ret - rz

- retries， 第 3 页
- retry-count， 第 4 页
- retry-interval， 第 6 页
- reval-period， 第 8 页
- revert webvpn all， 第 10 页
- revert webvpn AnyConnect-customization， 第 11 页
- revert webvpn customization， 第 13 页
- revert webvpn plug-in protocol， 第 15 页
- revert webvpn translation-table， 第 17 页
- revert webvpn url-list， 第 19 页
- revert webvpn webcontent， 第 20 页
- revocation-check， 第 21 页
- rewrite（已弃用），第 23 页
- re-xauth， 第 25 页
- rip authentication mode， 第 27 页
- rip authentication key， 第 29 页
- rip receive version， 第 31 页
- rip send version， 第 32 页
- rmdir， 第 33 页
- 路由， 第 35 页
- route-map， 第 38 页
- route priority high， 第 41 页
- router-alert， 第 42 页
- router bgp， 第 44 页
- router eigrp， 第 46 页
- router-id， 第 48 页
- router-id cluster-pool， 第 50 页
- router isis， 第 52 页
- router ospf， 第 53 页
- router rip， 第 55 页

- rtp-conformance， 第 57 页
- rtp-min-port rtp-max-port（已弃用），第 59 页

retries

要指定 ASA 未收到响应时重试 DNS 服务器列表的次数，请在全局配置模式下使用该**dnsretries**命令。要恢复默认设置，请使用此命 **no**令的形式。

retries编号
no retries [*number*]

Syntax Description

number 指定重试次数，从 0 到 10。默认值为 2。

Command Default

默认重试次数为 2。

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
7.1(1)	添加了此命令。

使用指南

使用 **name-server** 命令添加 DNS 服务器。

该命令替代了该 **dnsname-server**命令。

CR_Examples

以下示例将重试次数设置为 0。ASA 仅尝试每个服务器一次。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# retries 0
```

Related Commands

命令	说明
clearconfiguredns	删除所有 DNS 命令。
dnsserver-group	输入 dns 服务器组模式。
showrunning-configdnsserver-group	显示一个或所有现有 dns-server-group 配置。

retry-count

要设置在确定服务器不可达之前对云网络安全代理服务器连续轮询失败的次数值，请在 **retry-count** scansafe 常规选项配置模式下输入该命令。要恢复默认值，请使用此命 **no**令的形式。

retry-count值
no retry-count [*value*]

Syntax Description

value 输入重试计数器值（2 到 100 之间的值）。默认值为 5。

Command Default

默认值为 5。

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
Scansafe 常规选项配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

您订用思科 Cloud Web Security 服务后，系统会为您分配主用云网络安全代理服务器和备用代理服务器。

如有任何客户端无法访问主用服务器，ASA 将开始轮询信号塔以确定可用性。（如果没有客户端活动，ASA 将每隔 15 分钟轮询一次。）如果在重试次数达到所配置的次数（默认设置为 5 次；此设置可配置）之后代理服务器不可用，则系统会宣布该服务器无法访问，并且备用代理服务器进入活动状态。

如果在达到重试计数之前，客户端或ASA可以至少连续两次访问服务器，则停止轮询并且确定信号塔可访问。

如果启用了应用运行状况检查，重试计数也将适用于该检查。

故障切换到备用服务器后，ASA将继续轮询主用服务器。如果主用服务器可以访问，ASA将恢复使用主用服务器。

CR_Examples

以下示例将重试次数配置为 7：

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

命令	说明
class-maptypeinspectscansafe	为加入白名单的用户和组创建检查类映射。
defaultusergroup	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。
health-checkapplication	为故障转移启用云网络安全应用运行状况检查。
[**https**]（参数）	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspectscansafe	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的身份验证密钥，以指示请求来自哪个组织。
matchusergroup	匹配白名单的用户或组。
policy-maptypeinspectscansafe	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，即轮询代理服务器以检查其可用性之前等待的时间。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafegeneral-options	配置常规云网络安全服务器选项。
server{**primary**| **backup**}	配置主或备份云网络安全代理服务器的完全限定域名或 IP 地址。
showconnscansafe	显示所有云网络安全连接，标有大写 Z 标志。
showscansafeserver	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
showscansafestatistics	显示总计和当前 HTTP 连接数。
user-identitymonitor	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。

retry-interval

要配置上一个命令中指定的特定 AAA 服务器的重试尝试间隔时 **aaa-serverhost**间，请在 **retry-interval**aaa-server 主机模式下使用该命令。要将重试间隔重置为默认值，请使用此命令的 **no**形式。

retry-interval秒
no retry-interval

Syntax Description

seconds 指定请求的重试间隔（1-10 秒）。这是 ASA 在重试连接请求之前等待的时间。EXTEN

Command Default

默认重试间隔为 10 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
AAA-server host	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	已修改此命令以符合 CLI 准则。

使用指南

使用 **retry-interval** 命令指定或重置 ASA 在连接尝试之间等待的秒数。使用该 **timeout**命令指定 ASA 尝试连接到 AAA 服务器的时间长度。

此命令不适用于 RSA SecurID REST API 服务器组中的服务器。

注释 对于 RADIUS 协议，如果服务器回复“无法访问 ICMP 端口”消息，则系统会忽略 retry-interval 设置，并且 AAA 服务器会立即进入故障状态。如果这是 AAA 组中的唯一服务器，则会重新激活该服务器并向其发送另一个请求。这是预期行为。

CR_Examples

以下示例显示了上下文中 **retry-interval**的命令。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 7
```

```
ciscoasa
(config-aaa-server-host)# retry-interval 9
```

Related Commands

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。
timeout	指定 ASA 尝试连接到 AAA 服务器的时间长度。

reval-period

要指定 NAC 框架会话中每次成功姿态验证之间的 **reval-period**间隔，请使用 nac-policy-nac-framework 配置模式下的命令。要从 NAC 框架策略中删除命令，请使用此命令的 **no**形式。

reval-period秒
no reval-period[秒]

Syntax Description

秒每次成功姿势验证之间的秒数。范围为 300 到 86400。

Command Default

默认值为 36000。

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
nac-policy-nac-framework 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。
7.3(0)	“nac-”已从命令名称中删除。命令已从 group-policy 配置模式移至 nac-policy-nac-framework 配置模式。

使用指南

每次成功完成姿态验证后，ASA 都会启动重新验证计时器。此计时器到期会触发下一次无条件的安全状态验证。ASA 在重新验证期间维持姿态验证。如果访问控制服务器在安全状态验证或重新验证期间不可用，则默认组策略会生效。

