

q - res

- queue-limit (priority-queue)， 第 3 页
- queue-limit (tcp-map)， 第 5 页
- quick-start， 第 7 页
- quit， 第 9 页
- quota management-session， 第 11 页
- radius-common-pw， 第 13 页
- radius-reject-message， 第 15 页
- radius-with-expiry (已弃用)， 第 16 页
- raid， 第 18 页
- range， 第 20 页
- ras-rcf-pinholes， 第 22 页
- rate-limit， 第 24 页
- reactivation-mode， 第 26 页
- record-entry， 第 28 页
- record-route， 第 30 页
- redirect-fqdn， 第 32 页
- redistribute (ipv6 router ospf)， 第 34 页
- redistribute (router eigrp)， 第 36 页
- redistribute (router ospf)， 第 38 页
- redistribute (router rip)， 第 41 页
- redistribute isis， 第 43 页
- redundant-interface， 第 45 页
- regex， 第 47 页
- reload， 第 52 页
- remote-access threshold session-threshold-exceeded， 第 55 页
- rename (class-map)， 第 56 页
- rename (EXEC 特权)， 第 57 页
- renewal-reminder， 第 59 页
- replication http， 第 61 页
- request-command deny， 第 63 页

- request-data-size， 第 65 页
- request-queue， 第 67 页
- request-timeout (已弃用)， 第 69 页
- reserved-bits， 第 71 页
- reserve-port-protect， 第 73 页
- reset， 第 74 页
- resolver， 第 76 页
- responder-only， 第 77 页
- rest-api（已弃用），第 79 页
- restore， 第 81 页

queue-limit (priority-queue)

要指定优先级队列的深度，请使用优先级 **queue-limit**队列配置模式下的命令。要删除此规范，请使用此 **no**命令的形式。

注释 ASA 5580万兆以太网接口不支持此命令。（ASA 5585-X 上的优先级队列支持十千兆以太网接口。）ASA 5512-X 至 ASA 5555-X 管理接口也不支持此命令。ASA 服务模块不支持此命令。

queue-limit*number-of-packets*
no queue-limit*number-of-packets*

Syntax Description

number-of-packets	指定接口开始丢弃数据包之前，可以排队（即缓冲）的低延迟或正常优先级数据包的最大数量。数值范围的上限在运行时动态确定。要查看此限制，请在命令行上输入**help**或。**?**关键的决定因素是设备上支持的队列和可用的内存所需的内存。队列不得超过可用内存。理论最大数据包数为 2147483647。

Command Default

默认队列限制为 1024 个数据包。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
优先级队列配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

ASA 允许两类流量：针对高优先级、延迟敏感流量（例如语音和视频）的低延迟排队 (LLQ) 以及针对所有其他流量的默认尽力服务。ASA 识别优先级流量并实施适当的服务质量 (QoS) 策略。您可以配置的规模和深度优先级队列，以优化流量。

注释 您 必须 配置 **priority-queue** 命令才能为接口启用优先级排队。

您可以将一个 **priority-queue**命令应用于该命令可定义的 **nameif**任何接口。

该**priority-queue**命令进入优先级队列配置模式，如提示符所示。在优先级队列配置模式下，您可以配置在任何给定时间传输队列中允许的最大数据包数量（**tx-ring-limit**命令）以及在丢弃数据包之前允许缓冲的任一类型（优先级或尽力而为）的数据包数量（**queue-limit**命令）。

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

由于队列大小有限制，队列可以填满和溢出。如果队列已满，任何额外的数据包无法进入队列，并将丢弃。这是 尾部丢 弃。为了避免队列填满，您 **queue-limit**可以使用命令增加队列缓冲区大小。

CR_Examples

以下示例为名为 test 的接口配置优先级队列，指定队列限制为 234 个数据包，传输队列限制为 3 个数据包。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

Related Commands

命令	说明
clearconfigurepriority-queue	指定接口的当前优先级队列配置中移除。
priority-queue	配置优先级队列。在接口上。
showpriority-queuestatistics	显示指定接口的优先级队列统计信息。
showrunning-config[all]priority-queue	显示当前优先级队列配置。如果指定**all**关键字，此命令将显示所有当前优先级队列、队列限制和 tx-ring-limit 配置值。
tx-ring-limit	设置可在任何给定时间在以太网传输驱动器中排队的数据包的最大数量。

queue-limit (tcp-map)

如要配置TCP连接可缓冲并可排序的最大无序数据包数量，请在tcp-map配置模式下使用**queue-limit**命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令属于使用**setconnectionadvanced-options**命令启用的 TCP 规范化策略的一部分。

queue-limit*pkt_num***timeout***seconds*
no queue-limit

Syntax Description

pkt_num	指定 TCP 连接中可以缓冲并按顺序排列的无序数据包的最大数量，介于 1 到 250 之间。默认值为0，表示禁用此设置，并根据流量类型使用默认系统队列限制。有关详细信息，请参阅“使用指南”部分。
timeout 秒	（可选）设置无序数据包在缓冲区中保留的最长时间，介于 1 到 20 秒之间。默认值为 4 秒。如果数据包没有按顺序排列并在超时时间内传递，那么它们就会被丢弃。如果*pkt_num*参数设置为0，则无法更改任何流量的超时时间；您需要将限制设置为1或以上才能使关**timeout**键字生效。

Command Default

默认设置为 0，表示已禁用此命令。

默认的超时时间为 4 秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(4)/8.0(4)	添加了 **timeout** 关键字。

使用指南

要启用 TCP 规范化，请使用模块化策略框架：

1.tcp-map- 标识 TCP 规范化操作。

- **a.queue-limit**— 在 tcp-map 配置模式下，可以输入**queue-limit** 命令和许多其他命令。

2.class-map- 标识要对其执行 TCP 规范化的流量。

3.policy-map- 确定与每个类映射关联的操作。

- **a.**—**class**确定您想要执行操作的类映射。
- **b.setconnectionadvanced-options**-标识您创建的 tcp-map。

4.service-policy- 向接口或全局分配策略映射。

如果您未启用 TCP 规范化，或者该 **queue-limit**命令设置为默认值 0（即禁用），则根据流量类型使用默认系统队列限制：

- 应用程序检查（命 **inspect**令）、IPS（命 **ips**令）和 TCP 检查重传（TCP map 命令）的连接的 **check-retransmission** 队列限制为 3 个数据包。如果 ASA 收到具有不同窗口大小的 TCP 数据包，则队列限制会动态变化以符合传送的设置。
- 对于其他 TCP 连接，无序数据包会按原样通过。

如果将该 **queue-limit**命令设置为 1 或以上，则所有 TCP 流量允许的无序数据包数量均与此设置匹配。例如，对于应用程序检查、IPS 和 TCP 检查重传流量，将忽略 TCP 数据包中通告的任何设置，而采用该 **queue-limit**设置。对于其他 TCP 流量，现在会缓冲无序数据包并将其按顺序排列，而不是按原样通过。

CR_Examples

以下示例将所有 Telnet 连接的队列限制设置为 8 个数据包，将缓冲区超时设置为 6 秒：

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

命令	说明
class-map	识别服务策略的流量。
policy-map	标识要应用于服务策略中的流量的操作。
setconnectionadvanced-options	启用 TCP 规范化。
service-policy	将服务策略应用到接口。
show running-config tcp-map	显示 TCP 映射配置。
tcp-map	创建 TCP 映射，并允许对 tcp-map 配置模式的访问。

quick-start

要定义在具有 IP 选项检查的数据包头中出现快速启动 (QS) 选项时的操作，请在 **quick-start** 参数配置模式下使用该命令。要禁用此功能，请使用此**no** 命令的形式。

quick-startaction { **allow** | **clear** }
no quick-startaction { **allow** | **clear** }

Syntax Description

allow	允许包含快速启动 IP 选项的数据包。
clear	从数据包头中删除快速启动选项，然后允许数据包。

Command Default

默认情况下，IP 选项检查会丢弃包含快速启动 IP 选项的数据包。

您可以使用 IP **default**选项检查策略映射中的命令更改默认值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.5(1)	添加了此命令。

使用指南

此命令可配置的 IP 选项检查策略映射中。

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

CR_Examples

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

Related Commands

命令	说明
class	在策略映射中标识类映射名称。

命令	说明
class-maptypeinspect	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。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

quit

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 **quit**命令。

quit

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您还可以使用按键序列 **CtrlZ** 退出全局配置（及更高级别）模式。此按键序列不适用于特权或用户 EXEC 模式。

在特权或用户 EXEC 模式下输入 **quit**命令时，可从 ASA 注销。使用该 **disable**命令从特权 EXEC 模式返回到用户 EXEC 模式。

CR_Examples

以下示例显示如何使用 **quit**命令退出全局配置模式，然后从会话中注销：

```
ciscoasa(config)# quit
ciscoasa# quit
Logoff
```

以下示例显示如何使用 **quit**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)# quit
ciscoasa# disable
ciscoasa>
```

Related Commands

命令	说明
exit	退出配置模式或者从特权或用户 EXEC 模式中注销。

quota management-session

要设置 ASA 上允许的最大汇聚管理会话数（每用户每协议管理会话），请在全局配置模式下使用 **quotamanagement-session**命令。要将配额设置为默认值，请使用此命令的 **no**形式。

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*
no quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

Syntax Description

number	指定允许同时进行的 ASDM、SSH 和 Telnet 会话的最大数量。（9.12 及更高版本）当不输入任何其他关键字时，此参数将设置 1 到 15 之间的会话总数。默认值为 15。（9.10 和更低版本）有效值的范围为 0（无限制）到 10,000。
ssh	设置最大 SSH 会话数，介于 1 到 5 之间。默认值为 5。
telnet	设置最大 Telnet 会话数，介于 1 到 5 之间。默认值为 5。
http	设置最大 HTTPS（ASDM）会话数，介于 1 和 5 之间。默认值为 5。
user	设置每个用户的最大会话数，介于 1 到 5 之间。默认值为 5。

Command Default

（9.12 和更高版本）合计默认值为 15。

SSH、Telnet、HTTP 和用户的默认值为 5。

（9.10 及更早版本）默认值为 0，表示没有会话限制。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.1(2)	添加了此命令。
9.12(1)	现在，您可以在情景中而不是在系统中输入此命令。现在，除了合计限制外，您还可以设置每个用户和每个协议的限制。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。

使用指南

达到配额时，后续管理会话请求将被拒绝，并生成系统日志消息。管理会话配额机制永远不会阻止控制台会话，以防止设备锁定。

注释 在多情景模式下，如果最大 ASDM 会话数固定为 5，则无法配置会话数。

注释 如果您还使用该命令为每个上下文的最大管理会话（SSH 等）设置资源限 **limit-resource**制，则将使用较低的值。

CR_Examples

以下示例将汇聚管理会话配额配置为 8，并将单个会话限制配置为不同的数量：

