思科 ASA 系列命令参考，I 至 R 命令

更新日期：2014 年 11 月 12 日

Cisco Systems, Inc.
www.cisco.com

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

文本部件号： 不适用，仅限在线使用

思科 ASA 系列命令参考，I 至 R 命令

第 1 部分

I 命令

第 1 章

icmp 至 import webvpn webcontent 命令

icmp

要配置终止于 ASA 接口的 ICMP 流量的访问规则，请使用 **icmp** 命令。要删除配置，请使用此命令的 **no** 形式。

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

语法说明

deny	匹配条件时拒绝访问。
icmp_type	（可选） ICMP 消息类型 （请参阅表 1-1）。
if_name	接口名称。
ip_address	将 ICMP 消息发送到接口的主机的 IP 地址。
net_mask	要应用于该主机 IP 地址的网络掩码。
permit	匹配条件时允许访问。

默认值

ASA 的默认行为是允许所有 ICMP 流量到 ASA 接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

icmp 命令控制终止于任何 ASA 接口的 ICMP 流量。如果未配置 ICMP 控制列表， ASA 将接受终止于任何接口（包括外部接口）的所有 ICMP 流量。但在默认情况下， ASA 不响应传至广播地址的 ICMP 回应请求。

ASA 仅响应发送到接收流量的接口的 ICMP 流量；您无法通过接口将 ICMP 流量发送到远端接口。

icmp deny 命令禁止 ping 接口， **icmp permit** 命令则允许 ping 接口。禁用 ping 命令后，在网络上无法检测到 ASA。这也称为可配置的代理 ping。

对于通过 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。

建议对 ICMP 不可达消息类型 （类型 3）授予许可权限。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 ICMP 控制列表配置用于接口，则 ASA 会先匹配指定的 ICMP 流量，然后对该接口上所有其他 ICMP 流量应用隐含的拒绝。也就是说，如果先匹配的条目是 permit 条目，会继续处理 ICMP 数据包。如果第一个匹配的条目是 deny 条目或者条目不匹配， ASA 会丢弃 ICMP 数据包并生成系统日志消息。例外情况是未配置 ICMP 控制列表；这种情况下假定是 permit 语句。

表 1-1 列出了支持的 ICMP 类型值。

表 1-1　ICMP 类型和文字

ICMP 类型	文字
0	echo-reply
3	unreachable
8	echo
11	time-exceeded

示例

以下示例拒绝所有 ping 请求，而允许外部接口上所有不可达的消息：

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

继续对要在其上拒绝 ICMP 流量的每个其他接口输入 **icmp deny any** *interface* 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-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
```

相关命令

命令	说明
clear configure icmp	清除 ICMP 配置。
debug icmp	为 ICMP 启用调试信息的显示。
show icmp	显示 ICMP 配置。
timeout icmp	配置 ICMP 的空闲超时。

icmp unreachable

要配置终止于 ASA 接口的 ICMP 流量的不可达 ICMP 消息速率限制，请使用 **icmp unreachable** 命令。要删除配置，请使用此命令的 **no** 形式。

icmp unreachable rate-limit *rate* **burst-size** *size*

no icmp unreachable rate-limit *rate* **burst-size** *size*

语法说明

rate-limit *rate*	将不可达消息的速率限制设置在每秒 1 条消息和 100 消息之间。默认为每秒 1 条消息。
burst-size *size*	设置突发速率，值在 1 和 10 之间。系统目前未使用此关键字，因此您可以选择任何值。

默认值

默认速率限制为每秒 1 条消息。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(2)	引入了此命令。

使用指南

如果您允许 ICMP 消息 （包括不可达的消息）终止于 ASA 接口 （请参阅 **icmp** 命令），则您可以控制不可达消息的速率。

需要使用此命令及 **set connection decrement-ttl** 命令，才允许经过 ASA （它将 ASA 显示为其中一个跃点）的跟踪路由。

示例

以下示例用于减少生存时间并设置 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 1
```

相关命令

命令	说明
clear configure icmp	清除 ICMP 配置。
debug icmp	为 ICMP 启用调试信息的显示。
set connection decrement-ttl	减少数据包的生存时间值。
show icmp	显示 ICMP 配置。
timeout icmp	配置 ICMP 的空闲超时。

icmp-object

要将 ICMP 类型添加到 ICMP 对象组，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 **no** 形式。

icmp-object *icmp_type*

no icmp-object *icmp_type*

语法说明

icmp_type	指定 ICMP 类型名称或编号 (0-255)。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

icmp-object 命令与 **object-group icmp-type** 命令一起用于定义 ICMP 对象。它用于 icmp-type 配置模式中。

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

ICMP 类型编号和名称包括：

编号	ICMP 类型名称
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**

编号	ICMP 类型名称
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**

示例

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
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object-group** 命令。
object-group	定义对象组以优化配置。
show running-config object-group	显示当前对象组。

id-cert-issuer

要指示系统是否接受 CA 颁发的与此信任点关联的对等证书，在 crypto ca-trustpoint 配置模式下使用 **id-cert-issuer** 命令。要禁止 CA 颁发的与该信任点关联的证书，请使用此命令的 **no** 形式。这用于代表广泛使用的根 CA 的信任点。

id-cert-issuer

no id-cert-issuer

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为启用 （接受身份证书）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用此命令将仅允许接受广泛使用的根证书的下级证书颁发的证书。如果您不允许此功能， ASA 将拒绝此颁发机构签署的任何 IKE 对等证书。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并让管理员接受中心信任点的颁发机构签署的身份证书：

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

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。
default enrollment	将注册参数恢复为其默认值。
enrollment retry count	指定尝试发送注册请求的重试次数。
enrollment retry period	指定在尝试发送注册请求之前要等待的分钟数。
enrollment terminal	指定使用此信任点进行剪切粘贴注册。

id-mismatch

要对额外的 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，请使用此命令的 **no** 形式。

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] **action log**]

语法说明

count *number*	系统消息日志发送之前的最大不匹配实例数。
duration *seconds*	要监控的时段 （秒）。

默认值

此命令默认禁用。如果在此命令启用时未指定选项，默认速率是在 3 秒的时段内为 30。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	**修改**
7.2(1)	引入了此命令。

使用指南

DNS ID 不匹配程度高可能表示存在缓存中毒攻击。此命令可用于此类攻击的监控和告警。如果不匹配率超过配置的值，将显示系统消息日志摘要。 **id-mismatch** 命令为系统管理员提供基于事件的常规系统消息日志以外的其他信息。

示例

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
```

相关命令

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

id-randomization

要随机生成 DNS 查询的 DNS 标识符，在参数配置模式下使用 **id-randomization** 命令。要禁用此功能，请使用此命令的 **no** 形式。

id-randomization

no id-randomization

语法说明

此命令没有任何参数或关键字。

默认值

默认为禁用。来自 DNS 查询的 DNS 标识符未修改。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

ID 随机化可帮助防范缓存中毒攻击。

示例

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
```

相关命令

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

id-usage

要指定如何使用已注册的证书身份，请在 crypto ca trustpoint 配置模式下使用 **id-usage** 命令。要将证书的使用设为默认值，请使用此命令的 **no** 形式。

id-usage {**ssl-ipsec** | **code-signer** | **mdm-proxy**}

no id-usage {**ssl-ipsec** | **code-signer** | **mdm-proxy**}

语法说明

code-signer	此证书代表的设备身份用作 Java 代码签名人来验证提供给远程用户的小应用。
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。
mdm-proxy	此证书代表的设备身份可用于代表 MDM 客户端向 ISE MDM 服务器进行 ASA MDM 代理服务身份验证。

默认值

id-usage 命令默认为 **ssl-ipsec**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.3(1)	此命令现在可用于 MDM 代理服务。

使用指南

根据部署要求，远程访问 VPN 可以使用 SSL 和 / 或 IPsec 协议，以允许访问几乎任何网络应用或资源。 **id-usage** 命令可用于指定访问各种证书保护资源的类型。

CA 身份以及某些情况下的设备身份采用 CA 颁发的证书。 crypto ca trustpoint 配置模式下的所有命令控制 CA 特定配置参数，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。

一个信任点配置中只能显示 **id-usage** 命令的单个实例。要为 **code-signer** 和 / 或 **ssl-ipsec** 选项启用信任点，请使用可指定其中一个或两个选项的单个实例。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并将其指定为代码签名人证书：

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

以下示例进入一般信任点的 crypto ca trustpoint 配置模式，并将其指定为代码签名人证书及 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，并重置它以限制仅用于 SSL 或 IPsec 连接：

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# no id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

以下示例进入信任点 MDMtrustpoint 的 crypto ca trustpoint 配置模式，并将其指定为 mdm-proxy 证书：

```
ciscoasa(config)# crypto ca trustpoint MDMtrustpoint
ciscoasa(config-ca-trustpoint)# id-usage mdm-proxy
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。
java-trustpoint	配置 WebVPN Java 对象签名设施以使用来自指定信任点位置的 PKCS12 证书和密钥材料。
ssl trust-point	指定代表接口的 SSL 证书的证书。
trust-point (tunnel-group ipsec-attributes mode)	指定用于标识要发送到 IKE 对等项的证书的名称。
validation-policy	指定用于验证与用户连接关联的证书的条件。
trustpoint (config-mdm-proxy mode)	指定用于 ASA 向 ISE MDM 进行身份验证的信任点。

igmp

要在接口上恢复 IGMP 处理，请在接口配置模式下使用 **igmp** 命令。要在接口上禁用 IGMP 处理，请使用此命令的 **no** 形式。

igmp

no igmp

语法说明

此命令没有任何参数或关键字。

默认值

已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在运行的配置中只出现此命令的 **no** 形式。

示例

以下示例在所选的接口上禁用 IGMP 处理：

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

相关命令

命令	说明
show igmp groups	显示其接收器直接连接到 ASA 并且通过 IGMP 获知的组播组。
show igmp interface	显示接口的组播信息。

igmp access-group

要控制接口所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 **igmp access-group** 命令。要在接口上禁用组，请使用此命令的 **no** 形式。

igmp access-group *acl*

no igmp access-group *acl*

语法说明

acl	IP 访问列表的名称。您可以指定标准或 / 和扩展的访问列表。但是，如果您指定扩展的访问列表，只会匹配目标地址；对来源地址应指定 **any**。

默认值

所有组都可在一个接口上加入。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

示例

以下示例限制只有访问列表 1 允许的主机才能加入组：

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

相关命令

命令	说明
show igmp interface	显示接口的组播信息。

igmp forward interface

要将收到的所有 IGMP 主机报告和留言转发到指定的接口，请在接口配置模式下使用 **igmp forward interface** 命令。要取消转发，请使用此命令的 **no** 形式。

igmp forward interface *if-name*

no igmp forward interface *if-name*

语法说明

if-name	接口的逻辑名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

使用指南

在输入界面上输入此命令。此命令用于末节组播路由，无法与 PIM 同时配置。

示例

以下示例将 IGMP 主机报告从当前接口转发到指定的接口：

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

相关命令

命令	说明
show igmp interface	显示接口的组播信息。

igmp join-group

要将某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。要取消组成员身份，请使用此命令的 **no** 形式。

igmp join-group *group-address*

no igmp join-group *group-address*

语法说明

group-address	组播组的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

使用指南

此命令可将 ASA 接口配置为组播组的成员。**igmp join-group** 命令使 ASA 接受并转发发往指定组播组的组播数据包。

要将 ASA 配置为转发组播流量而不成为组播组的成员，可使用 **igmp static-group** 命令。

示例

以下示例配置所选接口以加入 IGMP 组 255.2.2.2：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp join-group 225.2.2.2
```

相关命令

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

igmp limit

要限制各接口上的 IGMP 状态数，请在接口配置模式下使用 **igmp limit** 命令。要恢复默认限制，请使用此命令的 **no** 形式。

igmp limit *number*

no igmp limit [*number*]

语法说明

number	接口上允许的 IGMP 状态数。有效值范围为 0 到 500。默认值为 500。将此值设为 0 可阻止添加所了解的组，但仍可添加手动定义的成员身份 （使用 **igmp join-group** 和 **igmp static-group** 命令）。

默认值

默认值为 500。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。它取代了 **igmp max-groups** 命令。

示例

以下示例将接口上的 IGMP 状态数限制为 250：

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

相关命令

命令	说明
igmp	恢复接口上的 IGMP 处理。
igmp join-group	将接口配置为指定组的本地连接成员。
igmp static-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 **igmp query-interval** 命令。要恢复默认频率，请使用此命令的 **no** 形式。

igmp query-interval *seconds*

no igmp query-interval *seconds*

语法说明

seconds	发送 IGMP 主机查询消息的频率 （秒）。有效值范围为 1 到 3600。默认值为 125 秒。

默认值

默认查询间隔为 125 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

使用指南

组播路由器发送主机查询消息来发现哪些组播组在连接到接口的网络上有成员。主机使用 IGMP 报告消息做出响应，表示它们要接收特定组的组播数据包。主机查询消息的目标地址为所有主机的组播组，其地址为 224.0.0.1， TTL 值为 1。

局域网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，根据局域网上运行的组播路由协议选择指定的路由器。
- 对于 IGMP 版本 2，指定的路由器是子网上 IP 地址最小的组播路由器。

如果路由器在超时期 （由 **igmp query-timeout** 命令控制）内没有收到任何查询，它将变成查询器。

注意事项　更改此值可能严重影响组播转发。

示例

以下示例将 IGMP 查询间隔改为 120 秒：

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

相关命令

命令	说明
igmp query-max-response-time	配置 IGMP 查询中通告的最长响应时间。
igmp query-timeout	配置在上一个查询器停止查询后路由器接管为接口的查询器之前的超时期。

igmp query-max-response-time

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

igmp query-max-response-time *seconds*

no igmp query-max-response-time *seconds*

语法说明

seconds	IGMP 查询中通告的最长响应时间 （秒）。有效值为从 1 到 25。默认值为 10 秒。

默认值

10 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

使用指南

此命令仅在 IGMP 版本 2 或 3 运行时才有效。

此命令控制响应方在路由器删除组之前可以响应 IGMP 查询消息的时间。

示例

以下示例将最长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
```

相关命令

命令	说明
igmp query-interval	配置接口发送 IGMP 主机查询消息的频率。
igmp query-timeout	配置在上一个查询器停止查询后路由器接管为接口的查询器之前的超时期。

igmp query-timeout

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

igmp query-timeout *seconds*

no igmp query-timeout *seconds*

语法说明

seconds	路由器在上一个查询器停止查询后接管为查询器之前等待的秒数。有效值为从 60 到 300 秒。默认值为 255 秒。

默认值

默认查询间隔为 255 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令需要 IGMP 版本 2 或 3。

示例

以下示例配置路由器在收到最后一条查询后等待 200 秒即接管为接口的查询器：

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

相关命令

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

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 **igmp static-group** 命令。要删除静态组条目，请使用此命令的 **no** 形式。

igmp static-group *group*

no igmp static-group *group*

语法说明

group	IP 组播组地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **igmp static-group** 命令配置时，ASA 接口不接受发往指定组本身的组播数据包，而只是转发它们。要将 ASA 配置为接受并转发特定组播组的组播数据包，请使用 **igmp join-group** 命令。如果 **igmp join-group** 命令配置用于与 **igmp static-group** 命令相同的组地址，则 **igmp join-group** 命令优先且该组像本地加入的组一样运行。

示例

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
```

相关命令

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

igmp version

要配置接口使用 IGMP 的哪个版本，请在接口配置模式下使用 **igmp version** 命令。要将版本恢复为默认值，请使用此命令的 **no** 形式。

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

语法说明

1	IGMP 版本 1。
2	IGMP 版本 2。

默认值

IGMP 版本 2。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已移到接口配置模式。早期版本要求您进入组播接口配置模式（该模式已不再可用）。

使用指南

子网上的所有路由器必须都支持相同的 IGMP 版本。主机可以拥有任何 IGMP 版本 （1 或 2），ASA 将正确检测其是否存在并适当地查询它们。

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

示例

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
```

相关命令

命令	说明
igmp query-max-response-time	配置 IGMP 查询中通告的最长响应时间。
igmp query-timeout	配置在上一个查询器停止查询后路由器接管为接口的查询器之前的超时期。

ignore-ipsec-keyusage

要取消 IPsec 客户端证书上的密钥使用检查，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

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	此命令当初是作为一种安全措施引入的，但同时被弃用。请注意，未来的版本可能不会提供取消密钥使用检查的功能。

使用指南

使用此命令表示不验证 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中的值。此命令将忽略密钥使用检查，可用于不合规的部署。

示例

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)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。

ignore lsa mospf

要在路由器收到 LSA 类型 6 MOSPF 数据包时取消发送系统日志消息，请在路由器配置模式下使用 **ignore lsa mospf** 命令。要恢复发送系统日志消息，请使用此命令的 **no** 形式。

ignore lsa mospf

no ignore lsa mospf

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

不支持类型 6 MOSPF 数据包。

示例

以下示例将忽略 LSA 类型 6 MOSPF 数据包：

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

相关命令

命令	说明
show running-config router ospf	显示 OSPF 路由器配置。

ignore-ssl-keyusage

要取消 SSL 客户端证书上的密钥使用检查，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

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	此命令当初是作为一种安全措施引入的，但同时被弃用。请注意，未来的版本可能不会提供取消密钥使用检查的功能。

使用指南

使用此命令表示不验证 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中的值。此命令将忽略密钥使用检查，可用于不合规的部署。

示例

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)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。

ike-retry-count

要配置使用 IKE 的 Cisco AnyConnect VPN 客户端在回退到 SSL 尝试连接之前应执行的连接重试最大数，请在组策略 webvpn 配置模式或用户名 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*]

语法说明

none	指定不允许重试。
value	指定 Cisco AnyConnect VPN 客户端在初始连接失败后执行的最大连接重试次数 (1-10)。

默认值

默认允许的重试次数为 3。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令

使用指南

使用 **ike-retry-count** 命令控制 Cisco AnyConnect VPN 客户端应尝试使用 IKE 连接的次数。如果客户端在此命令指定的重试次数后无法使用 IKE 连接，将回退到 SSL 来尝试连接。此值将覆盖 Cisco AnyConnect VPN 客户端中存在的任何值。

注　要支持从 IPsec 回退到 SSL， **vpn-tunnel-protocol** 命令必须配置有 **svc** 和 **ipsec** 参数。

示例

以下示例对名为 FirstGroup 的组策略将 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)#
```

以下示例对用户名 Finance 将 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)#
```

相关命令

命令	说明
group-policy	创建或编辑组策略。
ike-retry-timeout	指定两次 IKE 重试间隔的秒数。
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

要指定预共享密钥支持基于预共享密钥的 IKEv1 连接，请在隧道组 ipsec-attributes 配置模式下使用 **pre-shared-key** 命令。要恢复默认值，请使用此命令的 **no** 形式。

pre-shared-key *key*

no pre-shared-key

语法说明

key	指定在 1 到 128 个字符之间的字母数字密钥。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(1)	命令名称已从 **pre-shared-key** 修改为 **ikev1 pre-shared-key**。

使用指南

您可以将此属性应用于所有 IPsec 隧道组类型。

示例

以下命令在 config-ipsec 配置模式下输入，指定预共享密钥 XYZX 支持名为 209.165.200.225 的 IPSec 局域网至局域网隧道组的 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)#
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置此组的隧道组 IPsec 属性。

ikev1 trust-point

要指定信任点名称以标识要发送到 IKEv1 对等设备的证书，请在 tunnel-group ipsec-attributes 模式下使用 **trust-point** 命令。要消除信任点指定，请使用此命令的 **no** 形式。

trust-point *trust-point-name*

no trust-point *trust-point-name*

语法说明

trust-point-name	指定要使用的信任点的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
隧道组 ipsec 属性	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。
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。

示例

以下示例进入隧道 ipsec 配置模式，配置信任点，以便对名为 209.165.200.225 的 IPsec 局域网到局域网隧道组标识要发送到 IKEv1 对等设备的证书：

```
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
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置此组的隧道组 IPsec 属性。

ikev1 user-authentication

要配置在 IKE 期间使用混合身份验证，请在隧道组 ipsec 属性配置模式下使用 **ikev1 user-authentication** 命令。要禁用混合身份验证，请使用此命令的 **no** 形式。

ikev1 user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no ikev1 user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

语法说明

hybrid	指定在 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，也称为扩展的用户身份验证。

默认值

默认身份验证方法是 XAUTH 或扩展的用户身份验证。默认为所有接口。

注　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。如果将隧道组设为任何其他值 （例如 isakmp ikev1-user-authentication none），则无法建立 L2TP over IPsec 会话。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.4(1)	命令名称已从 **isakmp ikev1-user-authentication** 更改为 **ikev1 user-authentication**。

使用指南

需要对 ASA 身份验证使用数字证书而对远程 VPN 用户身份验证使用不同的传统方法 （如 RADIUS、TACACS + 或 SecurID）时，可使用此命令。此命令将 IKE 的第 1 阶段分为以下两步，这两步一起称为混合身份验证：

1. ASA 使用标准公共密钥技术对远程 VPN 用户进行身份验证。这将建立单向身份验证的 IKE 安全关联。
2. 先进行 XAUTH 交换，然后对远程 VPN 用户进行身份验证。此扩展的身份验证可以使用支持的传统身份验证方法之一。

注　必须先配置身份验证服务器、创建预共享密钥并配置信任点，然后才可将身份验证类型设置为混合。

当交换类型为主模式时，将会拒绝 IPsec 混合 RSA 身份验证类型。

省略可选的 *interface* 参数时，该命令将应用于所有接口，并在未指定各接口的命令时用作备用。如果为一个隧道组指定了两个 **ikev1 user-authentication** 命令，其中一个使用 *interface* 参数而另一个未使用，则指定接口的命令优先用于该特定接口。

示例

以下示例命令在称为 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)#
```

相关命令

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

ikev2 local-authentication

要为 IKEv2 局域网到局域网连接指定本地身份验证，请在隧道组 ipsec 属性配置模式下使用 **ikev2 local-authentication** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ikev2 local-authentication {**pre-shared-key** *key_value* | *certificate trustpoint*}

no ikev2 local-authentication {**pre-shared-key** *key_value* | *certificate trustpoint*}

语法说明

certificate	指定证书身份验证。
key_value	密钥值，从 1 到 128 个字符。
pre-shared-key	指定用于验证远程对等设备的本地预共享密钥。
trustpoint	指定用于标识要发送到远程对等设备的证书的信任点。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

此命令仅适用于 IPsec IKEv2 局域网至局域网隧道组。

示例

以下命令指定预共享密钥 XYZX 支持名为 209.165.200.225 的 IPsec 局域网到局域网隧道组的 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)# ikev2 local-authentication pre-shared-key XYZX
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置此组的隧道组 IPsec 属性。

ikev2 remote-authentication

要为 IPsec IKEv2 局域网到局域网连接指定远程身份验证，请在隧道组 ipsec 属性配置模式下使用 **ikev2 remote-authentication** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ikev2 remote-authentication {**pre-shared-key** *key_value* | **certificate** | }

no ikev2 remote-authentication {**pre-shared-key** *key_value* | **certificate** | }

语法说明

certificate	指定证书身份验证。
key_value	密钥值，从 1 到 128 个字符。
pre-shared-key	指定用于验证远程对等设备的本地预共享密钥。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

此命令仅适用于 IPsec IKEv2 局域网至局域网隧道组。

示例

以下命令指定预共享密钥 XYZX 支持名为 209.165.200.225 的 IPsec 局域网到局域网隧道组的 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

"ERROR: The local-authentication method is required to be certificate basedif
remote-authentication allows EAP
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置此组的隧道组 IPsec 属性。

im

要启用通过 SIP 收发即时消息，请在参数配置模式 （从策略映射配置模式可访问）下使用 **im** 命令。要禁用此功能，请使用此命令的 **no** 形式。

im

no im

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 SIP 检查策略映射中启用通过 SIP 收发即时消息：

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

相关命令

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

imap4s

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 命令模式中输入的任何命令，请使用此命令的 **no** 形式。

imap4s

no imap4s

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

IMAP4 是 Internet 服务器用以为您接收和保管电邮的客户端 / 服务器协议。您 （或您的电邮客户端）可以只查看信件的标题和发件人，然后决定是否下载该邮件。也可以在服务器上创建和操作多个文件夹、删除邮件或者搜索特定部分或整个记录。 IMAP 要求您在处理邮件时持续访问服务器。 IMAP4S 可让您通过 SSL 连接接收电邮。

示例

以下示例显示如何进入 IMAP4S 配置模式：

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

相关命令

命令	说明
clear configure imap4s	删除 IMAP4S 配置。
show running-config imap4s	显示 IMAP4S 正在运行的配置。

import webvpn customization

要将定制对象加载到 ASA 的闪存设备，请在特权 EXEC 模式下输入 **import webvpn customization** 命令。

import webvpn customization *name URL*

语法说明

name	用于标识定制对象的名称。最多 64 个字符。
URL	XML 定制对象来源的远程路径。最多 255 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

确保先在 ASA 接口上启用 WebVPN，然后输入 **import customization** 命令。为此，请输入 **show running-config** 命令。

ASA 在您导入定制对象时执行以下任务：

- 将定制对象从 URL 复制到 ASA 文件系统 disk0:/csco_config/customization as MD5*name*。
- 对该文件执行基本的 XML 语法检查。如果无效， ASA 将删除该文件。
- 检查 index.ini 中的文件包含记录 MD5*name*。如果未包含， ASA 会将 MD5*name* 添加到该文件。
- 将 MD5*name* 文件复制到 RAMFS /csco_config/customization/ with as ramfs *name*。

示例

以下示例从 URL 209.165.201.22/customization 导入到 ASA 定制对象 *General.xml*，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:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

相关命令

命令	说明
revert webvpn customization	从 ASA 的闪存设备中删除指定的定制对象。
show import webvpn customization	列出 ASA 的闪存设备上存在的定制对象。

import webvpn plug-in protocol

要将插件安装到 ASA 的闪存设备，请在特权 EXEC 模式下输入 **import webvpn plug-in protocol** 命令。

import webvpn plug-in protocol *protocol URL*

语法说明

protocol	• **rdp -** 远程桌面协议插件可让远程用户连接到运行 Microsoft 终端服务的计算机。思科会原样重分布此插件。包含原件的网站为 http://properjavardp.sourceforge.net/。 • **ssh,telnet -** 安全外壳插件可让远程用户建立到远程计算机的安全信道，或者让远程用户使用 Telnet 连接到远程计算机。思科会原样重分布此插件。包含原件的网站是 http://javassh.org/。 ⚠ **注意事项** **import webvpn plug-in protocol ssh,telnet** *URL* 命令会*同时*安装 SSH 和 Telnet 插件。请*勿*分别对 SSH 和 Telnet 各输入一次此命令。键入 **ssh,telnet** 字符串时，*不*要插入空格。使用 **revert webvpn plug-in protocol** 命令可删除不符合这些要求的所有 **import webvpn plug-in protocol** 命令。 • **vnc -** 虚拟网络计算插件可让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。思科会原样重分布此插件。包含原件的网站是 http://www.tightvnc.com/。
URL	插件来源的远程路径。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

在安装插件之前，请执行以下操作：

- 确保在 ASA 上的接口上启用无客户端 SSL VPN(“webvpn”)。为此，请输入 **show running-config** 命令。
- 在本地 TFTP 服务器 （例如具有主机名 “local_tftp_server” 的服务器）上创建名为 “plugins” 的临时目录，然后从思科网站将插件下载到 “plugins” 目录。在 **import webvpn plug-in protocol** 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路径。

ASA 在您导入插件时执行以下任务：

- 解压 *URL* 中指定的 .jar 文件。
- 将该文件写入 ASA 文件系统中的 csco-config/97/plugin 目录。
- 填写 ASDM 中 URL 属性旁边的下拉菜单。
- 为所有未来的无客户端 SSL VPN 会话启用该插件，并向门户页面的 Address （地址）字段旁边添加主菜单选项和下拉菜单选项。下表显示对门户页面的主菜单和地址字段的更改。

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

ASA 不会在配置中保留 **import webvpn plug-in protocol** 命令，而会自动加载 csco-config/97/plugin 目录的内容。辅助 ASA 从主要 ASA 获取插件。

当无客户端 SSL VPN 会话中的用户点击门户页面上相关的菜单选项时，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，并且在 Address （地址）字段中输入 URL 以建立连接。

注　除了支持之前的 SSH V1 和 Telnet 以外，还添加对 SSH V2 的支持。插件协议仍然相同 （ssh 和 telnet）， URL 格式如下：
ssh://<target> — uses SSH V2
ssh://<target>/?version=1 — uses SSH V1
telnet://<target> — uses telnet

要删除各 **import webvpn plug-in protocol** 命令并禁用协议支持，请使用 **revert webvpn plug-in protocol** 命令。

示例

以下命令添加对 RDP 的无客户端 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:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

以下命令添加对 SSH 和 Telnet 的无客户端 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:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

以下命令添加对 VNC 的无客户端 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:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

相关命令

命令	说明
revert webvpn plug-in protocol	从 ASA 的闪存设备中删除指定的插件。
show import webvpn plug-in	列出 ASA 的闪存设备上存在的插件。

import webvpn translation-table

要导入转换表 （用于转换显示给建立 SSL VPN 远程的连接用户的术语），请在特权 EXEC 模式下使用 **import webvpn translation-table** 命令。

import webvpn translation-table *translation_domain* **language** *language url*

语法说明

language	指定转换表的语言。以浏览器语言选项指示的方式输入 *language* 的值。
translation_domain	指定远程用户可见的功能区和相关消息。
url	指定用于创建定制对象的 XML 文件的 URL。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

对于向发起基于浏览器的无客户端 SSL VPN 连接的用户显示的门户网站和屏幕，以及向 AnyConnect VPN 客户端用户显示的用户界面， ASA 提供语言转换。

远程用户可见的每个功能区及其消息都有其自身的转换域，由 *translation_domain* 参数指定。下表显示转换域和转换的功能区。

转换域	转换的功能区
AnyConnect	在 Cisco AnyConnect VPN 客户端用户界面上显示的消息。
banners	VPN 访问被拒绝时显示给远程用户的横幅和消息。
CSD	适用于思科安全桌面 (CSD) 的消息。
customization	登录和注销页面、门户页面上的消息以及用户可定制的所有消息。
plugin-ica	适用于 Citrix 插件的消息。
plugin-rdp	适用于远程桌面协议插件的消息。
plugin-telnet,ssh	适用于 Telnet 和 SSH 插件的消息。
plugin-vnc	适用于 VNC 插件的消息。

转换域 （续）	转换的功能区 （续）
PortForwarder	显示给端口转发用户的消息。
url-list	用户为门户页面上的 URL 书签指定的文本。
webvpn	所有不可定制的第 7 层、 AAA 和门户消息。

转换模板是与转换表格式相同的 XML 文件，但所有转换为空。 ASA 的软件映像包包括属于标准功能的每个域的模板。插件模板随附于插件，用于定义其自己的转换域。因为您可以定制无客户端用户的登录和注销页面、门户页面以及 URL 书签，所以 ASA 会动态生成 **customization** 和 **url-list** 转换域模板，并且模板会自动反映您对这些功能区的更改。

使用 **export webvpn translation-table** 命令下载用于转换域的模板，并且使用 **import webvpn translation-table** 命令创建对象。您可以使用 **show import webvpn translation-table** 命令查看可用的对象。

请务必以浏览器语言选项指示的方式指定语言。 例如，Microsoft Internet Explorer 使用缩写 *zh* 表示简体中文。导入到 ASA 的转换表也必须命名为 *zh*。

除了 AnyConnect 转换域外，转换表没有任何影响，而且在您创建定制对象、确定要用于该对象的转换表并为用户或组策略指定定制之前，消息不会转换。对 AnyConnect 域转换表的更改会立即显示给 AnyConnect 客户端用户。有关详细信息，请参阅 **import webvpn customization** 命令。

示例

以下示例为影响 AnyConnect 客户端用户界面的转换域导入转换表，并且指定转换表用于中文。**show import webvpn translation-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
```

相关命令

命令	说明
export webvpn translation-table	导出转换表。
import webvpn customization	导入引用转换表的定制对象。
复原	从闪存中删除转换表。
show import webvpn translation-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 **import webvpn url-list** 命令。

import webvpn url-list *name URL*

语法说明

name	用于标识 URL 列表的名称。最多 64 个字符。
URL	URL 列表来源的远程路径。最多 255 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

确保在 ASA 接口上启用 WebVPN，然后输入 **import url-list** 命令。为此，请输入 **show running-config** 命令。

ASA 在您导入 URL 列表时执行以下任务：

- 将 URL 列表从 URL 复制到 ASA 文件系统 disk0:/csco_config/url-lists as *name on flash* = base 64*name*。
- 对该文件执行基本的 XML 语法检查。如果语法无效， ASA 将删除该文件。
- 检查 index.ini 中的文件是否包含记录 base 64*name*。如果未包含，ASA 会将 base 64*name* 添加到该文件。
- 将 *name* 文件复制到 RAMFS /csco_config/url-lists/ with ramfs name = *name*。

示例

以下示例将 URL 列表 *NewList.xml* 从 URL 209.165.201.22/url-lists 导入到 ASA，并且将其命名为 *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:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

相关命令

命令	说明
revert webvpn url-list	从 ASA 的闪存设备中删除指定的 URL 列表。
show import webvpn url-list	列出 ASA 的闪存设备上存在的 URL 列表。

import webvpn webcontent

要将内容导入到远程无客户端 SSL VPN 用户可见的闪存，请在特权 EXEC 模式下使用 **import webvpn webcontent** 命令。

import webvpn webcontent *destination url source url*

语法说明

destination url	要导出到的 URL。最多 255 个字符。
source url	ASA 闪存中内容所在的 URL。最多 64 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

远程无客户端用户可以看到使用 **webcontent** 选项导入的内容。这包括在无客户端门户上可见的帮助内容以及用于定制用户屏幕的定制对象使用的徽标。

使用路径 /+CSCOE+/ 导入到 URL 的内容只有授权的用户才可看到。

而使用路径 /+CSCOU+/ 导入到 URL 的内容，授权及未获授权的用户均可看到。

例如，导入为 /+CSCOU+/logo.gif 的公司徽标可能用在门户定制对象中，在登录页面和门户页面上可见。导入为 /+CSCOE+/logo.gif 的相同 logo.gif 文件仅在远程用户成功登录后才可见。

出现在各个应用屏幕上的帮助内容必须导入到特定的 URL。下表显示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
/+CSCOE+/help/*language*/app-access-hlp.inc	应用访问
/+CSCOE+/help/*language*/file-access-hlp.inc	浏览网络
/+CSCOE+/help/*language*/net_access_hlp.html	AnyConnect 客户端
/+CSCOE+/help/*language*/web-access-help.inc	Web 访问

下表显示为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
/+CSCOE+/help/*language*/ica-hlp.inc	MetaFrame 访问
/+CSCOE+/help/*language*/rdp-hlp.inc	Terminal Servers
/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	Telnet/SSH 服务器
/+CSCOE+/help/*language*/vnc-hlp.inc	VNC 连接

URL 路径中的 *language* 条目是您为帮助内容指定的语言缩写。 ASA 不会实际将文件转换为您指定的语言，但会使用语言缩写来标记该文件。

示例

以下示例将 HTML 文件 *application_access_help.html* 从 TFTP 服务器 209.165.200.225 导入到存储闪存中应用访问帮助内容的 URL。该 URL 以缩写 *en* 表示英语：

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

以下示例将 HTML 文件 *application_access_help.html* 从 TFTP 服务器 209.165.200.225 导入到存储闪存中应用访问帮助内容的 URL。该 URL 以缩写 *en* 表示英语：

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

相关命令

命令	说明
export webvpn webcontent	导出以前导入的、无客户端 SSL VPN 用户可见的内容。
revert webvpn webcontent	从闪存中删除内容。
show import webvpn webcontent	显示已导入内容的相关信息。

第 2 章

inspect ctiqbe 至 inspect xdmcp 命令

inspect ctiqbe

要启用 CTIQBE 协议检查，请在类配置模式下使用 **inspect ctiqbe** 命令。从策略映射配置模式可进入类配置模式。要禁用检查，请使用此命令的 **no** 形式。

inspect ctiqbe

no inspect ctiqbe

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了之前存在的 **fixup** 命令 （已弃用）。

使用指南

inspect ctiqbe 命令启用支持 NAT、PAT 和双向 NAT 的 CTIQBE 协议检查。这使思科 IP 软电话和其他思科 TAPI/JTAPI 应用能够成功配合 Cisco CallManager 在 ASA 范围内进行呼叫设置。

很多思科 VoIP 应用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)。思科 TAPI 服务提供商 (TSP) 使用计算机电话接口快速缓冲编码 (CTIQBE) 来与 Cisco CallManager 通信。

以下总结了使用 CTIQBE 应用检查时适用的限制：

- 不支持 CTIQBE 呼叫状态故障切换。
- 使用 **debug ctiqbe** 命令可能会延迟消息传输，这会影响实时环境中的性能。启用此调试或日志记录时，如果思科 IP 软电话似乎无法通过 ASA 完成呼叫设置，请在运行思科 IP 软电话的系统上的思科 TSP 设置中增加超时值。
- CTIQBE 应用检查*不*支持分散在多个 TCP 数据包中的 CTIQBE 消息。

以下内容说明在特定情况下使用 CTIQBE 应用检查时应特殊考虑的事项：

- 如果两部思科 IP 软电话向连接到 ASA 的不同接口的不同的 Cisco CallManager 注册，则这两部电话之间的呼叫将会失败。
- 当 Cisco CallManager 位于比思科 IP 软电话更高的安全接口上时，如果 Cisco CallManager IP 地址必须执行 NAT 或外部 NAT，则映射必须为静态，因为思科 IP 软电话需要在 PC 上的思科 TSP 配置中明确指定 Cisco CallManager IP 地址。
- 当使用 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）地址的同一端口上，以便成功注册思科 IP 软电话。CTIQBE 侦听端口 (TCP 2748) 是固定的，用户不能在 Cisco CallManager、思科 IP 软电话或思科 TSP 上进行配置。

检查信令消息

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

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时， **inspect ctiqbe** 命令不使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect ctiqbe** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

示例

以下示例启用 CTIQBE 检查引擎，这会创建一个与默认端口 (2748) 上的 CTIQBE 流量进行匹配的类映射。然后，服务策略会应用于外部接口。

```
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
```

要为所有接口启用 CTIQBE 检查，请使用 **global** 参数代替 **interface outside**。

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
show conn	显示不同连接类型的连接状态。
show ctiqbe	显示关于在 ASA 范围内建立的 CTIQBE 会话以及由 CTIQBE 检查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

要启用发往终端映射程序的 DCERPC 流量的检查，请在类配置模式下使用 **inspect dcerpc** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

语法说明

map_name	（可选） DCERPC 检查映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

inspect dcerpc 命令为 DCERPC 协议启用或禁用应用检查。

示例

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

```
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
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
policy-map type inspect	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	为 DCERPC 针孔配置超时，并覆盖全局系统针孔超时。

inspect dns

要启用 DNS 检查（如果之前已禁用）或配置 DNS 检查参数，请在类配置模式下使用 **inspect dns** 命令。从策略映射配置模式可进入类配置模式。要禁用 DNS 检查，请使用此命令的 **no** 形式。

inspect dns [*map_name*] [**dynamic-filter-snoop**]

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

语法说明

dynamic-filter-snoop	（可选）启用僵尸网络流量过滤器专用的动态过滤器监听。仅当使用僵尸网络流量过滤时包括此关键字。我们建议您仅在外部 DNS 请求即将到达的接口上启用 DNS 监听。启用针对所有 UDP DNS 流量（包括即将到达内部 DNS 服务器的流量）的 DNS 监听会在 ASA 上创建不必要的负载。
map_name	（可选）指定 DNS 映射的名称。

默认值

此命令默认已启用。默认情况下禁用僵尸网络流量过滤器监听。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令（已弃用）。
7.2(1)	将此命令修改为允许配置附加 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 检查，使用 preset_dns_map 检查类映射：

- DNS 消息的最大长度为 512 个字节。
- 客户端 DNS 消息的最大长度会自动设置为与 Resource Record（资源记录）相匹配。
- 已启用 DNS Guard（DNS 防护），因此一旦 ASA 转发 DNS 应答，ASA 便会拆解与 DNS 查询关联的 DNS 会话。 ASA 还会监控消息交换以确保 DNS 应答的 ID 与 DNS 查询的 ID 相匹配。
- 已启用基于 NAT 配置的 DNS 记录的转换。
- 已启用协议实施，这会启用 DNS 消息格式检查，包括域名长度不超过 255 个字符、标签长度不超过 63 个字符，以及压缩和环路指针等检查。

DNS 重写所需的 DNS 检查

启用 DNS 检查后， DNS 重写会为来自任何接口的 DNS 的 NAT 提供全面支持。

如果内部网络上的客户端请求对来自外部接口上的 DNS 服务器的内部地址进行 DNS 解析，则会正确转换 DNS A 记录。如果禁用 DNS 检查引擎，则不会转换 A 记录。

DNS 重写执行两项功能：

- 当 DNS 客户端在专用接口上时，将 DNS 应答中的公共地址 （可路由或 “ 映射的 ” 地址）转换为专用地址 （“ 真实 ” 地址）。
- 当 DNS 客户端在公共接口上时，将专用地址转换为公共地址。

只要 DNS 检查仍处于启用状态，您就可以为 NAT 配置 DNS 重写。

示例

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
```

以下示例将为所有 UDP DNS 流量创建一个类映射，使用默认 DNS 检查策略映射启用 DNS 检查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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
dynamic-filter enable	对某类流量或所有流量 （如果没有指定访问列表）启用僵尸网络流量过滤器。
policy-map	将类映射与特定安全操作关联。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用于一个或多个接口。

inspect esmtp

要启用 SMTP/ESMTP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect esmtp** 命令。类配置模式可从策略映射配置模式访问。要删除配置，请使用此命令的 **no** 形式。

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

语法说明

map_name	（可选） ESMTP 映射的名称。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

默认情况下，启用 ESMTP 检查，使用 _default_esmtp_map 检查策略映射。

- 已屏蔽服务器标识。
- 已检查加密的流量。
- 没有注意到发送方和接收方地址中的特殊字符，未采取任何操作。
- 已丢弃并记录了具有长度大于 512 个字符的命令行的连接。
- 已丢弃并记录了超过 100 个收件人的连接。
- 已记录正文长度超过 998 个字节的消息。
- 已丢弃并记录了标头行长度超过 998 个字符的连接。
- 已丢弃并记录了 MIME 文件名超过 255 个字符的消息。
- 已屏蔽与 “others” 相匹配的 EHLO 应答参数。

ESMTP 应用检查通过限制可通过 ASA 的 SMTP 命令的类型以及增加监控功能，来提升针对基于 SMTP 的攻击的保护。

ESMTP 是对 SMTP 协议的改进，且在很多方面与 SMTP 类似。为方便起见，本文档中使用术语 SMTP 来同时指代 SMTP 和 ESMTP。扩展的 SMTP 的应用检查进程类似于 SMTP 应用检查，并包括对 SMTP 会话的支持。扩展的 SMTP 会话中使用的大多数命令与在 SMTP 会话中使用的相同，但 ESMTP 会话快得多，并提供更多与可靠性和安全性相关的选项，例如交付状态通知。

扩展的 SMTP 应用检查增加了对这些扩展的 SMTP 命令的支持，包括 AUTH、 EHLO、 ETRN、 HELP、 SAML、 SEND、 SOML、 STARTTLS 和 VRFY。除对七个 RFC 821 命令 （DATA、 HELO、MAIL、NOOP、QUIT、RCPT、RSET）的支持外，ASA 还支持总共十五个 SMTP 命令。

不支持其他扩展的 SMTP 命令（例如 ATRN、ONEX、VERB、CHUNKING）和专用扩展。不支持的命令会转换为 X，被内部服务器拒绝。这会导致一条消息出现，例如 “500 Command unknown: 'XXX'. （500 命令未知：‘XXX’。）”。不完整的命令会被放弃。

ESMTP 检查引擎将服务器 SMTP 标识中的字符更改为除 “2”、“0”、“0” 字符外的星号。就忽略回车 (CR) 和 (LF) 换行符。

启用 SMTP 检查后，如果不遵守以下规则，则用于交互式 SMTP 的 Telnet 会话可能会挂起：SMTP 命令的长度必须大于四个字符；必须使用回车和换行符终止命令；必须在发出下一个应答前等待响应。

SMTP 服务器使用数字应答码和用户可读的可选字符串响应客户端请求。 SMTP 应用检查控制并减少用户可使用的命令以及服务器返回的消息。 SMTP 检查执行三个主要任务：

- 将 SMTP 请求限定为七个基本 SMTP 命令和八个扩展的命令。
- 监控 SMTP 命令响应序列。
- 生成审计追踪 - 当替换了邮件地址中嵌入的无效字符时，会生成审计记录 108002。有关更多信息，请参阅 RFC 821。

SMTP 检查监控以下异常签名的命令和响应序列：

- 截断的命令。
- 不正确的命令终止 （并非使用 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。将会扫描邮件地址，确定是否存在奇怪的字符。会删除管道字符 (|) （更改为一个空格），且仅当使用 “<” 和 “>” 定义邮件地址（“<” 必须在 “>” 前面）时才允许它们存在。
- 由 SMTP 服务器执行的意外过渡。
- 对于未知命令， ASA 将数据包中的所有字符更改为 X。这种情况下，服务器会向客户端生成错误代码。由于数据包中发生更改，必须重新计算或调整 TCP 校验和。
- TCP 流编辑。
- 命令管线。

示例

以下示例启用 SMTP 检查引擎，这会创建一个类映射来匹配默认端口 (25) 上的 SMTP 流量。然后，服务策略会应用于外部接口。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用于一个或多个接口。
show conn	显示不同连接类型 （包括 SMTP）的连接状态。

inspect ftp

要配置用于 FTP 检查的端口或启用增强检查，请在类配置模式下使用 **inspect ftp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

语法说明

map_name	FTP 检查映射的名称。
strict	（可选）启用 FTP 流量的增强检查并强制符合 RFC 标准。

默认值

默认情况下，启用 FTP 检查，且 ASA 侦听 FTP 的端口 21。

将 FTP 移至更高端口时，请小心使用。例如，如果您将 FTP 端口设置为 2021，则向端口 2021 发起的所有连接都会将其数据有效负载解释为 FTP 命令。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。添加了 *map_name* 选项。

使用指南

FTP 应用检查将检查 FTP 会话，并执行四个任务：

- 准备动态辅助数据连接
- 跟踪 FTP 命令响应序列
- 生成审计追踪
- 转换嵌入的 IP 地址

FTP 应用检查为 FTP 数据传输准备辅助信道。通过 PORT 或 PASV 命令来协商这些信道的端口。分配信道以响应文件上传、文件下载或目录列表事件。

注　仅将对应用于 FTP 控制连接的端口应用检查，而不对数据连接的端口应用。 ASA 状态检查引擎会根据需要动态准备数据连接。

如果使用 **no inspect ftp** 命令禁用 FTP 检查引擎，则出站用户仅可在备用模式下启动连接，且所有入站 FTP 都会被禁用。

Strict FTP

Strict FTP 通过阻止 Web 浏览器发送 FTP 请求中嵌入的命令来增加受保护网络的安全性。要启用 strict FTP，请使用包含 **strict** 选项的 **inspect ftp** 命令。

使用 strict FTP 时，可以选择性指定 FTP 检查策略映射来指定不允许通过 ASA 的 FTP 命令。

在接口上启用 **strict** 选项后， FTP 检查会强制实施以下行为：

- 必须在 ASA 允许新命令前确认 FTP 命令。
- ASA 丢弃发送嵌入命令的连接。
- 检查 227 和 PORT 命令以确保它们不出现在错误字符串中。

注意事项　使用 **strict** 选项可能导致不严格符合 FTP RFC 的 FTP 客户端出现故障。

如果启用 **strict** 选项，则会跟踪以下异常活动的每个 FTP 命令和响应序列：

- 截断的命令 - 检查 PORT 和 PASV 应答命令中的逗号数是否为五个。如果不是五个，则会假设要截断 PORT 命令并关闭 TCP 连接。
- 不正确的命令 - 检查 FTP 命令是否按照 RFC 的要求以 <CR><LF> 字符结束。如果没有，则会关闭连接。
- RETR 和 STOR 命令的大小 - 将它们与一个固定的常量进行比较。如果大小更大，则会记录一条错误消息，并关闭连接。
- 命令欺骗 - 应始终从客户端发送 PORT 命令。如果从服务器发送 PORT 命令，则会拒绝 TCP 连接。
- 应答欺骗 - 应始终从服务器发送 PASV 应答命令 (227)。如果从客户端发送 PASV 应答命令，则会拒绝 TCP 连接。这会阻止用户执行 “227 xxxxx a1, a2, a3, a4, p1, p2.” 时出现的安全漏洞。
- TCP 流编辑 - 如果 ASA 检测到 TCP 流编辑，则会关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于从 1 到 1024 的范围内的端口号已为熟知的连接保留，如果协商的端口属于此范围，则会释放 TCP 连接。
- 命令管线 - 参照常量值 8 对 PORT 和 PASV 应答命令中出现在端口号后的字符的数量进行交叉检查。如果超过 8，则会关闭 TCP 连接。
- ASA 使用一系列 X 替换 FTP 服务器对 SYST 命令的响应，来阻止服务器向 FTP 客户端揭示其系统类型。要覆盖此默认行为，请在 FTP 映射中使用 **no mask-syst-reply** 命令。

FTP 日志消息

FTP 应用检查生成以下日志消息：

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

示例

在提交用户名和密码前，为所有 FTP 用户呈现问候语横幅。默认情况下，此横幅包括有利于黑客尝试标识系统中的弱点的版本信息。以下示例显示如何屏蔽此横幅：

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
mask-syst-reply	隐藏来自客户端的 FTP 服务器响应。
policy-map	将类映射与特定安全操作关联。
policy-map type inspect	创建检查策略映射。
request-command deny	指定将不允许的 FTP 命令。
service-policy	将策略映射应用于一个或多个接口。

inspect gtp

要启用或禁用 GTP 检查或定义 GTP 映射以控制 GTP 流量或隧道，请在类配置模式下使用 **inspect gtp** 命令。从策略映射配置模式可进入类配置模式。使用此命令的 **no** 形式删除此命令。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

注　GTP 检查需要特殊许可。

语法说明

map_name	（可选） GTP 映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

GTP 是用于 GPRS 的隧道协议，有助于在无线网络上提供安全访问。 GPRS 是数据网络架构，专为与现有 GSM 网络集成而设计。它为企业网络和 Internet 提供不间断的移动用户和分组交换数据服务。有关 GTP 的概述，请参阅 CLI 配置指南。

默认情况下，不启用 GTP 检查。但是，如果您在未指定自己的检查映射时启用它，则会使用提供以下处理规则的默认映射。仅当您需要不同的值时才需要配置一个映射。

- 不允许错误。
- 最大请求数是 200。
- 最大隧道数是 500。
- GSN 超时是 30 分钟。
- PDP 情景超时是 30 分钟。
- 请求超时是 1 分钟。
- 信令超时是 30 分钟。
- 隧道超时是 1 小时。

- T3 响应超时是 20 秒。
- 已丢弃并记录未知消息 ID。

使用 **policy-map type inspect gtp** 命令为 GTP 定义参数。定义 GTP 映射后，您可以使用 **inspect gtp** 命令启用映射。然后，您可以使用 **class-map**、 **policy-map** 和 **service-policy** 命令定义一个流量类，将 **inspect** 命令应用于该类，并将策略应用于一个或多个接口。

GTP 的熟知端口是 UDP 3386 和 2123。

检查信令消息

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

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时， **inspect gtp** 命令不使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect gtp** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

示例

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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
clear service-policy inspect gtp	清除全局 GTP 统计信息。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用于一个或多个接口。
show service-policy inspect gtp	显示 **inspect gtp** 策略的状态和统计数据。

inspect h323

要启用 H.323 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect h323** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect h323 {**h225** | **ras**} [*map_name*]

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

语法说明

h225	启用 H.225 信令检查。
map_name	（可选） H.323 映射的名称。
ras	启用 RAS 检查。

默认值

默认端口分配如下：

- h323 h225 1720
- h323 ras 1718-1719

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

inspect h323 命令提供对符合 H.323 的应用 （例如 Cisco CallManager 和 VocalTec Gatekeeper）的支持。H.323 是由国际电信联盟 (ITU) 制定的一套协议，用于通过 LAN 开展多媒体会议。ASA 支持从 H.323 到版本 6 的应用，包括具有在一个呼叫信令信道上进行多次呼叫功能的 H.323 v3。

启用 H.323 检查后，ASA 支持在同一个呼叫信令信道上进行多次呼叫，这是一项随着 H.323 v3 引入的功能。此功能可减少呼叫设置时间和在 ASA 上使用的端口。

H.323 检查的两项主要功能如下：

- 对 H.225 和 H.245 消息中必要的嵌入 IPv4 地址执行 NAT。由于以 PER 编码格式对 H.323 消息进行编码， ASA 会使用 ASN.1 解码器来对 H.323 消息进行解码。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。

检查信令消息

对于检查信令消息， **inspect h323** 命令通常需要确定媒体终端 （例如 IP 电话）的位置。

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时，**inspect h323** 命令不使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect h323** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

示例

以下示例启用 H.323 检查引擎，这会创建一个类映射来与默认端口 (1720) 上的 H.323 流量进行匹配。然后，服务策略会应用于外部接口。

```
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
```

相关命令

命令	说明
policy-map type inspect	创建检查策略映射。
show h225	显示关于在 ASA 范围内建立的 H.225 会话的信息。
show h245	显示关于终端使用缓慢启动在 ASA 范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在 ASA 范围内建立的 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 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect http 命令**。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect http [*map_name*]

no inspect http [*map_name*]

语法说明

map_name	（可选） HTTP 检查映射的名称。

默认值

HTTP 的默认端口为 80。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

提示 您可以安装执行应用和 URL 过滤的服务模块，其中包括 HTTP 检查，例如 ASA CX 或 ASA FirePOWER。在 ASA 上运行的 HTTP 检查与这些模块不兼容。请注意，与尝试使用 HTTP 检查策略映射在 ASA 上手动配置应用过滤相比，使用针对特定用途的模块进行配置要轻松得多。

使用 HTTP 检查引擎针对特定攻击和其他与 HTTP 流量关联的威胁进行保护。

HTTP 应用检查扫描 HTTP 标头和正文，并对数据执行各种检查。这些检查可阻止各种 HTTP 结构、内容类型以及隧道和消息传送协议穿越安全设备。

增强的 HTTP 检查功能 （又称为应用防火墙，在配置 HTTP 检查策略映射时可用）可以帮助阻止攻击者使用 HTTP 消息来规避网络安全策略。

HTTP 应用检查可以拦截隧道应用以及 HTTP 请求和响应中的非 ASCII 字符，阻止恶意内容到达 Web 服务器。它还支持对 HTTP 请求和响应标头中的各种元素的大小限制、URL 拦截和 HTTP 服务器标头类型欺骗。

增强的 HTTP 检查为所有 HTTP 消息验证以下内容：

- 符合 RFC 2616
- 仅使用 RFC 定义的方法。
- 符合附加标准。

示例

在此示例中，对通过任何接口进入 ASA 的任何 HTTP 连接（端口 80 上的 TCP 流量）进行分类来执行 HTTP 检查。该策略是全局策略，因此检查仅在流量进入每个接口时发生。

```
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
```

相关命令

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

inspect icmp

要配置 ICMP 检查引擎，请在类配置模式下使用 **inspect icmp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect icmp

no inspect icmp

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

ICMP 检查引擎允许如 TCP 和 UDP 流量一样检查 ICMP 流量。没有 ICMP 检查引擎时，我们建议您不要允许 ICMP 通过 ACL 中的 ASA。没有状态检查时，ICMP 可用于攻击您的网络。ICMP 检查引擎可确保每个请求仅有一个响应，且序列号是正确的。

禁用 ICMP 检查 （这是默认配置）时，会拒绝从较低的安全接口到较高的安全接口的 ICMP 回显应答消息，即使是对 ICMP 回显请求的响应。

示例

您可以启用以下示例中所示的 ICMP 应用检查引擎，这会创建一个类映射来与使用 ICMP 协议 ID 的 ICMP 流量进行匹配，即 1 与 IPv4 匹配， 58 与 IPv6 匹配。然后，服务策略会应用于外部接口。要为所有接口启用 ICMP 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
icmp	为在 ASA 接口上终止的 ICMP 流量配置访问规则。
policy-map	定义一项策略，将安全操作与一个或多个流量类相关联。
service-policy	将策略映射应用于一个或多个接口。

inspect icmp error

要为 ICMP 错误消息启用应用检查，请在类配置模式下使用 **inspect icmp error** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect icmp error

no inspect icmp error

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

启用 ICMP 错误检查后， ASA 会根据 NAT 配置来为发送 ICMP 错误消息的中间跃点创建转换会话。 ASA 使用转换的 IP 地址覆盖数据包。

禁用 ICMP 错误检查后，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机和 ASA 之间的中间节点生成的 ICMP 错误消息会到达外部主机，不占用任何附加 NAT 资源。当外部主机使用跟踪路由命令跟踪跃点到 ASA 内部的目标时，这是不可取的。当 ASA 不转换中间跃点时，所有中间跃点都会与映射的目标 IP 地址一同出现。

扫描 ICMP 负载从原始数据包中检索五元组。使用检索的五元组执行查找以确定客户端的原始地址。 ICMP 错误检查引擎对 ICMP 数据包进行以下更改：

- 在 IP 标头中，映射的 IP 会更改为真实 IP （目标地址），并会修改 IP 校验和。
- 在 ICMP 标头中，会因 ICMP 数据包中的更改而修改 ICMP 校验和。
- 在负载中，进行了以下更改：
  - 原始数据包映射的 IP 已更改为真实 IP
  - 原始数据包映射的端口已更改为真实端口
  - 已重新计算原始数据包 IP 校验和

示例

以下示例启用 ICMP 错误应用检查引擎，这会创建一个类映射与使用 ICMP 协议 ID 的 ICMP 流量进行匹配，即 1 与 IPv4 匹配， 58 与 IPv6 匹配。然后，服务策略会应用于外部接口。要为所有接口启用 ICMP 错误检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
icmp	为在 ASA 接口上终止的 ICMP 流量配置访问规则。
inspect icmp	启用或禁用 ICMP 检查引擎。
policy-map	定义一项策略，将安全操作与一个或多个流量类相关联。
service-policy	将策略映射应用于一个或多个接口。

inspect ils

要启用 ILS 应用检查，请在类配置模式下使用 **inspect ils 命令**。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect ils

no inspect ils

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

inspect ils 命令提供对 Microsoft NetMeeting、SiteServer 和 Active Directory 产品（使用 LDAP 与 ILS 服务器交换目录信息）的 NAT 支持。

ASA 支持 ILS 的 NAT，用于在 ILS 或 SiteServer Directory 中注册和查找终端。不支持 PAT，因为 LDAP 数据库仅存储 IP 地址。

对于搜索响应，当 LDAP 服务器位于外部时，应将 NAT 视为允许内部对等设备在向外部 LDAP 服务器注册时进行本地通信。对于此类搜索响应，首先搜索 xlates，然后搜索 DNAT 条目以获取正确的地址。如果这两个搜索都失败，则不会更改地址。对于使用 NAT 0 （无 NAT）且不期望 DNAT 互动的站点，我们建议关闭检查引擎以提供更好的性能。

当 ILS 服务器位于 ASA 边界内时，附加配置可能是必要的。这就需要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 信道上， TCP 连接会在 TCP 非活动时间间隔后断开。默认情况下，此时间间隔为 60 分钟，可以使用 **timeout** 命令对其进行调整。

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，可能会创建几个会话。

在连接协商期间， BIND PDU 会从客户端发送到服务器。一旦收到来自服务器的成功 BIND RESPONSE，就可能会交换其他操作消息（例如 ADD、DEL、SEARCH 或 MODIFY）以在 ILS Directory 上执行操作。 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 检查执行以下操作：

- 使用 BER 解码功能对 LDAP REQUEST/RESPONSE PDU 进行解码。
- 解析 LDAP 数据包。
- 提取 IP 地址。
- 必要时转换 IP 地址。
- 使用 BER 编码功能对带有转换的地址的 PDU 进行编码。
- 将新编码的 PDU 复制回 TCP 数据包中。
- 执行增量 TCP 校验和和序列号调整。

ILS 检查具有以下限制：

- 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个体用户。

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

示例

您可以启用以下示例中所示的 ILS 检查引擎，这会创建一个类映射来与默认端口 (389) 上的 ILS 流量进行匹配。然后，服务策略会应用于外部接口。要为所有接口启用 ILS 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
policy-map type inspect	创建检查策略映射。
service-policy	将策略映射应用于一个或多个接口。

inspect im

要启用 Instant Messenger （即时消息）流量的检查，请在类配置模式下使用 **inspect im** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect im *map_name*

no inspect im *map_name*

语法说明

map_name	IM 映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

inspect im 命令启用或禁用用于 IM 协议的应用检查。即时消息 (IM) 检查引擎可让您控制 IM 的网络使用情况，停止机密数据泄露、蠕虫传播和对企业网络的其他威胁。

示例

以下示例显示如何定义 IM 检查策略映射：

```
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
```

相关命令

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	与检查类或策略映射中的特定 IM 协议进行匹配。

inspect ip-options

要启用数据包中的 IP 选项的检查，请在类或策略映射类型检查配置模式下使用 **inspect ip-options** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect ip-options [*map_name*]

no inspect ip-options *map_name*

语法说明

map_name	（可选） IP 选项映射的名称。

默认值

默认情况下，在全局策略中启用此命令。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
策略或类映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

在数据包中， IP 标头包含 Options （选项）字段。 Options （选项）字段 （通常称为 IP Options （IP 选项））提供某些情况下需要但并非最常用的通信所必需的控制功能。特别是， IP Options （IP 选项）包括对时间戳、安全性和特殊路由的调配。使用 IP Options （IP 选项）是可选的，此字段可包含 0 个、 1 个或多个选项。

您可以配置 IP 选项检查以控制允许哪些具有特定 IP 选项的 IP 数据包通过 ASA。配置此检查将指示 ASA 允许数据包通过，或清除指定的 IP 选项后允许该数据包通过。

IP Options （IP 选项）检查可以检查数据包中的以下三个 IP 选项：

- End of Options List （选项列表末端） (EOOL) 或 IP Option 0 （IP 选项 0） - 此选项 （仅包含一个零字节）出现在所有选项的末端来标记选项列表结束。根据标头长度，这可能与标头的末端不一致。
- No Operation （无操作） (NOP) 或 IP Option 1 （IP 选项 1） - IP 标头中的 Options （选项）字段可包含 0 个、 1 个或多个选项，这使得字段的总长度可变。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，则将 NOP 选项用作 “ 内边距 ” 以使 32 位边界上的选项对齐。
- Router Alert （路由器告警） (RTRALT) 或 IP Option 20 （IP 选项 20） - 此选项会通知中转路由器检查数据包的内容，即使数据包不发往该路由器。此检查在实施 RSVP 时十分有用，类似的协议需要沿着数据包交付路径从路由器中进行相对较复杂的处理。

您可以通过在策略映射类型检查配置模式下使用 **parameter** 命令来配置这三个 IP 选项的检查。有关这些命令的语法的详细信息，请参阅 **eool**、 **nop** 和 **router-alert** 命令页面。

注　默认情况下，在全局检查策略中包括 IP Options （IP 选项）检查。因此，当 ASA 处于路由模式中时， ASA 允许包含带有 Router Alert （路由器告警）选项 （选项 20）的数据包的 RSVP 流量通过。

丢弃包含 Router Alert （路由器告警）选项的 RSVP 数据包会导致 VoIP 实施中出现问题。

配置 ASA 以从 IP 标头中清除 Router Alert（路由器告警）选项时，IP 标头会通过以下方式更改：

- 填充 Options （选项）字段，以使该字段在 32 位边界上结束。
- Internet 标头长度 (IHL) 更改。
- 数据包的总长度更改。
- 重新计算校验和。

如果 IP 标头包含除 EOOL、NOP 或 RTRALT 外的附加选项，则无论是否将 ASA 配置为允许这些选项， ASA 都会丢弃该数据包。

示例

以下示例显示如何定义 IP Options（IP 选项）检查策略映射，允许 ASA 传递在数据包标头中包含 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
```

在允许数据包通过 ASA 前输入 **clear** 命令可从该数据包中清除 IP 选项。

相关命令

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 传递检查，请在类映射配置模式下使用 **inspect ipsec-pass-thru** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect ipsec-pass-thru [*map_name*]

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

语法说明

map_name	（可选） IPsec 传递映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

inspect ipsec-pass-thru 命令启用或禁用应用检查。 IPsec 传递应用检查提供 ESP（IP 协议 50）和 / 或与 IKE UDP 端口 500 连接相关联的 AH（IP 协议 51）流量的穿越便利。它可以避免冗长的访问列表配置以允许 ESP 和 AH 流量，还可使用超时和最大连接数提供安全性。

使用 IPsec 传递参数映射标识用于定义检查参数的特定映射。使用 **policy-map type inspect** 命令访问参数配置，这使您可以为 ESP 或 AH 流量指定限制。您可以在参数配置模式下设置每个客户端的最大连接数和空闲超时。

使用 **class-map**、**policy-map** 和 **service-policy** 命令定义一个流量类，将 **inspect** 命令应用于该类，并将策略应用于一个或多个接口。与 **inspect ipsec-pass-thru** 命令结合使用时，会启用定义的参数映射。

允许 NAT 和非 NAT 流量。但不支持 PAT。

注　在 ASA 7.0(1) 中，**inspect ipsec-pass-thru** 命令仅允许 ESP 流量传递。要在更高版本中保留相同的行为，如果未对 **inspect ipsec-pass-thru** 命令指定任何参数，则会创建并附加允许 ESP 的默认映射。在 **show running-config all** 命令的输出中可以查看此映射。

示例

以下示例显示如何使用访问列表标识 IKE 流量、定义 IPsec 传递参数映射、定义策略、以及将策略应用到外部接口上：

```
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
```

相关命令

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

inspect ipv6

要启用 IPv6 检查，请在类配置模式下使用 **inspect ipv6** 命令。从策略映射配置模式可访问类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect ipv6 [*map_name*]

no inspect ipv6 [*map_name*]

语法说明

map_name	（可选） IPv6 检查策略映射的名称。

默认值

默认情况下禁用 IPv6 检查。

如果启用 IPv6 检查且不指定检查策略映射，则会使用默认 IPv6 检查策略映射，并执行以下操作：

- 仅允许已知的 IPv6 扩展标头。丢弃并记录不一致的数据包。
- 实施 RFC 2460 规范中定义的 IPv6 扩展标头的顺序。丢弃并记录不一致的数据包。
- 丢弃任何带有路由类型标头的数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

IPv6 检查使您可以根据扩展标头选择性记录或丢弃 IPv6 流量。此外，IPv6 检查还可以检查 IPv6 数据包中的扩展标头的类型和顺序是否符合 RFC 2460。

示例

以下示例丢弃带有 “ 逐跳 ”、“ 目标选项 ”、“ 路由地址 ” 和 “ 路由类型 0” 标头的所有 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
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
match header	与 IPv6 检查策略映射中的 IPv6 标头进行匹配。
policy-map type inspect ipv6	为 IPv6 创建检查策略映射。
policy-map	创建第 3/4 层策略映射。
verify-header	配置 IPv6 检查参数。

inspect mgcp

要启用 MGCP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect mgcp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

语法说明

map_name	（可选） MGCP 映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

要使用 MGCP，通常至少需要配置两个 **inspect** 命令：一个用于网关接收命令的端口，一个用于 Call Agent （呼叫座席）接收命令的端口。通常，呼叫座席将命令发送到网关的默认 MGCP 端口 2427，网关将命令发送到呼叫座席的默认 MGCP 端口 2727。

MGCP 用于控制从称为媒体网关控制器或呼叫座席的外部呼叫元素控制媒体网关。媒体网关通常是网络元素，可提供电话电路上传输的音频信号和通过 Internet 或其他数据包网络传输的数据包之间的转换。与 MGCP 结合使用 NAT 和 PAT 使您能够在具有有限外部 （全局）地址集的内部网络上支持大量设备。

媒体网关示例为：

- 中继网关，电话网络和 IP 语音 (VoIP) 网络之间的接口。此类网关通常管理大量数字电路。
- 住宅网关，向 IP 语音 (VoIP) 网络提供传统模拟 (RJ11) 接口。住宅网关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。
- 企业网关，向 IP 语音 (VoIP) 网络提供传统数字 PBX 接口或集成软 PBX 接口。

通过 UDP 传输 MGCP 消息。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。在故障切换配置中正在使用多个呼叫座席以及接收命令的呼叫座席将控制权传递给备用呼叫座席 （随后发送响应）时会发生这种情况。

注　MGCP 呼叫座席发送 AUEP 消息来确定是否存在 MGCP 终端。这会建立一个通过 ASA 的流，并允许 MGCP 终端向呼叫座席注册。

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座席和网关的 IP 地址。在 MGCP 映射配置模式下使用 **command-queue** 命令指定命令队列中一次允许的最大 MGCP 命令数。

检查信令消息

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

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时，**inspect mgcp** 命令不使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect mgcp** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

可排队的最大 MGCP 命令数是 150。

示例

以下示例显示如何标识 MGCP 流量、定义 MGCP 检查映射、定义策略、以及将策略应用到外部接口上。这会创建一个类映射以与默认端口 （2427 和 2727）上的 MGCP 流量进行匹配。然后，服务策略会应用于外部接口。此配置允许呼叫座席 10.10.11.5 和 10.10.11.6 控制网关 10.10.10.115，并允许呼叫座席 10.10.11.7 和 10.10.11.8 控制 10.10.10.116 和 10.10.10.117 两个网关。要为所有接口启用 MGCP 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

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

inspect mmp

要配置 MMP 检查引擎，请在类配置模式下使用 **inspect mmp** 命令。要删除 MMP 检查，请使用此命令的 **no** 形式。

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

语法说明

name	指定 TLS 代理实例名称。
tls-proxy	为 MMP 检查启用 TLS 代理。 MMP 协议还可使用 TCP 传输；但是，CUMA 客户端仅支持 TLS 传输。因此，启用 MMP 检查需要 **tls-proxy** 关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

ASA 包括用于验证 CUMA 移动多路复用协议 (MMP) 的检查引擎。MMP 是用于在 CUMA 客户端和服务器之间传输数据实体的数据传输协议。 CUMA 客户端和服务器之间部署 ASA 且需要检查 MMP 数据包时，请使用 **inspect mmp** 命令。

必须使用 TLS 代理启用 MMP 检查，因为 MMP 流量仅通过 TLS 连接传输。

注　配置 MMP 检查引擎时，请注意仅可以在非默认检查类下添加该引擎。

示例

以下示例显示使用 **inspect mmp** 命令检查 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
```

相关命令

命令	说明
tls-proxy	配置 TLS 代理实例。

inspect netbios

要启用 NetBIOS 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect netbios 命令**。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

语法说明

map_name	（可选） NetBIOS 映射的名称。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

inspect netbios 命令为 NetBIOS 协议启用或禁用应用检查。默认情况下启用 NetBIOS 检查。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。您可以选择性地创建策略映射来丢弃或记录违反 NetBIOS 协议的行为。

示例

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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
policy-map type inspect netbios	为 NetBIOS 创建检查策略映射。
service-policy	将策略映射应用于一个或多个接口。

inspect pptp

要启用 PPTP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect pptp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect pptp

no inspect pptp

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

点对点隧道协议 (PPTP) 是一个用于隧道 PPP 流量的协议。 PPTP 会话由一个 TCP 信道和两个 PPTP GRE 隧道（通常）组成。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道传输两台主机之间的 PPP 会话。

启用后，PPTP 应用检查检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所必需的 GRE 连接和内部转换。仅支持 RFC 2637 中定义的版本 1。

仅当通过 PPTP TCP 控制信道协商时对 GRE [RFC 2637] 的修改版本执行 PAT。*不*对 GRE [RFC 1701, RFC 1702] 的未修改版本执行端口地址转换 (PAT)。

具体而言， ASA 检查 PPTP 版本公告和传出呼叫请求 / 响应序列。仅检查 RFC 2637 中定义的 PPTP 版本 1。如果任何一方宣布的版本不是版本 1，则会禁用对 TCP 控制信道的进一步检查。此外，还会跟踪传出呼叫请求和应答序列。将连接和内部转换动态分配为允许后续辅助 GRE 数据流量所必需的。

必须为要由 PAT 转换的 PPTP 流量启用 PPTP 检查引擎。此外，仅当通过 PPTP TCP 控制信道协商时才对 GRE (RFC2637) 的修改版本执行 PAT。不对 GRE （RFC 1701 和 RFC 1702）的未修改版本执行 PAT。

正如 RFC 2637 中所述， PPTP 协议主要用于从调制解调器库 PAC （PPTP 访问集中器）发起的 PPP 会话到数据头端 PNS （PPTP 网络服务器）的隧道。当按照这种方式使用时， PAC 是远程客户端， PNS 是服务器。

但是，当由 Windows 用于 VPN 时，互动是反向的。 PNS 是远程单用户 PC，可启动到数据头端 PAC 的连接以获得对中央网络的访问。

要为所有接口启用 PPTP 检查，请使用 **global** 参数代替 **interface outside**。

示例

您可以启用以下示例中所示的 PPTP 检查引擎，这会创建一个类映射来与默认端口 (1723) 上的 PPTP 流量进行匹配。然后，服务策略会应用于外部接口。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect radius-accouting

要启用或禁用 RADIUS 记账检查或定义映射以控制流量或隧道，请在类配置模式下使用 **inspect radius-accounting** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect radius-accounting *map_name*

no inspect radius-accounting [*map_name*]

语法说明

map_name	RADIUS 记账映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

RADIUS 记账检查的目的是阻止对使用 RADIUS 服务器的 GPRS 网络的过度计费攻击。尽管您不需要 GTP/GPRS 许可来实施 RADIUS 记账检查，但它没有用处，除非您正在实施 GTP 检查，且您具有 GPRS 设置。

使用 **policy-map type inspect radius-accounting** 命令创建用于为 RADIUS 记账定义参数的检查映射。输入参数命令后，您可以使用 **send response**、 **host**、 **validate-attribute**、 **enable gprs** 和 **timeout users** 命令定义检查特征和行为。

然后，您可以使用 **class-map type management**、 **policy-map** 和 **service-policy** 命令定义一个流量类，将 **inspect radius-accounting** 命令应用于该类，并将策略应用于一个或多个接口。

注　**inspect radius-accounting** 命令仅可与 **class-map type management** 命令结合使用。

示例

以下示例显示如何配置 RADIUS 记账检查映射并启用全局检查。

```
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
```

相关命令

命令	说明
parameters	定义要应用安全操作的流量类。
class-map type management	使您可以标识流向要向其应用操作的 ASA 的第 3 层或第 4 层管理流量。
policy-map type inspect radius-accounting	为 RADIUS 记账创建检查策略映射。
show and **clear service-policy**	使您可以查看和清除服务策略设置。
service-policy	将策略映射应用于一个或多个接口。

inspect rsh

要启用 RSH 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect rsh** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect rsh

no inspect rsh

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

RSH 协议使用从 RSH 客户端到 TCP 端口 514 上的 RSH 服务器的 TCP 连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要， RSH 检查支持对协商的端口号执行 NAT。

示例

以下示例启用 RSH 检查引擎，该引擎在默认端口 (514) 上创建一个与 RSH 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 RSH 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect rtsp

要启用 RTSP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect rtsp** 命令。从策略映射配置模式可访问类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

语法说明

map_name	（可选） RTSP 映射的名称。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

inspect rtsp 命令使 ASA 可以传递 RTSP 数据包。 RealAudio、 RealNetworks、 Apple QuickTime 4、 RealPlayer 和思科 IP/TV 连接使用 RTSP。

注　对于思科 IP/TV，请使用 RTSP TCP 端口 554 和 TCP 8554。

RTSP 应用使用熟知端口 554，其中 TCP （很少用 UDP）作为控制信道。 ASA 仅支持符合 RFC 2326 的 TCP 。根据客户端上配置的传输模式，使用此 TCP 控制信道协商将用于传输音频 / 视频流量的数据信道。

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

ASA 使用状态代码 200 解析设置响应消息。如果响应消息为入站消息，则服务器位于 ASA 的外部，且需要为来自服务器的入站连接打开动态信道。如果响应消息为出站消息，则 ASA 无需打开动态信道。

由于 RFC 2326 不需要客户端和服务器端口必须在设置响应消息中，因此 ASA 需要保持状态并记住设置消息中的客户端端口。 QuickTime 将客户端端口置于设置消息中，则服务器仅使用服务器端口进行响应。

使用 RealPlayer

使用 RealPlayer 时，正确配置传输模式十分重要。对于 ASA，将一条来自服务器的 **access-list** 命令语句添加到客户端，反之亦然。对于 RealPlayer，通过选择 **Options （选项） > Preferences （首选项） > Transport （传输） > RTSP Settings （设置）**来更改传输模式。

如果在 RealPlayer 上使用 TCP 模式，请选中 **Use TCP to Connect to Server（使用 TCP 与服务器连接）**和 **Attempt to use TCP for all content （尝试将 TCP 用于所有内容）**复选框。在 ASA 上，无需配置检查引擎。

如果在 RealPlayer 上使用 UDP 模式，请选中 **Use TCP to Connect to Server（使用 UDP 连接到服务器）**和 **Attempt to use UDP for static content （尝试将 UDP 用于静态内容）**复选框，且实时内容通过组播不可用。在 ASA 上，添加一条 **inspect rtsp** *port* 命令语句。

限定与限制

以下限定适用于 RSTP 检查。

- ASA 不支持通过 UDP 的组播 RTSP 或 RTSP 消息。
- ASA 不能标识 HTTP 掩蔽，即在 HTTP 消息中隐藏 RTSP 消息的位置。
- ASA 无法对 RTSP 消息执行 NAT，因为嵌入 IP 地址会作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。数据包可能会被拆分且 ASA 无法对分散的数据包执行 NAT。
- 使用思科 IP/TV，ASA 对消息的 SDP 部分执行的转换的数量与内容管理器中的程序列表（每个程序列表可以有至少六个嵌入 IP 地址）的数量成比例。
- 您可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器在外部网络上，且服务器在内部网络上，则思科 IP/TV 仅会与 NAT 结合使用。

示例

以下示例启用 RTSP 检查引擎，这会创建一个类映射来与默认端口 （554 和 8554）上的 RTSP 流量进行匹配。然后，服务策略会应用于外部接口。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect scansafe

要对类中的流量启用 Cloud Web Security （云网络安全）检查，请在类配置模式下使用 **inspect scansafe** 命令。您可以通过首先输入 **policy-map** 命令来访问类配置模式。要删除检查操作，请使用此命令的 **no** 形式。

inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

no inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

语法说明

scansafe_policy_name	指定 **policy-map type inspect scansafe** 命令定义的检查类映射名称。
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。

命令默认

fail-close 是默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

思科 云网络安全 通过软件即服务 (SaaS) 模式提供网络安全和网络过滤服务。其网络中具有 ASA 的企业可以使用 云网络安全 服务，而无需安装附加硬件。

注　此功能又称为 “ScanSafe”，因此 ScanSafe 名称会出现在某些命令中。

使用 Modular Policy Framework （模块化策略框架）配置此命令：

1. 使用 **policy-map type inspect scansafe** 命令创建检查策略映射，至少一个用于 HTTP，一个用于 HTTPS （假设您想要检查这两种类型的流量）。
2. （可选）使用 **class-map type inspect scansafe** 命令配置白名单。
3. 定义您想要使用 **class-map** 命令检查的流量。您必须为 HTTP 和 HTTPS 流量配置单独的类映射。
4. 输入 **policy-map** 命令定义策略。
5. 对于 HTTP，输入 **class** 命令引用 HTTP 类映射。
6. 输入 **inspect scansafe** 命令，引用 HTTP 检查策略映射。

7. 对于 HTTPS，输入 **class** 命令引用 HTTPS 类映射。
8. 输入 **inspect scansafe** 命令，引用 HTTPS 检查策略映射。
9. 最后，使用 **service-policy** 命令将策略映射应用到接口上。

示例

以下示例配置两个类：一个用于 HTTP，一个用于 HTTPS。每个 ACL 免除 HTTP 和 HTTPS 到达 www.cisco.com 和 tools.cisco.com 以及 DMZ 网络流量。将所有其他流量发送到云网络安全，但来自白名单上的几个用户和组的流量除外。然后，将策略应用到内部接口上。

```
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_HTTP 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)# 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
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

inspect sip

要启用 SIP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect sip** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

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

语法说明

phone-proxy *proxy_name*	为指定的检查会话启用电话代理。
sip_map	指定 SIP 策略映射名称。
tls-proxy *proxy_name*	为指定的检查会话启用 TLS 代理。关键字 **tls-proxy** 不能用作第 7 层策略映射名称。
uc-ime *proxy_name*	为 SIP 检查启用思科公司间媒体引擎代理。

默认值

默认情况下，使用默认检查映射启用 SIP 检查，其中包括以下内容：

- SIP 即时消息 (IM) 扩展：启用。
- SIP 端口上的非 SIP 流量：允许。
- 隐藏服务器和终端的 IP 地址：禁用。
- 屏蔽软件版本和非 SIP URI：禁用。
- 确保到达目标的跃点的数量大于 0：启用。
- 符合 RTP：未实施。
- 符合 SIP：不执行状态检查和标头验证。

另请注意未启用加密流量的检查。您必须配置一个 TLS 代理来检查加密的流量。

SIP 的默认端口分配为 5060。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	添加了 **tls-proxy** 关键字。
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

SIP 是一种用于 Internet 会议、电话、状态、事件通知和即时消息的广泛使用的协议。由于 SIP 网络基于文本性质和其灵活性，可能面临着大量安全威胁。

SIP 应用检查提供消息标头和正文中的地址转换、动态打开端口和基本健全性检查功能。它还支持应用安全和协议一致性，这会加强 SIP 消息的健全性，还会检测基于 SIP 的攻击。

默认情况下启用 SIP 检查。仅当您希望执行非默认处理或想要标识 TLS 代理以启用加密流量检查时才需要配置它。

要支持通过 ASA 的 SIP 呼叫，必须检查用于媒体连接地址的信令消息、媒体端口和用于媒体的初期连接，因为当通过熟知目标端口 (UDP/TCP 5060) 发送信令时，会动态分配媒体流。此外， SIP 还会将 IP 地址嵌入在 IP 数据包的用户数据部分中。 SIP 检查对这些嵌入的 IP 地址应用 NAT。

SIP 检查的限制

SIP 检查对嵌入的 IP 地址应用 NAT。但是，如果您配置 NAT 来同时转换源地址和目标地址，则不会重写外部地址 （用于 “trying （正在尝试的）” 响应消息的 SIP 标头中的 “from （发件人）”）。因此，当结合 SIP 流量使用时，您应使用对象 NAT，这样可以避免转换目标地址。

当与 SIP 结合使用 PAT 时，以下限制和限定适用：

- 如果远程终端尝试在一个受 ASA 保护的网络上向 SIP 代理进行注册，则在非常特定的条件下注册会失败，如下所示：
  - 为远程终端配置 PAT。
  - SIP 注册服务器位于外部网络上。
  - 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。这是因为 SIP 协议中存在限制，它不在 o= 字段中提供端口值。
- 使用 PAT 时，可能不会转换包含不带有端口的内部 IP 地址的任何 SIP 标头字段，因此会在外部泄露内部 IP 地址。如果您想要避免此泄露，请配置 NAT 而非 PAT。

检查信令消息

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

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时， **inspect sip** 命令不使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect sip** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

示例

以下示例启用 SIP 检查引擎，该引擎创建一个与默认端口 (5060) 上的 SIP 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 SIP 检查，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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map type inspect sip	为 SIP 创建一个检查策略。
show sip	显示关于通过 ASA 建立的 SIP 会话的信息。
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，然后设置最大会话数。

inspect skinny

要启用 SCCP (Skinny) 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect skinny** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

语法说明

phone-proxy *proxy_name*	为指定的检查会话启用电话代理。
skinny_map	指定 Skinny 策略映射名称。
tls-proxy *proxy_name*	为指定的检查会话启用 TLS 代理。关键字 **tls-proxy** 不能用作第 7 层策略映射名称。

默认值

默认情况下，使用这些默认值启用 SCCP 检查：

- 注册：未实施。
- 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。
- 符合 RTP：未实施。

另请注意未启用加密流量的检查。您必须配置一个 TLS 代理来检查加密的流量。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	添加了 **tls-proxy** 关键字。
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

Skinny (SCCP) 是一种 VoIP 网络中使用的简化协议。使用 SCCP 的思科 IP 电话可在 H.323 环境中共存。当与 Cisco CallManager 结合使用时， SCCP 客户端可以与符合 H.323 的终端互操作。

ASA 支持对 SCCP 执行 PAT 和 NAT。如果您的 IP 电话的数量比 IP 电话使用的全局 IP 地址多，则执行 PAT 是必要的。通过支持 SCCP 信令数据包的 NAT 和 PAT， Skinny 应用检查可确保所有 SCCP 信令和媒体数据包穿越 ASA。

Cisco CallManager 和思科 IP 电话之间的正常流量使用 SCCP，且无需任何特殊配置即可由 SCCP 检查处理。ASA 还支持 DHCP 选项 150 和 66，这通过将 TFTP 服务器的位置发送到思科 IP 电话和其他 DHCP 客户端来实现。思科 IP 电话还可能在其请求中包括 DHCP 选项 3，以设置默认路由。

注　ASA 支持对来自运行 SCCP 协议版本 22 及更早版本的思科 IP 电话的流量进行检查。

支持思科 IP 电话

在拓扑结构中，即当 Cisco CallManager 位于与思科 IP 电话有关的较高安全接口上时，如果 Cisco CallManager IP 地址必须执行 NAT 或外部 NAT，则映射必须为**静态**，因为思科 IP 电话需要在其配置中明确指定 Cisco CallManager IP 地址。静态身份条目允许位于较高安全接口上的 Cisco CallManager 接受来自思科 IP 电话的注册。

思科 IP 电话需要访问 TFTP 服务器以下载它们与 Cisco CallManager 服务器连接所需的配置信息。

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。您需要一个用于 TFTP 服务器的静态条目，而它无需一定是身份静态条目。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。

当思科 IP 电话位于比 TFTP 服务器和 Cisco CallManager *高*的安全接口上时，无需使用 ACL 或静态条目来允许思科 IP 电话发起连接。

限定与限制

如果为 NAT 或 PAT 将内部 Cisco CallManager 的地址配置为不同的 IP 地址或端口，则对外部思科 IP 电话的注册会失败，因为 ASA 当前不支持对通过 TFTP 传输的文件内容的 NAT 或 PAT。尽管 ASA 支持 TFTP 消息的 NAT 并为 TFTP 文件打开一个针孔，但 ASA 无法转换 Cisco CallManager IP 地址和嵌入在思科 IP 电话配置文件 （由 TFTP 在电话注册期间传输）中的端口。

注　ASA 支持 SCCP 呼叫的状态故障切换，处于呼叫设置中的呼叫除外。

检查信令消息

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

此信息用于在无需手动配置的情况下为媒体流量透明地穿越防火墙准备访问控制和 NAT 状态。

在确定这些位置时， **inspect skinny** 命令**不**使用隧道默认网关路由。隧道默认网关路由是表单 **route** *interface* **0 0** *metric* **tunneled** 的路由。此路由会覆盖从 IPsec 隧道出口的数据包的默认路由。因此，如果 VPN 流量需要 **inspect skinny** 命令，则不需要配置隧道默认网关路由。相反，请使用其他静态路由或动态路由。

示例

以下示例启用 SCCP 检查引擎，该引擎创建一个与默认端口 (2000) 上的 SCCP 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 SCCP 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map type inspect skinny	为 SCCP 创建一个检查策略。
show skinny	显示关于通过建立的 SCCP 会话的信息。
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，然后设置最大会话数。

inspect snmp

要启用 SNMP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect snmp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect snmp *map_name*

no inspect snmp *map_name*

语法说明

map_name	SNMP 映射的名称。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **inspect snmp** 命令启用 SNMP 检查，同时使用 SNMP 映射 （使用 **snmp-map** 命令创建）配置的设置。在 SNMP 映射配置模式下使用 **deny version** 命令将 SNMP 流量限定为 SNMP 的特定版本。

SNMP 的早期版本不够安全，因此您的安全策略可能会要求将 SNMP 流量限定为版本 2。要拒绝 SNMP 的特定版本，请在 SNMP 映射（使用 **snmp-map** 命令创建）中使用 **deny version** 命令。配置 SNMP 映射后，您可以使用 **inspect snmp** 命令启用映射，然后使用 **service-policy** 命令将其应用到一个或多个接口上。

要为所有接口启用严格 SNMP 应用检查，请使用 **global** 参数取代 **interface outside**。

示例

以下示例标识 SNMP 流量、定义 SNMP 映射、定义策略、启用 SNMP 检查、以及将策略应用到外部接口上：

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
deny version	不允许使用 SNMP 的特定版本的流量通过。
snmp-map	定义 SNMP 映射并启用 SNMP 映射配置模式。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect sqlnet

要启用 Oracle SQL*Net 应用检查，请在类配置模式下使用 **inspect sqlnet** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect sqlnet

no inspect sqlnet

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

分配的默认端口是 1521。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

SQL*Net 协议包含 ASA 可对其进行处理的不同数据包类型，以使数据流在 ASA 的任意一侧看上去与 Oracle 应用一致。

为 SQL*Net 分配的默认端口是 1521。这是 Oracle 为 SQL*Net 使用的值，但是此值与为结构化查询语言 (SQL) 分配的 IANA 端口不一致。使用 **class-map** 命令将 SQL*Net 检查应用到一些端口号上。

注　当在与 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 检查。ASA 在启用 SQL*Net 检查时充当代理，并会将导致数据传输问题的客户端窗口大小从 65000 减少到大约 16000。

ASA 对所有地址执行 NAT，并会在数据包中查找要为 SQL*Net 版本 1 打开的所有嵌入端口。

对于 SQL*Net 版本 2，将会修复数据长度为零、紧跟 REDIRECT 数据包的所有 DATA 或 REDIRECT 数据包。

这些需要修复的数据包包含以下格式的嵌入主机 / 端口地址：

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

不会扫描 SQL*Net 版本 2 TNSFrame 类型（连接、接受、拒绝、重新发送和标记）以获取要执行 NAT 的地址，检查也不会为数据包中的任何嵌入端口打开动态连接。

如果用于有效负载且数据长度为零的 REDIRECT TNSFrame 类型在前面，则会扫描 SQL*Net 版本 2 TNSFrame、Redirect 和 Data 数据包以获取要打开的端口和要执行 NAT 的地址。当数据长度为零的 Redirect 消息通过 ASA 时，将会在连接数据结构中设置一个标志，以期对随后的 Data 或 Redirect 消息执行 NAT 并动态打开端口。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 检查引擎将重新计算校验和，更改 IP、TCP 长度，并使用新旧消息的长度的增量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。扫描 TNSFrame 类型（Connect、Accept、Refuse、Resend、Marker、Redirect 和 Data）和所有数据包以获取端口和地址。对地址执行 NAT 并将打开端口连接。

示例

以下示例启用 SQL*Net 检查引擎，这会创建一个类映射来与默认端口 (1521) 上的 SQL*Net 流量进行匹配。然后，服务策略会应用于外部接口。要为所有接口启用 SQL*Net 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。
show conn	显示不同连接类型 （包括 SQL*Net）的连接状态。

inspect sunrpc

要启用 Sun RPC 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect sunrpc 命令**。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect sunrpc

no inspect sunrpc

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

要启用 Sun RPC 应用检查或更改 ASA 侦听的端口，请在策略映射类配置模式 （在策略映射配置模式内使用 **class** 命令可进入该模式）下使用 **inspect sunrpc** 命令。要删除配置，请使用此命令的 **no** 形式。

inspect sunrpc 命令启用或禁用用于 Sun RPC 协议的应用检查。 NFS 和 NIS 使用 Sun RPC。 Sun RPC 服务可以在系统上的任何端口上运行。当客户端尝试在服务器上访问 Sun RPC 服务时，它必须找出哪个端口正在运行该服务。通过在熟知端口 111 上查询端口映射程序进程可执行此查找。

客户端发送服务的 Sun RPC 程序号，然后取回端口号。从这一点开始，客户端程序会将其 Sun RPC 查询发送到该新端口。当服务器发出应答时， ASA 会拦截此数据包，并同时打开该端口上的初期 TCP 和 UDP 连接。

注　不支持 Sun RPC 有效负载信息的 NAT 或 PAT。

示例

以下示例启用 RPC 检查引擎，该引擎创建一个与默认端口 (111) 上的 XDMCP 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 RPC 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
clear configure sunrpc_server	使用 **sunrpc-server** 命令删除执行的配置。
clear sunrpc-server active	清除 Sun RPC 应用检查为特定服务 （例如 NFS 或 NIS）打开的针孔。
show running-config sunrpc-server	显示关于 Sun RPC 服务表配置的信息。
sunrpc-server	允许使用指定的超时为 Sun RPC 服务 （例如 NFS 或 NIS）创建的针孔。
show sunrpc-server active	显示针孔对 Sun RPC 服务开放。

inspect tftp

要禁用 TFTP 应用检查或启用它 （如果先前已禁用），请在类配置模式下使用 **inspect tftp** 命令。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect tftp

no inspect tftp

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

分配的默认端口是 69。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

RFC 1350 中所述的简单文件传输协议 (TFTP) 是一种用于在 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，以允许在 TFTP 客户端和服务器之间传输文件。具体而言，检查引擎检查 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)。

收到有效读取请求 (RRQ) 或写入请求 (WRQ) 时对动态辅助信道和 PAT 转换进行分配 （在必要时）。 TFTP 随后将此辅助信道用于文件传输或错误通知。

仅 TFTP 服务器可以通过辅助信道发起流量，且在 TFTP 客户端和服务器之间最多可以存在一个不完整的辅助信道。来自服务器的错误通知会关闭辅助信道。

如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检查。

示例

以下示例启用 TFTP 检查引擎，该引擎创建一个与默认端口 (69) 上的 TFTP 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 TFTP 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect waas

要启用 WAAS 应用检查，请在类配置模式下使用 **inspect waas** 命令。类配置模式可从策略映射配置模式访问。要删除配置，请使用此命令的 **no** 形式。

inspect waas

no inspect waas

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在默认检查类上启用 WAAS 应用检查。

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

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

inspect xdmcp

要启用 XDMCP 应用检查或更改 ASA 侦听的端口，请在类配置模式下使用 **inspect xdmcp 命令**。从策略映射配置模式可进入类配置模式。要删除配置，请使用此命令的 **no** 形式。

inspect xdmcp

no inspect xdmcp

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令，并取代了 **fixup** 命令 （已弃用）。

使用指南

inspect xdmcp 命令启用或禁用用于 XDMCP 协议的应用检查。

XDMCP 是一个使用 UDP 端口 177 协商 X 会话 （建立时使用 TCP）的协议。

为成功协商和开始 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 返回连接。要允许返回连接，请在 ASA 上使用 **established** 命令。一旦 XDMCP 顺利通过端口发送显示信息，就会征用 **established** 命令来验证是否应允许此返回连接。

XWindows 会话期间，管理器与熟知端口 6000 l n 上的显示 Xserver 进行对话。由于以下终端设置，每个显示信息都具有一个到 Xserver 的单独连接：

```
setenv DISPLAY Xserver:n
```

其中， *n* 是显示编号。

使用 XDMCP 时，使用 IP 地址协商显示，其中 ASA 可以执行 NAT （如果需要）。 XDCMP 检查不支持 PAT。

示例

以下示例启动 XDMCP 检查引擎，该引擎创建一个与默认端口 (177) 上的 XDMCP 流量匹配的类映射。然后，服务策略会应用于外部接口。要为所有接口启用 XDMCP 检查，请使用 **global** 参数代替 **interface outside**。

```
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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
policy-map	将类映射与特定安全操作关联。
service-policy	将策略映射应用于一个或多个接口。

第 3 章

integrity 至 ip verify reverse-path 命令

integrity

要指定用于 AnyConnect IPsec 连接的 IKEv2 安全关联 (SA) 中的 ESP 完整性算法，请在 IKEv2 策略配置模式下使用 **integrity** 命令。要删除命令并使用默认设置，请使用此命令的 **no** 形式：

integrity {**md5 | sha | sha256 | sha384 | sha512 | null**}

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

语法说明

md5	指定用于 ESP 完整性保护的 MD5 算法。
null	如果 AES-GCM 被指定为加密算法，则允许管理员选择 null 作为 IKEv2 完整性算法。
sha	（默认）指定安全哈希算法 (SHA) SHA 1，在美国 联邦信息处理标准 (FIPS) 中定义，用于 ESP 完整性保护。
sha256	指定具有 256 位摘要的安全哈希算法 SHA 2。
sha384	指定具有 384 位摘要的安全哈希算法 SHA 2。
sha512	指定具有 512 位摘要的安全哈希算法 SHA 2。

默认值

默认算法为 **sha** （SHA 1 算法）。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。输入 **crypto ikev2 policy** 命令后，使用 **integrity** 命令设置 ESP 协议的完整性算法。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。
8.4(2)	添加了 **sha256**、**sha384** 和 **sha512** 关键字以支持 SHA 2。
9.0(1)	添加了 null 选项作为 IKEv2 完整性算法。

