_0`
	对于子接口，您可以指定映射名称的范围。
	有关范围的详细信息，请参阅 “ 使用指南 ” 部分。

physical_interface	设置接口 ID，例如 **gigabit ethernet0/1**。请参阅**接口**命令可接受的值。不要在接口类型和端口号之间包含空格。
subinterface	设置子接口号。您可以标识子接口的范围。
visible	（可选）允许情景用户通过 **show interface** 命令查看物理接口属性，即使您已经设置了映射名称。

默认值

如果您设置了映射名称，则默认情况下，接口 ID 在 **show interface** 命令**输**出中是不可见的。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Context configuration	• 是	• 是	—	—	•

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以多次输入此命令以指定不同的范围。要更改映射名称或可见设置，请为给定接口 ID 重新输入命令，并设置新值；您不需要输入 **no allocate-interface** 命令来从头开始。如果您删除 **allocate-interface** 命令，则 ASA 会删除情景中的所有接口相关配置。

透明防火墙模式只允许两个接口通过流量；但是，在 ASA 上，您可以使用专用管理接口 Management 0/0（物理接口或子接口）作为管理流量的第三个接口。

注　当数据包不在 MAC 地址表中时，透明模式的管理接口不会将数据包以泛洪方式发送到接口之外。

必要时，您可以在路由模式下将上述接口分配给多个情景。透明模式不允许共享接口。

如果指定子接口的范围，可以指定匹配的映射名称的范围。关于范围，请遵循以下原则：

- 映射名称必须由后跟数字部分的字母部分组成。映射名称的字母部分必须与范围的两端匹配。例如，输入以下范围：

  int0-int10

  例如，如果您输入 **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**，则命令失败。

- 映射名称的数字部分包含的编号的数量必须与子接口范围的编号的数量相同。例如，两个范围都包括 100 个接口。

  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100

  例如，如果您输入 **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**，则命令失败。

示例

以下示例展示将 gigabitethernet0/1.100、gigabitethernet0/1.200 以及 gigabitethernet0/2.300 到 gigabitethernet0/1.305 分配给情景。映射名称为 int1 到 int8。

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

相关命令

命令	说明
context	在系统配置中创建安全情景并进入情景配置模式。
interface	配置接口并进入接口配置模式。
show context	显示情景列表（系统执行空间）或有关当前情景的信息。
show interface	显示接口的运行时状态和统计信息。
vlan	将 VLAN ID 分配给子接口。

allocate-ips

如果您已安装 AIP SSM，要将 IPS 虚拟传感器分配到安全情景，请在情景配置模式下使用 **allocate-ips** 命令。要从情景删除虚拟传感器，请使用此命令的 **no** 形式。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

语法说明

default	（可选）为每个情景设置一个传感器作为默认传感器；如果情景配置没有指定传感器名称，则情景使用此默认传感器。您只能为每个情景配置一个默认传感器。如果要更改默认传感器，在分配新的默认传感器之前，请输入 **no allocate-ips** 命令以删除当前默认传感器。如果不指定默认传感器且情景配置不包括传感器名称，则流量使用 AIP SSM 上的默认传感器。
mapped_name	（可选）设置一个映射命名而不是实际传感器名称，作为可在情景中使用的传感器的别名。如果您没有指定映射名称，则在情景中使用传感器名称。出于安全性考虑，您可能不希望情景管理员知道情景正在使用哪些传感器。或者您可能希望将情景配置通用化。例如，如果您希望所有情景都使用名为 “sensor1” 和 “sensor2” 的传感器，则可将 “highsec” 和 “lowsec” 传感器映射到情景 A 中的 sensor1 和 sensor2，而将 “medsec” 和 “lowsec” 传感器映射到情景 B 中的 sensor1 和 sensor2。
sensor_name	设置在 AIP SSM 上配置的传感器名称。要查看在 AIP SSM 上配置的传感器，请输入 **allocate-ips ?**。列出所有可用的传感器。您还可以输入 **show ips** 命令。在系统执行空间中，**show ips** 命令列出所有可用的传感器；如果您在情景中输入此命令，它会显示您已分配给情景的传感器。如果指定在 AIP SSM 上不存在的传感器名称，则会出现错误提示，但是 **allocate-ips** 命令会原样输入。情景会认为传感器已经关闭，直到您在 AIP SSM 上创建了一个具有该名称的传感器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Context configuration	• 是	• 是	—	—	•

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

您可以将一个或多个 IPS 虚拟传感器分配到每个情景。然后，在使用 **ips** 命令配置情景以将流量发送给 AIP SSM 时，您可以指定一个分配给情景的传感器；您不能指定未分配给情景的传感器。如果不将任何传感器分配给情景，则使用 AIP SSM 上配置的默认传感器。您可以将同一个传感器分配给多个情景。

注　您不需要为使用虚拟传感器而进入多情景模式；您可以在单一模式下为不同的流量流使用不同的传感器。

示例

以下示例将 sensor1 和 sensor2 分配给情景 A，将 sensor1 和 sensor3 分配给情景 B。这两个情景将传感器名称映射到 “ips1” 和 “ips2”。在情景 A 中，sensor1 被设置为默认传感器，但在情景 B 中没有设置默认传感器，因此使用在 AIP SSM 上配置的默认值。

```
ciscoasa(config-ctx)# context A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

相关命令

命令	说明
context	在系统配置中创建安全情景并进入情景配置模式。
ips	将流量转到 AIP SSM 以供检查。
show context	显示情景列表（系统执行空间）或有关当前情景的信息。
show ips	显示在 AIP SSM 上配置的虚拟传感器。

allow-ssc-mgmt

要将 ASA 5505 上的接口设置为 SSC 管理接口，请在接口配置模式下使用 **allow-ssc-mgmt** 命令。要取消分配接口，使用此命令的 **no** 形式。

allow-ssc-mgmt

no allow-ssc-mgmt

语法说明

此命令没有任何参数或关键字。

命令默认值

此命令在 VLAN 1 的出厂默认配置中已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.2(1)	我们引入了此命令。

使用指南

SSC 没有任何外部接口。您可以将 VLAN 配置为管理 VLAN 以允许通过背板访问内部管理 IP 地址。默认情况下，已为 SSC 管理地址启用 VLAN 1。您只能分配一个 VLAN 作为 SSC 管理 VLAN。

如果您打算使用 ASDM 来访问管理地址，请不要为管理地址配置 NAT。对于带有 ASDM 的初始设置，您需要访问实际地址。在初始设置后（您通过初始设置在 SSC 中设置密码），您可以在要访问 SSC 时配置 NAT 并为 ASDM 提供转换后的地址。

示例

以下示例在 VLAN 1 上禁用管理访问，并为 VLAN 2 启用管理访问：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

相关命令

命令	说明
interface	配置一个接口。
ip address	设置一个桥组的管理 IP 地址。
nameif	设置接口名称。

命令	说明
security-level	设置接口安全级别。
hw-module module ip	配置 SSC 的管理 IP 地址。
hw-module module allow-ip	设置获准访问管理 IP 地址的主机。

always-on-vpn

要配置 AnyConnect Always-On-VPN 的行为，请在组策略配置模式下使用 **always-on-vpn** 命令。

always-on-vpn [**profile-setting** | **disable**]

语法说明

disable	关闭 Always-On-VPN 功能。
profile-setting	使用在 AnyConnect 配置文件中配置的 **always-on-vpn** 设置。

命令默认值

默认情况下关闭 Always-On-VPN 功能。

命令历史

版本	修改
8.3(1)	我们引入了此命令。

使用指南

要为 AnyConnect 用户启用 Always-On-VPN 功能，请在配置文件编辑器中配置 AnyConnect 配置文件。然后配置相应策略的组策略属性。

示例

以下示例在 VLAN 1 上禁用管理访问，并为 VLAN 2 启用管理访问：

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

相关命令

命令	说明
webvpn	为 WebVPN 配置组策略。

anyconnect ask

要启用 ASA 以提示远程 SSL VPN 客户端用户下载客户端，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect ask** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

anyconnect ask {none | enable [default {webvpn | anyconnect} timeout *value*]}

no anyconnect ask none [default {webvpn | anyconnect}]

语法说明

default anyconnect timeout *value*	提示远程用户下载客户端，或转到无客户端连接的门户页面，并在采取默认操作（下载客户端）之前等待 *value* 时间。
default webvpn timeout *value*	提示远程用户下载客户端，或转到无客户端连接的门户页面，并在采取默认操作（显示 WebVPN 门户页面）之前等待 *value* 时间。
enable	提示远程用户下载客户端，或转到无客户端连接的门户页面，并无限期等待用户响应。
none	立即执行默认操作。

默认值

此命令的默认值是 **anyconnect ask none default webvpn**。ASA 立即显示无客户端连接的门户页面。

命令模式

下表展示可输入此命令的模式：

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

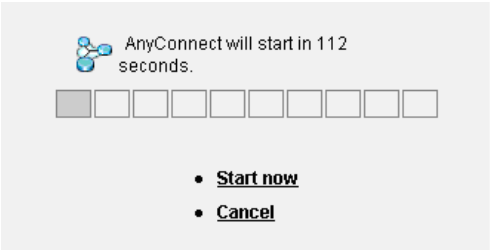
命令历史

版本	**修改**
8.0(2)	引入了此命令。
8.4(1)	**anyconnect ask** 命令取代了 **svc ask** 命令。

使用指南

图 2-1 显示当已配置 **default anyconnect timeout** *value* 命令 或 **default webvpn timeout** *value* 命令命令时向远程用户显示的提示：

图 2-1　向远程用户显示提示，提示其下载 SSL VPN 客户端



示例

以下示例配置 ASA 以提示远程用户下载客户端或转到门户页面，并在下载客户端之前等待 10 秒以便用户响应。

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

相关命令

命令	说明
show webvpn anyconnect	显示关于已安装 SSL VPN 客户端的信息。
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect image	指定 ASA 在缓存内存中扩展用于下载到远程 PC 的客户端软件包文件。

anyconnect df-bit-ignore

要忽略需要分段的数据包中的 DF 位，请在组策略 webvpn 配置模式下使用 **anyconnect-df-bit-ignore** 命令。要确认需要分段的 DF 位，请使用此命令的 **no** 形式。

anyconnect df-bit-ignore {enable | none}

no anyconnect df-bit-ignore {enable | none}

语法说明

enable	启用 AnyConnect 客户端的 DF 位忽略。
none	禁用 AnyConnect 客户端的 DF 位。

默认值

默认情况下不启用此选项。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了 **svc df-bit-ignore** 命令。
8.4(3)	**anyconnect df-bit-ignore** 命令取代了 **svc df-bit-ignore** 命令。

示例

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?

config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

要对 ASA 启用失效对等检测 (DPD) 并设置远程客户端或 ASA 对 SSL VPN 连接执行 DPD 的频率，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect dpd-interval** 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。

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

语法说明

client none	禁用客户端执行的 DPD。
client *seconds*	指定客户端执行 DPD 的频率，从 30 秒到 3600 秒。
gateway none	禁用 ASA 执行的 DPD。
gateway *seconds*	指定 ASA 执行 DPD 的频率，从 30 秒到 3600 秒。

默认值

默认情况下，DPD 被启用并对 ASA（网关）和客户端都将其设置为 30 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
7.1(1)	引入了此命令。
8.0(3)	默认设置从禁用更改为对 ASA（网关）和客户端都配置为 30 秒。
8.4(1)	**anyconnect dpd-interval** 命令取代了 **svc dpd-interval** 命令。

示例

以下示例展示如何为现有组策略 *sales* 将 ASA（网关）执行 DPD 的频率配置为 3000 秒，将客户端执行 DPD 的频率配置为 1000 秒：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

要在低带宽链路上为特定组或用户启用压缩，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect dtls compression** 命令。要从组中删除配置，请使用此命令的 **no** 形式。

anyconnect dtls compression {lzs | none}

no anyconnect dtls compression {lzs | none}

语法说明

lzs	启用无状态压缩算法。
none	禁用压缩。

默认值

默认情况下不启用 AnyConnect 压缩。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了 **anyconnect dtls compression** 命令。

示例

以下示例展示用于禁用压缩的序列：

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

要启用 ASA 以将 AnyConnect 客户端下载到远程计算机或连接到使用 AnyConnect 客户端的 ASA（通过 SSL 或 IKEv2），请在 webvpn 配置模式下使用 **anyconnect enable** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

anyconnect enable

no anyconnect enable

默认值

此命令的默认设置为禁用。ASA 不下载客户端。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	此命令作为 **svc enable** 引入。
8.4(1)	**anyconnect enable** 命令取代了 **svc enable** 命令。

使用指南

输入 **no anyconnect enable** 命令不会终止活动会话。

在使用 **anyconnect image xyz** 命令配置 AnyConnect 映像后，必须发出 **anyconnect enable** 命令。要使用 AnyConnect 客户端或 AnyConnect weblaunch，需要 **anyconnect enable**。如果 **anyconnect enable** 命令没有与 SSL 或 IKEv2 一起发出，则 AnyConnect 不按照预想的方式工作，而是会发生超时并出现 IPsec VPN 连接终止错误。结果，**show webvpn svc** 命令不会考虑要启用的 SSL VPN 客户端，也不列出已安装的 AnyConnect 软件包。

示例

以下示例展示如何启用 ASA 来下载客户端：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

相关命令

命令	说明
anyconnect image	指定 ASA 在缓存内存中扩展以用于下载到远程 PC 的 AnyConnect SSL VPN 客户端软件包文件。
anyconnect modules	指定 AnyConnect SSL VPN 客户端为可选功能要求的模块的名称。
anyconnect profiles	指定用来存储 ASA 下载到 Cisco AnyConnect SSL VPN 客户端的配置文件的文件的名称。
show webvpn anyconnect	显示关于在 ASA 上安装并加载到缓存内存以供下载到远程 PC 的 SSL VPN 客户端的信息。
anyconnect localization	指定用于存储下载到 Cisco AnyConnect VPN 客户端的本地化文件的软件包文件。

anyconnect firewall-rule

要建立公共 ACL 防火墙或提供 ACL 防火墙，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect firewall-rule** 命令。

anyconnect firewall-rule client interface {public | private} *ACL*

语法说明

ACL	指定访问控制列表
client interface	指定客户端接口
private	配置专用接口规则
public	配置公共接口规则

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
8.3(1)	引入了此命令。
8.4(1)	**anyconnect firewall-rule** 命令取代了 **svc firewall-rule** 命令。
9.0(1)	现在，命令中的 ACL 可以是用于指定 IPv4 和 IPv6 地址的统一访问控制规则。

使用指南

要按预期正常工作，此命令需要的版本为 AsyncOS for Web 版本 7.0，该版本为 AnyConnect 安全移动客户端提供 AnyConnect 安全移动许可支持。它还需要支持 AnyConnect 安全移动、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

以下说明阐明了 AnyConnect 客户端如何使用防火墙：

- 源 IP 不能用于防火墙规则。客户端将忽视防火墙规则中从 ASA 发送来的源 IP 信息。客户端将根据规则是公共还是私有来确定源 IP。公共规则适用于客户端上的所有接口。将专用规则应用到虚拟适配器。
- ASA 支持 ACL 规则的很多协议。但是，AnyConnect 防火墙功能仅支持 TCP、UDP、ICMP 和 IP。如果客户端收到一条具有不同协议的规则，它会将它视为无效的防火墙规则，然后禁用拆分隧道并出于安全考虑使用完整隧道。

请注意每个操作系统的以下行为差异：

- 对于 Windows 计算机，拒绝规则在 Windows 防火墙中优先于允许规则。如果 ASA 将一条允许规则下推到 AnyConnect 客户端，但用户创建了一条自定义拒绝规则，则不会实施 AnyConnect 规则。
- 在 Windows Vista 中，在创建防火墙规则时，Vista 获取采用逗号分隔字符串形式的端口号范围（例如 1-300 或者 5000-5300）。允许的最大端口数量是 300。如果您指定的数量大于 300 个端口，则防火墙规则仅应用于前 300 个端口。
- 防火墙服务必须由 AnyConnect 客户端启动（不能由系统自动启动）的 Windows 用户在建立 VPN 连接时所花的时间可能会显著增加。
- 在 Mac 计算机上，AnyConnect 客户端以 ASA 应用规则的顺序来依次应用规则。全局规则始终都在最后。
- 对于第三方防火墙，只有当 AnyConnect 客户端防火墙和第三方防火墙都允许该流量类型时才能通过流量。如果第三方防火墙阻止 AnyConnect 客户端允许的指定流量类型，则客户端会阻止该流量。

有关 AnyConnect 客户端防火墙的详细信息（包括用于本地打印和关联设备支持的 ACL 规则示例），请参阅 *AnyConnect 管理员指南*。

示例

以下示例启用 ACL *AnyConnect_Client_Local_Print* 作为公共防火墙：

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

相关命令

命令	说明
show webvpn anyconnect	显示关于已安装 SSL VPN 客户端的信息。
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect image	指定 ASA 在缓存内存中扩展用于下载到远程 PC 的客户端软件包文件。

anyconnect image

要安装或升级 AnyConnect 分发软件包并将其添加到运行配置中，请在 webvpn 配置模式下使用 **anyconnect image** 命令。要从运行配置删除 AnyConnect 分发软件包，请使用此命令的 **no** 形式。

anyconnect image *path order* [**regex** *expression*]

no anyconnect image *path order* [**regex** *expression*]

语法说明

order	对于多个客户端软件包文件，指定软件包文件的顺序，从 1 到 65535。ASA 按照您指定的顺序将每个客户端的各个部分下载到远程 PC，直至它实现与操作系统的匹配。
path	指定 AnyConnect 软件包的路径和文件名，最多为 255 个字符。
regex *expression*	指定 ASA 用来匹配浏览器传递的用户代理字符串的字符串。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	此命令作为 **svc image** 引入。
8.0(1)	添加了 **regex** 关键字。
8.4(1)	**anyconnect image** 命令取代了 **svc image** 命令。

使用指南

为软件包文件编号可建立 ASA 将它们下载到远程 PC 的顺序，直到实现与操作系统的匹配。它首先下载具有最小编号的软件包文件。因此，您应将最小编号分配给与在远程 PC 上最常用操作系统相匹配的软件包文件。

默认 order 为 1。如果您没有指定 *order* 参数，则您每次输入 **svc image** 命令时，都会覆盖之前被视为编号 1 的映像。

您还可以按任何顺序为每个客户端软件包文件输入 **anyconnect image** 命令。例如，您可以在输入 **anyconnect image** 命令指定要第一个下载的软件包文件 (*order* 1) 之前指定要第二个下载的软件包文件 (*order* 2)。

对于移动用户，您可以通过使用 **regex** 关键字来缩短移动设备的连接时间。当浏览器连接到 ASA 时，它在 HTTP 报头中包含用户代理字符串。在 ASA 收到该字符串后，如果字符串与为映像配置的表达式匹配，它会立即下载该映像，而不测试其他客户端映像。

注　在使用独立客户端时，忽略 **regex** 命令。它仅用于网络浏览器以实现性能改进，regex 字符串不匹配由独立客户端提供的任何用户或代理。

ASA 扩展缓存内存中的 AnyConnect 客户端和思科安全桌面 (CSD) 软件包文件。为使 ASA 成功扩展软件包文件，必须有足够的缓存内存来存储软件包文件的映像和文件。

如果 ASA 检测到没有足够的缓存内存来扩展软件包，则会向控制台显示一条错误消息。以下示例展示在尝试使用 **svc image** 命令安装软件包文件后报告的错误消息：

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

如果在您尝试安装软件包文件时发生这种情况，请在全局配置模式下使用 **dir cache:/** 命令检查剩余缓存内存和之前安装的软件包的大小。

注　如果您的 ASA 只有默认内部闪存大小或默认 DRAM 大小（对于缓存内存），则您可能无法在 ASA 上存储和加载多个 AnyConnect 客户端软件包。即使闪存足以容纳软件包文件，ASA 在解压和加载客户端映像时也可能会耗尽缓存内存。有关部署 ASA 时的 AnyConnect 内存要求以及可能升级 ASA 内存的更多信息，请参阅思科 ASA 5500 系列的最新版本说明。

示例

以下示例按照相应顺序为 Windows、MAC 和 Linux 加载 AnyConnect 客户端软件包文件：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

以下是 **show webvpn anyconnect** 命令的示例输出，其中展示加载的 AnyConnect 客户端软件包及其顺序：

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25

2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010

3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010

3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
anyconnect modules	指定 AnyConnect SSL VPN 客户端为可选功能要求的模块的名称。
anyconnect profiles	指定用来存储 ASA 下载到 Cisco AnyConnect SSL VPN 客户端的配置文件的文件的名称。
show webvpn anyconnect	显示关于在 ASA 上安装并加载到缓存内存以供下载到远程 PC 的 SSL VPN 客户端的信息。
anyconnect localization	指定用于存储下载到 Cisco AnyConnect VPN 客户端的本地化文件的软件包文件。

anyconnect keep-installer

注　此命令不适用于 AnyConnect 2.5 之后的版本，但是，为保持向后兼容性，仍提供了此命令。配置 **anyconnect keep-installer** 命令不会影响 AnyConnect 3.0 或更高版本。

要支持在远程 PC 上永久安装 SSL VPN 客户端，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect keep-installer** 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。

anyconnect keep-installer {**installed** | **none**}

no anyconnect keep-installer {**installed** | **none**}

语法说明

installed	禁用客户端的自动卸载功能。客户端仍然安装在远程 PC 上以供将来连接。
none	指定在活动连接终止后从远程计算机卸载客户端。

默认值

默认情况下启用客户端的永久安装。客户端在会话结束时仍在远程计算机上。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
7.1(1)	引入了此命令。
8.4(1)	**anyconnect keep-installer** 命令取代了 **svc keep-installer** 命令。

示例

在以下示例中，用户进入组策略 webvpn 配置模式并配置组策略，以在会话结束时删除客户端：

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

相关命令

命令	说明
show webvpn anyconnect	显示关于安装到 ASA 上并加载到缓存内存中以供下载到远程 PC 的 AnyConnect 客户端的信息。
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect enable	启用 ASA 以将 AnyConnect 客户端文件下载到远程 PC。
anyconnect image	指定 ASA 在缓存内存中扩展以供下载到远程 PC 中的 AnyConnect 客户端软件包文件。

anyconnect modules

要指定 AnyConnect SSL VPN 客户端为可选功能而要求的模块的名称，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect modules** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

anyconnect modules {**none** | **value** *string*}

no anyconnect modules {**none** | **value** *string*}

语法说明

string	可选模块的名称，名称最多可包含 256 个字符。使用逗号分隔多个字符串。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	此命令作为 **svc modules** 引入。
8.4(1)	**anyconnect modules** 命令取代了 **svc modules** 命令。

使用指南

为了尽量缩短下载时间，客户端只请求下载（从 ASA 下载）为支持的每个功能所需的模块。**anyconnect modules** 命令支持 ASA 下载这些模块。

下表展示了代表 AnyConnect 模块的字符串值。

代表 AnyConnect 模块的字符串	AnyConnect 模块名称
dart	AnyConnect DART（诊断和报告工具）
nam	AnyConnect 网络访问管理器
vpngina	AnyConnect SBL（登录前启动）
websecurity	AnyConnect 网络安全模块
telemetry	AnyConnect 遥测模块
posture	AnyConnect Posture 模块
none	如果您选择 **none**，则 ASA 下载不带可选模块的基本文件。现有模块将从组策略中删除。

示例

在以下示例中，用户进入组策略 *PostureModuleGroup* 的组策略属性模式和 webvpn 配置模式，指定字符串 *posture* 和 *telemetry*，以便在终端连接到 ASA 时将 AnyConnect Posture 模块和 AnyConnect Telemetry 模块下载到终端。

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry
ciscoasa(config-group-webvpn)# write mem
Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69

22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

要从组策略中删除模块，请重新发送此命令且只指定您要保留的模块值。例如，以下命令删除遥测模块：

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

相关命令

命令	说明
show webvpn anyconnect	显示关于加载到 ASA 上的缓存内存并可供下载的 AnyConnect 软件包的信息。
anyconnect enable	为特定组或用户启用 AnyConnect 客户端。
anyconnect image	指定 ASA 在缓存内存中扩展以供下载到远程 PC 中的 AnyConnect 客户端软件包文件。

anyconnect mtu

要调整由 Cisco AnyConnect VPN 客户端建立的 SSL VPN 连接的 MTU 大小，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect mtu** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

anyconnect mtu *size*

no anyconnect mtu *size*

语法说明

size	MTU 大小以字节为单位，从 256 字节到 1406 字节。

默认值

默认大小为 1406 字节。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.4(1)	**anyconnect mtu** 命令取代了 **svc mtu** 命令。

使用指南

此命令仅影响 AnyConnect 客户端。思科 SSL VPN 客户端无法调整为不同的 MTU 大小。

在默认组策略中此命令的默认值为 **no svc mtu**。根据连接所使用界面的 MTU，减去 IP/UDP/DTLS 开销，MTU 大小会自动调整。

此命令影响在纯 SSL 中建立的 AnyConnect 客户端连接以及在使用 DTLS 的 SSL 中建立的 AnyConnect 客户端连接。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密的成本，MTU 值应设置为不低于 1380。将接口设置为低于 1380 字节可能会导致丢包。

示例

以下示例为组策略 *telecommuters* 将 MTU 大小配置为 500 字节：

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

相关命令

命令	说明
anyconnect keep-installer	禁用客户端的自动卸载功能。初始下载后，客户端在连接终止后仍保留在远程 PC 上。
anyconnect ssl dtls	启用 DTLS 以支持 CVC 建立 SSL VPN 连接。
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。

anyconnect profiles（组策略或用户名属性）

要指定下载到 Cisco AnyConnect VPN 客户端 (CVC) 用户的 CVC 配置文件包，请在组策略 webvpn 或用户名属性 webvpn 配置模式下使用 **anyconnect profiles** 命令。要从配置中删除命令并使值得到继承，请使用此命令的 **no** 形式。

anyconnect profiles {**value** *profile* | **none**}

no anyconnect profiles {**value** *profile* | **none** } [**type** *type*]

语法说明

value *profile*	配置文件的名称。
none	ASA 不下载配置文件。
type *type*	对应于标准 AnyConnect 配置文件或任何字母数字值的用户。

默认值

默认值为 none。ASA 不下载配置文件。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
8.0(2)	引入了此命令。
8.3(1)	引入了可选类型 **value**。
8.4(1)	**anyconnect profiles** 命令取代了 **svc profiles** 命令。

使用指南

此命令在组策略 webvpn 或用户名属性 webvpn 配置模式下输入，支持 ASA 基于组策略或用户名将配置文件下载到 CVC 用户。要将 CVC 配置文件下载到所有 CVC 用户，请在 webvpn 配置模式下使用此命令。

CVC 配置文件是 CVC 用来配置在 CVC 用户界面中出现的连接条目的一组配置参数，包括主机的名称和地址。您可以使用 CVC 用户界面创建和保存配置文件。您也可以使用文本编辑器编辑此文件并设置无法通过用户界面访问的高级参数。

CVC 安装包含一个配置文件模板 (cvcprofile.xml)，您可以编辑并使用此模板来作为创建其他配置文件的基础。有关编辑 CVC 配置文件的详细信息，请参阅 *Cisco AnyConnect VPN 客户端管理员指南*。

示例

在以下示例中，用户输入 **anyconnect profiles value** 命令，以显示可用的配置文件：

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineerin
  sales
```

然后用户配置组策略以使用 CVC 配置文件 sales：

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

相关命令

命令	说明
show webvpn anyconnect	显示关于安装的 AnyConnect 客户端的信息。
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect image	指定 ASA 在缓存内存中扩展以供下载到远程 PC 中的 AnyConnect 客户端软件包文件。

anyconnect profiles (webvpn)

要指定一个文件作为 ASA 在缓存内存中加载的配置文件包并使其可供 Cisco AnyConnect VPN 客户端 (CVC) 用户的组策略和用户名属性使用，请在 webvpn 配置模式下使用 **anyconnect profiles** 命令。要从配置中删除命令并使 ASA 从缓存内存卸载软件包文件，请使用此命令的 **no** 形式。

anyconnect profiles {*profile path*}

no anyconnect profiles {*profile path*}

语法说明

path	ASA 的闪存中的配置文件的路径和文件名。
profile	要在缓存内存中创建的配置文件的名称。

默认值

默认值为 none。ASA 不将配置文件包加载到缓存内存中。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.4(1)	**anyconnect profiles** 命令取代了 **svc profiles** 命令。

使用指南

CVC 配置文件是 CVC 用来配置在 CVC 用户界面中出现的连接条目的一组配置参数，包括主机的名称和地址。您可以使用 CVC 用户界面创建和保存配置文件。

您也可以使用文本编辑器编辑此文件并设置无法通过用户界面访问的高级参数。CVC 安装包含一个配置文件模板 (cvcprofile.xml)，您可以编辑并使用此模板来作为创建其他配置文件的基础。有关编辑 CVC 配置文件的详细信息，请参阅 *Cisco AnyConnect VPN 客户端管理员指南*。

在创建新的 CVC 配置文件并将其上传到闪存后，请在 webvpn 配置模式下使用 **anyconnect profiles** 命令，向 ASA 将 XML 文件标识为配置文件。在您输入此命令后，文件将加载到 ASA 上的缓存内存中。然后，您可以在组策略 webvpn 配置或用户名属性配置模式下使用 **anyconnect profiles** 命令为组或用户指定配置文件。

示例

在以下示例中，用户以前基于 CVC 安装中提供的 cvcprofile.xml 文件创建了两个新配置文件（sales_hosts.xml 和 engineering_hosts.xml），并将它们上传到了 ASA 上的闪存中。

然后用户向 ASA 将这些文件标识为 CVC 配置文件，指定名称为 *sales* 和 *engineering*：

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

输入 **dir cache:stc/profiles** 命令会展示已上传到缓存内存中的配置文件：

```
ciscoasa(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

在组策略 webvpn 配置或用户名属性配置模式下，这些配置文件可供 **svc profiles** 命令使用：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

相关命令

命令	说明
show webvpn anyconnect	显示关于安装的 AnyConnect 客户端的信息。
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect image	指定 ASA 在缓存内存中扩展以供下载到远程 PC 的 AnyConnect 软件包文件。

anyconnect ssl compression

要为特定组或用户对 SSL VPN 连接上的 http 数据启用压缩，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect ssl compression** 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。

anyconnect ssl compression {**deflate** | **lzs** | **none**}

no anyconnect ssl compression {**deflate** | **lzs** | **none**}

语法说明

deflate	启用 deflate 压缩算法。
lzs	启用无状态压缩算法。
none	禁用压缩。

默认值

默认情况下，压缩设置为 none（禁用）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(2)	引入了 **anyconnect compression** 命令。

使用指南

对于 SSL VPN 连接，在 webvpn 配置模式下配置的 **compression** 命令会覆盖在组策略和用户名 webvpn 模式下配置的 **anyconnect ssl compression** 命令。

示例

在以下示例中，为组策略 sales 禁用 SVC 压缩：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

相关命令

命令	说明
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect keepalive	指定远程计算机的客户端通过 SSL VPN 连接将 keepalive 消息发送到 ASA 的频率。
anyconnect keep-installer	禁用客户端的自动卸载功能。客户端仍然安装在远程 PC 上以供将来连接。
anyconnect rekey	支持客户端对 SSL VPN 连接执行密钥更新。
compression	为所有 SSL、WebVPN 和 IPsec VPN 连接启用压缩。
show webvpn anyconnect	显示关于已安装 SSL VPN 客户端的信息。

anyconnect ssl df-bit-ignore

要为特定组或用户对 SSL VPN 连接上的数据包启用强制性分段（允许它们通过隧道），请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect ssl df-bit-ignore** 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。

anyconnect ssl df-bit-ignore {enable | disable}

no anyconnect ssl df-bit-ignore

语法说明

enable	为使用 SSL 的 AnyConnect 启用 DF 位忽略。
disable	为使用 SSL 的 AnyConnect 禁用 DF 位忽略。

默认值

DF 位忽略设置为*禁用*。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	**anyconnect ssl df-bit-ignore** 形式的命令取代了 **svc df-bit-ignore**。

使用指南

此功能允许已设置 DF 位的数据包进行强制分段，以使数据包通过隧道。示例用例适用于您网络中没有对 TCP MSS 协商作出正确响应的服务器。

示例

在以下示例中，为组策略 sales 启用 DF 位忽略：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

相关命令

命令	说明
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect keepalive	指定远程计算机的客户端通过 SSL VPN 连接将 keepalive 消息发送到 ASA 的频率。
anyconnect keep-installer	禁用客户端的自动卸载功能。客户端仍然安装在远程 PC 上以供将来连接。
anyconnect rekey	支持客户端对 SSL VPN 连接执行密钥更新。

anyconnect ssl dtls enable

要在接口上为与 Cisco AnyConnect VPN 客户端建立 SSL VPN 连接的特定组或用户启用数据报传输层安全 (DTLS) 连接，请在组策略 webvpn 或用户名属性 webvpn 配置模式下使用 **anyconnect ssl dtls enable** 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。

anyconnect ssl dtls enable *interface*

no anyconnect ssl dtls enable *interface*

语法说明

interface	接口的名称。

默认值

默认设置为启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。
8.4(1)	**anyconnect ssl dtls** 命令取代了 **svc dtls** 命令。

使用指南

启用 DTLS 使得建立 SSL VPN 连接的 AnyConnect 客户端可使用两个并发隧道 - 一个 SSL 隧道和一个 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。

如果不启用 DTLS，则建立 SSL VPN 连接的 AnyConnect 客户端用户仅使用 SSL 隧道进行连接。

此命令为特定组或用户启用 DTLS。要为所有 AnyConnect 客户端用户启用 DTLS，请在 webvpn 配置模式下使用 **anyconnect ssl dtls enable** 命令。

示例

以下示例进入组策略 *sales* 的 webvpn 配置模式并启用 DTLS：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

相关命令

命令	说明
dtls port	指定 DTLS 的 UDP 端口。
anyconnect dtls	为建立 SSL VPN 连接的组或用户启用 DTLS。
vpn-tunnel-protocol	指定 ASA 允许用于远程访问（包括 SSL）的 VPN 协议。

anyconnect ssl keepalive

要配置远程客户端通过 SSL VPN 连接向 ASA 发送 keepalive 消息的频率，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect ssl keepalive** 命令。使用此命令的 **no** 形式可从配置中删除命令并使值得到继承。

anyconnect ssl keepalive {**none** | *seconds*}

no anyconnect ssl keepalive {**none** | *seconds*}

语法说明

none	禁用 keepalive 消息。
seconds	启用 keepalive 消息并指定消息的频率，从 15 秒到 600 秒。

默认值

默认值为 20 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。
8.0(3)	默认设置从禁用改为 20 秒。
8.4(1)	**anyconnect ssl keepalive** 命令取代了 **svc keepalive** 命令。

使用指南

思科 SSL VPN 客户端 (SVC) 和 Cisco AnyConnect VPN 客户端都可在建立到 ASA 的 SSL VPN 连接时发送 keepalive 消息。

您可以指定 keepalive 消息的频率（以*秒*为单位），以确保通过代理、防火墙或 NAT 设备的 SSL VPN 连接保持畅通，即使设备限制了连接可以保持空闲状态的时间。

调整频率还可以确保客户端在远程用户没有主动运行基于套接字的应用（如 Microsoft Outlook 或 Microsoft Internet Explorer）时不会断开并重新连接。

注　默认情况下启用 keepalive。如果禁用 keepalive，则一旦发生故障切换事件，SSL VPN 客户端会话就无法转到备用设备。

示例

在以下示例中，用户将 ASA 配置为使客户端为名为 *sales* 的现有组策略发送 keepalive 消息，频率为 300 秒（5 分钟）：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

相关命令

命令	说明
anyconnect	为特定组或用户启用或要求 SSL VPN 客户端。
anyconnect dpd-interval	在 ASA 上启用失效对等检测 (DPD)，并设置客户端或 ASA 执行 DPD 的频率。
anyconnect keep-installer	禁用客户端的自动卸载功能。客户端仍然安装在远程 PC 上以供将来连接。
anyconnect ssl rekey	支持客户端对会话执行密钥更新。

anyconnect ssl rekey

要使远程客户端对 SSL VPN 连接执行密钥更新，请在组策略 webvpn 或用户名 webvpn 配置模式下使用 **anyconnect ssl rekey** 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。

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

语法说明

method ssl	指定客户端在密钥更新期间建立一个新隧道。
method new-tunnel	指定客户端在密钥更新期间建立一个新隧道。
method none	禁用密钥更新。
time *minutes*	指定从会话开始到密钥更新所经历的分钟数，从 4 分钟到 10080 分钟（1 周）。

默认值

默认值为 none。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
7.1(1)	此命令作为 **svc rekey** 引入。
8.0(2)	**svc rekey method ssl** 命令的行为更改为 **svc rekey method new-tunnel** 命令的行为，以防止 “ 人为截取 ” 攻击。
8.4(1)	**anyconnect ssl rekey** 命令取代了 **svc rekey** 命令。

使用指南

Cisco AnyConnect 安全移动客户端可对与 ASA 的 SSL VPN 连接执行密钥更新。将密钥更新方法配置为 **ssl** 或 **new-tunnel** 可指定客户端在密钥更新期间建立新隧道，而不是在密钥更新期间进行 SSL 重新协商。

示例

在以下示例中，用户指定属于组策略 *sales* 的远程客户端在密钥更新期间与 SSL 重新协商，在会话开始 30 分钟后发生密钥更新：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

相关命令

命令	说明
anyconnect enable	为特定组或用户启用或要求 AnyConnect 安全移动客户端。
anyconnect dpd-interval	在 ASA 上启用失效对等检测 (DPD)，并设置 AnyConnect 安全移动客户端或 ASA 执行 DPD 的频率。
anyconnect keepalive	指定远程计算机上的 AnyConnect 安全移动客户端向 ASA 发送 keepalive 消息的频率。
anyconnect keep-installer	支持将 AnyConnect 安全移动客户端永久安装到远程计算机上。

anyconnect-custom（版本 9.0 到 9.2）

要设置或更新自定义属性的值，请在 anyconnect-custom-attr 配置模式下使用 **anyconnect-custom** 命令。要删除自定义属性的值，请使用此命令的 **no** 形式。

anyconnect-custom *attr-name* **value** *attr-value*

anyconnect-custom *attr-name* **none**

no anyconnect-custom *attr-name*

语法说明

attr-name	当前组策略中属性的名称，由 **anyconnnect-custom-attr** 命令定义。
none	立即执行默认操作。
value *attr-value*	一个包含属性值的字符串。在连接建立过程中，值与属性名称关联并传递给客户端。最大长度是 450 个字符。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
anyconnect-custom-attr 配置	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令在组策略中设置自定义属性的值。*AnyConnect 管理员指南*列出了应用于该版本的自定义属性的有效值。使用 **anyconnect-custom-attr** 命令可创建自定义属性。

支持使用此命令的多个实例为属性建立一个多行值。与给定属性名称关联的所有数据将按照这些数据在 CLI 中的输入顺序发送给客户端。无法删除多行值的各个行。

此命令的 **no** 形式不允许 **value** 或 **none** 关键字。

如果与某个属性名关联的数据是在多个 CLI 行中输入的，则会将数据作为换行符 (\n) 分隔的单一连续字符串发送到终端。

示例

以下示例为 AnyConnect 延迟更新配置自定义属性：

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

相关命令

命令	说明
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。
show run group-policy	显示关于当前组策略的配置信息。
anyconnect-custom-attr	创建自定义属性。

anyconnect-custom（版本 9.3 和更高版本）

要设置或更新自定义属性的值，请在组策略或动态访问策略记录配置模式下使用 **anyconnect-custom** 命令。要删除自定义属性，请使用此命令的 **no** 形式。

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

语法说明

attr-type	自定义属性的类型，由 **anyconnnect-custom-attr** 命令定义。
none	此自定义属性从策略中显式省略。
value *attr-name*	自定义属性的名称，由 **anyconnect-custom-data** 命令定义。 自定义属性类型和指定的值在连接建立过程中传递给客户端。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略或动态访问策略记录	• 是	—	• 是	—	—

命令历史

版本	修改
9.3(1)	此命令已经重新定义。

使用指南

此命令在组策略或 DAP 中设置自定义属性的值。

*AnyConnect 管理员指南*列出了应用于该版本的自定义属性的有效值。使用 **anyconnect-custom-attr** 和 **anyconnect-custom-data** 命令创建自定义属性。

此命令的 **no** 形式不允许 **none** 关键字。

示例

以下示例为 AnyConnect 延迟更新配置自定义属性：

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

相关命令

命令	说明
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。
show run group-policy	显示关于当前组策略的配置信息。
show running-config dynamic-access-policy-record	显示在 DAP 策略中使用的自定义属性。
anyconnect-custom-attr	创建此命令使用的自定义属性类型。
anyconnect-custom-data	创建此命令使用的自定义属性指定的值。

anyconnect-custom-attr（版本 9.0 到 9.2）

要创建自定义属性，请在 Anyconnect-custom-attr 配置模式下使用 **anyconnect-custom-attr** 命令。要删除自定义属性，请使用此命令的 **no** 形式。

[**no**] **anyconnect-custom-attr** *attr-name* [**description** *description*]

语法说明

attr-name	属性的名称。在组策略语法和聚合身份验证协议消息中引用此名称。最大长度是 32 个字符。
description *description*	关于属性用法的自由形式的说明。当从组策略属性配置模式引用自定义属性时，此文本出现在命令帮助中。最大长度是 128 个字符。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Anyconnect-custom-attr 配置	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令创建自定义属性以支持特殊 AnyConnect 功能。在为特定功能创建自定义属性后，您将它们添加到组策略，以便该功能可应用到 VPN 客户端。此命令可确保所有定义的属性名称都是唯一的。

AnyConnect 的某些版本使用自定义属性来配置功能。各个版本的发布说明和 *AnyConnect 管理员指南*列出了需要自定义属性的所有功能。

如果您尝试删除正在组策略中使用的属性的定义，则会显示错误消息，并且删除操作将失败。如果用户尝试添加已作为自定义属性存在的属性，则将合并对说明的任何更改，但命令将被忽略。

支持使用此命令的多个实例为属性建立一个多行值。与给定属性名称关联的所有数据将按照这些数据在 CLI 中的输入顺序发送给客户端。无法删除多行值的各个行。

示例

以下示例为 AnyConnect 延迟更新配置自定义属性：

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

相关命令

命令	说明
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。
show run group-policy	显示关于当前组策略的配置信息。
anyconnect-custom	将自定义属性类型和指定的值与组策略或动态访问策略关联起来。

anyconnect-custom-attr（版本 9.3 和更高版本）

要创建自定义属性类型，请在 config-webvpn 配置模式下使用 **anyconnect-custom-attr** 命令。要删除自定义属性，请使用此命令的 **no** 形式。

[**no**] **anyconnect-custom-attr** *attr-type* [**description** *description*]

语法说明

attr-type	属性的类型。在组策略语法和 DAP 策略语法以及聚合身份验证协议消息中引用此类型。最大长度是 32 个字符。
description *description*	关于属性用法的自由形式的说明。当从组策略属性配置模式引用自定义属性时，此文本出现在命令帮助中。最大长度是个字符。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	此命令已经重新定义。

使用指南

此命令创建自定义属性以支持特殊 AnyConnect 功能。在为特定功能创建自定义属性后，您定义这些属性的值，然后将它们添加到组策略中，以便相关功能可应用于 VPN 客户端。此命令可确保所有定义的属性名称都是唯一的。

AnyConnect 的某些版本使用自定义属性来配置功能。各个版本的发布说明和 *AnyConnect 管理员指南*列出了需要自定义属性的所有功能。

如果您尝试删除正在组策略中使用的属性的定义，则会显示错误消息，并且删除操作将失败。如果用户尝试添加已作为自定义属性存在的属性，则将合并对说明的任何更改，但命令将被忽略。

示例

以下示例为 AnyConnect 延迟更新配置自定义属性：

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
```

相关命令

命令	说明
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。
show run group-policy	显示关于当前组策略的配置信息。
show running-config dynamic-access-policy-record	显示在 DAP 策略中使用的自定义属性。
anyconnect-custom	为策略使用而设置自定义属性的值。
anyconnect-custom-data	创建自定义属性指定的值。

anyconnect-custom-data

要创建自定义属性指定的值，请在全局配置模式下使用 **anyconnect-custom-data** 命令。要删除自定义属性，请使用此命令的 **no** 形式。

anyconnect-custom-data *attr-type attr-name attr-value*

no anyconnect-custom-data *attr-type attr-name*

语法说明

attr-type	以前使用 **anyconnect-custom-attr** 定义的属性的类型。
attr-name	具有指定值的属性的名称。在组策略和动态访问策略记录配置模式中可以引用它。
attr-value	一个包含属性值的字符串。 最大长度为 420 个字符。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局	• 是	—	• 是	—	—

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令定义自定义属性指定的值以支持特殊 AnyConnect 功能。在为特定功能创建自定义属性后，您定义这些属性的值，然后将它们添加到 DAP 或组策略，以便相关功能可应用于 VPN 客户端。

AnyConnect 的某些版本使用自定义属性来配置功能。各个版本的发布说明和 *AnyConnect 管理员指南*列出了需要自定义属性的所有功能。

如果您尝试删除正在组策略中使用的属性的指定值，则会显示错误消息，并且删除操作将失败。

支持使用此命令的多个实例为属性建立一个多行值。与给定属性名称关联的所有数据将按照这些数据在 CLI 中的输入顺序发送给客户端。无法删除多行值的各个行。

示例

以下示例为 AnyConnect 延迟更新配置自定义属性：

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

相关命令

命令	说明
show run webvpn	显示有关 WebVPN 的配置信息，包括 **anyconnect** 命令。
show run group-policy	显示关于当前组策略的配置信息。
show running-config dynamic-access-policy-record	显示在 DAP 策略中使用的自定义属性。
show run anyconnect-custom-data	显示所有定义的自定义属性的指定值。
anyconnect-custom	将自定义属性类型和值与组策略或 DAP 关联起来。
anyconnect-custom-attr	创建自定义属性。

anyconnect-essentials

要在 ASA 上启用 AnyConnect Essentials，请在组策略 webvpn 配置模式下使用 **anyconnect-essentials** 命令。要禁用使用 AnyConnect Essentials 并启用 premium AnyConnect 客户端，请使用此命令的 **no** 形式。

anyconnect-essentials

no anyconnect-essentials

默认值

默认情况下启用 AnyConnect Essentials。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

使用此命令可以在全功能 AnyConnect SSL VPN 客户端与 AnyConnect Essentials SSL VPN 客户端之间切换（假设已安装全功能 AnyConnect 客户端许可证）。AnyConnect Essentials 是一个单独许可的 SSL VPN 客户端，完全在 ASA 上配置，可提供高级 AnyConnect 功能，但以下情况除外：

- 没有 CSD（包括 HostScan/Vault/Cache Cleaner）
- 没有无客户端 SSL VPN

AnyConnect Essentials 客户端为运行 Microsoft Windows Vista、Windows Mobile、Windows XP 或 Windows 2000、Linux 或 Macintosh OS X 的远程最终用户提供思科 SSL VPN 客户端的优势。

使用 **anyconnect-essentials** 命令可启用或禁用 AnyConnect Essentials 客户端，但此操作仅当 ASA 上已安装 AnyConnect Essentials 许可证时才有意义。若没有此许可证，此命令将返回以下错误消息：

```
ERROR: Command requires AnyConnect Essentials license
```

注　此命令仅启用或禁用 AnyConnect Essentials 的使用。AnyConnect Essentials *许可证*本身不受 **anyconnect-essentials** 命令的设置的影响。

当 AnyConnect Essentials 许可证启用时，AnyConnect 客户端使用 Essentials 模式，无客户端 SSL VPN 访问被禁用。当 AnyConnect Essentials 许可证禁用时，AnyConnect 客户端使用全功能 AnyConnect SSL VPN 客户端许可证。

注　ASAv 上不支持此命令。有关详细信息，请参阅许可文档。

如果有活动的无客户端 SSL VPN 连接，并且您启用 AnyConnect Essentials 许可证，则所有连接会注销并需要重新建立。

示例

在以下示例中，用户进入 webvpn 配置模式并启用 AnyConnect Essentials VPN 客户端：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

apcf

要启用应用配置文件定制框架配置文件，请在 webvpn 配置模式下使用 **apcf** 命令。要禁用特定 APCF 脚本，请使用此命令的 **no** 形式。要禁用所有 APCF 脚本，请使用此命令的 **no** 形式，不带参数。

apcf URL/filename.ext

no apcf [URL/filename.ext]

语法说明

filename.extension	指定 APCF 定制脚本的名称。这些脚本始终采用 XML 格式。扩展名可能是 .xml、.txt、.doc 或众多其他扩展名之一。
URL	指定要在 ASA 上加载和使用的 APCF 配置文件的位置。使用以下 URL 之一：http://、https://、tftp://、ftp:/ ； flash:/、disk#:/' URL 可能包括服务器、端口和路径。如果仅提供文件名，则默认 URL 为 flash:/。您可以使用 **copy** 命令将 APCF 配置文件复制到闪存中。

默认值

没有默认行为或值。

命令模式

下表显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	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

apcf 命令支持 ASA 处理非标准 Web 应用和 Web 资源，以便它们在 WebVPN 连接上正确显示。APCF 配置文件包含一个脚本，其中指定为特定应用转换数据的时间（之前、之后）、位置（报头、正文、请求，响应）和转换的具体数据。

您可以在 ASA 上使用多个 APCF 配置文件。当您这样做时，ASA 以从最旧到最新的顺序应用每个配置文件。

我们建议您仅在思科 TAC 的支持下使用 APCF 命令。

示例

以下示例展示如何启用位于闪存中的 /apcf、名为 apcf1 的 APCF：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

以下示例展示如何启用名为 apcf2.xml 的 APCF，此 APCF 位于名为 myserver 的 HTTPS 服务器上，端口为 1440，路径为 /apcf：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
proxy-bypass	配置最少的内容重写为特定的应用。
rewrite	确定流量是否通过 ASA。
show running config webvpn apcf	显示 APCF 配置。

appl-acl

要标识之前配置的 webtype ACL 以应用于会话，请在 dap webvpn 配置模式下使用 **appl-acl** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。要删除所有 webtype ACL，请使用此命令的 **no** 形式，不带参数。

appl-acl [*identifier*]

no appl-acl [*identifier*]

语法说明

identifier	以前配置的 webtype ACL 的名称。最大长度是 240 个字符。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Dap webvpn configuration	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要配置 webtype ACL，请在全局配置模式下使用 **access-list webtype** 命令。

多次使用 **appl-acl** 命令可将多个 webtype ACL 应用于 DAP 策略。

示例

以下示例展示如何将以前配置的名为 newacl 的 webtype ACL 应用到动态访问策略：

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# appl-acl newacl
```

相关命令

命令	说明
dynamic-access-policy-record	创建 DAP 记录。
access-list_webtype	创建 webtype ACL。

application-access

要定制向经过身份验证的 WebVPN 用户显示的 WebVPN 主页的 “Application Access”（应用访问）字段和当用户选择应用时启动的 “Application Access”（应用访问）窗口，请在定制配置模式下使用 **application-access** 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。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

语法说明

message	更改在 “Application Access”（应用访问）字段的标题下显示的消息。
style	更改 “Application Access”（应用访问）字段的样式。
text	更改 “Application Access”（应用访问）字段的文本。
title	更改 “Application Access”（应用访问）字段的标题。
value	要显示的实际文本（最多 256 个字符）或级联样式表 (CSS) 参数（最多 256 个字符）。
window	更改 “Application Access”（应用访问）窗口。

默认值

“Application Access”（应用访问）字段的默认标题文本为 “Application Access”（应用访问）。

“Application Access”（应用访问）字段的默认标题样式是：

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

“Application Access”（应用访问）字段的默认消息文本是 “Start Application Client”（启动应用客户端）。

“Application Access”（应用访问）字段的默认消息样式是：

background-color:#99CCCC;color:maroon;font-size:smaller。

“Application Access”（应用访问）窗口的默认窗口文本是：

“Close this window when you finish using Application Access.Please wait for the table to be displayed before starting applications.”。

“Application Access”（应用访问）窗口的默认窗口样式是：

background-color:#99CCCC;color:black;font-weight:bold。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
定制配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用 **webvpn** 命令或者 **tunnel-group webvpn-attributes** 命令可访问此命令。

style 选项以任何有效的级联样式表 (CSS) 参数来表示。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。

以下提示可帮助您对 WebVPN 页作出最常见的更改 - 页面颜色更改：

- 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 “Application Access”（应用访问）字段的背景颜色定制为 RGB 十六进制值 66FFFF，表示绿色阴影：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

相关命令

命令	说明
application-access hide-details	启用或禁用在 “Application Access”（应用访问）窗口中显示应用详细信息。
browse-networks	定制 WebVPN 主页的 “Browse Networks”（浏览网络）字段。
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”（网络应用）字段。
web-bookmarks	定制 WebVPN 主页上的 Web Bookmarks 标题或链接。

application-access hide-details

要隐藏在 “WebVPN Applications Access”（WebVPN 应用访问）窗口中显示的应用详细信息，请在定制配置模式下使用 **application-access hide-details** 命令，使用 **webvpn** 命令或 **tunnel-group webvpn-attributes** 命令可进入定制配置模式。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。

application-access hide-details {**enable** | **disable**}

no application-access [**hide-details** {**enable** | **disable**}]

语法说明

disable	不在 “Application Access”（应用访问）窗口中隐藏应用详细信息。
enable	在 “Application Access”（应用访问）窗口中隐藏应用详细信息。

默认值

默认设置为禁用。在 “Application Access”（应用访问）窗口中出现应用详细信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
定制配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

示例

以下示例禁用应用详细信息的显示：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

相关命令

命令	说明
application-access	定制 WebVPN 主页的 “Application Access”（应用访问）字段。
browse-networks	定制 WebVPN 主页的 “Browse Networks”（浏览网络）字段。
web-applications	定制 WebVPN 主页的 “Web Application”（网络应用）字段。

area 至 auto-update timeout 命令

area

要创建 OSPF v2 或 OSPFv3 区域，请在路由器配置模式下使用 **area** 命令。要删除区域，请使用此命令的 **no** 形式。

area *area_id*

no area *area_id*

语法说明

area_id	所创建的区域 ID。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	增加了对 OSPFv3 的支持。

使用指南

您创建的区域没有设置任何参数。使用相关的 **area** 命令来设置区域参数。

示例

以下示例展示如何创建区域 ID 为 1 的 OSPF 区域：

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

相关命令

命令	说明
area nssa	将区域定义为末节区域。
area stub	将区域定义为存根区域。
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area authentication

要启用 OSPFv2 区域的身份验证，请在路由器配置模式下使用 **area authentication** 命令。要禁用区域身份验证，请使用此命令的 **no** 形式。

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

语法说明

area_id	将要启用身份验证的区域的标识符。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
message-digest	（可选）启用由 *area_id* 指定的区域的消息摘要 5 (MD5) 身份验证。

默认值

禁用区域身份验证。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果指定的 OSPFv2 区域不存在，则当输入此命令时，会创建该区域。输入 **area authentication** 命令且不含 **message-digest** 关键字，可启用简单密码身份验证。若包括 **message-digest** 关键字，则启用 MD5 身份验证。

示例

以下示例展示如何启用区域 1 的 MD5 身份验证：

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area default-cost

要指定发送到存根或 NSSA 的默认汇总路由的成本，请在路由器配置模式或 IPv6 路由器配置模式下使用 **area default-cost** 命令。要恢复默认成本值，请使用此命令的 **no** 形式。

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost** *cost*

语法说明

area_id	更改其默认成本的存根或 NSSA 的标识符。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
cost	指定用于存根或 NSSA 的默认汇总路由的成本。有效值范围为 0 到 65535

默认值

cost 的默认值为 1。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	支持多个情景模式和 OSPFv3。

使用指南

如果之前尚未使用 **area** 命令定义指定的区域，则此命令会通过指定的参数创建区域。

示例

以下示例展示如何指定发送到存根或 NSSA 的默认汇总路由的成本：

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

相关命令

命令	说明
area nssa	将区域定义为末节区域。
area stub	将区域定义为存根区域。
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area filter-list prefix

要过滤在 ABR 的各 OSPFv2 区域之间的类型 3 LSA 中通告的前缀，请在路由器配置模式下使用 **area filter-list prefix** 命令。要更改或取消过滤器，请使用此命令的 **no** 形式。

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

语法说明

area_id	标识配置过滤的区域。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
in	将配置的前缀列表应用到通告入站到指定区域的前缀。
list_name	指定前缀列表的名称。
out	将配置的前缀列表应用到通告从指定区域出站的前缀。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果之前尚未使用 **area** 命令定义指定的区域，则此命令会通过指定的参数创建区域。

只能过滤类型 3 LSA。如果已在专用网络中配置 ASBR，则会将泛洪发送到包括公共区域的整个 AS 的类型 5 LSA（说明专用网络）。

示例

以下示例过滤从所有其他区域发送到区域 1 的前缀：

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area nssa

要将区域配置为 NSSA，请在路由器配置模式或 IPv6 路由器配置模式下使用 **area nssa** 命令。要从区域删除 NSSA 指定，请使用此命令的 **no** 形式。

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

语法说明

area_id	标识指定为 NSSA 的区域。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
default-information-originate	用于生成默认至 NSSA 区域的类型 7。此关键字只在 NSSA ABR 或 NSSA ASBR 上生效。
metric *metric_value*	（可选）指定 OSPF 默认指标值。有效值范围为 0 到 16777214。
metric-type {**1** | **2**}	（可选）默认路由的 OSPF 指标类型。有效值包括以下值： • **1** - 类型 1 • **2** - 类型 2。 默认值为 2。
no-redistribution	（可选）如果路由器是 NSSA ABR 且您需要 **redistribute** 命令仅将路由导入到正常区域，而不导入到 NSSA 区域，则使用此命令。
no-summary	（可选）允许区域为末节区域，但是不允许将汇总路由注入其中。

默认值

默认值如下：

- 未定义 NSSA 区域。
- **metric-type** 为 2。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	支持多情景模式和 OSPFv3。

使用指南

如果之前尚未使用 **area** 命令定义指定的区域，则此命令会通过指定的参数创建区域。

如果为区域配置一个选项，稍后又指定另一个选项，则这两个选项都会设置。例如，单独输入以下两个命令会在配置中产生设置两个选项的单个命令：

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

示例

以下示例展示如何单独设置两个选项以在配置中产生单一命令：

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

相关命令

命令	说明
area stub	将区域定义为存根区域。
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area range (OSPFv2)

为了在区域边界上整合并汇总路由，请在路由器配置模式中使用 **area range** 命令。要禁用此功能，请使用此命令的 **no** 形式。

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

语法说明

address	子网范围的 IP 地址。
advertise	（可选）设置地址范围状态以通告并生成类型 3 汇总链路状态通告 (LSA)。
area_id	标识配置范围的区域。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
mask	IP 地址子网掩码。
not-advertise	（可选）地址范围状态设置为 DoNotAdvertise。抑制类型 3 汇总 LSA，并保持向其他网络隐藏组件网络。

默认值

地址范围状态设置为 advertise。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果之前尚未使用 **area** 命令定义指定的区域，则此命令会通过指定的参数创建区域。

area range 命令仅与 ABR 一起用于合并或汇总区域的路由。结果是通过 ABR 将单个汇总路由通告到其他区域。在区域边界压缩路由信息。在区域之外，对于每个地址范围通告单个路由。这个行为称为*路由汇总*。您可以为区域配置多个 **area range** 命令。这样，OSPF 可以汇总许多组不同地址范围的地址。

no area *area_id* **range** *ip_address netmask* **not-advertise** 命令仅删除 **not-advertise** 可选关键字。

示例

以下示例针对网络 10.0.0.0 上的所有子网和网络 192.168.110.0 上的所有主机，指定通过 ABR 通告一个到其他区域的汇总路由：

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area range (OSPFv3)

要在区域边界合并和汇总 OSPFv3 路由，请在 IPv6 路由器配置模式下使用 **area range** 命令。要禁用此功能，请使用此命令的 **no** 形式。

area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

语法说明

advertise	（可选）设置范围状态以通告并生成类型 3 汇总链路状态通告 (LSA)。
area_id	指定要汇总路由的区域的标识符。您可以将标识符指定为十进制数字或 IPv6 前缀。
cost *cost*	（可选）指定此汇总路由的指标或成本，用于在 OSPF SPF 计算期间确定到目的地的最短路径。有效值范围为 0 到 16777215。
ipv6-prefix	指定 IPv6 前缀。
not-advertise	（可选）将范围状态设置为 DoNotAdvertise。抑制类型 3 汇总 LSA，并保持向其他网络隐藏组件网络。
prefix-length	指定 IPv6 前缀长度。

默认值

默认情况下范围状态设置为 advertise。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

如果之前尚未使用 **area** 命令定义指定的区域，则此命令会通过指定的参数创建区域。

area range 命令仅与 ABR 一起使用。用于合并或汇总区域的路由。结果是通过 ABR 将单个汇总路由通告到其他区域。在区域边界压缩路由信息。在区域之外，针对每个 IPv6 前缀和前缀长度通告单个路由。这个行为称为*路由汇总*。您可以为区域配置多个 **area range** 命令。这样，OSPFv3 可以针对许多组不同 IPv6 前缀和前缀长度汇总路由。

示例

以下示例针对 IPv6 前缀 2000:0:0:4::2 且前缀长度 2001::/64，指定通过 ABR 通告一个汇总路由到其他区域：

```
ciscoasa(config-router)# area 1 range 2000:0:0:4::2/2001::/64
ciscoasa(config-router)#
```

相关命令

命令	说明
ipv6 router ospf	进入 OSPFv3 的 IPv6 路由器配置模式。
show running-config ipv6 router	显示全局路由器配置中的 IPv6 命令。

area stub

要将区域定义为存根区域，请在路由器配置模式或 IPv6 路由器配置模式下使用 **area stub** 命令。要删除存根区域，请使用此命令的 **no** 形式。

area *area_id* **stub** [**no-summary**]

no area *area_id* **stub** [**no-summary**]

语法说明

area_id	标识存根区域。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
no-summary	防止 ABR 发送汇总链路通告到存根区域。

默认值

默认行为如下所示：

- 未定义存根区域。
- 将汇总链路通告发送到存根区域。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
9.0(1)	增加了对 OSPFv3 的支持。

使用指南

仅在连接到存根或 NSSA 的 ABR 上使用命令。

有两个存根区域路由器配置命令：**area stub** 和 **area default-cost** 命令。在连接到存根区域的所有路由器和接入服务器中，应使用 **area stub** 命令将区域配置为存根区域。仅在连接到存根区域的 ABR 上使用 **area default-cost** 命令。**area default-cost** 命令提供通过 ABR 生成到存根区域的汇总默认路由的指标。

示例

以下示例将指定区域配置为存根区域：

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

相关命令

命令	说明
area default-cost	指定发送到存根或 NSSA 的默认汇总路由的成本。
area nssa	将区域定义为末节区域。
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

area virtual-link (OSPFv2)

要定义 OSPF 虚拟链路，请在路由器配置模式下使用 **area virtual-link** 命令。要重置选项或删除虚拟链路，请使用此命令的 **no** 形式。

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key**[**0** | **8**] *key*] | [**message-digest-key** *key_id* **md5** [**0** | **8**] *key*]]]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key** [**0** | **8**] *key*] | [**message-digest-key** *key_id* **md5** [**0** | **8**] *key*]]]]

语法说明

area_id	用于虚拟链路的中转区域的区域 ID。您可以将标识符指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。
authentication	（可选）指定身份验证类型。
authentication-key [**0** | **8**]*key*	（可选）指定供邻近路由设备使用的 OSPF 身份验证密码。
dead-interval *seconds*	（可选）指定在没有接收到问候数据包时宣告邻近路由设备关闭之前的间隔；有效值为 1 到 65535 秒。
hello-interval *seconds*	（可选）指定在接口上发送问候数据包之间的间隔；有效值为 1 到 65535 秒。
md5 [**0** | **8**] *key*	（可选）指定最多 16 字节的字母数字密钥。
message-digest	（可选）指定使用消息摘要身份验证。
message-digest-key *key_id*	（可选）启用消息摘要 5 (MD5) 身份验证并指定数字身份验证密钥 ID 号码；有效值为 1 到 255。
0	指定未加密的密码将跟随左右。
8	指定加密密码的将跟随左右。
null	（可选）指定不使用身份验证。覆盖配置给 OSPF 区域的密码或消息摘要身份验证。
retransmit-interval *seconds*	（可选）对属于该接口的相邻路由器指定 LSA 重新传送之间的时间；有效值为 1 到 65535 秒。
router_id	与虚拟链路邻居关联的路由器 ID。路由器 ID 通过每个路由器从内部派生自接口 IP 地址。必须以 IP 地址的格式输入此值。没有默认值。
transmit-delay *seconds*	（可选）指定在 OSPF 接收拓扑更改时与启动最短路径优先 (SPF) 计算（从 0 到 65535 秒）时之间的延迟时间。默认值为 5 秒。

注　不再支持单个数字密码和以数字开头、后跟随空格的密码。

默认值

默认值如下：

- *area_id*：没有预定义区域 ID。
- *router_id*：没有预定义路由器 ID。
- **hello-interval** *seconds*：10 秒。

- **retransmit-interval** *seconds*：5 秒。
- **transmit-delay** *seconds*：1 秒。
- **dead-interval** *seconds*：40 秒。
- **authentication-key** [**0 | 8**] *key*：没有预定义密钥。
- **message-digest-key** *key_id* **md5** [**0 | 8**] *key*：没有预定义密钥。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。

使用指南

在 OSPF 中，所有区域必须连接到主干区域。如果中断与主干的连接，可以通过建立虚拟链路进行修复。

问候间隔越小，越快检测到拓扑更改，但随之而来的路由流量也更多。

应保守设置重新传输，否则将发生不必要的重新传输。串行线路和虚拟链路的值应较大。

传输延迟值应考虑接口的传输和传播延迟。

只有通过 **area** *area_id* **authentication** 命令启用主干的身份验证时，才使用指定的身份验证密钥。

简单文本和 MD5 身份验证这两种身份验证方案相互排斥。可以指定其中之一，或者都不指定。您在 **authentication-key** [**0 | 8**] *key* or **message-digest-key** *key_id* **md5**[**0 | 8**] *key* 之后指定的任何关键字和参数都会被忽略。因此，请在这类关键字 / 参数组合之前指定任何可选参数。

如果没有为接口指定身份验证类型，接口会使用指定给区域的身份验证类型。如果尚未指定区域的身份验证类型，则区域默认为无身份验证。

注　每个虚拟链路邻居必须包括中转区域 ID 和对应的虚拟链路邻居路由器 ID，才可以正确配置虚拟链路。使用 **show ospf** 命令查看路由器 ID。

示例

以下示例建立具有 MD5 身份验证的虚拟链路：

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show ospf	显示有关 OSPF 路由进程的一般信息。
show running-config router	在全局路由器配置中显示的命令。

area virtual-link (OSPFv3)

要定义 OSPFv3 虚拟链路，请在 IPv6 路由器配置模式下使用 **area virtual-link** 命令。要重置选项或删除虚拟链路，请使用此命令的 **no** 形式。

area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [**ttl-security hops** *hop-count*]

no area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

语法说明

area_id	指定用于虚拟链路的中转区域的区域 ID。您可以将标识符指定为十进制数字或有效的 IPv6 前缀。有效十进制值范围为 0 到 4294967295。
dead-interval *seconds*	（可选）指定在邻居指示路由器关闭之前问候数据包不可见的时间（以秒为单位）。停顿间隔是不带正负号的整数值。与问候间隔一样，对于连接到公用网络的所有路由器和接入服务器，此值必须相同。有效值范围为 1 到 8192 秒。
hello-interval *seconds*	（可选）指定 ASA 在接口上发送的问候数据包之间的时间（以秒为单位）。问候间隔是问候数据包中通告的不带正负号的整数值。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 8192 秒。
retransmit-interval *seconds*	（可选）对于属于该接口的相邻路由器，指定 LSA 重新传输之间的时间（以秒为单位）。重新传输间隔是所连接的网络中任意两个路由器之间的预计往返延迟。值必须大于预计往返延迟。有效值范围为 1 到 8192 秒。
router_id	指定与虚拟链路邻居相关联的路由器 ID。路由器 ID 在 **show ipv6 ospf** 或 **show ipv6 display** 命令中。
transmit-delay *seconds*	（可选）指定在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。整数值必须大于零。更新数据包中的 LSA 在传输之前按此数量增加其时限。有效值范围为 1 到 8192 秒。
ttl-security hops *hop-count*	（可选）在虚拟链路上配置生存时间 (TTL) 安全。跃点计数的有效值范围为 1 到 254。

注　不再支持单个数字密码和以数字开头且后跟随空格的密码。

默认值

默认值如下：

- *area_id*：没有预定义区域 ID。
- *router_id*：没有预定义路由器 ID。
- **hello-interval**：10 秒。
- **retransmit-interval**：5 秒。
- **transmit-delay**：1 秒。
- **dead-interval**：40 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

在 OSPFv3 中，所有区域必须连接到主干区域。如果中断与主干的连接，可以通过建立虚拟链路进行修复。

问候间隔越小，越快检测到拓扑更改，但随之而来的路由流量也更多。

应保守设置重新传输间隔，否则将发生不必要的重新传输。串行线路和虚拟链路的值应较大。

传输延迟值应考虑接口的传输和传播延迟。

注　每个虚拟链路邻居必须包括中转区域 ID 和对应的虚拟链路邻居路由器 ID，才可以正确配置虚拟链路。使用 **show ipv6 ospf** 命令获取路由器 ID。

示例

以下示例在 OSPFv3 中建立虚拟链路：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

相关命令

命令	说明
ipv6 router ospf	进入 OSPFv3 的路由器配置模式。
show ipv6 ospf	显示关于 OSPFv3 路由进程的一般信息。
show running-config ipv6 router	显示全局路由器配置中的 IPv6 命令。

arp

要向 ARP 表添加静态 ARP 条目，请在全局配置模式下使用 **arp** 命令。要删除静态条目，请使用此命令的 **no** 形式。

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

语法说明

alias	（可选）启用此映射的代理 ARP。如果 ASA 接收到指定 IP 地址的 ARP 请求，则会使用 ASA MAC 地址进行响应。当 ASA 接收到属于 IP 地址的主机的流量时，ASA 会将流量转发到在此命令中指定的主机 MAC 地址。例如，此关键字在您有不执行 ARP 的设备时非常有用。 在透明防火墙模式下，会忽略此关键字； ASA 不执行代理 ARP。
interface_name	连接到主机网络的接口。
ip_address	主机 IP 地址。
mac_address	主机 MAC 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。

使用指南

尽管主机通过 IP 地址标识数据包目的地，但是以太网上数据包的实际交付还是依赖于以太网 MAC 地址。当路由器或主机要在直接连接的网络上交付数据包时，它会发送 ARP 请求，要求与 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器会保留 ARP 表，因此不必对需要交付的每个数据包发送 ARP 请求。通过网络发送 ARP 响应时会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果该条目不正确（例如，给定 IP 地址的 MAC 地址发生变化），则条目在可以更新之前会超时。

静态 ARP 条目将 MAC 地址映射到 IP 地址并标识到达主机所使用的接口。静态 ARP 条目不会超时，并可帮您解决网络问题。在透明防火墙模式下，静态 ARP 表与 ARP 检查搭配使用（参阅 **arp-inspection** 命令）。

注　在透明防火墙模式下，动态 ARP 条目用于 ASA 中进出的流量，如管理流量。

示例

以下示例在 outside 接口上对 MAC 地址为 0009.7cbe.2100 的 10.1.1.1 创建静态 ARP 条目：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

相关命令

命令	说明
arp timeout	设置 ASA 重建 ARP 表之前的时间。
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
show arp	显示 ARP 表。
show arp statistics	显示 ARP 统计数据。
show running-config arp	显示 ARP 超时的当前配置。

arp permit-nonconnected

要使 ARP 缓存还包括非直接连接的子网，请在全局配置模式下使用 **arp permit-nonconnected** 命令。要禁用未连接的子网，请使用此命令的 **no** 形式。

arp permit-nonconnected

no arp permit-nonconnected

语法说明

此命令没有任何参数或关键字。

命令默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4 (5)、9.0(1)	我们引入了此命令。

使用指南

ASA ARP 缓存默认情况下仅包含来自直接连接的子网的条目。通过此命令，您可以使 ARP 缓存还包括非直接连接的子网。我们不建议启用此功能，除非您知道安全风险。此功能有助于发动针对 ASA 的拒绝服务 (DoS) 攻击；任何接口上的用户可以发送许多 ARP 应答，用错误条目使 ASA ARP 表过载。

如果您使用以下项，则可能要使用此功能：

- 辅助子网。
- 用于流量转发的相邻路由上的代理 ARP。

示例

以下示例启用非连接的子网：

```
ciscoasa(config)# arp permit non-connected
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。

arp-inspection

要为透明防火墙模式弃用 ARP 检查，请在全局配置模式下使用 **arp-inspection** 命令。要禁用 ARP 检查，请使用此命令的 **no** 形式。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

语法说明

enable	启用 ARP 检查。
flood	（默认）指定将与静态 ARP 条目的任何元素都不匹配的数据包泛洪到除原始接口之外的所有接口。如果 MAC 地址、IP 地址或接口之间不匹配，则 ASA 丢弃数据包。 **注**　如果有管理特定接口，即使此参数设置为 flood，它也从不会泛洪数据包。
interface_name	要启用 ARP 检查的接口。
no-flood	（可选）指定丢弃没有完全匹配静态 ARP 条目的数据包。

默认值

默认情况下，所有接口上禁用 ARP 检查；所有 ARP 数据包允许通过 ASA。当您启用 ARP 检查时，默认值为泛洪不匹配的 ARP 数据包。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在启用 ARP 检查之前，使用 **arp** 命令配置静态 ARP 条目。

ARP 检查根据静态 ARP 条目检查所有 ARP 数据包（参阅 **arp** 命令）并阻止不匹配的数据包。此功能可防止 ARP 欺骗。

当您启用 ARP 检查时，ASA 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 ASA 丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的所有条目都不匹配，则可以将 ASA 设置为从所有接口转发数据包（泛洪），或丢弃数据包。

注　如果有专用管理接口，即使此参数设置为 flood，它也从不会泛洪数据包。

ARP 检查防止恶意用户冒充其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用 “ 中间人 ” 攻击。例如，主机发送 ARP 请求到网关路由器；网关路由器使用网关路由器 MAC 地址响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。然后，攻击者可以在主机流量转发到路由器之前拦截所有主机流量。

如果正确的 MAC 地址和关联的 IP 地址在静态 ARP 表中，则 ARP 检查可确保攻击者无法使用攻击者 MAC 地址发送 ARP 响应。

注　在透明防火墙模式下，动态 ARP 条目用于 ASA 中进出的流量，如管理流量。

示例

以下示例在 outside 接口上启用 ARP 检查，并将 ASA 设置为丢弃与静态 ARP 条目不匹配的所有 ARP 数据包。

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
clear configure arp-inspection	清除 ARP 检查配置。
firewall transparent	将防火墙模式设置为透明。
show arp statistics	显示 ARP 统计数据。
show running-config arp	显示 ARP 超时的当前配置。

arp timeout

要设置 ASA 重建 ARP 表之前的时间，请在全局配置模式下使用 **arp timeout** 命令。要恢复默认超时，请使用此命令的 **no** 形式。

arp timeout *seconds*

no arp timeout *seconds*

语法说明

seconds	ARP 表重建之间的秒数，从 60 到 4294967。

默认值

默认值为 14,400 秒（4 小时）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。

使用指南

自动重建 ARP 表会更新新主机信息和删除旧主机信息。因为主机信息频繁更改，您可能要减少超时。

示例

以下示例将 ARP 超时更改为 5,000 秒：

```
ciscoasa(config)# arp timeout 5000
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
show arp statistics	显示 ARP 统计数据。
show running-config arp timeout	显示 ARP 超时的当前配置。

as-path access-list

要通过正则表达式配置自主系统路径过滤器，请在全局配置模式下使用 **as-path access-list** 命令。要删除自主系统路径过滤器并从运行配置文件将其删除，请使用此命令的 **no** 形式。

as-path access-list *acl-name* {**permit** | **deny**} *regexp*

no as-path access-list *acl-name*

语法说明

acl-name	指定自主系统路径访问列表的名称。
permit	根据匹配条件允许通告。
deny	根据匹配条件拒绝通告。
regexp	定义自主系统路径过滤器的正则表达式。自主系统编号的表示范围为 1 到 65535。 要获取有关自主系统编号格式的更多详细信息，请参阅 **router bgp** 命令。 **注** 有关配置正则表达式的信息，请参阅*思科 IOS 终端服务配置指南*中的 “ 正则表达式 ” 附录。

默认值

没有创建自主系统路径过滤器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

使用 **as-path access-list** 命令配置自主系统路径过滤器。您可以将自主系统路径过滤器应用到入站和出站 BGP 路径。每个过滤器都通过正则表达式进行定义。如果正则表达式与表示为 ASCII 字符串的路由的自主系统路径匹配，则应用 **permit** 或 **deny** 条件。自主系统路径不应该包含本地自主系统编号。

思科实施 4 字节自主系统编号，使用 asplain（例如 65538）作为自主系统编号的默认正则表达式匹配和输出显示格式，但您可以如 RFC 5396 中所述配置 asplain 格式和 asdot 格式的 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令。当 asdot 格式启用为默认值时，必须使用 asdot 格式写入用来匹配 4 字节自主系统编号的所有正则表达式，否则正则表达式匹配将失败。

示例

在以下示例中，定义自主系统路径访问列表（编号 500），以配置 ASA 不将通过或从自主系统 65535 的任何路径通告到 10.20.2.2 邻居：

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asdm disconnect

要终止活动 ASDM 会话，请在特权 EXEC 模式下使用 **asdm disconnect** 命令。

asdm disconnect *session*

语法说明

session	要终止的活动 ASDM 会话的会话 ID。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **pdm disconnect** 命令更改为 **asdm disconnect** 命令。

使用指南

使用 **show asdm sessions** 命令以显示活动 ASDM 会话与其关联会话 ID 的列表。使用 **asdm disconnect** 命令以终止特定会话。

当您终止 ASDM 会话时，任何其余活动 ASDM 会话保留其关联的会话 ID。例如，如果有会话 ID 为 0、1 和 2 的三个活动 ASDM 会话且您终止会话 1，则其余活动 ASDM 会话保留会话 ID 0 和 2。此示例中的下一个新 ASDM 会话会分配会话 ID 1，而后面任何新会话从会话 ID 3 开始。

示例

以下示例终止会话 ID 为 0 的 ASDM 会话。**show asdm sessions** 命令在输入 **asdm disconnect** 命令前后显示活动 ASDM 会话。

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm sessions

1 192.168.1.2
```

相关命令

命令	说明
show asdm sessions	显示活动 ASDM 会话及其关联会话 ID 的列表。

asdm disconnect log_session

要终止活动 ASDM 日志记录会话，请在特权 EXEC 模式下使用 **asdm disconnect log_session** 命令。

asdm disconnect log_session *session*

语法说明

session	要终止的活动 ASDM 日志记录会话的会话 ID。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **show asdm log_sessions** 命令显示活动 ASDM 日志记录会话及其关联会话 ID 的列表。使用 **asdm disconnect log_session** 命令终止特定日志记录会话。

每个活动 ASDM 会话有一个或多个关联 ASDM 日志记录会话。ASDM 使用日志记录会话从 ASA 检索系统日志消息。终止日志会话可能会对活动 ASDM 会话有负面影响。要终止不需要的 ASDM 会话，请使用 **asdm disconnect** 命令。

注　因为每个 ASDM 会话至少有一个 ASDM 日志记录会话，所以 **show asdm sessions** 和 **show asdm log_sessions** 的输出可能相同。

当终止 ASDM 日志记录会话时，其余所有活动 ASDM 日志记录会话保留其关联的会话 ID。例如，如果有会话 ID 为 0、1 和 2 的三个活动 ASDM 日志记录会话，且您终止会话 1，则其余活动 ASDM 日志记录会话保留会话 ID 0 和 2。此示例中的下一个新 ASDM 日志记录会话会分配会话 ID 1，而之后的任何新日志记录会话将从会话 ID 3 开始。

示例

以下示例终止会话 ID 为 0 的 ASDM 会话。**show asdm log_sessions** 命令在输入 **asdm disconnect log_sessions** 命令前后显示活动 ASDM 会话。

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

```
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions

1 192.168.1.2
```

相关命令

命令	说明
show asdm log_sessions	显示活动 ASDM 日志记录会话及其关联会话 ID 的列表。

asdm history enable

要启用 ASDM 历史记录跟踪，请在全局配置模式下使用 **asdm history enable** 命令。要禁用 ASDM 历史记录跟踪，请使用此命令的 **no** 形式。

asdm history enable

no asdm history enable

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **pdm history enable** 命令更改为 **asdm history enable** 命令。

使用指南

通过启用 ASDM 历史记录跟踪获得的信息保存在 ASDM 历史记录缓冲区中。您可以使用 **show asdm history** 命令查看此信息。历史记录信息供 ASDM 用于设备监控。

示例

以下示例启用 ASDM 历史记录跟踪：

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

相关命令

命令	说明
show asdm history	显示 ASDM 历史记录缓冲区的内容。

asdm image

要指定闪存中 ASDM 软件映像的位置，请在全局配置模式下使用 **asdm image** 命令。要删除映像位置，请使用此命令的 **no** 形式。

asdm image *url*

no asdm image [*url*]

语法说明

url	设置闪存中 ASDM 映像的位置。参阅以下 URL 语法： • **disk0:/**[*path*/]*filename* 对于 ASA 5500 系列，此 URL 指示内部闪存。您还可以使用 **flash** 代替 **disk0**；它们互为别名。 • **disk1:/**[*path*/]*filename* 对于 ASA 5500 系列，此 URL 指示外部闪存卡。 • **flash:/**[*path*/]*filename* 此 URL 指示内部闪存。

默认值

如果在启动配置中不包括此命令，ASA 会在启动时使用它发现的第一个 ASDM 映像。它先后搜索内部闪存和外部闪存的根目录。然后，ASA 在发现映像时将 **asdm image** 命令插入到运行配置中。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以在闪存中保存多个 ASDM 软件映像。如果在有活动 ASDM 会话时输入 **asdm image** 命令指定新的 ASDM 软件映像，新命令不影响活动会话；活动 ASDM 会话会继续使用它们最初使用的 ASDM 软件映像。新 ASDM 会话使用新的软件映像。如果输入 **no asdm image** 命令，会从配置中删除命令。不过，您仍然可以使用最后配置的映像位置从 ASA 访问 ASDM。

如果在启动配置中不包括此命令，ASA 会在启动时使用它发现的第一个 ASDM 映像。它先后搜索内部闪存和外部闪存的根目录。然后，ASA 在发现映像时将 **asdm image** 命令插入到运行配置中。务必使用 **write memory** 命令将运行配置保存到启动配置。如果没有将 **asdm image** 命令保存到启动配置，则每次重新启动时，ASA 会搜索 ASDM 映像并将 **asdm image** 命令插入到运行配置中。如果您使用自动更新，启动时自动添加此命令会导致 ASA 上的配置与自动更新服务器上的配置不匹配。此不匹配导致 ASA 从自动更新服务器下载配置。要避免不必要的自动更新活动，请将 **asdm image** 命令保存到启动配置。

示例

以下示例将 ASDM 映像设置为 asdm.bin：

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

相关命令

命令	说明
show asdm image	显示当前 ASDM 映像文件。
boot	设置软件映像和启动配置文件。

asdm location

注意事项　请勿手动配置此命令。ASDM 将 **asdm location** 命令添加到运行配置并用于内部通信。此命令包含在文档中仅供参考。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

语法说明

if_name	安全性最高的接口的名称。如果您有多个接口处于最高安全性，则随机选择接口名称。不使用此接口名称，但它是必要参数。
ip_addr	供 ASDM 内部使用以定义网络拓扑的 IP 地址。
ipv6_addr/prefix	供 ASDM 内部使用以定义网络拓扑的 IPv6 地址和前缀。
netmask	*ip_addr* 的子网掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **pdm location** 命令更改为 **asdm location** 命令。

使用指南

请勿手动配置或删除此命令。

asp load-balance per-packet

对于多核 ASA，要更改负载平衡行为，请在全局配置模式下使用 **asp load-balance per-packet** 命令。要恢复默认负载平衡机制，请使用此命令的 **no** 形式。

asp load-balance per-packet [**auto**]

no asp load-balance per-packet

语法说明

auto	自动开启和关闭每个接口接收环上的每数据包 ASP 负载平衡。默认设置为禁用。

命令默认值

对于 **asp load-balance per-packet** 命令，默认情况下负载平衡机制支持多个接口。对于 **asp load-balance per-packet auto** 命令，默认行为是一次只允许一个核心从接口接收环接收数据包。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.1(1)	我们引入了此命令。
9.3(1)	添加了 **auto** 选项，以根据网络状况支持自动开启和关闭 ASP 负载平衡。

使用指南

针对在所有接口环统一接收数据包的情况优化默认行为。针对流量不对称分布在接口接收环的情况优化每个数据包行为。多核 ASA 的性能可根据处理器的数量、接口接收环的数量和所通过流量的性质而变化。使用 **asp load-balance per-packet** 命令可允许多个核心同时处理从单个接口接收环接收的数据包。如果收到的数据包遍布许多独立连接，则此命令提供并行处理。注意对于来自相同的相关连接的数据包，此命令可能导致额外的队列开销，因为这些数据包由一个核心处理。

如果系统丢弃数据包，并且 **show cpu** 命令输出远小于 100%，则此命令可在数据包属于许多无关的连接时帮助您提高吞吐量。CPU 使用率是有效使用多少核心的良好指标。

例如在包括八个核心的 ASA 5580-40 上，如果使用两个核心，则 **show cpu** 命令输出将为 25%；使用四个核心将为 50%；使用六个核心将为 75%。

auto 选项让 ASA 可检测是否已引入不对称流量。如果需要负载平衡，会释放接口接收环和核心之间的一对一锁定。此自适应 ASP 负载平衡机制有助于避免以下问题：

- 流上的突发流量峰值造成的溢出
- 批量流订用过多特定接口接收环造成的溢出
- 单核无法承受负载的相对严重过载接口接收环造成的溢出。

注　在自动模式下，只在高负载接口接收环（而非所有接口接收环）上启用每数据包 ASP 负载平衡。在升级期间，当启用或禁用每数据包 ASP 负载平衡时，您应保持正在运行的当前模式。您必须明确配置自动模式。

在自动模式下，每个接口接收环保持等待时间。若接口接收环视为处于忙碌状态，而每数据包 ASP 负载平衡因为大流量而自动启用，则接口接收环会保持自动为等待时间（默认为 200 毫秒）启用每数据包 ASP 负载平衡。如果接口接收环负载下降，但在 200 毫秒内由于大流量而重新获得负载，接口接收环会视为处于忙碌状态，等待时间会加倍，直到达到最多 6400 毫秒。如果接口接收环没有遇到连续大流量，则等待时间保持在 200 毫秒。此机制可降低在启用和禁用状态之间的每数据包 ASP 负载平衡摇摆，从而有助于在不同时间长度内避免溢出。

启用 **auto** 选项时，负载不高的环上会保持一对一锁定，因为这些环不需要多个核心的关注。此外，高负载环上不会保留一对一锁定，因为它们需要多个核心的关注以帮助处理其负载。

当在高负载环总数超过特定限制时，此功能自动关闭。

仅 ASA 5585-X 和 ASASM 支持使用此命令。

示例

以下示例展示如何更改默认负载平衡行为：

```
ciscoasa(config)# asp load-balance per-packet
```

以下示例启用每个数据包负载平衡的自动开启和关闭：

```
ciscoasa(config)# asp load-balance per-packet auto
```

相关命令

命令	说明
clear asp load-balance history	清除和重置每数据包 ASP 负载平衡历史统计信息。
show asp load-balance	显示负载平衡器队列大小的柱状图。
show asp load-balance per-packet	显示当前状态、上下限和全局阈值。
show asp load-balance per-packet history	显示当前状态、上下限、全局阈值、自上次重置以来开启和关闭每数据包 ASP 负载平衡的次数、具有时间戳的每数据包 ASP 负载平衡历史记录和开启和关闭的原因。

asp rule-engine transactional-commit

使用 **asp rule-engine transactional-commit** 命令启用或禁用规则引擎的交易执行模式。

asp rule-engine transactional-commit *option*

no asp rule-engine transactional-commit *option*

语法说明

option	对选定策略启用规则引擎的交易执行模式。选项包括： • **access-group** - 访问全局应用或应用到接口的规则。 • **nat** - 网络地址转换规则。

命令默认值

默认情况下，禁用交易执行模式。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(5)	我们引入了此命令。
9.3(1)	我们添加了 **nat** 关键字。

使用指南

默认情况下，当您更改基于规则的策略（例如访问规则）时，更改会立即生效。但是这种即时性会在一定程度上降低性能。对于每秒高连接环境的大量规则列表而言，例如当您更改具有 25,000 条规则的策略而 ASA 每秒处理 18,000 个连接时，性能降低更加明显。

因为规则引擎编译规则以启用更快的规则查找，所以性能会受到影响。默认情况下，系统在评估连接尝试以便可应用新的规则时，也搜索未编译的规则；因为规则没有编译，所以搜索需要更长时间。

您可以更改此行为，以便规则引擎在实施规则更改时使用交易模式，并在新规则编译并备妥可用之前继续使用旧规则。使用交易模式时，性能不应在规则编译期间降低。下表解释了行为差异。

型号	编译之前	编译期间	编译之后
默认	匹配旧规则。	匹配新规则。 （每秒连接率将降低。）	匹配新规则。
事务性	匹配旧规则。	匹配旧规则。 （每秒连接率将不受影响。）	匹配新规则。

交易模式的另一个优势是，当替换接口上的 ACL 时，在删除旧的 ACL 和应用新的 ACL 之间没有间隙。这将减少在操作期间丢失可接受连接的可能性。

提示　如果启用规则类型的交易模式，则会出现标记编译开始和结束的系统日志消息。这些消息从 780001 开始并往后编号。

示例

以下示例为访问组启用交易执行模式：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

相关命令

命令	说明
clear conf asp rule-engine transactional-commit	清除规则引擎的交易执行配置。
show run asp rule-engine transactional-commit	显示规则引擎的运行配置。

asr-group

要指定非对称路由接口组 ID，请在接口配置模式下使用 **asr-group** 命令。要删除 ID，请使用此命令的 **no** 形式。

asr-group *group_id*

no asr-group *group_id*

语法说明

group_id	非对称路由组 ID。有效值为从 1 到 32。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	—	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在启用主用 / 主用故障切换时，您可能遇到以下情况：负载平衡导致出站连接的返回流量通过对等单元上的活动情景进行路由，其中出站连接的情景在备用组中。

如果找不到传入接口的流，**asr-group** 命令会导致传入数据包使用相同 ASR 组的接口重新分类。如果重新分类查找另一接口的流，而且关联的情景处于备用状态，则该数据包转发至活动单元进行处理。

必须启用有状态的故障切换，此命令才会生效。

您可以使用 **show interface detail** 命令查看 ASR 统计信息。这些统计信息包括接口上 ASR 数据包的发送数、接收数和丢弃数。

注　在同一个 ASR 组中不应配置同一个情景中的两个接口。

示例

以下示例将选定接口分配给非对称路由组 1。

情景 ctx1 配置：

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

情景 ctx2 配置：

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

相关命令

命令	说明
interface	进入接口配置模式。
show interface	显示接口统计信息。

assertion-consumer-url

要标识安全设备用来联系 Assertion Consumer Service 所访问的 URL，请在 webvpn 配置模式下为该特定 SAML 类型 SSO 服务器使用 **assertion-consumer-url** 命令。要从声明删除 URL，请使用此命令的 **no** 形式。

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

语法说明

url	指定 SAML 类型 SSO 服务器使用的 Assertion Consumer Service 的 URL。URL 必须以 http:// 或 https:// 开始，且必须小于 255 个字母数字字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

单点登录 (SSO) 支持仅适用于 WebVPN，通过此功能，用户可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。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 SSO 服务器。

如果 URL 以 HTTPS 开始，则需要安装 Assertion Consumer Service SSL 证书的根证书。

示例

以下示例指定 SAML 类型 SSO 服务器的 Assertion Consumer URL：

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

相关命令

命令	说明
issuer	指定 SAML 类型 SSO 服务器安全设备名称。
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 WebVPN SSO 服务器。
trustpoint	指定信任点名称，其中包含用于签署 SAML 类型浏览器断言的证书。

attribute

要指定 ASA 写入 DAP 属性数据库的属性值对，请在 dap 测试属性模式下输入 **attribute** 命令。

attribute *name value*

语法说明

name	指定已知属性名称或包含 “ 标签 ” 标记的属性。标签标记对应于您配置给 DAP 记录中文件、注册、进程、防病毒、防间谍软件和个人防火墙终端属性的终端 ID。
value	分配给 AAA 属性的值。

命令默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
DAP 属性配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

多次使用此命令可输入多个属性值对。

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 在评估 DAP 记录的 AAA 选择属性和终端选择属性时，将其写入 DAP 子系统引用的属性数据库。

示例

以下示例假设如果授权用户是 SAP 组的成员并且在终端系统上安装了防病毒软件，则 ASA 选择两个 DAP 记录。防病毒软件终端规则的终端 ID 是 *nav*。

DAP 记录具有以下策略属性：

DAP 记录 1	DAP 记录 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
—	url-entry = enable

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
ciscoasa(config-dap-test-attr)# attribute endpoint.av.nav.exists true
ciscoasa(config-dap-test-attr)# exit

ciscoasa # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

ciscoasa #
```

相关命令 I

命令	说明
display	显示当前属性列表。
dynamic-access-policy-record	创建 DAP 记录。
test dynamic-access-policy attributes	输入属性。
test dynamic-access-policy execute	执行生成 DAP 的逻辑并将产生的访问策略显示到控制台。

auth-cookie-name

要指定身份验证 Cookie 的名称，请在 aaa-server 主机配置模式下使用 **auth-cookie-name** 命令。这是带有 HTTP Forms 命令的 SSO。

auth-cookie-name

语法说明

name	身份验证 Cookie 的名称。最大名称大小为 128 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server host configuration	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

ASA 的 WebVPN 服务器使用 HTTP POST 请求向 SSO 服务器提交单点登录 (SSO) 身份验证请求。如果身份验证成功，身份验证 Web 服务器将身份验证 Cookie 传回给客户端浏览器。然后客户端浏览器通过提供身份验证 Cookie，向 SSO 域中的其他 Web 服务器进行身份验证。**auth-cookie-name** 命令配置身份验证 Cookie 的名称以供 ASA 用于 SSO。

典型的身份验证 Cookie 格式是 Set-Cookie: *cookie name*=*cookie value* [;*cookie attributes*]。在以下身份验证 Cookie 示例中，SMSESSION 是使用 **auth-cookie-name** 命令配置的名称。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o
88uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma
5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;
Path=/
```

示例

在以下示例中，对从名称为 example.com 的 Web 服务器接收的身份验证 Cookie 指定身份验证 Cookie 名称 SMSESSION：

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	说明
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 Web 服务器 URI。
hidden-parameter	创建用于与身份验证 Web 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-parameter	指定用户名参数必须提交为用于 SSO 身份验证的 HTTP POST 请求的一部分。

authenticated-session-username

要指定当启用双重身份验证时与会话关联的身份验证用户名，请在 tunnel-group general-attributes 模式下使用 **authenticated-session-username** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

authenticated-session-username {**primary** | **secondary**}

no authenticated-session-username

语法说明

primary	使用来自主身份验证服务器的用户名。
secondary	使用来自辅助身份验证服务器的用户名。

默认值

默认值为 **primary**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

只有启用双重身份验证，此命令才有意义。**authenticated-session-username** 命令选择身份验证服务器，ASA 从中提取用户名以与会话关联。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的 IPsec 远程访问隧道组并指定将辅助身份验证服务器的用户名用于连接：

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
pre-fill-username	启用预先填写用户名功能。
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-from-certificate	在证书中指定要用作用于授权的用户名的字段。

authentication-attr-from-server

要指定当启用双重身份验证时将哪些身份验证服务器授权属性应用于连接，请在 tunnel-group general-attributes 模式下使用 **authentication-attr-from-server** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

authentication-attr-from-server {**primary** | **secondary**}

no authentication-attr-from-server

语法说明

primary	使用主身份验证服务器。
secondary	使用辅助身份验证服务器。

默认值

默认值为 **primary**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

只有启用双重身份验证，此命令才有意义。**authentication-attr-from-server** 命令选择身份验证服务器，ASA 从中提取要应用到连接的授权属性。

示例

以下示例在全局配置模式下输入，创建名为 remotegrp 的 IPsec 远程访问隧道组并指定将应用到连接的授权属性必须来自辅助身份验证服务器。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
pre-fill-username	启用预先填写用户名功能。
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-from-certificate	在证书中指定要用作用于授权的用户名的字段。

authentication-certificate

要从建立连接的 WebVPN 客户端要求证书，请在 webvpn 配置模式下使用 **authentication-certificate** 命令。要取消对客户端证书的要求，请使用此命令的 **no** 形式。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

语法说明

interface-name	用于建立连接的接口名称。可用接口名称如下： • **inside**　GigabitEthernet0/1 接口名称 • **outside**　GigabitEthernet0/0 接口名称

默认值

如果省略 **authentication-certificate** 命令，则禁用客户端证书身份验证。如果不使用 **authentication-certificate** 命令指定接口名称，则默认接口名称为 **inside**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要使此命令生效，必须在相应接口上已启用 WebVPN。使用 **interface**、**IP address** 和 **nameif** 命令配置并命名接口。

此命令仅适用于 WebVPN 客户端连接；但是，使用 **http authentication-certificate** 命令指定用于管理连接的客户端证书身份验证这一功能在所有平台都可用，包括不支持 WebVPN 的平台。

ASA 使用 PKI 信任点验证证书。如果证书没有通过验证，则会出现以下情形之一：

如果：	然后：
未启用 ASA 中嵌入的本地 CA。	ASA 关闭 SSL 连接。
启用本地 CA，但未启用 AAA 身份验证。	ASA 将客户端重新定向到本地 CA 的证书注册页面以获取证书。
本地 CA 和 AAA 身份验证都启用。	客户端重新定向到 AAA 身份验证页面。如果已进行配置，则还向客户端提供本地 CA 注册页面的链接。

示例

以下示例配置 outside 接口上用于 WebVPN 用户连接的证书身份验证：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
authentication (tunnel-group webvpn configuration mode)	指定隧道组的成员必须使用数字证书进行身份验证。
http authentication-certificate	指定通过与 ASA 的 ASDM 管理连接的证书进行身份验证。
interface	配置用于建立连接的接口。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl trust-point	配置 SSL 证书信任点。

authentication-exclude

要使最终用户浏览到配置的链接，且无需登录到无客户端 SSL VPN，请在 webvpn 配置模式下输入 **authentication-exclude** 命令。多次使用此命令可允许访问多个站点。

authentication-exclude *url-fnmatch*

语法说明

url-fnmatch	标识链接，通过这些链接可无需登录即连接到无客户端 SSL VPN。

命令默认值

已禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

当您需要一些内部资源可供公众通过 SSL VPN 使用时，此功能非常有用。

例如，您需要通过使用 SSL VPN 浏览至这些资源并将产生的 URL 复制到您分配的链接相关信息中，来将有关链接的信息分配给 SSL VPN 损坏形式的最终用户。

示例

以下示例展示如何使两个站点免于身份验证要求：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-exclude http://www.example.com/public/*
ciscoasa(config-webvpn)# authentication-exclude *example.html
ciscoasa(config-webvpn)# ciscoasa #
```

authentication

要配置 WebVPN 和邮件代理的身份验证方法，请在多种模式下使用 **authentication** 命令。若要恢复默认方法，请使用此命令的 **no** 形式。ASA 对用户进行身份验证以验证其身份。

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback**]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

语法说明

aaa	提供用户名和密码，ASA 使用它们与先前配置的 AAA 服务器进行核查。
certificate	提供 SSL 协商期间的证书。
mailhost	通过远程邮件服务器进行身份验证（仅适用于 SMTPS）。对于 IMAP4S 和 POP3S，mailhost 身份验证是必需的且不会显示为可配置选项。
piggyback	要求 HTTPS WebVPN 会话已存在。Piggyback 身份验证仅适用于邮件代理。

默认值

下表展示 WebVPN 和邮件代理的默认身份验证方法：

协议	默认身份验证方法
IMAP4S	Mailhost（必填）
POP3S	Mailhost（必填）
SMTPS	AAA
WebVPN	AAA

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
WebVPN 配置	• 是		• 是		

命令历史

版本	修改
8.0(2)	引入了此命令。
7.1(1)	此命令已在 WebVPN 配置模式下弃用并移至 WebVPN 的 tunnel-group webvpn-attributes 配置模式。
8.0(2)	修改了此命令以反映对证书身份验证要求的更改。

使用指南

至少需要一个身份验证方法。例如，对于 WebVPN，您可以指定 AAA 身份验证和 / 或证书身份验证。您可以按任意顺序输入这些命令。

WebVPN 证书身份验证要求 HTTPS 用户证书对于各接口是必要的。就是说，要使此选择可以操作，您必须在 **authentication-certificate** 命令中指定接口，才能指定证书身份验证。

如果在 webvpn 配置模式下输入此命令，它会转换为 tunnel-group webvpn-attributes 配置模式下的同一命令。

对于 WebVPN，您可能需要 AAA 和证书身份验证。在这种情况下，用户必须提供证书和用户名与密码。对于邮件代理身份验证，您可能需要多个身份验证方法。重新指定命令将覆盖当前配置。

示例

以下示例展示如何要求 WebVPN 用户提供证书进行身份验证。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

相关命令

命令	说明
authentication-certificate	请求建立连接的 WebVPN 客户端的证书。
show running-config	显示当前隧道组配置。
clear configure aaa	删除或重置已配置的 AAA 值。
show running-config aaa	显示 AAA 配置。

authentication eap-proxy

对于 L2TP over IPsec 连接，要启用 EAP 并允许 ASA 将 PPP 身份验证过程代理至外部 RADIUS 身份验证服务器，请在 tunnel-group ppp-attributes 配置模式下使用 **authentication eap-proxy** 命令。要将命令恢复其默认设置（允许 CHAP 和 MS-CHAP），请使用此命令的 **no** 形式。

authentication eap-proxy

no authentication eap-proxy

语法说明

此命令没有关键字或参数。

默认值

默认情况下，EAP 不是允许的身份验证协议。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Tunnel-group ppp-attributes 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

您只能将此属性应用到 L2TP 或 IPsec 隧道组类型。

示例

以下示例在 config-ppp 配置模式下输入，它对名称为 ppremotegrp 的隧道组允许 PPP 连接的 EAP：

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

相关命令

命令	说明
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示指定的证书映射条目。
tunnel-group-map default-group	将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联起来。

authentication key eigrp

要启用 EIGRP 数据包的身份验证并指定身份验证密钥，请在接口配置模式下使用 **authentication key eigrp** 命令。要禁用 EIGRP 身份验证，请使用此命令的 **no** 形式。

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

语法说明

as-number	经身份验证的 EIGRP 进程的自主系统编号。此值必须与为 EIGRP 路由进程配置的值相同。
key	用于对 EIGRP 更新进行身份验证的密钥。密钥可包含最多 16 个字符。
key-id *key-id*	密钥识别值；有效值范围为 1 到 255。

默认值

EIGRP 身份验证禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

您必须在接口上配置 **authentication mode eigrp** 和 **authentication key eigrp** 命令以启用 EIGRP 消息身份验证。使用 **show running-config interface** 命令查看在接口上配置的 **authentication** 命令。

示例

以下示例展示在 GigabitEthernet0/3 接口上配置 EIGRP 身份验证：

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

相关命令

命令	说明
authentication mode eigrp	指定用于 EIGRP 身份验证的身份验证类型。

authentication mode eigrp

要指定用于 EIGRP 身份验证的身份验证类型，请在接口配置模式下使用 **authentication mode eigrp** 命令。要恢复默认身份验证方式，请使用此命令的 **no** 形式。

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

语法说明

as-num	EIGRP 路由进程的自主系统编号。
md5	EIGRP 消息身份验证使用 MD5。

默认值

默认为不提供身份验证。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

您必须在接口上配置 **authentication mode eigrp** 和 **authentication key eigrp** 命令以启用 EIGRP 消息身份验证。使用 **show running-config interface** 命令查看在接口上配置的 **authentication** 命令。

示例

以下示例展示在 GigabitEthernet0/3 接口上配置 EIGRP 身份验证：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# authentication mode eigrp 100 md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

相关命令

命令	说明
authentication key eigrp	启用 EIGRP 数据包的身份验证并指定身份验证密钥。

authentication ms-chap-v1

对于 L2TP over IPsec 连接，要启用 PPP 的 Microsoft CHAP 版本 1 身份验证，请在 tunnel-group ppp-attributes 配置模式下使用 **authentication ms-chap-v1** 命令。要将命令恢复为默认设置（允许 CHAP 和 MS-CHAP），请使用此命令的 **no** 形式。要禁用 Microsoft CHAP 版本 1，请使用此命令的 **no** 形式。

authentication ms-chap-v1

no authentication ms-chap-v1

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Tunnel-group ppp-attributes 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

您只能将此属性应用到 L2TP 或 IPsec 隧道组类型。此协议类似于 CHAP，但是在此协议中服务器仅存储并比较加密密码而不是明文密码，所以安全性高于 CHAP。此协议还通过 MPPE 生成数据加密的密钥。

相关命令

命令	说明
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。

authentication ms-chap-v2

对于 L2TP over IPsec 连接，要启用 PPP 的 Microsoft CHAP 版本 2 身份验证，请在 tunnel-group ppp-attributes 配置模式下使用 **authentication ms-chap-v1** 命令。要将命令恢复其默认设置（允许 CHAP 和 MS-CHAP），请使用此命令的 **no** 形式。

authentication ms-chap-v2

no authentication ms-chap-v2

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Tunnel-group ppp-attributes 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

您只能将此属性应用到 L2TP 或 IPsec 隧道组类型。

此协议类似于 CHAP，但在此协议中服务器仅存储和比较加密密码而不是明文密码，所以安全性高于 CHAP。此协议还通过 MPPE 生成数据加密的密钥。

相关命令

命令	说明
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。

authentication pap

对于 L2TP over IPsec 连接，要允许 PPP 的 PAP 身份验证，请在 tunnel-group ppp-attributes 配置模式下使用 **authentication pap** 命令。要将命令恢复其默认设置（允许 CHAP 和 MS-CHAP），请使用此命令的 **no** 形式。

authentication pap

no authentication pap

语法说明

此命令没有关键字或参数。

默认值

默认情况下，PAP 不是允许的身份验证协议。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Tunnel-group ppp-attributes 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

您只能将此属性应用到 L2TP 或 IPsec 隧道组类型。

此协议在身份验证期间传递明文用户名和密码，因此并不安全。

示例

以下示例在 config-ppp 配置模式下输入，它对名称为 pppremotegrp 的隧道组允许 PPP 连接的 PAP：

```
ciscoasa(config)# tunnel-group pppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group pppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

相关命令

命令	说明
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示指定的证书映射条目。
tunnel-group-map default-group	将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联起来。

authentication-certificate

要从建立连接的 WebVPN 客户端要求证书，请在 webvpn 配置模式下使用 **authentication-certificate** 命令。要取消对客户端证书的要求，请使用此命令的 **no** 形式。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

语法说明

interface-name	用于建立连接的接口名称。可用接口名称如下： • **inside**　GigabitEthernet0/1 接口名称 • **outside**　GigabitEthernet0/0 接口名称

默认值

如果省略 **authentication-certificate** 命令，则禁用客户端证书身份验证。如果不使用 **authentication-certificate** 命令指定接口名称，则默认接口名称为 **inside**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要使此命令生效，必须在相应接口上已启用 WebVPN。使用 **interface**、**IP address** 和 **nameif** 命令配置并命名接口。

此命令仅适用于 WebVPN 客户端连接；但是，使用 **http authentication-certificate** 命令指定用于管理连接的客户端证书身份验证这一功能可用于所有平台，包括不支持 WebVPN 的平台。

ASA 使用 PKI 信任点验证证书。如果证书没有通过验证，则会出现以下情形之一：

如果：	然后：
未启用 ASA 中嵌入的本地 CA。	ASA 关闭 SSL 连接。
启用本地 CA，但未启用 AAA 身份验证。	ASA 将客户端重新定向到本地 CA 的证书注册页面以获取证书。
本地 CA 和 AAA 身份验证都启用。	客户端重新定向到 AAA 身份验证页面。如果已进行配置，则还向客户端提供本地 CA 注册页面的链接。

示例

以下示例配置 outside 接口上用于 WebVPN 用户连接的证书身份验证：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
authentication (tunnel-group webvpn configuration mode)	指定隧道组的成员必须使用数字证书进行身份验证。
http authentication-certificate	指定通过与 ASA 的 ASDM 管理连接的证书进行身份验证。
interface	配置用于建立连接的接口。
show running-config ssl	显示当前配置的 SSL 命令集。
ssl trust-point	配置 SSL 证书信任点。

authentication-port

要对此主机指定用于 RADIUS 身份验证的端口号，请在 aaa-server 配置主机配置模式下使用 **authentication-port** 命令。要删除身份验证端口指定，请使用此命令的 **no** 形式。

authentication-port *port*

no authentication-port

语法说明

port	RADIUS 身份验证的端口号，范围为 1 到 65535。

默认值

默认情况下，设备在端口 1645 上侦听 RADIUS（与 RFC 2058 一致）。如果没有指定端口，使用 RADIUS 身份验证默认端口号 1645。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server host configuration	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	对命令进行了语义更改，以支持基于每个主机对包含 RADIUS 服务器的服务器组指定服务器端口。

使用指南

此命令指定要分配身份验证功能的远程 RADIUS 服务器主机的目标 TCP/UDP 端口号。如果您的 RADIUS 身份验证服务器使用 1645 之外的端口，则必须将 ASA 配置给对应的端口，然后使用 **aaa-server** 命令启动 RADIUS 服务。

此命令仅对为 RADIUS 配置的服务器组有效。

示例

以下示例在主机 “1.2.3.4” 上配置名称为 “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，并配置身份验证端口 1650。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

相关命令

命令	说明
aaa authentication	在通过 **aaa-server** 命令或 ASDM 用户身份验证指定的服务器上启用或禁用 LOCAL、TACACS+ 或 RADIUS 用户身份验证。
aaa-server host	进入 AAA 服务器主机配置模式，在此模式下可以配置特定于主机的 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-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

authentication-server-group (imap4s, pop3s, smtps, config-mdm-proxy)

要指定一组身份验证服务器用于邮件代理和 MDM 代理，请在各种模式下使用 **authentication-server-group** 命令。要从配置中删除身份验证服务器，请使用此命令的 **no** 形式。

authentication-server-group *group_tag*

no authentication-server-group

语法说明

group_tag	标识先前配置的身份验证服务器或服务器组。

默认值

默认情况下没有配置任何身份验证服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
config-mdm-proxy 配置	• **是**	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(1)	此命令现已在 config-mdm-proxy 模式中可用。

使用指南

ASA 对用户进行身份验证以验证其身份。

如果您配置 AAA 身份验证，也必须配置此属性。否则，身份验证会一直失败。

使用 **aaa-server** 命令配置身份验证服务器。

示例

以下示例展示如何配置 IMAP4S 邮件代理使用名称为 “IMAP4SSVRS” 的一组身份验证服务器：

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

以下示例展示如何配置 MDM 代理使用名称为 “MDMSRVGRP” 的一组授权服务器：

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-pop3s)# authentication-server-group MDMSRVGRP
```

相关命令

命令	说明
aaa-server host	配置身份验证、授权和记账服务器。

authentication-server-group (tunnel-group general-attributes)

要指定 AAA 服务器组用于隧道组的用户身份验证，请在 tunnel-group general-attributes 配置模式下使用 **authentication-server-group** 命令。要恢复此属性的默认值，请使用此命令的 **no** 形式。

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

语法说明

interface_name	（可选）指定 IPsec 隧道终止所在的接口。
LOCAL	（可选）如果服务器组中的所有服务器由于通信故障而停用，则需要使用本地用户数据库进行身份验证。
server_group	标识先前配置的身份验证服务器或服务器组。

默认值

此命令中服务器组的默认设置是 **LOCAL**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令在 webvpn 配置模式中已弃用，并且已移至隧道组常规属性配置模式。
8.0(2)	增强了此命令以允许对 IPsec 连接进行每个接口的身份验证。

使用指南

您可以将此属性应用到所有隧道组类型。

使用 **aaa-server** 命令配置身份验证服务器，并使用 **aaa-server-host** 命令将服务器添加到先前配置的 AAA 服务器组。

示例

以下示例在 config-general 配置模式下输入，将名称为 aaa-server456 的身份验证服务器组配置给名称为 remotegrp 的 IPsec 远程访问隧道组：

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

相关命令

命令	说明
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。
aaa-server host	将服务器添加到先前配置的 AAA 服务器组并配置特定主机的 AAA 服务器参数。
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。

authorization-required

如果需要用户在连接之前成功授权，请在各种模式下使用 **authorization-required** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

authorization-required

no authorization-required

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令在 webvpn 配置模式中已弃用，并且已移至隧道组常规属性配置模式。
7.2(1)	使用 imap4s、pop3s 和 smtps 配置模式替换 webvpn 配置模式。

示例

以下示例在全局配置模式下输入，它需要基于完整 DN 的授权，用户才能通过名称为 remotegrp 的远程访问隧道组进行连接。第一个命令将隧道组类型 ipsec_ra（IPsec 远程访问）配置给名称为 remotegrp 的远程群组。第二个命令进入指定隧道组的 tunnel-group general-attributes 配置模式，最后一个命令指定命名的隧道组需要授权。

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

相关命令

命令	说明
authorization-dn-attributes	指定主要和辅助主题 DN 字段用作授权的用户名。
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示指定的证书映射条目。
tunnel-group general-attributes	指定命名的隧道组的常规属性。

authorization-server-group

要指定一组授权服务器以使用 WebVPN 和邮件代理，请在各种模式下使用 **authorization-server-group** 命令。要从配置中删除授权服务器，请使用此命令的 **no** 形式。

authorization-server-group *group_tag*

no authorization-server-group

语法说明

group_tag	标识先前配置的授权服务器或服务器组。使用 **aaa-server** 命令配置授权服务器。

默认值

默认情况下没有配置任何授权服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
隧道组常规属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令在 webvpn 配置模式中已弃用，并且已移至隧道组常规属性配置模式。

使用指南

ASA 使用授权以验证允许用户对网络资源的访问级别。

如果在 webvpn 配置模式下输入此命令，它会转换为 tunnel-group general-attributes 模式的相同命令。

当 VPN 授权定义为 LOCAL 时，强制执行默认组策略 DfltGrpPolicy 中配置的属性。

示例

以下示例展示如何配置 POP3S 邮件代理使用名称为 “POP3Spermit” 的一组授权服务器：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

以下示例在 tunnel-general 配置模式下输入，它将名称为 “aaa-server78” 的授权服务器组配置给名称为 “remotegrp” 的 IPsec 远程访问隧道组：

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

相关命令

命令	说明
aaa-server host	配置身份验证、授权和记账服务器。
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	指定命名的隧道组的常规属性。

auth-prompt

要指定或更改“通过 ASA”用户会话的 AAA 质询文本，请在全局配置模式下使用 **auth-prompt** 命令。要删除身份验证质询文本，请使用此命令的 **no** 形式。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

语法说明

accept	如果接受通过 Telnet 的用户身份验证，则显示提示 *string*。
prompt	AAA 质询提示字符串跟随在此关键字后面。
reject	如果拒绝通过 Telnet 的用户身份验证，则显示提示 *string*。
string	一个字符串，最多包含 235 个字母数字字符或 31 个单词，以两个最大值限制中先到达者为准。允许特殊字符、空格和标点符号。输入问号或按 **Enter** 键结束字符串。（问号出现在字符串中。）

默认值

如果不指定身份验证提示：

- FTP 用户看到 `FTP 身份验证`。
- HTTP 用户看到 `HTTP 身份验证`。
- Telnet 用户看不到任何质询文本。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	做了很小的语义更改。

使用指南

当需要 TACACS+ 或 RADIUS 服务器的用户身份验证时，可使用 **auth-prompt** 命令对通过 ASA 的 HTTP、FTP 和 Telnet 访问指定 AAA 质询文本。此文本主要用于装饰性用途并显示在当用户登录时看到的用户名和密码提示上方。

如果从 Telnet 进行用户的身份验证，您可以使用 **accept** 和 **reject** 选项显示不同状态提示，指出 AAA 服务器接受或拒绝身份验证尝试。

如果 AAA 服务器对用户进行身份验证，则 ASA 对用户显示 **auth-prompt accept** 文本（如果指定）；否则，显示 **reject** 文本（如果指定）。HTTP 和 FTP 会话的身份验证仅在提示时显示质询文本。不显示 **accept** 和 **reject** 文本。

注　Microsoft Internet Explorer 在身份验证提示中最多显示 37 个字符。Telnet 和 FTP 在身份验证提示中最多显示 235 个字符。

示例

以下示例将身份验证提示设置为字符串 “Please enter your username and password”：

```
ciscoasa(config)# auth-prompt prompt Please enter your username and password
```

在此字符串添加到配置后，用户将看到以下内容：

```
Please enter your username and password
User Name:
Password:
```

对于 Telnet 用户，当 ASA 接受或拒绝身份验证尝试时，您也可以提供要显示的单独消息；例如：

```
ciscoasa(config)# auth-prompt reject Authentication failed.Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

以下示例将身份验证成功的身份验证提示设置为字符串 “You’re OK.”

```
ciscoasa(config)# auth-prompt accept You’re OK.
```

在身份验证成功后，用户将看到以下消息：

```
You’re OK.
```

相关命令

命令	说明
clear configure auth-prompt	删除先前指定的身份验证提示质询文本并恢复为默认值（如果有）。
show running-config auth-prompt	显示当前身份验证提示质询文本。

auto-signon

要配置 ASA 将无客户端 SSL VPN 连接的用户登录凭证自动传递给内部服务器，请在以下三种模式中的任一模式下使用 **auto-signon** 命令：webvpn 配置、webvpn 组配置或 webvpn 用户名配置模式。要禁用自动登录到特定服务器，请使用此命令的 **no** 形式并搭配原始 **ip**、**uri** 和 **auth-type** 参数。要禁止自动登录到所有服务器，请使用此命令的 **no** 形式并不带参数。

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}]

语法说明

all	指定 NTLM 和 HTTP 基本身份验证方法。
allow	启用特定服务器的身份验证。
auth-type	启用身份验证方法的选择。
basic	指定 HTTP 基本身份验证方法。
ftp	Ftp 和 cifs 身份验证类型。
ip	指定 IP 地址和掩码以标识向其进行身份验证的服务器。
ip-address	与 *ip-mask* 一起使用，标识向其进行身份验证的服务器的 IP 地址范围。
ip-mask	与 *ip-address* 一起使用，标识向其进行身份验证的服务器的 IP 地址范围。
ntlm	指定 NTLMv1 身份验证方法。
resource-mask	标识向其进行身份验证的服务器的 URI 掩码。
uri	指定 URI 掩码以标识向其进行身份验证的服务器。

默认值

默认情况下，对所有服务器禁用此功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Webvpn 配置（全局）	• 是	—	• 是	—	—
Webvpn 组策略配置	• 是	—	• 是	—	—
Webvpn 用户名配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。
8.0(1)	增加了 NTLMv2 支持。**ntlm** 关键字包括 NTLMv1 和 NTLMv2。

使用指南

auto-signon 命令是无客户端 SSL VPN 用户的单点登录方法。它将登录凭证（用户名和密码）传递给内部服务器，以使用 NTLM 身份验证和 / 或 HTTP 基本身份验证进行身份验证。可输入多个自动登录命令并根据输入顺序进行处理（较早的命令优先处理）。

您可以在以下三种模式下使用自动登录功能：webvpn 配置组策略、webvpn 配置或 webvpn 用户名配置模式。应用典型的优先行为，其中用户名优先于组，组优先于全局。您选择的模式取决于所需的身份验证范围：

模式	适用范围
WebVPN 配置	所有 WebVPN 用户（全局）
Webvpn 组配置	组策略定义的 WebVPN 用户子集
Webvpn 用户名配置	个别 WebVPN 用户

示例

以下示例配置所有无客户端用户使用 NTLM 身份验证，自动登录到 IP 地址范围为 10.1.1.0 到 10.1.1.255 的服务器：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

以下示例配置所有无客户端用户使用 HTTP 基本身份验证，自动登录到 URI 掩码 https://*.example.com/* 定义的服务器：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