```
ciscoasa
(config)#
quota management-session 8
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

Related Commands

命令	说明
showrunquotamanagement-session	显示管理会话配额的当前值。
showquotamanagement-session	显示管理会话的统计信息。

radius-common-pw

要指定通过 ASA 访问 RADIUS 授权服务器的所有用户使用的通用密 **radius-common-pw** 码，请在 aaa-server 主机配置模式下使用该命令。要删除此规范，请使用此 **no**命令的形式。

radius-common-pw字符串
no radius-common-pw

Syntax Description

string 区分大小写的字母数字关键字，最多 127 个字符，用作与 RADIUS 服务器进行的所有授权交易的通用密码。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
aaa-server host	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令仅适用于 RADIUS 授权服务器。

RADIUS 授权服务器要求每个连接用户提供密码和用户名。ASA 自动提供用户名。在此输入密码。RADIUS 服务器管理员必须将 RADIUS 服务器配置为将此密码与通过此 ASA 获得服务器访问权限的每个用户相关联。请务必将此信息提供给 RADIUS 服务器管理员。

如果没有指定公用用户密码，则每个用户密码就是用户名。如果您将用户名用于公用用户密码，则出于安全预防措施，请勿在网络上的任何其他位置使用 RADIUS 服务器进行授权。

13-125



注释 字符串 参数实质上是一个空格填充符。RADIUS 服务器期望并需要该信息，但不使用它。用户不需要知道它。

CR_Examples

以下示例在主机“1.2.3.4”上配置名为“svrgrp1”的 RADIUS AAA 服务器组，将超时间隔设置为 9 秒，将重试间隔设置为 7 秒，并将 RADIUS Commnon 密码配置为“allauthpw”。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)#
radius-common-pw allauthpw
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

命令	说明
aaa-serverhost	进入 aaa-server 主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
clearconfigureaaa-server	从配置中删除所有 AAA 命令语句。
showrunning-configaaa-server	显示所有 AAA 服务器、特定服务器组、特定组中的特定服务器或特定协议的 AAA 服务器统计信息。

radius-reject-message

要在身份验证被拒绝时在登录屏幕上显示 RADIUS 拒绝消息，请使用隧道组 webvpn 属性配置模式下的 **radius-eject-message**命令。要从配置中删除命令，请使用以 **no**下命令形式：

radius-reject-message
no radius-reject-message

Command Default

默认设置为禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Tunnel-group webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

如果要向远程用户显示有关身份验证失败的 RADIUS 消息，请启用此命令。

CR_Examples

以下示例对名为 engineering 的连接配置文件启用 RADIUS 拒绝消息的显示：

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (已弃用)



注释 支持此命令的最后一个版本是版本 8.0(1)。

要让 ASA 在身份验证期间使用 MS-CHAPv2 与用户协商密码更新，请在 tunnel-group ipsec-attributes 配置模式下使用 **radius-with-expiry** 命令。要返回默认值，请使用此**no**命令形式。

radius-with-expiry
no radius-with-expiry

Syntax Description

此命令没有任何参数或关键字。

Command Default

该命令的默认设置是禁用的。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
7.1(1)	此命令已弃用。 **password-management** 命令将取代它。该 **no**命令的 **radius-with-expiry**形式不再受支持。
8.0(2)	此命令已弃用。

使用指南

您只能将此属性应用于 IPSec 远程访问隧道组类型。如果尚未配置 RADIUS 身份验证，ASA 将忽略此命令。

CR_Examples

以下示例在 config-ipsec 配置模式下为名为 remotegrp 的远程访问隧道组配置 Radius 过期：

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

Related Commands

命令	说明
clearconfiguretunnel-group	清除所有配置的隧道组。
password-management	启用密码管理。在隧道组常规属性配置模式下，此命令取代该 **radius-with-expiry**命令。
showrunning-configtunnel-group	显示指示的证书映射条目。
tunnel-group ipsec-attributes	配置该组的隧道组 ipsec 属性。

raid

要管理 RAID 中的 SSD，请使用特权 EXEC 模式下的 **raid**命令。



注释 仅在 Secure Firewall 3100 上支持此命令。

raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	将 SSD 添加到 RAID。将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。
psid	如果您添加的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入 *psid*。*Psid* 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。
remove	从 RAID 中删除 SSD 并保持数据不变。
remove-secure	从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全清除。
local-disk {**1** | **2**}	指定 SSD、disk1 或 disk2。

Command Default

如果您有两个 SSD，它们会在您启动时形成 RAID。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.17(1)	此命令是为安全防火墙 3100 引入的。

使用指南

防火墙通电时您可以执行以下任务：

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

示例

以下示例从 RAID 中删除 disk2 并执行安全清除。

```
ciscoasa# raid remove-secure local-disk 2
```

Related Commands

命令	说明
show raid	显示 RAID 状态。
show ssd	显示 SSD 状态。

range

要配置网络对象的地址范围，请在对象配置模式下使用 **range**命令。使用此命 **no**令的形式从配置中删除对象。

range*ip_addr_1ip_addr2*
no range*ip_addr_1ip_addr2*

Syntax Description

ip_addr_1	标识IP 地址范围（IPv4 或 IPv6）范围内的第一个地址。
ip_addr_2	标识范围中的最后一个 IP 地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
对象网络配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.3(1)	添加了此命令。
9.0(1)	我们增加了对 IPv6 地址的支持。

使用指南

如果使用不同的 IP 地址配置现有网络对象，则新配置将替换现有配置。

CR_Examples

以下示例显示如何创建范围网络对象：

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

Related Commands

命令	说明
clearconfigureobject	清除创建的所有对象。
description	向网络对象添加说明。
fqdn	指定完全限定域名网络对象。

命令	说明
host	指定主机网络对象。
nat	为网络对象启用 NAT。
objectnetwork	创建一个网络对象。
object-group network	创建网络对象组。
showrunning-configobjectnetwork	显示网络对象配置。
subnet	指定子网网络对象。

ras-rcf-pinholes

要在 Gatekeeper 位于网络内部时启用 H.323 端点之间的呼叫设置，请在参数配置模式下使用该 **ras-rcf-pinholes** 命令。要禁用此功能，请使用此**no** 命令的形式。

ras-rcf-pinholesenable
no ras-rcf-pinholesenable

Syntax Description

enable	启用 H.323 端点之间的呼叫设置。

Command Default

默认情况下，此选项已禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(5)	添加了此命令。

使用指南

ASA 包括基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息打开呼叫针孔的选项。由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。

CR_Examples

以下示例显示如何在策略映射中设置操作来为这些调用打开针孔：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	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。

命令	说明
showrunning-configpolicy-map	显示所有当前的策略映射配置。

rate-limit

使用模块化策略框架时，通过在 match 或 class 配置模式下使用 **match** 命令限制与 **rate-limit**命令或类映射匹配的消息包的速率。此速率限制操作在用于应用流量的检测策略映射（使用 **policy-maptypeinspect**命令）；但是，并非所有应用都允许此操作。要禁用此操作，请使用此命令的 no 形式。

rate-limit*rate*
no rate-limit*rate*

Syntax Description

rate	向流量应用速率限制，范围在 1-4294967295 之间。对于 ESMTP、GTP、RTSP 和 SIP，速率单位为数据包数/秒。对于 SCTP，速率以千比特每秒 (kbps) 为单位。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
匹配和类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
9.5(2)	此命令已扩展到SCTP检查，其中速率单位为kbps，而不是每秒的数据包数。

使用指南

检查策略图由一个或多个 **match**和 **class**命令组成。检查策略图可用的确切命令取决于应用程序。输入 **match** 或 **class** 命令标识应用流量（ **class** 命令是指现有的 **class-maptypeinspect**命令，该命令又包含 **match** 命令）后，可以输入 **rate-limit**命令限制消息的速率。

在第 3/4 层策略映射（下称 **policy-map** 命令）中使用 **inspect** 命令启用应用检测时，您可以启用包含此操作的检测策略映射，例如，输入 **inspectsipsip_policy_map** 命令，其中 sip_policy_map 是检测策略映射的名称。

CR_Examples

以下示例将邀请请求限制为每秒 100 条消息：

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(config-pmap-c)# rate-limit 100
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	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-maptypeinspect	定义特殊的应用检查操作。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

reactivation-mode

要指定用于重新激活组中出现故障的服务器的方法，请在aaa-server协议模式下使用**reactivation-mode**命令。要删除此规范，请使用此 **no**命令的形式。

reactivation-mode {**depletion** [**deadtime***minutes*] | **timed**}
no reactivation-mode {**depletion** [**deadtime***minutes*] | **timed**}

Syntax Description

deadtime分钟	（可选）指定禁用组中最后一台服务器与随后重新启用所有服务器之间经过的时间量（以分钟为单位，介于 0 到 1440 之间）。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。
depletion	仅当组内所有服务器都处于非活动状态时才重新激活出现故障的服务器。
timed	停机 30 秒后重新激活故障服务器。

Command Default

默认重新激活模式为 depletion，默认空载时间值为 10。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA-server 协议配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

每个服务器组都有一个用于指定其服务器重新激活策略的属性。

在 **depletion**模式下，当服务器被停用时，它将保持不活动状态，直到组中所有其他服务器都处于不活动状态。如果发生这种情况，组内所有服务器都会被重新激活。这种方法可最大限度减少因出现故障的服务器而发生的连接延迟。使用 **depletion** 模式时，您还可以指定 **deadtime** 参数。该参数指定禁**deadtime**用组中最后一台服务器和随后重新启用所有服务器之间经过的时间（以分钟为单位）。仅当服务器组与本地回退功能结合使用时，此参数才有意义。此外，如果您还将该组用于记帐，其中未使用本地回退，则空载时间将被取消。您可以通过为记帐创建一个不同的组（具有相同的服务器）来避免此问题。

