



Cisco 安全防火墙 ASA 系列命令参考，I - R 命令

上次修改日期: 2025 年 7 月 9 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. 保留所有权利。



第 I 部分

I 命令

- [ia - inr](#) , 第 1 页
- [inspect a - inspect z](#) , 第 73 页
- [int - ipu](#) , 第 157 页
- [ipv - ir](#) , 第 233 页
- [is - iz](#) , 第 317 页



ia – inr

- [icmp](#) , 第 3 页
- [icmp-object](#) , 第 5 页
- [icmp unreachable](#) , 第 7 页
- [id-cert-issuer](#) , 第 9 页
- [id-mismatch](#) , 第 11 页
- [id-randomization](#) , 第 13 页
- [id-usage](#) , 第 14 页
- [igmp](#) , 第 16 页
- [igmp access-group](#) , 第 17 页
- [igmp forward interface](#) , 第 18 页
- [igmp join-group](#) , 第 19 页
- [igmp limit](#) , 第 20 页
- [igmp query-interval](#) , 第 22 页
- [igmp query-max-response-time](#) , 第 24 页
- [igmp query-timeout](#) , 第 25 页
- [igmp static-group](#) , 第 26 页
- [igmp 版本](#) , 第 27 页
- [ignore-ipsec-keyusage \(已弃用\)](#) , 第 29 页
- [ignore lsa mospf](#) , 第 30 页
- [ignore-lsp-errors](#) , 第 31 页
- [ignore-ssl-keyusage \(已弃用\)](#) , 第 35 页
- [ike-retry-count](#) , 第 36 页
- [ikev1 pre-shared-key](#) , 第 38 页
- [ikev1 trust-point](#) , 第 40 页
- [ikev1 user-authentication](#) , 第 41 页
- [ikev2 local-authentication](#) , 第 43 页
- [ikev2 mobike-rrc](#) , 第 45 页
- [ikev2 remote-authentication](#) , 第 47 页
- [ikev2 rsa-sig-hash](#) , 第 49 页

- [im](#) , 第 50 页
- [imap4s](#) (已弃用) , 第 51 页
- [imi-traffic-descriptor](#) , 第 53 页
- [import](#) , 第 55 页
- [import webvpn AnyConnect-customization](#) , 第 58 页
- [import webvpn customization](#) , 第 60 页
- [import webvpn mst-translation](#) , 第 62 页
- [import webvpn plug-in protocol](#) , 第 63 页
- [import webvpn translation-table](#) , 第 66 页
- [import webvpn url-list](#) , 第 69 页
- [import webvpn webcontent](#) , 第 71 页

icmp

要为在 Cisco Secure Firewall ASA 接口终止的 ICMP 流量配置访问规则，请使用 **icmp** 命令。要删除配置，请使用此命令 **no** 的形式。

```
icmp {permit|deny} ip_addressnet_mask [icmp_type] if_name
no icmp {permit|deny} ip_addressnet_mask [icmp_type] if_name
```

Syntax Description

deny 如果条件匹配则拒绝访问。

icmp_type （可选）ICMP 消息类型（请参阅表 1-1）。

if_name 接口名称。

ip_address 向接口发送 ICMP 消息的主机的 IP 地址。

net_mask 要应用于主机 IP 地址的网络掩码。

permit 如果条件匹配则允许访问。

Command Default

ASA 的默认行为是允许所有 ICMP 流量到达 ASA 接口。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

icmp 命令控制在任何 ASA 接口上终止的 ICMP 流量。如果未配置 ICMP 控制列表，则 ASA 接受在任何接口（包括外部接口）终止的所有 ICMP 流量。但是，默认情况下，ASA 不会响应发送到广播地址的 ICMP 回显请求。

ASA 仅响应发送到流量进入接口的 ICMP 流量；您不能通过接口将 ICMP 流量发送到远端接口。

除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 VPN 访问。例如，如果 VPN 访问位于外部接口上，则只能直接向外部接口发起连接。应在 ASA 的可直接访问的接口上启用 VPN，并使用域名解析，以便您不必记住多个地址。

icmp deny 命令禁用对接口的 ping，而 icmp permit 命令则启用对接口的 ping。如果禁用 ping，则无法在网络上检测到 ASA。这也称为可配置代理 ping。

对通过 ASA 路由到受保护接口上的目标的 ICMP 流量使用 access-list Extended 或 access-group 命令。

我们建议您授予 ICMP 不可达消息类型（类型 3）的权限。拒绝 ICMP 不可达消息会禁用 ICMP 路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。有关路径 MTU 发现的详细信息，请参阅 RFC 1195 和 RFC 1435。

如果为接口配置了 ICMP 控制列表，则 ASA 首先匹配指定的 ICMP 流量，然后对该接口上的所有其他 ICMP 流量应用隐式拒绝。也就是说，如果第一个匹配的条目是允许条目，系统将继续处理 ICMP 数据包。如果第一个匹配的条目是拒绝条目或条目不匹配，则 ASA 会丢弃 ICMP 数据包并生成系统日志消息。但未配置 ICMP 控制列表时除外；在这种情况下，假定为 permit 语句。

下表列出了支持的 ICMP 类型值。

表 1: ICMP 类型和文字

ICMP 类型	文字	说明
0	echo-reply	回应应答是对回应请求的响应，用于指示成功的通信。
3	unreachable	设备无法将包传送到最终目的地。
8	echo	承载源地址的回应消息。此地址为 echo-reply 消息的目标。
11	time-exceeded	在处理包期间，设备将生存时间值识别为 0 且因此该包被丢弃。

CR_Examples

以下示例拒绝外部接口上的所有 ping 请求和所有传入 ICMP 连接（不可达消息除外）：

```
ciscoasa(config)# icmp permit any unreachable outside
```

继续为其他每个要拒绝其上的 ICMP 流量的 icmpdenyany 接口 输入 命令。

以下示例允许主机 172.16.2.15 或子网 172.22.1.0/16 上的主机 ping 外部接口：

```
ciscoasa(config)# icmp permit host 172.16.2.15 echo outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo outside
ciscoasa(config)# icmp permit any unreachable outside
```

Related Commands

命令	说明
clearconfigureicmp	清除 ICMP 配置。
debugicmp	启用显示 ICMP 的调试信息。
showicmp	显示 ICMP 配置。
timeouticmp	配置 ICMP 的空闲超时。

icmp-object

要将 ICMP 类型添加至 ICMP 对象组，请在 `icmp-type` 配置模式下使用 `icmp-object` 命令。要删除 ICMP 类型，请使用此命令的形式。

icmp-object*icmp_type*
no icmp-object*icmp_type*

Syntax Description

icmp_type 指定 ICMP 类型名称或编号 (0-255)。

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
ICMP 类型配置	• 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

icmp-object 命令与 **object-groupicmp-type** 命令一起使用以定义 ICMP 对象。它在 `icmp` 类型配置模式下使用。

不要使用此命令，而应使用 **object-groupservice** 和 **service-group** 命令创建包含 ICMP 类型的服务组。服务组可以包括 ICMP6 和 ICMP 代码，但 ICMP 对象不能。

ICMP 类型号和名称包括：

数字	ICMP 类型名称
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address

数字	ICMP 类型名称
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	address-mask-request
18	address-mask-reply
31	conversion-error
32	mobile-redirect

CR_Examples

以下示例显示如何在 icmp-type 配置模式下使用 **icmp-object** 命令：

```
ciscoasa(config)# object-group icmp-type icmp_allowed
ciscoasa(config-icmp-type)# icmp-object echo
ciscoasa(config-icmp-type)# icmp-object time-exceeded
ciscoasa(config-icmp-type)# exit
```

Related Commands

命令	说明
clearconfigureobject-group	从配置中 object-group 删除所有命令。
object-group	定义对象组以优化您的配置。
showrunning-configobject-group	显示当前对象组。

icmp unreachable

要为在 ASA 接口终止的 ICMP 流量配置不可达的 ICMP 消息速率限制，请使用 **icmpunreachable** 命令。要删除配置，请使用此命令 **no** 的形式。

icmp unreachable rate-limit*rateburst-sizesize*
no icmp unreachable rate-limit*rateburst-sizesize*

Syntax Description

rate-limit*rate* 设置不可达消息的速率限制，介于每秒 1 到 100 条消息之间。默认值为每秒 1 条消息。

burst-size*size* 设置突发率，介于 1 和 10 之间。发送的回复数量为突发大小，但在达到速率限制之前不会发送后续回复。

Command Default

默认的速率限制为每秒 1 条消息。

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(2) 添加了此命令。

使用指南

如果允许将 ICMP 消息（包括不可达消息）发送到 ASA 接口（请参阅 **icmp** 命令），则可以控制不可达消息的速率。

需要此命令和该 **setconnectiondecrement-ttl** 命令来允许通过 ASA 的跟踪路由，以将 ASA 显示为跳数之一。

CR_Examples

以下示例启用生存时间递减并设置 ICMP 不可达速率限制：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
```

```
ciscoasa(config)# icmp permit any unreachable outside
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 10
```

Related Commands

命令	说明
clearconfigureicmp	清除 ICMP 配置。
debugicmp	启用显示 ICMP 的调试信息。
setconnectiondecrement-ttl	减小数据包的生存时间值。
showicmp	显示 ICMP 配置。
timeouticmp	配置 ICMP 的空闲超时。

id-cert-issuer

要指示系统是否接受由与此信任点关联的 CA 颁发的对等证书，请在 `crypto ca-trustpoint` 配置模式下使用 **id-cert-issuer** 命令。要禁止与信任点关联的 CA 颁发的证书，请使用此命令的 **no** 形式。这对于代表广泛使用的根 CA 的信任点非常有用。

id-cert-issuer
no id-cert-issuer

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认设置为启用（接受身份证书）。

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
加密 ca-trustpoint 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

使用此命令可限制只接受由广泛使用的根证书中的从属证书颁发的证书。如果不允许此功能，ASA 将拒绝此颁发者签署的所有 IKE 对等体证书。

CR_Examples

以下示例进入 Trustpoint Central 的 `crypto ca trustpoint` 配置模式，并允许管理员接受由 trustpoint Central 的颁发者签名的身份证书：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# id-cert-issuer
ciscoasa(ca-trustpoint)#
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。
defaultenrollment	将注册参数还原为其默认值。

命令	说明
enrollmentretrycount	指定尝试发送注册请求的重试次数。
enrollmentretryperiod	指定在尝试发送注册请求之前等待的分钟数。
enrollmentterminal	指定向该信任点进行剪切并粘贴注册。

id-mismatch

要对过多的 DNS ID 不匹配启用日志记录，请在参数配置模式下使用 **id-mismatch** 命令。要禁用此功能，请使用此 **no** 命令的形式。

id-mismatch [*countnumber* *durationseconds*] **actionlog**
id-mismatch [*countnumber* *durationseconds*] **actionlog**

Syntax Description

countnumber 发送系统消息日志之前不匹配实例的最大数量。

durationseconds 要监控的时间段（以秒为单位）。

Command Default

此命令默认禁用。如果启用该命令时未指定选项，则默认速率为 3 秒内 30。

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。

使用指南

DNSID 不匹配率高可能表示存在缓存投毒攻击。可以启用此命令以监控和警告此类尝试。如果不匹配率超过配置的值，将打印摘要系统消息日志。 **id-mismatch** 命令为系统管理员提供在常规基于事件的系统消息日志之外的附加信息。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 ID 不匹配：

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

Related Commands

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

命令	说明
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。

id-randomization

要为 DNS 查询随机化 DNS 标识符，请在参数配置模式下使用 **id-randomization** 命令。要禁用此功能，请使用此 **no** 命令的形式。

id-randomization
no id-randomization

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下已禁用。不会修改来自 DNS 查询的 DNS 标识符。

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。

使用指南

ID 随机化有助于防御缓存毒化攻击。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 ID 随机化：

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

Related Commands

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

id-usage

要指定如何使用证书的已注册身份，请在 `crypto ca trustpoint` 配置模式下使用 **id-usage** 命令。要将证书的用途设置为默认，请使用此命令的 **no** 形式。

```
id-usage { ssl-ipsec | code-signer }
no id-usage { ssl-ipsec | code-signer }
```

Syntax Description	code-signer 此证书表示的设备身份用作 Java 代码签名者，以验证提供给远程用户的小程序。
	ssl-ipsec （默认）此证书代表的设备身份可用作 SSL 或 IPsec 加密连接的服务器端身份。

Command Default 该 **id-usage** 命令默认为 **ssl-ipsec**

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 trustpoint 配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南 根据部署要求，远程访问 VPN 可以使用 SSL、IPsec 或两种协议，以允许访问几乎任何网络应用程序或资源。**id-usage** 命令允许您指定对各种受证书保护的资源的访问类型。

CA 身份，以及某些情况下的设备身份，都基于 CA 颁发的证书。`crypto ca trustpoint` 配置模式中的所有命令均控制 CA 特定的配置参数，这些参数指定 ASA 如何获取 CA 证书、ASA 如何从 CA 获取其证书以及 CA 颁发的用户证书的身份验证策略。

信任点配置中只能存在 **id-usage** 命令的一个实例。要为 **code-signer** 和/或 **ssl-ipsec** 选项启用信任点，请使用一个实例，它可以指定一个或两个选项。

CR_Examples 以下示例进入信任点中心的加密 ca 信任点配置模式，并将其指定为代码签名者证书：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer
ciscoasa(config-ca-trustpoint)#
```

以下示例进入常规信任点的 `crypto ca trustpoint` 配置模式，并将其指定为代码签名者证书以及 SSL 或 IPsec 连接的服务器端身份：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

以下示例进入信任点 `checkin1` 的 `crypto ca trustpoint` 配置模式，并重置以限制其用于 SSL 或 IPsec 连接：

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# noid-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。
java-trustpoint	配置 WebVPN Java 对象签名工具以使用来自指定信任点位置的 PKCS12 证书和密钥材料。
ssltrust-point	指定代表接口的 SSL 证书的证书。
trust-point(tunnel-groupipsec-attributesmode)	指定要发送给 IKE 对等体的证书的名称，
validation-policy	指定验证与用户连接关联的证书的条件。

igmp

要恢复接口上的 IGMP 处理，请在 **igmp** 接口配置模式下使用该命令。要禁用接口上的 IGMP 处理，请使用此命 **no** 令的形式。

igmp
no igmp

Syntax Description 此命令没有任何参数或关键字。

Command Default 已启用。

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
7.0(1)	添加了此命令。

使用指南 此命令仅 **no** 形式出现在运行配置中。

CR_Examples 以下示例在所选接口上禁用 IGMP 处理：

```
ciscoasa(config-if)# no igmp
```

命令	说明
showigmpgroups	显示直接连接到 ASA 且通过 IGMP 获知的具有接收器的多播组。
showigmpinterface	显示接口的组播信息。

igmp access-group

要控制由接口提供服务的子网上的主机可以加入的组播组，请在接口配置模式下使用 **igmpaccess-group** 命令。要禁用接口上的组，请使用此命令 **no** 的形式。

igmp access-groupacl
no igmp access-groupacl

Syntax Description

acl IP 访问列表的名称。您可以指定标准和扩展访问列表。但是，如果指定扩展访问列表，则仅匹配目标地址，而不会选择目标地址。则应为源指定 **any**。

Command Default

所有组都可以通过某个接口加入。

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

7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

CR_Examples

以下示例限制了访问列表 1 允许的主机加入组的行为：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp access-group 1
```

Related Commands

命令	说明
showigmpinterface	显示接口的组播信息。

igmp forward interface

要允许将所有 IGMP 主机报告和离开消息转发到指定的接口，请在接口配置模式下使用 **igmpforwardinterface** 命令。要删除转发，请使用此命令 **no** 的形式。

```
igmp forward interfaceif-name
no igmp forward interfaceif-name
```

Syntax Description *if-name* 接口的逻辑名称。

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
接口配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

使用指南 在输入接口上输入此命令。此命令用于末节组播路由，不能与 PIM 同时配置。

CR_Examples 以下示例将 IGMP 主机报告从当前接口转发到指定接口：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp forward interface outside
```

命令	说明
showigmpinterface	显示接口的组播信息。

igmp join-group

要将接口配置为指定组的本地连接成员，请在接口配置模式下使用 **igmp join-group** 命令。要取消在组中的成员身份，请使用此命令的 **no** 形式。

igmp join-group group-address
no igmp join-group group-address

Syntax Description

group-address 多播组的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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

使用指南

此命令将 ASA 接口配置为多播组的成员。**igmp join-group** 命令导致 ASA 接受并转发以指定组播组为目标的组播数据包。

要将 ASA 配置为在不成为组播组成员的情况下转发组播流量，请使用 **igmpstatic-group** 命令。

CR_Examples

以下示例将所选接口配置为加入 IGMP 组 255.2.2.2：

```
ciscoasa(config)# interface gigabitethernet 0/0  
ciscoasa(config-if)# igmp join-group 255.2.2.2
```

Related Commands

命令	说明
igmpstatic-group	将接口配置为指定组播组的静态连接成员。

igmp limit

要基于每个接口限制IGMP状态数量，请在接口配置模式下使用 **igmplimit** 命令。要恢复默认限制，请使用此命 **no** 令的形式。

igmp limit编号
no igmp limit[编号]

Syntax Description	<i>number</i> 接口上允许的 IGMP 状态数。有效值范围是 0 到 5000。默认值为 500。将此值设置为 0 可防止添加学习组，但仍允许手动定义成员资格（使用 igmpjoin-group 和 igmpstatic-group 命令）。

Command Default	默认值为 500。

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
	7.0(1)	添加了此命令。它取代了 igmpmax-groups 命令。
	9.15(1)	igmp 限制从 500 增加到 5000。
	同样在 9.12(4) 中	

使用指南	此命令用于配置 IGMP 状态的限制。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发。 当您更改接口上具有活动加入的 IGMP 限制时，新限制不适用于现有组。仅当将新组添加到接口或 IGMP 加入计时器到期时，ASA 才会验证限制。要应用新的限制并立即生效，必须在接口上禁用并重新启用 IGMP。

CR_Examples	以下示例将接口上的 IGMP 状态数量限制为 250：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp limit 250
```


Related Commands

命令	说明
igmp	恢复接口上的 IGMP 处理。
igmpjoin-group	将接口配置为指定组的本地连接成员。
igmpstatic-group	将接口配置为指定组播组的静态连接成员。

igmp query-interval

要配置接口发送 IGMP 主机查询消息的频率，请在接口配置模式下使用 **igmpquery-interval** 命令。要恢复默认频率，请使用此命令 **no** 的形式。

igmp query-interval秒
no igmp query-interval秒

Syntax Description *seconds* 发送 IGMP 主机查询消息的频率（以秒为单位）。有效值范围为 1 至 3600。默认值为 125 秒。

Command Default 默认查询间隔为125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
接口配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

使用指南 多播路由器发送主机查询消息来发现哪些多播组在连接到接口的网络上拥有成员。主机以 IGMP 报告消息进行响应，表明它们想要接收特定组的多播数据包。主机查询消息发送给所有主机多播组，该组的地址为 224.0.0.1，TTL 值为 1。

- LAN 的指定路由器是发送 IGMP 主机查询消息的唯一路由器：
- 对于 IGMP 版本 1，系统将根据 LAN 上运行的组播路由协议选择指定路由器。
 - 对于 IGMP 版本 2，指定路由器是子网上 IP 地址最低的组播路由器。

如果路由器在超时期限（由 **igmpquery-timeout** 命令控制）内没有侦听查询，它将成为查询器。



注意 更改此值可能会严重影响组播转发。

CR_Examples 以下示例将 IGMP 查询间隔更改为 120 秒：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-interval 120
```

Related Commands	命令	说明
	igmpquery-max-response-time	配置 IGMP 查询中通告的最大响应时间。
	igmpquery-timeout	配置在上一个查询器已停止查询后，路由器接管接口的查询器之前的超时期限。

igmp query-max-response-time

要指定 IGMP 查询中通告的最大响应时间，请在接口配置模式下使用 **igmpquery-max-response-time** 命令。要恢复默认响应时间值，请使用此命令 **no** 的形式。

igmpquery-max-response-time*seconds*
no igmpquery-max-response-time*秒*

Syntax Description *seconds* IGMP 查询中通告的最大响应时间（以秒为单位）。有效值为 1 至 25。默认值为 10 秒。

Command Default 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
接口配置	• 是	—	• 是	—	—

Command History 版本 修改
7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

使用指南 此命令仅在 IGMP 版本 2 或 3 运行时有效。
此命令用于控制路由器删除组之前，响应方可以响应 IGMP 查询消息的时间段。

CR_Examples 以下示例将最大查询响应时间更改为 8 秒：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-max-response-time 8
```

命令	说明
igmpquery-interval	配置接口发送 IGMP 主机查询消息的频率。
igmpquery-timeout	配置在上一个查询器已停止查询后，路由器接管接口的查询器之前的超时期限。

igmp query-timeout

在上一个查询器停止查询后，要配置接口接管查询器作为查询器之前的超时期限，请在接口配置模式下使用 **igmpquery-timeout** 命令。要恢复默认值，请使用此命令的 **no** 形式。

igmpquery-timeout*seconds*
no igmpquery-timeout秒

Syntax Description

seconds 在之前的查询器停止查询之后且在其接管成为查询器之前路由器等待的秒数。有效值范围为 60 至 300 秒。默认值为 255 秒。

Command Default

默认查询间隔为255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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令需要 IGMP 版本 2 或 3。

CR_Examples

以下示例将路由器配置为从接收到最后一个查询之时起等待 200 秒，然后接管作为接口的查询器：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-timeout 200
```

Related Commands

命令	说明
igmpquery-interval	配置接口发送 IGMP 主机查询消息的频率。
igmpquery-max-response-time	配置 IGMP 查询中通告的最大响应时间。

igmp static-group

要将接口配置为指定组播组的静态连接成员，请在接口配置模式下使用 **igmpstatic-group** 命令。要删除静态组条目，请使用此命令 **no** 的形式。

```
igmp static-groupgroup
no igmp static-groupgroup
```

Syntax Description	group IP 多播组地址。

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
接口配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用 **igmpstatic-group** 命令表示，ASA 接口不接收发往指定组本身的组播数据包；而是接收。接收方仅会转发这些数据包。如要将 ASA 配置为同时接受和转发特定组播组的组播数据包，请使用 **igmpjoin-group** 命令。如果为与 **igmpjoin-group** 命令相同的组地址配置了 **igmpstatic-group** 命令，则 **igmpjoin-group** 命令优先，并且该组的行为类似于本地加入的组。

CR_Examples 以下示例将所选接口添加到组播组 239.100.100.101：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp static-group 239.100.100.101
```

Related Commands	命令	说明
	igmpjoin-group	将接口配置为指定组的本地连接成员。

igmp 版本

要配置接口使用的 IGMP 版本，请在接口配置模式下使用 **igmpversion** 命令。要将版本恢复为默认值，请使用此 **no** 命令的形式。

igmpversion { 1 | 2 }
no igmp version [1 | 2]

Syntax Description

1IGMP 版本

1。

2IGMP 版本

2。

Command Default

IGMP 版本 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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 该命令已移至接口配置模式。早期版本要求进入组播接口配置模式，此模式不再可用。

使用指南

子网上的所有路由器必须支持相同版本的 IGMP。主机可以具有任何 IGMP 版本（1 或 2），ASA 将正确检测主机是否存在并进行适当的查询。

某些命令需要 IGMP 版本 2，包括 as **igmpquery-max-response-time**和 **igmpquery-timeout** 命令。

CR_Examples

以下示例将所选接口配置为使用 IGMP 版本 1：

```
ciscoasa(config)# interface gigabitethernet 0/0  
ciscoasa(config-if)# igmp version 1
```

Related Commands

命令	说明
igmpquery-max-response-time	配置 IGMP 查询中通告的最大响应时间。

命令	说明
igmpquery-timeout	配置在上一个查询器已停止查询后，路由器接管接口的查询器之前的超时期限。

ignore-ipsec-keyusage (已弃用)

要禁止对 IPsec 客户端证书进行密钥用法检查，请在 `ca-trustpoint` 配置模式下使用 **ignore-ipsec-keyusage** 命令。要恢复密钥使用检查，请使用此命令的 **no** 形式。

ignore-ipsec-keyusage
no ignore-ipsec-keyusage

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
CA-trustpoint 配置	• 是	—	• 是	—	—

Command History 版本 修改

8.0(2) 此命令被添加为一项安全措施，但同时已被弃用。请注意，未来的版本可能不提供密钥用法检查抑制。

使用指南 使用此命令表示 IPsec 远程客户端证书的密钥用法和扩展密钥用法扩展中的值不被验证。此命令会忽略密钥使用检查，适用于不合规的部署。

CR_Examples 以下示例显示如何忽略密钥使用检查的结果：

```
ciscoasa(config)#crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。

ignore lsa mospf

要在路由器接收 LSA 6 类 MOSPF 数据包时抑制发送系统日志消息，请在路由器配置模式下使用 **ignorelsamospf** 命令。要恢复系统日志消息的发送，请使用此 **no** 命令的形式。

ignore lsa mospf
no ignore lsa mospf

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
路由器配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

不支持类型 6 MOSPF 数据包。

CR_Examples

以下示例导致 LSA 类型 6 MOSPF 数据包被忽略：

```
ciscoasa(config-router)# ignore lsa mospf
```

Related Commands

命令	说明
showrunning-configrouterospf	显示 OSPF 路由器配置。

ignore-lsp-errors

要让 ASA 忽略收到的内部校验和错误的 IS-IS 链路状态数据包而不是清除链路状态数据包，请在路由器 isis 配置模式下使用 **ignore-lsp-errors** 命令。要禁用该功能，请使用此命令的 **no** 形式。

ignore-lsp-errors
no ignore-lsp-errors

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下会启用此命令，也就是说，不会为网络清除损坏的 LSP，而是丢弃损坏的 LSP 稳定性

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

IS-IS 协议定义要求接收方清除接收到的具有不正确数据链路校验和的链路状态数据包，这会导致数据包的发起方重新生成该数据包。但是，如果网络中的某个链路导致数据损坏，但仍然传递具有正确数据链路校验和的链路状态数据包，则可能会发生连续清除和重新生成大量数据包的循环。

由于这可能导致网络无法正常工作，请使用 **ignore-lsp-errors** 命令忽略这些链路状态数据包，而不是清除数据包。接收路由器使用链路状态数据包来维护其路由表。

如果要明确清除损坏的 LSP，请发出 **noignore-lsp-errors** 命令。

CR_Examples

以下示例指示路由器忽略具有内部校验和的链路状态数据包

错误：

```
ciscoasa(config)# routerisis
```

```
ciscoasa(config-router)# ignore-lsp-errors
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isipassword	配置接口的认证密码。EXTEN
isipriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

ignore-ssl-keyusage (已弃用)

要禁止对 SSL 客户端证书进行密钥使用检查，请在 `ca-trustpoint` 配置模式下使用 **ignore-ssl-keyusage** 命令。要恢复密钥使用检查，请使用此命令的 **no** 形式。

ignore-ssl-keyusage
no ignore-ssl-keyusage

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
CA-trustpoint 配置	• 是	—	• 是	—	—

Command History 版本 修改

8.0(2) 此命令被添加为一项安全措施，但同时已被弃用。请注意，未来的版本可能不提供密钥用法检查抑制。

使用指南 使用此命令表示 IPsec 远程客户端证书的密钥用法和扩展密钥用法扩展中的值不被验证。此命令会忽略密钥使用检查，对于不合规的部署非常有用。

CR_Examples 以下示例显示如何忽略密钥使用检查的结果：

```
ciscoasa(config)#crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ssl-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
cryptoca	进入加密 ca 信任点配置模式。

ike-retry-count

如要配置使用 IKE 的思科 AnyConnect VPN 客户端在回退到 SSL 尝试连接之前应进行的最大连接重试尝试次数，请在 `group-policy webvpn` 配置模式或 `username webvpn` 配置模式下使用 **ike-retry-count** 命令。要从配置中删除此命令并将最大重试次数重置为默认值，请使用此命令的 **no** 形式。

```
ike-retry-count { none | value }
no ike-retry-count { none | value }
```

Syntax Description	none 指定不允许重试。
	value 指定思科 AnyConnect VPN 客户端在初始连接失败后要执行的最大连接重试次数（1-10 次）。

Command Default	允许重试的默认次数为 3 次。

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
组策略 webvpn 配置	• 是	—	• 是	—	—
用户名 webvpn 配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令

使用指南	使用 ike-retry-count 命令控制 Cisco AnyConnect VPN 客户端应尝试使用 IKE 进行连接的次数。如果客户端在达到此命令中指定的次数后仍使用 IKE 进行连接，则会回退到 SSL 来尝试连接。此值会覆盖 Cisco AnyConnect VPN 客户端中存在的任何值。



注释 为了支持从 IPsec 回退到 SSL，**vpn-tunnel-protocol** 命令必须同时配置 **svc** 和 **ipsec** 参数。

CR_Examples	以下示例将名为 FirstGroup 的组策略的 IKE 重试计数设置为 7：

```
ciscoasa
```



```
(config)# group-policy FirstGroup attributes
ciscoasa
(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)# ike-retry-count 7
ciscoasa
(config-group-webvpn)#
```

以下示例将用户名财务的 IKE 重试计数设置为 9:

```
ciscoasa
(config)#
username
Finance attributes
ciscoasa
(config-username)# webvpn
ciscoasa
(config-username-webvpn)# ike-retry-count 9
ciscoasa
(config-group-webvpn)#
```

Related Commands

命令	说明
group-policy	创建或编辑组策略。
ike-retry-timeout	指定 IKE 重试之间的秒数。
username	将用户添加到 ASA 数据库。
vpn-tunnel-protocol	配置 VPN 隧道类型（IPsec、L2TP over IPsec 或 WebVPN）。
webvpn	进入组策略 webvpn 配置模式或用户名 webvpn 配置模式。

ikev1 pre-shared-key

如要指定预共享密钥以支持基于预共享密钥的 IKEv1 连接，请在 tunnel-group ipsec-attributes 配置模式下使用 **pre-shared-key** 命令。要返回默认值，请使用此**no**命令形式。

pre-shared-key*key*
no pre-shared-key

Syntax Description *key* 指定介于 1 到 128 个字符之间的字母数字密钥。

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
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.4(1)	命令名称从 pre-shared-key 更改为 ikev1 pre-shared-key。

使用指南 您可以将此属性应用于所有 IPsec tunnel-group 类型。

CR_Examples 在 config-ipsec 配置模式下输入的以下命令指定预共享密钥 XYZX 以支持名为 209.165.200.225 的 IPSec LAN 间隧道组的 IKE 连接：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key xyzx
ciscoasa(config-tunnel-ipsec)#
```

命令	说明
clear-config tunnel-group	清除所有配置的隧道组。
showrunning-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。

命令	说明
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

ikev1 trust-point

要指定标识要发送给 IKEv1 对等方的证书的信任点的名称，请在 **trust-point** 隧道组 ipsec-attributes 模式下使用该命令。要消除信任点规范，请使用此命令 **no** 的形式。

trust-point *trust-point-name*
no trust-point *trust-point-name*

Syntax Description *trust-point-name* 指定要使用的信任点的名称。

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
隧道组 ipsec 属性	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 添加了此命令。

8.4(1) 命令名称已从 trust-point 更改为 ikev1 trust-point。

使用指南 您可以将此属性应用于所有 IPsec 隧道组类型。

CR_Examples 以下示例在 tunnel-ipsec 配置模式下配置一个信任点，用于识别要发送到名为 209.165.200.225 的 IPsec LAN 间隧道组的 IKEv1 对等体的证书：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 trust-point mytrustpoint
```

Related Commands

命令	说明
clear-config <i>tunnel-group</i>	清除所有配置的隧道组。
showrunning-config <i>tunnel-group</i>	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

ikev1 user-authentication

要在 IKE 期间配置混合身份验证，请在 `tunnel-group ipsec-attributes` 配置模式下使用 `ikev1user-authentication` 命令。要禁用混合身份验证，请使用此命令的形式。

```
ikev1user-authentication [ interface ] { none | xauth | hybrid }  
no ikev1user-authentication [ interface ] { none | xauth | hybrid }
```

Syntax Description

hybrid 指定 IKE 期间使用混合 XAUTH 身份验证。

interface （可选）指定在其上配置用户身份验证方法的接口。

none 在 IKE 期间禁用用户身份验证。

xauth 指定 XAUTH，也称为扩展用户身份验证。

Command Default

默认身份验证方法是 XAUTH 或扩展用户身份验证。默认值为所有接口。



注释 您必须保留 XAUTH 默认值，以避免中断任何已建立的 L2TP over IPsec 会话。如果 `tunnel-group` 设置为任何其他值（例如 `isakmp ikev1-user-authentication none`），则无法建立 L2TP over IPsec 会话。

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

7.2(1) 添加了此命令。

8.4(1) 命令名称从 `isakmp ikev1-user-authentication` 更改为 `ikev1user-authentication`。

使用指南

当您需要使用数字证书进行 ASA 身份验证并使用不同的传统方法进行远程 VPN 用户身份验证（例如 RADIUS、TACACS+ 或 SecurID）时，可以使用此命令。该命令将 IKE 的第 1 阶段分为以下两个步骤，统称为混合身份验证：

- 1. ASA 使用标准公钥方法对远程 VPN 用户进行身份验证。这将建立进行单向身份验证的 IKE 安全关联。
- 2. 然后，XAUTH 交换对远程 VPN 用户进行身份验证。此扩展身份验证可以使用其中一种受支持的传统身份验证方法。



注释 必须配置身份验证服务器，创建预共享密钥并配置信任点，然后才能将身份验证类型设置为混合。

交换类型为主模式时，IPsec 混合 RSA 身份验证类型会被拒绝。

当您省略可选接口参数时，该命令将应用于所有接口，并在未指定每个接口命令时充当备份。当为隧道组指定了两 **ikev1user-authentication** 个命令，其中一个使用接口参数而另一个不使用时，指定接口的命令优先于该特定接口。

CR_Examples

以下示例命令在名为 example-group 的隧道组的内部接口上启用混合 XAUTH:

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 user-authentication (inside) hybrid
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
aaa-server	定义 AAA 服务器。
pre-shared-key	创建用于支持 IKE 连接的预共享密钥。
tunnel-group	创建和管理 IPsec、L2TP/IPsec 和 WebVPN 连接的连接特定记录数据库。

ikev2 local-authentication

要为 IKEv2 LAN 间连接指定本地身份验证，请在 `tunnel-group ipsec-attributes` 配置模式下使用 `ikev2 local-authentication` 命令。要返回默认值，请使用此 `no` 命令形式。

ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** <*string*> | **certificate** **trustpoint** }
no ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** <*string*> | **certificate** **trustpoint** }

Syntax Description

certificate	指定证书身份验证。
hex	配置十六进制预共享密钥。
key_value	密钥值，长度为 1 到 128 个字符。
pre-shared-key	指定用于对远程对等体进行身份验证的本地预共享密钥。
string	输入一个介于 2 到 256 之间且字符数为偶数的十六进制预共享密钥。
信任点	指定用于标识要发送到远程对等方的证书的信任点。

Command Default

无默认为或值。

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
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History

版本 修改

8.4(1) 添加了此命令。

9.3(2) 添加了使用 EAP 的远程身份验证。

9.4(1) 添加了 hex 和 hex string 关键字。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

您只能为本地身份验证配置一个身份验证选项。

您必须先使用 **certificate** 选项配置此命令，然后才能使用 **ikev2remote-authentication** 命令启用 EAP 身份验证。

对于 IKEv2 连接，隧道组映射必须知道哪些身份验证方法允许远程身份验证（PSK、证书和 EAP）和本地身份验证（PSK 和证书），以及哪个信任点用于本地身份验证。

CR_Examples

以下命令指定预共享密钥 XYZX 以支持名为 209.165.200.225 的 IPsec LAN 间隧道组的 IKE 连接：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_121
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

以下命令将远程访问隧道组配置为使用其身份证书（与信任点 myIDcert 关联）向对等体验证 ASA。对等体还可以使用预先共享的密钥、证书或 EAP 进行身份验证。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_121
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key XYZX
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

命令	说明
clear-configretunnel-group	清除所有配置的隧道组。
showrunning-configtunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

ikev2 mobike-rrc

要在移动 IKE (mobike) 通信期间对 IPsec IKEv2 RA VPN 连接启用返回路由能力检查，请在 tunnel-group ipsec-attributes 配置模式下使用 **ikev2mobike-rrc** 命令。要禁用返回可路由性检查，请使用此命令的 **no** 形式。

ikev2 mobike-rrc
no ikev2 mobike-rrc

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

摩拜单车“永远在线”。此命令用于为 Mobike 连接启用 RRC。

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

9.8(1) 添加了此命令。

使用指南

此命令仅适用于 IPsec IKEv2 RA VPN 隧道组。

CR_Examples

以下示例命令对名为 example-group 的隧道组启用 mobike 的返回路由能力检查：

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 mobike-rrc
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
clear-configretunnel-group	清除所有配置的隧道组。
showrunning-configtunnel-group	显示所有隧道组或特定隧道组的隧道组配置。

命令	说明
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

ikev2 remote-authentication

要为 IPsec IKEv2 LAN 间连接指定远程身份验证，请在 `tunnel-group ipsec-attributes` 配置模式下使用 `ikev2remote-authentication` 命令。要返回默认值，请使用此 `no` 命令形式。

```
ikev2 remote-authentication { pre-shared-keykey_value | certificate | hex<string> | eap [ query-identity ] }
no ikev2 remote-authentication { pre-shared-keykey_value | certificate | hex<string> | eap [ query-identity ] }
```

Syntax Description

<code>certificate</code>	指定证书身份验证。
<code>eap</code>	指定可扩展身份验证协议 (EAP) 为支持对通用第三方 IKEv2 远程访问客户端（除 AnyConnect 外）进行用户身份验证的方法。
<code>hex</code>	配置十六进制预共享密钥。
<code>key_value</code>	密钥值，长度为 1 到 128 个字符。
<code>pre-shared-key</code>	指定用于对远程对等体进行身份验证的本地预共享密钥。
查询身份	向对等体请求 EAP 身份。
<code>string</code>	输入一个介于 2 到 256 之间且字符数为偶数的十六进制预共享密钥。

Command Default

无默认为或值。

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
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History

版本 修改

8.4(1) 添加了此命令。

9.3(2) 添加了 `eap` 和 `query-identity` 关键字。

9.4(1) 添加了 `hex` 和 `hex-string` 关键字。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

在启用 EAP 进行远程身份验证之前，您必须先使用 `key -value | certificatetrustpoint` 命令配置使用证书和有效信任点的`ikev2local-authenticationpre-shared-key`本地身份验证。否则，会发生错误并拒绝 EAP 身份验证请求。

您可以为远程身份验证配置多个身份验证选项。



注释 对于 IKEv2 连接，隧道组映射必须知道哪些身份验证方法允许远程身份验证（PSK、证书和 EAP）和本地身份验证（PSK 和证书），以及哪个信任点用于本地身份验证。当前，使用从对等体或对等体证书字段值（使用证书映射）获取的 IKE ID 执行映射。如果两个选项都失败，则传入连接将映射到默认远程访问隧道组。仅当远程对等体通过证书进行身份验证时，证书映射选项才适用。此映射允许映射到不同的隧道组。仅对证书身份验证使用规则或默认设置执行隧道组查找。对于 EAP 和 PSK 身份验证，使用客户端上的 IKE ID（与隧道组名称匹配）或使用默认设置执行隧道组查找。

CR_Examples

以下命令指定预共享密钥 XYZX，以支持名为 209.165.200.225 的 IPsec LAN 间隧道组的 IKEv2 连接：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key xyzx
```

以下命令显示 EAP 身份验证请求被拒绝：

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

命令	说明
<code>clear-configretunnel-group</code>	清除所有配置的隧道组。
<code>showrunning-configtunnel-group</code>	显示所有隧道组或特定隧道组的隧道组配置。
<code>tunnel-group ipsec-attributes</code>	为该组配置隧道组 IPsec 属性。

ikev2 rsa-sig-hash

要配置 IKEv2 RSA 签名散列，请在 tunnel-group ipsec-attributes 配置模式下使用 **ikev2rsa-sig-hash** 命令。要返回默认值，请使用此 **no** 命令形式。

ikev2rsa-sig-hashsha1
no ikev2rsa-sig-hashsha1

Syntax Description

sha1 使用 SHA-1 散列函数对 IKEv2 身份验证负载签名。

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
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History

版本 修改

9.12(1) 添加了此命令。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

CR_Examples

以下命令使用 SHA-1 函数对 IKEv2 身份验证负载签名：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 rsa-sig-hash sha
```

Related Commands

命令	说明
clear-config tunnel-group	清除所有配置的隧道组。
showrunning-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

im

要启用 SIP 即时消息，请在参数配置模式下使用 **im** 命令（此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。

im
noim

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
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

以下示例显示如何在 SIP 检查策略映射中启用通过 SIP 的即时消息传递：

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

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

imap4s (已弃用)



注释 此命令的最后支持版本是 9.5(1)。

要进入 IMAP4S 配置模式，请在全局配置模式下使用 **imap4s** 命令。要删除在 IMAP4S 命令模式下输入的任何命令，请使用此命令的 **no** 形式。

imap4s
no imap4s

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
全局配置	• 是	• 支持	—	—	• 是

Command History 版本 修改

7.0(1) 添加了此命令。

9.5(2) 此命令已弃用。

使用指南

IMAP4 是客户端/服务器协议，您的互联网服务器可以使用该协议接收和保留邮件。您（或您的邮件客户端）可以仅查看信函的标题和发件人，然后决定是否下载邮件。您还可以在服务器上创建和操作多个文件夹或邮箱，删除邮件，或搜索某些部分或整个便签。IMAP 要求在处理邮件期间持续访问服务器。IMAP4S 使您可以通过 SSL 连接接收邮件。

CR_Examples

以下示例显示如何进入 IMAP4S 配置模式：

```
ciscoasa
(config)#
imap4s
ciscoasa(config-imap4s)#
```

Related Commands

命令	说明
clearconfigureimap4s	删除 IMAP4S 配置。
showrunning-configimap4s	显示 IMAP4S 的运行配置。

imi-traffic-descriptor

要定义在具有 IP 选项检查的数据包头中出现 IMI 流量描述符 (IMITD) 选项时的操作，请在 **imi-traffic-descriptor** 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。

imi-traffic-descriptor action { **allow** | **clear** }
no imi-traffic-descriptor action { **allow** | **clear** }

Syntax Description

allow 允许包含 IMI 流量描述符 IP 选项的数据包。

clear 从数据包头中删除 IMI 流量描述符选项，然后允许数据包。

Command Default

默认情况下，IP 选项检查会丢弃包含 IMI 流量描述符 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，而无需更改或删除指定的 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)# imi-traffic-descriptor 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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

import

要在前缀委派客户端接口上将 ASA 从 DHCPv6 服务器获取的一个或多个参数提供给无状态地址自动配置 (SLAAC) 客户端，请在 ipv6 dhcp 池配置模式下使用 **import** 命令。要删除参数，请使用此命令的形式。

```
import { [dns-server] [domain-name] [nis-address] [nis-domain-name] [nip-address] [nip-domain-name] [sip-address] [sip-domain-name] [sntp-address] }  
no  
import { [dns-server] [domain-name] [nis-address] [nis-domain-name] [nip-address] [nip-domain-name] [sip-address] [sip-domain-name] [sntp-address] }
```

Syntax Description

dns-server	导入域名服务器 (DNS) 服务器的 IP 地址。
domain-name	导入域名。
nis-address	导入网络信息服务 (NIS) 服务器 IP 地址。
nisdomain-name	导入 NIS 域名。
nisp-address	导入 Network Information Service Plus (NIS+) 服务器 IP 地址。
nispdomain-name	导入 NIS+ 域名。
sip-address	导入 会话初始协议 (SIP) 服务器 IP 地址。
sipdomain-name	导入 SIP 域名。
sntp-address	导入简单网络时间协议 (SNTP) 服务器 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
Ipv6 dhcp 池配置	• 是	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以将 ASA 配置为在向 **ipv6dhcppool**ASA 发送信息请求 (IR) 数据包时提供信息，包括 DNS 服务器或域名。您可以混合搭配手动配置的参数与导

入的参数；但是手动配置的参数与使用 **import** 命令配置的参数不能相同。ASA 仅接受 IR 数据包，不向客户端分配地址。使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcp pool** 名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcp pool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。

命令	说明
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

import webvpn AnyConnect-customization

要将 AnyConnect 自定义对象加载到 ASA 的闪存设备，请在特权 EXEC 模式下输入 **importwebvpnAnyConnect-customization** 命令。

```
importwebvpnAnyConnect-customization type {binary | resource | transform} platform {linux | linux-64 | mac-intel | mac-powerpc | win | win-mobile} name URL [std {num_chars} data] quit }
```

Syntax Description	name	标识自定义对象的名称。最大数量为 64 个字符。
	platform {linux linux-64 mac-intel mac-powerpc win win-mobile}	对象应用到的客户端平台。
	stdin {num_charsdata dataquit}	指定将从标准输入提供数据。如果未指定字符数，则从标准输入读取的数据应进行 base64 编码，后跟 “\nquit\n”。
	type {binary resource transform}	正在导入的自定义对象的类型。
	URL	XML 自定义对象源的远程路径。最大数量为 255 个字符。

Command Default 无默认为或值。

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	—	• 是	—	—

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。

使用指南 在输入 **importcustomization** 命令之前，请确保在 ASA 接口上启用了 WebVPN。为此，请输入命令 **showrunning-config**

ASA 会将自定义对象从 URL 或 标准输入复制到 ASA 文件系统 disk0:/cisco_config/customization。AnyConnect 自定义可能包括自定义 AnyConnect GUI 资源、二进制自定义帮助文件、二进制 VPN 脚本以及安装程序转换。

Related Commands

命令	说明
revertwebvpnAnyConnect-customization	从 ASA 的闪存设备删除指定的自定义对象。
showimportwebvpnAnyConnect-customization	列出 ASA 的闪存设备上存在的自定义对象。

import webvpn customization

要将自定义对象加载到 ASA 的闪存设备，请在特权 EXEC 模式下输入 `importwebvpncustomization` 命令。

`import webvpn customization` 名称URL

Syntax Description	<i>name</i> 标识自定义对象的名称。最大数量为 64 个字符。
	URL XML 自定义对象源的远程路径。最大数量为 255 个字符。

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	—	• 是	—	—

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。

使用指南 在输入 `importcustomization` 命令之前，请确保在 ASA 接口上启用了 WebVPN。为此，请输入命令。
`showrunning-config`

导入自定义对象时，ASA 会执行以下操作：

- 将自定义对象作为 MD5名称从 URL 复制到 ASA 文件系统 `disk0:/cisco_config/customization`。
- 对文件执行基本 XML 语法检查。如果无效，ASA 将删除该文件。
- 检查 `index.ini` 中的文件是否包含记录 MD5名称。否则，ASA 将向文件添加 MD5名称。
- 将 MD5名称 文件复制到 `RAMFS /cisco_config/customization/`，其 名称为。

CR_Examples 以下示例从 URL `209.165.201.22/customization` 将自定义对象 `General.xml`导入到 ASA，并将其命名为 `custom1`。

```
ciscoasa# import webvpn customization custom1 tftp://209.165.201.22/customization /General.xml
```



```
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/cisco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

命令	说明
revertwebvpncustomization	从ASA的闪存设备删除指定的自定义对象。
showimportwebvpncustomization	列出ASA的闪存设备上存在的自定义对象。

import webvpn mst-translation

要将 MST (Microsoft 转换) 对象加载到 ASA 的闪存设备上，请在特权 EXEC 模式下输入 **importwebvpnmst-translation** 命令。

import webvpn mst-translation AnyConnect language语言**URL** | **stdin** { num_chars 数据 | 数据quit }

Syntax Description

languagelanguage

翻译语言。

stdin { num_charsdata|dataquit } 指定将从标准输入提供数据。如果未指定字符数，则从标准输入读取的数据应进行 base64 编码，后跟 “\nquit\n”。

URL

XML 自定义对象源的远程路径。最大数量为 255 个字符。

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	—	• 是	—	—

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。

使用指南

此文件可以转换 AnyConnect 安装程序。

Related Commands

命令	说明
showimportwebvpnmst-translation	列出 ASA 的闪存设备上存在的自定义对象。

import webvpn plug-in protocol

要将插件安装到 ASA 的闪存设备上，请在特权 EXEC 模式下输入 **importwebvpnplug-inprotocol** 命令。

import webvpn plug-in protocol*protocolURL*

Syntax Description

- protocol*
- **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。思科重新分发此插件，无需任何更改。包含原始文件的网站为 <http://properjavardp.sourceforge.net/>。
 - **ssh,telnet**—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。思科重新分发此插件，无需任何更改。包含原始文件的网站为 <http://javassh.org/>。

注意

importwebvpnplug-inprotocolssh,telnetURL 命令会安装 SSH 和 Telnet 插件。不要对 SSH 输入一次该命令，对 Telnet 输入一次该命令。键入字符 **ssh,telnet** 串时，不要插入空格。使用 **revertwebvpnplug-inprotocol** 命令删除不符合这些要求的任何 **importwebvpnplug-inprotocol** 命令。

- **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。思科重新分发此插件，无需任何更改。包含原始文件的网站为 <http://www.tightvnc.com/>。

URL 插件源的远程路径。

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
特权执行模式	• 是	—	• 是	—	—

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。

使用指南

在安装插件之前，请执行以下操作：

- 确保在 ASA 上的接口上启用了无客户端 SSL VPN（“webvpn”）。为此，请输入命令。
showrunning-config
- 在本地 TFTP 服务器（例如，使用主机名“local_tftp_server”）上创建名为“插件”的临时目录，然后从思科网站将插件下载到“插件”目录。在命令的 URL 字段中输入 TFTP 服务器的主机名或地址以及所需插件的 **importwebvpnplug-inprotocol** 路径。

在导入插件时，ASA 执行以下操作：

- 解压缩 URL 中指定的 .jar 文件。
- 将文件写入 ASA 文件系统中的 cisco-config/97/plugin 目录。
- 填充 ASDM 中 URL 属性旁边的下拉菜单。
- 为所有未来的无客户端 SSL VPN 会话启用插件，并在门户页面的地址字段旁边的下拉菜单中添加一个选项。下表显示了门户页面主菜单和地址栏的更改。

插件	添加到门户页面的主菜单选项	添加到门户页面的 Address 字段选项
citrix	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

ASA 不会在配置中 **importwebvpnplug-inprotocol** 保留该命令。相反，它会自动加载 cisco-config/97/plugin 目录的内容。辅助 ASA 会从主 ASA 获取插件。

当无客户端 SSL VPN 会话中的用户在门户页面上点击关联的菜单选项时，门户页面会在界面上显示一个窗口，并显示一个帮助窗格。用户可以选择下拉菜单中显示的协议，并在地址字段中输入 URL 来建立连接。



注释 除了以前的 SSH V1 和 Telnet，还添加了对 SSH V2 的支持。插件协议仍然相同（ssh 和 telnet），URL 格式如下：ssh://<target> — 使用 SSH V2ssh://<target>/?version=1 — 使用 SSH V1telnet://<target> — 使用 telnet

要删除相应的 **importwebvpnplug-inprotocol** 命令并禁用协议支持，请使用 **revertwebvpnplug-inprotocol** 命令。

CR_Examples

以下命令为 RDP 添加无客户端 SSL VPN 支持：

```
ciscoasa# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
```

```
Accessing
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/cisco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

以下命令为 SSH 和 Telnet 添加无客户端 SSL VPN 支持:

```
ciscoasa# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar
Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/cisco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

以下命令为 VNC 添加无客户端 SSL VPN 支持:

```
ciscoasa# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar
Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/cisco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

Related Commands

命令	说明
revertwebvpnplug-inprotocol	从 ASA 的闪存设备中删除指定的插件。
showimportwebvpnplug-in	列出 ASA 闪存设备上的插件。

import webvpn translation-table

要导入用于转换向建立 SSL VPN 连接的远程用户显示的术语的转换表，请在特权 EXEC 模式下使用 **importwebvpntranslation-table** 命令。

import webvpn translation-table*translation_domainlanguagelanguageurl*

Syntax Description

language	指定转换表的语言。按照浏览器语言选项表示的方式输入 <i>Language</i> 值。
translation_domain	指定功能区域和对远程用户可见的关联消息。
url	指定用于创建自定义对象的 XML 文件的 URL。

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	—	• 是	—	—

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。

使用指南

ASA 为向启动基于浏览器的无客户端 SSL VPN 连接的用户显示的门户和屏幕以及向 AnyConnect VPN 客户端用户显示的用户界面提供语言翻译。

远程用户可见的每个功能区域及其消息都有自己的转换域，并由 *translation_domain* 参数指定。下表显示了转换域和转换的功能区域。

转换域	转换的功能区域
AnyConnect	CiscoAnyConnectVPN 客户端用户界面上显示的消息。
banners	当 VPN 访问被拒绝时，向远程用户和消息显示的横幅。
CSD	思科安全桌面 (CSD) 的消息。
customization	登录和注销页面 门户 页面上的消息以及所有用户可自定义的消息。

转换域	转换的功能区域
plugin-ica	Citrix 插件的消息。
plugin-rdp	远程桌面协议插件的消息。
plugin-telnet,ssh	Telnet 和 SSH 插件的消息。
plugin-vnc	VNC 插件的消息。
PortForwarder	显示给端口转发用户的消息。
url-list	用户为门户页面上的 URL 书签指定的文本。
webvpn	所有不可定制的第 7 层、AAA 和门户消息。

转换模板是与转换表格式相同的 XML 文件，但所有转换为空。ASA 的软件映像包包含每个域的模板，该模板是标准功能的一部分。插件模板包含在插件中并定义其自己的翻译域。因为您可以动态地定制无客户端用户的登录 注销页面、门户页面和 URL 书签、ASA 生成定制化和翻 url-list 译域模板，并且模板会自动反映您对这些功能区域的更改。

使用 **exportwebvpntranslation-table** 命令下载转换域的模板，对消息进行更改，然后使用 **importwebvpntranslation-table** 命令创建对象。您可以使用 **showimportwebvpntranslation-table** 命令查看可用对象。

请务必以浏览器语言选项表示的方式指定语言。例如，Microsoft Internet Explorer 使用缩写词 ((zh)) 来表示中文。导入到 ASA 的转换表也必须命名为 "zh"。

除 AnyConnect 转换域外，转换表没有任何影响，并且只有在您创建自定义对象、确定要在该对象中使用的转换表并为组策略或用户指定自定义时，才会转换消息。AnyConnect 域的转换表的更改对用户来说是立即可 Secure Client 见的。请参阅命令 **importwebvpncustomization** 以了解更多信息。

CR_Examples

以下示例为影响 Secure Client 用户界面的转换域导入转换表，并指定该转换表适用于中文。
showimportwebvpntranslation-table 命令显示新对象：

```
ciscoasa# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
Translation Tables:
zh AnyConnect
```

Related Commands

命令	说明
export webvpn translation-table	导出翻译表。
import webvpn customization	导入引用转换表的自定义对象。
revert	从闪存中删除转换表。
showimportwebvpntranslation-table	显示可用的转换表模板和转换表。

import webvpn url-list

要将 URL 列表加载到 ASA 的闪存设备，请在特权 EXEC 模式下输入 **importwebvpnurl-list** 命令。

import webvpn url-list 名称 URL

Syntax Description

name 标识 URL 列表的名称。最大数量为 64 个字符。

URL URL 列表源的远程路径。最大数量为 255 个字符。

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。

9.0(1) 增加了多情景模式支持。

使用指南

在输入 **importurl-list** 命令之前，请确保在 ASA 接口上启用了 WebVPN。为此，请输入命令。
showrunning-config

导入 URL 列表时，ASA 会执行以下操作：

- 将 URL 列表从 URL 复制到 ASA 文件系统 disk0:/cisco_config/url-lists as *nameonflash=base 64name*。
- 对文件执行基本 XML 语法检查。如果语法无效，ASA 将删除该文件。
- 检查 index.ini 中的文件是否包含 base 64名称记录。否则，ASA 将向文件中添加 base-64名称。
- 将 名称 文件复制到 RAMFS /cisco_config/url-lists/，其中 ramfs name = *name*。

CR_Examples

以下示例将 URL 列表 *NewList.xml* 从 URL 209.165.201.22/url-lists 导入到 ASA 并将其命名为 *ABCList*。

```
ciscoasa# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Writing file disk0:/cisco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands	命令	说明
	revertwebvpnurl-list	从 ASA 的闪存设备中删除指定的 URL 列表。
	showimportwebvpnurl-list	列出 ASA 的闪存设备上存在的 URL 列表。

import webvpn webcontent

要将内容导入到闪存以向远程无客户端 SSL VPN 用户显示，请在特权 EXEC 模式下使用 **importwebvpnwebcontent** 命令。

目标**import webvpn webcontent**网址源网址

Syntax Description

destinationurl **TheURLtoexportto**. 最大数量为 255 个字符。

sourceurl 内容所在的 ASA 闪存中的 URL。最大数量为 64 个字符。

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	—	• 是	—	—

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。

使用指南

使用 **webcontent** 选项导入的内容对远程无客户端用户可见。这包括在无客户端门户上显示的帮助内容，以及定制用户屏幕的定制对象所使用的徽标。

导入到 URL 路径为 `/+CSCOE+/` 的内容仅对授权用户可见。

导入到 URL 中路径为 `/+CSCOU+/` 的内容对未经授权和已授权的用户均可见。

例如，作为 `/+CSCOU+/logo.gif` 导入的公司徽标可用于门户自定义对象中，并显示在登录页面和门户页面上。只有远程用户成功登录后，才能看到与 `/+CSCOE+/logo.gif` 导入的相同 `logo.gif` 文件。

在各种应用屏幕上显示的帮助内容必须导入至特定 URL。下表显示了为标准无客户端应用显示的帮助内容的 URL 和屏幕区域：

URL	无客户端屏幕区域
<code>/+CSCOE+/help/language /app-access-hlp.inc</code>	Application Access
<code>/+CSCOE+/help/language /file-access-hlp.inc</code>	Browse Networks

URL	无客户端屏幕区域
/+CSCO+/help/language/net_access_hlp.html	Secure Client
/+CSCO+/help/language/web-access-help.inc	Web Access

下表显示了向可选插件无客户端应用显示的帮助内容的 URL 和屏幕区域：

URL	无客户端屏幕区域
/+CSCO+/help/language/ica-hlp.inc	MetaFrame Access
/+CSCO+/help/language/rdp-hlp.inc	Terminal Servers
/+CSCO+/help/language/ssh,telnet-hlp.inc	Telnet/SSH Servers
/+CSCO+/help/language/vnc-hlp.inc	VNC Connections

URL 路径中的 语言 条目是您为帮助内容指定的语言缩写。ASA 实际上不会将文件转换为您指定的语言，但会使用语言缩写标记文件。

CR_Examples

以下示例将 HTML 文件 *application_access_help.html* 从位于 209.165.200.225 的 TFTP 服务器导入到将应用访问帮助内容存储在闪存中的 URL。URL 包含英语语言的缩写 *en*：

```
ciscoasa# import webvpn webcontent /+CSCO+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource '+CSCO+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

以下示例将 HTML 文件 *application_access_help.html* 从位于 209.165.200.225 的 tftp 服务器导入到将应用访问帮助内容存储在闪存中的 URL。URL 包含英语语言的缩写 *en*：

```
ciscoasa# import webvpn webcontent /+CSCO+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource '+CSCO+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

Related Commands

命令	说明
导出 webvpn webcontent	导出之前导入的无客户端 SSL VPN 用户可见的内容。
revert webvpn webcontent	从闪存中删除内容。
showimportwebvpnwebcontent	显示有关导入的内容的信息。



inspect a – inspect z

- inspect ctiqbe, 第 75 页
- inspect dcerpc, 第 77 页
- inspect diameter, 第 79 页
- inspect dns, 第 81 页
- inspect esmtp, 第 83 页
- inspect ftp, 第 86 页
- inspect gtp, 第 89 页
- inspect h323, 第 92 页
- inspect http, 第 94 页
- inspect icmp, 第 96 页
- inspect icmp error, 第 98 页
- inspect ils, 第 100 页
- inspect im, 第 103 页
- inspect ip-options, 第 105 页
- inspect ipsec-pass-thru, 第 108 页
- inspect ipv6, 第 110 页
- inspect lisp, 第 112 页
- inspect m3ua, 第 114 页
- inspect mgcp, 第 116 页
- inspect mmp, 第 119 页
- inspect netbios, 第 121 页
- inspect pptp, 第 122 页
- inspect radius-accounting, 第 124 页
- inspect rsh, 第 126 页
- inspect rtsp, 第 128 页
- inspect scansafe, 第 130 页
- 检查 SCTP, 第 133 页
- inspect sip, 第 135 页
- inspect skinny, 第 138 页

- [inspect snmp](#)，第 141 页
- [inspect sqlnet](#)，第 143 页
- [inspect stun](#)，第 145 页
- [inspect sunrpc](#)，第 147 页
- [inspect tftp](#)，第 149 页
- [inspect vxlan](#)，第 151 页
- [inspect waas](#)，第 153 页
- [inspect xdmcp](#)，第 154 页

inspect ctiqbe

要启用 CTIQBE 协议检测，请在类配置模式下使用 **inspectctiqbe** 命令。可以从 map configuration 模式访问 Class configuration 模式。要禁用检查，请使用此命令 **no** 的形式。

inspect ctiqbe
no inspect ctiqbe

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 我们添加了此命令，它取代了之前已弃用的 **fixup** 命令。

使用指南

该 **inspectctiqbe** 命令启用 CTIQBE 协议检查，支持 NAT、PAT 和双向 NAT。这使得 Cisco IP SoftPhone 和其他 Cisco TAPI/JTAPI 应用程序能够与 Cisco CallManager 成功协作，以便在 ASA 上设置呼叫。

许多思科 VoIP 应用都使用电话应用程序编程接口 (TAPI) 和 Java 电话应用程序编程接口 (JTAPI)。计算机电话接口快速缓冲编码 (CTIQBE) 由 Cisco TAPI 服务提供程序 (TSP) 用于与思科 CallManager 通信。

下面总结了使用 CTIQBE 应用检测时适用的限制：

- 不支持 CTIQBE 呼叫状态故障转移。
- 使用 **debugctiqbe** 命令可能会延迟消息传输，这可能会对实时环境中的性能造成影响。在启用此调试或日志记录功能且 Cisco IP SoftPhone 似乎无法通过 ASA 完成呼叫建立时，请在运行 Cisco IP SoftPhone 的系统上增加超时值。
- CTIQBE 应用检测不支持在多个 TCP 数据包中分段的 CTIQBE 消息。

下面总结了在特定情况下使用 CTIQBE 应用检测时的特殊注意事项：

- 如果两个 Cisco IP SoftPhone 注册到不同的 Cisco CallManager，并且连接到 ASA 的不同接口，则这两个电话之间的通话将会失败。

- 当 Cisco CallManager 位于比 Cisco IP SoftPhones 安全性更高的接口上时，如果 Cisco CallManager IP 地址需要 NAT 或外部 NAT，则映射必须是静态的，因为 Cisco IP SoftPhone 要求在 PC 上的 Cisco TSP 配置中明确指定 Cisco CallManager IP 地址。
- 使用 PAT 或外部 PAT 时，如果要转换 Cisco CallManager IP 地址，则必须将其 TCP 端口 2748 静态映射到 PAT（接口）地址的相同端口，以使 Cisco IP SoftPhone 注册成功。CTIQBE 监听端口 (TCP 2748) 是固定的，用户无法在 Cisco CallManager、Cisco IP SoftPhone 或 Cisco TSP 上配置。

检查信令消息

要检查信令消息，**inspectctiqbe**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，**inspectctiqbe**命令不使用隧道默认网关路由。隧道默认网关路由是采用 **route** 接口 **00** 指标 **tunneled** 形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要 **inspectctiqbe** 命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 CTIQBE 检测引擎，该引擎创建类映射来匹配默认端口（2748）上的 CTIQBE 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map ctiqbe-port
ciscoasa(config-cmap)# match port tcp eq 2748
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ctiqbe_policy

ciscoasa(config-pmap)# class ctiqbe-port
ciscoasa(config-pmap-c)# inspect ctiqbe
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ctiqbe_policy interface outside
```

要对所有接口启用 CTIQBE 检测，请使用 **global** 参数代替 **interfaceoutside**。

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
showconn	显示不同连接类型的连接状态。
showctiqbe	显示有关跨 ASA 建立的 CTIQBE 会话和由 CTIQBE 检测引擎分配的媒体连接的信息。
timeout	为不同协议和会话类型设置最大空闲持续时间。

inspect dcerpc

要启用对流向终端映射器的 DCERPC 流量的检测，请在类配置模式下使用 `inspect dcerpc` 命令。可以从 `map configuration` 模式访问 `Class configuration` 模式。要删除配置，请使用此命令 **no** 的形式。

inspect dcerpc [*map_name*]
no inspect dcerpc [*map_name*]

Syntax Description

map_name （可选）DCERPC 检测映射的名称。

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
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

该 **inspect dcerpc** 命令启用或禁用 DCERPC 协议的应用程序检查。

CR_Examples

以下示例显示如何使用为 DCERPC 针孔配置的超时定义 DCERPC 检测策略映射。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
ciscoasa(config)# class-map dcerpc
ciscoasa(config-cmap)# match port tcp eq 135
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class dcerpc
ciscoasa(config-pmap-c)# inspect dcerpc dcerpc_map
ciscoasa(config)# service-policy global-policy global
```

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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	创建检查策略映射。
show running-config policy-map	显示所有当前的策略映射配置。
timeout pinhole	配置 DCERPC 针孔的超时并覆盖全局系统针孔超时。

inspect diameter

要启用 Diameter 应用程序检查，请在类配置模式下使用 **inspect diameter** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect diameter [diameter_map] [tls-proxyproxy_name]
no inspect diameter [diameter_map] [tls-proxyproxy_name]
```



注释 Diameter 检测需要运营商许可证。

Syntax Description

diameter_map 指定 Diameter 策略映射名称。

tls-proxyproxy_name 使用指定的 TLS 代理，以便检查加密连接。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.5(2) 添加了此命令。

9.6(1) 添加了 **tls-proxy** 关键字。

使用指南

Diameter 是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。

Diameter 使用 TCP 和 SCTP 作为传输层，并使用 TCP/TLS 和 SCTP/DTLS 保障通信安全。另外，它也可以选择性地提供数据对象加密。有关 Diameter 的详细信息，请参阅 RFC 6733。

Diameter 应用执行服务管理任务，例如决定用户权限、服务授权、服务质量和收费率。虽然 Diameter 应用可出现在 LTE 架构的许多不同控制面板接口上，但 ASA 仅检测以下接口的 Diameter 命令编码和属性-值对 (AVP)：

- S6a：移动管理实体 (MME) - 家庭订用服务(HSS)。

- S9: PDN 网关 (PDG) - 3GPP AAA 代理/服务器。
- Rx: 策略收费规则功能 (PCRF) - 呼叫会话控制功能 (CSCF)。

Diameter 检测为 Diameter 终端打开针孔，以允许通信。该检测支持 3GPP 版本 12，并符合 RFC 6733 要求。您可以将其用于 TCP/TLS（通过在启用检测时指定 TLS 代理），但不能将其用于 SCTP。使用 Ipsec 可保障 SCTP Diameter 会话的安全。

您可以选择性地使用 Diameter 检测策略映射根据应用 ID、命令代码和 AVP 来过滤流量，以便应用特殊操作，例如丢弃数据包或连接或记录它们。可以为新注册的 Diameter 应用创建自定义 AVP。通过过滤，您可以微调网络上允许的流量。



注释 默认情况下，允许其他接口上运行的应用的 Diameter 消息通过。虽然无法基于这些不支持应用的命令代码或 AVP 指定操作，但您可以配置 Diameter 检测策略映射，根据应用 ID 丢弃这些应用。

CR_Examples

以下示例在默认端口（TCP/3868、TCP/5868 和 SCTP/3868）上全局应用 Diameter 检测。

```
ciscoasa(config)# policy-map global_policy

ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect diameter
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
inspect sctp	启用 SCTP 检查。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
show service-policy inspect diameter	显示检查策略的状态和统计信息。
tls-proxy	定义 TLS 代理。

inspect dns

要启用 DNS 检测（如果以前已禁用）或配置 DNS 检测参数，请在类配置模式下使用 **inspectdns** 命令。可以从 map configuration 模式访问 Class configuration 模式。要禁用 DNS 检查，请使用此命令的形式。

inspect dns [*map_name*] [**dynamic-filter-snoop**]
no inspect dns [*map_name*] [**dynamic-filter-snoop**]

Syntax Description

dynamic-filter-snoop （可选）启用动态过滤器侦听，仅由僵尸网络流量过滤器使用。应仅在使用僵尸网络流量过滤时包含此关键字。我们建议仅在外部 DNS 请求经过的接口上启用 DNS 监听。在所有 UDP DNS 流量（包括流向内部 DNS 服务器的流量）上启用 DNS 监听会为 ASA 形成不必要的负载。

map_name （可选）指定 DNS 映射的名称。

Command Default

默认情况下会启用此命令。默认情况下会禁用僵尸网络流量过滤器侦听。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

7.2(1) 此命令已修改为允许配置其他 DNS 检查参数。

8.2(1) 添加了 **dynamic-filter-snoop** 关键字。

使用指南

默认情况下，启用 DNS 检测，使用 preset_dns_map 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 最大客户端 DNS 消息长度是自动设置的，以与资源记录匹配。
- DNS Guard 已启用，因此 ASA 在转发 DNS 应答后立即终止与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- 根据 NAT 配置的 DNS 记录转换已启用。

- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

DNS 重写需要 DNS 检测

当启用 DNS 检测时，DNS 重写将为源自任何接口的 DNS 消息的 NAT 提供全面支持。

如果内部网络上的客户端请求从外部接口上的 DNS 服务器对内部地址进行 DNS 解析，则正确转换 DNS A 记录。如果禁用 DNS 检测引擎，则不转换 A 记录。

DNS 重写执行两个功能：

- 当 DNS 客户端位于专用接口上时，将 DNS 应答 中的公共地址（可路由或“映射”地址）转换为专用地址（“实际”地址）。
- 当 DNS 客户端位于公用接口上时，将专用地址转换为公用地址。

只要 DNS 检测保持启用状态，您就可以为 NAT 配置 DNS 重写。

CR_Examples

以下示例显示如何设置最大 DNS 消息长度：

```
ciscoasa(config)# policy-map type inspect dns dns-inspect
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 1024
```

以下示例为所有 UDP DNS 流量创建类映射，使用默认 DNS 检测策略映射启用 DNS 检测和僵尸网络流量过滤器监听，并将其应用于外部接口：

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
dynamic-filterenable	为一个流量类或为所有流量（如果不指定访问列表）启用僵尸网络流量过滤器。
policy-map	将类映射与特定的安全操作相关联。
policy-maptypeinspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

inspect esmtp

要启用 SMTP/ESMTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspectesmtplib** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no** 的形式。

inspect esmtp [*map_name*]
no inspect esmtp [*map_name*]

Syntax Description

map_name （可选）ESMTP 映射的名称。

Command Default

默认情况下会启用此命令。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

默认情况下，ESMTP 检测已启用，其中会使用 `_default_esmtp_map` 检测策略映射。

- 会掩蔽服务器横幅。
- 检查加密流量。
- 不会查找发件人和收件人地址中的特殊字符，不会执行任何操作。
- 会丢弃并记录命令行长度大于 512 的连接。
- 会丢弃并记录有多于 100 个收件人的连接。
- 会记录正文长度超过 998 字节的消息。
- 会丢弃并记录报头行长度大于 998 的连接。
- 会丢弃并记录 MIME 文件名超过 255 个字符的消息。
- 会掩蔽匹配 “others” 的 EHLO 应答参数。

ESMTP 应用程序检查通过限制可通过 ASA 的 SMTP 命令类型并添加监控功能，提供了针对基于 SMTP 的攻击的改进防护。

ESMTP 是增强型 SMTP 协议，在大多数方面和 SMTP 类似。为方便起见，本文档中用 SMTP 来同时指代 SMTP 和 ESMTP。扩展 SMTP 的应用检测流程类似于 SMTP 应用检测，这项检测支持 SMTP 会话。扩展 SMTP 会话中使用的大多数命令与 SMTP 会话中使用的命令相同，但 ESMTP 会话的速度快很多，而且提供了更多与可靠性和安全性相关的选项，例如，传送状态通知。

扩展 SMTP 应用检测增加了对如下扩展 SMTP 命令的支持：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOHL、STARTTLS 和 VRFY。除了支持七个 RFC 821 命令（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）之外，ASA 还支持总共十五个 SMTP 命令。

不支持其他扩展 SMTP 命令（例如 ATRN、ONEX、VERB、CHUNKING）和专用扩展。不受支持的命令将被转换为 X（内部服务器会拒绝这些命令）。这将会生成消息，例如 “500 Command unknown: 'XXX'”。不完整的命令将被丢弃。

ESMTP 检测引擎将服务器 SMTP 横幅中的字符更改为星号，但对 “2”、“0”、“0” 字符除外。会忽略回车符 (CR) 和换行符 (LF)。

在 SMTP 检测启用的情况下，如果不遵守以下规则，用于交互式 SMTP 的 Telnet 会话可能会挂起：SMTP 命令长度必须至少为四个字符；必须以回车符和换行符终止；且必须在获得响应后才能发出下一个应答。

SMTP 服务器使用数字应答代码和（可选）人可读字符串来响应客户端请求。SMTP 应用检测控制和减少用户可使用的命令以及服务器返回的消息。SMTP 检测主要执行以下三项任务：

- 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。
- 监控 SMTP 命令-响应序列。
- 生成审核线索 - 邮件地址中嵌入的无效字符被替换时，会生成审核记录 108002。有关详细信息，请参阅 RFC 821。

SMTP 检测监控以下异常签名的命令-响应序列：

- 截断的命令。
- 命令终止错误（不是以 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。会扫描邮件地址以检测异常字符。竖线 (|) 将被删除（更改为空格）；“<”和“>”只能用于定义邮件地址（“>”前面必须有“<”）。
- SMTP 服务器执行的意外转换。
- 对于未知命令，ASA 会将数据包中的所有字符更改为 X。在这种情况下，服务器会向客户端生成错误代码。由于数据包发生了变化，因此必须重新计算或调整 TCP 校验和。
- TCP 数据流编辑。
- 命令管道。

CR_Examples

以下示例启用 SMTP 检测引擎，从而创建类映射来匹配默认端口（25）上的 SMTP 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map smtp-port
```



```
ciscoasa(config-cmap)# match port tcp eq 25
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map smtp_policy

ciscoasa(config-pmap)# class smtp-port
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy smtp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
show conn	显示不同连接类型的连接状态，包括 SMTP。

inspect ftp

要为 FTP 检测配置端口或启用增强检测，请在类配置模式下使用 **inspectftp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect ftp [strict [ map_name ] ]
no inspect ftp [strict [ map_name ] ]
```

Syntax Description	map_name	FTP 检测映射的名称。
	strict	(可选) 启用 FTP 流量的增强型检测，并强制遵守 RFC 标准。

Command Default	默认情况下启用 FTP 检测，并且 ASA 会侦听 FTP 的端口 21。 将 FTP 移至更高的端口时请谨慎。例如，如果将 FTP 端口设置为 2021，则向端口 2021 发起的所有连接都将其数据负载解释为 FTP 命令。

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
	类配置	• 是	• 支持	• 支持	• 支持
					—

Command History	版本 修改
	7.0(1) 添加了此命令。它取代了已弃用的 fixup 命令。添加了 <i>map_name</i> 选项。

使用指南	FTP 应用检测用于检测 FTP 会话和执行四种任务： • 准备动态辅助数据连接 • 跟踪 FTP 命令-响应序列 • 生成审核线索 • 转换嵌入式 IP 地址

FTP 应用检测为 FTP 数据传输准备辅助信道。这些信道的端口是通过 PORT 或 PASV 命令协商的。这些信道根据文件上传、文件下载或目录列表事件进行分配。



注释 仅对 FTP 控制连接的端口而非数据连接的端口应用检测。ASA 状态检测引擎会根据需要动态准备数据连接。

如果使用该 **noinspectftp** 命令禁用 FTP 检查引擎，则出站用户只能以被动模式启动连接，并且所有入站 FTP 都将被禁用。

严格 FTP

严格 FTP 可防止 Web 浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全性。要启用严格 FTP，请在命令中包含严格选 **inspectftp** 项。

在使用严格 FTP 时，您可以选择指定 FTP 检测策略映射来指定不允许通过 ASA 的 FTP 命令。

在接口上启用该 **strict** 选项后，FTP 检查将强制执行以下行为：

- 必须先确认 FTP 命令，然后 ASA 才允许使用新命令。
- ASA 丢弃发送嵌入式命令的连接。
- 检查 227 命令和 PORT 命令，以确保这些命令不显示在错误字符串中。



注意 使用该 **strict** 选项可能会导致不严格遵守 FTP RFC 的 FTP 客户端失败。

如果启用该 **strict** 选项，则会跟踪每个 FTP 命令和响应序列是否存在以下异常活动：

- 截断命令 - 检查 PORT 和 PASV 应答命令中逗号的数量是否是五个。如果不是五个，将会截断 PORT 命令并关闭 TCP 连接。
- 错误命令 - 检查 FTP 命令以确定它是否以 <CR><LF> 字符结尾（如 RFC 所要求）。如果不是，将会关闭连接。
- RETR 和 STOR 命令的大小 - 根据某个固定常数检查这些命令的大小。如果命令大小大于该固定常数，将会记录错误消息并关闭连接。
- 命令欺骗 - PORT 命令应始终从客户端发送。如果 PORT 命令是从服务器发送，将会拒绝 TCP 连接。
- 应答欺骗 - PASV 应答命令 (227) 应始终从服务器发送。如果 PASV 应答命令是从客户端发送，将会拒绝 TCP 连接。这样可防止用户执行 “227 xxxxx a1, a2, a3, a4, p1, p2.” 时出现安全漏洞
- TCP 流编辑 - 如果检测到 TCP 流编辑，ASA 将关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于 1 至 1024 范围内的端口号是为已知连接保留的，因此，如果协商的端口在这个范围内，将会释放 TCP 连接。
- 命令管道 - 将 PORT 和 PASV 应答命令中在端口号后显示的字符数与常数值 8 进行比较。如果该字符数大于 8，将会关闭 TCP 连接。

- ASA 将 FTP 服务器对 SYST 命令的响应替换为一系列 X，以防止服务器向 FTP 客户端泄露其系统类型。要覆盖此默认行为，请使用 FTP **nomask-syst-reply** 映射中的命令。

FTP 日志消息

FTP 应用检测生成以下日志消息：

- 为检索或上传的每个文件生成审核记录 302002。
- 如果辅助动态信道准备因内存不足而失败，将会生成审核记录 201005。

CR_Examples

提交用户名和密码之前，所有 FTP 用户均可以看到问候横幅。默认情况下，该横幅包含对于试图发现系统缺陷的黑客来说很有用的版本信息。以下示例显示如何掩蔽该横幅：

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
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。
policy-map type inspect	创建检查策略映射。
request-command deny	指定要禁止的 FTP 命令。
service-policy	将策略映射应用到一个或多个接口。

inspect gtp

要启用 GTP 检查，请在 **inspectgtp** 类配置模式下使用该命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命令 **no** 的形式可以禁用 GTP 检查。

```
inspect gtp [map_name]
no inspect gtp [map_name]
```



注释 GTP 检查需要 GTP/GPRS 或运营商许可证。

Syntax Description

map_name （可选）GTP 检测策略映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.5(1) 增加了对 GTPv2 和 IPv6 地址的支持。

使用指南

GPRS 隧道协议用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。服务提供商网络使用 GTP 通过终端之间的 GPRS 主干隧道传输多协议数据包。

默认情况下，GTP 检测未启用。但是，如果在未指定检测映射的情况下启用 GTP 检测，将会使用默认映射（默认映射提供以下处理）。仅在需要不同值的情况下，才需要配置映射。

- 不允许错误。
- 最大请求数为 200。
- 最大隧道数为 500。
- GSN/端点超时为 30 分钟。

- PDP 情景超时是 30 分钟。在 GTPv2 中，此值为承载情景超时。
- 请求超时为 1 分钟。
- 信令超时是 30 分钟。
- 隧道超时为 1 小时。
- T3 响应超时为 20 秒。
- 丢弃并记录未知消息 ID。此行为限于 3GPP 为 S5S8 接口定义的消息。可能允许为其他 GPRS 接口定义的消息，最大程度地减少对它们应用的检测。

使用 **policy-map type inspect gtp** 命令定义 GTP 的参数。定义 GTP 映射后，可使用 **inspect gtp** 命令启用该映射。然后，使用 **class-map**、**policy-map** 和 **service-policy** 命令定义流量类，向该类应用 **inspect** 命令，并将策略应用到一个或多个接口。

已知的 GTP 端口是 UDP 3386、2123 和 2152。

检查信令消息

要检查信令消息，**inspect gtp** 命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令 **inspect gtp** 命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route** 接口 **00** 指标 **tunneled** 形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要 **inspect gtp** 命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例显示如何限制网络中隧道的数量：

```
ciscoasa(config)# policy-map type inspect gtp gmap

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default

ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
clear service-policy inspect gtp	将清除全局 GTP 统计数据。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

命令	说明
showservice-policyinspectgtp	显示 inspect gtp 策略的状态和统计信息。

inspect h323

要启用 H.323 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspecth323** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect h323 { h225 | ras } [ map_name ]
no inspect h323 { h225 | ras } [ map_name ]
```

Syntax Description	h225	启用 H.225 信令检测。
	<i>map_name</i>	（可选）H.323 映射的名称。
	ras	启用 RAS 检查。

Command Default	默认端口分配如下：	
	• h323 h225 1720	
	• h323 RAS 1718-1719	

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。它取代了已弃用的 fixup 命令。

使用指南 inspect h323 命令为符合 H.323 的应用程序（例如 Cisco CallManager 和 VocalTec Gatekeeper）提供支持。H.323 是国际电信联盟 (ITU) 为 LAN 上的多媒体会议定义的一套协议。ASA 支持 H.323 至版本 6，包括 H.323 v3 功能“一个呼叫信令信道上的多个呼叫”。

启用 H.323 检查后，ASA 支持在同一呼叫信令信道上进行多个呼叫，这是 H.323 版本 3 添加的功能。此功能可缩短呼叫建立时间并减少 ASA 上端口的使用。

H.323 检测具有如下两个主要功能：

- 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。

检查信令消息

要检查信令消息，**inspecth323**命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspecth323**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspecth323**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 H.323 检测引擎，该引擎创建类映射来匹配默认端口 (1720) 上的 H.323 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map h323-port
ciscoasa(config-cmap)# match port tcp eq 1720
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map h323_policy

ciscoasa(config-pmap)# class h323-port
ciscoasa(config-pmap-c)# inspect h323
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy h323_policy interface outside
```

Related Commands

命令	说明
policy-maptypeinspect	创建检查策略映射。
showh225	显示通过 ASA 建立的 H.225 会话的信息。
showh245	显示终端使用慢启动通过 ASA 建立的 H.245 会话的信息。
showh323ras	显示通过 ASA 建立的 H.323 RAS 会话的信息。
timeout {h225 h323}	配置关闭 H.225 信令连接或 H.323 控制连接前的空闲时间。

inspect http

要启用 HTTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspecthttpcommand**。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect http [map_name]
no inspect http [map_name]
```

Syntax Description	map_name （可选）HTTP检测映射的名称。

Command Default	HTTP 的默认端口为 80。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。它取代了已弃用的 fixup 命令。

使用指南



提示 可以安装执行应用和 URL 过滤（包括 HTTP 检测）的服务模块，例如 ASACX 或 ASA FirePOWER。ASA 上运行的 HTTP 检测与这些模块不兼容。请注意，使用专用模块配置应用过滤比尝试使用 HTTP 检测策略映射在 ASA 上手动配置要简单的多。

使用 HTTP 检测引擎可防御特定攻击以及与 HTTP 流量相关的其他威胁。

HTTP 应用检测扫描 HTTP 报头和正文，并对数据执行各种检查。这些检查可防止各种 HTTP 构造、内容类型、隧道协议和消息传送协议通过安全设备。

增强型 HTTP 检测功能（又称为应用防火墙，在配置 HTTP 检测策略映射时可使用此功能）有助于防止攻击者使用 HTTP 消息来避开网络安全策略。

HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达 Web 服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。

增强型 HTTP 检测验证所有 HTTP 消息是否满足以下条件：

- 符合 RFC 2616 的要求
- 仅使用 RFC 定义的方法。
- 符合其他条件。

CR_Examples

在本例中，任何通过 any 接口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。由于采用了全局策略，检测仅在流量流入每个接口时发生。

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-map type inspect	创建检查策略映射。

inspect icmp

要配置 ICMP 检测引擎，请在类配置模式下使用 **inspecticmp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect icmp
no inspect icmp

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南 ICMP 检查引擎允许像 TCP 和 UDP 流量一样检查 ICMP 流量。如果没有 ICMP 检测引擎，我们建议您在 ACL 中不要允许 ICMP 通过 ASA。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检查引擎确保每个请求只有一个响应，并且序列号是正确的

当禁用 ICMP 检查时（默认配置），系统会拒绝从较低安全性接口至较高安全性接口的 ICMP 回应应答消息，即使该接口是对 ICMP 回应请求的响应。

CR_Examples 如以下示例所示启用 ICMP 应用检测引擎，该引擎创建一个使用 ICMP 协议 ID（对于 IPv4 为 1，对于 IPv6 为 58）匹配 ICMP 流量的类映射。然后，服务策略会被应用到到外部接口。要对所有接口启用 ICMP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
icmp	为在 ASA 接口终止的 ICMP 流量配置访问规则。
policy-map	定义将安全操作与一个或多个流量类别关联的策略。
service-policy	将策略映射应用到一个或多个接口。

inspect icmp error

要启用 ICMP 错误消息的应用检测，请在类配置模式下使用 `inspecticmp error` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

inspect icmp error
no inspect icmp error

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 <code>fixup</code> 命令。

使用指南

当启用 ICMP 错误检测时，ASA 将基于 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。ASA 将使用转换的 IP 地址覆盖数据包。

禁用时，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机与 ASA 之间的中间节点生成的 ICMP 错误消息将会到达外部主机，而不占用任何其他 NAT 资源。如果外部主机使用 `traceroute` 命令来跟踪连接 ASA 内部目标的跃点，这种方式则不合适。当 ASA 不转换中间跃点时，显示的所有中间跃点将带有映射目标 IP 地址。

会扫描 ICMP 负载，以从原始数据包检索五元组。然后，会使用检索到的五元组进行查找，以确定客户端的原始地址。ICMP 错误检测引擎会对 ICMP 数据包进行以下更改：

- 在 IP 报头中，映射 IP 更改为实际 IP（目标地址）并修改 IP 校验和。
- 在 ICMP 报头中，会根据 ICMP 数据包的变化修改 ICMP 校验和。
- 在负载中，会进行以下更改：
 - 原始数据包映射 IP 更改为实际 IP
 - 原始数据包映射端口更改为实际端口
 - 重新计算原始数据包 IP 校验和

CR_Examples

以下示例启用 ICMP 错误应用检测引擎，该引擎创建一个使用 ICMP 协议 ID（对于 IPv4 为 1，对于 IPv6 为 58）匹配 ICMP 流量的类映射。然后，服务策略会被应用到外部接口。要对所有接口启用 ICMP 错误检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
icmp	为在 ASA 接口终止的 ICMP 流量配置访问规则。
inspecticmp	启用或禁用 ICMP 检查引擎。
policy-map	定义将安全操作与一个或多个流量类别关联的策略。
service-policy	将策略映射应用到一个或多个接口。

inspect ils

要启用 ILS 应用检测，请在类配置模式下使用 `inspect ilscommand`。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

`inspect ils`
`no inspect ils`

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 <code>fixup</code> 命令。

使用指南

该 `inspectils`命令为使用 LDAP 与 ILS 服务器交换目录信息的 Microsoft NetMeeting、SiteServer 和 Active Directory 产品提供 NAT 支持。

ASA 支持 ILS 的 NAT，用于在 ILS 或 SiteServer 目录中注册和定位端点。因为 LDAP 数据库仅存储 IP 地址，所以，无法支持 PAT。

对于搜索响应，当 LDAP 服务器位于外部时，应考虑使用 NAT，以允许内部对等设备在注册到外部 LDAP 服务器时进行本地通信。对于此类搜索响应，会先搜索 `xlate`，然后搜索 DNAT 条目以获得正确地址。如果上述两种搜索都失败，则地址未更改。对于使用 NAT 0（无 NAT）且不期望 DNAT 交互的站点，建议关闭检测引擎以提供更佳性能。

当 ILS 服务器位于 ASA 边界内时，可能需要进行其他配置。这就需要提供 一个孔来让外部客户端在指定的端口（通常为 TCP 389）上访问 LDAP 服务器。

由于 ILS 流量仅发生在辅助 UDP 通道上，因此 TCP 连接在 TCP 不活动间隔后断开。默认情况下，此间隔为 60 分钟，可以使用命令进行调 `timeout`整。

ILS/LDAP 遵循客户端/服务器模式，通过单个 TCP 连接处理会话。根据客户端的操作，将可能创建多个上述会话。

在连接协商期间，BIND PDU 会从客户端发送至服务器。一旦收到来自服务器的成功 BIND RESPONSE，系统就可能交换其他操作消息（例如 ADD、DEL、SEARCH 或 MODIFY），以对 ILS 目录执行多项操作。ADD REQUEST 和 SEARCH RESPONSE PDU 可能包含 NetMeeting 对等设备的

IP 地址，H.323（SETUP 和 CONNECT 消息）使用它建立 NetMeeting 会话。Microsoft NetMeeting v2.X 和 v3.X 提供 ILS 支持。

ILS 检测将执行以下操作：

- 使用 BER 解码功能解码 REQUEST/RESPONSE PDU。
- 解析 LDAP 数据包。
- 提取 IP 地址。
- 根据需要转换 IP 地址。
- 使用 BER 编码功能，用已转换地址对 PDU 进行编码。
- 将新编码的 PDU 复制回 TCP 数据包。
- 执行递增 TCP 校验和与序列号调整。

ILS 检测存在如下局限性：

- 不支持推荐请求和响应。
- 多个目录中的用户不统一。
- NAT 无法标识多个目录中具有多个身份的单一用户。



注释 由于 H.225 呼叫信令流量仅发生在辅助 UDP 通道上，因此 TCP 连接会在 TCP 命令指定的时间间隔后断 **timeout** 开。默认情况下，此间隔设置为 60 分钟。

CR_Examples

如下示例所示启用 ILS 检测引擎，该引擎创建一个类映射来匹配默认端口（389）上的 ILS 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 ILS 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map ils-port
ciscoasa(config-cmap)# match port tcp eq 389
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ils_policy

ciscoasa(config-pmap)# class ils-port
ciscoasa(config-pmap-c)# inspect ils
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ils_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。

命令	说明
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。

inspect im

要启用 Instant Messenger 流量检测，请在类配置模式下使用 `inspect im` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

inspect *immap_name*
no inspect *immap_name*

Syntax Description

map_name IM 映射的名称。

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
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

该 **inspect im** 命令启用或禁用 IM 协议的应用程序检查。使用即时消息 (IM) 检测引擎可以控制 IM 的网络使用情况，以及阻止机密数据泄露、蠕虫传播和针对公司网络的其他威胁。

CR_Examples

以下示例显示如何定义 IM 检查策略图：

```
ciscoasa(config)# regex loginname1 "user1@example.com"
ciscoasa(config)# regex loginname2 "user2@example.com"
ciscoasa(config)# regex loginname3 "user3@example.com"
ciscoasa(config)# regex loginname4 "user4@example.com"
ciscoasa(config)# regex yahoo_version_regex "1\\.0"
ciscoasa(config)# regex gif_files "\.gif"
ciscoasa(config)# regex exe_files "\.exe"
ciscoasa(config)# class-map type regex match-any yahoo_src_login_name_regex
ciscoasa(config-cmap)# match regex loginname1
ciscoasa(config-cmap)# match regex loginname2
ciscoasa(config)# class-map type regex match-any yahoo_dst_login_name_regex
ciscoasa(config-cmap)# match regex loginname3
ciscoasa(config-cmap)# match regex loginname4
ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
```

```

ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex
ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy2
ciscoasa(config-cmap)# match version regex yahoo_version_regex
ciscoasa(config)# class-map im inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all

```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	创建检查策略映射。
show running-config policy-map	显示所有当前的策略映射配置。
match protocol	匹配检测类或策略映射中的特定 IM 协议。

inspect ip-options

要启用数据包报头中 IP 选项的检测，请在类或策略映射类型检查配置模式下使用 `inspect ip-options` 命令。可以从 `map configuration` 模式访问 `Class configuration` 模式。要删除配置，请使用此命令 **no** 的形式。

inspect ip-options [*map_name*]
no inspect ip-options*map_name*

Syntax Description

map_name （可选。）IP 选项映射的名称。

Command Default

默认情况下，此命令在全局策略中启用。默认检测映射会允许带有 `router-alert` 选项的数据包，但会丢弃带有任何其他选项的数据包。

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
策略或类映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.2(2) 添加了此命令。支持的选项有 **coolnop**、和 **router-alert** 选项。如果 IP 报头包含除 EOOL、NOP 或 RTRALT 之外的其他选项，无论 ASA 是否配置为允许这些选项，ASA 都会丢弃该数据包。

9.5(1) 增加了对所有 IP 选项的支持。

使用指南

在数据包中，IP 报头包含选项 (Options) 字段。选项字段，通常称为 IP 选项，提供在某些情况下需要但对于大多数常见通信来说不必要的控制功能。具体来说，IP 选项提供了时间戳、安全性和特殊路由。IP 选项的使用是可选的，并且该字段可以包含零个、一个或多个选项。

您可以配置 IP 选项检测，以便基于数据包信头 IP Options 字段的内容控制允许的 IP 数据包。您可以丢弃包含不需要选项的数据包、清除选项（并允许数据包）或者允许该数据包而不做任何更改。

如果希望进行非默认处理，请创建 IP 选项检测策略映射，输入 **parameter** 命令，然后指定要对各个选项采取的操作。可以检测以下选项。在所有情况下，**allow** 操作允许包含指定选项且未经过修改的数据包；**clear** 操作允许包含指定选项的数据包，但会从报头中删除该选项。

使用命令 **no** 的形式从地图中删除选项。任何包含映射中未包括的选项的数据包都会被丢弃，即使数据包中包含其他允许或清除的选项。

有关 IP 选项的列表以及相关 RFC 的引用，请参阅 IANA 页面：

<http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml>。

- **{defaultactionallow| clear}**—为地图中未明确包含的任何选项设置默认操作。如果您未设置允许或清除的默认操作，则包含不允许选项的数据包将被丢弃。
- **{basic-securityactionallow| clear}**—允许或清除安全 (SEC) 选项。
- **{commercial-securityactionallow| clear}**—允许或清除商业安全 (CIPSO) 选项。
- **{eoolactionallow| clear}**—允许或清除选项列表末尾选项。此选项仅包含一个零字节，出现在所有选项的末尾，以标记选项列表的结束。根据标题长度，这可能与标题的末端不一致。
- **{exp-flow-controlactionallow| clear}**—允许或清除实验流控制 (FINN) 选项。
- **{exp-measurementactionallow| clear}**—允许或清除实验测量 (ZSU) 选项。
- **{extended-securityactionallow| clear}**—允许或清除扩展安全 (E-SEC) 选项。
- **{imi-traffic-descriptoractionallow| clear}**—允许或清除 IMI 流量描述符 (IMITD) 选项。
- **{nopactionallow| clear}**—允许或清除无操作选项。IP 报头中的选项字段可以包含零个、一个或多个选项，这使得该字段的总长度可变。但是，IP 报头必须是 32 位的倍数。如果所有选项的位数不是 32 位的倍数，NOP 选项将被作为“内部填充”，用于对齐 32 位边界上的选项。
- **{quick-startactionallow| clear}**—允许或清除快速启动 (QS) 选项。
- **{record-routeactionallow| clear}**—允许或清除记录路线 (RR) 选项。
- **{router-alertactionallow| clear}**—允许或清除路由器警报 (RTRALT) 选项。默认 IP 选项 (IP Options) 检测策略映射允许此选项。此选项通知传输路由器检测数据包的内容，即使数据包未流向该路由器。在实施 RSVP 和类似协议时，这种检查很有价值，因为这些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。丢弃包含 Router Alert 选项的 RSVP 数据包可能会导致 VoIP 的实施出现问题。
- **{timestampactionallow| clear}**—允许或清除时间戳 (TS) 选项。
- **{0-255} action {allow| clear}**—允许或清除由选项类型编号标识的选项。该编号是完整的选项类型，八位数（副本、类和选项编号），而不只是八位数的选项编号部分。这些选项类型可能不代表实际选项。非标准选项必须采用 Internet 协议 RFC 791 (<http://tools.ietf.org/html/rfc791>) 中定义的预期类型长度值格式。

CR_Examples

以下示例显示如何定义 IP 选项检测策略映射，以允许 ASA 传输数据包报头中包含 EOOL、NOP 和 RTRALT 选项的数据包。

```
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
```

以下示例显示如何设置新的默认操作，以允许具有任何 IP 选项的数据包。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action allow
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	创建检查策略映射。

inspect ipsec-pass-thru

要启用 IPsec 直通检测，请在类映射配置模式下使用 `inspect ipsec-pass-thru` 命令。可以从 `map configuration` 模式访问 `Class configuration` 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect ipsec-pass-thru [ map_name ]
no inspect ipsec-pass-thru [ map_name ]
```

Syntax Description *map_name* （可选）IPsec 直通映射的名称。

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
类配置	• 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

inspect ipsec-pass-thru 命令可以启用或禁用应用检测。IPsec 直通应用程序检查可方便地遍历与 IKE UDP 端口 500 连接相关的 ESP（IP 协议 50）和/或 AH（IP 协议 51）流量。它避免了冗长的访问列表配置以允许 ESP 和 AH 流量，并且还使用超时和最大连接提供安全性。

使用 IPsec 传递参数映射来标识要用于定义检测参数的特定映射。使用 `policy-map type inspect` 命令访问参数配置，它允许您指定 ESP 或 AH 流量的限制。您可以在参数配置模式下设置每客户端最大连接数和空闲超时。

使用 `class-map`、`policy-map` 和 `service-policy` 命令定义流量类，向该类应用 `inspect` 命令，以及将策略应用到一个或多个接口。定义的参数映射与 `inspect ipsec-pass-thru` 命令一起使用时启用。

允许 NAT 流量和非 NAT 流量。但是，不支持 PAT。



注释 在 ASA 7.0(1) 中，**inspect ipsec-pass-thru** 命令仅允许 ESP 流量通过。如果在未指定任何参数的情况下指定 **inspect ipsec-pass-thru** 命令，要在更高版本中保留相同的行为，则会创建并附加一个允许 ESP 的默认映射。此映射可在 `show running-config all` 命令的输出中看到。

CR_Examples

它避免了冗长的访问列表配置以允许 ESP 和 AH 流量，并且还使用超时和最大连接提供安全性。

```
ciscoasa(config)# access-list ipsecpassthruacl permit udp any any eq 500
ciscoasa(config)# class-map ipsecpassthru-traffic
ciscoasa(config-cmap)# match access-list ipsecpassthruacl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru iptmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
ciscoasa(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
ciscoasa(config)# policy-map inspection_policy
ciscoasa(config-pmap)# class ipsecpassthru-traffic
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru iptmap
ciscoasa(config)# service-policy inspection_policy interface outside
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。
match protocol	匹配检测类或策略映射中的特定 IM 协议。

inspect ipv6

要启用 IPv6 检测，请在类配置模式下使用 `inspect ipv6` 命令。可从策略映射配置模式访问类配置模式。要删除配置，请使用此命令 `no` 的形式。

```
inspect ipv6 [map_name]
no inspect ipv6 [map_name]
```

Syntax Description	<i>map_name</i> （可选。）IPv6 检测策略映射的名称。

Command Default	默认情况下，IPv6 检查是禁用的。 如果启用 IPv6 检测但不指定检测策略映射，将会使用默认 IPv6 检测策略映射并执行以下操作： • 仅允许已知的 IPv6 扩展报头。丢弃并记录不符合要求的数据包。 • 按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。 • 丢弃带有路由类型报头的任何数据包。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	8.2(1) 添加了此命令。

使用指南 IPv6 检测根据扩展报头有选择性地记录或丢弃 IPv6 流量。此外，IPv6 检测可以检查 Pv6 数据包中扩展报头的类型和顺序是否符合 RFC 2460 的要求。

CR_Examples 以下示例丢弃所有带有逐跳、目标选项、路由地址和路由类型 0 标头的 IPv6 流量：

```
policy-map type inspect ipv6 ipv6-pm
parameters
match header hop-by-hop
drop
match header destination-option
drop
match header routing-address count gt 0
```

```
drop
match header routing-type eq 0
drop
policy-map global_policy
class class-default
inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
匹配报头	匹配 IPv6 检测策略映射中的 IPv6 报头。
policy-map typeinspectipv6	为 IPv6 创建检查策略图。
policy-map	创建第 3/4 层策略映射。
verify-header	配置 IPv6 检测参数。

inspect lisp

要启用 LISP 检查，请在 **inspectlisp** 类配置模式下使用该命令。您可以通过首先输入命令来访问类配置 **policy-map** 模式。要禁用 LISP 检查，请使用此 **no** 命令的形式。

inspect lisp [*inspect_map_name*]
no inspect lisp [*inspect_map_name*]

Syntax Description

inspect_map_name 如果要限制 EID 或需要为 LISP 消息指定预共享密钥，请指定 LISP 检测映射名称 (**policy-maptypeinspectlisp**)。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.5(2) 我们添加了此命令。

使用指南

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

关于集群流移动性的 LISP 检查

ASA 检测 LISP 流量是否发生位置更改，然后使用此信息进行无缝集群操作。如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

集群流移动性包含多种相互关联的配置：

- （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。请参阅 **policy-maptypeinspectlisp**、**allowed-eid** 和 **validate-key** 命令。
- LISP 流量检查 - ASA 检查 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。查看 **inspectlisp** 命令。

3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。查看命令。 **clusterflow-mobilitylisp**
4. 站点 ID - ASA 使用每个集群设备的站点 ID 确定新的所有者。查看命令。 **site-id**
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。查看命令。 **flow-mobilitylisp**

CR_Examples

以下示例检查位于 192.168.50.89 的 LISP 路由器（位于内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（位于另一个 ASA 接口上）之间的 LISP 流量（UDP 4342）：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

Related Commands

命令	说明
allowed-eids	基于 IP 地址限制检测到的 EID。
clear cluster info flow-mobility counters	清除流移动性计数器。
clear lisp eid	从 ASA EID 表中删除 EID。
cluster flow-mobility lisp	为服务策略启用流移动性。
flow-mobility lisp	为集群启用流移动性。
inspect lisp	检测 LISP 流量。
policy-map type inspect lisp	定制 LISP 检测。
site-id	为集群机箱设置站点 ID。
show asp table classify domain inspect-lisp	显示 LISP 检测的 ASP 表。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show lisp eid	显示 ASA EID 表。
show service-policy	显示服务策略。
validate-key	输入预共享密钥以验证 LISP 消息。

inspect m3ua

要启用 M3UA 检测，请在类配置模式下使用 **inspectm3ua** 命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命令的 **no** 形式可禁用 M3UA 检测。

```
inspect m3ua [map_name]
no inspect m3ua [map_name]
```



注释 M3UA 检查需要运营商许可证。

Syntax Description

map_name （可选）M3UA 检测策略映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南

MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接 SS7 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。M3UA 在 RFC 4666 中定义。

M3UA 使用 SCTP 作为传输层。SCTP 端口 2905 是预期端口，但可以配置信令网关使用不同的端口。

MTP3 层提供网络功能，例如路由和节点寻址，但使用点代码来识别节点。M3UA 层可交换源点码 (OPC) 和目标点码 (DPC)。这与 IP 使用 IP 地址识别节点的方式类似。

M3UA 检测提供的协议符合具有限制性。

您可以选择创建 M3UA 检查策略图，以根据点代码或服务指标 (SI) 应用访问策略。此外，还可以基于消息类和类型应用速率限制。

CR_Examples

以下示例显示了 M3UA 检测策略映射和检测策略。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(hostname(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect m3ua m3ua-map
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
show service-policy inspect m3ua	显示检查 M3UA 策略的状态和统计信息。

inspect mgcp

要启用 MGCP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 `inspect mgcp` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

```
inspect mgcp [map_name]
no inspect mgcp [map_name]
```

Syntax Description `map_name` （可选）MGCP 映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 `fixup` 命令。

使用指南 要使用 MGCP，您通常至少需要配置至少两个 `inspect` 命令：一个用于网关接收命令的端口，另一个用于呼叫代理接收命令的端口。通常，呼叫代理将命令发送到网关的默认 MGCP 端口 (2427)，而网关将命令发送到呼叫代理的默认 MGCP 端口 (2727)。

MGCP 用于从称为媒体网关控制器或呼叫代理的外部呼叫控制元件控制媒体网关。媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。借助具有 MGCP 的 NAT 和 PAT，可以使用一组有限的外部（全局）地址来支持内部网络中的大量设备。

媒体网关示例如下：

- 中继网关：用于在电话网络和 IP 语音网络之间建立连接。这种网关通常管理大量的数字电路。
- 家庭网关：提供用于连接到 IP 语音网络的传统模拟 (RJ11) 接口。住宅网关的示例包括电缆调制解调器/电缆机顶盒、xDSL 设备和宽带无线设备。
- 商业网关，为 IP 语音网络提供传统的数字 *PBX* 接口或集成的软 *PBX* 接口。

MGCP 消息通过 UDP 传输。响应会发送回命令的源地址（IP 地址和 UDP 端口号），但响应可能不会到达收到命令的同一地址。如果在同一故障转移配置中使用多个呼叫代理，且接收命令的呼叫代理已经将控制转交给备用呼叫代理，由备用呼叫代理来发送响应，可能会发生这种情况。



注释 MGCP 呼叫代理发送 AUPEP 消息，以确定 MGCP 终端是否存在。这样将通过 ASA 建立一个数据流，并允许 MGCP 终端注册到呼叫代理。

在 MGCP 映射配置模式下使用 **call-agent** 和 **gateway** 命令配置一个或多个呼叫代理和网关的 IP 地址。在 MGCP 映射配置模式下，使用 **command-queue** 命令可指定命令队列中一次允许的最大 MGCP 命令数。

检查信令消息

要检查信令消息，**inspectmgcp** 命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令 **inspectmgcp** 命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route** 接口 **00** 指标 **tunneled** 形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要 **inspectmgcp** 命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

可排队的 MGCP 命令的最大数量为 150。

CR_Examples

以下示例显示如何识别 MGCP 流量、定义 MGCP 检查图、定义策略以及将策略应用于外部接口。这样将创建一个类映射，以便匹配默认端口（2427 和 2727）上的 MGCP 流量。然后，服务策略会被应用到外部接口。此配置允许呼叫代理 10.10.11.5 和 10.10.11.6 控制网关 10.10.10.115，并允许呼叫代理 10.10.11.7 和 10.10.11.8 控制两个网关 10.10.10.116 和 10.10.10.117。要对所有接口启用 MGCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2427

ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2727
ciscoasa(config)# class-map mgcp_port
ciscoasa(config-cmap)# match access-list mgcp_acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect mgcp inbound_mgcp
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-agent 10.10.11.5 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.6 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.7 102
ciscoasa(config-pmap-p)# call-agent 10.10.11.8 102
ciscoasa(config-pmap-p)# gateway 10.10.10.115 101
ciscoasa(config-pmap-p)# gateway 10.10.10.116 102
ciscoasa(config-pmap-p)# gateway 10.10.10.117 102
ciscoasa(config-pmap-p)# command-queue 150
ciscoasa(config-mgcp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class mgcp_port
ciscoasa(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map type inspect mgcp	为 MGCP 创建检查策略图。
show mgcp	显示通过 ASA 建立的 MGCP 会话的相关信息。
timeout	为不同协议和会话类型设置最大空闲持续时间。

inspect mmp

要配置 MMP 检测引擎，请在类配置模式下使用 **inspectmmp** 命令。要删除 MMP 检查，请使用此 **no** 命令的形式。

inspect mmp tls-proxy [名称]
no inspect mmp tls-proxy [名称]

Syntax Description

name 指定 TLS 代理实例名称。

tls-proxy 为 MMP 检测启用 TLS 代理。MMP 协议可以额外使用 TCP 传输；但是，CUMA 客户端仅支持 TLS 传输。因此，要启用 MMP 检测，必须使用 **tls-proxy** 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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.0(4) 命令已添加。

使用指南

ASA 包括用于验证 CUMA 移动多路复用协议 (MMP) 的检测引擎。MMP 是一种用于在 CUMA 客户端与服务器之间传输数据实体的数据传输协议。当 ASA 部署在 CUMA 客户端与服务器之间并需要检测 MMP 数据包时，请使用 **inspectmmp** 命令。

由于 MMP 流量只能通过 TLS 连接传输，因此必须带 TLS 代理启用 MMP 检测。



注释 请注意，在配置 MMP 检测引擎时，它只能添加到非默认检测类下。

CR_Examples

以下示例展示如何使用 **inspectmmp** 命令检测 MMP 流量：

```
ciscoasa
(config)#
class-map mmp
```

```
ciscoasa
(config-cmap) #
match port tcp eq 5443
ciscoasa
(config-cmap) #
exit
ciscoasa
(config) #
policy-map mmp-policy
ciscoasa
(config-pmap) #
class mmp
ciscoasa (config-pmap-c) # inspect mmp tls-proxy myproxy
ciscoasa (config-pmap-c) # exit
ciscoasa (config-pmap) # exit
ciscoasa
(config) #
service-policy mmp-policy interface outside
```

Related Commands

命令	说明
tls-proxy	配置 TLS 代理实例。

inspect netbios

要启用 NetBIOS 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect netbios** **command**。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect netbios [map_name]
no inspect netbios [map_name]
```

Syntax Description

map_name （可选）NetBIOS 映射的名称。

Command Default

默认情况下会启用此命令。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

inspectnetbios 命令启用或禁用 NetBIOS 协议的应用检查。默认情况下，NetBIOS 检测处于启用状态。NetBIOS 检查引擎根据 ASA NAT 配置转换 NetBIOS 名称服务 (NBNS) 数据包中的 IP 地址。或者可以创建策略映射以便丢弃或记录 NetBIOS 协议违规情况。

CR_Examples

以下示例显示如何定义 NetBIOS 检查策略映射：

```
ciscoasa(config)# policy-map type inspect netbios netbios_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation drop
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
policy-map type inspect netbios	为 NetBIOS 创建检查策略图。
service-policy	将策略映射应用到一个或多个接口。

inspect pptp

要启用 PPTP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 `inspect pptp` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

inspect pptp
no inspect pptp

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 <code>fixup</code> 命令。

使用指南

点对点隧道协议 (PPTP) 是用于通过隧道传送 PPP 流量的协议。PPTP 会话通常包括一个 TCP 信道和两个 PPTP GRE 隧道。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道承载两台主机之间的 PPP 会话。

启用后，PPTP 应用检测会检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所需的 GRE 连接和转换。仅支持 RFC 2637 中定义的版本 1。

仅当通过 PPTP TCP 控制通道进行协商时，才会对 GRE 的修改版本 [RFC 2637] 执行 PAT。未修改版本的 GRE [RFC 1701、RFC 1702] 不执行端口地址转换。

特别是，ASA 会检测 PPTP 版本通知和对外呼叫请求/响应序列。仅检查 RFC 2637 中定义的 PPTP 版本 1。如果任一端公布的版本不是版本 1，将会禁用对 TCP 控制信道的进一步检测。此外，还会跟踪传出呼叫请求和应答序列。连接和 xlate 根据需要动态分配，以允许后续的辅助 GRE 数据流量。

要以 PAT 方式转换 PPTP 流量，必须启用 PPTP 检测引擎。此外，仅对符合如下条件的 GRE 版本执行 PAT：经过修改的（如 RFC2637 所要求）；且是通过 TCP 控制信道协商的。未修改版本的 GRE（RFC 1701 和 RFC 1702）不会执行 PAT。

如 RFC 2637 中所述，PPTP 协议主要用于将从调制解调器组 PAC（PPTP 访问集中器）发起的 PPP 会话隧道传送到头端 PNS（PPTP 网络服务器）。按这种方式使用时，PAC 为远程客户端，而 PNS 为服务器。

但是，当 Windows 用于 VPN 时，交互作用是反向的。PNS 是一种远程单用户 PC，用于启动与头端 PAC 的连接以获取对中央网络的访问权限。

要对所有接口启用 PPTP 检测，请使用 **global** 参数代替 **interfaceoutside**。

CR_Examples

如以下例所示，启用 PPTP 检测引擎，该引擎创建一个类映射来匹配默认端口 (1723) 上的 PPTP 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# class-map pptp-port
ciscoasa(config-cmap)# match port tcp eq 1723
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pptp_policy
ciscoasa(config-pmap)# class pptp-port
ciscoasa(config-pmap-c)# inspect pptp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy pptp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect radius-accounting

要启用或禁用 RADIUS 计费检测，或者要定义用于控制流量或隧道的映射，请在类配置模式下使用 **inspectradius-accounting** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect radius-accountingmap_name
no inspect radius-accounting [map_name]
```

Syntax Description *map_name* RADIUS 计费映射的名称。

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
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

RADIUS 计费检测是为了防止使用 RADIUS 服务器的 GPRS 网络上出现过度计费攻击。虽然实施 RADIUS 计费检测无需 GTP/GPRS or Carrier 许可证，但它毫无意义，除非您正在实施 GTP 检测并已设置 GPRS。

使用 **policy-maptypeinspectradius-accounting**命令创建检测映射，以用于定义 RADIUS 计费的参数。输入 parameters 命令后，您可以使用 **sendresponse**、**host**、**validate-attribute**、**enablegprs**和 **timeoutusers** 命令定义检测特征和行为。

然后使用 **class-maptypemanagement**、**policy-map**和 **service-policy** 命令定义流量类，向该类应用 inspect radius-accounting 命令，并将策略应用到一个或多个接口。



注释 **inspectradius-accounting** 命令只能与 **class-maptypemanagement** 命令一起使用。

CR_Examples

以下示例显示如何配置 RADIUS 计费检测映射并全局启用检测。


```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

Related Commands

命令	说明
parameters	定义要应用的安全操作的流量类。
class-map type management radius-class	用于标识流向要应用操作的 ASA 的第 3 层或第 4 层管理流量。
policy-map type inspect radius-accounting	为 RADIUS 计费创建检查策略图。
show 和 clear service-policy	允许您查看和清除服务策略设置。
service-policy	将策略映射应用到一个或多个接口。

inspect rsh

要启用 RSH 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 `inspect rsh` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 `no` 的形式。

`inspect rsh`
`no inspect rsh`

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会启用此命令。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 <code>fixup</code> 命令。

使用指南 RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务端协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测支持协商端口号的 NAT。

CR_Examples

以下示例启用 RSH 检测引擎，创建类映射以匹配默认端口 (514) 上的 RSH 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 RSH 检测，请使用 `global` 参数代替 `interfaceoutside`。

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy

ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect rtsp

要启用 RTSP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 `inspect rtsp` 命令。可从策略映射配置模式访问类配置模式。要删除配置，请使用此命令 `no` 的形式。

```
inspect rtsp [map_name]
no inspect rtsp [map_name]
```

Syntax Description *map_name* （可选）RTSP 映射的名称。

Command Default 默认情况下会启用此命令。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 `fixup` 命令。

使用指南 `inspectrtsp` 命令允许 ASA 传递 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer 和思科 IP/TV 连接都使用 RTSP。



注释 对于 Cisco IP/TV，使用 RTSP TCP 端口 554 和 TCP 8554。

RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。根据 RFC 2326 要求，ASA 仅支持 TCP。此 TCP 控制通道用于协商将用于传输音频/视频流量的数据通道，具体取决于客户端上配置的传输模式。

支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。

ASA 解析状态代码为 200 的设置响应消息。如果响应消息要入站，服务器需相对于 ASA 处于外部，并需要为连接从服务器进入站内打开动态信道。如果响应消息要出站，则 ASA 无需打开动态信道。

由于 RFC 2326 不要求客户端和服务器端口必须位于设置响应消息中，因此 ASA 需要保持状态并记住设置消息中的客户端端口。QuickTime 将客户端端口放在设置消息中，然后服务器仅使用服务器端口进行响应。

使用 RealPlayer

使用 RealPlayer 时，正确配置传输模式非常重要。对于 ASA，从服务器向客户端添加命令 **access-list** 语句，反之亦然。对于 RealPlayer，请通过以下选择更改传输模式 **Options**、**Preferences**、**Transport**、**RTSPSettings**。

如果 RealPlayer 使用 TCP 模式，请选中 **UseTCPtoConnecttoServer** 和 **AttempttouseTCPforallcontent** 复选框。在 ASA 上无需配置检测引擎。

If using UDP mode on the RealPlayer, check the **UseTCPtoConnecttoServer** and **AttempttouseUDPforstaticcontent** check boxes, and for live content not available via Multicast. 在 ASA 中添加 **inspectrtsp** 端口 命令语句。

限制和局限性

RSTP 检测有以下局限性。

- ASA 不支持通过 UDP 的组播 RTSP 或 RTSP 消息。
- ASA 无法识别 RTSP 消息隐藏在 HTTP 消息中的 HTTP 掩蔽技术。
- ASA 无法对 RTSP 消息执行 NAT，因为嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。数据包可以分段，但 ASA 无法对分段的数据包执行 NAT。
- 对于思科 IP/TV，ASA 对消息 SDP 部分可执行的转换数与内容管理器中的程序列表数呈正比（每个程序列表至少可包含六个嵌入式 IP 地址）。
- 可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器位于外部网络，而服务器位于内部网络，则思科 IP/TV 只能采用 NAT。

CR_Examples

以下示例启用 RTSP 检测引擎，该引擎创建类映射来匹配默认端口（554 和 8554）上的 RTSP 流量。然后，服务策略会被应用到外部接口。

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554

ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic

ciscoasa(config-cmap)# match access-list rtsp-acl

ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy

ciscoasa(config-pmap)# class rtsp-traffic
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect scansafe

要对类中的流量启用云网络安全检测，请在类配置模式下使用 **inspectscansafe** 命令。您可以通过首先输入命令来访问类配置 **policy-map** 模式。要删除检查操作，请使用此命令 **no** 的形式。

inspect scansafescansafe_policy_name [**fail-open** | **fail-close**]
no inspect scansafescansafe_policy_name [**fail-open** | **fail-close**]

Syntax Description

scansafe_policy_name 指定由 **policy-map type inspect scansafe** 命令定义的检测类映射名称。

fail-open (可选) 如果云网络安全服务器不可用，则允许流量通过 ASA。

fail-close (可选) 如果云网络安全服务器不可用，则丢弃所有流量。**fail-close** 是默认设置。

Command Default

fail-close 为默认值。

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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

思科云网络安全通过软件即服务 (SaaS) 模式提供 Web 安全和 Web 过滤服务。如果企业的网络中配备 ASA，不必额外安装硬件即可使用云网络安全服务。



注释 此功能也称为“ScanSafe”，因此某些命令中会显示 ScanSafe 名称。

使用模块化策略框架配置此命令：

1. 使用 **policy-map type inspect scansafe** 命令创建检测策略映射，至少一个用于 HTTP，一个用于 HTTPS（假设您要检测两种类型的流量）。
2. （可选）使 **class-map type inspect scansafe** 用命令配置白名单。
3. 使用 **the class-map** 命令定义要检测的流量。您必须为 HTTP 和 HTTPS 流量配置单独的类映射。

4. 输入 **policy-map** 命令以定义策略。
5. 对于 HTTP，请输入 **class** 命令以引用 HTTP 类映射。
6. 输入引用 HTTP 检测策略映射的 **inspectscansafe** 命令。
7. 对于 HTTPS，请输入 **class** 命令以引用 HTTPS 类映射。
8. 输入引用 HTTPS 检测策略映射的 **inspectscansafe** 命令。
9. 最后，使用命令将策略映射应用到接 **service-policy** 口。

CR_Examples

以下示例配置两个类：一个是 HTTP 流量类，一个是 HTTPS 流量类。每个 ACL 都可以使 HTTP 和 HTTPS 流量免于被发送到 www.cisco.com 和 tools.cisco.com，以及 DMZ 网络。所有其他流量将被发送到云网络安全，但来自若干白名单用户和组的流量除外。然后，策略将被应用到内部接口。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object dmz_network eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443
ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config-cmap)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS
ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
```

```

ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside

```

Related Commands

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户身份，则指定默认用户名和/或组。
[https] (参数)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，以指示请求来自哪个组织。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前等待的时间。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-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。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

检查 SCTP

要启用或禁用流控制传输协议 (SCTP) 检测，请在类配置模式下使用 **inspect sctp** 命令。可以从 map configuration 模式访问 Class configuration 模式。使用此命令的形式可以禁用 SCTP 检查。

```
inspect sctp [map_name]
no inspect sctp [map_name]
```



注释 SCTP 检查需要运营商许可证。

Syntax Description *map_name* （可选）SCTP 检测策略映射的名称。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

9.5(2) 添加了此命令。

使用指南

SCTP（流控制传输协议）支持电话信令协议 SS7，也是 4G LTE 移动网络架构中多个接口的传输协议。如果有移动网络流量通过设备，则可以使用 SCTP 检测以及 GTP 和 Diameter 检测。

如果要过滤 SCTP 应用以提供可变服务，可以选择性地指定 SCTP 策略映射。您可以根据负载协议标识符 (PPID)，选择性地丢弃、记录或按速率限制 SCTP 流量类。使用 **policy-map type inspect sctp** 命令创建策略映射。

CR_Examples

以下示例创建的检测策略映射将丢弃未分配的 PPID（写入此示例时未分配）、按速率限制 PPID 32-40，并记录 Diameter PPID。该服务策略会对向匹配所有 SCTP 流量的 inspection_default 类应用检测。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
 drop
```

```
match ppid 26
  drop
match ppid 49
  drop
match ppid 32 40
  rate-limit 1000
match ppid diameter
  log
policy-map global_policy
class inspection_default
  inspect sctp sctp-pmap
!
service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
clearservice-policyinspect sctp	清除全局 Sctp 统计信息。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用到一个或多个接口。
showservice-policyinspect sctp	显示 inspect sctp 策略的状态和统计信息。

inspect sip

要启用 SIP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect sip** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-imeproxy** *name*]
no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-imeproxy** *name*]

Syntax Description

phone-proxy *proxy_name* 为指定的检测会话启用电话代理。

sip_map 指定 SIP 策略映射名称。

tls-proxy *proxy_name* 为指定的检测会话启用 TLS 代理。关键字 **tls-proxy** 不能用作第 7 层策略映射名称。

uc-imeproxy *name* 为 SIP 检查启用思科公司间媒体引擎代理。

Command Default

默认情况下，SIP 检测已通过默认检测映射启用，具体如下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：允许。
- 隐藏服务器和终端的 IP 地址：已禁用。
- 掩蔽软件版本和非 SIP URI：已禁用。
- 确保到目标的跳数大于 0：已启用。
- RTP 符合性：未执行。
- SIP 符合性：不执行状态检查和报头验证。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

SIP 的默认端口分配是 5060。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

8.0(2) 添加了 **tls-proxy** 关键字。

9.4(1) 删除了 **phone-proxy** 和 **uc-ime** 关键字。

使用指南

SIP 是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是 SIP 本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。

SIP 应用检测会在消息信头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。SIP 应用检测还支持应用安全和协议符合性（此功能强制对 SIP 消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。

为了支持 SIP 呼叫通过 ASA，必须检测媒体连接地址、媒体端口和媒体初期连接的信令消息，因为在已知目标端口 (UDP/TCP 5060) 上发送信令时，系统会动态分配媒体流。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。SIP 检查对这些嵌入式 IP 地址应用 NAT。

SIP 检查的限制

SIP 检测适用于嵌入式 IP 地址的 NAT。但是，如果配置 NAT 来转换源地址和目标地址，将不会重写外部地址（“trying” 响应消息的 SIP 报头中的 “from”）。因此，在处理 SIP 流量时应使用对象 NAT，从而避免转换目标地址。

当与 SIP 结合使用 PAT 时，有以下限制和限定：

- 如果远程终端尝试在 ASA 保护的网络上注册 SIP 代理，在非常特殊的条件下注册会失败，如下所示：
 - 对远程终端配置了 PAT。
 - SIP 注册服务器位于外部网络。
 - 在终端发送给代理服务器的 REGISTER 消息中，联系人字段中的端口缺失。
- 如果在 SIP 设备传输数据包时，该数据包的 SDP 部分的所有者/创建者字段 (o=) 中的 IP 地址与连接字段 (c=) 中的 IP 地址不同，则可能未正确转换 o= 字段中的 IP 地址。这是 SIP 协议的如下局限性造成的：不在 o= 字段中提供端口值。
- 使用 PAT 时，任何包含无端口的内部 IP 地址的 SIP 报头字段都可能不会转换，因此，内部 IP 地址将向外泄漏。如果要避免这种泄漏，请配置 NAT 来代替 PAT。

检查信令消息

要检查信令消息，**inspect sip** 命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspect sip**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route** 接口 **00** 指标 **tunneled** 形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要 **inspect sip** 命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 SIP 检测引擎，该引擎创建类映射来匹配默认端口 (5060) 上的 SIP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 SIP 检测，请使用 **global** 参数代替 **interface outside**。

```
ciscoasa(config)# class-map sip-port
ciscoasa(config-cmap)# match port tcp eq 5060
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sip_policy

ciscoasa(config-pmap)# class sip-port
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sip_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map type inspect sip	为 SIP 创建检查策略图。
show sip	显示通过 ASA 建立的 SIP 会话的相关信息。
show conn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。
tls-proxy	定义 TLS 代理实例并设置最大会话数。

inspect skinny

要启用 SCCP（瘦客户端）应用检测，请在类配置模式下使用 **inspect skinny** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect skinny [skinny_map] [tls-proxyproxy_name] [phone-proxyproxy_name]
no inspect skinny [skinny_map] [tls-proxyproxy_name] [phone-proxyproxy_name]

Syntax Description

phone-proxyproxy_name 为检测会话启用电话代理。

Skinny_map 指定 Skinny 策略映射名称。

tls-proxyproxy_name 为检测会话启用 TLS 代理。

Command Default

默认情况下，SCCP 检测已启用，默认设置如下：

- 注册：未执行。
- 最大消息 ID：0x181。
- 最小前缀长度：4
- 媒体超时：00:05:00
- 信令超时：01:00:00。
- RTP 符合性：未执行。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

8.0(2) 已添加关键 **tls-proxy** 字。

9.4(1) 该关 **phone-proxy** 键字已被弃用。

9.13(1) 该关 **tls-proxy** 键字已被弃用。该关键字将在未来的版本中被删除。

版本 修改

9.14(1) 已删除 **tls-proxy** 关键字，以及对 SCCP/Skinny 加密检测的支持。

使用指南

瘦客户端 (SCCP) 是用于 VoIP 网络的简化协议。使用 SCCP 的思科 IP 电话可共存于 H.323 环境中。与 Cisco CallManager 一起使用时，SCCP 客户端可以与符合 H.323 的终端进行互操作。

对于 SCCP，ASA 支持 PAT 和 NAT。如果要使用的 IP 电话多于 IP 电话可使用的全局 IP 地址，必须进行 PAT。通过支持 SCCP 信令数据包的 NAT 和 PAT，瘦应用检测可确保所有 SCCP 信令和媒体数据包均可通过 ASA。

Cisco CallManager 与思科 IP 电话之间的正常流量使用 SCCP，这些流量由 SCCP 检测处理，无需任何特殊配置。另外，ASA 还支持 DHCP 选项 150 和 66，将 TFTP 服务器的位置发送到思科 IP 电话及其他 DHCP 客户端即可完成操作。思科 IP 电话可能在请求中还包含 DHCP 选项 3（该选项用于设置默认路由）。



注释 ASA 支持检测来自运行 SCCP 协议版本 22 及更早版本的思科 IP 电话的流量。

支持 Cisco IP 电话

在思科 CallManager 位于思科 IP 电话较高安全性接口的拓扑中，如果需要对思科 CallManager IP 地址执行 NAT，则映射必须为静态，因为思科 IP 电话需要在其配置中显式指定思科 CallManager IP 地址。静态身份条目使位于安全性较高的接口的 Cisco CallManager 可以接受来自思科 IP 电话的注册。

Cisco IP 电话需要访问 TFTP 服务器来下载连接到 Cisco CallManager 服务器所需的配置信息。

当思科 IP 电话位于比 TFTP 服务器低的安全接口上时，必须使用 ACL 来与 UDP 端口 69 上的受保护 TFTP 服务器连接。虽然需要对 TFTP 服务器使用静态条目，但该静态条目不一定必须是身份静态条目。使用 NAT 时，身份静态条目会映射到同一 IP 地址。使用 PAT 时，它会映射到同一 IP 地址和端口。

当 Cisco IP 电话位于比 TFTP 服务器和 Cisco CallManager 安全性更高的接口上时，不需要 ACL 或静态条目即可允许 Cisco IP 电话发起连接。

限制和局限性

如果将内部 Cisco CallManager 的地址配置为通过 NAT 或 PAT 指向不同的 IP 地址或端口，则外部 Cisco IP 电话的注册将失败，因为 ASA 当前不支持通过 TFTP 传输文件内容的 NAT 或 PAT。虽然 ASA 支持 TFTP 消息的 NAT 并会为 TFTP 文件打开针孔，但在电话注册期间，ASA 无法转换通过 TFTP 传输的思科 IP 电话配置文件中嵌入的思科 CallManager IP 地址和端口。



注释 ASA 支持 SCCP 呼叫的状态故障转移，但呼叫建立过程中的呼叫除外。

检查信令消息

要检查信令消息，**inspect skinny** 命令通常需要确定媒体终端（例如，IP 电话）的位置。

此信息用于准备媒体流量的访问控制和 NAT 状态，以便以透明方式通过防火墙，而无需手动配置。

在确定这些位置时，命令**inspectskinny**命令会 **not** 使用隧道默认网关路由。隧道默认网关路由是采用 **route**接口 **00**指标 **tunneled**形式的路由。此路由会覆盖 IPsec 隧道传出数据包的默认路由。因此，如果 VPN 流量需要**inspectskinny**命令，请不要配置隧道默认网关路由。请改为使用其他静态路由或动态路由。

CR_Examples

以下示例启用 SCCP 检测引擎，创建类映射以匹配默认端口 (2000) 上的 SCCP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 SCCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map skinny-port
ciscoasa(config-cmap)# match port tcp eq 2000
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map skinny_policy

ciscoasa(config-pmap)# class skinny-port
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy skinny_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-maptypeinspectskinny	为 SCCP 创建检查策略图。
showskinny	显示通过 ASA 建立的 SCCP 会话的相关信息。
showconn	显示不同连接类型的连接状态。
timeout	为不同协议和会话类型设置最大空闲持续时间。
tls-proxy	定义 TLS 代理实例并设置最大会话数。

inspect snmp

要启用 SNMP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect snmp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect snmp [*map_name*]
no inspect snmp [*map_name*]

Syntax Description

map_name SNMP 映射的名称。

Command Default

从 9.14(1) 开始，此命令默认启用。它在以前的版本中默认被禁用。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.14(1)	命令默认已启用，并且 SNMP 映射变为可选项。

使用指南

从 9.14(1) 开始，SNMP 应用程序检查适用于到设备的流量和通过设备的流量。如果您配置的 SNMP v3 将用户限制在特定 SNMP 主机上，则必须进行此检测。如果未检测，定义的用户可以从任何允许的主机轮询设备。默认端口已启用 SNMP 检测，因此只有在使用非默认端口时才需要进行配置。默认端口为 UDP/161、162（适用于所有设备类型）和 UDP/4161（适用于同时运行安全防火墙可扩展操作系统 (FXOS) 的设备），因为 FXOS 在 UDP/161 上监听。

在 9.14(1) 之前的版本中，默认情况下未启用 SNMP 检测，并且它仅适用于通过设备的流量。

SNMP 应用程序检查还允许您将 SNMP 流量限制为特定版本的 SNMP。SNMP 早期版本的安全性较低；因此，安全策略可能要求拒绝使用某些 SNMP 版本。系统可能会拒绝 SNMP 1、2、2c 或 3 版本。要拒绝特定版本的 SNMP，请在您使用 **denyversion** 命令创建的 SNMP 映射中使用 **snmp-map** 命令。配置 SNMP 映射后，您可使用 **inspect snmp** 命令启用映射，然后使用 **service-policy** 命令将其应用到一个或多个接口。

从 9.14(1) 开始，如果您不需要控制版本，只需启用 SNMP 检查而无需地图。在以前的版本中，需要使用映射。

CR_Examples

以下示例识别 SNMP 流量，定义 SNMP 映射，定义策略，启用 SNMP 检测，并将策略应用到外部接口：

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
denyversion	禁止使用特定版本 SNMP 的流量。
snmp-map	定义 SNMP 映射并启用 SNMP 映射配置模式。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect sqlnet

要启用 Oracle SQL*Net 应用检测，请在类配置模式下使用 **inspect sqlnet** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect sqlnet
no inspect sqlnet

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会启用此命令。
默认端口分配为 1521。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

SQL*Net 协议由不同的数据包类型组成，ASA 处理这些数据包类型，以使数据流对于 ASA 两侧的 Oracle 应用程序而言保持一致。

SQL*Net 的默认端口赋值为 1521。这是 Oracle 用于 SQL*Net 的值，但是，该值与结构化查询语言 (SQL) 的 IANA 端口赋值不符。使用该 **class-map** 命令将 SQL*Net 检查应用于一系列端口号。



注释 当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。当启用 SQL*Net 检查时，ASA 充当代理，并将客户端窗口大小从 65000 减少到大约 16000，从而导致数据传输问题。

ASA NAT 所有地址并在数据包中查找为 SQL*Net 版本 1 打开的所有嵌入式端口。

对于 SQL*Net 版本 2，系统将修复紧跟 REDIRECT 数据包且数据长度为零的所有 DATA 或 REDIRECT 数据包。

需要修复的数据包包含以下格式的嵌入式主机/端口地址：

(ADDRESS=(PROTOCOL=tcp) (DEV=6) (HOST=a.b.c.d) (PORT=a))

将不在 SQL*Net 版本 2 TNSFrame 类型（连接、接受、拒绝、重新发送和标记）中扫描 NAT 地址，检测也将不为数据包中的任何嵌入式端口打开动态连接。

如果负载前面是数据长度为零的 REDIRECT TNSFrame 类型，则将在 SQL*Net 版本 2 TNSFrames、Redirect 和 Data 数据包中扫描要打开的端口和 NAT 地址。当数据长度为零的重定向消息通过 ASA 时，将在连接数据结构中设置一个标志，以期望随后的数据或重定向消息被 NAT 并且端口被动态打开。如果前段中的一个 TNS 帧在 Redirect 消息后到达，则会重置标志。

SQL*Net 检测引擎将使用新旧消息的长度差异，重新计算校验和，更改 IP、TCP 长度，并重新调整序列号和确认号。

在所有其他情况下假设使用 SQL*Net 版本 1。系统将在 TNSFrame 类型（连接、接受、拒绝、重新发送、标记、重定向和数据）和所有数据包中扫描端口和地址。地址将被 NAT 并且端口连接将被打开。

CR_Examples

以下示例启用 SQL*Net 检测引擎，该引擎创建类映射以匹配默认端口 (1521) 上的 SQL*Net 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 SQL*Net 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map sqlnet-port
ciscoasa(config-cmap)# match port tcp eq 1521
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sqlnet_policy

ciscoasa(config-pmap)# class sqlnet-port
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sqlnet_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。
showconn	显示不同连接类型的连接状态，包括 SQL*net。

inspect stun

要启用 NAT 会话实用程序 (STUN) 应用检测，请在类配置模式下使用 **inspect stun** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect stun
no inspect stun

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

默认端口分配为 TCP/3478 和 UDP/3478。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.6(2) 添加了此命令。

使用指南

WebRTC 客户端使用 RFC 5389 中定义的 NAT 会话穿越工具 (STUN) 进行基于浏览器的实时通信，因而不需要插件。WebRTC 客户端通常使用云 STUN 服务器获悉它们的公共 IP 地址和端口。WebRTC 使用交互式连接建立 (ICE, RFC 5245) 来验证客户端之间的连接。虽然这些客户端可以使用 TCP 或其他协议，但它们通常使用 UDP。

由于防火墙通常会阻止传出 UDP 流量，所以思科 Spark 等 WebRTC 产品在完成连接时可能会遇到问题。如果两端已确认连接检查，STUN 检测可为 STUN 终端打开针孔并实现基本的 STUN 和 ICE 合规，以便允许进行客户端通信。由此，可避免在访问规则中开放新端口来启用这些应用。

对于默认检测类启用 STUN 检测时，系统会监视 TCP/UDP 端口 3478 中的 STUN 流量。该检测仅支持 IPv4 地址和 TCP/UDP。

STUN 检测在 NAT 方面存在一些局限性。对于 WebRTC 流量，支持静态 NAT/PAT44。由于思科 Spark 不需要针孔，所以 Spark 可以支持其他类型的 NAT。您还可以使用 NAT/PAT64，包括带有 Cisco Spark 的动态 NAT/PAT。

故障转移和集群模式支持 STUN 检查，因为针孔被复制。但是，设备之间不进行事务 ID 的复制。如果设备在收到 STUN 请求后发生故障，并且另一台设备收到 STUN 响应，则该 STUN 响应将被丢弃。

CR_Examples

以下示例启用 STUN 检测作为默认全局检测规则的一部分。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect stun
ciscoasa(config)# service-policy global_policy global
```

Related Commands

命令	说明
class	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。
showconn	显示不同连接类型的连接状态，包括 STUN。
showservice-policyinspectdiameter	显示检查直径策略的状态和统计信息。

inspect sunrpc

要启用 Sun RPC 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 `inspect sunrpc` 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect sunrpc
no inspect sunrpc

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会启用此命令。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

要启用 Sun RPC 应用检测或更改 ASA 侦听的端口，请在策略映射类配置模式下使用 `inspect sunrpc` 命令，也可以在策略映射配置模式下通过使用 **class** 命令访问该模式。要删除配置，请使用此命令 **no** 的形式。

该 **inspect sunrpc** 命令启用或禁用 Sun RPC 协议的应用程序检查。Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可以在系统上的任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，它必须找出该服务正在哪个端口上运行。它通过查询知名端口 111 上的端口映射器进程来实现此目的。