示例

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
```

相关命令

命令	说明
encryption	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定加密算法。
group	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 Diffie-Hellman 组。
lifetime	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 SA 生存期。
prf	指定用于 AnyConnect IPsec 连接的 IKEv2 SA 中的伪随机函数。

intercept-dhcp

要启用 DHCP Intercept（DHCP 拦截），请在组策略配置模式下使用 **intercept-dhcp enable** 命令。要从正在运行的配置中删除 **intercept-dhcp （dhcp 拦截）**属性，并允许用户从默认或其他组策略中继承 DHCP Intercept （DHCP 拦截）配置，请使用此命令的 **no** 形式。

intercept-dhcp *netmask* {**enable** | **disable**}

no intercept-dhcp

语法说明

disable	禁用 DHCP 拦截。
enable	启用 DHCP 拦截。
netmask	提供隧道 IP 地址的子网掩码。

默认值

DHCP Intercept （DHCP 拦截）已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要禁用 DHCP Intercept （DHCP 拦截），请使用 **intercept-dhcp disable** 命令。

如果多个拆分隧道选项超过 255 字节，则 Microsoft XP 异常会导致域名瘫痪。为避免此问题，ASA 将其发送的路由数限制为 27 到 40 条路由 （路由数取决于路由类）。

DHCP Intercept（DHCP 拦截）允许 Microsoft XP 客户端对 ASA 使用拆分隧道技术。ASA 可直接向 Microsoft Windows XP 客户端回复 DHCP Inform （DHCP 通知）消息，其中包括为该客户端提供隧道 IP 地址的子网掩码、域名和无类的静态路由。DHCP Intercept（DHCP 拦截）为 Windows XP 版本之前的客户端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。

示例

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

要配置接口并进入接口配置模式，请在全局配置模式下使用 **interface** 命令。要删除子接口，请使用此命令的 **no** 形式；您无法删除物理接口或已映射的接口。

针对物理接口的命令 （适用于 ASASM 之外的所有型号）：

interface *physical_interface*

针对子接口的命令（不适用于 ASA 5505 或 ASASM，也不适用于 ASA 5512-X 到 ASA 5555-X 上的管理接口）：

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

针对多情景模式 （如果已分配映射名称）的命令：

interface *mapped_name*

语法说明

mapped_name	在多情景模式下，如果使用 **allocate-interface** 命令分配了映射的名称，请指定该名称。
physical_interface	将物理接口的类型、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。 物理接口的类型包括以下几个： • **以太网** • **千兆以太网** • **万兆以太网** • **管理** 输入类型，后面紧跟输入插槽 / 端口，例如 **gigabitethernet 0/1**。 管理接口仅用于管理流量。但是，可以用它传送流量 （如果需要），具体取决于型号 （请参阅 **management-only** 命令）。 请参阅您所用型号随附的硬件文档以标识接口类型、插槽和端口号。
subinterface	指定介于 1 和 4294967293 之间的一个整数来命名逻辑子接口。最大子接口数根据具体 ASA 型号而有所不同。子接口不适用于 ASA 5505 的 ASASM，也不适用于 ASA 5512-X 到 ASA 5555-X 上的管理接口。请参阅配置指南以获取每个平台的最大子接口数 （或 VLAN）的详细信息。具有一个或多个 VLAN 子接口的单个接口自动配置为 802.1Q 中继。

默认值

默认情况下， ASA 自动为所有物理接口生成 **interface** 命令。

在多情景模式下，ASA 自动为使用 **allocate-interface** 命令分配到该情景的所有接口生成 **interface** 命令。

接口的默认状态取决于类型和情景模式：

- 多情景模式，情景 - 所有已分配的接口默认情况下已启用，无论接口在系统执行空间中处于何种状态。但是，要通过该接口传递流量，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 - 接口有以下几种默认状态：
  - 物理接口 - 已禁用。
  - 子接口 - 已启用。但是，要通过该子接口传递流量，还必须启用该物理接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令经过修改以允许新子接口命名约定，以及在接口配置模式下将参数更改为单独的命令。

使用指南

在接口配置模式下，可以根据接口和安全情景模式的类型，配置硬件设置 （用于物理接口）、分配名称、分配 VLAN、分配 IP 地址以及配置很多其他设置。

对于要传递流量的已启用接口，请配置以下接口配置模式命令：**nameif** ；对于路由模式，配置 **ip address**。对于子接口，还配置 **vlan** 命令。

如果您要更改接口设置，并且不希望等到现有连接超时后才使用新安全信息，可以使用 **clear local-host** 命令清除连接。

ASA 5512-X 到 ASA 5555-X 上的管理 0/0 接口具有以下特性：

- 不支持通过流量
- 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。对于 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，在 ASA 上配置物理特性（例如启用接口）。

示例

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 子接口分配至 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
```

以下示例在多情景模式下配置用于情景配置的参数：

```
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
```

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
member-interface	将多个接口分配至一个冗余接口。
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行状态和统计信息。
vlan	将 VLAN 分配至子接口。

interface bvi

要为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，请使用此命令的 **no** 形式。

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

语法说明

bridge_group_number	将桥组号指定为介于 1 和 100 之间的一个整数；对于 9.3(1) 版本及更高版本，该范围增加至介于 1 和 250 之间。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。
9.3(1)	我们将编号范围增加至 1 和 250 之间以支持 250 个 BVI（网桥虚拟接口）。

使用指南

使用此命令可进入接口配置模式，以便配置桥组的管理 IP 地址。如果您不想支出安全情景的管理费用，或想要充分利用安全情景，您可以将多个接口组合在一个桥组中，然后配置多个桥组 （每个网络一个桥组）。各桥组的流量是分离的；流量不会路由至 ASA 内的另一个桥组，并且流量必须退出 ASA 后才能由外部路由器路由回 ASA 内的另一个桥组。虽然每个桥组的桥接功能是独立的，但所有桥组之间可共享很多其他功能。例如，所有桥组都共享一种系统日志服务器或 AAA 服务器配置。要实现完整的安全策略独立，请在每个情景中通过一个桥组使用安全情景。每个情景或在单模式下至少需要一个桥组。

每个桥组需要一个管理 IP 地址。 ASA 使用此 IP 地址作为源自桥组的数据包的源地址。管理 IP 地址必须在与所连接的网络相同的子网上。对于 IPv4 流量，需要管理 IP 地址以传递任何流量。对于 IPv6 流量，您必须至少配置本地链路地址以传递流量，但推荐配置全球管理地址以获取全部功能，包括远程管理和其他管理操作。要实现另一管理方法，您可配置独立于任何桥组的管理接口。

对于 9.2 版本及更早版本，您可在单模式或多模式的每个情景中配置最多 8 个桥组；对于 9.3(1) 版本及更高版本，您可配置最多 250 个桥组。每个桥组可包括最多 4 个接口。您无法将同一接口分配至多个桥组。请注意，您必须至少使用 1 个桥组；数据接口必须属于一个桥组。

注　尽管您可以在 ASA 5505 上配置多个桥组，但 ASA 5505 的透明模式下限定 2 个数据接口意味着您只能有效使用 1 个桥组。

注　对于单独的管理接口，不可配置的桥组 (ID 301) 会自动添加至您的配置。此桥组不包括在桥组限制中。

注　ASA 不支持基于辅助网络的流量；仅支持基于同一网络的流量，如同支持管理 IP 地址一样。

示例

以下示例包括两个桥组，每个桥组有三个接口以及一个仅管理接口：

```
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
```

相关命令

命令	说明
ace/bvi	清除网桥虚拟接口配置。
bridge-group	将透明防火墙接口组合在一个桥组中。
interface	配置接口。
ip address	设置一个桥组的管理 IP 地址。
show bridge-group	显示桥组信息，其中包括多个成员接口和 IP 地址。
show running-config interface bvi	显示桥组接口配置。

interface port-channel

要配置 EtherChannel 接口并进入接口配置模式，请在全局配置模式下使用 **interface port-channel** 命令。要删除 EtherChannel 接口，请使用此命令的 **no** 形式。

interface port-channel *number*

no interface port-channel *number*

语法说明

number	指定 EtherChannel 信道组 ID，介于 1 和 48 之间。如果将一个接口添加至该信道组，会自动创建此接口。如果您尚未添加接口，则此命令可创建端口信道接口。 **注**　您需要对该端口信道接口添加至少一个成员接口，然后才能配置它的逻辑参数，如名称。

默认值

默认情况下，端口信道接口已启用。但是，要通过 EtherChannel 传递流量，还必须启用该信道组物理接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。

使用指南

在接口配置模式下，您可以分配名称、分配 IP 地址以及配置很多其他设置。

对于要传递流量的已启用接口，请配置以下接口配置模式命令：**nameif**；对于路由模式，配置 **ip address**。

如果您要更改接口设置，并且不希望等到现有连接超时后才使用新安全信息，可以使用 **clear local-host** 命令清除连接。

注　ASA 5505 或 ASASM 上不支持此命令。您无法将 4GE SSM（包括 ASA 5550 上插槽 1 中集成的 4GE SSM）上的接口用作 EtherChannel 的一部分。

有关接口的详细信息，请参阅 CLI 配置指南。

示例

以下示例将三个接口作为 EtherChannel 的一部分进行配置。此外，还可将系统优先级设置为较高优先级，将千兆以太网 0/2 的优先级设置为高于其他接口，以防分配至 EtherChannel 的接口超过 8 个。

```
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
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

interface redundant

要配置冗余接口并进入接口配置模式，请在全局配置模式下使用 **interface redundant** 命令。要删除该冗余接口，请使用此命令的 **no** 形式。

interface redundant *number*

no interface redundant *number*

语法说明

number	指定逻辑冗余接口 ID，介于 1 和 8 之间。 **redundant** 和 ID 之间的空格是可选的。

默认值

默认情况下，启用冗余接口。但是，要通过冗余接口传递流量，还必须启用成员物理接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	我们引入了此命令。

使用指南

一个冗余接口对包含一个活动物理接口和一个备用物理接口 （请参阅 **member-interface** 命令）。当主用接口出现故障时，备用接口变为活动状态并开始传递流量。

所有 ASA 配置是指逻辑冗余接口，而非成员物理接口。

在接口配置模式下，您可以分配名称、分配 IP 地址以及配置很多其他设置。

对于要传递流量的已启用接口，请配置以下接口配置模式命令：**nameif**；对于路由模式，配置 **ip address**。

如果您要更改接口设置，并且不希望等到现有连接超时后才使用新安全信息，可以使用 **clear local-host** 命令清除连接。

注　ASA 5505 或 ASASM 上不支持此命令。

有关接口的详细信息，请参阅 CLI 配置指南。

示例

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
```

相关命令

命令	说明
clear interface	清除 **show interface** 命令的计数器。
debug redundant-interface	显示与冗余接口事件或错误相关的调试消息。
member-interface	将物理接口分配至冗余接口。
redundant-interface	更改活动成员接口。
show interface	显示接口的运行状态和统计信息。

interface vlan

对于 ASA 5505 和 ASASM，要配置 VLAN 接口并进入接口配置模式，请在全局配置模式下使用 **interface vlan** 命令。要删除 VLAN 接口，请使用此命令的 **no** 形式。

interface vlan *number*

no interface vlan *number*

语法说明

number	指定一个 VLAN ID。 对于 ASA 5505，请使用介于 1 和 4090 之间的 ID。默认情况下，VLAN 1 上启用 VLAN 接口 ID。 对于 ASASM，请使用介于 2 和 1000 之间以及 从 1025 到 4094 之间的 ID。

默认值

默认情况下， VLAN 接口启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	我们引入了此命令。
8.4(1)M	我们引入了 ASASM 支持。

使用指南

对于 ASASM，可以将任何 VLAN ID 添加至配置，但只有由交换机分配至 ASA 的 VLAN 可以传递流量。要查看已分配至 ASA 的所有 VLAN，请使用 **show vlan** 命令。如果您添加了尚未由交换机分配至 ASA 的 VLAN 接口，该接口将处于关闭状态。当您将 VLAN 分配至 ASA 后，该接口改为打开状态。请参阅 **show interface** 命令以获取有关接口状态的详细信息。

在接口配置模式下，您可以分配名称、分配 IP 地址以及配置很多其他设置。

对于要传递流量的已启用接口，请配置以下接口配置模式命令：**nameif**；对于路由模式，配置 **ip address**。对于 ASA 5505 交换机的物理接口，使用 **switchport access vlan** 命令将该物理接口分配至 VLAN 接口。

如果您要更改接口设置，并且不希望等到现有连接超时后才使用新安全信息，可以使用 **clear local-host** 命令清除连接。

有关接口的详细信息，请参阅 CLI 配置指南。

示例

以下示例配置三个 VLAN 接口。第三个主接口无法将流量转发至工作接口。

```
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，包括故障切换接口，需要使用 **failover lan** 命令单独配置该接口：

```
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
```

相关命令

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行状态和统计信息。

interface （VPN 负载平衡）

要在 VPN 负载平衡虚拟集群中指定 VPN 负载平衡的一个非默认公共或专用接口，请在 vpn 负载平衡模式下使用 **interface** 命令。要删除该接口指定并恢复为默认接口，请使用此命令的 **no** 形式。

interface {**lbprivate** | **lbpublic**} *interface-name*

no interface {**lbprivate** | **lbpublic**}

语法说明

interface-name	将接口名称作为 VPN 负载平衡集群的公共或专用接口名称进行配置。
lbprivate	指定此命令配置专用接口来实现 VPN 负载平衡。
lbpublic	指定此命令配置公共接口来实现 VPN 负载平衡。

默认值

如果您省略了 **interface** 命令，**lbprivate** 接口默认配置在**内部**，且 **lbpublic** 接口默认配置在**外部**。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
vpn load-balancing	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 vpn 负载平衡配置模式。

您还必须以前使用过 **interface**、**ip address** 和 **nameif** 命令以配置名称并将其分配至此命令指定的接口。

示例

以下示例是一个 **vpn load-balancing** 命令序列，其中包括 **interface** 命令，该命令将集群的公共接口指定为 “ 测试 ” 接口，将集群的专用接口恢复为默认值 （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)# no interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

相关命令

命令	说明
vpn load-balancing	进入 vpn 负载平衡配置模式。

interface-policy

要指定在监控检测到接口出现故障时适用的故障切换策略，请在故障切换组配置模式下使用 **interface-policy** 命令。要恢复默认值，请使用此命令的 **no** 形式。

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

语法说明

num	指定从 1 到 100 之间的一个数用作百分比，或指定 1 为接口的最大数。
%	（可选）指定数字 *num* 为受监控接口的百分比。

默认值

如果为设备配置了 **failover interface-policy** 命令，则 **interface-policy failover group** 命令的默认值采用该值。如果没有配置，则 *num* 为 1。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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满足所配置的策略并且 ASA 其他功能一切正常，则 ASA 将自身标记为出现故障且可能发生故障切换 （如果活动 ASA 是出现故障的 ASA）。只有由 **monitor-interface** 命令指定为监控的接口才能计入该策略。

示例

下面的部分示例显示了故障切换组的可能配置：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
failover interface-policy	配置接口监控策略。
monitor-interface	指定用于故障切换的监控接口。

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。此额外密码由 ASA 使用，用来对可以使用 SSO 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，请使用该命令的 **no** 版本。

internal-password enable

no internal password

语法说明

enable	支持使用内部密码。

默认值

默认设置为禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果已启用，最终用户在登录到无客户端 SSL VPN 会话时需要输入双重密码。无客户端 SSL VPN 服务器向使用 HTTPS 的身份验证服务器发送 SSO 身份验证请求，包括用户名和密码。如果该身份验证服务器批准身份验证请求，它会将 SSO 身份验证 Cookie 返回至该无客户端 SSL VPN 服务器。此 Cookie 将代表用户保留在 ASA 中，用于对受 SSO 服务器保护的域内安全网站的用户进行身份验证。

如果您要求内部密码不同于 SSL VPN 密码，则内部密码功能非常有用。尤其是，您可以使用一次性密码向 ASA 进行身份验证，使用另一个密码进行内部站点的身份验证。

示例

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)#
```

相关命令

命令	说明
webvpn	进入 webvpn 配置模式，以便配置无客户端 SSL VPN 连接的属性。

interval maximum

要配置在由 DDNS 更新方法建立的更新尝试之间的最大间隔，请在 DDNS 更新方法模式下使用 **interval** 命令。要从正在运行的配置中删除用于 DDNS 更新方法的间隔，请使用此命令的 **no** 形式。

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

语法说明

days	指定多次更新尝试之间的天数 （在 0 到 364 范围内）。
hours	指定多次更新尝试之间的小时数 （在 0 到 23 范围内）。
minutes	指定多次更新尝试之间的分钟数 （在 0 到 59 范围内）。
seconds	指定多次更新尝试之间的秒数 （在 0 到 59 范围内）。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Ddns 更新方法配置	• 是	—	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

将天、小时、分钟和秒加在一起以得到总间隔。

示例

以下示例配置称为 ddns-2 的方法以尝试每隔 3 分 15 秒进行一次更新：

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

相关命令

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。
ddns update	将 DDNS 更新方法与 ASA 接口或 DDNS 更新主机名关联。
ddns update method	创建用于动态更新 DNS 资源记录的方法。
dhcp-client update dns	配置 DHCP 客户端向 DHCP 服务器传送的更新参数。
dhcpd update dns	启用 DHCP 服务器以执行 DDNS 更新。

invalid-ack

要为带有无效 ACK 的数据包设置操作，请在 tcp 映射配置模式下使用 **invalid-ack** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令是使用 **set connection advanced-options** 命令启用的 TCP 规范化策略的一部分。

invalid-ack {**allow** | **drop**}

no invalid-ack

语法说明

allow	允许带有无效 ACK 的数据包。
drop	丢弃带有无效 ACK 的数据包。

默认值

默认操作是丢弃带有无效 ACK 的数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(4)/8.0(4)	引入了此命令。

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。
   a. **invalid-ack** - 在 tcp 映射配置模式下，您可以输入 **invalid-ack** 命令和许多其他命令。
2. **class-map** - 标识要执行 TCP 规范化的流量。
3. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced-options** - 标识您创建的 TCP 映射。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

您可能在以下实例中看到无效 ACK：

- 在 TCP 连接 SYN-ACK 已接收状态中，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一致，则是无效 ACK。
- 只要已接收的 TCP 数据包的 ACK 号大于正在发送的下一个 TCP 数据包的序列号，它就是无效 ACK。

注　WAAS 连接自动允许具有无效 ACK 的 TCP 数据包。

示例

以下示例设置 ASA 以允许带有无效 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)#
```

相关命令

命令	说明
class-map	为服务策略标识流量。
policy-map	标识要应用于服务策略中的流量的操作。
set connection advanced-options	启用 TCP 规范化。
service-policy	将服务策略应用于接口。
show running-config tcp-map	显示 TCP 映射配置。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

ip address

要设置接口 （在路由模式下）或网桥虚拟接口 (BVI) 或管理接口 （在透明模式下）的 IP 地址，请在接口配置模式下使用 **ip address** 命令。要删除该 IP 地址，请使用此命令的 **no** 形式。

ip address *ip_address* [*mask*] [**standby** *ip_address* | **cluster-pool** *poolname*]

no ip address [*ip_address*]

语法说明

cluster-pool *poolname*	（可选）对于 ASA 集群，设置由 **ip local pool** 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。每个集群成员可接收一个来自此池的本地 IP 地址。 您无法提前确定分配至每个设备的确切地址；要查看每个设备上使用的地址，请输入 **show ip local pool** *poolname* 命令。加入集群后，会对每个集群成员分配一个成员 ID。该 ID 确定该池所使用的本地 IP。
ip_address	接口的 IP 地址。
mask	（可选） IP 地址的子网掩码。如果您未设置掩码， ASA 将使用 IP 地址类的默认掩码。
standby *ip_address*	（可选）对于故障切换，设置备用设备的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	对于路由模式，此命令从全局配置模式命令更改为接口配置模式命令。
8.4(1)	对于透明模式，引入了桥组。现在您为 BVI 设置 IP 地址 （而不采用全局方式）。
9.0(1)	引入了 **cluster-pool** 关键字以支持 ASA 集群。

使用指南

此命令还设置了备用地址用于故障切换。

多情景模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一子网上。在多情景模式下，如果此接口位于一个共享的接口上，则每个 IP 地址必须是唯一的，但要在同一子网上。如果该接口是唯一的，则此 IP 地址可供其他情景使用 （如果需要）。

透明防火墙指南

透明防火墙不参与 IP 路由。ASA 所需的 IP 配置只是设置 BVI 地址。此地址是必需的，因为 ASA 将其用作在 ASA 上产生流量的源地址，例如系统消息或与 AAA 服务器的通信。您还可以将此地址用于远程管理访问。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，可在每个情景内设置管理 IP 地址。对于包含管理接口的型号，还可为此接口设置 IP 地址用于管理。

故障切换指南

备用 IP 地址必须与主 IP 地址位于同一子网上。

ASA 集群指南

将集群接口模式配置为单个 （**cluster-interface mode individual** 命令）时，仅能为个人接口设置集群池。唯一的例外是对仅管理接口：

- 您始终可将仅管理接口作为个人接口配置，即使在跨区 EtherChannel 模式下。管理接口即使在透明防火墙模式下也可以是个人接口。
- 在跨区 EtherChannel 模式下，如果您将管理接口作为个人接口配置，则您无法对该管理接口启用动态路由。您必须使用静态路由。

示例

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
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
ip address dhcp	设置接口以从 DHCP 服务器获取 IP 地址。
show ip address	显示分配至接口的 IP 地址。

ip address dhcp

要使用 DHCP 获取接口的 IP 地址，请在接口配置模式下使用 **ip address dhcp** 命令。要禁用此接口的 DHCP 客户端，请使用此命令的 **no** 形式。

ip address dhcp [**setroute**]

no ip address dhcp

语法说明

setroute	（可选）允许 ASA 使用由 DHCP 服务器提供的默认路由。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令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（而非仅外部接口）上启用此命令。

使用指南

重新输入此命令可重置 DHCP 租约并请求新的租约。

如果您尚未使用 **no shutdown** 命令启用接口，却输入了 **ip address dhcp** 命令，则一些 DHCP 请求可能不会发送。

注　ASA 拒绝任何超时设置小于 32 秒的租约。

示例

以下示例对 Gigabitethernet0/1 接口启用 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
```

相关命令

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 地址或设置透明防火墙的管理 IP 地址。
show ip address dhcp	显示从 DHCP 服务器获取的 IP 地址。

ip address pppoe

要启用 PPPoE，请在接口配置模式下使用 **ip address pppoe** 命令。要禁用 PPPoE，请使用此命令的 **no** 形式。

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

语法说明

ip_address	手动设置 IP 地址而不是从 PPPoE 服务器接收地址。
mask	指定 IP 地址的子网掩码。如果您未设置掩码，ASA 将使用 IP 地址类的默认掩码。
setroute	让 ASA 使用由 PPPoE 服务器提供的默认路由。如果 PPPoE 服务器尚未发送默认路由， ASA 会创建将访问集中器地址作为网关的默认路由。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

PPPoE 整合了以太网和 PPP 两个广泛接受的标准，以提供将 IP 地址分配至客户端系统的身份验证方法。互联网运营商部署 PPPoE，是因为它支持使用其现有远程访问基础设施进行高速宽带访问，其客户能够轻松使用。

在您使用 PPPoE 设置 IP 地址之前，请配置 **vpdn** 命令以设置用户名、密码和身份验证协议。如果您对多个接口启用此命令，例如将链路备用至自己的互联网运营商，您就可使用 **pppoe client vpdn group** 命令将每个接口分配至不同的 VPDN 组 （如有必要）。

最大传输单位 (MTU) 大小自动设置为 1492 字节，这是允许以太网帧内 PPPoE 传输的正确值。

重新输入此命令可重置并重新启动 PPPoE 会话。

您无法同时将此命令与 **ip address** 命令或 **ip address dhcp** 命令一同设置。

示例

以下示例对千兆以太网 0/1 接口启用 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
```

相关命令

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 client vpdn group	将此接口分配至特定 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，请使用此命令的 **no** 形式。

ip-address-privacy

no ip-address-privacy

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何通过 SIP 在 SIP 检查策略映射中启用 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
```

相关命令

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

要设置与攻击签名匹配的数据包的默认操作，请在全局配置模式下使用 **ip audit attack** 命令。要恢复该默认操作 （以重置连接），请使用此命令的 **no** 形式。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

语法说明

action	（可选）指定您要定义的一组默认操作。如果您未对任何操作使用此关键字，则 ASA 不采取任何措施。如果您未输入 **action** 关键字， ASA 将假设您输入了该关键字并在配置中显示 **action** 关键字。
alarm	（默认）生成一条系统消息，其中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。

默认值

默认操作是发送并报警。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可指定多个操作或指定无任何操作。当您使用 **ip audit name** 命令配置审核策略后，可使用此命令覆盖您设置的操作。如果您未在 **ip audit name** 命令中指定操作，则使用通过此命令设置的操作。

有关签名列表的信息，请参阅 **ip audit signature** 命令。

示例

以下示例设置用于报警并重置与攻击签名匹配的数据包的默认操作。内部接口的审核策略仅覆盖此用于报警的默认设置，而外部接口的策略通过 **ip audit attack** 命令使用已设置的默认设置。

```
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
```

相关命令

命令	说明
ip audit info	设置与信息签名匹配的数据包的默认操作。
ip audit interface	将审核策略分配至接口。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
ip audit signature	禁用签名。
show running-config ip audit attack	显示 **ip audit attack** 命令的配置。

ip audit info

要设置与信息签名匹配的数据包的默认操作，请在全局配置模式下使用 **ip audit info** 命令。要恢复默认操作 （以生成报警），请使用此命令的 **no** 形式。您可指定多个操作或指定无任何操作。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

语法说明

action	（可选）指定您要定义的一组默认操作。如果您未对任何操作使用此关键字，则 ASA 不采取任何措施。如果您未输入 **action** 关键字， ASA 将假设您输入了该关键字并在配置中显示 **action** 关键字。
alarm	（默认）生成一条系统消息，其中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。

默认值

默认操作是生成报警。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当您使用 **ip audit name** 命令配置审核策略后，可使用此命令覆盖您设置的操作。如果您未在 **ip audit name** 命令中指定操作，则使用通过此命令设置的操作。

有关签名列表的信息，请参阅 **ip audit signature** 命令。

示例

以下示例设置用于报警并重置与信息签名匹配的数据包的默认操作。内部接口的审核策略覆盖此用于报警并丢弃的默认设置，而外部接口的策略通过 **ip audit info** 命令使用已设置的默认设置。

```
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
```

相关命令

命令	说明
ip audit attack	设置与攻击签名匹配的数据包的默认操作。
ip audit interface	将审核策略分配至接口。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
ip audit signature	禁用签名。
show running-config ip audit info	显示 **ip audit info** 命令的配置。

ip audit interface

要将审核策略分配至接口，请在全局配置模式下使用 **ip audit interface** 命令。要从接口中删除该策略，请使用此命令的 **no** 形式。

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

语法说明

interface_name	指定接口的名称。
policy_name	使用 **ip audit name** 命令添加的策略的名称。您可将信息策略和攻击策略分配至每个接口。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例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
```

相关命令

命令	说明
ip audit attack	设置与攻击签名匹配的数据包的默认操作。
ip audit info	设置与信息签名匹配的数据包的默认操作。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
ip audit signature	禁用签名。
show running-config ip audit interface	显示 **ip audit interface** 命令的配置。

ip audit name

要创建一个指定的审核策略，用于标识与预定义的攻击签名或信息签名匹配的数据包时要采取的操作，请在全局配置模式下使用 **ip audit name** 命令。要删除该策略，请使用此命令的 **no** 形式。

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

语法说明

action	（可选）指定您要定义的一组操作。如果您未对任何操作使用此关键字，则 ASA 不采取任何措施。如果您未输入 **action** 关键字，则 ASA 使用由 **ip audit attack** 和 **ip audit info** 命令设置的默认操作。
alarm	（可选）生成一条系统消息，其中显示数据包与签名匹配。
attack	创建攻击签名的审核策略；数据包可能是对您网络攻击的一部分，例如 DoS 攻击或非法的 FTP 命令攻击。
drop	（可选）丢弃数据包。
info	创建信息签名的审核策略；数据包当前未攻击您的网络，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。

默认值

如果您未使用 **ip audit attack** 和 **ip audit info** 命令更改默认操作，则用于攻击签名和信息签名的默认操作将会生成报警。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

签名是与已知攻击模式匹配的活动。例如，有与 DoS 攻击匹配的签名。要应用该策略，请使用 **ip audit interface** 命令将其分配至接口。您可将信息策略和攻击策略分配至每个接口。

有关签名列表的信息，请参阅 **ip audit signature** 命令。

如果流量与签名匹配并且您想要采取操作阻止该流量，请使用 **shun** 命令以防止来自恶意主机的新连接且不允许来自任何现有连接的数据包。

示例

以下示例设置内部接口的审核策略以生成攻击和信息签名的报警，而外部接口的策略重置攻击的连接：

```
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
```

相关命令

命令	说明
ip audit attack	设置与攻击签名匹配的数据包的默认操作。
ip audit info	设置与信息签名匹配的数据包的默认操作。
ip audit interface	将审核策略分配至接口。
ip audit signature	禁用签名。
shun	阻止带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 **ip audit signature** 命令。要重新启用该签名，请使用此命令的 **no** 形式。

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

语法说明

disable	禁用该签名。
signature_number	指定要禁用的签名编号。请参阅表 3-1 以获取支持的签名列表。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果合法流量始终与签名匹配，您可能想要禁用签名并承担禁用签名的风险以避免大量的报警。表 3-1 列出了支持的签名和系统消息编号。

表 3-1　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 options-Bad Option List	信息性	在收到其 IP 数据报头中的 IP 选项列表不完整或格式不正确的 IP 数据报时触发。IP 选项列表包含用于执行各种网络管理或调试任务的一个或多个选项。
1001	400001	IP options-Record Packet Route	信息性	在收到其 IP 选项列表包括选项 7 (Record Packet Route) 的 IP 数据报时触发。
1002	400002	IP options-Timestamp	信息性	在收到其 IP 选项列表包括选项 4 (Timestamp) 的 IP 数据报时触发。
1003	400003	IP options-Security	信息性	在收到其 IP 选项列表包括选项 2 (Security options) 的 IP 数据报时触发。

表 3-1　　签名 ID 和系统消息编号 （续）

签名 ID	消息编号	签名标题	签名类型	说明
1004	400004	IP options-Loose Source Route	信息性	在收到其 IP 选项列表包括选项 3 (Loose Source Route) 的 IP 数据报时触发。
1005	400005	IP options-SATNET ID	信息性	在收到其 IP 选项列表包括选项 8 (SATNET stream identifier) 的 IP 数据报时触发。
1006	400006	IP options-Strict Source Route	信息性	在收到其 IP 选项列表包括选项 2 (Strict Source Routing) 的 IP 数据报时触发。
1100	400007	IP Fragment Attack	攻击	在收到其偏移量字段中显示的偏移值小于 5 但大于 0 的 IP 数据报时触发。
1102	400008	IP Impossible Packet	攻击	当收到源地址与目标地址相同的 IP 数据包时触发。此签名会捕获所谓的 Land 攻击。
1103	400009	IP Overlapping Fragments (Teardrop)	攻击	当包含在同一 IP 数据报的两个片段拥有表示它们在数据报内共享定位的偏移量时触发。这可能意味着片段 A 完全被片段 B 覆盖，或片段 A 部分被片段 B 覆盖。某些操作系统无法正确处理以这种方式重叠的片段，并可能会在接收重叠片段时引发异常或其他不可预料的行为， Teardrop 攻击即采用这种方式发动 DoS。
2000	400010	ICMP Echo Reply	信息性	在收到 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 （应答）的 IP 数据报时触发。
2001	400011	ICMP Host Unreachable	信息性	在收到 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 （主机无法到达）的 IP 数据报时触发。
2002	400012	ICMP Source Quench	信息性	在收到 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 Redirect	信息性	在收到 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。
2004	400014	ICMP Echo Request	信息性	在收到 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	ICMP Time Exceeded for a Datagram	信息性	在收到 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。
2006	400016	ICMP Parameter Problem on Datagram	信息性	在收到 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 （数据报参数问题）的 IP 数据报时触发。
2007	400017	ICMP Timestamp Request	信息性	在收到 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。

表 3-1　　签名 ID 和系统消息编号 （续）

签名 ID	消息编号	签名标题	签名类型	说明
2008	400018	ICMP Timestamp Reply	信息性	在收到 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 Information Request	信息性	在收到 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 Information Reply	信息性	在收到 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 Address Mask Request	信息性	在收到 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 Address Mask Reply	信息性	在收到 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	Fragmented ICMP Traffic	攻击	在收到 IP 报头的协议字段设置为 1 (ICMP) 且更多片段标志设置为 1 (ICMP) 或偏移量字段中有偏移量的 IP 数据报时触发。
2151	400024	Large ICMP Traffic	攻击	在收到 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	Ping of Death Attack	攻击	在收到的 IP 数据报符合以下条件时触发：IP 报头的协议字段设置为 1 (ICMP)，设置了最后片段，且 （IP 偏移量 * 8） + （IP 数据长度）大于 65535，即 IP 偏移量 （表示此片段在原始数据包中的起始位置，以 8 字节为单位）与其余数据包之和大于 IP 数据包的最大大小。
3040	400026	TCP NULL flags	攻击	在未设置 SYN、FIN、ACK 或 RST 标志的单个 TCP 数据包发送至特定主机时触发。
3041	400027	TCP SYN+FIN flags	攻击	在设置了 SYN 和 FIN 标志的单个 TCP 数据包发送至特定主机时触发。
3042	400028	TCP FIN only flags	攻击	在单个孤立的 TCP FIN 数据包发送至特定主机上的特权端口 （端口号小于 1024） 时触发。
3153	400029	FTP Improper Address Specified	信息性	在发出的端口命令的地址与请求主机不同时触发。
3154	400030	FTP Improper Port Specified	信息性	在发出端口命令使用的数据端口小于 1024 或大于 65535 时触发。
4050	400031	UDP Bomb attack	攻击	在指定的 UDP 长度小于指定的 IP 长度时触发。此格式不正确的数据包类型与拒绝服务尝试关联。
4051	400032	UDP Snork attack	攻击	在检测到源端口为 135、 7 或 19 且目标端口为 135 的 UDP 数据包时触发。

表 3-1　　签名 ID 和系统消息编号 （续）

签名 ID	消息编号	签名标题	签名类型	说明
4052	400033	UDP Chargen DoS attack	攻击	在检测到源端口为 7 且目标端口为 19 的 UDP 数据包时触发此签名。
6050	400034	DNS HINFO Request	信息性	在检测到有从 DNS 服务器访问 HINFO 记录的尝试时触发。
6051	400035	DNS Zone Transfer	信息性	在发生源端口为 53 的正常 DNS 区域传输时触发。
6052	400036	DNS Zone Transfer from High Port	信息性	在发生源端口不等于 53 的非法 DNS 区域传输时触发。
6053	400037	DNS Request for All Records	信息性	在一个 DNS 请求所有记录时触发。
6100	400038	RPC Port Registration	信息性	在检测到在目标主机上注册新 RPC 服务的尝试时触发。
6101	400039	RPC Port Unregistration	信息性	在检测到在目标主机上注销现有 RPC 服务的尝试时触发。
6102	400040	RPC Dump	信息性	在向目标主机发出 RPC 转储请求时触发。
6103	400041	Proxied RPC Request	攻击	在向目标主机的端口映射器发送代理 RPC 请求时触发。
6150	400042	ypserv (YP server daemon) Portmap Request	信息性	在向用于 YP 服务器后台守护程序 (ypserv) 端口的端口映射器发出请求时触发。
6151	400043	ypbind (YP bind daemon) Portmap Request	信息性	在向用于 YP 绑定后台守护程序 (ypbind) 端口的端口映射器发出请求时触发。
6152	400044	yppasswdd (YP password daemon) Portmap Request	信息性	在向用于 YP 密码后台守护程序 (yppasswdd) 端口的端口映射器发出请求时触发。
6153	400045	ypupdated (YP update daemon) Portmap Request	信息性	在向用于 YP 更新后台守护程序 (ypupdated) 端口的端口映射器发出请求时触发。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	信息性	在向用于 YP 传输后台守护程序 (ypxfrd) 端口的端口映射器发出请求时触发。
6155	400047	mountd (mount daemon) Portmap Request	信息性	在向用于安装后台守护程序 (mountd) 端口的端口映射器发出请求时触发。
6175	400048	rexd (remote execution daemon) Portmap Request	信息性	在向用于远程执行后台守护程序 (rexd) 端口的端口映射器发出请求时触发。
6180	400049	rexd (remote execution daemon) Attempt	信息性	在调用 rexd 程序时触发。远程执行后台守护程序是负责执行远程程序的服务器。这可能表示尝试对系统资源进行未经授权的访问。
6190	400050	statd Buffer Overflow	攻击	在发送大型 statd 请求时触发。这可能表示尝试导致缓冲区溢出并获得对系统资源的访问权限。

示例

以下示例禁用签名 6100：

```
ciscoasa(config)# ip audit signature 6100 disable
```

相关命令

命令	说明
ip audit attack	设置与攻击签名匹配的数据包的默认操作。
ip audit info	设置与信息签名匹配的数据包的默认操作。
ip audit interface	将审核策略分配至接口。
ip audit name	创建一个指定的审核策略，用于标识与攻击签名或信息签名匹配的数据包时要采取的操作。
show running-config ip audit signature	显示 **ip audit signature** 命令的配置。

ip-comp

要启用 LZS IP 压缩，请在组策略配置模式下使用 **ip-comp enable** 命令。要禁用 IP 压缩，请使用 **ip-comp disable** 命令。要从正在运行的配置中删除 **ip-comp** 属性，请使用此命令的 **no** 形式。

ip-comp {**enable** | **disable**}

no ip-comp

语法说明

disable	禁用 IP 压缩。
enable	启用 IP 压缩。

默认值

IP 压缩已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的 **no** 形式可从另一个组策略继承值。启用数据压缩可能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。

注意事项

数据压缩可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，我们建议您仅对使用调制解调器连接的远程用户启用数据压缩。专门针对调制解调器用户设计一个组策略，并仅对这些用户启用压缩。

如果终端生成 IP 压缩流量，您应该禁用 IP 压缩以避免不正确的数据包解压。如果对特定局域网到局域网隧道启用 IP 压缩，则主机 A 尝试将 IP 压缩数据从隧道一侧传送到另一侧时无法与主机 B 通信。

注　当启用 **ip-comp** 命令并为 “ 预加密 ” 配置 IPsec 片段时，您无法使用 IPsec 压缩（ip-comp_option 和预加密）。发送到加密芯片的 IP 报头变得混乱 （由于压缩所致），从而导致加密的芯片处理所提供的出站数据包时产生错误消息。您还可以检查 MTU 级别以确保它是一个很小的量 （如 600 字节）。

示例

以下示例显示如何对名为 “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，请在全局配置模式下使用 **ip local pool** 命令。要删除该地址池，请使用此命令的 **no** 形式。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

语法说明

first-address	指定 IP 地址范围内的起始地址。
last-address	指定 IP 地址范围内的最后地址。
mask *mask*	（可选）指定地址池的子网掩码。
poolname	指定 IP 地址池的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	通过在 **ip address** 命令中使用集群池的 IP 本地池，可以支持 ASA 集群。

使用指南

将 IP 地址分配到属于非标准网络的 VPN 客户端并且使用默认掩码不能正确路由数据时，您必须提供掩码值。典型的示例是如果 IP 本地池包含 10.10.10.0/255.255.255.0 地址 （因为这是默认的 A 类网络）。当 VPN 客户端需要通过不同接口访问 10 网络内的不同子网时，这会导致一些路由问题。例如，如果一台打印机的地址 10.10.100.1/255.255.255.0 通过接口 2 可用，但 10.10.10.0 网络需要通过 VPN 隧道并且是接口 1 才能用，则 VPN 客户端会对将打印机的路由数据发往何处产生混淆。10.10.10.0 和 10.10.100.0 子网均属于 10.0.0.0 A 类网络，因此打印机数据可能通过 VPN 隧道发送。

示例

以下示例显示如何配置名为 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
```

相关命令

命令	说明
clear configure ip local pool	删除所有 IP 本地池。
show running-config ip local pool	显示 IP 池配置。指定特定的 IP 地址池，包括命令中的名称。

ip-phone-bypass

要启用 IP 电话旁路，请在组策略配置模式下使用 **ip-phone-bypass enable** 命令。要从正在运行的配置中删除 IP 电话旁路属性，请使用此命令的 **no** 形式。

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

语法说明

disable	禁用 IP 电话旁路。
enable	启用 IP 电话旁路。

默认值

IP 电话旁路已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要禁用 IP 电话旁路，请使用 **ip-phone-bypass disable** 命令。此命令的 **no** 形式选项允许从另一个组策略中继承 IP 电话旁路的值。

IP 电话旁路可以使 IP 电话在硬件客户端后面进行连接，无需进行用户身份验证处理。如果已启用安全设备身份验证，它仍然有效。

仅当启用用户身份验证后，才需要配置 IP 电话旁路。

您还需要配置 **mac-exempt** 选项以免除客户端身份验证。请参阅 **vpnclient mac-exempt** 命令以获取详细信息。

示例

以下示例显示如何对名为 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
```

相关命令

命令	说明
user-authentication	要求硬件客户端后面的用户向 ASA 表明自己的身份，然后才能连接。

ips

要将流量从 ASA 转移至 AIP SSM 以便检查，请在类配置模式下使用 **ips** 命令。要删除此命令，请使用此命令的 **no** 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*}]

语法说明

fail-close	在 AIP SSM 出现故障时阻止流量。
fail-open	在 AIP SSM 出现故障时允许流量。
inline	将数据包发送到 AIP SSM； IPS 操作可能导致丢弃数据包。
promiscuous	复制 AIP SSM 的数据包； 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 （6.0 版本或更高版本）上使用虚拟传感器，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。列出可用的传感器。您还可以使用 **show ips** 命令。 如果您在 ASA 上使用多情景模式，您只能指定分配到情景的传感器（请参阅 **allocate-ips** 命令）。如果在情景中配置，请使用 *mapped_name* 参数。 如果您未指定传感器名称，则流量使用默认传感器。在多情景模式下，您可为情景指定默认传感器。在单模式下或如果您未在多模式下指定默认传感器，流量使用 AIP SSM 上设置的默认传感器。 如果您输入 AIP SSM 上尚未存在的名称，则会出现错误并会拒绝命令。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	增加了虚拟传感器支持。

使用指南

ASA 5500 系列支持 AIP SSM，后者运行高级 IPS 软件以提供前瞻式、全功能入侵防御服务，从而在恶意流量 （包括蠕虫和网络病毒）影响网络之前将其阻止。配置 **ips** 命令 （在 ASA 上）前后，在 AIP SSM 上配置安全策略。您可从 ASA 与 AIP SSM 进行会话 （使用 **session** 命令），也可以在 AIP SSM 的管理接口上使用 SSH 或 Telnet 直接与其连接。此外，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思科入侵防御系统传感器*。

要配置 **ips** 命令，您必须先配置 **class-map** 命令、 **policy-map** 命令以及 **class** 命令。

AIP SSM 从 ASA 运行单独的应用。但是，它集成到了 ASA 流量中。AIP SSM 自身不包含任何外部接口（管理接口除外）。当您对 ASA 上的流量类应用 **ips** 命令时，流量会以下列方式通过 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；请参阅 **promiscuous** 关键字，了解有关仅将流量发送到 AIP SSM 的信息）。
4. AIP SSM 将其安全策略应用于流量并执行适当操作。
5. 通过背板将有效流量发回 ASA； AIP SSM 根据其安全策略可能阻止某些流量，该流量不再传送。
6. 应用 VPN 策略 （如果已配置）。
7. 流量退出 ASA。

示例

在以下示例中，如果 AIP SSM 卡由于任何原因出现故障，所有 IP 流量将转移至采用混合模式的 AIP SSM，并阻止所有 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
```

在以下示例中，如果 AIP SSM 卡由于任何原因出现故障，去往 10.1.1.0 网络及 10.2.1.0 网络的所有 IP 流量将转移至采用内嵌模式的 AIP SSM，并允许所有流量通过。对于 my-ips-class 流量，使用 sensor1 ；对于 my-ips-class2 流量，使用 sensor2。

```
ciscoasa(config)# access-list my-ips-acl 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-acl
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
```

相关命令

命令	说明
allocate-ips	将虚拟传感器分配到安全情景。
class	指定要用于流量分类的类映射。
class-map	标识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。
show running-config policy-map	显示所有当前策略映射配置。

ipsec-udp

要启用 IPsec over UDP，请在组策略配置模式下使用 **ipsec-udp enable** 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

语法说明

disable	禁用 IPsec over UDP。
enable	启用 IPsec over UDP。

默认值

IPsec over UDP 已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的 **no** 形式可从另一个组策略继承 IPsec over UDP 的值。

IPsec over UDP，有时也称为 IPsec through NAT，可使思科 VPN 客户端或硬件客户端通过 UDP 连接至正在运行 NAT 的 ASA。

要禁用 IPsec over UDP，请使用 **ipsec-udp disable** 命令。

要使用 IPsec over UDP，您还必须配置 **ipsec-udp-port** 命令。

还必须配置思科 VPN 客户端以使用 IPsec over UDP （默认情况下进行了上述配置）。 VPN 3002 无需配置即可使用 IPsec over UDP。

IPsec over UDP 是专有的 （仅应用于远程访问连接）并要求模式配置，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 可能稍微降低系统性能。

ASA5505 作为 VPN 客户端运行时不支持 ipsec-udp-port 命令。在客户端模式下， ASA 5505 可在 UDP 端口 500 和 / 或 4500 上启动 IPsec 会话。

示例

以下示例显示如何对名为 FirstGroup 的组策略配置 IPsec over UDP：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

相关命令

命令	说明
ipsec-udp-port	指定 ASA 用于监听 UDP 流量的端口。

ipsec-udp-port

要设置 IPsec over UDP 的 UDP 端口号，请在组策略配置模式下使用 **ipsec-udp-port** 命令。要禁用该 UDP 端口，请使用此命令的 **no** 形式。

ipsec-udp-port *port*

no ipsec-udp-port

语法说明

port	使用 4001 到 49151 范围内的一个整数标识 UDP 端口号。

默认值

默认端口为 10000。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令的 **no** 形式可从另一个组策略继承 IPsec over UDP 端口的值。

在 IPsec 协商中。 ASA 在已配置的端口上进行侦听并为该端口转发 UDP 流量 （即使其他过滤规则丢弃 UDP 流量）。

您可以配置启用此功能的多个组策略，并且每个组策略可以使用不同的端口号。

示例

以下示例显示如何对名为 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
```

相关命令

命令	说明
ipsec-udp	使思科 VPN 客户端或硬件客户端通过 UDP 连接至正在运行 NAT 的 ASA。

ip verify reverse-path

要启用单播 RPF，请在全局配置模式下使用 **ip verify reverse-path** 命令。要禁用此功能，请使用此命令的 **no** 形式。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

语法说明

interface_name	要在其上启用单播 RPF 的接口。

默认值

默认禁用此功能。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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）。

通常情况下， ASA 在确定向何处转发数据包时只查看目标地址。单播 RPF 指示 ASA 还要查看源地址；这也是它称为逆向路径转发的原因。对于您想要允许通过 ASA 的任何流量， ASA 路由表必须包括返回源地址的路由。请参阅 RFC 2267 以获取详细信息。

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而路由表中不包含源地址，则 ASA 使用默认路由来将外部接口正确标识为源接口。

如果流量从路由表中包含的已知地址进入外部接口，但与内部接口关联，则 ASA 会丢弃该数据包。同样，因为匹配的路由 （默认路由）表示外部接口，如果流量从未知的源地址进入内部接口， ASA 会丢弃该数据包。

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。检查非初始数据包的目的是确保它们到达初始数据包所用的同一接口上。

示例

以下示例对外部接口启用单播 RPF：

```
ciscoasa(config)# ip verify reverse-path interface outside
```

相关命令

命令	说明
clear configure ip verify reverse-path	清除使用 **ip verify reverse-path** 命令的配置集。
clear ip verify statistics	清除单播 RPF 统计信息。
show ip verify statistics	显示单播 RPF 统计信息。
show running-config ip verify reverse-path	显示使用 **ip verify reverse-path** 命令的配置集。

第 4 章

ipv6 address 至 ipv6-vpn-filter 命令

ipv6 address

要在接口上（路由模式）或针对管理地址（透明模式）启用 IPv6 并配置 IPv6 地址，请使用 **ipv6 address** 命令。要删除 IPv6 地址，请使用此命令的 **no** 形式。

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-prefix* | **cluster-pool** *poolname*] | *ipv6-prefix*/*prefix-length* **eui-64** | *ipv6-address* **link-local** [**standby** *ipv6-address*]}

no ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address* | **cluster-pool** *poolname*] | *ipv6-prefix*/*prefix-length* **eui-64** | *ipv6-address* **link-local** [**standby** *ipv6-address*]}

语法说明

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会根据在路由器通告消息中收到的前缀来配置 IPv6 地址。当启用无状态自动配置时，会自动为接口生成一个基于修改的 EUI-64 接口 ID 的链路本地地址。不支持透明防火墙模式。 **注**　虽然 RFC 4862 指定了配置为无状态自动配置的主机不发送路由器通告消息，但 ASA 在这种情况下仍会发送路由器通告消息。请参阅 **ipv6 nd suppress-ra** 命令来抑制消息。
cluster-pool *poolname*	（可选）对于 ASA 集群，设置由 **ipv6 local pool** 命令定义的集群地址池。通过参数定义的主集群 IP 地址仅属于当前主设备。每个集群成员可接收一个来自此池的本地 IP 地址。 您无法预先确定为每个设备分配的准确地址，要查看每个设备上使用的地址，请输入 **show ipv6 local pool** *poolname* 命令。加入集群后，会对每个集群成员分配一个成员 ID。该 ID 确定该池所使用的本地 IP。
ipv6-address/*prefix-length*	为接口分配全局地址。当分配全局地址时，会自动为接口创建链路本地地址。
ipv6-prefix/*prefix-length* **eui-64**	通过将指定的前缀与根据接口 MAC 地址生成的接口 ID（采用修改的 EUI-64 格式）相结合来为接口分配全局地址。当分配全局地址时，会自动为接口创建链路本地地址。如果为 *prefix-length* 参数指定的值大于 64 位，前缀位将优先于接口 ID。如果另一台主机正在使用指定的地址，将显示一条错误消息。 您无需指定备用地址；接口 ID 将自动生成。 在 48 位链路层 (MAC) 地址的高 3 个字节（OUI 字段）和低 3 个字节（序列号）之间插入十六进制数 FFFE，就可以获得修改的 EUI-64 格式接口 ID。为确保选定地址来自唯一的以太网 MAC 地址，高位字节中的第二最低位将取反（统一 / 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。

ipv6-address **link-local**	仅手动配置链路本地地址。使用此命令指定的 *ipv6-address* 将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 和修改的 EUI-64 格式接口 ID 组成。 MAC 地址为 00E0.B601.3B7A 的接口的链路本地地址为 FE80::2E0:B6FF:FE01:3B7A。如果另一台主机正在使用指定的地址，将显示一条错误消息。
standby *ipv6-address*	（可选）指定故障切换对中的备用设备或故障切换组使用的接口地址。

默认值

禁用 IPv6。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。
8.2(2)	为命令增加了对备用地址的支持。
8.4(1)	对于透明模式，引入了桥组。您将设置 BVI 的地址，而且不是全局设置。
9.0(1)	引入了 **cluster-pool** 关键字以支持 ASA 集群。

使用指南

在接口上配置 IPv6 地址将在该接口上启用 IPv6 ；在指定 IPv6 地址后不需要使用 **ipv6 enable** 命令。

多情景模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一子网上。在多情景模式下，如果此接口位于一个共享的接口上，则每个 IP 地址必须是唯一的，但要在同一子网上。如果该接口是唯一的，则此 IP 地址可供其他情景使用 （如果需要）。

透明防火墙指南

透明防火墙不参与 IP 路由。ASA 所需的 IP 配置只是设置 BVI 地址。此地址是必需的，因为 ASA 将其用作在 ASA 上产生流量的源地址，例如系统消息或与 AAA 服务器的通信。您还可以将此地址用于远程管理访问。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，可在每个情景内设置管理 IP 地址。对于包含管理接口的型号，还可为此接口设置 IP 地址用于管理。

故障切换指南

备用 IP 地址必须与主 IP 地址位于同一子网上。

ASA 集群指南

只有将集群接口模式设置为单独 (**cluster-interface mode individual**) 后，才能为单独接口设置集群池。唯一的例外是对仅管理接口：

- 您始终可将仅管理接口作为个人接口配置，即使在跨区 EtherChannel 模式下。管理接口即使在透明防火墙模式下也可以是个人接口。
- 在跨区 EtherChannel 模式下，如果您将管理接口作为个人接口配置，则您无法对该管理接口启用动态路由。您必须使用静态路由。

示例

以下示例为所选接口分配 3FFE:C00:0:1::576/64 作为全局地址：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

以下示例自动为所选接口分配 IPv6 地址：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

以下示例为所选接口分配 IPv6 地址 3FFE:C00:0:1::/64，并在地址的低 64 位中指定 EUI-64 接口 ID。如果此设备是故障切换对的一部分，则无需指定 **standby** 关键字；将自动使用修改的 EUI-64 接口 ID 创建备用地址。

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

以下示例为所选接口分配 FE80::260:3EFF:FE11:6670 作为链路层地址：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

以下示例为所选接口分配 3FFE:C00:0:1::576/64 作为全局地址，分配 3FFE:C00:0:1::575 作为备用设备上相应接口的地址：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 3ffe:c00:0:1::576/64 standby 3ffe:c00:0:1::575
```

以下示例为故障切换对中主要设备上的所选接口分配 FE80::260:3EFF:FE11:6670 作为链路层地址，为备用设备上的相应接口分配 FE80::260:3EFF:FE11:6671 作为链路层地址。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

相关命令

命令	说明
debug ipv6 interface	显示 IPv6 接口的调试信息。
show ipv6 interface	显示配置为 IPv6 的接口的状态。

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 **ipv6 dhcprelay enable** 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*

语法说明

interface	指定目标的输出接口。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令允许在接口上启用 DHCPv6 中继服务。启用该服务后，该接口上的客户端的传入 DHCPv6 消息 （可能已被其他中继代理中继）将通过所有已配置的传出链路转发到所有已配置的中继目的地。对于多情景模式，无法在被多个情景 （即，共享接口）使用的接口上启用 DHCP 中继服务。

示例

以下示例演示如何在 ASA 外部接口上为 IP 地址为 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
```

相关命令

命令	说明
ipv6 dhcprelay server	指定客户端消息转发到的 IPv6 DHCP 服务器目的地址。
ipv6 dhcprelay timeout	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 server

要指定客户端消息转发到的 IPv6 DHCP 服务器目的地址，请在全局配置模式下使用 **ipv6 dhcprelay server** 命令。要删除 IPv6 DHCP 服务器目的地址，请使用此命令的 **no** 形式。

ipv6 dhcprelay server *ipv6-address* [*interface*]

no ipv6 dhcprelay server *ipv6-address* [*interface*]

语法说明

interface	（可选）指定目的地的输出接口。
ipv6-address	可以是链路范围的单播、组播、站点范围单播或全局 IPV6 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定客户端消息转发到的 IPv6 DHCP 服务器目的地址。客户端消息通过与输出接口连接的链路转发到目的地址。如果指定的地址是链路范围地址，则必须指定接口。未指定、环回和节点本地组播地址不允许作为中继目的地。最多可为每个环境指定 10 个服务器。

示例

以下示例演示如何在 ASA 外部接口上为 IP 地址为 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
```

相关命令

命令	说明
ipv6 dhcprelay enable	在接口上启用 IPv6 DHCP 中继服务。
ipv6 dhcprelay timeout	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

要设置允许 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，请在全局配置模式下使用 **ipv6 dhcprelay timeout** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

ipv6 dhcprelay timeout *seconds*

no ipv6 dhcprelay timeout *seconds*

语法说明

seconds	设置允许 DHCPv6 中继地址协商的秒数。有效值范围为 1 到 3600。

默认值

默认值为 60 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可设置允许 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）。

示例

以下示例演示如何在 ASA 外部接口上为 IP 地址为 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
```

相关命令

命令	说明
ipv6 dhcprelay server	指定客户端消息转发到的 IPv6 DHCP 服务器目的地址。
ipv6 dhcprelay enable	指定客户端消息转发到的 IPv6 DHCP 服务器目的地址。

ipv6 enable

要启用 IPv6 处理，如果您尚未配置显式 IPv6 地址，请在全局配置模式下使用 **ipv6 enable** 命令。要在未配置显式 IPv6 地址的接口上禁用 IPv6 处理，请使用此命令的 **no** 形式。

ipv6 enable

no ipv6 enable

语法说明

此命令没有任何参数或关键字。

默认值

禁用 IPv6。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

ipv6 enable 命令会自动在接口上配置 IPv6 链路本地单播地址，同时启用该接口以进行 IPv6 处理。

no ipv6 enable 命令不会禁用已配置显式 IPv6 地址的接口上的 IPv6 处理。

示例

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
```

相关命令

命令	说明
ipv6 address	配置接口的 IPv6 地址并在该接口上启用 IPv6 处理。
show ipv6 interface	显示配置为 IPv6 的接口的可用性状态。

ipv6 enforce-eui64

要在本地链路上的 IPv6 地址中实施修改的 EUI-64 格式接口标识符，请在全局配置模式下使用 **ipv6 enforce-eui64** 命令。要禁止实施修改的 EUI-64 地址格式，请使用此命令的 **no** 形式。

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

语法说明

if_name	指定要为其实施修改的 EUI-64 地址格式的接口名称，如 **nameif** 命令所指定。

默认值

禁止实施修改的 EUI-64 格式。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

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的 EUI-64 格式。如果 IPv6 数据包未对接口标识符使用修改的 EUI-64 格式，该数据包将被丢弃，并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed. (%ASA-3-325003: EUI-64 源地址检查失败。)
```

仅当创建流时才会执行地址格式验证。不会检查来自现有流的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器后面的主机接收的数据包将无法通过地址格式验证，并将被丢弃，因为其源 MAC 地址将是路由器 MAC 地址，而不是主机 MAC 地址。

在 48 位链路层 (MAC) 地址的高 3 个字节 （OUI 字段）和低 3 个字节 （序列号）之间插入十六进制数 FFFE，就可以获得修改的 EUI-64 格式接口标识符。为确保选定地址来自唯一的以太网 MAC 地址，高位字节中的第二最低位将取反 （统一 / 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。

示例

以下示例对在内部接口上接收的 IPv6 地址实施修改的 EUI-64 格式：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

相关命令

命令	说明
ipv6 address	在接口上配置 IPv6 地址。
ipv6 enable	在接口上启用 IPv6。

ipv6 icmp

要配置接口的 ICMP 访问规则，请在全局配置模式下使用 **ipv6 icmp** 命令。要删除 ICMP 访问规则，请使用此命令的 **no** 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*

语法说明

any	用于指定任意 IPv6 地址的关键字。 IPv6 前缀 ::/0 的缩写。
deny	在所选接口上阻止指定的 ICMP 流量。
host	指示地址指向特定主机。
icmp-type	指定访问规则过滤的 ICMP 消息类型。该值可以是有效的 ICMP 类型编号 （从 0 到 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
if-name	访问规则适用的接口名称，如 **nameif** 命令所指定。
ipv6-address	将 ICMPv6 消息发送到接口的主机的 IPv6 地址。
ipv6-prefix	将 ICMPv6 消息发送到接口的 IPv6 网络。
permit	在所选接口上允许指定的 ICMP 流量。
prefix-length	IPv6 前缀的长度。此值指示地址有多少个高阶相邻位用于构成前缀的网络部分。前缀长度前必须有斜线 (/)。

默认值

如果未定义任何 ICMP 访问规则，将允许所有 ICMP 流量。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

IPv6 中的 ICMP 与 IPv4 中的 ICMP 功能相同。ICMPv6 可生成错误消息，如 ICMP 目的无法到达消息以及 ICMP 回应请求与应答消息等信息性消息。此外，IPv6 中的 ICMP 数据包还用于 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 加密的成本，MTU 值应设置为不低于 1380。将接口设置为低于 1380 字节可能会导致丢包。

如果没有为接口定义任何 ICMP 访问规则，将允许所有 IPv6 ICMP 流量。

如果为接口定义了 ICMP 规则，则规则的处理顺序为处理第一条匹配规则，随后隐式拒绝所有规则。例如，如果第一条匹配的规则是允许规则，则处理 ICMP 数据包。如果第一条匹配的规则是拒绝规则，或者 ICMP 数据包不匹配该接口上的任何规则，则 ASA 将丢弃 ICMP 数据包并生成系统日志消息。

因此，您输入 ICMP 规则的顺序很重要。如果您输入了拒绝来自特定网络的所有 ICMP 流量的规则，接着输入允许来自该网络上特定主机的 ICMP 流量的规则，则主机规则永远不会被处理。ICMP 流量被网络规则阻止。但是，如果先输入主机规则，再输入网络规则，则主机 ICMP 流量将被允许，而来自该网络的所有其他 ICMP 流量将被阻止。

ipv6 icmp 命令用于配置在 ASA 接口终止的 ICMP 流量的访问规则。要配置穿透 ICMP 流量的访问规则，请参阅 **ipv6 access-list** 命令。

示例

以下示例在外部接口上拒绝所有 ping 请求并允许所有 packet-too-big （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
```

相关命令

命令	说明
ipv6 access-list	配置访问列表。

ipv6 local pool

要配置 IPv6 地址池，请在全局配置模式下使用 **ipv6 local pool** 命令。要删除地址池，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*

语法说明

ipv6_address	指定地址池的起始 IPv6 地址。
number_of_addresses	范围：1-16384.
pool_name	指定要为此 IPv6 地址池分配的名称。
prefix_length	范围：0-128.

默认值

默认情况下，未配置 IPv6 本地地址池。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	可以在 **ipv6 address** 命令中将 IPv6 本地池用于集群池，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（注意此命令中有 “s”）。组策略中的 ipv6-address-pools 设置将覆盖隧道组中的 ipv6-address-pools 设置。

示例

以下示例配置一个名为 firstipv6pool 的 IPv6 地址池，以用于为远程客户端分配地址：

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

相关命令

命令	说明
ipv6-address-pool	将 IPv6 地址池与 VPN 隧道组策略相关联。
ipv6-address-pools	将 IPv6 地址池与 VPN 组策略相关联。
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

要配置在重复地址检测过程中在接口上发送的连续邻居请求消息数量，请在接口配置模式下使用 **ipv6 nd dad attempts** 命令。要恢复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 *value*

no ipv6 nd dad attempts *value*

语法说明

value	从 0 至 600 的一个数字。输入 0 将禁用指定接口上的重复地址检测。输入 1 将配置没有后续传输的单次传输。默认值为 1 条消息。

默认值

默认尝试次数为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

在将地址分配到接口之前，重复地址检测会验证新单播 IPv6 地址的唯一性 （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。使用 **ipv6 nd ns-interval** 命令来配置发送邻居请求消息的频率。

重复地址检测在管理性关闭的接口上将暂停。当接口处于管理性关闭状态时，分配到该接口的单播 IPv6 地址均设置为挂起状态。

当接口恢复为管理性开启状态后，重复地址检测自动在该接口上重新启动。恢复为管理性开启状态的接口会针对该接口上的所有单播 IPv6 地址重新启动重复地址检测。

注　对接口的链路本地地址执行重复地址检测时，其他 IPv6 地址的状态仍设置为暂定。对链路本地地址的重复地址检测完成后，对其余 IPv6 地址执行重复地址检测。

当重复地址检测标识出重复地址时，该地址的状态设置为 DUPLICATE，并且该地址不会被使用。如果重复地址是接口的链路本地地址，则在该接口上将禁用 IPv6 数据包的处理，并发出类似下面的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

如果重复地址是接口的全局地址，则该地址不会被使用，并发出类似下面的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

当地址的状态设置为 DUPLICATE 时，与重复地址关联的所有配置命令均保持已配置状态。

如果接口的链路本地地址发生变化，将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）。

示例

以下示例配置了当对接口的暂定单播 IPv6 地址执行重复地址检测时，将发送 5 个连续邻居请求消息：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

以下示例禁用对所选接口的重复地址检测：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

相关命令

命令	说明
ipv6 nd ns-interval	配置接口上的 IPv6 邻居请求传输的间隔。
show ipv6 interface	显示配置为 IPv6 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记，请在接口配置模式下使用 **ipv6 nd managed config-flag** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

ipv6 nd managed-config-flag

no ipv6 managed-config-flag

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

IPv6 自动配置客户端主机可以使用此标记指示如下信息：必须使用状态地址配置协议 (DHCPv6)，才能获取除了衍生无状态自动配置地址以外的地址。

示例

以下示例在 IPv6 路由器通告数据包中为千兆以太网 0/0 接口设置托管地址配置标记：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

相关命令

命令	说明
ipv6 nd other-config-flag	将 ASA 配置为在 IPv6 路由器通告数据包中设置其他配置标记。

ipv6 nd ns-interval

要配置接口上的 IPv6 邻居请求重新传输的间隔，请在接口配置模式下使用 **ipv6 nd ns-interval** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

语法说明

value	IPv6 邻居请求传输的间隔 （以毫秒为单位）。有效值范围为 1000 至 3600000 毫秒。默认值为 1000 毫秒。

默认值

邻居请求传输的默认间隔为 1000 毫秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

此值将包括在此接口发出的所有 IPv6 路由器通告中。

示例

以下示例为千兆以太网 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
```

相关命令

命令	说明
show ipv6 interface	显示配置为 IPv6 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其他配置标记，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，请使用此命令的 **no** 形式。

ipv6 nd other-config-flag

no ipv6 other-config-flag

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

IPv6 自动配置客户端主机可以使用此标记指示如下信息：必须使用状态地址配置协议 (DHCPv6)，才能获取 DNS 服务器信息等非地址配置信息。

示例

以下示例在 IPv6 路由器通告数据包中为千兆以太网 0/0 接口设置其他配置标记：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

相关命令

命令	说明
ipv6 nd managed-config-flag	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记。

ipv6 nd prefix

要配置在 IPv6 路由器通告中包含哪些 IPv6 前缀，请在接口配置模式下使用 **ipv6 nd prefix** 命令。要删除前缀，请使用此命令的 **no** 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**]

语法说明

at *valid-date preferred-date*	生命期和首选项到期的日期和时间。在达到指定的日期和时间之前，前缀有效。日期以 *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* 的形式表示。
default	使用默认值。
infinite	（可选）有效生命期不过期。
ipv6-prefix	要包括在路由器通告中的 IPv6 网络号。 此参数必须是 RFC 2373 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
no-advertise	（可选）向本地链路上的主机指示指定的前缀并非用于 IPv6 自动配置。
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）指示指定的前缀并不用于 on-link （在线）确定。
preferred-lifetime	对指定的 IPv6 前缀进行通告的首选时间量 （以秒为单位）。有效值范围为 0 到 4294967295 秒。最大值表示无限，也可以通过 **infinite** 关键字指定。默认值为 604800 （7 天）。
prefix-length	IPv6 前缀的长度。此值指示地址有多少个高阶相邻位用于构成前缀的网络部分。前缀长度前必须有斜线 (/)。
valid-lifetime	对指定的 IPv6 前缀进行通告的有效时间量 （以秒为单位）。有效值范围为 0 到 4294967295 秒。最大值表示无限，也可以通过 **infinite** 关键字指定。默认值为 2592000 （30 天）。

默认值

发出 IPv6 路由器通告的接口上配置的所有前缀均以 2592000 秒（30 天）的有效生命期和 604800 秒 （7 天）的首选生命期进行通告，并且两者均设置 “onlink” （在线）和 “autoconfig” （自动配置）标记。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令允许控制每个前缀的各个参数，包括是否应通告前缀。

默认情况下，使用 **ipv6 address** 命令配置为接口上的地址的前缀会在路由器通告中进行通告。如果使用 **ipv6 nd prefix** 命令配置用于通告的前缀，则仅通告这些前缀。

可以使用 **default** 关键字设置所有前缀的默认参数。

可以设置日期来指定前缀的到期日期。有效生命期和首选生命期均实时倒计时。达到到期日期时，将不再通告前缀。

当 onlink （在线）为 “ 开启 ” （默认情况）时，指定的前缀分配到该链路。向包含指定前缀的地址发送流量的节点会考虑链路上本地可达到的目的地。

当 autoconfig （自动配置）为 “ 开启 ” （默认情况）时，指示对于本地链路上的主机，指定的前缀可用于 IPv6 自动配置。

示例

以下示例将有效生命期为 1000 秒以及首选生命期为 900 秒的 IPv6 前缀 2001:200::/35 包含在通过指定接口发出的路由器通告中：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

相关命令

命令	说明
ipv6 address	配置 IPv6 地址，并在接口上启用 IPv6 处理。
show ipv6 interface	显示配置为 IPv6 的接口的可用性状态。

ipv6 nd ra-interval

要配置接口上的 IPv6 路由器通告传输的间隔，请在接口配置模式下使用 **ipv6 nd ra-interval** 命令。要恢复默认间隔，请使用此命令的 **no** 形式。

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

语法说明

msec	（可选）指示所提供的值以毫秒为单位。如果不提供此关键字，则所提供的值以秒为单位。
value	IPv6 路由器通告传输的间隔。有效值的范围为 3 到 1800 秒，或 500 到 1800000 毫秒 （如果提供 **msec** 关键字）。默认值为 200 秒。

默认值

200 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果 ASA 配置为默认路由器，则传输间隔应小于或等于使用 **ipv6 nd ra-lifetime** 命令配置的 IPv6 路由器通告生命期。为防止与其他 IPv6 节点同步，应将使用的实际值随机调整到指定值的 20% 范围内。

示例

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
```

相关命令

命令	说明
ipv6 nd ra-lifetime	配置 IPv6 路由器通告的生命期。
show ipv6 interface	显示配置为 IPv6 的接口的可用性状态。

ipv6 nd ra-lifetime

要配置接口上的 IPv6 路由器通告中的 “ 路由器生命期 ” 值，请在接口配置模式下使用 **ipv6 nd ra-lifetime** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

语法说明

seconds	ASA 作为此接口上的默认路由器的有效期。有效值范围为 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。

默认值

1800 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

“ 路由器生命期 ” 值包含在通过接口发出的所有 IPv6 路由器通告中。该值表示 ASA 作为此接口上的默认路由器的有效期。

将该值设置为非零值指示应将 ASA 视为此接口上的默认路由器。“ 路由器生命期 ” 值的非零值不应小于路由器通告间隔。

将该值设置为 0 表示不应将 ASA 视为此接口上的默认路由器。

示例

以下示例为所选接口配置 1801 秒的 IPv6 路由器通告生命期：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

相关命令

命令	说明
ipv6 nd ra-interval	配置接口上的 IPv6 路由器通告传输的间隔。
show ipv6 interface	显示配置为 IPv6 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 节点被视为可到达的时间量，请在接口配置模式下使用 **ipv6 nd reachable-time** 命令。要恢复默认时间，请使用此命令的 **no** 形式。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

语法说明

value	远程 IPv6 节点被视为可到达的时间量 （以毫秒为单位）。有效值范围为 0 至 3600000 毫秒。默认值为 0。 当 *value* 参数为 0 时，可到达时间以不确定值的形式发送。由接收设备设置和跟踪可到达时间值。

默认值

零毫秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入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。配置的时间越短，就越快启用检测不可用邻居；但是，时间越短，在所有 IPv6 网络设备中消耗的 IPv6 网络带宽和处理资源就越多。在正常 IPv6 操作中，不建议使用非常短的配置时间。

要查看 ASA 使用的可到达时间（包括此命令设置为 0 时的实际值），请使用 **show ipv6 interface** 命令显示有关 IPv6 接口的信息，其中包括正在使用的 ND 可到达时间。

示例

以下示例为所选接口配置 1700000 毫秒的 IPv6 可到达时间：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

相关命令

命令	说明
show ipv6 interface	显示配置为 IPv6 的接口的可用性状态。

ipv6 nd suppress-ra

要抑制 LAN 接口上的 IPv6 路由器通告传输，请在接口配置模式下使用 **ipv6 nd suppress-ra** 命令。要重新启用在 LAN 接口上发送 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

语法说明

此命令没有任何参数或关键字。

默认值

如果启用 IPv6 单播路由，则在 LAN 接口上自动发送路由器通告。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **no ipv6 nd suppress-ra** 命令启用在非 LAN 接口类型（例如串行接口或隧道接口）上 IPv6 路由器通告传输的发送。

示例

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
```

相关命令

命令	说明
show ipv6 interface	显示配置为 IPv6 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 **ipv6 neighbor** 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 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

语法说明

if_name	**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 （硬件 MAC）地址。

默认值

在 IPv6 邻居发现缓存中不配置静态条目。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

ipv6 neighbor 命令与 **arp** 命令相似。如果邻居发现缓存中已存在指定的 IPv6 地址的条目 （通过 IPv6 邻居发现过程了解），该条目会自动转换为静态条目。当使用 **copy** 命令存储配置时，这些条目存储在配置中。

使用 **show ipv6 neighbor** 命令可查看 IPv6 邻居发现缓存中的静态条目。

clear ipv6 neighbors 命令用于删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。 **no ipv6 neighbor** 命令用于从邻居发现缓存中删除指定的静态条目；该命令不会从缓存中删除动态条目（通过 IPv6 邻居发现过程了解的条目）。通过使用 **no ipv6 enable** 命令禁用接口上的 IPv6 将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，该条目的状态更改为 INCMP [未完成]）。

邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。

示例

以下示例将 IPv6 地址为 3001:1::45A 以及 MAC 地址为 0002.7D1A.9472 的内部主机的静态条目添加到邻居发现缓存：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

相关命令

命令	说明
clear ipv6 neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。
show ipv6 neighbor	显示 IPv6 邻居缓存信息。

ipv6 ospf

要启用用于 IPv6 的 OSPFv3 接口配置，请在全局配置模式下使用 **ipv6 ospf** 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** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

语法说明

cost	显式指定在接口上发送数据包的成本。
database-filter	过滤目的地为 OSPFv3 接口的传出 LSA。
dead-interval *seconds*	设置在邻居指示路由器关闭前不得出现问候数据包的时间段 （以秒为单位）。该值对于网络上的所有节点都必须相同，范围为 1 到 65535。默认值是 **ipv6 ospf hello-interval** 命令设置的间隔的四倍。
flood-reduction	指定目的地为接口的 LSA 泛洪削减。
hello-interval *seconds*	指定在接口上发送问候数据包的间隔 （以秒为单位）。该值对于特定网络上的所有节点都必须相同，范围为 1 到 65535。对于以太网接口，默认间隔为 10 秒；对于非广播接口，默认间隔为 30 秒。
mtu-ignore	在收到 DBD 数据包时，禁用 OSPF MTU 不匹配检测。默认情况下启用 OSPF MTU 不匹配检测。
neighbor	配置 OSPFv3 路由器与非广播网络的互连。
network	将 OSPF 网络类型设置为除默认类型以外的类型，具体取决于网络类型。
priority	设置路由器优先级，这有助于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 过程。有效值范围为 1 到 65535。
retransmit-interval *seconds*	指定属于接口的邻接关系的 LSA 重新传输间隔 （以秒为单位）。该时间必须晚于所连接的网络中任意两台路由器之间的预计往返延迟。有效值范围为 1 到 65535 秒。默认值为 5 秒。
transmit-delay *seconds*	设置在接口上发送链路状态更新数据包的估计时间 （以秒为单位）。有效值范围为 1 到 65535 秒。默认值为 1 秒。

默认值

默认情况下，包含所有 IPv6 地址。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

必须启用 OSPFv3 路由过程，才能创建 OSPFv3 区域。

示例

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf area

要创建用于 ipv6 的 OSPFv3 区域，请在全局配置模式下使用 **ipv6 ospf area** 命令。要禁用用于 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**]

语法说明

area-num	指定要启用的 OSPFv3 区域。
instance	指定要分配到接口的区域实例 ID。

默认值

默认情况下，包含所有 IPv6 地址。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

必须在每个接口上单独配置 OSPFv3 路由。一个接口只能有一个 OSPFv3 区域，用于 ASA 的 OSPFv3 对于每个接口只支持一个实例。每个接口都使用不同的区域实例 ID。区域实例 ID 只影响 OSPF 数据包的接收，适用于普通 OSPF 接口和虚拟链路。

示例

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf cost

要显式指定在接口上发送数据包的成本，请在接口配置模式下使用 **ipv6 ospf cost** 命令。要将在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*

语法说明

interface-cost	指定以链路状态指标表示的无符号整数值，范围为 1 到 65535。

默认值

默认成本基于带宽。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可显式指定接口的数据包成本。

示例

以下示例将数据包成本设置为 65：

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf database-filter all out

要过滤目的地为 OSPFv3 接口的传出 LSA，请在接口配置模式下使用 **ipv6 ospf databse-filter all out** 命令。要恢复 LSA 到接口的转发，请使用此命令的 **no** 形式。

ipv6 ospf database-filter all out

no ipv6 ospf database-filter all out

语法说明

此命令没有任何参数或关键字。

默认值

所有传出 LSA 均会泛洪到该接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可过滤目的地为 OSPFv3 接口的传出 LSA。

示例

以下示例过滤目的地为指定接口的传出 LSA：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf dead-interval

要设置在邻居宣告路由器关闭前不得出现问候数据包的时间段，请在接口配置模式下使用 **ipv6 ospf dead-interva** 命令。要恢复默认时间，请使用此命令的 **no** 形式。

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

语法说明

seconds	以秒为单位指定间隔。该值对于网络上的所有节点都必须相同。有效值范围为 1 到 65535。

默认值

默认值是 **ipv6 ospf hello-interval** 命令设置的间隔的四倍。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭前不得出现问候数据包的间隔。

示例

以下示例将停顿间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf encryption

要指定接口的加密类型，请在接口配置模式下使用 **ipv6 ospf encryption** 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** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

no ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

语法说明

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。
encryption-algorithm	指定要与 ESP 配合使用的加密算法。有效值包括以下值： • **aes-cdc** - 启用 AES-CDC 加密。 • **3des** - 启用 3DES 加密。 • **des** - 启用 DES 加密。 • **null** - 指定无加密的 ESP。
esp	指定封装安全负载 (ESP)。
ipsec	指定 IP 安全协议。
key	指定消息摘要计算中使用的编号。使用 MD5 身份验证时，密钥的长度必须是 32 个十六进制位 （16 字节）。使用 SHA-1 身份验证时，密钥的长度必须是 40 个十六进制位 （20 字节）。
key-encryption-type	（可选）指定密钥加密类型，它可以是以下值之一： • **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* 值必须是介于 256 到 4294967295 之间的十进制数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定接口的加密类型。

示例

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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf flood-reduction

要指定 LSA 到接口的泛洪削减，请在接口配置模式下使用 **ipv6 ospf flood-reduction** 命令。要取消 LSA 到接口的泛洪削减，请使用此命令的 **no** 形式。

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

语法说明

此命令没有任何参数或关键字。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定 LSA 到接口的泛洪削减。

示例

以下示例启用 LSA 到接口的泛洪削减：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf hello-interval

要设置在邻居宣告路由器关闭前不得出现问候数据包的时间段，请在接口配置模式下使用 **ipv6 ospf dead-interva** 命令。要恢复默认时间，请使用此命令的 **no** 形式。

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

语法说明

seconds	以秒为单位指定间隔。该值对于网络上的所有节点都必须相同。有效值范围为 1 到 65535。

默认值

如果使用以太网，默认间隔为 10 秒；如果使用非广播，默认间隔为 30 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭前不得出现问候数据包的间隔。

示例

以下示例将停顿间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的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 最大传输单位 (MTU) 不匹配检测，请在接口配置模式下使用 **ipv6 ospf mtu-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

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用 OSPFv3 MTU 不匹配检测。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可在 ASA 接收 DBD 数据包时禁用 OSPFv3 MTU 不匹配检测。

示例

以下示例显示在 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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6 ospf neighbor

要为非广播网络配置 OSPFv3 路由器互连，请在接口配置模式下使用 **ipv6 ospf neighbor** 命令。要删除配置，请使用此命令的 **no** 形式。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

语法说明

cost *number*	（可选）向邻居分配整数形式 （1 到 65535）的成本。未配置特定成本的邻居将采用基于 **ipv6 ospf cost** 命令的接口成本。
database-filter	（可选）过滤目的地为 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。此参数必须是 RFC 2373 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
poll-interval *seconds*	（可选）表示轮询间隔时间的数值 （以秒为单位）。 RFC 2328 建议此值远大于问候间隔。默认值为 120 秒 （两分钟）。此关键字不适用于 “ 点对多点 ” 接口。
priority *number*	（可选）一个数字，指示与指定的 IPv6 前缀相关联的非广播邻居的路由器优先级值。默认值为 0。

默认值

默认值取决于网络类型。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可配置与非广播网络的 OSPFv3 路由器互连。

示例

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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
ipv6 ospf priority	确定指定网络的指定路由器。

ipv6 ospf network

要将 OSPFv3 网络类型配置为除默认类型以外的类型，请在接口配置模式下使用 **ipv6 ospf network** 命令。要恢复默认类型，请使用此命令的 **no** 形式。

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

no ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

语法说明

broadcast	设置要广播的网络类型。
point-to-point non-broadcast	将网络类型设置为点对点非广播。

默认值

默认值取决于网络类型。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可将 OSPFv3 网络类型配置为不同于默认类型的类型。

示例

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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
ipv6 ospf priority	确定指定网络的指定路由器。

ipv6 ospf priority

要设置路由器优先级 （帮助确定指定网络的指定路由器），请在接口配置模式下使用 **ipv6 ospf priority** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ipv6 ospf priority *number-value*

no ipv6 ospf priority *number-value*

语法说明

number-value	设置指定路由器优先级的数值。有效值范围为 0 到 255。

默认值

默认优先级为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可设置路由器的优先级。

示例

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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
ipv6 ospf retransmit-interval	指定属于接口的邻接关系的 LSA 重新传输的间隔。

ipv6 ospf retransmit-interval

要指定属于接口的邻接关系的 LSA 重新传输的间隔，请在接口配置模式下使用 **ipv6 ospf retransmit-interval** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval *seconds*

语法说明

seconds	指定重新传输的间隔 （以秒为单位）。该间隔必须大于所连接的网络中任意两台路由器之间的预计往返延迟。有效值范围为 1 到 65535 秒。

默认值

默认值为 5 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可指定属于接口的邻接关系的 LSA 重新传输的间隔。

示例

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
```

相关命令

命令	说明
ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
ipv6 ospf priority	确定指定网络的指定路由器。

ipv6 ospf transmit-delay

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 **ipv6 ospf transmit-delay** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay *seconds*

语法说明

seconds	指定发送链路状态更新所需的时间 （以秒为单位）。有效值范围为 1 到 65535 秒。

默认值

默认值为 1 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

使用此命令可设置在接口上发送链路状态更新数据包所需的估计时间。

示例

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
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
ipv6 ospf priority	确定指定网络的指定路由器。

ipv6 route

要向 IPv6 路由表添加 IPv6 路由，请在全局配置模式下使用 **ipv6 route** 命令。要删除 IPv6 默认路由，请使用此命令的 **no** 形式。

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

语法说明

administrative-distance	（可选）路由的管理距离。默认值为 1，这使得静态路由优先于除已连接路由以外的任何其他类型的路由。
if_name	要配置路由的接口的名称。
ipv6-address	可用于到达指定网络的下一跳的 IPv6 地址。
ipv6-prefix	作为静态路由目的地的 IPv6 网络。 此参数必须是 RFC 2373 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
prefix-length	IPv6 前缀的长度。此值指示地址有多少个高阶相邻位用于构成前缀的网络部分。前缀长度前必须有斜线 (*/*)。
tunneled	（可选）指定作为 VPN 流量的默认隧道网关的路由。

默认值

默认情况下，管理距离为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(1)	引入了对透明防火墙模式的支持。

使用指南

使用 **show ipv6 route** 命令可查看 IPv6 路由表的内容。

除了标准默认路由以外，您可以定义用于隧道流量的单独默认路由。使用 **tunneled** 选项创建默认路由后，来自 ASA 上终止隧道的所有流量 （无法使用已获知或静态路由进行路由）都将发送到此路由。对于来自隧道的新兴流量，此路由将覆盖任何其他已配置或已获知的默认路由。

以下限制适用于具有 **tunneled** 选项的默认路由：

- 不要在隧道路由的 Egress 接口上启用单播 RPF （**ip verify reverse-path** 命令）。在隧道路由的传出接口上启用 uRPF 将导致会话失败。
- 不要在隧道路由的 Egress 接口上启用 TCP 截取。这样做会导致会话失败。
- 不要将 VoIP 检查引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP 或 SKINNY）、DNS 检查引擎或 DCE RPC 检查引擎与隧道路由一起使用。这些检查引擎将忽略隧道路由。

您无法通过 **tunneled** 选项定义多个默认路由；不支持对隧道流量使用 ECMP。

示例

以下示例将网络 7fff::0/32 的数据包路由到地址为 3FFE:1100:0:CC00::1、管理距离为 110 的内部接口上的网络设备：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

相关命令

命令	说明
debug ipv6 route	显示 IPv6 路由表更新和路由缓存更新的调试消息。
show ipv6 route	显示 IPv6 路由表的当前内容。

ipv6 router ospf

要创建 OSPFv3 路由过程并进入 IPv6 路由器配置模式，请在全局配置模式下使用 **ipv6 router ospf** 命令。

ipv6 router ospf *process-id*

语法说明

process-id	指定内部标识，该标识本地分配，可以是从 1 到 65535 的正整数。所用编号是您在为 IPv6 路由过程启用 OSPFv3 时管理性分配的编号。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

ipv6 router ospf 命令是在 ASA 上运行的 OSPFv3 路由过程的全局配置命令。当输入 **ipv6 router ospf** 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。

当使用 **no ipv6 router ospf** 命令时，无需指定可选参数，除非这些参数提供必需信息。 **no ipv6 router ospf** 命令将终止其 *process-id* 参数指定的 OSPFv3 路由过程。您在 ASA 上本地分配 *process-id* 值。必须为每个 OSPFv3 路由过程分配唯一值。最多可以使用两个过程。

在 IPv6 路由器配置模式下使用 **ipv6 router ospf** 命令可通过以下特定于 OSPFv3 的选项配置 OSPFv3 路由过程：

- **area** - 配置 OSPFv3 区域参数。支持的参数包括从 0 到 4294967295 的十进制值形式的区域 ID 以及 **A.B.C.D** IP 地址格式的区域 ID。
- **default** - 将命令设置为其默认值。 **originate** 参数分布默认路由。
- **default-information** - 控制默认信息的分布。
- **distance** - 根据路由类型定义 OSPFv3 路由管理距离。支持的参数包括值为 1 到 254 的管理距离以及表示 OSPF 距离的 **ospf**。
- **exit -** 退出 IPv6 路由器配置模式。
- **ignore** - 当路由器接收类型 6 组播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，通过 **lsa** 参数抑制系统日志消息的发送。

- **log-adjacency-changes** - 将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息。如指定 **detail** 参数，将记录所有状态变化。
- **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** - 按照以下参数配置路由从一个路由域到另一个路由域的重分布。
  - **connected** - 指定连接的路由。
  - **ospf** - 指定 OSPF 路由。
  - **static** - 指定静态路由。
- **router-id** - 通过以下参数为指定过程创建固定的路由器 ID：
  - **A.B.C.D** - 指定 IP 地址格式的 OSPF 路由器 ID。
  - **cluster-pool** - 在配置第 3 层集群后配置 IP 地址池。
- **summary-prefix** - 将 IPv6 地址汇总配置为 0 到 128 的有效值。**X:X:X:X::X/** 参数指定 IPv6 前缀。
- **timers** - 通过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 限制计时器。

示例

以下示例启用 OSPFv3 路由过程，并进入 IPv6 路由器配置模式：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

相关命令

命令	说明
clear ipv6 ospf	删除 OSPFv3 路由过程中的所有 IPv6 设置。
debug ospfv3	为 OSPFv3 路由过程的故障排除提供调试信息。

ipv6-address-pool （隧道组常规属性模式）

要指定 IPv6 地址池的列表以为远程客户端分配地址，请在隧道组常规属性配置模式下使用 **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_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

语法说明

interface_name	（可选）指定要用于地址池的接口。
ipv6_address_pool	指定使用 **ipv6 local pool** 命令配置的地址池的名称。最多可以指定 6 个本地地址池。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

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

组策略 **ipv6-address-pools** 命令中的 IPv6 地址池设置将覆盖隧道组 **ipv6-address-pool** 命令中的 IPv6 地址池设置。

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

示例

以下示例在隧道组常规属性配置模式下输入，指定 IPv6 地址池的列表为远程客户端分配地址，以进行 IPsec 远程访问隧道组测试：

```
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)#
```

相关命令

命令	说明
ipv6-address-pools	配置组策略的 IPv6 地址池设置，该设置将覆盖隧道组中的相应设置。
ipv6 local pool	配置将用于 VPN 远程访问隧道的 IP 地址池。
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group	配置隧道组。

ipv6-address-pools

要指定用于向远程客户端分配地址的最多 6 个 IPv6 地址池的列表，请在组策略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允许从组策略的其他来源继承，请使用此命令的 **no** 形式。

ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

ipv6-address-pools none

no ipv6-address-pools none

语法说明

ipv6_address_pool	指定使用 **ipv6 local pool** 命令配置的最多 6 个 IPv6 地址池的名称。使用空格分隔 IPv6 地址池名称。
none	指定不配置任何 IPv6 地址池，并禁止从组策略的其他来源继承。
value	指定要用于分配地址的最多 6 个 IPv6 地址池的列表。

默认值

默认情况下， IPv6 地址池属性未配置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要配置 IPv6 地址池，请使用 **ipv6 local pool** 命令。

在 **ipv6-address-pools** 命令中指定池的顺序非常重要。 ASA 以这些池在此命令中出现的顺序分配这些池中的地址。

ipv6-address-pools none 命令将禁止此属性从其他策略来源（如 DefaultGrpPolicy）继承。 **no ipv6-address-pools none** 命令将从配置中删除 **ipv6-address-pools none** 命令，从而恢复默认值（允许继承）。

示例

以下示例在组策略属性配置模式下输入，用于配置一个名为 firstipv6pool 的 IPv6 地址池以供向远程客户端分配地址之用，然后将该池与 GroupPolicy1 相关联：

```
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)#
```

相关命令

命令	说明
ipv6 local pool	配置将用于 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	显示所有组策略的配置或特定组策略的配置。

ipv6-split-tunnel-policy

要设置 IPv6 拆分隧道策略，请在组策略配置模式下使用 **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

语法说明

excludespecified	定义流量可不受阻碍进入的网络的列表。若用户想要通过隧道连接到公司网络来访问本地网络上的设备 （如打印机），此功能非常有用。
ipv6-split-tunnel-policy	指示您正在设置隧道流量的规则。
tunnelall	指定没有流量可以不受阻碍地进入或到达 ASA 以外的任何其他目的地。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	将所有来自或流向指定网络的流量隧道化。此选项启用拆分隧道。可以让您创建要隧道化的地址的网络列表。数据不受阻碍地传送到所有其他地址，并由远程用户的互联网运营商进行路由。

默认值

默认情况下，禁用 IPv6 拆分隧道，即 **tunnelall**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

IPv6 拆分隧道主要是一个流量管理功能，而不是安全功能。事实上，为获得最优安全性，建议不要启用 IPv6 拆分隧道。

这允许从其他组策略继承 IPv6 拆分隧道的值。

IPv6 拆分隧道可以让远程访问 VPN 客户端有条件地通过 IPsec 或 SSL IPv6 隧道以加密形式传送数据包，或以明文形式将数据包传送到网络接口。启用 IPv6 拆分隧道时，若数据包不以另一侧 IPsec 或 SSL VPN 隧道终端为目的地，则不必加密、通过隧道发送、解密以及路由到最终目的地。

此命令将 IPv6 拆分隧道策略应用到特定网络。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置仅指定隧道的网络的拆分隧道策略：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

相关命令

命令	说明
split-tunnel-network-list none	指示不存在用于拆分隧道的访问列表。所有流量均通过隧道传输。
split-tunnel-network-list value	确定 ASA 用来区分需要和不需要隧道的网络的访问列表。

ipv6-vpn-address-assign

要指定为远程访问客户端分配 IPv6 地址的方法，请在全局配置模式下使用 **ipv6-vpn-addr-assign** 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** }

语法说明

aaa	ASA 从外部或内部 （本地） AAA （身份验证、授权和记账）服务器为每个用户检索地址。如果您使用已配置 IP 地址的身份验证服务器，建议使用此方法。
local	ASA 从内部配置的地址池分配 IPv6 地址。

默认值

默认情况下， AAA 和本地 vpn 地址分配选项均启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

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 地址为止。

示例

以下示例显示如何将 AAA 配置为地址分配方法。

示例：

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

以下示例显示如何为地址分配方法配置本地地址池的使用。

示例：

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

相关命令

命令	说明
ipv6 local pool	配置将用于 VPN 组策略的 IPv6 地址池。
show running-config group-policy	显示所有组策略的配置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，请在组策略配置模式或用户名配置模式下使用 **ipv6-vpn-filter** 命令。要删除 ACL （包括通过发出 **ipv6-vpn-filter none** 命令而创建的空值），请使用此命令的 **no** 形式。

ipv6-vpn-filter {**value** *IPV6-ACL-NAME* | **none**}

no ipv6-vpn-filter

语法说明

none	指示没有访问列表。设置一个空值，从而禁止访问列表。防止从其他组策略继承访问列表。
value *IPV6-ACL-NAME*	提供先前配置的访问列表的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	**ipv6-vpn-filter** 命令已废弃。应使用 **vpn-filter** 命令配置 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，才使用此 IPv6 过滤器。
9.1(4)	**ipv6-vpn-filter** 命令已禁用，只允许使用此命令的 “no” 形式。应使用 **vpn-filter** 命令配置 IPv4 和 IPv6 条目的统一过滤器。如果错误地使用此命令指定 IPv6 ACL，连接将被终止。

使用指南

无客户端 SSL VPN 不使用 **ipv6-vpn-filter** 命令中定义的 ACL。

no 选项允许继承其他组策略的值。要防止继承值，请使用 **ipv6-vpn-filter none** 命令。

您配置 ACL 来为此用户或组策略允许或拒绝各种类型的流量。然后使用 **ipv6-vpn-filter** 命令应用这些 ACL。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置可调用名为 ipv6_acl_vpn 的访问列表的过滤器。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipv6-vpn-filter value ipv6_acl_vpn
```

相关命令

命令	说明
access-list	创建访问列表，或使用可下载访问列表。
vpn-filter	指定将用于 VPN 连接的 IPv4 或 IPv6 ACL 的名称。

第 5 章

isakmp am-disable 至 issuer-name 命令

isakmp am-disable

要禁用入站积极模式连接，请在全局配置模式下使用 **isakmp am-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

语法说明

此命令没有任何参数或关键字。

默认值

默认值为启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp am-disable** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，禁用入站积极模式连接：

```
ciscoasa(config)# isakmp am-disable
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp disconnect-notify

要启用面向对等项的断开连接通知，请在全局配置模式下使用 **isakmp disconnect-notify** 命令。要禁用断开连接通知，请使用此命令的 **no** 形式。

isakmp disconnect-notify

no isakmp disconnect-notify

语法说明

此命令没有任何参数或关键字。

默认值

默认值为禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp disconnect-notify** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，启用面向对等项的断开连接通知：

```
ciscoasa(config)# isakmp disconnect-notify
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp enable

要在用于 IPsec 对等项与 ASA 进行通信的接口上启用 ISAKMP 协商，请在全局配置模式下使用 **isakmp enable** 命令。要在接口上禁用 ISAKMP，请使用此命令的 **no** 形式。

isakmp enable *interface-name*

no isakmp enable *interface-name*

语法说明

interface-name	指定要启用或禁用 ISAKMP 协商的接口的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp enable** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，显示如何在内部接口上禁用 ISAKMP：

```
ciscoasa(config)# no isakmp enable inside
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp identity

要设置将发送到对等项的阶段 2 ID，请在全局配置模式下使用 **isakmp identity** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

语法说明

address	使用交换 ISAKMP 身份信息的主机的 IP 地址。
auto	通过连接类型、预共享密钥的 IP 地址或用于证书身份验证的证书 DN 确定 ISKMP 协商。
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*	指定远程对等项用来查找预共享密钥的字符串。

默认值

默认 ISAKMP 身份为 **isakmp identity hostname** 命令。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp identity** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，它根据连接类型，在用于与 IPsec 对等项通信的接口上启用 ISAKMP 协商：

```
ciscoasa(config)# isakmp identity auto
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp ipsec-over-tcp

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 IPsec over TCP，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*]

语法说明

port *port1...port10*	（可选）指定设备接受 IPsec over TCP 连接的端口。最多可列出 10 个端口。端口号可以在 1 到 65535 的范围内。默认端口号为 10000。

默认值

默认值为禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp ipsec-over-tcp** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，在端口 45 上启用 IPsec over TCP：

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp keepalive

要配置 IKE 保持连接，请在隧道组 ipsec 属性配置模式下使用 **isakmp keepalive** 命令。要将 keepalive 参数恢复为以默认的阈值和重试间隔值启用，请使用此命令的 **no** 形式。

isakmp keepalive [threshold *seconds* **| infinite] [retry** *seconds] [***disable]**

no isakmp keepalive disable [threshold *seconds* **| infinite] [retry** *seconds] [***disable]**

语法说明

disable	禁用 IKE 保持连接处理，该处理默认为启用。
infinite	ASA 从不发起保持连接监控。
retry *seconds*	指定在未收到保持连接响应后重试的间隔 （以秒为单位）。范围为 2-10 秒。默认值为 2 秒。
threshold *seconds*	指定在开始保持连接监控之前对等项可以空闲的秒数。范围为 10-3600 秒。对于 LAN 到 LAN 组，默认值为 10 秒；对于远程访问组，默认值为 300 秒。

默认值

远程访问组的默认值为 300 秒的阈值和 2 秒的重试间隔。

对于 LAN 到 LAN 组，默认值为 10 秒的阈值和 2 秒的重试间隔。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在每个隧道组中， IKE 保持连接默认都以默认的阈值和重试间隔值启用。可以仅将此属性应用于 IPsec 远程访问和 IPsec LAN 到 LAN 隧道组类型。

示例

以下示例在隧道组 ipsec 属性配置模式下输入，为 IP 地址为 209.165.200.225 的 IPsec LAN 到 LAN 隧道组配置 IKE DPD、建立阈值 15 并指定重试间隔为 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)#
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置此组的隧道组 IPsec 属性。

isakmp nat-traversal

要全局启用 NAT 穿越，请确认已在全局配置模式下启用 ISAKMP（可以使用 **isakmp enable** 命令启用），然后使用 **isakmp nat-traversal** 命令。如果已启用 NAT 穿越，则可以使用此命令的 **no** 形式将其禁用。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

语法说明

natkeepalive	设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

默认值

默认情况下，禁用 NAT 穿越 （**isakmp nat-traversal** 命令）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp nat-traversal** 命令取代了此命令。

使用指南

在许多使用 IPsec 的网络中也同时使用网络地址转换 (NAT) （包括端口地址转换 (PAT)），但有大量不兼容因素阻止 IPsec 数据包成功穿越 NAT 设备。 NAT 穿越使 ESP 数据包可通过一个或多个 NAT 设备。

ASA 支持 NAT 穿越，如 IETF“UDP Encapsulation of IPsec Packets” （IPsec 数据包的 UDP 封装）草案的第 2 版和第 3 版 （可在 http://www.ietf.org/html.charters/ipsec-charter.html 下载）所述，并且动态和静态加密映射均支持 NAT 穿越。

此命令在 ASA 上全局启用 NAT-T。要在加密映射条目中禁用，请使用 **crypto map set nat-t-disable** 命令。

示例

以下示例在全局配置模式下输入，先启用 ISAKMP，再启用间隔为 30 秒的 NAT 穿越：

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp policy authentication

要在 IKE 策略内指定身份验证方法，请在全局配置模式下使用 **isakmp policy authentication** 命令。要删除 ISAKMP 身份验证方法，请使用 **clear configure** 命令。

isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

语法说明

crack	指定对已经过身份验证的加密密钥的 IKE 质询 / 响应 (CRACK) 为身份验证方法。
pre-share	指定预共享密钥为身份验证方法。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数， 1 表示最高优先级， 65534 表示最低优先级。
rsa-sig	指定 RSA 签名为身份验证方法。 RSA 签名提供 IKE 协商的不可否认性。这意味着您可以向第三方证明您是否已与对等项进行 IKE 协商。

默认值

默认的 ISAKMP 策略身份验证为 **pre-share** 选项。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

IKE 策略定义一组用于 IKE 协商的参数。如果指定 RSA 签名，则必须将 ASA 及其对等项配置为从证书颁发机构 (CA) 获取证书。如果指定预共享密钥，则必须在 ASA 及其对等项内单独配置这些预共享密钥。

示例

以下示例在全局配置模式下输入，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
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp policy encryption

要指定将在 IKE 策略中使用的加密算法，请在全局配置模式下使用 **isakmp policy encryption** 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 policy *priority* **encryption** {**aes** | **aes-192**| **aes-256** | **des** | **3des**}

no isakmp policy *priority* **encryption** {**aes** | **aes-192**| **aes-256** | **des** | **3des**}

语法说明

3des	指定在 IKE 策略中使用三重 DES 加密算法。
aes	指定将在 IKE 策略中使用的加密算法为带 128 位密钥的 AES。
aes-192	指定将在 IKE 策略中使用的加密算法为带 192 位密钥的 AES。
aes-256	指定将在 IKE 策略中使用的加密算法为带 256 位密钥的 AES。
des	指定将在 IKE 策略中使用的加密算法为 56 位 DES-CBC。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数， 1 表示最高优先级， 65534 表示最低优先级。

默认值

默认 ISAKMP 策略加密算法为 **3des**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp policy encryption** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，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输入，设置将在优先级编号为 40 的 IKE 策略中使用 3DES 算法：

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp policy group

要为 IKE 策略指定 Diffie-Hellman 组，请在全局配置模式下使用 **isakmp policy group** 命令。要将 Diffie-Hellman 组标识符重置为默认值，请使用此命令的 **no** 形式。

isakmp policy *priority* **group** {**1** | **2** | **5**}

no isakmp policy *priority* **group**

语法说明

group 1	指定在 IKE 策略中使用 768 位 Diffie-Hellman 组。此值为默认值。
group 2	指定在 IKE 策略中使用 1024 位 Diffie-Hellman 组 2。
group 5	指定在 IKE 策略中使用 1536 位 Diffie-Hellman 组 5。
priority	唯一标识互联网密钥交换 (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。

默认值

默认为组 2。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。增加了组 7。
7.2(1)	此命令已弃用。 **crypto isakmp policy group** 命令取代了此命令。
8.0(4)	**group 7** 命令选项已废弃。尝试配置组 7 将生成一条错误消息，并改用组 5。

使用指南

IKE 策略定义一组在 IKE 协商期间使用的参数。

有三个组选项：768 位（DH 组 1）、1024 位（DH 组 2）和 1536 位（DH 组 5）。1024 位和 1536 位 Diffie-Hellman 组提供更强的安全性，但需要更多 CPU 时间来执行。

注　思科 VPN 客户端版本 3.x 或更高版本需要 ISAKMP 策略才能配置 DH 组 2。（如果已配置 DH 组 1，思科 VPN 客户端无法连接。）

只有授权使用 VPN-3DES 的 ASA 提供 AES 支持。由于 AES 提供大型密钥，ISAKMP 协商应使用 Diffie-Hellman (DH) 组 5，而不是组 1 或组 2。这通过 **isakmp policy priority group 5** 命令完成。

示例

以下示例在全局配置模式下输入，设置将在优先级编号为 40 的 IKE 策略中使用组 2 （1024 位 Diffie Hellman）：

```
ciscoasa(config)# isakmp policy 40 group 2
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp policy hash

要指定 IKE 策略的散列算法，请在全局配置模式下使用 **isakmp policy hash** 命令。要将散列算法重置为默认值 SHA-1，请使用此命令的 **no** 形式。

isakmp policy *priority* **hash** {**md5** | **sha**}

no isakmp policy *priority* **hash**

语法说明

md5	指定将 MD5 （HMAC 变体）用作 IKE 策略中的散列算法。
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。

默认值

默认散列算法为 SHA-1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp policy hash** 命令取代了此命令。

使用指南

IKE 策略定义一组将在 IKE 协商期间使用的参数。

有两个散列算法选项：SHA-1 和 MD5。 MD5 的摘要较小，被认为略快于 SHA-1。

示例

以下示例在全局配置模式下输入，指定将在优先级编号为 40 的 IKE 策略中使用 MD5 散列算法：

```
ciscoasa(config)# isakmp policy 40 hash md5
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp policy lifetime

要指定 IKE 安全关联到期之前的生命期，请在全局配置模式下使用 **isakmp policy lifetime** 命令。要将安全关联生命期重置为默认值 86,400 秒 （一天），请使用此命令的 **no** 形式。

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

语法说明

priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数， 1 表示最高优先级， 65534 表示最低优先级。
seconds	指定每个安全关联在到期之前应存在多少秒。要设置有限生命期，请使用介于 120 到 2147483647 之间的整数秒。要设置无限生命期，请使用 0 秒。

默认值

默认值为 86,400 秒 （一天）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp policy lifetime** 命令取代了此命令。

使用指南

IKE 开始协商时，会寻求使其自身对话的安全参数达成一致。然后每个对等项的安全关联都会参考达成一致的参数。对等项会保留安全关联，直到生命期到期。安全关联到期之前，后续 IKE 协商可以使用它，这可以在设置新 IPsec 安全关联时节省时间。在当前安全关联到期之前，对等项将协商新的安全关联。

生命期越长， ASA 设置将来 IPsec 安全关联的速度就越快。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间 （大约每隔几分钟再生一次）。建议您接受默认设置，但如果对等项未设置生命期，您可以指定无限生命期。

注　如果 IKE 安全关联设置为无限生命期，但对等项提出有限生命期，则使用与对等项协商的有限生命期。

示例

以下示例在全局配置模式下输入，将优先级编号为 40 的 IKE 策略中的 IKE 安全关联的生命期设置为 50,400 秒 （14 小时）：

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

以下示例在全局配置模式下输入，将 IKE 安全关联设置为无限生命期。

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

isakmp reload-wait

要允许在重新启动 ASA 之前等待所有活动会话自行终止，请在全局配置模式下使用 **isakmp reload-wait** 命令。要禁止等待活动会话终止并继续重新启动 ASA，请使用此命令的 **no** 形式。

isakmp reload-wait

no isakmp reload-wait

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	此命令已弃用。 **crypto isakmp reload-wait** 命令取代了此命令。

示例

以下示例在全局配置模式下输入，告知 ASA 等待至所有活动会话均终止后再重新启动：

```
ciscoasa(config)# isakmp reload-wait
```

相关命令

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 SA 数据库。
show running-config isakmp	显示所有活动的配置。

issuer

要指定向 SAML 类型的 SSO 服务器发送声明的安全设备，请在 webvpn-sso-saml 配置模式下针对该特定 SAML 类型使用 **issuer** 命令。要删除签发方名称，请使用此命令的 **no** 形式。

issuer *identifier*

no issuer [*identifier*]

语法说明

identifier	指定安全设备名称，通常为设备的主机名。标识符必须少于 65 个字母数字字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Webvpn-sso-saml 配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

SSO 支持 （仅针对 WebVPN 提供）可让用户在不同的服务器上访问不同的安全服务，无需多次输入用户名和密码。ASA 当前支持 SAML POST 类型的 SSO 服务器和 SiteMinder 类型的 SSO 服务器。

此命令仅适用于 SAML 类型的 SSO 服务器。

示例

以下示例指定名为 asa1.example.com 的安全设备的签发方名称：

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

相关命令

命令	说明
assertion-consumer-url	指定安全设备用来与 SAML 类型的 SSO 服务器声明消费者服务进行联系的 URL。
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。
trustpoint	指定信任点名称，其中包含用于签署 SAML 类型浏览器声明的证书。

issuer-name

要指定所有已签发证书的签发方名称 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。要删除证书颁发机构证书的主题 DN，请使用此命令的 **no** 形式。

issuer-name *DN-string*

no issuer-name *DN-string*

语法说明

DN-string	指定证书的可分辨名称，这也是自签 CA 证书的主题名称 DN。使用逗号分隔属性值对。插入引号括起任何包含逗号的值。签发方名称必须少于 500 个字母数字字符。

默认值

默认签发方名称为 cn=*hostame.domain-name*，例如 cn=asa.example.com。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.3(1)	引入了此命令。
8.0(2)	增加了对引号的支持以保留 *DN-string* 值中的逗号。

使用指南

此命令指定在本地 CA 服务器创建的任何证书上显示的签发方名称。如果您希望签发方名称与默认 CA 名称不同，请使用此可选命令。

注　在通过发出 **no shutdown** 命令启用 CA 服务器并生成证书后，无法更改此签发方名称配置。

示例

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)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令的访问，从而允许您配置和管理本地 CA。
keysize	指定在证书注册时生成的公用密钥和私有密钥的大小。
lifetime	指定 CA 证书和已签发证书的生命期。
show crypto ca server	显示本地 CA 的特性。
show crypto ca server cert-db	显示本地 CA 服务器证书。

第 2 部分

J 至 M 命令

java-trustpoint 至 kill 命令

java-trustpoint

要将 WebVPN Java 签名设施配置为使用来自指定信任点位置的 PKCS12 证书和密钥内容，请在 webvpn 配置模式下使用 **java-trustpoint** 命令。要删除用于 Java 对象签名的信任点，请使用此命令的 **no** 形式。

java-trustpoint *trustpoint*

no java-trustpoint

语法说明

trustpoint	指定由 **crypto ca import** 命令配置的信任点位置。

默认值

默认情况下，用于 Java 对象签名信任点设置为 “ 无 ”。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(2)	引入了此命令。

使用指南

信任点是对证书颁发机构 (CA) 或身份密钥对的表示。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、对应于该证书的 RSA 专用密钥以及扩展到根 CA 的证书颁发机构链。这通常是通过使用 **crypto ca import** 命令导入 PKCS12 格式化捆绑包来实现的。可以从可信 CA 机构获取 PKCS12 捆绑包，或者使用开源工具 （例如 openssl）根据现有 X.509 证书或 RSA 专用密钥手动创建。

注　上传的证书不能用于对连同程序包 （例如 CSD 包）一起嵌入的 Java 对象进行签名。

示例

以下示例首先配置一个新的信任点，然后将其配置为用于 WebVPN Java 对象签名：

```
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)#
```

以下示例将新的信任点配置为用于 WebVPN Java 对象签名：

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

相关命令

命令	说明
crypto ca import	使用 PKCS12 数据为信任点导入证书和密钥对。

join-failover-group

要向故障切换组分配情景，请在情景配置模式下使用 **join-failover-group** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

join-failover-group *group_num*

no join-failover-group *group_num*

语法说明

group_num	指定故障切换组编号。

默认值

故障切换组 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

管理情景始终分配给故障切换组 1。可以使用 **show context detail** 命令来显示故障切换组与情景之间的关联。

必须使用 **failover group** 命令在系统情景中创建故障切换组后，才能向其分配情景。在情景处于活动状态的设备上输入此命令。默认情况下，未分配的情景都是故障切换组 1 的成员，因此，如果之前未向故障切换组分配情景，应该在故障切换组 1 处于活动状态的设备上输入此命令。

要从系统删除某个故障切换组，必须先使用 **no join-failover-group** 命令从该故障切换组删除所有情景。

示例

以下示例将名为 ctx1 的情景分配给故障切换组 2：

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

相关命令

命令	说明
context	进入指定情景的情景配置模式。
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
show context detail	显示情景详细信息，包括名称、类、接口、故障切换组关联和配置文件 URL。

jumbo-frame reservation

要对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　如果更改了此设置，需要重新启动 ASA。

jumbo-frame reservation

no jumbo-frame reservation

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，巨帧预留功能处于禁用状态。

默认情况下， ASASM 支持巨帧；不需要使用此命令。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.1(1)	针对 ASA 5580 引入了此命令。
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。

使用指南

巨帧是指大于标准最大字节数 （1518 字节）（包括第 2 层标头和 FCS）的以太网数据包，最多包含 9216 字节。支持巨帧需要额外内存，这可能会导致其他功能 （例如，访问列表）无法得到最充分利用。

管理 *n*/*n* 接口不支持巨帧。

请务必将需要传输巨帧的每个接口的 MTU 设置为高于默认值 1500 ；例如，使用 **mtu** 命令将此值设置为 9000。对于 ASASM，不需要设置 **jumbo-frame** 预留命令；它默认情况下支持巨帧。只需将 MTU 设置为所需的值。

此外，使用巨帧时，请务必为 TCP 配置 MSS （最大分段大小）值。 MSS 应该比 MTU 少 120 字节。例如，如果将 MTU 配置为 9000，则 MSS 应配置为 8880。可以使用 **sysopt connection tcpmss** 命令来配置 MSS。

设置后，主设备和辅助设备都需要重新启动，以使故障切换对支持巨帧。为避免停机时间，请执行以下操作：

- 在主用设备上发出命令。
- 在主用设备上保存运行配置。
- 同时重新启动主设备和辅助设备。

示例

以下示例启用巨帧预留，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
```

相关命令

命令	说明
mtu	指定接口的最大传输单位。
show jumbo-frame reservation	显示 **jumbo-frame reservation** 命令的当前配置。

kcd-server

要允许 ASA 加入 Active Directory 域，请在 webvpn 配置模式下使用 **kcd-server** 命令。要删除 ASA 的指定行为，请使用此命令的 **no** 形式。

kcd-server *aaa-server-group_name* **user** *username* **password** *password*

no kcd-server

语法说明

用户	指定具有服务级别权限的 Active Directory 用户。
password	指定特定用户的密码。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。

使用指南

可通过在 webvpn 配置模式下使用 **kcd-server** 命令来允许 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，但应该对应于在域控制器上具有服务级别权限的用户。成功或失败状态将显示为此命令的结果。还可以使用 **show webvpn kcd** 命令查看结果。

ASA 环境中的约束委派 (KCD) 为 WebVPN 用户提供对受到 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），并使用该服务票证对服务的用户进行身份验证。

为了使 **kcd-server** 命令起作用， ASA 必须在*源*域（ASA 所在的域）与*目标*或*资源*域（Web 服务所在的域）之间建立信任关系。 ASA 使用其独特格式使认证路径从源域跨越到目标域，并代表远程访问用户获取访问服务所需的票证。

这个过程称为跨领域身份验证。在跨领域身份验证的每个阶段， ASA 都依赖于特定域上的凭证以及与后续域之间的信任关系。

要将 ASA 配置为进行跨领域身份验证，必须使用以下命令以加入到 Active Directory 域：**ntp**、**hostname**、 **dns domain-lookup**、 **dns server-group**。

示例

以下示例显示 **kcd-server** 命令的用法：

```
ciscoasa(config)# aaa-server kcd-grp protocol kerberos
ciscoasa(config-aaa-server-group)# aaa-server kcd-grp host DC
ciscoasa(config-aaa-server-group)# kerberos-realm EXAMPLE.COM
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server kcd-grp user Administrator password Cisco123
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

以下是跨领域身份验证的一个配置示例，其中域控制器是 10.1.1.10 （可通过内部接口访问），域名是 PRIVATE.NET。此外，域控制器上服务帐户的用户名和密码分别是 dcuser 和 dcuser123!.