在模 **timed**式下，发生故障的服务器将在停机 30 秒后重新激活。当客户将服务器列表中的第一台服务器用作主服务器并希望它尽可能在线时，这非常有用。此策略不适用于UDP服务器。由于即使服

务器不存在，与 UDP 服务器的连接也不会失败，因此系统会随机重新连接 UDP 服务器。如果服务器列表包含多个无法访问的服务器，这可能会导致连接时间减慢或连接失败。

已启用同时记账的记账服务器组强制使用 **timed** 模式。这意味着给定列表中的所有服务器都是同等的。



注释 对于 SDI 服务器组，忽略此命令，因为 SDI 服务器组包含单个服务器。

CR_Examples

以下示例将名为“srvgrp1”的 TACACS+ AAA 服务器配置为使用耗尽重新激活模式，死区时间为 15 分钟：

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
ciscoasa
(config-aaa-server)#
exit
ciscoasa
(config)#
```

以下示例将名为“srvgrp1”的 TACACS+ AAA 服务器配置为使用定时重新激活模式：

```
ciscoasa
(config)# aaa-server svrgrp2 protocol tacacs+
ciscoasa
(config-aaa-server)# reactivation-mode timed
ciscoasa
(config-aaa-server)#
```

Related Commands

accounting-mode	指示记账消息是发送到单个服务器，还是发送到组中的所有服务器。
aaa-serverprotocol	进入aaa服务器组配置模式，以便您可以配置特定于组且对组内所有主机通用的 AAA 服务器参数。
max-failed-attempts	指定对于服务器组中的任意给定服务器，在停用之前可允许的故障次数。
clearconfigureaaa-server	删除所有 AAA 服务器配置。
showrunning-configaaa-server	显示所有 AAA 服务器、特定服务器组、特定组中的特定服务器或特定协议的 AAA 服务器统计信息。

record-entry

要指定用于创建 CTL 文件的信任点，请在 ctl-file 配置模式下使用 record-entry 命令。要从 CTL 中删除记录条目，请使用此命令的 **no** 形式。

record-entry [**capfcucmcucm-tftptftp**] **trustpoint***trustpoint***address***ip_address* [**domain-name***domain_name*]
no
record-entry [**capfcucmcucm-tftptftp**] **trustpoint***trustpoint***address***ip_address* [**domain-name***domain_name*]

Syntax Description

capf	指定此信任点的角色为 CAPF。只能配置一个 CAPF 信任点。
cucm	指定此信任点的角色为 CCM。可以配置多个 CCM 信任点。
cucm-tftp	指定此信任点的角色为 CCM+TFTP。可以配置多个 CCM+TFTP 信任点。
domain-name*domain_name*	（可选）指定用于创建信任点 DNS 字段的信任点的域名。将此名称附加到“使用者 DN”的“通用名称”字段中以创建 DNS 名称。当未为信任点配置 FQDN 时，应配置域名。
address*ip_address*	指定信任点的 IP 地址。
tftp	指定此信任点的角色为 TFTP。可以配置多个 TFTP 信任点。
trustpoint*trust_point*	设置安装的信任点的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(4)	命令已添加。

使用指南

只能指定一个 domain-name。如果 CTL 文件不存在，请将此证书从 CUCM 手动导出到 ASA。

仅当您尚未为电话代理配置 CTL 文件时，才使用此命令。当您已配置 CTL 文件时，请勿使用此命令。

ip_address 参数中指定的 IP 地址必须是全局地址或 IP 电话可见的地址，因为它将是用于信任点的 CTL 记录的 IP 地址。

为 CTL 文件中所需的每个实体添加其他记录条目配置。

CR_Examples

以下示例显示如何使用 **record-entry**命令指定用于创建 CTL 文件的信任点：

```
ciscoasa(config-ctl-file)# record-entrycucm-tftptrustpoint cucm1 address 192.168.1.2
```

Related Commands

命令	说明
ctl-file(global)	指定要为电话代理配置创建的 CTL 文件，或指定要从闪存中解析的 CTL 文件。
ctl-file(phone-proxy)	指定用于电话代理配置的 CTL 文件。
phone-proxy	配置电话代理实例。

record-route

要定义在具有 IP 选项检查的数据包头中出现记录路由 (RR) 选项时的操作，请在 **record-route** 参数配置模式下使用该命令。要禁用此功能，请使用此**no** 命令的形式。

record-routeaction {**allow** | **clear**}
no record-routeaction {**allow** | **clear**}

Syntax Description

allow	允许包含记录路由 IP 选项的数据包。
clear	从数据包头中删除记录路由选项，然后允许数据包。

Command Default

默认情况下，IP 选项检查会丢弃包含记录路由 IP 选项的数据包。

您可以使用 IP **default**选项检查策略映射中的命令更改默认值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.5(1)	添加了此命令。

使用指南

此命令可配置的 IP 选项检查策略映射中。

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

CR_Examples

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

Related Commands

命令	说明
class	在策略映射中标识类映射名称。

命令	说明
class-maptypeinspect	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。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

redirect-fqdn

要在 VPN 负载平衡模式下使用完全限定域名启用或禁用重定向，请在 **redirect-fqdnenable** 全局配置模式下使用该命令。

redirect-fqdn { **enable** | **disable** }
no redirect-fqdn { **enable** | **disable** }



注释 要使用 VPN 负载平衡，您必须拥有带有 Plus 许可证的 ASA Model 5510 或 ASA Model 5520 或更高版本。VPN 负载均衡还需要活动的 3DES/AES 许可证。在启用负载均衡之前，安全设备将检查此加密许可证是否存在。如果没有检测到活动的 3DES 或 AES 许可证，安全设备会阻止启用负载均衡，也会阻止负载均衡系统进行 3DES 的内部配置，除非许可证允许此使用。

Syntax Description

disable	禁用完全限定域名的重定向。
enable	使用完全限定域名启用重定向。

Command Default

默认情况下禁用此行为。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
VPN负载均衡模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

认情况下，ASA 仅将负载均衡重定向中的 IP 地址发给客户端。如果使用基于 DNS 名称的证书，则重定向到辅助设备时证书将无效。

作为 VPN 集群主用设备，该 ASA 在将 VPN 客户端连接重定向至一个集群设备（集群中的另一 ASA）时，可以通过反向 DNS 查找发送此集群设备的完全限定域名 (FQDN)，而不是其外部 IP 地址。

集群中的负载均衡设备上的所有外部和内部网络接口，都必须位于相同 IP 网络之上。

要使用 FQDN 而不是 IP 地址进行 WebVPN 负载平衡，您必须执行以下配置步骤：

1. 使用命令启用 FQDN 进行负载平 **redirect-fqdnenable**衡。
2. 将每个 ASA 外部接口的条目添加到 DNS 服务器中（如果其中尚无这些条目）。每个 ASA 外部 IP 地址都应该有一个与其关联的 DNS 条目用于查找。对于反向查找，也必须启用这些 DNS 条目。
3. 使用命令“dns domain-lookup inside”（或任何具有到您的 DNS 服务器的路由的接口）在您的 ASA 上启用 DNS 查找。
4. 在 ASA 上定义您的 DNS 服务器 IP 地址；例如：dns name-server 10.2.3.4（您的 DNS 服务器的 IP 地址）

CR_Examples

以下是禁用重定向的 **redirect-fqdn**命令的示例：

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

以下是 VPN 负载平衡命令序列的示例，其中包括一个接口命令，该命令启用完全限定域名的重定向，将集群的公共接口指定为“test”，将集群的私有接口指定为“foo”：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

Related Commands

命令	说明
clearconfigurevpnload-balancing	删除负载平衡运行时间配置并禁止负载平衡。
showrunning-configvpnload-balancing	显示当前 VPN 负载平衡虚拟集群配置。
showvpnload-balancing	显示 VPN 负载平衡运行时间统计信息。
vpnload-balancing	进入 vpn 负载均衡模式。

redistribute (ipv6 router ospf)

要将 IPv6 路由从一个 OSPFv3 路由域重新分发到 OSPFv3 路由域，请在 ipv6 router ospf 配置模式下使用 **redistribute** 命令。要禁用重新分配，请使用此命 **no**令的形式。

redistribute*source-protocol*[*process-id*] [**include-connected**{**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric**{*metric-value***transparent**}] [**metric-type***type-value***] [match**{**external**[**1** | **2**] | **internal** | **nssa-external**[**1** | **2**]}] [**tag***tag-value*] [**route-map***map-tag*]

no redistribute*source-protocol*[*process-id*] [**include-connected**{**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric**{*metric-value***transparent**}] [**metric-type***type-value***] [match**{**external**[**1** | **2**] | **internal** | **nssa-external**[**1** | **2**]}] [**tag***tag-value*] [**route-map***map-tag*]

Syntax Description

as_number	指定路由进程的自治系统编号。有效值范围为 1 到 65535。
外部	指定位于指定自治系统外部但作为类型 1 或类型 2 外部路由导入 OSPFv3 的 OSPFv3 度量路由。有效值为 1 或 2。
include-connected	（可选）允许目标协议重新分配源协议已获知的路由以及运行源协议的接口上的连接前缀。
internal	指定指定自治系统内部的 OSPFv3 度量路由。
level-1	指定对于中间系统到中间系统 (IS-IS)，将 1 级路由独立地重新分配到其他 IP 路由协议中。
level-1-2	指定对于 IS-IS，1 级和 2 级路由都独立地重新分配到其他 IP 路由协议中。
level-2	指定对于 IS-IS，第 2 级路由被独立地重新分配到其他 IP 路由协议中。
map-tag	指定已配置的路由图的标识符。
match	（可选）将路由重新分发到其他路由域中。
metric*metric_value*	（可选）指定 OSPFv3 默认指标值，其范围为 0 到 16777214。
metric-type*metric_type*	（可选）指定与通告到 OSPFv3 路由域的默认路由关联的外部链接类型。它可以是以下两个值之一：1 表示第 1 类外部路由，2 表示第 2 类外部路由。
nssa-external	指定位于自治系统外部的路由，但作为类型 1 或类型 2 外部路由导入到 IPv6 非末梢区域 (NSSA) 中的 OSPFv3 中。
process-id	（可选）指定在启用 OSPFv3 路由进程时管理分配的编号。
route-map*map_name*	（可选）指定用于过滤从源路由协议导入到当前 OSPFv3 路由协议的路由的路由映射的名称。如果已指定但未列出路线图标签，则不会导入任何路线。如果未指定，则重新分发所有路由。

source-protocol	指定重新分配路由的源协议。有效值可以是以下之一：connected、ospf 或 static。
tag*tag_value*	（可选）指定附加到每个外部路由的 32 位十进制值。OSPFv3 本身不使用该值，但可能用于 ASBR 之间传递信息。如果未指定，则远程自治系统编号用于来自 BGP 和 EGP 的路由；对于其他协议，则使用零。有效值范围为 0 到 4294967295。
transparent	（可选）使 RIP 使用重新分配路由的路由表度量作为 RIP 度量。

Command Default

以下是命令默认值：

- **metric***metric-value*: **0**
- **metric-type***type-value*: **2**
- **match**： **internal**、 **external1**、 **external2**
- **tag***tag-value*: **0**

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.0(1)	添加了此命令。

CR_Examples

以下示例显示如何将静态路由重新分发到当前 OSPFv3 进程中：