客户端发送服务的 Sun RPC 程序号，并获取返回的端口号。从此时起，客户端程序将其 Sun RPC 查询发送到该新端口。当服务器发出回复时，ASA 会拦截该数据包并在该端口上打开初始 TCP 和 UDP 连接。



注释 不支持 Sun RPC 负载信息的 NAT 或 PAT。

CR_Examples

以下示例启用 RPC 检测引擎，创建类映射以匹配默认端口 (111) 上的 RPC 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 RPC 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map sunrpc-port
ciscoasa(config-cmap)# match port tcp eq 111
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sample_policy
ciscoasa(config-pmap)# class sunrpc-port
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sample_policy interface outside
```

Related Commands

命令	说明
clearconfiguresunrpc_server	删除使用该命令执行的 sunrpc-server 配置。
clearsunrpc-serveractive	清除 Sun RPC 应用程序检查为特定服务（例如 NFS 或 NIS）打开的针孔。
showrunning-configsunrpc-server	显示有关 Sun RPC 服务表配置的信息。
sunrpc-server	允许以面向 Sun RPC 服务（如 NFS 或 NIS）的指定超时创建针孔。
showsunrpc-serveractive	显示为 Sun RPC 服务打开的针孔。EXTE

inspect tftp

要禁用 TFTP 应用检测（如果之前已禁用），请在类配置模式下使用 **inspect tftp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

inspect tftp
no inspect tftp

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会启用此命令。
默认端口分配为 69。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。它取代了已弃用的 **fixup** 命令。

使用指南

简单文件传输协议 (TFTP) 在 RFC 1350 中描述，是一种在 TFTP 服务器和客户端之间读取和写入文件的简单协议。

ASA 检查 TFTP 流量并在必要时动态创建连接和转换，以允许 TFTP 客户端和服务端之间的文件传输。具体来说，检查引擎检查 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。

只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务端之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。

如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

CR_Examples

以下示例启用 TFTP 检测引擎，创建类映射来匹配默认端口 (69) 上的 TFTP 流量。然后，服务策略会被应用到外部接口。要为所有接口启用 TFTP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map tftp-port
```

```
ciscoasa(config-cmap)# match port udp eq 69
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map tftp_policy

ciscoasa(config-pmap)# class tftp-port
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy tftp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect vxlan

要启用虚拟可扩展局域网 (VXLAN) 应用检查，请在类配置模式下使用 **inspectvxlan** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no** 的形式。

inspect vxlan
no inspect vxlan

Syntax Description 此命令没有任何参数或关键字。

Command Default 此命令默认禁用。

默认端口分配是 UDP/4789。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

9.4(1) 添加了此命令。

使用指南

虚拟可扩展局域网 (VXLAN) 检测适用于流经 ASA 的 VXLAN 封装流量。该检测可确保 VXLAN 报头格式符合标准，丢弃所有格式错误的数据包。系统对于将 ASA 用作 VXLAN 隧道终端 (VTEP) 或 VXLAN 网关的流量不执行 VXLAN 检测，因为在解除 VXLAN 数据包封装的正常环节中会执行那些检测。

VXLAN 数据包为 UDP，通常在端口 4789 上。该端口是 default-inspection-traffic 类的一部分，因此您只需将 VXLAN 检查添加到 Inspection_default 全局服务策略规则中即可。或者，也可以使用端口或 ACL 匹配创建一个类。

CR_Examples

以下示例启用 VXLAN 检测作为全局检测默认规则的一部分。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect vxlan
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect waas

要启用 WAAS 应用检测，请在类配置模式下使用 **inspectwaas** 命令。可以从策略图配置模式访问类配置模式。要删除配置，请使用此命令 **no** 的形式。

inspect waas
no inspect waas

Syntax Description 此命令没有任何参数或关键字。

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
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。

CR_Examples

以下示例显示如何在默认检测类上启用 WAAS 应用检测。

```
policy-map global_policy
  class inspection_default
    inspect waas
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。

inspect xdmcp

要启用 XDMCP 应用检测或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect xdmcp** 命令。可以从 map configuration 模式访问 Class configuration 模式。要删除配置，请使用此命令 **no** 的形式。

```
inspect xdmcp
no inspect xdmcp
```

Syntax Description 此命令没有任何参数或关键字。

Command Default 从 9.16 开始，此命令默认是禁用的。在先前版本中，它默认启用。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。它取代了已弃用的 fixup 命令。

使用指南

inspect xdmcp 命令启用或禁用 XDMCP 协议的应用检查。

XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。

为了成功协商和启动 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许反向连接，请使用 **established** ASA 上的命令。一旦 XDMCP 协商好端口来发送显示，就会查 **established** 阅命令来验证是否应该允许这个反向连接。

在 XWindows 会话期间，管理器通过知名端口 6000 | n 与显示器 Xserver 进行通信。由于以下终端设置，每个显示器都与 Xserver 建立单独的连接：

```
setenv DISPLAY Xserver:n
```

其中 *n* 为显示器编号。

使用 XDMCP 时，系统将使用 IP 地址协商显示，以便 ASA 可在需要时应用 NAT。XDCMP 检测不支持 PAT。

CR_Examples

以下示例启用 XDMCP 检测引擎，创建类映射以匹配默认端口 (177) 上的 XDMCP 流量。然后，服务策略会被应用到外部接口。要对所有接口启用 XDMCP 检测，请使用 **global** 参数代替 **interfaceoutside**。

```
ciscoasa(config)# class-map xdmcp-port
ciscoasa(config-cmap)# match port tcp eq 177
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map xdmcp_policy

ciscoasa(config-pmap)# class xdmcp-port
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy xdmcp_policy interface outside
```

Related Commands

命令	说明
class-map	定义要应用的安全操作的流量类。
policy-map	将类映射与特定的安全操作相关联。
service-policy	将策略映射应用到一个或多个接口。



int – ipu

- integrity, 第 159 页
- intercept-dhcp, 第 161 页
- interface (全局), 第 163 页
- interface (vpn load-balancing), 第 166 页
- interface bvi, 第 168 页
- interface loopback, 第 171 页
- interface-policy, 第 173 页
- interface port-channel, 第 175 页
- interface redundant, 第 177 页
- interface tunnel, 第 179 页
- interface vlan, 第 180 页
- interface vni, 第 183 页
- interim-accounting-update, 第 185 页
- internal-password, 第 187 页
- internal-port, 第 189 页
- internal-segment-id, 第 191 页
- interval maximum, 第 193 页
- invalid-ack, 第 195 页
- ip address, 第 197 页
- ip address dhcp, 第 200 页
- ip address pppoe, 第 202 页
- ip-address-privacy, 第 204 页
- ip audit attack, 第 205 页
- ip audit info, 第 207 页
- ip audit interface, 第 209 页
- ip audit name, 第 211 页
- ip audit signature, 第 213 页
- ip-client, 第 218 页
- ip-comp, 第 219 页

- [ip local pool](#)，第 221 页
- [ip unnumbered](#)，第 223 页
- [ip-phone-bypass](#)，第 224 页
- [ips](#)，第 226 页
- [ipsec-udp](#)，第 229 页
- [ipsec-udp-port](#)，第 231 页

integrity

要在 AnyConnect IPsec 连接的 IKEv2 安全关联 (SA) 中指定 ESP 完整性算法，请在 IKEv2 策略配置模式下使用 **integrity** 命令。要删除该命令并使用默认设置，请使用以下命令的 **no** 形式：

```
integrity { md5 | sha | sha256 | sha384 | sha512 | null }  
no integrity { md5 | sha | sha256 | sha384 | sha512 | null }
```

Syntax Description

md5	指定 ESP 完整性保护的 MD5 算法。
null	当指定 AES-GCM 作为加密算法时，允许管理员选择 null 作为 IKEv2 完整性算法。
sha	（默认）指定美国联邦信息处理标准 (FIPS) 中定义的安全散列算法 (SHA) SHA 1，用于 ESP 完整性保护。
sha256	指定具有 256 位摘要的安全散列算法 SHA 2。
sha384	指定具有 384 位摘要的安全散列算法 SHA 2。
sha512	指定具有 512 位摘要的安全散列算法 SHA 2。

Command Default

默认为 **sha**(SHA 1 算法)。

使用指南

IKEv2 SA 是在第 1 阶段使用的密钥，用于使 IKEv2 对等体能够在第 2 阶段安全通信。输入 **crypto ikev2 policy** 命令后，使用 **integrity** 命令为 ESP 协议设置完整性算法。

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

8.4(1) 添加了此命令。

8.4(2) 添加了 **sha256**、**sha384** 和 **sha512** 关键字以提供 SHA 2 支持。

9.0(1) 添加了 **null** 选项作为 IKEv2 完整性算法。

CR_Examples

以下示例进入 IKEv2 策略配置模式并将完整性算法设置为 MD5：

```
ciscoasa(config)# crypto ikev2 policy 1  
ciscoasa(config-ikev2-policy)# integrity md5
```

Related Commands

命令	说明
encryption	为 AnyConnect IPsec 连接指定 IKEv2 SA 中的加密算法。
group	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 群。
lifetime	指定 AnyConnect IPsec 连接的 IKEv2 SA 的 SA 生命周期。
prf	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定伪随机函数。

intercept-dhcp

要启用 DHCP 拦截，请在 **intercept-dhcpenable** 策略组配置模式下使用该命令。要从运行配置中删除 **intercept-dhcp** 属性并允许用户从默认或其他组策略继承 DHCP 拦截配置，请使用此命令的 **no** 形式。

intercept-dhcpnetmask { **enable** | **disable** }
no intercept-dhcp

Syntax Description

disable 禁用 DHCP 拦截。

enable 启用 DHCP 拦截。

网络掩 提供隧道 IP 地址的子网掩码。
码

Command Default

DHCP 拦截已禁用。

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
全局策略配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

要禁用 DHCP 拦截，请使用 **intercept-dhcpdisable** 命令。

如果分割隧道选项超过 255 个字节，则 Microsoft XP 会异常导致域名的损坏。为避免此问题，ASA 将其发送的路由数限制为 27 至 40 条路由，并且路由数取决于路由类。

通过 DHCP 拦截，Microsoft XP 客户端可以将分割隧道与 ASA 配合使用。ASA 直接回复 Microsoft Windows XP 客户端 DHCP Inform 消息，为该客户端提供隧道 IP 地址的子网掩码、域名和无类静态路由。对于 XP 之前的 Windows 客户端，DHCP Intercept 提供域名和子网掩码。这对于不适合使用 DHCP 服务器的环境很有用。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略设置 DHCP 拦截：

```
ciscoasa(config)# group-policy FirstGroup attributes  
ciscoasa(config-group-policy)# intercept-dhcp enable
```

interface（全局）

要配置接口并进入接口配置模式，请在 **interface** 全局配置模式下使用该命令。要删除子接口，请使用此命令的 **no** 形式；在配置管理器 时，您无法删除物理接口或映射接口。

对于物理接口（适用于除 ASASM 之外的所有型号）：

interface*physical_interface*

对于子接口（不适用于 ASA 5505 或 ASASM，或者 ASA 5506-X 到 ASA 5555-X 上的管理接口）：

interface { *physical_interface* | **redundantnumber** | **port-channelnumber** } . *subinterface*
no interface { *physical_interface* | **redundantnumber** | **port-channelnumber** } . *subinterface*

对于分配了映射名称的多情景模式：

interface*mapped_name*

Syntax Description

mapped_name 在多上下文模式下，如果使用命令分配了映射名称，则指定映射名 **allocate-interface** 称。

physical_interface 将物理接口类型、插槽和端口号指定为 *type[slot/]port*。类型和插槽/端口之间的空格是可选的。

物理接口类型包括：

- **ethernet**
- **gigabitethernet**
- **tengigabitethernet**
- **management**

输入类型，后跟插槽/端口，例如， **gigabitethernet0/1**。

管理接口仅用于管理流量。但是，如果需要，也可以将其用于直通流量，具体取决于您的型号（请参阅 **management-only** 命令）。

请参阅相应型号的硬件文档以确定接口类型、插槽和端口号。

subinterface 指定 1 至 4294967293 之间的整数，用于指定逻辑子接口。子接口的最大数量取决于您的 ASA 型号。子接口不适用于 ASA 5505、ASASM，也不适用于 ASA 5512-X 至 ASA 5555-X 上的管理接口。有关每个平台的最大子接口（或 VLAN）数，请参阅配置指南。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。

Command Default

默认情况下，ASA 会为所有物理接口自动生成 **interface** 命令。

在多情景模式下，ASA 会为所有分配到情景的接口使用 **allocate-interfaceinterface** 命令自动生成] 命令。

接口的默认状态取决于类型和上下文模式：

- 多上下文模式，上下文——所有分配的接口都默认启用，无论接口在系统执行空间中的状态如何。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。
- 单模式或多情景模式，系统 - 接口具有以下默认状态：
 - 物理接口 - 已禁用。
 - 子接口——已启用。但是，要使流量通过子接口，还必须启用物理接口。

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	• 支持

Command History

版本	修改
7.0(1)	修改了此命令以允许使用新的子接口命名约定，并将参数更改为接口配置模式下单独的命令。

使用指南

在接口配置模式下，可以配置硬件设置（物理接口）、分配名称、分配 VLAN、分配 IP 地址，并配置许多其他设置，具体取决于接口类型和安全情景模式。

对于启用已启用接口来传递流量，请配置以下接口配置模式命令：**nameif**，对于路由模式，配置**ipaddress**。对于子接口，还需配置**vlan** 命令。

如果您更改接口设置，并且不想等待现有连接超时后再使用新的安全信息，则可以使用该命令清除连**clearlocal-host** 接。

ASA 5512-X 到 ASA 5555-X 上的 Management 0/0 接口具有以下特征：

- 不支持直通流量
- 不支持子接口
- 不支持优先级队列
- 不支持组播 MAC
- IPS SSP软件模块共享管理0/0接口。ASA 和 IPS 模块支持单独的 MAC 地址和 IP 地址。您必须在 IPS 操作系统内执行 IPS IP 地址的配置。但是，物理特性（例如启用接口）在 ASA 上配置。

CR_Examples

以下示例在单模式下配置物理接口的参数：


```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

以下示例在单模式下配置子接口的参数：

```
ciscoasa(config)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

以下示例在多情景模式下配置用于系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配到 contextA：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# no shutdown
ciscoasa(config-subif)# context contextA
ciscoasa(config-ctx)# ...
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

以下示例以多上下文模式配置上下文配置的参数：

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

Related Commands

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
member-interface	将接口分配给冗余接口。
clearinterface	清除命令的计数 showinterface 器。
showinterface	显示接口的运行时间状态和统计信息。
vlan	为子接口分配 VLAN。

interface (vpn load-balancing)

要在 VPN 负载均衡虚拟集群中为 VPN 负载均衡指定非默认公共或专用接口，请在 vpn load-balancing 模式下使用 **interface**命令。要删除接口规范并恢复为默认接口，请使用此命令的 **no** 形式。

```
interface { lbprivate | lbpublic } interface-name
interface { lbprivate | lbpublic }
```

Syntax Description	<i>interface-name</i> 要配置为 VPN 负载均衡集群的公共或专用接口的接口的名称。
lbprivate	指定此命令配置 VPN 负载均衡的专用接口。
lbpublic	指定此命令为 VPN 负载均衡配置公共接口。

Command Default 如果省略 **interface** 命令，则 **lbprivate** 接口默认为 **inside**，**lbpublic** 接口默认为 **outside**。

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 load-balancing	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南 首先，必须已使用 **vpnload-balancing**命令进入 vpn load-balancing 配置模式。

此外，之前还必须使用过 **interface**、**ipaddress** 和 **nameif** 命令来配置和分配名称到您在此命令中指定的接口。

CR_Examples 以下是命令序列的示例，其 **vpnload-balancing** 中包括一个命令，该命令 **interface** 将集群的公共接口指定为“测试”，并将集群的私有接口恢复为默认值（内部）：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
```

```
ciscoasa(config-load-balancing)# interface lbpublic test  
ciscoasa(config-load-balancing)# nointerface lbprivate  
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224  
ciscoasa(config-load-balancing)# participate
```

```
ciscoasa(config-load-balancing)# participate
```

Related Commands

命令	说明
vpnload-balancing	进入 vpn 负载均衡配置模式。

interface bvi

要为网桥组配置网桥虚拟接口 (BVI)，请在全局配置模式下使用**interface bvi** 命令。要删除 BVI 配置，请使用此命令 **no** 的形式。

```
interface bvi bridge_group_number
no interface bvi bridge_group_number
```

Syntax Description	bridge_group_number 将网桥组编号指定为介于 1 和 100 之间的整数；对于 9.3(1) 及更高版本，范围扩大到 1 到 250 之间。

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	• 支持	—

Command History	版本 修改
	8.4(1) 添加了此命令。
	9.3(1) 编号范围扩大到 1 到 250，以支持 250 个 BVI。
	9.6(2) 每个网桥组的最大接口数量已从 4 增加到 64。

使用此命令可进入接口配置模式，以便为您的网桥组配置管理 IP 地址。如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组的流量与其他网桥组是分离的；流量不会路由至 ASA 中的另一个网桥组，并且流量必须退出 ASA 后才能通过外部路由器路由回 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。每个情景或在单模式下至少需要一个网桥组。

每个网桥组都需要一个管理 IP 地址。ASA 使用该 IP 地址作为源自网桥组的数据包的源地址。管理 IP 地址必须与已连接网络位于同一子网上。对于 IPv4 流量，需要管理 IP 地址来传递任何流量。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。对于另一种管理方法，您可以独立于任何网桥组配置管理接口。

对于 9.2 及更早版本，您可以在单模式下或多模式下的每个情景配置最多 8 个网桥组；对于 9.3(1) 及更高版本，最多可以配置 250 个网桥组。每个网桥组可包括最多 4 个接口。在 9.6(2) 及更高版本中，您可以向一个网桥组添加最多 64 个接口。您不能将同一接口分配至多个网桥组。请注意，您必须至少使用 1 个网桥组；数据接口必须属于网桥组。



注释 尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。



注释 对于单独的 management 接口，不可配置的桥组 (ID 301) 会自动添加至您的配置。此网桥组未包含在网桥组限制中。



注释 ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址位于同一网络上的流量。

CR_Examples

以下示例包括两个桥接组，每个组有三个接口，外加一个仅管理接口：

```
interface gigabitethernet 0/0
nameif inside
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside
security-level 0
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
nameif inside
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
nameif dmz
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
```

```
interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

Related Commands

命令	说明
ace/bvi	清除桥虚拟接口配置。
bridge-group	将透明防火墙接口分组到桥接组中。
interface	配置接口。
ipaddress	设置桥组的管理IP地址。
show bridge-group	显示网桥组信息，包括成员接口和IP地址。
显示运行配置接口 bvi	显示该桥组接口配置。

interface loopback

要创建环回接口，请在 **interface loopback** 全局配置模式下使用该命令。使用命令 **no** 的形式删除环回接口。

interface loopback 编号
no interface loopback number

Command Default

无默认为行为或值。

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	—

使用指南

环回接口是一种会模拟物理接口的纯软件接口。环回接口可通过多个物理接口来访问。您只能将环回接口用于传入/传出设备的流量。

以下功能支持环回接口：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- 系统日志
- Telnet
- VTI 源接口

Command History

版本	修改

9.18(2)	添加了此命令。

9.19(1)	添加了对 VTI 的支持。

版本 修改

920(1) 增加了对 DNS、HTTP 和 ICMP 的支持。

CR_Examples

以下示例创建新的环回接口：

```
ciscoasa(config)# interface loopback 10
```

Related Commands

命令	说明
tunnelsourceinterface	指定用于创建 VTI 隧道的源接口。
ssh	为接口配置 SSH。
logging host	指定系统日志主机。
neighbor update-source	将接口配置为 BGP 邻居的源。
snmp-server host	指定 SNMP 服务器。
telnet	为接口配置 Telnet。

interface-policy

要指定在监控功能检测到接口故障时的故障转移策略，请在故障转移组配置模式下使用 **interface-policy** 命令。要恢复默认值，请使用此 **no** 命令的形式。

```
interface-policy num [ % ]
no interface-policy num [ % ]
```

Syntax Description	num 使用百分比形式时，指定 1 到 100 之间的数字，或者 1 到最大接口数。
	% （可选）指定 number num 是受监控接口的百分比。

Command Default	如果为设备配置了 failover interface-policy 命令，则 interface-policy failovergroup 命令的默认值采用该值。如果不是，则 num 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
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 num 参数和可选的 % 关键字之间没有空格。

如果故障接口的数量符合配置的策略且另一台 ASA 正常运行，则此 ASA 会将自身标记为发生故障，并且可能发生故障转移（如果是主用 ASA 发生故障）。只有通过 **monitor-interface** 命令指定为监控的接口才会计入策略。

CR_Examples 以下部分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)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failoverinterface-policy	配置接口监控策略。
monitor-interface	指定正在监控故障转移的接口。

interface port-channel

要配置 EtherChannel 接口并进入接口配置模式，请在 **interfaceport-channel** 全局配置模式下使用该命令。要删除 EtherChannel 接口，请使用此命令 **no** 的形式。

interfaceport-channel编号
no interface port-channelnumber

Syntax Description

number 指定 EtherChannel 通道组 ID，介于 1 和 48 之间。在将接口添加到通道组时，将自动创建此接口。如果尚未添加接口，则此命令会创建端口通道接口。

注释
您需要向端口通道接口添加至少一个成员接口，然后才能为其配置逻辑参数（例如名称）。

Command Default

默认情况下，端口通道接口已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。

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	• 支持

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

对于启用已启用接口来传递流量，请配置以下接口配置模式命令：**nameif**，对于路由模式，配置 **ipaddress**。

如果您更改接口设置，并且不想等待现有连接超时后再使用新的安全信息，则可以使用该命令清除连 **clearlocal-host** 接。



注释 ASA 5505 或 ASASM 不支持此命令。您不能将 4GE SSM 上的接口（包括 ASA 5550 上插槽 1 中的集成 4GE SSM）用作 EtherChannel 的一部分。

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例将三个接口配置为 EtherChannel 的一部分。此示例还将系统优先级设置为较高的优先级，并在 EtherChannel 分配有超过 8 个接口的情况下将千兆以太网 0/2 的优先级设置为高于其他接口。

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

interface redundant

要配置冗余接口并进入接口配置模式，请在 **interfaceredundant** 全局配置模式下使用该命令。要删除冗余接口，请使用此命令 **no** 的形式。

interface redundant 编号
no interface redundant number

Syntax Description *number* 指定介于 1 和 8 之间的逻辑冗余接口 ID。 **redundant** 和 ID 之间的空格是可选的。

Command Default 默认情况下，冗余接口已启用。但是，要使流量通过冗余接口，还必须启用成员物理接口。

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	• 支持

Command History 版本 修改

8.0(2) 添加了此命令。

使用指南

冗余接口是将活动物理接口和备用物理接口配对（参见 **member-interface** 命令）。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。

所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

对于启用已启用接口来传递流量，请配置以下接口配置模式命令： **nameif**，对于路由模式，配置 **ipaddress**。

如果您更改接口设置，并且不想等待现有连接超时后再使用新的安全信息，则可以使用该命令清除连接 **clearlocal-host** 接。



注释 ASA 5505 或 ASASM 不支持此命令。

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

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	将物理接口分配给冗余接口。
redundant-interface	更改活动成员接口。
showinterface	显示接口的运行时间状态和统计信息。

interface tunnel

要创建新的 VTI 隧道接口，请使用全 **interface tunnel** 局配置模式下的命令。使用该命令的no形式删除VTI隧道接口。

interface tunnel编号
no interface tunnelnumber

Syntax Description

number 为隧道接口分配编号。该值可以是0-1024之间的任意值。

Command Default

无默认为行为或值。

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	• 否	• 是	• 否	• -

Command History

版本	修改
9.7(1)	引入了此命令及其子模式。
9.16 (1)	每设备支持的隧道接口数量从100增加到1024。

CR_Examples

以下示例创建新的隧道接口：

```
ciscoasa(config)# interface tunnel 10
```

Related Commands

命令	说明
tunnelsourceinterface	指定用于创建 VTI 隧道的源接口。
tunneldestination	指定 VTI 隧道目标的 IP 地址。
tunnelmode	指定将 IPsec 用于隧道保护。
tunnelprotectionipsec	指定将用于隧道保护的 IPsec 配置文件。

interface vlan

对于 ASA 5505 和 ASASM，要配置 VLAN 接口并进入接口配置模式，请在 **interfacevlan** 全局配置模式下使用该命令。要删除 VLAN 接口，请使用此命 **no** 令的形式。

interface vlan编号
no interface vlannumber

Syntax Description

number 指定 VLAN ID。

对于 ASA 5505，请使用介于 1 和 4090 之间的 ID。默认情况下，会在 VLAN 1 上启用 VLAN 接口 ID。

对于 ASASM，请使用介于 2 到 1000(1025 到 4094) 之间的 ID。

Command Default

默认情况下，VLAN 接口处于启用状态。

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	• 支持

Command History

版本 修改

7.2(1) 添加了此命令。

8.4(1) 已添加 ASASM 支持。

使用指南

对于 ASASM，您可以将任何 VLAN ID 添加到配置中，但只有交换机分配给 ASA 的 VLAN 才能传递流量。要查看分配给 ASA 的所有 VLAN，请使用该 **showvlan**命令。如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为启动状态。有关接口状态的 **showinterface** 更多信息，请参阅命令。

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

对于启用已启用接口来传递流量，请配置以下接口配置模式命令：**nameif**，对于路由模式，配置 **ipaddress**。对于 ASA 5505 交换机物理接口，请使用**switchportaccessvlan** 命令将物理接口分配给 VLAN 接口。

如果您更改接口设置，并且不想等待现有连接超时后再使用新的安全信息，则可以使用该命令清除连 **clearlocal-host** 接。

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例配置三个 VLAN 接口。第三个家庭接口无法将流量转发到工作接口。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

以下示例配置五个 VLAN 接口，包括使用 **failoverlan** 命令单独配置的故障转移接口：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
```

```

ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown

```

Related Commands

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
clearinterface	清除命令的计数 showinterface 器。
showinterface	显示接口的运行时间状态和统计信息。

interface vni

要配置 VXLAN 网络标识符 (VNI) 接口并进入接口配置模式，请在 **interfacevni** 全局配置模式下使用该命令。要删除 VNI 接口，请使用此命令 **no** 的形式。

interface vni编号
no interface vninumber

Syntax Description

number 将 ID 设置在 1 至 10000 之间。此 ID 仅为内部接口标识符。

Command Default

无默认为行为或值。

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

94(1) 添加了此命令。

使用指南

您必须使用 **vtep-nve** 命令将 VNI 接口与 VTEP 源接口相关联。您还必须将 **VXLANsegment-id**。

CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并将 VNI 1 接口与其关联：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

interim-accounting-update

要为 AAA 服务器组启用 RADIUS 临时记帐更新消息的生成，请在 `aaa-server group` 配置模式下使用 `interim-accounting-update` 命令。要禁用临时记账更新消息，请使用此命令的 **no** 形式。

interim-accounting-update [**periodic** *hours*]
no interim-accounting-update [**periodic** *hours*]

Syntax Description

periodic [*hours*] （可选）为每个配置为向相关服务器组发送会计记录的 VPN 会话启用定期生成和传输会计记录。可以选择包括发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。

将此选项用于为 ISE 身份验证更改配置的服务器组。

Command Default

默认情况下，不启用 `interim-accounting-update`。

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 group 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.2(1) 添加了 **periodic** 关键字。

使用指南

如果使用不带 **periodic** 关键字的此命令，则 ASA 仅会在将 VPN 隧道连接添加到无客户端 VPN 会话时发送临时审计更新消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。

如果要使用服务器组为远程访问 VPN 配置 ISE 授权更改，请添加 **periodic** 关键字。周期报告包括 AnyConnect 连接以及无客户端会话。

ISE 将基于其从 NAS 设备（如 ASA）收到的记帐记录，保留一个活动会话的目录。但是，如果 ISE 在 5 天内没有收到任何表明会话仍然处于活动状态（会计消息或姿态交易）的迹象，它将从其数据库中删除该会话记录。为了确保长期 VPN 连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记帐更新消息。

CR_Examples

以下示例显示如何为动态授权 (CoA) 更新和每小时定期记帐配置 ISE 服务器组。其中包括使用 ISE 配置密码身份验证的隧道组配置。

```

ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit

```

以下示例显示如何使用ISE为本地证书验证和授权配置隧道组。在这种情况下，您将该命令包含在 **authorize-only** 服务器组配置中，因为服务器组将不会用于身份验证。

```

ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit

```

Related Commands

命令	说明
authorize-only	为RADIUS服务器组启用仅授权模式。
dynamic-authorization	启用RADIUS服务器组的动态授权。

internal-password

要在无客户端 SSL VPN 门户页面上显示额外的密码字段，请在 **webvpn** 配置模式下使用 **internal-password** 命令。ASA 使用该附加密码对允许 SSO 的文件服务器的用户进行身份验证。

要禁用使用内部密码的功能，请使用此命令的 **no** 版本。

internal-passwordenable
no internal password

Syntax Description

enable 启用内部密码。

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
Webvpn 配置	• 是	—	• 是	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

使用指南

如果启用此选项，最终用户在登录无客户端 SSL VPN 会话时将键入第二个密码。无客户端 SSL VPN 服务器使用 HTTPS 向身份验证服务器发送包含用户名和密码的 SSO 身份验证请求。如果身份验证服务器批准身份验证请求，它会向无客户端 SSL VPN 服务器返回 SSO 身份验证 cookie。ASA 会代表用户保留此 Cookie 并将其用于对用户进行身份验证，以确保受 SSO 服务器保护的域内的网站安全。

如果要求内部密码与 SSL VPN 密码不同，则内部密码功能非常有用。特别是，可以使用一次性密码对 ASA 进行身份验证，对内部站点使用其他密码。

CR_Examples

以下示例显示如何启用内部密码：

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

```
internal password enable
ciscoasa(config-webvpn) #
```

Related Commands

命令	说明
webvpn	进入 webvpn 配置模式，在此模式下配置无客户端 SSL VPN 连接的属性。

internal-port

要为 Azure 上的 ASA Virtual 的 VNI 接口指定 VXLAN 内部端口，请在接口配置模式下使用 **internal-port** 命令。要删除端口，请使用此命令 **no** 的形式。

internal-port 端口

no internal-port 端口

Syntax Description

port 将端口设置在 1024 和 65535 之间。

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.19(1) 添加了此命令。

使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

命令	说明
debug vxlan	调试 VXLAN 流量。
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
external-port	设置外部 VXLAN 端口。
external-segment-id	指定 VNI 接口的 VXLAN 外部段 ID。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
internal-segment-id	指定 VNI 接口的 VXLAN 内部段 ID。
nve	指定网络虚拟化终端实例。
peer ip	手动指定对等 VTEP IP 地址。
proxy paired	将接口设置为配对代理模式。
show interface vni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show nve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

internal-segment-id

要为 Azure 上网关负载均衡器 (GWLb) 指定 ASA Virtual 的 VNI 接口的 VXLAN 内部网段 ID，请在接口配置模式下使用 **internal-segment-id** 命令。要删除 ID，请使用此命令 **no** 的形式。

internal-segment-id *id*
no internal-segment-id *id*

Syntax Description

D 将 ID 设置在 1 至 16777215 之间。

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.19(1) 添加了此命令。

使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

命令	说明
debug vxlan	调试 VXLAN 流量。

命令	说明
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
external-port	设置外部 VXLAN 端口。
external-segment-id	指定 VNI 接口的 VXLAN 外部段 ID。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
internal-port	设置内部 VXLAN 端口。
nve	指定网络虚拟化终端实例。
peer ip	手动指定对等 VTEP IP 地址。
proxy paired	将接口设置为配对代理模式。
show interface vni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show nve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

interval maximum

如要配置 DDNS 更新方法所尝试更新的最大间隔，请在 DDNS-update-method 模式下使用 **interval** 命令。要从运行配置中删除 DDNS 更新方法的间隔，请使用此命令的 **no** 形式。

天 小 **interval maximum** 时分钟 秒

天 小 **no interval maximum** 时分钟 秒

Syntax Description

天数 指定更新尝试之间的天数，范围为 0 至 364。

hours 指定更新尝试之间的间隔小时数，范围为 0 到 23。

分钟 指定更新尝试之间的分钟数，范围为 0 到 59。

seconds 指定更新尝试之间间隔的秒数，范围为 0 到 59。

Command Default

无默认为或值。

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
Ddns-update-method 配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

使用指南

将天、小时、分钟和秒相加得到总间隔。

CR_Examples

以下示例将名为 ddns-2 的方法配置为每隔 3 分 15 秒尝试一次更新：

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

Related Commands

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。

命令	说明
ddnsupdate	将 DDNS 更新方法与 ASA 接口或 DDNS 更新主机名关联。
ddns更新方法	创建一个用于动态更新 DNS 资源记录的方法。
dhcp-clientupdatedns	配置 DHCP 客户端传递给 DHCP 服务器的更新参数。
dhcpd 更新 dns	启用 DHCP 服务器来执行 DDNS 更新。

invalid-ack

要设置具有无效 ACK 的数据包的操作，请在 `tcp-map` 配置模式下使用 `invalid-ack` 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。

invalid-ack { allow | drop }
no invalid-ack

Syntax Description

allow 允许具有无效 ACK 的数据包。

drop 丢弃具有无效 ACK 的数据包。

Command Default

默认操作是丢弃具有无效 ACK 的数据包。

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
Tcp-map 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(4)/8.0(4)	添加了此命令。

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。
 1. **invalid-ack**— 在 `tcp-map` 配置模式下，可以输入 `invalid-ack` 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。
 1. **—class** 确定您想要执行操作的类映射。
 2. **setconnectionadvanced-options-** 标识您创建的 TCP 映射。
4. **service-policy-** 向接口或全局分配策略映射。

可能会在以下实例中看到无效 ACK：

- 在 TCP 连接 SYN-ACK 已接收状态下，如果已接收的 TCP 数据包的 ACK 号与正在发送的下一个 TCP 数据包的序列号不完全相同，则是无效 ACK。
- 如果已收到 TCP 数据包的 ACK 号大于发送的下一个 TCP 数据包的序列号，则为无效 ACK。



注释 对于 WAAS 连接，系统自动允许包含无效 ACK 的 TCP 数据包。

CR_Examples

以下示例将 ASA 设置为允许具有无效 ACK 的数据包：

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
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。

ip address

要为接口（在路由模式下）或网桥虚拟接口 (BVI)（路由模式或透明模式）设置 IP 地址，请在接口配置模式下使用 **ipaddress** 命令。要删除 IP 地址，请使用此命令 **no** 的形式。

ip address*ip_address* [*掩码*] **standby***ip_address* | **cluster-pool**池名称]
no ip address [*ip_address*]

Syntax Description

cluster-pool*poolname* （可选）对于 ASA 集群，设置 **iplocalpool** 命令定义的集群地址池。由 *ip_address* 参数定义的主集群 IP 地址仅属于当前主设备。每个集群成员都会从此池中收到一个本地 IP 地址。

您无法提前确定分配给每个单元的确切地址；要查看每个单元使用的地址，请输入 **showiplocalpool***poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。该 ID 决定了池中使用的本地 IP。

ip_address 接口的 IP 地址。

mask （可选）IP 地址的子网掩码。如果不设置掩码，ASA 将使用 IP 地址类的默认掩码。

standby*ip_address* （可选）对于故障转移，设置备用设备的 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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 对于路由模式，此命令已从全局配置命令更改为接口配置模式命令。

8.4(1) 对于透明模式，添加了桥接组。您现在为 BVI 设置 IP 地址，而不是全局 IP 地址。

9.0(1) 添加 **cluster-pool**关键字是为了支持 ASA 集群。

9.7(1) 对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。

使用指南

此命令还设置用于故障转移的备用设备地址。

多上下文模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一的子网上。在多情景模式下，如果此接口位于共享接口上，则每个 IP 地址必须唯一，但在同一子网上。如果接口是唯一的，则此 IP 地址可以在需要时由其他情景使用。

透明防火墙指南

透明防火墙不参与 IP 路由。如果要设置 BVI 地址，则只需对 ASA 进行 IP 配置。需要此地址是因为 ASA 使用此地址作为源自 ASA 的流量（例如系统消息或与 AAA 服务器的通信）的源地址。您还可以使用此地址进行远程管理访问。此地址必须与上游和下游路由器位于同一子网上。对于多情景模式，在每个情景内设置管理 IP 地址。对于包含管理接口的型号，您还可以为此接口设置 IP 地址以进行管理。

故障转移指南

备用 IP 地址必须与主 IP 地址位于同一子网。

ASA 集群指南

只有将集群接口模式配置为单个接口（**cluster-interface mode individual** 命令），才能为单个接口设置集群池。唯一的例外情况是仅管理接口：

- 您始终可以将仅管理接口配置为单独的接口，即使在跨网以太网通道模式下也是如此。即使在透明防火墙模式下，管理接口也可以是单独的接口。
- 在跨网以太网通道模式下，如果将管理接口配置为单独接口，则无法为管理接口启用动态路由。您必须使用静态路由。

/31 子网准则

对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

- 31-bit Subnet and Clustering - 可以为跨区以太网通道使用 31 位子网掩码。单个接口（包括跨区以太网通道模式下的管理 IP 地址）不支持 31 位子网。您也不能将 31 位子网用于集群控制链路。
- 31 位子网和故障转移 - 对于故障转移，当您使用 31 位子网作为 ASA 接口 IP 地址时，您无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障切换的接口应有一个备用 IP 地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用 IP 地址，ASA 无法执行任何网络测试；只能跟踪链路状态。对于故障切换和可选的独立状态链路（点对点连接），也可以使用 31 位子网。
- 31 位子网和管理 - 如果您有一个直接连接的管理站，则可以使用点对点连接在 ASA 上使用 SSH 或 HTTP，或者在管理站上使用 SNMP 或 Syslog。
- 31 位子网不支持的功能 - 以下功能不支持 31 位子网：

- 桥接组的 BVI 接口 - 桥接组至少需要 3 个主机地址：BVI 和连接到两个桥接组成员接口的两个主机。您必须使用 /29 子网或更小的子网。
- 组播路由

CR_Examples

以下示例设置两个接口的 IP 地址和备用地址：

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

以下示例设置网桥组 1 的管理地址和备用地址：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ipaddressdhcp	设置接口以从 DHCP 服务器获取 IP 地址。
showipaddress	显示分配给接口的 IP 地址。

ip address dhcp

要使用 DHCP 为接口获取 IP 地址，请在接口配置模式下使用 **ipaddressdhcp** 命令。要为此接口禁用 DHCP 客户端，请使用此命令的 **no** 形式。

ip address dhcp [**setroute**]
no ip address dhcp

Syntax Description **setroute** （可选）允许 ASA 使用 DHCP 服务器提供的默认路由。

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
接口配置	• 是	—	• 是	• 支持	—

Command History 版本 修改

7.0(1) 此命令已从全局配置命令更改为接口配置模式命令。您还可以在任何接口上启用此命令，而不是仅在外部接口上启用。

使用指南 重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入命令之前没有使用该 **noshutdown**命令启用接 **ipaddressdhcp**口，则某些 DHCP 请求可能不会被发送。



注释 ASA 将拒绝超时时间小于 32 秒的任何租用。

CR_Examples 以下示例在 Gigabitethernet0/1 接口上启用 DHCP：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ipaddress	设置该接口的 IP 地址或设置一个透明防火墙的管理 IP 地址。
showipaddressdhcp	显示从 DHCP 服务器获取的 IP 地址。

ip address pppoe

要启用 PPPoE，请在 **ipaddresspppoe**接口配置模式下使用该命令。要禁用 PPPoE，请使用此命 **no** 令的形式。

```
ip address [ ip_address [ mask ] ] pppoe [ setroute ]
no ip address [ ip_address [ mask ] ] pppoe
```

Syntax Description	<i>ip_address</i> 手动设置 IP 地址，而不是从 PPPoE 服务器接收地址。
	<i>mask</i> 指定 IP 地址的子网掩码。如果不设置掩码，ASA 将使用 IP 地址类的默认掩码。
	setroute 让 ASA 使用 PPPoE 服务器提供的默认路由。如果 PPPoE 服务器不发送默认路由，则 ASA 将创建一个以访问集中器地址作为网关的默认路由。

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
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 PPPoE 将以太网和 PPP 两个广泛接受的标准结合在一起，可提供将 IP 地址分配至客户端系统的身份验证方法。ISP 部署 PPPoE 的原因在于，PPPoE 支持使用其现有远程访问基础设施进行高速宽带访问，同时也更加便于客户使用。

在使用 PPPoE 设置 IP 地址之前，配置 **vpdn** 命令以设置用户名、密码和身份验证协议。如果在多个接口上启用此命令（例如通往 ISP 的备份链路），则如有必要，可以使用 **pppoe client vpdn group** 命令将每个接口分配到不同的 VPDN 组。

最大传输单位 (MTU) 大小会自动设置为 1492 字节，这是允许在以太网帧内进行 PPPoE 传输的正确值。

重新输入此命令以重置并重新启动 PPPoE 会话。

不能与 **ipaddress** 命令或 **ipaddressdhcp** 命令同时设置此命令。

CR_Examples

以下示例在 Gigabitethernet 0/1 接口上启用 PPPoE:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

以下示例手动设置 PPPoE 接口的 IP 地址:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ip address	设置接口的 IP 地址。
pppoe 客户端 vpdn 组	将此接口分配给特定 VPDN 组。
show ip address pppoe	显示从 PPPoE 服务器获取的 IP 地址。
vpdn group	创建 vpdn 组并配置 PPPoE 客户端设置。

ip-address-privacy

要启用 IP 地址隐私，请在参数配置模式下使用 **ip-address-privacy**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。

ip-address-privacy
no ip-address-privacy

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
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

以下示例显示如何在 SIP 检测策略映射中启用 SIP IP 地址隐私：

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

Related Commands

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

ip audit attack

要为匹配攻击签名的数据包设置默认操作，请在全局配置模式下使用 **ipauditattack** 命令。要恢复默认操作（重置连接），请使用此命令的 **no** 形式。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit attack

Syntax Description

action （可选）指定您正在定义一组默认操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果您未输入 **action** 关键字，ASA 会假定您已输入该关键字，并且 **action** 关键字会显示在配置中。

alarm （默认）生成一条系统消息，显示数据包与签名匹配。

drop （可选）丢弃数据包。

reset （可选）丢弃数据包并关闭连接。

Command Default

默认操作是发送 并发出警报。

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。

使用指南

您可以指定多个操作，或不指定任何操作。使用 **ipauditname** 命令配置审核策略时，可以覆盖使用此命令设置的操作。如果不在 **ipauditname** 命令中指定操作，则使用使用此命令设置的操作。

有关签名列表，请参阅 **ipauditsignature** 命令。

CR_Examples

以下示例将匹配攻击签名的数据包的默认操作设置为“警报”和“重置”。内部接口的审核策略会将此默认设置覆盖为仅警报，而外部接口的策略使用通过 **ipauditattack** 命令设置的审核策略。

```
ciscoasa(config)# ip audit attack action alarm reset
```

```
ciscoasa(config)# ip audit name insidepolicy attack action alarm
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

命令	说明
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauidsignature	禁用签名。
showrunning-configipauidattack	显示命令的 ipauditattack配置。

ip audit info

要为匹配信息签名的数据包设置默认操作，请在全局配置模式下使用 **ipauditinfo** 命令。要恢复默认操作（生成警报），请使用此命令的 **no** 形式。您可以指定多个操作，或不指定任何操作。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit info

Syntax Description

action （可选）指定您正在定义一组默认操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果您未输入 **action** 关键字，ASA 会假定您已输入该关键字，并且 **action** 关键字会显示在配置中。

alarm （默认）生成一条系统消息，显示数据包与签名匹配。

drop （可选）丢弃数据包。

reset （可选）丢弃数据包并关闭连接。

Command Default

默认操作是生成警报。

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。

使用指南

使用 **ipauditname** 命令配置审核策略时，可以覆盖使用此命令设置的操作。如果不在 **ipauditname** 命令中指定操作，则使用使用此命令设置的操作。

有关签名列表，请参阅 **ipauditsignature** 命令。

CR_Examples

以下示例将与信息性签名匹配的数据包的默认操作设置为警报和重置。内部接口的审核策略将将此默认设置覆盖为警报和丢弃，而外部接口的策略使用通过 **ipauditinfo** 命令设置的默认设置。

```
ciscoasa(config)# ip audit info action alarm reset
```

```
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauditsignature	禁用签名。
showrunning-configipauditinfo	显示命令的 ipauditinfo 配置。

ip audit interface

要将审核策略分配到接口，请在全局配置模式下使用 **ipauditinterface** 命令。要从接口中删除策略，请使用此命 **no** 令的形式。

ip audit interface *interface_name* *policy_name*
no ip audit interface *interface_name* *policy_name*

Syntax Description

interface_name 指定接口名称。

policy_name 使用 **ipauditname** 命令添加的策略的名称。您可以向每个接口分配信息策略和攻击策略。

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	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

CR_Examples

以下示例将审核策略应用于内部和外部接口：

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。

命令	说明
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauditsignature	禁用签名。
showrunning-configipauditinterface	显示命令的 ipauditinterface 配置。

ip audit name

要创建命名的审核策略来标识在数据包与预定义的攻击签名或信息签名匹配时要采取的操作，请在全局配置模式下使用 **ipauditname** 命令。要删除该策略，请使用此命令的形式 **no**。

```
ip audit name name {info | attack} [action [alarm] [drop] [reset]]
no ip audit name name {info | attack} [action [alarm] [drop] [reset]]
```

Syntax Description

action	（可选）指定您正在定义一组操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果不输入 action 关键字，则 ASA 使用 ipauditattack 和 ipauditinfo 命令设置的默认操作。
alarm	（可选）生成一条系统消息，显示数据包与签名匹配。
attack	为攻击签名创建审核策略；则该数据包可能是网络攻击的一部分，例如 DoS 攻击或非法 FTP 命令。
drop	（可选）丢弃数据包。
info	为信息签名创建审核策略；该数据包当前并未攻击您的网络，但可能是信息收集活动的一部分，例如端口扫描。
name	设置策略的名称。
reset	（可选）丢弃数据包并关闭连接。

Command Default

如果不使用 **ipauditattack** 和 **ipauditinfo** 命令更改默认操作，则针对攻击签名和信息签名的默认操作是生成警报。

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。

使用指南

签名是与已知攻击模式匹配的活动。例如，存在与 DoS 攻击匹配的签名。要应用策略，请使用 **ipauditinterface** 命令将其分配到接口。您可以向每个接口分配信息策略和攻击策略。

有关签名列表，请参阅**ipauditsignature** 命令。

如果流量与签名匹配，并且您要针对该流量执行操作，请使用 **shun** 命令防止来自违规主机的新连接，并禁止来自任何现有连接的数据包。

CR_Examples

以下示例设置内部接口的审核策略，以针对攻击和信息签名生成警报，而外部接口的策略重置攻击连接：

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditsignature	禁用签名。
shun	阻止具有特定源和目标地址的数据包。

ip audit signature

要禁用审核策略的签名，请在全局配置模式下使用 **ipauditsignature** 命令。要重新启用签名，请使用此命令的 **no** 形式。

ip audit signature*signature_number***disable**
no ip audit signature签名编号

Syntax Description

disable 禁用签名。

签名编号 指定要禁用的签名编号。有关支持的签名列表，请参阅表 3-1。
号

Command Default

无默认为行为或值。

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

7.0(1) 添加了此命令。

使用指南

如果合法流量持续匹配签名，并且您愿意冒着禁用签名的风险来避免大量警报，则您可能需要禁用签名。表 3-1 列出了支持的签名和系统消息编号。

表 2: 签名 ID 和系统消息编号

签名 ID	消息编号	签名标题	签名类型	说明
1000	400000	IP 选项 - 错误选项列表	信息	在收到 IP 数据报时触发，其中 IP 数据报报头中的 IP 选项列表不完整或格式错误。IP 选项列表包含一个或多个执行各种网络管理或调试任务的选项。
1001	400001	IP 选项 - 记录数据包路由	信息	在收到 IP 数据报，而该数据报的 IP 选项列表包括选项 7（记录数据包路由）时触发。

签名 ID	消息编号	签名标题	签名类型	说明
1002	400002	IP 选项 - 时间戳	信息	在收到 IP 数据报，而该数据报的 IP 选项列表包括选项 4（时间戳）时触发。
1003	400003	IP 选项 - 安全	信息	在收到 IP 数据报，而该数据报的 IP 选项列表包括选项 2（安全选项）时触发。
1004	400004	IP 选项 - 松散源路由	信息	在收到 IP 数据报，且该数据报的 IP 选项列表包括选项 3（松散源路由）时触发。
1005	400005	IP 选项 - SATNET ID	信息	在收到 IP 数据报，其中该数据报的 IP 选项列表包括选项 8（SATNET 数据流标识符）时触发。
1006	400006	IP 选项 - 严格源路由	信息	在收到 IP 数据报，而其中该数据报的 IP 选项列表包括选项 2（严格源路由）时触发。
1100	400007	IP 分段攻击	攻击	当收到任何 IP 数据报且在偏移字段中指示偏移值小于 5 但大于 0 时触发。
1102	400008	不可能的 IP 数据包	攻击	当源地址等于目标地址的 IP 数据包到达时触发。此签名可以捕获所谓的 LAND 攻击 (Land Attack)。
1103	400009	IP 重叠分片数 (Teardrop)	攻击	当同一 IP 数据报中包含的两个分段具有偏移量（表明它们在数据报中共享定位）时触发。这可能意味着分片 A 正在被分片 B 完全覆盖，或者分片 A 正在被分片 B 部分覆盖。某些操作系统无法正确处理以这种方式重叠的分片，可能会引发异常或以其他方式运行接收重叠分段，这就是 Teardrop 攻击创建 DoS 的方式。
2000	400010	ICMP 回应应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 0（回应应答）的 IP 数据报时触发。
2001	400011	ICMP 主机不可达	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 3（主机不可达）的 IP 数据报时触发。
2002	400012	ICMP 源抑制	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 4（源抑制）的 IP 数据报时触发。
2003	400013	ICMP 重定向	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 5（重定向）的 IP 数据报时触发。
1 月	400014	ICMP 回应请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 8（回应请求）的 IP 数据报时触发。
2005	400015	数据报的 ICMP 超时	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 11（数据报超时）的 IP 数据报时触发。

签名 ID	消息编号	签名标题	签名类型	说明
2006	400016	数据报上的 ICMP 参数问题	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 12 (数据报上的参数问题) 的 IP 数据报时触发。
2007	400017	ICMP 时间戳请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 13 (时间戳请求) 的 IP 数据报时触发。
2008	400018	ICMP 时间戳应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 14 (时间戳应答) 的 IP 数据报时触发。
2009	400019	ICMP 信息请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 15 (信息请求) 的 IP 数据报时触发。
2010	400020	ICMP 信息应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 16 (ICMP 信息应答) 的 IP 数据报时触发。
2011	400021	ICMP 地址掩码请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 17 (地址掩码请求) 的 IP 数据报时触发。
2012	400022	ICMP 地址掩码应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 18 (地址掩码应答) 的 IP 数据报时触发。
2150	400023	分段的 ICMP 流量	攻击	当收到 IP 报头的协议字段设置为 1 (ICMP) 的 IP 数据报并且更多分片标志设置为 1 (ICMP) 或者偏移字段中指示有偏移时触发。
2151	400024	大 ICMP 流量	攻击	收到 IP 报头的协议字段设置为 1 (ICMP) 且 IP 长度大于 1024 的 IP 数据报时触发。
2154	400025	死亡之 Ping 攻击	攻击	当收到 IP 报头的协议字段设置为 1 (ICMP)、最后分片位已设置, 并且 $(IP \text{ 偏移量} * 8) + (IP \text{ 数据长度}) \rightarrow 65535$ 也就是说, IP 偏移量 (表示此分段在原始数据包中的起始位置, 以 8 字节为单位) 加上数据包其余部分就大于 IP 数据包的最大大小。
3040	400026	TCP NULL 标志	攻击	当单个未设置 SYN、FIN、ACK 或 RST 标志的 TCP 数据包已发送到特定主机时触发。
3041	400027	TCP SYN+FIN 标志	攻击	当设置了 SYN 和 FIN 标志并将其发送到特定主机的单个 TCP 数据包时触发。
3042	400028	仅 TCP FIN 标志	攻击	当单个孤立 TCP FIN 数据包发送到特定主机上的特权端口 (端口号小于 1024) 时触发。
3153	400029	指定了不正确的 FTP 地址	Informational	在发出地址与请求主机不同的端口命令时触发。

签名 ID	消息编号	签名标题	签名类型	说明
3154	400030	指定了不正确的 FTP 端口	Informational	在发出的 port 命令指定的数据端口为 1024 或 65535 时触发。
4050	400031	UDP 炸弹攻击	攻击	当指定的 UDP 长度小于指定的 IP 长度时触发。这种格式错误的数据包类型与拒绝服务尝试相关。
4051	400032	UDP Snork 攻击	攻击	当检测到源端口为 135、7 或 19 且目的端口为 135 的 UDP 数据包时触发。
4052	400033	UDP Chargen DoS 攻击	攻击	当检测到源端口为 7 且目的端口为 19 的 UDP 数据包时触发此签名。
6050	400034	DNS HINFO 请求	信息	在尝试从 DNS 服务器访问 HINFO 记录时触发。
6051	400035	DNS 区域传输	信息	在正常 DNS 区域传输上触发，其中源端口为 53。
6052	400036	来自高端口的 DNS 区域传输	信息	在非法 DNS 区域传输（其中源端口不等于 53）时触发。
6053	400037	所有记录的 DNS 请求	信息	触发所有记录的 DNS 请求。
6100	400038	RPC 端口注册	信息	当尝试在目标主机上注册新的 RPC 服务时触发。
6101	400039	RPC 端口取消注册	信息	当尝试在目标主机上注销现有的 RPC 服务时触发。
6102	400040	RPC 转储	信息	当向目标主机发出 RPC 转储请求时触发。
6103	400041	通过代理发送的 RPC 请求	攻击	当向目标主机的端口映射器发送代理的 RPC 请求时触发。
6150	400042	ypserv（YP 服务器后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 服务器后台守护程序 (ypserv) 端口的请求时触发。
6151	400043	ypserv（YP 绑定后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 绑定后台守护程序 (ypbind) 端口的请求时触发。
6152	400044	yppasswdd（YP 密码后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 密码后台守护程序 (yppasswdd) 端口的请求时触发。
6153	400045	ypupdated（YP 更新后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 更新后台守护程序 (ypupdated) 端口的请求时触发。
6154	400046	ypxfrd（YP 传输后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 传输后台守护程序 (ypxfrd) 端口的请求时触发。
6155	400047	mountd（装载后台守护程序）端口映射请求	信息	当向端口映射程序发出安装后台守护程序 (mountd) 端口的请求时触发。
6175	400048	rexid（远程执行后台守护程序）端口映射请求	信息	当向端口映射程序请求远程执行后台守护程序 (rexid) 端口时触发。

签名 ID	消息编号	签名标题	签名类型	说明
6180	400049	rexid（远程执行后台守护程序）尝试	信息	当调用 rexd 程序时触发。远程执行后台守护程序是负责远程执行程序的服务端。这可能表示有人试图未经授权访问系统资源。
6190	400050	statd 缓冲区溢出	攻击	发送大型 statd 请求时触发。这可能是试图使缓冲区溢出并获得对系统资源的访问权限。

CR_Examples

以下示例禁用签名 6100：

```
ciscoasa(config)# ip audit signature 6100 disable
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
showrunning-configipauditsignature	显示命令的 ipauditsignature 配置。

ip-client

要允许 FXOS 发起管理流量并将其发送出 Firepower 2100 ASA 数据接口，请在全局配置模式下使用 **ip-client** 命令。要禁用流量启动，请使用此命令的 **no** 形式。

ip-client *interface_name*
no ip-client *interface_name*

Syntax Description

interface_name 指定 FXOS 可以通过其发送管理流量的接口名称。

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
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.8(2) 我们添加了此命令。

使用指南

您可以在 ASA 数据接口上启用 FXOS 管理流量启动，例如，这对于 SNMP 陷阱或 NTP 和 DNS 服务器访问是必需的。有关传入管理流量，请参阅 **fxospermit** 命令。

在 FXOS 配置中，请确保默认网关设置为 0.0.0.0，即将 ASA 设置为网关。请参阅 FXOS **setout-of-band** 命令。

CR_Examples

以下命令允许通过外部接口发起 FXOS 流量：

```
ciscoasa(config)# ip-client outside
```

Related Commands

命令	说明
connectfxos	从 ASA CLI 连接到 FXOS CLI。
fxospermit	允许在 ASA 数据接口上进行 FXOS 管理访问。
fxosport	设置 FXOS 管理访问端口。

ip-comp

要启用 LZS IP 压缩，请在 **ip-compenable** 策略组配置模式下使用该命令。要禁用 IP 压缩，请使用该命令 **ip-compdisable**。要禁用 IP 压缩，请使用该命令 **ip-comp** 的 **no** 形式。

ip-comp {enable | disable}
no ip-comp

Syntax Description

disable 禁用 IP 压缩。

enable 启用 IP 压缩。

Command Default

禁用 IP 压缩。

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
Group-policy 配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令 **no** 的形式允许从另一个组策略继承值。启用数据压缩可能会加快使用调制解调器连接的远程拨入用户的数据传输速率。



注意 数据压缩会增加每个用户会话的内存要求和 CPU 利用率，从而降低 ASA 的整体吞吐量。为此，建议仅对使用调制解调器连接的远程用户启用数据压缩。设计特定于调制解调器用户的组策略并仅对其启用压缩。

如果终端生成 IP 压缩流量，您应禁用 IP 压缩，以防止数据包解压缩不当。如果在特定 LAN 上启用了 LAN 间隧道，则主机 A 尝试将 IP 压缩数据从隧道的一端传递到另一端时，将无法与主机 B 进行通信。



注释 启用 **ip-comp** 命令并为“before-encryption”配置 IPsec 分片时，无法使用 IPsec 压缩（**ip-comp_option** 和 **pre-encryption**）。发送到加密芯片的 IP 报头会被模糊处理（由于压缩），导致加密芯片在处理提供的出站数据包时生成错误。您还可以检查您的 MTU 级别，以确保它是一个较小的值（例如 600 字节）。

CR_Examples

以下示例显示如何为名为“FirstGroup”的组策略启用 IP 压缩：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```


ip local pool

要配置 IP 地址池，请在**iplocalpool**全局配置模式下使用该命令。EXTE 要删除地址池，请使用此命令**no**的形式。

池名称**ip local pool**第一个地址最后一个地址 [mask掩 码]
no ip local pool*poolname*

Syntax Description

第一个地址	指定 IP 地址范围的起始地址。
最后一个地址	指定 IP 地址范围中的最后一个地址。
maskmask	(可选) 指定地址池的子网掩码。不能使用 255.255.255.254 (/31) 或 255.255.255.255 (/32) 子网掩码。
<i>poolname</i>	指定IP地址池的名称。

Command Default

无默认为行为或值。

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
7.0(1)	添加了此命令。
9.0(1)	已在 ipaddress 命令中添加集群池的 IP 本地池，以支持 ASA 集群。

使用指南

当分配给 VPN 客户端的 IP 地址属于非标准网络时，您必须提供掩码值，如果使用默认掩码，数据可能会被错误路由。这种情况的一个典型例子是本地 IP 地址池包含 10.10.10.0/255.255.255.0 地址，因为默认情况下这是 A 类网络。当 VPN 客户端需要通过不同的接口访问 10 个网络内的不同子网时，这可能会导致一些路由问题。例如，如果可以通过接口 2 使用地址 10.10.100.1/255.255.255.0 的打印机，但 10.10.10.0 网络通过 VPN 隧道可用，因此使用接口 1，VPN 客户端可能会混淆该将数据路由到何处打印机的数据包。10.10.10.0 和 10.10.100.0 子网都属于 10.0.0.0 A 类网络，因此打印机数据可能通过 VPN 隧道发送。

CR_Examples

以下示例配置名为 firstpool 的 IP 地址池。起始地址为 10.20.30.40，结束地址为 10.20.30.50。网络掩码为 255.255.255.0。

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

命令	说明
clearconfigureiplocalpool	删除所有 IP 本地池。
showrunning-configiplocalpool	显示 IP 池配置。要指定特定 IP 地址池，请在命令中包含名称。

ip unnumbered

要从接口（例如，环回接口）借用或继承 IP 地址，请在接口配置模式下使用 **ip unnumbered** 命令。要停止从接口继承 IP 地址，请使用此命令的 **no** 形式。

ip unnumbered *interface-name*
no ip unnumbered

Syntax Description

interface-name 指定要继承 IP 地址的接口的名称。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.19(1) 添加了此命令。

使用指南

ip unnumbered 命令用于将所选接口的 IP 地址继承为当前接口的地址。

CR_Examples

以下示例从环回接口借用 IP 地址：

```
ciscoasa(config)# interface tunnel 1
ciscoasa(conf-if)# ip unnumbered loopback1
```

Related Commands

命令	说明
ipv6 unnumbered <i>interface-name</i>	继承指定接口的 IPv6 地址。
interface loopback 环回编号	创建环回接口。

ip-phone-bypass

要启用 IP 电话绕行，请在 group-policy 配置模式下使用 **ip-phone-bypassenable**命令。要从运行配置中删除 IP 电话绕行属性，请使用此命令的 **no** 形式。

```
ip-phone-bypass { enable | disable }
no ip-phone-bypass
```

Syntax Description	disable 禁用 IP 电话绕行。
	enable 启用 IP 电话绕行。

Command Default	IP 电话旁路已禁用。

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
组策略配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南

要禁用 IP 电话绕行，请使用 **ip-phone-bypassdisable**命令。此命令选项的 **no**形式允许从另一个组策略继承“IP 电话旁路”的值。

通过 IP 电话绕行，硬件客户端背后的 IP 电话可以在不执行用户身份验证过程的情况下进行连接。如果启用，安全设备身份验证仍然生效。

仅当启用用户身份验证时，才需要配置 IP 电话绕行。

您还需要配置 **mac-exempt**选项以避免客户端进行身份验证。请参阅命 **vpnclientmac-exempt**令以了解更多信息。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用 IP 电话旁路：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

Related Commands

命令	说明
user-authentication	要求硬件客户端后面的用户在连接之前向 ASA 证明自己的身份。

ips

要将流量从 ASA 转移到 AIP SSM 进行检查，请在类配置模式下使用 **ips**命令。要删除此命令，请使用此命 **no**令的形式。

```
ips {inline | promiscuous} {fail-close | fail-open} [sensor {sensor_name | mapped_name}]
no ips {inline | promiscuous} {fail-close | fail-open} [sensor {sensor_name | mapped_name}]
```

Syntax Description	fail-close	如果 AIP SSM 失败，则阻止流量。
	fail-open	如果 AIP SSM 失败，则允许流量。
	inline	将数据包定向到 AIP SSM；数据包可能由于 IPS 操作而被丢弃。
	promiscuous	为 AIP SSM 复制数据包； AIP SSM 无法丢弃原始数据包。
	sensor {sensor_name mapped_name }	设置此流量的虚拟传感器名称。如果您在 AIP SSM（使用 6.0 或更高版本）上使用虚拟传感器，则可以使用此参数指定传感器名称。要查看可用的传感器名称，请输入 ips...sensor? 命令。系统将列出可用的传感器。您也可以使用该 showips 命令。 如果在 ASA 上使用多情景模式，则只能指定已分配到该情景的传感器（请参阅 allocate-ips 命令）。使用 <i>mapped_name</i> 参数（如果已在情景中配置）。 如果未指定传感器名称，则流量使用默认传感器。在多情景模式下，您可以为情景指定默认传感器。在单模式下，或者如果未在多模式下指定默认传感器，则流量将使用在 AIP SSM 上设置的默认传感器。 如果输入 AIP SSM 中尚不存在的名称，则会出现错误，命令也会被拒绝。

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
类配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	8.0(2) 添加了虚拟传感器支持。

使用指南

ASA 5500 系列支持 AIP SSM，该 SSM 运行高级 IPS 软件，可提供主动、功能齐全的入侵防御服务，以在恶意流量（包括蠕虫和网络病毒）影响您的网络之前将其阻止。在 ASA 上配置 **ips** 命令之前或之后，请在 AIP SSM 上配置安全策略。您可以从 ASA 连接到 AIP SSM（在 **session** 命令），也可以在其管理接口上使用 SSH 或 Telnet 直接连接到 AIP SSM。或者，您可以使用 ASDM。有关配置 AIP SSM 的详细信息，请参阅使用命令行界面配置 Cisco 入侵防御系统传感器。

要配置 **ips** 命令，您必须首先配置 **class-map** 命令、**policy-map** 命令和 **class** 命令。

AIP SSM 运行与 ASA 不同的应用程序。但是，会将其集成到 ASA 流量中。除管理接口外，AIP SSM 本身不包含任何外部接口。当您在 ASA 上对流量类应用 **ips** 命令时，流量将按以下方式流经 ASA 和 AIP SSM：

1. 流量进入 ASA。
2. 应用防火墙策略。
3. 通过背板将流量发送到 AIP SSM（使用 **inline** 关键字；有关仅将流量副本发送到 AIP SSM 的信息，请参阅 **promiscuous** 关键字）。
4. AIP SSM 将其安全策略应用于流量，并采取适当的措施。
5. 有效流量通过背板发送回 ASA；AIP SSM 可能会根据其安全策略阻止某些流量，并且不会传递这些流量。
6. 系统将应用 VPN 策略（如果已配置）。
7. 流量退出 ASA。

CR_Examples

以下示例将所有 IP 流量转移到混杂模式下的 AIP SSM，并在 AIP SSM 卡因任何原因而失败时阻止所有 IP 流量：

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

以下示例将以内联模式将发往 10.1.1.0 网络和 10.2.1.0 网络的所有 IP 流量转移到 AIP SSM，并且如果 AIP SSM 卡因任何原因出现故障，则允许所有流量通过。对于 my-ips-class 流量，使用 sensor1；my-ips-class2 流量使用 sensor2。

```
ciscoasa(config)# access-list my-ips-acl1 permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl1
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
```

```
ciscoasa(config-pmap-c) # ips inline fail-open sensor sensor2  
ciscoasa(config-pmap-c) # service-policy my-ips-policy interface outside
```

Related Commands

命令	说明
allocate-ips	将虚拟传感器分配给安全情景。
class	指定要用于流量分类的类映射。
class-map	识别要在策略映射中使用的流量。
policy-map	配置策略；即流量类与一个或多个操作的关联。
showrunning-configpolicy-map	显示所有当前策略图配置。

ipsec-udp

要启用 UDP 上的 IPsec，请在 **ipsec-udpenable** 策略组配置模式下使用该命令。要从当前组策略中删除 IPsec over UDP 属性，请使用此命令的 **no** 形式。

ipsec-udp { **enable** | **disable** }
no ipsec-udp

Syntax Description

disable 禁用 IPsec over UDP。

enable 启用 IPsec over UDP。

Command Default

UDP 上的 IPsec 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
组策略配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令的 **no** 形式允许从另一个组策略继承 IPsec over UDP 的值。

IPsec over UDP（有时称为 IPsec through NAT）允许 Cisco VPN 客户端或硬件客户端通过 UDP 连接到运行 NAT 的 ASA。

要禁用 IPsec over UDP，请使用 **ipsec-udpdisable** 命令。

要使用 IPsec over UDP，您还必须配置该 **ipsec-udp-port** 命令。

Cisco VPN 客户端还必须配置为使用 IPsec over UDP（默认情况下配置为使用它）。VPN 3002 无需配置即可使用 IPsec over UDP。

IPsec over UDP 是专有的，仅适用于远程访问连接，并且需要模式配置，这意味着 ASA 在协商 SA 时与客户端交换配置参数。

使用 IPsec over UDP 可能会略微降低系统性能。

在作为 VPN 客户端运行的 ASA5505 上不支持 **ipsec-udp-port** 命令。ASA 5505 在客户端模式下可在 UDP 端口 500 和/或 4500 上启动 IPsec 会话。

CR_Examples

以下示例显示如何为名为FirstGroup 的策略组配置 IPsec over UDP:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

Related Commands

命令	说明
ipsec-udp-port	指定 ASA 侦听 UDP 流量的端口。

ipsec-udp-port

要为 IPsec over UDP 设置 UDP 端口号，请在 `group-policy` 配置模式下使用 **ipsec-udp-port** 命令。要禁用 UDP 端口，请使用此命令的形式。

ipsec-udp-port*port*
noipsec-udp-port

Syntax Description

port 使用 4001 至 49151 范围内的整数标识 UDP 端口号。

Command Default

默认端口为 10000。

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
Group-policy 配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令的 **no** 形式允许从另一个组策略继承 IPsec over UDP 端口的值。

在 IPsec 协商中，ASA 会侦听配置的端口并转发该端口的 UDP 流量，即使其他过滤规则丢弃 UDP 流量。

可以配置多个组策略来启用此功能，并且每个组策略可以使用不同的端口号。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略将 IPsec UDP 端口设置为端口 4025：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

命令	说明
ipsec-udp	允许 Cisco VPN 客户端或硬件客户端通过 UDP 连接到运行 NAT 的 ASA。



ipv – ir

- [ipv4-prefix](#) , 第 235 页
- [ipv6 address](#) , 第 237 页
- [ipv6-address-pool](#) , 第 241 页
- [ipv6-address-pools](#) , 第 243 页
- [ipv6 dhcp client pd](#) , 第 245 页
- [ipv6 dhcp client pd hint](#) , 第 247 页
- [ipv6 dhcp pool](#) , 第 249 页
- [ipv6 dhcprelay enable](#) , 第 252 页
- [IPv6 dhcprelay 服务器](#) , 第 254 页
- [ipv6 dhcprelay timeout](#) , 第 256 页
- [ipv6 dhcp server](#) , 第 257 页
- [ipv6 enable](#) , 第 259 页
- [ipv6 enforce-eui64](#) , 第 260 页
- [ipv6 icmp](#) , 第 262 页
- [ipv6 local pool](#) , 第 265 页
- [ipv6 nd dad attempts](#) , 第 267 页
- [ipv6 nd managed-config-flag](#) , 第 269 页
- [ipv6 nd ns-interval](#) , 第 270 页
- [ipv6 nd other-config-flag](#) , 第 271 页
- [ipv6 nd prefix](#) , 第 272 页
- [ipv6 nd ra-interval](#) , 第 274 页
- [ipv6 nd ra-lifetime](#) , 第 275 页
- [ipv6 nd reachable-time](#) , 第 277 页
- [ipv6 nd suppress-ra](#) , 第 279 页
- [ipv6 neighbor](#) , 第 280 页
- [ipv6 ospf](#) , 第 282 页
- [ipv6 ospf area](#) , 第 284 页
- [ipv6 ospf cost](#) , 第 285 页
- [ipv6 ospf database-filter all out](#) , 第 286 页

- [ipv6 ospf dead-interval](#)，第 287 页
- [ipv6 ospf encryption](#)，第 288 页
- [ipv6 ospf flood-reduction](#)，第 290 页
- [ipv6 ospf hello-interval](#)，第 291 页
- [ipv6 ospf mtu-ignore](#)，第 292 页
- [ipv6 ospf neighbor](#)，第 293 页
- [ipv6 ospf network](#)，第 295 页
- [ipv6 ospf priority](#)，第 296 页
- [ipv6 ospf retransmit-interval](#)，第 297 页
- [ipv6 ospf transmit-delay](#)，第 298 页
- [ipv6-prefix](#)，第 299 页
- [ipv6 prefix-list](#)，第 301 页
- [ipv6 route](#)，第 303 页
- [ipv6 router ospf](#)，第 305 页
- [ipv6-split-tunnel-policy](#)，第 308 页
- [ipv6-vpn-address-assign](#)，第 310 页
- [ipv6-vpn-filter](#)，第 312 页
- [ip verify reverse-path](#)，第 314 页
- [ipv6 未编号](#)，第 316 页

ipv4-prefix

要为映射地址和端口 (MAP) 域中的基本映射规则配置 IPv4 前缀，请在 MAP 域基本映射规则配置模式下使用 **ipv4-prefix** 命令。使用此命令的形式来删除前缀。

ipv4-prefix*ipv4_network_addressnetmask*
no ipv4-prefix*ipv4_network_addressnetmask*

Syntax Description

ipv4_network_addressnetmask 定义客户边缘 (CE) 设备的 IPv4 地址池的 IPv4 前缀。指定网络地址和子网掩码，例如 192.168.3.0 255.255.255.0。不能在不同 MAP 域中使用相同的 IPv4 前缀。

Command Default

无默认值。

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
MAP域基本映射规则配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改

9.13(1)	引入了此命令。

使用指南

IPv4 前缀定义客户边缘 (CE) 设备的 IPv4 地址池。CE 设备首先将其 IPv4 地址转换为 IPv4 前缀定义的池中的地址（和端口号）。然后，MAP 会使用默认映射规则中的前缀将新地址转换为 IPv6 地址。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
```

```
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

ipv6 address

要启用 IPv6 并在接口上配置 IPv6 地址（在路由模式下），或为网桥组或管理接口地址（透明模式）配置 IPv6 地址，请使用 **ipv6address** 命令。要删除 IPv6 地址，请使用此命令的形式 **no**。

ipv6

peer {**autoconfig** | **autoconfig** [**default** | **dhcp ignore**] | **dhcp** [**default**] | **p6 address** | **peer rmp6 address** | **peer length** | **p6 address local** | **static p6 address** }

no ipv6

peer {**autoconfig** | **autoconfig** [**default** | **dhcp ignore**] | **dhcp** [**default**] | **p6 address** | **peer rmp6 address** | **peer length** | **p6 address local** | **static p6 address** }

Syntax Description

autoconfig

在接口上启用无状态自动配置。在接口上启用无状态自动配置可根据路由器通告消息中收到的前缀配置 IPv6 地址。当启用无状态自动配置时，将根据修改后的 EUI-64 接口 ID 自动为接口生成链路本地地址。不支持透明防火墙模式。

注释

尽管 RFC 4862 规定配置为无状态自动配置的主机不会发送路由器通告消息，但在这种情况下 ASA 会发送路由器通告消息。查看抑制消息的 **ipv6 nd suppress-ra** 命令。

cluster-pool poolname

（可选）对于 ASA 集群，设置 **ipv6 localpool** 命令定义的集群地址池。参数定义的主集群 IP 地址仅属于当前主设备。每个集群成员都会从此池中收到一个本地 IP 地址。

您无法提前确定分配给每个单元的确切地址；要查看每个单元使用的地址，请输入 **show ipv6 localpool poolname** 命令。每个集群成员在加入集群时都会分配到一个成员 ID。该 ID 决定了池中使用的本地 IP。

default

（可选）从路由器通告中获取默认路由。

defaulttrust

（可选）安装来自路由器通告的默认路由。

dhcp (autoconfig)

（可选）指定 ASA 仅使用来自可信来源（换句话说，来自提供 IPv6 地址的同一服务器）的路由器通告的默认路由。

dhcp

从 DHCPv6 服务器获取 IPv6 地址。

ignore

（可选）指定路由器通告可以来自另一个网络，这可能是一种更危险的方法。

ipv6_address/prefix_length

为接口分配全局地址。分配全局地址时，将为接口自动创建链路本地地址。

<i>ipv6_prefix/prefix_length</i> eui-64	通过将指定的前缀与使用修改后的 EUI-64 格式从接口 MAC 地址生成的接口 ID 相结合，为接口分配全局地址。分配全局地址时，将为接口自动创建 链路本地地址。如果为 +) 参数指定的值大于 64 位，则前缀位优先于接口 ID。如果另一台主机正在使用指定的地址，系统将显示错误消息。 您不需要指定备用接口；接口 ID 将会自动生成。 修改后的 EUI-64 格式接口 ID 是通过在 48 位链路层 (MAC) 地址的高三个字节 (OUI 字段) 和低三个字节 (序列号) 之间插入十六进制数 FFFE 得出的。为确保所选地址来自唯一以太网以太网 MAC 地址，高顺序字节中的倒数第二位将反转（通用/本地位），以指示 48 位地址的唯一性。例如，MAC 地址为 00E0.B601.3B7A 的接口的 64 位接口 ID 为 02E0:B6FF:FE01:3B7A。
<i>ipv6_address</i> link-local	仅手动配置链路本地地址。使用此命令指定的 <i>ipv6</i> 地址 会覆盖为接口自动生成的链路本地地址。链路本地地址由链路本地前缀 FE80::/64 和采用修改的 EUI-64 格式的接口 ID 组成。MAC 地址为 00E0.B601.3B7A 的接口的本地链路地址为 FE80::2E0:B6FF:FE01:3B7A。如果另一台主机正在使用指定的地址，系统将显示错误消息。
<i>prefix_name</i> <i>ipv6_address/prefix_length</i>	使用委托前缀。此功能要求 ASA 接口启用 DHCPv6 前缀委派客户端 (ipv6dhcpcclientpd)。通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:DB8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。
standby <i>ipv6_address</i>	(可选) 指定故障转移对中的辅助单元或故障转移组使用的接口地址。

Command Default

已禁用 IPv6。

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	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

8.2(1) 添加了对透明防火墙模式的支持。

8.2(2) 增加了对备用地址的支持。

8.4(1) 对于透明模式，添加了桥接组。您应为 BVI 设置 IP 地址，而不是全局设置。

9.0(1) 添加 **cluster-pool** 关键字是为了支持 ASA 集群。

9.6(2) 添加了以下选项：

- **autoconfigdefaulttrust {dhcp | ignore}**
- **dhcp[default]**
- *prefix_nameipv6_address/prefix_length*

使用指南

在接口上配置 IPv6 地址可在该接口上启用 IPv6；请参阅指定 IPv6 地址后，无需使用 **ipv6enable** 命令。

多上下文模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一的子网上。在多情景模式下，如果此接口位于共享接口上，则每个 IP 地址必须唯一，但在同一子网上。如果接口是唯一的，则此 IP 地址可以在需要时由其他情景使用。

多情景模式不支持 DHCPv6 和前缀代理选项。

透明防火墙指南

透明模式仅支持手动设置 IPv6 地址。透明防火墙不参与 IP 路由。如果要设置 BVI 地址，则只需对 ASA 进行 IP 配置。需要此地址是因为 ASA 使用此地址作为源自 ASA 的流量（例如系统消息或与 AAA 服务器的通信）的源地址。您还可以使用此地址进行远程管理访问。此地址必须与上游和下游路由器位于同一子网上。对于多情景模式，在每个情景内设置管理 IP 地址。对于包含管理接口的型号，您还可以为此接口设置 IP 地址以进行管理。

故障转移指南

备用 IP 地址必须与主 IP 地址位于同一子网。

ASA 集群指南

只有在将集群接口模式配置为单个接口 (**cluster-interface mode individual**) 后，您才能为单个接口设置集群池。唯一的例外情况是仅管理接口：

- 您始终可以将仅管理接口配置为单独的接口，即使在跨网以太网通道模式下也是如此。即使在透明防火墙模式下，管理接口也可以是单独的接口。
- 在跨网以太网通道模式下，如果将管理接口配置为单独接口，则无法为管理接口启用动态路由。您必须使用静态路由。

集群不支持 DHCPv6 和前缀委派选项。

CR_Examples

以下示例将 2001:0DB8:BA98::3210/64 分配为选定接口的全局地址，并将 2001:0DB8:BA98::3211 分配为备用设备上相应接口的地址：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

以下示例为所选接口自动分配 IPv6 地址：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

以下示例将 IPv6 前缀 2001:0DB8:BA98::/64 分配到所选接口，并在地址的低 64 位指定 EUI-64 接口 ID。如果此设备属于故障转移对，则无需指定 **standby** 关键字；备用地址将使用修改的 EUI-64 接口 ID 自动创建。

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

以下示例分配 FE80::260:3EFF:FE11:6670 作为所选接口的链路级地址：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

以下示例分配 FE80::260:3EFF:FE11:6670 作为故障转移对中主设备上所选接口的链路级地址，并分配 FE80::260:3EFF:FE11:6671 作为链路级地址已完成。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

以下示例分配 ::1:0:0:0:1/64 作为完成指定前缀的地址：

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

Related Commands

命令	说明
debug ipv6 interface	显示 IPv6 接口的调试信息。
show ipv6 interface	显示为 IPv6 配置的接口的状态。

ipv6-address-pool

要指定用于向远程客户端分配地址的 IPv6 地址池列表，请在 `tunnel-group general-attributes` 配置模式下使用 **ipv6-address-pool** 命令。要消除 IPv6 地址池，请使用此命令的 **no** 形式。

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [...*ipv6_address_pool6*]
no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [...*ipv6_address_pool6*]

Syntax Description

interface_name (可选) 指定用于地址池的接口。

ipv6_address_pool 指定使用 **ipv6localpool** 命令配置的地址池的名称。最多可以指定六个本地地址池。

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
Tunnel-group 隧道组常规属性配置	• 是	—	• 是	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

使用指南

您可以输入多个命令，每个接口一个。如果未指定接口，则 命令指定所有未显式引用的接口的默认值。

group-policy **ipv6-address-pools** 命令中的 IPv6 地址池设置会覆盖 tunnel group **ipv6-address-pool** 命令中的 IPv6 地址池设置。

地址池的指定顺序非常重要。ASA 按照这些地址池在此命令中出现的顺序分配这些地址池中的地址。

CR_Examples

以下示例在 `tunnel-group general-attributes` 配置模式下输入，指定用于将 IPsec 远程访问隧道组测试的地址分配给远程客户端的 IPv6 地址池列表：

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
```

```
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

Related Commands

命令	说明
ipv6-address-pools	配置组策略的 IPv6 地址池设置，这会覆盖隧道组的这些设置。
ipv6 local pool	配置用于 VPN 远程访问隧道的 IP 地址池。
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group	配置隧道组。

ipv6-address-pools

要指定最多包含六个 IPv6 地址池的列表（从中将地址分配给远程客户端），请在 `group-policy` 属性配置模式下使用 **ipv6-address-pools** 命令。要从组策略中删除属性并启用从其他组策略源继承，请使用此命令的 **no** 形式。

```
ipv6-address-pools valueipv6_address_pool1 [...ipv6_address_pool6]
no ipv6-address-pools valueipv6_address_pool1 [...ipv6_address_pool6]
ipv6-address-poolsnone
noipv6-address-poolsnone
```

Syntax Description

ipv6_address_pool 指定使用 **ipv6localpool** 命令配置的最多六个 IPv6 地址池的名称。使用空格分隔 IPv6 地址池名称。

none 指定不配置 IPv6 地址池，并禁用从其他组策略源继承。

value 指定包含最多六个 IPv6 地址池的列表，要从中分配地址。

Command Default

默认情况下，未配置 IPv6 地址池属性。

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
组策略属性配置	• 是	—	• 是	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

使用指南

要配置 IPv6 地址池，请使用 **ipv6localpool** 命令。

在命令中指定池的顺序 **ipv6-address-pools** 序很重要。ASA 按照这些地址池在此命令中出现的顺序分配这些地址池中的地址。

该 **ipv6-address-poolsnone** 命令禁止从其他策略源（例如 `DefaultGrpPolicy`）继承此属性。该命令 **ipv6-address-poolsnone** 令从配置中删除该命令，恢复默认值，即允许继承。 **noipv6-address-poolsnone**

CR_Examples

以下示例在 `group-policy` 属性配置模式下配置名为 `firstipv6pool` 的 IPv6 地址池用于向远程客户端分配地址，然后将该池与 `GroupPolicy1` 关联：

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
ipv6localpool	配置要用于 VPN 组策略的 IPv6 地址池。
clear configure group-policy	清除所有已配置的组策略。
show running-config group-policy	显示所有组策略或特定组策略的配置。

ipv6 dhcp client pd

要启用 DHCPv6 前缀委派客户端并命名在接口上获取的前缀，请在 **ipv6dhcpclientpd** 接口配置模式下使用该命令。要禁用客户端，请使用此命令 **no** 的形式。

ipv6 dhcp client pd*name*
no ipv6 dhcp client pd*name*

Syntax Description

name 设置此前缀的名称。*name* 最长为 200 个字符。在将 IP 地址分配给使用前缀 (**ipv6addressprefix_name**) 的接口时，将使用此名称。

Command Default

无默认为行为或值。

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

在一个或多个接口上启用 DHCPv6 前缀代理客户端。ASA 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 ASA 接口才能使用代理前缀衍生的地址。

此功能不支持集群。

无法在仅管理接口上配置此功能。

CR_Examples

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcp pool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcp client pd hint

要提供一个或多个有关您希望接收的授权前缀的提示，请在接口配置模式下使用 **ipv6dhcpclientpdhint** 命令。要禁用客户端，请使用此命令 **no** 的形式。

ipv6 dhcp client pd hint*ipv6_prefix/prefix_length*
no ipv6 dhcp client pd hint*ipv6_prefix/prefix_length*

Syntax Description

ipv6_prefix/prefix_length 指定要接收的 IPv6 前缀和长度。

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

通常，您需要请求特定的前缀长度（例如 `::/60`），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

CR_Examples

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。

命令	说明
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcp pool

要配置 IPv6 DHCP 池以包含您希望 DHCPv6 服务器向无状态地址自动配置 (SLAAC) 客户端提供的信息，请在全局配置模式下使用 **ipv6 dhcp pool** 命令。要删除池，请使用此命令 **no** 的形式。

ipv6 dhcp pool *pool_name*
no ipv6 dhcp pool *pool_name*

Syntax Description

pool_name 指定地址池。

Command Default

无默认为行为或值。

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	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA，使其在向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。使用 **ipv6 dhcp server** 命令配置 DHCPv6 无状态服务器；启用服务器时指定此池名称。如果需要，可以为每个接口配置单独的池，也可以在多个接口上使用相同的池。输入 **ipv6 dhcp pool** 命令后，您可以配置一个或多个要提供给客户端的参数。

使用 **ipv6 dhcp client pd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
```

```

ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcp pool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。

命令	说明
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcprelay enable

要在接口上启用 DHCPv6 中继服务，请在全局配置模式下使用 **ipv6dhcprelayenable** 命令。要禁用 DHCPv6 中继服务，请使用此命令的 **no** 形式。

ipv6 dhcprelay enable*interface*
no ipv6 dhcprelay enable*interface*

Syntax Description

接 指定目标的输出接口。
口

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	—	• 是	• 支持	—

Command History

版本 修改
9.0(1) 添加了此命令。

使用指南

此命令允许您在接口上启用 DHCPv6 中继服务。启用服务后，来自接口上的客户端的传入 DHCPv6 消息（可能已由另一个中继代理中继）将通过所有已配置的传出消息转发到所有已配置的中继目标链接。对于多上下文模式，您不能在由多个上下文（即共享接口）使用的接口上启用 DHCP 中继服务。

CR_Examples

以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

命令	说明
ipv6dhcprelayserver	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

命令	说明
ipv6dhcprelaytimeout	设置允许 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间量（以秒为单位）。

IPv6 dhcprelay 服务器

要指定客户端消息转发到的 IPv6 DHCP 服务器目标地址，请在 **ipv6dhcprelayserver** 全局配置模式下使用该命令。要删除 IPv6 DHCP 服务器目标地址，请使用此命令的 **no**形式。

```
ipv6 dhcprelay serveripv6-address [interface]
no ipv6 dhcprelay serveripv6-address [interface]
```

Syntax Description	接口（可选）指定目标的输出接口。
	ipv6-address 可以是链路范围的单播、多播、站点范围的单播或全局 IPV6 地址。

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	—	• 是	• 支持	—

Command History	版本 修改
	9.0(1) 添加了此命令。

使用指南	此命令可让您指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。客户端消息通过输出接口所连接的链路转发到目标地址。如果指定地址属于链路范围地址，则必须指定接口。不允许将未指定、环回和本地节点组播地址用作中继目标。您可以为每个情景指定最多十个服务器。

CR_Examples	以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands	命令	说明
	ipv6dhcprelayenable	在接口上启用 IPv6 DHCP 中继服务。

命令	说明
ipv6dhcprelaytimeout	设置允许 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间量（以秒为单位）。

ipv6 dhcprelay timeout

如要设置从DHCPv6服务器到通过中继绑定结构将响应传递至客户端所允许的时间（以秒为单位），请在全局配置模式下使用 **ipv6dhcprelaytimeout** 命令。要恢复默认设置，请使用此命 **no** 令的形式。

ipv6dhcprelaytimeoutseconds
noipv6dhcprelaytimeoutseconds

Syntax Description *seconds* 设置允许 DHCPv6 中继地址协商的秒数。有效值范围为 1 至 3600。

Command Default 默认值为 60 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
组配置	• 是	—	• 是	• 支持	—

Command History 版本 修改

9.0(1) 添加了此命令。

使用指南 此命令允许您设置 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间（以秒为单位）。

CR_Examples 以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

命令	说明
ipv6dhcprelayservice	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。
ipv6dhcprelayenable	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

ipv6 dhcp server

对于结合前缀委派功能和无状态地址自动配置 (SLAAC) 功能的客户端，请在接口配置模式下使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器。要禁用 DHCP 服务器，请使用此命令 **no** 的形式。

ipv6 dhcp server*pool_name*
no ipv6 dhcp server*pool_name*

Syntax Description

pool_name 设置使用 **ipv6dhcppool** 命令配置的 IPv6 池的名称。此池包含您想提供给给定接口上客户端的信息。

Command Default

无默认为行为或值。

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA，使其在向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
```

```

interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 enable

要启用 IPv6 处理，而您尚未配置显式 IPv6 地址，请在全局配置模式下使用 **ipv6enable** 命令。要禁用尚未配置明确 IPv6 地址的接口上的 IPv6 处理，请使用此 **no** 命令的形式。

ipv6 enable
no ipv6 enable

Syntax Description 此命令没有任何参数或关键字。

Command Default 已禁用 IPv6。

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	• 支持	—
全局配置	—	• 是	• 支持	• 支持	—

Command History 版本 修改

7.0(1) 添加了此命令。

8.2(1) 添加了对透明防火墙模式的支持。

使用指南 **ipv6enable** 命令会在接口上自动配置 IPv6 本地链路单播地址，同时还会启用接口以进行 IPv6 处理。该 **noipv6enable** 命令不会禁用配置了显式 IPv6 地址的接口上的 IPv6 处理。

CR_Examples 以下示例在所选接口上启用 IPv6 处理：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

Related Commands

命令	说明
ipv6address	为接口配置 IPv6 地址并在接口上启用 IPv6 处理。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 enforce-eui64

要强制在本地链路上的 IPv6 地址中使用修改后的 EUI-64 格式接口标识符，请在 **ipv6enforce-eui64** 全局配置模式下使用该命令。要禁用修改的 EUI-64 地址格式实施，请使用此命令的 **no** 形式。

```
ipv6 enforce-eui64if_name
no ipv6 enforce-eui64if_name
```

Syntax Description *if_name* 指定要启用修改后的 EUI-64 地址格式强制执行的接口的名称（由命 **nameif** 令指定）。

Command Default 已禁用修改的 EUI-64 格式实施。

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。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南 当在接口上启用此命令时，将根据源 MAC 地址验证该接口上接收的 IPv6 数据包的源地址，以确保接口标识符使用修改后的 EUI-64 格式。如果 IPv6 数据包不使用修改后的 EUI-64 格式作为接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器背后的主机接收的数据包将无法通过地址格式验证，且会被丢弃，因为其源 MAC 地址将是路由器 MAC 地址，而不是主机 MAC 地址。

修改后的 EUI-64 格式接口标识符由 48 位链路层 (MAC) 地址派生而来，通过在链路层地址的高三个字节（OUI 字段）和低三个字节（序列号）之间插入十六进制数 FFFE。为确保所选地址来自唯一以太网以太网 MAC 地址，高顺序字节中的倒数第二位将反转（通用/本地位），以指示 48 位地址的唯一性。例如，MAC 地址为 00E0.B601.3B7A 的接口的 64 位接口 ID 为 02E0:B6FF:FE01:3B7A。

CR_Examples 以下示例为在内部接口上接收的 IPv6 地址启用 EUI-64 修改格式的实施：


```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

Related Commands

命令	说明
ipv6address	在接口上配置 IPv6 地址。
ipv6enable	在接口上启用 IPv6。

ipv6 icmp

要配置接口的 ICMP 访问规则，请在 **ipv6icmp** 全局配置模式下使用该命令。要删除 ICMP 访问规则，请使用此命令 **no** 的形式。

ipv6 icmp { **permit** | **deny** } { *ipv6-prefix/prefix-length* | **any** | **host***ipv6-address* } [*icmp-type*] *if-name*
no ipv6 icmp { **permit** | **deny** } { *ipv6-prefix/prefix-length* | **any** | **host***ipv6-address* } [*icmp-type*] *if-name*

Syntax Description

any	指定任何 IPv6 地址的关键字。IPv6 前缀 ::/0 的缩写。
deny	阻止选定接口上的指定 ICMP 流量。
host	表示引用特定主机的地址。
<i>icmp-type</i>	指定由访问规则过滤的 ICMP 消息类型。该值可以是有效的 ICMP 类型编号（0 至 255）或以下 ICMP 类型文字之一： • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
<i>if-name</i>	应用访问规则的接口的名称，由 nameif 命令指定。
<i>ipv6-address</i>	向接口发送 ICMPv6 消息的主机的 IPv6 地址。
<i>ipv6-prefix</i>	向接口发送 ICMPv6 消息的 IPv6 网络。

permit 允许选定接口上的指定 ICMP 流量。

prefix-length IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。

Command Default

如果未定义 ICMP 访问规则，则允许所有 ICMP 流量。

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。

8.2(1) 添加了对透明防火墙模式的支持。

使用指南

IPv6 中的 ICMP 功能与 IPv4 中的 ICMP 相同。ICMPv6 生成错误消息，例如 ICMP 目的地不可达消息以及信息性消息（例如 ICMP 回应请求和应答消息）。另外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现过程和路径 MTU 发现。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密会产生开销，因此 MTU 值不应设置为低于 1380。将接口设置为低于 1380 字节可能会导致数据包丢失。

如果没有为接口定义 ICMP 规则，则允许所有 IPv6 ICMP 流量。

如果为接口定义了 ICMP 规则，则系统按照“匹配优先”的顺序处理这些规则，然后是隐式“拒绝所有”规则。例如，如果第一个匹配的规则是允许规则，将处理 ICMP 数据包。如果第一个匹配的规则是拒绝规则，或者 ICMP 数据包未与该接口上的任何规则匹配，则 ASA 将丢弃该 ICMP 数据包并生成一条系统日志消息。

因此，输入 ICMP 规则的顺序非常重要。如果输入一条拒绝来自特定网络的所有 ICMP 流量的规则，然后遵循该规则的是允许来自该网络上的特定主机的 ICMP 流量的规则，系统将永远不会处理主机规则。ICMP 流量被网络规则阻止。但是，如果先输入主机规则，后输入网络规则，将允许主机 ICMP 流量，而阻止该网络中的所有其他 ICMP 流量。

ipv6icmp 命令为在 ASA 接口终止的 ICMP 流量配置访问规则。要配置传递 ICMP 流量的访问规则，请参阅 **ipv6access-list** 命令。

CR_Examples

以下示例拒绝所有 ping 请求并允许外部接口上的所有数据包过大消息（以支持路径 MTU 发现）：

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

以下示例允许主机 2000:0:0:4::2 或前缀 2001::/64 上的主机 ping 外部接口:

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

命令	说明
ipv6access-list	配置访问列表。

ipv6 local pool

要配置 IPv6 地址池，请在 **ipv6localpool** 全局配置模式下使用该命令。要删除池，请使用此命令的 **no** 形式。

ipv6 local pool *pool_name* *ipv6_address/prefix_length* *number_of_addresses*
no ipv6 local pool *pool_name* *ipv6_address/prefix_length* *number_of_addresses*

Syntax Description

<i>ipv6_address</i>	指定池的起始 IPv6 地址。
<i>number_of_addresses</i>	范围：1-16384。
<i>pool_name</i>	指定要分配给此 IPv6 地址池的名称。
<i>prefix_length</i>	范围：0-128。

Command Default

默认情况下，未配置 IPv6 本地地址池。

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

8.0(2) 添加了此命令。

9.0(1) 已为 **ipv6address** 命令中的集群池添加了 IPv6 本地池，以支持 ASA 集群。

使用指南

对于 VPN，要分配 IPv6 本地池，请在隧道组中使用 **ipv6-local-pool** 命令或在组策略中使用 **ipv6-address-pools** 命令（请注意此命令上的“s”）。组策略中的 **ipv6-address-pools** 设置覆盖隧道组中的 **ipv6-address-pools** 设置。

CR_Examples

以下示例配置名为 **firstipv6pool** 的 IPv6 地址池，以便用于向远程客户端分配地址：

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

Related Commands

命令	说明
ipv6-address-pool	将 IPv6 地址池与 VPN 隧道组策略关联。
ipv6-address-pools	将 IPv6 地址池与 VPN 组策略关联。
clear configure IPv6 local pool	清除所有已配置的 IPv6 本地池。
show running-config ipv6	显示 IPv6 的配置。

ipv6 nd dad attempts

要配置重复地址检测期间接口上连续发送的邻居请求消息的数量，请在接口配置模式下使用 **ipv6nddadattempts** 命令。要恢复到发送的重复地址检测消息的默认数量，请使用此命令的 **no** 形式。

ipv6 nd dad attempts 值
no ipv6 nd dad attempts 值

Syntax Description

value 介于 0 到 600 之间的数字。输入 0 将禁用指定接口上的重复地址检测。输入 1 配置单次传输，无后续传输。默认值为 1 条消息。

Command Default

默认尝试次数为 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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

8.2(1) 添加了对透明防火墙模式的支持。

使用指南

重复地址检测会在将新单播 IPv6 地址分配给接口之前验证其唯一性（在执行重复地址检测时，新地址保持暂定状态）。重复地址检测使用邻居请求消息来验证单播 IPv6 地址的唯一性。发送邻居请求消息的频率使用 **ipv6ndns-interval** 命令进行配置。

在管理上处于关闭状态的接口上，重复地址检测将被暂停。当接口处于管理性关闭状态时，单播 IPv6 地址将分配给设置为处于暂停状态的接口。

当接口恢复到管理性启用状态时，重复地址检测将在接口上自动重启。返回管理状态的接口将重新启动该接口上所有单播 IPv6 地址的重复地址检测。



注释

对接口的链路本地地址执行重复地址检测时，其他 IPv6 地址的状态仍会设置为暂定。对链路本地地址完成重复地址检测后，将对其余 IPv6 地址执行重复地址检测。

当重复地址检测识别到一个重复地址时，地址的状态设置为“重复”，并且不使用该地址。如果重复地址是接口的链路本地地址，则接口上会禁用 IPv6 数据包的处理，并发出类似以下内容的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

如果重复地址是接口的全局地址，则不会使用该地址，并会发出类似如下的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

当地址状态设置为 DUPLICATE 时，与重复地址相关的所有配置命令仍保持配置状态。

如果接口的链路本地地址发生变化，则会对新的链路本地地址执行重复地址检测，并重新生成与该接口关联的所有其他 IPv6 地址（仅对新的链路本地地址执行重复地址检测）。

CR Examples

以下示例将配置为在对接口的暂定单播 IPv6 地址执行重复地址检测时，发送 5 条连续的邻居请求消息：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

以下示例在所选接口上禁用重复地址检测：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

Related Commands

命令	说明
ipv6ndns-interval	配置接口上 IPv6 邻居请求传输之间的间隔。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd managed-config-flag

要将 ASA 配置为在 IPv6 路由器通告数据包中设置托管地址配置标志，请在接口配置模式下使用 **ipv6ndmanagedconfig-flag** 命令。要恢复默认设置，请使用此命令 **no** 的形式。

ipv6 nd managed-config-flag
no ipv6 managed-config-flag

Syntax Description 此命令没有任何参数或关键字。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

9.0(1) 添加了此命令。

使用指南 IPv6 自动配置客户端主机可使用此标志来指示其必须使用有状态地址配置协议 (DHCPv6) 来获取除派生的无状态自动配置地址之外的地址。

CR_Examples

以下示例在接口 GigabitEthernet 0/0 的 IPv6 路由器通告数据包中设置托管地址配置标志：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

Related Commands

命令	说明
ipv6ndother-config-flag	配置 ASA 以设置 IPv6 路由器通告数据包中的另一个配置标志。

ipv6 nd ns-interval

要配置接口上 IPv6 邻居请求重新传输之间的间隔，请在 **ipv6ndns-interval**接口配置模式下使用该命令。要恢复默认值，请使用此命 **no** 令的形式。

ipv6 nd ns-interval值
no ipv6 nd ns-interval [*value*]

Syntax Description	<i>value</i> IPv6 邻居请求传输之间的间隔（以毫秒为单位）。有效值范围为 1000 至 3600000 毫秒。默认值为 1000 毫秒。

Command Default	邻居请求传输之间的默认间隔为 1000 毫秒。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	8.2(1) 添加了对透明防火墙模式的支持。

使用指南	此值将包含在通过此接口发送的所有 IPv6 路由器通告中。

CR_Examples	以下示例为 GigabitEthernet 0/0 配置 9000 毫秒的 IPv6 邻居请求传输间隔：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Related Commands	命令	说明
	showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd other-config-flag

要将 ASA 配置为在 IPv6 路由器通告数据包中设置 other config 标志，请在接口配置模式下使用 **ipv6 nd other-config-flag** 命令。要恢复默认设置，请使用此命令 **no** 的形式。

ipv6 nd other-config-flag
no ipv6 other-config-flag

Syntax Description

此命令没有任何参数或关键字。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

IPv6 自动配置客户端主机可以使用此标志来指示它必须使用状态地址配置协议 (DHCPv6) 获取非地址配置信息，例如 DNS 服务器信息。

CR_Examples

以下示例在接口 GigabitEthernet 0/0 的 IPv6 路由器通告数据包中设置其他配置标志：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

Related Commands

命令	说明
ipv6 nd managed-config-flag	配置 ASA 以在 IPv6 路由器通告数据包中设置托管地址配置标志。

ipv6 nd prefix

要配置 IPv6 路由器通告中包含的 IPv6 前缀，请在接口配置模式下使用 **ipv6ndprefix** 命令。要删除前缀，请使用此命令的形式。

ipv6 nd

prefix *ipv6-prefix* [*prefix-length*] **default** [*valid-lifetime* *preferred-lifetime*] [*at valid-date* *preferred-date*] [*infinite*] **no-advertise** **off-link** **no-autoconfig**

no ipv6 nd

prefix *ipv6-prefix* [*prefix-length*] **default** [*valid-lifetime* *preferred-lifetime*] [*at valid-date* *preferred-date*] [*infinite*] **no-advertise** **off-link** **no-autoconfig**

Syntax Description

at valid-date preferred-date	生命周期和偏好到期的日期和时间。EXTEN 到达此指定的日期和时间之前，前缀均有效。日期以 <i>date-valid -expire month-valid -expire hh:mm-valid -expire date-prefer -expire month-prefer -expire hh:mm-prefer -expire</i> 的形式表示。
default	已使用默认值。
infinite	（可选）有效的生命周期不会到期。
ipv6-prefix	路由器通告中包含的 IPv6 网络号。 此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
no-advertise	（可选）向本地链路上的主机指示指定的前缀不用于 IPv6 自动配置。对于 default 前缀，此设置仅适用于 on-link 前缀。除非您为特定 Off-link 前缀指定 no-advertise ，否则系统仍将通告 Off-link 前缀。
no-autoconfig	（可选）向本地链路上的主机指示指定的前缀不能用于 IPv6 自动配置。
off-link	（可选）表示指定的前缀不用于链路上确定。
首选有效期限	指定 IPv6 前缀被宣传为首选的时间量（以秒为单位）。值的范围为 0 到 4294967295 秒。最大值代表无穷大，也可以使用 infinite 关键字指定。默认值为 604800 秒（7 天）。
prefix-length	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
valid-lifetime	指定 IPv6 前缀被宣传为有效的时间量。值的范围为 0 到 4294967295 秒。最大值代表无穷大，也可以使用 infinite 关键字指定。默认值为 2592000 秒（30 天）。

Command Default

在发起 IPv6 路由器通告的接口上配置的所有前缀均采用 2592000 秒（30 天）的有效生命周期和 604800 秒（7 天）的首选生命周期进行通告，并同时设置 “onlink” 和 “autoconfig” 标志。

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	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令允许控制每个前缀的各个参数，包括是否应通告该前缀。

默认情况下，使用该命令在接口上配置为地址的**ipv6address**前缀将在路由器通告中通告。如果您使用该命令配置要通告的 **ipv6ndprefix** 前缀，则仅通告这些前缀。

该关 **default** 键字可用于为所有前缀设置默认参数。

可以设置日期来指定前缀的过期日期。实时倒计时有效有效期和首选有效期。达到到期日期时，将不再通告前缀。

当 **onlink** 为 “on”（默认）时，指定的前缀将分配给链接。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可访问。

当自动配置处于 “开启” 状态（默认）时，它向本地链路上的主机指示指定的前缀可用于 IPv6 自动配置。

CR_Examples

以下示例包含 IPv6 前缀 2001:200::/35，在指定接口上发出的路由器通告中，有效生命周期为 1000 秒，首选生命周期为 900 秒：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

命令	说明
ipv6address	配置 IPv6 地址并在接口上启用 IPv6 处理。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd ra-interval

要配置接口上 IPv6 路由器通告传输之间的间隔，请在 **ipv6ndra-interval** 接口配置模式下使用该命令。
要恢复默认间隔，请使用此命令 **no** 的形式。

ipv6 nd ra-interval [*msec*] *value*
no ipv6 nd ra-interval [[*msec*] *value*]

Syntax Description

msec （可选）表示提供的值以毫秒为单位。如果不存在此关键字，则提供的值为秒。

value IPv6 路由器通告传输之间的间隔。有效值范围为 3 至 1800 秒，或 500 至 1800000 毫秒（如果提供了关键字 **msec**）。默认值为 200 秒。

Command Default

200 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
接口配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

如果使用该命令将 ASA 配置为默认路由器，则传输间隔应小于或等于 IPv6 路由器通告生存 **ipv6ndra-lifetime** 期。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为指定值的 20% 以内。

CR_Examples

以下示例为所选接口配置 201 秒的 IPv6 路由器通告间隔：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Related Commands

命令	说明
ipv6ndra-lifetime	配置 IPv6 路由器通告的有效期。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd ra-lifetime

要在接口上配置 IPv6 路由器通告中的“路由器有效期”值，请在接口配置模式下使用 **ipv6ndra-lifetime** 命令。要恢复默认值，请使用此命令 **no** 的形式。

ipv6 nd ra-lifetime秒
no ipv6 nd ra-lifetime [秒]

Syntax Description

seconds ASA 作为此接口上的默认路由器的有效性。值的范围为 0 到 9000 秒。默认值为 1800 秒。0 表示 ASA 不应被视为所选接口上的默认路由器。

Command Default

1800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
接口配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

通过接口发送的所有 IPv6 路由器通告中都包含“路由器寿命”值。此值表示 ASA 作为此接口的默认路由器的益处。

将该值设置为非零值表示应将 ASA 视为此接口上的默认路由器。“路由器寿命”值的非零值不应小于路由器通告间隔。

将值设置为 0 表示 ASA 不应被视为此接口上的默认路由器。

CR_Examples

以下示例为所选接口配置 1801 秒的 IPv6 路由器通告有效期限：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

命令	说明
ipv6ndra-interval	配置接口上 IPv6 路由器通告传输之间的间隔。

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd reachable-time

要配置在发生可达性确认事件后远程 IPv6 节点被视为可达的时间量，请在 **ipv6ndreachable-time** 接口配置模式下使用该命令。要恢复默认时间，请使用此命令 **no** 的形式。

ipv6 nd reachable-time 值
no ipv6 nd reachable-time [*value*]

Syntax Description

value 远程 IPv6 节点被视为可达的时间量（以毫秒为单位）。有效值范围为 0 至 3600000 毫秒。默认值为 0。

当 值 参数使用 0 时，可达时间将作为未确定时间发送。由接收设备来设置和跟踪可访问时间的值。

Command Default

零毫秒。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

8.2(1) 添加了对透明防火墙模式的支持。

使用指南

配置的时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快；但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

要查看 ASA 使用的可访问时间（包括此命令设置为 0 时的实际值），请使用 **showipv6interface** 命令显示有关 IPv6 接口的信息，包括正在使用的 ND 可访问时间。

CR_Examples

以下示例为所选接口配置 1700000 毫秒的 IPv6 可访问时间：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd suppress-ra

要抑制 IPv6 路由器通告在 LAN 接口上的传输，请在接口配置模式下使用 **ipv6 nd suppress-ra** 命令。
要在 LAN 接口上重新启用发送 IPv6 路由器通告传输，请使用此命令的 **no** 形式。

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

此命令没有任何参数或关键字。

Command Default

如果启用了 IPv6 单播路由，将在 LAN 接口上自动发送路由器通告。

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	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

使用 **no ipv6 nd suppress-ra** 命令，可在非 LAN 接口类型（例如串行接口或隧道接口）上启用 IPv6 路由器通告传输。

CR_Examples

以下示例抑制所选接口上的 IPv6 路由器通告：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

Related Commands

命令	说明
show ipv6 interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 neighbor

要在 IPv6 邻居发现缓存中配置静态条目，请在全局配置模式下使用 **ipv6neighbor** 命令。要从邻居发现缓存中删除静态条目，请使用此命令的 **no** 形式。

```
ipv6 neighboripv6_addressif_namemac_address
no ipv6 neighboripv6_addressif_name [mac_address]
```

Syntax Description	if_name	由 nameif 命令指定的内部或外部接口名称。
	ipv6_address	与本地数据链路地址对应的 IPv6 地址。
	mac_address	本地数据线路（硬件 MAC）地址。

Command Default 静态条目不在 IPv6 邻居发现缓存中配置。

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。
	8.2(1) 添加了对透明防火墙模式的支持。

使用指南 该**ipv6neighbor**命令与该 **arp**命令类似。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用该命令存储配置时，**copy**这些条目将存储在配置中。

使用该 **showipv6neighbor**命令查看 IPv6 邻居发现缓存中的静态条目。

该**clearipv6neighbors**命令将删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。The **noipv6neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. 使用该命令禁用接口上的 **noipv6enable**IPv6 将会删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目除外（条目的状态更改为 INCOMPLETE [Incomplete]）。

邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。

CR_Examples

以下示例将 IPv6 地址为 3001:1::45A 和 MAC 地址为 0002.7D1A.9472 的内部主机的一个静态条目添加到邻居发现缓存：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

命令	说明
clearipv6neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。
showipv6neighbor	显示 IPv6 邻居缓存信息。

ipv6 ospf

要启用 IPv6 的 OSPFv3 接口配置，请在 **ipv6ospf** 全局配置模式下使用该命令。要禁用用于 IPv6 的 OSPFv3 接口配置，请使用此命令的 **no** 形式。

ipv6

ospf *[process-id]* *[cost]* *[database-filter database-filter-name]* *[flood-reduction]* *[hello-interval seconds]* *[mtu-ignore]* *[neighbor network priority]* *[transmit-delay seconds]*

no ipv6

ospf *[process-id]* *[cost]* *[database-filter database-filter-name]* *[flood-reduction]* *[hello-interval seconds]* *[mtu-ignore]* *[neighbor network priority]* *[transmit-delay seconds]*

Syntax Description

cost	显式指定在接口上发送数据包的成本。
database-filter	过滤发往 OSPFv3 接口的传出 LSA。
dead-interval 秒	设置在邻居指示路由器已关闭之前不得看到 hello 数据包的时间段（以秒为单位）。该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。默认值是命令设置的间隔的 ipv6ospfhello-interval 四倍。
flood-reduction	指定到接口的 LSA 泛洪减少量。
hello-interval 秒	指定接口上发送 hello 数据包之间的间隔（以秒为单位）。该值必须对于特定网络上的所有节点都相同，并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒，对于非广播接口为 30 秒。
mtu-ignore	收到 DBD 数据包时禁用 OSPF MTU 不匹配检测。默认情况下，OSPF MTU 不匹配检测已启用。
neighbor	配置 OSPFv3 路由器与非广播网络的互连。
network	将 OSPF 网络类型设置为默认类型以外的类型，这取决于网络类型。
priority	设置路由器优先级，帮助确定网络的指定路由器。有效值范围为 0 到 255。
process-id	指定要启用的 OSPFv3 进程。有效值范围为 1 到 65535。
retransmit-interval 秒	指定属于该接口的邻接关系的 LSA 重新传输之间的时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
transmit-delay 秒	设置在接口上发送链路状态更新数据包的预计时间（以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。

Command Default

默认情况下，包含所有 IPv6 地址。

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	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

您必须先启用 OSPFv3 路由进程，然后才能创建 OSPFv3 区域。

CR_Examples

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf area

要为 IPv6 创建 OSPFv3 区域，请在全局配置模式下使用 **ipv6 ospf area** 命令。要禁用 IPv6 的 OSPFv3 区域配置，请使用此命令的 **no** 形式。

ipv6 ospf area [*area-num*] [*instance*]
no ipv6 ospf area [*area-num*] [*instance*]

Syntax Description

area-num 指定要启用的 OSPFv3 区域。

instance 指定要分配给接口的区域实例 ID。

Command Default

默认情况下，包含所有 IPv6 地址。

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	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

您必须在每个接口上单独配置 OSPFv3 路由。接口只能有一个 OSPFv3 区域，并且 ASA 的 OSPFv3 仅支持每个接口一个实例。每个接口使用不同的区域实例 ID。区域实例 ID 仅影响 OSPF 数据包的接收，并适用于普通 OSPF 接口和虚拟链路。

CR_Examples

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf cost

要明确指定在接口上发送数据包的开销，请在接口配置模式下使用 **ipv6 ospf cost** 命令。要将接口上发送数据包的成本重置为默认值，请使用此命令的 **no** 形式。

ipv6 ospf cost *interface-cost*
no ipv6 ospf cost *interface-cost*

Syntax Description

interface-cost 指定表示链路状态度量的无符号整数值，范围从 1 到 65535。

Command Default

默认开销基于带宽。

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	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令可明确指定接口的数据包开销。

CR_Examples

以下示例将数据包开销设置为 65：

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

Related Commands

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf database-filter all out

要过滤发往 OSPFv3 接口的传出 LSA，请在 **ipv6ospfdatabse-filterallout** 接口配置模式下使用该命令。要恢复将 LSA 转发到接口，请使用此命令的 **no** 形式。

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

Syntax Description 此命令没有任何参数或关键字。

Command Default 所有传出的 LSA 均会泛洪至该接口。

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	• 支持	• 支持	—	—

Command History 版本 修改

9.0(1) 添加了此命令。

使用指南 使用此命令可以过滤发往 OSPFv3 接口的传出 LSA。

CR_Examples 以下示例将筛选到指定接口的传出 LSA：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf dead-interval

要设置在邻居声明路由器已关闭之前不得看到 hello 数据包的时间段，请在 **ipv6ospfdead-interval** 接口配置模式下使用该命令。要返回默认时间，请使用此命令 **no** 的形式。

ipv6 ospf dead-interval秒
no ipv6 ospf dead-interval秒

Syntax Description

秒指定间隔（以秒为单位）。网络中的所有节点的值必须相同。有效值范围为 1 到 65535。

Command Default

默认值是命令设置的间隔的 **ipv6ospfhello-interval** 四倍。

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	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭之前，看不到呼叫数据包的时间间隔。

CR_Examples

以下示例将 dead 间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf encryption

要指定接口的加密类型，请在 **ipv6ospfencryption** 接口配置模式下使用该命令。要删除接口的加密类型，请使用此命令的 **no**形式。

```
ipv6 ospf
encryption { ipsec spi esp encryption-algorithm [ [key-encryption-type] key] authentication-algorithm [key-encryption-type] key | null }
no ipv6 ospf
encryption { ipsec spi esp encryption-algorithm [ [key-encryption-type] key] authentication-algorithm [key-encryption-type] key | null }
```

Syntax Description	authentication-algorithm 指定要使用的加密算法。有效值为以下值之一： —md5启用消息摘要 5 (MD5)。 —sha1启用 SHA-1。
加密算法-	指定与 ESP 一起使用的加密算法。。有效值包括以下值： —aes-cdc启用 AES-CDC 加密。 —3des启用 3DES 加密。 —启des用 DES 加密。 —null指定不加密的 ESP。
esp	指定封装安全有效载荷 (ESP)。
ipsec	指定 IP 安全协议。
key	指定在计算消息摘要时使用的数字。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
key-encryption-type	（可选）指定密钥加密类型，可以是以下值之一： • 0- 密钥未加密。 • —7密钥已加密。
null	覆盖区域身份验证。
spi spi	指定 安全策略索引 (SPI) 值。spi 值必须为 256 到 4294967295 之间的数字，且须以十进制形式输入。

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
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令指定接口的加密类型。

CR_Examples

以下示例在接口上启用 SHA-1 加密：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf flood-reduction

要指定到接口的 LSA 泛洪减少，请在接口配置模式下使用该 **ipv6ospfflood-reduction** 命令。要取消对接口的 LSA 泛洪减少，请使用此命令的 **no** 形式。

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

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
接口配置	• 是	• 支持	• 支持	—	—

Command History 版本 修改

9.0(1) 添加了此命令。

使用指南 使用此命令指定到接口的 LSA 泛洪减少。

CR_Examples 以下示例启用减少到接口的 LSA 泛洪：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200vlan 200 nameif outside security-level
100 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31 ipv6 address 3001::1/64
standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6
ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf flood reduction
```

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf hello-interval

要设置在邻居声明路由器已关闭之前不得看到 hello 数据包的时间段，请在 **ipv6ospfdead-interval** 接口配置模式下使用该命令。要返回默认时间，请使用此命令 **no** 的形式。

ipv6 ospf dead-interval秒
no ipv6 ospf dead-interval秒

Syntax Description

秒指定间隔（以秒为单位）。网络中的所有节点的值必须相同。有效值范围为 1 到 65535。

Command Default

如果使用的是以太网，则默认间隔为 10 秒；如果使用的是非广播，则默认间隔为 30 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
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭之前，看不到呼叫数据包的时间间隔。

CR_Examples

以下示例将 dead 间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf mtu-ignore

要在 ASA 接收数据库描述符 (DBD) 数据包时禁用 OSPFv3 最大传输单元 (MTU) 不匹配检测，请在接口配置模式下使用 **ipv6ospfmtu-ignore** 命令。要在 ASA 接收 DBD 数据包时将 MTU 不匹配检测重置为默认值，请使用此命令的 **no** 形式。

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

Syntax Description	此命令没有任何参数或关键字。				
Command Default	默认情况下，OSPFv3 MTU 不匹配检测处于启用状态。				
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	• 支持	• 支持	—	—

Command History	版本	修改
	9.0(1)	添加了此命令。

使用指南 使用此命令可在 ASA 接收 DBD 数据包时禁用 OSPFv3 MTU 不匹配检测。

CR_Examples 以下示例在 ASA 接收 DBD 数据包时禁用 OSPFv3 MTU 不匹配检测：

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

Related Commands	命令	说明
	clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
	debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf neighbor

要配置与非广播网络的 OSPFv3 路由器互连，请在接口配置模式下使用 **ipv6ospfneighbor** 命令。当达到最大数量（由邻居最大前缀命令设置）时，条目中 **no** 会出现字符串 “PfxRcd”，邻居被关闭，连接处于空闲状态。

ipv6 ospf neighbor*ipv6-address* [**priority***number*] [**poll-interval***秒*] [**cost***number*] [**database-filter**]
no ipv6 ospf neighbor*ipv6-address* [**priority***number*] [**poll-interval***秒*] [**cost***number*] [**database-filter**]

Syntax Description

cost 编号	（可选）以 1 到 65535 之间的整数形式为邻居分配开销。未配置特定开销的邻居会根据 ipv6ospfcost 命令采用接口的开销。
database-filter	（可选）过滤到 OSPF 邻居的传出链路状态通告 (LSA)。
ipv6-address	邻居的链路本地 IPv6 地址。此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
poll-interval 秒	（可选）表示轮询间隔时间（以秒为单位）的数字值。RFC 2328 建议将此值远大于呼叫间隔。默认值为 120 秒（两分钟）。此关键字不适用于点对多点接口。
priority 编号	（可选）一个数字，表示与指定 IPv6 前缀关联的非广播邻居的路由器优先级值。默认值为 0。

Command Default

默认值取决于网络类型。

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	•	•		—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令配置 OSPFv3 路由器与非广播网络的互连。

CR_Examples

以下示例配置 OSPFv3 邻居路由器：

```
ciscoasa(config)# interface serial 0
```

```
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf network

要将 OSPFv3 网络类型配置为默认类型以外的其他类型，请在接口配置模式下使用 **ipv6 ospf network** 命令。要返回默认类型，请使用此命令的 **no** 形式。

ipv6 ospf network { broadcast | point-to-pointnon-broadcast }
no ipv6 ospf network { broadcast | point-to-pointnon-broadcast }

Syntax Description

广播 将网络类型设置为广播。
point-to-pointnon-broadcast 将网络类型设置为点对点非广播。

Command Default

默认值取决于网络类型。

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	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令可将 OSPFv3 网络类型配置为不同于默认值的类型。

CR_Examples

以下示例将 OSPFv3 网络设置为广播网络：

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf priority

要设置路由器优先级（这有助于为指定网络确定指定路由器），请在接口配置模式下使用 **ipv6 ospf priority** 命令。要返回默认值，请使用此 **no** 命令形式。

ipv6 ospf priority *number-value*
no ipv6 ospf priority *number-value*

Syntax Description	<i>number-value</i> 设置用于指定路由器优先级的数字值。有效值范围为 0 到 255。
Command Default	默认优先级为 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
接口配置	• 是	—	• 是	—	—

Command History	版本 修改
	9.0(1) 添加了此命令。

使用指南 使用此命令可设置路由器的优先级。

CR_Examples 以下示例将路由器的优先级设置为 4:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

Related Commands	命令	说明
	clear ipv6 ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
	ipv6 ospf retransmit-interval	指定属于该接口的邻接关系的 LSA 重新传输之间的时间。

ipv6 ospf retransmit-interval

要指定属于该接口的邻接关系的 LSA 重新传输之间的时间，请在 **ipv6ospfretransmit-interval** 接口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。

ipv6 ospf retransmit-interval秒

no ipv6 ospf retransmit-interval秒

Syntax Description

秒指定两次重新传输的间隔时间（以秒为单位）。该间隔必须大于所连接网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。

Command Default

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
接口配置	• 是	—	• 是	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

使用此命令可以指定属于该接口的邻接关系的 LSA 重新传输之间的时间。

CR_Examples

以下示例将重新传输间隔设置为 8 秒：

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

Related Commands

命令	说明
ipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf transmit-delay

如要设置在接口上发送链路状态更新数据包所需的估计时间，请在接口配置模式下使用 **ipv6ospftransmit-delay** 命令。要返回默认值，请使用此 **no** 命令形式。

ipv6 ospf transmit-delay秒
no ipv6 ospf transmit-delay秒

Syntax Description 秒指定发送链路状态更新所需的时间（以秒为单位）。有效值的范围为 1 到 65535 秒。

Command Default 默认值为 1 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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南 使用此命令设置在接口上发送链路状态更新数据包所需的估计时间。

CR_Examples 以下示例将传输延迟设置为 3 秒：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6-prefix

要为映射地址和端口 (MAP) 域中的基本映射规则配置 IPv6 前缀，请在 MAP 域基本映射规则配置模式下使用 **ipv6-prefix** 命令。使用此命令的形式来删除前缀。

ipv6-prefix*ipv6_prefix/prefix_length*
no ipv6-prefix*ipv6_prefix/prefix_length*

Syntax Description

ipv6_prefix/prefix_length IPv6 前缀定义客户边缘 (CE) 设备的 IPv6 地址的地址池。指定 IPv6 前缀和前缀长度，通常为 64，但不能小于 8。不能在不同 MAP 域中使用相同的 IPv6 前缀。

Command Default

无默认值。

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
MAP域基本映射规则配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改

9.13(1)	引入了此命令。

使用指南

IPv6 前缀定义 CE 设备 IPv6 地址的地址池。只有当数据包的目标地址具有该前缀，源地址具有默认映射规则中定义的 IPv6 前缀，且在正确的端口范围内时，MAP 才会将 IPv6 数据包翻译回 IPv4。任何从其他地址发送到 CE 设备的 IPv6 数据包都会被简单地作为 IPv6 流量处理，而不会进行 MAP 转换。来自 MAP 源/目的池但端口超出范围的数据包会被直接丢弃。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
```

```
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024

ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

ipv6 prefix-list

要在 IPv6 前缀列表中创建条目，请在全局配置模式下使用 **ipv6prefix-list** 命令。要删除条目，请使用此命令 **no** 的形式。

ipv6

prefix-list*list-name* [**seq***seq-number*] { **deny***ipv6-prefix* | *prefix-length* | **description***text* } [**ge***ge-value*] [**le***le-value*]
no ipv6 prefix-list*list-name*

Syntax Description

<i>list-name</i>	前缀列表的名称。 名称不能与现有访问列表相同。 注释 名称不能为“detail”或“summary”，因为它们是关键字。
seq <i>seq-number</i>	（可选）正在配置的前缀列表条目的序列号。
deny	拒绝符合条件的网络。
permit	允许符合条件的网络。
<i>ipv6-prefix</i>	向指定前缀列表分配的 IPv6 网络。 此参数必须采用 RFC 2373 中记录的形式，其中地址是用冒号分隔的十六进制 16 位值。
<i>prefix-length</i>	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
description 文本、	前缀列表的说明，最长可以为 80 个字符。
ge <i>ge-value</i>	（可选）指定前缀长度大于或等于 <i>ipv6-prefix/prefix-length</i> 参数。它是长度范围（长度范围的“起始”部分）的最小值。
le <i>le-value</i>	（可选）指定小于或等于 <i>ipv6-prefix/prefix-length</i> 参数的前缀长度。它是一个长度范围（长度范围的“至”部分）的最大值。

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

9.3(2) 添加了此命令。

Related Commands

命令	说明
showipv6prefix-list	显示 IPv6 前缀列表。
showipv6route	显示 IPv6 路由表的当前内容。

ipv6 route

要将 IPv6 路由添加到 IPv6 路由表，请在 **ipv6route** 全局配置模式下使用该命令。要删除 IPv6 默认路由，请使用此命令的形式。

ipv6 route *if_name* *ipv6-prefix* | *prefix-length* *ipv6-address* [*management-distance* | **tunneled**]
no ipv6 route *if_name* *ipv6-prefix* | *prefix-length* *ipv6-address* [*management-distance* | **tunneled**]

Syntax Description

<i>administrative-distance</i>	（可选）路由的管理距离。默认值为 1，这表示静态路由优先于任何其他类型的路由（连接路由除外）。
<i>if_name</i>	正在为其配置路由的接口的名称。
<i>ipv6-address</i>	可用于到达指定网络的下一跳的 IPv6 地址。
<i>ipv6-prefix</i>	作为静态路由目的的 IPv6 网络。 此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
<i>prefix-length</i>	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
tunneled	（可选）将路由指定为 VPN 流量的默认隧道网关。

Command Default

默认情况下，管理距离为 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。

8.2(1) 添加了对透明防火墙模式的支持。

使用指南

使用命令查看 IPv6 **show ipv6 route** 路由表的内容。

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：

- 不要在隧道路由的出口接口上启用单播 RPF（**ipverifyreverse-path** 命令）。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。这样做会导致会话失败。
- 请勿使用 VoIP 检查引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP 或 SKINNY）、DNS 检查引擎或带有隧道路由的 DCE RPC 检查引擎。这些检测引擎会忽略隧道路由。

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

CR_Examples

以下示例将网络 7fff::0/32 的数据包路由到位于 3FFE:1100:0:CC00::1 上的内部接口上的网络设备，管理距离为 110：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

命令	说明
debugipv6route	显示 IPv6 路由表更新和路由缓存更新的调试消息。
showipv6route	显示 IPv6 路由表的当前内容。

ipv6 router ospf

要创建 OSPFv3 路由进程并进入 IPv6 路由器配置模式，请在 **ipv6routerospf** 全局配置模式下使用该命令。

ipv6 router ospf*process-id*

Syntax Description

process-id 指定内部标识，该标识是本地分配的，可以是 1 到 65535 之间的正整数。使用的号码是当您为 IPv6 路由进程启用 OSPFv3 时管理分配的号码。

Command Default

无默认为行为或值。

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	—	• 是	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

ipv6routerospf命令是用于在 ASA 上运行的 OSPFv3 路由进程的全局配置命令。输入 **ipv6routerospf** 命令后，命令提示符显示为 (config-rtr)#，表示您处于 IPv6 路由器配置模式。

使用 **noipv6routerospf**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。

noipv6routerospf命令终止由其 *process-id* 参数指定的 OSPFv3 路由进程。在 ASA 上本地分配 *process-id* 值。必须为每个 OSPFv3 路由进程分配唯一值。您最多可以使用两个进程。

在 IPv6 路由器配置模式下，使用 **ipv6routerospf** 命令，通过以下特定于 OSPFv3 的选项配置 OSPFv3 路由进程：

- —**area**置 OSPFv3 区域参数。支持的参数包括从 0 到 4294967295 的十进制值区域 ID 和 的 IP 地址格式的区域 ID。 **A.B.C.D**
- —**default**将命令设置为其默认值。该 **originate**参数分发默认路由。
- —**default-information**控制默认信息的分发。
- —**distance**根据路由类型定义 OSPFv3 路由管理距离。支持的参数包括管理距离（值从 1 到 254）和 **ospf**OSPF 距离。

- 退出**exit**—IPv6 路由器配置模式。
- **lsa ignore**—当路由器接收到第 6 类多播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制发送带有该参数的系统日志消息。
- **log-adjacency-changes**—配置路由器在 OSPFv3 邻居启动或关闭时发送系统日志消息。通过该 **detail** 参数，所有状态变化都会被记录下来。
- **passive-interface**—使用以下参数抑制接口上的路由更新：
 - **GigabitEthernet**—指定千兆以太网 IEEE 802.3z 接口。
 - **Management**—指定管理接口。
 - **Port-channel**—指定接口的以太网通道。
 - **Redundant**—指定冗余接口。
 - **default**—抑制所有接口上的路由更新。
- **redistribute**—根据以下参数配置从一个路由域到另一个路由域的路由重新分配：
 - **connected**—指定连接的路线。
 - **ospf**—指定 OSPF 路由。
 - **static**—指定静态路由。
- **router-id**—使用以下参数为指定进程创建固定路由器 ID：
 - **A.B.C.D**—以 IP 地址格式指定 OSPF 路由器 ID。
 - **cluster-pool**—配置第 3 层集群时配置 IP 地址池。
- **summary-prefix**—配置 IPv6 地址摘要，有效值为 0 至 128。该 **X:X:X:X::X/X** 参数指定 IPv6 前缀。
- **timers**—使用以下参数调整路由计时器：
 - **lsa**—指定 OSPF LSA 计时器。
 - **pacing**—指定 OSPF 定步计时器。
 - **throttle**—指定 OSPF 节流计时器。

CR_Examples

以下示例启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式：

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

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6-split-tunnel-policy

要设置 IPv6 分割隧道策略，请在 group-policy 配置模式下使用 **ipv6-split-tunnel-policy** 命令。要从运行配置中删除 **ipv6-split-tunnel-policy** 属性，请使用此命令的 **no** 形式。

```
ipv6-split-tunnel-policy { tunnelall | tunnelspecified | excludespecified }
no ipv6-split-tunnel-policy
```

Syntax Description	excludespecified	定义流量明文传输到的网络列表。对于想要访问本地网络上的设备（如打印机），而通过隧道连接到公司网络的用户来说，此功能非常有用。
	ipv6-split-tunnel-policy 表示正在设置隧道流量规则。	
	tunnelall	指定流量不会被明文传送或流向 ASA 以外的任何其他目标。远程用户通过公司网络访问互联网，没有访问本地网络的权限。
	tunnelspecified	通过隧道传送进出指定网络的所有流量。此选项可启用分割隧道。它允许您创建要通过隧道传送的地址的网络列表。发往所有其他地址的数据均以明文形式传输，并由远程用户的互联网服务提供商进行路由。

Command Default IPv6 分割隧道默认为禁用状态，即 **tunnelall**。

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
组策略配置	• 是	—	• 是	—	—

Command History	版本 修改
	9.0(1) 添加了此命令。

使用指南 IPv6 分割隧道主要是一种流量管理功能，而不是安全功能。事实上，为了获得最佳安全性，我们建议您不要启用 IPv6 拆分隧道。

这使得可以从另一个组策略继承 IPv6 分割隧道的值。

IPv6 分割隧道允许远程访问 VPN 客户端有条件地以加密形式将数据包定向到 IPsec 或 SSL IPv6 隧道，或者以明文形式定向到网络接口。启用 IPv6 分割隧道后，未绑定到 IPsec 或 SSL VPN 隧道终端另一端的目標的数据包不必加密，通过隧道发送，解密，然后路由到最终目标。

此命令将 IPv6 分割隧道策略应用于特定网络。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略设置仅为指定网络建立隧道的拆分隧道策略：

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-split-tunnel-policy tunnelspecified
```

Related Commands

命令	说明
split-tunnel-network-listnone	表示分割隧道不存在访问列表。所有流量都通过隧道传输。
split-tunnel-network-listvalue	标识 ASA 用于区分需要建立隧道和不需要建立隧道的网络的访问列表。

ipv6-vpn-address-assign

要指定向远程访问客户端分配 IPv6 地址的方法，请在 **ipv6-vpn-addr-assign**全局配置模式下使用该命令。要从配置中删除该属性，请使用此命令的 **no**版本。要从 ASA 中删除所有已配置的 VPN 地址分配方法，请使用此命令的 **no**版本。不带参数。

```
ipv6-vpn-addr-assign { aaa | local }
no ipv6-vpn-addr-assign { aaa | local }
```

Syntax Description	aaa ASA 根据每个用户从外部或内部（本地）AAA（身份验证、授权和记帐）服务器检索地址。如果使用已配置 IP 地址的身份验证服务器，建议使用此方法。
	local ASA 会从内部配置的地址池中分配 IPv6 地址。

Command Default 默认情况下，会启用 AAA 和本地 VPN 地址分配选项。

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
	9.0(1) 添加了此命令。
	9.5(2) 增加了多情景模式支持。

使用指南 ASA 可以使用 AAA 或本地方法为远程访问客户端分配 IPv6 地址。如果配置多个地址分配方法，ASA 将搜索每个选项，直到找到 IPv6 地址。

CR_Examples 以下示例显示如何配置 AAA 作为地址分配方法。

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

以下示例显示如何配置使用本地地址池作为地址分配方法。

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

Related Commands

命令	说明
ipv6localpool	配置要用于 VPN 组策略的 IPv6 地址池。
show running-config group-policy	显示所有组策略或特定组策略的配置。
vpn-addr-assign	指定为远程访问客户端分配 IPv4 地址的方法。

ipv6-vpn-filter

要指定用于 VPN 连接的 IPv6 ACL 的名称，请在 **ipv6-vpn-filter**策略组配置或用户名配置模式下使用该命令。要删除 ACL（包括通过发出命令创建的 **ipv6-vpn-filternone**空值），请使用此命令的 **no**形式。

```
ipv6-vpn-filter {valueIPv6 ACL 名称| none}  
no ipv6-vpn-filter
```

Syntax Description	none	指示没有访问列表。设置一个空值，从而禁止访问列表。防止从其他组策略继承访问列表。
	valueIPv6 ACL 名称	提供先前配置的访问列表的名称。

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
组策略配置	• 是	—	• 是	—	—
用户名配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。
	9.0(1) 该 ipv6-vpn-filter 命令已被弃用。使用 vpn-filter 命令来配置具有 IPv4 和 IPv6 条目的统一过滤器。仅当 vpn-filter 命令指定的访问列表中 没有 IPv6 条目时，才会使用此 IPv6 过滤器。
	9.1(4) ipv6-vpn-filter 命令已禁用，仅允许使用该命令的“no”形式。使用 vpn-filter 命令为 IPv4 和 IPv6 条目配置统一过滤器。如果错误地使用此命令指定 IPv6 ACL，则连接将终止。

使用指南 无客户端 SSL VPN 不使用命令中定义的 **ipv6-vpn-filter**ACL。

no 选项允许从其他组策略继承值。为了防止继承值，请使 **ipv6-vpn-filternone**用命令。

您配置 ACL 来为此用户或组策略允许或拒绝各种类型的流量。然后，使用 **ipv6-vpn-filter** 命令以应用这些 ACL。

CR_Examples

以下示例显示如何设置一个过滤器，该过滤器为名为FirstGroup的组策略调用名为ipv6_acl_vpn的访问列表：

```
ciscoasa
(config)#
  group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
  ipv6-vpn-filter value ipv6_acl_vpn
```

Related Commands

命令	说明
access-list	创建访问列表，或使用可下载访问列表。
vpn-filter	指定要用于 VPN 连接的 IPv4 或 IPv6 ACL 的名称。

ip verify reverse-path

要启用单播 RPF，请在 **ipverifyreverse-path**全局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。

```
ip verify reverse-path interfaceinterface_name
no ip verify reverse-path interfaceinterface_name
```

Syntax Description *interface_name* 要在其上启用单播 RPF 的接口。

Command Default 默认情况下会禁用此功能。

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。

使用指南 单播 RPF 根据路由表来确保所有数据包均有与正确的源接口匹配的源 IP 地址，从而避免 IP 欺骗（即数据包使用不正确的源 IP 地址以掩盖其真正来源）。

通常，ASA 在确定将数据包转发到何处时仅查看目标地址。单播 RPF 指示 ASA 也查看源地址；这就是它被称为反向路径转发的原因。对于您想要允许通过 ASA 的任何流量，ASA 路由表必须包含返回源地址的路由。有关详细信息，请参阅 RFC 2267。

例如，对于外部流量，ASA 可以使用默认路由来满足单播 RPF 保护。如果流量从外部接口进入，并且路由表不知道源地址，则 ASA 使用默认路由将外部接口正确识别为源接口。

如果流量从路由表已知但与内部接口关联的地址进入外部接口，则ASA会丢弃该数据包。类似地，如果流量从未知源地址进入内部接口，ASA 会丢弃该数据包，因为匹配的路由（默认路由）指示的是外部接口。

单播 RPF 的实施过程如下：

- ICMP 数据包没有会话，因此要检查每个数据包。

- UDP和TCP有会话，因此初始数据包要求反向路由查找。对于在会话期间到达的后续数据包，使用作为部分会话来维护的现有状态进行检查。检查非初始数据包以确保它们到达初始数据包使用的同一接口。

CR_Examples

以下示例在外部接口上启用单播 RPF：

```
ciscoasa(config)# ip verify reverse-path interface outside
```