```
ciscoasa(config)# config t

-----Create an alias for the Domain Controller-------------

ciscoasa(config)# name 10.1.1.10 DC

----Configure the Name server-------------------------------

ciscoasa(config)# ntp server DC

----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 DC
ciscoasa(config-dns-server-group)# domain-name private.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 DC
ciscoasa(config-asa-server-group)# Kerberos-realm PRIVATE.NET

----Configure the Domain Join-------------------------------

ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123!
ciscoasa(config)#
```

相关命令

命令	说明
aaa-server	进入 AAA 服务器配置模式，在此模式下可以配置 AAA 服务器参数。
aaa-server host	进入 AAA 服务器主机配置模式，在此模式下可以配置特定于主机的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
dns	指定域名服务器。
domain-name	指定服务器的域名。
hostname	指定主机名。
ntp	指定传输协议。
show aaa-kerberos	显示所有 AAA Kerberos 服务器的服务器统计信息。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

keepout

（当 ASA 处于维护期间或故障排除期间时）要对新的用户会话显示管理员定义的消息而不是登录页面，请在 webvpn 配置模式下使用 **keepout** 命令。要删除之前设置的禁止页面，请使用此命令的 **no** 版本。

keepout

no keepout *string*

语法说明

string	用双引号括起来的字母数字字符。

默认值

没有禁止页面。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

启用此命令后，无客户端 WebVPN 门户页面变得不可用。您将会收到一条管理员定义的消息，指明是该门户 （而非该门户的登录页面）不可用。使用 **keepout** 命令可禁用无客户端访问，但仍允许 AnyConnect 访问。当进行维护时，还可以使用此命令来指明门户不可用。

示例

以下示例显示如何配置禁止页面：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# keepout "The system is unavailable until 7:00 a.m.EST."
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
webvpn	进入 webvpn 配置模式，以便配置无客户端 SSL VPN 连接的属性。

kerberos-realm

要指定 Kerberos 服务器的领域名，请在 aaa-server 主机配置模式下使用 **kerberos-realm** 命令。要删除领域名，请使用此命令的 **no** 形式：

kerberos-realm *string*

no kerberos-realm

语法说明

string	区分大小写的字母数字字符串，最多包含 64 个字符。字符串中不允许有空格。 **注**　Kerberos 领域名仅使用数字和大写字母。虽然 ASA 接受在 *string* 参数中使用小写字母，但不会将小写字母转换为大写字母。请务必仅使用大写字母。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅适用于 Kerberos 服务器。

如果是在适用于 Kerberos 领域的 Windows 2000 Active Directory 服务器上运行，*string* 参数的值应与 Microsoft Windows **set USERDNSDOMAIN** 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
```

string 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。

示例

以下序列显示在配置 AAA 服务器主机的情景下， **kerberos-realm** 命令将 Kerberos 领域设置为“EXAMPLE.COM”：

```
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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置子模式，在此模式下可以配置特定于主机的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

key （AAA 服务器主机）

要指定用于向 AAA 服务器对 NAS 进行身份验证的服务器密钥值，请在 AAA 服务器主机配置模式下使用 **key** 命令。可以从 AAA 服务器协议配置模式访问 AAA 服务器主机配置模式。要删除密钥，请使用此命令的 **no** 形式。

key *key*

no key

语法说明

key	字母数字关键字，最多包含 127 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

key 值是区分大小写的字母数字关键字，最多包含 127 个字符，此值与 TACACS+ 服务器上的密钥值相同。满 127 个字符之后的任何字符都将被忽略。密钥用于加密客户端和服务器之间的数据。客户端和服务器上的密钥必须相同。密钥不能包含空格，但可以包含其他特殊字符。密钥 （服务器密钥）值用于向 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。

示例

以下示例配置主机 “1.2.3.4” 上名为 “srvgrp1” 的 TACACS+ AAA 服务器，将超时设置为 9 秒，将重试间隔设置为 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
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，在此模式下可以配置特定于主机的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示 AAA 服务器配置。

key （集群组）

要设置用于控制集群控制链路上的流量的身份验证密钥，请在集群组配置模式下使用 **key** 命令。要删除密钥，请使用此命令的 **no** 形式。

key *shared_secret*

no key [*shared_secret*]

语法说明

shared_secret	将共享密钥设置为 ASCII 字符串，其中包含 1 至 63 个字符。共享密钥用于生成密钥。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

此命令不会影响数据路径流量 （包括连接状态更新和转发的数据包，它们始终以明文方式发送）。

示例

以下示例设置一个共享密钥：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时， ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接重新平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable （集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位数。
priority （集群组）	设置此设备的优先级以用于主控设备选定。

key config-key password-encryption

要设置用于生成加密密钥的口令，请在全局配置模式下使用 **key config-key password-encryption** 命令。要解密使用口令进行了加密的密码，请使用此命令的 **no** 形式。

key config-key password-encryption [*new pass phrase* [*old pass phrase*]]

no key config-key password-encryption [*current pass phrase*]

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

此命令启用后，会设置用于生成加密密钥的口令。如果是第一次配置口令，不需要输入当前密码。否则，必须输入当前密码。新口令的长度必须介于 8 到 128 个字符之间。口令接受除退格符和双引号以外的所有字符。

如果丢失了主口令，先执行 **write erase** 命令再执行 **reload** 命令可删除主口令。

示例

以下示例设置用于生成加密密钥的口令：

```
ciscoasa(config)# key config-key password-encryption
```

相关命令

命令	说明
password encryption aes	启用密码加密。
write erase	执行此命令后再执行 **reload** 命令将删除丢失的主口令。

key-hash

要为自注册安全复制 (SCP) 客户端的服务器手动添加经过哈希处理的 SSH 主机密钥，请在服务器配置模式下使用 **key-hash** 命令。要访问服务器配置模式，首先需要输入 **ssh pubkey-chain** 命令。要删除密钥，请使用此命令的 **no** 形式。

key-hash {**md5** | **sha256**} *fingerprint*

no key-hash {**md5** | **sha256**} *fingerprint*

语法说明

fingerprint	输入哈希密钥。
{**md5** | **sha256**}	设置使用的哈希类型（MD5 或 SHA-256）。ASA 始终在其配置中使用 SHA-256。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(5)	我们引入了此命令。

使用指南

可以使用自注册 SCP 客户端将文件复制到 ASA 或者从其中复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如有需要，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，可以指定 SSH 主机的 **key-string** （公共密钥）或 **key-hash** （哈希值）。**key-hash** 输入哈希密钥 （MD5 或 SHA-256 密钥）；例如，从 **show** 命令输出复制的密钥。

示例

以下示例为 10.86.94.170 上的服务器添加经过哈希处理的主机密钥：

```
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
```

相关命令

命令	说明
copy	将文件复制到 ASA 或者从其中复制文件。
key-hash	输入哈希 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
ssh pubkey-chain	在 ASA 数据库中手动添加或删除服务器及其密钥。
ssh stricthostkeycheck	为自注册安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

keypair

要指定将要对其公共密钥进行认证的密钥对，请在 crypto ca trustpoint 配置模式下使用 **keypair** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

keypair *name*

no keypair

语法说明

name	指定密钥对的名称。

默认值

默认设置是不包括密钥对。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并为中心信任点指定要认证的密钥对：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。
crypto key generate dsa	生成 DSA 密钥。
crypto key generate rsa	生成 RSA 密钥。
default enrollment	将注册参数恢复为其默认值。

keysize

要在用户证书注册时指定本地证书颁发机构 (CA) 服务器生成的公共密钥和专用密钥的大小，请在 CA 服务器配置模式下使用 **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 {**512** | **768** | **1024** | **2048**}

no keysize

语法说明

512	将证书注册时生成的公共密钥和专用密钥的大小指定为 512 位。
768	将证书注册时生成的公共密钥和专用密钥的大小指定为 768 位。
1024	将证书注册时生成的公共密钥和专用密钥的大小指定为 1024 位。
2048	将证书注册时生成的公共密钥和专用密钥的大小指定为 2048 位。

默认值

默认情况下，密钥对中每个密钥的大小是 1024 位。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

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的大小指定为 2048 位：

```
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的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)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令集的访问权限，使您能够配置和管理本地 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使用者名称 DN。

keysize server

要指定本地证书颁发机构 (CA) 服务器生成的公共密钥和专用密钥的大小来配置 CA 密钥对的大小，请在 CA 服务器配置模式下使用 **keysize server** 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 server{**512** | **768** | **1024** | **2048**}

no keysize server

语法说明

512	将证书注册时生成的公共密钥和专用密钥的大小指定为 512 位。
768	将证书注册时生成的公共密钥和专用密钥的大小指定为 768 位。
1024	将证书注册时生成的公共密钥和专用密钥的大小指定为 1024 位。
2048	将证书注册时生成的公共密钥和专用密钥的大小指定为 2048 位。

默认值

默认情况下，密钥对中每个密钥的大小是 1024 位。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例为 CA 证书将密钥大小指定为 2048 位：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# keysize server 2048
ciscoasa(config-ca-server)#
```

以下示例为 CA 证书将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)#
```

相关命令

命令	说明
crypto ca server	提供对 CA 服务器配置模式命令集的访问权限，使您能够配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
keysize	为用户证书指定密钥对大小。
subject-name-default	指定在 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使用者名称 DN。

key-string

要为自注册安全复制 (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。要访问服务器配置模式，首先需要输入 **ssh pubkey-chain** 命令。此命令会提示您输入密钥字符串。输入的字符串保存到配置后，系统会使用 SHA-256 对其进行哈希处理，并将其存储为 **key-hash** 命令。因此，要删除该字符串，请使用 **no key-hash** 命令。

key-string
key_string

语法说明

key_string	输入公共密钥。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(5)	我们引入了此命令。

使用指南

可以使用自注册 SCP 客户端将文件复制到 ASA 或者从其中复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如有需要，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，可以指定 SSH 主机的 **key-string** （公共密钥）或 **key-hash** （哈希值）。*key_string* 是远程对等设备的 Base64 编码的 RSA 公共密钥。可以从开放 SSH 客户端 （即 .ssh/id_rsa.pub 文件）获取公共密钥值。提交 Base64 编码的公共密钥后，该密钥将会通过 SHA-256 进行哈希处理。

示例

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
```

以下示例显示保存的哈希密钥：

```
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
```

相关命令

命令	说明
copy	将文件复制到 ASA 或者从其中复制文件。
key-hash	输入哈希 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
ssh pubkey-chain	在 ASA 数据库中手动添加或删除服务器及其密钥。
ssh stricthostkeycheck	为自注册安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

kill

要终止 Telnet 会话，请在 EXEC 特权模式下使用 **kill** 命令。

kill *telnet_id*

语法说明

telnet_id	指定 Telnet 会话 ID。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 **kill** 命令可终止 Telnet 会话。使用 **who** 命令可查看 Telnet 会话 ID。如果您终止 Telnet 会话，ASA 会使所有活动命令终止，然后在不发出警告的情况下断开连接。

示例

以下示例显示如何终止 ID 为 “2” 的 Telnet 会话。首先，输入 **who** 命令显示活动 Telnet 会话的列表。然后，输入 **kill 2** 命令终止 ID 为 “2” 的 Telnet 会话。

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

相关命令

命令	说明
telnet	配置对 ASA 的 Telnet 访问。
who	显示活动 Telnet 会话的列表。

第 7 章

l2tp tunnel hello 至 log-adjacency-changes 命令

l2tp tunnel hello

要在通过 IPsec 连接进行的 L2TP 上指定问候消息间的间隔，请在全局配置模式下使用 **l2tp tunnel hello** 命令。要将时间间隔重置为默认值，请使用此命令的 **no** 形式：

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

语法说明

interval	问候消息间的间隔，以秒为单位。默认值为 60 秒。范围为 10 到 300 秒。

默认值

默认值为 60 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

L2tp tunnel hello 命令将使 ASA 能够检测 L2TP 连接的物理层问题。默认值为 60 秒。如果您将其配置为较低的值，则遇到问题的连接将较早断开连接。

示例

以下示例将问候消息间的时间间隔配置为 30 秒：

```
ciscoasa(config)# l2tp tunnel hello 30
```

相关命令

命令	说明
show vpn-sessiondb detail remote filter protocol L2TPOverIPsec	显示 L2TP 连接的详细信息。
vpn-tunnel-protocol l2tp-ipsec	将 L2TP 作为特定隧道组的隧道协议启用。

lacp max-bundle

要指定 EtherChannel 信道组中主用接口的最大数量，请在接口配置模式下使用 **lacp max-bundle** 命令。要将此值设置为默认值，请使用此命令的 **no** 形式。

lacp max-bundle *number*

no lacp max-bundle

语法说明

number	指定信道组中允许的主用接口的最大数量，数值介于 1 到 8 之间；对于 9.2(1) 版及更高版本，最大值将提高为 16。如果您的交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更少。

命令默认

（9.1 版及更低版本）默认值为 8。

（9.2(1) 版及更高版本）默认值为 16。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。
9.2(1)	我们将主用接口的数量从 8 个提高到了 16 个。

使用指南

为端口通道接口输入此命令。每个信道组的最大主用接口数量为八个；要减少其数量，请使用此命令。

示例

以下示例将 EtherChannel 中的最大接口数量设置为四个：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

lacp port-priority

要在 EtherChannel 内设置物理接口的优先级，请在接口配置模式下使用 **acp port-priority** 命令。要将优先级设置为默认值，请使用此命令的 **no** 形式：

lacp port-priority *number*

no lacp port-priority

语法说明

number	将优先级设置为介于 1 到 65536 之间的值。值越高，优先级越低。

命令默认

默认值为 32768。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。

使用指南

为物理接口输入此命令。ASA 使用此设置来确定哪些接口处于活动状态，以及哪些接口将在您分配的接口数超过可用数量时备用。如果所有接口的优先级设置相同，则优先级将由接口 ID（插槽 / 端口）确定。ID 最小的接口的优先级最高。例如，千兆以太网 0/0 的优先级高于千兆以太网 0/1 的优先级。

如果您希望提高较高接口 ID 的活动优先级，请使用此命令调低值。例如，要让千兆以太网 1/3 先于千兆以太网 0/7 处于活动状态，请将 1/3 接口上的 **lacp port-priority** 值设置为 12345，并将 0/7 接口上的默认值设为 32768。

如果 EtherChannel 另一端的设备的端口优先级存在冲突，则将使用系统优先级来确定要使用哪个端口优先级。请参阅 **lacp system-priority** 命令。

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设备 (LACPDU)，进而汇聚接口。LACP 将协调自动添加和删除与 EtherChannel 的链路，而无需用户干预。它还将处理配置错误，并检查成员接口的两端是否连接到正确的信道组。

示例

以下示例将为千兆以太网 0/2 设置较低的端口优先级，因此它将用作先于千兆以太网 0/0 和 0/1 的 EtherChannel 的组成部分：

```
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
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

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 **lacp system-priority** 命令。要将此值设置为默认值，请使用此命令的 **no** 形式。

lacp system-priority *number*

no lacp system-priority

语法说明

number	为 LACP 系统设置优先级，值介于 1 到 65535 之间。默认值为 32768。值越高，优先级越低。此命令适用于 ASA （全局方式）。

命令默认

默认值为 32768。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。

使用指南

如果 EtherChannel 另一端的设备的端口优先级存在冲突，则将使用系统优先级来确定要使用哪个端口优先级。有关 EtherChannel 内的接口优先级，请参阅 **lacp port-priority** 命令。

示例

以下示例将系统优先级设置为高于默认值 （较低数值）的值：

```
ciscoasa(config)# lacp system-priority 12345
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
port-channel load-balance	配置负载平衡算法。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

ldap attribute-map

要创建并命名 LDAP 属性以将用户定义的属性名称映射到思科 LDAP 属性名称，请在全局配置模式下使用 **ldap attribute-map** 命令。要删除映射，请使用此命令的 **no** 形式。

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

语法说明

map-name	为 LDAP 属性映射指定用户定义的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

借助 **ldap attribute-map** 命令，您可将您自己的属性名称和值映射到思科属性名称。然后您可以将产生的属性映射绑定到 LDAP 服务器。典型步骤如下：

1. 在全局配置模式下使用 **ldap attribute-map** 命令创建一个未填充的属性映射。此命令进入 LDAP 属性映射配置模式。
2. 在 LDAP 属性映射配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 AAA 服务器主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。注意，此命令中的 ldap 后有连字符。

注意　要正确使用属性映射功能，您需要了解思科 LDAP 属性的名称和值以及用户定义的属性的名称和值。

示例

以下命令示例在全局配置模式中输入，它首先创建一个名为 myldapmap 的 LDAP 属性映射，然后对其填充或将其与 LDAP 服务器绑定：

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)#
```

相关命令

命令	说明
ldap-attribute-map（AAA 服务器主机模式）	将 LDAP 属性映射绑定到 LDAP 服务器。
map-name	将用户定义的 LDAP 属性名称映射到思科 LDAP 属性名称。
map-value	将用户定义的属性值映射到思科属性名称。
show running-config ldap attribute-map	显示特定的正在运行的 LDAP 属性映射或所有正在运行的属性映射。
clear configure ldap attribute-map	删除所有 LDAP 属性映射。

ldap-attribute-map

要将现有映射配置与 LDAP 主机绑定，请在 AAA 服务器主机配置模式下使用 **ldap-attribute-map** 命令。要删除绑定，请使用此命令的 **no** 形式。

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

语法说明

map-name	指定 LDAP 属性映射配置。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

如果思科定义的 LDAP 属性名称无法满足您的易用要求或其他要求，您可创建您自己的属性名称、将其映射到思科属性，然后再将生成的属性配置与 LDAP 服务器绑定。您通常的步骤包括：

1. 在全局配置模式下使用 **ldap attribute-map** 命令创建一个未填充的属性映射。此命令将进入 ldap-attribute-map 配置模式。请注意此命令中的 “ldap” 后没有连字符。
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 服务器主机模式下使用 **ldap-attribute-map** 命令，将属性映射配置与 LDAP 服务器绑定。

示例

以下命令示例在 AAA 服务器主机配置模式中输入，它将名为 myldapmap 的现有属性映射与名为 ldapsvr1 的 LDAP 服务器绑定：

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	说明
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于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 LDAP 属性名称映射到思科 LDAP 属性名称。
map-value	将一个用户定义属性值映射到思科属性。
show running-config ldap attribute-map	显示运行 ldap 属性映射配置的特定值或运行属性映射配置的所有值。
clear configure ldap attribute-map	删除所有 LDAP 属性映射。

ldap-base-dn

要在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置，请在 AAA 服务器主机配置模式下使用 **ldap-base-dn** 命令。AAA 服务器主机配置模式可从 AAA 服务器协议配置模式访问。要删除此指定，进而重置搜索让其从列表顶部开始，请使用此命令的 **no** 形式。

ldap-base-dn *string*

no ldap-base-dn

语法说明

string	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置、最多包含 128 个字符串，并区分大小写的字符串；例如 OU=Cisco。字符串中不得有空格，但允许使用其他特殊字符。

默认值

从列表顶部开始搜索。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅对 LDAP 服务器有效。

示例

以下示例将在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器、将超时设置为 9 秒、将重试间隔设置为 7 秒，并将 LDAP 基础 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
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，因此您可配置特定于主机的 AAA 服务器参数。
ldap-scope	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的范围。
ldap-naming-attribute	指定在 LDAP 服务器上唯一标识条目的相对可分辨名称属性。
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 配置配置模式下使用 **ldap-defaults** 命令。 Crl 配置配置模式可从 crypto ca trustpoint 配置模式访问。这些默认值仅在 LDAP 服务器有需要时使用。要放弃指定任何 LDAP 默认值，请使用此命令的 **no** 形式。

ldap-defaults *server* [*port*]

no ldap-defaults

语法说明

port	（可选）指定 LDAP 服务器端口。如果未指定此参数， ASA 将使用标准 LDAP 端口 (389)。
server	指定 LDAP 服务器的 IP 地址或域名。如果 CRL 分发点内存在 IP 地址或域名，则它将覆盖此值。

默认值

未设置默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例定义默认端口 (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
```

相关命令

命令	说明
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
protocol ldap	将 LDAP 指定为 CRL 的检索方法。

ldap-dn

要将 X.500 可分辨名称和密码传递到需要为 CRL 检索进行身份验证的 LDAP 服务器，请在 crl 配置配置模式下使用 **ldap-dn** 命令。 Crl 配置配置模式可从 crypto ca trustpoint 配置模式访问。这些参数仅在 LDAP 服务器有需要时使用。要放弃指定任何 LDAP DN，请使用此命令的 **no** 形式。

ldap-dn *x.500-name password*

no ldap-dn

语法说明

password	为此可分辨名称定义密码。支持的最大字段长度是 128 个字符。
x.500-name	定义访问此 CRL 数据库的目录路径，例如 cn=crl、 ou=certs、 o=CAName、 c=US。支持的最大字段长度是 128 个字符。

默认值

默认设置为不开启。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例为信任点中心指定 X.500 名称 CN=admin、 OU=devtest、 O=engineering 和密码 xxzzyy：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

相关命令

命令	说明
crl configure	进入 crl 配置配置模式。
crypto ca trustpoint	进入 CA 信任点配置模式。
protocol ldap	将 LDAP 指定为 CRL 的检索方法。

ldap-group-base-dn

要在动态访问策略所使用的 Active Directory 层次结构中为组搜索指定基础组，请在 AAA 服务器主机配置模式下使用 **ldap-group-base-dn** 命令。要从运行的配置中删除此命令，请使用此命令的 **no** 形式：

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

语法说明

string	最多包含 128 个字符且区分大小写的字符串，用于在 Active Directory 层次结构中指定服务器开始搜索的位置。例如， ou=Employees。字符串中不得有空格，但允许使用其他特殊字符。

默认值

没有默认行为或值。如果您未指定一组搜索 DN，则搜索将从基础 DN 开始。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(4)	引入了此命令。

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 **show ad-groups** 命令用于开始其组搜索的 Active Directory 层次结构级别。动态组策略使用从搜索检索到的组作为特定策略的选择标准。

示例

以下示例设置组基础 DN 以开始组织单位 (ou) 级别员工的搜索：

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

相关命令

命令	说明
group-search-timeout	调整 ASA 为一系列组等待 Active Directory 服务器响应的时间。
show ad-groups	显示列于 Active Directory 服务器中的组。

ldap-login-dn

要指定系统应将其绑定作为目录对象的名称，请在 AAA 服务器主机配置模式下使用 **ldap-login-dn** 命令。AAA 服务器主机配置模式可从 AAA 服务器协议配置模式访问。要删除此指定，请使用此命令的 **no** 形式。

ldap-login-dn *string*

no ldap-login-dn

语法说明

string	最多包含 128 个字符且区分大小写的字符串，用于在 LDAP 层次结构中指定目录对象名称。字符串中不得有空格，但允许使用其他特殊字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅对 LDAP 服务器有效。支持的最大字符串长度为 128 个字符。

一些 LDAP 服务器（包括 Microsoft Active Directory 服务器）需要 ASA 通过身份验证绑定建立握手，然后才会接受任何其他 LDAP 操作的请求。ASA 通过将登录 DN 字段附加到用户身份验证请求，进而标识自身进行身份验证绑定。登录 DN 字段描述 ASA 的身份验证特征。这些字符串应对应于那些具有管理员权限的用户。

对于*字符串*变量，请输入目录对象的名称进行 VPN 集中器身份验证绑定，例如：cn= 管理员、cn= 用户、 ou= 人员、 dc=XYZ 公司、 dc=com。对于匿名访问，请将此字段留空。

示例

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器、将超时设置为 9 秒、将重试间隔设置为 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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，因此您可配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置。
ldap-login-password	指定登录 DN 的密码。此命令仅对 LDAP 服务器有效。
ldap-naming-attribute	指定在 LDAP 服务器上唯一标识条目的相对可分辨名称属性。
ldap-scope	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的范围。

ldap-login-password

要指定 LDAP 服务器的登录密码，请在 AAA 服务器主机配置模式下使用 **ldap-login-password** 命令。AAA 服务器主机配置模式可从 AAA 服务器协议配置模式访问。要删除此密码指定，请使用此命令的 **no** 形式：

ldap-login-password *string*

no ldap-login-password

语法说明

string	最多包含 64 个字符且区分大小写的字母数字密码。密码不能包含空格字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅对 LDAP 服务器有效。最大密码字符串长度为 64 个字符。

示例

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器、将超时设置为 9 秒、将重试间隔设置为 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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，因此您可配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-naming-attribute	指定在 LDAP 服务器上唯一标识条目的相对可分辨名称属性。
ldap-scope	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的范围。

ldap-naming-attribute

要指定相对可分辨名称属性，请在 AAA 服务器主机配置模式下使用 **ldap-naming-attribute** 命令。 AAA 服务器主机配置模式可从 AAA 服务器协议配置模式访问。要删除此指定，请使用此命令的 **no** 形式：

ldap-naming-attribute *string*

no ldap-naming-attribute

语法说明

string	区分大小写的字母数字的相对可分辨名称属性，用于唯一标识 LDAP 服务器上条目，最多包含 128 个字符。字符串中不得有空格，但允许使用其他特殊字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

输入用于在 LDAP 服务器上唯一标识条目的相对可分辨名称属性。常见的命名属性包括公用名称 (cn) 和用户 ID (uid)。

此命令仅对 LDAP 服务器有效。支持的最大字符串长度为 128 个字符。

示例

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器、将超时设置为 9 秒、将重试间隔设置为 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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，因此您可配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置。
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。此命令仅对 LDAP 服务器有效。
ldap-scope	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的范围。

ldap-over-ssl

要在 ASA 与 LDAP 服务器之间建立安全 SSL 连接，请在 AAA 服务器主机配置模式下使用 **ldap-over-ssl** 命令。要为此连接禁用 SSL，请使用此命令的 **no** 形式。

ldap-over-ssl enable

no ldap-over-ssl enable

语法说明

enable	指定 SSL 保护与 LDAP 服务器的连接。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用此命令指定 ASA 与 LDAP 服务器之间的 SSL 安全连接。

注意　如果您使用纯文本身份验证，我们建议您启用此功能。请参阅 **sasl-mechanism** 命令。

示例

在 AAA 服务器主机的配置模式中输入的以下命令将在 ASA 与 IP 地址为 10.10.0.1、名为 ldapsvr1 的 LDAP 服务器之间的连接启用 SSL。它们还将配置纯 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)#
```

相关命令

命令	说明
sasl-mechanism	指定 LDAP 客户端与服务器之间的 SASL 身份验证。
server-type	指定 Microsoft 或 Sun 作为 LDAP 服务器供应商。
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于将用户定义的属性名称映射到思科 LDAP 属性名称。

ldap-scope

要在 LDAP 层次结构内指定服务器应在收到授权请求时开始搜索的范围，请在 AAA 服务器主机配置模式下使用 **ldap-scope** 命令。 AAA 服务器主机配置模式可从 AAA 服务器协议配置模式访问。要删除此指定，请使用此命令的 **no** 形式。

ldap-scope *scope*

no ldap-scope

语法说明

scope	LDAP 层次结构中服务器在收到授权请求时要搜索的级别数。有效值为： • **onelevel** - 仅搜索基础 DN 下的一级别 • **subtree** - 搜索基础 DN 下的所有级别

默认值

默认值为 **onelevel**。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

将范围指定为 **onelevel** 将加快搜索速度，因为此时仅搜索基础 DN 的下一级别。指定为 **subtree** 将减缓速度，因为此时将搜索基础 DN 下的所有级别。

此命令仅对 LDAP 服务器有效。

示例

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器、将超时设置为 9 秒、将重试间隔设置为 7 秒，并将 LDAP 范围配置为包含子树级别。

```
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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，因此您可配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定服务器应在收到授权请求时开始搜索的位置。
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。此命令仅对 LDAP 服务器有效。
ldap-naming-attribute	指定在 LDAP 服务器上唯一标识条目的相对可分辨名称属性。

leap-bypass

要启用 LEAP Bypass，请在组策略配置模式下使用 **leap-bypass enable** 命令。要禁用 LEAP Bypass，请使用 **leap-bypass disable** 命令。要将 LEAP Bypass 属性从运行的配置中删除，请使用此命令的 **no** 形式。此选项允许继承来自其他组策略中的 LEAP Bypass 值。

leap-bypass {**enable** | **disable**}

no leap-bypass

语法说明

disable	禁用 LEAP Bypass。
enable	启用 LEAP Bypass。

默认值

LEAP Bypass 已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

LEAP Bypass 启用后，可让来自 VPN 硬件客户端后的无线设备的 LEAP 数据包在用户身份验证之前通过 VPN 隧道。这样就可让使用思科无线接入点设备的工作站建立 LEAP 身份验证。然后，设备就能根据用户身份验证再次进行身份验证。

如果您启用交互式硬件客户端身份验证，则此功能将无法按照预期正常运行。

有关进一步信息，请参阅 CLI 配置指南。

注意　允许任何未经身份验证的流量通过隧道可能存在安全风险。

示例

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
```

相关命令

命令	说明
secure-unit-authentication	每当客户端启动一个隧道时，都需要 VPN 硬件客户端使用用户名和密码进行身份验证。
user-authentication	要求 VPN 硬件客户端后方的用户先对 ASA 确定自身身份，然后再进行连接。

license

要配置 ASA 发送到 云网络安全 代理服务器以指示请求来自哪些组织的身份验证密钥，请在 scansafe general-options 配置模式下使用 **license** 命令。要删除许可证，请使用此命令的 **no** 形式。

license *hex_key*

no license [*hex_key*]

语法说明

hex_key	指定身份验证密钥为 16 字节的十六进制数。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

每个 ASA 都必须使用您从云网络安全获得的身份验证密钥。身份验证密钥可让云网络安全标识与网络请求关联的公司，并确保 ASA 与有效的客户相关联。

您可对 ASA 使用两类身份验证密钥中的一种：公司密钥或组密钥。

公司身份验证密钥

公司身份验证密钥可用于同一公司内的多个 ASA。此密钥仅为您的 ASA 启用云网络安全服务。管理员将在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 内生成密钥；您有机会通过电邮发送密钥供稍后使用。稍后您无法在 ScanCenter 中查看此密钥； ScanCenter 中仅显示密钥的后四位。有关详细信息，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。

组身份验证密钥

组身份验证密钥是执行以下两项功能的 ASA 唯一特殊密钥：

- 为一个 ASA 启用云网络安全服务。
- 标识所有来自 ASA 的流量，从而为每个 ASA 创建 ScanCenter 策略。

管理员将在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 内生成密钥；您有机会通过电邮发送密钥供稍后使用。稍后您无法在 ScanCenter 中查看此密钥； ScanCenter 中仅显示密钥的后四位。有关详细信息，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。

示例

以下示例仅配置一台主服务器：

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

license-server address

要标识参与者的共享许可服务器的 IP 地址和共享密钥，请在全局配置模式下使用 **license-server address** 命令。要禁用共享许可参与，请使用此命令的 **no** 形式。共享许可证可让您购买大量 SSL VPN 会话，并根据需要在一组 ASA 间共享会话，方法是将一个 ASA 配置为共享许可服务器，并将其余 ASA 配置为共享许可参与者。

license-server address *address* **secret** *secret* [**port** *port*]

no license-server address [*address* **secret** *secret* [**port** *port*]]

语法说明

address	标识共享许可服务器的 IP 地址。
port *port*	（可选）如果您使用 **license-server port** 命令更改了服务器配置中的默认端口，请设置要匹配的备用服务器，值应介于 1 到 65535 之间。默认端口为 50554。
secret *secret*	标识共享密钥。密钥必须与 **license-server secret** 命令在服务器上设置的密钥匹配。

命令默认

默认端口为 50554。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

共享许可参与者必须有共享许可参与者密钥。使用 **show activation-key** 命令来检查您已安装的许可证。

对每名参与者，您只能指定一台共享许可证服务器。

以下步骤描述了共享许可证的运行方式：

1. 决定哪个 ASA 应是共享许可服务器，并购买使用此设备序列号的共享许可服务器许可证。
2. 决定哪个 ASA 应是共享许可参与者，包括共享许可备用服务器，并使用每个设备序列号为每台设备获取共享许可参与者许可证。
3. （可选）指定第二个 ASA 作为共享许可备用服务器。您只能指定一台备用服务器。

注　共享许可备用服务器只需要一个参与者许可证。

4. 在共享许可服务器上配置共享密钥；拥有共享密钥的任何参与者都可使用共享许可证。
5. 当您将 ASA 配置为参与者时，它将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　参与者需要能够通过 IP 网络与服务器通信；参与者不必位于同一子网中。

6. 共享许可服务器将响应有关参与者向服务器轮询的频率的信息。
7. 当参与者用尽本地许可证的会话时，它将向共享许可服务器发送请求，请求更多会话，每次增加 50 个会话。
8. 共享许可服务器将以共享许可证响应。参与者使用的总会话数不得超过平台型号的最大会话数。

注　如果共享许可服务器用尽本地会话，它还可参与共享许可证池。它不需要参与者许可证，以及参与的服务器许可证。

   a. 如果共享许可证池中的会话数量不够参与者使用，则服务器将以所有可用的会话响应。
   b. 参与者将继续发送刷新消息，请求更多会话，直到服务器能够充分地满足此请求。
9. 当某一参与者的负载降低时，它将向服务器发送一条消息，以释放共享会话。

注意　ASA 使用 SSL 来加密服务器与参与者之间的所有通信。

参与者与服务器之间的通信问题

请参阅以下指南了解参与者与服务器之间的通信问题：

- 如果参与者无法在 3 次刷新间隔后发送刷新，则服务器将释放会话，将其还给共享许可证池。
- 如果参与者无法访问许可证服务器发送刷新，则参与者可继续使用接收自服务器的共享许可证最多 24 小时。
- 如果参与者在 24 小时后仍无法与许可证服务器通信，则参与者将释放共享许可证，即便其仍需会话。参与者将离开已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果参与者在 24 小时期满之前与服务器重新连接，则参与者需要发送新的会话请求；服务器将以可重新分配到此参与者的会话数量响应。

示例

以下示例将设置许可证服务器 IP 地址和共享密钥，以及备用许可证服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	清除共享许可证统计信息。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup address

要标识参与者的共享许可备用服务器的 IP 地址，请在全局配置模式下使用 **license-server backup address** 命令。要禁用备用服务器使用，请使用此命令的 **no** 形式。

license-server backup address *address*

no license-server address [*address*]

语法说明

address	标识共享许可备用服务器的 IP 地址。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

对共享许可备用服务器必须配置 **license-server backup enable** 命令。

示例

以下示例将设置许可证服务器 IP 地址和共享密钥，以及备用许可证服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

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。要删除备用服务器配置，请使用此命令的 **no** 形式。

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

语法说明

address	标识共享许可备用服务器的 IP 地址。
backup-id *serial_number*	标识共享许可备用服务器的序列号。
ha-backup-id *ha_serial_number*	如果您使用备用服务器故障切换，请标识辅助共享许可备用服务器的序列号。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

您仅可标识 1 台备用服务器及其可选的备用设备。

要查看备用服务器的序列号，请输入 **show activation-key** 命令。

要启用参与者作为备用服务器，请使用 **license-server backup enable** 命令。

共享许可备用服务器必须向主共享许可服务器成功注册，然后才能承担备用角色。在注册时，主共享许可服务器将与备用许可服务器同步服务器设置及共享许可证信息，包括注册的参与者和当前许可证使用情况的列表。主服务器与备用服务器的数据同步间隔为 10 秒。初始同步完成后，备用服务器即可成功执行备用职责，即使在重新加载之后依旧如此。

当主服务器出现故障时，备用服务器将接管服务器运行。备用服务器最多可持续运行 30 天，此后，备用服务器将停止对参与者签发会话，现有会话将超时。请务必在这 30 天内恢复主服务器。第 15 天时，将发送严重级别的系统日志消息，并在第 30 天时再次发送。

主服务器恢复时，它将与备用服务器同步，并随后接管服务器的运行。

当备用服务器未处于活动状态时，它将充当主共享许可服务器的常规参与者。

注意　当您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。运行限制将逐日递增，直至达到第 30 天。此外，如果主服务器在随后的任何时间段内发生故障，备用服务器的运行限制都将逐日递减。当主服务器恢复时，备用服务器的运行限制将开始逐日递增。例如，如果主服务器发生故障 20 天，这期间备用服务器处于活动状态，则备用服务器只有 10 天限制。备用服务器将在作为不活动备用额外 20 天后 “ 充电 ” 最多 30 天。实施此充电功能旨在防止共享许可证的滥用。

示例

以下示例将设置共享密钥、更改刷新间隔和端口、配置备用服务器，并启用此设备作为内部接口和 dmz 接口上的共享许可服务器：

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup enable

要启用此部件作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。要禁用备用服务器，请使用此命令的 **no** 形式。

license-server backup enable *interface_name*

no license-server enable *interface_name*

语法说明

interface_name	指定参与者联系备用服务器的接口。您可根据需要为任意数量的接口重复此命令。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

备用服务器必须拥有共享许可参与者密钥。

共享许可备用服务器必须向主共享许可服务器成功注册，然后才能承担备用角色。在注册时，主共享许可服务器将与备用许可服务器同步服务器设置及共享许可证信息，包括注册的参与者和当前许可证使用情况的列表。主服务器与备用服务器的数据同步间隔为 10 秒。初始同步完成后，备用服务器即可成功执行备用职责，即使在重新加载之后依旧如此。

当主服务器出现故障时，备用服务器将接管服务器运行。备用服务器最多可持续运行 30 天，此后，备用服务器将停止对参与者签发会话，现有会话将超时。请务必在这 30 天内恢复主服务器。第 15 天时，将发送严重级别的系统日志消息，并在第 30 天时再次发送。

主服务器恢复时，它将与备用服务器同步，并随后接管服务器的运行。

当备用服务器未处于活动状态时，它将充当主共享许可服务器的常规参与者。

注意　当您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。运行限制将逐日递增，直至达到第 30 天。此外，如果主服务器在随后的任何时间段内发生故障，备用服务器的运行限制都将逐日递减。当主服务器恢复时，备用服务器的运行限制将开始逐日递增。例如，如果主服务器发生故障 20 天，这期间备用服务器处于活动状态，则备用服务器只有 10 天限制。备用服务器将在作为不活动备用额外 20 天后 “ 充电 ” 最多 30 天。实施此充电功能旨在防止共享许可证的滥用。

示例

以下示例将标识许可证服务器和共享密钥，并启用此设备作为内部接口和 dmz 接口上的备用共享许可证服务器。

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server enable

要标识此设备作为共享许可服务器，请在全局配置模式下使用 **license-server enable** 命令。要禁用共享许可服务器，请使用此命令的 **no** 形式。共享许可证可让您购买大量 SSL VPN 会话，并根据需要在一组 ASA 间共享会话，方法是将一个 ASA 配置为共享许可服务器，并将其余 ASA 配置为共享许可参与者。

license-server enable *interface_name*

no license-server enable *interface_name*

语法说明

interface_name	指定参与者用于联系服务器的接口。您可根据需要为任意数量的接口重复此命令。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

共享许可服务器必须拥有共享许可服务器密钥。使用 **show activation-key** 命令来检查您已安装的许可证。

以下步骤描述了共享许可证的运行方式：

1. 决定哪个 ASA 应是共享许可服务器，并购买使用此设备序列号的共享许可服务器许可证。
2. 决定哪个 ASA 应是共享许可参与者，包括共享许可备用服务器，并使用每个设备序列号为每台设备获取共享许可参与者许可证。
3. （可选）指定第二个 ASA 作为共享许可备用服务器。您只能指定一台备用服务器。

   注　共享许可备用服务器只需要一个参与者许可证。

4. 在共享许可服务器上配置共享密钥；拥有共享密钥的任何参与者都可使用共享许可证。
5. 当您将 ASA 配置为参与者时，它将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　参与者需要能够通过 IP 网络与服务器通信；参与者不必位于同一子网中。

6. 共享许可服务器将响应有关参与者向服务器轮询的频率的信息。
7. 当参与者用尽本地许可证的会话时，它将向共享许可服务器发送请求，请求更多会话，每次增加 50 个会话。
8. 共享许可服务器将以共享许可证响应。参与者使用的总会话数不得超过平台型号的最大会话数。

注　如果共享许可服务器用尽本地会话，它还可参与共享许可证池。它不需要参与者许可证，以及参与的服务器许可证。

   a. 如果共享许可证池中的会话数量不够参与者使用，则服务器将以所有可用的会话响应。
   b. 参与者将继续发送刷新消息，请求更多会话，直到服务器能够充分地满足此请求。

9. 当某一参与者的负载降低时，它将向服务器发送一条消息，以释放共享会话。

注意　ASA 使用 SSL 来加密服务器与参与者之间的所有通信。

参与者与服务器之间的通信问题

请参阅以下指南了解参与者与服务器之间的通信问题：

- 如果参与者无法在 3 次刷新间隔后发送刷新，则服务器将释放会话，将其还给共享许可证池。
- 如果参与者无法访问许可证服务器发送刷新，则参与者可继续使用接收自服务器的共享许可证最多 24 小时。
- 如果参与者在 24 小时后仍无法与许可证服务器通信，则参与者将释放共享许可证，即便其仍需会话。参与者将离开已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果参与者在 24 小时期满之前与服务器重新连接，则参与者需要发送新的会话请求；服务器将以可重新分配到此参与者的会话数量响应。

示例

以下示例将设置共享密钥、更改刷新间隔和端口、配置备用服务器，并启用此设备作为内部接口和 DMZ 接口上的共享许可服务器：

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server port

要设置共享许可服务器侦听来自参与者的 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，请使用此命令的 **no** 形式。

license-server port *port*

no license-server port [*port*]

语法说明

seconds	设置服务器侦听来自参与者的 SSL 连接的端口，在 1 到 65535 之间。默认值为 TCP 端口 50554。

命令默认

默认端口为 50554。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

如果您更改了端口的默认值，请务必使用 **icense-server address** 命令为每个参与者设置相同的端口。

示例

以下示例将设置共享密钥、更改刷新间隔和端口、配置备用服务器，并启用此设备作为内部接口和 DMZ 接口上的共享许可服务器：

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server refresh-interval

要设置提供给参与者的刷新间隔，进而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。要恢复默认刷新间隔，请使用此命令的 **no** 形式。

license-server refresh-interval *seconds*

no license-server refresh-interval [*seconds*]

语法说明

seconds	将刷新间隔设置为 10 到 300 秒之间的值。默认值为 30 秒。

命令默认

默认值为 30 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

每个参与者都将使用 SSL 定期与共享许可服务器通信，因而共享许可服务器能够跟踪当前许可证的使用情况，并接收和响应许可证请求。

示例

以下示例将设置共享密钥、更改刷新间隔和端口、配置备用服务器，并启用此设备作为内部接口和 dmz 接口上的共享许可服务器：

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server secret	设置共享许可服务器上的共享密钥。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

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-server secret** 命令。要删除密钥，请使用此命令的 **no** 形式。

license-server secret *secret*

no license-server secret *secret*

语法说明

secret	设置共享密钥，共享密钥为包含 4 到 128 个 ASCII 字符的字符串。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

license-server address 命令中所标识的任何参与者都可以使用许可服务器。

示例

以下示例将设置共享密钥、更改刷新间隔和端口、配置备用服务器，并启用此设备作为内部接口和 dmz 接口上的共享许可服务器：

```
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
```

相关命令

命令	说明
activation-key	输入许可证激活密钥。
clear configure license-server	清除共享许可服务器配置。
clear shared license	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的 IP 地址和共享密钥。
license-server backup address	标识参与者的共享许可备用服务器。
license-server backup backup-id	标识主共享许可服务器的备用服务器 IP 地址和序列号。
license-server backup enable	启用设备作为共享许可备用服务器。
license-server enable	启用设备作为共享许可服务器。
license-server port	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server refresh-interval	设置提供给参与者的刷新间隔，从而设置其与服务器通信的频率。
show activation-key	显示当前安装的许可证。
show running-config license-server	显示共享许可服务器配置。
show shared license	显示共享许可证统计信息。
show vpn-sessiondb	显示有关 VPN 会话的许可证信息。

lifetime （CA 服务器模式）

要指定本地证书颁发机构 (CA) 证书、每个已签发用户的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。要将生命周期重设为默认值，请使用此命令的 **no** 形式：

lifetime {**ca-certificate** | **certificate** | **crl**} *time*

no lifetime {**ca-certificate** | **certificate** | **crl**}

语法说明

ca-certificate	指定本地 CA 服务器证书的生命周期。
certificate	指定 CA 服务器签发的所有用户证书的生命周期。
crl	指定 CRL 的生命周期。
time	对于 CA 证书和所有已签发的证书， *time* 将指定证书有效的天数。有效范围是为 1 到 3650 天。 对于 CRL， *time* 将指定 CRL 有效的小时数。 CRL 的有效范围为 1 到 720 小时。

默认值

默认的生命周期为：

- CA 证书 - 三年
- 签发的证书 - 一年
- CRL - 6 小时

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

通过指定证书或 CRL 有效的天数或小时数，此命令可确定包含于证书或 CRL 的到期日期。

lifetime ca-certificate 命令将在本地 CA 服务器证书第一次生成（即当您最初配置本地 CA 服务器并发出 **no shutdown** 命令）时生效。 CA 证书过期后，配置的生命周期值将用于生成新的 CA 证书。您无法更改现有 CA 证书的生命周期值。

示例

以下示例将配置 CA 以签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))#
```

以下示例将配置 CA 签发有效期为两天的 CRL：

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# lifetime crl 48
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
cdp-url	指定包含于由 CA 签发的证书中的证书撤销列表分发点 (CDP)。
crypto ca server	提供 CA 服务器配置模式命令集的访问权限，从而允许您配置和管理本地 CA。
crypto ca server crl issue	强制签发 CRL。
show crypto ca server	以 ASCII 文本显示本地 CA 配置详细信息。
show crypto ca server cert-db	显示本地 CA 服务器证书。
show crypto ca server crl	显示本地 CA 的当前 CRL。

lifetime （ikev2 策略模式）

要在 IKEv2 安全关联 (SA) 中为 AnyConnect IPsec 连接指定加密算法，请在 IKEv2 策略配置模式下使用 **encryption** 命令。要删除命令并使用默认设置，请使用此命令的 **no** 形式：

lifetime {{ **seconds** *seconds*} | **none** }

语法说明

seconds	生命周期以秒为单位，值介于 120 到 2147483647 秒之间。默认值为 86,400 秒 （24 小时）。

默认值

默认值为 86,400 秒 （24 小时）。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。输入 **crypto ikev2 policy** 命令后，使用 **lifetime** 命令设置 SA 生命周期。

生命周期将为 IKEv2 SA 重新生成密钥设置间隔。使用关键字 none 将禁用对 SA 重新生成密钥。但是， AnyConnect 客户端仍可以对 SA 重新生成密钥。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。

示例

以下示例将进入 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
```

相关命令

命令	说明
encryption	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定加密算法。
group	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 Diffie-Hellman 组。
integrity	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 ESP 完整性算法。
prf	指定用于 AnyConnect IPsec 连接的 IKEv2 SA 中的伪随机函数。

limit-resource

要在多情景模式中指定某一类的资源限制，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 **no** 形式：ASA 通过将情景分配到资源类来管理资源。每个情景使用由类设置的资源限制。

limit-resource [**rate**] {**all** | *resource_name*} *number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

语法说明

all	为所有资源设置限制。
number[**%**]	将资源限制指定为大于或等于 1 的固定数值，或介于 1 到 100 （使用百分比符号 (%)）之间的系统限制百分比。将限制设置为 **0** 表示无限资源，或对于 VPN 资源类型，将限制设置为 none。对于没有系统限制的资源，您无法设置百分比 (%)；您仅能设置绝对值。
rate	指定您希望为资源设置的每秒速率。请参阅表 7-1 了解您可设置每秒速率的资源。
resource_name	指定您可设置限制的资源名称。此限制将覆盖为 **all** 设置的限制。

默认值

如果未向另一类分配情景，则所有情景都属于默认类；您无需主动为默认类分配情景。

对于大多数资源，默认类将为所有情景提供无限资源访问权限，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。）
- IPsec 会话 - 5 个会话。（每个情景的最大值。）
- MAC 地址 - 65535 个条目。（每个情景的最大值。）
- VPN 站点间隧道 - 0 个会话。（您必须手动配置类以允许任何 VPN 会话。）

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	创建了一种新的资源类型 （即 routes），以在每个情景中设置路由表条目的最大数量。 创建了新的资源类型 （即 vpn other 和 vpn burst other），以在每个情景中设置站点间 VPN 隧道的最大数量。

使用指南

默认情况下，所有安全情景都可无限制访问 ASA 的资源，但每个情景的最大限制将强制实施；唯一的例外是 VPN 资源，默认情况下此资源将被禁用。如果您发现一个或多个情景使用过多资源，且它们将导致其他情景连接被拒等情况，则您可配置资源管理，以限制每个情景的资源使用。对于 VPN 资源，您必须配置资源管理，以允许任何 VPN 隧道。

表 7-1 列出了资源类型和限制。另请参阅 **show resource types** 命令。

表 7-1　资源名称和限制

资源名称	速率或并发	每个情景的最小数量和最大数量	系统限制[1]	说明
asdm	并发	最少 1 个 最多 5 个	32	ASDM 管理会话。 **注**　ASDM 会话使用两个 HTTPS 连接：一个用于监控始终存在的连接，另一个用于对仅在更改时存在的连接进行配置更改。例如， 32 个 ASDM 会话的系统限制代表 64 个 HTTPS 会话的限制。
conns	并发或速率	不适用	并发连接：请参阅 CLI 配置指南了解您平台的连接限制。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接 （包括一台主机和多台其他主机之间的连接）。
hosts	并发	不适用	不适用	可通过 ASA 连接的主机。
inspects	速率	不适用	不适用	应用检查。
mac-addresses	并发	不适用	65,535	对于透明防火墙模式， 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。
ssh	并发	最少 1 个 最多 5 个	100	SSH 会话。
syslogs	速率	不适用	不适用	系统日志消息。
telnet	并发	最少 1 个 最多 5 个	100	Telnet 会话。
vpn burst other	并发	不适用	您型号的其他 VPN 会话数量减去为 **vpn other** 向所有情景分配的会话总和。	所允许的站点间 VPN 会话数超过了分配到某一包含 **vpn other** 的情景的会话数。例如，如果您的型号支持 5000 个会话，而您为包含 **vpn other** 的所有情景共分配了 4000 个会话，则剩余 1000 个会话可用于 **vpn burst other**。不同于能保证情景会话的 **vpn other**， **vpn burst other** 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
vpn other	并发	不适用	请参阅 CLI 配置指南中 “ 每个型号支持的功能许可证 ” 章节，了解可用于您的型号的其他 VPN 会话。	站点间 VPN 会话。您无法超订用此资源；所有结合的情景分配不得超过型号限制。您为此资源分配的会话均确保用于情景。
xlates	并发	不适用	不适用	地址转换。

1. 如果此列的值为 “ 不适用 ”，则您无法设置资源的百分比，因为没有针对此资源的硬系统限制。

示例

以下示例将 conns 的默认类限制设置为 10%，而非无限制：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

所有其他资源仍然不受限制。

要添加名为 gold 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
```

相关命令

命令	说明
class	创建资源类。
context	配置安全情景。
member	为资源类分配情景。
show resource allocation	显示如何跨类分配资源。
show resource types	显示可为其设置限制的资源类型。

lmfactor

要为仅拥有最后修改时间戳而无其他任何服务器组过期值的缓存对象重新验证策略，请在缓存配置模式下使用 **lmfactor** 命令。要设置新策略以重新验证此类对象，请再次使用此命令。要将属性重置为默认值 20，请输入此命令的 **no** 版本。

lmfactor *value*

no lmfactor

语法说明

value	介于 0 到 100 之间的整数。

默认值

默认值为 20。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

ASA 将使用 lmfactor 值估计缓存对象视为无更改的时间长度。这就是所谓的过期时间。ASA 将以自上次修改后经过的时间乘以 lmfactor 来估计过期时间。

将 lmfactor 设置为零等效于强制执行立即重新验证，而将其设置为 100 将形成重新验证之前最长的允许时间。

示例

以下示例显示如何设置值为 30 的 lmfactor：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(config-webvpn-cache)#
```

相关命令

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	配置不需要重新验证即缓存对象的到期时间。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义缓存对象的最小大小。

local-unit

要为此集群成员提供名称，请在集群组配置模式下使用 **local-unit** 命令。要删除该名称，请使用此命令的 **no** 形式。

local-unit *unit_name*

no local-unit [*unit_name*]

语法说明

unit_name	使用包含 1 到 38 个字符的唯一 ASCII 字符串为此集群成员命名。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

每个设备必须拥有唯一的名称。集群不允许设备使用重复名称。

示例

以下示例将此设备命名为“unit1”：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时， ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接重新平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable （集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
mtu cluster-interface	为集群控制链路接口指定最大传输单位数。
priority （集群组）	设置此设备的优先级以用于主控设备选定。

log

使用 模块化策略框架时，将在匹配或类配置模式下使用 **log** 命令记录与 **match** 命令或类映射匹配的数据包。此日志操作可用于应用流量的检查策略映射 （**policy-map type inspect** 命令）。要禁用此操作，请使用此命令的 **no** 形式。

log

no log

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。当您输入 **match** 或 **class** 命令以确定应用流量后（**class** 命令引用现有 **class-map type inspect** 命令，后者包含 **match** 命令）后，您可输入 **log** 命令，以记录与 **match** 命令或 **class** 命令相匹配的所有数据包。

在第 3/4 层策略映射中使用 **inspect** 命令启用应用检查 （**policy-map** 命令）时，您可以启用包含此操作的检查策略映射，例如，当 http_policy_map 是检查策略映射的名称时输入 **inspect http http_policy_map** 命令。

示例

以下示例在数据包与 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
```

相关命令

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

log-adj-changes (OSPFv2)

要在 OSPF 邻居运行或关闭时配置路由器以发送系统日志消息，请在路由器配置模式下使用 **log-adj-changes** 命令。要关闭此功能，请使用此命令的 **no** 形式。

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

语法说明

detail	（可选）在每个状态更改时发送系统日志消息，而非仅在邻居运行或关闭时发送。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

log-adj-changes 命令将默认启用；它将显示于运行的配置中，除非使用此命令的 **no** 形式将其删除。

示例

以下示例在 OSPF 邻居运行或关闭时禁用发送系统日志消息：

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show ospf	显示有关 OSPF 路由过程的一般信息。

log-adjacency-changes (OSPFv3)

要在 OSPFv3 邻居运行或关闭时配置路由器以发送系统日志消息，请在 IPv6 路由器配置模式下使用 **log-adjacency-changes** 命令。要关闭此功能，请使用此命令的 **no** 形式。

log-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

语法说明

detail	（可选）在每个状态更改时发送系统日志消息，而非仅在邻居运行或关闭时发送。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

log-adjacency-changes 命令将默认启用；它将显示于运行的配置中，除非使用此命令的 **no** 形式将其删除。

示例

以下示例将在 OSPFv3 邻居运行或关闭时禁用发送系统日志消息：

```
ciscoasa(config)# ipv6 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

相关命令

命令	说明
ipv6 router ospf	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。

第 8 章

logging asdm 至 logout message 命令

logging asdm

要将系统日志消息发送到 ASDM 日志缓冲区，请在全局配置模式中使用 **logging asdm** 命令。要禁用日志记录到 ASDM 日志缓冲区，请使用此命令的 **no** 形式。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、 2、 1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到 ASDM 日志缓冲区的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

ASDM 日志记录默认将禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在任何消息发送到 ASDM 日志缓冲区之前，您必须使用 **logging enable** 命令启用日志记录。

当 ASDM 日志缓冲区已满时， ASA 将删除最早的消息，以释放缓冲区空间供新消息使用。要控制保留于 ASDM 日志缓冲区中的系统日志消息数量，请使用 **logging asdm-buffer-size** 命令。

ASDM 日志缓冲区是不同于使用 **logging buffered** 命令启用的日志缓冲区的缓冲区。

示例

以下示例演示如何启用日志记录、发送严重性级别 0、 1 和 2 的日志缓冲区消息到 ASDM，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
```

相关命令

命令	说明
clear logging asdm	清除包含的所有消息的 ASDM 日志缓冲区。
logging asdm-buffer-size	指定保留于 ASDM 日志缓冲区中的 ASDM 消息数量。
logging enable	启用日志记录。
logging list	创建可重复使用的消息选择标准列表。
show logging	显示已启用的日志记录选项。
show running-config logging	显示日志记录配置。

logging asdm-buffer-size

要指定保留于 ASDM 日志缓冲区中的系统日志消息数量，请在全局配置模式中使用 **logging asdm-buffer-size** 命令。要将 ASDM 日志缓冲区重置回其 100 条消息的默认大小，请使用此命令的 **no** 形式。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

语法说明

num_of_msgs	指定 ASA 保留在 ASDM 日志缓冲区中的系统日志消息数量。

默认值

默认 ASDM 系统日志缓冲区大小为 100 条消息。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当 ASDM 日志缓冲区已满时， ASA 将删除最早的消息，以释放缓冲区空间供新消息使用。要控制是启用日志记录到 ASDM 日志缓冲区还是控制保留于 ASDM 日志缓冲区中的系统日志消息类型，请使用 **logging asdm** 命令。

ASDM 日志缓冲区是不同于使用 **logging buffered** 命令启用的日志缓冲区的缓冲区。

示例

以下示例演示如何启用日志记录、发送严重性级别 0、 1 和 2 的消息到 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
```

相关命令

命令	说明
clear logging asdm	清除包含的所有消息的 ASDM 日志缓冲区。
logging asdm	启用日志记录到 ASDM 日志缓冲区。
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示当前正在运行的日志记录配置。

logging buffered

要启用 ASA 向日志缓冲区发送系统日志消息，请在全局配置模式下使用 **logging buffered** 命令。要禁用日志记录到日志缓冲区，请使用此命令的 **no** 形式。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到日志缓冲区的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

默认值如下：

- 日志记录到缓冲区已禁用。
- 缓冲区大小为 4 KB。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在任何消息发送到日志缓冲区之前，您必须使用 **logging enable** 命令启用日志记录。

新消息将附加到缓冲区的末端。当缓冲区填充满时， ASA 将清除缓冲区并继续向其添加消息。当日志缓冲区已满时， ASA 将删除最早的消息，以释放缓冲区空间供新消息使用。每当缓冲区内容完成 “ 封装 ” 后，您都可自动保存缓冲区内容，这意味着自上次保存以来的所有消息都已替换成新消息。有关详细信息，请参阅 **logging flash-bufferwrap** 和 **logging ftp-bufferwrap** 命令。

您可随时将缓冲区内容保存到闪存中。有关详细信息，请参阅 **logging savelog** 命令。

您可使用 **show logging** 命令查看发送到缓冲区的系统日志消息。

示例

以下示例为严重性级别 0 和 1 的事件日志记录到缓冲区：

```
ciscoasa(config)# logging buffered alerts
ciscoasa(config)#
```

以下示例创建名为 “notif-list” 的列表，其中最大严重性级别为 7，并将为 “notif-list” 列表所标识的系统日志消息配置日志记录到缓冲区：

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffer-size	指定日志缓冲区大小。
logging enable	启用日志记录。
logging list	创建可重复使用的消息选择标准列表。
logging savelog	将日志缓冲区内容保存到闪存。

logging buffer-size

要指定日志缓冲区的大小，请在全局配置模式中使用 **logging buffer-size** 命令。要将日志缓冲区重置回其 4 KB 内存的默认大小，请使用此命令的 **no** 形式。

logging buffer-size *bytes*

no logging buffer-size *bytes*

语法说明

bytes	设置用于日志缓冲区的内存量，以字节为单位。例如，如果您指定为 8192，则 ASA 日志缓冲区将使用 8 KB 内存。

默认值

默认日志缓冲区大小为 4 KB 内存。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要查看 ASA 是否使用非默认缓冲区大小的日志缓冲区，请使用 **show running-config logging** 命令。如果未显示 **logging buffer-size** 命令，则 ASA 将使用 4 KB 日志缓冲区。

有关 ASA 如何使用缓冲区的详细信息，请参阅 **logging buffered** 命令。

示例

以下示例将启用日志记录、启用日志记录缓冲区，并指定 ASA 为日志缓冲区使用 16 KB 内存：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(config)#
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffered	启用日志记录到日志缓冲区。
logging enable	启用日志记录。
logging flash-bufferwrap	当日志缓冲区满时，将日志缓冲区写入闪存。
logging savelog	将日志缓冲区内容保存到闪存。

logging class

要根据日志记录目标为消息类配置最大严重性级别，请在全局配置模式中使用 **logging class** 命令。要删除消息类严重性级别配置，请使用此命令的 **no** 形式。

logging class *class destination level* [*destination level ...*]

no logging class *class*

语法说明

class	指定根据目标配置最大严重性级别的消息类。有关 *class* 的有效值，请参阅 “ 使用指南 ” 部分。
destination	为 *class* 指定日志记录目标。对于目标，*level* 将确定发送到 *destination* 的最大严重性级别。有关 *destination* 的有效值，请参阅以下 “ 使用指南 ” 部分。
level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、 2、 1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。

默认值

默认情况下， ASA 不会基于日志记录目标和消息类应用严重性级别。相反，每个启用的日志记录目标将在日志记录列表或启用日志记录目标时指定的严重性级别所确定的严重性级别，接收针对所有类的消息。

命令模式

下表将显示可输入命令的模式。

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	向有效的类值添加了 **eigrp**。
8.2(1)	向有效的类值添加了 **dap**。

使用指南

class 的有效值包括：

- **auth** - 用户身份验证。
- **bridge** - 透明防火墙。
- **ca** - PKI 证书颁发机构。
- **config** - 命令界面。
- **dap -** 动态访问策略。
- **eap** - 可扩展身份验证协议 (EAP)。记录以下事件类型，以支持网络准入控制：EAP 会话状态更改、 EAP 状态查询事件和 EAP 标头和数据包内容的十六进制转储。
- **eapoudp** - 基于 UDP 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 标头和数据包内容的完整记录。
- **eigrp** - EIGRP 路由。
- **email** - 电邮代理。
- **ha** - 故障切换。
- **ids -** 入侵检测系统。
- **ip** - IP 堆栈。
- **ipaa -** IP 地址分配
- **nac** - 网络准入控制。记录以下事件类型：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。
- **np** - 网络处理器。
- **ospf** - OSPF 路由。
- **rip** - RIP 路由。
- **rm** - 资源管理器。
- **session** - 用户会话。
- **snmp** - SNMP。
- **sys** - 系统。
- **vpn** - IKE 和 IPsec。
- **vpnc** - VPN 客户端。
- **vpnfo** - VPN 故障切换。
- **vpnlb** - VPN 负载平衡。

有效日志记录目标如下：

- **asdm** - 要了解有关此目标的信息，请参阅 **logging asdm** 命令。
- **buffered** - 要了解有关此目标的信息，请参阅 **logging buffered** 命令。
- **console** - 要了解有关此目标的信息，请参阅 **logging console** 命令。
- **history** - 要了解有关此目标的信息，请参阅 **logging history** 命令。
- **mail** - 要了解有关此目标的信息，请参阅 **logging mail** 命令。
- **monitor** - 要了解有关此目标的信息，请参阅 **logging monitor** 命令。
- **trap** - 要了解有关此目标的信息，请参阅 **logging trap** 命令。

示例

以下示例将指定：对于故障切换相关的消息， 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
```

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging console

要使 ASA 能够在控制台会话中显示系统日志消息，请在全局配置模式中使用 **logging console** 命令。要禁止在控制台会话中显示系统日志消息，请使用此命令的 **no** 形式。

logging console [*logging_list* | *level*]

no logging console

注　我们建议您不要使用此命令，因为它可能导致许多系统日志消息因缓冲区溢出而被丢弃。有关详细信息，请参阅 “ 使用指南 ” 部分。

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到控制台会话的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

默认情况下， ASA 将不会在控制台会话中显示系统日志消息。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在任何消息发送到控制台之前，您必须使用 **logging enable** 命令启用日志记录。

注意事项

使用 **logging console** 命令可显著降低系统性能。相反，应使用 **logging buffered** 命令启动日志记录，并使用 **show logging** 命令来查看消息。要更轻松地查看最新消息，请使用 **clear logging buffer** 命令来清除缓冲区。

示例

以下示例演示如何在控制台会话中显示严重性级别 0、 1、 2 和 3 的系统日志消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(config)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging list	创建可重复使用的消息选择标准列表。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging debug-trace

要将调试消息重定向到在严重性级别 7 签发的系统日志消息 711001，请在全局配置模式中使用 **logging debug-trace** 命令。要停止向日志发送调试日志消息，请使用此命令的 **no** 形式。

logging debug-trace

no logging debug-trace

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， ASA 不会在系统日志消息中包括调试输出。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

调试消息将作为严重性级别 7 的消息生成。它们将出现在系统日志消息编号 711001 的日志中，但不会出现在任何监控会话中。

示例

以下示例演示如何启用日志记录、发送日志消息到系统日志缓冲区、重定向调试输出至日志，以及开启磁盘活动的调试。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

以下是日志中可能出现的调试消息的输出示例：

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging device-id

要配置 ASA 在非 EMBLEM 格式系统日志消息中包括设备 ID，请在全局配置模式中使用 **logging device-id** 命令。要禁用使用设备 ID，请使用此命令的 **no** 形式。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

no logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

语法说明

cluster-id	在集群中指定单独 ASA 设备的唯一名称作为设备 ID。
hostname	指定 ASA 的主机名作为设备 ID。
ipaddress *interface_name*	在 *interface_name* 中指定设备 ID 或接口的 IP 地址。如果您使用 **ipaddress** 关键字，则发送到外部服务器的系统日志消息中将包括指定接口的 IP 地址，这与 ASA 向外部服务器发送日志数据所使用的接口无关。
string *text*	指定包含在 *text* 中作为设备 ID 的字符，最多可包含 16 个字符。您无法使用空白字符或任何以下字符： • & — 连字符 • ' — 单引号 • " — 双引号 • < — 小于号 • > — 大于号 • ? — 问号
系统	（可选）在集群环境中，规定成为接口上系统 IP 地址的设备 ID。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	**修改**
7.0(1)	引入了此命令。
9.0(1)	添加了 **cluster-id** 和 **system** 关键字。

使用指南

如果您使用 **ipaddress** 关键字，则设备 ID 将成为指定的 ASA 接口 IP 地址，这与消息发送的来源接口无关。此关键字为从设备发送的所有消息提供单个、一致的设备 ID。如果您使用 **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。

示例

以下示例演示如何配置名为 “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"
```

主机名将出现在系统日志消息的开始，如以下消息所示：

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging emblem

要对向除系统日志服务器以外的目标发送的日志消息使用 EMBLEM 格式，请在全局配置模式中使用 **logging emblem** 命令。要禁止使用 EMBLEM 格式，请使用此命令的 **no** 形式。

logging emblem

no logging emblem

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， ASA 不会对系统日志消息使用 EMBLEM 格式。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	此命令更改为独立于 **logging host** 命令。

使用指南

通过 **logging emblem** 命令，可为除系统日志服务器以外的所有日志记录目标启用 EMBLEM 格式的日志记录。如果您还启用了 **logging timestamp** 关键字，则将发送带时间戳的消息。

要为系统日志服务器启用 EMBLEM 格式日志记录，请使用 **logging host** 命令和 **format emblem** 选项。

示例

以下示例演示如何启用日志记录，并启用 EMBLEM 格式，从而日志记录到除系统日志服务器以外的所有日志记录目标：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging emblem
ciscoasa(config)#
```

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging enable

要为所有已配置的输出位置启用日志记录，请在全局配置模式中使用 **logging enable** 命令。要禁用日志记录，请使用此命令的 **no** 形式。

logging enable

no logging enable

语法说明

此命令没有任何参数或关键字。

默认值

日志记录默认将禁用。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	此命令从 **logging on** 命令更改而来。

使用指南

logging enable 命令用于启用或禁用向任何支持的日志记录目标发送系统日志消息。您也可使用 **no logging enable** 命令停止所有日志记录。

您可使用以下命令启用日志记录到个人日志记录目标：

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

示例

以下示例演示如何启用日志记录。 **show logging** 命令的输出显示为什么必须分别启用每个可能的日志记录目标：

```
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
```

相关命令

命令	说明
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging facility

要为发送到系统日志服务器的消息指定日志记录设施，请在全局配置模式中使用 **logging facility** 命令。要将日志记录设施重置为其默认值 20，请使用此命令的 **no** 形式。

logging facility *facility*

no logging facility

语法说明

facility	指定日志记录设施；有效值为 16 到 23。

默认值

默认设施为 20 (LOCAL4)。

命令模式

下表显示可输入命令的模式，语法说明部分所述的情况除外。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

系统日志服务器文件基于消息中的*设施*数量。有八个可能的设施：16 (LOCAL0) 到 23 (LOCAL7)。

示例

以下示例演示如何在系统日志消息中指定 ASA 将日志记录设施表示为 16。 **show logging** 命令的输出包括 ASA 正在使用的设施：

```
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
```

相关命令

命令	说明
logging enable	启用日志记录。
logging host	定义系统日志服务器。
logging trap	启用日志记录到系统日志服务器。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging flash-bufferwrap

要使 ASA 能够在缓冲区装满从未保存的消息时将日志缓冲区写入闪存，请在全局配置模式中使用 **logging flash-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。

logging flash-bufferwrap

no logging flash-bufferwrap

语法说明

此命令没有任何参数或关键字。

默认值

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。
- 最小可用闪存为 3 MB。
- 用于缓冲区日志记录的最大闪存分配是 1 MB。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使 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，日志缓冲区始终不将数据写入闪存。要启用日志记录到缓冲区，请使用 **logging buffered** 命令。

在 ASA 将日志缓冲区内容写入闪存时，它继续将任何新事件消息存储到日志缓冲区。

ASA 创建使用默认时间戳格式名称的日志文件，如下所示：

LOG-*YYYY-MM-DD-HHMMSS*.TXT

其中 *YYYY* 指年份， *MM* 指月份， *DD* 指月份中的天， *HHMMSS* 指时、分、秒。

闪存的可用性将影响 ASA 使用 **logging flash-bufferwrap** 命令保存系统日志消息的方式。有关详细信息，请参阅 **logging flash-maximum-allocation** 和 **logging flash-minimum-free** 命令。

示例

以下示例演示如何启用日志记录、启用日志缓冲区中，并启用 ASA 将日志缓冲区写入闪存：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)#
```

相关命令

命令	说明
clear logging buffer	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）。
logging buffered	启用日志记录到日志缓冲区。
logging buffer-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，请在全局配置模式中使用 **logging flash-maximum-allocation** 命令。要将此用途的最大闪存量重置为 1 MB 的默认大小，请使用此命令的 **no** 形式。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

语法说明

kbytes	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）。

默认值

日志数据的默认最大闪存分配容量为 1 MB。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令确定可用于 **logging savelog** 和 **logging flash-bufferwrap** 命令的闪存量。

如果由 **logging savelog** 或 **logging flash-bufferwrap** 保存的日志文件导致日志文件闪存使用超过 **logging flash-maximum-allocation** 命令所指定的最大容量，则 ASA 将删除最早的日志文件，以释放足够的内存用于新日志文件。如果没有要删除的文件或所有旧文件均已删除，所释放的内存对于新日志文件过小，则 ASA 无法保存新日志文件。

要查看 ASA 的最大闪存分配容量是否不同于默认大小，请使用 **show running-config logging** 命令。如果未显示 **logging flash-maximum-allocation** 命令，则 ASA 将为保存的日志缓冲区数据使用 1 MB 的最大量。分配的内存将同时用于 **logging savelog** 和 **logging flash-bufferwrap** 命令。

有关 ASA 如何使用日志缓冲区的详细信息，请参阅 **logging buffered** 命令。

示例

以下示例演示如何启用日志记录、启用日志缓冲区、启用 ASA 将日志缓冲区写入闪存，且用于写入日志文件的最大闪存量设置为约 1.2 MB 内存量：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-maximum-allocation 1200
ciscoasa(config)#
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffered	启用日志记录到日志缓冲区。
logging enable	启用日志记录。
logging flash-bufferwrap	当日志缓冲区满时，将日志缓冲区写入闪存。
logging flash-minimum-free	指定必须对 ASA 可用以允许将日志缓冲区写入闪存的最小闪存量。

logging flash-minimum-free

要指定必须在 ASA 保存新日志文件之前存在的最小可用闪存量，请在全局配置模式中使用 **logging flash-minimum-free** 命令。要将最低所需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。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

语法说明

kbytes	在 ASA 保存新日志文件之前必须可用的最小闪存量，以千字节为单位。

默认值

默认最小可用闪存量为 3 MB。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

logging flash-minimum-free 命令指定 **logging savelog** 和 **logging flash-bufferwrap** 命令必须随时保留多少闪存。

如果由 **logging savelog** 或 **logging flash-bufferwrap** 保存的日志文件将导致可用闪存量低于 **logging flash-minimum-free** 命令所指定的限制，则 ASA 将删除最早的日志文件，以确保在保存新日志文件后仍满足最低可用闪存量。如果没有要删除的文件，或删除所有旧文件后可用内存仍低于限制，则 ASA 无法保存新日志文件。

示例

以下示例演示如何启用日志记录、启用日志缓冲区、启用 ASA 将日志缓冲区写入闪存，并指定闪存的最低写入容量必须为 4000 KB：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(config)#
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffered	启用日志记录到日志缓冲区。
logging enable	启用日志记录。
logging flash-bufferwrap	当日志缓冲区满时，将日志缓冲区写入闪存。
logging flash-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 enable | disable

要启用 NetFlow 捕获的所有系统日志消息，请在全局配置模式中使用 **logging flow-export-syslogs enable** 命令。要禁用 NetFlow 捕获的所有系统日志消息，请在全局配置模式中使用 **logging flow-export-syslogs disable** 命令。

logging flow-export-syslogs {**enable** | **disable**}

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，启用 NetFlow 捕获的所有系统日志。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.1(1)	引入了此命令。

使用指南

如果配置了安全设备来导出 NetFlow 数据以提高性能，我们建议您输入 **logging flow-export-syslogs disable** 命令禁用冗余系统日志消息 （这些消息也由 NetFlow 捕获）。将禁用的系统日志消息如下所示：

系统日志消息	说明
106015	TCP 流量被拒绝，因为第一个数据包不是 SYN 数据包。
106023	通过 **access-group** 命令连接到接口的入口 ACL 或出口 ACL 拒绝的流。
106100	ACL 允许或拒绝的流。
302013 和 302014	TCP 连接和删除。
302015 和 302016	UDP 连接和删除
302017 和 302018	GRE 连接和删除。
302020 和 302021	ICMP 连接和删除。
313001	流向安全设备的 ICMP 数据包被拒绝。
313008	留向安全设备的 ICMPv6 数据包被拒绝。
710003	连接到安全设备的尝试被拒绝。

注　虽然这是一个配置模式命令，但它不会存储于配置中。只有 **no logging message xxxxxx** 命令才存储于配置中。

示例

以下示例演示如何禁用 NetFlow 捕获的冗余系统日志消息和显示的输出示例：

```
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* 是因通过 NetFlow 捕获了相同的信息而冗余的系统日志消息。该命令类似于命令别名，并将转换为一批 **no logging message xxxxxx** 命令。当您禁用系统日志消息后，您可使用 **logging message xxxxxx** 命令单独启用它们，其中 *xxxxxx* 指特定系统日志消息编号。

相关命令

命令	说明
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	指定 NetFlow 收集器的 IP 地址或主机名，以及 NetFlow 收集器正在监听的 UDP 端口。
flow-export template timeout-rate *minutes*	控制模板信息发送到 NetFlow 收集器的时间间隔。
show flow-export counters	显示 NetFlow 的一系列运行时间计数器。

logging from-address

要为 ASA 发送的系统日志消息指定发件人电邮地址，请在全局配置模式中使用 **logging from-address** 命令。所有发送的系统日志消息显示为来自您指定的地址。要删除发件人电邮地址，请使用此命令的 **no** 形式。

logging from-address *from-email-address*

no logging from-address *from-email-address*

语法说明

from-email-address	源电邮地址，即系统日志消息显示来自的电邮地址 （例如，cdb@example.com）。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

通过电邮发送系统日志消息由 **logging mail** 命令启用。

使用此命令指定的地址不需要对应现有电邮帐户。

示例

要启用日志记录并设置 ASA 通过电邮发送系统日志消息，请使用以下标准：

- 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消息。
- 向 admin@example.com 发送消息。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送消息。

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
```

相关命令

命令	说明
logging enable	启用日志记录。
logging mail	使 ASA 能够通过电邮发送系统日志消息，并确定哪些消息由电邮发送。
logging recipient-address	指定将系统日志消息发送到的电邮地址。
smtp-server	配置 SMTP 服务器。
show logging	显示已启用的日志记录选项。

logging ftp-bufferwrap

要使 ASA 能够在缓冲区装满从未保存的消息时将日志缓冲区发送到 FTP 服务器，请在全局配置模式中使用 **logging ftp-bufferwrap** 命令。要禁止向 FTP 服务器发送日志缓冲区，请使用此命令的 **no** 形式。

logging ftp-bufferwrap

no logging ftp-bufferwrap

语法说明

此命令没有任何参数或关键字。

默认值

默认值如下：

- 日志记录到缓冲区已禁用。
- 向 FTP 服务器发送日志缓冲区已禁用。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当您启用 **logging ftp-bufferwrap** 时， ASA 将向您通过 **logging ftp-serve** 命令指定的 FTP 服务器发送日志缓冲区数据。在 ASA 向 FTP 服务器发送日志数据时，它仍将任何新的事件消息存储到日志缓冲区中。

要使 ASA 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，日志缓冲区始终不将数据写入闪存。要启用日志记录到缓冲区，请使用 **logging buffered** 命令。

ASA 创建使用默认时间戳格式名称的日志文件，如下所示：

LOG-*YYYY-MM-DD-HHMMSS*.TXT

其中 *YYYY* 指年份， *MM* 指月份， *DD* 指月份中的天， *HHMMSS* 指时、分、秒。

示例

以下示例演示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器，并启用 ASA 将日志缓冲区写入 FTP 服务器。示例将指定主机名为 logserver-352 的 FTP 服务器。可使用用户名 logsupervisor 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)#
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffered	启用日志记录到日志缓冲区。
logging buffer-size	指定日志缓冲区大小。
logging enable	启用日志记录。
logging ftp-server	使用 **logging ftp-bufferwrap** 命令指定要使用的 FTP 服务器参数。

logging ftp-server

要指定 ASA 在 **logging ftp-bufferwrap** 启用时将日志缓冲区数据发送到的 FTP 服务器的详细信息，请在全局配置模式中使用 **logging ftp-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。

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

语法说明

0	（可选）指定将遵循的未加密的 （明文）用户密码。
8	（可选）指定将遵循的加密的用户密码。
ftp-server	外部 FTP 服务器的 IP 地址或主机名。 **注**　如果您指定主机名，请确保 DNS 在您的网络中工作正常。
password	指定用户名的密码，最多可包含 64 个字符。
path	供保存日志缓冲区数据的 FTP 服务器目录路径。此路径相对于 FTP 的根目录。例如： `/security_appliances/syslogs/appliance107`
username	适用于日志记录到 FTP 服务器的用户名。

默认值

默认情况下，不会指定 FTP 服务器。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.3(1)	添加了密码加密支持。

使用指南

您仅可指定一台 FTP 服务器。如果已经指定日志记录 FTP 服务器，请使用 **logging ftp-server** 命令将此 FTP 服务器配置替换为您所输入的新配置。

ASA 不会验证您指定的 FTP 服务器信息。如果您错误配置了任何详细信息，则 ASA 将无法向 FTP 服务器发送日志缓冲区数据。

在启动或升级 ASA 期间，不支持个位数密码，以及以数字开始且其后有空格的密码。例如， 0 pass 和 1 均为无效密码。

示例

以下示例演示如何启用日志记录、启用日志缓冲区、指定 FTP 服务器，并启用 ASA 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 访问该服务器。日志文件存储在 /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
```

以下示例演示如何输入加密密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

以下示例演示如何输入未加密 （明文）密码：

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

相关命令

命令	说明
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
logging buffered	启用日志记录到日志缓冲区。
logging buffer-size	指定日志缓冲区大小。
logging enable	启用日志记录。
logging ftp-bufferwrap	日志缓冲区已满时，向 FTP 服务器发送日志缓冲区。

logging history

要启用 SNMP 日志记录，并指定哪些消息将发送到 SNMP 服务器，请在全局配置模式中使用 **logging history** 命令。要禁用 SNMP 日志记录，请使用此命令的 **no** 形式。

logging history [*logging_list* | *level*]

no logging history

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到 SNMP 服务器的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

默认情况下， ASA 不会记录到 SNMP 服务器。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

logging history 命令可让您启用日志记录到 SNMP 服务器，并设置 SNMP 消息级别或事件列表。

示例

以下示例演示如何启用 SNMP 日志记录，并指定严重性级别 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)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging list	创建可重复使用的消息选择标准列表。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。
snmp-server	指定 SNMP 服务器详细信息。

logging host

要定义系统日志服务器，请在全局配置模式中使用 **logging host** 命令。要删除系统日志服务器定义，请使用此命令的 **no** 形式。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

no logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

语法说明

format emblem	（可选）为系统日志服务器启用 EMBLEM 格式日志记录。
interface_name	指定系统日志服务器驻留的接口。
port	指示系统日志服务器用于侦听消息的端口。对于每个协议，有效的端口值介于 1025 到 65535 之间。如果您输入零作为端口号，或使用无效的字符或符号，则将发生错误。
secure	（可选）指定与远程日志记录主机的连接应使用 SSL/TLS。此选项仅在选定协议为 TCP 时有效。 **注**　仅可使用支持 SSL/TLS 的系统日志服务器来建立安全日志记录连接。如果无法建立 SSL/TLS 连接，则所有新连接将被拒绝。可通过输入 **logging permit-hostdown** 命令来更改此默认行为。
syslog_ip	指定系统日志服务器的 IP 地址。
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 将消息发送到系统日志服务器。

默认值

默认协议是 UDP。

format emblem 选项的默认设置是 false。

secure 选项的默认设置是 false。

默认端口号如下：

- UDP—514
- TCP — 1470

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0	引入了此命令。
8.0(2)	添加了 **secure** 关键字。
8.4(1)	可启用和禁用连接屏蔽。

使用指南

logging host *syslog_ip* **format emblem** 命令用于为每个系统日志服务器启用 EMBLEM 格式记录。EMBLEM 格式日志记录仅可用于 UDP 系统日志消息。如果您为某特定系统日志服务器启用 EMBLEM 格式日志记录，则将向该服务器发送消息。如果您使用 **logging timestamp** 命令，则还将发送带时间戳的消息。

您可使用多个 **logging host** 命令指定将接收系统日志消息的所有其他服务器。但是，您只能指定一台服务器来接收 UDP 或 TCP 系统日志消息，而非同时接收两者。

如果配置了 **logging host** 命令来使用 TCP 向系统日志服务器发送消息，则将开启屏蔽连接的默认设置。如果配置了基于 TCP 的系统日志服务器，则您可使用 **logging permit-hostdown** 命令禁用连接屏蔽。

注　在 **logging host** 命令中使用 **tcp** 选项时，如果无法访问系统日志服务器，则 ASA 将放弃跨防火墙的连接。

您可通过使用 **show running-config logging** 命令并在列表中查找命令 （TCP 列为 6， UDP 列为 17）来仅显示*端口*和*协议*值。 TCP 端口只能用于系统日志服务器。*端口*必须是系统日志服务器用于侦听的端口。

注　如果您尝试将 UDP 与 **logging host** 命令和 **secure** 关键字结合使用，则将出现一条错误消息。

不支持在备用 ASA 上通过 TCP 发送系统日志。

示例

以下示例演示如何向使用默认协议和端口号的内部接口上的系统日志服务器发送严重性级别 0、1、 2 和 3 的系统日志消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging trap	启用日志记录到系统日志服务器。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging list

要创建用于其他命令的日志记录列表，以便指定按不同条件 （日志记录级别、事件类和消息 ID）划分的消息，请在全局配置模式中使用 **logging list** 命令。要删除列表，请使用此命令的 **no** 形式。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

语法说明

class *event_class*	（可选）为系统日志消息设置事件类。对于指定的级别，该命令仅标识指定类的系统日志消息。请参阅 “ 使用指南 ” 部分了解类列表的信息。
level *level*	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
message *start_id*[**-***end_id*]	指定消息 ID 或 ID 范围。要查找一条消息的默认级别，使用 **show logging** 命令或查看系统日志消息指南。
name	设置日志记录列表的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

可使用列表的日志记录命令如下：

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class 可能的值包括：

- **auth** - 用户身份验证。
- **bridge** - 透明防火墙。
- **ca** - PKI 证书颁发机构。
- **config** - 命令界面。
- **eap** - 可扩展身份验证协议 (EAP)。记录以下事件类型，以支持网络准入控制：EAP 会话状态更改、 EAP 状态查询事件和 EAP 标头和数据包内容的十六进制转储。
- **eapoudp** - 基于 UDP 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 标头和数据包内容的完整记录。
- **email** - 电邮代理。
- **ha** - 故障切换。
- **ids -** 入侵检测系统。
- **ip** - IP 堆栈。
- **nac** - 网络准入控制。记录以下事件类型：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。
- **np** - 网络处理器。
- **ospf** - OSPF 路由。
- **rip** - RIP 路由。
- **session** - 用户会话。
- **snmp** - SNMP。
- **sys** - 系统。
- **vpn** - IKE 和 IPSec。
- **vpnc** - VPN 客户端。
- **vpnfo** - VPN 故障切换。
- **vpnlb** - VPN 负载平衡。

示例

以下示例演示如何使用日志记录列表命令：