```
ciscoasa(config-if)# ipv6router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

命令	说明
ipv6routerospf	OSPFv3 进入路由器配置模式。
showrunning-configipv6router	显示 OSPFv3 的路由器配置中的命令。

redistribute (router eigrp)

要将路由从一个路由域重新分发到 EIGRP 路由进程，请在路由器 eigrp 配置模式下使用 **redistribute** 命令。要删除重新分配，请使用此命 **no**令的形式。

redistribute { { **eigrp***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** } [**metric***bandwidthdelay reliability load mtu*] [**route-map***map_name*
no redistribute { { **eigrp***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** } [**metric***bandwidthdelay reliability load mtu*] [**route-map***map_name*

Syntax Description

带宽	EIGRP 带宽指标（以千比特/秒为单位）。有效值范围为 1 至 4294967295。
connected	指定将连接到接口的网络重新分布到 EIGRP 路由过程中。
delay	EIGRP 延迟度量，以 10 微秒为单位。有效值为 0 到 4294967295。
外部 类型	指定处于指定自治系统外部的 EIGRP 指标路由；有效值为 **1** 或 **2**。
内部 类型	指定指定自治系统内部的 EIGRP 度量路由。
加载	EIGRP 有效带宽（负载）指标。有效值为 1 至 255，其中 255 表示 100% 加载。
match	（可选）指定将路由从 OSPF 重新分发到 EIGRP 的条件。
metric	（可选）指定重新分配到 EIGRP 路由进程中的路由的 EIGRP 度量值。 注释 不适用于静态路由的重新分发。请改用 prefix-list 或 access-list。
mtu	路径的 MTU。有效值为 1 至 65535。
nssa-external *type*	为 NSSA 的外部路由指定 EIGRP 指标类型；有效值为 **1** 或 **2**。
eigrp*pid*	用于将一个EIGRP路由进程重新分配到EIGRP路由进程中。 *pid* 指定 EIGRP 路由进程的内部使用标识参数；其有效值范围为 1 至 65535。
可靠性	EIGRP 可靠性指标。有效值为 0 至 255，其中 255 表示 100% 可靠性。
rip	指定将网络从 RIP 路由进程重新分配到 EIGRP 路由进程。
route-map*map_name*	（可选）路由映射的名称，该映射用于过滤从源路由协议到 EIGRP 路由进程的导入路由。如果未指定，则重新分发所有路由。
static	用于将静态路由重新分配到 EIGRP 路由进程中。 注释 不支持使用与指标匹配的路由映射重新分配静态路由。

Command Default

以下是命令默认值：

- **match： Internal、 external1、 external2**

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 eigrp 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。
9.20(1)	已添加 EIGRP IPv6 路由重新分发。

使用指南

如果您的 **metric**EIGRP 配置中没有命令，则必须使用 **default-metric**redistribute 命令指定。

CR_Examples

以下示例将静态路由和连接路由重新分配到 EIGRP 路由进程中：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

Related Commands

命令	说明
routereigrp	创建 EIGRP 路由进程并进入该进程的配置模式。
showrunning-configrouter	显示全局路由器配置中的 命令。

redistribute (router ospf)

要将路由从一个路由域重新分发到OSPF 路由进程，请在路由器 ospf配置模式下使用 **redistribute** 命令。要在不包含选项时删除重新分发，请使用此命令的 **no** 形式。带有选项的命令的 **no** 形式仅删除该选项的配置。

redistribute { { **ospf***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** | **eigrp***as-number* } [**metric***metric_value*] [**metric-type***metric_type*]
[**route-map***map_name*] [**tag***tag_value*] [**subnets**]
no redistribute { { **ospf***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** | **eigrp***as-number* } [**metric***metric_value*] [**metric-type***metric_type*]
[**route-map***map_name*] [**tag***tag_value*] [**subnets**]

Syntax Description

connected	指定将连接到接口的网络重新分发到 OSPF 路由过程中。
eigrp*as-number*	用于将 EIGRP 路由重新分配到 OSPF 路由进程中。as -*number*指定 EIGRP 路由进程的自治系统编号。有效值为 1 至 65535。
外部 类型	指定作为所指定自治系统外部的 OSPF 指标路由；有效值为 **1** 或 **2**。
内部类型	指定指定自治系统内部的 OSPF 度量路由。
match	（可选）指定将路由从一个路由协议重新分配到另一个路由协议的条件。
metric*metric_value*	（可选）指定 OSPF 默认指标值，范围为 0 到 16777214。 注释 不适用于静态路由的重新分发。请改用 prefix-list 或 access-list。
metric-type*metric_type*	（可选）与通告到 OSPF 路由域的默认路由关联的外部链接类型。它可以是以下两个值之一： **1**（第 1 类外部路由）或 **2**（第 2 类外部路由）。
nssa-external *type*	为 NSSA 的外部路由指定 OSPF 指标类型；有效值为 **1** 或 **2**。
ospf*pid*	用于将一个 OSPF 路由进程重新分配到当前 OSPF 路由进程中。 *pid* 指定 OSPF 路由进程内部使用的标识参数；其有效值范围为 1 至 65535。
rip	指定将网络从 RIP 路由进程重新分发到当前 OSPF 路由进程中。
route-map*map_name*	（可选）用于过滤从源路由协议到当前 OSPF 路由进程的导入路由的路由映射的名称。如果未指定，则重新分发所有路由。
static	用于将静态路由重新分发到 OSPF 进程。 注释 不支持使用与指标匹配的路由映射重新分配静态路由。

subnets	（可选）将路由重新分发到 OSPF 时，可确定指定协议的重新分发范围。如果未使用，则仅重新分发有类路由。
tag*tag_value*	（可选）附加到每个外部路由的 32 位十进制值。OSPF 本身不使用此值。它可用于在 ASBR 之间传递信息。如果未指定任何值，则会将远程自治系统编号用于来自 BGP 和 EGP 的路由；对于其他协议，使用零 (0)。有效值范围为 0 到 4294967295。

Command Default

以下是命令默认值：

- **metric***metric-value*: 0
- **metric-type**类型值： **2**
- **match**： **Internal**、 **external1**、 **external2**
- **tag***tag-value*: 0

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已修改为包括 **rip** 关键字。
8.0(2)	此命令已修改为包括 **eigrp** 关键字。
9.0(1)	增加了多情景模式支持。

CR_Examples

以下示例显示如何将静态路由重新分发到当前 OSPF 进程中：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

命令	说明
redistribute(RIP)	将路由重新分配到RIP路由进程中。

命令	说明
routerospf	进入路由器配置模式。
showrunning-configrouter	显示全局路由器配置中的 命令。

redistribute (router rip)

要将其他路由域中的路由重新分发到RIP路由进程，请在路由器RIP配置模式下使用 **redistribute** 命令。要删除重新分配，请使用此命 **no**令的形式。

redistribute { { **ospf***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** | **eigrp***as-number* } [**metric***metric_value*] [**transparent**] [**route-map***map_name*]
no redistribute { { **ospf***pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] }
| **rip** | **static** | **connected** | **eigrp***as-number* } [**metric***metric_value*] [**transparent**] [**route-map***map_name*]

Syntax Description

connected	指定将连接到接口的网络重新分发到 RIP 路由进程中。
eigrp*as-number*	用于将 EIGRP 路由重新分配到 RIP 路由进程中。as *-number*指定 EIGRP 路由进程的自治系统编号。有效值为 1 至 65535。
外部 类型	指定作为所指定自治系统外部的 OSPF 指标路由；有效值为 **1** 或 **2**。
内部类型	指定指定自治系统内部的 OSPF 度量路由。
match	（可选）指定将路由从 OSPF 重新分发到 RIP 的条件。
metric {*metric_value*|**transparent**}	（可选）指定正在重新分发的路由的RIP指标值。 *metric_value* 的有效值为0到16。将指标设置为 **transparent** 会导致使用当前的路由指标。 注释 不适用于静态路由的重新分发。请改用 prefix-list 或 access-list。
nssa-external *type*	为次末节区域 (NSSA) 外部路由指定 OSPF 指标类型；有效值为 **1** 或 **2**。
ospf*pid*	用于将OSPF路由进程重新分配到RIP路由进程中。 *pid* 指定OSPF路由进程内部使用的标识参数；其有效值范围为 1 至 65535。
route-map*map_name*	（可选）用于过滤从源路由协议到 RIP 路由进程的导入路由的路由映射的名称。如果未指定，则重新分发所有路由。
static	用于将静态路由重新分发到 OSPF 进程。 注释 不支持使用与指标匹配的路由映射重新分配静态路由。