Related Commands

命令	说明
clearconfigureipverifyreverse-path	使用命令清除配置 ipverifyreverse-path 集。
clearipverifystatistics	清除单播 RPF 统计信息。
showipverifystatistics	显示单播 RPF 统计数据。
showrunning-configipverifyreverse-path	显示使用该命令设置的 ipverifyreverse-path 配置。

ipv6 未编号

要从接口（例如，环回接口）借用或继承 IPv6 地址，请在接口配置模式下使用 **ipv6unnumbered** 命令。要停止从接口继承 IP 地址，请使用此命令的 **no**形式。

ipv6unnumbered *interface-name*
no ipv6 unnumbered

Syntax Description *interface-name* 指定要继承 IPv6 地址的接口的名称。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南 `ipv6 unnumbered` 命令用于继承所选 接口 的 IPv6 地址，作为当前接口的地址。

CR_Examples

以下示例从环回接口借用 IPv6 地址，并将其用于 VTI 隧道接口：

```
ciscoasa(config)# interface tunnel 1
ciscoasa(conf-if)# ipv6 unnumbered loopback1
```

命令	说明
ipunnumbered <i>interface-name</i>	继承指定接口的 IP 地址。
interfaceloopback <i>loopback-number</i>	创建环回接口。



is – iz

- [isakmp am-disable](#)（已弃用），第 318 页
- [isakmp disconnect-notify](#) (已弃用)，第 319 页
- [isakmp enable](#)（已弃用），第 320 页
- [isakmp identity](#) (已弃用)，第 321 页
- [isakmp ipsec-over-tcp](#) (已弃用)，第 323 页
- [isakmp keepalive](#)，第 324 页
- [isakmp nat-traversal](#)（已弃用），第 326 页
- [isakmp policy authentication](#)，第 328 页
- [isakmp policy encryption](#)（已弃用），第 330 页
- [isakmp policy group](#)（已弃用），第 332 页
- [isakmp policy hash](#)（已弃用），第 334 页
- [isakmp policy lifetime](#)（已弃用），第 336 页
- [isakmp reload-wait](#) (已弃用)，第 338 页
- [isis priority](#)，第 339 页
- [isis protocol shutdown](#)，第 343 页
- [isis retransmit-interval](#)，第 347 页
- [isis retransmit-throttle-interval](#)，第 351 页
- [isis tag](#)，第 355 页
- [is-type](#)，第 359 页
- [issuer](#) (Deprecated)，第 363 页
- [issuer-name](#)，第 365 页

isakmp am-disable（已弃用）

要禁用入站积极模式连接，请在全局配置模式下使用**isakmpam-disable** 命令。要启用入站积极模式连接，请使用此命令的 **no** 形式。

isakmp am-disable
no isakmp am-disable

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认值为启用。

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
	7.0(1) 添加了此命令。
	7.2(1) 此命令已弃用。该 cryptoisakmpam-disable 命令取而代之。

CR_Examples 以下示例在全局配置模式下禁用入站积极模式连接：

```
ciscoasa(config)# isakmp am-disable
```

Related Commands	命令	说明
	clearconfigureisakmp	清除所有 ISAKMP 配置。
	clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
	clearisakmpsa	清除 IKE 运行时间 SA 数据库。
	showrunning-configisakmp	显示所有活动配置。

isakmp disconnect-notify (已弃用)

要启用向对等体发送断开连接通知，请在全局配置模式下使用 **isakmpdisconnect-notify** 命令。要禁用断开连接通知，请使用此命令 **no** 的形式。

isakmp disconnect-notify
no isakmp disconnect-notify

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认值为禁用。

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
全局配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。该 **cryptoisakmpdisconnect-notify** 命令取而代之。

CR_Examples

以下示例在全局配置模式下输入，启用向对等体发送断开连接通知：

```
ciscoasa(config)# isakmp disconnect-notify
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp enable（已弃用）

要在 IPsec 对等体与 ASA 通信的接口上启用 ISAKMP 协商，请在全局配置模式下使用该**isakmpenable** 命令。要在接口上禁用 ISAKMP，请使用此**no**命令的形式。

isakmp enable*interface-name*
no isakmp enable*interface-name*

Syntax Description *interface-name* 指定启用或禁用 ISAKMP 协商的接口名称。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 cryptoisakmpenable 命令取而代之。

CR_Examples 以下示例在全局配置模式下输入了如何在内部接口上禁用 ISAKMP：

```
ciscoasa(config)# no isakmp enableinside
```

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp identity (已弃用)

如要设置发送至对等体的第 2 阶段 ID，请在全局配置模式下使用 **isakmpidentity** 命令。要恢复默认设置，请使用此 **no** 命令的形式。

isakmp identity { **address** | **hostname** | **key-id**key-id-string | **auto** }
no isakmp identity { **address** | **hostname** | **key-id**key-id-string | **auto** }

Syntax Description

address	使用交换 ISAKMP 身份信息的主机的 IP 地址。
auto	通过连接类型确定 ISKMP 协商；预共享密钥的 IP 地址或证书认证的证书 DN。
hostname	使用交换 ISAKMP 身份信息的主机的完全限定域名（默认）。此名称包含主机名和域名。
key-id key_id_string	指定远程对等体用于查找预共享密钥的字符串。

Command Default

默认 ISAKMP 身份是 **isakmpidentityhostname** 命令。

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

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。该 **cryptoisakmpidentity** 命令取而代之。

CR_Examples

以下示例进入全局配置模式，根据连接类型在接口上启用 ISAKMP 协商，以便与 IPSec 对等体进行通信：

```
ciscoasa(config)# isakmp identity auto
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。

命令	说明
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp ipsec-over-tcp (已弃用)

要启用 IPsec over TCP，请在全局配置模式下使用 **isakmp ipsec-over-tcp** 命令。要禁用 TCP 上的 IPsec，请使用此命令的 **no** 形式。

isakmp ipsec-over-tcp [**port**port1...port10]
no isakmp ipsec-over-tcp [**port**port1...port10]

Syntax Description

portport1...port10 （可选）指定设备在其上接受 IPsec over TCP 连接的端口。您最多可以列出 10 个端口。端口号可以在 1-65535 范围内。默认端口号为 10000。

Command Default

默认值为禁用。

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
全局配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。 **cryptoisakmp ipsec-over-tcp** 命令将取代它。

CR_Examples

此示例以全局配置模式输入，在端口 45 上启用 TCP 上的 IPsec：

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

命令	说明
clear configure isakmp	清除所有 ISAKMP 配置。
clear configure isakmp policy	清除所有 ISAKMP 策略配置。
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动配置。

isakmp keepalive

要配置 IKE 保持连接，请在 **isakmpkeepalive** 隧道组 ipsec-attributes 配置模式下使用该命令。要使用默认阈值和重试值将保持连接参数恢复为已启用，请使用此命令的 **no** 形式。

```
isakmp keepalive [thresholdseconds | 无限] [retry秒] [disable]
no isakmp keepalive [thresholdseconds | 无限] [retry秒] [disable]
```

Syntax Description	disable	禁用 IKE 保持连接处理（默认情况下处于启用状态）。
	无限	ASA 从不启动保持连接监控。
	retry秒	指定未收到保持连接响应后重试的间隔（秒）。范围是2-10秒。默认值为 2 秒。
	threshold秒	指定对等方在开始保持连接监控之前可以空闲的秒数。范围是 10-3600 秒。LAN 间组的默认值为 10 秒，远程访问组的默认值为 300 秒。

Command Default	远程访问组的默认值为阈值 300 秒，重试时间为 2 秒。 对于 LAN 间组，默认阈值为 10 秒，重试时间为 2 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
Tunnel-group ipsec-attributes 配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南 在每个隧道组中，默认启用 IKE 保持连接以及默认阈值和重试值。您可以仅将此属性应用于 IPsec 远程访问类型和 IPsec LAN 间隧道组类型。

CR_Examples 以下示例在 tunnel-group ipsec-attributes 配置模式下进入，配置 IKE DPD，将阈值确定为 15，并为 IP 地址为 209.165.200.225 的 IPsec LAN 间隧道组指定重试间隔为 10：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
```



```
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
clear-config tunnel-group	清除所有配置的隧道组。
showrunning-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	为该组配置隧道组 IPsec 属性。

isakmp nat-traversal（已弃用）

要全局启用 NAT 穿越，请在全局配置模式下检查 ISAKMP 是否已启用（可以使用命令启用 **isakmpenable** 它），然后使用该 **isakmpnat-traversal** 命令。如果已启用 NAT 遍历，则可以使用此命令的 **no** 形式禁用它。

isakmp nat-traversalnatkeepalive
no isakmp nat-traversalnatkeepalive

Syntax Description *natkeepalive* 设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

Command Default 默认情况下，NAT 穿越（**isakmpnat-traversal** 命令）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
全局配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	7.2(1) 此命令已弃用。该 cryptoisakmpnat-traversal 命令取而代之。

使用指南 许多使用 IPsec 的网络都使用网络地址转换 (NAT)，包括端口地址转换 (PAT)，但存在许多不兼容性，导致 IPsec 数据包无法成功通过 NAT 设备。NAT 遍历使 ESP 数据包能够穿过一个或多个 NAT 设备。

ASA 支持 NAT 遍历，如 IETF “IPsec 数据包的 UDP 封装” (UDP Encapsulation of IPsec Packets) 草案第 2 版和第 3 版所述（详见 <http://www.ietf.org/html.charters/ipsec-charter.html>）和 NAT 遍历动态和静态加密映射均支持。

此命令将在 ASA 上全局启用 NAT-T。要在加密映射条目中禁用，请使用 **cryptomapsetnat-t-disable** 命令。

CR_Examples 以下示例在全局配置模式下启用 ISAKMP，然后启用 NAT 遍历，间隔为 30 秒：

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy authentication

要在 IKE 策略中指定身份验证方法，请在全局配置模式下使用 **isakmppolicyauthentication** 命令。要删除 ISAKMP 身份验证方法，请使用 **clearconfigure** 命令。

优先事项**isakmp policyauthentication { crack | pre-share | rsa-sig }**

Syntax Description	crack	指定 IKE 认证加密密钥质询/响应 (CRACK) 作为认证方法。
	pre-share	指定预共享密钥作为身份验证方法。
	priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
	rsa-sig	指定 RSA 签名作为身份验证方法。 RSA 签名为 IKE 协商提供不可否认性。这意味着您可以向第三方证明您是否与对等体进行了 IKE 协商。

Command Default 默认 ISAKMP 策略身份验证是 **pre-share** 选项。

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

7.0(1) 添加了此命令。

使用指南 IKE 策略定义一组用于 IKE 协商的参数。如果指定 RSA 签名，则必须配置 ASA 及其对等体，从证书颁发机构 (CA) 获取证书。如果指定预共享密钥，则必须在 ASA 及其对等体中单独配置这些预共享密钥。

CR_Examples 以下示例在全局配置模式下设置要在优先级编号为 40 的 IKE 策略中使用的 RSA 签名身份验证方法：

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy encryption（已弃用）

要指定要在 IKE 策略中使用的加密算法，请在全局配置模式下使用 **isakmppolicyencryption** 命令。要将加密算法重置为默认值，请使用此命令的 **no** 形式。

isakmp policypriorityencryption { aes | aes-192 | aes-256 | des | 3des }
no isakmp policypriorityencryption { aes | aes-192 | aes-256 | des | 3des }

Syntax Description

3des	指定在 IKE 策略中使用三重 DES 加密算法。
aes	指定要在 IKE 策略中使用的加密算法是具有 128 位密钥的 AES。
aes-192	指定要在 IKE 策略中使用的加密算法是具有 192 位密钥的 AES。
aes-256	指定要在 IKE 策略中使用的加密算法是具有 256 位密钥的 AES。
des	指定要在 IKE 策略中使用的加密算法为 56 位 DES-CBC。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

Command Default

默认 ISAKMP 策略加密为 **3des**。

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

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。该 **cryptoisakmppolicyencryption** 命令取而代之。

CR_Examples

以下示例在全局配置模式下将 128 位密钥 AES 加密设置为要在优先级编号为 25 的 IKE 策略中使用的算法：

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

以下示例在全局配置模式下设置要在优先级数字为 40 的 IKE 策略中使用的 3DES 算法：

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy group（已弃用）

要为 IKE 策略指定 Diffie-Hellman 组，请在全局配置模式下使用 **isakmppolicygroup** 命令。要将 Diffie-Hellman 组标识符重置为默认值，请使用此命令的 **no** 形式。

```
isakmp policyprioritygroup { 1 | 2 | 5 }
no isakmp policyprioritygroup
```

Syntax Description	group1 指定在 IKE 策略中使用 768 位 Diffie-Hellman 组。这是默认值。
	group2 指定在 IKE 策略中使用 1024 位 Diffie-Hellman 组 2。
	group5 指定在 IKE 策略中使用 1536 位 Diffie-Hellman 组 5。
	priority 唯一标识 Internet 密钥交换 (IKE) 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

Command Default 默认为组 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	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。已添加组 7。
	7.2(1) 此命令已弃用。该 cryptoisakmppolicygroup 命令取而代之。

使用指南 IKE 策略定义在 IKE 协商期间使用的一组参数。

有三个组选项：768 位（DH 组 1）、1024 位（DH 组 2）和 1536 位（DH 组 5）。1024 位和 1536 位 Diffie-Hellman 组可提供更强的安全性，但需要更多的 CPU 时间来执行。



注释 思科 VPN 客户端版本 3.x 或更高版本需要使用 ISAKMP 策略才能配置 DH 组 2。（如果已配置 DH 组 1，则思科 VPN 客户端无法连接。）AES 支持仅在许可用于 VPN-3DES 的 ASA 上可用。由于 AES 提供的密钥较大，ISAKMP 协商应该使用 Diffie-Hellman (DH) 组 5，而不是组 1 或组 2。这是使用 **isakmppolicyprioritygroup5** 命令完成的。

CR_Examples

以下示例在全局配置模式下输入，设置组 2（1024 位 Diffie Hellman）以用于优先级编号为 40 的 IKE 策略：

```
ciscoasa(config)# isakmp policy 40 group 2
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy hash（已弃用）

要为 IKE 策略指定散列算法，请在全局配置模式下使用 **isakmppolicyhash** 命令。要将散列算法重置为 SHA-1 的默认值，请使用此命令的 **no** 形式。

isakmp policypriorityhash { md5 | sha }
no isakmp policypriorityhash

Syntax Description

md5 指定在 IKE 策略中使用 MD5（HMAC 变体）作为散列算法。

priority 唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

sha 指定将 SHA-1（HMAC 变体）用作 IKE 策略中的散列算法。

Command Default

默认散列算法是 SHA-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	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。 **cryptoisakmppolicyhash** 命令将取代它。

使用指南

IKE 策略定义在 IKE 协商期间使用的一组参数。

有两个散列算法选项：SHA-1 和 MD5。MD5 的摘要较小，被认为速度比 SHA-1 稍快。

CR_Examples

以下示例在全局配置模式下输入，指定在 IKE 策略中使用 MD5 散列算法，优先级数字为 40：

```
ciscoasa(config)# isakmp policy 40 hash md5
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。

命令	说明
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy lifetime（已弃用）

如要指定 IKE 安全关联到期前的生命周期，请在全局配置模式下使用**isakmppolicylifetime**命令。要将安全关联生命周期重置为默认值 86,400 秒（一天），请使用此命令的 **no** 形式。

isakmp policyprioritylifetimeseconds
no isakmp policyprioritylifetime

Syntax Description	<i>priority</i> 唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。 <i>seconds</i> 指定每个安全关联在到期前应存在的秒数。要建议有限生命周期，请使用 120 到 2147483647 秒之间的整数。要设置无限生命周期，请使用 0 秒。

Command Default	默认值为 86,400 秒（一天）。

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
全局配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	7.2(1) 此命令已弃用。该 cryptoisakmppolicylifetime 命令取而代之。

使用指南	当 IKE 开始协商时，它会设法就其自身会话的安全参数达成一致。然后，每个对等体上的安全关联都会引用商定的参数。对等体将保留安全关联，直到生命周期到期。在安全关联到期之前，后续 IKE 协商可以使用它，这可以节省设置新的 IPsec 安全关联的时间。对等体将在当前安全关联到期之前协商新的安全关联。

生命期越长，ASA 设置未来 IPsec 安全关联的速度就越快。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间（大约每隔几分钟再生一次）。建议您接受默认值，但如果对等体未提议生命周期，则可以指定无限生命周期。



注释	如果 IKE 安全关联设置为无限生命周期，但对等体提议有限生命周期，则使用对等体协商的有限生命周期。

CR_Examples

以下示例在全局配置模式下输入，在优先级编号为 40 的 IKE 策略中将 IKE 安全关联的生命周期设置为 50,4000 秒（14 小时）：

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

以下示例在全局配置模式下将 IKE 安全关联设置为无限生命周期。

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

Related Commands

clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp reload-wait (已弃用)

要允许等待所有活动会话自行终止后再重新启动 ASA，请在全局配置模式下使用 **isakmpreload-wait** 命令。要禁用等待活动会话终止并重新启动 ASA，请使用此命令的 **no** 形式。

isakmp reload-wait
no isakmp reload-wait

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
全局配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 添加了此命令。

7.2(1) 此命令已弃用。该 **cryptoisakmpreload-wait** 命令取而代之。

CR_Examples

以下示例在全局配置模式下输入，指示 ASA 等待所有活动会话终止后再重新启动：

```
ciscoasa(config)# isakmp reload-wait
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isis priority

要配置接口上指定 ASA 的优先级，请在接口 isis 配置模式下使用 **isispriority** 命令。要重置默认优先级，请使用此命令的形式。

isis priority*number-value* [**level-1** | **level-2**]
no isis priority [**level-1** | **level-2**]

Syntax Description

number-value 设置路由器的优先级。范围为 0 到 127。

level-1 (可选) 单独设置 1 级的优先级。

level-2 (可选) 单独设置 2 级的优先级。

Command Default

默认值为 64。

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 isis 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.6(1) 添加了此命令。

使用指南

此命令设置用于确定 LAN 上的哪个 ASA 将成为指定路由器或 DIS 的优先级。优先级将在呼叫数据包中通告。优先级最高的 ASA 将成为 DIS。



注释 在 IS-IS 中，没有指定备份的路由器。将优先级设置为 0 将降低此系统成为 DIS 的几率，但不会阻止其成为 DIS。如果具有更高优先级的 ASA 上线，它将接管当前 DIS 的角色。在优先级相等的情况下，最高 MAC 地址将打破平衡。

CR_Examples

以下示例展示通过将优先级设置为 80 提供优先级的第 1 级路由。此 ASA 现在更有可能成为 DIS：

```
ciscoasa(config)#  
interface GigabitEthernet0/0
```

```
ciscoasa(config-if)#
isis priority 80 level-1
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。

命令	说明
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isisspassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。

命令	说明
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis protocol shutdown

要禁用 IS-IS 协议，以使其无法在指定接口上形成邻接关系，并将该接口的 IP 地址放入 ASA 生成的 LSP 中，请在接口 isis 配置模式下使用该 **isisprotocolshutdown** 命令。要重新启用 IS-IS 协议，请使用此命令 **no** 的形式。

isis protocol shutdown
no isis protocol shutdown

Syntax Description

此命令没有任何参数或关键字。

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
接口 isis 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.6(1) 添加了此命令。

使用指南

此命令将使您能为指定接口禁用 IS-IS 协议，而不会删除配置参数。对于配置了该命令的接口，IS-IS 协议不会形成任何邻接关系，并且该接口的 IP 地址会放入 ASA 生成的 LSP 中。如果您不希望 IS-IS 在 **protocolshutdown** 任何接口上形成任何邻接关系并清除 IS-IS LSP 数据库，请使用该命令。

CR_Examples

以下示例在千兆以太网 0/0 上禁用 IS-IS 协议：

```
ciscoasa(config)#  
interface GigabitEthernet0/0  
ciscoasa(config-if)#  
isis protocol shutdown
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

命令	说明
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis retransmit-interval

要配置每个 IS-IS LSP 的重新传输之间的时间量，请在接口 isis 配置模式下使用 **isisretransmit-interval** 命令。要恢复默认值，请使用此命令 **no** 的形式。

isis retransmit-interval秒

no isis retransmit-interval秒

Syntax Description

秒（可选）每个 LSP 重新传输之间的时间。数字应该大于已连接网络上任意两个路由器之间的预计往返延迟。范围为 0 到 65535。

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
接口 isis 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.6(1) 添加了此命令。

使用指南

请确保保守地设置 *seconds* 参数，否则可能会导致不必要的重新传输。此命令对 LAN（多点）接口没有影响。

CR_Examples

以下示例将 GigabitEthernet 0/0 配置为大型串行线路的每 60 秒重新传输每个 IS-IS LSP：

```
ciscoasa(config)#  
interface GigabitEthernet0/0  
ciscoasa(config-if)#  
isis retransmit-interval 60
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

命令	说明
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis retransmit-throttle-interval

要配置接口上每个 IS-IS LSP 的重新传输之间的时间量，请在接口 isis 配置模式下使用 **isisretransmit-throttle-interval** 命令。要恢复默认值，请使用此命令 **no** 的形式。

isis retransmit-throttle-interval*milliseconds*
no isis retransmit-throttle-interval

Syntax Description

毫 （可选）接口上 LSP 重传之间的最小延迟。范围为 0 到 65535。
秒

Command Default

延迟由 **isislsp-interval** 命令确定。

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 isis 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.6(1) 添加了此命令。

使用指南

在包含很多 LSP 和很多接口的大型网络中，作为控制 LSP 重新传输流量的一种方式，此命令可能非常有效。此命令可以控制可在接口上重新发送 LSP 的速率。

该命令不同于接口上发送 LSP 的速率（由命令控 **isislsp-interval** 制）和单个 LSP 重传之间的周期（由命令控 **isisretransmit-interval** 制）。您可以组合使用这些命令，以控制从一个 ASA 到其邻居的路由流量的提供负载。

CR_Examples

以下示例配置 GigabitEthernet 0/0 以将 LSP 重新传输的速率限制为每 300 毫秒一次：

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-throttle-interval 300
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。

命令	说明
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。

命令	说明
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。

命令	说明
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis tag

当将某个 IP 前缀放入 IS-IS LSP 时，要在该接口配置的 IP 地址上设置标签，请在 **isistag** 接口 isis 配置模式下使用该命令。要停止标记 IP 地址，请使用此命令 **no** 的形式。

isis tag*tag-number*
no isis tag*tag-number*

Syntax Description

tag-number 用作 IS-IS 路由标签的数字。范围为 1 到 4294967295。

Command Default

没有与为接口配置的 IP 地址关联的路由标记。

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 isis 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.6(1) 添加了此命令。

使用指南

直到使用标签时，才会对设置该标签的路由进行操作，例如，重新分发路由或汇总路由。配置此命令将触发 ASA 生成新的 LSP，因为标签是数据包中新的信息片段。

CR_Examples

以下示例将 GigabitEthernet 0/0 配置为具有标记 100：

```
ciscoasa(config)#  
interface GigabitEthernet0/0  
ciscoasa(config-if)#  
isis tag 100
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

命令	说明
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

is-type

要配置 IS-IS 路由进程实例的路由级别，请在路由器 isis 配置模式下使用 **is-type** 命令。要重置默认值，请使用此命令的形式。

isis type [**level-1** | **level 1-2** | **level-2-only**]
no isis type [**level-1** | **level 1-2** | **level-2-only**]

Syntax Description

level-1	（可选）表示区域内路由。此 ASA 仅了解其区域内的目的地。2 级（区域间）路由由最近的 1-2 级 ASA 执行。
level-1-2	（可选）ASA 同时执行 1 级和 2 级路由。此 ASA 运行两个路由进程实例。它有一个用于区域内目的地（1 级路由）的链路状态数据包数据库 (LSDB)，并运行最短路径优先 (SPF) 计算来发现区域拓扑。它还具有另一个 LSDB，其中包含所有其他骨干网（第 2 级）路由器的链路状态数据包 (LSP)，并运行另一个 SPF 计算来发现骨干网的拓扑以及所有其他区域的存在。
level-2-only	（可选）表示区域间路由。此 ASA 是主干网的一部分，并且不与其所在区域内的仅限 1 级的 ASA 进行通信。

Command Default

在常规 IS-IS 配置中，ASA 作为第 1 级（区域内部）和第 2 级（区域间）路由器。

在多区域 IS-IS 配置中，配置 IS-IS 路由进程的第一个实例默认情况下是第 1-2 级（区域内部和区域间）路由器。配置的 IS-IS 进程的其余实例默认情况下是第 1 级路由器。

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

我们强烈建议您配置 IS-IS 路由进程的类型。如果要配置多区域 IS-IS，则必须配置路由器类型，或允许默认情况下配置路由器。默认情况下，使用 **routerisis** 命令配置的 IS-IS 路由进程的第一个实例是 1-2 级路由器。

如果网络中只有一个区域，则无需同时运行 1 级和 2 级路由算法。如果 IS-IS 用于无连接网络服务 (CLNS) 路由（并且只有一个区域），则在任何地方都必须仅使用第 1 级。如果 IS-IS 仅用于 IP 路由

（并且只有一个区域），则只能在任何位置运行第 2 级。在 1-2 级区域存在之后添加的区域，默认情况下是 1 级区域。

如果已为 1-2 级（IS-IS 路由进程的第一个实例的默认设置）配置路由器实例，则可以使用 **is-type** 命令删除区域的 2 级（区域间）路由。您还可以使用 **is-type** 命令为区域配置 2 级路由。

CR_Examples

以下示例指定区域路由器：

```
ciscoasa#
router isis
ciscoasa(config-router)#
is-type level-2-only
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型

命令	说明
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。

命令	说明
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

issuer (Deprecated)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定向 SAML 类型 SSO 服务器发送断言的安全设备，请在 webvpn-ss0-saml 配置模式下对该特定 SAML 类型使用 **issuer** 命令。要删除发行者名称，请使用此命令 **no** 的形式。

issuer*identifier*
no issuer [*identifier*]

Syntax Description

identifier 指定安全设备名称，通常是设备的主机名。标识符必须少于 65 个字母数字字符。

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
Webvpn-ss0-saml 配置	• 是	—	• 是	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

9.5(2) 此命令已弃用。

使用指南

SSO 支持仅适用于 WebVPN，让用户无需多次输入用户名和密码即可访问不同服务器上的不同安全服务。ASA 目前支持 SAML POST 类型的 SSO 服务器和 SiteMinder 类型的 SSO 服务器。

此命令仅适用于 SAML 类型的 SSO 服务器。

CR_Examples

以下示例指定名为 asa1.example.com 的安全设备的颁发者名称：

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-ss0-saml)# issuer asa1.example.com
ciscoasa(config-webvpn-ss0-saml)#
```

Related Commands

命令	说明
<code>assertion-consumer-url</code>	指定安全设备用于联系 SAML 类型 SSO 服务器断言消费者服务的 URL。
<code>request-timeout</code>	指定失败的 SSO 身份验证尝试超时之前的秒数。
<code>showwebvpnssso-server</code>	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
<code>ssso-server</code>	创建单点登录服务器。
信任点	指定包含用于对 SAML 类型浏览器断言进行签名的证书的信任点名称。

issuer-name

要指定所有已颁发证书的颁发者名称 DN，请在本地证书颁发机构 (CA) 服务器配置模式下使用 **issuer-name** 命令。要从证书颁发机构证书中删除使用者 DN，请使用此命令的 **no** 形式。

issuer-name *DN-string*
no issuer-name *DN-string*

Syntax Description

DN-string 指定证书的可分辨名称，也是自签名 CA 证书的主体名称 DN。使用逗号分隔属性-值对。在任何包含逗号的值两边插入引号。发行人名称必须少于 500 个字母数字字符。

Command Default

默认颁发者名称为 `cn=hostame.domain-name`，例如 `cn=asa.example.com`。

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

7.3(1) 添加了此命令。

8.0(2) 添加了对引号的支持，以保留 *DN* 字符串值中的逗号。

使用指南

该命令指定由本地 CA 服务器创建的任何证书上显示的颁发者名称。如果希望颁发者名称与默认 CA 名称不同，请使用此可选命令。



注释 通过发出 **noshutdown** 命令启用 CA 服务器并生成证书后，无法更改此颁发者名称配置。

CR_Examples

以下示例配置证书身份验证：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc."
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
<code>crypto ca server</code>	提供对 <code>ca</code> 服务器配置模式命令的访问，这些命令允许您配置和管理本地 CA。
keysize	指定证书注册时生成的公钥和私钥的大小。
lifetime	指定 CA 证书和颁发的证书的有效期。
showcryptocaserver	显示本地 CA 的特征。
showcryptocaservercert-db	显示本地 CA 服务器证书。



第 II 部分

J - M 命令

- [j - k](#)，第 369 页
- [l2 - lof](#)，第 401 页
- [log - lz](#)，第 495 页
- [maa - match d](#)，第 607 页
- [match e - match q](#)，第 689 页
- [match r - me](#)，第 751 页
- [mf - mz](#)，第 867 页



j – k

- [java-trustpoint](#)（已弃用），第 370 页
- [join-failover-group](#)，第 372 页
- [jumbo-frame reservation](#)，第 374 页
- [kcd-server](#)，第 376 页
- [keepout](#)，第 378 页
- [kerberos-realm](#)，第 380 页
- [key \(aaa-server host\)](#)，第 382 页
- [key \(cluster group\)](#)，第 384 页
- [key chain](#)，第 386 页
- [key config-key password-encryption](#)，第 388 页
- [key-hash](#)，第 390 页
- [keypair](#)，第 392 页
- [密钥大小](#)，第 394 页
- [keysize server](#)，第 396 页
- [key-string](#)，第 398 页
- [kill](#)，第 400 页

java-trustpoint（已弃用）

要将 WebVPN Java 对象签名工具配置为使用指定信任点位置的 PKCS12 证书和密钥内容，请在 webvpn 配置模式下使用 **java-trustpoint** 命令。要删除 Java 对象签名工具，请使用此命令的 **no** 形式。

java-trustpoint信任点
no java-trustpoint

Syntax Description 信任 指定 **cryptocaimport** 命令配置的信任点位置。
点

Command Default 默认情况下，Java 对象签名的信任点设置为 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
Webvpn 配置	• 是	—	• 是	—	—

Command History 版本 修改

7.1(2) 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 信任点是证书颁发机构 (CA) 或身份密钥对的代表。对于 **java-trustpoint** 命令，给定信任点必须包含应用签名实体的 X.509 证书、与该证书对应的 RSA 私钥以及向上扩展至根 CA 的证书授权链。这通常通过使用 **cryptocaimport** 命令导入 PKCS12 格式的捆绑包来实现。可以从受信任的 CA 颁发机构获取 PKCS12 捆绑包，也可以使用 openssl 等开源工具从现有 X.509 证书和 RSA 私钥手动创建一个捆绑包。



注释 上传的证书无法用于签署随软件包（例如，CSD 软件包）嵌入的 Java 对象。

CR_Examples

以下示例首先配置新信任点，然后为 WebVPN Java 对象签名配置它：

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
```

```
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

以下示例配置用于对 WebVPN Java 对象签名的新信任点:

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

Related Commands

命令	说明
cryptocaimport	使用 PKCS12 数据导入信任点的证书和密钥对。

join-failover-group

要将情景分配给故障转移组，请在情景配置模式下使用**join-failover-group** 命令。要恢复默认设置，请使用此命 **no** 令的形式。

```
join-failover-group group_num
no join-failover-group group_num
```

Syntax Description *group_num* 指定故障转移组编号。

Command Default 故障转移组 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
上下文配置	• 是	• 支持	—	• 是	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

管理环境始终分配给故障转移组 1。您可以使用 **show context detail** 命令来显示故障转移组和情景关联。

您必须先 在系统情景中使用 **failovergroup** 命令创建故障转移组，然后才能将情景分配给故障转移组。在情景处于活动状态的设备上输入此命令。默认情况下，未分配的情景是故障转移组 1 的成员，因此，如果情景之前尚未分配到故障转移组，则应在使故障转移组 1 处于主用状态的设备上输入此命令。

您必须先使用 **no join-failover-group** 命令从故障转移组中删除所有情景，然后才能从系统中删除故障转移组。

CR_Examples

以下示例将名为 **ctx1** 的情景分配到故障转移组 2：

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```


Related Commands

命令	说明
context	进入指定情景的情景配置模式。
failovergroup	定义主用/主动故障转移的故障转移组。
showcontextdetail	显示情景详细信息，包括名称、类、接口、故障转移组关联和配置文件 URL。

jumbo-frame reservation

要为受支持的型号启用巨帧，请在全局配置模式下使用 **jumbo-frame reservation** 命令。要禁用巨帧，请使用此命令的 **no** 形式。



注释 此设置的更改需要您重新启动 ASA。

jumbo-frame reservation
no jumbo-frame reservation

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下，ASA 硬件、ASA virtual和 ISA 3000 上禁用巨型帧预留。
其他型号默认支持巨型帧。

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	—	• 是

Command History	版本	修改
	8.1(1)	为 ASA 5580 添加了此命令。
	8.2(5)/8.4(1)	增加了对 ASA 5585-X 的支持。
	8.6(1)	增加了对 ASA 5512-X 至 ASA 5555-X 的支持。
	9.3(2)	增加了对 ASA 5506-X 的支持。
	9.3(3)	增加了对 ASA 5508-X 和 5516-X 的支持。

使用指南 此过程仅适用于 ASA 硬件型号、ISA 3000 和。ASA virtual其他型号默认支持巨型帧。
RAM 小于 8GB 的 ASAv5 和 ASAv10 不支持巨型帧。
巨型帧是一种大于标准最大值 1518 字节（包括第 2 层报头和 VLAN 标记，18 字节）的以太网数据包，最大可达 9216 字节。请注意， **mtu** 命令仅指定 负载值，因此对于 9216 字节的巨帧，请将 MTU 设置为 9198（9216-18 字节用于报头）

巨型帧支持需要额外的内存，这可能会限制其他功能（例如访问列表）的最大使用。

管理 *n/n* 接口不支持巨型帧。

确保将每个需要传输巨型帧的接口的 MTU 设置为高于默认值 1500 的值；例如，使用命令将值设置为 **mtu9198**。对于 ASASM，您无需设置 **jumbo-frame reservation** 命令；默认情况下，它支持巨帧。只需将 MTU 设置为所需的值即可。

此外，使用巨帧时，请务必为 TCP 配置 MSS（最大分段大小）值。MSS 应比 MTU 少 120 字节。例如，如果您将 MTU 配置为 9000，则应将 MSS 配置为 8880。您可以使用命令来为 **sysoptconnectiontcpmss** MSS 进行配置。

主设备和辅助设备都需要重新启动，以便故障转移对支持巨帧。为避免停机，请执行以下操作：

- 在主用设备上发出命令。
- 保存活动设备上的运行配置。
- 重新启动主设备和辅助设备，一次一台。

CR_Examples

以下示例将启用巨型帧预留、保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5
70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

Related Commands

命令	说明
mtu	指定接口的最大传输单元。指定接口的最大传输单元。
showjumbo-framereservation	显示命令的jumbo-framereservation当前配置。

kcd-server

要为无客户端 SSL 远程访问 VPN 配置 Kerberos 约束委派 (KCD)，请在 webvpn 配置模式下使用 **kcd-server** 命令。要禁用 KCD，请使用此命令的形式。

```
kcd-serveraaa-server-group_nameusernameuser_idpasswordpassword [ validate-server-certificate ]
no kcd-server
```

Syntax Description	username	指定具有管理员或服务级别权限可将设备添加到域的 Active Directory 用户。
	password	指定用户的密码。
	validate-server-certificate	(可选。) 指示 ASA 验证服务器证书，从而在加入域时验证服务器的身份。如果省略此选项，系统会假定域控制器有效。

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
Webvpn 配置	• 是	—	• 是	—	—

Command History	版本	修改
	8.4(1)	添加了此命令。
	9.15(1)	已添加关 validate-server-certificate 键字。

使用指南

在 webvpn 配置模式下使用 **kcd-server** 命令允许 ASA 加入 Active Directory 域。域控制器名称和领域在 **aaa-server-groupname**命令中指定。AAA 服务器组必须是 Kerberos 服务器类型。 **username** 和 **password** 选项不对应于具有管理员权限的用户，但应对应于在域控制器上具有服务级别权限的用户。要查看现有配置，请使用 **showwebvpnkcd**命令。

ASA 环境中的 Kerberos 约束委派 (KCD) 为无客户端 SSL 远程访问 VPN 用户提供对受 Kerberos 保护的所有 Web 服务的单点登录 (SSO) 访问权限。ASA 代表用户维护凭证（服务票证），并使用此票证对服务用户进行身份验证。

为了使命令发挥 **kcd-server**作用，ASA 必须在 源 域（ASA 所在的域）和 目标 或 资源域（Web 服务所在的域）之间建立信任关系。ASA 跨越从源域到目标域的认证路径，并代表远程访问用户获取访问服务所需的票证。

这条路径称为跨领域身份验证。在跨领域身份验证的每个阶段，ASA 依赖于特定领域上的凭证和与后续领域的信任关系。

KCD 配置还要求您将域控制器配置为 DNS 服务器（例如，在 DefaultDNS 组中），并在可通过其访问域控制器的接口上启用 DNS 查找。

CR_Examples

以下是 KCD 的配置示例，其中域控制器为 10.1.1.10（可通过内部接口访问），域名为 PRIVATE.NET。此外，域控制器上的服务账户用户名和密码为 duser 和 duser123!。

```

-----Enable a DNS lookup by configuring the DNS server and Domain name -----
ciscoasa
(config)#
dns domain-lookup inside
ciscoasa
(config)#
dns server-group DefaultDNS
ciscoasa
(config-dns-server-group)#
name-server 10.1.1.10
ciscoasa
(config-dns-server-group)#
domain-nameprivate.net
-----Configure the AAA server group with Server and Realm-----
ciscoasa
(config)#
aaa-server KerberosGroup protocol Kerberos
ciscoasa
(config-asa-server-group)#
aaa-server KerberosGroup (inside) host 10.1.1.10
ciscoasa
(config-asa-server-group)#
kerberos-realm PRIVATE.NET
-----Enable KCD-----
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
kcd-server KerberosGroup username dcuser password dcuser123! validate-server-certificate

```

Related Commands

命令	说明
aaa-server	进入aaa-server配置模式，可以配置AAA服务器参数。
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。
showaaakerberos	显示 Kerberos 票证。
showwebvpnkcd	显示 KCD 配置。

keepout

要显示管理员定义的消息而不是新用户会话的登录页面（当ASA进行维护或故障排除期间时），请在 webvpn 配置模式下使用**keepout**命令。要删除之前设置的禁止布线页面，请使用该命令的 **no** 版本。

keepout
no keepout字符串

Syntax Description *string* 用双引号引起来的字母数字字符串。

Command Default 无禁止布线区页面。

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
8.0(2)	添加了此命令。

使用指南 此命令启用后，无客户端 WebVPN 门户页面将不可用。您会收到管理员定义的消息，说明门户不可用，而不是收到门户的登录页面。使用 **keepout** 命令禁用无客户端访问，但仍允许 AnyConnect 访问。您还可以使用此命令在维护进行时指示门户不可用。



注释 如果已安装 HostScan，禁止布线区功能不会阻止 ASA 打开思科安全桌面门户等页面。为了避开思科安全桌面端口，需要卸载 HostScan。

CR_Examples 以下示例显示如何配置禁止布线区页面：

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

```
keepout "The system is unavailable until 7:00 a.m. EST."  
ciscoasa(config-webvpn)#
```

Related Commands

命令	说明
webvpn	进入 webvpn 配置模式，在此模式下配置无客户端 SSL VPN 连接的属性。

kerberos-realm

要指定此 Kerberos 服务器的领域名称，请在 aaa-server 主机配置模式下使用 **kerberos-realm**命令。要删除领域名称，请使用以下命令 **no** 命令的形式：

kerberos-realm字符串
no kerberos-realm

Syntax Description

string 区分大小写的字母数字字符串，最多 64 个字符。字符串中不允许有空格。

注释
Kerberos 领域名称仅使用数字和大写字母。尽管 ASA 接受字符串参数中的小写字母，但它不会将小写字母转换为大写字母。请务必仅使用大写字母。

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
AAA服务器主机配置	• 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

此命令仅对 Kerberos 服务器有效。

当在 Kerberos 领域的 Windows **setUSERDNSDOMAIN**2000 Active Directory 服务器上运行时，字符串参数的值应与 Microsoft Windows 命令的输出相匹配。在以下示例中，EXAMPLE.COM 是 Kerberos 领域名：

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

字符串参数只能使用数字和大写字母。**kerberos-realm** 命令区分大小写，ASA 不会将小写字母转换为大写字母。

CR_Examples

以下序列显示在配置 AAA 服务器主机的情景中将 kerberos 领域设置为 “EXAMPLE.COM” **kerberos-realm** 的命令：


```
ciscoasa
(config)# aaa-server svrgrp1 protocol kerberos
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)# kerberos-realm EXAMPLE.COM
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

命令	说明
aaa-serverhost	进入AAA服务器主机配置子模式，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。

key (aaa-server host)

要指定用于向 AAA 服务器验证 NAS 的服务器密钥值，请在 aaa-server 主机配置模式下使用 **key** 命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除密钥，请使用此 **no** 命令的形式。

key [**0** | **8**] *key*
no key

Syntax Description

key 字母数字关键字，最长可为 127 个字符。您可以选择在密钥之前添加一个数字，以表示已加密：

- 0 表示密钥未加密。这是默认值。
- 8 表示密钥是 AES 加密的 base64 散列值。

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服务器主机配置	• 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

密 钥值是区分大小写的字母数字关键字，最多 127 个字符，与 TACACS+ 服务器上的密钥值相同。超出 127 个字符后的所有字符都会被忽略。该密钥在客户端和服务器之间使用，用于加密它们之间的数据。客户端和服务器系统上的密钥必须相同。密钥不能包含空格，但允许包含其他特殊字符。密钥（服务器密钥）值向 AAA 服务器对 ASA 进行身份验证。

此命令仅适用于 RADIUS 和 TACACS+ 服务器。

CR_Examples

以下示例在主机“1.2.3.4”上配置名为“svrgrp1”的 TACACS+ AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将密钥配置为“myexclusivemumblekey”。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

命令	说明
aaa-server host	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。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示 AAA 服务器配置。

key (cluster group)

要设置集群控制链路上控制流量的身份验证密钥，请在 **key** 集群组配置模式下使用该命令。要删除密钥，请使用此 **no** 命令的形式。

```
keyshared_secret
no key [shared_secret]
```

Syntax Description *shared_secret* 将共享机密设置为 1 至 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。

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	• 支持	—	• 是

Command History 版本 修改

9.0(1) 添加了此命令。

使用指南 此命令不会影响数据路径流量，包括始终以明文发送的连接状态更新和转发数据包。

CR_Examples 以下示例设置共享密钥：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

命令	说明
clacpsystem-mac	使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。
cluster group	命名集群并进入集群配置模式。
cluster-interface	指定集群控制链路接口。
clusterinterface-mode	设置集群接口模式。
conn-rebalance	启用连接再均衡。

命令	说明
console-replicate	启用从从属设备到主设备的控制台复制。
enable(clustergroup)	启用集群。
health-check	启用集群健康检查功能，包括单元健康监控和接口健康监控。
key	为集群控制链路上的控制流量设置身份验证密钥。
local-unit	为集群成员命名。
mtucluster-interface	指定集群控制链路接口的最大传输单元。
priority(clustergroup)	设置此单元在主单元选举中的优先级。

key chain

要配置轮换密钥以对 IGP 对等体进行身份验证，请在全局配置模式下使用 **keychain** 命令。要删除配置，请使用命 **no** 令的形式。

```
key chainkey-chain-namekeykey-idkey-string { 0 | 8 } key-string-textcryptographic-algorithm
md5 [accept-lifetime [ local | start-time ] [ duration { duration value | infinite | end-time } ]

no key chainkey-chain-namekeykey-idkey-string { 0 | 8 } key-string-textcryptographic-algorithm
md5 [accept-lifetime [ local | start-time ] [ duration { duration value | infinite | end-time } ]
```

Syntax Description	key-chain-name 为 OSPFv2 身份验证配置的密钥链的名称。
key-id	密钥链中的唯一标识符；有效范围为 1 到 255。
0	指定将遵循未加密的密码。
8	指定将遵循的加密密码。
key-string-text	密钥 ID 的密码。该字符串可以是纯文本或加密值。
md5	支持的加密算法。仅支持 md5。
accept-lifetime	（可选）设备与另一台设备交换密钥时接受密钥的时间间隔。
send-lifetime	（可选）设备与另一台设备交换密钥时发送密钥的时间间隔。

Command Default 接受或发送生命周期如果未指定，则默认始终处于活动状态。

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	• 否

Command History	版本 修改
	9.12(1) 添加了此命令。

使用指南 使用 **keychain** 命令配置要在接口的 OSPFv2 身份验证中使用的密钥链。您必须输入 **keyid**、**keystring**、和 **cryptographic-algorithm**命令。输入 **acceptandsendlifetimes**以计划密钥轮换。生命周期变量有助

于处理安全密钥滚动更新。该设备使用密钥的生命周期来确定密钥链中的哪些密钥在任何给定时间点处于活动状态。未指定生命周期时，密钥链身份验证功能与无时间轴的 MD5 身份验证类似。使 **nokeychain** 用 删除钥匙串的配置。

CR_Examples

以下示例显示了密钥链配置命令：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite

ciscoasa(config-keychain-key)#
```

CR_Examples

以下示例提供了运行密钥链配置的输出：

```
ciscoasa# show running key chain
key chain CHAIN2
  key 1
    key-string KEY1CHAIN2
    cryptographic-algorithm md5
  key 2
    accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
    cryptographic-algorithm md5
key chain CHAIN1
  key 1
    key-string CHAIN1KEY1STRING
    accept-lifetime 11:22:33 Sep 1 2018 duration -1
    cryptographic-algorithm md5
ciscoasa# show runing key chain CHAIN1
key chain CHAIN1
  key 1
    key-string CHAIN1KEY1STRING
    accept-lifetime 11:22:33 Sep 1 2018 duration -1
    cryptographic-algorithm md5
ciscoasa#
```

Related Commands

命令	说明
showkeychain	显示已配置的钥匙串
showrunningkeychain	显示当前活动的钥匙串详细信息
clearconfigurekeychain	删除配置的密钥链

key config-key password-encryption

要设置用于生成加密密钥的主密码以便以加密格式安全地存储纯文本密码，请在全局配置模式下使用 **keyconfig-keypassword-encryption**命令。如要解密使用该密码加密的密码，请使用此命令的 no 形式。

```
key config-key password-encryptionpassphrase [old_passphrase]
no key config-key password-encryptionpassphrase
```

Syntax Description	passphrase 密码长度必须介于 8 到 128 个字符之间。除退格键和双引号之外的所有字符都可以作为密码。如果未在命令中输入密码，则系统将提示您输入。使用交互式提示用户输入密码，以避免密码被记录在命令历史缓冲区。
	old_passphrase 如果您要更改密码，请输入旧密码。

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	• 支持	—	• 是

Command History	版本 修改
	8.3(1) 添加了此命令。

- 使用指南 使用主密码的功能包括：
- OSPF
 - EIGRP
 - VPN 负载均衡
 - VPN（远程访问和站点间）
 - 故障转移
 - AAA 服务器
 - 日志记录

- 共享许可证

您必须以任意顺序输入 **keyconfig-keypassword-encrypt** 命令和 **passwordencryptionaes** 命令才能触发密码加密。输入 **writememory**，以将加密密码保存到启动配置。否则，启动配置中的密码可能仍然可见。在多情景模式下，请在系统执行空间中使用 **writememoryall** 保存所有情景配置。

此命令仅在安全会话中被接受，例如通过控制台、SSH 或通过 HTTPS 的 ASDM。

请谨慎使用该 **nokeyconfig-keypassword-encrypt** 命令，因为它会将加密密码更改为纯文本密码。
EXTENSION 当降级到不支持密码加密的 **no** 软件版本时，您可能会使用此命令的形式。

如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。

在主用/备用故障转移中启用或 **writestandby** 更改密码加密会导致将主用配置复制到备用单元。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主动/主动故障转移，您必须手动输入。**writestandby A** 可 **writestandby** 能会导致主动/主动模式下的流量中断，因为在同步新配置之前，辅助设备上的配置已被清除。您应该使用 **failoveractivegroup1** 和 **failoveractivegroup2** 命令使主 ASA 上的所有上下文处于活动状态 **writestandby**，输入，然后使用命令将第 2 组上下文恢复到辅助单 **nofailoveractivegroup2**元。

write 擦除命令（后跟 **reload** 命令）将删除主密码和所有配置（如果其丢失）。

CR_Examples

以下示例设置用于生成加密密钥的密码，并启用密码加密：

```
ciscoasa
(config)#
  key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

命令	说明
passwordencryptionaes	启用密码加密。
write erase	如果主密码在其后跟 reload 命令时丢失，则将其删除。

key-hash

要为板载安全复制 (SCP) 客户端的服务器手动添加散列 SSH 主机密钥，请在服务器配置模式下使用 **key-hash** 命令。您可以通过首先输入命令来访问服务器配置 **sshpubkey-chain** 模式。要删除密钥，请使用此 **no** 命令的形式。

```
key-hash { md5 | sha256 } fingerprint
no key-hash { md5 | sha256 } fingerprint
```

Syntax Description	指纹	输入散列密钥。
	{md5 sha256}	设置使用的散列类型，为 MD5 或 SHA-256。ASA 在其配置中始终使用 SHA-256。

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
服务器配置	• 是	• 支持	• 支持	—	• 是

Command History	版本 修改
	9.1(5) 添加了此命令。

使用指南 您可以使用板载 SCP 客户端在 ASA 之间复制文件，也可以从 ASA 复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器，您可以指定 SSH 主机的 **key-stringkey-hash**（公钥）或（哈希值）。输 **key-hash** 入已经散列的密钥（使用 MD5 或 SHA-256 密钥）；例如，您从 **show** 命令输出复制的密钥。

CR_Examples 以下示例为 10.86.94.170 上的服务器添加经过散列处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

命令	说明
copy	将文件复制到 ASA 或从 ASA 复制文件。
key-hash	输入散列 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
sshpubkey-chain	从 ASA 数据库中手动添加或删除服务器及其密钥。
sshstricthostkeycheck	为板载安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

keypair

要指定要认证其公钥的密钥对，请在 `crypto ca trustpoint` 配置模式下使用 **keypair** 命令。要恢复默认设置，请使用 **no** 命令的形式。

[no]
keypair*name* [**rsamodulus** | **2048** | **4096**] [**ecdsaelliptic-curve256** | **384** | **521**] [**eddsaedwards-curveEd25519**]

Syntax Description	<i>name</i> 指定用于非 CMP 注册的密钥对的名称。
	rsa 为任何 CMP 手动和自动注册生成 RSA 密钥。
	ecdsa 为任何 CMP 手动和自动注册生成 ECDSA 密钥。
	eddsa 为任何 CMP 手动和自动注册生成 EdDSA 密钥。

Command Default	默认设置是不包含密钥对。

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 trustpoint 配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	7.0(1)	添加了此命令。
	9.7(1)	添加了新的 EDCSA 和 RSA 密钥对。
	9.16 (1)	- 删除了对 RSA 密钥大小小于 2048 位的证书的支持。因此，rsa 模数选项已修改为显示 2048 位和更大的值。 - 已添加新的 EdDSA 密钥对。

CR_Examples 以下示例进入信任点中心的 `crypto ca` 信任点配置模式，并指定要为信任点中心认证的密钥对：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。
cryptokeygeneratedsa	生成 DSA 密钥。
cryptokeygeneratersa	生成 RSA 密钥。
defaultenrollment	将注册参数还原为其默认值。

密钥大小

要指定本地证书颁发机构 (CA) 服务器在用户证书注册时生成的公钥和私钥的大小，请在 `ca-server` 配置模式下使用 `keysize` 命令。要将密钥大小重置为默认长度 1024 位，请使用此命令的 `no` 形式。

keysize *size*
no keysize

Syntax Description	<i>size</i> 密钥的大小（位）。大小可以是以下其中一项： • 512 • 768 • 1024 • 2048 • 4096

Command Default	默认情况下，密钥对中每个密钥的长度均为 1024 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
ca-server 配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。
	9.13(1) 此命令行已删除。

CR_Examples	以下示例为本地 CA 服务器为用户生成的所有公共密钥和专用密钥对指定 2048 位的密钥长度：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize 2048
ciscoasa
```

```
(config-ca-server)
#
```

以下示例将本地CA服务器为用户生成的所有公共密钥和专用密钥对的密钥大小重置为默认长度 1024 位：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cryptocaserver	提供对 ca-server 配置模式命令集的访问，允许您配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
subject-name-default	指定要在 CA 服务器颁发的所有用户证书中与用户名一起使用的通用主题名称 DN。

keysize server

如要指定本地证书颁发机构 (CA) 服务器为配置 CA 密钥对大小而生成的公钥和私钥的大小，请在 ca-server 配置模式下使用 **keysizeserver** 命令。要将密钥大小重置为默认长度 1024 位，请使用此命令的 **no** 形式。

keysize serversize
no keysize server

Syntax Description	size 密钥的大小（位）。大小可以是以下其中一项： • 512 • 768 • 1024 • 2048 • 4096

Command Default	默认情况下，密钥对中每个密钥的长度均为 1024 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
Ca-server配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。
	9.13(1) 此命令行已删除。

CR_Examples	以下示例为 CA 证书指定 2048 位的密钥长度：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize server 2048
ciscoasa
```



```
(config-ca-server)
#
```

以下示例将 CA 证书的密钥大小重置为默认长度 1024 位：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize server
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cryptocaserver	提供对 ca-server 配置模式命令集的访问，允许您配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
keysize	指定用户证书的密钥对大小。
subject-name-default	指定要在 CA 服务器颁发的所有用户证书中与用户名一起使用的通用主题名称 DN。

key-string

要为板载安全复制 (SCP) 客户端的服务器手动添加公共 SSH 主机密钥，请在服务器配置模式下使用 **key-string** 命令。您可以通过首先输入命令来访问服务器配置 **sshpubkey-chain** 模式。此命令提示您输入密钥字符串。将字符串保存到配置中时，系统会使用 SHA-256 对其进行散列处理，并存储为 **key-hash** 命令中输入字符串。因此，要删除该字符串，请使用 **nokey-hash** 命令。

key-string*key_string*

Syntax Description	<i>key_string</i> 输入公钥。

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
服务器配置	• 是	• 支持	• 支持	—	• 是

Command History	版本 修改
	9.1(5) 添加了此命令。

使用指南 您可以使用板载 SCP 客户端在 ASA 之间复制文件，也可以从 ASA 复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器，您可以指定 SSH 主机的 **key-stringkey-hash**（公钥）或（哈希值）。*key_string* 是远端对等体的采用 Base64 编码的 RSA 公钥。您可以从打开的 SSH 客户端（即 .ssh/id_rsa.pub 文件）获得公钥值。在您提交采用 Base64 编码的公钥之后，系统会通过 SHA-256 对其进行散列处理。

CR_Examples 以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

以下示例显示了已保存的散列密钥：

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
    server 10.7.8.9
        key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

命令	说明
copy	将文件复制到 ASA 或从 ASA 复制文件。
key-hash	输入散列 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
sshpubkey-chain	从 ASA 数据库中手动添加或删除服务器及其密钥。
sshstricthostkeycheck	为板载安全复制(SCP)客户端启用 SSH 主机密钥检查。

kill

要终止 Telnet 会话，请在特权 EXEC 模式下使用 **kill** 命令。

kill*telnet_id*

Syntax Description	<i>telnet_id</i> 指定 Telnet 会话 ID。

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
特权 EXEC	• 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 kill 命令允许您终止 Telnet 会话。使用 who 命令查看 Telnet 会话 ID。终止 Telnet 会话时，ASA 允许终止任何活动命令，然后丢弃连接，而不发出警告。

CR_Examples	以下示例显示如何终止 ID 为“2”的 Telnet 会话。首先，输入 who 命令可显示活动 Telnet 会话的列表。然后输入 kill2 命令终止 ID 为“2”的 Telnet 会话。

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

Related Commands	命令	说明
	telnet	配置对 ASA 的 Telnet 访问。
	who	显示活动 Telnet 会话的列表。



I2 – Iof

- l2tp tunnel hello, 第 403 页
- lacp max-bundle, 第 404 页
- lacp port-priority, 第 406 页
- lacp rate, 第 408 页
- lacp system-priority, 第 410 页
- ldap-attribute-map, 第 412 页
- ldap-base-dn, 第 414 页
- ldap-defaults, 第 416 页
- ldap-dn, 第 417 页
- ldap-group-base-dn, 第 419 页
- ldap-login-dn, 第 420 页
- ldap-login-password, 第 422 页
- ldap-naming-attribute, 第 424 页
- ldap-over-ssl, 第 426 页
- ldap-scope, 第 428 页
- leap-bypass, 第 430 页
- 许可证, 第 432 页
- license-server address, 第 434 页
- license-server backup address, 第 437 页
- license-server backup backup-id, 第 439 页
- license-server backup enable, 第 442 页
- license-server enable, 第 444 页
- license-server port, 第 447 页
- license-server refresh-interval, 第 449 页
- license-server secret, 第 451 页
- license smart, 第 453 页
- license smart deregister, 第 455 页
- license smart plr set, 第 457 页
- license smart register, 第 459 页

- [license smart renew](#) , 第 461 页
- [license smart reservation](#) , 第 463 页
- [license smart reservation cancel](#) , 第 465 页
- [license smart reservation install](#) , 第 467 页
- [许可证智能预订通用](#) , 第 469 页
- [许可证智能预留返还](#) , 第 471 页
- [lifetime \(ca server mode\)](#) , 第 473 页
- [lifetime \(ikev2 policy mode\)](#) , 第 475 页
- [limit-resource](#) , 第 477 页
- [lmfactor](#) , 第 482 页
- [load-monitor](#) , 第 484 页
- [local-base-url](#) , 第 486 页
- [local-domain-bypass](#) , 第 488 页
- [local-unit](#) , 第 490 页
- [location-logging](#) , 第 492 页

l2tp tunnel hello

要指定 L2TP over IPsec 连接上的 hello 消息之间的间隔，请在全局配置模式下使用 **l2tp tunnel hello** 命令。要将间隔重置为默认值，请使用以下命令形 **no** 式：

l2tp tunnel hello*interval*
no l2tp tunnel hello*interval*

Syntax Description

间 问候消息之间的间隔（以秒为单位）。默认值为 60 秒。范围是 10 到 300 秒。
隔

Command Default

默认值为 60 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
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

7.2(1) 添加了此命令。

使用指南

l2tp tunnel hello 命令可使 ASA 检测 L2TP 连接的物理层问题。默认值为 60 秒。在使用默认设置的情况下，L2TP 隧道可能会在 180 秒后断开连接。如果将其配置为较小的值，遇到问题的连接会提前断开。L2TP 的最大重试次数是 3。

CR_Examples

以下示例将 hello 消息之间的间隔配置为 30 秒：

```
ciscoasa(config)# l2tp tunnel hello 30
```

Related Commands

命令	说明
show vpn-session db detail remote filter protocol L2TP over IPsec	显示 L2TP 连接的详细信息。
vpn-tunnel-protocol l2tp-ipsec	启用 L2TP 作为特定隧道组的隧道协议。

lacp max-bundle

如要指定 EtherChannel 通道组中允许的最大主用接口数，请在接口配置模式下使用**lacpmax-bundle** 命令。要将值设置为默认值，请使用此命 **no** 令的形式。



注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp max-bundle编号
no lacp max-bundle

Syntax Description *number* 指定通道组中允许的最大主用接口数（介于 1 和 8 之间）；在 9.2(1) 及更高版本中，最大数量提高到 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。

Command Default (9.1 及更早版本) 默认值为 8。
(9.2(1) 和更高版本) 默认值为 16。

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	• 支持	• 支持	—	—

Command History

版本	修改
8.4(1)	添加了此命令。
9.2(1)	主用接口的数量已从 8 增加到 16。

使用指南 为端口通道接口输入此命令。每个通道组的最大主用接口数量是 8；要减少数量，请使用此命令。

CR_Examples 以下示例将 EtherChannel 中的最大接口数设置为 4：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```


Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

lacp port-priority

要在 EtherChannel 中为物理接口设置优先级，请在接口配置模式下使用**lacpport-priority**命令。要将优先级设置为默认值，请使用此命令的 **no**形式。



注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp port-priority编号
no lacp port-priority

Syntax Description *number* 将优先级设置为 1 和 65535 之间。数字越大，优先级越低。

Command Default 默认值为 32768。

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	• 支持	• 支持	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

为物理接口输入此命令。如果分配的接口多于可用的接口，则ASA将使用此设置决定哪些接口是主用接口，哪些是备用接口。如果所有接口的端口优先级设置都相同，则优先级由接口 ID（插槽/端口）确定。最低接口 ID 具有最高优先级。例如，GigabitEthernet 0/0 的优先级高于 GigabitEthernet 0/1。

如果要将某个接口优先确定为主用接口（即使它具有较高的接口 ID 也如此），请将此命令设置为具有较低的值。例如，要使千兆以太网 1/3 在千兆以太网 0/7 之前处于活动状态，则将 1/3 接口上的 **lacpport-priority** 值设为 12345，将 0/7 接口上的值设为默认值 32768。

如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。查看命令。 **lacpsystem-priority**

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。

CR_Examples

以下示例为 GigabitEthernet 0/2 设置较低的端口优先级，使其先于 GigabitEthernet 0/0 和 0/1 用作 EtherChannel 的一部分：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载均衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

lacp rate

要设置接口为 EtherChannel 中的物理接口接收 LACP 数据单元的速率，请在接口配置模式下使用 **lacp rate** 命令。要将速率设置为默认值，请使用此命 **no** 令的形式。



注释 仅在 Cisco Secure Firewall 3100/4200 上受支持。

lacp rate {normal | fast}
no lacp rate

Syntax Description

normal 将接收 LACP 数据单元的速率设置为每 30 秒一次。“正常”也称为“缓慢”。

fast 将 LACP 数据单元接收速率设置为每秒一次。

Command Default

默认是正常的。

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
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本 修改

9.17(1) 添加了此命令。

使用指南

设置速率（正常或快速）时，设备会向连接的交换机请求该速率。作为回报，设备将按照连接的交换机请求的速率进行发送。我们建议您在两端设置相同的速率。

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。

CR_Examples

以下示例将 EtherChannel 1 中两个接口上的速率设置为“快速”：

```
ciscoasa(config)# interface Ethernet1/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
```

```
ciscoasa(config-if)# interface Ethernet1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。

lacp system-priority

对于 EtherChannel，要为 ASA 全局设置 LACP 系统优先级，请在全局配置模式下使用 **lacpsystem-priority**命令。要将值设置为默认值，请使用此命 **no** 令的形式。



注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp system-priority编号
no lacp system-priority

Syntax Description *number* 设置 LACP 系统优先级，范围为 1 到 65535。默认值为 32768。数字越大，优先级越低。对于 ASA 而言，此命令是全局命令。

Command Default 默认值为 32768。

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	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南 如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。有关以太网通道内的接口优先级，请参阅 **lacpport-priority** 命令。

CR_Examples 以下示例将系统优先级设置为高于默认值（较小的数字）：

```
ciscoasa(config)# lacp system-priority 12345
```

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。

命令	说明
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

ldap-attribute-map

要将现有映射配置绑定到LDAP主机，请在aaa-server主机配置模式下使用**ldap-attribute-map**命令。
要删除绑定，请使用此**no**命令的形式。

```
ldap-attribute-map map-name
no ldap-attribute-map map-name
```

Syntax Description **map-name** 指定LDAP属性映射配置。

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
AAA服务器主机配置	• 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** 如果思科定义的LDAP属性名称不能满足您的易用性或其他要求，您可以创建自己的属性名称，将其映射到思科属性，然后将生成的属性配置绑定到LDAP服务器。通常的步骤包括：
1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令进入ldap属性映射配置模式。请注意，此命令中的“ldap”后面没有连字符。
 2. 在ldap-attribute-map配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射配置。
 3. 在aaa-server主机模式下使用 **ldap-attribute-map** 命令将属性映射配置绑定到LDAP服务器。

CR_Examples 在aaa-server主机配置模式下输入的以下示例命令将名为myldapmap的现有属性映射绑定到名为ldapsvr1的LDAP服务器：

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```


Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
map-name	将用户定义的 LDAP 属性名称与思科 LDAP 属性名称映射。
map-value	将用户定义的属性值映射到思科属性。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射配置或所有运行属性映射配置。
clearconfigureldapattribute-map	删除所有 LDAP 属性映射。

ldap-base-dn

要指定服务器在收到授权请求时应在 LDAP 层次结构中开始搜索的位置，请在**ldap-base-dn**aaa-server 主机配置模式下使用该命令。可从 **aaa-server** 协议配置模式访问 **aaa-server** 主机配置模式。要删除该指定，从而将搜索重置为从列表顶部开始，请使用此命令的 **no** 形式。

ldap-base-dn字符串
no ldap-base-dn

Syntax Description	<i>string</i> 一个区分大小写的字符串，最多 128 个字符，用于指定服务器在收到授权请求时应在 LDAP 层次结构中开始搜索的位置；例如，OU=Cisco。

Command Default	从列表顶部开始搜索。

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服务器主机配置	• 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	该命令仅适用于 LDAP 服务器。

CR Examples	以下示例在主机 1.2.3.4 上配置名为 svrgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 基本 DN 配置为 starthere 。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
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
)# ldap-base-dn starthere
ciscoasa
```

```
(config-aaa-server-host)#  
exit
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。

ldap-defaults

要定义 LDAP 默认值，请在 `crl configure` 配置模式下使用 **ldap-defaults**命令。可从加密 `ca` 信任点配置模式访问 `Crl configure` 配置模式。这些默认值仅在 LDAP 服务器需要时使用。要指定无 LDAP 默认值，请使用此命令 **no** 的形式。

ldap-defaults*server* [*port*]
no ldap-defaults

Syntax Description	<i>port</i> （可选）指定 LDAP 服务器端口。如果未指定此参数，则 ASA 使用标准 LDAP 端口 (389)。
	<i>server</i> 指定LDAP服务器的IP地址或域名。如果 CRL 分发点中存在该证书，则它将覆盖该值。

Command Default	默认设置未设置。

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
Crl configure 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History	版本 修改
	7.0(1) 添加了此命令。

CR_Examples	以下示例定义默认端口 (389) 上的 LDAP 默认值：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands	命令	说明
	crlconfigure	进入 ca-crl 配置模式。
	cryptocatrustpoint	进入 trustpoint 配置模式。
	protocolldap	指定 LDAP 作为 CRL 的检索方法。

ldap-dn

要传递 X.500 可分辨名称和密码到要求对 CRL 检索进行身份验证的 LDAP 服务器，请在 `crl configure` 配置模式下使用 **ldap-dn** 命令。可从加密 `ca` 信任点配置模式访问 `Crl configure` 配置模式。这些参数仅在 LDAP 服务器需要时使用。要指定任何 LDAP DN，请使用此命令的 **no** 形式。

ldap-dn *x.500-namepassword*
no ldap-dn

Syntax Description

password 为此可分辨名称定义密码。最大字段长度为 128 个字符。

x.500 名 定义用于访问此 CRL 数据库的目录路径，例如：`cn=crl,ou=certs,o=CANAME,c=US`。最大字段长度为 128 个字符。

Command Default

默认设置未开启。

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
Crl configure 配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

CR_Examples

以下示例为 trustpoint Central 指定 X.500 名称 `CN=admin,OU=devtest,O=engineering` 和密码 `xx` 这样的信息：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzyy
```

Related Commands

命令	说明
crlconfigure	进入 <code>crl configure</code> 配置模式。
cryptocatrustpoint	进入 CA 信任点配置模式。

命令	说明
protocolldap	指定 LDAP 作为 CRL 的检索方法。

ldap-group-base-dn

要在 Active Directory 层次结构中指定用于组搜索的动态访问策略的基本组，请在 aaa-server 主机配置模式下使用 **ldap-group-base-dn** 命令。要从运行配置中删除该命令，请使用该命令的 no 形式：

ldap-group-base-dn [*string*]
no ldap-group-base-dn [*string*]

Syntax Description

string 区分大小写的字符串，最多 128 个字符，用于指定 Active Directory 层次结构中服务器应开始搜索的位置。例如，ou=Employees。该字符串中不允许使用空格，但是允许使用其他特殊字符。

Command Default

无默认行为或值。如果不指定组搜索 DN，则从基本 DN 开始搜索。

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主机配置模式	• 是	—	• 是	—	—

Command History

版本 修改

8.0(4) 添加了此命令。

使用指南

ldap-group-base-dn 命令仅适用于使用 LDAP 的 Active Directory 服务器，并指定 **showad-groups** 命令用于开始其组搜索的 Active Directory 层次结构级别。动态组策略将从搜索中检索到的组用作特定策略的选择条件。

CR_Examples

以下示例设置组基础 DN，以在组织单位 (ou) 级别 Employees 开始搜索：

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

Related Commands

命令	说明
group-search-timeout	调整 ASA 等待 Active Directory 服务器响应的时间，以获取组列表。
showad-groups	显示在 Active Directory 服务器上列出的组。

ldap-login-dn

如要指定系统应将其绑定为的目录对象名称，请在 `aaa-server` 主机配置模式下使用 `ldap-login-dn` 命令。可从 `aaa-server` 协议配置模式访问 `aaa-server` 主机配置模式。要删除此规范，请使用此 `no` 命令的形式。

ldap-login-dn 字符串
no ldap-login-dn

Syntax Description *string* 一个区分大小写的字符串，最多 128 个字符，用于指定 LDAP 层次结构中的目录对象的名称。该字符串中不允许使用空格，但是允许使用其他特殊字符。

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服务器主机配置	• 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 该命令仅适用于 LDAP 服务器。支持的最大字符串长度为 128 个字符。

某些 LDAP 服务器（包括 Microsoft Active Directory 服务器）要求 ASA 通过经过身份验证的绑定建立握手，然后才能接受对任何其他 LDAP 操作的请求。ASA 通过将 Login DN 字段关联到用户验证请求，为通过身份验证的绑定标识自己。Login DN 字段介绍 ASA 的身份验证特征。这些特征应与具有管理员权限的用户的特征相对应。

对于 字符串 变量，请为 VPN 集中器身份验证绑定输入目录对象的名称，例如：`cn=Administrator`、`cn=users`、`ou=person`、`dc=XYZ Corporation`、`dc=com`。对于匿名访问，请将此字段留空。

CR_Examples 以下示例在主机 1.2.3.4 上配置名为 `svrgrp1` 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 登录 DN 配置为 `myobjectname`。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
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)
# ldap-login-dn myobjectname
ciscoasa(config-aaa-server
-host)
#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-login-password

要指定 LDAP 服务器的登录密码，请在 aaa-server 主机配置模式下使用 **ldap-login-password** 命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除此密码规范，请使用以下命令 **no** 的形式：

ldap-login-password 字符串
no ldap-login-password

Syntax Description *string* 区分大小写的字母数字密码，最长 64 个字符。密码不能包含空格字符。

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
AAA服务器主机配置	• 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 该命令仅适用于 LDAP 服务器。密码字符串的最大长度为 64 个字符。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 svrgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 登录密码配置为 obscurepassword。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server)# timeout 9
ciscoasa
(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa
(config-aaa-server)#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-naming-attribute

要指定相对可分辨名称属性，请在 `aaa-server hostconfiguration [] configuration` 模式下使用 **ldap-naming-attribute** 命令。可从 `aaa-server` 协议配置模式访问 `aaa-server` 主机配置模式。要删除此规范，请使用此命令 **no** 的形式：

ldap-naming-attribute 字符串
no ldap-naming-attribute

Syntax Description *string* 区分大小写的字母数字相对可分辨名称属性，最多包含 128 个字符，用于唯一标识 LDAP 服务器上的条目。该字符串中不允许使用空格，但是允许使用其他特殊字符。

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服务器主机配置	• 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

输入唯一标识 LDAP 服务器上条目的相对可分辨名称属性。常见的命名属性有通用名称（cn）和用户 ID（uid）。

该命令仅适用于 LDAP 服务器。支持的最大字符串长度为 128 个字符。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 `svrgrp1` 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 命名属性配置为 `cn`。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
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
) # ldap-naming-attribute cn
ciscoasa
(config-aaa-server-host) #
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-over-ssl

要在 ASA 与 LDAP 服务器之间建立安全 SSL 连接，请在 aaa-server 主机配置模式下使用 **ldap-over-ssl** 命令。要禁用连接的 SSL，请使用此命令 **no** 的形式。

ldap-over-ssl [**enable** | **reference-identity** 引用 ID 名称]

no ldap-over-ssl [**enable** | **reference-identity** 引用 ID 名称]

Syntax Description	enable	指定使用 SSL 保护与 LDAP 服务器的连接。
	reference-identity 引用 ID 名称	指定引用身份名称来验证 LDAP 服务器身份。

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
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	7.1(1)	添加了此命令。
	9.18(1)	此命令已得到增强，以验证 LDAP 服务器身份。

使用指南 使用此命令可指定SSL 保护 ASA 和 LDAP 服务器之间的连接。



注释 如果您使用纯文本身身份验证，我们建议启用此功能。请参阅 **sasl-mechanism**命令。

CR_Examples

在 aaa-server 主机配置模式下输入的以下命令为 ASA 与 IP 地址为 10.10.0.1 的名为 ldapsvr1 的 LDAP 服务器之间的连接启用 SSL。它们还配置明文 SASL 身份验证机制。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
```

```
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)#
```

要通过指定引用身份名称验证 LDAP 服务器身份，请使用 **reference-identityref_id_name**。引用标识对象使用具有匹配条件的 **crypto ca reference-identity refidname** 来创建。在 **ldap aaa-server** 配置下配置 **reference-identity** 时，ASA 会尝试查找与 **ldap** 服务器证书匹配的主机名。如果无法解析主机或未找到匹配项，则连接将终止并显示错误消息。

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
    enable          Require an SSL connection to the LDAP server
    reference-identity Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
    WORD < 65 char Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
    <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

show running-config aaa server 将配置的 **reference-identity name** 显示为以下选项之一：

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

Related Commands

命令	说明
sasl-mechanism	指定 LDAP 客户端和服务端之间的 SASL 身份验证。
server-type	将 LDAP 服务器供应商指定为 Microsoft 或 Sun。
ssl-client-certificate	指定使用 LDAPS 时 ASA 应作为客户端证书呈现给 LDAP 服务器的证书。
crypto ca reference-identity refidname	要配置 reference-identity 对象。

ldap-scope

要指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围，请在 **ldap-scope**aaa-server 主机配置模式下使用该命令。可从 **aaa-server** 协议配置模式访问 **aaa-server** 主机配置模式。要删除此规范，请使用此 **no**命令的形式。

ldap-scope*scope*
no **ldap-scope**

Syntax Description

scope 服务器收到授权请求时要搜索的 LDAP 层次结构的级别数。有效值为：

- 一 **onelevel**搜索基本 DN 之下的一级
- **subtree**- 搜索基本 DN 以下的所有级别

Command Default

默认值为 **onelevel**。

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服务器主机配置	• 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

将范围指定为 **onelevel** 可使搜索速度加快，因为只会搜索 Base DN 以下的一个级别。指定 **subtree** 的速度较慢，因为系统会搜索 Base DN 以下的所有级别。

该命令仅适用于 LDAP 服务器。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 **svrgrp1** 的 LDAP AAA 服务器，设置超时时间为 9 秒，设置重试间隔为 7 秒，并将 LDAP 范围配置为包括子树级别。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
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)# ldap-scope subtree
ciscoasa
(config-aaa-server-host)#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-naming-attribute	指定唯一标识 LDAP 服务器上的条目的相对可分辨名称属性（或多个属性）。

leap-bypass

要启用 LEAP Bypass，请在 **leap-bypassenable** 策略组配置模式下使用该命令。要禁用 LEAP 绕行，请使用 **leap-bypassdisable**命令。要从运行配置中删除 LEAP Bypass 属性，请使用此命令的 **no**形式。此选项允许从另一个组策略继承 LEAP Bypass 的值。

```
leap-bypass { enable | disable }  
no leap-bypass
```

Syntax Description	disable 禁用 LEAP 旁路。
	enable 启用 LEAP 旁路。

Command Default	LEAP 旁路已禁用。

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
组策略配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南

启用后，LEAP Bypass 允许来自 VPN 硬件客户端后面的无线设备的 LEAP 数据包在用户身份验证之前通过 VPN 隧道传输。这样就可让使用思科无线接入点设备的工作站建立 LEAP 身份验证。然后，设备可以按用户身份再次进行身份验证。

如果启用交互式硬件客户端身份验证，则此功能无法按预期工作。

有关更多信息，请参阅 CLI 配置指南。



注释 允许任何未经身份验证的流量穿越隧道可能会存在安全风险。

CR_Examples

以下示例显示如何为名为 “FirstGroup” 的组策略设置 LEAP Bypass：

```
ciscoasa(config)# group-policy FirstGroup attributes  
ciscoasa(config-group-policy)# leap-bypass enable
```

Related Commands

命令	说明
secure-unit-authentication	要求 VPN 硬件客户端在每次启动隧道时使用用户名和密码进行身份验证。
user-authentication	要求 VPN 硬件客户端后面的用户在连接之前向 ASA 证明自己的身份。

许可证

要配置 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，请在 **licensescansafe** 常规选项配置模式下使用该命令。要删除许可证，请使用此命令的 **no** 形式。

```
licensehex_key
nolicense [hex_key]
```

Syntax Description *hex_key* 将身份验证密钥指定为 16 字节十六进制数。

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	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南 每个 ASA 必须使用您从云网络安全获取的身份验证密钥。身份验证密钥让云网络安全识别与网络请求相关的公司，并确保 ASA 与有效客户相关联。

可以为 ASA 使用两种身份验证密钥类型之一：公司密钥或组密钥。

公司认证密钥

公司身份验证密钥可在同一公司内的多个 ASA 上使用。此密钥仅为您的 ASA 启用云网络安全服务。管理员在 ScanCenter (<https://scancenter.scansafe.com/portal/admin/login.jsp>) 中生成此密钥；您可以通过邮件发送密钥以供日后使用。您稍后无法在 ScanCenter 中查找此密钥；则仅在 ScanCenter 中显示最后 4 位数字有关更多信息，请参阅云网络安全文档：
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html。

组认证密钥

组身份验证密钥是每个 ASA 独有的特殊密钥，可执行两项功能：

- 为 ASA 启用云网络安全服务。
- 识别 ASA 的所有流量，以便可以为每个 ASA 创建 ScanCenter 策略。

管理员在 ScanCenter (<https://scancenter.scansafe.com/portal/admin/login.jsp>) 中生成此密钥；您可以通过邮件发送密钥以供日后使用。您稍后无法在 ScanCenter 中查找此密钥；则仅在 ScanCenter 中显示最后 4 位数字有关更多信息，请参阅云网络安全文档：

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html。

CR_Examples

以下示例仅配置主服务器：

```
scansafe general-options server primary ip 180.24.0.62 port 8080 retry-count 5 license
366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户身份，则指定默认用户名和/或组。
[https] (参数)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，以指示请求来自哪个组织。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前等待的时间。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-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。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

license-server address

要标识供参与者使用的共享许可服务器 IP 地址和共享密钥，请在全局配置模式下使用 **license-serveraddress**命令。要禁用参与共享许可，请使用此命令的 **no** 形式。共享许可证允许您购买大量 SSL VPN 会话，并通过将其中一个 ASA 配置为共享许可服务器，将其余 ASA 配置为共享许可参与者，在一组 ASA 之间根据需要共享会话。

license-server address地址**secret**密钥 [**port**port]
no license-server address [地址**secret**密钥 [**port**port]]

Syntax Description

地址	标识共享许可服务器 IP 地址。
port端口	（可选）如果您使用该命令更改了服务器配置中的 license-serverport 默认端口，请将备份服务器的端口设置为匹配，介于 1 和 65535 之间。默认端口为 50554。
secretsecret	标识共享密钥。密钥必须与服务器上使用 license-serversecret 命令设置的密钥相匹配。

Command Default

默认端口为 50554。

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
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

共享许可参与者必须拥有共享许可参与者密钥。使用 **showactivation-key**命令检查已安装的许可证。只能为每个参与者指定一个共享许可证服务器。

以下步骤说明共享许可证的工作方式：

1. 确定哪一台 ASA 应充当共享许可服务器，然后使用该设备的序列号购买共享许可服务器许可证。
2. 确定哪些 ASA 应充当共享许可参与者（包括共享许可备用服务器），并使用每台设备的序列号获取每台设备的共享许可参与者许可证。
3. （可选）将另一台 ASA 指定为共享许可备用服务器。只能指定一台备用服务器。



注释 共享许可备用服务器仅需要参与者许可证。

1. 请在共享许可服务器上配置一个共享密钥；具有该共享密钥的所有参与者都可以使用共享许可证。
2. 将 ASA 配置为参与者时，它通过发送有关自身的信息（包括本地许可证和型号信息）向共享许可服务器注册。



注释 参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

1. 共享许可服务器会使用参与者应轮询服务器的频率的有关信息进行响应。
2. 当参与者用尽本地许可证的会话时，它会向共享许可服务器发出请求，从而获取更多会话（以 50 个会话为增量）。
3. 共享许可服务器使用共享许可证进行响应。参与者使用的会话总数不能超过平台型号的最大会话数。



注释 如果共享许可服务器的本地会话用完，它也可以参与共享许可证池。它进行参与既不需要参与者许可证，也不需要服务器许可证。

1. 如果在共享许可证池中没有为参与者留下足够多的会话，则服务器通过提供尽可能多的可用会话进行响应。
2. 参与者会继续发送请求更多会话的刷新消息，直到服务器可以充分满足请求。
3. 当参与者的负载减少时，它会向服务器发送消息，以释放共享会话。



注释 ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参与者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

- 如果参与者在 3 倍刷新间隔后未能发送刷新信息，则服务器会将会话释放回共享许可证池。
- 如果参与者无法访问许可证服务器以发送刷新消息，则参与者可以继续使用其从服务器收到的共享许可证，最多可使用 24 小时。
- 如果在 24 小时后，参与者仍无法与许可证服务器通信，则参与者将释放共享许可证，即使其仍然需要会话也如此。参与者会保留已建立的现有连接，但无法接受超过许可证限制的新连接。

- 如果在 24 小时的时间到期之前且服务器使参与者会话到期之后，参与者与服务器重新连接，则参与者需要为会话发送新的请求；服务器通过可向该参与者发送尽可能多的会话进行响应。

CR_Examples

以下示例设置许可服务器 IP 地址和共享密钥，以及备用许可服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新闻隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup address

要标识供参与者使用的共享许可备用服务器 IP 地址，请在全局配置模式下使用 **license-server backup address** 命令。要禁用备份服务器，请使用此命令的形式 **no**。

license-server backup address *address*
no license-server address [*address*]

Syntax Description

地 标识共享许可备用服务器 IP 地址。
 址

Command Default

无默认为或值。

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	—	• 是	—	—

Command History

版本 修改

8.2(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

共享许可备用服务器必须配置 **license-server backup enable** 命令。

CR_Examples

以下示例设置许可服务器 IP 地址和共享密钥，以及备用许可服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-server address	标识参与者的共享许可服务器 IP 地址和共享机密。

命令	说明
license-server backup backup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	使一个单元成为共享许可备份服务器。
license-server enable	使一个单元成为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新闻隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared-license	显示共享许可证统计信息。
show vpn-session db	显示有关 VPN 会话的许可证信息。

license-server backup backup-id

要在主共享许可服务器配置中标识共享许可备用服务器，请在全局配置模式下使用 **license-server backup backup-id** 命令。要删除备份服务器配置，请使用此命令的 **no** 形式。

license-server backup 地址 **backup-id** serial_number [**ha-backup-id** ha_serial_number]
no license-server backup 地址 [**backup-id** serial_number [**ha-backup-id** ha_serial_number]]

Syntax Description

地址	标识共享许可备用服务器 IP 地址。
backup-id serial_number	标识共享许可备用服务器序列号。
ha-backup-id ha_serial_number	如果对备用服务器使用故障转移，则标识辅助共享许可备用服务器序列号。

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	—	• 是	—	—

Command History

版本 修改

8.2(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

只能确定 1 台备用服务器及其可选的备用设备。

要查看备用服务器序列号，请输入 **show activation-key** 命令。

要使参与者成为备用服务器，请使用 **license-server backup enable** 命令。

共享许可备用服务器必须先成功向主共享许可服务器注册，然后才能承担备用角色。当其注册时，主共享许可服务器将与备用服务器同步服务器设置以及共享许可证信息，其中包括已注册参与者的列表以及当前的许可证使用情况。主服务器和备用服务器以 10 秒为间隔同步数据。在最初的同步之后，即使经过重新加载，备份服务器也能够成功履行备用职责。

当主服务器发生故障时，备用服务器会接管服务器操作。备用服务器可以连续运行最多 30 天，在此之后，备用服务器会停止向参与者发出会话，而且现有会话将会超时。请务必在此 30 天的时段内恢复主服务器。关键级别的系统日志消息会在 15 天时发送，并在 30 天时再次发送。

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

当备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。



注释 首次启动主共享许可服务器时，备用服务器仅可独立运行 5 天。运行限制将逐日延长，直至达到 30 天。此外，如果此后主服务器停止运行任意时长，则备用服务器的运行限制会逐日缩短。当主服务器恢复正常运行时，备用服务器的运行限制会开始再次逐日延长。例如，如果主服务器停止运行 20 天，在此期间备用服务器处于主用状态，则备用服务器的运行限制将仅剩余 10 天。备份服务器在继续充当非主用的备用服务器 20 天后，将“充值”至最长的 30 天运行限制。实施此“充值”功能是为了防止滥用共享许可证。

CR_Examples

以下示例设置共享密钥、更改刷新闻隔和端口、配置备用服务器，并在内部接口和 dmz 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新闻隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。

命令	说明
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup enable

要使此设备成为共享许可备用服务器，请在全局配置模式下使用 **license-server backup enable** 命令。
要禁用备份服务器，请使用此命令 **no** 的形式。

```
license-server backup enable interface_name
no license-server backup enable interface_name
```

Syntax Description *interface_name* 指定参与者联系备份服务器的接口。您可以为所需数量的接口重复此命令。

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
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

备用服务器必须具有共享许可参与者密钥。

共享许可备用服务器必须先成功向主共享许可服务器注册，然后才能承担备用角色。当其注册时，主共享许可服务器将与备用服务器同步服务器设置以及共享许可证信息，其中包括已注册参与者的列表以及当前的许可证使用情况。主服务器和备用服务器以 10 秒为间隔同步数据。在最初的同步之后，即使经过重新加载，备份服务器也能够成功履行备用职责。

当主服务器发生故障时，备用服务器会接管服务器操作。备用服务器可以连续运行最多 30 天，在此之后，备用服务器会停止向参与者发出会话，而且现有会话将会超时。请务必在此 30 天的时段内恢复主服务器。关键级别的系统日志消息会在 15 天时发送，并在 30 天时再次发送。

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

当备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。



注释 首次启动主共享许可服务器时，备用服务器仅可独立运行 5 天。运行限制将逐日延长，直至达到 30 天。此外，如果此后主服务器停止运行任意时长，则备用服务器的运行限制会逐日缩短。当主服务器恢复正常运行时，备用服务器的运行限制会开始再次逐日延长。例如，如果主服务器停止运行 20 天，在此期间备用服务器处于主用状态，则备用服务器的运行限制将仅剩余 10 天。备份服务器在继续充当非主用的备用服务器 20 天后，将“充值”至最长的 30 天运行限制。实施此“充值”功能是为了防止滥用共享许可证。

CR_Examples

以下示例标识许可证服务器和共享密钥，并启用此单元作为内部接口和 dmz 接口上的备份共享许可证服务器。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新闻隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server enable

要将此设备标识为共享许可服务器，请在全局配置模式下使用 **license-serverenable**命令。要禁用共享许可服务器，请使用此命 **no** 令的形式。共享许可证允许您购买大量 SSL VPN 会话，并通过将其中一个 ASA 配置为共享许可服务器，将其余 ASA 配置为共享许可参与者，在一组 ASA 之间根据需要共享会话。

license-server enable*interface_name*
no license-server enable*interface_name*

Syntax Description *interface_name* 指定参与者联系服务器的接口。您可以为所需数量的接口重复此命令。

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
全局配置	• 是	—	• 是	• 支持	—

Command History	版本	修改
	8.2(1)	添加了此命令。
	9.0(1)	增加了多情景模式支持。

- 使用指南** 共享许可服务器必须具有共享许可服务器密钥。使用 **showactivation-key**命令检查已安装的许可证。以下步骤说明共享许可证的工作方式：
1. 确定哪一台 ASA 应充当共享许可服务器，然后使用该设备的序列号购买共享许可服务器许可证。
 2. 确定哪些 ASA 应充当共享许可参与者（包括共享许可备用服务器），并使用每台设备的序列号获取每台设备的共享许可参与者许可证。
 3. （可选）将另一台 ASA 指定为共享许可备用服务器。只能指定一台备用服务器。



注释 共享许可备用服务器仅需要参与者许可证。

1. 请在共享许可服务器上配置一个共享密钥；具有该共享密钥的所有参与者都可以使用共享许可证。
2. 将 ASA 配置为参与者时，它通过发送有关自身的信息（包括本地许可证和型号信息）向共享许可服务器注册。



注释 参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

1. 共享许可服务器会使用参与者应轮询服务器的频率的有关信息进行响应。
2. 当参与者用尽本地许可证的会话时，它会向共享许可服务器发出请求，从而获取更多会话（以 50 个会话为增量）。
3. 共享许可服务器使用共享许可证进行响应。参与者使用的会话总数不能超过平台型号的最大会话数。



注释 如果共享许可服务器的本地会话用完，它也可以参与共享许可证池。它进行参与既不需要参与者许可证，也不需要服务器许可证。

1. 如果在共享许可证池中未能为参与者留下足够多的会话，则服务器通过提供尽可能多的可用会话进行响应。
2. 参与者会继续发送请求更多会话的刷新消息，直到服务器可以充分满足请求。
3. 当参与者的负载减少时，它会向服务器发送消息，以释放共享会话。



注释 ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参与者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

- 如果参与者在 3 倍刷新间隔后未能发送刷新信息，则服务器会将会话释放回共享许可证池。
- 如果参与者无法访问许可证服务器以发送刷新消息，则参与者可以继续使用其从服务器收到的共享许可证，最多可使用 24 小时。
- 如果在 24 小时后，参与者仍无法与许可证服务器通信，则参与者将释放共享许可证，即使其仍然需要会话也如此。参与者会保留已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果在 24 小时的时间到期之前且服务器使参与者会话到期之后，参与者与服务器重新连接，则参与者需要为会话发送新的请求；服务器通过可向该参与者发送尽可能多的会话进行响应。

CR_Examples

以下示例设置共享密钥、更改刷新闻隔和端口、配置备用服务器，并在内部接口和 DMZ 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新闻隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server port

要设置共享许可服务器在其上侦听来自参与者的 SSL 连接的端口，请在全局配置模式下使用 **license-server port** 命令。要恢复默认端口，请使用此命令 **no** 的形式。

license-server port 端口
no license-server port [端口]

Syntax Description

seconds 设置服务器侦听来自参与者的 SSL 连接的端口，介于 1 到 65535 之间。默认值为 TCP 端口 50554。

Command Default

默认端口为 50554。

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

8.2(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

如果您更改默认的端口，请务必使用 **license-server address** 命令为每个参与者设置相同的端口。

CR Examples

以下示例设置共享密钥、更改刷新间隔和端口、配置备用服务器，并在内部接口和 DMZ 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。

命令	说明
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server refresh-interval

要设置为参与者提供的刷新闻隔，以便设置它们应与共享许可服务器通信的频率，请在全局配置模式下使用 **license-server refresh-interval** 命令。要恢复默认刷新闻隔，请使用此命令 **no** 的形式。

license-server refresh-interval 秒
no license-server refresh-interval [秒]

Syntax Description *seconds* 将刷新闻隔设置为 10 到 300 秒。默认值为 30 秒。

Command Default 默认值为 30 秒。

Command Modes 下表展示可输入命令的模式：

命令模式	防火牆模式		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
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南 每个参与者定期与使用 SSL 的共享许可服务器通信，以便共享许可服务器可以跟踪当前许可证使用情况并接收和响应许可证请求。

CR_Examples

以下示例设置共享密钥、更改刷新闻隔和端口、配置备用服务器，并在内部接口和 dmz 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands	命令	说明
	activation-key	输入许可证激活密钥。

命令	说明
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server secret

要在共享许可服务器上设置共享密钥，请在全局配置模式下使用 **license-serversecret** 命令。要删除秘密，请使用此命令 **no** 的形式。

license-server secretsecret
no license-server secretsecret

Syntax Description

secret 设置共享密钥，一个介于 4 到 128 个 ASCII 字符之间的字符串。

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	—	• 是	—	—

Command History

版本 修改

8.2(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

任何在命令中识别出此秘密的 **license-serveraddress** 参与者都可以使用许可服务器。

CR_Examples

以下示例设置共享密钥、更改刷新间隔和端口、配置备用服务器，并在内部接口和 dmz 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。

命令	说明
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license smart

要设置智能许可授权请求，请在**licensesmart**全局配置模式下使用该命令。要删除授权并取消许可您的设备，请使用此命令的 **no** 形式。



注释 仅 ASA virtual 和机箱支持此功能。

license smart
no license smart

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
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.3(2)	添加此命令是为了提供 ASA virtual 支持。
9.4(1.152)	增加了对 Firepower 9300 的支持。
9.6(1)	增加了对 Firepower 4100 系列的支持。
9.8(2)	增加了对 Firepower 2100 系列的支持。

使用指南

此命令可进入许可证智能配置模式，在此模式下可以设置功能层和其他许可证授权。对于 ASA virtual，当您第一次请求授权时，您必须退出许可证智能配置模式才能使您的更改生效。

CR_Examples

以下示例将功能级别设置为“标准”，并将吞吐量级别设置为 2G：

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart deregister

要从智能许可的思科许可证颁发机构取消注册设备，请在特权 EXEC 模式下使用 **licensesmartderegister** 命令。



注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

license smart deregister

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
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本 修改

9.3(2) 添加此命令是为了提供 ASA virtual 支持。

9.8(2) 添加了对 Firepower 2100 系列的支持。

使用指南

取消注册 ASA 将从您的帐户删除 ASA。系统会删除 ASA 上的所有许可证授权和证书。您可能需要取消注册才能释放许可证以用于新的 ASA。此命令导致 ASA 重新加载。

CR_Examples

以下示例取消注册设备：

```
ciscoasa# license smart deregister
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。

命令	说明
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart plr set

要配置与 RAM 和 vCPU 无关的永久许可证预留（灵活的永久许可证预留模式），请在 **license smart plr set**全局配置模式下使用该命令。

要禁用灵活永久许可证预留，请在使用 **no license smart reservation** 命令禁用永久许可证预留模式后，使用此命令的 **no** 形式。



注释 此功能受支持。ASA virtual

license smart plr set { ASAV_5_UNIVERSAL | ASAV_10_UNIVERSAL | ASAV_30_UNIVERSAL | ASAV_50_UNIVERSAL | ASAV_100_UNIVERSAL | ASAV_U_UNIVERSAL }

Syntax Description	ASAV_5_UNIVERSAL	ASAv5 授权
	ASAV_10_UNIVERSAL	ASAv10 授权
	ASAV_30_UNIVERSAL	ASAv30 授权
	ASAV_50_UNIVERSAL	ASAv50 授权
	ASAV_100_UNIVERSAL	ASAv100 授权
	ASAV_U_UNIVERSAL	ASAvU 授权

Command Default 无默认为行为或值。

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	—	• 是

Command History	版本 修改
	923(1) 添加此命令是为了提供 ASA virtual 支持。

使用指南 您可以配置任何型号特定许可证，而不考虑分配给 ASA virtual 的 RAM 和 vCPU。此永久许可证预留模式称为灵活永久许可证预留模式。您指定的型号许可证会设置 ASA virtual 的吞吐量水平。您的内

存决 ASA virtual 定了最大安全客户端、TLS 代理会话、最大并发防火墙连接和 VLAN。这些不是由模型许可证决定的。但是，较低的 ASA virtual 内存配置文件将限制实际的会话和功能数量。

例如，如果 ASA virtual 有 8 GB RAM 并注册了 ASAV_50_UNIVERSAL，则分配的最大安全客户端会话数为 750。当会话超过此限制时，系统就会丢弃这些连接。

此永久许可证预留许可证模式的其他优势包括：

- 您可以在永久许可证预留许可证之间切换，而不考虑分配给 ASA virtual 的内存。但是，如果 ASA virtual 的vCPU 超过 16 个，则您只能配置 ASAvU（无限）许可证。
- 您可以更改分配给 ASA virtual 的内存和 vCPU，而无需更改型号许可证。

示例

要配置永久许可证预留的 ASAv30 授权，请执行以下操作：

```
ciscoasa (config)# license smart plr set ASAV_30_UNIVERSAL
ciscoasa (config)# license smart reservation
ciscoasa (config)#license smart reservation request universal
```

Related Commands

命令	说明
license smart reservation	启用永久许可证保留
license smart reservation request universal call-home	请求许可证代码以输入智能软件管理器。

license smart register

要向思科许可证颁发机构注册设备以获取智能许可，请在特权 EXEC 模式下使用 **licensesmartregister** 命令。



注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

license smart register idtokenid_token [force]

Syntax Description	idtokenid_token 在智能软件管理器中，请求并复制要添加此 ASA 的虚拟帐户的注册令牌。
	force 注册已注册但可能与许可证颁发机构不同步的 ASA。

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) 添加此命令是为了提供 ASA virtual 支持。
	9.8(2) 添加了对 Firepower 2100 系列的支持。

使用指南 当您注册 ASA 时，许可证颁发机构会颁发 ID 证书，用于 ASA 和许可证颁发机构之间的通信。它还将 ASA 分配给适当的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于通信问题等原因过期，您可能需要稍后重新注册 ASA。

CR_Examples 以下示例使用注册令牌进行注册：

```
ciscoasa# license smart register idtoken
YjE3Njc3MzYmQzMi00OTp4LWUwODItZmQ5NGRlYjUxLTM0NDYjADQzZl8wK2ozV3SE0ZkgQdRrZlNlNGlYRnBHUjcr0ZWlB4IU4w%0Ac2NmD0%3D%0A
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart renew

要为智能许可更新注册或许可证授权，请在特权 EXEC 模式下使用 **licensesmartrenew** 命令。



注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

license smart renew {id | auth}

Syntax Description

id 续订设备注册。

auth 续订许可证权利。

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) 添加此命令是为了提供 ASA virtual 支持。

9.8(2) 添加了对 Firepower 2100 系列的支持。

使用指南

默认情况下，ID 证书每 6 个月自动更新，许可证授权每 30 天更新。如果您访问互联网的时间有限，或者例如在智能软件管理器中进行了任何许可更改，则可能需要为其中任一项手动续约注册。

CR_Examples

以下示例更新注册和许可证授权：

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。

命令	说明
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart reservation

要启用永久许可证预留，请在全局配置模式下使用 **licensesmartreservation** 命令。要禁用永久许可证预留，请使用此命令的 **no** 形式。

license smart reservation
no license smart reservation



注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会禁用此功能。

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	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

对于无法访问互联网的 ASA，您可以从智能软件管理器 (<https://software.cisco.com/#SmartLicensing-Inventory>) 申请永久许可证。永久许可证可启用所有功能的最大级别。

对于 ASA virtual，当您输入 **licensesmartreservation** 命令时，将删除以下命令：

```
license smart
feature tier standard
throughput level {100M | 1G | 2G}
```

要使用常规智能许可，请使用此命令的 **no** 形式，然后重新输入上述命令。其他 Smart Call Home 配置保持不变，但未使用，因此您不需要重新输入这些命令。

对于机箱，您必须为任何非默认许可证输入 **licensesmart/feature** 命令；例如，对于情景许可证。需要使用这些命令，以便 ASA 知道 允许配置该功能。



注释 对于永久许可证预留，您必须在停用 ASA 之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新的 ASA。查看 **licensesmartreservationreturn** 命令。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQ12vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

license smart reservation cancel

如果尚未在智能软件管理器中输入代码，则要取消永久许可证预留请求，请在特权 EXEC 模式下使用 **licensesmartreservationcancel** 命令。

license smart reservation cancel



注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为或值。

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
	9.5(2.200)	引入此命令是为了支持 ASA virtual 。
	9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南 如果您使用 **licensesmartreservationrequestuniversal** 命令请求了要在智能软件管理器中输入的许可证代码，并且尚未将此代码输入到智能软件管理器中，则您可以使用 **licensesmartreservationcancel** 命令取消请求。

如果禁用永久许可证预留（**nolicensesmartreservation**），则所有待处理的请求都将被取消。

如果您已经将代码输入智能软件管理器，那么您必须完成将许可证应用到 ASA，然后才能使用命令返回许可 **licensesmartreservationreturn** 证。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入要输入的许可证代码，然后取消请求：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E  
ciscoasa(config)# license smart reservation cancel
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

license smart reservation install

要输入从智能软件管理器收到的永久许可证预留授权码，请在特权 EXEC 模式下使用 **licensesmartreservationinstall** 命令。

license smart reservation install*code*



注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description

code 从智能软件管理器接收的永久许可证预留授权码。

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
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

对于无法访问互联网的 ASA，您可以从智能软件管理器 (<https://software.cisco.com/#SmartLicensing-Inventory>) 申请永久许可证。请求使用命令进入智能软件管理器的 **licensesmartreservationrequestuniversal** 代码。在将代码输入智能软件管理器时，请复制生成的授权代码，并使用 **licensesmartreservationinstall** 命令将其输入到 ASA 中。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQ12vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

许可证智能预订通用

要请求许可证代码以在智能软件管理器中输入，请在特权 EXEC 模式下使用 **licensesmartreservationuniversal** 命令。

license smart reservation universal



注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为行为或值。

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
	9.5(2.200)	引入此命令是为了支持 ASA virtual 。
	9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南 对于无法访问互联网 ASA，您可以向智能软件管理器请求永久许可证。请求使用命令进入智能软件管理器的 **licensesmartreservationrequestuniversal** 代码。

ASA virtual 部署确定请求的许可证 (ASAv5/ASAv10/ASAv30)。

如果重新输入此命令，则会显示同一代码，即使在重新加载后也是如此。如果您尚未将此代码输入智能软件管理器并想要取消请求，请输入该 **licensesmartreservationcancel** 命令。

如果禁用永久许可证预留，则所有待处理请求也会被取消。如果您已将该代码输入智能软件管理器，则必须完成此程序才能将该许可证应用于 ASA，然后可以根据需要退回该许可证。查看 **licensesmartreservationreturn** 命令。

要请求授权代码，请转到智能软件管理器库存屏幕 (<https://software.cisco.com/#SmartLicensing-Inventory>)，然后点击 **Licenses** 选项卡。**Licenses** 选项卡显示与您的账户相关的所有现有许可证（普通类型和永久类型）。单击 **LicenseReservation**，然后在框中输入 ASA 代码。Click **ReserveLicense**。智能软件

管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您没有看到该按 **LicenseReservation** 钮，则表示您的帐户无权进行永久许可证保留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

使用 **licensesmartreservationinstall** 命令在 ASA 上输入授权码。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQL2vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

许可证智能预留返还

要生成用于将许可证退回智能软件管理器的退回代码，请在特权 EXEC 模式下使用 **licensesmartreservationreturn** 命令。

license smart reservation return



注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

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
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History	版本	修改
	9.5(2.200)	引入此命令是为了支持 ASA virtual 。
	9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

对于无法访问互联网 ASA，您可以向智能软件管理器请求永久许可证。如果您不再需要永久许可证（例如，您正在淘汰 ASA 或更改 ASA virtual 模型级别，因此需要新的许可证），则必须正式将许可证退还给智能软件管理器。如果您不归还许可证，则许可证将处于已使用状态，并且不能轻易释放以供其他地方使用。

输入该 **licensesmartreservationreturn** 命令后，ASA 立即变为未许可状态并进入评估状态。如果您需要再次查看此代码，请重新输入此命令。请注意，如果您申请新的永久许可证

（**licensesmartreservationrequestuniversal**）或更改模 ASA virtual 型级别（通过关闭电源并更改 vCPU/RAM），则无法重新显示此代码。确保捕获该代码以完成返还。

在智能软件管理器中输入代码之前，请使用命令查看 ASA 通用设备标识符 (UDI)，以便您可以在 **showlicenseudi** 智能软件管理器中找到此 ASA 实例。转至“智能软件管理器库存”屏幕 (<https://software.cisco.com/#SmartLicensing-Inventory>)，然后单击 **ProductInstances** 选项卡。该 **ProductInstances** 选项卡显示所有经 UDI 许可的产品。找到 ASA virtual 您想要取消许可的，选择

Actions>Remove，然后在框中输入 ASA 返回代码。点击 **RemoveProductInstance** 永久许可证被返还到可用池。

CR_Examples

以下示例在 ASA virtual上生成返回代码，并查看 ASA virtual UDI:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au343lrGRS00Ig5HQL2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

lifetime (ca server mode)

如要指定本地证书颁发机构 (CA) 证书、每个颁发的用户证书或证书撤销列表 (CRL) 的有效时间长度，请在 **ca** 服务器配置模式下使用 **lifetime** 命令。要将生存期重置为默认设置，请使用此命令的 **no** 形式。

lifetime { **ca-certificate** | **certificate** | **crl** } *time*

lifetime { **ca-certificate** | **certificate** | **crl** }

Syntax Description

ca-certificate 指定本地 CA 服务器证书的有效期。

certificate 指定 CA 服务器颁发的所有用户证书的有效期。

crl 指定 CRL 的有效期。

time 对于 CA 证书和所有已颁发的证书，*time* 指定证书有效的天数。有效期为 5 至 30 年。默认生命周期值为 15 年。

对于所有已颁发的用户证书，有效范围是一天到 4 年。默认生命周期值为 2 年。

对于 CRL，*time* 指定 CRL 有效的小时数。CRL 的有效范围为 1 至 720 小时。

Command Default

默认生命周期为：

- CA 证书 - 15 年
- 颁发证书——两年
- CRL - 六个小时

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。

9.12(1) **ca-certificate** 的允许值更改为 5 至 30 年，默认为 15 年。

证书的允许值更改为 1 天/ 4 年，默认值为 2 年。

使用指南

通过指定证书或 CRL 有效的天数或小时数，此命令可以确定证书或 CRL 中包含的到期日期。

该命令在 **lifetimeca-certificate**本地CA服务器证书首次生成时（即首次配置本地CA服务器并发出该 **noshutdown**命令时）生效。当 CA 证书到期时，配置的有效期值用于生成新的 CA 证书。您不能更改现有 CA 证书的有效期值，

CR_Examples

以下示例将 CA 配置为颁发有效期为三个月的证书：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime certificate 90
ciscoasa
(config-ca-server)
)#
```

以下示例将 CA 配置为颁发有效期为两天的 CRL：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime crl 48
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cdp-url	指定要包括在 CA 颁发的证书中的证书撤销列表分发点 (CDP)。
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。
cryptocaservercrlissue	强制颁发 CRL。
showcryptocaserver	以 ASCII 文本显示本地 CA 配置详细信息。
showcryptocaservercert-db	显示本地 CA 服务器证书。
showcryptocaservercrl	显示本地 CA 的当前 CRL。

lifetime (ikev2 policy mode)

要在 IKEv2 安全关联 (SA) 中为 AnyConnect IPsec 连接指定加密算法，请在 IKEv2 策略配置模式下使用 **encryption** 命令。要删除该命令并使用默认设置，请使用以下命令的 **no** 形式：

```
lifetime { {secondsseconds} | none }
```

Syntax Description

seconds 生命周期（以秒为单位），从 120 到 2,147,483,647 秒。默认值为 86,400 秒（24 小时）。

Command Default

默认值为 86,400 秒（24 小时）。

使用指南

IKEv2 SA 是在第 1 阶段使用的密钥，用于使 IKEv2 对等体能够在第 2 阶段安全通信。输入 **crypto ikev2 policy** 命令后，使用 **lifetime** 命令设置 SA 生命周期。

生命周期设置 IKEv2 SA 重新生成密钥的间隔。使用 **none** 关键字会禁用为 SA 重新生成密钥。但是，Secure Client 仍可以重新生成 SA 密钥。

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

8.4(1) 添加了此命令。

CR_Examples

以下示例进入 IKEv2 策略配置模式并将生命周期设置为 43,200 秒（12 小时）：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

Related Commands

命令	说明
encryption	为 AnyConnect IPsec 连接指定 IKEv2 SA 中的加密算法。
group	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 群。
integrity	为 AnyConnect IPsec 连接指定 IKEv2 SA 的 ESP 完整性算法。

命令	说明
prf	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定伪随机函数。

limit-resource

要在多情景模式下为类指定资源限制，请在类配置模式下使用**limit-resource** 命令。要将限制恢复为默认值，请使用此命令的形式。ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。

```
limit-resource [rate] {all | resource_name} number [%] }  
no limit-resource [rate] {all | resource_name }
```

Syntax Description

all	设置所有资源的限制。
number [%]	将资源限制指定为一个大于或等于 1 的固定数值，或指定为介于 1 和 100 之间的系统限制的百分比（与百分号 (%) 一起使用时）。将限制设置为 0 以指示不受限制的資源，或对于 VPN 资源类型，将限制设置为无。对于没有系统限制的資源，不能设置百分比 (%)；只能设置绝对值。
rate	指定要设置资源的每秒速率。有关可为其设置每秒速率的资源，请参阅 表 7-1 。
resource_name	指定要为其设置限制的資源名称。此限制会覆盖为 all 设置的限制。

Command Default

所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。

对于大多数资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

- Telnet 会话 - 5 个会话。（每个情景的最大值。）
- SSH 会话 - 5 个会话。（每个情景的最大值。）
- ASDM 会话 - 5 个会话。（每个情景的最大值。）
- IPsec 会话 - 5 个会话（每个情景的最大值。）
- MAC 地址 - （因型号而异）。（每个情景的最大值。）
- AnyConnect 对等体 - 0 个会话。（您必须将该类手动配置为允许任何 AnyConnect 对等体。）
- VPN 站点间隧道 - 0 个会话。（您必须将该类手动配置为允许任何 VPN 会话。）



注释

如果您还在 **quotamanagement-session** 上下文中设置命令来设置最大管理会话（SSH 等），则将使用较低的值。

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
类配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.2(1)	添加了此命令。
9.0(1)	创建了一种新的资源类型 routes ，用于设置每个上下文中路由表条目的最大数量。 创建了新的资源类型 vpnother 和 vpnburstother ，以设置每个环境中站点到站点 VPN 隧道的最大数量。
9.5(2)	创建了新的资源类型 vpnanyconnect 和 vpnburstanyconnect ，以设置每个环境中 AnyConnect VPN 对等体的最大数量。
9.6(2)	已创建新的资源类型 storage ，用于设置最大存储。

使用指南

默认情况下，除非为每个情景强制设置了最大限制，否则所有安全情景对 ASA 资源的访问都是不受限制的；但 VPN 资源是唯一一种例外情况，这些资源默认是禁用的。例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

表 7-1 列出了资源类型和限制。另请参阅 **showresourcetypes** 命令。

表 3: 资源名称和限制

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制 ¹	说明
asdm	并发	1（最小值） 5（最大值）	200	ASDM 管理会话。 注释 ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，200 个 ASDM 会话的系统限制代表 400 个 HTTPS 会话的限制。
conns	并发或速率	不适用	并发连接：有关平台的连接限制，请参阅 CLI 配置指南。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制 ¹	说明
hosts	并发	不适用	不适用	可以通过 ASA 连接的主机数。
inspects	Rate	不适用	不适用	应用检查。
mac-addresses	并发	不适用	(因型号而异)	对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
routes	并发	不适用	不适用	动态路由数。
ssh	并发	1 (最小值) 5 (最大值)	100	SSH 会话数。
storage	MB	最大值取决于您指定的闪存驱动器	最大值取决于您指定的闪存驱动器	情景目录的存储限制 (MB)。使用命令指定驱动 storage-url 器。
syslogs	Rate	不适用	不适用	系统日志消息。
telnet	并发	1 (最小值) 5 (最大值)	100	Telnet 会话数。
vpnburstanyconnect	并发	不适用	您型号的 AnyConnect 高级对等体数减去为 vpnanyconnect 向所有情景分配的会话总和。	允许的 AnyConnect 会话数超出了分配给上下文的数量。 vpnanyconnect 例如，如果您的模型支持 5000 个对等体，并且您在所有上下文中分配了 4000 个对等体 vpnanyconnect ，那么剩余的 1000 个会话可用于。 vpnburstanyconnect 与 vpnanyconnect 保证上下文会话的不同， vpnburstanyconnect 可以超额认购；突发池按照先到先得的原则提供给所有上下文。
vpnanyconnect	并发	不适用	请参阅 CLI 配置指南中的“每个型号支持的功能许可证”部分，了解适用于您的型号的 AnyConnect VPN 对等体。	AnyConnect 对等体。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的对等体数保证可供相应情景使用。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制 ¹	说明
vpnburstother	并发	不适用	您的模型的其他 VPN 会话数量减去分配给所有上下文的会话总和。 vpnother	允许的站点到站点 VPN 会话数超出了分配给上下文的数量。 vpnother 例如，如果您的模型支持 5000 个会话，并且您在所有上下文中分配了 4000 个会话 vpnother ，则剩余的 1000 个会话可用于。 vpnburstother 与 vpnother 保证上下文会话的不同， vpnburstother 可以超额认购；突发池按照先到先得的原则提供给所有上下文。
vpnother	并发	不适用	有关适用于您的型号的其他 VPN 会话的 CLI 配置指南，请参阅“每个型号支持的功能许可证”部分。	站点间 VPN 会话数。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的会话数保证可供相应情景使用。
xlates	并发	不适用	不适用	地址转换。

¹ 如果此列值为 N/A，则您无法设置资源的百分比，因为该资源没有硬系统限制。

CR_Examples

以下示例将 **conn** 的默认类限制设置为 10% 而不是不受限制：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

所有其他资源保持不受限制。

要添加名为 **gold** 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
```

Related Commands

命令	说明
class	创建资源类。
context	配置安全上下文。
member	将上下文分配给资源类。

命令	说明
显示资源分配	显示如何跨类分配资源。
show resource types	显示您可以设置限制的資源类型。

lmfactor

要设置重新验证策略以缓存仅具有上次修改时间戳的对象，而没有其他服务器设置过期值，请在缓存配置模式下使用 **lmfactor** 命令。要设置用于重新验证此类对象的新策略，请再次使用 命令。要将属性重置为默认值 20，请输入此命令的 **no** 版本。

lmfactor 值
no lmfactor

Syntax Description *value* 0 到 100 范围内的整数。

Command Default 默认值为 20。

Command Modes 下表显示了输入命令的模式：

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
缓存配置	• 是	—	• 是	—	—

Command History 版本 修改

7.1(1) 添加了此命令。

使用指南 ASA 使用 流率系数 的值来估计它认为缓存对象未更改的时间长度。这段时间称为到期时间。ASA 通过自上次修改以来经过的时间乘以 **lmfactor** 来估算到期时间。

将 **lmfactor** 设置为零相当于强制立即重新验证，而将其设置为 100 则会导致重新验证所需的最长允许时间。

CR_Examples 以下示例显示如何将 流明系数 设置为 30：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(config-webvpn-cache)#
```

Related Commands

命令	说明
cache	进入 WebVPN 缓存模式。
cache-compressed	配置 WebVPN 缓存压缩。
disable	禁用缓存。
expiry-time	配置缓存对象的到期时间而不重新验证它们。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义要缓存的最小对象大小。

load-monitor

要配置集群流量负载监控，请在集群配置模式下使用 **load-monitor**命令。要禁用此功能，请使用此 **no**命令的形式。

load-monitor [**frequency**秒] [**intervals**间隔]
no load-monitor [**frequency**秒] [**intervals**间隔]

Syntax Description

frequency秒 可选）设置监控消息之间的时间（以秒为单位），介于 10 到 360 秒之间。默认值为 20 秒。

intervals间 （可选）设置 ASA 维护数据的间隔数，介于 1 到 60 之间。默认值为 30。
隔

Command Default

默认情况下会启用此命令。默认频率为 20 秒。默认间隔为 30。

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
集群配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.13(1)	命令已添加。

使用指南

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的设备可以处理负载，您可以选择在设备上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。例如，对于每个机箱中具有 3 个安全模块的 Firepower 9300 上的机箱间集群，如果机箱中的 2 个安全模块离开集群，则与该机箱的相同数量的流量将被发送到剩余的模块，并可能压垮它。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用设备上的集群。

使 **showclusterinfo****load-monitor**用命令查看流量负载。

CR_Examples

以下示例将频率设置为 50 秒，将间隔设置为 25：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```


Related Commands

命令	说明
cluster	进入集群配置模式

local-base-url

（可选）配置用于 VPN 身份验证的 SAML 服务提供商的本地基本 URL。在 DNS 负载均衡集群中，当您在 ASA 上配置 SAML 身份验证时，您可以指定此 URL 来唯一解析应用该配置的设备。

要禁用此功能，请使用此命 **no** 令的形式

```
local base-url { url }
no local base-url
```

Syntax Description *url* 用于 VPN 身份验证的 SAML 服务提供商的本地基本 URL。

Command Default 无。

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	—

版本	修改
9.18(3)	添加了此命令。
9.19(1)S	添加了此命令。

使用指南 您必须将此命令与 **base-url** 命令结合使用。

CR_Examples 以下示例设置了本地 base-url:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp https://idp.com/<app-specific>
ciscoasa(config-webvpn-saml-idp)# base url https://asa-dns-group.vpn.customer.com
ciscoasa(config-webvpn-saml-idp)# local-base-url https://this-asa.vpn.customer.com
```

命令	说明
signature	在 SAML 请求中启用或禁用签名。默认情况下，签名是禁用的。

命令	说明
timeout	配置 SAML IdP 超时。
trustpoint	在 saml-idp 子模式下配置信任点。
url	配置 SAML IdP URL。
base-url	为 VPN 身份验证配置 SAML 服务提供商的基本 URL。

local-domain-bypass

要配置 DNS 请求绕过思科 Umbrella 的本地域，请在 Umbrella 配置模式下使用 **local-domain-bypass** 命令。使用此命令的形式可以恢复默认设置。

```
local-domain-bypass { regular_expression | regex classregex_classmap }
no local-domain-bypass { regular_expression | regex classregex_classmap }
```

Syntax Description	regular_expression	标识要绕过的本地域的正则表达式。它可以像本地域一样简单，例如 example.com。表达式最多可包含 100 个字符。 如果使用此选项，则可输入 local-domain-bypass 命令多次以定义多个本地域。
	regexclassregex_classmap	定义要绕过的本地域名的正则表达式类的名称。对与该类中的正则表达式相匹配的完全限定域名的任何 DNS 请求都会直接发送到已配置的 DNS 服务器，而不是发送到 Umbrella 服务器。

Command Default 默认情况下，所有域的 DNS 请求都会发送到 Cisco Umbrella。

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 以下是使用此命令的准则：

- 您可以输入此命令多次，以直接定义域名的正则表达式。
- 使用正则表达式类时，只能输入此命令一次。但是，您可以将命令的单个正则表达式类版本与直接使用正则表达式的多个实例结合使用。

CR_Examples 以下示例将 example.com 定义为要绕过的本地域。

```
ciscoasa(config)# umbrella-global
```

```
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

以下示例创建一个正则表达式来匹配 example.com，从而匹配 *example.com 上的任何完全限定域名。然后，该示例创建所需的正则表达式类映射，并将其用作 Umbrella 的本地域绕行。

```
ciscoasa(config)# regex example-com example.com
```

```
ciscoasa(config)# class-map type regex match-any umbrella-bypass
```

```
ciscoasa(config-cmap)# match regex example-com
```

```
ciscoasa(config)# umbrella-global
```

```
ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

Related Commands

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

local-unit

要为此集群成员提供名称，请在 **local-unit** 集群组配置模式下使用该命令。要删除名称，请使用**no**此命令的形式。

local-unit*unit_name*
no local-unit [*unit_name*]

Syntax Description *unit_name* 使用 1 至 38 个字符的唯一 ASCII 字符串命名该集群成员。

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
集群组配置	• 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 每台设备必须拥有唯一的名称。集群中不允许存在名称重复的设备。

CR_Examples 以下示例将此设备命名为 **unit1**：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

命令	说明
clacpsystem-mac	使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。
cluster group	命名集群并进入集群配置模式。
cluster-interface	指定集群控制链路接口。
clusterinterface-mode	设置集群接口模式。
conn-rebalance	启用连接再均衡。

命令	说明
console-replicate	启用从从属设备到主设备的控制台复制。
enable(clustergroup)	启用集群。
health-check	启用集群健康检查功能，包括单元健康监控和接口健康监控。
key	为集群控制链路上的控制流量设置身份验证密钥。
local-unit	为集群成员命名。
mtucluster-interface	指定集群控制链路接口的最大传输单元。
priority(clustergroup)	设置此单元在主单元选举中的优先级。

location-logging

要让 GTP 检测记录移动站的位置和位置更改，请在 GTP 检测策略映射参数配置模式下使用 **location-logging** 命令。使用此命令的 **no**形式可以禁用位置日志记录。

location-logging [**cell-id**]
no location-logging [**cell-id**]

Syntax Description **cell-id** 是否包括用户当前注册的单元 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。

Command Default 默认情况下，位置日志记录是禁用的。

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
参数配置模式	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.13(1)	引入了此命令。

使用指南 可以使用 GTP 检测跟踪移动站位置更改。跟踪位置更改可能会帮助您识别欺诈漫游费用，例如，如果您看到移动站在不太可能的时间断内从一个位置移至另一个位置，例如在 30 分钟内从美国的一个小区移至欧洲的一个小区。

启用位置日志记录后，系统会针对每个国际移动用户识别码 (IMSI) 的新位置或更改位置生成系统日志消息：

- 324010 表示创建新的 PDP 上下文，包括移动国家代码 (MCC)、移动网络代码 (MNC)、信息元素，以及可选的用户当前注册的小区 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。
- 324011 指示 IMSI 已从 PDP 情景创建过程中存储的位置移开。该消息显示先前和当前的 MCC/MNC 以及可选的小区 ID。

默认情况下，系统日志消息不包含时间戳信息。如果您计划分析这些消息来识别不太可能漫游时，还必须启用时间戳。时间戳日志记录不作为 GTP 检测映射的一部分。使用 **loggingtimestamp** 命令。

CR_Examples

以下示例将时间戳添加到系统日志消息，然后启用具有单元 ID 的位置日志记录。

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# location-logging cell-id
```

Related Commands

命令	说明
inspectgtp	启用 GTP 应用检查。
policy-maptypeinspectgtp	创建或编辑 GTP 检查策略图。
showservice-policyinspectgtp	显示 GTP 配置和统计信息。



log – lz

- [log](#) , 第 497 页
- [log-adjacency-changes](#) , 第 499 页
- [log-adj-changes](#) , 第 503 页
- [log-adjacency-changes](#) , 第 504 页
- [logging asdm](#) , 第 505 页
- [logging asdm-buffer-size](#) , 第 507 页
- [logging buffered](#) , 第 509 页
- [logging buffer-size](#) , 第 511 页
- [logging class](#) , 第 513 页
- [logging console](#) , 第 517 页
- [logging debug-trace](#) , 第 519 页
- [logging debug-trace persistent](#) , 第 521 页
- [logging device-id](#) , 第 523 页
- [logging emblem](#) , 第 525 页
- [logging enable](#) , 第 527 页
- [logging facility](#) , 第 529 页
- [logging flash-bufferwrap](#) , 第 531 页
- [logging flash-maximum-allocation](#) , 第 533 页
- [logging flash-minimum-free](#) , 第 535 页
- [logging flow-export-syslogs](#) , 第 537 页
- [logging from-address](#) , 第 539 页
- [logging ftp-bufferwrap](#) , 第 541 页
- [logging ftp-server](#) , 第 543 页
- [logging hide username](#) , 第 545 页
- [logging history](#) , 第 547 页
- [logging host](#) , 第 549 页
- [logging list](#) , 第 552 页
- [logging mail](#) , 第 556 页
- [logging message](#) , 第 558 页

- logging message standby, 第 560 页
- logging monitor, 第 561 页
- logging permit-hostdown, 第 563 页
- logging queue, 第 565 页
- logging rate-limit, 第 567 页
- logging recipient-address, 第 570 页
- logging savelog, 第 573 页
- logging standby, 第 575 页
- logging timestamp, 第 577 页
- logging trap, 第 579 页
- login, 第 581 页
- login-button, 第 583 页
- login-message, 第 585 页
- login-title, 第 587 页
- 徽标, 第 589 页
- logout, 第 591 页
- logout-message, 第 592 页
- lsp-full suppress, 第 594 页
- lsp-gen-interval, 第 598 页
- lsp-refresh-interval, 第 602 页

log

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，记录与 **log** 命令或类映射匹配的数据包。此日志操作在检测策略映射（**policy-map type inspect** 命令）中可用于应用流量。要禁用此操作，请使用此命令的 **no** 形式。

log
nolog

Syntax Description

此命令没有任何参数或关键字。

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。输入 **match** 或 **class** 命令标识应用流量（**class** 命令是指现有的 **class-map type inspect** 命令，后者包含 **match** 命令）后，可以输入 **log** 命令记录与 **match** 命令或 **class** 命令。

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 **inspect http http_policy_map** 命令，其中 **http_policy_map** 是检测策略映射的名称。

CR Examples

以下示例在数据包与 **http-traffic** 类映射匹配时发送日志。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	定义特殊的应用检查操作。
show running-config policy-map	显示所有当前的策略映射配置。

log-adjacency-changes

要使 IS-IS 在 NLSP IS-IS 邻接关系更改状态（打开或关闭）时发送系统日志消息，请在路由器 isis 配置模式下使用 **log-adjacency-changes** 命令。要关闭此功能，请使用此 **no** 命令的形式。

log-adjacency-changes [all]
no log-adjacency-changes [all]

Syntax Description

a （可选）包括非 IIIH 事件生成的更改。

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
IPv6 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

此命令允许监控 IS-IS 邻接状态更改。这在监控大型网络时可能非常有用。使用系统错误消息工具记录消息。消息的形式如下：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

CR_Examples

以下示例指示路由器记录邻接更改：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。

命令	说明
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。

命令	说明
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

log-adj-changes

要配置路由器在 OSPF 邻居启动或关闭时发送系统日志消息，请在 **log-adj-changes** 路由器配置模式下使用该命令。要关闭此功能，请使用此 **no** 命令的形式。

log-adj-changes [detail]
no log-adj-changes [detail]

Syntax Description

detail （可选）每次状态改变时都发送系统日志消息，而不仅仅是在邻居启动或关闭时发送。

Command Default

默认情况下会启用此命令。

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

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

默认情况下，将启用 **log-adj-changes** 命令；默认情况下，默认值为“禁用”。在这种情况下，除非使用 **no** 形式将其删除，否则它将显示在运行配置中。

CR_Examples

以下示例在 OSPF 邻居启动或关闭时禁用系统日志消息的发送：

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

Related Commands

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

log-adjacency-changes

要配置路由器在 OSPFv3 邻居启动或关闭时发送系统日志消息，请在 **log-adjacency-changes**IPv6 路由器配置模式下使用该命令。要关闭此功能，请使用此**no**命令的形式。

log-adjacency-changes [detail]
no log-adjacency-changes [detail]

Syntax Description **detail** （可选）每次状态改变时都发送系统日志消息，而不仅仅是在邻居启动或关闭时发送。

Command Default 默认情况下会启用此命令。

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
9.0(1)	添加了此命令。

使用指南 默认情况下，将启用**log-adjacency-changes**命令；默认情况下，默认值为“禁用”。在这种情况下，除非使用 **no** 形式将其删除，否则它将显示在运行配置中。

CR_Examples

以下示例在 OSPFv3 邻居启动或关闭时禁用发送系统日志消息：

```
ciscoasa(config)# ipv6router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

命令	说明
ipv6routerospf	进入路由器配置模式。
showipv6ospf	显示关于 OSPFv3 路由过程的一般信息。

logging asdm

要将系统日志消息发送到 ASDM 日志缓冲区，请在 **loggingasdm** 全局配置模式下使用该命令。要禁用记录到 ASDM 日志缓冲区的 **no** 功能，请使用此命令的形式。

loggingasdm [*logging_list* | *level*]
no loggingasdm [*logging_list* | *level*]

Syntax Description

水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或 **0emergencies**——系统不可用。
- 或 **1alerts**——需要立即采取行动。
- 或 **2critical**——危急情况。
- 或 **3errors**——错误情况。
- 或 **4warnings**——警告情况。
- 或 **5notifications**——正常但重要的情况。
- **6**或 **informational**——信息性消息。
- 或 **7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list 指定标识要发送到 ASDM 日志缓冲区的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，ASDM 日志记录处于禁用状态。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

在将任何消息发送到 ASDM 日志缓冲区之前，您必须使用 **loggingenable** 命令启用日志记录。

当 ASDM 日志缓冲区已满时，ASA 会删除最旧的消息，以便在缓冲区中为新消息腾出空间。要控制 ASDM 日志缓冲区中保留的系统日志消息数量，请使用该 **loggingasdm-buffer-size** 命令。

ASDM 日志缓冲区与该命令启用的日志缓冲区不 **loggingbuffered** 同。

CR_Examples

以下示例显示如何启用日志记录，将严重性级别为 0、1 和 2 的日志缓冲区消息发送到 ASDM，以及如何将 ASDM 日志缓冲区大小设置为 200 消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: disabled
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging: level critical, 48 messages logged
```

Related Commands

命令	说明
clearloggingasdm	清除 ASDM 日志缓冲区中包含的所有消息。
loggingasdm-buffer-size	指定 ASDM 日志缓冲区中保留的 ASDM 消息数
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示日志记录配置。

logging asdm-buffer-size

要指定 ASDM 日志缓冲区中保留的系统日志消息数，请在全局配置模式下使用 **loggingasdm-buffer-size** 命令。要将 ASDM 日志缓冲区大小重置为默认的 100 条消息，请使用此命令的 **no** 形式。

loggingasdm-buffer-sizenum_of_msgs
no loggingasdm-buffer-sizenum_of_msgs

Syntax Description

num_of_msgs 指定 ASA 在 ASDM 日志缓冲区中保留的系统日志消息数。

Command Default

默认 ASDM 系统日志缓冲区大小为 100 条消息。

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。

使用指南

当 ASDM 日志缓冲区已满时，ASA 会删除最旧的消息，以便在缓冲区中为新消息腾出空间。要控制是否启用记录到 ASDM 日志缓冲区的日志记录或控制保留在 ASDM 日志缓冲区中的系统日志消息的类型，请使用 **loggingasdm** 命令。

ASDM 日志缓冲区与该命令启用的日志缓冲区不 **loggingbuffered** 同。

CR_Examples

以下示例显示如何启用日志记录，将严重性级别为 0、1 和 2 的消息发送到 ASDM 日志缓冲区，以及如何将 ASDM 日志缓冲区大小设置为 200 条消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

命令	说明
clearloggingasdm	清除 ASDM 日志缓冲区中包含的所有消息。
loggingasdm	启用到 ASDM 日志缓冲区的日志记录。
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示当前正在运行的日志配置。

logging buffered

要使 ASA 能够将系统日志消息发送到日志缓冲区，请在 **loggingbuffered** 全局配置模式下使用该命令。要禁用将日志记录到日志缓冲区，请使用此命令的 **no** 形式。

loggingbuffered [*logging_list* | *level*]
no loggingbuffered [*logging_list* | *level*]

Syntax Description

水平

设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或 **0emergencies**——系统不可用。
- 或 **1alerts**——需要立即采取行动。
- 或 **2critical**——危急情况。
- 或 **3errors**——错误情况。
- 或 **4warnings**——警告情况。
- 或 **5notifications**——正常但重要的情况。
- **6**或 **informational**——信息性消息。
- 或 **7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

日志记录列表 指定标识要发送到日志缓冲区的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 缓冲区大小为 4 KB。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

在任何消息发送到日志缓冲区之前，必须使用 **loggingenable** 命令启用日志记录。

新消息将附加到缓冲区的末端。当缓冲区填满时，ASA 会清除缓冲区并继续向其中添加消息。当日志缓冲区已满时，ASA 会删除最旧的消息，以便在缓冲区中为新消息腾出空间。您可以在缓冲区的内容每次“包装”时自动保存缓冲区内容，这意味着自上次保存以来的所有邮件都已替换为新邮件。有关详细信息，请参阅 **loggingflash-bufferwrap**和 **loggingftp-bufferwrap**命令。

您可以随时将缓冲区的内容保存到闪存。有关详细信息，请参阅 **loggingsavelog**命令。

您可以使用 **showlogging** 命令查看已发送到缓冲区的系统日志消息。

CR_Examples

以下示例为严重性级别为 0 且事件为 1 的缓冲区配置日志记录：

```
ciscoasa(config)# logging buffered alerts
ciscoasa(config)#
```

以下示例创建一个名为“notif-list”的列表，最大严重性级别为 7，并为将日志记录配置到缓冲区，以便为“notif-list”列表标识的系统日志消息配置日志记录：

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
loggingsavelog	将日志缓冲区的内容保存到闪存。

logging buffer-size

要指定日志缓冲区的大小，请在全局配置模式下使用命令 **loggingbuffer-size**。要将日志缓冲区重置为其默认大小 4 KB 内存，请使用此命令的 **no** 形式。

loggingbuffer-sizebytes
no loggingbuffer-sizebytes

Syntax Description

bytes 设置用于日志缓冲区的内存量（以字节为单位）。例如，如果指定 8192，则 ASA 将 8 KB 的内存用于日志缓冲区。

Command Default

默认日志缓冲区大小为 4 KB 内存。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

要查看 ASA 是否使用的日志缓冲区大小不是默认缓冲区大小，请使用 **showrunning-configlogging** 命令。如果未显示 **loggingbuffer-size** 命令，则 ASA 使用 4 KB 的日志缓冲区。

有关 ASA 如何使用缓冲区的详细信息，请参阅 **loggingbuffered** 命令。

CR_Examples

以下示例启用日志记录缓冲区，并指定 ASA 将 16 KB 的内存用于日志缓冲区：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。

命令	说明
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingsavelog	将日志缓冲区的内容保存到闪存。

logging class

要为消息类配置每个日志记录目标的最大严重性级别，请在全局配置模式下使用 **loggingclass** 命令。要删除消息类别严重性级别配置，请使用此命令的 **no** 形式。

logging class类目标级别 [目标级别...]
no logging class class

Syntax Description	class 指定最大严重性级别按目标配置的消息类。有关 类 的有效值，请参阅“使用指南”部分。 destination 为 类指定日志记录目标。对于目标， 级别 确定发送到 目标 的最大严重性级别。有关 destination 的有效值，请参阅下面的“使用指南”部分。 水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或0emergencies——系统不可用。 • 或1alerts——需要立即采取行动。 • 或2critical——危急情况。 • 或3errors——错误情况。 • 或4warnings——警告情况。 • 或5notifications——正常但重要的情况。 • 6或informational——信息性消息。 • 或7debugging——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请 仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。 <tr><td>Command Default</td><td>默认情况下，ASA 不会对日志记录目标和消息类应用严重性级别。相反，每个已启用的日志记录目标接收其严重性级别（由日志记录列表确定）或接收启用日志记录目标时指定的严重性级别的所有类的消息。</td></tr>	Command Default	默认情况下，ASA 不会对日志记录目标和消息类应用严重性级别。相反，每个已启用的日志记录目标接收其严重性级别（由日志记录列表确定）或接收启用日志记录目标时指定的严重性级别的所有类的消息。
Command Default	默认情况下，ASA 不会对日志记录目标和消息类应用严重性级别。相反，每个已启用的日志记录目标接收其严重性级别（由日志记录列表确定）或接收启用日志记录目标时指定的严重性级别的所有类的消息。		

Command Modes 下表显示了您可以输入命令的模式。

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	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(2)	eigrp 选项已添加到有效的类别值。
8.2(1)	dap 选项已添加到有效的类别值。
9.12(1)	已为有效类别值添加 bfd, bgp, idb, ipv6, multicast, routing, object-group-search, pbr, sla 选项

使用指南

- 类别的有效值包括以下内容：
- 用**auth**户身份验证。
 - 用**bfd** BFD 路由
 - 用**bgp** BGP 路由
 - 用**bridge** 透明防火墙。
 - 用**ca** PKI 证书颁发机构。
 - 用**config** 命令界面。
 - 动态访问**dap** 策略。
 - 用**eap** 可扩展身份验证协议 (EAP)。记录以下类型的事件以支持网络准入控制：EAP 会话状态更改、EAP 状态查询事件以及 EAP 报头和数据包内容的十六进制转储。
 - 用**eapoudp** UDP 上的可扩展身份验证协议 (EAP)。记录 EAPoUDP 事件以支持网络准入控制，并生成 EAPoUDP 报头和数据包内容的完整记录。
 - 用**eigrp** EIGRP 路由。
 - 用**email** 邮件代理。
 - 用**failover** 故障转移。
 - 用**idb** 界面
 - 用**ids** 入侵检测系统。
 - 用**ip** IP 堆栈。

- IP地址 **ipaa**—址分配
- **ipv6**-IPv6 堆栈
- **multicast**—多播路由
- **nac**—网络准入控制。记录以下类型的事件：初始化、例外列表匹配、ACS 事务、无客户端身份验证、默认 ACL 应用和重新验证。
- 一网 **np** 络处理器。
- 一 **object-group-search** 对象组搜索
- 一 **ospf** OSPF 路由。
- 一基于 **pbr** 策略的路由
- 一 **rip** RIP 路由。
- 一资 **rm** 源管理器。
- **routing**- 所有路由
- 一用 **session** 户会话。
- **sla**-SLA 对象跟踪
- 一 **snmp** SNMP。
- -系 **sys** 统。
- 一 **vpn** IKE 和 IPsec。
- 一 **vpnc** VPN 客户端。
- 一 **vpnfo** VPN 故障转移。
- 一 **vpnlb** VPN 负载均衡。

有效的日志记录目的地如下：

- **asdm**- 要了解此目标，请参阅 **loggingasdm** 命令。
- **buffered**- 要了解此目标，请参阅 **loggingbuffered** 命令。
- **console**- 要了解此目标，请参阅 **loggingconsole** 命令。
- **history**- 要了解此目标，请参阅 **logginghistory** 命令。
- **mail**- 要了解此目标，请参阅 **loggingmail** 命令。
- **monitor**- 要了解此目标，请参阅 **loggingmonitor** 命令。
- **trap**- 要了解此目标，请参阅 **loggingtrap** 命令。

CR_Examples

以下示例指定，对于故障转移相关消息，ASDM日志缓冲区的最大严重性级别为2，系统日志缓冲区的最大严重性级别为 7：

```
ciscoasa(config)# logging class ha asdm 2 buffered 7
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging console