以下示例配置无客户端用户 ExamplePolicy 组策略使用 HTTP 基本或 NTLM 身份验证，自动登录到 URI 掩码 https://*.example.com/* 定义的服务器：

```
ciscoasa(config)# group-policy ExamplePolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

以下示例配置名为 Anyuser 的用户使用 HTTP 基本身份验证，自动登录到 IP 地址范围为 10.1.1.0 到 10.1.1.255 的服务器：

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

相关命令

命令	说明
show running-config webvpn auto-signon	显示运行配置的自动登录分配。

auto-summary

要启用将子网路由自动汇总到网络级路由，请在路由器配置模式下使用 **auto-summary** 命令。要禁用路由汇总，请使用此命令的 **no** 形式。

auto-summary

no auto-summary

语法说明

此命令没有任何参数或关键字。

默认值

为 RIP 版本 1、RIP 版本 2 和 EIGRP 启用路由汇总。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	增加了对 EIGRP 的支持。
9.0(1)	支持多情景模式。

使用指南

路由汇总可减少路由表中的路由信息数量。

RIP 版本 1 始终使用自动汇总。您无法对 RIP 版本 1 禁用自动汇总。

如果使用的是 RIP 版本 2，您可以通过指定 **no auto-summary** 命令关闭自动汇总。如果您必须在已断开连接的子网之间执行路由，则禁用自动汇总。当禁用自动汇总时，会通告子网。

EIGRP 汇总路由的管理距离值为 5。您无法配置此值。

在运行的配置中只出现此命令的 **no** 形式。

示例

以下示例禁用 RIP 路由汇总：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

以下示例禁用自动 EIGRP 路由汇总：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

相关命令

命令	说明
clear configure router	清除运行配置中的所有 **router** 命令和路由器配置模式命令。
router eigrp	启用 EIGRP 路由进程，然后进入 EIGRP 路由器配置模式。
router rip	启用 RIP 路由进程，然后进入 RIP 路由器配置模式。
show running-config router	显示运行配置中的 **router** 命令和路由器配置模式命令。

auto-update device-id

要配置 ASA 设备 ID 用于自动更新服务器，请在全局配置模式下使用 **auto-update device-id** 命令。要删除设备 ID，请使用此命令的 **no** 形式。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

语法说明

hardware-serial	使用 ASA 的硬件序列号唯一标识设备。
hostname	使用 ASA 的主机名唯一标识设备。
ipaddress [*if_name*]	使用 ASA 的 IP 地址唯一标识 ASA。默认情况下，ASA 使用与自动更新服务器通信所使用的接口。如果要使用不同的 IP 地址，请指定 *if_name* 选项。
mac-address [*if_name*]	使用 ASA 的 MAC 地址唯一标识 ASA。默认情况下，ASA 使用与自动更新服务器通信所使用的接口的 MAC 地址。如果要使用不同的 MAC 地址，请指定 *if_name* 选项。
string *text*	指定文本字符串以向自动更新服务器唯一标识设备。

默认值

默认 ID 是主机名。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例将设备 ID 设置为序列号：

```
ciscoasa(config)# auto-update device-id hardware-serial
```

相关命令

auto-update poll-period	设置 ASA 从自动更新服务器检查更新的频率。
auto-update server	标识自动更新服务器。
auto-update timeout	如果未在超时时间内连接到自动更新服务器，则阻止流量通过 ASA。
clear configure auto-update	清除自动更新服务器配置。
show running-config auto-update	显示自动更新服务器配置。

auto-update poll-at

要安排特定时间以供 ASA 轮询自动更新服务器，请在全局配置模式下使用 **auto-update poll-at** 命令。要删除安排给 ASA 轮询自动更新服务器的所有指定时间，请使用此命令的 **no** 形式。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

语法说明

days-of-the-week	任何一天或周内某些日的组合：周一、周二、周三、周四、周五、周六和周日。其他可能的值为每天（周一到周日）、工作日（周一到周五）和周末（周六和周日）。
randomize *minutes*	指定从指定开始时间之后的期间以随机化轮询时间。从 1 到 1439 分钟。
retry_count	指定第一次尝试失败后将尝试重新连接到自动更新服务器的次数。默认值为 0。
retry_period	指定连接尝试之间的等待时间。默认值为 5 分钟。范围为 1 到 35791 分钟。
time	以 HH:MM 格式指定开始轮询的时间。例如，8:00 是 8:00 AM，20:00 是 8:00 PM。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

auto-update poll-at 命令指定轮询更新的时间。如果启用 **randomize** 选项，会在第一个 *time* 选项和指定分钟数内的随机时间进行轮询。**auto-update poll-at** 和 **auto-update poll-period** 命令相互排斥。只能配置其中一个。

示例

在以下示例中，ASA 在每周五和周六晚上的以下时间内的随机时间轮询自动更新服务器：晚上 10:00 下午 11:00 前，提供四小时内响应的先行更换服务， 如果 ASA 无法连接到服务器，它将每 10 分钟再尝试两次。

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

相关命令

auto-update device-id	设置 ASA 设备 ID 用于自动更新服务器。
auto-update poll-period	设置 ASA 从自动更新服务器检查更新的频率。
auto-update timeout	如果未在超时时间内连接到自动更新服务器，则阻止流量通过 ASA。
clear configure auto-update	清除自动更新服务器配置。
management-access	启用对 ASA 上内部管理接口的访问。
show running-config auto-update	显示自动更新服务器配置。

auto-update poll-period

要配置 ASA 从自动更新服务器检查更新的频率，请在全局配置模式下使用 **auto-update poll-period** 命令。要将参数重置为默认值，请使用此命令的 **no** 形式。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

语法说明

poll_period	指定轮询自动更新服务器的频率，以分钟为单位且在 1 和 35791 之间。默认值为 720 分钟（12 小时）。
retry_count	指定第一次尝试失败后将尝试重新连接到自动更新服务器的次数。默认值为 0。
retry_period	指定连接尝试之间等待的时长，以分钟为单位且在 1 和 35791 之间。默认值为 5 分钟。

默认值

默认轮询周期是 720 分钟（12 小时）。

第一次尝试失败后将尝试重新连接到自动更新服务器的默认次数为 0。

在连接尝试之间等待的默认时间为 5 分钟。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

auto-update poll-at 和 **auto-update poll-period** 命令相互排斥。只能配置其中一个。

示例

以下示例将轮询周期设置为 360 分钟、重试次数设置为 1 及重试时间设置为 3 分钟：

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

相关命令

auto-update device-id	设置 ASA 设备 ID 用于自动更新服务器。
auto-update server	标识自动更新服务器。
auto-update timeout	如果未在超时时间内连接到自动更新服务器，则阻止流量通过 ASA。
clear configure auto-update	清除自动更新服务器配置。
show running-config auto-update	显示自动更新服务器配置。

auto-update server

要标识自动更新服务器，请在全局配置模式下使用 **auto-update server** 命令。要删除服务器，请使用此命令的 **no** 形式。

auto-update server *url* [**source** *interface*] {**verify-certificate** | **no-verification**}

no auto-update server *url* [**source** *interface*] {**verify-certificate** | **no-verification**}

语法说明

no-verification	不验证自动更新服务器证书。
source *interface*	指定将请求发送到自动更新服务器时要使用的接口。如果指定 **management-access** 命令所指定的同一接口，自动更新请求将通过用于管理访问的相同 IPsec VPN 隧道。
url	使用以下语法指定自动更新服务器的位置： **http**[**s**]**:**[[*user:password*@]*location* [*:port*]] **/** *pathname*
verify-certificate	对于 HTTPS，验证自动更新服务器返回的证书。此为默认设置。

默认值

9.1 及更低版本：禁用证书验证。

9.2(1) 及更高版本：默认情况下启用 **verify-certificate** 选项。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	修改了此命令以增加对多个服务器的支持。
9.2(1)	默认情况下启用自动更新服务器证书验证。添加了 **no-verification** 关键字。

使用指南

ASA 定期连接自动更新服务器以获取所有配置、操作系统和 ASDM 更新。

您可以配置多个服务器以使用自动更新。当检查更新时，会连接到第一台服务器，但如果失败，则连接下一台服务器。此过程会一直继续下去，直到尝试了所有服务器。如果所有服务器都无法连接，且已配置自动更新轮询周期来重试连接，则会尝试从第一个服务器开始重试。

要使正常自动更新功能正确运行，您必须使用 **boot system configuration** 命令并确保它指定有效的启动映像。此外，您必须搭配自动更新使用 **asdm image** 命令以更新 ASDM 软件映像。

如果在 **source** *interface* 参数中指定的接口是使用 **management-access** 命令指定的同一接口，则通过 VPN 隧道发送对自动更新服务器的请求。

9.2(1) 及更高版本：默认情况下已启用自动更新服务器证书验证；对于新的配置，您必须明确禁用证书验证。如果您从较早版本升级并且没有启用证书验证，则证书验证不启用并且出现以下警告：

```
WARNING: The certificate provided by the auto-update servers will not be verified.In order
to verify this certificate please use the verify-certificate option.
```

将迁移配置以明确配置不验证：

auto-update server no-verification

示例

以下示例设置自动更新服务器 URL 并将接口指定为 outside：

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside
verify-certificate
```

相关命令

auto-update device-id	设置 ASA 设备 ID 用于自动更新服务器。
auto-update poll-period	设置 ASA 从自动更新服务器检查更新的频率。
auto-update timeout	如果未在超时时间内连接到自动更新服务器，则阻止流量通过 ASA。
clear configure auto-update	清除自动更新服务器配置。
management-access	启用对 ASA 上内部管理接口的访问。
show running-config auto-update	显示自动更新服务器配置。

auto-update timeout

要设置连接自动更新服务器的超时时间，请在全局配置模式下使用 **auto-update timeout** 命令。要删除超时，请使用此命令的 **no** 形式。

auto-update timeout [*period*]

no auto-update timeout [*period*]

语法说明

period	指定超时时间，以分钟为单位且在 1 和 35791 之间。默认值为 0，表示没有超时。您不能将超时设置为 0；使用该命令的 **no** 形式可将其重置为 0。

默认值

默认超时值为 0，表示 ASA 设置为永不超时。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用系统日志消息 201008 报告超时情况。

如果在超时时间内尚未连接自动更新服务器，ASA 将阻止所有流量通过。设置超时以确保 ASA 具有最新的映像和配置。

示例

以下示例将超时设置为 24 小时：

```
ciscoasa(config)# auto-update timeout 1440
```

相关命令

auto-update device-id	设置 ASA 设备 ID 用于自动更新服务器。
auto-update poll-period	设置 ASA 从自动更新服务器检查更新的频率。
auto-update server	标识自动更新服务器。
clear configure auto-update	清除自动更新服务器配置。
show running-config auto-update	显示自动更新服务器配置。

backup 至 browse-networks 命令

备份

要备份 ASA 配置、证书、密钥和映像，请在特权 EXEC 模式下使用 **backup** 命令。

backup [**/noconfirm**] [**context** *name*] [**cert-passphrase** *value*] [**location** *path*]

语法说明

cert-passphrase *value*	在备份 VPN 证书和预共享密钥时，需要由 **cert-passphrase** 关键字标识的密钥才可对证书进行编码。必须提供要用于编码和解码 PKCS12 格式证书的口令。备份仅包括绑定至证书的 RSA 密钥对，不包括任何独立证书。
context *ctx-name*	在系统执行空间的多情景模式下，输入 **context** 关键字以备份指定的情景文件。
location *path*	备份**位置**可以是本地磁盘或远程 URL。如果您未提供位置，则使用以下默认名称： • 单模 - disk0:*hostname*.backup.*timestamp*.tar.gz • 多模式 - disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
/noconfirm	指定不提示的**位置**和**证明，密码短语**的参数。可以绕过警告和错误消息以继续进行备份。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

请参阅以下指导原则：

- 开始备份之前，备份位置应至少有 300 MB 的可用磁盘空间。
- 如果您更改任何配置，期间或之后备份，备份不会有这些变化。如果更改配置进行备份，然后执行恢复后的，此配置更改，将会覆盖。这样一来，ASA 行为可能不同。
- 一次只能启动一个备份。
- 您仅可恢复配置到同一 ASA 版本为您执行原始的备份。您无法使用恢复工具迁移配置从 ASA 到另一个版本。如果配置迁移是必需的 ASA 自动升级驻地的启动配置时，它会加载新 ASA 操作系统。

- 如果您使用集群，则只能备份启动配置、运行配置和身份证书。您必须创建和恢复备份单独为每个单元。
- 如果您使用故障切换，您必须创建和恢复备份单独的主用和备用设备。
- 如果您针对 ASA 设置主密码，则您需要该主密码短语恢复您使用此过程创建的备份配置。如果您不知道针对 ASA 的主密码时，请参阅 CLI 配置指南要了解如何重置密码才能继续与备份。
- 如果您导入 PKCS12 数据（使用 **crypto ca trustpoint** 命令）和信任点使用 RSA 密钥，导入的密钥对分配信任点相同的名称。由于此限制，如果您指定不同名称信任点和其密钥对，在恢复 ASDM 配置后，启动配置将能与原始配置相同，但运行配置将包括不同密钥对的名称。这意味着，如果您使用不同密钥对和信任点的名称，您无法恢复原始配置。要解决此问题，请确保您使用相同的名称为信任点和其密钥对。
- 无法使用 CLI 备份和恢复使用 ASDM，反之亦然。
- 每个备份文件包括以下内容：
  - 运行配置
  - 启动配置
  - 所有安全映像

    Cisco Secure Desktop 和 Host Scan 映像

    Cisco Secure Desktop 和 Host Scan 设置

    AnyConnect (SVC) 客户端映像和配置文件

    AnyConnect (SVC) 的自定义和转换
  - ID 书（包括 RSA 密钥对与 ID 书；不包括独立密钥）
  - VPN 的预共享密钥
  - SSL VPN 配置
  - 应用配置文件的自定义框架（生产能力）
  - 书签
  - 自定义设置
  - 动态访问策略 (DAP)
  - 插件
  - 连接配置文件的预填充脚本
  - 代理自动配置
  - 转换表
  - Web 内容
  - 版本信息

示例

以下示例展示如何创建备份：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!
```

```
Enter a passphrase to encrypt identity certificates.The default is cisco.You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption.If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the
current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

相关命令

命令	说明
restore	从备份文件恢复 ASA 配置、密钥、证书和映像。

backup interface

对于具有内置交换机的型号（如 ASA 5505），请在接口配置模式下使用 **backup interface** 命令将 VLAN 接口标识为例如到 ISP 的备用接口。要恢复正常运行，请使用此命令的 **no** 形式。

backup interface vlan *number*

no backup interface vlan *number*

语法说明

vlan *number*	指定备用接口的 VLAN ID。

默认值

默认情况下，**backup interface** 命令已禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
7.2(2)	Security Plus 许可证不再将正常流量的 VLAN 接口数量限制为 3，备用接口限制为 1 和故障切换限制为 1；您现在可以配置最多 20 个接口而没有任何其他限制。因此，无需 **backup interface** 命令即可启用超过 3 个接口。

使用指南

此命令只能在接口配置模式下对 VLAN 接口输入。此命令阻止所标识备用接口上所有通过的流量，除非通过主要接口的默认路由关闭。

使用 **backup interface** 命令配置 Easy VPN 后，如果备用接口变为主要接口，则 ASA 将 VPN 规则移至新的主要接口。请参阅 **show interface** 命令以查看备用接口的状态。

请确保在主要和备用接口上均已配置默认路由，以便主要接口发生故障时可以使用备用接口。例如，可以配置两个默认路由：一个用于较短管理距离的主要接口，一个用于较长距离的备用接口。请参阅 **dhcp client route distance** 命令以覆盖从 DHCP 服务器获取的默认路由的管理距离。要配置双 ISP 支持，请参阅 **sla monitor** 和 **track rtr** 命令以了解详细信息。

接口上已配置 **management-only** 命令时，您将无法配置备用接口。

示例

以下示例配置四个 VLAN 接口。backup-isp 接口仅当主要接口关闭时允许通过流量。**route** 命令创建主要和备用接口的默认路由，备用路由管理距离较短。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# backup interface vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

相关命令

命令	说明
forward interface	限制接口发起到另一个接口的流量。
interface vlan	创建 VLAN 接口并进入接口配置模式。
dhcp client route distance	覆盖从 DHCP 服务器获取的默认路由的管理距离。
sla monitor	创建静态路由跟踪的 SLA 监控操作。
track rtr	跟踪 SLA 监控操作状态。

backup-servers

要配置备用服务器，请在 group-policy 配置模式下使用 **backup-servers** 命令。要删除备用服务器，请使用此命令的 **no** 形式。

backup-servers {*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**}

no backup-servers [*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**]

语法说明

clear-client-config	指定客户端不使用备用服务器。ASA 将推送空服务器列表。
keep-client-config	指定 ASA 不将备用服务器信息发送到客户端。客户端使用自己的备用服务器列表（如果已配置）。
server1 server 2....server10	当主要 ASA 不可用时，为 VPN 客户端提供空格分隔、按优先级排序的服务器列表。通过 IP 地址或主机名来识别服务器。列表长度可为 500 个字符，但只能包含 10 个条目。

默认值

备用服务器不存在，直到您在客户端或主要 ASA 上进行配置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要从运行的配置中删除 backup-servers 属性，请使用此命令的 **no** 形式且不带参数。这样可实现从另一个组策略继承备用服务器的值。

主要 ASA 不可用时，IPsec 备用服务器允许 VPN 客户端连接到中心站点。当您配置备用服务器时，ASA 会在建立 IPsec 隧道时将服务器列表推送到客户端。

在客户端或主要 ASA 上配置备用服务器。如果您在 ASA 上配置了备用服务器，它会将备用服务器策略推送到组中的客户端，从而取代客户端上的备用服务器列表（如果已配置）。

注　如果使用主机名，最好将备用 DNS 和 WINS 服务器置于与主要 DNS 和 WINS 服务器不同的网络。否则，如果硬件客户端背后的客户端通过 DHCP 从硬件客户端获取 DNS 和 WINS 信息，则与主要服务器的连接将丢失，并且备用服务器具有不同的 DNS 和 WINS 信息，客户端无法更新，直至 DHCP 租用到期。此外，如果使用主机名且 DNS 服务器不可用，则可能出现显著延迟。

示例

以下示例展示如何使用 IP 地址 10.10.10.1 和 192.168.10.14 为名为 “FirstGroup” 的组策略配置备用服务器：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

要配置 ASDM、会话、登录或 message-of-the-day 标语，请在全局配置模式下使用 **banner** 命令。要从指定的标语关键字（**exec**、**login** 或 **motd**）删除所有行，请使用此命令的 **no** 形式。

banner {**asdm** | **exec** | **login** | **motd** *text*}

[**no**] **banner** {**asdm** | **exec** | **login** | **motd** [*text*]}

语法说明

asdm	将系统配置为在成功登录到 ASDM 后显示标语。系统将提示用户继续完成登录，或断开连接。此选项允许您要求用户在连接之前接受书面策略的条款。
exec	将系统配置为在显示 enable 提示符之前显示标语。
login	将系统配置为使用 Telnet 或串行控制台访问 ASA 时，在密码登录提示符之前显示标语。
motd	将系统配置为当您初次连接时显示 message-of-the-day 标语。
text	要显示的消息文本行。

默认值

默认值为无标语。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(4)/8.0(3)	添加了 **asdm** 关键字。
9.0(1)	**banner login** 命令支持串行控制台连接。

使用指南

banner 命令配置指定关键字要显示的标语。*text* 字符串包含第一个空白字符（空格）之后直到行尾（回车或换行符 [LF]）的所有字符。文本中的空格将被保留。但是，您无法通过 CLI 输入制表符。

除非首先清除标语，否则后续的 *text* 条目都将添加到现有标语的结尾。

注　标记 $(domain) 和 $(hostname) 将替换为 ASA 的主机名和域名。在情景配置中输入 $(system) 标记后，该情景会使用系统配置中所配置的标语。

标语中的多行通过为要添加的每一行输入一条新的 banner 命令进行处理。然后，每一行将附加到现有标语的结尾。

注　标语授权提示符的最大长度为 235 个字符或 31 个单词，以首先达到的限制为准。

通过 Telnet 或 SSH 访问 ASA 时，如果没有足够的系统内存可用于处理标语消息，或如果发生 TCP 写入错误，则会话将关闭。只有 **exec** 和 **motd** 标语支持通过 SSH 访问 ASA。登录标语不支持 SSHv1 客户端或 SSH 客户端，这些客户端不会将用户名作为初始连接的一部分传递。

要更换标语，请在添加新行之前使用 **no banner** 命令。

使用 **no banner** {**exec** | **login** | **motd**} 命令删除指定标语关键字的所有行。

no banner 命令不会选择性删除文本字符串，因此您在 **no banner** 命令结尾输入的任何*文本*都将被忽略。

示例

以下示例展示如何配置 **asdm**、**exec**、**login** 和 **motd** 标语：

```
ciscoasa(config)# banner asdm You successfully logged in to ASDM
ciscoasa(config)# banner motd Think on These Things
ciscoasa(config)# banner exec Enter your password carefully
ciscoasa(config)# banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

以下示例展示如何将第二行添加到 **motd** 标语：

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

相关命令

命令	说明
clear configure banner	删除所有标语。
show running-config banner	显示所有标语。

banner (group-policy)

要在远程客户端连接时在其上显示标语或欢迎文本，请在 group-policy 配置模式下使用 **banner** 命令。要删除标语，请使用此命令的 **no** 形式。

banner {**value** *banner_string* | **none**}

no banner

注　如果根据 VPN 组策略配置了多个标语，并且删除了任一标语，则所有标语都将被删除。

语法说明

none	使用空值设置标语，从而禁止标语。阻止从默认或指定的组策略继承标语。
value *banner_string*	构成标语文本。最大字符串大小为 500 个字符。使用 “\n” 序列插入回车。

默认值

没有默认标语。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要防止继承标语，请使用 **banner none** 命令。

IPsec VPN 客户端支持标语的完全 HTML。但是，无客户端门户和 AnyConnect 客户端支持部分 HTML。要确保标语对远程用户正常显示，请遵循以下原则：

- 对于 IPsec 客户端用户，请使用 /n 标记。
- 对于 AnyConnect 客户端用户，请使用
 标记。
- 对于无客户端用户，请使用
 标记。

示例

以下示例展示如何为名为 “FirstGroup” 的组策略创建标语：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

bgp aggregate-timer

要设置 BGP 路由将汇聚的间隔或禁用基于计时器的路由汇聚，请在地址系列配置模式下使用 **bgp aggregate-timer** 命令。要恢复默认值，请使用此命令的 **no** 形式。

bgp aggregate-timer *seconds*

no bgp aggregate-timer

语法说明

seconds	系统将汇聚 BGP 路由的间隔（以秒为单位）。 有效值位于从 6 到 60 的范围，否则为 0（零）。 默认值为 30。 值为 0（零）将禁用基于计时器的汇聚并立即开始汇聚。

默认值

bgp 汇聚计时器的默认值为 30 秒。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置、地址系列 IPv6 子模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令修改为在地址系列 IPv6 子模式下受支持。

使用指南

使用此命令以更改 BGP 路由汇聚的默认间隔。

在非常大的配置中，即使 **aggregate-address summary-only** 命令已配置，更具体的路由仍会通告并在稍后撤消。为避免这种行为，请将 **bgp aggregate-timer** 配置为 0（零），系统将立即检查汇聚路由并抑制特定的路由。

示例

以下示例以 20 秒的间隔配置 BGP 路由汇聚：

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

以下示例立即开始 BGP 路由汇聚：

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话。
aggregate-address	创建边界网关协议 (BGP) 数据库中的汇聚条目。

bgp always-compare-med

要允许比较不同自主系统中邻居路径的多出口标识符 (MED)，请在路由器配置模式下使用 **bgp always-compare-med** 命令。要禁止比较，请使用此命令的 **no** 形式。

bgp always-compare-med

no bgp always-compare-med

语法说明

此命令没有任何参数或关键字。

默认值

如果此命令未启用或输入了此命令的 **no** 形式，则 ASA 路由软件不会比较不同自主系统中邻居路径的 MED。

MED 仅当所比较路由的自主系统路径相同时进行比较。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

MED（如 RFC 1771 中所述）是一个可选的非过渡属性，为 4 位八进制非负整数。此属性的值可供 BGP 最佳路径选择过程用于分辨到相邻自主系统的多个出口点。

MED 是在多条备用路径中选择最佳路径时应考虑的参数之一。较低 MED 的路径优先于较高 MED 的路径。在最佳路径选择过程中，MED 比较仅在同一自主系统的路径之间进行。**bgp always-compare-med** 命令用于通过在所有路径（无论从哪个自主系统接收路径）之间实施 MED 比较来改变这种行为。

bgp deterministic-med 命令可配置为在从同一自主系统内接收的所有路径之间实施 MED 值的确定性比较。

示例

在以下示例中，本地 BGP 路由进程配置为比较备用路径（无论从哪个自主系统接收路径）的 MED：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

相关命令

命令	说明
bgp deterministic-med	在从同一自主系统内接收的所有路径之间实施多出口标识符 (MED) 值的确定性比较。

bgp asnotation dot

要将边界网关协议 (BGP) 4 字节自主系统编号的默认显示和正则表达式匹配格式从 asplain（十进制值）更改为点表示法，请在路由器配置模式下使用 **bgp asnotation dot** 命令。要将默认的 4 字节自主系统编号显示和正则表达式匹配格式重置为 asplain，请使用此命令的 **no** 形式。

bgp asnotation dot

no bgp asnotation dot

语法说明

此命令没有任何参数或关键字。

默认值

BGP 自主系统编号在屏幕输出中使用 asplain（十进制值）格式显示，且正则表达式中匹配 4 字节自主系统编号的默认格式为 asplain。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

在 2009 年 1 月以前，分配给公司的 BGP 自主系统编号是范围为 1 到 65535 的 2 个八进制数字，如 RFC 4271 的*边界网关协议 4 (BGP-4)* 中所规定。

由于自主系统编号需求的增加，互联网编号授权委员会 (IANA) 从 2009 年 1 月开始将分配范围为 65536 到 4294967295 的 4 个八位组自主系统编号。RFC 5396 的*自主系统 (AS) 编号的文本表示*部分记录了表示自主系统编号的三种方法。思科 /Cisco 已实施以下两种方法：

- Asplain - 这两个 2 字节和 4 字节的自主系统号由其十进制数值的十进制数值记法。例如，65526 是 2 字节自主系统编号和 234567 是 4 字节的自主系统编号。
- Asdot- 自主系统 dot 记法，其中 2 个字节的自主系统编号由其十进制数值，由 dot 记法表示 4 字节的自主系统编号。例如，65526 是 2 字节的自主系统编号，而 1.169031 是 4 字节的自主系统编号（这是 234567 十进制数值的点表示法）。

思科实施 4 字节自主系统编号，使用 asplain 作为自主系统编号的默认显示格式，但您可以同时配置 asplain 和 asdot 格式的 4 字节自主系统编号。此外，正则表达式中匹配 4 字节自主系统编号的默认格式为 asplain，因此，您必须确保匹配 4 字节自主系统编号的所有正则表达式均以 asplain 格式书写。如果要将默认的 **show** 命令输出更改为显示 asdot 格式的 4 字节自主系统编号，请在路由器配置模式下使用 **bgp asnotation dot** 命令。当 asdot 格式启用为默认值时，必须使用 asdot 格式写入用来匹配 4 字节自主系统编号的所有正则表达式，否则正则表达式匹配将失败。下表展示尽管您可以将 4 字节自主系统编号配置为 asplain 或 asdot 格式，但只有一种格式用于显示 **show** 命令输出和控制正则表达式的 4 字节自主系统编号匹配，默认值为 asplain 格式。

要以 asdot 格式在 **show** 命令输出中显示 4 字节自主系统编号和控制正则表达式的匹配，您必须配置 **bgp asnotation dot** 命令。启用 **bgp asnotation dot** 命令后，必须通过输入 **clearbgp *** 命令对所有 BGP 会话启动硬重置。

表 4-1　默认 Asplain 4 字节自主系统编号格式

格式	配置格式	Show 命令输出和正则表达式匹配格式
asplain	2 字节：1 至 6553 4 字节：65536 至 4294967295	2 字节：1 至 6553 4 字节：65536 至 4294967295
asdot	2 字节：1 至 6553 4 字节：1.0 至 65535.65535	2 字节：1 至 6553 4 字节：65536 至 4294967295

表 4-2　Asdot 4 字节自主系统编号格式

格式	配置格式	Show 命令输出和正则表达式匹配格式
asplain	2 字节：1 至 65535 4 字节：65536 至 4294967295	2 字节：1 至 65535 4 字节：1.0 至 65535.65535
asdot	2 字节：1 至 65535 4 字节：1.0 至 65535.65535	2 字节：1 至 65535 4 字节：1.0 至 65535.65535

示例

show bgp summary 命令的以下输出展示默认 asplain 格式的 4 字节自主系统编号。注意 asplain 格式的 4 字节自主系统编号，65536 和 65550。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15       0
```

系统执行以下配置以将默认输出格式更改为 asdot 表示法格式：

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

执行配置后，输出将转换为 asdot 表示法格式，如 **show bgp summary** 命令的以下输出中所示。注意 asdot 格式的 4 字节自主系统编号 1.0 和 1.14（这些是 65536 和 65550 自主系统编号的 asdot 转换）。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13       0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24       0
```

配置 **bgp asnotation dot** 命令后，4 字节自主系统路径的正则表达式匹配格式更改为 asdot 表示法格式。尽管 4 字节自主系统编号可在正则表达式中使用 asplain 格式或 asdot 格式进行配置，但只有使用当前默认格式配置的 4 字节自主系统编号匹配。在第一个示例中，**show bgp regexp** 命令采用 asplain 格式的 4 字节自主系统编号进行配置。匹配失败是因为默认格式当前为 asdot 格式且没有输出。在使用 asdot 格式的第二个示例中，匹配通过并且关于 4 字节自主系统路径的信息使用 asdot 表示法展示。

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

注　asdot 表示法使用句点，后者在思科正则表达式中为特殊字符。要消除特殊含义，请在点号之前使用反斜线。

相关命令

命令	说明
show bgp summary	显示所有边界网关协议 (BGP) 连接的状态。
show bgp regexp	显示匹配自主系统路径正则表达式的路由。

bgp bestpath compare-routerid

要配置边界网关协议 (BGP) 路由进程以在最佳路径选择过程中比较从不同外部对等设备接收的相同路由并选择具有最低路由器 ID 的路由作为最佳路径，请在路由器配置模式下使用 **bgp bestpath compare-routerid** 命令。

要将 BGP 路由进程恢复为默认操作，请使用此命令的 **no** 形式。

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

语法说明

此命令没有任何参数或关键字。

默认值

此命令的行为在默认情况下已禁用； BGP 在具有相同属性的两个路由接收时选择先收到的路由。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp bestpath compare-routerid 命令用于将 BGP 路由进程配置为使用路由器 ID 作为从两个不同对等设备接收两个相同路由（除路由器 ID 以外的所有属性均相同）时最佳路径选择的决定项。此命令启用后，如果所有其他属性均相同，将选择最低路由器 ID 作为最佳路径。

示例

在以下示例中，BGP 路由进程配置为比较和使用路由器 ID 作为从不同对等设备接收相同路径时最佳路径选择的决定项：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

要将边界网关协议 (BGP) 路由进程配置为分配无限大值到缺少多出口标识符 (MED) 属性的路由（使不带 MED 值的路径成为最不理想的路径），请在路由器配置模式下使用 **bgp bestpath med missing-as-worst** 命令。要使路由器恢复默认行为（将值 0 分配给缺少的 MED），请使用此命令的 **no** 形式。

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

语法说明

此命令没有任何参数或关键字。

默认值

ASA 软件将值 0 分配给缺少 MED 属性的路由，导致缺少 MED 属性的路由被视为最佳路径。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

在以下示例中，BGP 路由器进程配置为将缺少 MED 属性的路由视为具有无限大值 (4294967294)，从而使此路径成为最不理想的路径：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp default local-preference

要更改默认本地优先级值，请在路由器配置模式下使用 **bgp default local-preference** 命令。要将本地优先级值恢复为默认设置，请使用此命令的 **no** 形式。

bgp default local-preference *number*

no bgp default local-preference *number*

语法说明

number	从 0 到 4294967295 的本地优先级值。

默认值

如果此命令未启用或输入了此命令的 **no** 形式，则 ASA 软件应用本地优先级值 100。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

本地优先级属性是用于在 BGP 最佳路径选择过程中将优先级程度应用到路由的自由选择属性。此属性仅在 iBGP 对等设备之间进行交换，用于确定本地策略。首选使用具有最高本地优先级的路由。

示例

在以下示例中，本地优先级值设置为 200：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

要在从同一自主系统内接收的所有路径之间实施多出口标识符 (MED) 值的确定性比较，请在路由器配置模式下使用 **bgp deterministic-med** 命令。要禁用所需的 MED 比较，请使用此命令的 **no** 形式。

bgp deterministic-med

no bgp deterministic-med

语法说明

此命令没有任何参数或关键字。

默认值

ASA 软件不会在从同一自主系统内接收的所有路径之间实施 MED 变量的确定性比较。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp always-compare-med 命令用于启用对不同自主系统中邻居路径的多出口标识符 (MED) 比较。配置 **bgp always-compare-med** 命令后，从不同邻居（位于同一自主系统中）接收的、相同前缀的所有路径都将分在一组中并按 MED 值升序排列（仅接收路径将被忽略，不会进行分组或排序）。

然后，最佳路径选择算法将使用现有规则选择最佳路径；比较基于每个邻居自主系统然后再基于全局进行。此命令输入后，将立即进行路径分组和排序。为获得正确的结果，本地自主系统中的所有路由器必须启用（或禁用）此命令。

示例

在以下示例中，BGP 配置为在通过联盟内同一子自主系统通告的路由的路径选择过程中比较 MED：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

以下示例 **show bgp** 命令输出展示如何通过配置 **bgp deterministic-med** 命令影响路由选择。如果未启用 **bgp deterministic-med** 命令，则路由接收顺序将影响最佳路径选择的路由选择方式。**show bgp** 命令的以下示例输出展示收到相同前缀 (10.100.0.0) 的三条路径，并且 **bgp deterministic-med** 命令未启用：

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

如果路由器上未启用 bgp deterministic-med 功能，则路由接收顺序可能会影响路由选择。考虑路由器收到相同前缀的三条路径的以下场景：

输入 **clear bgp *** 命令以清除本地路由表中的所有路由。

```
ciscoasa(router)# clear bgp *
```

重新填充路由表后，再次发出 **show bgp** 命令。请注意，清除 BGP 会话后，路径顺序将发生变化。由于第二个会话的路径接收顺序不同，因此选择算法结果也会发生变化。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

如果 **bgp deterministic-med** 命令已启用，则选择算法的结果将始终相同，无论本地路由器接收路径的顺序如何。此场景下，在本地路由器上输入 **bgp deterministic-med** 命令后，始终生成以下输出：

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

相关命令

命令	说明
bgp always compare-med	允许对不同自主系统中邻居路径的多出口标识符 (MED) 比较。
clear bgp	使用软或硬重新配置重置 BGP 连接。
show bgp	显示边界网关协议 (BGP) 路由表中的条目。

bgp enforce-first-as

要将 ASA 配置为拒绝从传入更新中 AS_PATH 开头未列出其自主系统编号的外部 BGP (eBGP) 对等设备接收的更新，请在路由器配置模式下使用 **bgp enforce-first-as** 命令。要禁用此行为，请使用此命令的 **no** 形式。

bgp enforce-first-as

no bgp enforce-first-as

语法说明

此命令没有任何参数或关键字。

默认值

此命令的行为在默认情况下已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp enforce-first-as 命令用于拒绝从未列出其自主系统编号作为 AS_PATH 属性中第一段的 eBGP 对等设备接收的传入更新。启用此命令可阻止错误配置或未授权的对等设备通过将路由通告为如同源自另一个自主系统来错误指示流量（欺骗本地路由器）。

示例

在以下示例中，将检查来自 eBGP 对等设备的所有传入更新，以确保 AS_PATH 中的第一个自主系统编号为传输对等设备的本地 AS 编号。在以下示例中，如果第一个 AS 编号不是 65001，则来自 10.100.0.1 对等设备的更新将被丢弃：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 路由表。

bgp fast-external-fallover

要将边界网关协议 (BGP) 路由进程配置为在用于访问这些对等设备的链路断开时立即重置外部 BGP 对等会话，请在路由器配置模式下使用 **bgp fast-external-fallover** 命令。要禁用 BGP 快速外部故障切换，请使用此命令的 **no** 形式。

bgp fast-external-fallover

no bgp fast-external-fallover

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，BGP 快速外部故障切换已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp fast-external-fallover 命令用于禁用或启用 BGP 对等会话与直连外部对等设备的快速外部故障切换。如果链路断开，会话将立即重置。仅支持直连对等会话。如果 BGP 快速外部故障切换已禁用，则 BGP 路由进程将等待直到默认的保持计时器过期（3 个 keepalive）再重置对等会话。使用 **ip bgp fast-external-fallover** 接口配置命令，还可在逐个接口的基础上配置 BGP 快速外部故障切换。

示例

在以下示例中，BGP 快速外部故障切换功能已禁用。如果携带此会话的链路摆动，则连接将不会重置。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

相关命令

命令	说明
ip bgp fast-external-fallover	配置每个接口的快速外部故障切换。

bgp inject-map

要配置条件路由注入以将更多特定路由注入到边界网关协议 (BGP) 路由表中，请在地址系列配置模式下使用 **bgp inject-map** 命令。要禁用条件路由注入配置，请使用此命令的 **no** 形式。

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

no bgp inject-map *inject-map* **exist-map** *exist-map*

语法说明

inject-map	指定要注入本地 BGP 路由表中的前缀的路由映射名称。
exist-map *exist-map*	指定包含 BGP 发言方将跟踪的前缀的路由映射名称。
copy-attributes	（可选）配置注入路由以继承汇聚路由的属性。

默认值

没有特定路由注入到 BGP 路由表中。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
地址系列配置、地址系列 IPv6 子模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令修改为在地址系列 IPv6 子模式下受支持。

使用指南

bgp inject-map 命令用于配置条件路由注入。条件路由注入允许您发起更具体的前缀到 BGP 路由表中而无需对应的匹配。在全局配置模式下配置两个路由映射（*exist-map* 和 *inject-map*），然后在地址系列配置模式下使用 **bgp inject-map** 命令指定。

exist-map 参数指定定义 BGP 发言方将跟踪的前缀的路由映射。此路由映射必须包含用于指定汇聚前缀的 **match ip address prefix-list** 命令语句和用于指定路由来源的 **match ip route-source prefix-list** 命令语句。

inject-map 参数定义将创建并安装到路由表中的前缀。注入的前缀安装到本地 BGP RIB 中。必须存在有效的父路由；只能注入等于汇聚路由（现有前缀）或比其更具体的前缀。

可选的 **copy-attributes** 关键字用于可选地配置注入前缀，以继承与汇聚路由相同的属性。如果没有输入此关键字，则注入的前缀将使用本地发起路由的默认属性。

示例

在以下示例中，将配置条件路由注入。注入的前缀将继承汇聚（父）路由的属性。

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH
copy-attributes
```

相关命令

命令	说明
ip prefix-list	创建 prefix-list 或添加 prefix-list 条目。
set community	设置 BGP 社区属性。
address-family ipv4	进入 address-family 配置模式。

bgp log-neighbor-changes

要允许记录 BGP 邻居重置，请在路由器配置模式下使用 **bgp log-neighbor-changes** 命令。要禁止记录 BGP 邻居邻接关系更改，请使用此命令的 **no** 形式。

bgp log-neighbor-changes

no bgp log-neighbor-changes

语法说明

此命令没有任何参数或关键字。

默认值

BGP 邻居的记录已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp log-neighbor-changes 命令允许记录 BGP 邻居状态更改（运行或关闭）和重置，用于网络连接问题故障排除和测量网络稳定性。意外邻居重置可能表示网络中存在高错误率或高数据包丢失率的情况，应进行调查。

使用 **bgp log-neighbor-changes** 命令以允许状态更改消息记录而不会造成显著的性能影响；例如，与启用每个 BGP 更新的调试不同。

如果未启用 **bgp log-neighbor-changes** 命令，则不会跟踪邻居状态更改消息；除了出于重置原因，此情况始终可用作 **show bgp neighbors** 命令的输出。

eigrp log-neighbor-changes 命令允许记录增强型内部网关路由协议 (EIGRP) 邻居邻接关系，但 BGP 邻居的消息仅当使用 **bgp log-neighbor-changes** 命令特别启用时记录。

使用 **show logging** 命令以显示 BGP 邻居更改的日志。

示例

以下示例在路由器配置模式下记录 BGP 的邻居更改。

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

相关命令

命令	说明
show BGP neighbors	显示关于与邻居的 BGP 连接的信息。

bgp maxas-limit

要将边界网关协议 (BGP) 配置为丢弃 AS-path 中自主系统编号数量超过指定值的路由，请在路由器配置模式下使用 **bgp maxas-limit** 命令。要将路由器恢复为默认操作，请使用此命令的 **no** 形式。

bgp max-as limit *number*

no bgp max-as limit

语法说明

number	BGP 更新消息 AS-path 属性中的最大自主系统编号数量，范围从 1 到 254。除了在 AS-path 段内设置自主系统编号数量限制以外，该命令还将 AS-path 的段数限制为 10。允许 10 个 AS-path 段的行为将内置到 **bgp maxas-limit** 命令中。

默认值

不丢弃任何路由。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp maxas-limit 命令用于限制入站路由中允许的 AS-path 属性中的自主系统编号数量。如果接收的路由 AS-path 段超出配置的限制，则 BGP 路由进程将丢弃该路由。

示例

本示例将 AS-path 属性中自主系统编号的最大数量设置为 30。

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

要配置边界网关协议 (BGP) 下一跳地址跟踪，请在地址系列或路由器配置模式下使用 **bgp nexthop** 命令。要禁用 BGP 下一跳地址跟踪，请使用此命令的 **no** 形式。

bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

no bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

语法说明

trigger	指定使用 BGP 下一跳地址跟踪。将此关键字与 **delay** 关键字一起使用以更改下一跳跟踪延迟。将此关键字与 **enable** 关键字一起使用以启用下一跳地址跟踪。
delay	更改两次检查路由表中安装的更新下一跳路由之间的延迟间隔。
seconds	为延迟指定的秒数。有效值为从 0 到 100。默认值为 5。
enable	启用 BGP 下一跳地址跟踪。
route-map	指定使用适用于路由表中路由（分配为 BGP 前缀的下一跳路由）的路由映射。
map-name	路由映射的名称。

默认值

默认情况下，BGP 下一跳地址跟踪对 IPv4 已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
地址系列配置 地址系列 IPv6 子模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令修改为在地址系列 IPv6 子模式下受支持。

使用指南

BGP 下一跳地址跟踪是事件驱动的。BGP 前缀在对等会话建立后自动跟踪。下一跳更改在路由信息库 (RIB) 中更新后迅速报告给 BGP。此优化通过缩短 RIB 中所安装路由的下一跳更改响应时间来改善整体 BGP 融合。在两个 BGP 扫描程序周期之间运行最佳路径计算时，仅处理和跟踪更改。

注

- BGP 下一跳地址跟踪可显著改善 BGP 响应时间。不过，不稳定的内部网关协议 (IGP) 对等设备可能会引起 BGP 的不稳定。我们建议您积极抑制不稳定的 IGP 对等会话以减轻对 BGP 可能的影响。
- BGP 下一跳地址跟踪在 IPv6 地址系列下不支持。

将 **trigger** 关键字与 **delay** 关键字和 *seconds* 参数一起使用可更改两次 BGP 下一跳地址跟踪路由表遍历之间的延迟间隔。通过将两次完整路由表走查之间的延迟间隔调整为匹配 IGP 的调整参数，可提高 BGP 下一跳地址跟踪的性能。默认延迟间隔为 5 秒，即快速调整 IGP 的最佳值。如果 IGP 融合更缓慢，您可将延迟间隔更改为 20 秒或更长时间，具体取决于 IGP 融合时间。

将 **trigger** 关键字与 **enable** 关键字一起使用以启用 BGP 下一跳地址跟踪。默认情况下，BGP 下一跳地址跟踪已启用。

将 **route-map** 关键字与 *map-name* 参数一起使用以允许使用路由映射。路由映射在 BGP 最佳路径计算过程中使用，适用于覆盖 BGP 前缀 Next_Hop 属性的路由表中路由。如果下一跳路由未通过路由映射评估，则下一跳路由标记为不可访问。此命令基于地址系列，因此可对不同地址系列中的下一跳路由应用不同的路由映射。

注　路由映射中仅支持 **match ip address** 命令。不支持任何 **set** 命令或其他 **match** 命令。

示例

以下示例展示如何将两次 BGP 下一跳地址跟踪路由表走查之间的延迟间隔更改为在 IPv4 地址系列会话下每 20 秒进行一次。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

以下示例展示如何禁用 IPv4 地址系列的下一跳地址跟踪：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

以下示例展示如何配置路由映射，从而仅当地址掩码长度超过 25 时允许路由被视为下一跳路由。此配置会避免将任何前缀汇聚视为下一跳路由。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

要将 iBGP 配置为重分布到内部网关协议 (IGP)（例如 EIGRP 或 OSPF）中，请在地址系列配置模式下使用 **bgp redistribute-internal** 命令。要将路由器恢复为默认行为并停止将 iBGP 重分布到 IGP 中，请使用此命令的 **no** 形式。

bgp redistribute-internal

no bgp redistribute-internal

语法说明

此命令没有任何参数或关键字。

默认值

IBGP 路由重分布到 IGP 中。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置 地址系列 IPv6 子模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令修改为在地址系列 IPv6 子模式下受支持。

使用指南

bgp redistribute-internal 命令用于将 iBGP 配置为重分布到 IGP 中。必须输入 **clear bgp** 命令以在此命令配置后重置 BGP 连接。

将 BGP 重分布到任何 IGP 中之前，请确保使用 IP prefix-list 和 route-map 语句限制重分布的前缀数量。

注意事项

将 iBGP 重分布到 IGP 时应格外小心。使用 IP prefix-list 和 route-map 语句限制重分布的前缀数量。将未过滤的 BGP 路由表重分布到 IGP 中可能会对正常 IGP 网络运行产生不良影响。

示例

在以下示例中，BGP 到 OSPF 路由重分布已启用：

```
ciscoasa(config)# router ospf 300
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

要配置本地边界网关协议 (BGP) 路由进程的固定路由器 ID，请在地址系列路由器配置模式下使用 **bgp router-id** 命令。要从运行的配置文件中删除固定路由器 ID 并恢复默认路由器 ID 选择，请使用此命令的 **no** 形式。

bgp router-id *ip-address*

no bgp router-id

语法说明

ip-address	IP 地址形式的路由器标识符。

默认值

此命令未启用时，路由器 ID 设置为物理接口上的最高 IP 地址。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置路由器配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令已修改。

使用指南

bgp router-id 命令用于配置本地 BGP 路由进程的固定路由器 ID。路由器 ID 以 IP 地址格式输入。可以使用任何有效的 IP 地址，即使地址并非在路由器上本地配置。路由器 ID 更改后，对等会话将自动重置。可以每个情景使用单独的路由器 ID。

示例

以下示例展示如何使用固定 BGP 路由器 ID 192.168.254.254 配置本地路由器

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

要配置下一跳验证的边界网关协议 (BGP) 路由器扫描间隔，请在地址系列配置模式下使用 **bgp scan-time** 命令。要将路由器的扫描间隔恢复为其默认扫描间隔 60 秒，请使用此命令的 **no** 形式。

bgp scan-time *scanner-interval*

no bgp scan-time *scanner-interval*

语法说明

scanner-interval	BGP 路由信息的扫描间隔。 有效值为从 15 到 60 秒。默认值为 60 秒

默认值

默认扫描间隔为 60 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

输入此命令的 **no** 形式不会禁用扫描，但会将其从 **show running-config** 命令的输出中删除。

为地址系列启用 **bgp nexthop** 地址跟踪 (NHT) 时，将不会在该地址系列中接受 **bgp scan-time** 命令，并将保持默认值 60 秒。必须禁用 NHT，然后才能在路由器模式或地址系列模式下接受 **bgp scan-time** 命令。

示例

在以下路由器配置示例中，BGP 路由表 IPv4 单播路由下一跳验证的扫描间隔设置为 20 秒：

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

相关命令

命令	说明
show running-config	显示 ASA 中当前显示的配置。
bgp nexthop	配置 BGP 下一跳地址跟踪。

bgp suppress-inactive

要抑制未安装在路由信息库 (RIB) 中的路由的通告，请在地址系列或路由器配置模式下使用 **bgp suppress-inactive** 命令。

bgp suppress-inactive

no bgp suppress-inactive

语法说明

此命令没有任何参数或关键字。

默认值

不抑制任何路由。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置地址系列 IPv6 子模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。
9.3(2)	此命令修改为在地址系列 IPv6 子模式下受支持。

使用指南

bgp suppress-inactive 命令用于阻止未安装在 RIB 中的路由（非活动路由）通告到对等设备。如果此功能未启用，或如果使用此命令的 **no** 形式，则边界网关协议 (BGP) 将通告非活动路由。

注　BGP 使用 RIB-failure 标志来标记未安装到 RIB 中的路由。此标志还将在 **show bgp** 命令的输出中显示；例如 Rib-Failure (17)。此标志不指示路由器或 RIB 的错误或问题，可能仍会通告路由，具体取决于此命令的配置。输入 **show bgp rib-failure** 命令以查看关于非活动路由的详细信息。

示例

在以下示例中，BGP 路由进程配置为不通告 RIB 中未安装的路由：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

相关命令

命令	说明
show bgp	显示 BGP 路由表中的条目。
show bgp rib-failure	显示路由信息库 (RIB) 表中无法安装的 BGP 路由。

bgp transport

要全局启用所有边界网关协议 (BGP) 会话的 TCP 传输会话参数，请在路由器配置模式下使用 **bgp transport** 命令。要全局禁用所有 BGP 会话的 TCP 传输会话参数，请使用此命令的 **no** 形式。

bgp transport path-mtu-discovery

no bgp transport path-mtu-discovery

语法说明

path-mtu-discovery	启用传输路径最大传输单位 (MTU) 发现。

默认值

默认情况下，TCP 路径 MTU 发现对所有 BGP 会话均已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令在默认情况下已启用，因为其用于允许 BGP 会话利用较大的 MTU 链路，这可能对内部 BGP (iBGP) 会话非常重要。使用 **show bgp neighbors** 命令以确保 TCP 路径 MTU 发现已启用。

示例

以下示例展示如何禁用所有 BGP 会话的 TCP 路径 MTU 发现：

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

以下示例展示如何启用所有 BGP 会话的 TCP 路径 MTU 发现：

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

相关命令

命令	说明
show bgp neighbors	显示有关到邻居的 BGP 连接的信息。

bgp-community new format

要将 BGP 配置为以格式 AA:NN（自主系统 : 社区编号 /4 字节编号）显示社区，请在全局配置模式下使用 **bgp-community new-format** 命令。要将 BGP 配置为以 32 位编号显示社区，请使用此命令的 **no** 形式。

bgp-community new-format

no bgp-community new-format

语法说明

此命令没有任何参数或关键字。

默认值

如果此命令未启用，或如果输入了 **no** 形式，则 BGP 社区（也以 AA:NN 格式输入时）也显示为 32 位编号。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

bgp-community new-format 命令用于将本地路由器配置为以 AA:NN 格式显示 BGP 社区，从而符合 RFC-1997。

此命令仅影响 BGP 社区显示格式；它不影响社区或社区交换。但是，匹配本地配置正则表达式的扩展 IP 社区列表可能需要更新，以匹配 AA:NN 格式而不是 32 位编号。

RFC 1997 的 *BGP 社区属性*中指定 BGP 社区由两部分组成（长度各为 2 个字节）。第一部分是自主系统编号，而第二部分是网络运营商定义的 2 字节编号。

示例

在以下示例中，使用 32 位编号社区格式的路由器已升级为使用 AA:NN 格式：

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

以下示例输出展示 BGP 社区编号在 **bgp-community new-format** 命令启用时如何显示：

```
ciscoasa(router)# show bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
```

```
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

blocks

要将附加内存分配给块诊断程序（通过 **show blocks** 命令显示），请在特权 EXEC 模式下使用 **blocks** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

语法说明

*memory_size*s	（可选）设置块诊断程序的内存大小（以字节为单位），而不是应用动态值。如果该值大于可用内存，将显示错误消息且不接受该值。如果该值大于 50% 的可用内存，将显示警告消息，但接受该值。

默认值

分配给跟踪块诊断程序的默认内存为 2136 字节。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要查看当前分配的内存，请输入 **show blocks queue history** 命令。

如果重新加载 ASA，内存分配将恢复为默认值。

分配的内存量最多将为 150 KB，但从不超过可用内存的 50%。（可选）您可以手动指定内存大小。

示例

以下示例增加块诊断程序的内存大小：

```
ciscoasa# blocks queue history enable
```

以下示例将内存大小增加到 3000 字节：

```
ciscoasa# blocks queue history enable 3000
```

以下示例尝试将内存大小增加到 3000 字节，但该值已超出可用内存：

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

以下示例将内存大小增加到 3000 字节，但该值已超出 50% 的可用内存：

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

相关命令

命令	说明
clear blocks	清除系统缓冲区统计信息。
show blocks	显示系统缓冲区使用情况。

boot

要指定下次加载时系统使用哪个映像以及启动时系统使用哪个配置文件，请在全局配置模式下使用 **boot** 命令。要恢复默认值，请使用此命令的 **no** 形式。

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

语法说明

config	指定系统加载时使用哪个配置文件。
system	指定系统加载时使用哪个映像文件。
url	设置映像或配置的位置。在多情景模式下，所有远程 URL 均必须从管理情景可访问。参阅以下 URL 语法： • **disk0:/**[*path*/]*filename* 对于 ASA，此 URL 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* 对于 ASA，此 URL 表示外部闪存卡。此选项对 ASA 服务模块不可用。 • **flash:/**[*path*/]*filename* 此 URL 指示内部闪存。 • **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。 此选项仅适用于 ASA 5500 系列的 **boot system** 命令； **boot config** 命令要求启动配置位于闪存上。 只能配置一条 **boot system tftp:** 命令，并且必须首先配置该命令。

默认值

如果 **boot config** 命令未指定，则启动配置文件将保存到隐藏位置，并仅与配合使用的命令一起使用，例如 **show startup-config** 命令和 **copy startup-config** 命令。

对于 **boot system** 命令，没有默认值。如果没有指定位置，则 ASA 仅搜索内部闪存以获得第一个有效的引导映像。如果未找到有效的映像，则不会加载任何系统映像，并且 ASA 将引导循环，直到您打破循环进入 ROMMON 或监控模式。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **write memory** 命令将此命令保存到启动配置后，您还可以将设置保存到 BOOT 和 CONFIG_FILE 环境变量； ASA 在重新启动后使用这些变量来确定启动配置和要引导的软件映像。

您可以输入最多四个 **boot system** 命令条目，按顺序指定不同的引导映像，而 ASA 将引导其找到的第一个有效的映像。

如果要在与当前运行配置不同的新位置使用启动配置文件，则保存运行的配置后，确保将启动配置文件复制到新位置。否则，保存运行的配置时将覆盖新的启动配置。

提示　ASDM 映像文件通过 **asdm image** 命令指定。

示例

以下示例指定启动时 ASA 应加载名为 configuration.txt 的配置文件：

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

相关命令

命令	说明
asdm image	指定 ASDM 软件映像。
show bootvar	显示引导文件和配置环境变量。

border style

要定制向经过身份验证的 WebVPN 用户显示的 WebVPN 主页边框，请在定制配置模式下使用 **border style** 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。

border style *value*

no border style *value*

语法说明

value	指定要使用的层叠样式表 (CSS) 参数。允许的最大字符数为 256。

默认值

边框的默认样式为 background-color:#669999;color:white。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
定制配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的级联样式表 (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，取值范围为 0 到 255，分别表示每种颜色（红、绿、蓝）；以逗号分隔的条目用于指示彼此混合的每种颜色的强度级别。
- 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

以下示例将边框的背景颜色定制为 RGB 颜色 #66FFFF，一种绿色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

相关命令

命令	说明
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。

bridge-group

要在透明防火墙模式下将接口分配到桥组，请在接口配置模式下使用 **bridge-group** 命令。要取消分配接口，使用此命令的 **no** 形式。透明防火墙在其接口上连接相同的网络。最多四个接口可属于一个桥组。

bridge-group *number*

no bridge-group *number*

语法说明

number	指定一个介于 1 和 100 之间的整数。对于 9.3(1) 和更高版本，该范围增加至 1 到 250 之间。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。
9.3(1)	我们将编号范围增加至 1 和 250 之间以支持 250 个 BVI（网桥虚拟接口）。

使用指南

对于 9.2 版本及更早版本，您可在单模式或多模式的每个情景中配置最多 8 个桥组；对于 9.3(1) 版本及更高版本，您可配置最多 250 个桥组。每个桥组可包括最多 4 个接口。您无法将同一接口分配至多个桥组。请注意您必须至少使用 1 个桥组；数据接口必须属于一个桥组。

注　尽管您可以在 ASA 5505 上配置多个桥组，但是 ASA 5505 的透明模式下限定 2 个数据接口意味着您只能有效地使用 1 个桥组。

使用 **interface bvi** 命令，然后使用 **ip address** 命令，将管理 IP 地址分配到桥组。

每个桥组都连接到单独的网络。桥组的流量与其他桥组是分离的；流量不会路由至 ASA 内的另一个桥组，并且流量必须退出 ASA 后才能由外部路由器路由回 ASA 内的另一个桥组。

如果您不想支出安全情景的管理费用，或想要充分利用安全情景，您可能会想要使用多个桥组。虽然每个桥组的桥接功能是独立的，但所有桥组之间可共享很多其他功能。例如，所有桥组都共享系统日志服务器或 AAA 服务器的配置。为了完整的安全策略独立，请在每个情景中通过一个桥组使用安全情景。

示例

以下示例将 GigabitEthernet 1/1 分配给桥组 1：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

相关命令

命令	说明
interface	配置一个接口。
interface bvi	进入桥组的接口配置模式，以便能够设置管理 IP 地址。
ip address	设置一个桥组的管理 IP 地址。
nameif	设置接口名称。
security-level	设置接口安全级别。

browse-networks

要定制向经过身份验证的 WebVPN 用户显示的 WebVPN 主页的 Browse Networks（浏览网络）框，请在 webvpn 定制配置模式下使用 **browse-networks** 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。

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

语法说明

dropdown	指定对下拉列表的更改。
message	指定更改标题下显示的消息。
style	指定对样式的更改。
text	指定对文本的更改。
title	指定对标题的更改。
value	指示要显示的实际文本。允许的最大字符数为 256。该值也适用于层叠样式表 (CSS) 参数。

默认值

默认标题文本为 “Browse Networks”。

默认标题样式如下：

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

默认消息文本为 “Enter Network Path”。

默认消息样式为：

background-color:#99CCCC;color:maroon;font-size:smaller。

默认下拉列表文本为 “File Folder Bookmarks”。

默认下拉列表样式为：

border:1px solid black;font-weight:bold;color:black;font-size:80%。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Webvpn customization configuration	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的级联样式表 (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

以下示例将标题更改为 “Browse Corporate Networks”，并将样式内的文本更改为蓝色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

相关命令

命令	说明
application-access	定制 WebVPN 主页的 Application Access 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。
web-bookmarks	定制 WebVPN 主页上的 Web Bookmarks 标题或链接。

第 2 部分

C 命令

第 5 章

cache 至 clear compression 命令

cache

要进入缓存模式并设置缓存属性的值，请在 webvpn 配置模式下输入 **cache** 命令。要从配置中删除所有与缓存相关的命令并将它们重置为默认值，请输入此命令的 **no** 形式。

cache

no cache

默认值

启用每个缓存属性的默认设置。

命令模式

下表显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	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

缓存技术会在系统缓存中存储经常重新使用的对象，从而减少执行重复重写和内容压缩的需要。它可减少 WebVPN 与远程服务器和最终用户浏览器之间的流量，从而使多种应用更高效运行。

示例

以下示例展示如何进入缓存模式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

相关命令

命令	说明
cache-static-content	缓存不会被重写的内容。
disable	禁用缓存。
expiry-time	配置不需要重新验证即缓存对象的到期时间。
lmfactor	为缓存只有最后修改时间戳的对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义要缓存的对象的最小大小。

cache-time

要指定允许 CRL 在缓存中保留的分钟数（之后即认为其过期），请在 ca-crl 配置模式下使用 **cache-time** 命令，可以从 crypto ca 信任点配置模式访问该命令。要恢复默认值，请使用此命令的 **no** 形式。

cache-time *refresh-time*

no cache-time

语法说明

refresh-time	指定允许 CRL 在缓存中保留的分钟数。范围为 1 - 1440 分钟。如果 CRL 中不存在 NextUpdate 字段，则不缓存 CRL。

默认值

默认设置为 60 分钟。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Ca-crl 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入 ca-crl 配置模式，并为中心信任点指定 10 分钟的缓存时间刷新值：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# cache-time 10
ciscoasa(ca-crl)#
```

相关命令

命令	说明
crl configure	进入 crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
enforcenextupdate	指定如何处理证书中的 NextUpdate CRL 字段。

call-agent

要指定一组呼叫代理，请在 mgcp 映射配置模式下使用 **call-agent** 命令。要删除配置，请使用此命令的 **no** 形式。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

语法说明

group_id	呼叫代理组 ID，从 0 到 2147483647。
ip_address	网关的 IP 地址。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Mgcp 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **call-agent** 命令可指定一组可管理一个或多个网关的呼叫代理。呼叫代理组信息用于为组中的呼叫代理打开连接（网关向其发送命令的呼叫代理除外），以便任何呼叫代理都可以发送响应。具有相同 *group_id* 的呼叫代理属于同一组。一个呼叫代理可能属于多个组。

示例

以下示例允许呼叫代理 10.10.11.5 和 10.10.11.6 控制网关 10.10.10.115，并允许呼叫代理 10.10.11.7 和 10.10.11.8 控制网关 10.10.10.116 和 10.10.10.117：

```
ciscoasa(config)# mgcp-map mgcp_inbound
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

相关命令

命令	说明
debug mgcp	启用 MGCP 的调试信息的显示。
mgcp-map	定义 MGCP 映射并启用 mgcp 映射配置模式。
show mgcp	显示 MGCP 配置和会话信息。

call-duration-limit

要配置 H.323 呼叫的呼叫持续时间，请在参数配置模式下使用 **call-duration-limit** 命令。要禁用此功能，请使用此命令的 **no** 形式。

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

语法说明

hh:mm:ss	指定以小时、分钟和秒表示的持续时间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何配置 H.323 呼叫的呼叫持续时间：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-duration-limit 0:1:0
```

相关命令

命令	说明
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 层或第 4 层策略映射。
show running-config policy-map	显示所有当前策略映射配置。

call-party-numbers

要在 H.323 呼叫设置过程中强制发送呼叫方号码，请在参数配置模式下使用 **call-party-numbers** 命令。要禁用此功能，请使用此命令的 **no** 形式。

call-party-numbers

no call-party-numbers

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何在 H.323 呼叫的呼叫设置过程中强制发送呼叫方号码：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-party-numbers
```

相关命令

命令	说明
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 层或第 4 层策略映射。
show running-config policy-map	显示所有当前策略映射配置。

call-home

要进入 call home 配置模式，请在全局配置模式下使用 **call-home** 命令。

call-home

语法说明

此命令没有任何参数或关键字。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

在输入 **call-home** 命令后，提示符更改为主机名 (cfg-call-home)#，您可以访问以下 Call Home 配置命令：

- [**no**] **alert-group** {**group name** | **all**} - 启用或禁用 Smart Call Home 组。默认为所有警报组启用。
  group name：Syslog、diagnostic、environment、inventory、configuration、snapshot、threat、telemetry、test。
- [**no**] **contact-e-mail-addr e-mail-address** - 指定客户联系人邮件地址。此字段为必填字段。
  e-mail-address：客户邮件地址，最长 127 个字符。
- [**no**] **contact-name contact name** - 指定客户姓名。
  e-mail-address：客户姓名，最长 127 个字符。
- **copy profile src-profile-name dest-profile-name -** 将现有配置文件 (**src-profile-name**) 的内容复制到新配置文件 (**dest-profile-name**)。
  src-profile-name：现有配置文件的名称，最长 23 个字符。
  dest-profile-name：新配置文件的名称，最长 23 个字符。
- **rename profile src-profile-name dest-profile-name** - 更改现有配置文件的名称。
  src-profile-name：现有配置文件的名称，最长 23 个字符。
  dest-profile-name：新配置文件的名称，最长 23 个字符。
- **no configuration all** - 清除 Smart Call-home 配置。
  [**no**] **customer-id customer-id-string** - 指定客户 ID。
  customer-id-string：客户 ID，最长 64 个字符。XML 格式的消息需要此字段。
- [**no**] **event-queue-size queue_size** - 指定事件队列大小。
  queue-size：事件数为 5-60。默认值为 10。

- [**no**] **mail-server ip-address | name priority 1-100 all** - 指定 SMTP 邮件服务器。客户可以指定最多五个邮件服务器。要对 Smart Call Home 消息使用邮件传输，至少需要一个邮件服务器。
  ip-address：邮件服务器的 IPv4 或 IPv6 地址。
  name：邮件服务器的主机名。
  1-100：邮件服务器的优先级。数值越低，优先级越高。
- [**no**] **phone-number phone-number-string** - 指定客户的电话号码。此字段为可选字段。
  phone-number-string：电话号码。
- [**no**] **rate-limit msg-count** - 指定 Smart Call Home 每分钟可发送的消息数。
  msg-count：每分钟消息数。默认值为 10。
- [**no**] **sender** {**from e-mail-address | reply-to e-mail-address**} - 指定邮件消息的发件人 / 收件人邮件地址。此字段为可选字段。
  e-mail-address：发件人和收件人邮件地址。
- [**no**] **site-id site-id-string** - 指定客户站点 ID。此字段为可选字段。
  site-id-string：用于标识客户位置的站点 ID。
- [**no**] **street-address street-address** - 指定客户地址。此字段为可选字段。
  street-address：自由格式字符串，最长 255 个字符。
- [**no**] **alert-group-config environment** - 进入环境组配置模式。
  [**no**] **threshold** {**cpu | memory**} **low-high** - 指定环境资源阈值。
  low, high：有效值为 0-100。默认值为 85-90。
- [**no**] **alert-group-config snapshot** - 进入快照组配置模式。
  system, user：在系统或用户情景中运行 CLI（仅在多模式下可用）。
- [**no**] **add-command "cli command"** [{**system | user**}] - 指定要在快照组中捕获的 CLI 命令。
  cli command：要输入的 CLI 命令。
  system, user：在系统或用户情景中运行 CLI（仅在多模式下可用）。如果系统和用户均未指定，CLI 将同时在系统和用户情景中运行。默认为用户情景。
- [**no**] **profile profile-name | no profile all** - 创建、删除或编辑配置文件。进入配置文件配置模式并将提示符更改为主机名 (cfg-call-home-profile)#。
  profile-name：配置文件名称，最长 20 个字符。
- [**no**] **active** - 启用或禁用配置文件。默认设置为启用。
  no destination address {**e-mail | http**} **all | [no] destination** {**address** {**e-mail | http**} **e-mail-address | http-url** [**msg-format short-text | long-text | xml**] **| message-size-limit max-size | preferred-msg-format short-text | long-text | xml | transport-method e-mail | http**} - 配置 Smart Call Home 消息接收方的目标、消息大小、消息格式和传输方法。默认消息格式为 XML，默认启用的传输方法为邮件。
  e-mail-address：Smart Call Home 接收方的邮件地址，最长为 100 个字符。
  http-url：HTTP 或 HTTPS URL。
  max-size：最大消息大小（以字节为单位）。0 表示没有限制。默认为 5 MB。
- [**no**] **subscribe-to-alert-group alert-group-name** [**severity** {**catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging**}] - 订阅具有指定严重性级别的组事件。
  alert-group-name：Syslog、diagnostic、environment 或 threat 为有效值。
- [**no**] **subscribe-to-alert-group syslog** [{**severity** {**catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging**} **| message start** [**-end**]}] - 订阅具有严重性级别或消息 ID 的 syslog。
  start-[**end**]：一个系统日志消息 ID 或一组系统日志消息 ID。

- [**no**] **subscribe-to-alert-group inventory** [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]] - 订阅资产事件。
  day_of_month：月份中的天，1-31。
  day_of_week：周内某日（周日、周一、周二、周三、周四、周五、周六）。
  hh, mm：一天中的小时和分钟，24 小时格式。
- [**no**] **subscribe-to-alert-group configuration** [**export full** | **minimum**] [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]] - 订阅配置事件。
  full：导出运行配置、启动配置、功能列表、访问列表中的元素数量以及多模式中的情景名称的配置。
  minimum：仅导出功能列表、访问列表中的元素数量以及多模式中的情景名称的配置。
  day_of_month：月份中的天，1-31。
  day_of_week：周内某日（周日、周一、周二、周三、周四、周五、周六）。
  hh, mm：一天中的小时和分钟，24 小时格式。
- [**no**] **subscribe-to-alert-group telemetry periodic** {**hourly** | **daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**] - 订阅遥测周期性事件。
  day_of_month：月份中的天，1-31。
  day_of_week：周内某日（周日、周一、周二、周三、周四、周五、周六）。
  hh, mm：一天中的小时和分钟，24 小时格式。
- [**no**] **subscribe-to-alert-group snapshot periodic** {**interval minutes** | **hourly** [**mm**] | **daily** | **monthly day_of_month** |**weekly day_of_week** [**hh:mm**]} - 订阅快照周期性事件。
  minutes：间隔（以分钟为单位）。
  day_of_month：月份中的天，1-31。
  day_of_week：周内某日（周日、周一、周二、周三、周四、周五、周六）。
  hh, mm：一天中的小时和分钟，24 小时格式。

注意　Call-home HTTPS 消息只能使用 **ip http client source-interface** 命令通过 VRF 上的指定源接口发送，与此处介绍的 **vrf** 命令无关。

示例

以下示例展示如何配置联系人信息：

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

以下示例展示如何配置 Call Home 消息速率限制阈值：

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

以下示例展示如何将 Call Home 消息速率限制阈值设置为默认设置：

```
hostname(config)# call-home
hostname(cfg-call-home)# default rate-limit
```

以下示例展示如何创建与现有配置文件具有相同配置设置的新目标配置文件：

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

以下示例展示如何配置常规邮件参数（包括主要和辅助邮件服务器）：

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

相关命令

命令	说明
alert-group	启用警报组。
profile	进入 call-home 配置文件配置模式。
show call-home	显示 Call Home 配置信息。

call-home send

要执行 CLI 命令并将命令输出通过邮件发送到指定地址，请在特权 EXEC 模式下使用 **call-home send** 命令。

call-home send cli command [**email** *email*] [**service-number** *service number*]

语法说明

cli-command	指定要执行的 CLI 命令。命令输出通过邮件发送。
email *email*	指定将 CLI 命令输出发送到的邮件地址。如果未指定邮件地址，命令输出将发送到思科 TAC (attach@cisco.com)。
service-number *service number*	指定与命令输出相关的活动 TAC 案例编号。仅当未指定邮件地址（或 TAC 邮件地址）时才需要此编号，此编号将显示在邮件主题行中。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

此命令使指定的 CLI 命令在系统中执行。指定的 CLI 命令必须用引号 ("") 括起来，并且可以是任意 **run** 或 **show** 命令，包括所有模块的命令。

命令输出随后通过邮件发送到指定的邮件地址。如果未指定邮件地址，命令输出将发送到思科 TAC (attach@cisco.com)。邮件以长文本格式发送，并在主题行中显示服务编号（如果指定的话）。

示例

以下示例展示如何发送 CLI 命令以及通过邮件发送命令输出：

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

相关命令

call-home	进入 call home 配置模式。
call-home test	发送您定义的 Call Home 测试消息。
service call-home	启用或禁用 Call Home。
show call-home	显示 call-home 配置信息。

call-home send alert-group

要发送特定警报组消息，请在特权 EXEC 模式下使用 **call-home send alert-group** 命令。

call-home send alert-group {**configuration** | **telemetry** | **inventory** | **group snapshot**} [**profile** *profile-name*]

语法说明

configuration	将配置警报组消息发送到目标配置文件。
group snapshot	发送快照组。
inventory	发送资产 call-home 消息。
profile *profile-name*	（可选）指定目标配置文件的名称。
telemetry	将诊断警报组消息发送到特定模块、插槽 / 子插槽 / 或插槽 / 托架编号的目标配置文件。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

如果不指定 **profile** *profile-name*，消息会发送到所有已订阅的目标配置文件。

只有配置、诊断和资产警报组可以手动发送。目标配置文件不需要订阅到警报组。

示例

以下示例展示如何将配置警报组消息发送到目标配置文件：

```
hostname# call-home send alert-group configuration
```

以下示例展示如何将诊断警报组消息发送到特定模块、插槽 / 子插槽 / 或插槽 / 托架编号的目标配置文件：

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

以下示例展示如何将诊断警报组消息发送到特定模块、插槽 / 子插槽 / 或插槽 / 托架编号的所有目标配置文件：

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

以下示例展示如何发送资产 call-home 消息：

```
hostname# call-home send alert-group inventory
```

相关命令

call-home	进入 call home 配置模式。
call-home test	发送您定义的 Call Home 测试消息。
service call-home	启用或禁用 Call Home。
show call-home	显示 call-home 配置信息。

call-home test

要使用配置文件的配置手动发送 Call Home 测试消息，请在特权 EXEC 模式下使用 **call-home test** 命令。

call-home test [“*test-message*”] **profile** *profile-name*

语法说明

profile *profile-name*	指定目标配置文件的名称。
“*test-message*”	（可选）测试消息文本。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

此命令向指定的目标配置文件发送测试消息。如果输入测试消息文本，则必须用引号 ("") 括上文本（如果包含空格）。如果不输入消息，将发送默认消息。

示例

以下示例展示如何手动发送 Call Home 测试消息：

```
hostname# call-home test “test of the day” profile Ciscotac1
```

相关命令

call-home	进入 call home 配置模式。
call-home send alert-group	发送特定警报组消息。
service call-home	启用或禁用 Call Home。
show call-home	显示 Call Home 配置信息。

capability lls

默认情况下启用 LLS 功能。要在原始 OSPF 数据包中显式启用链路本地信令 (LLS) 数据块并重新启用 OSPF NSF 感知，请在路由器配置模式下使用 **lls command** 功能。要禁用 LLS 和 OSPF NSF 感知，请使用此命令的 no 形式。

capability lls

no capability lls

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 LLS 功能。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

您可能想要通过在原始 OSPF 数据包中禁用 LLS 数据块来禁用 NSF 感知。如果路由器没有使用 LLS 的应用，您可能想要禁用 NSF 感知。

如果 NSF 已配置并且您尝试禁用 LLS，您将收到错误消息 “OSPF Non-Stop Forwarding (NSF) must be disabled first”（必须先禁用 OSPF 不间断转发 (NSF)）。

如果 LLS 已禁用并且您尝试配置 NSF，您将收到错误消息 “OSPF Link-Local Signaling (LLS) capability must be enabled first”（必须先启用 OSPF 链路本地信令 (LLS) 功能）。

示例

以下示例启用 LLS 支持和 OSPF 感知：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability lls
```

相关命令

capability opaque	使 MPLS TE 信息通过不透明 LSA 泛洪网络。

capability opaque

要使多协议标签交换流量工程 (MPLS TE) 拓扑信息通过不透明 LSA 泛洪网络，请在路由器配置模式下使用 **capability opaque** 命令。要禁止 MPLS TE 拓扑信息通过不透明 LSA 泛洪网络，请使用此命令的 no 形式。

capability opaque

no capability opaque

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用不透明 LSA。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

capability opaque 命令用于通过所有范围（类型 9、10 和 11）的不透明 LSA 泛洪 MPLS TE 信息（类型 1 和 4）。

必须为 OSPF 启用控制不透明 LSA 支持功能才能支持 MPLS TE。

默认情况下，MPLS TE 拓扑信息通过不透明 LSA 泛洪到区域。

示例

以下示例启用不透明功能：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability opaque
```

相关命令

capability lls	在 OSPF 原始数据包中启用 LLS 数据块并启用 OSPF NSF 感知。

capture

要启用数据包捕获功能以进行数据包嗅探和网络故障隔离，请在特权 EXEC 模式下使用 **capture** 命令。要禁用数据包捕获功能，请使用此命令的 **no** 形式。

[**cluster exec**] **capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**interface asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

[**cluster exec**] **no capture** *capture_name* [**type {asp-drop all** [***drop-code***] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [***tag]*** | **webvpn user** ***webvpn-user***}] [**access-list** *access_list_name*] [**asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** ***interface_name***] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** ***prot*** {**host** *source-**ip*** | *source-**ip mask*** | **any**}{**host** *destination-**ip*** | *destination-**ip mask*** | **any**} [***operator*** **port**]

语法说明

access-list *access_list_name*	（可选）捕获与访问列表匹配的流量。在多情景模式下，这只在一个情景内可用。
any	指定任意 IP 地址而不是单个 IP 地址和掩码。
all	捕获 ASA 丢弃的所有数据包。
asa_dataplane	在 ASA 背板上捕获在 ASA 与使用背板的模块（如 ASA CX 或 ASA FirePOWER 模块）之间传递的数据包。
asp-drop *drop-code*	（可选）捕获通过加速安全路径丢弃的数据包。*drop-code* 指定通过加速安全路径丢弃的流量的类型。有关丢弃代码的列表，请参阅 **show asp drop frame** 命令。如果不输入 *drop-code* 参数，则捕获所有已丢弃的数据包。可以将此关键字与 **packet-length**、**circular-buffer** 和 **buffer** 关键字一起使用，但不能与 **interface** 或 **ethernet-type** 关键字一起使用。在集群中，从一个设备丢弃到另一个设备的转发数据包也会被捕获。在多情景模式下，当在系统情景中发出此选项时，所有丢弃的数据包都将被捕获；当在用户情景中发出此选项时，只有从属于用户情景的接口输入的丢弃数据包会被捕获。
buffer *buf_size*	（可选）定义用于存储数据包的缓存大小（以字节为单位）。一旦字节缓冲区已满，数据包捕获将停止。在集群中使用时，此值是每设备大小，而不是所有设备的总和。
capture_name	指定数据包捕获的名称。对多个 **capture** 语句使用相同名称以捕获多种类型的流量。当使用 **show capture** 命令查看捕获配置时，所有选项均合并到一行。
circular-buffer	（可选）当缓冲区已满时，从开头开始覆盖缓冲区。
cluster exec	（可选）在集群部署中仅用作封装器 CLI 前缀，可与 **capture** 和 **show capture** 命令一起使用。使您可以在一个设备中发出 **capture** 命令，同时在所有其他设备中运行该命令。
ethernet-type *type*	（可选）选择要捕获的以太网类型。支持的以太网类型包括 8021Q、ARP、IP、IP6、IPX、LACP、PPPOED、PPPOES、RARP 和 VLAN。802.1Q 或 VLAN 类型会出现异常。802.1Q 标记会被自动跳过，内部以太网类型用于匹配。
host *ip*	指定数据包发送到的主机的单个 IP 地址。
inline-tag *tag*	为特定 SGT 值指定标记或将其保持未指定状态以捕获标记了任何 SGT 值的数据包。

interface *interface_name*	设置将用于数据包捕获的接口的名称。必须为任何要捕获的数据包都配置接口。可以使用多个具有相同名称的 **capture** 命令配置多个接口。要在 ASA 的数据层面上捕获数据包，可以使用 **interface** 关键字并将 “asa_dataplane” 作为接口名称。可以指定 “cluster” 作为接口名称以捕获集群控制链路接口上的流量。接口名称 “cluster” 和 “asa-dataplane” 是固定名称，不可配置。如果配置了 **lacp** 类型的捕获，则接口名称为物理名称。
ikev1/ikev2	仅捕获 IKEv1 或 IKEv2 协议信息。
isakmp	（可选）捕获 VPN 连接的 ISAKMP 流量。ISAKMP 子系统无权访问上层协议。捕获是伪捕获，并将物理层、IP 层和 UDP 层结合在一起来满足 PCAP 解析器。对等设备地址通过 SA 交换获得，存储在 IP 层中。
lacp	（可选）捕获 LACP 流量。如果已配置，则接口名称为物理接口名称。**trace**、**match** 和 **access-list** 关键字不能与 **lacp** 关键字一起使用。
mask	IP 地址的子网掩码。指定网络掩码时，方法与 Cisco IOS 软件 **access-list** 命令不同。ASA 使用网络掩码（例如，对于 C 类掩码为 255.255.255.0）。思科 IOS 掩码使用通配符位（例如 0.0.0.255）。
match *prot*	指定与五元组匹配的数据包以允许过滤要捕获的数据包。在一行中最多可以使用三次此关键字。
operator	（可选）匹配源或目标使用的端口号。允许的运算符如下： • **lt** - 小于 • **gt** - 大于 • **eq -** 等于 • **neq** - 不等于 • **range** - 范围
packet-length *bytes*	（可选）设置每个要存储在捕获缓冲区中的数据包的最大字节数。
port	（可选），如果将协议设置为 **tcp** 或 **udp**，则指定 TCP 或 UDP 端口号或名称。
raw-data	（可选）捕获一个或多个接口上的入站和出站数据包。
real-time	实时持续显示捕获的数据包。要终止实时数据包捕获，请输入 **Ctrl + c**。要永久删除捕获，请使用此命令的 **no** 形式。此选项仅适用于 **raw-data** 和 **asp-drop** 捕获。当使用 **cluster exec capture** 命令时，不支持此选项。
reinject-hide	（可选）指定不捕获任何重新注入的数据包。仅适用于集群环境。
tls-proxy	（可选）通过一个或多个接口上的 TLS 代理捕获解密的入站和出站数据。
trace *trace_count*	（可选）捕获数据包跟踪信息和要捕获的数据包数量。将此选项与访问列表一起使用来向数据路径插入跟踪数据包，以确定是否已按预期处理数据包。
type	（可选）指定所捕获数据的类型。
user ***webvpn-user***	（可选）指定 WebVPN 捕获的用户名。
webvpn	（可选）捕获特定 WebVPN 连接的 WebVPN 数据。

默认值

默认值如下：

- 默认 **type** 为 **raw-data**。
- 默认 **buffer** *size* 为 512 KB。
- 默认以太网类型为 IP 数据包。
- 默认 **packet-length** 为 1518 字节。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
6.2(1)	引入了此命令。
7.0(1)	此命令修改为包括以下关键字：**type asp-drop**、**type isakmp**、**type raw-data** 和 **type webvpn**。
7.0(8)	增加了 **all** 选项以捕获 ASA 丢弃的所有数据包。
7.2(1)	此命令修改为包括以下选项：**trace** *trace_count*、**match** *prot*、**real-time**、**host** *ip*、**any**、 *mask* 和 *operator*。
8.0(2)	此命令修改为更新捕获内容的路径。
8.4(1)	增加了新的 **type** 关键字 **ikev1** 和 **ikev2**。
8.4(2)	为 IDS 的输出增加了附加详细信息。
8.4(4.1)	增加了 **asa_dataplane** 选项以支持通过背板流向 ASA CX 模块的流量。
9.0(1)	增加了 **cluster**、**cluster exec** 和 **reinject-hide** 关键字。增加了新的 **type** 选项 **lacp**。为 ISAKMP 增加了多情景模式支持。
9.1(3)	支持通过 **asa_dataplane** 选项过滤在 ASA CX 背板上捕获的数据包。
9.2(1)	扩展了 **asa_dataplane** 选项以支持 ASA FirePOWER 模块。
9.3(1)	增加了 **inline-tag** *tag* 关键字参数对以支持 SGT 加以太网标记功能。

使用指南

当对连接问题进行故障排除或监视可疑活动时，捕获数据包非常有用。可以创建多个捕获。要查看数据包捕获，请使用 **show capture** *name* 命令。要将捕获保存到文件，请使用 **copy capture** 命令。使用 **https://***ASA-ip-address***/***admin***/capture/***capture_name***[/pcap]** 命令在 Web 浏览器中查看数据包捕获信息。如果指定 **pcap** 可选关键字，则一个 libpcap 格式文件会下载到 Web 浏览器，并可以使用 Web 浏览器保存。（可以使用 TCPDUMP 或 Ethereal 查看 libcap 文件。）

如果将缓冲区内容以 ASCII 格式复制到 TFTP 服务器，将只能看到数据包的报头，而看不到详细信息和十六进制转储。要查看详细信息和十六进制转储，您需要传送 PCAP 格式的缓冲区并使用 TCPDUMP 或 Ethereal 读取。

注意　启用 WebVPN 捕获会影响 ASA 的性能。在生成故障排除所需的捕获文件后，务必禁用捕获。

输入 **no capture** 而不带可选关键字将删除捕获。如果指定 **access-list** 可选关键字，将从捕获中删除访问列表并保留捕获。如果指定 **interface** 关键字，将从指定的接口分离捕获并保留捕获。除非要清除捕获本身，否则请输入 **no capture** 命令并附带 **access-list** 或 **interface** 可选关键字。

当实时显示正在进行时，不能对捕获执行任何操作。由于性能考虑因素，将 **real-time** 关键字与慢速控制台连接一起使用可能导致过多非显示数据包。缓冲区的固定限制为 1000 个数据包。如果缓冲区填满，会保持已捕获数据包的计数器。如果打开另一个会话，则可以输入 **no capture real-time** 命令来禁用实时显示。

注意　在故障切换期间，**capture** 命令不会保存到运行配置，也不会复制到备用设备。

ASA 能跟踪所有流经它的 IP 流量，并能捕获所有以它为目标的 IP 流量，包括所有管理流量（如 SSH 和 Telnet 流量）。

ASA 架构包括三组不同的处理器进行数据包处理；这种架构对捕获功能具有某些限制。通常 ASA 中的大部分数据包转发功能由两个前端网络处理器处理，数据包仅在需要应用检查时才发送到控制平面通用处理器。仅当加速路径处理器中缺少会话时，数据包才发送到会话管理路径网络处理器。

由于 ASA 转发或丢弃的所有数据包都会到达两个前端网络处理器，因此在这两个网络处理器中实施数据包捕获功能。所以如果为流量接口配置合适的捕获，到达 ASA 的所有数据包都会被这两个前端处理器捕获。在入口端，在数据包到达 ASA 接口时捕获数据包，而在出口端，先捕获数据包，再在线发出。

当执行集群范围的捕获后，要同时将相同捕获文件从集群中的所有设备复制到 TFTP 服务器，请在主设备上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，如 filename_A.pcap、filename_B.pcap 等。在此示例中，A 和 B 是集群设备名称。

注意　如果在文件名末尾添加设备名称，将生成不同的目标名称。

以下是一些捕获功能限制。大多数限制由 ASA 架构的分布式性质以及 ASA 中使用的硬件加速器导致。

- 只能捕获 IP 流量；不能捕获非 IP 数据包（如 ARP）。
- 对于多情景模式下的集群控制链路捕获，只有在集群控制链路中发送的与情景关联的数据包会被捕获。
- 在多情景模式下，只能在系统空间中使用 **copy capture** 命令。语法如下所示：

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  Where *in-cap* is the capture configured in the context *context-name*

- 不支持 **cluster exec capture realtime** 命令。会显示以下错误信息：

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 对于共享 VLAN，以下准则适用：
  - 只能为 VLAN 配置一个捕获；如果在共享 VLAN 上的多个情景中配置捕获，则仅使用最后配置的捕获。
  - 如果删除最后配置的（活动）捕获，则没有捕获变为活动状态，即使之前已在其他情景中配置了捕获也是如此；必须删除捕获再重新添加才能使其变为活动状态。
  - 进入捕获所附加到的接口的所有流量（以及与捕获访问列表匹配的所有流量）都将被捕获，包括到共享 VLAN 上其他情景的流量。
  - 因此，如果在某个 VLAN 的情景 A 中启用捕获，而该 VLAN 也被情景 B 使用，则情景 A 和情景 B 的入口流量均会被捕获。
- 对于出口流量，只有具有活动捕获的情景的流量会被捕获。唯一的例外是当您未启用 ICMP 检查时（因此 ICMP 流量在加速路径中没有会话）。在这种情况下，共享 VLAN 上的所有情景的入口和出口 ICMP 流量均会被捕获。

- 配置捕获通常包括配置与需要捕获的流量匹配的访问列表。在配置与流量模式匹配的访问列表之后，您需要定义一个捕获并将此访问列表与该捕获以及需要配置的捕获所在的接口相关联。请注意，仅当访问列表和接口与捕获关联来捕获 IPv4 流量时，捕获才会工作。对于 IPv6 流量，不需要访问列表。
- 对于 ASA CX 模块流量，捕获的数据包包含一个附加的 AFBP 标头，您的 PCAP 查看器可能不了解该标头；请确保使用合适的插件以查看这些数据包。
- 对于内联 SGT 标记数据包，捕获的数据包包含一个附加的 CMD 标头，您的 PCAP 查看器可能不了解该标头。
- 如果没有入口接口并因而没有全局接口，则在背板上发送的数据包将被视为系统情景中的控制数据包。这些数据包将绕过访问列表检查并始终被捕获。此行为适用于单情景模式和多情景模式。

示例

要捕获数据包，请输入以下命令：

```
ciscoasa# capture captest interface inside
ciscoasa# capture captest interface outside
```

在 Web 浏览器中，可以在以下名为 “captest” 的位置查看发出的 **capture** 命令的内容：

```
https://171.69.38.95/admin/capture/captest
```

要将 libpcap 文件（Web 浏览器使用的文件）下载到本地机器，请输入以下命令：

```
https://171.69.38.95/capture/http/pcap
```

以下示例展示将位于 171.71.69.234 的外部主机的流量捕获到内部 HTTP 服务器：

```
ciscoasa# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
ciscoasa# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
ciscoasa# capture http access-list http packet-length 74 interface inside
```

以下示例展示如何捕获 ARP 数据包：

```
ciscoasa# capture arp ethernet-type arp interface outside
```

以下示例将五个跟踪数据包插入数据流，其中 *access-list 101* 定义了与 TCP 协议 FTP 匹配的流量：

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

要以易于阅读的方式查看跟踪的数据包以及有关数据包处理的信息，请使用 **show capture ftptrace** 命令。

以下示例展示如何实时显示捕获的数据包：

```
ciscoasa# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

以下示例展示如何配置与需要捕获的 IPv4 流量匹配的扩展访问列表：

```
ciscoasa (config)# access-list capture extended permit ip any any
```

以下示例展示如何配置捕获：

```
ciscoasa (config)# capture name access-list acl_name interface interface_name
```

默认情况下，配置捕获会创建一个 512 KB 大小的线性捕获缓冲区。您也可以配置一个循环缓冲区。默认情况下，仅将 68 个字节的数据包捕获到缓冲区中。您可以更改此值。

以下示例使用之前配置的适用于外部接口的捕获访问列表创建一个名为“ip-capture”的捕获：

```
ciscoasa (config)# capture ip-capture access-list capture interface outside
```

以下示例展示如何查看捕获：

```
ciscoasa (config)# show capture name
```

以下示例展示如何结束捕获，但保留缓冲区：

```
ciscoasa (config)# no capture name access-list acl_name interface interface_name
```

以下示例展示如何结束捕获并删除缓冲区：

```
ciscoasa (config)# no capture name
```

以下示例展示如何在单情景模式下过滤在背板上捕获的流量：

```
ciscoasa# capture x interface asa_dataplane access-list any4
ciscoasa# capture y interface asa_dataplane match ip any any
```

注意　控制数据包在单模式下捕获，即使您已指定访问列表也是如此。

以下示例展示如何在多情景模式下过滤在背板上捕获的流量：

用户情景中的使用：

```
ciscoasa (contextA)# capture x interface asa_dataplane access-list any4
ciscoasa (contextA)# capture y interface asa_dataplane match ip any any
```

系统情景中的使用：

```
ciscoasa# capture z interface asa_dataplane
```

注意　在多情景模式下，**access-list** 和 **match** 选项不可用于系统情景。

集群的捕获

要在集群中的所有设备上启用捕获，可以在每个命令的前面添加 **cluster exec** 关键字。

以下示例展示如何为集群环境创建 LACP 捕获：

```
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet0/0
```

以下示例展示如何针对集群链路中的控制路径数据包创建捕获：

```
ciscoasa (config)# cap cp interface cluster match udp any eq 49495 any
ciscoasa (config)# cap cp interface cluster match udp any any eq 49495
```

以下示例展示如何针对集群链路中的数据路径数据包创建捕获：

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

以下示例展示如何通过集群捕获数据路径流量：

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match dup host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

以下示例展示如何捕获真实源与真实目标匹配的流的逻辑更新消息，以及如何捕获通过 CCL 转发的真实源与真实目标匹配的数据包：

```
ciscoasa (config)# access-list dp permit real src real dst
```

以下示例展示如何捕获特定类型的数据层面消息（如 icmp 回应请求响应），该消息通过 **match** 关键字或该消息类型的访问列表从一个 ASA 转发到另一个 ASA：

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

以下示例展示如何在集群环境中通过在集群控制链路上使用访问列表 103 来创建捕获。

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster
```

在前一个示例中，如果 A 和 B 是 CCL 接口的 IP 地址，则只有在这两个设备之间发送的数据包会被捕获。

如果 A 和 B 是直通设备流量的 IP 地址，则存在以下情况：

- 如果源和目标 IP 地址与访问列表匹配，则转发的数据包会被照常捕获。
- 如果数据路径逻辑更新消息用于 A 和 B 之间的流或者用于访问列表（例如，访问列表 103），则该消息会被捕获。捕获与嵌入式流的五元组匹配。
- 虽然 UDP 数据包中的源地址和目标地址是 CCL 地址，但如果此数据包要更新与地址 A 和 B 关联的流，则该数据包也会被捕获。也就是说，只要数据包中嵌入的地址 A 和 B 匹配，该数据包也会被捕获。

相关命令

命令	说明
clear capture	清除捕获缓冲区。
copy capture	将捕获文件复制到服务器。
show capture	在未指定选项时显示捕捉配置。

cd

要将当前工作目录切换到指定目录，请在特权 EXEC 模式下使用 **cd** 命令。

cd [**disk0: | disk1: | flash:**] [*path*]

语法说明

disk0:	指定 内部闪存，后跟冒号。
disk1:	指定可拆卸的外部闪存卡，后跟冒号。
flash:	指定 内部闪存，后跟冒号。在 ASA 5500 系列中，**flash** 关键字是 **disk0** 的别名。
path	（可选）目录要切换到的绝对路径。

默认值

如果不指定目录，目录将切换到根目录。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何切换到 “config” 目录：

```
ciscoasa# cd flash:/config/
```

相关命令

命令	说明
pwd	系统随即会显示当前工作目录。

cdp-url

要指定将包含在本地 CA 颁发的证书中的 CDP，请在 CA 服务器配置模式下使用 **cdp-url** 命令。要恢复为默认 CDP，请使用此命令的 **no** 形式。

[**no**] **cdp-url** *url*

语法说明

url	指定验证方用来获得本地 CA 颁发的证书的撤销状态的 URL。URL 必须少于 500 个字母数字字符。

默认值

默认 CDP URL 是 ASA 的包括本地 CA 的 URL。默认 URL 的格式为：http://hostname.domain/+CSCOCA+/asa_ca.crl。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

CDP 是可以包含在已颁发证书中的扩展，用于指定验证方可用来获得证书的撤销状态的位置。一次只能配置一个 CDP。

注意　如果指定 CDP URL，则管理员负责维护从该位置对当前 CRL 的访问权限。

示例

以下示例针对本地 CA 服务器颁发的证书将 CDP 配置在 10.10.10.12：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问，这允许您配置和管理本地 CA。
crypto ca server crl issue	强制签发 CRL。
crypto ca server revoke	在证书数据库和 CRL 中将本地 CA 服务器颁发的证书标记为已撤销。
crypto ca server unrevoke	解除撤销以前撤销的本地 CA 服务器颁发的证书。
lifetime crl	指定证书撤销列表的生命期。

certificate

要添加指定的证书，请在加密 ca 证书链配置模式下使用 **certificate** 命令。要删除证书，请使用此命令的 **no** 形式。

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

语法说明

ca	指示证书是 CA 颁发的证书。
certificate-serial-number	指定十六进制格式的证书序列号，以 “quit” 一词结尾。
ra-encrypt	指示证书是用于 SCEP 的 RA 密钥加密证书。
ra-general	指示证书是用于 SCEP 消息中的数字签名和密钥加密的 RA 证书。
ra-sign	指示证书是用于 SCEP 消息的 RA 数字签名证书。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
加密 ca 证书链配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当发出此命令时，ASA 会将其包含的数据解释为十六进制格式的证书。**quit** 字符串表示证书末尾。

CA 是网络中颁发和管理用于消息加密的安全凭证和公共密钥的机构。作为公共密钥基础设施的一部分，CA 会检查 RA 以验证数字证书请求者提供的信息。如果 RA 验证请求者信息，则 CA 随后可以颁发证书。

示例

以下示例添加序列号为 29573D5FF010FE25B45 的 CA 证书：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crypto ca certificate chain central
ciscoasa(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
```

```
30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
BEA3C1FE 5EE2AB6D 91
quit
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。
crypto ca certificate chain	进入证书加密 ca 证书链模式。
crypto ca trustpoint	进入 ca 信任点模式。
show running-config crypto map	显示所有加密映射的所有配置。

certificate-group-map

要将证书映射中的规则条目与隧道组关联，请在 webvpn 配置模式下使用 **certificate-group-map** 命令。要清除当前的隧道组映射关联，请使用此命令的 **no** 形式。

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

语法说明

certificate_map_name	证书映射的名称。
index	证书映射中映射条目的数字标识符。索引值可在 1-65535 的范围内。
tunnel_group_name	映射条目与证书匹配时所选隧道组的名称。*隧道组名称*必须已存在。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

certificate-group-map 生效时，如果从 WebVPN 客户端收到的证书对应于某个映射条目，则生成的隧道组与连接关联，并覆盖用户选择的任何隧道组。

多个 **certificate-group-map** 命令实例允许多个映射。

示例

以下示例展示如何关联名为 tgl 的隧道组的规则 6：

```
ciscoasa(config)# webvpn
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

相关命令

命令	说明
crypto ca certificate map	进入 ca 证书映射配置模式来根据证书颁发者和主题辨别名称 (DN) 配置规则。
tunnel-group-map	配置基于证书的 IKE 会话映射到隧道组所依据的策略和规则。

chain

要允许发送证书链，请在隧道组 IPsec 属性配置模式下使用 **chain** 命令。要将此命令恢复为默认值，请使用此命令的 **no** 形式。

chain

no chain

语法说明

此命令没有任何参数或关键字。

默认值

此命令的默认设置禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Tunnel-group ipsec-attributes configuration	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以将此属性应用于所有 IPsec 隧道组类型。

输入此命令将在传输中包括根证书以及任何下级 CA 证书。

示例

在隧道组 IPsec 属性配置模式下输入以下示例，将允许为 IP 地址为 209.165.200.225 的 IPSec LAN 到 LAN 隧道组发送证书链，其中包括根证书以及任何下级 CA 证书：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# chain
ciscoasa(config-tunnel-ipsec)#
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示当前隧道组配置。
tunnel-group ipsec-attributes	配置隧道组 ipsec 属性为此组。

change-password

要使用户更改其帐户密码，请在特权 EXEC 模式下使用 **change-password** 命令。

change-password [**/silent**] [**old-password** *old-password* [**new-password** *new-password*]]

语法说明

new-password *new-password*	指定新密码。
old-password *old-password*	对用户重新执行身份验证。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	• 是	—	—	• 是
全局配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.4(4.1)	引入了此命令。

使用指南

如果用户忽略了密码，ASA 会提示其输入。当用户输入 **change-password** 命令时，会被要求保存其运行配置。当用户成功更改密码后，会显示一条消息提醒用户保存配置更改。

示例

以下示例更改用户帐户密码：

```
ciscoasa# change-password old-password myoldpassword000 new password mynewpassword123
```

相关命令

命令	说明
show run password-policy	显示当前情景的密码策略。
clear configure password-policy	将当前情景的密码策略重置为默认值。
clear configure username	从用户帐户中删除用户名。

changeto

要在安全情景和系统之间切换，请在特权 EXEC 模式下使用 **changeto** 命令。

changeto {**system** | **context** *name*}

语法说明

context *name*	切换到具有指定名称的情景。
system	切换到系统执行空间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果登录到系统执行空间或管理情景，则可以在情景之间切换并在每个情景内执行配置和监控任务。您在配置模式下编辑或者在 **copy** 或 **write** 命令中使用的 “ 运行 ” 配置取决于您所在的执行空间。在系统执行空间中时，运行配置仅包含系统配置；在情景执行空间中时，运行配置仅包含该情景。例如，输入 **show running-config** 命令无法查看所有运行配置（系统以及所有情景）。仅显示当前配置。

示例

以下示例在特权 EXEC 模式下在情景和系统之间切换：

```
ciscoasa/admin# changeto system
ciscoasa# changeto context customerA
ciscoasa/customerA#
```

以下示例在接口配置模式下在系统和管理情景之间切换。在执行空间之间切换时，如果您处于配置模式，则模式切换到新执行空间的全局配置模式。

```
ciscoasa(config-if)# changeto context admin
ciscoasa/admin(config)#
```

相关命令

命令	说明
admin-context	设置情景为管理情景。
context	在系统配置中创建安全情景并进入情景配置模式。
show context	显示情景列表（系统执行空间）或有关当前情景的信息。

channel-group

要为 EtherChannel 分配物理接口，请在接口配置模式下使用 **channel-group** 命令。要取消分配接口，请使用此命令的 **no** 形式。

channel-group *channel_id* **mode** {**active** | **passive** | **on**} [**vss-id** {**1** | **2**}]

no channel-group *channel_id*

语法说明

channel_id	指定要将此接口分配到的 EtherChannel，在 1 和 48 之间。
vss-id {**1** | **2**}	（可选）对于集群，如果要将 ASA 连接到 VSS 或 vPC 中的两个交换机，则配置 **vss-id** 关键字以标识此接口连接到的交换机（1 或 2）。还必须对端口通道接口使用 **port-channel span-cluster vss-load-balance** 命令。
mode {**active** | **passive** | **on**}	可以将 EtherChannel 中的每个物理接口配置为： • Active（主动）- 发送和接收链路聚合控制协议 (LACP) 更新。主动 EtherChannel 可以与主动或被动 EtherChannel 建立连接。除非需要最大限度地减少 LACP 流量，否则应使用主用模式。 • Passive（被用）- 接收 LACP 更新。被动 EtherChannel 只能与主动 EtherChannel 建立连接。 • On（开启）- EtherChannel 始终开启，不使用 LACP。“ 开启 ” 的 EtherChannel 只能与另一个 “ 开启 ” 的 EtherChannel 建立连接。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。
9.0(1)	我们添加了 **vss-id** 关键字以支持 ASA 集群和跨区 EtherChannel。

使用指南

每个通道组可以有 8 个活动接口。请注意，最多可以为一个通道组分配 16 个接口。当只有 8 个接口处于活动状态时，其余接口可以用作备用链路，以防接口故障。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口决定正确的类型和速度。

如果此通道 ID 的端口通道接口尚未存在于配置中，则添加一个端口通道接口：

interface port-channel *channel_id*

链路聚合控制协议 (LACP) 将在两个网络设备之间交换链路聚合控制协议数据单元 (LACPDU)，进而聚合接口。LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。它还将处理配置错误，并检查成员接口的两端是否连接到正确的信道组。当接口出现故障时，“ 开启 ” 模式不能使用通道组中的备用接口，并且不会检查连接和配置。

ASA 集群

可以将每 ASA 的多个接口包括在跨区 EtherChannel 中。每 ASA 有多个接口专用于连接到 VSS 或 vPC 中的两个交换机。如果将 ASA 连接到 VSS 或 vPC 中的两个交换机，则应该使用 **vss-load-balance** 关键字启用 VSS 负载平衡。此功能可确保 ASA 与 VSS（或 vPC ）对之间的物理链路连接实现均衡。启用负载平衡前，您必须在 **channel-group** 命令中为每个成员接口配置 **vss-id** 关键字。

示例

以下示例为通道组 1 分配接口：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# channel-group 1 mode passive
```

相关命令

命令	说明
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

character-encoding

要指定 WebVPN 入口页面中的全局字符编码，请在 webvpn 配置模式下使用 **character-encoding** 命令。要删除字符编码属性的值，请使用此命令的 **no** 形式。

character-encoding *charset*

no character-encoding *charset*

语法说明

charset	字符串包含最多 40 个字符，并且其值与在 http://www.iana.org/assignments/character-sets 中标识的有效字符集之一相等。您可以使用在此页面上列出的字符集的名称或别名。示例包括 iso-8859-1、shift_jis 和 ibm850。 字符串不区分大小写。命令解释程序在 ASA 配置中将大写字母转换为小写字母。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

字符编码（也称为 “ 字符代码 ” 和 “ 字符集 ”）是用来表示数据的原始数据（如 0s 和 1s）和字符对。语言决定了要使用的字符编码方法。一些语言使用相同的方法，另一些不是。通常，地理区域决定了浏览器使用的默认编码方法，但用户可以更改此设置。浏览器也可以检测页面上指定的编码，并相应地呈现文档。字符编码属性可让用户指定 WebVPN 入口页面中的字符编码方法的值，以确保浏览器正确呈现该页面，而不管用户使用浏览器时所在的区域或对浏览器进行的任何更改。

默认情况下，字符编码属性是所有 WebVPN 入口页面都会继承的全局设置。但是，用户可以覆盖通用互联网文件系统 (CIFS) 服务器的文件编码属性，这些服务器使用与字符编码属性值不同的字符编码。对需要不同字符编码的 CIFS 服务器使用不同的文件编码值。

从 CIFS 服务器下载到 WebVPN 用户的 WebVPN 入口页面会对用于标识服务器的 WebVPN 文件编码属性的值进行编码，否则这些页面将继承字符编码属性的值。远程用户浏览器将此值映射到字符编码集中的条目，以确定要使用的正确字符集。如果 WebVPN 配置未指定 CIFS 服务器的文件编码条目，并且字符编码属性未设置，则 WebVPN 入口页面不指定值。如果 WebVPN 入口页面未指定字符编码，或者指定了远程浏览器不支持的字符编码值，则远程浏览器将使用自己的默认编码。

如果正确呈现文件名或目录路径以及页面是一个问题，则 CIFS 服务器到相应字符编码的映射（全局使用 webvpn 字符编码属性，个别使用文件编码覆盖）会提供 CIFS 页面的准确处理和显示。

注意　字符编码和文件编码值未排除浏览器将使用的字体系列。如以下示例所示，如果使用日文 Shift_JIS 字符编码，则用户需要在 webvpn 定制命令模式下使用 **page style** 命令补充其中一个值的设置，或者在 webvpn 定制命令模式下输入 **no page style** 命令删除字体系列。

当 WebVPN 入口页面的字符集属性没有值时，远程浏览器上设置的编码类型决定了此属性。

示例

以下示例将字符编码属性设置为支持日文 Shift_JIS 字符，删除字体系列，并保留默认背景颜色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# character-encoding shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

相关命令

命令	说明
debug webvpn cifs	显示有关 CIFS 服务器的调试消息。
file-encoding	指定 CIFS 服务器以及相关的字符编码以覆盖此属性的值。
show running-config [**all**] **webvpn**	显示 WebVPN 的运行配置。使用 **all** 关键字以包括默认配置。

checkheaps

要配置 checkheaps 验证间隔，请在全局配置模式下使用 **checkheaps** 命令。要将此值设置为默认值，请使用此命令的 **no** 形式。

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

语法说明

check-interval	设置缓冲区验证间隔。缓冲区验证过程会检查堆（已分配和已释放的内存缓冲区）的健全性。每次调用该过程时，ASA 都会检查整个堆，验证每个内存缓冲区。如果存在差异，ASA 将发出 “allocated buffer error”（分配的缓冲区错误）或 “free buffer error”（空闲缓冲区错误）。如果存在错误，ASA 将在可能的情况下转储回溯信息并重新加载。
seconds	设置间隔（以秒为单位，在 1 到 2147483 之间）。
validate-checksum	设置代码空间校验和验证间隔。当 ASA 首次启动时，ASA 会计算整个代码的哈希值。之后，在定期检查期间，ASA 生成新的哈希值并将其与原始值进行比较。如果存在不匹配，ASA 将发出 “text checksum checkheaps error”（文本校验和 checkheaps 错误）。如果存在错误，ASA 将在可能的情况下转储回溯信息并重新加载。

默认值

默认间隔为 60 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

Checkheaps 是验证堆内存缓冲区健全性（动态内存分配自系统堆内存区域）和代码区域完整性的定期过程。

示例

以下示例将缓冲区分配间隔设置为 200 秒，将代码空间校验和间隔设置为 500 秒：

```
ciscoasa(config)# checkheaps check-interval 200
ciscoasa(config)# checkheaps validate-checksum 500
```

相关命令

命令	说明
show checkheaps	显示 checkheaps 统计信息。

check-retransmission

为防止 TCP 重传式攻击，请在 tcp 映射配置模式下使用 **check-retransmission** 命令。要删除此指定，请使用此命令的 **no** 形式。

check-retransmission

no check-retransmission

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TCP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

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** 命令定义流量类别，并使用 **tcp-map** 命令定制 TCP 检查。使用 **policy-map** 命令应用新的 TCP 映射。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。为防止不一致重新传输的终端系统解释中出现 TCP 重传式攻击，请在 tcp 映射配置模式下使用 **check-retransmission** 命令。

ASA 将努力验证重传数据是否与原始数据相同。如果数据不匹配，则连接将被 ASA 丢弃。启用此功能后，只按顺序允许 TCP 连接上的数据包。有关详细信息，请参阅 **queue-limit** 命令。

示例

以下示例对所有 TCP 流启用 TCP 校验重传功能：

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# check-retransmission
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	说明
class	指定要用于流量分类的类映射。
help	显示 **policy-map**、**class** 和 **description** 命令的语法帮助。
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。

checksum-verification

要启用或禁用 TCP 校验和验证，请在 tcp 映射配置模式下使用 **checksum-verification** 命令。要删除此指定，请使用此命令的 **no** 形式。

checksum-verification

no checksum-verification

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用校验和验证。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TCP 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

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** 命令定义流量类别，并使用 **tcp-map** 命令定制 TCP 检查。使用 **policy-map** 命令应用新的 TCP 映射。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 映射配置模式下使用 **checksum-verification** 命令以启用 TCP 校验和验证。如果校验失败，数据包将被丢弃。

示例

以下示例对 10.0.0.0 到 20.0.0.0 的 TCP 连接启用 TCP 校验和验证：

```
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)# checksum-verification

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	说明
class	指定要用于流量分类的类映射。
help	显示 **policy-map**、**class** 和 **description** 命令的语法帮助。
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。

cipc security-mode authenticated

要使 Cisco IP Communicator (CIPC) 软电话在语音和数据 VLAN 场景中部署后工作在已验证模式，请在电话代理配置模式下使用 **cipc security-mode authenticated** 命令。要在 CIPC 软电话支持加密时关闭此命令，请使用此命令的 **no** 形式。

cipc security-mode authenticated

no cipc security-mode authenticated

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，通过此命令的 no 形式禁用此命令。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

通过 VLAN 分离语音和数据流量是一项安全最佳实践，可以使语音流避开试图渗透数据 VLAN 的安全威胁。但是，Cisco IP Communicator (CIPC) 软电话应用必须连接到语音 VLAN 上相应的 IP 电话。此要求使分离语音和数据 VLAN 成为一个问题，因为 SIP 和 SCCP 协议会针对范围广泛的端口动态协商 RTP/RTCP 端口。此动态协商需要在两个 VLAN 之间开放一系列端口。

注意　不支持身份验证模式的 CIPC 早期版本不支持电话代理。

要允许数据 VLAN 上的 CIPC 软电话连接到语音 VLAN 上相应的 IP 电话，而无需访问两个 VLAN 之间的广泛端口，可以使用 **cipc security-mode authenticated** 命令配置电话代理。

此命令允许电话代理查找 CIPC 配置文件并强制 CIPC 软电话处于已验证模式而不是加密模式，因为 CIPC 的当前版本不支持加密模式。

此命令启用后，电话代理解析电话配置文件以确定电话是否为 CIPC 软电话并将安全模式更改为已验证。此外，仅当默认情况下电话代理强制所有电话处于加密模式时，CIPC 软电话才支持已验证模式。

示例

以下示例展示当在语音和数据 VLAN 场景中部署 Cisco IP Communicator (CIPC) 软电话时，如何使用 **cipc security-mode authenticated** 命令强制 CIPC 软电话工作在已验证模式。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)#cipc security-mode authenticated
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。

clacp static-port-priority

要禁用集群跨区 EtherChannel（活动的 EtherChannel 成员超过 8 个时需要）的 LACP 中的动态端口优先级，请在全局配置模式下使用 **clacp static-port-priority** 命令。要启用动态端口优先级，请使用此命令的 **no** 形式。

clacp static-port-priority

no clacp static-port-priority

语法说明

此命令没有任何参数或关键字。

命令默认值

默认情况下禁用此命令；启用动态端口优先级。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	我们引入了此命令。

使用指南

某些交换机不支持动态端口优先级，因此此命令可提高交换机兼容性。此外，它可支持 8 个以上的活动跨区 EtherChannel 成员，最多支持 32 个成员。如果不使用此命令，则仅支持 8 个活动成员和 8 个备用成员。

ASA EtherChannel 最多支持 16 条活动链路。对于*跨区* EtherChannel，如果与 vPC 中的两个交换机一起使用并且您使用 **clacp static-port-priority** 命令禁用了动态端口优先级，则该功能将扩展为支持集群中的最多 32 条活动链路。交换机必须支持具有 16 条活动链路的 EtherChannel，例如，具有 F2 系列 10 千兆以太网模块的 Nexus 7000。

对于 VSS 或 vPC 中支持 8 条活动链路的交换机，可以在跨区 EtherChannel 中配置 16 条活动链路（每个交换机连接 8 条活动链路）。

注意　如果想要在跨区 EtherChannel 中使用 8 条以上的活动链路，则无法同时使用备用链路；要支持 9 至 32 条活动链路，需要您禁用允许使用备用链路的 cLACP 动态端口优先级。

示例

以下示例禁用动态端口优先级：

```
ciscoasa(config)# clacp static-port-priority
```

相关命令

命令	说明
clacp system-mac	设置 cLACP 系统 ID。

clacp system-mac

要手动配置 ASA 集群中主设备上的 cLACP 系统 ID，请在集群组配置模式下使用 **clacp system-mac** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

no clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

语法说明

mac_address	手动设置 *H.H.H* 形式的系统 ID，其中 H 是 16 位十六进制数。例如，MAC 地址 00-0A-00-00-AA-AA 输入为 000A.0000.AAAA。
auto	自动生成系统 ID。
system-priority ***number***	设置系统优先级，在 1 和 65535 之间。优先级用于决定哪个设备负责做出捆绑决策。默认情况下，ASA 使用优先级 1，即最高优先级。该优先级需要高于交换机上的优先级。

命令默认值

默认情况下，系统 mac 自动生成 (**auto**)。

默认情况下，系统优先级为 1。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。集群中的 ASA 在 cLACP 协商中协作，以便它们对交换机表现为单个（虚拟）设备。cLACP 协商中的一个参数是 MAC 地址格式的系统 ID。所有 ASA 均使用同一系统 ID：由主设备（默认）自动生成并复制到所有从设备；或在此命令中手动指定。您可能想要手动配置 MAC 地址，例如进行故障排除，因此可以使用易于识别的 MAC 地址。通常，将使用自动生成的 MAC 地址。

此命令并非引导程序配置的一部分，而是从主设备复制到从属设备上的。但是，在启用集群后无法更改此值。

示例

以下示例手动配置系统 ID：

```
cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    health-check
    clacp system-mac 000a.0000.aaaa
    enable noconfirm
```

相关命令

命令	说明
cluster group	配置集群参数。

class (global)

要创建将安全情景分配到的资源类，请在全局配置模式下使用 **class** 命令。要删除类，请使用此命令的 **no** 形式。

class *name*

no class *name*

语法说明

name	指定字符串形式的名称，最长 20 个字符。要设置默认类的限制，请输入 **default** 作为名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

默认情况下，除非对每个情景实施最大限制，否则所有安全情景可以无限访问 ASA 的资源。但是，如果您发现一个或者多个情景使用过多资源，例如，它们导致其他情景被拒绝连接，那么您可以配置资源管理来限制每个情景对资源的使用。

ASA 通过将情景分配到资源类来管理资源。每个情景使用由类设置的资源限制。

当创建类时，ASA 不会为分配到该类的每个情景都留出一部分资源；相反，ASA 会设置情景的上限。如果超订用资源或允许某些资源无限制，一些情景可以 “ 用尽 ” 这些资源，而可能影响其他情景的服务。请参阅 **limit-resource** 命令设置类的资源。

如果未向另一类分配情景，则所有情景都属于默认类别；您无需主动为默认类分配情景。

如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类有任何未定义的设置，则成员情景使用默认类的相应限制。例如，如果创建的类对所有并发连接具有 %2 限制，但没有任何其他限制，则所有其他限制均继承自默认类。相反，如果创建的类对所有资源都有限制，则该类不使用默认类的设置。

默认情况下，默认类提供对所有情景的资源的无限制访问，除了以下默认设置为每个情景所允许的上限的限制：

- Telnet 会话 - 5 个会话。
- SSH 会话 - 5 个会话。
- MAC 地址 - 65535 个条目。

示例

以下示例将 conns 的默认类限制设置为 10%，而非无限制：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

所有其他资源仍然不受限制。

要添加名为 gold 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
```

相关命令

命令	说明
clear configure class	清除类配置。
context	配置安全情景。
limit-resource	设置类的资源限制。
member	为资源类分配情景。
show class	显示分配到类的情景。

class (policy-map)

要为用于向类映射流量分配操作的策略映射分配类映射，请在策略映射配置模式下使用 **class** 命令。要从策略映射中删除类映射，请使用此命令的 **no** 形式。

class *classmap_name*

no class *classmap_name*

语法说明

classmap_name	指定类映射的名称。对于第 3/4 层策略映射（**policy-map** 命令），必须指定第 3/4 层类映射名称（**class-map** 或 **class-map type management** 命令）。对于检查策略映射（**policy-map type inspect** 命令），必须指定检查类映射名称（**class-map type inspect** 命令）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使用 **class** 命令，请使用模块化策略框架。要在第 3/4 层策略映射中使用类，请输入以下命令：

1. **class-map** - 标识要对其执行操作的流量。
2. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. *所支持功能的命令* - 对于给定的类映射，可以为各个功能配置多种操作，包括 QoS、应用检查、CSC 或 AIP SSM、TCP 和 UDP 连接限制以及超时和 TCP 规范化。有关每种功能可使用的命令的更多详细信息，请参阅 CLI 配置指南。
3. **service-policy** - 向接口分配策略映射或全局分配策略映射。

要在检查策略映射中使用类，请输入以下命令：

1. **class-map type inspect** - 标识要对其执行操作的流量。
2. **policy-map type inspect** - 标识与每个类映射关联的操作。
   a. **class** - 标识要对其执行操作的检查类映射。

b. *应用类型的命令* - 请参阅 CLI 配置指南了解每种应用类型可使用的命令。检查策略映射的类配置模式支持的操作包括：

– 丢弃数据包

– 丢弃连接

– 重置连接

– 记录

– 对消息进行速率限制

– 屏蔽内容

c. **parameters** - 配置影响检查引擎的参数。CLI 进入参数配置模式。请参阅 CLI 配置指南了解可用命令。

3. **class-map** - 标识要对其执行操作的流量。

4. **policy-map** - 标识与每个类映射关联的操作。

a. **class** - 标识要对其执行操作的第 3/4 层类映射。

b. **inspect** *application inspect_policy_map* - 启用应用检查，并调用检查策略映射以执行特殊操作。

5. **service-policy** - 向接口分配策略映射或全局分配策略映射。

配置始终包括匹配所有流量的名为 **class-default** 的类映射。在每个第 3/4 层策略映射的末尾，配置包括未定义任何操作的 **class-default** 类映射。当您想要匹配所有流量，但不想创建另一个类映射时，可以使用此类映射。实际上，某些功能只能为 **class-default** 类映射配置，如 **shape** 命令。

包括 **class-default** 类映射在内，在一个策略映射中最多可以配置 63 个 **class** 和 **match** 命令。

示例

以下是包含 **class** 命令的连接策略的 **policy-map** 命令示例。它限制了允许到达 Web 服务器 10.1.1.1 的连接数：

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server

ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

以下示例展示了多匹配在策略映射中的工作原理：

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

以下示例展示了流量如何与第一个可用的类映射进行匹配，以及将不会与在同一功能域中指定操作的任何后续类映射进行匹配：

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

启动 Telnet 连接时，它会与 **class telnet_traffic** 进行匹配。同样，如果启动 FTP 连接，则它会与 **class ftp_traffic** 进行匹配。对于除 Telnet 和 FTP 外的任何 TCP 连接，它将与 **class tcp_traffic** 进行匹配。即使 Telnet 或 FTP 连接可与 **class tcp_traffic** 进行匹配，ASA 也不会执行此匹配，因为它们之前已与其他类进行匹配。