Command Default

以下是命令默认值：

- **metric***metric-value*: 0
- **match**： **Internal**、 **external1**、 **external2**

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 RIP 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(2)	此命令已修改为包括 **eigrp** 关键字。
9.0(1)	支持多上下文模式。

CR_Examples

以下示例显示如何将静态路由重新分发到当前 RIP 进程：

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# redistribute static metric 2
```

Related Commands

命令	说明
redistribute(routereigrp)	将路由从其他路由域重新分发到 EIGRP。
redistribute(routerospf)	将路由从其他路由域重新分发到 OSPF。
routerrip	启用 RIP 路由进程并进入该进程的路由器配置模式。
showrunning-configrouter	显示全局路由器配置中的 命令。

redistribute isis

要将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级，请在 **redistributeisis**路由器 isis 配置模式下使用该命令。要禁用重新分配，请使用此命 **no**令的形式。

redistribute isis ip{**level-1** | **level-2**}**into**{**level-2** | **level-1**}[[**distribute-list**列表编号] | [**route-map***map-tag*]]
no redistribute isis ip{**level-1** | **level-2**}**into**{**level-2** | **level-1**}[[**distribute-list**列表编号] | [**route-map***map-tag*]]

Syntax Description

level-1|level-2	您要重新分配 IS-IS 路由的级别。
into	将要重新分配的路由级别与要将路由重新分配到的级别分隔开的关键字。
distribute-list列表编号	（可选）控制 IS-IS 重新分发的分发列表编号。您可以指定分发列表或路由图，但不能同时指定两者。
route-map*map-tag*	（可选）控制 IS-IS 重新分配的路由图的名称。您可以指定分发列表或路由映射，而不是同时指定两者。

Command Default

此命令没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 isis 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

在 IS-IS 中，所有区域都是末节区域，这意味着不会将主干（第 2 级）中的任何路由信息泄漏到末节区域（第 1 级）。仅第 1 级路由器使用到其区域内最近的 Level 1-Level 2 路由器的默认路由。此命令使您可以将第 2 级 IP 路由重新分发到第 1 级区域。此重新分发使仅第 1 级路由器可以选择 IP 前缀的最佳路径来离开区域。这是一个仅 IP 功能，CLNS 路由仍为末节路由。

要提高控制力和稳定性，您可以配置分发列表或路由映射，以控制可以重新分发到第 1 级的第 2 级 IP 路由。这使大型 IS-IS-IP 网络可以使用区域获得更好的可扩展性。



注释 您必须指定 **metric-stylewide**命令才能使 **redistributeisis**命令起作用。

CR_Examples

在以下示例中，访问列表 100 控制 IS-IS 从第 1 级到第 2 级的重新分发：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 distribute-list 100
ciscoasa(config-router)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

在以下示例中，名为 match-tag 的路由映射控制 IS-IS 从第 1 级到第 2 级的重新分发，以便只重新分发标记有 110 的路由：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
ciscoasa(config-router)# route-map match-tag permit 10
ciscoasa(config-router)# match tag 11
```

Related Commands

redundant-interface

要设置冗余接口的哪个成员接口处于活动状态，请在 **redundant-interface** 特权 EXEC 模式下使用该命令。

redundant-interfaceredundant*number***active-member***physical_interface*

Syntax Description

active-member*physical_interface*	设置活动成员。有关接受的值，请参阅 **interface** 命令。两个成员接口均必须为相同的物理类型。
redundant*number*	指定标识冗余接口 ID，例如 **redundant1**。

Command Default

默认情况下，主用接口是在配置中列出的第一个成员接口（如果可用）。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

要查看哪个接口处于活动状态，请输入以下命令：

```
ciscoasa# show interface redundantnumberdetail| grep Member
```

例如：

```
ciscoasa# show interface redundant1detail| grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

CR_Examples

以下示例创建了一个冗余接口。默认情况下，gigabitethernet 0/0 处于活动状态，因为它是配置中的第一个接口。redundancy-interface 命令将gigabitethernet 0/1 设置为主用接口。

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

Related Commands

命令	说明
clearinterface	清除命令的计数 **showinterface**器。
debugredundant-interface	显示与冗余接口事件或错误相关的调试消息。
interfaceredundant	创建冗余接口。
member-interface	将成员接口分配给冗余接口对。
showinterface	显示接口的运行时间状态和统计信息。

regex

要创建正则表达式来匹配文本，请在 **regex** 全局配置模式下使用该命令。要删除正则表达式，请使用此命 **no**令的形式。

regex*nameregular_expression*
regex*name* [*regular_expression*]

Syntax Description

name	指定正则表达式名称，长度最多为 40 个字符。
regular_expression	指定正则表达式，最多 100 个字符的长度。请参阅“使用指南”部分，了解可在正则表达式中使用的元字符列表。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

regex 命令可用于需要文本匹配的各种功能。例如，您可以使用模块化策略框架和 检测策略映射 为应用检测配置特殊操作（请参阅 **policymaptypeinspect** 命令）。在检测策略映射中，您可以创建包含一个或多个 **match** 命令的检测类映射，标识要对其执行操作的流量，也可以直接在检测策略映射中使用 **match** 命令。某些 **match** 命令可使用正则表达式标识数据包中的文本，请参阅；例如，可以匹配 HTTP 数据包内的 URL 字符串。可以对正则表达式类映射中的正则表达式进行分组（请参阅 **class-maptyperegex** 命令）。

正则表达式可以逐字匹配文本字符串作为精确字符串，或者通过使用元字符来匹配文本字符串的多种变体。您可以使用正则表达式来匹配某些应用程序流量的内容；例如，您可以匹配 HTTP 数据包内的正文。



注释 为了优化性能，ASA 可在去模糊化的 URL 中搜索。去模糊化处理将多个正斜杠 (/) 压缩为一个斜杠。对于通常使用双斜杠的字符串（例如“http://”），请务必搜索“http:/”。

表 18-1 列出了具有特殊含义的元字符。

表 *1:* 正则表达式元字符

字符	说明	注
.	点	匹配任何单个字符。例如， **d.g** 匹配 dog、dag、dtg 以及包含这些字符的任何单词，例如 doggonnit。
(*exp***)**	子表达式	子表达式将字符与其周围的字符分隔开，从而可以在子表达式上使用其他元字符。例如， **d(o|a)g**匹配 dog 和 dag，但 **do|ag** 匹配 do 和 ag。子表达式还可以与重复限定符配合使用，以区分意味着重复的字符。例如，匹 **ab(xy){3}z**配 abxyxyxyz。
|	交替	匹配其分隔的任意一个表达式。例如， **dog|cat**匹配狗或猫。
?	问号	一个限定符，表示前面有 0 个或 1 个表达式。例如， **lo?se**匹配 lse 或 lose。 **注释** 您必须输入 **Ctrl+V** 和问号，否则将调用帮助功能。
*	星号	一个限定符，表示前面有 0 个、1 个或任意数量的表达式。例如，**lo*se**匹配 lse、lose、loose 等等。
+	加号	一个限定符，表示前面至少有 1 个表达式。例如，比 **lo+se**赛有 lose 和 loose，但没有 lse。
{*x* **}**或 **{***x***,}**	最小重复限定符	至少重复 *x* 次。例如， **ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等等。
[*abc***]**	字符类	匹配方括号中的任意字符。例如， **[abc]** 匹配 a、b 或 c。
[^*abc***]**	求反字符类	匹配不包含在方括号中的单个字符。例如，**[^abc]**匹配除 a、b 或 c 之外的任意字符。 **[^A-Z]** 匹配任何非大写字母的单个字符。
[*a-c***]**	字符范围类	匹配范围内的任意字符。 **[a-z]** 匹配任意小写字母。您可以混合字符和范围： **[abcq-z]**匹配 a、b、c、q、r、s、t、u、v、w、x、y、z，[也是如此。**a-cq-z]** 仅当破折号 (-) 字符是括号内的最后一个或第一个字符时，它才是文字：**[abc-]**或。 **[-abc]**
""	引号	保留字符串中的尾随空格或前导空格。例如，在 “**test**”寻找匹配项时保留前导空格。
^	脱字号	指定行首。
\	转义字符	当与元字符一起使用时，可以匹配原义字符。例如， **\[** 匹配左方括号。

字符	说明	注
char	字符	当字符不是元字符时，匹配原义字符。
\r	回车符	匹配回车符 0x0d。
\n	换行符	匹配换行符 0x0a。
\t	Tab	匹配制表符 0x09。
\f	换页符	匹配换页符 0x0c。
\x*NN*	转义的十六进制数字	匹配十六进制的 ASCII 字符（必须是两位数）。
\NNN	转义的八进制数字	匹配八进制的 ASCII 字符（必须是三位数）。例如，字符 040 代表空格。

使用指南

要测试正则表达式以确保它与您认为匹配的 **testregex** 内容相匹配，请输入命令。

正则表达式的性能影响取决于两个主要因素：

- 搜索正则表达式匹配项需要的文本长度。

当搜索长度较短时，正则表达式引擎只会对 ASA 性能产生较小的影响。

- 搜索某个正则表达式匹配项需要的正则表达式链式表的数量。

搜索长度如何影响性能

配置正则表达式搜索时，通常会对照正则表达式数据库检查搜索文本的每个字节，找到匹配项。搜索的文本越长，搜索时间就越长。下面是一个性能测试案例，它说明了这种现象。

- HTTP 事务包括一个 300 字节长的 GET 请求和一个 3250 字节长的响应。
- 445 个正则表达式用于 URI 搜索，34 个正则表达式用于请求正文搜索。
- 55 个用于响应正文搜索的正则表达式。

当策略配置为仅搜索 HTTP GET 请求中的 URI 和正文时，吞吐量为：

- 420 Mbps（未搜索相应的正则表达式数据库时）。
- 413 Mbps 时搜索相应的正则表达式数据库（这表明使用正则表达式的开销相对较小）。

但是，当策略也配置为搜索整个 HTTP 响应正文时，由于响应正文（3250 字节）搜索较长，吞吐量降至 145 Mbps。

以下列出了会增加正则表达式搜索的文本长度的因素：

- 在多个不同的协议字段上配置了正则表达式搜索。例如，在 HTTP 检测中，如果为正则表达式匹配仅配置了 URI，则仅在 URI 字段中搜索正则表达式匹配，并且搜索长度随后会限制为 URI 长度。但是，如果还为正则表达式匹配配置了其他协议字段（例如报头、正文等），则搜索长度将增加以包括报头长度和正文长度。

- 要搜索的字段过长。例如，如果 URI 配置为用于正则表达式搜索，则 GET 请求中的长 URI 将具有较长的搜索长度。此外，目前 HTTP 正文搜索长度默认限制为 200 个字节。但是，如果策略配置为搜索正文，并且正文搜索长度更改为 5000 字节，则会由于正文搜索较长而对性能造成严重影响。

链接的正则表达式表的数量对性能的影响

目前，为同一协议字段配置的所有正则表达式（例如 URI 的所有正则表达式）均内置于由一个或多个正则表达式链表组成的数据库中。表的数量取决于所需的总内存以及建立表时的内存可用性。在以下任一情况下，正则表达式数据库将拆分为多个表：

- 由于最大表大小限制为 32 MB，所需的总内存超过 32 MB 时。
- 当最大连续内存的大小不足以构建完整的正则表达式数据库时，将构建较小但多个表以容纳所有正则表达式。请注意，内存碎片的程度取决于许多相互关联的因素，几乎不可能预测碎片的级别。

使用多个链式表时，必须在每个表中搜索正则表达式匹配项，因此搜索时间与搜索的表数量成正比。

某些类型的正则表达式往往会显着增加表的大小。谨慎的做法是，在设计正则表达式时尽可能避免通配符和重复因素。有关以下元字符的说明，请参阅 表 18-1 ：

- 具有通配符类型规格的正则表达式：
- 句点 (.)
- 各种字符类别，与类别中的任何字符匹配：
- [^a-z]
- [a-z]
- [abc]]
- 具有重复类型规格的正则表达式：
- *
- +
- {n，}
- 组合使用通配符类型和重复类型的正则表达式会显着增加表的大小，例如：
- 123.*xyz
- 123.+xyz
- [^a-z]+
- [^a-z]*
- .*123.* （不应这样做，因为它相当于匹配“123”）。

以下示例说明包含和不包含通配符和重复项的正则表达式的内存消耗有何不同。

- 以下 4 个正则表达式的数据库大小为 958,464 字节。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 以下 4 个正则表达式的数据库大小仅为 10240 字节。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

大量的正则表达式会增加正则表达式数据库所需的总内存，因此如果内存分段，会增加生成更多表的可能性。以下是不同数量的正则表达式的内存消耗示例：

- 100 个示例 URI：3,079,168 字节
- 200 个示例 URI：7,156,224 字节
- 500 个示例 URI：11,198,971 字节



注释 每个情景的正则表达式最大数量为 2048。 **debugmenuregex4010** 命令可用于显示每个正则表达式数据库中有多少个链式表。

CR_Examples

以下示例创建两个用于检测策略映射的正则表达式：

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
```