要使 ASA 能够在控制台会话中显示系统日志消息，请在全局配置模式下使用 **loggingconsole**命令。要禁用控制台会话中系统日志消息的 **no**显示，请使用此命令的形式。

```
loggingconsole [logging_list | level]
nologgingconsole
```



注释 我们建议您不要使用此命令，因为它可能会导致许多系统日志消息因缓冲区溢出而被丢弃。有关更多信息，请参阅“使用指南”部分。

Syntax Description	水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别3、2、1和0的系统日志消息。您可以指定编号或名称，如下所示： • 或0emergencies——系统不可用。 • 或1alerts——需要立即采取行动。 • 或2critical——危急情况。 • 或3errors——错误情况。 • 或4warnings——警告情况。 • 或5notifications——正常但重要的情况。 • 6 或informational——信息性消息。 • 或7debugging——调试消息。 注释 由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与Cisco技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
	<i>logging_list</i> 指定标识要发送到控制台会话的消息的列表。有关创建列表的信息，请参阅 logginglist 命令。

Command Default 默认情况下，ASA 不在控制台会话中显示系统日志消息。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

在将任何消息发送到控制台之前，必须使用 **loggingenable** 命令启用日志记录。



注意 使用 **loggingconsole** 命令可能会显着降低系统性能。而是使用 **logging buffered** 命令启动日志记录，并使用 **show logging** 命令查看消息。要查看最新消息，请使用 **clear logging buffer** 命令清除缓冲区。

CR_Examples

以下示例显示如何使严重性级别为 0、1、2 和 3 的系统日志消息显示在控制台会话中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging debug-trace

要将调试消息作为在严重性级别 7 发出的系统日志消息 711001 重定向到日志，请在全局配置模式下使用 **loggingdebug-trace** 命令。要停止将调试消息发送到日志，请使用此命令的 **no** 形式。

loggingdebug-trace
nologgingdebug-trace

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，ASA 不在系统日志消息中包括调试输出。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

调试消息生成为严重性级别为 7 的消息。它们显示在系统日志消息编号为 711001 的日志中，但不会显示在任何监控会话中。

CR_Examples

以下示例显示如何启用日志记录、将日志消息发送到系统日志缓冲区、将调试输出重定向到日志，以及打开磁盘活动调试。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

以下是可能在日志中显示的调试消息的输出示例：

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

命令	说明
loggingenable	启用日志记录。

命令	说明
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging debug-trace persistent

要启用特定会话中的调试系统日志活动（即使在会话结束后），请在全局配置模式下使用 **loggingdebug-tracepersistent** 命令。要禁用特定持久调试配置，请使用此命令的 **no** 形式。这将从本地会话和持久调试中将其清除。

loggingdebug-tracepersistent
nologgingdebug-tracepersistent

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，当会话结束时，在该特定会话中启用的所有调试命令在配置中不再存在，因此不再登录到系统日志服务器。

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	• 支持

Command History

版本 修改

9.5(2) 添加了此命令。

使用指南

在启用 **logging debug-trace persistent** 命令时，从任何会话输入的调试命令将全局保存，并对所有会话均可见。此命令将保存到运行配置中，并在系统重新启动时保存。

CR_Examples

以下示例显示如何启用日志记录，将日志消息发送到系统日志缓冲区，将调试输出重定向到日志，以及打开磁盘活动的持久调试。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace persistent
ciscoasa(config)# debug disk filesystem
```

以下是可能在日志中显示的调试消息的输出示例：

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging device-id

要将 ASA 配置为在非 EMBLEM 格式的系统日志消息中包含设备 ID，请在 **loggingdevice-id** 全局配置模式下使用该命令。要禁用设备 ID，请使用此命令 **no** 的形式。

loggingdevice-id { **cluster-id** | **context-name** | **hostnameipaddressinterface_name** [**system**] | **stringtext** }
no logging device-id

Syntax Description	cluster-id	将集群中单个 ASA 单元的唯一名称指定为设备 ID。
	hostname	将 ASA 的主机名指定为设备 ID。
	ipaddressinterface_name	在 <i>interface_name</i> 中指定接口的设备 ID 或 IP 地址。如果使用 ipaddress 关键字，则发送到外部服务器的系统日志消息包括指定接口的 IP 地址，而不考虑 ASA 使用哪个接口将日志数据发送到外部服务器。
	string 文本、	指定作为设备 ID 的文本中包含的字符，长度最多可以为 16 个字符。不能使用空格字符或以下任何字符： • &—与号 • '—单引号 • "—双引号 • < - 小于号 • >—大于号 • ? - 问号
	system	（可选）在集群环境中，规定设备 ID 成为接口上的系统 IP 地址。

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	• 支持

Command History	版本 修改
	7.0(1) 添加了此命令。

版本 修改

9.0(1) 已添加 **cluster-id**和关 **system**键字。

使用指南

如果使用 **ipaddress** 关键字，则设备 ID 将成为指定的 ASA 接口 IP 地址，无论消息从哪个接口发送。此关键字为从设备发送的所有消息提供单一、一致的设备 ID。如果使用 **system** 关键字，则指定的 ASA 将使用系统 IP 地址而不是集群中设备的本地 IP 地址。**cluster-id** 和 **system** 关键字仅适用于 ASA 5580 和 5585-X。

CR_Examples

以下示例显示如何配置名为 “secappl-1” 的主机：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

主机名显示在系统日志消息的开头，如以下消息所示：

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

要删除设备 ID，请使用不带参数命令的 **no** 形式； **no** 形式不适用于参数。

```
ciscoasa(config)# show running-config logging
logging buffered informational
logging device-id hostname
firepower(config)# no logging device-id
ciscoasa(config)# show running-config logging
logging buffered informational
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging emblem

要对发送到系统日志服务器之外的目标的系统日志消息使用 EMBLEM 格式，请在全局配置模式下使用 **loggingemblem** 命令。要禁用 EMBLEM 格式，请使用此命令 **no** 的形式。

loggingemblem
nologgingemblem

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下，ASA 不对系统日志消息使用 EMBLEM 格式。

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	• 支持

Command History 版本 修改

7.0(1) 此命令已更改为独立于 **logginghost** 命令。

使用指南

通过 **logging** 徽章命令，您可以为系统日志服务器以外的所有日志记录目标启用 EMBLEM 格式日志记录。如果还启用了 **loggingtimestamp** 关键字，则会发送带有时间戳的消息。

要为系统日志服务器启用 EMBLEM 格式日志记录，请将 **formatemblem** 选项与 **logginghost** 命令配合使用。



注释 徽章格式的时间戳字符串不包括年份。要在事件系统日志中显示年份，可以根据 RFC 5424 使用 **logging timestamp rfc5424** 命令启用时间戳。以下是 RFC 5424 格式的输出示例：

```
<166>2018-06-27T12: 17: 46Z asa: □ASA-6-110002: 无法定位从源接口: 源IP /源端口到目标IP /目标端口的协议出口接口
```

或者，您可以使用该 **logging device-id** 命令。

CR_Examples

以下示例显示如何启用日志记录并使用 EMBLEM 格式以将日志记录发送到除系统日志服务器之外的所有日志记录目标：

```
ciscoasa(config)# logging enable
```

```
ciscoasa(config)# logging emblem
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging enable

要为所有已配置的输出位置启用日志记录，请在全局配置模式下使用 **loggingenable** 命令。要禁用日志记录，请使用此命令 **no** 的形式。

loggingenable
nologgingenable

Syntax Description

此命令没有任何参数或关键字。

Command Default

日志记录默认将禁用。

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	• 支持	• 支持	• 支持	• 支持

Command History

版本 修改

7.0(1) 此命令由该 **loggingon** 命令改变而来。

使用指南

loggingenable 命令允许您启用或禁用将系统日志消息发送到任何受支持的日志记录目标。您可以使用 **no logging enable** 命令停止所有日志记录。

您可以使用以下命令启用到各个日志记录目标的日志记录：

- **loggingasdm**
- **loggingbuffered**
- **loggingconsole**
- **logginghistory**
- **loggingmail**
- **loggingmonitor**
- **loggingtrap**

CR_Examples

以下示例显示如何启用日志记录。 **showlogging** 命令的输出说明了必须如何单独启用每个可能的日志记录目标：

logging enable

```
ciscoasa
(config)#
logging enable
ciscoasa
(config)#
show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: disabled
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging: disabled
```

Related Commands

命令	说明
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging facility

要指定将消息发送到系统日志服务器的日志记录工具，请在全局配置模式下使用 **logging facility** 命令。要将日志记录功能重置为默认值 20，请使用此命令的 **no** 形式。

logging facility facility
no logging facility

Syntax Description

facility 指定日志记录设备；有效值为16到23。

Command Default

默认设备为 20 (LOCAL4)。

Command Modes

下表显示可输入 命令的模式，“语法说明”部分注明了例外情况。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

系统日志服务器根据消息中的设备编号生成文件消息。有八个可能的设施：16 (LOCAL0) 至 23 (LOCAL7)。

CR_Examples

以下示例显示如何指定 ASA 在系统日志消息中将日志记录设备指示为 16。 **show logging** 命令的输出包括 ASA 正在使用的工具：

```
ciscoasa(config)# logging facility 16
ciscoasa(config)# show logging
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
  History logging: disabled
  Device ID: 'inside' interface IP address "10.1.1.1"
  Mail logging: disabled
  ASDM logging: disabled
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging flash-bufferwrap

要使ASA可在每次日志缓冲区填满从未保存的消息时将日志缓冲区写入闪存，请在全局配置模式下使用 **loggingflash-bufferwrap** 命令。要禁止将日志缓冲区写入闪存，请使用此命令的 **no**形式。

loggingflash-bufferwrap
nologgingflash-bufferwrap

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 将日志缓冲区写入闪存已禁用。
- 缓冲区大小为 4 KB。
- 最低可用闪存为 3 MB。
- 为缓冲区日志记录分配的最大闪存为 1 MB。

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	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

为了使ASA将日志缓冲区写入闪存，您必须启用日志记录到缓冲区；否则，日志缓冲区永远不会有数据写入闪存。您可以使用 **logging buffered** 命令，启用缓冲区的日志记录。但是，如果配置的日志记录缓冲区大小超过 2 MB，则内部日志缓冲区不会写入闪存。

在 ASA 将日志缓冲区内容写入闪存时，ASA 会继续将新的事件消息存储到日志缓冲区。

ASA 将创建其名称使用默认时间戳格式的日志文件，如下所示：

```
LOG-YYYY  
-MM  
-DD
```

-HHMMSS
.TXT

其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

闪存的可用性会影响 ASA 使用 **loggingflash-bufferwrap** 命令保存系统日志消息的方式。有关详细信息，请参阅 **loggingflash-maximum-allocation**和 **loggingflash-minimum-free**命令。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区，以及使ASA可将日志缓冲区写入闪存：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到 TFTP 或 FTP 服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。

logging flash-maximum-allocation

要指定 ASA 用于存储日志数据的最大闪存量，请在全局配置模式下使用 **loggingflash-maximum-allocation** 命令。要将用于此目的的最大闪存量重置为其默认的 1 MB 闪存大小，请使用此命令的 **no** 形式。

loggingflash-maximum-allocation 千字节
no loggingflash-maximum-allocation 千字节

Syntax Description

千字节 ASA 可用于保存日志缓冲区数据的最大闪存量（以千字节为单位）。节

Command Default

为日志数据分配的最大闪存默认为 1 MB。

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	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

该命令确定有多少闪存可用于 **loggingsave log** 和 **loggingflash-bufferwrap** 命令。

如果要由 **loggingsave log** 或 **loggingflash-bufferwrap** 保存的日志文件导致日志文件的闪存使用量超过 **loggingflash-maximum-allocation** 命令指定的最大数量，则 ASA 将删除最早的日志文件，以便为新的日志文件释放足够的内存。如果没有要删除的文件，或者在删除所有旧文件后，可用内存对于新日志文件来说太小，则 ASA 无法保存新日志文件。

要查看 ASA 分配的最大闪存大小是否与默认大小不同，请使用 **showrunning-config logging** 命令。如果未显示 **loggingflash-maximum-allocation** 命令，则 ASA 最多为已保存的日志缓冲区数据使用 1 MB 的空间。分配的内存同时用于 **loggingsave log** 和 **loggingflash-bufferwrap** 命令。

有关 ASA 如何使用日志缓冲区的更多信息，请参阅 **loggingbuffered** 命令。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、使 ASA 能够将日志缓冲区写入闪存，其中用于写入日志文件的最大闪存量设置为大约 1.2 MB 内存：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-maximum-allocation 1200
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除日志缓冲区中包含的所有系统日志消息。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingflash-minimum-free	指定必须可供 ASA 使用的最小闪存量，以允许将日志缓冲区写入闪存。

logging flash-minimum-free

要指定 ASA 保存新日志文件之前必须存在的最小可用闪存量，请在全局配置模式下使用 **loggingflash-minimum-free** 命令。要将所需的最小可用闪存量重置为其默认大小 3 MB，请使用此命令的 **no** 形式。

loggingflash-minimum-free 千字节

nologgingflash-minimum-free 千字节

Syntax Description

千字节 在 ASA 保存新的日志文件之前必须可用的最小闪存量（以千字节为单位）。

Command Default

默认的最小可用闪存为 3 MB。

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。

使用指南

logging flash-minimum-free 命令指定 **loggingsavelog** 和 **loggingflash-bufferwrap** 命令始终必须保留的闪存量。

如果要保存的日志文件 **loggingsavelog** 件 **loggingflash-bufferwrap** 会导致可用闪存量低于命令指定的限制 **loggingflash-minimum-free**，则 ASA 会删除最旧的日志文件，以确保在保存新日志文件后仍有足够的可用内存。如果没有要删除的文件，或者在删除所有旧文件后，可用内存仍然低于限制，则 ASA 将无法保存新的日志文件。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、启用 ASA 以将日志缓冲区写入闪存，并指定可用闪存的最小值为 4000 KB：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。
loggingflash-bufferwrap	当日志缓冲区已满时，将日志缓冲区写入到闪存。
loggingflash-maximum-allocation	指定可用于写入日志缓冲区内容的最大闪存量。

logging flow-export-syslogs

要启用或禁用 NetFlow 捕获的所有系统日志消息，请在全局配置模式下使用 **loggingflow-export-syslogs** 命令。

loggingflow-export-syslogs { **enable** | **disable** }

Syntax Description

enable 启用 Netflow 捕获的所有系统日志消息。

disable 禁用 Netflow 捕获的所有系统日志消息。

Command Default

默认情况下，NetFlow 捕获的所有系统日志均已启用。

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	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.1(1) 添加了此命令。

使用指南

如果安全设备配置为导出 NetFlow 数据，为提高性能，我们建议您通过输入 **loggingflow-export-syslogsdisable** 命令禁用冗余系统日志消息（NetFlow 也捕获的日志消息）。将禁用的系统日志消息如下：

系统日志消息	说明
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	被通过命令附加到接口的入口 ACL 或出口 ACL 拒绝的 access-group 流。
106100	ACL 允许或拒绝的流。
302013 and 302014	TCP 连接和删除。
302015 and 302016	UDP 连接和删除。
302017 and 302018	GRE 连接和删除。
302020 and 302021	ICMP 连接和删除。

系统日志消息	说明
313001	发送至安全设备的 ICMP 数据包被拒绝。
313008	发送至安全设备的 ICMPv6 数据包被拒绝。
710003	尝试连接安全设备被拒绝。



注释 虽然这是一个配置模式命令，但它并不存储在配置中。只有 **nologgingmessagexxxxxx** 命令存储在配置中。

CR_Examples

以下示例显示如何禁用 NetFlow 捕获的冗余系统日志消息以及显示的样本输出：

```
ciscoasa(config)# logging flow-export-syslogs disable
ciscoasa(config)# show running-config logging
no logging message xxxxx1
no logging message xxxxx2
```

其中 *xxxxx1* 和 *xxxxx2* 是系统日志消息，由于已通过 NetFlow 捕获相同的信息，因此这些消息是冗余的。此命令类似于命令别名，并将转换为一批无日志记录消息 **xxxxxx** 命令。在禁用系统日志消息后，可以使用 **loggingmessagexxxxxx** 命令单独启用它们，其中 *xxxxxx* 是特定系统日志消息编号。

Related Commands

命令	说明
flow-exportdestination	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器侦听的 UDP 端口。
flow-exporttemplatetimeout-rate	控制将模板信息发送到 NetFlow 收集器的间隔。
showflow-exportcounters	显示一组 NetFlow 运行时计数器。

logging from-address

要指定 ASA 发送的系统日志消息的发件人邮件地址，请在全局配置模式下使用 **loggingfrom-address** 命令。所有已发送的系统日志消息都似乎来自您指定的地址。要删除发件人电子邮件地址，请使用此命令的 **no** 形式。

loggingfrom-address发件人电子邮件地址
no loggingfrom-address发件人电子邮件地址

Syntax Description	发件人电子邮件地址 源邮件地址，即系统日志消息显示为来自的邮件地址（例如， cdb@example.com）。

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	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南	使用 loggingmail 命令启用通过邮件发送系统日志消息。
	使用此命令指定的地址无需对应于现有的邮件帐户。

CR_Examples	要启用日志记录并将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：
	• 发送重要、警报或紧急消息。
	• 使用 ciscosecurityappliance@example.com 作为发件人地址发送邮件。
	• 将邮件发送到 admin@example.com。
	• 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送邮件。

输入以下命令：

```
ciscoasa
```

```
(config)#
logging enable
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingmail	启用 ASA 通过邮件发送系统日志消息，并确定通过邮件发送系统日志消息。
loggingrecipient-address	指定系统日志消息的发送目标邮件地址。
smtp-server	配置 SMTP 服务器。
showlogging	显示已启用的日志记录选项。

logging ftp-bufferwrap

要使 ASA 能够在每次缓冲区填满从未保存的消息时，将缓冲区中已满的从未保存的消息发送到 FTP 服务器，请在全局配置模式下使用 **loggingftp-bufferwrap** 命令。要禁止将日志缓冲区发送到 FTP 服务器，请使用此命令的 **no** 形式。

loggingftp-bufferwrap
no loggingftp-bufferwrap

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值如下：

- 日志记录到缓冲区已禁用。
- 已禁用将日志缓冲区发送到 FTP 服务器。

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。

使用指南

当启用 **loggingftp-bufferwrap** 时，ASA 将日志缓冲区数据发送到您使用 **loggingftp-server** 命令指定的 FTP 服务器。在 ASA 向 FTP 服务器发送日志数据的同时，它会继续将所有新的事件消息存储到日志缓冲区。

为了使 ASA 能够将日志缓冲区内容发送到 FTP 服务器，您必须启用日志记录到缓冲区；否则，日志缓冲区永远不会有数据写入闪存。要启用缓冲区记录功能，请使用该 **loggingbuffered** 命令。

ASA 将创建其名称使用默认时间戳格式的日志文件，如下所示：

```
LOG-YYYY  
-MM  
-DD  
-HHMMSS  
.TXT
```

其中 YYYY 是年，MM 是月，DD 是月日期，HHMMSS 是时间（以小时、分钟和秒为单位）。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器以及使 ASA 可将日志缓冲区写入 FTP 服务器。此示例指定主机名为 logserver-352 的 FTP 服务器。可以使用用户名 logovernor 和密码 1luvMy10gs 访问该服务器。日志文件将存储在 /syslogs 目录中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(config)#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
loggingftp-server	指定与 loggingftp-bufferwrap 命令配合使用的 FTP 服务器参数。

logging ftp-server

要指定启用 **loggingftp-bufferwrap** 时 ASA 向其发送日志缓冲区数据的 FTP 服务器的详细信息，请在全局配置模式下使用 **loggingftp-server** 命令。要删除有关 FTP 服务器的所有详细信息，请使用此命令的 **no** 形式。

loggingftp-server*ftp_serverpathusername* [*0* | *8*] *password*
no loggingftp-server*ftp_serverpathusername* [*0* | *8*] *password*

Syntax Description

0 (可选) 指定将遵循未加密的 (明文) 用户密码。

8 (可选) 指定将遵循加密的用户密码。

ftp-server 外部 FTP 服务器 IP 地址或主机名。

注释

如果指定主机名，请确保 DNS 在您的网络上正常运行。

password 指定用户名的密码，最长可以包含 64 个字符。

path FTP 服务器上保存日志缓冲区数据的目录路径。此路径相对于 FTP 根目录。例如：

/security_appliances/syslogs/appliance107

username 有效的登录 FTP 服务器的用户名。

Command Default

默认情况下，没有指定 FTP 服务器。

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。

8.3(1) 增加了对密码加密的支持。

使用指南

只能指定一个 FTP 服务器。如果已指定日志记录 FTP 服务器，使用 **loggingftp-server** 命令会将 FTP 服务器配置替换为您输入的新配置。

ASA 不会验证您指定的 FTP 服务器信息。如果任何详细信息配置错误，ASA 将无法将日志缓冲区数据发送到 FTP 服务器。

在 ASA 启动或升级期间，不支持单位数密码以及以数字开头后跟空格的密码。例如，0 为通过，1 为无效密码。

CR_Examples

以下示例显示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器以及使 ASA 可将日志缓冲区写入 FTP 服务器。此示例指定主机名为 logserver 的 FTP 服务器。可使用用户名 user1 和密码 pass1 访问服务器。日志文件将存储在 /path1 目录中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

以下示例显示如何输入加密的密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

以下示例显示如何输入未加密（明文）密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingbuffer-size	指定日志缓冲区大小。
loggingenable	启用日志记录。
loggingftp-bufferwrap	当日志缓冲区已满时，将日志缓冲区发送到 FTP 服务器。

logging hide username

当用户名的有效性未知时，要在系统日志中隐藏用户名（例如，“*****”），请在全局配置模式下使用 **logginghideusername** 命令。要查看这些用户名，请使用此命令的 **no** 形式。

logginghideusername
no logginghideusername

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认为隐藏用户名。

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

9.3(3) 添加了此命令。

使用指南 **logginghideusername** 命令允许您在系统日志中隐藏用户名，直到它们被验证为有效为止。



注释 此命令在版本 9.4(1) 中不可用。

CR_Examples

以下示例显示如何在系统日志中隐藏用户名，直到这些用户名被验证为有效：

```
ciscoasa(config)# logging hide username
ciscoasa# show logging
Syslog logging: enabled
...
Hide Username logging: enabled | disabled
...
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。

命令	说明
showrunning-configlogging	显示运行配置的日志相关部分。

logging history

要启用 SNMP 日志记录并指定要发送到 SNMP 服务器的消息，请在 **logging history** 全局配置模式下使用该命令。要禁用 SNMP 日志记录，请使用此命令 **no** 的形式。

logginghistory [**rate-limit**number interval**level**level | *logging_list* | level]
no logging history

Syntax Description	<i>interval</i> 指定日志记录间隔（以秒为单位）（在 rate-limit 下），从而限制将日志转发到 SNMP 的速率。如果设置 logging rate-limit 命令，则该命令优先于本设置。
	level 指定历史速率限制的日志记录级别。转发到 SNMP 的消息仅限于指定的系统日志级别。
	水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或 0emergencies——系统不可用。 • 或 1alerts——需要立即采取行动。 • 或 2critical——危急情况。 • 或 3errors——错误情况。 • 或 4warnings——警告情况。 • 或 5notifications——正常但重要的情况。 • 6或 informational——信息性消息。 • 或 7debugging——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
	<i>logging_list</i> 指定标识要发送到 SNMP 服务器的消息的列表。有关创建列表的信息，请参阅 logginglist 命令。
	<i>number</i> 当使用 rate-limit 时，请指定要在该间隔期间记录的消息数。
	rate-limit 限制转发到 SNMP 的日志。指定 rate-limit （秒）以记录系统日志。
Command Default	默认情况下，ASA 不记录到 SNMP 服务器。
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。
920(1)	添加了 rate-limit 关键字，以对发送到 SNMP 的日志进行速率限制。

使用指南

logginghistory 命令允许您启用到 SNMP 服务器的日志记录，并设置 SNMP 消息级别或事件列表。

CR_Examples

以下示例显示如何启用 SNMP 日志记录并指定将严重性级别为 0、1、2 和 3 的消息发送到配置的 SNMP 服务器：

```
ciscoasa(config)# logging enable
ciscoasa(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
ciscoasa(config)# snmp-server enable traps syslog
ciscoasa(config)# logging history errors
ciscoasa(config)#
```

CR_Examples

以下示例将发送到 SNMP 的关键系统日志速率限制为 15 条消息/15 秒。

```
ciscoasa(config)# logging history rate-limit 15 15 level critical
```

使用 **no logging history** 命令以缓解设备的内存泄漏。此命令不会影响到系统日志服务器的常规日志记录。

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。
snmp-server	指定 SNMP 服务器的详细信息。

logging host

要定义系统日志服务器，请在全局配置模式下使用 **logging host** 命令。要删除 syslog 服务器定义，请使用此命令 **no** 的形式。

```
logging host interface_name syslog_ip [tcp [/port] | udp [/port]] [format
emblem | timestamp [legacy | rfc5424]] [secure [reference-identity reference_identity_name]]
no logging host interface_name syslog_ip [tcp [/port] | udp [/port]] [format
emblem | timestamp [legacy | rfc5424]] [secure [reference-identity reference_identity_name]]
```

Syntax Description

format emblem	（可选）为系统日志服务器启用 EMBLEM 格式日志记录。EMBLEM 格式日志记录仅适用于 UDP 系统日志消息。
<i>interface_name</i>	指定系统日志服务器所在的接口。
<i>port</i>	指示 syslog 服务器侦听消息的端口。对于任一协议，有效的端口值都是 1025 - 65535。如果输入零作为端口号或使用无效字符或符号，将会发生错误。
secure	（可选）指定与远程日志记录主机的连接应使用 SSL/TLS。仅在所选的协议为 TCP 的情况下此选项才有效。 注释 只能与支持 SSL/TLS 的系统日志服务器建立安全日志记录连接。如果无法建立 SSL/TLS 连接，所有新连接都将被拒绝。您可以输入 logging permit-hostdown 命令来更改此默认行为。
<i>syslog_ip</i>	指定系统日志服务器的 IP 地址（IPv4 或 IPv6）。
tcp	指定 ASA 应使用 TCP 向系统日志服务器发送消息。
udp	指定 ASA 应使用 UDP 向系统日志服务器发送消息。
<i>reference_identity_name</i>	指定引用标识对象的名称，该对象启用 RFC 6125 引用标识检查以提高安全性。根据此先前配置的引用身份对象对收到的服务器证书进行身份检查
timestamp [legacy rfc5424]	（可选）启用时间戳格式，可以指定为传统格式或 RFC5424 格式（yyyy-MM-THH:mm:ssZ，其中字母 Z 表示 UTC 时区）。

Command Default

默认协议为 UDP。

format emblem 选项的默认设置为 false。

secure 选项的默认设置为 false。

默认端口号如下：

- UDP—514

- TCP -1470

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	添加了此命令。
8.0(2)	添加了 secure 关键字。
8.4(1)	可以启用和禁用连接阻止。
9.6.2	增加了 reference-identity 选项。
9.7(1)	现在，可以将 IPv6 地址用于系统日志服务器。如果您有直接连接的系统日志服务器，可以使用 ASA 和系统日志服务器上的 /31 子网创建点对点连接。

使用指南

logginghostsyslog_ip format徽章命令允许您为每个系统日志服务器启用 EMBLEM 格式日志记录。EMBLEM 格式日志记录仅适用于 UDP 系统日志消息。如果为特定系统日志服务器启用 EMBLEM 格式日志记录，则消息会发送到该服务器。如果使用 **loggingtimestamp** 命令，则带有时间戳的消息也会发送。

您可以使用多个日志主机命令来指定所有接收系统日志消息的附加服务器。但是，只能指定服务器来接收 UDP 或 TCP 系统日志消息，而不是同时接收两者。

如果服务器证书中显示的身份与配置的身份不匹配 **reference-identity**，则不会建立连接并记录错误。

当已将 **logginghost** 命令配置为使用 TCP 向系统日志服务器发送消息时，连接阻止的默认设置为打开。如果配置了基于 TCP 的系统日志服务器，则可以使用 **loggingpermit-hostdown** 命令禁用连接阻止。



注释 在**logginghost**命令中使用 **tcp** 选项时，如果无法访问系统日志服务器，ASA 将丢弃穿过防火墙的连接。

您可以仅显示之前输入的 端口 和 协议 值，方法是使用 **showrunning-configlogging** 命令并在列表中查找该命令 - TCP 会列出为 6，UDP 会列出为 17。TCP 端口仅适用于系统日志服务器。该 端口 必须与系统日志服务器侦听的端口相同。



注释 如果尝试将 **logginghost** 命令和 **secure** 关键字与 UDP 配合使用，则会出现错误消息。

不支持在备用 ASA 上通过 TCP 发送系统日志。

在 9.18.2.4 版中，允许使用路由查找转发系统日志流量。这使得流量能够被转发，而不管日志主机 **interface_name ip_address** 配置中指定的接口是什么。但是，在 9.18.3.60 及更高版本中，9.18.2.4 中引入的更改已被删除。因此，日志主机接口名称 **ip_address** 中指定的配置优先于路由查找，并且系统日志流量从指定的接口转发。

CR_Examples

以下示例显示如何将严重性级别为 0、1、2 和 3 的系统日志消息发送到使用默认协议和端口号的内部接口上的系统日志服务器：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 2001:192:168:88::111
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging list

要创建日志记录列表以便在其他命令中使用，以根据各种标准（日志记录级别、事件类别和消息 ID）指定消息，请在 **logginglist** 全局配置模式下使用该命令。要删除列表，请使用此命 **no** 令的形式。

```
logging listname { level level [ classevent_class ] | messagestart_id [-end_id] }
nologginglistname
```

Syntax Description	classevent_class（可选）设置系统日志消息的事件类别。对于指定的级别，命令仅标识指定类的系统日志消息。请参阅“使用指南”部分以获取类别列表。
level级别	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或0emergencies—系统不可用。 • 或1alerts——需要立即采取行动。 • 或2critical——危急情况。 • 或3errors——错误情况。 • 或4warnings——警告情况。 • 或5notifications——正常但重要的情况。 • 6或informational—信息性消息。 • 或7debugging——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
messagestart_id [-end_id]	已指定消息 ID 或 ID 范围。要查找消息的默认级别，请使用 showlogging 命令或参阅系统日志消息指南。
name	设置日志记录列表名称。

Command Default 无默认为行为或值。

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	• 支持

Command History

版本 修改

7.2(1) 添加了此命令。

使用指南

可以使用列表的日志记录命令如下：

- **loggingasdm**
- **loggingbuffered**
- **loggingconsole**
- **logginghistory**
- **loggingmail**
- **loggingmonitor**
- **loggingtrap**

event_class 可能的值包括：

- 一用**auth**户身份验证。
- 一**bridge**透明防火墙。
- 一**caPKI**证书颁发机构。
- 一**config**命令界面。
- 一**eap**可扩展身份验证协议(EAP)。记录以下类型的事件以支持网络准入控制：EAP会话状态更改、EAP状态查询事件以及EAP报头和数据包内容的十六进制转储。
- 一**eapoudp**UDP上的可扩展身份验证协议(EAP)。记录EAPoUDP事件以支持网络准入控制，并生成EAPoUDP报头和数据包内容的完整记录。
- 一电子**email**邮件代理。
- 一故障**ha**转移。
- 一入**ids**入侵检测系统。
- 一**ip**IP堆栈。

- 一网nac络准入控制。记录以下类型的事件：初始化、例外列表匹配、ACS 事务、无客户端身份验证、默认 ACL 应用和重新验证。
- 一网np络处理器。
- 一ospfOSPF路由。
- 一ripRIP路由。
- 一用session户会话。
- 一snmpSNMP。
- -系sys统。
- 一vpnlKE 和 IPSec。
- 一vpncVPN 客户端。
- 一vpnfoVPN 故障转移。
- 一vpnlbVPN负载均衡。

CR_Examples

以下示例显示如何使用 logging list 命令：

```
ciscoasa(config)# logging list my-list 100100-100110
ciscoasa(config)# logging list my-list level critical
ciscoasa(config)# logging list my-list level warning class vpn
ciscoasa(config)# logging buffered my-list
```

前面的示例说明匹配指定条件的系统日志消息将被发送到日志记录缓冲区。此示例中指定的条件为：

- Syslog 消息 ID 在 100100 到 100110 范围内
- 所有具有严重或更高级别（紧急、警报或严重）的系统日志消息
- 所有具有警告级别或更高级别（紧急、警报、严重、错误或警告）的 VPN 类系统日志消息

如果系统日志消息满足其中任何一个条件，它就会被记录到缓冲区。



注释 在设计列表条件时，条件可以指定重叠的消息集。通常会记录与多组条件匹配的系统日志消息。

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。

命令	说明
showrunning-configlogging	显示运行配置的日志相关部分。

logging mail

要使ASA能够通过邮件发送系统日志消息以及确定通过邮件发送的消息，请在全局配置模式下使用 **loggingmail** 命令。要禁用系统日志消息的电子邮件发送，请使用此命令的 **no** 形式。

```
loggingmail [logging_list | level]
no loggingmail [logging_list | level]
```

Syntax Description

水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为3，则ASA将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**——系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**——信息性消息。
- 或**7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list 指定标识要发送给邮件收件人的邮件的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，电子邮件记录功能是禁用的。

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
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。

使用指南

通过邮件发送的系统日志消息显示在所发送邮件的主题行中。

CR_Examples

要将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：

- 发送重要、警报或紧急消息。
- 使用 `ciscosecurityappliance@example.com` 作为发件人地址发送邮件。
- 将邮件发送到 `admin@example.com`。
- 使用 SMTP、主要服务器 `pri-smtp-host` 和辅助服务器 `sec-smtp-host` 发送邮件。

输入以下命令：

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingfrom-address	指定邮件系统日志消息似乎来自的邮件地址。
logginglist	创建可重复使用的消息选择标准列表。
loggingrecipient-address	指定邮件系统日志消息的发送目标邮件地址。
smtp-server	配置 SMTP 服务器。

logging message

要启用系统日志消息的日志记录，或更改消息级别，请在全局配置模式下使用 **loggingmessage** 命令。
要禁用消息日志记录或将其设置为默认级别，请使用此命令的 **no** 形式。

```
loggingmessagesyslog_id [levellevel | standby]
no loggingmessagesyslog_id [levellevel | standby]
```

Syntax Description

level级 别 （可选）设置指定系统日志消息的严重性级别。您可以指定编号或名称，如下所示：

- 或**0emergencies**——系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- **6**或**informational**——信息性消息。
- 或**7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请 仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

要查找消息的默认级别，请使用 **showlogging** 命令或参阅系统日志消息指南。

syslog_id 您希望启用或禁用或希望修改其严重性级别的系统日志消息的 ID。

standby （可选）带 **no**] 关键字指定命令的 **standby**] 形式，可阻止在备用设备上生成特定系统日志消息。

Command Default

默认情况下，系统会启用所有系统日志消息，并将所有消息的严重性级别设置为其默认级别。

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	• 支持

Command History

版本	修改

7.0(1)	添加了此命令。

9.4(1)	添加了 standby 关键字。

使用指南

您可以将 **loggingmessage** 命令用于以下目的：

- 指定消息是否启用或禁用。
- 在备用设备上禁用生成系统日志消息。
- 设置消息的严重性级别。

您可以使用 **showlogging** 命令来确定当前分配给消息的级别以及是否已启用该消息。

要防止 ASA 生成特定系统日志消息，请在全局配置模式下使用 **loggingmessage** 命令的 **no** 形式（不带 **level** 关键字）。要让 ASA 生成特定系统日志消息，请使用 **loggingmessage** 命令（不带 **level** 关键字）。您可以并行使用这两个版本的 **loggingmessage** 命令。

CR_Examples

以下示例中的一系列命令显示了如何使用 **loggingmessage** 命令指定是否已启用消息以及消息的严重性级别：

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)
ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled), standby logging (disabled)
ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

命令	说明
clearconfigurelogging	清除所有日志记录配置或仅清除消息配置。
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging message standby

要解除阻止备用单元上之前阻止生成的特定系统日志消息，请在 **loggingmessagestandby** 全局配置模式下使用该命令。要阻止在备用单元上生成特定的系统日志消息，请使用此命令的 **no**形式。

loggingmessagesyslog_idstandby
no loggingmessagesyslog_idstandby

Syntax Description *syslog_id* 要在备用设备上启用或禁用的系统日志消息的ID。

Command Default 默认情况下，所有系统日志消息都在备用设备上生成（仅当启用 **logging standby** 命令时）。

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	• 支持

Command History 版本 修改
9.4(1) 添加了此命令。

使用指南 您可以使用 **[no]loggingmessagesyslog_idstandby** 命令指定在备用设备上启用还是禁用系统日志消息。
您可以使用 **showlogging**命令确定是否已启用系统日志消息。

CR_Examples 以下示例中的命令系列显示如何使用 **loggingmessagesyslog_idstandby** 命令指定是否已在备用设备上启用系统日志消息：

```
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled), standby logging disabled
```

命令	说明
clearconfigurelogging	清除所有日志记录配置或仅系统日志消息配置。
loggingenable	启用日志记录。
showrunning-configlogging	显示运行配置的日志相关部分。

logging monitor

要使 ASA 显示 SSH 和 Telnet 会话中的系统日志消息，请在全局配置模式下使用 **loggingmonitor** 命令。要禁用 SSH 和 Telnet 会话中的系统日志消息显示，请使用此命令的 **no** 形式。

loggingmonitor [*logging_list* | *level*]
nologgingmonitor

Syntax Description

水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或 **0emergencies**——系统不可用。
- 或 **1alerts**——需要立即采取行动。
- 或 **2critical**——危急情况。
- 或 **3errors**——错误情况。
- 或 **4warnings**——警告情况。
- 或 **5notifications**——正常但重要的情况。
- **6**或 **informational**——信息性消息。
- 或 **7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

logging_list 指定标识要发送到 SSH 或 Telnet 会话的消息的列表。有关创建列表的信息，请参阅 **logginglist** 命令。

Command Default

默认情况下，ASA 不在 SSH 和 Telnet 会话中显示系统日志消息。

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。

使用指南

loggingmonitor 命令为当前情景中的所有会话启用系统日志消息；在每个会话中， **terminal** 命令可以控制系统日志消息是否显示在该会话中。

CR_Examples

以下示例显示如何在控制台会话中启用系统日志消息的显示。使用 **errors** 关键字表示严重性级别为 0、1、2 和 3 的消息应显示在 SSH 和 Telnet 会话中。 **terminal** 命令使该消息显示在当前会话中：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。
terminal	设置终端线路参数。

logging permit-hostdown

要使基于 TCP 的系统日志服务器的状态与新用户会话无关，请在全局配置模式下使用 **loggingpermit-hostdown** 命令。要使 ASA 在基于 TCP 的系统日志服务器不可用时拒绝新用户会话，请使用此命令的 **no** 形式。

loggingpermit-hostdown
nologgingpermit-hostdown

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，如果您已启用到使用 TCP 连接的系统日志服务器的日志记录，则当系统日志服务器因任何原因不可用时，ASA 不允许新的网络访问会话。**loggingpermit-hostdown** 命令的默认设置为 false。

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。

使用指南

如果使用 TCP 作为日志记录传输协议用于将消息发送到系统日志服务器，并且在 ASA 无法访问系统日志服务器时，ASA 将拒绝新的网络访问会话，作为一项安全措施。您可以使用 **loggingpermit-hostdown** 命令删除此限制。

CR_Examples

以下示例使基于 TCP 的系统日志服务器的状态与 ASA 是否允许新会话无关。当 **loggingpermit-hostdown** 命令在其输出中包括 **show running-config logging** 命令时，基于 TCP 的系统日志服务器的状态与新的网络访问会话无关。

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
loggingtrap	启用到系统日志服务器的日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging queue

如要指定 ASA 在根据日志记录配置进行处理之前可在其队列中保留的系统日志消息数，请在全局配置模式下使用 **loggingqueue** 命令。要将日志记录队列大小重置为默认值 512 条消息，请使用此命令的 **no** 形式。

loggingqueuequeue_size
nologgingqueuequeue_size

Syntax Description

queue_size 在处理系统日志消息之前，用于存储系统日志消息的队列中允许的系统日志消息数量。有效值为 0 到 8192 条消息，具体取决于平台类型。如果日志队列设置为零，则队列将是最大可配置大小（8192 条消息），具体取决于平台。在 ASA-5505 上，最大队列大小为 1024。在 ASA-5510 上，此值为 2048；在所有其他平台上，此值为 8192。

Command Default

默认队列大小为 512 条消息。

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	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

当流量太大以致于队列已满时，ASA 可能会丢弃消息。在 ASA 5505 上，最大队列大小为 1024。在 ASA-5510 上为 2048。在所有其他平台上，它是 8192。



注意

在低端平台上增加日志记录队列大小可能会减少其他功能（例如 ASDM、WebVPN、DHCP 服务器等）的可用 DMA 内存量。如果系统耗尽 DMA 内存，这些功能会停止运行。使用 **showmemorydetail** 命令检查 MEMPOOL_DMA 池中的可用 DMA 内存量。

CR_Examples

以下示例显示如何显示 logging queue 和 show logging queue 命令的输出：

```
ciscoasa(config)# logging queue 0
ciscoasa(config)# show logging queue
```

```
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

在本例中，logging queue 命令设置为 0，表示队列设置为最大值 8192。ASA 以日志记录配置指定的方式处理队列中的系统日志消息，例如将系统日志消息发送至邮件收件人、将其保存至闪存等。

此 show logging queue 命令示例的输出显示有 5 条消息已排队，3513 条消息是自 ASA 最后一次启动后队列中一次的最大消息数，且已丢弃 1 条消息。即使队列设置为可容纳无限消息，该消息仍会被丢弃，因为没有块内存可用于将消息添加到队列。

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging rate-limit

要限制生成系统日志消息的速率，请在特权 EXEC 模式下使用 **logging rate-limit** 命令。要禁用速率限制，请在特权 EXEC 模式下使用此命令的 **no** 形式。

```
logging rate-limit { unlimited | dynamic { blockvalue [ message limit值 ] } | { num [ interval ] } | message { syslog_id | levelseverity_level } }
[ no ] logging rate-limit { unlimited | dynamic { blockvalue [ message limit值 ] } | { num [ interval ] } | message { syslog_id | levelseverity_level } }
```

Syntax Description

block 值	用作速率限制阈值的块的百分比。
dynamic	当大小为 256 的块使用率超过指定的阈值时，限制记录率。当块使用率恢复正常值时禁用速率限制。
间隔	（可选）用于测量消息生成速率的时间间隔（以秒为单位）。间隔值的有效范围为 0 到 2147483647。
levelseverity_level	将所设置的速率限制应用于属于特定严重性级别的所有系统日志消息。处于指定严重性级别的所有系统日志消息都将单独进行速率限制。严重性_级别 的有效范围为 1 到 7。
message	抑制此系统日志消息的报告。
message limit 值	动态速率限制允许的消息数量。
num	在指定时间间隔内可以生成的系统日志消息的数量。num 值的有效范围为 0 到 2147483647。
syslog_id	要抑制的系统日志消息的 ID。值的有效范围为 100000 - 999999。
unlimited	禁用速率限制，这意味着日志记录速率没有限制。

Command Default

interval 的默认设置为 1。

message limit值的默认设置为 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
特权 EXEC	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(4)	添加了此命令。
9.18(1)	添加了用于速率限制的动态选项。

使用指南

系统日志消息严重性级别如下：

- 0 - 系统不可用
- 1——需要立即采取行动
- 2—危急情况
- 3—错误情况
- 4—警告情况
- 5 - 正常但重大的情况
- 6—信息消息
- 7—调试消息



注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

CR_Examples

要限制系统日志消息生成速率，可以输入特定消息 ID。以下示例显示如何使用特定消息 ID 和时间间隔来限制系统日志消息生成的速率：

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

在指定的 600 秒间隔内达到速率限制 100 后，此示例禁止将系统日志消息 302020 发送到主机。

要限制系统日志消息生成速率，可以输入特定严重性级别。以下示例显示如何使用特定严重性级别和时间间隔来限制系统日志消息生成的速率。

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

此示例将严重性级别为 6 下的所有系统日志消息在 600 秒的指定时间间隔内抑制到指定的速率限制 1000。每条严重性级别为 6 的系统日志消息的速率限制为 1000。

要在大小为 256 的块使用率较高时启用消息的动态速率限制，请使用 **dynamic** 关键字。您可以指定空闲 256 个块的百分比作为触发动态速率限制的阈值。您还可以使用 **message limit** 关键字来允许进行动态速率限制的消息数。其默认值为 10。

```

asa(config)# logging rate-limit ?

configure mode commands/options:
  <1-2147483647> Specify logging rate-limit number
  dynamic       Specify dynamic option for rate-limit
  unlimited     Specify unlimited option for rate-limit

asa(config)# logging rate-limit dynamic ?

configure mode commands/options:
  block Dynamic rate-limit for block usage

asa(config)# logging rate-limit dynamic block ?

configure mode commands/options:
  <1-100> Specify 256 blocks free percentage to trigger dynamic rate-limit
asa(config)# logging rate-limit dynamic block 50 ?

configure mode commands/options:
  messagelimit Specify the number of messages allowed for dynamic rate-limit

asa(config)# logging rate-limit dynamic block 50 messagelimit ?

configure mode commands/options:
  <1-100> Specify logging rate-limit interval

```

Related Commands

命令	说明
clearrunning-configloggingrate-limit	将日志记录速率限制设置重置为其默认值。
showlogging	显示当前位于内部缓冲区或日志记录配置设置中的消息。
showrunning-configloggingrate-limit	显示当前日志记录速率限制设置。

logging recipient-address

要指定 ASA 发送的系统日志消息的接收邮件地址，请在全局配置模式下使用 **loggingrecipient-address** 命令。要删除接收电子邮件地址，请使用此命令的 **no** 形式。

loggingrecipient-addressaddress [levellevel]

nologgingrecipient-addressaddress [levellevel]

Syntax Description

地 址 通过电子邮件发送系统日志消息时指定收件人电子邮件地址。

level 表示严重性级别如下。

水平 设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示：

- 或**0emergencies**——系统不可用。
- 或**1alerts**——需要立即采取行动。
- 或**2critical**——危急情况。
- 或**3errors**——错误情况。
- 或**4warnings**——警告情况。
- 或**5notifications**——正常但重要的情况。
- 或**6informational**——信息性消息。
- 或**7debugging**——调试消息。

注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，**请** 仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

注释

我们不建议在 **loggingrecipient-address** 命令中使用大于 3 的严重性级别。较高的严重性级别可能会因缓冲区溢出而导致系统日志消息被丢弃。

由 **loggingrecipient-address** 命令指定的消息严重性级别会覆盖由 **loggingmail** 命令指定的消息严重性级别。例如，如果 **loggingrecipient-address** 命令指定的严重性级别为 7，但 **loggingmail** 命令指定的严重性级别为 3，则 ASA 将所有消息都发送给收件人，包括严重性级别为 4、5、6 和 7 的消息。

Command Default

默认值设置为 errors logging level。

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。

使用指南

您最多可以配置 5 个收件人地址。如果需要，每个收件人地址可以具有不同于 **loggingmail** 命令指定的邮件级别。使用 **loggingmail** 命令启用通过邮件发送系统日志消息。

使用此命令可将更紧急的邮件发送给更多的收件人。

CR_Examples

要将 ASA 设置为通过邮件发送系统日志消息，请使用以下条件：

- 发送重要、警报或紧急消息。
- 使用 `ciscosecurityappliance@example.com` 作为发件人地址发送邮件。
- 将邮件发送到 `admin@example.com`。
- 使用 SMTP、主要服务器 `pri-smtp-host` 和辅助服务器 `sec-smtp-host` 发送邮件。

输入以下命令：

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

命令	说明
loggingenable	启用日志记录。
loggingfrom-address	指定系统日志消息出现的邮件地址。

命令	说明
loggingmail	启用 ASA 通过邮件发送系统日志消息，并确定通过邮件发送系统日志消息。
smtp-server	配置 SMTP 服务器。
showlogging	显示已启用的日志记录选项。

logging savelog

要将日志缓冲区保存到闪存，请在 **loggingsavelog** 特权 EXEC 模式下使用该命令。

loggingsavelog [*savefile*]

Syntax Description

savefile （可选）已保存的闪存文件名。如果您未指定文件名，ASA 将使用默认时间戳格式保存日志文件，如下所示：

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

其中 YYYY 是年，MM 是月，DD 是月日期，HHMMSS 是时间（以小时、分钟和秒为单位）。

Command Default

默认值如下：

- 缓冲区大小为 4 KB。
- 最低可用闪存为 3 MB。
- 为缓冲区日志记录分配的最大闪存为 1 MB。
- “语法说明” 部分介绍了默认日志文件名。

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	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

在您将日志缓冲区保存到闪存之前，您必须启用日志记录到缓冲区；否则日志缓冲区始终不会将数据保存到闪存。要启用缓冲区记录功能，请使用该 **loggingbuffered**命令。



注释 该 **loggingsavelog**命令不会清除缓冲区。要清除缓冲区，请使用 **clearloggingbuffer**命令。

CR_Examples

以下示例启用日志记录和日志缓冲区，退出全局配置模式，并使用文件名 latest-logfile.txt 将日志缓冲区保存到闪存：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# exit
ciscoasa# logging savelog latest-logfile.txt
ciscoasa#
```

Related Commands

命令	说明
clearloggingbuffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到 TFTP 或 FTP 服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。
loggingbuffered	启用将日志记录记录到日志缓冲区。
loggingenable	启用日志记录。

logging standby

要使故障转移备用 ASA 能够将系统日志消息发送到日志记录目标，请在全局配置模式下使用 **loggingstandby** 命令。要禁用 syslog 消息传递和 SNMP 日志记录，请使用此命令的 **no**形式。

loggingstandby
nologgingstandby

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下，logging standalone 命令是禁用的。

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
全局配置	• 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 您可以启用该 **loggingstandby**命令，以确保发生故障转移时故障转移备用 ASA 的系统日志消息保持同步。



注释 使用该 **loggingstandby**命令会导致共享日志记录目标（例如 syslog 服务器、SNMP 服务器和 FTP 服务器）的流量增加一倍。

CR_Examples

以下示例使 ASA 能够将系统日志消息发送到故障转移备用 ASA。**showlogging** 命令的输出表示此功能已启用：

```
ciscoasa(config)# logging standby
ciscoasa(config)# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: enabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

命令	说明
failover	启用故障转移功能。
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging timestamp

要指定系统日志消息应包含消息的生成日期和时间，请在全局配置模式下使用 **loggingtimestamp** 命令。要从系统日志消息中删除日期和时间，请使用此命令的 **no**形式。

loggingtimestamp [**rfc5424**]
nologgingtimestamp

Syntax Description

rfc5424 （可选）所有系统日志消息的时间戳都将按照 RFC 5424 格式显示时间：

```
YYYY
-MM
-DD
THH:MM:SS
Z
```

其中 YYYY 是年，MM 是月，DD 是月日期，HHMMSS 是时间（以小时、分钟和秒为单位）。

Command Default

默认情况下，ASA 不在系统日志消息中包含日期和时间。

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。
	9.10(1)	TheoptiontoenabletimestampasperRFC5424formatwasadded

使用指南

logging timestamp 命令使 ASA 在所有系统日志消息中包含时间戳。在版本 9.10(1) 之前，系统日志的时间戳符合 RFC 3164，其中时间戳以 “MM DD YYYY HH:MM:SS” 格式显示。

此格式在 SIEM 中不是首选格式，因此 9.10(1) 中引入了 RFC 5424 选项。

将 RFC 5424 选项与 logging timestamp 命令配合使用，以按照 RFC 5424 启用系统日志支持时区。

CR_Examples

以下示例启用在所有系统日志消息中包含时间戳信息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp
ciscoasa(config)#
```

以下示例启用在所有系统日志消息中包含 RFC 5424 格式的时间戳信息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp rfc5424
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

logging trap

要指定 ASA 将哪些系统日志消息发送到系统日志服务器，请在全局配置模式下使用 **loggingtrap** 命令。要从配置中删除此命令，请使用此命令 **no** 的形式。

loggingtrap [*logging_list* | *level*]
nologgingtrap

Syntax Description	水平	设置系统日志消息的最大严重性级别。例如，如果将严重性级别设置为 3，则 ASA 将生成严重性级别 3、2、1 和 0 的系统日志消息。您可以指定编号或名称，如下所示： • 或 0emergencies——系统不可用。 • 或 1alerts——需要立即采取行动。 • 或 2critical——危急情况。 • 或 3errors——错误情况。 • 或 4warnings——警告情况。 • 或 5notifications——正常但重要的情况。 • 或 6informational——信息性消息。 • 或 7debugging——调试消息。 注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。
	日志记录列表	指定要发送到 syslog 服务器的消息的列表。有关创建列表的信息，请参阅 logginglist 命令。

Command Default 未定义默认系统日志消息陷阱。

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。

使用指南

如果使用 TCP 作为日志记录传输协议，并且在 ASA 无法访问系统日志服务器、系统日志服务器配置错误或磁盘已满时，作为一项安全措施，ASA 将拒绝新的网络访问会话。

如果系统日志服务器发生故障，基于 UDP 的日志记录不会阻止 ASA 传递流量。

CR_Examples

以下示例显示如何将严重性级别为 0、1、2 和 3 的系统日志消息发送到位于内部接口上并使用默认协议和端口号的系统日志服务器。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

Related Commands

命令	说明
loggingenable	启用日志记录。
logginghost	定义系统日志服务器。
logginglist	创建可重复使用的消息选择标准列表。
showlogging	显示已启用的日志记录选项。
showrunning-configlogging	显示运行配置的日志相关部分。

login

要使用本地用户数据库登录到特权 EXEC 模式（请参阅 `username` 命令）或更改用户名，请在用户 EXEC 模式下使用 `login` 命令。

login

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	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南 在用户 EXEC 模式下，您可以使用 `login` 命令以本地数据库中的任何用户名身份登录特权 EXEC 模式。当您启用了 `enable` 身份验证（请参阅 `aaaauthenticationconsole` 命令）时，`login` 命令类似于 `enable` 命令。与 `enable authentication` 不同，`login` 命令只能使用本地用户名数据库，并且使用此命令需要始终进行身份验证。您还可以从任何 CLI 模式下使用 `login` 命令更改用户。

如要允许用户在登录后访问特权 EXEC 模式（以及所有命令），请将用户权限级别设置为 2（默认）到 15。如果配置本地命令授权，则用户只能输入分配给该权限级别或更低级别的命令。请参阅 `aaaauthorizationcommand` 了解更多信息。



注意 如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可以使用 RADIUS 或 TACACS+ 身份验证，或者您可以将所有本地用户设置为级别 1，以便您可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

CR_Examples 以下示例显示了您输入 `login` 命令后的提示符：

```
ciscoasa> login
Username:
```

Related Commands	命令	说明
	aaaauthorizationcommand	启用 CLI 访问的命令授权。
	aaaauthenticationconsole	需要进行控制台、Telnet、HTTP、SSH 或 enable 命令访问的身份验证。
	logout	注销 CLI。
	username	将用户添加到本地数据库。

login-button

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面登录框的登录按钮，请使用 `webvpn` 自定义配置模式下的 **login-button** 命令。要从配置中删除命令并导致值被继承，请使用命令 **no** 的形式。

login-button { **text** | **style** } *value*

[**no**] **login-button** { **text** | **style** } *value*

Syntax Description

style 指示您正在更改样式。

text 指示您正在更改文本。

value 要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

登录按钮的默认文本为 “Login”。

默认登录按钮样式为：

border: 1px solid black;background-color:white;font-weight:bold; font-size: 80%

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 自定义配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

该 **style** 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。

- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。



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

CR_Examples

以下示例使用文本 “OK” 自定义登录按钮：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

Related Commands

命令	说明
login-title	自定义 WebVPN 页面登录框的标题。
group-prompt	自定义 WebVPN 页面登录框的群组提示。
password-prompt	自定义 WebVPN 页面登录框的密码提示。
username-prompt	自定义 WebVPN 页面登录框的用户名提示。

login-message

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面的登录消息，请使用 `webvpn` 自定义配置模式下的 **login-message** 命令。要从配置中删除命令并导致值被继承，请使用命令 **no** 的形式。

login-message { **text** | **style** } *value*

[**no**] **login-message** { **text** | **style** } *value*

Syntax Description

text 指示您正在更改文本。

style 指示您正在更改样式。

value 要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认登录消息是“请输入您的用户名和密码”。

默认登录消息样式为背景颜色：#CCCCCC;颜色：黑色。

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 自定义配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

该 **style** 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

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



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

CR_Examples

在以下示例中，登录消息文本设置为 “username and password”：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

Related Commands

命令	说明
login-title	自定义 WebVPN 页面上登录框的标题。EXTENSI
username-prompt	自定义 WebVPN 页面登录的用户名提示。
password-prompt	自定义 WebVPN 页面登录的密码提示。
group-prompt	定制 WebVPN 页面登录的群组提示。

login-title

要自定义向 WebVPN 用户显示的 WebVPN 页面上的登录框的标题，请使用 `webvpn` 自定义配置模式下的 `login-title` 命令。要从配置中删除命令并导致值被继承，请使用命令 `no` 的形式。

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

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

Syntax Description

text 指示您正在更改文本。

style 指定您正在更改 HTML 样式。

value 要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认登录文本为“Login”。

登录标题的默认 HTML 样式为背景颜色: #666666;颜色: 白色。

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 自定义配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

该 **style** 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

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



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

CR_Examples

以下示例配置登录标题样式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

命令	说明
login-message	自定义 WebVPN 登录页面的登录消息。
username-prompt	自定义 WebVPN 登录页面的用户名提示。
password-prompt	自定义 WebVPN 登录页面的密码提示。
group-prompt	自定义 WebVPN 登录页面的组提示。

徽标

要自定义 WebVPN 用户连接到安全设备时显示的 WebVPN 页面上的徽标，请使用 `webvpn` 自定义模式下的 `logo` 命令。要从配置中删除徽标并重置默认值（思科徽标），请使用此命令的 `no` 形式。

`logo { none | file { 路径值 } }`

`[no] logo { { none | file { 路径值 } } }`

Syntax Description

file	表示您提供的文件中包含徽标。
none	表示无徽标。设置一个空值，从而不允许使用徽标。防止继承徽标。
path	文件名的路径。可能的路径为 <code>disk0:</code> 、 <code>disk1:</code> 或 <code>flash:</code>
value	指定徽标的文件名。最大长度为 255 个字符，无空格。文件类型必须为 JPG、PNG 或 GIF，并且必须小于 100 KB。

Command Default

默认徽标是思科徽标。

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 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

如果指定的文件名不存在，将显示错误消息。如果删除徽标文件，但配置仍指向该文件，则不会显示任何徽标。

文件名不能包含空格。

CR_Examples

在下面的示例中，`cisco_logo.gif` 文件包含一个自定义徽标：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Related Commands

命令	说明
title	自定义 WebVPN 页面的标题。
page style	定制使用层叠样式表 (CSS) 参数的 WebVPN 页面。

logout

要退出 CLI，请在用户 EXEC 模式下使用 **logout**命令。

logout

Syntax Description 此命令没有任何参数或关键字。

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
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 **logout**命令允许您注销 ASA。您可以使用 **exit**或**quit** 命令返回到非特权模式。

CR_Examples 以下示例显示如何注销 ASA：

```
ciscoasa> logout
```

Related Commands

命令	说明
login	启动登录提示。
exit	退出访问模式。
quit	退出配置模式或特权模式。

logout-message

要自定义 WebVPN 用户从 WebVPN 服务注销时向其显示的 WebVPN 注销屏幕的注销消息，请在 webvpn 自定义配置模式下使用 **logout-message**命令。要从配置中删除命令并导致值被继承，请使用命令 **no** 的形式。

logout-message { **text** | **style** } 数值

[**no**] **logout-message** { **text** | **style** } 数值

Syntax Description

style 指示您正在更改样式。

text 指示您正在更改文本。

value 要显示的实际文本（最多 256 个字符）或层叠样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认的注销消息文本为 “Goodbye”。

默认注销消息样式为背景颜色：#999999;颜色：黑色。

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 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。

- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。



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

CR_Examples

以下示例配置注销消息样式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# logout-message style background-color: rgb(51,51,255);color:
  rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
  bold
```

Related Commands

命令	说明
logout-title	自定义 WebVPN 页面的注销标题。
group-prompt	自定义WebVPN页面登录框的群组提示。
password-prompt	自定义WebVPN页面登录框的密码提示。
username-prompt	自定义WebVPN页面登录框的用户名提示。

lsp-full suppress

要控制在链路状态协议数据单元 (PDU) 变满时抑制哪些路由，请在路由器 isis 配置模式下使用 **lsp-fullsuppress** 命令。要停止抑制已重新分发的路由，请指定此命令的 **no** 形式。

lsp-fullsuppress { **external** [**interlevel**] | **interlevel** [**external**] | **none** }
nolsp-fullsuppress

Syntax Description	external 抑制此 ASA 上的任何重新分配路由。
	级别间 抑制来自其他级别的任何路由。例如，如果 Level-2 LSP 已满，则将抑制来自 Level 1 的路由。
	无 不抑制任何路由。

Command Default 抑制重新分发的路由。

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
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 此命令允许监控 IS-IS 邻接状态更改。这在监控大型网络时可能非常有用。使用系统错误消息工具记录消息。消息的形式如下：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

CR_Examples

以下示例显示如何指定在 LSP 已满时，将从 LSP 抑制重新分发的路由和来自其他级别的路由：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-full suppress interlevel external
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
iscircuit-type	配置用于 IS-IS 的邻接类型。
iscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
ishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
ishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
ishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isiprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
pnprotocolshutdow	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

lsp-gen-interval

要自定义 LSP 生成的 IS-IS 限制，请在路由器 isis 配置模式下使用 **lsp-gen-interval** 命令。要恢复默认值，请使用此命令 **no** 的形式。

lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait* *lsp-second-wait*]
no **lsp-gen-interval**

Syntax Description	level-1	（可选）仅适用于 1 级区域。
	level-2	（可选）仅适用于 2 级区域。
	<i>lsp-max-wait</i>	指示生成 LSP 的两次连续出现之间的最大间隔。范围为 1 到 120 秒。
	<i>lsp-initial-wait</i>	（可选）表示初始 LSP 生成延迟。范围为 1 到 120,000 毫秒。
	<i>lsp-second-wait</i>	（可选）指示第一次和第二次 LSP 生成之间的保持时间。范围为 1 到 120,000 毫秒。

Command Default	<i>lsp-max-wait</i> :	5 秒
	<i>lsp-initial-wait</i> :	50 毫秒
	<i>lsp-second-wait</i> :	5000 毫秒

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
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 以下描述可帮助确定是否更改此命令的默认值：
- *lsp-initial-wait* 参数表示生成第一个 LSP 之前的初始等待时间。
 - 第三个参数指示在生成第一个和第二个 LSP 之间等待的时长。
 - 每个后续的等待间隔都是前一个的两倍，直到等待间隔达到指定的 *lsp-max-wait* 间隔 为止，因此，在初始间隔和第二个间隔之后，该值会导致 LSP 生成节流或减慢。一旦达到此间隔，等待间隔就会以此间隔继续，直到网络稳定下来。

- 网络稳定下来并且在两倍 *lsp-max-wait* 间隔内没有触发器后，将恢复快速行为（初始等待时间）。

CR_Examples

以下示例为 LSP 生成限制配置间隔：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。

命令	说明
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。

命令	说明
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

lsp-refresh-interval

如要设置 LSP 刷新闻隔，请在路由器 isis 配置模式下使用 **lsp-refresh-interval** 命令。要恢复默认刷新闻隔，请使用此命 **no** 令的形式。

lsp-refresh-interval 秒
no lsp-refresh-interval

Syntax Description 秒 LSP 的刷新闻隔。范围为 1 到 65535 秒。

Command Default 默认值为 900 秒（15 分钟）。

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 刷新闻隔确定该软件在 LSP 中定期发送其始发的路由拓扑信息的速率。这样做是为了防止数据库信息过时。



注释 在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果设置的 LSP 有效期比 LSP 刷新闻隔低很多，该软件将缩短 LSP 刷新闻隔以防止 LSP 超时。

CR_Examples

以下示例将 IS-IS LSP 刷新闻隔配置为 1080 秒：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-refresh-interval 1080
```

Related Commands	命令	说明
	advertise passive-only	配置 ASA 以通告被动接口。

命令	说明
area-password	配置 IS-IS 区域身份验证密码。
authentication key	全局启用 IS-IS 身份验证。
authentication mode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authentication send-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clear isis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hello padding	将 IS-IS hello 配置为完整 MTU 大小。
hostname dynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isis adjacency-filter	过滤 IS-IS 邻接关系的建立。
isis advertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isis authentication key	启用接口的身份验证。
isis authentication mode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isis authentication send-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isis circuit-type	配置用于 IS-IS 的邻接类型。
isis csnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isis hello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isis hello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isis hello padding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isis lsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。

命令	说明
isis metric	配置 IS-IS 度量的值。
isis password	配置接口的认证密码。EXTEN
isis priority	配置接口上指定 ASA 的优先级。
isis protocol shutdown	禁用每个接口的 IS-IS 协议。
isis retransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis retransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis tag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-full suppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocol shutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistribute isis	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。
route priority high	为 IS-IS IP 前缀分配高优先级。
router isis	启用 IS-IS 路由。

命令	说明
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
show clns	显示 CLNS 特定信息。
show isis	显示 IS-IS 信息。
show route isis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。



maa – match d

- [mac address](#) , 第 609 页
- [mac-address](#) , 第 611 页
- [mac-address auto](#) , 第 614 页
- [mac-address pool](#) , 第 619 页
- [mac-address-table aging-time](#) , 第 620 页
- [mac-address-table static](#) , 第 622 页
- [mac-learn disable](#) , 第 624 页
- [mac-learn 泛洪](#) , 第 626 页
- [mac-list](#) , 第 627 页
- [mail-relay](#) , 第 629 页
- [management-access](#) , 第 631 页
- [management-only](#) , 第 633 页
- [map-domain](#) , 第 635 页
- [map-name](#) , 第 637 页
- [mapping-service \(已弃用\)](#) , 第 639 页
- [map-value](#) , 第 641 页
- [mask](#) , 第 643 页
- [mask-banner](#) , 第 645 页
- [mask-syst-reply](#) , 第 646 页
- [match access-list](#) , 第 647 页
- [match any](#) , 第 649 页
- [match apn](#) , 第 651 页
- [match application-id](#) , 第 652 页
- [match as-path](#) , 第 654 页
- [match avp](#) , 第 656 页
- [match body](#) , 第 659 页
- [match called-party](#) , 第 661 页
- [match calling-party](#) , 第 662 页
- [match certificate](#) , 第 663 页

- [匹配证书允许过期证书（已弃用），第 667 页](#)
- [match certificate skip revocation-check，第 668 页](#)
- [match cmd，第 669 页](#)
- [match command-code，第 671 页](#)
- [match community，第 673 页](#)
- [match default-inspection-traffic，第 675 页](#)
- [match dns-class，第 678 页](#)
- [match dns-type，第 680 页](#)
- [match domain-name，第 682 页](#)
- [match dpc，第 684 页](#)
- [match dscp，第 686 页](#)

mac address

要为主用设备和备用设备指定虚拟 MAC 地址，请在故障转移组配置模式下使用 **macaddress** 命令。要恢复默认虚拟 MAC 地址，请使用此 **no** 命令的形式。

```
mac address phy_if [active_mac] [standby_mac]
no mac address phy_if [active_mac] [standby_mac]
```

Syntax Description

<i>phy_if</i>	设置 MAC 地址的接口的物理名称。
<i>active_mac</i>	主用设备的虚拟 MAC 地址。MAC 地址必须以 h.h.h 格式输入，其中 h 是 16 位十六进制数。
<i>standby_mac</i>	备用设备的虚拟 MAC 地址。MAC 地址必须以 h.h.h 格式输入，其中 h 是 16 位十六进制数。

Command Default

默认值如下：

- 主用设备默认 MAC 地址：00a0.c9physical_port_number . failover_group_id 01。
- 备用设备默认 MAC 地址：00a0.c9physical_port_number . failover_group_id 02。

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

如果没有为故障转移组定义虚拟 MAC 地址，则会使用默认值。

如果您在同一网络上有多个主用/主用故障转移对，则分配给一对接口的默认虚拟 MAC 地址可能与分配给其他对接口的默认虚拟 MAC 地址相同。虚拟 MAC 地址确定。为避免网络中出现重复的 MAC 地址，请确保为每个物理接口分配一个虚拟的主用和备用 MAC 地址。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

CR_Examples

以下部分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)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failovermacaddress	为物理接口指定虚拟 MAC 地址。

mac-address

要手动为接口或子接口分配私有 MAC 地址，请在 **mac-address** 接口配置模式下使用该命令。在多情景模式下，此命令可以在每个情景中为接口分配不同的 MAC 地址。对于集群中的单个接口，您可以分配 MAC 地址集群池。要将 MAC 地址恢复为默认值，请使用此命令的 **no** 形式。

```
mac-address { mac_address [ standby mac_address | site-id number [ site-ip ip_address ] ] | cluster-pool pool_name }
no
mac-address { mac_address [ standby mac_address | site-id number [ site-ip ip_address ] ] | cluster-pool pool_name }
```

Syntax Description

cluster-pool pool_name 对于单个接口模式下的集群（请参阅 **clusterinterface-mode** 命令），或对于任何集群接口模式下的管理接口，设置要用于每个集群成员上给定接口的 MAC 地址池。使用 **mac-address pool** 命令定义地址池。

mac_address 以 H.H.H 格式设置此接口的 MAC 地址，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。如果使用故障转移，则此 MAC 地址为主用 MAC 地址。

注释

因为自动生成的 **mac-address auto** 地址（命令）以 A2 开头，所以如果您还想使用自动生成，则不能以 A2 开头手动 MAC 地址。

site-id 编号 （可选；仅限路由模式）对于站点间集群，为每个站点配置站点特定的 MAC 地址。

site-ip ip_address （可选；仅限路由模式）对于站点间集群，为每个站点配置一个站点特定的 IP 地址。该 IP 地址必须与全局 IP 地址位于同一子网。

standby mac_address （可选）设置故障转移的备用 MAC 地址。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

Command Default

默认 MAC 地址是烧录的物理接口 MAC 地址。子接口将继承物理接口 MAC 地址。有些命令会设置物理接口 MAC 地址（包括单情景模式下的此命令），因此继承的地址取决于该配置。

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	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(5)/8.2(2)	与 mac-addressauto 命令一起使用时，使用 A2 来启动 MAC 地址会受到限制。
9.0(1)	添加 cluster-pool 关键字是为了支持集群。
9.5(1)	已添加关 site-id 键字。
9.6(1)	已添加关 site-ip 键字。

使用指南

在多情景模式下，如果在情景之间共享接口，则可以将唯一 MAC 地址分配给每个情景的接口。借助此功能，ASA 可轻松地将数据包分类到适当的情景中。可使用没有唯一 MAC 地址的共享接口，但受到一些限制。有关详细信息，请参阅 CLI 配置指南。

您可以使用此命令手动分配每个 MAC 地址，也可以使用该命令自动为上下文中的 **mac-addressauto** 共享接口生成 MAC 地址。如果自动生成MAC地址，则可以使用该 **mac-address**命令覆盖生成的地址。

对于单情景模式，或者多情景模式下不共享的接口，您可能想要给予接口分配唯一 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

对于集群，必须为跨网络EtherChannel配置全局MAC地址。如果是手动配置的MAC地址，该MAC地址将始终属于当前的主设备。在多上下文模式下，如果在上下文之间共享一个接口，则应启用 MAC 地址的自动生成。请注意，您必须为非共享接口手动配置 MAC 地址。

对于路由模式下的站点间集群，请在主设备上为每个站点配置一个站点特定的MAC地址和IP地址，然后在每台设备上使用 **site-id** 命令将其分配给站点。

CR_Examples

以下示例为 GigabitEthernet 0/1.1 配置 MAC 地址：

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

以下示例为跨区以太网通道端口通道 1 配置站点特定的 MAC 地址：

```
ciscoasa(config-if)# interface port-channel 1
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.7.7.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.7.7.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.7.7.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.7.7.4
```


Related Commands

命令	说明
failovermacaddress	主用/备用故障转移的物理接口的主用和备用 MAC 地址。
macaddress	主用/主用故障转移的物理接口的主用和备用 MAC 地址。
mac-addressauto	在多情景模式下自动为共享接口生成 MAC 地址（主用和备用）。
mode	将安全上下文模式设置为多重或单一。
showinterface	显示接口特征，包括 MAC 地址。

mac-address auto

要自动将专用 MAC 地址分配给每个共享情景接口，请在全局配置模式下使用 **mac-addressauto** 命令。要禁用自动 MAC 地址，请使用此命令 **no** 的形式。

mac-addressauto [*prefixprefix*]
no mac-address auto

Syntax Description

prefix前缀 （可选）将用户定义的前缀设置为 MAC 地址的一部分。前缀是0~65535之间的十进制值。如果未输入前缀，ASA 将生成默认前缀。

将此前缀转换为 4 位十六进制号码。该前缀可确保每个 ASA 使用唯一的 MAC 地址（使用不同的前缀值），因此，例如，您可以在一个网段上拥有多个 ASA。

Command Default

默认情况下会禁用自动 MAC 地址生成，但 ASASM 除外，其默认情况下会启用。如果已启用，ASA 根据接口 (ASA 5500-X) 或背板 (ASASM) 中 MAC 地址的最后两个字节自动生成前缀。如果需要，您也可以自定义该前缀。

如果禁用 MAC 地址生成，请参阅以下默认 MAC 地址：

- 对于 ASA 5500-X 系列设备 - 物理接口使用固化 MAC 地址，并且该物理接口的所有子接口都使用同一固化 MAC 地址。
- 对于 ASASM - 所有 VLAN 接口都使用派生自背板 MAC 地址的同一 MAC 地址。

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
7.2(1)	添加了此命令。
8.0(5)/8.2(2)	添加了 prefix 关键字。MAC 地址格式已更改为使用前缀、使用固定起始值(A2)，并且对故障转移对中的主单元和辅助单元 MAC 地址使用不同的方案。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。
8.5(1)	现在，自动生成仅对 ASASM 默认启用 (mac-addressauto)。

版本	修改
8.6(1)	ASA 现在将自动 MAC 地址生成配置转换为使用默认前缀。ASA 根据接口 (ASA 5500) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。传统的 MAC 地址生成方法不再可用。 注释 为了保持故障转移对无中断升级，如果已启用故障转移，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。

使用指南

为了允许上下文共享接口，我们建议您为每个共享上下文接口分配唯一的 MAC 地址。MAC 地址用于在情景中对数据包进行分类。如果共享某个接口，但在每个情景中没有该接口的唯一 MAC 地址，则使用目标 IP 地址对数据包进行分类。目的地址与情景 NAT 配置相匹配，与 MAC 地址方法相比，此方法有一些限制。有关对数据包进行分类的信息，请参阅 CLI 配置指南。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以在情景中为接口手动设置 MAC 地址。请参阅 **mac-address** 手动设置 MAC 地址的命令。

与手动 MAC 地址的交互

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。

由于自动生成的地址以 A2 开头，因此如果您还想使用自动生成，则不能以 A2 开头手动 MAC 地址。

故障转移 MAC 地址

为了能用于故障切换，ASA 会为每个接口生成主用和备用 MAC 地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。请参阅 <xref> 部分以了解更多信息。

有关使用添加 **prefix** 关键字之前的 **mac-address auto** 命令的旧版升级故障转移，请参阅 <xref> 部分的详细信息。

使用前缀的 MAC 地址格式

ASA 使用以下格式生成 MAC 地址：

A2xx.yyzz.zzzz

其中 xx.yy 是用户定义的前缀或基于接口 (ASA 5500) 或背板 (ASASM) MAC 地址的最后两个字节自动生成的前缀，zz.zzzz 是 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

举例来说，如果您设置前缀 77，则 ASA 会将 77 转换为十六进制值 004D (yyxx)。在 MAC 地址中使用 时，前缀会被反转 (xyyy) 以匹配 ASA 本机形式：

A24D.00zz.zzz.xz

对于前缀 1009 (03F1)，MAC 地址为：

A2F1.03zz.zzz.xz

不带前缀的 MAC 地址格式（传统方法）

如果您使用故障转移并且已升级到 8.6 或更高版本，则可以使用此方法；在这种情况下，您必须手动启用前缀方法。

如果没有前缀，则 MAC 地址使用以下格式生成：

- 主用设备 MAC 地址：12_插槽.port_subid.contextid 的值。
- 备用设备 MAC 地址：02_插槽.port_subid.contextid 的值。

对于没有接口插槽的平台，插槽始终为 0。端口是接口端口。subid 是子接口的内部 ID，不可见。contextid 是情景的内部 ID，可使用 **showcontextdetail** 命令查看。例如，ID 为 1 的情景中的接口 GigabitEthernet 0/1.200 具有以下生成的 MAC 地址，其中子接口 200 的内部 ID 为 31：

- 主用号码：1200.0131.0001
- 备用：0200.0131.0001

此 MAC 地址生成方法不允许在重新加载之间使用永久 MAC 地址，不允许在同一网段上有多个 ASA（因为不能保证 MAC 地址唯一），并且不会防止与手动分配的 MAC 地址重叠。我们建议在生成 MAC 地址时使用前缀来避免这些问题。

当生成 MAC 地址时

当你在上下文 **nameif** 中为接口配置命令时，新的 MAC 地址会立即生成。如果在配置上下文接口后启用此命令，则输入该命令后会立即为所有接口生成 MAC 地址。如果使用该命令 **no mac-address auto**，每个接口的 MAC 地址将恢复为默认 MAC 地址。例如，GigabitEthernet 0/1 的子接口恢复为使用 GigabitEthernet 0/1 的 MAC 地址。

使用其他方法设置 MAC 地址

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

在系统配置中查看 MAC 地址

要从系统执行空间查看分配的 MAC 地址，请输入 **show running-config all context** 命令。

需要该 **all** 选项才能查看分配的 MAC 地址。虽然此命令仅在全局配置模式下可由用户配置，但该命令在 **mac-address auto** 每个上下文的配置中与分配的 MAC 地址一起显示为只读条目。仅使用上下文中的命令 **nameif** 配置的已分配接口才会分配 MAC 地址。



注释 如果您手动向接口分配 MAC 地址，但也启用了自动生成，则自动生成的地址会继续显示在配置中，即使正在使用的是手动 MAC 地址也如此。如果随后删除手动 MAC 地址，则会使用所显示的自动生成的地址。

查看上下文中的 MAC 地址

要查看上下文中每个接口使用的 MAC 地址，请输入 **show interface | include (Interface) | (MAC)** 命令。



注释 该命令显示 **showinterface** 正在使用的 MAC 地址；如果您手动分配 MAC 地址并启用自动生成，那么您只能从系统配置中查看未使用的自动生成的地址。

CR_Examples

以下示例启用自动 MAC 地址生成，前缀为 78：

```
ciscoasa(config)# mac-address auto prefix 78
```

该命令的以下输出显示了分配给 Management0/0 接口的 **showrunning-configallcontextadmin** 主 MAC 地址和备用 MAC 地址：

```
ciscoasa# show running-config all context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

该命令的以下输出显示 **showrunning-configallcontext** 示了所有上下文接口的所有 MAC 地址（主 MAC 地址和备用 MAC 地址）。请注意，由于 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口未在上下文中使用命令 **nameif** 进行配置，因此没有为它们生成 MAC 地址。

```
ciscoasa# show running-config all context
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!
context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!
context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
```

```
config-url disk0:/CTX2.cfg
!
```

Related Commands

命令	说明
failovermacaddress	主用/备用故障转移的物理接口的主用和备用 MAC 地址。
macaddress	主用/主用故障转移的物理接口的主用和备用 MAC 地址。
mac-address	为物理接口或子接口手动设置 MAC 地址（主用和备用）。在多情景模式下，您可以为同一接口在每个情景中设置不同的 MAC 地址。
mode	将安全上下文模式设置为多重或单一。
showinterface	显示接口特征，包括 MAC 地址。

mac-address pool

要添加 MAC 地址池以用于 ASA 集群中的单个接口，请在全局配置模式下使用 **mac-addresspool** 命令。要删除未使用的池，请使用此命令 **no** 的形式。

mac-address pool*name**start_mac_address - end_mac_address*
no mac-address pool*name* [*start_mac_address - end_mac_address*]

Syntax Description

<i>name</i>	为池命名，长度最大为 63 个字符。
<i>start_mac_address</i> <i>-end_mac_address</i>	指定第一个 MAC 地址和最后一个 MAC 地址。请注意在短划线 (-) 两侧添加一个空格。

Command Default

无默认为行为或值。

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	—	• 是

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

您可以在接口配置模式下的 **mac-addresscluster-pool** 命令中使用该池。为接口手动配置 MAC 地址并不常见，但如果您有特殊需求，则此池用于为每个接口分配唯一的 MAC 地址。

CR_Examples

以下示例添加具有 8 个 MAC 地址的 MAC 地址池，并将其分配给千兆以太网 0/0 接口：

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

Related Commands

命令	说明
interface	配置接口。
mac-address	为接口配置 MAC 地址。

mac-address-table aging-time

要设置 MAC 地址表条目的超时，请在 **mac-address-tableaging-time** 全局配置模式下使用 **命令**。要恢复默认值5分钟，请使用此命 **no**令的形式。

mac-address-tableaging-time*timeout_value*
no mac-address-table aging-time

Syntax Description	<i>timeout_value</i> MAC 地址条目超时之前在 MAC 地址表中停留的时间，该值介于 5 到 720 分钟（12 小时）之间。默认值为 5 分钟。

Command Default	默认超时是 5 分钟。

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。
	9.7(1) 使用集成路由和桥接时，现在可以在路由模式下配置此命令。

使用指南 没有使用指南。

CR_Examples 以下示例将 MAC 地址超时设置为 10 分钟：

```
ciscoasa(config)# mac-address-timeout aging time 10
```

Related Commands	命令	说明
	arp-inspection	启用 ARP 检测，即将 ARP 数据包与静态 ARP 条目进行比较。
	firewalltransparent	将防火墙模式设置为透明。
	mac-address-tablestatic	将静态 MAC 地址条目添加到 MAC 地址表。
	mac-learn	禁用 MAC 地址学习。

命令	说明
showmac-address-table	显示 MAC 地址表，包括动态和静态条目。

mac-address-table static

要将静态条目添加到 MAC 地址表，请在全局配置模式下使用 **mac-address-table static** 命令。要删除静态条目，请使用此命令的形式。通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。如有必要，可以将静态 MAC 地址添加到 MAC 地址表中。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果具有与静态条目相同 MAC 地址的客户端尝试将流量发送到与静态条目不匹配的接口，则 ASA 会丢弃该流量并生成系统消息。

mac-address-table static*interface_name**mac_address*
no mac-address-table static*interface_name**mac_address*

Syntax Description	<i>interface_name</i> 源桥组成员接口。
	<i>mac_address</i> 您希望添加至此表的 MAC 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
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。
	9.7(1) 使用集成路由和桥接时，现在可以在路由模式下配置此命令。

CR_Examples 以下示例将一个静态 MAC 地址条目添加到 MAC 地址表：

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

命令	说明
arp	添加一个静态 ARP 条目。
firewalltransparent	将防火墙模式设置为透明。
mac-address-tableaging-time	设置动态 MAC 地址条目的超时。

命令	说明
mac-learn	禁用 MAC 地址学习。
showmac-address-table	显示 MAC 地址表条目。

mac-learn disable

要禁用接口的 MAC 地址获悉，请在全局配置模式下使用 **mac-learn**命令。要重新启用 MAC 地址学习，请使用此命 **no**令的形式。默认情况下，每个接口都会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加至 MAC 地址表。您可以根据需要禁用 MAC 地址获悉。

mac-learn*interface_name***disable**
no mac-learn*interface_name*

Syntax Description	<i>interface_name</i> 要在其上禁用 MAC 学习的桥接组成员接口。
	disable 禁用 MAC 学习。

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	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.7(1) 使用集成路由和桥接时，现在可以在路由模式下配置此命令。

CR_Examples 以下示例在外部接口上禁用 MAC 获悉：

```
ciscoasa(config)# mac-learn outside disable
```

Related Commands	命令	说明
	clearconfiguremac-learn	将 mac-learn 配置设置为默认值。
	firewalltransparent	将防火墙模式设置为透明。
	mac-address-tablestatic	将静态 MAC 地址条目添加到 MAC 地址表。
	showmac-address-table	显示 MAC 地址表，包括动态和静态条目。

命令	说明
showrunning-configmac-learn	显示 mac-learn 配置。

mac-learn 泛洪

要启用针对非 IPv4/IPv6 数据包的未知 MAC 地址泛洪，请在全局配置模式下使用 **mac-learn flood** 命令。要禁用 MAC 地址泛洪，请使用此命令的形式。

mac-learn flood
no mac-learn flood

Command Default 已禁用泛洪。

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
9.7(1)	添加了此命令。

CR_Examples

以下示例启用 MAC 泛洪：

```
ciscoasa(config)# mac-learn flood
```

命令	说明
clearconfiguremac-learn	将 mac-learn 配置设置为默认值。
mac-address-tablestatic	将静态 MAC 地址条目添加到 MAC 地址表。
showmac-address-table	显示 MAC 地址表，包括动态和静态条目。
showrunning-configmac-learn	显示 mac-learn 配置。

mac-list

如要指定用于使 MAC 地址豁免身份验证和/或授权的 MAC 地址列表，请在全局配置模式下使用 **mac-list** 命令。要删除 MAC 列表条目，请使用此命令 **no** 的形式。

```
mac-list id { deny | permit } mac macmask
no mac-list id { deny | permit } mac macmask
```

Syntax Description

deny	如果在 aaamac-exempt 命令中指定流量，则表示匹配此 MAC 地址的流量不匹配 MAC 列表，并且应同时接受身份验证和授权。如果使用 MAC 地址掩码（例如，ffff.ffff.0000）允许一系列 MAC 地址，并且要强制该范围内的一个 MAC 地址进行身份验证和授权，您可能需要在 MAC 列表中添加拒绝条目。
ID	指定十六进制 MAC 访问列表号。要将一组 MAC 地址分组，请根据需要多次使用相同的 ID 值输入 mac-list 命令。条目的顺序很重要，因为数据包使用它匹配的第一个条目，而不是最佳匹配场景。如果有一个 permit 条目，但想要拒绝 permit 条目允许的地址，请务必在 permit 条目之前输入 deny 条目。
mac	指定 12 位十六进制形式的源 MAC 地址；即 nnnn.nnnn.nnnn
macmask	指定应该用于匹配的 MAC 地址部分。例如，ffff.ffff.ffff 与 MAC 地址完全匹配。ffff.ffff.0000 仅匹配前 8 位数。
permit	表示匹配此 MAC 地址的流量与 MAC 列表匹配，并且在 aaamac-exempt 命令中指定该流量时可免除身份验证和授权。

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

7.0(1) 添加了此命令。

使用指南

要启用 MAC 地址豁免执行身份验证和授权，请使用 **aaamac-exempt** 命令。您仅可以添加 **aaamac-exempt** 命令的一个实例，因此请确保您的 MAC 列表包括要豁免的所有 MAC 地址。您可以创建多个 MAC 列表，但一次只能使用一个。

CR_Examples

以下示例绕过单个 MAC 地址的身份验证：

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

以下条目绕过硬件 ID 为 0003.E3 的所有思科 IP 电话的身份验证：

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

以下示例绕过对除 00a0.c95d.02b2 之外的一组 MAC 地址的身份验证。将 **deny** 语句输入 **permit** 语句之前，因为 00a0.c95d.02b2 也匹配 **permit** 语句，如果它放在最前面，则永远不会匹配 **deny** 语句。

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

Related Commands

命令	说明
aaaauthentication	启用用户身份验证。
aaaauthorization	启用用户授权服务。
aaamac-exempt	豁免 MAC 地址列表的身份验证和授权。
clearconfiguremac-list	删除先前由 mac-list 命令指定的 MAC 地址列表。
showrunning-configmac-list	显示先前在 mac-list 命令中指定的 MAC 地址列表。

mail-relay

要配置本地域名，请在参数配置模式下使用 **mail-relay** 命令。要禁用此功能，请使用此 **no** 命令的形式。

```
mail-relay domain_name action { drop-connection | log }
no mail-relay domain_name action { drop-connection | log }
```

Syntax Description

domain_name 域名。

drop-connection 关闭连接。

log 生成系统日志消息。

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

以下示例显示如何为特定域配置邮件中继：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

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

management-access

要允许在使用 VPN 时对进入 ASA 的接口以外的接口进行管理访问，请在 **management-access** 全局配置模式下使用该命令。要禁用管理访问，请使用此命令 **no** 的形式。

management-access 管理接口

no management-access 管理接口

Syntax Description

管理接 指定从另一个接口进入 ASA 时想要访问的管理接口的名称。可以指定物理或虚拟接口。
口

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	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。
9.9(2)	现在，可以指定虚拟接口。
9.14(1)	SNMP 不再受支持。
9.17(1)	如果您使用 CiscoSSH 堆栈（命令 ssh stack ciscossh ），则 SSH 不支持此功能。

使用指南

此命令允许您连接到除使用完整隧道 IPsec VPN 或 SSL VPN 客户端（AnyConnect 2.x 客户端、SVC 1.x）时或跨站点间 IPsec 进入 ASA 的接口以外的接口。隧道。您可以使用 Telnet、SSH、Ping 或 ASDM 连接至 ASA 接口。您还可以使用管理访问接口作为通过 VPN 隧道发送的系统日志消息的源接口。

只能定义一个管理访问接口。

在 9.5(1) 及更高版本中，由于使用单独的管理和数据路由表进行路由考虑，VPN 终止接口和管理访问接口需要是同一类型：两者都需要是仅管理接口或常规数据接口。因此，请勿在仅管理接口上配置管理访问，除非在极少数情况下 VPN 终端接口会仅用于管理。

如果您使用 CiscoSSH 堆栈（命 **ssh stack ciscossh** 令），则 SSH 不支持此功能。

9.14(1) 及更高版本的 SNMP 不支持此功能。对于 VPN 上的 SNMP，我们建议在 9.18(2) 及更高版本中的环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。

在管理访问接口网络和 VPN 网络之间使用身份 NAT（VPN 流量的常见 NAT 配置）时，必须指定 **natroute-lookup** 命令。如果没有路由查找，ASA 就会将流量从命令中指定的 **nat** 接口发送出去，而不管路由表的内容是什么。例如，配置 **management-accessinside**，以便在外部输入的 VPN 用户可以管理内部接口。如果 **identity nat** 命令指定 (**inside,outside**)，则您不希望 ASA 将管理流量发送到内部网络；它将永远不会返回内部接口 IP 地址。路由查询选项允许 ASA 将流量直接发送到内部接口 IP 地址，而不是流入内部网络。对于从 VPN 客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。

CR_Examples

以下示例显示如何将名为 inside 的防火墙接口配置为管理访问接口：

```
ciscoasa(config)# management-access inside
```

Related Commands

命令	说明
clearconfiguremanagement-access	为 ASA 的管理访问删除内部接口的配置。
showmanagement-access	显示为管理访问配置的内部接口的名称。

management-only

要将接口设置为仅接受管理流量，请在 **management-only** 接口配置模式下使用该命令。要允许通过流量，请使用此命令的 **no** 形式。

management-only [**individual**]

no management-only [**individual**]

Syntax Description

individual 对于 Firepower 9300 ASA 安全模块集群，您必须在跨区接口模式下为管理接口指定 **individual** 关键字。

Command Default

管理 是否 适用接口（如果适用） 默认情况下将设置为管理专用模式。

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	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 运行配置中此命令的位置已移至接口部分的顶部，以支持 ASA 集群，其中对管理接口有特殊豁免。

9.4(1.152) 添加了 **individual** 关键字。

使用指南

大多数型号包含一个名为 管理 *n/n* 的专用管理接口，用于支持流向 ASA 的流量。但是，您可以使用该 **management-only** 命令将任何接口配置为仅管理接口。



注释 对于除 ASA 5585-X 之外的所有型号，您无法禁用管理接口的仅管理模式默认情况下，此命令始终处于启用状态。EXTENSI

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口（物理接口、子接口[如果所用的型号支持]或由管理接口组成的 EtherChannel 接口[如果有多个管理接口]）用作单独的管理接口。您不能将任何其他接口类型用作管理接口。

如果您的模型不包含管理接口，则必须从数据接口管理透明防火墙。

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要为每个情景提供管理，您可以创建管理接口的子接口，然后向每个情景分配管理子接口。请注意，除 ASA 5585-X 外，管理接口不允许子接口，因此对于每个上下文管理，您必须连接到数据接口。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

CR_Examples

以下示例禁用管理接口上的仅管理模式：

```
ciscoasa(config)# interface management0/0
ciscoasa(config-if)# no management-only
```

以下示例在子接口上启用仅管理模式：

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# management-only
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。

map-domain

要配置映射地址和端口 (MAP) 域，请在全局配置模式下使用 **map-domain** 命令。使用此 **no** 命令的形式删除 MAP 域。

map-domain*name*
no map-domain*name*

Syntax Description

name MAP 域的名称，是最多 48 个字符的字母数字字符串。该名称还可以包含以下特殊字符：句点 (.)、斜线 (/) 和冒号 (:)。

Command Default

无默认值。

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
全局配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改

9.13(1)	引入了此命令。

使用指南

映射地址和端口（映射）主要是在服务提供商（SP）网络中使用的一项功能。服务提供商可以运行 IPv6 网络、映射域，同时支持 IPv4 用户，以及与公共互联网上的 IPv4 站点通信的需要。映射在 RFC7597、RFC7598 和 RFC7599 中定义。

对于 MAP 域内的服务提供商来说，MAP 相对于 NAT46 的优势在于，用 IPv6 地址替换用户的 IPv4 地址（在 SP 网络边缘再返回到 IPv4）是无状态的。与 NAT46 相比，这提高了 SP 网络的效率。

有两种 MAP 技术：MAP 转换 (MAP-T) 和 MAP 封装 (MAP-E)。ASA 支持 MAP-T；不支持 MAP-E。

要配置 MAP-T，您需要创建一个或多个域。在客户边缘 (CE) 和边界中继 (BR) 设备上配置 MAP-T 时，请确保将参与每个域的每台设备使用相同的参数。

您最多可以配置 25 个 MAP-T 域。在多情景模式下，您最多可以在每个情景中配置 25 个域。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1
```

```
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024

ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

map-name

要将用户定义的属性名称映射到思科属性名称，请在 `ldap-attribute-map` 配置模式下使用 **map-name** 命令。

要删除此映射，请使用此命令的形式。

map-name *user-attribute-name* *Cisco-attribute-name*
no **map-name** *user-attribute-name* *Cisco-attribute-name*

Syntax Description

user-attribute-name 指定要映射到思科属性的用户定义属性的名称。

Cisco-attribute-name 指定映射至用户定义名称的思科属性名称。

Command Default

默认情况下，不存在名称映射。

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
ldap-attribute-map 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

通过 **map-name** 命令，您可以将自己的属性名称映射到思科属性名称。然后，可以将生成的属性映射绑定到 LDAP 服务器。通常的步骤包括：

1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令将进入 `ldap-attribute-map` 配置模式。
2. 在 `ldap-attribute-map` 配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 `aaa-server` 主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。请注意此命令中“ldap”后面的连字符。



注释 要正确使用属性映射功能，您需要了解 Cisco LDAP 属性名称和值以及用户定义的属性名称和值。

CR_Examples

以下示例命令将用户定义的属性名称 Hours 映射到 LDAP 属性映射 myldapmap 中的思科属性名称 cVPN3000-Access-Hours:

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
ciscoasa(config-ldap-attribute-map)#
```

在 ldap-attribute-map 配置模式下，您可以输入 “?” 显示思科 LDAP 属性名称的完整列表:

```
ciscoasa(config-ldap-attribute-map)# map-name <name>
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
  :
  :
  cVPN3000-X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map(aaa-serverhostmode)	将 LDAP 属性映射绑定到 LDAP 服务器。
map-value	将用户定义的属性值映射到思科属性。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射或所有运行属性映射。
clearconfigureldapattribute-map	删除所有 LDAP 属性映射。

mapping-service (已弃用)

要为 Cisco Intercompany Media Engine 代理配置映射服务，请使用 UC-IME 配置模式下的 **mapping-service** 命令。要从代理中删除映射服务，请使用此命令的 **no** 形式。

mapping-service **listening-interface** 接口 [**listening-port** 端口] **uc-ime-interface** 接口
no **mapping-service** **listening-interface** 接口 [**listening-port** 端口] **uc-ime-interface** 接口

Syntax Description

interface	指定要用于侦听接口或 uc-ime 接口的接口的名称。
listening-interface	配置 ASA 用来侦听映射请求的接口。
listening-port	(可选) 配置映射服务的侦听端口。
port	(可选) 指定 ASA 侦听映射请求的 TCP 端口号。端口号必须为 1024 或更高版本，以避免与设备上的其他服务（例如 Telnet 或 SSH）冲突。默认情况下，端口号为 TCP 8060。
uc-ime-interface	配置连接到远程 Cisco UCM 的接口。

Command Default

默认情况下，思科公司间媒体引擎代理的路径外部部署的映射服务侦听 TCP 端口 8060。

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
UC-IME 配置	• 是	—	• 是	—	—

Command History

版本 修改

8.3(1) 添加了此命令。

9.4(1) 此命令与所 **uc-ime** 有模式命令一起已被弃用。

使用指南

对于 ASA 上思科公司间媒体引擎代理的路径外部部署，会将映射服务添加到代理配置。要配置映射服务，必须指定侦听映射请求的外部接口（远程企业端）以及连接到远程思科 UCM 的接口。



注释 您只能为 Cisco Intercompany Media Engine 代理配置一个映射服务器。

为路径外部部署配置思科公司间媒体引擎代理时，您需要配置映射服务。

在关闭路径部署中，进站和出站思科公司间媒体引擎呼叫将通过启用了思科公司间媒体引擎代理的自适应安全设备。自适应安全设备位于 DMZ 中，并配置为主要支持思科公司间媒体引擎。正常的面向互联网的流量不会流经此 ASA。

对于所有进站呼叫，信令将定向至 ASA，因为有目的思科 UCM 是使用 ASA 上的全局 IP 地址进行配置的。对于出站呼叫，被叫方可以是互联网上的任何 IP 地址；因此，ASA 配置了映射服务，以便在 ASA 上为互联网上被叫方的每个全局 IP 地址动态提供内部 IP 地址。

思科 UCM 将所有出站呼叫直接发送到自适应安全设备上的映射内部 IP 地址，而不是被叫方在互联网上的全局 IP 地址。然后，ASA 将呼叫转发至被叫方的全局 IP 地址。

CR_Examples

以下示例显示...:

```
ciscoasa
(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
uc-ime-interface outside
```

Related Commands

命令	说明
showrunning-configuc-ime	显示思科公司间媒体引擎代理的运行中配置。
showuc-ime	显示有关回退通知、映射服务会话和信令会话的统计数据或详细信息。
uc-ime	在 ASA 上创建 Cisco Intercompany Media Engine 代理实例。

map-value

要将用户定义的值映射到思科 LDAP 值，请在 `ldap-attribute-map` 配置模式下使用 **map-value** 命令。要删除映射中的条目，请使用此命令的 **no** 形式。

map-value *user-attribute-name user-value-string Cisco-value-string*
no **map-value** *user-attribute-name user-value-string Cisco-value-string*

Syntax Description

思科值字符串	为思科属性指定思科值字符串。
user-attribute-name	指定要映射到思科属性名称的用户定义属性名称。
用户值字符串	指定要映射到思科属性值的用户定义值字符串。

Command Default

默认情况下，没有映射到思科属性的用户定义值。

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
ldap-attribute-map 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

通过 **map-value** 命令，您可以将自己的属性值映射到思科属性名称和值。然后，可以将生成的属性映射绑定到 LDAP 服务器。通常的步骤包括：

1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令将进入 `ldap-attribute-map` 配置模式。
2. 在 `ldap-attribute-map` 配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 `aaa-server` 主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。请注意此命令中“ldap”后面的连字符。



注释 要正确使用属性映射功能，您需要了解 Cisco LDAP 属性名称和值以及用户定义的属性名称和值。

CR_Examples

以下示例在 ldap-attribute-map 配置模式下输入，将用户属性 Hours 的用户定义值设置为名为 workDay 的用户定义时间策略和思科定义的名为 Daytime 的时间策略：

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map(aaa-serverhostmode)	将 LDAP 属性映射绑定到 LDAP 服务器。
map-name	将用户定义的 LDAP 属性名称与思科 LDAP 属性名称映射。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射或所有运行属性映射。
clearconfigureldapattribute-map	删除所有 LDAP 映射。

mask

使用模块化策略框架时，通过在匹配或类配置模式下使用 **match** 命令掩蔽与 **mask** 命令或类映射匹配的数据包部分。此掩码操作在用于应用流量的检测策略映射（使用 **policy-map type inspect** 命令）中可用；但是，并非所有应用都允许此操作。例如，您可以使用 **mask** 命令进行 DNS 应用检测，以便在允许流量通过 ASA 之前掩蔽报头标志。要禁用此操作，请使用此命令的 **no** 形式。

mask [**log**]
nomask [**log**]

Syntax Description **lg** 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-map type inspect** 命令，该命令转而包含 **match** 命令），可以输入 **mask** 命令来掩蔽匹配的部分数据包使用 **match** 命令或 **class** 命令。

在第 3/4 层策略映射（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，输入 **inspect dns dns_policy_map** 命令，其中 **dns_policy_map** 是检测策略映射的名称。

CR_Examples

以下示例在允许流量通过 ASA 之前掩蔽 DNS 报头中的 RD 和 RA 标志的示例：

```
ciscoasa(config-cmap)# policy-map type inspect dns dns-map1
ciscoasa(config-pmap-c)# match header-flag RD
ciscoasa(config-pmap-c)# mask log
ciscoasa(config-pmap-c)# match header-flag RA
ciscoasa(config-pmap-c)# mask log
```

Related Commands

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

mask-banner

要模糊服务器横幅，请在参数配置模式下使用 **mask-banner** 命令。要禁用此功能，请使用此 **no** 命令的形式。

mask-banner
no mask-banner

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为行为或值。

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

以下示例显示如何屏蔽服务器横幅：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

Related Commands

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

mask-syst-reply

要对客户端隐藏 FTP 服务器响应，请在 FTP 映射配置模式下使用 **mask-syst-reply** 命令。通过使用 **ftp-map** 命令可以进入该模式。要删除配置，请使用此命令的 no 形式。

mask-syst-reply
no mask-syst-reply

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下会启用此命令。

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 与严格 FTP 检测配合使用 **mask-syst-reply** 命令可保护 FTP 服务器系统免受客户端侵害。启用此命令后，服务器对 **syst** 命令的应答将替换为一串 X。

CR_Examples 以下示例导致 ASA 将 FTP 服务器对 **syst** 命令的应答替换为 X：

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

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。
policy-map	将类映射与特定的安全操作相关联。
request-commanddeny	指定要禁止的 FTP 命令。

match access-list

当使用模块化策略框架时，通过在类映射配置模式下使用 **matchaccess-list** 命令，使用访问列表来标识要应用操作的流量。要删除该 **matchaccess-list** 命令，请使用此 **no** 命令的形式。

```
match access-listaccess_list_name
no match access-listaccess_list_name
```

Syntax Description *access_list_name* 指定用作匹配条件的访问列表的名称。

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
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。

使用指南 配置模块化策略框架包括四项任务：

- 1. 标识要使用**class-map** 命令应用操作的第 3 层和第 4 层流量。

输入 **class-map** 命令后，您可以输入 **matchaccess-list**命令来标识流量。或者，您也可以输入其他类型的 **match** 命令，例如**matchport** 命令。类映射中只能包含一个 **matchaccess-list**命令，且不能将其与其他类型的 **match** 命令组合使用。例外情况是，如果您定义 **matchdefault-inspection-traffic**命令匹配 ASA 可检测的所有应用使用的默认 TCP 和 UDP 端口，则可以使用 **matchaccess-list**命令缩小要匹配的流量。由于该命令指定了要匹配的端口，因此 **matchdefault-inspection-traffic** 访问列表中的任何端口都将被忽略。

- 1. （仅限应用检测）使用 **policy-maptypesinspect** 命令定义应用检测流量的特殊操作。
- 2. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
- 3. 使用 **service-policy** 命令在接口上激活这些操作。

CR_Examples 以下示例创建与三个访问列表匹配的三个第 3/4 层类映射：

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp
ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp
ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match any

使用模块化策略框架时，请在类映射配置模式下使用 **matchany** 命令匹配要应用操作的所有流量。要删除该 **matchany** 命令，请使用此命令的形式。

match any
no match any

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
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。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用 **class-map** 命令应用操作的第 3 层和第 4 层流量。

输入 **class-map** 命令后，您可以输入 **matchany** 命令来标识所有流量。或者，您也可以输入其他类型的 **match** 命令，例如 **matchport** 命令。您不能将 **matchany** 命令与其他类型的 **match** 命令结合使用。

1. （仅限应用检测）使用 **policy-maptypeinspect** 命令定义应用检测流量的特殊操作。
2. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
3. 使用 **service-policy** 命令在接口上激活这些操作。

CR_Examples

此示例显示如何使用类映射和 **matchany** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchany
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchaccess-list	根据访问列表匹配流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match apn

如要配置 GTP 消息中的无线接入点名称匹配条件，请在策略映射配置模式下使用 **matchapn** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] apnregex { regex_name | classregex_class_name }
no match [not] apnregex [regex_name | classregex_class_name]
```

Syntax Description

<i>regex_name</i>	指定正则表达式。
class <i>regex_class_name</i>	指定正则表达式类映射。

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
策略映射配置	• 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

可以在 GTP 策略映射中配置此命令。

CR_Examples

以下示例显示如何为 GTP 检测策略映射中的无线接入点名称配置匹配条件：

```
ciscoasa(config-pmap)# match apn class gtp_regex_apn
```

Related Commands

命令	说明
inspectgtp	配置 GTP 流量检测。

match application-id

要配置 Diameter 消息的 Diameter 应用标识符的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchapplication-id** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] application-idapp_id [app_id_2]
no match [not] application-idapp_id [app_id_2]
```

Syntax Description *app_id* Diameter 应用程序名称或编号 (0-4294967295)。如果要匹配某个连续编号的应用范围，可以再添加一个 ID。您可以按应用名称或编号来定义范围，该范围将适用于第一个 ID 和第二个 ID 之间的所有编号。

Command Default Diameter 检测允许所有应用。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南 可以在 Diameter 检测类映射或策略映射中配置此命令。使用它可根据 Diameter 应用 ID 过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

这些应用会注册到 IANA。以下是支持的核心应用，但您可以对其他应用进行过滤。有关应用名称的列表，请参阅 CLI 帮助。

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0)。这是基础 Diameter 协议。

IETF 在 <http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml> 上列出了已注册的应用程序、命令代码和属性值对，但 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

CR_Examples

以下示例显示如何为 3gpp-s6a 和 3gpp-s13 应用 ID 配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-any log_app
ciscoasa(config-cmap)# match application-id 3gpp-s6a
ciscoasa(config-cmap)# match application-id 3gpp-s13
```

Related Commands

命令	说明
class-map type inspect	创建检查类别图。
inspect diameter	启用 Diameter 检测。
policy-map type inspect	创建检查策略映射。

match as-path

要匹配 BGP 自治系统路径访问列表，请在路由映射配置模式下使用 `match as-path` 命令。要删除路径列表条目，请使用此命令的 `no` 形式。

match as-path 路径列表编号
no match as-path 路径列表编号

Syntax Description	路径列表编号 自治系统路径访问列表编号。 号

Command Default	未定义任何路径列表。

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
路由图配置	• 是	—	• 是	• 支持	—

Command History	版本 修改
	92(1) 添加了此命令。

使用指南

`match as-path` 和 `set weight` 命令设置的值会覆盖全局值。例如，使用 `match as-path` 和 `set weight route-map` 配置命令分配的权重会覆盖使用 `neighbor weight` 命令分配的权重。

路由映射可包含多个部分。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。如果仅修改某些数据，则必须指定显式匹配项来配置第二个 `route-map` 部分。它可以接受多个 `path-list-name`。

CR_Examples

以下示例设置自治系统路径，以匹配 BGP 自治系统路径访问列表 `as-path-acl`：

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

Related Commands	命令	说明
	set-weight	指定路由表的 BGP 权重。

命令	说明
neighbor-weight	为邻居连接分配权重。

match avp

要为 Diameter 消息中的 Diameter 属性值对 (AVP) 配置匹配条件，请在类映射或策略映射配置模式下使用 **matchavp** 命令。要删除匹配条件，请使用此 **no**命令的形式。

要仅按属性匹配 AVP，请使用以下命令：

```
match [not] avpcode [code-2] [vendor-idid_number]
no match [not] avpcode [code-2] [vendor-idid_number]
```

要基于属性的值匹配 AVP，请使用以下命令：

```
match [not] avpcode [vendor-idid_number] value
no match [not] avpcode [vendor-idid_number] value
```

Syntax Description	code	属性值对的名称或编号（1-4294967295）。对于第一个代码，您可以指定自定义 AVP 的名称或已在 RFC 或 3GPP 技术规范中注册且受该软件直接支持的某个 AVP 的名称。如果要匹配 AVP 的范围，请仅按编号指定第二个代码。如果要按值匹配 AVP，则无法指定第二个代码。有关 AVP 名称的列表，请参阅 CLI 帮助。
	value	AVP 的值部分。只有 AVP 的数据类型受支持，才能配置此项目。例如，可以为具有地址数据类型的 AVP 指定 IP 地址。有关如何配置此参数的详细信息，请参阅下面的“使用”部分。
	vendor-idid_number	（可选。）也要一并匹配的供应商的 ID 编号，范围为 0-4294967295。例如，3GPP 供应商 ID 为 10415，IETF 为 0。

Command Default Diameter 检测允许所有 AVP。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.5(2) 添加了此命令。

使用指南

可以在 Diameter 检测类映射或策略映射中配置此命令。可用于根据 Diameter AVP 过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

使用 CLI 帮助获取 AVP 名称列表。IETF 在上有一个注册应用程序、命令代码和属性值对的列表 <https://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml>，尽管 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

如果您正在配置值匹配，以下是支持的数据类型的值选项的具体语法：

- Diameter Identity、Diameter URI、Octet String - 使用正则表达式或正则表达式类对象匹配这些数据类型。

{regexregex_name | classregex_class}

- Address - 指定要匹配的 IPv4 或 IPv6 地址。例如，10.100.10.10 或 2001:DB8::0DB8:800:200C:417A。
- Time - 指定开始和结束日期及时间。两者均为必填项目。时间采用 24 小时格式。

dateyearmonthdaytimehh:mm:ssdateyearmonthdaytimehh:mm:ss

例如：

date2015feb5time12:00:00date2015mar9time12:00:00

- Numeric - 指定编号的范围：

rangenumber_1number_2

有效的编号范围取决于数据类型：

- Integer32: -2147483647 到 2147483647
- Integer64: -9223372036854775807 到 9223372036854775807
- Unsigned32: 0 到 4294967295
- Unsigned64: 0 到 18446744073709551615
- Float32: 小数点表示方式，精度为 8 位数
- Float64: 小数点表示方式，精度为 16 位数

CR_Examples

以下示例显示如何为 host-ip-address AVP on Capability Exchange 请求/应答命令消息上显示的特定 IP 地址配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

命令	说明
class-map type inspect	创建检查类别图。
diameter	创建自定义属性-值对。
inspect diameter	启用 Diameter 检测。
policy-map type inspect	创建检查策略映射。

match body

要配置 ESMTP 消息正文消息的长度或行长度的匹配条件，请在类映射或策略映射配置模式下使用 **matchbody** 命令。要删除已配置的部分，请使用**no**此命令的形式。

match [**not**] **body** [**length** | **linelength**] **gt**字节
no match [**not**] **body** [**length** | **linelength**] **gt**字节

Syntax Description

length 指定 ESMTP 正文消息的长度。

线 指定 ESMTP 正文消息的行长度。
长

bytes 指定要匹配的数量（以字节为单位）。

Command Default

无默认为行为或值。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检查策略映射中配置正文行长度的匹配条件：

```
ciscoasa
(config)#
policy-map type inspect esmtp esmtp_map
ciscoasa (config-pmap)#matchbodylinelengthgt1000
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match called-party

要配置 H.323 被叫方的匹配条件，请在策略映射配置模式下使用 **matchcalled-party** 命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **called-party** [**regex***regex*]
no match [**not**] **match** [**not**] **called-party** [**regex***regex*]

Syntax Description

regex 指定匹配正则表达式。
regex

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例展示如何在 H.323 检测类映射中为被叫配置匹配条件：

```
ciscoasa(config-cmap)# match called-party regex caller1
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match calling-party

要配置 H.323 主叫方的匹配条件，请在策略映射配置模式下使用 **matchcalling-party** 命令。要禁用此功能，请使用此**no**命令的形式。

```
match [not] calling-party [regexregex]
nomatch [not] match [not] calling-party [regexregex]
```

Syntax Description	regex regex	指定匹配正则表达式。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.2(1) 添加了此命令。

CR_Examples	以下示例显示如何在 H.323 检测类映射中为主叫方配置匹配条件：

```
ciscoasa(config-cmap) # match calling-party regex caller1
```

Related Commands	命令	说明
	class-map	创建第 3/4 层类映射。
	clearconfigureclass-map	删除所有类映射。
	matchany	包括类映射中的所有流量。
	matchport	标识类映射中的特定端口号。
	showrunning-configclass-map	显示有关类映射配置的信息。

match certificate

要配置证书匹配规则，请在 `crypto ca trustpoint` 配置模式下使用 **matchcertificate** 命令。要从配置中删除规则，请使用此命令 **no** 的形式。

matchcertificate *map-name* [**overrideocsp** [*trustpointtrustpoint-name*] *seq-numurlURL*] | **overridecdp** *seq-numurlURL*]
nomatchcertificate *map-name* [**overrideocsp** [*seq-numurlURL*] | **overridecdp** [*seq-numurlURL*]]

Syntax Description

<i>map-name</i>	指定与此规则匹配的证书映射的名称。在配置匹配规则之前，必须配置证书映射。最大长度为 65 个字符。
覆盖 OSCP	指定该规则旨在覆盖证书中的 OSCP URL。
<i>seq-num</i>	设置此匹配规则的优先级。有效范围是 1 至 10000。ASA 首先评估具有最小序列号的匹配规则，然后评估序列号较大的匹配规则，直到找到匹配项。
信任点	（可选）指定使用信任点来验证 OSCP 响应方证书。
<i>trustpoint-name</i>	（可选）标识要与覆盖一起使用的信任点，以验证响应方证书。
<i>url</i>	指定访问 URL 获取 OSCP 吊销状态。
<i>URL</i>	标识用于访问 OSCP 吊销状态的 URL。
覆盖 cdp	指定规则的目的是覆盖证书中的 CRL URL。
<i>seq-num</i>	设置列表中每个 URL 的等级。指定 1 到 5 之间的值。ASA 首先尝试最低等级 (1) 的 URL。
<i>url</i>	指定访问 URL 获取 CRL 吊销状态。
<i>URL</i>	用于访问 CRL 吊销状态的 URL。

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
crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
9.13(1)	添加了用于配置 <code>cdp</code> 覆盖的调配。
9.15(1)	在此版本之前，静态 CDP 可以唯一地映射到正在验证的链中的每个证书。但是，每个证书仅支持一个此类映射。 在此版本中， <code>match certificate cdp override</code> 命令接受同一映射名称的多个实例。

使用指南

在 PKI 证书验证过程中，ASA 将通过使用 CRL 检查或在线证书状态协议 (OCSP) 来检查证书吊销状态以维护安全性。通过 CRL 检查，ASA 可以检索、解析和缓存 CRL，从而提供已撤销证书的完整列表。OCSP 提供了一种更具可扩展性的检查撤销状态的方法，因为 OCSP 将证书状态本地化在验证机构上，并查询特定证书的状态。

证书匹配规则允许您配置 OCSP URL 覆盖，即指定要检查撤销状态的 URL，而不是远程用户证书 AIA 字段中的 URL。通过匹配规则，您还可以配置用于验证 OCSP 响应方证书的信任点，这可以让 ASA 验证来自任何 CA 的响应方证书，包括自签名证书和客户端证书验证路径外部的证书。

与 OCSP 类似，您可以使用 `matchcertificate` 命令来配置 CDP URL 覆盖。此命令支持通过证书映射识别静态 CDP URL。对于需要 CRL 验证的每个证书，根据证书中的 CDP 扩展和此配置中映射的任何 URL 检索 CRL。在 `[ config-ca-crl` 子模式下，可以使用 `policy` 命令用于从证书或静态 CDP 中排除 CDP。

您现在可以将多个静态 CDP 配置到单个映射。要删除单个实例，请在命令的 `no` 形式中指定 URL 和序号。确保指定的 URL 和序列号与您配置的值相同。如果您未提及任何特定信息，则映射的所有条目都将被删除。具有或删除映射的多个实例的调配不适用于 OCSP。

配置 OCSP 时，请注意以下要求：

- 可在一个信任点配置中配置多个匹配规则，但每个 `crypto CA` 证书映射只能有一个匹配规则。但是，您可以配置多个加密 CA 证书映射，并将其与同一信任点关联。
- 在配置匹配规则之前，必须配置证书映射。
- 要配置信任点以验证自签名 OCSP 响应者证书，您需要将自签名响应者证书作为受信任的 CA 证书导入到其自己的信任点。然后，您在 `matchcertificate` 客户端证书验证信任点中配置命令，以使用包含自签名 OCSP 响应者证书的信任点来验证响应者证书。这同样适用于验证客户端证书验证路径之外的响应者证书。
- 如果同一 CA 颁发客户端证书和响应方证书，则信任点可以同时验证这两个证书。但是，如果不同的 CA 颁发客户端证书和响应方证书，则需要配置两个信任点，每个证书一个信任点。
- OCSP 服务器（响应者）证书通常会签署 OCSP 响应收到响应后，ASA 会尝试验证响应方证书。CA 通常会将其 OCSP 响应方证书的生命周期设置为相对较短的时间段，以将被破坏的几率降到最低。CA 通常还会在响应方证书中包含 `ocsp-no-check` 扩展，指示此证书不需要处于吊销状态正在检查。但如果此扩展不存在，ASA 会尝试使用信任点中指定的相同方法检查其撤销状态。如果响应者证书无法验证，则撤销检查失败。为了避免这种可能性，请在 `revocation-checknone` 配置响应方证书验证信任点时使用该命令，并在 `revocation-checkocsp` 配置客户端证书时使用该命令。

- 如果 ASA 未找到匹配项，它将使用 **ocspurl** 命令中指定的 URL。如果尚未配置 **ocspurl** 命令，ASA 将使用远程用户证书的 AIA 字段。如果证书没有 AIA 扩展，则吊销状态检查失败。

CR_Examples

以下示例显示如何为名为 **newtrust** 的信任点创建证书匹配规则。该规则有一个名为 **mymap** 的映射、序列号为 4、一个名为 **mytrust** 的信任点，并且指定了 URL 10.22.184.22。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
ciscoasa(config-ca-trustpoint)#
```

以下示例显示如何配置加密 CA 证书映射，然后配置匹配证书规则，以识别包含 CA 证书的信任点以验证响应方证书。如果 **newtrust** 信任点中识别的 CA 未颁发 OSCP 响应方证书，则需要此证书。

1. 配置标识映射规则应用到的客户端证书的证书映射。在本示例中，证书映射的名称是 **mymap**，序列号是 1。subject-name 的 CN 属性等于 mycert 的任何客户端证书都与 mymap 条目匹配。

```
ciscoasa(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)#
```

2. 配置包含用于验证 OSCP 响应方证书的 CA 证书的信任点。对于自签名证书，这是自签名证书本身，已导入且受本地信任。此外，您还可以通过外部 CA 注册获取用于此目的的证书。当系统提示您进行操作时，粘贴 CA 证书。

```
ciscoasa(config-ca-cert-map)# exit
ciscoasa(config)# crypto ca trustpoint mytrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBNjCCAQCcCBEPopG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMnJMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMnJMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHV
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsJl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCS0ihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJmluQX14wclPCCAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit

INFO: Certificate has the following attributes:
Fingerprint: 7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

3. 配置原始信任点 **newtrust**，使用 OSCP 作为吊销检查方法。然后，设置一个包含在步骤 2 中配置的证书映射 **mymap** 和自签名信任点 **mytrust** 的匹配规则。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate newtrust
```

```

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsJl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCS0ihb2NH6mga2eLqEsFPloVbBteSkEAm+NRCDK7udl13D6UC01EgkKJ81QtCk
AxQMnJMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHV
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZht761N+/8xGxC3DIVB8u7T/b
gQCS0ihb2NH6mga2eLqEsFPloVbBteSkEAm+NRCDK7udl13D6UC01EgkKJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJm1uQXl4wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEP0pG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMnJMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint: 9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust
4 url 10.22.184.22

```

使用 **newtrust** 信任点进行客户端证书身份验证的任何连接都会检查客户端证书，以确定客户端证书是否与 **mymap** 证书映射中指定的属性规则匹配。如果是，ASA 将访问 10.22.184.22 的 OCSF 响应方获取证书撤销状态，然后使用 **mytrust** 信任点验证响应方证书。



注释 **newtrust** 信任点配置为通过 OCSF 为客户端证书执行吊销检查。但是，会为默认吊销检查方法（无）配置 **mytrust** 信任点。因此，不会对 OCSF 响应方证书执行吊销检查。

以下示例显示使用 CDP 配置匹配证书规则。该规则有一个名为 **test** 的映射名称，1、2 和 3 分别为序号和静态 URL。为证书选择 CDP 时，ASA 会为与名为 **test** 的证书映射匹配的任何证书选择 3 个 CDP。如果 ASA 确定在验证证书时需要 CRL，将按给定顺序尝试 URL，直到成功检索到 CRL 为止。

```

ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 1 url http://1.1.1.1
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 2 url http://1.1.1.2
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 3 url http://1.1.1.3
ciscoasa(config-ca-trustpoint)#

```

Related Commands

命令	说明
crypto ca certificate map	创建加密 CA 证书映射。在全局配置模式下使用此命令。
cryptocatrustpoint	进入加密 ca 信任点配置模式。在全局配置模式下使用此命令。
ocspdisable-nonce	禁用 OCSF 请求的 nonce 扩展。
ocspurl	指定要用于检查与信任点关联的所有证书的 OCSF 服务器。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

匹配证书允许过期证书（已弃用）

要允许管理员豁免对某些证书进行过期检查，请在 `ca-trustpool` 配置模式下使用 `matchcertificateallowexpired-certificate` 命令。要禁用某些证书的豁免，请使用此命令的 `no` 形式。

match certificate<map>allow expired-certificate
no match certificate<map>allow expired-certificate

Syntax Description

allow 允许接受过期的证书。

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
CA-trustpool 配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

9.13(1) 此命令行已删除。

使用指南

`trustpool match` 命令利用证书映射对象为全局信任池策略配置证书特定的例外情况或覆盖。匹配规则是相对于正在验证的证书编写的。

Related Commands

命令	说明
<code>matchcertificateskiprevocationcheck</code>	豁免某些证书执行吊销检查。

match certificate skip revocation-check

要允许管理员免于对某些证书执行吊销检查，请在 `ca-trustpool` 配置模式下使用 `matchcertificateskiprevocation-check` 命令。要禁用吊销检查豁免，请使用此命令的 `no` 形式。

`matchcertificatemapskiprevocation-check`
`nomatchcertificatemapskiprevocation-check`

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
CA-trustpool 配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南 `trustpool match` 命令利用证书映射对象为全局信任池策略配置证书特定的例外情况或覆盖。匹配规则是相对于正在验证的证书编写的。

CR_Examples

以下示例显示跳过对使用者 DN 公用名称为 “mycompany123” 的证书的有效性检查。

```
crypto ca certificate map mycompany lsubject-name attr cn eq mycompany123crypto ca trustpool
policymatch certificate mycompany skip revocation-check
```

命令	说明
<code>matchcertificateallowexpired-certificate</code>	豁免对某些证书进行到期检查。

match cmd

要在 ESMTP 命令谓词上配置匹配条件，请在策略映射配置模式下使用 **matchcmd** 命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **cmd** [**verbverb** | **linelengthgtbytes** | **RCPTcountgtrecipients_number**]
no match [**not**] **cmd** [**verbverb** | **linelengthgtbytes** | **RCPTcountgtrecipients_number**]

Syntax Description

动词 动词	指定 ESMTP 命令谓词。
行长度 <i>gt</i> 字节	指定线的长度。
RCPT count <i>gtrecipients_number</i>	指定收件人邮件地址的数量。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检测策略映射中为 ESMTP 事务中交换的谓词（方法）NOOP 配置匹配条件：

```
ciscoasa(config-pmap) # match cmd verb NOOP
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match command-code

要为 Diameter 消息的 Diameter 命令代码配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **match command-code** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] command-code code [code_2]
no match [not] command-code code [code_2]
```

Syntax Description

code Diameter 命令代码名称或编号（0-4294967295）。如果要匹配某个连续编号的命令代码范围，可以再添加一个代码。您可以按命令代码名称或编号来定义范围，该范围将适用于第一个代码和第二个代码之间的所有编号。请参阅 CLI 帮助以获取命令代码名称列表。EXTEN

Command Default

Diameter 检测允许所有命令代码。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.5(2) 添加了此命令。

使用指南

可以在 Diameter 检测类映射或策略映射中配置此命令。使用它可根据 Diameter 命令代码过滤流量。然后，可以丢弃数据包、连接或记录匹配的流量。

IETF 在<http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml> 上列出了已注册的应用程序、命令代码和属性值对，但 Diameter 检查并不支持所有列出的项目。有关它们的技术规范，请参阅 3GPP 网站。

CR_Examples

以下示例显示如何为 host-ip-address AVP on Capability Exchange 请求/应答命令消息上显示的特定 IP 地址配置匹配条件。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

Related Commands

命令	说明
class-map type inspect	创建检查类别图。
inspect diameter	启用 Diameter 检测。
policy-map type inspect	创建检查策略映射。

match community

要匹配边界网关协议 (BGP) 社区，请在路由映射配置模式下使用 `match community` 命令。要从配置文件中删除 `match community` 命令并将系统恢复到软件删除 BGP 社区列表条目的默认状态，请使用此命令的 `no` 形式。

```
match community { standard-list-number | expanded-list-number | community-list-name [ exact ] }
no match community { standard-list-number | expanded-list-number | community-list-name [ exact ] }
```

Syntax Description	标准列表编号	指定从 1 到 99 的标准社区列表编号，用于标识一个或多个允许或拒绝社区组。
	扩展列表编号	指定从 100 到 500 的扩展社区列表编号，用于标识一个或多个允许或拒绝社区组
	community-list-name	社区列表名称。
	精确的	(可选) 表示需要完全匹配。所有社区以及仅指定社区必须存在。

Command Default 没有与路由映射匹配的社区列表。

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
路由图配置	• 是	—	• 是	• 支持	—

Command History	版本 修改
	92(1) 添加了此命令。

使用指南 路由映射可包含多个部分。任何与 `route-map` 命令相关的至少一个 `match` 命令不匹配的路由将被忽略；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。如果仅修改某些数据，则必须指定显式匹配项来配置第二个 `route-map` 部分。

基于社区列表编号的匹配是适用于 BGP 的一种匹配命令类型。

CR_Examples 以下示例显示匹配社区列表 1 的路由的权重设置为 100。社区值为 109 的任何路由的权重都会设置为 100。

```
ciscoasa(config)# community-list 1 permit 109
```

```
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1
ciscoasa(config-route-map)# set weight 100
```

以下示例显示匹配社区列表 1 的路由的权重设置为 200。只有社区为 109 的任何路由都会将权重设置为 200。

```
ciscoasa(config)# community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

在以下示例中，与社区列表 LIST_NAME 匹配的路由的权重将设置为 100。只有社区为 101 的任何路由都会将权重设置为 100。

```
ciscoasa(config)# community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

以下示例显示与扩展社区列表 500。具有扩展社区 1 的任何路由都将权重设置为 150。

```
ciscoasa(config)# community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

Related Commands

命令	说明
set-weight	指定路由表的 BGP 权重。
community-list	创建或配置 BGP 社区列表。

match default-inspection-traffic

如要为类映射中的 **inspect** 命令指定默认流量，请在 **class-map** 配置模式下使用 **matchdefault-inspection-traffic** 命令。要删除此规范，请使用此 **no** 命令的形式。

matchdefault-inspection-traffic
nomatchdefault-inspection-traffic

Syntax Description

此命令没有任何参数或关键字。

Command Default

有关每个检测的默认流量，请参阅使用指南部分。

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。

9.6(2) 为 DNS over TCP 检测添加了 TCP/53，默认情况下未启用该检测。还添加了 M3UA 和 STUN 的默认端口。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 **class-map** 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 **matchdefault-inspection-traffic** 命令，您可以匹配各个 **inspect** 命令的默认流量。

matchdefault-inspection-traffic 命令可与其他 **match** 命令结合使用，该命令通常是 **permitipsrc-ipdst-ip** 形式的访问列表。

将第二个 **match** 命令与 **matchdefault-inspection-traffic** 命令结合使用的规则是使用 **matchdefault-inspection-traffic** 命令指定协议和端口信息，使用第二个 **match** 命令指定所有其他信息（例如 IP 地址）。对于 **[match]** 命令，在第二个 **inspect** 命令中指定的任何协议或端口信息都将被忽略。

例如，下例中指定的端口 65535 将被忽略：

```

ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# match port 65535

```

用于检测的默认流量如下：

InspectionType	ProtocolType	SourcePort	DestinationPort
ctiqbe	tcp	不适用	2748
dcerpc	tcp	不适用	135
diameter	tcp、 sctp	不适用	3868
dns	udp, tcp	53	53
ftp	tcp	不适用	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	不适用	1720
h323 ras	udp	不适用	1718-1719
http	tcp	不适用	80
icmp	icmp	不适用	不适用
ils	tcp	不适用	389
im	tcp	不适用	1-65539
ip-options	rsvp	不适用	不适用
ipsec 直通	udp	不适用	500
m3ua	sctp	不适用	2905
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	不适用
radius-accounting	udp	不适用	1646
rpc	udp	111	111
rsh	tcp	不适用	514
rtsp	tcp	不适用	554
sctp	sctp	any	any
SIP	tcp, udp	不适用	5060

skinny	tcp	不适用	2000
smtp	tcp	不适用	25
sqlnet	tcp	不适用	1521
stun	tcp, udp	不适用	3478
tftp	udp	不适用	69
waas	tcp	不适用	1-65535
xdmcp	udp	177	177

CR_Examples

以下示例显示如何使用类映射和 **matchdefault-inspection-traffic** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchdefault-inspection-traffic
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match dns-class

要为 DNS 资源记录或“问题”部分中的域系统类配置匹配条件，请在类映射或策略映射配置模式下使用 **matchdns-class** 命令。要删除已配置的类，请使用此命令 **no** 的形式。

```
match [not] dns-class {eqc_well_known | c_val} {rangec_val1 c_val2}
no match [not] dns-class {eqc_well_known | c_val} {rangec_val1 c_val2}
```

Syntax Description	eq	指定精确匹配项。
	c_ware_known	按已知名称 IN 指定 DNS 类。
	c_val	在 DNS class 字段中指定任意值 (0-65535)。
	range	指定范围。
	c_val1 c_val2	指定范围匹配中的值。每个值介于 0 到 65535 之间。

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
类映射或策略映射配置	• 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 默认情况下，此命令检查 DNS 消息的所有字段（问题和 RR）并与指定的类匹配。DNS 查询和响应都会被检查。

使用以下两个命令可以将匹配范围缩小到 DNS 查询的问题部分：**match not header-flag QR** 和 **match question**。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何为 DNS 检测策略映射中的 DNS 类配置匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match dns-type

要为 DNS 类型（包括查询类型和 RR 类型）配置匹配条件，请在类映射或策略映射配置模式下使用 **matchdns-type** 命令。要删除已配置的 DNS 类型，请使用此命令的形式。

```
match [not] dns-type {eqt_well_known | t_val} {ranget_val1 t_val2}
no match [not] dns-type {eqt_well_known | t_val} {ranget_val1 t_val2}
```

Syntax Description	eq	指定精确匹配项。
	良好知悉	按已知名称指定 DNS 类型：A、NS、CNAME、SOA、TSIG、IXFR 或 AXFR。
	t_val	在 DNS 类型字段中指定任意值 (0-65535)。
	range	指定范围。
	t_val1 t_val2	指定范围匹配中的值。每个值介于 0 到 65535 之间。

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
类映射或策略映射配置	• 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 默认情况下，此命令检查 DNS 消息的所有部分（问题和 RR）并匹配指定的类型。DNS 查询和响应都会被检查。

使用以下两个命令可以将匹配范围缩小到 DNS 查询的问题部分：**match not header-flag QR** 和 **match question**。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何为 DNS 检测策略映射中的 DNS 类型配置匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match domain-name

要为 DNS 消息域名列表配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchdomain-name** 命令。要删除已配置的部分，请使用**no**此命令的形式。

```
match [not] domain-nameregexregex_id
match [not] domain-nameregexclassclass_id
no match [not] domain-nameregexregex_id
no match [not] domain-nameregexclassclass_id
```

Syntax Description	regex	指定正则表达式。
	regex_id	指定正则表达式ID。
	class	指定包含多个正则表达式条目的类映射。
	class_id	指定正则表达式类映射ID。

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
类映射或策略映射配置	• 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 此命令将 DNS 消息中的域名与预定义列表进行匹配。压缩域名将在匹配之前进行扩展。结合其他 DNS 匹配命令，可以将匹配条件缩小到某个特定字段。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何在 DNS 检查策略映射中匹配 DNS 域名：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match dpc

要为 M3UA 数据消息的目的点代码 (DPC) 配置匹配条件，请在策略映射配置模式下使用 **matchdpc** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] dpccode
no match [not] dpccode
```

Syntax Description *code* Zone -Region -sp 格式的目标点代码。

Command Default M3UA 检测允许所有目的点代码。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南 您可以在 M3UA 检测策略映射中配置此命令。可以根据目标点代码丢弃数据包。点代码采用 区域-地区 -sp 格式，其中每个元素的可能值取决于 SS7 变体。可以在策略映射中的 **ss7variant** 命令中定义变体。

- ITU - 点代码为 14 位，格式为 3-8-3。值范围为 [0-7]-[0-255]-[0-7]。这是默认的 SS7 变量。
- ANSI - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
- Japan - 点代码为 16 位，格式为 5-4-7。值范围为 [0-31]-[0-15]-[0-127]。
- China - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。

CR_Examples 以下示例显示如何为 ITU 配置特定目标点代码的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```


Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
matchopc	匹配 M3UA 始发点代码。
policy-maptypeinspect	创建检查策略映射。
ss7variant	标识要在策略映射中使用的 SS7 变量。

match dscp

要在类映射中标识 IETF 定义的 DSCP 值（在 IP 报头中），请在 `class-map` 配置模式下使用 `matchdscp` 命令。要删除此规范，请使用此 `no` 命令的形式。

```
matchdscp { values }
no match dscp { values }
```

Syntax Description `values` 在 IP 报头中指定最多八个不同的 IETF 定义的 DSCP 值。范围是 0 到 63。

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。

使用指南

`match` 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 `class-map` 全局配置命令定义流量类。在 `class-map` 配置模式下，可以使用 `match` 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 `match` 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 `matchdscp` 命令，可以匹配 IP 报头中 IETF 定义的 DSCP 值。

CR_Examples

以下示例显示如何使用类映射和 `matchdscp` 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchdscp af43 cs1 ef
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchport	指定 TCP/UDP 端口作为该接口上接收的数据包的比较条件。
showrunning-configclass-map	显示有关类映射配置的信息。



match e – match q

- [match ehlo-reply-parameter](#)，第 691 页
- [match filename](#)，第 693 页
- [match filetype](#)，第 695 页
- [match flow ip destination-address](#)，第 697 页
- [match header \(policy-map type inspect esmtp\)](#)，第 699 页
- [match header \(policy-map type inspect ipv6\)](#)，第 701 页
- [match header-flag](#)，第 703 页
- [match im-subscriber](#)，第 705 页
- [match interface](#)，第 707 页
- [match invalid-recipients](#)，第 709 页
- [match ip address](#)，第 711 页
- [match ip next-hop](#)，第 713 页
- [match ip route-source](#)，第 715 页
- [match ipv6 address](#)，第 717 页
- [match login-name](#)，第 719 页
- [match media-type](#)，第 721 页
- [match message class](#)，第 723 页
- [match message id](#)，第 725 页
- [match message length](#)，第 727 页
- [match message-path](#)，第 728 页
- [match metric](#)，第 730 页
- [match mime](#)，第 732 页
- [match msisdn](#)，第 734 页
- [match opc](#)，第 736 页
- [match peer-ip-address](#)，第 738 页
- [match peer-login-name](#)，第 740 页
- [match port](#)，第 741 页
- [match ppid](#)，第 743 页
- [匹配优先级](#)，第 745 页

- [match protocol](#) , 第 747 页
- [match question](#) , 第 748 页

match ehlo-reply-parameter

要在 ESMTP ehlo 应答参数上配置匹配条件，请在策略映射配置模式下使用 **match ehlo-reply-parameter** 命令。要禁用此功能，请使用此 **no** 命令的形式。

match [**not**] **ehlo-reply-parameter** *parameter*
no match [**not**] **ehlo-reply-parameter** *parameter*

Syntax Description

参 指定 ehlo 应答参数。
数

Command Default

无默认为行为或值。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检测策略映射中配置 ehlo 应答参数的匹配条件：

```
ciscoasa
(config)#
policy-map type inspect esmtp esmtp_map
ciscoasa (config-pmap)#matchehlo-reply-parameterauth
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clear configure class-map	删除所有类映射。
match any	包括类映射中的所有流量。
match port	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match filename