```
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
```

之前的示例表明与指定标准匹配的系统日志消息将发送到日志记录缓冲区。此示例中指定的标准是：

- 100100 到 100110 之间的系统日志消息 ID
- 关键级别或更高级别的所有系统日志消息 （紧急、警报或关键）
- 警告级别或更高级别的所有 VPN 类系统日志消息 （紧急、警报、关键、错误或警告）

如果系统日志消息满足以下标准之一，则它将记录到缓冲区。

注　在设计列表标准时，标准可指定重叠消息集。通常将记录与一个以上的标准组匹配的系统日志消息。

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging mail

要使 ASA 能够通过电邮发送系统日志消息并确定哪些消息由电邮发送，请在全局配置模式中使用 **logging mail** 命令。要禁止用电邮发送系统日志消息，请使用此命令的 **no** 形式。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到电邮收件人的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

默认为禁用日志记录到电邮。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

通过电邮发送的系统日志消息将出现于已发送的电邮主题行中。

示例

要设置 ASA 通过电邮发送系统日志消息，请使用以下标准：

- 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消息。
- 向 admin@example.com 发送消息。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送消息。

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
```

相关命令

命令	说明
logging enable	启用日志记录。
logging from-address	指定通过电邮发送的系统日志消息显示的发件人电邮地址。
logging list	创建可重复使用的消息选择标准列表。
logging recipient-address	指定通过电邮发送的系统日志消息的收件人的电邮地址。
smtp-server	配置 SMTP 服务器。

logging message

要指定系统日志消息的日志记录级别，请在全局配置模式中使用带 **level** 关键字的 **logging message** 命令。要将消息的日志记录级别重置为默认级别，请使用此命令的 **no** 形式。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

语法说明

level *level*	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
syslog_id	您希望启用或禁用或您希望修改其严重性级别的系统日志消息的 ID。要查找一条消息的默认级别，使用 **show logging** 命令或查看系统日志消息指南。

默认值

默认情况下，所有系统日志消息都已启用，所有消息的严重性级别均设置为其默认级别。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可将 **logging message** 命令用于以下用途：

- 指定消息是启用还是禁用。
- 指示消息的严重性级别。

您可使用 **show logging** 命令来确定当前已分配到消息的级别，以及是否已启用消息。

要防止 ASA 生成特定系统日志消息，请在全局配置模式中使用 **ogging message** 命令（不含 **level** 关键字）命令的 **no** 形式。要让 ASA 生成特定系统日志消息，请使用 **logging message** 命令（不含 **level** 关键字）。您可同时使用 **logging message** 命令的两个版本。

示例

以下示例中的命令系列将演示使用 **logging message** 命令指定是否启用消息和消息的严重性级别：

```
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 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

相关命令

命令	说明
clear configure logging	清除所有日志记录配置或仅清除消息配置。
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging monitor

要使 ASA 能够在 SSH 和 Telnet 会话中显示系统日志消息，请在全局配置模式中使用 **logging monitor** 命令。要禁止在 SSH 和 Telnet 会话中显示系统日志消息，请使用此命令的 **no** 形式。

logging monitor [*logging_list* | *level*]

no logging monitor

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到 SSH 和 Telnet 会话的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

ASA 默认情况下，不会在 SSH 和 Telnet 会话中显示系统日志消息。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

logging monitor 命令将在当前情景中为所有会话启用系统日志消息；但在每个会话中，**terminal** 命令控制是否在该会话中显示系统日志消息。

示例

以下示例演示如何在控制台会话中显示系统日志消息。使用 **errors** 关键字表明消息的严重性级别 0、 1、 2 和 3 应显示在 SSH 和 Telnet 会话中。 **terminal** 命令将在当前会话中显示消息：

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging list	创建可重复使用的消息选择标准列表。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。
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不相关，请在全局配置模式中使用 **logging permit-hostdown** 命令。要让 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。

logging permit-hostdown

no logging permit-hostdown

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，如果已启用日志记录到使用 TCP 连接的系统日志服务器，则 ASA 将在系统日志服务器因任何原因不可用时不允许新网络访问会话。 **logging permit-hostdown** 命令的默认设置为 false。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您使用 TCP 作为向系统日志服务器发送消息的日志记录传输协议，且 ASA 无法访问系统日志服务器，则 ASA 将拒绝新网络访问会话作为一种安全措施。您可使用 **logging permit-hostdown** 命令删除此限制。

示例

以下示例将让基于 TCP 的系统日志服务器状态与 ASA 是否允许新会话无关。 **logging permit-hostdown** 命令在其输出中包含 **show running-config logging** 命令时，基于 TCP 的系统日志服务器状态将与新网络访问会话无关。

```
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)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging host	定义系统日志服务器。
logging trap	启用日志记录到系统日志服务器。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging queue

要指定 ASA 在根据日志记录配置处理系统日志消息之前可在其队列中保持系统日志消息的数量，请在全局配置模式中使用 **logging queue** 命令。要将日志记录队列大小重置为 512 条消息的默认值，请使用此命令的 **no** 形式。

logging queue *queue_size*

no logging queue *queue_size*

语法说明

queue_size	处理之前队列中允许用于存储系统日志消息的系统日志消息数。有效值根据平台类型的不同而介于 0 到 8192 条消息之间。如果日志记录队列设为零，则队列将为最大可配置的大小（8192 条消息），具体取决于平台。在 ASA-5505 上，最大的队列大小是 1024 条。在 ASA-5510 上，最大的队列大小为 2048 条，在所有其他平台上，最大队列大小为 8192 条。

默认值

默认队列大小为 512 条消息。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当流量较大导致队列排满时，ASA 可能会丢弃消息。在 ASA 5505 上，最大队列大小是 1024 条。在 ASA-5510 上，最大队列大小为 2048 条。对于所有其他平台，最大队列大小为 8192 条。

示例

以下示例演示如何显示 **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.
```

在此示例中，**logging queue** 命令设为 0，这意味着队列设置为最大值 8192。队列中的系统日志消息由 ASA 按照日志记录配置中表述的方式处理，例如将系统日志消息发送到邮件收件人，将它们保存到闪存等。

在此示例 **show logging queue** 命令的输出中显示有 5 条消息正在排队等候，3513 条消息是自 ASA 上次启动之后一次排队等候的最大消息数量，另外有 1 条消息已丢弃。尽管队列设置为不受限制的消息，但仍有消息已丢弃，因为没有数据块内存可用于将消息添加到队列中。

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging rate-limit

要限制系统日志消息生成的速率，请在特权 EXEC 模式中使用 **logging rate-limit** 命令。要禁用速率限制，请在特权 EXEC 模式中使用此命令的 **no** 形式。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

语法说明

interval	（可选）用于测量消息生成速率的时间间隔 （以秒为单位）。有效的 *interval* 值范围介于 0 到 2147483647 之间。
level *severity_level*	对所有属于特定严重性级别的系统日志消息应用速率限制。指定严重性级别的所有系统日志消息都是单独限速的。*Severity_level* 的有效范围是 1 到 7。
message	禁止报告此系统日志消息。
num	在指定的时间间隔中可生成的系统日志消息数量。有效的 *num* 值范围是 0 到 2147483647。
syslog_id	要禁止的系统日志消息 ID。有效值范围介于 100000 到 999999 之间。
unlimited	禁用速率限制，这意味着日志记录速率不受限制。

默认值

interval 的默认设置为 1。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

系统日志消息的严重性级别如下所示：

- 0 - 系统不可用
- 1 - 需要立即采取行动
- 2 - 严重情况
- 3 - 错误情况
- 4 - 警告情况
- 5 - 正常，但有重要的情况
- 6 - 信息性消息
- 7 - 调试消息

示例

要限制系统日志消息生成的速率，您可输入特定的消息 ID。以下示例显示如何使用特定的消息 ID 和时间间隔，限制系统日志消息生成的速率：

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

此示例禁止系统日志消息 302020 在指定的时间间隔 600 秒中达到 100 的速率限制之后向主机发送。

要限制系统日志消息生成的速率，您可输入特定的严重性级别。以下示例演示如何使用特定的严重性级别和时间间隔，限制系统日志消息生成的速率。

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

此示例在指定时间间隔 600 秒内，将严重性级别 6 以下的所有系统日志消息禁止为指定速率限制 1000。严重性级别 6 中的每个系统日志消息的速率限制为 1000。

相关命令

命令	说明
clear running-config logging rate-limit	将日志记录速率限制重置为其默认值。
show logging	在内部缓冲区或日志记录配置中显示当前消息。
show running-config logging rate-limit	显示当前日志记录速率限制设置。

logging recipient-address

要为 ASA 发送的系统日志消息指定接收电邮地址，请在全局配置模式中使用 **logging recipient-address** 命令。要删除接收电邮地址，请使用此命令的 **no** 形式。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

语法说明

address	通过电邮发送系统日志消息时，请指定收件人电邮地址。
level	表示遵循的严重性级别。
level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、2、1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。 **注**　我们不建议将大于 3 的严重性级别与 **logging recipient-address** 命令结合使用。更高的严重性级别很可能会因缓冲区溢出造成系统日志消息丢弃。 **logging recipient-address** 命令指定的消息严重性级别将覆盖 **logging mail** 命令所指定的消息严重性级别。例如，如果 **logging recipient-address** 命令指定严重性级别为 7，但 **logging mail** 命令指定严重性级别为 3，则 ASA 将所有消息发送给收件人，其中包括严重性级别 4、5、6 和 7。

默认值

默认值设置为错误日志记录级别。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可配置最多 5 个收件人地址。如有需要，每个收件人地址可拥有不同于通过 **logging mail** 命令所指定的消息级别。通过电邮发送系统日志消息由 **logging mail** 命令启用。

使用此命令将更紧急的消息发送给更多收件人。

示例

要设置 ASA 通过电邮发送系统日志消息，请使用以下标准：

- 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消息。
- 向 admin@example.com 发送消息。
- 使用 SMTP、主要服务器 pri-smtp-host 和辅助服务器 sec-smtp-host 发送消息。

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
```

相关命令

命令	说明
logging enable	启用日志记录。
logging from-address	指定系统日志消息所显示的发件人电邮地址。
logging mail	使 ASA 能够通过电邮发送系统日志消息，并确定哪些消息由电邮发送。
smtp-server	配置 SMTP 服务器。
show logging	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，请在特权 EXEC 模式中使用 **logging savelog** 命令。

logging savelog [*savefile*]

语法说明

savefile	（可选）已保存的闪存文件名称。如果您未指定文件名，则 ASA 将使用如下所示的默认时间戳格式保存日志文件： LOG-*YYYY-MM-DD-HHMMSS*.TXT 其中 *YYYY* 指年份， *MM* 指月份， *DD* 指月份中的天， *HHMMSS* 指时、分、秒。

默认值

默认值如下：

- 缓冲区大小为 4 KB。
- 最小可用闪存为 3 MB。
- 用于缓冲区日志记录的最大闪存分配是 1 MB。
- 默认日志文件名称在 “ 语法说明 ” 部分中说明。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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。要启用日志记录到缓冲区，请使用 **logging buffered** 命令。

注　**logging savelog** 命令不会清除缓冲区。要清除缓冲区，请使用 **clear logging buffer** 命令。

示例

以下示例将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#
```

相关命令

命令	说明
clear logging buffer	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）。
logging buffered	启用日志记录到日志缓冲区。
logging enable	启用日志记录。

logging standby

要使故障切换备用 ASA 能够将系统日志消息发送到日志记录目标，请在全局配置模式中使用 **logging standby** 命令。要禁用系统日志消息和 SNMP 日志记录，请使用此命令的 **no** 形式。

logging standby

no logging standby

语法说明

此命令没有任何参数或关键字。

命令默认

默认情况下，将禁用 logging standby 命令。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可启用 **logging standby** 命令，以确保故障切换备用 ASA 的系统日志消息在发生故障切换时保持同步。

注　使用 **logging standby** 命令将导致共享日志记录目标 （如系统日志服务器、 SNMP 服务器和 FTP 服务器）上的流量翻倍。

示例

以下示例使 ASA 能够向故障切换备用 ASA 发送系统日志信息。 **show logging** 命令的输出表明已启用此功能：

```
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
```

相关命令

命令	说明
failover	启用故障切换功能。
logging enable	启用日志记录。
logging host	定义系统日志服务器。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging timestamp

要指定系统日志消息应包括生成消息的日期和时间，请在全局配置模式中使用 **logging timestamp** 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。

logging timestamp

no logging timestamp

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， ASA 不会在系统日志消息中包括日期和时间。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

logging timestamp 命令将让 ASA 在所有系统日志消息中包含时间戳。

示例

以下示例将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)#
```

相关命令

命令	说明
logging enable	启用日志记录。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

logging trap

要指定 ASA 向系统日志服务器发送的系统日志消息，请在全局配置模式中使用 **logging trap** 命令。要从配置中删除此命令，请使用此命令的 **no** 形式。

logging trap [*logging_list* | *level*]

no logging trap

语法说明

level	为系统日志消息设置最大严重性级别。例如，如果您将严重性级别设置为 3，则 ASA 将为严重性级别 3、 2、 1 和 0 生成系统日志消息。您可指定编号或名称，如下所示： • **0** 或 **emergencies** - 系统不可用。 • **1** 或 **alerts** - 需要立即采取行动。 • **2** 或 **critical** - 严重情况。 • **3** 或 **errors** - 错误情况。 • **4** 或 **warnings** - 警告情况。 • **5** 或 **notifications** - 正常，但有重要情况。 • **6** 或 **informational** - 信息性消息。 • **7** 或 **debugging** - 调试消息。
logging_list	指定标识将消息发送到系统日志服务器的列表。有关创建列表的信息，请参阅 **logging list** 命令。

默认值

未定义默认系统日志消息陷阱。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您正在使用 TCP 作为日志记录传输协议，且 ASA 无法访问系统日志服务器，系统日志服务器配置不正确，或磁盘已满，则 ASA 将拒绝新网络访问会话作为安全措施。

如果系统日志服务器发生故障，基于 UDP 的日志记录也无法阻止 ASA 传递流量。

示例

以下示例演示如何向驻留于内部接口、使用默认协议和端口号的系统日志服务器发送严重性级别 0、 1、 2 和 3 的系统日志消息。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

相关命令

命令	说明
logging enable	启用日志记录。
logging host	定义系统日志服务器。
logging list	创建可重复使用的消息选择标准列表。
show logging	显示已启用的日志记录选项。
show running-config logging	显示运行配置的日志记录相关部分。

login

要使用本地用户数据库 （请参阅 username 命令）登录特权 EXEC 模式，或更改用户名，请在用户 EXEC 模式中使用 **login** 命令。

login

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在用户 EXEC 模式中，您可使用 **login** 命令，以本地数据库中的任何用户名登录特权 EXEC 模式。当您启用身份验证时 （请参阅 **aaa authentication console** 命令）， **login** 命令与 **enable** 命令相似。与启用身份验证不同， **login** 命令只能使用本地用户名数据库，而身份验证则始终需要使用此命令。您还可使用 **login** 命令从任何 CLI 模式更改用户。

要允许用户在登录时访问特权 EXEC 模式 （和所有命令），请将用户特权级别设置为 2 （默认值）到 15 之间。如果您配置了本地命令授权，则用户仅可输入分配到该权限级别或更低级别的命令。请参阅 **aaa authorization command** 了解详细信息。

注意事项

如果您将可访问 CLI 的用户及您不希望其进入特权 EXEC 模式的用户添加到本地数据库，则您应配置命令授权。如果没有命令授权，而用户的特权级别为 2 或大于 2（2 为默认值），则用户可在 CLI 使用其密码访问特权 EXEC 模式 （和所有命令）。或者，您可使用 RADIUS 或 TACACS+ 身份验证，也可将所有本地用户设置为 1 级，从而控制可使用系统启用密码访问特权 EXEC 模式的用户。

示例

以下示例将演示您在输入 **login** 命令后的提示：

```
ciscoasa> login
Username:
```

相关命令

命令	说明
aaa authorization command	为 CLI 访问启用命令授权。
aaa authentication console	需要对控制台、Telnet、HTTP、SSH 或 **enable** 命令访问进行身份验证。
logout	注销 CLI。
username	将用户添加到本地数据库。

login-button

要定制 WebVPN 用户连接安全设备时所看到的 WebVPN 页面登录框中的登录按钮，请在 webvpn 定制配置模式中使用 **login-button** 命令。要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

语法说明

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

默认值

默认登录按钮文本是 Login （登录）。

默认登录按钮样式是：

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

以下示例定制文本 “OK” 与登录按钮：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

相关命令

命令	说明
login-title	定制 WebVPN 页面登录框标题。
group-prompt	定制 WebVPN 页面登录框组提示。
password-prompt	定制 WebVPN 页面登录框密码提示。
username-prompt	定制 WebVPN 页面登录框用户名提示。

login-message

要定制 WebVPN 用户连接安全设备时所看到的 WebVPN 页面登录消息，请从 webvpn 定制配置模式中使用 **login-message** 命令。要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

语法说明

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

默认值

默认登录消息是 Please enter your username and password （请输入您的用户名和密码）。

默认登录消息样式为背景颜色：background-color:#CCCCCC;color:black。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

在以下示例中，将登录消息文本设置为 username and password （用户名和密码）：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

相关命令

命令	说明
login-title	定制 WebVPN 页面上登录对话框的标题。
username-prompt	定制 WebVPN 页面登录用户名提示。
password-prompt	定制 WebVPN 页面登录密码提示。
group-prompt	定制 WebVPN 页面登录组提示。

login-title

要定制向 WebVPN 用户显示的 WebVPN 页面上的登录对话框标题，请在 webvpn 定制配置模式中使用 **login-title** 命令。要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

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

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

语法说明

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）或级联样式表 (CSS) 参数 （最多 256 个字符）。

默认值

默认登录文本是 Login （登录）。

登录标题的默认 HTML 样式是：background-color: #666666; color: white。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

以下示例将配置登录标题样式：

```
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
```

相关命令

命令	说明
login-message	定制 WebVPN 登录页面登录消息。
username-prompt	定制 WebVPN 登录页面用户名提示。
password-prompt	定制 WebVPN 登录页面密码提示。
group-prompt	定制 WebVPN 登录页面组提示。

logo

要定制 WebVPN 用户连接安全设备时所看到的 WebVPN 页面徽标，请在 webvpn 定制配置模式中使用 **logo** 命令。要从配置中删除徽标并重置回默认值 （思科徽标），请使用此命令的 **no** 形式。

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

语法说明

file	表示您正在提供包含徽标的文件。
none	表示无徽标。设置空值，从而禁止使用徽标。防止继承徽标。
path	文件名的路径。可以使用的路径是 disk0:、 disk1: 或 flash:
value	指定徽标的文件名。最大长度为 255 个字符，不含空格。文件类型必须是 JPG、 PNG、 GIF，且必须小于 100 KB。

默认值

默认徽标是思科徽标。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

如果您指定的文件名不存在，则将显示一条错误消息。如果您删除徽标文件，但仍有配置指向它，则不显示徽标。

文件名不能包含空格。

示例

在以下示例中，文件 cisco_logo.gif 包含定制徽标：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

相关命令

命令	说明
title	定制 WebVPN 页面标题。
page style	定制使用层叠样式表 (CSS) 参数的 WebVPN 页面。

logout

要从 CLI 退出，请在用户 EXEC 模式中使用 **logout** 命令。

logout

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

logout 命令可让您从 ASA 注销。您可使用 **exit** 或 **quit** 命令返回到非特权模式。

示例

以下示例显示如何从 ASA 注销：

```
ciscoasa> logout
```

相关命令

命令	说明
login	启动登录提示。
exit	退出访问模式。
quit	退出配置或特权模式。

logout-message

要定制 WebVPN 用户从 WebVPN 服务注销时看到的 WebVPN 注销屏幕注销消息，请在 webvpn 定制配置模式中使用 **logout-message** 命令。要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

语法说明

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

默认值

默认注销消息文本为 Goodbye （再见）。

默认注销消息样式为：background-color:#999999;color:black。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

以下示例将配置注销消息样式：

```
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
```

相关命令

命令	说明
logout-title	定制 WebVPN 页面注销标题。
group-prompt	定制 WebVPN 页面登录框组提示。
password-prompt	定制 WebVPN 页面登录框密码提示。
username-prompt	定制 WebVPN 页面登录框用户名提示。

mac address 至 match dscp 命令

mac address

要为主用设备和备用设备指定虚拟 MAC 地址，请在故障切换组配置模式下使用 **mac address** 命令。要恢复默认虚拟 MAC 地址，请使用此命令的 **no** 形式。

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

语法说明

phy_if	要设置 MAC 地址的接口的物理名称。
active_mac	主用设备的虚拟 MAC 地址。必须以 h.h.h 格式输入 MAC 地址，其中 h 是一个 16 位的十六进制数字。
standby_mac	备用设备的虚拟 MAC 地址。必须以 h.h.h 格式输入 MAC 地址，其中 h 是一个 16 位的十六进制数字。

默认值

默认值如下：

- 主用设备的默认 MAC 地址：00a0.c9*physical_port_number.failover_group_id*01。
- 备用设备的默认 MAC 地址：00a0.c9*physical_port_number.failover_group_id*02。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果没有为故障切换组定义虚拟 MAC 地址，则使用默认值。

如果您在同一网络中有不止一个主用 / 主用故障切换对，则根据确定默认虚拟 MAC 地址的方法，很可能分配给某一对接口的默认虚拟 MAC 地址与分配给其他对接口的默认虚拟 MAC 地址相同。为避免您的网络中出现重复的 MAC 地址，请确保为每个物理接口都分配虚拟主用 MAC 地址和备用 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，则使用的 MAC 地址取决于许多变量，因而可能无法预测。

示例

下面的部分示例显示了故障切换组的可能配置：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
failover mac address	为物理接口指定虚拟 MAC 地址。

mac-address

要给接口或子接口手动分配专用 MAC 地址，请在接口配置模式下使用 **mac-address** 命令。在多情景模式中，此命令可以给每个情景中的接口分配一个不同的 MAC 地址。对于集群中的单个接口，您可以分配一个 MAC 地址集群池。要恢复到默认的 MAC 地址，请使用此命令的 **no** 形式。

mac-address {*mac_address* [**standby** *mac_address*] | **cluster-pool** *pool_name*}

no mac-address [*mac_address* [**standby** *mac_address*] | **cluster-pool** *pool_name*]

语法说明

cluster-pool *pool_name*	对于单个接口模式中的集群 （参见 **cluster interface-mode** 命令），或者对于任何集群接口模式中的管理接口，可设置一个 MAC 地址池以用于每个集群成员上的指定接口。使用 **mac-address pool** 命令定义池。
mac_address	以 H.H.H 格式为此接口设置 MAC 地址，其中 H 是一个 16 位的十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 将输入为 000C.F142.4CDE。如果使用故障切换，则此 MAC 地址是主用 MAC 地址。 **注**　由于自动生成的地址 （**mac-address auto** 命令）以 A2 开头，所以如果您也要使用自动生成，则不能让手动 MAC 地址以 A2 开头。
standby *mac_address*	（可选）为故障切换设置备用 MAC 地址。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用活动 MAC 地址以最小化网络中断，而旧的主用设备使用备用地址。

默认值

默认 MAC 地址是物理接口的固化 MAC 地址。子接口继承物理接口 MAC 地址。有些命令设置物理接口 MAC 地址 （将此命令包含在单模式中），因此继承的地址取决于该配置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(5)/8.2(2)	当还与 **mac-address auto** 命令一起使用时，MAC 地址不能以 A2 开头。
9.0(1)	我们添加了 **cluster-pool** 关键字来支持集群。

使用指南

在多情景模式中，如果在情景之间共享一个接口，您可以为每个情景中的此接口分配一个唯一 MAC 地址。此功能让 ASA 轻松地将数据包分类到适当的情景中。共享接口也可以不使用唯一 MAC 地址，但会有一些限制。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，或者使用 **mac-address auto** 命令为情景中的共享接口自动生成 MAC 地址。如果自动生成 MAC 地址，您可以使用 **mac-address** 命令覆盖生成的地址。

对于单情景模式，或者多情景模式中不共享的接口，您可能想要给子接口分配唯一 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，则使用的 MAC 地址取决于许多变量，因而可能无法预测。

示例

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
```

相关命令

命令	说明
failover mac address	为主用 / 备用故障切换设置物理接口的主用和备用 MAC 地址。
mac address	为主用 / 主用故障切换设置物理接口的主用和备用 MAC 地址。
mac-address auto	为多情景模式中的共享接口自动生成 MAC 地址 （主用和备用）。
mode	将安全情景模式设置为多或单模式。
show interface	显示接口特征，包括 MAC 地址。

mac-address auto

要给每个共享情景接口自动分配专用 MAC 地址，请在全局配置模式下使用 **mac-address auto** 命令。要禁用自动 MAC 地址，请使用此命令的 **no** 形式。

mac-address auto [**prefix** *prefix*]

no mac-address auto

语法说明

prefix *prefix*	（可选）设置一个用户定义的前缀作为 MAC 地址的一部分。*prefix* 是一个介于 0 和 65535 之间的十进制数值。如果不输入前缀，则 ASA 生成一个默认前缀。 此前缀被转换为一个 4 位的十六进制数字。前缀可确保每个 ASA 使用唯一 MAC 地址 （使用不同的前缀值），因此 （比如说）在某个网段可以具有多个 ASA。

默认值

自动 MAC 地址生成已启用 — 使用一个自动生成的前缀。 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。您无法使用传统的自动生成方法 （无前缀）。

如果禁用 MAC 地址生成，请参阅以下默认 MAC 地址：

- 对于 ASA 5500 系列设备 — 物理接口使用固化 MAC 地址，且该物理接口的所有子接口也使用同一固化 MAC 地址。
- 对于 ASASM — 所有 VLAN 接口都使用同一 MAC 地址，源自背板 MAC 地址。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(5)/8.2(2)	增加了 **prefix** 关键字。 MAC 地址格式更改为使用前缀，以便为故障切换对中的主和辅设备 MAC 地址使用固定的开头值 (A2) 以及使用不同的方案。现在，在重新加载时 MAC 地址保持不变。命令解析器现在检查自动生成是否已启用；如果您也想手动分配 MAC 地址，则不能让手动 MAC 地址以 A2 开头。

版本	修改
8.5(1)	自动生成现在默认启用 (**mac-address auto**)。
8.6(1)	ASA 现在转换自动 MAC 地址生成配置以使用默认前缀。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。在您重新加载或者重新启用 MAC 地址生成时会自动发生此转换。传统的 MAC 地址生成方法不再可用。 **注**　为了保持故障切换对的无中断升级，如果已启用故障切换，则 ASA 在重新加载时*不*转换现有配置中的 MAC 地址方法。

使用指南

为了允许情景共享接口，我们建议您给每个共享情景接口分配唯一 MAC 地址。MAC 地址用于对情景中的数据包进行分类。如果您共享接口，但每个情景中的接口不具有唯一 MAC 地址，则使用目标 IP 地址对数据包进行分类。目标地址与情景 NAT 配置匹配，相对于 MAC 地址方法，此方法具有一些局限性。有关对数据包进行分类的信息，请参阅 CLI 配置指南。

在生成的 MAC 地址与您网络中的另一个专用 MAC 地址冲突时（这种情况极少出现），您可以为情景中的接口手动设置 MAC 地址。请参见 **mac-address** 命令以手动设置 MAC 地址。

与手动 MAC 地址交互

如果您手动分配 MAC 地址并且也启用了自动生成，则使用手动分配的 MAC 地址。如果后来删除了手动 MAC 地址，则使用自动生成的地址。

由于自动生成的地址以 A2 开头，所以如果您还要使用自动生成，则不能让手动 MAC 地址以 A2 开头。

故障切换 MAC 地址

为了用于故障切换， ASA 为每个接口都生成一个活动 MAC 地址和一个备用 MAC 地址。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用活动 MAC 地址以最小化网络中断。请参阅“使用前缀的 MAC 地址格式”部分以获取更多信息。

有关在 **prefix** 关键字引入之前利用旧版本的 **mac-address auto** 命令升级故障切换设备的信息，请参阅“没有前缀的 MAC 地址格式（传统方法）”部分。

使用前缀的 MAC 地址格式

ASA 使用以下格式生成 MAC 地址：

A2*xx*.*yyzz*.*zzzz*

其中 *xx*.*yy* 是一个用户定义的前缀或基于接口 (ASA 5500) 或背板 (ASASM) MAC 地址最后两个字节自动生成的前缀，而 *zz*.*zzzz* 是 ASA 生成的一个内部计数器。备用 MAC 地址除了内部计数器增加 1 之外，与此地址相同。

举一个如何使用前缀的例子：如果您设置一个前缀 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。当在 MAC 地址中使用时，前缀会颠倒 (*xxyy*) 以匹配 ASA 本地形式：

A2**4D.00***zz*.*zzzz*

对于前缀 1009 (03F1)， MAC 地址是：

A2**F1.03***zz*.*zzzz*

没有前缀的 MAC 地址格式 （传统方法）

如果使用故障切换且已升级到版本 8.6 或更高版本，则可以使用此方法；在这种情况下，必须手动启用前缀方法。

没有前缀时，使用以下格式生成 MAC 地址：

- 主用设备 MAC 地址：12*_slot.port_subid.contextid*。
- 备用设备 MAC 地址：02*_slot.port_subid.contextid*。

对于没有接口插槽的平台，插槽始终为 0。*port* 是接口端口。*subid* 是子接口的内部 ID，它是不可查看的。*contextid* 是情景的内部 ID，可使用 **show context detail** 命令进行查看。例如，情景中 ID 为 1 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：

- 主用地址：1200.0131.0001
- 备用地址：0200.0131.0001

此 MAC 地址生成方法不允许在重新加载时保持 MAC 地址不变，不允许在同一网段中有多个 ASA （因为不能保证唯一 MAC 地址），以及不会阻止 MAC 地址与手动分配的 MAC 地址的重叠。我们建议对 MAC 地址生成使用一个前缀以避免这些问题。

何时生成 MAC 地址

当您为情景中的接口配置一个 **nameif** 命令时，会立即生成新的 MAC 地址。如果在配置情景接口后启用此命令，则在您输入命令后会立即为所有接口生成 MAC 地址。如果使用 **no mac-address auto** 命令，则各接口的 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，则使用的 MAC 地址取决于许多变量，因而可能无法预测。

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。

查看分配的 MAC 地址需要 **all** 选项。尽管此命令仅在全局配置模式中是用户可配置的，但 **mac-address auto** 命令与分配的 MAC 地址在每个情景的配置中都显示为只读项。只有在情景中配置了 **nameif** 命令的所分配接口才具有分配的 MAC 地址。

注　如果您给接口手动分配 MAC 地址，但是也启用了自动生成，则自动生成的地址继续显示在配置中，即使手动 MAC 地址是正在使用的地址。如果以后删除手动 MAC 地址，则会使用所显示的自动生成的地址。

查看情景中的 MAC 地址

要查看情景中每个接口在使用的 MAC 地址，请输入 **show interface | include (Interface)|(MAC)** 命令。

注　**show interface** 命令显示正在使用的 MAC 地址；如果您手动分配 MAC 地址并且启用了自动生成，则只能从系统配置中查看未使用的自动生成的地址。

示例

以下示例启用前缀为 78 的自动 MAC 地址生成：

```
ciscoasa(config)# mac-address auto prefix 78
```

以下来自 **show running-config all context admin** 命令的输出显示了分配给 Management0/0 接口的主 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
```

以下来自 **show running-config all context** 命令的输出显示了所有情景接口的所有 MAC 地址（主地址和备用地址）。注意，由于没有在情景中为 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口配置 **nameif** 命令，所以没有为它们生成 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
!
```

相关命令

命令	说明
failover mac address	为主用 / 备用故障切换设置物理接口的主用和备用 MAC 地址。
mac address	为主用 / 主用故障切换设置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）。在多情景模式中，您可以为同一个接口在每个情景中设置不同的 MAC 地址。
mode	将安全情景模式设置为多或单模式。
show interface	显示接口特征，包括 MAC 地址。

mac-address pool

要添加一个 MAC 地址池以用在 ASA 集群中的单个接口上，请在全局配置模式下使用 **mac-address pool** 命令。要删除未使用的地址池，请使用此命令的 **no** 形式。

mac-address pool *name start_mac_address* **-** *end_mac_address*

no mac-address pool *name* [*start_mac_address* **-** *end_mac_address*]

语法说明

name	对池进行命名，名称最多包含 63 个字符。
start_mac_address **-** *end_mac_address*	指定第一个 MAC 地址和最后一个 MAC 地址。注意在连字符 (-) 两端各添加一个空格。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您可以在接口配置模式下在 **mac-address cluster-pool** 命令中使用地址池。为接口手动配置 MAC 地址并不常见，但如果有特殊需要来这样做，可以用该池给每个接口分配唯一 MAC 地址。

示例

以下示例添加一个具有 8 个 MAC 地址的 MAC 地址池，并将其分配给 gigabitethernet 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
```

相关命令

命令	说明
interface	配置接口。
mac-address	配置接口的 MAC 地址。

mac-address-table aging-time

要为 MAC 地址表条目设置超时，请在全局配置模式下使用 **mac-address-table aging-time** 命令。要恢复默认值 5 分钟，请使用此命令的 **no** 形式。

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

语法说明

timeout_value	MAC 地址条目在超时之前保留在 MAC 地址表中的时间，介于 5 到 720 分钟 （12 小时）之间。 5 分钟是默认值。

默认值

默认超时是 5 分钟。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

无使用指南。

示例

以下示例将 MAC 地址超时设置为 10 分钟：

```
ciscoasa(config)# mac-address-timeout aging time 10
```

相关命令

命令	说明
arp-inspection	启用 ARP 检查，即将 ARP 数据包与静态 ARP 条目进行比较。
firewall transparent	将防火墙模式设置为透明。
mac-address-table static	向 MAC 地址表添加静态 MAC 地址条目。
mac-learn	禁用 MAC 地址学习。
show mac-address-table	显示 MAC 地址表，包括动态和静态条目。

mac-address-table static

要向 MAC 地址表添加静态条目，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 **no** 形式。通常，当来自特定 MAC 地址的流量进入接口时， MAC 地址会动态添加到 MAC 地址表。您可以根据需要向 MAC 地址表添加静态 MAC 地址。添加静态条目的一个好处是防止 MAC 欺骗。如果具有与静态条目相同的 MAC 地址的客户端尝试将流量发送到不匹配静态条目的接口，则 ASA 会丢弃流量并产生一条系统消息。

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

语法说明

interface_name	源接口。
mac_address	您想要添加到表中的 MAC 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例向 MAC 地址表添加一个静态 MAC 地址条目：

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

相关命令

命令	说明
arp	添加一个静态 ARP 条目。
firewall transparent	将防火墙模式设置为透明。
mac-address-table aging-time	为动态 MAC 地址条目设置超时。
mac-learn	禁用 MAC 地址学习。
show mac-address-table	显示 MAC 地址表条目。

mac-learn

要禁用接口的 MAC 地址学习，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，请使用此命令的 **no** 形式。默认情况下，每个接口自动学习输入流量的 MAC 地址，然后 ASA 将相应的条目添加到 MAC 地址表。您可以根据需要禁用 MAC 地址学习。

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

语法说明

interface_name	要禁用 MAC 学习的接口。
disable	禁用 MAC 学习。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例在外部接口上禁用 MAC 学习：

```
ciscoasa(config)# mac-learn outside disable
```

相关命令

命令	说明
clear configure mac-learn	将 **mac-learn** 配置设置为默认值。
firewall transparent	将防火墙模式设置为透明。
mac-address-table static	向 MAC 地址表添加静态 MAC 地址条目。
show mac-address-table	显示 MAC 地址表，包括动态和静态条目。
show running-config mac-learn	显示 **mac-learn** 配置。

mac-list

要指定 MAC 地址列表以用于免除对这些 MAC 地址进行身份验证和 / 或授权，请在全局配置模式下使用 **mac-list** 命令。要删除 MAC 列表条目，请使用此命令的 **no** 形式。

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

语法说明

deny	表示与此 MAC 地址匹配的流量不匹配 MAC 列表；当在 **aaa mac-exempt** 命令中指定时，会同时进行身份验证和授权。如果您允许使用 MAC 地址掩码 （如 ffff.ffff.0000）的 MAC 地址范围，并且要强制对该范围内的 MAC 地址进行身份验证和授权，您可能需要向 MAC 列表添加 deny 条目。
id	指定一个十六进制 MAC 访问列表编号。要将一组 MAC 地址组织在一起，请根据需要使用同一 ID 值多次输入 **mac-list** 命令。条目顺序至关重要，因为在非最佳匹配场景下，数据包会使用它匹配的第一个条目。 如果您有一个 permit 条目，并且想要拒绝此 permit 条目允许的地址，请确保在 permit 条目前面输入 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 精确匹配 MAC 地址。 ffff.ffff.0000 仅匹配前 8 位。
permit	表示与此 MAC 地址匹配的流量匹配 MAC 列表，并且在 **aaa mac-exempt** 命令中指定时将同时免除身份验证和授权。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要支持 MAC 地址免除身份验证和授权，请使用 **aaa mac-exempt** 命令。您只能添加 **aaa mac-exempt** 命令的一个实例，因此请确保您的 MAC 列表包括要免除的所有 MAC 地址。您可以创建多个 MAC 列表，但是一次只能使用一个。

示例

以下示例对单个 MAC 地址跳过身份验证：

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

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

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

以下示例对除 00a0.c95d.02b2 之外的一组 MAC 地址跳过身份验证。在 permit 语句前面输入 deny 语句，因为 00a0.c95d.02b2 也匹配 permit 语句，而如果它是第一条语句，则 deny 语句将永远不会被匹配。

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

相关命令

命令	说明
aaa authentication	启用用户身份验证。
aaa authorization	启用用户授权服务。
aaa mac-exempt	免除 MAC 地址列表的身份验证和授权。
clear configure mac-list	删除之前由 **mac-list** 命令指定的 MAC 地址列表。
show running-config mac-list	显示之前在 **mac-list** 命令中指定的 MAC 地址列表。

mail-relay

要配置一个本地域名，请在参数配置模式下使用 **mail-relay** 命令。要禁用此功能，请使用此命令的 **no** 形式。

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

语法说明

domain_name	指定域名。
drop-connection	关闭连接。
log	生成系统日志消息。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何为特定的域配置邮件中继：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

相关命令

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

management-access

要允许对某接口 （并非使用 VPN 时用来进入 ASA 的接口）的管理访问，请在全局配置模式下使用 **management-access** 命令。要禁用管理访问，请使用此命令的 **no** 形式。

management-access *mgmt_if*

no management-access *mgmt_if*

语法说明

mgmt_if	指定从另一个接口进入 ASA 时要访问的管理接口的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令允许您连接到一个接口（在使用完全隧道 IPsec VPN 或 SSL VPN 客户端（AnyConnect 2.x 客户端， SVC 1.x）或通过站点到站点 IPsec 隧道时不通过此接口进入 ASA）。您可以使用 Telnet、 SSH、 Ping 或 ASDM 连接到 ASA 接口。

您仅可定义一个管理访问接口。

注　当在管理访问接口网络和 VPN 网络之间使用身份 NAT（VPN 流量的一种常见 NAT 配置）时，必须指定 **nat** 命令 **route-lookup** 关键字。在不使用路由查找的情况下， ASA 将流量发出到 **nat** 命令中指定的接口，而不管路由表的内容如何。例如，您配置 **management-access inside**，因此，从外部接口进入的 VPN 用户能够管理内部接口。如果身份 **nat** 命令指定了 **(inside,outside)**，则您不想要 ASA 将管理流量发出到内部网络；它将永远不会返回到内部接口 IP 地址。路由查找选项让 ASA 将流量直接发送到内部接口 IP 地址而不是内部网络。对于从 VPN 客户端到内部网络中主机的流量，路由查找选项仍会导致正确的输出接口 （内部），因此正常流量不受影响。

示例

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
ciscoasa(config)# show running-config management-access
management-access inside
```

相关命令

命令	说明
clear configure management-access	删除 ASA 的管理访问内部接口的配置。
show management-access	显示为管理访问配置的内部接口的名称。

management-only

要设置一个接口仅接受管理流量，请在接口配置模式下使用 **management-only** 命令。要允许通过流量，请使用此命令的 **no** 形式。

management-only

no management-only

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， Management *n*/*n* 接口 （如果对您的型号可用）设置为仅管理 (management-only) 模式。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	此命令在运行配置中的位置已移至接口部分的顶端以支持 ASA 集群，该集群对管理接口有特殊的免除。

使用指南

某些型号包含称为 Management *n*/*n* 的专用管理接口，用于支持到 ASA 的流量。不过，您可以使用 **management-only** 命令将任何接口配置为仅管理接口。此外，对于 Management *n*/*n*，您可以禁用仅管理模式，以便此接口像任何其他接口一样通过流量。

注　对于从 ASA 5512-X 到 ASA 5555-X 系列产品，您不能禁用 Management 接口的仅管理模式。默认情况下，此命令始终处于启用状态。

在透明防火墙模式中，除了允许的通过流量接口最大数之外，您还可以将 Management 接口用作单独的管理接口，此类接口是物理接口 （即您的型号支持的子接口），或是由 Management 接口组成的 EtherChannel 接口 （如果您有多个 Management 接口）。您不能将任何其他接口类型用作管理接口。

如果您的型号不具有 Management 接口，则必须从数据接口管理透明防火墙。

在多情景模式中，您无法在情景之间共享任何接口，包括 Management 接口。要提供针对每个情景的管理，您可以创建 Management 接口的子接口，并给每个情景分配一个 Management 子接口。注意，从 ASA 5512-X 到 ASA 5555-X 都不允许 Management 接口上的子接口，因此为了针对每个情景进行管理，您必须连接到数据接口。

管理接口不是普通网桥组的一部分。注意，出于可操作性目的，它是不可配置的网桥组的一部分。

示例

以下示例在 Management 接口上禁用仅管理模式：

```
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
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。

map-name

要将一个用户定义的属性名称映射到思科属性名称，请在 LDAP 属性映射配置模式下使用 **map-name** 命令。

要删除此映射，请使用此命令的 **no** 形式。

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

语法说明

user-attribute-name	指定将要映射到思科属性的用户定义属性名称。
Cisco-attribute-name	指定要映射到用户定义名称的思科属性名称。

默认值

默认情况下，不存在名称映射。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
LDAP 属性映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用 **map-name** 命令，您可以将自己的属性名称映射到思科属性名称。然后您可以将产生的属性映射绑定到 LDAP 服务器。您通常的步骤包括：

1. 在全局配置模式下使用 **ldap attribute-map** 命令创建一个未填充的属性映射。此命令进入 LDAP 属性映射配置模式。
2. 在 LDAP 属性映射配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 AAA 服务器主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。注意此命令中 “ldap” 后面的连字符。

注　要正确使用属性映射功能，您需要了解思科 LDAP 属性的名称和值以及用户定义的属性的名称和值。

示例

以下示例命令在 LDAP 属性映射 myldapmap 中将用户定义属性名称 Hours 映射到思科属性名称 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 属性映射配置模式中，您可以输入 “?” 来显示思科 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)#
```

相关命令

命令	说明
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map（AAA 服务器主机模式）	将 LDAP 属性映射绑定到 LDAP 服务器。
map-value	将一个用户定义属性值映射到思科属性。
show running-config ldap attribute-map	显示特定的正在运行的 LDAP 属性映射或所有正在运行的属性映射。
clear configure ldap attribute-map	删除所有 LDAP 属性映射。

map-value

要将用户定义值映射到思科 LDAP 值，请在 LDAP 属性映射配置模式下使用 **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*

语法说明

Cisco-value-string	为思科属性指定思科值字符串。
user-attribute-name	指定将映射到思科属性名称的用户定义属性名称。
user-value-string	指定将映射到思科属性值的用户定义值字符串。

默认值

默认情况下，没有用户定义值被映射到思科属性。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
LDAP 属性映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用 **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。然后您可以将产生的属性映射绑定到 LDAP 服务器。您通常的步骤包括：

1. 在全局配置模式下使用 **ldap attribute-map** 命令创建一个未填充的属性映射。此命令进入 LDAP 属性映射配置模式。
2. 在 LDAP 属性映射配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射。
3. 在 AAA 服务器主机模式下使用 **ldap-attribute-map** 命令将属性映射绑定到 LDAP 服务器。注意此命令中 “ldap” 后面的连字符。

注　要正确使用属性映射功能，您需要了解思科 LDAP 属性的名称和值以及用户定义的属性的名称和值。

示例

在以下示例中，进入 LDAP 属性映射配置模式，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名为 Daytime 的思科定义时间策略：

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

相关命令

命令	说明
ldap attribute-map（全局配置模式）	创建并命名一个 LDAP 属性映射，用于将用户定义的属性名称映射到思科 LDAP 属性名称。
ldap-attribute-map（AAA 服务器主机模式）	将 LDAP 属性映射绑定到 LDAP 服务器。
map-name	将用户定义 LDAP 属性名称映射到思科 LDAP 属性名称。
show running-config ldap attribute-map	显示特定的正在运行的 LDAP 属性映射或所有正在运行的属性映射。
clear configure ldap attribute-map	删除所有 LDAP 映射。

mapping-service

要为思科公司间媒体引擎代理配置映射服务，请在 UC-IME 配置模式下使用 **mapping-service** 命令。要从代理删除映射服务，请使用此命令的 **no** 形式。

mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

no mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

语法说明

interface	指定将用作侦听接口或 uc-ime 接口的接口名称。
listening-interface	配置 ASA 用于侦听映射请求的接口。
listening-port	（可选）为映射服务配置侦听端口。
port	（可选）指定 ASA 用于侦听映射请求的 TCP 端口号。端口号必须为 1024 或更高，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	配置连接到远程思科 UCM 的接口。

默认值

默认情况下，思科公司间媒体引擎代理的 off-path 部署的映射服务在 TCP 端口 8060 上侦听。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

为了实现 ASA 上思科公司间媒体引擎代理的 off-path 部署，将映射服务添加到代理配置。要配置映射服务，您必须指定用于侦听映射请求的外部接口 （远程企业端）和连接到远程思科 UCM 的接口。

注　您只能为思科公司间媒体引擎代理配置一个映射服务器。

当为 off-path 部署配置了思科公司间媒体引擎代理时，您才配置映射服务。

在 off-path 部署中，入站和出站思科公司间媒体引擎呼叫都会流经一个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，并被配置为主要支持思科公司间媒体引擎。面向互联网的普通流量不流经此 ASA。

对于所有入站呼叫，因为目标思科 UCM 被配置具有 ASA 上的全局 IP 地址，所以信令被定向到 ASA。对于出站呼叫，被叫方可能是互联网中的任何 IP 地址；因此，ASA 被配置一个映射服务，用于为互联网中被叫方的每个全局 IP 地址动态提供 ASA 上的一个内部 IP 地址。

思科 UCM 将所有出站呼叫直接发送到所映射的 自适应安全设备 上的内部 IP 地址，而不是发送到互联网中被叫方的全局 IP 地址。然后 ASA 将呼叫转发到被叫方的全局 IP 地址。

示例

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
```

相关命令

命令	说明
show running-config uc-ime	显示思科公司间媒体引擎代理的正在运行的配置。
show uc-ime	显示有关回退通知、映射服务会话和信令会话的统计数据或详细信息。
uc-ime	在 ASA 上创建思科公司间媒体引擎代理实例。

mask

当使用 模块化策略框架 时，通过在匹配或类配置模式下使用 **mask** 命令，屏蔽匹配 **match** 命令或类映射的部分数据包。此掩码操作在检查策略映射 （**policy-map type inspect** 命令）中对应用流量可用；然而，并非所有应用都允许此操作。例如，您可以对 DNS 应用检查使用 **mask** 命令，以在允许流量通过 ASA 之前屏蔽报头标志。要禁用此操作，请使用此命令的 **no** 形式。

mask [log]

no mask [log]

语法说明

log	记录匹配。系统日志消息数量取决于应用。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。在输入 **match** 或 **class** 命令来标识应用流量之后 （**class** 命令引用一个现有的 **class-map type inspect** 命令，后者又包含 **match** 命令），您可以输入 **mask** 命令来屏蔽匹配 **match** 命令或 **class** 命令的部分数据包。

当您在 3/4 层策略映射 （**policy-map** 命令）中使用 **inspect** 命令启用应用检查时，您可以启用包含此操作的检查策略映射，例如，输入 **inspect dns dns_policy_map** 命令，其中 dns_policy_map 是检查策略映射的名称。

示例

以下示例在允许流量通过 ASA 之前屏蔽 DNS 报头中的 RD 和 RA 标志：

```
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
```

相关命令

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

mask-banner

要对服务器标识进行模糊处理，请在参数配置模式下使用 **mask-banner** 命令。要禁用此功能，请使用此命令的 **no** 形式。

mask-banner

no mask-banner

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何屏蔽服务器标识：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

相关命令

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

mask-syst-reply

要从客户端隐藏 FTP 服务器响应，请在 FTP 映射配置模式下使用 **mask-syst-reply** 命令 （可通过使用 **ftp-map** 命令进入该模式）。要删除配置，请使用此命令的 **no** 形式。

mask-syst-reply

no mask-syst-reply

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用 mask-syst-reply 命令和严格的 FTP 检查，从客户端保护 FTP 服务器系统。启用此命令后，对 **syst** 命令的服务器应答将被一系列 X 取代。

示例

在以下示例中， ASA 用一系列 X 取代对 syst 命令的 FTP 服务器应答：

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

命令	说明
class-map	定义要应用安全操作的流量类。
ftp-map	定义一个 FTP 映射并启用 FTP 映射配置模式。
inspect ftp	应用特定的 FTP 映射以用于应用检查。
policy-map	将类映射与特定安全操作关联。
request-command deny	指定将不允许的 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 **match access-list** 命令，用访问列表来标识要应用操作的流量。要删除 **match access-list** 命令，请使用此命令的 **no** 形式。

match access-list *access_list_name*

no match access-list *access_list_name*

语法说明

access_list_name	指定将用作匹配条件的访问列表的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 命令标识要应用操作的第 3 层和第 4 层流量。

   在输入 **class-map** 命令之后，您可以输入 **match access-list** 命令来标识流量。或者，可以输入一个不同类型的 **match** 命令，例如 **match port** 命令。您仅可在类映射中包含一个 **matchaccess-list** 命令，并且不能将其与其他类型的 **match** 命令结合在一起使用。一种例外情况是，如果定义了 **match default-inspection-traffic** 命令（该命令匹配 ASA 可检查的所有应用所用的默认 TCP 和 UDP 端口），则您可以使用 **match access-list** 命令缩小匹配的流量范围。由于 **match default-inspection-traffic** 命令会指定进行匹配的端口，所以访问列表中的任何端口都会被忽略。

2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。

3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。

4. 使用 **service-policy** 命令在接口上激活操作。

示例

以下示例创建三个可匹配三个访问列表的 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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match any

当使用 模块化策略框架 时，通过在类映射配置模式下使用 **match any** 命令，匹配要应用操作的所有流量。要删除 **match any** 命令，请使用此命令的 **no** 形式。

match any

no match any

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 命令标识要应用操作的第 3 层和第 4 层流量。

   在输入 **class-map** 命令之后，您可以输入 **match any** 命令来标识所有流量。或者，可以输入一个不同类型的 **match** 命令，例如 **match port** 命令。您不能将 **match any** 命令与其他类型的 **match** 命令结合在一起使用。

2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。
3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。
4. 使用 **service-policy** 命令在接口上激活操作。

示例

以下示例显示如何使用类映射和 **match any** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
```

相关命令

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 access-list	根据访问列表匹配流量。
match port	标识类映射中的特定端口号。
show running-config class-map	显示有关类映射配置的信息。

match apn

要为 GTP 消息中的接入点名称配置一个匹配条件，请在类映射和策略映射配置模式下使用 **match apn** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] apn regex [*regex_name* | **class** *regex_class_name*]

no match [not] apn regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 GTP 类映射或策略映射中配置。在 GTP 类映射中只能输入一个条目。

示例

以下示例显示如何在 GTP 检查类映射中为接入点名称配置一个匹配条件。

```
ciscoasa(config-cmap)# match apn class gtp_regex_apn
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match as-path

要匹配 BGP 自主系统路径访问列表，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 *path-list-number*

no match as-path *path-list-number*

语法说明

path-list-number	自主系统路径访问列表编号。

默认值

没有定义路径列表。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

match as-path 和 **set weight** 命令设置的值将覆盖全局值。例如，使用 **match as-path** 和 **set weight** 路由映射配置命令分配的权重将覆盖使用 **neighbor weight** 命令分配的权重。

一个路由映射可有多个部分。任何至少不匹配 **route-map** 命令的一个相关 **match** 子句的路由都将忽略；也就是说，这样的路由将不会被出站路由映射所通告，也不会被入站路由映射所接受。如果您想要仅修改一些数据，您必须配置另一个指定了显式匹配的路由映射部分。它可以接受不止一个路径列表名称。

示例

以下示例设置自主系统路径来匹配 BGP 自主系统路径访问列表 as-path-acl：

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

相关命令

命令	说明
set-weight	为路由表指定 BGP 权重。
neighbor-weight	为邻居连接分配权重。

match body

要为 ESMTP 正文消息长度或行长度配置匹配条件，请在类映射或策略映射配置模式下使用 **match body** 命令。要删除配置的部分，请使用此命令的 **no** 形式。

match [not] body [length | line length] gt *bytes*

no match [not] body [length | line length] gt *bytes*

语法说明

length	指定 ESMTP 正文消息的长度。
line length	指定 ESMTP 正文消息的行的长度。
bytes	指定要匹配的字节数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中为正文行长度配置一个匹配条件。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match body line length gt 1000
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match called-party

要为 H.323 被叫方配置匹配条件，请在策略映射配置模式下使用 **match called-party** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] called-party [regex *regex***]**

no match [not] match [not] called-party [regex *regex***]**

语法说明

regex *regex*	指定要匹配正则表达式。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 H.323 检查类映射中为被叫方配置一个匹配：

```
ciscoasa(config-cmap)# match called-party regex caller1
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match calling-party

要为 H.323 主叫方配置匹配条件，请在策略映射配置模式下使用 **match calling-party** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] calling-party [regex *regex***]**

no match [not] match [not] calling-party [regex *regex***]**

语法说明

regex *regex*	指定要匹配正则表达式。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 H.323 检查类映射中为主叫方配置匹配条件：

```
ciscoasa(config-cmap)# match calling-party regex caller1
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match certificate

要配置证书匹配规则，请在加密 CA 信任点配置模式下使用 **match certificate** 命令。要从配置删除规则，请使用此命令的 **no** 形式。

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

语法说明

map-name	指定将匹配到此规则的证书映射的名称。您必须在配置匹配规则之前先配置证书映射。最大长度是 65 个字符。
override ocsp	指定规则的目的是覆盖证书中的 OCSP URL。
seq-num	设置此匹配规则的优先级。有效范围为 1 至 10000。 ASA 评估匹配规则的顺序是，从最低序列号开始，依次增高，直到找到匹配项。
trustpoint	（可选）指定使用信任点验证 OCSP 响应器证书。
trustpoint-name	（可选）标识将用于覆盖的信任点以验证响应器证书。
url	指定访问一个 URL 以获得 OCSP 撤销状态。
URL	标识将访问的 URL 以获得 OCSP 撤销状态。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在 PKI 证书验证过程中，ASA 通过使用 CRL 检查或在线证书状态协议 (OCSP) 检查证书撤销状态来维护安全。利用 CRL 检查， ASA 获取、分析并缓存 CRL （CRL 提供已撤销证书的完整列表）。 OCSP 提供一种可扩展性更高的撤销状态检查方法，因为 OCSP 将证书状态局部化在验证授权机构中，而它在此机构中查询特定证书状态。

证书匹配规则允许您配置 OCSP URL 覆盖，这会指定一个用于检查撤销状态的 URL，而不是远程用户证书的 AIA 字段中的 URL。匹配规则还允许您配置信任点来用于验证 OCSP 响应器证书，这让 ASA 可以从任何 CA 验证响应器证书 （包括自签证书和客户端证书验证路径之外的证书）。

配置 OCSP 时，请注意以下要求：

- 您可以在一个信任点配置中配置多个匹配规则，但是对每个加密 CA 证书映射只能有一个匹配规则。不过，您可以配置多个加密 CA 证书映射，并将它们与同一信任点相关联。
- 您必须在配置匹配规则之前先配置证书映射。
- 要配置信任点来验证自签 OCSP 响应器证书，请将自签的响应器证书作为受信任 CA 证书导入到它自己的信任点中。然后在客户端证书验证信任点中配置 **match certificate** 命令，以使用包含自签 OCSP 响应器证书的信任点来验证响应器证书。这同样适用于验证客户端证书验证路径之外的响应器证书。
- 如果同一 CA 既颁发了客户端证书，也颁发了响应器证书，那么一个信任点可以对二者都进行验证。但如果是不同 CA 颁发的客户端证书和响应器证书，则需要配置两个信任点，每种证书一个信任点。
- OCSP 服务器（响应器）证书通常签发 OCSP 响应。在收到响应后，ASA 尝试验证响应器证书。CA 通常将 OCSP 响应器证书的寿命设置为一个相当短的时期以尽量避免被盗用。CA 通常还在响应器证书中包含一个 ocsp-no-check 扩展，表示此证书不需要进行撤销状况检查。但是，如果此扩展不存在， ASA 将尝试使用信任点中指定的相同方法检查其撤销状态。如果响应器证书不可验证，则撤销检查失败。为了避免这种可能性，请在配置响应器证书验证信任点时使用 **revocation-check none** 命令，并在配置客户端证书时使用 **revocation-check ocsp** 命令。
- 如果 ASA 未找到匹配项，它将使用 **ocsp url** 命令中指定的 URL。如果尚未配置 **ocsp url** 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，则撤销状态检查失败。

示例

以下示例显示如何为名为 newtrust 的信任点创建证书匹配规则。此规则具有名为 mymap 的映射名称、序列号 4、名为 mytrust 的信任点，并指定 10.22.184.22 的 URL。

```
ciscoasa(config)# crypto ca trustpoint newtrust
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来标识信任点（包含 CA 证书来验证响应器证书）。如果 newtrust 信任点中标识的 CA 没有颁发 OCSP 响应器证书，则此证书是必需的。

步骤 1　配置证书映射用于标识将应用映射规则的客户端证书。在本示例中，证书映射的名称是 mymap，序列号为 1。任何包含值为 mycert 的 CN 属性且具有主题名称的客户端证书均匹配 mymap 条目。

```
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)#
```

步骤 2　配置一个信任点，其中包含用于验证 OCSP 响应器证书的 CA 证书。在自签证书情况下，这是自签证书本身，它被导入并在本地受信任。您也可以通过外部 CA 注册获取用于此目的的证书。当出现提示时，粘贴到 CA 证书中。

```
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
```

```
MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
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
```

步骤 3　配置原始信任点 newtrust，以 OCSP 作为撤销检查方法。然后设置匹配规则，它包含在步骤 2 中配置的证书映射 mymap 和自签信任点 mytrust。

```
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
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
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
```

对客户端证书身份验证使用 newtrust 信任点的任何连接都检查客户端证书是否匹配 mymap 证书映射中指定的属性规则。如果匹配，则 ASA 在 10.22.184.22 处访问 OCSP 响应器以获得证书撤销状态，然后使用 mytrust 信任点验证响应器证书。

注　newtrust 信任点被配置为通过 OCSP 对客户端证书执行撤销检查。但是， mytrust 信任点是为默认撤销检查方法而配置的，但现在没有此方法。因此，不会对 OCSP 响应器证书执行撤销检查。

相关命令

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。
crypto ca trustpoint	进入 crypto ca trustpoint 配置模式。在全局配置模式下使用此命令。
ocsp disable-nonce	禁用 OCSP 请求的 nonce 扩展。
ocsp url	指定 OCSP 服务器以用来检查与信任点关联的所有证书。
revocation-check	指定用于撤销检查的方法以及尝试它们的顺序。

match certificate allow expired-certificate

要允许管理员免除对某些证书的过期检查，请在 CA 信任池配置模式下使用 **match certificate allow expired-certificate** 命令。要禁用某些证书的免除，请使用此命令的 **no** 形式。

match certificate <map> allow expired-certificate

no match certificate <map> allow expired-certificate

语法说明

allow	允许接受过期证书。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
CA 信任池配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

信任池匹配命令利用证书映射对象来将证书特定的例外或覆盖配置到全局信任池策略中。匹配规则是相对于正在被验证的证书而写的。

相关命令

命令	说明
match certificate skip revocation check	免除对某些证书的撤销检查。

match certificate skip revocation-check

要允许管理员免除对某些证书的撤销检查，请在 CA 信任池配置模式下使用 **match certificate skip revocation-check** 命令。要禁用免除撤销检查，请使用此命令的 **no** 形式。

match certificate map skip revocation-check

no match certificate map skip revocation-check

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
CA 信任池配置	• 是	• 是	• 是	—	—

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

信任池匹配命令利用证书映射对象来将证书特定的例外或覆盖配置到全局信任池策略中。匹配规则是相对于正在被验证的证书而写的。

示例

以下示例显示对具有主题 DN 公用名称 “mycompany123” 的证书跳过验证检查。

```
crypto ca certificate map mycompany 1
subject-name attr cn eq mycompany123
crypto ca trustpool policy
match certificate mycompany skip revocation-check
```

相关命令

命令	说明
match certificate allow expired-certificate	免除对某些证书的过期检查。

match cmd

要在 ESMTP 命令动词上配置一个匹配条件，请在策略映射配置模式下使用 **match cmd** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] cmd [verb *verb* **| line length gt** *bytes* **| RCPT count gt** *recipients_number]*

no match [not] cmd [verb *verb* **| line length gt** *bytes* **| RCPT count gt** *recipients_number]*

语法说明

verb *verb*	指定 ESMTP 命令动词。
line length gt *bytes*	指定行的长度。
RCPT count gt *recipients_number*	指定收件人电邮地址的数量。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中为 ESMTP 事务中交换的动词 （方法） NOOP 配置一个匹配条件：

```
ciscoasa(config-pmap)# match cmd verb NOOP
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match community

要匹配一个边界网关协议 (BGP) 社区，请在路由映射配置模式下使用 **match community** 命令。要从配置文件删除 **match community** 命令并将系统恢复到其默认状态 （即软件删除 BGP 社区列表条目），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]**}

语法说明

standard-list-number	指定一个从 1 到 99 的标准社区编号，用于标识一个或多个社区允许组或拒绝组。
expanded-list-number	指定一个从 100 到 500 的扩展的社区列表编号，用于标识一个或多个社区允许组或拒绝组。
community-list-name	社区列表名称。
exact	（可选）表示需要精确匹配。所有且仅有这些指定的社区必须存在。

默认值

没有与路由映射匹配的社区列表。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

一个路由映射可有多个部分。任何至少不匹配 **route-map** 命令的一个相关 **match** 命令的路由都将忽略；也就是说，这样的路由将不会被出站路由映射所通告，也不会被入站路由映射所接受。如果您想要仅修改一些数据，您必须配置另一个指定了显式匹配的路由映射部分。

基于社区列表编号的匹配是一种适用于 BGP 的 **match** 命令类型。

示例

以下示例显示匹配社区列表 1 的路由将权重设置为 100。具有社区 109 的任何路由都将权重设置为 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 的路由将权重设置为 200。仅具有社区 109 的任何路由都将权重设置为 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，匹配社区列表 LIST_NAME 的路由将权重设置为 100。仅具有社区 101 的任何路由都将权重设置为 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
```

以下示例显示匹配扩展的社区列表 500 的路由。具有扩展的社区 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
```

相关命令

命令	说明
set-weight	为路由表指定 BGP 权重。
community-list	创建或配置 BGP 社区列表。

match default-inspection-traffic

要为类映射中的检查命令指定默认流量，请在类映射配置模式下使用 **match default-inspection-traffic** 命令。要删除此指定，请使用此命令的 **no** 形式。

match default-inspection-traffic

no match default-inspection-traffic

语法说明

此命令没有任何参数或关键字。

默认值

请参阅 “ 使用指南 ” 小节，了解每个检查的默认流量。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

使用 **match default-inspection-traffic** 命令，您可以为单个 **inspect** 命令匹配默认流量。 **match default-inspection-traffic** 命令可以与另一个 match 命令结合使用，通常是一个 **permit ip** *src-ip dst-ip* 形式的访问列表。

match default-inspection-traffic 命令与另一个 **match** 命令相结合的规则是，使用 **match default-inspection-traffic** 命令指定协议和端口信息，使用另一个 **match** 命令指定其他信息 （例如 IP 地址）。对于 **inspect** 命令来说，另一个 **match** 命令中指定的任何协议或端口信息都会被忽略。

例如，以下示例中指定的端口 65535 将被忽略：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# match port 65535
```

检查的默认流量如下：

检查类型	协议类型	源端口	目标端口
ctiqbe	tcp	不适用	1748
dcerpc	tcp	不适用	135
dns	udp	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
ipsec-pass-thru	udp	不适用	500
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	不适用
rpc	udp	111	111
rsh	tcp	不适用	514
rtsp	tcp	不适用	554
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
tftp	udp	不适用	69
xdmcp	udp	177	177

示例

以下示例显示如何使用类映射和 **match default-inspection-traffic** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)#
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
match any	包括类映射中的所有流量。
show running-config class-map	显示有关类映射配置的信息。

match dns-class

要在 DNS Resource Record （DNS 资源记录）或 Question （问题）部分为 Domain System Class（域名系统类）配置一个匹配条件，请在类映射或策略映射配置模式下使用 **match dns-class** 命令。要删除已配置的类，请使用此命令的 **no** 形式。

match [not] dns-class {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [not] dns-class {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

语法说明

eq	指定确切匹配。
c_well_known	按众所周知的名称指定 DNS 类为 IN。
c_val	在 DNS 类字段中指定一个任意值 (0-65535)。
range	指定范围。
c_val1 c_val2	在范围匹配中指定值。每个值都介于 0 到 65535 之间。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

默认情况下，此命令检查 DNS 消息的所有字段（问题和 RR），并匹配指定的类。DNS 查询和响应都会经过检查。

通过使用以下两个命令，可将匹配范围缩小到 DNS 查询的问题部分：**match not header-flag QR** 和 **match question**。

此命令可在 DNS 类映射或策略映射内进行配置。在一个 DNS 类映射内只能输入一个条目。

示例

以下示例显示如何在 DNS 检查策略映射中为 DNS 类配置一个匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

相关命令

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。
show running-config class-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）配置一个匹配条件，请在类映射或策略映射配置模式下使用 **match dns-type** 命令。要删除已配置的 DNS 类型，请使用此命令的 **no** 形式。

match [not] dns-type {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [not] dns-type {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

语法说明

eq	指定确切匹配。
t_well_known	按众所周知的名称指定 DNS 类型：A、NS、CNAME、SOA、TSIG、IXFR 或 AXFR。
t_val	在 DNS 类型字段中指定一个任意值 (0-65535)。
range	指定范围。
t_val1 t_val2	在范围匹配中指定值。每个值都介于 0 到 65535 之间。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

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 查询和响应都会经过检查。

通过使用以下两个命令，可将匹配范围缩小到 DNS 查询的问题部分：**match not header-flag QR** 和 **match question**。

此命令可在 DNS 类映射或策略映射内进行配置。在一个 DNS 类映射内只能输入一个条目。

示例

以下示例显示如何在 DNS 检查策略映射中为 DNS 类型配置一个匹配条件。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match domain-name

要为 DNS 消息域名列表配置一个匹配条件，请在类映射和策略映射配置模式下使用 **match domain-name** 命令。要删除配置的部分，请使用此命令的 **no** 形式。

match [not] domain-name regex *regex_id*

match [not] domain-name regex class *class_id*

no match [not] domain-name regex *regex_id*

no match [not] domain-name regex class *class_id*

语法说明

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。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令将 DNS 消息中的域名与预定义列表进行匹配。压缩域名在进行匹配前将被展开。结合其他 DNS **match** 命令，匹配条件可以缩窄到某个具体字段。

此命令可在 DNS 类映射或策略映射内进行配置。在一个 DNS 类映射内只能输入一个条目。

示例

以下示例显示如何匹配 DNS 检查策略映射中的 DNS 域名：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match dscp

要标识类映射中 IETF 定义的 DSCP 值（在 IP 报头中），请在类映射配置模式下使用 **match dscp** 命令。要删除此指定，请使用此命令的 **no** 形式。

match dscp {*values*}

no match dscp {*values*}

语法说明

values	在 IP 报头中指定最多 8 个不同的 IETF 定义的 DSCP 值。范围为 0 到 63。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

使用 **match dscp** 命令，您可以匹配 IP 报头中 IETF 定义的 DSCP 值。

示例

以下示例显示如何使用类映射和 **dscp** 命令定义流量类。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match dscp af43 cs1 ef
ciscoasa(config-cmap)#
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
match port	指定 TCP/UDP 端口作为该接口上接收到的数据包的比较条件。
show running-config class-map	显示有关类映射配置的信息。

第 10 章

match ehlo-reply-parameter 至 match question 命令

match ehlo-reply-parameter

要配置 ESMTP ehlo reply 参数的匹配条件，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，请使用此命令的 **no** 形式。

match [not] ehlo-reply-parameter *parameter*

no match [not] ehlo-reply-parameter *parameter*

语法说明

parameter	指定 ehlo reply 参数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中配置 ehlo reply 参数的匹配条件：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match ehlo-reply-parameter auth
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match filename

要配置 FTP 传输的文件名的匹配条件，请在类映射或策略映射配置模式下使用 **match filename** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] filename regex [*regex_name* | **class** *regex_class_name*]

no match [not] filename regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 FTP 类映射或策略映射中配置。在 FTP 类映射中只能输入一个条目。

示例

以下示例显示如何在 FTP 检查类映射中配置 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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match filetype

要配置 FTP 传输文件类型的匹配条件，请在类映射或策略映射配置模式下使用 **match filetype** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] filetype regex [*regex_name* | **class** *regex_class_name*]

no match [not] filetype regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 FTP 类映射或策略映射中配置。在 FTP 类映射中只能输入一个条目。

示例

以下示例显示如何在 FTP 检查策略映射中配置 FTP 传输文件类型的匹配条件：

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match flow ip destination-address

要在类映射中指定流 IP 目标地址，请在类映射配置模式下使用 **match flow ip destination-address** 命令。要删除此指定，请使用此命令的 **no** 形式。

match flow ip destination-address

no match flow ip destination-address

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

要在隧道组上启用基于流的策略操作，请将 **match flow ip destination-address** 和 **match tunnel-group** 命令与 **class-map**、**policy-map** 和 **service-policy** 命令配合使用。定义流量的条件是目标 IP 地址。所有前往唯一 IP 目标地址的流量都被视为流。策略操作应用到每个流而不是整个流量类。使用 **match flow ip destination-address** 命令应用 QoS 操作管制。使用 **match tunnel-group** 将隧道组中的每一条隧道管制为指定的速率。

示例

以下示例显示如何在隧道组中启用基于流的策略以及将每个隧道限于指定的速率。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match tunnel-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)#
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
show running-config class-map	显示有关类映射配置的信息。
tunnel-group	创建和管理 VPN 连接特定记录的数据库。

match header （策略映射类型检查 esmtp）

要配置 ESMTP 报头的匹配条件，请在策略映射类型检查 esmtp 配置模式下使用 **match header** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] header [[length | line length] gt *bytes* **| to-fields count gt** *to_fields_number*]

no match [not] header [[length | line length] gt *bytes* **| to-fields count gt** *to_fields_number*]

语法说明

length gt *bytes*	指定此项可匹配 ESMTP 报头消息的长度。
line length gt bytes	指定此项可匹配 ESMTP 报头消息行的长度。
to-fields count gt *to_fields_number*	指定此项可匹配 To:（收件人：）字段的数量。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
策略映射类型检查 esmtp 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中配置报头的匹配条件：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match header length gt 512
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match header （策略映射类型检查 ipv6）

要配置 IPv6 报头的匹配条件，请在策略映射类型检查 ipv6 配置模式下使用 **match header** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [**not**] **header** {**ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** {**eq** | **range**} *number*}

no match [**not**] **header** {**ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** {**eq** | **range**} *number*}

语法说明

ah	匹配 IPv6 身份验证扩展报头
count gt *number*	指定 IPv6 扩展报头的最大数量 （0 到 255）。
destination-option	匹配 IPv6 目标选项扩展报头。
esp	匹配 IPv6 封装安全负载 (ESP) 扩展报头。
fragment	匹配 IPv6 片段扩展报头。
hop-by-hop	匹配 IPv6 逐跃点扩展报头。
not	（可选）与指定的参数不匹配。
routing-address count gt *number*	设置 IPv6 路由报头类型 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 路由报头类型 （0 到 255）。对于范围，用空格分隔值。例如， **30 40**。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
策略映射类型检查 ipv6 配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

指定要匹配的报头。默认情况下，该数据包已记录 (**log**)；如果要丢弃 （可选择同时记录）该数据包，请在匹配配置模式下输入 **drop** 和可选的 **log** 命令。

为您要匹配的每个扩展重新输入 **match** 命令和可选的 **drop** 操作：

示例

以下示例创建检查策略映射，该映射将丢弃并记录带有逐跃点、目标选项、路由地址和路由类型 0 报头的所有 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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match header-flag

要配置 DNS 报头标志的匹配条件，请在类映射或策略映射配置模式下使用 **match header-flag** 命令。要删除配置的报头标志，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*}

语法说明

eq	指定确切匹配。如果未配置，指定 **match-all** 位掩码匹配。
f_well_known	通过众所周知的名称指定 DNS 报头标志位。可输入多个标志位及逻辑 OR （或）。 QR （查询，注：QR=1，表示 DNS 响应） AA （权威答案） TC （截断） RD （需要递归） RA （递归可用）
f_value	以十六进制形式指定任意 16 位值。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 DNS 类映射或策略映射中进行配置。在 DNS 类映射中只能输入一个条目。

示例

以下示例显示如何在 DNS 检查策略映射中配置 DNS 报头标志的匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match im-subscriber

要配置 SIP IM 用户的匹配条件，请在类映射或策略映射配置模式下使用 **match im-subscriber** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] im-subscriber regex [*regex_name* | **class** *regex_class_name*]

no match [not] im-subscriber regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 SIP 类映射或策略映射中配置。在 SIP 类映射中只能输入一个条目。

示例

以下示例显示如何在 SIP 检查策略映射中配置 SIP IM 用户的匹配条件：

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match interface

要分发其下一跃点并非指定接口之一的任何路由，请在路由映射配置模式下使用 **match interface** 命令。要删除匹配接口条目，请使用此命令的 **no** 形式。

match interface *interface-name*

no match interface *interface-name*

语法说明

interface-name	接口 （并非物理接口）的名称。可以指定多个接口名称。

默认值

没有定义匹配接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

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 参数值。

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。您可以按任意顺序指定 **match** 命令。所有 **match** 命令必须 “ 通过 ” 才可使路由根据 **set** 命令指定的设置操作重分布。 **match** 命令的 **no** 形式可删除指定的匹配条件。如果 **match** 命令中指定了多个接口，则 **no match interface** *interface-name* 可用于删除单个接口。

一个路由映射可有多个部分。不匹配至少一个与 **route-map** 命令相关的匹配子句的任何路由都会被忽略。如果您要只修改部分数据，则必须配置第二个路由映射部分，并指定显式匹配。

示例

以下示例显示其下一跃点超出分发范围的路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

相关命令

命令	说明
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
match ip route-source	重分布已通过位于访问列表所指定地址的路由器和访问服务器通告的路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match invalid-recipients

要配置 ESMTP 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 **match invalid-recipients** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] invalid-recipients count gt *number*

no match [not] invalid-recipients count gt *number*

语法说明

count gt *number*	指定此项可匹配无效收件人数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中配置无效收件人数的匹配条件：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match invalid-recipients count gt 1000
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match ip address

要重分布路由地址或匹配数据包通过指定访问列表之一传递的任何路由，请在路由映射配置模式下使用 **match ip address** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

match ip address {*acl...*} **prefix-list**

no match ip address {*acl...*} **prefix-list**

语法说明

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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

示例

以下示例显示如何重分布内部路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
match ipv6 address	分发 IPv6 路由地址或匹配数据包通过指定访问列表之一传递的任何路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match ipv6 address

要重分布 IPv6 路由地址或匹配数据包通过指定访问列表之一传递的任何路由，请在路由映射配置模式下使用 **match ipv6 address** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

match ipv6 address {*acl...*} **prefix-list**

no match ipv6 address {*acl...*} **prefix-list**

语法说明

acl	指定访问列表的名称。可以指定多个访问列表。
prefix-list	指定匹配前辍列表的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

示例

以下示例显示如何重分布内部路由：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
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
match ip address	分发路由地址或匹配数据包通过指定访问列表之一传递的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match ip next-hop

要重分布下一跃点路由器地址通过指定访问列表之一传递的任何路由，请在路由映射配置模式下使用 **match ip next-hop** 命令。要删除下一跃点条目，请使用此命令的 **no** 形式。

match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

no match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

语法说明

acl	ACL 的名称。可以指定多个 ACL。
prefix-list *prefix_list*	前缀列表的名称。

默认值

路由可自由分发，无需匹配下一跃点地址。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

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 *acl* 参数值。

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。您可以按任意顺序输入 **match** 命令。所有 **match** 命令必须“ 通过 ” 才可使路由根据 **set** 命令指定的设置操作重分布。 **match** 命令的 **no** 形式可删除指定的匹配条件。

当您通过路由映射传递路由时，一个路由映射可以有多个部分。不匹配至少一个与 **route-map** 命令相关的匹配子句的任何路由都会被忽略。要想只修改部分数据，必须配置第二个路由映射部分并且指定显式匹配。

示例

以下示例显示如何分发下一跃点路由器地址通过访问列表 acl_dmz1 或 acl_dmz2 传递的路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

相关命令

命令	说明
match interface	分发其下一个跃点跃出指定的接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match ip route-source

要重分布已通过位于 ACL 所指定地址的路由器和访问服务器通告的路由，请在路由映射配置模式下使用 **match ip route-source** 命令。要删除下一跃点条目，请使用此命令的 **no** 形式。

match ip route-source {*acl...*} | **prefix-list** *prefix_list*

no match ip route-source {*acl...*}

语法说明

acl	ACL 的名称。可以指定多个 ACL。
prefix_list	前缀列表的名称。

默认值

不对路由来源进行过滤。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

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 access-list-name 参数值。

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。您可以按任意顺序输入 **match** 命令。所有 **match** 命令必须“ 通过 ” 才可使路由根据 **set** 命令指定的设置操作重分布。 **match** 命令的 **no** 形式可删除指定的匹配条件。

一个路由映射可有多个部分。不匹配至少一个与 **route-map** 命令相关的匹配子句的任何路由都会被忽略。要想只修改部分数据，必须配置第二个路由映射部分并且指定显式匹配。路由的下一跃点和源路由器地址在某些情况下并不相同。

示例

以下示例显示如何分发通过位于 ACL acl_dmz1 和 acl_dmz2 所指定地址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
```

相关命令

命令	说明
match interface	分发其下一个跃点跃出指定的接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的 ACL 之一所传递的任何路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match login-name

要配置即时消息客户端登录名的匹配条件，请在类映射或策略映射配置模式下使用 **match login-name** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] login-name regex [*regex_name* | **class** *regex_class_name*]

no match [not] login-name regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 IM 类映射或策略映射中配置。在 IM 类映射中只能输入一个条目。

示例

以下示例显示如何在即时消息类映射中配置客户端登录名的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

相关命令

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。
show running-config class-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，请使用此命令的 **no** 形式。

match [not] media-type [audio | data | video]

no match [not] media-type [audio | data | video]

语法说明

audio	指定此项可匹配音频媒体类型。
data	指定此项可匹配数据媒体类型。
video	指定此项可匹配视频媒体类型。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 H.323 检查类映射中配置音频媒体类型的匹配条件：

```
ciscoasa(config-cmap)# match media-type audio
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match message id

要为 GTP 消息 ID 配置匹配条件，请在类映射或策略映射配置模式下使用 **match message id** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] message id [*message_id* | **range** *lower_range upper_range*]

no match [not] message id [*message_id* | **range** *lower_range upper_range*]

语法说明

message_id	指定介于 1 到 255 之间的字母数字标识符。
range *lower_range upper_range*	指定 ID 的上限和下限。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 GTP 类映射或策略映射中配置。在 GTP 类映射中只能输入一个条目。

示例

以下示例显示如何在 GTP 检查策略映射中配置消息 ID 的匹配条件：

```
ciscoasa(config-cmap)# match message id 33
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match message length

要为 GTP 消息 ID 配置匹配条件，请在类映射或策略映射配置模式下使用 **match message length** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] message length min *min_length* **max** *max_length*

no match [not] message length min *min_length* **max** *max_length*

语法说明

min *min_length*	指定最短消息 ID 长度。值介于 1 到 65536 之间。
max *max_length*	指定最长消息 ID 长度。值介于 1 到 65536 之间。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 GTP 类映射或策略映射中配置。在 GTP 类映射中只能输入一个条目。

示例

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-cmap)# match message length min 8 max 200
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match message-path

要配置 SIP 消息所采用路径 （如 Via 报头字段中所指定）的匹配条件，请在类映射或策略映射配置模式下使用 **match message-path** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] message-path regex [*regex_name* | **class** *regex_class_name*]

no match [not] message-path regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 SIP 类映射或策略映射中配置。在 SIP 类映射中只能输入一个条目。

示例

以下示例显示如何为 SIP 检查类映射中 SIP 消息采取的路径配置匹配条件：

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match metric

要重分布指定了指标的路由，请在路由映射配置模式下使用 **match metric** 命令。要删除条目，请使用此命令的 **no** 形式。

match metric *number*

no match metric *number*

语法说明

number	路由指标，可以是 IGRP 的五部分指标；有效值为 0 到 4294967295。

默认值

不对指标值进行过滤。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。可以按任何顺序指定 **match** 命令，并且所有 **match** 命令都必须 “ 通过 ” 才可使路由根据 **set** 命令指定的设置操作重分布。**match** 命令的 **no** 形式可删除指定的匹配条件。

一个路由映射可有多个部分。不匹配至少一个与 **route-map** 命令相关的匹配子句的任何路由都会被忽略。要想只修改部分数据，必须配置第二个路由映射部分并且指定显式匹配。

示例

以下示例显示如何采用指标 5 重分布路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

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 **match mime** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] mime [encoding *type* **| filename length gt** *bytes* **| filetype** *regex***]**

no match [not] mime [encoding *type* **| filename length gt** *bytes* **| filetype** *regex***]**

语法说明

encoding *type*	指定此项可匹配编码类型。
filename length gt *bytes*	指定此项可匹配文件名长度。
filetype *regex*	指定此项可匹配文件类型。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何在 ESMTP 检查策略映射中配置 mime 文件名长度的匹配条件：

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match mime filename length gt 255
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match peer-ip-address

要配置即时消息对等设备 IP 地址的匹配条件，请在类映射或策略映射配置模式下使用 **match peer-ip-address** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] peer-ip-address *ip_address ip_address_mask*

no match [not] peer-ip-address *ip_address ip_address_mask*

语法说明

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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 IM 类映射或策略映射中配置。在 IM 类映射中只能输入一个条目。

示例

以下示例显示如何在即时消息类映射中配置对等设备 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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match peer-login-name

要配置即时消息对等设备登录名的匹配条件，请在类映射或策略映射配置模式下使用 **match peer-login-name** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] peer-login-name regex [*regex_name* | **class** *regex_class_name*]

no match [not] peer-login-name regex [*regex_name* | **class** *regex_class_name*]

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 IM 类映射或策略映射中配置。在 IM 类映射中只能输入一个条目。

示例

以下示例显示如何在即时消息类映射中配置对等设备登录名的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

相关命令

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。
show running-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，通过在类映射配置模式下使用 **match port** 命令将 TCP 或 UDP 端口匹配您要应用的操作。要删除 **match port** 命令，请使用此命令的 **no** 形式。

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

语法说明

eq *port*	指定一个端口名称或端口号。
range *beg_port end_port*	指定介于 1 到 65535 之间的开始和结束端口范围值。
tcp	指定 TCP 端口。
udp	指定 UDP 端口。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 或 **class-map type management** 命令标识您要对其应用操作的第 3 层和第 4 层流量。

   输入 **class-map** 命令后，您可以输入 **matchport** 命令以标识该流量。或者，您可以输入不同类型的 **match** 命令，例如 **match access-list** 命令 （**class-map type management** 命令只允许 match port 命令）。您只能在类映射中包含一条 **match port** 命令，无法将其与其他类型的 **match** 命令组合使用。
2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。
3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。
4. 使用 **service-policy** 命令在接口上激活操作。

示例

以下示例显示如何使用类映射和 **match port** 命令定义流量类。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

相关命令

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 access-list	根据访问列表匹配流量。
match any	包括类映射中的所有流量。
show running-config class-map	显示有关类映射配置的信息。

match precedence

要在类映射中指定优先级值，请在类映射配置模式下使用 **match precedence** 命令。要删除此指定，请使用此命令的 **no** 形式。

match precedence *value*

no match precedence *value*

语法说明

value	最多指定四个优先级值 （用空格分隔）。范围为 0 到 7。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

使用 **match precedence** 命令以指定通过 IP 报头中的 TOS 字节表示的值。

示例

以下示例显示如何使用类映射和 **match precedence** 命令定义流量类。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match precedence 1
ciscoasa(config-cmap)#
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
match any	包括类映射中的所有流量。
show running-config class-map	显示有关类映射配置的信息。

match protocol

要配置特定即时消息协议（例如 MSN 或雅虎）的匹配条件，请在类映射或策略映射配置模式下使用 **match protocol** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] protocol {**msn-im** | **yahoo-im**}

no match [not] protocol {**msn-im** | **yahoo-im**}

语法说明

msn-im	指定此项可匹配 MSN 即时消息协议。
yahoo-im	指定此项可匹配雅虎即时消息协议。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	**修改**
7.2(1)	引入了此命令。

使用指南

此命令可在 IM 类映射或策略映射中配置。在 IM 类映射中只能输入一个条目。

示例

以下示例显示如何在即时消息类映射中配置雅虎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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match question

要配置 DNS 问题或资源记录的匹配条件，请在类映射或策略映射配置模式下使用 **match question** 命令。要删除配置的部分，请使用此命令的 **no** 形式。

match {**question** | {**resource-record answer** | **authority** | **additional**}}

no match {**question** | {**resource-record answer** | **authority** | **additional**}}

语法说明

question	指定 DNS 消息的问题部分。
resource-record	指定 DNS 消息的资源记录部分。
answer	指定答案 RR 部分。
authority	指定机构 RR 部分。
additional	指定附加 RR 部分。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

默认情况下，此命令检查 DNS 报头并匹配指定的字段。它可以与其他 DNS **match** 命令配合使用，从而定义特定问题或 RR 类型的检查。

此命令可在 DNS 类映射或策略映射内进行配置。在一个 DNS 类映射内只能输入一个条目。

示例

以下示例显示如何在 DNS 检查策略映射中配置 DNS 问题的匹配条件：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match question
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

第 11 章

match regex 至 message-length 命令

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 **match regex** 命令。要从类映射删除正则表达式，请使用此命令的 **no** 形式。

match regex *name*

no match regex *name*

语法说明

name	使用 **regex** 命令添加的正则表达式名称。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Class-map type regex 配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
7.0(2)	我们引入了此命令。

使用指南

regex 命令可用于各种需要文本匹配的功能。您可以先后使用 **class - map type regex** 命令和多个 **match regex** 命令组织正则表达式类映射中的多个正则表达式。

例如，您可以使用检查策略映射配置特殊的应用检查操作 （请参阅 **policy map type inspect** 命令）。在检查策略映射中，可以通过创建包含一个或多个 **match** 命令的检查类映射来标识要操作的流量，也可以直接在检查策略映射中使用 **match** 命令。有些 **match** 命令可让您标识数据包中使用正则表达式的文本，例如，您可以匹配 HTTP 数据包中的 URL 字符串。

示例

下面是 HTTP 检查策略映射和相关类映射的示例。此策略映射由服务策略启用的第 3/4 层策略映射激活。

```
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
```

相关命令

命令	说明
class-map type regex	创建正则表达式类映射。
regex	添加正则表达式。
test regex	测试正则表达式。

match req-resp

要配置 HTTP 请求和响应的匹配条件，请在策略映射配置模式下使用 **match req-resp** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] req-resp content-type mismatch

no match [not] req-resp content-type mismatch

语法说明

content-type	指定将响应中的内容类型与请求中的接受类型匹配。
mismatch	指定响应中的内容类型字段必须与请求的接受字段中的一个 mime 类型匹配。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令启用下列检查：

- 检查报头内容类型的值是否在支持的内容类型的内部列表中。
- 检查报头内容类型与消息的数据或正文部分的实际内容是否匹配。
- 检查 HTTP 响应中的内容类型字段与相应 HTTP 请求消息中的 **accept** 字段是否匹配。

如果消息未通过以上检查， ASA 将执行配置的操作。

以下是支持的内容类型列表。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	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 |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

此列表中的某些内容类型可能没有对应的正则表达式 （幻数），因此无法在消息的正文部分验证。此时将允许 HTTP 消息。

示例

以下示例显示在 HTTP 策略映射中如何基于 HTTP 消息的内容类型限制 HTTP 流量：

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# match req-resp content-type mismatch
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match request-command

要限制特定 FTP 命令，请在类映射或策略映射配置模式下使用 **match request-command** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] request-command *ftp_command [ftp_command...]*

no match [not] request-command *ftp_command [ftp_command...]*

语法说明

ftp_command	指定一个或多个要限制的 FTP 命令。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 FTP 类映射或策略映射中配置。在 FTP 类映射中只能输入一个条目。

示例

以下示例显示如何为 FTP 检查策略映射中的特定 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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match request-method

要为 SIP 方法类型配置匹配条件，请在类映射或策略映射配置模式下使用 **match request - method** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] request-method *method_type*

no match [not] request-method *method_type*

语法说明

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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 SIP 类映射或策略映射中配置。在 SIP 类映射中只能输入一个条目。

示例

以下示例显示如何为 SIP 检查类映射中 SIP 消息采取的路径配置匹配条件：

```
ciscoasa(config-cmap)# match request-method ack
```

相关命令

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。
show running-config class-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，请在策略映射配置模式下使用 **match request method** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] request {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

no match [not] request {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

语法说明

built-in-regex	指定内容类型、方法或传输编码的内置 regex。
class *class_map name*	指定 regex 类型的类映射名称。
regex *regex_name*	指定使用 **regex** 命令配置的正则表达式名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

表 11-1　内置 Regex 值

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

示例

以下示例显示如何定义 HTTP 检查策略映射，以允许和记录尝试使用方法 “GET” 或 “PUT” 访问 “www\.example.com/.*\.asp” 或 “www\example[0-9][0-9]\.com” 的任何 HTTP 连接。默认允许所有其他 URL/ 方法组合：

```
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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match route-type

要重分布指定类型的路由，请在路由映射配置模式下使用 **match route-type** 命令。要删除路由类型条目，请使用此命令的 **no** 形式。

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

语法说明

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。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

route-map 全局配置命令以及 **match** 和 **set** 配置命令可用于定义在不同路由协议之间重分布路由的条件。每个 **route-map** 命令都有关联的 **match** 和 **set** 命令。 **match** 命令指定匹配条件 - 允许当前 **route-map** 命令重分布的条件。**set** 命令指定设置操作 - 在满足 **match** 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。您可以按任意顺序输入 **match** 命令。所有 **match** 命令必须“通过”才可使路由根据 **set** 命令指定的设置操作重分布。 **match** 命令的 **no** 形式可删除指定的匹配条件。

一个路由映射可有多个部分。不匹配至少一个与 **route-map** 命令相关的匹配子句的任何路由都会被忽略。要想只修改部分数据，必须配置第二个路由映射部分并且指定显式匹配。

对于 OSPF，**external type-1** 关键字只匹配 1 类外部路由，**external type-2** 关键字只匹配 2 类外部路由。

示例

以下示例显示如何重分布内部路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

相关命令

命令	说明
match interface	分发其下一跃点并非指定接口之一的任何路由。
match ip next-hop	分发下一跃点路由器地址由指定的访问列表之一所传递的任何路由。
match metric	重分布指定了指标的路由。
route-map	定义从一个路由协议到另一个的重分布路由的条件。
set metric	指定目标路由协议中用于路由映射的指标值。

match rtp

要在类映射中指定偶数端口号的 UDP 端口范围，请在类映射配置模式下使用 **match rtp** 命令。要删除此指定，请使用此命令的 **no** 形式。

match rtp *starting_port range*

no match rtp *starting_port range*

语法说明

starting_port	指定偶数 UDP 目标端口下限。范围是 2000-65535
range	指定 RTP 端口的范围。范围是 0-16383。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

使用 **match rtp** 命令匹配 RTP 端口 （*starting_port* 与 *starting_port* 之间的偶数 UDP 端口号加上 *range*）。

示例

以下示例显示如何使用类映射和 **match rtp** 命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match rtp 20000 100
ciscoasa(config-cmap)#
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
match any	包括类映射中的所有流量。
show running-config class-map	显示有关类映射配置的信息。

match sender-address

要在 ESMTP 发件人电邮地址上配置匹配条件，请在策略映射配置模式下使用 **match sender-address** 命令。要禁用此功能，请使用此命令的 **no** 形式。

match [not] sender-address [length gt *bytes* **| regex** *regex***]**

no match [not] sender-address [length gt *bytes* **| regex** *regex***]**

语法说明

length gt *bytes*	指定要匹配发件人电邮地址长度。
regex *regex*	指定要匹配正则表达式。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何为 ESMTP 检查策略映射中长度大于 320 个字符的发件人电邮地址配置匹配条件：

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match server

要为 FTP 服务器配置匹配条件，请在类映射或策略映射配置模式下使用 **match server** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] server regex [*regex_name* | **class** *regex_class_name]*

no match [not] server regex [*regex_name* | **class** *regex_class_name]*

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 FTP 类映射或策略映射中配置。在 FTP 类映射中只能输入一个条目。

ASA 使用在连接到 FTP 服务器时显示在登录提示上方的初始 220 服务器消息匹配服务器名称。220 服务器消息可能包含多行。服务器匹配不是基于通过 DNS 解析的服务器名称的 FQDN。

示例

以下示例显示如何为 FTP 检查策略映射中的 FTP 服务器配置匹配条件。

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

相关命令

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。
show running-config class-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，请在类映射或策略映射配置模式下使用 **match service** 命令。要删除匹配条件，请使用此命令的 **no** 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**}

语法说明

chat	指定要匹配即时消息聊天服务。
file-transfer	指定要匹配即时消息文件传输服务。
games	指定要匹配即时消息游戏服务。
voice-chat	指定要匹配即时消息语音聊天服务。
webcam	指定要匹配即时消息网络摄像头服务。
conference	指定要匹配即时消息会议服务。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 IM 类映射或策略映射中配置。在 IM 类映射中只能输入一个条目。

示例

以下示例显示如何为即时消息类映射中的聊天服务配置匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match third-party-registration

要为第三方注册的请求者配置匹配条件，请在类映射或策略映射配置模式下使用 **match third-party-registration** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] third-party-registration regex [*regex_name* | **class** *regex_class_name]*

no match [not] third-party-registration regex [*regex_name* | **class** *regex_class_name]*

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 SIP 类映射或策略映射中配置。在 SIP 类映射中只能输入一个条目。

third-party registration match 命令用于标识可以向 SIP 注册服务器或 SIP 代理注册他人的用户。在 From 和 To 值不匹配时，通过 REGISTER 消息中的 From 报头字段标识。

示例

以下示例显示如何为 SIP 检查类映射中的第三方注册配置匹配条件：

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match tunnel-group

要匹配属于以前定义的隧道组的类映射中的流量，请在类映射配置模式下使用 **match tunnel-group** 命令。要删除此指定，请使用此命令的 **no** 形式。

match tunnel-group *name*

no match tunnel-group *name*

语法说明

name	隧道组名称的文本。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

match 命令用于标识类映射的流量类中包含的流量。它们使用不同的标准来定义类映射中的流量。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。从类映射配置模式，可以使用 **match** 命令定义要包含在类中的流量。

在流量类应用到接口之后，该接口上收到的数据包将与类映射的 **match** 语句定义的条件进行比较。如果数据包符合指定的条件，它将包含在流量类中，并且会遭受与该流量类关联的任何操作。不符合任何流量类中任何条件的数据包将被分配给默认流量类。

要启用基于流的策略操作，请使用 **match flow ip destination-address** 和 **match tunnel-group** 命令以及 **class-map**、**policy-map** 和 **service-policy** 命令。定义流量的条件是目标 IP 地址。所有前往唯一 IP 目标地址的流量都被视为流。策略操作应用到每个流而不是整个流量类。使用 **police** 命令应用 QoS 操作管制。使用 **match tunnel-group** 及 **match flow ip destination-address** 将隧道组中的每个隧道限于指定的速率。

示例

以下示例显示如何在隧道组中启用基于流的策略以及将每个隧道限于指定的速率。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match tunnel-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
```

相关命令

命令	说明
class-map	将流量类应用到接口。
clear configure class-map	删除所有流量映射定义。
match access-list	标识类映射内的访问列表流量。
show running-config class-map	显示有关类映射配置的信息。
tunnel-group	创建和管理 IPsec 及 L2TP 的连接特定记录数据库。

match uri

要为 SIP 报头中的 URI 配置匹配条件，请在类映射或策略映射配置模式下使用 **match uri** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] uri {**sip** | **tel**} **length gt** *gt_bytes*

no match [not] uri {**sip** | **tel**} **length gt** *gt_bytes*

语法说明

sip	指定 SIP URI。
tel	指定电话 URI。
length gt *gt_bytes*	指定 URI 的最大长度。值介于 0 到 65536 之间。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 SIP 类映射或策略映射中配置。在 SIP 类映射中只能输入一个条目。

示例

下例显示如何为 SIP 消息中的 URI 配置匹配条件：

```
ciscoasa(config-cmap)# match uri sip length gt
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match url-filter

要为 RTSP 消息中的 URL 过滤配置匹配条件，请在类映射或策略映射配置模式下使用 **match url-filter** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] url-filter regex [*regex_name* | **class** *regex_class_name]*

no match [not] url-filter regex [*regex_name* | **class** *regex_class_name]*

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

此命令可在 RTSP 类别映射或策略映射中配置。

示例

以下示例显示如何为 RTSP 检查策略映射中的 URL 过滤配置匹配条件。

```
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
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match user group

要将用户或组指定到云网络安全的白名单，请在参数配置模式下使用 **match user group** 命令。您可以先输入 **class-map type inspect scansafe** 命令来访问参数配置模式。要取消匹配，请使用此命令的 **no** 形式。

match [**not**] {[**user** *username*] [**group** *groupname*]}

no match [**not**] {[**user** *username*] [**group** *groupname*]}

语法说明

not	（可选）指定应使用云网络安全过滤的用户和 / 或组。例如，如果将组“cisco” 加入白名单，但您想扫描来自用户 “johncrichton” 和 “aerynsun” 的流量，便可对这些用户指定 **match not**。
user *username*	将用户指定到白名单。
group *groupname*	将组指定到白名单。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

如果使用 AAA 规则或 IDFW，您可以配置 ASA，使来自特定用户或组的网络流量 （原来匹配服务策略规则）不会重定向到云网络安全代理服务器进行扫描。绕过云网络安全扫描时， ASA 直接从原来请求的网络服务器检索内容，而不用连接代理服务器。当它收到网络服务器的响应时，会将数据发送到客户端。此过程称为 “ 白名单 ” 流量。