相关命令

命令	说明
class-map	创建第 3/4 层类映射。
class-map type management	为管理流量创建第 3/4 层类映射。
clear configure policy-map	删除所有策略映射配置，除了 **service-policy** 命令中正在使用的任何策略映射。
match	定义流量匹配参数。
policy-map	配置策略；即，一个或多个流量类的关联，每个类与一个或多个操作关联。

class-map

使用 模块化策略框架 时，通过在全局配置模式下使用 **class-map** 命令（不带 **type** 关键字）来标识您想要对其应用操作的第 3 层或第 4 层流量。要删除类映射，请使用此命令的 **no** 形式。

class-map *class_map_name*

no class-map *class_map_name*

语法说明

class_map_name	指定类映射名称，最长 40 个字符。名称 “class-default” 和任何以 “_internal” 或 “_default” 开头的名称均已保留。所有类型的类映射均使用同一名称空间，因此无法重复使用已被其他类型的类映射使用的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此类型的类映射仅用于第 3/4 层通过流量。对于以 ASA 为目标的管理流量，请参阅 **class-map type management** 命令。

第 3/4 层类映射标识您要应用操作的第 3 层和第 4 层流量。您可以为每个第 3/4 层策略映射创建多个第 3/4 层类映射。

默认类映射

配置包括 ASA 在默认全局策略中使用的默认第 3/4 层类映射。它的名称为 **inspection_default**，并与默认检查流量匹配：

```
class-map inspection_default
 match default-inspection-traffic
```

默认配置中存在的另一个类映射名为 class-default，它匹配所有流量：

```
class-map class-default
 match any
```

此类映射出现在所有第 3/4 层策略映射的末尾，并从实质上告知 ASA 不要对所有其他流量执行任何操作。如果需要，可以使用 class-default 类映射，而不是创建您自己的 **match any** 类映射。实际上，某些功能只能用于 class-default，如 QoS 流量整形。

最大类映射数量

在单模式或多模式的每个情景中，所有类型的类映射的最大数量为 255。类映射包括下列类型：

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- 策略映射类型检查配置模式中的 **match** 命令

此限制还包括所有类型的默认类映射。

配置概述

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 或 **class-map type management** 命令标识您要对其应用操作的第 3 层和第 4 层流量。
2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。
3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。
4. 使用 **service-policy** 命令在接口上激活操作。

使用 **class-map** 命令进入类映射配置模式。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。一个第 3/4 层类映射最多包含一个用于标识类映射中包括的流量的 **match** 命令（**match tunnel-group** 和 **match default-inspection-traffic** 命令除外）。

示例

以下示例创建四个第 3/4 层类映射：

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp

ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp

ciscoasa(config-cmap)# class-map all_http
ciscoasa(config-cmap)# description "This class-map matches all HTTP traffic"
ciscoasa(config-cmap)# match port tcp eq http

ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

相关命令

命令	说明
class-map type management	为流向 ASA 的流量创建类映射。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
service-policy	通过将策略映射与一个或多个接口关联，创建安全策略。
show running-config class-map	显示有关类映射配置的信息。

class-map type inspect

使用 模块化策略框架 时，通过在全局配置模式下使用 **class-map type inspect** 命令来匹配特定于检查应用的条件。要删除检查类映射，请使用此命令的 **no** 形式。

class-map type inspect *application* [**match-all** | **match-any**] *class_map_name*

no class-map [**type inspect** *application* [**match-all** | **match-any**]] *class_map_name*

语法说明

application	指定要匹配的应用流量的类型。可用类型包括： • **dns** • **ftp** • **h323** • **http** • **im** • **scansafe** • **sip**
class_map_name	指定类映射名称，最长 40 个字符。名称 “class-default” 和任何以 “_internal” 或 “_default” 开头的名称均已保留。所有类型的类映射均使用同一名称空间，因此无法重复使用已被其他类型的类映射使用的名称。
match-all	（可选）指定流量必须匹配所有条件才能匹配类映射。如果未指定选项，则 **match-all** 为默认值。
match-any	（可选）指定流量可以匹配一个或多个条件以匹配类映射。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	增加了 **match-any** 关键字。

使用指南

模块化策略框架 让您可以配置用于许多应用检查的特殊操作。在第 3/4 层策略映射中启用检查引擎时，还可以启用在*检查策略映射*中定义的操作（请参阅 **policy-map type inspect** 命令）。

在检查策略映射中，可以通过创建检查类映射来标识要对其执行操作的流量。类映射包含一个或多个 **match** 命令。（如果要将单个条件与操作配对，还可以直接在检查策略映射中使用 **match** 命令）。可以匹配特定于应用的条件。例如，对于 DNS 流量，可以在 DNS 查询中匹配域名。

类映射将多个流量匹配分组（在 match-all 类映射中），或让您匹配一系列匹配中的任意一个（在 match-any 类映射中）。创建类映射与直接在检查策略映射中定义流量匹配的差异是，类映射可让您将多个匹配命令分组，并且您可以重复使用类映射。对于在此类映射中标识的流量，可以指定丢弃、重置和 / 或在检查策略映射中记录连接等操作。

在单模式或多模式的每个情景中，所有类型的类映射的最大数量为 255。类映射包括下列类型：

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- 策略映射类型检查配置模式中的 **match** 命令

此限制还包括所有类型的默认类映射。请参阅 **class-map** 命令以了解详细信息。

示例

以下示例创建必须匹配所有条件的 HTTP 类映射：

```
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
```

以下示例创建可匹配任意条件的 HTTP 类映射：

```
ciscoasa(config-cmap)# class-map type inspect http match-any monitor-http
ciscoasa(config-cmap)# match request method get
ciscoasa(config-cmap)# match request method put
ciscoasa(config-cmap)# match request method post
```

相关命令

命令	说明
class-map	为通过流量创建第 3/4 层类映射。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
service-policy	通过将策略映射与一个或多个接口关联，创建安全策略。
show running-config class-map	显示有关类映射配置的信息。

class-map type management

使用 模块化策略框架 时，通过在全局配置模式下使用 **class-map type management** 命令来标识以您想要对其应用操作的 ASA 为目标的第 3 层或第 4 层管理流量。要删除类映射，请使用此命令的 **no** 形式。

class-map type management *class_map_name*

no class-map type management *class_map_name*

语法说明

class_map_name	指定类映射名称，最长 40 个字符。名称 “class-default” 和任何以 “_internal” 或 “_default” 开头的名称均已保留。所有类型的类映射均使用同一名称空间，因此无法重复使用已被其他类型的类映射使用的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	对于流向 ASA 的管理流量，**set connection** 命令现在可用于第 3/4 层管理类映射。只有 **conn-max** 和 **embryonic-conn-max** 关键字可用。

使用指南

此类型的类别映射仅用于管理流量。对于通过流量，请参阅 **class-map** 命令（不带 **type** 关键字）。

对于流向 ASA 的管理流量，您可能想要执行特定于此类流量的操作。可用于策略映射中的管理类映射的操作类型专用于管理流量。例如，此类型的类映射可让您检查 RADIUS 记账流量和设置连接限制。

第 3/4 层类映射标识您要应用操作的第 3 层和第 4 层流量。在单模式或多模式的每个情景中，所有类型的类映射的最大数量为 255。

您可以为每个第 3/4 层策略映射创建多个第 3/4 层类映射（管理或通过流量）。

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 和 **class-map type management** 命令标识您要对其应用操作的第 3 层和第 4 层流量。
2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。
3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。
4. 使用 **service-policy** 命令在接口上激活操作。

使用 **class-map type management** 命令进入类映射配置模式。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。您可以指定可与访问列表或者 TCP 或 UDP 端口匹配的管理类映射。一个第 3/4 层类映射最多可包含一个用于标识类映射中包括的流量的 **match** 命令。

在单模式或多模式的每个情景中，所有类型的类映射的最大数量为 255。类映射包括下列类型：

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- 策略映射类型检查配置模式中的 **match** 命令

此限制还包括所有类型的默认类映射。请参阅 **class-map** 命令以了解详细信息。

示例

以下示例创建第 3/4 层管理类映射：

```
ciscoasa(config)# class-map type management radius_acct
ciscoasa(config-cmap)# match port tcp eq 10000
```

相关命令

命令	说明
class-map	为通过流量创建第 3/4 层类映射。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
service-policy	通过将策略映射与一个或多个接口关联，创建安全策略。
show running-config class-map	显示有关类映射配置的信息。

class-map type regex

使用 模块化策略框架 时，通过在全局配置模式下使用 **class-map type regex** 命令来分组与匹配文本一起使用的正则表达式。要删除正则表达式类映射，请使用此命令的 **no** 形式。

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

语法说明

class_map_name	指定类映射名称，最长 40 个字符。名称“class-default”和任何以“_internal”或“_default”开头的名称均已保留。所有类型的类映射均使用同一名称空间，因此无法重复使用已被其他类型的类映射使用的名称。
match-any	指定如果流量仅匹配其中一个正则表达式，则其匹配类映射。**match-any** 是唯一选项。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

模块化策略框架 让您可以配置用于许多应用检查的特殊操作。在第 3/4 层策略映射中启用检查引擎时，还可以启用在*检查策略映射*中定义的操作（请参阅 **policy-map type inspect** 命令）。

在检查策略映射中，您可以确定您要采取相应的通过创建包含检测类映射的流量或更多匹配的命令您也可以使用直接中检查策略映射匹配的命令。一些匹配的命令，您可以标识使用正则表达式；数据包中的文本例如，您可以匹配 URL 字符串内部 HTTP 数据包。可以在正则表达式类映射中分组正则表达式。

在创建正则表达式类映射之前，请使用 **regex** 命令创建正则表达式。然后，使用 **match regex** 命令标识在类映射配置模式下指定的正则表达式。

在单模式或多模式的每个情景中，所有类型的类映射的最大数量为 255。类映射包括下列类型：

- **class-map**
- **class-map type management**
- **class-map type inspection**

- **class-map type regex**
- 策略映射类型检查配置模式中的 **match** 命令

此限制还包括所有类型的默认类映射。请参阅 **class-map** 命令以了解详细信息。

示例

以下示例创建两个正则表达式，并将它们添加到正则表达式类映射。如果流量包含字符串“example.com”或“example2.com”，则其匹配该类映射。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
```

相关命令

命令	说明
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
service-policy	通过将策略映射与一个或多个接口关联，创建安全策略。
regex	创建正则表达式。

clear aaa kerberos

要清除有关 ASA 的所有 Kerberos 票证信息，请在 webvpn 配置模式下使用 **clear aaa kerberos** 命令。

[**cluster exec**] **clear aaa kerberos** [**username** *user* | **host** *ip* | *hostname*]

语法说明

cluster exec	（可选）在集群环境中，让您在一个设备中发出 **clear aaa kerberos** 命令，同时在所有其他设备中运行该命令。
host	指定要从 Kerberos 票证清除的特定主机。
hostname	指定主机名。
ip	指定主机的 IP 地址。
username	指定要从 Kerberos 票证清除的特定用户。

默认值

此命令不存在默认值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了 **cluster exec** 选项。

使用指南

在 webvpn 配置模式下使用 **clear aaa kerberos** 命令可清除 ASA 上缓存的所有 Kerberos 票证。**username** 和 **host** 关键字用于清除特定用户或主机的 Kerberos 票证。

示例

以下示例展示 **clear aaa kerberos** 命令的用法：

```
ciscoasa(config)# clear aaa kerberos
```

相关命令

命令	说明
show aaa kerberos	显示 ASA 上缓存的所有 Kerberos 票证。

clear aaa local user fail-attempts

要将失败的用户身份验证尝试次数重置为零，并且不修改用户锁定状态，请在特权 EXEC 模式下使用 **clear aaa local user fail-attempts** 命令。

[**cluster exec**] **clear aaa local user authentication fail-attempts** {**username** *name* | **all**}

语法说明

all	将所有用户的失败尝试计数器重置为 0。
cluster exec	（可选）在集群环境中，让您在一个设备中发出 **clear aaa local user authentication fail-attempts** 命令，同时在所有其他设备中运行该命令。
name	指定特定用户名，其失败尝试计数器将重置为 0。
username	指示以下参数是用户名，其失败尝试计数器将重置为 0。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了 **cluster exec** 选项。

使用指南

如果用户在几次尝试后无法进行身份验证，请使用此命令。

在经过配置的失败身份验证尝试次数后，用户会被系统锁定，且无法成功登录，直到系统管理员解锁该用户名或系统重启。当用户成功通过身份验证或 ASA 重新启动后，失败尝试次数将重置为零，并且锁定状态重置为 No（否）。此外，如果配置最近经过修改，系统会将该计数器重置为零。

锁定或解锁用户名会产生系统日志消息。具有 15 级权限的系统管理员无法被锁定。

示例

以下示例展示如何使用 **clear aaa local user authentication fail-attempts** 命令将用户名 anyuser 的失败尝试计数器重置为 0：

```
ciscoasa(config)# clear aaa local user authentication fail-attempts username anyuser
ciscoasa(config)#
```

以下示例展示如何使用 **clear aaa local user authentication fail-attempts** 命令将所有用户的失败尝试计数器重置为 0：

```
ciscoasa(config)# clear aaa local user authentication fail-attempts all
ciscoasa(config)#
```

相关命令

命令	说明
aaa local authentication attempts max-fail	配置允许的用户身份验证失败尝试次数限制。
clear aaa local user lockout	将用户身份验证失败尝试次数重置为零，并且不修改用户的锁定状态。
show aaa local user [locked]	显示当前锁定的用户名的列表。

clear aaa local user lockout

要清除指定用户的锁定状态并将其失败尝试计数器设置为 0，请在特权 EXEC 模式下使用 **clear aaa local user lockout** 命令。

[**cluster exec**] **clear aaa local user lockout** {**username** *name* | **all**}

语法说明

all	将所有用户的失败尝试计数器重置为 0。
cluster exec	（可选）在集群环境中，让您在一个设备中发出 **clear aaa local user lockout** 命令，同时在所有其他设备中运行该命令。
name	指定特定用户名，其失败尝试计数器将重置为 0。
username	指示以下参数是用户名，其失败尝试计数器将重置为 0。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了 **cluster exec** 选项。

使用指南

您可以使用 **username** 选项指定单个用户或使用 **all** 选项指定全部用户。

此命令仅影响被锁定用户的状态。

管理员无法被设备锁定。

锁定或解锁用户名会生成系统日志消息。

示例

以下示例展示如何使用 **clear aaa local user lockout** 命令清除锁定状态并将用户名 anyuser 的失败尝试计数器重置为 0：

```
ciscoasa(config)# clear aaa local user lockout username anyuser
ciscoasa(config)#
```

相关命令

命令	说明
aaa local authentication attempts max-fail	配置允许的用户身份验证失败尝试次数限制。
clear aaa local user fail-attempts	将用户身份验证失败尝试次数重置为零，并且不修改用户的锁定状态。
show aaa local user [**locked**]	显示当前锁定的用户名的列表。

clear aaa-server statistics

要重置 AAA 服务器的统计信息，请在特权 EXEC 模式下使用 **clear aaa-server statistics** 命令。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

语法说明

groupname	（可选）清除组中服务器的统计信息。
host *hostname*	（可选）清除组中特定服务器的统计信息。
LOCAL	（可选）清除 LOCAL 用户数据库的统计信息。
protocol *protocol*	（可选）清除指定协议的服务器的统计信息： • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

默认值

删除所有组内的所有 AAA 服务器统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为遵守 CLI 指南。在协议值中，**nt** 取代了较早的 **nt-domain**，**sdi** 取代了较早的 **rsa-ace**。

示例

以下示例展示如何重置组中特定服务器的 AAA 统计信息：

```
ciscoasa(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

以下示例展示如何重置整个服务器组的 AAA 统计信息：

```
ciscoasa(config)# clear aaa-server statistics svrgrp1
```

以下示例展示如何重置所有服务器组的 AAA 统计信息：

```
ciscoasa(config)# clear aaa-server statistics
```

以下示例展示如何重置特定协议（此例中为 TACACS+）的 AAA 统计信息：

```
ciscoasa(config)# clear aaa-server statistics protocol tacacs+
```

相关命令

命令	说明
aaa-server protocol	指定并管理 AAA 服务器连接数据的分组。
clear configure aaa-server	删除所有非默认 AAA 服务器组或清除指定组。
show aaa-server	显示 AAA 服务器统计信息。
show running-config aaa-server	显示当前 AAA 服务器配置值。

clear access-list

要清除访问列表计数器，请在全局配置模式下使用 **clear access-list** 命令。

clear access-list *id* **counters**

语法说明

counters	清除访问列表计数器。
id	访问列表的名称或编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当输入 **clear access-list** 命令时，必须指定访问列表的 *id* 才能清除计数器。

示例

以下示例展示如何清除特定访问列表计数器：

```
ciscoasa# clear access-list inbound counters
```

相关命令

命令	说明
access-list extended	向配置添加访问列表并通过防火墙配置 IP 流量的策略。
access-list standard	添加访问列表以标识 OSPF 路由的目标 IP 地址，在路由映射中可使用这些 IP 地址进行 OSPF 重新分配。
clear configure access-list	从运行配置中清除访问列表。
show access-list	按编号显示访问列表条目。
show running-config access-list	显示在自适应安全设备上运行的访问列表配置。

clear arp

要清除动态 ARP 条目或 ARP 统计信息，请在特权 EXEC 模式下使用 **clear arp** 命令。

clear arp [**statistics**]

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除所有 ARP 统计信息：

```
ciscoasa# clear arp statistics
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
arp-inspection	在透明防火墙模式下，检查 ARP 数据包来防止 ARP 欺骗。
show arp statistics	显示 ARP 统计数据。
show running-config arp	显示 ARP 超时的当前配置。

clear asp drop

要清除加速安全路径 (ASP) 丢弃统计信息，请在特权 EXEC 模式下使用 **clear asp drop** 命令。

clear asp drop [**flow** *type* | **frame** *type*]

语法说明

flow	（可选）清除已丢弃的流统计信息。
frame	（可选）清除已丢弃的数据包统计信息。
type	（可选）清除特定过程的已丢弃的流或数据包统计信息。

默认值

默认情况下，此命令清除所有丢弃统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

处理类型包括以下类型：

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
no-ipv6-ipsec
non_tcp_syn
```

```
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

示例

以下示例清除所有丢弃统计信息：

```
ciscoasa# clear asp drop
```

相关命令

命令	说明
show asp drop	显示已丢弃数据包的加速安全路径计数器。

clear asp load-balance history

要清除每个数据包的 ASP 负载平衡历史记录并重置发生自动切换的次数，请在特权 EXEC 模式下使用 **clear asp load-balance history** 命令。

clear asp load-balance history

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令会清除每个数据包的 ASP 负载平衡历史记录并重置发生自动切换的次数。只有 ASA 5585-X 和 ASASM 支持使用此命令。

示例

以下示例清除每个数据包的 ASP 负载平衡历史记录并重置发生自动切换的次数：

```
ciscoasa# clear asp load-balance history
```

相关命令

命令	说明
asp load-balance per-packet	更改负载平衡行为。
show asp load-balance	显示负载平衡器队列大小的柱状图。
show asp load-balance per-packet	显示当前状态、上下限和全局阈值。
show asp load-balance per-packet history	显示当前状态、上下限、全局阈值、自上次重置以来开启和关闭每数据包 ASP 负载平衡的次数、具有时间戳的每数据包 ASP 负载平衡历史记录和开启和关闭的原因。

clear asp table

要清除 ASP ARP 表、ASP 分类表或两者中的命中计数器，请在特权 EXEC 模式下使用 **clear asp table** 命令。

clear asp table [**arp** | **classify**]

语法说明

arp	仅清除 ASP ARP 表中的命中计数器。
classify	仅清除 ASP 分类表中的命中计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	**修改**
7.2(4)	引入了此命令。

使用指南

只有两个选项 **arp** 和 **classify** 在 **clear asp table** 命令中有命中。

示例

以下示例清除所有 ASP 表统计信息：

```
ciscoasa# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands!ciscoasa#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands!ciscoasa#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands!ciscoasa(config)# clear asp
table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands!ciscoasa# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

相关命令

命令	说明
show asp table arp	显示加速安全路径的内容，这可帮助您排查问题。

clear asp table filter

要清除 ASP 过滤表的命中计数器，请在特权 EXEC 模式下使用 **clear asp table filter** 命令。

clear asp table filter [**access-list** *acl-name*]

语法说明

acl-name	仅清除指定访问列表的命中计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

只有 **access-list** 选项在 **clear asp table filter** 命令中有命中。

示例

以下示例清除所有 ASP 过滤表统计信息：

```
ciscoasa# clear asp table filter
```

相关命令

命令	说明
show asp table arp	显示加速安全路径的内容，这可帮助您排查问题。

clear bgp

要使用硬 / 软重新配置来重置边界网关协议 (BGP) 连接，请在特权 EXEC 模式下使用 clear bgp 命令。

多模式 - 系统情景

clear bgp *

多模式 - 用户情景 / 单模式

clear bgp {* [ipv4 {unicast} [**in** | **out** | **soft** [**in** | **out**]] |*autonomous-system-number* | *neighbor-address* **}** [**in** | **out** | **soft** [**in** | **out**]]

语法说明

*	指定将重置所有当前 BGP 会话。
autonomous-system-number	将重置所有 BGP 对等会话的自主系统的编号。在从 1 到 65535 范围内的数量。支持的 4 字节自主系统编号的范围为 65536 到 4294967295（asplain 记数法）以及 1.0 到 65535.65535（asdot 记数法）。 有关自主系统编号格式的更多详细信息，请参阅 router bgp 命令。
neighbor-address	指定仅重置已标识的 BGP 邻居。此参数的值可以是 IPv4 或 IPv6 地址。
in	（可选）启动入站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
out	（可选）启动入站或出站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
soft	（可选）以强制方式清除慢速对等设备状态，并将其移至原始更新组。
ipv4	使用硬 / 软重新配置来重置 IPv4 地址系列会话的 BGP 连接。
unicast	（可选）指定单播地址系列会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

clear bgp 命令可用于启动硬重置或软重新配置。硬重置会断开并重建指定的对等会话并重建 BGP 路由表。软重新配置使用存储的前缀信息来重新配置并激活 BGP 路由表，无需断开现有对等会话。软重新配置使用存储的更新信息（以使用额外内存存储更新为代价），允许您应用新 BGP 策略而无需中断网络。软重新配置可针对入站或出站会话进行配置。

1. 多模式 - 系统情景：

```
ciscoasa(config)# clear bgp *


This command will reset BGP in all contexts.
Are you sure you want to continue ?[no]:
```

2. 单模式 / 多模式 - 用户情景：

```
ciscoasa/c1(config)# clear bgp ?
```

exec 模式命令 / 选项：

```
  *               Clear all peers
  <1-4294967295>  Clear peers with the AS number
  <1.0-XX.YY>     Clear peers with the AS number
  A.B.C.D         BGP neighbor address to clear
  external        Clear all external peers
  ipv4            Address family
  table-map       Update BGP table-map configuration
```

示例

1. 在以下示例中，在系统情景中给定 clear bgp 命令时，所有情景中的所有 bgp 会话都将重置。由于此命令将重置所有 bgp 会话，因此将发出一个警告来确认操作：

```
ciscoasa# clear bgp ?
*  Clear all peers
ciscoasa# clear bgp *


This command will reset BGP in ALL contexts.
Are you sure you want to continue?[no]:
```

2. 在以下示例中，所有 bgp 会话均在单模式或多模式用户情景中重置。不应发出警告来确认单模式 / 用户情景中的操作。

```
ciscoasa# clear bgp * (Single mode)
ciscoasa/c1(config)# clear bgp * (Multiple mode user context)
```

3. 在以下示例中，针对邻居为 10.100.0.1 的入站会话启动软重新配置，出站会话不受影响：

```
ciscoasa(config)# clear bgp 10.100.0.1 soft in (Single mode)
ciscoasa/c1(config)# clear bgp 10.100.0.1 soft in (Multiple mode user context)
```

4. 在以下示例中，在 BGP 邻居路由器上启用路由刷新功能，并针对邻居为 172.16.10.2 的入站会话启动软重新配置，出站会话不受影响：

```
ciscoasa(config)# clear bgp 172.16.10.2 in (Single mode)
ciscoasa/c1(config)# clear bgp 172.16.10.2 in (Multiple mode user context)
```

5. 在以下示例中，针对编号 35700 的自主系统中的所有路由器的会话启动硬重置：

```
ciscoasa(config)# clear bgp 35700 (Single mode)
ciscoasa/c1(config)# clear bgp 35700 (Multiple mode user context)
```

相关命令

命令	说明
clear bgp external	使用硬 / 软重新配置来重置外部边界网关协议 (eBGP) 对等会话。
clear bgp ipv4	使用硬 / 软重新配置来重置 IPv4 地址系列会话的边界网关协议 (BGP) 连接。
clear bgp table-map	在边界网关协议 (BGP) 路由表中刷新表映射配置信息。

clear bgp external

要使用硬 / 软重新配置来重置外部边界网关协议 (eBGP) 对等会话，请在特权 EXEC 模式下使用 clear bgp external 命令。

clear bgp external [**in** |**out** | **soft** [**in**|**out**] | **ipv4 {unicast}** [**in** | **out** | **soft** [**in** | **out**]]

语法说明

in	（可选）启动入站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
out	（可选）启动入站或出站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
soft	（可选）以强制方式清除慢速对等设备状态，并将其移至原始更新组。
ipv4	使用硬 / 软重新配置来重置 IPv4 地址系列会话的 BGP 连接。
unicast	（可选）指定单播地址系列会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

clear bgp external 命令可用于启动 eBGP 邻居会话的硬重置或软重新配置。硬重置会断开并重建指定的对等会话并重建 BGP 路由表。软重新配置使用存储的前缀信息来重新配置并激活 BGP 路由表，无需断开现有对等会话。软重新配置使用存储的更新信息（以使用额外内存存储更新为代价），允许您应用新 BGP 策略而无需中断网络。软重新配置可针对入站或出站会话进行配置。

该命令在系统情景中无效。

示例

在以下示例中，针对所有入站 eBGP 对等会话配置软重新配置：

```
ciscoasa(config)# clear bgp external soft in (Single mode)
ciscoasa/c1(config clear bgp external soft in (Multiple mode user context)
```

在以下示例中，清除所有出站地址系列 IPv4 组播 eBGP 对等会话：

```
ciscoasa(config)# clear bgp external ipv4 multicast out (Single mode)
ciscoasa/c1(config)# clear bgp external ipv4 multicast out (Multiple mode user context)
```

相关命令

命令	说明
clear bgp	使用硬 / 软重新配置来重置边界网关协议 (eBGP) 对等会话。
clear bgp ipv4	使用硬 / 软重新配置来重置 IPv4 地址系列会话的边界网关协议 (BGP) 连接。
clear bgp table-map	在边界网关协议 (BGP) 路由表中刷新表映射配置信息。

clear bgp ipv4

要使用硬 / 软重新配置来重置 IPv4 地址系列会话的边界网关协议 (eBGP) 对等会话，请在特权 EXEC 模式下使用 **clear bgp ipv4** 命令。

clear bgp ipv4 unicast {autonomous-system-number [in |out | soft [in|out]}

语法说明

autonomous-system-number	将重置所有 BGP 对等会话的自主系统的编号。在从 1 到 65535 范围内的数量。支持的 4 字节自主系统编号的范围为 65536 到 4294967295（asplain 记数法）以及 1.0 到 65535.65535（asdot 记数法）。 有关自主系统编号格式的更多详细信息，请参阅 router bgp 命令。
in	（可选）启动入站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
out	（可选）启动入站或出站重新配置。如果未指定 in 和 out 关键字，入站和出站会话都会重置。
soft	（可选）以强制方式清除慢速对等设备状态，并将其移至原始更新组。
unicast	（可选）指定单播地址系列会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

clear bgp ipv4 命令可用于启动硬重置或软重新配置。硬重置会断开并重建指定的对等会话并重建 BGP 路由表。软重新配置使用存储的前缀信息来重新配置并激活 BGP 路由表，无需断开现有对等会话。软重新配置使用存储的更新信息（以使用额外内存存储更新为代价），允许您应用新 BGP 策略而无需中断网络。软重新配置可针对入站或出站会话进行配置。

该命令在系统情景中无效。

示例

1. 在以下示例中，针对自主系统 65400 的 IPv4 单播地址系列会话中的 BGP 邻居入站会话启动软重新配置，出站会话不受影响：

```
ciscoasa(config)# clear bgp ipv4 unicast 65400 soft in (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 65400 soft in (Multiple mode user context)
```

2. 在以下示例中，针对编号为 65538（asplain 记数法）的 4 字节自主系统的 IPv4 单播地址系列会话中的 BGP 邻居启动硬重置。

```
ciscoasa(config)# clear bgp ipv4 unicast 65538 (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 65538 (Multiple mode user context)
```

3. 在以下示例中，针对编号为 1.2（asdot 记数法）的 4 字节自主系统的 IPv4 单播地址系列会话中的 BGP 邻居启动硬重置。

```
ciscoasa(config)# clear bgp ipv4 unicast 1.2 (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 1.2 (Multiple mode user context)
```

相关命令

命令	说明
clear bgp	使用硬 / 软重新配置来重置边界网关协议 (eBGP) 对等会话。
clear bgp external	使用硬 / 软重新配置来重置外部边界网关协议 (BGP) 连接。
clear bgp table-map	在边界网关协议 (BGP) 路由表中刷新表映射配置信息。

clear bgp table-map

要刷新边界网关协议 (BGP) 路由表中的表映射配置信息，请在特权 EXEC 模式下使用 **clear bgp table-map** 命令。

clear bgp [**ipv4 unicast**] **table-map**

语法说明

ipv4	（可选）刷新 IPv4 地址系列会话的表映射配置信息。
unicast	（可选）刷新单播地址系列会话的表映射配置信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

clear bgp table-map 命令用于清除或刷新 BGP 路由表中的表映射配置信息。此命令可用于清除配置了 BGP 策略记账功能的流量索引信息。

该命令在系统情景中无效。

示例

1. 在以下示例中，配置表映射并设置流量索引。在输入 clear bgp table-map 命令后，将应用新策略。

```
ciscoasa(config)# route-map SET_BUCKET permit 10
ciscoasa (config-route-map)# match community 1
ciscoasa (config-route-map)# set origin incomplete
ciscoasa (config-route-map)# exit
ciscoasa (config)# router bgp 50000
ciscoasa (config-router)# address-family ipv4
ciscoasa (config-router-af)# table-map SET_BUCKET
ciscoasa (config-router-af)# end
ciscoasa # clear  bgp table-map
```

2. 以下示例清除 IPv4 单播对等会话的表映射：

```
ciscoasa # clear bgp ipv4 unicast table-map.
```

相关命令

命令	说明
clear bgp	使用硬 / 软重新配置来重置边界网关协议 (eBGP) 对等会话。
clear bgp external	使用硬 / 软重新配置来重置外部边界网关协议 (BGP) 连接。
clear bgp ipv4	使用硬 / 软重新配置来重置 IPv4 地址系列会话的边界网关协议 (BGP) 对等会话。

clear blocks

要重置数据包缓冲区计数器（如低水印和历史记录信息），请在特权 EXEC 模式下使用 **clear blocks** 命令。

clear blocks [**snapshot** | **history**]

语法说明

history	清除所有快照的历史记录。
snapshot	清除所有快照。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.1(5)	增加了 **history** 和 **snapshot** 选项。

使用指南

将低水印计数器重置为每个池中当前可用的块数。此外，此命令会清除上次缓冲区分配失败时存储的历史记录信息。

示例

以下示例清除块数：

```
ciscoasa# clear blocks
```

相关命令

命令	说明
blocks	增加为块诊断分配的内存。
show blocks	显示系统缓冲区利用率。

clear-button

要定制显示给连接到 ASA 的 WebVPN 用户的 WebVPN 页面登录字段的 Clear（清除）按钮，请在定制配置模式下使用 **clear-button** 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。

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

语法说明

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

默认值

默认文本为 “Clear”。

默认样式为 border:1px solid black;background-color:white;font-weight:bold;font-size:80%。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
定制配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的级联样式表 (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。

注意　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 Clear（清除）按钮的默认背景颜色从黑色更改为蓝色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

相关命令

命令	说明
group-prompt	定制 WebVPN 页面登录字段的组提示。
login-button	定制 WebVPN 页面登录字段的登录按钮。
login-title	定制 WebVPN 页面登录字段的标题。
password-prompt	定制 WebVPN 页面登录字段的密码提示。
username-prompt	定制 WebVPN 页面登录字段的用户名提示。

clear capture

要清除捕获缓冲区，请在特权 EXEC 模式下使用 **clear capture** *capture_name* 命令。

clear capture *capture_name*

语法说明

capture_name	数据包捕获的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

不支持 **clear capture** 的缩短形式（例如，**cl cap** 或 **clear cap**），以防止所有数据包捕获被意外破坏。

示例

以下示例展示如何清除捕获缓冲区 “example”：

```
ciscoasa(config)# clear capture example
```

相关命令

命令	说明
capture	启用数据包捕获功能以进行数据包嗅探和网络故障隔离。
show capture	在未指定选项时显示捕捉配置。

clear cluster info

要清除集群统计信息，请在特权 EXEC 模式下使用 **clear cluster info** 命令。

clear cluster info {trace | transport}

语法说明

trace	清除集群事件跟踪信息。
transport	清除集群传输统计信息。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

要查看集群统计信息，请使用 **show cluster info** 命令。

示例

以下示例清除集群事件跟踪信息：

```
ciscoasa# clear cluster info trace
```

相关命令

命令	说明
show cluster info	显示集群统计信息。

clear compression

要清除所有 SVC 和 WebVPN 连接的压缩统计信息，请在特权 EXEC 模式下使用 **clear compression** 命令。

clear compression {**all** | **svc** | **http-comp**}

语法说明

all	清除所有压缩统计信息。
http-comp	清除 HTTP-COMP 统计数据。
svc	清除 SVC 压缩统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

示例

以下示例清除用户的压缩配置：

```
hostname# clear configure compression
```

相关命令

命令	说明
compression	对所有 SVC 和 WebVPN 连接启用压缩。
svc compression	对特定组或用户的 SVC 连接上的数据启用压缩。

第 6 章

clear configure 至 clear isakmp sa 命令

clear configuration session

要删除配置会话，请在全局配置模式下使用 **clear configuration session** 命令。

clear configuration session [*session_name*]

语法说明

session_name	现有配置会话的名称。可对当前会话列表使用 **show configuration session** 命令。如果省略此参数，将删除所有现有会话。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(2)	引入了此命令。

使用指南

可将此命令与 **configure session** 命令配合使用；后者为编辑 ACL 及其对象创建独立会话。如果确定不再需要创建的会话，也不想应用在会话中定义的更改，使用此命令可删除会话及其中的更改。

如果只想清除在会话中所做的更改而不删除会话，请使用 **clear session** 命令。

示例

以下示例删除名为 old-session 的会话：

```
ciscoasa(config)# clear configuration session old-session
```

相关命令

命令	说明
clear session	清除配置会话的内容或重置配置会话的访问标志。
configure session	创建或打开会话。
show configuration session	显示在每个当前会话中所做的更改。

clear configure

要清除运行配置，请在全局配置模式下使用 **clear configure** 命令。

clear configure {**primary** | **secondary** | **all** | *command*}

语法说明

all	清除整个运行配置。
command	清除指定命令的配置。对于可用的命令，请使用 **clear configure ?** 命令查看 CLI 帮助。
primary	对于故障切换对，清除主要设备配置。
secondary	对于故障切换对，清除辅助设备配置。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果在安全情景中输入此命令，将仅清除情景配置。如果在系统执行空间中输入此命令，将清除系统运行配置和所有情景运行配置。在这种情况下，由于会清除系统配置中的所有情景条目（请参阅 **context** 命令），因此，情景将不再运行，且不能更改情景执行空间。

清除配置之前，请确保将 **boot config** 命令（此命令指定启动配置位置）的任何更改保存到启动配置；如果仅在运行配置中更改了启动配置位置，将在重新启动时从默认位置加载配置。

注意　输入 **clear configure all** 命令并不会删除用于密码加密的主口令。关于主口令的详细信息，请参阅 **config key password-encryption** 命令。

示例

以下示例清除整个运行配置：

```
ciscoasa(config)# clear configure all
```

以下示例清除 AAA 配置：

```
ciscoasa(config)# clear configure aaa
```

相关命令

命令	说明
show running-config	显示运行的配置。

clear conn

要清除特定连接或多个连接，请在特权 EXEC 模式下使用 **clear conn** 命令。

clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*] [**user** [*domain_nickname*\\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **zone** [*zone_name*]]

语法说明

address	（可选）清除具有指定的源 IP 地址或目标 IP 地址的连接。
all	（可选）清除所有连接（包括到设备的连接）。如果没有 **all** 关键字，则仅清除通过设备的连接。
dest_ip	（可选）指定目标 IP 地址（IPv4 或 IPv6）。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如： `10.1.1.1-10.1.1.5`
dest_port	（可选）指定目标端口号。要指定范围，请使用破折号 (-) 分隔各个端口号。例如： `1000-2000`
netmask *mask*	（可选）指定要与给定 IP 地址配合使用的子网掩码。
port	（可选）清除与指定源端口或目标端口之间的连接。
protocol {tcp | udp}	（可选）清除与协议 **tcp** 或 **udp** 之间的连接。
src_ip	（可选）指定源 IP 地址（IPv4 或 IPv6）。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如： `10.1.1.1-10.1.1.5`
src_port	（可选）指定源端口号。要指定范围，请使用破折号 (-) 分隔各个端口号。例如： `1000-2000`
user [*domain_nickname*\\]*user_name*	（可选）清除属于指定用户的连接。如果不包含 *domain_nickname* 参数，ASA 将清除默认域中用户的连接。
user-group [*domain_nickname*\\]*user_group_name*	（可选）清除属于指定用户组的连接。如果不包含 *domain_nickname* 参数，ASA 将清除默认域中用户组的连接。
zone [*zone_name*]	清除属于流量区域的连接。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(8)/7.2(4)/8.0(4)	引入了此命令。
8.4(2)	添加了 **user** 和 **user-group** 关键字，用于支持身份防火墙。
9.3(2)	添加了 **zone** 关键字。

使用指南

此命令支持 IPv4 和 IPv6 地址。

如果对配置更改安全策略，所有*新*连接都将使用新的安全策略。现有连接将继续使用在连接建立时配置的策略。要确保所有连接都使用新策略，需要使用 **clear conn** 命令断开当前连接；断开的连接重新连接后即会使用新策略。可以使用 **clear local-host** 命令清除每台主机的连接，或者使用 **clear xlate** 命令清除使用动态 NAT 的连接。

当 ASA 创建用于允许辅助连接的针孔时，将在 **show conn** 命令输出中显示为不完整的连接。要清除此不完整的连接，请使用 **clear conn** 命令。

示例

以下示例展示如何删除所有连接，然后清除 10.10.10.108:4168 与 10.0.8.112:22 之间的管理连接：

```
ciscoasa# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

ciscoasa# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

相关命令

命令	说明
clear local-host	按特定本地主机或所有本地主机清除所有连接。
clear xlate	清除动态 NAT 会话以及使用 NAT 的任何连接。
show conn	显示连接信息。
show local-host	显示本地主机的网络状态。
show xlate	显示 NAT 会话。

clear console-output

要删除当前捕获的控制台输出，请在特权 EXEC 模式下使用 **clear console-output** 命令。

clear console-output

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何删除当前捕获的控制台输出：

```
ciscoasa# clear console-output
```

相关命令

命令	说明
console timeout	设置与 ASA 之间的控制台连接的空闲超时。
show console-output	显示捕获的控制台输出。
show running-config console timeout	显示与 ASA 之间的控制台连接的空闲超时。

clear coredump

要清除核心转储日志，请在全局配置模式下使用 **clear coredump** 命令。

clear coredump

语法说明

此命令没有参数或关键字。

默认值

默认情况下，核心转储未启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

此命令删除核心转储文件系统的内容和核心转储日志。核心转储文件系统将保持完好。当前核心转储配置将保持不变。

示例

以下示例删除核心转储文件系统的内容和核心转储日志：

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

相关命令

命令	说明
coredump enable	启用核心转储功能。
clear configure coredump	从系统中删除核心转储文件系统及其内容。
show coredump filesystem	在核心转储文件系统中显示文件。
show coredump log	显示核心转储日志。

clear counters

要清除口令计数器，请在全局配置模式下使用 **clear counters** 命令。

clear counters [**all** | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [*:**counter_name***]] [**threshold** *N*]

语法说明

all	（可选）清除所有过滤器详细信息。
context *context-name*	（可选）指定情景名称。
:*counter_name*	（可选）按名称指定计数器。
detail	（可选）清除计数器详细信息。
protocol *protocol_name*	（可选）清除指定协议的计数器。
summary	（可选）清除计数器摘要。
threshold *N*	（可选）清除达到或超过指定阈值的计数器。范围为 1 到 4294967295。
top *N*	（可选）清除达到或超过指定阈值的计数器。范围为 1 到 4294967295。

默认值

clear counters summary detail 命令是默认值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何清除协议堆栈计数器：

```
ciscoasa(config)# clear counters
```

相关命令

命令	说明
show counters	显示协议堆栈计数器。

clear crashinfo

要删除闪存中的故障文件的内容，请在特权 EXEC 模式下使用 **clear crashinfo** 命令。

clear crashinfo

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何删除故障文件：

```
ciscoasa# clear crashinfo
```

相关命令

crashinfo force	强制 ASA 出现故障。
crashinfo save disable	禁止故障信息写入到闪存。
crashinfo test	测试 ASA 将故障信息保存到闪存中文件的能力。
show crashinfo	显示存储在闪存中的故障文件的内容。

clear crypto accelerator statistics

要从加密加速器 MIB 中清除全局统计信息和加速器特定统计信息，请在特权 EXEC 模式下使用 **clear crypto accelerator statistics** 命令。

clear crypto accelerator statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示了可输入此命令的模式：

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

命令历史

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

示例

以下示例在全局配置模式下显示加密加速器统计信息：

```
ciscoasa(config)# clear crypto accelerator statistics
ciscoasa(config)#
```

相关命令

命令	说明
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto accelerator statistics	显示加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

clear crypto ca crls

要清空与指定信任点关联的所有 CRL 的 CRL 缓存要从缓存中清空与信任池关联的所有 CRL，或者要清空所有 CRL 的 CRL 缓存，请在特权 EXEC 模式下使用 **clear crypto ca crls** 命令。

clear crypto ca crls [**trustpool** | trustpoint *trustpointname*]

语法说明

trustpointname	信任点的名称。如果不指定名称，此命令将清除系统上所有缓存 CRL。如果提供没有信任点名称的信任点关键字，此命令将失败。
trustpool	表示操作应仅应用于与信任池中证书关联的 CRL。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

以下在特权 EXEC 配置模式下发出的独立示例清除信任池的所有 CRL，清除与 trustpoint123 关联的所有 CRL，并从 ASA 删除所有缓存 CRL：

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

相关命令

命令	说明
crypto ca crl request	根据信任点的 CRL 配置下载 CRL。
show crypto ca crl	显示所有缓存 CRL 或指定信任点的缓存 CRL。

clear crypto ca trustpool

要从信任池中删除所有证书，请在全局配置模式下使用 **clear crypto ca trustpool** 命令。

clear crypto ca trustpool [**noconfirm**]

语法说明

noconfirm	禁止用户确认提示，此命令将根据请求进行处理。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

用户在执行此操作之前，需要先确认操作。

示例

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool.Do you want to continue?(y/n)
ciscoasa#
```

相关命令

命令	说明
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。
crypto ca trustpool remove	从信任池中删除一个指定的证书。

clear crypto ikev1

要删除 IPsec IKEv1 SA 或统计信息，请在特权 EXEC 模式下使用 **clear crypto ikev1** 命令。要清除所有 IKEv1 SA，请使用此命令的不带参数形式。

clear crypto ikev1 {**sa** *IP_address_hostname* | **stats**}

语法说明

sa	清除 SA。
IP_address_hostname	IP 地址或主机名。
stats	清除 IKEv1 统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

要清除所有 IPsec IKEv1 SA，请使用此命令的不带参数的形式。

示例

以下在全局配置模式下发出的示例从 ASA 删除所有 IPsec IKEv1 统计信息：

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

以下示例在全局配置模式下删除具有与 10.86.1.1 对等的 IP 地址的 SA：

```
ciscoasa# clear crypto ikev1 peer 10.86.1.1
ciscoasa#
```

相关命令

命令	说明
clear configure crypto map	从配置中清除所有或指定的加密映射。
clear configure isakmp	清除所有 ISAKMP 策略配置。
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto ikev2

要删除 IPsec IKEv2 SA 或统计信息，请在特权 EXEC 模式下使用 **clear crypto ikev2** 命令。要清除所有 IKEv2 SA，请使用此命令的不带参数形式。

clear crypto ikev2 {**sa** *IP_address_hostname* | **stats**}

语法说明

sa	清除 SA。
IP_address_hostname	IP 地址或主机名。
stats	清除 IKEv2 统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

要清除所有 IPsec IKEv2 SA，请使用此命令的不带参数的形式。

示例

以下在全局配置模式下发出的示例从 ASA 删除所有 IPsec IKEv2 统计信息：

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

以下示例在全局配置模式下删除具有与 10.86.1.1 对等的 IP 地址的 SA：

```
ciscoasa# clear crypto ikev2 peer 10.86.1.1
ciscoasa#
```

相关命令

命令	说明
clear configure crypto map	从配置中清除所有或指定的加密映射。
clear configure isakmp	清除所有 ISAKMP 策略配置。
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto ipsec sa

要删除 IPsec SA 计数器、条目、加密映射或对等连接，请在特权 EXEC 模式下使用 **clear crypto ipsec sa** 命令。要清除所有 IPsec SA，请使用此命令的不带参数形式。

clear [**crypto**] **ipsec sa** [**counters** | **entry** {*hostname* | *ip_address*} {**esp** | **ah**} *spi* | **map** *map name* | **peer** {*hostname* | *ip_address*}]

语法说明

ah	身份验证报头。
counters	清除每个 SA 的所有 IPsec 统计信息。
entry	删除与指定 IP 地址 / 主机名、协议和 SPI 值匹配的隧道。
esp	加密安全协议。
hostname	识别分配给 IP 地址的主机名。
ip_address	识别 IP 地址。
map	删除与指定加密映射（通过映射名称识别）关联的所有隧道。
map name	识别加密映射的字母数字字符串。最多可包含 64 个字符。
peer	删除通过指定主机名或 IP 地址识别的对等设备的所有 IPsec SA。
spi	确定安全参数索引（十六进制数）。必须是入站 SPI。此命令不支持出站 SPI。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

要清除所有 IPsec SA，请使用此命令的不带参数形式。

示例

以下示例在全局配置模式下从 ASA 删除所有 IPsec SA：

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

以下示例在全局配置模式下删除具有与 10.86.1.1 对等的 IP 地址的 SA：

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
ciscoasa#
```

相关命令

命令	说明
clear configure crypto map	从配置中清除所有或指定的加密映射。
clear configure isakmp	清除所有 ISAKMP 策略配置。
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto protocol statistics

要清除加密加速器 MIB 中的协议特定统计信息，请在特权 EXEC 模式下使用 **clear crypto protocol statistics** 命令。

clear crypto protocol statistics *protocol*

语法说明

protocol	指定要清除统计信息的协议的名称。协议选项如下所示： • **all**- 当前支持的所有协议。 • **ikev1**- 互联网密钥交换 (IKE) 版本 1。 • **ikev2**- 互联网密钥交换 (IKE) 版本 2。 • **ipsec-client** - IP 安全 (IPsec) 阶段 2 协议。 • **other** - 保留以用于新协议。 • **srtp** - 安全 RTP (SRTP) 协议 • **ssh** - 安全外壳 (SSH) 协议 • **ssl-client -** 安全套接字层 (SSL) 协议。

默认值

没有默认行为或值。

命令模式

下表展示了可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	添加了 **ikev1** 和 **ikev2** 关键字。
9.0(1)	增加了多情景模式支持。

示例

以下示例在全局配置模式下清除所有加密加速器统计信息：

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

相关命令

命令	说明
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
show crypto accelerator statistics	显示来自加密加速器 MIB 的全局统计信息和加速器特定统计信息。
show crypto protocol statistics	显示加密加速器 MIB 中的协议特定统计信息。

clear cts

要清除 ASA 在与 Cisco TrustSec 集成时使用的数据，请在全局配置模式下使用 **clear cts** 命令。

clear cts {**environment-data** | **pac**}

语法说明

environment-data	清除所有 CTS 环境数据。
pac	清除存储的 CTS PAC。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

将 **environment-data** 关键字与 **clear cts** 命令结合使用可清除从思科 ISE 下载的 Cisco TrustSec 环境数据。可以手动触发下一次环境数据刷新，或者由 ASA 在刷新计时器到期时刷新数据。运行 **clear cts environment-data** 不会从 ASA 删除 Cisco TrustSec PAC。由于运行 **clear cts nvironment-data** 命令会影响流量策略，因此，系统会提示您确认此操作。

将 **pac** 关键字与 **clear cts** 命令结合使用可清除存储在 ASA 上的 NVRAM 中的 PAC 信息。如果没有 PAC，ASA 将无法下载 Cisco TrustSec 环境数据。但是，会继续使用已在 ASA 上的环境数据。由于运行 **clear cts pac** 命令会导致 ASA 无法检索环境数据更新，系统会提示您确认此操作。

限制

- HA：在高可用性 (HA) 配置中，此命令在备用设备上不受支持。如果在备用设备上运行 **clear cts** [**environment-data** | **pac**]，将显示以下错误消息：

  此命令仅在主要设备上允许执行。

- 集群：此命令仅在主设备上受支持。如果在从设备上运行 **clear cts** [**environment-data** | **pac**]，将显示以下错误消息：

  此命令仅在主设备上允许执行。

示例

以下示例展示如何从 ASA 清除用于将 ASA 与 Cisco TrustSec 集成的数据：

```
ciscoasa# clear cts pac
Are you sure you want to delete the cts PAC?(y/n)

ciscoasa# clear cts environment-data
Are you sure you want to delete the cts environment data?(y/n)
```

相关命令

命令	说明
clear configure all	清除 ASA 中的整个运行配置。
clear configure cts	清除用于将 ASA 与 Cisco TrustSec 集成的配置。
cts sxp enable	在 ASA 中启用 SXP 协议。

clear dhcpd

要清除 DHCP 服务器绑定和统计信息，请在特权 EXEC 模式下使用 **clear dhcp** 命令。

clear dhcpd {**binding** [*ip_address*] | **statistics**}

语法说明

binding	清除所有客户端地址绑定。
ip_address	（可选）清除指定 IP 地址的绑定。
statistics	清除统计信息计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果在 **clear dhcpd binding** 命令中包含可选 IP 地址，将仅清除该 IP 地址的绑定。

要清除所有 DHCP 服务器命令，请使用 **clear configure dhcpd** 命令。

示例

以下示例展示如何清除 **dhcpd** 统计信息：

```
ciscoasa# clear dhcpd statistics
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
show dhcpd	显示 DHCP 绑定、统计信息或状态信息。

clear dhcprelay statistics

要清除 DHCP 中继统计信息计数器，请在特权 EXEC 模式下使用 **clear dhcprelay statistics** 命令。

clear dhcprelay statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear dhcprelay statistics 命令仅清除 DHCP 中继统计信息计数器。要清除整个 DHCP 中继配置，请使用 **clear configure dhcprelay** 命令。

示例

以下示例展示如何清除 DHCP 中继统计信息：

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
debug dhcprelay	显示 DHCP 中继代理的调试信息。
show dhcprelay statistics	显示 DHCP 中继代理统计信息。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

clear dns

要清除与指定的完全限定域名 (FQDN) 主机关联的所有 IP 地址，请在特权 EXEC 模式下使用 **clear dns** 命令。

clear dns [**host** *fqdn_name*]

语法说明

fqdn_name	（可选）指定所选主机的完全限定域名。
host	（可选）指示指定主机的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

示例

以下示例清除与指定 FQDN 主机关联的 IP 地址：

```
ciscoasa# clear dns 10.1.1.2 www.example.com
```

注意　此命令忽略 **dns expire-entry** 关键字的设置。新的 DNS 查询将发送到每个已激活的 FQDN 主机。

相关命令

命令	说明
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	配置 DNS 服务器地址。
dns retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
dns timeout	指定在尝试下一 DNS 服务器之前等待的时间量。
show dns-hosts	显示 DNS 缓存。

clear dns-hosts cache

要清除 DNS 缓存，请在特权 EXEC 模式下使用 **clear dns-hosts cache** 命令。

clear dns-hosts cache

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令不会清除用 **name** 命令添加的静态条目。

示例

以下示例清除 DNS 缓存：

```
ciscoasa# clear dns-hosts cache
```

相关命令

命令	说明
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	配置 DNS 服务器地址。
dns retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
dns timeout	指定在尝试下一 DNS 服务器之前等待的时间量。
show dns-hosts	显示 DNS 缓存。

clear dynamic-filter dns-snoop

要清除僵尸网络流量过滤器 DNS 监听数据，请在特权 EXEC 模式下使用 **clear dynamic-filter dns-snoop** 命令。

clear dynamic-filter dns-snoop

语法说明

此命令没有任何参数或关键字。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下示例清除所有僵尸网络流量过滤器 DNS 监听数据：

```
ciscoasa# clear dynamic-filter dns-snoop
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。

命令	说明
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

clear dynamic-filter reports

要清除僵尸网络流量过滤器的报告数据，请在特权 EXEC 模式下使用 **clear dynamic-filter reports** 命令。

clear dynamic-filter reports {**top** [**malware-sites** | **malware-ports** | **infected-hosts**] | **infected-hosts**}

语法说明

malware-ports	（可选）清除前 10 个恶意软件端口的报告数据。
malware-sites	（可选）清除前 10 个恶意软件站点的报告数据。
infected-hosts (**top**)	（可选）清除前 10 个受感染主机的报告数据。
top	清除前 10 个恶意软件站点、端口和受感染主机的报告数据。
infected-hosts	清除受感染主机的报告数据。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。
8.2(2)	**botnet-sites** 和 **botnet-ports** 关键字分别更改为 **malware-sites** 和 **malware-ports**。添加了 **top** 关键字，用于区分前 10 个报告的清除与受感染主机新报告的清除。添加了 **infected-hosts** 关键字（不包含 **top**）。

示例

以下示例清除僵尸网络流量过滤器前 10 个报告的所有数据：

```
ciscoasa# clear dynamic-filter reports top
```

以下示例仅清除前 10 个恶意软件站点的报告数据：

```
ciscoasa# clear dynamic-filter reports top malware-sites
```

以下示例清除所有受感染主机的报告数据：

```
ciscoasa# clear dynamic-filter reports infected-hosts
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports infected-hosts	生成受感染主机的报告。
show dynamic-filter reports top	生成前 10 个恶意软件站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

clear dynamic-filter statistics

要清除僵尸网络流量过滤器统计信息，请在特权 EXEC 模式下使用 **clear dynamic-filter statistics** 命令。

clear dynamic-filter statistics [**interface** *name*]

语法说明

interface *name*	（可选）清除特定接口的统计信息。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下示例清除所有僵尸网络流量过滤器 DNS 统计信息：

```
ciscoasa# clear dynamic-filter statistics
```

相关命令

命令	说明
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。

命令	说明
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports infected-hosts	生成受感染主机的报告。
show dynamic-filter reports top	生成前 10 个恶意软件站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

clear eigrp events

要清除 EIGRP 事件日志，请在特权 EXEC 模式下使用 **clear eigrp events** 命令。

clear eigrp [*as-number*] **events**

语法说明

as-number	（可选）指定要清除事件日志的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此，无需指定自主系统编号（进程 ID）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

可以使用 **show eigrp events** 命令查看 EIGRP 事件日志。

示例

以下示例清除 EIGRP 事件日志：

```
ciscoasa# clear eigrp events
```

相关命令

命令	说明
show eigrp events	显示 EIGRP 事件日志。

clear eigrp neighbors

要从 EIGRP 邻居表清除条目，请在特权 EXEC 模式下使用 **clear eigrp neighbors** 命令。

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

语法说明

as-number	（可选）指定要删除邻居条目的 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此，无需指定自主系统编号 (AS)（即进程 ID）。
if-name	（可选）通过 **nameif** 命令指定的接口的名称。指定接口名称将删除通过该接口获悉的所有邻居表条目。
ip-addr	（可选）要从邻居表删除的邻居的 IP 地址。
soft	导致 ASA 与邻居重新同步但不重置邻接。

默认值

如果不指定邻居 IP 地址或接口名称，将从邻居表删除所有动态条目。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

clear eigrp neighbors 命令不会从邻居表删除用 **neighbor** 命令定义的邻居。此命令仅删除动态发现的邻居。

可以使用 **show eigrp neighbors** 命令查看 EIGRP 邻居表。

示例

以下命令从 EIGRP 邻居表删除所有条目：

```
ciscoasa# clear eigrp neighbors
```

以下示例从 EIGRP 邻居表删除通过名为 “outside” 的接口获悉的所有条目：

```
ciscoasa# clear eigrp neighbors outside
```

相关命令

命令	说明
debug eigrp neighbors	显示 EIGRP 邻居的调试信息。
debug ip eigrp	显示 EIGRP 协议数据包的调试信息。
show eigrp neighbors	显示 EIGRP 邻居表。

clear eigrp topology

要从 EIGRP 拓扑表删除条目，请在特权 EXEC 模式下使用 **clear eigrp topology** 命令。

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

语法说明

as-number	（可选）指定 EIGRP 进程的自主系统编号。由于 ASA 仅支持一个 EIGRP 路由进程，因此，无需指定自主系统编号 (AS)（即进程 ID）。
ip-addr	要从拓扑表清除的 IP 地址。
mask	（可选）要应用于 *ip-addr* 参数的网络掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

此命令从 EIGRP 拓扑表清除现有 EIGRP 条目。可以使用 **show eigrp topology** 命令查看拓扑表条目。

示例

以下示例从 EIGRP 拓扑表删除 192.168.1.0 网络中的条目：

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

相关命令

命令	说明
show eigrp topology	显示 EIGRP 拓扑表。

clear failover statistics

要清除故障切换统计信息计数器，请在特权 EXEC 模式下使用 **clear failover statistics** 命令。

clear failover statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令清除用 **show failover statistics** 命令显示的统计信息以及 **show failover** 命令输出的 “ 状态故障切换逻辑更新统计信息 ” 部分中的计数器。要删除故障切换配置，请使用 **clear configure failover** 命令。

示例

以下示例展示如何清除故障切换统计信息计数器：

```
ciscoasa# clear failover statistics
ciscoasa#
```

相关命令

命令	说明
debug fover	显示故障切换调试信息。
show failover	显示有关故障切换配置和运行统计信息的信息。

clear flow-export counters

要将与 NetFlow 数据关联的运行时间计数器重置为 0，请在特权 EXEC 模式下使用 **clear flow-export counters** 命令。

clear flow-export counters

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.1(1)	引入了此命令。

使用指南

运行时间计数器包含统计信息和错误数据。

示例

以下示例展示如何重置与 NetFlow 数据关联的运行时间计数器：

```
ciscoasa# clear flow-export counters
```

相关命令

命令	说明
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate *minutes*	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 中的所有运行时间计数器。

clear fragment

要清除 IP 分段重组模块的运行数据，请在特权 EXEC 模式下使用 **clear fragment** 命令。

clear fragment {**queue** | **statistics**} [*interface*]

语法说明

interface	（可选）指定 ASA 接口。
queue	清除 IP 分段重组队列。
statistics	清除 IP 分段重组统计信息。

默认值

如果未指定*接口*，此命令将应用于所有接口。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	将命令分成了两个命令（**clear fragment** 和 **clear configure fragment**），以区分配置数据的清除与运行数据的清除。

使用指南

此命令清除当前在队列中等待重组的分段（如果输入了 **queue** 关键字），或者清除所有 IP 分段重组统计信息（如果输入了 **statistics** 关键字）。统计信息即为计数器，可显示成功重组了多少个分段链，有多少分段链重组失败，以及由于缓冲区溢出而造成超过最大分段大小的次数。

示例

以下示例展示如何清除 IP 分段重组模块的运行数据：

```
ciscoasa# clear fragment queue
```

相关命令

命令	说明
clear configure fragment	清除 IP 分段重组配置并重置默认值。
fragment	提供额外的数据包分段管理并改进与 NFS 之间的兼容性。
show fragment	显示 IP 分段重组模块的运行数据。
show running-config fragment	显示 IP 分段重组配置。

clear gc

要删除垃圾收集 (GC) 进程统计信息，请在特权 EXEC 模式下使用 **clear gc** 命令。

clear gc

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何删除 GC 进程统计信息：

```
ciscoasa# clear gc
```

相关命令

命令	说明
show gc	显示 GC 进程统计信息。

clear igmp counters

要清除所有 IGMP 计数器，请在特权 EXEC 模式下使用 **clear igmp counters** 命令。

clear igmp counters [*if_name*]

语法说明

if_name	通过 **nameif** 命令指定的接口名称。如果在此命令中包含接口名称，则仅会清除指定接口的计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除 IGMP 统计信息计数器：

```
ciscoasa# clear igmp counters
```

相关命令

命令	说明
clear igmp group	从 IGMP 组缓存清除发现的组。
clear igmp traffic	清除 IGMP 流量计数器。

clear igmp group

要从 IGMP 组缓存清除发现的组，请在特权 EXEC 模式下使用 **clear igmp** 命令。

clear igmp group [*group* | **interface** *name*]

语法说明

group	IGMP 组地址。指定特定组将从缓存删除指定的组。
interface *name*	通过 **namif** 命令指定的接口名称。如果指定接口名称，将删除与该接口关联的所有组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果不指定组或接口，将从所有接口清除所有组。如果指定组，将仅清除指定组的条目。如果指定接口，将清除指定接口上的所有组。如果指定组和接口，将仅清除指定组和指定接口。

此命令不会清除静态配置的组。

示例

以下示例展示如何从 IGMP 组缓存清除所有发现的 IGMP 组：

```
ciscoasa# clear igmp group
```

相关命令

命令	说明
clear igmp counters	清除所有 IGMP 计数器。
clear igmp traffic	清除 IGMP 流量计数器。

clear igmp traffic

要清除 IGMP 流量计数器，请在特权 EXEC 模式下使用 **clear igmp traffic** 命令。

clear igmp traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除 IGMP 统计流量计数器：

```
ciscoasa# clear igmp traffic
```

相关命令

命令	说明
clear igmp group	从 IGMP 组缓存清除发现的组。
clear igmp counters	清除所有 IGMP 计数器。

clear interface

要清除接口统计信息，请在特权 EXEC 模式下使用 **clear interface** 命令。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

语法说明

interface_name	（可选）识别通过 **nameif** 命令设置的接口名称。
mapped_name	（可选）在多情景模式下，识别映射名称（如果使用 **allocate-interface** 命令分配了该名称）。
physical_interface	（可选）识别接口 ID（例如 **gigabitethernet0/1**）。请参阅**接口**命令可接受的值。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

默认值

默认情况下，此命令清除所有接口统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果在情景之间共享接口，当在某个情景中输入此命令时，ASA 只会清除当前情景的统计信息。如果在系统执行空间输入此命令，ASA 将清除统计信息组合。

不能在系统执行空间中使用接口名称，因为 **nameif** 命令只能用于情景中。同样，如果使用 **allocate-interface** 命令将接口 ID 映射到某个映射名称，则只能在情景中使用该映射名称。

示例

以下示例清除所有接口统计信息：

```
ciscoasa# clear interface
```

相关命令

命令	说明
clear configure interface	清除接口配置。
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。
show running-config interface	显示接口配置。

clear ip audit count

要清除审核策略的签名匹配项数，请在特权 EXEC 模式下使用 **clear ip audit count** 命令。

clear ip audit count [**global** | **interface** *interface_name*]

语法说明

global	（默认）清除所有接口的匹配项数。
interface *interface_name*	（可选）清除指定接口的匹配项数。

默认值

如果未指定关键字，此命令将清除所有接口的匹配项 (**global**)。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除所有接口的匹配项数：

```
ciscoasa# clear ip audit count
```

相关命令

命令	说明
ip audit interface	将审核策略分配至接口。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
show ip audit count	显示审核策略的签名匹配项数。
show running-config ip audit attack	显示 **ip audit attack** 命令的配置。

clear ip verify statistics

要清除单播 RPF 统计信息，请在特权 EXEC 模式下使用 **clear ip verify statistics** 命令。

clear ip verify statistics [**interface** *interface_name*]

语法说明

interface *interface_name*	设置要清除单播 RPF 统计信息的接口。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要启用单播 RPF，请参阅 **ip verify reverse-path** 命令。

示例

以下示例清除单播 RPF 统计信息：

```
ciscoasa# clear ip verify statistics
```

相关命令

命令	说明
clear configure ip verify reverse-path	清除 **ip verify reverse-path** 配置。
ip verify reverse-path	启用单播 RPF 功能以防止 IP 欺骗。
show ip verify statistics	显示单播 RPF 统计信息。
show running-config ip verify reverse-path	显示 **ip verify reverse-path** 配置。

clear ipsec sa

要完全或根据指定参数清除 IPsec SA，请在特权 EXEC 模式下使用 **clear ipsec sa** 命令。

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

语法说明

counters	（可选）清除所有计数器。
entry	（可选）清除指定 IPsec 对等设备、协议和 SPI 的 IPsec SA。
inactive	（可选）清除无法传递流量的 IPsec SA。
map *map-name*	（可选）清除指定加密映射的 IPsec SA。
peer	（可选）清除指定对等设备的 IPsec SA。
peer-addr	指定 IPsec 对等设备的 IP 地址。
protocol	指定 IPsec 协议：**esp** 或 **ah**。
spi	指定 IPsec SPI。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

还可以使用此命令的替代形式执行相同功能：**clear crypto ipsec sa**。

示例

以下示例在全局配置模式下清除所有 IPsec SA 计数器：

```
ciscoasa# clear ipsec sa counters
ciscoasa#
```

相关命令

命令	说明
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec stats	显示来自 IPsec 流 MIB 的全局 IPsec 统计信息。

clear ipv6 access-list counters

要清除 IPv6 访问列表统计信息计数器，请在特权 EXEC 模式下使用 **clear ipv6 access-list counters** 命令。

clear ipv6 access-list *id* **counters**

语法说明

id	IPv6 访问列表标识符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何清除 IPv6 访问列表 2 的统计信息：

```
ciscoasa# clear ipv6 access-list 2 counters
ciscoasa#
```

相关命令

命令	说明
clear configure ipv6	从当前配置中清除 **ipv6 access-list** 命令。
ipv6 access-list	配置 IPv6 访问列表。
show ipv6 access-list	在当前配置中显示 **ipv6 access-list** 命令。

clear ipv6 dhcprelay binding

要清除 IPv6 DHCP 中继绑定条目，请在特权 EXEC 模式下使用 **clear ipv6 dhcprelay binding** 命令。

clear ipv6 dhcprelay binding [**ip**]

语法说明

ip	（可选）指定 DHCP 中继绑定的 IPv6 地址。如果指定 IP 地址，将仅清除与指定 IP 地址关联的中继绑定条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

以下示例展示如何清除 IPv6 DHCP 中继绑定的统计信息：

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

相关命令

命令	说明
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。
show ipv6 dhcprelay statistics	显示 IPv6 DHCP 中继代理信息。

clear ipv6 dhcprelay statistics

要清除 IPv6 DHCP 中继代理统计信息，请在特权 EXEC 模式下使用 **clear ipv6 dhcprelay statistics** 命令。

clear ipv6 dhcprelay statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

以下示例展示如何清除 IPv6 DHCP 中继代理的统计信息：

```
ciscoasa# clear ipv6 dhcprelay statistics
ciscoasa#
```

相关命令

命令	说明
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。
show ipv6 dhcprelay statistics	显示 IPv6 的 DHCP 中继代理信息。

clear ipv6 mld traffic

要清除 IPv6 组播侦听程序发现 (MLD) 流量计数器，请在特权 EXEC 模式下使用 **clear ipv6 mld traffic** 命令。

clear ipv6 mld traffic

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(4)	引入了此命令。

使用指南

使用 **clear ipv6 mld traffic** 命令可以重置所有 MLD 流量计数器。

示例

以下示例展示如何清除 IPv6 MLD 的流量计数器：

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

相关命令

命令	说明
debug ipv6 mld	显示 MLD 的所有调试消息。
show debug ipv6 mld	在当前配置中显示 IPv6 的 MLD 命令。

clear ipv6 neighbors

要清除 IPv6 邻居发现缓存，请在特权 EXEC 模式下使用 **clear ipv6 neighbors** 命令。

clear ipv6 neighbors

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令从缓存中删除所有发现的 IPv6 邻居，但不会删除静态条目。

示例

以下示例删除 IPv6 邻居发现缓存中除静态条目以外的所有条目：

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

相关命令

命令	说明
ipv6 neighbor	在 IPv6 邻居发现缓存中配置静态条目。
show ipv6 neighbor	显示 IPv6 邻居缓存信息。

clear ipv6 ospf

要清除 OSPFv3 路由参数，请在特权 EXEC 模式下使用 **clear ipv6 ospf** 命令。

clear ipv6 [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

语法说明

counters	重置 OSPF 进程计数器。
events	清除 OSPF 事件日志。
force-ospf	清除 OSPF 进程的 SPF。
process	重置 OSPFv3 进程。
process_id	清除进程 ID 号。有效值范围为 1 到 65535。
redistribution	清除 OSPFv3 路由重分布。
traffic	清除与流量相关的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令删除所有 OSPFv3 路由参数。

示例

以下示例展示如何清除所有 OSPFv3 路由重分布：

```
ciscoasa# clear ipv6 ospf redistribution
ciscoasa#
```

相关命令

命令	说明
show running-config ipv6 router	显示 OSPFv3 进程的运行配置。
clear configure ipv6 router	清除 OSPFv3 路由进程。

clear ipv6 traffic

要重置 IPv6 流量计数器，请在特权 EXEC 模式下使用 **clear ipv6 traffic** 命令。

clear ipv6 traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用此命令将重置 **show ipv6 traffic** 命令输出中的计数器。

示例

以下示例重置 IPv6 流量计数器。**ipv6 traffic** 命令输出表明计数器已重置：

```
ciscoasa# clear ipv6 traffic
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
```

```
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

相关命令

命令	说明
show ipv6 traffic	显示 IPv6 流量统计信息。

clear isakmp sa

要删除所有 IKE 运行时间 SA 数据库，请在全局配置模式或特权 EXEC 模式下使用 **clear isakmp sa** 命令。

clear isakmp sa

语法说明

此命令没有关键字或参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	—	• 是	• 是	—
全局配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	**clear isakmp sa** 命令更改为 **clear crypto isakmp sa**。
9.0(1)	增加了多情景模式支持。

示例

以下示例从配置中删除 IKE 运行时间 SA 数据库：

```
ciscoasa# clear isakmp sa
ciscoasa#
```

相关命令

命令	说明
clear isakmp	清除 IKE 运行时 SA 数据库。
isakmp enable	在 IPsec 对等设备与 ASA 进行通信的接口上启用 ISAKMP 协商。
show isakmp stats	显示运行时间统计信息。
show isakmp sa	显示 IKE 运行时间 SA 数据库及其他信息。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

第 7 章

clear local-host 至 clear xlate 命令

clear local-host

要重新初始化每个客户端的运行时状态（例如，连接限制和半开限制），请在特权 EXEC 模式下使用 **clear local-host** 命令。

clear local-host [*ip_address*] [**all**]

语法说明

all	（可选）清除所有连接，包括流向设备的流量。如果没有 **all** 关键字，则只会清除通过设备的流量。
ip_address	（可选）指定本地主机 IP 地址。

默认值

清除所有通过设备的流量的运行时状态。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果对配置更改安全策略，所有*新*连接都将使用新的安全策略。现有连接将继续使用在连接建立时配置的策略。要确保所有连接都使用新策略，需要使用 **clear local-host** 命令断开当前连接；断开的连接重新连接后即会使用新策略。或者，可以使用 **clear conn** 命令进行更精细的连接清除，也可以使用 **clear xlate** 命令来清除使用 NAT 的连接。

clear local-host 命令根据主机许可证上限释放主机。输入 **show local-host** 命令可以查看计入许可证上限的主机数量。

示例

以下示例清除主机 10.1.1.15 的运行时状态及关联连接：

```
ciscoasa# clear local-host 10.1.1.15
```

相关命令

命令	说明
clear conn	终止处于任何状态的连接。
clear xlate	清除动态 NAT 会话以及使用 NAT 的任何连接。
show local-host	显示本地主机的网络状态。

clear logging asdm

要清除 ASDM 日志记录缓冲区，请在特权 EXEC 模式下使用 **clear logging asdm** 命令。

clear logging asdm

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **clear pdm logging** 命令更改为 **clear asdm log** 命令。

使用指南

ASDM 系统日志消息和 ASA 系统日志消息存储在不同的缓冲区中。清除 ASDM 日志记录缓冲区只会清除 ASDM 系统日志消息，而不会清除 ASA 系统日志消息。要查看 ASDM 系统日志消息，请使用 **show asdm log** 命令。

示例

以下示例清除 ASDM 日志记录缓冲区：

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

相关命令

命令	说明
show asdm log_sessions	显示 ASDM 日志记录缓冲区的内容。

clear logging buffer

要清除日志缓冲区，请在特权 EXEC 模式下使用 **clear logging buffer** 命令。

clear logging buffer

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何清除日志缓冲区的内容：

```
ciscoasa# clear logging buffer
```

相关命令

命令	说明
logging buffered	配置日志缓冲区。
show logging	显示日志记录信息。

clear logging queue bufferwrap

要清除保存的日志缓冲区（ASDM、内部缓冲区、FTP 和闪存），请在特权 EXEC 模式下使用 **clear logging queue bufferwrap** 命令。

clear logging queue bufferwrap

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下示例展示如何清除保存的日志缓冲区的内容：

```
ciscoasa# clear logging queue bufferwrap
```

相关命令

命令	说明
logging buffered	配置日志缓冲区。
show logging	显示日志记录信息。

clear mac-address-table

要清除动态 MAC 地址表条目，请在特权 EXEC 模式下使用 **clear mac-address-table** 命令。

clear mac-address-table [*interface_name*]

语法说明

interface_name	（可选）清除选定接口的 MAC 地址表条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除动态 MAC 地址表条目：

```
ciscoasa# clear mac-address-table
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
firewall transparent	将防火墙模式设置为透明。
mac-address-table aging-time	为动态 MAC 地址条目设置超时。
mac-learn	禁用 MAC 地址学习。
show mac-address-table	显示 MAC 地址表条目。

clear mdm-proxy statistics

要清除 MDM 代理服务计数器，请将这些计数器设置为 0。

clear mdm-proxy statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

示例

```
ciscoasa (config)# clear mdm-proxy statistics<cr>
```

相关命令

命令	说明
show mdm-proxy statistics	显示 MDM 代理服务统计信息。
mdm-proxy	进入 config-mdm-proxy 模式以配置 MDM 代理服务。

clear memory delayed-free-poisoner

要清除 delayed free-memory poisoner 工具队列和统计信息，请在特权 EXEC 模式下使用 **clear memory delayed-free-poisoner** 命令。

clear memory delayed-free-poisoner

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear memory delayed-free-poisoner 命令在不进行验证的情况下将保留在 delayed free-memory poisoner 工具队列中的所有内存返回到系统，并清除所有相关的统计信息计数器。

示例

以下示例清除 delayed free-memory poisoner 工具队列和统计信息：

```
ciscoasa# clear memory delayed-free-poisoner
```

相关命令

命令	说明
memory delayed-free-poisoner enable	启用 delayed free-memory poisoner 工具。
memory delayed-free-poisoner validate	强制验证 delayed free-memory poisoner 工具队列。
show memory delayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。

clear memory profile

要清除内存分析功能保留的内存缓冲区，请在特权 EXEC 模式下使用 **clear memory profile** 命令。

clear memory profile [**peak**]

语法说明

peak	（可选）清除峰值内存缓冲区的内容。

默认值

默认清除当前 “ 使用中 ” 的配置文件缓冲区。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear memory profile 命令释放分析功能保留的内存缓冲区，因此，需要停止分析后才能清除内存缓冲区。

示例

以下示例清除分析功能保留的内存缓冲区：

```
ciscoasa# clear memory profile
```

相关命令

命令	说明
memory profile enable	启用对内存使用（内存分析）的监控。
memory profile text	配置要分析的内存的文本范围。
show memory profile	显示 ASA 内存使用情况（分析）的信息。

clear mfib counters

要清除 MFIB 路由器数据包计数器，请在特权 EXEC 模式下使用 **clear mfib counters** 命令。

clear mfib counters [*group* [*source*]]

语法说明

group	（可选）组播组的 IP 地址。
source	（可选）组播路由源的 IP 地址。这是采用四点分十进制记数法的单播 IP 地址。

默认值

当此命令不带参数时，将清除所有路由的路由计数器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除所有 MFIB 路由器数据包计数器：

```
ciscoasa# clear mfib counters
```

相关命令

命令	说明
show mfib count	显示 MFIB 路由和数据包计数数据。

clear module

要清除有关 ASA 上 SSM 的信息、有关 ASA 5505 上 SSC 的信息、有关安装在 ASA 5585-X 上的 SSP 的信息、有关安装在 ASA 5585-X 上的 IPS SSP 的信息、有关 ASA 服务模块的信息以及系统信息，请在特权 EXEC 模式下使用 **clear module** 命令。

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

语法说明

all	（默认）清除所有 SSM 信息。
console	（可选）清除模块的控制台日志信息。
details	（可选）清除其他信息，包括 SSM 的远程管理配置（例如 ASA-SSM-*x*0）。
log	（可选）清除模块的日志信息。
mod_id	清除用于软件模块的模块名称（例如 IPS）。
recover	（可选）对于 SSM，清除 **hw-module module recover** 命令的设置。 **注**　仅在将 **configure** 关键字与 **hw-module module recover** 命令结合使用为 SSM 创建了恢复配置的情况下，**recover** 关键字才有效。 （可选）对于安装在 ASA 5512-X、5515-X、5525-X、5545-X 或 5555-X 上的 IPS 模块，清除 **sw-module module** *mod_id* **recover configure image** *image_location* 命令的设置。
slot	清除模块插槽编号（可以是 0 或 1）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	支持 SSC。
8.2(5)	支持 ASA 5585-X 和 ASA 5585-X 上的 IPS SSP。
8.4(2)	支持安装两个 SSP。
8.5(1)	支持 ASASM。
8.6(1)	支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X。

使用指南

此命令清除有关 SSC、SSM、ASASM、IPS SSP、设备接口和内置接口的信息。

示例

以下示例清除 SSM 的恢复设置：

```
ciscoasa# clear module 1 recover
```

相关命令

命令	说明
hw-module module recover	通过从 TFTP 服务器加载恢复映像来恢复 SSM。
hw-module module reset	关闭 SSM 并执行硬件重置。
hw-module module reload	重新加载 SSM 软件。
hw-module module shutdown	关闭 SSM 软件，以便在关闭电源时不会丢失配置数据。
show module	显示 SSM 信息。

clear nac-policy

要重置 NAC 策略使用统计信息，请在全局配置模式下使用 **clear nac-policy** 命令。

clear nac-policy [*nac-policy-name*]

语法说明

nac-policy-name	（可选）要重置使用统计信息的 NAC 策略的名称。

默认值

如果不指定名称，CLI 将重置所有 NAC 策略的使用统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例重置名为 framework1 的 NAC 策略的使用统计信息：

```
ciscoasa(config)# clear nac-policy framework1
```

以下示例重置所有 NAC 策略使用统计信息：

```
ciscoasa(config)# clear nac-policy
```

相关命令

命令	说明
show nac-policy	显示 ASA 中的 NAC 策略使用统计信息。
show vpn-session_summary.db	显示 IPsec、WebVPN 和 NAC 会话数。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。

clear nat counters

要清除 NAT 策略计数器，请在全局配置模式下使用 **clear nat counters** 命令。

clear nat counters [*src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

语法说明

dst_ifc	（可选）指定要过滤的目标接口。
dst_ip	（可选）指定要过滤的目标 IP 地址。
dst_mask	（可选）指定目标 IP 地址的掩码。
src_ifc	（可选）指定要过滤的源接口。
src_ip	（可选）指定要过滤的源 IP 地址。
src_mask	（可选）指定源 IP 地址的掩码。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0 (4)	引入了此命令。

示例

以下示例展示如何清除 NAT 策略计数器：

```
ciscoasa(config)# clear nat counters
```

相关命令

命令	说明
nat	识别一个接口上转换为另一个接口上的映射地址的地址。
nat-control	启用或禁用 NAT 配置要求。
show nat counters	显示协议堆栈计数器。

clear object-group

要清除网络对象组中对象的命中数，请在特权 EXEC 模式下使用 **show object-group** 命令。

clear object-group *obj-name* **counters**

语法说明

counters	识别网络对象组中的计数器。
obj-name	识别现有网络对象组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

使用此命令只能清除网络对象组中对象的命中数。

示例

以下示例展示如何清除名为 “Anet” 的网络对象组的网络对象命中数：

```
ciscoasa# clear object-group Anet counters
```

相关命令

命令	说明
show object-group	显示对象组信息，并显示指定对象组为网络对象组类型时的命中数。

clear ospf

要清除 OSPF 进程信息，请在特权 EXEC 模式下使用 **clear ospf** 命令。

clear ospf [*pid*] {**process** | **counters**}

语法说明

counters	清除 OSPF 计数器。
pid	（可选）OSPF 路由进程内部使用的识别参数；有效值为 1 到 65535。
process	重新启动 OSPF 路由进程。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

此命令不会删除配置的任何部分。使用配置命令的 **no** 形式可以从配置中清除特定命令，使用 **clear configure router ospf** 命令可以从配置中删除所有全局 OSPF 命令。

注意　**clear configure router ospf** 命令不会清除在接口配置模式下输入的 OSPF 命令。

示例

以下示例展示如何清除 OSPF 邻居计数器：

```
ciscoasa# clear ospf counters
```

相关命令

命令	说明
clear configure router	从运行配置中清除所有全局路由器命令。

clear pclu

要清除 PC 逻辑更新统计信息，请在特权 EXEC 模式下使用 **clear pclu** 命令。

clear pclu

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例清除 PC 信息：

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

要清除电话代理数据库中的安全电话条目，请在特权 EXEC 模式下使用 **clear phone-proxy secure-phones** 命令。

clear phone-proxy secure-phones [*mac_address* | **noconfirm**]

语法说明

mac_address	从电话代理数据库中删除带有指定 MAC 地址的 IP 电话。
noconfirm	在不提示确认的情况下删除电话代理数据库中的所有安全电话条目。如果不指定 **noconfirm** 关键字，系统会提示您确认是否删除所有安全电话条目。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

由于安全电话在启动时始终请求 CTL 文件，因此，电话代理会创建一个将电话标记为安全电话的数据库。配置的指定超时结束后（通过 **timeout secure-phones** 命令配置），将删除安全电话数据库中的条目。或者，可以使用 **clear phone-proxy secure-phones** 命令清除电话代理数据库而无需等待配置的超时结束。

示例

以下示例清除电话代理数据库中的安全条目：

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

相关命令

命令	说明
timeout secure-phones	配置从电话代理数据库中删除安全电话条目前的空闲超时。

clear pim counters

要清除 PIM 流量计数器，请在特权 EXEC 模式下使用 **clear pim counters** 命令。

clear pim counters

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅清除流量计数器。要清除 PIM 拓扑表，请使用 **clear pim topology** 命令。

示例

以下示例清除 PIM 流量计数器：

```
ciscoasa# clear pim counters
```

相关命令

命令	说明
clear pim reset	通过重置强制 MRIB 同步。
clear pim topology	清除 PIM 拓扑表。
show pim traffic	显示 PIM 流量计数器。

clear pim reset

要通过重置强制 MRIB 同步，请在特权 EXEC 模式下使用 **clear pim reset** 命令。

clear pim reset

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令会从拓扑表中清除所有信息并重置 MRIB 连接。此命令可用于在 PIM 拓扑表和 MRIB 数据库之间进行状态同步。

示例

以下示例清除拓扑表并重置 MRIB 连接：

```
ciscoasa# clear pim reset
```

相关命令

命令	说明
clear pim counters	清除 PIM 计数器和统计信息。
clear pim topology	清除 PIM 拓扑表。
clear pim counters	清除 PIM 流量计数器。

clear pim topology

要清除 PIM 拓扑表，请在特权 EXEC 模式下使用 **clear pim topology** 命令。

clear pim topology [*group*]

语法说明

group	（可选）指定要从拓扑表中删除的组播组地址或名称。

默认值

如果不指定可选的 *group* 参数，将从拓扑表中清除所有条目。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令从 PIM 拓扑表中清除现有 PIM 路由。会保留从 MRIB 表获得的信息（例如，IGMP 本地成员身份）。如果指定组播组，则仅清除指定组的条目。

示例

以下示例清除 PIM 拓扑表：

```
ciscoasa# clear pim topology
```

相关命令

命令	说明
clear pim counters	清除 PIM 计数器和统计信息。
clear pim reset	通过重置强制 MRIB 同步。
clear pim counters	清除 PIM 流量计数器。

clear priority-queue statistics

要清除某个接口或所有配置的接口的优先级队列统计信息计数器，请在全局配置模式或特权 EXEC 模式下使用 **clear priority-queue statistics** 命令。

clear priority-queue statistics [*interface-name*]

语法说明

interface-name	（可选）指定要显示尽力而为队列和低延迟队列详细信息的接口的名称。

默认值

如果省略接口名称，此命令将清除所有配置的接口的优先级队列统计信息。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是	—
全局配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示在特权 EXEC 模式下使用 **clear priority-queue statistics** 命令来删除名为 “test” 的接口的优先级队列统计信息：

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

相关命令

命令	说明
clear configure priority queue	从指定接口删除优先级队列配置。
priority-queue	在接口上配置优先级队列。
show priority-queue statistics	显示指定接口或所有接口的优先级队列统计信息。
show running-config priority-queue	显示指定接口的当前优先级队列配置。

clear process

要清除正在 ASA 上运行的指定进程的统计信息，请在特权 EXEC 模式下使用 **clear process** 命令。

clear process [**cpu-hog** | **internals**]

语法说明

cpu-hog	清除 CPU 占用统计信息。
internals	清除进程内部统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何清除 CPU 占用统计信息：

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

相关命令

命令	说明
cpu hog granular-detection	触发实时 CPU 占用检测信息。
show processes	显示正在 ASA 上运行的进程的列表。

clear resource usage

要清除资源使用统计信息，请在特权 EXEC 模式下使用 **clear resource usage** 命令。

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

语法说明

context *context_name*	（仅限多模式）指定要清除统计信息的情景名称。为所有情景指定 **all**（默认值）。
resource [**rate**] *resource_name*	清除特定资源的使用统计信息。为所有资源指定 **all**（默认值）。指定 **rate** 将清除资源的使用率。按使用率测量的资源包括 **conns**、**inspects** 和 **syslogs**。对于这些资源类型，必须指定 **rate** 关键字。conns 资源也可以按并发连接数来测量；要查看每秒连接数，必须使用 **rate** 关键字。 资源包括以下类型： • **asdm** - ASDM 管理会话。 • **conns** - 任意两台主机（包括一台主机和多台其他主机之间的连接）之间的 TCP 或 UDP 连接。 • **inspects** - 应用检查。 • **hosts** - 可通过 ASA 连接的主机。 • **mac-addresses** - 对于透明防火墙模式，MAC 地址表中允许的 MAC 地址数量。 • **ssh** - SSH 会话。 • **syslogs** - 系统日志消息。 • **telnet** - Telnet 会话。 • （仅限多模式）**VPN Other** - 站点间 VPN 会话。 • （仅限多模式）**VPN Burst Other** - 站点间 VPN 突发会话。 • **xlates** - NAT 转换。
summary	（仅限多模式）清除合并的情景统计信息。
system	（仅限多模式）清除系统范围（全局）的使用统计信息。

默认值

对于多情景模式，默认情景为 **all**（清除每个情景的使用统计信息）。对于单模式，将忽略情景名称，并清除所有资源统计信息。

默认资源名称为 **all**（清除所有资源类型）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例清除全部情景的所有资源使用统计信息，但不清除系统范围的使用统计信息：

```
ciscoasa# clear resource usage
```

以下示例清除系统范围的使用统计信息：

```
ciscoasa# clear resource usage system
```

相关命令

命令	说明
context	添加安全情景。
show resource types	显示资源类型列表。
show resource usage	显示 ASA 的资源使用情况。

clear route all

要从配置中删除动态获知的路由，请在特权 EXEC 模式下使用 **clear route all** 命令。

clear route all

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下示例展示如何删除动态获知的路由：

```
ciscoasa# clear route all
```

相关命令

命令	说明
clear route *network <mask>*	删除指定的目标路由。
show route	显示路由信息。
show running-config route	随即会显示配置的路由。

clear route *network<mask>*

要删除指定的目标路由，请在特权 EXEC 模式下使用 **clear route** ***network <mask>*** 命令。

clear route [*ip_address ip_mask*]

语法说明

ip_address ip_mask	指定要删除的目标 IP 地址和子网掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

以下示例展示如何删除动态获知的路由：

```
ciscoasa# clear route 10.118.86.3
```

相关命令

命令	说明
clear route all	删除并更新所有路由。
show route	显示路由信息。
show running-config route	随即会显示配置的路由。

clear service-policy

要清除已启用策略的运行数据或统计信息（如果有），请在特权 EXEC 模式下使用 **clear service-policy** 命令。

clear service-policy [**global** | **interface** *intf*] [**user-statistics**]

语法说明

global	（可选）清除全局服务策略的统计信息。
interface *intf*	（可选）清除特定接口的服务策略统计信息。
user-statistics	（可选）清除用户统计信息的全局计数器，但不清除每个用户的统计信息。使用 **show user-identity statistics** 命令仍可以查看每个用户或每个用户组的统计信息。 如果为 **user-statistics** 命令指定 **accounting** 关键字，将清除发送的数据包、接收的数据包以及发送并丢弃的数据包的所有全局计数器。如果为 **user-statistics** 命令指定 **scanning** 关键字，将清除发送并丢弃的数据包的全局计数器。 对于要收集这些用户统计信息的 ASA，必须配置要用于收集用户统计信息的策略映射。请参阅本指南中的 **user-statistics** 命令。

默认值

默认情况下，此命令清除所有已启用的服务策略的所有统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

【要清除检测引擎的服务策略统计信息，请参阅 **clear service-policy inspect** 命令。

示例

以下示例展示 **clear service-policy** 命令的语法：

```
ciscoasa# clear service-policy outside_security_map interface outside
```

相关命令

命令	说明
clear service-policy inspect gtp	清除 GTP 检测引擎的服务策略统计信息。
clear service-policy inspect radius-accounting	清除 RADIUS 计费检测引擎的服务策略统计信息。
show service-policy	显示服务策略。
show running-config service-policy	显示在运行配置中配置的服务策略。
clear configure service-policy	清除服务策略配置。
service-policy	配置服务策略。

clear service-policy inspect gtp

要清除全局 GTP 统计信息，请在特权 EXEC 模式下使用 **clear service-policy inspect gtp** 命令。

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

语法说明

all	清除所有 GTP PDP 情景。
apn	（可选）根据指定的 APN 清除 PDP 情景。
ap_name	识别特定接入点名称。
gsn	（可选）识别 GPRS 支持节点（该节点是 GPRS 无线数据网络和其他网络之间的接口）。
gtp	（可选）清除 GTP 的服务策略。
imsi	（可选）根据指定的 IMSI 清除 PDP 情景。
IMSI_value	用于识别特定 IMSI 的十六进制值。
interface	（可选）识别特定接口。
int	识别要清除信息的接口。
IP_address	要清除统计信息的 IP 地址。
ms-addr	（可选）根据指定的 MS 地址清除 PDP 情景。
pdp-context	（可选）识别数据包数据协议情景。
requests	（可选）清除 GTP 请求。
statistics	（可选）清除 **inspect gtp** 命令的 GTP 统计信息。
tid	（可选）根据指定的 TID 清除 PDP 情景。
tunnel_ID	用于识别特定隧道的十六进制值。
version	（可选）根据 GTP 版本清除 PDP 情景。
version_num	指定 PDP 情景的版本。有效范围为 0 至 255。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

数据包数据协议情景通过隧道 ID 识别（隧道 ID 是 IMSI 与 NSAPI 的组合）。GTP 隧道由不同 GSN 节点中的两个关联的 PDP 情景定义，并通过隧道 ID 识别。在外部数据包数据网络和移动站 (MS) 用户之间转发数据包需要 GTP 隧道。

示例

以下示例清除 GTP 统计信息：

```
ciscoasa# clear service-policy inspect gtp statistics
```

相关命令

命令	说明
debug gtp	显示有关 GTP 检查的详细信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的 GTP 映射。
show service-policy inspect gtp	显示 GTP 配置。
show running-config gtp-map	显示配置的 GTP 映射。

clear service-policy inspect radius-accounting

要清除 RADIUS 计费用户，请在特权 EXEC 模式下使用 **clear service-policy inspect radius-accounting** 命令。

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

语法说明

all	清除所有用户。
ip_address	清除使用此 IP 地址的用户。
policy_map	清除与指定策略映射关联的用户。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例清除所有 RADIUS 计费用户：

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear shared license

要将共享许可证统计信息、共享许可证客户端统计信息和共享许可证备份服务器统计信息重置为 0，请在特权 EXEC 模式下使用 **clear shared license** 命令。

clear shared license [**all** | **backup** | **client** [*hostname*]]

语法说明

all	（可选）清除所有统计信息。这是默认设置。
backup	（可选）清除备份服务器的统计信息。
client	（可选）清除所有参与者的统计信息。
hostname	（可选）清除特定参与者的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

共享许可证计数器包括统计信息和错误数据。

示例

以下示例展示如何重置所有共享许可证计数器：

```
ciscoasa# clear shared license all
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
license-server address	标识参与者的共享许可服务器的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。

命令	说明
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

clear shun

要禁用当前已启用的所有规避功能并清除规避统计信息，请在特权 EXEC 模式下使用 **clear shun** 命令。

clear shun [*statistics*]

语法说明

statistics	（可选）仅清除接口计数器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何禁用当前已启用的所有规避功能并清除规避统计信息：

```
ciscoasa(config)# clear shun
```

相关命令

命令	说明
shun	阻止新连接并禁止通过任何现有连接传输数据包，从而允许对攻击主机作出动态响应。
show shun	显示规避信息。

clear snmp-server statistics

要清除 SNMP 服务器统计信息（SNMP 数据包输入和输入计数器），请在特权 EXEC 模式下使用 **clear snmp-server statistics** 命令。

clear snmp-server statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何清除 SNMP 服务器统计信息：

```
ciscoasa# clear snmp-server statistics
```

相关命令

命令	说明
clear configure snmp-server	清除 SNMP 服务器配置。
show snmp-server statistics	显示 SNMP 服务器配置信息。

clear ssl

要清除 SSL 信息以便进行调试，请在特权 EXEC 模式下使用 **clear ssl** 命令。

clear ssl {cache [**all**] | errors | mib | objects}

语法说明

all	清除 SSL 会话缓存中的所有会话和统计信息。
cache	清除 SSL 会话缓存中已过期的会话。
errors	清除 SSL 错误。
mib	清除 SSL MIB 统计信息。
objects	清除 SSL 对象统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

不会清除 DTLS 缓存，因为这样做会影响 AnyConnect 功能。

示例

以下示例清除 SSL 缓存并清除 SSL 会话缓存中的所有会话和统计信息：

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared

ciscoasa# clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

要从内存中清除配置错误消息，请在特权 EXEC 模式下使用 **clear startup-config errors** 命令。

clear startup-config errors

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要查看 ASA 加载启动配置时生成的配置错误，请使用 **show startup-config errors** 命令。

示例

以下示例从内存中清除所有配置错误：

```
ciscoasa# clear startup-config errors
```

相关命令

命令	说明
show startup-config errors	显示 ASA 加载启动配置时生成的配置错误。

清除 sunrpc 服务器活动

要清除通过 Sun RPC 应用检查打开的针孔，请在特权 EXEC 模式下使用 **clear sunrpc-server active** 命令。

clear sunrpc-server active

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **clear sunrpc-server active** 命令可清除通过 Sun RPC 应用检查打开的针孔，这些针孔允许服务流量（例如 NFS 或 NIS）通过 ASA。

示例

以下示例展示如何清除 SunRPC 服务表：

```
ciscoasa# clear sunrpc-server
```

相关命令

命令	说明
clear configure sunrpc-server	从 ASA 清除 Sun 远程处理器调用服务。
inspect sunrpc	启用或禁用 Sun RPC 应用检查并配置使用的端口。
show running-config sunrpc-server	显示有关 SunRPC 服务配置的信息。
show sunrpc-server active	显示有关活动的 Sun RPC 服务的信息。

clear threat-detection rate

要在使用 **threat-detection basic-threat** 命令启用基本威胁检测时清除统计信息，请在特权 EXEC 模式下使用 **clear threat detection rate** 命令。

clear threat-detection rate

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例清除检测率统计信息：

```
ciscoasa# clear threat-detection rate
```

相关命令

命令	说明
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 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。

clear threat-detection scanning-threat

要在使用 **threat-detection scanning-threat** 命令启用扫描威胁检测后清除攻击者和目标，请在特权 EXEC 模式下使用 **clear threat-detection scanning-threat** 命令。

clear threat-detection scanning-threat [**attacker** [*ip_address* [*mask*]] |
target [*ip_address* [*mask*]]

语法说明

attacker	（可选）仅清除攻击者。
ip_address	（可选）清除特定 IP 地址。
mask	（可选）设置子网掩码。
target	（可选）仅清除目标。

默认值

如果不指定 IP 地址，将释放所有主机。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要查看当前的攻击者和目标，请使用 **show threat-detection scanning-threat** 命令。

示例

以下示例使用 **show threat-detection scanning-threat** 命令显示目标和攻击者，然后清除所有目标：

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
ciscoasa# clear threat-detection scanning-threat target
```

相关命令

命令	说明
show threat-detection shun	显示当前规避的主机。
show threat-detection statistics host	显示主机统计信息。
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。
threat-detection scanning-threat	启用扫描威胁检测。

clear threat-detection shun

要在使用 **threat-detection scanning-threat** 命令启用扫描威胁检测并自动规避攻击主机后释放当前规避的主机，请在特权 EXEC 模式下使用 **clear threat-detection shun** 命令。

clear threat-detection shun [*ip_address* [*mask*]]

语法说明

ip_address	（可选）解除对特定 IP 地址的规避。
mask	（可选）设置规避的主机 IP 地址的子网掩码。

默认值

如果不指定 IP 地址，将释放所有主机。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要查看当前规避的主机，请使用 **show threat-detection shun** 命令。

示例

以下示例使用 **show threat-detection shun** 命令查看当前规避的主机，然后解除对主机 10.1.1.6 的规避：

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

相关命令

命令	说明
show threat-detection shun	显示当前规避的主机。
show threat-detection statistics host	显示主机统计信息。
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。
threat-detection scanning-threat	启用扫描威胁检测。

clear threat-detection statistics

要在使用 **threat-detection statistics tcp-intercept** 命令启用 TCP 拦截统计信息后清除统计信息，请在特权 EXEC 模式下使用 **clear threat-detection scanning-threat** 命令。

clear threat-detection statistics [**tcp-intercept**]

语法说明

tcp-intercept	（可选）清除 TCP 拦截统计信息。

默认值

消除 TCP 拦截统计信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

要查看 TCP 拦截统计信息，请输入 **show threat-detection statistics top** 命令。

示例

以下示例使用 **show threat-detection statistics top tcp-intercept** 命令显示 TCP 拦截统计信息，然后清除所有统计信息：

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)

ciscoasa# clear threat-detection statistics
```

相关命令

命令	说明
show threat-detection statistics top	显示前 10 个统计信息。
threat-detection statistics	启用威胁检测统计信息。

clear traffic

要重置传输和接收活动的计数器，请在特权 EXEC 模式下使用 **clear traffic** 命令。

clear traffic

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear traffic 命令重置使用 **show traffic** 命令显示的传输和接收活动的计数器。这些计数器指明自上一次输入 clear traffic 命令或自 ASA 进入在线状态以来通过每个接口的数据包和字节的数量。秒数表示自 ASA 上一次重新启动后处于在线状态的持续时间。

示例

以下示例展示 **clear traffic** 命令：

```
ciscoasa# clear traffic
```

相关命令

命令	说明
show traffic	显示传输和接收活动的计数器。

clear uauth

要删除某个用户或所有用户的所有身份验证和授权缓存信息，请在特权 EXEC 模式下使用 **clear uauth** 命令。

clear uauth [*username*]

语法说明

username	（可选）通过用户名指定要删除的用户身份验证信息。

默认值

省略 *username* 参数将删除所有用户的身份验证和授权信息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear uauth 命令删除一个用户或所有用户的 AAA 授权和身份验证缓存，从而强制用户在下一次创建连接时重新进行身份验证。

此命令与 **timeout** 命令配合使用。

每个用户主机 IP 地址都有一个与之连接的授权缓存。如果有用户尝试从正确的主机访问已缓存的服务，ASA 会认为该用户已获得预授权，并会立即充当连接代理。例如，一旦获得授权访问网站，就无需每次加载图像时都连接授权服务器（假设图像来自同一个 IP 地址）。此过程可大大提高性能并减少授权服务器的负载。

缓存允许每个用户主机最多可以有 16 个地址和服务对。

注意　如果启用扩展身份验证，将为分配给客户端的 IP 地址向用户身份验证表添加一个条目（可通过 **show uauth** 命令显示）。但是，如果在网络扩展模式下将扩展身份验证与简易虚拟专用网 (VPN) 远程接入功能结合使用，会在网络间创建 IPsec 隧道，如此一来，位于防火墙后面的用户将无法与单个 IP 地址关联。因此，完成扩展身份验证后将无法创建用户身份验证条目。如果需要 AAA 授权或计费服务，可以启用 AAA 身份验证代理对防火墙后面的用户进行身份验证。有关 AAA 身份验证代理的详细信息，请参阅 AAA 命令。

可使用 **timeout uauth** 命令指定在用户连接进入空闲状态后应保留缓存多长时间。可使用 **clear uauth** 命令删除所有用户的所有授权缓存，这样将强制用户在下一次创建连接时重新进行身份验证。

示例

以下示例展示如何促使用户重新进行身份验证：

```
ciscoasa(config)# clear uauth user
```

相关命令

命令	说明
aaa authentication	启用、禁用或查看 LOCAL、TACACS+ 或 RADIUS 用户身份验证（在使用 **aaa-server** 命令指定的服务器上）。
aaa authorization	启用、禁用或查看 TACACS+ 或 RADIUS 用户授权（在使用 **aaa-server** 命令指定的服务器上）。
show uauth	显示当前的用户身份验证和授权信息。
timeout	设置最长空闲持续时间。

clear uc-ime

要清除用于显示有关思科公司间媒体引擎代理的统计信息的计数器，请在特权 EXEC 模式下使用 **clear uc-ime** 命令。

clear uc-ime [[**mapping-service-sessions** | **signaling-sessions** | **fallback-notification**] **statistics**]

语法说明

fallback-notification	（可选）清除回退通知统计信息的计数器。
mapping-service-sessions	（可选）清除映射服务会话统计信息的计数器。
signaling-sessions	（可选）清除信令会话统计信息的计数器。
statistics	（可选）用于配置要为思科公司间媒体引擎代理清除哪些计数器的关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

示例

以下示例清除用于显示信令会话统计信息的计数器：

```
ciscoasa# clear configure signaling-sessions statistics
```

相关命令

命令	说明
clear configure uc-ime	清除 ASA 上思科公司间媒体引擎代理的运行配置。
show running-config uc-ime	显示思科公司间媒体引擎代理的正在运行的配置。
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信息或详细信息。
uc-imc	在 ASA 上创建思科公司间媒体引擎代理实例。

clear url-block block statistics

要清除数据块缓冲区使用计数器，请在特权 EXEC 模式下使用 **clear url-block block statistics** 命令。

clear url-block block statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear url-block block statistics 命令清除数据块缓冲区使用计数器，但当前保留的数据包数量（全局）计数器除外。

示例

以下示例清除 URL 数据块统计信息并显示清除后的计数器的状态：

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
-----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

相关命令

命令	说明
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-block	管理用于网络服务器响应的 URL 缓冲区。
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。

clear url-cache statistics

要从配置中删除 **url-cache** 命令语句，请在特权 EXEC 模式下使用 **clear url-cache** 命令。

clear url-cache statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear url-cache 命令从配置中删除 URL 缓存统计信息。

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。获得符合安全需求的使用情况分析后，输入 **url-cache** 命令以提高吞吐量。使用 **url-cache** 命令时，计费日志会面向 Websense 协议 V4 和 N2H2 URL 过滤进行更新。

示例

以下示例清除 URL 缓存统计信息：

```
ciscoasa# clear url-cache statistics
```

相关命令

命令	说明
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，该缓存在等待来自 N2H2 或 Websense 过滤服务器的响应时用于缓冲 URL。
url-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
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。

clear url-server

要清除 URL 过滤服务器统计信息，请在特权 EXEC 模式下使用 **clear url-server** 命令。

clear url-server statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear url-server 命令从配置中删除 URL 过滤服务器统计信息。

示例

以下示例清除 URL 服务器统计信息：

```
ciscoasa# clear url-server statistics
```

相关命令

命令	说明
filter url	将流量引导至 URL 过滤服务器。
show url-server	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-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
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。

clear user-identity active-user-database

要将身份防火墙将指定用户的状态设置为 “ 注销 ”，请在特权 EXEC 模式下使用 **clear user-identity active-user-database** 命令。

clear user-identity active-user-database [**user** [*domain_nickname*\]*use_rname*] | **user-group** [*domain_nickname*\\]*user_group_name*]

语法说明

*domain_nickname**user_group_name*	指定要清除统计信息的用户组。 *group_name* 可包含任何字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}。]。如果 *domain_NetBIOS_name**group_name* 包含空格，必须用引号将域名和用户名引起来。
*domain_nickname**use_rname*	指定要清除统计信息的用户。 *user_name* 可包含任何字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}。]。如果 *domain_NetBIOS_name**user_name* 包含空格，必须用引号将域名和用户名引起来。
user	指定要清除用户的统计信息。
user-group	指定要清除用户组的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

此命令将指定用户、属于指定用户组的所有用户或者所有用户的状态设置为 “ 注销 ”。

如果指定 **user-group** 关键字时，会将属于指定用户组的所有用户的状态设置为 “ 注销 ”。如果不一起指定 *domain_nickname* 参数和 **user-group** 关键字，默认域中带有 *user_group_name* 的组的用户将被设置为 “ 注销 ” 状态。

如果指定 **user** 关键字，指定用户的状态将被设置为 “ 注销 ”。如果不一起指定 *domain_nickname* 参数和 **user** 关键字，默认域中带有 *user_name* 的用户将被设置为 “ 注销 ” 状态。

如果不指定 **user** 或 **user-group** 关键字，所有用户的状态都将被设置为 “ 注销 ”。

示例

以下示例将 SAMPLE 域中用户组 users1 的所有用户的状态设置为 “ 注销 ”。

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

相关命令

命令	说明
clear configure user-identity	清除身份防火墙功能的配置。
show user-identity user active	显示身份防火墙的活动用户。

clear user-identity ad-agent statistics

要清除身份防火墙的 AD 代理统计信息，请在特权 EXEC 模式下使用 **clear user-identity ad-agent statistics** 命令。

clear user-identity ad-agent statistics

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

ASA 维护以下有关主要和辅助 AD 代理的信息：

- AD 代理状态
- 域状态
- AD 代理统计信息

使用 **clear user-identity ad-agent statistics** 命令可清除 AD 代理的统计信息。

示例

以下示例清除身份防火墙的 AD 代理统计信息：

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics

    Primary AD Agent                Total  Last Activity
    -------------------------  ----------  ------------------------
    Input packets:                      0  N/A
    Output packets:                     0  N/A
    Send updates:                       0  N/A
    Recv updates:                       0  N/A
    Keepalive failed:                   0  N/A
    Send update failed:                 0  N/A
    Query failed:                       0  N/A
```

```
Secondary AD Agent              Total  Last Activity
------------------------  ----------  ------------------------
Input packets:                      0  N/A
Output packets:                     0  N/A
Send updates:                       0  N/A
Recv updates:                       0  N/A
Keepalive failed:                   0  N/A
Send update failed:                 0  N/A
Query failed:                       0  N/A
```

相关命令

命令	说明
clear configure user-identity	清除身份防火墙功能的配置。
show user-identity ad-agent [**statistics**]	显示身份防火墙的 AD 代理统计信息。

clear user-identity statistics

要清除用于显示有关身份防火墙的统计信息的计数器，请在特权 EXEC 模式下使用 **clear user-identity statistics** 命令。

clear user-identity statistics [**user** [*domain_nickname*\]*use_rname*] | **user-group** [*domain_nickname*\\]*user_group_name*]

语法说明

*domain_nickname**user_group_name*	指定要清除统计信息的用户组。 *group_name* 可包含任何字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}。]。如果 *domain_NetBIOS_name**group_name* 包含空格，必须用引号将域名和用户名引起来。
*domain_nickname**use_rname*	指定要清除统计信息的用户。 *user_name* 可包含任何字符，包括 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}。]。如果 *domain_NetBIOS_name**user_name* 包含空格，必须用引号将域名和用户名引起来。
user	指定要清除用户的统计信息。
user-group	指定要清除用户组的统计信息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

如果未在指定 *user_group_name* 之前指定 *domain_nickname*，ASA 将删除默认域中带有 *user_group_name* 的组的身份防火墙统计信息。

如果未在指定 *user_name* 之前指定 *domain_nickname*，ASA 将删除默认域中带有 *user_name* 的用户的身份防火墙统计信息。

示例

以下示例清除用于显示某个用户组的统计信息的计数器：

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

相关命令

命令	说明
clear configure user-identity	清除身份防火墙功能的配置。
show user-identity statistics	显示身份防火墙的用户或用户组统计信息。

clear user-identity user-not-found

要清除身份防火墙的 ASA“ 找不到的用户 ” 本地数据库，请在特权 EXEC 模式下使用 **clear user-identity user-not-found** 命令。

clear user-identity user-not-found

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

ASA 维护未能在 Microsoft Active Directory 中找到的 IP 地址的 “ 找不到的用户 ” 本地数据库。ASA 仅保留 “ 找不到的用户 ” 列表的最新 1024 个数据包（来自同一个源的连续数据包将被当作一个数据包），而不会在数据库中保留整个列表。

使用 **clear user-identity user-not-found** 命令可清除 ASA 上的本地数据库。

提示　使用 **show user-identity user-not-found** 命令可显示未能在 Microsoft Active Directory 中找到的用户的 IP 地址。

示例

以下示例清除身份防火墙的 “ 找不到的用户 ” 本地数据库：

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

相关命令

命令	说明
clear configure user-identity	清除身份防火墙功能的配置。
show user-identity user-not-found	显示未能在 ASA“ 找不到的用户 ” 数据库中找到的 Active Directory 用户的 IP 地址。

clear user-identity user no-policy-activated

要清除 ASA 上未激活的身份防火墙用户的本地记录，请在特权 EXEC 模式下使用 **clear user-identity user no-policy-activated** 命令。

clear user-identity user no-policy-activated

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

使用 **clear user-identity user no-policy-activated** 命令可清除未通过任何安全策略激活的用户的本地记录（用户未激活意味着，用户不是已激活用户组的一部分，或者未在访问列表或服务策略配置中被引用）。

clear user-identity user no-policy-activated 还清除处于活动状态但未激活的用户的 IP 地址。

如果为身份防火墙创建用户组，必须激活创建的用户组；这意味着，创建的用户组必须是导入用户组（在访问列表或服务策略配置中被定义为用户组）或本地用户组（使用 object-group user 定义）。

示例

以下示例清除 ASA 上未激活的用户的本地记录：

```
ciscoasa# clear user-identity user no-policy-activated
```

相关命令

命令	说明
clear configure user-identity	清除身份防火墙功能的配置。
show user-identity group	显示身份防火墙的已激活用户组列表。

clear vpn-sessiondb statistics

要清除有关 VPN 会话的信息（包括所有统计信息或者特定会话或协议），请在特权 EXEC 模式下使用 **clear vpn-sessiondb statistics** 命令。

clear vpn-sessiondb {**all** | **anyconnect** | **email-proxy** | **global** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol* | **ra-ikev1-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn**}

语法说明

all	清除所有会话的统计信息。
anyconnect	清除 AnyConnect VPN 客户端会话的统计信息。
email-proxy	清除邮件代理会话的统计信息。
global	清除全局会话数据的统计信息。
index *indexnumber*	按索引号清除单个会话的统计信息。**show vpn-sessiondb detail** 命令的输出显示每个会话的索引号。
ipaddress *IPaddr*	清除指定 IP 地址的会话的统计信息。
l2l	清除 VPN LAN-to-LAN 会话的统计信息。
protocol *protocol*	清除以下协议的统计信息： • ikev1 - 使用 IKEv1 协议的会话。 • ikev2 - 使用 IKEv2 协议的会话。 • 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。 • ospfv3 - OSPFv3 over IPsec 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	清除 IPsec IKEv1 和 L2TP 会话的统计信息。
tunnel-group *groupname*	清除指定的隧道组（连接配置文件）的会话的统计信息。
vpn-lb	清除 VPN 负载平衡管理会话的统计信息。
webvpn	清除无客户端 SSL VPN 会话的统计信息。

默认值

没有默认行为和默认值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

clear wccp

要重置 WCCP 信息，请在特权 EXEC 模式下使用 **clear wccp** 命令。

clear wccp [**web-cache** | *service_number*]

语法说明

web-cache	指定网络缓存服务。
service-number	动态服务标识符，表示缓存所指定的服务定义。动态服务编号可以是 0 至 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。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何重置网络缓存服务的 WCCP 信息：

```
ciscoasa# clear wccp web-cache
```

相关命令

命令	说明
show wccp	显示 WCCP 配置。
wccp redirect	启用 WCCP 重定向支持。

clear webvpn sso-server statistics

要重置来自 WebVPN 单点登录 (SSO) 服务器的统计信息，请在特权 EXEC 模式下使用 **clear webvpn sso-server statistics** 命令。

clear webvpn sso-server statistics *servername*

语法说明

servername	指定要重置的 SSO 服务器的名称。

默认值

没有默认行为或值。

命令模式

下表展示了可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

此命令不重置 “ 待处理请求 ” 统计信息。

示例

以下示例展示加密加速器统计信息：

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

相关命令

命令	说明
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto accelerator statistics	显示加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

clear xlate

要清除当前的动态转换和连接信息，请在特权 EXEC 模式下使用 **clear xlate** 命令。

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*]

语法说明

global *ip1*[**-***ip2*]	（可选）按全局 IP 地址或地址范围清除活动转换。
gport *port1*[*-port2*]	（可选）按全局端口或端口范围清除活动转换。
interface *if_name*	（可选）按接口显示活动转换。
local *ip1*[**-***ip2*]	（可选）按本地 IP 地址或地址范围清除活动转换。
lport *port1*[*-port2*]	（可选）按本地端口或端口范围清除活动转换。
netmask *mask*	（可选）指定用于限定全局或本地 IP 地址的网络掩码。
state *state*	（可选）按状态清除活动转换。可以输入以下一种或多种状态： • **static** - 指定**静态**转换。 • **portmap** - 指定 PAT 全局转换。 • **norandomseq** - 指定带有 **norondomseq** 设置的 **nat** 或**静态**转换。 • **identity** - 指定 **nat 0** 身份地址转换。 指定多于一种状态时，请用空格将状态隔开。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

clear xlate 命令清除转换槽的内容（“xlate” 是指转换槽）。转换槽在密钥更改后仍可继续存在。在配置中添加、更改或删除 **global** 或 **nat** 命令后，务必要使用 **clear xlate** 命令。

转换描述 NAT 或 PAT 会话。可使用带有 **detail** 选项的 **show xlate** 命令查看这些会话。有两种类型的转换：静态和动态。

静态转换是使用 **static** 命令创建的持久转换。**clear xlate** 命令不会清除静态条目中主机的转换。只能通过从配置中删除 **static** 命令来删除静态转换； **clear xlate** 命令不会删除静态转换规则。如果从配置中删除某个静态命令，使用该静态规则的先前存在的连接仍可转发流量。使用 **clear local-host** 或 **clear conn** 命令可停用这些连接。

动态转换是根据流量处理的需求创建的转换（通过使用 **nat** 或**全局**命令）。**clear xlate** 命令删除动态转换以及与这些转换关联的连接。也可以使用 **clear local-host** 或 **clear conn** 命令清除转换及关联的连接。如果从配置中删除 **nat** 或**全局**命令，动态转换及关联的连接仍可保持活动状态。使用 **clear xlate** 命令可删除这些连接。

示例

以下示例展示如何清除当前的转换和连接槽信息：

```
ciscoasa# clear xlate global
```

相关命令

命令	说明
clear local-host	清除本地主机网络信息。
clear uauth	清除用户身份验证和授权缓存信息。
show conn	显示所有活动连接。
show local-host	显示本地主机网络信息。
show xlate	显示当前转换信息。

第 8 章

client-access-rule 至 crl enforcenextupdate 命令

client-access-rule

要配置规则以限制可通过 ASA 的 IPsec 连接的远程访问客户端的类型和版本，请在组策略配置模式下使用 **client-access-rule** 命令。要删除规则，请使用此命令的 **no** 形式。

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

语法说明

deny	拒绝特定类型和 / 或版本设备的连接。
none	允许无客户端访问规则。将 **client-access-rule** 设置为一个空值，从而允许不加限制。防止从默认或指定的组策略继承值。
permit	允许特定类型和 / 或版本设备的连接。
priority	确定规则的优先级。具有最小整数的规则具有最高优先级。因此，与客户端类型和 / 或版本匹配的具有最小整数的规则是应用的规则。如果一个较低优先级的规则与之冲突，ASA 会忽略它。
type *type*	通过任意形式的字符串（例如 VPN 3002）标识设备类型。除可以使用 * 字符作为通配符外，字符串必须与 **show vpn-sessiondb remote** 命令输出完全匹配。
version *version*	通过任意形式的字符串标识设备版本，例如 7.0。除可以使用 * 字符作为通配符外，字符串必须与 **show vpn-sessiondb remote** 命令输出完全匹配。

默认值

默认情况下，无访问规则。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要删除所有规则，请使用 **no client-access-rule 命令**（仅带有 *priority* 参数）。这删除所有已配置的规则，包括通过发出 **client-access-rule none** 命令创建的空规则。

当无客户端访问规则时，用户继承默认组策略中的任何规则。要防止用户继承客户端访问规则，请使用 **client-access-rule none** 命令。此操作使得所有客户端类型和版本可以连接。

根据以下附加说明构建规则：

- 如果不定义任何规则，ASA 将允许所有连接类型。
- 如果一个客户端与所有规则均不匹配，ASA 将拒绝此连接。这意味着如果定义一个拒绝规则，还必须至少定义一个允许规则，否则 ASA 将拒绝所有连接。
- 对于软件和硬件客户端，类型和版本必须与 **show vpn-sessiondb remote** 命令输出中的类型与版本完全匹配。
- * 字符是通配符，可以在每个规则中多次使用。例如，**client-access-rule 3 deny type * version 3.*** 创建一个优先级为 3 的客户端访问规则，该规则拒绝运行软件发布版本 3.x 的所有客户端类型。
- 您可以为每个组策略最多构建 25 个规则。
- 对整套规则的限制为 255 个字符。
- 可以为不发送客户端类型和 / 或版本的客户端使用 n/a（不适用）。

示例

以下示例展示如何为名为 FirstGroup 的组策略创建客户端访问规则。这些规则允许运行软件版本 4.1 的 VPN 客户端，同时拒绝所有 VPN 3002 硬件客户端：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-access-rule 1 d t VPN3002 v *
ciscoasa(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-bypass-proxy

要在 ASA 仅希望管理 IPv6 流量时配置其如何管理 IPv4 流量，或者要在 ASA 仅希望管理 IPv4 流量时配置其如何管理 IPv6 流量，请在组策略配置模式下使用 **client-bypass-proxy** 命令。要清除客户端旁路协议设置，请使用此命令的 **no** 形式。

client-bypass-protocol {**enable** | **disable**}

no client-bypass-protocol {**enable** | **disable**}

语法说明

enable	如果 Client Bypass Protocol（客户端旁路协议）已启用，则从客户端以明文发送尚未分配 IP 地址类型的 ASA 的 IP 流量。
disable	如果 Client Bypass Protocol（客户端旁路协议）已禁用，则丢弃尚未分配 IP 地址类型的 ASA 的 IPv6 流量。