CR_Examples

以下示例将重新验证计时器更改为 86400 秒：

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

以下示例从 NAC 策略中删除重新验证计时器：

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

命令	说明

EOU 超时	更改在 NAC 框架配置中将 EAP over UDP 消息发送到远程主机之后等待的秒数。
开方周期	指定NAC框架会话中每次成功的姿态验证与下一次主机姿态变化查询之间的间隔。
nac-policy	创建和访问思科 NAC 策略，并指定其类型。
调试 nac	启用 NAC 框架事件的日志记录。
eou 重新验证	强制对一个或多个 NAC 框架会话立即进行安全状态重新验证。

revert webvpn all

要从 ASA 闪存中删除所有与 Web 相关的数据（自定义、插件、转换表、URL 列表和 Web 内容），请在特权 EXEC 模式下输入 **revertwebvpnall**命令。

revert webvpn all

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpnall**命令禁用 ASA 的闪存中并从中删除所有与 Web 相关的信息（自定义、插件、转换表、URL 列表和 Web 内容）。删除所有与网络相关的数据将恢复默认设置（如适用）。

CR_Examples

以下命令从 ASA 中删除所有与 Web 相关的配置数据：

```
ciscoasa# revert webvpn all
ciscoasa
```

Related Commands

命令	说明
showimportwebvpn(option)	显示各种导入的 WebVPN 数据和插件。当前存在于 ASA 上的闪存中。

revert webvpn AnyConnect-customization

要从 自定义安全客户端*GUI*的ASA 中删除文件，请在特权 EXEC 模式下使用 **revertwebvpnAnyConnect-customization**命令。

revert webvpn AnyConnect-customizationtype*type***platform***platform***name***name*

Syntax Description

type	自定义文件的类型： • 二进制文件 - 替换 AnyConnect GUI 的可执行文件。 • resource - 资源文件，例如公司徽标。 • transform - 自定义 MSI 的转换。
platform	运行 Secure Client的终端设备的操作系统。指定以下选项之一：linux、mac-intel、mac-powerpc、win 或 win-mobile。
name	标识要删除的文件的名称（最多 64 个字符）。

Command Default

此命令没有默认行为。

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
特权 EXEC	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。

使用指南

有关自定义 Secure Client GUI 的详细程序，请参阅《AnyConnect VPN 客户端管理员指南》。

CR_Examples

以下示例删除之前作为资源文件导入的用于自定义 AnyConnect GUI 的思科徽标：

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

Related Commands

命令	说明
customization	指定要用于隧道组、组或用户的自定义对象。
exportcustomization	导出自定义对象。
importcustomization	安装自定义对象。
revertwebvpnall	删除所有与 webvpn 相关的数据（自定义、插件、转换表、URL 列表和 Web 内容）。
showwebvpncustomization	显示 ASA 的闪存设备上存在的当前自定义对象。

revert webvpn customization

要从 ASA 缓存中删除自定义对象，请在特权 EXEC 模式下输入 **revertwebvpncustomization**命令。

revert webvpn customization*name*

Syntax Description

name	指定要删除的自定义对象的名称。

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpncustomization** 命令删除指定自定义的无客户端 SSL VPN 支持，并将其从 ASA 上的缓存中删除。删除自定义对象会在适用的情况下恢复默认设置。自定义对象包含特定、命名的门户页面的配置参数。

版本 8.0 软件扩展了配置自定义的功能，新进程与以前的版本不兼容。在升级到 8.0 软件期间，安全设备通过使用旧设置生成新的自定义对象来保留当前配置。此过程仅发生一次，并且不仅仅是从旧格式到新格式的简单转换，因为旧值只是新值的部分子集。

注释 仅当在升级到版本 8.0 之前，在版本 7.2(x) 配置文件的相应接口上启用了无客户端 SSL VPN (WebVPN) 时，版本 7.2 门户自定义和 URL 列表才可在 Beta 8.0 配置中使用。

CR_Examples

以下命令删除名为 GroupB 的自定义对象：

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

Related Commands

命令	说明
customization	指定要用于隧道组、组或用户的自定义对象。
exportcustomization	导出自定义对象。
importcustomization	安装自定义对象。
revertwebvpnall	删除所有与 webvpn 相关的数据（自定义、插件、转换表、URL 列表和 Web 内容）。
showwebvpncustomization	显示 ASA 的闪存设备上存在的当前自定义对象。

revert webvpn plug-in protocol

要从 ASA 的闪存设备中删除插件，请在特权 EXEC 模式下输入 **revertwebvpnplug-inprotocol** 命令。

revert plug-in protocol*protocol*

Syntax Description

protocol 输入以下字符串之一：

- rdp

远程用户可通过远程桌面协议插件连接到运行 Microsoft 终端服务的计算机。

- **ssh**

安全外壳插件使远程用户能够建立与远程计算机的安全通道，或者使远程用户能够使用 Telnet 连接到远程计算机。

- **vnc**

虚拟网络计算插件允许远程用户使用显示器、键盘和鼠标来查看和控制打开了远程桌面共享的计算机。

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpnplug-inprotocol** 命令禁用和删除对基于 Java 的指定客户端应用的无客户端 SSL VPN 支持，并将其从 ASA 的闪存驱动器中删除。

CR_Examples

以下命令删除对 RDP 的支持：

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

Related Commands

命令	说明
importwebvpnplug-inprotocol	将指定的插件从URL复制到ASA的闪存设备。发出此命令后，无客户端SSL VPN自动支持在未来的会话中使用基于Java的客户端应用。
showimportwebvpnplug-in	列出ASA闪存设备上的插件。

revert webvpn translation-table

要从 ASA 闪存中删除转换表，请在特权 EXEC 模式下输入 **revertwebvpntranslation-table**命令。

翻译领域**revert webvpn translation-tablelanguage**语 言

Syntax Description

翻译域	可用的转换域： • **AnyConnect** • **PortForwarder** • **banners** • **csd** • **customization** • **url-list** • **webvpn** • 转换来自 Citrix、RPC、Telnet-SSH 和 VNC 插件的消息（如果可用）。
language语言	指定要删除的语言。使用 2 个字符的代码指定语言。输入 ?查看安装了哪些语言。使用 **showimportwebvpntranslation-table** 命令查看已安装的每个域中的哪些语言。

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpntranslation-table** 命令禁用和删除导入的转换表，并从闪存中删除该转换表。如果适用，删除转换表将恢复默认设置。

CR_Examples

以下命令删除法语版的 AnyConnect 转换表：

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

Related Commands

命令	说明
revertwebvpnall	删除所有与 webvpn 相关的数据(自定义、插件、转换表、URL 列表和 Web 内容)。
showimportwebvpntranslation-table	显示闪存设备上当前存在的转换表。

revert webvpn url-list

要从 ASA 中删除 URL 列表，请在特权 EXEC 模式下输入 **revertwebvpnurl-list**命令。

revert webvpn url-list template*name*

Syntax Description

template*name*	指定URL列表的名称。

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpnurl-list**命令禁用并从 ASA 的闪存驱动器中删除当前 URL 列表。适用时，删除 url 列表会恢复默认设置。

该命令使用的 **revertwebvpnurl-list** 模板参数指定先前配置的 URL 列表的名称。要配置这样的列表，请在 **url-list**全局配置模式下使用该命令。