虽然当您使用 ACL 配置要发送到云网络安全的流量类时，同样可以根据用户或组排除流量，但您可能会发现使用白名单更直接。请注意，白名单功能只能基于用户和组，而不能基于 IP 地址。

将白名单创建为检查策略映射的一部分 (**policy-map type inspect scansafe**) 之后，您可以在使用 **inspect scansafe** 命令指定云网络安全操作时使用此映射。

示例

以下示例将 HTTP 及 HTTPS 检查策略映射的相同用户和组加入白名单：

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

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前所等待的时长。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

match username

要为 FTP 用户名配置匹配条件，请在类映射或策略映射配置模式下使用 **match username** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] username regex [*regex_name* | **class** *regex_class_name]*

no match [not] username regex [*regex_name* | **class** *regex_class_name]*

语法说明

regex_name	指定正则表达式。
class *regex_class_name*	指定正则表达式类映射。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	**修改**
7.2(1)	引入了此命令。

使用指南

此命令可在 FTP 类映射或策略映射中配置。在 FTP 类映射中只能输入一个条目。

示例

以下示例显示如何为 FTP 检查类映射中的 FTP 用户名配置匹配条件。

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

match version

要为 GTP 消息 ID 配置匹配条件，请在类映射或策略映射配置模式下使用 **match message length** 命令。要删除匹配条件，请使用此命令的 **no** 形式。

match [not] version [*version_id* | **range** *lower_range upper_range]*

no match [not] version [*version_id* | **range** *lower_range upper_range]*

语法说明

vresion_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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
类映射或策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 GTP 类映射或策略映射中配置。在 GTP 类映射中只能输入一个条目。

示例

以下示例显示如何为 GTP 检查类映射中的消息版本配置匹配条件：

```
ciscoasa(config-cmap)# match version 1
```

相关命令

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。
show running-config class-map	显示有关类映射配置的信息。

max-failed-attempts

要指定服务器组中任何给定服务器在禁用之前允许的最大失败尝试次数，请在 AAA 服务器组配置模式下使用 **max-failed-attempts** 命令。要删除此指定并恢复为默认值，请使用此命令的 **no** 形式。

max-failed-attempts *number*

no max-failed-attempts

语法说明

number	1-5 范围内的整数，指定在之前的 **aaa-server** 命令中指定的服务器组中任何给定服务器允许的连接尝试失败次数。

默认值

number 的默认值是 3。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

必须配置了 AAA 服务器或组后才可发出此命令。

示例

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 4
ciscoasa(config-aaa-server-group)#
```

相关命令

命令	说明
aaa-server *server-tag* **protocol** *protocol*	进入 AAA 服务器组配置模式，以便您配置组特定的并适用于组中所有主机的 AAA 服务器参数。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

max-forwards-validation

要对 Max-forwards 报头字段 0 启用检查，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，请使用此命令的 **no** 形式。

max-forwards-validation action {drop | drop-connection | reset | log} [log]

no max-forwards-validation action {drop | drop-connection | reset | log} [log]

语法说明

drop	如果发生违规，则丢弃数据包。
drop-connection	丢弃违规的连接。
reset	重置违规的连接。
log	指定违规情况下的独立或附加日志。它可以关联到任何操作。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令将统计到达目标所经过的跃点数，在到达目标之前不能为 0。

示例

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
```

相关命令

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

max-header-length

要基于 HTTP 报头长度限制 HTTP 流量，请在 HTTP 映射配置模式（可使用 **http-map** 命令访问）下使用 **max-header-length** 命令。要删除此命令，请使用此命令的 **no** 形式。

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

语法说明

action	消息未通过此命令检查时执行的操作。
allow	允许消息。
drop	关闭连接。
bytes	字节数，范围是 1-65535。
log	（可选）生成系统日志。
request	请求消息。
reset	将 TCP 重置消息发送到客户端和服务器。
response	（可选）响应消息。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在启用 **max-header-length** 命令后，ASA 只允许消息的 HTTP 报头长度在配置的限制范围内，否则将执行指定的操作。使用 **action** 关键字使 ASA 重置 TCP 连接，并且选择性地创建系统日志条目。

示例

以下示例将 HTTP 请求限于其 HTTP 报头不超过 100 字节的请求。如果报头太长， ASA 会重置 TCP 连接并创建系统日志条目。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug appfw	显示与增强型 HTTP 检查关联的流量详细信息。
http-map	为配置增强型 HTTP 检查定义 HTTP 映射。
inspect http	应用要用于应用检查的特定 HTTP 映射。
policy-map	将类映射与特定安全操作关联。

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，请再次使用该命令。

max-object-size *integer range*

语法说明

integer range	0 - 10000 KB

默认值

1000 KB

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

最大对象大小必须大于最小对象大小。如果启用了缓存压缩， ASA 将在压缩对象后计算大小。

示例

以下示例显示如何将最大大小设置为 4000 KB：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# max-object-size 4000
ciscoasa(config-webvpn-cache)#
```

相关命令

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	配置不需要重新验证即缓存对象的到期时间。
lmfactor	为缓存只有最后修改时间戳的对象设置重新验证策略。
min-object-size	定义要缓存的对象的最小大小。

max-retry-attempts

要配置在请求超时之前 ASA 重试失败的 SSO 身份验证尝试次数，请在特定 SSO 服务器类型的 webvpn 配置模式下使用 **max-retry-attempts** 命令。

要恢复默认值，请使用此命令的 **no** 形式。

max-retry-attempts *retries*

no max-retry-attempts

语法说明

retries	ASA 在 SSO 身份验证尝试失败后的重试次数。范围为 1 至 5 次重试。

默认值

此命令的默认值是 3。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
config-webvpn-sso-saml	• 是	—	• 是	—	—
config-webvpn-sso-siteminder	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

单点登录支持，仅适用于 WebVPN，可让用户访问不同服务器上的不同安全服务，而无需重复输入用户名和密码。ASA 当前支持 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。

在配置 ASA 支持 SSO 身份验证后，可以调整两个超时参数。

- 使用 **max-retry-attempts** 命令设置的在 ASA SSO 身份验证尝试失败后的重试次数。
- 失败的 SSO 身份验证尝试超时的秒数 （请参阅 **request-timeout** 命令）。

示例

以下示例 （在 webvpn-sso-siteminder 配置模式中）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)#
```

相关命令

命令	说明
policy-server-secret	创建用于对发往 SiteMinder SSO 服务器的身份验证请求进行加密的密钥。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

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（可使用 **http-map** 命令访问）下使用 **max-uri-length** 命令。要删除此命令，请使用此命令的 **no** 形式。

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

语法说明

action	消息未通过此命令检查时执行的操作。
allow	允许消息。
drop	关闭连接。
bytes	字节数，范围是 1-65535。
log	（可选）生成系统日志。
reset	将 TCP 重置消息发送到客户端和服务器。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在启用 **max-uri-length** 命令后，ASA 只允许消息的 URI 在配置的限制范围内，否则将执行指定的操作。使用 **action** 关键字使 ASA 重置 TCP 连接，并且创建系统日志条目。

长度小于或等于配置值的 URI 将被允许。否则会执行指定的操作。

示例

以下示例将 HTTP 请求限于其 URI 不超过 100 字节的请求。如果 URI 太长，ASA 会重置 TCP 连接并创建系统日志条目。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
debug appfw	显示与增强型 HTTP 检查关联的流量详细信息。
http-map	为配置增强型 HTTP 检查定义 HTTP 映射。
inspect http	应用要用于应用检查的特定 HTTP 映射。
policy-map	将类映射与特定安全操作关联。

maximum-paths

要控制路由表中可安装的最大并行 BGP 路由数，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*

no maximum-paths [**ibgp**] *number-of-paths*

语法说明

ibgp	（可选）这可让您控制可以安装到路由表中的最大内部 BGP 路由数。
number-of-paths	要安装到路由表的路由数。

默认值

默认情况下， BGP 只在路由表中安装一个最佳路径。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **maximum-paths** 命令，可以为 BGP 对等会话配置等价或非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，路由的下一个跃点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 路由过程仍会通告到 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、自主系统路径 （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。

示例

以下示例配置安装两个并行 iBGP 路径：

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

相关命令

命令	说明
show bgp	显示 BGP 路由表中的条目。

mcc

要标识用于 IMSI 前缀过滤的移动国家 / 地区代码和移动网络代码，请在 GTP 映射配置模式下使用 **mcc** 命令。要删除配置，请使用此命令的 **no** 形式。

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

语法说明

country_code	用于标识移动国家 / 地区代码的非零三位数值。一位或两位数条目前面将附加 0 来创建三位数值。
network_code	用于标识网络代码的两位或三位数值。

默认值

默认情况下， ASA 不检查有效的 MCC/MNC 组合。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令用于 IMSI 前缀过滤。收到的数据包的 IMSI 中的 MCC 和 MNC 与使用此命令配置的 MCC/MNC 进行比较，如果不匹配，就会丢弃数据包。

必须使用此命令才能启用 IMSI 前缀过滤。您可以配置多个实例来指定允许的 MCC 和 MNC 组合。默认情况下， ASA 不检查 MNC 和 MCC 组合的有效性，因此，您必须验证所配置的组合的有效性。要查找有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议 *Identification Plan for Land Mobile Stations （陆上移动站的标识计划）*。

示例

以下示例标识 MCC 为 111 和 MNC 为 222 的 IMSI 前缀过滤的流量：

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# mcc 111 mnc 222
ciscoasa(config-gtpmap)#
```

相关命令

命令	说明
clear service-policy inspect gtp	清除全局 GTP 统计信息。
debug gtp	显示有关 GTP 检查的详细信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的特定 GTP 映射。
show service-policy inspect gtp	显示 GTP 配置。

mdm-proxy

要进入 MDM 代理配置模式，请在全局配置模式下使用 **mdm-proxy** 命令。要删除在 MDM 命令模式中输入的任何命令，请使用此命令的 **no** 形式。

mdm-proxy

no mdm-proxy

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

mdm-proxy 命令配置移动设备管理代理（Cisco Mobile Enablement 解决方案的一个组件）。MDM 代理将 ASA 配置为 AnyConnect 设备管理客户端与 ISE MDM 服务器之间的代理，从而允许外部部署移动设备以与内部部署移动设备完全相同的方式参与企业移动设备管理。

指定以下 （在 config-mdm-proxy 模式下）参数以配置 MDM 代理：

- **accounting-server-group** - 输入记帐服务器组的名称
- **authentication-server-group** - 输入身份验证服务器组的名称
- **password-management** - 启用密码管理
- **trustpoint** - 输入与 ASA 要用于代表 MDM 客户端向 MDM 服务器验证自身的证书关联的信任点名称。
- **port** - 配置用于 MDM 注册的端口
- **session-limit** - 设置并行 MDM 会话的最大数
- **session-timeout** - 设置 MDM 注册和签入会话的最长持续时间
- **enable** - 在指定的接口上启用 MDM 代理

示例

以下示例显示如何在 ASA 上配置 MDM 代理：

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# authentication-server-group MDM
ciscoasa(config-mdm-proxy)# accounting-server-group MDM
ciscoasa(config-mdm-proxy)# trustpoint ASDM_TrustPoint1
ciscoasa(config-mdm-proxy)# password-management
ciscoasa(config-mdm-proxy)# port enrollment 443 checkin 444
ciscoasa(config-mdm-proxy)# enable outside
ciscoasa(config-mdm-proxy)# exit
ciscoasa(config)#
```

相关命令

命令	说明
clear configure mdm-proxy	删除 MDM 代理配置。
show running-config mdm-proxy	显示 MDM 代理的运行配置。
show mdm-proxy	显示 MDM 代理统计信息和会话。

media-termination

要指定媒体终端实例以用于到电话代理功能的媒体连接，请在全局配置模式下使用 **media-termination** 命令。

要从电话代理配置删除媒体终端地址，请使用此命令的 **no** 形式。

media-termination *instance_name*

no media-termination *instance_name*

语法说明

instance_name	指定使用媒体终端地址的接口名称。每个接口只能配置一个媒体终端地址。

默认值

此命令没有默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。
8.2(1)	更新了此命令，允许对媒体终端地址使用 NAT。 **rtp-min-port** 和 **rtp-max-ports** 关键字已从命令语法中删除，可作为单独的命令

使用指南

ASA 必须具有符合以下条件的媒体终端 IP 地址：

对于媒体终端实例，您可以为所有接口配置一个全局媒体终端地址，或者为不同的接口分别配置一个媒体终端地址。但不能同时使用全局媒体终端地址以及为每个接口配置的媒体终端地址。

如果为多个接口配置一个媒体终端地址，您必须在 ASA 与 IP 电话通信时使用的每个接口上配置一个地址。

IP 地址是公开路由的地址，也是该接口的地址范围内未使用的 IP 地址。

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

示例

以下示例显示使用媒体终端地址命令指定用于媒体连接的 IP 地址：

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。

media-type

要将媒体类型设置为铜缆或光纤千兆位以太网，请在接口配置模式下使用 **media-type** 命令。ASA 5500 系列自适应安全设备的 4GE SSM 上有光纤 SFP 连接器。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**}

no media-type [rj45 | sfp]

语法说明

rj45	（默认）将媒体类型设为铜缆 RJ-45 连接器。
sfp	将媒体类型设为光纤 SFP 连接器。

默认值

默认值为 **rj45**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

sfp 设置使用固定速度 (1000 Mbps)，因此，**speed** 命令可用于设置接口是否协商链路参数。**sfp** 不支持 **duplex** 命令。

示例

以下示例将媒体类型设为 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
```

相关命令

命令	说明
interface	配置接口并进入接口配置模式。
show interface	显示接口的运行状态和统计信息。
show running-config interface	显示接口配置。
speed	设置接口速度。

member

要为资源类分配情景，请在情景配置模式下使用 **member** 命令。要从类删除情景，请使用此命令的 **no** 形式。

member *class_name*

no member *class_name*

语法说明

class_name	指定使用 **class** 命令创建的类名称。

默认值

默认情况下，情景分配到默认类。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

默认情况下，除非对每个情景实施最大限制，否则所有安全情景可以无限访问 ASA 的资源。但是，如果您发现一个或者多个情景使用过多资源，例如，它们导致其他情景变成被拒绝连接，那么您可以配置资源管理来限制每个情景对资源的使用。 ASA 通过将情景分配到资源类来管理资源。每个情景使用由类设置的资源限制。

示例

以下示例将情景测试分配到 gold 类：

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

相关命令

命令	说明
class	创建资源类。
context	配置安全情景。
limit-resource	设置资源的限制。
show resource allocation	显示如何跨类分配资源。
show resource types	显示可为其设置限制的资源类型。

member-interface

要将物理接口分配到冗余接口，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。您可以将两个成员接口分配到一个冗余接口。要删除成员接口，请使用此命令的 **no** 形式。不能从冗余接口删除全部两个成员接口；冗余接口至少需要一个成员接口。

member-interface *physical_interface*

no member-interface *physical_interface*

语法说明

physical_interface	标识接口 ID，例如 **gigabitethernet 0/1**。请参阅 **interface** 命令了解接受的值。两个成员接口必须属于同一物理类型。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

两个成员接口必须属于同一物理类型。例如，都是以太网。

如果为其中一个成员接口配置了名称，则无法将物理接口添加到冗余接口。必须先使用 **no nameif** 命令删除该名称。

注意事项　如果您正在使用配置中已有的物理接口，删除名称会清除引用该接口的所有配置。

唯一可用于冗余接口对中物理接口的配置是物理参数，例如 **speed** 和 **duplex** 命令、**description** 命令、 **shutdown** 命令。也可以输入运行时命令，例如 **default** 和 **help**。

如果关闭主用接口，则备用接口变为主用接口。

要更改主用接口，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。如果更改配置中成员接口的顺序，MAC 地址会更改以匹配目前列出的第一个接口的 MAC 地址。您也可以将 MAC 地址分配到冗余接口，这样无论成员接口的 MAC 地址为何，都会使用冗余接口上的 MAC 地址（请参阅 **mac-address** 命令或 **mac-address auto** 命令）。当主用接口故障切换到备用接口时，MAC 地址保持不变，因此流量不会中断。

示例

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
```

相关命令

命令	说明
clear interface	清除 **show interface** 命令的计数器。
debug redundant-interface	显示与冗余接口事件或错误相关的调试消息。
interface redundant	创建冗余接口。
redundant-interface	更改活动成员接口。
show interface	显示接口的运行状态和统计信息。

memberof

要指定此用户所属组名称列表，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，请使用此命令的 **no** 形式。

memberof *group_1*[,*group_2*,...*group_n*]

no memberof *group_1*[,*group_2*,...*group_n*]

语法说明

group_1 through group_n	指定此用户所属的组。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
用户名属性配置	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

输入此用户所属组名称的逗号分隔列表。

示例

以下示例是在全局配置模式下输入的，用于创建一个名为 newuser 的用户名，然后将该 newuser 指定为 DevTest 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)#
```

相关命令

命令	说明
clear configure username	清除整个用户名数据库或只清除指定的用户名。
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。
username	创建和管理用户名数据库。

memory delayed-free-poisoner enable

要启用 delayed free-memory poisoner 工具，请在特权 EXEC 模式下使用 **memory delayed-free-poisoner enable** 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在被应用释放后有何变化。

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

语法说明

此命令没有任何参数或关键字。

默认值

memory delayed-free-poisoner enable 命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

启用 delayed free-memory poisoner 工具对内存使用和系统性能有重大影响。此命令应只在思科 TAC 的指导下使用。在大量使用系统的生产环境下不应该运行此工具。

启用此工具时，要求释放 ASA 上运行的应用所用内存的请求将写入 FIFO 队列。当每个请求写入队列时，低层内存管理不需要的每个关联内存字节会写入值 0xcc 而 “ 中毒 ”。

释放的内存请求会一直保留在队列中，直到应用要求的内存超过可用内存。需要内存时，将从队列中提取第一个释放的内存请求，并且验证中毒的内存。

如果内存未经修改，将返回到低层内存池，然后该工具从发出初始请求的应用重新发出内存请求。此过程会持续到为请求的应用释放足够的内存为止。

如果中毒的内存已修改，则系统发生故障并产生诊断输出来确定故障的原因。

delayed free-memory poisoner 工具自动定期验证队列的所有元素。也可以使用 **memory delayed-free-poisoner validate** 命令手动启动验证。

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。

示例

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  |  ..[...`.....l&[.
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                         |  ........

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
```

表 11-2 介绍输出的重要部分。

表 11-2　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	byte offset （字节偏移）与 heap region （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。任何系统堆报头后的八个字节是此工具用来保存各系统报头哈希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。

相关命令

命令	说明
clear memory delayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。
memory delayed-free-poisoner validate	强制验证 delayed free-memory poisoner 工具队列中的元素。
show memory delayed-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 **memory delayed-free-poisoner** 队列中的所有元素，请在特权 EXEC 模式下使用 **memory delayed-free-poisoner validate** 命令。

memory delayed-free-poisoner validate

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

必须先使用 **memory delayed-free-poisoner enable** 命令启用 delayed free-memory poisoner 工具，然后才可发出 **memory delayed-free-poisoner validate** 命令。

memory delayed-free-poisoner validate 命令将使 **memory delayed-free-poisoner** 队列的每个元素得到验证。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。如果没有出现非预期的值，这些元素将保留在队列中被工具正常处理； **memory delayed-free-poisoner validate** 命令不会使队列中的内存返回到系统内存池。

注　delayed free-memory poisoner 工具自动定期验证队列的所有元素。

示例

以下示例将使 **memory delayed-free-poisoner** 队列中的所有元素得到验证：

```
ciscoasa# memory delayed-free-poisoner validate
```

相关命令

命令	说明
clear memory delayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。
memory delayed-free-poisoner enable	启用 delayed free-memory poisoner 工具。
show memory delayed-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，请在特权 EXEC 模式下使用 **memory caller-address** 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，请使用此命令的 **no** 形式。

memory caller-address *startPC endPC*

no memory caller-address

语法说明

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。

默认值

实际调用方 PC 会被记录以用于内存跟踪。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。

使用指南

使用 **memory caller-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　启用调用方地址跟踪时， ASA 的性能可能会临时下降。

示例

以下示例显示使用 **memory caller-address** 命令配置的地址范围，以及 **show memory-caller address** 命令的显示结果：

```
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
```

相关命令

命令	说明
memory profile enable	启用对内存使用 （内存分析）的监控。
memory profile text	配置要分析的内存的文本范围。
show memory	显示最大物理内存及操作系统当前可用内存的摘要。
show memory binsize	显示为特定存储空间分配的区块的摘要信息。
show memory profile	显示 ASA 内存使用情况 （分析）的信息。
show memory-caller address	显示 ASA 上配置的地址范围。

memory profile enable

要启用对内存使用 （内存分析）的监控，请在特权 EXEC 模式下使用 **memory profile enable** 命令。要禁用内存分析，请使用此命令的 **no** 形式。

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

语法说明

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。

默认值

内存分析默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。

使用指南

在启用内存分析之前，必须先使用 **memory profile text** 命令配置要分析的内存文本范围。

部分内存由分析系统保留，直到您输入 **clear memory profile** 命令。请参阅 **show memory status** 命令的输出。

注　启用内存分析时， ASA 的性能可能会临时下降。

以下示例启用内存分析：

```
ciscoasa# memory profile enable
```

相关命令

命令	说明
memory profile text	配置要分析的内存的文本范围。
show memory profile	显示 ASA 内存使用情况 （分析）的信息。

memory profile text

要配置用于分析的内存的程序文本范围，请在特权 EXEC 模式下使用 **memory profile text** 命令。要禁用，请使用此命令的 **no** 形式。

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

语法说明

all	指定内存块的整个文本范围。
endPC	指定内存块的结束文本范围。
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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。

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。

在使用 **memory profile text** 命令输入文本范围后，必须输入 **memory profile enable** 命令才可开始内存分析。内存分析默认禁用。

注　启用内存分析时， ASA 的性能可能会临时下降。

示例

以下示例显示如何在分辨率为 4 的条件下配置要分析的内存文本范围：

```
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　要开始内存分析，必须输入 **memory profile enable** 命令。内存分析默认禁用。

相关命令

命令	说明
clear memory profile	清除内存分析功能保留的缓冲区。
memory profile enable	启用对内存使用 （内存分析）的监控。
show memory profile	显示 ASA 内存使用情况 （分析）的信息。
show memory-caller address	显示 ASA 上配置的地址范围。

memory-size

要在 ASA 上配置 WebVPN 的各个组件可以使用的内存量，请在 webvpn 模式下使用 **memory-size** 命令。您可以 KB 为单位配置具体的内存量，或者将其配置为总内存的百分比。要删除已配置的内存大小，请使用此命令的 **no** 形式。

注　需要重新启动才能使新的内存大小设置生效。

memory-size {**percent** | **kb**} *size*

no memory-size [{**percent** | **kb**} *size*]

语法说明

kb	以千字节指定内存量。
percent	将内存量指定为 ASA 总内存的百分比。
size	指定内存量 （KB 或总内存的百分比）。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

配置的内存量会立即分配。在配置此命令之前，使用 show memory 检查可用的内存量。如果使用总内存的百分比来配置，请确保配置的值小于可用的百分比。如果使用千字节值来配置，请确保配置的值小于以千字节表示的可用内存量。

示例

以下示例显示如何配置 30% 的 WebVPN 内存大小：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

相关命令

命令	说明
show memory webvpn	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，请在特权 EXEC 模式下使用 **memory tracking enable** 命令。要禁用内存跟踪，请使用此命令的 **no** 形式。

memory tracking enable

no memory tracking enable

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(8)	引入了此命令。

使用指南

使用 **memory tracking enable** 命令跟踪堆内存请求。要禁用内存跟踪，请使用此命令的 **no** 形式。

示例

以下示例启用跟踪堆内存请求：

```
ciscoasa# memory tracking enable
```

相关命令

命令	说明
clear memory tracking	清除所有当前收集的信息。
show memory tracking	显示当前分配的内存。
show memory tracking address	列出工具跟踪的每个当前已分配的内存块的大小、位置以及最上方的调用方函数。
show memory tracking dump	此命令显示指定内存地址的大小、位置、部分调用栈和内存转储。
show memory tracking detail	显示用于了解工具内部行为的各种内部详细信息。

merge-dacl

要将可下载 ACL 与思科 AV 对中从 RADIUS 数据包收到的 ACL 进行合并，请在 AAA 服务器组配置模式下使用 **merge-dacl** 命令。要禁止将可下载 ACL 与思科 AV 对中从 RADIUS 数据包收到的 ACL 进行合并，请使用此命令的 **no** 形式。

merge dacl {**before_avpair** | **after_avpair**}

no merge dacl

语法说明

after_avpair	指定可下载 ACL 条目应置于思科 AV 对条目后面。此选项仅适用于 VPN 连接。对于 VPN 用户， ACL 可采用思科 AV 对 ACL、可下载 ACL 以及 ASA 上配置的 ACL 等形式。此选项用于确定可下载 ACL 与 AV 对 ACL 是否合并，不适用于 ASA 上配置的任何 ACL。
before_avpair	指定可下载 ACL 条目应置于思科 AV 对条目前面。

默认值

默认设置为 **no merge dacl**，指定可下载 ACL 不会与思科 AV 对 ACL 合并。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果同时收到了 AV 对和可下载 ACL，将优先使用 AV 对。

示例

以下示例指定可下载 ACL 条目应置于思科 AV 对条目前面：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

相关命令

命令	说明
aaa-server host	标识服务器及其所属的 AAA 服务器组。
aaa-server protocol	标识服务器组名称和协议。
max-failed-attempts	指定向组中的 AAA 服务器发送多少次请求后再尝试下一个服务器。

message-length (DNS Map)

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** 形式可删除此命令。

message-length maximum {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}

no message-length maximum {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}

语法说明

length	DNS 消息中允许的最大字节数 (512-65535)。
client {*length* | **auto**}	客户端 DNS 消息中允许的最大字节数 (512-65535)，或输入 **auto** 以将最大长度设为资源记录中的值。
server {*length* | **auto**}	服务器 DNS 消息中允许的最大字节数 (512-65535)，或输入 **auto** 以将最大长度设为资源记录中的值。

默认值

默认检查将 DNS 最大消息长度设为 512，而客户端长度为 **auto**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

您可以将最大 DNS 消息长度配置为 DNS 检查映射中的参数。

示例

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
```

相关命令

命令	说明
parameter	在策略映射配置模式下进入参数配置模式。
policy-map type inspect dns	创建 DNS 检查策略映射。

message-length (GTP Map)

要过滤不符合配置的最大和最小长度的 GTP 数据包，请在 GTP 映射配置模式 （使用 **gtp-map** 命令访问）下使用 **message-length** 命令。使用 **no** 形式可删除此命令。

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

语法说明

max	指定 UDP 负载中允许的最大字节数。
max_bytes	UDP 负载中的最大字节数。范围为 1 至 65536。
min	指定 UDP 负载中允许的最少字节数。
min_bytes	UDP 负载中的最少字节数。范围为 1 至 65536。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令指定的长度是 GTP 报头与消息其他部分之和，是 UDP 数据包的负载。

示例

以下示例允许长度在 20 字节到 300 字节之间的消息：

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# permit message-length min 20 max 300
ciscoasa(config-gtpmap)#
```

相关命令

命令	说明
clear service-policy inspect gtp	清除全局 GTP 统计信息。
debug gtp	显示有关 GTP 检查的详细信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的特定 GTP 映射。
show service-policy inspect gtp	显示 GTP 配置。

第 12 章

mfib forwarding 至 mus server 命令

mfib forwarding

要在接口上重新启用 MFIB 转发，请在接口配置模式下使用 **mfib forwarding** 命令。要在接口上禁用 MFIB 转发，请使用此命令的 **no** 形式。

mfib forwarding

no mfib forwarding

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， **multicast-routing** 命令将在所有接口上启用 MFIB 转发。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

启用组播路由后，默认情况下 MFIB 转发将在所有接口上启用。使用该命令的 **no** 形式可在特定接口上禁用 MFIB 转发。运行的配置中仅显示该命令的 **no** 形式。

在接口上禁用 MFIB 转发后，该接口不接受任何组播数据包，除非通过其他方法专门进行配置。MFIB 转发禁用时还将阻止 IGMP 数据包。

示例

以下示例在指定的接口上禁用 MFIB 转发：

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

相关命令

命令	说明
multicast-routing	启用组播路由。
pim	在接口上启用 PIM。

migrate

要将 LAN-to-LAN (IKEv1) 或远程访问配置 （SSL 或 IKEv1）迁移到 IKEv2，请从全局配置模式下使用 **migrate** 命令：

migrate {**l2l** | **remote-access** {**ikev2** | **ssl**} | **overwrite**}

语法说明

l2l	将 IKEv1 LAN-to-LAN 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。
overwrite	覆盖现有的 IKEv2 配置。

默认值

没有默认值或行为。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

migrate l2l 命令将所有 LAN-to-LAN IKEv1 配置迁移到 IKEv2。

如果您使用 **overwrite** 关键字，则 ASA 会采用迁移命令覆盖任何现有 IKEv2 配置而不是将其合并。

migrate remote-access 命令将 IKEv1 或 SSL 设置迁移到 IKEv2，但您仍然必须执行以下配置任务：

- 在 webvpn 配置模式下加载 AnyConnect 客户端软件包文件。
- 配置 AnyConnect 客户端配置文件，并为组策略指定这些配置文件。
- 将您用于 IKEv1 连接的任何定制对象与用于 IKEv2 连接的隧道组关联。
- 使用 **crypto ikev2 remote-access trust-point** 命令指定服务器身份验证身份证书 （信任点）。ASA 使用信任点向与 IKEv2 连接的远程 AnyConnect 客户端验证自身。
- 指定 IKEv2 和 / 或 SSL 用于您可能已配置的任何隧道组或组策略，默认组或组策略除外（DefaultWEBVPNGroup 隧道组和默认组策略配置为允许 IKEv2 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。

- 进行任何其他全局、隧道组、组策略设置以更改客户端行为。
- 使用 **crypto ikev2 enable** <*interface*> [**client-services** [*port*]] 命令，配置客户端用于为 IKEv2 下载文件和 / 或执行软件升级的端口。

相关命令

命令	说明
crypto ikev2 enable	在 IPsec 对等设备进行通信的接口上启用 IKEv2 协商。
show run crypto ikev2	显示 IKEv2 配置信息。

min-object-size

要设置 ASA 能够缓存 WebVPN 会话的最小对象大小，请在缓存模式下使用 min-object-size 命令。要更改大小，请再次使用该命令。要设置无最小对象大小，请输入零 (0) 值。

min-object-size *integer range*

语法说明

integer range	0 - 10000 KB。

默认值

默认大小为 0 KB。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

最小对象大小必须小于最大对象大小。如果启用了缓存压缩， ASA 将在压缩对象后计算大小。

示例

以下示例显示如何将最大大小设置为 40 KB：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# min-object-size 40
ciscoasa(config-webvpn-cache)#
```

相关命令

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	配置不需要重新验证即缓存对象的到期时间。
lmfactor	为缓存只有最后修改时间戳的对象设置重新验证策略。
max-object-size	定义要缓存的对象的最大大小。

mkdir

要创建新目录，请在特权 EXEC 模式下使用 **mkdir** 命令。

mkdir [/noconfirm] [disk0: | disk1: | flash:]*path*

语法说明

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）指定外部闪存卡，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， **flash** 关键字是 **disk0** 的别名。
path	要创建的目录的名称和路径。

默认值

如果没有指定路径，则在当前工作目录中创建该目录。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果已存在具有相同名称的目录，则不会创建新目录。

示例

以下示例显示如何创建名为 “backup” 的新目录：

```
ciscoasa# mkdir backup
```

相关命令

命令	说明
cd	将当前工作目录更改为指定的目录。
dir	显示目录内容。
rmdir	删除指定的目录。
pwd	显示当前工作目录。

mobile-device portal

对于所有移动设备，要将无客户端 vpn 访问网络门户从迷你门户更改为完整浏览器门户，请从 webvpn 配置模式下使用 **mobile-device portal** 命令。您只需对运行较旧操作系统（例如 Windows CE）的智能手机进行此配置。您不需要使用现代智能手机配置此选项，因为这些手机在默认情况下使用完整浏览器门户。

mobile-device portal {**full**}

no mobile-device portal {**full**}

语法说明

mobile-device portal {full}	对所有移动设备，将无客户端 vpn 访问门户从迷你门户更改为完整浏览器门户。

命令默认

在您运行该命令之前，默认行为是部分移动设备通过迷你门户访问无客户端 vpn，部分设备使用完整门户进行访问。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(5)	我们在 8.2(5) 和 8.4(2) 中同时引入了此命令。
8.4(2)	我们在 8.2(5) 和 8.4(2) 中同时引入了此命令。

使用指南

仅当思科技术支持中心 (TAC) 建议您这样做时才使用此命令。

示例

对所有移动设备，将无客户端 vpn 访问门户更改为完整浏览器门户。

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

相关命令

命令	说明
show running-config webvpn	显示 webvpn 正在运行的配置。

mode

要将安全情景模式设置为单模式或多模式，请在全局配置模式下使用 **mode** 命令。您可以将一个 ASA 分区为多个虚拟设备，称为安全情景。每个情景像一个独立设备一样有自己的安全策略、接口和管理员。多个情景类似于拥有多个独立设备。在单模式下， ASA 具有单一配置并且行为如同单一设备。在多模式下，您可以创建多个情景，这些情景有各自的配置。允许的情景数量取决于您的许可证。

mode {**single** | **multiple**} [**noconfirm**]

语法说明

multiple	设置多情景模式。
noconfirm	（可选）设置模式而不提示您确认。此选项对于自动化脚本非常有用。
single	将情景模式设置为单模式。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在多情景模式下， ASA 包括每个情景的配置，确定您可以在独立设备上配置的安全策略、接口以及几乎所有选项 （请参阅 **config-url** 命令以确定情景配置位置）。系统管理员可通过在系统配置（该配置与单模式配置类似，是启动配置）中进行配置来添加和管理情景。系统配置可确定 ASA 的基本设置。系统配置本身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，它使用指定作为管理员情景的情景之一。

使用 **mode** 命令更改情景模式时，系统将提示您重新引导。

情景模式 （单模式或多模式）没有存储在配置文件中，不过它在经过重新引导后仍会保留。如果您需要将配置复制到另一个设备，则使用 **mode** 命令设置要匹配的新设备上的模式。

当您从单模式转换为多模式时， ASA 会将正在运行的配置转换成两个文件：包含系统配置的新启动配置，以及包含管理员情景的 admin.cfg （位于内部闪存的根目录中）。原来运行的配置另存为 old_running.cfg （位于内部闪存的根目录中）。原来的启动配置没有保存。 ASA 将管理员情景的条目自动添加到系统配置并采用名称 “admin”。

如果您从多模式转换为单模式，您可能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适用于单模式设备的、正常工作的完整配置。

多情景模式下并非支持所有功能。有关详细信息，请参阅 CLI 配置指南。

示例

以下示例将模式设置为多模式：

```
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模式：

```
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...
```

相关命令

命令	说明
context	在系统配置中配置情景并进入情景配置模式。
show mode	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测，请在全局配置模式下使用 **monitor-interface** 命令。要禁用接口监测，请使用此命令的 **no** 形式。

monitor-interface {*if_name* | **service-module**}

no monitor-interface {*if_name* | **service-module**}

语法说明

if_name	指定所监控接口的名称。
service-module	监控服务模块。如果不希望硬件模块故障（例如 ASA FirePOWER 模块）触发故障切换，可以使用此命令的 **no** 形式禁用模块监控。

默认值

物理接口和服务模块监控默认已启用；而逻辑接口监控默认已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.3(1)	添加了 service-module 关键字。

使用指南

ASA 可以监控的接口数取决于平台，可通过查看 **show failover** 命令输出来确定。

问候消息在每个接口轮询频率时段内在 ASA 故障切换对之间交换。故障切换接口轮询时间为 3 到 15 秒。例如，如果轮询时间设置为 5 秒，则接口上有 5 个连续的问候未收听到（25 秒）时将在该接口上开始测试。

监控的故障切换接口可以具有以下状态：

- Unknown（未知）- 初始状态。此状态也可能意味着状态无法确定。
- Normal（正常）- 接口正在接收流量。
- Testing（测试）- 该接口上有 5 个轮询时间未收听到问候消息。
- Link Down（链路关闭）- 接口或 VLAN 被管理性关闭。
- No Link（无链路）- 接口的物理链路已关闭。
- Failed（故障）- 在该接口上没有收到流量，但在对等设备接口上收听到流量。

在主用 / 主用故障切换中，此命令仅在情景内有效。

示例

以下示例在名为 “inside” 的接口上启用监测：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

相关命令

命令	说明
clear configure monitor-interface	恢复所有接口的默认接口运行状况监控。
failover interface-policy	指定发生故障切换时发生故障的受监控接口必须达到的数量或百分比。
failover polltime	指定接口上两次收到问候消息之间的时间间隔 （主用 / 备用故障切换）。
polltime interface	指定接口上两次收到问候消息之间的时间间隔 （主用 / 主用故障切换）。
show running-config monitor-interface	显示运行的配置中的 **monitor-interface** 命令。

more

要显示文件的内容，请在特权 EXEC 模式下使用 **more** 命令。

more {**/ascii** | **/binary**| **/ebcdic** | **disk0**: | **disk1**: | **flash**: | **ftp**: | **http**: | **https**: | **system**: | **tftp**:}*filename*

语法说明

/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）显示内部闪存中的文件。
disk1:	（可选）显示外部闪存卡中的文件。
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， **flash** 关键字是 **disk0** 的别名。
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 TFTP 服务器上的文件。

默认值

ASCII 模式

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

more filesystem: 命令会提示您输入本地目录或文件系统的别名。

注　当您使用 **more** 命令查看已保存的配置文件时，该配置文件中的隧道组密码将以明文显示。

示例

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
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

相关命令

命令	说明
cd	更改为指定的目录。
pwd	显示当前工作目录。

mount (CIFS)

要使通用互联网文件系统 (CIFS) 对安全设备可访问，请在全局配置模式下使用 **mount** 命令。此命令可让您进入 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。

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

语法说明

domain *domain-name*	（可选）此参数指定 Windows NT 域名 （仅适用于 CIFS 文件系统）。允许最多 63 个字符。
name	指定要分配到本地 CA 的现有文件系统的名称。
no	删除已装载的 CIFS 文件系统并使其无法访问。
password *password*	确定文件系统装载的授权密码。
server *server-name*	指定 CIFS 文件系统服务器的预定义名称 （或以点分十进制表示的 IP 地址）。
share *sharename*	按名称显式标识特定服务器共享 （文件夹）以访问服务器内的数据。
status enable/disable	将文件系统的状态标识为已装载或未装载 （可用或不可用）。
type	指定要装载的文件系统的 CIFS 类型。有关备选的 **type** 关键字，请参阅 **mount (FTP)** 命令。
type cifs	指定所装载的文件系统为 CIFS，即为 CIFS 共享目录提供卷装载功能的文件系统。
user *username*	文件系统装载的授权用户名。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

mount 命令使用可安装文件系统 (IFS) 来装载 CIFS 文件系统。 IFS 是一个文件系统 API，它使安全设备能够标识和加载文件系统的驱动程序。

mount 命令将安全设备上的 CIFS 文件系统连接到 UNIX 文件树。相反地， **no mount** 命令将其分离。

mount 命令中指定的 *mount-name* 可供其他 CLI 命令用于引用安全设备上已装载的文件系统。例如，为本地证书颁发机构设置文件存储的 **database** 命令需要现有已装载文件系统的装载名称，以将数据库文件保存到非闪存存储。

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，它是 Microsoft 开放式、跨平台服务器消息块 (SMB) 协议 （Windows 操作系统中内置的文件共享协议）的增强版本。

使用 **mount** 命令后，始终从 root shell 退出。mount-cifs-config 模式下的 **exit** 关键字会将用户返回到全局配置模式。

要重新连接，请将您的连接重新映射到存储。

注　支持装载 CIFS 和 FTP 文件系统。（请参阅 **mount** *name* **type ftp** 命令。）此版本不支持装载网络文件系统 (NFS) 卷。

示例

以下示例装载 *cifs://amer;chief:big-boy@myfiler02/my_share* 作为标签 *cifs_share*：

```
ciscoasa(config)# mount cifs_share type CIFS
ciscoasa (config-mount-cifs)# server myfiler02a
```

相关命令

命令	说明
debug cifs	记录 CIFS 调试消息。
debug ntdomain	记录 Web VPN NT 域调试消息。
debug webvpn cifs	记录 WebVPN CIFS 调试消息。
dir all-filesystems	显示 ASA 上装载的所有文件系统的文件。

mount (FTP)

要使文件传输协议 (FTP) 文件系统对安全设备可访问，请在全局配置模式下使用 **mount** *name* **type ftp** 命令进入装载 FTP 配置模式。 **no mount** *name* **type ftp** 命令用于卸载 FTP 网络文件系统。

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

语法说明

exit	退出装载 FTP 配置模式并返回到全局配置模式。
ftp	指定所装载的文件系统为 FTP（一个 Linux 内核模块），通过允许您装载 FTP 共享目录的 FTP 卷装载功能增强虚拟文件系统 (VFS)。
mode	将 FTP 传输模式标识为主动或被动。
no	删除已装载的 FTP 文件系统，使其无法访问。
password *password*	确定文件系统装载的授权密码。
path *pathname*	指定到指定 FTP 文件系统服务器的目录路径名。路径名不能包含空格。
server *server-name*	指定 FTPFS 文件系统服务器的预定义名称 （或以点分十进制表示的 IP 地址）。
status enable/disable	将文件系统的状态标识为已装载或未装载 （可用或不可用）。
username *username*	指定文件系统装载的授权用户名。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

mount *name* **type ftp** 命令使用可安装文件系统 (IFS) 来装载指定的网络文件系统。IFS 是一个文件系统 API，它使安全设备能够标识和加载文件系统的驱动程序。

要确认 FTP 文件系统实际已装载，请使用 **dir all-filesystems** 指令。

mount 命令中指定的 mount-name 在其他 CLI 命令引用安全设备上已装载的文件系统时使用。例如，为本地证书颁发机构设置文件存储的 **database** 命令需要已装载文件系统的装载名称，以将数据库文件保存到非闪存存储。

注　创建要求 FTP 服务器必须具有 UNIX 目录列表样式的 FTP 类型装载时，使用 **mount** 命令。Microsoft FTP 服务器将 MS-DOS 目录列表样式作为其默认设置。

注　支持装载 CIFS 和 FTP 文件系统。（请参阅 **mount** *name* **type ftp** 命令。）此版本不支持装载网络文件系统 (NFS) 卷。

示例

本示例装载 *ftp://amor;chief:big-kid@myfiler02* 作为标签 *my ftp*：

```
ciscoasa(config)# mount myftp type ftp server myfiler02a path status enable username chief
password big-kid
```

相关命令

命令	说明
debug webvpn	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

要配置静态组播路由，请在全局配置模式下使用 **mroute** 命令。要删除静态组播路由，请使用此命令的 **no** 形式。

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

语法说明

dense *output_if_name*	（可选）密集模式输出的接口名称。 **dense** *output_if_name* 关键字和参数对仅支持 SMR 末节组播路由（igmp 转发）。
distance	（可选）路由的管理距离。首选距离较短的路由。默认值为 0。
in_if_name	指定 mroute 的传入接口名称。
rpf_addr	指定 mroute 的传入接口。如果 RPF 寻址 PIM 邻居，则 PIM 加入、移植和修剪消息都将发送给它。*rpf-addr* 参数可以是直连系统或网络 / 子网号的主机 IP 地址。当它为路由时，将从单播路由表进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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令可让您静态配置组播源所在的位置。ASA 预期在它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，例如绕过不支持组播路由的路由时，组播数据包可能需要采用与单播数据包不同的路径。

静态组播路由不会进行通告或重分布。

使用 **show mroute** 命令可显示组播路由表的内容。使用 **show running-config mroute** 命令可显示运行的配置中的 mroute 命令。

示例

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
```

相关命令

命令	说明
clear configure mroute	从配置中删除 **mroute** 命令。
show mroute	显示 IPv4 组播路由表。
show running-config mroute	显示配置中的 **mroute** 命令。

mschapv2-capable

要启用到 RADIUS 服务器的 MS-CHAPv2 身份验证请求，请在 aaa-server host 配置模式下使用 **mschapv2-capable** 命令。要禁用 MS-CHAPv2，请使用此命令的 **no** 形式。

mschapv2-capable

no mschapv2-capable

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， MS-CHAPv2 已启用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

要启用 MS-CHAPv2 作为 ASA 与 RADIUS 服务器之间使用的协议用于 VPN 连接，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从 ASA 到 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令的说明。

如果您使用双重身份验证并在隧道组中启用密码管理，则主要和辅助身份验证请求都包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则您可以通过使用 **no mschapv2-capable** 命令将该服务器配置为发送非 MS-CHAPv2 身份验证请求。

示例

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
```

相关命令

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 在远程用户登录时通知用户的当前密码即将到期或已过期。然后， ASA 向用户提供机会来更改密码。
secondary-authentication-server-group	指定辅助 AAA 服务器组，该组不能是 SDI 服务器组。

msie-proxy except-list

要为客户端设备上的本地绕行配置浏览器代理例外列表设置，请在组策略配置模式下输入 **msie-proxy except-list** 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 {**value** *server*[*:port*] | **none**}

no msie-proxy except-list

语法说明

none	表示没有 IP 地址 / 主机名或端口并阻止继承例外列表。
value *server:port*	指定 MSIE 服务器的 IP 地址或名称以及适用于此客户端设备的端口。端口号是可选的。

默认值

默认情况下， msie-proxy except-list 已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

包含代理服务器 IP 地址或主机名以及端口号的行的长度必须小于 100 个字符。

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1（Cisco AnyConnect 安全移动客户端管理员指南，3.1 版）*或适用于您的移动设备的版本说明。

示例

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，包含位于 IP 地址 192.168.20.1、使用端口 880 的服务器：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

相关命令

命令	说明
show running-configuration group-policy	显示配置的 group-policy 属性的值。
clear configure group-policy	删除所有配置的 group-policy 属性。

msie-proxy local-bypass

要配置客户端设备的浏览器代理本地绕行设置，请在组策略配置模式下输入 **msie-proxy local-bypass** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy local-bypass {**enable** | **disable**}

no msie-proxy local-bypass {**enable** | **disable**}

语法说明

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。

默认值

默认情况下， msie-proxy local-bypass 已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1 （Cisco AnyConnect 安全移动客户端管理员指南，3.1 版）*或适用于您的移动设备的版本说明。

示例

以下示例显示如何为名为 FirstGroup 的组策略启用 Microsoft Internet Explorer 代理本地绕行：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

相关命令

命令	说明
show running-configuration group-policy	显示配置的 group-policy 属性的值。
clear configure group-policy	删除所有配置的 group-policy 属性。

msie-proxy lockdown

启用此功能将在 AnyConnect VPN 会话持续时间内隐藏浏览器中的 Connections （连接）选项卡。禁用该功能将使 Connections （连接）选项卡的显示保持不变。

要在 AnyConnect VPN 会话持续时间内隐藏 Connections （连接）选项卡或使其保持不变，请在组策略配置模式下使用 **msie-proxy lockdown** 命令。

msie-proxy lockdown [enable | disable]

语法说明

disable	将浏览器中的 Connections （连接）选项卡保持不变。
enable	在 AnyConnect VPN 会话持续时间内隐藏浏览器中的 Connections （连接）选项卡。

默认值

默认组策略中此命令的默认值为 enable。每个组策略都将从默认组策略继承其默认值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(3)	引入了此命令。

使用指南

此命令在 AnyConnect VPN 会话持续时间内对用户注册表进行临时更改。当 AnyConnect 关闭 VPN 会话后，它会将注册表恢复为会话之前的状态。

您可能会启用此功能以阻止用户指定代理服务和更改 LAN 设置。阻止用户访问这些设置可在 AnyConnect 会话期间增强终端安全性。

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1 （Cisco AnyConnect 安全移动客户端管理员指南，3.1 版）*或适用于您的移动设备的版本说明。

示例

以下示例在 AnyConnect 会话持续时间内隐藏 Connections （连接）选项卡：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

以下示例将使 Connections （连接）选项卡保持不变：

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

相关命令

命令	说明
msie-proxy except-list	指定客户端设备上浏览器代理服务器的例外列表。
msie-proxy local-bypass	绕过客户端设备上配置的本地浏览器代理设置。
msie-proxy method	指定客户端设备的浏览器代理操作。
msie-proxy pac-url	指定从其检索定义代理服务器的代理自动配置文件的 URL。
msie-proxy server	配置客户端设备上浏览器的代理服务器。
show running-config group-policy	显示运行的配置中的组策略设置。

msie-proxy method

要配置客户端设备的浏览器代理操作 （“ 方法 ”），请在组策略配置模式下输入 **msie-proxy method** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

注　有关适用于此语法的资格，请参阅 “ 使用指南 ” 部分。

语法说明

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	对此客户端设备，将浏览器中的 HTTP 浏览器代理服务器设置保持不变。
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-proxy pac-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	将浏览器中的 HTTP 代理服务器设置设为使用 **msie-proxy server** 命令中配置的值。

默认值

默认方法是 use-server。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	添加了 use-pac-url 选项。

使用指南

包含代理服务器 IP 地址或主机名以及端口号的行最多可包含 100 个字符。

此命令支持以下选项组合：

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

您可以使用文本编辑器为您的浏览器创建代理自动配置 (.pac) 文件。.pac 文件是一个 JavaScript 文件，它包含指定要使用的一个或多个代理服务器的逻辑，具体取决于 URL 的内容。.pac 文件位于网络服务器上。当您指定 **use-pac-url** 后，浏览器使用 .pac 文件确定代理设置。使用 **msie-proxy pac-url** 命令指定从其检索 .pac 文件的 URL。

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1（Cisco AnyConnect 安全移动客户端管理员指南，3.1 版）*或适用于您的移动设备的版本说明。

示例

以下示例显示如何将名为 FirstGroup 的组策略的 Microsoft Internet Explorer 代理设置配置为 auto-detect：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

以下示例显示如何将名为 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)#
```

相关命令

命令	说明
msie-proxy pac-url	指定从其检索代理自动配置文件的 URL。
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	显示配置的 group-policy 属性的值。
clear configure group-policy	删除所有配置的 group-policy 属性。

msie-proxy pac-url

要告知浏览器在哪里查找代理信息，请在组策略配置模式下输入 **msie-proxy pac-url** 命令。要从配置中删除该属性，请使用该命令的 **no** 形式。

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

语法说明

none	指定没有 URL 值。
value *url*	指定网站 URL，浏览器在该地址可获得定义要使用的一个或多个代理服务器的代理自动配置文件。

默认值

默认值为 none。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要求

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。要允许使用代理自动配置 URL，您还必须配置 **msie-proxy method** 命令及 **use-pac-url** 选项。

为什么使用此命令

许多网络环境都定义将网络浏览器连接到特定网络资源的 HTTP 代理。 HTTP 流量仅当在浏览器中指定代理并且客户端将 HTTP 流量路由到该代理时才能访问该网络资源。SSLVPN 隧道增加了 HTTP 代理定义的复杂性，因为建立到企业网络的隧道时所需的代理与连接到通过宽带连接的互联网或位于第三方网络上时所需的代理可能不同。

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基于瞬息万变的情况进行选择。通过使用 .pac 文件，管理员可以制作单一脚本文件，从而确定将众多代理中的哪一个用于整个企业范围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平衡。
- 按当天时间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时使用的备用代理服务器。
- 基于本地子网，为漫游用户指定最近的代理。

如何使用代理自动配置功能

您可以使用文本编辑器为您的浏览器创建代理自动配置 (.pac) 文件。.pac 文件是一个 JavaScript 文件，它包含指定要使用的一个或多个代理服务器的逻辑，具体取决于 URL 的内容。使用 **msie-proxy pac-url** 命令指定从其检索 .pac 文件的 URL。然后，当您在 **msie-proxy method** 命令中指定 **use-pac-url** 后，浏览器将使用 .pac 文件确定代理设置。

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1（Cisco AnyConnect 安全移动客户端管理员指南，3.1 版）*或适用于您的移动设备的版本说明。

示例

以下示例显示如何为名为 FirstGroup 的组策略将浏览器配置为从 URL www.example.com 获取其代理设置：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

以下示例对名为 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)#
```

相关命令

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	显示配置的 group-policy 属性的值。
clear configure group-policy	删除所有配置的 group-policy 属性。

msie-proxy server

要配置客户端设备的浏览器代理服务器和端口，请在组策略配置模式下输入 **msie-proxy server** 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**}

no msie-proxy server

语法说明

none	表示没有为代理服务器指定的 IP 地址 / 主机名或端口并阻止继承服务器。
value *server:port*	指定 MSIE 服务器的 IP 地址或名称以及适用于此客户端设备的端口。端口号是可选的。

默认值

默认情况下，未指定任何 msie 代理服务器。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

包含代理服务器 IP 地址或主机名以及端口号的行的长度必须小于 100 个字符。

有关代理设置的进一步信息，请参阅 *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*（*Cisco AnyConnect 安全移动客户端管理员指南，3.1 版*）或适用于您的移动设备的版本说明。

示例

以下示例显示如何为名为 FirstGroup 的组策略配置 IP 地址 192.168.10.1 作为 Microsoft Internet Explorer 代理服务器（使用端口 880）：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

相关命令

命令	说明
show running-configuration group-policy	显示配置的 group-policy 属性的值。
clear configure group-policy	删除所有配置的 group-policy 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。

mtu *interface_name bytes*

no mtu *interface_name bytes*

语法说明

bytes	MTU 中的字节数；有效值为 64 到 9198 字节 （9000 适用于 ASAv）。
interface_name	内部或外部网络接口名称。

默认值

以太网接口的默认 *bytes* 为 1500。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

mtu 命令可让您设置连接上发送的数据大小。大于 MTU 值的数据在发送前将分段。

ASA 支持 IP 路径 MTU 发现 （如 RFC 1191 中所定义），该功能允许主机动态查找和处理沿路径各链路允许的最大 MTU 大小差异。有时， ASA 可能无法转发数据报，原因是数据包大于您为接口设置的 MTU，但 “ 不要分段 ”(DF) 位已设置。网络软件将消息发送到发送主机，提醒其有关问题。主机必须为目标将数据包分段，以使其满足沿路径所有链路的最小数据包大小。

以太网接口块中的默认 MTU 为 1500 字节 （同时也是最大值）。该值足以满足大多数应用，但如果网络状况需要，您可以选择较小的数字。

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 加密的成本，MTU 值应设置为不低于 1380。将接口设置为低于 1380 字节可能会导致丢包。

示例

本例显示如何指定接口的 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
```

相关命令

命令	说明
clear configure mtu	清除所有接口上配置的最大传输单位值。
show running-config mtu	显示当前最大传输单位块大小。

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 **mtu cluster** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

mtu cluster *bytes*

no mtu cluster [*bytes*]

语法说明

bytes	指定集群控制链路接口的最大传输单位，介于 64 到 65,535 字节之间。默认 MTU 为 1500 字节。

命令默认

默认 MTU 为 1500 字节。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

我们建议将 MTU 设置为 1600 字节或更大，这将需要您使用 **jumbo-frame reservation** 命令启用巨型帧保留。

此命令是全局配置命令，但也是引导程序配置的一部分，该配置不会在单位之间复制。

示例

以下示例将集群控制链路 MTU 设置为 9000 字节：

```
ciscoasa(config)# mtu cluster 9000
```

相关命令

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

要配置管理范围组播地址的组播边界，请在接口配置模式下使用 **multicast boundary** 命令。要删除边界，请使用此命令的 **no** 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利用相同的组播组地址。

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

语法说明

acl	指定一个访问列表名称或端口号。访问列表定义受边界影响的地址范围。此命令仅使用标准 ACL，不支持扩展的 ACL。
filter-autorp	过滤边界 ACL 拒绝的自动 RP 消息。如果没有指定，将传递所有自动 RP 消息。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

使用此命令配置接口上的管理范围边界，用于过滤通过 *acl* 参数定义的范围中的组播组地址。标准访问列表定义受影响的地址范围。配置此命令时，不允许任何组播数据包在任一方向流经边界。通过限制组播数据包流，可在不同的管理域中重复利用相同的组播组地址。

如果配置 **filter-autorp** 关键字，则管理范围边界还将检查自动 RP 发现和通告消息，并从边界 ACL 拒绝的自动 RP 数据包中删除任何自动 RP 组范围通告。仅当边界 ACL 允许自动 RP 组范围中的所有地址时，边界才允许并传递自动 RP 组范围通告。如果不允许任何地址，则整个组范围都将被过滤掉并从自动 RP 消息中删除，然后转发自动 RP 消息。

示例

以下示例设置所有管理范围地址的边界并过滤自动 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
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

multicast-routing

要在 ASA 上启用 IP 组播路由，请在全局配置模式下使用 **multicast routing** 命令。要禁用 IP 组播路由，请使用此命令的 **no** 形式。

multicast-routing

no multicast-routing

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， **multicast-routing** 命令在所有接口上启用 PIM 和 IGMP。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

multicast-routing 命令在所有接口上启用 PIM 和 IGMP。

注 PIM 不受 PAT 支持。 PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。

如果安全设备为 PIM RP，请使用安全设备的未转换的外部地址作为 RP 地址。

组播路由表中的条目数量受系统中 RAM 量的限制。表 12-1 根据安全设备中的 RAM 量列出特定组播表的最大条目数量。达到这些限制后，任何新条目都将丢弃。

表 12-1　组播表的条目限制

表	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP 组	1000	3000	5000
PIM 路由	3000	7000	12000

示例

以下示例在 ASA 上启用 IP 组播路由：

```
ciscoasa(config)# multicast-routing
```

相关命令

命令	说明
igmp	在接口上启用 IGMP。
pim	在接口上启用 PIM。

mus

要指定 ASA 在其上标识 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。仅注册在指定子网和接口上找到的 WSA。

mus *IPv4 address IPv4 mask interface_name*

no mus *IPv4 address IPv4 mask interface_name*

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

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

可能有以下命令：

- A.B.C.D - 授权访问 ASA 的 WSA IP 地址。
- host - 客户端通过向虚构主机发送请求，定期检查网络安全设备的连接。默认情况下，虚构主机 URL 为 mus.cisco.com。启用 AnyConnect 安全移动后，网络安全设备将拦截目标为虚构主机的请求并回应客户端。
- password - 配置 WSA 密码。
- server - 配置 WSA 服务器

示例

以下示例允许位于 1.2.3.x 子网上的 WSA 服务器访问 *inside* 接口上的安全移动解决方案：

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

相关命令

命令	说明
mus password	设置 AnyConnect 安全移动通信的共享密钥。
mus server	指定 ASA 在其上侦听 WSA 通信的端口。
show webvpn mus	显示关于活动 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 **mus host** 命令。这是从 ASA 发送到 AnyConnect 客户端的遥测 URL。AnyConnect 客户端使用此 URL 联系专用网络中的 WSA 以实现 MUS 相关服务。要删除使用此命令输入的任何命令，请使用 **no mus host** 命令。

mus host *host name*

no mus host

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

您可以为指定的端口启用 AnyConnect 安全移动。 WSA 端口值为 1 到 21000。如果在命令中没有指定端口，则使用端口 11999。

在执行此命令之前，您必须配置 AnyConnect 安全移动共享密钥。

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

示例

以下示例显示如何输入 AnyConnect 安全移动主机并进入 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
```

相关命令

命令	说明
mus	指定 ASA 在其上标识 WSA 的 IP 范围和接口。
mus password	设置 AnyConnect 安全移动通信的共享密钥。
show webvpn mus	显示关于活动 WSA 连接安全设备的信息。

mus password

要设置 AnyConnect 安全移动通信的共享密钥，请在全局配置模式下输入 **mus password** 命令。要删除共享密钥，请使用 **no mus password** 命令。

mus password

no mus password

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

语法说明

此命令没有任何参数或关键字。

默认值

有效密码通过正则表达式 [0-9, a-z, A-Z,:;_/-]{8,20} 定义。共享密钥的总长度最少为 8 个字符，最多为 20 个字符。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

此 WebVPN 子模式可让您配置 WebVPN 的全局设置。您可以设置 AnyConnect 安全移动通信的共享密钥。

示例

以下示例显示如何输入 AnyConnect 安全移动密码并进入 WebVPN 命令子模式：

```
ciscoasa(config)# mus password <password_string>
ciscoasa(config-webvpn)#
```

相关命令

命令	说明
mus	指定 ASA 在其上标识 WSA 的 IP 范围和接口。
mus server	指定 ASA 在其上侦听 WSA 通信的端口。
show webvpn mus	显示关于活动 WSA 连接安全设备的信息。

mus server

要指定 ASA 在其上监听 WSA 通信的端口，请在全局配置模式下输入 **mus server** 命令。要删除使用此命令输入的任何命令，请使用 **no mus server** 命令。

mus server enable

no mus server enable

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

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

您必须指定 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 （值为 1 到 21000）上的安全 SSL 连接进行。

在执行此命令之前，您必须配置 AnyConnect 安全移动共享密钥。

示例

以下示例显示如何输入 AnyConnect 安全移动密码并进入 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
```

相关命令

命令	说明
mus	指定 ASA 在其上标识 WSA 的 IP 范围和接口。
mus password	设置 AnyConnect 安全移动通信的共享密钥。
show webvpn mus	显示关于活动 WSA 连接安全设备的信息。

第 3 部分

N 至 R 命令

第 13 章

nac-authentication-server-group 至 num-packets 命令

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，请在隧道组常规属性配置模式下使用 **nac-authentication-server-group** 命令。要继承默认远程访问组的身份验证服务器组，请访问其所继承的备用组策略，然后使用此命令的 **no** 形式。

nac-authentication-server-group *server-group*

no nac-authentication-server-group

语法说明

server-group	安全状态验证服务器组的名称，即在 ASA 中使用 **aaa-server host** 命令所配置的名称。该名称必须与该命令中指定的 server-tag 变量匹配。

默认值

此命令没有任何参数或关键字。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(1)	此命令已弃用。 nac-policy-nac-framework 配置模式下的 **authentication-server-group** 命令已取代此命令。

使用指南

配置至少一台访问控制服务器以支持 NAC。使用 **aaa-server** 命令以命名 ACS 组。然后使用 **nac-authentication-server-group** 命令 （对该服务器组使用相同的名称）。

示例

以下示例将 acs-group1 标识为用于 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)
```

以下示例继承默认远程访问组的身份验证服务器组。

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

相关命令

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。
debug eap	启用 EAP 事件的日志记录以调试 NAC 消息。
debug eou	启用 EAP over UDP (EAPoUDP) 事件的日志记录以调试 NAC 消息。
debug nac	启用 NAC 事件的日志记录。
nac	启用对组策略的网络准入控制。

nac-policy

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**

语法说明

nac-policy-name	NAC 策略的名称。输入最多 64 个字符的字符串以命名 NAC 策略。**show running-config nac-policy** 命令显示安全设备中已存在的每个 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。思科访问控制服务器必须位于网络上才能为 ASA 提供 NAC 框架服务。 如果指定此类型，提示将表明您处于 config--nac-policy-nac-framework 配置模式下。此模式可让您配置 NAC 框架策略。

默认值

此命令没有默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.1(2)	此命令已弃用。

使用指南

对要分配到组策略的每个 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 Cisco AnyConnect VPN 隧道后，ASA 会应用与正在使用的组策略关联的 NAC 策略。

如果 NAC 策略已分配到一个或多个组策略，则无法使用 **no nac-policy** *name* 命令将其删除。

示例

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)
```

相关命令

命令	说明
show running-config nac-policy	显示 ASA 中每个 NAC 策略的配置。
show nac-policy	显示 ASA 中的 NAC 策略使用统计信息。
clear nac-policy	重置 NAC 策略使用统计信息。
nac-settings	将 NAC 策略分配到组策略。
clear configure nac-policy	从正在运行的配置中删除所有 NAC 策略，但分配到组策略的那些策略除外。

nac-settings

要将 NAC 策略分配到组策略，请在组策略配置模式下使用 **nac-settings** 命令，如下所示：

nac-settings {**value** *nac-policy-name* | **none**}

[**no**] **nac-settings** {**value** *nac-policy-name* | **none**}

语法说明

nac-policy-name	要分配到组策略的 NAC 策略。您命名的 NAC 策略必须位于 ASA 的配置中。**show running-config nac-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* 并禁止对此组策略使用 NAC 策略。组策略不会继承默认组策略的 nac-settings 值。
value	将要命名的 NAC 策略分配到组策略。

默认值

此命令没有任何参数或关键字。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
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，然后使用此命令将其分配到组策略。

show running-config nac-policy 命令显示每个 NAC 策略的名称和配置。

当您将 NAC 策略分配到组策略后， ASA 自动为该组策略启用 NAC。

示例

以下命令从组策略中删除 *nac-policy-name*。组策略会继承默认组策略的 *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* 并禁止对此组策略使用 NAC 策略。组策略不会继承默认组策略的 nac-settings 值。

```
ciscoasa(config-group-policy)# nac-settings none
ciscoasa(config-group-policy)
```

相关命令

命令	说明
nac-policy	创建并访问思科 NAC 策略，然后指定其类型。
show running-config nac-policy	显示 ASA 中每个 NAC 策略的配置。
show nac-policy	显示 ASA 中的 NAC 策略使用统计信息。
show vpn-session_summary.db	显示数字 IPsec、 WebVPN 和 NAC 会话。
show vpn-session.db	显示关于 VPN 会话的信息，包括 NAC 结果。

name

要将名称与 IP 地址关联，请在全局配置模式下使用 **name** 命令。要禁止使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_address name* [**description** *text*]]

no name *ip_address* [*name* [**description** *text*]]

语法说明

description	（可选）指定 IP 地址名称的说明。
ip_address	指定所命名主机的 IP 地址。
name	指定分配给该 IP 地址的名称。使用字符 a 至 z、A 至 Z、0 至 9、破折号和下划线。*name* 不得超过 63 个字符。此外， *name* 不能以数字开头。
text	指定说明的文本。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.0(4)	此命令得到增强以包括可选说明。
8.3(1)	在 **nat** 命令或 **access-list** 命令中不再允许使用命名的 IP 地址；您必须使用 **object network** 名称代替。尽管对象组中的 **network-object** 命令接受 **object network** 名称，但您仍可使用通过 **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。只能将一个名称与一个 IP 地址关联。

必须首先使用 **names** 命令，然后使用 **name** 命令。使用 **names** 命令后立即使用 **name** 命令，然后使用 **write memory** 命令。

name 命令可让您通过文本名称标识主机并将文本字符串映射到 IP 地址。 **no name** 命令可以禁止使用文本名称，但不会将其从配置中删除。使用 **clear configure name** 命令可从配置中清除名称列表。

要禁止显示 **name** 值，请使用 **no names** 命令。

name 和 **names** 命令均保存在配置中。

name 命令不支持将名称分配给网络掩码。例如，以下命令将被拒绝：

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```

注　需要掩码的任何命令都不能将名称处理为接受的网络掩码。

示例

本例显示允许您使用 **name** 命令的 **names** 命令。 **name** 命令取代 **sa_inside** 引用 192.168.42.3，取代 **sa_outside** 引用 209.165.201.3。将 IP 地址分配给网络接口后，您可以将这些名称与 **ip address** 命令一起使用。**no names** 命令禁止显示 **name** 命令值。以后再次使用 **names** 命令将恢复 **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
```

相关命令

命令	说明
clear configure name	从配置中清除名称列表。
names	启用名称与 IP 地址的关联。
show running-config name	显示与 IP 地址关联的名称。

name （动态过滤器黑名单或白名单）

要将域名添加到僵尸网络流量过滤器黑名单或白名单，请在动态过滤器黑名单或白名单配置模式下使用 **name** 命令。要删除该名称，请使用此命令的 **no** 形式。静态数据库可让您使用要加入白名单或黑名单的域名或 IP 地址扩充动态数据库。

name *domain_name*

no name *domain_name*

语法说明

domain_name	将名称添加到黑名单。您可以多次输入此命令以添加多个条目。最多可以添加 1000 个黑名单条目。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

进入动态过滤器白名单或黑名单配置模式后，您可以使用 **address** 和 **name** 命令，手动输入要在白名单中标记为好名称或在黑名单中标记为坏名称的域名或 IP 地址 （主机或子网）。

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

将域名添加到静态数据库后，ASA 会等待 1 分钟，然后发送该域名的 DNS 请求并将域名 /IP 地址配对添加到 *DNS 主机缓存*。（此操作是后台进程，不会影响继续配置 ASA 的能力。）

如果您没有为 ASA 配置的域名服务器，或其不可用，则您可以改为启用具有僵尸网络流量过滤器监听的 DNS 数据包检查 （请参阅 **inspect dns dynamic-filter-snooping** 命令）。使用 DNS 监听时，如果受感染的主机发送一条 DNS 请求来获取静态数据库中的某一名称，则 ASA 会查看 DNS 数据包内有无该域名和关联的 IP 地址，然后将名称和 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 **inspect dns dynamic-filter-snooping** 命令。

DNS 主机缓存中的条目具有 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，该值将截短为 1 天 （最大值）。

对 DNS 主机缓存，条目超时后， ASA 会定期请求刷新该条目。

示例

以下示例创建黑名单和白名单的条目：

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

相关命令

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

nameif

要提供接口的名称，请在接口配置模式下使用 **nameif** 命令。要删除该名称，请使用此命令的 **no** 形式。 ASA 的所有配置命令中均使用接口名称而不是接口类型和 ID （例如 gigabitethernet0/1），因此需要提供该名称，流量才能通过接口。

nameif *name*

no nameif

语法说明

name	设置长度最多为 48 个字符的名称。该名称不区分大小写。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令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，必须使用 **vlan** 命令分配 VLAN，然后输入 **nameif** 命令。

您可以通过重新输入此命令的新值来更改该名称。请勿输入 **no** 形式，因为该命令会导致删除引用该名称的所有命令。

示例

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
```

相关命令

命令	说明
clear xlate	重置现有连接的所有转换，从而导致重置这些连接。
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。只能将一个名称与一个 IP 地址关联。要禁止显示 **name** 值，请使用 **no names** 命令。

names

no names

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要启用名称与 IP 地址的关联，请使用 **names** 命令。只能将一个名称与一个 IP 地址关联。

必须首先使用 **names** 命令，然后使用 **name** 命令。使用 **names** 命令后立即使用 **name** 命令，然后使用 **write memory** 命令。

要禁止显示 **name** 值，请使用 **no names** 命令。

name 和 **names** 命令均保存在配置中。

示例

本例显示允许您使用 **name** 命令的 **names** 命令。 **name** 命令取代 **sa_inside** 引用 192.168.42.3，取代 **sa_outside** 引用 209.165.201.3。将 IP 地址分配给网络接口后，您可以将这些名称与 **ip address** 命令一起使用。**no names** 命令禁止显示 **name** 命令值。以后再次使用 **names** 命令将恢复 **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
```

相关命令

命令	说明
clear configure name	从配置中清除名称列表。
name	将名称与 IP 地址关联。
show running-config name	显示与 IP 地址关联的名称列表。
show running-config names	显示 IP 地址到名称的转换。

name-separator

要指定一个字符作为电邮与 VPN 用户名和密码之间的分隔符，请在适用的电邮代理模式下使用 **name-separator** 命令。要恢复为默认值 “:”，请使用此命令的 **no** 版本。

name-separator [*symbol*]

no name-separator

语法说明

symbol	（可选）电邮与 VPN 用户名和密码的分隔字符。选项包括 “@”(at)、“|”（管道）、“:”（冒号）、“#”（井号）、“,”（逗号）和 “;”（分号）。

默认值

默认值为 “:”（冒号）。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

名称分隔符必须与服务器分隔符不同。

示例

以下示例显示如何将井号 (#) 设置为 POP3S 的名称分隔符：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# name-separator #
```

相关命令

命令	说明
server-separator	分隔电邮和服务器名称。

name-server

要标识一台或多台 DNS 服务器，请在 dns 服务器组配置模式下使用 **name-server** 命令。要删除一台或多台服务器，请使用此命令的 **no** 形式。ASA 使用 DNS 解析 SSL VPN 配置或证书配置中的服务器名称（有关支持的命令列表，请参阅 “ 使用指南 ”）。定义服务器名称（例如 AAA）的其他功能不支持 DNS 解析。您必须通过使用 **name** 命令输入 IP 地址或将该名称手动解析为 IP 地址。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

语法说明

ip_address	指定 DNS 服务器 IP 地址。您可以通过单独的命令指定最多六个地址；或者为方便起见，在一条命令中指定最多六个地址（以空格分隔）。如果在一条命令中输入了多台服务器，则 ASA 会在配置中以各单独命令保存每台服务器。 ASA 将按顺序尝试每台 DNS 服务器，直至收到回应。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
dns 服务器组配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

要启用 DNS 查找，请在 dns 服务器组配置模式下使用 **domain-name** 命令。如果没有启用 DNS 查找，则不会使用 DNS 服务器。

支持 DNS 解析的 SSL VPN 命令包括以下各项：

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**
- **url-list**

支持 DNS 解析的证书命令包括以下各项：

- **enrollment url**
- **url**

您可以使用 **name** 命令手动输入名称和 IP 地址。

示例

以下示例将三台 DNS 服务器添加到组 “dnsgroup1”：

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA 以单独的命令保存配置，如下所示：

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

要添加两台额外的服务器，您可以将其作为一条命令输入：

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

要验证 dns 服务器组配置，请在全局配置模式下输入 **show running-config dns** 命令：

```
ciscoasa(config)# show running-config dns
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
name-server 10.5.1.1
name-server 10.8.3.8
...
```

或者，您可以将其作为两条单独的命令输入：

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.5.1.1
ciscoasa(config)# name-server 10.8.3.8
```

要删除多台服务器，您可以将其作为多条命令或作为一条命令输入，如下所示：

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

相关命令

命令	说明
domain-name	设置默认域名。
retries	指定当 ASA 没有收到回应时 DNS 服务器列表的重试次数。
timeout	指定在尝试下一 DNS 服务器之前等待的时间量。
show running-config dns server-group	显示一个或所有现有 dns 服务器组配置。

nat （全局）

要为 IPv4、 IPv6 或 IPv4 与 IPv6 之间 (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 **no** 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** {*real_src_mapped_dest_svc_obj* | **any**} *mapped_src_real_dest_svc_obj*] [**net-to-net**]
[**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**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** {*real_src_mapped_dest_svc_obj* | **any**} *mapped_src_real_dest_svc_obj*] [**net-to-net**]
[**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*]

对于动态 NAT：

nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}]
source dynamic {*real_obj* | **any**}
{[*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]]
[**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*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]]
[**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

no nat {*line* | **after-auto** *line*}

语法说明

(*real_ifc*,*mapped_ifc*)	（可选）指定真实接口和映射接口。如果没有指定真实接口和映射接口，则使用所有接口。您还可以指定关键字 **any** 用于一种或两种接口。在透明模式下，必须指定真实接口和映射接口；无法使用 **any**。 由于两次 NAT 可以同时转换源和目标地址，因此这些接口可以更好地理解为源和目标接口。
after-auto	将 NAT 表第 3 部分末尾的规则插入到网络对象 NAT 规则之后。默认情况下，两次 NAT 规则将添加到第 1 部分。您可以使用 *line* 参数将规则插入第 3 部分中的任意位置。
any	（可选）指定通配符值。 **any** 的主要用途包括： • 接口 - 您可以将 **any** 用于一种或两种接口（例如，**(any,outside)**）。如果没有指定接口，则 **any** 为默认值。 **any** 在透明模式下不可用。 • 静态 NAT 源的真实和映射 IP 地址 - 您可以指定 **source static any any** 以便为所有地址启用身份 NAT。 • 动态 NAT 或 PAT 源的真实地址 - 您可以通过指定 **source dynamic any** *mapped_obj* 转换源接口上的所有地址。 对于静态 NAT，尽管 **any** 也可用于真实源端口 / 映射目标端口，或者可用于源或目标真实地址（不使用 **any** 作为映射地址），但这些用途可能导致不可预测的行为。 **注**　“any” 流量（IPv4 与 IPv6）的定义取决于规则。在 ASA 对数据包执行 NAT 之前，该数据包必须为 IPv6 到 IPv6 或 IPv4 到 IPv4；通过这一前提条件，ASA 可以确定 NAT 规则中 **any** 的值。例如，如果配置从 “any” 到 IPv6 服务器的规则，并且该服务器从 IPv4 地址映射，则 **any** 是指 “ 任意 IPv6 流量 ”。如果配置从 “any” 到 “any” 的规则，并且将源映射到接口 IPv4 地址，则 **any** 是指 “ 任意 IPv4 流量 ”，因为映射接口地址暗示目标也为 IPv4。
description *desc*	（可选）提供最多 200 个字符的说明。
destination	（可选）配置目标地址的转换。尽管两次 NAT 的主要特征是包括目标 IP 地址，但目标地址是可选的。如果确实指定了目标地址，您可以配置该地址的静态转换或对其仅使用身份 NAT。您可能想要配置不带目标地址的两次 NAT 以利用两次 NAT 的一些其他特性，包括对真实地址使用网络对象组，或手动对规则进行排序。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 (**inspect dns**)（该功能在默认情况下已启用）。如果配置了 **destination** 地址，则无法配置 **dns** 关键字。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。通过在转换信息中包括目标地址和端口，扩展 PAT 对每项*服务*（而不是每个 IP 地址）使用 65535 个端口。通常，创建 PAT 转换时不考虑目标端口和地址，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）分配端口时允许使用 1024 到 65535 的整个端口范围。选择转换的映射端口号时， ASA 使用真实源端口号 （如果可用）。但是，如果不使用此选项，则真实端口 *不*可用时，映射端口默认情况下从与真实端口号相同的范围进行选择：即 1 到 511、512 到 1023 和 1024 到 65535。为避免耗尽低范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，还应指定 **include-reserve** 关键字。
inactive	（可选）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要使其重新激活，请重新输入完整命令但不带 **inactive** 关键字。
interface [**ipv6**]	（可选）使用接口 IP 地址作为映射地址。如果指定 **ipv6**，则使用接口的 IPv6 地址。 对于动态 NAT 源映射地址，如果您指定映射对象或组并后跟 **interface** 关键字，则仅当所有其他映射地址均已分配时使用该映射接口的 IP 地址。 对于动态 PAT，您可以指定 **interface** 单独用于源映射地址。 对于具有端口转换的静态 NAT （源或目标），请确保也配置了 **service** 关键字。 对于此选项，您必须配置 *mapped_ifc* 的特定接口。 此选项在透明模式下不可用。
line	（可选）在 NAT 表第 1 部分中的任意位置插入规则。默认情况下，NAT 规则添加到第 1 部分的末尾 （有关详细信息，请参阅 CLI 配置指南）。如果要将规则添加到第 3 部分 （网络对象 NAT 规则之后），则使用 **after-auto** *line* 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。
mapped_object	标识映射网络对象或对象组 （**object network** 或 **object-group network**）。 对于动态 NAT，通常配置为将较大的一组地址映射到较小的组。 **注**　映射的对象或组不能包含子网。 如果需要，您可以跨不同的动态 NAT 规则共享此映射 IP 地址。 您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。 对于动态 PAT，应配置为将一组地址映射到单一地址。您可以将真实地址转换为您所选择的单一映射地址，也可以将其转换为映射接口地址。如果要使用接口地址，请不要配置映射地址的网络对象；而应使用 **interface** 关键字。 对于静态 NAT，映射通常是一对一的，因此真实地址与映射地址的数量相同。不过，如果需要，您可以有不同的数量。有关详细信息，请参阅 CLI 配置指南。
mapped_src_real_dest_svc_obj	（可选）对于静态 NAT，指定映射源端口、真实目标端口或同时指定两者。有关详细信息，请参阅 **service** 关键字。
net-to-net	（可选）对于静态 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如果不使用此选项，则使用 IPv4 嵌入式方法。对于一对一转换，您必须使用此关键字。
no-proxy-arp	（可选）对于静态 NAT，禁用代理 ARP 以将数据包传入到映射 IP 地址。

pat-pool *mapped_obj*	（可选）启用地址的 PAT 池；该对象中的所有地址均用作 PAT 地址。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。
real_dest_svc_obj	（可选）对于动态 NAT/PAT，指定真实目标端口 （目标转换始终为静态）。有关详细信息，请参阅 **service** 关键字。
real_ifc	（可选）指定可能是数据包的源接口的名称。适用于源选项。对于源选项， origin_ifc 为真实接口。对于目标选项， real_ifc 为映射接口。
real_object	标识真实网络对象或对象组 （**object network** 或 **object-group network**）。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。
real_src_mapped_dest_svc_obj	（可选）对于静态 NAT，指定真实源端口、映射目标端口或同时指定两者。有关详细信息，请参阅 **service** 关键字。
round-robin	（可选）为 PAT 池启用轮询地址分配。默认情况下，将分配 PAT 地址的所有端口，然后使用下一个 PAT 地址。轮询方法分配池中每个 PAT 地址的地址 / 端口，然后返回再次使用第一个地址，再次使用第二个地址，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）确定传出接口。如果没有在 NAT 命令中指定接口，则默认情况下使用路由查找。
service	（可选）指定端口转换。 • 动态 NAT 和 PAT - 动态 NAT 和 PAT 不支持 （额外的）端口转换。不过，由于 *destination* 转换始终为静态，因此您可以执行目标端口的端口转换。服务对象 (**object service**) 可能同时包含源和目标端口，但在此情况下仅使用目标端口。如果指定了源端口，该端口将被忽略。 • 具有端口转换的静态 NAT - 应指定两个服务对象的源*或*目标端口。仅当您的应用使用固定源端口 （例如一些 DNS 服务器）时，才应*同时*指定源和目标端口；但固定源端口非常罕见。 对于源端口转换，对象必须指定源服务。在这种情况下，该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 **service** *mapped_port real_port*。在同时指定对象中的源和目标端口的极少数情况下，第一个服务对象包含真实源端口 / 映射目标端口；第二个服务对象包含映射源端口 / 真实目标端口。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，只需对真实和映射端口 （源和 / 或目标端口，具体取决于您的配置）使用相同的服务对象即可。不支持 “ 不等于 ”(**neq**) 运算符。 NAT 仅支持 TCP 或 UDP。转换端口时，请确保真实和映射服务对象中的协议完全相同 （均为 TCP 或均为 UDP）。
source	配置源地址的转换。
static	配置静态 NAT 或具有端口转换的静态 NAT。
unidirectional	（可选）对于静态 NAT，进行从源到目标的单向转换；目标地址无法启动到源地址的流量。此选项对于测试目的可能非常有用。

默认值

- 默认情况下，该规则添加到 NAT 表第 1 部分的末尾。
- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**，即将规则应用于所有接口。
- （8.3(1)、8.3(2) 和 8.4(1)）身份 NAT 的默认行为禁用代理 ARP。您无法配置此设置。（8.4(2) 和更高版本）身份 NAT 的默认行为启用了代理 ARP，从而匹配其他静态 NAT 规则。如果需要，您可以禁用代理 ARP。
- 如果指定可选接口，则 ASA 使用 NAT 配置确定传出接口。（8.3(1) 至 8.4(1)）唯一例外是身份 NAT，它始终使用路由查找，无论 NAT 配置如何。（适用于 8.4(2) 和更高版本）对于身份 NAT，默认行为是使用 NAT 配置，但您可以选择始终使用路由查找。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。
8.3(2)	从 8.3 以前版本的 NAT 免除配置迁移时，将对结果静态身份 NAT 规则添加关键字 **unidirectional**。
8.4(2)/8.5(1)	添加了 **no-proxy-arp**、**route-lookup**、**pat-pool** 和 **round-robin** 关键字。 身份 NAT 的默认行为更改为启用代理 ARP，从而匹配其他静态 NAT 规则。 对于 8.3 以前版本的配置，将 NAT 免除规则 （**nat 0 access-list** 命令）迁移到 8.4(2) 和更高版本现在包括以下关键字以禁用代理 ARP 和使用路由查找：**no-proxy-arp** 和 **route-lookup**。曾用于迁移到 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) 升级到 8.4(2) 时，所有身份 NAT 配置现在都包括 **no-proxy-arp** 和 **route-lookup** 关键字，用于保持现有的功能。 **unidirectional** 关键字已删除。
8.4(3)	添加了 **extended**、 **flat** 和 **include-reserve** 关键字。 使用具有轮询分配的 PAT 池时，如果主机有一个现有连接，则来自该主机的后续连接将使用相同的 PAT IP 地址 （如果端口可用）。 *此功能在 8.5(1) 中不可用。*
9.0(1)	NAT 现已支持 IPv6 流量，以及 IPv4 与 IPv6 之间的转换。透明模式下不支持 IPv4 与 IPv6 之间的转换。我们添加了 **interface ipv6** 选项和 **net-to-net** 选项。

使用指南

两次 NAT 可让您在一个规则中标识源和目标地址。例如，同时指定源和目标地址可让您指定如下规则 （仅为示例）：访问目标 X 时源地址应转换到 A，但访问目标 Y 时应转换到 B。

注　对于静态 NAT，该规则是双向的，因此请注意，在本指南范围内的命令和说明中使用了 “ 源 ” 和 “ 目标 ”，即使指定的连接可能源自 “ 目标 ” 地址。例如，如果您配置了具有端口转换的静态 NAT，指定源地址作为 Telnet 服务器，并且想要访问该 Telnet 服务器的所有流量将端口从 2323 转换为 23，则必须在命令中指定要进行转换的*源*端口 （真实：23，映射：2323）。您指定源端口是因为指定了 Telnet 服务器地址作为**源**地址。

目标地址是可选的。如果指定了目标地址，您可以将其映射到自身 （身份 NAT），也可以将其映射到不同的地址。目标映射始终为静态映射。

两次 NAT 还可让您将服务对象用于具有端口转换的静态 NAT ；网络对象 NAT 仅接受内嵌定义。

有关两次 NAT 与网络对象 NAT 之间区别的详细信息，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（如果已指定）第 3 部分。有关 NAT 排序的详细信息，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 IP 地址。如果为该规则指定 **any** 接口，则禁止所有接口 IP 地址。对于接口 PAT （仅限路由模式），请使用 **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。

前提条件

- 对于真实和映射这两种地址，配置网络对象或网络对象组 （**object network** 或 **object-group network** 命令）。对于创建具有不连续 IP 地址范围或者多个主机或子网的映射地址池，网络对象组特别有用。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。
- 对于具有端口转换的静态 NAT，请配置 TCP 或 UDP 服务对象 （**object service** 命令）。

NAT 中使用的对象和对象组不能未定义；它们必须包括 IP 地址。

清除转换会话

如果您更改了 NAT 配置，并且不想等到现有转换超时再使用新的 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，原因是每条 A 记录有多个适用的 PAT 规则，而要使用的 PAT 规则不明确。
- 如果可用，真实源端口号将用于映射端口。但是，如果真实端口*不*可用，则默认情况下从与真实端口号相同的范围选择映射端口：即 0 到 511、 512 到 1023 和 1024 到 65535。因此，低于 1024 的端口只有一个小型 PAT 池可供使用。（8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果有许多流量使用较低的端口范围，则您现在可以指定平面范围的端口代替三个大小不等的层：即 1024 到 65535 或 1 到 65535。
- （8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果您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，如果一个规则指定扩展 PAT 和平面范围，则另一个规则也必须指定扩展 PAT 和平面范围。

PAT 池的扩展 PAT 指南

- 许多应用检查不支持扩展 PAT。有关不支持的检查的完整列表，请参阅配置指南。
- 如果为动态 PAT 规则启用了扩展 PAT，则 PAT 池中的地址无法同时用作具有端口转换的单独静态 NAT 规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则不能使用 10.1.1.1 作为 PAT 地址来创建具有端口转换的静态 NAT 规则。
- 如果您使用 PAT 池并指定了用于回退的接口，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 依靠 PAT 绑定来实现对所有目标都相同。

PAT 池的轮询指南

- （8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果主机有一个现有连接，则来自该主机的后续连接将使用相同的 PAT IP 地址 （如果端口可用）。**注**：此 “ 粘性 ” 在故障切换后不再存在。如果 ASA 进行故障切换，则来自主机的后续连接可能未使用初始 IP 地址。
- （8.4(2)、 8.5(1) 和 8.6(1)）如果主机有一个现有连接，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，您在访问交换该主机信息的两个站点 （例如电子商务站点和支付站点）时可能出现问题。当这些站点发现两个不同的 IP 地址被视为单一主机时，交易可能会失败。

NAT 和 IPv6

您可以使用 NAT 实现 IPv6 网络之间的转换，以及 IPv4 和 IPv6 网络之间的转换 （仅限路由模式）。我们建议使用以下最佳实践：

- NAT66（IPv6 到 IPv6）- 建议使用静态 NAT。尽管您可以使用动态 NAT 或 PAT，但鉴于 IPv6 地址供应量巨大，因此您不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则 （仅限两次 NAT）。
- NAT46 （IPv4 到 IPv6） - 建议使用静态 NAT。由于 IPv6 地址空间比 IPv4 地址空间大得多，您可轻松支持静态转换。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限两次 NAT）。当转换到 IPv6 子网（/96 或更低）时，结果映射地址为 IPv4 嵌入式 IPv6 地址，其中 32 位的 IPv4 地址嵌入到 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附加到该地址的最后 32 位。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将映射到 201b::0.192.168.1.4 （用混合表示法显示）。如果前缀较小 （例如 /64），则 IPv4 地址附加到该前缀之后，并在该 IPv4 地址之后附加后缀 0s。
- NAT64 （IPv6 到 IPv4） - 您可能没有足够的 IPv4 地址容纳 IPv6 地址的数量。我们建议使用动态 PAT 池来提供大量的 IPv4 转换。

示例

以下示例包括一台主机，该主机位于 10.1.2.0/24 网络上并访问两台不同服务器。当主机访问位于 209.165.201.11 的服务器时，真实地址将转换为 209.165.202.129:*port*。当主机访问位于 209.165.200.225 的服务器时，真实地址将转换为 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
```

以下示例显示源和目标端口的使用。位于 10.1.2.0/24 网络上的主机访问一台主机以同时实现网络服务和 Telnet 服务。当主机访问服务器以实现 Telnet 服务时，真实地址将转换为 209.165.202.129:*port*。当主机访问同一服务器以实现网络服务时，真实地址将转换为 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
```

以下示例显示具有端口转换的静态接口 NAT 的使用。外部主机通过连接到外部接口 IP 地址 （目标端口 65000 至 65004 ）来访问内部 FTP 服务器。流量未转换到位于 192.168.10.100:6500 至 :65004 的内部 FTP 服务器。请注意，应在服务对象中指定源端口范围 （而不是目标端口），因为您要按照命令中的标识来转换源地址和端口；目标端口为 “any”。由于静态 NAT 是双向的，因此 “ 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及端口取决于哪台主机发送该数据包。在本例中，连接从外部向内部发起，因此 FTP 服务器的 “ 源 ” 地址和端口实际上是原始数据包中的目标地址和端口。

```
ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-obvject)# service tcp source range 65000 65004

ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-obvject)# 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
```

以下示例配置在访问 IPv4 209.165.201.1/27 网络上的服务器及 203.0.113.0/24 网络上的服务器时用于 IPv6 内部网络 2001:DB8:AAAA::/96 的动态 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
```

以下示例配置在访问外部 IPv6 Telnet 服务器 2001:DB8::23 时用于内部网络 192.168.1.0/24 的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任意服务器时使用 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
```

相关命令

命令	说明
clear configure nat	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	显示关于 NAT 池的信息。
show running-config nat	显示 NAT 配置。
show xlate	显示 NAT 会话 (xlate) 信息。

nat （对象）

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，请使用此命令的 **no** 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**]]] [**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**]]] [**interface** [**ipv6**]]} [**dns**]

对于静态 NAT 和具有端口转换的静态 NAT：

nat [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

no nat [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

语法说明

(*real_ifc*,*mapped_ifc*)	（可选）对于静态 NAT，指定真实和映射接口。如果没有指定真实接口和映射接口，则使用所有接口。您还可以指定关键字 **any** 用于一种或两种接口。确保您的命令中包含括号。在透明模式下，必须指定真实接口和映射接口；无法使用 **any**。
dns	（可选）转换 DNS 应答。确保 DNS 检查 (**inspect dns**) 已启用 （该功能在默认情况下已启用）。如果指定了 **service** 关键字 （用于静态 NAT），则此选项不可用。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。通过在转换信息中包括目标地址和端口，扩展 PAT 对每项*服务*（而不是每个 IP 地址）使用 65535 个端口。通常，创建 PAT 转换时不考虑目标端口和地址，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）分配端口时允许使用 1024 到 65535 的整个端口范围。选择转换的映射端口号时， ASA 使用真实源端口号 （如果可用）。但是，如果不使用此选项，则真实端口*不*可用时，映射端口默认情况下从与真实端口号相同的范围进行选择：即 1 到 511、512 到 1023 和 1024 到 65535。为避免耗尽低范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，还应指定 **include-reserve** 关键字。

interface [**ipv6**]	（可选）对于动态 NAT，如果您指定映射 IP 地址、对象或组并后跟 **interface** 关键字，则仅当所有其他映射地址均已分配时才会使用该映射接口的 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，则使用接口 IP 地址作为映射 IP 地址。当您要使用接口 IP 地址时必须使用此关键字；您不能将其内嵌或作为对象输入。 如果指定 **ipv6**，则使用接口的 IPv6 地址。 对于具有端口转换的静态 NAT，如果也配置了 **service** 关键字，您可以指定 **interface** 关键字。 对于此选项，您必须配置 *mapped_ifc* 的特定接口。 您无法在透明模式下指定 **interface**。
mapped_inline_host_ip	指定映射地址作为内嵌值。如果您指定 **dynamic**，则使用主机 IP 地址配置动态 PAT。
mapped_inline_ip	对于静态 NAT，指定映射 IP 地址作为内嵌值。映射网络的网络掩码或范围与真实网络相同。例如，如果真实网络为主机，则该地址将为主机地址。如果是一个范围，则映射地址包括与真实范围相同的地址数量。例如，如果真实地址定义为从 10.1.1.1 至 10.1.1.6 的范围，并且您指定 172.20.1.1 作为映射地址，则映射范围将包括 172.20.1.1 至 172.20.1.6。
mapped_obj	指定映射 IP 地址作为网络对象 (**object network**) 或对象组 (**object-group network**)。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。 对于动态 NAT，对象或组不能包含子网。如果需要，您可以跨不同的动态 NAT 规则共享此映射对象。有关禁止的映射 IP 地址的信息，请参阅第 13-32 页上的 “ 映射地址指南 ” 一节。 对于静态 NAT，通常可配置与真实地址相同数量的映射地址以实现一对一映射。但是，地址数量可以不一致。有关详细信息，请参阅 CLI 配置指南。
mapped_port	（可选）指定映射的 TCP 或 UDP 端口。您可以通过文字名称或 0 到 65535 范围内的数字指定端口。
net-to-net	（可选）对于 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如果不使用此选项，则使用 IPv4 嵌入式方法。对于一对一转换，您必须使用此关键字。
no-proxy-arp	（可选）对于静态 NAT，禁用代理 ARP 以将数据包传入到映射 IP 地址。
pat-pool *mapped_obj*	（可选）启用地址的 PAT 池；该对象中的所有地址均用作 PAT 地址。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。
real_port	（可选）对于静态 NAT，指定真实 TCP 或 UDP 端口。您可以通过文字名称或 0 到 65535 范围内的数字指定端口。
round-robin	（可选）为 PAT 池启用轮询地址分配。默认情况下，将分配 PAT 地址的所有端口，然后使用下一个 PAT 地址。轮询方法分配池中每个 PAT 地址的地址 / 端口，然后返回再次使用第一个地址，再次使用第二个地址，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）确定传出接口。如果没有在 NAT 命令中指定接口，则默认情况下使用路由查找。

service {tcp | udp}	（可选）对于具有端口转换的静态 NAT，指定端口转换的协议。仅支持 TCP 和 UDP。
static	配置静态 NAT 或具有端口转换的静态 NAT。

默认值

- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**，即将规则应用于所有接口。
- （8.3(1)、8.3(2) 和 8.4(1)）身份 NAT 的默认行为禁用代理 ARP。您无法配置此设置。（8.4(2) 和更高版本）身份 NAT 的默认行为为启用了代理 ARP，从而匹配其他静态 NAT 规则。如果需要，您可以禁用代理 ARP。
- 如果指定可选接口，则 ASA 使用 NAT 配置确定传出接口。（8.3(1) 至 8.4(1)）唯一例外是身份 NAT，它始终使用路由查找，无论 NAT 配置如何。（适用于 8.4(2) 和更高版本）对于身份 NAT，默认行为是使用 NAT 配置，但您可以选择始终使用路由查找。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。
8.4(2)/8.5(1)	添加了 **no-proxy-arp**、**route-lookup**、**pat-pool** 和 **round-robin** 关键字。 身份 NAT 的默认行为更改为启用代理 ARP，从而匹配其他静态 NAT 规则。 从 8.3(1)、8.3(2) 和 8.4(1) 升级到 8.4(2) 时，所有身份 NAT 配置现在都包括 **no-proxy-arp** 和 **route-lookup** 关键字，用于保持现有的功能。
8.4(3)	添加了 **extended**、 **flat** 和 **include-reserve** 关键字。 使用具有轮询分配的 PAT 池时，如果主机有一个现有连接，则来自该主机的后续连接将使用相同的 PAT IP 地址 （如果端口可用）。 *此功能在 8.5(1) 中不可用。*
9.0(1)	NAT 现已支持 IPv6 流量，以及 IPv4 与 IPv6 之间的转换。透明模式下不支持 IPv4 与 IPv6 之间的转换。我们添加了 **interface ipv6** 选项和 **net-to-net** 选项。

使用指南

数据包进入 ASA 时，将根据网络对象 NAT 规则检查源和目标 IP 地址。如果进行单独的匹配，则数据包中的源和目标地址可以通过单独的规则进行转换。这些规则并非彼此绑定；根据流量可以使用不同的规则组合。

由于规则从未配对，因此您无法指定访问目标 X 时源地址应转换到 A，但访问目标 Y 时应转换到 B。实现该种功能需要使用两次 NAT （两次 NAT 可让您在一个规则中标识源和目标地址）。

有关两次 NAT 与网络对象 NAT 之间区别的详细信息，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 排序的详细信息，请参阅 CLI 配置指南。

根据配置的不同，您可以将映射地址配置为内嵌式 （如果需要），也可以为映射地址创建一个网络对象或网络对象组 （**object network** 或 **object-group network** 命令）。对于创建具有不连续 IP 地址范围或者多个主机或子网的映射地址池，网络对象组特别有用。您不能使用同时具有 IPv4 和 IPv6 地址的对象组；对象组只能包含一种类型的地址。

NAT 中使用的对象和对象组不能未定义；它们必须包括 IP 地址。

您只能为指定的对象定义一个 NAT 规则；如果要配置多个 NAT 规则，您需要创建指定相同 IP 地址的多个对象，例如 **object network obj-10.10.10.1-01**、 **object network obj-10.10.10.1-02**，以此类推。

映射地址指南

映射 IP 地址池不能包括：

- 映射接口 IP 地址。如果为该规则指定 **any** 接口，则禁止所有接口 IP 地址。对于接口 PAT （仅限路由模式），请使用 **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。

清除转换会话

如果您更改了 NAT 配置，并且不想等到现有转换超时再使用新的 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，原因是每条 A 记录有多个适用的 PAT 规则，而要使用的 PAT 规则不明确。
- 如果可用，真实源端口号将用于映射端口。但是，如果真实端口*不*可用，则默认情况下从与真实端口号相同的范围选择映射端口：即 0 到 511、 512 到 1023 和 1024 到 65535。因此，低于 1024 的端口只有一个小型 PAT 池可供使用。（8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果有许多流量使用较低的端口范围，则您现在可以指定平面范围的端口代替三个大小不等的层：即 1024 到 65535 或 1 到 65535。
- （8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果您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，如果一个规则指定扩展 PAT 和平面范围，则另一个规则也必须指定扩展 PAT 和平面范围。

PAT 池的扩展 PAT 指南

- 许多应用检查不支持扩展 PAT。有关不支持的检查的完整列表，请参阅配置指南。
- 如果为动态 PAT 规则启用了扩展 PAT，则 PAT 池中的地址无法同时用作具有端口转换的单独静态 NAT 规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则不能使用 10.1.1.1 作为 PAT 地址来创建具有端口转换的静态 NAT 规则。
- 如果您使用 PAT 池并指定了用于回退的接口，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 依靠 PAT 绑定来实现对所有目标都相同。

PAT 池的轮询指南

- （8.4(3) 和更高版本，不包括 8.5(1) 或 8.6(1)）如果主机有一个现有连接，则来自该主机的后续连接将使用相同的 PAT IP 地址 （如果端口可用）。**注**：此 “ 粘性 ” 在故障切换后不再存在。如果 ASA 进行故障切换，则来自主机的后续连接可能未使用初始 IP 地址。
- （8.4(2)、 8.5(1) 和 8.6(1)）如果主机有一个现有连接，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，您在访问交换该主机信息的两个站点 （例如电子商务站点和支付站点）时可能出现问题。当这些站点发现两个不同的 IP 地址被视为单一主机时，交易可能会失败。
- 轮询 （尤其是与扩展 PAT 组合时）可能消耗大量内存。

NAT 和 IPv6

您可以使用 NAT 实现 IPv6 网络之间的转换，以及 IPv4 和 IPv6 网络之间的转换 （仅限路由模式）。我们建议使用以下最佳实践：

- NAT66（IPv6 到 IPv6）- 建议使用静态 NAT。尽管您可以使用动态 NAT 或 PAT，但鉴于 IPv6 地址供应量巨大，因此您不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则 （仅限两次 NAT）。
- NAT46 （IPv4 到 IPv6） - 建议使用静态 NAT。由于 IPv6 地址空间比 IPv4 地址空间大得多，您可轻松支持静态转换。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限两次 NAT）。当转换到 IPv6 子网（/96 或更低）时，结果映射地址为 IPv4 嵌入式 IPv6 地址，其中 32 位的 IPv4 地址嵌入到 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附加到该地址的最后 32 位。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将映射到 201b::0.192.168.1.4 （用混合表示法显示）。如果前缀较小 （例如 /64），则 IPv4 地址附加到该前缀之后，并在该 IPv4 地址之后附加后缀 0s。
- NAT64 （IPv6 到 IPv4） - 您可能没有足够的 IPv4 地址容纳 IPv6 地址的数量。我们建议使用动态 PAT 池来提供大量的 IPv4 转换。

示例

动态 NAT 示例

以下示例配置动态 NAT，该动态 NAT 将 192.168.2.0 网络隐藏到外部地址范围 2.2.2.1-2.2.2.10 后面：