默认值

默认情况下，在 DfltGrpPolicy 中禁用 Client Bypass Protocol（客户端旁路协议）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

Client Bypass Protocol（客户端旁路协议）功能允许在 ASA 仅希望管理 IPv6 流量时配置其如何管理 IPv4 流量，或在 ASA 仅希望管理 IPv4 流量时配置其如何管理 IPv6 流量。

当 AnyConnect 客户端对 ASA 进行 VPN 连接时，ASA 可以为客户端分配一个 IPv4、IPv6 或 IPv4 和 IPv6 两个地址。如果 ASA 对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol（客户端旁路协议）丢弃 ASA 尚未分配 IP 地址的网络流量，或允许该流量绕过 ASA 并从客户端以未加密或 “ 明文 ” 形式发送。

举例来说，假设 ASA 只分配一个 IPv4 地址到 AnyConnect 连接且终端被双堆叠。当终端尝试接入 IPv6 地址时，如果客户端绕过协议被禁用，IPv6 流量会终止，但如果客户端绕过协议被启用，IPv6 流量会通过客户端不受阻碍的发送。

示例

以下示例启用客户端旁路协议：

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

以下示例禁用客户端旁路协议：

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

以下示例清除客户端旁路协议设置：

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

client（CTL 提供程序）

要指定允许连接至证书信任列表提供程序的客户端，或要指定客户端身份验证的用户名和密码，请在 CTL 提供程序配置模式下使用 **client** 命令。要删除配置，请使用此命令的 **no** 形式。

client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

语法说明

encrypted	指定密码加密。
interface *if_name*	指定允许连接的接口。
ipv4_addr	指定客户端的 IP 地址。
password *password*	指定用于客户端身份验证的密码。
username *user_name*	指定用于客户端身份验证的用户名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CTL 提供程序配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 CTL 提供程序配置模式下使用 **client** 命令指定允许连接至 CTL 提供程序的客户端，并为客户端身份验证设置用户名和密码。可以发出多个命令定义多个客户端。用户名和密码必须与 CallManager 集群的 CCM 管理员的用户名和密码匹配。

示例

以下示例展示如何创建 CTL 提供程序实例：

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

相关命令

命令	说明
ctl	解析来自 CTL 客户端的 CTL 文件并安装信任点。
ctl-provider	在 CTL 提供程序配置模式下配置 CTL 提供程序实例。
export	指定要导出至客户端的证书
service	指定 CTL 提供程序侦听的端口。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

client（TLS 代理）

要配置信任点、密钥对和密码套件，请在 TLS 代理配置模式下使用 **client** 命令。要删除配置，请使用此命令的 **no** 形式。

client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

语法说明

cipher-suite *cipher_suite*	指定密码套件。选项包括 des-sha1、3des-sha1、aes128-sha1、aes256-sha1 或 null-sha1。
issuer *ca_tp_name*	指定颁发客户端动态证书的本地 CA 信任点。
keypair *key_label*	指定由客户端动态证书使用的 RSA 密钥对。
ldc	指定本地动态证书颁发者或密钥对。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
TLS 代理配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 TLS 代理配置模式下使用 **client** 命令，可在 TLS 代理中以 TLS 客户端角色身份为 ASA 控制 TLS 握手参数。这包括密码套件配置，或设置本地动态证书颁发者或密钥对。颁发客户端动态证书的本地 CA 是通过 **crypto ca trustpoint** 命令定义的，且必须已经由 **proxy-ldc-issuer** 命令或默认的本地 CA 服务器 (LOCAL-CA-SERVER) 配置了信任点。

必须通过 **crypto key generate** 命令生成了密钥对值。

对于客户端代理（充当连接到服务器的 TLS 客户端的代理），用户定义的密码套件取代了默认的密码套件，或通过 **ssl encryption** 命令定义密码套件。使用此命令可在两个 TLS 会话之间获取不同的密码。应将 AES 密码与 CallManager 服务器配合使用。

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	说明
ctl-provider	定义 CTL 提供程序实例，然后进入 CTL 提供程序配置模式。
server trust-point	指定要在 TLS 握手期间提供的代理信任点证书。
show tls-proxy	显示 TLS 代理。
tls-proxy	定义 TLS 代理实例并设置会话的最大数。

client-firewall

要在 IKE 隧道协商过程中设置 ASA 推送 VPN 客户端的个人防火墙策略，请在组策略配置模式下使用 **client-firewall** 命令。要删除防火墙策略，请使用此命令的 **no** 形式。

client-firewall none

no client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

注意　当防火墙类型为 **zonelabs-integrity** 时，请不要包含参数。Zone Labs Integrity 服务器确定策略。

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

语法说明

acl-in *acl*	提供客户端对入站流量使用的策略。
acl-out *acl*	提供客户端对出站流量使用的策略。
AYT	指定客户端 PC 防火墙应用控制防火墙策略。ASA 检查以确保防火墙已运行。将询问：“Are You There”？如果没有响应，ASA 将拆解隧道。
cisco-integrated	指定 Cisco Integrated 防火墙类型。
cisco-security-agent	指定 Cisco Intrusion Prevention Security Agent 防火墙类型。
CPP	指定 Policy Pushed 作为 VPN 客户端防火墙策略的源。
custom	指定 Custom 防火墙类型。
description *string*	描述防火墙。
networkice-blackice	指定 Network ICE Black ICE 防火墙类型。
none	指示无客户端防火墙策略。设置具有空值的防火墙策略，从而禁止一个策略。防止从默认或指定的组策略继承防火墙策略。
opt	指示可选的防火墙类型。
product-id	标识防火墙产品。
req	指示需要的防火墙类型。

sygate-personal	指定 Sygate Personal 防火墙类型。
sygate-personal-pro	指定 Sygate Personal Pro 防火墙类型。
sygate-security-agent	指定 Sygate Security Agent 防火墙类型。
vendor-id	标识防火墙供应商。
zonelabs-integrity	指定 Zone Labs Integrity Server 防火墙类型。
zonelabs-zonealarm	指定 Zone Labs Zone Alarm 防火墙类型。
zonelabs-zonealarmorpro policy	指定 Zone Labs Zone Alarm 或 Pro 防火墙类型。
zonelabs-zonealarmpro policy	指定 Zone Labs Zone Alarm Pro 防火墙类型。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	添加了 **zonelabs-integrity** 防火墙类型。

使用指南

仅可配置此命令的一个实例。

要删除所有防火墙策略，请使用无参数的 **no client-firewall** 命令。此命令将删除所有已配置的防火墙策略，包括通过发出 **client-firewall none** 命令创建的空策略。

当没有防火墙策略时，用户将继承默认或其他组策略中的任何策略。要防止用户继承这些防火墙策略，请使用 **client-firewall none** 命令。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置需要思科入侵防御安全代理的客户端防火墙策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

要指定为思科统一存在服务器 (CUPS) 配置 TLS 代理时，在 TLS 握手期间显示的代理信任点证书，请在 TLS 代理配置模式下使用 **client trust-point** 命令。要删除代理信任点证书，请使用此命令的 **no** 形式。

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint*]

语法说明

proxy_trustpoint	指定 **crypto ca trustpoint** 命令定义的信任点。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
TLS 代理配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

client trust-point 命令指定 ASA 充当 TLS 客户端角色时 ASA 在握手中使用的信任点和关联的证书。该证书必须由 ASA （身份证书）拥有。

该证书可以是自签证书，由证书颁发机构注册，或来自导入的凭证。**client trust-point** 命令的优先级高于全局 **ssl trust-point** 命令。

示例

以下示例展示 **client trust-point** 命令指定如何对 TLS 服务器在 TLS 握手中使用信任点“ent_y_proxy”。握手可能源于实体 Y 至实体 X，TLS 服务器驻留在其中。ASA 作为实体 Y 的 TLS 代理。

```
ciscoasa(config-tlsp)# client trust-point ent_y_proxy
```

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。

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)# client-types ssl
ciscoasa(config-ca-trustpoint)#
```

以下示例进入 checkin1 信任点的 crypto ca trustpoint 配置模式，并将其指定为 IPsec 信任点：

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# client-types ipsec
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 trustpoint 配置模式。
id-usage	指定可以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。

client-update

要在所有隧道组上或对特定隧道组上为所有活动的远程 VPN 软件和硬件客户端以及配置为 Auto Update（自动更新）客户端的 ASA 发布客户端更新，请在特权 EXEC 模式下使用 **client-update** 命令。

要在全局范围内配置并更改客户端更新参数，包括 VPN 软件和硬件客户端以及配置为 Auto Update（自动更新）客户端的 ASA，请在全局配置模式下使用 **client-update** 命令。

要配置和更改 VPN 软件和硬件客户端的客户端更新隧道组 IPSec 属性参数，请在隧道组 IPSec 属性配置模式下使用 **client-update** 命令。

要禁用客户端更新，请使用此命令的 **no** 形式。

全局配置模式命令：

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

隧道组 IPSec 属性配置模式命令：

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

特权 EXEC 模式命令：

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

语法说明

all	（仅在特权 EXEC 模式下可用。）对所有隧道组中的所有活动远程客户端应用此操作。无法通过命令的 **no** 形式使用关键字 **all**。
component {**asdm** | **image**}	配置为 Auto Update（自动更新）客户端的 ASA 的软件组件。
device-id *dev_string*	如果将 Auto Update（自动更新）客户端配置为使用唯一字符串标识自身，则指定该客户端使用的同一字符串。最大长度是 63 个字符。
enable	（仅在全局配置模式下可用）。启用远程客户端软件更新。
family *family_name*	如果将 Auto Update（自动更新）客户端配置为通过设备系列标识自身，则指定该客户端使用的同一设备系列。它可以是 ASA、PIX 或具有最大长度为 7 个字符的文本字符串。
rev-nums *rev-nums*	（在特权 EXEC 模式下不可用。）为此客户端指定软件或固件映像。对于 Windows、WIN9X、WinNT 和 VPN3002 客户端，最多输入 4 个任意顺序的字符串，用逗号分隔。对于 ASA，只允许输入一个字符串。字符串的最大长度为 127 个字符。
tunnel-group	（仅在特权 EXEC 模式下可用。）为远程客户端更新指定有效的隧道组的名称。

type *type*	（在特权 EXEC 模式下不可用。）指定远程 PC 的操作系统或 ASA（配置为 Auto Update（自动更新）客户端）的类型以通知客户端更新。该列表如下： • asa5505：思科 5505 自适应安全设备 • asa5510：思科 5510 自适应安全设备 • asa5520：思科 5520 自适应安全设备 • asa5540：思科 5540 自适应安全设备 • linux：Linux 客户端 • mac：MAC OS X 客户端 • pix-515：思科 PIX 515 防火墙 • pix-515E：思科 PIX 515E 防火墙 • pix-525：思科 PIX 525 防火墙 • pix-535：思科 PIX 535 防火墙 • Windows：所有基于 Windows 的平台 • WIN9X：Windows 95、Windows 98 和 Windows ME 平台 • WinNT：Windows NT 4.0、Windows 2000 和 Windows XP 平台 • vpn3002：VPN 3002 硬件客户端 • 最多 15 个字符的文本字符串
url *url-string*	（在特权 EXEC 模式下不可用。）为软件 / 固件映像指定 URL。此 URL 必须指向一个适合此客户端的文件。最大字符串长度为 255 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
特权 EXEC	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	增加了隧道组 IPsec 属性配置模式。
7.2(1)	增加了 **component**、**device-id** 和 **family** 关键字及其参数以支持的 ASA。

使用指南

在隧道组 IPsec 属性配置模式下，您只能将此属性应用到 IPsec 远程访问隧道组类型。

client-update 命令使您可启用更新；指定要应用更新的客户端类型和修订号；提供获取更新的 URL 或 IP 地址；以及对于 Windows 客户端，可以选择通知应更新其 VPN 客户端版本的用户。如果客户端已经运行了修订号列表中包含的软件版本，则无需更新其软件。如果客户端未运行列表中包含的软件版本，则应进行更新。

对于 Windows 客户端，您可以为用户提供一种完成该更新的机制。对于 VPN 3002 硬件客户端用户，将在没有通知的情况下自动进行更新。当客户端类型为另一 ASA 时，此 ASA 将作为自动更新服务器。

注意　对于所有 Windows 客户端和 Auto Update（自动更新）客户端，您必须使用协议 “http://” 或 “https://” 作为 URL 的前缀。而对于 VPN 3002 硬件客户端，您必须指定协议 “tftp://”。

另外，对于 Windows 客户端和 VPN 3002 硬件客户端，您可以只对各自的隧道组配置客户端更新，而不是对所有特定类型的客户端进行更新。

注意　您可以通过将应用的名称包含在 URL 的末尾以使浏览器自动启动该应用，例如：https://support/updates/vpnclient.exe。

启用客户端更新后，可以为特定的 IPSec 远程访问隧道组定义一组客户端更新参数。为此，请在隧道组 IPSec 属性模式下，指定隧道组的名称及其类型，以及获得更新映像的 URL 或 IP 地址。此外，您必须指定修订号。如果用户客户端修订号与其中一个指定的修订号匹配，则无需更新客户端；例如，对所有 Windows 客户端发布客户端更新。

或者，您可以向具有过时 Windows 客户端（其 VPN 客户端需要更新）的活动用户发送一个通知。对于这些用户，将显示一个对话框，提供一个启动浏览器并下载 URL 指定的站点的更新软件的机会。此消息中唯一可配置的部分是 URL。非活动用户在下次登录时将收到一个通知消息。您可以向所有隧道组上的所有活动客户端发送此通知，或者，您可以将其发送到特定隧道组上的客户端。

如果用户客户端修订号与指定的修订号中的一个匹配，则无需更新客户端且用户不会收到通知消息。VPN 3002 客户端更新无需用户干预，并且用户不会收到通知消息。

注意　如果指定客户端更新类型为 **windows**（指定所有基于 Windows 的平台），然后要对同一实体输入 **win9x** 或 **winnt** 的客户端更新类型，必须先使用此命令的 **no** 形式删除 Windows 客户端类型，然后使用新的 **client-update** 命令指定新客户端类型。

示例

以下示例进入全局配置模式，为所有隧道组上的所有活动远程客户端启用客户端更新：

```
ciscoasa(config)# client-update enable
ciscoasa#
```

以下示例仅适用于 Windows（Win9x、WinNT）。进入全局配置模式，为所有基于 Windows 的客户端配置客户端更新参数，包括修订号 4.7 和获取更新的 URL (https://support/updates)。

```
ciscoasa(config)# client-update type windows url https://support/updates/ rev-nums 4.7
ciscoasa(config)#
```

以下示例仅适用于 VPN 3002 硬件客户端。进入隧道组 IPSec 属性配置模式，为 IPSec 远程访问隧道组 “salesgrp” 配置客户端更新参数。指定修订号 4.7 并使用 TFTP 协议从 IP 地址为 192.168.1.1 的网站获取更新的软件：

```
ciscoasa(config)# tunnel-group salesgrp type ipsec-ra
ciscoasa(config)# tunnel-group salesgrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
ciscoasa(config-tunnel-ipsec)#
```

以下示例展示如何对配置为 Auto Update（自动更新）客户端的思科 5520 ASA 的客户端发布客户端更新：

```
ciscoasa(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

以下示例进入特权 EXEC 模式，为名为 “remotegrp” 的隧道组中的所有需要更新其客户端软件的已连接的远程客户端发送一个客户端更新通知。其他组中的客户端不会收到更新通知。

```
ciscoasa# client-update remotegrp
ciscoasa#
```

以下示例进入特权 EXEC 模式，通知所有隧道组上的所有活动客户端：

```
ciscoasa# client-update all
ciscoasa#
```

相关命令

命令	说明
clear configure client-update	清除整个客户端更新配置。
show running-config client-update	显示当前客户端更新配置。
tunnel-group ipsec-attributes	配置隧道组 ipsec 属性为此组。

clock set

要在 ASA 上手动设置时钟，请在特权 EXEC 模式下使用 **clock set** 命令。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

语法说明

day	设置月的日期，从 1 至 31。例如，根据标准日期格式，可以输入日和月为 **april 1** 或 **1 april**。
hh:*mm*:*ss*	以 24 小时时间格式设置小时、分钟和秒。例如，将 **20:54:00** 设置为下午 8:54。
month	设置月。根据标准日期格式，可以输入日和月为 **april 1** 或 **1 april**。
year	使用四位数字设置年，例如 **2004**。年范围为 1993 至 2035。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果未输入任何 **clock** 配置命令，则 **clock set** 命令的默认时区为 UTC。如果输入 **clock set** 命令后，使用 **clock timezone** 命令更改时区，则时间自动调整到新的时区。但如果在输入 **clock set** 命令之前，先通过 **clock timezone** 命令建立了时区，则输入的时间适合新的时区而不适合 UTC。同样，如果在输入 **clock summer-time** 命令之前，先输入 **clock set** 命令，则时间调整为夏令时。如果在输入 **clock set** 命令前，先输入 **clock summer-time** 命令，则输入夏令时的正确时间。

此命令将时间设置在硬件芯片中，不在配置文件中保存时间。此时间将持续到重新启动。与其他 **clock** 命令不同，此命令为特权执行命令。要重置时钟，需要为 **clock set** 命令设置新的时间。

示例

以下示例将时区设置为 MST，美国的默认夏令时期间，且 MDT 的当前时间为 2004 年 7 月 27 日下午 1:15：

```
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa(config)# exit
ciscoasa# clock set 13:15:0 jul 27 2004
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

以下示例将时钟设置为 UTC 时区中 2004 年 7 月 27 日 8:15，然后将时区设置为 MST 及美国的默认夏令时期间。结束时间（MDT 中的 1:15）与前一个示例的时间相同。

```
ciscoasa# clock set 20:15:0 jul 27 2004
ciscoasa# configure terminal
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

相关命令

命令	说明
clock summer-time	设置显示夏令时的日期范围。
clock timezone	设置时区。
show clock	显示当前时间。

clock summer-time

要设置 ASA 时间的显示夏令时的日期范围，请在全局配置模式下使用 **clock summer-time** 命令。要禁用夏令时日期，请使用此命令的 **no** 形式。

clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]]

语法说明

date	指定夏令时的开始和结束日期为特定年的特定日期。如果使用此关键字，需要每年重置日期。
day	设置月的日期，从 1 至 31。例如，根据标准日期格式，可以输入日和月为 **April 1** 或 **1 April**。
hh:mm	以 24 小时时间格式设置小时和分钟。
month	将月设置为字符串。对于 **date** 命令，可以输入日和月为 **April 1** 或 **1 April**，例如，根据您的标准日期格式。
offset	（可选）设置分钟数以将时间更改为夏令时。默认情况下，此值为 60 分钟。
recurring	以月的天和时间格式指定夏令时的开始和结束日期，而不是特定年中的特定日期。此关键字允许设置循环日期范围，无需每年更改。如果未指定任何日期，ASA 采用美国的默认日期范围：从三月份的第二个星期日上午 2:00 到 11 月的第一个星期日的上午 2:00 。
week	（可选）指定月的一周是介于 1 和 4 之间的整数，还是文字 **first** 或 **last**。例如，如果某天可能落入第五周，则指定 **last**。
weekday	（可选）指定星期几：**Monday**、**Tuesday**、**Wednesday** 等等。
year	使用四位数字设置年，例如 **2004**。年范围为 1993 至 2035。
zone	将时区指定为字符串，例如 **PDT** 表示太平洋夏令时间。当 ASA 根据您用此命令设置的日期范围显示夏令时的时候，时区将更改为此处设置的值。请参阅 **clock timezone** 命令将基本时区设置为除 UTC 之外的任一时区。

默认值

默认偏移量为 60 分钟。

默认的循环日期范围从三月的第二个周日上午 2:00 开始 11 月的第一个星期日的上午 2:00 。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	默认的循环日期范围将更改为三月的第二个周日上午 2:00 11 月的第一个星期日的上午 2:00 。

使用指南

对于南半球，ASA 接受的起始月比结束要晚，例如，从十月至三月。

示例

以下示例设置澳大利亚的夏令时日期范围：

```
ciscoasa(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

某些国家 / 地区在某个特定日期开始夏令时。在以下示例中，将夏令时配置为从 2008 年 4 月 1 日上午 3 时开始 至 2008 年 10 月 1 日上午 4 时结束

```
ciscoasa(config)# clock summer-time UTC date 1 April 2008 3:00 1 October 2008 4:00
```

相关命令

命令	说明
clock set	在 ASA 上手动设置时钟。
clock timezone	设置时区。
ntp server	标识 NTP 服务器。
show clock	显示当前时间。

clock timezone

要设置 ASA 时钟的时区，请在全局配置模式下使用 **clock timezone** 命令。要将时区设置为返回 UTC 的默认值，请使用此命令的 **no** 形式。

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

语法说明

[**-**]*hours*	设置与 UTC 的偏移的小时数。例如，PST 为 -8 小时。
minutes	（可选）设置与 UTC 偏移的分钟数。
zone	将时区指定为字符串，例如，PST 表示太平洋标准时间。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要设置夏令时，请参阅 **clock summer-time** 命令。

clock set 命令或来自 NTP 服务器的时间以 UTC 设置时间。必须使用此命令将时区设置为 UTC 偏移。

示例

以下示例将时区设置为太平洋标准时间，与 UTC 相差 -8 小时：

```
ciscoasa(config)# clock timezone PST -8
```

相关命令

命令	说明
clock set	在 ASA 上手动设置时钟。
clock summer-time	设置显示夏令时的日期范围。
ntp server	标识 NTP 服务器。
show clock	显示当前时间。

cluster-ctl-file

要使用存储在闪存中的从现有 CTL 文件创建的信任点，请在 CTL 文件配置模式下使用 **cluster-ctl-file** 命令。要删除 CTL 文件配置，以便创建新的 CTL 文件，请使用此命令的 **no** 形式。

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

语法说明

filename_path	指定存储在磁盘或闪存中的 CTL 文件的路径和文件名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CTL 文件配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

配置此命令时，电话代理解析存储在闪存中的 CTL 文件并从该 CTL 文件安装信任点，然后使用闪存中的文件创建新的 CTL 文件。

示例

以下示例解析存储在闪存中的 CTL 文件以安装来自该文件的信任点：

```
ciscoasa(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

相关命令

命令	说明
ctl-file (global)	指定要为电话代理配置创建的 CTL 文件，或者要从闪存解析的 CTL 文件。
ctl-file (phone-proxy)	指定要用于电话代理配置的控制文件。
phone-proxy	配置电话代理实例。

cluster encryption

要为在虚拟负载平衡集群上交换的消息启用加密，请在 VPN 负载平衡配置模式下使用 **cluster encryption** 命令。要禁用加密，请用使此命令的 **no** 形式。

cluster encryption

no cluster encryption

注意　VPN 负载平衡需要具有一个有效的 3DES/AES 许可。ASA 在启用负载平衡前检查是否存在此加密许可证。如果未检测到有效的 3DES 或 AES 许可证，ASA 将阻止启用负载平衡，并通过负载平衡系统阻止 3DES 的内部配置，除非许可证允许此应用。

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用加密。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令对虚拟负载平衡集群上交换的消息打开或关闭加密。

在配置 **cluster encryption** 命令前，必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡配置模式。还必须用 **cluster key** 命令配置集群共享的密钥后，才能启用集群加密。

注意　在使用加密时，必须首先配置命令 **isakmp enable** *inside*，其中 *inside* 指定负载平衡内部接口。如果在负载平衡内部接口上未启用 ISAKMP，则在尝试配置集群加密时会出现一条错误消息。

示例

以下是 VPN 负载平衡命令序列的示例，其中包括为虚拟负载平衡集群启用加密的 **cluster encryption** 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)# 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)# participate
```

相关命令

命令	说明
cluster key	指定集群的共享密钥。
vpn load-balancing	进入 vpn 负载平衡配置模式。

cluster exec

要对集群内的所有设备或特定成员执行一个命令，请在特权 EXEC 模式下使用 **cluster exec** 命令。

cluster exec [**unit** *unit_name*] *command*

语法说明

unit *unit_name*	（可选）对特定设备执行此命令。要查看成员名称，请输入 **cluster exec unit ?**（可查阅除当前设备之外的所有名称），或输入 **show cluster info** 命令。
command	指定要执行的命令。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

向所有成员发送 **show** 命令以收集所有输出并将其显示在当前设备的控制台上。其他命令，如 **capture** 和 **copy**，也可在整个集群范围内执行。

示例

要同时将同一捕获文件从集群中的所有设备复制到 TFTP 服务器，请在主设备上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件的名称自动附有设备名称，如 capture1_asa1.pcap、capture1_asa2.pcap 等等。在本示例中，asa1 和 asa2 是集群设备名称。

以下示例输出 **cluster exec show port-channel** 摘要命令显示集群内每个成员的 EtherChannel 信息：

```
ciscoasa# cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes  Gi0/0(P)
2         Po2             LACP      Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
```

```
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes   Gi0/0(P)
2         Po2             LACP      Yes   Gi0/1(P)
```

相关命令

命令	说明
cluster group	输入集群组配置模式。
show cluster info	显示集群信息。

cluster group

要配置集群引导程序参数和其他集群设置，请在全局配置模式下使用 **cluster group** 命令。要清除集群配置，请使用此命令的 **no** 形式。

cluster group *name*

no cluster group *name*

语法说明

name	指定集群名称为 1 到 38 个字符之间的 ASCII 字符串。您只能为每个设备配置一个集群组。集群的所有成员必须使用同一名称。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

集群中的每个设备均需引导程序配置以加入集群。通常，配置的第一个加入集群的设备将是主设备。启用集群并经过选择期间后，集群将选择一个主设备。由于最初在集群中仅有一个设备，则该设备将成为主设备。您添加到集群的后续设备将成为从属设备。

您需使用 **cluster interface-mode** 命令设置集群接口模式，才能配置集群。

您必须使用控制台端口或 ASDM 启用或禁用集群。不能使用 Telnet 或 SSH。

示例

以下示例将配置管理接口，为集群控制链路配置设备本地 EtherChannel，禁用状况检查（临时），然后对称为“unit1”的 ASA（因第一个添加到集群中而成为主设备）启用集群：

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown
```

```
interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    no health-check
    enable noconfirm
```

以下示例包括对从属设备 unit2 的配置：

```
interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    no health-check
    enable as-slave
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接再平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable（集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

cluster ip address

要为虚拟负载平衡集群设置 IP 地址，请在 VPN 负载平衡配置模式下使用 **cluster ip address** 命令。要删除 IP 地址指定，请使用此命令的 **no** 形式。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

语法说明

ip-address	要分配到虚拟负载平衡集群的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡配置模式并配置虚拟集群 IP 地址适用的接口。

集群 IP 地址必须与您正在为其配置虚拟集群的接口位于同一子网中。

在命令的 **no** 形式中，如果指定可选的 *ip-address* 值，则该值必须与现有的集群 IP 地址匹配，才能完成 **no cluster ip address** 命令。

示例

以下示例展示 VPN 负载平衡命令序列，包括将虚拟负载平衡集群的 IP 地址设置为 209.165.202.224 的 **cluster ip address** 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)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

相关命令

命令	说明
interface	设置设备的接口。
nameif	将名称分配到接口。
vpn load-balancing	进入 vpn 负载平衡配置模式。

cluster key

要对虚拟负载平衡集群设置 IPSec 站点间隧道交换的共享密钥，请在 VPN 负载平衡配置模式下使用 **cluster key** 命令。要删除此指定，请使用此命令的 **no** 形式。

cluster key *shared-secret*

no cluster key [*shared-secret*]

语法说明

shared-secret	用来定义 VPN 负载平衡集群的共享密钥的一个包含 3 到 17 个字符的字符串。字符串中可以包含特殊字符串，但不能包含空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡配置模式。在 **cluster key** 命令中定义的共享密钥也用于集群加密。

您必须首先使用 **cluster key** 命令配置共享密钥，才能启用集群加密。

如果在此命令的 **no cluster key** 形式中为 *shared-secret* 指定一个值，则共享密钥的值必须与现有配置匹配。

示例

以下示例展示 VPN 负载平衡命令序列，包括将虚拟负载平衡集群的共享密钥设置为 123456789 的 **cluster key** 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)# 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)# participate
```

相关命令

命令	说明
vpn load-balancing	进入 vpn 负载平衡配置模式。

cluster master unit

要将新的设备设置为 ASA 集群的主设备，请在特权 EXEC 模式下使用 **cluster master unit** 命令。

cluster master unit *unit_name*

注意事项　更改主设备的最佳方法是在主设备上禁用集群（请参阅 **no cluster enable** 命令），等待新的主设备选择，然后重新启用集群。如果必须指定要其成为主设备的确切的设备，请使用 **cluster master unit** 命令。但请注意，对于集中功能，如果您使用此命令强制更改主控设备，则所有连接都将被丢弃，您必须在新主控设备上重新建立连接。

语法说明

unit_name	指定要成为新的主设备的本地设备的名称。要查看成员名称，请输入 **cluster master unit ?**（可查阅除当前设备之外的所有名称），或输入 **show cluster info** 命令。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您将需要重新连接到主集群 IP 地址。

示例

以下示例将 asa2 设置为主设备：

```
ciscoasa# cluster master unit asa2
```

相关命令

命令	说明
cluster exec	将命令发送到所有集群成员。
cluster group	配置集群。
cluster remove unit	从集群中删除设备。

cluster remove unit

要从 ASA 集群中删除设备，请在特权 EXEC 模式下使用 cluster remove unit 命令。

cluster remove unit *unit_name*

语法说明

unit_name	指定要从集群中删除的本地设备的名称。要查看成员名称，请输入 **cluster remove unit ?** 或输入 **show cluster info** 命令。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

引导程序配置保持不变且从主设备最后同步配置，因此，您可稍后重新添加该设备而不会丢失配置。如果在从属设备上输入此命令来删除主设备，会选择一个新的主设备。

示例

以下示例检查设备的名称，然后从集群中删除 asa2：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2.To bring it back
to the cluster please logon to that unit and re-enable clustering
```

相关命令

命令	说明
cluster exec	将命令发送到所有集群成员。
cluster group	配置集群。
cluster master unit	将新的设备设置为 ASA 集群的主设备。

cluster-interface

要指定集群控制链路物理接口和 IP 地址，请在集群组配置模式下使用 **cluster-interface** 命令。要删除集群接口，请使用此命令的 **no** 形式。

cluster-interface *interface_id* **ip** *ip_address mask*

no cluster-interface [*interface_id* **ip** *ip_address mask*]

语法说明

interface_id	指定物理接口、EtherChannel 或冗余接口。不允许子接口和管理接口。此接口不能配置 **nameif**。对于具有 IPS 模块 的 ASA 5585-X，无法为集群控制链路使用 IPS 模块接口。
ip *ip_address mask*	指定 IP 地址的 IPv4 地址；此接口不支持 IPv6。对于每个设备，请在同一网络指定不同的 IP 地址。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您需启用集群控制链路接口，才能加入集群。

如果您有足够的接口，我们建议您将多个集群控制链路接口合并到 EtherChannel 中。EtherChannel 对 ASA 而言是本地的，而非跨区 EtherChannel。我们建议您为集群控制链路使用十千兆位以太网接口。我们建议使用 EtherChannel 成员接口的 ON 模式减少集群控制链路上不必要的流量。由于集群控制链路是单独、稳定的网络，无需 LACP 流量开销。

集群控制链路接口配置不能从主设备复制到从属设备；但每个设备必须使用相同的配置。由于不会复制此配置，每个设备必须单独配置集群控制链路接口。

有关集群控制链路的详细信息，请参阅配置指南。

示例

以下示例为 TenGigabitEthernet 0/6 和 TenGigabitEthernet 0/7 创建 EtherChannel、Port-channel 2，然后将端口通道分配为集群控制链路。在将接口分配到通道组时，将自动创建端口通道接口。

```
interface tengigabitethernet 0/6
    channel-group 2 mode on
    no shutdown
```

```
interface tengigabitethernet 0/7
    channel-group 2 mode on
    no shutdown

cluster group cluster1
    cluster-interface port-channel2 ip 10.1.1.1 255.255.255.0
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接再平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable（集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

cluster-mode

要指定集群的安全模式，请在电话代理配置模式下使用 **cluster-mode** 命令。要将集群的安全模式设置为默认模式，请使用此命令的 **no** 形式。

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

语法说明

mixed	配置电话代理功能时，将集群模式指定为混合模式。
nonsecure	配置电话代理功能时，将集群模式指定为非安全模式。

默认值

默认集群模式为非安全模式。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

当您配置要在混合模式（安全和非安全模式）集群中运行的电话代理时，也必须配置 LDC 发布者，以防某些电话配置为身份验证或加密模式：

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

示例

以下示例将电话代理的安全模式设置为混合（IP 电话将在安全和非安全的模式下运行）：

```
ciscoasa(config-phone-proxy)# cluster-mode mixed
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。
tls-proxy	配置 TLS 代理实例。

cluster port

要为虚拟负载平衡集群设置 UDP 端口，请在 VPN 负载平衡配置模式下使用 **cluster port** 命令。要删除端口指定，请使用此命令的 **no** 形式。

cluster port *port*

no cluster port [*port*]

语法说明

port	要分配到虚拟负载平衡集群的 UDP 端口。

默认值

默认集群端口为 9023。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡配置模式。

可指定任何有效的 UDP 端口号。范围为 1 65535。

如果在用此命令的 **no cluster port** 形式为 *port* 指定一个值，则指定的端口号必须与现有的已配置的端口号匹配。

示例

以下示例将虚拟负载平衡集群的 UDP 端口设置为 9023：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
```

相关命令

命令	说明
vpn load-balancing	进入 vpn 负载平衡配置模式。

command-alias

要为命令创建别名，请在全局配置模式下使用 **command-alias** 命令。要删除别名，请使用此命令的 **no** 形式。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

语法说明

command_alias	为现有命令指定新名称。
mode	指定要在其中创建命令别名的命令模式，例如，**exec**（表示用户和特权 EXEC 模式）、**configure** 或 **interface**。
original_command	指定要为其创建命令别名的现有命令或带关键字的命令。

默认值

默认情况下，将配置以下用户 EXEC 模式别名：

- **h** 表示 **help**
- **lo** 表示 **logout**
- **p** 表示 **ping**
- **s** 表示 **show**

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当您输入命令别名时，将调用原始命令。例如，您可能要创建命令别名为长命令提供快捷方式。

您可以为任何命令的第一部分创建别名，并仍可正常输入其他关键字和参数。

当您使用 CLI 帮助时，命令别名用星号 (*) 表示，并显示为以下格式：

```
*command-alias=original-command
```

例如，**lo** 命令别名与其他以 “lo” 开头的特权 EXEC 模式命令一起显示，如下所示：

```
ciscoasa# lo?
*lo=logout login  logout
```

您可以在不同的模式下使用同一别名。例如，可在特权 EXEC 模式和配置模式下对不同的命令使用 “happy” 作为别名，如下所示：

```
ciscoasa(config)# happy?

configure mode commands/options:
*happy="username employee1 password test"

exec 模式命令 / 选项：
*happy=enable
```

要仅列出命令而忽略别名，则以空格开始您的输入行。另外，要忽略命令别名，请在输入命令前使用空格。在以下示例中，因为 **happy?** 前有一个空格，所以不显示别名 “happy”。命令创建虚拟接口。

```
ciscoasa(config)# alias exec test enable
ciscoasa(config)# exit
ciscoasa#   happy?
ERROR: % Unrecognized command
```

如同命令一样，您可使用 CLI 帮助显示命令别名后可跟随的参数和关键字。

您必须输入完整的命令别名。不接受别名缩写。在以下示例中，解析器不会将 **hap** 命令识别为指示名为 “happy” 的别名：

```
ciscoasa# hap
% Ambiguous command: "hap"
```

示例

以下示例展示如何为 **copy running-config startup-config** 命令创建名为 “save” 的命令别名：

```
ciscoasa(config)# command-alias exec save copy running-config startup-config
ciscoasa(config)# exit
ciscoasa# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
ciscoasa#
```

相关命令

命令	说明
clear configure command-alias	清除所有非默认命令别名。
show running-config command-alias	显示所有已配置的非默认命令别名。

command-queue

要指定等待响应时排队的 MGCP 命令的最大数量，请在 MGCP 映射配置模式下使用 **command-queue** 命令。要删除配置，请使用此命令的 **no** 形式。

command-queue *limit*

no command-queue *limit*

语法说明

limit	指定可排队的命令的最大数，从 1 到 2147483647。

默认值

此命令默认禁用。

MGCP 命令队列的默认值为 200。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
MGCP 映射配置	•	•	•	•	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **command-queue** 命令指定等待响应时排队的 MGCP 命令的最大数。允许的值范围从 1 到 4294967295。默认值为 200。当已达到限制并有新命令到达时，将删除队列中等待时间最长的命令。

示例

以下示例将 MGCP 命令队列限制为 150 个命令：

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)#command-queue 150
```

相关命令

命令	说明
debug mgcp	启用 MGCP 的调试信息的显示。
mgcp-map	定义 MGCP 映射并启用 mgcp 映射配置模式。
show mgcp	显示 MGCP 配置和会话信息。
timeout	配置经过此时间将关闭 MGCP 媒体或 MGCP PAT Xlate 连接的闲置超时。

community-list

要创建或配置边界网关协议 (BGP) 社区列表并控制对它的访问，请在全局配置命令中使用 **community-list** 命令。要删除社区列表，请使用此命令的 **no** 形式

Standard Community Lists

community-list {*standard* | **standard** *list-name*} {**deny** | **permit**} [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]

no community-list {*standard* | **standard** *list-name*}

Expanded Community Lists

community-list {*expanded* | **expanded** *list-name*} {**deny** | **permit**} *regexp*

no community-list {*expanded* | **expanded** *list-name*}

语法说明

standard	使用从 1 到 99 之间的数子配置一个标准社区列表，以标识一个或多个社区允许组或拒绝组。
standard *list-name*	配置指定的标准社区列表。
permit	允许匹配条件访问。
deny	拒绝匹配条件访问。
community-number	（可选）将社区指定为从 1 到 4294967200 之间的一个 32 位数。可输入一个或多个社区，用空格分隔。
AA:NN	（可选）输入自主系统编号和网络号（以 4 字节新社区格式）。此值通过由冒号分隔的两个 2 字节数配置。每个 2 字节数可输入介于 1 至 65535 之间的一个数。可输入一个或多个社区，用空格分隔。
internet	（可选）指定 Internet 社区。具有此社区的路由通告到所有对等（内部和外部）。
no-export	（可选）指定 no-export 社区。 具有此社区的路由仅通告到在同一自主系统中的对等或联盟内的其他子自主系统。这些路由不会通告给外部对等。
local-AS	（可选）指定 local-as 社区。具有社区的路由仅通告给作为本地自主系统部分的对等或联盟的子自主系统内的对等。这些路由不会通告给外部对等或联盟内的其他子自主系统。
no-advertise	（可选）指定 no-advertise 社区。具有此社区的路由不会通告给任何对等（内部或外部）。
Expanded	配置一个从 100 到 500 的扩展的社区列表编号，用于标识一个或多个社区允许组或拒绝组。
expanded *list-name*	配置指定的扩展社区列表。
regexp	配置用于指定模式匹配输入字符串的正则表达式。 **注**　只能通过扩展的社区列表使用正则表达式。

默认值

默认情况下，不启用 BGP 社区交换。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

community-list 命令用于配置 BGP 社区过滤。将 BGP 社区值配置为 32 位数（旧格式）或为 4 字节数（新格式）。当在全局配置模式下输入 **bgp-community new-format** 命令时，启用新的社区格式。新的社区格式包含一个 4 字节的值。

前两个字节表示自主系统编号，后面的两个字节表示用户定义的网络号。支持对社区列表进行命名和编号。当为指定的邻居配置 **neighbor send-community** 命令时，启用 BGP 对等之间的 BGP 社区属性交换。在 RFC 1997 和 RFC 1998 中定义 BGP 社区属性。

默认情况下，不启用 BGP 社区交换。使用 **neighbor send-community** 命令将基于每个邻居启用 BGP 社区交换。默认情况下，Internet 社区应用到所有路由或前缀，直到通过此命令或 **set community** 命令配置了任何其他社区的值。

如果已配置允许值匹配一组给定的社区，则社区列表默认为隐式拒绝所有其他社区值。

Standard Community Lists

标准社区列表用于配置知名的社区和特定的社区编号。在标准社区列表中，最多可配置 16 个社区。如果您尝试配置超过 16 个社区，则不会处理后面超过限制的社区，也不会将其保存到运行配置文件中。

Expanded Community Lists

扩展的社区列表通过正则表达式用于过滤社区。正则表达式用于配置匹配社区属性的模式。使用 * 或 + 字符匹配的指令优先成为最长的结构。从外到内匹配嵌套结构。在左侧开始匹配连接结构。如果正则表达式可与输入字符串的两个不同部分匹配，则它将优先匹配最早输入的部分。有关配置正则表达式的详细信息，请参阅《*思科 IOS 终端服务配置*指南》的 “ 正则表达式 ” 附录。

社区列表处理

当在同一社区列表语句中配置多个值时，会创建逻辑 AND 条件。所有社区值必须匹配以满足 AND 条件。当在单独的社区列表语句中配置多个值时，会创建逻辑 OR 条件。处理与条件匹配的第一个列表。

示例

在以下示例中，配置标准社区列表允许从自主系统 50000 中的网络 10 路由：

```
ciscoasa(config)#  community-list 1 permit 50000:10
```

在以下示例中，配置标准社区列表允许仅从同一自主系统中的对等或从同一联盟中的子自主系统对等路由：

```
ciscoasa(config)#  community-list 1 permit no-export
```

在以下示例中，配置标准社区列表拒绝路由，即从自主系统 65534 中的网络 40 和自主系统 65412 中的网络 60 承载社区。此示例展示逻辑 AND 条件；所有社区值必须匹配才能处理列表。

```
ciscoasa(config)#  community-list 2 deny 65534:40 65412:60
```

在以下示例中，配置指定的标准社区列表，允许本地自主系统内的所有路由或允许从自主系统 40000 中的网络 20 路由。此示例展示逻辑 OR 条件；处理第一个匹配。

```
ciscoasa(config)#  community-list standard RED permit local-AS
ciscoasa(config)#  community-list standard RED permit 40000:20
```

在以下示例中，配置扩展的社区列表将拒绝从任何专用自主系统承载社区的路由：

```
ciscoasa(config)#  community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

在以下示例中，配置指定的扩展的社区列表拒绝从自主系统 50000 中的网络 1 至 99 路由：

```
ciscoasa(config)#  community-list expanded BLUE deny 50000:[0-9][0-9]_
```

相关命令

命令	说明
bgp-community-new format	配置 BGP 显示格式为 AA:NN（自主系统 : 社区编号 /4 字节数）的社区。
neighbor send-community	指定应发送给 BGP 邻居的社区属性
set community	设置 BGP 社区属性。

compatible rfc1583

要恢复用于根据 RFC 1583 计算汇总路由成本的方法，请在路由器配置模式下使用 **compatible rfc1583** 命令。要禁用 RFC 1583 的兼容性，请使用此命令的 **no** 形式。

compatible rfc1583

no compatible rfc1583

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

仅此命令的 **no** 形式会出现在配置中。

示例

以下示例展示如何禁用 RFC 1583 兼容性路由汇总成本计算：

```
ciscoasa(config-router)# no compatible rfc1583
ciscoasa(config-router)#
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

compression

要启用用于 SVC 连接和 WebVPN 连接的压缩，请在全局配置模式下使用 **compression** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

语法说明

all	指定启用所有可用的压缩技术。
http-comp	指定用于 WebVPN 连接的压缩。
svc	指定用于 SVC 连接的压缩。

默认值

默认为 *all*（全部）。启用所有可用的压缩技术。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

对于 SVC 连接，全局配置模式下配置的 **compression** 命令覆盖组策略 WebVPN 配置模式及用户名 WebVPN 配置模式下配置的 **svc compression** 命令。

例如，如果您在组策略 WebVPN 配置模式下为某个组输入 **svc compression** 命令，然后在全局配置模式下输入 **no compression** 命令，则覆盖已为该组配置的 **svc compression** 命令设置。

相反，如果您在全局配置模式下通过 **compression** 命令启用压缩返回，则任何组设置生效，且这些设置最终确定压缩行为。

如果通过 **no compression** 命令禁用压缩，则仅影响新的连接。活动的连接不受影响。

示例

在以下示例中，启用了用于 SVC 连接的压缩：

```
hostname(config)# compression svc
```

在以下示例中，禁用了用于 SVC 连接和 WebVPN 连接的压缩：

```
hostname(config)# no compression svc http-comp
```

相关命令

命令	说明
show webvpn svc	显示有关 SVC 安装的信息。
svc	为特定组或用户启用或要求 SVC。
svc compression	为特定组或用户通过 SVC 连接启用 HTTP 数据的压缩。

config-register

要设置下次重新加载 ASA 所用的配置注册值，请在全局配置模式下使用 **config-register** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。

config-register *hex_value*

no config-register

语法说明

hex_value	将配置注册值设置为 0x0 和 0xFFFFFFFF 之间的一个十六进制数。此数显示为 32 位，且每个十六进制字符显示为 4 位。每个位控制不同的特征。但 32 至 20 位，既可留作将来使用，用户不能对其进行设置，当前也不能由 ASA 使用；因此，您可以忽略代表这些为的三个字符，因为始终将它们设置为 0。由 5 个十六进制字符代表相关的位：0x*nnnnn*。 无需包括前面的 0。需要包括后面的 0。例如，0x2001 等同于 0x02001；但 0x10000 需要所有零。有关相关位的可用值的详细信息，请参阅表 8-1。

默认值

默认值为 0x1，该值从本地映像引导并启动配置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅在 ASA 5500 系列上受支持。配置注册值确定从哪个映像引导以及其他引导参数。

五个字符从右到左从 0 至 4 进行编号，这对十六进制和二进制数是标准的。您可为每个字符选择一个值，并酌情混合及匹配各值。例如，您可为字符数 3 选择 0 或 2。某些值在与其他值冲突时会优先得到采用。例如，如果设置 0x2011，其设置 ASA 既从 TFTP 服务器引导，也从本地映像启动，则 ASA 从 TFTP 服务器引导。由于此值还规定，如果 TFTP 引导失败，ASA 应直接引导至 ROMMON，然后忽略指定从默认映像引导的操作。

除非另有指定，否则值 0 意味着无操作。

表 8-1 列出与每个十六进制字符关联的操作；为每个字符选择一个值：

表 8-1　配置寄存器的值

前缀	十六进制字符数 4、3、2、1 和 0				
0x	0	0	0[1]	0[2]	0
	1 在启动期间，禁用 10 秒 ROMMON 倒计时。通常，您可在倒计时过程中按 Escape 进入 ROMMON。	2 如果设置 ASA 从 TFTP 服务器引导，而此引导失败，则此值直接引导进入 ROMMON。		1 按照 ROMMON 引导参数（如果存在，与 **boot system tftp** 命令一样）中的指定，从 TFTP 服务器映像进行引导。此值优先于为字符 1 设置的值。	1 通过第一个 **boot system** *local_flash* 命令引导指定的映像。如果该映像未加载，ASA 尝试通过随后的 **boot system** 命令引导每个指定的映像，直到其引导成功。
					2、4、6、8 通过特定的 **boot system** *local_flash* 命令引导指定的映像。值 3 引导第一个 **boot system** 命令中指定的映像，值 5 引导第二个映像，等等。 如果映像未能成功引导，ASA 不能尝试恢复到其他 **boot system** 命令映像（这是使用值 1 和值 3 之间的差异）。然而，ASA 有故障保护的功能，在引导失败的情况下尝试引导在 内部闪存 的根目录中可找到的任何映像。如果您不想故障保护功能生效，请将映像保存在根目录以外的其他目录中。
				4[3] 忽略启动配置并加载默认配置。	3、5、7、9 从 ROMMON 中，如果输入不带任何参数的 **boot** 命令，则 ASA 通过特定的 **boot system** *local_flash* 命令引导指定的映像。值 3 引导第一个 **boot system** 命令中指定的映像，值 5 引导第二个映像，等等。此值不会自动引导映像。
				5 执行以上两个操作。	

1. 已保留供将来使用。
2. 如果字符数 0 和 1 未设置自动引导映像，则 ASA 直接引导至 ROMMON。
3. 如果您使用 **service password-recovery** 命令禁用密码恢复，则无法设置配置注册来忽略启动配置。

配置注册值不会复制到备用设备，但当在活动设备上设置配置注册时会显示以下警告：

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

您还可以用 **confreg** 命令在 ROMMON 中设置配置注册值。

示例

以下示例设置配置注册以从默认映像引导：

```
ciscoasa(config)# config-register 0x1
```

相关命令

命令	说明
boot	设置引导映像并启动配置。
service password-recovery	启用或禁用密码恢复。

配置出厂默认设置

要将配置恢复为出厂默认设置，请在全局配置模式下使用 **configure factory-default** 命令。

configure factory-default [*ip_address* [*mask*]]

语法说明

ip_address	设置管理或内部接口的 IP 地址，而不是使用默认地址 192.168.1.1。有关您的型号配置何种接口的详细信息，请参阅 “ 使用指南 ” 部分。
mask	设置接口的子网掩码。如果未设置掩码，ASA 将使用适用于 IP 地址类的掩码。

默认值

默认 IP 地址和掩码为 192.168.1.1 和 255.255.255.0。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	增加了 ASA 5505 出厂默认配置。

使用指南

出厂默认配置是思科对新的 ASA 应用的配置。除 PIX 525 和 PIX 535 ASA 外的所有平台均支持此命令。

对于 PIX 515/515E 和 ASA 5510 及更高版本的 ASA，出厂默认配置自动配置管理接口，使您能够用 ASDM 与其进行连接，然后通过它完成配置。对于 ASA 5505，出厂默认配置自动配置接口和 NAT，以便 ASA 准备在您的网络中使用。

此命令仅用于路由防火墙模式；透明模式不支持接口的 IP 地址，且设置接口的 IP 地址是此命令的任务之一。此命令也只适用于单情景模式；具有已清除配置的 ASA 没有任何定义的情景来使用此命令自动配置。

此命令将清除当前的运行配置，然后配置多个命令。

如果在 **configure factory-default** 命令中设置 IP 地址，则 **http** 命令使用指定的子网。同样，**dhcpd address** 命令范围包含指定的子网内的地址。

在恢复出厂默认配置后，使用 **write memory** 命令将其保存到 内部闪存 中。**write memory** 命令将运行配置保存到启动配置的默认位置，即使之前配置的 **boot config** 命令设置了不同的位置；清除配置后，路径也随之清除。

注意　此命令还将清除 **boot system** 命令（如果存在）和其他配置。**boot system** 命令允许从特定映像引导，包括 外部闪存卡 上的映像。下次恢复出厂配置后重新加载 ASA，将从 内部闪存 中的第一个映像引导；如果 内部闪存 中没有映像，ASA 将不引导。

要配置用于完整配置的其他设置，请参阅 **setup** 命令。

ASA 5505 配置

ASA 5505 的默认出厂配置如下：

- 一个包括以太网 0/1 至 0/7 交换机端口的内部 VLAN 1 接口。如果在 **configure factory-default** 命令中未设置 IP 地址，则 VLAN 1 IP 地址和掩码为 192.168.1.1 和 255.255.255.0。
- 一个包括以太网 0/0 交换机端口的外部 VLAN 2 接口。VLAN 2 使用 DHCP 生成其 IP 地址。
- 默认路由也从 DHCP 生成。
- 使用接口 PAT 访问外部时，将转换所有内部 IP 地址。
- 默认情况下，内部用户可使用访问列表访问外部，而禁止外部用户访问内部。
- 在 ASA 上启用 DHCP 服务器，所以连接到 VLAN 1 接口的 PC 接收一个 192.168.1.2 和 192.168.1.254 之间的地址。
- 为 ASDM 启用 HTTP 服务器，而且 192.168.1.0 网络上的用户可以对其进行访问。

配置由以下命令组成：

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
```

```
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 及更高配置

ASA 5510 及更高配置的默认出厂配置如下：

- 管理 Management 0/0 接口。如果在 **configure factory-default** 命令中未设置 IP 地址，则 IP 地址和掩码为 192.168.1.1 和 255.255.255.0。
- 在 ASA 上启用 DHCP 服务器，所以连接到该接口的 PC 接收一个 192.168.1.2 和 192.168.1.254 之间的地址。
- 为 ASDM 启用 HTTP 服务器，而且 192.168.1.0 网络上的用户可以对其进行访问。

配置由以下命令组成：

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E 安全设备配置

PIX 515/515E 安全设备配置的默认出厂配置如下：

- 内部 Ethernet1 接口。如果在 **configure factory-default** 命令中未设置 IP 地址，则 IP 地址和掩码为 192.168.1.1 和 255.255.255.0。
- 在 PIX 安全设备上启用 DHCP 服务器，所以连接到该接口的 PC 接收一个 192.168.1.2 和 192.168.1.254 之间的地址。
- 为 ASDM 启用 HTTP 服务器，而且 192.168.1.0 网络上的用户可以对其进行访问。

配置由以下命令组成：

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

示例

以下示例将配置重置为出厂默认配置，将 IP 地址 10.1.1.1 分配到接口，然后将新配置另存为启动配置：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
ciscoasa(config)#
ciscoasa(config)# copy running-config startup-config
```

相关命令

命令	说明
boot system	设置从何处引导软件映像。
clear configure	清除运行配置。
copy running-config startup-config	将运行配置复制到启动配置中。
setup	提示配置 ASA 的基本设置。
show running-config	显示运行的配置。

configure http

要将 HTTP(S) 服务器的配置文件与运行配置合并，请在全局配置模式下使用 **configure http** 命令。

configure http[**s**]**://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path***/**]*filename*

语法说明

:password	（可选）对于 HTTP(S) 身份验证，指定密码。
:*port*	（可选）指定端口。对于 HTTP，默认端口为 80。对于 HTTPS，默认端口为 443。
@	（可选）如果输入名称和 / 或密码，在服务器 IP 地址前使用符号 (@)。
filename	指定配置文件名。
http[**s**]	指定 HTTP 或 HTTPS。
path	（可选）指定文件名的路径。
server	指定服务器的 IP 地址或名称。对于 IPv6 服务器地址，如果指定端口，则必须将 IP 地址括在括号内，以便 IP 地址中的冒号不会被误认为端口号前的冒号。例如，输入以下地址和端口： `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（可选）对于 HTTP(S) 身份验证，指定用户名。

默认值

对于 HTTP，默认端口为 80。对于 HTTPS，默认端口为 443。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令支持 IPv4 和 IPv6 地址。合并将所有命令从新配置添加到运行配置中，并用新版本覆盖所有冲突的命令。例如，如果命令允许多个实例，则将新命令添加到运行配置中的现有命令。如果命令仅允许一个实例，则新命令将覆盖运行配置中的命令。合并不会删除运行配置中的命令，也不在新配置中设置命令。

此命令等同于 **copy http running-config** 命令。对于多情景模式，该命令只能在系统执行空间中使用，因此，**configure http** 命令是另一个在情景内使用的命令。

示例

以下示例将配置文件从 HTTPS 服务器复制到运行配置中：

```
ciscoasa(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

相关命令

命令	说明
clear configure	清除运行配置。
configure memory	将启动配置与运行配置合并。
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
configure factory-default	将在 CLI 中输入的命令添加到运行配置中。
show running-config	显示运行的配置。

configure memory

要将启动配置与运行配置合并，请在全局配置模式下使用 **configure memory** 命令。

configure memory

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

合并将所有命令从新配置添加到运行配置中，并用新版本覆盖所有冲突的命令。例如，如果命令允许多个实例，则将新命令添加到运行配置中的现有命令。如果命令仅允许一个实例，则新命令将覆盖运行配置中的命令。合并不会删除运行配置中的命令，也不在新配置中设置命令。

如果您不想合并配置，可以清除运行配置，该操作通过 ASA 中断所有通信，然后输入 **configure memory** 命令加载新的配置。

此命令等同于 **copy startup-config running-config** 命令。

对于多情景模式，情景启动由 **config-url** 命令指定的位置处的配置。

示例

以下示例将启动配置复制到运行配置中：

```
ciscoasa(config)# configure memory
```

相关命令

命令	说明
clear configure	清除运行配置。
configure http	将指定的 HTTP(S) URL 的配置文件与运行配置合并。
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
configure factory-default	将在 CLI 中输入的命令添加到运行配置中。
show running-config	显示运行的配置。

configure net

要将来自 TFTP 服务器的配置文件与运行配置合并，请在全局配置模式下使用 **configure net** 命令。

configure 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。 如果在此命令中指定文件名，并在 **tftp-server** 命令中指定一个名称，则 ASA 将 **tftp-server** 命令的文件名视为目录，并将 **configure net** 命令的文件名作为文件添加该到目录下。 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）。对于 IPv6 服务器地址，必须将 IP 地址括在括号内，以便 IP 地址中的冒号不会被误认为文件名前的冒号。例如，输入以下地址： [fe80::2e0:b6ff:fe01:3b7a] 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

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令支持 IPv4 和 IPv6 地址。合并将所有命令从新配置添加到运行配置中，并用新版本覆盖所有冲突的命令。例如，如果命令允许多个实例，则将新命令添加到运行配置中的现有命令。如果命令仅允许一个实例，则新命令将覆盖运行配置中的命令。合并不会删除运行配置中的命令，也不在新配置中设置命令。

此命令等同于 **copy tftp running-config** 命令。对于多情景模式，该命令只能在系统执行空间中使用，因此，**configure net** 命令是另一个在情景内使用的命令。

示例

以下示例在 **tftp-server** 命令中设置服务器和文件名，然后用 **configure net** 命令覆盖服务器。使用同一文件名。

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:
```

以下示例覆盖服务器和文件名。文件名的默认路径为 /tftpboot/configs/config1。默认情况下，当您不用斜杠 (/) 引领文件名时，包括路径的 /tftpboot/ 部分。由于您想覆盖此路径，而文件也在 tftpboot 中，包括 **configure net** 命令中的 tftpboot 路径。

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

以下示例仅在 **tftp-server** 命令中设置服务器。**configure net** 命令仅指定文件名。

```
ciscoasa(config)# tftp-server inside 10.1.1.1
ciscoasa(config)# configure net :configs/config1
```

相关命令

命令	说明
configure http	将指定的 HTTP(S) URL 的配置文件与运行配置合并。
configure memory	将启动配置与运行配置合并。
show running-config	显示运行的配置。
tftp-server	设置用于其他命令的默认 TFTP 服务器和路径。
write net	将运行配置复制到 TFTP 服务器。

configure terminal

要在命令行配置运行配置，请在特权 EXEC 模式下使用 **configure terminal** 命令。

configure terminal

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令进入全局配置模式，是您能够输入更改配置命令。

示例

以下示例进入全局配置模式：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

相关命令

命令	说明
clear configure	清除运行配置。
configure http	将指定的 HTTP(S) URL 的配置文件与运行配置合并。
configure memory	将启动配置与运行配置合并。
configure net	将指定的 TFTP URL 中的配置文件与运行配置合并。
show running-config	显示运行的配置。

config-url

要标识系统可从中下载情景配置的 URL，请在情景配置模式下使用 **config-url** 命令。

config-url *url*

语法说明

url	设置情景配置的 URL。所有远程 URL 必须可从管理情景中访问。参阅以下 URL 语法： • **disk0:/**[*path*/]*filename* 对于 ASA 5500 系列，此 URL 指示内部闪存。您还可用 **flash** 命令代替 **disk0** 命令；它们是别名。 • **disk1:/**[*path*/]*filename* 对于 ASA 5500 系列，此 URL 指示外部闪存卡。 • **flash:/**[*path*/]*filename* 此 URL 指示内部闪存。 • **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。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Context configuration	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当您添加情景 URL 时，系统立即加载情景以便运行。

注意　输入 **allocate-interface** 命令，然后输入 **config-url** 命令。ASA 加载情景配置前必须向情景分配接口；情景配置可能包括引用接口的命令（**interface**、**nat**、**global**）。如果先输入 **config-url** 命令，ASA 立即加载情景配置。如果情景包括任何引用接口的命令，这些命令将失败。

文件名不需要文件扩展名，但建议您使用 “.cfg”。

管理情景文件必须存储在 内部闪存 中。

如果从 HTTP 或 HTTPS 服务器下载情景配置，则无法使用 **copy running-config startup-config** 命令将更改保存回这些服务器。但可使用 **copy tftp** 命令将运行配置复制到 TFTP 服务器。

如果系统由于服务器不可用或文件不存在而无法检索情景配置文件，则系统将创建空情景以便您可以通过命令行界面配置。

要更改 URL，请重新输入带有新 URL 的 **config-url** 命令。

ASA 将新的配置与当前的运行配置合并。重新输入同一 URL 也可将已保存的配置与运行配置合并。合并将新配置中的所有新命令添加到运行配置中。如果配置是相同的，不会发生任何更改。如果命令冲突，或命令影响情景的运行，则合并的影响取决于命令。可能显示错误，也可能出现意外结果。如果运行配置为空（例如，如果服务器不可用且从未下载配置），则使用新的配置。如果您不想合并配置，可清除运行配置，该操作通过情景中断所有通信，然后从新的 URL 重新加载配置。

示例

以下示例将管理情景设置为 “administrator”，在 内部闪存 中创建名为 “administrator” 的情景，然后从 FTP 服务器添加两个情景：

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

相关命令

命令	说明
allocate-interface	将接口分配到情景。
context	在系统配置中创建安全情景并进入情景配置模式。
show context	显示情景列表（系统执行空间）或有关当前情景的信息。

conn-rebalance

要在集群成员之间启用连接再平衡，请在集群组配置模式下使用 **conn-rebalance** 命令。要禁用连接再平衡，请使用此命令的 **no** 形式。

conn-rebalance [**frequency** *seconds*]

no conn-rebalance [**frequency** *seconds*]

语法说明

frequency *seconds*	（可选）指定加载信息交换频率，介于 1 至 360 秒之间。默认值为 5 秒。

命令默认值

默认情况下，禁用连接再平衡。

如果启用，默认频率为 5 秒

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

如果上游或下游路由器的加载平衡功能导致流量分布不平衡，可配置过载设备将新流量重定向到其他设备。现有流量将不会移至其他设备。如果启用，ASA 将定期交换负载信息，并将新连接从负载较高的设备转移到负载较低的设备。

此命令并非引导程序配置的一部分，而是从主设备复制到从属设备上的。

示例

以下示例将连接再平衡频率设置为 60 秒：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。

命令	说明
cluster interface-mode	设置集群接口模式。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable（集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

console timeout

要对已经过身份验证的串行控制台会话（**AAA 身份验证串行控制台**）设置非活动超时，以便用户超时后注销登录控制台，或对已经过身份验证的启用会话（**AAA 身份验证启用控制台**）设置非活动超时，以便用户超时后退出特权 EXEC 模式并恢复为用户 EXEC 模式，请在全局配置模式下使用 **console timeout** 命令。要对已经身份验证的串行控制台会话禁用非活动超时，请使用此命令的 **no** 形式。

console timeout [*number*]

no console timeout [*number*]

语法说明

number	指定空闲时间在几分钟（0 至 60）后，控制台会话结束。0 表示控制台永不超时。

默认值

默认超时值为 0，表示控制台会话将不会超时。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

console timeout 命令仅适用于已经身份验证的串行连接或启用连接。此命令不改变 Telnet、SSH 或 HTTP 超时；这些访问方法均维持自己的超时值。此命令不影响未经身份验证的控制台连接。

no console timeout 命令将控制台超时值重置为默认超时值 0，表示控制台将不会超时。

示例

以下示例展示如何将控制台超时设置为 15 分钟：

```
ciscoasa(config)# console timeout 15
```

相关命令

命令	说明
clear configure console	恢复默认控制台连接设置。
clear configure timeout	恢复配置中的默认空闲持续时间。
show running-config console timeout	显示与 ASA 之间的控制台连接的空闲超时。

console-replicate

要启用从 ASA 集群中的从属设备到主设备的控制台复制，请在集群组配置模式下使用 **console-replicate** 命令。要禁用控制台复制，请使用此命令的 **no** 形式。

console-replicate

no console-replicate

语法说明

此命令没有任何参数或关键字。

命令默认值

默认情况下，禁用控制台复制。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

ASA 对于某些关键事件，直接打印出一些消息到控制台。如果启用控制台复制，从属设备将发送控制台消息到主设备，因此，您只需监控集群的控制台端口。

此命令并非引导程序配置的一部分，而是从主设备复制到从属设备上的。

示例

以下示例启用控制台复制：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# console-replicate
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接再平衡。

命令	说明
enable（集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

content-length

要限制基于 HTTP 消息主体长度的 HTTP 流量，请在 HTTP 映射配置模式下使用 **content-length** 命令。要删除此命令，请使用此命令的 **no** 形式。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

语法说明

action	指定此检查消息失败时执行的操作。
allow	允许消息。
bytes	指定字节数。对于 **min** 选项，允许的范围为 1 至 65535，且对于 **max** 选项，允许的范围为 1 至 50000000。
drop	关闭连接。
log	（可选）生成系统日志。
max	（可选）指定允许的最大内容长度。
min	指定允许的最小内容长度。
reset	发送 TCP 重置消息到客户端和服务器。

默认值

默认情况下禁用此命令。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

启用 **content-length** 命令后，ASA 仅允许配置范围内的消息，否则采取指定的操作。使用 **action** 关键字使 ASA 重置 TCP 连接，并且创建系统日志条目。

示例

以下示例将 HTTP 流量限制为消息 100 字节或更大，但不超过 2000 字节。如果消息超出此范围，ASA 重置 TCP 连接并创建系统日志条目。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# content-length min 100 max 2000 action reset log
ciscoasa(config-http-map)# exit
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
http-map	为配置增强型 HTTP 检查定义 HTTP 映射。
debug appfw	显示与增强型 HTTP 检查关联的流量详细信息。
inspect http	应用要用于应用检查的特定 HTTP 映射。
policy-map	将类映射与特定安全操作关联。

context

要在系统配置中创建安全情景并进入情景配置模式，请在全局配置模式下使用 **context** 命令。要删除情景，请使用此命令的 **no** 形式。

context *name*

no context *name* [**noconfirm**]

语法说明

name	将名称设置为最多包含 32 个字符的字符串。此名称区分大小写，这样，您可以使用名称分别为 “customerA” 和 “CustomerA” 的两个情景。您可以使用字母、数字或连字符，但名称的开头或结尾不能使用连字符。 “System” 或 “Null”（大写或小写字母）是保留名称，不能使用。
noconfirm	（可选）删除情景而不提示进行确认。此选项对于自动化脚本非常有用。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在情景配置模式下，可标识配置文件 URL 和情景可使用的接口。如果没有管理情景（例如，如果清除配置），则添加的第一个情景必须是管理情景。要添加管理情景，请参阅 **admin-context** 命令。指定管理情景后，可输入 **context** 命令配置管理情景。

您可通过编辑系统配置仅删除情景。使用此命令的 **no** 形式不能删除当前管理情景；只有使用 **clear configure context** 命令删除所有情景时才能删除它。

示例

以下示例将管理情景设置为 “administrator”，在 内部闪存 中创建名为 “administrator” 的情景，然后从 FTP 服务器添加两个情景：

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg
```

```
ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

相关命令

命令	说明
allocate-interface	将接口分配到情景。
changeto	在情景和系统执行空间之间更改。
config-url	指定情景配置的位置。
join-failover-group	为故障切换组分配情景。
show context	显示情景信息。

copy

要复制文件到 ASA 闪存中或从中复制文件，请在特权 EXEC 模式下使用 **copy** 命令。

copy [**/noconfirm**] [**/pcap**] [**/noverify**] {*url* | **running-config** | **startup-config**}
{**running-config** | **startup-config** | *url*}

语法说明

/noconfirm	（可选）复制文件而不提示确认。
/pcap	（可选）指定 **capture** 命令的原始数据包捕获转储。
/noverify	（可选）复制开发密钥签名的映像时使用跳过签名验证。
running-config	指定存储在系统内存中的运行配置。
startup-config	指定存储在闪存中的启动配置。单模式的启动配置或多情景模式中系统的启动配置均为闪存中的隐藏文件。在情景中，**config-url** 命令指定启动配置的位置。例如，如果为 **config-url** 命令指定 **HTTP 服务器**，然后输入 **copy startup-config running-config** 命令，ASA 使用管理情景接口从 HTTP 服务器复制启动配置。
url	指定要在本地和远程位置之间复制的源或目标文件。（您无法从远程服务器复制到另一个远程服务器。）在情景中，您可以使用情景接口将运行或启动配置复制到 TFTP 或 FTP 服务器，但无法从服务器复制到运行的或启动配置。有关其他选项，请参阅 **startup-config** 关键字。从 TFTP 服务器下载到运行情景配置，请使用 **configure net** 命令。使用此命令的以下 URL 语法： • **cache:/**[[*path*/]*filename*] - 指示文件系统中的缓存。 • **capture:/**[[*context_name*/]*buffer_name*] - 指示捕获缓冲区中的输出。 • **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*] - **flash** 和 **disk0** 指示 内部闪存。可使用任一选项。 • **disk1:/**[[*path*/]*filename*] - 指示外部内存。 • **smb:/**[[*path*/]*filename*] - 指示 UNIX 服务器本地文件系统。使用 LAN 管理器及类似的网络系统中的 Server Message Block（服务器消息块）文件系统协议包装数据并与其他系统交换信息。 • **ftp://**[[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*]] - **type** 可以是这些关键字的其中一个：**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*] • **scp://**[[*user*[**:***password*]@]*server*[**/***path*]**/***filename*[**;int=***interface_name*]] - **;int=***interface* 选项绕过路由查找，并始终使用指定的接口连接到安全复制 (SCP) 服务器。 • **system:/**[[*path*/]*filename*] - 表示系统内存。 • **tftp://**[[*user*[**:***password*]@]*server*[**:***port*]**/**[*path*/]*filename*[**;int=***interface_name*]] 路径名不能包含空格。如果路径名有空格，在 **tftp-server** 命令中而非 **copy tftp** 命令中设置路径。**;int=** *interface* 选项绕过路由查找，并始终使用指定的接口连接到 TFTP 服务器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
特权 EXEC	• 是	• 是	• 是	• 是[1]	• 是

1. 在情景中，只能将 running-config 或 startup-config 复制到外部 URL。

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	以增加对 DNS 名称的支持。
8.0(2)	增加了 **smb** 选项。
9.1(5)	增加了 **scp** 选项。
9.3(2)	增加了 **noverify** 选项。

使用指南

- 当您将配置复制到运行配置时，将合并这两个配置。合并将新配置中的所有新命令添加到运行配置中。如果配置是相同的，不会发生任何更改。如果命令冲突，或命令影响情景的运行，则合并的影响取决于命令。可能显示错误，也可能出现意外结果。
  如果 RSA 密钥无法保存到 NVRAM 中，则会显示以下错误消息：

  ```
  ERROR: NV RAM does not have enough space to save keypair keypair name
  ```

- 执行一个整个集群范围内的捕获后，您可以通过在主设备上输入以下命令，将同一个捕获文件同时从集群中的所有设备复制到 TFTP 服务器：

  ```
  hostname (config-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

  多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名自动附有设备名称，如 filename_A.pcap、filename_B.pcap，其中 A 和 B 是集群设备名称。

  注　如果在文件名末尾添加设备名称，会生成不同的目标名称。

示例

以下示例展示如何将文件从磁盘复制到系统执行空间中的 TFTP 服务器：

```
ciscoasa(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

以下示例展示如何将文件从磁盘的一个位置复制到其他位置。目标文件的名称可以是源文件的名称或其他名称。

```
ciscoasa(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

以下示例展示如何将 ASDM 文件从 TFTP 服务器复制到内部闪存：

```
ciscoasa(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

以下示例展示如何将情景中的运行配置复制到 TFTP 服务器：

```
ciscoasa(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy 命令支持此版本前面示例中所示的 DNS 名称及 IP 地址：

```
ciscoasa(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

以下示例展示输入 **copy capture** 命令而未指定完整路径时提供的提示：

```
ciscoasa(config)# copy capture:abc tftp
Address or name of remote host [209.165.200.224]?
Source file name [username/cdisk]?
copying capture to tftp://209.165.200.224/username/cdisk:
[yes|no|again]?y
!!!!!!!!!!!!!
```

您可以按如下所示指定完整的路径：

```
ciscoasa(config)# copy capture:abc tftp:209.165.200.224/tftpboot/abc.cap
```

如果已经配置了 TFTP 服务器，可以不指定位置或文件名，如下所示：

```
ciscoasa(config)# tftp-server outside 209.165.200.224 tftp/cdisk
ciscoasa(config)# copy capture:abc tftp:/tftp/abc.cap
```

以下示例展示如在不对开发密钥签名的映像不进行验证的情况下对其进行复制：

```
ciscoasa(config)# copy /noverify lfbff.SSA exa_lfbff.SSA

Source filename [lfbff.SSA]?

Destination filename [exa_lfbff.SSA]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

相关命令

命令	说明
configure net	将文件从 TFTP 服务器复制到运行配置中。
copy capture	将捕获文件复制到 TFTP 服务器。
tftp-server	设置默认 TFTP 服务器。
write memory	将运行配置保存到启动配置。
write net	将运行配置复制到 TFTP 服务器。

cpu hog granular-detection

要在短期内提供实时占用检测并设置 CPU 占用阈值，请在特权 EXEC 模式下使用 **CPU HOG granular-detection** 命令。

cpu hog granular-detection [**count** *number*] [**threshold** *value*]

语法说明

count *number*	指定已执行的代码执行中断的数量。有效值为 1 到 10000000。默认值和建议值均为 1000。
threshold *value*	范围为 1 至 100。如果未设置，则使用默认值，平台之间有所不同。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

cpu hog granular-detection 命令每隔 10 毫秒中断当前代码执行并总计中断数。CPU 占用的中断检查。如果存在，则登录。此命令可缩短数据路径中 CPU 占用检测的时间间隔。

每个基于安排的占用最多与 5 个基于中断的占用条目关联；每个条目可最多有 3 个回溯。无法覆盖基于中断的占用；如果没有空间，将丢弃新的。根据 LRU 策略仍可重用基于安排的占用，且当时会清除其关联的基于中断的占用。

注意　具有小 UDP 数据包的 ASA 5585-X 的性能可能会受到影响。

示例

以下示例展示如何触发 CPU 占用检测：

```
ciscoasa# cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer under heavy
traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

相关命令

命令	说明
show process cpu-hog	显示占用 CPU 的进程。
clear process cpu-hog	清除占用 CPU 的进程。

cpu profile activate

要启动 CPU 配置文件，请在特权 EXEC 模式下使用 **cpu profile activate** 命令。

cpu profile activate *n-samples* [**sample-process** *process-name*] [**trigger cpu-usage** *cpu %* [*process-name*]]

语法说明

n-samples	分配用于存储 *n* 采样号的内存。有效值为从 1 到 100,000。
sample-process *process-name*	仅对特定进程采样。
trigger cpu-usage *cpu %*	在全局 CPU 百分比大于 5 秒之前防止分析器启动，并且在 CPU 百分比低于此值时，停止分析器。
trigger cpu-usage *cpu % process-name*	使用进程 5 秒 CPU 百分比作为触发器。

默认值

n-samples 默认值为 1000。

cpu % 默认值为 0。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.1(2)	添加了 **sample-process** *process-name*、**trigger cpu-usage** *cpu %*、和 **trigger cpu-usage** *cpu % process-name* 选项。更新了输出格式。

使用指南

CPU 分析器可帮助您确定哪个进程正在使用 CPU。在计时器中断时，分析 CPU 可捕获已在 CPU 上运行的进程地址。无论 CPU 负载如何，每隔 10 毫秒进行此分析。例如，如果需要 5000 份采样，分析确切的需要 50 秒完成。如果 CPU 分析器使用的 CPU 时间数量相对较低，则收集采样的时间会更长。CPU 配置文件记录在单独的缓冲区进行采样。

将 **show cpu profile** 命令与 **cpu profile activate** 命令配合使用可显示可收集的信息，以及 TAC 可用于排除 CPU 问题的故障的信息。**show cpu profile dump** 命令输出是十六进制格式。

如果 CPU 分析器等待启动条件发生，**show cpu profile** 命令会显示以下输出：

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
```

```
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

示例

以下示例激活分析器并指示其存储 1000 份采样。

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

以下示例展示分析的状态（正在进行和已完成）：

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

相关命令

命令	说明
show cpu profile	显示 CPU 分析进程。
show cpu profile dump	显示不完整的或已完成的分析结果。

coredump enable

要启用核心转储功能，请输入 **coredump enable** 命令。要禁用此命令，请使用此命令的 **no** 形式。

coredump enable [**filesystem** [**disk0**: | **disk1**: | **flash**:] [**size** [**default** | **size_in_MB**]]

[**no**] **coredump enable** [**filesystem** [**disk0**: | **disk1**: | **flash**:] [**size** [**default** | **size_in_MB**]]

语法说明

default	将默认值指定为建议使用的值，因为 ASA 会计算出此值。
filesystem disk0: | disk1: | flash:	指定要保存核心转储文件的磁盘。
size	定义在 ASA 闪存中为核心转储文件系统映像分配的总大小。在配置核心转储时，如果没有足够的空间，将会出现错误消息。将 **size** 选项视为容器非常有用，这意味着不允许生成的核心转储在磁盘空间中的消耗超过此大小。
size_in_MB	（如果空间可用）指定 ASA 将覆盖的默认值并为核心转储文件系统分配以 MB 为单位的指定的值。

默认值

默认情况下，核心转储未启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

启用此功能将提供重要的故障排除信息。禁用此功能将导致在系统崩溃时不能为所有组件生成核心转储文件。此外，禁用此功能不会删除以前的核心转储文件系统映像和 / 或核心转储文件系统映像内容。当您启用核心转储时，将提示您允许创建核心转储文件系统。该提示是一个包含要创建的核心转储文件系统的大小（以 MB 单位）的确认。启用或禁用核心转储后保存配置很重要。

当启用核心转储时，将创建以下文件元素。您始终不应显式操作这些文件元素。

- coredumpfsys – 包括核心转储映像的目录
- coredumpfsysimage.bin – 用于管理核心转储的核心转储文件系统映像
- coredumpinfo – 包括核心转储日志的目录

注意　禁用核心转储不会影响 crashinfo 文件生成。

思科 TAC 可能要求您启用核心转储功能来故障排除 ASA 的应用或系统崩溃。

注意 确保您存档了核心转储文件，因为后续核心转储可能导致删除以前的核心转储来适应当前的核心转储。核心转储文件位于已配置的文件系统中（例如，“disk0:/coredumpfsys” 或 “disk1:/coredumpfsys”），并可从 ASA 中删除。

要启用核心转储，请执行下列操作：

1. 确保处于 /root 目录中。要验证目录所处控制台的位置，请输入 **pwd** 命令。
2. 如果需要，通过输入 **cd disk0:/**、**cd disk1:/** 或 **cd flash:/** 命令更改目录。
3. 输入 **coredump enable** 命令。

当使用 **coredump** 命令对 ASA 的崩溃故障排除时，崩溃后可能不保存核心转储文件。当已启用核心转储功能并创建了带有预分配磁盘空间的核心转储文件系统时，可能出现此情况。对已分配大量 RAM 的 ASA 繁忙工作数周后出现崩溃进行故障排除时，通常出现这种情况。

在 **show coredump** 命令输出中，将显示与以下类似的内容：

```
Coredump Aborted as the complete coredump could not be written to flash
   Filesystem full on 'disk0', current coredump size <size> bytes too big for allocated
   filesystem
```

要解决此问题，您需要有足够大的核心转储文件系统卡，可包含所有内存并为核心转储文件系统分配相应的空间。

示例

这些示例中的每个感叹号 (!) 表示已写入 1 MB 的核心转储文件系统。

以下示例使用默认值和 **disk0:** 创建核心转储文件系统。

```
hostname(config)# coredump enable
Warning: Enabling coredump on an ASA5505 platform will delay the reload of the system in
the event of software forced reload.The exact time depends on the size of the coredump
generated.
Proceed with coredump filesystem allocation of 60 MB on 'disk0:' (Note this may take a
while) [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

以下示例展示如何通过在 **disk1:** 上创建一个 120 MB 的核心转储文件系统指定文件系统和大小：

```
hostname(config)# coredump enable filesystem disk1: size 120
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 120 MB
on 'disk1:' (Note this may take a while) ?[confirm]
Making coredump file system image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

以下示例展示如何将核心转储文件系统的大小从 120 MB 调整到 100 MB：

注意 不保留 120 MB 核心转储文件系统的内容，因此，请确保在执行此操作前存储以前的核心转储。

```
hostname(config)# coredump enable filesystem disk1: size 100
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
```

```
The exact time depends on the size of the coredump generated.
Proceeding with resizing to 100 MB results in
deletion of current 120 MB coredump filesystem and
its contents on 'disk1:', proceed ?[confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

以下示例最初在 **disk0:** 上启用核心转储，然后在 **disk1:** 上启用。另请注意 **default** 关键字的使用。

> **注意** 我们不允许两个活动的核心转储文件系统，因此，您必须删除以前的核心转储文件系统才能继续。

```
hostname(config)# coredump enable filesystem disk1: size default
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Coredump is currently configured on 'disk0:', upon successful
configuration on 'disk1:', the coredump filesystem will be
deleted on 'disk0:', proceed ?[confirm]
Proceed with coredump filesystem allocation of 100 MB
on 'disk1:' (Note this may take a while) ?[confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

以下示例展示如何禁用核心转储文件系统。但当前核心转储文件系统映像及其内容不受影响。

```
hostname(config)# no coredump enable
```

要重新启用核心转储，请重新输入您最初用于配置核心转储文件系统的命令。

以下示例禁用并重新启用核心转储：

- 使用默认值：

```
hostname(config)# coredump enable
hostname(config)# no coredump enable
hostname(config)# coredump enable
```

- 使用显式值：

```
hostname(config)# coredump enable filesystem disk1: size 200
hostname(config)# no coredump enable
hostname(config)# coredump enable filesystem disk1: size 200
```

相关命令

命令	说明
clear configure coredump	从系统中删除核心转储文件系统及其内容。同时清除核心转储日志。
clear coredump	删除当前存储在核心转储文件系统的所有核心转储并清除核心转储日志。
show coredump filesystem	显示核心转储文件系统上的文件并指示其充满程度。
show coredump log	显示核心转储日志。

crashinfo console disable

要抑制崩溃信息输出到控制台，请在全局配置模式下使用 **crashinfo console disable** 命令。

crashinfo console disable

no crashinfo console disable

语法说明

disable	在崩溃事件中抑制控制台输出。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

此命令是您能够抑制崩溃信息输出到控制台。崩溃信息可能包含不太适合连接到该设备的所有用户查看的敏感信息。使用此命令时，您还应确保崩溃信息已写入闪存，可在设备重新启动后进行检查。此命令影响崩溃信息和校验堆的输出，这些信息应保存到闪存中并足以满足故障排除的需要。

示例

以下示例展示如何抑制崩溃信息输出到控制台：

```
hostname(config)# crashinfo console disable
```

相关命令

命令	说明
clear configure fips	清除 NVRAM 中存储的系统或模块 FIPS 配置信息。
fips enable	启用或禁用策略检查以在系统或模块上实施 FIPS 合规性。
fips self-test poweron	执行加电自检。
show crashinfo console	读、写和配置崩溃信息输出到闪存。
show running-config fips	显示在 ASA 上运行的 FIPS 配置。

crashinfo force

要强制 ASA 崩溃，请在特权 EXEC 模式下使用 **crashinfo force** 命令。

crashinfo force [**page-fault** | **watchdog**]

语法说明

page-fault	（可选）在页面出错时强制 ASA 崩溃。
watchdog	（可选）在出现某种监视结果时强制 ASA 崩溃。

默认值

ASA 默认情况下将崩溃信息文件保存到闪存。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以使用 **crashinfo force** 命令测试崩溃输出生成。在故障输出时，实际崩溃与 **crashinfo force page-fault** 或 **crashinfo force watchdog** 命令导致的崩溃没有任何不同（因为这些都是真实的崩溃）。ASA 将在崩溃转储完成后重新加载。

注意事项　请勿在生产环境中使用 **crashinfo force** 命令。**crashinfo force** 命令使 ASA 崩溃并强制其重新加载。

示例

以下示例展示输入 **crashinfo force page-fault** 命令时显示的警告：

```
ciscoasa# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
   Do you wish to proceed?[confirm]:
```

如果输入回车（按键盘上的 Return 或 Enter 键）、“Y” 或 “y”，ASA 崩溃并重新加载；这些响应均被解释为确认。将任何其他字符解释为否，ASA 返回命令行提示。

相关命令

clear crashinfo	清除崩溃信息文件的内容。
crashinfo save disable	禁止故障信息写入到闪存。
crashinfo test	测试 ASA 将故障信息保存到闪存中文件的能力。
show crashinfo	显示崩溃信息文件的内容。

crashinfo save disable

要禁止崩溃信息写入闪存，请在全局配置模式下使用 **crashinfo save** 命令。要允许崩溃信息写入闪存并返回默认行为，请使用此命令的 **no** 形式。

crashinfo save disable

no crashinfo save disable

语法说明

此命令没有任何参数或关键字。

默认值

ASA 默认情况下将崩溃信息文件保存到闪存。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	弃用了 **crashinfo save enable** 命令。使用 **no crashinfo save disable** 命令代替。

使用指南

崩溃信息先写入闪存，然后写入控制台。

注意 如果 ASA 在启动过程中崩溃，则不保存崩溃信息文件。ASA 必须完全初始化并首先运行，才能将崩溃信息保存到闪存。

使用 **no crashinfo save disable** 命令重新启用将崩溃信息保存到闪存。

示例

以下示例展示如何禁止崩溃信息写入闪存：

```
ciscoasa(config)# crashinfo save disable
```

相关命令

clear crashinfo	清除崩溃文件的内容。
crashinfo force	强制 ASA 出现故障。
crashinfo test	测试 ASA 将故障信息保存到闪存中文件的能力。
show crashinfo	显示崩溃文件的内容。

crashinfo test

要测试 ASA 将崩溃信息保存到闪存中的文件的功能，请在特权 EXEC 模式下使用 **crashinfo test** 命令。

crashinfo test

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果以前的崩溃信息文件已存在于闪存中，则覆盖该文件。

注意 输入 **crashinfo test** 命令不会使 ASA 崩溃。

示例

以下示例展示崩溃信息文件测试的输出：

```
ciscoasa# crashinfo test
```

相关命令

clear crashinfo	删除崩溃文件的内容。
crashinfo force	强制 ASA 崩溃。
crashinfo save disable	禁止故障信息写入到闪存。
show crashinfo	显示崩溃文件的内容。

crl

要指定 CRL 配置选项，请在 crypto ca trustpoint 配置模式下使用 **crl** 命令。

crl {**required** | **optional** | **nocheck**}

语法说明

nocheck	指示 ASA 不执行 CRL 检查。
optional	ASA 仍可接受对等证书（如果所需的 CRL 不可用）。
required	所需的 CRL 必须可用于对等证书才能验证。

默认值

默认值为 **nocheck**。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Crypto ca trustpoint 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。以下形式的 **revocation-check** 命令代替它。 • **revocation-check crl none** 替换 **crl optional** • **revocation-check crl** 替换 **crl required** • **revocation-check none** 替换 **crl nocheck**

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并要求为此信任点验证 CRL 可用于对等证书：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl required
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
clear configure crypto ca trustpoint	删除所有信任点。
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。
crl configure	进入 crl 配置模式。
url	为 CRL 检索指定 URL。

crl cache-time

要配置信任池 CRL 在 ASA 刷新前可在 CRL 缓存中保留的时间（分钟），请在 ca-trustpool 配置模式下使用 **crl cache-time** 命令。要接受默认值 60 分钟，请使用此命令的 **no** 形式。

crl cache-time

no crl cache-time

语法说明

cache-time	以分钟为单位的值（1 至 1440 分钟）。

默认值

默认值为 **60** 分钟。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 信任池配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令与信任点配置模式中支持的此命令版本一致。

示例

```
ciscoasa(ca-trustpool)# crl cache-time 30
```

相关命令

命令	说明
crl enforcenextupdate	指定如何处理 NextUpdate CRL 字段。

crl configure

要进入 CRL 配置模式，请在 crypto ca trustpoint 配置模式下使用 **crl configure** 命令。

crl configure

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 CRL 配置模式：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)#
```

crl enforcenextupdate

要指定如何处理 NextUpdate CRL 字段，请在 ca-trustpool 配置模式下使用 **crl enforcenextupdate** 命令。如果已启用，则 CRL 需要有尚未失效的 NextUpdate 字段。若不执行此限制，请使用此命令的 **no** 形式：

crl enforcenextupdate

no crl enforcenextupdate

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 信任池配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

如果已启用，则 CRL 需要有尚未过时的 NextUpdate 字段。此命令与信任点配置模式中支持的此命令版本一致。

相关命令

命令	说明
crl cache-time	配置 ASA 刷新前 CRL 可在 CRL 缓存中保留的时间。

crypto am-disable 至 crypto ipsec ikev1 transform-set mode transport 命令

crypto am-disable

要禁用 IPsec IKEv1 入站积极模式连接，请在全局配置模式下使用 **crypto ikev1 am-disable** 命令。要启用入站挑战模式连接，请使用此命令的 **no** 形式。

crypto ikev1 am-disable

no crypto ikev1 am-disable

语法说明

此命令没有任何参数或关键字。

默认值

默认值为启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp am-disable** 命令。
7.2.(1)	**crypto isakmp am-disable** 命令取代了 **isakmp am-disable** 命令。
8.4(1)	命令名称从 **crypto isakmpam-disable** 更改为 **crypto ikev1 am-disable**。

示例

以下示例在全局配置模式下输入，禁用入站挑战模式连接：

```
ciscoasa(config)# crypto ikev1 am-disable
```

相关命令

命令	说明
clear configure crypto isakmp	清除 ISAKMP 配置。
clear configure crypto isakmp policy	清除 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示活动配置。

crypto ca authenticate

要安装与信任点关联的 CA 证书并对其进行身份验证，请在全局配置模式下使用 **crypto ca authenticate** 命令。要删除 CA 证书，请使用此命令的 **no** 形式。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive**]

no crypto ca authenticate *trustpoint*

语法说明

fingerprint	指定包含 ASA 用来对 CA 证书进行身份验证的字母数字字符的哈希值。如果提供了指纹，则 ASA 将该指纹与 CA 证书的计算指纹进行比较，并且仅当这两个值匹配时才接受该证书。如果没有指纹，ASA 将显示计算指纹并且询问是否接受该证书。
hexvalue	标识指纹的十六进制值。
nointeractive	使用 nointeractive 模式获得此信任点的 CA 证书；仅供设备管理器使用。在这种情况下，如果没有指纹，ASA 毫无疑问会接受该证书。
trustpoint	指定从其获得 CA 证书的信任点。最大名称长度为 128 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令

使用指南

如果为 SCEP 注册配置了信任点，则通过 SCEP 下载 CA 证书。否则，ASA 提示您将 base-64 格式的 CA 证书粘贴到终端。

此命令的调用不会成为正在运行的配置的一部分。

示例

以下示例展示 ASA 请求 CA 的证书。CA 发送其证书并且 ASA 提示管理员通过检查 CA 证书指纹验证 CA 的证书。ASA 管理员应确认指纹值显示为已知的正确值。如果 ASA 显示的指纹与正确值匹配，您应该接受证书为有效证书。

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate?[yes/no] y#
ciscoasa(config)#
```

以下示例展示为基于终端的注册（手动）配置的信任点 tp9。ASA 提示管理员将 CA 证书粘贴到终端。在显示证书的指纹后，ASA 会提示管理员确认保留证书。

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate?[yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca enroll	开始使用 CA 进行注册。
crypto ca import certificate	安装从 CA 收到的证书以响应手动注册请求。
crypto ca trustpoint	进入指定信任点的加密 CA 信任点配置模式。

crypto ca certificate chain

要进入指定信任点的证书链配置模式，请在全局配置模式下使用 **crypto ca certificate chain** 命令。

crypto ca certificate chain *trustpoint*

语法说明

trustpoint	指定用于配置证书链的信任点。

默认值

无默认值或行为。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的证书链配置模式：

```
ciscoasa(config)# crypto ca certificate chain central
ciscoasa(config-cert-chain)#
```

相关命令

命令	说明
clear configure crypto ca trustpoint	删除所有信任点。

crypto ca certificate map

要维护证书映射规则的优先级列表，请在全局配置模式下使用 **crypto ca certificate map** 命令。要删除加密 CA 配置映射规则，请使用此命令的 **no** 形式。

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

语法说明

map-name	指定证书到组映射的名称。
sequence-number	为您正创建的证书映射规则指定编号。范围为 1 到 65535。您可以在创建隧道组映射时使用此编号，从而将一个隧道组映射到一个证书映射规则。

默认值

map-name 的默认值为 DefaultCertificateMap。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	添加了 *map-name* 选项。

使用指南

输入此命令会将 ASA 置于 CA 证书映射配置模式，在这种模式下，您可以基于证书的颁发者和主题可分辨名称 (DN) 配置规则。序列号对映射规则进行排序。这些规则的通用格式如下：

- *DN match-criteria match-value*
- *DN* 为 *subject-name* 或 *issuer-name*。DN 在 ITU-T X.509 标准中进行定义。
- *match-criteria* 包括以下表达式或运算符：

attr *tag*	限制只能与特定 DN 属性进行比较，例如公用名称 (CN)。
co	包含
eq	平等
nc	不包含
ne	不等于

DN 匹配表达式不区分大小写。

示例

以下示例使用名为 example-map 的映射和序列号 1（规则 # 1）进入 CA 证书映射模式，并且指定 subject-name 的公用名称 (CN) 属性必须与示例 1 匹配：

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

以下示例使用名为 example-map 的映射和序列号 1 进入 CA 证书映射模式，并且指定其中任何位置的 subject-name 包含值 cisco：

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

相关命令

命令	说明
issuer-name	表示规则条目应用于 IPsec 对等设备证书的颁发者 DN。
subject-name (crypto ca certificate map)	表示规则条目应用于 IPsec 对等设备证书的主题 DN。
tunnel-group-map enable	将使用 **crypto ca certificate map** 命令创建的证书映射条目与隧道组关联起来。

crypto ca crl request

要根据指定信任点的配置参数请求 CRL，请在加密 CA 信任点配置模式下使用 **crypto ca crl request** 命令。

crypto ca crl request *trustpoint*

语法说明

trustpoint	指定信任点。允许的最大字符数为 128。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的调用不会成为正在运行的配置的一部分。

示例

以下示例基于名为 central 的信任点请求 CRL：

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

相关命令

命令	说明
crl configure	进入 crl 配置模式。

crypto ca enroll

要开始向 CA 进行注册的流程，请在全局配置模式下使用 **crypto ca enroll** 命令。

crypto ca enroll *trustpoint* [**noconfirm**]

语法说明

noconfirm	（可选）抑制所有提示。可能会提示的注册选项必须在信任点中预先配置。此选项可用在脚本、ASDM 中，或用于其他非交互性需求。
trustpoint	指定要注册的信任点的名称。允许的最大字符数为 128。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当信任点为 SCEP 注册而配置时，ASA 立即显示 CLI 提示并且状态消息异步显示在控制台上。当信任点为手动注册而配置时，ASA 将 base-64 编码的 PKCS10 证书请求写入控制台，之后将显示 CLI 提示符。

此命令会生成不同的交互式提示，具体取决于引用的信任点的配置状态。为使此命令成功运行，信任点必须正确配置。

示例

以下示例使用信任点 tp1（使用 SCEP 注册）请求身份证书的注册信任。ASA 提示输入信任点配置中没有存储的信息。

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password.You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name?[yes/no]: no
% Include an IP address in the subject name?[no]: no
Request certificate from CA [yes/no]: yes
```

```
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

ciscoasa(config)#
```

以下示例展示 CA 证书的手动注册：

```
ciscoasa(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name?[yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name?[no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal?[yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request?[yes/no]: no
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca authenticate	获取此信任点的 CA 证书。
crypto ca import pkcs12	安装从 CA 收到的证书以响应手动注册请求。
crypto ca trustpoint	进入指定信任点的加密 CA 信任点配置模式。

crypto ca export

要以 PKCS12 格式导出 ASA 信任点配置及所有相关密钥和证书，或以 PEM 格式导出设备身份证书，请在全局配置模式下使用 **crypto ca export** 命令。

crypto ca export *trustpoint* **identity-certificate**

语法说明

identity-certificate	指定与指定的信任点关联的已注册证书将显示在控制台上。
trustpoint	指定将显示其证书的信任点的名称。信任点名称所允许的最大字符数为 128。

默认值

无默认值或行为。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	此命令已更改为支持以 PEM 格式导出证书。

使用指南

此命令的调用不会成为活动配置的一部分。PEM 或 PKCS12 数据被写入控制台。

Web 浏览器使用 PKCS12 格式存储专用密钥，附带的公共密钥证书通过基于密码的对称密钥保护。ASA 以 base64 编码 PKCS12 格式导出与信任点关联的证书和密钥。此功能可用于在 ASA 之间移动证书和密钥。

证书的 PEM 编码是 PEM 报头中包含的 X.509 证书的 base64 编码。这种编码为 ASA 之间基于文本的证书传输提供了一种标准方法。当 ASA 充当客户端时， PEM 编码可用于导出使用 SSL/TLS 协议代理的 *proxy-ldc-issuer* 证书。

示例

以下示例将信任点 222 的 PEM 格式证书作为控制台显示来导出：

```
ciscoasa (config)# crypto ca export 222 identity-certificate

Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
```

```
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
ciscoasa (config)#
```

相关命令

命令	说明
crypto ca authenticate	获取此信任点的 CA 证书。
crypto ca enroll	开始使用 CA 进行注册。
crypto ca import	安装从 CA 收到的证书以响应手动注册请求。
crypto ca trustpoint	进入指定信任点的加密 CA 信任点配置模式。

crypto ca import

要安装从 CA 接收的证书以响应手动注册请求或导入使用 PKCS12 数据的信任点的证书和密钥对，请在全局配置模式下使用 **crypto ca import** 命令。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

语法说明

certificate	告知 ASA 从信任点表示的 CA 导入证书。
nointeractive	（可选）使用 nointeractive 模式导入证书，这会抑制所有提示。此选项可用在脚本、ASDM 中，或用于其他非交互性需求。
passphrase	指定用于解密 PKCS12 数据的口令。
pkcs12	告知 ASA 使用 PKCS12 格式导入信任点的证书和密钥对。
trustpoint	指定关联导入操作的信任点。允许的最大字符数为 128。如果您导入 PKCS12 数据并且信任点使用 RSA 密钥，则为导入的密钥对分配的名称与信任点相同。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例手动导入信任点 Main 的证书：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
ciscoasa (config)#
```

以下示例将 PKCS12 数据手动导入到信任点 central：

```
ciscoasa (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
ciscoasa (config)#
```

以下示例在全局配置模式下输入，因 NVRAM 中没有足够的空间保存 RSA 密钥对而生成一条警告消息。

```
ciscoasa(config)# crypto ca import central pkcs12 mod 2048
INFO: The name for the keys will be: central
Keypair generation process begin.Please wait...
NV RAM will not have enough space to save keypair central.Remove any unnecessary keypairs
and save the running config before using this keypair.
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca export	以 PKCS12 格式导出信任点证书和密钥对。
crypto ca authenticate	获取信任点的 CA 证书。
crypto ca enroll	开始使用 CA 进行注册。
crypto ca trustpoint	进入指定信任点的加密 CA 信任点配置模式。

crypto ca server

要设置和管理 ASA 上的本地 CA 服务器，请在全局配置模式下使用 **crypto ca server** 命令。要从 ASA 删除已配置的本地 CA 服务器，请使用此命令的 **no** 形式。

crypto ca server

no crypto ca server

语法说明

此命令没有任何参数或关键字。

默认值

在 ASA 上未启用证书颁发机构服务器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 ASA 上只能存在一个本地 CA。

crypto ca server 命令配置 CA 服务器，但不启用它。在 CA 服务器配置模式下使用 **shutdown** 命令的 **no** 形式可启用本地 CA。

当使用 **no shutdown** 命令激活 CA 服务器时，您可以建立 CA 的 RSA 密钥对和名为 LOCAL-CA-SERVER 的信任点以持有自签证书。这张新生成的自签证书始终已设置数字签名、CRL 签名和证书签名密钥使用设置。

注意事项

无论本地 CA 服务器的当前状态如何，**crypto ca server** 命令都会删除已配置的本地 CA 服务器、其 RSA 密钥对和关联的信任点。

示例

以下示例进入 CA 服务器配置模式，然后列出在该模式下可用的本地 CA 服务器命令。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
```

```
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

以下示例在 CA 服务器配置模式下使用 **crypto ca server** 命令的 **no** 形式，以删除 ASA 上已配置和启用的 CA 服务器。

```
ciscoasa(config-ca-server)# no crypto ca server

Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

相关命令

命令	说明
debug crypto ca server	显示您配置本地 CA 服务器时的调试消息。
show crypto ca server	显示已配置的 CA 服务器的状态和参数。
show crypto ca server cert-db	显示本地 CA 服务器证书。

crypto ca server crl issue

要强制签发证书撤销列表 (CRL)，请在特权 EXEC 模式下使用 **crypto ca server crl issue** 命令。

crypto ca server crl issue

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用此命令可恢复丢失的 CRL。通常，CRL 在到期时通过重新对现有 CRL 进行签名而重新签发。**crypto ca server crl issue** 命令基于证书数据库重新生成 CRL，并且仅应根据需要基于证书数据库内容重新生成。

示例

以下示例由本地 CA 服务器强制签发 CRL：

```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
cdp-url	指定要包括在 CA 颁发的证书中的证书撤销列表分发点。
crypto ca server	提供 CA 服务器配置模式命令集的访问权限，从而允许您配置和管理本地 CA。
crypto ca server revoke	将本地 CA 服务器颁发的证书标记为在证书数据库和 CRL 中撤销。
show crypto ca server crl	显示本地 CA 的当前 CRL。

crypto ca server revoke

要将本地证书颁发机构 (CA) 服务器颁发的证书标记为在证书数据库和 CRL 中撤销，请在特权 EXEC 模式下使用 **crypto ca server revoke** 命令。

crypto ca server revoke *cert-serial-no*

语法说明

cert-serial-no	指定要撤销的证书的序列号，必须采用十六进制格式。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

您可以通过在 ASA 上输入 **crypto ca server revoke** 命令撤销 ASA 上的本地 CA 颁发的特定证书。当此命令将证书标记为在 CA 服务器上的证书数据库和 CRL 中撤销时，即完成撤销。您可以通过输入十六进制格式的证书序列号指定要撤销的证书。

指定的证书撤销后，会自动重新生成 CRL。

示例

以下示例撤销本地 CA 服务器颁发的序列号为 782ea09f 的证书：

```
ciscoasa(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked.A new CRL has been issued.
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server crl issue	强制签发 CRL。
crypto ca server unrevoke	解除撤销本地 CA 服务器颁发的已撤销证书。
crypto ca server user-db remove	从 CA 服务器用户数据库删除用户。

命令	说明
show crypto ca server crl	显示本地 CA 的当前 CRL。
show crypto ca server user-db	显示包括在 CA 服务器用户数据库中的用户。

crypto ca server unrevoke

要解除撤销本地 CA 服务器颁发的已撤销证书，请在特权 EXEC 模式下使用 **crypto ca server unrevoke** 命令。

crypto ca server unrevoke *cert-serial-no*

语法说明

cert-serial-no	指定要解除撤销的证书的序列号，该序列号必须采用十六进制格式。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

您可以通过输入 ASA**crypto ca server unrevoke** 命令解除撤销本地 CA 颁发且已撤销的证书。当此命令在证书数据库中将证书标记为有效时，该证书的有效性即恢复。您可以通过输入十六进制格式的证书序列号指定要解除撤销的证书。

指定证书解除撤销后，会重新生成 CRL。

示例

以下示例解除撤销本地 CA 服务器颁发的序列号为 782ea09f 的证书：

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked.A new CRL has been
issued.
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供 CA 服务器配置模式命令集的访问权限，从而允许您配置和管理本地 CA。
crypto ca server crl issue	强制签发 CRL。

命令	说明
crypto ca server revoke	将本地 CA 服务器颁发的证书标记为在证书数据库和 CRL 中撤销。
crypto ca server user-db add	将用户添加到 CA 服务器用户数据库。
show crypto ca server cert-db	显示本地 CA 服务器证书。
show crypto ca server user-db	显示包括在 CA 服务器用户数据库中的用户。

crypto ca server user-db add

要将新用户插入到 CA 服务器用户数据库，请在特权 EXEC 模式下使用 **crypto ca server user-db add** 命令。

crypto ca server user-db add *user* [**dn** *dn*] [**email** *e-mail-address*]

语法说明

dn *dn*	为向已添加用户颁发的证书指定 subject-name 可分辨名称。如果 DN 字符串包含空格，请用双引号将值括起来。您只能使用逗号分隔 DN 属性（例如，"OU=Service, O=Company, Inc."）。
email *e-mail-address*	指定新用户的邮件地址。
user	指定向其授予注册权限的单个用户。username 可以是简单的用户名或邮件地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

user 参数可以是简单的用户名（例如 user1）或邮件地址（例如 user1@example.com）。*username* 必须与注册页面中最终用户指定的用户名匹配。

username 作为没有权限的用户添加到数据库。您必须使用 **crypto ca server allow** 命令授予注册权限。

username 参数与一次性密码一起使用，用于在注册接口页面上注册用户。

注意　对于一次性密码 (OTP) 的邮件通知，应在 *username* 或 *email-address* 参数中指定邮件地址。因在发送邮件时缺少邮件地址产生错误。

email *e-mail-address* 关键字参数对仅作为邮件地址来通知用户进行注册和续约提醒，不会出现在颁发的证书中。

包括邮件地址可确保有任何问题时可以联系到用户并在注册时向用户通知所需的一次性密码。

如果没有为用户指定可选 DN，主题名称 DN 采用 *username* 的形式，并且主题名称默认 DN 设置为 cn=*username*、subject-name-default。

示例

以下示例以 user1@example.com 用户名和完整的主题名称 DN 将用户添加到用户数据库：

```
ciscoasa(config-ca-server)# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
ciscoasa(config-ca-server)#
```

以下示例将注册权限授予名为 user2 的用户。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user2
ciscoasa(config-ca-server)
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令集的访问，从而允许您配置和管理本地 CA。
crypto ca server user-db allow	允许 CA 服务器数据库中特定用户或用户子集向 CA 注册。
crypto ca server user-db remove	从 CA 服务器数据库删除用户。
crypto ca server user-db write	将 CA 服务器数据库中的用户信息复制到 **database path** 命令指定的文件。
database path	指定本地 CA 数据库的路径或位置。默认位置是闪存。

crypto ca server user-db allow

要允许某个用户或一组用户在本地 CA 服务器数据库中注册，请在特权 EXEC 模式下使用 **crypto ca server user-db allow** 命令。此命令还包括生成并显示一次性密码或通过邮件将其发送给用户的选项。

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]

语法说明

all-certholders	指定将注册权限授予数据库中已颁发证书（不论证书是否有效）的所有用户。这与授予续订权限类似。
all-unenrolled	指定将注册权限授予数据库中尚未颁发证书的所有用户。
email-otp	（可选）将一次性密码通过邮件发送给指定用户的已配置邮件地址。
replace-otp	（可选）指定为最初具有有效一次性密码的所有指定用户重新生成一次性密码。
display-otp	（可选）在控制台上显示所有指定用户的一次性密码。
username	指定向其授予注册权限的单个用户。username 可以是简单的用户名或邮件地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

replace-otp 关键字生成所有指定用户的 OTP。这些新的 OTP 取代为指定用户生成的任何有效 OTP。

在进行注册时，OTP 不存储在 ASA 上，而会根据需要生成和重新生成以通知用户或对用户进行身份验证。

示例

以下示例将注册权限授予数据库中尚未注册的所有用户：

```
ciscoasa(config-ca-server)# crypto ca server user-db allow all-unenrolled
ciscoasa(config-ca-server)#
```

以下示例将注册权限授予名为 user1 的用户：

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user1
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令集的访问，从而允许您配置和管理本地 CA。
crypto ca server user-db add	将用户添加到 CA 服务器用户数据库。
crypto ca server user-db write	将 CA 服务器数据库中的用户信息复制到 **database path** 命令指定的文件。
enrollment-retrieval	指定注册用户可以检索 PKCS12 注册文件的时间（以小时为单位）。
show crypto ca server cert-db	显示本地 CA 颁发的所有证书。

crypto ca server user-db email-otp

要将 OTP 通过邮件发送给本地 CA 服务器数据库中特定的用户或用户子集，请在特权 EXEC 模式下使用 **crypto ca server user-db email-otp** 命令。

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

语法说明

all-certholders	指定 OTP 通过邮件发送给数据库中已颁发证书（无论该证书是否有效）的所有用户。
all-unenrolled	指定 OTP 通过邮件发送给数据库中从未颁发证书或者只持有过期或已撤销证书的所有用户。
username	指定单个用户的 OTP 通过邮件发送给该用户。username 可以是用户名或邮件地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例通过邮件将 OTP 发送给数据库中所有未注册的用户：

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
ciscoasa(config-ca-server)#
```

以下示例通过邮件将 OTP 发送给名为 user1 的用户：

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp user1
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server user-db show-otp	显示 CA 服务器数据库中特定的用户或用户子集的一次性密码。
show crypto ca server cert-db	显示本地 CA 颁发的所有证书。
show crypto ca server user-db	显示包括在 CA 服务器用户数据库中的用户。

crypto ca server user-db remove

要从本地 CA 服务器用户数据库删除用户，请在特权 EXEC 模式下使用 **crypto ca server user-db remove** 命令。

crypto ca server user-db remove *username*

语法说明

username	以用户名或邮件地址的形式指定要删除的用户的用户名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

此命令从 CA 用户数据库删除用户名，从而使用户无法注册。此命令还提供撤销之前颁发的有效证书的选项。

示例

以下示例从 CA 服务器用户数据库删除用户名为 user1 的用户：

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked.Certificates issued to user user1
should be revoked if necessary.

ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server crl issue	强制签发 CRL。
crypto ca server revoke	将本地 CA 服务器颁发的证书标记为在证书数据库和 CRL 中撤销。
show crypto ca server user-db	显示包括在 CA 服务器用户数据库中的用户。
crypto ca server user-db write	将本地 CA 数据库中配置的用户信息写入 **database path** 命令指定的文件。

crypto ca server user-db show-otp

要显示本地 CA 服务器数据库中特定的用户或用户子集的 OTP，请在特权 EXEC 模式下使用 **crypto ca server user-db show-otp** 命令。

crypto ca server user-db show-otp {*username* | **all-certholders** | **all-unenrolled**}

语法说明

all-certholders	显示数据库中已颁发证书（无论该证书当前是否有效）的所有用户的 OTP。
all-unenrolled	显示数据库中从未颁发证书或者只持有过期或已撤销证书的所有用户的 OTP。
username	指定显示单个用户的 OTP。*username* 可以是用户名或邮件地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例展示数据库中持有有效或无效证书的所有用户的 OTP：

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp all-certholders
ciscoasa(config-ca-server)#
```

以下示例展示用户名为 user1 的用户的 OTP：

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp user1
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server user-db add	将用户添加到 CA 服务器用户数据库。
crypto ca server user-db allow	允许 CA 服务器数据库中特定的用户或用户子集向本地 CA 注册。
crypto ca server user-db email-otp	通过邮件将一次性密码发送给 CA 服务器数据库中特定的用户或用户子集。
show crypto ca server cert-db	显示本地 CA 颁发的所有证书。

crypto ca server user-db write

要配置一个目录位置存储所有本地 CA 数据库文件，请在特权 EXEC 模式下使用 **crypto ca server user-db write** 命令。

crypto ca server user-db write

语法说明

此命令没有关键字或参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 服务器配置	• 是	—	• 是	—	—
全局配置	• 是	—	• 是	—	—
特权 EXEC	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

crypto ca server user-db write 命令用于将新的基于用户的配置数据保存到数据库路径配置指定的存储中。当使用 **crypto ca server user-db add** 和 **crypto ca server user-db allow** 命令添加或允许新用户时，生成该信息。

示例

以下示例将本地 CA 数据库中配置的用户信息写入存储：

```
ciscoasa(config-ca-server)# crypto ca server user-db write
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server user-db add	将用户添加到 CA 服务器用户数据库。
database path	指定本地 CA 数据库的路径或位置。默认位置是闪存。
crypto ca server user-db remove	从 CA 服务器用户数据库删除用户。

命令	说明
show crypto ca server cert-db	显示本地 CA 颁发的所有证书。
show crypto ca server user-db	显示包括在 CA 服务器用户数据库中的用户。

crypto ca trustpoint

要进入指定信任点的加密 CA 信任点配置模式，请在全局配置模式下使用 **crypto ca trustpoint** 命令。要删除指定的信任点，请使用此命令的 **no** 形式。

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

语法说明

noconfirm	抑制所有交互式提示
ipsec	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。
trustpoint-name	标识要管理的信任点的名称。允许的最大名称长度为 128 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	增加了支持 OCSP 的选项。其中包括 **match certificate map**、**ocsp disable-nonce**、**ocsp url** 和 **revocation-check**。
8.0(2)	增加了支持证书验证的选项。其中包括 **id-usage** 和 **validation-policy**。以下项被弃用：**accept-subordinates**、**id-cert-issuer** 和 **support-user-cert-validation**。
8.0(4)	增加了 **self** 选项以支持受信任企业间（例如电话代理和 TLS 代理之间）自签证书 **enrollment** 的注册。

使用指南

使用 **crypto ca trustpoint** 命令声明 CA。执行此命令可使您进入加密 CA 信任点配置模式。

此命令管理信任点信息。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。信任点模式中的命令控制特定于 CA 的配置参数，这些参数指定 ASA 如何获取 CA 证书、ASA 如何从 CA 获取其证书以及 CA 颁发的用户证书的身份验证策略。

您可以使用以下命令指定信任点的特征：

- **accept-subordinates** - 已弃用。指示如果在一期 IKE 交换期间传输，是否接受与信任点关联的 CA 下级证书（之前未在 ASA 上安装时）。
- **crl required | optional | nocheck** - 指定 CRL 配置选项。

- **crl configure** - 进入 CRL 配置模式（请参阅 **crl** 命令）。
- **default enrollment** - 将所有注册参数恢复为系统默认值。此命令的调用不会成为活动配置的一部分。
- **email** *address* - 在注册过程中，要求 CA 在证书的主题备用扩展名中包括指定的邮件地址。
- **enrollment retry period** - 指定 SCEP 注册的重试时间段（以分钟为单位）。
- **enrollment retry count** - 指定 SCEP 注册允许的最大重试次数。
- **enrollment terminal** - 指定使用此信任点进行剪切和粘贴注册。
- **enrollment self** - 指定生成自签证书的注册。
- **enrollment url** *url* - 指定 SCEP 注册使用此信任点进行注册并配置注册 URL (*url*)。
- **exit** - 退出配置模式。
- **fqdn** *fqdn* - 在注册过程中要求 CA 将指定 FQDN 包括在证书的主题备用扩展名中。
- **id-cert-issuer** - 已弃用。指示系统是否接受与此信任点关联的 CA 颁发的对等设备证书。
- **id-usage** - 指定如何使用信任点的已注册身份。
- **ip-addr** *ip-address* - 在注册过程中要求 CA 将 ASA 的 IP 地址包括在证书中。
- **keypair** *name* - 指定其公钥将经过认证的密钥对。
- **match certificate** *map-name* **override ocsp** - 将证书映射与 OCSP 覆盖规则匹配。
- **ocsp disable-nonce** - 禁用 nonce 扩展，这样可通过加密方式将撤销请求与响应绑定以避免重播攻击。
- **ocsp url** - 指定此 URL 中的 OCSP 服务器检查与此信任点关联的所有证书，以了解撤销状态。
- **exit** - 退出配置模式。
- **password** *string* - 指定在注册过程中向 CA 注册时的质询短语。CA 通常使用此短语对后续撤销请求进行身份验证。
- **revocation check** - 指定撤销检查方法，包括 CRL、OCSP 和 none。
- **serial-number** - 在注册过程中要求 CA 将 ASA 序列号包括在证书中。
- **subject-name** *X.500 name* - 在注册过程中要求 CA 将指定主题 DN 包括在证书中。如果 DN 字符串包括逗号，请用双引号将值字符串括起来（例如 O="Company, Inc."）
- **support-user-cert-validation** - 已弃用。如果启用，则该信任点向颁发远程证书的 CA 进行身份验证时，可从此信任点获取验证远程用户证书的配置设置。此选项适用于与子命令 **crl required | optional | nocheck** 关联的配置数据和 CRL 模式下的所有设置。
- **validation-policy** - 指定验证与用户连接关联的证书的信任点条件。

注意　当您尝试连接时，在尝试从信任点检索 ID 证书的过程中会出现表示信任点不包含 ID 证书的警告。

示例

以下示例进入 CA 信任点配置模式，以管理名为 central 的信任点：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
clear configure crypto ca trustpoint	删除所有信任点。
crypto ca authenticate	获取此信任点的 CA 证书。
crypto ca certificate map	进入 crypto ca certificate map 配置模式。定义基于证书的 ACL。
crypto ca crl request	基于指定信任点的配置参数请求 CRL。
crypto ca import	安装从 CA 收到的证书以响应手动注册请求。

crypto ca trustpool export

要导出建立 PKI 信任池的证书，请在特权 EXEC 模式下使用 **crypto ca trustpool export** 命令。

crypto ca trustpool export *filename*

语法说明

filename	要在其中存储已导出信任池证书的文件。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令将活动信任池的全部内容复制到 PEM 编码格式的指定文件路径。

示例

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE

<More>
```

相关命令

命令	说明
crypto ca trustpool import	导入构成 PKI 信任池的证书。

crypto ca trustpool import

要导入建立 PKI 信任池的证书，请在全局配置模式下使用 **crypto ca trustpool import** 命令。

crypto ca trustpool import [**clean**] **url** *url* [**noconfirm** [**signature-required**]]

crypto ca trustpool import [**clean**] **default** [**noconfirm**]

语法说明

clean	在导入之前删除所有下载的信任池证书。
default	还原 ASA 的默认受信任 CA 列表。
noconfirm	抑制所有交互式提示。
signature-required	指示仅接受经过签署的文件。
url	要导入的信任池文件的位置。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令可在从 cisco.com 下载信任池捆绑包时验证文件上的签名。当从其他源下载捆绑包或其格式不支持签名时，有效签名不是必填项。用户获悉签名状态并且可以选择是否接受捆绑包。

可能出现的交互警告如下：

- 具有无效签名的思科捆绑包格式
- 非思科捆绑包格式
- 具有有效签名的思科捆绑包格式

仅当选择 **noconfirm** 选项时，才可以使用 **signature-required** 关键字。如果包括 **signature-required** 关键字，但签名不存在或无法验证，则导入失败。

注　除非您通过其他方法验证了文件的合法性，否则在文件签名无法验证时请勿安装证书。

以下示例展示抑制交互式提示和要求签名时 **crypto ca trustpool** 导入命令的行为：

```
ciscoasa(config)# crypto ca trustpool import url ?

configure mode commands/options:
disk0:   Import from disk0: file system
disk1:   Import from disk1: file system
flash:   Import from flash: file system
ftp:     Import from ftp: file system
http:    Import from http: file system
https:   Import from https: file system
smb:     Import from smb: file system
system:  Import from system: file system
tftp:    Import from tftp: file system

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com ?
exec mode commands/options:
noconfirm  Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com  noconfirm ?
exec mode commands/options:
signature-required  Indicate that only signed files will be accepted
```

相关命令

命令	说明
crypto ca trustpool export	导出构成 PKI 信任池的证书。

crypto ca trustpool policy

要进入提供定义信任池策略的命令的子模式，请在全局配置模式下使用 **crypto ca trustpool policy** 命令。

crypto ca trustpool policy

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

```
ciscoasa(config)# crypto ca trustpool ?

configure mode commands/options:
policy Define trustpool policy

ciscoasa(config)# crypto ca trustpool policy
ciscoasa(config-ca-trustpool)# ?

CA Trustpool configuration commands:
crl               CRL options
exit              Exit from certificate authority trustpool entry mode
match             Match a certificate map
no                Negate a command or set its defaults
revocation-check  Revocation checking options
ciscoasa(config-ca-trustpool)#
```

相关命令

命令	说明
show crypto ca trustpool policy	显示已配置的信任池策略。

crypto ca trustpool remove

要从 PKI 信任池删除一个指定的证书，请在特权 EXEC 模式下使用 **crypto ca trustpool remove** 命令。

crypto ca trustpool remove *cert fingerprint* [**noconfirm**]

语法说明

cert fingerprint	十六进制数据。
noconfirm	指定此关键字以抑制所有交互式提示。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

由于此命令会导致受信任的根证书内容发生变化，会提示交互式用户确认其操作。

示例

```
ciscoasa# crypto ca trustpool remove ?