要为 FTP 传输配置文件名匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchfilename** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] filenameregex [regex_name | class regex_class_name]  
no match [not] filenameregex [regex_name | class regex_class_name]
```

Syntax Description

正则表达式名称	指定正则表达式。
<i>class</i> <i>regex_class_name</i>	指定正则表达式类映射。

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
类映射或策略映射配置	• 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

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在 FTP 检测类映射中配置 FTP 传输文件名的匹配条件：

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1  
ciscoasa(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing /root  
ciscoasa(config-cmap)# match username regex class ftp_regex_user  
ciscoasa(config-cmap)# match filename regex ftp-file
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match filetype

要为 FTP 传输的文件类型配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchfiletype** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

match [**not**] **filetyperegex** [*regex_name* | **classregex_class_name**]
no match [**not**] **filetyperegex** [*regex_name* | **classregex_class_name**]

Syntax Description

正则表达式名称	指定正则表达式。
<i>class</i> <i>regex_class_name</i>	指定正则表达式类映射。

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
类映射或策略映射配置	• 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

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在 FTP 检测策略映射中为 FTP 传输文件类型配置匹配条件：

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。

命令	说明
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match flow ip destination-address

如要在类映射中指定流 IP 目的地址，请在 class-map 配置模式下使用 **matchflowipdestination-address** 命令。要删除此规范，请使用此 **no**命令的形式。

matchflowipdestination-address
nomatchflowipdestination-address

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为行为或值。

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。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 **class-map** 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

要对隧道组启用基于流的策略操作，请将 **matchflowipdestination-address** 和 **matchtunnel-group** 命令与 **class-map**、**policy-map**和 **service-policy** 命令配合使用。定义流的条件是目的 IP 地址。所有流向某唯一 IP 目标地址的流量都被视为流。策略操作应用于每个数据流，而不是整个流量类。QoS 操作策略使用 **matchflowipdestination-address** 命令应用。使用**matchtunnel-group** 策略以指定隧道组内的每个隧道为指定速率。

CR_Examples

以下示例展示如何在隧道组内启用基于流的策略管制，并将每个隧道限制为指定的速率：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchtunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
```

```
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
showrunning-configclass-map	显示有关类映射配置的信息。
tunnel-group	创建并管理 VPN 连接特定记录的数据库。

match header (policy-map type inspect esmtp)

要配置 ESMTP 报头的匹配条件，请在 policy-map type inspect esmtp 配置模式下使用 **matchheader** 命令。要禁用此功能，请使用此 **no** 命令的形式。

```
match [not] header [ [length | linelength] gtbytes | to-fieldscountgtto_fields_number ]
no match [not] header [ [length | linelength] gtbytes | to-fieldscountgtto_fields_number ]
```

Syntax Description

length gt 个字节	指定为匹配 ESMTP 报头消息的长度。
行长度 gt 字节	指定匹配 ESMTP 报头消息的行长度。
目标字段数 (to-fields count gt to_fields_number)	指定匹配“收件人：”字段的数量。

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
Policy-map type inspect esmtp configuration	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何为 ESMTP 检测策略映射中的报头配置匹配条件：

```
ciscoasa
(config)#
  policy-map type inspect esmtp esmtp_map
ciscoasa (config-pmap)#matchheaderlengthgt512
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match header (policy-map type inspect ipv6)

要配置 IPv6 报头的匹配条件，请在 policy-map type inspect ipv6 配置模式下使用 **matchheader** 命令。
要禁用此功能，请使用此 **no** 命令的形式。

```
match[not]header{ah|countgtnumber|destination-option|esp|fragment|hop-by-hop|routing-addresscountgtnumber|routing-type{eq|range}number}
no
match[not]header{ah|countgtnumber|destination-option|esp|fragment|hop-by-hop|routing-addresscountgtnumber|routing-type{eq|range}number}
```

Syntax Description

ah	匹配 IPv6 身份验证扩展标头
countgtnumber	指定 IPv6 扩展头的最大数量，从 0 到 255。
destination-option	匹配 IPv6 目标选项扩展头。
esp	与 IPv6 封装安全有效负载 (ESP) 扩展头匹配。
fragment	匹配 IPv6 分片扩展头。
hop-by-hop	匹配 IPv6 逐跳扩展头。
not	(可选) 与指定参数不匹配。
routing-addresscountgtnumber	设置 IPv6 路由头类型 0 地址的最大数量，大于 0 到 255 之间的数字。
routing-type{eq range} number	匹配 IPv6 路由头类型，从 0 到 255。对于范围，用空格分隔值，例如。 3040

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
Policy-map type inspect ipv6 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.2(1) 添加了此命令。

使用指南

指定要匹配的报头。默认情况下，将对数据包进行日志记录 (**log**)；如果要丢弃（也可以选择记录）该数据包，请在匹配配置模式下输入 **drop** 和可选的 **log** 命令。

对要匹配的每个分机号重新输入 **match** 命令和可选的 **drop** 操作：

CR_Examples

以下示例创建一个检查策略映射，该策略映射将丢弃并记录所有具有逐跳、目标选项、路由地址和路由类型 0 标头的 IPv6 数据包：

```
policy-map type inspect ipv6 ipv6-pm
  parameters
    match header hop-by-hop
      drop log
    match header destination-option
      drop log
    match header routing-address count gt 0
      drop log
    match header routing-type eq 0
      drop log
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match header-flag

要为 DNS 报头配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchheader-flag** 命令。
要删除已配置的标头标志，请使用此命令的 **no**形式。

```
match [not] header-flag [eq] {f_well_known|f_value}  
no match [not] header-flag [eq] {f_well_known|f_value}
```

Syntax Description	eq指定精确匹配项。如果未配置，则指定 match-all 位掩码匹配项。
f_ware_known	按已知名称指定 DNS 报头标志位。可以输入多个标志位并进行逻辑“或”运算。 QR（查询，注意：QR=1，表示 DNS 响应） AA（权威应答） TC（截断） RD（期望递归） RA（可递归）
f_value	指定十六进制形式的任意 16 位值。

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
类映射或策略策略映射配置	• 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 可以在 DNS 类映射或策略映射中配置此命令。一个 DNS 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何为 DNS 检测策略映射中的 DNS 报头标志配置匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map  
ciscoasa(config-pmap)# match header-flag AA
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match im-subscriber

要为 SIP IM 用户配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchim-subscriber** 命令。要删除匹配条件，请使用此**no**命令的形式。

match [**not**] **im-subscriberregex** [*regex_name* | **class***regex_class_name*]
no match [**not**] **im-subscriberregex** [*regex_name* | **class***regex_class_name*]

Syntax Description

正则表达式名称	指定正则表达式。
<i>class</i> <i>regex_class_name</i>	指定正则表达式类映射。

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
类映射或策略映射配置	• 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

可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在 SIP 检测类映射中为 SIP IM 用户配置匹配条件：

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。

命令	说明
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match interface

若要分发使其下一跳离开其中一个指定接口的任何路由，请在路由映射配置模式下使用 **matchinterface** 命令。要删除匹配的接口条目，请使用此命令 **no** 的形式。

matchinterface *interface-name*
nomatchinterface *interface-name*

Syntax Description

interface-name 接口（而非物理接口）的名称。可以指定多个接口名称。

Command Default

未定义匹配接口。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

命令语法中的省略号 (...) 表示命令输入可以包含多个 **interface-type interface-number** 参数的值。

route-mapglobal 配置命令以及 **match** 和 **set** 配置命令允许您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 **match** 和 **set** 命令与其关联。**match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。**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。**noroute-map** 命令可删除路由映射。

matchroute-map 配置命令具有多种格式。您可以按任何顺序提供 **match** 命令。所有 **match** 命令都必须“通过”，才能根据通过 **set** 命令指定的 set 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。如果在 **match** 命令中指定了多个接口。则 **nomatchinterfaceinterface-name** 可用于删除单个接口。

路由映射可包含多个部分。任何与 **route-map** 命令相关的至少一个 **match** 子句不匹配的路由都将被忽略。如果仅修改某些数据，则必须配置第二个路由映射部分并指定显式匹配。

CR_Examples

以下示例显示对其下一跳在路由外部的路由进行分发：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

Related Commands

命令	说明
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
matchiproute-source	重新分配由访问列表指定的地址的路由器和访问服务器所通告的路由。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match invalid-recipients

要配置 ESMTTP 无效收件人地址的匹配条件，请在策略映射配置模式下使用 **matchinvalid-recipients** 命令。要禁用此功能，请使用此**no**命令的形式。

match [not] invalid-recipientscountgtnumber
nomatch [not] invalid-recipientscountgtnumber

Syntax Description

count gt number 指定匹配无效的收件人号码。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何在 ESMTTP 检测策略映射中为无效收件人计数配置匹配条件：

```
ciscoasa
(config)#
policy-map type inspect esmtp esmtp_map
ciscoasa (config-pmap)#matchinvalid-recipientscountgt1000
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match ip address

要重新分配具有由指定的访问列表之一传递的路由地址或匹配数据包的任何路由，请在 **match ip address** 路由映射配置模式下使用该命令。要恢复默认设置，请使用此命令的 **no** 形式。

```
match ip address {acl_id... | prefix-list prefix_list_id...}
no match ip address {acl_id... | prefix-list prefix_list_id...}
```

Syntax Description

acl_id 指定访问列表的名称。可以指定多个访问列表。

prefix-list ID 前缀列表 指定前缀列表的名称。可以指定多个前缀列表。
注释
不支持 OSPF。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

9.20(2) 对于 OSPF，不再支持前缀列表。

使用指南

该 **route-map** 命令和配 **match** 置命令允许您 **set** 定义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。每个 **route-map** 命令都有 **match** 和 **set** 命令与其关联。 **match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。 **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** 命令可删除路由映射。

CR Examples

以下示例显示如何重新分配内部路由：

```
ciscoasa(config)# route-map test
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由，
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
match ipv6 address	分配具有 IPv6 路由地址的任何路由或匹配由指定的访问列表之一传递的数据包。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match ip next-hop

要重新分发具有由一个指定的访问列表传递的下一跳路由器地址的任何路由，请在路由映射配置模式下使用 **matchipnext-hop** 命令。要删除下一跳条目，请使用此命令 **no** 的形式。

```
matchipnext-hop {acl . . .} | prefix-list prefix_list
no matchipnext-hop {acl . . .} | prefix-list prefix_list
```

Syntax Description

acl ACL 的名称。可以指定多个 ACL。

prefix-list prefix_list 前缀列表的名称。

Command Default

路由自由分发，无需匹配下一跳地址。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

命令语法中的省略号 (...) 指示命令输入可以包含多个 *acl* 参数值。

route-map global 配置命令以及 **match** 和 **set** 配置命令允许您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 **match** 和 **set** 命令与其关联。 **match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。 **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** 命令可删除路由映射。

match route-map 配置命令具有多种格式。您可以按任何顺序输入 **match** 命令。所有 **match** 命令都必须“通过”，才能根据 **set** 命令给定的 set 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。

通过路由映射传递路由时，路由映射可以有多个部分。任何与 **route-map** 命令相关的至少一个 **match** 子句不匹配的路由都将被忽略。要仅修改部分数据，您必须配置第二个路由映射部分并指定显式匹配。

CR_Examples

以下示例显示如何分发具有通过访问列表 `acl_dmz1` 或 `acl_dmz2` 传递的下一跳路由器地址的路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由。
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match ip route-source

要重新分发已由位于 ACL 指定的地址处的路由器和接入服务器通告的路由，请在 **route-map** 配置模式下使用 **matchiproute-source** 命令。要删除下一跳条目，请使用此命令的形式。

```
matchiproute-source {acl . . . } prefix-list prefix_list
matchiproute-source {acl . . . }
```

Syntax Description

acl ACL 的名称。可以指定多个 ACL。

prefix_list 前缀列表的名称。

Command Default

未对路由源进行过滤。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

命令语法中的省略号 (...) 指示命令输入可以包含多个 **access-list-name** 参数值。

route-mapglobal 配置命令以及 **match** 和 **set** 配置命令允许您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 **match** 和 **set** 命令与其关联。 **match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。 **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。 **noroute-map** 命令可删除路由映射。

matchroute-map 配置命令具有多种格式。您可以按任何顺序输入 **match** 命令。所有 **match** 命令都必须“通过”，才能根据 **set** 命令给定的 **set** 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。

路由映射可包含多个部分。任何与 **route-map** 命令相关的至少一个 **match** 子句不匹配的路由都将被忽略。要仅修改部分数据，您必须配置第二个路由映射部分并指定显式匹配。在某些情况下，路由的下一跳和源路由器地址不同。

CR_Examples

以下示例显示如何分发由位于 ACL acl_dmz1 和 acl_dmz2 指定的地址处的路由器和接入服务器通告的路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由。
matchipnext-hop	分发具有由其中一个指定的 ACL 传递的下一跳路由器地址的任何路由。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match ipv6 address

要重新分配具有 IPv6 路由地址或匹配由指定的访问列表之一传递的数据包的任何路由，请在 **matchipv6address** 路由映射配置模式下使用该命令。要恢复默认设置，请使用此命令 **no** 的形式。

matchipv6address{*acl* . . . }**prefix-list**
no matchipv6address{*acl* . . . }**prefix-list**

Syntax Description

acl 指定访问列表的名称。可以指定多个访问列表。

prefix-list 指定匹配前缀列表的名称。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.1(2) 添加了此命令。

使用指南

route-mapglobal 配置命令以及 **match** 和 **set** 配置命令允许您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 **match** 和 **set** 命令与其关联。 **match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。 **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。 **noroute-map** 命令可删除路由映射。

CR_Examples

以下示例显示如何重新分发内部路由： **access-list acl_dmz1 Extended permit ipv6 any <net><mask>**

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由，
match ip address	分配具有由指定的访问列表之一传递的路由地址或匹配数据包的任何路由。

命令	说明
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match login-name

要配置即时消息的客户端登录名匹配条件，请在 `class-map` 或 `policy-map` 配置模式下使用 **matchlogin-name** 命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **login-nameregex** [*regex_name* | **class***regex_class_name*]
no match [**not**] **login-nameregex** [*regex_name* | **class***regex_class_name*]

Syntax Description

<i>regex_name</i>	指定正则表达式。
<i>class</i> <i>regex_class_name</i>	指定正则表达式类映射。

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
类映射或策略映射配置	• 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

可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

CR_Examples

以下示例展示如何在即时消息类映射中为客户端登录名配置匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match media-type

要配置 H.323 媒体类型的匹配条件，请在策略映射配置模式下使用 **match media-type** 命令。要禁用此功能，请使用此 **no** 命令的形式。

match [**not**] **media-type** [**audio** | **data** | **video**]
no match [**not**] **media-type** [**audio** | **data** | **video**]

Syntax Description

音 指定要匹配的音频媒体类型。
頻

数 指定要匹配的数据介质类型。
据

视 指定以匹配视频媒体类型。
頻

Command Default

无默认为或值。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例展示如何在 H.323 检测类映射中配置音频媒体类型的匹配条件：

```
ciscoasa(config-cmap)# match media-type audio
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clear configure class-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match message class

要配置消息类和 M3UA 消息类型的匹配条件，请在策略映射配置模式下使用 **matchmessageclass** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] messageclass class_id [idmessage_id]
no match [not] messageclass class_id [idmessage_id]
```

Syntax Description

class_id 消息类别。有关受支持的类别和类型的列表，请参阅“用法”部分。

idmessage_id 指定类中的消息类型。

Command Default

M3UA 检测允许所有消息类和类型，没有速率限制。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.6(2) 添加了此命令。

使用指南

您可以在 M3UA 检测策略映射中配置此命令。可以根据消息类和类型丢弃数据包或按速率限制数据包。下表列出了可能的值。有关这些消息的详细信息，请参阅 M3UA RFC 和文档。

M3UA 消息类	消息 ID 类型
0（管理消息）	0-1
1（传输消息）	1
2（SS7 信令网络管理消息）	1-6
3（ASP 状态维护消息）	1-6
4（ASP 流量维护消息）	1-4
9（路由密钥管理消息）	1-4

CR_Examples

以下示例显示如何配置 M3UA 消息的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match message class 2 id 6
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
```

Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
policy-maptypeinspect	创建检查策略映射。

match message id

要配置 GTP 消息 ID 的匹配条件，请在策略映射配置模式下使用 **matchmessageid**命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] message {v1 | v2} id [message_id | range lower_range upper_range]
no match [not] message {v1 | v2} id [message_id | range lower_range upper_range]
```

Syntax Description	{v1 v2}	(从 9.5(1) 开始。) 指示 GTP 版本。对于 GTPv0-1，请使用 v1 ；对于 GTPv2，请使用 v2 。
	message_id	消息 ID，可介于 1 到 255 之间。
	range lower_range upper_range	消息 ID 范围。指定范围的下边界和上限。

Command Default 无默认为或值。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.2(1) 添加了此命令。
	9.5(1) {v1v2} 添加了 关键字。

使用指南 可以在 GTP 策略映射中配置此命令。

CR_Examples 以下示例显示如何为 GTP 检测策略映射中的消息 ID 配置匹配条件：

```
ciscoasa(config-pmap)# match message id 33

从版本 9.5(1) 开始，您需要将 {v1 | v2} 关键字：

ciscoasa(config-pmap)# match message v2 id 33
```

Related Commands

命令	说明
<code>inspectgtp</code>	配置 GTP 流量检测。

match message length

要配置 GTP 消息 ID 的匹配条件，请在策略映射配置模式下使用 **matchmessageid** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

match [**not**] **messageid** **min** *min_length* **max** *max_length*
no match [**not**] **messageid** **min** *min_length* **max** *max_length*

Syntax Description

min *min_length* 指定最小消息 ID 长度。值介于 1 和 65536 之间。

max *max_length* 指定最大消息 ID 长度。值介于 1 和 65536 之间。

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
策略映射配置	• 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

可以在 GTP 策略映射中配置此命令。

CR_Examples

以下示例显示如何在 GTP 检查策略映射中配置消息长度的匹配条件：

```
ciscoasa(config-pmap)# match message length min 8 max 200
```

Related Commands

命令	说明
inspectgtp	配置 GTP 流量检测。
matchmessageid	根据消息 ID 匹配流量。

match message-path

要配置 SIP 消息所采用路径的匹配条件（如 Via 报头字段中指定的），请在类映射或策略映射配置模式下使用 **matchmessage-path** 命令。要删除匹配条件，请使用此**no**命令的形式。

```
match [not] message-pathregex [regex_name | classregex_class_name]
no match [not] message-pathregex [regex_name | classregex_class_name]
```

Syntax Description	regex_name	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	72(1) 添加了此命令。

使用指南 可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

CR_Examples 以下示例展示如何为 SIP 检测类映射中的 SIP 消息配置匹配条件：

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

Related Commands	命令	说明
	class-map	创建第 3/4 层类映射。
	clearconfigureclass-map	删除所有类映射。
	matchany	包括类映射中的所有流量。

命令	说明
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match metric

要重新分发具有指定指标的路由，请在路由映射配置模式下使用 **matchmetric** 命令。要删除该条目，请使用此命 **no** 令的形式。

matchmetric*number*
nomatchmetric*number*

Syntax Description *number* 路由度量，可以是由五部分组成的 IGRP 度量； ；有效值为 0 到 4294967295。

Command Default 未过滤指标值。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

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

使用指南

route-mapglobal 配置命令以及 **match** 和 **set**配置命令允许您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 **match** 和 **set** 命令与其关联。**match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。**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。**noroute-map** 命令可删除路由映射。

matchroute-map 配置命令具有多种格式。**match** 命令可以按任意顺序给出，并且所有 **match** 命令必须“通过”，以便根据使用 **set** 命令给定的 set 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。

路由映射可包含多个部分。任何与 **route-map** 命令相关的至少一个 **match** 子句不匹配的路由都将被忽略。要仅修改部分数据，您必须配置第二个路由映射部分并指定显式匹配。

CR_Examples

以下示例显示如何重新分发度量为 5 的路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由，
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match mime

要配置 ESMTP MIME 编码类型、MIME 文件名长度或 MIME 文件类型的匹配条件，请在策略映射配置模式下使用 **matchmime** 命令。要禁用此功能，请使用此**no**命令的形式。

match [**not**] **mime** [**encoding**类型 | **filenamelengthgt**bytes | **filetype**正则表达式]
no match [**not**] **mime** [**encoding**类型 | **filenamelengthgt**bytes | **filetype**正则表达式]

Syntax Description	编码类型	指定要匹配编码类型。
	文件名长度 gt 字节数	指定要匹配的文件名长度。
	文件类型正则表达式	指定要匹配的文件类型。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.2(1) 添加了此命令。

CR_Examples 以下示例显示如何在 ESMTP 检测策略映射中为 MIME 文件名长度配置匹配条件：

```
ciscoasa
(config)#
policy-map type inspect esmtp esmtp_map
ciscoasa (config-pmap)#matchmimefilenamelengthgt255
```

Related Commands	命令	说明
	class-map	创建第 3/4 层类映射。
	clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match msisdn

要为创建 PDP 情景请求、创建会话请求和修改承载响应消息中的 GTP 移动站国际用户目录编号 (MSISDN) 信息元素配置匹配条件，请在策略映射配置模式下使用 **matchmsisdn**命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] msisdnregex { regex_name | classclass_name }
no match [not] msisdnregex { regex_name | classclass_name }
```

Syntax Description	regex_name	正则表达式对象的名称。
	classclass_name	正则表达式类的名称。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	9.10(1)	引入了此命令。

使用指南 可以在 GTP 策略映射中配置此命令。

您可以在创建 PDP 情景请求中过滤移动站点国际订户目录号 (MSISDN) 信息元素。您可以根据特定 MSISDN 或 MSISDN 范围的前 x 位数丢弃或记录消息。可以使用正则表达式指定 MSISDN。MSISDN 过滤仅支持 GTPv1 和 GTPv2。

CR_Examples 以下示例显示如何使用正则表达式对象配置 MSISDN 匹配条件。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match msisdn regex msisdn1
ciscoasa(config-pmap-c)# drop log
```

以下示例显示如何使用正则表达式类配置 MSISDN 匹配条件。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map  
ciscoasa(config-pmap)# match msisdn regex class msisdn2  
ciscoasa(config-pmap-c)# drop log
```

Related Commands

命令	说明
drop	丢弃符合条件的数据包。
log	记录匹配条件的数据包。
inspectgtp	启用 GTP 应用检查。
policy-maptypeinspectgtp	创建或编辑 GTP 检查策略图。

match opc

要为 M3UA 数据消息的始发点代码 (OPC) 配置匹配条件，请在策略映射配置模式下使用 **matchopc** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

match [not] opc代码
no match [not] opc代码

Syntax Description *code* 区域-地区-*sp* 格式的源点代码。

Command Default M3UA 检测允许所有源点编码。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南 您可以在 M3UA 检测策略映射中配置此命令。可以根据始发点代码丢弃数据包。点代码采用 区域-地区-*sp* 格式，其中每个元素的可能值取决于 SS7 变体。可以在策略映射中的 **ss7variant** 命令中定义变体。

- ITU - 点代码为 14 位，格式为 3-8-3。值范围为 [0-7]-[0-255]-[0-7]。这是默认的 SS7 变量。
- ANSI - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
- Japan - 点代码为 16 位，格式为 5-4-7。值范围为 [0-31]-[0-15]-[0-127]。
- China - 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。

CR_Examples

以下示例显示如何为 ITU 配置特定始发点代码的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match opc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
matchdpc	匹配 M3UA 目标点代码。
policy-maptypeinspect	创建检查策略映射。
ss7variant	标识要在策略映射中使用的 SS7 变量。

match peer-ip-address

要为即时消息配置对等体 IP 地址的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchpeer-ip-address** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] peer-ip-addressip_address ip_address_mask
no match [not] peer-ip-addressip_address ip_address_mask
```

Syntax Description	ip_address	指定客户端或服务器的主机名或 IP 地址。
	ip_address_mask	指定客户端或服务器 IP 地址的网络掩码。

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
类映射或策略映射配置	• 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 可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

CR_Examples 以下示例展示如何在即时消息类映射中配置对等体 IP 地址的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match peer-login-name

要配置即时消息的对等体登录名匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchpeer-login-name** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] peer-login-nameregex [regex_name | classregex_class_name]
no match [not] peer-login-nameregex [regex_name | classregex_class_name]
```

Syntax Description	正则表达式名称	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 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 可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

CR_Examples 以下示例展示如何在即时消息类映射中配置对等体登录名的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

命令	说明
class-map type inspect	创建检查类别图。
showrunning-config class-map	显示有关类映射配置的信息。

match port

使用模块化策略框架时，在类映射配置模式下使用 **matchport** 命令匹配要应用操作的端口。要删除该 **matchport** 命令，请使用此命令的 **no** 形式。

```
matchport { tcp | udp | sctp } { eqport | rangebeg_portend_port }  
no matchport { tcp | udp | sctp } { eqport | rangebeg_portend_port }
```

Syntax Description

eq 端口	指定单个端口名称或编号。
range 请求端口结束端口	指定介于 1 和 65535 之间的开始和结束端口范围值。 口
tcp	指定 TCP 端口。
sctp	指定 SCTP 端口。
udp	指定 UDP 端口。

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。

9.7(1) 添加了 **sctp** 关键字。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用 **class-map** 或 **class-maptype management** 命令应用操作的第 3 层和第 4 层流量。

输入 **class-map** 命令后，您可以输入 **matchport** 命令来标识流量。或者，您也可以输入其他类型的 **match** 命令，例如 **matchaccess-list** 命令（**class-maptype management** 命令仅允许 **match port** 命令）。类映射中只能包含一个 **matchport** 命令，且不能将其与其他类型的 **match** 命令组合使用。

1. （仅限应用检测）使用 **policy-maptype inspect** 命令定义应用检测流量的特殊操作。

- 2. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
- 3. 使用 **service-policy** 命令在接口上激活这些操作。

CR_Examples

以下示例显示如何使用类映射和 **matchport**命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchaccess-list	根据访问列表匹配流量。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match ppid

要配置 SCTP 检测的负载协议标识符 (PPID) 的匹配条件，请在检测策略映射配置模式下使用 **matchppid** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] ppidppid_1 [ppid_2]
no match [not] ppidppid_1 [ppid_2]
```

Syntax Description

ppid_1 指定 SCTP PPID，可以通过 PPID 编号 (0-4294967295) 或名称 (有关可用名称，请参阅 CLI 帮助) 指定。您可以包含第二个 (更高) PPID 来指定范围。

Command Default

无默认为行为或值。

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
检测策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.5(2) 添加了此命令。

使用指南

可以在 SCTP 检查策略映射中配置此命令。使用它来过滤 PPID，以对这些 ID 应用特殊操作，例如丢弃、记录日志或速率限制。

如果决定对 PPID 进行过滤，请记住以下几点：

- PPID 位于数据块中，给定的数据包可以有多个数据块。如果数据包包含具有不同 PPID 的数据分块，系统不会过滤该数据包，且不会将分配的操作应用于该数据包。
- 如果使用 PPID 过滤来丢弃数据包或限制数据包速率，请注意发射器会重新发送被丢弃的任何数据包。虽然下次尝试时可能会让 PPID 速率受限制的数据包通过，但 PPID 丢弃的数据包仍会被丢弃。您可能需要评估网络中反复出现这些丢弃所带来的最终结果。

CR_Examples

以下示例创建了一个 SCTP 检查策略图，它将删除未分配的 PPID（在编写此示例时未分配），限制 PPID 32-40 的速率，并记录 Diameter PPID。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
```

```
drop
match ppid 26
drop
match ppid 49
drop
match ppid 32 40
rate-limit 1000
match ppid diameter
log
```

Related Commands

命令	说明
drop	丢弃匹配的流量。
inspectstcp	启用 SCTP 检查。
log	记录匹配的流量。
policy-maptypeinspectstcp	创建 SCTP 检查策略图。
rate-limit	将速率限制应用于匹配的流量。

匹配优先级

如要在类映射中指定优先级值，请在 `class-map` 配置模式下使用 `matchprecedence` 命令。要删除此规范，请使用此 `no` 命令的形式。

`matchprecedence` 值
`nomatchprecedence` 值

Syntax Description `value` 指定以空格分隔的最多四个优先级值。范围为 0 至 7。

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。

使用指南

`match` 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 `class-map` 全局配置命令定义流量类。在 `class-map` 配置模式下，可以使用 `match` 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 `match` 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 `matchprecedence` 命令指定 IP 报头中的 TOS 字节表示的值。

CR_Examples

以下示例显示如何使用类映射和 `matchprecedence` 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchprecedence 1
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match protocol

要为特定即时消息协议（如 MSN 或 Yahoo）配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchprotocol** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] protocol { msn-im | yahoo-im }
no match [not] protocol { msn-im | yahoo-im }
```

Syntax Description

msn-im 指定以匹配 MSN 即时消息协议。

yahoo-im 指定以匹配 Yahoo 即时消息协议。

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
类映射或策略映射配置	• 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

可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在即时消息类映射中配置 Yahoo 即时消息协议的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match protocol yahoo-im
```

Related Commands

命令	说明
class-map type inspect	创建检查类别图。
show running-config class-map	显示有关类映射配置的信息。

match question

要为 DNS 问题或资源记录配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchquestion** 命令。要删除已配置的部分，请使用**no**此命令的形式。

```
match { question | { resource-recordanswer | authority | additional } }
no match { question | { resource-recordanswer | authority | additional } }
```

Syntax Description	问题	指定 DNS 消息的问题部分。
	资源记录	指定 DNS 消息的资源记录部分。
	应答	指定“应答 RR”部分。
	权威	指定“颁发机构 RR”部分。
	补充	指定“其他 RR”部分。

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
类映射或策略映射配置	• 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 默认情况下，此命令检查 DNS 报头并匹配指定的字段。它可与其他 DNS 匹配命令结合使用，以定义对特定问题或 RR 类型的检测。

可以在 DNS 类映射或策略映射内配置此命令。在 DNS 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何为 DNS 检测策略映射中的 DNS 问题配置匹配条件：

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


Related Commands

命令	说明
class-map type inspect	创建检查类别图。
policy-map type inspect	创建检查策略映射。



match r – me

- [match regex](#) , 第 753 页
- [match req-resp](#) , 第 755 页
- [match request-command](#) , 第 757 页
- [match request-method](#) , 第 759 页
- [match request method](#) , 第 761 页
- [match route-type](#) , 第 763 页
- [match rtp](#) , 第 765 页
- [match selection-mode](#) , 第 767 页
- [match sender-address](#) , 第 769 页
- [match server](#) , 第 770 页
- [match service](#) , 第 772 页
- [match service-indicator](#) , 第 774 页
- [match third-party-registration](#) , 第 776 页
- [match tunnel-group](#) , 第 778 页
- [match uri](#) , 第 780 页
- [match url-filter](#) , 第 782 页
- [match user group](#) , 第 784 页
- [match username](#) , 第 786 页
- [match uuid](#) , 第 788 页
- [match version](#) , 第 790 页
- [max-area-addresses](#) , 第 791 页
- [max-failed-attempts](#) , 第 795 页
- [max-forwards-validation](#) , 第 797 页
- [max-header-length](#) , 第 799 页
- [max-lsp-lifetime](#) , 第 801 页
- [maximum-paths \(BGP\)](#) , 第 805 页
- [maximum-paths \(IS-IS\)](#) , 第 807 页
- [max-object-size](#) , 第 811 页
- 最大重试次数（已弃用）, 第 813 页

- max-uri-length, 第 815 页
- mcast-group, 第 817 页
- mcc, 第 820 页
- media-termination (已弃用), 第 822 页
- media-type, 第 824 页
- member, 第 826 页
- member-interface, 第 828 页
- memberof, 第 830 页
- memory appcache-threshold enable, 第 832 页
- memory delayed-free-poisoner enable, 第 834 页
- memory delayed-free-poisoner validate, 第 837 页
- memory caller-address, 第 839 页
- memory logging, 第 841 页
- memory profile enable, 第 843 页
- memory profile text, 第 845 页
- memory-size, 第 847 页
- memory tracking enable, 第 849 页
- memory-utilization, 第 851 页
- merge-dacl, 第 852 页
- message-authenticator-required, 第 854 页
- message-length, 第 855 页
- message-tag-validation, 第 857 页
- metric, 第 859 页
- metric-style, 第 863 页

match regex

要标识正则表达式类映射中的正则表达式，请在 `class-map type regex` 配置模式下使用 **matchregex** 命令。要从类映射中删除正则表达式，请使用此命令的 **no** 形式。

matchregex名称
nomatchregex*name*

Syntax Description *name* 通过 **regex** 命令添加的正则表达式的名称。

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
类映射类型正则表达式配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
7.0(2)	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。您可以使用 **class-map type regex** 命令，然后使用多个 **matchregex** 命令，对正则表达式类映射中的正则表达式进行分组。

例如，您可以使用检查策略图配置应用程序检查的特殊操作（参见 **polycymaptypeinspect**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。

CR_Examples

以下是 HTTP 检测策略映射和相关类映射的示例。此策略映射由第 3/4 层策略映射激活，而第 3/4 层策略映射由服务策略启用。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
```

```
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
[a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy test interface outside
```

Related Commands

命令	说明
class-maptypepregex	创建正则表达式类映射。
regex	添加正则表达式。
testregex	测试正则表达式。

match req-resp

要为 HTTP 请求和响应配置匹配条件，请在策略映射配置模式下使用 **matchreq-resp** 命令。要禁用此功能，请使用此**no**命令的形式。

match [not] req-respcontent-type mismatch
nomatch [not] req-respcontent-type mismatch

Syntax Description

内容类型不匹 将 HTTP 响应中的 content-type 字段与相应 HTTP 请求消息中的 accept 字段不匹配配 的流量进行匹配。

Command Default

无默认为或值。

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
策略映射配置	• 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

此命令可启用以下检查：

- 验证报头 content-type 的值是否在受支持内容类型的内部列表中，
- 验证报头内容类型是否与消息的数据或实体正文部分中的实际内容匹配。
- 验证 HTTP 响应中的内容类型字段是否与相应 HTTP 请求消息中的 **accept** 字段匹配。

如果该消息未通过上述任一检查，则 ASA 将执行已配置的操作。

以下是受支持的内容类型列表。

音频/*	音频/基本	视频/x-msvideo
音频/mpeg 转换	x-adpcm 音频/x-adpcm	音频/midi
音频/x-ogg 音频	x-wav 音频/x-wav	音频/x-aiff 音频
application/octet-stream	application/pdf	application/msword

application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arming	application/x-msn-messenger	application/x-gzip
图片	application/x-java-xm	application/zip
image/jpeg	image/cgf	image/gif
image/x-3ds	image/png	image/tiff
image/x-portable-bitmap	image/x-bitmap	x-niff image/x-niff
text/*	image/x-portable-greymap image/x-portable-greymap	image/x-xpm 映像
text/plain	text/css	text/html
text/xmcd	text/richtext	text/sgml
video/-flc	text/xml	video/*
视频/Sgi	视频/mpeg	视频/quicktime
视频/x-mng	视频/x-avi	视频/x-fli

此列表中的某些内容类型可能没有相应的正则表达式（幻数），因此无法在邮件的正文部分中对其进行验证。当发生这种情况时，将允许 HTTP 消息。

CR_Examples

以下示例显示如何根据 HTTP 策略映射中 HTTP 消息的内容类型来限制 HTTP 流量：

```
ciscoasa
(config)#
  policy-map type inspect http http_map
ciscoasa
(config-pmap)#
  match req-resp content-type mismatch
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
showrunning-configclass-map	显示有关类映射配置的信息。

match request-command

要限制特定 FTP 命令，请在 class-map 或 policy-map 配置模式下使用 **matchrequest-command** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] request-command ftp_command [ftp_command . . .]
no match [not] request-command ftp_command [ftp_command . . .]
```

Syntax Description

ftp_命 指定要限制的一个或多个 FTP 命令。
令

Command Default

无默认为行为或值。

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
类映射或策略映射配置	• 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

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

CR_Examples

以下示例显示如何在 FTP 检测策略映射中为特定 FTP 命令配置匹配条件：

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match request-method

要配置 SIP 方法类型的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **match request-method** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

match [**not**] **request-method** *method_type*
no match [**not**] **request-method** *method_type*

Syntax Description

method_type 根据 RFC 3261 和支持的扩展指定方法类型。支持的方法类型包括：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。

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
类映射或策略映射配置	• 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

可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

CR_Examples

以下示例展示如何为 SIP 检测类映射中的 SIP 消息配置匹配条件：

```
ciscoasa(config-cmap)# match request-method ack
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clear configure class-map	删除所有类映射。
match any	包括类映射中的所有流量。
match port	标识类映射中的特定端口号。

命令	说明
showrunning-configclass-map	显示有关类映射配置的信息。

match request method

要配置 HTTP 请求的匹配条件，请在 `policy-map` 配置模式下使用 **matchrequestmethod** 命令。要禁用此功能，请使用此 **no** 命令的形式。

```
match [not] request { built-in-regex | regex { regex_name | classclass_map_name } }
no match [not] request { built-in-regex | regex { regex_name | classclass_map_name } }
```

Syntax Description

built-in-regex 指定内容类型、方法或传输编码的内置正则表达式。

classclass_map name 指定正则表达式类型的类映射的名称。

regexregex_name 指定使用 **regex** 命令配置的正则表达式的名称。

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
策略映射配置	• 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

表 4: 内置 **Regex** 值

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	锁定
mkcol	mkdir	迁移	notify
选项	poll	岗位	propfind
proppatch	put	revadd	revlabel

revlog	revnum	保存	搜索
设置属性	开始/旋转	stoprev	订阅
trace	unedit	解锁	unsubscribe

CR_Examples

以下示例显示如何定义 HTTP 检查策略映射，该策略映射将允许并记录任何尝试使用方法“GET”或“PUT”访问“www.example.com/*.asp”或“www.example[0-9][0-9].com”的 HTTP 连接。所有其他 URL/方法组合将被默认：

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp"
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
showrunning-configclass-map	显示有关类映射配置的信息。

match route-type

要重新分发指定类型的路由，请在 route-map 配置模式下使用 **matchroute-type** 命令。要删除路由类型条目，请使用此命令 **no** 的形式。

```
matchroute-type { local | internal | { external [ type-1 | type-2 ] } | { nssa-external [ type-1 | type-2 ] } }  
no matchroute-type { local | internal | { external [ type-1 | type-2 ] } | { nssa-external [ type-1 | type-2 ] } }
```

Syntax Description

external	OSPF 外部路由或 EIGRP 外部路由。
internal	OSPF 区域内和区域间路由或 EIGRP 内部路由。
local	本地生成的 BGP 路由。
nssa-external	指定外部 NSSA。
type-1	（可选）指定路由类型 1。
type-2	（可选）指定路由类型 2。

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
路由映射配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

通过 **route-map** 使用全局配置命令以及 **match** 和 **set** 配置命令，您可以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 **match** 和 **set** 命令与其关联。**match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。**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。**noroute-map** 命令可删除路由映射。

matchroute-map 配置命令具有多种格式。您可以按任何顺序输入 **match** 命令。所有 **match** 命令都必须“通过”，才能根据 **set** 命令给定的 set 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。

路由映射可包含多个部分。任何与 **route-map** 命令相关的至少一个 **match** 子句不匹配的路由都将被忽略。要仅修改部分数据，您必须配置第二个路由映射部分并指定显式匹配。

对于 OSPF，**externaltype-1** 关键字仅匹配 1 类外部路由，**externaltype-2** 关键字仅匹配 2 类外部路由。

CR_Examples

以下示例显示如何重新分配内部路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

Related Commands

命令	说明
matchinterface	分发任何下一跳位于指定接口之一的路由，
matchipnext-hop	分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。
matchmetric	根据指定的度量重新分配路由。
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
setmetric	为路由映射指定目标路由协议中的指标值。

match rtp

如要在类映射中指定偶数端口的 UDP 端口范围，请在 class-map 配置模式下使用 **matchrtp** 命令。要删除此规范，请使用此 **no** 命令的形式。

matchrtp*starting_port*范围
nomatchrtp*starting_port*范围

Syntax Description	起始端 指定偶数 UDP 目标端口的下限。范围为 2000-65535 口
	<i>range</i> 指定 RTP 端口范围。范围是 0-16383。

Command Default 无默认为行为或值。

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。

使用指南 **match** 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 **matchrtp** 命令匹配 RTP 端口（偶数 UDP 端口号介于 *starting_port* 与 *starting_port* 加上 范围）。

CR_Examples 以下示例显示如何使用类映射和 **matchrtp**命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchrtp 20000 100
ciscoasa(config-cmap)#
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match selection-mode

要为创建 PDP 情景请求中的选择模式信息元素配置匹配，请在策略映射配置模式下使用 **matchselection-mode**命令。要删除匹配条件，请使用此 **no**命令的形式。

match [**not**] **selection-mode**模式值
nomatch [**not**] **selection-mode**模式值

Syntax Description	模式值 创建PDP上下文请求中的选择模式信息元素。选择模式指定消息中的无线接入点名称 (APN) 来源，可以是以下项目之一。 • 0 - 已验证。由移动站点或网络提供 APN，并且已验证订用。 • 1 - 移动站点。由移动站点提供 APN，并且已验证订用。 • 2 - 网络。由网络提供 APN，并且已验证订用。 • 3 - 保留，未使用。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.10(1) 引入了此命令。

使用指南 可以在 GTP 策略映射中配置此命令。

您可以根据创建 PDP 上下文请求中的选择模式信息元素进行过滤。选择模式指定消息中接入点名称（APN）的来源。您可以根据这些模式丢弃和选择记录消息。选择模式过滤仅支持 GTPv1 和 GTPv2。

CR_Examples 以下示例显示如何匹配选择模式 1 和 2，以及如何丢弃和记录采用这两种模式的创建 PDP 情景消息。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
```

```
ciscoasa(config-pmap) # match selection-mode 1

ciscoasa(config-pmap-c) # drop log

ciscoasa(config-pmap) # match selection-mode 2

ciscoasa(config-pmap-c) # drop log
```

Related Commands

命令	说明
drop	丢弃符合条件的数据包。
log	记录匹配条件的数据包。
inspectgtp	启用 GTP 应用检查。
policy-maptypeinspectgtp	创建或编辑 GTP 检查策略图。

match sender-address

要配置 ESMTP 发件人邮件地址的匹配条件，请在策略映射配置模式下使用 **matchsender-address** 命令。要禁用此功能，请使用此 **no** 命令的形式。

match [**not**] **sender-address** [**length** **gt** **bytes** | **regex** **regex**]
nomatch [**not**] **sender-address** [**length** **gt** **bytes** | **regex** **regex**]

Syntax Description

length **gt** **bytes** 指定要匹配发件人邮件地址的长度。

regex **regex** 指定匹配正则表达式。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.2(1) 添加了此命令。

CR_Examples

以下示例显示如何在 ESMTP 检测策略映射中为长度超过 320 个字符的发件人邮件地址配置匹配条件：

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match server

要配置 FTP 服务器的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchserver** 命令。要删除匹配条件，请使用此 **no** 命令的形式。

```
match [not] serverregex [regex_name | classregex_class_name]
no match [not] serverregex [regex_name | classregex_class_name]
```

Syntax Description	regex_name	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 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 可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

ASA 使用连接到 FTP 服务器时登录提示上方显示的初始 220 服务器消息来匹配服务器名称。220 服务器消息可能包含多行。服务器匹配不基于通过 DNS 解析的服务器名称的 FQDN。

CR_Examples 以下示例显示如何在 FTP 检测策略映射中配置 FTP 服务器的匹配条件：

```
ciscoasa (config-pmap) # match server class regex ftp-server
```

Related Commands	命令	说明
	class-map	创建第 3/4 层类映射。
	clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match service

要为特定即时消息服务配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchservice** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] { service { chat | file-transfer | games | voice-chat | webcam | conference }
no match [not] { service { chat | file-transfer | games | voice-chat | webcam | conference }
```

Syntax Description	chat	指定 来匹配即时消息聊天服务。
	file-transfer	指定 来匹配即时消息文件传输服务。
	游戏	指定 以匹配即时消息游戏服务。
	语音聊天	指定 以匹配即时消息通话聊天服务。
	网络摄像头	指定 以匹配即时消息网络摄像头服务。
	会议	指定以匹配即时消息会议服务。

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
类映射或策略映射配置	• 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 可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何在即时消息类映射中配置聊天服务的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```


Related Commands

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。
showrunning-configclass-map	显示有关类映射配置的信息。

match service-indicator

要配置 M3UA 消息的服务指示符的匹配条件，请在策略映射配置模式下使用 **matchservice-indicator** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] service-indicatornumber
no match [not] service-indicatornumber
```

Syntax Description *number* 服务指示器编号，0-15。有关受支持的服务指示符列表，请参阅用量部分。

Command Default M3UA 检测允许所有服务指示符。

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
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南 您可以在 M3UA 检测策略映射中配置此命令。可以根据服务指标丢弃数据包。下面是可用的服务指示符。有关这些服务指示符的详细信息，请参阅 M3UA RFC 和文档。

- 0 - 信令网络管理消息
- 1 - 信令网络测试和维护消息
- 2 - 信令网络测试和维护特殊消息
- 3 - SCCP
- 4 - 电话用户部分
- 5 - ISDN 用户部分
- 6 - 数据用户部分（呼叫和电路相关消息）
- 7 - 数据用户部分（设备注册和取消消息）
- 8 - 预留用于 MTP 测试用户部分
- 9 - 宽带 ISDN 用户部分

- 10 - 卫星 ISDN 用户设备
- 11 - 预留
- 12 - AAL 第 2 类信令
- 13 - 承载独立呼叫控制
- 14 - 网关控制协议
- 15 - 预留

CR_Examples

以下示例显示如何配置 M3UA 服务指示符的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
policy-maptypeinspect	创建检查策略映射。

match third-party-registration

要为第三方注册请求者配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchthird-party-registration** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] third-party-registrationregex [regex_name | classregex_class_name]
no match [not] third-party-registrationregex [regex_name | classregex_class_name]
```

Syntax Description	regex_name	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 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 可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

third-party registration match 命令用于识别可使用 SIP 注册器或 SIP 代理注册其他用户的用户。在 From 和 To 值不匹配的情况下，可通过 REGISTER 消息中的 From 报头字段进行标识。

CR_Examples 以下示例显示如何在 SIP 检测类映射中配置第三方注册的匹配条件：

```
ciscoasa (config-cmap) # match third-party-registration regex class sip_regist
```

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match tunnel-group

要匹配属于之前定义的隧道组的类映射中的流量，请在 class-map 配置模式下使用 **matchtunnel-group** 命令。要删除此规范，请使用此 **no** 命令的形式。

matchtunnel-group*name*
nomatchtunnel-group*name*

Syntax Description
name 隧道组名称的文本。

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。

使用指南
match 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

要启用基于流的策略操作，请将 **matchflowipdestination-address** 和 **matchtunnel-group** 命令配合使用 **class-map**、**policy-map**和 **service-policy** 命令。定义流的条件是目的 IP 地址。所有流向某唯一 IP 目标地址的流量都被视为流。策略操作应用于每个数据流，而不是整个流量类。QoS 操作策略使用 **police** 命令应用。使用**matchtunnel-group** 和 **matchflowipdestination-address** 会将隧道组中的每个隧道策略为指定的速率。

CR_Examples
以下示例展示如何在隧道组内启用基于流的策略管制，并将每个隧道限制为指定的速率：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchtunnel-group
```

```
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

Related Commands

命令	说明
class-map	将流量类应用于接口。
clearconfigureclass-map	删除所有流量映射定义。
matchaccess-list	识别类映射中的访问列表流量。
showrunning-configclass-map	显示有关类映射配置的信息。
tunnel-group	创建和管理 IPsec 和 L2TP 连接特定记录数据库，

match uri

要配置 SIP 报头中 URI 的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchuri** 命令。
要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] uri {sip | tel} lengthtgt_bytes
no match [not] uri {sip | tel} lengthtgt_bytes
```

Syntax Description	sip	指定 SIP URI。
	tel	指定 TEL URI。
	lengthtgt_bytes	指定 URI 的最大长度。值介于 0 和 65536 之间。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	— • 是

Command History	版本 修改
	7.2(1) 添加了此命令。

使用指南 可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

CR_Examples 以下示例展示如何为 SIP 消息中的 URI 配置匹配条件：

```
ciscoasa(config-cmap) # match uri sip length gt
```

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match url-filter

要配置 RTSP 消息中 URL 过滤的匹配条件，请在 `class-map` 或 `policy-map` 配置模式下使用 `matchurl-filter` 命令。要删除匹配条件，请使用此 `no` 命令的形式。

```
match [not] url-filterregex [regex_name | classregex_class_name]
no match [not] url-filterregex [regex_name | classregex_class_name]
```

Syntax Description	regex_name	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南 可以在 RTSP 类映射或策略映射中配置此命令。

CR_Examples 以下示例显示如何在 RTSP 检查策略映射中配置 URL 过滤的匹配条件：

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

Related Commands	命令	说明
	class-map	创建第 3/4 层类映射。
	clearconfigureclass-map	删除所有类映射。

命令	说明
matchany	包括类映射中的所有流量。
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match user group

如要指定云网络安全白名单中的用户或组，请在 class-map 配置模式下使用 **matchusergroup** 命令。
要删除匹配，请使用此命 **no** 令的形式。

用户名**match** [**not**] { [**user**] [**group**组名] }
用户名**no match** [**not**] { [**user**] [**group**组名] }

Syntax Description	not (可选) 指定应使用 Web 云安全过滤用户和/或组。例如，如果您将组 “cisco” 列入白名单，但想要扫描用户 “johnrichton” 和 “aerynsun” 的流量，则可以 matchnot 为这些用户指定。
	userusername 将用户指定到白名单。
	groupgroupname 指定要白名单的组。

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
类映射配置模式	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.0(1) 添加了此命令。

使用指南 如果您使用 AAA 规则或 IDFW，则可以配置 ASA，以便来自特定用户或组的、与服务策略规则匹配的 Web 流量不会重定向到云 Web 安全代理服务器进行扫描。当绕过云网络安全扫描时，ASA 会直接从最初请求的 Web 服务器检索内容，而不联系代理服务器。当它收到 Web 服务器的响应时，它会将数据发送至客户端。此过程被称作将流量 “列入白名单”。

虽然当您使用 ACL 配置发送到云网络安全的流量类别时，您可以实现基于用户或组豁免流量的相同结果，但您可能会发现使用白名单更为直接。请注意，白名单功能仅基于用户和组，而不基于 IP 地址。

在检测策略映射 (**policy-maptypeinspectscansafe**) 中创建白名单后，当您使用 **inspectscansafe** 命令指定云网络安全操作时，可以使用此映射。

CR_Examples

以下示例将 HTTP 及 HTTPS 检测策略映射的相同用户和组加入白名单：

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

Related Commands

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
inspect scansafe	对类中的流量启用云网络安全检查。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
whitelist	对流量类执行白名单操作。

match username

要配置 FTP 用户名的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchusername** 命令。
要删除匹配条件，请使用此**no**命令的形式。

```
match [not] usernameregex [regex_name | classregex_class_name]
no match [not] usernameregex [regex_name | classregex_class_name]
```

Syntax Description	regex_name	指定正则表达式。
	class regex_class_name	指定正则表达式类映射。

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
类映射或策略映射配置	• 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 可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

CR_Examples 以下示例显示如何在 FTP 检测类映射中配置 FTP 用户名的匹配条件：

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

命令	说明
class-map	创建第 3/4 层类映射。
clearconfigureclass-map	删除所有类映射。
matchany	包括类映射中的所有流量。

命令	说明
matchport	标识类映射中的特定端口号。
showrunning-configclass-map	显示有关类映射配置的信息。

match uuid

要配置 DCERPC 消息的通用唯一标识符 (UUID) 的匹配条件，请在类映射或策略映射配置模式下使用 **matchuuid** 命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] uuidtype
nomatch [not] uuidtype
```

Syntax Description	<i>type</i> 要匹配的 UUID 类型。以下项之一： • ms-rpc-epm- 匹配 Microsoft RPC EPM 消息。 • ms-rpc-isystemactivator- 匹配 ISystemMapper 消息。 • ms-rpc-oxidresolver- 匹配 OxidResolver 消息。

Command Default	DCERPC 检测允许所有消息类型。

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
类映射或策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.5(2) 添加了此命令。

使用指南	可以在 DCERPC 检测类映射或策略映射中配置此命令。使用它可根据 DCERPC UUID 过滤流量。然后，可以重置或记录匹配的流量。

CR_Examples	以下示例显示如何为 DCERPC 消息中的 ms-rpc-isiustemactivator UUID 配置匹配条件：

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap
ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```


Related Commands

命令	说明
class-map type inspect	创建检查类别图。
policy-map type inspect	创建检查策略映射。

match version

要在 GTP 检测中配置 GTP 版本的匹配条件，请在策略映射配置模式下使用 **matchversion**命令。要删除匹配条件，请使用此 **no**命令的形式。

```
match [not] version [version_idlower_rangeupper_range | range]
no match [not] version [version_idlower_rangeupper_range | range]
```

Syntax Description	version_id	指定介于 0 和 255 之间的版本。
	range lower_range upper_range	指定版本的下限和上限范围。

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
策略映射配置	• 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	可以在 GTP 策略映射中配置此命令。

CR_Examples	以下示例显示如何为 GTP 检测策略映射中的消息版本配置匹配条件：

```
ciscoasa(config-pmap) # match version 1
```

Related Commands	命令	说明
	inspectgtp	配置 GTP 流量检测。

max-area-addresses

要为 IS-IS 区域配置其他手动地址，请在路由器 isis 配置模式下使用 **max-area-addresses** 命令。要禁用手动地址，请使用此命令 **no** 的形式。

max-area-addresses 编号
no max-area-addresses *number*

Syntax Description

number 要添加的手动地址数量。范围是 3 到 234。

Command Default

没有为 IS-IS 区域配置手动地址。

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

此命令使您可以通过配置其他手动地址来最大化 IS-IS 区域的大小。您指定要添加的地址数，并分配一个 NET 地址来创建每个手动地址。

CR_Examples

以下示例配置三个地址：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addresses 3
```

Related Commands

命令	说明
advertise passive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authentication key	全局启用 IS-IS 身份验证。
authentication mode	指定IS-IS实例全局使用的IS-IS报文认证方式。

命令	说明
authentication send-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clear isis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hello padding	将 IS-IS hello 配置为完整 MTU 大小。
hostname dynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isis adjacency-filter	过滤 IS-IS 邻接关系的建立。
isis advertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isis authentication key	启用接口的身份验证。
isis authentication mode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isis authentication send-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isis circuit-type	配置用于 IS-IS 的邻接类型。
isis csnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isis hello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isis hello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isis hello padding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isis lsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isis metric	配置 IS-IS 度量的值。
isis password	配置接口的认证密码。EXTEN
isis priority	配置接口上指定 ASA 的优先级。

命令	说明
isis protocol shutdown	禁用每个接口的 IS-IS 协议。
isis retransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis retransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isis tag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-full suppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocol shutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistribute isis	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。
route priority high	为 IS-IS IP 前缀分配高优先级。
router isis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。

命令	说明
show clns	显示 CLNS 特定信息。
show isis	显示 IS-IS 信息。
show route isis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

max-failed-attempts

要指定服务器组中的任何给定服务器在停用之前允许该服务器执行的失败 AAA 事务数，请在 **aaa-server** 组配置模式下使用 **max-failed-attempts** 命令。要删除此规范并恢复为默认值，请使用此命令的 **no** 形式。

max-failed-attempts 编号

nomax-failed-attempts

Syntax Description

number 1-5 范围内的整数，用于指定之前 **aaa-server** 命令中指定的服务器组中的任何给定服务器允许的失败 AAA 事务数。

Command Default

number 的默认值为 3。

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 group 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

必须已配置 AAA 服务器或组，才能发出此命令。

CR_Examples

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# max-failed-attempts 4
ciscoasa
(config-aaa-server-group)#
```

Related Commands

命令	说明
aaa-serverserver-tagprotocolprotocol	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。
clearconfigureaaa-server	删除所有 AAA 服务器配置。

命令	说明
showrunning-configaaa	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。

max-forwards-validation

要启用对 Max-forwards 报头字段是否为 0 的检查，请在参数配置模式下使用 **max-forwards-validation** 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。

max-forwards-validation action { drop | drop-connection | reset | log } [log]
no max-forwards-validation action { drop | drop-connection | reset | log } [log]

Syntax Description

drop	如果进行验证，则丢弃数据包。
drop-connection	发生违规时丢弃连接。
reset	发生违规时重置连接。
log	指定违规情况下的独立或附加日志。可将其与任何操作相关联。

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
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。

使用指南

此命令计算到目标的跳数，在到达目标之前目标不能为 0。

CR_Examples

以下示例显示如何在 SIP 检查策略映射中启用最大转发验证：

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action log
```

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

max-header-length

要根据 HTTP 标头长度限制 HTTP 流量，请在 **max-header-length** HTTP 映射配置模式下使用该命令，可以使用该 **http-map** 命令访问。要删除此命令，请使用此命令 **no** 的形式。

max-header-length { **request** 字节数 字节 [**response** 数] | **response** 字节数 } **action** { **allow** | **reset** | **drop** } [**log**]
no max-header-length { **request** 字节数 字节 [**response** 数] | **response** 字节数 } **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	当邮件未通过此命令检查时采取的操作。
allow	允许消息。
drop	关闭连接。
bytes	字节数，范围为 1 到 65535。
log	（可选）生成系统日志。
request	请求消息。
reset	向客户端和服务器发送 TCP 重置消息。
response	（可选）响应消息。

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
HTTP 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

启用 **max-header-length** 命令后，ASA 仅允许 HTTP 报头在配置的限制范围内的消息，否则采取指定的操作。使用 **action** 关键字导致 ASA 重置 TCP 连接和创建系统日志条目（可选）。

CR_Examples

以下示例将 HTTP 请求限制为 HTTP 报头长度不超过 100 个字节的请求。如果报头太大，ASA 将重置 TCP 连接并创建一个系统日志条目。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

Related Commands

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

max-lsp-lifetime

如要设置 LSP 可在不刷新的情况下保留在 ASA 数据库中的最长时间，请在路由器配置模式下使用 **max-lsp-lifetime** 命令。要恢复默认生存期，请使用此命 **no** 令的形式。

max-lsp-lifetime秒
nomax-lsp-lifetime

Syntax Description

秒LSP 的生命周期（以秒为单位）。范围为 1 到 65535。

Command Default

默认值为 1200 秒（20 分钟）。

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

如果在新 LSP 到达前超出有效期，该 LSP 将从数据库中删除。

如果使用 **lsp-refresh-interval** 命令更改了 LSP 刷新闻隔，则可能需要调整最大 LSP 有效期。在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果您错误地将 LSP 生存时间配置得与 LSP 刷新闻隔相比太低，则软件会减少 LSP 刷新闻隔以防止 LSP 超时。

您可能更愿意为每个命令使用更高的值以减少控制流量，但这样做的代价是使来自崩溃或无法访问的路由器的过时 LSP 在数据库中保留的时间更长（从而浪费内存），或增加未检测到的不良 LSP 保持活动状态的风险（非常罕见）。

CR_Examples

以下示例将 LSP 生存期配置为 40 分钟：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isipassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

maximum-paths (BGP)

要控制可安装在路由表中的并行 BGP 路由的最大数量，请在 address-family 配置模式下使用 maximum-paths 命令。要恢复默认值，请使用此命令的 no 形式。

```
maximum-paths [ibgp] number-of-paths
nomaximum-paths [ibgp] number-of-paths
```

Syntax Description	ibgp（可选）这将使您能够控制可以安装到路由表的内部 BGP 路由的最大数量。
	number-of-paths 安装到路由表中的路由数。

Command Default 默认情况下，BGP 仅在路由表中安装一个最佳路径。

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
Address-family 配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。

使用指南 maximum-paths 命令用于为 BGP 对等会话配置等价或不等价多路径负载共享。要将路由安装为 BGP 路由表中的多路径，路由的下一跳不能与已安装的另一个路由相同。配置 BGP 多路径负载共享时，BGP 路由进程仍会通告到 BGP 对等成员的最佳路径。对于等价路由，来自路由器 ID 最小的相邻设备的路径被通告为最佳路径。

要配置 BGP 等价多路径负载共享，所有路径属性必须相同。路径属性包括权重、本地优先级、自治系统路径（整个属性，而不只是长度）、源代码，多出口标识符 (MED) 和内部网关协议 (IGP) 距离。

CR_Examples

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Related Commands

命令	说明
<code>showbgp</code>	显示 BGP 路由表中的条目。

maximum-paths (IS-IS)

要为 IS-IS 协议配置多路径负载共享，请在路由器 isis 配置模式下使用 **maximum-paths** 命令。要为 ISIS 路由禁用多路径负载共享，请使用此命令的 **no** 形式。

maximum-paths*number-of-paths*
no**maximum-paths***number-of-paths*

Syntax Description

number-of-paths 要安装到路由表中的路由数。范围为 1 到 8。

Command Default

默认情况下，IS-IS 仅在路由表中安装一个最佳路径。

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 ASA 中 **maximum-paths**配置了 ECMP 时，此命令用于配置 ISIS 多路径负载共享。

CR_Examples

以下示例将路由表中的最大路径数配置为 8：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。

命令	说明
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。

命令	说明
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。

命令	说明
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

max-object-size

要设置 ASA 可为 WebVPN 会话缓存的最大对象大小，请在缓存模式下使用 `max-object-size` 命令。
要更改大小，请再次使用 命令。

max-object-size整数范围

Syntax Description

整数范 0 - 10000
围 KB

Command Default

1000 KB

Command Modes

下表显示了输入命令的模式：

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
Cache mode	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命
令。

使用指南

最大对象尺寸必须大于最小对象尺寸。如果已启用缓存压缩，ASA 会在压缩对象后计算大小。

CR_Examples

以下示例显示如何将最大对象大小设置为 4000 KB：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa (config-webvpn-cache)# max-object-size4000
ciscoasa (config-webvpn-cache)#
```

Related Commands

命令	说明
cache	进入 WebVPN 缓存模式。
cache-compressed	配置 WebVPN 缓存压缩。

命令	说明
disable	禁用缓存。
expiry-time	配置缓存对象的到期时间而不重新验证它们。
lmfactor	为仅具有最后修改时间戳的缓存对象设置重新验证策略。
min-object-size	定义要缓存的最小对象大小。

最大重试次数（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 ASA 在让请求超时之前重试失败的 SSO 身份验证的次数，请在特定 SSO 服务器类型的 webvpn 配置模式下使用 **max-retry-attempts** 命令。

要返回默认值，请使用此 **no** 命令形式。

max-retry-attempts *retries*
no **max-retry-attempts**

Syntax Description *retries* ASA 重试失败的 SSO 身份验证的次数。重试次数范围为 1 到 5。

Command Default 此命令的默认值为 3。

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
类映射类型正则表达式配置	• 是	—	• 是	—	—
config webvpn ssminder	• 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 目前支持 SiteMinder 类型的 SSO 服务器和 SAML POST 类型的 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：

- ASA 重试 SSO 身份验证尝试失败的次数。 **max-retry-attempts** 命令。
- SSO 身份验证尝试失败之前的超时秒数（参见 **request-timeout** 命令）。

CR_Examples

以下示例在 webvpn-sso-siteminder 配置模式下为名为 my-sso-server 的 SiteMinder SSO 服务器配置四次身份验证重试：

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)#max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

Related Commands

命令	说明
policy-server-secret	创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
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。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

max-uri-length

要根据 HTTP 请求消息中 URI 的长度限制 HTTP 流量，请在 HTTP 映射配置模式下使用 **max-uri-length** 命令。此模式可使用 **http-map** 命令访问。要删除此命令，请使用此命令 **no** 的形式。

max-uri-length bytes action { **allow** | **reset** | **drop** } [**log**]
no max-uri-length bytes action { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action 当邮件未通过此命令检查时采取的操作。

allow 允许消息。

drop 关闭连接。

bytes 字节数，范围为 1 到 65535。

log （可选）生成系统日志。

reset 向客户端和服务器发送 TCP 重置消息。

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
HTTP 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

启用 **max-uri-length** 命令后，ASA 仅允许 URI 在配置的限制范围内的消息，否则执行指定的操作。使用 **action** 关键字导致 ASA 重置 TCP 连接并创建系统日志条目。

允许使用长度小于或等于配置值的 URI。否则，将执行指定的操作。

CR_Examples

以下示例将 HTTP 请求限制为 URI 不超过 100 个字节的请求。如果 URI 太大，ASA 将重置 TCP 连接并创建一个系统日志条目。

```
ciscoasa(config)# http-map inbound_http
```

```
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

Related Commands

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

mcast-group

要为 VXLAN VNI 接口指定组播组，请在接口配置模式下使用 **mcast-group** 命令。要删除该组，请使用此命令 **no** 的形式。

```
mcast-group mcast_ip
no mcast-group
```

Syntax Description	mcast_ip 设置多播组 IP 地址，IPv4 或 IPv6。

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
接口配置	• 是	• 支持	• 支持	—	—

Command History	版本 修改
	9.4(1) 添加了此命令。
	9.20(1) 此命令现在支持 IPv6。

使用指南

ASA 向对等体 VTEP 后的设备发送数据包时，ASA 需要两条重要信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

ASA 可以通过两种方式找到这些信息：

- 单个对等体 VTEP IP 地址可以在 ASA 上静态配置。

无法手动定义多个对等体。

然后，ASA 将向 VTEP 发送一条 VXLAN 封装的 ARP 广播，以了解结束节点 MAC 地址。

- 可以使用该命令在每个 VNI 接口上（或在 **mcast-group** 整个 VTEP 上）配置多播组。

ASA 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 ASA 可以获悉远程 VTEP IP 地址以及远程结束节点的目标 MAC 地址。

ASA 维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

如果没有为 VNI 接口设置多播组，则使用 VTEP 源接口配置中的默认组（如果可用）（**default-mcast-group**命令）。如果使用该命令为 VTEP 源接口手动设置 VTEP 对 **peerip**等 IP，则无法为 VNI 接口指定多播组。多情景模式下不支持组播。

CR_Examples

以下示例配置 VNI 1 接口并指定组播组 236.0.0.100:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。

命令	说明
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

mcc

要在 GTP 检测中标识用于 IMSI 前缀过滤的移动国家/地区代码和移动网络代码，请在策略映射参数配置模式下使用 **mcc** 命令。要删除配置，请使用此命令的 **no** 形式。

```
[drop] mcccountrymncnetwork_code
no [drop] mcccountrymncnetwork_code
```

Syntax Description	drop 指定应丢弃与前缀组合匹配的连接。因此，组合将指示不必要的前缀。 如果没有此关键字，连接必须与允许的前缀组合匹配。 给定映射中的所有前缀过滤都必须一致，要么全部丢弃，要么全部允许。
	country_code 非零的三位数值，用于标识移动国家/地区。一位数或两位数条目将添加0前缀以创建三位数值。
	network_code 标识网络代码的两位或三位数值。

Command Default	默认情况下，GTP 检查不会检查有效的 MCC/MNC 组合。

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。
	9.16 (1) 添加了 drop 关键字。

使用指南	您可以根据需要多次输入命令，以指定所有目标 MCC/MNC 对，但策略映射中的所有命令都必须是 mcc 或 drop mcc。这些命令不能组合使用。 默认情况下，GTP 检测不检查移动国家/地区代码 (MCC)/移动网络代码 (MNC) 组合的有效性。如果配置 IMSI 前缀过滤，接收到的数据包 IMSI 中的 MCC 和 MNC 将会与配置的 MCC/MNC 组合进行比较。然后，系统会根据命令采取以下行动之一： • mcc 命令 - 如果数据包不匹配，则丢弃该数据包。 • drop mcc 命令 - 如果数据包匹配，则将其丢弃。

移动设备国家/地区代码是非零的三位数值；应在一位或两位数值前添加零作为前缀。移动网络代码是两位或三位数值。

添加您希望允许或放弃的所有 MCC 和 MNC 组合。默认情况下，ASA 不会检查 MNC 和 MCC 组合的有效性，所以您必须验证配置组合的有效性。有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议《*Identification Plan for Land Mobile Stations*》（陆地移动站识别计划）。

CR_Examples

以下示例标识需要 MCC 为 111 且 MNC 为 222 的 IMSI 前缀过滤的流量：

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

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。
showservice-policyinspectgtp	显示 GTP 配置。

media-termination (已弃用)

要指定用于至电话代理功能的媒体连接的媒体终止实例，请在电话代理配置模式下使用 **media-termination** 命令。

要从电话代理配置中删除媒体终止地址，请使用此命令的 **no** 形式。

```
media-terminationinstance_name
no media-terminationinstance_name
```

Syntax Description instance_name 指定使用介质终端地址的接口名称。每个接口只能配置一个媒体终止地址。

Command Default 此命令没有默认设置。

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

8.0(4) 命令已添加。

8.2(1) 此命令已更新，以允许使用具有媒体终止地址的 NAT。**rtp-min-port** 和 **rtp-max-ports** 关键字已从命令语法中删除，并作为单独的命令包含在内。

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

ASA 必须具有符合以下条件的媒体终端 IP 地址：

对于媒体终止实例，您可以为所有接口配置全局媒体终止地址，或为不同接口配置媒体终止地址。但是，不能同时使用全局媒体终止地址和为每个接口配置的媒体终止地址。

如果为多个接口配置媒体终端地址，则必须在 ASA 与 IP 电话通信时使用的每个接口上配置地址。IP 地址是公开的可路由地址，并且是该接口上的地址范围内未使用的 IP 地址。

请参阅《CLI 配置指南》，查看在创建介质终止实例和配置介质终止地址时必须遵循的完整前提条件列表。

CR_Examples

以下示例显示使用 media-termination address 命令来指定用于媒体连接的 IP 地址：

```
ciscoasa(config-phone-proxy) # media-termination mta_instance1
```

Related Commands

命令	说明
phone-proxy	配置电话代理实例。

media-type

要将介质类型设置为铜缆或千兆光纤以太网，请在接口配置模式下使用 **media-type** 命令。光纤 SFP 连接器在 ASA 5500 系列自适应安全设备的 4GE SSM 上可用。要将媒体类型设置恢复为默认值，请使用此命令的 **no**形式。

```
media-type {rj45 | sfp}
nomedia-type [rj45 | sfp]
```

Syntax Description	rj45 （默认）将介质类型设置为铜 RJ-45 连接器。
	sfp 将介质类型设置为光纤 SFP 连接器。

Command Default	默认值为 rj45 。

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	• 支持	• 支持	—	• 是

Command History	版本 修改
	7.0(4) 添加了此命令。

使用指南	sfp 设置使用固定速度 (1000 Mbps)，因此 speed 命令允许您设置接口是否协商链路参数。不支持该 duplex 命令。 sfp

CR_Examples	以下示例将介质类型设置为 SFP：

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands	命令	说明
	interface	配置接口并进入接口配置模式。

命令	说明
showinterface	显示接口的运行时间状态和统计信息。
showrunning-configinterface	显示接口配置。
speed	设置接口速度。

member

要将情景分配给资源类，请在情景配置模式下使用 **member** 命令。要从类中删除上下文，请使用此命令 **no** 的形式。

```
memberclass_name
nomemberclass_name
```

Syntax Description *class_name* 指定使用 **class** 命令创建的类名称。

Command Default 默认情况下，系统会将情景分配给默认类。

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
上下文配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南 默认情况下，所有安全上下文都可以无限制地访问ASA的资源，除非强制执行每个上下文的最大限制。但是，如果您发现一个或多个上下文使用了太多资源，并且导致其他上下文被拒绝连接，那么您可以配置资源管理来限制每个上下文的资源使用。ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。

CR_Examples 以下示例将情景 test 分配到 gold 类：

```
ciscoasa(config-ctx) # contexttest
ciscoasa(config-ctx) # allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx) # allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx) # allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx) # config-urlftp://user1:passwd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx) # member gold
```

命令	说明
class	创建资源类。

命令	说明
context	配置安全上下文。
limit-resource	设置资源的限制。
显示资源分配	显示如何跨类分配资源。
show resource types	显示您可以设置限制的資源类型。

member-interface

要将物理接口分配给冗余接口，请在接口配置模式下使用 **member-interface**命令。此命令仅适用于冗余接口类型。您可以向冗余接口分配两个成员接口。要删除成员接口，请使用此命 **no** 令的形式。您不能从冗余接口中同时删除两个成员接口；冗余接口至少需要一个成员接口。

member-interface*physical_interface*
no**member-interface***physical_interface*

Syntax Description *physical_interface* 标识接口ID，例如，**gigabitethernet0/1** 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。

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
接口配置	• 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 两个成员接口均必须为相同的物理类型。例如，二者都必须以太网接口。

如果已为物理接口配置了名称，则不能将该物理接口添加到冗余接口。您必须先使用 **no nameif** 命令删除名称。



注意 如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

对于属于冗余接口对的物理接口，唯一可用的配置是物理参数，例如 **speed** 和 **duplex** 命令、**description** 命令和 **shutdown** 命令。还可以输入 **default** 和 **help**等运行时命令。

如果关闭主用接口，则备用接口变为主用接口。

要更改活动接口，请输入**redundant-interface** 命令。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址会发生更改，以与当前最先列出的接口的 MAC 地址相匹配。或者，您可以为冗余接口分配一

个 MAC 地址，无论成员接口 MAC 地址如何，都会使用该 **mac-address** 地址（请参阅命令或命令 **mac-addressauto**）。当活动接口故障转移到备用接口时，将保持相同的 MAC 地址，因此流量不会中断。

CR_Examples

以下示例创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

命令	说明
clearinterface	清除命令的计数器 showinterface 。
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。
redundant-interface	更改活动成员接口。
showinterface	显示接口的运行时间状态和统计信息。

memberof

要指定此用户所属的组名列表，请在用户名属性配置模式下使用 **memberof** 命令。要从配置中删除此属性，请使用此命令 **no** 的形式。

```
memberofgroup_1[,group_2,...group_n]
no memberofgroup_1[,group_2,...group_n]
```

Syntax Description	group_1至group_n指定此用户所属的组。

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
用户名属性配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南	输入此用户所属组的名称的逗号分隔列表。

CR_Examples	以下示例是在全局配置模式下输入的，创建名为 newuser 的用户名，然后指定 newuser 是 DevTest 组和管理组的成员：

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

命令	说明
清除配置用户名	清除整个用户名数据库或仅清除指定的用户名。
show running-config username	显示指定用户或所有用户当前运行的用户名配置。

命令	说明
username	创建和管理用户名数据库。

memory appcache-threshold enable

要启用内存应用缓存阈值，请在配置模式下使用 **memoryappcache-thresholdenable**命令。要禁用，请使 **memoryappcache-threshold**, 用此命 **no**令的形式。

memoryappcache-thresholdenable
nomemoryappcache-thresholdenable

Syntax Description 此命令没有任何参数或关键字。

Command Default 在 ASA 5585-X FirePOWER SSP-60 (5585-60) 上，默认启用此 **memoryappcache-thresholdenable**命令。

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
配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.10(1)	引入了此命令。

使用指南

启用内存 appcache-threshold 会在达到特定内存阈值后限制应用程序缓存分配，以便保留内存来维持设备的稳定性和可管理性。

在 ASA 9.10.1 版本中，在 5585-60 上实施内存应用缓存阈值功能，以将应用缓存分配限制为仅通过设备的连接。

此命令将应用缓存分配阈值配置为系统内存的 85%。当内存使用率达到阈值级别时，系统会丢弃新的通过设备的连接。

命令的 **no** 形式会导致所有内存分配限制被释放以供使用，而无需验证。当前统计计数器将被保留，以维护故障排除历史记录，直到 **clearmemoryappcache-threshold** 命令被执行。

对于 9.10.1 版本，仅管理 SNP Conn Core 00 应用缓存类型。此名称与 “show mem app-cache” 的输出一致。

CR_Examples

以下示例启用 appcache-memory 阈值：

```
ciscoasa(config)# memory appcache-threshold enable
```

Related Commands

命令	说明
show memory appcache-threshold	显示内存 appcache-threshold 的状态和命中计数
clear memory appcache-threshold	清除内存应用缓存阈值的命中计数

memory delayed-free-poisoner enable

要启用延迟释放内存毒化工具，请在 **memorydelayed-free-poisonerenable**特权 EXEC 模式下使用该命令。要禁用 delayed free-memory poisoner 工具，请使用此命令的 **no** 形式。delayed free-memory poisoner 工具可用于监视可用的内存存在被应用释放后有何变化。

memorydelayed-free-poisonerenable
nomemorydelayed-free-poisonerenable

Syntax Description 此命令没有任何参数或关键字。

Command Default 该命令默认为禁用。 **memorydelayed-free-poisonerenable**

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

启用 delayed free-memory poisoner 工具对内存使用和系统性能有重大影响。该命令只能在 Cisco TAC 的监督下使用。在大量使用系统的生产环境下不应该运行此工具。

启用此工具后，ASA 上运行的应用程序释放内存的请求将被写入 FIFO 队列。当每个请求写入队列时，低级内存管理不需要的每个相关内存字节都会被写入值 0xcc，从而受到“污染”。

释放的内存请求将保留在队列中，直到应用程序所需的内存多于可用内存池中的内存为止。当需要内存时，系统会从队列中提取第一个释放的内存请求，并验证中毒的内存。

如果内存未被修改，则将其返回到较低级别的内存池，并且该工具从发出初始请求的应用程序重新发出内存请求。该过程持续进行，直到为请求的应用程序释放足够的内存。

如果中毒内存已被修改，则系统会强制崩溃并产生诊断输出以确定崩溃的原因。

delayed free-memory poisoner 工具自动定期验证队列的所有元素。也可以使用命令手动启动验证 **memorydelayed-free-poisonervvalidate**证。

若使用此命令的 **no** 形式，则队列中请求引用的所有内存不经过验证即返回到可用内存池，同时清除所有统计数据计数器。

CR_Examples

以下示例启用 delayed free-memory poisoner 工具：

```
ciscoasa# memory delayed-free-poisoner enable
```

下面是 delayed free-memory poisoner 工具检测到非法内存重用时的示例输出：

```
delayed-free-poisoner validate failed because a
    data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:          ef cd 1c a1 e1 00 00 00 | .....
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02 | #.....`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02 | ..[...`.1&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc | .....
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc | .....
025b1cd0: cc cc cc cc cc cc cc cc cc | .....
An internal error occurred. Specifically, a programming assertion was
violated. Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file. Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

<xref> 描述输出的重要部分。

表 5: 非法内存使用输出说明

字段	说明
heap region	可供请求的应用使用的地址区域以及内存区域大小。这与请求的大小不同，根据发出内存请求时系统分配内存的方式，它可能小于请求的大小。
memory address	内存中检测到故障的位置。
byte offset	字节偏移与堆区域的开头有关，可在结果用于保存以此地址开头的数据结构时用于查找修改的字段。0 或大于堆区域字节计数的值可能表示问题是低层堆数据包中的值异常。
allocated by/freed by	指示最近发出的、涉及此特定内存区域的 malloc/calloc/realloc 和释放调用的地址。
Dumping...	一个或两个内存区域的转储，具体取决于检测到的故障相距堆内存区域开头的距离。任何系统堆信头后的八个字节是此工具用来保存各系统报头散列值以及队列链路的内存。区域中在遇到任何系统堆尾部之前的所有其他字节应设置为 0xcc。

Related Commands

命令	说明
clearmemorydelayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。

命令	说明
memorydelayed-free-poisonervvalidate	强制验证延迟释放内存毒化工具队列中的元素。
showmemorydelayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。

memory delayed-free-poisoner validate

要强制验证 **memorydelayed-free-poisoner** 队列中的所有元素，请在特权 EXEC 模式下使用 **memorydelayed-free-poisonervvalidate** 命令。

memorydelayed-free-poisonervvalidate

Syntax Description

此命令没有任何参数或关键字。

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
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

在发出 **memorydelayed-free-poisonervvalidate** 命令之前，您必须使用 **memorydelayed-free-poisonerenable** 命令启用 delayed free-memory poisoner 工具。

memorydelayed-free-poisonervvalidate 命令导致 **memorydelayed-free-poisoner** 队列的每个元素被验证。如果有元素包含非预期的值，则系统发生故障并产生诊断输出来确定故障的原因。如果没有遇到意外值，元素将保留在队列中并由工具正常处理；该 **memorydelayed-free-poisonervvalidate** 命令不会导致队列中的内存返回到系统内存池。



注释 delayed free-memory poisoner 工具自动定期验证队列的所有元素。

CR_Examples

以下示例导致验证 **memorydelayed-free-poisoner** 队列中的所有元素：

```
ciscoasa# memory delayed-free-poisoner validate
```

Related Commands

命令	说明
clearmemorydelayed-free-poisoner	清除延迟的空闲内存毒化工具队列和统计信息。

命令	说明
memorydelayed-free-poisonerenable	启用延迟释放内存毒化工具。
showmemorydelayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。

memory caller-address

要为调用跟踪或调用方 PC 配置特定范围的程序内存以帮助隔离内存问题，请在 **memorycaller-address** 特权 EXEC 模式下使用该命令。调用方 PC 是调用内存分配基元的程序的地址。要删除地址范围，请使用此命令 **no** 的形式。

memorycaller-address *startPC* *endPC*
no **memorycaller-address**

Syntax Description

endPC 指定内存块的结束地址范围。

startPC 指定内存块的开始地址范围。

Command Default

实际调用方 PC 会被记录以用于内存跟踪。

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	—	• 是	• 支持

Command History

版本 修改

7.0 添加了此命令。

使用指南

使用该 **memorycaller-address** 命令将内存问题隔离到特定的内存块。

在某些情况下，内存分配基元的实际调用方 PC 是程序中许多位置使用的已知库功能。要隔离程序中的个别位置，请配置库功能的开始和结束程序地址，从而记录库功能调用方的程序地址。



注释 启用呼叫者地址跟踪时，ASA 的性能可能会暂时下降。

CR_Examples

以下示例显示了使用命令配置的 **memorycaller-address** 地址范围以及命令的 **showmemory-calleraddress** 结果显示：

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08  
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
```

```
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

命令	说明
memoryprofileenable	启用对内存使用（内存分析）的监控。
memoryprofiletext	配置要分析的内存的文本范围。
showmemory	显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
showmemorybinsize	显示为特定存储空间分配的数据块的摘要信息。
showmemoryprofile	显示有关 ASA 内存使用情况（分析）的信息。
showmemory-calleraddress	显示在 ASA 上配置的地址范围。

memory logging

要启用内存日志记录，请在 **memorylogging** 全局配置模式下使用该命令。要禁用内存日志记录功能，请使用此命令的 **no** 形式。

memory logging [**1024-4194304**] [**wrap**] [**size** [**1-2147483647**]] [**process**进程名称、] [**context**情景名称]

nomemorylogging

Syntax Description

1024-4194304	指定内存日志记录缓冲区中的日志记录条目数。这是唯一需要指定的参数。
context <i>context-name</i>	指定要监控的虚拟情景和情景名称。
process <i>process-name</i>	指定要监视的进程和进程名称。 注释 Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。
size -2147483647	指定要监控的条目的大小和数量。
wrap	回绕时保存缓冲区。缓冲区只能保存一次。如果它 wrap 多次，会被覆写。当缓冲区 wrap 时，系统会将触发器发送到事件管理器，以启用数据保存。

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	—	• 是	• 支持

Command History

版本 修改

9.4(1) 添加了此命令。

使用指南

要更改内存日志记录参数，必须将其禁用，然后重新启用。

CR_Examples

以下示例启用内存日志记录：

```
ciscoasa
(config)#
memory logging 202980
```

Related Commands

命令	说明
eventmemory-logging-wrap	启用响应内存日志记录包装事件。
showmemorylogging	显示内存日志记录结果。

memory profile enable

要启用内存使用情况监控（内存分析），请在 **memoryprofileenable** 特权 EXEC 模式下使用该命令。要禁用内存分析功能，请使用此命令的 **no** 形式。

memoryprofileenablepeakpeak_value
nomemoryprofileenablepeakpeak_value

Syntax Description

peak_value 指定内存使用阈值，达到此阈值就会在峰值使用缓冲区中保存内存使用率快照。此缓冲区的内容以后可用来分析以确定系统的峰值内存需求。

Command Default

内存分析默认禁用。

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
特权 EXEC	• 是	• 支持	—	• 是	• 支持

Command History

版 修改
本

7.0 添加了此命令。

使用指南

在启用内存分析之前，您必须首先使用该命令配置要分析的 **memoryprofiletext** 内存文本范围。

在您输入命令之前，分析系统会保留一些内 **clearmemoryprofile** 存。查看命令的 **showmemorystatus** 输出。



注释 启用内存分析时，ASA 的性能可能会暂时下降。

以下示例启用内存分析：

```
ciscoasa# memory profile enable
```

Related Commands

命令	说明
memoryprofiletext	配置要分析的内存的文本范围。

命令	说明
showmemoryprofile	显示有关 ASA 内存使用情况（分析）的信息。

memory profile text

要配置要分析的程序文本内存范围，请在 **memoryprofiletext** 特权 EXEC 模式下使用该命令。要禁用此功能，请使用此命令的 **no** 形式。

memoryprofiletext { *startPC* *endPC* | **all** *resolution* }
nomemoryprofiletext { *startPC* *endPC* | **all** *resolution* }

Syntax Description

all 指定内存块的整个文本范围。

endPC 指定内存块的整个文本范围。

resolution 指定源文本区域的跟踪分辨率。

startPC 指定内存块的开始文本范围。

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
特权 EXEC	• 是	• 支持	—	• 是	• 支持

Command History

版 修改
本

7.0 添加了此命令。

使用指南

如果文本范围小，分辨率“4”通常便可跟踪对指令的调用。如果文本范围较大，低分辨率对第一遍可能够了，但在下一遍时范围可能需要缩小到一组更小的区域。

使用命令输入文本范围 **memoryprofiletext** 后，您必须输入命令来开始内 **memoryprofileenable** 存分析。内存分析默认禁用。



注释 启用内存分析时，ASA 的性能可能会暂时下降。

CR_Examples

以下示例显示如何配置要分析的文本范围的内存，分辨率为 4：

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

以下示例显示文本范围的配置和内存分析的状态 (OFF):

```
ciscoasa# show memory profile
InUse profiling: OFF Peak profiling: OFF Profile: 0x004018b4-0x004169d0 (00000004)
```



注释 要开始内存分析，您必须输入 **memoryprofileenable**命令。内存分析默认禁用。

Related Commands

命令	说明
clearmemoryprofile	清除内存分析功能保留的缓冲区。
memoryprofileenable	启用对内存使用（内存分析）的监控。
showmemoryprofile	显示有关ASA内存使用情况（分析）的信息。
showmemory-calleraddress	显示在 ASA 上配置的地址范围。

memory-size

要配置 WebVPN 的各种组件可访问的 ASA 上的内存量，请在 webvpn 模式下使用 **memory-size** 命令。您可以将内存量配置为设定的内存量（以 KB 为单位）或总内存的百分比。要删除已配置的内存大小，请使用此命令的 **no** 形式。



注释 需要重新启动才能使新的内存大小设置生效。

memory-size { percent | kb } size
nomemory-size [{ percent | kb } size]

Syntax Description

kb	指定内存量（以千字节为单位）。
percent	在 ASA 上指定内存量占总内存的百分比。
size	以 KB 为单位或以总内存的百分比的形式指定内存量。

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
Webvpn 模式	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

将立即分配配置的内存量。在配置此命令之前，请使用 **show memory** 检查可用内存量。如果使用总内存的一定百分比进行配置，请确保配置的值低于可用百分比。如果使用千字节值进行配置，请确保配置的值小于可用内存量（以千字节为单位）。

CR_Examples

以下示例显示如何将 WebVPN 内存大小配置为 30%：

```
ciscoasa
(config)#
webvpn
```

```
ciscoasa
(config-webvpn)#
memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

Related Commands

命令	说明
showmemorywebvpn	显示 WebVPN 内存使用统计信息。

memory tracking enable

要启用堆内存请求的跟踪，请在 **memorytrackingenable** 特权 EXEC 模式下使用该命令。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

memorytrackingenable
nomemorytrackingenable

Syntax Description 此命令没有任何参数或关键字。

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
特权 EXEC	• 是	• 支持	—	• 是	• 支持

Command History 版本 修改

7.0(8) 添加了此命令。

使用指南 使用 **memorytrackingenable** 命令跟踪堆内存请求。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

在启用内存跟踪之前，请确保将 **app-agent heartbeat** 命令中的默认间隔和计数值更改为以下值：

app-agent heartbeat interval 6000 retry-count 6

CR_Examples 以下示例启用跟踪堆内存请求：

```
ciscoasa# memory tracking enable
```

Related Commands

命令	说明
clearmemorytracking	清除所有当前收集的信息。
showmemorytracking	显示当前分配的内存。
showmemorytrackingaddress	列出工具跟踪的每个当前分配的内存块的大小、位置和最顶层调用函数。

命令	说明
showmemorytrackingdump	此命令显示给定内存地址的大小、位置、部分调用堆栈和内存转储。
showmemorytrackingdetail	显示用于深入了解工具内部行为的各种内部细节。

memory-utilization

使用 `memory usage` 命令将 ASA 配置为在系统内存用尽量达到预定义级别后自动重新启动或使 ASA 崩溃。一旦内存使用率达到配置的阈值限制，系统就会自动重新加载。阈值的范围可能为 90-99%。

memory-utilizationreload-threshold<%>
memory-utilizationreload-threshold<%> [**crashinfo**]

Syntax Description

reload-threshold 指定系统内存限制阈值。

crashinfo (可选) 指定使用崩溃信息后，系统会在系统重新加载之前保存崩溃信息。

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	• 支持	• 支持	—

Command History

版本 修改

9.7(1) 添加了此命令。

使用指南

建议您不要在已知处于高内存使用率环境中的系统上配置此功能。使用可选的 `crashinfo` 参数在系统重新加载之前生成崩溃信息文件。

CR_Examples

以下示例显示了如何在 ASA 上配置内存利用率功能：

```
ciscoasa# memory-utilization reload-threshold 95
```

Related Commands

命令	说明
memoryprofiletext	配置要分析的内存的文本范围。
memoryprofileenable	启用对内存使用（内存分析）的监控。
clearmemoryprofile	清除内存分析功能保留的缓冲区。
showmemoryprofile	显示有关 ASA 内存使用情况（分析）的信息。

merge-dacl

要将可下载的 ACL 与从 RADIUS 数据包的 Cisco AV 对中接收的 ACL 合并，请在 **merge-dacl**aaa-server group 配置模式下使用该命令。要禁用可下载 ACL 与从 RADIUS 数据包的 Cisco AV 对中接收的 ACL 的合并，请使用此命令的 **no**形式。

```
mergedacl { before_avpair | after_avpair }
nomergedacl
```

Syntax Description

after_avpair 指定可下载的 ACL 条目应放置在 Cisco AV 对条目之后。此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。

before_avpair 指定可下载的 ACL 条目应放置在 Cisco AV 对条目之前。

Command Default

默认设置为 **nomergedacl**，指定可下载的 ACL 不会与 Cisco AV 对 ACL 合并。

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 group 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。

CR_Examples

以下示例指定可下载的 ACL 条目应放置在 Cisco AV 对条目之前：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

Related Commands

命令	说明
aaa-serverhost	标识服务器及其所属的 AAA 服务器组。

命令	说明
aaa-serverprotocol	确定服务器组名称和协议。
max-failed-attempts	指定在尝试下一个服务器之前向组中的 AAA 服务器发送的最大请求数。

message-authenticator-required

要指定 Message-Authenticator 属性必须存在于 RADIUS 请求和响应中，请在 **message-authenticator-required**aaa-server 主机配置模式下使用该命令。要禁用消息身份验证器要求，请使用此命令的 **no** 形式。

message-authenticator-required
no message-authenticator-required

Syntax Description 此命令没有任何参数或关键字。

Command Default 不需要消息身份验证器 (Message-Authenticator) 属性。

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服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
923(1)	添加了此命令。

使用指南 Message-Authenticator 属性用于防御 Blast-RADIUS 攻击。如果已升级 RADIUS 服务器使其支持消息身份验证器，则可以启用此选项来帮助防御这些攻击。启用后，所有请求和响应都必须有消息身份验证器，否则身份验证将失败。

示例

以下示例启用该功能

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-host)# message-authenticator-required
```

命令	说明
aaa-server host	标识 AAA 服务器组的 AAA 服务器。

message-length

要过滤不符合配置的最大长度的 DNS 数据包，请在参数配置模式下使用 `message-length` 命令。使用 `no` 表单删除该命令。

message-lengthmaximum { 长度 | **client** { 长度 | **auto** } | **server** { 长度 | **auto** } }

no message-lengthmaximum { 长度 | **client** { 长度 | **auto** } | **server** { 长度 | **auto** } }

Syntax Description

length	DNS 消息中允许的最大字节数，从 512 到 65535。
client { <i>length</i> auto }	客户端 DNS 消息中允许的最大字节数，从 512 到 65535，或 auto 将最大长度设置为资源记录中的值。
server { <i>length</i> auto }	服务器 DNS 消息中允许的最大字节数，范围为 512 到 65535，或使用 auto 将最大长度设置为资源记录中的值。

Command Default

默认检测将 DNS 最大消息长度设置为 512，并将客户端长度设置为 **auto**。

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

您可以将最大 DNS 消息长度配置为 DNS 检测映射中的参数。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中配置最大 DNS 消息长度：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

Related Commands

命令	说明
parameter	在策略图配置模式下进入参数配置模式。

命令	说明
policy-map type inspect dns	创建 DNS 检测策略映射。

message-tag-validation

要验证 M3UA 消息中某些字段的内容，请在参数配置模式下使用 **message-tag-validation** 命令。首先输入命令即可进入参数配置 **policy-map type inspect m3ua** 模式。使用此命令的形式来删除设置。

message-tag-validation { **dupu** | **error** | **notify** }
no message-tag-validation { **dupu** | **error** | **notify** }

Syntax Description

dupu 启用对目的用户部分不可用 (DUPU) 消息的验证。用户/原因字段必须存在，并且必须仅包含有效的原因和用户代码。

error 为错误消息启用验证。所有必填字段必须存在并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。

notify 为通知消息启用验证。状态类型和状态信息字段必须仅包含允许的值。

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
参数配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.7(1) 添加了此命令。

使用指南

使用此命令确保针对指定的 M3UA 消息类型检查并验证某些字段的内容。验证失败的消息将被丢弃。

CR_Examples

以下示例在 M3UA 检测中启用对 DUPU、错误和通知消息的消息验证。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

Related Commands

命令	说明
inspectm3ua	启用 M3UA 检测。
policy-maptypeinspect	创建检查策略映射。
showservice-policyinspectm3ua	显示 M3UA 统计信息。

metric

要全局更改所有 IS-IS 接口的指标值，请在路由器 isis 配置模式下使用 **metric** 命令。要禁用指标值并恢复默认指标值 10，请使用此命令的 **no** 形式。

```
metric default-value [level-1 | level-2]
no metric default-value [level-1 | level-2]
```

Syntax Description	默认 分配给链路并用于计算通过链路到目的地的路径成本的度量值。范围为 1 到 63。 值
	level-1 （可选）设置 IS-IS 第 1 级 IPv4 或 IPv6 度量。
	level-2 （可选）设置 IS-IS 第 2 级 IPv4 或 IPv6 度量。

Command Default	默认值为 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
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 当需要更改所有 IS-IS 接口的默认度量值时，建议您使用 in 命令对 **metric**所有接口进行全局配置。以全局方式配置指标值可以防止出现用户错误，如从某一接口意外删除已设置的指标，而又没有配置新值，并且意外允许该接口恢复为默认指标 10，从而成为网络中的高度优先接口。

输入命令 **metric** 更改默认 IS-IS 接口指标值后，已启用的接口将使用新值而不是默认值 10。被动接口继续使用指标值 0。

CR_Examples 以下示例将 IS-IS 接口配置为全局度量为 111：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isipassword	配置接口的认证密码。EXTEN
isipriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

metric-style

要配置运行 IS-IS 的路由器，使其仅生成和接受新式类型、长度、值对象 (TLV)，请在路由器 isis 配置模式下使用 **metric-style** 命令。要禁用该功能，请使用此命令的 **no** 形式。

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
nometric [**level-1** | **level-2** | **level-1-2**]

Syntax Description

narrow 指示 ASA 使用具有窄度量的旧式 TLV。

transition （可选）指示 ASA 在过渡期间接受旧式和新式 TLV。

wide 指示 ASA 使用新样式的 TLV 来承载更广泛的度量。

level-1 （可选）在路由级别 1 上启用此命令。

level-2 （可选）在路由级别 2 上启用此命令。

level-1-2 （可选）指示路由器接受旧式和新式 TLV。

Command Default

默认值为 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
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

如果输入 **metric-space** 宽命令，则 ASA 仅生成和接受新式 TLV。因此，与同时生成旧式和新式 TLV 时相比，ASA 使用的内存和其他资源更少。

此样式适用于跨整个网络启用 MPLS 流量工程。

CR_Examples

以下示例将 ASA 配置为在第 1 级生成和接受新式 TLV：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertise-prefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
ispriority	配置接口上指定 ASA 的优先级。
isiprotocolshutdown	禁用每个接口的 IS-IS 协议。
isiretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isiretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

命令	说明
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。



mf – mz

- [mfib forwarding](#) , 第 868 页
- [迁移](#) , 第 869 页
- [min-object-size](#) , 第 871 页
- [mkdir](#) , 第 873 页
- [mobile-device portal](#) , 第 875 页
- [mode](#) , 第 876 页
- [monitor-interface](#) , 第 878 页
- [more](#) , 第 880 页
- [mount type cifs](#) , 第 883 页
- [mount type ftp](#) , 第 885 页
- [mroute](#) , 第 887 页
- [mschapv2-capable](#) , 第 889 页
- [msie-proxy except-list](#) , 第 891 页
- [msie-proxy local-bypass](#) , 第 893 页
- [msie-proxy lockdown](#) , 第 894 页
- [msie-proxy method](#) , 第 896 页
- [msie-proxy pac-url](#) , 第 898 页
- [msie-proxy server](#) , 第 900 页
- [mtu](#) , 第 902 页
- [mtu cluster](#) , 第 904 页
- [multicast boundary](#) , 第 905 页
- [multicast-routing](#) , 第 907 页
- [mus](#) , 第 909 页
- [mus host](#) , 第 911 页
- [mus password](#) , 第 913 页
- [mus server](#) , 第 915 页

mfib forwarding

要重新启用接口上的 MFIB 转发，请在 **mfibforwarding** 接口配置模式下使用该命令。要禁用接口上的 MFIB 转发，请使用此命令 **no** 的形式。

mfibforwarding
nomfibforwarding

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下， **multicast-routing** 命令可在所有接口上启用 MFIB 转发。

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
7.1(1)	添加了此命令。

使用指南

当您启用组播路由时，默认情况下将在所有接口上启用 MFIB 转发。使用命令的 **no** 形式可在特定接口上禁用 MFIB 转发。只有 **no** 形式会出现在运行配置中。

在接口上禁用 MFIB 转发时，除非通过其他方法进行专门配置，否则该接口不接受任何组播数据包。当禁用 MFIB 转发时，也会阻止 IGMP 数据包。

CR_Examples

以下示例在指定接口上禁用 MFIB 转发：

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

命令	说明
multicast-routing	启用多播路由。
pim	在接口上启用 PIM。

迁移

要将 LAN 间 (IKEv1) 或远程访问配置 (SSL 或 IKEv1) 迁移到 IKEv2，请在全局配置模式下使用 migrate 命令：

migrate { **l2l** | **remote-access** { **ikev2** | **ssl** } | **overwrite** }

Syntax Description	l2l	将 IKEv1 LAN 间配置迁移到 IKEv2。
	remote-access	指定远程访问配置。
	ikev2	将远程访问 IKEv1 配置迁移到 IKEv2。
	ssl	将远程访问 SSL 配置迁移到 IKEv2。
	覆盖	覆盖现有 IKEv2 配置。

Command Default 没有默认值或行为。

Command Modes 下表显示了输入命令的模式：

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
	8.4(1)	添加了此命令。
	9.0(1)	增加了多情景模式支持。

使用指南 **migratel2l** 命令将所有 LAN 间 IKEv1 配置迁移到 IKEv2。

如果使用 **overwrite** 关键字，ASA 会使用迁移的命令覆盖任何现有 IKEv2 配置，而不是将其合并。

migrateremote-access 命令将 IKEv1 或 SSL 设置迁移到 IKEv2，但您仍必须执行以下配置任务：

- 在 webvpn 配置模式下加载 Secure Client 个软件包文件。
- 配置 Secure Client 配置文件，并为组策略指定它们。
- 请将用于 IKEv1 连接的任何自定义对象与用于 IKEv2 连接的隧道组关联。

- 使用 **cryptoikev2remote-access-trust-point** 命令指定服务器身份验证身份证书（信任点）。ASA 使用信任点自行向通过 IKEv2 连接的远程 Secure Client 进行身份验证。
- 除默认隧道组或组策略（DefaultWEBVPNGroup 隧道组和默认策略组配置为允许 IKEv2 或 SSL）外，请为您可能已配置的任何隧道组或组策略指定 IKEv2 和/或 SSL。
- 在隧道组中配置组别名或组 URL，以使客户端能够连接到默认组以外的组。
- 更新任何外部组策略和/或用户记录。
- 任何其他全局、隧道组、组策略设置来更改客户端行为。
- 使用 **cryptoikev2enable** 为 IKEv2 配置客户端用于下载文件和/或执行软件升级的端口。<interface> [client-services [port]] 命令设置。

Related Commands

命令	说明
cryptoikev2enable	在 IPsec 对等体通信的接口上启用 IKEv2 协商。
showrun cryptoikev2	显示 IKEv2 配置信息。

min-object-size

要设置 ASA 可为 WebVPN 会话缓存的最小对象大小，请在缓存模式下使用 min-object-size 命令。要更改大小，请再次使用 命令。要设置最小对象大小，请输入值零 (0)。

min-object-size整数范围

Syntax Description

整数范 0 - 10000
围 KB。

Command Default

默认大小为 0 KB。

Command Modes

下表显示了输入命令的模式：

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
缓存配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

最小对象尺寸必须小于最大对象尺寸。如果已启用缓存压缩，ASA 会在压缩对象后计算大小。

CR_Examples

以下示例显示如何将最大对象大小设置为 40 KB：

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
cache
ciscoasa(config-webvpn-cache)# min-object-size40
ciscoasa(config-webvpn-cache)#
```

Related Commands

命令	说明
cache	进入 WebVPN 缓存模式。
cache-compressed	配置 WebVPN 缓存压缩。

命令	说明
disable	禁用缓存。
expiry-time	配置缓存对象的到期时间而不重新验证它们。
lmfactor	为仅具有最后修改时间戳的缓存对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。

mkdir

要创建新目录，请在 **mkdir** 特权 EXEC 模式下使用该命令。

mkdir [**/noconfirm**] [**disk0:** | **disk1:** | | **flash:**] *path*

Syntax Description

noconfirm	（可选）抑制确认提示。
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。在 ASA 5500 系列自适应安全设备中，该 flash 关键字的别名为 disk0 。
<i>path</i>	要创建的目录的名称和路径。

Command Default

如果不指定路径，则会在当前工作目录中创建目录。

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

如果已存在同名目录，则不会创建新目录。

CR_Examples

以下示例显示如何创建名为 “backup” 的新目录：

```
ciscoasa# mkdir backup
```

Related Commands

命令	说明
cd	将当前工作目录更改为指定的目录。
dir	系统随即会显示目录的内容。

命令	说明
rmdir	删除指定的目录。
pwd	显示当前工作目录。

mobile-device portal

要将所有移动设备的无客户端 VPN 访问 Web 门户从迷你门户更改为完整浏览器门户，请在 webvpn 配置模式下使用 **mobile-deviceportal** 命令。您只需对运行 Windows CE 等旧版操作系统的智能手机进行此配置。使用现代智能手机则无需配置此选项，因为它们默认使用完整浏览器门户。

mobile-deviceportal { full }
nomobile-deviceportal { full }

Syntax Description

mobile-deviceportal{full} 为所有移动设备将无客户端 VPN 访问门户从迷你门户更改为支持完整浏览器的门户。

Command Default

运行 命令之前，默认行为是某些移动设备通过迷你门户获得无客户端 VPN 访问，而某些移动设备使用完整门户。

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 configuration	• 是	—	• 是	—	—

Command History

版本 修改

8.2(5) 此命令是在 8.2(5) 和 8.4(2) 中同时添加的。

8.4(2) 此命令是在 8.2(5) 和 8.4(2) 中同时添加的。

使用指南

仅当思科 Technical Assistance Center (TAC) 建议您使用时，才使用此命令。

CR_Examples

将无客户端 VPN 访问门户更改为所有移动设备的完整浏览器门户。

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

Related Commands

命令	说明
show running-config webvpn	显示 webvpn 的运行配置。

mode

要将安全情景模式设置为单一或多个，请在全局配置模式下使用 **mode** 命令。您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个环境都像一个独立的设备，有自己的安全策略、接口和管理员。多个环境类似于拥有多个独立设备。在单模式下，ASA 具有单配置，并且作为单设备运行。在多模式下，您可以创建多个情景，每个情景都有自己的配置。允许的情景数量取决于您的许可证。

mode { **single** | **multiple** } [**noconfirm**]

Syntax Description	multiple	设置多情景模式。
	noconfirm	（可选）设置模式而不提示您确认。该选项对于自动化脚本非常有用。
	single	将情景模式设置为单情景模式。

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	• 支持	—	• 是

Command History	版本	修改
	7.0(1)	添加了此命令。

使用指南 在多情景模式下，ASA 包含每个情景的配置，用于标识安全策略、接口以及您可以在独立设备上配置的几乎所有选项（请参阅命令 **config-url** 以识别情景配置位置）。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，是启动配置。系统配置可标识 ASA 的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

当您使用 **mode** 命令更改情景模式时，系统会提示您重新启动。

情景模式（单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果需要将配置复制到另一台设备，请使用命令将新设备上的模式设置为匹配 **mode** 配置。

当您从单一模式转换为多模式时，ASA 会将运行配置转换为两个文件：包含系统配置的新启动配置和包含管理上下文的 **admin.cfg**（位于内部闪存的根目录中）。原始运行配置保存为 **old_running.cfg**

（在内部Flash存储器的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为“admin”。

如果从多模式转换为单模式，可能需要先将完整的启动配置（如果可用）复制到 ASA。从多模式继承的系统配置并非单模式设备的完整运行配置。

并非所有功能都支持多上下文模式。有关详细信息，请参阅 CLI 配置指南。

CR_Examples

以下示例将模式设置为多：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting...
Booting system, please wait...
```

以下示例将模式设置为单一：

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting...
Booting system, please wait...
```

Related Commands

命令	说明
context	在系统配置中配置情景并进入情景配置模式。
showmode	显示当前情景模式（单模式或多模式）。

monitor-interface

要在特定接口上启用运行状况监控，请在全局配置模式下使用 **monitor-interface** 命令。要禁用接口监控，请使用此命 **no** 令的形式。

```
monitor-interface { if_name | service-module }
nomonitor-interface { if_name service-module }
```

Syntax Description	if_name	指定被监控的接口的名称。
	service-module	监控服务模块。如果您不希望硬件模块故障（例如 ASA FirePOWER 模块）触发故障转移，则可以使用此命令的 no 形式禁用模块监控。

Command Default 默认情况下，启用物理接口和服务模块监控；请参阅对逻辑接口的监控默认被禁用。

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	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.3(1) 添加了 service-module 关键字。

使用指南 可以为 ASA 监控的接口数因平台而异，并且可通过查看 **showfailover** 命令输出来确定。

ASA 故障转移对之间在每个接口轮询频率时间段内交换 Hello 消息。故障转移接口轮询时间为 3 至 15 秒。例如，如果轮询时间设置为 5 秒，则如果在接口上未侦听到 5 个连续呼叫（25 秒），则开始在该接口上进行测试。

- 监测的故障切转移口可以具有以下状态：
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
 - Normal - 接口正在接收流量。
 - Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
 - Link Down - 接口或 VLAN 通过管理方式关闭。
 - No Link - 接口的物理链路关闭。

- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

在主用/主用故障转移中，此命令仅在某个情景中有效。

CR_Examples

以下示例对名为 “inside” 的接口启用监控：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfiguremonitor-interface	恢复所有接口的默认接口运行状况监控。
failoverinterface-policy	指定要进行故障转移，必须被监控的接口的数量或百分比。
failoverpolltime	指定接口上 hello 消息之间的间隔（主用/备用故障转移）。
polltimeinterface	指定接口上 hello 消息之间的间隔（主用/主用故障转移）。
showrunning-configmonitor-interface	显示正在 monitor-interface 运行的配置中的命令。

more

要显示文件的内容，请在 **more** 特权 EXEC 模式下使用该命令。

more {/ascii | /binary | /ebcdic /disk0: | disk1: | flash: | ftp: | http: | https: | system: | tftp: } 文件名

Syntax Description

/ascii	（可选）在二进制模式下显示二进制文件和 ASCII 文件。
/binary	（可选）在二进制模式下显示任何文件。
/ebcdic	（可选）以 EBCDIC 显示二进制文件。
disk0:	（可选）显示内部闪存上的文件。
disk1:	（可选）显示外部闪存卡上的文件。
filename	指定要显示的文件的名称。
flash:	（可选）指定内部闪存，后跟冒号。在 ASA 5500 系列自适应安全设备中，该关 flash 键字的别名为 。 disk0
ftp:	（可选）显示 FTP 服务器上的文件。
http:	（可选）显示网站上的文件。
https:	（可选）显示安全网站上的文件。
system:	（可选）显示文件系统。
tftp:	（可选）显示 FTP 服务器上的文件。

Command Default

ASCII 模式

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

morefilesystem: 命令提示您输入本地目录或文件系统的别名。



注释 当您查看使用 **more** 命令保存的配置文件时，配置文件中的隧道组密码以明文显示。

CR_Examples

以下示例显示如何显示名为 “test.cfg” 的本地文件的内容：

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
```

more

```
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

命令	说明
cd	更改为指定的目录。
pwd	系统随即会显示当前工作目录。

mount type cifs

要使安全设备可以访问通用互联网文件系统 (CIFS)，请在全局配置模式下使用 **mounttypecifs** 命令。此命令允许您进入 **mount cifs** 配置模式。要卸载 CIFS 网络文件系统，请使用此命令的 **no** 形式。

```
mounttypecifs server server-name share shared {statusenable|statusdisable} [domain domain-name] username username password password
[no] mounttypecifs server server-name share shared {statusenable|statusdisable} [domain domain-name] username username password password
```

Syntax Description

域 域名	(可选) 此参数仅用于 CIFS 文件系统，指定 Windows NT 域名。最多允许 63 个字符。
<i>name</i>	指定要分配给本地 CA 的现有文件系统的名称。
password 密码	标识文件系统安装的授权密码。
servers server-name	指定 CIFS 文件系统服务器的预定义名称（或 IP 地址，采用点分十进制表示法）。
share 共享名称	按名称明确标识特定服务器共享（文件夹），以访问服务器中的文件数据。
statusenable 或者 disable	将文件系统的状态标识为已安装或已取消安装（可用或不可用）。
user username	用于安装文件系统的授权用户名。

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	• 支持	—	• 是

Command History

版本 修改

8.0(2) 添加了此命令。

使用指南

mount 命令使用可安装文件系统 (IFS) 来安装 CIFS 文件系统。IFS 是文件系统 API，使安全设备能够识别并加载文件系统的驱动程序。

该 **mount**命令将安全设备上的 CIFS 文件系统附加到 UNIX 文件树。相反， **nomount** 命令会将其分离。

其他 CLI 命令使用 **mount** 命令中指定的 安装名称 来指代安全设备上已安装的文件系统。例如，为本地证书颁发机构设置文件存储的 **database**命令需要现有已安装文件系统的安装名称，以便将数据库文件保存到非闪存。

CIFS 远程文件访问协议与应用在本地磁盘和网络文件服务器上共享数据的方式兼容。CIFS 在 TCP/IP 上运行并使用互联网的全局 DNS，是 Microsoft 的开放式跨平台服务器消息块 (SMB) 协议的增强版，SMB 协议是 Windows 操作系统中的本地文件共享协议。

使用 **mount**命令后，始终从根 shell 退出。在 mount-cifs-config 模式下使用 **exit** 关键字会使用户返回到全局配置模式。

要重新连接，请重新映射到存储的连接。



注释 支持安装 CIFS 和 FTP 文件系统。（请参阅 **mountname typeftp**命令。）此版本不支持安装网络文件系统 (NFS) 卷。

CR_Examples

以下示例将 *cifs://amer;chief:BIG-Boy@myfiler02/my_share* 装载为标签 *cifs_share*:

```
ciscoasa
(config)#
mount cifs_share type CIFS

ciscoasa (config-mount-cifs)#
server myfiler02a
```

Related Commands

命令	说明
调试 cif	记录 CIFS 调试消息。
debug ntdomain	记录 Web VPN NT 域调试消息
debugwebvpncifs	记录 WebVPN CIFS 调试消息。
dir all-file systems	显示 ASA 上安装的所有文件系统的文件。

mount type ftp

要使安全设备可访问文件传输协议 (FTP) 文件系统，请在全局配置模式下使用 **mounttypeftp** 命令进入 mount FTP 配置模式。**nomounttypeftp** 命令用于卸载 FTP 网络文件系统。

[no]**mounttypeftp** *server-name path name* {*statusenable* | *statusdisable*} {*modeactive* | *modepassive*} *username username* *password password*

Syntax Description	modeactive 或者 passive 将 FTP 传输模式标识为主动或被动。				
	否	删除已安装的 FTP 文件系统，使其不可访问。			
	password 密码	标识文件系统安装的授权密码。			
	path 路径名	指定 FTP 文件系统服务器的目录路径名。路径名不能包含空格。			
	server <i>server-name</i>	指定 FTPFS 文件系统服务器的预定义名称（或采用点分十进制表示法的 IP 地址）。			
	statusenable 或者 disable	将文件系统的状态标识为已安装或已卸载（可用或不可用）。			
	username <i>username</i>	指定用于文件系统安装的授权用户名。			

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	• 支持	—	• 是

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南 **mountname typeftp** 命令使用可安装文件系统 (IFS) 挂载指定的网络文件系统。IFS 是文件系统 API，使安全设备能够识别并加载文件系统的驱动程序。

要确认实际已安装 FTP 文件系统，请使用 **dirall-filesystems** 指令

当其他 CLI 命令引用已在安全设备上安装的文件系统时，将使用 **mount** 命令中指定的安装名称。例如，为本地证书颁发机构设置文件存储的 **database**命令需要已安装文件系统的安装名称，以便将数据库文件保存到非闪存。



注释 创建 FTP 类型安装时使用 **mount** 命令要求 FTP 服务器必须为 UNIX 目录列表样式。Microsoft FTP 服务器默认采用 MS-DOS 目录列表样式。



注释 支持安装 CIFS 和 FTP 文件系统。（请参阅 **mountname typeftp**命令。）此版本不支持安装网络文件系统 (NFS) 卷。

CR_Examples

此示例将 `ftp://amor;chief:Big-kid@myfiler02` 装载为标签 `my ftp`:

```
ciscoasa
(config)#
mount myftp type ftp server myfiler02a path status enable username chief password big-kid
```

Related Commands

命令	说明
debugwebvpn	记录 WebVPN 调试消息。
ftp mode passive	控制 ASA 上的 FTP 客户端与 FTP 服务器之间的交互。

mroute

要配置静态多播路由，请在 **mroute** 全局配置模式下使用该命令。要删除静态多播路由，请使用此命令 **no** 的形式。

```
mroutesrcsmask { in_if_name [ denseoutput_if_name ] | rpf_addr } [ distance ]  
nomroute srcsmask { in_if_name [ denseoutput_if_name ] | rpf_addr } [ distance ]
```

Syntax Description

denseoutput_if_name （可选）密集模式输出的接口名称。

denseoutput_if_name 关键字和参数对仅支持 SMR 存根多播路由（igmp 转发）。

distance （可选）路由的管理距离。距离较短的路由具有优先权。默认值为 0。

in_if_name 指定组播路由的传入接口名称。

rpf_addr 指定组播路由的传入接口。如果 RPF 地址 PIM 邻居，则会向其发送 PIM 加入消息、移植消息和删除消息。**rpf-addr** 参数可以是直接连接的系统的主机 IP 地址，也可以是网络/子网号。如果是路由，则会从单播路由表中执行递归查找，以查找直连系统。

smask 指定组播源网络地址掩码。

src 指定组播源的 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
全局配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

此命令允许您静态配置组播源所在的位置。ASA 希望在其用于将单播数据包发送到特定源的同一接口上接收组播数据包。在某些情况下，例如绕过不支持多播路由的路由，多播数据包可能会采用与单播数据包不同的路径。

静态组播路由不能通告或重分布。

使用该 **showmroute** 命令显示多播路由表的内容。使用该 **showrunning-configmroute** 命令显示运行配置中的 **mroute** 命令。

CR_Examples

以下示例显示如何使用 **mroute** 命令配置静态组播路由：

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

命令	说明
clearconfiguremroute	从配置中 mroute 删除命令。
showmroute	显示 IPv4 多播路由表。
showrunning-configmroute	显示配 mroute 置中的命令。

mschapv2-capable

要对 RADIUS 服务器启用 MS-CHAPv2 身份验证请求，请在 `aaa-server` 主机配置模式下使用 `mschapv2-capable` 命令。要禁用 MS-CHAPv2，请使用此命令的形式。

mschapv2-capable
nomschapv2-capable

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下会启用 MS-CHAPv2。

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 服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.2(1) 添加了此命令。

使用指南

要启用 MS-CHAPv2 作为 ASA 和 RADIUS 服务器之间用于 VPN 连接的协议，必须在隧道组常规属性中启用密码管理。启用密码管理会生成一个从 ASA 向 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 `password-management` 命令的描述。

如果在隧道组中使用双重身份验证并启用密码管理，则主身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则可以使用该命令配置该服务器发送非 MS-CHAPv2 身份验证请求 `nomschapv2-capable` 求。

CR_Examples

以下示例为 RADIUS 服务器 `authsrv1.cisco.com` 禁用 MS-CHAPv2：

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

Related Commands

命令	说明
aaa-server host	标识 AAA 服务器组的 AAA 服务器。
password-management	当您配置密码管理命令时，ASA 会在远程用户登录时通知用户当前密码即将过期或已过期。然后，ASA 为用户提供机会更改密码。
secondary-authentication-server-group	指定备用 AAA 服务器组，不能是 SDI 服务器组。

msie-proxy except-list

要在客户端设备上配置本地旁路的浏览器代理例外列表设置，请在 **msie-proxyexcept-list** 策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy except-list { *valueserver* [:*port*] | **none** }
nomsie-proxyexcept-list

Syntax Description

none 表示没有 IP 地址/主机名或端口，并阻止继承例外列表。

valueserver:port 指定适用于此客户端设备的 MSIE 服务器和端口的 IP 地址或名称。端口号可选。

Command Default

默认情况下，会禁用 msie-proxy except-list。

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

7.2(1) 添加了此命令。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南3.1 版》或移动设备的 [版本说明](#)。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略设置 Microsoft Internet Explorer 代理例外列表，该列表由 IP 地址为 192.168.20.1、使用端口 880 的服务器组成：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。

命令	说明
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy local-bypass

要为客户端设备配置浏览器代理本地旁路设置，请在 **msie-proxylocal-bypass** 策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxylocal-bypass { **enable** | **disable** }
no **msie-proxylocal-bypass** { **enable** | **disable** }

Syntax Description

disable 禁用客户端设备的浏览器代理本地绕行设置。

enable 启用客户端设备的浏览器代理本地绕行设置。

Command Default

默认情况下，会禁用 **msie-proxy local-bypass**。

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

7.2(1) 添加了此命令。

使用指南

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南3.1 版》或移动设备的 [版本说明](#)。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用 Microsoft Internet Explorer 代理本地旁路：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy lockdown

要在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的连接 (Connections) 选项卡和“设置” (Settings) 应用中的系统代理选项卡或保持不变，请在 group-policy 配置模式下使用 **msie-proxylockdown** 命令。

msie-proxylockdown [enable | disable]

Syntax Description	disable 保持 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的“系统代理”选项卡不变。
	enable 在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的系统代理选项卡。

Command Default 默认组策略中该命令的默认值是enable。每个组策略都从默认组策略继承其默认值。

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
策略组配置	• 是	• 支持	• 支持	—	—

Command History	版本 修改
	8.2(3) 添加了此命令。

使用指南 启用此功能将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡。此外，从 Windows 10 版本 1703（或更高版本）开始，启用此功能还会在 AnyConnect VPN 会话期间隐藏“设置”应用中的系统代理选项卡。禁用该功能将使 Microsoft Internet Explorer 中的“连接”选项卡和“设置”应用中的系统代理选项卡的显示保持不变。

要使用此功能，您还必须指定私有端代理。



注释 在 AnyConnect VPN 会话期间隐藏“设置”应用中的系统代理选项卡需要 AnyConnect 版本 4.7.03052 或更高版本。

此命令可在 AnyConnect VPN 会话期间临时更改用户注册表。当 AnyConnect 关闭 VPN 会话时，它将注册表返回到会话开始前的状态。

您可以启用此功能以防止用户指定代理服务 and 更改 LAN 设置。防止用户访问这些设置可增强 AnyConnect 会话期间的终端安全。

有关代理设置的详细信息，请参阅 Cisco 安全客户端 管理员指南，或者参阅您的移动设备的 [版本说明](#)。

CR_Examples

以下示例在 AnyConnect 会话期间隐藏 Connections 选项卡：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

以下示例保持 Connections 选项卡不变：

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

Related Commands

命令	说明
msie-proxyexcept-list	为客户端设备上的浏览器指定一个代理服务器例外列表。
msie-proxylocal-bypass	绕过客户端设备上配置的本地浏览器代理设置。
msie-proxymethod	指定客户端设备的浏览器代理操作。
msie-proxypac-url	指定要从中检索定义代理服务器的代理自动配置文件的 URL。
msie-proxyserver	为客户端设备上的浏览器配置代理服务器。
show running-config group-policy	显示运行配置中的组策略设置。

msie-proxy method

要为客户端设备配置浏览器代理操作（“方法”），请在 **msie-proxymethod**策略组配置模式下输入命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

```
msie-proxymethod [ auto-detect | no-modify | no-proxy | use-server | use-pac-url ]
no msie-proxymethod [ auto-detect | no-modify | no-proxy | use-server | use-pac-url ]
```



注释 有关适用于此语法的限定条件，请参阅使用指南部分。

Syntax Description

- auto-detect** 允许在客户端设备的浏览器中使用自动代理服务器检测。
- no-modify** 对于此客户端设备，保持浏览器中的 HTTP 浏览器代理服务器设置不变。
- no-proxy** 禁用客户端设备浏览器中的 HTTP 代理设置。
- use-pac-url** 指示浏览器从 **msie-proxypac-url** 命令中指定的代理自动配置文件 URL 检索 HTTP 代理服务器设置。
- use-server** 设置浏览器中的 HTTP 代理服务器设置以使用命令中配置的 **msie-proxyserver**值。

Command Default

默认方法是 **use-server**。

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
组策略配置	• 是	—	• 是	—	—

Command History

- 版本 修改
- 7.2(1) 添加了此命令。
- 8.0(2) 添加了 **use-pac-url** 选项。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行最多可包含 100 个字符。
该命令支持以下选项组合：

- **[no]msie-proxymethodno-proxy**

- **[no]msie-proxymethodno-modify**
- **[no]msie-proxymethod[auto-detect][use-server][use-pac-url]**

可以使用文本编辑器为浏览器创建代理自动配置 (.pac) 文件。 .pac 文件是一个 JavaScript 文件，其中包含用于根据 URL 的内容来指定要使用的一个或多个代理服务器的逻辑。 .pac 文件位于 Web 服务器上。当您指定 **use-pac-url**，浏览器将使用 .pac 文件来确定代理设置。使用 **msie-proxypac-url** 命令指定从中检索 .pac 文件的 URL。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南3.1 版》或移动设备的 [版本说明](#)。

CR_Examples

以下示例显示如何将自动检测配置为名为FirstGroup 的组策略的 Microsoft Internet Explorer 代理设置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

以下示例将名为FirstGroup 的组策略的 Microsoft Internet Explorer 代理设置配置为使用服务器 QAserver、端口 1001 作为客户端 PC 的服务器：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
msie-proxypac-url	指定要从中检索代理自动配置文件的 URL。
msie-proxyserver	配置客户端设备的浏览器代理服务器和端口。
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。
clearconfiguregroup-policy	删除所有已配置的组策略属性。

msie-proxy pac-url

要指示浏览器查找代理信息的位置，请在 group-policy 配置模式下输入 **msie-proxypac-url** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxypac-url { none | valueurl }
nomsie-proxypac-url

Syntax Description	无指定没有 URL 值。
	valueurl 指定浏览器可获取代理自动配置文件的网站，该代理自动配置文件定义要使用的代理服务器。

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
组策略配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南 要求

要使用代理自动配置功能，远程用户必须使用 Cisco AnyConnect VPN 客户端。要启用代理自动配置 URL 的使用，还必须使用 **msie-proxymethod**] 选项配置 **use-pac-url** 命令。

为什么使用此命令

许多网络环境都定义将 Web 浏览器连接到特定网络资源的 HTTP 代理。仅当在浏览器中指定了代理并且客户端将 HTTP 流量路由到代理时，HTTP 流量才可以到达网络资源。SSL VPN 隧道会将 HTTP 代理的定义复杂化，因为在通过隧道传送到企业网络时所需的代理与通过宽带连接来连接到互联网时或位于第三方网络上时所需的代理不同。

此外，具有大型网络的公司可能需要配置多个代理服务器并让用户根据瞬态条件在其之间进行选择。通过使用 .pac 文件，管理员可以编写一个脚本文件来确定众多代理中的哪些代理将用于整个企业内的所有客户端计算机。

以下是如何使用 PAC 文件的一些示例：

- 从列表中随机选择一个代理以实现负载均衡。
- 按时刻或星期几轮换代理以适应服务器维护计划。
- 指定在主代理发生故障的情况下使用的备份代理服务器。
- 根据本地子网为漫游用户指定位置最近的代理。

如何使用代理自动配置功能

可以使用文本编辑器为浏览器创建代理自动配置 (.pac) 文件。 .pac 文件是一个 JavaScript 文件，其中包含用于根据 URL 的内容来指定要使用的一个或多个代理服务器的逻辑。使用 **msie-proxypac-url** 命令指定从中检索 .pac 文件的 URL。然后，当您 **use-pac-url** 在命令中 **msie-proxy method** 指定时，浏览器会使用 .pac 文件来确定代理设置。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南 3.1 版》或移动设备的 [版本说明](#)。

CR_Examples

以下示例显示如何配置浏览器以从 URL www.example.com 获取名为 FirstGroup 的组策略的代理设置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

以下示例为名为 FirstGroup 的组策略禁用代理自动配置功能：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
msie-proxy method	配置客户端设备的浏览器代理操作（“方法”）。
msie-proxy server	配置客户端设备的浏览器代理服务器和端口。
show running-configuration group-policy	显示已配置的组策略属性的值。
clear configure group-policy	删除所有已配置的组策略属性。

msie-proxy server

要为客户端设备配置浏览器代理服务器和端口，请在 **msie-proxyserver** 策略组配置模式下输入命令。
要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy server { **value**server [:port] | **none** }
nomsie-proxyserver

Syntax Description

none 表示没有为代理服务器指定 IP 地址/主机名或端口并防止继承服务器。

value服务器: 端 指定适用于此客户端设备的 MSIE 服务器和端口的 IP 地址或名称。端口号可选。
口

Command Default

默认情况下，未指定 msie-proxy 服务器。

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
组策略配置	• 是	—	• 是	—	—

Command History

版本 修改

7.2(1) 添加了此命令。

使用指南

包含代理服务器 IP 地址或主机名和端口号的行的长度必须小于 100 个字符。

有关代理设置的详细信息，请参阅《思科 安全客户端 管理员指南3.1 版》或移动设备的 [版本说明](#)。

CR_Examples

以下示例显示如何将 IP 地址 192.168.10.1 配置为 Microsoft Internet Explorer 代理服务器，使用端口 880，用于名为 FirstGroup 的组策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
showrunning-configurationgroup-policy	显示已配置的组策略属性的值。

命令	说明
clearconfiguregroup-policy	删除所有已配置的组策略属性。

mtu

要指定接口的最大传输单位，请在全局配置模式下使用 **mtu** 命令。要将以太网接口的 MTU 块大小重置为 1500，请使用此命令的 **no** 形式。此命令支持 IPv4 和 IPv6 流量。

```
mtuinterface_namebytes
nomtuinterface_namebytes
```

Syntax Description	bytes	MTU 中的字节数；有效值为 64 到 9198 字节（对于 Secure Client 和 Firepower 9300 ASA 安全模块为 9000 字节）。
	interface_name	内部或外部网络接口名称。

Command Default 以太网接口的默认 字节数为 1500。

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	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.1(6) 最大 MTU 已从 65535 更改为 9198（或 9000，具体取决于型号）。

使用指南 **mtu** 命令可以设置在连接上发送的负载大小（不包括第 2 层报头或 VLAN 标记）。大于 MTU 值的数据将分片后再发送。以太网接口的默认 MTU 为 1500 字节（这也是没有巨帧预留的最大值）。在这种情况下，带有第 2 层报头（14 字节）和 VLAN 标记（4 字节）的数据包大小是 1518 字节。对于大多数应用而言，此值已足够，但如果网络条件需要，也可选择较小的数字。

ASA 支持 IP 路径 MTU 发现（如 RFC 1191 中所定义），使主机能够动态发现和处理路径沿途各种链路的最大允许 MTU 大小差异。有时，由于数据包大于为接口设置的 MTU，ASA 无法转发数据报，但已设置“不分段” (DF) 位。网络软件向发送主机发送一条消息，提醒其注意该问题。主机必须为目标对数据包进行分片，以适应路径上所有链路中最小数据包的大小。

使用第 2 层隧道协议 (L2TP) 时，我们建议您将 MTU 大小设置为 1380，以考虑 L2TP 报头和 IPsec 报头长度。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密会产生开销，因此 MTU 值不应设置为低于 1380。将接口设置为低于 1380 字节可能会导致数据包丢失。

从版本 9.1(6) 开始，ASA 可以使用的最大 MTU 为 9198 字节。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。如果您的 MTU 设置为高于 9198 的值，则升级后 MTU 会自动降低。在某些情况下，这种 MTU 变化可能导致 MTU 不匹配；请务必将连接的所有设备设置为使用新的 MTU 值。

CR_Examples

此示例显示如何为接口指定 MTU：

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

命令	说明
clearconfiguremtu	清除所有接口上已配置的最大传输单位值。
showrunning-configmtu	显示当前最大传输单元块大小。

mtu cluster

要设置集群控制链路的最大传输单位，请在全局配置模式下使用 **mtucluster** 命令。要恢复默认设置，请使用此命令 **no** 的形式。

mtucluster*bytes*
no**mtucluster** [*bytes*]

Syntax Description 字 指定集群控制链路接口的最大传输单元，介于 64 到 65,535 字节之间。我们不建议将集群控制节 链路 MTU 设置在 2561 和 8362 之间；由于块池处理，此 MTU 大小对于系统操作来说不是最佳的。默认 MTU 为 1500 字节。

Command Default 默认 MTU 为 1500 字节。

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	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南 我们建议将 MTU 设置为 1600 字节或更大，这需要您使用命令启用巨型帧预留 **jumbo-frame-reservation** 留。

该命令是全局配置命令，但也是引导配置的一部分，不会在单元之间复制。

CR_Examples 以下示例将集群控制链路 MTU 设置为 9000 字节：

```
ciscoasa(config)# mtu cluster 9000
```

命令	说明
cluster-interface	标识集群控制链路接口。
jumbo frame-reservation	允许使用巨型以太网帧。

multicast boundary

要管理范围的组播地址配置组播边界，请在接口配置模式下使用 **multicastboundary** 命令。要删除边界，请使用此命令的形式。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。

multicastboundary *acl* [**filter-autorp**]
nomulticastboundary *acl* [**filter-autorp**]

Syntax Description

acl 指定访问列表名称或编号。访问列表定义受边界影响的地址范围。在此命令中仅使用标准 ACL；不支持扩展 ACL。

filter-autorp 过滤边界 ACL 拒绝的 Auto-RP 消息。如果未指定，则允许所有 Auto-RP 消息通过。

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
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

使用此命令可在接口上配置管理权限范围的边界，以过滤 *acl* 参数定义范围内的组播组地址。标准访问列表定义了受影响的地址范围。配置此命令后，不允许任何多播数据包在任何一个方向跨越边界。限制组播数据包流量可以在不同的管理域中重复使用相同的组播组地址。

如果配置 **filter-autorp** 关键字，则管理范围边界还会检查 Auto-RP 发现和通知消息，并从边界 ACL 拒绝的 Auto-RP 数据包中删除任何 Auto-RP 组范围通知。仅在 Auto-RP 组范围中的所有地址获边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

CR_Examples

以下示例为所有具有管理作用域的地址设置边界并过滤 Auto-RP 消息：

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
```

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

multicast-routing

要在 ASA 上启用 IP 多播路由，请在全局配置模式下使用该 **multicast-routing** 命令。要禁用 IP 多播路由，请使用此 **no** 命令的形式。

multicast-routing
nomulticast-routing

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下， **multicast-routing** 命令可在所有接口上启用 PIM 和 IGMP。

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
7.0(1)	添加了此命令。

使用指南 **multicast-routing** 命令可在所有接口上启用 PIM 和 IGMP。



注释 PAT 不支持 PIM。PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。如果安全设备是 PIM RP，请使用安全设备未转换的外部地址作为 RP 地址。

多播路由表中的条目数量受系统 RAM 数量限制。根据安全设备上的 RAM 数量列出特定多播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

表 6: 多播表的条目限制（组合静态和动态条目）

表	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP 组	1000	3000	5000

表	16 MB	128 MB	128+ MB
PIM 路由	3000	7000	12000

CR_Examples

以下示例在 ASA 上启用 IP 组播路由：

```
ciscoasa(config)# multicast-routing
```

Related Commands

命令	说明
igmp	启用接口上的 IGMP。
pim	在接口上启用 PIM。

mus

要指定 ASA 标识 WSA 的 IP 范围和接口，请在全局配置模式下使用 **mus** 命令。要关闭该服务，请使用此命令的 **no** 形式。此命令支持 IPv4 和 IPv6 流量。仅注册在指定的子网和接口上找到的 WSA。

mus IPv4 地址 IPv4 掩码 *interface_name*
no **mus** IPv4 地址 IPv4 掩码 *interface_name*



注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

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
全局配置	• 是	—	• 是	—	—

Command History

版本 修改

8.3(1) 添加了此命令。

使用指南

可以使用以下命令：

- ABCD - 获授权访问 ASA 的 WSA IP 地址。
- host - 客户端通过向虚拟主机发送请求，定期检查与网络安全设备的连接。默认情况下，虚拟主机 URL 为 mus.cisco.com。启用 AnyConnect 安全移动性后，网络安全设备会拦截发往虚拟主机的请求并回复客户端。
- password - 配置 WSA 密码。
- server - 配置 WSA 服务器

CR_Examples

以下示例允许 1.2.3.x 子网上的 WSA 服务器访问 内部 接口上的安全移动解决方案：

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

Related Commands

命令	说明
mus password	为 AnyConnect 安全移动通信设置共享密钥。
mus server	指定 ASA 侦听 WSA 通信的端口。
show webvpn mus	显示有关活动 WSA 连接安全设备的信息。

mus host

要在 ASA 上指定 MUS 主机名，请在全局配置模式下输入命令 **mus host**。这是从 ASA 发送到 Secure Client 的遥测 URL。Secure Client 使用此 URL 与专用网络中的 WSA 联系，以获得 MUS 相关服务。要删除使用此命令输入的任何命令，请使用该 **nomus host** 命令。

mus host *hostname*
nomus host

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
全局配置	• 是	—	• 是	—	—

Command History

版本 修改

8.3(1) 添加了此命令。

使用指南

您可以为给定端口启用 AnyConnect 安全移动。WSA 端口值为 1 到 21000。如果未在命令中指定端口，则将使用端口 11999。

您必须在执行此命令之前配置 AnyConnect 安全移动共享密钥。



注释

要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

CR_Examples

以下示例显示如何进入 AnyConnect Secure Mobility 主机和 WebVPN 命令子模式：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside
ciscoasa(config-webvpn)# mus password abcdefgh123
```

```
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
muspassword	为 AnyConnect 安全移动通信设置共享密钥。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。

mus password

要为 AnyConnect 安全移动通信设置共享安全，请在全局配置模式下输入**muspassword** 命令。要删除共享密钥，请使用 **nomuspassword** 命令。

muspassword
nomuspassword



注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提 供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

Syntax Description 此命令没有任何参数或关键字。

Command Default 。有效的密码由正则表达式 [0-9, az, AZ,;,:_/-]{8,20} 定义。共享密钥密码的整体长度最少为 8 个字符，最多为 20 个字符。

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

8.3(1) 添加了此命令。

使用指南 此 WebVPN 子模式允许您配置 WebVPN 的全局设置。您可以设置 AnyConnect 安全移动通信的共享密钥。

CR_Examples 以下示例显示如何进入 AnyConnect 安全移动密码和 WebVPN 命令子模式：

```
ciscoasa
(config)#
mus password <password_string>
ciscoasa
(config-webvpn)#
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
musserver	指定 ASA 侦听 WSA 通信的端口。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。

mus server

要指定 ASA 侦听 WSA 通信的端口，请在全局配置模式下输入 **musserver** 命令。要删除使用此命令输入的任何命令，请使用该 **nomusserver** 命令。

musserverenable
nomusserverenable



注释 要按预期运行，此命令需要发布 AsyncOS for Web 版本 7.0，该版本为安全客户端 AnyConnect 安全移动客户端提供许可支持。它还需要支持 AnyConnect Secure Mobility、ASA 8.3 和 ASDM 6.3 的 AnyConnect 版本。

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
全局配置	• 是	—	• 是	—	—

Command History 版本 修改

8.3(1) 添加了此命令。

使用指南

您必须指定 AnyConnect 安全移动服务使用的端口。ASA 与 WSA 之间的通信通过管理员指定的端口（范围为 1 至 21000）上的安全 SSL 连接进行。

您必须在执行此命令之前配置 AnyConnect 安全移动共享密钥。

CR_Examples

以下示例显示如何进入 AnyConnect 安全移动密码和 WebVPN 命令子模式：

```
ciscoasa
(config-webvpn)#
mus server enable
?
webvpn mode commands/options
  port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

Related Commands

命令	说明
mus	指定 ASA 识别 WSA 的 IP 范围和接口。
muspassword	为 AnyConnect 安全移动通信设置共享密钥。
showwebvpnmus	显示有关活动 WSA 连接安全设备的信息。