CR_Examples

以下命令删除 URL 列表 servers2：

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

Related Commands

命令	说明
revertwebvpnall	删除所有与 webvpn 相关的数据（自定义、插件、转换表、URL 列表和 Web 内容）。
showrunning-configurationurl-list	显示当前配置的 URL 列表命令集。
url-list(WebVPNmode)	将 WebVPN 服务器和 URL 列表应用于特定用户或组策略。

revert webvpn webcontent

要从 ASA 闪存中的某个位置删除指定的 Web 对象，请在特权 EXEC 模式下输入 **revertwebvpnwebcontent**命令。

revert webvpn webcontent*filename*

Syntax Description

filename	指定包含要删除的Web内容的闪存文件的名称。

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
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

使用 **revertwebvpncontent**命令禁用和删除包含 Web 内容的文件，并从 ASA 的闪存中删除该文件。如果适用，删除 Web 内容会恢复默认设置。

CR_Examples

以下命令从 ASA 闪存中删除 Web 内容文件 ABCLogo：

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

Related Commands

命令	说明
revertwebvpnall	删除所有与webvpn相关的数据（自定义、插件、转换表、URL列表和Web内容）。
showwebvpnwebcontent	显示 ASA 上闪存中当前存在的 Web 内容。

revocation-check

要定义信任池策略是否需要吊销检查，请在 crypto ca trustpool 配置模式下使用 **revocation-check** 命令。要恢复默认的吊销检查方法（ 无），请使用此命令的 **no** 形式。

revocation-check{ [**crl**] [**ocsp**] [**none**] }
no revocation-check{ [**crl**] [**ocsp**] [**none**] }

Syntax Description

crl	指定 ASA 应使用 CRL 作为吊销检查方法。
none	指定 ASA 应将证书状态解释为有效，即使所有方法都返回一个错误也是如此。
ocsp	指定 ASA 应使用 OCSP 作为吊销检查方法。

Command Default

默认值为 *none*。

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
Crypto ca trustpool 配置模式	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。
9.5(1)	添加了使用 OCSP URL 进行吊销检查的接口关键字 。
9.13(1)	由于 CRL 或 OCSP 服务器的连接问题而绕过撤销检查的选项已被删除。
9.15(1)	绕过吊销检查的选项（在 9.13(1) 中被删除）已恢复。

使用指南

OCSP 响应的签名者通常是 OCSP 服务器（响应者）证书。收到响应后，设备尝试验证响应方证书。

通常，CA 会将其 OCSP 响应器证书的有效期设置为相对较短的时间段，以最大限度地减少危及其安全性的可能性。CA 在响应者证书中包含一个 ocsp-no-check 扩展，表明它不需要吊销状态检查。但如果此扩展不存在，设备将尝试使用您通过此 **revocation-check** 命令为信任点配置的吊销方法来检查证书吊销状态。如果 OCSP 响应方证书没有 ocsp-no-check 扩展，则它必须可验证，因为 OCSP 吊销检查会失败，除非您还设置 *none* 选项以忽略状态检查。

注释 对可选参数进行任何排列，最后使用的关键字不得为 *none* 。

ASA 会按照配置方法的顺序尝试这些方法，并且仅当前一种方法返回错误（例如，服务器关闭）时，才会尝试第二种和第三种方法，而不是发现状态为已撤销。

您可以在客户端证书验证信任点中设置吊销检查方法，也可以在响应方证书验证信任点中配置无吊销检查 (**revocation-checknone)**) 。请参阅 **matchcertificate** 命令。

如果您已使用 **revocation-checkcrlnone** 命令配置 ASA，则当客户端连接至 ASA 时，客户端会自动开始下载 CRL（因为 CRL 尚未缓存），然后验证证书并完成 CRL 的下载。在此情况下，如果 CRL 没有缓存，ASA 将在下载 CRL 之前验证证书。

以下用于绕过吊销检查的选项（已在 ASA 9.13(1) 中被删除，稍后已恢复）：

选项	操作
revocation-check crl none	如果无法访问 CRL，则绕过吊销检查
revocation-check ocsp none	如果无法执行 OCSP 检查，则绕过吊销检查
revocation-check crl ocsp none	如果无法访问 CRL，请尝试 OCSP。如果无法执行 OCSP，则绕过吊销检查
revocation-check ocsp crl none	如果无法执行 OCSP，请尝试 CRL，否则请绕过吊销检查

当您分配 OCSP URL 进行撤销检查时，您可以指定可从中访问 OCSP 的管理接口。此接口值确定路由决策。

CR_Examples

```
ciscoasa(config-ca-trustpoint)# revocation-chec
k ?
crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)# ocsp
ocsp interface mgmt url http://1.1.1.1:8888
```

其中，mgmt 是管理接口的名称

Related Commands

命令	说明
cryptocatrustpoolpolicy	进入子模式，可提供定义 trustpool 策略的命令。
匹配证书允许过期证书	允许管理员对某些证书豁免到期检查。
match certificate skip revocation-check	允许管理员豁免对某些证书进行吊销检查。

rewrite（已弃用）

要通过 WebVPN 连接禁用内容重写特定应用或流量类型，请在 webvpn 模式下使用 **rewrite**命令。要消除重写规则，请使用此命令的**no**形式并带有规则编号（唯一标识规则）。要消除所有重写规则，请使用不带规则编号的命令的 **no**形式。

默认情况下，ASA 重写或转换所有 WebVPN 流量。

rewrite order*integer*{**enable | disable**}**resource-mask***string*[**资源name**名 称]
no rewrite order*integer*{**enable | disable**}**resource-mask***string*[**资源name**名 称]

Syntax Description

disable	将此重写规则定义为对指定流量禁用内容重写的规则。禁用内容重写时，流量不会通过安全设备。
启用	将此重写规则定义为对指定流量启用内容重写的规则。
integer	在所有已配置的规则中设置规则的顺序。范围为 1-65534。
name	（可选）标识规则应用到的应用或资源的名称。
order	定义 ASA 应用规则的顺序。
资源掩码	标识规则的应用或资源。
资源名称	（可选）指定规则应用到的应用或资源。最多 128 个字节。
字符串	指定要匹配的可以包含正则表达式的应用名称或资源名称。您可以使用以下通配符： 指定要匹配的模式，可以包含正则表达式。您可以使用以下通配符： * - 匹配所有内容。此通配符不能单独使用。它必须附带字母数字字符串。 ? —匹配任意单个字符。 [!seq] — 匹配任何不按顺序的字符。 [seq] — 匹配序列中的任意字符。 最多 300 字节。

Command Default

默认值为重写所有内容。

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。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

使用指南

ASA 对应用执行内容重写，以确保它们通过 WebVPN 连接正确呈现。某些应用程序不需要进行此处理，例如外部公共网站。对于这些应用，您可以选择关闭内容重写。

您可以通过使用带有 disable 选项的 rewrite 命令选择性地关闭内容重写，以使用户直接浏览特定站点，而不通过 ASA。这类似于 IPsec VPN 连接中的分割隧道。