Related Commands

命令	说明
class-maptypeinspect	创建一个检查类别图来匹配特定于应用程序的流量。
policy-map	通过将流量类和一个或多个操作关联，创建策略映射。
policy-maptypeinspect	定义特殊的应用检查操作。
class-maptyperegex	创建正则表达式类映射。
testregex	测试正则表达式。

reload

要重新启动并重新加载配置，请在特权 EXEC 模式下使用 **reload** 命令。

reload[**at***hh*: *mm*[*month day*|*day month*]] [**cancel**] [**in** [*hh*:] *mm*] [**max-hold-time** [*hh*:] *mm*] [**noconfirm**] [**quick**] [**reason**文本] [**save-config**]

Syntax Description

at*hh*:*mm*	（可选）安排在指定时间重新加载软件（使用 24 小时制）。如果不指定月份和日期，则重新加载在当天的指定时间（如果指定的时间晚于当前时间）或次日的指定时间（如果指定的时间早于当前时间）进行。 ）。指定 00:00 可安排在午夜重新加载。重新加载必须在 24 小时内进行。
cancel	（可选）取消计划的重新加载。
day	（可选）天数，范围为 1 至 31。
in [*hh*:]*mm*]	（可选）安排软件重新加载，使其在指定的分钟或小时和分钟内生效。重新加载必须在 24 小时内进行。
max-hold-time [*hh*:*mm*	（可选）指定 ASA 在关闭或重新启动之前等待通知其他子系统的最大保持时间。这段时间过后，系统会进行快速（强制）关闭/重新启动。
month	（可选）指定月份的名称。输入足够的字符，创建唯一的字符串作为月份名称。例如，“Jul”不是唯一的，因为它可能代表六月或七月，但“Jul”是唯一的，因为没有其他月份以这三个字母开头。
noconfirm	（可选）允许 ASA 在无需用户确认的情况下重新加载。
quick	（可选）强制快速重新加载，而不通知或正确关闭所有子系统。
reason 文本、	（可选）指定重新加载的原因，范围为 1 到 255 个字符。原因文本发送到所有打开的 IPsec VPN 客户端、终端、控制台、Telnet、SSH 和 ASDM 连接/会话。 **注释** 某些应用（例如 ISAKMP）需要额外配置才能将原因文本发送到 IPsec VPN 客户端。有关详细信息，请参阅 VPN CLI 配置指南。
save-config	（可选）关闭前将运行配置保存到内存中。如果不输入 **save-config** 关键字，任何尚未保存的配置更改都将在重新加载后丢失。
保存显示技术	（可选）在重新加载发生之前，将 **showtech** 命令的输出保存到文件。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	已修改此命令，添加以下新参数和关键字： *day*、 *hh*、 *mm*、 *on*、 **quick**、 **save-config**和 *text*。
9.1(3)	添加了 **save-show-tech** 关键字。

使用指南

命令允许您重新启动 ASA 并从闪存重新加载配置。

默认情况下，该 **reload**命令是交互式的。ASA 首先检查配置是否已修改但未保存。如果需要，ASA 会提示您保存配置。在多情景模式下，ASA 会为每个情景提示未保存的配置。如果指定 **save-config** 关键字，系统会保存配置而不提示您。然后，ASA 将提示您确认是否确实要重新加载系统。只有响应 **y** 或按下 **Enter** 键会导致重新加载。确认后，ASA 将启动或安排重新加载过程，具体取决于您是否指定了 delay 关键字（**in** 或 **at**）。

默认情况下，重新加载过程在“graceful”模式下运行。在即将重启时，所有已注册的子系统都会收到通知，从而允许这些子系统在重启前正常关闭。要避免等到发生此类关闭，请指定 **max-hold-time** 关键字来指定要等待的最长时间。或者，您可以使用 **quick** 关键字强制重新加载过程突然开始，而不通知受影响的子系统或等待正常关闭。

您可以通过指定 **noconfirm** 关键字强制 **reload** 命令以非交互方式运行。在这种情况下，除非已指定 **save-config** 关键字，否则 ASA 不会检查未保存的配置。ASA 在重新启动系统之前不会提示您进行确认。除非您指定了 delay 关键字，否则它将立即启动或安排重新加载过程，但您可以指定 **max-hold-time** 或 **quick** 关键字来控制行为或重新加载过程。

使用 **reloadcancel**命令取消计划的重新加载。您无法取消已经在进行的重新加载。



注释 重新加载后，未写入闪存分区的配置更改将会丢失。在重新引导之前，输入 **writememory** 命令以将当前配置存储在闪存分区中。

CR_Examples

以下示例显示如何重新启动并重新加载配置：

```
ciscoasa# reload
Proceed with ?  [confirm]
 y
Rebooting...
XXX
Bios VX.X
...
```

Related Commands

命令	说明
showreload	显示ASA的重新加载状态。

remote-access threshold session-threshold-exceeded

要设置阈值，请在 **remote-accessthreshold** 全局配置模式下使用该命令。要删除阈值，请使用此命令的 **no**版本。此命令指定活动的远程访问会话的数量，达到达到数量时，ASA 会发送陷阱。

remote-access threshold session-threshold-exceeded*threshold-value*
*no***remote-access threshold session-threshold-exceeded**

Syntax Description

threshold-value	指定一个小于或等于 ASA 支持的会话限制的整数。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0 (1)	添加了此命令。

CR_Examples

以下示例显示如何设置阈值 1500：

```
ciscoasa# remote-access threshold session-threshold-exceeded 1500
```

Related Commands

命令	说明
snmp-serverenabletrapremote-access	启用阈值陷阱。

rename (class-map)

要重命名类映射，请在 class-map 配置模式下输入 **rename** 命令。

rename*new_name*

Syntax Description

new_name 指定类映射的新名称，最长为 40 个字符。保留名称“class-default”。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例显示如何将类映射从 test 重命名为 test2：

```
ciscoasa(config)# class-map test
ciscoasa(config-cmap)# rename test2
```

Related Commands

命令	说明
class-map	创建类映射。

rename (EXEC 特权)

要将文件或目录从源文件名重命名为目标文件名，请在特权 EXEC 模式下使用 **rename**命令。

rename[**/noconfirm**] [**disk0:** | **disk1:** | **flash:**] 源路径 [**disk0:** | **disk1:** | **flash:**] 目的路径