第 III 部分

N - R 命令

- [n](#)，第 919 页
- [室外](#)，第 1081 页
- [pa - pn](#)，第 1135 页
- [po - pq](#)，第 1259 页
- [pr - pz](#)，第 1325 页
- [q - res](#)，第 1395 页
- [ret - rz](#)，第 1479 页



n

- [nac-authentication-server-group](#) (已弃用), 第 921 页
- [nac-policy](#) (已弃用), 第 923 页
- [nac-settings](#) (已弃用), 第 925 页
- [name](#) (dynamic-filter blacklist 或 whitelist), 第 927 页
- [name](#) (全局), 第 930 页
- [nameif](#), 第 932 页
- [names](#), 第 934 页
- [name-separator](#) (pop3s, imap4s, smtps) (已弃用), 第 936 页
- [name-server](#), 第 938 页
- [nat](#) (global), 第 940 页
- [nat](#) (object), 第 951 页
- [nat](#) (vpn load-balancing), 第 960 页
- [nat-assigned-to-public-ip](#), 第 962 页
- [nat-rewrite](#), 第 965 页
- [nbns-server](#), 第 966 页
- [neighbor](#) (router eigrp), 第 968 页
- [neighbor](#) (router ospf), 第 970 页
- [neighbor activate](#), 第 972 页
- [neighbor advertise-map](#), 第 974 页
- [neighbor advertisement-interval](#), 第 976 页
- [neighbor default-originate](#), 第 978 页
- [邻居描述](#), 第 980 页
- [neighbor disable-connected-check](#), 第 982 页
- [neighbor distribute-list](#), 第 984 页
- [neighbor ebgp-multihop](#), 第 986 页
- [neighbor fall-over bfd](#) (router bgp), 第 988 页
- [neighbor filter-list](#), 第 990 页
- [neighbor ha-mode graceful-restart](#), 第 992 页
- [neighbor local-as](#), 第 994 页
- [neighbor maximum-prefix](#), 第 998 页

- neighbor next-hop-self, 第 1000 页
- neighbor password, 第 1002 页
- neighbor prefix-list, 第 1005 页
- neighbor remote-as, 第 1007 页
- neighbor remove-private-as, 第 1009 页
- neighbor route-map, 第 1011 页
- neighbor send-community, 第 1013 页
- neighbor shutdown, 第 1014 页
- neighbor timers, 第 1016 页
- neighbor transport, 第 1018 页
- neighbor ttl-security, 第 1020 页
- neighbor update-source, 第 1022 页
- neighbor version, 第 1024 页
- neighbor weight, 第 1026 页
- nem, 第 1028 页
- netmod, 第 1029 页
- network (address-family), 第 1031 页
- network (router eigrp), 第 1033 页
- network (router rip), 第 1034 页
- network-acl, 第 1036 页
- network area, 第 1038 页
- network-object, 第 1040 页
- network-service-member, 第 1042 页
- nis address, 第 1043 页
- nis domain-name, 第 1046 页
- nisp address, 第 1049 页
- nisp domain-name, 第 1052 页
- nop, 第 1055 页
- nsf cisco, 第 1057 页
- nsf cisco helper, 第 1059 页
- nsf ietf, 第 1061 页
- nsf ietf helper, 第 1063 页
- nt-auth-domain-controller, 第 1065 页
- ntp authenticate, 第 1067 页
- ntp authentication-key, 第 1069 页
- ntp server, 第 1071 页
- ntp trusted-key, 第 1073 页
- num-packets, 第 1075 页
- nve, 第 1077 页
- nve-only, 第 1079 页

nac-authentication-server-group (已弃用)

要标识用于网络准入控制安全状态验证的身份验证服务器组，请在 `tunnel-group general-attributes` 配置模式下使用 **nac-authentication-server-group** 命令。要从默认远程访问组继承身份验证服务器组，请访问要从中继承它的备用组策略，然后使用此命令的 **no** 形式。

nac-authentication-server-group *server-group*
no **nac-authentication-server-group**

Syntax Description

server-group 姿态验证服务器组的名称，使用命令在 ASA 上配置 **aaa-server** *host*。该名称必须与该命令中指定的 *server-tag* 变量匹配。

Command Default

此命令没有任何参数或关键字。

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
隧道组常规属性配置	• 是	• —	• 是	• —	—

Command History

版本 修改

7.2(1) 添加了此命令。

8.0(1) 此命令已弃用。nac-policy-nac-framework 配置模式下的 **authentication-server-group** 命令取而代之。

使用指南

将至少一个访问控制服务器配置为支持 NAC。使用该 **aaa-server** 命令命名 ACS 组。然后使用该 **nac-authentication-server-group** 命令，对服务器组使用相同的名称。

CR_Examples

以下示例将 `acs-group1` 标识为要用于 NAC 安全状态验证的身份验证服务器组：

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

以下示例从默认远程访问组继承身份验证服务器组。

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

Related Commands

命令	说明
aaa-server	创建 AAA 服务器或组的记录，并设置主机特定的 AAA 服务器属性。
调试 eap	启用 EAP 事件日志记录以调试 NAC 消息传送。
调试 EOU	启用 EAP over UDP (EAPoUDP) 事件日志记录以调试 NAC 消息传送。
调试 nac	启用 NAC 事件的日志记录。
nac	在组策略上启用网络准入控制。

nac-policy (已弃用)



注释 此命令的最后支持版本是版本 9.1(1)。

要创建或访问思科网络准入控制 (NAC) 策略并指定其类型，请在全局配置模式下使用 **nac-policy** 命令。要从配置中删除 NAC 策略，请使用此命令的 **no** 形式。

nac-policy *nac-policy-name* **nac-framework**
no nac-policy *nac-policy-name* **nac-framework**

Syntax Description

nac-policy-name NAC 策略的名称。输入最多 64 个字符的字符串，为 NAC 策略命名。该 **showrunning-config** **nac-policy** 命令显示安全设备上已存在的每个 NAC 策略的名称和配置。

nac-framework 指定使用 NAC 框架为远程主机提供网络访问策略。网络上必须存在 Cisco 访问控制服务器才能为 ASA 提供 NAC 框架服务。

如果指定此类型，提示符表明您处于 **config--nac-policy-nac-framework** 配置模式。此模式允许配置 NAC 框架策略。

Command Default

此命令没有默认设置。

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

8.0(2) 添加了此命令。

9.1(2) 此命令已弃用。

使用指南

对要分配给组策略的每个 NAC 设备使用此命令一次。然后使用 **nac-settings** 命令将 NAC 策略分配给每个适用的组策略。设置 IPsec 或思科 AnyConnect VPN 隧道后，ASA 应用与使用的组策略关联的 NAC 策略。

如果 NAC 策略已分配给一个或多个组策略，则无法使用 **nonac-policyname** 命令将其删除。

CR_Examples

以下命令创建并访问名为 `nac-framework1` 的 NAC 框架策略：

```
ciscoasa
(config)
# nac-policy nac-framework1 nac-framework
ciscoasa
(config-nac-policy-nac-framework)
```

以下命令删除名为 `nac-framework1` 的 NAC 框架策略：

```
ciscoasa
(config)
# no nac-policy nac-framework1
ciscoasa
(config-nac-policy-nac-framework)
```

Related Commands

命令	说明
showrunning-confignac-policy	显示 ASA 上每个 NAC 策略的配置。
shownac-policy	显示 ASA 上 NAC 策略使用统计信息。
clearnac-policy	重置 NAC 策略使用统计信息。
nac-settings	将 NAC 策略分配到组策略。
clearconfigurenac-policy	从正在运行的配置中删除所有 NAC 策略，分配给组策略的策略除外。

nac-settings (已弃用)



注释 此命令的最后支持版本是版本 9.1(1)。

要将 NAC 策略分配给组策略，请在 **nac-settings**策略组配置模式下使用以下命令：

```
nac-settings { value nac-policy-name | none }
no nac-settings { value nac-policy-name | none }
```

Syntax Description	nac-policy-name	要分配到组策略的 NAC 策略。您命名的 NAC 策略必须存在于 ASA 配置中。该 showrunning-confignac-policy 命令显示每个 NAC 策略的名称和配置。
	none	从组策略中删除 nac - policy-name 并禁止此组策略使用 NAC 策略。组策略不会从默认组策略继承 nac-settings 值。
	value	将要命名的 NAC 策略分配给组策略。

Command Default 此命令没有任何参数或关键字。

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
组策略配置	• 是	• —	• 是	• —	—

Command History	版本 修改
	8.0(2) 添加了此命令。
	9.1(2) 此命令已弃用。

使用指南 使用 **nac-policy** 命令指定 NAC 策略的名称和类型，然后使用此命令将策略分配给组策略。该 **showrunning-confignac-policy**命令显示每个 NAC 策略的名称和配置。当您为 ASA 分配 NAC 策略时，ASA 会自动为组策略启用 NAC。

CR_Examples

以下命令从组策略中删除 `nac - policy-name`。组策略从默认组策略继承了 `nac -settings`值：

```
ciscoasa(config-group-policy)
# no nac-settings
ciscoasa(config-group-policy)
```

以下命令从组策略中删除 `nac - policy-name` 并禁用此组策略使用 NAC 策略。组策略不会从默认组策略继承 `nac-settings` 值。

```
ciscoasa(config-group-policy)
# nac-settings none
ciscoasa(config-group-policy)
```

Related Commands

命令	说明
nac-policy	创建和访问思科 NAC 策略，并指定其类型。
showrunning-confignac-policy	显示 ASA 上每个 NAC 策略的配置。
shownac-policy	显示 ASA 上 NAC 策略使用统计信息。
showvpn-session_summary.db	显示 IPsec、WebVPN 和 NAC 会话的数量。
showvpn-session.db	显示有关 VPN 会话的信息，包括 NAC 结果。

name (dynamic-filter blacklist 或 whitelist)

要将域名添加到僵尸网络流量过滤器黑名单或白名单，请在 dynamic-filter 黑名单或白名单配置模式下使用 **name** 命令。要删除名称，请使用 **no** 此命令的形式。静态数据库允许您通过要列入白名单或黑名单的域名或 IP 地址扩充动态数据库。

namedomain_name
no namedomain_name

Syntax Description *domain_name* 将名称添加到黑名单。可以多次输入此命令以获得多个条目。您最多可以添加 1000 个黑名单条目。

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
动态过滤器黑名单或白名单配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.2(1)	添加了此命令。

使用指南

进入动态过滤器白名单或黑名单配置模式后，您可以使用 **address** 和 **name** [键，手动输入要标记为白名单中的好名称或黑名单中的不良名称的域名或 IP 地址（主机或子网）。命令。

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

当您域名添加到静态数据库时，ASA 会等待 1 分钟，然后发送该域名的 DNS 请求，并将域名/IP 地址对添加到 *DNS* 主机缓存。（此操作是一个后台进程，不会影响您继续配置 ASA）。

如果没有为 ASA 配置域名服务器，或域名服务器不可用，则可以启用包含僵尸网络流量过滤器侦听的 DNS 数据包检测（请参阅 **inspectdnsdynamic-filter-snooping** 命令）。利用 DNS 监听，当受感染主机发送对静态数据库中的名称的 DNS 请求时，ASA 将在 DNS 数据包内查找域名和关联的 IP 地址，并将名称和 IP 地址添加到 DNS 反向查找缓存。有关 DNS 反向查找缓存的信息，请参阅 **inspectdnsdynamic-filter-snooping** 命令。

DNS 主机缓存中的条目有一个由 DNS 服务器提供的生存时间 (TTL) 值。允许的最大 TTL 值为 1 天（24 小时）；如果 DNS 服务器提供更大的 TTL，则会截断为最大值 1 天。

对于 DNS 主机缓存，在条目超时后，ASA 会定期请求刷新该条目。

CR Examples

以下示例为黑名单和白名单创建条目：

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-l1ist)# name bad1.example.com
ciscoasa(config-l1ist)# name bad2.example.com
ciscoasa(config-l1ist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-l1ist)# dynamic-filter whitelist
ciscoasa(config-l1ist)# name good.example.com
ciscoasa(config-l1ist)# name great.example.com
ciscoasa(config-l1ist)# name awesome.example.com
ciscoasa(config-l1ist)# address 10.1.1.2255.255.255.255
```

Related Commands

命令	说明
address	将 IP 地址添加到黑名单或白名单。
clear configure dynamic-filter	清除正在运行的僵尸网络流量过滤器配置。
cleardynamic-filterdns-snoop	清除僵尸网络流量过滤器 DNS 监听数据。
cleardynamic-filterreports	清除僵尸网络流量过滤器报告数据。
cleardynamic-filterstatistics	清除僵尸网络流量过滤器统计信息。
dns domain-lookup	使 ASA 能够向 DNS 服务器发送 DNS 请求以执行支持的命令的名称查找。
dns server-group	标识 ASA 的 DNS 服务器。
dynamic-filterblacklist	编辑僵尸网络流量过滤器黑名单。
动态过滤器数据库获取	手动检索僵尸网络流量过滤器动态数据库。
dynamic-filterdatabasefind	搜索域名或 IP 地址的动态数据库。
动态过滤器数据库清除	手动删除僵尸网络流量过滤器动态数据库。
dynamic-filterenable	为一个流量类或为所有流量（如果不指定访问列表）启用僵尸网络流量过滤器。
dynamic-filterupdater-clientenable	启用下载动态数据库。
dynamic-filteruse-database	允许使用动态数据库。
dynamic-filterwhitelist	编辑僵尸网络流量过滤器白名单。
inspectdnsdynamic-filter-snoop	启用包含僵尸网络流量过滤器侦听的 DNS 检查。
name	将名称添加到黑名单或白名单。

命令	说明
showasptabledynamic-filter	显示加速安全路径中安装的僵尸网络流量过滤器规则。
showdynamic-filterdata	显示有关动态数据库的信息，包括上次下载动态数据库的时间、数据库的版本、数据库包含的条目数和 10 个示例条目。
showdynamic-filterdns-snoop	显示僵尸网络流量过滤器 DNS 监听摘要，或与 detail 关键字一起显示实际 IP 地址和名称。
showdynamic-filterreports	生成有关前 10 个僵尸网络站点、端口和受感染主机的报告。
showdynamic-filterstatistics	显示受僵尸网络流量过滤器监控的连接数，以及其中与白名单、黑名单和灰名单匹配的连接数。
showdynamic-filterupdater-client	显示更新程序服务器的相关信息，包括服务器 IP 地址、ASA 下次与服务器连接的时间和上次安装的数据库版本。
show running-config dynamic-filter	显示僵尸网络流量过滤器运行配置。

name（全局）

要将名称与 IP 地址相关联，请在全局配置模式下使用 **name** 命令。要禁用文本名称但不将其从配置中删除，请使用此命令的 **no** 形式。

```
name IP 地址 [名称 [description 文本]]
no name IP 地址 [名称 [description 文本]]
```

Syntax Description

description	（可选）指定 IP 地址名称说明。
<i>ip_address</i>	指定所命名的主机的 IP 地址。
<i>name</i>	指定分配给 IP 地址的名称。使用字符 a 到 z、A 到 Z、0 到 9、破折号和下划线。名称不得超过 63 个字符。此外，名称不能以数字开头。
文本	指定说明的文本。

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
7.0(1)	添加了此命令。
7.0(4)	此命令已增强，包括可选说明。
8.3(1)	不能再在 nat 命令或 access-list 命令中使用命名的 IP 地址；必须改用 objectnetwork 名称。虽然对象组中的 network-object 命令接受 objectnetwork 名称，但您仍然可以使用由 name 命令标识的命名 IP 地址。

使用指南

要启用名称与 IP 地址的关联，请使用 **names** 命令。一个 IP 地址只能关联一个名称。

在使用 **names** 命令之前，必须先使用 **name** 命令。紧随使用 **name** 命令之后、使用 **writememory** 命令之前，使用 **name** 命令。

通过 **name** 命令，您可以通过文本名称标识主机并将文本字符串映射到 IP 地址。**noname** 命令允许您禁用文本名称，但不会将其从配置中删除。使用 **clearconfigurename** 命令清除配置中的名称列表。

要禁用显示 **name** 值，请使用 **nonames** 命令。

name 和 **name** 命令都会保存在配置中。

name 命令不支持为网络掩码分配名称。例如，以下命令会被拒绝：

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```



注释 需要掩码的所有 命令都无法将名称作为接受的网络掩码来处理。

CR_Examples

此示例显示 **names** 命令允许您使用 **name** 命令。 **name** 命令用 **sa_inside** 替代对 192.168.42.3 的引用，用 **sa_outside** 替代对 209.165.201.3 的引用。为网络接口分配 IP 地址时，您可以将这些名称与 **ipaddress** 命令配合使用。 **nonames** 命令禁用 **name** 命令值的显示。随后再次使用 **names** 命令可恢复 **name** 命令值显示。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

Related Commands

命令	说明
clearconfigurename	从配置中清除名称列表。
names	启用名称与 IP 地址的关联。
showrunning-configname	显示与 IP 地址关联的名称。

nameif

要为接口提供名称，请在 **nameif**接口配置模式下使用该命令。要删除名称，请使用**no**此命令的形式。ASA 上的所有配置命令中都会使用接口名称来代替接口类型和 ID（例如，**gigabitethernet0/1**），因此必须具备接口名称，流量才能通过接口。

nameif*name*
no nameif

Syntax Description

name 设置长度最多为 48 个字符的名称。该名称不区分大小写。

请勿使用 “Metrics_History” 或 “MH” 名称；其原因是，ASDM 将接口显示为关闭状态。

请勿使用名称 “internal”，因为它会阻止配置其他功能，例如静态 ARP。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 此命令已从全局配置命令更改为接口配置模式命令。

使用指南

对于子接口，在输入 **nameif** 命令之前，必须使用 **vlan** 命令分配 VLAN。

使用一个新值重新输入此命令可更改名称。不要输入该 **no** 表单，因为该命令会导致所有引用该名称的命令被删除。

CR_Examples

以下示例将两个接口的名称配置为 “inside” 和 “outside”：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```


Related Commands

命令	说明
clearxlate	重置现有连接的所有转换，导致连接重置。
interface	配置接口并进入接口配置模式。
security-level	设置接口的安全级别。
vlan	将 VLAN ID 分配给子接口。

names

要启用名称与 IP 地址的关联，请在全局配置模式下使用 **names** 命令。一个 IP 地址只能关联一个名称。要禁用显示 **name** 值，请使用 **nonames** 命令。

names
no names

Syntax Description 此命令没有任何参数或关键字。

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
7.0(1)	添加了此命令。

使用指南

要启用名称与 IP 地址的关联，请使用 **names** 命令。一个 IP 地址只能关联一个名称。

在使用 **names** 命令之前，必须先使用 **name** 命令。紧随使用 **name** 命令之后、使用 **writememory** 命令之前，使用 **name** 命令。

要禁用显示 **name** 值，请使用 **nonames** 命令。

name 和 **name** 命令都会保存在配置中。

CR_Examples

此示例显示 **names** 命令允许您使用 **name** 命令。 **name** 命令用 **sa_inside** 替代对 192.168.42.3 的引用，用 **sa_outside** 替代对 209.165.201.3 的引用。为网络接口分配 IP 地址时，您可以将这些名称与 **ipaddress** 命令配合使用。 **nonames** 命令禁用 **name** 命令值的显示。随后再次使用 **names** 命令可恢复 **name** 命令值显示。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
```

```

inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
    
```

Related Commands

命令	说明
clearconfigurename	从配置中清除名称列表。
name	将名称与 IP 地址相关联。
showrunning-configname	显示与 IP 地址关联的名称列表。
showrunning-confignames	显示 IP 地址到名称的转换。

name-separator (pop3s, imap4s, smtps) (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定一个字符作为邮件与 VPN 用户名和密码之间的分隔符，请在相应的邮件代理模式下使用 **name-separator** 命令。要恢复默认的 “:”，请使用此命令的 **no** 版本。

name-separator [*symbol*]
no name-separator

Syntax Description *symbol* （可选）分隔邮件和 VPN 用户名和密码的字符。选项包括 “@”、（在） “|” （竖线）、 “.” （冒号）、 “#” （散列）、 “,” （逗号）和 “;” （分号）查找。

Command Default 默认值为 “.” （冒号）。

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
Pop3s	• 是	• —	• 是	• —	—
Imap4s	是	—	是	—	—
Smtps	是	—	是	—	—

Command History	版本	修改
	7.0(1)	添加了此命令。
	9.5(2)	此命令已弃用。

使用指南 名称分隔符必须与服务器分隔符不同。

CR_Examples 以下示例显示如何将散列字符 (#) 设置为 POP3S 的名称分隔符：

```
ciscoasa
(config) #
```

```
pop3s
ciscoasa(config-pop3s)# name-separator #
```

Related Commands	命令	说明
	server-separator	分隔邮件名称和服务名称。

name-server

要标识一个或多个 DNS 服务器以便 ASA 可将主机名解析为 IP 地址，请在 dns 服务器组配置模式下使用 **name-server**命令。要删除服务器，请使用此命令的 **no** 形式。



注释 ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，大多数命令都要求您输入 IP 地址，并且只有当您手动配 **name**置命令以将名称与 IP 地址关联并使用该命令启用名称时才能使用名 **names**称。

```
name-serverip_address [ip_address2] [...] [ip_address6] [interface_name]
no name-serverip_address [ip_address2] [...] [ip_address6] [interface_name]
```

Syntax Description

interface_name （可选）指定 ASA 与服务器通信的接口名称。如果未指定接口，ASA 将检查数据路由表；如果没有匹配项，则会检查仅管理路由表。

ip_address 指定 DNS 服务器 IP 地址。您最多可以指定六个地址，将其作为单独的命令；或者为方便起见，在一个命令中最多指定六个地址，以空格分隔。如果在一个 命令中输入多个服务器，ASA 会将每个服务器保存在配置中的单独命令中。ASA 按顺序尝试每台 DNS 服务器，直至收到响应。

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
dns server-group 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.1(1)	添加了此命令。
9.5(1)	添加了 <i>interface_name</i> 参数。

使用指南

要在接口上启用 DNS 查找，请配置 **dnsdomain-lookup** 命令。如果不启用 DNS 查找，则不能使用 DNS 服务器。

默认情况下，ASA 使用服务 **dnsserver-groupDefaultDNS**器组来处理传出请求。您可以使用 **dns-group** 命令。其他服务器组可与特定域相关联。与 DNS 服务器组关联的域匹配的 DNS 请求将使用该组。例如，如果您希望发往内部 eng.cisco.com 服务器的流量使用内部 DNS 服务器，则可以将 eng.cisco.com

映射到内部 DNS 组。与域映射不匹配的所有 DNS 请求都将使用没有关联域的默认 DNS 服务器组。例如，DefaultDNS 组可以包括外部接口上可用的公共 DNS 服务器。可为 VPN 隧道组配置其他 DNS 服务器组。有关详细信息，请参阅 **tunnel-group** 命令。

某些 ASA 功能需要使用 DNS 服务器通过域名访问外部服务器；例如，僵尸网络流量过滤器功能需要 DNS 服务器访问动态数据库服务器并解析静态数据库中的条目；思科智能软件许可需要 DNS 来解析许可证颁发机构地址。通过其他功能，例如 **ping** 或 **traceroute** 命令，可输入要 ping 或 traceroute 的名称，而且 ASA 能够通过与 DNS 服务器进行通信来解析名称。许多 SSL VPN 和证书命令也支持名称。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

如果没有指定接口 **name-server**，ASA 将检查数据路由表；如果没有匹配项，它将检查仅管理路由表。请注意，如果有通过数据接口的默认路由，则所有 DNS 流量都将与该路由匹配，从不检查管理专用路由表。在此场景中，如果您需要通过管理接口访问服务器，请始终指定 接口。

CR_Examples

以下示例将三个 DNS 服务器添加到 “DefaultDNS” 组：

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA 会将配置保存为单独的命令，如下所示：

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

要添加两台其他服务器，可以将它们作为一个 命令输入：

```
ciscoasa(config)# dns server-groupDefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

要删除多个服务器，可以将其作为多个命令或作为一个命令输入，如下所示：

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

Related Commands

命令	说明
domain-name	设置默认域名。
retries	指定当 ASA 未收到响应时重试 DNS 服务器列表的次数。
timeout	指定尝试下一个 DNS 服务器之前等待的时间量。
showrunning-configdns-server-group	显示一个或所有现有 dns-server-group 配置。

nat (global)

要为 IPv4、IPv6 或 IPv4 与 IPv6 之间的 NAT (NAT64) 配置两次 NAT，请在全局配置模式下使用 **nat** 命令。要删除两次 NAT 配置，请使用此命令的形式。

对于静态 NAT：

```

nat [ (real_ifc,mapped_ifc) ] [line | { after-auto [line] } ] source
static{real_obj|any} {mapped_obj|interface [ipv6] | any} ] [destination
static{mapped_obj|interface [ipv6] } {real_obj|any} ] [service {mapped_dest_svc_obj real_dest_svc_obj}
[ dns ] [ unidirectional ] [ noypap ] [ nothkup ] [ inactive ] [ description desc ]

no nat [ (real_ifc,mapped_ifc) ] [line | { after-auto [line] } ] source
static{real_obj|any} {mapped_obj|interface [ipv6] | any} ] [destination
static{mapped_obj|interface [ipv6] } {real_obj|any} ] [service {mapped_dest_svc_obj real_dest_svc_obj}
[ dns ] [ unidirectional ] [ inactive ] [ description desc ]

```

对于动态 NAT：

```

nat [ (real_ifc,mapped_ifc) ] [line | { after-auto [line] } ] source
dynamic{real_obj|any} {mapped_obj|interface [ipv6] | pat-pool mapped_obj [round-robin] [extended]
[ flat [include-reserve] ] [ block-allocation ] [ interface [ipv6] ] | interface [ipv6] } [destination
static{mapped_obj|interface [ipv6] } {real_obj|any} ] [service {mapped_dest_svc_obj real_dest_svc_obj}
[ dns ] [ unidirectional ] [ inactive ] [ description desc ]

no nat [ (real_ifc,mapped_ifc) ] [line | { after-auto [line] } ] source
dynamic{real_obj|any} {mapped_obj|interface [ipv6] | pat-pool mapped_obj [round-robin] [extended]
[ flat [include-reserve] ] [ block-allocation ] [ interface [ipv6] ] | interface [ipv6] } [destination
static{mapped_obj|interface [ipv6] } {real_obj|any} ] [service {mapped_dest_svc_obj real_dest_svc_obj}
[ dns ] [ unidirectional ] [ inactive ] [ description desc ]

```

或

```
nonat {line after-autoline }
```

Syntax Description

(real_ifc,mapped_ifc)	（可选）指定真实接口和映射接口。如果您未指定真实接口和映射接口，则使用所有接口。您还可以 any 为一个或两个接口指定关键字。对于桥接组成员接口（在透明或路由模式下），必须指定实际接口和映射接口；则不能使用 any。 由于两次 NAT 可以转换源地址和目标地址，因此最好将这些接口理解为源接口和目标接口。
after-auto	在 NAT 表第 3 部分的末尾、网络对象 NAT 规则之后插入规则。默认情况下，两次 NAT 规则会添加到第 1 部分。您可以使用行参数在第 3 部分的任何位置插入规则。

any	(可选) 指定通配符值。 any 的主要用途包括： - 接口 - 您可以使用 any 表示一个或两个接口（例如 (any,outside)）。如果您没有指定接口，那么就 any 是默认的。但是， any 不适用于桥接组成员接口，并且 any 在透明模式下不可用。 - 静态 NAT 源实际和映射 IP 地址 - 您可以指定 sourcestaticanyany，以启用所有地址的身份 NAT。 - 动态 NAT 或 PAT 源实际地址 - 通过指定 sourcedynamicanymapped_obj，可以转换源接口上的所有地址。 对于静态 NAT，虽然 any 也可用于实际源端口/映射目标端口，或可用于源或目标实际地址（不带 any 作为映射地址），但使用这些命令可能会导致不可预测的行为。 注释 “任何”流量（IPv4 与 IPv6）的定义取决于规则。在 ASA 对数据包执行 NAT 之前，数据包必须是 IPv6 到 IPv6 或 IPv4 到 IPv4；有了这个先决条件，ASA 才能确定 NAT 规则中的值。 any 例如，如果您配置一条从“任何”到 IPv6 服务器的规则，并且该服务器是从 IPv4 地址映射的， any 则表示“任何 IPv6 流量”。如果您配置从“任何”到“任何”的规则，并且将源映射到接口 IPv4 地址，则意味 any 着“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。
block-allocation	启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与兼容 round-robin，但不能使用 extended 或 flat[include-reserve] 选项。也无法使用接口 PAT 回退。
descriptiondesc	(可选) 提供最多 200 个字符的描述。
目的	(可选) 配置目标地址的转换。尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅《CLI 配置指南》。
dns	(可选) 转换 DNS 应答。确保 DNS 检查已启用 (inspectdns) (默认启用)。如果配置了 dns 地址，则不能配置关键 destination 字。请勿将此选项与 PAT 规则一起使用。有关详细信息，请参阅 CLI 配置指南。

dynamic	为源地址配置动态 NAT 或 PAT。目标转换始终为静态。
extended	（可选）为 PAT 池启用扩展 PAT。扩展 PAT 通过在转换信息中包含目标地址和端口，为每个服务（而不是每个 IP 地址）使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。
flat [include-reserve] include-reserve	（可选，9.15 之前版本）分配端口时允许使用整个 1024 到 65535 端口范围。当选择要转换的映射端口号时，ASA 将使用实际源端口号（如果可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，另请指定 include-reserve 关键字。 (9.15+) 从 9.15 开始，平面是 PAT 池的默认且不可配置的行为。include-reserve 关键字独立于平面关键字，因此您仍然可以选择在 PAT 池中包含保留端口 1-1023。
inactive	（可选）要使此规则不活动而不必删除命令，请使用 inactive 关键字。要将其重新激活，请重新输入没有 inactive 关键字的整个命令。
interface[ipv6]	（可选）使用接口 IP 地址作为映射地址。如果指定 ipv6，则稍后使用该接口的 IPv6 地址。 对于动态 NAT 源映射地址，如果您指定映射对象或组，后跟 interface 关键字，则仅在所有其他映射地址已分配时，才会使用映射接口的 IP 地址。 对于动态 PAT，可以为源映射地址单独指定 interface。 对于支持端口转换（源或目标）的静态 NAT，请务必同时配置 service 关键字。 对于此选项，您必须为 <i>mapped_ifc</i> 配置一个特定的接口。 此选项在透明模式下不可用。在路由模式下，如果目标接口为桥接组成员，则不能使用此选项。
折线图	（可选）在 NAT 表第 1 部分的任意位置插入规则。默认情况下，NAT 规则将添加到第 1 部分的末尾（有关详细信息，请参阅 CLI 配置指南）。如果您想将规则添加到第 3 部分（网络对象 NAT 规则之后），请使用 after-auto 线路选项。
mapped_dest_svc_obj	（可选）对于动态 NAT/PAT，指定映射目标端口（目标转换始终为静态）。有关详细信息，请参阅 service 关键字。

<i>mapped_object</i>	标识映射的网络对象或对象组（objectnetwork或object-groupnetwork）。 对于动态 NAT，您通常会配置一组较大的地址来映射到一组较小的地址。 注释 映射对象或组不能包含子网。如果需要，可以在不同的动态 NAT 规则之间共享此映射 IP 地址。不能使用同时包含 IPv4 和 IPv6 地址的对象组；只有在对象组中才可以使用。对象组只能包含一种类型的地址。 对于动态 PAT，请将一组地址配置为映射到一个地址。您可以将实际地址转换为您选择的单个映射地址，也可以将其转换为映射接口地址。如果要使用接口地址，请勿为映射地址配置网络对象；请注意而是使用 interface 关键字。 对于静态 NAT，映射通常是一对一的，因此实际地址与映射地址的数量相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅《CLI 配置指南》。
<i>mapped_src_real_dest_svc_obj</i>	（可选）对于静态 NAT，指定映射源端口和/或实际目的端口。有关详细信息，请参阅 service 关键字。
net-to-net	（可选）对于静态 NAT 46，指 net-to-net 定将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个转换为第二个，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。
no-proxy-arp	（可选）对于静态 NAT，禁用发往映射 IP 地址的传入数据包的代理 ARP。
pat-pool <i>mapped_obj</i>	（可选）启用地址 PAT 池；对象中的所有地址均用作 PAT 地址。对于动态 NAT，可以将 PAT 池配置为回退方法。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
<i>real_dest_svc_obj</i>	（可选）对于动态 NAT/PAT，指定实际目标端口（目标转换始终为静态）。有关详细信息，请参阅 service 关键字。
<i>real_ifc</i>	（可选）指定数据包可能源自的接口的名称。对于源选项。对于 source 选项， <i>origin_ifc</i> 是实际接口。对于目标选项， <i>real_ifc</i> 是映射接口。
<i>real_object</i>	标识实际网络对象或对象组（ objectnetwork 或 object-groupnetwork ）。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
<i>real_src_mapped_dest_svc_obj</i>	（可选）对于静态 NAT，指定实际源端口和/或映射目标端口。有关详细信息，请参阅 service 关键字。

round-robin	（可选）为 PAT 池启用循环地址分配。默认情况下，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
route-lookup	（可选）对于路由模式下的身份 NAT，使用路由查找而不是使用 NAT 命令中指定的接口来确定出口接口。如果不在 NAT 命令中指定接口，默认情况下将使用路由查找。
service	（可选）指定端口转换。 • 动态 NAT 和 PAT - 动态 NAT 和 PAT 不支持（其他）端口转换。但是，由于目标转换始终是静态的，因此您可以对目标端口执行端口转换。服务对象（objectservice）可以同时包含源端口和目标端口，但在这种情况下只使用目标端口。系统将忽略您指定的源端口。 • 带端口转换的静态 NAT — 您应该为两个服务对象指定源端口或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。 对于源端口转换，对象必须指定源服务。在本例中，命令中服务对象的顺序为 service real_port mapped_port。对于目标端口转换，对象必须指定目标服务。在这种情况下，服务对象的顺序为 servicemapped_port real_port。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。有关“源”和“目标”术语的详细信息，请参阅“使用指南”部分。 对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。不支持“不等于”（neq）运算符。 NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。
source	配置源地址的转换。
static	配置静态 NAT 或带端口转换的静态 NAT。
unidirectional	（可选）对于静态 NAT，使从源到目标的单向转换；目标地址无法发起流向源地址的流量。此选项可用于测试目的。

Command Default

- 默认情况下，该规则被添加到 NAT 表第 1 部分的末尾。
- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**，表示将规则应用于所有接口。

- (8.3(1)、8.3(2)和8.4(1)) 用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。(8.4(2) 及更高版本) 用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。
- 如果指定可选接口，则 ASA 使用 NAT 配置来确定出口接口。(8.3(1) 到 8.4(1)) 唯一的例外是面向身份 NAT，其中该身份 NAT 始终使用路由查询，无论 NAT 配置如何。(8.4(2) 及更高版本) 对于身份 NAT，默认行为是使用 NAT 配置，但可以选择始终使用路由查找。

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
8.3(1)	添加了此命令。
8.3(2)	当从 8.3 之前版本的 NAT 豁免配置进行迁移时，系统会为生成的静态身份 NAT 规则添加关键字 unidirectional 。
8.4(2)/8.5(1)	添加 no-proxy-arp 了、route-lookuppat-pool和round-robin 键字。 身份 NAT 的默认行为已更改为启用代理 ARP，以匹配其他静态 NAT 规则。 对于 8.3 之前的配置，NAT 豁免规则（命 nat0access-list 令）迁移到 8.4(2) 及更高版本现在包括以下关键字，以禁用代理 ARP 并使用路由查找：no-proxy-arp 和 route-lookup 用于迁移到 8.3(2) 和 8.4(1) 的 unidirectional 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置此时都将包含 no-proxy-arp 和 route-lookup 关键字，以便维持现有功能。unidirectional 关键字将被删除。
8.4(3)	添加 extended flat、和include-reserve 键字。 组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机后续连接将使用相同的 PAT IP 地址。 此功能在 8.5(1) 中不可用。
9.0(1)	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。添加了 interfaceipv6 选项和 net-to-net 选项。
9.5(1)	添加了 block-allocation 关键字。
9.15(1)	已删除 flat 关键字，并且 include-reserve 关键字不再是平面的子参数。现在，所有 PAT 池都使用平面端口范围 1024-65535，并且您可以选择包含保留的端口 1-1023。

版本	修改
9.17(1)	可以将 FQDN 网络对象指定为转换（映射）目的。

使用指南

使用指南

两次 NAT 可供您在单一规则中同时标识源和目标地址。例如，同时指定源和目标地址可以指定：源地址在前往目标 X 时转换为 A，而在前往目标 Y 时转换为 B。



注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果您配置带有端口转换的静态 NAT，并将源地址指定为 Telnet 服务器，并且您希望所有到该 Telnet 服务器的流量的端口从 2323 转换为 23，那么在命令中，您必须指定要转换的源端口（实际：23，映射：2323）。您指定源端口是因为您指定了 Telnet 服务器地址作为地 **source** 址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

两次 NAT 还可以让您将服务对象用于支持端口转换的静态 NAT；网络对象 NAT 仅接受内联定义。

有关两次 NAT 和网络对象 NAT 之间差异的详细信息，请参阅《CLI 配置指南》。

两次 NAT 规则将添加到 NAT 规则表的第 1 部分或第 3 部分（如果已指定）。有关 NAT 排序的更多信息，请参阅 CLI 配置指南。

映射地址指南

映射 IP 地址池不能包括：

- 映射接口的 IP 地址。如 **any** 果为规则指定接口，则所有接口 IP 地址都将被禁止。对于接口 PAT（仅限路由模式），使用关 **interface** 键字而不是 IP 地址。
- （透明模式）管理 IP 地址。
- （动态 NAT）启用 VPN 时的备用接口 IP 地址。
- 现有的 VPN 池地址。

必备条件

- 对于实际地址和映射地址，请使用 **objectnetwork** 或 **object-groupnetwork** 命令）配置网络对象或网络对象组。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- 对于支持端口转换的静态 NAT，请配置 TCP 或 UDP 服务对象（使用 **objectservice** 命令）。

NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。

清除会话转换

如果您更改 NAT 配置，并且不想等待现有转换超时后再使用新的 NAT 信息，则可以使用 `clear xlate` 命令清除转换表。但是，清除转换表会断开所有当前连接。

PAT 池指南

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 记录，而且要使用的 PAT 规则不确定。
- (9.15 之前) 如果可用，则使用真实源端口号作为映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。(8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)) 如果有大量流量使用较低的端口范围，您现在可以指定要使用的固定端口范围，而不是三个大小不等的层级：1024 到 65535，或 1 到 65535。
- (9.15+) 端口映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

在集群中运行时，每个地址的 512 个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。
- 如果将包含主机地址的对象组用于动态 NAT 映射 IP 地址，启用 PAT 池则可以将这些主机地址的使用从 PAT 回退更改为动态 NAT。
- (8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)) 如果在两个单独的规则中使用相同的 PAT 池对象，请确保为每个规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和不分段范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

PAT 池指南的扩展 PAT

- 许多应用检测不支持扩展 PAT。请参阅配置指南以获取不受支持的检查的完整列表。
- 如果为动态 PAT 规则启用扩展 PAT，则您不能将 PAT 池中的地址用作单独的静态 NAT 带端口转换规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。

PAT 池的轮询准则

- (8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)) 如果主机已存在连接，则如果有可用端口，来自该主机的后续连接将使用相同的 PAT IP 地址。： **Note** 这种“粘性”在故障转移后无法继续存在。如果 ASA 发生故障转移，则来自主机的后续连接可能不会使用初始 IP 地址。

- (8.4(2)、8.5(1) 和 8.6(1)) 如果主机具有现有连接，则由于轮询分配，来自该主机的后续连接可能对每个连接使用不同的 PAT 地址。在这种情况下，当您访问交换主机信息的两个网站（例如电子商务网站和支付网站）时可能会遇到问题。当这些站点发现本应是单个主机的两个不同 IP 地址时，事务可能会失败。

NAT 和 IPv6

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践。请注意，当接口是同一网桥组的成员时，不能执行 NAT64/46。

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）当转换为 IPv6 子网（/96 或更低）时，生成的映射地址是 IPv4 嵌入的 IPv6 地址，其中 IPv4 地址的 32 位嵌入在 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

CR_Examples

以下示例包括 10.1.2.0/24 网络上访问两个不同服务器的主机。当主机访问 209.165.201.11 的服务器时，真实地址被转换为 209.165.202.129:port。当主机访问 209.165.200.225 的服务器时，真实地址被转换为 209.165.202.130:port。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

以下示例显示了源端口和目标端口的使用。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机访问服务器进行 Telnet 服务时，真实地址被转换为 209.165.202.129:port。当主机访问同一台服务器进行 Web 服务时，真实地址被转换为 209.165.202.130:port。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
```



```

ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11
ciscoasa(config)# object network PATAddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# service tcp destination eq telnet
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATAddress1 destination
static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
ciscoasa(config)# object network PATAddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# service tcp destination eq http
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATAddress2 destination
static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj

```

以下示例展示支持端口转换的静态接口 NAT 的用途。外部主机通过目标端口 65000 至 65004 连接至外部接口 IP 地址，从而访问内部 FTP 服务器。流量未经转换就通过 192.168.10.100:6500 到 :65004 到达内部 FTP 服务器。请注意，应在服务对象中指定源端口范围（而不是指定目标端口），因为要在命令中将源地址和端口转换为已标识状态；目标端口为“any”。由于静态 NAT 是双向的，“源”和“目标”主要指命令关键字；数据包中的实际源和目标地址与端口取决于发送数据包的主机。在此示例中，连接源自外部，通向内部，因此，FTP 服务器的“源”地址和端口实际是源数据包中的目标地址和端口。

```

ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-object)# service tcp source range 65000 65004
ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-object)# host 192.168.10.100
ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE

```

以下示例在访问 IPv4 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为 IPv6 内部网络 2001:DB8:AAAA::/96 配置动态 NAT：

```

ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254
ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158
ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination static
SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination static
SERVERS_2 SERVERS_2

```

以下示例为内部网络 192.168.1.0/24 配置访问外部 IPv6 Telnet 服务器 2001:DB8::23 时的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任何服务器时使用 PAT 池的动态 PAT。

```

ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200
ciscoasa(config)# object network TELNET_SVR
ciscoasa(config-network-object)# host 2001:DB8::23

```

```
ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23
ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL destination
static SERVERS SERVERS
```

Related Commands

命令	说明
clearconfigurenat	删除 NAT 配置（两次 NAT 和网络对象 NAT）。
show nat	显示 NAT 策略统计信息。
show nat pool	显示有关 NAT 池的信息。
showrunning-confignat	显示 NAT 配置。
show xlate	显示 NAT 会话（转换）信息。
xlateblock-allocation	配置 PAT 端口块分配特征。

nat (object)

要为网络对象配置 NAT，请在对象网络配置模式下使用 **nat** 命令。要删除 NAT 配置，请使用此命令 **no** 的形式。

对于动态 NAT 和 PAT：

```
nat [ (real_ifc,mapped_ifc) ] dynamic { mapped_inline_host_ip [interface [ipv6]] | [mapped_obj]
[pat-pool mapped_obj [round-robin] [extended] [flat [include-reserve]] [block-allocation]]
[interface [ipv6]] } [dns]
```

```
no nat [ (real_ifc,mapped_ifc) ] dynamic { mapped_inline_host_ip [interface [ipv6]] | [mapped_obj]
[pat-pool mapped_obj [round-robin] [extended] [flat [include-reserve]] [block-allocation]]
[interface [ipv6]] } [dns]
```

对于静态 NAT 和带端口转换的静态 NAT：

```
nat [ (real_ifc,mapped_ifc) ] static { mapped_inline_host_ip | mapped_obj | interface [ipv6] } [net-to-net]
[dns | service { tcp | udp | sctp } real_port mapped_port] [no-proxy-arp] [route-lookup]
```

```
no nat [ (real_ifc,mapped_ifc) ] static { mapped_inline_host_ip | mapped_obj | interface [ipv6] } [net-to-net]
[dns | service { tcp | udp | sctp } real_port mapped_port] [no-proxy-arp] [route-lookup]
```

Syntax Description

(real_ifc,mapped_ifc) (可选) 对于静态 NAT，指定实际接口和映射接口。如果您未指定真实接口和映射接口，则使用所有接口。您还可以 **any** 为一个或两个接口指定关键字。确保在命令中包含括号。对于桥接组成员接口（在透明或路由模式下），必须指定实际接口和映射接口；则不能使用 **any**。

block-allocation 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与兼容 **round-robin**，但不能使用 **extended** 或 **flat[include-reserve]** 选项。也无法使用接口 PAT 回退。

dns (可选) 转换 DNS 应答。确保 DNS 检查 (**inspect dns**) 已启用（默认启用）。如果指定了 **service** 关键字（用于静态 NAT），则此选项不可用。请勿将此选项与 PAT 规则一起使用。有关详细信息，请参阅《CLI 配置指南》。

dynamic 配置动态 NAT 或 PAT。

extended (可选) 为 PAT 池启用扩展 PAT。扩展 PAT 通过在转换信息中包含目标地址和端口，为每个服务（而不是每个 IP 地址）使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。

flat [include-reserve]	（可选，9.15 之前版本）分配端口时允许使用整个 1024 到 65535 端口范围。
include-reserve	当选择要转换的映射端口号时，ASA 将使用实际源端口号（如果可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，另请指定 include-reserve 关键字。 (9.15+) 从 9.15 开始，平面是 PAT 池的默认且不可配置的行为。include-reserve 关键字独立于平面关键字，因此您仍然可以选择在 PAT 池中包含保留端口 1-1023。
interface[ipv6]	（可选）对于动态 NAT，如果您在 interface 关键字后指定映射 IP 地址、对象或组，则仅在所有其他映射地址均已分配时才会使用映射接口的 IP 地址。 对于动态 PAT，如果您指定 interface 关键字而不是映射 IP 地址、对象或组，则要将接口 IP 地址用于映射 IP 地址。要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。 如果指定 ipv6，则稍后使用该接口的 IPv6 地址。 对于支持端口转换的静态 NAT，如果另外配置了 service] 关键字，则可以指定 interface 关键字。 对于此选项，您必须为 <i>mapped_ifc</i> 配置一个特定的接口。 不能在透明模式下指定 interface。在路由模式下，如果目标接口为桥接组成员，则不能使用此选项。
mapped_inline_host_ip	如果指定 dynamic，则使用主机 IP 地址来配置动态 PAT。如果指定 static，则映射网络的网络掩码或范围与真实网络的网络掩码或范围相同。比如真实网络里有一个主机，那么这个地址就会被当做主机地址。对于范围或子网，映射地址包含的地址数量与实际范围或子网相同。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 172.20.1.1 指定为映射地址，则映射范围将包括 172.20.1.1 到 172.20.1.6。如果需要多对一映射（我们不建议使用此映射），请使用主机网络对象而非内联地址。
mapped_obj	将映射 IP 地址指定为网络对象 (objectnetwork) 或对象组 (object-groupnetwork)。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。 对于动态 NAT，对象或组不能包含子网。如果需要，可以在不同的动态 NAT 规则之间共享此映射对象。有关不允许的映射 IP 地址的信息，请参阅“映射地址指南”。 对于静态 NAT，通常配置与真实地址相同数量的映射地址，以实现一对一映射。然而，地址数量可以不匹配。有关详细信息，请参阅《CLI 配置指南》。
mapped_port	（可选）指定映射的 TCP/UDP/SCTP 端口。可以通过文字名称或 0 至 65535 范围内的数字指定端口。

net-to-net	(可选) 对于 NAT 46, 指 net-to-net 定将第一个 IPv4 地址转换为第一个 IPv6 地址, 将第二个转换为第二个, 依此类推。如不使用此选项, 则将使用 IPv4 嵌入式方法。对于一对一转换, 必须使用此关键字。
no-proxy-arp	(可选) 对于静态 NAT, 禁用发往映射 IP 地址的传入数据包的代理 ARP。
pat-poolmapped_obj	(可选) 启用地址 PAT 池; 对象中的所有地址均用作 PAT 地址。对于动态 NAT, 可以将 PAT 池配置为回退方法。不能使用同时包含 IPv4 和 IPv6 地址的对象组, 对象组只能包括一种类型的地址。
real_port	(可选) 对于静态 NAT, 指定实际 TCP/UDP/SCTP 端口。可以通过文字名称或 0 至 65535 范围内的数字指定端口。
round-robin	(可选) 为 PAT 池启用循环地址分配。默认情况下, 在使用下一个 PAT 地址之前, 将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口, 然后才返回再次使用第一个地址, 接着是第二个地址, 以此类推。
route-lookup	(可选) 对于路由模式下的身份 NAT, 使用路由查找而不是使用 NAT 命令中指定的接口来确定出口接口。如果不在 NAT 命令中指定接口, 默认情况下将使用路由查找。
service{tcp udp sctp}	(可选) 对于支持端口转换的静态 NAT, 指定用于端口转换的协议: TCP、UDP、SCTP。
static	配置静态 NAT 或带端口转换的静态 NAT。

Command Default

- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**, 表示将规则应用于所有接口。
- (8.3(1)、8.3(2) 和 8.4(1)) 用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。(8.4(2) 及更高版本) 用于身份 NAT 的默认行为已启用代理 ARP, 匹配其他静态 NAT 规则。如果需要, 可以禁用代理 ARP。
- 如果指定可选接口, 则 ASA 使用 NAT 配置来确定出口接口。(8.3(1) 到 8.4(1)) 唯一的例外是面向身份 NAT, 其中该身份 NAT 始终使用路由查询, 无论 NAT 配置如何。(8.4(2) 及更高版本) 对于身份 NAT, 默认行为是使用 NAT 配置, 但可以选择始终使用路由查找。

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。
8.4(2)/8.5(1)	添加 no-proxy-arp 了、、、 route-lookuppat-pool 和关 round-robin 键字。 身份 NAT 的默认行为已更改为启用代理 ARP，以匹配其他静态 NAT 规则。 从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置此时都将包含 no-proxy-arp 和 route-lookup 关键字，以便维持现有功能。
8.4(3)	添加 extended 了 flat 、和关 include-reserve 键字。 组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。 此功能在 8.5(1) 中不可用。
9.0(1)	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。添加了 interfaceipv6 选项和 net-to-net 选项。
9.5(1)	添加了 block-allocation 关键字。
9.5(2)	已添加关 servicesctp 键字。
9.15(1)	已删除 flat 关键字，并且 include-reserve 关键字不再是平面的子参数。现在，所有 PAT 池都使用平面端口范围 1024-65535，并且您可以选择包含保留的端口 1-1023。

使用指南

当数据包进入 ASA 时，将根据网络对象 NAT 规则检查源 IP 地址和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为 规则从未配对，所以不能指定源地址在前往目标 X时应转换为 A，但在前往目标 Y时应转换为 B。对此类功能使用两次 NAT（两次 NAT 可让您识别将源和目标地址放在一起）。

有关两次 NAT 和网络对象 NAT 之间差异的详细信息，请参阅《CLI 配置指南》。

网络对象 NAT 规则将添加到 NAT 规则表的第 2 部分。有关 NAT 排序的更多信息，请参阅 CLI 配置指南。

根据配置，可以根据需要内联配置映射地址，也可以为映射地址创建网络对象或网络对象组（使用 **objectnetwork** 或 **object-groupnetwork** 命令）。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。

NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。

您只能为给定对象定义一条 NAT 规则；如果要配置多条 NAT 规则，则需要创建多个指定相同 IP 地址的对象 **objectnetworkobj-10.10.10.1-01**， **objectnetworkobj-10.10.10.1-02**例如，等等。

映射地址指南

映射 IP 地址池不能包括：

- 映射接口的 IP 地址。如 **any** 果为规则指定接口，则所有接口 IP 地址都将被禁止。对于接口 PAT（仅限路由模式），使用 **interface** 关键字而不是 IP 地址。
- （透明模式）管理 IP 地址。
- （动态 NAT）启用 VPN 时的备用接口 IP 地址。
- 现有的 VPN 池地址。

清除会话转换

如果您更改 NAT 配置，并且不想等待现有转换超时后再使用新的 NAT 信息，则可以使用 `clear xlate` 命令清除转换表。但是，清除转换表会断开所有当前连接。

PAT 池指南

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 记录，而且要使用的 PAT 规则不确定。
- （9.15 之前）如果可用，则使用真实源端口号作为映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。（8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果有大量流量使用较低的端口范围，您现在可以指定要使用的固定端口范围，而不是三个大小不等的层级：1024 到 65535，或 1 到 65535。
- （9.15+）端口映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

在集群中运行时，每个地址的 512 个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。

如果将包含主机地址的对象组用于动态 NAT 映射 IP 地址，启用 PAT 池则可以将这些主机地址的使用从 PAT 回退更改为动态 NAT。

- （8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果在两个单独的规则中使用相同的 PAT 池对象，请确保为每个规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和不分段范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

PAT 池指南的扩展 PAT

- 许多应用检测不支持扩展 PAT。请参阅配置指南以获取不受支持的检查的完整列表。
- 如果为动态 PAT 规则启用扩展 PAT，则您不能将 PAT 池中的地址用作单独的静态 NAT 带端口转换规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。

- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。

PAT 池的轮询准则

- (8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)) 如果主机已存在连接，则如果有可用端口，来自该主机的后续连接将使用相同的 PAT IP 地址。： **Note** 这种“粘性”在故障转移后无法继续存在。如果 ASA 发生故障转移，则来自主机的后续连接可能不会使用初始 IP 地址。
- (8.4(2)、8.5(1) 和 8.6(1)) 如果主机具有现有连接，则由于轮询分配，来自该主机的后续连接可能对每个连接使用不同的 PAT 地址。在这种情况下，当您访问交换主机信息的两个网站（例如电子商务网站和支付网站）时可能会遇到问题。当这些站点发现本应是单个主机的两个不同 IP 地址时，事务可能会失败。
- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。

NAT 和 IPv6

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践。请注意，当接口是同一网桥组的成员时，不能执行 NAT64/46。

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）当转换为 IPv6 子网（/96 或更低）时，生成的映射地址是 IPv4 嵌入的 IPv6 地址，其中 IPv4 地址的 32 位嵌入在 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

CR_Examples

动态 NAT 示例

以下示例配置动态 NAT，将 192.168.2.0 网络隐藏在外部地址范围 2.2.2.1-2.2.2.10 之后：

```
ciscoasa(config)# object network my-range-obj
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

以下示例使用动态 PAT 备份配置 动态 NAT。内部网络 10.76.11.0 中的主机首先映射到 nat-range 1 池 (10.10.10.10-10.10.10.20)。分配 nat-range1 池中的所有地址之后，使用 pat-ip1

地址 (10.10.10.21) 执行动态 PAT。在不太可能发生 PAT 转换也用完的情况下，使用外部接口地址执行动态 PAT。

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20
ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21
ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

以下示例使用动态 PAT 备份配置动态 NAT，将 IPv6 主机转换为 IPv4 主机。内部网络 2001:DB8::/96 上的主机首先映射到 IPv4_NAT_RANGE 池（209.165.201.1 到 209.165.201.30）。分配 IPv4_NAT_RANGE 池中的所有地址之后，使用 IPv4_PAT 地址（209.165.201.31）执行动态 PAT。在 PAT 转换也被用完的情况下，使用外部接口地址执行动态 PAT。

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30
ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31
ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

动态 PAT 示例

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在地址 2.2.2.2 后面：

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口地址后面：

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

以下示例配置动态 PAT，使用 PAT 池将内部 IPv6 网络转换为外部 IPv4 网络：

```
ciscoasa(config)# object network IPv4_POOL
ciscoasa(config-network-object)# range 203.0.113.1 203.0.113.254
ciscoasa(config)# object network IPv6_INSIDE
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

静态 NAT 示例

以下示例配置静态 NAT，将内部的真实主机 1.1.1.1 配置为外部的 2.2.2.2，并启用 DNS 重写。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

以下示例使用映射对象为内部的真实主机 1.1.1.1 配置到外部的 2.2.2.2 的静态 NAT。

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

以下示例配置静态 NAT，将 TCP 端口 21 处的 1.1.1.1 转换为端口 2121 处的外部接口。

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

以下示例将内部 IPv4 网络映射到外部 IPv6 网络。

```
ciscoasa(config)# object network inside_v4_v6
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

以下示例将内部 IPv6 网络映射到外部 IPv6 网络。

```
ciscoasa(config)# object network inside_v6
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

身份 NAT 示例

以下示例使用内联映射地址将主机地址映射到它本身：

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 10.1.1.1
```

以下示例使用网络对象 将主机地址映射到它本身：

```
ciscoasa(config)# object network my-host-obj1-identity
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

Related Commands

命令	说明
clearconfigurenat	删除 NAT 配置（两次 NAT 和网络对象 NAT）。
show nat	显示 NAT 策略统计信息。
show nat pool	显示有关 NAT 池的信息。
showrunning-confignat	显示 NAT 配置。
show xlate	显示转换信息。
xlateblock-allocation	配置 PAT 端口块分配特征。

nat (vpn load-balancing)

要设置 NAT 将此设备的 IP 地址转换为的 IP 地址，请在 VPN 负载均衡配置模式下使用 **nat**命令。要禁用此 NAT 转换，请使用此命令 **no** 的形式。

```
nat ip-address
no nat [ ip-address]
```

Syntax Description *ip-address* 您希望此 NAT 将此设备的 IP 地址转换为的 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
VPN 负载均衡配置	• 是	• —	• 是	• —	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南 必须先使用 **vpnload-balancing**命令进入 VPN 负载均衡模式。

在命令的 **nonat** 形式中，如果指定可选的 *ip-address* 值，则该 IP 地址必须与运行配置中的现有 NAT IP 地址相匹配。

CR_Examples 以下 VPN 负载均衡命令序列示例包含一条 **nat**命令，该命令将 NAT 转换地址设置为 192.168.10.10：

```
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 port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

Related Commands

命令	说明
vpnload-balancing	进入 VPN 负载均衡模式。

nat-assigned-to-public-ip

要自动将 VPN 对等体的本地 IP 地址转换回对等体的实际 IP 地址，请在 tunnel-group general-attributes 配置模式下使用 **nat-assigned-to-public-ip** 命令。要禁用 NAT 规则，请使用此命令的 **no** 形式。

```
nat-assigned-to-public-ip interface
no nat-assigned-to-public-ip interface
```

Syntax Description *interface* 指定要应用 NAT 的接口。

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
隧道组常规属性配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
8.4(3)	添加了此命令。

使用指南 在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 IP 地址。

可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。您可以使用命令查看规则。 **shownat**

数据流

以下步骤介绍启用此功能时通过 ASA 的数据包流：

- VPN 对等体向 ASA 发送数据包。
- 外部源/目的包含对等体公共 IP 地址/ASA IP 地址。加密的内部源/目的地包含 VPN 分配的 IP 地址/内部服务器地址。
- ASA 将解密数据包（删除外部源/目标）。
- ASA 为内部服务器执行路由查找，并将数据包发送到内部接口。

4. 自动创建的 VPN NAT 策略会将 VPN 分配的源 IP 地址转换为对等体公用 IP 地址。
5. ASA 将转换后的数据包发送到服务器。
6. 服务器响应数据包，并将其发送到对等体的公共 IP 地址。
7. ASA 接收响应，将目标 IP 地址逆向转换为 VPN 分配的 IP 地址。
8. ASA 将未转换的数据包转发到外部接口并在其中对其进行加密，并添加由 ASA IP 地址/对等体公共 IP 地址组成的外部源/目的地。
9. ASA 将数据包发回对等体。
10. 对等体解密并处理数据。

限制

由于路由问题，除非您确定自己需要此功能，否则我们不建议使用此功能。请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制：

- 仅支持 Cisco IPsec 和 Secure Client。
- 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。
- 如果启用反向路由注入（请参阅 `setreverse-route` 命令），则仅通告 VPN 分配的 IP 地址。
- 不支持负载均衡（由于路由问题）。
- 不支持漫游（公共 IP 更改）。

CR_Examples

以下示例对“vpnclient”隧道组启用到公共 IP 的 NAT：

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

以下是 `show nat detail` 命令的输出示例，其中显示一条自动 NAT 规则，来自网段为 209.165.201.10（已分配 IP 为 10.1.226.174）的设备：

```
ciscoasa# show nat detail
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

Related Commands

命令	说明
<code>show nat</code>	显示当前网络地址转换。
<code>tunnel-group general-attributes</code>	设置隧道组的常规属性。
<code>debug menu webvpn 99</code>	对于 AnyConnect SSL 会话，VPN NAT 接口存储在会话中。

命令	说明
debugmenuike2 <i>peer_ip</i>	对于思科 IPsec 客户端会话，VPN NAT 接口存储在 SA 中。
调试 nat 3	显示 NAT 的调试消息。

nat-rewrite

要为 DNS 响应的 A 记录中嵌入的 IP 地址启用 NAT 重写，请在参数配置模式下使用 **nat-rewrite** 命令。要禁用此功能，请使用此 **no** 命令的形式。

nat-rewrite
no nat-rewrite

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，NAT 重写已启用。配置 **inspectdns** 后，即使未定义 **policy-map type inspect dns**，也可以启用此功能。要禁用，必须在策略映射配置中明确声明 **nonat-rewrite**。如果未配置 **inspectdns**，则不执行 NAT 重写。

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。

使用指南

此功能对 DNS 响应中的 A 类型资源记录 (RR) 执行 NAT 转换。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 NAT 重写：

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

Related Commands

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

nbns-server

要配置 NBNS 服务器，请在 tunnel-group webvpn-attributes 配置模式下使用 **nbns-server** 命令。要从配置中删除 NBNS 服务器，请使用此命令的 **no** 形式。

ASA 查询 NBNS 服务器以将 NetBIOS 名称映射到 IP 地址。WebVPN 需要 NetBIOS 来访问或共享远程系统上的文件。

```
nbns-server {ipaddr | 主机名} [master ] [timeout timeout] [retry retries]
no nbns-server
```

Syntax Description

hostname	指定 NBNS 服务器的主机名。
ipaddr	指定 NBNS 服务器的 IP 地址。
master	表示这是主浏览器而不是 WINS 服务器。
retry	表示后面是一个重试值。
retries	指定重试 NBNS 服务器查询的次数。在发送错误消息之前，ASA 会按照您在此处指定的次数循环遍历服务器列表。默认值为 2；范围为 1 至 10。
timeout	表示后面是超时值。
timeout	指定 ASA 再次发送查询之前等待的时间（如果只有一个服务器，则向同一服务器发送查询；如果有多个 NBNS 服务器，则向另一个服务器发送查询）。默认超时是 2 秒，范围是 1 至 30 秒。

Command Default

默认没有配置NBNS服务器。

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-attributes 配置	• 是	• —	• 是	• —	—

Command History

版本	修改
7.0(1)	添加了此命令。
7.1(1)	已从 webvpn 模式进入隧道组 webvpn 配置模式。

使用指南

在版本 7.1(1) 中，如果您在 `webvpn` 配置模式下输入此命令，它将转换为 `tunnel-group webvpn-attributes` 配置模式下的相同命令。

最多 3 个服务器条目。您配置的第一台服务器为主服务器，其他为备用服务器（用于实现冗余）。

使用 **no** 选项从配置中删除匹配的条目。

CR_Examples

以下示例显示如何配置具有 NBNS 服务器（作为主浏览器）的隧道组 “test”，IP 地址为 10.10.10.19，超时值为 10 秒，重试次数为 8。它还显示如何使用 IP 地址 10.10.10.24、15 秒的超时值和 8 次重试来配置 NBNS WINS 服务器。

```
ciscoasa
(config)#
  tunnel-group test type webvpn
ciscoasa
(config)#
  tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

命令	说明
<code>clear configure group-policy</code>	删除特定组策略或所有组策略的配置。
<code>show running-config group-policy</code>	显示特定组策略或所有组策略正在运行的配置。
<code>tunnel-group webvpn-attributes</code>	指定命名隧道组的 WebVPN 属性。

neighbor (router eigrp)

要定义与其交换路由信息的 EIGRP 邻居路由器，请在路由器 eigrp 配置模式下使用 **neighbor** 命令。
要删除邻居条目，请使用此命令的形式。

neighbor IP 地址 interface 名称
no neighbor IP 地址 interface 名称

Syntax Description	interface name nameif 命令所指定的接口名称，通过该接口可访问邻居。
	ip_address 与其交换路由信息的邻居路由器的 IPv4 或 IPv6 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
路由器 eigrp 配置	—	•	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。
	9.20(1) 增加了对 IPv6 的支持。

使用指南	可以使用多个 neighbor 语句来与特定 EIGRP 邻居建立对等会话。必须在 neighbor 语句中指定 EIGRP 交换路由更新所使用的接口。两个 EIGRP 邻居交换路由更新所使用的接口必须使用来自同一网络的 IP 地址进行配置。



注释 为接口配置该命令将抑制该接口上的 **passive-interface** 所有传入和传出的路由更新和 hello 消息。无法在配置为被动的接口上建立或维护 EIGRP 邻居邻接关系。

EIGRP 问候消息作为单播消息发送到使用 **neighbor** 命令定义的邻居。

CR_Examples	以下示例配置与 192.168.1.1 和 192.168.2.2 邻居的 EIGRP 对等会话：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

CR_Examples

以下示例配置与 fe80::250:56ff:feb9:b41b 和 fe80::250:56ff:fe9f:13f4 邻居的 EIGRP 对等会话：

```
ciscoasa(config)# rtr eigrp 100
ciscoasa(config-rtr)# neighbor fe80::250:56ff:feb9:b41b interface gig1
ciscoasa(config-rtr)# neighbor fe80::250:56ff:fe9f:13f4 interface branch_office
```

Related Commands

命令	说明
debugeigrpneighbors	显示 EIGRP 邻居消息的调试信息。
showeigrpneighbors	显示 EIGRP 邻居表。

neighbor (router ospf)

要在点对点非广播网络上定义静态邻居，请在路由器 ospf 配置模式下使用 **neighbor** 命令。要从配置中删除静态定义的邻居，请使用此命令的 **no** 形式。

neighbor IP 地址 [interface 名称]
no neighbor IP 地址 [interface 名称]

Syntax Description	interfacename （可选）指定 nameif 命令所指定的可以通过其访问邻居的接口名称。
	ip_address 指定邻居路由器的 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
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。
	9.0(1) 增加了多情景模式支持。

使用指南

neighbor 命令用于通过 VPN 隧道通告 OSPF 路由。必须为每个已知的非广播网络邻居包含一个邻居条目。邻居地址必须在接口的主地址上。

当邻居与系统的任何直接连接的接口不在同一网络上时，需要指定 **interface** 选项。此外，必须创建静态路由才能到达邻居。

CR_Examples

以下示例使用地址 192.168.1.1 定义了邻居路由器：

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

Related Commands	命令	说明
	routerospf	进入路由器配置模式。

命令	说明
showrunning-configrouter	显示全局路由器配置中的 命令。

neighbor activate

要启用与边界网关协议 (BGP) 邻居的信息交换，请在 address-family 配置模式下使用 neighbor activate 命令。要禁用与 BGP 邻居交换地址，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } activate
no neighbor { ip_address | ipv6-address } activate
```

Syntax Description	ip_address	BGP 路由器的 IP 地址。
	ipv6-address	BGP 路由器的 IPv6 地址

Command Default 对于 IPv4 地址系列，默认情况下与 BGP 邻居启用地址交换。无法为任何其他地址系列启用地址交换。



注释 默认情况下，对于通过 neighbor remote-as 命令定义的每个 BGP 路由会话，启用 IPv4 地址系列的地址交换；否则，除非在配置 neighbor remote-as 命令之前配置了 no bgp default ipv4-activate 命令，或者使用了 no neighbor activate 命令禁用了与特定邻居的地址交换。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 增加了 ipv6-address 参数以及对 IPv6 地址系列的支持。

使用指南 您可以使用此命令以 IP 前缀的形式通告地址信息。地址前缀信息在 BGP 中称为网络层可达性信息 (NLRI)。

CR_Examples 以下示例为 BGP 邻居 172.16.1.1 启用 IPv4 地址系列单播的地址交换：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
```



```
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

以下示例显示如何为名为 **group2** 的 BGP 对等体组中的所有邻居以及 BGP 邻居 7000::2 启用地址系列 IPv6 的地址交换：

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

命令	说明
neighborremote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。

neighbor advertise-map

要通告 BGP 表中与已配置的路由映射匹配的路由，请在路由器配置模式下使用 neighbor advertise-map 命令。要禁用路由通告，请使用此命令的no形式。

```
neighbor { ip_address | ipv6-address } advertise-map map-name { exist-map map-name |
non-exist-map map-name } [ check-all-paths ]
no neighbor { ip_address | ipv6-address } advertise-map map-name { exist-map map-name |
non-exist-map map-name } [ check-all-paths ]
```

Syntax Description	ipv4_address	指定应接收条件通告的路由器的 IPv4 地址。
	ipv6_address	指定应接收条件通告的路由器的 IPv6 地址。
	advertise-map map-name	指定在满足存在映射或不存在映射的条件时将被通告的路由映射的名称。
	exist-map map-name	指定 exist-map 的名称，与 BGP 表中的路由进行比较，以确定是否通告 advertise-map 路由。
	non-exist-map map-name	指定不存在的映射表名称，与 BGP 表中的路由进行比较，以确定是否发布 advertise-map 路由。
	check-all-paths	（可选）启用 BGP 表中带有前缀的现有映射检查所有路径。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.3(1) 添加了此命令。

使用指南 使用 neighbor advertise-map 命令有条件地通告选定路由。有条件通告的路由（前缀）在两个路由映射中定义：通告映射以及存在映射或非存在映射。

与存在映射或非存在映射关联的路由映射指定 BGP 发言者将跟踪的前缀。

与通告映射关联的路由映射指定条件满足时将通告到指定邻居的前缀。

如果配置了存在映射，则当前缀同时存在于广告映射和存在映射中时，满足条件。

如果配置了不存在的映射，则当前缀在广告映射中存在，但在不存在的映射中不存在时，满足条件。

如果条件未满足，则路由将撤消并且不会进行条件通告。可能已动态通告或未通告的所有路由都需要在 BGP 路由表中存在才能进行条件通告。

CR_Examples

以下路由器配置示例将 BGP 配置为检查所有：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

以下地址系列配置示例将 BGP 配置为使用非存在映射有条件地向 10.1.1.1 邻居通告前缀。

如果前缀存在于 MAP3 中而不是 MAP4 中，则满足条件并通告前缀。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

以下对等组配置示例将 BGP 配置为针对 BGP 邻居的前缀检查所有路径：

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor routel send-community both
ciscoasa(config-router-af)# neighbor routel advertise-map MAP1 exist-map MAP2 check-all-paths
```

Related Commands

命令	说明
address-family ipv4	进入地址系列配置模式。

neighbor advertisement-interval

要设置发送 BGP 路由更新之间的最小路由通告间隔 (MRAI)，请在 address-family 配置模式下使用 neighbor advertise-interval 命令。要恢复默认值，请使用此命令的no形式

```
neighbor { ip_address | ipv6-address } advertisement-intervalseconds
no neighbor { ip_address | ipv6-address } advertisement-intervalseconds
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址
	seconds	发送 BGP 路由更新的最小时间间隔。
		有效值介于 0 到 600 之间。

Command Default	不在 VRF 中的 eBGP 会话：30 秒
	VRF 中的 eBGP 会话：0 秒
	iBGP 会话：0 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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 当 MRAI 等于 0 秒时，一旦 BGP 路由表发生更改，就会发送 BGP 路由更新。

CR_Examples 以下示例将发送 BGP 路由更新的最小间隔时间设置为 10 秒：

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

以下示例将发送 BGPv6 路由更新的最小间隔时间设置为 100 秒：

```
asa(config-router-af)# neighbor 2001::1 advertisement-interval 100
```

Related Commands

命令	说明
neighbor remote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor default-originate

要允许 BGP 发言者（本地路由器）将默认路由 0.0.0.0 发送至邻居以用作默认路由，请在 address-family 配置模式下使用 neighbor default-originate 命令。要不发送任何路由作为默认值，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } default-originate [ route-map route-map name ]
no neighbor { ip_address | ipv6-address } default-originate [ route-map route-map name ]
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	route-map	路由映射名称 （可选）路线图的名称。路由映射允许有条件地注入路由 0.0.0.0。

Command Default 不会向邻居发送默认路由。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此命令不要求本地路由器中存在 0.0.0.0。与路由图一起使用时，如果路由图包含匹配 IP 地址子句并且存在与 IP 访问列表完全匹配的路由，则会注入默认路由 0.0.0.0。路由映射还可以包含其他 match 子句。

可以将标准或扩展访问列表与 neighbor default-Originate 命令配合使用。

CR_Examples 在以下示例中，本地路由器无条件地将路由 0.0.0.0 注入邻居 72.16.2.3：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
In the following example, the local router injects route 0.0.0.0 to the neighbor 2001::1:
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

Related Commands

命令	说明
neighbor remote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。
neighbor activate	启用与 BGP 邻居的信息交换。

邻居描述

要将描述与邻居关联，请在地址系列配置模式下使用 `neighbor description` 命令。要删除描述，请使用此命令的`no`形式。

neighbor { *ip_address* | *ipv6-address* } **description** 文本
no neighbor { *ip_address* | *ipv6-address* } **description** 文本

Syntax Description	<i>ip_address</i>	邻居路由器的 IP 地址。
	<i>ipv6-address</i>	邻居路由器的 IPv6 地址。
	文本	用于描述邻居的文本（长度最多为 80 个字符）。

Command Default 没有该邻居的说明信息。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本	修改
	9.2(1)	添加了此命令。
	9.3(2)	添加了 <code>ipv6-address</code> 参数，并添加了对 IPv6 地址系列的支持。

CR_Examples 在以下示例中，邻居的说明是“peer with example.com”：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

在以下示例中，IPv6 邻居的描述为“peer with example.com”：

```
ciscoasa(config-router-af)#neighbor 2001::1 description peer with example.com
```

Related Commands	命令	说明
	neighborremote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。

命令	说明
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor disable-connected-check

要禁用连接验证以与使用环回接口的单跳对等体建立 eBGP 对等会话，请在地址系列配置模式下使用邻居 disable-connected-check 命令。要启用 eBGP 对等会话的连接验证，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } disable-connected-check
no neighbor { ip_address | ipv6-address } disable-connected-check
```

Syntax Description	ip_address 邻居路由器的 IP 地址。
	ipv6-address 邻居路由器的 IPv6 地址。

Command Default BGP路由进程会默认验证单跳eBGP对等会话（TTL=254）的连接性，判断eBGP对等体是否直连到同一个网段。如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 neighbour disable-connected-check 命令用于禁用可通过单跳到达但在环回接口上配置或使用非直接连接 IP 地址配置的 eBGP 对等会话的连接验证过程。

仅当邻居 ebgp-multihop 命令配置的 TTL 值为 1 时，才需要此命令。单跳 eBGP 对等体的地址必须可访问。必须配置 neighbor update-source 命令，以允许 BGP 路由进程将环回接口用于对等会话。

CR_Examples

在以下示例中，配置了可在同一网段上通过每台路由器上的本地环回接口访问的两个 BGP 对等体之间的单跳 eBGP 对等会话：

BGP Peer 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
```

```
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
BGP Peer 2
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
BGPv6 Peer
ciscoasa(config-router)# neighbor 2001::1 disable-connected-check
```

Related Commands

命令	说明
neighborremote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。
neighbor ebgp-multihop	接受或启动与位于非直接连接网络上的外部对等体的 BGP 连接。

neighbor distribute-list

要分发访问列表中指定的 BGP 邻居信息，请在地址系列配置模式下使用 neighbor Distribution-list 命令。要删除条目，请使用此命令的 no 形式。

```
neighborip_addressdistribute-list {access-list-name} {in|out}
no neighborip_addressdistribute-list {access-list-name} {in|out}
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	access-list-name	标准访问列表的名称。
	范围	访问列表适用于该邻居的传入广告
	out	访问列表适用于向该邻居发出的通告

Command Default 未指定 BGP 邻居。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。

- 使用指南 使用分发列表是过滤通告的多种方法的一种。也可以使用以下方法过滤通告：
- 自治系统路径过滤器可以使用 ip as-path access-list 和 neighbor filter-list 命令进行配置。
 - 可以使用 access-list（IP standard）命令配置标准访问列表，用于过滤通告。
 - 可以使用 route-map (IP) 命令过滤通告。可以使用自治系统过滤器、前缀过滤器、访问列表和分发列表来配置路由映射。

标准访问列表可用于过滤路由更新。但是，对于使用无类域间路由 (CIDR) 的路由过滤，标准访问列表不提供配置网络地址和掩码高级过滤所需的精细级别。

CR_Examples

在以下示例中，标准访问列表分发列表 `acl` 中的 BGP 邻居信息被应用于传入到邻居 172.16.4.1 的通告。

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
网络	指定要由 BGP 通告的网络。
access-list permit	指定要转发的数据包。
access-list deny	指定要拒绝的数据包。

neighbor ebgp-multihop

要接受并尝试与未直接连接的网络上的外部对等体建立 BGP 连接，请在 address-family 配置模式下使用 neighbor ebgp-multihop 命令。要恢复默认值，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } ebgp-multihop [ ttl ]
no neighbor { ip_address | ipv6-address } ebgp-multihop
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	ttl	（可选）生存时间。
		有效值介于 1 至 255 跳之间。

Command Default 仅允许直接连接的邻居。

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
地址族配置模式	• 是	• —	• 是	• 支持	—

Command History	版本	修改
	9.2(1)	添加了此命令。
	9.3(2)	添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此功能只能在思科技术支持人员的指导下使用。为了防止通过振荡路由创建环路，如果通往多跳对等体的唯一路由是默认路由 (0.0.0.0)，则将不会建立多跳。

CR_Examples 以下示例允许进出邻居 10.108.1.1 的连接，该邻居位于未直连的网络上：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

以下示例允许进出邻居 2001::1 的连接，该邻居位于未直连的网络上：

```
ciscoasa(config)# router bgp 3
```

```
ciscoasa(config-router)# address-family ipv6  
ciscoasa(config-router-af) neighbor 12001::1 ebgp-multihop
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor fall-over bfd (router bgp)

要配置对 BGP 的 BFD 支持，以便注册 BGP 以接收来自 BFD 的转发路径检测失败消息，请在配置邻居时使用 **fall-over** 选项。

neighbor*ip_address* | *ipv6_address***fall-over bfd**

Syntax Description *ip_address/ipv6_address* 邻居路由器的 IP/IPv6 地址 ABCD/ X:X:X:X::X 格式。

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 BFD 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(2)	添加了此命令。

使用指南 为多跳配置 BGP 的 BFD 支持时，请确保已为源目标对创建 BFD 映射。

CR_Examples 以下示例为 172.16.10.2 和 1001::2 邻居配置 BFD 支持：

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.10.2 fall-over bfd
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 1001::2 fall-over bfd
```

命令	说明
authentication	在 BFD 模板中为单跳和多跳会话配置身份验证。
bfd echo	在接口上启用 BFD 回声模式，
bfdinterval	在接口上配置基准 BFD 参数。
bfd 映射	配置将地址与多跳模板关联的 BFD 映射。

命令	说明
bfd 慢计时器	配置 BFD 慢速计时器值。
BFD模板	将单跳 BFD 模板绑定到接口。
bfd-template单跳 多跳	配置 BFD 模板并进入 BFD 配置模式。
清除 BFD 计数器	清除 BFD 计数器。
echo	在 BFD 单跳模板中配置回应。
show bfd drops	显示 BFD 中已丢弃的数据包数。
show bfd map	显示配置的 BFD 映射。
show bfd neighbors	显示现有 BFD 邻接关系逐行列表。
show bfd summary	显示 BFD 的概要信息。

neighbor filter-list

要设置 BGP 过滤器，请在地址系列配置模式下使用 neighbor filter-list 命令。要禁用该功能，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } filter-list access-list-name { in | out }
no neighbor { ip_address | ipv6-address } filter-list access-list-name { in | out }
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	access-list-name	自主系统路径访问列表的名称。您可以使用 as-path access-list 命令定义此访问列表。
	范围	访问列表应用于传入路由。
	out	访问列表将应用于传出路由。

Command Default 不使用 BGP 过滤器。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此命令将在入站和出站 BGP 路由上建立过滤器。



注释 请勿在任何给定方向（入站或出站）上同时将邻居分发列表和邻居前缀列表命令应用于邻居。这两个命令是互斥的，并且每个入站或出站方向只能应用一个命令（邻居分发列表或邻居前缀列表）。

CR_Examples 在以下地址系列配置模式示例中，不会向使用 IP 地址 172.16.1.1 的 BGP 邻居发送通过或从相邻自治系统 123 发送的有关任何路径的通告：

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_  
ciscoasa(config)# as-path access-list as-path-acl deny ^123$  
ciscoasa(config)#router bgp 109  
ciscoasa(config-router)# address-family ipv4  
ciscoasa(config-router-af)# network 10.108.0.0  
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123  
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47  
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

在以下地址系列配置模式示例中，系统不会向 IP 地址为 2001::1 的 BGPv6 邻居发送关于任何通过或从相邻自治系统传递的路径的通告：

```
ciscoasa(config-router-af)# neighbor 2001::1 filter-list as-path-acl out
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。
网络	指定 BGP 路由进程要通告的网络。

neighbor ha-mode graceful-restart

要为 BGP 邻居启用或禁用边界网关协议 (BGP) 平稳重启功能，请在 address-family 配置模式下使用 neighbor ha-mode graceful-restart 命令。要从配置中删除邻居的 BGP 平稳重启功能，请使用此命令的 no 形式。

```
neighborip_addressha-mode graceful-restart [ disable ]
no neighborip_addressha-mode graceful-restart
```

Syntax Description	ip_address 邻居的 IP 地址。
	disable （可选）禁用邻居的 BGP 平滑重启功能。

Command Default BGP平滑重启功能处于关闭状态。

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
Address-family 配置	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.3(1) 添加了此命令。

使用指南 neighbor ha-mode graceful-restart 命令用于为单个 BGP 邻居启用或禁用平稳重启功能。如果以前为 BGP 对等体启用了平稳重启，则使用 disable 关键字可禁用平稳重启功能。

会话建立过程中，在 OPEN 消息中支持无间断转发 (NSF) 和 NSF 感知的对等体之间协商平稳重启功能。如果在建立 BGP 会话后启用了平滑重启功能，则需要通过软重置或硬重置重新启动会话。

具备 NSF 功能和 NSF 感知的 ASA 支持平稳重启功能。支持 NSF 功能的 ASA 可以执行状态切换 (SSO) 操作（平稳重启），并且可以通过在 SSO 操作期间保留路由表信息来协助对等体重启。支持 NSF 感知的 ASA 与支持 NSF 功能但无法执行 SSO 操作的路由器类似。



注释 要对所有 BGP 邻居全局启用 BGP 平稳重启功能，请使用 bgp graceful-restart 命令。为单个邻居配置 BGP 平稳重启功能时，每种配置重启的方法具有相同的优先级，并且最后的配置实例将应用于邻居。

使用 show bgp neighbors 命令验证 BGP 邻居的 BGP 平稳重启配置。

CR_Examples

以下示例为 BGP 邻居 172.21.1.2 启用 BGP 平稳重启功能：

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

Related Commands

命令	说明
bgpgraceful-restart	为所有 BGP 邻居全局启用或禁用 BGP 平稳重启功能。
show bgp neighbors	显示有关与邻居的 TCP 和 BGP 连接的信息。

neighbor local-as

要自定义从外部边界网关协议 (eBGP) 邻居接收的路由的 AS_PATH 属性，请在地址系列配置模式下使用邻居 local-as 命令。要禁用 AS_PATH 属性定制，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } local-as [ autonomous-system-number [ no-prepend [ replace-as [ dual-as ] ] ] ]
no neighbor { ip_address | ipv6-address } local-as
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	自治系统编号	（可选）要添加到 AS_PATH 属性的自治系统编号。此参数的值范围是从 1 到 65535 的任意有效的自治系统编号。 注释 使用此参数，您无法从本地 BGP 路由进程或远程对等方的网络指定自治系统编号。 有关自治系统编号格式的详细信息，请参阅 router bgp 命令。
	无预置	（可选）不要将本地自治系统编号添加到从 eBGP 邻居接收的任何路由之前。
	替换为	（可选）在 eBGP 更新中将实际自治系统编号替换为本地自治系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。
	双重 AS	（可选）配置 eBGP 邻居使用真实自治系统编号（来自本地 BGP 路由进程）或使用通过 autonomous-system-number 参数配置的自治系统编号 (local-as) 建立对等会话。

Command Default 默认情况下，本地 BGP 路由进程的自治系统编号会被添加到所有外部路由的前面。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南

`neighbour local-as` 命令用于通过添加和删除从 eBGP 邻居接收的路由的自治系统编号来定制 `AS_PATH` 属性。为了支持自治系统编号迁移，此命令的配置允许路由器作为其他自治系统的成员显示为外部对等体。此功能允许网络运营商在正常服务时段将客户迁移到新配置而无需中断现有的对等布置，简化了在 BGP 网络中更改自治系统编号的过程。



注意 BGP 预置路由穿越的每个 BGP 网络的自治系统号，以维护网络可达性信息和防止路由环路。此命令应仅针对自主系统迁移进行配置，并且应在转换完成后取消配置。此程序应仅由经验丰富的网络操作员尝试执行。配置不当可能会造成路由环路

此命令仅可用于真正的 eBGP 对等会话。此命令不适用于联盟的不同子自治系统中的两个对等体。

为确保顺利过渡，我们建议将使用 4 字节自主系统编号标识的自主系统中的所有 BGP 发言者升级为支持 4 字节自主系统编号。

CR_Examples

本地 AS 示例

以下示例使用 `local-as` 功能通过自治系统 300 在 Router 1 和 Router 2 之间建立对等关系：

Router1(Localrouter)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300Router 2 (Remote router)
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

无预置关键字配置示例

以下示例将 BGP 配置为不将自治系统 500 预置到从 192.168.1.1 邻居接收的路由：

```
ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend
```

替换为关键字配置示例

以下示例从 172.20.1.1 邻居的出站路由更新中删除专用自治系统 64512，并将其替换为自治系统 600：

```
ciscoasa(config)# router bgp 64512

ciscoasa(config-router)# address-family ipv4

ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as
```

```
ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as
```

双重 as 关键字配置示例

以下示例显示了两个运营商网络和一个客户网络的配置。路由器 1 属于自治系统 100，路由器 2 属于自治系统 200。自治系统 200 正在合并到自治系统 100 中。发生这种转换需要在不中断自治系统 300（客户网络）中路由器 3 的服务的情况下进行。在路由器 1 上配置 neighbor local-as 命令，以允许路由器 3 在过渡期间保持与自治系统 200 的对等关系。在过渡完成后，可以在正常维护窗口或其他计划停机期间，将路由器 3 上的配置更新为自治系统 100 的对等体。

Router1Configuration(LocalProviderNetwork)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

Router2Configuration(RemoteProviderNetwork)

```
ciscoasa(config)# router bgp 200

ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

Router3Configuration(RemoteCustomerNetwork)

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

为了在两个自治系统合并后完成迁移，需要在路由器 3 上更新对等会话：

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

BGPv6 配置

```
ciscoasa(config-router-af)# neighbor 2001::1 local-as 500 no-prepend
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
bgp router-id	为本地边界网关协议 (BGP) 路由进程配置固定的路由器 ID。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	向 BGP 或多协议 BGP 邻居表添加一个条目。

命令	说明
网络	指定 BGP 路由进程要通告的网络。
synchronization	实现 BGP 与内部网关协议 (IGP) 系统之间的同步

neighbor maximum-prefix

要控制可从邻居接收的前缀的数量，请在地址系列配置模式下使用 `neighbor maximum-prefix` 命令。要禁用该功能，请使用此命令的 `no` 形式。

```
neighbor { ip_address | ipv6-address } maximum-prefix maximum [ threshold ] [ restart restart-interval ] [ warning-only ]
no neighbor { ip_address | ipv6-address } maximum-prefix maximum
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	最大值	此邻居允许的最大前缀数。
	阈值	（可选）整数，指定路由器在达到最大值的百分比时开始生成警告消息。范围为 1 至 100，默认值为 75（百分比）。
	restart	（可选）配置运行 BGP 的路由器，以自动重新建立因超过最大前缀限制而被禁用的对等会话。重启计时器使用 restart-interval 参数配置。
	restart-interval	（可选）重新建立对等会话的时间间隔（以分钟为单位）。范围是 1 至 65535 分钟。
	仅警告	（可选）允许路由器在超过最大值时生成日志消息，而不是终止对等连接。

Command Default 此命令默认禁用。前缀的数量没有限制。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 使用此命令可以配置允许 BGP 路由器从对等体接收的前缀的最大数量。它添加了另一种机制（除了分发列表、过滤列表和路由映射之外）来控制从对等体接收的前缀。

当收到的前缀数量超过配置的最大数量时，路由器将终止对等（默认情况下）。但是，如果配置了 **warning-only** 关键字，则路由器只发送日志消息，但会继续与发送方建立对等关系。如果对等体终止，对等体将保持关闭，直到发出 **clear bgp** 命令为止。

CR_Examples

以下示例将允许从 192.168.6.6 的邻居发送的前缀的最大数量设置为 1000：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

以下示例将所允许的来自 2001::1 的邻居的前缀的最大数量设置为 1000：

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
网络	指定 BGP 路由进程要通告的网络。

neighbor next-hop-self

要将路由器配置为 BGP 发言邻居的下一跳，请在地址系列配置模式下使用 neighbor next-hop-self 命令。要禁用此功能，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } next-hop-self
no neighbor { ip_address | ipv6-address } next-hop-self
```

Syntax Description	ip_address 邻居路由器的 IP 地址。
	ipv6-address 邻居路由器的 IPv6 地址。
	仅警告 （可选）允许路由器在超过最大值时生成日志消息，而不是终止对等连接。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此命令在无网状结构的网络（例如帧中继或 X.25）中非常有用，在该类网络中，BGP 邻居可能没有对同一 IP 子网上所有其他邻居的直接访问权限。

CR_Examples 以下示例强制以 10.108.1.1 为目标的所有更新将此路由器通告为下一跳：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

以下示例强制以 2001::1 为目标的所有更新将此路由器通告为下一跳：

```
ciscoasa(config-router-af)#neighbor 2001::1 next-hop-selfs
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor password

要在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 5 (MD5) 身份验证，请在地址系列配置模式下使用 neighbor password 命令。要禁用该功能，请使用此命令的no形式

```
neighbor { ip_address | ipv6-address } password [ 0-7 ] string
no neighbor { ip_address | ipv6-address } password
```

Syntax Description	ip_address 邻居路由器的 IP 地址。
	ipv6-address 邻居路由器的 IPv6 地址。
	字符串 区分大小写的密码，长度最多为 25 个字符。 第一个字符不能为数字。此字符串包含任意字母数字字符，包括空格。不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。
	0-7 (可选) 加密类型。0-6 表示未加密。7 用于加密。

Command Default 未对两个 BGP 对等体之间的 TCP 连接进行 MD5 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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 您可以在两个 BGP 对等体之间配置 MD5 身份验证，这意味着在对等体之间的 TCP 连接上发送的每个数据段都需要验证。必须在两个 BGP 对等体上使用相同的密码配置 MD5 身份验证；否则，将无法在它们之间建立连接。配置 MD5 身份验证会使 ASA 软件生成和检查 TCP 连接上发送的每个分段的 MD5 摘要。

配置时，无论是否启用 service password-encryption 命令，都可以提供区分大小写的密码（最多 25 个字符）。如果密码的长度超过 25 个字符，将显示错误消息，并且不接受密码。此字符串包含任意字母数字字符，包括空格。密码不能配置为 number-space-anything 格式。数字后的空格会导致身份验证失败。您还可以使用以下符号字符与字母数字字符的任意组合：

`~!@#\$\$%^&*()-_+=+|\}][[\"':;/><.,?



注意 如果身份验证字符串配置不正确，则不会建立 BGP 对等会话。我们建议您在配置身份验证后仔细输入身份验证字符串，并验证对等会话是否建立。

如果一个路由器为邻居配置了密码，但邻居路由器没有配置密码，那么当路由器尝试在它们之间建立 BGP 会话时，控制台上会显示如下消息：

%TCP-6-BADAUTH: 从 [对等体的 IP 地址]: 11003 到 [本地路由器的 IP 地址]: 179 没有 MD5 摘要

同样，如果两个路由器配置了不同的密码，屏幕上会显示如下消息：

%TCP-6-BADAUTH: 从 [对等体的 IP 地址]: 11004 到 [本地路由器的 IP 地址]: 179 的 MD5 摘要无效

在已建立的 BGP 会话中配置 MD5 密码

如果配置或更改用于两个 BGP 对等体之间 MD5 身份验证的密码或密钥，则在您配置密码后，本地路由器不会终止现有会话。本地路由器将尝试使用新密码保持对等会话，直到 BGP 抑制计时器到期。默认时间段为 180 秒。如果在抑制计时器到期之前未在远程路由器上输入或更改密码，则会话将超时。



注释 为抑制计时器配置新的计时器值只有在会话重置后才会生效。因此，无法更改抑制计时器的配置，以避免重置 BGP 会话。

CR_Examples

以下示例为 10.108.1.1 邻居的对等会话配置 MD5 身份验证。在抑制计时器到期之前，必须在远程对等体上配置相同的密码：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

以下示例在禁用 service password-encryption 命令时为超过 25 个字符的密码配置。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
ciscoasa(config-router-af)# neighbor 209.165.200.225 password 1234567891234567891234567890
```

```
% BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
no service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

在以下示例中，如果在启用 service password-encryption 命令的情况下配置超过 25 个字符的密码，则会出现错误消息。

```
Router(config)# service password-encryption
```

```
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 1234567891234567891234567890

% BGP: Password length must be less than or equal to 25.
Router(config-router)# do show run | i password service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

Related Commands

命令	说明
address-familyipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
bgp router-id	为本地边界网关协议(BGP)路由进程配置固定的路由器 ID。
neighbor remote-as	向 BGP 或多协议 BGP 邻居表中添加一个条目。

neighbor prefix-list

要阻止分发前缀列表中指定的边界网关协议 (BGP) 邻居信息，请在地址系列配置模式下使用 **neighbor prefix-list** 命令。要删除过滤器列表，请使用此命令的 **no** 形式。

```
neighbor { ip_address | ipv6-address } prefix-list prefix-list-name { in | out }  
no neighbor { ip_address | ipv6-address } prefix-list prefix-list-name { in | out }
```

Syntax Description

<i>ip_address</i>	邻居路由器的 IP 地址。
IPv6 地址	邻居路由器的 IPv6 地址。
<i>prefix-list-name</i>	前缀列表的名称。
范围	过滤列表适用于来自该邻居的传入广告。
<i>out</i>	过滤列表适用于向该邻居发出的通告。

Command Default

所有外部地址和通告的地址前缀都会分发给 BGP 邻居。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

9.3(2) 添加了 **ipv6-address** 参数，并添加了对 IPv6 地址系列的支持。

使用指南

使用前缀列表是过滤 BGP 通告的三种方法的一种。您还可以使用 AS 路径过滤器来过滤 BGP 通告。AS 路径过滤器通过 **ip as-path access-list** 全局配置命令进行定义，并在 **neighbor filter-list** 命令中使用。过滤 BGP 通告的第三种方法是将访问列表或前缀列表与 **neighbor deploy-list** 命令配合使用。



注释

请勿在任何给定方向（入站或出站）上同时将邻居分发列表和邻居前缀列表命令应用于邻居。这两个命令是互斥的，并且每个入站或出站方向只能应用一个命令（邻居分发列表或邻居前缀列表）。

CR_Examples

以下地址系列配置模式示例将名为 abc 的前缀列表应用于从邻居 10.23.4.1 传入的通告：

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

以下地址系列路由器配置模式示例将名为 CustomerA 的前缀列表应用于传出到邻居 10.23.4.3 的传出通告：

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
The following address family router configuration mode example applies the prefix list named
CustomerA to outgoing advertisements to neighbor 2001::1:
ciscoasa(config-router-af)#neighbor 2001::1 prefix-list CustomerA out
```

Related Commands

命令	说明
address-familyipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
网络	指定 BGP 路由进程要通告的网络。

neighbor remote-as

要将条目添加到 BGP 或多协议 BGP 邻居表，请在 address-family 配置模式下使用 neighbor remote-as 命令。要从表中删除条目，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } remote-as autonomous-system-number  
no neighbor { ip_address | ipv6-address } remote-as autonomous-system-number
```

Syntax Description

ip_address	邻居路由器的 IP 地址。
ipv6-address	邻居路由器的 IPv6 地址。
自治系统编号	邻居所属的自治系统的编号，范围为 1 到 65535。 有关自治系统编号格式的详细信息，请参阅 router bgp 命令。 与关键字 Alternative-as 一起使用时，最多可输入五个自治系统编号。

Command Default

没有 BGP 或多协议 BGP 邻居对等体。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南

如果为邻居指定的邻居的自治系统编号与在路由器 bgp 全局配置命令中指定的自治系统编号相匹配，则该邻居标识为本地自治系统的内部邻居。否则，邻居将被视为外部邻居。

默认情况下，在路由器配置模式下使用 neighbor remote-as 命令定义的邻居仅交换单播地址前缀。

使用 alternate-as 关键字用于指定最多五个备用自治系统，可以在这些系统中标识动态 BGP 邻居。BGP 动态邻居支持允许 BGP 与由一系列 IP 地址定义的一组远程邻居。使用一系列 IP 地址和 BGP 对等体组配置 BGP 动态邻居。在使用 bgp listen 命令配置子网范围并将其与 BGP 对等组关联后，如果为该子网范围内的 IP 地址启动 TCP 会话，则会动态创建新的 BGP 邻居作为该组的成员。新 BGP 邻居将继承该组的所有配置或模板。

思科 4 字节自治系统编号的实施使用 asplain（例如 65538）作为自治系统编号的默认正则表达式匹配和输出显示格式，但您可以使用 asplain 格式和 asdot 格式配置 4 字节自治系统编号。RFC 5396 中所述。要更改默认的正则表达式匹配并将 4 字节自治系统编号的输出显示为 asdot 格式，请使用 bgp asnotation dot 命令，后跟 clear bgp * 命令以硬重置所有当前 BGP 会话。

CR_Examples

以下示例指定位于地址 10.108.1.2 的路由器是编号为 65200 的自治系统中的内部 BGP (iBGP) 邻居：

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

以下示例将一台 BGP 路由器分配给自治系统 65400，并且两个网络被列为源自自治系统。然后列出三个远程路由器（及其自治系统）的地址。正在配置的路由器将与邻居路由器共享有关网络 10.108.0.0 和 192.168.7.0 的信息。第一个路由器是与输入此配置的路由器（eBGP 邻居）位于不同自治系统中的远程路由器；第二个 neighbor remote-as 命令显示地址为 10.108.234.2 的内部 BGP 邻居（具有相同的自治系统编号）；last neighbor remote-as 命令指定的邻居与输入此配置的路由器位于不同的网络上（也是 eBGP 邻居）。

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

以下示例将自治系统 65001 中的邻居 10.108.1.1 配置为仅交换单播路由：

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31.1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
网络	指定 BGP 路由进程要通告的网络。
邻居删除专用 AS	从 eBGP 出站路由更新中删除私有自治系统编号。

neighbor remove-private-as

要从 eBGP 出站路由更新中删除专用自治系统编号，请在 address-family 配置模式下使用 neighbor remove-private-as 命令。要禁用该功能，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } remove-private-as [ all [ replace-as ] ]
no neighbor { ip_address | ipv6-address } remove-private-as [ all [ replace-as ] ]
```

Syntax Description	ip_address 邻居路由器的 IP 地址。
	ipv6-address 邻居路由器的 IPv6 地址。
	all （可选）从传出更新的 AS 路径中删除所有专用 AS 编号。
	replace-as （可选）只要指定了 all 关键字，replace-as 关键字就会导致 AS 路径中的所有专用 AS 编号替换为路由器的本地 AS 编号。

Command Default 不会从 AS 路径中删除专用 AS 编号。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此命令仅适用于外部 BGP (eBGP) 邻居。专用 AS 值范围为从 64512 到 65535。当更新传递到外部邻居时，如果 AS 路径包含专用 AS 编号，软件将丢弃专用 AS 编号

- neighbor remove-private-as 命令从 AS 路径中删除专用 AS 编号，即使路径同时包含公共和专用 ASN
- 即使 AS 路径仅包含专用 AS 编号，neighbor remove-private-as 命令也会删除专用 AS 编号。不可能出现 0 长度的 AS 路径，因为此命令只能应用于 eBGP 对等体，在这种情况下，本地路由器的 AS 编号会附加到 AS 路径。neighbor remove-private-as 命令会删除专用 AS 号，即使专用 ASN 在 AS 路径中出现在联盟网段之前也是如此。

- 从 AS 路径中删除专用 AS 编号后，发送的前缀的路径长度将减少。由于 AS 路径长度是 BGP 最佳路径选择的关键元素，因此可能有必要保留路径长度。通过将所有删除的 AS 编号替换为本地路由器的 AS 编号，**replace-as** 关键字可确保保留路径长度。
- 该功能可应用于每个地址系列的邻居。因此，您可以将该功能应用于一个地址系列中的邻居，而不应用于另一个地址系列中的邻居，从而影响仅针对配置了该功能的地址系列的出站端上的更新消息。

CR_Examples

以下示例显示从发送到 172.16.2.33 的更新中删除专用 AS 编号的配置。结果是，10.108.1.1 通过 AS 100 通告的路径的 AS 路径将仅包含“100”（如自治系统 2051 所示）。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer

ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as

Router-in-AS100# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
    172.16.2.33
    65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
    172.16.2.32 from 172.16.2.32
      Origin IGP, metric 0, localpref 100, valid, external, best
```

Related Commands

命令	说明
address-familyipv4	进入地址族配置模式。
邻居描述	将说明与邻居相关联
neighbor remote-as	将 BGP 或多协议 BGP 路由条目添加到路由表。

neighbor route-map

要将路由映射应用于传入或传出路由，请在地址系列配置模式下使用 `neighbor route-map` 命令。要删除路由图，请使用此命令的 `no` 形式。

neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }

Syntax Description

<i>ip_address</i>	邻居路由器的 IP 地址。
<i>ipv6-address</i>	邻居路由器的 IPv6 地址。
<i>map-name</i>	路由映射的名称。
范围	将路线图应用于传入路线。
out	将路由图应用于传出的路由。

Command Default

没有路由映射应用于对等体。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

9.3(2) 添加了 `ipv6-address` 参数，并添加了对 IPv6 地址系列的支持。

使用指南

在地址系列配置模式下指定时，此命令仅将路由映射应用于该特定地址系列。在路由器配置模式下指定此命令时，此命令将仅将路由映射应用于 IPv4 单播路由。

如果指定了出站路由映射，则适当的行为是仅通告至少与路由映射的一个部分匹配的路由。

CR_Examples

以下示例将名为 `internal-map` 的路由映射应用于来自 172.16.70.24 的 BGP 传入路由：

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
```

```
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

以下示例将名为 `internal-map` 的路由映射应用于来自 `2001::1` 的 BGP 传入路由：

```
ciscoasa(config-router-af)# neighbor 2001::1 route-map internal-map in
```

Related Commands

命令	说明
address-familyipv4	进入地址族配置模式。
match as-path	匹配访问列表指定的 BGP 自治系统路径
route-map	定义将路由从一个路由协议重新分发到另一个路由协议的条件。
match as-path	匹配访问列表指定的 BGP 自治系统路径。
set local-preference	指定自治系统路径的首选值。

neighbor send-community

要指定应将社区属性发送到 BGP 邻居，请在 address-family 配置模式下使用 neighbor send-community 命令。要删除该条目，请使用此命令的 no 形式。

neighbor { ip_address | ipv6-address } send-community
no neighbor { ip_address | ipv6-address } send-community

Syntax Description

ip_address 邻居路由器的 IP 地址。

ipv6-address 邻居路由器的 IPv6 地址。

Command Default

没有向任何邻居发送社区属性。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

CR_Examples

在以下地址系列配置模式示例中，路由器属于自治系统 109，并被配置为将社区属性发送到 IP 地址为 172.16.70.23 的其邻居：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

在以下示例中，路由器被配置为将社区属性发送到 IP 地址为 2001::1 的邻居：

```
ciscoasa(config-router-af)# neighbor 2001::1 send-community
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。

neighbor shutdown

要禁用邻居，请在地址系列配置模式下使用 `neighbor shutdown` 命令。要重新启用该邻居，请使用此命令的 `no` 形式。

neighborip_addressshutdown
no neighborip_addressshutdown

Syntax Description *ip_address* 邻居路由器的 IP 地址。

Command Default 不会更改任何 BGP 邻居的状态。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

`neighbor shutdown` 命令用于终止指定邻居的任何活动会话，并删除所有关联的路由信息。

要显示 BGP 邻居摘要，请使用 `show bgp summary` 命令。具有空闲状态和管理条目的邻居已被 `neighbor shutdown` 命令禁用。

“State/PfxRcd” 显示 BGP 会话的当前状态或路由器从邻居接收的前缀数量。当达到最大数量（由邻居最大前缀命令设置）时，条目中会出现字符串 “PfxRcd”，邻居被关闭，连接处于空闲状态。

CR_Examples

以下示例为邻居 172.16.70.23 禁用所有活动会话：

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

命令	说明
address-familyipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

命令	说明
show bgp summary	显示 BGP 邻居状态的摘要。

neighbor timers

要为特定 BGP 对等体设置计时器，请在地址系列配置模式下使用 `neighbor timers` 命令。要清除特定 BGP 对等体的计时器，请使用此命令的 `no` 形式。

neighbor { *ip_address* | *ipv6-address* } **timers** *keepalive holdtime* [*min-holdtime*]

noneighbor { *ip_address* | *ipv6-address* } **timers**

Syntax Description	<i>ip_address</i>	邻居路由器的 IP 地址。
	<i>ipv6-address</i>	邻居路由器的 IPv6 地址。
	<i>keepalive</i>	ASA 软件向其对等方发送保持连接消息的频率（以秒为单位）。默认值为 60 秒。范围是 0 至 65535。
	<i>holdtime</i>	未收到保持连接消息后软件宣布对等体死亡的时间间隔（以秒为单位）。默认值为 180 秒。范围是从 0 到 65535。
	<i>min-holdtime</i>	（可选）指定来自 BGP 邻居的最短可接受保持时间的时间间隔（以秒为单位）。可接受的最小保持时间必须小于或等于保持时间参数中指定的间隔。范围是从 0 到 65535。

Command Default	保活时间：60秒
	保持时间：180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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 <code>ipv6-address</code> 参数，并添加了对 IPv6 地址系列的支持。

使用指南	• 为特定邻居配置的计时器将覆盖为所有 BGP 邻居使用 <code>timers bgp</code> 命令配置的计时器。

- 当将保持时间参数配置为小于 20 秒的值时，将显示以下警告：保持时间小于 20 秒会增加对等端抖动的可能性。
- 如果可接受的最小保持时间间隔大于指定的保持时间，则会显示一条通知：可接受的最小保持时间应小于或等于配置的保持时间。



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

CR_Examples

以下示例将 BGP 对等体 192.168.47.0 的保持连接计时器更改为 70 秒，将保持时间计时器更改为 210 秒：

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

以下示例将 BGP 对等体 192.168.1.2 的保持连接计时器更改为 70 秒，保持时间计时器更改为 130 秒，最小保持时间间隔更改为 100 秒：

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

以下示例将 BGP 对等体 2001::1 的保持连接计时器更改为 70 秒，将保持时间计时器更改为 210 秒：

```
ciscoasa(config-router-af)# neighbor 2001::1 timers 70 210
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor transport

要为边界网关协议 (BGP) 会话启用 TCP 传输会话选项，请在路由器或地址系列配置模式下使用 neighbor transport 命令。要禁用 BGP 会话的 TCP 传输会话选项，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } transport { connection-mode { active | passive }
| path-mtu-discovery [ disable ] }
no neighbor { ip_address | ipv6-address } transport { connection-mode { active | passive }
| path-mtu-discovery [ disable ] }
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	连接模式	指定连接类型 - 主动或被动。
	active	指定活动连接。
	被动	指定被动连接。
	path-mtu-discovery	启用 TCP 传输路径最大传输单元 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。
	disable	禁用 TCP 路径 MTU 发现。

Command Default 如果未配置此命令，则默认情况下会启用 TCP 路径 MTU 发现，但不会启用其他 TCP 传输会话选项。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 此命令用于指定各种传输选项。可以为 BGP 会话指定主动或被动传输连接。可以启用 TCP 传输路径 MTU 发现，以允许 BGP 会话利用更大的 MTU 链路。使用 show bgp neighbors 命令可确定是否启

用了 TCP 路径 MTU 发现。如果您使用 **disable** 关键字禁用发现，则在继承禁用了发现的模板的任何对等体上也会禁用发现。

CR_Examples

以下示例显示如何将 TCP 传输连接配置为单个内部 BGP (iBGP) 邻居的活动连接：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

以下示例显示如何将单个外部 BGP (eBGP) 邻居的 TCP 传输连接配置为被动：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

以下示例显示如何对单个 BGP 邻居禁用 TCP 路径 MTU 发现：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

以下示例显示如何将单个 BGPv6 邻居的 TCP 传输连接配置为活动连接：

```
ciscoasa(config-router-af)#neighbor 2001::1 transport connection-mode active
```

以下示例显示如何为单个 BGPv6 邻居启用 TCP 路径 MTU 发现：

```
ciscoasa(config-router-af)#neighbor 2001::1 transport path-mtu-discovery
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	向 BGP 或多协议 BGP 路由表添加条目。
show bgp neighbor	显示有关 BGP 邻居的信息

neighbor ttl-security

要保护边界网关协议 (BGP) 对等会话并配置用于分隔两个外部 BGP (eBGP) 对等体的最大跳数，请在 address-family 配置模式下使用 neighbor ttl-security 命令。要禁用此功能，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } ttl-security hops hop-count
no neighbor { ip_address | ipv6-address } ttl-security hops hop-count
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	hop-count	分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 参数计算得出。 有效值为 1 至 254 之间的数字。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 neighbour ttl-security 命令提供了一种轻量级的安全机制来保护 BGP 对等会话免受基于 CPU 利用率的攻击。这些类型的攻击通常是暴力拒绝服务 (DoS) 攻击，即通过使数据包报头中包含伪造的源和目标 IP 地址的 IP 数据包充斥网络来尝试禁用网络。

此功能通过仅接受 TTL 计数等于或大于本地配置值的 IP 数据包来利用 IP 数据包的设计行为。准确伪造 IP 数据包中的 TTL 计数通常被视为不可能。如果没有源或目标网络的内部访问权限，则准确伪造数据包以匹配来自信任对等体的 TTL 计数是不可能的。

应在每个参与的路由器上配置此功能。它仅在传入方向保护 BGP 会话，对传出 IP 数据包或远程路由器没有影响。启用此功能后，仅当 IP 数据包报头中的 TTL 值等于或大于为对等会话配置的 TTL 值时，BGP 才会建立或维护会话。此功能对 BGP 对等会话没有影响，如果未收到保持连接数据包，

对等会话仍可能过期。如果接收的数据包中的 TTL 值小于本地配置的值，则系统会以静默方式丢弃该数据包，并且不会生成互联网控制消息协议 (ICMP) 消息。这是有意设计的行为；对伪造的数据包没有必要作出响应。

要最大限度地提高此功能的有效性，“hop-count”值应严格配置为匹配本地与外部网络之间的跃点数。但是，为多跃点对等会话配置此功能时，您还应该考虑路径变化。

以下限制适用于此命令的配置：

- 内部 BGP (iBGP) 对等体不支持此功能。
- 无法为已配置邻居 `ebgp-multihop` 命令的对等体配置邻居 `ttl-security` 命令。这些命令的配置互相排斥，只需要使用其中一个命令即可启用多跳 eBGP 对等会话。如果尝试为同一对等会话配置这两个命令，控制台中将会显示错误消息。
- 在大直径多跳对等互连中，此功能的有效性会降低。针对配置为大直径对等关系的 BGP 路由器发起基于 CPU 利用率的攻击，您可能仍需要关闭受影响的对等会话来处理攻击。
- 此功能不能有效抵御来自自己在网络内部受到危害的对等体的攻击。此限制还包括位于源网络和目标网络之间的网段上的对等体。

CR_Examples

以下示例将直接连接的邻居的跳数计数设置为 2。由于 `hop-count` 参数设置为 2，因此 BGP 仅接受报头中 TTL 计数等于或大于 253 的 IP 数据包。如果收到的数据包在 IP 数据包报头中包含任何其他 TTL 值，数据包将被静默丢弃。

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

以下示例将一个直接连接的 BGPv6 邻居的跳数设置为 2。

```
ciscoasa(config-router-af)#neighbor 2001::1 ttl-security hops 2
```

Related Commands

命令	说明
address-familyipv4	进入地址族配置模式。
<code>neighbor activate</code>	启用与 BGP 邻居的信息交换。
<code>neighbor ebgp-multihop</code>	接受并尝试与非直接连接网络上的外部对等体建立 BGP 连接

neighbor update-source

要将接口配置为 BGP 发言邻居的源，请在地址系列配置模式下使用 **neighbor update-source** 命令。
要禁用此功能，请使用此命令的 no 形式。

neighbor { *ipv_address* | *ipv6-address* } **update-source** { *interface name* }

Syntax Description	<i>ip_address</i>	邻居路由器的 IP 地址。
	<i>ipv6-address</i>	邻居路由器的 IPv6 地址。
	<i>interface name</i>	指定 <code>nameif</code> 命令所指定的 ASA 用作 BGP 路由源的接口的名称。

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
地址族配置模式。	• 是	—	• 是	• 支持	—

Command History	版本	修改
	9.18(2)	添加了此命令。

使用指南 此命令适用于在环回接口上运行 BGP 协议，并允许环回接口参与重新分发和前缀通告。

CR_Examples 以下示例将环回接口 loop1 更新为 BGP 邻居 10.108.1.1 的源：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 109
ciscoasa(config-router-af)# neighbor 10.108.1.1 update-source loop1
```

以下示例将环回接口 loop1 更新为 BGP 邻居 2001::1 的源：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 2001::1 remote-as 109
ciscoasa(config-router-af)# neighbor 2001::1 update-source loop1
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	将 BGP 或多协议 BGP 路由条目添加到路由表。

neighbor version

要将 ASA 软件配置为仅接受特定 BGP 版本，请在地址系列配置模式下使用 neighbor version 命令。要使用邻居的默认版本级别，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } versionnumber
no neighbor { ip_address | ipv6-address } versionnumber
```

Syntax Description	ip_address 邻居路由器的 IP 地址。
	ipv6-address 邻居路由器的 IPv6 地址。
	数字 BGP 版本号。版本可以设置为 2，以强制软件仅对指定邻居使用版本 2。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

Command Default BGP 版本 4。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 输入此命令会禁用动态版本协商。

CR_Examples 以下示例锁定到 BGP 协议版本 4：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
ciscoasa(config-router-af)# neighbor 2001::1 version 4
```

Related Commands	命令	说明
	address-familyipv4	进入地址族配置模式。

命令	说明
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor weight

要为邻居连接分配权重，请在地址系列配置模式下使用 neighbor weight 命令。要删除权重分配，请使用此命令的 no 形式。

```
neighbor { ip_address | ipv6-address } weightnumber
no neighbor { ip_address | ipv6-address } weightnumber
```

Syntax Description	ip_address	邻居路由器的 IP 地址。
	ipv6-address	邻居路由器的 IPv6 地址。
	数字	要分配的权重。
		有效值介于 0 与 65535 之间。

Command Default 通过另一个 BGP 对等体获知的路由的默认权重为 0，而来自本地路由器的路由的默认权重为 32768。

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
地址族配置模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.2(1) 添加了此命令。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 从此邻居获知的所有路由最初都将具有已分配的权重。当特定网络有多个路由可用时，具有最高权重的路由将被选择作为首选路由。

使用 set weight route-map 命令分配的权重会覆盖使用 neighbor weight 命令分配的权重。

CR_Examples 以下地址系列配置模式示例将通过 172.16.12.1 获知的所有路由的权重设为 50：

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

以下地址系列配置模式示例设置通过 2001::1 获知的所有路由的权重：

```
ciscoasa(config-router-af)# neighbor 2001::1 weight 50
```

Related Commands

命令	说明
address-family ipv4	进入地址族配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

nem

要为硬件客户端启用网络扩展模式，请在 **nemenable** 策略组配置模式下使用该命令。要禁用NEM，请使用该 **nemdisable** 命令。要从运行配置中删除 NEM 属性，请使用此**no**命令的形式。此选项允许从其他组策略继承值。

```
nem { enable|disable }
no nem
```

Syntax Description	disable 禁用网络扩展模式。
	enable 启用网络扩展模式。

Command Default 网络扩展模式已禁用。

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
组策略配置	• 是	—	• 是	—	—

使用指南 网络扩展模式允许硬件客户端通过 VPN 隧道向远程专用网络呈现单个可路由的网络。IPsec 封装从硬件客户端后面的专用网络到 ASA 后面的网络的所有流量。PAT 不适用。因此，ASA 后面的设备可以通过隧道直接访问硬件客户端后面的专用网络上的设备，并且只能通过隧道访问，反之亦然。硬件客户端必须启动隧道，但是在建立隧道之后，任一端都可发起数据交换。

Command History	版本 修改
	7.0(1) 添加了此命令。

CR_Examples 以下示例显示如何为名为 FirstGroup 的组策略设置 NEM：

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


netmod

要禁用网络模块，请在全局配置模式下使用 **netmod** 命令。要启用网络模块，请使用此命令的 **no** 形式。



注释 仅在 Secure Firewall 3100 上支持此命令。

netmod 2 disable
no netmod 2 disable

Syntax Description	2	指定插槽 2 中的模块。
	disable	禁用网络模块。

Command Default 如果该模块在首次启动时安装，则会将其启用。

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	• 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 如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。如果您需要在初始启动后更改网络模块安装，请使用此命令。

添加新模块或永久删除模块需要重新加载。您可以将网络模块热插拔为相同类型的新模块，而无需重新加载。但是，您必须关闭当前模块才能安全地将其删除。如果您更换了其他类型的网络模块，则需要重新加载。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

示例

以下示例禁用网络模块。

```
ciscoasa(config)# netmod 2 disable
```

以下示例启用 网络模块。

```
ciscoasa(config)# no netmod 2 disable
```

network (address-family)

要指定将由边界网关协议 (BGP) 路由进程通告的网络，请在 address-family 配置模式下使用 network 命令。要从路由表中删除条目，请使用此命令的 no 形式。

network { ipv4_address [masknetwork_mask] | IPv6_prefix | prefix_length | prefix_delegation_name [subnet_prefix | prefix_length] } [route-map route_map_name]
no network { ipv4_address [masknetwork_mask] | IPv6_prefix | prefix_length | prefix_delegation_name [subnet_prefix | prefix_length] } [route-maproute_map_name]

Syntax Description

ipv4_address	BGP 或多协议 BGP 将通告的 IPv4 网络。
ipv6_prefix/prefix_length	BGP 或多协议 BGP 将通告的 IPv6 网络。
mask network_mask	(可选) 带有掩码地址的网络或子网掩码。
prefix_delegation_name	如果您启用 DHCPv6 前缀委派客户端 (ip6dhcpclientpd)，那么您可以通告前缀。
subnet_prefix/prefix_length	(可选) 要为前缀划分子网，请指定 subnet_prefix/prefix 长度。
route-map route_map_name	(可选) 已配置路由图的标识符。应检查路由映射，以过滤要通告的网络。如果未指定，则通告所有网络。如果指定了关键字，但没有列出路由图标签，则不会通告任何网络。

Command Default

未指定任何网络。

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
Address-family 配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

9.6(2) 添加了 prefix_delegation_name [subnet_prefix/prefix_length] 参数。

使用指南

可以从连接的路由、动态路由和静态路由源获知 BGP 和多协议 BGP 网络。

可以使用的网络命令的最大数量取决于路由器的资源（例如，配置的 NVRAM 或 RAM）。

CR_Examples

以下示例将网络 10.108.0.0 设置为包含在 BGP 更新中：

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

Related Commands

命令	说明
showbgpinterfaces	显示 BGP 路由表中的条目。

network (router eigrp)

要为 EIGRP 路由进程指定网络列表，请在路由器配置模式下使用 **network** 命令。要删除网络定义，请使用此命令的 **no** 形式。

network *ip_addr* [*mask*]
no network *ip_addr* [*mask*]

Syntax Description

ip_addr 直接连接网络的 IP 地址。连接到指定网络的接口将参与 EIGRP 路由进程。

mask （可选）IP 地址的网络掩码。

Command Default

未指定任何网络。

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	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

使用指南

network 命令在指定网络中具有至少一个 IP 地址的所有接口上启动 EIGRP。它将插入 EIGRP 拓扑表中指定网络的连接子网。

然后，ASA 通过匹配的接口建立邻居。对可在 ASA 上配置的 **network** 命令数量没有限制。

CR_Examples

以下示例将 EIGRP 定义为用于连接到网络 10.0.0.0 和 192.168.7.0 的所有接口上的路由协议：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

Related Commands

命令	说明
showeigrpinterfaces	显示为 EIGRP 配置的接口信息。
showeigrptopology	显示 EIGRP 拓扑表。

network (router rip)

要为 RIP 路由进程指定网络列表，请在路由器配置模式下使用该 **network** 命令。要删除网络定义，请使用此命令的 **no** 形式。

```
network { ip_addr | ipv6-address } | <prefix-length>
no network { ip_addr | ipv6-address } | <prefix-length> [ route-map route-map-name ]
```

Syntax Description	ip_addr	直接连接网络的 IP 地址。连接到指定网络的接口将参与 RIP 路由过程。
	ipv6-address	要使用的 IPv6 地址。IPv6 地址必须以 X:X:X:X:X 格式输入。
	prefix-length	IPv6 前缀的长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值前面必须有斜线标记。 有效值介于 0 到 128 之间。
	route-map-name	将修改其属性的路由映射。

Command Default 未指定任何网络。

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， 地址系列配置 模式	• 是	—	• 是	• 支持	—

Command History	版本 修改
	7.2(1) 添加了此命令。
	9.0(1) 增加了多情景模式支持。
	9.3(2) 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。

使用指南 指定的网络号不得包含任何子网信息。可在路由器上使用的网络命令的数量没有限制。RIP 路由更新将仅通过指定网络上的接口发送和接收。此外，如果未指定接口的网络，则该接口将不会在任何 RIP 更新中被通告。

CR_Examples 以下示例将 RIP 定义为用于连接到网络 10.0.0.0 和 192.168.7.0 的所有接口的路由协议：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
In the following example the attributes of the test-route-map route map connected to the
2001::1 network will be modified.
ciscoasa(config-router)# network 2001:0:0:0::1 route-map test-route-map
```

Related Commands

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

network-acl

如要指定之前使用 **access-list** 命令配置的防火墙 ACL 名称，请在 **dynamic-access-policy-record** 配置模式下使用 **network-acl**命令。要删除现有网络 ACL，请使用此命令的 **no** 形式。要删除所有网络 ACL，请使用不带参数的 命令。

network-acl*name*
no network-acl [名称]

Syntax Description *name* 指定网络 ACL 的名称。名称的最大长度为 240 个字符。

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
动态访问策略记录配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南 多次使用此命令，以便将多个防火墙 ACL 分配给 DAP 记录。

ASA会验证您指定的每个ACL，以确保它们仅包含允许规则或仅包含访问列表条目的拒绝规则。如果任何指定的 ACL 包含混合的允许和拒绝规则，ASA 将拒绝该命令。

以下示例显示如何将名为财务限制 (Finance Restrictions) 的网络 ACL 应用于名为财务 (Finance) 的 DAP 记录。

```
ciscoasa
(config)#
dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
network-acl Finance Restrictions
ciscoasa
(config-dynamic-access-policy-record)#
```


Related Commands

命令	说明
access-policy	配置防火墙访问策略。
dynamic-access-policy-record	创建 DAP 记录。
showrunning-configdynamic-access-policy-record [名称]	显示所有 DAP 记录或指定 DAP 记录正在使用的配置。

network area

要定义运行 OSPF 的接口并定义这些接口的区域 ID，请在 **networkarea** 路由器配置模式下使用该命令。要禁用使用地址/网络掩码对定义的接口的 OSPF 路由，请使用此命令的 **no**形式。

```
networkaddr maskareaarea_id
no networkaddr maskareaarea_id
```

Syntax Description	addr	IP 地址。
	areaarea_id	指定与 OSPF 地址范围关联的区域。可以 IP 地址格式或十进制格式指定 area_id。以十进制格式指定时，有效值范围为 0 至 4294967295。
	mask	网络掩码。

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	• —	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南 要在接口上运行 OSPF，接口的地址必须被 **networkarea** 命令覆盖。如果 **networkarea** 命令未涵盖接口的 IP 地址，则不会通过该接口启用 OSPF。

您可在 ASA 上使用的 **networkarea** 命令没有数量限制。

CR_Examples 以下示例在 192.168.1.1 接口上启用 OSPF，并将其分配到 area 2：

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

Related Commands	命令	说明
	routerospf	进入路由器配置模式。

命令	说明
showrunning-configrouter	显示全局路由器配置中的命令。

network-object

要将主机对象、网络对象或子网对象添加到网络对象组，请在 `object-group` 网络配置模式下使用 `network-object` 命令。要删除网络对象，请使用此命令的 `no` 形式。

```
network-object { hostaddress | IPv4_address mask | IPv6_address | IPv6_prefix | objectname }
no network-object { hostip_address | ip_address mask | objectname }
```

Syntax Description	hostip_address	指定主机 IPv4 或 IPv6 地址。
	IPv4_addressmask	指定 IPv4 网络地址和子网掩码。
	IPv6 地址/IPv6 前缀	指定 IPv6 网络地址和前缀长度。
	objectname	指定网络对象（通过 <code>objectnetwork</code> 命令创建）。

Command Default 无默认为或值。

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
Object-group 网络配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	8.3(1) 添加 <code>object</code> 参数是为了支持网络对象（ <code>objectnetwork</code> 命令）。
	9.0(1) 以前，网络对象组只能包含所有 IPv4 地址或所有 IPv6 地址。现在网络对象组可以支持 IPv4 和 IPv6 地址的混合，尽管您不能在 NAT 中使用混合组。

使用指南 `network-object` 命令与 `object-group` 命令一起使用来定义主机对象、网络对象或子网对象。

CR_Examples 以下示例显示如何使用 `network-object` 命令在网络对象组中创建新主机对象：

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfigureobject-group	从配置中 object-group 删除所有命令。
group-object	添加网络对象组。
object network	添加网络对象。
object-groupnetwork	定义网络对象组。
showrunning-configobject-group	显示当前对象组。

network-service-member

要将网络服务对象添加到网络服务组，请在对象组配置模式下使用 **network-service-member** 命令。
使用命令形 **no** 式从组中删除对象

```
network-service-member object_name
no network-service-member object_name
```

Syntax Description *object_name* 网络服务对象的名称。如果名称中有空格，请用双引号括起来。

Command Default 没有默认值。

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
网络服务对象组配置模式	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	9.17(1)	添加了此命令。

示例
以下示例将三个现有网络服务对象添加到网络服务对象组。

```
object-group network-service SaaS_Applications
  description This group includes relevant 'Software as a Service' applications
  network-service-member "outlook 365"
  network-service-member webex
  network-service-member box
```

Related Commands	命令	说明
	clear object-group	清除对象组的命中计数。
	object-group network-service	定义网络服务对象组。
	show object-group network-service	显示网络服务对象及其命中次数。

nis address

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供网络信息服务 (NIS) 地址，请在 ipv6 dhcp 池配置模式下使用 **nisaddress** 命令。要删除 NIS 服务器，请使用此命令 **no** 的形式。

```

nis addressnis_ipv6_address
no nis addressnis_ipv6_address
    
```

Syntax Description *nis_ipv6_address* 指定 NIS IPv6 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
Ipv6 dhcp 池配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA **ipv6dhcppool**，使其在向 ASA 发送信息请求 (IR) 数据包时以提供信息（包括 NIS 地址）。ASA 仅接受 IR 数据包，不向客户端分配地址。使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool** 名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```

ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
    
```

```

interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。

命令	说明
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

nis domain-name

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供网络信息服务 (NIS) 域名，请在 ipv6 dhcp 池配置模式下使用 **nisdomain-name**命令。要删除 NIS 域名，请使用此命 **no** 令的形式。

```
nis domain-namenis_domain_name
no nis domain-namenis_domain_name
```

Syntax Description	nis_domain_name 指定 NIS 域名。

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
Ipv6 dhcp 池配置	• 是	—	• 是	—	—

Command History	版本 修改
	9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以将 ASA 配置为在向 **ipv6dhcppool**ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 域名。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
```

```

nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。

命令	说明
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

nisp address

要在配置 DHCPv6 服务器时无状态地址自动配置 (SLAAC) 客户端提供 Network Information Service Plus (NIS+) 服务器 IP 地址，请在 `ipv6 dhcp` 池配置模式下使用 **nispaddress** 命令。要删除 NIS+ 服务器，请使用此命令的形式。

nisp address *nisp_ipv6_address*
no nisp address *nisp_ipv6_address*

Syntax Description

nisp_ipv6_address 指定 NIS+ 服务器 IPv6 地址。

Command Default

无默认为行为或值。

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
Ipv6 dhcp 池配置	• 是	—	• 是	—	—

Command History

版本 修改

9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA **ipv6dhcppool**，使其在向 ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 服务器。ASA 仅接受 IR 数据包，不向客户端分配地址。使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool** 名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```

```

interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。

命令	说明
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

nisp domain-name

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供网络信息服务 (NIS+) 域名，请在 ipv6 dhcp 池配置模式下使用 **nispdomain-name**命令。要删除 NIS+ 域名，请使用此命 **no**令的形式。

```
nisp domain-namenisp_domain_name
no nisp domain-namenisp_domain_name
```

Syntax Description	nisp_domain_name 指定 NIS+ 域名。

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
Ipv6 dhcp 池配置	• 是	—	• 是	—	—

Command History	版本 修改
	9.6(2) 我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以将 ASA 配置为在向 **ipv6dhcppool**ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 域名。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```



```

interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcpserver	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示 DHCPv6 前缀委派客户端获取的所有前缀以及该前缀到其他进程的 ASA 分发。

命令	说明
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

nop

要定义在具有 IP 选项检查的数据包头中出现无操作 IP 选项时的操作，请在 **nop** 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。

```
nop action { allow | clear }
no nop action { allow | clear }
```

Syntax Description	<i>allow</i> 允许包含无操作 IP 选项的数据包。
	<i>clear</i> 从数据包头中删除无操作选项，然后允许数据包。

Command Default 默认情况下，IP 选项检查会丢弃包含无操作 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，而无需更改或删除指定的 IP 选项，然后允许数据包通过。
IP 报头中的选项字段可以包含零个、一个或多个选项，这使得该字段的总长度可变。但是，IP 报头必须是 32 位的倍数。如果所有选项的位数不是 32 位的倍数，则使用无操作 (NOP) 或 IP 选项 1 作为“内部填充”，以使选项与 32 位边界对齐。

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)# 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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

nsf cisco

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科不间断转发 (NSF) 操作，请在路由器配置模式下使用 `nsf cisco` 命令。要恢复默认值，请使用此命令的 `no` 形式。

nsf cisco [enforce global]
no nsf cisco [enforce global]

Syntax Description

enforceglobal （可选）如果在重启过程中在任何接口上检测到不具有 NSF 感知能力的相邻网络设备，则取消所有接口上的 NSF 重启。

Command Default

默认情况下，思科 NSF 平稳重启处于禁用状态。

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
路由器配置模式	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.3(1) 添加了此命令。

使用指南

此命令可在 OSPF 路由器上启用思科 NSF。当在路由器上启用 NSF 时，该路由器也支持 NSF，并将在重启模式下运行。

如果路由器预计与仅执行 NSF 平稳重启的邻居协作，则邻居路由器必须运行支持 NSF 的思科软件版本，但无需在路由器上配置 NSF。当路由器运行支持 NSF 的思科软件版本时，路由器可感知 NSF。

默认情况下，可识别 NSF 的相邻路由器在平滑重启期间将运行在 NSF 助手模式下。

在 NSF 平稳重启期间，如果在网络接口上检测到无法识别 NSF 的邻居，则仅在该接口上中止重启，而在其他接口上继续平稳重启。要在重启期间检测到无法识别 NSF 的邻居时取消整个 OSPF 进程的重启，请将此命令配置为带有 `enforce global` 关键字。



注释 当在任何接口上检测到邻居邻接重置或 OSPF 接口关闭时，整个过程的 NSF 平稳重启也会被取消。

CR_Examples

以下示例使用 `enforce global` 选项启用思科 NSF 平稳重启：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# cisco nsf enforce global
```

Related Commands

命令	说明
nsf cisco helper	在 ASA 上启用思科 NSF 助手模式。
nsfietf	启用 IETF NSF

nsf cisco helper

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科无间断转发 (NSF) 助手模式，请在路由器配置模式下使用 `nsf cisco helper` 命令。默认情况下会启用思科 NSF 助手模式，可以通过在路由器配置模式下发出 `no nsf cisco helper` 来禁用此模式。

nsf ciscohelper
no nsf ciscohelper

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下启用 Cisco NSF 帮助程序模式。

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
路由器配置模式	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.3(1) 添加了此命令。

使用指南

当 ASA 启用了 NSF 时，ASA 称为支持 NSF 并将在平稳重启模式下运行 - OSPF 路由器进程由于路由处理器 (RP) 切换而执行不间断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 可感知 NSF，并将在 NSF 助手模式下运行。当具有 NSF 功能的 ASA 执行平滑重启时，辅助 ASA 会协助不间断转发恢复过程。如果您不希望 ASA 通过不间断转发恢复来帮助重新启动的邻居，请输入 `no nsf cisco helper` 命令。

CR_Examples

以下示例禁用 NSF 助手模式：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# no nsf cisco helper
```

Related Commands

命令	说明
<code>nsf cisco</code>	在 ASA 上启用思科 NSF。

命令	说明
nsfietf	启用 IETF NSF

nsf ietf

要在运行 OSPF 的 ASA 上配置互联网工程任务组 (IETF) NSF 操作，请在路由器配置模式下使用 nsf ietf 命令。要恢复默认值，请使用此命令的 no 形式。

nsf ietf [**restart-interval** 秒]
no nsf ietf

Syntax Description	<i>restart-interval</i><i>seconds</i> （可选）指定平滑重启间隔的长度（以秒为单位）。范围是从 1 到 1800。默认值为 120。 注释 对于低于 30 秒的重启间隔，将终止平稳重启。

Command Default	IETF NSF 平稳重启模式已禁用。

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
路由器配置模式	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.3(1) 添加了此命令。

使用指南	此命令可在 ASA 上启用 IETF NSF。在 ASA 上启用 NSF 时，ASA 将支持 NSF 功能并将在重新启动模式下运行。 如果 ASA 应与仅执行 NSF 平稳重启的邻居协作，则邻居 ASA 必须支持 NSF，但路由器上不需要配置 NSF。当 ASA 运行支持 NSF 的应用时，ASA 可感知 NSF。

CR_Examples	以下示例禁用 NSF 助手模式：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# nsf ietf restart-interval 240
```

Related Commands

命令	说明
nsf cisco	在 ASA 上启用思科 NSF。
nsfciscohelper	在 ASA 上启用思科 NSF 助手模式。
nsf ietf helper	在 ASA 上启用 IETF NSF 助手模式。

nsf ietf helper

默认情况下启用 IETF NSF 帮助模式。要明确启用 IETF NSF 助手模式，请在路由器配置模式下使用 `nsf ietf helper` 命令。可以使用该命令的 `no` 形式来禁用它。

或者，可以使用 `nsf ietf helper strict-lsa-checking` 命令启用严格链路状态通告 (LSA) 检查。

nsf ietf helper [strict-lsa-checking]
no nsf ietf helper

Syntax Description 严格 LSA 检查（可选）为助手模式启用严格链路状态通告 (LSA) 检查。

Command Default 默认情况下启用 IETF NSF 帮助模式。

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
路由器配置模式	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

9.3(1) 添加了此命令。

使用指南 当 ASA 启用了 NSF 时，这意味着 ASA 也支持 NSF 功能，并将在平稳重启模式下运行 - OSPF 进程会由于路由处理器 (RP) 切换而执行不间断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 可感知 NSF，并将在 NSF 助手模式下运行。当具有 NSF 功能的 ASA 执行平滑重启时，辅助 ASA 会协助不间断转发恢复过程。如果您不希望 ASA 帮助重启的邻居进行不间断转发恢复，请输入 `no nsf ietf helper` 命令。

要在支持 NSF 和支持 NSF 的 ASA 上启用严格 LSA 检查，请输入 `nsf ietf helper strict-lsa-checking` 命令。但是，直到 ASA 在 IETF 平稳重启过程中成为助手 ASA 后，严格 LSA 检查才会生效。启用严格 LSA 检查后，如果辅助 ASA 检测到要泛洪到重启 ASA 的 LSA 发生更改，或者在启动平滑重启过程时重启 ASA 的重传列表中存在已更改的 LSA，则辅助 ASA 将终止重启 ASA 的帮助过程。

CR_Examples 以下示例启用具有严格 LSA 检查的 IETF NSF 助手：

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa
(config-router)# nsf ietf helper strict-lsa-checking
```

Related Commands

命令	说明
nsf cisco	在 ASA 上启用思科 NSF。
nsfciscohelper	在 ASA 上启用思科 NSF 助手模式。
nsf ietf	在 ASA 上启用 IETF NSF。

nt-auth-domain-controller

要指定该服务器的 NT 主域控制器名称，请在 `aaa-server` 主机配置模式下使用 **nt-auth-domain-controller** 命令。要删除此规范，请使用此 **no** 命令的形式。

nt-auth-domain-controller 字符串
no nt-auth-domain-controller

Syntax Description

string 为主域控制器指定此服务器的名称，长度最大为 16 个字符。

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 服务器主机配置	• 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

此命令仅适用于 NT 身份验证 AAA 服务器。首先，必须已使用 **aaa-serverhost** 命令进入主机配置模式。字符串 变量中的名称必须与服务器本身上的 NT 条目匹配。

CR_Examples

以下示例将此服务器的 NT 主域控制器的名称配置为 “primary1”：

```
ciscoasa
(config)# aaa-server svrgrp1 protocol nt
ciscoasa
(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa
(config-aaa-server-host)#
```

Related Commands

命令	说明
aaaserverhost	进入 aaa 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。

命令	说明
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。

ntp authenticate

要启用 NTP 服务器的身份验证，请在 **ntpauthenticate** 全局配置模式下使用该命令。要禁用 NTP 身份验证，请使用此命令 **no** 的形式。

ntp authenticate
no ntp authenticate

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为行为或值。

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	• —	是

Command History 版本 修改

7.0(1) 添加了此命令。

使用指南

如果启用身份验证，ASA 仅当在数据包中使用正确的受信任密钥时，才会与 NTP 服务器通信（请参阅 **ntptrusted-key** 命令）。您还必须指定服务器密钥（请参阅 **ntpserverkey** 命令），否则即使您配置了 **ntpauthenticate** 命令，ASA 也将在不进行身份验证的情况下与服务器通信。ASA 还使用身份验证密钥与 NTP 服务器同步（请参阅 **ntpauthentication-key** 命令）。

CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

命令	说明
ntpauthentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。

命令	说明
ntpserver	标识 NTP 服务器。
ntptrusted-key	为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。
showntpassociations	显示与 ASA 关联的 NTP 服务器。
showntpstatus	显示 NTP 关联的状态。

ntp authentication-key

要设置密钥以使用 NTP 服务器进行身份验证，请在全局配置模式下使用 **ntpauthentication-key** 命令。要删除密钥，请使用此 **no**命令的形式。