您可以多次使用此命令。配置条目的顺序非常重要，因为 ASA 会按顺序编号搜索重写规则并应用匹配的第一个规则。

CR_Examples

以下示例显示如何配置顺序号为 1 的重写规则，该规则关闭域 cisco.com 的 URL 的内容重写：

```
ciscoasa
(config-webpn)#
 rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

命令	说明
apcf	指定用于特定应用的非标准规则。
proxy-bypass	配置特定应用的最小内容重写。

re-xauth

要要求 IPsec 用户在 IKE 重新密钥时重新进行身份验证，请在 **re-xauthenable** 策略组配置模式下发出该命令。要禁用 IKE 重新密钥时的用户重新身份验证，请使用该 **re-xauthdisable**命令。

要从运行配置中删除 re-xauth 属性，请使用此命令的 **no**形式。这使得可以从另一个组策略继承 IKE 重新密钥时重新认证的值。

re-xauth{**enable**[**extended**]|**disable**}
no re-xauth

Syntax Description

disable	禁用在 IKE 重新生成密钥时重新进行身份验证
enable	启用 IKE 密钥更新时的重新认证
扩展	将允许的重新输入身份验证凭证的时间延长到所配置的SA的最大生存期为止。

Command Default

IKE 重新密钥时的重新认证功能已禁用。

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
策略组配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.0.4	添加了 **extended** 关键字。

使用指南

“IKE 重新生成密钥”仅适用于 IPsec 连接。

如果在 IKE 重新密钥时启用重新身份验证，则 ASA 会在初始第 1 阶段 IKE 协商期间提示用户输入用户名和密码，并且在每次发生 IKE 重新密钥时提示用户进行身份验证。重新身份验证提供额外的安全性。

用户有 30 秒时间输入凭证，在 SA 过期（大约两分钟）并且隧道终止之前最多可进行三次尝试。以允许用户重新输入身份验证凭证 **extended**，直至达到所配置的 SA 的最大生存期为止。

要检查配置的重新密钥间隔，请在监控模式下发出命 **showcryptoipsecsa**令来查看安全关联的生存期（以秒为单位）和生存期（以千字节为单位）。

注释 如果连接的另一端没有用户，则重新认证失败。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略启用重新密钥重新身份验证：

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip authentication mode

要指定 RIP 版本 2 数据包中使用的身份验证类型，请在接口配置模式下使用 **ripauthenticationmode** 命令。要恢复默认的身份验证方法，请使用此命令的 **no**形式。

rip authentication mode {**text | md5**}
no rip authentication mode

Syntax Description

md5	使用 MD5 进行 RIP 消息身份验证。
text	使用明文进行 RIP 消息身份验证（不推荐）。

Command Default

默认情况下使用明文身份验证。

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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

如果您指定 RIP 第 2 版，您可以启用邻居身份验证和使用基于 MD5 加密进行身份验证的 RIP 更新。

使用 **showinterface** 命令可查看接口上的 **ripauthentication** 命令。

CR_Examples

以下示例显示了在接口 GigabitEthernet0/3 上配置的 RIP 身份验证：

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

命令	说明
ripauthenticationkey	启用 RIP 第 2 版验证并指定验证密钥。
ripreceiveversion	指定要接受时接收更新特定接口上的 RIP 版本。
ripsendversion	指定要从特定的接口发送更新时使用的RIP版本。

命令	说明
showrunning-configinterface	显示指定接口的配置命令。
version	指定 ASA 全局使用的 RIP 版本。

rip authentication key

要启用 RIP 第 2 版数据包验证并指定验证密钥，请在接口配置模式下使用 **ripauthenticationkey**命令。要禁用 RIP 第 2 版验证，请使用此命令的 **no** 形式。

rip authentication key [**0**|**8**] *string***key_id***id*
no rip authentication key

Syntax Description

0	指定将遵循未加密的密码。
8	指定将遵循的加密密码。
ID	指定密钥标识值；有效值范围为 1 到 255。
key	指定要用于身份验证密钥字符串的共享密钥。密钥可包含最多 16 个字符。
string	指定未加密（明文）的用户密码。

Command Default

RIP 验证功能已禁用。

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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

如果您指定 RIP 第 2 版，您可以启用邻居身份验证和使用基于 MD5 加密进行身份验证的 RIP 更新。启用邻居身份验证时，必须确保 *key* 和 *key_id* 参数与提供 RIP 版本 2 更新的邻居设备所使用的参数相同。密钥是最多 16 个字符的文本字符串。

使用 **showinterface** 命令可查看接口上的 **ripauthentication** 命令。

CR_Examples

以下示例显示了在接口 GigabitEthernet 0/3 上配置的 RIP 身份验证：

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

Related Commands

命令	说明
ripauthenticationmode	指定 RIP 第 2 版数据包中使用的身份验证类型。
ripreceiveversion	指定要接受时接收更新特定接口上的 RIP 版本。
ripsendversion	指定要从特定的接口发送更新时使用的RIP版本。
showrunning-configinterface	显示指定接口的配置命令。
version	指定 ASA 全局使用的 RIP 版本。

rip receive version

要指定接口上接受的 RIP 版本，请在 **ripreceiveversion**接口配置模式下使用该命令。要恢复默认设置，请使用此命 **no**令的形式。

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

Syntax Description

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

Command Default

ASA 接受版本 1 和版本 2 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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

您可以通过在接口上输入命令来覆盖每个接口的 **ripreceiveversion**全局设置。

如果您指定 RIP 第 2 版，您可以启用邻居身份验证和使用基于 MD5 加密进行身份验证的 RIP 更新。

CR_Examples

以下示例将 ASA 配置为从指定接口接收 RIP 版本 1 和 2 数据包：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

命令	说明
ripsendversion	指定要从特定的接口发送更新时使用的 RIP 版本。
routerrip	启用 RIP 路由进程并进入该进程的路由器配置模式。
version	指定 ASA 全局使用的 RIP 版本。

rip send version

要指定用于在接口上发送 RIP 更新的 RIP 版本，请在 **ripsendversion**接口配置模式下使用该命令。要恢复默认设置，请使用此命 **no**令的形式。

rip send version{[**1**][**2**]}
no rip send version

Syntax Description

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

Command Default

ASA 发送 RIP 版本 1 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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

您可以通过在接口上输入命令来覆盖每个接口的**ripsendversion**全局 RIP 发送版本设置。

如果您指定 RIP 第 2 版，您可以启用邻居身份验证和使用基于 MD5 加密进行身份验证的 RIP 更新。

CR_Examples

以下示例将 ASA 配置为在指定接口上发送和接收 RIP 版本 1 和 2 数据包：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

命令	说明
ripreceiveversion	指定要接受时接收更新特定接口上的 RIP 版本。
routerrip	启用 RIP 路由过程和路由器配置模式下输入此过程。
version	指定 ASA 全局使用的 RIP 版本。

rmdir

要删除现有目录，请在 **rmdir** 特权 EXEC 模式下使用该命令。

rmdir[/**no confirm**][**disk0:**| **disk1:**| **flash:**]*path*

Syntax Description

/noconfirm	（可选）抑制确认提示。
disk0：	（可选）指定不可移动的内部闪存，后跟冒号。
disk1：	（可选）指定可移动的外部闪存卡，后跟冒号。
flash：	（可选）指定不可移动的内部闪存，后跟冒号。在 ASA 5500 系列自适应安全设备中，该 **flash**关键字的别名为 。 **disk0**
path	（可选）要删除的目录的绝对或相对路径。

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

如果目录不为空，则 **rmdir** 命令失败。

CR_Examples

以下示例展示如何删除名为 “test”的现有目录：