  Hex-data  Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm  Specify this keyword to suppress all interactive prompting.
```

相关命令

命令	说明
clear crypto ca trustpool	从信任池删除所有证书。
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。

crypto dynamic-map match address

要匹配动态加密映射条目的访问列表地址，请在全局配置模式下使用 **crypto dynamic-map match address** 命令。要禁用地址匹配，请使用此命令的 **no** 形式。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

语法说明

acl-name	标识要匹配动态加密映射条目的访问列表。
dynamic-map-name	指定动态加密映射集的名称。
dynamic-seq-num	指定动态加密映射条目对应的序列号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

请参阅 crypto map match address 命令了解有关此命令的更多信息。

示例

以下示例展示使用 **crypto dynamic-map** 命令匹配名为 aclist1 的访问列表中的地址：

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	清除所有动态加密映射的所有配置。
show running-config crypto dynamic-map	显示所有动态加密映射的所有配置。

crypto dynamic-map set df-bit

要设置每个签名算法 (SA) 的不分段 (DF) 策略，请在全局配置模式下使用 **crypto dynamic-map set df-bit** 命令。要禁用 DF 策略，请使用此命令的 **no** 形式。

crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

语法说明

name	指定加密动态映射集的名称。
priority	指定分配给动态加密映射条目的优先级。

默认值

默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

原始 DF 策略命令被保留，并且用作接口上的全局策略设置，但用于 SA 时被 **crypto map** 命令取代。

crypto dynamic-map set nat-t-disable

要根据此加密映射条目对连接禁用 NAT-T，请在全局配置模式下使用 **crypto dynamic-map set nat-t-disable** 命令。要对此加密映射条目启用 NAT-T，请使用此命令的 **no** 形式。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

语法说明

dynamic-map-name	指定加密动态映射集的名称。
dynamic-seq-num	指定分配给动态加密映射条目的编号。

默认值

默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

使用 **isakmp nat-traversal** 命令全局启用 NAT-T。然后，可使用 **crypto dynamic-map set nat-t-disable** 命令对特定加密映射条目禁用 NAT-T。

示例

以下命令对名为 mymap 的动态加密映射条目禁用 NAT-T：

```
ciscoasa(config)# crypto dynamic-map mymap 10 set nat-t-disable
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	清除所有动态加密映射的所有配置。
show running-config crypto dynamic-map	显示所有动态加密映射的所有配置。

crypto dynamic-map set peer

请参阅 **crypto map set peer** 命令了解有关此命令的更多信息。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

语法说明

dynamic-map-name	指定动态加密映射集的名称。
dynamic-seq-num	指定动态加密映射条目对应的序列号。
hostname	通过主机名识别动态加密映射条目中的对等设备，如 **name** 命令所定义。
ip_address	通过 IP 地址识别动态加密映射条目中的对等设备，如 **name** 命令所定义。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

示例

以下示例展示将名为 mymap 的动态映射的对等设备设置为 IP 地址 10.0.0.1：

```
ciscoasa(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	清除所有动态加密映射的所有配置。
show running-config crypto dynamic-map	显示所有动态加密映射的所有配置。

crypto dynamic-map set pfs

要指定动态加密映射集，请在全局配置模式下使用 **crypto map dynamic-map set pfs** 命令。要删除指定的动态映射加密映射集，请使用此命令的 **no** 形式。

请参阅 **crypto map set pfs** 命令了解有关此命令的更多信息。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1 | group2 | group5**]

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1 | group2 | group5**]

语法说明

dynamic-map-name	指定动态加密映射集的名称。
dynamic-seq-num	指定动态加密映射条目对应的序列号。
group1	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 768 位 Diffie-Hellman 主模数组。
group2	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1024 位 Diffie-Hellman 主模数组。
group5	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1536 位 Diffie-Hellman 主模数组。
set pfs	配置 IPsec 以在请求此动态加密映射条目的新安全关联时要求完全前向保密 (PFS)，或在接收新安全关联的请求时要求 PFS。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，添加了 Diffie-Hellman 组 7。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。
9.0(1)	增加了多情景模式支持。

使用指南

crypto dynamic-map 命令，例如 **match address**、**set peer** 和 **set pfs** 都用 **crypto map** 命令进行描述。如果对等设备发起协商，并且本地配置指定 PFS，则对等设备必须执行 PFS 交换，否则协商会失败。如果本地配置不指定组，ASA 将使用默认值（组 2）。如果本地配置不指定 PFS，它将接受对等设备提供的任何 PFS。

与思科 VPN 客户端交互时，ASA 不使用 PFS 值，而使用在第 1 阶段协商的值。

示例

以下示例指定在为加密动态映射 mymap 10 协商新安全关联时应使用 PFS。指定的组是组 2：

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	清除所有动态加密映射的所有配置。
show running-config crypto dynamic-map	显示所有动态加密映射的所有配置。

crypto dynamic-map set reverse route

请参阅 crypto map set reverse-route 命令了解有关此命令的更多信息。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

语法说明

dynamic-map-name	指定加密映射集的名称。
dynamic-seq-num	指定分配给加密映射条目的编号。

默认值

此命令的默认值是 off。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

示例

以下命令为名为 mymap 的动态加密映射启用反向路由注入：

```
ciscoasa(config)# crypto dynamic-map mymap 10 set reverse route
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	清除所有动态加密映射的所有配置。
show running-config crypto dynamic-map	显示所有动态加密映射的所有配置。

crypto dynamic-map set ikev1 transform-set

要指定在动态加密映射条目中使用的 IKEv1 转换集，请在全局配置模式下使用 **crypto dynamic-map set ikev1 transform-set** 命令。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

要从动态加密映射条目删除转换集，请指定此命令的 **no** 形式：

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

要删除动态加密映射条目，请使用此命令的 **no** 形式并且指定所有转换集或不指定任何转换集。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

语法说明

dynamic-map-name	指定动态加密映射集的名称。
dynamic-seq-num	指定动态加密映射条目对应的序列号。
transform-set-name1 *transform-set-name11*	指定转换集的一个或多个名称。此命令中指定的任何转换集必须在 **crypto ipsec ikev1 transform-set** 命令中定义。每个加密映射条目支持最多 11 个转换集。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。
7.2(1)	更改了加密映射条目中转换集的最大数量。
8.4(1)	增加了 **ikev1** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

动态加密映射是未配置所有参数的加密映射。它用作策略模板，稍后通过 IPsec 协商动态获取缺失的参数以满足对等设备要求。如果其 IP 地址并未在之前的静态或动态加密映射中标识，ASA 将应用动态加密映射以让对等设备协商隧道。以下类型的对等设备会发生上述情况：

- 具有动态分配的公共 IP 地址的对等设备。

  LAN-to-LAN 与远程访问对等设备可以使用 DHCP 获取公共 IP 地址。ASA 仅使用此地址启动隧道。

- 具有动态分配的专用 IP 地址的对等设备。

  请求远程访问隧道的对等设备通常具有头端分配的专用 IP 地址。通常情况下，LAN-to-LAN 隧道有一组预先确定的专用网络，用于配置静态映射，进而用于建立 IPsec SA。

作为配置静态加密映射的管理员，您可能不知道动态分配的 IP 地址（通过 DHCP 或其他方法），而且您可能不知道其他客户端的专用 IP 地址（无论它们如何分配）。VPN 客户端通常没有静态 IP 地址；这些客户端需要动态加密映射来支持 IPsec 协商。例如，头端在 IKE 协商期间向思科 VPN 客户端分配 IP 地址，该客户端则用分配的 IP 地址协商 IPsec SA。

动态加密映射可以简化 IPsec 配置，我们建议将其用于并不总是预先确定对等设备的网络。使用思科 VPN 客户端（如移动用户）的动态加密映射和获取动态分配的 IP 地址的路由器。

提示　请小心使用 **permit** 条目中的 **any** 关键字。如果此类 **permit** 条目覆盖的流量可能包括组播或广播流量，请将相应地址范围的 **deny** 条目插入到访问列表中。记住为网络和子网广播流量以及任何 IPsec 不应保护的其他流量插入 **deny** 条目。

动态加密映射仅用于与发起连接的远程对等设备协商 SA。ASA 不能使用动态加密映射发起与远程对等设备的连接。配置动态加密映射后，如果出站流量与访问列表的 permit 条目匹配并且对应的 SA 不存在，ASA 会丢弃流量。

加密映射集可能包括动态加密映射。动态加密映射集应是加密映射集中优先级最低的加密映射（即它们具有最高序列号），以便 ASA 先评估其他加密映射。仅当其他（静态）映射条目不匹配时，它才检查动态映射集。

类似于静态加密映射集，动态加密映射集包括具有相同动态映射名称的所有动态加密映射。动态序列号用于区分一个动态加密映射集中的动态加密映射。如果您配置动态加密映射，请插入允许 ACL 为加密访问列表标识 IPsec 对等设备的数据流。否则 ASA 会接受对等设备提供的所有数据流身份。

注意事项　请勿将要通过隧道传输的流量的静态（默认）路由分配给使用动态加密映射集配置的 ASA 接口。要标识应通过隧道传输的流量，请将 ACL 添加到动态加密映射。配置与远程访问隧道关联的 ACL 时，请小心标识合适的地址池。仅在隧道启用后使用反向路由注入安装路由。

您可以在一个加密映射集中同时包含静态和动态映射条目。

示例

以下示例创建名为 dynamic0 的动态加密映射条目（包括相同的 10 个转换集）。

```
ciscoasa(config)# crypto dynamic-map dynamic0 1 set ikev1 transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

相关命令

命令	说明
crypto ipsec ikev1 transform-set	配置 IKEv1 转换集。
crypto map set transform-set	指定要在加密映射条目中使用的转换集。
clear configure crypto dynamic-map	从配置中清除所有动态加密映射。
show running-config crypto dynamic-map	显示动态加密映射配置。
show running-config crypto map	显示加密映射配置。

crypto dynamic-map set ikev2 ipsec-proposal

要指定在动态加密映射条目中使用的 IKEv2 的 IPsec 建议，请在全局配置模式下使用 **crypto dynamic-map set ikev2 ipsec-proposal** 命令。要从动态加密映射条目删除转换集的名称，请使用此命令的 **no** 形式。

crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

语法说明

dynamic-map-name	指定动态加密映射集的名称。
transform-set-name1 *transform-set-name11*	指定转换集的一个或多个名称。此命令中指定的任何转换集必须在 **crypto ipsec ikev2 transform-set** 命令中定义。每个加密映射条目支持最多 11 个转换集。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

crypto dynamic-map set ikev2 ipsec-proposal

要指定在动态加密映射条目中使用的 IKEv2 的 IPsec 建议，请在全局配置模式下使用 **crypto dynamic-map set ikev2 ipsec-proposal** 命令。要从动态加密映射条目删除转换集的名称，请使用此命令的 **no** 形式。

crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

语法说明

dynamic-map-name	指定动态加密映射集的名称。
transform-set-name1 *transform-set-name11*	指定转换集的一个或多个名称。此命令中指定的任何转换集必须在 **crypto ipsec ikev2 transform-set** 命令中定义。每个加密映射条目支持最多 11 个转换集。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

crypto dynamic-map set pfs

要设置 IPsec 在为此动态加密映射条目要求新的安全关联时要求 PFS 或在接收新安全关联请求时要求 PFS，请在全局配置模式下使用 **crypto dynamic-map set pfs** 命令。要指定 IPsec 不应要求 PFS，请使用此命令的 **no** 形式。

crypto dynamic-map *map-name map-index* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

no crypto dynamic-map *map-name map-index* **set pfs**[**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

语法说明

group1	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 768 位 Diffie-Hellman 主模数组。
group2	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1024 位 Diffie-Hellman 主模数组。
group5	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1536 位 Diffie-Hellman 主模数组。
group14	指定要使用的 Diffie-Hellman 密钥交换组。
group19	指定要使用的 Diffie-Hellman 密钥交换组。
group20	指定要使用的 Diffie-Hellman 密钥交换组。
group21	指定要使用的 Diffie-Hellman 密钥交换组。
group24	指定要使用的 Diffie-Hellman 密钥交换组。
map-name	指定加密映射集的名称。
map-index	指定分配给加密映射条目的编号。

默认值

默认情况下，未设置 PFS。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，添加了 Diffie-Hellman 组 7。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。
9.0(1)	增加了多情景模式支持。

使用指南

借助 PFS，每次协商新的安全关联时，就会发生新的 Diffie-Hellman 交换，这需要额外的处理时间。PFS 会添加另一层安全保护，因为，如果一个密钥被攻击者破解，只有通过该密钥发送的数据受到威胁。

crypto dynamic-map set tfc-packets

要对 IPsec SA 启用虚拟通信业务流保密性 (TFC) 数据包，请在全局配置模式下使用 **crypto dynamic-map set tfc-packets** 命令。要在 IPsec SA 上禁用 TFC 数据包，请使用此命令的 **no** 形式。

crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]

no crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]

语法说明

name	指定加密映射集的名称。
priority	指定分配给加密映射条目的优先级。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令为加密映射配置现有 DF 策略（在 SA 级）。

crypto dynamic-map set validate-icmp-errors

要指定是否验证通过 IPsec 隧道接收的传入 ICMP 错误消息（它们预定前往专用网络的内部主机），请在全局配置模式下使用 **crypto dynamic-map set validate-icmp-errors** 命令。要取消对来自加密动态映射条目的传入 ICMP 错误消息的验证，请使用此命令的 **no** 形式。

crypto dynamic-map *name priority* **set validate-icmp-errors**

no crypto dynamic-map *name priority* **set validate-icmp-errors**

语法说明

name	指定加密动态映射集的名称。
priority	指定分配给动态加密映射条目的优先级。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

以下加密映射命令仅适用于验证传入的 ICMP 错误消息。

crypto engine accelerator-bias

要更改对称多处理技术 (SMP) 平台上加密核心的分配，请在全局配置模式下使用 **crypto engine accelerator-bias** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

no crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

语法说明

balanced	均匀分配加密硬件资源（Admin/SSL 和 IPsec 核心）
ipsec -client	分配加密硬件资源以支持 IPsec 核心（包括 SRTP 加密语音流量）。
ssl-client	分配加密硬件资源以支持 Admin/SSL 核心。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

加密核心再平衡在以下平台上可用：ASA 5585、5580、5545/5555 和 ASASM。

示例

以下示例展示可用于配置 crypto engine acccelerator-bias 命令的选项。

```
ciscoasa (config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

ciscoasa (config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec-client - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl-client - Allocate crypto hardware resources to favor SSL

ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

要将 ASA 5510、5520、5540 或 5550 上的大模数运算从软件切换到硬件，请在全局配置模式下使用 **crypto engine large-mod-accel** 命令。要从配置中删除命令，请使用此命令的 **no** 形式。

crypto engine large-mod-accel

no crypto engine large-mod-accel

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 在软件中执行大模数运算。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(2)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令仅对 ASA 型号 5510、5520、5540 和 5550 可用。它将大模数运算从软件切换到硬件。切换到硬件可加快以下操作的速度：

- 2048 位 RSA 公共密钥证书处理。
- Diffie Hellman 组 5 (DH5) 密钥生成。

我们建议您在必要时使用此命令，以增加每秒连接数。根据负载，可能对 SSL 吞吐量具有有限的性能影响。

我们还建议您在使用较少时或维护期间使用此命令的任一形式，从而在软件与硬件处理之间的过渡过程中最大限度地减少临时数据包丢失。

注　ASA 5580/5500-X 平台已经集成此功能以切换大模数运算；因此，**crypto engine** 命令不适用于这些平台。

示例

以下示例将大模数运算从软件切换到硬件：

```
ciscoasa(config)# crypto engine large-mod-accel
```

以下示例从配置删除之前的命令并将大模数运算切换回软件：

```
ciscoasa(config)# no crypto engine large-mod-accel
```

相关命令

命令	说明
show running-config crypto engine	显示大模数运算是否切换到硬件。
clear configure crypto engine	将大模数运算切换回软件。此命令等同于 **no crypto engine large-mod-accel** 命令。

crypto ikev1 enable

要在 IPsec 对等设备与 ASA 通信的接口上启用 ISAKMP IKEv1 协商，请在全局配置模式下使用 **crypto ikev1 enable** 命令。要在接口上禁用 ISAKMP IKEv1，请使用此命令的 **no** 形式。

crypto ikev1 enable *interface-name*

no crypto ikev1 enable *interface-name*

语法说明

interface-name	指定要在其上启用或禁用 ISAKMP IKEv1 协商的接口的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此 **isakmp enable** 命令。
7.2(1)	**crypto isakmp enable** 命令取代了 **isakmp enable** 命令。
8.4(1)	由于增加了 IKEv2 功能，**crypto isakmp enable** 命令更改为 **crypto ikev1 enable** 命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例在全局配置模式下输入，显示如何禁用内部接口上的 ISAKMP：

```
ciscoasa(config)# no crypto isakmp enable inside
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev1 ipsec-over-tcp

要启用 IPsec over TCP，请在全局配置模式下使用 **crypto ikev1 ipsec-over-tcp** 命令。要禁用 IPsec over TCP，请使用此命令的 **no** 形式。

crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

no crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

语法说明

port *port1...port10*	（可选）指定设备接受 IPsec over TCP 连接的端口。最多可列出 10 个端口。端口号可以在 1 到 65535 的范围内。默认端口号为 10000。

默认值

默认值为禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp ipsec-over-tcp** 命令。
7.2.(1)	**crypto isakmp ipsec-over-tcp** 命令取代了 **isakmp ipsec-over-tcp** 命令。
8.4(1)	命令名称从 **crypto isakmp ipsec-over-tcp** 更改为 **crypto ikev1 ipsec-over-tcp**。

示例

以下示例在全局配置模式下输入，在端口 45 上启用 IPsec over TCP：

```
ciscoasa(config)# crypto ikev1 ipsec-over-tcp port 45
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev1 limit max-in-negotiation-sa

要限制 ASA 上的 IKEv2 协商中的（开放）SA 数量，请在全局配置模式下使用 **crypto ikev1 limit max-in-negotiation-sa** 命令。要禁用对开放 SA 数量的限制，请使用此命令的 **no** 形式：

crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

语法说明

threshold percentage	对于 ASA 允许的 SA 总数相对于协商中允许的 SA 总数（开放）的百分比。在达到阈值后，其他连接均会遭到拒绝。范围为 1% 至 100%。默认为 100%。

默认值

默认设置为禁用。ASA 不限制开放 SA 的数量。

使用指南

crypto ikev1 limit-max-in-negotiation-sa 命令限制可随时协商的 SA 的最大数量。

crypto kev2 limit max in-negotiation-sa 命令阻止其他连接协商以保护当前连接，并防止 Cookie 质询功能可能无法拦截的内存和 / 或 CPU 攻击。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

示例

以下示例将协商中的 IKEv1 连接数限制为允许的最大 IKEv1 连接数的 70%：

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

相关命令

命令	说明
crypto ikev1 limit max-sa	限制 ASA 上的 IKEv1 连接数。
clear configure crypto isakmp	清除所有 ISAKMP 配置。

命令	说明
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev1 policy

要创建 IPsec 连接的 IKEv1 安全关联 (SA)，请在全局配置模式下使用 **crypto ikev2 policy** 命令。要删除该策略，请使用此命令的 **no** 形式。

crypto ikev1 policy *priority*

no crypto ikev1 policy *priority*

语法说明

priority	策略包优先级。范围是 1-65535，最高为 1，最低为 65535。

默认值

没有默认行为和默认值。

使用指南

该命令进入 IKEv1 策略配置模式，在该模式下可指定其他 IKEv1 SA 设置。IKEv1 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv1 对等设备以在第 2 阶段中进行安全通信。在输入 **crypto ikev1 policy** 命令后，您可以使用其他命令设置 SA 加密算法、DH 组、完整性算法、生命期和散列算法。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例创建优先级 1 IKEv1 SA，然后进入 IKEv1 策略配置模式：

```
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev2-policy)#
```

相关命令

命令	说明
crypto ikev2 cookie-challenge	使 ASA 能够将 Cookie 质询发送到对等设备以响应 SA 启动数据包。
clear configure crypto isakmp	清除所有 ISAKMP 配置。

命令	说明
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 enable

要在 IPsec 对等设备与 ASA 通信的接口上启用 ISAKMP IKEv2 协商，请在全局配置模式下使用 **crypto ikev2 enable** 命令。要在接口上禁用 ISAKMP IKEv2，请使用此命令的 **no** 形式。

crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

no crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

语法说明

interface-name	指定要在其上启用或禁用 ISAKMP IKEv2 协商的接口的名称。
client-services	为接口上的 IKEv2 连接启用客户端服务。客户端服务包括增强的 AnyConnect 安全移动客户端功能，其中包括软件更新、客户端配置文件、GUI 本地化（转换）和定制、思科安全桌面和 SCEP 代理。如果禁用客户端服务，AnyConnect 客户端仍会建立与 IKEv2 的基本 IPsec 连接。
port *port*	指定要为 IKEv2 连接启用客户端服务的端口。范围为 1 65535。默认为端口 443。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

单独使用此命令不会启用客户端服务。

示例

以下示例在全局配置模式下输入，它显示如何在外部接口上启用 IKEv2：

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 cookie-challenge

要使 ASA 能够将 Cookie 质询发送到对等设备以响应 SA 启动数据包，请在全局配置模式下使用 **crypto ikev2 cookie-challenge** 命令。要禁用 Cookie 质询，请使用此命令的 **no** 形式：

crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

语法说明

threshold percentage	对于 ASA 允许的 SA 总数相对于协商中总数的百分比，该百分比会触发所有将来的 SA 协商的 Cookie 质询。范围为 0 到 99%。默认为 50%。
always	始终对传入 SA 进行 Cookie 质询。
never	从不对传入 SA 进行 Cookie 质询。

默认值

没有默认行为或值。

使用指南

向对等设备进行 Cookie 质询可防止发生拒绝服务 (DoS) 攻击。当对等设备发送 SA 启动数据包并且 ASA 发送其响应但对等设备不再响应时，攻击者发动 DoS 攻击。如果对等设备持续这样做，ASA 上所有允许的 SA 请求会用尽，直到其停止响应。

使用 **crypto ikev2 cookie-challenge** 命令启用阈值百分比会限制开放 SA 协商的数量。例如，在使用默认设置 50% 的情况下，当允许的 SA 的 50% 在协商中（开放）时，ASA 会对到达的任何额外的 SA 启动数据包进行 Cookie 质询。对于具有 10000 个允许的 IKEv2 SA 的思科 ASA 5580，在 5000 个 SA 变为开放后，任何其他传入 SA 都要经过 Cookie 质询。

如果与 **crypto kev2 limit max in-negotiation-sa** 命令一起使用，则配置低于最大协商中阈值的 Cookie 质询阈值以进行有效交叉检查。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

示例

在以下示例中，Cookie 质询阈值设置为 30%：

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

相关命令

命令	说明
crypto ikev2 limit max-sa	限制 ASA 上的 IKEv2 连接数。
crypto ikev2 limit max-in-negotiation-sa	限制 ASA 上 IKEv2 协商中 SA 的数量。
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 limit max-in-negotiation-sa

要限制 ASA 上 IKEv2 协商中（开放）SA 的数量，请在全局配置模式下使用 **crypto ikev2 limit max in-negotiation-sa** 命令。要禁用对开放 SA 数量的限制，请使用此命令的 **no** 形式：

crypto ikev2 limit max in-negotiation-sa *threshold percentage*

no crypto ikev2 limit max in-negotiation-sa *threshold percentage*

语法说明

threshold percentage	对于 ASA 允许的 SA 总数相对于协商中允许的 SA 总数（开放）的百分比。在达到阈值后，其他连接均会遭到拒绝。范围为 1% 至 100%。默认为 100%。

默认值

默认设置为禁用。ASA 不限制开放 SA 的数量。

使用指南

crypto ikev2 limit-max-in-negotiation-sa 命令限制可随时协商的 SA 的最大数量。如果与 **crypto ikev2 cookie-challenge** 命令一起使用，则配置低于此限制的 Cookie 质询阈值以进行有效的交叉检查。

不同于用 Cookie 对传入连接的 **crypto ikev2 cookie-challenge** 命令进行质询，**crypto kev2 limit max in-negotiation-sa** 命令阻止进一步连接进行协商以保护当前连接并防止 Cookie 质询功能可能无法阻止的内存和 / 或 CPU 攻击。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例将协商中的 IKEv2 连接数限制为允许的最大 IKEv2 连接数的 70%：

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

相关命令

命令	说明
crypto ikev2 limit max-sa	限制 ASA 上的 IKEv2 连接数。
crypto ikev2 cookie-challenge	启用 ASA 将 Cookie 质询到对等设备以响应 SA 启动的数据包。
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 limit max-sa

要限制 ASA 上的 IKEv2 连接数，请在全局配置模式下使用 **crypto ikev2 limit max-sa** 命令。要禁用连接数的限制，请使用此命令的 **no** 形式：

crypto ikev2 limit max-sa *number*

no crypto ikev2 limit max-sa *number*

语法说明

number	ASA 上允许的 IKEv2 连接数。在达到限制后，其他连接均会遭到拒绝。范围是 1 到 10000。

默认值

默认设置为禁用。ASA 不限制 IKEv2 连接数。允许的最大 IKEv2 连接数等于许可证指定的最大连接数。

使用指南

crypto ikev2 limit max-sa 命令限制 ASA 上的最大 SA 数量。

如果与 **crypto ikev2 cookie-challenge** 命令一起使用，则配置低于此限制的 Cookie 质询阈值以进行有效的交叉检查。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例将 IKEv2 连接数限制为 5000：

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

相关命令

命令	说明
crypto ikev2 cookie-challenge	启用 ASA 将 Cookie 质询到对等设备以响应 SA 启动的数据包。
clear configure crypto isakmp	清除所有 ISAKMP 配置。

命令	说明
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 policy

要创建 AnyConnect IPsec 连接的 IKEv2 安全关联 (SA)，请在全局配置模式下使用 **crypto ikev2 policy** 命令。要删除该策略，请使用此命令的 **no** 形式。

crypto ikev2 policy *priority policy_index*

no crypto ikev2 policy *priority policy_index*

语法说明

policy index	访问 IKEv2 策略配置模式。
priority	策略包优先级。范围是 1-65535，1 代表最高优先级，65535 代表最低优先级。组 [1] [2] [5] 成为组 [1] [2] [5] [14] [24] 以支持 Diffie-Hellman 组 14 和 24 作为 IKEv2 密钥派生的一部分。

默认值

没有默认行为或值。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。输入 **crypto ikev2 policy** 命令后，进入 IKEv2 策略配置模式，您可以在该模式下指定其他 IKEv2 SA 设置。您可以使用其他命令设置 SA 加密算法、DH 组、完整性算法、生命期和散列算法。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。增加了策略索引选项。

示例

以下示例创建优先级 1 IKEv2 SA，然后进入 IKEv2 策略配置模式：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)#
```

相关命令

命令	说明
crypto ikev2 cookie-challenge	启用 ASA 将 Cookie 质询到对等设备以响应 SA 启动的数据包。
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 redirect

要指定从主控设备到集群成员发生负载平衡重新定向的 IKEv2 阶段，请在全局配置模式下使用 **crypto ikev2 redirect** 命令。要删除命令，请使用此命令的 **no** 形式。

crypto ikev2 redirect {during-init | during-auth}

no crypto ikev2 redirect {during-init | during-auth}

语法说明

during-auth	在 IKEv2 身份验证交换过程中，启用负载平衡重新定向到集群成员。
during-init	在 IKEv2 SA 启动的交换期间，启用负载平衡重新定向到集群成员。

默认值

默认为负载平衡重新定向到集群成员，此行为在 IKEv2 身份验证交换过程中发生。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

示例

以下示例设置在 IKEv2 启动的交换过程中发生负载平衡重新定向到集群成员：

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

相关命令

命令	说明
crypto ikev2 cookie-challenge	启用 ASA 将 Cookie 质询到对等设备以响应 SA 启动的数据包。
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto ikev2 remote-access trust-point

要指定作为 AnyConnect IKEv2 连接的 ASA 的身份证书信任点引用和使用的全局信任点，请在隧道组配置模式下使用 **crypto ikev2 remote-access trust-point** 命令。要从配置中删除命令，请使用该此命令的 **no** 形式：

crypto ikev2 remote-access trust-point *name* [*line number*]

no crypto ikev2 remote-access trust-point *name* [*line number*]

语法说明

name	信任点的名称，最多 65 个字符。
line number	指定要在其中插入信任点的行编号。通常，此选项用于在顶部插入信任点，而不删除并重新添加另一行。如果未指定行，ASA 将在列表末尾添加信任点。

默认值

没有默认行为或值。

使用指南

对于所有 IKEv2 连接，使用 **crypto ikev2 remote-access trust-point** 命令配置 ASA 的信任点向 AnyConnect 客户端验证自身。使用此命令允许 AnyConnect 客户端支持为用户选择组。

您可以同时配置两个信任点：两个 RSA、两个 ECDSA 或各一个。ASA 扫描已配置的信任点列表并选择该客户端支持的第一个信任点。如果首选 ECDSA，则您应先配置 ECDSA 信任点，再配置 RSA 信任点。

如果您尝试添加已存在的信任点，将收到一条错误消息。如果使用 **no crypto ikev2 remote-access trustpoint** 命令而不指定要删除哪个信任点名称，则会删除所有信任点配置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了对多情景模式和两个信任点配置的支持。

示例

以下示例指定信任点 *cisco_asa_trustpoint*：

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

要配置 IPsec 数据包的 DF 位策略，请在全局配置模式下使用 **crypto ipsec df-bit** 命令。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

语法说明

clear-df	（可选）指定外部 IP 报头将清除 DF 位，并且 ASA 可能将数据包分段以添加 IPsec 封装。
copy-df	（可选）指定 ASA 在原始数据包中查找外部 DF 位设置。
set-df	（可选）指定外部 IP 报头将设置 DF 位；但如果原始数据包已清除 DF 位，ASA 可能将数据包分段。
interface	指定接口名称。

默认值

此命令默认禁用。如果启用此命令但没有指定的设置，则 ASA 将 **copy-df** 设置用作默认设置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

具有 IPsec 隧道功能的 DF 位允许您指定 ASA 是否可从封装的报头中清除、设置或复制不分段 (DF) 位。IP 报头中的 DF 位确定是否允许设备对数据包分段。

在全局配置模式下使用 **crypto ipsec df-bit** 命令配置 ASA 以指定封装报头中的 DF 位。此命令在应用加密时处理明文数据包的 DF 位设置并且清除、设置或将其复制到外部 IPsec 报头。

在封装隧道模式 IPsec 流量时，对 DF 位使用 **clear-df** 设置。此设置可让设备发送大于可用 MTU 大小的数据包。此外，如果您不知道可用 MTU 大小，此设置适用。

注意事项　如果您设置了以下冲突配置，数据包将被丢弃：
crypto ipsec fragmentation after-encryption（将数据包分段）
crypto ipsec df-bit set-df outside（设置 DF 位）

示例

以下示例在全局配置模式下输入，将 IPsec DF 策略设置为 **clear-df**：

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

相关命令

命令	说明
crypto ipsec fragmentation	配置 IPsec 数据包的分段策略。
show crypto ipsec df-bit	显示指定接口的 DF 位策略。
show crypto ipsec fragmentation	显示指定接口的分段策略。

crypto ipsec fragmentation

要配置 IPsec 数据包的分段策略，请在全局配置模式下使用 **crypto ipsec fragmentation** 命令。

crypto ipsec fragmentation {after-encryption | before-encryption} *interface*

语法说明

after-encryption	指定 ASA 将加密后接近最大 MTU 大小的 IPsec 数据包分段（禁用预分段）。
before-encryption	指定 ASA 将加密前接近最大 MTU 大小的 IPsec 数据包分段（启用预分段）。
interface	指定接口名称。

默认值

默认情况下启用预加密。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

当数据包接近加密 ASA 的出站链路的 MTU 大小时，它采用 IPsec 报头进行封装，这时很可能超过出站链路的 MTU。这会导致在加密后进行数据包分段，从而使解密设备在处理路径中重新组合。通过让 IPsec VPN 预分段在高性能 CEF 路径而不是处理路径中运行，可增强解密时的设备性能。

IPsec VPN 的预分段可让加密设备预先确定来自转换集中可用信息的封装数据包大小，这些转换集作为 IPsec SA 的一部分而配置。如果设备预先确定数据包将超出输出接口的 MTU，则设备在加密之前对数据包进行分段。这可在解密之前避免进程级别重组，并帮助提高解密性能和整体 IPsec 流量吞吐量。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密的成本，MTU 值应设置为不低于 1380。将接口设置为低于 1380 字节可能会导致丢包。

注意事项　如果您设置了以下冲突配置，数据包将被丢弃：
crypto ipsec fragmentation after-encryption（将数据包分段）
crypto ipsec df-bit set-df outside（设置 DF 位）

示例

以下示例在全局配置模式中输入，在设备上全局启用 IPsec 数据包的预分段：

```
ciscoasa(config)# crypto ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

以下示例在全局配置模式下输入，禁止对接口上 IPsec 数据包进行预分段：

```
ciscoasa(config)# crypto ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

相关命令

命令	说明
crypto ipsec df-bit	配置 IPsec 数据包的 DF 位策略。
show crypto ipsec fragmentation	显示 IPsec 数据包的分段策略。
show crypto ipsec df-bit	显示指定接口的 DF 位策略。

crypto ipsec security-association pmtu-aging

要启用路径最大传输单位 (PMTU) 时效，请在全局配置模式下使用 **crypto ipsec security-association pmtu-aging** 命令。要禁用 PMTU 老化，请使用该命令的 no 形式：

crypto ipsec security-association pmtu-aging *reset-interval*

[**no**] **crypto ipsec security-association pmtu-aging** *reset-interval*

语法说明

reset-interval	设置 PMTU 值重置的间隔。

默认值

默认情况下启用此功能。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

重置间隔以秒为单位指定。

crypto ipsec ikev2 ipsec-proposal

要创建 IKEv2 建议，请在全局配置模式下使用 **crypto ipsec ikev2 ipsec-proposal** 命令。要删除建议，请使用此命令的 **no** 形式。

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

语法说明

proposal name	访问 IPsec ESP 建议子模式。
proposal tag	IKEv2 IPsec 建议的名称（从 1 到 64 个字符的字符串）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此命令创建建议并进入 IPsec 建议配置模式，在该模式下可为建议指定多个加密和完整性类型。

示例

以下示例创建名为 secure 的 IPsec 建议，然后进入 IPsec 建议配置模式：

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)#
```

相关命令

命令	说明
show running-config ipsec	显示所有转换集的配置。
crypto map set transform-set	指定要在加密映射条目中使用的转换集。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
show running-config crypto map	显示加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。

crypto ipsec ikev2 sa-strength-enforcement

确保 IKEv2 加密密码的强度高于其子 IPsec SA 的加密密码强度。要禁用此功能，请使用此命令的 **no** 形式。

crypto ipsec ikev2 sa-strength-enforcement

no crypto ipsec ikev2 sa-strength-enforcement

默认值

默认情况下启用实施。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

当子 SA 比其父 IKEv2 连接的加密密码强度高时，安全性不会增加。它是配置 IPsec 以防止这种情况出现的良好安全实践。强度实施设置仅影响加密密码；它不修改完整性或密钥交换算法。IKEv2 系统比较每个子 SA 选择的加密密码的相对强度，如下所示：

启用之后，验证子 SA 的已配置加密密码强度不高于父 IKEv2 加密密码强度。如果发现高于父 IKEv2 加密密码强度，子 SA 将更新以使用父密码。如果未找到兼容密码，则子 SA 协商中止。系统日志和调试消息会记录这些操作。

支持的加密密码按强度从最高到最低的顺序在下面列出。出于此检查目的，同一行中的密码具有同等强度。

- AES-GCM-256、AES-CBC-256
- AES-GCM-192、AES-CBC-192
- AES-GCM-128、AES-CBC-128
- 3DES
- DES
- AES-GMAC（任意大小）、NULL

相关命令

命令	说明
show running-config ipsec	启用时，显示加密 IPsec IKEv2 SA 强度实施。

crypto ipsec security-association lifetime

要配置全局生命期值，请在全局配置模式下使用 **crypto ipsec security-association lifetime** 命令。要将全局生命期值重置为默认值，请使用此命令的 **no** 形式。

crypto ipsec security-association lifetime {seconds *seconds* **| kilobytes** *kilobytes* **|** unlimited}

no crypto ipsec security-association lifetime {seconds *seconds* **| kilobytes** *kilobytes* **|** unlimited}

语法说明

kilobytes	指定使用特定安全关联的对等设备之间在该安全关联到期前可通过的流量（以千字节为单位）。范围为 10 到 2147483647 千字节。默认值为 4,608,000 千字节。
seconds	指定安全关联在到期之前生存的秒数。范围为 120 到 214783647 秒。默认值为 28,800 秒（8 小时）。
unlimited	当 ASA 是隧道的发起者时，在快速模式 1 下不发送千字节数据包。

默认值

默认千字节数为 4,608,000 ；默认秒数为 28,800。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。
9.1(2)	添加了无限制参数。

使用指南

crypto ipsec security-association lifetime 命令更改协商 IPsec 安全关联时使用的全局生命期值。

IPsec 安全关联使用共享密钥。这些密钥及其安全关联一起超时。

假设特定的加密映射条目没有配置生命期值，当 ASA 在协商过程中请求新安全关联时，它会在向对等设备发出的请求中指定全局生命期值；它使用此值作为新安全关联的生命期。当 ASA 接收来自对等设备的协商请求时，它使用对等设备指定的生命期值或本地配置的生命期值中较小的值作为新安全关联的生命期。

有两个生命期：“ 定时 ” 生命期和 “ 流量 ” 生命期。只要到达这两个生命期之一（无论先到达哪一个），安全关联就会到期。

ASA 允许用户随时更改加密映射、动态映射和 IPsec 设置。如果更改了此设置，ASA 仅中断受更改影响的连接。如果用户更改与加密映射关联的现有访问列表，尤其是通过删除访问列表内的条目来进行，则仅中断关联的连接。基于访问列表中其他条目的连接不受影响。

要更改全局定时生命期，请使用 **crypto ipsec security-association lifetime seconds** 命令。定时生命期导致安全关联在经过指定的秒数后超时。

要更改全局流量生命期，请使用 **crypto ipsec security-association lifetime kilobytes** 命令。使用流量生命期时，在安全关联密钥保护指定量的流量（以千字节为单位）后，安全关联会超时。

较短的生命期增加了成功恢复密钥攻击的难度，因为攻击者在同一密钥下对较少的数据加密。然而，较短的生命期需要更多的 CPU 处理时间来建立新的安全关联。

安全关联（和相应的密钥）在经过一定秒数后或一定量的流量（以千字节为单位）后过期，以两者中较早发生者为准。

示例

以下示例指定安全关联的全局定时生命期：

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有 IPsec 配置（即全局生命期和转换集）。
show running-config crypto map	显示所有加密映射的所有配置。

crypto ipsec security-association replay

要配置 IPsec 反重播窗口大小，请在全局配置模式下使用 **crypto ipsec security-association replay** 命令。要将窗口大小重置为默认值，请使用此命令的 **no** 形式。

crypto ipsec security-association replay {window-size *n* **| disable}**

no crypto ipsec security-association replay {window-size *n* **| disable}**

语法说明

n	设置窗口大小。值可以是 64、128、256、512 或者 1024。默认值为 64。
disable	禁用反重播检查。

默认值

默认窗口大小是 64。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

Cisco IPsec 身份验证通过为每个加密数据包分配唯一序列号来提供反重播保护，防止攻击者复制加密数据包。（安全关联反重播是一项安全服务，接收方可用于拒绝旧的或重复的数据包以免受重播攻击。）解密程序核对以前看到的序列号。加密程序以升序分配序列号。解密程序会记住看到过的最高序列号值 X。N 是窗口大小，而且，解密程序也记得是否看到过序列号为 X-N+1 到 X 的数据包。序列号 X-N 的任何数据包将被丢弃。当前，N 设置为 64，因此只有 64 个数据包可以由解密程序跟踪。

但通常 64 个数据包的窗口大小是不够的。例如，QoS 优先向高优先级数据包提供，这可能会使某些低优先级数据包被丢弃，即使它们可能是解密程序收到的最后 64 个数据包之一；此事件可以生成警告系统日志消息，这是虚假警告。**crypto ipsec security-association replay** 命令可以扩展窗口大小，使解密程序跟踪 64 个以上的数据包。

提高反重播窗口大小对吞吐量和安全性没有影响。由于每个传入 IPsec SA 仅需额外的 128 个字节来存储解密程序上的序列号，对内存的影响可以忽略。我们建议您使用完整的 1024 窗口大小以避免将来出现反重播问题。

示例

以下示例指定安全关联的反重播窗口大小：

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有 IPsec 配置（即全局生命期和转换集）。
shape	启用流量整形。
priority	启用优先级队列。
show running-config crypto map	显示所有加密映射的所有配置。

crypto ipsec ikev1 transform-set

要创建或删除 IKEv1 转换集，请在全局配置模式下使用 **crypto ipsec ikev1 transform-set** 命令。要删除转换集，请使用此命令的 **no** 形式。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

no crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

语法说明

authentication	（可选）指定以下身份验证方法之一以确保 IPsec 数据流的完整性： **esp-md5-hmac** 使用 MD5/HMAC-128 作为散列算法。 **esp-sha-hmac** 使用 SHA/HMAC-160 作为散列算法。 **esp-none** 不使用 HMAC 身份验证。
encryption	指定以下加密方法之一以保护 IPsec 数据流： **esp-aes** 使用具有 128 位密钥的 AES。 **esp-aes-192** 使用具有 192 位密钥的 AES。 **esp-aes-256** 使用具有 256 位密钥的 AES。 **esp-des** 使用具有 56 位密钥的 DES-CBC。 **esp-3des** 使用三重 DES 算法。 **esp-null** 不使用加密。
transform-set-name	正创建或修改的转换集的名称。要查看配置中已存在的转换集，请输入 **show running-config ipsec** 命令。

默认值

默认身份验证设置为 esp-none（无身份验证）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。
7.2(1)	重写了本节。
8.4(1)	添加了 **ikev1** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

此命令标识转换集要使用的 IPsec 加密和散列算法。

配置转换集后，将其分配到加密映射。您可以将最多六个转换集分配到一个加密映射。当对等设备尝试建立 IPsec 会话时，ASA 使用每个加密映射的访问列表评估对等设备，直到找到匹配项。然后，ASA 使用转换集中分配到加密映射的设置评估所有协议、算法和对等设备协商的其他设置，直到找到匹配项。如果 ASA 将对等设备的 IPsec 协商与转换集中的设置匹配，它会将这些设置作为其 IPsec 安全关联的一部分应用于受保护的流量。如果 ASA 无法将对等设备与访问列表匹配且找不到对等设备与分配到加密映射的转换集中设置的确切匹配，则它会终止 IPsec 会话。

您可以先指定加密或身份验证。您可以指定加密而不指定身份验证。如果您在正创建的转换集中指定身份验证，必须为其指定加密。如果您在正修改的转换集中仅指定身份验证，则转换集保留其当前加密设置。

如果使用 AES 加密，我们建议您也在全局配置模式下使用 **isakmp policy priority group 5** 命令以分配 Diffie-Hellman 组 5 来适应 AES 提供的大型密钥大小。

提示　当将转换集应用到加密映射或动态加密映射并查看分配到该映射的转换集时，如果转换集的名称反映其配置，将非常有用。例如，下面第一个示例中的名称 “3des-md5” 显示转换集中使用的加密和身份验证。该名称后的值是分配到转换集的实际加密和身份验证设置。

示例

以下命令展示所有可能的加密和身份验证选项，不包括未指定加密和身份验证的那些选项：

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac
ciscoasa(config)#
```

相关命令

命令	说明
show running-config ipsec	显示所有转换集的配置。
crypto map set transform-set	指定要在加密映射条目中使用的转换集。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
show running-config crypto map	显示加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。

crypto ipsec ikev1 transform-set mode transport

要为 IPsec IKEv1 连接指定传输模式，请在全局配置模式下使用 **crypto ipsec ikev1 transform-set mode transport** 命令。要删除命令，请使用此命令的 **no** 形式。

crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

no crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

语法说明

transform-set-name	正修改的转换集的名称。要查看配置中已存在的转换集，请输入 **show running-config ipsec** 命令。

默认值

传输模式的默认设置为禁用。IPsec 使用网络隧道模式。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	重写了此命令。
8.4(1)	添加了 **ikev1** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

使用 **crypto ipsec ikev1 transform-set mode transport** 命令指定 IPsec 的主机到主机传输模式，而不是默认的网络隧道模式。

示例

以下命令展示所有可能的加密和身份验证选项，不包括未指定加密和身份验证的那些选项：

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

相关命令

命令	说明
show running-config ipsec	显示所有转换集的配置。
crypto map set transform-set	指定要在加密映射条目中使用的转换集。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
show running-config crypto map	显示加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。

第 10 章

crypto isakmp disconnect-notify 至 cxsc auth-proxy port 命令

crypto isakmp disconnect-notify

要启用面向对等设备的断开连接通知，请在全局配置模式下使用 **crypto isakmp disconnect-notify** 命令。要禁用断开连接通知，请使用此命令的 **no** 形式。

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

语法说明

此命令没有任何参数或关键字。

默认值

默认值为禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp disconnect-notify** 命令。
7.2.(1)	**crypto isakmp disconnect-notify** 命令取代了 **isakmp disconnect-notify** 命令。
9.0(1)	增加了多情景模式支持。

使用指南

您可以使用以下删除原因向对等设备启用断开连接通知：

- IKE_DELETE_RESERVED = 0
  代码无效。不发送。
- IKE_DELETE_BY_ERROR = 1
  预期保持连接的响应或任何其他 IKE 数据包 ACK 时因超时或失败而发生的传输错误。默认文本是 “Connectivity to client lost”（客户端连接中断）。
- IKE_DELETE_BY_USER_COMMAND = 2
  SA 已被用户或管理员主动人工删除。默认文本是 “Manually Disconnected by Administrator”（已被管理员手动断开）。
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3
  SA 已到期。默认文本是 “Maximum Configured Lifetime Exceeded”（超过了配置的最长生命期）。
- IKE_DELETE_NO_ERROR = 4
  未知错误导致了删除。
- IKE_DELETE_SERVER_SHUTDOWN = 5
  服务器正在关闭。

- IKE_DELETE_SERVER_IN_FLAMES = 6
  服务器存在一些严重问题。默认文本是 “Peer is having heat problems”（对等设备有问题）。
- IKE_DELETE_MAX_CONNECT_TIME = 7
  活动隧道允许的最长时间已到。此原因与 EXPIRED_LIFETIME 不同，它表示 IKE 协商 / 控制的整个隧道将会断开，而不只是这一个 SA。默认文本是 “Maximum Configured Connection Time Exceeded”（已超过配置的最长连接时间）。
- IKE_DELETE_IDLE_TIMEOUT = 8
  隧道的空闲时间已达到允许的最长时间；因此 IKE 协商的整个隧道已断开，而不只是这一个 SA。默认文本是 “Maximum Idle Time for Session Exceeded”（已超过会话的最长空闲时间）。
- IKE_DELETE_SERVER_REBOOT = 9
  服务器正在重新启动。
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10
  第 2 阶段提议不匹配。
- IKE_DELETE_FIREWALL_MISMATCH = 11
  防火墙参数不匹配。
- IKE_DELETE_CERT_EXPIRED = 12
  需要用户证书。默认消息为 “User or Root Certificate has Expired”（用户或根证书已过期）。
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13
  不允许客户端类型或版本。
- IKE_DELETE_FW_SERVER_FAIL = 14
  无法连接 Zone Integrity 服务器。
- IKE_DELETE_ACL_ERROR = 15
  从 AAA 下载的 ACL 无法插入。默认消息为 “ACL parsing error”（ACL 解析错误）。

示例

以下示例在全局配置模式下输入，启用面向对等设备的断开连接通知：

```
ciscoasa(config)# crypto isakmp disconnect-notify
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp identity

要设置将发送到对等设备的第 1 阶段 ID，请在全局配置模式下使用 **crypto isakmp identity** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

语法说明

address	使用交换 ISAKMP 身份信息的主机的 IP 地址。
auto	按连接类型确定 ISAKMP 协商；用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN。
hostname	使用交换 ISAKMP 身份信息的主机的完全限定域名（默认）。此名称包含主机名和域名。
key-id *key_id_string*	指定远程对等设备用来查找预共享密钥的字符串。

默认值

默认 ISAKMP 身份是 **crypto isakmp identity auto**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp identity** 命令。
7.2(1)	**crypto isakmp identity** 命令取代了 **isakmp identity** 命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例在全局配置模式下输入，根据连接类型，在用于与 IPsec 对等设备通信的接口上启用 ISAKMP 协商：

```
ciscoasa(config)# crypto isakmp identity auto
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp nat-traversal

要全局启用 NAT 穿越，请确认已在全局配置模式下启用 ISAKMP（可使用 **crypto isakmp enable** 命令启用）。要禁用 NAT 穿越，请使用此命令的 **no** 形式。

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

语法说明

natkeepalive	设置 NAT 保持连接的间隔时间：10-3600 秒。默认值为 20 秒。

默认值

默认启用 NAT 穿越。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp nat-traversal** 命令。
7.2.(1)	**crypto isakmp nat-traversal** 命令取代了 **isakmp nat-traversal** 命令。
8.0(2)	默认启用 NAT 穿越。
9.0(1)	增加了多情景模式支持。

使用指南

NAT（包括 PAT）用于许多也使用 IPsec 的网络，但存在许多不兼容，使 IPsec 数据包无法成功穿越 NAT 设备。NAT 穿越使 ESP 数据包可通过一个或多个 NAT 设备。

ASA 支持 NAT 穿越，如 IETF“UDP Encapsulation of IPsec Packets”（IPsec 数据包的 UDP 封装）草案的第 2 版和第 3 版（可在 http://www.ietf.org/html.charters/ipsec-charter.html 下载）所述，并且动态和静态加密映射均支持 NAT 穿越。

此命令在 ASA 上全局启用 NAT-T。要在加密映射条目中禁用，请使用 **crypto map set nat-t-disable** 命令。

示例

以下示例在全局配置模式下输入，它先启用 ISAKMP，再设置保持连接间隔为 30 秒的 NAT 穿越：

```
ciscoasa(config)# crypto isakmp enable
ciscoasa(config)# crypto isakmp nat-traversal 30
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp policy authentication

要在 IKE 策略中指定身份验证方法，请在全局配置模式下使用 **crypto isakmp policy authentication** 命令。要删除 ISAKMP 身份验证方法，请使用相关的 **clear configure** 命令。

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

语法说明

crack	指定 IKE CRACK 作为身份验证方法。
pre-share	指定预共享密钥为身份验证方法。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
rsa-sig	指定 RSA 签名为身份验证方法。 RSA 签名提供 IKE 协商的不可否认性。这基本上意味着您可以向第三方证明您是否已与对等设备进行 IKE 协商。

默认值

默认 ISAKMP 策略身份验证是**预共享**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp policy authentication** 命令。
7.2.(1)	**crypto isakmp policy authentication** 命令取代了 **isakmp policy authentication** 命令。

使用指南

IKE 策略定义一组用于 IKE 协商的参数。

如果指定 RSA 签名，您必须配置 ASA 及其对等设备以从 CA 服务器获取证书。如果指定预共享密钥，必须在 ASA 及其对等设备中分别配置这些预共享密钥。

示例

以下示例在全局配置模式下输入，它展示如何使用 **crypto isakmp policy authentication** 命令。本示例设置将在优先级编号为 40 的 IKE 策略中使用的 RSA 签名的身份验证方法。

```
ciscoasa(config)# crypto isakmp policy 40 authentication rsa-sig
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp policy encryption

要指定 IKE 策略中使用的加密算法，请在全局配置模式下使用 **crypto isakmp policy encryption** 命令。要将加密算法重置为默认值 **des**，请使用此命令的 **no** 形式。

crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

no crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

语法说明

3des	指定在 IKE 策略中使用三重 DES 加密算法。
aes	指定将在 IKE 策略中使用的加密算法为带 128 位密钥的 AES。
aes-192	指定将在 IKE 策略中使用的加密算法为带 192 位密钥的 AES。
aes-256	指定将在 IKE 策略中使用的加密算法为带 256 位密钥的 AES。
des	指定将在 IKE 策略中使用的加密算法为 56 位 DES-CBC。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

默认值

默认 ISAKMP 策略加密算法为 **3des**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp policy encryption** 命令。
7.2.(1)	**crypto isakmp policy encryption** 命令取代了 **isakmp policy encryption** 命令。

示例

以下示例在全局配置模式下输入，它展示 **crypto isakmp policy encryption** 命令的使用；它将 128 位密钥 AES 加密设置为要在优先级编号为 25 的 IKE 策略中使用的算法。

```
ciscoasa(config)# crypto isakmp policy 25 encryption aes
```

以下示例在全局配置模式下输入，它设置将在优先级编号为 40 的 IKE 策略中使用的 3DES 算法。

```
ciscoasa(config)# crypto isakmp policy 40 encryption 3des
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp policy group

要为 IKE 策略指定 Diffie-Hellman 组，请在全局配置模式下使用 **crypto isakmp policy group** 命令。要将 Diffie-Hellman 组标识符重置为默认值，请使用此命令的 **no** 形式。

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

语法说明

group 1	指定在 IKE 策略中使用 768 位 Diffie-Hellman 组。此值为默认值。
group 2	指定在 IKE 策略中使用 1024 位 Diffie-Hellman 组 2。
group 5	指定在 IKE 策略中使用 1536 位 Diffie-Hellman 组 5。
priority	唯一标识 IIKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

默认值

默认组策略是组 2。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp policy group** 命令。
7.2.(1)	**crypto isakmp policy group** 命令取代了 **isakmp policy group** 命令。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。

使用指南

IKE 策略定义一组在 IKE 协商期间使用的参数。

有三个组选项：768 位（DH 组 1）、1024 位（DH 组 2）和 1536 位（DH 组 5）。1024 位和 1536 位 Diffie-hellman 组提供更强的安全性，但需要更多 CPU 时间来执行。

注意　思科 VPN 客户端 3.x 版或更高版本要求 ISAKMP 策略使用 DH 组 2。（如果配置 DH 组 1，思科 VPN 客户端无法连接。）

只有授权使用 VPN-3DES 的 ASA 提供 AES 支持。由于 AES 提供大型密钥，ISAKMP 协商应使用 Diffie-hellman (DH) 组 5，而不是组 1 或组 2。要配置组 5，请使用 **crypto isakmp policy priority group 5** 命令。

示例

以下示例在全局配置模式下输入，它展示如何使用 **crypto isakmp policy group** 命令。本示例设置组 2（1024 位 Diffie Hellman）以用于优先级编号为 40 的 IKE 策略。

```
ciscoasa(config)# crypto isakmp policy 40 group 2
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp policy hash

要为 IKE 策略指定哈希算法，请在全局配置模式下使用 **crypto isakmp policy hash** 命令。要将哈希算法重置为默认值 SHA-1，请使用此命令的 **no** 形式。

crypto isakmp policy *priority* hash {**md5** | **sha**}

no crypto isakmp policy *priority* **hash**

语法说明

md5	指定 MD5（HMAC 变体）作为 IKE 策略的哈希算法。
priority	唯一标识优先级并将其分配到策略。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
sha	指定 SHA-1（HMAC 变体）作为 IKE 策略的哈希算法。

默认值

默认哈希算法是 SHA-1（HMAC 变体）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp policy hash** 命令。
7.2.(1)	**crypto isakmp policy hash** 命令取代了 **isakmp policy hash** 命令。

使用指南

IKE 策略定义一组将在 IKE 协商期间使用的参数。

有两个散列算法选项：SHA-1 和 MD5。MD5 的摘要较小，被认为略快于 SHA-1。

示例

以下示例在全局配置模式下输入，它展示如何使用 **crypto isakmp policy hash** 命令。本示例为优先级编号为 40 的 IKE 策略指定 MD5 哈希算法。

```
ciscoasa(config)# crypto isakmp policy 40 hash  md5
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp policy lifetime

要指定 IKE 安全关联到期之前的生命期，请在全局配置模式下使用 **crypto isakmp policy lifetime** 命令。要将安全关联生命期重置为默认值 86,400 秒（一天），请使用此命令的 **no** 形式。

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

语法说明

priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
seconds	指定每个安全关联在到期之前应存在多少秒。要提出有限生命期，请使用介于 120 到 2147483647 之间的整数秒。要提出无限生命期，请使用 0 秒。

默认值

默认值为 86,400 秒（一天）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp policy lifetime** 命令。
7.2.(1)	**crypto isakmp policy lifetime** 命令取代了 **isakmp policy lifetime** 命令。

使用指南

IKE 开始协商时，会寻求使其自身对话的安全参数达成一致。然后每个对等设备的安全关联都会参考达成一致的参数。对等设备会保留安全关联，直到生命期到期。如果对等设备未提出生命期，您可以指定无限生命期。安全关联到期之前，后续 IKE 协商可以使用它，这可以在设置新 IPsec 安全关联时节省时间。在当前安全关联到期之前，对等设备将协商新的安全关联。

生命期越长，ASA 设置将来 IPsec 安全关联的速度就越快。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间（大约每隔几分钟再生一次）。建议接受默认值。

注意　如果 IKE 安全关联设置为无限生命期，但对等设备提出有限生命期，则使用与对等设备协商的有限生命期。

示例

以下示例在全局配置模式下输入，将优先级编号为 40 的 IKE 策略的 IKE 安全关联生命期设置为 50,400 秒（14 小时）：

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 50400
```

以下示例在全局配置模式下输入，将 IKE 安全关联设置为无限生命期：

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 0
```

相关命令

clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto isakmp reload-wait

要允许在重新启动 ASA 之前等待所有活动会话自行终止，请在全局配置模式下使用 **crypto isakmp reload-wait** 命令。要禁止等待活动会话终止并继续重新启动 ASA，请使用此命令的 **no** 形式。

crypto isakmp reload-wait

no crypto isakmp reload-wait

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了 **isakmp reload-wait** 命令。
7.2.(1)	**crypto isakmp reload-wait** 命令取代了 **isakmp reload-wait** 命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例在全局配置模式下输入，告知 ASA 等待至所有活动会话均终止后再重新启动：

```
ciscoasa(config)# crypto isakmp reload-wait
```

相关命令

命令	说明
clear configure crypto isakmp	清除所有 ISAKMP 配置。
clear configure crypto isakmp policy	清除所有 ISAKMP 策略配置。
clear crypto isakmp sa	清除 IKE 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的配置。

crypto key generate rsa

要生成身份证书的 RSA 密钥对，请在全局配置模式下使用 **crypto key generate rsa** 命令。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**] **dsa** [**label name** | **elliptic-curve** [**256** | **384** | **521**]

语法说明

dsa [**label name**]	生成密钥对时使用 Suite B EDCSA 算法。
elliptic-curve [**256** | **384** | **521**]	生成密钥对时使用 Suite B EDCSA 算法。
general-keys	生成一对通用密钥。这是默认密钥对类型。
label *key-pair-label*	指定要与密钥对关联的名称。此密钥对必须有唯一标签。如果尝试创建另一个具有相同标签的密钥，ASA 将显示一条警告消息。如果在密钥生成时未提供标签，密钥对将静态命名为 Default-RSA-Key。
modulus *size*	指定密钥对的系数大小：512、768、1024 和 2048。默认系数大小是 1024。
noconfirm	抑制所有交互式提示。
usage-keys	生成两个密钥对，一个用于签名，一个用于加密。这意味着需要两个相应身份的证书。

默认值

默认密钥对类型是**通用密钥**。默认系数大小是 1024。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **crypto key generate rsa** 命令生成 RSA 密钥对，以支持 SSL、SSH 和 IPsec 连接。生成的密钥对以标签标识，该标签可作为命令语法的一部分提供。未引用密钥对的信任点可以使用默认密钥对 Default-RSA-Key。SSH 连接始终使用此密钥。这不会影响 SSL，因为除非信任点配置证书或密钥，否则 SSL 会动态生成自己的证书或密钥。

注　用于存储密钥对的 NVRAM 空间容量根据 ASA 平台而有所不同。如果生成的密钥对超过 30 个，可能会达到限制。

注　仅 ASA 5580、5585 或更新平台才支持 4096 位 RSA 密钥。

注意事项　许多使用其 RSA 密钥对超过 1024 位的身份证书的 SSL 连接，可能导致 ASA 耗用过多 CPU，从而拒绝无客户端登录。

示例

以下示例在全局配置模式下输入，生成带标签 mypubkey 的 RSA 密钥对：

```
ciscoasa(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
ciscoasa(config)#
```

以下示例在全局配置模式下输入，它会无意中尝试生成带标签 mypubkey 的重复 RSA 密钥对：

```
ciscoasa(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them?[yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
ciscoasa(config)#
```

以下示例在全局配置模式下输入，生成带默认标签的 RSA 密钥对：

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin.Please wait...
ciscoasa(config)#
```

以下示例在全局配置模式下输入，因为 RSA 密钥对保存空间不足而生成警告消息：

```
ciscoasa(config)# crypto key generate rsa label mypubkey mod 2048
INFO: The name for the keys will be: mypubkey
Keypair generation process begin.Please wait...
NV RAM will not have enough space to save keypair mypubkey.Remove any unnecessary keypairs
and save the running config before using this keypair.
ciscoasa(config)#
```

相关命令

命令	说明
crypto key zeroize	删除 RSA 密钥对。
show crypto key	显示 RSA 密钥对。

crypto key zeroize

要删除指定类型（rsa 或 dsa）的密钥对，请在全局配置模式下使用 **crypto key zeroize** 命令。

crypto key zeroize {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

语法说明

default	删除不带标签的 RSA 密钥对。此关键字仅适用于 RSA 密钥对。
dsa	指定 DSA 为密钥类型。
label *key-pair-label*	删除指定类型（**rsa** 或 **dsa**）的密钥对。如果不提供标签，ASA 将删除指定类型的所有密钥对。
noconfirm	抑制所有交互式提示。
rsa	指定 RSA 为密钥类型。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在全局配置模式下输入，删除所有 RSA 密钥对：

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys?[yes/no] y
ciscoasa(config)#
```

相关命令

命令	说明
crypto key generate dsa	生成身份证书的 DSA 密钥对。
crypto key generate rsa	生成身份证书的 RSA 密钥对。

crypto large-cert-acceleration enable

要允许 ASA 在硬件中执行 2048 位 RSA 密钥操作，请在全局配置模式下使用 **crypto large-cert-acceleration enable** 命令。要在软件中执行 2048 位 RSA 密钥操作，请使用 **no crypto large-cert-acceleration enable** 命令。

crypto large-cert-acceleration enable

no crypto large-cert-acceleration enable

语法说明

此命令没有关键字或参数。

默认值

默认在软件中执行 2048 位 RSA 密钥操作。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(3)	引入了此命令。

使用指南

此命令只适用于 ASA 5510、ASA 5520、ASA 5540 和 5550， 不适用于 ASA 5580。

示例

以下示例展示已在硬件中启用 2048 位 RSA 密钥操作。

```
ciscoasa (config)# show running-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
ciscoasa (config)#
```

相关命令

命令	说明
clear configure crypto	清除具有其余加密配置的 2048 位 RSA 密钥配置。
show running-config crypto	显示具有其余加密配置的 2048 位 RSA 密钥配置。

crypto map interface

要将以前定义的加密映射集应用到接口，请在全局配置模式下使用 **crypto map interface** 命令。要从接口删除加密映射集，请使用此命令的 **no** 形式。

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

语法说明

interface-name	指定要用于与 VPN 对等设备建立隧道的 ASA 接口。如果启用 ISAKMP，并且您使用 CA 获取证书，此接口应使用 CA 证书中指定的地址。
map-name	指定加密映射集的名称。
ipv6-local-address *ipv6-address*	指定 IPv6 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.3(1)	添加了 **ipv6-local-address** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

使用此命令将加密映射集分配到任何活动的 ASA 接口。ASA 支持 IPsec 终止于任何及所有活动接口。必须先将加密映射集分配到接口，然后该接口才可提供 IPsec 服务。

只能将一个加密映射集分配到一个接口。如果多个加密映射条目的映射名称相同，但序列号不同，则它们属于同一映射集并且全部应用到接口。ASA 先评估序列号最小的加密映射条目。

当接口上配置有多个 IPv6 地址时使用 **ipv6-local-address** 关键字，并且在 IPv6 环境中配置 ASA 以支持局域网至局域网 VPN 隧道。

注意　ASA 可让您即时更改加密映射、动态映射和 IPsec 设置。如果您更改，ASA 只减少受更改影响的连接。如果更改与加密映射关联的现有访问列表，特别是通过删除访问列表中的条目进行更改，则只会减少关联的连接。基于访问列表中其他条目的连接不受影响。

每个静态加密映射必须定义三部分：访问列表、转换集和 IPsec 对等设备。如果缺少其中一部分，加密映射就不完整，并且 ASA 会移至下一个条目。但是，如果加密映射与访问列表匹配，但不符合另外一个或两个要求，此 ASA 会丢弃流量。

请使用 **show running-config crypto map** 命令确保每个加密映射完整。要修复某个不完整的加密映射，请删除该加密映射，添加缺少的条目，然后重新应用它。

示例

以下示例在全局配置模式下输入，将名为 mymap 的加密映射集分配到外部接口。当流量通过外部接口时，ASA 将使用 mymap 集中的所有加密映射条目评估它。当出站通信与其中一个 mymap 加密映射条目中的访问列表匹配时，ASA 将使用该加密映射条目的配置建立安全关联。

```
ciscoasa(config)# crypto map mymap interface outside
```

以下示例展示加密映射最低配置要求：

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap set transform-set my_t_set1
ciscoasa(config)# crypto map mymap set peer 10.0.0.1
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map ipsec-isakmp dynamic

若需要指定的加密映射条目引用现有动态加密映射，请在全局配置模式下使用 **crypto map ipsec-isakmp dynamic** 命令。要删除交叉引用，请使用此命令的 **no** 形式。

使用 **crypto dynamic-map** 命令创建动态加密映射条目。在创建动态加密映射集后，使用 **crypto map ipsec-isakmp dynamic** 命令将动态加密映射集添加到静态加密映射。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

语法说明

dynamic-map-name	指定引用现有动态加密映射的加密映射条目名称。
ipsec-isakmp	指示 IKE 为此加密映射条目建立 IPsec 安全关联。
map-name	指定加密映射集的名称。
seq-num	指定分配给加密映射条目的编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，删除了 **ipsec-manual** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

在定义加密映射条目之后，可以使用 **crypto map interface** 命令将动态加密映射集分配到接口。

动态加密映射提供两项功能：过滤 / 分类要保护的流量，以及定义应用到该流量的策略。第一项功能影响接口上的流量流；第二项功能影响代表该流量执行（通过 IKE）的协商。

IPsec 动态加密映射识别以下内容：

- 要保护的流量
- 与其建立安全关联的 IPsec 对等设备
- 要用于受保护流量的转换集
- 如何使用或管理密钥和安全关联

加密映射集是加密映射条目的集合，每个条目的序列号 (*seq-num*) 不同，但映射名称相同。因此，对于指定的接口，您可以对转发到一个对等设备的特定流量应用指定的安全保护，对转发到同一或不同对等设备的其他流量应用 IPsec 安全保护。为实现此目的，需创建两个加密映射条目，它们的映射名称相同，但序列号不同。

不能随便用一个数字作为 *seq-num* 参数的编号。此编号会对加密映射集中的多个加密映射条目进行排名。序列号较低的加密映射条目先于序列号较高的映射条目进行评估；也就是说，序列号低的映射条目优先级更高。

注意　将加密映射链接到动态加密映射时，必须指定动态加密映射。这会将加密映射链接到之前使用 **crypto dynamic-map** 命令定义的现有动态加密映射。现在，您在加密映射条目转换后对其执行的任何更改都不会生效。例如，对映射集对等设置的更改不会生效。但 ASA 在运行时会存储更改。当动态加密映射转换回加密映射时，更改将会生效并显示在 **show running-config crypto map** 命令的输出中。ASA 在重新启动之前会一直保持这些设置。

示例

以下命令在全局配置模式下输入，配置加密映射 mymap 引用名为 test 的动态加密映射：

```
ciscoasa(config)# crypto map mymap ipsec-isakmp dynamic test
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map match address

要将访问列表分配到加密映射条目，请在全局配置模式下使用 **crypto map match address** 命令。要从加密映射条目删除访问列表，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

语法说明

acl_name	指定加密访问列表的名称。此名称应匹配所匹配的指定加密访问列表的 name 参数。
map-name	指定加密映射集的名称。
seq-num	指定分配给加密映射条目的编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

此命令对所有静态加密映射都是必要的。如果是定义动态加密映射（使用 **crypto dynamic-map** 命令），则此命令不是必要的，但强烈建议使用。

使用 **access-list** 命令定义访问列表。访问列表命中计数仅当隧道启动时才会增加。在隧道启动后，命中计数不会在每个数据包流上增加。如果隧道关闭后重新启动，命中计数就会增加。

ASA 使用访问列表将要使用 IPsec 加密保护的流量与不需要保护的流量区分开来。它保护匹配允许 ACE 的出站数据包，并确保匹配允许 ACE 的入站数据包获得保护。

当 ASA 将数据包匹配到 deny 语句时，它将使用加密映射中的其余 ACE 跳过数据包评估，并按顺序使用下一个加密映射中的 ACE 继续数据包评估。*级联 ACL* 涉及使用 deny ACE 来绕过 ACL 中其余 ACE 的评估，并且使用分配到加密映射集中下一个加密映射的 ACL 继续流量评估。由于您可以将每个加密映射与不同的 IPsec 设置关联，因此可以使用 deny ACE 将特殊流量从相应加密映射的进一步评估中排除，并且将特殊流量匹配到另一个加密映射中的 permit 语句，以提供或要求不同的安全保护。

注意　加密访问列表无法决定是允许还是拒绝流量通过接口。使用 **access-group** 命令直接应用到接口的访问列表做出该决定。

在透明模式下，目标地址应为 ASA 的 IP 地址 - 管理地址。透明模式下只允许到 ASA 的隧道。

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set connection-type

要为此加密映射条目指定备用站点到站点功能的连接类型，请在全局配置模式下使用 **crypto map set connection-type** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

no crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

语法说明

answer-only	指定此对等设备在初始属性交换时只响应入站 IKE 连接，以确定要连接的适当对等设备。
bidirectional	指定此对等设备可根据此加密映射条目接受和发起连接。这是所有站点到站点连接的默认连接类型。
map-name	指定加密映射集的名称。
originate-only	指定此对等设备发起第一次属性交换以确定要连接的适当对等设备。
seq-num	指定分配给加密映射条目的编号。
set connection-type	为此加密映射条目指定备用站点到站点功能的连接类型。有三种类型的连接：只应答、只发起和双向。

默认值

默认设置为双向。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。
9.0	增加了多情景模式支持。

使用指南

crypto map set connection-type 命令指定备用局域网至局域网功能的连接类型。它允许在连接的一端指定多个备用对等设备。

此功能仅在以下平台之间可用：

- 两个思科 ASA 5500 系列
- 思科 ASA 5500 系列与思科 VPN 3000 集中器
- 思科 ASA 5500 系列与运行思科 PIX 安全设备软件版本 7.0 或更高版本的安全设备

要配置备用局域网至局域网连接，建议使用 **originate-only** 关键字将连接的一端配置为只发起，使用 **answer - only** 关键字将具有多个备用设备的一端配置为只应答。在只发送端，使用 **crypto map set peer** 命令排列对等设备的优先级。只发送 ASA 会尝试与列表中的第一个对等设备协商。如果该对等设备未响应，ASA 将在列表中下移，尝试与其他对等设备协商，直到有对等设备响应或者列表结束。

以这种方式配置时，只发起对等设备最初会尝试建立专用隧道并与对等设备协商。然后，任一对等设备都可建立正常的局域网至局域网连接，并且来自任一端的数据都可以发起隧道连接。

在透明防火墙模式下，您可以看到此命令，但对属于已附加到接口的加密映射中的加密映射条目，连接类型值不能设置为只应答以外的任何值。

表 10-1 列出了所有支持的配置。其他组合可能导致不可预测的路由问题。

表 10-1　　支持的备用局域网至局域网连接类型

远端	中心端
只发起	只应答
双向	只应答
双向	双向

示例

以下示例在全局配置模式下输入，配置加密映射 mymap 并将连接类型设为只发起。

```
ciscoasa(config)# crypto map mymap 10 set connection-type originate-only
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set df-bit

要设置每签名算法 (SA) 不分段 (DF) 策略，请在全局配置模式下使用 **crypto map set df-bit** 命令。要禁用 DF 策略，请使用此命令的 **no** 形式。

crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

语法说明

name	指定加密映射集的名称。
priority	指定分配给加密映射条目的优先级。

默认值

默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

原始 DF 策略命令被保留，并且用作接口上的全局策略设置，但用于 SA 时被 **crypto map** 命令取代。

crypto map set ikev2 pre-shared-key

要指定 AnyConnect IKEv2 连接的预共享密钥，请在全局配置模式下使用 **crypto map set ikev2 pre-shared-key** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

语法说明

key	1 到 128 个字符的字母数字字符串。
map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

示例

以下示例配置预共享密钥 SKTIWHT：

```
ciscoasa(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set inheritance

要设置为此加密映射条目生成的安全关联粒度（单粒度或多粒度），请在全局配置模式下使用 **set inheritance** 命令。要删除此加密映射条目的继承设置，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

no crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

语法说明

data	为规则中指定的地址范围内的每个地址对指定一个隧道。
map-name	指定加密映射集的名称。
rule	为此加密映射关联的每个 ACL 条目指定一个隧道。此为默认值。
seq-num	指定分配到加密映射条目的编号。
set inheritance	指定继承的类型：**数据或规则**。继承允许为每个安全策略数据库 (SPD) 生成一个安全关联 (SA)，或者为范围中的每个地址生成多个安全 SA。

默认值

默认值为 **rule**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

此命令仅在 ASA 发起隧道时运行，在响应隧道时不运行。使用数据设置可能会创建大量 IPsec SA。这会占用内存，而且减少整体隧道。您应该仅为对安全极为敏感的应用使用数据设置。

示例

以下示例在全局配置模式下输入，配置加密映射 mymap 并将继承类型设为数据：

```
ciscoasa(config)# crypto map mymap 10 set inheritance data
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set nat-t-disable

要对基于此加密映射条目的连接禁用 NAT-T，请在全局配置模式下使用 **crypto map set nat-t-disable** 命令。要对此加密映射条目启用 NAT-T，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

语法说明

map-name	指定加密映射集的名称。
seq-num	指定分配给加密映射条目的编号。

默认值

此命令的默认设置不是打开（因此默认启用 NAT-T）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

使用 **isakmp nat-traversal** 命令全局启用 NAT-T。然后可以使用 **crypto map set nat-t-disable** 命令对特定加密映射条目禁用 NAT-T。

示例

以下命令在全局配置模式下输入，对名为 mymap 的加密映射条目禁用 NAT-T：

```
ciscoasa(config)# crypto map mymap 10 set nat-t-disable
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
isakmp nat-traversal	对所有连接启用 NAT-T。
show running-config crypto map	显示加密映射配置。

crypto map set peer

要在加密映射条目中指定 IPsec 对等设备，请在全局配置模式下使用 **crypto map set peer** 命令。使用此命令的 **no** 形式会从加密映射条目中删除 IPsec 对等设备。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

语法说明

hostname	通过 ASA **name** 命令定义的主机名指定对等设备。
ip_address	通过其 IP 地址（IPv4 或 IPv6）指定对等设备。
map-name	指定加密映射集的名称。
peer	通过主机名或 IP 地址（IPv4 或 IPv6）在加密映射条目中指定 IPsec 对等设备。IKEv2 不支持多个对等设备。
seq-num	指定分配到加密映射条目的编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，允许最多 10 个对等地址。
9.0(1)	增加了多情景模式支持。

使用指南

此命令对所有静态加密映射都是必要的。如果是定义动态加密映射（使用 **crypto dynamic-map** 命令），此命令不是必要的，而且在大多数情况下不使用，因为对等设备通常未知。

配置多个对等设备相当于提供一个回退列表。对于每个隧道，ASA 会尝试与列表中的第一个对等设备协商。如果该对等设备未响应，ASA 将在列表中下移，尝试与其他对等设备协商，直到有对等设备响应或者列表结束。仅当使用备用局域网至局域网功能时（也就是说，在加密映射连接类型为只发起时）才可设置多个对等设备。有关详细信息，请参阅 **crypto map set connection-type** 命令。

注意　IKEv2 不支持多个对等设备。

示例

以下示例在全局配置模式下输入，它展示使用 IKE 建立安全关联的加密映射配置。在此示例中，您可以与 10.0.0.1 上的对等设备或 10.0.0.2 上的对等设备建立安全关联：

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap 10 set transform-set my_t_set1
ciscoasa(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set pfs

在全局配置模式下，使用 **crypto map set pfs** 命令设置 IPsec 在请求为此加密映射条目建立新安全关联时要求 PFS，或者设置 IPsec 在收到建立新安全关联的请求时要求 PFS。要指定 IPsec 不应要求 PFS，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

no crypto map *map-name seq-num* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

语法说明

group1	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 768 位 Diffie-Hellman 主模数组。
group2	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1024 位 Diffie-Hellman 主模数组。
group5	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1536 位 Diffie-Hellman 主模数组。
map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。

默认值

默认情况下 PFS 未设置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，添加了 Diffie-Hellman 组 7。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。
9.0(1)	增加了多情景模式支持。

使用指南

有了 PFS，每次协商新的安全关联时，就会发生新的 Diffie-Hellman 交换，这需要更多的处理时间。PFS 会添加另一层安全保护，因为，如果一个密钥被攻击者破解，只有通过该密钥发送的数据受到威胁。

在协商期间，此命令使 IPsec 在请求为加密映射条目建立新安全关联时要求 PFS。如果 **set pfs** 语句未指定组，ASA 将发送默认值（组 2）。

如果对等设备发起协商，并且本地配置指定 PFS，则对等设备必须执行 PFS 交换，否则协商会失败。如果本地配置不指定组，ASA 将使用默认值（组 2）。如果本地配置指定组 2 或组 5，该组必须是对等设备内容的一部分，否则协商会失败。

为使协商成功，必须在局域网至局域网隧道的两端都设置 PFS（无论是否有 Diffie-Hellman 组）。如有设置，这些组必须完全匹配。ASA 不接受对等设备的 PFS 提供的任何内容。

1536 位 Diffie-Hellman 主模数组（组 5）的安全性高于组 1 或组 2，但需要的处理时间比其他组长。

与思科 VPN 客户端交互时，ASA 不使用 PFS 值，而使用在第 1 阶段协商的值。

示例

以下示例在全局配置模式下输入，指定只要是为加密映射 mymap 10 协商新的安全关联，就应使用 PFS：

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 set pfs group2
```

相关命令

命令	说明
clear isakmp sa	删除活动的 IKE 安全关联。
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。
tunnel-group	配置隧道组及其参数。

crypto map set ikev1 phase1-mode

要指定在发起主要或积极连接时第 1 阶段使用的 IKEv1 模式，请在全局配置模式下使用 **crypto map set ikev1 phase1-mode** 命令。要删除第 1 阶段 IKEv1 协商的设置，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

语法说明

aggressive	指定第 1 阶段 IKEv1 协商的积极模式。
group1	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 768 位 Diffie-Hellman 主模数组。
group2	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1024 位 Diffie-Hellman 主模数组。
group5	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1536 位 Diffie-Hellman 主模数组。
main	指定第 1 阶段 IKEv1 协商的主要模式。
map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。

默认值

第 1 阶段默认模式为**主要**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。
8.4(1)	添加了 **ikev1** 关键字。
9.0(1)	增加了多情景模式支持。

使用指南

此命令仅适用于发起者模式；不适用于响应者模式。可以选择性包括积极模式的 Diffie-Hellman 组。若未包括，ASA 将使用组 2。

示例

以下示例在全局配置模式下输入，配置加密映射 mymap，并且将第 1 阶段模式设为积极，使用组 2：

```
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
ciscoasa(config)#
```

相关命令

命令	说明
clear isakmp sa	删除活动的 IKE 安全关联。
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set ikev2 phase1-mode

要指定在发起主要或积极连接时第 1 阶段使用的 IKEv2 模式，请在全局配置模式下使用 **crypto map set ikev2 phase1-mode** 命令。要删除第 1 阶段 IKEv2 协商的设置，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

语法说明

aggressive	指定第 1 阶段 IKEv2 协商的积极模式。
group1	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 768 位 Diffie-Hellman 主模数组。
group2	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1024 位 Diffie-Hellman 主模数组。
group5	指定 IPsec 在执行新的 Diffie-Hellman 交换时应使用 1536 位 Diffie-Hellman 主模数组。
main	指定第 1 阶段 IKEv2 协商的主要模式。
map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。

默认值

第 1 阶段默认模式为**主要**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。
9.0(1)	增加了多情景模式支持。

使用指南

此命令仅适用于发起者模式；不适用于响应者模式。可以选择性包括积极模式的 Diffie-Hellman 组。若未包括，ASA 将使用组 2。

示例

以下示例在全局配置模式下输入，配置加密映射 mymap，并且将第 1 阶段模式设为积极，使用组 2：

```
ciscoasa(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
ciscoasa(config)#
```

相关命令

命令	说明
clear isakmp sa	删除活动的 IKE 安全关联。
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set reverse-route

要对基于此加密映射条目的所有连接启用反向路由注入，请在全局配置模式下使用 **crypto map set reverse-route** 命令。要对基于此加密映射条目的任何连接禁用反向路由注入，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set reverse-route**

no crypto map *map-name seq-num s***et reverse-route**

语法说明

map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。

默认值

此命令的默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。

示例

以下示例在全局配置模式下输入，对名为 mymap 的加密映射启用反向路由注入。

```
ciscoasa(config)# crypto map mymap 10 set reverse-route
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set security-association lifetime

要覆盖（对于特定加密映射条目）在协商 IPsec 安全关联时使用的全局生命期值，请在全局配置模式下使用 **crypto map set security-association lifetime** 命令。要将加密映射条目的生命期值设为全局值，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | unlimited}

no crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes* | unlimited}

语法说明

kilobytes	指定使用特定安全关联的对等设备之间在该安全关联到期前可通过的流量（以千字节为单位）。 默认值为 4,608,000 千字节。
map-name	指定加密映射集的名称。
seconds	指定安全关联在到期之前生存的秒数。默认值为 28,800 秒（8 小时）。
seq-num	指定分配到加密映射条目的编号。
unlimited	当 ASA 是隧道的发起者时，在快速模式 1 下不发送千字节数据包。

默认值

默认千字节数为 4,608,000 ；默认秒数为 28,800。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。
9.1(2)	添加了无限制参数。

使用指南

加密映射的安全关联根据全局生命期进行协商。

IPsec 安全关联使用共享密钥。这些密钥及其安全关联一起超时。

假设特定加密映射条目配置了生命期值，则当 ASA 在安全关联协商期间请求新的安全关联时，它会在向对等设备发出的请求中指定其加密映射生存时间值；它将使用这些值作为新安全关联的生命期。当 ASA 收到对等设备的协商请求时，它会使用对等设备提出的生命期值或本地配置的生命期值（取较小者）作为新安全关联的生命期。

有两个生命期：定时生命期和流量生命期。会话密钥和安全关联在达到第一个生命期后到期。您可以使用一个命令同时指定两者。

注意　ASA 可让您即时更改加密映射、动态映射和 IPsec 设置。如果您更改，ASA 只减少受更改影响的连接。如果更改与加密映射关联的现有访问列表，尤其是通过删除访问列表中的条目进行更改，结果只会减少关联的连接。基于访问列表中其他条目的连接不受影响。

要更改定时生命期，请使用 **crypto map set security-association lifetime seconds** 命令。定时生命期会使密钥和安全关联在经过指定的秒数后超时。

示例

以下命令在全局配置模式下输入，以秒和千字节指定加密映射 mymap 的安全关联生命期：

```
ciscoasa(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。

crypto map set ikev1 transform-set

要指定在加密映射条目中使用的 IKEv1 转换集，请在全局配置模式下使用 **crypto map set transform-set** 命令。要从加密映射条目中删除转换集的名称，请使用此命令的 **no** 形式并在命令中包含指定的转换集名称。要指定所有转换集或不指定任何转换集并且删除加密映射条目，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set**

语法说明

map-name	指定加密映射集的名称。
seq-num	指定对应于加密映射条目的序列号。
transform-set-name1 *transform-set-name11*	指定转换集的一个或多个名称。此命令中指定的任何转换集都必须在 **crypto ipsec transform-set** 命令中定义。每个加密映射条目支持最多 11 个转换集。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	修改了加密映射条目中的转换集最大数。
9.0(1)	增加了多情景模式支持。

使用指南

此命令对于所有加密映射条目都是必要的。

IPsec 发起的相对端的对等设备使用安全关联的第一个匹配转换集。如果本地 ASA 发起协商，则在 **crypto map** 命令中指定的顺序将确定 ASA 向对等设备显示转换集内容的顺序。如果对等设备发起协商，本地 ASA 将使用加密映射条目中第一个与对等设备发送的 IPsec 参数匹配的转换集。

如果 IPsec 发起的相对端的对等设备与转换集的值不匹配，IPsec 不会建立安全关联。发起者将丢弃流量，因为没有安全关联保护它。

要更改转换集列表，请指定新列表以替换旧列表。

如果使用此命令修改加密映射，ASA 只修改具有您指定的序列号的加密映射条目。例如，如果您输入以下命令，ASA 将在最后位置插入名为 56des-sha 的转换集：

```
ciscoasa(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
ciscoasa(config)# crypto map map1 1 transform-set 56des-sha
ciscoasa(config)#
```

对以下命令的响应显示了前两个命令的累积效应：

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

要重新配置加密映射条目中的转换集序列，请删除该条目，指定映射名称和序列号；然后重新创建条目。例如，以下命令重新配置名为 map2、序列号为 3 的加密映射条目：

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

示例

crypto ipsec transform-set（创建或删除转换集）部分显示十个转换集命令。以下示例创建一个名为 map2 的加密映射条目，其中包括相同的十个转换集：

```
ciscoasa(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

以下示例在全局配置模式下输入，它展示在 ASA 使用 IKE 建立安全关联时要求的最低加密映射配置：

```
ciscoasa(config)# crypto map map2 10 ipsec-isakmp
ciscoasa(config)# crypto map map2 10 match address 101
ciscoasa(config)# crypto map map2 set transform-set 3des-md5
ciscoasa(config)# crypto map map2 set peer 10.0.0.1
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	从配置中清除所有动态加密映射。
clear configure crypto map	从配置中清除所有加密映射。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
crypto ipsec transform-set	配置转换集。
show running-config crypto dynamic-map	显示动态加密映射配置。
show running-config crypto map	显示加密映射配置。

crypto map set ikev2 ipsec-proposal

要指定在加密映射条目中使用的 IKEv2 提议，请在全局配置模式下使用 **crypto map set ikev2 ipsec-proposal** 命令。要从加密映射条目中删除提议的名称，请使用此命令的 **no** 形式并在命令中包含指定的提议名称。要指定所有提议或不指定任何提议并且删除加密映射条目，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

语法说明

map-name	指定加密映射集的名称。
seq-num	指定对应于加密映射条目的序列号。
propsal-name1 *proposal-name11*	为 IKEv2 指定 IPsec 提议的一个或多个名称。此命令中指定的任何提议都必须在 **crypto ipsec ikev2 ipsec-proposal** 命令中定义。每个加密映射条目支持最多 11 个提议。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

对于所有加密映射条目，IKEv1 转换集或 IKEv2 提议是必要的。

IPsec IKEv2 发起的相对端的对等设备使用安全关联的第一个匹配提议。如果本地 ASA 发起协商，则在 **crypto map** 命令中指定的顺序将确定 ASA 向对等设备显示提议内容的顺序。如果对等设备发起协商，本地 ASA 将使用加密映射条目中第一个与对等设备发送的 IPsec 参数匹配的提议。

如果 IPsec 发起的相对端的对等设备与提议的值不匹配，IPsec 不会建立安全关联。发起者将丢弃流量，因为没有安全关联保护它。

要更改提议列表，请创建新列表并指定它以替换旧列表。

如果使用此命令修改加密映射，ASA 只修改具有您指定的序列号的加密映射条目。例如，如果您输入以下命令，ASA 将在最后位置插入名为 56des-sha 的提议：

```
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 128aes-md5 128aes-sha
192aes-md5
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 56des-sha
ciscoasa(config)#
```

对以下命令的响应显示了前两个命令的累积效应：

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

要重新配置加密映射条目中的提议序列，请删除该条目，指定映射名称和序列号；然后重新创建条目。例如，以下命令重新配置名为 *map2*、序列号为 3 的加密映射条目：

```
asa2(config)# no crypto map map2 3 set ikev2 ipsec-proposal
asa2(config)# crypto map map2 3 set ikev2 ipsec-proposal 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

示例

以下示例创建一个名为 map2 的加密映射条目，其中包括十个提议。

```
ciscoasa(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto dynamic-map	从配置中清除所有动态加密映射。
clear configure crypto map	从配置中清除所有加密映射。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
crypto ipsec transform-set	配置转换集。
show running-config crypto dynamic-map	显示动态加密映射配置。
show running-config crypto map	显示加密映射配置。

crypto map set tfc-packets

要在 IPsec SA 上启用虚拟 Traffic Flow Confidentiality (TFC) 数据包，请在全局配置模式下使用 **crypto map set tfc-packets** 命令。要在 IPsec SA 上禁用 TFC 数据包，请使用此命令的 **no** 形式。

crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

no crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

语法说明

name	指定加密映射集的名称。
priority	指定分配给加密映射条目的优先级。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令为加密映射配置现有 DF 策略（在 SA 级）。

crypto map set trustpoint

要指定信任点（用于标识要发送以在加密映射条目的第 1 阶段协商期间进行身份验证的证书），请在全局配置模式下使用 **crypto map set trustpoint** 命令。要从加密映射条目删除信任点，请使用此命令的 **no** 形式。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

语法说明

chain	（可选）发送证书链。CA 证书链包括从根证书到身份证书的证书层次结构中的所有 CA 证书。默认值为禁用（无链）。
map-name	指定加密映射集的名称。
seq-num	指定分配到加密映射条目的编号。
trustpoint-name	标识要在第 1 阶段协商期间发送的证书。默认值为 none。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

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

使用指南

以下加密映射命令适用于发起连接。有关响应者端的信息，请参阅 **tunnel-group** 命令。

示例

以下示例在全局配置模式下输入，为加密映射 mymap 指定名为 tpoint1 的信任点，并且包括证书链：

```
ciscoasa(config)# crypto map mymap 10 set trustpoint tpoint1 chain
ciscoasa(config)#
```

相关命令

命令	说明
clear configure crypto map	清除所有加密映射的所有配置。
show running-config crypto map	显示加密映射配置。
tunnel-group	配置隧道组。

crypto map set validate-icmp-errors

要指定是否验证通过 IPsec 隧道收到的发往专用网络上外部主机的传入 ICMP 错误消息，请在全局配置模式下使用 **crypto map set validate-icmp-errors** 命令。要从加密映射条目删除信任点，请使用此命令的 **no** 形式。

crypto map *name priority* **set validate-icmp-errors**

no crypto map *name priority* **set validate-icmp-errors**

语法说明

name	指定加密映射集的名称。
priority	指定分配给加密映射条目的优先级。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

以下加密映射命令仅适用于验证传入的 ICMP 错误消息。

csc

要让 ASA 向 CSC SSM 发送网络流量，请在类配置模式下使用 **csc** 命令。要删除配置，请使用此命令的 **no** 形式。

csc {**fail-open** | **fail-close**}

no csc

语法说明

fail-close	指定自适应 ASA 应在 CSC SSM 失败时阻止流量。这仅适用于类映射所选择的流量。其他未发送到 CSC SSM 的流量不受 CSC SSM 失败的影响。
fail-open	指定自适应 ASA 应在 CSC SSM 失败时允许流量。这仅适用于类映射所选择的流量。其他未发送到 CSC SSM 的流量不受 CSC SSM 失败的影响。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

从策略映射配置模式可进入类配置模式。

csc 命令配置安全策略以向 CSC SSM 发送相关类映射匹配的所有流量。这发生在 ASA 允许流量继续前往其目标之前。

您可以指定当 CSC SSM 不可用于扫描流量时 ASA 如何处理匹配的流量。**fail-open** 关键字指定即使 CSC SSM 不可用，也允许 ASA 流量继续前往目标。**fail-close** 关键字指定 ASA 在 CSC SSM 不可用时永远不让匹配的流量前往其目标。

CSC SSM 可扫描 HTTP、SMTP、POP3 和 FTP 流量。它仅当请求连接的数据包的目标端口是协议已知端口时才支持这些协议，也就是说，CSC SSM 只能扫描以下连接：

- 对 TCP 端口 21 开放的 FTP 连接
- HTTP connections opened to TCP port 80
- 对 TCP 端口 110 开放的 POP3 连接
- SMTP connections opened to TCP port 25

如果使用 **csc** 命令的策略选择对其他协议误用这些端口的连接，ASA 将数据包传送到 CSC SSM；而 CSC SSM 不扫描数据包就传送它们。

为了最大限度地提高 CSC SSM 的效率，请如下实施 **csc** 命令，配置策略使用的类映射：

- 只选择您希望 CSC SSM 扫描的支持协议。例如，如果您不希望扫描 HTTP 流量，请确保服务策略不会将 HTTP 流量转移至 CSC SSM。
- 只选择受 ASA 保护的风险可信主机的连接。这些连接从外部或不受信任的网络到内部网络。我们建议扫描以下连接：
  - 出站 HTTP 连接
  - 从 ASA 内部客户端到 ASA 外部服务器的 FTP 连接
  - 从 ASA 内部客户端到 ASA 外部服务器的 POP3 连接
  - 前往内部邮件服务器的传入 SMTP 连接

FTP 扫描

CSC SSM 仅当 FTP 会话的主要通道使用标准端口（即 TCP 端口 21）时才支持 FTP 文件传输扫描。

对于您希望被 CSC SSM 扫描的 FTP 流量，必须启用 FTP 检查。这是因为 FTP 对数据传输使用动态分配的辅助通道。ASA 确定为辅助通道分配的端口，并且打开针孔以允许数据传输。如果 CSC SSM 配置为扫描 FTP 数据，ASA 会将数据流量转移至 CSC SSM。

您可以全局应用 FTP 检查或者应用到 **csc** 命令所应用的同一接口。默认全局启用 FTP 检查。如果没有更改默认检查配置，无需进一步的 FTP 检查配置即可启用 CSC SSM 的 FTP 扫描。

有关 FTP 检查或默认检查配置的详细信息，请参阅 CLI 配置指南。

示例

ASA 应配置为将流量转移至从 HTTP、FTP 和 POP3 连接的内部网络客户端到外部网络的 CSC SSM 请求，以及从外部主机到 DMZ 网络上邮件服务器的传入 SMTP 连接。不应扫描从内部网络到 DMZ 网络中 Web 服务器的 HTTP 请求。

以下配置创建两个服务策略。第一个策略 csc_out_policy 应用到内部接口，并且使用 csc_out 访问列表确保扫描 FTP 和 POP3 的所有出站请求。csc_out 访问列表也可确保扫描从内部到外部接口上网络的 HTTP 连接，但该访问列表包括拒绝 ACE，会排除从内部到 DMZ 网络上服务器的 HTTP 连接。

第二个策略 csc_in_policy 应用到外部接口，并且使用 csc_in 访问列表确保 CSC SSM 扫描从外部接口到 DMZ 网络的 SMTP 和 HTTP 请求。扫描 HTTP 请求可确保避免对 Web 服务器进行 HTTP 文件上传。

```
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
ciscoasa(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0 eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

ciscoasa(config)# class-map csc_outbound_class
ciscoasa(config-cmap)# match access-list csc_out

ciscoasa(config)# policy-map csc_out_policy
ciscoasa(config-pmap)# class csc_outbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_out_policy interface inside

ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80
```

```
ciscoasa(config)# class-map csc_inbound_class
ciscoasa(config-cmap)# match access-list csc_in

ciscoasa(config)# policy-map csc_in_policy
ciscoasa(config-pmap)# class csc_inbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_in_policy interface outside
```

注意　必须启用 FTP 检查，使 CSC SSM 扫描 FTP 传输的文件。默认情况下启用 FTP 检测。

相关命令

命令	说明
class (policy-map)	为流量分类指定类映射。
class-map	创建用于策略映射的流量类映射。
match port	使用目标端口匹配流量。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
service-policy	通过将策略映射与一个或多个接口关联，创建安全策略。

csd enable

要对无客户端 SSL VPN 远程访问或使用 AnyConnect 客户端的远程访问启用思科安全桌面 (CSD)，请在 webvpn 配置模式下使用 **csd enable** 命令。要禁用 CSD，请使用此命令的 **no** 形式。

csd enable

no csd enable

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

对于向 ASA 发起的所有远程访问连接尝试，CSD 会全局启用或禁用，只有一个例外。

csd enable 命令执行以下操作：

1. 提供有效性检查，以补充之前的 **csd image** *path* 命令所执行的检查。
2. 在 disk0 中创建 sdesktop 文件夹（如果没有此文件夹）。
3. 在 sdesktop 文件夹中插入 data.xml（思科安全桌面配置）文件（如果没有此文件）。
4. 将 data.xml 从闪存设备加载到运行配置。
5. 启用 CSD。

注

- 您可以输入 **show webvpn csd** 命令来确定思科安全桌面是否启用。
- 在输入 **csd enable** 命令之前，必须在运行配置中输入 **csd image** *path* 命令。
- **no csd enable** 命令在运行配置中禁用 CSD。如果 CSD 禁用，则不能访问 CSD Manager，远程用户也无法使用 CSD。
- 如果传输或替换 data.xml 文件，请禁用 CSD，然后再启用，以将该文件加载到运行配置。
- 对于向 ASA 发起的所有远程访问连接尝试，CSD 会全局启用或禁用。您无法对单个连接配置文件或组策略启用或禁用 CSD。

例外：可对无客户端 SSL VPN 连接的连接配置文件进行配置，使得当计算机尝试使用组 URL 连接 ASA 并且 CSD 已全局启用时，CSD 不会在客户端计算机上运行。例如：

```
ciscoasa(config)# tunnel-group group-name webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://www.url-string.com
ciscoasa(config-tunnel-webvpn)# without-csd
```

示例

以下命令显示如何查看 CSD 映像的状态并启用该映像：

```
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
csd image	将命令中指定的 CSD 映像从路径中指定的闪存驱动器复制到运行配置。
show webvpn csd	识别 CSD（如果已启用）的版本。若未启用，CLI 将指示 “Secure Desktop is not enabled”（安全桌面未启用）。
without-csd	对无客户端 SSL VPN 会话的连接配置文件进行配置，使得当计算机尝试使用组 URL 连接 ASA 并且 CSD 已全局启用时，CSD 不会在客户端计算机上运行。

csd hostscan image

要安装或升级思科主机扫描分发软件包并将其添加到运行配置，请在 webvpn 配置模式下使用 **csd hostscan image** 命令。要从运行配置删除主机扫描分发软件包，请使用此命令的 **no** 形式：

csd hostscan image *path*

no csd hostscan image *path*

语法说明

path	指定思科主机扫描软件包的路径和文件名，最多 255 个字符。 主机扫描软件包可能是单机版，文件名约定为 hostscan-*version*.pkg ；或者是完整的 AnyConnect 安全移动客户端软件包，可从 Cisco.com 下载，文件名约定为 anyconnect-win-*version*-k9.pkg。当客户指定 AnyConnect 安全移动客户端时，ASA 将从 AnyConnect 软件包提取主机扫描软件包并进行安装。 主机扫描软件包中包含主机扫描软件以及主机扫描库和支持图表。 此命令不能上传 CSD 映像。上传 CSD 映像需要使用 **csd image** 命令。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

输入 **show webvpn csd hostscan** 命令可确定当前安装和启用的主机扫描映像版本。

在使用 **csd hostscan image** 命令安装主机扫描后，使用 **csd enable** 命令启用映像。

输入 **write memory** 命令可保存运行配置，以确保主机扫描映像在 ASA 下次重新启动后可用。

示例

以下命令显示如何安装、启用、查看思科主机扫描软件包以及在闪存驱动器中保存配置：

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
```

```
ciscoasa(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
show webvpn csd hostscan	识别思科主机扫描（如果已启用）的版本。若未启用，CLI 将指示“Secure Desktop is not enabled”（安全桌面未启用）。
csd enable	为管理和远程用户访问启用 CSD。

csd image

要验证思科安全桌面 (CSD) 分发软件包并将其添加到运行配置，请在 webvpn 配置模式下使用 **csd image** 命令有效地安装 CSD。要从运行配置删除 CSD 分发软件包，请使用此命令的 **no** 形式：

csd image *path*

no csd image *path*

语法说明

path	指定 CSD 软件包的路径和文件名，最多 255 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

在输入此命令之前，输入 **show webvpn csd** 命令确定 CSD 映像是否启用。CLI 会指示当前安装的 CSD 映像（如果已启用）版本。

在将思科安全桌面下载到计算机并传输到闪存驱动器后，使用 **csd image** 命令安装新映像或升级现有映像。下载时，请确保为 ASA 获取正确的文件；其形式为 securedesktop_asa_<n>_<n>*.pkg。

输入 **no csd image** 命令可删除对 CSD Manager 的管理访问以及远程用户对 CSD 的访问。输入此命令时，ASA 不会对闪存驱动器上的 CSD 软件和 CSD 配置做任何更改。

注意　输入 **write memory** 命令保存运行配置，以确保 CSD 在 ASA 下次重新启动后可用。

示例

以下命令显示如何查看当前 CSD 分发软件包、查看闪存文件系统的内容和升级到新版本。

```
ciscoasa# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
```

```
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
ciscoasa(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
show webvpn csd	识别 CSD（如果已启用）的版本。若未启用，CLI 将指示 “Secure Desktop is not enabled”（安全桌面未启用）。
csd enable	为管理和远程用户访问启用 CSD。

ctl

为使证书信任列表 (CTL) 提供程序解析来自 CTL 客户端的 CTL 文件并安装信任点，请在 CTL 提供程序配置模式下使用 **ctl** 命令。要删除配置，请使用此命令的 **no** 形式。

ctl install

no ctl install

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CTL 提供程序配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 CTL 提供程序配置模式下使用 **ctl** 命令，让 CTL 提供程序解析来自 CTL 客户端的 CTL 文件，并且为来自 CTL 文件的条目安装信任点。此命令安装的信任点的名称具有前缀“_internal_CTL_<ctl_name>”。

如果禁用此命令，必须通过 **crypto ca trustpoint** 和 **crypto ca certificate chain** 命令手动导入和安装每个 CallManager 服务器和 CAPF 证书。

示例

以下示例展示如何创建 CTL 提供程序实例：

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

相关命令

命令	说明
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 握手期间提供的代理信任点证书。
show tls-proxy	显示 TLS 代理。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

ctl-file (global)

要指定 CTL 实例为电话代理创建或解析存储在闪存中的 CTL 文件，请在全局配置模式下使用 **ctl-file** 命令。要删除 CTL 实例，请使用此命令的 **no** 形式。

ctl-file *ctl_name* **noconfirm**

no ctl-file *ctl_name* **noconfirm**

语法说明

ctl_name	指定 CTL 实例的名称。
noconfirm	（可选）与 **no** 命令一起使用，可在取消将 CTL 文件打印到 ASA 控制台时停止关于删除信任点的警告。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

如果用户具有需要 LSC 调配的电话，在使用 **ctl-file** 命令配置 CTL 文件实例时还必须将 CAPF 证书从 CUMC 导入到 ASA。有关详细信息，请参阅 CLI 配置指南。

注意　要创建 CTL 文件，请在 CTL 文件配置模式下使用 **no shutdown** 命令。要在 CTL 文件中修改或添加条目或者删除 CTL 文件，请使用 **shutdown** 命令。

使用此命令的 **no** 形式可删除电话代理内部创建的 CTL 文件和所有已注册信任点。此外，删除 CTL 文件会删除从相关证书颁发机构收到的所有证书。

示例

以下示例展示如何配置用于电话代理功能的 CTL 文件：

```
ciscoasa(config)# ctl-file myctl
```

相关命令

命令	说明
ctl-file (phone-proxy)	指定在配置电话代理实例时使用的 CTL 文件。
cluster-ctl-file	解析存储在闪存中、用以安装信任点的 CTL 文件。
phone-proxy	配置电话代理实例。
record-entry	指定要用于创建 CTL 文件的信任点。
sast	指定要在 CTL 记录中创建的 SAST 证书数。

ctl-file (phone-proxy)

要指定在配置电话代理时使用的 CTL 实例，请在电话代理配置模式下使用 **ctl-file** 命令。要删除 CTL 实例，请使用此命令的 **no** 形式。

ctl-file *ctl_name*

no ctl-file *ctl_name*

语法说明

ctl_name	指定 CTL 实例的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

示例

以下示例展示使用 **ctl-file** 命令配置用于电话代理功能的 CTL 文件：

```
ciscoasa(config-phone-proxy)# ctl-file myctl
```

相关命令

命令	说明
ctl-file (global)	指定要为电话代理配置创建的 CTL 文件，或者要从闪存解析的 CTL 文件。
phone-proxy	配置电话代理实例。

ctl-provider

要在 CTL 提供程序模式下配置 CTL 提供程序实例，请在全局配置模式下使用 **ctl-provider** 命令。要删除配置，请使用此命令的 **no** 形式。

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

语法说明

ctl_name	指定 CTL 提供程序实例的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **ctl-provider** 命令进入 CTL 提供程序配置模式，以创建 CTL 提供程序实例。

示例

以下示例展示如何创建 CTL 提供程序实例：

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

相关命令

命令	说明
client	指定允许连接到 CTL 提供程序的客户端以及用于客户端身份验证的用户名和密码。
ctl	解析来自 CTL 客户端的 CTL 文件并安装信任点。
export	指定要导出到客户端的证书。
service	指定 CTL 提供程序侦听的端口。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

cts import-pac

要从思科 ISE 导入 Protected Access Credential (PAC) 文件，请在全局配置模式下使用 **cts import-pac** 命令：

cts import-pac *filepath* **password** *value*

语法说明

filepath	指定以下 **exec** 模式命令和选项之一： **单模式** • **disk0**：disk0 上的路径和文件名 • **disk1**：disk1 上的路径和文件名 • **flash**：闪存上的路径和文件名 • **ftp**：FTP 上的路径和文件名 • **http**：HTTP 上的路径和文件名 • **https**：HTTPS 上的路径和文件名 • **smb**：SMB 上的路径和文件名 • **tftp**：TFTP 上的路径和文件名 **多模式** • **http**：HTTP 上的路径和文件名 • **https**：HTTPS 上的路径和文件名 • **smb**：SMB 上的路径和文件名 • **tftp**：TFTP 上的路径和文件名
password *value*	指定用于加密 PAC 文件的密码。此密码与 ISE 上配置为设备凭证一部分的密码无关。 此密码必须与请求 PAC 文件时提供的密码匹配，在解密 PAC 数据时必须输入。此密码与 ISE 上配置为设备凭证一部分的密码无关。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

将 PAC 文件导入到 ASA 可与 ISE 建立连接。在通道建立后，ASA 将发起与 ISE 的安全 RADIUS 事务，并且下载思科 TrustSec 环境数据；具体而言，ASA 会下载安全组表。该安全组表将 SGT 映射到安全组名称。安全组名称创建于 ISE 上，为安全组提供便于用户使用的名称。在 RADIUS 事务之前未建立任何通道。ASA 使用 PAC 进行身份验证，发起与 ISE 的 RADIUS 事务。

提示　PAC 文件包含共享密钥，允许 ASA 和 ISE 保护它们之间发生的 RADIUS 事务。鉴于此密钥的敏感性，必须将其安全地存储在 ASA 中。

在成功导入该文件后，ASA 无需 ISE 中配置的设备密码即可从 ISE 下载思科 TrustSec 环境数据。

ASA 将 PAC 文件存储在 NVRAM 区域（通过用户界面无法访问该区域）。

必备条件

- ASA 必须先配置为 ISE 中识别的思科 TrustSec 网络设备，然后 ASA 才可生成 PAC 文件。ASA 可以导入任何 PAC 文件，但仅当该文件是由配置正确的 ISE 生成时才可在 ASA 上运行。
- 获取解密在 ISE 上生成的 PAC 文件的密码。

  ASA 需要此密码来导入和解密 PAC 文件。
- 访问 ISE 生成的 PAC 文件。ASA 可以从闪存或者通过 TFTP、FTP、HTTP、HTTPS 或 SMB 从远程服务器导入 PAC 文件。（PAC 文件不在 ASA 闪存中时也可以导入。）
- 已为 ASA 配置服务器组。

限制

- 当 ASA 是 HA 配置的一部分时，必须将 PAC 文件导入到主要 ASA 设备。
- 当 ASA 是集群配置的一部分时，必须将 PAC 文件导入到主设备。

示例

以下示例从 ISE 导入 PAC：

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

相关命令

命令	说明
cts refresh environment-data	当 ASA 与思科 TrustSec 集成时，更新来自 ISE 的思科 TrustSec 环境数据
cts sxp enable	在 ASA 中启用 SXP 协议。

cts manual

要启用 SGT plus Ethernet Tagging（也称为 Layer 2 SGT Imposition）并进入 cts 手动接口配置模式，请在接口配置模式下使用 **cts manual** 命令。要禁用 SGT plus Ethernet Tagging，请使用此命令的 **no** 形式。

cts manual

no cts manual

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令启用 Layer 2 SGT Imposition 并进入 cts 手动接口配置模式。

限制

- 仅在物理接口、VLAN 接口、端口通道接口和冗余接口上受支持。
- 在逻辑接口或虚拟接口（例如 BVI、TVI 和 VNI）上不受支持。
- 不支持故障切换链路。
- 不支持集群控制链路。

示例

以下示例启用 Layer 2 SGT Imposition 并进入 cts 手动接口配置模式：

```
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)#
```

相关命令

命令	说明
policy static sgt	将策略应用于手动配置的 CTS 链路中。
propagate sgt	在接口上启用安全组标记（称为 **sgt**）的传播。

cts refresh environment-data

要刷新来自 ISE 的思科 TrustSec 环境数据并且将协调计时器重置为配置的默认值，请在全局配置模式下使用 **cts refresh environment-data** 命令。

cts refresh environment-data

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

当 ASA 与思科 TrustSec 集成时，ASA 将从 ISE 下载环境数据，其中包括安全组标记 (SGT) 名称表。当您在 ASA 上完成以下任务时，ASA 会自动刷新其从 ISE 获取的环境数据：

- 配置 AAA 服务器与 ISE 通信。
- 从 ISE 导入 PAC 文件。
- 识别 ASA 将用于检索思科 TrustSec 环境数据的 AAA 服务器组。

通常，您无需手动刷新来自 ISE 的环境数据；但可在 ISE 上更改安全组。这些更改在您于 ASA 中刷新数据之前不会反映在 ASA 中。刷新 ASA 上的数据以确保 ISE 上建立的任何安全组都反映在 ASA 中。

提示　建议安排 ISE 上的策略配置更改，并且在维护期间手动刷新 ASA 上的数据。以这种方式处理策略配置更改，安全组名称被解析和安全策略在 ASA 上立即启用的可能性最大。

必备条件

ASA 必须配置为 ISE 中识别的思科 TrustSec 网络设备，并且 ASA 必须成功导入 PAC 文件，以便对思科 TrustSec 的更改应用到 ASA。

限制

- 当 ASA 是 HA 配置的一部分时，必须在主要 ASA 设备上刷新环境数据。
- 当 ASA 是集群配置的一部分时，必须在主设备上刷新环境数据。

示例

以下示例从 ISE 下载思科 TrustSec 环境数据：

```
ciscoasa(config)# cts refresh environment-data
```

相关命令

命令	说明
cts import-pac	当 ASA 与思科 TrustSec 集成时，从思科 ISE 导入 Protected Access Credential (PAC) 文件。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts role-based sgt-map

要手动配置 IP-SGT 绑定，请在全局配置模式下使用 **cts role-based sgt-map** 命令。要删除配置，请使用此命令的 **no** 形式。

cts role-based sgt-map [*IPv4_addr* | *IPv6_addr*] **sgt** *sgt_value*

no cts role-based sgt-map [*IPv4_addr* | *IPv6_addr*] **sgt** *sgt_value*

语法说明

IPv4_addr	指定要使用的 IPv4 地址。
IPv6_addr	指定要使用的 IPv6 地址。
sgt *sgt_value*	指定 IP 地址映射到的 SGT 编号。有效值为 2 到 65519。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令可让您手动配置 IP-SGT 绑定。

示例

以下示例配置 IP-SGT 绑定表条目：

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

相关命令

命令	说明
clear configure cts role-based [**sgt-map**]	删除用户定义的 IP-SGT 绑定表条目。
show running-config [**all**] **cts role-based** [**sgt-map**]	显示用户定义的 IP-SGT 绑定表条目。

cts server-group

要识别 ASA 用于与思科 TrustSec 集成以检索环境数据的 AAA 服务器组，请在全局配置模式下使用 **cts server-group** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts server-group *aaa-server-group-name*

no cts server-group [*aaa-server-group-name*]

语法说明

aaa-server-group-name	指定本地配置的现有 AAA 服务器组的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

在配置 ASA 与思科 TrustSec 集成的过程中，必须将 ASA 配置为能与 ISE 通信。在 ASA 上只能为思科 TrustSec 配置一个服务器组实例。

必备条件

- 引用的服务器组必须存在。如果在 *aaa-server-group-name* 参数中指定未定义的服务器组名称，ASA 将会显示错误消息。
- 引用的服务器组必须配置为使用 RADIUS 协议。如果将非 RADIUS 服务器组添加到 ASA，功能配置将失败。
- 如果 ISE 也用于用户身份验证，请获取使用 ISE 注册 ASA 时在 ISE 上输入的共享密钥。如果您没有此信息，请联系 ISE 管理员。

示例

以下示例在 ASA 上为 ISE 本地配置 AAA 服务器组，并且配置 ASA 使用该 AAA 服务器组将 ASA 与思科 TrustSec 集成：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

相关命令

命令	说明
aaa-server *server-tag* **protocol radius**	创建 AAA 服务器组并配置 AAA 服务器参数，使 ASA 与 ISE 服务器通信；其中 *server-tag* 指定服务器组名称。
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	将 AAA 服务器配置为 AAA 服务器组的一部分，并且设置主机特定连接数据；其中 (*interface-name*) 指定 ISE 服务器所在的网络接口，*server-tag* 为思科 TrustSec 集成的 AAA 服务器组名称，*server-ip* 指定 ISE 服务器的 IP 地址。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts sxp connection peer

要将 SXP 设置为 SXP 对等设备，请在全局配置模式下使用 **cts sxp connection peer** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **mode**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

no cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] [**password** {**default** | **none**}] [**mode** {**local** | **peer**}] [**speaker** | **listener**]

语法说明

default	与 **password** 关键字一起使用。指定使用为 SXP 连接配置的默认密码。
listener	指定 ASA 用作 SXP 连接的监听方；这意味着 ASA 可以接收来自下游设备的 IP-SGT 映射。需要为 ASA 指定用于 SPX 连接的发言方或监听方。
local	与 **mode** 关键字一起使用。指定使用本地 SXP 设备。
mode	（可选）指定 SXP 连接的模式。
none	与 **password** 关键字一起使用。指定不对 SXP 连接使用密码。
password	（可选）指定是否对 SXP 连接使用身份验证密钥。
peer	与 **mode** 关键字一起使用。指定使用对等 SXP 设备。
peer_ip_address	指定 SXP 对等设备的 IPv4 或 IPv6 地址。对等设备 IP 地址必须可从 ASA 传出接口访问。
source *source_ip_address*	（可选）指定 SXP 连接的本地 IPv4 或 IPv6 地址。
speaker	指定 ASA 用作 SXP 连接的发言方；表示 ASA 可以将 IP-SGT 映射转发到上游设备。需要为 ASA 指定用于 SPX 连接的发言方或监听方。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

对等设备之间的 SXP 连接是点对点连接，并且使用 TCP 作为基础传输协议。SXP 连接按 IP 地址设置；一个设备对可以服务于多个 SXP 连接。

限制

- ASA 不支持 SXP 连接的每连接密码。
- 使用 **cts sxp default password** 配置默认 SXP 密码时，您应该将 SXP 连接配置为使用默认密码；相反，若未配置默认密码，也不应为 SXP 连接配置默认密码。如果不遵从这两个准则，SXP 连接可能失败。
- 使用默认密码配置 SXP 连接但 ASA 未配置默认密码时，SXP 连接将会失败。
- 配置 SXP 连接的源 IP 地址时，必须指定与 ASA 出站接口相同的地址。如果源 IP 地址与出站接口的地址不匹配，SXP 连接将会失败。

  当 SXP 连接的源 IP 地址未配置时，ASA 将执行路由 /ARP 查找来确定 SXP 连接的出站接口。建议不要为 SXP 连接配置源 IP 地址，而让 ASA 执行路由 /ARP 查找来确定 SXP 连接的源 IP 地址。
- 不支持为 SXP 对等设备或源配置 IPv6 本地链路地址。
- 不支持在同一接口上为 SXP 连接配置多个 IPv6 地址。

示例

以下示例在 ASA 上创建 SXP 连接：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password
default mode peer speaker
```

相关命令

命令	说明
cts sxp default password	指定 SXP 连接的默认密码。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts sxp default password

要配置使用 SXP 对等设备进行 TCP MD5 身份验证时的默认密码，请在全局配置模式下使用 **cts sxp default password** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp default password [**0** | **8**] *password*

no cts sxp default password [**0** | **8**] [*password*]

语法说明

0	（可选）指定默认密码对加密级别使用未加密明文。您只能为默认密码设置一个加密级别。
8	（可选）指定默认密码对加密级别使用加密文本。
password	指定最长 162 个字符的加密字符串或最长 80 个字符的 ASCII 密钥字符串。

默认值

默认情况下，SXP 连接未设置密码。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用默认密码配置 SXP 连接但 ASA 未配置默认密码时，SXP 连接将会失败。

限制

- ASA 不支持 SXP 连接的每连接密码。
- 使用 **cts sxp default password** 配置默认 SXP 密码时，您应该将 SXP 连接配置为使用默认密码；相反，若未配置默认密码，也不应为 SXP 连接配置默认密码。如果不遵从这两个准则，SXP 连接可能失败。

示例

以下示例展示如何设置所有 SXP 连接的默认值，包括 SXP 连接的默认密码：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

相关命令

命令	说明
cts sxp connection peer	将 ASA 的 SXP 连接配置到 SXP 对等设备。使用此命令指定 **password default** 关键字会允许对该 SXP 连接使用默认密码。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts sxp default source-ip

要为 SXP 连接配置默认本地 IP 地址，请在全局配置模式下使用 **cts sxp default source-ip** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp default source-ip *ipaddress*

no cts sxp default source-ip [*ipaddress*]

语法说明

ipaddress	指定源 IP 地址的 IPv4 或 IPv6 地址。

默认值

默认情况下，SXP 连接未设置默认源 IP 地址。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

为 SXP 连接配置默认源 IP 地址时，必须指定与 ASA 出站接口相同的地址。如果源 IP 地址与出站接口的地址不匹配，SXP 连接将会失败。

当 SXP 连接的源 IP 地址未配置时，ASA 将执行路由 /ARP 查找来确定 SXP 连接的出站接口。建议不要为 SXP 连接配置默认源 IP 地址，而让 ASA 执行路由 /ARP 查找来确定 SXP 连接的源 IP 地址。

示例

以下示例展示如何设置所有 SXP 连接的默认值，包括 SXP 连接的默认源 IP 地址：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

相关命令

命令	说明
cts sxp connection peer	配置 ASA 的 SXP 连接。使用此命令指定 **source** *source_ip_address* 关键字和参数会允许对该 SXP 连接使用默认源 IP 地址。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts sxp enable

要在 ASA 上启用 SXP 协议，请在全局配置模式下使用 **cts sxp enable** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp enable

no cts sxp 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，ASA 上禁用 SXP 协议。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

以下示例在 ASA 上启用 SXP 协议：