```
ntp authentication-keykey_id{ md5 | sha1 | sha256 | sha512 | cmac} key
no ntp authentication-keykey_id [ { md5 | sha1 | sha256 | sha512 | cmac} [0|8] key]
```

Syntax Description	0	（可选）表示<key_value>为纯文本。如果 0 或 8 不存在，则格式为纯文本。
	8	（可选）表示<key_value>为加密文本。如果 0 或 8 不存在，则格式为纯文本。
	key	将密钥值设置为长度最大为 32 个字符的字符串。
	key_id	确定介于 1 和 4294967295 之间的密钥 ID。您必须使用 ntptrusted-key 命令将此 ID 指定为受信任密钥。
	md5	指定认证算法为 MD5。
	sha1	指定身份验证算法为 SHA-1。
	sha256	指定身份验证算法为 SHA-256。
	sha512	指定身份验证算法为 SHA-512。
	cmac	指定身份验证算法为 AES-CMAC。

Command Default	无默认为或值。

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	• —	是

Command History	版本	修改
	7.0(1)	添加了此命令。
	9.13(1)	添加了 sha1sha512 、、 sha256 和关 cmac 键字。

使用指南	要使用 NTP 身份验证，还需配置 ntpauthenticate 命令和 ntpserverkey 命令。

CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

命令	说明
ntpauthenticate	启用NTP身份验证。
ntpserver	标识 NTP 服务器。
ntptrusted-key	为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。
showntpassociations	显示与 ASA 关联的 NTP 服务器。
showntpstatus	显示 NTP 关联的状态。

ntp server

要标识要在 ASA 上设置时间的 NTP 服务器，请在全局配置模式下使用 **ntpserver** 命令。要删除服务器，请使用此命令的形式。

```
ntp server ip_address [ key_id ] [ source_interface_name ] [ prefer ]
no ntp server ip_address [ key_id ] [ source_interface_name ] [ prefer ]
```

Syntax Description

ip_address	设置 NTP 服务器的 IPv4 或 IPv6 IP 地址。
key_id	如果使用 ntp authenticate 命令启用身份验证，则设置此服务器的受信任密钥 ID。另请参阅 ntp trusted-key 命令。
source_interface_name	如果您不想使用路由表中的默认接口，则标识 NTP 数据包的传出接口。由于在多情景模式下系统不包含任何接口，请指定在管理情景中定义的接口名称。
prefer	如果多个服务器具有相似的精度，则将此 NTP 服务器设置为首选服务器。NTP 使用一种算法确定最准确的服务器，然后与该服务器同步。如果多台服务器的准确度相似， prefer 关键字将指定使用这些服务器中的哪台服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。例如，ASA 使用层数为 2 的服务器，而不是优先使用层数为 3 的服务器。

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	• 支持	—	• 是

Command History

版本	修改
7.0(1)	此命令已修改，以使源接口可选。
9.12(1)	我们添加了 IPv6 支持。
9.14(1)	添加了 NTPv4 支持。

使用指南

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。可配置多个 NTP 服务器。ASA 选择层级最低的服务器，作为衡量数据可靠性的方式。在多情景模式下，仅在系统配置中设置 NTP 服务器。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

ASA 支持 NTPv4。

CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

Related Commands

命令	说明
ntpauthenticate	启用NTP身份验证。
ntpauthentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntptrusted-key	为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。
showntpassociations	显示与 ASA 关联的 NTP 服务器。
showntpstatus	显示 NTP 关联的状态。

ntp trusted-key

要将身份验证密钥 ID 指定为可信密钥（这是使用 NTP 服务器进行身份验证所必需的），请在 **ntptrusted-key** 全局配置模式下使用该命令。要删除可信密钥，请使用此命令的形式。可输入多个受信任密钥，供多台服务器使用。

ntp trusted-key *key_id*
no ntp trusted-key *key_id*

Syntax Description

key_id 设置介于 1 和 4294967295 之间的密钥 ID。

Command Default

无默认为行为或值。

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	• —	是

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

要使用 NTP 身份验证，还需配置 **ntpauthenticate** 命令和 **ntpserverkey** 命令。要与服务器同步，请使用 **ntpauthentication-key** 命令为密钥 ID 设置身份验证密钥。

CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

命令	说明
ntpauthenticate	启用NTP身份验证。

命令	说明
ntpauthentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntpserver	标识 NTP 服务器。
showntpassociations	显示与 ASA 关联的 NTP 服务器。
showntpstatus	显示 NTP 关联的状态。

num-packets

如要指定 SLA 操作期间发送的请求数据包数，请在 SLA 监控协议配置模式下使用 **num-packets** 命令。要恢复默认值，请使用此命令 **no** 的形式。

num-packets 编号
no num-packets *number*

Syntax Description	<i>number</i> SLA 操作期间发送的数据包数量。有效值为 1 至 100。 注释 当指定为 <i>number</i> 参数（在此命令中）的所有数据包都丢失时，表明被跟踪的路由发生故障。

Command Default 为回应类型发送的默认数据包数为 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
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 增加发送的数据包的默认数量，以防止由于丢包而导致错误的可达性信息。

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。被跟踪的路由必须丢失所有 5 个数据包

```
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
request-data-size	指定请求数据包负载的大小。
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。

nve

要为 VXLAN 封装创建网络虚拟化终端 (NVE) 实例，请在全局配置模式下使用 **nve** 命令。要删除 NVE 实例，请使用此命令 **no** 的形式。

nve 1
no nve 1

Syntax Description

1 指定 NVE 实例，它始终为 1。

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	• 支持	• 支持	—

Command History

版本 修改

9.4(1) 添加了此命令。

使用指南

每个 ASA 或安全情景可以配置一个 VTEP 源接口。您可以配置一个用于指定此 VTEP 源接口的 NVE 实例。所有 VNI 接口都必须与此 NVE 实例关联。

CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并将 VNI 1 接口与其关联：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

nve-only

要指定 VXLAN 源接口为仅 NVE，请在接口配置模式下使用 **nve-only** 命令。要删除仅限 NVE 的限制，请使用此命令的形式。

nve-only
[cluster]
no nve-only

Syntax Description

Syntax Description **cluster** 在配置 ASA virtual 集群时，必须为集群控制链路指定 **nve-only cluster**。

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
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.4(1) 添加了此命令。

9.17(1) 我们添加了 **cluster** 关键字来支持 ASA virtual 集群。

使用指南

每个 ASA 或安全情景可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)；此时，VXLAN VTEP 是唯一受支持的 NVE。

在透明模式下，VTEP 接口需要 **nve-only** 设置，它允许您为接口配置 IP 地址。在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情况下此命令是可选的。

对于 ASA virtual 集群，必须对集群控制链路使用 VXLAN 接口；在这种情况下，请指定 **nve-only cluster**。

CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并指定它是仅限 NVE 的：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。



室外

- [object-group](#)，第 1082 页
- [object-group-search](#)，第 1087 页
- [object network](#)，第 1090 页
- [object network-service](#)，第 1092 页
- [object service](#)，第 1095 页
- [ocsp disable-nonce](#)，第 1097 页
- [ocsp interface](#)，第 1099 页
- [ocsp url](#)，第 1101 页
- [on](#) 屏幕键盘（已弃用），第 1103 页
- [ospf authentication](#)，第 1104 页
- [ospf authentication-key](#)，第 1106 页
- [ospf cost](#)，第 1108 页
- [ospf database-filter](#)，第 1110 页
- [ospf dead-interval](#)，第 1111 页
- [ospf hello-interval](#)，第 1113 页
- [ospf message-digest-key](#)，第 1114 页
- [ospf mtu-ignore](#)，第 1116 页
- [ospf network point-to-point non-broadcast](#)，第 1117 页
- [ospf priority](#)，第 1119 页
- [ospf retransmit-interval](#)，第 1120 页
- [ospf transmit-delay](#)，第 1121 页
- [otp expiration](#)，第 1122 页
- [output console](#)，第 1124 页
- [output file](#)，第 1125 页
- [output none](#)，第 1127 页
- [outstanding](#)（已弃用），第 1128 页
- [override-account-disable](#)（已弃用），第 1130 页
- [override-svc-download](#)，第 1132 页

object-group

要定义可用于优化配置的对象组，请在全局配置模式下使用 **object-group** 命令。使用此命令的形式从配置中删除对象组。

```
object-group {protocol | network | icmp-type | security | user | network-service} grp_name
object-group servicegrp_name [tcp | udp | tcp-udp]
```

Syntax Description	grp_name	标识对象组（1 到 64 个字符），可以是字母、数字以及 “_”、“-”、“。” 的任意组合。个字符。
	icmp-type	（不推荐，请使用 service 。）定义一组 ICMP 类型，例如 echo 和 echo-reply。输入 object-groupicmp-type 命令后，使用 icmp-object 和 group-object 命令添加 ICMP 对象。
	network	定义一组主机或子网 IP 地址。输入 object-groupnetwork 命令后，使用 network-object 和 group-object 命令添加网络对象。您可以创建一个混合有 IPv4 和 IPv6 地址的组。 注释 不能使用混合对象组进行 NAT。
	network-service	使用可选服务规范定义一组子网或域名。输入此命令后，使用 network-service-member 命令添加网络服务对象，或使用 domain 和 subnet 命令直接添加成员。
	protocol	（不推荐，请使用 service 。）定义一组协议，例如 TCP 和 UDP。输入 object-groupprotocol 命令后，使用 protocol-object 和 group-object 命令添加协议对象。
	security	定义与思科 TrustSec 配合使用的安全组对象。输入 object-groupprotocol 命令后，使用 security-group 和 group-object 命令添加安全组对象。
	service	根据协议、ICMP 类型和 TCP/UDP/SCTP 端口定义服务。
	[tcp udp tcp-udp]	要定义混合服务组或 SCTP 端口，请不要为对象组指定协议类型。输入命令 object-groupservice 后，使用 service-object 和 命令将服务对象添加到服务组中。 group-object 这是首选方法，即使对象旨在仅包含 TCP 或 UDP（或两者）端口列表。 不建议在 object-group service 命令中直接使用 tcp 、 udp 和 tcp-udp 关键字。相反，请将这些关键字放在命令之外，并在 service-object 命令上配置 TCP 和 UDP 端口。如果您包含其中一个关键字，请使用 port-object 和 group-object 命令添加端口组。
	user	定义可用于控制身份防火墙访问的用户和用户组。输入 object-groupprotocol 命令后，使用 user 、 user-group 和 group-object 命令添加用户和用户组对象。

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	• 支持	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

8.4(2) 添加了对 **user** 关键字的支持以支持身份防火墙。

9.0(1) 您现在可以创建支持 IPv4 和 IPv6 地址混合的网络对象组。

添加了对 **security** 关键字的支持以支持思科 TrustSec。

9.14 该 **icmp-type** 关键字已被弃用。请使用 **service** 关键字，并在对象中指定 **serviceicmp**。

9.17(1) 添加了 **network-service** 关键字。

使用指南

可以对主机或服务等对象进行分组，然后可以在 ACL (**access-list**) 和 NAT (**nat**) 等功能中使用对象组。此示例显示如何在 ACL 中使用网络对象组：

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group NWgroup1
```

您可以按层次结构对命令进行分组；；对象组可以是其他对象组的成员。

CR_Examples

以下示例显示如何使用 **object-group network** 命令创建网络对象组：

```
ciscoasa(config)# object-group network sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.eng.ftp.servcers
ciscoasa(config-network-object-group)# network-object host 172.23.56.194
ciscoasa(config-network-object-group)# network-object 192.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# exit
```

以下示例显示如何使用 **object-group network** 命令创建包含现有对象组的网络对象组：

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers

ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224

ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

以下示例显示如何使用 **group-object** 模式创建一个包含先前定义的对象的新对象组，以及如何在 ACL 中使用这些对象：

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)# access-list all permit tcp object-group all_hosts any eq www
```

如果没有 **group-object** 命令，则需要定义 *all_hosts* 组，以包含 *host_grp_1* 和 *host_grp_2* 中已定义的所有 IP 地址。使用 **group-object** 命令，可以消除主机的重复定义。

以下示例显示如何将 TCP 和 UDP 服务添加到服务对象组：

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示如何将多个服务对象添加到服务对象组：

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object-group)# service tcp destination eq ssh
ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object-group)# service eigrp
ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object-group)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# group-object SSH
ciscoasa(config-service-object-group)# group-object EIGRP
ciscoasa(config-service-object-group)# group-object HTTPS
```

以下示例显示如何在服务对象组中添加协议、端口和 ICMP 混合格规：

```
ciscoasa(config)# object-group service mixed
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

以下示例显示如何使用 **service-object** 子命令，该命令对于对 TCP 和 UDP 服务进行分组非常有用：

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
ciscoasa(config-network-object-group)# network-object host kqk.suu.py1.gnl
```



```

ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group locals
object-group remote

```

以下示例显示如何使用 **object-group user** 命令创建用户组对象：

```

ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3

```

（不建议使用，请改用服务对象。）以下示例显示如何使用 **object-group icmp-type** 模式创建 ICMP 对象组：

```

ciscoasa(config)# object-group icmp-type icmp-allowed
ciscoasa(config-icmp-object-group)# icmp-object echo
ciscoasa(config-icmp-object-group)# icmp-object time-exceeded
ciscoasa(config-icmp-object-group)# exit

```

（不建议使用，请改用服务对象。）以下示例显示如何使用 **object-group protocol** 模式创建协议对象组：

```

ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit
ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit

```

（不建议使用，无需使用 **tcp** 关键字，而是使用 **service-object** 命令定义端口。）以下示例显示如何使用 **object-group service** 模式创建 TCP 端口对象组：

```

ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service-object-group)# group-object eng_www_service
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object range 2000 2005
ciscoasa(config-service-object-group)# exit

```

以下示例显示如何使用对象组简化访问列表配置。此分组支持在 1 行中配置访问列表，而不是在不使用分组的情况下需要 24 行。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100
ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```



注释 `showrunning-configaccess-list` 命令显示配置的对象组名称的访问列表。`showaccess-list`命令显示此信息以及使用组扩展为单个条目（不含其对象分组）的访问列表条目。

以下示例使用先前定义的网络服务对象配置一组 SaaS 应用程序。

```
object-group network-service SaaS_Applications
description This group includes relevant 'Software as a Service' applications
network-service-member "outlook 365"
network-service-member webex
network-service-member box
```

Related Commands

命令	说明
<code>clearconfigureobject-group</code>	从配置中删除所有对象组命令。
<code>group-object</code>	添加网络对象组。
<code>network-object</code>	向网络对象组添加网络对象。
<code>port-object</code>	将端口对象添加到服务对象组。
<code>security-group</code>	将安全组添加到安全组对象组。
<code>showrunning-configobject-group</code>	显示当前对象组。
<code>user</code>	将用户名添加到用户组对象。
<code>user-group</code>	向用户组对象添加用户组名。

object-group-search

要启用 ACL 优化，请在 **object-group-search** 全局配置模式下使用该命令。使用此命令 **no** 的形式可以禁用 ACL 优化。

```
object-group-search { access-control | threshold }
no object-group-search { access-control | threshold }
```

Syntax Description	access-control 启用对象组搜索访问控制规则。
	threshold 为对象组搜索处理启用最大阈值。有关详细信息，请参阅使用说明。

Command Default (9.18 之前) 默认情况下禁用对象组搜索。默认情况下，阈值也是禁用的。
从 9.18 开始，默认启用对象组搜索以控制新部署的访问。

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
	8.3(1) 添加了此命令。
	9.12(1) 添加了 threshold 关键字。9.8、9.9 和 9.10 的临时版本中还添加了 关键字。
	9.18(1) 对于新部署，访问控制的默认设置已更改为启用。如果以前未启用此功能，则必须在升级时启用它。

使用指南 **object-group-search**命令优化入站方向的所有 ACL。

通过启用对象组搜索可降低搜索访问规则所需的内存，但此规则会影响查询性能及增加 CPU 使用量。启用后，对象组搜索不会扩展 ASP 表中 使用网络或服务对象的 ACL，而是根据这些组定义搜索访问规则以查找匹配项。您将在 **showaccess-list** 输出中看到这一点。

对象组搜索受限于一个阈值。对于每个连接，将根据网络对象匹配源和目标 IP 地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。此检查是为了防止性能降低。配置规则以防止过多的匹配项。避免创建重复的对象，以防止达到阈值。

从版本 9.12(1) 开始，在回到 9.8(x) 的临时版本中，默认情况下此阈值处于禁用状态。使用 **showrunning-configallobject-group-search** 命令来确定是否配置了阈值选项；如果已配置，则确定当前设置。

启用对象组搜索时，如果为访问组启用了大量功能、大量活动连接和大型 ACL，则在操作期间会断开连接，并且在建立新连接时性能会下降。即使您启用事务性提交 (**asprule-enginetransactional-commitaccess-group**)，也可能发生这些丢弃。



注释 对象组搜索仅适用于网络和服务对象。它不适用于安全组或用户对象。如果 ACL 包括安全组，请勿启用此功能。结果可能是非活动的 ACL 或其他意外行为。

CR_Examples

以下示例显示如何使用该 **object-group-search** 命令启用 ACL 优化：

```
ciscoasa(config)# object-group-search access-control
```

以下是未启用时 **object-group-search** 的 **showaccess-list** 命令示例输出：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group BLK-LAN
0x724c956b
access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 192.168.4.0
255.255.255.0 (hitcnt=10) 0x30fe29a6
access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
255.255.255.0 (hitcnt=4) 0xc6ef2338
access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 14.14.14.0
255.255.255.0 (hitcnt=2) 0xce8596ec
access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

以下是启用时 **object-group-search** 命令的 **showaccess-list** 示例输出：

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2) (hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

Related Commands

命令	说明
clearconfigobject-groupsearch	清除 object-group-search 配置。
showobject-group	如果对象组是网络对象组类型，则显示命中计数。
showrunning-configobject-group	显示当前对象组。
showrunning-configobject-group-search	显示运行配置中的 object-group-search 配置。

object network

要配置命名网络对象，请在全局配置模式下使用 **objectnetwork**命令。使用此命 **no**令的形式从配置中删除对象。

```
name object network renamenew_obj_name []
no object networkname
```

Syntax Description	name	指定网络对象的名称。名称长度可以是 1 到 64 个字符，由字母、数字和以下特殊字符组成：下划线、连字符、逗号、正斜杠和句点。对象和对象组共享相同的命名空间。
	renamenew_obj_name	（可选）将对象重命名为新的对象名称。

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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	8.3(1)	添加了此命令。
	8.4(2)	添加了对完全限定域名 (FQDN) 的支持。请参阅 fqdn 命令。

使用指南 网络对象可以包含主机、网络、范围 IP 地址（IPv4 或 IPv6）或 FQDN。输入命令后，请使用 **host**、**fqdn**、**subnet**或 **range** 命令向对象添加一个地址。

您还可以使用 **nat** 命令在此网络对象上启用 NAT 规则。您只能为给定对象定义一条 NAT 规则；如果要配置多条 NAT 规则，则需要创建多个指定相同 IP 地址的对象 **objectnetworkobj-10.10.10.1-01**，**objectnetworkobj-10.10.10.1-02**例如，等等。

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网络对象：

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

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。
host	指定主机网络对象。
nat	为网络对象启用 NAT。
object-group network	创建网络对象组。
range	指定网络对象的地址范围。
showrunning-configobjectnetwork	显示网络对象配置。
subnet	指定子网网络对象。

object network-service

要配置命名的网络服务对象，请在全局配置模式下使用 **object network-service** 命令。使用此命令 **no** 的形式从配置中删除对象。

```
object network-service name [ dynamic ]
no object network-service name
```

Syntax Description	dynamic （可选。） dynamic 关键字意味着对象不会保存到运行配置，它将仅显示在 show object 输出中。 dynamic 关键字主要供外部设备管理器使用。
	<i>name</i> 名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。

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	• 支持	• 支持	—

Command History	版本 修改
	9.17(2) 添加了此命令。

使用指南 网络服务对象定义了一个应用。它通过子网规范或更常见的DNS域名来定义应用的位置。您也可以选择包括协议和端口，以缩小应用的范围。

只能在网络服务组对象中使用这些对象；不能在访问控制列表条目(ACE)中直接使用网络服务对象。

使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **domain domain_name [service]** - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 **www.example.com**）或部分名称（例如 **example.com**），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 **www.example.com**、**www1.example.com**、**long.server.name.example.com** 等）。如果存在完全匹配的名称，则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。

- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} [service] - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时，才指定服务。默认情况下，与已解析 IP 地址的任何连接都与对象相匹配。

protocol [operator port]

其中：

- *protocol* 是连接中使用的协议，例如 tcp、udp、ip 等。使用 ? 查看协议列表。
- （仅限 TCP/UDP。）*operator* 为以下选项之一：
 - **eq** 等于指定的端口号。
 - **lt** 表示小于指定端口号的任何端口。
 - **gt** 表示大于指定端口号的任何端口。
 - **range** 表示两个指定端口之间的任何端口。
- （仅限 TCP/UDP。）*port* 是端口号 1-65535 或助记符，例如 www。使用 ? 查看助记符。对于范围，必须指定两个端口，并且第一个端口号要小于第二个端口号。

示例

以下是网络服务对象的示例。

```
object network-service outlook365
  description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Related Commands

命令	说明
app-id	指定对象的应用 ID。
clear object	清除网络服务对象的命中计数。
description	为对象添加描述。
domain	指定对象的域名。
object-group network-service	创建网络服务对象组。
show object	显示网络服务对象。

命令	说明
subnet	指定对象的子网。

object service

要将某个服务对象配置为自动反映在使用该对象的所有配置中，请在全局配置模式下使用 **object service** 命令。使用此命令 **no** 的形式来删除对象。

object servicename [**renamenew_obj_name**]
no object service 对象名称 [**renamenew_obj_name**]

Syntax Description

name 指定服务对象的名称。名称长度可以是 1 到 64 个字符，由字母、数字和以下特殊字符组成：下划线、连字符、逗号和句点。对象名称必须以字母开头。

renamenew_obj_name （可选）将对象重命名为新的对象名称。

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
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

8.3(1) 添加了此命令。

使用指南

服务对象可以包含协议、ICMP、ICMPv6 或 TCP /UDP/SCTP 端口或端口范围。输入命令后，使用 **service** 命令向对象添加一个服务规格。

如果使用不同的协议和端口（或多个端口）配置现有的服务对象，则新配置将用新的协议和端口（或多个端口）替换现有的协议和端口（或多个端口）。

CR_Examples

以下示例显示如何创建服务对象：

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

Related Commands

命令	说明
clearconfigureobject	清除创建的所有对象。

命令	说明
service	配置服务对象的协议和端口。

ocsp disable-nonce

要禁用 nonce 扩展，请在 `crypto ca trustpoint` 配置模式下使用 `ocsp disable-nonce` 命令。要重新启用随机数扩展，请使用此命令的 **no** 形式。

ocsp disable-nonce
no ocsp disable-nonce

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下，OCSP 请求包括一个随机数扩展。

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 trustpoint 配置	• 是	• 支持	• 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 使用此命令时，OCSP 请求不包括 OCSP 随机数扩展，ASA 也不会检查。默认情况下，OCSP 请求包含一个 nonce 扩展，它以加密方式绑定请求和响应以避免重放攻击。但是，某些 OCSP 服务器使用不包含此匹配随机数扩展的预生成响应。要将 OCSP 用于这些服务器，必须禁用 nonce 扩展。

CR_Examples 以下示例显示如何禁用名为 `newtrust` 的信任点的随机数扩展。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。在全局配置模式下使用此命令。
match certificate	配置 OCSP 覆盖规则。
ocspinterfacenameif	指定可用于 OCSP 吊销检查的接口。

命令	说明
ocspurl	指定要用于检查与信任点关联的所有证书的 OCSP 服务器。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

ocsp interface

要配置使 ASA 访问 OCSF 的源接口，请在 `crypto ca trustpool` 配置模式下使用 **interface nameif** 命令。
要从配置中删除接口，请使用此 命 令的no形式。

ocsp interface nameif
no ocsp interface nameif

Syntax Description	interface 指定 ASA 用于访问 OCSF 服务器的接口。 <i>nameif</i>

Command Default	此命令没有默认值。

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
Crypto ca trustpoint 配置。	• 是	• 支持	• 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	默认情况下，OCSF 使用不包括管理接口条目的全局路由表。如果 OCSF 位于管理接口之后，则 OCSF 吊销检查不会成功。当您使用此命令时，可以将 OCSF 吊销检查配置为使用接口，包括管理接口（视需要而定）。

CR_Examples	以下示例显示如何配置 OCSF 的源接口。

```

ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSF Nonce Extension
  interface      Configure Source interface
  url            OCSF server URL
ciscoasa(config-ca-trustpoint)# ocsp interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
    
```

```
inside      Name of interface GigabitEthernet0/0.100
inside1     Name of interface GigabitEthernet0/0.41
mgmt        Name of interface Management0/0
outside     Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url ?

crypto-ca-trustpoint mode commands/options:
  LINE < 500 char  URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url http://lal-bagh:8888
```

Related Commands

命令	说明
ocsp url	指定要用于检查与信任点关联的所有证书的 OCSP 服务器。
ocsp disable-nonce	禁用 OCSP 请求的 nonce 扩展。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

ocsp url

要为 ASA 配置 OCSP 服务器以用于检查与信任点（而不是客户端证书的 AIA 扩展中指定的服务器）关联的所有证书，请在 **ocspurl**crypto ca trustpoint 配置模式下使用该命令。要从配置中删除服务器，请使用此命 **no** 令的形式。

ocsp url*URL*
no ocsp url

Syntax Description	<i>URL</i> 指定 OCSP 服务器的 HTTP URL。 注释 同时支持 IPv4 和 IPv6 OCSP URL。将 IPv6 地址括在方括号中，例如： <i>http://[0:0:0:0:18:0a01:7c16]</i>。

Command Default	无默认为或值。

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
Crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History	版本 修改 7.2(1) 添加了此命令。 9.20(1) 添加了对 IPv6 OCSP URL 的支持。

使用指南	ASA 仅支持 HTTP URL，而您只能为每个信任点指定一个 URL。 ASA 提供三种定义 OCSP 服务器 URL 的方法，并且 ASA 会按照您的定义方式尝试使用 OCSP 服务器，顺序如下： • 您使用 matchcertificate 命令设置的 OCSP 服务器。 • 使用 ocspurl 命令设置的 OCSP 服务器。 • 客户端证书的 AIA 字段中的 OCSP 服务器。

如果您不通过 **matchcertificate** 命令或 **ocspurl** 命令配置 OCSP URL，ASA 将使用客户端证书的 AIA 扩展中的 OCSP 服务器。如果证书没有 AIA 扩展，则吊销状态检查失败。

CR_Examples

以下示例显示如何使用 URL http://10.1.124.22 配置 OCSP 服务器。

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

以下示例显示如何使用 IPv6 URL 配置 OCSP:

```
ciscoasa(config)# crypto ca trustpointnewtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://[0:0:0:0:ffff:0a01:7c16]
ciscoasa(config-ca-trustpoint)#
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。在全局配置模式下使用此命令。
match certificate	配置 OCSP 覆盖规则。
ocspdisable-nonce	禁用 OCSP 请求的 nonce 扩展。
ocspinterfacenameif	指定可用于 OCSP 吊销检查的接口。
revocation-check	指定用于吊销检查的方法以及尝试这些方法的顺序。

on 屏幕键盘（已弃用）

要将屏幕键盘插入登录窗格或具有登录名/密码要求的所有窗格，请在 `webvpn` 模式下使用 `onscreen-keyboard` 命令。要删除以前配置的屏幕键盘，请使用此命令的 `no` 版本。

onscreen-keyboard { **logon** | **all** }
no onscreen-keyboard [**logon** | **all**]

Syntax Description

logon 为登录窗格插入屏幕键盘。

all 为登录窗格以及有登录名/密码要求的所有其他窗格插入屏幕键盘。

Command Default

没有屏幕键盘。

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配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	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

通过屏幕键盘，您可以输入用户凭证而无需按键。

CR_Examples

以下示例显示如何为登录页面启用屏幕键盘：

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
onscreen-keyboard logon
ciscoasa (config-webvpn)#
```

Related Commands

命令	说明
<code>webvpn</code>	进入 <code>webvpn</code> 模式，该模式让您配置无客户端 SSLVPN 连接的属性。

ospf authentication

要启用 OSPF 验证，请在接口配置模式下使用 **ospfauthentication** 命令。要恢复默认的身份验证立场，请使用此命令的 **no**形式。

```
ospfauthentication { key-chain key-chain-name | message-digest | null }
no ospf authentication
```

Syntax Description	key-chain （可选）指定用于身份验证的密钥链。key-name 参数最多可以为 63 个字母数字字符。 <i>key-chain-name</i>
	message-digest （可选）指定使用 OSPF 消息摘要身份验证。
	null （可选）指定不使用 OSPF 身份验证。

Command Default 默认情况下，未启用 OSPF 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	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.0(1) 增加了多情景模式支持。
	9.12(1) 添加了密钥链功能，以支持 OSPF 身份验证的轮换密钥。

使用指南

在使用 **ospfauthentication** 命令之前，使用 **ospfauthentication-key** 命令为接口配置密码。如果您使用 **message-digest** 关键字，请为带有 **ospfmessage-digest-key** 命令的接口配置 message-digest key。

为了获得后向兼容性，仍然支持区域的身份验证类型。如果没有为接口指定身份验证类型，则将使用区域的身份验证类型（区域默认为空身份验证）。

使用不带任何选项的此命令时，将启用简单密码身份验证。

CR_Examples

以下示例显示如何在所选接口上为 OSPF 启用简单密码身份验证：

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

以下示例显示如何在所选接口上为 OSPF 启用密钥链密码身份验证：

```
ciscoasa(config)# interface gigabitEthernet 0/0
ciscoasa(config-if)# ospf authentication key-chain CHAIN-INT-OSPFKEYS
```

Related Commands

命令	说明
ospf authentication-key	指定相邻路由设备使用的密码。
ospfmessage-digest-key	启用 MD5 身份验证并指定 MD5 密钥。

ospf authentication-key

要指定相邻路由设备使用的密码，请在接口配置模式下使用 **ospfauthentication-key** 命令。要删除密码，请使用此命令 **no** 的形式。

```
ospfauthentication-key [ 0|8 ] password
no ospf 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。
	password	分配 OSPF 身份验证密码，供相邻路由设备使用。密码必须少于 9 个字符。可以在两个字符之间包含空格。密码开头或结尾的空格将被忽略。

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
接口配置	• 是	—	• 是	• 支持	—

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

使用指南 该命令创建的密码将用作密钥，在发起路由协议数据包时直接插入到 OSPF 报头中。可以为每个接口的每个网络指定单独的密码。同一网络上的所有相邻路由器都必须具有同一密码才能交换 OSPF 信息。

CR_Examples 以下示例显示如何指定 OSPF 身份验证的密码：

```
ciscoasa(config-if)# ospf authentication-key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands	命令	说明
	areaauthentication	为指定区域启用 OSPF 身份验证。

命令	说明
ospfauthentication	启用 OSPF 身份验证。

ospf cost

要指定通过接口发送数据包的开销，请在接口配置模式下使用 **ospf cost** 命令。要将接口成本重置为默认值，请使用此命令的 **no**形式。

ospf cost*interface_cost*
no ospf cost

Syntax Description	<i>interface_cost</i> 通过接口发送数据包的开销（一种链路状态度量）。这是一个无符号整数，范围介于 0 至 65535 之间。0 表示直接连接到接口的网络，并且接口带宽越高，通过该接口发送数据包的关联开销就越低。换句话说，较大的开销值表示低带宽接口，而较低开销值表示高带宽接口。 ASA 上的 OSPF 接口默认成本为 10。此默认值与 Cisco IOS 软件不同，后者的默认开销为 1（适用于快速以太网和千兆以太网）和 10（适用于 10BaseT）。如果您在网络中使用 ECMP，则必须此情况考虑在内。

Command Default	默认接 口成本为 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
接口配置	• 是	—	• 是	• 支持	—

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

使用指南	该 ospf cost 命令允许您明确指定在接口上发送数据包的成本。<i>interface_cost</i> 参数是一个从 0 到 65535 的无符号整数值。 noospf cost命令允许您将路径开销重置为默认值。

CR_Examples	以下示例展示如何指定在所选接口上发送数据包的开销：

```
ciscoasa(config-if)# ospf cost 4
```


Related Commands

命令	说明
showrunning-configinterface	显示指定接口的配置。

ospf database-filter

要在同步和泛洪期间过滤掉到 OSPF 接口的所有传出 LSA，请在 **ospfdatabase-filter** 接口配置模式下使用该命令。要恢复 LSA，请使用此命令 **no** 的形式。

ospf database-filterallout
no ospf database-filterallout

Syntax Description **allout** 过滤所有传出到 OSPF 接口的 LSA。

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
接口配置	• 是	—	• 是	—	—

Command History 版本 修改
7.0(1) 添加了此命令。

使用指南 该 **ospfdatabase-filter**命令过滤发往 OSPF 接口的 LSA。 **noospfdatabase-filterallout** 命令恢复将 LSA 转发到接口。

CR_Examples 以下示例显示如何使用 **ospfdatabase-filter** 命令过滤传出 LSA：

```
ciscoasa(config-if)# ospf database-filter all out
```

命令	说明
showinterface	显示接口状态信息。

ospf dead-interval

要指定邻居声明路由器关闭之前的间隔，请在接口配置模式下使用 **ospfdead-interval**命令。要恢复默认值，请使用此命 **no** 令的形式。

ospf dead-interval { 秒 **minimal** | **hello-multiplier** 乘数 }
no ospf dead-interval

Syntax Description	<i>seconds</i>	未发现呼叫数据包的时间长度。 <i>seconds</i> 的默认值是 ospfhello-interval 命令设置的间隔的四倍（其范围为 1 至 65535）。
	最低	将 dead 间隔设置为 1 秒。使用此关键字要求还配置了 hello-multiplier 关键字和 multiplier 参数。
	hello-multiplier 乘数	范围为 3 至 20 的整数，表示 1 秒内发送的呼叫数据包的数量。

Command Default 秒 的默认值是命令设置的间隔的 **ospfhello-interval**四倍。

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	• 支持	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.0(1) 增加了多情景模式支持。
	9.2(1) 添加了对 Fast Hello 数据包的支持。

使用指南 通过 **ospf dead-interval** 命令，您可以设置 dead 间隔之前邻居的声明路由器关闭（看不到呼叫数据包的时间长度）。 *seconds* 参数用于指定 dead 间隔，它对于网络上的所有节点都必须相同。 *seconds* 的默认值是 **ospfhello-interval** 命令设置的间隔的四倍，范围为 1 到 65535。

no ospf dead-interval 命令可恢复默认间隔值。

Dead 间隔在 OSPF 呼叫数据包中通告。此值对于特定网络上的所有网络设备都必须相同。

指定较小的死亡间隔（秒）将更快地检测到邻居关闭并改善收敛，但可能会导致更多的路由不稳定性。

快速呼叫数据包 OSPF 支持

通过指定带有 multiplier 参数的 maximum 和 hello-multiplier 关键字，可以启用 OSPF 快速呼叫数据包。minimal 关键字将死间隔设置为 1 秒，hello-multiplier 值设置在该 1 秒内发送的 hello 数据包的数量，从而提供亚秒级或“快速”hello 数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为 1 秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

使用 show ospf interface 命令验证 dead 间隔和 fast hello 间隔。

CR_Examples

在以下示例中，通过指定 minimal 关键字以及 hello-multiplier 关键字和值来启用 OSPF 对快速 Hello 数据包的支持。由于乘数设置为 5，因此每秒将发送五个呼叫数据包。

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

Related Commands

命令	说明
ospfhello-interval	指定接口发送 hello 数据包的间隔。
showospfinterface	显示OSPF相关的接口信息。

ospf hello-interval

要指定接口上发送的 hello 数据包之间的间隔，请在 **ospfhello-interval** 接口配置模式下使用该命令。要将呼叫间隔恢复为默认值，请使用此命令的 **no** 形式。

ospfhello-interval秒
no ospf hello-interval

Syntax Description

seconds 指定在接口上发送呼叫数据包的间隔；其有效值范围为 1 至 65535 秒。

Command Default

秒的默认 值为 **hello-interval**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
接口配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

该值在 hello 数据包中公布。问候间隔越小，检测到的拓扑变化就越快，但随之而来的路由流量也越多。对于特定网络上的所有路由器和接入服务器，此值必须相同。

CR_Examples

以下示例将 OSPF 呼叫间隔设置为 5 秒：

```
ciscoasa(config-if)# ospf hello-interval 5
```

Related Commands

命令	说明
ospfdead-interval	指定邻居声明路由器关闭之前的间隔。
showospfinterface	显示OSPF相关的接口信息。

ospf message-digest-key

要启用 OSPF MD5 验证，请在接口配置模式下使用 **ospfmessage-digest-key** 命令。要删除 MD5 密钥，请使用此命 **no** 令的形式。

```
ospfmessage-digest-keykey-idmd5 [0|8] key
no ospf message-digest-key
```

Syntax Description	key-id 启用 MD5 身份验证并指定数字身份验证密钥 ID 号码；有效值为 1 到 255。
md5密 钥	最多 16 个字节的字母数字密码。您可以在关键字之间添加空格。密钥开头或结尾的空格将被忽略。MD5 身份验证负责验证通信的完整性、认证信源并检查时效性。
0	指定将遵循未加密的密码
8	指定将遵循的加密密码。

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
接口配置	• 是	—	• 是	• 支持	—

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

使用指南 ospf message-digest-key 命令允许您启用 MD5 身份验证。通过该命令的 **no** 形式，可删除旧的 MD5 密钥。key_id 是身份验证密钥的数字标识符，范围介于 1 到 255 之间。key 是最多 16 字节的字母数字密码。MD5 负责验证通信的完整性、认证信源并检查时效性。

CR_Examples 以下示例显示如何指定用于 OSPF 身份验证的 MD5 密钥：

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

Related Commands

命令	说明
areaauthentication	启用 OSPF 区域验证。
ospfauthentication	启用 OSPF 身份验证。

ospf mtu-ignore

要禁用接收数据库数据包时的 OSPF 最大传输单元 (MTU) 不匹配检测，请在 **ospfmtu-ignore**接口配置模式下使用该命令。要恢复 MTU 不匹配检测，请使用此命令的 **no** 形式。

ospfmtu-ignore
no ospf mtu-ignore

- Syntax Description**
- 此命令没有任何参数或关键字。
- Command Default**
- 默认情况下，处于启 **ospfmtu-ignore**用状态。
- 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
- 7.0(1) 添加了此命令。

使用指南

OSPF 检查邻居在公用接口上是否使用同一 MTU。当邻居交换数据库描述符 (DBD) 数据包时，将执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，则不会建立 OSPF 邻接。该命令禁用接收 DBD 数据包时的 **ospfmtu-ignore**OSPF MTU 不匹配检测。该类别在默认情况下已启用。

CR_Examples

以下示例显示如何禁用该 **ospfmtu-ignore**命令：

```
ciscoasa(config-if)# ospf mtu-ignore
```

命令	说明
showinterface	显示接口状态信息。

ospf network point-to-point non-broadcast

要将 OSPF 接口配置为点对点非广播网络，请在接口配置模式下使用 **ospfnetworkpoint-to-pointnon-broadcast** 命令。要从配置中删除此命令，请使用此命令 **no** 的形式。

ospf network point-to-point non-broadcast
no ospf network point-to-point non-broadcast

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认为行为或值。

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
接口配置	• 是	—	• 是	• 支持	—

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

使用指南

该 **ospfnetworkpoint-to-pointnon-broadcast**命令允许您通过 VPN 隧道传输 OSPF 路由。

将接口指定为点对点接口时，必须手动配置 OSPF 邻居；无法进行动态发现。要手动配置 OSPF 邻居，请在路由器配置模式下使用 **neighbor** 命令。

当接口配置为点对点时，适用以下限制：

- > 您只能为接口定义一个邻居。
- 您无需定义指向加密终端的静态路由。
- 除非显式配置邻居，否则接口无法形成邻接关系。
- 如果接口上运行着基于隧道的 OSPF，则不能在同一接口上运行具有上游路由器的常规 OSPF。
- 您应该在指定 OSPF 邻居之前将加密映射绑定到接口，以确保 OSPF 更新通过 VPN 隧道传递。如果在指定 OSPF 邻居后将加密映射绑定到接口，请使用该**clearlocal-hostall**命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接关系。

CR_Examples 以下示例显示如何将所选接口配置为点对点非广播接口：

```
ciscoasa(config-if)# ospf network point-to-point non-broadcast  
ciscoasa(config-if)#
```

Related Commands

命令	说明
neighbor	指定手动配置的 OSPF 邻居。
showinterface	显示接口状态信息。

ospf priority

要更改 OSPF 路由器优先级，请在接口配置模式下使用 **ospfpriority** 命令。要恢复默认优先级，请使用此命令 **no** 的形式。

ospf priority 编号
no ospf priority [*number*]

Syntax Description

number 指定路由器的优先级；有效值为 0 到 255。

Command Default

数字的默认值为 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
接口配置	• 是	—	• 是	• 支持	—

使用指南

如果连接到网络的两台路由器同时尝试成为指定路由器，则优先采用具有较高优先级的路由器。如果优先级相同，则优先采用具有较高路由器 ID 的路由器。优先级设置为 0 的路由器没有资格成为指定路由器或备用指定路由器。只为多路访问网络（即，不为点对点网络）的接口配置路由器优先级。

在多情景模式下，对于共享接口，请指定 0 以确保设备不会成为指定路由器。OSPFv2 实例无法跨共享接口相互建立邻接关系。

CR_Examples

以下示例显示如何更改所选接口上的 OSPF 优先级：

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

Related Commands

命令	说明
showospfinterface	显示 OSPF 相关的接口信息。

ospf retransmit-interval

要指定属于该接口的邻接关系的 LSA 重新传输之间的时间，请在 **ospfretransmit-interval**接口配置模式下使用该命令。要恢复默认值，请使用此命 **no** 令的形式。

```
ospf retransmit-interval [seconds]
no ospf retransmit-interval [seconds]
```

Syntax Description *seconds* 指定属于接口的相邻路由器的 LSA 重新传输的间隔时间；； 其有效值范围为 1 至 65535 秒。

Command Default 秒的默认 **retransmit-interval**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
接口配置	• 是	—	• 是	• 支持	—

Command History

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

使用指南

当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有收到确认，它将重新发送 LSA。

此参数设置应保守，否则将导致不必要的重新传输。串行线路和虚拟链路的值应较大。

CR_Examples

以下示例显示如何更改 LSA 的重新传输间隔：

```
ciscoasa(config-if)# ospf retransmit-interval 15
ciscoasa(config-if)#
```

命令	说明
showospfinterface	显示OSPF相关的接口信息。

ospf transmit-delay

如要设置在接口上发送链路状态更新数据包所需的估计时间，请在接口配置模式下使用 **ospftransmit-delay** 命令。要恢复默认值，请使用此命令 **no** 的形式。

ospf transmit-delay [秒]

no ospf transmit-delay [秒]

Syntax Description

seconds 设置在接口上发送链路状态更新数据包所需的估计时间。默认值为 1 秒，范围为 1 至 65535 秒。

Command Default

秒的默认值为 1 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
接口配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.0(1) 增加了多情景模式支持。

使用指南

更新数据包中的 LSA 在传输之前必须将其年龄增加秒数参数中指定的量。分配的值应将接口的传输和传播延迟考虑在内。

如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。此设置对于超低速链路意义更大。

CR_Examples

以下示例将选定接口的传输延迟设置为 3 秒：

```
ciscoasa(config-if)# ospf retransmit-delay 3
ciscoasa(config-if)#
```

Related Commands

命令	说明
showospfinterface	显示 OSPF 相关的接口信息。

otp expiration

要为本地证书颁发机构(CA)注册页面指定一次性密码(OTP)的有效持续时间（以小时为单位），请在 `ca` 服务器配置模式下使用 **otpexpiration**命令。要将持续时间重置为默认小时数，请使用此命令的 **no**形式。

otp expiration*timeout*
no otp expiration

Syntax Description *timeout* 指定在注册页面的 OTP 到期之前，用户必须从本地 CA 注册证书的时间（以小时为单位）。有效值范围为 1 至 720 小时（30 天）。

Command Default 默认情况下，证书注册的 OTP 过期时间为 72 小时（3 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 OTP 过期期限指定用户必须登录到 CA 服务器注册页面的小时数。在用户登录并注册证书之后，**enrollmentretrieval** 命令指定的时间段开始。



注释 用户在注册界面页面上注册证书时使用的 OTP 也用作解锁包含为该用户颁发的证书和密钥对的 PKCS12 文件的密码。

CR_Examples 以下示例指定注册页面的 OTP 应用 24 小时：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# otp expiration 24
ciscoasa
(config-ca-server)
#
```

以下示例将 OTP 持续时间重置为默认值 72 小时：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# no otp expiration
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。
enrollment-retrieval	指定注册用户可以检索 PKCS12 注册文件的时间（以小时为单位）。
showcryptocaserver	显示证书颁发机构配置。

output console

要将 **action** 命令的输出发送到控制台，请在事件管理器小程序配置模式下使用 **outputconsole** 命令。
要删除控制台作为输出目的地，请使用此命令的 **no**形式。

output console
no output console

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南 使用此命令可将 **action** 命令的输出发送到控制台。

CR_Examples 以下示例将命令的输出发 **action**送到控制台：

```
ciscoasa(config-applet)# output console
```

命令	说明
输出文件附加	将命令输出写入单个文件，但每次都会附加到该 action 文件。
outputfilenew	将命令的输出发 action 送到每个被调用的小程序的新文件。
outputfileoverwrite	将 action 命令输出写入单个文件，每次都会被截断。
outputfilerotate	创建一组轮换的文件。
outputnone	丢弃命令的 action 所有输出。

output file

要将 **action** 命令输出重定向到指定文件，请在事件管理器小程序配置模式下使用 **outputfile** 命令。要删除指定操作，请使用此命令的形式。

output file [**append***filename* | **new** | **overwrite***filename* | **rotaten**]
no output file [**append***filename* | **new** | **overwrite***filename* | **rotaten**]

Syntax Description

append <i>filename</i>	连续将输出附加到指定的文件名，该文件是本地（到 ASA）文件名。
new	创建一个名为 <i>eem-applet-timestamp.log</i> 的新输出文件，其中 <i>applet</i> 是事件管理器小程序的名称， <i>timestamp</i> 是 YYYYMMDD-hhmmss 格式的时间戳。
覆盖文件名	将输出写入指定的文件，但每次调用事件管理器小程序时都会截断输出。
rotaten	创建一个名为 <i>eem-applet-x.log</i> 的输出文件，其中 <i>applet</i> 是事件管理器小程序的名称， <i>x</i> 是文件编号。当要写入新文件时，最旧的文件会被删除，且所有后续文件都会在写入第一个文件之前进行重新编号。最新的文件用 0 表示，最旧的文件用最高数字 (<i>n-1</i>) 表示。 <i>n</i> 参数指定轮换值。有效值范围为 2 到 100。

Command Default

无默认为或值。

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

使用指南

使用 **outputfile** 命令将 **action** 命令输出重定向到指定文件。

CR_Examples

以下示例将输出附加到单个文件：

```
ciscoasa(config-applet)# output file append examplefile1
```

以下示例将 **action** 命令的输出发送到新文件：

```
ciscoasa(config-applet)# output file new
```

以下示例将输出写入单个截断文件：

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

以下示例创建一组轮换的文件：

```
ciscoasa(config-applet)# output file rotate 50
```

Related Commands

命令	说明
outputconsole	将命令的输出发 action 送到控制台。
outputnone	丢弃命令的 action 所有输出。

output none

要放弃 **action** 命令的任何输出，请在事件管理器小程序配置模式下使用 **outputnone** 命令。要保留 **action** 命令的输出，请使用此命令的 **no** 形式。

output none
no output none

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认设置为丢弃来自 **action** 命令的任何输出。

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
事件管理器小程序配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.2(1) 添加了此命令。

使用指南

使用此命令可丢弃来自 **action** 命令的任何输出。

CR_Examples

以下示例丢弃 **action** 命令的任何输出：

```
ciscoasa(config-applet)# output none
```

Related Commands

命令	说明
outputconsole	将命令的输出发 action 送到控制台。
输出文件附加	将命令输出写入单个文件，但每次都会附加到该 action 文件。
outputfilenew	将命令的输出发 action 送到每个被调用的小程序的新文件。
outputfileoverwrite	将 action 命令输出写入单个文件，每次都会被截断。
outputfilerotate	创建一组轮换的文件。

outstanding（已弃用）



注释 支持此命令的最后一个版本是版本 9.5(1)。

要限制未经身份验证的邮件代理会话的数量，请在相应的邮件代理配置模式下使用 **outstanding** 命令。要从配置中删除属性，请使用此 **no** 命令的形式。

```
outstanding { number }
no outstanding
```

Syntax Description *number* 允许的未经身份验证的会话数。范围是从 1 到 1000。

Command Default 默认值为 20。

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
Pop3s	• 是	—	• 是	•	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。
	9.5(2) 此命令已弃用。

使用指南 使用此命令的 **no** 版本可从配置中删除此属性，此配置允许无限数量的未经身份验证的会话。这也会限制邮件端口上的 DOS 攻击。

电子邮件代理连接有三种状态：

- 1. 新的邮件连接进入 “unauthenticated” 状态。
- 2. 当连接出现用户名时，它进入 “正在验证” 状态。
- 3. 当 ASA 对连接进行身份验证时，它会进入 “已验证” 状态。

如果处于未经身份验证状态的连接数超过配置的限制，ASA 将终止最早的未经身份验证的连接，以防止过载。它不会终止经过身份验证的连接。

CR_Examples

以下示例显示如何为 POP3S 邮件代理设置 12 个未经身份验证的会话的限制。

```
ciscoasa
(config)#
  pop3s
ciscoasa(config-pop3s)
#
  outstanding 12
```

override-account-disable (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要覆盖来自 AAA 服务器的帐户禁用指示，请在**override-account-disable**隧道组常规属性配置模式下使用该命令。要禁用覆盖，请使用此命 **no** 令的形式。

override-account-disable
no override-account-disable

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
隧道组常规属性配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.1(1) 添加了此命令。
	9.5(2) 此命令已弃用。

使用指南 此命令适用于返回“account-disabled”指示的服务器，例如使用 NT LDAP 的 RADIUS 和 Kerberos。您可以为 IPsec RA 和 WebVPN 隧道组配置此属性。

CR_Examples 以下示例允许从 AAA 服务器为 WebVPN 隧道组“testgroup”覆盖“account-disabled”指示符：

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

以下示例允许从 AAA 服务器为 IPsec 远程访问隧道组 “QAgrou” 覆盖 “account-disabled” 指示符：

```
ciscoasa(config)# tunnel-group QAgrou type ipsec-ra
ciscoasa(config)# tunnel-group QAgrou general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

Related Commands	命令	说明
	clearconfigretunnel-group	清除隧道组数据库或特定隧道组的配置。
	tunnel-group general-attributes	配置隧道组常规属性值。

override-svc-download

要配置连接配置文件以覆盖下载 AnyConnect 或 SSL VPN 客户端的组策略或用户名属性配置，请在 tunnel-group webvpn attributes 配置模式下使用 **override-svc-download** 命令。要从配置中删除命令，请使用以 **no** 下命令形式：

override-svc-downloadenable
no override-svc-downloadenable

Command Default 默认设置为禁用。ASA 不会覆盖组策略或用户名属性配置来下载客户端。

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

安全设备允许远程用户进行无客户端、AnyConnect 或 SSL VPN 客户端连接，具体取决于是否在组策略或用户名属性中使用命令启用了无客户端和/或 SSL **vpn-tunnel-protocol**VPN。该 **svcask**命令通过提示用户下载客户端或返回 WebVPN 主页来进一步修改客户端用户体验。

但是，您可能希望在特定隧道组下登录的无客户端用户不会遇到等待下载提示过期后才显示无客户端 SSL VPN 主页的延迟。可以使用 **override-svc-download** 命令在连接配置文件级别防止这些用户遇到延迟。此命令使通过连接配置文件登录的用户立即看到无客户端 SSL VPN 主页，无论 **vpn-tunnel-protocol**或 **svcask**命令设置如何。

CR_Examples

在以下示例中，用户进入连接配置文件 *>engineering* 的隧道组 webvpn 属性配置模式，并启用连接配置文件来覆盖客户端下载提示的组策略和用户名属性设置：

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

命令	说明
showwebvpnsvc	显示有关已安装的 SSL VPN 客户端的信息。

命令	说明
svc	为特定组或用户启用或需要 SSL VPN 客户端。
svcimage	指定 ASA 在缓存内存中扩展的客户端包文件，以便下载到远程 PC。

■ **override-svc-download**



pa - pn

- packet-tracer, 第 1137 页
- pager, 第 1179 页
- page style, 第 1181 页
- parameters, 第 1183 页
- participate, 第 1185 页
- passive-interface (ipv6 router ospf), 第 1187 页
- passive-interface (isis), 第 1188 页
- passive-interface (router eigrp), 第 1192 页
- passive-interface (router rip), 第 1194 页
- passwd, 第 1196 页
- password (crypto ca trustpoint), 第 1198 页
- password encryption aes, 第 1200 页
- password-history, 第 1202 页
- password-management, 第 1204 页
- password-parameter, 第 1207 页
- password-policy authenticate enable, 第 1209 页
- password-policy lifetime, 第 1210 页
- password-policy minimum-changes, 第 1211 页
- password-policy minimum-length, 第 1212 页
- password-policy minimum-lowercase, 第 1213 页
- password-policy minimum-numeric, 第 1214 页
- password-policy minimum-special, 第 1215 页
- password-policy minimum-uppercase, 第 1216 页
- password-policy reuse-interval, 第 1217 页
- 密码策略用户名检查, 第 1219 页
- password-storage, 第 1221 页
- peer-group, 第 1222 页
- peer-id-validate, 第 1224 页
- peer ip, 第 1226 页
- perfmon, 第 1228 页

- [periodic](#) , 第 1230 页
- [periodic-authentication certificate](#) , 第 1232 页
- [permit-errors](#) , 第 1233 页
- [permit-response](#) , 第 1234 页
- [pfs](#) , 第 1236 页
- [phone-proxy](#) (已弃用) , 第 1237 页
- [pim](#) , 第 1239 页
- [pim accept-register](#) , 第 1240 页
- [pim bidir-neighbor-filter](#) , 第 1241 页
- [pim bsr-border](#) , 第 1243 页
- [pim bsr-candidate](#) , 第 1245 页
- [pim dr-priority](#) , 第 1247 页
- [pim hello-interval](#) , 第 1248 页
- [pim join-prune-interval](#) , 第 1249 页
- [pim neighbor-filter](#) , 第 1250 页
- [pim old-register-checksum](#) , 第 1251 页
- [pim rp-address](#) , 第 1252 页
- [pim spt-threshold infinity](#) , 第 1254 页
- [ping](#) , 第 1255 页

packet-tracer

可在特权 EXEC 模式下使用 **packet-tracer** 命令，以根据防火墙的当前配置生成 5 到 6 元组数据包。为了清楚起见，数据包跟踪器语法分别针对 ICMP、TCP/UDP/SCTP 和 IP 数据包建模显示。您可以使用 **pcap** 关键字重放多个数据包并跟踪完整的工作流程。

```
packet-tracer input ifc_name [vlan-id vlan_id] icmp [inline-tag tag]
{ src_ip | user username | security-group { name name | tag tag } | fqdn fqdn_string } icmp_value [icmp_code]
[ dmac ] { dst_ip | security-group { name name | tag tag } | fqdn fqdn_string } [detailed] [xml]
```

```
packet-tracer input ifc_name [vlan-id vlan_id] rawip [inline-tag tag]
{ src_ip | user username | security-group { name name | tag tag } | fqdn fqdn_string } 协议 [dmac]
{ dst_ip | security-group { name name | tag tag } | fqdn fqdn_string } [detailed] [xml]
```

```
packet-tracer input ifc_name [vlan-id vlan_id] { tcp | udp | sctp }
[ inline-tag tag ] { src_ip | user username | security-group { name name | tag tag }
| fqdn fqdn_string } src_port [dmac]
{ dst_ip | security-group { name name | tag tag } | fqdn fqdn_string } dst_port [选项] [detailed] [xml]
```

```
packet-tracer
input ifc_name pcap pcap_filename [bypass-checks | decrypted | detailed | persist | transmit | xml | json | force]
```

Syntax Description

bypass-checks	(可选) 绕过针对模拟数据包的安全检查。
decrypted	(可选) 将模拟数据包视为 IPsec/SSL VPN 解密。
detailed	(可选) 提供详细的跟踪结果信息。
<i>dmac</i>	指定目的 MAC 地址。通过显示输出接口选择以及由于未知目标 MAC 地址而导致的丢包，提供交换数据包整个生命周期的全过程。
<i>dst_ip</i>	指定数据包跟踪的目标 IPv4 或 IPv6 地址。
<i>dst_port</i>	指定 TCP/UDP/SCTP 数据包跟踪的目标端口。根据端口，您可能有其他选项，包括 vxlan 和 geneve 内部数据包。
<i>fqdn</i> <i>fqdn_string</i>	指定主机的完全限定域名，该主机可以是源 IP 地址和目标 IP 地址。仅支持 IPv4 的 FQDN。
force	删除现有的 pcap 跟踪并执行新的 pcap 文件。
icmp	指定要使用的协议为 ICMP。
<i>icmp_type</i>	指定 ICMP 数据包跟踪的 ICMP 代码。确保使用 ICMPv6 数据包跟踪器的 V6 类型。
<i>icmp_code</i>	指定与 ICMP 数据包跟踪器的类型对应的 ICMP 代码。确保使用 ICMPv6 数据包跟踪器的 V6 代码。

input <i>ifc_name</i>	指定数据包的入口接口。
inline-tagtag	指定要嵌入第 2 层 CMD 信头中的安全组标记值。有效值范围为 0 - 65533。
json	（可选）以 JSON 格式显示跟踪结果。
pcap	指定 pcap 作为输入。
<i>pcap_filename</i>	包含要跟踪的数据包的 pcap 文件名。
<i>protocol</i>	指定原始 IP 数据包跟踪的协议编号，从 0 到 255。
persist	（可选）启用长期跟踪，并在集群中进行跟踪。
rawip	指定要使用的协议为原始 IP。
sctp	指定要使用的协议为 SCTP。
security-group { <i>name</i> <i>name</i> <i>tagtag</i> }	指定基于用于 Trustsec 的 IP-SGT 查找的源安全组和目标安全组。您可以指定安全组名称或标签编号。
<i>src_port</i>	指定 TCP/UDP/SCTP 数据包跟踪的源端口。
<i>src_ip</i>	指定数据包跟踪的源 IPv4 或 IPv6 地址。
tcp	指定要使用的协议为 TCP。
transmit	（可选）允许从设备传输模拟数据包
<i>type</i>	指定 ICMP 数据包跟踪的 ICMP 代码。
udp	指定要使用的协议为 UDP。
user 用户名	如果要用户指定为源 IP 地址，请以“域\用户”格式指定用户身份。跟踪中使用最近为用户映射的地址（如有）。
vlan-id <i>vlan_id</i>	（可选）指定数据流的 VLAN 身份。值的范围是 1 - 4096。
xml	（可选）以 XML 格式显示跟踪结果。

Command Default

此命令没有默认设置。

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	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
8.4(2)	增加了两个关键字-参数对: <code>user username</code> 和 <code>fqdn fqdn_string</code> 。重命名和重新定义了多个关键字。添加了对 IPv6 源地址的支持。
9.0(1)	增加了对用户身份的支持。仅支持 IPv4 完全限定域名 (FQDN)。
9.3(1)	添加了 inline-tag 标记 关键字-参数对, 以支持嵌入到第 2 层 CMD 报头中的安全组标记值。
9.4(1)	增加了两个关键字参数对: vlan-id <code>vlan_id</code> 和 vxlan-inner <code>vxlan_inner_tag</code> 。
9.5(2)	已添加 <code>sctp</code> 关键字。
9.7(1)	支持透明防火墙模式。引入了用于目标 MAC 地址的新跟踪模块。
9.9(1)	引入了对集群持久跟踪的支持。使用该功能可跟踪集群设备上的数据包。添加了新的选项: <code>persistent</code> 、 <code>bypass-checks</code> 、 <code>decrypted</code> 、 <code>transmit</code> 、 <code>id</code> 和 <code>origin</code> 。
9.14(1)	增强了数据包跟踪器输出, 以提供在路由数据包时允许/丢弃数据包的具体原因。
9.17(1)	增强了 <code>packet-tracer</code> 命令, 以允许 <code>pcap</code> 文件作为跟踪的输入。还添加了对 geneve 的支持。
7.6	启用对象组搜索后, 对象组搜索阶段中会添加更多详细信息。

使用指南

除了使用捕获命令捕获数据包之外, 还可以通过 ASA 跟踪数据包的生命周期, 以查看其是否按预期运行。 `packet-tracer` 命令使您能够执行以下操作:

- 调试生产网络中的所有数据包丢失。
- 验证配置是否达到预期。
- 显示适用于数据包和导致规则添加的 CLI 行的所有规则。
- 显示数据路径中数据包更改时间线。

- 将跟踪数据包注入数据路径。
- 根据用户身份和 FQDN 搜索 IPv4 或 IPv6 地址。
- 跨集群节点调试数据包。

该 **packet-tracer** 命令提供有关数据包以及 ASA 如何处理它们的详细信息。该实用程序的强大之处在于能够通过使用协议和端口信息指定源地址和目标地址来模拟真实世界的流量。 **packet-tracer** 允许防火墙管理员将虚拟数据包注入安全设备并跟踪从入口到出口的流量。在此过程中，将根据流和路由查找、协议检查和 NAT 对数据包进行评估。



- 记住
- 在现有连接上执行数据包跟踪器时，跟踪器不会查阅 ACL。
 - 在集群环境中，必须在入口、出口、asp 和 集群上执行同时数据包捕获。

可选的 **vlan-id** 关键字允许数据包跟踪器进入父接口，父接口稍后会重定向到与 VLAN 身份匹配的子接口。VLAN 身份是仅适用于非子接口的可选条目。管理接口是一个例外，其中父管理专用接口只能有管理专用子接口。

可以进行目的 MAC 地址查找。

在透明防火墙模式下，当输入接口为VTEP时，如果在VLAN中输入一个值，则可以选择性地启用目标MAC地址。而在网桥组成员接口中，目标 MAC 地址为必填字段，但在输入 **vlan-id** 时则为可选字段。

在路由防火墙模式下，当输入接口为桥接组成员接口时，**vlan-id** 关键字和 **dmac** 参数是可选的。

下表提供了分别在透明和路由防火墙模式下有关 VLAN 身份和目标 MAC 地址的接口相关行为的完整信息。

Transparentfirewallmode:

接口	VLAN	目标 MAC 地址
管理	已启用（可选）	禁用
VTEP	已启用（可选）	已禁用。当用户在 VLAN 中输入值时，系统将启用目的 MAC 地址，但该地址是可选的。
网桥虚拟接口(BVI)	已启用（可选）	已启用（强制）。当用户在 VLAN 中输入值时，目的 MAC 地址为可选。

Routedfirewallmode:

接口	VLAN	目标 MAC 地址
管理	已启用（可选）	禁用

接口	VLAN	目标 MAC 地址
路由接口	已启用（可选）	禁用
桥接组成员	已启用（可选）	已启用（可选）

当您使用输入入口接口运行 **packet-tracer** 命令时，如果数据包未被丢弃，则数据包会经历不同的阶段，例如 UN-NAT、ACL、NAT、IP-OPTIONS 和 FLOW-CREATION。系统将显示生成的消息：“ALLOW”。

在防火墙配置可能导致实时流量被丢弃的情况下，模拟的跟踪器数据包也将被丢弃。在某些情况下，将会提供特定丢弃原因。例如，如果由于无效的标头验证而丢弃数据包，则会出现以下消息：“由于错误的 IP 标头（原因）而丢弃数据包。”如果目标 MAC 地址未知，则交换顺序中的数据包会被丢弃。它启动 ASA 以搜索目标 MAC 地址。如果找到目标 MAC 地址，则可以再次执行 **packet-tracer**，并且 L2 查找成功。

通过 **packet-tracer** 中的 VXLAN 和 Geneve 支持，您可以指定内部数据包第 2 层源和目标 MAC 地址、第 3 层源和目标 IP 地址、第 4 层协议、第 4 层源和目标端口号以及虚拟网络接口 (VNI)。号码。内部数据包仅支持 TCP、SCTP、UDP、原始 IP 和 ICMP。

您可以使用域/用户格式为源指定用户身份。ASA 搜索用户的 IP 地址并将其用于数据包跟踪测试。如果用户映射到多个 IP 地址，则使用最新的登录 IP 地址，并且输出显示存在更多 IP 地址-用户映射。如果在此命令的源部分指定了用户身份，则 ASA 将根据用户输入的目标地址类型搜索用户的 IPv4 或 IPv6 地址。

您可以指定安全组名称或安全组标记作为源。ASA 会根据安全组名称或安全组标记搜索 IP 地址，并在数据包跟踪测试中使用该地址。如果安全组标记或安全组名称映射到多个 IP 地址，则使用其中一个 IP 地址，输出显示存在更多 IP 地址到安全组标记映射。

您还可以将 FQDN 指定为源地址和目标地址。ASA 先执行 DNS 查找，然后为数据包构建检索第一个返回的 IP 地址。

对于第 3 层到桥接虚拟接口以及桥接虚拟接口到桥接虚拟接口等流量场景（其中目标 IP 是通过 ASA 上的 BVI 接口进行的下一跳），数据包跟踪器会执行双重 ROUTE-LOOKUP。此外，也不会创建流。

在清除 ARP 和 MAC 地址表条目的情况下，数据包跟踪器始终执行两次 ROUTE-LOOKUP，然后解析目标 MAC 地址并将其存储在数据库中。而对于任何其他流量场景则不是这种情况。如果目标 MAC 地址为 L3 接口，则永远不会解析该地址并将其存储在数据库中。由于 BVI 接口是使用 *nameif* 进行配置并具有 L3 属性，因此不应执行 DMAC 查找。

此行为仅在第一次尝试、没有 MAC 地址和 ARP 条目时出现。显示 DMAC 的条目后，数据包跟踪器输出将符合预期。系统将创建流。

通过持久跟踪，可以跟踪在集群设备之间传递的数据包。必须使用 **persist** 选项注入您想要跨集群单元跟踪的数据包。每个数据包的持久跟踪配备数据包 id 和跳数，可以通过集群节点确定注入的数据包来源和数据包跳数阶段。**packet-id** 是下列各项的组合<node name of the device where the packet originated>和一个递增编号。对于在节点上首次接收的每个新数据包，数据包 ID 是唯一的。每当数据包从一个集群成员移动到另一个集群成员时，都会填充跳数计数。例如，集群中的数据包根据外部负载均衡编号列表到达成员。Host-1 向 Host-2 发送数据包。注入的数据包在发送到 Host-2 之前，

会在集群节点之间重定向。元数据输出分别显示 Tracer origin-id B:7 hop 0、Tracer origin-id B:7 hop 1 和 Tracer origin-id B:7 hop 2。其中 B 是数据包源自的集群节点的名称。7 是递增的数字，表示这是源自此集群节点的第 7 个数据包。此数字随着从此节点发出的每个新数据包而增加。“B”和“7”一起构成用于标识数据包的唯一 id。集群设备本地名称对于通过此设备传递的每个数据包都是相同的。当全局缓冲区使用 unique-id 和跳数时，可区分每个数据包。跟踪数据包后，每个节点上将提供持久跟踪，直到您手动丢弃它们以释放一些内存。情景中已启用的持久跟踪存储在每个情景的缓冲区中。将来源所有者 ID（两个值<origin-owner><id>），以便在跟踪集中查找跟踪。

可以允许模拟数据包离开 ASA。通过 packet-tracer 使用传输选项，可以在网络上传输数据包。默认情况下，数据包跟踪器会在传输数据包之前丢弃该数据包。传出数据包后，会在流表中生成流。

通过 packet-tracer 使用 bypass-checks 选项，可以绕过 ACL、VPN 过滤器、uRPF 和 IPsec 欺骗检查。它同时适用于入口和出口条件，并且不会丢弃模拟的 IPsec 数据包。

可以将已解密的数据包注入 VPN 隧道，这是通用的，适用于 IPsec 和 TLS。还可以模拟通过 VPN 隧道的数据包。模拟的“已解密”数据包将与现有的 VPN 隧道进行匹配，并应用关联的隧道策略。但是，此功能不适用于基于路由的 VPN 隧道。

packet-tracer 注入和跟踪单个数据包时，使用 **pcap** 关键字可使数据包跟踪器重放多个数据包（最多 100 个数据包）并跟踪整个数据流。您可以提供 pcap 文件作为输入，并以 XML 或 JSON 格式获取结果以进行进一步分析。要清除跟踪输出，请使用 **clear packet-tracer** 的 **pcap trace** 子命令。在跟踪过程中，您无法使用跟踪输出。

当您重放包含 Dot1q 标记数据包的 **pcap** 时，请确保数据包包含在防火墙上配置的传输子接口的标签。

以下示例显示当前行为：

```
----- INSIDE (VLAN 100) FTD (VLAN 200) OUTSIDE -----
```

如果在 INSIDE 子接口上注入 TCP SYN 数据包，则该数据包的 Dot1q 标记必须为 VLAN 100。同样，返回流量（例如，TCP SYN/ACK）的 Dot1q 标记中必须包含 VLAN 200。



注释 如果重放 INSIDE 接口上的捕获，并且所有数据包的 Dot1q 标签中都有 VLAN 100，则重放将失败（SYN/ACK 也将注入 INSIDE 子接口）。

以下示例显示如何使用 pcap 文件作为输入运行 packet-tracer：

```
ciscoasa# packet-tracer input inside pcap http_get.pcap detailed xml
```

以下示例显示如何通过清除现有的 pcap 跟踪缓冲区并提供 pcap 文件作为输入来运行 packet-tracer：

```
ciscoasa# packet-tracer input inside pcap http_get.pcap force
```

CR_Examples

以下示例跟踪来自内部接口的 ICMP 数据包。结果表明，由于反向路径验证失败（RPF），数据包被丢弃。失败的原因可能是流量从路由表已知但与内部接口关联的地址进入外部接

口。同样，如果流量从未知源地址进入内部接口，则设备会丢弃数据包，因为匹配的路由（默认路由）指示外部接口。

```
ciscoasa# packet-tracer input inside icmp 10.15.200.2 8 0$

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
  Forward Flow based lookup yields rule:
    in  id=0xd793b4a0, priority=12, domain=capture, deny=false
        hits=621531641, user_data=0xd7bbe720, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
  Forward Flow based lookup yields rule:
    in  id=0xd7dc31d8, priority=1, domain=permit, deny=false
        hits=23451445222, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in    10.15.216.0      255.255.252.0      inside

Phase: 4
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in    0.0.0.0          0.0.0.0            outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (rpf-violated) Reverse-path verify failed
```

以下示例跟踪从 201.1.1.1 到 202.1.1.1 的 HTTP 端口的 TCP 数据包。

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Result:
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```

```

ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC Address Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC address lookup resulted in egress ifc outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbe83542f0, priority=1, domain=permit, deny=false
hits=7313, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbd94026a0, priority=12, domain=permit, deny=false
hits=8, user_data=0x7fdbf07cbd00, cs_id=0x0, use_real_addr,
flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=10, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fdbe8363790, priority=0, domain=inspect-ip-options, deny=true
hits=212, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any
Phase: 6
Type: NAT
Subtype: per-session

```

```

Result: ALLOW
Config:
Additional Information:

Reverse Flow based lookup yields rule:
in id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=12, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fdbd93dfc10, priority=0, domain=inspect-ip-options, deny=true
hits=110, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 221, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
44# command example
ciscoasa(config)# command example
resulting screen display here
<Text omitted.>

```

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```

ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW

```

```

Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule

```

以下示例显示如何使用用户名 CISCOabc 跟踪从内部主机 10.0.0.2 到外部主机 20.0.0.2 的数据包:

```

ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2
Source: CISCO\abc 10.0.0.2
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

```

以下示例显示如何跟踪来自用户名为 CISCO\abc 的内部主机 20.0.0.2 的数据包, 并以 XML 格式显示跟踪结果:

```

<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>
<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>

```

以下示例显示如何跟踪从内部主机 xyz.example.com 到外部主机 abc.example.com 的数据包。

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)
Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

以下示例显示该命令的 **packet-tracer** 输出，以显示安全组标签映射到 IP 地址：

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.0 outside....
-----More-----
```

以下示例显示 **packet-tracer** 命令的输出，显示第 2 层 SGT 实施：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

以下示例概述 VXLAN 对 UDP/TCP 和 ICMP 内部数据包的支持

```
packet-tracer in inside udp 30.0.0.2 12345 30.0.0.100 vxlan vxlan-inner 1234 1.1.1.1 11111
2.2.2.2 22222 aaaa.bbbb.cccc aaaa.bbbb.dddd detailedOuter packet: UDP from 30.0.0.2 to
30.0.0.100 (vtep/nve source-interface IP) with default vxlan destination port.
Inner packet: VXLAN in-tag 1234, UDP from 1.1.1.1/11111 to 2.2.2.2/22222 with smac
aaaa.bbbb.cccc and dmac aaaa.bbbb.dddd
```

以下示例显示在集群设备之间传递持久跟踪时的输出：

```
ciscoasa# cluster exec show packet-tracer
B(LOCAL):*****
tracer 10/8 (allocate/freed), handle 10/8 (allocated/freed), error 0
===== Tracer origin-id B:7, hop 0 =====
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 5
Type: CLUSTER-EVENT
```

```

Subtype: forward
Result: ALLOW
Config:
Additional Information:
To A(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
===== Tracer origin-id B:7, hop 2 =====
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From A(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-4: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) have been elected owner by (0).
<Snipping phase 6-16: ACCESS-LIST, NAT, IP-OPTIONS, INSPECT, INSPECT, FLOW-CREATION,
ACCESS-LIST, NAT, IP-OPTIONS, ROUTE-LOOKUP, ADJACENCY-LOOKUP>
A:*****
tracer 6/5 (allocate/freed), handle 6/5 (allocated/freed), error 0
===== Tracer origin-id B:7, hop 1 =====
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From B(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-7: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP, ACCESS-LIST, NAT, IP-OPTIONS>
Phase: 8
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (0) am director, not creating dir flow for ICMP pkt recvd by (1).
Phase: 9
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To B(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
ciscoasa#

```

以下示例显示使用 **origin** 和 **id** 选项从集群节点跟踪数据包时的输出:

```

cluster2-asa5585a# cluster exec show packet-tracer | i origin-id
b(LOCAL):*****
===== Tracer origin-id b:2, hop 0 =====
===== Tracer origin-id b:2, hop 2 =====
a:*****

```



```

===== Tracer origin-id a:17, hop 0 =====
===== Tracer origin-id b:2, hop 1 =====
===== Tracer origin-id b:2, hop 3 =====
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer ori
cluster2-asa5585a# cluster exec show packet-tracer origin b id 2
b(LOCAL):*****
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
===== Tracer origin-id b:2, hop 0 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 4
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
===== Tracer origin-id b:2, hop 2 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From a(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

```

```

MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW

```

```

Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: FULL
I (1) am redirecting to (0) due to matching action (1).
Phase: 15
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
a:*****
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
===== Tracer origin-id b:2, hop 1 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:

```

```

Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am director, found static rule to classify owner as (253).
Phase: 7
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To b(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
===== Tracer origin-id b:2, hop 3 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule

```

```
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
```

```

Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 70, packet dispatched to next module
Phase: 19
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc identity
Phase: 20
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface outside
adjacency Active
mac address 0000.0000.0000 hits 1730 reference 6
Phase: 21
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc inside is not same as existing ifc outside
Doing adjacency lookup lookup on existing ifc outside2
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer origin a
b(LOCAL):*****
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:*****
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
===== Tracer origin-id a:17, hop 0 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity

```

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
```

```

Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer id 17
b(LOCAL):*****
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:*****
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
===== Tracer origin-id a:17, hop 0 =====
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP

```



```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
```

```

Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 0.0.0.0 using egress ifc identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#

```

以下示例概述了如何从集群节点中清除持久跟踪:

```
ciscoasa# cluster exec clear packet-tracer
```

要在 IPsec 隧道中注入解密的数据包，需要满足一些条件。如果未协商 IPsec 隧道，系统会显示错误消息。第二次协商 IPsec 隧道后，数据包通过。

以下示例说明何时 **not** 协商 IPsec 隧道以注入解密数据包：

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
decrypted
*****
WARNING: An existing decryption SA was not found. Please confirm the
IPsec Phase 2 SA or Anyconnect Tunnel is established.
*****
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
```

```

Additional Information:
Phase: 8
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect ftp
service-policy global_policy global
Additional Information:
Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: DROP
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
cluster2-asa5585a(config)#

```

以下示例说明何时协商 IPSec 隧道以注入解密数据包:

```

cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 decrypted
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global

```

```
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
```

```

Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW

```

```

Config:
Implicit Rule
Additional Information:
Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module
Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow

```

以下示例使用传输 选项来允许模拟的数据包传出并在传出接口上捕获模拟的数据包:

```

cluster2-asa5585a(config)# packet-tracer input outside icmp 211.1.1.10 8 0 213.1.1.10
transmit
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface

```

```

Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

```



```

Phase: 13
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6449, packet dispatched to next module
Phase: 15
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 16
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 19
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 15 reference 1
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
cluster2-asa5585a(config)#

```

以下示例概述在传出接口上捕获的 ICMP 数据包：

```

cluster2-asa5585a(config)# cluster exec show capture test | i icmp
a(LOCAL):*****
14: 02:18:16.717736      802.1Q vlan#212 P0 211.1.1.10 > 213.1.1.10: icmp: echo request

```

```
cluster2-asa5585a(config)#
```

数据包跟踪器的绕行检查选项的示例将通过所列的以下阶段进行概述。下面为每种情况提供了具体示例：

- 分支和集线器之间未创建 IPSec 隧道。
- 两个设备之间的 IPSec 隧道必须协商，并且初始数据包触发隧道建立。
- IPSec 协商完成，隧道启动。
- 隧道启动后，注入的数据包将通过隧道发送。将绕过或跳过与数据包路径一起提供的安全检查（ACL、VPN 过滤等）。

未创建 IPSec 隧道：

```
cluster2-asa5585a(config)# sh crypto ipsec sa
There are no ipsec sas
cluster2-asa5585a(config)#
```

隧道协商过程开始：

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc outside2

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: encrypt
```

```

Result: DROP
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
cluster2-asa5585a(config)#

```

协商 IPsec 隧道并且隧道启动后:

```

cluster2-asa5585a#
cluster2-asa5585a(config)# sh crypto ipsec sa
interface: outside2
  Crypto map tag: crypto-map-peer4, seq num: 1, local addr: 214.1.1.10
    access-list toPeer4 extended permit ip host 211.1.1.1 host 213.1.1.2
    local ident (addr/mask/prot/port): (211.1.1.1/255.255.255.0/0)
    remote ident (addr/mask/prot/port): (213.1.1.2/255.255.255.0/0)
    current_peer: 214.1.1.9
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 214.1.1.10/500, remote crypto endpt.: 214.1.1.9/500
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: A642726D
    current inbound spi : CF1E8F90

  inbound esp sas:
    spi: 0xCF1E8F90 (3474886544)
      SA State: active
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings = {L2L, Tunnel, IKEv2, }
      slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
      sa timing: remaining key lifetime (kB/sec): (4285440/28744)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
        0x00000000 0x00000001

  outbound esp sas:
    spi: 0xA642726D (2789372525)
      SA State: active
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings = {L2L, Tunnel, IKEv2, }
      slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
      sa timing: remaining key lifetime (kB/sec): (4239360/28744)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
        0x00000000 0x00000001
cluster2-asa5585a(config)#

```

隧道启动后，允许数据包通过，并且由于应用了bypass-checks选项，因此会跳过安全检查：

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 bypass-checks
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
```

```

Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

```

```
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module
Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
```

```

Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow

```

以下示例跟踪具有下一跳 ARP 条目的直连主机中的 TCP 数据包。

```
ciscoasa# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80 detailed
```

```

Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0

```



```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
```

```

Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow

```

以下示例跟踪由于缺少有效的下一跳 ARP 条目而被丢弃的 TCP 数据包。请注意，丢弃原因提供了检查 ARP 表的提示。

```

<Displays same phases as in the previous example till Phase 8>
Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has entry
for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA

```

以下示例描述了使用 NAT 和可访问的下一跳进行次优路由的数据包跟踪器。

```

ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
ciscoasa# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log

```

```
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ae2a89delb0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
```

```

dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snf_fp_inspect_ip_options
snf_fp_tcp_normalizer
snf_fp_translate
snf_fp_adjacency
snf_fp_fragment
snf_fp_tracer_drop
snf_ifc_stat

Module information for reverse flow ...
snf_fp_inspect_ip_options
snf_fp_translate
snf_fp_tcp_normalizer
snf_fp_adjacency
snf_fp_fragment
snf_fp_tracer_drop
snf_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop

```

```

Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
The following example depicts packet tracer for sub-optimal routing with NAT, where, the
packet is dropped due to non-reachable nexthop.
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24

<Displays same phases as in the previous example till Phase 11>
Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA

启用对象组搜索时，跟踪包括对象查找步骤。从 9.22(1) 开始，这些信息包括源对象表和目
标对象表中的查找总数、总体查找计数以及对象查找阶段所花费的总时间。以下是对对象组搜
索信息的示例。

Phase: 2

```

```
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 47005 ns
Config:
Additional Information:
Source object-group match count:      2
Source NSG match count:               0
Destination NSG match count:         0
Classify table lookup count:          4
Total lookup count:                   3
Duplicate key pair count:             0
Classify table match count:           3
```

Related Commands

命令	说明
capture	捕获数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕获配置。
show packet-tracer	显示最近在PCAP文件上运行的数据包跟踪器的跟踪缓冲区输出。

pager

要设置在 Telnet 会话出现 “ ---More--- ” 提示符之前页面上显示的默认行数，请在全局配置模式下使用 **pager** 命令。

pager [**lines**] *lines*

Syntax Description	[<i>lines</i>] <i>lines</i> 设置在出现 “ ---更多--- ” 提示之前页面上的行数。默认值为 24 行； 0 表示无页面限制。范围是 0 到 2147483647 行。 lines 关键字是可选的，并且无论有或没有该关键字，命令的功能都是相同的。

Command Default	默认值为 24 行。

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	• 支持

Command History	版本 修改
	7.0(1) 此命令已从特权 EXEC 模式命令更改为全局配置模式命令。 terminalpager 命令被添加为特权 EXEC 模式命令。

使用指南	此命令更改 Telnet 会话的默认寻呼线路设置。如果只想暂时更改当前会话的设置，请使用 terminalpager 命令。

如果您通过 Telnet 进入管理上下文，则当您切换到其他上下文时，寻呼机线路设置将跟随您的 **pager** 会话，即使给定上下文中的命令具有不同的设置。要更改当前分页器设置，请输入带有新设置的 **terminalpager** 命令，也可以在当前上下文中输入该 **pager** 命令。除了将新的寻呼机设置保存到上下文配置之外，该 **pager** 命令还将新设置应用于当前 Telnet 会话。

CR_Examples	以下示例将显示的行数更改为 20:

```
ciscoasa(config)# pager 20
```

Related Commands	命令	说明
	clear configure terminal	清除终端显示宽度设置。

命令	说明
show running-config terminal	显示当前终端设置。
terminal	允许系统日志消息显示在 Telnet 会话中。
terminal pager	设置在 “---more---” 提示之前在 Telnet 会话中显示的行数。此命令不会保存到配置中。
terminal width	在全局配置模式中设置终端显示宽度。

page style

要定制 WebVPN 用户连接到安全设备时显示的 WebVPN 页面，请在 webvpn 定制配置模式下使用该 **pagestyle** 命令。要从配置中删除命令并导致值被继承，请使用此命令的 **no** 形式。

page style 值
[no] **page style** *value*

Syntax Description *value* 级联样式表 (CSS) 参数（最多 256 个字符）。

Command Default 默认页面样式为 background-colour:white;font-family:Arial,Helv,sans-serif

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 自定义配置	• 是	—	• 是	—	—

Command History 版本 修改

7.1(1) 添加了此命令。

使用指南

该 **style** 选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

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



注释

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

CR_Examples

以下示例将页面样式自定义为large:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

Related Commands

命令	说明
logo	定制 WebVPN 页面上的徽标。
title	自定义 WebVPN 页面的标题

parameters

要进入参数配置模式以为检测策略映射设置参数，请在策略映射配置模式下使用 **parameters** 命令。

parameters

Syntax Description

此命令没有任何参数或关键字。

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
策略映射配置	• 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

通过模块化策略框架，您可以为许多应用检测配置特殊操作。当您使用第 3/4 层策略映射中的 **inspect** 命令（**policy-map** 命令）启用检测引擎时，您还可以选择启用 **policy-map type inspect** 命令创建的检测策略映射中定义的操作。例如，输入 **inspect dns dns_policy_map** 命令，其中 **dns_policy_map** 是检测策略映射的名称。

检测策略映射可能支持一个或多个 **parameters** 命令。参数影响检查引擎的行为。参数配置模式下可用的命令取决于应用。

CR_Examples

以下示例显示如何在默认检测策略映射中设置 DNS 数据包的最大消息长度：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

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

participate

要强制设备加入虚拟负载均衡集群，请在 VPN 负载均衡配置模式下使用 **participate** 命令。要取消设备对集群的参与，请使用此命令的 **no** 形式。

participate
no participate

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认行为是，设备不加入 VPN 负载均衡集群。

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 负载平衡配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 添加了此命令。

使用指南

您必须先使用 **interface** 和 **nameif** 命令配置接口，然后使用 **vpnload-balancing** 命令进入 VPN 负载均衡模式。您还必须先前使用该命令配置集群 IP 地址 **clusterip**，并配置虚拟集群 IP 地址所引用的接口。

此命令会强制此设备加入虚拟负载均衡集群。必须显式发出此命令启用设备的参与。

参与集群的所有设备必须共享相同的集群特定值：IP 地址、加密设置、加密密钥和端口。



注释 使用加密时，您必须事先配置命令 **isakmpenableinside**，其中 *inside* 指定负载均衡内部接口。如果未在负载均衡内部接口上启用 **isakmp**，您会在尝试配置集群加密时收到错误消息。如果 **isakmp** 在配置 **clusterencryption** 命令时已启用，但在配置 **participate** 命令之前已被禁用，则您 **participate** 会出现错误消息，并且本地设备不会加入集群。

CR_Examples

以下是一个 VPN 负载均衡命令序列示例，其中包含使当前设备能够加入 VPN 负载均衡集群的 **participate** 命令：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

命令	说明
vpnload-balancing	进入 VPN 负载均衡模式。

passive-interface (ipv6 router ospf)

要抑制在接口上或使用 OSPFv3 进程的所有接口上发送和接收路由更新，请在 ipv6 router ospf 配置模式下使用 **passive-interface** 命令。要在接口上或在使用 OSPFv3 进程的所有接口上重新启用路由更新，请使用此命令的 **no** 形式。

passive-interface [*interface_name*]
no passive-interface [*interface_name*]

Syntax Description

interface_name （可选）指定运行 OSPFv3 进程的接口名称。

Command Default

无默认为行为或值。

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
Ipv6 路由器 ospf 配置	• 是	—	• 是	—	—

Command History

版本 修改

9.0(1) 添加了此命令。

使用指南

此命令可在接口上启用被动路由。

CR_Examples

以下示例抑制内部接口上路由更新的发送和接收。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

Related Commands

命令	说明
showrunning-configrouter	显示运行配置中的路由器配置命令。

passive-interface (isis)

要选择接口上的 ISIS hello 数据包和路由更新，同时仍将接口地址包含在拓扑数据库中，请在 **passive-interface** 路由器 isis 配置模式下使用该命令。要重新启用传出呼叫数据包和路由更新，请使用此命令的 **no** 形式。

```
passive-interface [ default | inside | management | management2 ]
no passive-interface [ default | inside | management | management2 ]
```

Syntax Description	default	抑制所有接口上的路由更新。
	inside	接口 GigabithEthernet0/0 的名称。
	management	接口 Management0/0 的名称。
	management2	接口 Management0/1 的名称。

Command Default 默认设置是抑制所有接口上的路由更新。

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 此命令可在接口上启用被动路由。

CR_Examples 以下示例抑制内部接口上路由更新的发送和接收。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# passive-interface inside
```

Related Commands	命令	说明
	advertisepassive-only	配置 ASA 以通告被动接口。

命令	说明
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定 IS-IS 实例全局使用的 IS-IS 报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。

命令	说明
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新闻隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的 NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。

命令	说明
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

passive-interface (router eigrp)

要禁用接口上 EIGRP 路由更新的发送和接收，请在 **passive-interface** 路由器 eigrp 配置模式下使用该命令。要重新启用接口上的路由更新，请使用此命令的 **no** 形式。

```
passive-interface { default | if_name }
no passive-interface { default | if_name }
```

Syntax Description	default （可选）将所有接口设置为被动模式。
	if_name （可选）由 nameif 命令指定的接口名称，用于禁用路由更新。

Command Default 当为该接口启用路由时，所有接口都针对活动路由启用（发送和接收路由更新）。

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	—	—

Command History	版本 修改
	7.2(1) 添加了此命令。
	8.0(2) 添加了对 EIGRP 路由的支持。
	9.20(1) 增加了对 EIGRP IPv6 路由的支持。

使用指南 在接口上启用被动路由。对于 EIGRP，这会禁用该接口上路由更新的传输和接收。

您可以在 EIGRP 配置中使用多个 **passive-interface** 命令。您可以使用 **passive-interfacedefault** 命令在所有接口上禁用 EIGRP 路由，然后使用 **nopassive-interface** 命令在特定接口上启用 EIGRP 路由。

CR_Examples 以下示例将外部接口设置为被动 EIGRP。安全设备上的其他接口会发送和接收 EIGRP 更新。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

以下示例将除内部接口之外的所有接口设置为被动 EIGRP。只有内部接口会发送和接收 EIGRP 更新。

```
ciscoasa(config)# router eigrp 100  
ciscoasa(config-router)# network 10.0.0.0  
ciscoasa(config-router)# passive-interface default  
ciscoasa(config-router)# no passive-interface inside
```

Related Commands

命令	说明
showrunning-configrouter	显示运行配置中的路由器配置命令。

passive-interface (router rip)

要禁用接口上的 RIP 路由更新传输，请在 **passive-interface** 路由器 RIP 配置模式下使用该命令。要在接口上重新启用 RIP 路由更新，请使用此命令的 **no** 形式。

```
passive-interface { default | if_name }
no passive-interface { default | if_name }
```

Syntax Description	default （可选）将所有接口设置为被动模式。
	if_name （可选）将指定接口设置为被动模式。

Command Default	如果启用了 RIP，系统会为活动 RIP 启用所有接口。
	如果未指定接口或 default 关键字，则命令默认为 default ，并在配置中显示为 passive-interface default 。

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。
	9.0(1) 增加了多情景模式支持。

使用指南	在接口上启用被动 RIP。该接口侦听 RIP 路由广播并使用该信息填充路由表，但不会广播路由更新。

CR_Examples	以下示例将外部接口设置为被动 RIP。安全设备上的其他接口会发送和接收 RIP 更新。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

Related Commands	命令	说明
	clearconfigurerip	从运行配置中清除所有 RIP 命令。
	routerrip	启用 RIP 路由进程并进入 RIP 路由器配置模式。

命令	说明
showrunning-configrip	显示运行配置中的 RIP 命令。

passwd

要设置Telnet的登录密码，请在**passwd** 全局配置模式下使用该命令。要重置密码，请使用此命 **no** 令的形式。

passwd*password* [**encrypted**]
no passwd密码

Syntax Description

encrypted （可选）指定密码为加密形式。密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。如果由于某种原因您需要将密码复制到另一个 ASA 但不知道原始密码，则可以输入带 **passwd**有加密密码和此关键字的命令。通常，只有在输入命令时才会看到这个关 **showrunning-configpasswd**键字。

password 将密码设置为最多 80 个字符的字符串，区分大小写。密码不得包含空格。

Command Default

9.1(1): 默认密码是 “cisco” 。

9.1(2): 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	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.3(1)	删除了别名 password 命令；仅支持 passwd 。
8.4(2)	SSH 默认用户名不再受支持；您无法再使用带有 pix 或 asa 用户名和登录密码的 SSH 连接到 ASA。
9.0(2)、 9.1(2)	默认密码 “cisco” 已被删除；您必须主动设置登录密码。使用 nopasswd 或 clearconfigurepasswd 命令可删除密码；默认情况下）。从前 会将其重置为默认值 “cisco” 。

使用指南

当您使用 **telnet** 命令启用 Telnet 时，您可以使用 **passwd** 命令设置的密码登录。输入登录密码后，您将处于用户 EXEC 模式。如果使用 **aaaauthenticationtelnetconsole** 命令为 Telnet 配置每用户 CLI 身份验证，则不会使用此密码。

此密码也用于从交换机到 ASASM 的 Telnet 会话（参见命 **session** 令）。

CR_Examples

以下示例将密码设置为 Pa\$\$w0rd:

```
ciscoasa(config)# passwd Pa$$w0rd
```

以下示例将 password 设置为您从另一个 ASA 复制的加密密码:

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

命令	说明
clearconfigurepasswd	清除登录密码。
enable	进入特权 EXEC 模式。
enablepassword	设置启用密码。
showcurpriv	显示当前登录的用户名和用户权限级别。
showrunning-configpasswd	以加密形式显示登录密码。

password (crypto ca trustpoint)

要指定在注册期间向 CA 注册的质询短语，请在 crypto ca trustpoint 配置模式下使用 **password** 命令。
要恢复默认设置，请使用此命令 **no** 的形式。

password字符串
no password字符串

Syntax Description *string* 将密码的名称指定为字符串。第一个字符不能为数字。该字符串可以包含任何字母数字字符（包括空格），最多 80 个字符。您不能以数字-空格-任何格式指定密码。数字后有空格会导致问题。例如，“hello 21”是合法密码，但“21 hello”不是。密码检查区分大小写。例如，密码“Secret”与密码“secret”不同。

Command Default 默认设置为不包含密码。

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 trustpoint 配置	• 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 此命令允许您在实际证书注册开始之前指定证书的吊销密码。当 ASA 将更新的配置写入 NVRAM 时，指定的密码将被加密。
CA 通常使用质询短语来验证后续的撤销请求。
如果启用此命令，则在证书注册期间系统不会提示您输入密码。

CR_Examples

以下示例进入 trustpoint Central 的 crypto CA trustpoint 配置模式，并且在 trustpoint Central 的注册请求中包含向 CA 注册的质询短语：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

Related Commands

命令	说明
cryptocatrustpoint	进入 trustpoint 配置模式。
defaultenrollment	将注册参数还原为其默认值。

password encryption aes

要使用主密码启用密码加密，请在全局配置模式下使用 **passwordencryptionaes** 命令。要禁用密码加密，请使用此命令 **no** 的形式。

password encryption aes
no password encryption aes

Syntax Description 此命令没有任何参数或关键字。

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	—	• 是

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

您必须以任意顺序输入 **keyconfig-keypassword-encrypt** 命令和 **passwordencryptionaes**命令才能触发密码加密。输入 **writememory**，以将加密密码保存到启动配置。否则，启动配置中的密码可能仍然可见。在多情景模式下，请在系统执行空间中使用 **writememoryall** 保存所有情景配置。如果您稍后使用该命令禁用密码加密，则所有现有的 **nopasswordencryptionaes**加密密码都将保持不变，并且只要主密码存在，就会根据应用程序的要求解密加密密码。

此命令仅在安全会话中被接受，例如通过控制台、SSH 或通过 HTTPS 的 ASDM。

在主用/备用故障转移中启用或 **writestandby**更改密码加密会导致将主用配置复制到备用单元。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主动/主动故障转移，您必须手动输入。 **writestandby A** 可 **writestandby**能会导致主动/主动模式下的流量中断，因为在同步新配置之前，辅助设备上的配置已被清除。您应该使用 **failoveractivegroup1** 和 **failoveractivegroup2** 命令使主 ASA 上的所有上下文处于活动状态 **writestandby**，输入，然后使用命令将第 2 组上下文恢复到辅助单 **nofailoveractivegroup2**元。

write擦除命令（后跟**reload**命令）将删除主密码和所有配置（如果其丢失）。

CR_Examples

以下示例设置用于生成加密密钥的密码，并启用密码加密：

```
ciscoasa
(config)#
  key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

命令	说明
keyconfig-keypassword-encryption	设置用于生成加密密钥的密码。
write erase	如果主密码在其后跟 reload 命令时丢失，则将其删除。

password-history

当您启用 **password-policyreuse-interval** 命令且用户不可配置时，此命令出现在 **usernameattributes** 命令的配置中。它以加密形式存储以前的密码。

password-history 散列 1,散列 2,散列 3...

Syntax Description	散列 1,散列 2,散列 3... 显示已使用 PBKDF2（基于密码的密钥派生功能 2）进行散列处理的先前密码。

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
	用户名属性配置	• 是	• 支持	• 支持	—

Command History	版本 修改
	9.8(1) 我们引入了此命令。

使用指南	此命令不可由用户配置，并且仅在启用 password-policyreuse-interval 命令时才会显示在 show 输出中。

CR_Examples	以下示例将密码更改两次，然后显示以前的散列密码：

```
ciscoasa(config)# username test password pw1
ciscoasa(config)# show running-config username test
username test password $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbilks6eo381KmlqOiwqnQ== pbkdf2
ciscoasa(config)# username test password pw2
ciscoasa(config)# show running-config username test
username test password $sha512$5000$d8ebNCK2oTyZSiHjSh2T6w==$surDQ/+9sOPwi4IUftWFMcw== pbkdf2
username test attributes
    password-history $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbilks6eo381KmlqOiwqnQ==
ciscoasa(config)# password test pw3
ciscoasa(config)# show running-config username test
username test password $sha512$5000$o8WLalqnLdp2Js4OlW+NdQ==$4Be4eHtPmOxdpfH6j+F4qQ== pbkdf2
username test attributes
    password-history
$sha512$5000$d8ebNCK2oTyZSiHjSh2T6w==$surDQ/+9sOPwi4IUftWFMcw=, $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbilks6eo381KmlqOiwqnQ=
ciscoasa(config)#
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 username 登录历史。
password-history	存储以前的 username 密码。用户无法配置此命令。
password-policyreuse-interval	禁止重复使用 username 密码。
password-policyusername-check	禁止使用与 username 名称匹配的密码。
showaaalogin-history	显示本地 username 登录历史记录。
username	配置本地用户。

password-management

要启用密码管理，请在 tunnel-group general-attributes 配置模式下使用password-management 命令。要禁用密码管理，请使用此命令 **no** 的形式。要将天数重置为默认值，请使用命令的 **no** 形式并指定 password-expire-in-days 关键字。

```
password-management [password-expire-in-days天]
npassword-management
npassword-managementpassword-expire-in-days [days]
```

Syntax Description	天	指定当前密码到期前的天数（0 至 180）。如果指定 password-expire-in-days 关键字，则需要此参数。
	password-expire-in-days	（可选）表示紧随其后的参数指定 ASA 在当前密码到期之前多少天开始警告用户有关即将到期的情况。此选项仅对 LDAP 服务器有效。请参阅使用说明部分以了解更多信息。

Command Default 默认设置为无密码管理。如果没有为 LDAP 服务器指定 password-expire-in-days 关键字，则在当前密码到期之前，默认开始警告的时间长度为 14 天。如果禁用此功能，ASA 将使用密码身份验证协议 (PAP) 的身份验证方法。

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
隧道组常规属性配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.1(1) 添加了此命令。

使用指南 ASA 支持 RADIUS 和 LDAP 协议的密码管理。对于 LDAP，它仅支持 “password-expire-in-days” 选项。

可以为 IPsec 远程访问和 SSL VPN 隧道组配置密码管理。

当您配置密码管理命令时，ASA 会在远程用户登录时通知用户当前密码即将过期或已过期。然后，ASA 为用户提供机会更改密码。如果当前密码尚未到期，用户仍可使用该密码登录。

此命令对于支持此类通知的AAA服务器有效；即，对于LDAP服务器和RADIUS服务器本身有效，代理到 NT 4.0 或 Active Directory 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。



注释 某些支持 MSCHAP 的 RADIUS 服务器当前不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此请与您的供应商核实。

使用 LDAP 或支持 MS-CHAPv2 的任何 RADIUS 配置进行身份验证时，ASA 版本 7.1 及更高版本通常支持以下连接类型的密码管理：

- AnyConnect VPN 客户端（ASA 软件 8.0 及更高版本）
- IPsec VPN 客户端
- 无客户端 SSL VPN（ASA 软件版本 8.0 及更高版本）WebVPN（ASA 软件版本 7.1 至 7.2.x）
- SSL VPN 客户端 全隧道客户端

这些 RADIUS 配置包括使用 LOCAL 身份验证的 RADIUS、使用 Active Directory/Kerberos Windows DC 的 RADIUS、使用 NT/4.0 域的 RADIUS 以及使用 LDAP 的 RADIUS。

对于 Kerberos/Active Directory（Windows 密码）或 NT 4.0 域，所有这些连接类型都不支持密码管理。RADIUS 服务器（例如，思科 ACS）可能会将身份验证请求以代理方式发送到另一个身份验证服务器。但是，ASA 仅与 RADIUS 服务器通信。



注释 对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前，ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。

本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下，LDAP 使用端口 636。

请注意，此命令不会改变密码过期前的天数，而是改变 ASA 在密码即将过期前多少天开始警告用户密码即将过期。

如果指定 **password-expire-in-days** 关键字，还必须指定天数。

指定此命令且天数设置为 0 会禁用此命令。ASA 不会通知用户密码即将到期，但是用户可以在密码到期后更改密码。



注释 Radius 不提供密码更改，也不提供密码更改提示。

CR_Examples

以下示例对于 WebVPN 隧道组 “testgroup”，将距离密码到期以开始警告用户即将到期的警告设置为 90：

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

以下示例使用默认值，即距离密码到期 14 天开始警告用户 IPsec 远程访问隧道组 “QAgrou” 即将到期：

```
ciscoasa(config)# tunnel-group QAgrou type ipsec-ra
ciscoasa(config)# tunnel-group QAgrou general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

Related Commands

命令	说明
clearconfigurepasswd	清除登录密码。
passwd	设置登录密码。
radius-with-expiry	在 RADIUS 身份验证期间启用密码更新协商（已弃用）。
showrunning-configpasswd	以加密形式显示登录密码。
tunnel-group general-attributes	配置隧道组常规属性值。

password-parameter

要指定必须提交用户密码以进行 SSO 身份验证的 HTTP POST 请求参数的名称，请在 **password-parameter** aaa-server-host 配置模式下使用该命令。这是使用 HTTP 表单命令的 SSO。

password-parameter 字符串



注释 要正确配置 HTTP 的 SSO，您必须具备有关身份验证和 HTTP 交换的全面工作知识。

Syntax Description	<i>string</i> HTTP POST 请求中包含的密码参数的名称。密码最大长度为 128 个字符。				
Command Default	没有默认值或行为。				
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
Aaa-server-host 配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.1(1) 添加了此命令。

使用指南 ASA 的 WebVPN 服务器使用 HTTP POST 请求向身份验证 Web 服务器提交单点登录身份验证请求。必需命 **password-parameter** 令指定 POST 请求必须包含用于 SSO 身份验证的用户密码参数。



注释 登录时，用户输入实际密码值，该密码值输入到 POST 请求中并传递给身份验证 Web 服务器。

CR_Examples 以下示例在 aaa-server-host 配置模式下指定名为 user_password 的 password 参数：

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

Related Commands

命令	说明
action-uri	指定要接收用于单点登录身份验证的用户名和密码的网络服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建用于与身份验证网络服务器交换的隐藏参数。
start-url	指定用于提取登录前 Cookie 的 URL。
user-parameter	指定 HTTP POST 请求参数的名称，其中必须提交用户名以进行 SSO 身份验证。

password-policy authenticate enable

要确定是否允许用户修改其自己的用户账号，请在全局配置模式下使用 **password-policy authenticate enable** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy authenticate enable
no password-policy authenticate enable

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，身份验证是禁用的。

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
全局配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.1(2) 添加了此命令。

使用指南

如果启用身份验证，**username** 命令不允许用户更改自己的密码或删除自己的帐户。此外，**clear configure username** 命令不允许用户删除自己的帐户。

CR_Examples

以下示例显示如何使用户能够修改其用户账户：

```
ciscoasa(config)# password-policy authenticate enable
```

Related Commands

命令	说明
password-policy minimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字母数。

password-policy lifetime

要为当前情景设置密码策略和密码过期的间隔（天），请在全局配置模式下使用 **password-policylifetime** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy lifetime值
no password-policy lifetime值

Syntax Description *value* 指定密码有效期。有效值范围为 0 至 65535 天。

Command Default 默认生命周期值为 0 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
全局配置	• 是	—	• 是	• 支持	—

Command History 版本 修改
9.1(2) 添加了此命令。

使用指南 密码具有指定的最长有效期限。0 天的生命周期间隔指定本地用户密码永不过期。请注意，密码将在有效期到期后的次日上午 12:00 到期。

CR_Examples 以下示例指定密码有效期值为 10 天：

```
ciscoasa(config)# password-policy lifetime 10
```

命令	说明
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policyminimumlength	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字母数。

password-policy minimum-changes

如要设置新密码和旧密码必须更改的最小字符数，请在全局配置模式下使用 **password-policy minimum-changes** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-changes 值
no password-policy minimum-changes 值

Syntax Description

value 指定新旧密码之间必须更改的字符数。有效值范围为 0 到 64 个字符。

Command Default

更改的字符数默认为 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
全局配置	• 是	—	• 是	• 支持	—

Command History

版本 修改

9.1(2) 添加了此命令。

使用指南

新密码必须在当前密码的基础上至少更改 4 个字符，并且仅当它们未出现在当前密码的任何位置时，才会被视为已更改。

CR_Examples

以下示例指定新旧密码之间最小字符更改数（6 个字符）：

```
ciscoasa(config)# password-policy minimum-changes 6
```

Related Commands

命令	说明
password-policy lifetime	设置密码有效期（以天为单位，在该天后密码将到期）。
password-policy minimum-length	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字母数。

password-policy minimum-length

要设置密码最小长度，请在全局配置模式下使用 **password-policyminimum-length** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-length值
no password-policy minimum-length值

Syntax Description *value* 指定密码的最小长度。有效值范围为 3 到 32 个字符。

Command Default 默认最小长度为 3。

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
9.1(2) 添加了此命令。

使用指南 如果最小长度小于任何其他最小属性（更改、小写字母、大写字母、数字和特殊字符），则会显示错误消息，并且不会更改最小长度。建议密码长度为 8 个字符。

CR_Examples 以下示例将密码的最小字符数指定为 8：

```
ciscoasa(config)# password-policy minimum-length 8
```

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置旧密码和新密码之间允许的最小已更改字符数。
password-policy minimum-lowercase	设置密码可以包含的最小小写字符数。

password-policy minimum-lowercase

要设置密码可能包含的最小小写字符数，请在全局配置模式下使用 **password-policy minimum-lowercase** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-lowercase 值
no password-policy minimum-lowercase 值

Syntax Description

value 指定密码的最小小写字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小小写字符数为 0，表示没有最低要求。

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

9.1(2) 添加了此命令。

使用指南

此命令设置密码可以包含的最小小写字符数。有效值范围为 0 到 64 个字符。

CR_Examples

以下示例将密码可具有的最小小写字符数指定为 6：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

Related Commands

命令	说明
password-policy lifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policy minimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-numeric

要设置密码可包含的最小数字字符数，请在全局配置模式下使用 **password-policyminimum-numeric** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-numeric值
no password-policy minimum-numeric值

Syntax Description *value* 指定密码的最小数字字符数。有效值范围为 0 到 64 个字符。

Command Default 默认的最小数字字符数为 0，表示没有最小字符数。

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
9.1(2) 添加了此命令。

使用指南 此命令设置密码可以包含的最小数字字符数。有效值范围为 0 到 64 个字符。

CR_Examples 以下示例指定密码可包含的最小数字字符数为 8：

```
ciscoasa(config)# password-policy minimum-numeric 8
```

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-special

要设置密码可包含的最小特殊字符数，请在全局配置模式下使用 **password-policy minimum-special** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-special 值
no password-policy minimum-special 值

Syntax Description

value 指定密码的最小特殊字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小特殊字符数为 0，表示没有最小字符数。

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

9.1(2) 添加了此命令。

使用指南

此命令设置密码可以包含的特殊字符的最小数量。特殊字符包括以下字符：!、@、#、\$、%、^、%、*、“(”和“)”。

CR_Examples

以下示例将密码可具有的最小特殊字符数指定为 2：

```
ciscoasa(config)# password-policy minimum-special 2
```

Related Commands

命令	说明
password-policy lifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policy minimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-uppercase

要设置密码可包含的最小大写字符数，请在全局配置模式下使用 `password-policyminimum-uppercase` 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 `no` 形式。

`password-policy minimum-uppercase`值
`no password-policy minimum-uppercase`值

Syntax Description `value` 指定密码的最小大写字符数。有效值范围为 0 到 64 个字符。

Command Default 默认的最小大写字符数为 0，表示没有最小字符数。

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
9.1(2) 添加了此命令。

使用指南 此命令设置密码可以包含的最小大写字符数。有效值范围为 0 到 64 个字符。

CR_Examples 以下示例将密码可包含的最小大写字符数指定为 4：

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

命令	说明
<code>password-policylifetime</code>	设置密码有效期值，以天为单位，在该值后密码到期。
<code>password-policyminimum-changes</code>	设置新旧密码之间必须更改的最小字符数。
<code>password-policy minimum-length</code>	设置密码的最小长度。

password-policy reuse-interval

要禁止对本地用户名重复使用密码，请在全局配置模式下使用 **password-policy reuse-interval** 命令。要删除此限制，请使用此 **no** 命令的形式。

password-policy reuse-interval 值
no password-policy reuse-interval [*value*]

Syntax Description

value 设置创建新密码时可使用的先前密码的数量，该值介于 2 到 7 之间。

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	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.8(1) 我们引入了此命令。

使用指南

您可以禁止重复使用与以前使用过的密码相匹配的密码。先前的密码使用该命令以加密形式存储 **username** 在每个配置 **password-history** 下；此命令不是用户可配置的。

CR_Examples

以下示例将密码续用间隔设置为 5：

```
ciscoasa(config)# password-policy reuse-interval 5
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 username 登录历史。
password-history	存储以前的 username 密码。用户无法配置此命令。
password-policy reuse-interval	禁止重复使用 username 密码。
password-policy username-check	禁止使用与 username 名称匹配的密码。
showaaalogin-history	显示本地 username 登录历史记录。

命令	说明
username	配置本地用户。

密码策略用户名检查

要禁止与用户名匹配的密码，请在全局配置模式下使用 **password-policy username-check** 命令。要删除此限制，请使用此 **no** 命令的形式。

password-policy username-check
no password-policy username-check

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	• 支持	• 支持	• 支持	—

Command History

版本 修改

9.8(1) 我们引入了此命令。

使用指南

可以禁止使用与 **username** 命令中的名称匹配的密码。

CR_Examples

以下示例限制密码与用户名 **john_crichton** 匹配：

```
ciscoasa(config)# password-policy username-check
ciscoasa(config)# username john_crichton password moya privilege 15
ciscoasa(config)# username aeryn_sun password john_crichton privilege 15
ERROR: Password must contain:
ERROR: a value that complies with the password policy
ERROR: Username addition failed.
ciscoasa(config)#
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 username 登录历史。
password-history	存储以前的 username 密码。用户无法配置此命令。
password-policyreuse-interval	禁止重复使用 username 密码。
password-policyusername-check	禁止使用与 username 名称匹配的密码。

命令	说明
showaaalogin-history	显示本地 username 登录历史记录。
username	配置本地用户。

password-storage

要让用户在客户端系统上存储他们的登录密码，请在 **password-storageenable** 策略组配置模式或用户名配置模式下使用该命令。要禁用密码存储，请使用该 **password-storagedisable** 命令。

要从运行配置中删除密码存储属性，请使用此 **no** 命令的形式。这使得可以从另一个组策略继承密码存储的值。

password-storage { enable | disable }
no password-storage

Syntax Description

disable 禁用密码存储。

enable 启用密码存储。

Command Default

密码存储已禁用。

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
组策略配置	• 是	—	• 是	—	—
用户名配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

使用指南

仅在已知处于安全站点中的系统上启用密码存储。

此命令与交互式硬件客户端身份验证或硬件客户端的个人用户身份验证无关。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用密码存储：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

peer-group

要标识 VXLAN 集群控制链路的 ASA virtual 集群节点，请在 nve 配置模式下使用 **peer-group** 命令。
要删除对等组，请使用此命令 **no** 的形式。

```
peer-group network_object_name
no peer-group network_object_name
```

Syntax Description	network_object_name 标识 object-group network 命令定义的网络对象。

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
Nve 配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.17(1) 添加了此命令。

使用指南

通过使用命令创建网络对象组来识别 VTEP 对 **object-group network**等 IP 地址。

VTEP 之间的基础 IP 网络独立于 VNI 接口使用的集群控制链路网络。VTEP 网络可能包含其他设备，VTEP 对等体甚至可能不在同一子网中。

VTEP 源接口 IP 地址应作为对等体之一包含在网络对象组中。

CR_Examples

以下是使用内联定义的主机来创建网络对象组的示例：

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

以下是创建引用独立网络对象的网络对象组的示例：

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54
```

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

以下示例将千兆以太网接口 0/7 定义为集群控制链路 VTEP 源接口，并将 cluster-peers 网络对象组标识为 peer-group:

```
interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

interface vni 1
    segment-id 1000
    vtep-nve 1
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
nve	指定网络虚拟化终端实例。
nve-only cluster	指定 NVE 用于集群控制链路。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

peer-id-validate

要指定是否使用对等方的证书验证对等方的身份，请在 **peer-id-validate**隧道组 ipsec-attributes 模式下使用该命令。要返回默认值，请使用此**no**命令形式。

peer-id-validate*option*
no peer-id-validate

Syntax Description	选 指定以下选项之一： 项 • : req必需的 • : cert如果有证书支持 • nocheck: 不检查

Command Default	此命令的默认设置为 req 。

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
隧道组 ipsec 属性	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南	您可以将此属性应用于所有 IPsec tunnel-group 类型。

CR_Examples	以下示例在 config-ipsec 配置模式下需要使用名为 209.165.200.225 的 IPsec LAN 间隧道组的对等体证书标识来验证对等体：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
clear-config tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置该组的隧道组 ipsec 属性。

peer ip

要手动指定对等体 VXLAN 隧道终端 (VTEP) IP 地址，请在 nve 配置模式下使用 **peerip** 命令。要删除对等地址，请使用此命 **no** 令的形式。

peer ip *ip_address*
no peer ip

Syntax Description *ip_address* 设置对等体 VTEP IP 地址，包括 IPv4 或 IPv6。

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
Nve 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.4(1)	添加了此命令。
9.20(1)	此命令现在支持 IPv6。

使用指南 如果指定对等体 IP 地址，则无法使用组播组发现。在多情景模式中不支持组播，因此只能选择手动配置。只能为 VTEP 指定一个对等体。

CR_Examples 以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并指定对等 IP 地址为 10.1.1.2:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。

命令	说明
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

perfmmon

要显示性能信息，请在 **perfmmon**特权 EXEC 模式下使用该命令。

perfmmon { **verbose** | **interval**秒 | **quiet** | **settings** } [详细信息]

Syntax Description	verbose	在 ASA 控制台上显示性能监视器信息。
	interval seconds	指定控制台上刷新性能显示前的秒数。
	quiet	禁用性能监控显示。
	settings	显示间隔以及它是安静的还是详细的。
	detail	显示有关性能的详细信息。

Command Default seconds 是 120 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
特权 EXEC	• 是	• 支持	• 支持	• 支持	—

Command History	版本	修改
	7.0	在ASA上添加了对此命令的支持。
	7.2(1)	增加了对关 detail 键字的支持。

使用指南 perfmmon 命令允许您监控 ASA 的性能。使用 show perfmmon 命令立即显示信息。使用 perfmmon verbose 命令可每 2 分钟显示一次此信息。将 perfmmon interval seconds 命令与 perfmmon verbose 命令配合使用，每隔指定的秒数显示一次该信息。

系统显示性能信息示例，如下所示：

PERFMON 统计信息：	当前	平均
Xlate	33/s	20/s
连接	110/s	10/s

TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP 修复	5/s	5/s
FTP 修复	7/s	4/s
AAA 身份验证	10/s	5/s
AAA 创建者	9/s	5/s
AAA帐户	3/s	3/s

此信息列出每秒发生的转换、连接、Websense 请求、地址转换（称为“修复”）和 AAA 事务的数量。

CR_Examples

此示例显示如何在 ASA 控制台上每 30 秒显示一次性能监视器统计数据：

```
ciscoasa(config)# perfmom interval 120
ciscoasa(config)# perfmom quiet
ciscoasa(config)# perfmom settings
interval: 120 (seconds)
quiet
```

Related Commands

命令	说明
showperfmom	显示性能信息。

periodic

要为支持时间范围功能的功能指定重复（每周）时间范围，请在 **periodic** 时间范围配置模式下使用该命令。要禁用此功能，请使用此命令的 **no** 形式。

```
periodicdays-of-the-weektimeto [days-of-the-week] time
no periodicdays-of-the-weektimeto [days-of-the-week] time
```

Syntax Description

一周内某天（可选）此参数第一次出现是关联时间范围生效的开始日期或星期几。第二次出现是指关联对账单生效的结束日期或星期几。

此参数是任意单日或多日组合：星期一、星期二、星期三、星期四、星期五、星期六和星期日。其他可能的值包括：

- day - 星期一到星期日
- weekdays - 星期一至星期五
- Weekend - 星期六和星期日

如果一周的结束日期与一周的开始日期相同，则可以省略它们。

time 以 HH:MM 格式指定时间。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。

to 要填写“从开始时间到结束时间”的范围，需要输入 **to** 关键字。

Command Default

如果未与 **periodic** 命令一起输入值，则根据 **time-range** 命令定义对 ASA 的访问立即生效并始终有效。

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
时间范围配置	• 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

要实现基于时间的 **time-rangeACL**，请使用命令定义一天和一周的特定时间。然后使用命令将 **time-range** 访问列表绑定到 ACL。

periodic 命令是指定时间范围生效的方法之一。另一种方法是使用 **absolute** 命令指定绝对时间段。在 **time-range** 全局配置命令（该命令指定时间范围的名称）后使用这些命令。每个 **time-range** 命令允许多个 **periodic** 条目。

如果结束 **days-of-the-week** 值与开始值相同，则可以省略它们。

如果 **time-range** 命令同时指定了 **absolute** 和 **periodic** 值，则仅在 **periodic** 达到 **absolutestart** 时间后评估命令，并且在达到 **absoluteend** 时间后不会进一步评估。

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

CR_Examples

以下是一些示例：

如果需要：	输入：
仅限星期一至星期五，上午 8:00 至下午 6:00	periodic weekdays 8:00 to 18:00
仅限一周中的每天上午 8:00 至下午 6:00	periodic daily 8:00 to 18:00
从星期一上午 8:00 到星期五晚上 8:00 每分钟一次	periodic monday 8:00 to friday 20:00
所有周末，从星期六早上到星期日晚上	periodic weekend 00:00 to 23:59
星期六和星期日，从中午到午夜	periodic weekend 12:00 to 23:59

以下示例显示如何允许仅在星期一至星期五的上午 8:00 至下午 6:00 访问 ASA：

```
ciscoasa(config-time-range) # periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range) #
```

以下示例显示如何允许在特定日期（星期一、星期二和星期五）上午 10:30 至下午 12:30 访问 ASA：

```
ciscoasa(config-time-range) # periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range) #
```

Related Commands

命令	说明
absolute	定义时间范围生效时的绝对时间。
access-list extended	配置允许或拒绝 IP 流量通过 ASA 的策略。
default	恢复命令 absolute 和 periodic 关 time-range 键字的默认设置。
time-range	基于时间定义对 ASA 的访问控制。

periodic-authentication certificate

要启用定期证书验证，请使用 **periodic-authentication certificate** 命令。要从默认组策略继承设置，请使用此命令的 **no** 形式。

periodic-authentication certificate<time in hours>**none**
no periodic-authentication certificate<time in hours>**none**

Syntax Description	时间（小时）	设置介于 1 和 168 小时之间的间隔。
	none	禁用定期身份验证。

Command Default 定期证书验证默认处于禁用状态。

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
默认策略组配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.4(1) 添加了此命令。

使用指南 默认情况下，对于默认组策略，命令将为 **periodic-authentication certificate none**。其他组策略会从默认策略继承该设置，除非做出更改。

CR Examples

```
100(config-group-policy)# periodic-authentication ?
group-policy mode commands/options:
  certificate  Configure periodic certificate authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>    Enter periodic authentication interval in hours
  none       Disable periodic authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>    Enter periodic authentication interval in hours
  none       Disable periodic authentication
100(config-group-policy)# help periodic-authentication
```

permit-errors

要允许无效 GTP 数据包或否则会解析失败并被丢弃的数据包，请在策略映射参数配置模式下使用 **permit-errors** 命令。返回到默认行为，其中所有无效数据包或解析失败的数据包都将被丢弃。请使用此命令的 **no** 形式。

permit-errors
no permit-errors

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，所有无效数据包或解析失败的数据包都会被丢弃。

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

在 GTP 检测策略映射参数中使用 **permit-errors** 命令，以允许通过 ASA 发送消息检测期间无效或遇到错误的任何数据包，而不是丢弃这些数据包。根据在策略映射中定义的操作，仍然可以丢弃数据包。

CR_Examples

以下示例允许包含无效数据包或解析失败的数据包的流量通过：

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-errors
```

Related Commands

命令	说明
policy-map type inspect gtp	定义 GTP 检查策略图。
inspect gtp	适用于特定的 GTP 映射，以用于应用检查。

permit-response

要配置 GSN 或 PGW 池，请在策略映射参数配置模式下使用 `permit-response` 命令。使用此命令的 `no` 形式可删除共享关系。

```
permit-responseto-object-group to_obj_group_id from-object-group from_obj_group_id
no permit-responseto-object-group to_obj_group_id from-object-group from_obj_group_id
```

Syntax Description	from-object-group 源对象组 ID	标识 GSN/PGW 终端的网络对象组。这必须是对象组（ object-group 命令）。这些终端可以向 to-object-group 发送请求并接收响应。 从版本 9.5(1) 开始，对象组可以包含 IPv6 地址，而不仅仅是 IPv4 地址。
	to-object-group 目标对象组 ID	标识 SGSN/SGW 的网络对象组。这必须是对象组（ object-group 命令）。这些地址可以接收来自 from-object-group 中标识的终端集的响应。 从版本 9.5(1) 开始，对象组可以包含 IPv6 地址，而不仅仅是 IPv4 地址。

Command Default ASA 会丢弃 GTP 请求中未指定的 GSN 或 PGW 的 GTP 响应。

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
参数配置模式	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	7.0(4) 添加了此命令。GTP 检查仅支持 IPv4 地址。
	9.5(1) 增加了对 IPv6 地址的支持。

使用指南 当 ASA 执行 GTP 检测时，ASA 默认会丢弃来自 GSN 或 PGW 而 GTP 请求中未指定的 GTP 响应。在 GSN 或 PGW 池中使用负载均衡来提供 GPRS 的效率和扩展性时，会发生这种情况。

要创建 GSN/PGW 轮询以便支持负载均衡，请创建一个指定 GSN/PGW 终端的网络对象组，并在 `from-object-group` 参数中指定该组。同样，为 SGSN/SGW 创建一个网络对象组并在 `to-object-group` 参数中选择该组。如果 GSN/PGW 响应与 GTP 请求被发送到的 GSN/PGW 属于同一个对象组，并且 SGSN/SGW 位于允许响应 GSN/PGW 向其发送 GTP 响应的对象组中，则 ASA 允许该响应。

网络对象组可通过主机地址或包含终端的子网标识它们。

CR_Examples

以下示例允许从 192.168.32.0 网络上的任何主机到 IP 地址为 192.168.112.57 的主机的 GTP 响应:

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1

ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit

ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# permit-response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

命令	说明
policy-map type inspect gtp	定义 GTP 检查策略图。
inspect gtp	适用于特定的 GTP 映射，以用于应用检查。
show service-policy inspect gtp	显示 GTP 配置。

pfs

要启用 PFS，请在 **pfsenable** 策略组配置模式下使用该命令。要禁用 PFS，请使用该 **pfsdisable** 命令。要从运行配置中删除 PFS 属性，请使用此命令的 **no**形式。

```
pfs { enable | disable }
no pfs
```

Syntax Description	disable 禁用 PFS。
	enable 启用 PFS。

Command Default PFS 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
组策略配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南 VPN 客户端和 ASA 上的 PFS 设置必须匹配。

使用此命令的 **no** 形式可允许从其他组策略继承 PFS 的值。

在 IPsec 协商中，PFS 确保每个新的加密密钥与任何先前的密钥无关。

CR_Examples

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


phone-proxy (已弃用)

要配置电话代理实例，请在 **phone-proxy**全局配置模式下使用该命令。

要删除电话代理实例，请使用此命 **no** 令的形式。

```
phone-proxyPhone_proxy_name
no phone-proxyPhone_proxy_name
```

Syntax Description	Phone_proxy_name 指定电话代理实例的名称。

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
全局配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(4) 命令已添加。
	9.4(1) 此命令已弃用。

使用指南	只能在 ASA 上配置一个电话代理实例。
	如果为 HTTP 代理服务器配置了 NAT，则与 IP 电话相关的 HTTP 代理服务器的全局或映射 IP 地址将写入电话代理配置文件。

CR_Examples	以下示例显示如何使 phone-proxy 用命令配置电话代理实例：

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa
(config-phone-proxy)#
media-termination address 192.0.2.25 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa
```

```
(config-phone-proxy) #
ctl-file asactl
ciscoasa
(config-phone-proxy) #
cluster-mode nonsecure
ciscoasa
(config-phone-proxy) #
timeout secure-phones 00:05:00
ciscoasa
(config-phone-proxy) #
disable service-settings
```

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。
tls-proxy	配置 TLS 代理实例。

pim

要重新启用接口上的 PIM，请在接口配置模式下使用 **pim** 命令。要禁用 PIM，请使用此命令 **no** 的形式。

pim
no pim

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下， **multicast-routing** 命令会在所有接口上启用 PIM。

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
7.0(1)	添加了此命令。

使用指南 默认情况下， **multicast-routing** 命令会在所有接口上启用 PIM。仅 **no** 命令的 **pim** 形式会保存在配置中。



注释 PAT 不支持 PIM。PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。

CR_Examples 以下示例在所选接口上禁用 PIM：

```
ciscoasa(config-if)# no pim
```

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim accept-register

要配置 ASA 以筛选 PIM 注册消息，请在全局配置模式下使用 **pim accept-register** 命令。要删除过滤，请使用此命令 **no** 的形式。

pimaccept-register { **listacl** | **route-map**映射名称 }
no pim accept-register

Syntax Description	listacl	指定访问列表名称或编号。使用此命令时只能使用扩展主机 ACL。
	route-mapmap-name	指定 route-map 名称。在引用的路由映射中使用扩展主机 ACL。

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	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南 此命令用于防止未授权的源向 RP 注册。如果未授权的源向 RP 发送注册消息，ASA 将立即发回注册停止消息。

CR_Examples 以下示例将 PIM 注册消息限制为来自名为 “no-ssm-range” 的访问列表中定义的源的注册消息：

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

Related Commands	命令	说明
	multicast-routing	在 ASA 上启用组播路由。

pim bidir-neighbor-filter

要控制哪些支持 bidir 的邻居可参与 DF 选举，请在接口配置模式下使用 **pim bidir-neighbor-filter** 命令。要删除过滤，请使用此命令的形式。

```
pim bidir-neighbor-filteracl
no pim bidir-neighbor-filteracl
```

Syntax Description	acl 指定访问列表名称或编号。此访问列表定义可以参与 bidir DF 选举的邻居。在此命令中仅使用标准 ACL；不支持扩展 ACL。

Command Default	所有路由器都被视为支持 bidir。

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 双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须为 bidir 双向启用分片中的所有组播路由器。

该命令允许您指定应参与 DF **pimbidir-neighbor-filter**选举的路由器，同时仍允许所有路由器参与稀疏模式域，从而实现从仅稀疏模式网络到双向网络的转换。支持 bidir 的路由器可以从它们本身当中选择 DF，即使分片上有非 bidir 路由器。非 bidir 路由器上的组播边界可防止 bidir 组中的 PIM 消息和数据泄漏到 bidir 子集云中或从 bidir 子集云泄漏出去。

启用该 **pimbidir-neighbor-filter**命令后，ACL 允许的路由器将被视为具有 bidir 功能。因此：

- 如果允许的邻居不支持 bidir，则不会发生 DF 选举。
- 如果被拒绝的邻居支持 bidir，则不会发生 DF 选举。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选举。

CR_Examples	以下示例允许 10.1.1.1 成为 PIM bidir 邻居：

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

命令	说明
multicastboundary	为管理范围的多播地址定义多播边界。
multicast-routing	在 ASA 上启用组播路由。

pim bsr-border

要阻止通过接口发送或接收自举路由器 (BSR) 消息，请在接口配置模式下使用 `pim bsr-border` 命令。



注释 对于 PIM 稀疏模式 (PIM-SM) 域中的边界接口，需要采取特殊的预防措施，以避免与可通过该接口访问的相邻域交换某些流量，尤其是在该域同时运行 PIM-SM 的情况下。

pim bsr-border
no pim bsr-border

Syntax Description 此命令没有任何参数或关键字。

Command Default 该命令默认为禁用。

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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南 当在接口上配置此命令时，将不会通过该接口发送或接收任何 PIM 版本 2 BSR 消息。使用此命令配置与另一个 PIM 域邻接的接口，以避免在两个域之间交换 BSR 消息。不应在不同的域之间交换 BSR 消息，因为一个域中的路由器可能会选举另一个域中的交汇点 (RP)，从而导致协议故障或失去域之间的隔离。



注释 此命令不会设置组播边界。它仅设置 PIM 域 BSR 消息边界。

CR_Examples

以下示例将接口配置为 PIM 域边界：

```
ciscoasa(config)# interface gigabit 0/0
ciscoasa(config-if)# pim bsr-border
ciscoasa(config)# show runn interface gigabitEthernet 0/0
!
```

```
interface GigabitEthernet0/0
 nameif outsideA
 security-level 0
 ip address 2.2.2.2 255.255.255.0
 pim bsr-border
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。
pim bsr-candidate	将 ASA 配置为候选 BSR

pim bsr-candidate

要配置路由器宣布其作为引导程序路由器 (BSR) 的候选，请在全局配置模式下使用 `pim bsr-candidate` 命令。要删除此路由器作为引导程序路由器的候选者，请使用此命令的 `no` 形式。

```
pim bsr-candidate interface-name [ hash-mask-length [ priority ] ]
no pim bsr-candidate
```

Syntax Description	interface-name	从其派生 BSR 地址的此路由器上的接口名称。此地址在 BSR 消息中发送。
	散列掩码长度	（可选）在调用 PIMv2 哈希函数之前，要与组地址进行“与”运算的掩码长度（最多 32 位）。所有具有相同种子哈希的组都对应相同的会合点 (RP)。 例如，如果此值为 24，则组地址只有前 24 位起作用。散列掩码长度允许一个 RP 用于多个组。 默认散列掩码长度为 0。
	priority	（可选）候选 BSR (C-BSR) 的优先级。范围是从 0 到 255。优先选择具有最高优先级值的 C-BSR。如果优先级值相同，则 IP 地址较大的路由器是 BSR。 默认优先级为 0。

Command Default 该命令默认为禁用。

当将设备配置为没有散列长度和优先级的 bsr 候选者时，它假设默认散列长度为 0，优先级为 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
全局配置	• 是	—	• 是	—	—

Command History	版本 修改
	9.5(2) 添加了此命令。

使用指南 此命令导致 ASA 将引导程序消息发送到其所有 PIM 邻居，其中指定接口的地址作为 BSR 地址。每个邻居会将 BSR 地址与它从先前引导程序消息（不必在同一接口上接收）中获取的地址进行比较。如果当前地址是相同或更高的地址，则它缓存当前地址并转发引导程序消息。否则，它会丢弃引导程序消息。

此 ASA 将继续作为 BSR，直到收到来自另一个候选 BSR 的引导程序消息，表明自己具有更高的优先级（或者，如果优先级相同，则具有更高的 IP 地址）。

CR_Examples

以下示例将 ASA 配置为内部接口上的候选自举路由器 (C-BSR)，散列长度为 30，优先级为 10：

```
ciscoasa(config)# pim bsr-candidate inside 30 10
ciscoasa(config)# sh runn pim
pim bsr-candidate inside 30 10
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。
pim bsr-border	将 ASA 配置为边界 BSR

pim dr-priority

要在 ASA 上配置用于指定路由器选举的邻居优先级，请在接口配置模式下使用 **pimdr-priority** 命令。要恢复默认优先级，请使用此命令 **no** 的形式。

pim dr-priority 编号
no pim dr-priority

Syntax Description	<i>number</i> 介于 0 到 4294967294 之间的数字。在确定指定路由器时，此数字用于确定设备的优先级。指定 0 可防止 ASA 成为指定路由器。

Command Default	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
接口配置	• 是	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南	接口上具有最大优先级值的设备将成为 PIM 指定路由器。如果多台设备具有相同的指定路由器优先级，则具有最高 IP 地址的设备将成为 DR。如果设备在 Hello 消息中未包含 DR-Priority 选项，则该设备会被视为优先级最高的设备并成为指定路由器。如果多台设备未在其 Hello 消息中包含此选项，则具有最高 IP 地址的设备将成为指定路由器。

CR_Examples 以下示例将接口的 DR 优先级设置为 5：

```
ciscoasa(config-if)# pim dr-priority 5
```

Related Commands	命令	说明
	multicast-routing	在 ASA 上启用组播路由。

pim hello-interval

如要配置 PIM 呼叫消息的频率，请在接口配置模式下使用 **pimhello-interval** 命令。要将 hello-interval 恢复为默认值，请使用此命令的 **no** 形式。

pim hello-interval秒
no pim hello-interval [秒]

Syntax Description *seconds* ASA 在发送 hello 消息之前等待的秒数。值的范围为 1 到 3600 秒。默认值为 30 秒。

Command Default 间隔默认为30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
接口配置	• 是	—	• 是	—	—

Command History 版本 修改

7.0(1) 添加了此命令。

CR_Examples 以下示例将 PIM 呼叫间隔设置为 1 分钟：

```
ciscoasa(config-if)# pim hello-interval 60
```

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim join-prune-interval

如要配置 PIM 加入/删除间隔，请在接口配置模式下使用 **pimjoin-prune-interval** 命令。要将间隔恢复为默认值，请使用此命令的 **no**形式。

pimjoin-prune-interval秒
no pimjoin-prune-interval [*seconds*]

Syntax Description *seconds* ASA 在发送加入/删除消息之前等待的秒数。有效值范围为 10 至 600 秒。默认值为 60 秒。

Command Default 默认间隔为 60 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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples 以下示例将 PIM 加入/删除间隔设置为 2 分钟：

```
ciscoasa(config-if)# pim join-prune-interval 120
```

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim neighbor-filter

要控制哪些邻居路由器可以加入 PIM，请在接口配置模式下使用 **pimneighbor-filter** 命令。要删除过滤，请使用此命 **no** 令的形式。

pim neighbor-filteracl
no pim neighbor-filteracl

Syntax Description *al* 指定访问列表名称或编号。在此命令中仅使用标准 ACL；不支持扩展 ACL。

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
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 此命令定义了可以参与 PIM 的邻居路由器。如果配置中不存在此命令，则没有限制。

必须启用组播路由和 PIM，此命令才会显示在配置中。如果禁用组播路由，则会从配置中删除此命令。

CR_Examples 以下示例允许 IP 地址为 10.1.1.1 的路由器成为接口 GigabitEthernet 0/2 上的 PIM 邻居：

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim old-register-checksum

要在使用旧注册校验和方法的交汇点 (RP) 上实现向后兼容，请在全局配置模式下使用 **pim old-register-checksum** 命令。要生成符合 PIM RFC 标准的寄存器，请使用此命令的 **no** 形式。

pim old-register-checksum
no pim old-register-checksum

Syntax Description 此命令没有任何参数或关键字。

Command Default ASA 可生成符合 PIM RFC 标准的寄存器。

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

7.0(1) 添加了此命令。

使用指南 ASA 软件接受在 PIM 报头以及仅接下来 4 个字节上包含校验和的注册消息，而不是使用思科 IOS 方法 - 接受具有所有 PIM 消息类型的完整 PIM 消息的注册消息。 **pimold-register-checksum** 命令生成与 Cisco IOS 软件兼容的寄存器。

CR_Examples 以下示例将 ASA 配置为使用旧校验和计算：

```
ciscoasa(config)# pim old-register-checksum
```

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim rp-address

要配置 PIM 交汇点 (RP) 的地址，请在全局配置模式下使用 **pimrp-address** 命令。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 **no**时间。

```
pim rp-addressip_address[acl] [bidir]
no pim rp-addressip_address
```

Syntax Description	acl（可选）定义 RP 应与哪些多播组一起使用的标准访问列表的名称或编号。请勿在使用此命令时一起使用主机 ACL。 bidir（可选）指示指定的组播组将在双向模式下运行。如果配置 命令时不使用此选项，则指定的组将在 PIM 稀疏模式下运行。 ip_address 将成为 PIM RP 的路由器的 IP 地址。这是一个由四部分点分十进制表示的单播 IP 地址。

Command Default 未配置 PIM RP 地址。

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
	7.0(1) 添加了此命令。

使用指南 公共 PIM 稀疏模式 (PIM-SM) 或 bidir 域内的所有路由器都需要了解众所周知的 PIM RP 地址。使用此命令静态配置地址。



注释 ASA 不支持自动 RP；您必须使 **pimrp-address**用命令指定 RP 地址。

您可以配置单个 RP 来为多个组提供服务。访问列表中指定的组范围决定了 PIM RP 组映射。如果未指定访问列表，则该组的 RP 将应用于整个 IP 多播组范围 (224.0.0.0/4)。



注释 无论实际的 bidir 配置如何，ASA 始终在 PIM hello 消息中通告 bidir 功能。

CR_Examples

以下示例将所有组播组的 PIM RP 地址设置为 10.0.0.1:

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

Related Commands

命令	说明
pimaccept-register	配置候选RP，过滤PIM注册消息。

pim spt-threshold infinity

要更改最后一跳路由器的行为以始终使用共享树且从不执行最短路径树 (SPT) 切换，请在全局配置模式下使用 **pim spt-threshold infinity** 命令。要恢复默认值，请使用此命令 **no** 的形式。

pim spt-threshold infinity [*group-list acl*]
no pim spt-threshold

Syntax Description **group-list acl** （可选）指示受访问列表限制的源组。*acl* 参数必须指定标准 ACL；不支持扩展 ACL。

Command Default 默认情况下，最后一跳 PIM 路由器切换到最短路径源树。

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
7.0(1) 添加了此命令。

使用指南 如果未使用 **group-list** 关键字，则此命令适用于所有组播组。

CR_Examples 以下示例导致最后一跳 PIM 路由器始终使用共享树而不是切换到最短路径源树：

ciscoasa(config)# **pim spt-threshold infinity**

命令	说明
mcast-routing	在 ASA 上启用组播路由。

ping

要测试从指定接口到 IP 地址的连接，请在 **ping** 特权 EXEC 模式下使用该命令。与 TCP ping 相比，常规的基于 ICMP 的 ping 可用的参数有所不同。输入不带参数的命令，系统会提示输入值，包括不能用作参数的特征。

```
ping [if_name] host [repeatcount] [timeoutseconds] [datapattern] [sizebytes] [validate]
ping tcp [if_name] host port [repeatcount] [timeoutseconds] [sourcehost port]
ping
```



注释 source 和 port 选项仅与 tcp 选项配合使用；data、size 和 validate 选项不适用于 tcp 选项。

Syntax Description	
datapattern	（可选，仅限 ICMP。）指定十六进制格式的 16 位数据模式，范围为 0 到 FFFF。默认值为 0xabcd。
host	指定要 ping 的主机的 IPv4 地址或名称。对于 ICMP ping，可以指定 IPv6 地址（TCP ping 不支持该地址）。 使用主机名时，名称可以是 DNS 名称或使用 name 命令分配的名称。DNS 名称的最大字符数为 128，使用 name 命令创建的名称的最大字符数为 63。必须配置 DNS 服务器以使用 DNS 名称。
if_name	（可选）指定用于 ping 源的 IP 地址的接口名称；但实际的出口接口是通过使用数据路由表的路由查找来确定的。
port	（仅限 TCP。）为您正在 ping 的主机指定 TCP 端口号 (1-65535)。
repeat 计数	（可选）指定重复 ping 请求的次数。默认值为 5。
sizebytes	（可选，仅限 ICMP。）指定数据报大小（以字节为单位）。默认值为 100。
sourcehostport	（可选，仅限 TCP。）指定从其发送 ping 的某个 IP 地址和端口（对于随机端口，使用端口 = 0）。源地址不会影响数据包的路由方式。
tcp	（可选）测试基于 TCP 的连接（默认为 ICMP）。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。您还可以同时运行最多 2 个 TCP ping 操作。
timeoutseconds	（可选）指定超时间隔的秒数。默认值为 2 秒。
validate	（可选，仅限 ICMP。）验证回复数据。

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	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	添加了对 DNS 名称的支持。
8.4(1)	添加了 tcp 选项。
9.18(2)	如果您在命令中指定接口，则源 IP 地址与指定的接口 IP 地址匹配，但实际出口接口将由使用数据路由表的路由查找来确定。

使用指南

该 **ping** 命令允许您确定 ASA 是否具有连接或网络上是否有主机可用。

当使用基于 ICMP 的常规 **ping** 时，请确保您没有禁止这些数据包的 **icmp** 规则（如果您不使用 ICMP 规则，则允许所有 ICMP 流量）。如果希望内部主机通过 ICMP 对外部主机 **ping** 操作，必须执行以下操作之一：

- 创建用于回应应答的 ICMP **access-list** 命令；例如，要为所有主机提供 **ping** 访问权限，请使用 **access-list acl_grppermiticmp any any** 命令，然后将 **access-list** 命令绑定到要使用 **access-group** 命令测试的接口。
- 使用 **inspect icmp** 命令配置 ICMP 检测引擎。例如，将 **inspect icmp** 命令添加到全局服务策略的 **class default_inspection** 类，将允许通过 ASA 对内部主机发起的回应请求进行回应。

使用 TCP **ping** 时，您必须确保访问策略允许在您指定的端口上的 TCP 流量。

需要此配置来允许 ASA 响应并接受从命令生成的 **ping** 消息。**ping** 命令输出显示是否接收了响应。如果输入 **ping** 命令后主机未响应，将出现如下所示的类似消息：

```
ciscoasa(config)# ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ASA 会使用数据路由表来路由 **ping** 数据包，并且仅当数据表中没有匹配的路由时才会回退到管理路由表。为 TCP **ping** 指定源 IP 地址不会影响数据包的路由方式。例如，即使您手动指定源地址来匹配接口 IP 地址，也不会从该接口发出 **ping**。出口接口仅由路由查找确定。

使用该 **show interface** 命令确保 ASA 已连接到网络并正在传输流量。指定 **if_name** 的地址用作 **ping** 的源地址，除非指定了其他源地址（仅限 TCP **ping**）。

您还可以输入不带参数的 **ping** 来执行扩展 ping。系统将提示您输入参数，包括一些不能用作关键字的特征。

CR_Examples

以下示例显示如何确定其他 IP 地址对 ASA 是否可见：

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下示例使用 DNS 名称指定主机：

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下是扩展 ping 的示例：

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
The following are examples of the ping tcp command:
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7

Source IP port: [0] 465

Repeat count: [5]
Timeout in seconds: [2] 5

Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
```

```
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms
ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Related Commands

命令	说明
icmp	为在接口终止的 ICMP 流量配置访问规则。
showinterface	显示有关 VLAN 配置的信息。



po - pq

- 管制，第 1260 页
- 策略，第 1263 页
- policy-list，第 1265 页
- policy-map，第 1267 页
- policy-map type inspect，第 1271 页
- policy-route，第 1276 页
- policy-server-secret (已弃用)，第 1278 页
- policy static sgt，第 1280 页
- polltime interface，第 1282 页
- poll-timer，第 1284 页
- pop3s (已弃用)，第 1286 页
- port (已弃用)，第 1288 页
- portal-access-rule (已弃用)，第 1290 页
- port-channel load-balance，第 1293 页
- port-channel min-bundle，第 1297 页
- port-channel span-cluster，第 1299 页
- port-forward (已弃用)，第 1301 页
- port-forward-name (已弃用)，第 1304 页
- 端口对象，第 1306 页
- post-max-size，第 1309 页
- 内嵌式电源，第 1311 页
- power-supply，第 1313 页
- pppoe client route distance，第 1314 页
- pppoe client route track，第 1316 页
- pppoe client secondary，第 1318 页
- prc-interval，第 1320 页

管制

要将 QoS 策略管制应用于类映射，请在类配置模式下使用 **police**命令。要取消速率限制，请使用此命 **no**令的形式。

```
police { output | input } conform-rate [ conform-burst ] [ conform-action [ drop | transmit ]
[ exceed-action [ drop | transmit ] ] ]
no police
```

Syntax Description

合格率	设置此流量类别的速率限制，范围为每秒 8000 至 2000000000 比特。对于 ASA virtual 和 Firepower 4100/9300，范围为 8000-1000000000000。例如，要将流量限制为 5Mbps，请输入 5000000。
conform-burst	指定控制到符合速率值之前连续突发中允许的最大即时字节数，该值介于 1000 到 512000000 字节之间。对于 ASA virtual 和 Firepower 4100/9300，范围为 1000-256000000000。 如果省略此参数，则默认值为 conform-rate（以字节为单位）的 1/32（也就是说，在符合率为 100,000 的情况下，默认 conform-burst 值为 100,000/32 = 3,125）。请注意，conform-rate 的单位为位/秒，而 conform-burst 的单位为字节。
conform-action[drop transmit]	设置流量低于管制速率和突发大小时要执行的操作。您可以 drop 或 transmit 流量。默认为传输流量。
exceed-action[drop transmit]	设置流量超过策略管制速率和突发大小时要执行的操作。您可以拦截超出监管速率和突发大小的数 drop 据 transmit 包。默认情况下会丢弃多余的数据包。
input	启用输入方向的流量监管。
output	启用输出方向的流量监管。

Command Default

无默认行为或变量。

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
类配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	添加了 input 选项。现在支持入站方向的策略管制。

使用指南

监管是一种确保没有流量超过您配置的最大速率（以比特/秒为单位）的方法，从而确保没有任何一个流量可以接管整个资源。如果流量超过最大速率，ASA 将丢弃超额的流量。策略管制还设定了允许的单次最大突发流量。

要启用策略管制，请使用模块化策略框架：

1.class-map—识别要执行监管的流量。

2.policy-map- 标识与每个类映射关联的操作。

- **a.class**- 标识要对其执行操作的类映射。
- **b.police**- 为类映射启用策略管制。

3.service-policy- 将策略映射分配到接口或全局。

如果需要，可以为 ASA 单独配置各种 QoS 功能。不过，ASA 上通常会配置多种 QoS 功能以便可以优先排列某些流量，并防止其他流量导致带宽问题。

请参阅以下每个接口支持的功能组合：

- 标准优先级排队（针对特定流量）+ 监管（针对其余流量）。

无法对同一组的流量配置优先级排队和策略管制。

- 流量整形（适用于接口上的所有流量）+ 分级式优先级排队（适用于一部分流量）。

通常，如果您启用流量整形，也不会为相同的流量启用策略管制，但 ASA 不限制您进行这种配置。

请参阅以下准则：

- QoS 是单向应用的；只有进入应用策略映射的接口的流量才会受到影响（或退出接口，取决于您是否指定 **input** 或 **output**）。
- 如果从已建立现有流量的接口应用或删除服务策略，则 QoS 策略不会从流量流应用或删除。要为此类连接应用或删除 QoS 策略，您必须清除连接并重新建立连接。查看命令 **clearconn**。
- 不支持到箱流量。
- 不支持进出 VPN 隧道绕行接口的流量。
- 当您匹配隧道组类映射时，仅支持出站监管。

CR_Examples

以下是输出方向的 **police** 命令的示例，该命令将符合速率设置为 100,000 位/秒，突发值为 20,000 字节。

```
ciscoasa(config)# policy-map localpolicy1
```

```
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass

ciscoasa(config-pmap-c)# police output 100000 20000
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

以下示例展示如何对发往内部 Web 服务器的流量执行速率限制：

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

Related Commands

class	指定用于流量分类的类映射。
clearconfigurepolicy-map	删除所有策略映射配置，但如果策略映射正在用于服务策略命令，则不会删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
showrunning-configpolicy-map	— 确定您想要执行操作的类映射。

策略

要指定检索 CRL 的源，请在 `ca-crl` 配置模式下使用 `policy` 命令。

`policy { static | cdp | both }`

Syntax Description

- both** 指定如果使用 CRL 分发点获取 CRL 失败，则使用静态 CDP 重试，最多可重试 5。
- cdp** 使用正在检查的证书中嵌入的 CDP 扩展。在此情况下，ASA 从正在验证的证书的 CDP 扩展检索最多五个 CRL 分发点，并在必要时使用已配置的默认值扩充其信息。如果 ASA 尝试使用主 CDP 检索 CRL 失败，它将使用列表中的下一个可用 CDP 重试。这个过程会一直持续到 ASA 检索到 CRL 或排尽列表。
- static** 最多使用五个静态 CRL 分发点。如果指定此选项，还需使用 `protocol` 命令指定 LDAP 或 HTTP URL。

Command Default

默认设置为 `cdp`。

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
Crl 配置	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

CR_Examples

以下示例进入 `ca-crl` 配置模式，并使用正在检查的证书中的 CRL 分发点扩展来配置 CRL 检索，或者如果失败，则使用静态 CDP：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

Related Commands

命令	说明
<code>crlconfigure</code>	进入 <code>ca-crl</code> 配置模式。
<code>cryptocatrustpoint</code>	进入 <code>trustpoint</code> 配置模式。

命令	说明
<code>url</code>	创建和维护用于检索 CRL 的静态 URL 列表。

policy-list

要创建边界网关协议 (BGP) 策略列表，请在策略映射配置模式下使用 **policy-list** 命令。要删除策略列表，请使用此命令 **no** 的形式。

policy-list*policy-list-name* { **permit** | **deny** }
no policy-list*policy-list-name*

Syntax Description

policy-list-name 配置的策略列表的名称。

permit 允许符合条件的访问。

deny 因条件匹配而拒绝访问。

Command Default

默认情况下不启用此命令。

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

9.2(1) 添加了此命令。

使用指南

当在路由映射中引用策略列表时，将评估和处理策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略 — 使用 AND 语义或 OR 语义评估路由映射内配置的列表。策略列表也可以与任何其他预先存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

此处列出 **policy-list** 子命令：

子命令	详细信息
<i>match as-path [path-list-number]</i>	匹配 as-path，并且它可以采用多个 as-path 路径列表号
匹配社区 [社区名称][精确匹配]	社区名称是必须的，精确匹配可为可选项。可以指定多个名称
<i>Match interface [interface-name]</i>	可以采用多个接口名称

子命令	详细信息
匹配指标 (0-4294967295)	它可能需要多个号码
<i>Match ip address [acl name prefix-list [prefix-listname]]</i>	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
<i>Matchipnext-hop[acl name aclname]prefix-list[prefix-listname]]</i>	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
<i>Match ip route-source [acl 名称 prefix-list [prefix-listname]]</i>	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
默认匹配	默认情况下，“match”下将包含上述所有选项
<i>Help</i>	后续命令的帮助
否	命令的否定
<i>Exit</i>	退出策略映射模式

CR_Examples

在以下示例中，配置了一个策略列表，允许与 AS 1 和指标 10 匹配的所有网络前缀：

```
ciscoasa(config)# policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

在以下示例中，配置了一个策略列表，允许与社区 20 和指标 10 匹配的流量：

```
ciscoasa(config)# policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

在以下示例中，配置了一个策略列表来拒绝与社区 20 和指标 10 匹配的流量：

```
ciscoasa(config)# policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

使用模块化策略框架时，在全局配置模式下使用 **policy-map** 命令（不带 **type** 关键字）可以为使用第 3/4 层类映射（**class-map** 或 **class-map type management** 命令）标识的流量分配操作。要删除第 3/4 层策略映射，请使用此命令的 **no** 形式。

policy-map *name*
no policy-map *name*

Syntax Description

name 指定此策略映射的名称，长度最大为 40 个字符。所有类型的策略映射都使用同一命名空间，因此无法重复使用已被另一类型的策略映射使用的名称。

Command Default

默认情况下，配置包含一项策略（全局策略），该策略匹配所有默认应用检测流量并将某些检测应用到所有接口上的流量。并非所有检测都默认被启用。仅能应用一个全局策略，因此如果想要改变全局策略，则需要编辑默认策略或禁用默认策略并应用新策略。（对于某项特定功能，接口策略覆盖全局策略。）

默认策略包括以下应用检测：

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

默认策略配置包括以下命令：

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

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。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用 **class-map** 或 **class-map type management** 命令应用操作的第 3 层和第 4 层流量。
2. （仅限应用检测）使用 **policy-map type inspect** 命令定义应用检测流量的特殊操作。
3. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。
4. 使用 **service-policy** 命令在接口上激活这些操作。

策略映射最大数量为 64 个，但每个接口只能应用一个策略映射。可以将同一策略映射应用到多个接口。您可以在第 3/4 层策略映射中识别多个第 3/4 层类映射（请参阅命令），并且可以将来自一个或多个功能类型的 **class** 多个操作分配给每个类映射。

CR_Examples

以下 **policy-map** 是连接策略命令的示例。它限制了允许到达 Web 服务器 10.1.1.1 的连接数：

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

以下示例显示多匹配在策略映射中如何运行：

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

以下示例显示流量如何与第一个可用的类映射匹配而不匹配同一功能域中指定操作的任何后续类映射：

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

当发起 Telnet 连接时，它会匹配 **class telnet_traffic** 类似地，如果发起了 FTP 连接，则匹配 **class ftp_traffic** 对于除 Telnet 和 FTP 之外的任何 TCP 连接，它都会匹配。即使 Telnet 或 FTP 连接可以匹配 **class tcp_traffic**，ASA 也不会进行此匹配，因为它们之前已匹配其他类。

NetFlow 事件通过模块化策略框架进行配置。如果没有为 NetFlow 配置模块化策略框架，则不会记录任何事件。流量将根据类的配置顺序进行匹配。检测到某个匹配后，不检查任何其他类。对于 NetFlow 事件，配置要求如下：

- 流导出目的地（即 NetFlow 收集器）由其 IP 地址唯一标识。

- 支持的事件类型为 flow-create、flow-teardown、flow-denied、flow-update 等，其中包括前面列出的四种事件类型。
- 使用 **flow-exportevent-type {all | flow-create | [] flow-denied | [] flow-update | [] flow-teardown} destination** 命令来配置 NetFlow 收集器和过滤器的地址，以确定应将哪些 NetFlow 记录发送到每个收集器。
- 接口策略不支持流导出操作。
- 仅在 **class-default** 命令中以及在使用 **matchany** 或 **matchaccess-list** 命令的类中支持流导出操作。
- 如果未定义 NetFlow 收集器，则不会发生任何配置操作。
- 接口策略不支持流导出操作。

以下示例将主机 10.1.1.1 和 20.1.1.1 之间的所有 NetFlow 事件导出到目标 15.1.1.1。

```
ciscoasa(config)# access-listflow_export_aclpermit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination 15.1.1.1
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
clearconfigurepolicy-map	删除所有策略映射配置。如果策略映射正在用于 service-policy 命令中，则不会删除该策略映射。
class-map	定义流量类映射。
service-policy	将策略映射分配给某个接口或全局分配给所有接口。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

policy-map type inspect

使用模块化策略框架时，通过在全局配置模式下使用 **policy-map type inspect** 命令为检测应用流量定义特殊操作。要删除检测策略映射，请使用此命令的 **no** 形式。

```
policy-map type inspectapplicationpolicy_map_name  
no policy-map [typeinspectapplication] policy_map_name
```

Syntax Description	应用 指定要对其执行操作的应用流量类型。可用类型包括： • dcerpc • diameter • dns • esmtp • ftp • gtp • h323 • http • im • ip-options • ipsec-pass-thru • ipv6 • lisp • m3ua • mgcp • netbios • radius-accounting • rtsp • scansafe • sctp • sip • skinny • snmp <i>policy_map_name</i> 指定此策略映射的名称，长度最大为 40 个字符。以 “_internal” 或 “_default” 开头的名称为预留名称，无法使用。所有类型的策略映射都使用同一命名空间，因此无法重复使用已被另一类型的策略映射使用的名称。
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。

8.2(1) 添加 **ipv6** 关键字是为了支持 IPv6 检测。

9.0(1) 添加 **scansafe** 关键字是为了支持云网络安全。

9.5(2) 添加 **lisp** 关键字是为了支持 LISP 检查。

9.5(2) 添加了 **diameter** 和 **sctp** 关键字。

9.6(2) 添加了 **m3ua** 关键字。

使用指南

通过模块化策略框架，您可以为许多应用检测配置特殊操作。当您使用第 3/4 层策略映射中的 **inspect** 命令（**policy-map** 命令）启用检测引擎时，您还可以选择启用 **policy-map type inspect** 命令创建的检测策略映射中定义的操作。例如，输入 **inspect http http_policy_map** 命令，其中 **http_policy_map** 是检测策略映射的名称。

检测策略映射包含在策略映射配置模式下输入的以下一个或多个命令组成。检查策略图可用的确切命令取决于应用程序。

- **match** 命令 - 您可以直接在检测策略映射中定义 **match** 命令，以便将应用流量与特定于应用的条件（例如 URL 字符串）进行匹配。然后，在匹配配置模式下启用操作，例如 **drop**、**reset**、**log** 等。可用的 **match** 命令取决于应用程序。
- **class** 命令 - 此命令标识策略映射中的检测类映射（请参阅 **class-map type inspect** 命令以创建检测类映射）。检测类映射包括 **match** 命令，这些命令将应用流量与应用特定的条件（例如 URL 字符串）进行匹配，然后可在策略映射中为其启用操作。创建类映射和直接在检查策略映射中使用 **match** 命令之间的区别在于，您可以对多个匹配进行分组，并且可以重复使用类映射。
- **parameters** 命令——参数影响检查引擎的行为。参数配置模式下可用的命令取决于应用。

您可以在策略映射中指定多个 **class** 或 **match** 命令。

有些 **match** 命令可以指定正则表达式来匹配数据包内的文本。请参阅 **regex** 命令和 **class-map type regex** 命令，它将多个正则表达式分组。

默认检查策略图配置包括以下命令：

```
policy-map type inspect dns preset_dns_map
  parameters
```

```

message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite

```

如果数据包与多个 **match** 不同的命令匹 **class** 配，则 ASA 应用操作的顺序由内部 ASA 规则决定，而不是由它们添加到策略映射的顺序决定。内部规则由应用类型和解析数据包的逻辑顺序确定，并且不可由用户配置。例如，对于 HTTP 流量，解析 Request Method 字段优先于解析 Header Host Length 字段；Request Method 字段的操作早于 Header Host Length 字段的操作。例如，以下匹配命令可以按任意顺序输入，但该 **matchrequestmethodget** 命令首先匹配。

```

ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log

```

如果某个操作丢弃了一个数据包，则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 **match** 的命令。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 **match** 命令同时配置 **reset**（或 **drop-connection** 等。）和 **log** 操作，在这种情况下，将在针对给定匹配重置数据包之前记录数据包。）

如果数据包匹配多个 **match** 或 **class** 相同的命令，则按照它们在策略图中出现的顺序进行匹配。例如，如果一个数据包的报头长度为 1001，则该数据包匹配以下第一个命令，执行记录，然后再匹配第二个命令并进行重置。如果您颠倒这两 **match** 个命令的顺序，那么在数据包能够匹配第二个命令之前，它将被丢弃并且连接将被重 **match** 置；它将永远不会被记录。

```

ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset

```

根据类映射中优先级最低的 **match** 命令来确定一个类映射是否与另一个类映射或 **match** 命令属于同一类型（优先级基于内部规则）。如果一个类映射具有与另一个类映射相同类型的最低优 **match** 优先级命令，则类映射将按照添加到策略映射的顺序进行匹配。如果每个类映射的最低优先级命令不同，则首先匹配 **match** 具有较高优先级命令的类映射。

如果要将正在使用的检查策略映射交换为不同的 **inspect** 映射名称，则必须删除协议映射命令，然后使用新映射再次输入该命令。例如：

```

ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# noinspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2

```

CR_Examples

以下是 HTTP 检测策略映射和相关类映射的示例。此策略映射由第 3/4 层策略映射激活，而第 3/4 层策略映射由服务策略启用。

```

ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# matchregexexample
ciscoasa(config-cmap)# matchregexexample2

```

```
ciscoasa(config-cmap) # class-map type inspect http match-all http-traffic
ciscoasa(config-cmap) # match req-resp content-type mismatch
ciscoasa(config-cmap) # match request body length gt 1000
ciscoasa(config-cmap) # match not request uri regex class URLs
ciscoasa(config-cmap) # policy-map type inspect http http-map1
ciscoasa(config-pmap) # class http-traffic
ciscoasa(config-pmap-c) # drop-connection log
ciscoasa(config-pmap-c) # match req-resp content-type mismatch
ciscoasa(config-pmap-c) # reset log
ciscoasa(config-pmap-c) # parameters
ciscoasa(config-pmap-p) # protocol-violation action log
ciscoasa(config-pmap-p) # policy-map test
ciscoasa(config-pmap) # class test
(a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c) # inspect http http-map1
ciscoasa(config-pmap-c) # service-policy inbound_policy interface outside
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
parameters	进入检查策略图的参数配置模式。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

policy-route

要在接口上配置基于策略的路由，请在接口配置模式下使用 **policy-route** 命令。

```
policy-route {route-maproute_map_name | cost值 | path-monitoring{IPv4 | IPv6 | auto |
auto4 | auto6}
no policy-route {route-maproute_map_name | cost值 | path-monitoring{IPv4 | IPv6 | auto
| auto4 | auto6}}
```

Syntax Description	costvalue	为基于策略的路由评估设置接口的相对开销。值可以是 1-65535。默认值为 0，您可以使用命令中的 no 版本进行重置。数值越低，优先级越高。例如，1 的优先级高于 2。
	route-maproute_map_name	指定要用于基于策略的路由的路由映射的名称。
	path-monitoring	设置接口对等体的监控类型以收集灵活的指标。

Command Default 没有默认路由映射。默认成本为 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
接口配置	• 是	—	• 是	• 支持	—

Command History	版本 修改
	9.4(1) 添加了此命令。
	9.17(1) 添加了 cost 关键字。
	9.18(1) 此命令已增强，包括用于 PBR 的路径监控功能，以确定路由流量的最佳路径。

使用指南 配置指定匹配条件的路由映射以及在所有匹配子句得到满足时生成的操作后，使用 **policy-route route-map** 命令将其应用于特定接口。

如果在路由图中使用 **set adaptive-interface cost** 它作为标准，请使用命令设置接口上的 **policy-route cost** 成本。

当您设置策略-路由成本，并在路由映射中使用 **set adaptive-interface cost** 命令时，出口流量将在具有相同接口成本的任何选定接口（假设它们处于启用状态）之间进行循环负载均衡。如果成本不同，则使用成本较高的接口作为成本最低的接口的备选。

例如，通过在 2 个 WAN 链路上设置相同的成本，您可以负载均衡这些链路上的流量以提高性能。但是，如果一条 WAN 链路的带宽高于另一条 WAN 链路，则可以将带宽较高的链路的成本设置为 1，将带宽较低的链路设置为 2，以便仅在带宽较高的链路关闭时使用带宽较低的链路。

CR_Examples

以下示例将路由映射应用于基于策略的路由的接口。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmapv4
ciscoasa(config)# show run interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  policy-route route-map testmapv4
!
ciscoasa(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
  Match clauses:
    ip address (access-lists): testaclv4
  Set clauses:
    ip next-hop 1.1.1.1
```

以下示例设置了不平等的成本，因此 output1 是首选链接，并且仅当 output1 发生故障时才使用 output2。要跨接口配置负载均衡，请设置相等开销值。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

路径监控功能检测到不再转发流量的路由链路或路径存在故障。它使威胁防御能够收集 RTT、抖动、丢包和平均意见得分 (MOS) 等性能指标，以确定转发流量的最佳路径。

要配置路径监控，请使用 **policy-route** 命令。您必须指定设备从对等网关收集性能指标时必须使用的监控类型。对于自动选项，默认路由的下一跳将用作要监控的对等体。首先尝试 IPv4，然后尝试 IPv6。对于 VTI 接口，不支持 auto 选项。必须指定其对等体的 IPv4 或 IPv6 地址。

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost          set interface cost
  path-monitoring Keyword for path monitoring
  route-map     Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D       peer-ipv4
  X:X:X:X:X     peer-ipv6
  auto          Use remote peer IPv4/6 based on config
  auto4         Use only IPv4 address based on config
  auto6         Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

policy-server-secret (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

如要配置用于加密发送到 SiteMinder SSO 服务器的身份验证请求的密钥，请在 webvpn-ss0-siteminder 配置模式下使用 **policy-server-secret** 命令。要删除密钥，请使用此 **no**命令的形式。

```
policy-server-secret secret-key
no policy-server-secret
```



注释 SiteMinder SSO 身份验证需要此命令。

Syntax Description

secret-key 用作加密身份验证通信的密钥的字符串。无字符最小或最大数量限制。

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
配置模式	• 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。您首先使用 **ss0-server** 命令创建 SSO 服务器。对于 SiteMinder SSO 服务器，**policy-server-secret** 命令可保护 ASA 与 SSO 服务器之间的身份验证通信。

命令参数 *secret-key*类似于密码：您创建它、保存它并配置它。它在 ASA 上使用命令进行配置，并在 **policy-server-secret** SiteMinder 策略服务器上使用 Cisco Java 插件身份验证方案进行配置。

此命令仅适用于 SiteMinder 类型的 SSO 服务器。

CR_Examples

在 config-webvpn-sso-siteminder 模式下输入的以下命令包含一个随机字符串作为参数，用于创建 SiteMinder SSO 服务器身份验证通信的密钥：

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

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。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息
sso-server	创建单点登录服务器。
test sso-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。

policy static sgt

要将策略应用于手动配置的思科 TrustSec 链路，请在 cts 手动接口配置模式下使用 **policy static sgt** 命令。要删除手动配置的 CTS 链路下的策略，请使用此命令的 **no** 形式。

```
policy static sgtsgt_number [ trusted ]
no policy static sgtsgt_number [ trusted ]
```

Syntax Description	sgtsgt_number 指定应用于来自对等方的传入流量的 SGT 编号。有效值为 2 到 65519。
static	为链路上的传入流量指定 SGT 策略。
trusted	表示命令中指定的 SGT 的接口上的入口流量不应被其 SGT 覆盖。默认设置为 Untrusted。

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
Cts 手动接口配置	• 是	• 支持	• 支持	• 支持	—

Command History	版本 修改
	9.3(1) 添加了此命令。

使用指南 此命令将策略应用于手动配置的 CTS 链接。

限制

- 仅支持物理接口、VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI、TVI 和 VNI。

CR_Examples 以下示例为第 2 层 SGT 实施启用接口并定义此接口是否可信：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Related Commands

命令	说明
ctsmanual	启用第 2 层 SGT 强制并进入 cts 手动接口配置模式。
propagatesgt	在接口上传播安全组标签（称为 sgt ）。默认情况下，传送被启用。

polltime interface

要在主用/主用故障转移配置中指定数据接口轮询时间和保持时间，请在故障转移组配置模式下使用 **polltime interface** 命令。要恢复默认值，请使用此命令的形式。

轮询**polltime interface [msec] [holdtime时 间]**
轮询**no polltime interface [msec] [holdtime时 间]**

Syntax Description

holdtime时 间 （可选）设置从对等单元最后收到的 **hello** 消息与开始接口测试之间的时间（作为计算），以确定接口的健康状况。它还将每次接口测试的持续时间设置为保持时间/16。有效值范围为 5 至 75 秒。默认值是 *polltime* 的 5 倍。您不能输入小于轮询时间五倍的保持时间值。

要计算开始接口测试之前的时间（y），请执行以下操作：

1. $x = (holdtime / polltime) / 2$ ，四舍五入到最接近的整数。（.4 和向下四舍五入；0.5 和向上四舍五入。）

2. $y = x * polltime$

例如，如果使用默认保持时间25和轮询时间5，则y = 15秒。

interface时 间 指定向对等方发送 **hello** 数据包之间等待的时间。有效值范围为 1 至 15 秒。默认值为 5。如果使用可选关 **msec**键字，则有效值为 500 至 999 毫秒。

msec （可选）指定给定时间，以毫秒为单位。

Command Default

轮询 时间为5秒。

holdtime时间 为轮询 时间 的5 倍。

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。

7.2(1) 已更改命令，以包含可选的 **holdtime**时间 值，并且可以以毫秒为单位指定轮询时间。

此命令仅适用于主用/主用故障转移。请在主用/备用故障转移配置中使用 **failoverpolltimeinterface** 命令。

通过更快的轮询时间，ASA 可以更快地检测故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

您可以在配置中同时包含 **polltimeunit** 和 **polltimeinterface** 命令。



注释 当 CTIQBE 流量通过故障转移配置中的 ASA 时，应将 ASA 上的故障转移保持时间减少到 30 秒以下。CTIQBE 保持连接超时为 30 秒，并且在故障转移情况下可能在发生故障转移之前超时。如果 CTIQBE 超时，与思科 CallManager 的思科 IP SoftPhone 连接将被丢弃，并且 IP SoftPhone 客户端需要向 CallManager 重新注册。

CR_Examples

以下部分示例显示了故障转移组的一种可能配置。对于故障转移组 1 中的数据接口，接口轮询时间设置为 500 毫秒，保持时间设置为 5 秒。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failoverpolltime	指定设备故障转移轮询和保持时间。
failoverpolltimeinterface	指定主用/备用故障转移配置的接口轮询和保持时间。

poll-timer

要指定 ASA 在多长时间內查询 DNS 服务器以解析网络对象组中定义的完全限定域名 (FQDN)，请在 dns 服务器组配置模式下仅对 DefaultDNS 服务器组使用 **poll-timer** 命令。要删除计时器，请使用此命令 **no** 的形式。

poll-timer minutes分钟
no poll-timer minutes分钟

Syntax Description

minutes分 指定计时器（以分钟为单位）。有效值为 1 至 65535 分钟。
钟

Command Default

默认情况下，DNS 计时器为 240 分钟或 4 小时。

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
dns server-group 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本 修改
8.4(2) 添加了此命令。

使用指南

此命令仅支持 DefaultDNS 服务器组。
此命令指定 ASA 查询 DNS 服务器以解析网络对象组中定义的 FQDN 的计时器。当轮询 DNS 计时器到期或已解析 IP 条目的 TTL 到期时（以先到者为准），会定期解析 FQDN。
此命令仅当至少激活一个网络对象组时才生效。

CR Examples

以下示例将 DNS 轮询计时器设置为 240 分钟：

```
ciscoasa(config)# dns server-group DefaultDNS  
ciscoasa(config-dns-server-group)# poll-timer minutes 240
```

Related Commands

命令	说明
clearconfiguredns	删除所有 DNS 命令。

命令	说明
dnsserver-group	进入 dns-server-group 模式，在此模式下，您可以配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有的 DNS 服务器组配置。

pop3s (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要进入POP3S配置模式，请使用全局配置模式下的 **pop3s** 命令。要删除在 POP3S 命令模式下输入的任何命令，请使用此命令的 **no**版本。

POP3 是一种客户端/服务器协议，您的互联网服务器可以使用该协议接收并保留邮件。您（或您的客户端邮件收件人）应定期检查服务器上的邮箱并下载所有邮件。此标准协议内置于大多数常用邮件产品中。POP3S 使您可以通过 SSL 连接接收邮件。

pop3s
no pop3

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
全局配置	• 是	• 支持	—	—	• 是

Command History 版本 修改

7.0(1) 添加了此命令。

9.5(2) 此命令已弃用。

CR_Examples

以下示例显示如何进入 POP3S 配置模式：

```
ciscoasa
(config)#
pop3s
ciscoasa(config-pop3s)#
```

Related Commands

命令	说明
clearconfigurepop3s	删除 POP3S 配置。

命令	说明
showrunning-configpop3s	显示 POP3S 的运行配置。

port (已弃用)



注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定邮件代理侦听的端口，请在适用的邮件代理命令模式下使用 **port** 命令。要恢复默认值，请使用此命令的 **no** 版本。

port*portnum*
no port

Syntax Description

portnum 供邮件代理要使用的端口。为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

Command Default

邮件代理的默认端口如下：

邮件代理	默认端口
IMAP4S	993
POP3S	995
SMTPS	988

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
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

Command History

版本 修改

7.0(1) 添加了此命令。

9.5(2) 此命令已弃用。

使用指南

为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

CR_Examples

以下示例显示如何为 IMAP4S 邮件代理设置端口 1066：

```
ciscoasa
(config)#
  imap4s
ciscoasa(config-imap4s)# port 1066
```

portal-access-rule（已弃用）

此命令允许客户配置全局无客户端 SSL VPN 访问策略，以根据 HTTP 标头中的数据允许或拒绝无客户端 SSL VPN 会话。如果访问遭到拒绝，系统会向客户端返回错误代码。由于此拒绝操作是在用户身份验证之前发生的，所以可以减少处理资源的使用。

```
portal-access-rule none
no portal-access-rule priority [ { permit | deny [ codecode ] } { any | user-agent match string }
no portal-access-rule priority [ { permit | deny [ codecode ] } { any | user-agent match string } ]
clear configure webvpn portal-access-rule
```

Syntax Description

无	删除所有门户访问规则。无客户端 SSL VPN 会话不会基于 HTTP 报头进行限制。
priority	规则的优先级。范围：1-65535。
permit	允许基于 HTTP 标头进行访问。
deny	根据 HTTP 标头拒绝访问。
代码	根据返回的 HTTP 状态代码允许或拒绝访问。默认值：403。
code	允许或拒绝访问所依据的 HTTP 状态代码编号。范围：200-599。
任意	匹配任何 HTTP 报头字符串。
user-agent match	启用 HTTP 报头中字符串的比较。
string	在 HTTP 报头中指定要匹配的字符串。对于包含您的字符串的匹配项，使用通配符 (*) 将您要搜索的字符串括起来，或者不使用通配符指定您的字符串的精确匹配项。 注释 建议在搜索字符串中使用通配符。如果没有它们，规则可能无法匹配任何字符串，或者匹配的字符串可能比您预期的要少得多。 如果您要搜索的字符串中包含空格，则必须将该字符串括在引号中；例如“a string”。同时使用引号和通配符时，搜索字符串将如下所示：“*a string*”。
no portal-access-rule	使用 来删除单个门户访问规则。
清除配置 webvpn 门户访问规则	相当于 portal-access-rule none 命令。

Command Default

portal-access-rulenone

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配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.2(5)	此命令同时添加到 ASA 8.2.5 和 8.4(2) 中。
8.4(2)	此命令同时添加到 ASA 8.2.5 和 8.4(2) 中。
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

此检查在用户身份验证之前执行。

CR_Examples

以下示例创建三个门户访问规则：

- 当 ASA 返回代码 403 且 Thunderbird 位于 HTTP 报头中时，门户访问规则 1 拒绝尝试的无客户端 SSL VPN 连接。
- 当 MSIE 8.0 (Microsoft Internet Explorer 8.0) 在 HTTP 报头中时，门户访问规则 10 允许尝试的无客户端 SSL VPN 连接。
- 门户访问规则 65535 允许所有其他尝试的无客户端 SSL VPN 连接。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```



注释 如果已安装 HostScan，则端口访问规则功能不会阻止 ASA 打开思科安全桌面门户等页面。为了避免思科安全桌面端口，需要卸载 HostScan。

Related Commands

命令	说明
showrunwebvpn	显示 webvpn 配置，包括所有门户访问规则。
showvpn-sessiondbdetailwebvpn	显示有关 VPN 会话的信息。命令包括用于完整或详细显示信息的选项，可让您指定要显示的会话的类型，并提供用于对信息进行过滤和排序的选项。

命令	说明
debugwebvpnrequestn	启用特定调试级别的调试消息的日志记录。默认值：1。范围：1-255。

port-channel load-balance

对于 EtherChannel，要指定负载均衡算法，请在接口配置模式下使用 **port-channel load-balance** 命令。要将值设置为默认值，请使用此命令 **no** 的形式。



注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

```
port-channel <id> <ip> <mac> <dst-ip> <dst-ip-port> <dst-mac> <dst-port> <src-dst-ip> <src-dst-ip-port>
no port-channel load-balance
```

Syntax Description	dst-ip	根据数据包的以下特征来均衡接口上的数据包负载： 目标 IP 地址 (Destination IP address)
	dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： - 目标 IP 地址 (Destination IP address) - 目标端口 (Destination Port)
	dst-mac	根据数据包的以下特征来均衡接口上的数据包负载： 目标 MAC 地址
	dst-port	根据数据包的以下特征来均衡接口上的数据包负载： 目标端口
	src-dst-ip	(默认) 根据数据包的以下特征来均衡接口上的数据包负载： - 源 IP 地址 - 目的 IP 地址
	src-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： - 源 IP 地址 - 目的 IP 地址 - 源端口 (Source Port) - 目的端口

src-dst-mac	根据数据包的以下特征来均衡接口上的数据包负载： • 源 MAC 地址 • 目的 MAC 地址
src-dst-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源端口 • 目的端口
src-ip	根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址
src-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址 • 源端口
src-mac	根据数据包的以下特征来均衡接口上的数据包负载： • 源 MAC 地址
src-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源端口
vlan-dst-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 目标 IP 地址 (Destination IP address)
vlan-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 目标 IP 地址 (Destination IP address) • 目标端口
vlan-only	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN

vlan-src-dst-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目的 IP 地址
vlan-src-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目的 IP 地址 • 源端口 • 目的端口
vlan-src-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址
vlan-src-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 源端口

Command Default

默认值为 **src-dst-ip**。

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	• 支持	• 支持	—	• 是

Command History

版本 修改

8.4(1) 添加了此命令。

使用指南

ASA 通过对数据包的源和目标 IP 地址进行哈希处理 (**src-dst-ip**) 将数据包分发到 EtherChannel 中的接口。在模数运算中, 将得到的散列值除以主用链路数, 得到的余数确定哪个接口拥有流量。

$hash\_value \bmod active\_links$ 结果为 0 的所有数据包都将转到 EtherChannel 中的第一个接口, 结果为 1 的数据包将转到第二个接口, 结果为 2 的数据包将转到第三个接口, 依此类推。例如, 如果您有 15 个主用链路, 则模数运算的值为 0 到 14。如果有 6 个主用链路, 则值为 0 到 5, 依此类推。

对于集群中跨网络 EtherChannel, 系统会逐个 ASA 进行负载均衡。例如, 如果 8 个 ASA 之间的跨网络 EtherChannel 中有 32 个主用接口, 而 EtherChannel 中的每个 ASA 又有 4 个接口, 则仅会在 ASA 上的 4 个接口之间进行负载均衡。

如果主用接口发生故障且未由备用接口替代, 则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽, 因此故障转移对其他网络设备是透明的。

CR_Examples

以下示例将负载均衡算法设置为使用源及目标 IP 地址和端口:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载均衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息 (例如流量统计信息)、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

port-channel min-bundle

对于以太网通道，要指定端口通道接口变为活动状态所需的最小活动接口数，请在**port-channel min-bundle** 接口配置模式下使用该命令。要将值设置为默认值，请使用此命令的形式。



注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

port-channel*min-bundle**number*
no port-channel*min-bundle*

Syntax Description	<i>number</i> 指定端口通道接口变为活动状态所需的最小活动接口数（介于 1 和 8 之间）；对于 9.2(1) 及更高版本，活动接口可介于 1 和 16 之间。

Command Default	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
接口配置	• 是	• 支持	• 支持	—	• 是

Command History	版本 修改
	8.4(1) 添加了此命令。
	9.2(1) 主用接口数量从 8 增加到 16。

使用指南	为端口通道接口输入此命令。如果通道组中的主用接口数小于此值，则端口通道接口将会发生故障，并可能会触发设备级故障转移。

CR_Examples	以下示例将端口通道变为活动状态所需的最小活动接口数设置为两个：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

Related Commands	命令	说明
	channel-group	将接口添加到以太网通道。

命令	说明
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacsytem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

port-channel span-cluster

要在 ASA 集群中将此 EtherChannel 设置为跨区以太网通道，请在接口配置模式下使用 **port-channelspan-cluster** 命令。要禁用跨越，请使用此命令的形式。



注释 仅在 ASA 硬件型号上受支持。其他型号隐式将数据 EtherChannel 设置为跨区模式。

port-channel span-cluster [**vss-load-balance**]
no port-channel span-cluster [**vss-load-balance**]

Syntax Description

vss-load-balance （可选）启用 VSS 负载均衡。如果将 ASA 连接到 VSS 或 vPC 中的两个交换机，则应启用 VSS 负载平衡。此功能可确保 ASA 与 VSS（或 vPC）对之间的物理链路连接实现均衡。启用 **vss-id** 负载均衡前，必须为每个成员接口配置命令中 **channel-group** 的关键字。

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
接口配置	• 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

您必须处于跨区以太网通道模式 (**clusterinterface-modespanned**) 才能使用此功能。

此功能允许您将每个单元的一个或多个接口分组到跨集群中所有单元的以太网通道中。EtherChannel 汇聚通道中所有可用活动接口上的流量。跨网以太网通道可以在路由和透明防火墙模式下配置。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配给桥接组，而不是接口。负载均衡属于 EtherChannel 固有的基本操作。

CR_Examples

以下示例创建 EtherChannel（端口通道 2），并将 **tengigabitethernet 0/8** 接口作为唯一成员，然后在整个集群中扩展 EtherChannel。两个子接口添加到端口通道 2。

```
interface tengigabitethernet 0/8
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Related Commands

命令	说明
interface	进入接口配置模式。
clusterinterface-mode	为跨网络 EtherChannel 或单个接口设置集群接口模式。

port-forward（已弃用）

要配置无客户端 SSL VPN 会话用户可通过转发的 TCP 端口访问的应用集，请在 webvpn 配置模式下使用 **port-forward** 命令。

port-forward { *list_name* *local_port* *remote_server* *remote_port* *description* }

要配置对多个应用的访问权限，请多次将此命令与相同的 *list_name* 配合使用，每个应用一次。

要从列表中删除已配置应用，请使用 **no port-forward** *list_name* *local_port* 命令（无需包括 *remote_server* 和 *remote_port* 参数）。

no port-forward *list_name* *local_port*

要删除整个配置的列表，请使用 **no port-forward** *list_name* 命令。

no port-forward *list_name*

Syntax Description

<i>description</i>	提供在最终用户端口转发 Java 小程序屏幕上显示的应用名称或简短说明。最多 64 个字符。
<i>list_name</i>	无客户端 SSL VPN 会话用户可以访问的应用集（转发的 TCP 端口）的组。最多 64 个字符。
<i>local_port</i>	指定侦听应用程序 TCP 流量的本地端口。对于 <i>list_name</i> ，您只能使用一次本地端口号。输入 1-65535 范围内的端口号。如要避免与现有服务冲突，请使用大于 1024 的端口号。
<i>remote_port</i>	指定此应用在远程服务器上的连接端口。这是应用使用的实际端口。请输入 1-65535 范围内的端口号或端口名称。
<i>remote_server</i>	为应用程序提供远程服务器的 DNS 名称或 IP 地址。如果输入 IP 地址，可以使用 IPv4 或 IPv6 格式输入。我们建议使用主机名，这样您就不必为特定的 IP 地址配置客户端应用程序。dns server-group 命令 name-server 必须将主机名解析为 IP 地址。

Command Default

没有默认端口转发列表。

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配置模式	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.0(2)	命令模式已更改为 webvpn。
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

端口转发不支持 Microsoft Outlook Exchange (MAPI) 代理。但是，您可以为 Microsoft Outlook Exchange 2010 配置智能隧道支持。

CR_Examples

下表显示用于示例应用的值。

应用程序	本地端口	服务器 DNS 名称	远程端口	说明
IMAP4S 邮件	20143	IMAP4S 服务器	143	获取邮件
SMTPS 邮件	20025	SMTPS 服务器	25	发送邮件
基于 SSH 的 DDTS	20022	DDTS 服务器	22	基于 SSH 的 DDTS
Telnet	20023	Telnet服务器	23	Telnet

以下示例显示如何创建名为 *SalesGroupPorts* 的端口转发列表，该列表提供对这些应用的访问：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

Related Commands

命令	说明
port-forwardauto-start	此命令是在 group-policy webvpn 或 username webvpn 模式下输入的，可以自动启动端口转发，并在用户登录无客户端 SSL VPN 会话时分配指定的端口转发列表。

命令	说明
port-forwardenable	此命令在组策略 webvpn 或用户名 webvpn 模式下输入后，将在用户登录时开始分配指定的端口转发列表，但要求用户使用无客户端 SSL VPN 门户上的 ApplicationAccess = StartApplications 按钮手动启动端口转发。页面上。
port-forwarddisable	在 group-policy webvpn 或 username webvpn 模式下输入此命令可关闭端口转发。

port-forward-name（已弃用）

要为特定用户或策略组配置标识TCP端口转发到最终用户的显示名称，请在port-forward-namewebvpn模式下使用从组策略或用户名模式输入的命令。要删除显示名称（包括使用该命令创建的port-forward-namename空值），请使用该命令的no形式。该no选项恢复默认名称“应用程序访问”。要防止显示名称，请使用该port-forwardnone命令。

```
port-forward-name { valuename | none }
no port-forward-name
```

Syntax Description	none	表示无显示名称。设置空值，从而不允许显示名称。防止继承值。
	valuename	向最终用户介绍端口转发。最多 255 个字符。

Command Default	默认名称是“应用程序访问”。

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	• 是	—	• 是	—	—

Command History	版本	修改
	7.0(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。

CR_Examples 以下示例显示如何为名为FirstGroup的组策略设置名称“远程访问 TCP 应用程序”：

```
ciscoasa
(config)#
group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

Related Commands	命令	说明
	webvpn	在组策略配置模式或用户名配置模式下使用。让您可以进入 WebVPN模式以配置应用于组策略或用户名的参数。

命令	说明
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

端口对象

要将端口对象添加至 TCP、UDP 或 TCP-UDP 类型的服务对象组，请在 `object-group` 服务配置模式下使用 `port-object` 命令。要删除端口对象，请使用此命令的 `no` 形式。

```
port-object {eqport | rangebegin_portend_port}
no port-object {eqport | rangebegin_portend_port}
```

Syntax Description	rangebegin_port end_port 指定端口范围（含 0 和 65535）。				
eq端口	指定服务对象的十进制数（介于 0 和 65535 之间）或 TCP 或 UDP 端口名称。				

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
对象网络服务配置	• 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 `port-object` 命令与 `object-group service protocol` 命令配合使用，定义为特定端口或端口范围的对象。

如果为 TCP 或 UDP 服务指定了名称，则名称必须是受支持的 TCP 或/和 UDP 名称之一，并且必须与对象组的协议类型一致。例如，对于 `tcp`、`udp` 和 `tcp-udp` 协议类型，`names` 必须分别为有效的 TCP 服务名称、有效的 UDP 服务名称或有效的 TCP 和 UDP 服务名称。

如果指定了编号，则在显示对象时，将根据协议类型转换为其相应名称（如果存在）。

支持以下服务名称：

TCP	UDP	TCP 和 UDP
bgp	biff	discard
chargen	bootpc	domain

TCP	UDP	TCP 和 UDP
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
EXEC	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

CR_Examples

此示例显示如何在服务配置模式下使用 **port-object** 命令创建新的端口（服务）对象组：

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

Related Commands

命令	说明
clearconfigureobject-group	从配置中 object-group 删除所有命令。
group-object	添加网络对象组。
network-object	向网络对象组添加网络对象。
object-group	定义对象组以优化您的配置。
showrunning-configobject-group	显示当前对象组。

post-max-size

要指定允许发布的对象的最大大小，请在 **post-max-size** 组策略 webvpn 配置模式下使用该命令。要从配置中删除此对象，请使用此命令的 **no** 版本。

post-max-size *size*
no post-max-size

Syntax Description

size 指定允许发布对象的最大大小。范围为 0 到 2147483647。将大小设置为 0 可以有效地禁止对象发布。

Command Default

默认大小为 2147483647。

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
组策略 webvpn 配置模式	• 是	—	• 是	—	—

Command History

版本 修改

8.0(2) 添加了此命令。

CR_Examples

以下示例将发布对象的最大大小设置为 1500 字节：

```
ciscoasa
(config)#
group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
post-max-size 1500
```

Related Commands

命令	说明
download-max-size	指定要下载的对象的最大大小。
upload-max-size	指定要上传的对象的最大大小。

命令	说明
webvpn	在组策略配置模式或用户名配置模式下使用。让您可以进入 WebVPN 模式以配置应用于组策略或用户名的参数。
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

内嵌式电源

要在支持的端口上启用或禁用以太网供电 (PoE)，请在接口配置模式下使用 **powerinline** 命令。要返回默认状态，请使用此命令 **no** 的形式。

power inline { **auto** | **never** | **consumption wattage** 毫瓦 }



注释 仅支持 5505、1010 和 1210CP。不支持 1010E/1210CE/1220CX。

Syntax Description

consumptionwattage 手动指定瓦数（毫瓦），从 4000 到 30000（1010）或 90000（1210CP）。如果您要手动设置功率而不是使用通过 LLDP 协商的功率，请使用此命令。

auto 使用适合受电设备类别的功率自动向受电设备供电。防火墙使用 LLDP 进一步协商正确的瓦数。当连接某个类别的设备时，它会被调配到该等级的最大功率，以防需要使用更多电能。例如，如果您添加请求的功率为 12.95W 的 4 类设备，即使它当前没有使用该功率，系统也会为其分配 30W。某些设备可以重新协商电源需求。如果您知道您的设备所需的电量少于分配的电量，您可以 **consumption wattage** 手动设置以释放电量用于其他设备。

never 禁用 PoE。

Command Default

默认值为 **auto**。

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	• 支持	• 支持	—	• 是

Command History

版本 修改

7.2(1) 添加了此命令。

9.13(1) 增加了对 Firepower 1010 的支持。

9.22(1) 增加了对 Cisco Secure Firewall 1210CP 的支持。

9.23(1) 1210CP 增加了对 IEEE 802.3bt（PoE++ 和 Hi-PoE）的支持，以及每端口最高 90 瓦的功率。还增加了对多上下文模式的支持。

使用指南

- PoE 在以下端口上可用：
- ASA 5505 - 以太网 0/6 和以太网 0/7 使用 IEEE 802.3af (PoE)，每个端口最高 15 瓦，总计最高 30 瓦。
 - Firepower 1010 - 使用 IEEE 802.3af (PoE) 和 802.3at (PoE+) 的以太网 1/7 和 1/8，每个端口最高 30 瓦，总功率最高 60 瓦。
 - Cisco Secure Firewall 1210CP - 以太网 1/5、1/6、1/7 和 1/8，使用 IEEE 802.3af (PoE)、802.3at (PoE+)和 802.3bt (PoE++ 和 Hi-PoE)，每个端口最高 90 瓦，合计最高 120 瓦。



注释 1010E、1210CE 和 1220CX 不支持 PoE。

PoE+ 或更高版本使用链路层发现协议 (LLDP) 来协商功率级别。仅在需要时提供功率。
如果关闭接口，则会禁用设备电源。

CR_Examples

以下示例为以太网 1/7 手动设置功率，为以太网 1/8 设置功率为自动：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

Related Commands

命令	说明
showpowerinline	显示 PoE 状态。

power-supply

对于 ISA 3000 中的双电源，要在 ASA OS 中将双电源建立为预期配置，请在全局配置模式下使用该 **power-supply** 命令。要禁用双电源，请使用此命令的 **no** 形式。

power-supply dual
no power-supply dual

Syntax Description

dual 指定双电源。

Command Default

默认情况下，双电源处于禁用状态。

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	—	—

Command History

版本 修改

9.6(1) 我们引入了此命令。

使用指南

如果其中一个电源发生故障，ASA 会发出报警。默认情况下，ASA 需要单个电源，只要它包含一个工作电源，就不会发出警报。

CR_Examples

以下示例建立双电源：

```
ciscoasa(config)# power-supply dual
```

pppoe client route distance

要配置通过 PPPoE 获知的路由的管理距离，请在接口配置模式下使用 **pppoeclientroutedistance** 命令。要恢复默认设置，请使用此命令 **no** 的形式。

```
pppoe client route distance distance
no pppoe client route distance distance
```

Syntax Description *distance* 要应用于通过 PPPoE 学习的路由的管理距离。有效值为从 1 到 255。

Command Default 默认情况下，通过 PPPoE 获知的路由的管理距离为 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
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 仅当路由通过 PPPoE 获知时，才会检查 **pppoeclientroutedistance** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutedistance** 命令，则指定的管理距离不会影响现有获知的路由。只有在输入命令后获知的路由才具有指定的管理距离。

您必须在 [**ipaddresspppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。在多个接口上启用 PPPoE 客户端仅支持对象跟踪。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples 以下示例通过 GigabitEthernet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
ppoeclientroutetrack	关联通过 PPPoE 获知的路由与跟踪条目对象。
slamonitor	定义 SLA 监控操作。
trackrtr	创建跟踪条目以轮询 SLA。

pppoe client route track

如要将 PPPoE 客户端配置为将添加的路由与指定的被跟踪对象编号相关联，请在接口配置模式下使用 **pppoe client route track** 命令。要删除 PPPoE 路由跟踪，请使用此命令的形式。

pppoe client route track 编号
no pppoe client route track

Syntax Description *number* 跟踪条目对象 ID。有效值范围为 1 至 500。

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
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 仅当路由通过 PPPoE 获知时，才会检查 **pppoeclientroutetrack** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutetrack** 命令，则现有的获知路由不与跟踪对象关联。只有在输入 命令后获知路由才能与指定的跟踪对象关联。

您必须在 [**ipaddresspppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。仅对象跟踪支持在多个接口上启用 PPPoE 客户端。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples 以下示例通过 GigabitEthernet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
ppoeclientroutedistance	为通过 PPPoE 获知的路由分配管理距离。
slamonitor	定义 SLA 监控操作。
trackrtr	创建跟踪条目以轮询 SLA。

pppoe client secondary

如要将 PPPoE 客户端配置为注册为被跟踪对象的客户端，并根据跟踪状态启动或关闭，请在接口配置模式下使用 **pppoeclientsecondary** 命令。要删除客户端注册，请使用此命令 **no** 的形式。

pppoe client secondary track编号
no pppoe client secondary track

Syntax Description *number* 跟踪条目对象 ID。有效值范围为 1 至 500。

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
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

仅当 PPPoE 会话启动时，才会检查 **pppoeclientsecondary** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutetrack**命令，则现有的获知路由不与跟踪对象关联。只有在输入 命令后获知的路由才能与指定的跟踪对象关联。

您必须在 [**ipaddresspppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。仅对象跟踪支持在多个接口上启用 PPPoE 客户端。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples

以下示例通过 GigabitEthernet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
ppoeclientroutedistance	为通过 PPPoE 获知的路由分配管理距离。
ppoeclientroutetrack	关联通过 PPPoE 获知的路由与跟踪条目对象。
slamonitor	定义 SLA 监控操作。

prc-interval

要自定义部分路由计算 (PRC) 的 IS-IS 限制，请在路由器 isis 配置模式下使用 **prc-interval** 命令。要恢复默认值，请使用此命令 **no** 的形式。

```
prc-interval prc-max-wait [prc-initial-wait prc-second-wait]
no prc-interval
```

Syntax Description	prc 最大等待 指示两次连续PRC计算之间的最大间隔。范围为 1 到 120 秒。
	prc-initial-wait （可选）表示拓扑更改后的初始 PRC 计算延迟。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。
	prc-second-wait （可选）表示第一次和第二次 PRC 计算之间的保持时间（以毫秒为单位）。范围为 1 到 120,000 毫秒。

Command Default	默认值包括：
	prc-max-wait: 5 秒
	prc-initial-wait: 2000 毫秒
	prc-second-wait: 5000 毫秒

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
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	PRC 是一种不执行最短路径优先 (SPF) 计算的路由计算软件过程。当路由系统本身的拓扑结构没有改变，但在特定 IS 宣布的信息中检测到变化，或者当需要尝试在路由信息库 (RIB) 中重新安装此类路由时，这种情况是可能的。 以下说明有助于确定是否更改此命令的默认值： • prc-initial-wait 参数表示生成第一个 LSP 之前的初始等待时间（以毫秒为单位）。 • prc-second-wait 参数表示首次和第二个 LSP 生成之间的等待时长（以毫秒为单位）。

- 每个后续等待间隔都是前一个等待间隔的两倍，直到等待间隔达到指定的 *prcmax-wait* 为止，因此，在初始和第二个间隔之后，该值会导致 PRC 计算节流或减慢。一旦达到此间隔，等待间隔就会以此间隔继续，直到网络稳定下来。
- 网络平稳运行并且在两倍的 *prc-max-wait* 间隔内没有触发器后，快速行为将恢复（初始等待时间）。

CR_Examples

以下是 PRC 的间隔示例。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# prc-interval 2 50 100
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型

命令	说明
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置 LSP 刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。

命令	说明
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	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。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

prc-interval



pr - pz

- [pre-fill-username](#)，第 1327 页
- [preempt](#)，第 1329 页
- [prefix-list](#)，第 1331 页
- 前缀列表说明，第 1334 页
- 前缀列表序列号，第 1336 页
- [prf](#)，第 1337 页
- [primary](#)，第 1339 页
- [priority](#)（类别），第 1341 页
- [priority](#)（集群组），第 1344 页
- [priority](#)（VPN负载均衡），第 1346 页
- [priority-queue](#)，第 1348 页
- [privilege](#)，第 1350 页
- [profile](#)，第 1353 页
- [prompt](#)，第 1356 页
- [propagate sgt](#)，第 1358 页
- [protocol](#)，第 1360 页
- [protocol-enforcement](#)，第 1363 页
- [protocol http](#)，第 1365 页
- [protocol ldap](#)，第 1366 页
- [protocol-object](#)，第 1367 页
- [protocol scep](#)，第 1369 页
- [protocol shutdown](#)，第 1370 页
- [protocol-violation](#)，第 1371 页
- [proxy-auth](#)，第 1373 页
- [proxy-auth_map sdi](#)，第 1374 页
- [proxy-bypass](#)，第 1376 页
- [proxy-ldc-issuer](#)，第 1379 页
- [proxy paired](#)，第 1381 页
- [proxy-server](#) (已弃用)，第 1383 页
- [proxy single-arm](#)，第 1385 页

- [ptp domain](#) , 第 1387 页
- [ptp enable](#) , 第 1388 页
- [ptp 模式](#) , 第 1389 页
- [public-key](#) , 第 1390 页
- [publish-crl](#) , 第 1392 页
- [pwd](#) , 第 1394 页

pre-fill-username

要从客户端证书中提取用户名以用于身份验证和授权，请在 **pre-fill-username** 隧道组 webvpn-attributes 模式下使用该命令。要从配置中删除属性，请使用此命令 **no** 的形式。

pre-fill-username { **client** | **clientless** }
no pre-fill-username

Syntax Description	client 为 AnyConnect VPN 客户端连接启用此功能。在 9.8(1)+ 中，请使用 client 关键字。
	ssl-client
	clientless 为无客户端连接启用此功能。

Command Default 没有默认值或行为。

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
Tunnel-group webvpn-attributes 配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(4) 添加了此命令。
	9.8(1) 关键字 ssl-client 已更改为 client 。

使用指南 该命令允 **pre-fill-username** 许使用从命令中指定的证书字段中提取的 **username-from-certificate** 用户名作为用户名/密码认证和授权的用户名。如要使用证书功能中的此预填充用户名，必须配置这两个命令。

要启用此功能，您还必须在 tunnel-group general-attributes 模式下配置 **username-from-certificate** 命令。

CR_Examples 以下示例以全局配置模式输入，创建一个名为 remotegrp 的 IPsec 远程访问隧道组，并指定 SSL VPN 客户端的身份验证或授权查询的名称必须来自数字证书：

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

```
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

命令	说明
pre-fill-username	启用预填充用户名功能。
show running-config tunnel-group	显示指示的隧道组配置。
tunnel-group general-attributes	指定命名的隧道组的常规属性。
username-from-certificate	指定证书中用作授权用户名的字段。

preempt

要使故障转移组在首选设备上变成活动状态，请在故障转移组配置模式下使用 **preempt** 命令。要取消抢占，请使用此命 **no** 令的形式。

```
preempt [delay]
no preempt [delay]
```

Syntax Description *seconds* 对等设备抢占之前的等待时间（以秒为单位）。有效值范围为 1 至 1200 秒。

Command Default 默认情况下，没有延迟。

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。
9.0(1)	较早的软件版本中允许“同时”启动，以便故障转移组无需 preempt 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障转移组在要启动的第一台设备上都变为主用状态。

使用指南 将 **primary** 或 **secondary** 首选项分配给故障转移组可指定在设置 **preempt** 命令时故障转移组在哪个设备上将变为主用状态。两个故障转移组都会在第一个启动的单元上变为活动状态（即使看起来它们同时启动，但一个单元会先变为活动状态），无论该组的 **primary**或 **secondary**设置如何。当另一台设备上线时，将第二台设备作为优先级的任何故障转移组都不会在第二台设备上变为活动状态，除非故障转移组使用 **preempt** 命令进行了配置，或者使用 **nofailoveractive** 命令手动强制到另一台设备请参阅如果使用该命令配置了故障转移 **preempt**组，则故障转移组将在指定单元上自动变为活动状态。



注释 如果启用状态故障转移，则抢占会延迟，直到连接从当前处于主用状态的故障转移组所在的设备中复制为止。

CR_Examples

以下示例配置了故障转移组 1，其中主设备为较高优先级，并配置了故障转移组 2，其中辅助设备为较高优先级。两个故障转移组均使用 **preempt** 命令配置为 100 秒的等待时间，因此，在设备变为可用 100 秒后，两个组将在其首选设备上自动变为主用状态。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
primary	为正在配置的故障转移组的故障转移对中的主设备提供优先级。
secondary	为正在配置的故障转移组的故障转移对中的辅助设备提供优先级。

prefix-list

OSPFv2、EIGRP 和 BGP 协议全部在全局配置模式下使用 **prefix-list** 命令。要删除前缀列表条目，请使用此命令的 **no** 形式。

prefix-list*prefix-list-name* [**seqseq_num**] {**permit** | **deny**} *network/len* [**gemin_value**] [**lmax_value**]
no prefix-list*prefix-list-name* [**seqseq_num**] {**permit** | **deny**} *network/len* [**gemin_value**] [**lmax_value**]

Syntax Description

/	网络 和 <i>len</i> 值之间的必需分隔符。
deny	因条件匹配而拒绝访问。
gemin_value	（可选）指定要匹配的最小前缀长度。 <i>min_value</i> 参数的值必须大于 <i>len</i> 参数的值并小于或等于 <i>max_value</i> 参数（如果有）。
lmax_value	（可选）指定要匹配的最大前缀长度。 <i>max_value</i> 参数的值必须大于或等于 <i>min_value</i> 参数（如果有）的值，或者，如果 <i>min_value</i> 参数不存在，则该值必须大于 <i>len</i> 参数的值。
<i>len</i>	网络掩码的长度。有效值为 0 至 32。
网络	网络地址。
permit	允许访问匹配条件。
<i>prefix-list-name</i>	前缀列表的名称。前缀列表名称不能包含空格。
seqseq_num	（可选）将指定序列号应用于正在创建的前缀列表。

Command Default

如果未指定序列号，则系统将为前缀列表中的第一个条目分配序列号 5，并且每个后续条目的序列号都将增加 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
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) 增加了多情景模式支持。

 版本 修改

92(1) 添加了对 BGP 的支持。

使用指南

prefix-list 命令是 ABR 类型 3 LSA 过滤命令。ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。一旦配置了前缀列表，则只有指定的前缀才会从一个区域发送到另一个区域。所有其他前缀都限于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。ASA 从前缀列表的顶部开始搜索具有最小序列号的条目。创建匹配后，ASA 不会浏览列表中的其余项。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。

默认情况下，系统会自动生成序列号。可以使用 **noprefix-listsequence-number** 命令抑制这些警报。序列号以 5 为增量生成。前缀列表中生成的第一个序列号为 5。该列表中的下一个条目的序号为 10，以此类推。如果为某个条目指定了值，但不为后续条目指定值，则生成的序列号将以 5 为增量从指定的值开始增加。例如，如果指定前缀列表中第一个条目的序号为 3，然后另外两个条目未指定序号，则为这两个条目自动生成的序号为 8，13。

您可以使用 **ge** 和 **le** 关键字来指定比 **network/len** 参数更具体的前缀匹配的前缀长度范围。既未指定 **ge** 也未指定 **le** 关键字时，假定完全匹配。如果仅指定了 **ge** 关键字，则范围为 *min_value* 到 32。如果仅指定了 **le** 关键字，则范围为 *len* 到 *max_value*。

min_value 和 *max_value* 参数的值必须满足以下条件：

$$len < min\_value \leq max\_value \leq 32$$

使用命令的 **no** 形式可从前缀列表中删除特定条目。使用 **clearconfigureprefix-list** 命令来删除前缀列表。clear **configureprefix-list** 命令还会从配置中删除关联的 **prefix-listdescription** 命令（如果有）。

CR_Examples

以下示例拒绝默认路由 0.0.0.0/0：

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

以下示例允许使用前缀 10.0.0.0/8：

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

以下示例显示如何在前缀为 192/8 的路由中接受最多 24 位的掩码长度：

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

以下示例显示如何拒绝前缀为 192/8 的路由中掩码长度大于 25 位的路由：

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

以下示例显示如何在所有地址空间中允许 8 至 24 位的掩码长度：

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

以下示例显示如何在所有地址空间中拒绝长度超过 25 位的掩码：


```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

以下示例显示如何拒绝前缀为 10/8 的所有路由：

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

以下示例显示如何拒绝前缀为 192.168.1/24 的路由的所有长度大于 25 位的掩码：

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

以下示例显示如何允许所有前缀为 0/0 的路由：

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

命令	说明
clearconfigureprefix-list	从运行配置中删除 prefix-list 命令。
prefix-listdescription	用于输入前缀列表的说明。
prefix-listsequence-number	启用前缀列表顺序编号。
showrunning-configprefix-list	显示正在 prefix-list 运行的配置中的命令。

前缀列表说明

要向前缀列表添加说明，请在全局配置模式下使用 **prefix-list description** 命令。要删除前缀列表描述，请使用此 **no**命令的形式。

```
prefix-list prefix-list-name description text
no prefix-list prefix-list-name description [text]
```

Syntax Description	prefix-list-name 前缀列表的名称。
	文本 前缀列表说明的文本。最多可以输入 80 个字符。

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	—	• 是	—	—

Command History	版本 修改
	7.0(1) 添加了此命令。

使用指南

对于特定前缀列表名称，可以按任意顺序输入**prefix-list** 和 **prefix-listdescription**命令。在输入前缀列表说明之前，不需要创建前缀列表。在配置中， **prefix-listdescription** 命令将始终显示在关联前缀列表之前的行中，无论您输入命令的顺序如何。

如果为已有说明的前缀列表条目输入 **prefix-listdescription** 命令，新说明将替换原始说明。

使用此命令的 **no** 形式时，无需输入文本说明。

CR_Examples

以下示例为名为 MyPrefixList 的前缀列表添加说明。 **showrunning-configprefix-list** 命令显示，虽然前缀列表说明已添加到运行配置，但前缀列表本身尚未配置。

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

Related Commands

命令	说明
clearconfigureprefix-list	从运行配置中删除 prefix-list 命令。
prefix-list	定义 ABR 3 类 LSA 筛选的前缀列表。
showrunning-configprefix-list	显示正在 prefix-list 运行的配置中的命令。

前缀列表序列号

要启用前缀列表序列编号，请在全局配置模式下使用 **prefix-list sequence-number** 命令。要禁用前缀列表序列编号，请使用此命令的 **no** 形式。

prefix-list sequence-number

Syntax Description	此命令没有任何参数或关键字。
Command Default	默认情况下，启用前缀列表序列编号。
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
	7.0(1) 添加了此命令。

使用指南	配置中 no 仅出现此命令的形式。当配置中使用此命令的 no 形式时，系统会从配置中的 prefix-list 命令中删除序列号（包括手动配置的序列号），并且不会为新的前缀列表条目分配序列号。 启用前缀列表序列编号后，系统将使用默认编号方法为所有前缀列表条目分配序列号（从 5 开始，每个数字加 5）。如果在禁用编号之前手动为前缀列表条目分配了序号，则会恢复手动分配的编号。在自动编号禁用时，手动分配的序列号也会恢复，即使在编号禁用时它们不会显示。

CR_Examples	以下示例禁用前缀列表序列编号： <pre>ciscoasa(config)# no prefix-list sequence-number</pre>

Related Commands	命令	说明
	prefix-list	定义 ABR 3 类 LSA 筛选的前缀列表。
	showrunning-configprefix-list	显示正在 prefix-list 运行的配置中的命令。

prf

要在 AnyConnect IPsec 连接的 IKEv2 安全关联 (SA) 中指定伪随机函数 (PRF)，请在 IKEv2 策略配置模式下使用 **prf** 命令。要删除该命令并使用默认设置，请使用此命令的 **no** 形式：

```
prf { md5 | sha | sha256 | sha384 | sha512 }
no prf { md5 | sha | sha256 | sha384 | sha512 }
```

Syntax Description	md5	指定 MD5 算法。
	sha	（默认）指定安全散列算法 SHA 1。
	sha256	指定具有 256 位摘要的安全散列算法 SHA 2。
	sha384	指定具有 384 位摘要的安全散列算法 SHA 2。
	sha512	指定具有 512 位摘要的安全散列算法 SHA 2。

Command Default	默认值为 sha (SHA 1)。

使用指南	IKEv2 SA 是在第 1 阶段使用的密钥，用于使 IKEv2 对等体能够在第 2 阶段安全通信。输入 crypto ikev2 policy 命令后，使用该命令选择 prf 用于构建 SA 中使用的所有加密算法的密钥材料的伪随机函数。

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
	8.4(1)	添加了此命令。
	8.4(2)	添加了 sha256、sha384 和 sha512 关键字以提供 SHA 2 支持。

CR_Examples	以下示例进入 IKEv2 策略配置模式并将 PRF 设置为 MD5：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

Related Commands

命令	说明
encryption	为 AnyConnect IPsec 连接指定 IKEv2 SA 中的加密算法。
group	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 群。
integrity	为 AnyConnect IPsec 连接指定 IKEv2 SA 的 ESP 完整性算法。
lifetime	指定 AnyConnect IPsec 连接的 IKEv2 SA 的 SA 生命周期。

primary

要在使用 **preempt** 命令时设置故障转移组的首选设备，请在故障转移组配置模式下使用 **primary** 命令。要恢复默认值，请使用此命令 **no** 的形式。

primary
no primary

Syntax Description	此命令没有任何参数或关键字。
Command Default	如果未为故障转移组指定 primary 或 secondary ，则故障转移组默认为 primary 。
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。
	9.0(1) 较早的软件版本中允许“同时”启动，以便故障转移组无需 preempt 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障转移组在要启动的第一台设备上都变为主用状态。

使用指南	将 primary 或 secondary 首选项分配给故障转移组可指定在设置 preempt 命令时故障转移组在哪个设备上将变为主用状态。两个故障转移组都会在第一个启动的单元上变为活动状态（即使看起来它们同时启动，但一个单元会先变为活动状态），无论该组的 primary 或 secondary 设置如何。当另一台设备上线时，将第二台设备作为优先级的任何故障转移组都不会在第二台设备上变为活动状态，除非故障转移组使用 preempt 命令进行了配置，或者使用 nofailoveractive 命令手动强制到另一台设备请参阅如果使用该命令配置了故障转移 preempt 组，则故障转移组将在指定单元上自动变为活动状态。

CR_Examples	以下示例配置了故障转移组 1，其中主设备为较高优先级，并配置了故障转移组 2，其中辅助设备为较高优先级。两个故障转移组均使用 preempt 命令进行配置，因此，当设备变得可用时，两个组将在其首选设备上自动变为主用状态。 <pre> ciscoasa(config)# failover group 1 ciscoasa(config-fover-group)# primary </pre>

```
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
preempt	当设备变得可用时，强制故障转移组在其首选设备上变为主用状态。
secondary	给予辅助设备高于主设备的优先级。

priority（类别）

要启用 QoS 优先级排队，请在类配置模式下使用 **priority**命令。对于不能容忍延迟的关键流量，例如 IP 语音 (VoIP)，您可以识别低延迟排队 (LLQ) 的流量，以便始终以最低速率传输。要删除优先级要求，请使用此命 **no**令的形式。



注释 ASA 服务模块不支持此命令。

priority
no priority

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认行为或变量。

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
类配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南 LLQ 优先级排队使您可以在处理其他流量之前优先处理某些流量（例如，像语音和视频之类的延迟敏感型流量）。

ASA 支持两种类型的优先级排队：

- 标准优先级排队——标准优先级排队在 **priority-queue** 接口上使用 LLQ 优先级队列（参见命令），而所有其他流量都进入“尽力而为”队列。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。这称为 尾部丢 弃。为了避免队列填满，您可以增加队列缓冲区的大小。还可以优化允许进入传输队列的数据包的最大数。这些选项使您能够控制优先级排队的延迟和稳定性。LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

- 分层优先级排队 - 分层优先级排队用在启用流量整形队列（**shape** 命令）的接口上。可以对整形的流量的子集进行优先级排序。不使用标准优先级队列。请参阅以下有关分层优先级排队的准则：
- 优先级数据包始终排在整形队列的开头，因此它们始终先于其他未优先排队的数据包传输。
- 优先级数据包永远不会从整形队列中丢弃，除非优先级流量的持续速率超过整形速率。
- 对于 IPsec 加密的数据包，只能根据 DSCP 或优先级设置来匹配流量。
- 优先级流量分类不支持 IPsec-over-TCP。

使用模块化策略框架配置 QoS

要启用优先级排队，请使用模块化策略框架。您可以使用标准优先级排队或分层优先级排队。

对于标准优先级排队，请执行以下任务：

1. **class-map** 确定您想要执行优先级排队的流量。

2. **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. priority** - 为类映射启用优先级排队。

3. **service-policy** - 向接口或全局分配策略映射。

对于分层优先级排队，请执行以下任务：

1. **class-map** 确定您想要执行优先级排队的流量。

2. **policy-map** (for priority queuing) - 标识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. priority** - 为类映射启用优先级排队。如果要分层使用，只能在此策略映射中包含 **priority** 命令。

3. **policy-map** （适用于流量整形）- 标识与 **class-default** 类映射关联的操作。

- **a. class class-default** 确定您想要执行操作的 **class-default** 类映射。
- **b. shape** - 将流量整形应用到类映射。
- **c. service-policy** - 调用您在其中配置了 **priority** 命令的优先级排队策略映射，以便将优先级排队应用于整形流量子集。

4. **service-policy** - 向接口或全局分配策略映射。

CR_Examples

以下是策略映射配置模式下的 **priority** 命令的示例：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
```

```
ciscoasa(config-pmap-c) # class class-default
ciscoasa(config-pmap-c) #
```

Related Commands	class	指定要用于流量分类的类映射。
	clearconfigurepolicy-map	删除所有策略映射配置，但如果策略映射正在用于服务策略命令，则不会删除该策略映射。
	policy-map	配置策略；即流量类与一个或多个操作的关联。
	showrunning-configpolicy-map	— 确定您想要执行操作的类映射。

priority（集群组）

要设置此设备在 ASA 集群中主设备选举的优先级，请在集群组配置模式下使用 **priority** 命令。要删除优先级，请使用此 **no**命令的形式。

```
prioritypriority_number
no priority[priority_number]
```

Syntax Description *priority_number* 设置此单元在主单元选举中的优先级，介于 1 和 100 之间，其中 1 为最高优先级。

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
集群组配置	• 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** 集群成员通过集群控制链路进行通信来选举主单元，如下所示：
1. 当为设备启用集群（或当设备首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
 2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
 3. 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为主设备。



注释 如果多个单元并列最高优先级，则使用集群单元名称，然后序列号来确定主单元。

4. 如果稍后有优先级更高的设备加入群集，则该设备不会自动成为主设备；现有主设备将一直作为主设备，除非它停止响应，届时将选举新的主设备。



注释 您可以使用命令手动强制某个单元成为主单元**clustermasterunit**。对集中功能而言，如果强制更改主设备，则所有连接都将断开，而您必须新的主设备上重新建立连接。有关集中功能的列表，请参阅配置指南。

CR_Examples

以下示例将优先级设置为 1（最高）：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

Related Commands

命令	说明
clacpsystem-mac	使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。
cluster group	命名集群并进入集群配置模式。
cluster-interface	指定集群控制链路接口。
clusterinterface-mode	设置集群接口模式。
conn-rebalance	启用连接再均衡。
console-replicate	启用从从属设备到主设备的控制台复制。
enable(clustergroup)	启用集群。
health-check	启用集群健康检查功能，包括单元健康监控和接口健康监控。
key	为集群控制链路上的控制流量设置身份验证密钥。
local-unit	为集群成员命名。
mtucluster-interface	指定集群控制链路接口的最大传输单元。
priority(clustergroup)	设置此单元在主单元选举中的优先级。

priority（VPN负载均衡）

要设置参与虚拟负载均衡集群的本地设备的优先级，请在 VPN 负载均衡模式下使用 **priority**命令。
要恢复默认优先级规范，请使用此命 **no** 令的形式。

priority*priority*
no priority

Syntax Description *priority* 您要分配给此设备的优先级，取值范围为 1 到 10。

Command Default 默认优先级取决于设备型号：

型号编号	默认优先级
5520	5
5540	7

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	—	—	• 是	—	—

Command History 版本 修改
7.0(1) 添加了此命令。

使用指南 必须先使用 **vpnload-balancing**命令进入 VPN 负载均衡模式。
此命令设置加入虚拟负载均衡集群的本地设备的优先级。
优先级必须是介于 1（最低）到 10（最高）之间的整数。
在主设备选择过程中，优先级会作为一种方式来确定 VPN 负载均衡集群中的哪台设备会成为集群的主设备或主设备。有关主设备选择过程的详细信息，请参阅 CLI 配置指南。
命令的 **no** 形式可将指定的优先级恢复为默认值。

CR_Examples

以下是一个 VPN 负载均衡命令序列示例，其中包含一条 **priority** 命令，该命令将当前设备的优先级设置为 9:

```
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)# 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)# participate
```

Related Commands

命令	说明
vpnload-balancing	进入 VPN 负载均衡模式。

priority-queue

要在接口上创建标准优先级队列以与 **priority** 命令配合使用，请在全局配置模式下使用**priority-queue** 命令。要删除队列，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。

```
priority-queueinterface-name
no priority-queueinterface-name
```

Syntax Description	interface-name 指定要启用优先级队列的物理接口的名称，或者对于 ASA 5505 或 ASASM，指定 VLAN 接口的名称。

Command Default	默认情况下，优先级排队处于禁用状态。

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
	7.0(1)	添加了此命令。
	8.2(3)/8.4(1)	ASA 5585-X 增加了对十千兆以太网接口的支持。

使用指南 LLQ 优先级排队使您可以在处理其他流量之前优先处理某些流量（例如，像语音和视频之类的延迟敏感型流量）。

ASA 支持两种类型的优先级排队：

- 标准优先级排队——标准优先级排队在您使用命令创建的接口上使用 LLQ 优先级 **priority-queue** 队列，而所有其他流量进入“尽力而为”队列。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。这被称为 尾部丢弃。为了避免队列填满，您可以增加队列缓冲区大小（ **queue-limit**命令）。您还可以微调允许进入传输队列的最大数据包数量（ **tx-ring-limit**命令）。这些选项使您能够控制优先级排队的延迟和稳定性。LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

- 分层优先级排队 - 分层优先级排队用在启用了流量整形队列的接口上。可以对整形的流量的子集进行优先级排序。不使用标准优先级队列。



注释 仅在 ASA 5505 上，在一个接口上配置优先级队列会覆盖所有其他接口上的相同配置；所有接口上仅存在最后应用的配置。此外，如果从一个接口删除优先级队列配置，则该配置也会从所有接口删除。要解决此问题，请仅在一个接口上配置 **priority-queue** 命令。如果不同的接口需要对 **queue-limit** 和/或 **tx-ring-limit** 命令进行不同的设置，请在任何一个接口上使用所有队列限制中的最大者和所有 **tx-ring-limits** 中最小者（CSCsi13132）。

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 30,000 个数据包，传输队列限制为 256 个数据包。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

Related Commands

命令	说明
queue-limit	指定在优先级队列丢弃数据前可排入该队列的最大数据包数。
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。
policy-map	配置策略；即流量类与一个或多个操作的关联。
clearconfigurepriority-queue	删除当前优先级队列配置。
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。

privilege

要配置与命令授权一起使用的命令权限级别（仅限本地、RADIUS 和 LDAP（映射）），请在全局配置模式下使用 **privilege** 命令。要不允许配置，请使用此命 **no** 令的形式。

```
privilege [show | clear | configure] levellevel [modecli_mode] command命令
no privilege [ show | clear | configure] levellevel [modecli_mode ]command命令
```

Syntax Description	clear （可选）仅为 clear 形式设置命令的权限。如果不使用、或 configureclearshow关键字，则该命令的所有形式都会受到影响。
command命令	指定您正在配置的命令。您只能配置主命令的权限级别。例如可以配置所 aaa有命令的级别，但不能配置某条命 aaaauthentication 令和某条命令的 aaaauthorization 级别。
configure	（可选）仅为命令的配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 show或 clear 前缀），或者是以 no 形式。如果不使用、或configureclearshow关键字，则该命令的所有形式都会受到影响。
level级别	指定特权级别；有效值为 0 至 15。较低特权级别数字表示较低特权级别。
modecli_mode	（可选）如果可以在多个 CLI 模式下输入命令，例如用户执行/特权 EXEC 模式、全局配置模式或命令配置模式，则可以分别设置这些模式的权限级别。如果不指定模式，则该命令的所有版本都使用同一级别。请参阅以下模式： • exec - 指定用户 EXEC 模式和特权 EXEC 模式。 • —configure指定全局配置模式， configureterminal使用命令访问。 • command_config_mode - 指定命令配置模式，在全局或其他命令配置模式下使用命令名称进行访问。 例如， mac-address该命令可以在全局配置模式和接口配置模式下输入。mode 关键字用于为每种模式单独设置级别。 如果在为 命令设置级别，则无法使用此命令
show	（可选）仅为 show 形式的命令设置权限。如果不使用、或configureclearshow关键字，则该命令的所有形式都会受到影响。

Command Default	默认情况下，会为以下命令分配 0 级权限，所有其他命令均处于级别 15。 • showchecksum • showcurpriv • enable • help

- **showhistory**
- **login**
- **logout**
- **pager**
- **showpager**
- **clearpager**
- **quit**
- **showversion**

如果将任何配置模式命令移动到低于 15 的 **configure** 级别，请确保也将该命令移动到该级别，否则用户将无法进入配置模式。

要查看所有权限级别，请参阅 **showrunning-configallprivilegeall** 命令。

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

8.0(2) 增加了对具有 Cisco VSA CVPN3000-Privilege-Level 的 RADIUS 用户的支持。如果使用 **ldapmap-attributes**命令将 LDAP 属性映射到 CVPN3000-Privilege-Level，则支持 LDAP 用户。

使用指南

当您配置 **privilege** 命令时，[**aaaauthorizationcommandLOCAL** 命令允许您设置 ASA 命令的权限级别。即使命令使用 **LOCAL** 关键字，此关键字也将启用本地、RADIUS 和 LDAP（映射）授权。

CR_Examples

例如，命令有 **filter**以下形式：

- **filter**（以 **configure**选项表示）
- **showrunning-configfilter**
- **clearconfigurefilter**

您可以为每种形式分别设置权限级别，或通过忽略此选项为所有形式设置同一权限级别。例如，分别设置每个表单，如下所示：

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

或者，您可以将所有过滤命令设置为同一级别：

```
ciscoasa(config)# privilege level 5 command filter
```

该命令将 **show privilege** 显示中的各个表单分开。

以下示例显示 **mode** 关键字的使用。该 **enable** 命令必须从用户 EXEC 模式输入，而在 **enable password** 配置模式下可访问的命令需要最高权限级别。

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

以下示例显示了两种模式下的 **mac-address** 命令以及 **show**、**clear** 和 **cmd version** 的不同级别：

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

Related Commands

命令	说明
clear configure privilege	从配置中删除特权命令语句。
show curpriv	显示当前权限级别。
show running-config privilege	显示命令的权限级别。

profile

要创建或编辑报障配置文件，请在报障配置模式下使用 **profile** 命令。要删除一个或所有已配置的报障配置文件，请使用此命令的 **no** 形式指定一个或所有配置文件。您可以通过首先输入命令来访问 call-home 配置 **call-home** 模式。

profile *profile-name*
no profile {*profile-name* | **all**}

Syntax Description

profile-name 配置文件名称，最长 20 个字符。

all 包括所有已配置的配置文件。

Command Default

已提供默认配置文件。CiscoTAC 默认配置文件包含一组要监控的预定义组（诊断、环境、清单、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。最初配置 Smart Call Home 时，系统将自动创建默认配置文件。目标邮件地址为 callhome@cisco.com，目标 URL 为 <https://tools.cisco.com/its/service/oddce/services/DDCEService>。

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
报障配置	• 是	• 支持	• 支持	—	• 是

Command History

版本 修改

8.2(1) 我们引入了此命令。

8.2(2) 添加了关键字 **all**。

9.3(2) 我们为智能软件许可添加了 **License** 配置文件。

9.6(2) 引入了 **destinationaddresshttp** 的 reference-identity 选项。

使用指南

以下命令用于模板配置模式。

启用或禁用配置文件

要启用 call-home 配置文件，请在 call-home-profile 配置模式下使用 **active** 命令。要禁用 call-home 配置文件，请在 call-home-profile 配置模式下使用 **noactive** 命令。您可以通过首先输入 **then** 命令来访问 call-home-profile 配置 **call-home** 模 **profile** 式。默认设置为启用。

active

no active

将配置文件命令设置为默认值

要将 call home 配置文件设置恢复为默认值，请在 call-home-profile 配置模式下使用 default 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home** 模 **profile** 式。您也可以从该模式重置报障配置模式设置。使用命令帮助、**default?** 确定和重置所有报障配置文件和常规设置。

default { activedestinationemail-subjectsubscribe-to-alert-group }

目标类型、地址和设置

要为 Smart Call Home 消息接收方设置目标地址、引用标识、消息格式和传输方法，请在 call-home-profile 配置模式下使用 **destination** 命令。要删除目标参数或将其重置为默认值，请使用 **nodeestination** 或 **default** 命令。

默认的邮件格式为 XM，默认的邮件大小为 5MB（0 表示无限制），默认传输方式为邮件。您必须指定以前配置的引用标识。这用于在连接时验证报障服务器的证书。它仅适用于 http 目标。

destinationaddress { e-mail-mail-addresshttphttp-url }

nodeestinationaddress { e-mailhttp[all] }

destinationaddresshttphttp-urlreference-identity 引用 ID 名称

nodeestinationaddresshttphttp-urlreference-identity 引用 ID 名称

destinationaddress { e-mail-mail-addresshttphttp-url } msg-format { short-textlong-textxml }

nodeestinationaddress { e-mail-mail-addresshttphttp-url } msg-format { short-textlong-textxml }

destinationmessage-size-limit max-size

nodeestinationmessage-size-limit max-size

destinationpreferred-msg-format { short-textlong-textxml }

nodeestinationpreferred-msg-format { short-textlong-textxml }

destinationtransport-method { e-mailhttp }

nodeestinationtransport-method { e-mailhttp }

配置邮件主题

要设置 call-home 邮件的邮件主题前缀或后缀，请在 call-home-profile 配置模式下使用 **email-subject** 命令。要清除这些字段，请使用 **noemail-subject** 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home** 模 **profile** 式。

email-subject { appendprepend } chars

noemail-subject { appendprepend } chars

订阅警报组

要订用警报组，请在 call-home-profile 配置模式下使用 **subscribe-to-alert-group** 命令。要清除这些订用，请使用 **no subscribe-to-alert-group** 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home** 模 **profile** 式。

- [编号] 订阅警报组警报组名称[严重性|灾难性] | 灾难 | 突发事件警报 | 警报 | 严重 | 错误 | 警告 | 通知 | 通知信息 | debug} - 订用具有指定严重性级别的事件。alert-group-name: 系统日志、诊断、环境或威胁都是有效值。

- [no] subscribe-to-alert-group syslog [{严重性 {灾难性 | 灾难 | 突发事件警报 | 警报 | 严重 | 错误 | 警告 | 通知 | 通知信息 | 调试} | message start [-end]]} - 订阅具有严重性级别或消息 ID 的系统日志。start[-end]: 一个系统日志消息 ID 或一系列系统日志消息 ID。



注释

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

- [no] subscribe-to-alert-group inventory [periodic {每日 | 重复每月 day_of_month | 每月 week day_of_week [hh:mm]}] - 订阅资产事件。day_of_month: 星期几，1-31。day_of_week: 星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）。hh, mm: 24 小时制、一天的小时数和分钟数。
- [no] subscribe-to-alert-group configuration [export full | [no] subscribe-to-alert-group configuration [export full]最小值] [周期 {每日 | 周期每月 day_of_month | 每月 week day_of_week [hh:mm]}] - 订用配置事件。full: 要导出运行配置、启动配置、功能列表、访问列表中的元素数量以及多模式中情景名称的配置。minimum: 要导出的配置-仅限功能列表、访问列表中的元素数量以及多模式中的情景名称。day_of_month: 星期几，1-31。day_of_week: 星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）。hh, mm: 一天中的小时和分钟，采用 24 小时制。
- [no] subscribe-to-alert-group 遥测定期 {每小时 | 每日 | 每月 day_of_month | 每月 week day_of_week [hh:mm]} - 订用遥测周期性事件。day_of_month: 月份中的日期，1-31。day_of_week: 星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）。hh, mm: 24 小时制、一天的小时数和分钟数。
- [no] subscribe-to-alert-group snapper period {interval minutes | hourly [mm] | daily | monthly day_of_month | weekly day_of_week [hh:mm]} — 订阅快照定期事件。minutes: 间隔时间（分钟）。day_of_month: 每月的某一天，1-31。day_of_week: 星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）。hh, mm: 一天的小时和分钟，以 24 小时制表示。

Related Commands

命令	说明
call-home	使用户进入报障配置模式
showcall-home	显示 Call Home 配置信息。
reference-identity	配置引用标识对象。

prompt

要自定义 CLI 提示符，请在全局配置模式下使用 `prompt` 命令。要恢复默认提示，请使用此命令的 `no` 形式。

```
prompt { [hostname] [context ] [domain] [slot] [state] [priority] [cluster-unit ]
no prompt [ hostname] [context] [domain ] [slot ] [state] [priority ] [cluster-unit
]
```

Syntax Description	cluster-unit	显示集群设备名称。集群中的每台设备都有一个唯一的名称。
	context	（仅限多种模式）显示当前上下文。
	domain	显示域名。
	hostname	显示主机名。
	priority	显示故障转移优先级 <code>pri</code> （主要）或 <code>sec</code> （辅助）。使用命令设置优先 failoverlanunit 级。
	state	显示设备的流量传递状态或角色。 对于故障转移，关 state键字显示以下值： - act - 已启用故障转移，设备正在传递流量。 - stby - 已启用故障转移，设备未在传递流量，并且处于备用、故障或其他非活动状态。 - actNoFailover - 未启用故障转移，设备正在传递流量。 - stbyNoFailover - 未启用故障转移，设备未在传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。 对于聚类，关 state键字显示以下值： - control node - data node 例如，如果您设置 prompthostnamecluster-unitstate，那么在提示符 “<code>ciscoasa/cl2/data></code>” 中，主机名是 <code>ciscoasa</code>，单元名称是 <code>cl2</code>，状态名称是 <code>data</code>

Command Default 默认提示符是主机名。在多情景模式下，主机名后跟当前情景名称 (*hostname /context*)。

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	—	• 是

Command History

版本 修改

7.2(1) 添加了此命令。

9.0(1) 该 **cluster-unit** 选项已添加。已更新集群的 **state** 关键字。

9.19(1) 对于集群，**state** 显示已从 **主设备** 和 **从属设备** 更改为 **控制节点** 和 **数据节点**。

使用指南

输入关键字的顺序确定提示符中各元素的顺序（各元素以斜线 (/) 分隔）。

在多情景模式中，您可以在登录到系统执行空间或管理情景时查看扩展的提示符。在非管理情景中，您仅可看到默认提示符，即主机名和情景名称。

利用为提示符添加信息这项功能，可以大体了解在您有多个模块时登录哪一台 ASA。故障转移起价你，如果两台 ASA 具有相同的主机名，则此功能非常有用。

CR_Examples

以下示例显示提示中可用于故障转移的所有可用元素：

```
ciscoasa(config)# prompt hostname context slot state priority
```

提示符更改为以下字符串：

```
ciscoasa/admin/pri/act(config)#
```

Related Commands

命令	说明
清除配置提示	清除配置的提示。
showrunning-configprompt	显示配置的提示。

propagate sgt

要在接口上启用安全组标记（称为 **sgt**）的传播，请在 **cts** 手动接口配置模式下使用 **propagatesgt** 命令。要在接口上禁用安全组标记（称为 **sgt**）的传播，请使用此命令的 **no** 形式。

propagatesgt
nopropagatesgt

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认情况下，传送被启用。

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
Cts 手动接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.3(1)	添加了此命令。

使用指南 此命令可在 CTS 第 2 层 SGT 实施中启用和禁用安全组标记的传播。

限制

- 仅支持物理接口、VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI、TVI 和 VNI。

CR_Examples 以下示例启用第 2 层 SGT 实施接口并指示未传播 SGT：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

命令	说明
cts manual	启用第 2 层 SGT 强制并进入 cts 手动接口配置模式。

命令	说明
polycstaticsgt	将策略应用于手动配置的 CTS 链接。

protocol

要为 IKEv2 连接指定 IPsec 提议的协议和加密类型，请在 IPsec 提议配置模式下使用 **protocol** 命令。
如要删除协议和加密类型，请使用该命令的 **no** 形式：

```

protocol
esp { encryption { des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256
| null } | integrity { md5 | sha-1 | sha-256 | sha-384 | sha-512 | null }
no protocol
esp { encryption { des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256
| null } | integrity { md5 | sha-1 | sha-256 | sha-384 | sha-512 | null }
    
```

Syntax Description	
esp	指定封装安全有效负载 (ESP) IPsec 协议（当前唯一支持的 IPsec 协议）。
des	为 ESP 指定 56 位 DES-CBC 加密。
3des	（默认）为 ESP 指定三重 DES 加密算法。
aes	为 ESP 指定带有 128 位密钥加密的 AES。
aes-192	为 ESP 指定带有 192 位密钥加密的 AES。
aes-256	为 ESP 指定带有 256 位密钥加密的 AES。
aes-gcm	指定要使用的 AES-GCM 或 AES-GMAC 算法。
aes-gcm-192	指定要使用的 AES-GCM 或 AES-GMAC 算法。
aes-gcm-256	指定要使用的 AES-GCM 或 AES-GMAC 算法。
aes-gmac	指定要使用的 AES-GCM 或 AES-GMAC 算法。
aes-gmac-192	指定要使用的 AES-GCM 或 AES-GMAC 算法。
aes-gmac-256	指定要使用的 AES-GCM 或 AES-GMAC 算法。
null	不对 ESP 使用加密。
integrity	指定 IPsec 协议的完整性算法。
md5	指定 ESP 完整性保护的 md5 算法。
sha-1	（默认）指定美国联邦信息处理标准 (FIPS) 中定义的安全散列算法 (SHA) SHA-1，用于 ESP 完整性保护。
sha-256	指定要用作 IPsec 完整性算法的算法。
sha-384	指定要用作 IPsec 完整性算法的算法。
sha-512	指定要用作 IPsec 完整性算法的算法。

null 选择是否将 AES-GCM/GMAC 配置为加密算法。

Command Default

IPsec 提议的默认设置是加密类型 3DES 和完整性类型 SHA-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
IPsec 提议配置	• 是	• 支持	• 支持	—	—

Command History

版本 修改

8.4(1) 添加了此命令。

9.0(1) 添加了对 AES-GCM 或 AES-GMAC 算法的支持。增加了选择要用作 IPsec 完整性算法的算法的功能。

使用指南

IKEv2 IPsec 提议可以有多个加密和完整性类型。使用此命令可指定类型，这将允许对等体根据需要进行选择。

如果将 AES-GMC/GMAC 配置为加密算法，则必须选择空完整性算法。

CR_Examples

以下示例创建 IPsec 提议 proposal_1，配置 ESP 加密类型 DES 和 3DES，并指定用于完整性保护的加密算法 MD5 和 SHA-1：

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

Related Commands

命令	说明
cryptoikev2enable	在 IPsec 对等体通信的接口上启用 ISAKMP IKEv2 协商。
cryptoipsecikev2ipsec-proposal	创建 IPsec 提案并进入 IPsec 提案配置模式，您可以在其中为提案指定多种加密和完整性类型。
showrunning-configipsec	显示所有转换集的配置。
cryptomapsettransform-set	指定要在加密映射条目中使用的转换集。
cryptodynamic-mapsettransform-set	指定要在动态加密映射条目中使用的转换集。
showrunning-configcryptomap	显示加密映射配置。

命令	说明
show running-config crypto dynamic-map	显示动态加密映射配置。

protocol-enforcement

要启用域名、标签长度和格式检查（包括压缩和循环指针检查），请在参数配置模式下使用 **protocol-enforcement** 命令。要禁用协议执行，请使用此命令 **no** 的形式。

protocol-enforcement
no protocol-enforcement

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下启用协议实施。配置 **inspectdns** 后，即使未定义 **policy-map type inspect dns**，也可以启用此功能。要禁用，必须在策略映射配置中明确声明 **no protocol-enforcement**。如果未配置 **inspectdns**，则不执行 NAT 重写。

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。

使用指南

在某些情况下，即使禁用了命令，协议实施仍会执行。当出于其他目的（例如 DNS 资源记录分类、NAT 或 TSIG 检查）需要解析 DNS 资源记录时，会发生这种情况。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用协议实施：

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

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

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

protocol http

要将 HTTP 指定为用于检索 CRL 的允许分发点协议，请在 **ca-crl** 配置模式下使用 **protocolhttp** 命令。
要将 HTTP 作为允许的 CRL 检索方法删除，请使用此命令的 **no** 形式。

protocol http
no protocol http

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认设置是允许 HTTP。

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-crl 配置	• 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 如果使用此命令，请务必将 HTTP 规则分配给公共接口过滤器。CRL 分发点的内容根据权限确定检索方法（HTTP、LDAP 和/或 SCEP）。

CR_Examples 以下示例进入 **ca-crl** 配置模式，并允许 HTTP 作为检索信任点集中式 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central  
ciscoasa(ca-trustpoint)# crl configure  
ciscoasa(ca-crl)# protocol http
```

Related Commands

命令	说明
crlconfigure	进入 ca-crl 配置模式。
cryptocatrustpoint	进入 trustpoint 配置模式。
protocolldap	指定 LDAP 作为 CRL 的检索方法。
protocolscep	指定 SCEP 作为 CRL 的检索方法。

protocol ldap

要将LDAP指定为用于检索CRL的分发点协议，请在ca-crl配置模式下使用**protocolldap**命令。CRL分发点的内容根据权限确定检索方法（HTTP、LDAP和/或SCEP）。

要将LDAP协议作为允许的CRL检索方法删除，请使用此命令的**no**形式。

protocol ldap
no protocol ldap

Syntax Description 此命令没有任何参数或关键字。

Command Default 默认设置是允许LDAP。

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
crl 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例进入ca-crl配置模式，并允许LDAP作为检索信任点集中式CRL的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

命令	说明
crlconfigure	进入ca-crl配置模式。
cryptocatrustpoint	进入trustpoint配置模式。
protocolhttp	指定HTTP作为CRL的检索方法
protocolscep	指定SCEP作为CRL的检索方法

protocol-object

要将协议对象添加到协议对象组，请在协议配置模式下使用 protocol-object 命令。要删除端口对象，请使用此命令的 no 形式。

```
protocol-object protocol
no protocol-object protocol
```

Syntax Description protocol 协议名称或编号。

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
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 protocol-object 命令与 object-group 命令配合使用，以在协议配置模式下定义协议对象。

可以使用 protocol 参数指定 IP 协议名称或编号。udp 协议编号为 17，tcp 协议编号为 6，egp 协议编号为 47。

CR_Examples 以下示例显示如何定义协议对象：

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfigureobject-group	从配置中删除所有对象组命令。
group-object	添加网络对象组。
network-object	向网络对象组添加网络对象。
object-group	定义对象组以优化您的配置。
showrunning-configobject-group	显示当前对象组。

protocol scep

要指定 SCEP 作为用于检索 CRL 的分发点协议，请在 `crl` 配置模式下使用 **protocol scep** 命令。CRL 分发点的内容根据权限确定检索方法（HTTP、LDAP 和/或 SCEP）。

要将 SCEP 协议从允许的 CRL 检索方法中删除，请使用此命令的 **no** 形式。

protocol scep
no protocol scep

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认设置是允许 SCEP。

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
Crl 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本 修改

7.0(1) 添加了此命令。

CR_Examples

以下示例进入 `ca-crl` 配置模式，并允许 SCEP 作为检索信任点集中器的 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

Related Commands

命令	说明
crlconfigure	进入 <code>ca-crl</code> 配置模式。
cryptocatrustpoint	进入 <code>trustpoint</code> 配置模式。
protocolhttp	指定 HTTP 作为 CRL 的检索方法。
protocolldap	指定 LDAP 作为 CRL 的检索方法。

protocol shutdown

要禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接关系并清除 IS-IS LSP 数据库，请在 **protocolshutdown** 路由器 isis 配置模式下使用该命令。要重新启用 IS-IS 协议，请使用此命令的 **no** 形式

protocol shutdown
no protocol shutdown

Syntax Description 此命令没有任何参数或关键字。

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 此命令允许您禁用特定路由实例的 IS-IS 协议，而无需删除任何现有的 IS-IS 配置参数。输入该命令后，IS-IS **protocolshutdown** 协议继续在 ASA 上运行，并且可以使用当前的 IS-IS 配置，但 IS-IS 不会在任何接口上形成任何邻接关系，并且还会清除 IS-IS LSP 数据库。

如果要禁用特定接口的 IS-IS 协议，请使用该 **isisprotocolshutdown** 命令。

CR_Examples

以下示例为特定路由实例禁用 IS-IS 协议：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

Related Commands

protocol-violation

要定义 HTTP 和 NetBIOS 检测中发生协议违规时的操作，请在参数配置模式下使用 **protocol-violation** 命令来定义检测的操作。要禁用此功能，请使用此 **no** 命令的形式。

protocol-violation *action* [**drop** [**log**] | **log**]
no protocol-violation *action* [**drop** [**log**] | **log**]

Syntax Description

drop 指定丢弃不符合协议的数据包。
log 指定记录协议违规。

Command Default

无默认为行为或值。

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。

使用指南

可以在 HTTP 或 NetBIOS 策略映射中配置此命令。当 HTTP 或 NetBIOS 解析器无法在消息的前几个字节中检测到有效的 HTTP 或 NetBIOS 消息时，将发出系统日志。例如，当分块编码格式错误且无法解析消息时，会发生这种情况。

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 http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

Related Commands

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

命令	说明
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。

proxy-auth

要将隧道组标记为特定代理身份验证隧道组，请在 webvpn 配置模式下使用 **proxy-auth** 命令。

proxy-auth [**sdi**]

Syntax Description **sdi** 将 RADIUS/TACACS SDI 代理消息解析为本机 SDI 指令。

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
Webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南 使用 **proxy-auth** 命令启用将 aaa-server 代理身份验证文本消息解析为本地协议指令。

proxy-auth_map sdi

要将 RADIUS 代理服务器返回的 RADIUS 质询消息映射到本地 SDI 消息，请在 aaa-server 配置模式下使用 **proxy-auth_mapsd**i 命令。

proxy-auth_mapsdi [sdi_message] [radius_challenge_message]

Syntax Description

radius_challenge_message 指定用于映射特定 SDI 消息的 RADIUS 质询消息，可以是以下任意消息：

- new-pin-meth - 新的 PIN 码方式，[默认值] 是否要输入自己的 PIN 码
- new-pin-reenter - 重新输入新 PIN，[默认] 重新输入 PIN：
- new-pin-req - 请求的新 PIN，[默认] 输入新的字母数字 PIN
- new-pin-sup - 提供的新 PIN 码，[默认值] 请记住您的新 PIN 码
- new-pin-sys-ok - 接受新 PIN，[默认值] 接受新 PIN
- next-ccode-and-reauth - 在更改令牌时重新进行身份验证，[默认]使用下一个卡代码的新 PIN
- 下一个代码 - 提供不带 PIN 的令牌代码，[默认] 输入下一个密码
- ready-for-sys-pin - 接受系统生成的 PIN，[默认值] 接受系统生成的 PIN

sdi_message 指定本地 SDI 消息。

Command Default

ASA 上的默认映射对应于思科 ACS 上的默认设置（包括系统管理、配置和 RSA SecureID 提示），这些设置也与 RSA 身份验证管理器上的默认设置同步。

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服务器配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

要启用对来自 RADIUS 代理的 RADIUS 质询消息的解析和映射，您必须在隧道组配置模式下启用 **proxy-auth** 命令。然后将使用默认映射值。您可以使用 **proxy-auth_map** 命令更改默认映射值。

远程用户通过 Secure Client 连接到 ASA，并尝试使用 RSA SecurID 令牌进行身份验证。ASA 可配置为使用 RADIUS 代理服务器，而 ASA 则与关于该身份验证的 SDI 服务器进行通信。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。当 ASA 直接与 SDI 服务器通信时的消息文本与 ASA 通过 RADIUS 代理通信时的消息文本不同。

因此，为了作为的本地 SDI 服务器出现 Secure Client，ASA 必须解释来自 RADIUS 服务器的消息。此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。否则，向远程客户端用户显示的提示可能不适用于身份验证期间所需的操作。可 Secure Client 能无法响应，并且身份验证可能会失败。

Related Commands

命令	说明
proxy-auth	启用来自 RADIUS 代理的 RADIUS 质询消息的解析和映射。

proxy-bypass

要将 ASA 配置为执行最小内容重写并指定要重写的内容类型（外部链路和/或 XML），请在 webvpn 配置模式下使用 **proxy-bypass** 命令。要禁用代理绕过，请使用命 **no** 令的形式。

```
proxy-bypass interface interfacename { port portnumber | path-mask path
mask } target url [ rewrite { link | xml | none } ]
no proxy-bypass interface interfacename { port portnumber | path-mask path
mask } target url [ rewrite { link | xml | none } ]
```

Syntax Description

主机	标识要将流量转发到的主机。使用主机 IP 地址或主机名。
interface	标识用于代理绕行的 ASA 接口。
interfacename	通过名称指定 ASA 接口。
link	指定绝对外部链接的重写。
none	指定不重写。
路径掩码	指定要匹配的模式。
路径掩码	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 128 个字节。
port	确定为代理绕行保留的端口。
端口数值	指定为代理绕行保留的高位端口。端口范围为 20000-21000。一个端口只能用于一个代理绕行规则。
rewrite	（可选）指定其他重写规则：无或 XML 和链接的组合。
target	标识要将流量转发到的远程服务器。
url	以 http(s)://Fully_qualified_domain_name[:port] 格式输入 URL。最多 128 个字节。HTTP 的端口为 80，HTTPS 的端口为 443，除非您指定其他端口。
xml	指定重写 XML 内容。

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
WebVPN 配置	• 是	—	• 是	—	—

Command History

版本 修改

7.1(1) 添加了此命令。

使用指南

将代理绕行用于可更好地抑制内容重写的应用和 Web 资源。proxy-bypass 命令确定如何处理通过 ASA 传输的特定 Web 应用。

您可以多次使用此命令。配置条目的顺序并不重要。接口和路径掩码或接口和端口将唯一标识代理绕行规则。

如果您使用端口而不是路径掩码来配置代理旁路，则根据您的网络配置，您可能需要更改防火墙配置以允许这些端口访问 ASA。使用路径掩码可避免此限制。但请注意，路径掩码可能会发生变化，因此您可能需要使用多个路径掩码语句来穷尽所有可能性。

路径是 URL 中 .com 或 .org 或其他类型域名之后的任何内容。例如，在 URL `www.example.com/hrbenefits` 中，`hrbenefits` 就是路径。同样，对于 URL `www.example.com/hrinsurance`，`hrinsurance` 就是路径。如果要对所有 hr 站点使用代理绕过，则可以使用 * 通配符来避免多次使用该命令，如下所示：`/hr*`。

CR_Examples

以下示例显示如何将 ASA 配置为使用端口 20001 进行 webvpn 接口上的代理旁路（使用 HTTP 及其默认端口 80）将流量转发至 `example.com` 并重写 XML 内容。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

下一个示例显示如何配置 ASA 以在外部接口上将路径掩码用于代理绕行，使用 HTTP 及其默认端口 443 将流量转发到 `example.com`，并重写 XML 和链接内容。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

Related Commands

命令	说明
apcf	指定用于特定应用的非标准规则。
rewrite	确定流量是否通过 ASA。

proxy-ldc-issuer

要颁发 TLS 代理本地动态证书，请在 `crypto ca trustpoint` 配置模式下使用 `proxy-ldc-issuer` 命令。要删除配置，请使用此命令 `no` 的形式。

proxy-ldc-issuer
no proxy-ldc-issuer

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
Crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	—

Command History 版本 修改

8.0(2) 添加了此命令。

使用指南 使用 `proxy-ldc-issuer` 命令可颁发 TLS 代理本地动态证书。`proxy-ldc-issuer` 命令授予加密信任点作为本地 CA 的角色来颁发 LDC，该命令可从 `crypto ca trustpoint` 配置模式访问。

`proxy-ldc-issuer` 命令为该信任点定义了本地 CA 角色，以便为 TLS 代理颁发动态证书。此命令只能在使用“`enrollment self`”的信任点下配置。

CR_Examples

以下示例显示如何创建内部本地 CA 来签署电话的 LDC。此本地 CA 创建为启用了 `proxy-ldc-issuer` 的常规自签名信任点。

```
ciscoasa(config)# crypto ca trustpoint ldc_server
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my_ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

Related Commands

命令	说明
ctl-provider	定义CTL 提供程序实例，然后进入提供程序配置模式。
servertrust-point	指定要在 TLS 握手期间呈现的代理信任点证书。
showtls-proxy	显示 TLS 代理。
tls-proxy	定义 TLS 代理实例并设置最大会话数。

proxy paired

要为 Azure 网关负载均衡器 (GWLB) 将 VNI 接口设置为 ASA Virtual 的配对代理模式，请在接口配置模式下使用 **proxy paired** 命令。要删除代理，请使用此命令的形式。

proxy paired
no proxy paired

Command Default 无默认为行为或值。

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
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

命令	说明
debug vxlan	调试 VXLAN 流量。
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。

命令	说明
external-port	设置外部 VXLAN 端口。
external-segment-id	指定 VNI 接口的 VXLAN 外部段 ID。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
internal-port	设置内部 VXLAN 端口。
internal-segment-id	指定 VNI 接口的 VXLAN 内部段 ID。
nve	指定网络虚拟化终端实例。
peer ip	手动指定对等 VTEP IP 地址。
show interface vni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show nve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

proxy-server (已弃用)

要为以下项下的电话代理功能配置 HTTP 代理（该功能已写入 IP 电话的配置文件）：
<proxyServerURL>标记，请在电话代理配置模式下使用 **proxy-server** 命令。要从电话代理中删除 HTTP 代理配置，请使用此命令的 **no** 形式。

proxy-server *address* *ip_address* *listen_port* [*ifc*] **interface**
no proxy-server *address* *ip_address* *listen_port* [*ifc*] **interface**

Syntax Description

interface *ifc* 在 ASA 上指定 HTTP 代理所在的接口。

ip_address 指定 HTTP 代理的 IP 地址。

侦听端口 指定 HTTP 代理的侦听端口。如果未指定，则默认为 8080。

Command Default

如果未指定侦听端口，则默认情况下会将端口配置为 8080。

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

8.0(4) 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

为电话代理设置代理服务器配置选项，可以在 DMZ 或外部网络上使用 HTTP 代理，其中的所有 IP 电话 URL 都将定向到电话上服务的代理服务器。此设置容纳不允许返回公司网络的非安全 HTTP 流量。

根据 IP 电话和 HTTP 代理服务器所在位置，输入的 *ip_address* 应该是全局 IP 地址。

如果代理服务器位于 DMZ 中而 IP 电话位于网络外部，则 ASA 会查找以查看是否存在 NAT 规则，并使用全局 IP 地址写入配置文件。

当主机名可由 ASA 解析为 IP 地址（例如，配置了 DNS 查找）时，您可以在 *ip_address* 参数中输入主机名，因为 ASA 会将主机名解析为 IP 地址。

默认情况下，“企业参数”下配置的电话 URL 参数在 URL 中使用 FQDN。如果 HTTP 代理的 DNS 查找无法解析 FQDN，则可能需要更改这些参数以使用 IP 地址。

要确保代理服务器 URL 已正确写入 IP 电话配置文件，请在以下路径下检查 IP 电话上的 URL：设置 (Settings) = “设备配置” (Device Configuration) = “HTTP 配置” (HTTP configuration) = “代理服务器 URL” (Proxy Server URL)。

电话代理不会检查此流向代理服务器的 HTTP 流量。

如果 ASA 位于 IP 电话和 HTTP 代理服务器的路径中，请使用现有的调试技术（例如系统日志和捕获）对代理服务器进行故障排除。

使用电话代理时，您只能配置一个代理服务器，您可以在其中选择一个代理服务器。配置代理服务器

CR_Examples

以下示例显示如何使 proxy-server 用命令为电话代理配置 HTTP 代理服务器：

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

Related Commands

命令	说明
phone-proxy	配置电话代理实例。

proxy single-arm

要为 VXLAN VNI 接口启用单臂代理，请在接口配置模式下使用 **proxy single-arm** 命令。要禁用代理，请使用此命令的形式。

proxy single-arm
no proxy single-arm

此命令没有任何参数或关键字。

Command Default

无默认为或值。

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
接口配置	• 是	• —	• 是	• —	—

Command History

版本	修改

9.17(1)	我们添加了此命令。

使用指南

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。此使用案例要求您将 VNI 接口配置为单臂代理。另请确保启用 **same-security-traffic permit intra-interface**，以允许流量从 VTEP 源接口流出。

CR_Examples

以下示例将 VNI 接口配置为单臂代理：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。

命令	说明
encapsulationgeneve	将 NVE 实例设置为 Geneve 封装。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。

ptp domain

要指定 ISA 3000 上所有 PTP 端口的域编号，请在特权 EXEC 或全局配置模式下使用 **ptpdomain** 命令。域编号，范围为 0 至 255；默认值为 0。在与配置的域不同的域上接收到的数据包将被视为常规多播数据包，并且不会经过任何 PTP 处理。要将域号重置为默认值 0，请使用此命令的 **no** 形式。

ptp domain*domain_num*
no ptp domain



注释 此命令仅在 Cisco ISA 3000 设备上可用。

Syntax Description

domain_num 为 ISA 3000 上所有启用 PTP 的端口指定域编号。

Command Default

默认 **ptpdomain** 数量为 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
特权 EXEC	• 是	• 支持	• 支持	—	—

Command History

版本 修改

9.7(1) 添加了此命令。

使用指南

该命令也 **ptpdomain** 可在全局配置模式下使用。

CR_Examples

以下示例展示如何使用 **ptpdomain** 命令将 PTP 域编号设置为 127：

```
ciscoasa# ptp domain 127
```

Related Commands

命令	说明
showptpport	显示 PTP 接口/端口信息。

ptp enable

要在 ISA 3000 的接口上启用 PTP，请在接口配置模式下使用该 **ptpenable** 命令。使用 **ptpmode** 命令指定将启用 PTP 的模式。要禁用接口上的 PTP，请使用此命令 **no** 的形式。出入该接口的 PTP 数据包将像常规组播数据包一样处理。

ptp enable
no ptp enable



注释 此命令仅在 Cisco ISA 3000 设备上可用。

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，在透明模式下对所有 ISA 3000 接口启用 PTP。在路由模式下，必须添加必要的配置以确保允许 PTP 数据包通过设备。

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	• 支持	• 支持	—	—

Command History

版本 修改
9.7(1) 添加了此命令。

使用指南

该命令只能在接口配置模式下输入。

仅允许在物理接口上使用此命令。不允许在子接口、其他虚拟接口或管理接口上使用此类型。

加入父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。

如果未在任何模式下启用 PTP，则接受此命令，但不会产生任何效果。将发出警告。

Related Commands

命令	说明
showptpclock	显示 PTP 时钟属性。

ptp 模式

要在 ISA 3000 上指定 PTP 时钟模式，请在特权 EXEC 或全局配置模式下使用 **ptp mode** 命令。要在所有接口上禁用 PTP，请使用此命令的形式。

ptp mode e2transparent
no ptp mode



注释 此命令仅在 Cisco ISA 3000 设备上可用。

Syntax Description **e2transparent** 在 ISA 3000 上所有启用 PTP 的接口上启用端到端透明模式。

Command Default 默认情况下，端到端透明模式已禁用。

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
特权 EXEC	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.7(1)	添加了此命令。

使用指南 禁用端到端透明模式时，系统将像处理任何其他组播数据包一样处理所有 PTP 数据包。这相当于转发模式。

该命令也 **ptp mode** 可在全局配置模式下使用。

CR_Examples 以下示例展示如何使用 **ptp mode** 命令将 PTP 时钟模式设置为端到端透明模式：

```
ciscoasa# ptp mode e2transparent
```

命令	说明
show ptp internal-info	显示 PTP 统计数据和计数器信息。

public-key

要指定思科 Umbrella 所需的证书验证的 DNSCrypt 提供程序公钥，请在 Umbrella 配置模式下使用 **public-key** 命令。使用此 **no** 命令的形式可以删除密钥并使用默认密钥。

```
public-key dncrypt_key
no public-key [ dncrypt_key]
```

Syntax Description

dncrypt_key

Cisco Umbrella 服务器用于 DNSCrypt 的公钥。只有在用于 Cisco Umbrella 的 DNS 检测策略映射中启用 dncrypt 时，此项才与密钥相关。

密钥是一个 32 字节的十六进制值。在 ASCII 中输入十六进制值，每个 2 字节使用一个冒号分隔符。密钥长度为 79 个字节。从思科 Umbrella 获取此密钥。

Command Default

将使用默认密钥。

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
	9.10(1)	添加了此命令。

使用指南

如果想要在 DNS 检测策略映射中启用 DNSCrypt DNS，则可以选择配置用于证书验证的 DNSCrypt 提供商公钥。如果未配置密钥，则使用当前分布分发的默认公钥进行验证。

仅当 Cisco Umbrella 更改其用于 DNSCrypt 加密的公钥时，才需要配置密钥。

CR_Examples

以下示例配置与 Cisco Umbrella 配合使用的公钥。示例还显示如何在默认 DNS 检测策略映射（该映射用于全局 DNS 检测）中启用 DNSCrypt。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)#
public-keyB735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
```

```
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

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

Related Commands

命令	说明
dnsencrypt	为设备和思科 Umbrella 之间的连接启用 DNSCrypt 加密。
inspectdns	启用 DNS 检测。
policy-map type inspect dns	创建 DNS 检测策略映射。
timeoutedns	配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。
token	确定在思科 Umbrella 中注册时所需的 API 令牌。
umbrella-global	配置思科 Umbrella 全局参数。

publish-crl

要允许其他 ASA 验证本地 CA 颁发的证书的吊销状态，请在 `ca-server` 配置模式下使用 `publish-crl` 命令允许直接从和 ASA 上的接口下载 CRL。要使 CRL 不可下载，请使用此命令的 `no` 形式。

`[no] publish-crl interface interface [port portnumber]`

Syntax Description	<code>interface interface</code> 指定用于接口的 <code>nameif</code> ，例如 <code>gigabitethernet0/1</code> 。有关详细信息，请参阅 <code>interface</code> 命令。
	<code>port portnumber</code> （可选）指定接口设备期望在其上下载 CRL 的端口。端口号可以在 1-65535 范围内。

Command Default 默认状态 `publish-crl` 为 `no`。TCP 端口 80 是 HTTP 的默认端口。

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-server配置	• 是	—	• 是	—	—

Command History	版本 修改
	8.0(2) 添加了此命令。

使用指南

默认情况下，CRL 不可访问。您必须在需要的接口和端口上启用对 CRL 文件的访问。

TCP 端口 80 是 HTTP 默认端口号。如果配置非默认端口（端口 80 除外），请确保 `cdp-url` 配置包含新端口号，以便其他设备知道要访问此特定端口。

CRL 分发点 (CDP) 是 CRL 在本地 CA ASA 上的位置。您使用 `cdp-url` 命令配置的 URL 会嵌入到任何已颁发的证书中。如果没有为 CDP 配置特定位置，则默认 CDP URL 为：
`http://hostname.domain/+CSCOCA+/asa_ca.crl`。

如果在同一接口上启用无客户端 SSL VPN，则 HTTP 重定向和 CRL 下载请求将由同一 HTTP 侦听程序处理。侦听程序检查传入 URL，如果其与使用 `cdp-url` 命令配置的 URL 匹配，则下载 CRL 文件。如果 URL 与 `cdp-url` 命令不匹配，则连接将重定向到 HTTPS（如果启用了 HTTP 重定向）。

CR_Examples

在 `ca-server` 配置模式下输入的 `publish-crl` 命令示例启用外部接口的端口 70 以进行 CRL 下载：

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

Related Commands

命令	说明
cdp-url	为自动生成的 CRL 指定特定位置。
showinterface	显示接口的运行时间状态和统计信息。

pwd

要显示当前工作目录，请在特权 EXEC 模式下使用 **pwd**命令。

pwd

Syntax Description 此命令没有任何参数或关键字。

Command Default 根目录 (/) 为默认值。

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
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History	版本 修改
	7.0 添加了此命令。

使用指南 此命令在功能上与 **dir** 命令类似。

CR_Examples 以下示例显示如何显示当前工作目录：

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

Related Commands	命令	说明
	cd	将当前工作目录更改为指定的目录。
	dir	系统随即会显示目录的内容。
	more	显示文件的内容。



q - res

- [queue-limit \(priority-queue\)](#)，第 1397 页
- [queue-limit \(tcp-map\)](#)，第 1399 页
- [quick-start](#)，第 1401 页
- [quit](#)，第 1403 页
- [quota management-session](#)，第 1405 页
- [radius-common-pw](#)，第 1407 页
- [radius-reject-message](#)，第 1409 页
- [radius-with-expiry \(已弃用\)](#)，第 1410 页
- [raid](#)，第 1412 页
- [range](#)，第 1414 页
- [ras-rcf-pinholes](#)，第 1416 页
- [rate-limit](#)，第 1418 页
- [reactivation-mode](#)，第 1420 页
- [record-entry](#)，第 1422 页
- [record-route](#)，第 1424 页
- [redirect-fqdn](#)，第 1426 页
- [redistribute \(ipv6 router ospf\)](#)，第 1428 页
- [redistribute \(router eigrp\)](#)，第 1430 页
- [redistribute \(router ospf\)](#)，第 1432 页
- [redistribute \(router rip\)](#)，第 1435 页
- [redistribute isis](#)，第 1437 页
- [redundant-interface](#)，第 1439 页
- [regex](#)，第 1441 页
- [reload](#)，第 1446 页
- [remote-access threshold session-threshold-exceeded](#)，第 1449 页
- [rename \(class-map\)](#)，第 1450 页
- [rename \(EXEC 特权\)](#)，第 1451 页
- [renewal-reminder](#)，第 1453 页
- [replication http](#)，第 1455 页
- [request-command deny](#)，第 1457 页

- [request-data-size](#)，第 1459 页
- [request-queue](#)，第 1461 页
- [request-timeout](#) (已弃用)，第 1463 页
- [reserved-bits](#)，第 1465 页
- [reserve-port-protect](#)，第 1467 页
- [reset](#)，第 1468 页
- [resolver](#)，第 1470 页
- [responder-only](#)，第 1471 页
- [rest-api](#) (已弃用)，第 1473 页
- [restore](#)，第 1475 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 <i>pkt_num</i> 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，而无需更改或删除指定的 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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

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	<i>number</i> 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	<i>string</i> 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，将超时时间间隔设置为 9 秒，将重试间隔设置为 7 秒，并将 RADIUS Common 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 <i>psid</i> 。 <i>Psid</i> 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。使用此命令 **no** 的形式从配置中删除对象。

```
range ip_addr_1 ip_addr2
no range ip_addr_1 ip_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
```

命令	说明
clear configure object	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
```

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

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-map type inspect**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 ESMTTP、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-map type inspect**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 **inspect sip sip_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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	定义特殊的应用检查操作。
show running-config policy-map	显示所有当前的策略映射配置。

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 [ deadtimeminutes ] | timed }
no reactivation-mode { depletion [ deadtimeminutes ] | 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 “svrgrp1” 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-servers-group)# reactivation-mode depletion deadtime 15
ciscoasa
(config-aaa-server)#
exit
ciscoasa
(config)#
```

以下示例将名为 “svrgrp1” 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] trustpointtrustpointaddressip_address [domain-namedomain_name]
no
record-entry [capfcucmcucm-tftptftp] trustpointtrustpointaddressip_address [domain-namedomain_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-namedomain_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。
	addressip_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。
	trustpointtrust_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 cucml 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	<i>allow</i> 允许包含记录路由 IP 选项的数据包。
	<i>clear</i> 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，而无需更改或删除指定的 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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

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 进行负载平衡 **redirect-fqdnenable**。
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，请使用此命令的 **no** 形式。

```
redistributesource-protocol [ process-id] [include-connected{level-1|level-1-2|level-2}] [as-number]
[metric{metric-valuetransparent}] [metric-typetype-value] [match{external [1|2]
|internal|nssa-external [1|2] }] [tagtag-value] [route-mapmap-tag]
```

```
no redistributesource-protocol [ process-id] [include-connected{level-1|level-1-2|level-2}]
[as-number] [metric{metric-valuetransparent}] [metric-typetype-value] [match{external [1|2]
|internal|nssa-external [1|2] }] [tagtag-value] [route-mapmap-tag]
```

Syntax Description

<i>as_number</i>	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。
<i>map-tag</i>	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 <i>metric_value</i>	（可选）指定 OSPFv3 默认指标值，其范围为 0 到 16777214。
metric-type <i>metric_type</i>	（可选）指定与通告到 OSPFv3 路由域的默认路由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。
<i>process-id</i>	（可选）指定在启用 OSPFv3 路由进程时管理分配的编号。
route-map <i>map_name</i>	（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。
tagtag_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：

- **metricmetric-value: 0**
- **metric-typetype-value: 2**
- **match: internal、external1、external2**
- **tagtag-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 { { eigrppid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }  
| rip | static | connected } [metric bandwidth delay reliability load mtu] [route-map map_name]  
no redistribute { { eigrppid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }  
| rip | static | connected } [metric bandwidth delay 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 。
	eigrppid	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
router eigrp	创建 EIGRP 路由进程并进入该进程的配置模式。
show running-config router	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 { { ospfpid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }  
| rip | static | connected | eigrpas-number } [metricmetric_value] [metric-typemetric_type]  
[route-mapmap_name] [tagtag_value] [subnets]  
no redistribute { { ospfpid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }  
| rip | static | connected | eigrpas-number } [metricmetric_value] [metric-typemetric_type]  
[route-mapmap_name] [tagtag_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。
	eigrpas-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。
	metricmetric_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-typemetric_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 。
	ospfpid	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-mapmap_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。
tagtag_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
- **tagtag-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，请使用此命令 **no** 的形式。

```
redistribute { { ospfpid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }
| rip | static | connected | eigrpas-number } [metricmetric_value] [transparent] [route-mapmap_name]
no redistribute { { ospfpid [match { internal | external [1 | 2] | nssa-external [1 | 2] } ] }
| rip | static | connected | eigrpas-number } [metricmetric_value] [transparent] [route-mapmap_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。
eigrpas-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 。
ospfpid	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-mapmap_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：

- **metricmetric-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 **redistribute isis** 路由器 isis 配置模式下使用该命令。要禁用重新分配，请使用此命令 **no** 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-interface*redundantnumberactive-memberphysical_interface*

Syntax Description	active-member <i>physical_interface</i> 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。
	redundantnumber 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，请使用此命令 **no** 的形式。

```
regexname regular_expression
regexname [regular_expression]
```

Syntax Description

<i>name</i>	指定正则表达式名称，长度最多为 40 个字符。
<i>regular_expression</i>	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 **polycymaptypeinspect** 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-maptypepregex** 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 7: 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
<i>char</i>	字符	当字符不是元字符时，匹配原义字符。
<code>\r</code>	回车符	匹配回车符 0x0d。
<code>\n</code>	换行符	匹配换行符 0x0a。
<code>\t</code>	Tab	匹配制表符 0x09。
<code>\f</code>	换页符	匹配换页符 0x0c。
<code>\xNN</code>	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）。
<code>\NNN</code>	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 [ athh: mm[month day|day month] ] [cancel] [in [hh:] mm] [max-hold-time [hh:] mm] [noconfirm] [quick] [reason文本] [save-config]
```

Syntax Description	athh: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-access threshold** 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 添加了此命令。
(1)

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-server enable trap remote-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
```

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”：

rename (EXEC 特权)

```
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-reminderdays** 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-command deny** 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

无默认为行为或值。

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，请使用此命令 **no** 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 排队等待响应的最大 GTP 请求数，从 1 到 4294967295。 数

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
<code>showservice-policyinspectgtp</code>	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-attempts** 命令。）

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

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-map type inspect** 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 **lg** 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-map type inspect** 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 **inspect http http_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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	定义特殊的应用检查操作。
show running-config policy-map	显示所有当前的策略映射配置。

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。使用此命令 **no** 的形式可以恢复默认设置。

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

Syntax Description	ipv4ip_address 要使用的 Umbrella DNS 服务器的 IPv4 地址。
	ipv6ip_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 无默认为行为或值。

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-121-1fbff-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-121-1fbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-1fbff-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] [contextctx-name] [interfaceiname] [cert-passphrasevalue] [locationpath]

Syntax Description	cert-passphrasevalue	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。
	contextctx-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。
	interfaceiname	（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。
	locationpath	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 interfaceiname 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（使用命令 **cryptocatrustpoint**）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。



ret - rz

- [retries](#) , 第 1481 页
- [retry-count](#) , 第 1482 页
- [retry-interval](#) , 第 1484 页
- [reval-period](#) , 第 1486 页
- [revert webvpn all](#) , 第 1488 页
- [revert webvpn AnyConnect-customization](#) , 第 1489 页
- [revert webvpn customization](#) , 第 1491 页
- [revert webvpn plug-in protocol](#) , 第 1493 页
- [revert webvpn translation-table](#) , 第 1495 页
- [revert webvpn url-list](#) , 第 1497 页
- [revert webvpn webcontent](#) , 第 1498 页
- [revocation-check](#) , 第 1499 页
- [rewrite \(已弃用\)](#) , 第 1501 页
- [re-xauth](#) , 第 1503 页
- [rip authentication mode](#) , 第 1505 页
- [rip authentication key](#) , 第 1507 页
- [rip receive version](#) , 第 1509 页
- [rip send version](#) , 第 1510 页
- [rmdir](#) , 第 1511 页
- [路由](#) , 第 1513 页
- [route-map](#) , 第 1516 页
- [route priority high](#) , 第 1519 页
- [router-alert](#) , 第 1520 页
- [router bgp](#) , 第 1522 页
- [router eigrp](#) , 第 1524 页
- [router-id](#) , 第 1526 页
- [router-id cluster-pool](#) , 第 1528 页
- [router isis](#) , 第 1530 页
- [router ospf](#) , 第 1531 页
- [router rip](#) , 第 1533 页

- [rtp-conformance](#) , 第 1535 页
- [rtp-min-port rtp-max-port](#) (已弃用) , 第 1537 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，请使用此命令 **no** 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，请使用此命令 **no** 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-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default usergroup	如果 ASA 无法确定进入 ASA 的用户身份，则指定默认用户名和/或组。
health-check application	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。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，以指示请求来自哪个组织。
match usergroup	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即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。
scansafe general-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。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
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-intervalaaa-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
<code>nac-policy-nac-framework</code> 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 <code>group-policy</code> 配置模式移至 <code>nac-policy-nac-framework</code> 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。
cou 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
```

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 **revert webvpn AnyConnect-customization** 命令。

revert webvpn AnyConnect-customization *type 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。
revertwebvpnull	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。
revertwebvpncustomization	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	<i>protocol</i> 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： <pre>ciscoasa# revert webvpn plug-in protocol rdp ciscoasa</pre>

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-table**language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
revertwebvpnnall	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 templatenam

Syntax Description	templatenam 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
```

命令	说明
revertwebvpnull	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-check ?
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 orderinteger {enable | disable} resource-maskstring [资源name 名称]
no rewrite orderinteger {enable | disable} resource-maskstring [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-webvpn)#
rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

命令	说明
<code>apcf</code>	指定用于特定应用的非标准规则。
<code>proxy-bypass</code>	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令 **showcryptoipsecsa** 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**] *stringkey_idid*
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。
	<i>ID</i>	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。
	<i>string</i>	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 yWlvi0qJAnGK5MRWQzrhIohkGPlwKb 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，请使用此命令 **no** 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*] [**tracknumber**] | **tunneled**]
接口**no route**名称 IP地址 网络掩码 网关IP[[*metric*] [**tracknumber**] **tunneled**]

Syntax Description

<i>gateway_ip</i>	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， <i>gateway_ip</i> 参数是可选的。
<i>interface_name</i>	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。
<i>ip_address</i>	指定内部或外部网络 IP 地址。
<i>metric</i>	（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。
<i>netmask</i>	指定要应用于 <i>ip_address</i> 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 **tunneledECMP**。

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

<i>name</i>	为路线图定义一个有意义的名称。 <code>redistribute</code> 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。
<i>permit</i>	如果满足此路由映射的匹配条件，并且指定了 <code>permit</code> 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 <code>permit</code> 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。 <code>permit</code> 关键字是默认的。
<i>deny</i>	如果满足路由映射的匹配条件并且指定了 <code>deny</code> 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。
<i>sequence-number</i>	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 <code>no</code> 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。
92l(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，也不会为进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 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:Incomplete 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 **routepriorityhigh** 命令。要删除 IP 前缀优先级，请使用此命令的 **no** 形式

route priority hightag-value
no route priority hightag-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 **routepriorityhigh**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 **routepriorityhigh** 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	<i>allow</i> 允许包含 Router Alert IP 选项的数据包。
	<i>clear</i> 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，而无需更改或删除指定的 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)# eoool 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-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
show running-config policy-map	显示所有当前的策略映射配置。

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 **router eigrp** 命令。要禁用 EIGRP 路由，请使用此命令 **no** 的形式。

```
router eigrpas-number
no router eigrpas-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 **router eigrp** 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：

- 启用 **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。
- 一定 **default-metric** 义重新分配到 EIGRP 路由进程的路由的默认指标。
- 一定 **distance eigrp** 配置内部和外部 EIGRP 路由的管理距离。
- 一定 **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。
- 一定 **eigrplog-neighbor-warnings** 用/禁用邻居警告消息的记录。
- **eigrp router-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-idid** 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.Dip_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
	<i>ip_pool</i>	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-idid** 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 ospfpid
no router ospfpid

Syntax Description	<i>pid</i> OSPF 路由进程内部使用的标识参数；其有效值范围为 1 至 65535。 <i>pid</i> 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 <i>pid</i> 指定的 <i>OSPF</i> 路由进程。在 ASA 上本地分配 <i>PID</i> 。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 **router rip** 命令。要禁用 RIP 路由进程，请使用此命令 **no** 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 **router rip** 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 **no router rip** 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 **router rip** 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。

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

- 启用 **auto-summary** 用/禁用路由自动汇总。
- **default-information originate**- 分发默认路由。
- **distribute-list in**- 过滤传入路由更新中的网络。
- **distribute-list out**- 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。
- 用 **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-listmyriplistextendedpermitudpnyanyeqrip
```

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 根据信令交换将负载类型强制为音频/视频。
型

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-map type inspect	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-port rtp-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-max-port port2
no rtp-min-port port1 rtp-max-port 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-max-port 32770
```

Related Commands

命令	说明
phone-proxy	配置电话代理实例。

rtp-min-port rtp-max-port (已弃用)

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。