```
ciscoasa# rmdir test
```

Related Commands

命令	说明
dir	系统随即会显示目录的内容。
mkdir	创建新目录。

命令	说明
pwd	系统随即会显示当前工作目录。
showfile	显示有关文件系统的信息。

路由

要为指定的接口输入静态路由或默认路由，请在全局配置模式下使用 **route** 命令。要从指定接口删除路由，请使用此命 **no**令的形式。

接口route名称 *IP*地址 网络掩码 网关*IP*[[*metric*] ［**track***number*］|**tunneled**］
接口no route名称 *IP*地址 网络掩码 网关*IP*[[*metric*] [**track***number*] **tunneled**］

Syntax Description

gateway_ip	指定网关路由器的 IP 地址（此路由的下一跳地址）。 注释 在透明模式下， *gateway_ip* 参数是可选的。
interface_name	指定流量通过其路由的接口名称。请为透明模式指定网桥组成员接口名称。对于具有网桥组的路由模式，请指定 BVI 名称。在路由模式下，将不需要的**null0**流量“黑洞化”，进入接口。
ip_address	指定内部或外部网络 IP 地址。
metric	（可选）指定此路由的管理距离。有效值范围为 1 到 255。默认值为 1。
netmask	指定要应用于 *ip_address* 的网络掩码。
track数字	（可选）将跟踪条目与此路由关联。有效值范围为 1 至 500。 注释 该 **track**选项仅在单一路由模式下可用。
tunneled	指定路由作为 VPN 流量的默认隧道网关。 注释 虽然隧道静态路由也包含在 **show route management-only** 输出中，但该接口是非管理专用。

Command Default

指标 默认值为 1。

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
7.0(1)	添加了此命令。
7.2(1)	添加了 **track**数字 值。
9.2(1)	添加了 **null0**界面选项。
9.7(1)	使用集成路由和桥接时，增加了对路由模式下的BVI接口的支持。

使用指南

使用 **route** 命令可输入接口的默认路由或静态路由。要输入默认路由，请将 *ip_address* 和 *netmask* 设置为 **0.0.0.0,**或使用缩写形式**0**。在保存配置时，配置中将会存储使用 **route** 命令输入的所有路由。

您可以为隧道流量定义单独的默认路由以及标准默认路由。当您使用该 **tunneled**选项创建默认路由时，来自终止于ASA的隧道且无法使用学习或静态路由进行路由的所有流量都将发送到此路由。对于从隧道传出的流量，此路由将覆盖任何其他已配置或学习到的默认路由。

以下限制适用于带 **tunneled** 选项的默认路由：

- 请勿在隧道路由的传出接口上启用单播RPF (**ipverifyreverse-path**)。在隧道路由的传出接口上启用 uRPF 会导致会话失败。
- 不要在隧道路由的出口接口上启用 TCP 拦截，因为会话将会失败。
- 请勿使用带有VLAN映射选项或隧道路由的VoIP检查引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS 检查引擎或 DCE RPC 检查引擎。这些检测引擎将忽略 vlan 映射设置，这可能会导致错误地路由数据包。

您不能使用该选项定义多个默认路由；不支持隧道流量的 **tunneled**ECMP。

创建静态路由，以访问在任何接口上的路由器外部连接的网络。例如，ASA 使用以下静态路由命令发送通过 192.168.1.5 路由器发往 192.168.42.0 网络的所有数据包。

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

输入每个接口的 IP 地址后，ASA 会在路由表中创建一个 CONNECT 路由。当您使用 **clearroute** 或 **clearconfigureroute** 命令时，不会删除此条目。

与 ACL 不同，静态 **null0** 路由不会导致任何性能下降。 **null0** 配置用于防止路由环路。BGP 利用远程触发黑洞路由的 **null0**配置。

CR_Examples

以下示例显示如何为外部接口指定一个默认路由命令：

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

以下示例显示了如何添加这些静态路由命令以提供网络访问：

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

以下示例使用 SLA 操作在外部接口上安装到 10.1.1.1 网关的默认路由。SLA 操作会监控该网关的可用性。如果 SLA 操作失败，则使用 DMZ 接口上的备用路由。

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

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

以下示例显示如何配置静态 null0 路由：

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

Related Commands

命令	说明
clearconfigureroute	删除静态配置的 **route** 命令。
clearroute	删除通过动态路由协议（例如RIP）获知的路由。
showroute	显示路由信息。
showrunning-configroute	显示已配置的路由。

route-map

要定义将路由从一个路由协议重新分发到另一个路由协议的条件，或者要启用策略路由，请在全局配置模式下使用 route-map 命令并在 route-map 配置模式下使用 match 和 set 命令。要删除条目，请使用此命令的no形式。

名称route-map[**permit | deny**][序列号]
名称no route-map[**permit | deny**][序列号]

Syntax Description

name	为路线图定义一个有意义的名称。redistribute路由器配置命令使用此名称来引用此路由映射。多个路由映射可以共享相同的名称。
permit	如果满足此路由映射的匹配条件，并且指定了 permit 关键字，则路由将按照设置的操作控制重新分发。在策略路由的情况下，数据包进行策略路由。 如果不满足匹配条件，则指定了 permit 关键字，则测试下一个具有相同映射标记的路由映射。如果路由未向共享相同名称的路由映射组传递任何匹配条件，则该组不会重新分发路由。 permit 关键字是默认的。
deny	如果满足路由映射的匹配条件并且指定了 deny 关键字，则不重新分发路由。在策略路由的情况下，系统不对数据包进行策略路由，并且不会进一步检查共享相同映射标记名称的路由映射。如果数据包未经过策略路由，则使用普通转发算法。
sequence-number	数字，指示新路由映射在已配置为相同名称的路由映射列表中的位置。如果使用此命令的 no 形式指定，则应删除路由映射的位置。

Command Default

默认情况下，路由映射配置为允许和序列号 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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.2(1)	此命令已得到增强，在命令不完整时显示警告消息。

使用指南

使用路由映射重新分发路由

使用 route-map 全局配置命令以及 match 和 set route-map configuration 命令定义将路由从一个路由协议重新分发到另一个路由协议的条件。每个 route-map 命令都有一个与其关联的 match 和 set 命令列表。match 命令指定匹配条件，即允许对当前 route-map 命令进行重新分发的条件。set 命令指定 set 操作 - 当满足 match 命令执行的条件时要执行的特定重新分发操作。no route-map 命令具有此命令即可删除路由映射。

match route-map 配置命令有多种格式。匹配命令可以按任何顺序提供，并且所有匹配命令必须“通过”，以使路由根据使用 set 命令给出的 set 操作重新分发。match 命令的 no 形式将删除指定的匹配条件。

当需要对路由在路由进程之间的重新分发方式进行详细控制时，请使用路由映射。目标路由协议是使用路由器全局配置命令指定的协议。源路由协议是使用 redistribute 路由器配置命令指定的协议。请参阅“示例”部分中有关如何配置路由映射的说明。

通过路由映射传递路由时，路由映射可以有多个部分。不匹配至少一个与 route-map 命令相关的 match 子句的任何路由将被忽略；也就是说，系统将不为出站路由映射通告路由，也不会为入站路由映射接受路由。如果只想修改某些数据，则必须配置第二个路由映射部分，并指定显式匹配项。

序列号参数的工作原理如下：

1. 如果没有定义具有路由映射名称的条目，则会创建一个序列号参数设置为 10 的条目。

2. 如果仅使用路由映射名称定义了一个条目，则该条目将成为以下路由映射命令的默认条目。该条目的序列号参数保持不变。

3. 如果使用路由映射名称定义了多个条目，则会打印一条错误消息，表明需要序列号参数。

4. 如果指定 no route-map name 命令（不带 sequence-number 参数），则删除整个路由图。

CR_Examples

以下示例显示如何将跳数等于 1 的路由重新分发到 OSPF。ASA 将这些路由重新分配为度量为 5、度量类型为 1 类型的外部 LSA：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

以下示例显示如何使用配置的指标值将 10.1.1.0 静态路由重新分发到 eigrp 进程 1：

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

以下示例显示未指定操作和序列号时的 default-behavior：