```
ciscoasa(config)# cts sxp enable
```

相关命令

命令	说明
clear cts	清除 ASA 与思科 TrustSec 集成时使用的数据。
cts sxp connection peer	将 ASA 的 SXP 连接配置到 SXP 对等设备。

cts sxp reconciliation period

要 …，请在全局配置模式下使用 **cts sxp reconciliation period** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp reconciliation period *timervalue*

no cts sxp reconciliation period [*timervalue*]

语法说明

timervalue	指定协调计时器的默认值。输入在 1-64000 秒范围内的秒数。

默认值

默认情况下，*timervalue* 为 120 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

在 SXP 对等设备终止其 SXP 连接后，ASA 将启动抑制计时器。如果 SXP 对等设备在抑制计时器运行时连接，ASA 将启动协调计时器；然后，ASA 更新 SXP 映射数据库以获知最新映射。

当协调计时器到期时，ASA 会扫描 SXP 映射数据库以识别过时的映射条目（在上一个连接会话中获知的条目）。ASA 将这些连接标记为过时。当协调计时器到期时，ASA 会从 SXP 映射数据库中删除过时的条目。

不能为该计时器指定 0，因为指定 0 将使协调计时器无法启动。若不允许协调计时器运行，则会使过时条目保留不确定的时间，导致策略实施出现意外结果。

示例

以下示例展示如何设置所有 SXP 连接的默认值，包括默认协调计时器：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

相关命令

命令	说明
cts sxp connection peer	将 ASA 的 SXP 连接配置到 SXP 对等设备。
cts sxp enable	在 ASA 中启用 SXP 协议。

cts sxp retry period

要指定 ASA 尝试在 SXP 对等设备之间设置新 SXP 连接的默认时间间隔，请在全局配置模式下使用 **cts sxp retry period** 命令。要禁用此命令的支持，请使用此命令的 **no** 形式。

cts sxp retry period *timervalue*

no cts sxp retry period [*timervalue*]

语法说明

timervalue	指定重试计时器的默认值。输入在 0-64000 秒范围内的秒数。

默认值

默认情况下，*timervalue* 为 120 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

指定 ASA 尝试在 SXP 对等设备之间设置新 SXP 连接的默认时间间隔。ASA 会继续进行连接尝试，直到成功建立连接。

只要 ASA 上有一个 SXP 连接未运行，重试计时器就会触发。

如果您指定 0 秒，则计时器永不过期，ASA 不会尝试连接到 SXP 对等设备。

在重试计时器到期时，ASA 将仔细检查连接数据库，如果数据库包含任何已关闭或处于 “ 等待打开 ” 状态的连接，ASA 会重新启动重试计时器。

建议将重试计时器配置为与其 SXP 对等设备不同的值。

示例

以下示例展示如何设置所有 SXP 连接的默认值，包括默认重试期：

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

相关命令

命令	说明
cts sxp connection peer	将 ASA 的 SXP 连接配置到 SXP 对等设备。
cts sxp enable	在 ASA 中启用 SXP 协议。

customization

要指定用于隧道组、组或用户的定制，请在隧道组 webvpn 属性配置模式或 webvpn 配置模式下使用 **customization** 命令。若不指定定制，请使用此命令的 **no** 形式。

customization *name*

no customization *name*

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

语法说明

name	指定要应用到组或用户的 WebVPN 定制的名称。
none	对组或用户禁用定制，并防止继承定制。
value *name*	指定要应用到组策略或用户的定制的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组 WebVPN 属性配置	• 是	—	• 是	—	—
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

在隧道组 webvpn 属性配置模式下输入 **customization** 命令之前，必须在 webvpn 配置模式下使用 **customization** 命令命名并配置定制。

模式相关命令选项

可用于 **customization** 命令的关键字根据您所处的模式而不同。在组策略属性配置模式和用户名属性配置模式中，会出现额外的关键字 **none** 和 **value**。

例如，如果从用户名属性配置模式输入 **customization none** 命令，则 ASA 不会查找组策略或隧道组中的值。

示例

以下示例所示的命令序列先建立名为 “123” 的 WebVPN 定制来定义密码提示。然后定义名为 “test” 的 WebVPN 隧道组，并使用 **customization** 命令指定使用名为 “123” 的 WebVPN 定制：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization 123
ciscoasa(config-webvpn-custom)# password-prompt Enter password
ciscoasa(config-webvpn)# exit
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# customization 123
ciscoasa(config-tunnel-webvpn)#
```

以下示例展示名为 “cisco” 的定制应用到名为 “cisco_sales” 的组策略。请注意，通过 webvpn 配置模式在组策略属性配置模式下输入的 **customization** 命令需要额外的命令选项 **value**：

```
ciscoasa(config)# group-policy cisco_sales attributes
ciscoasa(config-group-policy)#  webvpn
ciscoasa(config-group-webvpn)# customization value cisco
```

相关命令

命令	说明
clear configure tunnel-group	删除所有隧道组配置。
show running-config tunnel-group	显示当前隧道组配置。
tunnel-group webvpn-attributes	进入 webvpn 配置模式以配置 WebVPN 隧道组属性。

cxsc

要将流量重定向到 ASA CX 模块，请在类配置模式下使用 **cxsc** 命令。要删除 ASA CX 操作，请使用此命令的 **no** 形式。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

no cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

语法说明

auth-proxy	（可选）启用活动的身份验证需要的身份验证代理。
fail-close	设置 ASA 在 ASA CX 模块不可用时阻止所有流量。
fail-open	设置 ASA 在 ASA CX 模块不可用时允许所有流量通过且不进行检查。
monitor-only	（仅用于演示）指定 **monitor-only** 以将流量的只读副本发送到 ASA CX 模块。配置此选项后，您将看到如下所示的警告消息： `WARNING: Monitor-only mode should be used for demonstrations and evaluations only.`

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(4.1)	我们引入了此命令。
9.1(2)	添加了 **monitor-only** 关键字来支持演示功能。
9.1(3)	您现在可以配置每个情景的 ASA CX 策略。

使用指南

可以先输入 policy-map 命令来访问类配置模式。

在 ASA 上配置 **cxsc** 命令之前或之后，在使用 Cisco Prime Security Manager (PRSM) 的 ASA CX 模块上配置安全策略。

要配置 **cxsc** 命令，必须先配置 **class-map** 命令、**policy-map** 命令和 **class** 命令。

交通流量

ASA CX 模块与 ASA 运行不同的应用。但是将其集成到 ASA 流量。当您对 ASA 上的流量类应用 **cxsc** 命令时，流量会以下列方式通过 ASA 和 ASA CX 模块：

1. 流量进入 ASA。

2. 流入 VPN 流量被解密。
3. 应用防火墙策略。
4. 流量通过背板发送到 ASA CX 模块。
5. ASA CX 模块将其安全策略应用到流量并采取适当的措施。
6. 有效的流量通过背板发送回 ASA； ASA CX 模块根据其安全策略可能会阻止某些流量，而该流量不再传递。
7. 流出 VPN 流量被加密。
8. 流量退出 ASA。

关于身份验证代理的信息

当 ASA CX 需要对 HTTP 用户进行身份验证（利用身份策略）时，您必须配置 ASA 作为身份验证代理：ASA CX 模块将身份验证请求重定向到 ASA 接口 IP 地址 / 代理端口。默认情况下，端口为 885（用户可使用 **cxsc auth-proxy port** 命令配置）。将此功能配置为服务策略的一部分，以将流量从 ASA 转移至 ASA CX 模块。如果不启用身份验证代理，则只有被动身份验证可用。

与 ASA 功能的兼容性

ASA 带有诸多高级应用检查功能，其中包括 HTTP 检查。但是，ASA CX 模块提供的 HTTP 检查比 ASA 提供的更高级，还提供用于其他应用的附加功能，包括监控应用的使用。

要充分利用 ASA CX 模块功能，请参阅适用于发送到 ASA CX 模块的流量的以下指导原则：

- 请勿对 HTTP 流量配置 ASA 检查。
- 请勿配置云网络安全 (ScanSafe) 检查。如果为同一流量配置 ASA CX 操作和云网络安全检查，则 ASA 只执行 ASA CX 操作。
- ASA 上的其他应用检查与 ASA CX 模块兼容，包括默认检查。
- 不要启用移动用户安全 (MUS) 服务器；它与 ASA CX 模块不兼容。
- 不要启用 ASA 集群；它与 ASA CX 模块不兼容。
- 如果启用故障切换，则当 ASA 故障切换时，所有现有 ASA CX 流量都会传输到新的 ASA，但流量可以通过 ASA，而且 ASA CX 模块不会对其执行操作。ASA CX 模块只会对 ASA 收到的新流量执行操作。

Monitor-Only 模式

为测试和演示，您可以使用 **monitor-only** 关键字配置 ASA 将只读流量的重复流发送到 ASA CX 模块，这样便可了解模块如何检查流量而不影响 ASA 流量。在此模式下，ASA CX 模块像平常一样检查流量、制定策略决策和生成事件。但是，由于数据包是只读副本，模块操作不会影响实际流量。相反，模块在检查后会丢弃副本。

请参阅以下指导原则：

- 在 ASA 上，您无法同时配置仅监控模式和正常内联模式。只允许一种安全策略。
- 在仅监控模式下不支持以下功能：
  - 拒绝策略
  - 活动身份验证
  - 解密策略
- ASA CX 在仅监控模式下不执行数据包缓冲，事件也将按照尽力的原则生成。例如，有些事件（比如具有跨越数据包边界的长 URL 的事件）可能因缺少缓冲而受到影响。
- 确保为 ASA 策略和 ASA CX 配置一致的模式：两者都为仅监控模式，或都为普通内嵌模式。

示例

在以下示例中，如果 ASA CX 模块卡因任何原因而失败，所有 HTTP 流量都会转移至 ASA CX 模块，并且阻止所有 HTTP 流量：

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

在以下示例中，如果 ASA CX 模块卡因任何原因而失败，去往 10.1.1.0 网络及 10.2.1.0 网络的所有 IP 流量将转移至 ASA CX 模块，并允许所有流量通过：

```
ciscoasa(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list my-cx-acl
ciscoasa(config)# class-map my-cx-class2
ciscoasa(config-cmap)# match access-list my-cx-acl2
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap)# class my-cx-class2
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy interface outside
```

相关命令

命令	说明
class	指定要用于流量分类的类映射。
class-map	识别策略映射中使用的流量。
cxsc auth-proxy port	设置身份验证代理端口。
debug cxsc	启用 ASA CX 调试消息。
hw-module module password-reset	将模块密码重置为默认值。
hw-module module reload	重新加载模块。
hw-module module reset	执行重置，然后重新加载模块。
hw-module module shutdown	关闭模块。
policy-map	配置策略；即流量类与一个或多个操作的关联。
session do get-config	获取模块配置。
session do password-reset	将模块密码重置为默认值。
session do setup host ip	配置模块管理地址。
show asp table classify domain cxsc	显示为将流量发送到 ASA CX 模块而创建的 NP 规则。
show asp table classify domain cxsc-auth-proxy	显示为 ASA CX 模块的身份验证代理而创建的 NP 规则。
show module	显示模块状态。
show running-config policy-map	显示当前所有策略映射 配置。
show service-policy	显示服务策略统计信息。

cxsc auth-proxy port

要设置 ASA CX 模块流量的身份验证代理端口，请在全局配置模式下使用 **cxsc auth-proxy port** 命令。要将端口设置为默认值，请使用此命令的 **no** 形式。

cxsc auth-proxy port *port*

no cxsc auth-proxy port [*port*]

语法说明

port *port*	将身份验证代理端口设置为大于 1024 的值。默认值为 885。

命令默认值

默认端口为 885。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(4.1)	我们引入了此命令。
9.1(3)	您现在可以配置每个情景的 ASA CX 策略。

使用指南

如果在配置 **cxsc** 命令时启用身份验证代理，可以使用此命令更改端口。

当 ASA CX 需要对 HTTP 用户进行身份验证（利用身份策略）时，您必须配置 ASA 作为身份验证代理：ASA CX 模块将身份验证请求重定向到 ASA 接口 IP 地址 / 代理端口。默认情况下，端口为 885。将此功能配置为服务策略的一部分，以将流量从 ASA 转移至 ASA CX 模块。如果不启用身份验证代理，则只有被动身份验证可用。

示例

以下示例为 ASA CX 流量启用身份验证代理，然后将端口更改为 5000：

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
ciscoasa(config)# cxsc auth-port 5000
```

相关命令

命令	说明
class	指定要用于流量分类的类映射。
class-map	识别策略映射中使用的流量。
cxsc	将流量重定向到 ASA CX 模块。
debug cxsc	启用 ASA CX 调试消息。
hw-module module password-reset	将模块密码重置为默认值。
hw-module module reload	重新加载模块。
hw-module module reset	执行重置，然后重新加载模块。
hw-module module shutdown	关闭模块。
policy-map	配置策略；即流量类与一个或多个操作的关联。
session do get-config	获取模块配置。
session do password-reset	将模块密码重置为默认值。
session do setup host ip	配置模块管理地址。
show asp table classify domain cxsc	显示为将流量发送到 ASA CX 模块而创建的 NP 规则。
show asp table classify domain cxsc-auth-proxy	显示为 ASA CX 模块的身份验证代理而创建的 NP 规则。
show module	显示模块状态。
show running-config policy-map	显示当前所有策略映射 配置。
show service-policy	显示服务策略统计信息。

第 3 部分

D 命令

第 11 章

database path 至 dhcp-server 命令

database path

要指定本地 CA 服务器数据库的路径或位置，请在 CA 服务器配置模式下使用 **database** 命令。要重置闪存的路径，请使用此命令的 **no** 形式。

[**no**] **database path** *mount-name directory-path*

语法说明

directory-path	指定用于存储 CA 文件的安装点上目录的路径。
mount-name	指定安装名称。

默认值

默认情况下，CA 服务器数据库存储在闪存中。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

存储在数据库中的本地 CA 文件包括证书数据库、用户数据库文件、临时 PKCS12 文件和当前 CRL 文件。*mount-name* 参数与用于为 ASA 指定文件系统的 **mount** 命令中的 *name* 参数相同。

注意　这些 CA 文件是内部存储的文件，不能修改。

示例

以下示例将 CA 数据库的安装点定义为 cifs_share，将安装点上的数据库文件目录定义为 ca_dir/files_dir：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# database path cifs_share ca_dir/files_dir/
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式 CLI 命令集的访问，它允许用户配置和管理本地 CA。
crypto ca server user-db write	将本地 CA 中配置的用户信息写入到磁盘。

命令	说明
debug crypto ca server	在用户配置本地 CA 服务器时显示调试消息。
mount	使 ASA 可访问通用互联网文件系统 (CIFS) 和 / 或文件传输协议文件系统 (FTPFS）。
show crypto ca server	在 ASA 上显示 CA 配置的特征。
show crypto ca server cert-db	显示 CA 服务器颁发的证书。

ddns

要指定动态 DNS (DDNS) 更新方法类型，请在 ddns-update-method 模式下使用 **ddns** 命令。要从运行配置中删除更新方法类型，请使用此命令的 **no** 形式。

ddns [**both**]

no ddns [**both**]

语法说明

both	（可选）指定更新 DNS A 和 PTR 资源记录 (RR)。

默认值

只更新 DNS A RR。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Ddns-update-method	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

DDNS 更新 DNS 维护的名称 - 地址和地址 - 名称映射。执行 DDNS 更新有两种方法 - RFC 2136 定义的 IETF 标准和通用 HTTP 方法，ASA 在此版本中支持 IETF 方法。

两种类型的 RR 中都包含名称和地址映射：

- A 资源记录包含域名 -IP 地址映射。
- PTR 资源记录包含 IP 地址 - 域名映射。

DDNS 更新可用于在 DNS A 与 PTR RR 类型之间保持一致的信息。

在 ddns-update-method 配置模式下发出的 **ddns** 命令定义是只更新 DNS A RR，还是同时更新 DNS A 和 PTR RR 类型。

示例

以下示例配置使用名为 ddns-2 的 DDNS 更新方法更新 DNS A 和 PTR RR：

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

相关命令

命令	说明
ddns update	将 DDNS 更新方法与 ASA 接口或一个 DDNS 更新主机名关联。
ddns update method	创建一个用于动态更新 DNS 资源记录的方法。
dhcp-client update dns	配置 DHCP 客户端要向 DHCP 服务器传送的更新参数。
dhcpd update dns	启用 DHCP 服务器以执行 DDNS 更新。
interval maximum	配置 DDNS 更新方法的更新尝试之间的最大间隔。

ddns update

要将动态 DNS (DDNS) 更新方法与 ASA 接口或更新主机名关联，请在接口配置模式下使用 **ddns update** 命令。要从运行配置删除 DDNS 更新方法与接口或主机名之间的关联，请使用此命令的 **no** 形式。

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

语法说明

hostname	指定命令字符串中的下一项是主机名。
hostname	指定要用于更新的主机名。
method-name	指定要与所配置的接口关联的方法名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在定义 DDNS 更新方法后，必须将其与 ASA 接口关联以触发 DDNS 更新。

主机名可以是完全限定域名 (FQDN) 或只是主机名。如果只是主机名，ASA 会将域名附加到主机名以创建 FQDN。

示例

以下示例将接口 GigabitEthernet0/2 与名为 ddns-2 的 DDNS 更新方法以及主机名 hostname1.example.com 进行关联：

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

相关命令

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update method	创建一个用于动态更新 DNS 资源记录的方法。

命令	说明
dhcp-client update dns	配置 DHCP 客户端要向 DHCP 服务器传送的更新参数。
dhcpd update dns	启用 DHCP 服务器以执行 DDNS 更新。
interval maximum	配置 DDNS 更新方法的更新尝试之间的最大间隔。

ddns update method

要创建动态更新 DNS 资源记录 (RR) 的方法，请在全局配置模式下使用 **ddns update method** 命令。要从运行配置删除动态 DNS (DDNS) 更新方法，请使用此命令的 **no** 形式。

ddns update method *name*

no ddns update method *name*

语法说明

name	指定动态更新 DNS 记录的方法的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

DDNS 更新 DNS 维护的名称 - 地址和地址 - 名称映射。**ddns update method** 命令配置的更新方法确定 DDNS 更新执行的时间和频率。执行 DDNS 更新有两种方法 - RFC 2136 定义的 IETF 标准和通用 HTTP 方法，ASA 在此版本中支持 IETF 方法。

名称和地址映射包含在两种类型的资源记录 (RR) 中：

- A 资源记录包含域名 -IP 地址映射。
- PTR 资源记录包含 IP 地址 - 域名映射。

DDNS 更新可用于在 DNS A 与 PTR RR 类型之间保持一致的信息。

注意　必须使用 **dns** 命令配置可达的默认 DNS 服务器并且在接口上启用域查找，**ddns update method** 命令才会运行。

示例

以下示例配置名为 ddns-2 的 DDNS 更新方法：

```
ciscoasa(config)# ddns update method ddns-2
```

相关命令

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update	将 DDNS 更新方法与 ASA 接口或一个 DDNS 更新主机名关联。
dhcp-client update dns	配置 DHCP 客户端要向 DHCP 服务器传送的更新参数。
dhcpd update dns	启用 DHCP 服务器以执行动态 DNS 更新。
interval maximum	配置 DDNS 更新方法的更新尝试之间的最大间隔。

debug

要显示给定功能的调试消息，请在特权 EXEC 模式下使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。

debug *feature* [*subfeature*] [*level*]

no debug *feature* [*subfeature*]

语法说明

level	（可选）指定调试级别。该级别可能并非对所有功能都适用。
feature	指定要为其启用调试的功能。要查看可用的功能，请使用 **debug?** 命令查看 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能启用调试消息。

默认值

默认调试级别为 1。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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，请仅使用 **debug** 命令排除特定问题，或只在思科技术支持人员的故障排除会话期间使用。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段内调试可降低增加的 **debug** 命令处理开销影响系统使用的可能性。

示例

以下是 **debug aaa internal** 命令的示例输出：

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated.remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user .remote address: 10.42.15.172, session id: 2147483841
```

default (crl configure)

要将所有 CRL 参数恢复为系统默认值，请在 crl configure 配置模式下使用 **default** 命令。

default

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crl 配置配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的调用不会成为活动配置的一部分。crl configure 配置模式可从 crypto ca trustpoint 配置模式进行访问。这些参数仅在 LDAP 服务器有需要时使用。

示例

以下示例进入 ca-crl 配置模式并将 CRL 命令值恢复为其默认值：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# default
ciscoasa(ca-crl)#
```

相关命令

命令	说明
crl configure	进入 crl 配置配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
protocol ldap	将 LDAP 指定为 CRL 的检索方法。

default（接口）

要将接口命令恢复为系统默认值，请在接口配置模式下使用 **default** 命令。

default *command*

语法说明

command	指定要设置为默认值的命令。例如： **default activation key**

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令是运行时命令；当您输入它时，它不会成为活动配置的一部分。

示例

以下示例进入接口配置模式并将安全级别恢复为默认值：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

相关命令

命令	说明
interface	进入接口配置模式。

default (OSPFv3)

要将 OSPFv3 参数恢复为默认值，请在路由器配置模式下使用 **default** 命令。

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

语法说明

area	（可选）指定 OSPFv3 区域参数。
auto-cost	（可选）根据带宽指定 OSPFv3 接口成本。
default-information	（可选）分配默认信息。
default-metric	（可选）指定重分布路由的指标。
discard-route	（可选）启用或禁用丢弃路由安装。
distance	（可选）指定管理距离。
distribute-list	（可选）在路由更新中过滤网络。
ignore	（可选）忽略特定事件。
log-adjacency-changes	（可选）记录相邻状态的更改。
maximum-paths	（可选）通过多条路径转发数据包。
passive-interface	（可选）抑制接口上的路由更新。
redistribute	（可选）从另一个路由协议重新分配 IPv6 前缀。
router-id	（可选）指定特定路由进程的路由器 ID。
summary-prefix	（可选）指定 OSPFv3 摘要前缀。
timers	（可选）指定 OSPFv3 计时器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令将 OSPFv3 参数重置为默认值。

示例

以下示例将 OSPFv3 计时器参数重置为默认值：

```
ciscoasa(config-router)# default timers spf
```

相关命令

命令	说明
distance	指定 OSPFv3 路由进程的管理距离。
default-information originate	将默认外部路由生成到 OSPFv3 路由域。
log-adjacency-changes	配置路由器在 OSPFv3 邻居启动或关闭时发送系统日志消息。

default (time-range)

要恢复 **absolute** 和 **periodic** 命令的默认设置，请在 time-range 配置模式下使用 **default** 命令。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

语法说明

absolute	定义时间范围生效的绝对时间。
days-of-the-week	此参数首次出现的时间是关联的时间范围生效的开始时间或周内某日。第二次出现在周的结束日或关联的语句生效的周内某日。 此参数是任何一天或周内某些日的组合：周一、周二、周三、周四、周五、周六和周日。其他可能的值是： • 每日 - 周一至周日 • 工作日 - 周一至周五 • 周末 - 周六和周日 如果周的结束日与周的开始日相同，则您可以忽略它们。
periodic	指定支持时间范围功能的各功能的重复（每周）时间范围。
time	以 HH:MM 格式指定时间。例如，8:00 是上午 8:00， 20:00 是下午 8:00。
to	需要输入 **to** 关键字来填写 “ 从开始时间到结束时间 ” 的范围。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
时间范围配置	•	•	•	•	

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果周的结束日值与开始值相同，则您可以忽略它们。

如果 **time-range** 命令同时指定了 **absolute** 值和 **periodic** 值，则仅在达到 absolute start 时间后才会对 periodic 命令进行评估，且在达到 **absolute end** 时间后不再进一步对该命令进行评估。

时间范围功能依赖于 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

以下示例展示如何恢复 **absolute** 关键字的默认行为：

```
ciscoasa(config-time-range)# default absolute
```

相关命令

命令	说明
absolute	定义时间范围生效的绝对时间。
periodic	指定支持时间范围功能的各功能的重复（每周）时间范围。
time-range	定义对 ASA 基于时间的访问控制。

default user group

对于云网络安全，要指定当 ASA 无法确定进入 ASA 的用户身份时的默认用户名和 / 或组，请在参数配置模式下使用 **default user group** 命令。要删除默认用户或组，请使用此命令的 **no** 形式。您可以先输入 **policy-map type inspect scansafe** 命令来访问参数配置模式。

default {[**user** *username*] [**group** *groupname*]}

no default [**user** *username*] [**group** *groupname*]

语法说明

username	指定默认用户名。
groupname	指定默认组名称。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

如果 ASA 无法确定进入 ASA 的用户的身份，则会在 HTTP 报头中包含默认用户和 / 或组。

示例

以下示例将默认名称设置为 “Boulder”，将组名称设置为 “Cisco”：

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
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。

命令	说明
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	配置一般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、备用服务器还是不可达。
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。
whitelist	对流量类执行白名单操作。

default-acl

要指定将 ACL 用作安全状态验证失败时 NAC 框架会话的默认 ACL，请在 nac-policy-nac-framework 配置模式下使用 **default-acl** 命令。要从 NAC 策略中删除此命令，请使用此命令的 **no** 形式。

[**no**] **default-acl** *acl-name*

语法说明

acl-name	命名要应用到会话的访问控制列表。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Nac-policy-nac-framework 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	从命令名称中删除了 “nac-”。命令已从 group-policy 配置模式移到 nac-policy-nac-framework 配置模式。

使用指南

每个组策略指向要应用到与策略匹配且适用于 NAC 的主机的默认 ACL。ASA 在安全状态验证之前应用 NAC 默认 ACL。在安全状态验证后，ASA 将默认 ACL 替换为从远程主机的访问控制服务器获取的 ACL。如果安全状态验证失败，它将保留默认 ACL。

ASA 在无客户端身份验证启用（默认设置）时也会应用 NAC 默认 ACL。

示例

以下示例将 acl-1 确定为安全状态验证成功之前应用的 ACL：

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

以下示例从默认组策略继承 ACL：

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

相关命令

命令	说明
nac-policy	创建和访问 Cisco NAC 策略，并指定其类型。
nac-settings	将 NAC 策略分配到组策略。
debug nac	启用日志记录的 NAC 框架事件。
show vpn-session_summary.db	显示 IPsec、WebVPN 和 NAC 会话数。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。

default enrollment

要将所有注册参数恢复为系统默认值，请在 crypto ca trustpoint 配置模式下使用 **default enrollment** 命令。

default enrollment

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca trustpoint 配置	•	•	•	•	•

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的调用不会成为活动配置的一部分。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并且将所有注册参数恢复为其在中心信任点的默认值：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
clear configure crypto ca trustpoint	删除所有信任点。
crl configure	进入 crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。

default-domain

要设置组策略用户的默认域名，请在 group-policy 配置模式下使用 **default-domain** 命令。要删除域名，请使用此命令的 **no** 形式。

default-domain {**value** *domain-name* | **none**}

no default-domain [*domain-name*]

语法说明

none	表示没有默认域名。使用 null 值设置默认域名，从而禁止使用默认域名。防止从默认或指定的组策略继承默认域名。
value *domain-name*	标识组的默认域名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要防止用户继承域名，请使用 **default-domain none** 命令。

ASA 将默认域名传递到 AnyConnect 安全移动客户端或传统 VPN 客户端 (IPsec/IKEv1)，以附加到省略域字段的 DNS 查询。此域名仅适用于隧道数据包。没有默认域名时，用户将继承默认组策略中的默认域名。

默认域名只能使用字母数字字符、连字符 (-) 和点 (.)。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置 FirstDomain 的默认域名：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

相关命令

命令	说明
split-dns	提供要通过拆分隧道解析的域列表。
split-tunnel-network-list	确定 ASA 用来区分需要和不需要隧道的网络的访问列表。
split-tunnel-policy	让 IPsec 客户端有条件地以加密形式使数据包通过 IPsec 隧道，或以明文形式传递到网络接口。

default-group-policy

要指定用户默认继承的属性集，请在隧道组常规属性配置模式下使用 **default-group-policy** 命令。要消除默认组策略名称，请使用此命令的 **no** 形式。

default-group-policy *group-name*

no default-group-policy *group-name*

语法说明

group-name	指定默认组的名称。

默认值

默认组名称是 DfltGrpPolicy。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	webvpn 配置模式下的 **default-group-policy** 命令已弃用。代之以隧道组常规属性模式下的 **default-group-policy** 命令。

使用指南

在版本 7.1(1) 中，如果您在 webvpn 配置模式下输入此命令，它将转换为隧道组常规属性模式下的相同命令。

默认组策略 DfltGrpPolicy 具有 ASA 的初始配置。您可以将此属性应用于所有隧道组类型。

示例

以下示例在 config-general 配置模式下输入，为名为 “standard-policy” 的 IPsec 局域网至局域网隧道组指定默认继承的一组用户属性。此命令集定义记帐服务器、身份验证服务器、授权服务器和地址池。

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
group-policy	创建或编辑组策略
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	指定命名的隧道组的常规属性。

default-group-policy (webvpn)

要指定当 WebVPN 或邮件代理配置未指定组策略时使用的组策略名称，请在各配置模式下使用 **default-group-policy** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

default-group-policy *groupname*

no default-group-policy

语法说明

groupname	标识先前配置的组策略以用作默认组策略。使用 **group-policy** 命令配置组策略。

默认值

名为 *DfltGrpPolicy* 的默认组策略在 ASA 上始终存在。此 **default-group-policy** 命令可用于替换为 WebVPN 和邮件代理会话创建的默认组策略。另一种方式是编辑 DfltGrpPolicy。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令在 webvpn 配置模式中已弃用，并且已移至隧道组常规属性配置模式。

使用指南

WebVPN、IMAP4S、POP3S 和 SMTPS 会话需要指定的或默认组策略。对于 WebVPN，请在 webvpn 配置模式下使用此命令。对于邮件代理，请在适用的邮件代理模式下使用此命令。

在版本 7.1(1) 中，如果您在 webvpn 配置模式下输入此命令，它将在隧道组常规属性配置模式下转换为相同的命令。

您可以编辑系统 DefaultGroupPolicy，但不能删除它。它具有以下 AVP：

属性	默认值
wins-server	none
dns-server	none
dhcp-network-scope	none

属性	默认值
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn 属性	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	none

示例

以下示例展示如何为 WebVPN 指定称为 WebVPN7 的默认组策略：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

要为 WebVPN 用户设置默认空闲超时时间值，请在 webvpn 配置模式下使用 **default-idle-timeout** 命令。要从配置删除默认空闲超时值并重置默认值，请使用此命令的 **no** 形式。

default-idle-timeout *seconds*

no default-idle-timeout

语法说明

seconds	指定空闲超时的秒数。最小值为 60 秒，最大值为 1 天（86400 秒）。

默认值

1800 秒（30 分钟）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果没有为用户定义空闲超时、超时值为 0 或不在有效范围内，ASA 将使用您在此处设置的值。默认空闲超时时间可防止过期的会话。

建议将此命令设置为较短时间，因为浏览器设置为禁用 Cookie（或提示 Cookie，然后拒绝它们），可能导致用户未连接但仍然出现在会话数据库中。如果允许的连接最大数设置为 1（通过 **vpn-simultaneous-logins** 命令），则用户无法重新登录，因为数据库表示已达到连接最大数。设置短空闲超时可快速删除此类假会话，让用户重新登录。

示例

以下示例展示如何将默认空闲超时设置为 1200 秒（20 分钟）：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

相关命令

命令	说明
vpn-simultaneous-logins	设置允许的并发 VPN 会话最大数。

default-information (EIGRP)

要控制 EIGRP 路由进程的候选默认路由信息，请在路由器配置模式下使用 **default-information** 命令。要抑制入站或出站更新中的 EIGRP 候选默认路由信息，请使用此命令的 **no** 形式。

default-information {**in** | **out**} [*acl-name*]

no default-information {**in** | **out**}

语法说明

acl-name	（可选）指定命名的标准访问列表。
in	配置 EIGRP 接受外部默认路由信息。
out	配置 EIGRP 通告外部路由信息。

默认值

接受并发送外部路由。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

运行配置中只出现此命令的 **no** 形式或指定了访问列表的 **default-information** 命令，因为在默认情况下接受并发送候选默认路由信息。此命令的 **no** 形式不带 *acl-name* 参数。

示例

以下示例禁止接收外部或候选默认路由信息：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

相关命令

命令	说明
router eigrp	创建 EIGRP 路由进程并进入配置模式下为此过程。

default-information originate (BGP)

要配置边界网关协议 (BGP) 路由进程以分配默认路由（网络 0.0.0.0），请在地址系列配置模式下使用 **default-information originate** 命令。要禁用默认路由通告，请使用此命令的 **no** 形式。

default-information originate

no default-information originate

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

default-information originate 命令用于配置 BGP 路由进程以通告默认路由（网络 0.0.0.0）。还必须配置重分布语句来完成此配置，否则不会通告默认路由。

BGP 中 **default-information originate** 命令的配置类似于 **network (BGP)** 命令的配置。但 **default-information originate** 命令需要显式重分布路由 0.0.0.0。**network** 命令只需要内部网关协议 (IGP) 路由表中存在路由 0.0.0.0。因此，**network** 命令是首选。

注意　**default-information originate** 命令和 **neighbor default-originate** 命令不应在同一路由器上配置。而应配置其中之一。

示例

在以下示例中，路由器配置为将默认路由从 OSPF 重分布到 BGP 路由进程：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

相关命令

命令	说明
network	指定要由边界网关协议 (BGP) 和多协议 BGP 路由进程通告的网络。
neighbor default-originate	允许 BGP 发言方（本地路由器）将默认路由 0.0.0.0 发送到邻居以用作默认路由。

default-information originate（OSPFv2 和 OSPFv3）

要生成到 OSPFv2 和 OSPFv3 路由域的默认外部路由，请在路由器配置模式或 IPv6 路由器配置模式下使用 **default-information originate** 命令。要禁用此功能，请使用此命令的 **no** 形式。

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *map-name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *map-name*]]

语法说明

always	（可选）无论软件是否有默认路由，始终通告默认路由。
metric *value*	（可选）指定从 0 到 16777214 的 OSPF 默认指标值。
metric-type {**1** | **2**}	（可选）指定与通告到 OSPF 路由域中的默认路由相关联的外部链路类型。有效值如下所示： • **1** - 类型 1 外部路由。 • **2** - 类型 2 外部路由。
route-map *map-name*	（可选）指定要应用的路由映射的名称。

默认值

默认值如下所示：

- **metric** *value* 为 1。
- **metric-type** 为 2。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	增加了对 OSPFv3 的支持。

使用指南

使用此命令的 **no** 形式并且包含可选关键字和参数只会从命令中删除可选信息。例如，输入 **no default-information originate metric** *3* 命令将会从运行配置中删除命令的 **metric** *3* 选项。要从运行配置删除整个命令，请使用不带任何选项的 **no** 形式命令：**no default-information originate**。

示例

以下示例展示如何使用带可选指标和指标类型的 **default-information originate** 命令：

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	显示全局路由器配置中的 OSPFv2 命令。
ipv6 router ospf	进入 IPv6 路由器配置模式。
show running-config ipv6 router	显示全局路由器配置中的 OSPFv3 命令。

default-information originate (RIP)

要生成到 RIP 的默认路由，请在路由器配置模式下使用 **default-information originate** 命令。要禁用此功能，请使用此命令的 **no** 形式。

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]]

语法说明

route-map *name*	（可选）要应用的路由映射的名称。如果满足路由映射，路由进程将生成默认路由。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在 **default-information originate** 命令中引用的路由映射不能使用扩展访问列表；只能使用标准访问列表。

示例

以下示例展示如何生成到 RIP 的默认路由：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

相关命令

命令	说明
router rip	进入 RIP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

default-language

要设置无客户端 SSL VPN 页面上显示的默认语言，请在 webvpn 配置模式下使用 **default-language** 命令。

default-language *language*

语法说明

language	指定以前导入的转换表的名称。

默认值

默认语言是 en-us（美国英语）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

对于向发起基于浏览器的无客户端 SSL VPN 连接的用户显示的门户网站和屏幕，以及向 AnyConnect VPN 客户端用户显示的用户界面，ASA 提供语言转换。

默认语言在无客户端 SSL VPN 用户最初连接到 ASA 但登录之前显示。此后，显示的语言受隧道组或组策略设置及其引用的任何定制影响。

示例

以下示例使用 with the name *Sales* 将默认语言更改为中文：

```
ciscoasa(config-webvpn)# default-language zh
```

相关命令

命令	说明
import webvpn translation-table	导入转换表。
revert	从缓存内存删除转换表。
show import webvpn translation-table	显示已导入的转换表相关信息。

default-metric

要指定重分布路由的 EIGRP 指标，请在路由器配置模式下使用 **default-metric** 命令。要恢复默认值，请使用此命令的 **no** 形式。

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

语法说明

bandwidth	路由的最小带宽（以每秒千字节为单位）。有效值为从 1 到 4294967295。
delay	路由延迟（以十微秒为单位）。有效值为 1 到 4294967295。
loading	路由的有效带宽（以 1 到 255 的数字表示，255 是 100% 负载）。
mtu	允许的 MTU 最小值，以字节表示。有效值为从 1 到 65535。
reliability	数据包成功传输的可能性（以 0 到 255 的数字表示）。255 表示 100% 可靠； 0 表示不可靠。

默认值

若无默认指标，则只能重分布已连接的路由。重分布的已连接路由指标设为 0。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

除非在 **redistribute** 命令中使用 **metric** 关键字和属性，否则必须使用默认指标将协议重分布到 EIGRP。指标默认值经过仔细设置，适用于各种各样的网络。更改这些值时要非常小心。仅当您从静态路由重分布时才支持保持相同的指标。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密的成本，MTU 值应设置为不低于 1380。将接口设置为低于 1380 字节可能会导致丢包。

示例

以下示例展示重分布的 RIP 路由指标如何转换成如下值的 EIGRP 指标：带宽 = 1000，延迟 = 100，可靠性 = 250，负载 = 100 和 MTU = 1500。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 172.16.0.0
```

```
ciscoasa(config-router)# redistribute rip
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

相关命令

命令	说明
router eigrp	创建 EIGRP 路由进程并进入该进程的路由器配置模式。
redistribute (EIGRP)	将路由重分布到 EIGRP 路由进程。

delay

要设置接口的延迟值，请在接口配置模式下使用 **delay** 命令。要恢复默认延迟值，请使用此命令的 **no** 形式。

delay *delay-time*

no delay

语法说明

delay-time	延迟时间（以十微秒为单位）。有效值为从 1 到 16777215。

默认值

默认延迟取决于接口类型。使用 **show interface** 命令查看接口的延迟值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

输入的值以十微秒为单位。**show interface** 输出中显示的延迟值以微秒为单位。

示例

以下示例将接口上的延迟从默认值 1000 更改为 2000。包含了 **delay** 命令前后的 **show interface** 命令输出删节部分，用以显示该命令对延迟值的影响。延迟值出现在 **show interface** 输出的第二行中 DLY 标签后面。

请注意，将延迟值更改为 2000 的命令是 **delay 200**，不是 **delay 2000**。因为使用 **delay** 命令输入的值以十微秒为单位，而 **show interface** 输出显示微秒。

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
!Remainder of the output removed
```

```
ciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
!Remainder of the output removed
```

相关命令

命令	说明
show interface	显示接口的统计信息和设置。

delete

要从闪存中删除文件，请在特权 EXEC 模式下使用 **delete** 命令。

delete [**/noconfirm**] [**/recursive**] [**/replicate**] [**disk0: | disk1: | flash:**] [*path/*] *filename*

语法说明

/noconfirm	（可选）不提示确认。
/recursive	（可选）循环删除所有子目录中指定的文件。
/replicate	（可选）删除备用设备上指定的文件。
disk0:	（可选）指定内部闪存。
disk1:	（可选）指定外部闪存卡。
filename	指定要删除的文件的名称。
flash:	（可选）指定内部闪存。此关键字与 **disk0** 相同。
path/	（可选）指定文件的路径。

默认值

如果不指定目录，则默认为当前工作目录。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果未指定路径，将从当前工作目录删除文件。删除文件时支持通配符。删除文件时，会提示文件名，您必须确认删除。

示例

以下示例展示如何从当前工作目录中删除名为 test.cfg 的文件：

```
ciscoasa# delete test.cfg
```

相关命令

命令	说明
cd	将当前工作目录更改为指定的目录。
rmdir	删除文件或目录。
show file	显示指定的文件。

deny-message

要更改传送到已成功登录 WebVPN 的远程用户的消息，但又没有 VPN 权限，请在 group-webvpn 配置模式下使用 **deny-message value** 命令。要删除字符串而不让远程用户收到消息，请使用此命令的 **no** 形式。

deny-message value *string*

no deny-message value

语法说明

string	允许最多 491 个字母数字字符，包括特殊字符、空格和标点符号。

默认值

默认拒绝消息为：“Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.”（登录成功，但由于不符合某些条件或者某些特定组策略的原因，您没有权限使用任何 VPN 功能。请联系 IT 管理员了解更多信息。）

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Group-webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令已从隧道组 webvpn 配置模式移到 group-webvpn 配置模式。

使用指南

在输入此命令之前，必须先在全局配置模式下输入 **group-policy** *name* **attributes** 命令，然后输入 **webvpn** 命令。（此步骤假设您已创建策略名称。）

no deny-message none 命令从 group-webvpn 配置中删除属性。策略继承属性值。

在 **deny-message value** 命令中键入字符串时，即使命令被截断显示也要继续键入。

远程用户登录后其浏览器上显示的文本，与用于 VPN 会话的隧道策略无关。

示例

以下示例展示用于创建内部组策略 group2 的第一个命令。后续命令修改与该策略关联的拒绝消息：

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK.However,
you have not been granted rights to use the VPN features.Contact your administrator for
more information."
ciscoasa(config-group-webvpn)
```

相关命令

命令	说明
clear configure group-policy	删除所有组策略配置。
group-policy	创建组策略。
group-policy attributes	进入组策略属性配置模式。
show running-config group-policy	显示指定策略的运行组策略配置。
webvpn	进入组策略 webvpn 配置模式。

deny version

要拒绝特定版本的 SNMP 流量，请在 snmp-map 配置模式下使用 **deny version** 命令。要禁用此命令，请使用此命令的 **no** 形式。

deny version *version*

no deny version *version*

语法说明

version	指定 ASA 丢弃的 SNMP 流量的版本。允许的值是 **1**、**2**、**2c** 和 **3**。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Snmp-map 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **deny version** 命令将流量限定为特定的 SNMP 版本。SNMP 的早期版本不够安全，因此您的安全策略可能指定将 SNMP 流量限定为版本 2。在 SNMP 映射（使用 **snmp-map** 命令配置，可通过在全局配置模式下输入 **snmp-map** 命令来访问）中使用 **deny version** 命令。创建 SNMP 映射后，您可以使用 **inspect snmp** 命令启用映射，然后使用 **service-policy** 命令将其应用到一个或多个接口。

示例

以下示例展示如何标识 SNMP 流量、定义 SNMP 映射、定义策略以及将策略应用到外部接口：

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
inspect snmp	启用 SNMP 应用检查。
policy-map	将类映射与特定安全操作关联。
snmp-map	定义 SNMP 地图并启用 SNMP 映射配置模式。
service-policy	将策略映射应用于一个或多个接口。

description

要对指定的配置单元（例如，对情景或对象组，或者对 DAP 记录）添加说明，请在各种配置模式下使用 **description** 命令。要删除说明，请使用此命令的 **no** 形式。

description *text*

no description

语法说明

text	将说明设置为最多 200 个字符的文本字符串。说明在配置中添加有用的注释。对于 dynamic-access-policy-record 模式，最大长度为 80 个字符。对于事件管理器小应用，最大长度为 256 个字符。 如果要在字符串中包含问号 (?)，必须在键入问号之前键入 **Ctrl-V**，以免无意中调用 CLI 帮助。

默认值

没有默认行为或值。

命令模式

此命令可用于各种配置模式。

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	增加了对 dynamic-access-policy-record 配置模式的支持。
9.2(1)	增加了对事件管理器小应用配置模式的支持。

示例

以下示例向 “ 管理情景配置 ” 添加说明：

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)# config-url flash://admin.cfg
```

相关命令

命令	说明
class-map	识别在 **policy-map** 命令中要应用操作的流量。
context	在系统配置中创建安全情景并进入情景配置模式。
gtp-map	控制 GTP 检测引擎的参数。
interface	配置接口并进入接口配置模式。
object-group	识别要包含在 **access-list** 命令中的流量。
policy-map	识别要应用到 **class-map** 命令确定的流量的操作。

dhcp client route distance

要为通过 DHCP 获知的路由配置管理距离，请在接口配置模式下使用 **dhcp client route distance** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

dhcp client route distance *distance*

no dhcp client route distance *distance*

语法说明

distance	应用于通过 DHCP 获知的路由的管理距离。有效值为从 1 到 255。

默认值

默认情况下，为通过 DHCP 获知的路由提供的管理距离为 1。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

仅当从 DHCP 获知路由时，才检查 **dhcp client route distance** 命令。如果在从 DHCP 获知路由后输入 **dhcp client route distance** 命令，则指定的管理距离不影响现有已获知的路由。仅输入该命令后获知的路由才具有指定的管理距离。

必须在 **ip address dhcp** 命令中指定 **setroute** 选项才可通过 DHCP 获取路由。

如果已在多个接口上配置 DHCP，则您必须在每个接口上使用 **dhcp client route distance** 命令来指示已安装路由的优先级。

示例

以下示例在千兆位以太网 0/2 接口上通过 DHCP 获得默认路由。通过跟踪条目对象 1 可跟踪路由。SLA 操作可监控外部接口外 10.1.1.1 网关的可用性。如果 SLA 操作失败，则会在 GigabitEthernet0/3 上使用通过 DHCP 获取的备用路由。为备用路由分配的管理距离为 254。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
```

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

相关命令

命令	说明
dhcp client route track	将通过 DHCP 获知的路由与跟踪条目对象关联。
ip address dhcp	使用通过 DHCP 获得的 IP 地址配置指定接口。
sla monitor	定义 SLA 监控操作。
track rtr	创建用于轮询 SLA 的跟踪条目。

dhcp client route track

要配置 DHCP 客户端以将已添加的路由与指定的跟踪对象编号关联，请在接口配置模式下使用 **dhcp client route track** 命令。要禁用 DHCP 客户端路由跟踪，请使用此命令的 **no** 形式。

dhcp client route track *number*

no dhcp client route track

语法说明

number	跟踪条目对象 ID。有效值为从 1 到 500。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

仅当从 DHCP 获知路由时，才检查 **dhcp client route track** 命令。如果在从 DHCP 获知路由后输入 **dhcp client route track** 命令，则现有已获知的路由不与跟踪对象关联。必须按正确顺序添加以下两个命令。确保始终先输入 **dhcp client route track** 命令，然后输入 **ip address dhcp setroute** 命令。如果已输入 **ip address dhcp setroute** 命令，则删除它，然后按上述顺序重新输入。仅输入该命令后获知的路由才与指定的跟踪对象关联。

必须在 **ip address dhcp** 命令中指定 **setroute** 选项才可通过 DHCP 获取路由。

如果已在多个接口上配置 DHCP，则您必须在每个接口上使用 **dhcp client route distance** 命令来指示已安装路由的优先级。

示例

以下示例在千兆位以太网 0/2 接口上通过 DHCP 获得默认路由。通过跟踪条目对象 1 可跟踪路由。SLA 操作可监控外部接口外 10.1.1.1 网关的可用性。如果 SLA 操作失败，则会在 GigabitEthernet0/3 上使用通过 DHCP 获取的备用路由。为备用路由分配的管理距离为 254。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
```

```
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

相关命令

命令	说明
dhcp client route distance	将管理距离分配给通过 DHCP 获知的路由。
ip address dhcp	使用通过 DHCP 获得的 IP 地址配置指定接口。
sla monitor	定义 SLA 监控操作。
track rtr	创建用于轮询 SLA 的跟踪条目。

dhcp-client broadcast-flag

要允许 ASA 在 DHCP 客户端数据包中设置广播标志，请在全局配置模式下使用 **dhcp-client broadcast-flag** 命令。要禁止广播标志，请使用此命令的 **no** 形式。

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

语法说明

此命令没有任何参数或关键字。

默认值

默认禁用广播标志。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果使用 **ip address dhcp** 命令为接口启用 DHCP 客户端，则当 DHCP 客户端发送发现请求 IP 地址时，便可使用此命令在 DHCP 数据包报头中将广播标志设置为 1。DHCP 服务器侦听此广播标志，并在标志设置为 1 时广播应答数据包。

如果输入 **no dhcp-client broadcast-flag** 命令，则广播标志设置为 0，并且 DHCP 服务器使用提供的 IP 地址将应答数据包单播到客户端。

DHCP 客户端可从 DHCP 服务器接收广播和单播。

示例

以下示例启用广播标志：

```
ciscoasa(config)# dhcp-client broadcast-flag
```

相关命令

命令	说明
ip address dhcp	对接口启用 DHCP 客户端。
interface	进入接口配置模式，让您设置 IP 地址。
dhcp-client client-id	将 DHCP 请求数据包选项 61 设置为包含接口 MAC 地址。
dhcp-client update dns	对 DHCP 客户端启用 DNS 更新。

dhcp-client client-id

要强制 MAC 地址存储在选项 61 的 DHCP 请求数据包内而不是默认内部生成的字符串内，请在全局配置模式下使用 **dhcp-client client-id** 命令。要禁止 MAC 地址，请使用此命令的 **no** 形式。

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

语法说明

interface *interface_name*	指定要为选项 61 启用 MAC 地址的接口。

默认值

默认情况下，内部生成的 ASCII 字符串用于选项 61。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果使用 **ip address dhcp** 命令对接口启用 DHCP 客户端，某些 ISP 预期选项 61 将成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。使用 **dhcp-client client-id** 命令包含选项 61 的接口 MAC 地址。

示例

以下示例为外部接口启用选项 61 的 MAC 地址：

```
ciscoasa(config)# dhcp-client client-id interface outside
```

相关命令

命令	说明
ip address dhcp	对接口启用 DHCP 客户端。
interface	进入接口配置模式，让您设置 IP 地址。
dhcp-client broadcast-flag	在 DHCP 客户端数据包中设置广播标志。
dhcp-client update dns	对 DHCP 客户端启用 DNS 更新。

dhcp-client update dns

要配置 DHCP 客户端传递到 DHCP 服务器的更新参数，请在全局配置模式下使用 **dhcp-client update dns** 命令。要删除 DHCP 客户端传递到 DHCP 服务器的参数，请使用此命令的 **no** 形式。

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

语法说明

both	DHCP 服务器更新 DNS A 和 PTR 资源记录的客户端请求。
none	DHCP 服务器不执行 DDNS 更新的客户端请求。
server	指定 DHCP 服务器接收客户端请求。

默认值

默认情况下，ASA 请求 DHCP 服务器只执行 PTR RR 更新。客户端不将 FQDN 选项发送到服务器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令也可在接口配置模式下输入，但不能使用连字符连接。请参阅 **dhcp client update dns** 命令。在接口模式下输入时，**dhcp client update dns** 命令会覆盖此命令在全局配置模式下配置的设置。

示例

以下示例配置客户端请求 DHCP 服务器不更新 A 或 PTR RR：

```
ciscoasa(config)# dhcp-client update dns server none
```

以下示例配置客户端请求服务器更新 A 和 PTR RR：

```
ciscoasa(config)# dhcp-client update dns server both
```

相关命令

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update	将 DDNS 更新方法与 ASA 接口或 DDNS 更新主机名关联。
ddns update method	创建一个用于动态更新 DNS 资源记录的方法。

命令	说明
dhcpd update dns	启用 DHCP 服务器以执行 DDNS 更新。
interval maximum	配置 DDNS 更新方法的更新尝试之间的最大间隔。

dhcp-network-scope

要指定 ASA DHCP 服务器用来向此组策略的用户分配地址的 IP 地址范围，请在 group-policy 配置模式下使用 **dhcp-network-scope** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

dhcp-network-scope {*ip_address*} | **none**

no dhcp-network-scope

语法说明

ip_address	指定 DHCP 服务器用来向此组策略的用户分配 IP 地址的 IP 子网。
none	将 DHCP 子网设置为 null 值，从而不允许 IP 地址。防止从默认或指定的组策略继承值。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Group-policy	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令允许从其他组策略继承值。要禁止继承值，请使用 **dhcp-network-scope none** 命令。

示例

以下示例展示如何为组策略 FirstGroup 设置 10.10.85.1 的 IP 子网：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

dhcp-server

要配置支持 DHCP 服务器在 VPN 隧道建立时向客户端分配地址，请在隧道组常规属性配置模式下使用 **dhcp-server** 命令。要将此命令恢复为默认值，请使用此命令的 **no** 形式。

dhcp-server [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

语法说明

ip1	DHCP 服务器的地址
ip2-ip10	（可选）额外 DHCP 服务器的地址。最多可以指定 10 个地址，可在一个命令中指定，也可分布于多个命令中。
link-selection	（可选）指定 ASA 应发送 DHCP 子选项 5 - 中继信息选项 82 的链路选择子选项，由 RFC 3527 定义。这只能用于支持此 RFC 的服务器。
subnet-selection	（可选）指定 ASA 应发送 DHCP 选项 118 - IPv4 子网选择选项，由 RFC 3011 定义。这只能用于支持此 RFC 的服务器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(5)	添加了 **link-selection** 和 **subnet-selection** 关键字。

使用指南

您可以将此属性只应用到远程访问隧道组类型。

示例

以下命令在 config-general 配置模式下输入，用于将三个 DHCP 服务器（dhcp1、dhcp2 和 dhcp3）添加到 IPsec 远程访问隧道组 “remotegrp”：

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

相关命令

命令	说明
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	指定命名的隧道组的常规属性。

第 12 章

dhcpd address 至 distribute-list out (BGP) 命令

dhcpd address

要定义 DHCP 服务器使用的 IP 地址池，请在全局配置模式下使用 **dhcpd address** 命令。要删除现有 DHCP 地址池，请使用此命令的 **no** 形式。

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

语法说明

interface_name	向其分配地址池的接口。
IP_address1	DHCP 地址池的开始地址。
IP_address2	DHCP 地址池的结束地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA DHCP 服务器的地址池必须在与用于启用该地址池的 ASA 接口相同的子网内，且您必须使用 *interface_name* 指定关联的 ASA 接口。

ASA 上地址池的大小不得超过每个池 256 个地址。如果地址池范围大于 253 个地址，则 ASA 接口的网络掩码不能为 C 类地址（例如 255.255.255.0）且需要成为更大的地址，例如 255.255.254.0。

DHCP 客户端必须在物理上连接到 ASA DCHP 服务器接口的子网。

dhcpd address 命令无法使用带有 “-”（破折号）字符的接口名称，因为此字符解释为范围说明符而不是对象名称的一部分。

no dhcpd address *interface_name* 命令删除您为指定接口配置的 DHCP 服务器地址池。

请参阅 *CLI 配置指南*，了解有关如何在 ASA 中实施 DHCP 服务器功能的信息。

示例

以下示例展示如何在 ASA 的 DMZ 接口上为 DHCP 客户端配置地址池和 DNS 服务器：

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

以下示例展示如何在内部接口上配置 DHCP 服务器。**dhcpd address** 命令在该接口上向 DHCP 服务器分配一个包含 10 个 IP 地址的池。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
dhcpd enable	在指定接口上启用 DHCP 服务器。
show dhcpd	显示 DHCP 绑定、统计或状态信息。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd auto_config

要使 ASA 能够自动根据从运行 DHCP 或 PPPoE 客户端的接口或从 VPN 服务器获取的值为 DHCP 服务器配置 DNS、WINS 和域名值，请在全局配置模式下使用 **dhcpd auto_config** 命令。要终止 DHCP 参数的自动配置，请使用此命令的 **no** 形式。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

语法说明

client_if_name	指定运行提供 DNS、WINS 和域名参数的 DHCP 客户端的接口。
interface *if_name*	指定要应用操作的接口。
vpnclient-wins-override	使用 VPN 客户端参数覆盖接口 DHCP 或 PPPoE 客户端 WINS 参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果使用 CLI 命令指定 DNS、WINS 或域名参数，则 CLI 配置的参数覆盖通过自动配置获取的参数。

示例

以下示例展示如何在内部接口上配置 DHCP。**dhcpd auto_config** 命令用于将从外部接口上的 DHCP 客户端获取的 DNS、WINS 和域信息传递给内部接口上的 DHCP 客户端。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
dhcpd enable	在指定接口上启用 DHCP 服务器。
show ip address dhcp server	显示有关 DHCP 服务器为充当 DHCP 客户端的接口提供的 DHCP 选项的详细信息。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd dns

要定义 DHCP 客户端的 DNS 服务器，请在全局配置模式下使用 **dhcpd dns** 命令。要清除定义的服务器，请使用此命令的 **no** 形式。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

语法说明

dnsip1	指定 DHCP 客户端的主 DNS 服务器的 IP 地址。
dnsip2	（可选）指定 DHCP 客户端的备用 DNS 服务器的 IP 地址。
interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

dhcpd dns 命令允许您指定 DHCP 客户端的 DNS 服务器的 IP 地址或地址。您可以指定两个 DNS 服务器。**no dhcpd dns** 命令允许您从配置中删除 DNS IP 地址。

示例

以下示例展示如何在 ASA 的 DMZ 接口上为 DHCP 客户端配置地址池和 DNS 服务器。

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
dhcpd address	在指定接口上指定 DHCP 服务器使用的地址池。
dhcpd enable	在指定接口上启用 DHCP 服务器。

命令	说明
dhcpd wins	定义 DHCP 客户端的 WINS 服务器。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd domain

要定义 DHCP 客户端的 DNS 域名，请在全局配置模式下使用 **dhcpd domain** 命令。要清除 DNS 域名，请使用此命令的 **no** 形式。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

语法说明

domain_name	指定 DNS 域名 (example.com)。
interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

dhcpd domain 命令允许您指定 DHCP 客户端的 DNS 域名。**no dhcpd domain** 命令允许您从配置中删除 DNS 域服务器。

示例

以下示例展示如何配置 ASA 上的 DHCP 服务器向 DHCP 客户端提供的域名：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd enable

要启用 DHCP 服务器，请在全局配置模式下使用 **dhcpd enable** 命令。要禁用 DHCP 服务器，请使用此命令的 **no** 形式。

dhcpd enable *interface*

no dhcpd enable *interface*

语法说明

interface	指定要启用 DHCP 服务器的接口。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

DHCP 服务器向 DHCP 客户端提供网络配置参数。对在 ASA 中的 DHCP 服务器的支持意味着 ASA 可以使用 DHCP 配置连接的客户端。**dhcpd enable** *interface* 命令允许您启用 DHCP 后台守护程序以在启用 DHCP 的接口上侦听 DHCP 客户端请求。**no dhcpd enable** 命令在指定接口上禁用 DHCP 服务器功能。

注意　对于多情景模式，您无法在多个情景使用的接口（共享 VLAN）上启用 DHCP 服务器。

在 ASA 响应 DHCP 客户端请求时，它将接收请求的接口的 IP 地址和子网掩码用作响应中的默认网关的 IP 地址和子网掩码。

注意　ASA DHCP 服务器后台守护程序不支持直接连接到 ASA 接口的客户端。

请参阅 CLI 配置指南，了解有关如何在 ASA 中实施 DHCP 服务器功能的信息。

示例

以下示例展示如何在内部接口上启用 DHCP 服务器：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
debug dhcpd	显示 DHCP 服务器的调试信息。
dhcpd address	在指定接口上指定 DHCP 服务器使用的地址池。
show dhcpd	显示 DHCP 绑定、统计或状态信息。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd lease

要指定 DHCP 租赁长度，请在全局配置模式下使用 **dhcpd lease** 命令。要恢复租赁的默认值，请使用此命令的 **no** 形式。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

语法说明

interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。
lease_length	指定 DHCP 服务器向 DHCP 客户端授予的 IP 地址租赁的长度（以秒为单位）。有效值为从 300 到 1048575 秒。

默认值

默认 *lease_length* 为 3600 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

dhcpd lease 命令允许您指定向 DHCP 客户端授予的租赁的长度（以秒为单位）。此租赁指示 DHCP 客户端可以使用 DHCP 服务器授予的所分配 IP 地址的时间长度。

通过 **no dhcpd lease** 命令，您可以从配置中删除指定的租赁长度并使用默认值 3600 秒替换此值。

示例

以下示例展示如何为 DHCP 客户端指定 DHCP 信息的租赁的长度：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd option

要配置 DHCP 选项，请在全局配置模式下使用 **dhcpd option** 命令。要清除该选项，请使用此命令的 **no** 形式。

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

语法说明

ascii *string*	指定选项参数是不带有空格的 ASCII 字符字符串。
code	指定一个代表正在设置的 DHCP 选项的数字。有效值为 0 到 255，其中存在几个例外。请参阅 “ 使用指南 ” 部分，了解不支持的 DHCP 选项代码的列表。
hex *hex_string*	指定选项参数是十六进制字符串，其中包含偶数个数字，且没有空格。您无需使用 0x 前缀。
interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。
ip	指定选项参数是 IP 地址。您可使用 **ip** 关键字指定最多两个 IP 地址。
IP_address	指定一个点分十进制 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以使用 **dhcpd option** 命令向思科 IP 电话和路由器提供 TFTP 服务器信息。

当 DHCP 选项请求到达 ASA DHCP 服务器时，ASA 将 **dhcpd option** 命令指定的一个或多个值置于对客户端的响应中。

dhcpd option 66 和 **dhcpd option 150** 命令指定思科 IP 电话和路由器可用于下载配置文件的 TFTP 服务器。使用以下这些命令：

- **dhcpd option 66 ascii** *string*，其中 *string* 是 TFTP 服务器的 IP 地址或主机名。仅可为选项 66 指定一个 TFTP 服务器。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]，其中 *IP_address* 是 TFTP 服务器的 IP 地址。您可为选项 150 指定最多两个 IP 地址。

注意　**dhcpd option 66** 命令仅采用一个 **ascii** 参数，且 **dhcpd option 150** 仅采用一个 **ip** 参数。

在为 **dhcpd option 66 | 150** 命令指定 IP 地址时，请使用以下指南：

- 如果 TFTP 服务器位于 DHCP 服务器接口上，请使用 TFTP 服务器的本地 IP 地址。
- 如果 TFTP 服务器所在接口的安全性低于 DHCP 服务器接口，则应用通用出站规则。为 DHCP 客户端创建一组 NAT 全局访问列表条目，并使用 TFTP 服务器的实际 IP 地址。
- 如果 TFTP 服务器位于更安全的接口上，则应用通用入站规则。为 TFTP 服务器创建一组静态访问列表语句，并使用 TFTP 服务器的全局 IP 地址。

有关其他 DHCP 选项的信息，请参阅 RFC 2132。

注意　ASA 不验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值匹配。例如，您可以输入 **dhcpd option 46 ascii hello** 命令，虽然在 RFC 2132 中将选项 46 定义为单个数字的十六进制值，但 ASA 接受配置。

您无法使用 **dhcpd option** 命令配置以下 DHCP 选项：

选项代码	说明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

示例

以下示例展示如何指定 DHCP 选项 66 的 TFTP 服务器：

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd ping_timeout

要更改 DHCP ping 的默认超时，请在全局配置模式下使用 **dhcpd ping_timeout** 命令。要恢复默认值，请使用此命令的 **no** 形式。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

语法说明

interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。
number	ping 的超时值，以毫秒为单位。最小值为 10，最大值为 10000。默认值为 50。

默认值

number 的默认毫秒数是 50。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

为避免地址冲突，DHCP 服务器先将两个 ICMP ping 数据包发送到一个地址，然后将该地址分配给 DHCP 客户端。ASA 先等待两个 ICMP ping 数据包超时，然后将 IP 地址分配给 DHCP 客户端。例如，如果使用默认值，则 ASA 在分配 IP 地址前等待 1500 毫秒（每个 ICMP ping 数据包需要等待 750 毫秒）。

长 ping 超时值会对 DHCP 服务器的性能造成不利影响。

示例

以下示例展示如何使用 **dhcpd ping_timeout** 命令更改 DHCP 服务器的 ping 超时值：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcpd update dns

要使 DHCP 服务器能够执行 DDNS 更新，请在全局配置模式下使用 **dhcpd update dns** 命令。要通过 DHCP 服务器禁用 DDNS，请使用此命令的 **no** 形式。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

语法说明

both	指定 DHCP 服务器更新 A 和 PTR DNS RR。
interface	指定要应用 DDNS 更新的 ASA 接口。
override	指定 DHCP 服务器覆盖 DHCP 客户端请求。
srv_ifc_name	指定要应用此选项的接口。

默认值

默认情况下，DHCP 服务器仅执行 PTR RR 更新。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

DDNS 更新 DNS 维护的名称 - 地址和地址 - 名称映射。配合 DHCP 服务器执行更新。**dhcpd update dns** 命令通过服务器启用更新。

名称和地址映射包含在两种类型的 RR 中：

- A 资源记录包含域名 -IP 地址映射。
- PTR 资源记录包含 IP 地址到域名的映射。

DDNS 更新可用于保持 A 和 PTR RR 类型之间的信息一致。

使用 **dhcpd update dns** 命令，您可以将 DHCP 服务器配置为执行 A 和 PTR RR 更新或仅执行 PTR RR 更新。您也可以将其配置为覆盖来自 DHCP 客户端的更新请求。

示例

以下示例配置 DDNS 服务器以执行 A 和 PTR 更新并覆盖来自 DHCP 客户端的请求：

```
ciscoasa(config)# dhcpd update dns both override
```

相关命令

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update	将 DDNS 更新方法与 ASA 接口或一个 DDNS 更新主机名关联。
ddns update method	创建一个用于动态更新 DNS 资源记录的方法。
dhcp-client update dns	配置 DHCP 客户端要向 DHCP 服务器传送的更新参数。
interval maximum	配置 DDNS 更新方法的更新尝试之间的最大间隔。

dhcpd wins

要定义 DHCP 客户端的 WINS 服务器 IP 地址，请在全局配置模式下使用 **dhcpd wins** 命令。要从配置中删除 WINS 服务器 IP 地址，请使用此命令的 **no** 形式。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

语法说明

interface *if_name*	指定要应用输入到服务器的值的接口。如果未指定接口，则将值应用于所有服务器。
server1	指定主 Microsoft NetBIOS 名称服务器（WINS 服务器）的 IP 地址。
server2	（可选）指定备用 Microsoft NetBIOS 名称服务器（WINS 服务器）的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

dhcpd wins 命令允许您指定 DHCP 客户端的 WINS 服务器的地址。**no dhcpd wins** 命令从配置中删除 WINS 服务器 IP 地址。

示例

以下示例展示如何指定发送给 DHCP 客户端的 WINS 服务器信息：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

相关命令

命令	说明
clear configure dhcpd	删除所有 DHCP 服务器设置。
dhcpd address	在指定接口上指定 DHCP 服务器使用的地址池。
dhcpd dns	定义 DHCP 客户端的 DNS 服务器。
show dhcpd	显示 DHCP 绑定、统计或状态信息。
show running-config dhcpd	显示当前 DHCP 服务器配置。

dhcprelay enable

要启用 DHCP 中继代理，请在全局配置模式下使用 **dhcprelay enable** 命令。要禁用 DHCP 中继代理，请使用此命令的 **no** 形式。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

语法说明

interface_name	DHCP 中继代理用来接受客户端请求的接口的名称。

默认值

禁用 DHCP 中继代理。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

DHCP 中继代理允许将 DHCP 请求从指定的 ASA 接口转发到指定的 DHCP 服务器。

要让 ASA 使用 **dhcprelay enable** *interface_name* 命令启动 DHCP 中继代理，您必须已在配置中具有一个 **dhcprelay server** 命令。否则，ASA 显示类似于以下内容的错误消息：

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

您无法在以下条件下启用 DHCP 中继：

- 您无法在同一接口上启用 DHCP 中继和 DHCP 中继服务器。
- 您无法在同一接口上启用 DCHP 中继和 DHCP 服务器 (**dhcpd enable**)。
- 如果也启用了 DHCP 服务器，则无法启用 DHCP 中继代理。
- 对于多情景模式，您无法在多个情景使用的接口（共享 VLAN）上启用 DHCP 中继。

no dhcprelay enable *interface_name* 命令为仅由 *interface_name* 参数指定的接口删除 DHCP 中继代理配置。

示例

以下示例展示如何使用以下信息为 DHCP 服务器配置 DHCP 中继代理：ASA 的外部接口上具有 IP 地址 10.1.1.1、ASA 的内部接口上具有客户端请求，以及超时值最多 90 秒：

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

以下示例展示如何禁用 DHCP 中继代理：

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
debug dhcp relay	显示 DHCP 中继代理的调试信息。
dhcprelay server	指定 DHCP 中继代理要向其转发 DHCP 请求的 DHCP 服务器。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay information trust-all

要将指定接口配置为受信任接口，请在全局配置模式下使用 **dhcprelay information trust-all** 命令。

dhcprelay information trust-all

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令将给定接口配置为受信任接口。要查看特定于接口的受信任配置，请在接口配置模式下使用 **show running-config dhcprelay interface** 命令。要在接口配置模式下将给定接口配置为受信任接口，请使用 **dhcprelay information trusted** 命令。要在全局配置模式下将给定接口视为受信任接口，请使用 **show running-config dhcprelay** 命令。

示例

以下示例展示如何在全局配置模式下将指定接口配置为受信任接口：

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。
dhcprelay timeout	指定 DHCP 中继代理的超时值。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay information trusted

要将指定接口配置为受信任接口，请在接口配置模式下使用 **dhcprelay information trusted** 命令。

dhcprelay information trusted

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令将给定接口配置为受信任接口。要查看特定于接口的受信任配置，请在接口配置模式下使用 **show running-config dhcprelay interface** 命令。要在全局配置模式下将给定接口配置为受信任接口，请使用 **dhcprelay information trust-all** 命令。要在全局配置模式下将给定接口视为受信任接口，请使用 **show running-config dhcprelay** 命令。

示例

以下示例展示如何将指定接口配置为受信任接口：

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。

命令	说明
dhcprelay timeout	指定 DHCP 中继代理的超时值。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay server (global)

要指定向其转发 DHCP 请求的 DHCP 服务器，请在全局配置模式下使用 **dhcpreplay server** 命令。要从 DHCP 中继配置中删除 DHCP 服务器，请使用此命令的 **no** 形式。

dhcprelay server [*interface_name*]

no dhcprelay server [*interface_name*]

语法说明

interface_name	指定 DHCP 服务器所驻留的 ASA 接口的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

DHCP 中继代理允许将 DHCP 请求从指定的 ASA 接口转发到指定的 DHCP 服务器。您可以为每个接口添加最多十个 DHCP 中继服务器。在输入 **dhcprelay enable** 命令前，您必须至少向 ASA 配置添加一个 **dhcprelay server** 命令。您无法在配置了 DHCP 中继服务器的接口上配置 DHCP 客户端。

一旦将 **dhcprelay enable** 命令添加到配置，**dhcprelay server** 命令就会在指定接口上打开 UDP 端口 67 并启动 DHCP 中继任务。

示例

以下示例展示如何使用以下信息为 DHCP 服务器配置 DHCP 中继代理：ASA 的外部接口上具有 IP 地址 10.1.1.1、ASA 的内部接口上具有客户端请求，以及超时值最多 90 秒：

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。
dhcprelay timeout	指定 DHCP 中继代理的超时值。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay server（接口）（9.1(2) 及更高版本）

要指定向其转发 DHCP 请求的 DHCP 中继接口服务器，请在接口配置模式下使用 **dhcpreplay server** 命令。要从 DHCP 中继配置中删除 DHCP 中继接口服务器，请使用此命令的 **no** 形式。

dhcprelay server *ip_address*

no dhcprelay server *ip_address*

语法说明

ip_address	指定 DHCP 中继代理要向其转发客户端 DHCP 请求的 DHCP 中继接口服务器的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

DHCP 中继代理允许将 DHCP 请求从指定的 ASA 接口转发到指定的 DHCP 服务器。您可以为每个接口添加最多四个 DHCP 中继服务器。在输入 **dhcprelay enable** 命令前，您必须至少向 ASA 配置添加一个 **dhcprelay server** 命令。您无法在配置了 DHCP 中继服务器的接口上配置 DHCP 客户端。

一旦将 **dhcprelay enable** 命令添加到配置，**dhcprelay server** 命令就会在指定接口上打开 UDP 端口 67 并启动 DHCP 中继任务。

在接口配置模式下，您可以使用 **dhcprelay server** *ip_address* 命令在每个接口上配置一个 DHCP 中继服务器（称为帮助程序）地址。这意味着，当接口上收到 DHCP 请求时，它对帮助程序地址进行配置，然后仅将该请求转发到那些服务器。

使用 **no dhcprelay server** *ip_address* 命令时，接口停止将 DHCP 数据包转发到该服务器，并为仅由 *ip_address* 参数指定的 DHCP 服务器删除 DHCP 中继代理配置。

此命令优先于在全局配置模式下配置的 DHCP 中继服务器。这意味着 DHCP 中继代理首先将客户端发现消息转发到 DHCP 中继接口服务器，然后到 DHCP 全局中继服务器。

示例

以下示例展示如何使用以下信息为 DHCP 中继接口服务器配置 DHCP 中继代理：ASA 的外部接口上具有 IP 地址 10.1.1.1、ASA 的内部接口上具有客户端请求，以及超时值最多 90 秒：

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90

interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。
dhcprelay timeout	指定 DHCP 中继代理的超时值。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay setroute

要在 DHCP 应答中设置默认网关地址，请在全局配置模式下使用 **dhcprelay setroute** 命令。要删除默认路由器，请使用此命令的 **no** 形式。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

语法说明

interface	配置 DHCP 中继代理以将第一个默认 IP 地址（在从 DHCP 服务器发送的数据包中）更改为 *interface* 的地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令导致指定的 ASA 接口的地址取代 DHCP 应答的默认 IP 地址。**dhcprelay setroute** *interface* 命令允许您启用 DHCP 中继代理以将第一个默认路由器地址（在从 DHCP 服务器发送的数据包中）更改为 *interface* 的地址。

如果数据包中没有默认路由器选项，则 ASA 添加一个包含 *interface* 的地址的路由器选项。此操作允许客户端将其默认路由设置为指向 ASA。

不配置 **dhcprelay setroute** *interface* 命令（且数据包中有一个默认路由器选项）时，它通过 ASA 且不更改路由器地址。

示例

以下示例展示如何在从外部 DHCP 服务器到 ASA 内部接口的 DHCP 应答中设置默认网关：

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。
dhcprelay server	指定 DHCP 中继代理要向其转发 DHCP 请求的 DHCP 服务器。
dhcprelay timeout	指定 DHCP 中继代理的超时值。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dhcprelay timeout

要设置 DHCP 中继代理超时值，请在全局配置模式下使用 **dhcprelay timeout** 命令。要将超时值恢复为其默认值，请使用此命令的 **no** 形式。

dhcprelay timeout *seconds*

no dhcprelay timeout

语法说明

seconds	指定 DHCP 中继地址协商所允许的秒数。

默认值

DHCP 中继超时的默认值为 60 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

dhcprelay timeout 命令允许您设置将来自 DHCP 服务器的响应通过中继绑定结构传递给 DHCP 客户端所允许的时间量（以秒为单位）。

示例

以下示例展示如何使用以下信息为 DHCP 服务器配置 DHCP 中继代理：ASA 的外部接口上具有 IP 地址 10.1.1.1、ASA 的内部接口上具有客户端请求，以及超时值最多 90 秒：

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

相关命令

命令	说明
clear configure dhcprelay	删除所有 DHCP 中继代理设置。
dhcprelay enable	在指定接口上启用 DHCP 中继代理。

命令	说明
dhcprelay server	指定 DHCP 中继代理要向其转发 DHCP 请求的 DHCP 服务器。
dhcprelay setroute	定义用作 DHCP 应答中的默认路由器地址的 DHCP 中继代理的 IP 地址。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

dialog

要定制向 WebVPN 用户显示的对话框消息，请在 WebVPN 定制配置模式下使用 **dialog** 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。

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

语法说明

border	指定对边界的更改。
message	指定对消息的更改。
style	指定对样式的更改。
title	指定对标题的更改。
value	要显示的实际文本或 CSS 参数（最大值是 256 个字符）。

默认值

默认标题样式是 background-color:#669999;color:white。

默认消息样式是 background-color:#99CCCC;color:black。

默认边界样式是 border:1px solid black;border-collapse:collapse。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 定制配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的 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，请查询网址为 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。

注意　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

以下示例定制对话框消息，其中将前景色更改为蓝色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# dialog message style color:blue
```

相关命令

命令	说明
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。

dir

要显示目录内容，请在特权 EXEC 模式下使用 **dir** 命令。

dir [**/all**] [**all-filesystems**] [**/recursive**] [**disk0: | disk1: | flash: | system:**] [*path*]

语法说明

/all	（可选）显示所有文件。
/recursive	（可选）递归显示目录内容。
all-filesystems	（可选）显示所有文件系统的文件。
disk0:	（可选）指定内部闪存后 , 跟冒号。
disk1:	（可选）指定外部闪存卡后 , 跟冒号。
flash:	（可选）显示默认闪存分区的目录内容。
path	（可选）指定特定路径。
system:	（可选）显示文件系统的目录内容。

默认值

如果不指定目录，则默认为当前工作目录。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

没有关键字或参数的 **dir** 命令显示当前目录的内容。

示例

以下示例展示如何显示目录内容：

```
ciscoasa# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

以下示例展示如何递归显示整个文件系统的内容：

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

以下示例展示如何显示闪存分区的内容：

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

相关命令

命令	说明
cd	将当前工作目录更改为指定的目录。
pwd	系统随即会显示当前工作目录。
mkdir	创建目录。
rmdir	删除目录。

disable

要退出特权 EXEC 模式并返回到无特权 EXEC 模式，请在特权 EXEC 模式下使用 **disable** 命令。

disable

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **enable** 命令进入特权模式。**disable** 命令允许您退出特权模式并返回到无特权模式。

示例

以下示例展示如何进入特权模式：

```
ciscoasa> enable
ciscoasa#
```

以下示例展示如何退出特权模式：

```
ciscoasa# disable
ciscoasa>
```

相关命令

命令	说明
enable	启用特权 EXEC 模式。

disable（缓存）

要禁用对 WebVPN 的缓存，请在缓存配置模式下使用 **disable** 命令。要重新启用缓存，请使用此命令的 **no** 版本。

disable

no disable

默认值

使用每个缓存属性的默认设置启用缓存。

命令模式

下表显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	单个	情景	系统
缓存配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

缓存技术会在系统缓存中存储经常重新使用的对象，从而减少执行重复重写和内容压缩的需要。它可减少 WebVPN 与远程服务器和最终用户浏览器之间的流量，从而提高许多应用的运行效率。

示例

以下示例展示如何禁用缓存，然后如何重新启用它。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

相关命令

命令	说明
cache	进入 WebVPN 缓存配置模式。
cache-compressed	配置 WebVPN 缓存压缩。
expiry-time	配置不需要重新验证即缓存对象的到期时间。
lmfactor	为缓存只有最后修改时间戳的对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义要缓存的对象的最小大小。

disable service-settings

要在使用电话代理功能时禁用 IP 电话上的服务设置，请在电话代理配置模式下使用 **disable service-settings** 命令。要保留 IP 电话上的设置，请使用此命令的 **no** 形式。

disable service-settings

no disable service-settings

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用服务设置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

默认情况下，IP 电话上禁用以下设置：

- PC 端口
- 无为 ARP
- 语音 VLAN 访问
- Web 访问
- 跨接到 PC 端口

要保留在配置的每个 IP 电话的 CUCM 上配置的设置，请配置 **no disable service-settings** 命令。

示例

以下示例展示如何保留使用 ASA 上的电话代理功能的 IP 电话的设置：

```
ciscoasa(config-phone-proxy)# no disable service-settings
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。
show phone-proxy	显示电话代理特定信息。

display

要显示 ASA 写入 DAP 属性数据库的属性值对，请在 DAP 测试属性模式下输入 **display** 命令。

display

命令默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
DAP 测试属性	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

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。**display** 命令允许您向控制台显示这些属性。

相关命令

命令	说明
attributes	进入属性配置模式，您可以在其中设置属性值对。
dynamic-access-policy-record	创建 DAP 记录。
test dynamic-access-policy attributes	进入属性子模式。
test dynamic-access-policy execute	执行生成 DAP 的逻辑并向控制台显示因此发生的访问策略。

distance bgp

要配置 BGP 路由的管理距离，请在地址系列配置模式下使用 **distance bgp** 命令。要将管理距离恢复为默认值，请使用此命令的 **no** 形式。

distance bgp *external-distance internal-distance local-distance*

no distance bgp

语法说明

external-distance	外部 BGP 路由的管理距离。从外部自主系统获知的路由是外部路由。此参数的值的范围为从 1 到 255。
internal-distance	内部 BGP 路由的管理距离。从本地自主系统中的对等设备获知的路由是内部路由。此参数的值的范围为从 1 到 255。
local-distance	本地 BGP 路由的管理距离。本地路由是使用 **network** 路由器配置命令为正在从另一进程重分布的路由器或网络列出的网络（通常作为后门）。此参数的值的范围为从 1 到 255。

默认值

如果没有配置此命令，或输入了 no 形式，则使用以下值：

external-distance: 20
internal-distance: 200
local-distance: 200

注意　距离为 255 的路由未安装在路由表中。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

distance bgp 命令可用于配置对路由信息源（例如单个路由器或路由器组）可信度的评分。从数字上看，管理距离为 1 到 255 的正整数。

一般来说，值越大，信任评分就越低。管理距离为 255 意味着根本无法信任路由信息源，应将其忽略。如果知道另一个协议为节点提供的路由优于通过外部 BGP (eBGP) 实际获知的路由，或 BGP 应首选特定内部路由，则使用此命令。

注意事项　更改内部 BGP 路由的管理距离存在风险，不推荐这样做。配置不正确会导致路由表不一致和路由中断。

distance bgp 命令取代了 **distance mbgp** 命令

示例

在以下示例中，外部距离设置为 10，内部距离设置为 50，且本地距离设置为 100：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

要配置内部和外部 EIGRP 路由的管理距离，请在路由器配置模式下使用 **distance eigrp** 命令。要恢复默认值，请使用此命令的 **no** 形式。

distance eigrp *internal-distance external-distance*

no distance eigrp

语法说明

external-distance	EIGRP 外部路由的管理距离。外部路由是为其从自主系统外部的邻居获知最佳路径的路由。有效值为从 1 到 255。
internal-distance	EIGRP 内部路由的管理距离。内部路由是从同一自主系统中的另一个实体获知的路由。有效值为从 1 到 255。

默认值

默认值如下所示：

- *external-distance* 是 170
- *internal-distance* 是 90

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

由于各个路由协议的指标基于各不相同的算法，因此对于不同路由协议生成的到达同一目标的两个路由，并非始终可以确定 “ 最佳路径 ”。当存在两个或多个到达同一目标的不同路由（来自两个不同的路由协议）时，管理距离是 ASA 用于选择最佳路径的路由参数。

如果在 ASA 上运行多个路由协议，则您可以使用 **distance eigrp** 命令调整与其他路由协议相关的 EIGRP 路由协议发现的路由的默认管理距离。表 12-1 列出了 ASA 支持的路由协议的默认管理距离。

表 12-1　默认管理距离

路由来源	默认管理距离
已连接的接口	0
静态路由	1
EIGRP 总结路由	5
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部路由	170
未知	255

该命令的 **no** 形式不采用任何关键字或参数。使用该命令的 **no** 形式恢复内部和外部 EIGRP 路由的默认管理距离。

示例

以下示例使用 **distance eigrp** 命令将所有 EIGRP 内部路由的管理距离设置为 80，将所有 EIGRP 外部路由的管理距离设置为 115。将 EIGRP 外部路由管理距离设置为 115 会让 EIGRP 发现的到某特定目标的路由优先于 RIP（而非 OSPF）发现的同一路由。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# distance eigrp 90 115
```

相关命令

命令	说明
router eigrp	创建 EIGRP 路由进程并进入配置模式下为此过程。

distance (OSPFv3)

要定义基于路由类型的 OSPFv3 路由管理距离，请在 IPv6 路由器配置模式下使用 **distance** 命令。要恢复默认值，请使用此命令的 **no** 形式。

distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

no distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

语法说明

distance	指定管理距离。有效值范围为 10 到 254。
external	（可选）指定 OSPFv3 路由的外部类型 5 和类型 7 路由。
inter-area	（可选）指定 OSPFv3 路由的区域间路由。
intra-area	（可选）指定 OSPFv3 路由的区域内路由。
ospf	（可选）指定 OSPFv3 路由的管理距离。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令设置 OSPFv3 路由的管理距离。

示例

以下示例将 OSPFv3 的外部类型 5 和类型 7 路由的管理距离设置为 200：

```
ciscoasa(config-if)# ipv6 router ospf
ciscoasa(config-router)# distance ospf external 200
```

相关命令

命令	说明
default-information originate	将默认外部路由生成到 OSPFv3 路由域。
redistribute	将 IPv6 路由从一个路由域重分布到另一个路由域。

distance ospf (OSPFv2)

要定义基于路由类型的 OSPFv2 路由管理距离，请在路由器配置模式下使用 **distance ospf** 命令。要恢复默认值，请使用此命令的 **no** 形式。

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

语法说明

d1、*d2* 和 *d3*	指定每个路由类型的距离。有效值范围为 1 到 255。
external	（可选）设置来自通过重分布获知的其他路由域的路由的距离。
inter-area	（可选）设置从一个区域到另一个区域的所有路由的距离。
intra-area	（可选）设置一个区域内所有路由的距离。

默认值

d1、*d2* 和 *d3* 的默认值是 110。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须指定至少一个关键字和参数。您可以分别为每种类型的管理距离输入命令，但是它们在配置中显示为单个命令。如果重新输入管理距离，则仅更改该路由类型的管理距离；任何其他路由类型的管理距离仍不会受到影响。

该命令的 **no** 形式不采用任何关键字或参数。使用该命令的 **no** 形式可恢复所有路由类型的默认管理距离。如果要在配置了多个路由类型时恢复单个路由类型的默认管理距离，则您可以执行以下操作之一：

- 手动将该路由类型设置为默认值。
- 使用该命令的 **no** 形式删除整个配置，然后重新输入要保留的路由类型的配置。

示例

以下示例将外部路由的管理距离设置为 150：

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

以下示例展示分别为每个路由类型输入命令如何在路由器配置中显示为单个命令：

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

以下示例展示如何将每个管理距离设置为 105，然后仅将外部管理距离更改为 150。**show running-config router ospf** 命令展示如何仅更改外部路由类型值，而其他路由类型保留以前设置的值。

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

相关命令

命令	说明
router ospf	进入 OSPFv2 的路由器配置模式。
show running-config router	显示全局路由器配置中的 OSPFv2 命令。

distribute-list

要过滤在开放最短路径优先 (OSPF) 更新中接收或传输的网络，请在路由器配置模式下使用 **distribute-list** 命令。要更改或取消过滤，请使用此命令的 no 形式。

distribute-list *access-list name* [**in** |**out**] [**interface** *if_name*]

no distribute-list *access-list name* [**in** |**out**]

语法说明

access-list name	标准 IP 访问列表名称。列表定义在路由更新中要接收和抑制哪些网络。
in	将访问列表或路由策略应用于传入的路由更新。
out	将访问列表或路由策略应用于传出的路由更新。**out** 关键字仅在路由器配置模式下可用。
interface *if_name*	（可选）要应用路由更新的接口。指定接口会导致仅将访问列表应用于在该接口上收到的路由更新。

默认值

不过滤网络。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

如果未指定任何接口，则会将访问列表应用于所有传入的更新。

示例

以下示例过滤在外部接口上收到的 OSPF 路由更新。它接受 10.0.0.0 网络中的路由并丢弃所有其他路由。

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

相关命令

命令	说明
distribute-list in	过滤传入的路由更新。
router ospf	进入 OSPF 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

distribute-list in

要过滤传入的路由更新，请在路由器配置模式下使用 **distribute-list in** 命令。要删除过滤，请使用此命令的 **no** 形式。

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

语法说明

acl	标准访问列表的名称。
interface *if_name*	（可选）要应用传入的路由更新的接口。指定接口会导致仅将访问列表应用于在该接口上收到的路由更新。

默认值

在传入的更新中不过滤网络。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果未指定任何接口，则会将访问列表应用于所有传入的更新。

示例

以下示例过滤在外部接口上收到的 RIP 路由更新。它接受 10.0.0.0 网络中的路由并丢弃所有其他路由。

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

以下示例过滤在外部接口上收到的 EIGRP 路由更新。它接受 10.0.0.0 网络中的路由并丢弃所有其他路由。

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

相关命令

命令	说明
distribute-list out	过滤传出的路由更新。
router eigrp	进入 EIGRP 路由进程的路由器配置模式。
router rip	进入 RIP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

distribute-list in (BGP)

要过滤在传入的边界网关协议 (BGP) 更新中接收的路由或网络，请在地址系列配置模式下使用 **distribute-list in** 命令。要删除分发列表并将其从正在运行的配置文件中删除，请使用此命令的 **no** 形式。

distribute-list {*acl-name* | ***prefix*** *list-name*} **in**

no distribute-list {*acl-name* | ***prefix*** *list-name*} **in**

语法说明

acl-name	IP 访问列表名称。访问列表定义在路由更新中要接收和抑制哪些网络。
prefix *list-name*	前缀列表的名称。前缀列表根据匹配的前缀定义在路由更新中要接收和抑制哪些网络。

默认值

如果配置此命令时未使用预定义的访问列表或前缀列表，则分发列表将默认为允许所有流量。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

distribute-list in 命令用于过滤传入的 BGP 更新。必须在配置此命令前定义访问列表或前缀列表。支持标准访问列表和扩展的访问列表。IP 前缀列表用于基于前缀的位长度进行过滤。可以指定整个网络、子网、超网或单个主机路由。配置分发列表时，前缀列表和访问列表配置是互斥的。必须使用 **clear bgp** 命令重置会话，分发列表才会生效。

注

- 接口类型和编号参数可能会在 CLI 中显示，具体取决于您正在使用的思科 IOS 软件的版本。但是，任何思科 IOS 软件版本都不支持接口参数。
- 我们建议您使用 IP 前缀列表（在全局配置模式下使用 **ip prefix-list** 命令配置）而非分发列表。IP 前缀列表提供改进的性能且更易于配置。未来会将分发列表配置从 CLI 中删除。

示例

在以下示例中，定义前缀列表和分发列表以将 BGP 路由进程配置为仅接受来自网络 10.1.1.0/24、网络 192.168.1.0 和网络 10.108.0.0 的流量。发起入站路由更新以激活分发列表。

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

在以下示例中，定义访问列表和分发列表以将 BGP 路由进程配置为仅接受来自网络 192.168.1.0 和网络 10.108.0.0 的流量。发起入站路由更新以激活分发列表。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0
ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

相关命令

命令	说明
clear bgp	使用软或硬重新配置重置 BGP 连接。
ip prefix-list	创建前缀列表或添加前缀列表条目。

distribute-list out

要过滤传出的路由更新，请在路由器配置模式下使用 **distribute-list out** 命令。要删除过滤，请使用此命令的 **no** 形式。

distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

语法说明

acl	标准访问列表的名称。
connected	（可选）仅过滤连接的路由。
eigrp *as_number*	（可选）仅从指定的自主系统编号过滤 EIGRP 路由。*as_number* 参数是 ASA 上的 EIGRP 路由进程的自主系统编号。
interface *if_name*	（可选）要应用传出的路由更新的接口。指定接口会导致仅将访问列表应用于在该接口上收到的路由更新。
ospf *pid*	（可选）仅过滤指定的 OSPF 进程发现的 OSPF 路由。
rip	（可选）仅过滤 RIP 路由。
static	（可选）仅过滤静态路由。

默认值

在发送的更新中不过滤网络。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	添加了 **eigrp** 关键字。

使用指南

如果未指定任何接口，则会将访问列表应用于所有传出的更新。

示例

以下示例阻止在从任何接口发出的 RIP 更新中通告 10.0.0.0 网络：

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

以下示例阻止 EIGRP 路由进程在外部接口上通告 10.0.0.0 网络：

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

相关命令

命令	说明
distribute-list in	过滤传入的路由更新。
router eigrp	进入 EIGRP 路由进程的路由器配置模式。
router rip	进入 RIP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

distribute-list out (BGP)

要抑制在出站边界网关协议 (BGP) 更新中通告网络，请在路由器配置模式下使用 **distribute-list out** 命令。要删除分发列表并将其从正在运行的配置文件中删除，请使用此命令的 **no** 形式。

distribute-list {*acl-name* | ***prefix*** *list-name*} **out** [*protocol process-number* | ***connected*** | **static**]

no distribute-list {*acl-name* | ***prefix*** *list-name*} **out** [*protocol process-number* | ***connected*** | **static**]

语法说明

acl-name	IP 访问列表名称。访问列表定义在路由更新中要接收和抑制哪些网络。
prefix *list-name*	前缀列表的名称。前缀列表根据匹配的前缀定义在路由更新中要接收和抑制哪些网络。
protocol process-number	指定路由协议以应用分发列表。支持 BGP、EIGRP、OSPF 和 RIP。为所有路由协议输入进程编号，RIP 除外。进程编号是从 1 到 65 的值。
connected	指定通过连接的路由获知的对等设备和网络。
static	指定通过静态路由获知的对等设备和网络。

默认值

如果配置此命令时未使用预定义的访问列表或前缀列表，则分发列表将默认为允许所有流量。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

distribute-list out 命令用于过滤出站 BGP 更新。必须在配置此命令前定义访问列表或前缀列表。仅支持标准访问列表。

IP 前缀列表用于基于前缀的位长度进行过滤。可以指定整个网络、子网、超网或单个主机路由。配置分发列表时，前缀列表和访问列表配置是互斥的。必须使用 **clear bgp** 命令重置会话，分发列表才会生效。

注

- 接口类型和编号参数可能会在 CLI 中显示，具体取决于您正在使用的思科 IOS 软件的版本。但是，任何思科 IOS 软件版本都不支持接口参数。
- 我们建议您使用 IP 前缀列表（在全局配置模式下使用 **ip prefix-list** 命令配置）而非分发列表。IP 前缀列表提供改进的性能且更易于配置。未来会将分发列表配置从 CLI 中删除。

输入 *protocol* 和 / 或 *process-number* 参数会导致仅将分发列表应用于源自指定路由进程的路由。配置分发列表后，不会在传出的路由更新中通告未在分发列表命令中指定的地址。

要抑制在入站更新中接收网络或路由，请使用 **distribute-list in** 命令。

示例

在以下示例中，定义前缀列表和分发列表以将 BGP 路由进程配置为仅通告网络 192.168.0.0。发起出站路由更新以激活分发列表。

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

在以下示例中，定义访问列表和分发列表以将 BGP 路由进程配置为仅通告网络 192.168.0.0。发起出站路由更新以激活分发列表。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 0.0.255.255
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 255.255.255.255
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

相关命令

命令	说明
clear bgp	使用软或硬重新配置重置 BGP 连接。
ip prefix-list	创建前缀列表或添加前缀列表条目。

第 13 章

dns domain-lookup 至 dynamic-filter whitelist 命令

dns domain-lookup

要使 ASA 能够将 DNS 请求发送给 DNS 服务器以执行对支持的命令的名称查找，请在全局配置模式下使用 **dns domain-lookup** 命令。要禁用 DNS 请求，请使用此命令的 **no** 形式。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

语法说明

interface_name	指定配置的接口的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

该命令使 ASA 能够将 DNS 请求发送给 DNS 服务器以执行对支持的命令的名称查找。

示例

以下示例使 ASA 能够将 DNS 请求发送给 DNS 服务器以执行对内部接口的名称查找。

```
ciscoasa(config)# dns domain-lookup inside
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。

dns expire-entry-timer

要在解析的 FQDN 的 TTL 到期后删除其 IP 地址，请在全局配置模式下使用 **dns expire-entry-timer** 命令。要删除该计时器，请使用此命令的 **no** 形式。

dns expire-entry-timer minutes *minutes*

no dns expire-entry-timer minutes *minutes*

语法说明

minutes *minutes*	指定计时器时间（以分钟为单位）。有效值的范围为从 1 到 65535 分钟。

默认值

默认情况下，DNS 到期条目计时器值为 1 分钟。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

该命令指定要在解析的 FQDN 的 TTL 到期后删除其 IP 地址的时间。删除 IP 地址时，ASA 重新编译 tmatch 查找表。

仅当激活 DNS 的关联网络对象时，指定此命令才有效。

默认 DNS 到期条目计时器值为 1 分钟，这意味着在 DNS 条目的 TTL 到期后 1 分钟内删除 IP 地址。

注意　若常用 FQDN 主机（例如 www.sample.com）的解析的 TTL 是较短时间段，默认设置可能会导致频繁重新编译 tmatch 查找表。您可以指定较长的 DNS 到期条目计时器值，从而在维护安全的同时降低 tmatch 查找表的重新编译频率。

示例

以下示例在 240 分钟后删除解析的条目：

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。

dns name-server

要为 ASA 配置 DNS 服务器，请在全局配置模式下使用 **dns name-server** 命令。要删除配置，请使用此命令的 **no** 形式。

dns name-server *ipv4_addr* | *ipv6_addr*

no dns name-server *ipv4_addr* | *ipv6_addr*

语法说明

ipv4_addr	指定 DNS 服务器的 IPv4 地址。
ipv6_addr	指定 DNS 服务器的 IPv6 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。
9.0(1)	增加了对 IPv6 地址的支持。

使用指南

使用此命令可识别 ASA 的 DNS 服务器地址。ASA 支持 DNS 服务器的 IPv4 和 IPv6 地址。

示例

以下示例配置具有 IPv6 地址的 DNS 服务器：

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
ciscoasa(config)# dns retries 4
ciscoasa(config)# dns timeout 10
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。

dns poll-timer

要指定在 ASA 查询 DNS 服务器以解析在网络对象组中定义的完全限定域名 (FQDN) 期间的计时器，请在全局配置模式下使用 **dns poll-timer** 命令。要删除该计时器，请使用此命令的 **no** 形式。

dns poll-timer minutes *minutes*

no dns poll-timer minutes *minutes*

语法说明

minutes *minutes*	指定计时器（以分钟为单位）。有效值为 1 到 65535 分钟。

默认值

默认情况下，DNS 计时器为 240 分钟（即 4 小时）。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

此命令指定在 ASA 查询 DNS 服务器以解析在网络对象组中定义的 FQDN 期间的计时器。在轮询 DNS 计时器到期时或解析的 IP 条目的 TTL 到期时（以先到期者为准），定期解析 FQDN。

仅当激活至少一个网络对象组时，此命令才生效。

示例

以下示例将 DNS 轮询计时器设置为 240 分钟：

```
ciscoasa(config)# dns poll-timer minutes 240
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。

dns update

要不等待 DNS 轮询计时器到期即启动 DNS 查找以解析指定的主机名，请在特权 EXEC 模式下使用 **dns update** 命令。

dns update [**host** *fqdn_name*] [**timeout seconds** *seconds*]

语法说明

host *fqdn_name*	指定要运行 DNS 更新的主机的完全限定域名。
timeout seconds *seconds*	指定超时（以秒为单位）。

默认值

默认情况下，超时为 30 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

此命令立即启动 DNS 查找以解析指定的主机名，而不等待 DNS 轮询计时器到期。在不指定选项的情况下运行 DNS 更新时，将为 DNS 查找选择所有激活的主机组和 FQDN 主机。当命令结束运行时，ASA 在命令提示符下显示 [Done] 并生成系统日志消息。

当更新操作开始时，创建一个起始更新日志。当更新操作结束或在计时器到期后暂停时，生成另一个系统日志消息。仅允许一个未完成的 DNS 更新操作。如果重新发出命令，则出现错误消息。

示例

以下示例执行 DNS 更新：

```
ciscoasa# dns update
ciscoasa# …
ciscoasa# [Done] dns update
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。

dns-group

要指定将 DNS 服务器用于 WebVPN 隧道组，请在隧道组 WebVPN 配置模式下使用 **dns-group** 命令。要恢复默认 DNS 组，请使用此命令的 **no** 形式。

dns-group *name*

no dns-group

语法说明

name	指定用于隧道组的 DNS 服务器组配置的名称。

默认值

默认值为 DefaultDNS。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组 WebVPN 属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

该名称可以指定任何 DNS 组。**dns-group** 命令将主机名解析为适于隧道组的 DNS 服务器。

您使用 **dns server-group** 命令配置 DNS 组。

示例

以下示例展示指定使用名为 “dnsgroup1” 的 DNS 组的定制命令：

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组模式，您可以在其中配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有 DNS 服务器组配置。
tunnel-group webvpn-attributes	进入用于配置 WebVPN 隧道组属性的配置 WebVPN 模式。

dns-guard

要启用 DNS 防护功能，即对每个查询实施一次 DNS 响应，请在参数配置模式下使用 **dns-guard** 命令。要禁用此功能，请使用此命令的 **no** 形式。

dns-guard

no dns-guard

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 DNS 防护。配置 **inspect dns** 命令时可以启用此功能，即使未定义 **policy-map type inspect dns** 命令。要禁用，必须在策略映射配置中明确声明 **no dns-guard** 命令。如果未配置 **inspect dns** 命令，则行为由 **global dns-guard** 命令确定。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

DNS 报头中的标识字段用于将 DNS 响应与 DNS 报头匹配。对每个查询，允许一次响应通过 ASA。

示例

以下示例展示如何在 DNS 检查策略映射中启用 DNS 防护：

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

相关命令

命令	说明
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。

dns-server

要设置主 DNS 服务器和辅助 DNS 服务器的 IP 地址，请在组策略配置模式下使用 **dns-server** 命令。要从运行配置中删除属性，请使用此命令的 **no** 形式。

dns-server {**value** *ip_address* [*ip_address*] | **none**}

no dns-server

语法说明

none	将 **dns-server** 命令设置为空值以允许无 DNS 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 DNS 服务器的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令允许从另一个组策略继承 DNS 服务器。要阻止继承服务器，请使用 **dns-server none** 命令。

每次发出 **dns-server** 命令都会覆盖现有设置。例如，如果配置 DNS 服务器 x.x.x.x，然后配置 DNS 服务器 y.y.y.y，第二条命令将覆盖第一条，并且 y.y.y.y 成为唯一 DNS 服务器。对于多个服务器也一样。要添加 DNS 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 DNS 服务器的 IP 地址。

示例

以下示例展示如何为名为 FirstGroup 的组策略配置 IP 地址为 10.10.10.15 和 10.10.10.45 的 DNS 服务器。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dns-server value 10.10.10.15 10.10.10.45
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
show running-config dns server-group	显示当前正在运行的 DNS 服务器组配置。

dns server-group

要指定用于隧道组的 DNS 服务器的域名、名称服务器、重试次数和超时值，请在全局配置模式下使用 **dns server-group** 命令。要删除特定 DNS 服务器组，请使用此命令的 **no** 形式。

dns server -group *name*

no dns server-group

语法说明

name	指定用于隧道组的 DNS 服务器组配置的名称。

默认值

默认值为 DefaultDNS。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

该名称可以指定任何 DNS 组。您使用 **dns server-group** 命令配置 DNS 组。

示例

以下示例配置名为 “eval” 的 DNS 服务器组：

```
ciscoasa(config)# dns server-group eval
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
show running-config dns server-group	显示当前正在运行的 DNS 服务器组配置。

domain-name

要设置默认域名，请在全局配置模式下使用 **domain-name** 命令。要删除域名，请使用此命令的 **no** 形式。

domain-name *name*

no domain-name [*name*]

语法说明

name	设置域名，最多 63 个字符。

默认值

默认域名为 default.domain.invalid。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 将域名作为后缀附加到非限定名称。例如，如果您将域名设置为“example.com”并通过非限定名称“jupiter”指定系统日志服务器，则 ASA 将该名称限定为“jupiter.example.com”。对于多情景模式，您可以设置每个情景的域名，以及在系统执行空间中设置域名。

示例

以下示例将域设置为 example.com：

```
ciscoasa(config)# domain-name example.com
```

相关命令

命令	说明
dns domain-lookup	使 ASA 能够执行名称查找。
dns name-server	标识 ASA 的 DNS 服务器。
hostname	设置 ASA 主机名。
show running-config domain-name	展示域名配置。

domain-name (dns server-group)

要设置默认域名，请在 DNS 服务器组配置模式下使用 **domain-name** 命令。要删除域名，请使用此命令的 **no** 形式。

domain-name *name*

no domain-name [*name*]

语法说明

name	设置域名，最多 63 个字符。

默认值

默认域名为 default.domain.invalid。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	此命令取代了已弃用的 **dns domain-lookup** 命令。

使用指南

ASA 将域名作为后缀附加到非限定名称。例如，如果您将域名设置为“example.com”并通过非限定名称“jupiter”指定系统日志服务器，则 ASA 将该名称限定为“jupiter.example.com”。对于多情景模式，您可以设置每个情景的域名，以及在系统执行空间中设置域名。

示例

以下示例为“dnsgroup1”将域设置为“example.com”：

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

相关命令

命令	说明
clear configure dns	消除所有 DNS 命令。
dns server-group	进入 DNS 服务器组配置模式，您可以在其中配置 DNS 服务器组。
domain-name	全局设置默认域名。
show running-config dns-server group	展示一个或所有当前 DNS 服务器组配置。

downgrade

要降级您的软件版本，请在全局配置模式下使用 **downgrade** 命令。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

语法说明

activation-key *old_key*	（可选）如果需要复原激活密钥，则您可以输入旧的激活密钥。
old_config_url	指定保存的迁移之前的配置的路径（默认情况下此配置已保存在 disk0 上）。
old_image_url	指定 disk0、disk1、tftp、ftp 或 smb 上的旧映像的路径。
/noconfirm	（可选）在不给出提示的情况下降级。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

此命令可快速完成以下功能：

1. 清除引导映像配置 (**clear configure boot**)。
2. 将引导映像设置为旧映像 (**boot system**)。
3. （可选）输入新的激活密钥 (**activation-key**)。
4. 将正在运行的配置保存到启动 (**write memory**)。这会将 BOOT 环境变量设置为旧映像，因此在重新加载时会加载旧映像。
5. 将旧配置复制到启动配置 (**copy** *old_config_url* **startup-config**)。
6. 重新加载 (**reload**)。

示例

以下示例在不给出确认的情况下执行降级：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

相关命令

命令	说明
activation-key	输入激活密钥。
boot system	设置要从中引导的映像。
clear configure boot	清除引导映像配置。
copy startup-config	将配置复制到启动配置。

download-max-size

要指定允许对象下载的最大大小，请在组策略 WebVPN 配置模式下使用 **download-max-size** 命令。要从配置中删除此对象，请使用此命令的 **no** 版本。

download-max-size *size*

no download-max-size

语法说明

size	指定下载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

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
组策略 WebVPN 配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

将大小设置为 0 可有效禁止对象下载。

示例

以下示例将下载的对象的最大大小设置为 1500 字节：

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# download-max-size 1500
```

相关命令

命令	说明
post-max-size	指定要发布对象的最大大小。
upload-max-size	指定上传对象的最大大小。
webvpn	在组策略配置模式或用户名配置模式下使用。用于进入 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。

drop

要丢弃所有与 **match** 命令或 **class** 命令匹配的数据包，请在匹配或类配置模式下使用 **drop** 命令。要禁用此操作，请使用此命令的 **no** 形式。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

语法说明

log	日志匹配。系统日志消息数取决于应用。
send-protocol-error	发送协议错误消息。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
匹配和类配置	• **是**	• **是**	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

使用 模块化策略框架 时，通过在匹配或类配置模式下使用 **drop** 命令，丢弃与 **match** 命令或类映射匹配的数据包。此丢弃操作在用于应用流量的检查策略映射（**policy-map type inspect** 命令）中可用；但是，并非所有应用都允许此操作。

一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。输入 **match** 或 **class** 命令以识别应用流量（**class** 命令是指相应包括 **match** 命令的现有 **class-map type inspect** 命令）后，您可以输入 **drop** 命令以丢弃所有与 **match** 命令或 **class** 命令匹配的数据包。

如果丢弃数据包，则检查策略映射中不会执行任何进一步的操作。例如，如果第一个操作是丢弃数据包，则不会与任何进一步的 **match** 或 **class** 命令匹配。如果第一个操作是记录数据包，则会发生进一步操作，例如丢弃该数据包。您可以为同一 **match** 或 **class** 命令同时配置 **drop** 和 **log** 操作，这样在为给定匹配丢弃数据包前会记录该数据包。

在第 3/4 层策略映射中使用 **inspect** 命令启用应用检查（**policy-map** 命令）时，您可以启用包含此操作的检查策略映射，例如，当 http_policy_map 是检查策略映射的名称时输入 **inspect http http_policy_map** 命令。

示例

以下示例丢弃与 HTTP 流量类映射匹配的数据包并发送日志。如果同数据包还与匹配第二个匹配的命令，它不会处理因为它已删除。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

相关命令

命令	说明
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。
policy-map type inspect	定义特殊的应用检查操作。
show running-config policy-map	显示所有当前的策略映射配置。

drop-connection

使用 模块化策略框架 时，通过在匹配或类配置模式下使用 **drop-connection** 命令，丢弃数据包并关闭用于与 **match** 命令或类映射匹配的流量的连接。要禁用此操作，请使用此命令的 **no** 形式。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

语法说明

send-protocol-error	发送协议错误消息。
log	日志匹配。系统日志消息数量取决于应用。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
匹配和类配置	• **是**	• **是**	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

连接会从 ASA 上的连接数据库中删除。针对丢弃的连接的进入 ASA 的任何后续数据包都会被丢弃。此丢弃连接操作在用于应用流量的检查策略映射（**policy-map type inspect** 命令）中可用；但是，并非所有应用都允许此操作。一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。输入 **match** 或 **class** 命令以识别应用流量（**class** 命令是指相应包括 **match** 命令的现有 **class-map type inspect** 命令）后，您可以输入 **drop-connection** 命令以丢弃数据包并关闭用于与 **match** 命令或 **class** 命令匹配的流量的连接。

如果丢弃数据包或关闭连接，则检查策略映射中不会执行任何进一步的操作。例如，如果第一个操作是丢弃数据包并关闭连接，则不会与任何进一步的 **match** 或 **class** 命令匹配。如果第一个操作是记录数据包，则会发生进一步操作，例如丢弃该数据包。您可以为同一 **match** 或 **class** 命令同时配置 **drop-connection** 和 **log** 操作，这样在为给定匹配丢弃数据包前会记录该数据包。

在第 3/4 层策略映射中（**policy-map** 命令）使用 **inspect** 命令启用应用检查时，您可以启用包含此操作的检查策略映射。例如，输入 **inspect http http_policy_map** 命令，其中 http_policy_map 是检查策略映射的名称。

示例

以下示例丢弃与 HTTP 流量类映射匹配的数据包，关闭连接并发送日志。如果同数据包还与匹配第二个匹配的命令，它不会处理因为它已删除。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

相关命令

命令	说明
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。
policy-map type inspect	定义特殊的应用检查操作。
show running-config policy-map	显示所有当前的策略映射配置。

dtls port

要指定用于 DTLS 连接的端口，请从 WebVPN 配置模式中使用 **dtls port** 命令。要从配置中删除命令，请使用此命令的 **no** 形式：

dtls port *number*

no dtls port *number*

语法说明

number	UDP 端口号，从 1 到 65535。

默认值

默认端口号为 443。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

此命令使用 DTLS 指定要用于 SSL VPN 连接的 UDP 端口。

DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并改进对数据包延迟敏感的实时应用的性能。

示例

以下示例进入 WebVPN 配置模式并指定端口 444 用于 DTLS：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

相关命令

命令	说明
dtls enable	在接口上启用 DTLS。
svc dtls	为建立 SSL VPN 连接的组或用户启用 DTLS。
vpn-tunnel-protocol	指定 ASA 允许用于远程访问（包括 SSL）的 VPN 协议。

duplex

要设置铜缆 (RJ-45) 以太网接口的双工，请在接口配置模式下使用 **duplex** 命令。要将双工设置恢复为默认值，请使用此命令的 **no** 形式。

duplex {**auto** | **full** | **half**}

no duplex

语法说明

auto	自动检测双工模式。
full	将双工模式设置为全双工。
half	将双工模式设置为半双工。

默认值

默认值为自动检测。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	• 是

命令历史

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。

使用指南

仅在物理接口上设置双工模式。

duplex 命令不可用于光纤媒体。

如果网络不支持自动检测，则将双工模式设置为特定值。

对于 ASA 5500 系列上的 RJ-45 接口，默认自动协商设置还包括自动 MDI/MDIX 功能。在自动协商阶段检测到直通电缆时，自动 MDI/MDIX 通过执行内部交叉消除对交叉电缆的需求。必须将速度或双工设置为自动协商以对接口启用自动 MDI/MDIX。如果同时将速度和双工明确设置为固定值，然后禁用这两种设置的自动协商，则也会禁用自动 MDI/MDIX。

如果将双工设置为 PoE 端口上除 **auto** 外的任何值，则不会检测不支持 IEEE 802.3af 的思科 IP 电话和思科无线接入点（如果有），且不会为它们提供电源。

示例

以下示例将双工模式设置为全双工：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

相关命令

命令	说明
clear configure interface	清除接口的所有配置。
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。
show running-config interface	显示接口配置。
speed	设置接口速度。

dynamic-access-policy-config

要配置 DAP 记录和与之关联的访问策略属性，请在全局配置模式下使用 **dynamic-access-policy-config** 命令。要删除现有 DAP 配置，请使用此命令的 **no** 形式。

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

语法说明

activate	激活 DAP 选择配置文件。
name	指定 DAP 记录的名称。名称的长度最多可以为 64 个字符，且不能包含空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
全局配置（名称）	• **是**	• **是**	• **是**	• 是	—
特权 EXEC（激活）	• **是**	• **是**	• **是**	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

在全局配置模式下使用 **dynamic-access-policy-config** 命令可创建一个或多个 DAP 记录。要激活 DAP 选择配置文件，请使用带有 *activate* 参数的 **dynamic-access-policy-config** 命令。

使用此命令时，您进入动态访问策略记录模式，您可以在其中设置指定的 DAP 记录的属性。您可以在动态访问策略记录模式下使用以下命令：

- **action**
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

示例

以下示例展示如何配置名为 user1 的 DAP 记录：

```
ciscoasa(config)# dynamic-access-policy-config user1
ciscoasa(config-dynamic-access-policy-record)#
```

相关命令

命令	说明
dynamic-access-policy-record	使用访问策略属性填充 DAP 记录。
show running-config dynamic-access-policy-record	显示所有 DAP 记录或指定 DAP 记录正在运行的配置。

dynamic-access-policy-record

要创建 DAP 记录并为其填充访问策略属性，请在全局配置模式下使用 **dynamic-access-policy-record** 命令。要删除现有 DAP 记录，请使用此命令的 **no** 形式。

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

语法说明

name	指定 DAP 记录的名称。名称的长度最多可以为 64 个字符，且不能包含空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在全局配置模式下使用 **dynamic-access-policy-record** 命令可创建一个或多个 DAP 记录。使用此命令时，您进入动态访问策略记录模式，您可以在其中设置指定的 DAP 记录的属性。您可以在动态访问策略记录模式下使用以下命令：

- **action**（**continue**、**terminate** 或 **quarantine**）
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

示例

以下示例展示如何创建名为 Finance 的 DAP 记录。

```
ciscoasa(config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)#
```

相关命令

命令	说明
clear config dynamic-access-policy-record	删除所有 DAP 记录或指定的 DAP 记录。
dynamic-access-policy-config url	配置 DAP 选择配置文件。
show running-config dynamic-access-policy-record	显示所有 DAP 记录或指定 DAP 记录正在运行的配置。

dynamic-authorization

要为 AAA 服务器组启用 RADIUS 动态授权（授权更改）服务，请在 AAA 服务器主机配置模式下使用 **dynamic-authorization** 命令。要禁用动态授权，请使用此命令的 **no** 形式。

dynamic-authorization port *number*

no dynamic-authorization port *number*

语法说明

port *port_number*	（可选）指定 ASA 上的动态授权端口。范围为 1 至 65535。

默认值

默认 RADIUS 端口为 1645。默认情况下未启用动态授权。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

定义后，注册相应的 RADIUS 服务器组以用于 CoA 通知，且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口。

以下示例展示如何通过单个服务器添加一个 RADIUS 组：

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

以下示例展示如何为仅授权、动态授权 (CoA) 更新和每小时定期记账配置 ISE 服务器对象：

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
```

以下示例展示如何使用 ISE 为密码身份验证配置隧道组：

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

以下示例展示如何使用 ISE 为本地证书验证和授权配置隧道组：

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

相关命令

命令	说明
authorize-only	为 RADIUS 服务器组启用仅授权模式。
interim-accounting-update	启用 RADIUS 临时记账更新消息的生成。
without-csd	关闭对为特定隧道组建立的连接的 hostscan 处理。

dynamic-filter ambiguous-is-black

要将列入僵尸网络流量过滤器灰名单的流量视为要丢弃的黑名单流量，请在全局配置模式下使用 **dynamic-filter ambiguous-is-black** 命令。要允许灰名单流量，请使用此命令的 **no** 形式。

dynamic-filter ambiguous-is-black

no dynamic-filter ambiguous-is-black

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

如果先后配置了 **dynamic-filter enable** 命令和 **dynamic-filter drop blacklist** 命令，则此命令将灰名单流量视为要丢弃的黑名单流量。如果不启用此命令，则不会丢弃灰名单流量。

不明确的地址与多个域名关联，但并非所有这些域名都在黑名单上。这些地址在灰名单上。

示例

以下示例监控外部接口上的所有端口 80 流量，然后丢弃位于常规或更高威胁级别的黑名单和灰名单流量：

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。

命令	说明
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter blacklist

要编辑僵尸网络流量过滤器黑名单，请在全局配置模式下使用 **dynamic-filter blacklist** 命令。要删除黑名单，请使用此命令的 **no** 形式。

dynamic-filter blacklist

no dynamic-filter blacklist

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

进入动态过滤器黑名单配置模式后，您可以使用 **address** 和 **name** 命令，手动输入要在黑名单中标记为坏名称的域名或 IP 地址（主机或子网）。您还可以在白名单中输入名称或 IP 地址（请参阅 **dynamic-filter whitelist** 命令），以便仅将同时出现在动态黑名单和白名单上的名称或地址识别为系统日志消息和报告中的白名单地址。请注意在系统日志消息中查看白名单地址，即使该地址也不在动态黑名单中。

始终使用非常高的威胁级别指定静态黑名单条目。

将域名添加到静态数据库后，ASA 会等待 1 分钟，然后发送该域名的 DNS 请求并将域名 /IP 地址配对添加到 *DNS 主机缓存*。（此操作是后台进程，不会影响继续配置 ASA 的能力。） 我们建议也使用僵尸网络流量过滤器监听启用 DNS 数据包检查（请参阅 **inspect dns dynamic-filter-snooping** 命令）。ASA 使用僵尸网络流量过滤器监听而非常规 DNS 查找，以在下列情况下解析静态黑名单域名：

- ASA DNS 服务器不可用。
- 在 ASA 发送常规 DNS 请求前的 1 分钟等待时间内发起连接。

如果使用 DNS 监听，则当受感染的主机发送 DNS 请求以获取静态数据库上的某个名称时，ASA 在 DNS 数据包中查找域名和关联的 IP 地址，并将该名称和 IP 地址添加到 DNS 反向查找缓存。

静态数据库允许您使用要列入黑名单的域名或 IP 地址来增强动态数据库。

如果不启用僵尸网络流量过滤器监听，且出现上述情况之一，则僵尸网络流量过滤器不会监控该流量。

注意　此命令需要 ASA 使用 DNS 服务器；请参阅 **dns domain-lookup** 和 **dns server-group** 命令。

示例

以下示例创建黑名单和白名单的条目：

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。

命令	说明
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter database fetch

要为僵尸网络流量过滤器测试动态数据库的下载，请在特权 EXEC 模式下使用 **dynamic-filter database fetch** 命令。

dynamic-filter database fetch

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

实际数据库不存储在 ASA 上；它会被下载并丢弃。此命令仅用于测试目的。

示例

以下示例测试动态数据库的下载：

```
ciscoasa# dynamic-filter database fetch
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。

命令	说明
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter database find

要检查域名或 IP 地址是否已包括在僵尸网络流量过滤器的动态数据库中，请在特权 EXEC 模式下使用 **dynamic-filter database find** 命令。

dynamic-filter database find *string*

语法说明

string	*string* 可以是完整的域名或 IP 地址，或您可以输入名称或地址的一部分，其中搜索字符串最小为 3 个字符。数据库搜索不支持正则表达式。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

如果存在多个匹配项，则显示前两个匹配项。要优化搜索以获取更具体的匹配项，请输入更长的字符串。

示例

以下示例对字符串 “example.com” 进行搜索，并找到一个匹配项：

```
ciscoasa# dynamic-filter database find bad.example.com

   bad.example.com
Found 1 matches
```