Syntax Description

/noconfirm	（可选）抑制确认提示。
目的路径	指定目标文件的路径。
disk0:	（可选）指定内部闪存，后跟冒号。
disk1:	（可选）指定外部闪存，后跟冒号。
flash:	（可选）指定内部闪存，后跟冒号。
源路径	指定源文件的路径。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

renameflash:flash: 命令提示您输入源文件名和目标文件名。

无法跨文件系统重命名文件或目录。

例如：

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

CR_Examples

以下示例显示如何将名为“test”的文件重命名为“test1”：

```
ciscoasa# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

Related Commands

命令	说明
mkdir	创建新目录。
rmdir	删除目录。
showfile	显示有关文件系统的信息。

renewal-reminder

如要指定在用户证书到期前多少天向证书所有者发送初始重新注册提醒，请在ca服务器配置模式下使用 **renewal-reminder** 命令。要将时间重置为默认值 14 天，请使用此命令的 **no**形式。

renewal-reminder天
no renewal-reminder

Syntax Description

天指定在已颁发证书到期之前，首次提醒证书所有者重新注册的时间（以天为单位）。有效值范围为 1 至 90 天。

Command Default

默认值为 14 天。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
ca 服务器配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

共有三个提醒。如果在用户数据库中指定了电子邮件地址，则每次提醒时都会自动向证书所有者发送一封电子邮件。如果邮件地址不存在，将会生成一条系统日志消息提醒管理员进行了续约。

默认情况下，CA 服务器在证书到期之前按指定顺序发送以下三封邮件：

1. 认证注册邀请

2. 提醒：认证注册邀请

3. 最后提醒：认证注册邀请

第一封电子邮件是邀请邮件，第二封电子邮件是提醒邮件，第三封邮件是最后提醒邮件。此通知的默认设置为 14 天，这意味着在证书到期前 14 天发出初始邀请提醒邮件，在证书到期前 7 天发出提醒邮件，在证书到期前 3 天发出最后提醒邮件过期时间。

您可以使用 **renewal-reminder***days* 命令自定义续约提醒间隔。

CR_Examples

以下示例指定 ASA 在证书到期前 7 天向用户发送到期通知：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# renewal-reminder 7
ciscoasa
(config-ca-server)
#
```

以下示例在证书到期前将到期通知时间重置为默认值：14 天：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no renewal-reminder
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
crypto ca server	提供对ca服务器配置模式命令集的访问，允许您配置和管理本地CA。
lifetime	指定 CA 证书、所有颁发的证书和 CRL 的有效期。
showcryptocaserver	显示本地 CA 服务器的配置详细信息。

replication http

要为故障转移组启用 HTTP 连接复制，请在故障转移组配置模式下使用 **replicationhttp** 命令。要禁用 HTTP 连接复制，请使用此命 **no**令的形式。

replicationhttp
no replicationhttp

Syntax Description

此命令没有任何参数或关键字。

Command Default

已禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
故障转移组配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

默认情况下，当启用状态故障转移时，ASA 不会复制 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。 **replicationhttp** 命令用于在状态故障转移环境中启用 HTTP 会话的状态复制，但可能会对系统性能造成负面影响。

此命令仅适用于主用/主用故障转移。它提供与用于主用/备用故障转移的 **failoverreplicationhttp** 命令相同的功能，但主用/主用故障转移配置中的故障转移组除外。

CR_Examples

以下示例显示了故障转移组的一种可能配置：

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failoverreplicationhttp	配置状态故障转移以复制 HTTP 连接。

request-command deny

要禁止 FTP 请求中的特定命令，请在 FTP 映射配置模式下使用 **request-commanddeny** 命令，可使用 **ftp-map** 命令访问该模式。要删除配置，请使用此命令的 no 形式。

request-command deny {**appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou**}
no request-command deny {**appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou**}

Syntax Description

appe	禁止 附加到文件的命令。
cdup	不允许更改当前工作目录的父目录的命令。
dele	禁止执行在服务器上删除文件的命令。
get	禁止使用客户端命令从服务器检索文件。
help	禁止提供帮助信息的命令。
mkd	不允许在服务器上创建目录的命令。
put	禁止使用客户端命令 将文件发送到服务器。
rmd	禁止执行在服务器上删除目录的 命令。
rnfr	禁止指定 rename-from filename 的命令。
rnto	禁止指定 rename-to filename 的命令。
site	不允许特定于服务器系统的 命令。通常用于远程管理。
stou	不允许使用唯一文件名存储文件的命令。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
FTP 映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令用于控制在使用严格 FTP 检测时遍历 ASA 的 FTP 请求中允许的命令。

CR_Examples

以下示例导致 ASA 丢弃包含 **stor**、 **stou**或 **appe** 命令的 FTP 请求：

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# request-command deny put stou appe
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
ftp-map	定义 FTP 映射并启用 FTP 映射配置模式。
inspectftp	应用特定的FTP映射来用于应用程序检查。
mask-syst-reply	隐藏来自客户端的 FTP 服务器响应。
policy-map	将类映射与特定的安全操作相关联。

request-data-size

要设置 SLA 操作请求包中有效载荷的大小，请使用 sla 监控 **request-data-size**协议配置模式下的命令。要恢复默认值，请使用此命 **no**令的形式。

request-data-size*bytes*
no request-data-size

Syntax Description

bytes 请求数据包有效负载的大小（以字节为单位）。有效值为 0 至 16384。最小值取决于所使用的协议。对于回送类型，最小值为 28 个字节。请勿将此值设置为高于协议或 PMTU 允许的最大值。

注释
ASA 会在负载中添加一个 8 字节时间戳，因此实际负载为 字节数 + 8。

Command Default

The default *bytes* is 28.

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

为了实现可达性，可能需要增加默认数据大小来检测源和目标之间的 PMTU 变化。较低的 PMTU 可能会影响会话性能，如果检测到，则可能表明使用了辅助路径。

CR_Examples

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求/响应时间探测操作。它将回显请求数据包的有效载荷大小设置为 48 字节，并将 SLA 操作期间发送的回显请求数量设置为 5。

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

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
```

```
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

命令	说明
num-packets	指定要在SLA操作期间发送的请求数据包数。
slamonitor	定义 SLA 监控操作。
typeecho	将 SLA 操作配置为回应响应时间探测操作。

request-queue

要指定排队等待响应的 GTP 请求的最大数量，请在策略映射参数配置模式下使用 request-queue 命令。使用此命令的 **no**形式将此数字恢复为默认值 200。

request-queue最大请求数
no request-queue最大请求数

Syntax Description

最大请求数	排队等待响应的最大 GTP 请求数，从 1 到 4294967295。

Command Default

默认值为 200。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

request-queue 命令指定排队等待响应的最大GTP请求数。达到限制后，如果有新请求到达，将会删除队列中等待时间最长的请求。错误提示、不支持的版本和 SGSN 情景确认消息不被视为请求，且不会进入请求队列中等待响应。

CR_Examples

以下示例指定最大请求队列大小 300：

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# request-queue 300
```

Related Commands

命令	说明
clearservice-policyinspectgtp	将清除全局 GTP 统计数据。
inspectgtp	适用于特定的GTP映射，以用于应用检查。

命令	说明
showservice-policyinspectgtp	显示 GTP 配置。

request-timeout (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要配置 SSO 身份验证尝试失败之前的超时秒数，请在 **request-timeout** webvpn 配置模式下使用该命令。

要返回默认值，请使用此**no**命令形式。

request-timeout秒
no request-timeout

Syntax Description

seconds	失败的 SSO 身份验证尝试超时之前的秒数。范围是 1 到 30 秒。不支持分数。

Command Default

此命令的默认值为 5 秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

此命令适用于这两种类型的 SSO 服务器。

将 ASA 配置为支持 SSO 身份验证后，您可以选择调整以下两个超时参数：

- 使用该命令进行 SSO 身份验证尝试失败之前的 **request-timeout** 超时秒数。
- ASA 重试失败的 SSO 身份验证的次数。（请参阅 **max-retry-attemptscommand.)**

CR_Examples

以下示例在 webvpn-config-sso-siteminder 模式下进入，为 SiteMinder 类型 SSO 服务器“example”配置 10 秒的身份验证超时：

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# request-timeout 10
```

Related Commands

命令	说明
max-retry-attempts	配置 ASA 重试失败的 SSO 身份验证的次数。
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
showwebvpnsso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
testsso-server	使用试用身份验证请求测试 SSO 服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

reserved-bits

要清除 TCP 报头中的保留位，或丢弃设置了保留位的数据包，请在 tcp-map 配置模式下使用 **reserved-bits** 命令。要删除此规范，请使用此 **no**命令的形式。

reserved-bits { **allow** | **clear** | **drop** }
no reserved-bits { **allow** | **clear** | **drop** }

Syntax Description

allow	允许 TCP 标头中带有保留位的数据包。
clear	清除 TCP 标头中的保留位并允许数据包。
drop	丢弃 TCP 标头中带有保留位的数据包。

Command Default

默认情况下，允许使用保留位。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该 **tcp-map**命令与模块化策略框架基础设施一起使用。使用命令定义流量类 **class-map** 别并使用命令定制 TCP 检 **tcp-map** 查。使用命令应用新的 **policy-map** TCP 映射。使 **service-policy**用命令激活 TCP 检查。

使 **tcp-map**用命令进入tcp-map配置模式。在 tcp-map 配置模式下，使用 **reserved-bits** 命令可消除终端主机如何处理带保留位的数据包的不明确性，否则可能导致 ASA 失去同步。可以选择清除 TCP 报头中的保留位，或者甚至丢弃设置了保留位的数据包。

CR_Examples

以下示例展示如何使用设置了保留位的 TCP 流上的数据包清除数据包：

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# reserved-bits clear
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
```

```
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

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。
setconnection	配置连接值。
tcp-map	创建 TCP 映射，并允许对 tcp-map 配置模式的访问。

reserve-port-protect

要在媒体协商期间限制预留端口的使用，请在参数配置模式下使用 **reserve-port-protect**命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此**no** 命令的形式。

reserve-port-protect
no reserve-port-protect

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。

CR_Examples

以下示例显示如何在 RTSP 检查策略映射中保护保留端口：

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	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。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

reset

使用模块化策略框架时，对于与 **match** 命令或类映射（在 match 或 class 配置模式下使用 **reset**命令）匹配的流量，丢弃数据包、关闭连接并发送 TCP 重置。此重置操作在用于应用流量的检测策略映射（使用 **policy-maptypeinspect**命令）中可用；但是，并非所有应用都允许此操作。要禁用此操作，请使用此命令的 no 形式。

reset [**log**]
no reset [**log**]

Syntax Description

log 记录匹配。系统日志消息数取决于应用。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
匹配和类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

检查策略图由一个或多个 **match**和 **class**命令组成。检查策略图可用的确切命令取决于应用程序。在输入 **match** 或 **class** 命令标识应用流量后（ **class** 命令是指现有的 **class-maptypeinspect**命令，该命令又包含 **match** 命令），可以输入 **reset**命令丢弃数据包并关闭匹配 **match** 命令或 **class** 命令的流量。