```
ciscoasa(config)#route-map test ?
 <0-65535>     Sequence to insert to/delete from existing route-map entry
 deny          Route map denies set operations
 ordering-seq  Named ordering sequence
 permit        Route map permits set operations
```

```
ciscoasa(config)#route-map test
%Warning:Incomplete command: Operation Missing.The CLI will be deprecated soon
%Warning:lncomplete command: Sequence Number Missing.The CLI will be deprecated soon

ciscoasa#sh run | sec route-map
route-map test permit 10
```

注释 如果未指定操作和序列号，则会显示有关不完整 CLI 命令的警告消息，尽管使用默认值配置了路由映射。

Related Commands

命令	说明
redistribute	将路由从一个路由域重新分发到另一个路由域。
route	为接口创建静态或默认路由。
路由器	进入指定协议的路由器配置模式。

route priority high

要为 IS-IS IP 前缀分配高优先级，请在路由器 isis 配置模式下使用 **routeprioritythigh** 命令。要删除 IP 前缀优先级，请使用此命令的 **no** 形式

route priority high*tag-value*
no route priority high*tag-value*

Syntax Description

tag-value	为具有特定路由标记的 IS-IS IP 前缀分配高优先级。范围为 1 到 4294967295。

Command Default

未设置 IP 前缀优先级。

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

当使用该命令标记更高优先级的 **routeprioritythigh**IS-IS IP前缀以便在全局路由表中更快地处理和安装时，可以实现更快的收敛。例如，您可以帮助IP语音(VoIP)网关地址首先得到处理，以帮助VoIP流量比其他类型的数据包更快地更新。

CR_Examples

以下示例使用 **routeprioritythigh** 命令将标签值 100 分配给 IS-IS IP 前缀：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# route priority high tag 100
```

Related Commands

router-alert

要定义在具有 IP 选项检查的数据包头中出现路由器警报 IP 选项时的操作，请在 **router-alert**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。

router-alert action {**allow | clear**}
no router-alert action {**allow | clear**}

Syntax Description

allow	允许包含 Router Alert IP 选项的数据包。
clear	从数据包头中删除路由器警报选项，然后允许数据包。

Command Default

默认情况下，IP 选项检查允许包含路由器警报 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
8.2(2)	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。

路由器警报 (RTRALT) 或 IP 选项 20 会通知中转路由器检查数据包的内容，即使数据包不是发往该路由器。当实施 RSVP 和类似协议需要数据包传送路径上的路由器进行相对复杂的处理时，这种检查很有价值。

CR_Examples

以下示例显示如何在策略映射中设置针对协议违规的操作：

```
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
```

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。

router bgp

要配置边界网关协议 (BGP) 路由进程，请在全局配置模式下使用 router bgp 命令。要删除 BGP 路由进程，请使用此命令的 no 形式。

router bgp自治系统编号
no router bgp自治系统编号

Syntax Description

自治系统编号	自治系统的编号，用于向其他 BGP 路由器标识路由器并标记所传递的路由信息。范围从 1 到 65535 的数字。

Command Default

默认情况下未启用任何 BGP 路由进程。

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	—	• 是	• 支持	• 支持

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

通过此命令，您可以设置分布式路由核心，自动保证在自主系统之间无环路交换路由信息。

2009 年 1 月之前，分配给公司的 BGP 自主系统编号是 2 个八位组编号，范围介于 1 到 65535 之间，如 RFC 4271 边界网关协议 4 (BGP-4) 中所述。

由于对自治系统编号的需求不断增加，互联网编号分配机构 (IANA) 分配了 65536 到 4294967295 范围内的四个八位组的自治系统编号。

RFC 5396 自治系统 (AS) 编号的文本表示法 (RFC 5396) 介绍了自治系统编号的三种表示方法。Cisco 已实施以下两种方法：

- Asplain - 十进制值表示法，其中 2 字节和 4 字节自治系统编号都按其十进制值表示。例如，65526 是 2 字节的自治系统编号，234567 是 4 字节的自治系统编号。
- Asdot - 自治系统的点表示法，其中 2 字节自治系统编号用十进制值表示，4 字节自治系统编号用点表示法表示。例如，65526 是 2 字节自治系统编号，1.169031 是 4 字节自治系统编号（这是 234567 的十进制数字的点点表示法）。

有关表示自治系统号的第三种方法的详细信息，请参阅 RFC 5396。

CR_Examples

以下示例显示如何为编号为 100 的自治系统配置 BGP 进程：

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

Related Commands

命令	说明
showroutebgp	显示路由表。
showbgpsummary	显示所有边界网关协议 (BGP) 连接的状态

router eigrp

要启动 EIGRP 路由进程并为该进程配置参数，请在全局配置模式下使用 **routereigrp** 命令。要禁用 EIGRP 路由，请使用此命 **no**令的形式。

router eigrp*as-number*
no router eigrp*as-number*

Syntax Description

as_number	标识通往其他EIGRP路由器的路由的自治系统编号。它还用于标记路由信息。有效值为 1 至 65535。

Command Default

禁用 EIGRP 路由。

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	—	• 是	• 支持	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	支持多上下文模式。

使用指南

该 **routereigrp**命令创建一个 EIGRP 路由进程或进入现有 EIGRP 路由进程的路由器配置模式。您只能在 ASA 上创建单个 EIGRP 路由进程。

使用以下路由器配置模式命令来配置 EIGRP 路由进程：

- —启**auto-summary**用/禁用自动路由汇总。
- **default-information**- 启用/禁用接收和发送默认路由信息。
- — 定**default-metric**义重新分配到 EIGRP 路由进程的路由的默认指标。
- —**distanceeigrp**配置内部和外部 EIGRP 路由的管理距离。
- — 过**distribute-list**滤路由更新中接收和发送的网络。
- **eigrplog-neighbor-changes**- 启用/禁用邻居状态更改的日志记录。
- —启**eigrplog-neighbor-warnings**用/禁用邻居警告消息的记录。
- **eigrprouter-id**- 创建固定路由器 ID。