```
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
```

以下示例配置动态 NAT 及动态 PAT 备用。位于内部网络 10.76.11.0 上的主机首先映射到 nat-range1 池 (10.10.10.10-10.10.10.20)。 nat-range1 池中的所有地址均已分配后，使用 pat-ip1 地址 (10.10.10.21) 执行动态 PAT。在极少数情况下， PAT 转换亦会用尽，此时，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
```

以下示例配置动态 NAT 及动态 PAT 备用以将 IPv6 主机转换为 IPv4。位于内部网络 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）。IPv4_NAT_RANGE 池中的所有地址均已分配后，使用 IPv4_PAT 地址 (209.165.201.31) 执行动态 PAT。如果 PAT 转换亦已用尽，则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

以下示例配置将 192.168.2.0 网络隐藏到地址 2.2.2.2 后面的动态 PAT：

```
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
```

以下示例配置将 192.168.2.0 网络隐藏到外部接口地址后面的动态 PAT：

```
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 及 PAT 池以将内部 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，在启用 DNS 重写的情况下将内部真实主机 1.1.1.1 转换到外部的 2.2.2.2。

```
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
```

以下示例配置静态 NAT，使用映射对象将内部真实主机 1.1.1.1 转换到外部的 2.2.2.2。

```
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
```

以下示例配置具有端口转换的静态 NAT，将位于 TCP 端口 21 的 1.1.1.1 转换到位于端口 2121 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

以下示例使用内嵌式映射地址将主机地址映射到自身：

```
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自身：

```
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
```

相关命令

命令	说明
clear configure nat	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	显示关于 NAT 池的信息。
show running-config nat	显示 NAT 配置。
show xlate	显示 xlate 信息。

nat （vpn 负载平衡）

要设置 NAT 将此设备 IP 地址转换到的 IP 地址，请在 VPN 负载平衡配置模式下使用 **nat** 命令。要禁用此 NAT 转换，请使用此命令的 **no** 形式。

nat *ip-address*

no nat [*ip-adddress*]

语法说明

ip-address	您想要此 NAT 将此设备 IP 地址转换到的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡模式。

在该命令的 **no nat** 形式中，如果您指定了可选的 *ip-address* 值，则该 IP 地址必须匹配正在运行的配置中现有的 NAT IP 地址。

示例

以下是 VPN 负载平衡命令序列的示例，其中包括将 NAT 转换地址设置为 192.168.10.10 的 **nat** 命令：

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

相关命令

命令	说明
vpn load-balancing	进入 VPN 负载平衡模式。

nat-assigned-to-public-ip

要将 VPN 对等设备的本地 IP 地址转换回对等设备的真实 IP 地址，请在隧道组常规属性配置模式下使用 **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*

语法说明

interface	指定要应用 NAT 的接口。

命令默认

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(3)	我们引入了此命令。

使用指南

在极少数情况下，您可能想要使用内部网络上 VPN 对等设备的真实 IP 地址而不是分配的本地 IP 地址。通常在使用 VPN 时，对等设备将被分配一个本地 IP 地址用于访问内部网络。但是，您可能要将该本地 IP 地址转换回对等设备的真实公共 IP 地址；例如，当您的内部服务器和网络安全基于对等设备的真实 IP 地址时。

您可以在每个隧道组的一个接口上启用此功能。当 VPN 会话建立或断开连接时，将动态添加和删除对象 NAT 规则。您可以使用 **show nat** 命令查看这些规则。

数据流

以下步骤介绍启用此功能时流过 ASA 的数据包：

1. VPN 对等设备将一个数据包发送到 ASA。

   外部源 / 目标包含对等设备公共 IP 地址 /ASA IP 地址。加密的内部源 / 目标包含 VPN 分配的 IP 地址 / 内部服务器地址。

2. ASA 将解密该数据包 （删除外部源 / 目标）。
3. ASA 对内部服务器执行路由查找，然后将该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 地址转换为对等设备公共 IP 地址。
5. ASA 将转换的数据包发送到服务器。
6. 服务器将回应该数据包，然后将其发送到对等设备的公共 IP 地址。

7. ASA 接收回应，然后取消目标 IP 地址到 VPN 分配 IP 地址的转换。
8. ASA 将未转换的数据包转发到其加密的外部接口，然后添加包含 ASA IP 地址 / 对等设备公共 IP 地址的外部源 / 目标。
9. ASA 将数据包发送到对等设备。
10. 对等设备将解密并处理数据。

限制

由于路由问题，除非您知道您需要此功能，否则我们不建议使用此功能；请联系思科 TAC 确认您的网络的功能兼容性。请了解以下限制：

- 仅支持 Cisco IPsec 和 AnyConnect 客户端。
- 返回到公共 IP 地址的流量必须路由回 ASA，以便能够应用 NAT 策略和 VPN 策略。
- 如果启用反向路由注入 （请参阅 **set reverse-route** 命令），则只通告 VPN 分配的 IP 地址。
- 不支持负载平衡 （由于路由问题）。
- 不支持漫游 （公共 IP 更改）。

示例

以下示例为 “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** 命令的示例输出，显示来自具有分配 IP 10.1.226.174 的对等设备 209.165.201.10 的自动 NAT 规则：

```
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
```

相关命令

命令	说明
show nat	显示当前 xlate。
tunnel-group general-attributes	设置隧道组的常规属性。
debug menu webvpn 99	对于 AnyConnect SSL 会话， VPN NAT 接口存储在会话中。
debug menu ike 2 *peer_ip*	对于 Cisco IPsec 客户端会话， VPN NAT 接口存储在 SA 中。
debug nat 3	显示 NAT 的调试消息。

nat-rewrite

要对 DNS 响应 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，请使用此命令的 **no** 形式。

nat-rewrite

no nat-rewrite

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， NAT 重写已启用。配置 **inspect dns** 后（即使 **policy-map type inspect dns** 未定义）即可启用此功能。要禁用此功能，必须在策略映射配置中显式声明 **no nat-rewrite**。如果没有配置 **inspect dns**，则不会执行 NAT 重写。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此功能执行 DNS 响应中 A 类资源记录 (RR) 的 NAT 转换。

示例

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
```

相关命令

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

nbns-server （隧道组 webvpn 属性模式）

要配置 NBNS 服务器，请在隧道组 webvpn 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 才能在远程系统上访问或共享文件。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

语法说明

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	表示后跟重试值。
retries	指定 NBNS 服务器查询重试次数。 ASA 循环遍历服务器列表，具体次数即您在此处指定的值，然后发送错误消息。默认值为 2 ；范围为 1 到 10。
timeout	表示后跟超时值。
timeout	指定将查询再次发送到同一服务器 （如果只有一台服务器）或其他服务器 （如果有多台 NBNS 服务器）之前 ASA 等待的时间量。默认值为 2 秒；范围为 1 到 30 秒。

默认值

默认情况下没有配置任何 NBNS 服务器。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	已从 webvpn 模式转至隧道组 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，它将在隧道组 webvpn 属性配置模式下转变为相同的命令。

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** 选项可从配置中删除匹配的条目。

示例

以下示例显示如何配置隧道组 “test”，其 NBNS 服务器是 IP 地址为 10.10.10.19、超时值为 10 秒并且可重试 8 次的主浏览器。该示例还显示如何配置 IP 地址为 10.10.10.24、超时值为 15 并且可重试 8 次的 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)#
```

相关命令

命令	说明
clear configure group-policy	删除特定组策略或所有组策略的配置。
show running-config group-policy	显示特定组策略或所有组策略正在运行的配置。
tunnel-group webvpn-attributes	指定命名隧道组的 WebVPN 属性。

nbns-server （webvpn 模式）

要配置 NBNS 服务器，请在隧道组 webvpn 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 才能在远程系统上访问或共享文件。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

语法说明

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	表示后跟重试值。
retries	指定 NBNS 服务器查询重试次数。 ASA 循环遍历服务器列表，具体次数即您在此处指定的值，然后发送错误消息。默认值为 2 ；范围为 1 到 10。
timeout	表示后跟超时值。
timeout	指定将查询再次发送到同一服务器 （如果只有一台服务器）或其他服务器（如果有多台 NBNS 服务器）之前 ASA 等待的时间量。默认值为 2 秒；范围为 1 到 30 秒。

默认值

默认情况下没有配置任何 NBNS 服务器。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	已从 webvpn 模式转至隧道组 webvpn 配置模式。

使用指南

此命令在 webvpn 配置模式下已弃用。隧道组 webvpn 属性配置模式下的 nbns-server 命令将取代该命令。在版本 7.1(1) 中，如果您在 webvpn 配置模式下输入此命令，它将在隧道组 webvpn 属性模式下转变为相同的命令。

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** 选项可从配置中删除匹配的条目。

示例

以下示例显示如何配置 NBNS 服务器，该服务器是 IP 地址为 10.10.10.19、超时值为 10 秒并且可重试 8 次的主浏览器。该示例还显示如何配置 IP 地址为 10.10.10.24、超时值为 15 并且可重试 8 次的 NBNS WINS 服务器。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

要定义点对点非广播网络上的静态邻居，请在路由器配置模式下使用 **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_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

语法说明

interface *name*	（可选）指定接口名称 （与通过 **nameif** 命令指定一样），通过该名称可访问邻居。
ip_address	指定邻居路由器的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

neighbor 命令用于通告 VPN 隧道上的 OSPF 路由。必须为每个已知的非广播网络邻居包括一个邻居条目。邻居地址必须位于接口的主要地址上。

若邻居与任何直连系统接口都没有位于同一网络，需要指定 **interface** 选项。此外，必须创建静态路由以访问邻居。

示例

以下示例定义了地址为 192.168.1.1 的邻居路由器：

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	显示全局路由器配置中的命令。

neighbor (EIGRP)

要定义与之交换信息的 EIGRP 邻居路由器，请在路由器配置模式下使用 **neighbor** 命令。要删除邻居条目，请使用此命令的 **no** 形式。

neighbor *ip_address* **interface** *name*

no neighbor *ip_address* **interface** *name*

语法说明

interface *name*	接口名称 （由 **nameif** 命令指定），通过该名称可访问邻居。
ip_address	邻居路由器的 IP 地址。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

可以使用多条 neighbor 语句与特定 EIGRP 邻居建立对等会话。 EIGRP 用来交换路由更新的接口必须在 neighbor 语句中指定。两个 EIGRP 邻居用来交换路由更新的接口必须配置为具有来自同一网络的 IP 地址。

注　为接口配置 **passive-interface** 命令可抑制该接口上的所有传入和传出路由更新以及问候消息。EIGRP 相邻关系无法在配置为被动的接口上建立或维持。

EIGRP 问候消息作为单播消息发送到使用 **neighbor** 命令定义的邻居。

示例

以下示例配置具有 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
```

相关命令

命令	说明
debug eigrp neighbors	显示 EIGRP 邻居消息的调试信息。
show eigrp neighbors	显示 EIGRP 邻居表。

neighbor activate

要允许与边界网关协议 (BGP) 邻居交换信息，请在地址系列配置模式下使用 **neighbor activate** 命令。要禁止与 BGP 邻居交换地址，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **activate**

no neighbor{*ip_address*} **activate**

语法说明

ip_address	BGP 路由器的 IP 地址。

默认值

对于 IPv4 地址系列，默认情况下已启用与 BGP 邻居进行地址交换。您无法为任何其他地址系列启用地址交换。

注 对于通过 **neighbor remote-as** 命令定义的每个 BGP 路由会话，默认情况下已启用 IPv4 地址系列的地址交换；除非您在配置 **neighbor remote-as** 命令之前配置 **no bgp default ipv4-activate** 命令，或者通过使用 **no neighbor activate** 命令禁止与特定邻居进行地址交换。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

您可以使用此命令以 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)。

示例

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 对等设备组中的所有邻居及 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
```

相关命令

命令	说明
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。

neighbor advertise-map

要通告匹配所配置路由映射的 BGP 表中的路由，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 {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}[**check-all-paths**]

no neighbor {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}[**check-all-paths**]

语法说明

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*	指定满足存在映射或不存在映射条件时将通告的路由映射名称。
exist-map *map-name*	指定与 BGP 表中的路由进行比较的存在映射名称，以确定通告映射路由是否已通告。
non-exist-map *map-name*	指定与 BGP 表中的路由进行比较的非存在映射名称，以确定通告映射路由是否已通告。
check-all-paths	（可选）通过具有 BGP 表中前缀的存在映射启用对所有路径的检查。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

使用 neighbor advertise-map 命令有条件地通告所选路由。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，则前缀在通告映射和存在映射中都存在时才满足条件。

如果配置了非存在映射，则前缀在通告映射中存在并且在非存在映射中不存在时才满足条件。

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。

示例

以下路由器配置示例将 BGP 配置为检查所有内容：

```
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配置 BGP 以使用非存在映射将前缀有条件地通告到 10.1.1.1 邻居。如果前缀存在于 MAP3 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
```

以下对等设备组配置示例将 BGP 配置为根据 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 route1 send-community both
ciscoasa(config-router-af)# neighbor route1 advertise-map MAP1 exist-map MAP2
check-all-paths
```

相关命令

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 路由更新之间的最短路由通告时间间隔 (MRAI)，请在地址系列配置模式下使用 **neighbor advertisement-interval** 命令。要恢复默认值，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **advertisement-interval** *seconds*

no neighbor {*ip_address*} **advertisement-interval** *seconds*

语法说明

ip_address	邻居路由器的 IP 地址。
seconds	发送 BGP 路由更新之间的最短时间间隔。 有效值介于 0 到 600 之间。

默认值

不在 VRF 中的 eBGP 会话：30 秒

VRF 中的 eBGP 会话：0 秒

iBGP 会话：0 秒。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

MRAI 等于 0 秒时，在 BGP 路由表发生变化后立即发送 BGP 路由更新。

示例

以下示例将发送 BGP 路由更新之间的最短时间设置为 10 秒：

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

相关命令

命令	说明
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
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 发送到邻居用作默认路由，请在地址系列配置模式下使用 **neighbor default-originate** 命令。如果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*} **default-originate** [**route-map** *route-map name*]

no neighbor {*ip_address*} **default-originate** [**route-map** *route-map name*]

语法说明

ip_address	邻居路由器的 IP 地址。
route-map *route-map name*	（可选）路由映射的名称。路由映射允许有条件地注入路由 0.0.0.0。

默认值

没有向邻居发送任何默认路由。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令不需要本地路由器中存在 0.0.0.0。与路由映射一起使用时，如果路由映射包含 **match ip address** 子句并且有与 IP 访问列表确切匹配的路由，则注入默认路由 0.0.0.0。路由映射还可包含其他匹配子句。

您可以将标准或扩展访问列表与 **neighbor default-originate** 命令一起使用。

示例

在以下示例中，本地路由器将路由 0.0.0.0 无条件注入到邻居 72.16.2.3：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
```

在以下示例中，本地路由器将路由 0.0.0.0 注入到邻居 2001::1：

```
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

相关命令

命令	说明
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor description

要将说明与邻居关联，请在地址系列配置模式下使用 **neighbor description** 命令。要删除说明，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **description** *text*

no neighbor {*ip_address*} **description** *text*

语法说明

ip_address	邻居路由器的 IP 地址。
text	描述邻居的文本 （长度最多为 80 个字符）。

默认值

没有邻居的说明。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

在以下示例中，邻居的说明是 “peer with example.com”：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

相关命令

命令	说明
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
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跃点对等设备建立 eBGP 对等会话，请在地址系列配置模式下使用 **neighbor disable-connected-check** 命令。要为 eBGP 对等会话启用连接验证，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **disable-connected-check**

no neighbor {*ip_address*} **disable-connected-check**

语法说明

ip_address	邻居路由器的 IP 地址。

默认值

BGP 路由过程将验证单跃点 eBGP 对等会话的连接 (TTL=254) 以确定 eBGP 对等设备在默认情况下是否直连到同一网段。如果对等设备没有直连到同一网段，连接验证将阻止建立对等会话。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

neighbor disable-connected-check 命令用于禁用 eBGP 对等会话的连接验证过程，这些会话可通过单跃点访问但在环回接口上配置，或者通过非直连 IP 地址配置。

仅当 **neighbor ebgp-multihop** 命令将 TTL 值配置为 1 时才需要此命令。单跃点 eBGP 对等设备的地址必须可访问。必须配置 **neighbor update-source** 命令以允许 BGP 路由过程为对等会话使用环回接口。

示例

在以下示例中，单跃点 eBGP 对等会话在两个 BGP 对等设备之间配置，通过每一路由器上的本地环回接口在同一网段上可访问这两个设备：

BGP 对等设备 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 对等设备 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
```

相关命令

命令	说明
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
neighbor ebgp-multihop	接受或发起与位于非直连网络上的外部对等设备的 BGP 连接。

neighbor distribute-list

要按照访问列表中指定的设置分发 BGP 邻居信息，请在地址系列配置模式下使用 **neighbor distribute-list** 命令。要删除条目，请使用此命令的 **no** 形式。

neighbor *ip_address* **distribute-list** {*access-list-name*} {**in** | **out**}

no neighbor *ip_address* **distribute-list** {*access-list-name*} {**in** | **out**}

语法说明

ip_address	邻居路由器的 IP 地址。
access-list-name	标准访问列表的名称。
in	访问列表应用于该邻居的传入通告
out	访问列表应用于该邻居的传出通告

默认值

没有指定 BGP 邻居。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用分发列表是过滤通告的多种方法之一。通告还可以使用以下方法进行过滤：

- 可以通过 **ip as-path access-list** 和 **neighbor filter-list** 命令配置自主系统路径过滤器。
- **access-list (IP standard)** 命令可用于配置标准访问列表以实现通告的过滤
- **route-map (IP)** 命令可用于过滤通告。路由映射可以通过自主系统过滤器、前缀过滤器、访问列表和分发列表进行配置。

标准访问列表可用于过滤路由更新。但是，如果在使用无类域间路由 (CIDR) 时进行路由过滤，则标准访问列表不会提供配置网络地址和掩码的高级过滤所需的粒度级别。

示例

在以下示例中，标准访问列表 distribute-list-acl 中的 BGP 邻居信息应用于邻居 `172.16.4.1` 的传入通告。

```
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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
network	指定要由 BGP 进行通告的网络。
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

要接受并尝试与位于非直连网络上的外部对等设备的 BGP 连接，请在地址系列配置模式下使用 **neighbor ebgp-multihop** 命令。要恢复默认值，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **ebgp-multihop [ttl]**

no neighbor{*ip_address*} **ebgp-multihop**

语法说明

ip_address	邻居路由器的 IP 地址。
ttl	（可选）存活时间。 有效值介于 1 到 255 个跃点之间。

默认值

只允许直连的邻居。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

应仅在思科技术支持人员的指导下使用此功能。为阻止通过不稳定的路由创建环路，如果到多跃点对等设备的唯一路由是默认路由 (0.0.0.0)，将不会建立多跃点。

示例

以下示例允许与位于非直连网络上的邻居 10.108.1.1 之间的往来连接：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

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。要禁用此功能，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **filter-list** *access-list-name* {**in** | **out**}

no neighbor {*ip_address*} **filter-list** *access*-list-name {**in** | **out**}

语法说明

ip_address	邻居路由器的 IP 地址。
access-list-name	自主系统路径访问列表的名称。您可使用 **as-path access-list** 命令定义此访问列表。
in	访问列表应用于传入路由。
out	访问列表应用于传出路由。

命令默认

不使用 BGP 过滤器。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令在入站和出站 BGP 路由上都建立过滤器。

注 请勿将 **neighbor distribute-list** 和 **neighbor prefix-list** 命令同时应用于任何指定方向（入站或出站）的邻居。这两条命令是互斥的，只有一条命令（**neighbor distribute-list** 或 **neighbor prefix-list**）能应用于每个入站或出站方向。

示例

在以下地址系列配置模式示例中，IP 地址为 172.16.1.1 的 BGP 邻居不会与相邻的自主系统 123 相互发送关于任何路径的通告：

```
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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
network	指定要通过 BGP 路由过程进行通告的网络。

neighbor ha-mode graceful-restart

要启用或禁用 BGP 邻居的边界网关协议 (BGP) 平滑重启功能，请在地址系列配置模式下使用 neighbor ha-mode graceful-restart 命令。要从配置中删除邻居的 BGP 平滑重启功能，请使用此命令的 no 形式。

neighbor *ip_address* **ha-mode graceful-restart** [**disable**]

no neighbor *ip_address* **ha-mode graceful-restart**

语法说明

ip_address	邻居的 IP 地址。
disable	（可选）禁用邻居的 BGP 平滑重启功能。

命令默认

BGP 平滑重启功能已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

neighbor ha-mode graceful-restart 命令用于启用或禁用单个 BGP 邻居的平滑重启功能。如果以前为 BGP 对等设备启用了平滑重启，则使用 disable 关键字可禁用平滑重启功能。

会话建立过程中，在 OPEN 消息中支持无中断转发 (NSF) 和 NSF 感知的对等设备之间协商平滑重启功能。如果在 BGP 会话建立后启用平滑重启功能，该会话需要通过软重置或硬重置重新启动。

支持 NSF 和 NSF 感知的 ASA 支持平滑重启功能。支持 NSF 的 ASA 可以执行状态切换 (SSO) 操作（平滑重启），并可通过在 SSO 操作过程中保留路由表信息来帮助重新启动对等设备。NSF 感知的 ASA 与支持 NSF 但无法执行 SSO 操作的路由器功能类似。

注　要为所有 BGP 邻居全局启用 BGP 平滑重启功能，请使用 **bgp graceful-restart** 命令。为单独的邻居配置 BGP 平滑重启功能后，配置平滑重启的每种方法具有相同的优先级，并且最后一个配置实例将应用于邻居。

使用 show bgp neighbors 命令可验证 BGP 邻居的 BGP 平滑重启配置。

示例

以下示例为 BGP 邻居 172.21.1.2 启用 BGP 平滑重启功能：

```
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
```

相关命令

命令	说明
bgp graceful-restart	为所有 BGP 邻居全局启用或禁用 BGP 平滑重启功能。
show bgp neighbors	显示关于与邻居的 TCP 和 BGP 连接的信息。

neighbor local-as

要定制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 **neighbor 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*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor {*ip_address*} **local-as**

语法说明

ip_address	邻居路由器的 IP 地址。
autonomous-system-number	（可选）预置到 AS_PATH 属性之前的自主系统编号。此参数值的范围为 1 到 65535 的任何有效自主系统编号。 **注**　您无法使用此参数指定来自本地 BGP 路由过程或来自远程对等设备网络的自主系统编号。 有关自主系统编号格式的更多详情，请参阅 **router bgp** 命令。
no-prepend	（可选）不将本地自主系统编号预置到从 eBGP 邻居接收的任何路由之前。
replace-as	（可选）将真实自主系统编号替换为 eBGP 更新中的本地自主系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。
dual-as	（可选）配置 eBGP 邻居以建立对等会话，方法是使用真实自主系统编号（来自本地 BGP 路由过程）或使用通过 *autonomous-system-number* 参数 (local-as) 配置的自主系统编号。

命令默认

默认情况下，来自本地 BGP 路由过程的自主系统编号将预置到所有外部路由之前。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

通过添加和删除从 eBGP 邻居接收的路由的自主系统编号， **neighbor local-as** 命令可用于定制 AS_PATH 属性。为了支持自主系统编号迁移，此命令的配置允许路由器作为其他自主系统的成员显示为外部对等设备。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 网络中更改自主系统编号的过程。

注意事项

BGP 预置路由穿越的每个 BGP 网络的自主系统编号，以维护网络可达性信息和防止路由环路。此命令应仅配置用于自主系统迁移，并且应在过渡完成后取消配置。此过程应仅由经验丰富的网络运营商尝试进行。配置不正确可能会产生路由环路。

此命令只能用于真正的 eBGP 对等会话。此命令不适用于联盟的不同子自主系统中的两个对等设备。

为确保顺利过渡，我们建议使用 4 字节自主系统编号标识自主系统内的所有 BGP 发言者升级为支持 4 字节自主系统编号。

示例

Local-AS 示例

以下示例使用 local-as 功能通过自主系统 300 建立路由器 1 与路由器 2 之间的对等：

路由器 1 （本地路由器）

```
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 300
```

路由器 2 （远程路由器）

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

No-prepend 关键字配置示例

以下示例将 BGP 配置为不将自主系统 500 预置到从 192.168.1.1 邻居接收的路由之前：

```
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
```

Replace-as 关键字配置示例

以下示例将专用自主系统 64512 从 172.20.1.1 邻居的带外路由更新中剥离，并将其替换为自主系统 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
```

Dual-as 关键字配置示例

以下示例显示两个提供商网络和一个客户网络的配置。路由器 1 属于自主系统 100，而路由器 2 属于自主系统 200。自主系统 200 将合并到自主系统 100。需要进行此过渡而不中断对自主系统 300 （客户网络）中路由器 3 的服务。 **neighbor local-as** 命令在路由器 1 中配置，以便路由器 3 在此过渡期间保持与自主系统 200 对等。过渡完成后，路由器 3 上的配置可以在正常维护时段或其他计划停机期间更新为与自主系统 100 对等。

路由器 1 配置 （本地提供商网络）

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
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
```

路由器 2 配置 （远程提供商网络）

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

路由器 3 配置 （远程客户网络）

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

要在两个自主系统合并后完成迁移，请在路由器 3 上更新对等会话：

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
bgp router-id	配置本地边界网关协议 (BGP) 路由过程的固定路由器 ID。
neighbor activate	启用与 BGP 邻居的信息交换。
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。
network	指定要通过 BGP 路由过程进行通告的网络。
synchronization	启用 BGP 与您的内部网关协议 (IGP) 系统之间的同步

neighbor maximum-prefix

要控制可从邻居接收多少个前缀，请在地址系列配置模式下使用 **neighbor maximum-prefix** 命令。要禁用此功能，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

no neighbor {*ip_address*} **maximum-prefix** *maximum*

语法说明

ip_address	邻居路由器的 IP 地址。
maximum	允许来自此邻居的最大前缀数量。
threshold	（可选）整数，用于指定路由器开始生成警告消息的*最大值*百分比。范围为 1 到 100；默认值为 75（百分比）。
restart	（可选）配置运行 BGP 的路由器，在由于超出最大前缀限制而禁用后自动重新建立对等会话。重新启动计时器使用 *restart-interval* 参数进行配置。
restart-interval	（可选）重新建立对等会话的时间间隔（以分钟为单位）。范围为 1 到 65535 分钟。
warning-only	（可选）允许路由器在超出*最大值*时生成日志消息，而不是终止对等。

命令默认

此命令默认禁用。前缀数量没有限制。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令可以配置允许 BGP 路由器从对等设备接收的最大前缀数量。它会添加其他机制（除了分发列表、过滤器列表和路由映射以外）以控制从对等设备接收的前缀数。

当接收的前缀数量超出配置的最大数量时，路由器会终止对等（默认情况下）。不过，如果配置了 **warning-only** 关键字，则路由器仅发送日志消息，但继续与发送方对等。如果对等设备终止，则对等设备保持关闭，直到发出 **clear bgp** 命令。

示例

以下示例将允许从位于 192.168.6.6 的邻居接收的最大前缀数量设置为 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
```

以下示例将允许从位于 2001::1 的邻居接收的最大前缀数量设置为 1000：

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
network	指定要通过 BGP 路由过程进行通告的网络。

neighbor next-hop-self

要将路由器配置为 BGP 发言邻居的下一个跃点，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*} **next-hop-self**

no neighbor {*ip_address*} **next-hop-self**

语法说明

ip_address	邻居路由器的 IP 地址。
warning-only	（可选）允许路由器在超出*最大值*时生成日志消息，而不是终止对等。

命令默认

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令在无网状结构的网络 （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。

示例

以下示例强制以 10.108.1.1 为目标的所有更新将此路由器作为下一个跃点进行通告：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。

neighbor password

要对两个 BGP 对等设备之间的 TCP 连接启用 message digest5 (MD5) 身份验证，请在地址系列配置模式下使用 **neighbor password** 命令。要禁用此功能，请使用此命令的 **no** 形式

neighbor {*ip_address*} **password** [**0-7**] *string*

no neighbor {*ip_address*} **password**

语法说明

ip_address	邻居路由器的 IP 地址。
string	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。该字符串可以包含任意字母数字字符，包括空格。您无法指定 *number-space-anything* 格式的密码。数字后的空格可导致身份验证失败。
0-7	（可选）加密类型。 0-6 为未加密。 7 用于加密。

命令默认

MD5 不对两个 BGP 对等设备之间的 TCP 连接进行身份验证。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

您可以在两个 BGP 对等设备之间配置 MD5 身份验证，这意味着对两个对等设备之间的 TCP 连接上发送的每个网段进行验证。MD5 身份验证必须在两个 BGP 对等设备上配置为使用相同的密码；否则，将不会建立它们之间的连接。配置 MD5 身份验证将使思科 ASA 软件生成并检查 TCP 连接上发送的每个网段的 MD5 摘要。

配置时，您可以提供最多 25 个字符的、区分大小写的密码，无论 **service password-encryption** 命令是否已启用。如果密码长度超过 25 个字符，将显示错误消息，并且不接受该密码。该字符串可以包含任意字母数字字符，包括空格。密码不能配置为 “ 数字 - 空格 - 任意字符 ” 格式。数字后的空格可导致身份验证失败。您还可以使用以下符号字符以及字母数字字符的任意组合：

` ~ !@ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < ., ?

注意事项　如果身份验证字符串配置不正确，将不会建立 BGP 对等会话。建议您小心地输入身份验证字符串，并在完成身份验证配置后验证对等会话是否已建立。

如果路由器为邻居配置了密码，但邻居路由器没有配置，则路由器尝试在两者之间建立 BGP 会话时将在控制台上显示类似如下的消息：

%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179（%TCP-6-BADAUTH：没有从 [对等设备的 IP 地址]:11003 到 [本地路由器的 IP 地址]:179 的 MD5 摘要）

类似地，如果两个路由器配置了不同的密码，则将在屏幕上显示类似如下的消息：

%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179 （%TCP-6-BADAUTH：从 [对等设备的 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

如果您配置或更改用于两个 BGP 对等设备之间 MD5 身份验证的密码或密钥，则本地路由器在您配置该密码后将不会关闭现有会话。本地路由器将尝试使用新密码保持对等会话，直到 BGP 抑制计时器过期。默认时段为 180 秒。如果在抑制计时器过期前仍未在远程路由器上输入或更改密码，则会话将超时。

注　为抑制计时器配置新计时器值仅当会话重置后才生效。因此，无法通过更改抑制计时器的配置来避免重置 BGP 会话。

示例

以下示例配置与 10.108.1.1 邻居的对等会话的 MD5 身份验证。 必须在抑制计时器过期前在远程对等设备上配置相同的密码。

```
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 **service password-encryption** 命令禁用时配置超过 25 个字符的密码。

```
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 12345678912345678912345678901
% 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 123456789123456789123456
```

以下示例在 **service password-encryption** 命令启用时配置超过 25 个字符的密码，并因此显示错误消息。

```
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 12345678912345678912345678901
% 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 123456789123456789123456
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
bgp router-id	配置本地边界网关协议 (BGP) 路由过程的固定路由器 ID。
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 邻居表。

neighbor prefix-list

要阻止按照前缀列表中的指定设置分发边界网关协议 (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*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*ip_address*} **p prefix-list** *prefix-list-name* {**in** | **out**}

语法说明

ip_address	邻居路由器的 IP 地址。
prefix-list-name	前缀列表的名称。
in	过滤器列表应用于来自该邻居的传入通告。
out	过滤器列表应用于到该邻居的传出通告。

命令默认

所有外部和通告的地址前缀均分发到 BGP 邻居。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用前缀列表是过滤 BGP 通告的三种方式之一。您还可以使用 AS 路径过滤器，该过滤器通过 **ip as-path access-list** 全局配置命令定义，在 **neighbor filter-list** 命令中用于过滤 BGP 通告。过滤 BGP 通告的第三种方式是将访问或前缀列表与 **neighbor distribute-list** 命令一起使用。

注　请勿将 **neighbor distribute-list** 和 **neighbor prefix-list** 命令同时应用于任何指定方向（入站或出站）的邻居。这两条命令是互斥的，只有一条命令（**neighbor distribute-list** 或 **neighbor prefix-list**）能应用于每个入站或出站方向。

示例

以下地址系列配置模式示例将名为 *abc* 的前缀列表应用于来自邻居 10.23.4.1 的传入通告：

```
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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
network	指定要通过 BGP 路由过程进行通告的网络。

neighbor remote-as

要将条目添加到 BGP 或多协议 BGP 邻居表，请在地址系列配置模式下使用 **neighbor remote-as** 命令。要从该表中删除条目，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **remote-as** *autonomous-system-number*

no neighbor {*ip_address*} **remote-as** *autonomous-system-number*

语法说明

ip_address	邻居路由器的 IP 地址。
autonomous-system-number	邻居所属的自主系统编号，范围为 1 到 65535。 有关自主系统编号格式的更多详情，请参阅 **router bgp** 命令。 与 **alternate-as** 关键字一起使用时，最多可输入五个自主系统编号。

命令默认

没有 BGP 或多协议 BGP 邻居对等设备。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

指定一个自主系统编号与 **router bgp** 全局配置命令中所指定自主系统编号匹配的邻居，即可将该邻居视为位于本地自主系统内部。否则，该邻居被视为外部。

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** 关键字指定最多五个可在其中标识动态 BGP 邻居的备用自主系统。 BGP 动态邻居支持允许与通过 IP 地址范围定义的一组远程邻居的 BGP 对等。使用 IP 地址范围和 BGP 对等设备组来配置 BGP 动态邻居。使用 **bgp listen** 命令配置子网范围并与 BGP 对等设备组关联，以及对子网范围内的 IP 地址发起 TCP 会话后，新 BGP 邻居将动态创建为该组的成员。新的 BGP 邻居将继承该组的任何配置或模板。

思科实施 4 字节自主系统编号，使用 asplain （例如 65538）作为自主系统编号的默认正则表达式匹配和输出显示格式，但您可以如 RFC 5396 中所述配置 asplain 格式和 asdot 格式的 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为 asdot 格式，请使用 **bgp asnotation dot** 命令后跟 **clear bgp *** 命令执行所有当前 BGP 会话的硬重置。

示例

以下示例指定位于地址 10.108.1.2 的路由器作为自主系统编号 65200 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 BGP 路由器分配到自主系统 65400，而两个网络作为自主系统中的源列出。然后列出三个远程路由器 （及其自主系统）的地址。所配置的路由器将与邻居路由器共享关于网络 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位于不同自主系统中的远程路由器（eBGP 邻居）；第二条 **neighbor remote-as** 命令显示位于地址 10.108.234.2 的内部 BGP 邻居 （具有相同的自主系统编号）；最后一条 **neighbor remote-as** 命令指定与输入此配置的路由器位于不同网络中的邻居 （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
```

以下示例将自主系统 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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
network	指定要通过 BGP 路由过程进行通告的网络。
neighbor remove private-as	从 eBGP 出站路由更新中删除专用自主系统编号。

neighbor remove-private-as

要从 eBGP 出站路由更新中删除专用自主系统编号，请在地址系列配置模式下使用 **neighbor remove-private-as** 命令。要禁用此功能，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **remove-private-as** [**all** [**replace-as**]]

no neighbor {*ip_address*} **remove-private-as** [**all** [**replace-as**]]

语法说明

ip_address	邻居路由器的 IP 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** 关键字就会将 AS 路径中的所有专用 AS 编号替换为路由器的本地 AS 编号。

命令默认

没有从 AS 路径中删除任何专用 AS 编号。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令仅适用于外部 BGP (eBGP) 邻居。专用 AS 值为 64512 到 65535。更新传递到外部邻居后，如果 AS 路径包括专用 AS 编号，则软件将丢弃专用 AS 编号

- 即使该路径同时包含公用和专用 ASN，**neighbor remove-private-as** 命令也会从 AS 路径中删除专用 AS 编号
- 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。不可能有 0 长度的 AS 路径，因为此命令只能应用于 eBGP 对等设备。在这种情况下，本地路由器的 AS 编号将附加到 AS 路径。即使专用 ASN 在 AS 路径中的联盟网段之前显示，**neighbor remove-private-as** 命令也会删除专用 AS 编号。
- 从 AS 路径中删除专用 AS 编号后，发送出去的前缀路径长度也将缩短。由于 AS 路径长度是 BGP 最佳路径选择的重要元素，因此可能有必要保留该路径长度。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。
- 该功能可以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 （而不是另一个地址系列）中的邻居，从而仅影响配置该功能的地址系列出站端的更新消息。

示例

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。结果是通过 AS 100 由 10.108.1.1 通告的路径的 AS 路径将仅包含 “100”（如自主系统 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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor description	将说明与邻居关联
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。要删除路由映射，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip_address*} **route-map** *map-name* {**in** | **out**}

语法说明

ip_address	邻居路由器的 IP 地址。
map-name	路由映射的名称。
in	将路由映射应用于传入路由。
out	将路由映射应用于传出路由。

命令默认

没有路由映射应用于对等设备。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

在地址系列配置模式下指定时，此命令将路由映射仅应用于该特定地址系列。在路由器配置模式下指定时，此命令将路由映射仅应用于 IPv4 单播路由。

如果指定了出站路由映射，则仅通告至少匹配一个路由映射区段的路由是正确的行为。

示例

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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
match as-path	匹配由访问列表指定的 BGP 自主系统路径
route-map	定义从一个路由协议到另一个的重分布路由的条件。
match as-path	匹配由访问列表指定的 BGP 自主系统路径。
set local-preference	指定自主系统路径的首选项值。

neighbor send-community

要指定应将社区属性发送给 BGP 邻居，请在地址系列配置模式下使用 **neighbor send-community** 命令。要删除条目，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **send-community** [**both** | **standard**]

no neighbor{*ip_address*} **send-community** [**both** | **standard**]

语法说明

ip_address	邻居路由器的 IP 地址。
both	（可选）指定将发送标准和扩展社区。
standard	（可选）指定仅发送标准社区。

命令默认

不会向任何邻居发送任何社区属性。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

示例

在以下地址系列配置模式示例中，路由器属于自主系统 109 并配置为将社区属性发送到其位于 IP 地址 172.16.70.23 的邻居：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。

neighbor shutdown

要禁用邻居，请在地址系列配置模式下使用 **neighbor shutdown** 命令。要重新启用邻居，请使用此命令的 **no** 形式。

neighbor *ip_address* **shutdown**

no neighbor *ip_address* **shutdown**

语法说明

ip_address	邻居路由器的 IP 地址。

命令默认

不会对任何 BGP 邻居的状态进行更改。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

neighbor shutdown 命令会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 邻居的摘要，请使用 **show bgp summary** 命令。这些邻居的状态为 Idle （空闲），并且 **neighbor shutdown** 命令已禁用管理员输入。

“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。达到最大数量 （如 **neighbor maximum-prefix** 命令所设置）时，条目中显示字符串 “PfxRcd”，邻居将关闭，并且连接空闲。

示例

以下示例禁用邻居 172.16.70.23 的任何活动会话：

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	启用与 BGP 邻居的信息交换。
show bgp summary	显示 BGP 邻居状态的摘要。

neighbor timers

要设置特定 BGP 对等设备的计时器，请在地址系列配置模式下使用 **neighbor timers** 命令。要清除特定 BGP 对等设备的计时器，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **timers** *keepalive* holdtime [*min- holdtime*]

no neighbor {*ip_address*} **timers**

语法说明

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

命令默认

Keepalive 时间：60 秒

Holdtime：180 秒

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

- 为特定邻居配置的计时器将覆盖使用 **timers bgp** 命令为所有 BGP 邻居配置的计时器。
- 当 *holdtime* 参数配置的值小于 20 秒时，将显示以下警告：A hold time of less than 20 seconds increases the chances of peer flapping.（小于 20 秒的保持时间会增加对等设备摆动的几率。）
- 如果最短可接受保持时间的时间间隔大于指定的保持时间，将显示一条通知：Minimum acceptable hold time should be less than or equal to the configured hold time.（最短可接受保持时间应小于或等于配置的保持时间。）

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

示例

以下示例将 BGP 对等设备 192.168.47.0 的 keepalive 计时器更改为 70 秒并将 hold-time 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 对等设备 192.168.1.2 的 keepalive 计时器更改为 70 秒、hold-time 计时器更改为 130 秒以及最短保持时间的时间间隔更改为 100 秒：

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	允许与 BGP 邻居交换信息。

neighbor transport

要启用边界网关协议 (BGP) 会话的 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*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** [**disable**]}

no neighbor {*ip_address*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** [**disable**]}

语法说明

ip_address	邻居路由器的 IP 地址。
connection-mode	指定连接的类型 - 主动或被动。
active	指定主动连接。
passive	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， TCP 路径 MTU 发现已启用。
disable	禁用 TCP 路径 MTU 发现。

命令默认

如果没有配置此命令，则默认情况下 TCP 路径 MTU 发现已启用，但未启用任何其他 TCP 传输会话选项。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令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** 命令确定 TCP 路径 MTU 发现是否已启用。如果使用 **disable** 关键字禁用发现，则在继承了禁用发现模板的任何对等设备中也将禁用发现。

示例

以下示例显示如何将一个内部 BGP (iBGP) 邻居的 TCP 传输连接配置为主动：

```
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一个外部 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
```

以下示例显示如何禁用一个 BGP 邻居的 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
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	允许与 BGP 邻居交换信息。
neighbor remote-as	将条目添加到 BGP 或多协议 BGP 路由表。
show bgp neighbor	显示关于 BGP 邻居的信息

neighbor ttl-security

要保护边界网关协议 (BGP) 对等会话和配置分隔两个外部 BGP (eBGP) 对等设备的最大跃点数，请在地址配置模式下使用 **neighbor ttl-security** 命令。要禁用此功能，请使用此命令的 **no** 形式。

neighbor {*ip_address*} **ttl-security hops** *hop-count*

no neighbor {*ip_address*} **ttl-security hops** *hop-count*

语法说明

ip_address	邻居路由器的 IP 地址。
hop-count	分隔 eBGP 对等设备的跃点数。 TTL 值根据来自配置的 *hop-count* 参数由路由器计算。 有效值是 1 到 254 之间的数字。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

neighbor ttl-security 命令提供了一种轻型安全机制，用于保护 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设备的 TTL 计数是不可能的。

应在每个参与的路由器上配置此功能。它仅保护传入方向的 BGP 会话，对传出的 IP 数据包或远程路由器没有影响。启用此功能后，BGP 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 keepalive 数据包，对等会话仍可过期。如果收到的数据包中的 TTL 值小于本地配置的值，则数据包以静默方式丢弃，并且不会生成互联网控制消息协议 (ICMP) 消息。这是设计的行为；不必响应伪造的数据包。

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) 对等设备不支持此功能。
- 对于已使用 **neighbor ebgp-multihop** 命令配置的对等设备，无法配置 **neighbor ttl-security** 命令。这些命令的配置是互斥的，只需其中一条命令来启用多跃点 eBGP 对等会话。如果您尝试为同一对等会话配置两条命令，控制台中将显示错误消息。
- 此功能的有效性在大范围的多跃点对等中会降低。如果基于 CPU 利用率的攻击针对为大范围对等配置的 BGP 路由器，您可能仍需要关闭受影响的对等会话以处理攻击。
- 对于来自已危及网络内部的对等设备的攻击，此功能无效。此限制还包括位于源与目标网络之间网段上的对等设备。

示例

以下示例将直连邻居的跃点数设置为 2。由于 *hop-count* 参数设置为 2， BGP 仅接受报头中的 TTL 计数等于或大于 253 的 IP 数据包。如果接收的数据包的 IP 数据包报头中有任何其他 TTL 值，该数据包将以静默方式丢弃。

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	允许与 BGP 邻居交换信息。
neighbor ebgp-multihop	接受并尝试与位于非直连网络上外部对等设备的 BGP 连接

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*} **version** *number*

no neighbor{*ip_address*} **version** *number*

语法说明

ip_address	邻居路由器的 IP 地址。
number	BGP 版本号。版本可以设置为 2 以强制软件对指定的邻居仅使用版本 2。默认使用版本 4 并可根据请求动态协商降至版本 2。

命令默认

BGP 版本 4。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

输入此命令可禁用动态版本协商。

示例

以下示例锁定至 BGP 协议的版本 4：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	允许与 BGP 邻居交换信息。

neighbor weight

要将权重分配给邻居连接，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*} **weight** *number*

no neighbor {*ip_address*} **weight** *number*

语法说明

ip_address	邻居路由器的 IP 地址。
number	要分配的权重。 有效值介于 0 到 65535 之间。

命令默认

通过另一个 BGP 对等设备获知的路由默认权重为 0，而源自本地路由器的路由默认权重为 32768。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
地址系列配置模式	• 是	—	• 是	• 是	—

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

从该邻居获知的所有路由都有初始分配权重。特定网络有多个可用的路由时，将选择具有最高权重的路由作为首选路由。

通过 **set weight** route-map 命令分配的权重将覆盖使用 **neighbor weight** 命令分配的权重。

示例

以下地址系列配置模式示例设置通过 172.16.12.1 至 50 获知的所有路由的权重：

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

相关命令

命令	说明
address-family ipv4	进入地址系列配置模式。
neighbor activate	允许与 BGP 邻居交换信息。

nem

要为硬件客户端启用网络扩展模式，请在组策略配置模式下使用 **nem enable** 命令。要禁用 NEM，请使用 **nem disable** 命令。要从正在运行的配置中删除 NEM 属性，请使用此命令的 **no** 形式。此选项允许从其他组策略继承值。

nem {**enable** | **disable**}

no nem

语法说明

disable	禁用网络扩展模式。
enable	启用网络扩展模式。

默认值

网络扩展模式已禁用。

命令模式

下表显示可输入命令的模式：

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

使用指南

网络扩展模式可让硬件客户端为 VPN 隧道上的远程专用网络提供单一、可路由的网络。 IPsec 封装从硬件客户端后面的专用网络到 ASA 后面的网络的所有流量。 PAT 不适用。因此， ASA 后面的设备可直接访问隧道上（并且仅限隧道上）硬件客户端后面的专用网络中的设备，反之亦然。硬件客户端必须启动隧道，但隧道运行后，任一端均可发起数据交换。

命令历史

版本	**修改**
7.0(1)	引入了此命令。

示例

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 enabl
```

network

要指定 RIP 路由过程的网络列表，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*}

no network {*ip_addr*}

语法说明

ip_addr	直连网络的 IP 地址。连接到指定网络的接口将参与 RIP 路由过程。

默认值

没有指定任何网络。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

指定的网络号不得包含任何子网信息。您可以在路由器上使用的 network 命令的数量没有限制。RIP 路由更新仅通过指定网络上的接口进行发送和接收。此外，如果未指定接口的网络，则接口不会在任何 RIP 更新中进行通告。

示例

以下示例将 RIP 定义为要在连接到网络 10.0.0.0 和 192.168.7.0 的所有接口上使用的路由协议：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
```

相关命令

命令	说明
router rip	进入路由器配置模式。
show running-config router	显示全局路由器配置中的命令。

network (EIGRP)

要指定 EIGRP 路由过程的网络列表，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*]

语法说明

ip_addr	直连网络的 IP 地址。连接到指定网络的接口将参与 EIGRP 路由过程。
mask	（可选） IP 地址的网络掩码。

默认值

没有指定任何网络。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

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。它从 EIGRP 拓扑表中指定的网络插入连接的子网。

ASA 随即通过匹配的接口建立邻居。 ASA 上可配置的 **network** 命令的数量没有限制。

示例

以下示例将 EIGRP 定义为要在连接到网络 10.0.0.0 和 192.168.7.0 的所有接口上使用的路由协议：

```
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
```

相关命令

命令	说明
show eigrp interfaces	显示关于为 EIGRP 配置的接口的信息。
show eigrp topology	显示 EIGRP 拓扑表。

network BGP

要指定通过边界网关协议 (BGP) 路由过程通告的网络，请在地址系列配置模式下使用 **network** 命令。要从路由表中删除条目，请使用此命令的 **no** 形式。

network {*network-number [***mask** *network-mask]*} *[***route-map** *map-tag]*

no network {*network-number [***mask** *network-mask]*} *[***route-map** *map-tag]*

语法说明

network-number	BGP 或多协议 BGP 将通告的网络。
mask *network-mask*	（可选）网络或子网掩码及掩码地址。
route-map *map-tag*	（可选）配置的路由映射的标识符。应检查路由映射以过滤要通告的网络。如果没有指定，将通告所有网络。如果已指定关键字，但未列出任何路由映射标记，将不会通告任何网络。

默认值

没有指定任何网络。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

BGP 和多协议 BGP 网络可从连接的路由、动态路由和静态路由来源获知。

您可以使用 **network** 命令的最大数量由路由器资源 （例如已配置的 NVRAM 或 RAM）确定。

示例

以下示例设置要包含在 BGP 更新中的网络 10.108.0.0：

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

相关命令

命令	说明
show bgp interfaces	显示 BGP 路由表中的条目。

network-acl

要指定以前使用 **access-list** 命令配置的防火墙 ACL 名称，请在动态访问策略记录配置模式下使用 **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，请使用该命令且不带参数。

network-acl *name*

no network-acl [*name*]

语法说明

name	指定网络 ACL 的名称。名称的最大数量是 240 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

多次使用此命令以将多个防火墙 ACL 分配给 DAP 记录。

ASA 验证您指定的每个 ACL 以确保其只包含访问列表条目的允许规则或只包含拒绝规则。如果任何指定的 ACL 包含混合的允许和拒绝规则，则 ASA 会拒绝该命令。

以下示例显示如何将名为 Finance Restrictions 的网络 ACL 应用于名为 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)#
```

相关命令

命令	说明
access-policy	配置防火墙访问策略。
dynamic-access-policy-record	创建 DAP 记录。
show running-config dynamic-access-policy-record [*name*]	显示所有 DAP 记录或指定 DAP 记录正在运行的配置。

network area

要定义 OSPF 在其上运行的接口和定义这些接口的区域 ID，请在路由器配置模式下使用 **network area** 命令。要禁用通过地址 / 网络掩码对定义的接口的 OSPF 路由，请使用此命令的 **no** 形式。

network *addr mask* **area** *area_id*

no network *addr mask* **area** *area_id*

语法说明

addr	IP 地址。
area *area_id*	指定要与 OSPF 地址范围关联的区域。*area_id* 可以指定为 IP 地址格式或十进制格式。指定为十进制格式时，有效值范围为 0 到 4294967295。
mask	网络掩码。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使 OSPF 在接口上运行，该接口的地址必须在 **network area** 命令的覆盖范围内。如果 **network area** 命令未覆盖该接口的 IP 地址，则该接口上将不会启用 OSPF。

您可以在 ASA 上使用的 **network area** 命令的数量没有限制。

示例

以下示例在 192.168.1.1 接口上启用 OSPF 并将其分配给区域 2：

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

相关命令

命令	说明
router ospf	进入路由器配置模式。
show running-config router	显示全局路由器配置中的命令。

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，请在对象组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 {**host** *address* | *IPv4_address mask* | *IPv6_address*/*IPv6_prefix* | **object** *name*}

no network-object {**host** *ip_address* | *ip_address mask* | **object** *name*}

语法说明

host *ip_address*	指定主机 IPv4 或 IPv6 地址。
IPv4_address mask	指定 IPv4 网络地址和子网掩码。
IPv6_address/*IPv6_prefix*	指定 IPv6 网络地址和前缀长度。
object *name*	指定网络对象 （通过 **object network** 命令创建）。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
对象组网络配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
8.3(1)	添加了 **object** 参数以支持网络对象 （**object network** 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，虽然在 NAT 中无法使用混合的组。

使用指南

network-object 命令与 **object-group** 命令一起使用可定义主机对象、网络对象或子网对象。

示例

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)#
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object-group** 命令。
group-object	添加网络对象组。
object network	添加网络对象。
object-group network	定义网络对象组。
show running-config object-group	显示当前对象组。

nop

要定义具有 IP 选项检查的数据包中出现 No Operation （无操作） IP 选项时的操作，请在参数配置模式下使用 **nop** 命令。要禁用此功能，请使用此命令的 **no** 形式。

nop action {**allow** | **clear**}

no nop action {**allow** | **clear**}

语法说明

allow	指示 ASA 允许包含 No Operation （无操作） IP 选项的数据包通过。
clear	指示 ASA 从数据包清除 No Operation（无操作）IP 选项，然后允许该数据包通过。

默认值

默认情况下， IP 选项检查丢弃包含 No Operation （无操作） IP 选项的数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

此命令可在 IP 选项检查策略映射中进行配置。

您可以配置 IP 选项检查以控制允许哪些具有特定 IP 选项的 IP 数据包通过 ASA。配置此检查将指示 ASA 允许数据包通过，或清除指定的 IP 选项后允许该数据包通过。

IP 报头中的 Options （选项）字段可包含零个、一个或多个选项，因此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并非 32 位的倍数，则 No Operation (NOP)（无操作 [NOP]）或 IP Option 1 （IP 选项 1）将用作 “ 内部填充 ” 以在 32 位边界上对齐选项。

示例

以下示例显示如何在策略映射中设置 IP 选项检查的操作：

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

相关命令

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

nsf cisco

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科无中断转发 (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]

语法说明

enforce global	（可选）重新启动过程中检测到任何接口上的相邻网络设备并非 NSF 感知时，取消所有接口上的 NSF 重新启动。

默认值

默认情况下，思科 NSF 平滑重启已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令在 OSPF 路由器上启用思科 NSF。在路由器上启用 NSF 后，路由器将支持 NSF 并在重新启动模式下运行。

如果路由器应仅与执行 NSF 平滑重启的邻居合作，则邻居路由器必须运行支持 NSF 的思科软件版本，但无需在该路由器上配置 NSF。路由器运行支持 NSF 的思科软件版本时，该路由器即为 NSF 感知。

默认情况下，在平滑重启过程中，相邻的 NSF 感知路由器将在 NSF 助手模式下运行。

如果 NSF 平滑重启过程中网络接口上检测到的邻居并非 NSF 感知，则仅该接口上的重新启动中止，并且平滑重启将在其他接口上继续。要在重新启动过程中检测到邻居并非 NSF 感知时取消整个 OSPF 过程的重新启动，请使用 **enforce global** 关键字配置此命令。

注　任何接口上检测到相邻关系重置或 OSPF 接口关闭时，也会取消整个过程的 NSF 平滑重启。

示例

以下示例启用思科 NSF 平滑重启并带有 enforce global 选项：

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# cisco nsf enforce global
```

相关命令

命令	说明
nsf cisco helper	在 ASA 上启用思科 NSF 助手模式。
nsf ietf	启用 IETF NSF

nsf cisco helper

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科无中断转发 (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，思科 NSF 助手模式已启用，可通过在路由器配置模式下发出 **no nsf cisco helper** 禁用该模式。

nsf cisco helper

no nsf cisco helper

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，思科 NSF 助手模式已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

ASA 启用 NSF 时， ASA 据称支持 NSF，并将在平滑重启模式下运行 - 由于路由处理器 (RP) 切换，因此 OSPF 路由器进程执行无中断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 是 NSF 感知，并将在 NSF 助手模式下运行。支持 NSF 的 ASA 执行平滑重启时，助手 ASA 将协助无中断转发恢复过程。如果不想 ASA 通过无中断转发恢复帮助重新启动邻居，请输入 **no nsf cisco helper** 命令。

示例

以下示例禁用 NSF 助手模式：

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# no nsf cisco helper
```

相关命令

命令	说明
nsf cisco	在 ASA 上启用思科 NSF。
nsf ietf	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 *seconds***]**

no nsf ietf

语法说明

restart-interval *seconds*	（可选）指定平滑重启时间间隔的长度 （以秒为单位）。范围为 1 至 1800。默认值为 120。 **注**　对于低于 30 秒的重新启动时间间隔，平滑重启将终止。

默认值

IETF NSF 平滑重启模式已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令在 ASA 上启用 IETF NSF。在 ASA 上启用 NSF 后，ASA 将支持 NSF 并在重新启动模式下运行。

如果 ASA 应仅与执行 NSF 平滑重启的邻居合作，则邻居 ASA 必须支持 NSF，但无需在该路由器上配置 NSF。 ASA 运行支持 NSF 的应用时， ASA 即为 NSF 感知。

示例

以下示例禁用 NSF 助手模式：

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# nsf ietf restart-interval 240
```

相关命令

命令	说明
nsf cisco	在 ASA 上启用思科 NSF。
nsf cisco helper	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， IETF NSF 助手模式已启用。要显式启用 IETF NSF 助手模式，请在路由器配置模式下使用 **nsf ietf helper** 命令。使用该命令的 **no** 形式即可禁用该模式。

（可选）使用 **nsf ietf helper strict-lsa-checking** 命令可以启用严格链路状态通告 (LSA) 检查。

nsf ietf helper [strict-lsa-checking]

no nsf ietf helper

语法说明

strict-lsa-checking	（可选）为助手模式启用严格链路状态通告 (LSA) 检查。

默认值

默认情况下， IETF NSF 助手模式已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

ASA 启用 NSF 时，据称其支持 NSF，并将在平滑重启模式下运行 - 由于路由处理器 (RP) 切换，OSPF 进程执行无中断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 是 NSF 感知，并将在 NSF 助手模式下运行。支持 NSF 的 ASA 执行平滑重启时，助手 ASA 将协助无中断转发恢复过程。如果不想 ASA 通过无中断转发恢复帮助重新启动邻居，请输入 **no nsf ietf helper** 命令。

要在 NSF 感知和支持 NSF 的 ASA 上启用严格 LSA 检查，请输入 **nsf ietf helper strict-lsa-checking** 命令。但是，严格 LSA 检查将不会生效，直到 ASA 在 IETF 平滑重启过程中变为助手 ASA。严格 LSA 检查启用后，如果助手 ASA 检测到将导致重新启动 ASA 的 LSA 变更，或平滑重启过程启动时重启 ASA 的重新传输列表上有更改的 LSA，它将终止帮助重新启动 ASA 的过程。

示例

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
```

相关命令

命令	说明
nsf cisco	在 ASA 上启用思科 NSF。
nsf cisco helper	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

要指定此服务器的 NT 主域控制器的名称，请在 AAA 服务器主机配置模式下使用 **nt-auth-domain-controller** 命令。要删除此指定，请使用此命令的 **no** 形式。

nt-auth-domain-controller *string*

no nt-auth-domain-controller

语法说明

string	指定此服务器主域控制器的名称，最多 16 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅对 NT 身份验证 AAA 服务器有效。您必须首先使用 **aaa-server host** 命令进入主机配置模式。 *string* 变量中的名称必须匹配服务器本身上的 NT 条目。

示例

以下示例将此服务器 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)#
```

相关命令

命令	说明
aaa server host	进入 AAA 服务器主机配置模式，以便能够配置主机特定的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

ntp authenticate

要启用通过 NTP 服务器的身份验证，请在全局配置模式下使用 **ntp authenticate** 命令。要禁用 NTP 身份验证，请使用此命令的 **no** 形式。

ntp authenticate

no ntp authenticate

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您启用身份验证，则数据包中使用正确的受信任密钥时 ASA 仅与 NTP 服务器通信（请参阅 **ntp trusted-key** 命令）。 ASA 还使用身份验证密钥与 NTP 服务器同步（请参阅 **ntp authentication-key** 命令）。

示例

以下示例将 ASA 配置为仅同步到在其 NTP 数据包中提供身份验证密钥 42 的系统：

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp authentication-key 42 md5 aNiceKey
ciscoasa(config)# ntp trusted-key 42
```

相关命令

命令	说明
ntp authentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntp server	标识 NTP 服务器。
ntp trusted-key	提供 ASA 在数据包中使用的密钥 ID 以向 NTP 服务器进行身份验证。
show ntp associations	显示与 ASA 关联的 NTP 服务器。
show ntp status	显示 NTP 关联的状态。

ntp authentication-key

要设置密钥以通过 NTP 服务器进行身份验证，请在全局配置模式下使用 **ntp authentication-key** 命令。要删除密钥，请使用此命令的 **no** 形式。

ntp authentication-key *key_id* **md5** *key*

no ntp authentication-key *key_id* [**md5** [0 | 8] *key*]

语法说明

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多 32 个字符的字符串。
key_id	标识介于 1 到 4294967295 之间的密钥 ID。您必须使用 **ntp trusted-key** 命令将此 ID 指定为受信任密钥。
md5	将身份验证算法指定为 MD5，这是唯一支持的算法。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使用 NTP 身份验证，还应配置 **ntp authenticate** 命令。

示例

以下示例启用身份验证，标识受信任密钥 ID 1 和 2，并设置每个受信任密钥 ID 的身份验证密钥：

```
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
```

相关命令

命令	说明
ntp authenticate	启用 NTP 身份验证。
ntp server	标识 NTP 服务器。
ntp trusted-key	提供 ASA 在数据包中使用的密钥 ID 以向 NTP 服务器进行身份验证。
show ntp associations	显示与 ASA 关联的 NTP 服务器。
show ntp status	显示 NTP 关联的状态。

ntp server

要标识 NTP 服务器以在 ASA 上设置时间，请在全局配置模式下使用 **ntp server** 命令。要删除服务器，请使用此命令的 **no** 形式。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

语法说明

ip_address	设置 NTP 服务器的 IP 地址或主机名。
key *key_id*	如果您使用 **ntp authenticate** 命令启用身份验证，请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，因此指定在管理情景中定义的接口名称。
prefer	如果多台服务器具有类似的准确性，则将此 NTP 服务器设置为首选服务器。 NTP 使用算法来确定哪台服务器最准确并同步到该服务器。如果各服务器具有类似的准确性，则 **prefer** 关键字指定要使用哪台服务器。但是，如果某服务器的准确性显著高于首选服务器，则 ASA 使用更准确的服务器。例如， ASA 使用第 2 层的服务器取代第 3 层的首选服务器。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	此命令已修改以使源接口可选。

使用指南

您可以标识多台服务器； ASA 会使用最准确的服务器。在多情景模式下，仅在系统配置中设置 NTP 服务器。

示例

以下示例标识两台 NTP 服务器，并启用密钥 ID 1 和 2 的身份验证：

```
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
```

相关命令

命令	说明
ntp authenticate	启用 NTP 身份验证。
ntp authentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntp trusted-key	提供 ASA 在数据包中使用的密钥 ID 以向 NTP 服务器进行身份验证。
show ntp associations	显示与 ASA 关联的 NTP 服务器。
show ntp status	显示 NTP 关联的状态。

ntp trusted-key

要指定作为受信任密钥的身份验证密钥 ID（通过 NTP 服务器进行身份验证时需要该项），请在全局配置模式下使用 **ntp trusted-key** 命令。要删除受信任密钥，请使用此命令的 **no** 形式。您可以输入多个受信任密钥，以与多台服务器一起使用。

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

语法说明

key_id	设置介于 1 到 4294967295 之间的密钥 ID。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

要使用 NTP 身份验证，还应配置 **ntp authenticate** 命令。要与服务器同步，请使用 **ntp authentication-key** 命令设置密钥 ID 的身份验证密钥。

示例

以下示例启用身份验证，标识受信任密钥 ID 1 和 2，并设置每个受信任密钥 ID 的身份验证密钥：

```
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
```

相关命令

命令	说明
ntp authenticate	启用 NTP 身份验证。
ntp authentication-key	设置加密的身份验证密钥以与 NTP 服务器同步。
ntp server	标识 NTP 服务器。
show ntp associations	显示与 ASA 关联的 NTP 服务器。
show ntp status	显示 NTP 关联的状态。

num-packets

要指定 SLA 操作过程中发送的请求数据包数量，请在 SLA 监控协议配置模式下使用 **num-packets** 命令。要恢复默认值，请使用此命令的 **no** 形式。

num-packets *number*

no num-packets *number*

语法说明

number	SLA 操作过程中发送的数据包数量。有效值为从 1 到 100。 **注**　当指定为 number 参数 （本命令中）的所有数据包均丢失时，跟踪的路由失败。

默认值

发送的回应类型数据包的默认数量为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

增加发送数据包的默认数量以防止由于丢包导致可达性信息不正确。

示例

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求 / 响应时间探测操作。它将回应请求数据包的负载大小设置为 48 字节，并将 SLA 操作过程中发送的回应请求数量设置为 5。所有 5 个数据包必须全部丢失才会删除跟踪的路由

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

相关命令

命令	说明
request-data-size	指定请求数据包负载的大小。
sla monitor	定义 SLA 监控操作。
type echo	将 SLA 操作配置为回应响应时间探测操作。

第 14 章

object network 至 override-svc-download 命令

object network

要配置指定的网络对象，请在全局配置模式下使用 **object network** 命令。使用此命令的 **no** 形式可从配置中删除该对象。

object network *name* [**rename** *new_obj_name*]

no object network *name*

语法说明

name	指定网络对象的名称。名称长度可为 1 到 64 个字符，包含字母、数字和以下特殊字符：下划线、连字符、逗号、正斜线和句点。对象和对象组共享相同的命名空间。
rename *new_obj_name*	（可选）将对象重命名为新对象名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。
8.4(2)	引入了对完全限定域名 (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、 IP 地址范围 （IPv4 或 IPv6）或 FQDN。输入该命令后，使用 **host**、 **fqdn**、 **subnet** 或 **range** 命令将一个地址添加到该对象。

您还可以使用 **nat** 命令对此网络对象启用 NAT 规则。您只能为指定的对象定义一个 NAT 规则；如果要配置多个 NAT 规则，您需要创建指定相同 IP 地址的多个对象，例如 **object network obj-10.10.10.1-01**、 **object network obj-10.10.10.1-02**，以此类推。

如果您使用不同的 IP 地址配置现有网络对象，则新配置将取代现有配置。

示例

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
```

相关命令

命令	说明
clear configure object	清除创建的所有对象。
description	将说明添加到网络对象。
fqdn	指定完全限定域名网络对象。
host	指定主机网络对象。
nat	对网络对象启用 NAT。
object-group network	创建网络对象组。
range	指定网络对象的地址范围。
show running-config object network	显示网络对象配置。
subnet	指定子网的网络对象。

object service

要配置在使用该对象的所有配置中自动反映的服务对象，请在全局配置模式下使用 **object service** 命令。使用此命令的 **no** 形式可删除该对象。

object service *name* [**rename** *new_obj_name*]

no object service *object name* [**rename** *new_obj_name*]

语法说明

name	指定服务对象的名称。名称长度可为 1 到 64 个字符，包含字母、数字和以下特殊字符：下划线、连字符、逗号和句点。对象名称必须以字母开头。
rename *new_obj_name*	（可选）将对象重命名为新对象名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

服务对象可以包含协议、 ICMP、 ICMPv6、 TCP 或 UDP 端口或者端口范围。输入该命令后，使用 **service** 命令以将一个指定的服务添加到该对象。

如果您使用不同的协议以及一个或多个端口配置现有服务对象，则新配置将使用新协议和端口取代现有的协议和端口。

示例

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
```

相关命令

命令	说明
clear configure object	清除创建的所有对象。
service	配置服务对象的协议和端口。

object-group

要定义可用于优化您的配置的对象组，请在全局配置模式下使用 **object-group** 命令。使用此命令的 **no** 形式可从配置中删除对象组。

object-group {**protocol** | **network** | **icmp-type** | **security** | **user**} *grp_name*

object-group service *grp_name* [**tcp** | **udp** | **tcp-udp**]

语法说明

grp_name	标识对象组 （1 到 64 个字符），可以是字母、数字以及 “_”、 “-”、 “.” 字符的任意组合。
icmp-type	（不建议使用，请使用 **service** 代替。）定义一组 ICMP 类型，例如回显和回显回复。输入 **object-group icmp-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-group network** 命令后，使用 **network-object** 和 **group-object** 命令添加网络对象。您可以使用 IPv4 和 IPv6 地址的混合创建一个组。 **注**　您无法对 NAT 使用混合的对象组。
protocol	（不建议使用，请使用 **service** 代替。）定义一组协议，例如 TCP 和 UDP。输入 **object-group protocol** 命令后，使用 **protocol-object** 和 **group-object** 命令添加协议对象。
curity	定义与 Cisco TrustSec 一起使用的安全组对象。输入 **object-group protocol** 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 端口定义服务。
[**tcp** | **udp** | **tcp-udp**]	要定义一组混合的服务，请不要指定对象组的协议类型。输入 **object-group service** 命令后，使用 **service-object** 和 **group-object** 命令将服务对象添加到服务组。这是首选的方法，即使该对象应仅包含 TCP 或 UDP （或两者）端口列表。 不建议直接在 object-group service 命令中使用 **tcp**、**udp** 和 **tcp-udp** 关键字。相反，在该命令中不使用这些关键字，而在 **service-object** 命令中配置 TCP 和 UDP 端口。 如果包含上述关键字之一，则使用 **port-object** 和 **group-object** 命令添加端口组。
user	定义可用于通过身份防火墙控制访问权限的用户和用户组。输入 **object-group protocol** 命令后，使用 **user**、 **user-group** 和 **group-object** 命令添加用户和用户组对象。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	我们引入了此命令。
8.4(2)	我们添加了对 **user** 关键字的支持，用于支持身份防火墙。
9.0(1)	现在，您可以创建能支持 IPv4 和 IPv6 地址混合的网络对象组。 我们添加了对 **security** 关键字的支持，用于支持 Cisco TrustSec。

使用指南

可以将对象 （如主机或服务）分组，然后可以在如 ACL (**access-list**) 和 NAT (**nat**) 之类的功能中使用对象组。本例显示在 ACL 中使用网络对象组：

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group
NWgroup1
```

您可以按层次结构来组合命令；一个对象组可以是另一个对象组的成员。

示例

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** 模式创建包含以前定义对象的新对象组，以及随后如何在 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，您需要定义 *all_hosts* 组以包含 *host_grp_1* 和 *host_grp_2* 中已经定义的所有 IP 地址。通过 **group-object** 命令可避免主机的重复定义。

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一个服务对象组：

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh

ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object)# service eigrp

ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object)# 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一个服务对象组中添加指定的各个协议、端口和 ICMP：

```
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，该子命令对分组 TCP 和 UDP 服务非常有用：

```
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.pyl.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，请用服务对象代替。）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，请用服务对象代替。）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，请不要使用 **tcp** 关键字，而用 **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。此分组能够在 1 行而不是 24 行中配置访问列表，不使用任何分组时将需要此功能。

```
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　**show running-config access-list** 命令显示访问列表，如采用对象组名称所配置。 **show access-list** 命令显示此信息以及访问列表条目，这些条目使用扩展为单个条目的组，而无需其对象分组。

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object group** 命令。
group-object	添加网络对象组。
network-object	将网络对象添加到网络对象组。
port-object	将端口对象添加到服务对象组。
security-group	将安全组添加到安全组对象组。
show running-config object-group	显示当前对象组。
user	将用户名添加到用户组对象。
user-group	将用户组名称添加到用户组对象。

object-group-search

要启用 ACL 优化，请在全局配置模式下使用 **object-group-search** 命令。使用此命令的 **no** 形式可禁用 ACL 优化。

object-group-search access-control

no object-group-search access-control

语法说明

access-control	搜索访问控制域。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

object-group-search 命令可优化入站方向的所有 ACL。

您可以通过启用对象组搜索减少搜索访问规则所需的内存，但这会降低查找性能。启用后，对象组搜索不使用 ASP 表中的网络对象扩展 ACL，而是基于这些组定义来搜索访问规则有无匹配。您将在 **show access-list** 输出中看到此内容。

在 ASA 上启用 **object-group-search access-control** 命令后，随着大量功能的启用、大量活动连接的建立以及大型 ACL 的加载，操作期间会有掉线，并且建立新连接时将出现性能下降。

示例

以下示例显示如何使用 **object-group-search** 命令启用 ACL 优化：

```
ciscoasa(config)# object-group-search access-control
```

以下是 **object-group-search** 未启用时 **show access-list** 命令的示例输出：

```
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 **object-group-search** 启用时 **show access-list** 命令的示例输出：

```
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
```

相关命令

命令	说明
clear config object-group search	清除 object-group-search 配置。
show object-group	显示对象组为网络对象组类型时的命中数。
show running-config object-group	显示当前对象组。
show running-config object-group-search	显示运行的配置中的 object-group-search 配置。

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 nonce 扩展，请使用此命令的 **no** 形式。

ocsp disable-nonce

no ocsp disable-nonce

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， OCSP 请求包含 nonce 扩展。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

当您使用此命令时， OCSP 请求不包含 OCSP nonce 扩展，并且 ASA 不会进行检查。默认情况下， OCSP 请求包含一个 nonce 扩展，它通过加密方式将请求与响应绑定，以避免重播攻击。但是，有些 OCSP 服务器使用预生成的响应，不包含此匹配的 nonce 扩展。要将 OCSP 与这些服务器一起使用，则必须禁用 nonce 扩展。

示例

以下示例显示如何对名为 newtrust 的信任点禁用 nonce 扩展。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 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。
ocsp url	指定 OCSP 服务器以用来检查与信任点关联的所有证书。
revocation-check	指定用于撤销检查的方法及其尝试顺序。

ocsp url

要为 ASA 配置用于检查与信任点关联的所有证书的 OCSP 服务器 （而不是客户端证书 AIA 扩展中指定的服务器），请在 crypto ca trustpoint 配置模式下使用 **ocsp url** 命令。要从配置中删除该服务器，请使用此命令的 **no** 形式。

ocsp url *URL*

no ocsp url

语法说明

URL	指定 OCSP 服务器的 HTTP URL。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

ASA 仅支持 HTTP URL，并且每个信任点只能指定一个 URL。

ASA 提供三种方式用于定义 OCSP 服务器 URL，并根据您进行定义的方式按以下顺序尝试使用 OCSP 服务器：

- 您使用 **match certificate** 命令设置的 OCSP 服务器。
- 您使用 **ocsp url** 命令设置的 OCSP 服务器。
- 客户端证书 AIA 字段中的 OCSP 服务器。

如果您没有通过 **match certificate** 命令或 **ocsp url** 命令配置 OCSP URL，则 ASA 使用客户端证书 AIA 扩展中的 OCSP 服务器。如果证书没有 AIA 扩展，则撤销状态检查失败。

示例

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 trustpoint newtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

相关命令

命令	说明
crypto ca trustpoint	进入 crypto ca trustpoint 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。
ocsp disable-nonce	禁用 OCSP 请求的 nonce 扩展。
revocation-check	指定用于撤销检查的方法及其尝试顺序。

onscreen-keyboard

要将屏幕键盘插入到登录窗格或具有登录 / 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，请使用该命令的 **no** 版本。

onscreen-keyboard {**logon** | **all**}

no onscreen-keyboard [logon | all]

语法说明

logon	为登录窗格插入屏幕键盘。
all	为登录窗格以及具有登录 / 密码要求的所有其他窗格插入屏幕键盘。

默认值

没有屏幕键盘。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

屏幕键盘可让您输入用户凭证而无需按键。

示例

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)#
```

相关命令

命令	说明
webvpn	进入 webvpn 模式，从而可让您配置无客户端 SSLVPN 连接的属性。

ospf authentication

要允许使用 OSPF 身份验证，请在接口配置模式下使用 **ospf authentication** 命令。要恢复默认身份验证，请使用此命令的 **no** 形式。

ospf authentication [**message-digest** | **null**]

no ospf authentication

语法说明

message-digest	（可选）指定此项可使用 OSPF 消息摘要身份验证。
null	（可选）指定此项表示不使用 OSPF 身份验证。

默认值

默认情况下， OSPF 身份验证未启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

使用 **ospf authentication** 命令之前，请使用 **ospf authentication-key** 命令配置接口的密码。如果使用 **message-digest** 关键字，则使用 **ospf message-digest-key** 命令配置接口的消息摘要密钥。

为实现向后兼容性，仍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 （区域默认类型为 Null 身份验证）。

如果不带任何选项使用此命令，则启用简单密码身份验证。

示例

以下示例显示如何在选定接口上为 OSPF 启用简单密码身份验证：

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

相关命令

命令	说明
ospf authentication-key	指定相邻路由设备使用的密码。
ospf message-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 **ospf authentication-key** 命令。要删除该密码，请使用此命令的 **no** 形式。

ospf authentication-key [**0** | **8**] *password*

no ospf authentication-key

语法说明 <

0	指定将后跟未加密的密码。
8	指定将后跟加密的密码。
password	分配相邻路由设备使用的 OSPF 身份验证密码。密码必须小于 9 个字符。您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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

发起路由协议数据包时，此命令创建的密码用作直接插入 OSPF 报头中的密钥。可以为每个接口的每个网络指定单独的密码。同一网络上的所有邻居路由器都必须有相同的密码，以便能交换 OSPF 信息。

示例注意

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
```

相关命令

命令	说明
area authentication	对指定的区域启用 OSPF 身份验证。
ospf authentication	允许使用 OSPF 身份验证。

ospf cost

要指定通过接口发送数据包的成本，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

语法说明

interface_cost	通过接口发送数据包的成本 （链路状态指标）。该项是 0 到 65535 的无符号整数值。 0 表示网络直接连接到接口；接口带宽越高，通过该接口发送数据包的关联成本越低。换句话说，较大的成本值表示低带宽接口，而较小的成本值表示高带宽接口。 ASA 上的 OSPF 接口默认成本为 10。此默认值与思科 IOS 软件不同，后者的默认成本为 1（适用于快速以太网和千兆位以太网）和 10（适用于 10BaseT）。如果您在网络中使用 ECMP，将此情况考虑在内非常重要。

默认值

默认 *interface_cost* 为 10。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

ospf cost 命令可让您显式指定在接口上发送数据包的成本。*interface_cost* 参数是 0 到 65535 的无符号整数值。

no ospf cost 命令可将路径成本重置为默认值。

示例

以下示例显示如何指定在选定接口上发送数据包的成本：

```
ciscoasa(config-if)# ospf cost 4
```

相关命令

命令	说明
show running-config interface	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，请在接口配置模式下使用 **ospf database-filter** 命令。要恢复 LSA，请使用此命令的 **no** 形式。

ospf database-filter all out

no ospf database-filter all out

语法说明

all out	过滤到 OSPF 接口的所有传出 LSA。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ospf database-filter 命令过滤到 OSPF 接口的传出 LSA。 **no ospf database-filter all out** 命令恢复到接口的 LSA 转发。

示例

以下示例显示如何使用 **ospf database-filter** 命令过滤传出 LSA：

```
ciscoasa(config-if)# ospf database-filter all out
```

相关命令

命令	说明
show interface	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 **ospf dead-interval** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ospf dead-interval {*seconds*| **minimal hello-multiplier** *multiplier*}

no ospf dead-interval

语法说明

seconds	以秒为单位的时长，在此期间看不到任何问候数据包。 *seconds* 的默认值是通过 **ospf hello-interval** 命令设置的间隔 （范围从 1 到 65535）的四倍。
minimal	将停顿间隔设置为 1 秒。使用此关键字还要求配置 hello-multiplier 关键字和 multiplier 参数。
hello-multiplier *multiplier*	范围从 3 到 20 的整数值，表示 1 秒钟内发送的问候数据包数量。

默认值

seconds 的默认值是通过 **ospf hello-interval** 命令设置的间隔的四倍。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。
9.2(1)	引入了对快速问候数据包的支持。

使用指南

通过 **ospf dead-interval** 命令，您可以设置邻居声明路由器关闭之前的停顿间隔 （即未看到任何问候数据包的时长）。 *seconds* 参数指定停顿间隔，并且该停顿间隔必须对网络上的所有节点相同。 *seconds* 的默认值是通过 **ospf hello-interval** 命令设置的间隔 （从 1 到 65535）的四倍。

no ospf dead-interval 命令恢复默认间隔值。

停顿间隔在 OSPF 问候数据包中通告。该值对特定网络上的所有网络设备必须相同。

指定较小的停顿间隔 （秒数）将更快地检测被关闭的邻居并提高融合，但可能导致路由更加不稳定。

快速问候数据包的 OSPF 支持

通过指定 minimal 和 hello-multiplier 关键字及 multiplier 参数，您可启用 OSPF 快速问候数据包。minimal 关键字将停顿间隔设置为 1 秒，而 hello-multiplier 值设置在该 1 秒钟内发送的问候数据包数量，从而提供亚秒级或“快速”问候数据包。

在接口上配置快速问候数据包后，从此接口发送出的问候数据包中通告的问候间隔将设置为 0。通过此接口接收的问候数据包中的问候间隔将被忽略。

停顿间隔在一个网段内必须一致，无论是设置为 1 秒 （适用于快速问候数据包）还是设置为任何其他值。 hello multiplier 无需对整个网段相同，只要至少有一个问候数据包在停顿间隔内发送即可。

使用 **show ospf interface** 命令验证停顿间隔和快速问候间隔。

示例

在以下示例中，通过指定 minimal 关键字以及 hello-multiplier 关键字和值启用快速问候数据包的 OSPF 支持。由于 multiplier 设置为 5，因此每秒将发送 5 个问候数据包。

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

相关命令

命令	说明
ospf hello-interval	指定在接口上两次发送问候数据包之间的间隔。
show ospf interface	显示 OSPF 相关接口信息。

ospf hello-interval

要指定在接口上两次发送问候数据包之间的间隔，请在接口配置模式下使用 **ospf hello-interval** 命令。要将问候间隔重置为默认值，请使用此命令的 **no** 形式。

ospf hello-interval *seconds*

no ospf hello-interval

语法说明

seconds	指定在接口上两次发送问候数据包之间的间隔；有效值为 1 到 65535 秒。

默认值

hello-interval *seconds* 的默认值为 10 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

该值在问候数据包中通告。问候间隔越小，越快检测到拓扑变化，但随之而来的路由流量也更多。对一个特定网络内的所有路由器和访问服务器，该值必须相同。

示例

以下示例将 OSPF 问候间隔设置为 5 秒：

```
ciscoasa(config-if)# ospf hello-interval 5
```

相关命令

命令	说明
ospf dead-interval	指定邻居声明路由器关闭之前的间隔。
show ospf interface	显示 OSPF 相关接口信息。

ospf message-digest-key

要启用 OSPF MD5 身份验证，请在接口配置模式下使用 **ospf message-digest-key** 命令。要删除 MD5 密钥，请使用此命令的 **no** 形式。

ospf message-digest-key *key-id* **md5** [**0** | **8**] *key*

no ospf message-digest-key

语法说明

key-id	启用 MD5 身份验证并指定数值身份验证密钥 ID 号；有效值为 1 到 255。
md5 *key*	最多 16 个字节的字母数字密码。您可以在密钥字符之间包含空格。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、对信源进行身份验证并检查时效性。
0	指定将后跟未加密的密码。
8	指定将后跟加密的密码。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

ospf message-digest-key 命令可让您启用 MD5 身份验证。该命令的 **no** 形式可让您删除旧的 MD5 密钥。*key_id* 是 1 到 255 的数字标识符，适用于身份验证密钥。*key* 是最多 16 个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。

示例

以下示例显示如何指定 OSPF 身份验证的 MD5 密钥：

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

相关命令

命令	说明
area authentication	启用 OSPF 区域身份验证。
ospf authentication	允许使用 OSPF 身份验证。

ospf mtu-ignore

要对接收的数据库数据包禁用 OSPF 最大传输单位 (MTU) 不匹配检测，请在接口配置模式下使用 **ospf mtu-ignore** 命令。要恢复 MTU 不匹配检测，请使用此命令的 **no** 形式。

ospf mtu-ignore

no ospf mtu-ignore

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， **ospf mtu-ignore** 已启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

OSPF 会检查邻居是否在通用接口上使用相同的 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，将不会建立 OSPF 邻接关系。 **ospf mtu-ignore** 命令将对接收的 DBD 数据包禁用 OSPF MTU 不匹配检测。该功能在默认情况下已启用。

示例

以下示例显示如何禁用 **ospf mtu-ignore** 命令：

```
ciscoasa(config-if)# ospf mtu-ignore
```

相关命令

命令	说明
show interface	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 **ospf network point-to-point non-broadcast** 命令。要从配置中删除此命令，请使用此命令的 **no** 形式。

ospf network point-to-point non-broadcast

no ospf network point-to-point non-broadcast

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

ospf network point-to-point non-broadcast 命令可让您通过 VPN 隧道传输 OSPF 路由。

当接口指定为点对点时，必须手动配置 OSPF 邻居；无法实现动态发现。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，具有以下限制：

- 您只能为该接口定义一个邻居。
- 您需要定义一个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。
- 如果隧道上的 OSPF 在接口上运行，则具有上游路由器的普通 OSPF 无法在同一接口上运行。
- 您应该在指定 OSPF 邻居之前将 crypto-map 绑定至接口，以确保 OSPF 更新通过 VPN 隧道进行传递。如果在指定 OSPF 邻居之后将 crypto-map 绑定至接口，则使用 **clear local-host all** 命令清除 OSPF 连接，以便能够在 VPN 隧道上建立 OSPF 邻接关系。

示例

以下示例显示如何将选定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)#
```

相关命令

命令	说明
neighbor	指定手动配置的 OSPF 邻居。
show interface	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 **ospf priority** 命令。要恢复默认优先级，请使用此命令的 **no** 形式。

ospf priority *number*

no ospf priority [*number*]

语法说明

number	指定路由器的优先级；有效值为 0 到 255。

默认值

number 的默认值为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

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路由器优先级的路由器。如果优先级相同，则优先采用具有较高路由器 ID 的路由器。路由器优先级设置为零的路由器没有资格成为指定路由器或备用指定路由器。配置的路由器优先级仅适用于多接入网络的接口 （换句话说，不适用于点对点网络）。

示例

以下示例显示如何更改选定接口上的 OSPF 优先级：

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

相关命令

命令	说明
show ospf interface	显示 OSPF 相关接口信息。

ospf retransmit-interval

要为属于接口的邻接关系指定两次 LSA 重新传输之间的时间，请在接口配置模式下使用 **ospf retransmit-interval** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ospf retransmit-interval [*seconds*]

no ospf retransmit-interval [*seconds*]

语法说明

seconds	指定属于接口的相邻路由器的两次 LSA 重新传输之间的时间；有效值为 1 到 65535 秒。

默认值

retransmit-interval *seconds* 的默认值为 5 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

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，它将重新发送该 LSA。

此参数应保守设置，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。

示例

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)#
```

相关命令

命令	说明
show ospf interface	显示 OSPF 相关接口信息。

ospf transmit-delay

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 **ospf transmit-delay** 命令。要恢复默认值，请使用此命令的 **no** 形式。

ospf transmit-delay [*seconds*]

no ospf transmit-delay [*seconds*]

语法说明

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 到 65535 秒。

默认值

seconds 的默认值为 1 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

更新数据包中的 LSA 在传输之前必须通过 *seconds* 参数中指定的量增加其时限。分配的值应考虑接口的传输和传播延迟。

如果在链路上传输之前没有添加延迟，则 LSA 在链路上传播的时间不考虑在内。此设置在速度非常低的链路上更重要。

示例

以下示例将选定接口的传输延迟设置为 3 秒：

```
ciscoasa(config-if)# ospf restransmit-delay 3
ciscoasa(config-if)#
```

相关命令

命令	说明
show ospf interface	显示 OSPF 相关接口信息。

otp expiration

要指定发出的一次性密码 (OTP) 对本地证书颁发机构 (CA) 注册页面有效的持续时间 （以小时为单位），请在 ca server 配置模式下使用 **otp expiration** 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

语法说明

timeout	指定注册页面的 OTP 过期之前用户必须注册本地 CA 证书的时间 （以小时为单位）。有效值范围为 1 到 720 小时 （30 天）。

默认值

默认情况下，证书注册的 OTP 期限为 72 小时 （3 天）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

OTP 过期时段指定用户必须登录到 CA 服务器注册页面的小时数。用户登录并注册证书后，**enrollment retrieval** 命令指定的时段开始。

注　通过注册接口页面注册证书的用户 OTP 还可用作密码来解锁包含该用户颁发的证书和密钥对的 PKCS12 文件。

示例

以下示例将注册页面适用的 OTP 指定为 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)#
```

相关命令

命令	说明
crypto ca server	提供 CA 服务器配置模式命令集的访问权限，从而允许您配置和管理本地 CA。
enrollment-retrieval	指定注册用户可以检索 PKCS12 注册文件的时间 （以小时为单位）。
show crypto ca server	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，请在事件管理器小应用配置模式下使用 **output console** 命令。要删除作为输出目标的控制台，请使用此命令的 **no** 形式。

output console

no output console

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用此命令可将 **action** 命令的输出发送到控制台。

示例

以下示例将 **action** 命令的输出发送到控制台：

```
ciscoasa(config-applet)# output console
```

相关命令

命令	说明
output file append	将 **action** 命令输出写入到一个文件，但该文件每次追加内容。
output file new	对于调用的每个小应用，将 **action** 命令的输出发送到一个新文件。
output file overwrite	将 **action** 命令输出写入到一个文件，该文件将每次截短。
output file rotate	创建一组轮换的文件。
output none	丢弃 **action** 命令的所有输出。

output file

要将 **action** 命令输出重定向到指定的文件，请在事件管理器小应用配置模式下使用 **output file** 命令。要删除指定的操作，请使用此命令的 **no** 形式。

output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

no output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

语法说明

append *filename*	将输出不断追加到指定文件名，即本地 （对于 ASA 来说）文件名。
new	为输出创建名为 eem-*applet-timestamp*.log 的新文件，其中 *applet* 是事件管理器小应用的名称，而 *timestamp* 是格式为 YYYYMMDD-hhmmss 的带日期时间戳。
overwrite *filename*	将输出写入到指定文件名，但每次调用事件管理器小应用时截短输出。
rotate *n*	为输出创建名为 eem-*applet-x*.log 的文件，其中 *applet* 是事件管理器小应用的名称，而 *x* 为编号。要写入新文件时，最旧的文件将被删除，并且在第一个文件写入之前，所有后续文件将重新编号。最新文件由 0 表示，最旧的文件由最高数字 (*n*-1) 表示。 *n* 参数指定轮换值。有效值范围从 2 到 100。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用 **output file** 命令可将 **action** 命令输出重定向到指定的文件。

示例

以下示例将输出追加到一个文件：

```
ciscoasa(config-applet)# output file append examplefile1
```

以下示例将 **action** 命令的输出发送到一个新文件：

```
ciscoasa(config-applet)# output file new
```

以下示例将输出写入到一个截短的文件：

```
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
```

相关命令

命令	说明
output console	将 **action** 命令的输出发送到控制台。
output none	丢弃 **action** 命令的所有输出。

output none

要丢弃 **action** 命令的所有输出，请在事件管理器小应用配置模式下使用 **output none** 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

语法说明

此命令没有任何参数或关键字。

默认值

默认值是丢弃 **action** 命令的所有输出。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

使用此命令可丢弃 **action** 命令的所有输出。

示例

以下示例丢弃 **action** 命令的所有输出：

```
ciscoasa(config-applet)# output none
```

相关命令

命令	说明
output console	将 **action** 命令的输出发送到控制台。
output file append	将 **action** 命令输出写入到一个文件，但该文件每次追加内容。
output file new	对于调用的每个小应用，将 **action** 命令的输出发送到一个新文件。
output file overwrite	将 **action** 命令输出写入到一个文件，该文件将每次截短。
output file rotate	创建一组轮换的文件。

outstanding

要限制未经身份验证的邮件代理会话数，请在适用的邮件代理配置模式下使用 **outstanding** 命令。要从配置中删除该属性，请使用此命令的 **no** 形式。

outstanding {*number*}

no outstanding

语法说明

number	允许的未经身份验证会话数。范围为 1 至 1000。

默认值

默认值为 20。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用此命令的 **no** 版本可从配置中删除该属性，从而允许不限数量的未经身份验证会话。这还将限制电邮端口上的 DOS 攻击。

电邮代理连接有三种状态：

1. 新电邮连接进入 “ 未经身份验证 ” 状态。
2. 连接提供用户名后，其进入 “ 正在进行身份验证 ” 状态。
3. ASA 对连接进行身份验证后，其进入 “ 已经过身份验证 ” 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 会终止最早的未经身份验证连接，以防止过载。它不会终止已经过身份验证的连接。

示例

以下示例显示如何为 POP3S 电邮代理设置 12 个未经身份验证会话的限制。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# outstanding 12
```

override-account-disable

要覆盖来自 AAA 服务器的 account-disabled 指示，请在 tunnel-group general-attributes 配置模式下使用 **override-account-disable** 命令。要禁用覆盖，请使用此命令的 **no** 形式。

override-account-disable

no override-account-disable

语法说明

此命令没有任何参数或关键字。

默认值

此命令默认禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1.1	引入了此命令。

使用指南

此命令适用于返回 “account-disabled” 指示的服务器 （例如具有 NT LDAP 的 RADIUS 和 Kerberos）。

您可以为 IPsec RA 和 WebVPN 隧道组配置此属性。

示例

以下示例允许对 WebVPN 隧道组 “testgroup” 覆盖来自 AAA 服务器的 “account-disabled” 指示器：

```
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)#
```

以下示例允许对 IPsec 远程访问隧道组 “QAgroup” 覆盖来自 AAA 服务器的 “account-disabled” 指示器：

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

相关命令

命令	说明
clear configure tunnel-group	清除 tunnel-group 数据库或特定隧道组的配置。
tunnel-group general-attributes	配置 tunnel-group general-attributes 值。

override-svc-download

要配置连接配置文件以覆盖用于下载 AnyConnect 或 SSL VPN 客户端的组策略或用户名属性配置，请从 tunnel-group webvpn attributes 配置模式下使用 **override-svc-download** 命令。要从配置中删除该命令，请使用该命令的 **no** 形式：

override-svc-download enable

no override-svc-download enable

默认值

默认设置为禁用。 ASA 不会覆盖用于下载客户端的组策略或用户名属性配置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

通过 **vpn-tunnel-protocol** 命令，安全设备根据在组策略或用户名属性中是否已启用无客户端和 / 或 SSL VPN，确定是否允许远程用户的无客户端、AnyConnect 或 SSL VPN 客户端连接。**svc ask** 命令通过提示用户下载客户端或返回到 WebVPN 主页来进一步改善客户端用户体验。

不过，您可能想要无客户端用户在特定隧道组下登录，从而无需体验延迟 （即等待下载提示过期，然后显示无客户端 SSL VPN 主页）。您可以使用 **override-svc-download** 命令在连接配置文件级别阻止这些用户的延迟。此命令导致向通过连接配置文件登录的用户立即显示无客户端 SSL VPN 主页，无论 **vpn-tunnel-protocol** 或 **svc ask** 命令设置如何。

示例

在以下示例中，用户针对连接配置文件 *engineering* 进入 tunnel-group webvpn attributes 配置模式，然后启用该连接配置文件以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
```

相关命令

命令	说明
show webvpn svc	显示关于已安装 SSL VPN 客户端的信息。
svc	为特定组或用户启用或要求 SSL VPN 客户端。
svc image	指定一个客户端软件包文件， ASA 在缓存内存中扩展该文件以用于下载到远程 PC。

第 15 章

packet-tracer 至 ping 命令

packet-tracer

要通过指定测试防火墙规则的 5 元组来启用数据包跟踪功能以进行故障排除，请在特权 EXEC 模式下使用 **packet-tracer** 命令。为清楚起见，下面分开展示了 ICMP、 TCP/UDP 和 IP 数据包建模的语法。

packet-tracer input *ifc_name* **icmp** [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
type code [*ident*]
{*dip* / **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
[**detailed**] [**xml**]

packet-tracer input *ifc_name* {**tcp** | **udp**} [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *sport*
{*dip* / **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dport*
[**detailed**] [**xml**]

packet-tracer input *ifc_name* **rawip** [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *protocol*
{*dip* / **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
[**detailed**] [**xml**]

语法说明

code	指定 ICMP 数据包跟踪的 ICMP 代码。
detailed	（可选）提供详细的跟踪结果信息。
dip	指定数据包跟踪的目标 IPv4 或 IPv6 地址。
dport	指定 TCP/UDP 数据包跟踪的目标端口。
fqdn *fqdn-string*	指定主机的完全限定域名，可以是源 IP 地址和目标 IP 地址。仅支持 IPv4 的 FQDN。
icmp	指定要使用的协议为 ICMP。
ident	（可选。）指定 ICMP 数据包跟踪的 ICMP 标识符。
inline-tag *tag*	指定要嵌入第 2 层 CMD 报头中的安全组标记值。有效值范围从 0 到 65533。
input *ifc_name*	指定在其上跟踪数据包的源接口的名称。
protocol	指定原始 IP 数据包跟踪的协议编号，从 0 到 255。
rawip	指定要使用的协议为原始 IP。
security-group {**name** *name* | **tag** *tag*}	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记编号。
sip	指定数据包跟踪的源 IPv4 或 IPv6 地址。
sport	指定 TCP/UDP 数据包跟踪的源端口。
tcp	指定要使用的协议为 TCP。
type	指定 ICMP 数据包跟踪的 ICMP 类型。
udp	指定要使用的协议为 UDP。
user *username*	如果您要指定用户为源 IP 地址，请以域 \ 用户格式指定用户身份。在跟踪中使用用户最近映射的地址 （如果有）。
xml	（可选）以 XML 格式显示跟踪结果。