以下示例对字符串 “bad” 进行搜索，并找到两个以上的匹配项：

```
ciscoasa# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

相关命令

命令	说明
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter database purge

要从正在运行的内存中手动删除僵尸网络流量过滤器动态数据库，请在特权 EXEC 模式下使用 **dynamic-filter database purge** 命令。

dynamic-filter database purge

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

数据库文件存储在正在运行的内存中；它们不存储在闪存中。如果需要删除数据库，请使用 **dynamic-filter database purge** 命令。

在清除数据库文件前，请使用 **no dynamic-filter use-database** 命令禁用数据库的使用。

示例

以下示例先禁用数据库的使用，然后清除数据库：

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。

命令	说明
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter drop blacklist

要使用僵尸网络流量过滤器自动丢弃黑名单流量，请在全局配置模式下使用 **dynamic-filter drop blacklist** 命令。要禁用自动丢弃，请使用此命令的 **no** 形式。

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

no dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

语法说明

action-classify-list *sub_access_list*	（可选）识别要丢弃的流量的子集。请参阅 **access-list extended** 命令，创建访问列表。 丢弃的流量必须始终等于 **dynamic-filter enable** 命令识别的监控流量，或是该流量的子集。例如，如果指定 **dynamic-filter enable** 命令的访问列表，且为此命令指定 **action-classify-list**，则该访问列表必须是 **dynamic-filter enable** 访问列表的子集。
interface *name*	（可选）将监控范围限制到特定接口。丢弃的流量必须始终等于 **dynamic-filter enable** 命令识别的监控流量，或是该流量的子集。 任何特定于接口的命令优先于全局命令。
threat-level {***eq*** *level* | ***range*** *min max*}	（可选）通过设置威胁级别限制丢弃的流量。如果未明确设置威胁级别，则使用的级别为 **threat-level range moderate very-high**。 **注**　我们强烈建议使用默认设置，除非您有更改此设置的充分理由。 *level*、*min* 和 *max* 选项是： • **very-low** • **low** • **moderate** • **high** • **very-high** **注**　始终使用非常高的威胁级别指定静态黑名单条目。

默认值

此命令默认禁用。

默认威胁级别为 **threat-level range moderate very-high**。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

请确保首先为要丢弃的任何流量配置 **dynamic-filter enable** 命令；丢弃的流量必须始终等于监控的流量或是其子集。

您可以为每个接口和全局策略多次输入此命令。请确保您未在用于给定接口 / 全局策略的多个命令中指定重叠的流量。由于您无法控制匹配命令的确切顺序，重叠的流量意味着您不知道该匹配哪个命令。例如，请勿同时指定与所有流量匹配的命令（不带有 **action-classify-list** 关键字）和用于给定接口的带有 **action-classify-list** 关键字的命令。在这种情况下，流量可能不会与带有 **action-classify-list** 关键字的命令匹配。同样，如果指定多个带有 **action-classify-list** 关键字的命令，请确保每个访问列表是唯一的且网络不重叠。

示例

以下示例监控外部接口上的所有端口 80 流量，然后丢弃位于常规或更高威胁级别的流量：

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。

命令	说明
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter enable

要启用僵尸网络流量过滤器，请在全局配置模式下使用 **dynamic-filter enable** 命令。要禁用僵尸网络流量过滤器，请使用此命令的 **no** 形式。

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

no dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

语法说明

classify-list *access_list*	识别要使用扩展的访问列表监控的流量（请参阅 **access-list extended** 命令）。如果不创建访问列表，则默认情况下监控所有流量。
interface *name*	将监控范围限制到特定接口。

默认值

默认情况下禁用僵尸网络流量过滤器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

僵尸网络流量过滤器将每个初始连接数据包中的源和目标 IP 地址与动态数据库、静态数据库、DNS 反向查找缓存和 DNS 主机缓存中的 IP 地址进行比较，并发送系统日志消息或丢弃任何匹配的流量。

恶意软件是安装在未知主机上的出于恶意而开发的软件。当恶意软件启动与已知错误 IP 地址的连接时，僵尸网络流量过滤器可以检测到尝试进行网络活动（例如发送密码、信用卡号、键击或专有数据等私人数据）的恶意软件。僵尸网络流量过滤器检查动态数据库的传入和传出连接以查找已知错误的域名和 IP 地址，然后记录任何可疑活动。您也可以通过在本地 “blacklist” 或 “whitelist” 中输入 IP 地址或域名，来使用静态数据库补充动态数据库。

单独启用 DNS 监听（请参阅 **inspect dns dynamic-filter-snoop** 命令）。通常，为最大限度使用僵尸网络流量过滤器，您需要启用 DNS 监听，但您可以独立使用僵尸网络流量过滤器日志记录（如果需要）。在不具有用于动态数据库的 DNS 监听时，僵尸网络流量过滤器仅在动态数据库中使用静态数据库条目以及任何 IP 地址；不在动态数据库中使用域名。

僵尸网络流量过滤器地址类别

僵尸网络流量过滤器监控的地址包括：

- 已知恶意软件地址 - 这些地址在 “blacklist” 上。
- 已知允许的地址 - 这些地址在 “whitelist” 上。

- 不明确的地址 - 这些地址与多个域名关联，但并非所有这些域名都在黑名单上。这些地址在“greylist” 上。
- 未列出的地址 - 这些地址是未知的且不包括在任何列表上。

用于已知地址的僵尸网络流量过滤器操作

您可以使用 **dynamic-filter enable** 命令配置僵尸网络流量过滤器以记录可疑活动，也可以选择性地使用 **dynamic-filter drop blacklist** 命令将其配置为自动拦截可疑流量。

未列出的地址不生成任何系统日志消息，但黑名单、白名单和灰名单上的地址生成按类型区分的系统日志消息。僵尸网络流量过滤器生成编号为 338*nnn* 的详细系统日志消息。消息会按照传入和传出连接、黑名单、白名单或灰名单地址和许多其他变量等进行区分。（灰名单包括与多个域名关联的地址，但并非所有这些域名都在黑名单上。）

请参阅 系统日志消息指南，了解有关系统日志消息的详细信息。

示例

以下示例监控外部接口上的所有端口 80 流量，然后丢弃位于常规或更高威胁级别的流量：

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。

命令	说明
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter updater-client enable

要启用为僵尸网络流量过滤器从思科更新服务器下载动态数据库，请在全局配置模式下使用 **dynamic-filter updater-client enable** 命令。要禁用下载动态数据库，请使用此命令的 **no** 形式。

dynamic-filter updater-client enable

no dynamic-filter updater-client enable

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用下载。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

如果 ASA 上未安装数据库，则它在约 2 分钟后下载数据库。更新服务器确定 ASA 轮询服务器用于未来更新的频率，通常是每小时轮询一次。

僵尸网络流量过滤器可以从思科更新服务器收到动态数据库的定期更新。

此数据库列出数千个已知错误的域名和 IP 地址。当 DNS 应答中的域名与动态数据库中的名称匹配时，僵尸网络流量过滤器将名称和 IP 地址添加到 *DNS reverse lookup cache*。当受感染的主机启动到恶意软件站点的 IP 地址的连接时，ASA 发送系统日志消息，通知您存在可疑活动。

要使用数据库，请确保为 ASA 配置域名服务器，以便它可以访问 URL。要在动态数据库中使用域名，您需要使用僵尸网络流量过滤器监听启用 DNS 数据包检查； ASA 在 DNS 数据包中查找域名和关联的 IP 地址。

在某些情况下，动态数据库提供了 IP 地址本身，且僵尸网络流量过滤器将任何流量记录到该 IP 地址，而无需检查 DNS 请求。

数据库文件存储在正在运行的内存中；它们不存储在闪存中。如果需要删除数据库，请使用 **dynamic-filter database purge** 命令。

注意　此命令需要 ASA 使用 DNS 服务器；请参阅 **dns domain-lookup** 和 **dns server-group** 命令。

示例

以下多模式示例启用动态数据库的下载，并启用在 context1 和 context2 中使用该数据库：

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

以下单模式示例启用动态数据库的下载，并启用该数据库的使用：

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns name-server	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter use-database	允许使用动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。

命令	说明
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter use-database

要启用将动态数据库用于僵尸网络流量过滤器，请在全局配置模式下使用 **dynamic-filter use-database** 命令。要禁用动态数据库的使用，请使用此命令的 **no** 形式。

dynamic-filter use-database

no dynamic-filter use-database

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下禁用数据库的使用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

在多情景模式下可能需要禁止使用下载的数据库，这样您就可以为每个情景配置数据库的使用。要启用动态数据库的下载，请参阅 **dynamic-filter updater-client enable** 命令。

示例

以下多模式示例启用动态数据库的下载，并启用在 context1 和 context2 中使用该数据库：

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

以下单模式示例启用动态数据库的下载，并启用该数据库的使用：

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter whitelist	编辑僵尸网络流量过滤器白名单。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

dynamic-filter whitelist

要编辑僵尸网络流量过滤器白名单，请在全局配置模式下使用 **dynamic-filter whitelist** 命令。要删除白名单，请使用此命令的 **no** 形式。

dynamic-filter whitelist

no dynamic-filter whitelist

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

静态数据库允许您使用要列入白名单的域名或 IP 地址来增强动态数据库。进入动态过滤器白名单配置模式后，您可以使用 **address** 和 **name** 命令，手动输入要在白名单中标记为好名称的域名或 IP 地址（主机或子网）。仅将同时出现在动态黑名单和静态白名单上的名称或地址识别为系统日志消息和报告中的白名单地址。请注意在系统日志消息中查看白名单地址，即使该地址也不在动态黑名单中。您可以使用 **dynamic-filter blacklist** 命令在静态黑名单中输入名称或 IP 地址。

将域名添加到静态数据库后，ASA 会等待 1 分钟，然后发送该域名的 DNS 请求并将域名 /IP 地址配对添加到 *DNS 主机缓存*。（此操作是后台进程，不会影响继续配置 ASA 的能力。） 我们建议也使用僵尸网络流量过滤器监听启用 DNS 数据包检查（请参阅 **inspect dns dynamic-filter-snooping** 命令）。ASA 使用僵尸网络流量过滤器监听而非常规 DNS 查找，以在下列情况下解析静态黑名单域名：

- ASA DNS 服务器不可用。
- 在 ASA 发送常规 DNS 请求前的 1 分钟等待时间内发起连接。

如果使用 DNS 监听，则当受感染的主机发送 DNS 请求以获取静态数据库上的某个名称时，ASA 在 DNS 数据包中查找域名和关联的 IP 地址，并将该名称和 IP 地址添加到 DNS 反向查找缓存。

如果不启用僵尸网络流量过滤器监听，且出现上述情况之一，则僵尸网络流量过滤器不会监控该流量。

注意　此命令需要 ASA 使用 DNS 服务器；请参阅 **dns domain-lookup** 和 **dns server-group** 命令。

示例

以下示例创建黑名单和白名单的条目：

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

相关命令

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
clear dynamic-filter dns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
clear dynamic-filter reports	清除僵尸网络流量过滤器报告数据。
clear dynamic-filter statistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	启用 ASA 将 DNS 请求发送到 DNS 服务器以执行所支持命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filter ambiguous-is-black	将灰名单流量视为要操作的黑名单流量。
dynamic-filter blacklist	编辑僵尸网络流量过滤器黑名单。
dynamic-filter database fetch	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filter database find	搜索动态数据库来查找某域名或 IP 地址。
dynamic-filter database purge	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filter drop blacklist	自动丢弃黑名单流量。
dynamic-filter enable	对某类流量或所有流量（如果没有指定访问列表）启用僵尸网络流量过滤器。
dynamic-filter updater-client enable	允许下载动态数据库。
dynamic-filter use-database	允许使用动态数据库。
inspect dns dynamic-filter-snoop	启用具有僵尸网络流量过滤器监听的 DNS 检查。
name	将名称添加到白名单或黑名单。
show asp table dynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
show dynamic-filter data	显示关于动态数据库的信息，包括动态数据库上次下载时间、数据库版本、数据库包含多少条目以及 10 个示例条目。
show dynamic-filter dns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要；或通过 **detail** 关键字显示实际 IP 地址和名称。
show dynamic-filter reports	生成前 10 个僵尸网络站点、端口和受感染主机的报告。
show dynamic-filter statistics	显示有多少连接通过僵尸网络流量过滤器进行监测；以及其中有多少连接匹配白名单、黑名单和灰名单。

命令	说明
show dynamic-filter updater-client	显示关于更新程序服务器的信息，包括服务器 IP 地址、下次 ASA 与服务器连接的时间以及上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器正在运行的配置。

第 4 部分

E 至 H 命令

第 14 章

eigrp log-neighbor-changes 至 export webvpn webcontent 命令

eigrp log-neighbor-changes

要启用记录 EIGRP 相邻关系更改，请在路由器配置模式下使用 **eigrp log-neighbor-changes** 命令。要关闭此功能，请使用此命令的 **no** 形式。

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

默认情况下启用 **eigrp log-neighbor-changes** 命令；运行配置中仅显示此命令的 **no** 形式。

示例

以下示例禁用 EIGRP 邻居更改记录：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

相关命令

命令	说明
eigrp log-neighbor-warnings	启用邻居警告消息记录。
router eigrp	进入 EIGRP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

eigrp log-neighbor-warnings

要启用 EIGRP 邻居警告消息记录，请在路由器配置模式下使用 **eigrp log-neighbor-warnings** 命令。要关闭此功能，请使用此命令的 **no** 形式。

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

语法说明

seconds	（可选）重复的邻居警告消息之间的时间间隔（以秒为单位）。有效值为从 1 到 65535。不会记录在此间隔期间重复出现的警告。

默认值

此命令默认已启用。将记录所有邻居警告消息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

默认情况下启用 **eigrp log-neighbor-warnings** 命令；运行配置中仅显示此命令的 **no** 形式。

示例

以下示例禁用 EIGRP 邻居警告消息记录：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

以下示例记录 EIGRP 邻居警告消息，并以 5 分钟（300 秒）为间隔重复显示警告消息：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

相关命令

命令	说明
eigrp log-neighbor-messages	启用 EIGRP 相邻关系更改记录。
router eigrp	进入 EIGRP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

eigrp router-id

要指定 EIGRP 路由进程使用的路由器 ID，请在路由器配置模式下使用 **eigrp router-id** 命令。要恢复默认值，请使用此命令的 **no** 形式。

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

语法说明

ip-addr	IP 地址（点分十进制）格式中的路由器 ID。不能将 0.0.0.0 或 255.255.255.255 用作路由器 ID。

默认值

如果未指定的最高级别的 IP 地址上的 ASA 用作路由器 ID。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

如果未配置 **eigrp router-id** 命令，在 EIGRP 进程启动后，EIGRP 会自动选择 ASA 上的最高位 IP 地址作为路由器 ID。路由器 ID 不会改变，除非使用 **no router eigrp** 命令删除 EIGRP 进程，或者使用 **eigrp router-id** 命令手动配置路由器 ID。

路由器 ID 用于标识外部路由的始发路由器。如果使用本地路由器 ID 接收外部路由，接收到的路由将被丢弃。为避免这种情况，请使用 **eigrp router-id** 命令为路由器 ID 指定一个全局地址。

应该为每个 EIGRP 路由器配置唯一的值。

示例

以下示例将 172.16.1.3 配置为 EIGRP 路由进程的固定路由器 ID：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

相关命令

命令	说明
router eigrp	进入 EIGRP 路由进程的路由器配置模式。
show running-config router	在全局路由器配置中显示的命令。

eigrp stub

要将 EIGRP 路由进程配置为末节路由进程，请在路由器配置模式下使用 **eigrp stub** 命令。要删除 EIGRP 末节路由，请使用此命令的 **no** 形式。

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

语法说明

connected	（可选）通告连接的路由。
receive-only	（可选）将 ASA 设置为接收专用邻居。
redistributed	（可选）从其他路由协议通告重分布的路由。
static	（可选）通告静态路由。
summary	（可选）通告摘要路由。

默认值

末节路由未启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

使用 **eigrp stub** 命令可以将 ASA 配置为末节，以使 ASA 将所有 IP 流量发送到分布路由器。

使用 **receive-only** 关键字可以禁止 ASA 与自主系统中的任何其他路由器共享其任何路由； ASA 只会从 EIGRP 邻居接收更新。**receive-only** 关键字不能与任何其他关键字结合使用。

可以指定 **connected**、**static**、**summary** 和 **redistributed** 关键字当中的一个或多个。如果将这些关键字当中的任何一个与 **eigrp stub** 命令结合使用，则只会发送特定关键字指定的路由类型。

connected 关键字允许 EIGRP 末节路由进程发送连接的路由。如果连接的路由不包含在任何 **network** 语句中，可能需要在 EIGRP 进程中使用 **redistribute** 命令重分布连接的路由。

static 关键字允许 EIGRP 末节路由进程发送静态路由。如果不配置此选项，EIGRP 不会发送任何静态路由（包括通常会自动重分布的内部静态路由）。在这种情况下，仍必须使用 **redistribute static** 命令重分布静态路由。

summary 关键字允许 EIGRP 末节路由进程发送摘要路由。可以使用 **summary-address eigrp** 命令手动创建摘要路由，或者通过启用 **auto-summary** 命令自动创建摘要路由（默认情况下启用此命令）。

redistributed 关键字允许 EIGRP 末节路由进程从其他路由协议将重分布的路由发送到 EIGRP 路由进程。如果不配置此选项，EIGRP 不会通告重分布的路由。

示例

以下示例使用 **eigrp stub** 命令将 ASA 配置为会通告连接的路由和摘要路由的 EIGRP 末节：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

以下示例使用 **eigrp stub** 命令将 ASA 配置为会通告连接的路由和静态路由的 EIGRP 末节。不允许发送摘要路由。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

以下示例使用 **eigrp stub** 命令将 ASA 配置为仅接收 EIGRP 更新的 EIGRP 末节。不会发送有关连接的路由、摘要路由和静态路由的信息。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp
ciscoasa(config-router)# eigrp stub receive-only
```

以下示例使用 **eigrp stub** 命令将 ASA 配置为会从其他路由协议通告重分布到 EIGRP 路由的 EIGRP 末节。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

以下示例使用不带任何可选参数的 **eigrp stub** 命令。当 **eigrp stub** 命令不带参数时，默认情况下会通告连接的路由和静态路由。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

相关命令

命令	说明
router eigrp	将清除运行配置中的 EIGRP 路由器配置模式命令。
show running-config router eigrp	显示运行配置中的 EIGRP 路由器配置模式命令。

eject

要支持移除 ASA 外部紧凑型闪存设备，请在用户 EXEC 模式下使用 **eject** 命令。

eject [**/noconfirm**] *disk1:*

语法说明

disk1:	指定要弹出的设备。
/noconfirm	指定在从 ASA 实际移除外部闪存设备之前不需要确认设备移除。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **eject** 命令可以从 ASA 5500 系列安全移除紧凑型闪存设备。

以下示例展示如何在从 ASA 实际移除 *disk1* 之前使用 **eject** 命令正常关闭该设备：

```
ciscoasa# eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

相关命令

命令	说明
show version	显示有关操作系统软件的信息。

email

要在注册过程中将指示的邮件地址包含在使用者备用名称扩展名中，请在 crypto ca-trustpoint 配置模式下使用 **email** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

email *address*

no email

语法说明

address	指定邮件地址。最大长度是 64 个字符。

默认值

未设置默认设置。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并将邮件地址 user1@user.net 包含在中心信任点的注册请求中：

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca-trustpoint	进入 crypto ca-trustpoint 配置模式。

enable

要进入特权 EXEC 模式，请在用户 EXEC 模式下使用 **enable** 命令。

enable [*level*]

语法说明

level	（可选）权限级别（0 到 15）。不与 “ 启用身份验证 ” 功能（**aaa authentication enable console** 命令）结合使用。

默认值

输入权限级别 15，除非要使用 “ 启用身份验证 ” 功能（使用 **aaa authentication enable console** 命令）；在后一种情况下，默认级别取决于为用户名配置的级别。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

默认启用密码为空。请参阅 **enable password** 命令设置密码。

如果不使用 “ 启用身份验证 ” 功能，当输入 **enable** 命令时，用户名将更改为 enable_*level*，其中的默认级别为 15。如果使用 “ 启用身份验证 ” 功能（使用 **aaa authentication enable console** 命令），将保留用户名及关联的级别。保留用户名对于命令授权很重要（**aaa authorization command** 命令，使用本地或 TACACS+ 命令授权）。

使用级别 2 或更高级别将进入特权 EXEC 模式。使用级别 0 和 1 将进入用户 EXEC 模式。要使用中间级别，请启用本地命令授权（**aaa authorization command LOCAL** 命令），然后使用 **privilege** 命令将命令设置为其他权限级别。TACACS+ 命令授权不使用在 ASA 上配置的权限级别。

要查看当前权限级别，请参阅 **show curpriv** 命令。

输入 **disable** 命令会退出特权 EXEC 模式。

示例

以下示例进入特权 EXEC 模式：

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

以下示例进入级别 10 的特权 EXEC 模式：

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

相关命令

命令	说明
enable password	设置启用密码。
disable	退出特权 EXEC 模式。
aaa authorization command	配置命令授权。
privilege	设置本地命令授权的命令权限级别。
show curpriv	显示当前登录的用户名和用户特权级别。

enable (webvpn, e-mail proxy, config-mdm-proxy)

要在之前配置的接口上启用 WebVPN、MDM 代理或邮件代理访问，请使用 **enable** 命令。对于 WebVPN，请在 webvpn 配置模式下使用此命令。对于邮件代理（IMAP4S、 POP3S 和 SMTPS），请在适用的邮件代理配置模式下使用此命令。对于 MDM 代理，请在 config-mdm-proxy 模式下使用此命令。要在接口上禁用 WebVPN，请使用此命令的 **no** 形式。

enable *ifname*

no enable

语法说明

ifname	标识之前配置的接口。使用 **nameif** 命令可配置接口。

默认值

默认情况下禁用 WebVPN。默认情况下禁用 MDM 代理。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Imap4s 配置	• 是	—	• 是	—	—
Pop3s 配置	• 是	—	• 是	—	—
SMTPS 配置	• 是	—	• 是	—	—
WebVPN 配置	• 是	—	• 是	—	—
config-mdm-proxy 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(1)	此命令现已在 config-mdm-proxy 模式中可用。

示例

以下示例展示如何在名为 Outside 的接口上启用 WebVPN：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable Outside
```

以下示例展示如何在名为 Outside 的接口上配置 POP3S 邮件代理：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# enable Outside
```

以下示例展示如何在名为 Outside 的接口上配置 MDM 代理：

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# enable Outside
```

enable（集群组）

要启用集群，请在集群组配置模式下使用 **enable** 命令。要禁用集群，请使用此命令的 **no** 形式。

enable [**as-slave** | **noconfirm**]

no enable

语法说明

as-slave	（可选）启用集群而不检查不兼容命令的运行配置，并确保从设备会加入到集群但不会在任何当前选定中成为主设备。从设备的配置将被同步自主设备的配置覆盖。
noconfirm	（可选）如果输入 **enable** 命令，ASA 会扫描不兼容命令的运行配置，以确定集群不支持的功能（包括默认配置中可能存在的命令）。系统会提示您删除不兼容命令。如果您选择 **No**，将不会启用集群。使用 **noconfirm** 关键字可绕过确认步骤并自动删除不兼容命令。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

对于启用的第一台设备，将进行主设备选定。由于启用的第一台设备到目前为止应该是集群的唯一成员，因此，该设备将成为主设备。请勿在此期间更改任何配置。

如果已经有主设备，并打算向集群添加从设备，可以通过使用 **enable as-slave** 命令来避免任何配置不兼容情况（主要是集群存在未配置的接口这种情况）。

要禁用集群，请输入 **no enable** 命令。

注　如果禁用集群，所有数据接口将关闭，只有管理接口会处于活动状态。如果要从集群完全删除设备（以使有数据接口处于活动状态），需要删除整个集群组配置。

示例

以下示例启用集群并删除不兼容的配置：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
```

```
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands?[Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接再平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位数。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

enable gprs

要启用具有 RADIUS 计费功能的 GPRS，请在 radius-accounting 参数配置模式下使用 **enable gprs** 命令。要禁用此命令，请使用此命令的 **no** 形式。

enable gprs

no enable gprs

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Radius-accounting 参数配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

可使用 **inspect radius-accounting** 命令来访问此命令。ASA 在 Accounting-Request Stop 消息中检查 3GPP VSA 26-10415，以便正确处理辅助 PDP 情景。默认情况下该选项处于禁用状态。启用此功能需要有 GTP 许可证。

示例

以下示例展示如何启用具有 RADIUS 计费功能的 GPRS：

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

相关命令

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

enable password

要设置特权 EXEC 模式的启用密码，请在全局配置模式下使用 **enable password** 命令。要删除级别的密码（级别 15 除外），请使用此命令的 **no** 形式。

enable password *password* [**level** *level*] [**encrypted**]

no enable password level *level*

语法说明

encrypted	（可选）指定密码采用加密形式。密码以加密形式保存在配置中，因此您在输入原始密码后无法查看原始密码。如果出于某种原因需要将密码复制到另一个 ASA，但却不知道原始密码，则您可以输入带有加密密码和此关键字的 **enable password** 命令。一般情况下，仅当输入 **show running-config enable** 命令时才会看到此关键字。
level *level*	（可选）为权限级别（0 到 15）设置密码。
password	将密码设置为包含 3 到 32 个字母数字字符和特殊字符的区分大小写的字符串。可以在密码中使用除问号和空格以外的任何字符。

默认值

默认密码为空。默认级别为 15。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

启用级别 15（默认级别）的默认密码为空。要将密码重置为空，请不要为 *password* 参数输入任何文本。不能删除级别 15 的密码。

对于多情景模式，可以为系统配置和每个情景创建启用密码。

要使用默认级别（级别 15）以外的权限级别，请配置本地命令授权（参阅 **aaa authorization command** 命令并指定 **LOCAL** 关键字），然后使用 **privilege** 命令将命令设置为其他权限级别。如果不配置本地命令授权，将忽略启用级别，而且无论设置的级别是什么，都只能访问级别 15。要查看当前权限级别，请参阅 **show curpriv** 命令。

使用级别 2 或更高级别将进入特权 EXEC 模式。使用级别 0 和 1 将进入用户 EXEC 模式。

示例

以下示例将启用密码设置为 Pa$$w0rd：

```
ciscoasa(config)# enable password Pa$$w0rd
```

以下示例将级别 10 的启用密码设置为 Pa$$w0rd10：

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

以下示例将启用密码设置为从另一个 ASA 复制的加密密码：

```
ciscoasa(config)# enable password jMorNbK0514fadBh encrypted
```

相关命令

命令	说明
aaa authorization command	配置命令授权。
enable	进入特权 EXEC 模式。
privilege	设置本地命令授权的命令权限级别。
show curpriv	显示当前登录的用户名和用户特权级别。
show running-config enable	以加密形式显示启用密码。

encryption

要在 IKEv2 安全关联 (SA) 中为 AnyConnect IPsec 连接指定加密算法，请在 ikev2 策略配置模式下使用 **encryption** 命令。要删除命令并使用默认设置，请使用此命令的 **no** 形式：

encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

no encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

语法说明

des	为 ESP 指定 56 位 DES-CBC 加密。
3des	（默认）为 ESP 指定三重 DES 加密算法。
aes	为 ESP 指定带有 128 位密钥加密的 AES。
aes-192	为 ESP 指定带有 192 位密钥加密的 AES。
aes-256	为 ESP 指定带有 256 位密钥加密的 AES。
aes-gcm	为 IKEv2 加密指定 AES-GCM 算法。
aes-gcm-192	为 IKEv2 加密指定 AES-GCM 算法。
aes-gcm-256	为 IKEv2 加密指定 AES-GCM 算法。
null	如果将 AES-GCM/GMAC 配置为加密算法，则选择 Null 完整性算法。

默认值

默认值为 3DES。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。输入 **crypto ikev2 policy** 命令后，可以使用 **encryption** 命令设置 SA 加密算法。

如果在接口上启用了 OSPFv3 加密，并且配置了 IPsec 隧道，则在建立相邻关系时可能会出现延迟。使用 **show crypto sockets**、**show ipsec policy** 和 **show ipsec sa** 命令可确定 IPsec 隧道的潜在状态以及是否正在进行处理。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Ikev2-policy 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	添加了此命令。
9.0(1)	添加了用于 IKEv2 加密的 AES-GCM 算法。

示例

以下示例进入 ikev2-policy 配置模式并将加密设置为 AES-256：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

相关命令

命令	说明
group	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 Diffie-Hellman 组。
integrity	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 ESP 完整性算法。
prf	指定用于 AnyConnect IPsec 连接的 IKEv2 SA 中的伪随机函数。
lifetime	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 SA 生命期。

endpoint

要向 HSI 组添加终端以进行 H.323 协议检查，请在 HSI 组配置模式下使用 **endpoint** 命令。要禁用此功能，请使用此命令的 **no** 形式。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

语法说明

if_name	终端连接到 ASA 所经过的接口。
ip_address	要添加的终端的 IP 地址。每个 HSI 组最多可有 10 个终端。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
HSI 组配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何向 H.323 检查策略映射中的 HSI 组添加终端：

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

相关命令

命令	说明
class-map	创建第 3/4 层类映射。
hsi-group	创建 HSI 组。
hsi	向创建的 HSI 组添加 HSI。
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。

endpoint-mapper

要配置用于 DCERPC 检查的终端映射程序选项，请在参数配置模式下使用 **endpoint-mapper** 命令。要禁用此功能，请使用此命令的 **no** 形式。

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

语法说明

epm-service-only	指定要在绑定过程中强制执行终端映射程序服务。
lookup-operation	指定要对终端映射程序服务启用查找操作。
timeout *value*	指定查找操作中的针孔超时。范围是 0:0:1 到 1193:0:0。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何在 DCERPC 策略映射中配置终端映射程序：

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

相关命令

命令	说明
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。

enforcenextupdate

要指定如何处理 NextUpdate CRL 字段，请在 ca-crl 配置模式下使用 **enforcenextupdate** 命令。要允许使用失效或缺少的 NextUpdate 字段，请使用此命令的 **no** 形式。

enforcenextupdate

no enforcenextupdate

语法说明

此命令没有任何参数或关键字。

默认值

强制使用默认设置（已启用）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Ca-crl 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果设置了此命令，CRL 必须带有未失效的 NextUpdate 字段。如果不使用此命令，ASA 允许在 CRL 中使用缺少或失效的 NextUpdate 字段。

示例

以下示例进入 crypto ca-crl 配置模式，并要求 CRL 带有对于中心信任点来说未过期的 NextUpdate 字段：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

相关命令

命令	说明
cache-time	指定缓存刷新时间（以分钟为单位）。
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。

enrollment-retrieval

要指定注册用户可以检索 PKCS12 注册文件的时间（以小时为单位），请在本地 crypto ca-server 配置模式下使用 **enrollment-retrieval** 命令。要将时间重置为默认小时数 (24)，请使用此命令的 **no** 形式。

enrollment-retrieval *timeout*

no enrollment-retrieval

语法说明

timeout	指定用户必须从本地 CA 注册网页检索已签发证书的小时数。有效的超时值范围是 1 到 720 小时。

默认值

默认情况下，将存储 PKCS12 注册文件，可供 24 小时检索。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Crypto ca-server 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

PKCS12 注册文件包含已签发证书和密钥对。该文件存储在本地 CA 服务器上，并在使用 **enrollment-retrieval** 命令指定的时段内可供从注册网页上检索。

被标记为允许注册的用户可以在 **otp expiration** 命令中指定的时间内使用密码进行注册。一旦用户注册成功，就会生成并存储 PKCS12 文件，并通过注册网络返回该文件的一份副本。在 **enrollment-retrieval** 命令中指定的命令时间段内，用户可以出于任何原因（例如，尝试注册时下载失败）返回以获取该文件的另一份副本。

注意　该时间段独立于 OTP 过期时段。

示例

以下示例指定可在签发证书后 48 小时内从本地 CA 服务器上检索 PKCS12 注册文件：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

以下示例将检索时间重置为默认值（24 小时）：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令的访问，从而允许您配置和管理本地 CA。
OTP expiration	指定发出的一次性密码对 CA 注册页面有效的持续时间（以小时为单位）。
smtp from-address	指定要在 CA 服务器生成的所有邮件的 E-mail From:（发件人）字段中使用的邮件地址。
smtp subject	指定要在本地 CA 服务器生成的所有邮件的主题字段中显示的文本。
subject-name-default	指定要在 CA 服务器签发的所有用户证书中与用户名一起使用的通用使用者名称 DN。

enrollment retry count

要指定重试次数，请在 crypto ca-trustpoint 配置模式下使用 **enrollment retry count** 命令。要恢复重试次数的默认设置，请使用此命令的 **no** 形式。

enrollment retry count *number*

no enrollment retry count

语法说明

number	尝试发送注册请求的最大次数。有效值为 0 到 100。

默认值

number 参数的默认设置为 0（无限）。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

请求证书后，ASA 会等待从 CA 接收证书。如果 ASA 在配置的重试时间段内未能收到证书，它会发送另一个证书请求。ASA 会重复发送请求，直至收到响应或配置的重试时间段结束。此命令是可选的，仅在配置了自动注册的情况下适用。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并在中心信任点中将注册重试次数配置为 20：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment retry period	指定在重新发送注册请求之前要等待的分钟数。

enrollment retry period

要指定重试时间段，请在 crypto ca trustpoint 配置模式下使用 **enrollment retry period** 命令。要恢复重试时间段的默认设置，请使用此命令的 **no** 形式。

enrollment retry period *minutes*

no enrollment retry period

语法说明

minutes	注册请求发送尝试之间相隔的分钟数。有效范围是 1 到 60 分钟。

默认值

默认设置为 1 分钟。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

请求证书后，ASA 会等待从 CA 接收证书。如果 ASA 在指定的重试时间段内未能收到证书，它会发送另一个证书请求。此命令是可选的，仅在配置了自动注册的情况下适用。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并在中心信任点中将注册重试时间段配置为 10 分钟：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。
default enrollment	将所有注册参数恢复为系统默认值。
enrollment retry count	定义注册请求尝试次数。

enrollment terminal

要指定使用此信任点进行剪切粘贴注册（又称为手动注册），请在 crypto ca-trustpoint 配置模式下使用 **enrollment terminal** 命令。要恢复此命令的默认设置，请使用此命令的 **no** 形式。

enrollment terminal

no enrollment terminal

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并为中心信任点指定 CA 剪切粘贴注册方法：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment retry count	指定尝试发送注册请求的重试次数。
enrollment retry period	指定在重新发送注册请求之前要等待的分钟数。
enrollment url	指定使用信任点进行自动注册 (SCEP) 并配置 URL。

enrollment url

要指定使用信任点进行自动注册 (SCEP) 并配置注册 URL，请在 crypto ca-trustpoint 配置模式下使用 **enrollment url** 命令。要恢复此命令的默认设置，请使用此命令的 **no** 形式。

enrollment url *url*

no enrollment url

语法说明

url	指定用于自动注册的 URL 的名称。最大长度为 1K 个字符（实际上不会达到此限制）。

默认值

默认设置为关闭。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并在 URL https://enrollsite 上为中心信任点指定 SCEP 注册：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment retry count	指定尝试发送注册请求的重试次数。
enrollment retry period	指定在重新发送注册请求之前要等待的分钟数。
enrollment terminal	指定使用此信任点进行剪切粘贴注册。

enrollment-retrieval

要指定注册用户可以检索 PKCS12 注册文件的时间（以小时为单位），请在本地 ca-server 配置模式下使用 **enrollment-retrieval** 命令。要将时间重置为默认小时数 (24)，请使用此命令的 **no** 形式。

enrollment-retrieval *timeout*

no enrollment-retrieval

语法说明

timeout	指定用户必须从本地 CA 注册网页检索已签发证书的小时数。有效的超时值范围是 1 到 720 小时。

默认值

默认情况下，将存储 PKCS12 注册文件，可供 24 小时检索。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 服务器配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

PKCS12 注册文件包含已签发证书和密钥对。该文件存储在本地 CA 服务器上，并在使用 **enrollment-retrieval** 命令指定的时段内可供从注册网页上检索。

被标记为允许注册的用户可以在通过 **otp expiration** 命令指定的时间内使用密码进行注册。一旦用户注册成功，就会生成并存储 PKCS12 文件，并通过注册网络返回该文件的一份副本。在 **enrollment-retrieval** 命令中指定的时间段内，用户可以出于任何原因（例如，尝试注册时下载失败）返回以获取该文件的另一份副本。

注意　该时间段独立于 OTP 过期时段。

示例

以下示例指定可在签发证书后 48 小时内从本地 CA 服务器上检索 PKCS12 注册文件：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

以下示例将检索时间重置为默认值（24 小时）：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令的访问，从而允许您配置和管理本地 CA。
OTP expiration	指定发出的一次性密码对 CA 注册页面有效的持续时间（以小时为单位）。
smtp from-address	指定要在 CA 服务器生成的所有邮件的 E-mail From:（发件人）字段中使用的邮件地址。
smtp subject	指定要在本地 CA 服务器生成的所有邮件的主题字段中显示的文本。
subject-name-default	指定要在 CA 服务器签发的所有用户证书中与用户名一起使用的通用使用者名称 DN。

eool

要定义具有 IP 选项检查的数据包中出现 End of Options List（选项列表末端）(EOOL) 选项时的操作，请在参数配置模式下使用 **eool** 命令。要禁用此功能，请使用此命令的 **no** 形式。

eool action {allow | clear}

no eool action {allow | clear}

语法说明

allow	指示 ASA 允许包含 End of Options List（选项列表末端）IP 选项的数据包通过。
clear	指示 ASA 从数据包清除 End of Options List（选项列表末端）IP 选项，然后允许数据包通过。

默认值

默认情况下，IP 选项检查会丢弃包含 End of Options List（选项列表末端）IP 选项的数据包。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

此命令可配置的 IP 选项检查策略映射中。

您可以配置 IP 选项来控制哪些 IP 数据包与特定的 IP 选项允许通过 ASA。检测 这种检查配置 ASA 以允许数据包通过或清除指定的 IP 选项，然后允许该数据包与过去指示

End of Options List（选项列表末端）选项（仅包含一个零字节）出现在所有选项的末端来标记选项列表结束。根据标题长度，这可能与标题的末端不一致。

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

相关命令

命令	说明
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。

eou allow

要在 NAC 框架配置中启用无客户端身份验证，请在全局配置模式下使用 **eou allow** 命令。要从配置中删除此命令，请使用此命令的 **no** 形式。

eou allow {**audit** | **clientless** | **none**}

no eou allow {**audit** | **clientless** | **none**}

语法说明

audit	执行无客户端身份验证。
clientless	执行无客户端身份验证。
none	禁用无客户端身份验证。

默认值

默认配置包含 **eou allow clientless** 配置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	添加了 **audit**（审核）选项。
9.1(2)	此命令已弃用。

使用指南

ASA 仅在以下两种情况都属实时使用此命令：

- 组策略被配置为使用 NAC 框架 NAC 策略类型。
- 会话中的主机没有响应 EAPoUDP 请求。

示例

以下示例使用 ACS 来执行无客户端身份验证：

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

以下示例展示如何将 ASA 配置为使用审核服务器来执行无客户端身份验证：

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

以下示例展示如何禁用审核服务器：

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

相关命令

命令	说明
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
eou clientless	在 NAC 框架配置中更改要发送到 ACS 以进行无客户端身份验证的用户名和密码。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。

eou clientless

要在 NAC 框架配置中更改要发送到访问控制服务器以进行无客户端身份验证的用户名和密码，请在全局配置模式下使用 **eou clientless** 命令。要使用默认值，则使用此命令的 **no** 形式。

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

语法说明

password	输入以更改发送到访问控制服务器的密码，以获取对没有响应 EAPoUDP 请求的远程主机的无客户端身份验证。
password	输入在访问控制服务器上配置的密码以支持无客户端主机。输入 4 到 32 个 ASCII 字符。
username	输入以更改发送到访问控制服务器的用户名，以获取对没有响应 EAPoUDP 请求的远程主机的无客户端身份验证。
username	输入在访问控制服务器上配置的用户名以支持无客户端主机。输入 1 到 64 个 ASCII 字符，不得包含前导空格、尾部空格、井号 (#)、问号 (?)、引号 (")、星号 (*) 以及尖括号（< 和 >）。

默认值

username（用户名）和 password（密码）属性的默认值为 clientless。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

此命令仅在以下情况都属实时有效：

- 在网络上配置了访问控制服务器来支持无客户端身份验证：
- 在 ASA 上启用了无客户端身份验证。
- 在 ASA 上配置了 NAC。

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例将无客户端身份验证的用户名更改为 sherlock：

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

以下示例将无客户端身份验证的用户名更改为默认值 clientless：

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

以下示例将无客户端身份验证的密码更改为 secret：

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

以下示例将无客户端身份验证的密码更改为默认值 clientless：

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

相关命令

命令	说明
eou allow	在 NAC 框架配置中启用无客户端身份验证。
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
debug nac	启用日志记录的 NAC 框架事件。

eou initialize

要清除分配给一个或多个 NAC 框架会话的资源并对每个这些会话发起无条件、全新的安全状态验证，请在特权 EXEC 模式下使用 **eou initialize** 命令。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

语法说明

all	重新验证 ASA 上的所有 NAC 框架会话。
group	重新验证分配给隧道组的所有 NAC 框架会话。
ip	重新验证单个 NAC 框架会话。
ip-address	隧道的远程对等端的 IP 地址。
tunnel-group	用于协商参数以设置隧道的隧道组名称。

默认值

没有默认行为或值。

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

如果远程对等设备的安全状态发生变化或者分配的访问策略（即，下载的 ACL）发生变化，且您想要清除分配给会话的资源，则可以使用此命令。输入此命令会清除用于安全状态验证的 EAPoUDP 关联和访问策略。NAC 默认 ACL 在重新验证期间是有效的，因此，会话初始化可能会中断用户流量。此命令不会影响免于接受安全状态验证的对等设备。

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例初始化所有 NAC 框架会话：

```
ciscoasa# eou initialize all
ciscoasa
```

以下示例初始化分配给名为 tg1 的隧道组的所有 NAC 框架会话：

```
ciscoasa# eou initialize group tg1
ciscoasa
```

以下示例初始化 IP 地址为 209.165.200.225 的终端的 NAC 框架会话：

```
ciscoasa# eou initialize 209.165.200.225
ciscoasa
```

相关命令

命令	说明
eou revalidate	强制立即状况一个或多个 NAC 框架会话的重新验证。
reval-period	指定 NAC 框架会话中每次成功安全状态验证之间的时间间隔。
sq-period	指定主机状态中的 NAC 框架会话中的每个成功安全状态验证和下一步的查询的更改的时间间隔。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。
debug nac	启用日志记录的 NAC 框架事件。

eou max-retry

要更改 ASA 向远程计算机重新发送 EAP over UDP 消息的次数，请在全局配置模式下使用 **eou max-retry** 命令。要使用默认值，则使用此命令的 **no** 形式。

eou max-retry *retries*

no eou max-retry

语法说明

retries	限制为响应重传计时器过期而连续重试发送消息的次数。可输入 1 到 3 之间的值。

默认值

默认值为 3。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

此命令仅在以下情况都属实时有效：

- 在网络上配置了访问控制服务器来支持无客户端身份验证：
- 在 ASA 上启用了无客户端身份验证。
- 在 ASA 上配置了 NAC。

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例将 EAP over UDP 重传次数限制为 1：

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

以下示例将 EAP over UDP 重传次数更改为默认值 3：

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

相关命令

eou timeout	更改将 EAP 通过 UDP 消息发送到 NAC 框架配置中的远程主机后等待秒的数。
sq-period	指定主机状态中的 NAC 框架会话中的每个成功安全状态验证和下一步的查询的更改的时间间隔。
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
debug nac	启用日志记录的 NAC 框架事件。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。

eou port

要更改 NAC 框架配置中用于与 Cisco Trust Agent 进行 EAP over UDP 通信的端口号，请在全局配置模式下使用 **eou port** 命令。要使用默认值，则使用此命令的 **no** 形式。

eou port *port_number*

no eou port

语法说明

port_number	客户端终端上将被指定用于 EAP over UDP 通信的端口号。此端口号是在 Cisco Trust Agent 上配置的端口号。可输入 1024 到 65535 之间的值。

默认值

默认值为 21862。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例将用于 EAP over UDP 通信的端口号更改为 62445：

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

以下示例将用于 EAP over UDP 通信的端口号更改为默认值：

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

相关命令

命令	说明
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
eou initialize	清除分配给一个或多个 NAC 框架会话的资源，并对每个会话发起无条件、全新的安全状态验证。
eou revalidate	强制立即状况一个或多个 NAC 框架会话的重新验证。
show vpn-session.db	显示有关 VPN 会话的信息，包括 VLAN 映射和 NAC 结果。
show vpn-session_summary.db	显示 IPsec 会话、Cisco AnyConnect 会话和 NAC 会话的数量（包括 VLAN 映射会话数据）。

eou revalidate

要强制立即重新验证一个或多个 NAC 框架会话的安全状态，请在特权 EXEC 模式下使用 **eou revalidate** 命令。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

语法说明

all	重新验证 ASA 上的所有 NAC 框架会话。
group	重新验证分配给隧道组的所有 NAC 框架会话。
ip	重新验证单个 NAC 框架会话。
ip-address	隧道的远程对等端的 IP 地址。
tunnel-group	用于协商参数以设置隧道的隧道组名称。

默认值

没有默认行为或值。

命令模式

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

如果对等设备的安全状态或分配的访问策略（即，下载的 ACL，如果有）发生变化，可使用此命令。此命令启动无条件、全新的安全状态验证。安全状态验证以及在您输入此命令之前已生效的分配的访问策略将保持有效，直至新的安全状态验证成功或失败。此命令不会影响免于接受安全状态验证的对等设备。

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例重新验证所有 NAC 框架会话：

```
ciscoasa# eou revalidate all
ciscoasa
```

以下示例重新验证分配给名为 tg-1 的隧道组的所有 NAC 框架会话：

```
ciscoasa# eou revalidate group tg-1
ciscoasa
```

以下示例重新验证 IP 地址为 209.165.200.225 的终端的 NAC 框架会话：

```
ciscoasa# eou revalidate ip 209.165.200.225
ciscoasa
```

相关命令

命令	说明
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
eou initialize	清除分配给一个或多个 NAC 框架会话的资源，并对每个会话发起无条件、全新的安全状态验证。
eou timeout	更改将 EAP 通过 UDP 消息发送到 NAC 框架配置中的远程主机后等待秒的数。
reval-period	指定 NAC 框架会话中每次成功安全状态验证之间的时间间隔。
sq-period	指定主机状态中的 NAC 框架会话中的每个成功安全状态验证和下一步的查询的更改的时间间隔。

eou timeout

要更改将 EAP over UDP 消息发送到 NAC 框架配置中的远程主机后等待的秒数，请在全局配置模式下使用 **eou timeout** 命令。要使用默认值，则使用此命令的 **no** 形式。

eou timeout {**hold-period** | **retransmit**} *seconds*

no eou timeout {**hold-period** | **retransmit**}

语法说明

hold-period	发送 EAPoUDP 消息后等待的最长时间等于 EAPoUDP 尝试次数。**eou initialize** 或 **eou revalidate** 命令也可清除此计时器。如果此计时器过期，ASA 会发起与远程主机之间的新的 EAP over UDP 关联。
retransmit	发送 EAPoUDP 消息后等待的最长时间。来自远程主机的响应将清除此计时器。**eou initialize** 或 **eou revalidate** 命令也可清除此计时器。如果此计时器过期，ASA 会向远程主机重新传输 EAPoUDP 消息。
seconds	ASA 等待的秒数。为 hold-period（保持期）属性输入一个 60 到 86400 之间的值，为 retransmit（重传）属性输入一个 1 到 60 之间的值。

默认值

hold-period（保持期）选项的默认值是 180。

retransmit（重传）选项的默认值是 3。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

此命令仅适用于思科 NAC 的框架实现。

示例

以下示例将发起新的 EAP over UDP 关联之前等待的时间更改为 120 秒：

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

以下示例将发起新的 EAP over UDP 关联之前等待的时间更改为默认值：

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

以下示例将重传计时器更改为 6 秒：

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

以下示例将重传计时器更改为默认值：

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

相关命令

命令	说明
debug eou	启用 EAP over UDP 事件的日志记录以调试 NAC 框架消息。
eou max-retry	更改 ASA 向远程计算机重新发送 EAP over UDP 消息的次数。

erase

要擦除并重新格式化文件系统，请在特权 EXEC 模式下使用 **erase** 命令。此命令覆盖所有文件并擦除文件系统（包括隐藏的系统文件），然后重新安装文件系统。

erase [**disk0: | disk1: | flash:**]

语法说明

disk0:	（可选）指定 f，后跟冒号。
disk1:	（可选）指定外部紧凑式闪存卡，后跟冒号。
flash:	（可选）指定内部闪存后 , 跟冒号。

注意事项　擦除闪存还会删除许可信息（这些信息存储在闪存中）。请在擦除闪存之前保存许可信息。

在 ASA 5500 系列上，**flash** 关键字是 **disk0:** 的别名。

默认值

没有默认行为或默认值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

erase 命令会擦除闪存中使用 OxFF 模式的所有数据，然后将一个空的文件系统分配表重新写入到设备。

要删除所有可见的文件（隐藏的系统文件除外）请输入 **delete /recursive** 命令而不是 **erase** 命令。

注意　在思科 ASA 5500 系列上，**erase** 命令会销毁磁盘中使用 0xFF 模式的所有用户数据。相反，**format** 命令仅重置文件系统的控制结构。使用原始磁盘读取工具仍可看到磁盘中的信息。

示例

以下示例擦除并重新格式化文件系统：

```
ciscoasa# erase flash:
```

相关命令

命令	说明
delete	删除所有可见的文件，但不删除隐藏的系统文件。
format	擦除所有文件（包括隐藏的系统文件）并格式化文件系统。

esp

要指定 ESP 隧道和 AH 隧道的参数以进行 IPsec 传递检查，请在参数配置模式下使用 **esp** 命令。要禁用此功能，请使用此命令的 **no** 形式。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

语法说明

esp	指定 ESP 隧道的参数。
ah	指定 AH 隧道的参数。
per-client-max *num*	指定一个客户端的最大隧道数。
timeout *time*	指定 ESP 隧道的空闲超时。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何允许 UDP 500 流量：

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl

ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

相关命令

命令	说明
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。

established

要允许基于已建立连接的端口上存在返回连接，请在全局配置模式下使用 **established** 命令。要禁用 **established** 功能，请使用此命令的 **no** 形式。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

语法说明

est_protocol	指定要用于已建立的连接查找的 IP 协议（UDP 或 TCP）。
dest_port	指定要用于已建立的连接查找的目标端口。
permitfrom	（可选）允许来自指定端口的返回协议连接。
permitto	（可选）允许发往指定端口的返回协议连接。
port [*-port*]	（可选）指定返回连接的（UDP 或 TCP）目标端口。
protocol	（可选）返回连接使用的 IP 协议（UDP 或 TCP）。
source_port	（可选）指定要用于已建立的连接查找的源端口。

默认值

默认值如下：

- *dest_port*—0 (wildcard)
- *source_port*—0 (wildcard)

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	从 CLI 中删除了 **to** 和 **from** 这两个关键字， 取而代之的是 **permitto** 和 **permitfrom** 关键字。

使用指南

使用 **established** 命令可允许出站连接的返回访问通过 ASA。此命令适用于从网络出站并受 ASA 保护的原始连接，也适用于外部主机上相同两台设备之间的返回入站连接。使用 **established** 命令可指定用于连接查找的目标端口。新增的关键字有利于更好地控制命令，并提供对于目标端口已知但源端口未知的协议的支持。**permitto** 和 **permitfrom** 关键字定义返回入站连接。

注意事项　我们建议始终为 **established** 命令指定 **permitto** 和 **permitfrom** 关键字。不将这两个关键字与 **established** 命令结合使用将造成安全风险，因为连接到外部系统时，外部系统可能会与涉及连接的内部主机进行不受限制的连接。攻击者可能会利用这种情况来攻击您的内部系统。

示例

以下一组示例展示如果不正确使用 **established** 命令可能会发生的潜在安全违规情况。

此示例展示如果内部系统与端口 4000 上的一个外部主机进行 TCP 连接，则该外部主机可使用任何协议通过任何端口返回：

```
ciscoasa(config)# established tcp 4000 0
```

如果协议未指定使用了哪些端口，您可以将源端口和目标端口指定为 **0**。应仅在必要时使用通配符端口 (0)。

```
ciscoasa(config)# established tcp 0 0
```

注意　要使 **established** 命令能够正常工作，客户端必须侦听使用 **permitto** 关键字指定的端口。

established 命令可与 **nat 0** 命令结合使用（在没有 **global** 命令的情况下）。

注意　**established** 命令不可与 PAT 结合使用。

有了 **established** 命令，ASA 可支持 XDMCP。

注意事项　通过 ASA 使用 XWindows 系统应用可能会造成安全风险。

XDMCP 默认情况下已启用，但它要等到您输入如下 **established** 命令后才会完成会话：

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

输入 **established** 命令会使装有 XDMCP 的内部（UNIX 或 ReflectionX）主机访问装有 XDMCP 的外部 XWindows 服务器。基于 UDP/177 的 XDMCP 会协商基于 TCP 的 XWindows 会话，且后续 TCP 返回连接将获允许。由于返回流量的源端口未知，因此，请将 *source_port* 字段指定为 0（通配符）。*dest_port* 应为 6000 + *n*，其中，*n* 代表本地显示编号。使用以下 UNIX 命令可更改此值：

```
ciscoasa(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

需要使用 **established** 命令，因为会（基于用户交互）生成很多 TCP 连接，且这些连接的源端口是未知的。只有目标端口是静态端口。ASA 以透明方式执行 XDMCP 修复。无需任何配置，但必须输入 **established** 命令以支持 TCP 会话。

以下示例展示两台主机之间使用协议 A 从源端口 C 发往端口 B 的连接。要允许返回连接通过 ASA 和协议 D（协议 D 可以不同于协议 A），源端口必须对应于端口 F，且目标端口必须对应于端口 E。

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

以下示例展示内部主机如何使用 TCP 目标端口 6060 和任何源端口向外部主机发起连接。ASA 允许这两台主机之间的返回流量通过 TCP 目标端口 6061 和任何 TCP 源端口。

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

以下示例展示内部主机如何使用 UDP 目标端口 6060 和任何源端口向外部主机发起连接。ASA 允许这两台主机之间的返回流量通过 TCP 目标端口 6061 以及 1024 到 65535 之间的 TCP 源端口。

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

以下示例展示本地主机如何在端口 9999 上向外部主机发起 TCP 连接。此示例允许来自端口 4242 上外部主机的数据包返回到端口 5454 上的本地主机。

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

相关命令

命令	说明
clear configure established	删除所有已建立的命令。
show running-config established	显示根据已建立的连接获允许的入站连接。

event crashinfo

要在 ASA 上出现故障时触发事件管理器小程序，请在事件管理器小程序配置模式下使用 **event crashinfo** 命令。要删除故障事件，请使用此命令的 **no** 形式。

event crashinfo

no event crashinfo

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
事件管理器小应用配置	• 是	• Ye	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

无论 **output** 命令的值如何，**action** 命令都指向故障信息文件。输出在 **show tech** 命令之前生成。

注意　当 ASA 发生故障时，其状态通常是未知的。在这种情况下，运行某些 CLI 命令可能不安全。

示例

以下示例在 ASA 发生故障时触发小程序：

```
ciscoasa(config-applet)# event crashinfo
```

相关命令

命令	说明
event none	手动调用事件管理器小应用。
event syslog id	向事件管理器小应用添加系统日志事件。
event timer absolute time	配置绝对事件计时器。
event timer countdown time	配置倒计时计时器事件。
event timer watchdog time	配置监视器计时器事件。

event manager applet

要创建或编辑会将事件与操作和输出关联起来的事件管理器小程序，请在全局配置模式下使用事件管理器小程序命令。要删除事件管理器小程序，请使用此命令的 **no** 形式。

event manager applet *name*

no event manager applet *name*

语法说明

name	指定事件管理器小程序的名称。此名称最多可包含 32 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **event manager applet** 命令可进入事件管理器小程序配置模式。

示例

以下示例创建事件管理器小程序并进入事件管理器小程序配置模式：

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

相关命令

命令	说明
description	描述小应用。
event manager run	运行事件管理器小应用。
show event manager	显示已配置的每个事件管理器小应用的统计信息。
debug event manager	管理事件管理器的调试跟踪记录。

event none

要手动调用事件管理器小程序，请在事件管理器小程序配置模式下使用 **event none** 命令。要删除手动调用，请使用此命令的 **no** 形式。

event none

no event none

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
事件管理器小应用配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

可以使用 **event none** 命令配置任何其他事件。

示例

以下示例手动调用事件管理器小程序：

```
ciscoasa(config-applet)# event none
```

相关命令

命令	说明
event crashinfo	在 ASA 上出现故障时触发事件管理器小应用。
event syslog id	向事件管理器小程序添加系统日志事件。
event timer absolute time	配置绝对事件计时器。
event timer countdown time	配置倒计时计时器事件。
event timer watchdog time	配置监视器计时器事件。

event syslog id

要向事件管理器小程序添加系统日志事件，请在事件管理器小程序配置模式下使用 **event syslog id** 命令。要从事件管理器小程序删除系统日志事件，请使用此命令的 **no** 形式。

event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

no event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

语法说明

nnnnnn	标识系统日志消息 ID。
occurs *n*	指明调用小程序之前系统日志消息必须出现的次数。默认值为 1。有效值为 1 到 4294967295。
period *seconds*	指明事件必须发生的时间段（以秒为单位），并将小程序调用频率限制为在配置的时间段内最多调用一次。有效值为 0 到 604800。值 0 表示未定义时间段。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
事件管理器小应用配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **event syslog id** 命令可标识触发小程序的单个系统日志消息或一系列系统日志消息。

示例

以下示例指明系统日志消息 106201 会触发小程序：

```
ciscoasa(config-applet)# event syslog id 106201
```

相关命令

命令	说明
event crashinfo	在 ASA 上出现故障时触发事件管理器小应用。
event none	手动调用事件管理器小应用。
event timer absolute time	配置绝对事件计时器。
event timer countdown time	配置倒计时计时器事件。
event timer watchdog time	配置监视器计时器事件。

event timer

要配置计时器事件，请在事件管理器小程序配置模式下使用 **event timer** 命令。要删除计时器事件，请使用此命令的 **no** 形式。

event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

no event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

语法说明

absolute time	指定事件每天在指定的时间发生一次并自动重新启动。
countdown time	指定事件发生一次，且在删除并重新添加后才会重新启动。
hh:mm:ss	指定时间格式。时间范围是 00:00:00（午夜）到 23:59:59。
seconds	指定秒数。有效值范围是 0 到 604800。值 0 会禁用计时器。
watchdog time	指定事件在每个配置的时间段内发生一次并自动重新启动。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
事件管理器小应用配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **event timer absolute time** 命令可促使事件每天在指定的时间发生一次并自动重新启动。

使用 **event timer countdown time** 命令可促使事件发生一次且在删除并重新添加后才会重新启动。

使用 **event timer watchdog time** 命令可促使事件在每个配置的时间段内发生一次并自动重新启动。

示例

以下示例促使事件每天在显示的指定时间发生一次：

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

以下示例促使事件每天在显示的指定时间发生一次：

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

以下示例促使事件每天发生一次并自动重新启动：

```
ciscoasa(config-applet)# event timer watchdog time 30
```

相关命令

命令	说明
event crashinfo	在 ASA 上出现故障时触发事件管理器小应用。
event none	手动调用事件管理器小应用。
event syslog id	向事件管理器小应用添加系统日志事件。
event timer countdown time	配置倒计时计时器事件。
event timer watchdog time	配置监视器计时器事件。

exceed-mss

要允许或丢弃数据长度超过对等设备在三次握手期间设置的 TCP 最大分段大小 (MSS) 的数据包，请在 tcp-map 配置模式下使用 **exceed-mss** 命令。要删除此指定，请使用此命令的 **no** 形式。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

语法说明

allow	允许长度超过 MSS 的数据包。此为默认设置。
drop	丢弃长度超过 MSS 的数据包。

默认值

默认情况下允许此类数据包。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(4)/8.0(4)	默认设置从 **drop** 更改为 **allow**。

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。使用 **policy-map** 命令应用新 TCP 映射。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 **exceed-mss** 命令可丢弃数据长度超过对等设备在三次握手期间设置的 TCP 最大分段大小的 TCP 数据包。

示例

以下示例丢弃端口 21 上大小超过 MSS 的流量：

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
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	说明
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 advanced-options	配置高级连接功能（包括 TCP 规范化）。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

exempt-list

要向免于接受安全状态验证的远程计算机类型的列表添加条目，请在 nac-policy-nac-framework 配置模式下使用 **exempt-list** 命令。要从免除列表删除条目，请使用此命令的 **no** 形式，并指定要删除的条目中的操作系统和 ACL。

exempt-list os "*os-name*" [**disable | filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable | filter** *acl-name* [**disable**]]

语法说明

acl-name	指定 ASA 配置中 ACL 的名称。如果指定了该名称，它必须跟在 **filter** 关键字后面。
disable	执行两种功能之一，具体如下： • 如果在 “os-name” 后面输入此部分，ASA 会忽略免除项，并将 NAC 安全状态验证应用于运行该操作系统的远程主机。 • 如果在 *acl-name* 后面输入此部分，ASA 会免除指定的操作系统，但不会将 ACL 分配给关联的流量。
filter	如果计算机的操作系统与 *os name* 匹配，将应用 ACL 以过滤流量。**filter/***acl-name* 对是可选的。
os	免除操作系统接受安全状态验证。
os name	操作系统名称。仅在名称包含空格时需要使用引号（例如，"Windows XP"）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Nac-policy-nac-framework 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	命令名称从 **vpn-nac-exempt** 更改为 **exempt-list**。命令在组策略配置模式下移到 nac- 策略 -nac- 框架配置模式。

使用指南

当此命令指定操作系统时，它不会覆盖之前向免除列表添加的条目；请为要免除的每个操作系统和 ACL 输入此命令一次。

no exempt-list 命令会从 NAC 框架策略删除所有免除项。在发出此命令的 **no** 形式时指定条目从免除列表删除该条目。

要从与该 NAC 策略关联的免除列表删除所有条目，请在不指定其他关键字的情况下使用此命令的 **no** 形式。

示例

以下示例将运行 Windows XP 的所有主机添加到免于接受安全状态验证的计算机列表：

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

以下示例免除运行 Windows XP 的所有主机，并将 ACL acl-1 应用于来自这些主机的流量：

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

以下示例从免除列表删除同一个条目：

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

以下示例从免除列表删除所有条目：

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

相关命令

命令	说明
debug nac	启用日志记录的 NAC 框架事件。
nac-policy	创建和访问 Cisco NAC 策略，并指定其类型。
nac-settings	将 NAC 策略分配到组策略。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。
show vpn-session_summary.db	显示 IPsec 会话、Cisco AnyConnect 会话和 NAC 会话的数量。

exit

要退出当前配置模式或者从特权或用户 EXEC 模式中注销，请使用 **exit** 命令。

exit

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

还可以使用按键序列 **Ctrl+Z** 退出全局配置（及更高配置）模式。此按键序列不起作用的特权或用户执行模式。

当您在特权或用户 EXEC 模式下输入 **exit** 命令时，您会从 ASA 注销。使用**禁用**命令返回特权 EXEC 模式下的用户执行模式。

示例

以下示例展示如何使用 **exit** 命令退出全局配置模式，然后从会话中注销：

```
ciscoasa(config)# exit
ciscoasa# exit

Logoff
```

以下示例展示如何使用 **exit** 命令退出全局配置模式，然后使用 **disable** 命令退出特权 EXEC 模式：

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

相关命令

命令	说明
quit	退出配置模式或者从特权或用户 EXEC 模式中注销。

expiry-time

要配置不需要重新验证即缓存对象的到期时间，请在缓存配置模式下使用 **expiry-time** 命令。要从配置中删除到期时间并将到期时间重置为默认值，请使用此命令的 **no** 形式。

expiry-time *time*

no expiry-time

语法说明

time	ASA 在不重新验证对象的情况下缓存对象的时间长度（以分钟为单位）。

默认值

默认值为 1 分钟。

命令模式

下表显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	单个	情景	系统
缓存配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

到期时间是指 ASA 在不重新验证对象的情况下缓存对象的时间长度，以分钟为单位。重新验证包括重新检查内容。

示例

以下示例展示如何将到期时间设置为 13 分钟：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

相关命令

命令	说明
cache	进入 WebVPN 缓存配置模式。
cache-compressed	配置 WebVPN 缓存压缩。
disable	禁用缓存。
lmfactor	为缓存只有最后修改时间戳的对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义要缓存的对象的最小大小。

export

要指定要导出到客户端的证书，请在 ctl-provider 配置模式下使用 **export** 命令。要删除配置，请使用此命令的 **no** 形式。

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

语法说明

certificate *trustpoint_name*	指定要导出到客户端的证书。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Ctl-provider 配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在 ctl-provider 配置模式下使用 **export** 命令可指定要导出到客户端的证书。信任点名称由 **crypto ca trustpoint** 命令定义。指定的证书将添加到 CTL 客户端撰写的 CTL 文件中。

示例

以下示例展示如何创建 CTL 提供程序实例：

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

相关命令

命令	说明
ctl	解析来自 CTL 客户端的 CTL 文件并安装信任点。
ctl-provider	在 ctl-provider 配置模式下配置 CTL 提供程序实例。
client	指定允许连接到 CTL 提供程序的客户端以及用于客户端身份验证的用户名和密码。
service	指定 CTL 提供程序侦听的端口。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

export webvpn AnyConnect-customization

要导出可定制 AnyConnect 客户端 GUI 的定制对象，请在特权 EXEC 模式下使用 **export webvpn AnyConnect-customization** 命令：

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

语法说明

name	用于标识定制对象的名称。最多 64 个字符。
type	定制类型： • 二进制 - 取代 AnyConnect GUI 的可执行文件。 • 转型 - 自定义 MSI 的转换。
url	用于导出 XML 定制对象的远程路径和文件名，以 *URL/filename* 的形式表示（最多可包含 255 个字符）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

AnyConnect 定制对象是驻留在缓存内存中的 XML 文件，用于为 AnyConnect 客户端用户定制 GUI 屏幕。导出定制对象时，会在指定的 URL 创建一个包含 XML 标记的 XML 文件。

由名为 *Template* 的定制对象创建的 XML 文件包含空的 XML 标记，为创建新的定制对象提供了基础。不能更改或从缓存内存中删除该对象，但可以导出、编辑并将它重新导入到 ASA，使它成为新的定制对象。

Template 的内容与初始 DfltCustomization 对象状态相同。

有关使用 AnyConnect GUI 的资源文件及其文件名的完整列表，请参阅 *《AnyConnect VPN 客户端管理员指南》*。

示例

以下示例导出 AnyConnect GUI 上使用的思科徽标：

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

相关命令

命令	说明
import webvpn customization	将 XML 文件作为定制对象导入到缓存内存。
revert webvpn customization	从缓存内存中删除定制对象。
show import webvpn customization	显示有关位于缓存内存中的定制对象的信息。

export webvpn customization

要导出可定制对无客户端 SSL VPN 用户可见的屏幕的定制对象，请在特权 EXEC 模式下使用 **export webvpn customization** 命令。

export webvpn customization *name url*

语法说明

name	用于标识定制对象的名称。最多 64 个字符。
url	用于导出 XML 定制对象的远程路径和文件名，以 *URL/filename* 的形式表示（最多可包含 255 个字符）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

定制对象是驻留在缓存内存中的 XML 文件，可用于定制对无客户端 SSL VPN 用户可见的屏幕（包括登录屏幕、注销屏幕、门户页面和可用语言）。导出定制对象时，会在指定的 URL 创建一个包含 XML 标记的 XML 文件。

由名为 *Template* 的定制对象创建的 XML 文件包含空的 XML 标记，为创建新的定制对象提供了基础。不能更改或从缓存内存中删除该对象，但可以导出、编辑并将它重新导入到 ASA，使它成为新的定制对象。

Template 的内容与初始 DfltCustomization 对象状态相同。

可以使用 **export webvpn customization** 命令导出定制对象，更改 XML 标记，以及使用 **import webvpn customization** 命令将文件导入为新对象。

示例

以下示例导出默认定制对象 (DfltCustomization) 并创建名为 dflt_custom 的 XML 文件：

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

相关命令

命令	说明
import webvpn customization	将 XML 文件作为定制对象导入到缓存内存。
revert webvpn customization	从缓存内存中删除定制对象。
show import webvpn customization	显示有关位于缓存内存中的定制对象的信息。

export webvpn plug-in

要从 ASA 的闪存设备导出插件，请在特权 EXEC 模式下输入 **export webvpn plug-in** 命令。

import webvpn plug-in protocol *protocol URL*

语法说明

protocol	• **rdp** 插件的远程桌面协议可以使远程用户连接到计算机运行 Microsoft 终端服务。思科会原样重分布此插件。包含原件的网站是 http://properjavardp.sourceforge.net/。 • **ssh,telnet** Secure Shell 插件可以使远程用户建立远程计算机的安全信道或可以使远程用户使用 Telnet 连接到远程计算机。思科会原样重分布此插件。包含原件的网站是 http://javassh.org/。 **注意事项** **export webvpn plug-in protocol ssh,telnet** *URL* 命令导出 SSH *和* Telnet 插件。请*勿*分别对 SSH 和 Telnet 各输入一次此命令。键入 **ssh,telnet** 字符串时，*不*要插入空格。 • **vnc** 虚拟网络计算插件使远程用户可以使用显示器、键盘和鼠标来查看和控制一台计算机打开远程桌面设备共享。思科会原样重分布此插件。包含原件的网站是 http://www.tightvnc.com/。
URL	远程设备的路径。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

导出插件不会从闪存中删除插件。导出时会在指定的 URL 创建所导出插件的副本。

示例

以下命令导出 RDP 插件：

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

相关命令

命令	说明
import webvpn plugin	将指定的插件从本地设备导出到 ASA 闪存。
revert webvpn plug-in protocol	从 ASA 的闪存设备中删除指定的插件。
show import webvpn plug-in	列出插件 ASA。闪存设备上存在

export webvpn mst-translation

要导出转换 AnyConnect 安装程序的 Microsoft 转换文件 (MST)，请在特权 EXEC 模式下使用 **export webvpn mst-translation** 命令：

export webvpn mst-translation *component* **language** *language URL*

语法说明

component	应用此 MST 的组件。唯一有效的选项是 AnyConnect。
language	导出的 MST 的语言代码。应以浏览器要求的格式使用语言代码。
URL	用于导出转换文件的远程路径和文件名，以 *URL/filename* 的形式表示（最多可包含 255 个字符）。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

正如 AnyConnect 客户端 GUI 一样，您可以翻译客户端安装程序显示的消息。ASA 使用转换文件翻译安装程序显示的消息。转换文件将更改安装，但已签署安全性的原始 MSI 将保持原样。这些转换文件仅翻译安装程序屏幕，不会翻译客户端 GUI 屏幕。

每个语言都有各自的转换文件。您可以用转换文件编辑器（例如 Orca）编辑转换文件，并更改消息字符串。然后将转换文件导入到 ASA。当用户下载客户端时，客户端会检测计算机的首选语言（在操作系统安装过程中指定的区域设置）并应用相应的转换文件。

我们目前提供 30 种语言的转换文件。可在 cisco.com 的 AnyConnect 客户端软件下载页面下载包含这些转换文件的以下 .zip 文件：

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

在此文件中，<VERSION> 是 AnyConnect 的发行版本（例如 2.2.103）。

示例

以下示例将英文版的转换文件导出为 AnyConnect_Installer_English：

```
ciscoasa# export webvpn mst-translation AnyConnect language es
tftp://209.165.200.225/AnyConnect_Installer_English
```

相关命令

命令	说明
import webvpn customization	将 XML 文件作为定制对象导入到缓存内存。
revert webvpn customization	从缓存内存中删除定制对象。
show import webvpn customization	显示有关位于缓存内存中的定制对象的信息。

export webvpn translation-table

要导出转换表（用于转换显示给建立 SSL VPN 连接的远程用户的术语），请在特权 EXEC 模式下使用 **export webvpn translation-table** 命令。

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

语法说明

language	指定以前导入的转换表的名称。以浏览器语言选项指示的方式输入值。
translation_domain	功能区和相关消息。表 14-1 列出了可用的转换域。
url	指定对象的 URL。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

对于向发起基于浏览器的无客户端 SSL VPN 连接的用户显示的门户网站和屏幕，以及向 AnyConnect VPN 客户端用户显示的用户界面，ASA 提供语言转换。

远程用户可见的每个功能区及其消息都有其自身的转换域，由 *translation_domain* 参数指定。表 14-1 显示转换域和转换的功能区。

表 14-1　　转换域和受影响的功能区

转换域	转换的功能区
AnyConnect	在 Cisco AnyConnect VPN 客户端用户界面上显示的消息。
banners	VPN 访问被拒绝时显示给远程用户的标语和消息。
CSD	适用于思科安全桌面 (CSD) 的消息。
customization	登录和注销页面、门户页面上的消息以及用户可定制的所有消息。
plugin-ica	适用于 Citrix 插件的消息。
plugin-rdp	适用于远程桌面协议插件的消息。
plugin-telnet,ssh	适用于 Telnet 和 SSH 插件的消息。
plugin-vnc	适用于 VNC 插件的消息。

转换域	转换的功能区
PortForwarder	显示给端口转发用户的消息。
url-list	用户为门户页面上的 URL 书签指定的文本。
webvpn	所有不可定制的第 7 层、AAA 和门户消息。

转换模板是与转换表格式相同的 XML 文件，但所有转换为空。ASA 的软件映像包包括属于标准功能的每个域的模板。插件模板随附于插件，用于定义其自己的转换域。因为您可以定制无客户端用户的登录和注销页面、门户页面以及 URL 书签，所以 ASA 会动态生成 customization 和 url-list 转换域模板，并且模板会自动反映您对这些功能区的更改。

导出之前导入的转换表会在 URL 位置创建该转换表的 XML 文件。可以使用 **show import webvpn translation-table** 命令以列表形式查看可用模板和之前导入的表。

可以使用 **export webvpn translation-table** 命令下载模板或转换表，更改消息，以及使用 **import webvpn translation-table** 命令导入转换表。

示例

以下示例导出转换域 *customization* 的模板（该转换域用于转换登录和注销页面、门户页面以及所有显示给建立无客户端 SSL VPN 连接的远程用户的可定制消息）。ASA 创建一个名为 *Sales* 的 XML 文件：

```
ciscoasa# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

以下示例导出之前为名为 *zh* 的中文导入的转换表（这里的 zh 与 Microsoft Internet Explorer 浏览器的“Internet 选项”中指定的代表中文的缩写词相一致）。ASA 创建一个名为 *Chinese* 的 XML 文件：

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

相关命令

命令	说明
import webvpn translation-table	导入转换表。
revert	从缓存内存删除转换表。
show import webvpn translation-table	显示已导入的转换表相关信息。

export webvpn url-list

要将 URL 列表导出到远程位置，请在特权 EXEC 模式下使用 **export webvpn url-list** 命令。

export webvpn url-list *name url*

语法说明

name	用于标识 URL 列表的名称。最多可包含 64 个字符。
url	URL 列表来源的远程路径。最多 255 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

默认情况下，WebVPN 中没有任何 URL 列表。

可以使用 **export webvpn url-list** 命令下载名为 Template 的对象。不能更改或删除 Template 对象。可以编辑 Template 对象的内容并将其保存为定制 URL 列表，还可以使用 **import webvpn url-list** 命令导入该对象的内容以添加定制 URL 列表。

导出之前导入的 URL 列表会在 URL 位置创建该列表的 XML 文件。可以使用 **show import webvpn url-list** 命令以列表形式查看可用模板和之前导入的表。

示例

以下示例导出名为 *servers* 的 URL 列表：

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

相关命令

命令	说明
import webvpn url-list	导入 URL 列表。
revert webvpn url-list	从缓存内存中删除 URL 列表。
show import webvpn url-list	显示有关所导入 URL 列表的信息。

export webvpn webcontent

要导出远程无客户端 SSL VPN 用户可见的闪存中之前导入的内容，请在特权 EXEC 模式下使用 **export webvpn webcontent** 命令。

export webvpn webcontent *source url destination url*

语法说明

destination url	要导出到的 URL。最多 255 个字符。
source url	ASA 闪存中内容所在的 URL。最多 64 个字符。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

远程无客户端用户可以看到使用 **webcontent** 选项导出的内容。这些内容包括之前导入的在无客户端门户上可见的帮助内容以及定制对象使用的徽标。

可以通过在 **export webvpn webcontent** 命令后面输入问号 (**?**) 来查看可供导出的内容列表。例如：

```
ciscoasa# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.
  /+CSCOU+/cisco_logo.gif
```

示例

以下示例使用 TFTP 将文件 *logo.gif* 以文件名 *logo_copy.gif* 导出到 209.165.200.225：

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

相关命令

命令	说明
import webvpn webcontent	导入无客户端 SSL VPN 用户可见的内容。
revert webvpn webcontent	从闪存中删除内容。
show import webvpn webcontent	显示已导入内容的相关信息。

第 15 章

failover 至 fallback 命令

failover

要启用故障切换，请在全局配置模式下使用 **failover** 命令。要禁用故障切换，请使用此命令的 **no** 形式。

failover

no failover

语法说明

此命令没有任何参数或关键字。

默认值

禁用故障切换。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令被限制为在配置中启用或禁用故障切换（请参阅 **failover active** 命令）。

使用指南

使用此命令的 **no** 形式可禁用故障切换。

注意事项

通过故障切换和状态故障切换链路发送的所有信息均以明文发送，除非您使用故障切换密钥加密通信。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果要使用 ASA 端接 VPN 隧道，建议通过故障切换密钥来加密故障切换通信。

ASA 5505 设备只允许无状态故障切换，并且仅当未用作 Easy VPN 硬件客户端时才允许。

示例

以下示例禁用故障切换：

```
ciscoasa(config)# no failover
ciscoasa(config)#
```

相关命令

命令	说明
clear configure failover	从运行配置中清除 **failover** 命令并恢复故障切换默认值。
failover active	将备用设备切换到主用状态。
show failover	显示设备的故障切换状态的信息。
show running-config failover	显示运行配置中的 **failover** 命令。

failover active

要将备用 ASA 或故障切换组切换到主用状态，请在特权 EXEC 模式下使用 **failover active** 命令。要将主用 ASA 或故障切换组切换到备用状态，请使用此命令的 **no** 形式。

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

语法说明

group *group_id*	（可选）指定要变为主用状态的故障切换组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为包括故障切换组。

使用指南

使用 **failover active** 命令从备用设备发起故障切换，或使用 **no failover active** 命令从主用设备发起故障切换。您可以使用此功能使故障设备恢复服务，或强制主用设备离线以进行维护。如果不使用 “ 状态故障切换 ”，所有活动连接都将被丢弃，并且在进行故障切换之后必须由客户端重新建立。

故障切换组的切换仅适用于 Active/Active（主用 / 主用）故障切换。如果在未指定故障切换组的情况下针对 Active/Active（主用 / 主用）故障切换设备输入 **failover active** 命令，则该设备上的所有故障切换组都变为主用状态。

示例

以下示例将备用组 1 切换到主用状态：

```
ciscoasa# failover active group 1
```

相关命令

命令	说明
failover reset	使 ASA 从故障状态变为备用状态。

failover exec

要在故障切换对中的特定设备上执行命令，请在特权 EXEC 模式或全局配置模式下使用 **failover exec** 命令。

failover exec {**active** | **standby** | **mate**} *cmd_string*

语法说明

active	指定在故障切换对中的主用设备或故障切换组上执行命令。在主用设备或故障切换组上输入的配置命令将复制到备用设备或故障切换组。
cmd_string	要执行的命令。支持 **Show**、configuration 和 EXEC 命令。
mate	指定在故障切换对等设备上执行命令。
standby	指定在故障切换对中的备用设备或故障切换组上执行命令。在备用设备或故障切换组上执行的配置命令不会复制到主用设备或故障切换组。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

您可以使用 **failover exec** 命令向故障切换对中的特定设备发送命令。

由于配置命令从主用设备或情景复制到备用设备或情景，因此可以使用 **failover exec** 命令在正确的设备上输入配置命令，无论您登录到哪个设备。例如，如果您登录到备用设备，则可以使用 **failover exec active** 命令向主用设备发送配置更改。这些更改随后会复制到备用设备。请勿使用 **failover exec** 命令向备用设备或情景发送配置命令；这些配置更改不会复制到主用设备，而且两个配置将不再同步。

configuration、exec 和 **show** 命令的输出显示在当前终端会话中，因此您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

命令模式

failover exec 命令会保持独立于您的终端会话命令模式的命令模式状态。默认情况下，**failover exec** 命令模式是指定设备的全局配置模式。您可以使用 **failover exec** 命令发送适当的命令（如 **interface** 命令）来更改该命令模式。

更改指定设备的 **failover exec** 命令模式不会更改用于访问设备的会话的命令模式。例如，如果您登录到故障切换对的主用设备并且在全局配置模式下发出以下命令，您将保持在全局配置模式下，但使用 **failover exec** 命令发送的任何命令都将在接口配置模式下执行：

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(config)#
```

更改设备当前会话的命令模式不会影响 **failover exec** 命令使用的命令模式。例如，如果您处于主用设备上的接口配置模式，并且未更改 **failover exec** 命令模式，则以下命令将在全局配置模式下执行：

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

使用 **show failover exec** 命令可显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。

安全注意事项

failover exec 命令使用故障切换链路向对等设备发送命令以及接收对等设备命令执行的输出。您应该使用 **failover key** 命令加密故障切换链路以防止窃听或中间人攻击。

限制

- 如果使用零停机时间升级过程升级一个设备而不升级另一个设备，则两个设备都必须运行支持 **failover exec** 命令的软件，该命令才能工作。
- 命令完成和情景帮助不适用于 *cmd_string* 参数中的命令。
- 在多情景模式下，只能向对等设备上的对等情景发送命令。要向其他情景发送命令，必须先切换到您登录到的设备上的情景。
- 不能通过 **failover exec** 命令使用以下命令：
  - **changeto**
  - **debug** (**undebug**)
- 如果备用设备处于故障状态，只要故障是由服务卡故障产生的，则仍然可以收到来自 **failover exec** 命令的命令；否则，远程命令执行将失败。
- 不能使用 **failover exec** 命令在故障切换对等设备上从特权 EXEC 模式切换到全局配置模式。例如，如果当前设备处于特权 EXEC 模式，并且您输入 **failover exec mate configure terminal** 命令，则 **show failover exec mate** 命令输出将显示故障切换 exec 会话处于全局配置模式。但是，使用 **failover exec** 命令输入对等设备的配置命令将失败，直到您进入当前设备的全局配置模式。
- 不能输入递归 **failover exec** 命令，如 **failover exec mate failover exec mate** *命令*。
- 需要用户输入或确认的命令必须使用 **/nonconfirm** 选项。

示例

以下示例展示如何使用 **failover exec** 命令显示主用设备上的故障切换信息。执行命令的设备是主用设备，因此命令在本地执行。

```
ciscoasa(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
```

```
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
ciscoasa(config)#
```

以下示例使用 **failover exec** 命令显示对等设备的故障切换状态。命令在主要设备（主用设备）上执行，因此所显示的信息来自辅助设备（备用设备）。

```
ciscoasa(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
```

```
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

以下示例使用 **failover exec** 命令显示故障切换对等设备的故障切换配置。命令在主要设备（主用设备）上执行，因此所显示的信息来自辅助设备（备用设备）。

```
ciscoasa(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

以下示例使用 **failover exec** 命令从备用设备创建主用设备上的情景。该命令从主用设备复制回备用设备。注意两条“Creating context…”（正在创建情景 ...）消息。一条来自创建情景时对等设备的 **failover exec** 命令输出，另一条来自当复制命令本地创建情景时的本地设备。

```
ciscoasa(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

ciscoasa(config)# failover exec active context text

Creating context 'text'... Done.(2)
Creating context 'text'... Done.(3)

ciscoasa(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

以下示例展示使用 **failover exec** 命令向处于备用状态的故障切换对等设备发送配置命令时返回的警告：

```
ciscoasa# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

       **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
ciscoasa(config)#
```

以下示例使用 **failover exec** 命令向备用设备发送 **show interface** 命令：

```
ciscoasa(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

```
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

以下示例展示当向对等设备发出非法命令时返回的错误消息：

```
ciscoasa# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

以下示例展示在禁用故障切换的情况下使用 **failover exec** 命令时返回的错误消息：

```
ciscoasa(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

相关命令

命令	说明
debug fover	显示故障切换相关的调试消息。
debug xml	显示 **failover exec** 命令使用的 XML 解析器的调试消息。
show failover exec	显示 **failover exec** 命令模式。

failover group

要配置 Active/Active（主用 / 主用）故障切换组，请在全局配置模式下使用 **failover group** 命令。要删除故障切换组，请使用此命令的 **no** 形式。

failover group *num*

no failover group *num*

语法说明

num	故障切换组编号。有效值为 1 或 2。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

最多可以定义两个故障切换组。**failover group** 命令只能添加到为多情景模式配置的设备的系统情景中。仅当禁用故障切换时，才可以创建和删除故障切换组。

输入此命令会将您置于故障切换组命令模式。在故障切换组配置模式下可使用 **primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address** 和 **polltime interface** 命令。使用 **exit** 命令可返回全局配置模式。

注意　**failover polltime interface**、**failover interface-policy**、**failover replication http** 和 **failover mac address** 命令对 Active/Active（主用 / 主用）故障切换配置没有影响。它们被以下故障切换组配置模式命令覆盖：**polltime interface**、**interface-policy**、**replication http** 和 **mac address**。

当删除故障切换组时，必须最后删除故障切换组 1。故障切换组 1 始终包含管理情景。任何未分配到故障切换组的情景都默认分配到故障切换组 1。不能删除已显式分配了情景的故障切换组。

注意　如果您在同一网络中有不止一个主用 / 主用故障切换对，那么由于确定默认虚拟 MAC 地址的方法所致，很可能分配给某一对接口的默认虚拟 MAC 地址与分配给其他对接口的默认虚拟 MAC 地址相同。为避免网络上出现重复的 MAC 地址，请确保使用 **mac address** 命令为每个物理接口分配一个虚拟主用和备用 MAC 地址。

示例

以下部分示例显示两个故障切换组的可能配置：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

相关命令

命令	说明
asr-group	指定非对称路由接口组 ID。
interface-policy	指定当监控检测接口故障时的故障切换策略。
join-failover-group	为故障切换组分配情景。
mac address	为故障切换组中的情景定义虚拟 mac 地址。
polltime interface	指定发送到受监控接口的问候消息的时间间隔。
preempt	指定具有更高优先级的设备在重新启动后成为主用设备。
primary	为故障切换组的主要设备给予更高优先级。
replication http	为所选故障切换组指定 HTTP 会话复制。
secondary	为故障切换组的辅助设备给予更高优先级。

failover interface ip

要指定故障切换接口和状态故障切换接口的 IPv4 地址和掩码或 IPv6 地址和前缀，请在全局配置模式下使用 **failover interface ip** 命令。要删除该 IP 地址，请使用此命令的 **no** 形式。

failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

语法说明

if_name	故障切换或状态故障切换接口的接口名称。
ip_address mask	指定主要设备上的故障切换或状态故障切换接口的 IP 地址和掩码。
ipv6_address	指定主要设备上的故障切换或状态故障切换接口的 IPv6 地址。
prefix	指示地址的多少个高位连续位构成 IPv6 前缀（IPv6 地址的网络部分）。
standby *ip_address*	指定与主要设备通信的辅助设备所使用的 IP 地址。
standby*ipv6_address*	指定与主要设备通信的辅助设备所使用的 IPv6 地址。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(2)	为此命令增加了 IPv6 地址支持。

使用指南

备用地址必须与主要地址在同一子网中。

在配置中只能有一个 **failvover interface ip** 命令。因此，故障切换接口可以有一个 IPv6 或 IPv4 地址；不能同时为接口分配 IPv6 和 IPv4 地址。

故障切换和状态故障切换接口是第 3 层的功能（即使 ASA 在透明防火墙模式下工作时），并且对于系统是全局性的。

在多情景模式下，在系统情景中配置故障切换（**monitor-interface** 命令除外）。

当引导 ASA 进行 LAN 故障切换时，此命令必须是配置的一部分。

示例

以下示例展示如何为故障切换接口指定 IPv4 地址和掩码：

```
ciscoasa(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

以下示例展示如何为故障切换接口指定 IPv6 地址和前缀：

```
ciscoasa(config)# failover interface ip lanlink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

相关命令

命令	说明
clear configure failover	从运行配置中清除 **failover** 命令并恢复故障切换默认值。
failover lan interface	指定用于故障切换通信的接口。
failover link	指定用于状态故障切换的接口。
monitor-interface	监控指定接口的运行状况。
show running-config failover	显示运行配置中的 **failover** 命令。

failover interface-policy

要指定当监控检测接口故障时的故障切换策略，请在全局配置模式下使用 **failover interface-policy** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

语法说明

num	用作百分比时，指定一个介于 1 至 100 之间的数字；用作数字时，指定最大接口数为 1。
%	（可选）指定数字 *num* 为受监控接口的百分比。

默认值

默认值如下：

- *num* 为 1。
- 默认情况下启用物理接口监控，禁用逻辑接口监控。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

num 参数和可选 **%** 关键字之间没有空格。

如果故障接口数满足已配置的策略，并且另一个 ASA 工作正常，则 ASA 会将自身标记为故障，并可能进行故障切换（如果主用 ASA 发生故障）。只有由 **monitor-interface** 命令指定为监控的接口才能计入该策略。

注意　此命令仅适用于 Active/Standby（主用 / 备用）故障切换。在 Active/Active（主用 / 主用）故障切换中，在故障切换组配置模式下使用 **interface-policy** 命令为每个故障切换组配置接口策略。

示例

以下示例展示两种指定故障切换策略的方式：

```
ciscoasa(config)# failover interface-policy 20%

ciscoasa(config)# failover interface-policy 5
```

相关命令

命令	说明
failover polltime	指定设备和接口轮询时间。
failover reset	将故障设备恢复为无故障状态。
monitor-interface	指定用作故障切换的监控接口。
show failover	显示有关设备的故障切换状态的信息。

failover ipsec pre-shared-key

要在设备间的故障切换和状态链路上建立 IPsec LAN 到 LAN 隧道以加密所有故障切换通信，请在全局配置模式下使用 **failover ipsec pre-shared-key** 命令。要删除密钥，请使用此命令的 **no** 形式。

failover ipsec pre-shared-key *key*

no failover ipsec pre-shared-key

语法说明

0	指定未加密的密码。此为默认值。
8	指定加密的密码。如果使用主口令（请参阅 **password encryption aes** 和 **key config-key password-encryption** 命令），则在配置中加密密钥。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。 **注**　**failover ipsec pre-shared-key** 在 **show running-config** 输出中显示为 **** ；这种遮掩密钥无法复制。
key	在两个设备上均指定的*密钥*，被 IKEv2 用来建立隧道，最长为 128 个字符。

命令默认值

0（未加密）为默认值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.1(2)	我们引入了此命令。

使用指南

除非加密故障切换通信，否则通过故障切换和状态故障切换链路发送的所有信息均以明文发送。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果使用 ASA 端接 VPN 通道，建议加密故障切换通信。

建议在传统 **failover key** 方法的基础上使用 **failover ipsec pre-shared-key** 方法加密。

不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。但是，如果使用主口令（请参阅 **password encryption aes** 和 **key config-key password-encryption** 命令），必须先使用 **no failover key** 命令删除故障切换密钥，然后再配置 IPsec 加密。

注意　故障切换 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。

示例

以下示例配置 IPsec 预共享密钥：

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

相关命令

命令	说明
show running-config failover	显示运行配置中的故障切换命令。
show vpn-sessiondb	显示有关 VPN 隧道的信息，包括故障切换 IPsec 隧道。

failover key

要指定故障切换对中的设备间的加密和经过身份验证的通信（在故障切换和状态链路上）的密钥，请在全局配置模式下使用 **failover key** 命令。要删除密钥，请使用此命令的 **no** 形式。

failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

no failover key

语法说明

0	指定未加密的密码。此为默认值。
8	指定加密的密码。如果使用主口令（请参阅 **password encryption aes** 和 **key config-key password-encryption** 命令），则在配置中加密共享密钥。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密共享密钥。 **注**　**failover key** 在 **show running-config** 输出中显示为 **** ；这种遮掩密钥无法复制。
hex *key*	为加密密钥指定十六进制值。密钥必须是 32 个十六进制字符（0-9、a-f）。
shared_secret	指定字母数字共享密钥。密钥长度可以介于 1 到 63 个字符之间。有效字符是数字、字母或标点符号的任意组合。共享密钥用于生成加密密钥。

默认值

0（未加密）为默认值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **failover lan key** 修改为 **failover key**。
7.0(4)	此命令修改为包括 **hex** *key* 关键字和参数。
8.3(1)	此命令修改为支持具有 **0** 和 **8** 关键字的主口令。

使用指南

除非加密故障切换通信，否则通过故障切换和状态故障切换链路发送的所有信息均以明文发送。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果使用 ASA 端接 VPN 通道，建议加密故障切换通信。

建议在传统 **failover key** 方法的基础上使用 **failover ipsec pre-shared-key** 方法加密。

不能同时使用 IPsec 加密（**failover ipsec pre-shared-key** 命令）和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。但是，如果使用主口令（请参阅 **password encryption aes** 和 **key config-key password-encryption** 命令），必须先使用 **no failover key** 命令删除故障切换密钥，然后再配置 IPsec 加密。

示例

以下示例展示如何指定共享密钥来加密故障切换对中的设备间的故障切换通信：

```
ciscoasa(config)# failover key abcdefg
```

以下示例展示如何指定十六进制密钥来加密故障切换对中两个设备间的故障切换通信：

```
ciscoasa(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

以下示例展示从 **more system:running-config** 输出复制并粘贴的加密密码：

```
ciscoasa(config)# failover key 8 TPZCVNgdegLhWMa
```

相关命令

命令	说明
show running-config failover	显示运行配置中的故障切换命令。

failover lan interface

要指定用于故障切换通信的接口，请在全局配置模式下使用 **failover lan interface** 命令。要删除故障切换接口，请使用此命令的 **no** 形式。

failover lan interface *if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}]

语法说明

if_name	指定专用于故障切换的 ASA 接口的名称。
phy_if	指定物理接口。
sub_if	（可选）指定子接口号。
vlan_if	在 ASA 5505 上用于指定 VLAN 接口作为故障切换链路。

默认值

未配置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为包括 *phy_if* 参数。
7.2(1)	此命令修改为包括 *vlan_if* 参数。

使用指南

LAN 故障切换需要专用接口来传递故障切换流量。不过，也可以将 LAN 故障切换接口用于 Stateful Failover（状态故障切换）链路。

注意　如果为 LAN 故障切换和 Stateful Failover（状态故障切换）使用同一接口，则该接口需要足够的处理能力才能同时处理基于 LAN 的故障切换和 Stateful Failover（状态故障切换）流量。

可以将设备上的任意未使用的以太网接口用作故障切换接口。无法指定当前已配置名称的接口。故障切换接口不配置为常规网络接口；它仅为故障切换通信而存在。此接口只应该用于故障切换链路（或用于状态链路）。连接基于 LAN 的故障切换链路的方式可以是：使用专用交换机且链路上没有主机或路由器，或使用交叉以太网电缆直接连接设备。

注意　在使用 VLAN 时，将专用 VLAN 用于故障切换链路。与任何其他 VLAN 共享故障切换链路 VLAN 都可能导致间歇性流量问题以及 ping 和 ARP 故障。如果使用交换机连接故障切换链路，请使用交换机和 ASA 上的专用于故障切换链路的接口；请勿将该接口与承载常规网络流量的子接口共用。

在多情景模式下运行的系统上，故障切换链路位于系统情景中。此接口和状态链路（如果使用的话）是仅有的可以在系统情景中配置的接口。所有其他接口均分配到安全情景内部并从其中配置。

注意　在发生故障切换时，故障切换链路的 IP 地址和 MAC 地址不会更改。

此命令的 **no** 形式也会清除故障切换接口 IP 地址配置。

当引导 ASA 进行 LAN 故障切换时，此命令必须是配置的一部分。

注意事项　通过故障切换和状态故障切换链路发送的所有信息均以明文发送，除非您使用故障切换密钥加密通信。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果要使用 ASA 端接 VPN 隧道，建议通过故障切换密钥来加密故障切换通信。

示例

以下示例使用 ASA 5500 系列（ASA 5505 除外）上的子接口配置故障切换 LAN 接口：

```
ciscoasa(config)# failover lan interface folink GigabitEthernet0/3.1
```

以下示例在 ASA 5505 上配置故障切换 LAN 接口：

```
ciscoasa(config)# failover lan interface folink Vlan6
```

相关命令

命令	说明
failover lan unit	指定基于 LAN 的故障切换主要或辅助设备。
failover link	指定 Stateful Failover（状态故障切换）接口。

failover lan unit

要将 ASA 配置为 LAN 故障切换配置中的主要或辅助设备，请在全局配置模式下使用 **failover lan unit** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

语法说明

primary	指定 ASA 为主要设备。
secondary	指定 ASA 为辅助设备。

默认值

辅助。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

对于 Active/Standby（主用 / 备用）故障切换，故障切换设备的主要和辅助标识是指哪个设备在引导时成为主用设备。在以下情况下，主要设备在引导时成为主用设备：

- 主要和辅助设备均在第一个故障切换轮询检查过程内完成其引导序列。
- 主要设备先于辅助设备引导。

如果辅助设备在主要设备引导时已经是主用设备，则主要设备不会获取控制权；它将成为备用设备。在这种情况下，您需要在辅助（主用）设备上输入 **no failover active** 命令以强制主要设备恢复主用状态。

对于 Active/Active（主用 / 主用）故障切换，每个故障切换组均被分配一个主要或辅助设备首选项。此首选项确定当故障切换对中的两个设备同时启动时（在故障切换轮询时间段内），故障切换组中的情景在哪个设备上启动时变为活动状态。

当引导 ASA 进行 LAN 故障切换时，此命令必须是配置的一部分。

示例

以下示例将 ASA 设置为基于 LAN 的故障切换中的主要设备：

```
ciscoasa(config)# failover lan unit primary
```

相关命令

命令	说明
failover lan interface	指定用于故障切换通信的接口。

failover link

要指定 Stateful Failover（状态故障切换）接口，请在全局配置模式下使用 **failover link** 命令。要删除 Stateful Failover（状态故障切换）接口，请使用此命令的 **no** 形式。

failover link *if_name* [*phy_if*]

no failover link

语法说明

if_name	指定专用于 Stateful Failover（状态故障切换）的 ASA 接口的名称。
phy_if	（可选）指定物理或逻辑接口端口。如果 Stateful Failover（状态故障切换）接口与分配到故障切换通信的接口共用，或者共用标准防火墙接口，则不需要此参数。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为包括 *phy_if* 参数。
7.0(4)	此命令修改为接受标准防火墙接口。

使用指南

此命令在不支持 Stateful Failover（状态故障切换）的 ASA 5505 上不可用。

当没有共用故障切换通信或标准防火墙接口时，需要物理或逻辑接口参数。

failover link 命令用于启用 Stateful Failover（状态故障切换）。输入 **no failover link** 命令可禁用 Stateful Failover（状态故障切换）。如果使用专用的 Stateful Failover（状态故障切换）接口，则 **no failover link** 命令也会清除 Stateful Failover（状态故障切换）接口 IP 地址配置。

要使用 Stateful Failover（状态故障切换），必须配置 Stateful Failover（状态故障切换）链路以传递所有状态信息。有三种方式配置 Stateful Failover（状态故障切换）链路：

- 可以使用专用于 Stateful Failover（状态故障切换）链路的以太网接口。
- 如果要使用基于 LAN 的故障切换，则可以共用故障切换链路。
- 可以共用常规数据接口，如内部接口。但是，不推荐使用此选项。

如果使用专用于 Stateful Failover（状态故障切换）链路的以太网接口，则可以使用交换机或交叉电缆直接连接设备。如果使用交换机，则此链路上不应有任何其他主机或路由器。

注意　在直接连接到 ASA 的思科交换机端口上启用 PortFast 选项。

如果使用故障切换链路作为 Stateful Failover（状态故障切换）链路，则应该使用可用的最快以太网接口。如果在该接口上遇到性能问题，请考虑将一个独立接口专用于 Stateful Failover（状态故障切换）接口。

如果使用数据接口作为 Stateful Failover（状态故障切换）链路，则在您指定该接口作为 Stateful Failover（状态故障切换）链路时，会收到以下警告：

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

与 Stateful Failover（状态故障切换）接口共用数据接口可能使您容易遭受重播攻击。此外，接口上可能会发送大量状态故障切换流量，导致该网段出现性能问题。

注意　只有在单情景路由模式下支持将数据接口用作状态故障切换接口。

在多情景模式下，状态故障切换链路位于系统情景中。此接口和故障切换接口是系统情景中仅有的接口。所有其他接口均分配到安全情景内部并从其中配置。

注意　除非状态故障切换链路配置在常规数据接口上，否则状态故障切换链路的 IP 地址和 MAC 地址不会在故障切换时更改。

注意事项　通过故障切换和状态故障切换链路发送的所有信息均以明文发送，除非您使用故障切换密钥加密通信。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果要使用 ASA 端接 VPN 隧道，建议通过故障切换密钥来加密故障切换通信。

示例

以下示例展示如何指定专用接口作为状态故障切换接口。示例中的接口没有现有配置。

```
ciscoasa(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

相关命令

命令	说明
failover interface ip	配置 **failover** 命令和状态故障切换接口的 IP 地址。
failover lan interface	指定用于故障切换通信的接口。

failover mac address

要指定物理接口的故障切换虚拟 MAC 地址，请在全局配置模式下使用 **failover mac address** 命令。要删除虚拟 MAC 地址，请使用此命令的 **no** 形式。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

语法说明

active_mac	分配到主用 ASA 的指定接口的 MAC 地址。必须以 h.h.h 格式输入 MAC 地址，其中 h 是一个 16 位的十六进制数字。
phy_if	将设置 MAC 地址的接口的物理名称。
standby_mac	分配到备用 ASA 的指定接口的 MAC 地址。必须以 h.h.h 格式输入 MAC 地址，其中 h 是一个 16 位的十六进制数字。

默认值

未配置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

failover mac address 命令可让您配置 Active/Standby（主用 / 备用）故障切换对的虚拟 MAC 地址。如果未定义虚拟 MAC 地址，则各个故障切换设备启动时会将固化的 MAC 地址用于其接口，并与其故障切换对等设备交换这些地址。主要设备上的接口的 MAC 地址用于主用设备上的接口。

但是，如果两个设备同时不在线，并且辅助设备先启动且成为主用设备，它会将固化的 MAC 地址用于自己的接口。当主要设备上线时，辅助设备将从主要设备获取 MAC 地址。此更改可能中断网络流量。配置接口的虚拟 MAC 地址可确保辅助设备在成为主用设备时使用正确的 MAC 地址，即使它在主要设备之前上线也是如此。

在为基于 LAN 的故障切换配置的接口上，**failover mac address** 命令是不必要的（因此也不能使用），因为在故障切换时，**failover lan interface** 命令不会更改 IP 和 MAC 地址。当 ASA 配置 Active/Active（主用 / 主用）故障切换时，此命令没有影响。

当向配置添加 **failover mac address** 命令时，最好配置虚拟 MAC 地址，将配置保存到闪存，然后重新加载故障切换对。如果在存在活动连接时添加虚拟 MAC 地址，则这些连接将停止。此外，还必须将完整配置（包括 **failover mac address** 命令）写入辅助 ASA 的闪存才能使虚拟 MAC 地址生效。

如果在主要设备的配置中指定 **failover mac address**，则也应在辅助设备的引导程序配置中指定此命令。

注意　此命令仅适用于 Active/Standby（主用 / 备用）故障切换。在 Active/Active（主用 / 主用）故障切换中，在故障切换组配置模式下使用 **mac address** 命令为故障切换组中的每个接口配置虚拟 MAC 地址。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，那么使用的 MAC 地址会取决于许多变量，因而可能成为不可预测的。

示例

以下示例为名为 intf2 的接口配置主用和备用 MAC 地址：

```
ciscoasa(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

相关命令

命令	说明
show interface	显示接口状态、配置和统计信息。

failover polltime

要指定故障切换设备轮询和保持时间，请在全局配置模式下使用 **failover polltime** 命令。要恢复默认轮询和保持时间，请使用此命令的 **no** 形式。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

语法说明

holdtime *time*	（可选）设置设备在故障切换链路上必须收到问候消息的时间，在此时间过后，对等设备将被声明为故障。 有效值介于 3 至 45 秒之间或 800 至 999 毫秒之间（如果使用可选的 **msec** 关键字）。
msec	（可选）指定给定的时间以毫秒为单位。
poll_time	设置问候消息之间的时间量。 有效值介于 1 至 15 秒之间或 200 至 999 毫秒之间（如果使用可选的 **msec** 关键字）。
unit	（可选）指示命令用于设备轮询和保持时间。 向命令添加此关键字不会对命令有任何影响，但可以使此命令在配置中更容易与 **failover polltime interface** 命令区分开。

默认值

ASA 上的默认值如下：

- *poll_time* 为 1 秒。
- **holdtime** *time* 为 15 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **failover poll** 命令更改为 **failover polltime** 命令，并且现在包括 **unit** 和 **holdtime** 关键字。
7.2(1)	向 **holdtime** 关键字添加了 **msec** 关键字。**polltime** 最小值从 500 毫秒减至 200 毫秒。**holdtime** 最小值从 3 秒减至 800 毫秒。

使用指南

输入的 **holdtime** 值不能小于设备轮询时间的三倍。轮询时间越短，ASA 便可以更快地检测故障并触发故障切换。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

如果设备在一个轮询周期内没有在故障切换通信接口或电缆上收听到问候消息，则通过其余接口进行额外测试。如果在保持时间内仍没有来自对等设备的响应，该设备将被视为出故障；如果故障设备为主用设备，备用设备将接管主用设备。

您可以将 **failover polltime** [**unit**] 和 **failover polltime interface** 命令都包含在配置中。

注意　当 CTIQBE 流量通过故障切换配置中的 ASA 时，应该将 ASA 上的故障切换保持时间减至低于 30 秒。CTIQBE 保持连接超时为 30 秒，而且可能会在故障切换发生在故障切换情况中前超时。如果 CTIQBE 超时，则会丢弃 Cisco IP SoftPhone 到 Cisco CallManager 的连接，IP SoftPhone 客户端需要重新向 CallManager 注册。

示例

以下示例将设备轮询时间频率更改为 3 秒：

```
ciscoasa(config)# failover polltime 3
```

以下示例将 ASA 配置为每 200 毫秒发送一次问候数据包，并且如果在 800 毫秒内未在故障切换接口上收到问候数据包，则认为设备故障。可选 **unit** 关键字包含在命令中。

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

相关命令

命令	说明
failover polltime interface	为主用 / 备用故障切换配置指定接口轮询和保持时间。
polltime interface	指定 Active/Active（主用 / 主用）故障切换配置的接口轮询和保持时间。
show failover	显示故障切换配置信息。

failover polltime interface

要指定 Active/Standby（主用 / 备用）故障切换配置中的数据接口轮询和保持时间，请在全局配置模式下使用 **failover polltime** interface 命令。要恢复默认轮询和保持时间，请使用此命令的 **no** 形式。

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

语法说明

holdtime *time*	（可选）设置数据接口必须收到问候消息的时间，在该时间后，对等设备被声明发生故障。有效值为从 5 到 75 秒。
interface *time*	指定接口监控的轮询时间。有效值范围为 1 到 15 秒。如果使用可选 **msec** 关键字，则有效值为 500 到 999 毫秒。
msec	（可选）指定给定的时间以毫秒为单位。

默认值

默认值如下所示：

- poll *time* 为 5 秒。
- **holdtime** *time* 是 poll *time* 的 5 倍。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **failover poll** 命令更改为 **failover polltime** 命令，并且包括 **unit**、**interface** 和 **holdtime** 关键字。
7.2(1)	增加了可选的 **holdtime** *time* 以及指定轮询时间（以毫秒为单位）的能力。

使用指南

使用 **failover polltime interface** 命令可更改在数据接口发出问候数据包的频率。此命令仅适用于 Active/Standby（主用 / 备用）故障切换。对于 Active/Active（主用 / 主用）故障切换，请在故障切换组配置模式下使用 **polltime interface** 命令而不是 **failover polltime interface** 命令。

输入的 **holdtime** 值不能小于设备轮询时间的五倍。轮询时间越短，ASA 便可以更快地检测故障并触发故障切换。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。在超过一半的保持时间内未听到 hello 数据包时，会开始接口测试。

您可以在配置中包括 **failover polltime unit** 和 **failover polltime interface** 命令。

注意　当 CTIQBE 流量通过故障切换配置中的 ASA 时，应该将 ASA 上的故障切换保持时间减至低于 30 秒。CTIQBE 保持连接超时为 30 秒，而且可能会在故障切换发生在故障切换情况中前超时。如果 CTIQBE 超时，则会丢弃 Cisco IP SoftPhone 到 Cisco CallManager 的连接，IP SoftPhone 客户端需要重新向 CallManager 注册。

示例

以下示例将接口轮询时间频率设置为 15 秒：

```
ciscoasa(config)# failover polltime interface 15
```

以下示例将接口轮询时间频率设置为 500 毫秒，将保持时间设置为 5 秒：

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

相关命令

命令	说明
failover polltime	指定设备故障切换轮询和保持时间。
polltime interface	指定 Active/Active（主用 / 主用）故障切换配置的接口轮询时间。
show failover	显示故障切换配置信息。

failover reload-standby

要强制备用设备重新启动，请在特权 EXEC 模式下使用 **failover reload-standby** 命令。

failover reload-standby

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当故障切换设备不同步时，请使用此命令。备用设备会重新启动并在完成启动后与主用设备重新同步。

示例

以下示例展示如何在主用设备上使用 **failover reload-standby** 命令强制备用设备重新启动：

```
ciscoasa# failover reload-standby
```

相关命令

命令	说明
write standby	将运行配置写入备用设备的内存。

failover replication http

要启用 HTTP（端口 80）连接复制，请在全局配置模式下使用 **failover replication http** 命令。要禁用 HTTP 连接复制，请使用此命令的 **no** 形式。

failover replication http

no failover replication http

语法说明

此命令没有任何参数或关键字。

默认值

已禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令从 **failover replication http** 更改为 **failover replication http**。

使用指南

默认情况下，ASA 启用状态化故障切换时就不会复制的 HTTP 会话信息。因为 HTTP 会话通常短暂的且由于 HTTP 客户端通常重试失败的连接尝试，无法进行复制 HTTP 会话提高系统性能，而不会造成严重的数据或失去连接。**failover replication http** 命令可在状态故障切换环境下启用 HTTP 会话的状态复制，但可能对系统性能有负面影响。

在 Active/Active（主用 / 主用）故障切换配置中，在故障切换组配置模式下使用 **replication http** 命令控制每个故障切换组的 HTTP 会话复制。

示例

以下示例展示如何启用 HTTP 连接复制：

```
ciscoasa(config)# failover replication http
```

相关命令

命令	说明
replication http	启用特定故障切换组的 HTTP 会话复制。
show running-config failover	显示运行配置中的 **failover** 命令。

failover replication rate

要配置批量同步连接复制速率，请在全局配置模式下使用 **failover replication rate** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

failover replication rate *rate*

no failover replication rate

语法说明

rate	设置每秒连接数。值和默认设置取决于您的型号的每秒最大连接数。

命令默认值

根据您的型号而有所不同。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.4(4.1)/8.5(1.7)	我们引入了此命令。

使用指南

您可以配置 ASA 在使用状态故障切换时将连接复制到备用设备的速率。默认情况下，连接在 15 秒内复制到备用设备。但是，当执行批量同步时（例如，首次启用故障切换时），由于每秒最大连接数的限制，15 秒可能不足以同步大量连接。例如，ASASM 的最大连接数为 8 百万；在 15 秒内复制 8 百万个连接意味着每秒创建 533 K 个连接。但是，每秒的最大连接数是 300 K。您现在可以指定复制速率小于或等于每秒最大连接数，同步期间将会调整，直到所有连接均同步为止。

示例

以下示例将故障切换复制速率设置为每秒 20000 个连接：

```
ciscoasa(config)# failover replication rate 20000
```

相关命令

命令	说明
failover rate http	启用 HTTP 连接复制。

failover reset

要将出现故障的 ASA 恢复为无故障状态，请在特权 EXEC 模式下使用 **failover reset** 命令。

failover reset [**group** *group_id*]

语法说明

group	（可选）指定故障切换组。**group** 关键字仅适用于 Active/Active（主用 / 主用）故障切换。
group_id	故障切换组编号。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为添加可选故障切换组 ID。

使用指南

failover reset 命令允许您将故障设备或组切换为无故障状态。**failover reset** 命令可在任一设备上输入，但我们建议您始终在主用设备上输入该命令。在主用设备输入 **failover reset** 命令将使备用设备 “ 无故障 ”。

可以使用 **show failover** 或 **show failover state** 命令显示设备的故障切换状态。

此命令没有 **no** 形式。

在 Active/Active（主用 / 主用）故障切换中，输入 **failover reset** 将重置整个设备。使用该命令指定故障切换组仅会重置指定的组。

示例

以下示例展示将故障设备切换为无故障状态：

```
ciscoasa# failover reset
```

相关命令

命令	说明
failover interface-policy	指定当监控检测接口故障时的故障切换策略。
show failover	显示设备的故障切换状态的信息。

failover standby config-lock

要锁定故障切换对中的备用设备或备用情景的配置更改，请在全局配置模式下使用 **failover standby config-lock** 命令。要允许备用设备上的配置，请使用此命令的 **no** 形式。

failover standby config-lock

no failover standby config-lock

语法说明

此命令没有任何参数或关键字。

命令默认值

默认情况下，允许备用设备 / 情景上的配置，但会显示一条警告消息。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.3(2)	我们引入了此命令。

使用指南

您可以锁定备用设备（主用 / 备用故障切换）或备用情景（主用 / 主用故障切换）上的配置更改，这样无法在常规配置同步之外的备用设备上进行更改。

示例

以下示例禁止备用设备上的配置：

```
ciscoasa(config)# failover standby config-lock
```

相关命令

命令	说明
clear configure failover	从运行配置中清除 **failover** 命令并恢复故障切换默认值。
failover active	将备用设备切换到主用状态。
show failover	显示设备的故障切换状态的信息。
show running-config failover	显示运行配置中的 **failover** 命令。

failover timeout

要指定不对称路由会话的故障切换重新连接超时值，请在全局配置模式下使用 **failover timeout** 命令。要恢复默认超时值，请使用此命令的 **no** 形式。

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

语法说明

hh	指定超时值中的小时数。有效值范围为 -1 到 1193。默认情况下，此值设置为 0。 将该值设置为 -1 将禁用超时，从而允许连接在任意时间量后重新连接。 将此值设置为 0 而不指定任何其他超时值，会将命令设置回默认值，这可防止连接重新连接。输入 **no failover timeout** 命令也会将此值设置为默认值 (0)。 **注**　设置为默认值时，此命令不会出现在运行配置中。
mm	（可选）指定超时值中的分钟数。有效值范围为 0 到 59。默认情况下，此值设置为 0。
ss	（可选）指定超时值中的秒数。有效值范围为 0 到 59。默认情况下，此值设置为 0。

默认值

默认情况下，*hh*、*mm* 和 *ss* 为 0，这可防止连接重新连接。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令修改为出现在命令列表中。

使用指南

此命令与带 **nailed** 选项的 **static** 命令一起使用。**nailed** 选项允许在启动后或系统变为活动状态后在指定的时间量内重新建立连接。**failover timeout** 命令用于指定该时间量。如果不配置，连接无法重新建立。**failover timeout** 命令不会影响 **asr-group** 组命令。

注意　向 **static** 命令添加 **nailed** 选项会导致连接跳过 TCP 状态跟踪和顺序检查。

输入此命令的 **no** 形式可恢复默认值。输入 **failover timeout 0** 也会恢复默认值。设置为默认值时，此命令不会出现在运行配置中。

示例

以下示例将备用组 1 切换到主用状态：

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(config)# show running-config failover
no failover
failover timeout 12:30:00
```

相关命令

命令	说明
static	通过将本地 IP 地址映射到全局 IP 地址来配置永久性一对一地址转换规则。

fallback

要配置 Cisco Intercompany Media Engine 用来在连接完整性降低时从 VoIP 回退到 PSTN 的回退计时器，请在 uc-ime 配置模式下使用 **fallback** 命令。要删除回退设置，请使用此命令的 **no** 形式。

fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

no fallback fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

语法说明

filename	指定敏感文件的文件名。输入包括 .fbs 文件扩展名的磁盘文件名。要指定文件名，可以包括本地磁盘上的路径，例如 `disk0:/file001.fbs`。
hold-down timer	设置 ASA 在通知 Cisco UCM 是否回退到 PSTN 前等待的时间量。
monitoring timer	设置 ASA 对从互联网接收的 RTP 数据包进行采样的间隔。ASA 使用数据采样来确定呼叫是否需要回退到 PSTN。
sensitivity-file	指定要用于呼叫中 PSTN 回退的文件。敏感文件由 ASA 解析并输入到 RMA 库中。
timer_millisec	指定监控计时器的长度（以毫秒为单位）。输入一个在 10-600 范围内的整数。默认情况下，监控计时器的长度为 100 毫秒。
timer_sec	指定抑制计时器的长度（以秒为单位）。输入一个在 10-360 范围内的整数。默认情况下，抑制计时器的长度为 20 秒。

默认值

默认情况下，监控计时器的长度为 100 毫秒。

默认情况下，抑制计时器的长度为 20 秒。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Uc-ime 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

指定 Cisco Intercompany Media Engine 的回退计时器。

互联网连接的质量可能变化很大且随时间变化。因此，即使由于连接质量良好而通过 VoIP 发出呼叫，连接质量也可能在呼叫中变差。为确保最终用户的整体体验良好，Cisco Intercompany Media Engine 会尝试执行呼叫中回退。

执行呼叫中回退需要 ASA 监控来自互联网的 RTP 数据包，并将信息发送到 RTP 监控算法 (RMA) API，该 API 将向 ASA 发出指示是否需要回退。如果需要回退，ASA 会向 Cisco UCM 发送 REFER 消息，告知其需要将呼叫回退到 PSTN。

注意　当为 SIP 检查启用 Cisco Intercompany Media Engine 代理时，无法更改回退计时器。先从 SIP 检查中删除 Cisco Intercompany Media Engine 代理，再更改回退计时器。

示例

以下示例展示如何在指定回退计时器时配置 Cisco Intercompany Media Engine：

```
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
```

以下示例展示在指定敏感文件时配置 Cisco Intercompany Media Engine：

```
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 sensitivity-file local_uc-ime_fallback_policy
```

相关命令

命令	说明
show running-config uc-ime	显示思科公司间媒体引擎代理的正在运行的配置。
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信息或详细信息。
uc-ime	在 ASA 上创建思科公司间媒体引擎代理实例。

第 16 章

file-bookmarks 至 functions 命令

file-bookmarks

要定制 WebVPN 主页上向已通过身份验证的 WebVPN 用户显示的文件书签标题或文件书签链接，请在 webvpn 定制配置模式下使用 **file-bookmarks** 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。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

语法说明

link	指定对链接的更改。
title	指定对标题的更改。
style	指定对 HTML 样式的更改。
text	指定对文本的更改。
value	要显示的实际文本或 CSS 参数（最多为 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 “File Folder Bookmarks”。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Webvpn customization configuration	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的 CSS 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的详细信息，请参阅 W3C 网站（网址为 www.w3.org）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，取值范围为 0 到 255，分别表示每种颜色（红、绿、蓝）；以逗号分隔的条目用于指示彼此混合的每种颜色的强度级别。
- 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。

注意　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

以下示例将文件书签标题定制为 “Corporate File Bookmarks”：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

相关命令

命令	说明
application-access	定制 WebVPN 主页的 Application Access 框。
browse-networks	定制 WebVPN 主页的 Browse Networks 框。
web-applications	定制 WebVPN 主页的 Web Application 框。
web-bookmarks	定制 WebVPN 主页上的 Web Bookmarks 标题或链接。

file-browsing

要为文件服务器或共享启用或禁用 CIFS/FTP 文件浏览，请在 dap webvpn 配置模式下使用 **file-browsing** 命令。

file-browsing enable | disable

语法说明

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

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

以下使用说明适用于文件浏览：

- 文件浏览不支持国际化。
- 浏览要求使用 NBNS（主浏览器或 WINS）。如果 NBNS 发生故障或未配置，则使用 DNS。

ASA 可应用来自各种来源的属性值。它根据以下层次结构应用这些属性值：

1. DAP 记录
2. 用户名
3. 组策略
4. 隧道组的组策略
5. 默认组策略

属性的 DAP 值的优先级高于为用户、组策略和隧道组配置的 DAP 值。

当您启用或禁用 DAP 记录的属性时，ASA 应用并实施该值。例如，当您在 dap webvpn 配置模式下禁用文件浏览时，ASA 不会继续查找值。如果您没有为 **file-browsing** 命令设置任何值，则在 DAP 记录中不存在属性，这样，ASA 下移到用户名的 AAA 属性，必要时下移到组策略，以查找要应用的值。