- **eigrpstub**- 为末节 EIGRP 路由配置 ASA。
- —**neighbor**静态定义 EIGRP 邻居。
- —**network**配置参与 EIGRP 路由进程的网络。
- —**passive-interface**将接口配置为充当被动接口。
- —**redistribute**将其他路由进程的路由重新分配到 EIGRP 中。

使用以下接口配置模式命令来配置特定于接口的 EIGRP 参数：

- **authenticationkeyeigrp**- 定义用于 EIGRP 消息身份验证的身份验证密钥。
- **authenticationmodeeigrp**- 定义用于 EIGRP 消息身份验证的身份验证算法。
- —**delay**配置接口的延迟度量。
- **hello-intervaleigrp**- 更改从接口发送出去的 EIGRP 呼叫数据包的间隔。
- **hold-timeeigrp**- 更改 ASA 通告的保持时间。
- **split-horizoneigrp**- 在接口上启用/禁用 EIGRP 水平分割。
- **summary-addresseigrp**- 手动定义汇总地址。

CR_Examples

以下示例显示如何进入自治系统编号为 100 的 EIGRP 路由进程的配置模式：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

Related Commands

命令	说明
clearconfigureeigrp	从运行配置中清除 EIGRP 路由器配置模式命令。
showrunning-configroutereigrp	显示运行配置中的 EIGRP 路由器配置模式命令。

router-id

要使用固定路由器 ID，请在路由器配置模式（适用于 OSPFv2）或 IPv6 路由器配置模式（适用于 OSPFv3）下使用 **router-id** 命令。要重置 OSPF 以使用之前的路由器 ID 行为，请使用此命令的 **no** 形式。

router-id*id*
no router-id [*id*]

Syntax Description

D	以 IP 地址格式指定路由器 ID。

Command Default

如果未指定，则使用 ASA 上最高级别的 IP 地址作为路由器 ID。

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
路由器配置	• 是	—	• 是	• 支持	—
IPv6 路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.0(2)	此命令的处理顺序已更改。命令现在处理先于 OSPFv2 配置中的 **network** 命令。
9.0(1)	支持多上下文模式和 OSPFv3。

使用指南

默认情况下，ASA 使用 OSPF 配置中 **network** 命令涵盖的接口上的最高级别 IP 地址。如果最高级别的 IP 地址是专用地址，则该地址在问候数据包和数据库定义中发送。要使用特定路由器 ID，请使用 **router-id** 命令指定路由器 ID 的全局地址。

路由器 ID 在 OSPF 路由域中必须是唯一的。如果同一 OSPF 域中的两个路由器使用相同的路由器 ID，则路由可能无法正常工作。

在 OSPF 配置中输入 **router-id** 命令之前，应输入 **network** 命令。这可以防止与 ASA 生成的默认路由器 ID 可能发生的冲突。如果有冲突，您将收到以下消息：

```
ERROR: router-id id in use by ospf process pid
```

要输入存在冲突的 ID，请删除包含导致冲突的 IP 地址的 **network** 命令，输入 **router-id** 命令，然后重新输入 **network** 命令。

集群

在第 2 层集群中，您需要配置 **router-id***id* 命令或者将路由器 ID 留空（前提是所有设备都接收相同的路由器 ID）。

CR_Examples

以下示例将路由器 ID 设置为 192.168.1.1：

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

Related Commands

命令	说明
routerospf	进入路由器配置模式。
showospf	显示关于OSPFv2路由过程的一般信息。

router-id cluster-pool

要为第 3 层集群部署指定路由器 ID 集群池，请在 OSPFv2 的路由器配置模式或 OSPFv3 的 IPv6 路由器配置模式下使用 **router-idcluster-pool** 命令。

router-id cluster-pool hostname | A.B.C.D*ip_pool*

Syntax Description

cluster-pool	在配置了第 3 层集群时，启用 IP 地址池的配置。
hostname | **A.B.C.D**	指定此 OSPF 进程的 OSPF 路由器 ID。EXTEN
ip_pool	指定IP地址池的名称。

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
路由器配置	• 是	—	• 是	—	—
IPv6 路由器配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

路由器 ID 在集群中的 OSPFv2 或 OSPFv3 路由域中必须是唯一的。如果同一 OSPFv2 或 OSPFv3 域中的两个路由器使用相同的路由器 ID，则集群中的路由可能无法正常工作。

在第 2 层集群中，您需要配置 **router-id***id* 命令或者将路由器 ID 留空（前提是所有设备都接收相同的路由器 ID）。

配置第 3 层集群接口时，每台设备都必须具有唯一的接口 IP 地址。为确保每台设备都有唯一的接口 IP 地址，可以使用 **router-idcluster-pool** 命令为 OSPFv2 或 OSPFv3 配置本地 IP 地址池。

CR_Examples

以下示例显示在为 OSPFv2 配置第 3 层集群时如何配置 IP 地址池：

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
```

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

以下示例显示在为 OSPFv3 配置第 3 层集群时如何配置 IP 地址池：

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

Related Commands

命令	说明
ipv6 router ospf	进入 IPv6 路由器配置模式。
routerospf	进入路由器配置模式。
show ipv6 ospf	显示关于OSPFv3路由过程的一般信息。
showospf	显示关于OSPFv2路由过程的一般信息。

router isis

要启用 IS-IS 路由协议并指定 IS-IS 进程，请在全局配置模式下使用 **routerisis** 命令。要禁用 IS-IS 路由，请使用此**no**命 令的形式。

router isis
no router isis

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令用于为区域启用 IS-IS 路由。必须配置适当的网络实体标题 (NET)，以指定 区域的区域地址和 ASA 的系统 ID。必须先在一个或多个接口上启用路由，然后才能建立邻接并实现动态路由。有关用于配置 IS-IS 的命令列表，请参阅相关命令表。

CR_Examples

以下示例中启用了 IS-IS 路由：

```
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Related Commands

router ospf

要启动 OSPF 路由进程并配置该进程的参数，请在 **routerospf**全局配置模式下使用该命令。要禁用 OSPF 路由，请使用此命 **no**令的形式。

router ospf*pid*
no router ospf*pid*

Syntax Description

pid	OSPF 路由进程内部使用的标识参数；其有效值范围为 1 至 65535。 *pid* 不需要匹配其他路由器上的 OSPF 进程的 ID。

Command Default

OSPF 路由已禁用。

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
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	支持多上下文模式。

使用指南

routerospf命令是用于在 ASA 上运行的 OSPF 路由进程的全局配置命令。输入 **routerospf** 命令后，命令提示符将显示为 (config-router)#，表示当前处于路由器配置模式。