如果重置连接，则检查策略映射中不会执行进一步的操作。例如，如果第一个操作是重置连接，那么它将永远不会匹配任何进一步的 **match**或 **class**命令。如果第一个操作是记录数据包，则会发生第二个操作，例如，重置连接。可以为同一个 **match** 或 **class** 命令配置 **reset** 和 **log** 操作，在这种情况下，将先记录数据包，然后针对给定匹配重置数据包。

在第 3/4 层策略映射（下简称 **policy-map** 命令）中使用 **inspect** 命令启用应用检测时，您可以启用包含此操作的检测策略映射，例如，请输入 **inspecthttphttp_policy_map** 命令，其中 http_policy_map 是检测策略映射的名称。

CR_Examples

以下示例在网络隧道与 http-traffic 类映射匹配时重置连接并发送日志。如果同一数据包也与第二个 **match** 命令匹配，则不会处理该数据包，因为它已被丢弃。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	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-maptypeinspect	定义特殊的应用检查操作。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

resolver

要配置解析 DNS 请求的 Cisco Umbrella DNS 服务器的地址，请在 Umbrella 配置模式下使用 **resolver** 命令。使用此命 **no**令的形式可以恢复默认设置。

resolver {**ipv4** | **ipv6**} *ip_address*
no resolver {**ipv4** | **ipv6**} *ip_address*

Syntax Description

ipv4*ip_address*	要使用的 Umbrella DNS 服务器的 IPv4 地址。
ipv6*ip_address*	要使用的 Umbrella DNS 服务器的 IPv6 地址。

Command Default

默认 DNS 解析器为 208.67.220.220 和 2620:119:53::53。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Umbrella 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.12(1)	添加了此命令。

使用指南

您可以通过两次输入命令来配置 IPv4 和 IPv6 地址。您只能指定有效的 Umbrella DNS 服务器。

CR_Examples

以下示例定义 Cisco Umbrella 的非默认 DNS 解析器。这两台服务器为 208.67.222.222 和 2620:119:35::35。

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

Related Commands

命令	说明
umbrella-global	配置思科 Umbrella 全局参数。

responder-only

要将VTI隧道的一端配置为仅用作响应方，请在IPsec配置文件配置模式下使用responder-only命令。使用此命令的no形式删除仅响应者模式。

responder-only
no responder-only

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
IPsec 配置文件配置	• 是	• 否	• 是	—	—

Command History

版本	修改
9.7(1)	我们引入了此命令。

使用指南

使用此命令，可将 VTI 隧道的一端配置为仅充当响应方。

仅响应方端不会发起隧道或重新生成密钥。

当冲突处理不可用时，或在使用 IKEv1 的实例中隧道两端同时尝试启动隧道时，此选项非常有用。即使已配置，也将忽略仅响应方端上的 IKE 或 IPsec 隧道的所有重新生成密钥配置。

CR_Examples

以下示例将仅响应方模式添加到 IPsec 配置文件：

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# responder-only
```

Related Commands

命令	说明
cryptoipsecprofile	创建新的 IPsec 配置文件。
setikev1transform-set	指定 IPsec 配置文件配置中要使用的 IKEv1 转换集。
setpfs	指定要在 IPsec 配置文件配置中使用的 PFS 组。

命令	说明
setsecurity-associationlifetime	在 IPsec 配置文件配置中指定安全关联的持续时间。这可以以千字节或秒为单位或同时以两者为单位指定。
设置信任点	指定一个信任点，该信任点定义启动 VTI 隧道连接时要使用的证书。

rest-api（已弃用）

使用 **agent** 关键字从闪存启用已安装的 REST API 代理。使用此命令的no形式禁用代理。

将 REST API 软件包下载至此 ASA（使用 **copy**命令）以验证并安装软件包。REST API 代理的版本必须与 ASA 版本匹配。要卸载此软件包，请使用此命令的no形式。]

rest-api [**agent** | **image disk0:** /*package*]
no rest-api [**agent** | **image disk0:** /*package*]

Syntax Description

代理	启用已安装的 REST API 代理。
imagedisk0:/软件包	安装之前下载的 REST API 映像，由 程序包 标识。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
启用/禁用 REST API 代理	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.3(2)	添加了此命令。
9.17(1)	此命令已弃用。

使用指南

发出带 **image** 关键字的此命令，以对指定的 REST API 包执行兼容性和验证检查。如果软件包通过了所有检查，则会安装到内部闪存。

REST API 配置保存在启动配置文件中。使用 **clearconfigure** 命令清除此配置。

安装或更新 REST API 包不会触发 ASA 重新启动。

将此命令与 **agent** 关键字配合使用，可启用已安装的 REST API 代理。

CR_Examples

此示例从 cisco.com 下载 REST API 包，然后安装它：

```
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-9.3.2-32.pkg  disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
```

此示例通过禁用正在运行的 REST API 代理，然后下载、安装并启动新的 REST API 代理，升级现有 REST API 代理：

```
ciscoasa(config)# no rest-api agent
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-121-lfbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
ciscoasa(config)# rest-api agent
```

Related Commands

命令	说明
copy	将指定的 REST API 包从 TFTP 服务器复制到内部闪存。
show rest-api agent	确定 REST API 代理是否正在运行。
clearconfigure	清除运行配置，包括 REST API 配置。

restore

要从备份文件恢复 ASA 配置、证书、密钥和映像，请在特权 EXEC 模式下使用 **restore** 命令。

restore[**/noconfirm**][**context***ctx-name*][**interface***name*][**cert-passphrase***value*][**location***path*]

Syntax Description

cert-passphrase*value*	在VPN证书和预共享密钥恢复过程中，需要使用关键字标识的**cert-passphrase**密钥来解密证书。您必须提供用于解码 PKCS12 格式的证书的密码。
context*ctx-name*	在多上下文模式下从系统执行空间输入关 **context**键字来恢复指定的上下文。必须单独恢复每个备份的 **restore**上下文文件；也就是说，为每个文件重新输入命令。
interface*name*	（可选）指定将通过其复制备份的接口名称。如果不指定接口，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。
location*path*	恢复 **location**可以是本地磁盘或远程 URL。如果不提供位置，则会使用以下默认名称： • 单模式—disk0:*hostname.backup.timestamp.tar.gz* • 多模式—disk0:*hostname.context -ctx-name.backup.timestamp.tar.gz*
/noconfirm	指定不提示输入 **location** 和 **cert-passphrase** 参数。允许您绕过警告和错误消息以继续备份。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.3(2)	添加了此命令。
9.5(1)	已添加 **interface***name* 参数。

使用指南

请参阅以下准则：

- 在开始还原之前，还原位置应至少有 300 MB 的可用磁盘空间。

- 如果您在备份期间或之后进行任何配置更改，则这些更改将不会包含在备份中。如果在进行备份后更改配置，然后执行恢复后的，则会覆盖此配置更改。因此，ASA 的行为可能会有所不同。
- 一次只能启动一个还原。
- 只能将配置恢复为与执行原始备份时相同的 ASA 版本。无法使用恢复工具将配置从一个 ASA 版本迁移到另一个版本。如果需要迁移配置，ASA 会在加载新 ASA OS 时自动升级驻留的启动配置。
- 如果您使用集群，则只能恢复启动配置、运行配置和身份证书。必须为每台设备单独创建和恢复备份。
- 如果使用故障转移，则必须为主用设备和备用设备单独创建和恢复备份。
- 如果您针对ASA设置主密码，则需要该主密码短语来恢复您使用此程序创建的备份配置。如果您不知道 ASA 的主密码，请参阅 CLI 配置指南，了解如何在继续备份之前重置它。
- 如果您导入PKCS12数据（使用命**cryptocatrustpoint**令）并且信任点使用RSA密钥，则导入的密钥对将分配与信任点相同的名称。由于此限制，如果在恢复ASDM配置后为信任点及其密钥对指定其他名称，则启动配置将与原始配置相同，但运行配置将包含其他密钥对名称。这意味着，如果对密钥对和信任点使用不同的名称，则无法恢复原始配置。要解决此问题，请确保对信任点及其密钥对使用同一名称。
- 如果不指定接口，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。请注意，如果有一个通过管理专用接口的默认路由，则所有**restore**流量都将匹配该路由，并且从不检查数据路由表。在此场景中，如果您需要通过数据接口恢复，请始终指定 接口。
- 无法使用 CLI 进行备份及使用 ASDM 进行恢复，反之亦然。
- 每个备份文件包含以下内容：
- 运行配置
- 启动配置
- 所有安全映像

思科安全桌面和主机扫描映像

思科安全桌面和主机扫描设置

AnyConnect (SVC) 客户端映像和配置文件

AnyConnect (SVC) 自定义和转换

- 身份证书（包括绑定到身份证书的 RSA 密钥对；独立密钥除外）
- VPN 预共享密钥
- SSL VPN 配置
- 应用配置文件自定义框架 (APCF)
- 书签

- 自定义
- 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

CR_Examples

以下示例显示如何恢复备份：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
is required to restore running configuration, startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] ⋯ Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ⋯ Done!
Backing up [SSL VPN Configurations: Bookmarks]⋯ Done!
Backing up [SSL VPN Configurations: Customization] ⋯ Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ⋯ Done!
Backing up [SSL VPN Configurations: Plug-in] ⋯ Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ⋯ Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ⋯ Done!
Backing up [SSL VPN Configurations: Translation table] ⋯ Done!
Backing up [SSL VPN Configurations: Web Content] ⋯ Done!
Backing up [Anyconnect(SVC) client images and profiles] ⋯ Done!
Backing up [Anyconnect(SVC) customizations and transforms] ⋯ Done!
Backing up [Cisco Secure Desktop and Host Scan images] ⋯ Done!
Backing up [UC-IME tickets] ⋯ Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
device, please note them for future reference.
ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the IP
is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the IP
is already used as media-termination address on interface inside.
```

```
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
 configuration file if you want to preserve the old http- and https-proxy configurations.
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
cisco. If the passphrase is not correct, certificates will not be restored.
No passphrase was provided for identity certificates. Using the default value: cisco. If
the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

Related Commands

命令	说明
backup	从备份文件备份ASA配置、密钥、证书和映像。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。