示例

以下示例展示如何为名为 Finance 的 DAP 记录启用文件浏览：

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# file-browsing enable
ciscoasa(config-dap-webvpn)#
```

相关命令

命令	说明
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。

file-encoding

要为来自通用互联网文件系统服务器的页面指定字符编码，请在 webvpn 配置模式下使用 **file-encoding** 命令。要删除文件编码属性的值，请使用此命令的 **no** 形式。

file-encoding {**server-name** | **server-ip-addr**} *charset*

no file-encoding {**server-name** | **server-ip-addr**}

语法说明

charset	字符串包含最多 40 个字符，并且其值与在 http://www.iana.org/assignments/character-sets 中标识的有效字符集之一相等。您可以使用在此页面上列出的字符集的名称或别名。示例包括 iso-8859-1、shift_jis 和 ibm850。 字符串不区分大小写。命令解释程序在 ASA 配置中将大写字母转换为小写字母。
server-ip-addr	您希望为其指定字符编码的 CIFS 服务器的 IP 地址，该地址采用点分十进制计数法。
server-name	您希望为其指定字符编码的 CIFS 服务器的名称。 ASA 保留您指定的大小写，不过，在将名称与服务器匹配时，它将忽略大小写。

默认值

来自 WebVPN 配置中没有显式文件编码条目的所有 CIFS 服务器的页面将继承字符编码属性的字符编码值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

为需要的字符编码条目值与 webvpn 字符编码属性值不同的所有 CIFS 服务器，输入字符编码条目。

从 CIFS 服务器下载并呈现给 WebVPN 用户的 WebVPN 门户页面对用来标识服务器的 WebVPN 文件编码属性的值进行编码，如果没有进行编码，则会继承字符编码属性的值。远程用户的浏览器将此值映射到其字符编码集的一个条目，以确定要使用的正确字符集。如果 WebVPN 配置没有为 CIFS 服务器指定文件编码条目，并且字符编码属性尚未设置，则 WebVPN 门户页面不会指定值。如果 WebVPN 门户页面未指定字符编码或指定了浏览器不支持的字符编码值，则远程浏览器使用自己的默认编码。

当文件名或目录路径以及页面无法正确呈现时，CIFS 服务器到适当字符编码的映射（在全局映射时使用 WebVPN 字符编码属性，在单独映射时使用文件编码覆盖）可正确处理和显示 CIFS 页面。

注意　字符编码值和文件编码值不排除浏览器将使用的字体系列。如果您正在使用日文 Shift_JIS 字符编码（如下例所示），您需要在 webvpn 定制命令模式下使用 **page style** 命令补充这些值的设置来替换字体系列，或在 webvpn 定制命令模式下输入 **no page style** 命令来删除该字体系列。

示例

以下示例设置名为 “CISCO-server-jp” 的 CIFS 服务器的文件编码属性以支持日文 Shift_JIS 字符、删除此字体系列，并保留默认背景颜色：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding CISCO-server-jp shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

以下示例设置 CIFS 服务器 10.86.5.174 的文件编码属性，以支持 IBM860（别名 “CP860”）字符：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(config-webvpn)
```

相关命令

命令	说明
character-encoding	指定在所有 WebVPN 门户页面（来自在 WebVPN 配置中的文件编码条目中指定的服务器的页面除外）中使用的全局字符编码。
show running-config webvpn	显示 WebVPN 的运行配置。使用 **all** 关键字以包括默认配置。
debug webvpn cifs	显示有关通用互联网文件系统的调试消息。

file-entry

要启用或禁用用户输入文件服务器名称来访问服务器的功能，请在 dap webvpn 配置模式下使用 **file-entry** 命令。

file-entry enable | disable

语法说明

enable | disable	启用或禁用输入要访问的文件服务器名称的功能。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

ASA 可根据以下层次结构应用来自各种来源的属性值。

1. DAP 记录
2. 用户名
3. 组策略
4. 连接配置文件（隧道组）的组策略
5. 默认组策略

属性的 DAP 值的优先级高于为用户、组策略或连接配置文件而配置的 DAP 值。

当您启用或禁用 DAP 记录的属性时，ASA 应用并实施该值。例如，当您在 dap webvpn 配置模式下禁用文件条目时，ASA 不会继续查找值。如果您没有为 **file-entry** 命令设置任何值，则 DAP 记录中不存在属性，这样，ASA 下移到用户名的 AAA 属性，必要时下移到组策略，以查找要应用的值。

示例

以下示例展示如何为名为 Finance 的 DAP 记录启用文件条目：

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

相关命令

命令	说明
dynamic-access-policy-record	创建 DAP 记录。
file-browsing	启用或禁用浏览文件服务器或共享的功能。

filter

要指定访问列表的名称以用于此组策略或用户名的 WebVPN 连接，请在 webvpn 配置模式下使用 **filter** 命令。要删除访问列表，请使用此命令的 **no** 形式。

filter {**value** *ACLname* | **none**}

no filter

语法说明

none	指示没有 WebVPN 类型访问列表。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 *ACLname*	提供先前配置的访问列表的名称。

默认值

WebVPN 访问列表不适用，直到您使用 **filter** 命令指定它们。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

no 选项允许继承其他组策略的值。为防止继承过滤器值，请使用 **filter value 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 **filter** 命令，为 WebVPN 流量应用这些 ACL。

WebVPN 不使用在 **vpn - filter** 命令中定义的 ACL。

示例

以下示例展示如何设置一个过滤器，为名为 FirstGroup 的组策略调用名为 *acl_in* 的访问列表：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# filter acl_in
```

相关命令

命令	说明
access-list	创建访问列表，或使用可下载访问列表。
webvpn	在组策略配置模式或用户名配置模式下使用。允许您进入 webvpn 配置模式，以配置应用于组策略或用户名的参数。

filter activex

要删除经过 ASA 的 HTTP 流量中的 ActiveX 对象，请在全局配置模式下使用 **filter activex** 命令。要删除配置，请使用此命令的 **no** 形式。

filter activex *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask*

no filter activex *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask*

语法说明

except	创建之前的过滤器条件的例外。
foreign_ip	要求访问的最低安全级别接口的 IP 地址。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
foreign_mask	*foreign_ip* 参数的网络掩码。始终指定特定掩码值。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
local_ip	发出访问请求的最高安全级别接口的 IP 地址。您可以将此地址设置为 0.0.0.0（或采用缩短形式 0）来指定所有主机。
mask	*local_ip* 参数的网络掩码。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
port	应用过滤的 TCP 端口。通常，这是端口 21，但也接受其他值。http 或 url 文字可用于端口 21。允许值的范围是 0 到 65535。
-port	（可选）指定端口范围。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ActiveX 对象可能导致安全风险，因为它们可能包含旨在攻击位于受保护网络上的主机和服务器的代码。您可以使用 **filter activex** 命令来禁用 ActiveX 对象。

ActiveX 控件（以前称为 OLE 或 OCX 控件）是您可以在网页或其他应用中插入的组件。这些控件包括定制表单、日历或其他用于搜集或显示信息的任何第三方表单。作为一项技术，ActiveX 为网络客户端制造了许多潜在问题，包括导致工作站故障、引入网络安全问题或被用来攻击服务器。

filter activex 命令通过在 HTML 网页中注释掉 HTML **object** 命令来阻止这些命令。通过有选择性地用注释来替换 <applet> 和 </applet> 以及 <object classid> 和 </object> 标记，执行 HTML 文件的 ActiveX 过滤。通过将顶级标记转换为注释来支持嵌套标记的过滤。

注意事项　<object> 标记还用于 Java 小应用、图像文件以及多媒体对象，此标记也将被此命令阻止。

如果 <object> 或者 </object> HTML 标记在网络数据包中分开，或者标记中包含的代码比 MTU 中的字节数长，则 ASA 无法阻止标记。

当用户访问 **alias** 命令所引用或者用于 WebVPN 流量的 IP 地址时，不会发生 ActiveX 阻止。

示例

以下示例指定在所有出站连接上阻止 ActiveX 对象：

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

此命令指定 ActiveX 对象阻止应用于端口 80 上来自任何本地主机和用于任何外部主机连接的网络流量。

相关命令

命令	说明
filter url	将流量引导至 URL 过滤服务器。
filter java	从流经 ASA 的 HTTP 流量删除 Java 小应用。
show running-config filter	显示过滤配置。
url-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
url-server	标识使用 **filter** 命令的 anN2H2 或 Websense 服务器。

filter ftp

要标识将由 Websense 或 N2H2 服务器过滤的 FTP 流量，请在全局配置模式下使用 **filter ftp** 命令。要删除配置，请使用此命令的 **no** 形式。

filter ftp *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]

no filter ftp *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]

语法说明

allow	（可选）当服务器不可用时，允许出站连接经过 ASA 而不过滤。如果省略此选项且 N2H2 或 Websense 服务器变为离线状态，则 ASA 停止出站端口 80 (Web) 流量，直到 N2H2 或者 Websense 服务器重新上线。
except	创建之前的过滤器条件的例外。
foreign_ip	访问所请求的最低安全级别的接口的 IP 地址。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
foreign_mask	*foreign_ip* 参数的网络掩码。始终指定特定掩码值。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
interact-block	（可选）阻止用户通过交互式 FTP 程序连接到 FTP 服务器。
local_ip	寻求访问的最高安全级别接口的 IP 地址。您可以将此地址设置为 0.0.0.0（或采用缩短形式 0）来指定所有主机。
mask	*local_ip* 参数的网络掩码。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
port	应用过滤的 TCP 端口。通常，这是端口 21，但也接受其他值。ftp 文字可用于端口 80。
-*port*	（可选）指定端口范围。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

filter ftp 命令可标识将由 N2H2 或 Websense 服务器过滤的 FTP 流量。

在启用此功能后，当用户向服务器发出 FTP GET 请求时，ASA 将请求发送给 FTP 服务器，同时将请求发给 Websense 或 N2H2 服务器。如果 Websense 或 N2H2 服务器允许连接，则 ASA 允许成功的 FTP 返回码未加更改地抵达用户。例如，“250: CWD command successful” 就是一个成功的返回码。

如果 Websense 或者 N2H2 服务器拒绝连接，则 ASA 更改 FTP 返回码以显示连接被拒绝。例如，ASA 将代码 250 修改为“550 Requested file is prohibited by URL filtering policy”。Websense 仅过滤 FTP GET 命令而不过滤 PUT 命令。

使用 **interactive-block** 选项来阻止不提供整个目录路径的交互式 FTP 会话。交互式 FTP 客户端允许用户更改目录，而无需键入整个路径。例如，用户可能会输入 **cd ./files** 而不是 **cd /public/files**。您必须在使用这些命令之前标识并启用 URL 过滤服务器。

示例

以下示例展示如何启用 FTP 过滤：

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter ftp 21 0 0 0 0
ciscoasa(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

相关命令

命令	说明
filter https	标识将由 Websense 或者 N2H2 服务器过滤的 HTTPS 流量。
filter java	从流经 ASA 的 HTTP 流量删除 Java 小应用。
filter url	将流量引导至 URL 过滤服务器。
show running-config filter	显示过滤配置。
url-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

filter https

要标识将由 N2H2 或 Websense 服务器过滤的 HTTPS 流量，请在全局配置模式下使用 **filter https** 命令。要删除配置，请使用此命令的 **no** 形式。

filter https *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**]

no filter https *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**]

语法说明

allow	（可选）当服务器不可用时，允许出站连接经过 ASA 而不过滤。如果省略此选项且 N2H2 或 Websense 服务器变为离线状态，则 ASA 停止出站端口 443 流量，直到 N2H2 或者 Websense 服务器重新上线。
except	（可选）创建之前的过滤器条件的例外。
foreign_ip	要求访问的最低安全级别接口的 IP 地址。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
foreign_mask	*foreign_ip* 参数的网络掩码。始终指定特定掩码值。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
local_ip	寻求访问的最高安全级别接口的 IP 地址。您可以将此地址设置为 0.0.0.0（或采用缩短形式 0）来指定所有主机。
mask	*local_ip* 参数的网络掩码。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
port	应用过滤的 TCP 端口。通常，这是端口 443，但也接受其他值。https 文字可用于端口 443。
-*port*	（可选）指定端口范围。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 支持使用外部 Websense 或 N2H2 服务器对 HTTPS 和 FTP 站点进行过滤。

HTTPS 过滤的工作原理是阻止不允许的站点完成 SSL 连接协商。浏览器显示一条错误消息，例如 “The Page or the content cannot be displayed”（页面或内容无法显示）。

由于 HTTPS 内容被加密，ASA 在没有目录和文件名信息的情况下发送 URL 查找。

示例

以下示例过滤所有出站 HTTPS 连接，但来自 10.0.2.54 主机的出站 HTTPS 连接除外。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

相关命令

命令	说明
filter activex	从流经 ASA 的 HTTP 流量中删除 ActiveX 对象。
filter java	从流经 ASA 的 HTTP 流量删除 Java 小应用。
filter url	将流量引导至 URL 过滤服务器。
show running-config filter	显示过滤配置。
url-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

filter java

要从流经 ASA 的 HTTP 流量中删除 Java 小应用，请在全局配置模式下使用 **filter java** 命令。要删除配置，请使用此命令的 **no** 形式。

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

语法说明

except	（可选）创建之前的过滤器条件的例外。
foreign_ip	访问所请求的最低安全级别的接口的 IP 地址。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
foreign_mask	*foreign_ip* 参数的网络掩码。始终指定特定掩码值。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
local_ip	发出访问请求的最高安全级别接口的 IP 地址。您可以将此地址设置为 0.0.0.0（或采用缩短形式 0）来指定所有主机。
local_mask	*local_ip* 参数的网络掩码。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
port	应用过滤的 TCP 端口。通常，这是端口 80，但也接受其他值。http 或 url 文字可用于端口 80。
*port***-***port*	（可选）指定端口范围。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

Java 小应用可能导致安全风险，因为它们可能包含旨在攻击位于受保护网络上的主机和服务器的代码。您可以使用 **filter java** 命令来删除 Java 小应用。

filter java 命令会过滤掉从出站连接返回到 ASA 的 Java 小应用。用户仍可接收 HTML 页面，但小应用的网页源会被注释掉，使得小应用无法执行。**filter java** 命令不过滤 WebVPN 流量。

如果 <applet> 或者 </applet> HTML 标记在网络数据包中分开，或者标记中包含的代码比 MTU 中的字节数长，则 ASA 无法阻止标记。如果已知 Java 小应用位于 <object> 标记中，则使用 **activex** 命令来删除它们。

示例

以下示例指定在所有出站连接上阻止 Java 小应用：

```
ciscoasa(config)# filter java 80 0 0 0 0
```

以下示例指定 Java 小应用阻止应用于端口 80 上来自任何本地主机和用于任何外部主机连接的网络流量。

以下示例阻止将 Java 小应用下载到位于受保护网络上的主机：

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

相关命令

命令	说明
filter activex	从流经 ASA 的 HTTP 流量中删除 ActiveX 对象。
filter url	将流量引导至 URL 过滤服务器。
show running-config filter	显示过滤配置。
url-server	标识与 **filter** 命令一起使用的 N2H2 或 Websense 服务器。

filter url

要将流量转到 URL 过滤服务器，请在全局配置模式下使用 **filter url** 命令。要删除配置，请使用此命令的 **no** 形式。

filter url *port* [**-***port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate | longurl-deny**] [**proxy-block**]

no filter url *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate | longurl-deny**] [**proxy-block**]

语法说明

allow	当服务器不可用时，允许出站连接流经 ASA 而不过滤。如果省略此选项且 N2H2 或 Websense 服务器变为离线状态，则 ASA 停止出站端口 80 (Web) 流量，直到 N2H2 或者 Websense 服务器重新上线。
cgi_truncate	如果 URL 有以问号 (?) 开头的参数列表，如 CGI 脚本，则通过删除问号之后的所有字符以及问号本身来截取发送给过滤服务器的 URL。
except	创建之前的**过滤器**条件的例外。
foreign_ip	要求访问的最低安全级别接口的 IP 地址。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
foreign_mask	*foreign_ip* 参数的网络掩码。始终指定特定掩码值。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
http	指定端口 80。您可以输入 http 或 www（而不是 80）来指定端口 80。
local_ip	寻求访问的最高安全级别接口的 IP 地址。您可以将此地址设置为 0.0.0.0（或采用缩短形式 0）来指定所有主机。
local_mask	*local_ip* 参数的网络掩码。您可以使用 0.0.0.0（或缩短形式 0）指定所有主机。
longurl-deny	如果 URL 超出 URL 缓冲区大小限制或 URL 缓冲区不可用，则拒绝 URL 请求。
longurl-truncate	如果 URL 超出 URL 缓冲区限制，则仅向 N2H2 或 Websense 服务器发送源主机名或 IP 地址。
-*port*	（可选）应用过滤的 TCP 端口。通常，这是端口 80，但也接受其他值。http 或 url 文字可用于端口 80。在连字符后添加另一个端口（可选）可标识端口范围。
proxy-block	阻止用户连接到 HTTP 代理服务器。
url	从流经 ASA 的数据中过滤 URL。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

通过 **filter url** 命令，您可以防止出站用户访问您使用 N2H2 或 Websense 过滤应用指定的万维网 URL。

注意　必须首先配置 **url-server** 命令，之后方可发出 **filter url** 命令。

filter url 命令的 **allow** 选项确定 ASA 在 N2H2 或 Websense 服务器变为离线状态的行为方式。如果将 **allow** 选项与 **filter url** 命令一起使用且 N2H2 或 Websense 服务器变为离线状态，则端口 80 流量经过 ASA 而不过滤。如果此命令不与 **allow** 选项一起使用且服务器处于离线状态，则 ASA 停止出站端口 80 (Web) 流量，直到服务器重新上线，或者，如果有其他 URL 服务器可用，则将控制权转交给该 URL 服务器。

注意　在设置 **allow** 选项后，如果 N2H2 或者 Websense 服务器变为离线状态，则 ASA 将控制权交给备用服务器。

N2H2 或 Websense 服务器与 ASA 一起使用，以基于公司安全策略拒绝用户访问网站。

使用过滤服务器

Websense 协议版本 4 支持主机与 ASA 之间的组和用户名身份验证。ASA 执行用户名称查找，然后 Websense 服务器处理 URL 过滤和用户名记录。

N2H2 服务器必须是 Windows 工作站（2000、NT 或 XP），运行 IFP 服务器，建议具有至少 512 MB 内存。此外，N2H2 服务的长 URL 支持不超过 3 KB，低于 Websense 的上限。

Websense 协议版本 4 包含以下增强功能：

- URL 过滤允许 ASA 使用 Websense 服务器上定义的策略来检查传出 URL 请求。
- 用户名记录跟踪 Websense 服务器上的用户名、组和域名。
- 用户名查找支持 ASA 使用用户身份验证表将主机的 IP 地址映射到用户名。

以下网站提供关于 Websense 的信息：

http://www.websense.com/

配置过程

按照以下步骤操作以过滤 URL：

1. 使用 **url-server** 命令的相应供应商特定形式来指定 N2H2 或 Websense 服务器。
2. 通过 **filter** 命令启用过滤。
3. 如果需要，使用 **url-cache** 命令来改善吞吐量。但是，此命令不更新 Websense 日志，可能影响 Websense 记账报告。在使用 **url-cache** 命令之前累积 Websense 运行日志。
4. 使用 **show url-cache statistics** 和 **show perfmon** 命令来查看运行信息。

使用长 URL

对于 Websense 过滤服务器，支持最高 4 KB 的过滤 URL，对于 N2H2 过滤服务器，支持最高 3KB 的过滤 URL。

使用 **longurl-truncate** 和 **cgi-truncate** 选项以允许处理长度超过最大允许大小的 URL 请求。

如果 URL 的长度超过最大长度且您不启用 **longurl-truncate** 或 **longurl-deny** 选项，则 ASA 丢弃数据包。

在 URL 的长度超过允许的最大长度时，**longurl-truncate** 选项使 ASA 只将用于评估的 URL 的主机名或 IP 地址部分发送到过滤服务器。如果 URL 的长度超过允许的最大长度，则使用 **longurl-deny** 选项来拒绝出站 URL 流量。

使用 **cgi-truncate** 选项来截取 CGI URL，使其只包含 CGI 脚本位置和脚本名称，不带任何参数。许多长 HTTP 请求是 CGI 请求。如果参数列表很长，则等待和发送完整 CGI 请求（包括参数列表）可能会耗尽内存资源并降低 ASA 性能。

缓冲 HTTP 响应

默认情况下，当用户发出连接到特定网站的请求时，ASA 同时将请求发送给 Web 服务器和过滤服务器。如果过滤服务器的响应时间晚于 Web 内容服务器，则 Web 服务器的响应被丢弃。从 Web 客户端角度来看，这会延迟 Web 服务器响应。

通过启用 HTTP 响应缓冲区，来自 Web 内容服务器的响应被缓冲，如果过滤服务器允许连接，还会转发给请求用户。这样可以防止原本会出现的延迟。

要启用 HTTP 响应缓冲区，输入以下命令：

```
ciscoasa(config)# url-block block block-buffer-limit
```

用将要缓冲的最大块数来取代 *block-buffer-limit* 参数。允许的值介于 1 和 128 之间，指定一次可缓冲 1550 字节块的数量。

示例

以下示例过滤所有出站 HTTPS 连接，但来自 10.0.2.54 主机的出站 HTTP 连接除外。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

以下示例阻止准备发给在 8080 端口上侦听的代理服务器的所有出站 HTTP 连接。

```
ciscoasa(config)# filter url 8080 0 0 0 0 proxy-block
```

相关命令

命令	说明
filter activex	从流经 ASA 的 HTTP 流量中删除 ActiveX 对象。
filter java	从流经 ASA 的 HTTP 流量删除 Java 小应用。
url-block	管理在等待来自过滤服务器的过滤决策时用于 Web 服务器响应的 URL 缓冲区。
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。

fips enable

要启用策略检查以对系统或模块实施 FIPS 合规性，请在全局配置模式下使用 **fips enable** 命令。要禁用策略检查，请使用此命令的 **no** 形式。

fips enable

no fips enable

语法说明

enable	启用或禁用策略检查以实施 FIPS 合规性。

默认值

此命令没有默认设置。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(4)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

要以 FIPS 合规模式运行，必须应用 **fips enable** 命令以及在安全策略中指定的正确配置。内部 API 允许设备在运行时迁移以实施正确配置。

当在启动配置中存在 FIPS 合规模式时，FIPS POST 将运行并显示以下控制台消息：

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec.52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec.252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

示例

下面显示为在系统上实施 FIPS 合规性而执行的策略检查：

```
ciscoasa(config)# fips enable
```

相关命令

命令	说明
clear configure fips	清除 NVRAM 中存储的系统或模块 FIPS 配置信息。
crashinfo console disable	禁止对闪存读取、写入和配置故障写入信息。
fips self-test poweron	执行加电自检。
show crashinfo console	对闪存执行故障写入信息的读取、写入和配置。
show running-config fips	显示在 ASA 上运行的 FIPS 配置。

fips self-test poweron

要执行加电自检，请在特权 EXEC 模式下使用 **fips self-test powereon** 命令。

fips self-test poweron

语法说明

poweron	执行加电自检。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(4)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

输入此命令会导致设备运行 FIPS 140-2 合规性所要求的一切自检。测试包括加密算法测试、软件完整性测试和关键功能测试。

示例

以下示例展示系统执行加电自检：

```
ciscoasa(config)# fips self-test poweron
```

相关命令

命令	说明
clear configure fips	清除 NVRAM 中存储的系统或模块 FIPS 配置信息。
crashinfo console disable	禁止对闪存读取、写入和配置故障写入信息。
fips enable	启用或禁用用于对系统或模块实施 FIPS 合规性的策略检查。
show crashinfo console	对闪存执行故障写入信息的读取、写入和配置。
show running-config fips	显示在 ASA 上运行的 FIPS 配置。

firewall transparent

要将防火墙模式设置为透明模式，请在全局配置模式下使用 **firewall transparent** 命令。要恢复路由模式，请使用此命令的 **no** 形式。

firewall transparent

no firewall transparent

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 处于路由模式。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.5(1)/9.0(1)	您可以在多情景模式下根据情景来设置此命令。

使用指南

透明防火墙是 2 层防火墙，充当 “ 线缆中的块 ” 或 “ 隐藏防火墙 ”，并且不会被视为所连接设备的路由器跃点。

您可以在多情景模式中根据场景来设置此命令。

在更改模式时，ASA 会清除配置，因为许多命令不能同时支持两种模式。如果您已经拥有填充配置，在更改模式之前请务必备份您的配置；在创建新配置时，可以使用此备份作为参考。

如果将一个文本配置下载到 ASA 且使用 **firewall transparent** 命令来更改模式，请确保将该命令放在配置的顶部； ASA 会在读取命令后立即更改模式并继续读取下载的配置。如果命令位于配置中靠后的位置，则 ASA 清除配置中所有之前的行。

示例

以下示例将防火墙模式更改为透明：

```
ciscoasa(config)# firewall transparent
```

相关命令

命令	说明
arp-inspection	启用 ARP 检测，就是将 ARP 数据包与静态 ARP 条目进行比较。
mac-address-table static	向 MAC 地址表添加静态 MAC 地址条目。
mac-learn	禁用 MAC 地址学习。
show firewall	显示防火墙模式。
show mac-address-table	显示 MAC 地址表，包括动态和静态条目。

firewall vlan-group (IOS)

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 vlan-group *firewall_group vlan_range*

no firewall 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* 可以是通过以下方式之一来标识的一个或多个 VLAN（2 到 1000 以及 1025 到 4094）： • 单一号码 (*n*) • 范围 (*n-x*) 不同的号码或范围用逗号分隔。例如，输入以下号码： `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。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在思科 IOS 软件中，使用 **firewall vlan-group** 命令创建最多 16 个防火墙 VLAN 组，然后将这些组分配给 ASA（使用 **firewall module** 命令）。例如，您可以将所有 VLAN 分配给一个组，也可以创建一个内部组和一个外部组，还可以为每位客户创建一个组。每个组可以包含多个 VLAN，个数不限。

您不能将同一个 VLAN 分配到多个防火墙组；但是，可以将多个防火墙组分配到一个 ASA，也可以将单个防火墙组分配给多个 ASA。例如，要分配到多个 ASA 的 VLAN 可与各 ASA 唯一的 VLAN 分处于不同的组中。

示例

以下示例展示如何创建三个防火墙 VLAN 组：为每个 ASA 创建一个，并且一个包含分配给两个 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** 命令的示例输出：

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

以下是 **show firewall module** 命令的示例输出，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	说明
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。

flow-export active refresh-interval

要指定在流更新事件之间的时间间隔，请在全局配置模式下使用 **flow-export active refresh-interval** 命令。

flow-export active refresh-interval *value*

语法说明

value	指定在流更新事件之间的时间间隔（以分钟为单位）。有效值为 1 到 60 分钟。

默认值

默认值为 1 分钟。

命令模式

下表展示可输入此命令的模式。

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

如果已配置 **flow-export delay flow-create** 命令，然后使用比延迟值长不到 5 秒的间隔值来配置 **flow-export active refresh-interval** 命令，则在控制台上显示以下警告消息：

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

如果已配置 **flow-export active refresh-interval** 命令，然后使用比间隔值少不到 5 秒的延迟值来配置 **flow-export delay flow-create** 命令，则在控制台上显示以下警告消息：

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

示例

以下示例展示如何配置 30 分钟的时间间隔：

```
ciscoasa(config)# flow-export active refresh-interval 30
```

相关命令

命令	说明
clear flow-export counters	将 NetFlow 中的所有运行时计数器重置为零。
flow-export destination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

flow-export delay flow-create

要延迟 flow-create 事件的导出，请在全局配置模式下使用 **flow-export delay flow-create** 命令。要无延迟导出 flow-create 事件，请使用此命令的 **no** 形式。

flow-export delay flow-create *seconds*

no flow-export delay flow-create *seconds*

语法说明

seconds	指定导出 flow-create 事件的延迟，以秒为单位。有效值为 1 到 180 秒。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式。

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

命令历史

版本	修改
8.1(2)	引入了此命令。

使用指南

如果没有配置 **flow-export delay flow-create** 命令，则会无延迟导出 flow-create 事件。

如果流在配置的延迟时间之前中断，则不会发送 flow-create 事件；而是会发送延期流中断事件。

示例

以下示例展示如何将 flow-create 事件的导出延迟 10 秒：

```
ciscoasa(config)# flow-export delay flow-create 10
```

相关命令

命令	说明
clear flow-export counters	将 NetFlow 中的所有运行时计数器重置为零。
flow-export destination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

flow-export destination

要配置向其发送 NetFlow 数据包的收集器，请在全局配置模式下使用 **flow-export destination** 命令。要删除 NetFlow 数据包的收集器，请使用此命令的 **no** 形式。

flow-export destination *interface-name ipv4-address | hostname udp-port*

no flow-export destination *interface-name ipv4-address | hostname udp-port*

语法说明

hostname	指定 NetFlow 收集器的主机名。
interface-name	指定接口名，通过该接口可抵达目的地。
ipv4-address	指定 NetFlow 收集器的 IP 地址。仅支持 IPv4。
udp-port	指定 NetFlow 收集器侦听的 UDP 端口。有效值为 1 到 65535。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式。

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

命令历史

版本	修改
8.1(1)	引入了此命令。
8.1(2)	流导出目的地的最大数增加到五。

使用指南

您可以使用 **flow-export destination** 命令来配置 ASA，以将 NetFlow 数据导出到 NetFlow 收集器。

注意 对于每个安全情景，最多可以输入五个导出目的地（收集器）。当您输入新目的地时，模板记录被发送到新添加的收集器。如果您尝试添加五个以上目的地，则会显示以下错误消息：

“ERROR: A maximum of 5 flow-export destinations can be configured.”

如果将 ASA 配置为导出 NetFlow 数据以改进性能，我们建议您通过输入 **logging flow-export-syslogs disable** 命令来禁用冗余系统日志消息（NetFlow 也会捕获这些消息）。

示例

以下示例展示如何为 NetFlow 数据配置收集器：

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

相关命令

命令	说明
clear flow-export counters	将 NetFlow 中的所有运行时计数器重置为零。
flow-export delay flow-create	将 flow-create 事件的导出延迟指定的时间。
flow-export template timeout-rate	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

flow-export event-type destination

要配置 NetFlow 收集器和过滤器的地址以确定应将哪些 NetFlow 记录发送到每个收集器，请在策略映射类配置模式下使用 **flow-export event-type destination** 命令。要删除 NetFlow 收集器和过滤器的地址，请使用此命令的 **no** 形式。

flow-export event-type {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination**

no flow-export event-type {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination**

语法说明

all	指定所有四个事件类型。
flow-create	指定 flow-create 事件。
flow-denied	指定 flow-denied 事件。
flow-teardown	指定 flow-teardown 事件。
flow-update	指定 flow-update 事件。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式。

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
策略映射类配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.1(2)	引入了此命令。

使用指南

NetFlow 事件可通过模块化策略框架配置。如果模块化策略框架未为 NetFlow 进行配置，则将不会记录任何事件。流量根据配置类的顺序进行匹配。检测到匹配后，将不会检查其他任何类。对于 NetFlow 事件，配置要求如下：

- 流导出目标（即 NetFlow 收集器）的唯一标识是其 IP 地址。
- 支持的事件类型是 flow-create、flow-teardown、flow-denied、flow-update 等，其中包括之前已列出的四个事件类型。
- 接口策略中不支持流导出操作。
- 仅在 **class-default** 命令和使用 **match any** 或 **match access-list** 命令的类中支持流导出操作。
- 如果未定义 NetFlow 收集器，则不会发生配置操作。
- NetFlow 安全事件日志过滤与顺序无关。

注意　要创建有效的 NetFlow 配置，必须拥有 flow-export 目的地配置和 flow-export 事件类型配置。flow-export 目的地配置本身不执行任何操作。您还必须为 flow-export 事件类型配置配置一个类映射。这可以是默认类映射或者您创建的类映射。

示例

以下示例将主机 10.1.1.1 与主机 20.1.1.1 之间的所有 NetFlow 事件导出到目的地 15.1.1.1。

```
ciscoasa(config)# access-list flow_export_acl permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 15.1.1.1
```

相关命令

命令	说明
clear flow-export counters	将 NetFlow 中的所有运行时计数器重置为零。
flow-export delay flow-create	将 flow-create 事件的导出延迟指定的时间。
flow-export template timeout-rate	控制模板信息发送到 NetFlow 收集器的时间间隔。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

flow-export template timeout-rate

要控制将模板信息发送到 NetFlow 收集器的间隔，请在全局配置模式下使用 **flow-export template timeout-rate** 命令。要将模板超时值重置为默认值，请使用此命令的 **no** 形式。

flow-export template timeout-rate *minutes*

no flow-export template timeout-rate *minutes*

语法说明

minutes	指定时间间隔，以分钟为单位。有效值为 1 到 3600 分钟。
template	为配置导出模板启用 **timeout-rate** 关键字。
timeout-rate	指定模板首次发送到重新发送之前经过的时间（间隔）。

默认值

间隔的默认值为 30 分钟。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.1(1)	引入了此命令。

使用指南

您应基于正使用的收集器以及收集器所期望的模板刷新速度来配置超时速度。

如果配置了安全设备来导出 NetFlow 数据，以提高性能，则我们建议您输入 **logging flow-export-syslogs disable** 命令禁用冗余系统日志消息（那些也已由 NetFlow 捕获的消息）。

示例

以下示例展示如何配置 NetFlow，从而每 60 分钟向所有收集器发送一次模板记录：

```
ciscoasa(config)# flow-export template timeout-rate 60
```

相关命令

命令	说明
clear flow-export counters	重置与 NetFlow 数据有关的所有运行时计数器。
flow-export destination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
logging flow-export-syslogs enable	在您输入 **logging flow-export-syslogs disable** 命令后，启用系统日志消息，以及与 NetFlow 数据相关联的系统日志消息。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

flowcontrol

要为流控制启用暂停 (XOFF) 帧，请在接口配置模式下使用 **flowcontrol** 命令。要禁用暂停帧，请使用此命令的 **no** 形式。

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

语法说明

high_water	对于 10 千兆以太网，将高水位标记设置为 0 到 511 KB 之间，对于 1 千兆以太网，将高水位标记设置为 0 到 47 KB 之间（或者，对于 4GE-SSM 上的千兆以太网接口，设置为 0 到 11 KB 之间）。当缓冲区使用超过高水位标记时，NIC 发送暂停帧。
low_water	对于 10 千兆以太网，将低水位标记设置为 0 到 511 KB 之间，对于 1 千兆以太网，将低水位标记设置为 0 到 47 KB 之间（或者，对于 4GE-SSM 上的千兆以太网接口，设置为 0 到 11 KB 之间）。在网络接口控制器 (NIC) 发送暂停帧后，当缓冲区使用降至低水位标记以下时，NIC 发送 XON 帧。链路伙伴在收到 XON 帧之后恢复流量。
noconfirm	应用此命令而不作确认。由于此命令重置接口，若不用此选项，会要求您确认配置更改。
pause_time	设置暂停刷新阈值，此值在 0 到 65535 个插槽之间。每插槽是传输 64 字节的时间，因此，每单位的时间取决于您的链路速度。链路伙伴在收到 XON 之后恢复流量，或者在 XOFF 到期后（由暂停帧中的此定时器值来控制）恢复流量。如果缓冲区使用一直高于高水位标记，则重复发送暂停帧 - 由暂停刷新阈值来控制暂停帧的发送。默认值为 26624。

命令默认值

默认情况下暂停帧被禁用。

关于 10 千兆以太网，请参阅以下默认设置：

- 默认高水位标记是 128 KB。
- 默认低水位标记是 64 KB。
- 默认暂停刷新阈值是 26624 个插槽。

关于 1 千兆以太网，请参阅以下默认设置：

- 默认高水位标记是 24 KB。
- 默认低水位标记是 16 KB。
- 默认暂停刷新阈值是 26624 个插槽。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
8.2(2)	为 ASA 5580 上的 10 千兆以太网接口引入了此命令。
8.2(3)	增加了对 ASA 5585-X 的支持。
8.2(5)/8.4(2)	增加了对所有型号上的 1 千兆以太网的支持。

使用指南

1 千兆以太网和 10 千兆以太网接口均支持此命令。此命令不支持管理接口。

为一个物理接口输入此命令。

如果您有流量突发，则流量突发超过 NIC 上的 FIFO 缓冲区和接收环路缓冲区的缓冲容量时，会发生数据包丢弃。为流控制启用暂停帧可以缓解此问题。

当您启用此命令时，NIC 硬件会根据 FIFO 缓冲区使用情况自动生成暂停 (XOFF) 和 XON 帧：

1. 当缓冲区使用超过高水位标记时，NIC 发送暂停帧。
2. 在发送暂停帧后，当缓冲区使用低于低水位标记时，NIC 发送 XON 帧。
3. 链路伙伴在收到 XON 之后恢复流量，或者在 XOFF 到期后（由暂停帧中的定时器值来控制）恢复流量。
4. 如果缓冲区使用一直高于高水位标记，则 NIC 重复发送暂停帧 - 由暂停刷新阈值来控制暂停帧的发送。

当您使用此命令时，会显示以下警告消息：

```
Changing flow-control parameters will reset the interface.Packets may be lost during the
reset.
Proceed with flow-control changes?
```

要更改参数而不会被提示，请使用 **noconfirm** 关键字。

注　仅支持 802.3x 中定义的流量控制帧。不支持基于优先级的流量控制。

示例

以下示例支持使用默认设置的暂停帧：

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface.Packets may be lost during the
reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

相关命令

命令	说明
interface	进入接口配置模式。

format

要清除所有文件并将文件系统格式化，请在特权 EXEC 模式下使用 **format** 命令。

format {disk0: | disk1: | flash:}

语法说明

disk0*:*	指定 内部闪存，后跟冒号。
disk1:	指定 外部闪存卡，后跟冒号。
flash:	指定 内部闪存，后跟冒号。在 ASA 5500 系列中，**flash** 关键字是 **disk0** 的别名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

format 命令清除指定文件系统上的所有数据，然后将 FAT 信息重写到设备上。

注意事项

使用 **format** 命令时应极其小心，仅在必要时才清除损坏闪存上的数据。

要删除所有可见的文件（不包括隐藏的系统文件），请输入 **delete /recursive** 命令，而不是 **format** 命令。

注意

在思科 ASA 5500 系列上，**erase** 命令会销毁磁盘中使用 0xFF 模式的所有用户数据。相反，**format** 命令仅重置文件系统的控制结构。使用原始磁盘读取工具仍可看到磁盘中的信息。

要修复损坏的文件系统，请先输入 **fsck** 命令，再输入 **format** 命令。

示例

以下示例展示如何格式化闪存：

```
ciscoasa# format flash:
```

相关命令

命令	说明
delete	删除用户可见的所有文件。
erase	删除所有文件并格式化闪存。
fsck	修复损坏的文件系统。

forward interface

对于有内置交换机的型号，如 ASA 5505，请在接口配置模式下使用 **forward interface** 命令，以将一个 VLAN 的连接性从初始触点恢复到其他 VLAN。要限制一个 VLAN 发起到其他 VLAN 的连接，请使用此命令的 **no** 形式。

forward interface vlan *number*

no forward interface vlan *number*

语法说明

vlan *number*	指定此 VLAN 接口无法向其启动流量的 VLAN ID。

默认值

默认情况下，所有接口均可启动到所有其他接口的流量。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
接口配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

您可能需要根据您的许可证所支持的 VLAN 数来限制一个 VLAN。

在路由模式下，您可以使用 ASA 5505 基础许可证配置最多三个活动 VLAN，使用 Security Plus 许可证配置最多五个活动 VLAN。活动 VLAN 是一个已经配置 **nameif** 命令的 VLAN。对于上述任一许可证，您均可在 ASA 5505 上配置最多五个非活动 VLAN，但如果您使其处于活动状态，请务必遵循您的许可证的指导原则。

对于基础许可证，必须使用 **no forward interface** 接口命令来配置第三个 VLAN，以限制此 VLAN 发起到其他 VLAN 的连接。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部工作网络，第三个 VLAN 分配给您的家庭网络。家庭网络不需要访问工作网络，因此，您可以在家庭 VLAN 上使用 **no forward interface** 命令；工作网络可以访问家庭网络，但家庭网络无法访问工作网络。

如果您已经使用 **nameif** 命令配置了两个 VLAN 接口，则在第三个接口上，请务必先输入 **no forward interface** 命令，再输入 **nameif** 命令；在 ASA 5505 上，ASA 不允许凭借基础许可证使用三个全功能的 VLAN 接口。

示例

以下示例配置了三个 VLAN 接口。第三个家庭接口无法将流量转发到工作接口。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

...
```

相关命令

命令	说明
backup interface	例如，将一个接口作为备用链路分配给 ISP。
clear interface	清除 **show interface** 命令的计数器。
interface vlan	创建 VLAN 接口并进入接口配置模式。
show interface	显示接口的运行时状态和统计信息。
switchport access vlan	将交换机端口分配给 VLAN。

fqdn (crypto ca trustpoint)

在进行注册时，要在证书的主体可选名称扩展名中包含指示的 FQDN，请在 crypto ca trustpoint 配置模式下使用 **fqdn** 命令。要恢复 FQDN 的默认设置，请使用此命令的 **no** 形式。

fqdn [*fqdn* | **none**]

no fqdn

语法说明

fqdn	指定 FQDN。最大长度是 64 个字符。
none	指定不使用完全限定域名。

默认值

默认设置不包括 FQDN。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Crypto ca-trustpoint 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您正在配置 ASA 来支持使用证书的 Nokia VPN 客户端的身份验证，请使用 **none** 关键字。有关 Nokia VPN 客户端的支持证书身份验证的详细信息，请参阅 **crypto isakmp identity** 或 **isakmp identity** 命令。

示例

以下示例进入中心信任点的 crypto ca-trustpoint 配置模式，并在中心信任点的注册请求中包含 FQDN 工程：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca-trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment retry count	指定尝试发送注册请求的重试次数。
enrollment retry period	指定在尝试发送注册请求之前要等待的分钟数。
enrollment terminal	指定使用此信任点进行剪切粘贴注册。

fqdn（网络对象）

要配置网络对象的 FQDN，请在对象配置模式下使用 **fqdn** 命令。要从配置中删除对象，请使用此命令的 **no** 形式。

fqdn [**v4** | **v6**] *fqdn*

no fqdn [**v4** | **v6**] *fqdn*

语法说明

fqdn	指定 FQDN，包括主机和域。FQDN 必须以数字或字母来开头和结尾。内部字符仅允许使用字母、数字和短划线。标签由点分隔（例如 www.cisco.com）。
v4	（可选）指定 IPv4 域名。
v6	（可选）指定 IPv6 域名。

默认值

默认情况下，域名为 IPv4 域。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
对象网络配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.4(2)	引入了此命令。

使用指南

如果您使用不同的值来配置现有网络对象，则新的配置将取代现有配置。

示例

以下示例展示如何创建网络对象：

```
ciscoasa (config)# object network FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

相关命令

命令	说明
clear configure object	清除所有已创建对象。
description	将添加到网络对象的说明。
fqdn	指定完全限定域名网络对象。
host	指定主机的网络对象。

命令	说明
nat	实现网络对象的 NAT。
object network	创建网络对象。
object-group network	创建网络对象组。
range	指定网络对象的地址范围。
show running-config object network	显示网络对象的配置。
subnet	指定子网的网络对象。

fragment

要提供数据包分段的额外管理并改进与 NFS 之间的兼容性，请在全局配置模式下使用 **fragment** 命令。要恢复默认值，请使用此命令的 **no** 形式。

fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

语法说明

chain *limit*	指定一个完整 IP 数据包的最大分段数量。
interface	（可选）指定 ASA 接口。如果未指定接口，则此命令应用于所有接口。
reassembly full | **virtual**	指定通过 ASA 来路由的 IP 分段的完全或虚拟重组。在 ASA 终止的 IP 分段始终会完全重组。
size *limit*	设置可在 IP 重组数据库中等待重组的分段的最大数量。 **注**　在整个队列大小达到 2/3 满之后，ASA 不接受不是现有交换矩阵链的一部分的任何分段。队列的剩余 1/3 用于接受这样的分段：其中的源 / 目标 IP 地址和 IP 标识号与已部分排队的不完整分段链的分段相同。此限制是一种 DoS 保护机制，在有分段泛洪攻击时，可帮助合法分段链进行重组。
timeout *limit*	指定等待整个分段数据包到达的最大秒数。在数据包的第一个分段到达后计时器启动。如果在指定秒数后数据包的分段没有全部抵达，则已收到的数据包的所有分段将被丢弃。

默认值

默认值如下：

- **chain** 是 24 个数据包。
- *interface* 是所有接口。
- **size** 是 200。
- **timeout** 为 5 秒。
- 虚拟重组被启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改，现在您必须选择以下关键字之一：**chain**、**size** 或 **timeout**。若不输入这些关键字之一，您无法再输入 **fragment** 命令，而在软件的先前版本中支持这样做。
8.0(4)	添加了 **reassembly full** | **virtual** 选项。

使用指南

默认情况下，ASA 接受最多 24 个分段，以重建完整 IP 数据包。根据您的网络安全策略，您应该考虑配置 ASA 以防止分段数据包穿越 ASA，方法是在每个接口上输入 **fragment chain 1** *interface* 命令。设置限值为 1 表示所有数据包必须是完整的，即未分段。

如果通过 ASA 的大部分网络流量是 NFS，则可能有必要进行其他调整以避免数据库溢出。

在 NFS 服务器与客户端之间的 MTU 大小很小的环境中，如 WAN 接口，**chain** 关键字可能需要额外的调整。在这种情况下，我们建议使用 NFS over TCP 以提高效率。

将 **size** *limit* 设置为一个大值可能导致 ASA 更容易因分段泛洪而受到 DoS 攻击。请勿将 **size** *limit* 设置为等于或大于 1550 或 16384 池中的块总数。

默认值将限制分段泛洪导致的 DoS 攻击。

无论 **reassembly** 选项的设置如何，均会执行以下过程：

- 收集 IP 片段，直到片段集形成或超时间隔已到（请参阅 **timeout** 选项）。
- 如果分段集形成，则对片段集执行完整性检查。这些检查包括无重叠、无尾部溢出和无链溢出（参阅 **chain** 选项）。

如果配置了 **fragment reassembly virtual** 命令，则片段集被转发到传输层，以供进一步处理。

如果配置了 **fragment reassembly full** 命令，则片段集会首先合并为单个 IP 数据包。然后，该单个 IP 数据包被转发到传输层，以供进一步处理。

示例

以下示例展示如何阻止外部和内部接口上的分段数据包：

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

在您希望在其上防止分段数据包的每个额外接口上继续输入 **fragment chain 1** *interface* 命令。

以下示例展示如何在外部接口上将分段数据库配置为最大大小 2000、最大链长 45 和等待时间 10 秒：

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

以下示例展示带有 **reassembly virtual** 选项的 **show fragment** 命令的输出：

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

相关命令

命令	说明
clear configure fragment	将所有 IP 分段重组配置重置为默认值。
clear fragment	清除 IP 分段重组模块的运行数据。
show fragment	显示 IP 分段重组模块的运行数据。
show running-config fragment	显示 IP 分段重组配置。

frequency

要设置所选 SLA 操作的重复率，请在 SLA 监控协议配置模式下使用 **frequency** 命令。要恢复默认值，请使用此命令的 **no** 形式。

frequency *seconds*

no frequency

语法说明

seconds	各 SLA 探测之间的秒数。有效值为从 1 到 604800 秒。此值不得低于 **timeout** 值。

默认值

默认频率为间隔 60 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在操作的生命期中，SLA 操作以给定的频率重复。例如：

- 频率为 60 秒的 **ipIcmpEcho** 操作：在操作的生命期内，每 60 秒发送一次回应请求数据包。
- 在回应操作中，默认数据包数量为 1。此数据包在操作开始时发送，并在 60 秒后再次发送。

如果单个 SLA 操作的执行时间大于指定频率值，则名为 “busy” 的统计计数器的数值会增加，而不是立即重复操作。

为 **frequency** 命令指定的值不得小于为 **timeout** 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 操作的频率设置为 3 秒，超时值设置为 1000 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)# 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	说明
sla monitor	定义 SLA 监控操作。
timeout	定义 SLA 操作等待响应的时间。

fsck

要执行文件系统检查和修复损坏，请在特权 EXEC 模式下使用 **fsck** 命令。

fsck [**/noconfirm**] {**disk0:** | **disk1:** | **flash:**}

语法说明

/noconfirm	（可选）不会提示您进行修复确认。
disk0:	指定 内部闪存，后跟冒号。
disk1:	指定 外部闪存卡，后跟冒号。
flash:	指定 内部闪存，后跟冒号。**flash** 关键字是 **disk0:** 的别名。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

fsck 命令检查并尝试修复损坏的文件系统。请在尝试更永久性的修复过程之前使用此命令。

如果 FSCK 实用程序修复磁盘损坏实例（例如由于电源故障或异常关闭导致的损坏），则会创建名为 FSCK*xxx*.REC 的恢复文件。这些文件可以包含 FSCK 在运行时恢复的文件的一小部分或整个文件。在极少数情况下，您可能需要检查这些文件以恢复数据；通常不需要这些文件，可以将其安全删除。

注意　FSCK 实用程序在启动时自动运行，因此，即使没有手动输入 **fsck** 命令，您也可能看到这些恢复文件。

示例

以下示例展示如何检查闪存的文件系统：

```
ciscoasa# fsck disk0:
```

相关命令

命令	说明
delete	删除用户可见的所有文件。
erase	删除所有文件并格式化闪存。
format	清除文件系统上的所有文件，包括隐藏的系统文件，并重新安装文件系统。

ftp mode passive

要将 FTP 模式设置为被动模式，请在全局配置模式下使用 **ftp mode passive** 命令。要将 FTP 客户端重置为主用模式，请使用此命令的 **no** 形式。

ftp mode passive

no ftp mode passive

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ftp mode passive 命令将 FTP 模式设置为被动模式。ASA 还可使用 FTP 在 FTP 服务器上上传或下载映像文件或配置文件。**ftp mode passive** 命令控制 ASA 上的 FTP 客户端如何与 FTP 服务器交互。

在被动 FTP 中，客户端启动控制连接和数据连接。被动模式是指这样一种服务器状态，即服务器被动接受由客户端启动的控制连接和数据连接。

在被动模式下，目标端口和源端口是临时端口（大于 1023）。此模式在客户端发出 **passive** 命令以启动被动数据连接的设置时由客户端设置。服务器（被动模式下数据连接的接收方）通过它用于侦听特定连接的端口号来响应。

示例

以下示例将 FTP 模式设置为被动：

```
ciscoasa(config)# ftp mode passive
```

相关命令

copy	向 FTP 服务器上传或从 FTP 服务器下载映像文件或配置文件。
debug ftp client	显示有关 FTP 客户端活动的详细信息。
show running-config ftp mode	显示 FTP 客户端配置。

functions

在版本 8.0(2) 中，您不能使用 **functions** 命令。此命令已弃用，仅为向后兼容而包含在本命令参考中。使用 **import** 和 **export** 命令，为网站、文件访问以及插件、定制和语言转换创建 URL 列表。

要为此用户或组策略在 WebVPN 上配置端口转发 Java 小应用、Citrix 支持、文件访问、文件浏览、文件服务器条目、webtype ACL 应用、HTTP 代理、端口转发或 URL 条目的自动下载，请在 webvpn 配置模式下使用 **functions** 命令。要删除已配置的功能，请使用此命令的 **no** 形式。

functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none**}

no functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none**}

语法说明

auto-download	在 WebVPN 登录后启用或禁用端口转发 Java 小应用的自动下载。您必须首先启用端口转发、Outlook/Exchange 代理或 HTTP 代理。
citrix	启用或禁用从 MetaFrame 应用服务器到远程用户的终端服务的支持。此关键字让 ASA 用作安全 Citrix 配置中的安全网关。这些服务通过标准 Web 浏览器为用户提供对 MetaFrame 应用的访问。
file-access	启用或禁用文件访问。在启用时，WebVPN 主页在服务器列表中列出文件服务器。您必须启用文件访问来启用文件浏览和 / 或文件输入。
file-browsing	为文件服务器和共享启用或禁用浏览。您必须启用文件浏览，以允许用户进入文件服务器。
file-entry	允许或禁止用户输入文件服务器名称。
filter	应用 webtype ACL。在启用时，ASA 应用通过 WebVPN **filter** 命令定义的 webtype ACL。
http-proxy	启用或禁用将 HTTP 小应用代理转发到远程用户。对于用来适当处理解析的技术（例如 Java、ActiveX 和 Flash）来说，代理非常有用。它会绕过解析，同时确保继续使用 ASA。转发的代理自动修改浏览器的原有代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新的代理配置。它支持几乎所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。它唯一支持的浏览器是 Microsoft Internet Explorer。
none	为所有 WebVPN 功能设置一个空值。防止从默认或指定组策略继承功能。
port-forward	启用端口转发。在启用时，ASA 使用通过 WebVPN **port-forward** 命令定义的端口转发列表。
url-entry	启用或禁用用户输入 URL。在启用时，ASA 仍使用所有已配置的 URL 或网络 ACL 来限制 URL。在禁用 URL 输入时，ASA 限制 WebVPN 用户访问主页上的 URL。

默认值

默认情况下禁用这些功能。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	添加了 **auto-download** 和 **citrix** 关键字。
8.0(2)	此命令已弃用。

使用指南

要删除所有已配置的功能，包括通过发出 **functions none** 命令创建的空值，请使用此命令的 **no** 形式，不带任何参数。**no** 选项允许继承其他组策略的值。为阻止继承功能值，请使用 **functions none** 命令。

示例

以下示例展示如何为名为 FirstGroup 的组策略配置文件访问和文件浏览：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# functions file-access file-browsing
```

相关命令

命令	说明
webvpn	在组策略配置模式或用户名配置模式下使用。用于进入 WebVPN 模式以配置应用于组策略或用户名的参数。

第 17 章

gateway 至 hw-module module shutdown 命令

gateway

要指定哪个呼叫代理组正在管理特定网关，请在 mgcp 映射配置模式下使用 **gateway** 命令。要删除配置，请使用此命令的 **no** 形式。

gateway *ip_address* [*group_id*]

语法说明

gateway	正在管理特定网关的呼叫代理组。
group_id	呼叫代理组 ID，从 0 到 2147483647。
ip_address	网关的 IP 地址。

默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Mgcp 映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **gateway** 命令指定哪个呼叫代理组正在管理特定网关。使用 *ip_address* 选项指定网关的 IP 地址。*group_id* 选项是一个介于 0 到 4294967295 之间的数字，此数字必须与正在管理网关的呼叫代理的 *group_id* 对应。一个网关只能属于一个组。

示例

以下示例允许呼叫代理 10.10.11.5 和 10.10.11.6 控制网关 10.10.10.115，并允许呼叫代理 10.10.11.7 和 10.10.11.8 控制网关 10.10.10.116 和 10.10.10.117：

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

相关命令

命令	说明
debug mgcp	启用 MGCP 的调试信息的显示。
mgcp-map	定义 MGCP 映射并启用 mgcp 映射配置模式。
show mgcp	显示 MGCP 配置和会话信息。

gateway-fqdn

配置 ASA 的 FQDN。使用 **gateway-fqdn** 命令。要删除配置，请使用此命令的 **no** 形式。

gateway-fqdn value {**FQDN_Name** | **none**}

no gateway-fqdn

语法说明

fqdn-name	定义要推送到 AnyConnect 客户端的 ASA FQDN。
none	定义 FQDN 为空值，即不指定 FQDN。如果可用，将使用通过 hostname 和 domain-name 命令配置的全局 FQDN。

默认值

在默认组策略中没有设置默认 FQDN 名称。将新的组策略设置为继承此值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

如果您已在 ASA 之间配置负载平衡，请指定 ASA 的 FQDN，以解析用于重建 VPN 会话的 ASA IP 地址。此设置对于支持不同 IP 协议的网络之间的客户端漫游非常关键（例如 IPv4 到 IPv6）。

在漫游之后，您无法使用 AnyConnect 配置文件中的 ASA FQDN 来获取 ASA IP 地址。在负载平衡方案中，地址可能与正确的设备（与之建立隧道的设备）不匹配。

如果 ASA 的 FQDN 没有推送到客户端，客户端将尝试重新连接到隧道在以前建立的任何 IP 地址。为了支持不同协议的网络（从 IPv4 到 IPv6）之间的漫游，AnyConnect 必须在漫游之后执行设备 FQDN 的名称解析，以便为重新建立隧道确定使用哪个 ASA 地址。在初始连接中，客户端使用其配置文件中的 ASA FQDN。如果可用，在后续会话重新连接期间，它总是使用由 ASA 推送（并由管理员在组策略中配置）的设备 FQDN。如果 FQDN 未配置，则 ASA 会根据 ASDM 中“Device Setup > Device Name/Password and Domain Name”（设备设置 > 设备名 / 密码和域名）下的设置来获取设备 FQDN（并将其发送给客户端）。

如果 ASA 没有推送设备 FQDN，则在完成不同 IP 协议的网络之间的漫游后客户端无法重建 VPN 会话。

示例

以下示例将 ASA 的 FQDN 定义为 ASAName.example.cisco.com。

```
ciscoasa(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
ciscoasa(config-group-policy)#
```

以下示例从组策略中删除 ASA 的 FQDN。之后组策略从默认组策略继承该值。

```
ciscoasa(config-group-policy)# no gateway-fqdn
ciscoasa(config-group-policy)#
```

以下示例将 FQDN 定义为没有值。如果可用，将使用采用 ciscoasa 和 domain-name 命令来配置的全局 FQDN。

```
ciscoasa(config-group-policy)# gateway-fqdn none
ciscoasa(config-group-policy)#
```

group

要在 IKEv2 安全关联 (SA) 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 组，请在 ikev2 策略配置模式下使用 **group** 命令。要删除命令并使用默认设置，请使用此命令的 **no** 形式：

group {1 | 2 | 5 | 14 | 19 | 20 | 21 | 24}

no group {1 | 2 | 5 | 14 | 19 | 20 | 21 | 24}

语法说明

1	指定 768 位 Diffie-Hellman 组 1（在 FIPS 模式下不支持）。
2	指定 1024 位 Diffie-Hellman 组 2。
5	指定 1536 位 Diffie-Hellman 组 5。
14	选择 ECDH 组作为 IKEv2 DH 密钥交换组。
19	选择多个 ECDH 组作为 IKEv2 DH 密钥交换组。
20	选择多个 ECDH 组作为 IKEv2 DH 密钥交换组。
21	选择多个 ECDH 组作为 IKEv2 DH 密钥交换组。
24	选择多个 ECDH 组作为 IKEv2 DH 密钥交换组。

默认值

默认 Diffie-Hellman 组是组 2。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。在输入 **crypto ikev2 policy** 命令后，您可以使用 **group** 命令来设置 SA Diffie-Hellman 组。ASA 和 AnyConnect 客户端使用组标识符获取共享密钥而无需相互传输。Diffie-Hellman 组号越低，则其执行所需的 CPU 时间越少。Diffie-Hellman 组号越高，则安全性越高。

当 AnyConnect 客户端在非 FIPS 模式下运行时，ASA 支持 Diffie-Hellman 组 1、2 和 5。在 FIPS 模式下，它支持组 2 和 5。因此，如果您将 ASA 配置为*仅*使用组 1，则在 FIPS 模式下 AnyConnect 客户端将无法连接。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Ikev2 策略配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.4(1)	添加了此命令。
9.0(1)	增加了选择 ECDH 组作为 IKEv2 DH 密钥交换组的功能。

示例

以下示例进入 ikev2 策略配置模式并将 Diffie-Hellman 组设置为组 5：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 5
```

相关命令

命令	说明
encryption	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定加密算法。
group	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 Diffie-Hellman 组。
lifetime	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 SA 生命期。
prf	指定用于 AnyConnect IPsec 连接的 IKEv2 SA 中的伪随机函数。

group-alias

要创建用户可用来引用隧道组的一个或多个备用名称，请在 tunnel-group webvpn 配置模式下使用 **group-alias** 命令。要从列表中删除别名，请使用此命令的 **no** 形式。

group-alias *name* [**enable | disable**]

no group-alias *name*

语法说明

disable	禁用组别名。
enable	启用一个之前禁用的组别名。
name	指定隧道组别名的名称。这可以是您选择的任何字符串，只是字符串不能包含空格。

默认值

没有默认组别名，但如果指定组别名，则默认情况下启用该别名。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

您指定的组别名出现在登录页面的下拉列表中。每个组可以有多个别名或没有别名。这样，当同一组有几个常见名称时，例如 “Devtest” 和 “QA”，此命令很有用。

示例

以下示例展示几个命令，这些命令用于配置名为 “devtest” 的隧道组并为该组建立别名 “QA” 和 “Fra-QA”：

```
ciscoasa(config)# tunnel-group devtest type webvpn
ciscoasa(config)# tunnel-group devtest webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias QA
ciscoasa(config-tunnel-webvpn)# group-alias Fra-QA
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
clear configure tunnel-group	清除整个隧道组数据库或指定的隧道组配置。
show webvpn group-alias	显示指定隧道组或所有隧道组的别名。
tunnel-group webvpn-attributes	为配置 WebVPN 隧道组属性进入 tunnel-group webvpn 配置模式。

group-delimiter

要启用组名解析并指定在解析组名（组名来自协商隧道时接收的用户名）时使用的分隔符，请在全局配置模式下使用 **group-delimiter** 命令。要禁用此组名解析，请使用此命令的 **no** 形式。

group-delimiter *delimiter*

no group-delimiter

语法说明

delimiter	指定作为组分隔符的字符。有效值是：@、# 和 !。

默认值

默认情况下，不指定分隔符，因此禁用组名解析。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当协商隧道时，使用分隔符解析来自用户名的隧道组名称。默认情况下，未指定分隔符，因此禁用组名解析。

示例

此示例展示 **group-delimiter** 命令，该命令将组分隔符更改为井号 (#)：

```
ciscoasa(config)# group-delimiter #
```

相关命令

命令	说明
clear configure group-delimiter	清除已配置的组分隔符。
show running-config group-delimiter	显示当前组分隔符值。
strip-group	启用或禁用条带组处理。

group-lock

要将远程用户限制为只能通过隧道组访问，请在组策略配置模式下或用户名配置模式下发出 **group-lock** 命令。要从运行配置删除 **group-lock** 属性，请使用此命令的 **no** 形式。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

语法说明

none	将 group-lock 设置为空值，从而允许无组锁定限制。防止从默认或指定组策略继承组锁定值。
value *tunnel-grp-name*	指定 ASA 要求用户连接的现有隧道组的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
组策略配置	• 是	—	• 是	—	—
用户名配置	• 是	—	• 是	—	—

使用指南

要禁用组锁定，请使用 **group-lock none** 命令。**no group-lock** 命令允许从其他组策略继承值。

组锁定通过检查在 VPN 客户端上配置的组与用户被分配到的隧道组是否相同来限制用户。如果不一样，ASA 会阻止用户进行连接。如果不配置组锁定，则 ASA 对用户进行身份验证而不考虑分配的组。

命令历史

版本	**修改**
7.0(1)	引入了此命令。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置组锁定：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# group-lock value tunnel group name
```

group-object

要向对象组添加组对象，请在配置对象时使用 **group-object** 命令。要删除组对象，请使用此命令的 **no** 形式。

group-object *obj_grp_name*

no group-object *obj_grp_name*

语法说明

obj_grp_name	标识对象组（1 到 64 个字符），可以是字母、数字以及“_”、“-”、“.”字符的任意组合。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
协议、网络、服务、icmp 类型、安全组和用户对象组配置模式	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(2)	增加了对以下功能的支持：在对象组用户配置模式下添加对象组以供与身份防火墙功能一起使用。

使用指南

group-object 命令与 **object-group** 命令一起使用，用来添加本身是对象组的对象。此子命令允许对同一种类型对象进行逻辑分组以及分层对象组的构建，以实现结构化配置。

如果对象是组对象，则允许在对象组中存在重复对象。例如，如果对象 1 既在组 A 又在组 B 中，则允许定义一个组 C，其中包括组 A 和组 B。但是，所包括的组对象不能导致组层次结构变为循环结构。例如，不允许使组 A 包括组 B，之后又使组 B 包括组 A。

分层对象组允许的最大层数为 10。

注意　ASA 不支持 IPv6 嵌套网络对象组，因此，您不能将具有 IPv6 条目的对象放到其他 IPv6 对象组下面。

示例

以下示例展示如何使用 **group-object** 命令来消除对重复主机的需求：

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network)# network-object host 172.23.56.1
ciscoasa(config-network)# network-object host 172.23.56.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network)# group-object host_grp_1
ciscoasa(config-network)# group-object host_grp_2
ciscoasa(config-network)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)# access-list all permit tcp object-group all-hosts any eq w
```

以下示例展示如何使用 **group-object** 对象命令将本地用户组添加到用户组对象：

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object-group** 命令。
object-group	定义对象组以优化配置。
show running-config object-group	显示当前对象组。

group-policy

要创建或编辑组策略，请在全局配置模式下使用 **group-policy** 命令。要从配置中删除组策略，请使用此命令的 **no** 形式。

group-policy *name* {**internal** [**from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

语法说明

external server-group *server_group*	指定组策略为外部策略，并标识 AAA 服务器组，以供 ASA 查询属性。
from *group-policy_name*	将此内部组策略属性初始化为一个预先存在的组策略的值。
internal	将组策略标识为内部策略。
name	指定组策略的名称。名称的长度最多为 64 个字符，可以包含空格。带空格的组名必须包含在双引号中，例如 “Sales Group”。
password *server_password*	提供密码，以供在从外部 AAA 服务器组检索属性时使用。密码的长度最多为 128 个字符，不能包含空格。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0.1	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

名为 “DefaultGroupPolicy” 的默认组策略在 ASA 中始终存在。但是，此默认组策略直至您为使用它而配置 ASA 时才会生效。有关配置说明，请参阅 CLI 配置指南。

使用 **group-policy attributes** 命令进入组策略配置模式，在该模式下您可以配置任何组策略属性值对。DefaultGroupPolicy 包含这些属性值对：

属性	默认值
backup-servers	keep-client-config
banner	none

属性	默认值
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

此外，还可以为组策略配置 webvpn 配置模式属性，方法有两种：在组策略配置模式下输入 **webvpn** 命令；或者输入 **group-policy attributes** 命令，然后在 group-webvpn 配置模式下输入 **webvpn** 命令。关于详细信息，请参阅 **group-policy attributes** 命令的说明。

示例

以下示例展示如何创建名为“FirstGroup”的内部组策略。

```
ciscoasa(config)# group-policy FirstGroup internal
```

以下示例展示如何创建名为“ExternalGroup”、AAA 服务器组为“BostonAAA”、密码为“12345678”的外部组策略。

```
ciscoasa(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

相关命令

命令	说明
clear configure group-policy	删除特定组策略或所有组策略的配置。
group-policy attributes	进入组策略配置模式，在该模式下您可以为指定的组策略配置属性和值，在该模式下也可以进入 webvpn 配置模式以为组配置 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 webvpn 配置模式。

group-policy attributes

要进入组策略配置模式，请在全局配置模式下使用 **group-policy attributes** 命令。要从组策略删除所有属性，请使用此命令的 **no** 形式。

group-policy *name* **attributes**

no group-policy *name* **attributes**

语法说明

name	指定组策略的名称。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在组策略配置模式下，您可以为指定的组策略配置属性值对，或者进入组策略 webvpn 配置模式以为组配置 WebVPN 属性。

属性模式下的命令语法具有以下共同特征：

- **no** 形式从运行配置中删除属性，并支持从其他组策略继承值。
- **none** 关键字将运行配置中的属性设置为空值，从而防止继承。
- 布尔型属性有用于启用和禁用设置的显式语法。

名为 DefaultGroupPolicy 的默认组策略在 ASA 上始终存在。但是，此默认组策略直至您为使用它而配置 ASA 时才会生效。有关配置说明，请参阅 CLI 配置指南。

group-policy attributes 命令进入组策略配置模式，在此模式下您可以配置任何组策略属性值对。DefaultGroupPolicy 包含这些属性值对：

属性	默认值
backup-servers	keep-client-config
banner	none
client-access-rule	none

属性	默认值
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

此外，您可以输入 **group-policy attributes** 命令，然后在组策略配置模式下输入 **webvpn** 命令，以为组策略配置 webvpn-mode 属性。有关详细信息，请参阅 **webvpn** 命令的说明（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 FirstGroup 的组策略组进入组策略属性模式：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)#
```

相关命令

命令	说明
clear configure group-policy	删除特定组策略或所有组策略的配置。
group-policy	创建、编辑或删除组策略。
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 group-webvpn 配置模式，在该模式下可以为指定的组配置 WebVPN 属性。

group-prompt

要定制当 WebVPN 用户连接到 ASA 时向其显示的 WebVPN 页面登录框的组提示，请在 webvpn 定制配置模式下使用 **group-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。

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

语法说明

text	指定对文本的更改。
style	指定样式更改。
value	要显示的实际文本或层叠样式表 (CSS) 参数（最大值是 256 个字符）。

默认值

组提示的默认文本是 “GROUP:”。

组提示的默认样式是 color:black;font-weight:bold;text-align:right。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Webvpn customization configuration	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

style 选项表示为任何有效的 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，取值范围为 0 到 255，分别表示每种颜色（红、绿、蓝）；以逗号分隔的条目用于指示彼此混合的每种颜色的强度级别。
- 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。

注意　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 Group:”，将字体粗细更改为粗体，以更改默认样式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# group-prompt text Corporate Group:
ciscoasa(config-webvpn-custom)# group-prompt style font-weight:bolder
```

相关命令

命令	说明
password-prompt	定制 WebVPN 页面的密码提示。
username-prompt	定制 WebVPN 页面的用户名提示。

group-search-timeout

要指定等待使用 **show ad-groups** 查询 Active Directory 服务器的响应的最大时间，请在 aaa-server 主机配置模式下使用 **group-search-timeout** 命令。要从配置中删除该命令，请使用该命令的 **no** 形式：

group-search-timeout *seconds*

no group-search-timeout *seconds*

语法说明

seconds	等待 Active Directory 服务器的响应的时间，从 1 秒到 300 秒。

默认值

默认值为 10 秒。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server host configuration	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入此命令。

使用指南

show ad-groups 命令只适用于使用 LDAP 的 Active Directory 服务器，该命令显示在 Active Directory 服务器上列出的组。使用 **group-search-timeout** 命令来调整等待服务器的响应的时间。

示例

以下示例将超时设置为 20 秒。

```
ciscoasa(config-aaa-server-host)#group-search-timeout 20
```

相关命令

命令	说明
ldap-group-base-dn	指定服务器在 Active Directory 的层次结构的哪个级别开始搜索动态组策略所使用的组。
show ad-groups	显示列于 Active Directory 服务器中的组。

group-url

要为组指定传入 URL 或 IP 地址，请在隧道组 webvpn 配置模式下使用 **group-url** 命令。要从列表中删除 URL，请使用此命令的 **no** 形式。

group-url *url* [**enable** | **disable**]

no group-url *url*

语法说明

disable	禁用 URL，但不从列表中删除它。
enable	启用 URL。
url	为此隧道组指定 URL 或 IP 地址。

默认值

没有默认 URL 或 IP 地址，但如果指定 URL 或 IP 地址，则默认情况下会启用它们。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组 webvpn 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

指定组 URL 或 IP 地址后，用户在登录时无需选择组。当用户登录时，ASA 在隧道组策略表中查找用户的传入 URL/ 地址。如果它发现 URL/ 地址且此命令在隧道组中启用，则 ASA 自动选择关联的隧道组并在登录窗口向用户只显示用户名和密码字段。这简化了用户界面，并且还有一个好处：绝不会向用户显示组列表。用户看到的登录窗口使用为该隧道组而配置的定制。

如果 URL/ 地址被禁用，并且配置了 **group-alias**，则还会显示组下拉列表，用户必须作出选择。

您可以为一个组配置多个 URL/ 地址。可以分别启用或禁用每个 URL/ 地址。您必须为每个指定的 URL/ 地址使用单独的 **group-url** 命令。必须指定完整 URL/ 地址，包括 HTTP 或者 HTTPS 协议。

您不能将同一个 URL/ 地址与多个组关联。ASA 在为隧道组接受 URL/ 地址之前会验证其唯一性。

示例

以下示例所显示的命令用于配置名为“test”的 WebVPN 隧道组命令并为隧道组建立两个组 URL：“http://www.cisco.com”和“https://supplier.example.com”：

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
ciscoasa(config-tunnel-webvpn)# group-url https://supplier.example.com
ciscoasa(config-tunnel-webvpn)#
```

以下示例为名为 RadiusServer 的隧道组启用组 URL http://www.cisco.com 和 http://192.168.10.10：

```
ciscoasa(config)# tunnel-group RadiusServer type webvpn
ciscoasa(config)# tunnel-group RadiusServer general-attributes
ciscoasa(config-tunnel-general)# authentication server-group RADIUS
ciscoasa(config-tunnel-general)# accounting-server-group RADIUS
ciscoasa(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com enable
ciscoasa(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
ciscoasa(config-tunnel-webvpn)#
```

相关命令

命令	说明
clear configure tunnel-group	清除整个隧道组数据库或指定的隧道组配置。
show webvpn group-url	显示指定的隧道组或所有隧道组的 URL。
tunnel-group webvpn-attributes	进入 webvpn 配置模式以配置 WebVPN 隧道组属性。

h245-tunnel-block

要在 H.323 中阻止 H.245 隧道，请在参数配置模式下使用 **h245-tunnel-block** 命令。要禁用此功能，请使用此命令的 **no** 形式。

h245-tunnel-block action [**drop-connection** | **log**]

no h245-tunnel-block action [**drop-connection** | **log**]

语法说明

drop-connection	当检测到 H.245 隧道时，丢弃呼叫设置连接。
log	当检测到 H.245 隧道时，发出日志。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何对 H.323 呼叫阻止 H.245 隧道：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# h245-tunnel-block action drop-connection
```

相关命令

命令	说明
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。

health-check

要启用集群状况检查功能，请在集群组配置模式下使用 **health-check** 命令。要禁用状况检查，请使用此命令的 **no** 形式。

health-check [**holdtime** *timeout*] [**vss-enabled**]

no health-check [**holdtime** *timeout*] [**vss-enabled**]

语法说明

holdtime *timeout*	（可选）确定在 keepalive 或接口状态消息之间的时间，此时间在 0.8 到 45 秒之间。默认值为 3 秒。
vss-enabled	如果将集群控制链路配置为 EtherChannel（推荐）且它连接到 VSS 或 vPC 对，则您可能需要启用 **vss-enabled** 选项。对于某些交换机，当 VSS/vPC 中的某个设备关闭或启动时，连接到该交换机的 EtherChannel 成员接口可能会对 ASA 呈现为启用，但是它们没有传送交换机侧的流量。如果您将 ASA 保持时间超时设置为一个较低值（如 0.8 秒），则可将 ASA 从集群中匿名删除，ASA 会将 keepalive 消息发送到这些 EtherChannel 接口之一。当您启用 **vss-enabled** 时，ASA 会将 keepalive 消息发送到集群控制链路中的所有 EtherChannel 接口上，以确保至少有一个交换机可以接收消息。

命令默认值

默认情况下启用状况检查，保持时间为 3 秒钟。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
集群组配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。
9.1(4)	我们添加了 **vss-enabled** 关键字。

使用指南

在拓扑结构发生变化时（如添加或删除数据接口、启用或禁用 ASA 或者交换机上的接口，或者添加其他交换机以组成 VSS 或 vPC 时），我们建议您使用 **no health-check** 命令来暂时禁用状况检查。在集群拓扑稳定后，必须重新启用集群状况检查功能。

成员之间的 keepalive 消息确定成员状况。如果设备在保持期内未接收到来自对等设备的任何 keepalive 消息，则对等设备被视为无响应或无法工作。接口状态消息检测链路故障。如果接口在某个设备上出现故障，但同一接口在其他设备上处于活动状态，则从集群中将该设备删除。

如果设备在保持时间内没有收到接口状态消息，则 ASA 从集群中删除成员之前所经过的时间取决于接口类型以及设备是已建立的成员还是正在加入集群。对于 EtherChannel（无论是否跨区），如果接口在已建立的成员上关闭，则 ASA 在 9 秒后删除成员。如果设备作为新成员加入集群，则 ASA 等待 45 秒，然后拒绝新设备。对于非 EtherChannel，将在 500 毫秒后删除设备，无论成员状态如何。

此命令并非引导程序配置的一部分，而是从主设备复制到从属设备上的。

示例

以下示例禁用状况检查：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时，ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接再平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable（集群组）	启用集群。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位数。
priority（集群组）	设置此设备的优先级以用于主控设备选定。

hello-interval

要指定在接口上发送的 EIGRP 问候数据包的发送间隔，请在接口配置模式下使用 **hello-interval** 命令。要将问候间隔重置为默认值，请使用此命令的 **no** 形式。

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

语法说明

as-number	指定 EIGRP 路由进程的自主系统编号。
seconds	指定在接口上发送的问候数据包的发送间隔。有效值为从 1 到 65535 秒。

默认值

默认值为 5 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

问候间隔越小，则检测到的拓扑变化越快，但也会产生更多的路由流量。该值对特定网络上的所有路由器和访问服务器必须相同。

示例

以下示例将 EIGRP 问候间隔设置为 10 秒，将保持时间设置为 30 秒：

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

相关命令

命令	说明
hold-time	配置在问候数据包中通告的 EIGRP 保持时间。

help

要显示指定命令的帮助信息，请在用户 EXEC 模式下使用 **help** 命令。

help {*command* | **?**}

语法说明

?	显示在当前权限级别和模式下可用的所有命令。
command	指定为其显示 CLI 帮助的命令。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

help 命令显示关于所有命令的帮助信息。您可以输入 **help** 命令后跟命令名，以获取某个命令的帮助。如果不指定命令名而是输入 **?**， 则会显示当前权限级别和模式下可用的所有命令。

如果启用 **pager** 命令，则在显示 24 行之后暂停显示，出现以下提示：

```
<--- More --->
```

More 提示使用的语法类似于 UNIX **more** 命令，如下所示：

- 要查看另一屏文本，请按 **Space** 键。
- 要查看下一行，请按 **Enter** 键。
- 要返回到命令行，请按 **q** 键。

示例

以下示例展示如何显示 **rename** 命令的帮助：

```
ciscoasa# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:
```

```
rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

ciscoasa#
```

以下示例展示如何通过输入命令名称和问号来显示帮助：

```
ciscoasa(config)# enable ?
usage: enable password <pwd> [encrypted]
```

在命令提示符下输入 **?** 可获得核心命令（并非 **show**、**no** 或者 **clear** 命令） 的帮助：

```
ciscoasa(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

相关命令

命令	说明
show version	显示有关操作系统软件的信息。

hidden-parameter

要在 ASA 提交到身份验证 Web 服务器中以供 SSO 身份验证的 HTTP POST 请求中指定隐藏参数，请在 aaa-server-host 配置模式下使用 **hidden-parameter** 命令。要从运行配置删除所有隐藏参数，请使用此命令的 **no** 形式。

hidden-parameter *string*

no hidden-parameter

注意　要正确配置带有 HTTP 协议的 SSO，您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	一个在表单中嵌入并发送到 SSO 服务器的隐藏参数。您可以在多行中输入此参数。每行的最大字符数为 255。所有行（整个隐藏参数）的最大字符数为 2048。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Aaa-server-host 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

这是带有 HTTP Forms 命令的 SSO。

ASA 的 WebVPN 服务器使用 HTTP POST 请求向身份验证 Web 服务器提交 SSO 身份验证请求。该请求可能要求来自 SSO HTML 表单、对于用户不可见的特定隐藏参数（用户名和密码除外）。您可以通过在从 Web 服务器上接收的表单上使用 HTTP 报头分析器来查看 Web 服务器在 POST 请求中期望的隐藏参数。

通过 **hidden-parameter** 命令，您可以指定由 Web 服务器在身份验证 POST 请求中要求的隐藏参数。如果使用报头分析器，则可以复制并粘贴整个隐藏的参数字符串，包括任何经过编码的 URL 参数。

为方便输入，您可以在连续多行中输入隐藏参数。然后，ASA 会将多行内容连接为一个隐藏参数。尽管每个隐藏参数行最多包含 255 个字符，但您可以在每行输入较少的字符。

注意　字符串中的任何问号的前面必须放置 **Ctrl+v** 转义序列。

示例

以下示例展示一个隐藏参数，此参数由四个表单条目及其值组成，并用 & 分隔。源自 POST 的四个条目和它们的值为：

- SMENC，其值为 ISO-8859-1
- SMLOCALE，其值为 US-EN
- target，其值为 https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason，其值为 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
ciscoasa(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
ciscoasa(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
ciscoasa(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	说明
action-uri	指定为 SSO 身份验证接收用户名和密码的 Web 服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
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	指定要在其上检索登录前 Cookie 的 URL。
user-parameter	在必须提交用户名以供 SSO 身份验证时指定 HTTP POST 请求参数的名称。

hidden-shares

要控制 CIFS 文件的隐藏共享的可见性，请在 group-webvpn 配置模式下使用 **hidden-shares** 命令。要从配置中删除隐藏共享选项，请使用此命令的 **no** 形式。

hidden-shares {**none** | **visible**}

[**no**] **hidden-shares** {**none** | **visible**}

语法说明

none	指定任何配置的隐藏共享均对用户不可见或不可访问。
visible	显示隐藏共享使其可供用户访问。

默认值

此命令的默认行为是无。

命令模式

下表展示可输入此命令的模式：

命令模式	防火墙模式		安全情景		
				多个	
	路由	透明	单个	情景	系统
Group-webvpn 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

隐藏共享通过位于共享名称结尾的美元符号 ($) 来标识。例如，驱动器 C 作为 C$ 来共享。采用隐藏共享时，不会显示共享文件夹，并且用户无法浏览或访问这些隐藏的资源。

hidden-shares 命令的 **no** 形式将此选项从配置中删除并禁用作为组策略属性的隐藏共享。

示例

以下示例使得与 GroupPolicy2 有关的 WebVPN CIFS 隐藏共享可见：

```
ciscoasa(config)# webvpn
ciscoasa(config-group-policy)# group-policy GroupPolicy2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# hidden-shares visible
ciscoasa(config-group-webvpn)#
```

相关命令

命令	说明
debug webvpn cifs	显示关于 CIFS 的调试消息。
group-policy attributes	进入组策略配置模式，在该模式下您可以为指定的组策略配置属性和值，在该模式下也可以进入 webvpn 配置模式以为组配置 WebVPN 属性。
url-list	配置一组 URL，以供 WebVPN 用户访问。
url-list	适用于特定用户或组策略 WebVPN 服务器和 Url 的列表。

hold-time

要在 EIGRP 问候数据包中指定由 ASA 通告的保持时间，请在接口配置模式下使用 **hold-time** 命令。要将问候间隔重置为默认值，请使用此命令的 **no** 形式。

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

语法说明

as-number	EIGRP 路由进程的自主系统编号。
seconds	指定保持时间，以秒为单位。有效值为从 1 到 65535 秒。

默认值

默认值为 15 秒。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

在 ASA 发送的 EIGRP 问候数据包中通告此值。该接口上的 EIGRP 邻居使用此值来确定 ASA 的可用性。在通告的保持时间内，如果这些邻居没有从 ASA 上接收到 问候数据包，则 EIGRP 邻居将认为 ASA 不可用。

在非常拥塞的大型网络上，默认保持时间可能不足以令所有路由器和访问服务器从其邻居那里接收问候数据包。在这种情况下，您可能希望增加保持时间。

我们建议保持时间至少为问候间隔的三倍。如果 ASA 在指定保持时间内未收到问候数据包，则认为通过此邻居的路由不可用。

增加保持时间会延迟整个网络的路由聚合。

示例

以下示例将 EIGRP 问候间隔设置为 10 秒，将保持时间设置为 30 秒：

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

相关命令

命令	说明
hello-interval	指定在接口上发送的 EIGRP 问候数据包的时间间隔。

homepage

要指定在登录后为此 WebVPN 用户或者组策略显示的网页的 URL，请在 webvpn 配置模式下使用 **homepage** 命令。要删除已配置的主页，包括通过发出 **homepage none** 命令来创建空值，请使用此命令的 **no** 形式。

homepage {**value** *url-string* | **none**}

no homepage

语法说明

none	指示没有 WebVPN 主页。设置空值，从而禁止主页。防止继承主页。
value *url-string*	提供主页的 URL。字符串必须以 http:// 或 https:// 开头。

默认值

没有默认主页。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要为与组策略关联的用户指定主页 URL，请在此命令中为 URL 字符串输入一个值。要从默认组策略继承主页，请使用此命令的 **no** 形式。**no** 选项允许从其他组策略继承值。为防止继承主页，请使用 **homepage none** 命令。

在身份验证成功后，立即向无客户端用户显示此页面。在 VPN 连接成功建立之后，AnyConnect 启动默认 Web 浏览器并访问此 URL。在 Linux 平台上，AnyConnect 目前不支持此命令，会将其忽略。

示例

以下示例展示如何为名为 FirstGroup 的组策略指定 www.example.com：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
```

相关命令

命令	说明
webvpn	允许您进入 webvpn 配置模式，以配置应用于组策略或用户名的参数。

homepage use-smart-tunnel

在使用无客户端 SSL VPN 时，要允许组策略主页使用智能隧道功能，请在组策略 webvpn 配置模式下使用 **homepage use-smart-tunnel** 命令。

homepage {**value** *url-string* | **none**}

homepage use-smart-tunnel

语法说明

none	指示没有 WebVPN 主页。设置空值，从而禁止主页。防止继承主页。
value *url-string*	提供主页的 URL。字符串必须以 http:// 或 https:// 开头。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

您可以使用 HTTP 捕获工具监控浏览器会话并验证智能隧道在 WebVPN 连接期间已经启动。您在浏览器捕获中看到的内容确定请求是否转发到网页而不存在降级以及是否使用智能隧道。如果看到诸如 https://172.16.16.23/+CSCOE+portal.html 之类的信息，则 *+CSCO** 指示内容已由 ASA 降级。在智能隧道启动时，您会看到针对特定 URL 的 **http get** 命令，不带 +CSCO*（如 GET 200 html http://mypage.example.com）。

示例

如果您考虑到供应商 V 要为合作伙伴 P 提供对其内部库存服务器页面的无客户端访问，则供应商 V 的管理员必须决定以下内容：

- 用户在登录到无客户端 SSL VPN 之后是否拥有库存页面的访问权限，无论他们是否通过无客户端门户时都是如此？
- 因为页面包括 Microsoft Silverlight 组件，智能隧道是否是理想的访问方式？
- tunnel-all 策略是否适当？因为一旦浏览器已经建立隧道，则所有隧道策略会强制所有浏览器流量通过供应商 V 的 ASA，使得合作伙伴 P 的用户无法访问内部资源。

假设库存页面在 inv.example.com (10.0.0.0) 上托管，以下示例创建仅包含一个主机的隧道策略：

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
ciscoasa(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

以下示例将一个隧道指定的隧道策略应用于合作伙伴的组策略：

```
ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

以下示例指定组策略主页并对其启用智能隧道：

```
ciscoasa(config-group-webvpn)# homepage value http://inv.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
```

host（网络对象）

要配置网络对象的主机，请在对象网络配置模式下使用 **host** 命令。要从对象删除主机，请使用此命令的 **no** 形式。

host *ip_address*

no host *ip_address*

语法说明

ip_address	标识对象的主机 IP 地址，采用 IPv4 或 IPv6 协议。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
对象配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

如果您使用不同 IP 地址配置现有网络对象，新配置将会替换现有配置。

示例

以下示例展示如何创建主机网络对象：

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

相关命令

命令	说明
clear configure object	清除所有已创建对象。
nat	实现网络对象的 NAT。
object network	创建网络对象。
object-group network	创建网络对象组。
show running-config object network	显示网络对象的配置。

host (parameters)

要指定一个要交互的、使用 RADIUS 记账的主机，请在 radius-accounting 参数配置模式下使用 **host** 命令，在策略映射类型检查 radius-accounting 子模式下使用 **parameters** 命令可进入此模式。要禁用指定主机，请使用此命令的 **no** 形式。

host *address* [**key** *secret*]

no host ***address*** [**key** *secret*]

语法说明

host	指定发送 RADIUS 记账消息的单个终端。
address	发送 RADIUS 记账消息的客户端或服务器的 IP 地址。
key	一个可选关键字，用于指定发送记账消息的无为副本的终端的密钥。
secret	发送用于验证消息的记账消息的终端的共享密钥。共享密钥最多包含 128 个字母数字字符。

默认值

默认情况下禁用 **no** 选项。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令允许有多个实例。

示例

以下示例展示如何指定带有 RADIUS 记账的主机：

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# host 209.165.202.128 key cisco123
```

相关命令

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

hostname

要设置 ASA 主机，请在全局配置模式下使用 **hostname** 命令。要恢复默认主机名，请使用此命令的 **no** 形式。

hostname *name*

no hostname [*name*]

语法说明

name	指定一个主机名，最长为 63 个字符。主机名必须以字母或数字开头和结尾，并且内部字符只能是字母、数字或连字符。

默认值

默认主机名取决于您的平台。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	您无法再使用非字母数字字符（连字符除外）。

使用指南

主机名作为命令行提示符出现，如果您建立与多个设备的会话，则主机名可帮助您跟踪您输入命令的位置。对于多情景模式，您在系统执行空间中指定的主机名会在所有情景的命令行中出现。

您在情景中可选择设置的主机名不会在命令行中出现，但可用于 **banner** 命令 **$(hostname)** 令牌。

示例

以下示例将主机名设置为 firewall1：

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

相关命令

命令	说明
banner	设置登录、当日消息标语或启用标语。
domain-name	设置默认域名。

hpm topn enable

要在通过 ASA 连接的顶部主机的 ASDM 中启用实时报告，请在全局配置模式下使用 **hpm topn enable** 命令。要禁用主机报告，请使用此命令的 **no** 形式。

hpm topn enable

no hpm topn enable

语法说明

此命令没有任何参数或关键字。

命令默认值

此命令默认禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

您可能需要禁用此命令，以最大限度地提升系统性能。此命令填充 “ASDM Home > Firewall Dashboard > Top 200 Hosts”（ASDM 主页 > 防火墙控制面板 > 顶部 200 个主机）窗格。

示例

以下示例启用顶部主机报告：

```
ciscoasa(config)# hpm topn enable
```

相关命令

命令	说明
clear configure hpm	清除 HPM 配置。
show running-config hpm	显示 HPM 配置。

hsi

要将 HSI 添加到 HSI 组以进行 H.323 协议检查，请在 hsi 组配置模式下使用 **hsi** 命令。要禁用此功能，请使用此命令的 **no** 形式。

hsi *ip_address*

no hsi *ip_address*

语法说明

ip_address	要添加的主机的 IP 地址。每个 HSI 组允许最多五个 HSI。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Hsi 组配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何将 HSI 添加到 H.323 检查策略映射的 HSI 组中：

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

相关命令

命令	说明
class-map	创建第 3/4 层类映射。
endpoint	将一个终端添加到 HSI 组。
hsi-group	创建 HSI 组。
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。

hsi-group

要为 H.323 协议检查定义 HSI 组并进入 hsi 组配置模式，请在参数配置模式下使用 **hsi-group** 命令。要禁用此功能，请使用此命令的 **no** 形式。

hsi-group *group_id*

no hsi-group *group_id*

语法说明

group_id	HSI 组 ID 号，从 0 到 2147483647。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例展示如何在 H.323 检查策略映射中配置 HSI 组：

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

相关命令

命令	说明
class-map	创建第 3/4 层类映射。
endpoint	将一个终端添加到 HSI 组。
hsi	向创建的 HSI 组添加 HSI。
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。

html-content-filter

要为此用户或组策略的 WebVPN 会话过滤 Java、ActiveX、图像、脚本和 Cookie，请在 webvpn 配置模式下使用 **html-content-filter** 命令。要删除内容过滤器，请使用此命令的 **no** 形式。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

语法说明

cookies	从图像删除 Cookie，提供受限的广告过滤和隐私。
images	删除对图像的引用（删除 <IMG> 标记）。
java	删除对 Java 和 ActiveX 的引用（删除 <EMBED>、<APPLET> 和 <OBJECT>）。
none	指示不过滤。设置空值，从而禁用过滤。防止继承过滤值。
scripts	删除对脚本的引用（删除 <SCRIPT> 标记）。

默认值

不发生过滤。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要删除所有内容过滤器，包括通过发出 **html-content-filter none** 命令创建的空值，请使用此命令的 **no** 形式，不带参数。**no** 选项允许继承其他组策略的值。为防止继承 HTML 内容过滤器，请使用 **html-content-filter none** 命令。

再次使用该命令将覆盖以前的设置。

示例

以下示例展示如何为名为 FirstGroup 的组策略设置 Java 和 ActiveX、cookies 以及图像的过滤。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# html-content-filter java cookies images
```

相关命令

命令	说明
webvpn	允许您进入 webvpn 配置模式，以配置应用于组策略或用户名的参数。 允许您进入全局配置模式以为 WebVPN 配置全局设置。

http

要指定可访问 ASA 内部的 HTTP 服务器，请在全局配置模式下使用 **http** 命令。要删除一个或多个主机，请使用此命令的 **no** 形式。要从配置中删除属性，请使用此命令的 **no** 形式，不带参数。

http *ip_address subnet_mask interface_name*

no http

语法说明

interface_name	提供主机用来访问 HTTP 服务器的 ASA 接口的名称。
ip_address	提供可以访问 HTTP 服务器的主机的 IP 地址。
subnet_mask	提供可以访问 HTTP 服务器的主机的子网掩码。

默认值

没有主机可以访问 HTTP 服务器。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何允许 IP 地址为 10.10.99.1、子网掩码为 255.255.255.255 的主机通过外部接口来访问 HTTP 服务器：

```
ciscoasa(config)# http 10.10.99.1 255.255.255.255 outside
```

下一个示例展示如何允许任何主机通过外部接口来访问 HTTP 服务器：

```
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置：禁用 HTTP 服务器并删除可以访问 HTTP 服务器的主机。
http authentication-certificate	要求通过建立与 ASA 的 HTTPS 连接的用户提供的证书来进行身份验证。
http redirect	指定 ASA 将 HTTP 连接重新定向到 HTTPS。
http server enable	启用 HTTP 服务器。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。

http authentication-certificate

要为使用 ASDM HTTPS 连接的身份验证要求证书，请在全局配置模式下使用 **http authentication-certificate** 命令。要从配置中删除该属性，请使用此命令的 **no** 版本。要从配置中删除所有 **http authentication-certificate** 命令，请使用 **no** 版本，不带参数。

ASA 针对 PKI 信任点来验证证书。如果证书未通过验证，则 ASA 关闭 SSL 连接。

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

语法说明

interface	指定要求证书身份验证的 ASA 上的接口。

默认值

HTTP 证书身份验证已禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0.3	启用了此命令以支持 **ssl certificate-authentication** 命令。
8.2.1	重新添加了此命令；为向后兼容，保留了全局 **ssl certificate-authentication** 命令。
8.4.7，9.1.3	启用了仅证书身份验证。过去，在您启用 **aaa authentication http console** 命令之后，此命令仅向用户身份验证添加证书身份验证。

使用指南

您应为每个接口配置证书身份验证，使得受信任 / 内部接口上的连接无需提供证书。您可以多次使用命令以在多个接口上启用证书身份验证。

示例

以下示例展示如何为连接到名为 outside 和 external 的客户端要求证书身份验证：

```
ciscoasa(config)# http authentication-certificate inside
ciscoasa(config)# http authentication-certificate external
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置：禁用 HTTP 服务器并删除可以访问 HTTP 服务器的主机。
http	指定可以通过 IP 地址和子网掩码来访问 HTTP 服务器的主机。指定主机用来访问 HTTP 服务器的 ASA 接口。
http redirect	指定 ASA 将 HTTP 连接重新定向到 HTTPS。
http server enable	启用 HTTP 服务器。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。
ssl authentication-certificate	为 SSL 连接要求证书。

http[s]（参数）

要为 scansafe 检查策略映射指定服务类型，请在参数配置模式下使用 **http**[**s**] 命令。要删除服务类型，请使用此命令的 **no** 形式。您可以通过首先输入 **policy-map type inspect scansafe** 命令来访问参数配置模式。

{**http** | **https**}

no {**http** | **https**}

语法说明

此命令没有任何参数或关键字。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您只能为 Scansafe 检查策略映射指定一种服务类型，或者是 **http**，或者是 **https**。没有默认值；您必须指定一种类型：

示例

以下示例创建一种检查策略映射，并将服务类型设置为 HTTP：

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
```

相关命令

命令	说明
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。
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。

命令	说明
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	配置一般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、备用服务器还是不可达。
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。
whitelist	对流量类执行白名单操作。

http-comp

要在特定组或用户的 WebVPN 连接上的 HTTP 数据启用压缩，请在组策略 webvpn 和用户名 webvpn 配置模式下使用 **http-comp** 命令。要从配置中删除命令并进行值继承，请使用此命令的 **no** 形式。

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

语法说明

gzip	指定为组或用户启用压缩。
none	指定为组或用户禁用压缩。

默认值

默认情况下，压缩设置为启用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

对于 WebVPN 连接，在全局配置模式下配置的 **compression** 命令会覆盖在组策略和用户 webvpn 配置模式下配置的 **http-comp** 命令。

示例

以下示例为组策略 sales 禁用压缩：

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# http-comp none
```

相关命令

命令	说明
compression	为所有 SVC、WebVPN 和 IPsec VPN 连接启用压缩。

http-proxy (call-home)

要为智能许可和 Smart Call Home 设置 HTTP(S) 代理，请在 call-home 模式下使用 **http-proxy** 命令。要删除代理，请使用此命令的 **no** 形式。

http-proxy *ip_address* **port** *port*

no http-proxy [*ip_address* **port** *port*]

语法说明

ip_address	设置 HTTP 代理服务器的 IP 地址。
port *port*	设置 HTTP 代理的端口号。例如，为 HTTPS 服务器使用 443。

命令默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Call-home 配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.3(2)	我们引入了此命令。

使用指南

此命令为 Smart Call Home 和智能许可设置全局 HTTP 或者 HTTPS 代理。

示例

以下示例设置 HTTP 代理：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

相关命令

命令	说明
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。
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。

命令	说明
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。
throughput level	设置智能许可的吞吐量级别。

http-proxy (dap)

要启用或禁用 HTTP 代理端口转发，请在 dap-webvpn 配置模式下使用 **http-proxy** 命令。要从配置中删除此属性，请使用此命令的 **no** 形式。

http-proxy {**enable** | **disable** | **auto-start**}

no http-proxy

语法说明

auto-start	为 DAP 记录启用并自动启动 HTTP 代理端口转发。
enable/disable	为 DAP 记录启用或禁用 HTTP 代理端口转发。

默认值

没有默认值或行为。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

ASA 可应用来自各种来源的属性值。它根据以下层次结构应用这些属性值：

1. DAP 记录
2. 用户名
3. 组策略
4. 隧道组的组策略
5. 默认组策略

属性的 DAP 值的优先级高于为用户、组策略和隧道组配置的 DAP 值。

当您启用或禁用 DAP 记录的属性时，ASA 应用并实施该值。例如，如果在 dap-webvpn 配置模式下禁用了 HTTP 代理，则 ASA 不会进一步查找值。如果为 **http-proxy** 命令使用 **no** 值，则在 DAP 记录中不存在此属性，所以，ASA 下移到用户名中的 AAA 属性，必要时下移到组策略，以查找要应用的值。

示例

以下示例展示如何为名为 Finance 的 DAP 记录启用 HTTP 代理端口转发。

```
ciscoasa (config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# http-proxy enable
ciscoasa(config-dap-webvpn)#
```

相关命令

命令	说明
dynamic-access-policy-record	创建 DAP 记录。
show running-config dynamic-access-policy-record	显示所有 DAP 记录或指定 DAP 记录正在运行的配置。

http-proxy (webvpn)

要配置 ASA 以使用外部代理服务器来处理 HTTP 请求，请在 webvpn 配置模式下使用 **http-proxy** 命令。要从配置中删除 HTTP 代理服务器，请使用此命令的 **no** 形式。

http-proxy {*host* [*port*] [**exclude** `url`] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

语法说明

host	外部 HTTP 代理服务器的主机名或 IP 地址。
pac *pacfile*	标识 PAC 文件，其中包含一个指定一个或多个代理的 JavaScript 函数。
password	（可选，仅在您指定用户名时可用）输入此关键字，以为每个 HTTP 代理请求提供一个密码，从而提供基本的代理身份验证。
password	要随同每个 HTTP 请求发送到代理服务器的密码。
port	（可选）HTTP 代理服务器使用的端口号。默认端口是 80，如果您不提供值，ASA 将使用该默认端口。范围为 1 到 65535。
url	输入要从可发送给代理服务器的 URL 中排除的一个 URL 或包含多个 URL 的列表（由逗号分隔）。字符串没有字符数限制，但整个命令不能超过 512 个字符。您可以指定文本 URL 或使用以下通配符： • ***** 匹配任意字符串，包括斜杠 (/) 和句点 (.)。此通配符必须与字母数字字符串一起使用。 • **?** 匹配任意单个字符，包括斜杠和句点。 • [*x*-*y*] 匹配 *x* 与 *y* 之间的任何单个字符，其中 *x* 代表 ANSI 字符集中的一个字符，*y* 代表 ANSI 字符集中的另一个字符。 • [**!***x*-*y*] 匹配不在此范围内的任何单个字符。
username	（可选）输入此关键字，为每个 HTTP 代理请求随附一个用户名，以提供基本的代理身份验证。
username	随同每个 HTTP 请求将用户名发送给代理服务器。

默认值

默认情况下，不配置任何 HTTP 代理服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	添加了 **exclude**、**username** 和 **password** 关键字。

使用指南

要求通过组织控制的服务器来访问互联网，这为通过过滤来确保安全互联网访问和管理控制提供了又一个机会。

ASA 仅支持 **http-proxy** 命令的一个实例。如果在运行配置中已存在此命令的一个实例，之后又输入了一个实例，则 CLI 会覆盖之前的实例。如果您输入 **show running-config webvpn** 命令，则 CLI 会列出运行配置中的所有 **http-proxy** 命令。如果响应未列出 **http -proxy** 命令，则说明不存在此命令。

注意　在 **http-proxy** 中不支持代理 NTLM 身份验证。仅支持无身份验证和采用基本身份验证的代理。

示例

以下示例展示如何配置使用 IP 地址为 209.165.201.2 的 HTTP 代理服务器（使用默认端口 443）：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# http-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

以下示例展示如何配置使用同一个代理服务器，并随同每个 HTTP 请求发送用户名和密码：

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

以下示例展示相同的命令，但当 ASA 接收 HTTP 请求中的特定 URL www.example.com 时除外，此时它解析请求而不是将其传递给代理服务器：

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

以下示例展示如何使用 **exclude** 选项：

```
ciscoasa(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
ciscoasa(config-webvpn)
```

以下示例展示如何使用 **pac** 选项。

```
ciscoasa(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

相关命令

命令	说明
https-proxy	配置使用外部代理服务器，以处理 HTTPS 请求。
show running-config webvpn	显示 SSL VPN 的运行配置，包括所有 HTTP 和 HTTPS 代理服务器。

http redirect

要指定 ASA 将 HTTP 重新定向到 HTTPS 连接，请在全局配置模式下使用 **http redirect** 命令。要从配置中删除指定的 **http redirect** 命令，请使用此命令的 **no** 形式。要从配置中删除所有 **http redirect** 命令，请使用此命令的 **no** 形式，不带参数。

http redirect *interface* [*port*]

no http redirect [*interface*]

语法说明

interface	标识 ASA 为其将 HTTP 请求重新定向到 HTTPS 的接口。
port	标识 ASA 用于侦听 HTTP 请求的端口，之后它将此请求重新定向到 HTTPS。默认情况下，它侦听端口 80，

默认值

HTTP 重新定向被禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

接口要求一个允许 HTTP 的访问列表。否则 ASA 无法侦听端口 80 或者您为 HTTP 配置的其他端口。

如果 **http redirect** 重新定向命令失败，将显示以下消息：

```
"TCP port <port_number> on interface <interface_name> is in use by another feature.Please choose a different port for the HTTP redirect service"
```

为 HTTP 重新定向服务使用其他端口。

示例

以下示例展示如何为内部接口配置 HTTP 重新定向，从而保留默认端口 80：

```
ciscoasa(config)# http redirect inside
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置：禁用 HTTP 服务器并删除可以访问 HTTP 服务器的主机。
http	指定可以通过 IP 地址和子网掩码来访问 HTTP 服务器的主机。指定主机用来访问 HTTP 服务器的 ASA 接口。
http authentication-certificate	要求通过建立与 ASA 的 HTTPS 连接的用户提供的证书来进行身份验证。
http server enable	启用 HTTP 服务器。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。

http server enable

要启用 ASA HTTP 服务器，请在全局配置模式下使用 **http server enable** 命令。要禁用 HTTP 服务器，请使用此命令的 **no** 形式。

http server enable [*port*]

语法说明 no http

port	为 HTTP 连接使用的端口。范围为 1 65535。默认端口为 443。

默认值

HTTP 服务器被禁用。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例展示如何启用 HTTP 服务器。

```
ciscoasa(config)# http server enable
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置：禁用 HTTP 服务器并删除可以访问 HTTP 服务器的主机。
http	指定可以通过 IP 地址和子网掩码来访问 HTTP 服务器的主机。指定主机用来访问 HTTP 服务器的 ASA 接口。
http authentication-certificate	要求通过建立与 ASA 的 HTTPS 连接的用户提供的证书来进行身份验证。
http redirect	指定 ASA 将 HTTP 连接重新定向到 HTTPS。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。

http server idle-timeout

要设置与 ASA 的 ASDM 连接的空闲超时，请在全局配置模式下使用 **http server idle-timeout** 命令。要禁用超时，请使用此命令的 **no** 形式。

http server idle-timeout [*minutes*]

no http server idle-timeout [*minutes*]

语法说明

minutes	空闲超时，从 1 分钟到 1440 分钟。

默认值

默认设置为 20 分钟。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下示例将 ASDM 会话的空闲超时设置为 500 分钟：

```
ciscoasa(config)# http server idle-timeout 500
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置，禁用 HTTP 服务器，并删除可以访问 HTTP 服务器的主机。
http	指定可通过 IP 地址和子网掩码访问 HTTP 服务器的主机以及主机用来访问 HTTP 服务器的接口。
http authentication-certificate	要求通过建立与 ASA 的 HTTPS 连接的用户提供的证书来进行身份验证。
http server enable	为 ASDM 会话启用 HTTP 服务器。
http server session-timeout	将 ASDM 会话的会话时间限制为 ASA。
http redirect	指定 ASA 将 HTTP 连接重新定向到 HTTPS。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。

http server session-timeout

要设置与 ASA 的 ASDM 连接的会话超时，请在全局配置模式下使用 **http server session-timeout** 命令。要禁用超时，请使用此命令的 **no** 形式。

http server session-timeout [*minutes*]

no http server session-timeout [*minutes*]

语法说明

minutes	会话超时，从 1 分钟到 1440 分钟。

默认值

会话超时被禁用。ASDM 连接没有会话时间限制。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

示例

以下示例将 ASDM 连接的会话超时设置为 1000 分钟：

```
ciscoasa(config)# http server session-timeout 1000
```

相关命令

命令	说明
clear configure http	删除 HTTP 配置：禁用 HTTP 服务器并删除可以访问 HTTP 服务器的主机。
http	指定可通过 IP 地址和子网掩码访问 HTTP 服务器的主机以及主机用来访问 HTTP 服务器的接口。
http authentication-certificate	要求通过建立与 ASA 的 HTTPS 连接的用户提供的证书来进行身份验证。
http server enable	为 ASDM 会话启用 HTTP 服务器。
http server idle-timeout	将 ASDM 会话的空闲时间限制为 ASA。
http redirect	指定 ASA 将 HTTP 连接重新定向到 HTTPS。
show running-config http	显示可以访问 HTTP 服务器的主机以及 HTTP 服务器是否启用。

https-proxy

要配置 ASA 来使用外部代理服务器以处理 HTTPS 请求，请在 webvpn 配置模式下使用 **https-proxy** 命令。要从配置中删除 HTTPS 代理服务器，请使用此命令的 **no** 形式。

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

语法说明

host	外部 HTTPS 代理服务器的主机名或 IP 地址。
password	（可选，仅在您指定用户名时可用）输入此关键字，以为每个 HTTP 代理请求提供一个密码，从而提供基本的代理身份验证。
password	要随同每个 HTTPS 请求发送到代理服务器的密码。
port	（可选）HTTPS 代理服务器使用的端口号。默认端口是 443，如果您不提供值，ASA 将使用该默认端口。范围为 1 到 65535。
url	输入要从可发送给代理服务器的 URL 中排除的一个 URL 或包含多个 URL 的列表（由逗号分隔）。字符串没有字符数限制，但整个命令不能超过 512 个字符。您可以指定文本 URL 或使用以下通配符： • ***** 匹配任意字符串，包括斜杠 (/) 和句点 (.)。此通配符必须与字母数字字符串一起使用。 • **?** 匹配任意单个字符，包括斜杠和句点。 • [*x*-*y*] 匹配 *x* 与 *y* 之间的任何单个字符，其中 *x* 代表 ANSI 字符集中的一个字符，*y* 代表 ANSI 字符集中的另一个字符。 • [**!***x*-*y*] 匹配不在此范围内的任何单个字符。
username	（可选）输入此关键字，为每个 HTTP 代理请求随附一个用户名，以提供基本的代理身份验证。
username	要随同每个 HTTPS 请求发送给代理服务器的用户名。

默认值

默认情况下，不配置任何 HTTPS 代理服务器。

命令模式

下表展示可输入此命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
WebVPN 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	添加了 **exclude**、**username** 和 **password** 关键字。

使用指南

要求通过组织控制的服务器来访问互联网，这为通过过滤来确保安全互联网访问和管理控制提供了又一个机会。

ASA 仅支持 **https-proxy** 命令的一个实例。如果在运行配置中已存在此命令的一个实例，之后又输入了一个实例，则 CLI 会覆盖之前的实例。如果您输入 **show running-config webvpn** 命令，则 CLI 会列出运行配置中的所有 **https-proxy** 命令。如果响应未列出 **https-proxy** 命令，则说明不存在此命令。

示例

以下示例展示如何配置使用 IP 地址为 209.165.201.2 的 HTTP 代理服务器（使用默认端口 443）：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# https-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

以下示例展示如何配置使用同一个代理服务器，并随同每个 HTTP 请求发送用户名和密码：

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

以下示例展示同一个命令，但当 ASA 接收 HTTPS 请求中的特定 URL www.example.com 时除外，此时它解析请求而不是将其传递给代理服务器：

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

以下示例展示如何使用 **exclude** 选项：

```
ciscoasa(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
ciscoasa(config-webvpn)
```

以下示例展示如何使用 **pac** 选项。

```
ciscoasa(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

相关命令

命令	说明
http-proxy	配置使用外部代理服务器，以处理 HTTP 请求。
show running-config webvpn	显示 SSL VPN 的运行配置，包括所有 HTTP 和 HTTPS 代理服务器。

hw-module module allow-ip

对于 ASA 5505 上的 AIP SSC，要设置允许访问管理 IP 地址的主机，请在特权 EXEC 模式下使用 **hw-module module** 命令。

hw-module module 1 allow-ip *ip_address netmask*

语法说明

1	指定插槽编号，编号始终为 1。
ip_ address	指定主机 IP 地址。
netmask	指定子网掩码。

默认值

在出厂默认配置中，允许 IP 地址从 192.168.1.5 到 192.168.1.254 的以下主机管理 IPS 模块。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

仅当 SSC 处于启用状态时此命令才有效。

这些设置会写入到 IPS 应用配置而不是 ASA 配置中。您可使用 **show module details** 命令从 ASA 中查看这些设置。

您也可以从 IPS CLI 使用 IPS 应用 **setup** 命令配置此设置。

示例

以下示例展示如何在 SSC 上配置主机参数：

```
ciscoasa# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

相关命令

命令	说明
hw-module module ip	配置 AIP SSC 管理地址。
show module	显示模块状态信息。

hw-module module ip

对于 ASA 5505 上的 AIP SSC，要配置管理 IP 地址，请在特权 EXEC 模式下使用 **hw-module module ip** 命令。

hw-module module 1 ip *ip_address netmask gateway*

语法说明

1	指定插槽编号，编号始终为 1。
gateway	指定网关 IP 地址。
ip_address	指定管理 IP 地址。
netmask	指定子网掩码。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

确保此地址与 ASA VLAN IP 地址处于同一子网中。例如，如果您将 10.1.1.1 分配给 ASA 的 VLAN，则应为 IPS 管理地址分配该网络上的其他 IP 地址，例如 10.1.1.2。

如果管理站位于直连的 ASA 网络上，则将网关设置为分配给 IPS 管理 VLAN 的 ASA IP 地址。在所述的示例中，将网关设置为 10.1.1.1。如果管理站位于远程网络上，则将网关设置为 IPS 管理 VLAN 上的上游路由器的地址。

注意　这些设置会写入到 IPS 应用配置而不是 ASA 配置中。您可使用 **show module details** 命令从 ASA 中查看这些设置。

您也可以从 IPS CLI 使用 IPS 应用 **setup** 命令配置此设置。

示例

以下示例展示如何配置 IPS 模块的管理地址：

```
ciscoasa# hw-module module 1 ip 209.165.200.254 255.255.255.224 209.165.200.225
```

相关命令

命令	说明
hw-module module allow-ip	配置 AIP SSC 管理主机地址。
show module	显示模块状态信息。

hw-module module password-reset

要将硬件模块上默认管理员用户的密码重置为默认值，请在特权 EXEC 模式下使用 **hw-module module password-reset** 命令。

hw-module module 1 password-reset

语法说明

1	指定插槽编号，编号始终为 1。

默认值

默认用户名和密码取决于您的模块：

- IPS 模块 - 用户名：**cisco**；密码：**cisco**
- CSC 模块 - 用户名：**cisco**；密码：**cisco**
- ASA CX 模块 - 用户名：**admin**；密码：**Admin123**

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.2(2)	引入了此命令。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。

使用指南

仅当硬件模块处于工作状态并支持密码重置时此命令才有效。对于 IPS，如果模块正在运行 IPS 版本 6.0 或更高版本，则支持密码重置。在重置密码后，您应该使用模块应用将密码更改为唯一值。重置模块密码会导致模块重启。在模块重启时服务不可用，重启可能需要几分钟。您可以运行 **show module** 命令来监控模块状态。

此命令始终提示予以确认。如果命令成功，则不会出现其他输出。如果命令失败，则会出现错误消息，说明失败原因。可能的错误消息如下：

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type
```

```
The module in slot 1 does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

示例

以下示例将重置插槽 1 中硬件模块上的密码：

```
ciscoasa(config)# hw-module module 1 password-reset
Reset the password on module in slot 1?[confirm] y
```

相关命令

命令	说明
hw-module module recover	从 TFTP 服务器加载恢复映像以恢复模块。
hw-module module reload	重新加载模块软件。
hw-module module reset	关闭并重置模块硬件。
hw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

hw-module module recover

要从 TFTP 服务器将恢复软件映像加载到安装的模块，或者要配置网络设置来访问 TFTP 服务器，请在特权 EXEC 模式下使用 **hw-module module recover** 命令。您可能需要使用此命令来恢复模块，例如在模块无法加载本地映像时。

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

语法说明

1	指定插槽编号，编号始终为 1。
boot	根据 **configure** 关键字设置来启动此模块的恢复并下载恢复映像。之后从新映像重启模块。
configure	配置网络参数以下载恢复映像。如果在 **configure** 关键字后没有输入网络参数，则系统会提示您输入所有参数。此命令会提示您为 TFTP 服务器输入 URL、管理接口 IP 地址和网络掩码、网关地址以及 VLAN ID。在 ROMMON 中配置这些网络参数；您在模块应用配置中配置的网络参数对于 ROMMON 不可用，因此，您必须在这里单独设置。
gateway *gateway_ip_address*	（可选）用于通过 SSM 管理接口来访问 TFTP 服务器的网关 IP 地址。
ip *module_address*	（可选）模块管理接口的 IP 地址。
stop	停止恢复操作并停止下载恢复映像。模块从原始映像启动。在使用 **hw-module module recover boot** 命令开始恢复之后，必须在 30 到 45 秒内输入此命令。如果在此期间过后发出 **stop** 命令，则可能会导致意外结果，例如模块变为无响应。
url *tfp_url*	（可选）TFTP 服务器上的映像的 URL，使用以下格式： **tftp://***server*/[*path*/]*filename*
vlan *vlan_id*	（可选）指定管理接口的 VLAN ID。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果模块失败，并且模块应用映像无法运行，可以从 TFTP 服务器将新映像重新安装到模块上。

注意　请勿在模块软件中使用 **upgrade** 命令来安装映像。

请确保您指定的 TFTP 服务器可以传输大小高达 60 MB 的文件。此过程大约需要 15 分钟，具体取决于您的网络状况和映像的大小。

此命令仅在模块处于启用、关闭、无响应或恢复状态时才可用。有关状态信息，请参阅 **show module** 命令。

您可以使用 **show module 1 recover** 命令来查看恢复配置。

注意　以下模块支持此命令：ASA CX、ASA FirePOWER。

示例

以下示例设置模块以从 TFTP 服务器下载映像：

```
ciscoasa# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

以下示例恢复模块：

```
ciscoasa# hw-module module 1 recover boot
The module in slot 1 will be recovered.This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1?[confirm]
```

相关命令

命令	说明
debug module-boot	显示关于模块引导进程的调试消息。
hw-module module reset	关闭模块并执行硬件重置。
hw-module module reload	重新加载模块软件。
hw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

hw-module module reload

要为物理模块重新加载模块软件，请在特权 EXEC 模式下使用 **hw-module module reload** 命令。

hw-module module 1 reload

语法说明

1	指定插槽编号，编号始终为 1。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
9.2(1)	我们增加了对 ASA FirePOWER 模块的支持。

使用指南

此命令不同于 **hw-module module reset** 命令，该命令在重新加载模块之前也执行硬件重置。仅在模块处于启用状态时此命令才有效。有关状态信息，请参阅 **show module** 命令。

示例

以下示例重新加载插槽 1 中的模块：

```
ciscoasa# hw-module module 1 reload
Reload module in slot 1?[confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
hw-module module recover	从 TFTP 服务器加载恢复映像以恢复模块。
hw-module module reset	关闭模块并执行硬件重置。

命令	说明
hw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

hw-module module reset

要重置模块硬件并重新加载模块软件，请在特权 EXEC 模式下使用 **hw-module module reset** 命令。

hw-module module 1 reset

语法说明

1	指定插槽编号，编号始终为 1。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
9.2(1)	我们增加了对 ASA FirePOWER 模块的支持。

使用指南

当模块处于工作状态时，**hw-module module reset** 命令提示您在重置前关闭软件。

您可以使用 **hw-module module recover** 命令恢复模块（如果支持）。如果在模块处于恢复状态时输入 **hw-module module reset** 命令，则模块不会中断恢复过程。**hw-module module** reset 命令执行模块的硬件重置，并且模块恢复在硬件重置后继续。如果模块挂起，在恢复期间您可能希望重置模块；硬件重置可能会解决此问题。

此命令不同于 **hw-module module reload** 命令，后者只重新加载软件，不执行硬件重置。

此命令仅在模块状态为启用、关闭、无响应或恢复时才可用。有关状态信息，请参阅 **show module** 命令。

示例

以下示例重置插槽 1 中处于工作状态的模块：

```
ciscoasa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1?[confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
hw-module module recover	从 TFTP 服务器加载恢复映像以恢复模块。
hw-module module reload	重新加载模块软件。
hw-module module shutdown	关闭模块软件，为电源关闭做好准备，不会失去配置数据。
show module	显示模块信息。

hw-module module shutdown

要关闭模块软件，请在特权 EXEC 模式下使用 **hw-module module shutdown** 命令。

hw-module module 1 shutdown

语法说明

1	指定插槽编号，编号始终为 1。

默认值

没有默认行为或值。

命令模式

下表展示可输入此命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(4.1)	我们增加了对 ASA CX 模块的支持。
9.2(1)	我们增加了对 ASA FirePOWER 模块的支持。

使用指南

关闭模块软件使得模块可以安全断电而不会丢失配置数据。

仅在模块状态为启用或无响应时此命令才有效。有关状态信息，请参阅 **show module** 命令。

示例

以下示例关闭插槽 1 中的模块：

```
ciscoasa# hw-module module 1 shutdown
Shutdown module in slot 1?[confirm] y
Shutdown issued for module in slot 1
ciscoasa#
%XXX-5-505001: Module in slot 1 is shutting down.Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

相关命令

命令	说明
debug module-boot	显示关于模块引导过程的调试消息。
hw-module module recover	从 TFTP 服务器加载恢复映像以恢复模块。

命令	说明
hw-module module reload	重新加载模块软件。
hw-module module reset	关闭模块并执行硬件重置。
show module	显示模块信息。