使用 **norouterospf**命令时，除非可选参数提供必要的信息，否则无需指定可选参数。 **norouterospf**命令终止由其 *pid* 指定的 *OSPF* 路由进程。在 ASA 上本地分配 *PID* 。必须为每个 OSPF 路由进程分配唯一的值。

routerospf 命令与以下 OSPF 特定命令一起使用，以配置 OSPF 路由进程：

- **area**- 配置常规 OSPF 区域。
- —**compatiblerfc1583**恢复根据 RFC 1583 计算汇总路由成本的方法。
- —**default-informationoriginate**在 OSPF 路由域中生成默认外部路由。
- —**distance**根据路由类型定义 OSPF 路由管理距离。
- —**ignore**当路由器接收到类型 6 多播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制发送系统日志消息。

- —**log-adj-changes**配置路由器在 OSPF 邻居启动或关闭时发送系统日志消息。
- —指**neighbor**定邻居路由器。用于允许通过 VPN 隧道建立邻接关系。
- — 定**network**义运行 OSPF 的接口以及这些接口的区域 ID。
- —**redistribute**根据指定的参数配置从一个路由域到另一个路由域的路由重新分配。
- **router-id**- 创建固定路由器 ID。
- — 为 OSPF**summary-address**创建聚合地址。
- **timerlsaarrival**- 定义接受来自 OSPF 邻居的相同链路状态通告 (LSA) 的最小间隔（以毫秒为单位）。
- — 定**timerpacingflood**义洪泛队列中的 LSA 更新之间的最小间隔（以毫秒为单位）。
- **timerpacinglsa-group**- 定义 LSA 组被刷新或管理的间隔（以秒为单位）。
- **timerpacingretransmission**- 定义邻居重新传输的最小间隔（以毫秒为单位）。
- — 定**timerthrottlelsa**义生成第一个 LSA 的延迟（以毫秒为单位）。
- **timerthrottlespf**— 定义接收 SPF 计算更改之间的延迟（以毫秒为单位）。
- **timernsfwait**- 定义 NSF 重新启动期间的接口等待间隔。默认值为 20 秒。允许的范围是 1 至 65535 秒。

CR_Examples

以下示例显示如何进入编号为 5 的 OSPF 路由进程的配置模式：

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

Related Commands

命令	说明
clearconfigurerouter	从运行配置中清除OSPF路由器命令。
showrunning-configrouterospf	显示运行配置中的OSPF路由器命令。

router rip

要启动 RIP 路由进程并为该进程配置参数，请在全局配置模式下使用 **routerrip**命令。要禁用 RIP 路由进程，请使用此命 **no**令的形式。

router rip
no router rip

Syntax Description

此命令没有任何参数或关键字。

Command Default

RIP 路由被禁用。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

routerrip命令是用于在 ASA 上配置 RIP 路由进程的全局配置命令。您只能在 ASA 上配置一个 RIP 进程。该 **norouterrip** 命令终止 RIP 路由进程并删除该进程的所有路由器配置。

输入 **routerrip** 命令时，命令提示符更改为 ciscoasa(config-router)#，表示当前处于路由器配置模式。

routerrip 命令与以下路由器配置命令一起使用，以配置 RIP 路由进程：

- —启**auto-summary**用/禁用路由自动汇总。
- **default-informationoriginate**- 分发默认路由。
- **distribute-listin**- 过滤传入路由更新中的网络。
- **distribute-listout**- 过滤传出路由更新中的网络。
- **network**- 在路由进程中添加/删除接口。
- **passive-interface**- 将特定接口设置为被动模式。
- —**redistribute**将其他路由进程的路由重新分配到 RIP 路由进程中。
- **version**- 设置 ASA 使用的 RIP 协议版本。

此外，您可以在接口配置模式下使用以下命令逐个接口配置 RIP 属性：

- 一设**ripauthenticationkey**置身份验证密钥。
- **ripauthenticationmode**- 设置 RIP 版本 2 使用的身份验证类型。
- **ripsendversion**- 设置用于从接口发送更新的 RIP 版本。这会覆盖在全局路由器配置模式下设置的版本（如有）。
- **ripreceiveversion**- 设置接口接受的 RIP 版本。这会覆盖在全局路由器配置模式下设置的版本（如有）。

透明模式不支持 RIP。默认情况下，ASA 拒绝所有 RIP 广播和组播数据包。要允许这些 RIP 消息通过在透明模式下运行的 ASA，必须定义访问列表条目以允许这些流量。例如，要允许 RIP 版本 2 流量通过 ASA，请创建如下所示的访问列表条目：

ciscoasa(config)# **access-listmyriplistextendedpermitipanyhost224.0.0.9**

要允许 RIP 版本 1 广播，请创建如下访问列表条目：

ciscoasa(config)# **access-listmyriplistextendedpermitudpanyanyeqrip**

使用 **access-group**命令将这些访问列表条目应用于适当的接口。

您可以在 ASA 上同时启用 RIP 和 OSPF 路由。

CR_Examples

以下示例显示如何进入编号为 5 的 OSPF 路由进程的配置模式：

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

Related Commands

命令	说明
clearconfigurerouterrip	从运行配置中清除 RIP 路由器命令。
showrunning-configrouterrip	显示运行配置中的 RIP 路由器命令。

rtp-conformance

要检查流经针孔的RTP数据包的H.323和SIP协议符合性，请在参数配置模式下使用**rtp-conformance**命令。要禁用此功能，请使用此**no** 命令的形式。

rtp-conformance [**enforce-payloadtype**]
no rtp-conformance [**enforce-payloadtype**]

Syntax Description

实施负载类型	根据信令交换将负载类型强制为音频/视频。

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
7.2(1)	添加了此命令。

CR_Examples

以下示例显示在 H.323 呼叫中如何检查流经针孔的 RTP 数据包的协议符合性：

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

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。
调试 rtp	显示与 H.323 和 SIP 检查相关的 RTP 数据包的调试信息和错误消息。
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。

rtp-min-port rtp-max-port（已弃用）

要为电话代理功能配置 rtp 最小端口和 rtp 最大端口限制，请在电话代理配置模式下使用 **rtp-min-portrtp-max-port**命令。要从电话代理配置中删除限制，请使用此命令的 **no**形式。

rtp-min-port*port1***rtp-maxport***port2*
no rtp-min-port*port1***rtp-maxport***port2*

Syntax Description

port1	指定媒体终端的 RTP 端口范围的最小值，其中 *port1* 可以是 1024 到 16384 之间的值。
port2	指定媒体终端点的 RTP 端口范围的最大值，其中 *port2* 可以是 32767 到 65535 之间的一个值。

Command Default

默认情况下， **rtp-min-port** 关键字的 *port1* 值为 16384， **rtp-max-port** 关键字的 *port2* 值为 32767。

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
电话代理配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	命令已添加。
9.4(1)	此命令与所 **phone-proxy**有模式命令一起已被弃用。

使用指南

需要扩展电话代理支持的呼叫数量时，请配置媒体终端点的 RTP 端口范围。

CR_Examples

以下示例展示如何使用 **rtp-min-port**命令指定用于媒体连接的端口：

```
ciscoasa
(config-phone-proxy)#
rtp-min-port 2001 rtp-maxport 32770
```

Related Commands

命令	说明
phone-proxy	配置电话代理实例。

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。