默认值

此命令没有默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.4(2)	添加了两个关键字参数对：**user** *username* 和 **fqdn** *fqdn string*。已重命名和重新定义多个关键字。已增加对 IPv6 源地址的支持。
9.0(1)	已增加对用户身份的支持。仅支持 IPv4 完全限定域名 (FQDN)。
9.3(1)	添加了 **inline-tag** *tag* 关键字参数对来支持要嵌入第 2 层 CMD 报头中的安全组标记值。

使用指南

除捕捉数据包外，还可以通过 ASA 跟踪数据包的寿命，查看它的行为是否与预期一致。**packet-tracer** 命令使您能够执行以下操作：

- 调试生产网络中的所有丢包。
- 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的时间线。
- 向数据路径中注入跟踪数据包。
- 基于用户身份和 FQDN 搜索 IPv4 或 IPv6 地址。

packet-tracer 命令提供有关数据包的详细信息以及 ASA 处理它们的方式。如果配置的命令没有导致数据包丢弃，则 **packet-tracer** 命令以易读格式提供有关原因的信息。例如，如果因无效报头验证丢弃了数据包，将显示以下消息：“packet dropped due to bad ip header (reason).（数据包因错误的 IP 报头 [原因] 而丢弃。）”

您可以在此命令的源部分中以域 \ 用户格式指定用户身份。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，则使用最近登录的 IP 地址，输出将显示存在更多 IP 地址到用户的映射。如果在此命令的源部分中指定了用户身份，则 ASA 会根据用户输入的目标地址类型搜索用户的 IPv4 或 IPv6 地址。

您可以在此命令的源部分中指定安全组名称或安全组标记。ASA 基于安全组名称或安全组标记搜索 IP 地址，并将其用于数据包跟踪测试。如果一个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，输出将显示存在更多 IP 地址到安全组标记的映射。

此命令支持 FQDN，这意味着您还可以将 FQDN 指定为源地址和目标地址。 ASA 首先执行 DNS 查找，然后检索第一个返回的 IP 地址来构建数据包。如果解析了多个 IP 地址，输出将显示存在更多 DNS 解析的 IP 地址。仅支持 IPv4 FQDN。

示例

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。结果表明隐含的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 CISCO\abc 的用户名跟踪从内部主机 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-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

以下示例显示如何使用 CISCO\abc 的用户名跟踪来自内部主机 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:
```

以下示例列出 **packet-tracer** 命令的输出，以展示安全组标记到 IP 地址的映射：

```
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 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

以下示例显示 **packet-tracer** 命令的输出以展示第 2 层 SGT 实施：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

相关命令

命令	说明
capture	捕捉数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕捉配置。

page style

要定制在 WebVPN 用户连接到安全设备时向其显示的 WebVPN 页面，请在 WebVPN 定制配置模式下使用 **page style** 命令。要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

page style *value*

[**no**] **page style** *value*

语法说明

value	级联样式表 (CSS) 参数 （最多 256 个字符）。

默认值

默认页面样式是 background-color:white;font-family:Arial,Helv,sans-serif

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

以下示例将页面样式定制为大型：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

相关命令

命令	说明
logo	定制 WebVPN 页面上的徽标。
title	定制 WebVPN 页面的标题

pager

要设置在 Telnet 会话中出现 “---More---” 提示符之前页面上的默认行数，请在全局配置模式下使用 **pager** 命令。

pager [**lines**] *lines*

语法说明

[**lines**] *lines*	设置在出现 “---More---” 提示符前页面上的行数。默认值为 24 行； 0 表示没有页面限制。范围为从 0 到 2147483647 行。 **lines** 关键字是可选的，有无此选项对命令无影响。

默认值

默认值为 24 行。

命令模式

下表显示可输入命令的模式：

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

命令历史

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。 **terminal pager** 命令已添加为特权 EXEC 模式命令。

使用指南

此命令更改 Telnet 会话的默认分页程序行设置。如果您要仅为当前会话暂时更改此设置，请使用 **terminal pager** 命令。

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

示例

以下示例将显示的行数更改为 20：

```
ciscoasa(config)# pager 20
```

相关命令

命令	说明
clear configure terminal	清除终端显示宽度设置。
show running-config terminal	显示当前终端设置。
terminal	允许系统日志消息显示在 Telnet 会话上。
terminal pager	设置在出现 “`---more---`” 提示符前要在 Telnet 会话中显示的行数。此命令不会保存到配置中。
terminal width	在全局配置模式中设置终端显示宽度。

parameters

要进入参数配置模式以设置检查策略映射的参数，请在策略映射配置模式下使用 **parameters** 命令。

parameters

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
策略映射配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

模块化策略框架 让您可以配置用于许多应用检查的特殊操作。使用第 3/4 层策略映射（**policy-map** 命令）中的 **inspect** 命令启用检查引擎时，您还可以选择性地启用在由 **policy-map type inspect** 命令创建的检查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 是检查策略映射的名称。

检查策略映射可支持一个或多个 **parameters** 命令。参数影响检查引擎的行为。参数配置模式中可用的命令取决于应用。

示例

以下示例显示如何在默认检查策略映射中设置 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
```

相关命令

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

participate

要强制设备参与虚拟负载平衡集群，请在 VPN 负载平衡配置模式下使用 **participate** 命令。要删除参与集群的设备，请使用此命令的 **no** 形式。

participate

no participate

语法说明

此命令没有任何参数或关键字。

默认值

默认行为是设备不参与 VPN 负载平衡集群。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **interface** 和 **nameif** 命令配置接口，然后使用 **vpn load-balancing** 命令进入 VPN 负载平衡模式。您还必须已事先使用 **cluster ip** 命令配置集群 IP 地址，并已配置虚拟集群 IP 地址指代的接口。

此命令可强制此设备参与虚拟负载平衡集群。您必须明确发出此命令来使设备参与集群。

参与集群的所有设备必须采用相同的集群特定值：IP 地址、加密设置、加密密钥和端口。

注　使用加密时，您必须已事先配置 **isakmp enable** *inside* 命令，其中 *inside* 特指接口内的负载平衡。如果未在接口内的负载平衡上启用 isakmp，则您在尝试配置集群加密时会收到错误消息。

如果在配置 **cluster encryption** 命令时已启用 isakmp，但在配置 **participate** 命令前禁用了它，则您在输入 **participate** 命令时会收到错误消息，且本地设备将不参与集群。

示例

以下是 VPN 负载平衡命令序列的示例，其中包括使当前设备参与 VPN 负载平衡集群的 **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
```

相关命令 ciscoasa

命令	说明
vpn load-balancing	进入 VPN 负载平衡模式。

passive-interface (RIP)

要在接口上禁用 RIP 路由更新传输，请在路由器配置模式下使用 **passive-interface** 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*}

语法说明

default	（可选）将所有接口设置为被动模式。
if_name	（可选）将指定的接口设置为被动模式。

默认值

启用 RIP 时，将为主动 RIP 启用所有接口。

如果未指定接口或 **default** 关键字，命令将默认为 **default**，然后将在配置中显示为 passive-interface default。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

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来填充路由表，但不广播路由更新。

示例

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可发送和接收 RIP 更新。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

相关命令

命令	说明
clear configure rip	清除正在运行的配置中的所有 RIP 命令。
router rip	启用 RIP 路由过程，然后进入 RIP 路由器配置模式。
show running-config rip	显示正在运行的配置中的 RIP 命令。

passive-interface (EIGRP)

要在接口上禁用发送和接收 EIGRP 路由更新，请在路由器配置模式下使用 **passive-interface** 命令。要在接口上重新启用路由更新，请使用此命令的 **no** 形式。

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

语法说明

default	（可选）将所有接口设置为被动模式。
if_name	（可选） **nameif** 命令指定的处于被动模式的接口的名称。

默认值

为该接口启用路由时，将为主动路由 （发送和接收路由更新）启用所有接口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	已增加对 EIGRP 路由的支持。

使用指南

在接口上启用被动路由。对于 EIGRP，这会在该接口上禁用传输和接收路由更新。

EIGRP 配置中可包含多个 **passive-interface** 命令。您可以使用 **passive-interface default** 命令在所有接口上禁用 EIGRP 路由，然后使用 **no passive-interface** 命令在特定接口上启用 EIGRP 路由。

示例

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可发送和接收 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外的所有接口设置为被动 EIGRP。仅内部接口将发送和接收 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
```

相关命令

命令	说明
show running-config router	显示正在运行的配置中的路由器配置命令。

passive-interface (OSPFv3)

要在一个接口上或在使用 OSPFv3 进程的所有接口上抑制路由更新的发送和接收，请在路由器配置模式下使用 **passive-interface** 命令。要在一个接口上或在使用 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*]

语法说明

interface_name　（可选）指定正运行 OSPFv3 进程的接口的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

此命令在接口上启用被动路由。

示例

以下示例在内部接口上抑制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)#
```

相关命令

命令	说明
show running-config router	显示正在运行的配置中的路由器配置命令。

passwd, password

要设置 Telnet 的登录密码，请在全局配置模式下使用 **passwd** 或 **password** 命令。要重置密码，请使用此命令的 **no** 形式。

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

语法说明

encrypted	（可选）指定密码采用加密形式。密码以加密形式保存在配置中，因此您在输入原始密码后无法查看原始密码。如果因某种原因需要将密码复制到另一个 ASA 中，但却不知道原始密码，则您可以输入带有加密密码和此关键字的 **passwd** 命令。一般情况下，仅当输入 **show running-config passwd** 命令时才会看到此关键字。
passwd | **password**	您可以输入任一命令；它们互为别名。
password	将密码设置为包含最多 80 个字符的区分大小写的字符串。密码不能包含空格。

默认值

9.1(1)：默认密码是 “cisco”。

9.1(2)：无默认行为或默认值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.4(2)	不再支持 SSH 默认用户名；您无法再使用 **pix** 或 **asa** 用户名和登录密码连接到使用 SSH 的 ASA。
9.0 (2)、 9.1(2)	默认密码 “cisco” 已删除；您必须主动设置登录密码。使用 **no passwd** 或 **clear configure passwd** 命令可删除密码；以前，此命令可将密码重置为默认的 “cisco”。

使用指南

使用 **telnet** 命令启用 Telnet 时，您可以使用由 **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。如果您使用 **aaa authentication telnet console** 命令配置 Telnet 的每用户 CLI 身份验证，则不会使用此密码。

此密码也可用于从交换机到 ASASM 的 Telnet 会话 （请参阅 **session** 命令）。

示例

以下示例将密码设置为 Pa$$w0rd：

```
ciscoasa(config)# passwd Pa$$w0rd
```

以下示例将密码设置为您从另一个 ASA 复制的加密密码：

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

相关命令

命令	说明
clear configure passwd	清除登录密码。
enable	进入特权 EXEC 模式。
enable password	设置启用密码。
show curpriv	显示当前登录的用户名和用户特权级别。
show running-config passwd	显示加密形式的登录密码。

password encryption aes

要启用密码加密，请在全局配置模式下使用 password encryption aes 命令。要禁用密码加密，请使用此命令的 **no** 形式。

password encryption aes

no password encryption aes

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。

使用指南

一旦开启密码加密且主口令可用时，所有用户密码都将得到加密。正在运行的配置将以加密格式显示密码。如果在启用密码加密时未配置口令，则命令会成功预测未来将存在口令。此命令将在故障切换对等设备之间自动同步。

如果丢失了主口令，先执行 **write erase** 命令再执行 **reload** 命令可删除主口令。

示例

以下示例启用密码加密：

```
Router (config)# password encryption aes
```

相关命令

命令	说明
key config-key password-encryption	设置用于生成加密密钥的口令。
write erase	执行此命令后再执行 **reload** 命令将删除丢失的主口令。

password (crypto ca trustpoint)

要指定在注册过程中向 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，请使用此命令的 **no** 形式。

password *string*

no password

语法说明

string	指定密码的名称作为字符字符串。第一个字符不能为数字。字符串可以包含任何字母数字字符，包括空格，最多为 80 个字符。您不能以 “数字 - 空格 - 任何字符 ” 格式指定密码。数字后有空格会导致问题。例如， “hello 21” 是合法的密码，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。

默认值

默认设置是不包括密码。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令让您可以在实际证书注册开始前指定证书的撤销密码。当更新的配置由 ASA 写入 NVRAM 中时，指定的密码会得到加密。

CA 通常使用质询短语来对后续撤销请求进行身份验证。

如果启用此命令，则在证书注册期间将不会提示您输入密码。

示例

以下示例进入中心信任点的 crypto ca trustpoint 配置模式，并包括在中心信任点的注册请求中向 CA 注册的质询短语：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

相关命令

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

password-management (tunnel-group general-attributes, config-mdm-proxy)

要启用密码管理，请在 tunnel-group general-attributes 配置模式和 config-mdm-proxy 模式下使用 **password-management** 命令。要禁用密码管理，请使用此命令的 **no** 形式。要将天数重置为默认值，请使用此命令带有指定的 **password-expire-in-days** 关键字的 **no** 形式。

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

语法说明

days	指定当前密码过期前的天数 （从 0 至 180）。如果您指定 **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当前密码过期前的天数，此时 ASA 开始警告用户密码即将过期。此选项仅对 LDAP 服务器有效。有关更多信息，请参阅 “ 使用说明 ” 部分。

默认值

默认为无密码管理。如果您没有为 LDAP 服务器指定 **password-expire-in-days** 关键字，则在当前密码过期前开始警告的默认时间长度是 14 天。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。
9.3(1)	此命令现已在 config-mdm-proxy 模式中可用。

使用指南

ASA 支持 RADIUS 和 LDAP 协议的密码管理。它仅对 LDAP 支持 “password-expire-in-days” 选项。

您可以为 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 在远程用户登录时通知用户的当前密码即将到期或已过期。然后， ASA 向用户提供机会来更改密码。如果当前密码尚未过期，用户仍可以使用该密码登录。

此命令对支持此类通知的 AAA 服务器有效，即对 LDAP 服务器的本地服务器和 NT 4.0 或 Active Directory 服务器的 RADIUS 代理服务器有效。如果尚未配置 RADIUS 或 LDAP 身份验证，则 ASA 会忽略此命令。

注　当前支持 MSCHAP 的某些 RADIUS 服务器不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此请联系您的供应商进行确认。

ASA （7.1 版及更高版本）在使用 LDAP 或任何支持 MS-CHAPv2 的 RADIUS 配置进行身份验证时，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 版及更高版本）
- IPsec VPN 客户端
- 无客户端 SSL VPN （ASA 软件 8.0 版及更高版本） WebVPN （ASA 软件 7.1 版至 7.2.x 版）
- SSL VPN 客户端全隧道客户端

这些 RADIUS 配置包括支持 LOCAL 身份验证的 RADIUS、具有 Active Directory/Kerberos Windows DC 的 RADIUS、具有 NT/4.0 域的 RADIUS 和支持 LDAP 的 RADIUS。

Kerberos/Active Directory （Windows 密码）或 NT 4.0 域的上述任何连接类型*不*支持密码管理。RADIUS 服务器（例如思科 ACS）可将身份验证请求由另一个身份验证服务器来代理。但是，从 ASA 角度来看，它仅与一个 RADIUS 服务器通信。

注　对于 LDAP，更改密码的方法取决于市场上不同的 LDAP 服务器。当前， ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。

本地 LDAP 需要 SSL 连接。在尝试为 LDAP 执行密码管理前，您必须启用通过 SSL 的 LDAP。默认情况下， LDAP 使用端口 636。

请注意，此命令不更改密码过期前的天数，而会更改 ASA 开始警告用户密码即将过期的过期前天数。

如果确实指定了 **password-expire-in-days** 关键字，则您还必须指定天数。

将天数设置为 0 表示禁用此命令。 ASA 不会通知用户密码即将过期，但用户可以在过期后更改密码。

注　RADIUS 不提供密码更改功能，也不提供密码更改提示。

示例

以下示例为 WebVPN 隧道组 “testgroup” 将开始警告用户密码即将过期的过期前天数设置为 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)#
```

以下示例为 IPsec 远程访问隧道组 “QAgroup” 使用默认值 - 开始警告用户密码即将过期的过期前 14 天：

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

以下示例显示使用默认密码过期设置的 MDM 代理：

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# password-managment
```

相关命令

命令	说明
clear configure passwd	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）。
show running-config passwd	显示加密形式的登录密码。
tunnel-group general-attributes	配置 tunnel-group general-attributes 值。
mdm-proxy	配置 MDM 代理。

password-parameter

要指定必须提交用户密码以供 SSO 身份验证时的 HTTP POST 请求参数的名称，请在 aaa-server-host 配置模式下使用 **password-parameter** 命令。这是带有 HTTP Forms 命令的 SSO。

password-parameter *string*

注　要正确配置带有 HTTP 的 SSO，您必须透彻地了解身份验证和 HTTP 交换的工作原理。

语法说明

string	HTTP POST 请求中包含的密码参数的名称。最大密码长度为 128 个字符。

默认值

无默认值或行为。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

ASA 的 WebVPN 服务器可使用 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。所需命令 **password-parameter** 可指定 POST 请求必须包括用于 SSO 身份验证的用户密码参数。

注　登录时，用户可输入实际密码值，该值将输入到 POST 请求中并被传递给身份验证 Web 服务器。

示例

以下示例指定名为 user_password 的密码参数 （在 aaa-server-host 配置模式中输入）：

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

相关命令

命令	说明
action-uri	指定要接收用于单点登录身份验证的用户名和密码的 Web 服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建用于与身份验证 Web 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	指定必须提交用户名以供 SSO 身份验证的 HTTP POST 请求参数的名称。

password-policy authenticate enable

要确定是否允许用户修改自己的用户帐户，请在全局配置模式下使用 **password-policy authenticate enable** 命令。要将相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

语法说明

此命令没有任何参数或关键字。

默认值

默认为禁用身份验证。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

如果启用身份验证， **username** 命令将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** 命令也不允许用户删除自己的帐户。

示例

以下示例显示如何使用户能够修改自己的用户帐户：

```
ciscoasa(config)# password-policy authenticate enable
```

相关命令

命令	说明
password-policy minimum-changes	设置新密码与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	设置密码可能具有的最少小写字符数。

password-policy lifetime

要设置当前情景的密码策略和密码过期后的天数间隔，请在全局配置模式下使用 **password-policy lifetime** 命令。要将相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 *value*

no password-policy lifetime *value*

语法说明

value	指定密码生存期。有效值范围为 0 到 65535 天。

默认值

默认生存期值为 0 天。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

密码具有指定的最长生存期。生存期间隔为 0 天表示本地用户密码永不过期。请注意，密码会在生存期过期后的第一天上午 12:00 过期。

示例

以下示例指定密码生存期值为 10 天：

```
ciscoasa(config)# password-policy lifetime 10
```

相关命令

命令	说明
password-policy minimum-changes	设置新密码与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	设置密码可能具有的最少小写字符数。

password-policy minimum-changes

要设置新密码与旧密码之间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。要将相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 *value*

no password-policy minimum-changes *value*

语法说明

value	指定新密码与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。

默认值

更改的字符数默认为 0。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

新密码必须包括当前密码中的至少 4 个字符更改，且仅当它们不出现在当前密码中的任何位置时才被视为更改。

示例

以下示例指定新密码与旧密码之间更改的最小字符数为 6 个字符：

```
ciscoasa(config)# password-policy minimum-changes 6
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期 （天数），经过此时间段后密码将过期。
password-policy minimum-length	设置密码的最小长度。
password-policy minimum-lowercase	设置密码包含的最小小写字符数。

password-policy minimum-length

要设置密码的最小长度，请在全局配置模式下使用 **password-policy minimum-length** 命令。要将相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 *value*

no password-policy minimum-length *value*

语法说明

value	指定密码的最小长度。有效值范围为 0 到 64 个字符。

默认值

默认最小长度是 0。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

如果最小长度小于其他任何最小属性 （更改字符、小写字符、大写字符、数字字符和特殊字符），则会出现错误消息，且最小长度不会更改。推荐的密码长度为 8 个字符。

示例

以下示例指定密码的最小字符数为 8：

```
ciscoasa(config)# password-policy minimum-length 8
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期值 （天数），经过此时间段后密码将过期。
password-policy minimum-changes	设置新密码与旧密码之间允许更改的最小字符数。
password-policy minimum-lowercase	设置密码可能具有的最少小写字符数。

password-policy minimum-lowercase

要设置密码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。要将相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 *value*

no password-policy minimum-lowercase *value*

语法说明

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。

默认值

最小小写字符数默认为 0，表示没有最小值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令设置密码包含的最少小写字符数。有效值范围为 0 到 64 个字符。

示例

以下示例指定密码包含的最少小写字符数为 6：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期值 （天数），经过此时间段后密码将过期。
password-policy minimum-changes	设置新密码与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

要设置密码包含的最小数字字符数，请在全局配置模式下使用 **password-policy minimum-numeric** 命令。要将相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 *value*

no password-policy minimum-numeric *value*

语法说明

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。

默认值

最小数字字符数默认为 0，表示没有最小值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令设置密码包含的最小数字字符数。有效值范围为 0 到 64 个字符。

示例

以下示例指定密码包含的最小数字字符数为 8：

```
ciscoasa(config)# password-policy minimum-numeric 8
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期值 （天数），经过此时间段后密码将过期。
password-policy minimum-changes	设置新密码与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。要将相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 *value*

no password-policy minimum-special *value*

语法说明

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。

默认值

最小特殊字符数默认为 0，表示没有最小值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令设置密码包含的最小特殊字符数。特殊字符包括以下字符：!、@、#、$、%、^、&、*、'(‘ 和 ‘)’。

示例

以下示例指定密码包含的最小特殊字符数为 2：

```
ciscoasa(config)# password-policy minimum-special 2
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期值 （天数），经过此时间段后密码将过期。
password-policy minimum-changes	设置新密码与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

要设置密码包含的最小大写字符数，请在全局配置模式下使用 **password-policy minimum-uppercase** 命令。要将相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 *value*

no password-policy minimum-uppercase *value*

语法说明

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。

默认值

最小大写字符数默认为 0，表示没有最小值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

此命令设置密码包含的最小大写字符数。有效值范围为 0 到 64 个字符。

示例

以下示例指定密码包含的最小大写字符数为 4：

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

相关命令

命令	说明
password-policy lifetime	设置密码生存期值 （天数），经过此时间段后密码将过期。
password-policy minimum-changes	设置新密码与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-prompt

要定制在 WebVPN 用户连接到安全设备时向其显示的 WebVPN 页面登录框的密码提示，请在 WebVPN 定制模式下使用 **password-prompt** 命令：

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

要从配置中删除该命令并使值得到继承，请使用此命令的 **no** 形式。

语法说明

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

默认值

密码提示的默认文本是 “PASSWORD:”。

密码提示的默认样式是 color:black;font-weight:bold;text-align:right。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

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

以下是对 WebVPN 页面进行最常见更改 （页面颜色）的一些技巧：

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

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

示例

在以下示例中，文本更改为 “Corporate Password:”，且默认样式因字体增粗也发生更改：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# password-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# password-prompt style font-weight:bolder
```

相关命令

命令	说明
group-prompt	定制 WebVPN 页面的组提示
username-prompt	定制 WebVPN 页面的用户名提示

password-storage

要让用户将其登录密码存储在客户端系统上，请在组策略配置模式或用户名配置模式下使用 **password-storage enable** 命令。要禁用密码存储，请使用 **password-storage disable** 命令。

要删除正在运行的配置中的密码存储属性，请使用此命令的 **no** 形式。这样可实现从另一个组策略继承用于密码存储的值。

password-storage {**enable** | **disable**}

no password-storage

语法说明

disable	禁用密码存储。
enable	启用密码存储。

默认值

已禁用密码存储。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

仅在您视为安全站点的系统上启用密码存储。

此命令对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没有影响。

示例

以下示例显示如何对名为 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-id-validate

要指定是否使用对等设备的证书验证对等设备的身份，请在 tunnel-group ipsec-attributes 模式下使用 **peer-id-validate** 命令。要恢复默认值，请使用此命令的 **no** 形式。

peer-id-validate *option*

no peer-id-validate

语法说明

option	指定以下选项之一： • **req**：必需 • **cert**：如果受证书支持 • **nocheck**：不检查

默认值

此命令的默认设置是 **req**。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
隧道组 ipsec 属性	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以将此属性应用于所有 IPsec 隧道组类型。

示例

以下示例在 config-ipsec 配置模式中输入，它需要对名为 209.165.200.225 的 IPsec 局域网到局域网隧道组使用对等设备证书的身份来验证对等设备的身份：

```
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)#
```

相关命令

命令	说明
clear-configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	为此组配置隧道组 IPsec 属性。

perfmon

要显示性能信息，请在特权 EXEC 模式下使用 **perfmon** 命令。

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail]*

语法说明

verbose	在 ASA 控制台上显示性能监控信息。
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，以及它是安静模式还是详细模式。
detail	显示有关性能的详细信息。

默认值

seconds 为 120 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0	ASA 已引入对此命令的支持。
7.2(1)	已增加对 **detail** 关键字的支持。

使用指南

perfmon 命令允许您监控 ASA 的性能。使用 **show perfmon** 命令可立即显示该信息。使用 **perfmon verbose** 命令可每 2 分钟持续显示该信息。结合使用 **perfmon verbose** 命令和 **perfmon interval** *seconds* 命令可按照您指定的秒数间隔持续显示该信息。

如下所示为性能信息的示例：

性能统计信息：	当前	平均
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

以上信息列出了每秒发生的转换数、连接数、 Websense 请求数、地址转换（称为“修复”）数和 AAA 事务数。

示例

以下示例显示如何在 ASA 控制台上每隔 30 秒显示性能监控统计信息：

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

相关命令

命令	说明
show perfmon	显示性能信息。

periodic

要为支持时间范围的功能指定经常性（每周）时间范围，请在时间范围配置模式下使用 **periodic** 命令。要禁用，请使用此命令的 **no** 形式。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

语法说明

days-of-the-week	（可选）此参数首次出现的时间是关联的时间范围生效的开始时间或周内某日。第二次出现的时间是关联的时间范围生效的结束时间或周内某日。 此参数是任何一天或周内某几日的组合：周一、周二、周三、周四、周五、周六和周日。其他可能的值是： • 每日 - 周一至周日 • 工作日 - 周一至周五 • 周末 - 周六和周日 如果周的结束日与周的开始日相同，则您可以忽略它们。
time	以 HH:MM 格式指定时间。例如， 8:00 是上午 8:00，20:00 是下午 8:00。
to	需要输入 **to** 关键字来填写 “ 从开始时间到结束时间 ” 的范围。

默认值

如果不使用 **periodic** 命令输入值，则使用 **time-range** 命令定义的对 ASA 的访问将立即生效并将始终有效。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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

periodic 命令是指定时间范围何时生效的一种方式。另一种方式是使用 **absolute** 命令指定绝对时间段。在用于指定时间范围的名称的 **time-range** 全局配置命令后可使用上述命令之一。每个 **time-range** 命令允许多次输入 **periodic**。

如果周的结束日值与开始值相同，则您可以忽略它们。

如果 **time-range** 命令同时指定了 **absolute** 值和 **periodic** 值，则仅在达到 **absolute start** 时间后才会对 **periodic** 命令进行评估，且在达到 **absolute end** 时间后不再进一步对该命令进行评估。

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

示例

下面是一些示例：

如果要设置以下时间范围：	请输入：
周一至周五，仅上午 8:00 至下午 6:00 的时段	**periodic weekdays 8:00 to 18:00**
周内每日，仅上午 8:00 至下午 6:00 的时段	**periodic daily 8:00 to 18:00**
周一上午 8:00 至周五下午 8:00 的每一分钟	**periodic monday 8:00 to friday 20:00**
所有周末，周六早上至周日晚上	**periodic weekend 00:00 to 23:59**
周六和周日，中午至午夜	**periodic weekend 12:00 to 23:59**

以下示例显示如何允许访问 ASA （周一至周五，仅上午 8:00 至下午 6:00 ）：

```
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访问 ASA （在特定日，即周一、周二和周五，上午 10:30 至下午 12:30）：

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

相关命令

命令	说明
absolute	定义时间范围生效的绝对时间。
access-list extended	配置允许或拒绝 IP 流量通过 ASA 的策略。
default	恢复 **time-range** 命令 **absolute** 和 **periodic** 关键字的默认设置。
time-range	定义对 ASA 基于时间的访问控制。

permit errors

要允许无效 GTP 数据包或因解析失败而被丢弃的其他数据包通过，请在 GTP 映射配置模式 （可通过使用 **gtp-map** 命令访问）下使用 **permit errors** 命令。要恢复默认行为，即丢弃所有无效数据包或解析失败的数据包，请使用此命令的 **no** 形式。

permit errors

no permit errors

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下，丢弃所有无效数据包或解析失败的数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在 GTP 映射配置模式下使用 **permit errors** 命令可允许通过 ASA 发送（而非丢弃）无效的或在消息检测期间出错的任何数据包。

示例

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：

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# permit errors
```

相关命令

命令	说明
clear service-policy inspect gtp	清除全局 GTP 统计信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的特定 GTP 映射。
permit response	支持负载平衡 GSN。
show service-policy inspect gtp	显示 GTP 配置。

permit response

要支持负载平衡 GSN，请在 GTP 映射配置模式（可通过使用 **gtp-map** 命令访问）下使用 **permit response** 命令。使用此命令的 **no** 形式可允许 ASA 丢弃来自 GSN 的 GTP 响应（接收请求的主机除外）。

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

语法说明

from-object-group *from_obj_group_id*	指定使用 **object-group** 命令配置的对象组的名称，其中该对象组可将响应发送给由 *to_obj_group_id* 参数指定的对象组中的 GSN 集。 ASA 仅支持包含具有 IPv4 地址的网络对象的对象组。GTP 当前不支持 IPv6 地址。
to-object-group *to_obj_group_id*	指定使用 **object-group** 命令配置的对象组的名称，其中该对象组可接收来自由 *from_obj_group_id* 参数指定的对象组中的 GSN 集的响应。 ASA 仅支持包含具有 IPv4 地址的网络对象的对象组。GTP 当前不支持 IPv6 地址。

默认值

默认情况下， ASA 会丢弃来自 GSN 的 GTP 响应 （接收请求的主机除外）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(4)	引入了此命令。

使用指南

在 GTP 映射配置模式下使用 **permit response** 命令可支持负载平衡 GSN。**permit response** 命令配置 GTP 映射以允许来自不同 GSN （即不同于接收响应的 GSN）的 GTP 响应。

您可以将负载平衡 GSN 池标识为网络对象。同样，您也可以将 SGSN 标识为网络对象。如果做出响应的 GSN 与接收 GTP 请求的 GSN 同属一个对象组，且 SGSN 位于允许做出响应的 GSN 向其发送 GTP 响应的对象组中，则 ASA 将允许该响应。

示例

以下示例允许 192.168.32.0 网络上的任何主机发往 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)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

相关命令

命令	说明
clear service-policy inspect gtp	清除全局 GTP 统计信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的特定 GTP 映射。
permit errors	允许无效 GTP 数据包。
show service-policy inspect gtp	显示 GTP 配置。

pfs

要启用 PFS，请在组策略配置模式下使用 **pfs enable** 命令。要禁用 PFS，请使用 **pfs disable** 命令。要从正在运行的配置中删除 PFS 属性，请使用此命令的 **no** 形式。

pfs {**enable** | **disable**}

no pfs

语法说明

disable	禁用 PFS。
enable	启用 PFS。

默认值

PFS 已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

VPN 客户端和 ASA 上的 PFS 设置必须匹配。

使用此命令的 **no** 形式可允许从另一个组策略继承用于 PFS 的值。

在 IPsec 协商中， PFS 可确保每个新加密密钥与任何以前的密钥均无关。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置 PFS：

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

phone-proxy

要配置电话代理实例，请在全局配置模式下使用 **phone-proxy** 命令。

要删除电话代理实例，请使用此命令的 **no** 形式。

phone-proxy *phone_proxy_name*

no phone-proxy *phone_proxy_name*

语法说明

phone_proxy_name	指定电话代理实例的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

在 ASA 上仅能配置一个电话代理实例。

如果已为 HTTP 代理服务器配置 NAT，则与 IP 电话相关的 HTTP 代理服务器的全局 IP 地址或映射的 IP 地址将写入电话代理配置文件中。

示例

以下示例显示使用 **phone-proxy** 命令来配置电话代理实例：

```
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
```

相关命令

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

pim

要在接口上重新启用 PIM，请在接口配置模式下使用 **pim** 命令。要禁用 PIM，请使用此命令的 **no** 形式。

pim

no pim

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下， **multicast-routing** 命令在所有接口上启用 PIM。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

默认情况下， **multicast-routing** 命令在所有接口上启用 PIM。仅 **pim** 命令的 **no** 形式保存在配置中。

注 PIM 不受 PAT 支持。 PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。

示例

以下示例在选定接口上禁用 PIM：

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

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim accept-register

要配置 ASA 来过滤 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，请使用此命令的 **no** 形式。

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

语法说明

list *acl*	指定一个访问列表名称或端口号。在使用此命令时仅使用扩展主机 ACL。
route-map *map-name*	指定路由映射名称。在引用的路由映射中使用扩展主机 ACL。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令用于防止未经授权的来源向 RP 进行注册。如果未经授权的来源向 RP 发送了注册消息，则 ASA 会立即返回注册停止消息。

示例

以下示例将 PIM 注册消息的接收对象限制为从名为 “no-ssm-range” 的访问列表中定义的来源：

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim bidir-neighbor-filter

要控制哪些支持双向功能邻居可参与 DF 选定，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 **no** 形式。

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

语法说明

acl	指定一个访问列表名称或端口号。访问列表定义可参与双向 DF 选定的邻居。此命令仅使用标准 ACL，不支持扩展的 ACL。

默认值

所有路由器均被视为具有双向功能。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

双向 PIM 允许组播路由器保持减少的状态信息。网段中的所有组播路由器都必须已双向启用双向功能来选定 DF。

pim bidir-neighbor-filter 命令可通过让您指定应参与 DF 选定的路由器，同时仍允许所有路由器参与解析模式域，来实现从仅解析模式网络到双向网络的过渡。已启用双向功能的路由器可从它们自身中选择 DF，即使网段上存在非双向路由器。非双向路由器上的组播边界可防止 PIM 消息和来自双向组的数据漏入双向子集云或从中外泄。

启用 **pim bidir-neighbor-filter** 命令后， ACL 允许的路由器将被视为具有双向功能。因此：

- 如果允许的邻居不支持双向功能，则不发生 DF 选定。
- 如果拒绝的邻居支持双向功能，则不发生 DF 选定。
- 如果拒绝的邻居不支持双向功能，则可能发生 DF 选定。

示例

以下示例允许 10.1.1.1 成为 PIM 双向邻居：

```
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
```

相关命令

命令	说明
multicast boundary	定义管理范围内的组播地址的组播边界。
multicast-routing	在 ASA 上启用组播路由。

pim dr-priority

要在 ASA 上配置用于指定路由器选定的邻居优先级，请在接口配置模式下使用 **pim dr-priority** 命令。要恢复默认优先级，请使用此命令的 **no** 形式。

pim dr-priority *number*

no pim dr-priority

语法说明

number	从 0 至 4294967294 的一个数字。在确定指定的路由器时，此数字可用于确定设备的优先级。指定 0 可以防止 ASA 成为指定的路由器。

默认值

默认值为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在接口上具有最大优先级值的设备会成为 PIM 指定路由器。如果多个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。如果设备在问候消息中不包括 DR-Priority（DR 优先级）选项，则它将被视为具有最高优先级的设备，并将成为指定的路由器。如果多个设备未在其问候消息中包括此选项，则具有最高 IP 地址的设备将成为指定的路由器。

示例

以下示例将接口的 DR 优先级设置为 5：

```
ciscoasa(config-if)# pim dr-priority 5
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim hello-interval

要配置 PIM 问候消息的频率，请在接口配置模式下使用 **pim hello-interval** 命令。要将问候间隔恢复为默认值，请使用此命令的 **no** 形式。

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

语法说明

seconds	发送问候消息前 ASA 等待的秒数。有效值范围为 1 到 3600 秒。默认值为 30 秒。

默认值

默认间隔为 30 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例将 PIM 问候间隔设置为 1 分钟：

```
ciscoasa(config-if)# pim hello-interval 60
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim join-prune-interval

要配置 PIM 联接 / 修剪间隔，请在接口配置模式下使用 **pim join-prune-interval** 命令。要将间隔恢复为默认值，请使用此命令的 **no** 形式。

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

语法说明

seconds	发送联接 / 修剪消息前 ASA 等待的秒数。有效值范围为 10 到 600 秒。60 秒是默认值。

默认值

默认间隔为 60 秒

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例将 PIM 联接 / 修剪间隔设置为 2 分钟：

```
ciscoasa(config-if)# pim join-prune-interval 120
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim neighbor-filter

要控制哪些相邻路由器可参与 PIM，请在接口配置模式下使用 **pim neighbor-filter** 命令。要删除过滤，请使用此命令的 **no** 形式。

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

语法说明

acl	指定一个访问列表名称或端口号。此命令仅使用标准 ACL，不支持扩展的 ACL。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令定义哪些相邻路由器可参与 PIM。如果此命令不存在于配置中，则没有任何限制。

必须为此命令启用组播路由和 PIM，此命令才会出现在配置中。如果您禁用了组播路由，则此命令将从配置中删除。

示例

以下示例允许 IP 地址为 10.1.1.1 的路由器成为 GigabitEthernet0/2 接口上的 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
```

相关命令

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集合点 (RP) 上允许向后兼容性，请在全局配置模式下使用 **pim old-register-checksum** 命令。要生成符合 PIM RFC 的注册，请使用此命令的 **no** 形式。

pim old-register-checksum

no pim old-register-checksum

语法说明

此命令没有任何参数或关键字。

默认值

ASA 生成符合 PIM RFC 的注册。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 软件接受带有 PIM 报头校验和的注册消息和接下来的仅 4 个字节，而非使用思科 IOS 方法，后者接受带有所有 PIM 消息类型的 PIM 消息的注册消息。**pim old-register-checksum** 命令可生成与思科 IOS 软件兼容的注册。

示例

以下示例配置 ASA 来使用旧校验和计算：

```
ciscoasa(config)# pim old-register-checksum
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim rp-address

要配置 PIM 集合点 (RP) 的地址，请在全局配置模式下使用 **pim rp-address** 命令。要删除 RP 地址，请使用此命令的 **no** 形式。

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

语法说明

acl	（可选）定义在使用 RP 时应一起使用哪些组播组的标准访问列表的名称或编号。请不要在使用此命令时一起使用主机 ACL。
bidir	（可选）表示指定的组播组将在双向模式下运行。如果未使用此选项配置命令，则指定的组将在 PIM 解析模式下运行。
ip_address	要成为 PIM RP 的路由器的 IP 地址。这是采用四点分十进制记数法的单播 IP 地址。

默认值

未配置 PIM RP 地址。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

常见 PIM 解析模式 (PIM-SM) 或双向域中的所有路由器都需要了解众所周知的 PIM RP 地址。使用此命令可静态配置该地址。

注　ASA 不支持自动 RP；您必须使用 **pim rp-address** 命令指定 RP 地址。

您可以配置单个 RP 来支持多个组。访问列表中指定的组范围确定 PIM RP 组映射。如果未指定访问列表，则组的 RP 将应用于整个 IP 组播组范围 (224.0.0.0/4)。

注　无论实际双向配置如何， ASA 始终在 PIM 问候消息中通告双向功能。

示例

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
```

相关命令

命令	说明
pim accept-register	配置用于过滤 PIM 注册消息的候选 RP。

pim spt-threshold infinity

要将最后一个跃点路由器的行为更改为始终使用共享树而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，请使用此命令的 **no** 形式。

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

语法说明

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。

默认值

默认情况下，最后一个跃点 PIM 路由器会切换到最短路径源树。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果未使用 **group-list** 关键字，则此命令应用于所有组播组。

示例

以下示例使最后一个跃点 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
```

相关命令

命令	说明
multicast-routing	在 ASA 上启用组播路由。

ping

要测试从指定接口到某 IP 地址的连接性，请在特权 EXEC 模式下使用 **ping** 命令。与 TCP ping 相比，对基于 ICMP 的常规 ping 可用的参数会有所不同。输入不带参数的命令以提示输入值，其中包括无法用作参数的特征。

ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

ping tcp [*if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]

ping

注　只有通过 **tcp** 选项才可使用 **source** 和 *port* 选项；通过 **tcp** 选项无法使用 **data**、**size** 和 **validate** 选项。

语法说明

data *pattern*	（可选，仅适用于 ICMP）指定采用十六进制格式的 16 位数据模式，从 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，您可以指定 IPv6 地址 （TCP ping 不支持）。 当使用主机名时，名称可以是 DNS 名称或使用 **name** 命令分配的名称。DNS 名称的最大字符数是 128，使用 **name** 命令创建的名称的最大字符数是 63。您必须配置 DNS 服务器来使用 DNS 名称。
if_name	（可选）对于 ICMP，这是接口名称 （按照 **nameif** 命令的配置），通过它可访问 *host*。如果不提供，则 *host* 将解析为 IP 地址，并会参考路由表来确定目标接口。对于 TCP，这是来源用来发送 SYN 数据包的输入接口。
port	（仅适用于 TCP）为您正在 ping 的主机指定 TCP 端口号 (1-65535)。
repeat *count*	（可选）指定重复 ping 请求的次数。默认值为 5。
size *bytes*	（可选，仅适用于 ICMP）以字节为单位指定数据报大小。默认值为 100。
source *host port*	（可选，仅适用于 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）。
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。
timeout *seconds*	（可选）指定超时间隔的秒数。默认值为 2 秒。
validate	（可选，仅适用于 ICMP）验证应答数据。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	已增加对 DNS 名称的支持。
8.4(1)	添加了 **tcp** 选项。

使用指南

ping 命令使您能够确定 ASA 是否已连接或某主机在网络上是否可用。

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 （如果不使用 ICMP 规则，则允许所有 ICMP 流量）。如果您要内部主机通过 ICMP 来 ping 外部主机，您必须执行以下操作之一：

- 为响应应答创建 ICMP **access-list** 命令；例如，要通过 ping 访问所有主机，请使用 **access-list acl_grp permit icmp any any** 命令，并将 **access-list** 命令与您要使用 **access-group** 命令进行测试的接口进行绑定。
- 使用 **inspect icmp** 命令配置 ICMP 检查引擎。例如，若将 **inspect icmp** 命令添加到全局服务策略的 **class default_inspection** 类中，则允许对内部主机发起的响应请求做出的响应应答通过 ASA。

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，以允许 ASA 响应和接受通过 **ping** 命令生成的消息。 **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)
```

使用 **show interface** 命令可确保 ASA 连接到网络并正在传递流量。指定的 *if_name* 的地址用作 ping 的源地址。

您也可以通过输入不带参数的 **ping** 来执行扩展 ping。您会收到输入参数的提示，其中包括一些无法作为关键字使用的特征。

示例

以下示例显示如何确定其他 IP 地址是否通过 ASA 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
```

以下是 **ping tcp** 命令的示例：

```
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
```

相关命令

命令	说明
icmp	为在接口上终止的 ICMP 流量配置访问规则。
show interface	显示有关 VLAN 配置的信息。

第 16 章

police 至 pppoe client secondary 命令

police

要将服务质量 (QoS) 管制应用于类映射中，请在类配置模式下使用 **police** 命令。要删除速率限制要求，请使用此命令的 **no** 形式。管制是一种确保流量不超过您配置的最大速率 （以位 / 秒为单位）的方法，进而可确保流量不会占用整个资源。当流量超过最大速率时， ASA 会丢弃超额流量。管制也会设置允许的最大单次突发流量。

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

no police

语法说明

conform-burst	在限制为符合速率值前，指定在持续突发中允许的最大瞬时字节数 （在 1000 和 512000000 字节之间）。
conform-action	设置当速率小于 *conform_burst* 值时要采取的操作。
conform-rate	设置此流量的速率限制；在 8000 和 2000000000 位 / 秒之间。
drop	丢弃数据包。
exceed-action	设置当速率介于 *conform-rate* 值与 *conform-burst* 值之间时要采取的操作。
input	启用输入方向的流量管制。
output	启用输出方向的流量管制。
transmit	传输数据包。

默认值

没有默认行为或变量。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	添加了 **input** 选项。现在支持入站方向的流量管制。

使用指南

要启用管制，请使用 Modular Policy Framework （模块化策略框架）：

1. **class-map** - 标识您要对其执行管制的流量。
2. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **police** - 为类映射启用管制。
3. **service-policy** - 向接口分配策略映射或全局分配策略映射。

注　**police** 命令仅执行最大速率和突发速率，强制它们达到符合速率值。如果指定了 **conform-action** 或 **exceed-action**，该命令不会执行它们。

注　省略 conform-burst 参数时，默认值将设定为以字节为单位的符合速率的 1/32 （即符合速率为 100,000 时，默认的符合突发值为 100,000/32 = 3,125）。请注意，符合速率以位 / 秒为单位，而符合突发以字节为单位。

如果需要，您可以为 ASA 单独配置每个服务质量功能。但是，您通常可在 ASA 上配置多个服务质量功能，以便设置一些流量的优先级 （示例），并阻止其他流量引发带宽问题。

请参阅以下对每个接口支持的功能组合：

- 标准优先级队列 （用于特定流量） + 管制 （用于其余流量）。

  您无法配置同一流量集的优先级队列和管制。
- 流量整形 （用于接口上的所有流量） + 分层优先级队列 （用于流量的子集）。

通常，如果启用流量整形，则您无需再为同一流量启用管制，不过 ASA 不会限制您进行此配置。

请参阅以下指南：

- 服务质量需单向应用；仅进入您对其应用策略映射的接口 （或退出接口，具体取决于您指定了 **input** 还是 **output**）的流量会受到影响。
- 如果在已建立现有流量的接口中已应用或删除服务策略，则不会在流量流中应用或删除服务质量策略。要应用或删除此类连接的服务质量策略，您必须清除连接，然后重新建立它们。请参阅 **clear conn** 命令。
- 不支持 to-the-box 流量 （传入的所有流量）。
- 不支持到达和来自 VPN 隧道旁路接口的流量。
- 在与隧道组类映射进行匹配时，仅支持出站管制。

示例

以下是输出方向的 **police** 命令的示例，它将符合速率设置为 100,000 位 / 秒，突发值为 20,000 字节，并指定将丢弃超过突发速率的流量：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass
ciscoasa(config-pmap-c)# police output 100000 20000 exceed-action drop
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

以下示例显示如何对以内部 Web 服务器为目标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)#
```

相关命令

class	指定用于流量分类的类映射。
clear configure policy-map	删除所有策略映射配置，除非策略映射正在 service-policy 命令中使用，才可不删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config policy-map	显示所有当前策略映射配置。

policy

要指定检索 CRL 的来源，请在 ca-crl 配置模式下使用 **policy** 命令。

policy {**static** | **cdp** | **both**}

语法说明

both	指定如果使用 CRL 分发点获取 CRL 失败，则使用静态 CDP 重试最多五次。
cdp	使用在经受检查的证书中嵌入的 CDP 扩展。在这种情况下，ASA 可从正在验证的证书的 CDP 扩展中检索多达五个 CRL 分发点，如有必要，还可增加它们所含配置的默认值的信息。如果 ASA 尝试使用主要 CDP 检索 CRL 失败，则它会使用列表中的下一个可用 CDP 进行重试。此过程会持续，直到 ASA 检索到 CRL 或列表中的 CDP 全部试完。
static	使用最多五个静态 CRL 分发点。如果指定此选项，请也使用 **protocol** 命令指定 LDAP 或 HTTP URL。

默认值

默认设置为 **cdp**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入 ca-crl 配置模式，然后使用经受检查的证书中的 CRL 分发点扩展配置要发生的 CRL 检索，如果检索失败则使用静态 CDP：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

相关命令

命令	说明
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
url	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，请使用此命令的 **no** 形式。

policy-list *policy-list-name* {**permit** | **deny**}

no policy-list *policy-list-name*

语法说明

policy-list-name	配置的策略列表的名称。
permit	允许访问匹配条件。
deny	拒绝访问匹配条件。

默认值

默认情况下，此命令未启用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

当在路由映射中引用策略列表时，策略列表中的所有匹配语句均可得到评估和处理。使用一个路由映射可配置两个或更多策略列表。使用 AND 语义或 OR 语义可评估路由映射中配置的策略列表。策略列表也可与在同一路由映射中（位于策略列表以外）配置的任何其他先前存在的匹配和设置语句共存。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。

此处列出了 **policy-list** 子命令：

子命令	详细信息
match **as-path [path-list-number]**	与 as-path 进行匹配，这可能需要多个 as-path 路径列表数字
Match community [community-name] [exact-match]	社区名称是必填项， exact-match 是可选项。可提供多个名称
Match interface [interface-name]	可使用多个接口名称
match **metric <0-4294967295>**	可使用多个数字
Match ip address [acl name | prefix-list [prefix-listname]]	可提供用于 acl 和 prefix-list 的多个名称，但一个名称无法与其他名称共存，即任一策略列表均可具有前缀列表或 acl
Match ip next-hop [acl name | prefix-list [prefix-listname]]	可提供用于 acl 和 prefix-list 的多个名称，但一个名称无法与其他名称共存，即任一策略列表均可具有前缀列表或 acl
Match ip route-source [acl name | prefix-list [prefix-listname]]	可提供用于 acl 和 prefix-list 的多个名称，但一个名称无法与其他名称共存，即任一策略列表均可具有前缀列表或 acl
Default match	默认在 “match” （匹配）下具有上述所有选项
Help	后续命令的帮助
No	命令的否定形式
Exit	退出策略映射模式

示例

以下示例中，策略列表配置为允许与 AS 1 和 metric 10 相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
```

以下示例中，策略列表配置为允许与 community 20 和 metric 10 相匹配的流量：

```
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
```

以下示例中，策略列表配置为拒绝与 community 20 和 metric 10 相匹配的流量：

```
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，通过在全局配置模式下使用 **policy-map** 命令 （无 **type** 关键字），将操作分配给您使用第 3/4 层类映射 （**class-map** 或 **class-map type management** 命令）标识的流量。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*

语法说明

name	指定此策略映射的名称 （长度最多为 40 个字符）。所有类型的策略映射都使用同一命名空间，因此您无法重新使用另一类型的策略映射已使用的名称。

默认值

默认情况下，配置中包括与所有默认应用检查流量进行匹配的策略，并会将某些检查应用于所有接口上的流量中 （全局策略）。并非所有检查均已默认启用。您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。（接口策略可覆盖全局策略来实现特定功能。）

默认策略包括以下应用检查：

- 对最大报文长度为 512 字节的 DNS 检查
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP 选项

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
```

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

配置模块化策略框架包含四项任务：

1. 使用 **class-map** 或 **class-map type management** 命令标识您要对其应用操作的第 3 层和第 4 层流量。
2. （仅适用于应用检查）使用 **policy-map type inspect** 命令定义应用检查流量的特殊操作。
3. 使用 **policy-map** 命令将操作应用到第 3 层和第 4 层流量。
4. 使用 **service-policy** 命令在接口上激活操作。

最大策略映射数为 64，但是每个接口仅能应用一个策略映射。您可以将同一策略映射应用于多个接口。您可以标识第 3/4 层策略映射中的多个第 3/4 层类映射 （请参阅 **class** 命令），还可以将来自一个或更多功能类型的多个操作分配给每个类映射。

示例

以下是用于连接策略的 **policy-map** 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的工作原理：

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

以下示例显示流量如何与第一个可用的类映射进行匹配，且不与在同一功能域中指定操作的任何后续类映射进行匹配：

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

启动 Telnet 连接时，它会与 **class telnet_traffic** 进行匹配。同样，如果启动 FTP 连接，则它会与 **class ftp_traffic** 进行匹配。对于除 Telnet 和 FTP 外的任何 TCP 连接，它将与 **class tcp_traffic** 进行匹配。即使 Telnet 或 FTP 连接可与 **class tcp_traffic** 进行匹配， ASA 也不会执行此匹配，因为它们之前已与其他类进行匹配。

NetFlow 事件通过模块化策略框架配置。如果模块化策略框架未针对 NetFlow 进行配置，则不会记录任何事件。流量根据配置类的顺序进行匹配。检测到匹配后，将不会检查其他任何类。对于 NetFlow 事件，配置要求如下：

- 流导出目标 （即 NetFlow 收集器）的唯一标识是其 IP 地址。
- 支持的事件类型有 flow-create、 flow-teardown、 flow-denied、 flow-update 等，其中包括之前已列出的四个事件类型。
- 使用 **flow-export event-type {all | flow-create | flow-denied | flow-update | flow-teardown} destination** 命令可配置 NetFlow 收集器和过滤器的地址，用于确定应向每个收集器发送哪些 NetFlow 记录。
- 接口策略中不支持流导出操作。
- 仅在 **class-default** 命令和使用 **match any** 或 **match access-list** 命令的类中支持流导出操作。
- 如果未定义 NetFlow 收集器，则不会发生配置操作。
- NetFlow 安全事件日志过滤与顺序无关。

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 中。

```
ciscoasa(config)# access-list flow_export_acl permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 15.1.1.1
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
clear configure policy-map	删除所有策略映射配置。如果策略映射正在 **service-policy** 命令中使用，则不删除该策略映射。
class-map	定义流量类映射。
service-policy	向接口分配策略映射或向所有接口全局分配策略映射。
show running-config policy-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** 命令来定义用于检查应用流量的特殊操作。要删除检查策略映射，请使用此命令的 **no** 形式。

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

语法说明

application	指定您要对其采取操作的应用流量的类型。可用的类型包括： • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **ip-options** • **ipsec-pass-thru** • **ipv6** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **scansafe** • **sip** • **skinny** • **snmp**
policy_map_name	指定此策略映射的名称 （长度最多为 40 个字符）。以 “_internal” 或 “_default” 开始的名称会保留且无法使用。所有类型的策略映射都使用同一命名空间，因此您无法重新使用另一类型的策略映射已使用的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.2(1)	添加了 **ipv6** 关键字来支持 IPv6 检查。
9.0(1)	添加了 **scansafe** 关键字来支持云网络安全。

使用指南

模块化策略框架 让您可以配置用于许多应用检查的特殊操作。使用第 3/4 层策略映射（**policy-map** 命令）中的 **inspect** 命令启用检查引擎时，您还可以选择性地启用在由 **policy-map type inspect** 命令创建的检查策略映射中定义的操作。例如，当 http_policy_map 是检查策略映射的名称时，输入 **inspect http http_policy_map** 命令。

一个检查策略映射包括在策略映射配置模式中输入的一个或多个以下命令。检查策略映射可用的确切命令取决于应用。

- **match** 命令 - 您可以在检查策略映射中直接定义 **match** 命令，以将应用流量与特定于应用的标准 （例如 URL 字符串）进行匹配。然后，您可在匹配配置模式 （例如 **drop**、 **reset**、 **log** 等）中启用操作。可用的 **match** 命令取决于应用。
- **class** 命令 - 此命令可标识策略映射中的检查类映射（请参阅 **class-map type inspect** 命令来创建检查类映射）。检查类映射包括将应用流量与特定于该应用的标准 （例如 URL 字符串）进行匹配的 **match** 命令，然后您可在策略映射中启用对其的操作。创建类映射与在检查策略映射中直接使用 **match** 命令之间的区别在于，您可以将多个匹配集合在一起，还可以重新使用类映射。
- **parameters** 命令 - 参数影响检查引擎的行为。参数配置模式中可用的命令取决于应用。

您可以在一个策略映射中指定多个 **class** 或 **match** 命令。

一些 **match** 命令可以指定与数据包中的文本匹配的正则表达式。请参阅 **regex** 命令和 **class-map type regex** 命令，它们可将多个正则表达式集合在一起。

默认检查策略映射配置包括以下命令：

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

如果一个数据包与多个不同的 **match** 或 **class** 命令匹配，则 ASA 应用操作的顺序取决于内部 ASA 规则而非将它们添加到策略映射中的顺序。内部规则由应用类型和解析数据包的逻辑过程确定，且用户无法对其进行配置。例如，对于 HTTP 流量，解析 “Request Method” （请求方法）字段先于解析 “Header Host Length” （主机报头长度）字段；用于 “ 请求方法 ” 字段的操作在用于 “ 主机报头长度 ” 字段的操作前发生。例如，可按任何顺序输入以下匹配命令，但是会首先对 **match request method get** 命令进行匹配。

```
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
```

如果操作丢弃数据包，则不会执行进一步操作。例如，如果首个操作是重置连接，则它不会与任何进一步的 **match** 命令进行匹配。如果首个操作是记录数据包，则可能会发生第二个操作，如重置连接。（您可以为同一 **match** 命令配置 **reset**（或 **drop-connection** 等）和 **log** 操作，在这种情况下，为给定的匹配重置数据包后会记录该数据包。）

如果一个数据包与相同的多个 **match** 或 **class** 命令进行匹配，则它们会按出现在策略映射中的顺序进行匹配。例如，对于报头长度为 1001 的数据包，它将与下面的首个命令进行匹配，被记录下来，然后与第二个命令进行匹配并进行重置。如果您颠倒两个 **match** 命令的顺序，则在数据包与第二个 **match** 命令进行匹配前，它将被丢弃且会重置连接；该数据包将不会被记录。

```
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（优先级基于内部规则），确定类映射与另外一个类映射或 **match** 命令具有相同类型。如果类映射具有与另一个类映射相同类型的优先级最低的 **match** 命令，则根据将类映射添加到策略映射中的顺序对它们进行匹配。如果每个类映射的优先级最低的命令不同，则首先对具有更高优先级的 **match** 命令的类映射进行匹配。

请在修改检查策略映射时参阅以下指南：

- HTTP 检查策略映射 - 如果修改正在使用的 HTTP 检查策略映射 (**policy-map type inspect http**)，则您必须删除并重新应用 **inspect http** *map* 操作以使更改生效。例如，如果修改 “http-map” 检查策略映射，则您必须从第 3/4 层策略删除并重新添加 **inspect http http-map** 命令：

  ```
  ciscoasa(config)# policy-map test
  ciscoasa(config-pmap)# class http0
  ciscoasa(config-pmap-c)# no inspect http http-map
  ciscoasa(config-pmap-c)# inspect http http-map
  ```

- 所有检查策略映射 - 如果要用正在使用的检查策略映射交换不同的映射名称，则您必须删除 **inspect** *protocol map* 命令，然后使用新映射来读取它。例如：

  ```
  ciscoasa(config)# policy-map test
  ciscoasa(config-pmap)# class sip
  ciscoasa(config-pmap-c)# no inspect sip sip-map1
  ciscoasa(config-pmap-c)# inspect sip sip-map2
  ```

示例

下面是 HTTP 检查策略映射和相关类映射的示例。此策略映射由服务策略启用的第 3/4 层策略映射激活。

```
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 example
ciscoasa(config-cmap)# match regex 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 inbound_policy interface outside
```

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
parameters	进入用于检查策略映射的参数配置模式。
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-server-secret

要配置用于加密发送给 SiteMinder SSO 服务器的身份验证请求的密钥，请在 webvpn-sso-siteminder 配置模式下使用 **policy-server-secret** 命令。要删除密钥，请使用此命令的 **no** 形式。

policy-server-secret *secret-key*

no policy-server-secret

注　SiteMinder SSO 身份验证需要此命令。

语法说明

secret-key	将字符串用作密钥来加密身份验证通信。不存在最小字符数或最大字符数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Config-webvpn-sso-siteminder 配置	• 是	—	• 是	—	—

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

单点登录支持，仅适用于 WebVPN，可让用户访问不同服务器上的不同安全服务，而无需重复输入用户名和密码。首先使用 **sso-server** 命令创建 SSO 服务器。对于 SiteMinder SSO 服务器，**policy-server-secret** 命令保护 ASA 与 SSO 服务器之间的身份验证通信。

命令参数 *secret-key* 与密码类似：您可以创建它，保存它，然后配置它。使用 **policy-server-secret** 命令可在 ASA 上对其进行配置，使用思科 Java 插件身份验证方案可在 SiteMinder 策略服务器上对其进行配置。

此命令仅适用于 SiteMinder 类型的 SSO 服务器。

示例

以下命令（在 config-webvpn-sso-siteminder 模式中输入，包括作为参数的随机字符串）创建用于 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)#
```

相关命令

命令	说明
max-retry-attempts	配置 SSO 身份验证尝试失败后 ASA 的重试次数。
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 Cisco TrustSec 链路，请在 cts 手动接口配置模式下使用 **policy static sgt** 命令。要删除对手动配置的 CTS 链路的策略，请使用此命令的 **no** 形式。

policy static sgt *sgt_number* [**trusted**]

no policy static sgt *sgt_number* [**trusted**]

语法说明

sgt *sgt_number*	指定要应用于来自对等设备的传入流量的 SGT 编号。有效值为 2 到 65519。
static	指定对链路上的传入流量的 SGT 策略。
trusted	表示在命令中指定 SGT 的接口上的入口流量不应覆盖其 SGT。默认为不受信任。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令将策略应用于手动配置的 CTS 链路中。

限制

- 仅在物理接口、 VLAN 接口、端口通道接口和冗余接口上受支持。
- 在逻辑接口或虚拟接口 （例如 BVI、 TVI 和 VNI）上不受支持。

示例

以下示例为第 2 层 SGT 实施启用接口并定义接口是否可信：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

相关命令

命令	说明
cts manual	启用第 2 层 SGT 实施，然后进入 cts 手动接口配置模式。
propagate sgt	在接口上传播安全组标记 （称为 **sgt**）。默认情况下启用传播。

polltime interface

要在主用 / 主用故障切换配置中指定数据接口轮询和保持时间，请在故障切换组配置模式下使用 **polltime interface** 命令。要恢复默认值，请使用此命令的 **no** 形式。

polltime interface [**msec**] *time* [**holdtime** *time*]

no polltime interface [**msec**] *time* [**holdtime** *time*]

语法说明

holdtime *time*	（可选）设置数据接口必须从对等设备接口接收问候消息的时间，在该时间后，对等设备接口声明发生故障。有效值为从 5 到 75 秒。
interface *time*	指定数据接口轮询时间段。有效值为从 3 到 15 秒。如果使用可选的 **msec** 关键字，则有效值为 500 到 999 毫秒。
msec	（可选）指定给定时间，以毫秒为单位。

默认值

poll *time* 为 5 秒。

holdtime *time* 是 poll *time* 的 5 倍。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	命令已更改为包括可选的 **holdtime** *time* 值，并能够以毫秒为单位指定轮询时间。

使用指南

使用 **polltime interface** 命令可更改在与指定的故障切换组关联的接口发出问候数据包的频率。此命令仅用于主用 / 主用故障切换。请在主用 / 备用故障切换配置中使用 **failover polltime interface** 命令。

您不能输入少于轮询时间 5 倍的 **holdtime** 值。轮询时间越短， ASA 可以越快地检测故障并触发故障切换。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。在超过一半的保持时间内未听到问候数据包时，会开始接口测试。

您可以在配置中包括 **failover polltime unit** 和 **failover polltime interface** 命令。

注　当 CTIQBE 流量通过故障切换配置中的 ASA 时，您应将 ASA 上的故障切换保持时间减少为 30 秒以下。CTIQBE 保持连接超时为 30 秒，而且可能会在应该发生故障切换但尚未发生之前超时。如果 CTIQBE 超时，则会丢弃 Cisco IP SoftPhone 到 Cisco CallManager 的连接， IP SoftPhone 客户端需要重新向 CallManager 注册。

示例

以下部分示例显示了故障切换组的可能配置。在故障切换组 1 中，接口轮询时间设置为 500 毫秒，数据接口的保持时间设置为 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)#
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
failover polltime	指定设备故障切换轮询和保持时间。
failover polltime interface	为主用 / 备用故障切换配置指定接口轮询和保持时间。

pop3s

要进入 POP3S 配置模式，请在全局配置模式下使用 **pop3s** 命令。要删除在 POP3S 命令模式中输入的任何命令，请使用此命令的 **no** 版本。

POP3 是 Internet 服务器用以为您接收和保管电邮的客户端 / 服务器协议。您 （或您的客户端电邮接收方）可在服务器上定期检查您的邮箱并下载任何邮件。此标准协议已内置在最常用的电邮产品中。 POP3S 可让您通过 SSL 连接接收电邮。

pop3s

no pop3

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例显示如何进入 POP3S 配置模式：

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)#
```

相关命令

命令	说明
clear configure pop3s	删除 POP3S 配置。
show running-config pop3s	显示 POP3S 正在运行的配置。

port （电邮代理）

要指定电邮代理的侦听端口，请在适用的电邮代理命令模式下使用 **port** 命令。要恢复到默认值，请使用此命令的 **no** 版本。

port {*portnum*}

no port

语法说明

portnum	电邮代理要使用的端口。为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

默认值

电邮代理的默认端口如下：

电邮代理	默认端口
IMAP4S	993
POP3S	995
SMTPS	988

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

示例

以下示例显示如何为 IMAP4S 电邮代理设置端口 1066：

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# port 1066
```

port (config-mdm-proxy)

此命令为 MDM 注册和签入配置 MDM 代理服务的侦听端口。要恢复到默认值，请使用此命令的 **no** 版本指定已配置的值。

[no] port [enrollment *enroll_port***] [checkin** *checkin_port***]**

语法说明

enroll_port	用于 MDM 客户端身份验证和注册请求的侦听端口号。有效范围为 1 到 65535。默认情况下使用 TCP 端口 443。
checkin_port	用于 MDM 签入请求的侦听端口号。无默认值 （值是必需的）。有效范围为 1 到 65535。其他服务不能占用此端口。

默认值

MDM 代理注册的默认端口是 TCP 端口 443。没有默认的签入端口，必须对其进行配置。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
config-mdm-proxy	• 是	—	• 是	—	—

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

如果在端口子命令的 “no” 形式中指定的任一端口号与当前配置中的行都不匹配，则会显示错误消息。

如果 MDM 签入端口号与其他服务当前使用的端口匹配，则在该接口上启用 MDM 代理时会显示错误消息。

示例

以下示例显示如何为 MDM 代理设置签入端口：

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# port checkin 1077
ciscoasa (config-mdm-proxy)# enable outside
```

port-channel load-balance

对于 EtherChannel，要指定负载平衡算法，请在接口配置模式下使用 **port-channel load-balance** 命令。要将此值设置为默认值，请使用此命令的 **no** 形式。

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

no port-channel load-balance

语法说明

dst-ip	根据数据包的以下特征来平衡接口上的数据包负载： • 目标 IP 地址
dst-ip-port	根据数据包的以下特征来平衡接口上的数据包负载： • 目标 IP 地址 • 目标端口
dst-mac	根据数据包的以下特征来平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平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平衡接口上的数据包负载： • 源 IP 地址 • 目标 IP 地址
src-dst-ip-port	根据数据包的以下特征来平衡接口上的数据包负载： • 源 IP 地址 • 目标 IP 地址 • 源端口 • 目标端口
src-dst-mac	根据数据包的以下特征来平衡接口上的数据包负载： • 源 MAC 地址 • 目标 MAC 地址
src-dst-port	根据数据包的以下特征来平衡接口上的数据包负载： • 源端口 • 目标端口
src-ip	根据数据包的以下特征来平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平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平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平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平衡接口上的数据包负载： • VLAN • 目标 IP 地址
vlan-dst-ip-port	根据数据包的以下特征来平衡接口上的数据包负载： • VLAN • 目标 IP 地址 • 目标端口
vlan-only	根据数据包的以下特征来平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平衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目标 IP 地址
vlan-src-dst-ip-port	根据数据包的以下特征来平衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目标 IP 地址 • 源端口 • 目标端口
vlan-src-ip	根据数据包的以下特征来平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平衡接口上的数据包负载： • VLAN • 源 IP 地址 • 源端口

命令默认　默认为 **src-dst-ip**。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。

使用指南

ASA 通过对数据包 (**src-dst-ip**) 的源 IP 地址和目标 IP 地址进行哈希处理，向 EtherChannel 中的接口分发数据包。在模数运算中，将得到的哈希值除以主用链路数，得到的余数确定哪个接口拥有流量。 *hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的数据包发往第二个接口，结果为 2 的数据包发往第三个接口，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。

对于集群中的跨区 EtherChannel，负载平衡基于每个 ASA 来进行。例如，如果您在 8 个 ASA 上的跨区 EtherChannel 中有 32 个主用接口 （在 EtherChannel 中每个 ASA 有 4 个接口），则负载平衡仅发生在 ASA 上的 4 个接口间。

如果主用接口发生故障且未被备用接口取代，则流量会在剩余的链路之间重新实现平衡。从第 2 层的生成树和第 3 层的路由表中可屏蔽该故障，因此切换对其他网络设备没有影响。

示例

以下示例设置使用源 IP 地址和目标 IP 地址及端口的负载平衡算法：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel min-bundle	指定端口通道接口变成主用接口所需的最小主用接口数。
show lacp	显示 LACP 信息 （例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

port-channel min-bundle

对于 EtherChannel，要指定端口通道接口变成主用接口所需的最小主用接口数，请在接口配置模式下使用 **port-channel min-bundle** 命令。要将此值设置为默认值，请使用此命令的 **no** 形式。

port-channel min-bundle *number*

no port-channel min-bundle

语法说明

number	指定端口通道接口变成主用接口所需的最小主用接口数（介于 1 和 8 之间）；对于 9.2(1) 及更高版本，主用接口数可在 1 和 16 之间。

命令默认

默认值为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	我们引入了此命令。
9.2(1)	我们已将主用接口数从 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低于此值，则端口通道接口会发生故障，并可能触发设备级故障切换。

示例

以下示例将端口通道接口变成主用接口所需的最小主用接口数设置为两个：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

相关命令

命令	说明
channel-group	将接口添加到 EtherChannel。
interface port-channel	配置 EtherChannel。
lacp max-bundle	指定通道组中允许的最大主用接口数。
lacp port-priority	为通道组中的物理接口设置优先级。
lacp system-priority	设置 LACP 系统优先级。
port-channel load-balance	配置负载平衡算法。
show lacp	显示 LACP 信息 （例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口通道信息。
show port-channel load-balance	显示端口通道负载平衡信息，以及哈希结果和为给定参数集选择的成员接口。

port-channel span-cluster

要在 ASA 集群中将此 EtherChannel 设置为跨区 EtherChannel，请在接口配置模式下使用 **port-channel span-cluster** 命令。要禁用跨区，请使用此命令的 **no** 形式。

port-channel span-cluster [**vss-load-balance**]

no port-channel span-cluster [**vss-load-balance**]

语法说明

vss-load-balance	（可选）启用 VSS 负载平衡。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平衡。启用负载平衡前，您必须在 **channel-group** 命令中为每个成员接口配置 **vss-id** 关键字。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

您必须在跨区 EtherChannel 模式 (**cluster interface-mode spanned**) 中使用此功能。

此功能让您可以将每个设备的一个或多个接口组合为一个贯穿集群中所有设备的 EtherChannel。EtherChannel 可汇总通道中所有可用主用接口间的流量。在路由和透明防火墙模式中可配置跨区 EtherChannel。在路由模式中，EtherChannel 可配置为具有单个 IP 地址的路由接口。在透明模式中，可将 IP 地址分配给桥组而非接口。作为基本操作的一部分， EtherChannel 本身可提供负载平衡。

示例

以下示例使用万兆位以太网 0/8 接口将 EtherChannel (port-channel 2) 创建为唯一成员，然后使该 EtherChannel 贯穿整个集群。两个子接口添加到 port-channel 2 中。

```
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
```

相关命令

命令	说明
interface	进入接口配置模式。
cluster interface-mode	为跨区 EtherChannel 或个别接口设置集群接口模式。

port-forward

要配置无客户端 SSL VPN 会话的用户可通过转发的 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，请多次使用带有相同 *list_name* 的此命令，对每个应用使用一次。

要从列表中删除已配置的应用，请使用 **no port-forward** *list_name local_port* 命令 （您无需包括 *remote_server* 和 *remote_port* 参数）。

no port-forward *listname localport*

要删除整个已配置列表，请使用 **no port-forward** *list_name* 命令。

no port-forward *list_name*

语法说明

description	提供在最终用户 Port Forwarding Java （端口转发 Java）小应用屏幕上显示的应用名称或简短说明。最多 64 个字符。
list_name	组合无客户端 SSL VPN 会话的用户可访问的应用集 （转发的 TCP 端口）。最多 64 个字符。
local_port	为应用指定侦听 TCP 流量的本地端口。您仅可对 *list_name* 使用一次本地端口号。输入 1 到 65535 范围内的端口号。为避免与现有服务冲突，请使用大于 1024 的端口号。
remote_port	在远程服务器上为此应用指定要连接到的端口。这是应用使用的实际端口。输入 1 到 65535 范围内的端口号或端口名称。
remote_server	为应用提供远程服务器的 DNS 名称或 IP 地址。如果输入 IP 地址，可以 IPv4 或 IPv6 格式输入。我们建议使用主机名，这样您无需为特定 IP 地址配置客户端应用。 DNS 服务器组命令 **name-server** 必须将主机名解析为 IP 地址。

默认值

没有默认端口转发列表。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	命令模式已更改为 WebVPN。

使用指南

端口转发不支持 Microsoft Outlook Exchange (MAPI) 代理。但是，您可以配置对 Microsoft Outlook Exchange 2010 的 Smart Tunnel （智能隧道）支持。

示例

下表显示示例应用使用的值。

应用	本地端口	服务器 DNS 名称	远程端口	说明
IMAP4S 电邮	20143	IMAP4Sserver	143	接收邮件
SMTPS 电邮	20025	SMTPSserver	25	发送邮件
基于 SSH 的 DDTS	20022	DDTSserver	22	基于 SSH 的 DDTS
Telnet	20023	Telnetserver	23	Telnet

以下示例显示如何创建名为 *SalesGroupPorts* 的端口转发列表 （提供对上述应用的访问）：

```
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
```

相关命令

命令	说明
port-forward auto-start	在组策略 WebVPN 或用户名 WebVPN 模式中输入此命令后，它会自动开始端口转发，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。
port-forward enable	在组策略 WebVPN 或用户名 WebVPN 模式中输入此命令后，它会在用户登录时分配指定的端口转发列表，但需要用户使用无客户端 SSL VPN 门户页面上的 **Application Access （应用访问） > Start Applications （启动应用）**按钮来手动开始端口转发。
port-forward disable	在组策略 WebVPN 或用户名 WebVPN 模式中输入此命令后，它会关闭端口转发。

port-forward-name

要为特定用户或组策略配置用于标识对最终用户的 TCP 端口转发的显示名称，请在 WebVPN 模式（可从组策略或用户名模式进入）中使用 **port-forward-name** 命令。要删除显示名称（包括通过使用 **port-forward-name none** 命令创建的空值），请使用该命令的 no 形式。使用 **no** 选项可恢复默认名称 -“Application Access”。要阻止显示名称，请使用 **port-forward none** 命令。

port-forward-name {**value** *name* | **none**}

no port-forward-name

语法说明

none	表示没有显示名称。设置空值，从而禁止显示名称。阻止继承值。
value *name*	描述对最终用户的端口转发。最多 255 个字符。

默认值

默认名称为 “Application Access”。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例显示如何为名为 FirstGroup 的组策略设置名称 -“Remote Access TCP Applications”：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

相关命令

命令	说明
webvpn	在组策略配置模式或用户名配置模式下使用。用于进入 WebVPN 模式以配置应用于组策略或用户名的参数。
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

port-object

要将端口对象添加到 TCP、 UDP 或 TCP-UDP 类型的服务对象组中，请在对象组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 {**eq** *port* | **range** *begin_port end_port*}

no port-object {**eq** *port* | **range** *begin_port end_port*}

语法说明

range *begin_port end_port*	指定端口范围，在 0 和 65535 之间 （含）。
eq *port*	指定十进制数（在 0 和 65535 之间）或服务对象的 TCP 或 UDP 端口的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
对象网络服务配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	我们引入了此命令。

使用指南

port-object 命令可与 **object-group service** *protocol* 命令一起使用，来定义作为特定端口或系列端口的对象。

如果为 TCP 或 UDP 服务指定名称，则必须是支持的 TCP 或 / 和 UDP 名称之一，且其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，名称必须分别是有效的 TCP 服务名称、有效的 UDP 服务名称或有效的 TCP 和 UDP 服务名称。

如果指定编号，则将在显示对象时根据协议类型转换为相应的名称 （如果存在）。

支持以下服务名称：

TCP	UDP	TCP 和 UDP
bgp	biff	discard
chargen	bootpc	domain
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	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

示例

以下例显示如何在服务配置模式下使用 **port-object** 命令创建新端口（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
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object-group** 命令。
group-object	添加网络对象组。
network-object	将网络对象添加到网络对象组。
object-group	定义对象组以优化配置。
show running-config object-group	显示当前对象组。

portal-access-rule

此命令允许客户配置全局无客户端 SSL VPN 访问策略，以基于 HTTP 报头中存在的数据允许或拒绝无客户端 SSL VPN 会话。如果被拒绝，错误代码将返回给客户端。在用户身份验证前执行此拒绝，从而最大限度减少使用处理资源。

portal-access-rule none

portal-access-rule *priority* **[{permit | deny [code** *code***]} {any | user-agent match** *string*}

no portal-access-rule *priority* **[{permit | deny [code** *code***]} {any | user-agent match** *string*}**]**

clear configure webvpn portal-access-rule

语法说明

none	删除所有门户访问规则。无客户端 SSL VPN 会话不会基于 HTTP 报头受到限制。
priority	规则的优先级。范围：1 到 65535。
permit	允许基于 HTTP 报头的访问。
deny	拒绝基于 HTTP 报头的访问。
code	允许或拒绝基于返回的 HTTP 状态代码的访问。默认值：403。
code	HTTP 状态代码编号，它是您允许或拒绝访问的依据。范围：200 到 599。
any	与任何 HTTP 报头字符串进行匹配。
user-agent match	启用 HTTP 报头中的字符串比较。
string	指定要在 HTTP 报头中进行匹配的字符串。使用通配符 (*) 来搜索包含您的字符串的匹配字符串，或不使用通配符来搜索与您的字符串完全匹配的字符串。 **注**　我们建议在您的搜索字符串中使用通配符。若不使用通配符，规则可能不与任何字符串匹配，或相匹配的字符串比您预期的少得多。 如果您正在搜索的字符串中有空格，则该字符串必须用引号括起；例如，“*a string*”。同时使用引号和通配符时，您的搜索字符串将如此处所示：“**a string***”。
no portal-access-rule	用于删除单个门户访问规则。
clear configure webvpn portal-access-rule	等同于 portal-access-rule none 命令。

默认值

portal-access-rule none

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(5)	ASA 8.2.5 和 8.4(2) 中同时引入了此命令。
8.4(2)	ASA 8.2.5 和 8.4(2) 中同时引入了此命令。

使用指南

在用户身份验证前执行此检查。

示例

以下示例创建三个门户访问规则：

- 当 ASA 返回代码 403 且 Thunderbird 在 HTTP 报头中时，门户访问规则 1 拒绝所尝试的无客户端 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 允许所尝试的无客户端 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
```

相关命令

命令	说明
show run webvpn	显示包括所有门户访问规则的 WebVPN 配置。
show vpn-sessiondb detail webvpn	显示有关 VPN 会话的信息。命令包括用于显示完整或详细信息的选项，让您可以指定要显示的会话类型，并提供用于过滤和分类信息的选项。
debug webvpn request ***n***	在特定调试级别启用调试消息日志记录。默认值：1。范围：1 到 255。

post-max-size

要指定对象发布所允许的最大大小，请在组策略 WebVPN 配置模式下使用 **post-max-size** 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

语法说明

size	指定已发布的对象所允许的最大大小。范围为 0 到 2147483647。

默认值

默认大小为 2147483647。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

将大小设置为 0 可有效禁止对象发布。

示例

以下示例将已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
```

相关命令

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。
webvpn	在组策略配置模式或用户名配置模式下使用。用于进入 WebVPN 模式以配置应用于组策略或用户名的参数。
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

pppoe client route distance

要为通过 PPPoE 获知的路由配置管理距离，请在接口配置模式下使用 **pppoe client route distance** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

pppoe client route distance *distance*

no pppoe client route distance *distance*

语法说明

distance	应用于通过 PPPoE 获知的路由的管理距离。有效值为从 1 到 255。

默认值

默认情况下，为通过 PPPoE 获知的路由提供的管理距离为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

仅当从 PPPoE 获知路由时，才使用 **pppoe client route distance** 命令。如果在从 PPPoE 获知路由后输入 **pppoe client route distance** 命令，则指定的管理距离不影响现有已获知的路由。仅输入该命令后获知的路由才具有指定的管理距离。

您必须在 **ip address pppoe** 命令上指定 **setroute** 选项来通过 PPPoE 获取路由。

如果已在多个接口上配置 PPPoE，则您必须在每个接口上使用 **pppoe client route distance** 命令来指示已安装路由的优先级。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，则您将无法配置故障切换。

示例

以下示例在千兆位以太网 0/2 接口上通过 PPPoE 获得默认路由。通过跟踪条目对象 1 跟踪路由。SLA 操作监控外部接口外 10.1.1.1 网关的可用性。如果 SLA 操作失败，则会在千兆位以太网 0/3 接口上通过 PPPoE 获得二级路由。

```
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
```

相关命令

命令	说明
ip address pppoe	使用通过 PPPoE 获得的 IP 地址配置指定接口。
ppoe client secondary	配置对二级 PPPoE 客户端接口的跟踪。
pppoe client route track	将通过 PPPoE 获知的路由与跟踪条目对象关联。
sla monitor	定义 SLA 监控操作。
track rtr	创建用于轮询 SLA 的跟踪条目。

pppoe client route track

要配置 PPPoE 客户端以将已添加的路由与指定的跟踪对象编号关联，请在接口配置模式下使用 **pppoe client route track** 命令。要删除 PPPoE 路由跟踪，请使用此命令的 **no** 形式。

pppoe client route track *number*

no pppoe client route track

语法说明

number	跟踪条目对象 ID。有效值为从 1 到 500。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

仅当从 PPPoE 获知路由时才使用 **pppoe client route track** 命令。如果在从 PPPoE 获知路由后输入 **pppoe client route track** 命令，则现有已获知的路由不与跟踪对象关联。仅输入该命令后获知的路由才与指定的跟踪对象关联。

您必须在 **ip address pppoe** 命令上指定 **setroute** 选项来通过 PPPoE 获取路由。

如果已在多个接口上配置 PPPoE，则您必须在每个接口上使用 **pppoe client route distance** 命令来指示已安装路由的优先级。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，则您将无法配置故障切换。

示例

以下示例在千兆位以太网 0/2 接口上通过 PPPoE 获得默认路由。通过跟踪条目对象 1 跟踪路由。SLA 操作监控外部接口外 10.1.1.1 网关的可用性。如果 SLA 操作失败，则会在千兆位以太网 0/3 接口上通过 PPPoE 获得二级路由。

```
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
```

相关命令

命令	说明
ip address pppoe	使用通过 PPPoE 获得的 IP 地址配置指定接口。
ppoe client secondary	配置对二级 PPPoE 客户端接口的跟踪。
pppoe client route distance	将管理距离分配给通过 PPPoE 获知的路由。
sla monitor	定义 SLA 监控操作。
track rtr	创建用于轮询 SLA 的跟踪条目。

pppoe client secondary

要配置 PPPoE 客户端以将其注册为跟踪对象的客户端并根据跟踪状态进行上下调整，请在接口配置模式下使用 **pppoe client secondary** 命令。要删除客户端注册，请使用此命令的 **no** 形式。

pppoe client secondary track *number*

no pppoe client secondary track

语法说明

number	跟踪条目对象 ID。有效值为从 1 到 500。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

仅当 PPPoE 会话开始时才使用 **pppoe client secondary** 命令。如果在从 PPPoE 获知路由后输入 **pppoe client route track** 命令，则现有已获知的路由不与跟踪对象关联。仅输入该命令后获知的路由才与指定的跟踪对象关联。

您必须在 **ip address pppoe** 命令上指定 **setroute** 选项来通过 PPPoE 获取路由。

如果已在多个接口上配置 PPPoE，则您必须在每个接口上使用 **pppoe client route distance** 命令来指示已安装路由的优先级。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，则您将无法配置故障切换。

示例

以下示例在千兆位以太网 0/2 接口上通过 PPPoE 获得默认路由。通过跟踪条目对象 1 跟踪路由。SLA 操作监控外部接口外 10.1.1.1 网关的可用性。如果 SLA 操作失败，则会在千兆位以太网 0/3 接口上通过 PPPoE 获得二级路由。

```
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
```

相关命令

命令	说明
ip address pppoe	使用通过 PPPoE 获得的 IP 地址配置指定接口。
ppoe client secondary	配置对二级 PPPoE 客户端接口的跟踪。
pppoe client route distance	将管理距离分配给通过 PPPoE 获知的路由。
pppoe client route track	将通过 PPPoE 获知的路由与跟踪条目对象关联。
sla monitor	定义 SLA 监控操作。

第 17 章

pre-fill-username 至 pwd 命令

pre-fill-username

要支持从客户端证书提取用户名用于身份验证和授权，请在隧道组 WebVPN 属性模式下使用 **pre-fill-username** 命令。要从配置中删除属性，请使用此命令的 **no** 形式。

pre-fill-username {**ssl-client** | **clientless**}

no pre-fill-username

语法说明

ssl-client	为 AnyConnect VPN 客户端连接启用此功能。
clientless	为无客户端连接启用此功能。

默认值

无默认值或行为。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

通过 **pre-fill-username** 命令，您可以从 **username-from-certificate** 命令中指定的证书字段中提取用户名作为用于用户名 / 密码身份验证和授权的用户名。要使用此从证书预填充用户名的功能，您必须配置这两个命令。

要启用此功能，您还必须在隧道组常规属性模式中配置 **username-from-certificate** 命令。

注　在 8.0.4 和 8.1.2 版本中，不预填充用户名；相反，在用户名字段中发送的任何数据都被忽略。

示例

以下示例 （在全局配置模式中输入）创建名为 remotegrp 的 IPsec 远程访问隧道组，并指定用于 SSL VPN 客户端的身份验证或授权查询的名称必须来源于数字证书：

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# pre-fill-username ssl-client
ciscoasa(config-tunnel-webvpn)#
```

相关命令

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	在证书中指定要用作授权的用户名的字段。

preempt

要使设备在启动时激活 （如果它具有较高优先级），请在故障切换组配置模式下使用 **preempt** 命令。要删除预占，请使用此命令的 **no** 形式。

preempt [*delay*]

no preempt [*delay*]

语法说明

seconds	预占对等设备前的等待时间 （以秒为单位）。有效值为从 1 到 1200 秒。

默认值

默认情况下，没有延迟。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当两个设备同时启动时 （在设备轮询时间内），将主要优先级或次要优先级分配给故障切换组可指定该故障切换组在哪个设备上激活。但是，如果一个设备在另一个设备前启动，则两个故障切换组都会在该设备上激活。当另一个设备联机时，以第二个设备优先的任何故障切换组都不会在第二个设备上激活，除非使用 **preempt** 命令对故障切换组进行配置，或使用 **no failover active** 命令手动强制该故障切换组在另一个设备上激活。如果使用 **preempt** 命令配置故障切换组，则该故障切换组会自动在指定设备上激活。

注　如果启用 Stateful Failover （状态故障切换），则抢占会延迟，直到连接从当前激活的故障切换组所在的设备中复制为止。

示例

以下示例将主要设备作为更高优先级来配置故障切换组 1，将辅助设备作为更高优先级来配置故障切换组 2。使用 **preempt** 命令对这两个故障切换组进行了配置，其中等待时间为 100 秒，因此在设备可用后，这两个组会自动在首选设备上激活达 100 秒。

```
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)#
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
primary	对于所配置的故障切换组，为故障切换对中的主要设备提供优先级。
secondary	对于所配置的故障切换组，为故障切换对中的辅助设备提供优先级。

prefix-list

OSPFv2、 EIGRP 和 BGP 协议都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* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

语法说明

/	*network* 和 *len* 值之间必需的分隔符。
deny	拒绝访问匹配条件。
ge *min_value*	（可选）指定要匹配的最小前缀长度。*min_value* 参数的值必须大于 *len* 参数的值，并小于或等于 *max_value* 参数的值 （如果存在）。
le *max_value*	（可选）指定要匹配的最大前缀长度。 *max_value* 参数的值必须大于或等于 *min_value* 参数的值 （如果存在），或大于 *len* 参数的值 （如果 *min_value* 参数不存在）。
len	网络掩码的长度。有效值为从 0 到 32。
network	网络地址。
permit	允许访问匹配条件。
prefix-list-name	前缀列表的名称。前缀列表名称不能包含空格。
seq *seq_num*	（可选）将指定的序列号应用于正在创建的前缀列表中。

默认值

如果不指定序列号，则会将序列号 5 分配给前缀列表中的第一个条目，每个后续条目的序列号会以 5 为增量递增。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。
9.2(1)	引入了对 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 过滤可扩展 ABR 的功能，即运行 OSPF 来过滤不同 OSPF 区域之间的类型 3 LSA。配置前缀列表后，仅指定的前缀才会从一个区域发送到另一个区域。所有其他前缀仅限于在其 OSPF 区域中使用。您可以将此类型的区域过滤应用于流入和 / 或流出 OSPF 区域的流量。

当前缀列表的多个条目与给定的前缀相匹配时，使用序列号最低的条目。 ASA 在前缀列表的顶部从序列号最低的条目开始搜索。找到匹配项后， ASA 不再搜索列表的其余部分。为提高效率，您可以手动将较低的序列号分配给最常用的匹配项或拒绝项来将它们置于列表顶部附近。

默认情况下，序列号会自动生成。使用 **no prefix-list sequence-number** 命令可抑制它们。序列号会以 5 为增量生成。前缀列表中生成的第一个序列号会是 5。该列表中下一个条目的序列号会是 10，然后依此类推。如果您为一个条目指定值，然而不为后续条目指定值，则生成的序列号会从指定的值开始以 5 为增量递增。例如，如果您指定前缀列表中的第一个条目的序列号为 3，然后添加了两个条目，则在不为附加条目指定序列号的情况下，这两个条目自动生成的序列号会是 8 和 13。

您可以使用 **ge** 和 **le** 关键字指定要与前缀 （比 *network/len* 参数更明确）相匹配的前缀长度的范围。未指定 **ge** 或 **le** 关键字时，会假设执行完全匹配。如果仅指定 **ge** 关键字，则范围为从 *min_value* 到 32 ；如果仅指定 **le** 关键字，则范围为从 *len* 到 *max_value*。

min_value 和 *max_value* 参数的值必须满足以下条件：

len < *min_value* <= *max_value* <= 32

使用该命令的 **no** 形式可从前缀列表中删除特定条目。使用 **clear configure prefix-list** 命令可删除前缀列表。 **clear configure prefix-list** 命令还可从配置中删除关联的 **prefix-list description** 命令（如果有）。

示例

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带有前缀 192/8 的路由中接受多达 24 位的掩码长度：

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

以下示例显示如何在带有前缀 192/8 的路由中拒绝大于 25 位的掩码长度：

```
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 到 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大于 25 位的掩码长度：

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

以下示例显示如何拒绝带有前缀 10/8 的所有路由：

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

以下示例显示如何为带有前缀 192.168.1/24 的路由拒绝长度大于 25 位的所有掩码：

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

以下示例显示如何允许带有前缀 0/0 的所有路由：

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

相关命令

命令	说明
clear configure prefix-list	从正在运行的配置中删除 **prefix-list** 命令。
prefix-list description	让您可以输入前缀列表的说明。
prefix-list sequence-number	启用前缀列表序列编号。
show running-config prefix-list	显示正在运行的配置中的 **prefix-list** 命令。

prefix-list description

要将说明添加到前缀列表中，请在全局配置模式下使用 **prefix-list description** 命令。要删除前缀列表说明，请使用此命令的 **no** 形式。

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

语法说明

prefix-list-name	前缀列表的名称。
text	前缀列表说明的文本。您可输入最多 80 个字符。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您可以为特定前缀列表名称以任何顺序输入 **prefix-list** 和 **prefix-list description** 命令；无需一定在输入前缀列表说明前创建前缀列表。无论您以什么顺序输入命令， **prefix-list description** 命令都始终出现在配置中关联的前缀列表前的行上。

如果您为已有说明的前缀列表条目输入 **prefix-list description** 命令，则新说明将替换原始说明。

使用此命令的 **no** 形式时，您不需要输入文本说明。

示例

以下示例为名为 MyPrefixList 的前缀列表添加说明。 **show running-config prefix-list** 命令显示虽然前缀列表说明已添加到正在运行的配置中，但前缀列表本身尚未得到配置。

```
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
!
```

相关命令

命令	说明
clear configure prefix-list	从正在运行的配置中删除 **prefix-list** 命令。
prefix-list	为 ABR 类型 3 LSA 过滤定义前缀列表。
show running-config prefix-list	显示正在运行的配置中的 **prefix-list** 命令。

prefix-list sequence-number

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

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用前缀列表序列编号。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

仅此命令的 **no** 形式会出现在配置中。当此命令的 **no** 形式在配置中时，序列号 （包括手动配置的）会从配置中的 **prefix-list** 命令中删除，且不会为新前缀列表条目分配序列号。

启用前缀列表序列编号时，使用默认的编号方法 （从 5 开始且每个数字以 5 为增量递增）为所有前缀列表条目分配序列号。如果在禁用编号前将序列号手动分配给前缀列表条目，将恢复手动分配的编号。在禁用自动编号时手动分配的序列号也会恢复，即使它们不会在禁用编号时显示。

示例

以下示例禁用前缀列表序列编号：

```
ciscoasa(config)# no prefix-list sequence-number
```

相关命令

命令	说明
prefix-list	为 ABR 类型 3 LSA 过滤定义前缀列表。
show running-config prefix-list	显示正在运行的配置中的 **prefix-list** 命令。

prf

要在用于 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**}

语法说明

md5	指定 MD5 算法。
sha	（默认）指定安全哈希算法 SHA 1。
sha256	指定具有 256 位摘要的安全哈希算法 SHA 2。
sha384	指定具有 384 位摘要的安全哈希算法 SHA 2。
sha512	指定具有 512 位摘要的安全哈希算法 SHA 2。

默认值

默认为 **sha** (SHA 1)。

使用指南

IKEv2 SA 是在第 1 阶段中使用的密钥，用于启用 IKEv2 对等设备以在第 2 阶段中进行安全通信。输入 **crypto ikev2 policy** 命令后，请使用 **prf** 命令选择伪随机函数，用于为在 SA 中使用的所有加密算法构造密钥内容。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	添加了此命令。
8.4(2)	添加了 **sha256**、**sha384** 和 **sha512** 关键字以支持 SHA 2。

示例

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
```

相关命令

命令	说明
encryption	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定加密算法。
group	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 Diffie-Hellman 组。
integrity	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 ESP 完整性算法。
lifetime	在用于 AnyConnect IPsec 连接的 IKEv2 SA 中指定 SA 生存期。

primary

要为主要设备提供故障切换组的较高优先级，请在故障切换组配置模式下使用 **primary** 命令。要恢复默认值，请使用此命令的 **no** 形式。

primary

no primary

语法说明

此命令没有任何参数或关键字。

默认值

如果未对故障切换组指定 **primary** 或 **secondary**，则故障切换组将默认采用 **primary**。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

当两个设备同时启动时 （在设备轮询时间内），将主要优先级或次要优先级分配给故障切换组可指定该故障切换组在哪个设备上激活。如果两个设备先后启动，则两个故障切换组都会在先启动的设备上激活。当另一个设备联机时，以第二个设备优先的任何故障切换组都不会在第二个设备上激活，除非使用 **preempt** 命令对故障切换组进行配置，或使用 **no failover active** 命令手动强制该故障切换组在另一个设备上激活。

示例

以下示例将主要设备作为更高优先级来配置故障切换组 1，将辅助设备作为更高优先级来配置故障切换组 2。使用 **preempt** 命令对这两个故障切换组都进行了配置，因此在设备可用后，这两个组会自动在其首选设备上激活。

```
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)#
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
preempt	在设备可用后，强制故障切换组自动在其首选设备上激活。
secondary	为辅助设备提供高于主要设备的优先级。

priority （类）

要启用 QoS 优先级队列，请在类配置模式下使用 **priority** 命令。对于无法容忍延迟的关键流量，例如 IP 语音 (VoIP)，您可以标识用于低延迟队列 (LLQ) 的流量，以便始终以最低速率传输它。要删除优先级要求，请使用此命令的 **no** 形式。

注　ASA 服务模块上不支持此命令。

priority

no priority

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或变量。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

通过 LLQ 优先级队列，您可以先处理某些流量流 （例如语音和视频等延迟敏感型流量，再处理其他流量。

ASA 支持两种类型的优先级队列：

- 标准优先级队列 - 标准优先级队列可在接口上使用 LLQ 优先级队列 （请参阅 **priority-queue** 命令），所有其他流量进入 “ 尽力而为 ” 队列。队列大小并非无限的，因此它们会充满并溢出。当队列充满时，任何其他数据包都无法进入队列而被丢弃。这称为 *tail drop* （队尾丢弃）。为避免队列充满，您可以增加队列缓冲区大小。您还可以微调允许进入传输队列的最大数据包数。这些选项让您可以控制优先级队列的延迟和稳定性。 LLQ 队列中数据包的传输始终优先于 “ 尽力而为 ” 队列中的数据包。
- 分层优先级队列 - 在启用流量整形队列（**shape** 命令）的接口上使用分层优先级队列。整形流量的子集可得到优先处理。不使用标准优先级队列。请参阅以下有关分层优先级队列的指南：
  - 优先级数据包始终排在整形队列的队首，因此它们始终先于其他非优先级排队的数据包得到传输。
  - 优先级数据包绝不被整形队列丢弃，除非优先级流量的持续速率超过整形速率。

– 对于 IPsec 加密数据包，您仅可根据 DSCP 或优先级设置对流量进行匹配。
– 优先级流量分类不支持通过 TCP 的 IPsec。

使用模块化策略框架配置 QoS

要启用优先级队列，请使用模块化策略框架。您可以使用标准优先级队列或分层优先级队列。

对于标准优先级队列，请执行以下任务：

1. **class-map** - 标识用于执行优先级队列的流量。
2. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **priority** - 为类映射启用优先级队列。
3. **service-policy** - 向接口分配策略映射或全局分配策略映射。

对于分层优先级队列，请执行以下任务：

1. **class-map** - 标识用于执行优先级队列的流量。
2. **policy-map** （用于优先级队列） - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **priority** - 为类映射启用优先级队列。如果要使用的是分层优先级队列，则您仅可在此策略映射中包括优先级命令。
3. **policy-map** （用于流量整形） - 标识与 **class-default** 类映射关联的操作。
   a. **class class-default** - 标识要对其执行操作的 **class-default** 类映射。
   b. **shape** - 将流量整形应用于类映射。
   c. **service-policy** - 调用您在其中配置 **priority** 命令的优先级队列策略映射，以便将优先级队列应用于整形流量的子集。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

示例

以下是策略映射配置模式中的 **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)#
```

相关命令

class	指定要用于流量分类的类映射。
clear configure policy-map	删除所有策略映射配置，除非策略映射正在 service-policy 命令中使用，才可不删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
show running-config policy-map	显示所有当前策略映射配置。

priority （集群组）

要在 ASA 集群中设置此设备的优先级以用于主控设备选定，请在集群组配置模式下使用 **priority** 命令。要删除优先级，请使用此命令的 **no** 形式。

priority *priority_number*

no priority [*priority_number*]

语法说明

priority_number	设置此设备的优先级以用于主控设备选定，在 1 和 100 之间，其中 1 为最高优先级。

命令默认

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

集群成员可通过集群控制链路通信来选定主控设备，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，它会每 3 秒广播一个选定请求。
2. 具有较高优先级的任何其他设备都会响应选定请求；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，则该设备会成为主控设备。

   注　如果多个设备具有相同的最高优先级，则使用集群设备名称和序列号来确定主控设备。

4. 如果设备后来以较高优先级加入集群，则它不会自动成为主控设备；现有主控设备始终依然是主控设备，除非它停止响应，届时将选定新主控设备。

注　您可以使用 **cluster master unit** 命令手动强制设备成为主控设备。对于集中功能，如果您强制更改主控设备，则所有连接都将被丢弃，您必须在新主控设备上重新建立连接。请参阅配置指南以获取集中功能列表。

示例

以下示例将优先级设置为 1 （最高）：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

相关命令

命令	说明
clacp system-mac	使用跨区 EtherChannel 时， ASA 使用 cLACP 来与邻居交换机协商 EtherChannel。
cluster group	为集群命名，然后进入集群配置模式。
cluster-interface	指定集群控制链路接口。
cluster interface-mode	设置集群接口模式。
conn-rebalance	启用连接重新平衡。
console-replicate	启用从从属设备到主控设备的控制台复制。
enable （集群组）	启用集群。
health-check	启用集群运行状况检查功能，其中包括设备运行状况监控和接口运行状况监控。
key	设置用于在集群控制链路上控制流量的身份验证密钥。
local-unit	为集群成员命名。
mtu cluster-interface	为集群控制链路接口指定最大传输单位数。

priority （VPN 负载平衡）

要设置参与虚拟负载平衡集群的本地设备的优先级，请在 VPN 负载平衡模式下使用 **priority** 命令。要恢复到默认的优先级指定，请使用此命令的 **no** 形式。

priority *priority*

no priority

语法说明

priority	您想要分配给此设备的优先级 （在 1 到 10 的范围内）。

默认值

默认优先级取决于设备的型号：

型号编号	默认优先级
5520	5
5540	7

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
VPN 负载平衡	—	—	• 是	—	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

您必须首先使用 **vpn load-balancing** 命令进入 VPN 负载平衡模式。

此命令设置参与虚拟负载平衡集群的本地设备的优先级。

优先级必须是 1 （最低）到 10 （最高）的范围内的整数。

优先级是主控设备选定过程中的一种方法，用于确定 VPN 负载平衡集群中的哪个设备成为集群的主控或主要设备。请参阅 CLI 配置指南 获取有关主控设备选定过程的详细信息。

该命令的 **no** 形式可将优先级指定恢复为默认值。

示例

以下是 VPN 负载平衡命令序列 （包括用于将当前设备的优先级设置为 9 的 **priority** 命令）的示例：

```
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
```

相关命令 ciscoasa

命令	说明
vpn load-balancing	进入 VPN 负载平衡模式。

priority-queue

要在接口上创建与 **priority** 命令一起使用的标准优先级队列，请在全局配置模式下使用 **priority-queue** 命令。要删除队列，请使用此命令的 **no** 形式。

注　ASA 5580 万兆位以太网接口上不支持此命令。（ASA 5585-X 上的优先级队列支持万兆位以太网接口。） ASA 5512-X 到 ASA 5555-X 管理接口也不支持此命令。

ASA 服务模块上不支持此命令。

priority-queue *interface-name*

no priority queue *interface-name*

语法说明

interface-name	指定要启用优先级队列的物理接口的名称或 VLAN 接口的名称（对于 ASA 5505 或 ASASM）。

默认值

默认情况下禁用优先级队列。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.2(3)/8.4(1)	为 ASA 5585-X 添加了对万兆位以太网接口的支持。

使用指南

通过 LLQ 优先级队列，您可以先处理某些流量流 （例如语音和视频等延迟敏感型流量，再处理其他流量。

ASA 支持两种类型的优先级队列：

- 标准优先级队列 - 标准优先级队列在使用 **priority-queue** 命令创建的接口上使用 LLQ 优先级队列，所有其他流量进入 “ 尽力而为 ” 队列。队列大小并非无限的，因此它们会充满并溢出。当队列充满时，任何其他数据包都无法进入队列而被丢弃。这称为 *tail drop* （队尾丢弃）。为避免队列充满，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 （**tx-ring-limit** 命令）。这些选项让您可以控制优先级队列的延迟和稳定性。 LLQ 队列中数据包的传输始终优先于 “ 尽力而为 ” 队列中的数据包。
- 分层优先级队列 - 在启用流量整形队列的接口上使用分层优先级队列。整形流量的子集可得到优先处理。不使用标准优先级队列。

注　（仅适用于 ASA 5505）在一个接口上配置优先级队列会覆盖所有其他端口上的相同配置；仅最后一次应用的配置存在于所有接口上。此外，如果从一个接口中删除优先级队列配置，则会从所有接口中删除它。要解决此问题，请仅在一个接口上配置 **priority-queue** 命令。如果不同的接口对 **queue-limit** 和 / 或 **tx-ring-limit** 命令需要不同设置，请在任一接口 (CSCsi13132) 上使用所有队列限制中的最大值和所有 tx 环限制中的最小值。

示例

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)#
```

相关命令

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	在以太网传输驱动程序中设置可在任何给定时间排队的最大数据包数。
policy-map	配置策略；即流量类与一个或多个操作的关联。
clear configure priority-queue	删除当前优先级队列配置。
show running-config [all] priority-queue	显示当前优先级队列配置。如果您指定 **all** 关键字，则此命令会显示所有当前优先级队列、队列限制和 tx 环限制配置值。

privilege

要配置命令特权级别以与命令授权 （仅本地、 RADIUS 和 LDAP （已映射））一起使用，请在全局配置模式下使用 **privilege** 命令。要禁止配置，请使用此命令的 **no** 形式。

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*

no privilege [**show** | **clear** | **configure**] **level** *level* **mode** *cli_mode*] **command** *command*

语法说明

clear	（可选）设置仅用于该命令的 clear 形式的特权。如果不使用 **clear**、**show** 或 **configure** 关键字，则命令的所有形式都会受到影响。
command *command*	指定正在配置的命令。您仅可配置 *main* 命令的特权级别。例如，您可以配置所有 **aaa** 命令的级别，而非分别配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。
configure	（可选）设置仅用于该命令的 configure 形式的特权。命令的 configure 形式通常是导致配置更改的形式，更改为未修改的命令 （无 **show** 或 **clear** 前缀）或 **no** 形式。如果不使用 **clear**、 **show** 或 **configure** 关键字，则命令的所有形式都会受到影响。
level *level*	指定特权级别；有效值为 0 到 15。较低特权级别编号是较低特权级别。
mode *cli_mode*	（可选）如果可在多个 CLI 模式 （例如用户 EXEC/ 特权 EXEC 模式、全局配置模式或命令配置模式）中输入命令，则您可以分别设置这些模式的特权级别。如果未指定模式，则命令的所有版本使用相同的级别。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，使用 **configure terminal** 命令访问。 • *command_config_mode* - 指定命令配置模式，使用全局配置模式或另一命令配置模式中的命令名称访问。 例如，可在全局配置模式和接口配置模式中输入 **mac-address** 命令。模式关键字让您可以分别为每个模式设置级别。 您不能使用此命令来设置命令的级别。
show	（可选）设置仅用于该命令的 show 形式的特权。如果不使用 **clear**、**show** 或 **configure** 关键字，则命令的所有形式都会受到影响。

默认值

默认情况下，将以下命令分配给特权级别 0。所有其他命令都位于级别 15。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**

- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移动到低于 15 的级别，请务必也将 **configure** 命令移动到该级别，否则用户将无法进入配置模式。

要查看所有特权级别，请参阅 **show running-config all privilege all** 命令。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	添加了对具有 Cisco VSA CVPN3000-Privilege-Level 的 RADIUS 用户的支持。如果使用 **ldap map-attributes** 命令将 LDAP 属性映射到 CVPN3000-Privilege-Level，则会支持 LDAP 用户。

使用指南

privilege 命令让您可以在配置 **aaa authorization command LOCAL** 命令时为 ASA 命令设置特权级别。尽管该命令使用 **LOCAL** 关键字，但此关键字可启用本地、 RADIUS 和 LDAP （已映射）授权。

示例

例如， **filter** 命令具有以下形式：

- **filter** （以 **configure** 选项来表示）
- **show running-config filter**
- **clear configure filter**

您可以分别为每个形式设置特权级别，或通过忽略此选项来为所有形式设置相同的特权级别。例如，分别设置每个形式，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相同的级别：

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 命令可在显示中分离这些形式。

以下示例显示 **mode** 关键字的用途。 **enable** 命令必须从用户 EXEC 模式中输入，可在配置模式中访问的 **enable password** 命令需要最高特权级别。

```
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
```

以下示例在两个模式中显示 **mac-address** 命令，以及 show、 clear 和 cmd 版本的不同级别：

```
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
```

相关命令

命令	说明
clear configure privilege	从配置中删除特权命令语句。
show curpriv	显示当前特权级别。
show running-config privilege	显示命令的特权级别。

prompt

要定制 CLI 提示符，请在全局配置模式下使用 **prompt** 命令。要恢复到默认提示符，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**]

语法说明

cluster-unit	显示集群设备名称。集群中的每个设备可具有唯一名称。
context	（仅限于多模式）显示当前情景。
domain	显示域名。
hostname	显示主机名。
priority	将故障切换优先级显示为 pri （主要）或 sec （辅助）。使用 **failover lan unit** 命令设置优先级。
state	显示设备的流量传递状态或角色。 对于故障切换，将为 **state** 关键字显示以下值： • act - 故障切换已启用，设备正在主动传递流量。 • stby - 故障切换已启用，设备未传递流量且处于待机、故障或其他非活动状态。 • actNoFailover - 故障切换未启用，设备正在主动传递流量。 • stbyNoFailover - 故障切换未启用，设备未传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。 对于集群，将为 **state** 关键字显示以下值： • master • slave 例如，如果您设置 **prompt hostname cluster-unit state**，则在提示符 “ciscoasa/cl2/slave>” 中主机名是 ciscoasa，设备名称是 cl2 且状态名称是 slave。

默认值

默认提示符是主机名。在多情景模式中，当前情景名称 (*hostname*/*context*) 紧随主机名后。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
9.0(1)	添加了 **cluster-unit** 选项。针对集群更新了 **state** 关键字。

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。

通过将信息添加到提示符中的功能，您可以粗略查看在具有多个模块时已登录的 ASA。在故障切换期间，此功能在两个 ASA 具有相同主机名时有用。

示例

以下示例显示对故障切换可用的提示符中的所有可用元素：

```
ciscoasa(config)# prompt hostname context slot state priority
```

提示符将更改为以下字符串：

```
ciscoasa/admin/pri/act(config)#
```

相关命令

命令	说明
clear configure prompt	清除配置的提示符。
show running-config prompt	显示配置的提示符。

propagate sgt

要在接口上启用安全组标记 （称为 **sgt**）传播，请在 cts 手动接口配置模式下使用 **propagate sgt** 命令。要在接口上禁用安全组标记 （称为 **sgt**）传播，请使用此命令的 **no** 形式。

propagate sgt

no propagate sgt

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用传播。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.3(1)	引入了此命令。

使用指南

此命令用于启用和禁用安全组标记在 CTS 第 2 层 SGT 实施中的传播。

限制

- 仅在物理接口、 VLAN 接口、端口通道接口和冗余接口上受支持。
- 在逻辑接口或虚拟接口 （例如 BVI、 TVI 和 VNI）上不受支持。

示例

以下示例为第 2 层 SGT 实施启用接口并表示不传播 SGT：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# no propagate sgt
```

相关命令

命令	说明
cts manual	启用第 2 层 SGT 实施，然后进入 cts 手动接口配置模式。
policy static sgt	将策略应用于手动配置的 CTS 链路。

protocol

要为用于 IKEv2 连接的 IPsec 建议指定协议和加密类型，请从 IPsec 建议配置模式下使用 **protocol** 命令。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**}

语法说明

esp	指定封装式安全措施负载 (ESP) IPsec 协议 （当前仅支持的 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	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
aes-gcm-192	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
aes-gcm-256	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
aes-gmac	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
aes-gmac-192	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
aes-gmac-256	指定要使用哪个 AES-GCM 或 AES-GMAC 算法。
null	不对 ESP 使用加密。
integrity	为 IPsec 协议指定完整性算法。
md5	指定用于 ESP 完整性保护的 md5 算法。
sha-1	（默认）指定安全哈希算法 (SHA) SHA-1，已在美国 联邦信息处理标准 (FIPS) 中定义，用于 ESP 完整性保护。
sha-256	指定哪个算法要用作 IPsec 完整性算法。
sha-384	指定哪个算法要用作 IPsec 完整性算法。
sha-512	指定哪个算法要用作 IPsec 完整性算法。
null	选择是否将 AES-GCM/GMAC 配置为加密算法。

默认值

IPsec 建议的默认设置是加密类型 3DES 和完整性类型 SHA-1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.4(1)	引入了此命令。
9.0(1)	添加了 AES-GCM 或 AES-GMAC 算法支持。增加了选择一种算法以用作 IPsec 完整性算法的功能。

使用指南

IKEv2 IPsec 建议可具有多个加密和完整性类型。使用此命令可指定类型，对等设备可根据需要选取这些类型。

如果将 AES-GMC/GMAC 配置为加密算法，则您必须选择 Null 完整性算法。

示例

以下示例创建 IPsec 建议 *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
```

相关命令

命令	说明
crypto ikev2 enable	在 IPsec 对等设备的通信接口上启用 ISAKMP IKEv2 协商。
crypto ipsec ikev2 ipsec-proposal	创建 IPsec 建议，然后进入 IPsec 建议配置模式，您可以在其中指定建议的多个加密和完整性类型。
show running-config ipsec	显示所有转换集的配置。
crypto map set transform-set	指定要在加密映射条目中使用的转换集。
crypto dynamic-map set transform-set	指定要在动态加密映射条目中使用的转换集。
show running-config crypto map	显示加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。

protocol-enforcement

要启用域名、标签长度和格式检查 （包括压缩和环路指针检查），请在参数配置模式下使用 **protocol-enforcement** 命令。要禁用协议实施，请使用此命令的 **no** 形式。

protocol-enforcement

no protocol-enforcement

语法说明

此命令没有任何参数或关键字。

默认值

默认情况下启用协议实施。配置 **inspect dns** 后 （即使 **policy-map type inspect dns** 未定义）即可启用此功能。要禁用，必须在策略映射配置中明确规定 **no protocol-enforcement**。如果没有配置 **inspect dns**，则不会执行 NAT 重写。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

在某些情况下，即使禁用了该命令，也会执行协议实施。例如，在用于必须解析 DNS 资源记录的其他用途时，例如 DNS 资源记录分类、 NAT 或 TSIG 检查。

示例

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
```

相关命令

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

protocol http

要将 HTTP 指定为检索 CRL 所允许的分发点协议，请在 ca-crl 配置模式下使用 **protocol http** 命令。要删除作为允许的 CRL 检索方法的 HTTP，请使用此命令的 **no** 形式。

protocol http

no protocol http

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为允许 HTTP。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Ca-crl 配置	• 是	• 是	• 是	• 是	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果您使用此命令，请务必将 HTTP 规则分配给公共接口过滤器。获得许可后， CRL 分发点的内容会确定检索方法 （HTTP、 LDAP 和 / 或 SCEP）。

示例

以下示例进入 ca-crl 配置模式，并允许 HTTP 作为用于检索中心信任点的 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

相关命令

命令	说明
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
protocol ldap	将 LDAP 指定为 CRL 的检索方法。
protocol scep	将 SCEP 指定为 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 **protocol ldap** 命令。获得许可后， CRL 分发点的内容会确定检索方法 （HTTP、 LDAP 和 / 或 SCEP）。

要删除作为允许的 CRL 检索方法的 LDAP，请使用此命令的 **no** 形式。

protocol ldap

no protocol ldap

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为允许 LDAP。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入 ca-crl 配置模式，并允许 LDAP 作为用于检索中心信任点的 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

相关命令

命令	说明
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
protocol http	将 HTTP 指定为 CRL 的检索方法
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol scep

要将 SCEP 指定为用于检索 CRL 的分发点协议，请在 crl 配置模式下使用 **protocol scep** 命令。获得许可后， CRL 分发点的内容会确定检索方法 （HTTP、 LDAP 和 / 或 SCEP）。

要删除作为允许的 CRL 检索方法的 SCEP，请使用此命令的 no 形式。

protocol scep

no protocol scep

语法说明

此命令没有任何参数或关键字。

默认值

默认设置为允许 SCEP。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

以下示例进入 ca-crl 配置模式，并允许 SCEP 作为用于检索中心信任点的 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)#
```

相关命令

命令	说明
crl configure	进入 ca-crl 配置模式。
crypto ca trustpoint	进入 trustpoint 配置模式。
protocol http	将 HTTP 指定为 CRL 的检索方法
protocol ldap	将 LDAP 指定为 CRL 的检索方法。

protocol-object

要将协议对象添加到协议对象组中，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*

语法说明

protocol	协议名称或编号。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

protocol-object 命令与 **object-group** 命令一起使用，用于在协议配置模式中定义协议对象。

您可以使用 *protocol* 参数来指定 IP 协议名称或编号。udp 协议编号是 17，tcp 协议编号是 6，egp 协议编号是 47。

示例

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)#
```

相关命令

命令	说明
clear configure object-group	从配置中删除所有 **object group** 命令。
group-object	添加网络对象组。
network-object	将网络对象添加到网络对象组。
object-group	定义对象组以优化配置。
show running-config object-group	显示当前对象组。

protocol-violation

要通过 HTTP 和 NetBIOS 检查定义发生协议违反行为时的操作，请在参数配置模式下使用 **protocol-violation** 命令。要禁用此功能，请使用此命令的 **no** 形式。

protocol-violation action [**drop** [**log**] | **log**]

no protocol-violation action [**drop** [**log**] | **log**]

语法说明

drop	指定将丢弃不符合协议的数据包。
log	指定将记录协议违反行为。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

此命令可在 HTTP 或 NetBIOS 策略映射中配置。当 HTTP 或 NetBIOS 解析器无法在消息的前几个字节中检测到有效 HTTP 或 NetBIOS 消息时，将会发出系统日志。例如，当数据块编码形式不正确且无法解析该消息时会发生这种情况。

示例

以下示例显示如何在策略映射中设置用于协议违反行为的操作：

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

相关命令

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

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**]

语法说明 I

sdi	将 RADIUS/TACACS SDI 代理消息解析为本地 SDI 指令。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用 **proxy-auth** 命令来启用将 AAA 服务器代理身份验证文本消息解析为本地协议指令。

proxy-auth_map sdi

要将从 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 服务器配置模式下使用 **proxy-auth_map sdi** 命令。

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

语法说明 I

radius_challenge_message	指定用于映射特定 SDI 消息的 RADIUS 质询消息，可以是以下任何一个： • new-pin-meth—New PIN Method, [default] Do you want to enter your own pin • new-pin-reenter—Reenter new PIN, [default] Reenter PIN: • new-pin-req—New PIN requested, [default] Enter your new Alpha-Numerical PIN • new-pin-sup—New PIN supplied, [default] Please remember your new PIN • new-pin-sys-ok—New PIN accepted, [default] New PIN Accepted • next-ccode-and-reauth—Reauthenticate on token change, [default] new PIN with the next card code • next-code—Provide the tokencode without PIN, [default] Enter Next PASSCODE • ready-for-sys-pin—Accept system generated PIN, [default] ACCEPT A SYSTEM GENERATED PIN
sdi_message	指定本地 SDI 消息。

默认值

ASA 上的默认映射对应于思科 ACS （包括系统管理、配置和 RSA SecureID 提示符）上的默认设置，还会与 RSA Authentication Manager 上的默认设置同步。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

要启用解析和映射来自 RADIUS 代理的 RADIUS 质询消息，您必须在隧道组配置模式中启用 **proxy-auth** 命令。然后使用默认映射值。您可以使用 **proxy-auth_map** 命令更改默认映射值。

远程用户可使用 AnyConnect 客户端连接到 ASA，然后尝试使用 RSA SecurID 令牌进行身份验证。 ASA 可配置为使用 RADIUS 代理服务器，该服务器进而与 SDI 服务器进行有关该身份验证的通信。

在身份验证期间，RADIUS 服务器将访问质询消息呈现给 ASA。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。与 ASA 通过 RADIUS 代理通信相比，当 ASA 与 SDI 服务器直接通信时的消息文本是不同的。

因此，要对 AnyConnect 客户端显示为本地 SDI 服务器，ASA 必须解释来自 RADIUS 服务器的消息。此外，由于 SDI 消息在 SDI 服务器上是可配置的，ASA 上的消息文本必须与 SDI 服务器上的消息文本 （全部或部分）相匹配。否则，对远程客户端用户显示的提示符可能不适用于在身份验证期间所需的操作。 AnyConnect 客户端可能无法响应，且身份验证可能失败。

相关命令

命令	说明
proxy-auth	启用对来自 RADIUS 代理的 RADIUS 质询消息的解析和映射。

proxy-bypass

要配置 ASA 以执行最少的内容重写，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。要禁用代理旁路，请使用该命令的 **no** 形式。

proxy-bypass interface *interface name* {**port** *port number***| path-mask** *path mask*} **target** *url* **[rewrite** {**link | xml | none**}**]**

no proxy-bypass interface *interface name* {**port** *port number***| path-mask** *path mask*} **target** *url* **[rewrite** {**link | xml | none**}**]**

语法说明 |

host	标识要向其转发流量的主机。使用主机 IP 地址或主机名。
interface	标识代理旁路的 ASA 接口。
interface name	按名称指定 ASA 接口。
link	指定绝对外部链路的重写。
none	指定无重写。
path-mask	指定要匹配的模式。
path-mask	指定要匹配的模式，可包含正则表达式。您可以使用以下通配符： * - 与所有内容匹配。您不能单独使用此通配符。它必须附带字母数字字符串。 ？ - 与任何单个字符匹配。 [!seq] - 与不在序列中的任何字符匹配。 [seq] - 与序列中的任何字符匹配。 最多 128 个字节。
port	标识为代理旁路保留的端口。
port number	指定为代理旁路保留的高编号端口。端口范围为 20000 到 21000。您可以仅对一个代理旁路规则使用一个端口。
rewrite	（可选）指定重写的附加规则：无规则或 XML 与链路的组合。
target	标识要向其转发流量的远程服务器。
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，除非您指定了另一个端口。
xml	指定重写 XML 内容。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

将代理旁路用于应用和 Web 资源，它们可在内容重写极少时发挥更好作用。代理旁路命令确定如何处理通过 ASA 的特定 Web 应用。

您可以多次使用此命令。您配置条目的顺序并不重要。接口和路径掩码或接口和端口用于唯一标识代理旁路规则。

如果您使用端口而非路径掩码配置代理旁路 （具体取决于您的网络配置），则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。但是，请注意，该路径掩码可更改，因此您可能需要使用多个路径掩码语句来穷尽可能性。

在 URL 中， .com 或 .org 或其他类型的域名后面的内容都是路径。例如，在 URL www.example.com/hrbenefits 中，*hrbenefits* 是路径。同样，对于 URL www.example.com/hrinsurance，*hrinsurance* 是路径。如果您想要将代理旁路用于所有 hr 站点，则您可以通过使用 * 通配符 （如 /hr*）来避免多次使用该命令。

示例

以下示例显示如何配置 ASA，以通过 WebVPN 接口将端口 20001 用于代理旁路，使用 HTTP 及其默认端口 80 将流量转发到 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 mypath/* 用于代理旁路，使用 HTTP 及其默认端口 443 将流量转发到 example.com 并重写 XML 和链路内容。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://example.com rewrite xml,link
```

相关命令

命令	说明
apcf	指定要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

要发出 TLS 代理本地动态证书，请在加密 CA 信任点配置模式下使用 **proxy-ldc-issuer** 命令。要删除配置，请使用此命令的 **no** 形式。

proxy-ldc-issuer

no proxy-ldc-issuer

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **proxy-ldc-issuer** 命令可发出 TLS 代理本地动态证书。**proxy-ldc-issuer** 命令可授予加密信任点发出 LDC 的本地 CA 的角色，您可从加密 CA 信任点配置模式中访问它。

proxy-ldc-issuer 命令可为信任点定义本地 CA 角色，以发出 TLS 代理的动态证书。此命令仅可通过 “ 自助注册 ” 在信任点下配置。

示例

以下示例显示如何创建内部本地 CA 来签署用于电话的 LDC。此本地 CA 已创建为常规自签信任点且已启用 **proxy-ldc-issuer**。

```
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
```

相关命令

命令	说明
ctl-provider	定义 CTL 提供程序实例，然后进入提供程序配置模式。
server trust-point	指定要在 TLS 握手期间提供的代理信任点证书。
show tls-proxy	显示 TLS 代理。
tls-proxy	定义 TLS 代理实例，然后设置最大会话数。

proxy-server

要为 Phone Proxy （电话代理）功能配置 HTTP 代理 （写入 IP 电话配置文件中的 <proxyServerURL> 标记下），请在电话代理配置模式下使用 **proxy-server** 命令。要从 Phone Proxy （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*] **interface** *ifc*

no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

语法说明

interface *ifc*	指定 ASA 上用于驻留 HTTP 代理的接口。
ip_address	指定 HTTP 代理的 IP 地址。
listen_port	指定 HTTP 代理的侦听端口。如果未指定，默认端口为 8080。

默认值

如果未指定侦听端口，则该端口将默认配置为 8080。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

通过为电话代理设置代理服务器配置选项，可允许 HTTP 代理位于 DMZ 或外部网络上，其中所有 IP 电话 URL 都指向代理服务器来提供电话上的服务。此设置可调节不安全的 HTTP 流量，禁止其返回到公司网络中。

您输入的 *ip_address* 应该是基于 IP 电话和 HTTP 代理服务器所在位置的全局 IP 地址。

如果代理服务器位于 DMZ 中且 IP 电话位于网络以外，则 ASA 会进行查找以查看是否存在 NAT 规则，并使用全局 IP 地址来写入配置文件中。

由于 ASA 会将主机名解析为 IP 地址，因此当 ASA 可将主机名解析为 IP 地址时 （例如已配置 DNS 查找），您可以在 *ip_address* 参数中输入该主机名。

默认情况下，在 Enterprise Parameters （企业参数）下配置的 Phone URL Parameters （电话 URL 参数）会使用 URL 中的 FQDN。如果用于 HTTP 代理的 DNS 查找不能解析 FQDN，则可能需要更改参数以使用 IP 地址。

为确保代理服务器 URL 正确写入 IP 电话配置文件中，请检查 Settings （设置） > Device Configuration （设备配置） > HTTP configuration （HTTP 配置） > Proxy Server URL （代理服务器 URL）下的 IP 电话上的 URL。

电话代理不会检测这种流向代理服务器的 HTTP 流量。

如果 ASA 在 IP 电话和 HTTP 代理服务器的路径中，请使用现有调试技术 （例如系统日志和捕捉）对代理服务器进行故障排除。

电话代理正在使用时，您仅可配置一个代理服务器；但是，如果在配置代理服务器后 IP 电话已下载其配置文件，则您必须重启 IP 电话，以便它们获取包含代理服务器地址的配置文件。

示例

以下示例显示使用 **proxy-server** 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
```

相关命令

命令	说明
phone-proxy	配置电话代理实例。

publish-crl

要允许其他 ASA 验证本地 CA 发出的证书的撤销状态，请在 CA 服务器配置模式下使用 **publish-crl** 命令来允许直接从 ASA 上的接口下载 CRL。要禁止下载 CRL，请使用此命令的 **no** 形式。

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

语法说明

interface *interface*	指定用于接口的 *nameif*，例如 **gigabitethernet0/1**。请参阅 **interface** 命令获取详细信息。
port *portnumber*	（可选）指定接口设备用于下载 CRL 的端口。端口号可以在 1 到 65535 的范围内。

默认值

默认 **publish-crl** 状态是 **no publish**。 TCP 端口 80 是 HTTP 的默认端口。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

默认情况下无法访问 CRL。您必须在接口和所需端口上启用对 CRL 文件的访问。

TCP 端口 80 是 HTTP 默认端口号。如果您配置非默认端口 （除端口 80 以外），请确保 **cdp-url** 配置中包括新端口号，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 会嵌入到任何已发出的证书中。如果您没有为 CDP 配置特定位置，则默认 CDP URL 是：http://hostname.domain/+CSCOCA+/asa_ca.crl。

如果同一接口上启用了无客户端 SSL VPN，则 HTTP 重定向和 CRL 下载请求会由同一 HTTP 侦听程序处理。侦听程序将检查传入的 URL，如果它与使用 **cdp-url** 命令配置的 URL 相匹配，则会下载 CRL 文件。如果 URL 与 **cdp-url** 命令不匹配，则连接会重定向到 HTTPS （如果已启用 HTTP 重定向）。

示例

publish-crl 命令示例 （在 CA 服务器配置模式中输入）为 CRL 下载启用了外部接口的端口 70：

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

相关命令

命令	说明
cdp-url	为自动生成的 CRL 指定特定位置。
show interface	显示接口的运行状态和统计信息。

pwd

要显示当前工作目录，请在特权 EXEC 模式下使用 **pwd** 命令。

pwd

语法说明

此命令没有任何参数或关键字。

默认值

根目录 (/) 是默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0	引入了此命令。

使用指南

此命令在功能上类似于 **dir** 命令。

示例

以下示例显示如何显示当前工作目录：

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

相关命令

命令	说明
cd	将当前工作目录更改为指定的目录。
dir	显示目录内容。
more	显示文件的内容。

第 18 章

queue-limit 至 reset 命令

queue-limit (priority-queue)

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

注　ASA 5580 万兆位以太网接口上不支持此命令。（ASA 5585-X 上的优先级队列支持万兆位以太网接口。） ASA 5512-X 到 ASA 5555-X 管理接口也不支持此命令。

ASA 服务模块上不支持此命令。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

语法说明

number-of-packets	指定在接口开始丢弃数据包前可排队 （即缓冲）的最大低延迟或普通优先级数据包数。值的范围的上限会在运行时动态确定。要查看此限制，请在命令行上输入 **help** 或 **?**。关键决定因素是设备上支持队列所需的内存和可用内存。队列不得超过可用内存。最大理论数据包数是 2147483647。

默认值

默认队列限制为 1024 个数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

ASA 允许两个流量类：用于具有较高优先级的延迟敏感型流量 （例如语音和视频）的低延迟队列 (LLQ)，以及用于所有其他流量的 “ 尽力而为 ” 队列 （默认）。 ASA 标识优先级流量，并实施适当的服务质量 (QoS) 策略。您可以配置优先级队列的大小和深度以微调流量。

注　您*必须*配置 **priority-queue** 命令以对接口启用优先级队列。

您可以将一个 **priority-queue** 命令应用于可由 **nameif** 命令定义的任何接口。

如提示中所示， **priority-queue** 命令进入优先级队列配置模式。在优先级队列配置模式下，在任何给定时间，您可以通过 **tx-ring-limit** 命令配置传输队列中允许的最大数据包数，通过 **queue-limit** 命令配置在丢弃数据包前允许缓冲的任一类型（优先级或尽力而为）的数据包数。

您指定的 tx 环限制和队列限制会同时影响具有较高优先级的低延迟队列和“尽力而为”队列。tx 环限制指允许进入驱动程序的任一类型的数据包的数量。若超过该数量，驱动程序会将数据包推回位于接口前的队列以缓冲数据包，直到拥塞清除为止。通常情况下，您可以调整这两个参数来优化低延迟流量的流动。

队列大小并非无限的，因此它们会充满并溢出。当队列充满时，任何其他数据包都无法进入队列而被丢弃。这称为 *tail drop*（队尾丢弃）。为避免让队列充满，您可以使用 **queue-limit** 命令增加队列缓冲区大小。

示例

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
```

相关命令

命令	说明
clear configure priority-queue	在指定接口上删除当前优先级队列配置。
priority-queue	在接口上配置优先级队列。
show priority-queue statistics	为指定接口显示优先级队列统计数据。
show running-config [all] priority-queue	显示当前优先级队列配置。如果您指定 **all** 关键字，则此命令会显示所有当前优先级队列、队列限制和 tx 环限制配置值。
tx-ring-limit	在以太网传输驱动程序中设置可在任何给定时间排队的最大数据包数。

queue-limit (tcp-map)

要配置可缓冲的最大无序数据包数，并排列其顺序以用于 TCP 连接，请在 TCP 映射配置模式下使用 **queue-limit** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令是使用 **set connection advanced-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

语法说明

pkt_num	指定可缓冲的最大无序数据包数（1 到 250 之间），并排列其顺序以用于 TCP 连接。默认值为 0，这意味着禁用此设置，且会根据流量类型使用默认系统队列限制。有关更多信息，请参阅“使用指南”部分。
timeout *seconds*	（可选）设置无序数据包可在缓冲区中停留的最大时间量（1 到 20 秒之间）。默认值为 4 秒。如果数据包未按顺序排列且未在超时期间内传递，则会丢弃它们。如果 *pkt_num* 参数设置为 0，则您无法为任何流量更改超时；您需要将**限制**设置为 1 或以上以使 **timeout** 关键字生效。

默认值

默认设置是 0，这意味着禁用此命令。

默认超时为 4 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(4)/8.0(4)	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 映射配置模式下，您可以输入 **queue-limit** 命令和许多其他命令。
2. **class-map** - 标识要执行 TCP 规范化的流量。
3. **policy-map** - 标识与每个类映射关联的操作。
   a. **class** - 标识您要对其执行操作的类映射。
   b. **set connection advanced-options** - 标识您创建的 TCP 映射。
4. **service-policy** - 向接口分配策略映射或全局分配策略映射。

如果您未启用 TCP 规范化，或 **queue-limit** 命令设置为默认值 0 （这意味着禁用此命令），则会根据流量类型使用默认系统队列限制：

- 用于应用检查 （**inspect** 命令）、 IPS （**ips** 命令）和 TCP 检查重新传输 （TCP 映射 **check-retransmission** 命令）的连接具有 3 个数据包的队列限制。如果 ASA 收到具有不同窗口大小的 TCP 数据包，则会动态更改队列限制以匹配通告设置。
- 对于其他 TCP 连接，无序数据包会按原样通过。

如果您将 **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的数量都会匹配此设置。例如，对于应用检查、IPS 和 TCP 检查重新传输流量，为支持 **queue-limit** 设置会忽略来自 TCP 数据包的任何通告设置。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。

示例

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)#
```

相关命令

命令	说明
class-map	为服务策略标识流量。
policy-map	标识要应用于服务策略中的流量的操作。
set connection advanced-options	启用 TCP 规范化。
service-policy	将服务策略应用于接口。
show running-config tcp-map	显示 TCP 映射配置。
tcp-map	创建 TCP 映射，并允许对 TCP 映射配置模式的访问。

quit

要退出当前配置模式，或从特权或用户 EXEC 模式中注销，请使用 **quit** 命令。

quit

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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

当您在特权或用户 EXEC 模式下输入 **quit** 命令时，您会从 ASA 注销。使用 **disable** 命令可从特权 EXEC 模式返回到用户 EXEC 模式。

示例

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>
```

相关命令

命令	说明
exit	退出配置模式或从特权或用户 EXEC 模式中注销。

quota management-session

要设置 ASA 上允许的并发 ASDM、 SSH 和 Telnet 会话的最大数量，请在全局配置模式下使用 **quota management-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 *number*

no quota management-session *number*

语法说明

number	指定允许的并发 ASDM、 SSH 和 Telnet 会话的最大数量。有效值为从 0 到 10,000。

默认值

默认值为 0，这意味着没有会话限制。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.1(2)	引入了此命令。

使用指南

当达到配额时，后续管理会话请求均会遭到拒绝，并生成系统日志消息。管理会话配额机制不会拦截控制台会话，以阻止设备锁定。

示例

以下示例将管理会话配额配置为 100：

```
ciscoasa(config)# quota management-session 100
```

相关命令

命令	说明
show run quota management-session	显示管理会话配额的当前值。
show quota management-session	显示用于管理会话的统计数据。

radius-common-pw

要为通过 ASA 访问 RADIUS 授权服务器的所有用户指定要使用的常用密码，请在 AAA 服务器主机配置模式下使用 **radius-common-pw** 命令。要删除此指定，请使用此命令的 **no** 形式。

radius-common-pw *string*

no radius-common-pw

语法说明

string	将包含最多 127 个字符、区分大小写的字母数字关键字用作与 RADIUS 服务器的所有授权业务的常用密码。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

此命令仅对 RADIUS 授权服务器有效。

RADIUS 授权服务器要求每个连接用户提供用户名和密码。ASA 会自动提供用户名。您可以在此处输入密码。 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 向服务器授权的每个用户相关联。请务必向您的 RADIUS 服务器管理员提供此信息。

如果您未指定常用用户密码，则每个用户密码就是用户名。如果您将用户名作为常用用户密码，则为安全起见，不要在您网络以外的任何地方使用 RADIUS 服务器进行授权。

注　*string* 参数基本上被空格填充。 RADIUS 服务器期望获取该参数且需要它，但不会使用它。用户无需了解此参数。

示例

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，将重试时间间隔设置为 7 秒，并将 RADIUS 常用密码配置为 “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)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，以便能够配置特定于主机的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

radius-reject-message

要启用当身份验证被拒绝时在登录屏幕上显示 RADIUS 拒绝消息，请从隧道组 WebVPN 属性配置模式中使用 **radius-eject-message** 命令。要从配置中删除该命令，请使用该命令的 **no** 形式：

radius-reject-message

no radius-reject-message

默认值

默认设置为禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

如果要向远程用户显示有关身份验证故障的 RADIUS 消息，请启用此命令。

示例

以下示例为名为 engineering 的连接配置文件启用 RADIUS 拒绝消息显示：

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

radius-with-expiry (removed)

要让 ASA 在身份验证期间使用 MS-CHAPv2 与用户协商密码更新，请在隧道组 IPsec 属性配置模式下使用 **radius-with-expiry** 命令。要恢复默认值，请使用此命令的 **no** 形式。

radius-with-expiry

no radius-with-expiry

语法说明

此命令没有任何参数或关键字。

默认值

禁用此命令的默认设置。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.1(1)	此命令已弃用。 **password-management** 命令取代了它。不再支持 **radius-with-expiry** 命令的 **no** 形式。
8.0(2)	此命令已弃用。

使用指南

此属性仅可应用于 IPsec 远程访问隧道组类型。如果尚未配置 RADIUS 身份验证，则 ASA 会忽略此命令。

示例

以下示例在配置 IPsec 配置模式下输入，对名为 remotegrp 的远程访问隧道组配置 Radius with Expiry：

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

相关命令

命令	说明
clear configure tunnel-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，此命令会取代 **radius-with-expiry** 命令。
show running-config tunnel-group	显示指定的证书映射条目。
tunnel-group ipsec-attributes	为此组配置隧道组 IPsec 属性。

range

要为网络对象配置一个地址范围，请在对象配置模式下使用 **range** 命令。使用此命令的 **no** 形式可从配置中删除该对象。

range *ip_addr_1 ip_addr2*

no range *ip_addr_1 ip_addr2*

语法说明

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

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.3(1)	引入了此命令。
9.0(1)	添加了对 IPv6 地址的支持。

使用指南

如果您使用不同的 IP 地址配置现有网络对象，则新配置将取代现有配置。

示例

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
```

相关命令

命令	说明
clear configure object	清除创建的所有对象。
description	将说明添加到网络对象。
fqdn	指定完全限定域名网络对象。
host	指定主机网络对象。
nat	对网络对象启用 NAT。
object network	创建网络对象。
object-group network	创建网络对象组。
show running-config object network	显示网络对象配置。
subnet	指定子网的网络对象。

ras-rcf-pinholes

要在网守位于网络内部时在 H.323 终端之间启用呼叫设置，请在参数配置模式下使用 **ras-rcf-pinholes** 命令。要禁用此功能，请使用此命令的 **no** 形式。

ras-rcf-pinholes enable

no ras-rcf-pinholes enable

语法说明

enable	在 H.323 终端之间启用呼叫设置。

默认值

默认情况下，禁用此选项。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(5)	引入了此命令。

使用指南

ASA 包括为基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息的呼叫打开针孔的选项。由于这些 RRQ/RCF 消息的发送方和接收方是网守，呼叫终端的 IP 地址是未知的，且 ASA 会通过源 IP 地址 / 端口 0/0 打开针孔。

示例

以下示例显示如何在策略映射中设置操作，为这些呼叫打开针孔：

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

相关命令

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

rate-limit

使用 模块化策略框架 时，通过在匹配或类配置模式下使用 **rate-limit** 命令，可为匹配 **match** 命令或类映射的数据包限制消息的速率。此速率限制操作在用于应用流量的检查策略映射（**policy-map type inspect** 命令）中可用；但是，并非所有应用允许此操作。要禁用此操作，请使用此命令的 **no** 形式。

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

语法说明

messages_per_second	限制每秒的消息数。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。输入 **match** 或 **class** 命令（**class** 命令是一个现有的 **class-map type inspect** 命令，后者又包括 **match** 命令）来标识应用流量后，您可以输入 **rate-limit** 命令来限制消息的速率。

当您在 3/4 层策略映射 （**policy-map** 命令）中使用 **inspect** 命令启用应用检查时，您可以启用包含此操作的检查策略映射，例如，输入 **inspect dns dns_policy_map** 命令，其中 dns_policy_map 是检查策略映射的名称。

示例

以下示例将邀请请求限制为每秒 100 个消息：

```
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
```

相关命令

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

reactivation-mode

要指定重新激活组中出现故障的服务器的方法，请在 AAA 服务器协议模式下使用 **reactivation-mode** 命令。要删除此指定，请使用此命令的 **no** 形式。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

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

语法说明

deadtime *minutes*	（可选）指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时间量，以分钟为单位 （0 到 1440 之间）。默认值为 10 分钟。
depletion	仅在组内所有服务器均为非活动状态后重新激活出现故障的服务器。
timed	在 30 秒钟的停机时间后重新激活出现故障的服务器。

默认值

默认重新激活模式是耗尽，且默认死区时间值是 10。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
AAA 服务器协议配置	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

每个服务器组均具有一项属性，即为其服务器指定重新激活策略。

在 **depletion** 模式下，当停用一台服务器时，它会保持非活动状态直到组内所有其他服务器为非活动状态。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。**deadtime** 参数指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时间量 （以分钟为单位）。仅当服务器组正在与本地回退功能结合使用时，此参数才有意义。

在 **timed** 模式下，出现故障的服务器会在 30 秒钟的停机时间后重新激活。当客户将服务器列表中的第一台服务器用作主服务器且希望它尽可能随时在线时，这点十分有用。在使用 UDP 服务器的情况下，此策略无效。由于与 UDP 服务器进行连接不会失败，即使不存在服务器， UDP 服务器也会被盲目地置于在线状态。如果服务器列表中包含多台无法访问的服务器，则这样可能会导致连接缓慢或出现连接故障。

已启用并发记账的记账服务器组被强制使用 **timed** 模式。这意味着给定列表中的所有服务器都是等效的。

示例

以下示例配置一台名为 “svrgrp1” 的 TACACS+ AAA 服务器来使用耗尽重新激活模式，其中死区时间为 15 分钟：

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

以下示例配置一台名为 “srvgrp1” 的 TACACS+ AAA 服务器来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)#
```

相关命令

accounting-mode	表示是否将记账消息发送到一台服务器或发送到组内所有服务器。
aaa-server protocol	进入 AAA 服务器组配置模式，以便您配置特定于组且组内所有主机公用的 AAA 服务器参数。
max-failed-attempts	指定服务器组中的任何给定服务器在被停用前可容忍的故障数。
clear configure aaa-server	删除所有 AAA 服务器配置。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定组内特定服务器或特定协议的 AAA 服务器统计信息。

record-entry

要指定用于创建 CTL 文件的信任点，请在 CTL 文件配置模式下使用 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 [capf | cucm | cucm-tftp | tftp] trustpoint *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

no record-entry [capf | cucm | cucm-tftp | tftp] trustpoint *trust_point* **address** *ip_address* [**domain-name** *domain_name*]

语法说明

capf	指定此信任点的角色是 CAPF。仅可配置一个 CAPF 信任点。
cucm	指定此信任点的角色是 CCM。可以配置多个 CCM 信任点。
cucm-tftp	指定此信任点的角色是 CCM+TFTP。可以配置多个 CCM+TFTP 信任点。
domain-name *domain_name*	（可选）指定信任点的域名，用于为该信任点创建 DNS 字段。将此域名附加到 Subject DN（主题 DN）的 Common Name（公用名称）字段中以创建 DNS 名称。当未为信任点配置 FQDN 时应配置域名。
address *ip_address*	指定信任点的 IP 地址。
tftp	指定此信任点的角色是 TFTP。可以配置多个 TFTP 信任点。
trustpoint *trust_point*	设置安装的信任点的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(4)	引入了此命令。

使用指南

仅可指定一个域名。如果 CTL 文件不存在，则手动将此证书从 CUCM 导出到 ASA 中。

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

您在 *ip_address* 参数中指定的 IP 地址必须是 IP 电话可看到的全局地址或地址，因为它会是用于信任点的 CTL 记录的 IP 地址。

为 CTL 文件中所需的每个实体添加附加记录条目配置。

示例

以下示例显示使用 **record-entry** 命令来指定要用于创建 CTL 文件的信任点：

```
ciscoasa(config-ctl-file)# record-entry cucm-tftp trustpoint cucm1 address 192.168.1.2
```

相关命令

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

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，请在全局配置模式下使用 **redirect-fqdn enable** 命令。

redirect-fqdn {**enable** | **disable**}

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

注　要使用 VPN 负载平衡，您必须具有带 Plus 许可的 ASA 型号 5510 或 ASA 型号 5520 或更高版本。VPN 负载平衡还需要具有一个有效的 3DES/AES 许可。在启用负载平衡前，安全设备会检查是否存在此加密许可。如果它检测不到有效的 3DES 或 AES 许可，则安全设备会阻止负载平衡启用，还会通过负载平衡系统阻止内部配置 3DES，除非许可允许此使用。

语法说明

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

默认值

默认情况下禁用此行为。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
VPN 负载平衡模式	• 是	—	• 是	—	—

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

默认情况下， ASA 仅向客户端发送负载平衡重定向中的 IP 地址。如果正在使用基于 DNS 名称的证书，则证书会在重定向到辅助设备时失效。

作为 VPN 主集群，此 ASA 在将 VPN 客户端连接重定向到该集群设备时可使用集群设备 （集群中的另一个 ASA）的反向 DNS 查找 （而非其外部 IP 地址）来发送完全限定域名 (FQDN)。

集群中的负载平衡设备上的所有外部和内部网络接口必须在同一 IP 网络上。

要使用 FQDN （而非 IP 地址）执行 WebVPN 负载平衡，您必须执行以下配置步骤：

步骤 1　使用 **redirect-fqdn enable** 命令启用用于负载平衡的 FQDN。

步骤 2　将用于每个 ASA 外部接口的条目添加到您的 DNS 服务器 （如果此类条目尚未存在）。每个 ASA 外部 IP 地址都应具有一个与其关联的 DNS 条目用于查找。还必须启用这些 DNS 条目用于反向查找。

步骤 3　使用命令 “dns domain-lookup inside”（或任何一个具有到您的 DNS 服务器的路由的接口）在您的 ASA 上启用 DNS 查找。

步骤 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）。

示例

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，其中包括可为完全限定域名启用重定向的接口命令，并将集群的公共接口指定为 “test”，将集群的专用接口指定为 “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
```

相关命令

命令	说明
clear configure vpn load-balancing	删除负载平衡运行时配置并禁用负载平衡。
show running-config vpn load-balancing	显示当前 VPN 负载平衡虚拟集群配置。
show vpn load-balancing	显示 VPN 负载平衡运行时统计数据。
vpn load-balancing	进入 VPN 负载平衡模式。

redistribute

要重分布从一个路由域到另一个路由域的路由，请在适当的配置模式下使用 **redistribute** 命令。要禁用重分布，请使用此命令的 **no** 形式。

redistribute *protocol* [*process-id*] [*autonomous-system-number*][**metric** {*metric-value* | **transparent**}][**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] [*autonomous-system-number*][**metric** {*metric-value* | **transparent**}][**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

语法说明

protocol	要从其重分布路由的源协议。它可以是以下关键字之一： **bgp**、 **connected**、 **eigrp**、 **ospf**、 **static** 或 **rip**。 **static** 关键字用于重分布 IP 静态路由。 **connected** 关键字是指通过在接口上启用 IP 自动建立的路由。对于路由协议 （例如开放最短路径优先 (OSPF)），会重分布这些路由作为自主系统的外部路由。
process-id	（可选）对于 **bgp** 或 **eigrp** 关键字，这是自主系统编号，一个 16 位十进制数。 对于 **ospf** 关键字，这是适当的 OSPF 进程 ID，可从其重分布路由。这会标识路由过程。此值采用非零十进制数的形式。 对于 **rip** 关键字，不需要 *process-id* 值。 默认情况下不定义进程 ID。
autonomous-system-number	（可选）用于重分布的路由的自主系统编号。编号在从 1 到 65535 的范围内。 • 在思科 IOS 版本 12.0(32)SY8、 12.0(33)S3、 12.2(33)SRE、 12.2(33)XNE、 12.2(33)SXI1、思科 IOS XE 版本 2.4 及更高版本中，采用 asplain 标记法支持从 65536 到 4294967295 范围内的 4 个字节自主系统编号，采用 asdot 标记法支持从 1.0 到 65535.65535 范围内的 4 个字节自主系统编号。 • 在思科 IOS 版本 12.0(32)S12、12.4(24)T 和思科 IOS XE 版本 2.3 中，仅采用 asdot 标记法支持从 1.0 到 65535.65535 范围内的 4 个字节自主系统编号。 有关自主系统编号格式的更多详情，请参阅 **router bgp** 命令。
metric *metric-value*	（可选）当在同一路由器上从一个 OSPF 进程到另一个 OSPF 进程进行重分布时，如果未指定任何指标值，则会将指标从一个进程携带至另一个进程。当将其他进程重分布给一个 OSPF 进程时，如果未指定任何指标值，则默认指标是 20。默认值为 0。
metric transparent	（可选）导致 RIP 将用于重分布的路由的路由表指标用作 RIP 指标。

metric-type *type-value*	（可选）对于 OSPF，指定与通告到 OSPF 路由域中的默认路由相关联的外部链路类型。它可以是两个值之一： • **1** - 类型 1 外部路由 • **2** - 类型 2 外部路由 如果未指定 **metric-type**，则思科 IOS 软件采用类型 2 外部路由。
match {internal | external 1 | external 2}	（可选） OSPF 路由重分布到其他路由域所依据的标准。它可以是下列类型之一： • **internal （内部）** - 特定自主系统内部的路由。 • **external 1 （外部 1）** - 自主系统外部的路由，但会将其作为类型 1 外部路由导入到 OSPF 中。 • **external 2 （外部 2）** - 自主系统外部的路由，但会将其作为类型 1 外部路由导入到 OSPF 中。 默认为 internal （内部）和 external 1 （外部 1）。
tag *tag-value*	（可选）指定附加到每个外部路由的 32 位十进制值。OSPF 本身不使用此值。可以使用它在自主系统边界路由器 (ASBR) 之间传递信息。如果未指定任何值，则会将远程自主系统编号用于来自边界网关协议 (BGP) 和外部网关协议 (EGP) 的路由；对于其他协议，使用零 (0)。
route-map	（可选）指定应询问的路由映射，以过滤从此源路由协议导入当前路由协议的路由。如果未指定，将重分布所有路由。如果指定此关键字，但没有列出路由映射标记，则不会导入任何路由。
map-tag	（可选）配置的路由映射的标识符。
subnets	（可选）将路由重分布到 OSPF 时，特定协议的重分布范围。默认情况下不定义子网。
nssa-only	（可选）为重分布到 OSPF 中的所有路由设置 nssa-only 属性。

默认值

禁用路由重分布。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

更改或禁用任何关键字不会影响其他关键字的状态。

一台接收带有内部指标的链路状态协议的路由器会考虑从自身到重分布的路由器的路由成本，以及到达目标的通告成本。外部指标仅考虑到达目标的通告指标。

必须通过 **distribute-list out** 路由器配置命令过滤重分布的路由信息。本指南可确保仅将由管理员准备的这些路由传递给接收的路由协议。

只要您使用 **redistribute** 或 **default-information** 路由器配置命令将路由重分布到 OSPF 路由域中，路由器都会自动成为 ASBR。但是，默认情况下， ASBR 不会生成一条到 OSPF 路由域中的*默认路由*。

若从除 OSPF 或 BGP 外的协议将路由重分布到 OSPF 中，且尚未使用 **metric-type** 关键字和 *type-value* 参数指定任何指标，则 OSPF 会使用 20 作为默认指标。若从 BGP 将路由重分布到 OSPF 中， OSPF 会使用 1 作为默认指标。若将路由从一个 OSPF 进程到另一个 OSPF 进程进行重分布，则外部自主系统 (AS) 和末节区域 (NSSA) 路由会使用 20 作为默认指标。若区域内和区域间路由在 OSPF 进程之间进行重分布，则在重分布目标进程中将来自重分布源进程的内部 OSPF 指标通告为外部指标。（仅在这种情况下才会当将路由重分布到 OSPF 中时保留路由表指标。）

当将路由重分布到 OSPF 中时，如果未指定 **subnets** 关键字，则仅重分布未划分子网的路由。

在 NSSA 区域内部的路由器上，**nssa-only** 关键字会导致最初的类型 7 NSSA LSA 将其传播 (P) 位设置为零，这样可阻止区域边界路由器将这些 LSA 转换为类型 5 外部 LSA。在与 NSSA 和正常区域连接的区域边界路由器上， **nssa-only** 关键字会导致将路由仅重分布到 NSSA 区域中。

使用受此 **redistribute** 命令影响的 **connected** 关键字配置的路由是未通过 **network** 路由器配置命令指定的路由。

您无法使用 **default-metric** 命令影响用于通告连接的路由的指标。

注　**redistribute** 命令中指定的 **metric** 值会取代使用 **default-metric** 命令指定的 **metric** 值。

除非指定 **default-information originate** 路由器配置命令，否则不允许将 IGP 或 EGP 默认重分布到 BGP 中。

使用 redistribute 命令的 no 形式

删除为 **redistribute** 命令配置的选项需要您谨慎使用 **redistribute** 命令的 **no** 形式，以确保您获得您所期望的结果。有关更多信息，请参阅“示例”部分。

4 字节自主系统编号支持

思科 4 字节自主系统编号实施使用 asplain 格式 （例如 65538），因为默认正则表达式为自主系统编号匹配和输出显示格式，但您可以如 RFC 5396 中所述采用 asplain 格式和 asdot 格式配置 4 字节自主系统编号。要将 4 字节自主系统编号的默认正则表达式匹配和输出显示更改为以 asdot 格式，请使用 **bgp asnotation dot** 命令。

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

示例

以下示例显示如何将 OSPF 路由重分布到 BGP 域中：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# redistribute ospf
```

以下示例导致将 EIGRP 路由重分布到 OSPF 域中：

```
ciscoasa(config)# router ospf 110
ciscoasa(config-router)# redistribute eigrp
```

以下示例导致将指定的 EIGRP 进程路由重分布到 OSPF 域中。源自 EIGRP 的指标会被重新映射为 100， RIP 路由会被重新映射为 200。

```
ciscoasa(config)# router ospf 109
ciscoasa(config-router)# redistribute eigrp 108 metric 100 subnets
ciscoasa(config-router)# redistribute rip metric 200 subnets
```

在以下示例中，网络 172.16.0.0 会在 OSPF 1 中显示为外部链路状态通告 (LSA)，其中成本为 100（保留成本）：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ip address 172.16.0.1 255.0.0.0
ciscoasa(config)#  ospf cost 100
ciscoasa(config)# interface ethernet 1
ciscoasa(config-if)#ip address 10.0.0.1 255.0.0.0
!
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0 0.255.255.255 area 0
ciscoasa(config-router)# redistribute ospf 2 subnet
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

以下示例显示如何将 BGP 路由重分布到 OSPF 中，并为其分配采用 asplain 格式的本地 4 字节自主系统编号。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# redistribute bgp 65538
```

以下示例从 **redistribute connected metric 1000 subnets** 命令中删除 **connected metric 1000 subnets** 选项，并在配置中保留 **redistribute connected** 命令：

```
ciscoasa(config-router)# no redistribute connected metric 1000 subnets
```

以下示例从 **redistribute connected metric 1000 subnets** 命令中删除 **metric 1000** 选项，并在配置中保留 **redistribute connected subnets** 命令：

```
ciscoasa(config-router)# no redistribute connected metric 1000
```

以下示例从 **redistribute connected metric 1000 subnets** 命令中删除 **subnets** 选项，并在配置中保留 **redistribute connected metric 1000** 命令：

```
ciscoasa(config-router)# no redistribute connected subnets
```

以下示例从配置中删除 **redistribute connected** 命令以及为 **redistribute connected** 命令配置的任何选项之一：

```
ciscoasa(config-router)# no redistribute connected
```

redistribute (EIGRP)

要将来自一个路由域的路由重分布到 EIGRP 路由过程中，请在路由器配置模式下使用 **redistribute** 命令。要删除重分布，请使用此命令的 **no** 形式。

redistribute {{**eigrp** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

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

语法说明

bandwidth	EIGRP 带宽指标，以每秒千位为单位。有效值为从 1 到 4294967295。
connected	指定将与接口连接的网络重分布到 EIGRP 路由过程中。
delay	EIGRP 延迟指标，以 10 微秒为单位。有效值为从 0 到 4294967295。
external *type*	指定在指定的自主系统外部的 EIGRP 指标路由；有效值为 **1** 或 **2**。
internal *type*	指定在指定的自主系统内部的 EIGRP 指标路由。
load	EIGRP 有效带宽（负载）指标。有效值为从 1 到 255，其中 255 表示负载达到 100%。
match	（可选）指定将路由从 OSPF 重分布到 EIGRP 中的条件。
metric	（可选）指定用于将路由的 EIGRP 指标重分布到 EIGRP 路由过程中的值。
mtu	路径的 MTU。有效值为从 1 到 65535。
nssa-external *type*	指定 NSSA 外部的路由的 EIGRP 指标类型；有效值为 **1** 或 **2**。
eigrp *pid*	用于将 EIGRP 路由过程重分布到 EIGRP 路由过程中。*pid* 为 EIGRP 路由过程指定内部使用的标识参数；有效值为从 1 到 65535。
reliability	EIGRP 可靠性度量。有效值为从 0 到 255，其中 255 表示 100% 可靠。
rip	指定从 RIP 路由过程将网络重分布到 EIGRP 路由过程中。
route-map *map_name*	（可选）路由映射的名称，用于过滤从源路由协议到 EIGRP 路由过程的导入路由。如果未指定，将重分布所有路由。
static	用于将静态路由重分布到 EIGRP 路由过程中。

默认值

以下是命令默认值：

- **match**: **Internal**, **external 1**, **external 2**

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

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

示例

以下示例将静态和连接的路由重分布到 EIGRP 路由过程中：

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

相关命令

命令	说明
router eigrp	创建 EIGRP 路由过程并为该进程进入配置模式。
show running-config router	显示全局路由器配置中的命令。

redistribute (OSPF)

要将来自一个路由域的路由重分布到 OSPF 路由过程中，请在路由器配置模式下使用 **redistribute** 命令。要在不包括选项时删除重分布，请使用此命令的 **no** 形式。带有选项的命令的 **no** 形式仅删除对该选项的配置。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected** | **eigrp** *as-number*} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

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

语法说明

connected	指定将与接口连接的网络重分布到 OSPF 路由过程中。
eigrp *as-number*	用于将 EIGRP 路由重分布到 OSPF 路由过程中。*as-number* 指定 EIGRP 路由过程的自主系统编号。有效值为从 1 到 65535。
external *type*	指定在指定的自主系统外部的 OSPF 指标路由；有效值为 **1** 或 **2**。
internal *type*	指定在指定的自主系统内部的 OSPF 指标路由。
match	（可选）指定将路由从一个路由协议重分布到另一个路由协议中的条件。
metric *metric_value*	（可选）指定从 0 到 16777214 的 OSPF 默认指标值。
metric-type *metric_type*	（可选）与通告到 OSPF 路由域中的默认路由相关联的外部链路类型。它可以是以下两个值之一：**1**（类型 1 外部路由）或 **2**（类型 2 外部路由）。
nssa-external *type*	指定 NSSA 外部的路由的 OSPF 指标类型；有效值为 **1** 或 **2**。
ospf *pid*	用于将 OSPF 路由过程重分布到当前 OSPF 路由过程中。 *pid* 为 OSPF 路由过程指定内部使用的标识参数；有效值为从 1 到 65535。
rip	指定从 RIP 路由过程将网络重分布到当前 OSPF 路由过程中。
route-map *map_name*	（可选）路由映射的名称，用于过滤从源路由协议到当前 OSPF 路由过程的导入路由。如果未指定，将重分布所有路由。
static	用于将静态路由重分布到 OSPF 进程中。
subnets	（可选）对于将路由重分布到 OSPF 中，为指定的协议界定重分布。如果不使用，则仅重分布有类路由。
tag *tag_value*	（可选）附加到每个外部路由的 32 位十进制值。 OSPF 本身不使用此值。可以使用它在 ASBR 之间传递信息。如果未指定任何值，则会将远程自主系统编号用于来自 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。

默认值

以下是命令默认值：

- **metric** *metric-value*: 0
- **metric-type** *type-value*: **2**
- **match**: **Internal**, **external 1**, **external 2**
- **tag** *tag-value*: 0

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	将此命令修改为包括 **rip** 关键字。
8.0(2)	将此命令修改为包括 **eigrp** 关键字。
9.0(1)	支持多情景模式。

示例

以下示例显示如何将静态路由重分布到当前 OSPF 进程中：

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

相关命令

命令	说明
redistribute (RIP)	将路由重分布到 RIP 路由过程中。
router ospf	进入路由器配置模式。
show running-config router	显示全局路由器配置中的命令。

redistribute (OSPFv3)

要将来自一个 OSPFv3 路由域的 IPv6 路由重分布到 OSPFv3 路由域中，请在 IPv6 路由器配置模式下使用 **redistribute** 命令。要禁用重分布，请使用此命令的 **no** 形式。

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

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

语法说明

as-number	指定路由过程的自主系统编号。有效值范围为 1 到 65535。
external	指定在指定的自主系统外部的 OSPFv3 指标路由，但会将其作为类型 1 或类型 2 外部路由导入到 OSPFv3 中。有效值为 1 或 2。
include-connected	（可选）允许目标协议在正在运行源协议的接口上重分布源协议和连接的前缀已了解的路由。
internal	指定在指定的自主系统内部的 OSPFv3 指标路由。
level-1	指定对于中间系统到中间系统 (IS-IS)，独立将第 1 级路由重分布到其他 IP 路由协议中。
level-1-2	指定对于 IS-IS，独立将第 1 级和第 2 级路由重分布到其他 IP 路由协议中。
level-2	指定对于 IS-IS，独立将第 2 级路由重分布到其他 IP 路由协议中。
map-tag	指定配置的路由映射的标识符。
match	（可选）将路由重分布到其他路由域中。
metric *metric_value*	（可选）指定从 0 到 16777214 的范围内的 OSPFv3 默认指标值。
metric-type *metric_type*	（可选）指定与通告到 OSPFv3 路由域中的默认路由相关联的外部链路类型。它可以是以下两个值之一：1 用于类型 1 外部路由，或 2 用于类型 2 外部路由。
nssa-external	指定在指定的自主系统外部的路由，但会将其作为类型 1 或类型 2 外部路由导入到用于 IPv6 的末节区域 (NSSA) 中的 OSPFv3 中。
process-id	（可选）指定启用 OSPFv3 路由过程时管理性分配的编号。
route-map *map_name*	（可选）指定路由映射的名称，用于过滤从源路由协议导入到当前 OSPFv3 路由协议的路由。如果指定此名称，但没有列出路由映射标记，则不会导入任何路由。如果未指定，将重分布所有路由。
source-protocol	指定要从其中重分布路由的源协议。有效值可以是以下值之一：connected、 ospf 或 static。
tag *tag_value*	（可选）指定附加到每个外部路由的 32 位十进制值。OSPFv3 本身不使用此值，但可以使用它在 ASBR 之间传递信息。如果未指定任何值，则会将远程自主系统编号用于来自 BGP 和 EGP 的路由；对于其他协议，使用零。有效值范围为 0 到 4294967295。
transparent	（可选）导致 RIP 将用于重分布的路由的路由表指标用作 RIP 指标。

默认值

以下是命令默认值：

- **metric** *metric-value*: **0**
- **metric-type** *type-value*: **2**
- **match**: **internal**, **external 1**, **external 2**
- **tag** *tag-value*: **0**

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

示例

以下示例显示如何将静态路由重分布到当前 OSPFv3 进程中：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

相关命令

命令	说明
ipv6 router ospf	进入 OSPFv3 的路由器配置模式。
show running-config ipv6 router	显示 OSPFv3 的路由器配置中的命令。

redistribute (RIP)

要将来自另一个路由域的路由重分布到 RIP 路由过程中，请在路由器配置模式下使用 **redistribute** 命令。要删除重分布，请使用此命令的 **no** 形式。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

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

语法说明

connected	指定将与接口连接的网络重分布到 RIP 路由过程中。
eigrp *as-number*	用于将 EIGRP 路由重分布到 RIP 路由过程中。 *as-number* 指定 EIGRP 路由过程的自主系统编号。有效值为从 1 到 65535。
external *type*	指定在指定的自主系统外部的 OSPF 指标路由；有效值为 **1** 或 **2**。
internal *type*	指定在指定的自主系统内部的 OSPF 指标路由。
match	（可选）指定将路由从 OSPF 重分布到 RIP 中的条件。
metric {*metric_value* | **transparent**}	（可选）为正在重分布的路由指定 RIP 指标值。 *metric_value* 的有效值为从 0 到 16。将指标设置为 **transparent** 会导致使用当前路由指标。
nssa-external *type*	为在末节区域 (NSSA) 外部的路由指定 OSPF 指标类型；有效值为 **1** 或 **2**。
ospf *pid*	用于将 OSPF 路由过程重分布到 RIP 路由过程中。 *pid* 为 OSPF 路由过程指定内部使用的标识参数；有效值为从 1 到 65535。
route-map *map_name*	（可选）路由映射的名称，用于过滤从源路由协议到 RIP 路由过程的导入路由。如果未指定，将重分布所有路由。
static	用于将静态路由重分布到 OSPF 进程中。

默认值

以下是命令默认值：

- **metric** *metric-value*: 0
- **match**: **Internal**, **external 1**, **external 2**

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。
8.0(2)	将此命令修改为包括 **eigrp** 关键字。
9.0(1)	支持多情景模式。

示例

以下示例显示如何将静态路由重分布到当前 RIP 进程中：

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

相关命令

命令	说明
redistribute (EIGRP)	将来自其他路由域的路由重分布到 EIGRP 中。
redistribute (OSPF)	将来自其他路由域的路由重分布到 OSPF 中。
router rip	启用 RIP 路由过程并进入该进程的路由器配置模式。
show running-config router	显示全局路由器配置中的命令。

redundant-interface

要将冗余接口的哪个成员接口设置为活动状态，请在特权 EXEC 模式下使用 **redundant-interface** 命令。

redundant-interface redundant*number* **active-member** *physical_interface*

语法说明

active-member *physical_interface*	设置活动成员。请参阅 **interface** 命令了解接受的值。两个成员接口必须属于同一物理类型。
redundant *number*	指定冗余接口 ID，例如 **redundant1**。

默认值

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）。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

要查看哪个接口处于活动状态，请输入以下命令：

```
ciscoasa# show interface redundantnumber detail | grep Member
```

例如：

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

示例

以下示例创建一个冗余接口。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。 redundant-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
```

相关命令

命令	说明
clear interface	清除 **show interface** 命令的计数器。
debug redundant-interface	显示与冗余接口事件或错误相关的调试消息。
interface redundant	创建冗余接口。
member-interface	将一个成员接口分配给一个冗余接口对。
show interface	显示接口的运行状态和统计信息。

regex

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

regex *name regular_expression*

no regex *name* [*regular_expression*]

语法说明

name	指定正则表达式名称，长度最多 40 个字符。
regular_expression	指定正则表达式，长度最多 100 个字符。有关正则表达式中可使用的元字符的列表，请参阅 “ 使用指南 ” 部分。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

regex 命令可用于各种需要文本匹配的功能。例如，您可以使用 *inspection policy map* 为使用 模块化策略框架 的应用检查配置特殊操作 （请参阅 **policy map type inspect** 命令）。在检查策略映射中，可以通过创建包含一个或多个 **match** 命令的检查类映射来标识要操作的流量，也可以直接在检查策略映射中使用 **match** 命令。有些 **match** 命令可让您标识数据包中使用正则表达式的文本，例如，您可以匹配 HTTP 数据包中的 URL 字符串。您可以在正则表达式类映射中组合多个正则表达式 （请参阅 **class-map type regex** 命令）。

正则表达式实际上会匹配作为完全匹配字符串的文本字符串，或通过使用 *metacharacters* 进行匹配，因此您可以与文本字符串的多个变体进行匹配。您可以使用正则表达式来匹配某些应用流量的内容；例如，您可以与 HTTP 数据包内的正文文本进行匹配。

注　作为一种优化， ASA 会在消除模糊的 URL 上搜索。消除模糊将多个正斜线 (/) 压缩为单一斜线。对于常用双斜线的字符串 （如 “http://”），请务必搜索 “http:/”。

表 18-1 列出了有特殊意义的元字符。

表 18-1　正则表达式元字符

字符	说明	备注
.	圆点	匹配任何单个字符。例如， **d.g** 会匹配 dog、 dag、 dtg，以及包含这些字符的任何词 （例如 doggonnit）。
(*exp*)	子表达式	子表达式将字符与周围字符隔开，以便使用子表达式上的其他元字符。例如， **d(ola)g** 会匹配 dog 和 dag，而 **dolag** 会匹配 do 和 ag。子表达式也可以与重复限定符结合使用来区分重复字符。例如，**ab(xy){3}z** 会匹配 abxyxyxyz。
|	间隔	匹配它隔开的任一表达式。例如， **dog|cat** 会匹配 dog 或 cat。
?	问号	一个限定符，表示 0 个或 1 个上一表达式。例如，**lo?se** 会匹配 lse 或 lose。 **注**　您必须输入 **Ctrl + V** 然后输入问号，否则会调用帮助功能。
*	星号	一个限定符，表示有 0 个、 1 个或任意数量的上一表达式。例如， **lo*se** 会匹配 lse、 lose、 loose 等。
+	加	一个限定符，表示至少有 1 个上一表达式。例如，**lo+se** 会匹配 lose 和 loose 而非 lse。
{*x*} 或 {*x*,}	最小重复限定符	至少重复 *x* 次。例如， **ab(xy){2,}z** 会匹配 abxyxyz、abxyxyxyz 等。
[*abc*]	字符类	匹配方括号中的任一字符。例如，**[abc]** 会匹配 a、b 或 c。
[^*abc*]	求反字符类	匹配括号中不包含的单个字符。例如， **[^abc]** 会匹配除 a、b 或 c 外的任何字符。**[^A-Z]** 会匹配不是大写字母的任何单个字符。
[*a-c*]	字符范围类	匹配范围内的任一字符。**[a-z]** 会匹配任一小写字母。您可以将字符和范围进行混合：**[abcq-z]** 会匹配 a、b、c、q、r、s、t、u、v、w、x、y、z，**[a-cq-z]** 也会与它们进行匹配。 破折号 (-) 字符仅在其是括号中的最后一个字符或第一个字符时 （ **[abc-]** 或 **[-abc]**）才有原义。
“”	引号	保留字符串中的尾部或前导空格。例如， **" test"** 会在查找匹配时保留前导空格。
^	插入符号	指定行的起点。
\	转义字符	当与元字符结合使用时，与原义字符进行匹配。例如， **\[** 会匹配左方括号。
char	字符	当字符不是元字符时，与原义字符进行匹配。
\r	回车	匹配回车 0x0d。
\n	新行	匹配新行 0x0a。
\t	制表符	匹配制表符 0x09。

表 18-1　正则表达式元字符 （续）

字符	说明	备注
\f	换页符	匹配换页符 0x0c。
\x*NN*	转义的十六进制数	匹配使用十六进制 （确切指两位数）的 ASCII 字符。
NNN	转义的八进制数	匹配作为八进制数 （确切指三位数）的 ASCII 字符。例如，字符 040 代表空格。

要测试正则表达式以确保其匹配符合您的预期，请输入 **test regex** 命令。

正则表达式性能影响由两个主要因素确定：

- 需要为正则表达式匹配搜索的文本的长度。

  当搜索长度小时，正则表达式引擎对 ASA 性能的影响不大。
- 需要为正则表达式匹配搜索的正则表达式链接表的数量。

搜索长度对性能的影响

配置正则表达式搜索时，通常会参照正则表达式数据库来检查搜索的文本的每个字节以查找匹配。搜索的文本越长，搜索时间就会越长。以下是说明这种现象的性能测试案例。

- HTTP 事务包括一个长度为 300 字节的 GET 请求和一个长度为 3250 字节的响应。
- 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 个正则表达式用于响应正文搜索。

当策略配置为仅在 HTTP GET 请求中搜索 URI 和正文时，吞吐量是：

- 当不搜索相应的正则表达式数据库时为 420 Mbps。
- 当搜索相应的正则表达式数据库时为 413 Mbps （这显示使用正则表达式的成本相对较小）。

但是，当策略配置为同时搜索整个 HTTP 响应正文时，由于响应正文搜索较长 （3250 个字节），吞吐量会下降到 145 Mbps。

以下列出的一些因素会增加用于正则表达式搜索的文本长度：

- 在多个不同协议字段上配置正则表达式搜索。例如，在 HTTP 检查中，如果仅为正则表达式匹配配置 URI，则仅会搜索 URI 字段以进行正则表达式匹配，且搜索长度会限定为 URI 长度。但是，如果也配置附加协议字段 （例如标头、正文等）以进行正则表达式匹配，则搜索长度会增加为包括标头长度和正文长度。
- 要搜索的字段较长。例如，如果为正则表达式搜索配置 URI，则 GET 请求中较长的 URI 会具有较长的搜索长度。此外，当前默认情况下将 HTTP 正文搜索长度限制为 200 个字节。但是，如果策略配置为搜索正文，且将正文搜索长度更改为 5000 个字节，则会由于正文搜索较长而严重影响性能。

正则表达式链接表数对性能的影响

当前，将为同一协议字段配置的所有正则表达式 （例如用于 URI 的所有正则表达式）构建到一个数据库中，该数据库包含一个或多个正则表达式链接表。表数由所需总内存和表构建时的可用内存确定。符合以下任一条件时，正则表达式数据库会拆分为多个表：

- 当所需总内存大于 32 MB 时 （因为最大表大小会限制为 32 MB）。
- 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，会构建多个较小的表以容纳所有正则表达式。请注意，内存碎片程度取决于许多因素，这些因素相互关联且几乎无法预测碎片级别。

具有多个链接表时，必须搜索每个表来进行正则表达式匹配，因此搜索时间与搜索的表的数量成正比。

某些类型的正则表达式往往会显著增加表大小。设计正则表达式时尽可能避免通配符和重复因素是明智之举。请参阅表 18-1 了解以下元字符的说明：

- 带有指定的通配符类型的正则表达式：
  - 圆点 (.)
- 匹配类中的任何字符的各种字符类：
  - [^a-z]
  - [a-z]
  - [abc]]
- 带有指定的重复类型的正则表达式：
  - *
  - +
  - {n,}
- 正则表达式的通配符和重复类型的组合可以显著增加表大小，例如：
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.* （不应如此执行，因为这相当于与 “123” 进行匹配）。

以下示例说明正则表达式是否带有通配符和重复对内存消耗有何不同。

- 以下 4 个正则表达式的数据库大小为 958,464 个字节。

```
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为 10240 个字节。

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

大量正则表达式会增加正则表达式数据库所需的总内存，从而会增加表的拆分可能性 （如果内存碎片化）。以下是不同数量的正则表达式的内存消耗的示例：

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

注　每个情景的最大正则表达式数为 2048。

可以使用 **debug menu regex 40 10** 命令显示每个正则表达式数据库中有多少链接表。

示例

以下示例创建在检查策略映射中使用的两个正则表达式：

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

相关命令

命令	说明
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
policy-map	通过将流量类与一个或多个操作关联来创建策略映射。
policy-map type inspect	定义特殊的应用检查操作。
class-map type regex	创建正则表达式类映射。
test regex	测试正则表达式。

reload

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

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

语法说明

at *hh*:*mm*	（可选）计划在指定的时间 （使用 24 小时制）重新加载软件。如果未指定月和日，则会在当天 （如果指定的时间晚于当前时间）或第二天（如果指定的时间早于当前时间）的指定时间重新加载。指定 00:00 会计划在午夜重新加载。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）天数在从 1 到 31 的范围内。
in [*hh*:]*mm*]	（可选）计划在指定的分钟或小时和分钟内重新加载软件。重新加载必须在 24 小时内进行。
max-hold-time [*hh*:]*mm*	（可选）在关闭或重启前指定 ASA 通知其他子系统前等待的最大保持时间。此时间间隔后，会发生快速 （强制）关闭 / 重启。
month	（可选）指定月的名称。输入充足的字符以为月的名称创建唯一字符串。例如，“Ju” 不是唯一字符串，因为它可能代表 6 月、7 月，但 “Jul” 是唯一字符串，因为没有其他月的名称以这三个字母开始。
noconfirm	（可选）允许 ASA 重新加载而无需用户确认。
quick	（可选）强制快速重新加载，而无需通知或正确关闭所有子系统。
reason *text*	（可选）指定重新加载的原因 （1 到 255 个字符）。将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**　某些应用 （如 ISAKMP）需要附加配置以将原因文本发送到 IPsec VPN 客户端。有关更多信息，请参阅 《VPN CLI 配置指南》。
save-config	（可选）在关闭前将正在运行的配置保存到内存中。如果不输入 **save-config** 关键字，则在重新加载后会丢失尚未保存的任何配置更改。
save-show-tech	（可选）在重新加载前，将 **show tech** 命令的输出保存到文件中。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式。

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

命令历史

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

使用指南

该命令可让您重启 ASA 并从闪存中重新加载配置。

默认情况下， **reload** 命令是交互式的。 ASA 首先检查是否已修改但未保存配置。如果是，则 ASA 会提示您保存配置。在多情景模式下， ASA 会为每个情景提示有未保存的配置。如果您指定 **save-config** 关键字，则会保存配置而不提示您。然后， ASA 会提示您确认真正要重新加载的系统。仅回应 **y** 或按 **Enter** 键会导致重新加载。确认后， ASA 会启动或计划重新加载进程，具体取决于是否已指定延迟关键字 （**in** 或 **at**）。

默认情况下，重新加载进程在 “ 平滑 ” 模式下运行。当即将重启时通知所有注册的子系统，允许这些子系统在重启前正确关闭。为避免等待系统关闭，请指定 **max-hold-time** 关键字以指定最大等待时间。或者，您可以使用 **quick** 关键字强制重新加载进程突然开始，而无需通知受影响的子系统或等待其平滑关闭。

您可以通过指定 **noconfirm** 关键字来强制 **reload** 命令非交互式运行。这种情况下，ASA 不检查是否有未保存的配置，除非已指定 **save-config** 关键字。 ASA 不会在重启系统前提示您进行确认。它会立即启动或计划重新加载进程 （除非已指定延迟关键字），不过您可以指定 **max-hold-time** 或 **quick** 关键字来控制行为或重新加载进程。

使用 **reload cancel** 命令取消计划的重新加载。您无法取消已在进行中的重新加载。

注　重新加载后会丢失未写入闪存分区的配置更改。重启前，请输入 **write memory** 命令来将当前配置存储在闪存分区中。

示例

以下示例显示如何重启并重新加载配置：

```
ciscoasa# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

相关命令

命令	说明
show reload	显示 ASA 的重新加载状态。

remote-access threshold session-threshold-exceeded

要设置阈值，请在全局配置模式下使用 **remote-access threshold** 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，达到此数量时 ASA 会发送陷阱。

remote-access threshold session-threshold-exceeded {*threshold-value*}

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

语法说明

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

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0 (1)	引入了此命令。

示例

以下示例显示如何设置阈值为 1500：

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

相关命令

命令	说明
snmp-server enable trap remote-access	启用阈值陷阱。

rename

要将文件或目录的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:**] *source-path* [**disk0**: | **disk1**: | **flash:**] *destination-path*

语法说明

/noconfirm	（可选）抑制确认提示。
destination-path	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）指定外部闪存卡，后跟冒号。
flash:	（可选）指定内部闪存，后跟冒号。
source-path	指定源文件的路径。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

rename flash: flash: 命令提示您输入源文件名和目标文件名。

您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
```

示例

以下示例显示如何将名为 “test” 的文件重命名为 “test1”：

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

相关命令

命令	说明
mkdir	创建新目录。
rmdir	删除目录。
show file	显示关于文件系统的信息。

rename （类映射）

要重命名类映射，请在类映射配置模式下输入 **rename** 命令。

rename *new_name*

语法说明

new_name	指定类映射的新名称，长度最多 40 个字符。“class-default” 是保留名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

示例

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
```

相关命令

命令	说明
class-map	创建类映射。

renewal-reminder

要指定用户证书过期前的天数 （超过此天数则向证书所有者发送重新注册的初始提醒），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 *days*

no renewal-reminder

语法说明

days	指定颁发的证书过期前的时间 （以天数形式），超过此天数则首次提醒证书所有者重新注册证书。有效值范围为 1 到 90 天。

默认值

默认值为 14 天。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

总共有三次提醒。如果在用户数据库中指定了电邮地址，则每次提醒时都会自动向证书所有者发送电邮。如果不存在任何电邮地址，则会生成系统日志消息，提示管理员续约。

默认情况下， CA 服务器在证书过期前按照指定的顺序发送以下三个电邮消息：

1. 证书注册邀请
2. 提醒：证书注册邀请
3. 最后提醒：证书注册邀请

第一封电邮是邀请，第二封电邮是提醒，第三封电邮是最后提醒。此通知的默认设置为 14 天，这意味着初始邀请会在证书过期前 14 天发出，提醒电邮在证书过期前 7 天发出，最后提醒电邮在证书过期前 3 天发出。

您可以使用 **renewal-reminder** *days* 命令定制续约提醒间隔。

示例

以下示例指定 ASA 在证书过期前 7 天向用户发送过期通知：

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

以下示例将过期通知时间重置为默认值，即证书过期前 14 天：

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

相关命令

命令	说明
crypto ca server	提供 CA 服务器配置模式命令集的访问权限，从而允许您配置和管理本地 CA。
lifetime	指定 CA 证书、所有颁发的证书和 CRL 的生存期。
show crypto ca server	显示本地 CA 服务器的配置详细信息。

replication http

要为故障切换组启用 HTTP 连接复制，请在故障切换组配置模式下使用 **replication http** 命令。要禁用 HTTP 连接复制，请使用此命令的 **no** 形式。

replication http

no replication http

语法说明

此命令没有任何参数或关键字。

默认值

已禁用。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
故障切换组配置	• 是	• 是	—	—	• 是

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

默认情况下， ASA 不会在启用 Stateful Failover （状态故障切换）时复制 HTTP 会话信息。由于 HTTP 会话通常较短暂，且 HTTP 客户端通常会在连接尝试失败后重试，因此不复制 HTTP 会话会提高系统性能，不会造成严重的数据或连接丢失。 **replication http** 命令可在状态故障切换环境中启用 HTTP 会话的状态复制，但会对系统性能有负面影响。

此命令仅用于主用 / 主用故障切换。它提供与 **failover replication http** 命令相同的用于 Active/Standby （主用 / 备用）故障切换的功能，但 Active/Active （主用 / 主用）故障切换配置中的故障切换组除外。

示例

以下示例显示用于故障切换组的可能配置：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

相关命令

命令	说明
failover group	为 Active/Active （主用 / 主用）故障切换定义故障切换组。
failover replication http	配置状态故障切换以复制 HTTP 连接。

request-command deny

要禁止 FTP 请求内的特定命令，请在 FTP 映射配置模式（可使用 **ftp-map** 命令访问）下使用 **request-command deny** 命令。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** }

语法说明

appe	禁止追加到文件中的命令。
cdup	禁止用于更改为当前正在工作的目录的父目录的命令。
dele	禁止用于删除服务器上的文件的命令。
get	禁止用于从服务器检索文件的客户端命令。
help	禁止用于提供帮助信息的命令。
mkd	禁止用于在服务器上创建目录的命令。
put	禁止用于向服务器发送文件的客户端命令。
rmd	禁止用于删除服务器上的目录的命令。
rnfr	禁止用于指定重命名源文件名的命令。
rnto	禁止用于指定重命名目标文件名的命令。
site	禁止特定于服务器系统的命令。通常用于远程管理。
stou	禁止使用唯一文件名存储文件的命令。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

在使用严格 FTP 检查时，此命令用于控制穿越 ASA 的 FTP 请求中允许的命令。

示例

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
```

相关命令

命令	说明
class-map	定义要应用安全操作的流量类。
ftp-map	定义一个 FTP 映射并启用 FTP 映射配置模式。
inspect ftp	应用特定的 FTP 映射以用于应用检查。
mask-syst-reply	隐藏来自客户端的 FTP 服务器响应。
policy-map	将类映射与特定安全操作关联。

request-data-size

要在 SLA 操作请求数据包中设置负载的大小，请在 SLA 监控协议配置模式下使用 **request-data-size** 命令。要恢复默认值，请使用此命令的 **no** 形式。

request-data-size *bytes*

no request-data-size

语法说明

bytes	请求数据包负载的大小（以字节为单位）。有效值为从 0 到 16384。最小值取决于所使用的协议。对于回应类型，最小值为 28 个字节。不能将此值设置为高于协议或 PMTU 允许的最大值。 **注**　ASA 将 8 字节时间戳添加到负载中，因此实际负载是 *字节数* + 8。

默认值

默认 *字节数*是 28。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

为了实现可达性，可能需要增加默认数据大小，以检测源和目标之间的 PMTU 更改。低 PMTU 可能会影响会话性能，且如果被检测到，则可能表示使用了辅助路径。

示例

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求 / 响应时间探测操作。它将回应请求数据包的负载大小设置为 48 字节，并将 SLA 操作过程中发送的回应请求数量设置为 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
```

相关命令

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

request-queue

要指定将排队等待响应的 GTP 请求的最大数量，请在 GTP 映射配置模式（使用 **gtp-map** 命令可访问）下使用 **request-queue** 命令。使用此命令的 **no** 形式可将此数字恢复为默认值 200。

request-queue *max_requests*

no request-queue *max_requests*

语法说明

max_requests	排队等待响应的最大 GTP 请求数。值范围为 1 到 4294967295。

默认值

max_requests 默认值为 200。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

gtp request-queue 命令指定排队等待响应的最大 GTP 请求数。当达到该限制且新请求到达时，会删除在队列中等待时间最长的请求。Error Indication（错误指示）、Version Not Supported（版本不受支持）和 SGSN Context Acknowledge （SGSN 情景确认）消息不会被视为请求，这些消息也不会进入请求队列等待响应。

示例

以下示例指定最大请求队列大小为 300 个字节：

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# request-queue-size 300
```

相关命令

命令	说明
clear service-policy inspect gtp	清除全局 GTP 统计信息。
debug gtp	显示有关 GTP 检查的详细信息。
gtp-map	定义 GTP 映射并启用 GTP 映射配置模式。
inspect gtp	应用要用于应用检查的特定 GTP 映射。
show service-policy inspect gtp	显示 GTP 配置。

request-timeout

要配置 SSO 身份验证失败后尝试超时之前的秒数，请在 WebVPN 配置模式下使用 **request-timeout** 命令。

要恢复默认值，请使用此命令的 **no** 形式。

request-timeout *seconds*

no request-timeout

语法说明

seconds	SSO 身份验证失败后尝试超时之前的秒数。范围为 1 到 30 秒。不支持分数。

默认值

此命令的默认值为 5 秒。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1.1	引入了此命令。

使用指南

单点登录支持，仅适用于 WebVPN，可让用户访问不同服务器上的不同安全服务，而无需重复输入用户名和密码。 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。

配置 ASA 为支持 SSO 身份验证后，您可以选择调整两个超时参数：

- SSO 身份验证失败后使用 **request-timeout** 命令尝试超时之前的秒数。
- ASA 在 SSO 身份验证尝试失败后的重试次数。（请参阅 **max-retry-attempts** 命令。）

示例

在 webvpn-config-sso-siteminder 模式下输入的以下示例为 SiteMinder 类型的 SSO 服务器 “example” 将身份验证超时配置为十秒：

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

相关命令

命令	说明
max-retry-attempts	配置 SSO 身份验证尝试失败后 ASA 的重试次数。
policy-server-secret	创建用于对发往 SiteMinder SSO 服务器的身份验证请求进行加密的密钥。
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。

reserve-port-protect

要限制在媒体协商期间使用保留端口，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，请使用此命令的 **no** 形式。

reserve-port-protect

no reserve-port-protect

语法说明

此命令没有任何参数或关键字。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

示例

以下示例显示如何在 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
```

相关命令

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

reserved-bits

要清除 TCP 标头中的保留位或丢弃带有保留位集的数据包，请在 TCP 映射配置模式下使用 **reserved-bits** 命令。要删除此指定，请使用此命令的 **no** 形式。

reserved-bits {**allow** | **clear** | **drop**}

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

语法说明

allow	允许 TCP 标头中带有保留位的数据包通过。
clear	清除 TCP 标头中的保留位，并允许该数据包通过。
drop	丢弃 TCP 标头中带有保留位的数据包。

默认值

默认情况下允许保留位。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

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

使用 **tcp-map** 命令进入 TCP 映射配置模式。在 TCP 映射配置模式下使用 **reserved-bits** 命令明确终端主机如何处理带有保留位的数据包，这可能会导致 ASA 失去同步。您可以选择清除 TCP 标头中的保留位甚或丢弃带有保留位集的数据包。

示例

以下示例显示如何在所有 TCP 流上清除带有保留位集的数据包：

```
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
```

相关命令

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

reset

使用 模块化策略框架 时，通过在匹配或类配置模式下使用 **reset** 命令，来丢弃数据包，关闭连接，并发送用于与 **match** 命令或类映射匹配的流量的 TCP 重置。此重置操作在用于应用流量的检查策略映射 （**policy-map type inspect** 命令）中可用；但是，并非所有应用都允许此操作。要禁用此操作，请使用此命令的 **no** 形式。

reset [log]

no reset [log]

语法说明

log	记录匹配。系统日志消息数量取决于应用。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

一个检查策略映射包含一个或多个 **match** 和 **class** 命令。检查策略映射可用的确切命令取决于应用。在输入 **match** 或 **class** 命令来标识应用流量 （**class** 命令引用一个现有的 **class-map type inspect** 命令，后者又包括 **match** 命令）后，您可以输入 **reset** 命令来丢弃数据包，并关闭用于与 **match** 命令或 **class** 命令匹配的流量的连接。

如果您重置连接，则检查策略映射中不会执行任何进一步的操作。例如，如果第一个操作是重置连接，则它不会与任何进一步的 **match** 或 **class** 命令进行匹配。如果首个操作是记录数据包，则可能会发生第二个操作，如重置连接。您可以为同一 **match** 或 **class** 命令配置 **reset** 和 **log** 操作，其中会在为给定匹配重置数据包前将其记录下来。

在第 3/4 层策略映射中使用 **inspect** 命令启用应用检查 （**policy-map** 命令）时，您可以启用包含此操作的检查策略映射，例如，当 http_policy_map 是检查策略映射的名称时输入 **inspect http http_policy_map** 命令。

示例

以下示例重置连接，并在它们与 http-traffic 类映射匹配时发送日志。如果同一数据包还与第二个 **match** 命令进行匹配，则不会处理它，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
```

相关命令

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

第 19 章

retries 至 rtp-min-port rtp-max-port 命令

retries

要指定当 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 **dns retries** 命令。要恢复默认设置，请使用此命令的 **no** 形式。

retries *number*

no retries [*number*]

语法说明

number	指定重试次数，从 0 到 10。默认值为 2。

默认值

默认重试次数为 2。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

使用 **name-server** 命令添加 DNS 服务器。

此命令取代了 **dns name-server** 命令。

示例

以下示例将重试次数设置为 0。 ASA 对每台服务器只尝试一次。

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

相关命令

命令	说明
clear configure dns	删除所有 DNS 命令。
dns server-group	进入 dns 服务器组模式。
show running-config dns server-group	显示一个或所有现有 dns 服务器组配置。

retry-count

要设置在轮询云网络安全代理服务器连续失败多少次后才确定服务器不可达，请在 scansafe 常规选项配置模式下输入 **retry-count** 命令。要恢复默认值，请使用此命令的 **no** 形式。

retry-count *value*

no retry-count [*value*]

语法说明

value	输入重试计数器值，从 2 到 100。默认值为 5。

命令默认

默认值为 5。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	路由	透明	单个	情景	系统
Scansafe 常规选项配置	• 是	• 是	• 是	—	• 是

命令历史

版本	修改
9.0(1)	我们引入了此命令。

使用指南

订用思科云网络安全服务时，将为您分配云网络安全主代理服务器和备用代理服务器。

如有任何客户端无法连接主服务器， ASA 将开始轮询设备塔来确定可用性。（如果没有客户端活动， ASA 每隔 15 分钟轮询一次。）如果代理服务器在配置的重试次数 （默认为 5，此设置可配置）后不可用，将宣告该服务器不可达，并启用备用代理服务器。

如果客户端或 ASA 在达到重试次数之前至少可以两次连续连接到服务器，轮询将会停止并且确认设备塔可达。

故障切换到备用服务器后， ASA 继续轮询主服务器。如果主服务器变得可达，则 ASA 将恢复使用主服务器。

示例

以下示例将重试次数值配置为 7：

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 7
```

相关命令

命令	说明
class-map type inspect scansafe	为加入白名单的用户和组创建检查类映射。
default user group	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和 / 或组。
http[**s**] (parameters)	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspect scansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器以指示请求来自哪个组织的身份验证密钥。
match user group	匹配白名单的用户或组。
policy-map type inspect scansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafe general-options	配置一般云网络安全服务器选项。
server {**primary** | **backup**}	配置主要或备用云网络安全代理服务器的完全限定域名或 IP 地址。
show conn scansafe	显示所有云网络安全连接，标有大写 Z 标志。
show scansafe server	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是不可达。
show scansafe statistics	显示总计和当前 HTTP 连接数。
user-identity monitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

retry-interval

要配置重试访问之前 **aaa-server host** 命令中所指特定 AAA 服务器的间隔时间，请在 AAA 服务器主机模式下使用 **retry-interval** 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 *seconds*

no retry-interval

语法说明

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。

默认值

默认重试间隔为 10 秒。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
AAA 服务器主机	• 是	• 是	• 是	• 是	—

命令历史

版本	修改
7.0(1)	此命令已根据 CLI 指南进行修改。

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 **timeout** 命令指定 ASA 尝试连接到 AAA 服务器时的时长。

注　无论输入的重试间隔设置是什么，后续重试之间的间隔时间都是 50 或 100 毫秒。这是预期的行为。

示例

以下示例显示情景中的 **retry-interval** 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
ciscoasa(config-aaa-server-host)#
```

相关命令

命令	说明
aaa-server host	进入 AAA 服务器主机配置模式，以便能够配置特定于主机的 AAA 服务器参数。
clear configure aaa-server	从配置中删除所有 AAA 命令语句。
show running-config aaa-server	显示所有 AAA 服务器、特定服务器组、特定服务器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 服务器时的时长。

reval-period

要指定 NAC 框架会话中每次成功安全状态验证之间的间隔时间，请在 nac-policy-nac-framework 配置模式下使用 **reval-period** 命令。要从 NAC 框架策略中删除该命令，请使用此命令的 **no** 形式。

reval-period *seconds*

no reval-period [*seconds*]

语法说明

seconds	每次成功安全状态验证之间的秒数。范围是 300 到 86400。

默认值

默认值为 36000。

命令模式

下表显示可输入命令的模式：

	防火墙模式		安全情景		
				多个	
命令模式	**路由**	**透明**	**单个**	**情景**	**系统**
nac-policy-nac-framework 配置	• 是	—	• 是	—	—

命令历史

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

使用指南

ASA 在每个成功的安全状态验证后启动重新验证计时器。此计时器到期时会触发下一个无条件安全状态验证。 ASA 在重新验证期间保持安全状态验证。如果访问控制服务器在安全状态验证或重新验证时不可用，则会使用默认组策略。

示例

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 策略删除重新验证计时器：

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

相关命令

命令	说明
eou timeout	更改将 EAP over UDP 消息发送到 NAC 框架配置中的远程主机后等待的秒数。
sq-period	指定 NAC 框架会话中每个成功的安全状态验证与下次查询主机状态更改的间隔时间。
nac-policy	创建并访问思科 NAC 策略，然后指定其类型。
debug nac	启用 NAC 框架事件的日志记录。
eou revalidate	强制立即重新验证一个或多个 NAC 框架会话的状态。

revert webvpn all

要从 ASA 闪存删除所有网络相关数据 （定制、插件、转换表、 URL 列表和网络内容），请在特权 EXEC 模式下输入 **revert webvpn all** 命令。

revert webvpn all

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn all** 命令禁用并从 ASA 的闪存删除所有网络相关信息 （定制、插件、转换表、 URL 列表和网络内容）。删除所有网络相关数据会导致在适用时恢复默认设置。

示例

以下命令从 ASA 中删除所有网络相关的配置数据：

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

相关命令

命令	说明
show import webvpn (*option***)**	显示 ASA 的闪存中当前导入的各种 WebVPN 数据和插件 。

revert webvpn AnyConnect-customization

要从定制 AnyConnect 客户端 GUI 的 ASA 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*

语法说明

type	定制文件的类型： • 二进制 - 可执行文件，用于取代 AnyConnect GUI。 • 资源 - 资源文件，如公司徽标。 • 转换 - 用于定制 MSI 的转换。
platform	运行 AnyConnect 客户端的终端设备的操作系统。指定以下各项之一：**linux**、**mac-intel**、 **mac-powerpc**、 **win** 或 **win-mobile**。
name	标识要删除的文件的名称 （最多 64 个字符）。

默认值

此命令没有默认行为。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

有关定制 AnyConnect 客户端 GUI 的详细步骤，请参阅 *AnyConnect VPN Client Administrator Guide* （AnyConnect VPN 客户端管理员指南）。

示例

以下示例删除以前导入为资源文件来定制 AnyConnect GUI 的思科徽标：

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

相关命令

命令	说明
customization	指定要用于隧道组、组或用户的定制对象。
export customization	导出定制对象。
import customization	安装定制对象。
revert webvpn all	删除所有 webvpn 相关数据 （定制、插件、转换表、 URL 列表和网络内容）。
show webvpn customization	显示 ASA 的闪存设备上目前存在的定制对象。

revert webvpn customization

要从 ASA 缓存删除定制对象，请在特权 EXEC 模式下输入 **revert webvpn customization** 命令。

revert webvpn customization *name*

语法说明

name	指定要删除的定制对象的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn customization** 命令可删除指定定制的无客户端 SSL VPN 支持，并且将其从 ASA 的缓存中删除。删除定制对象会导致在适用时恢复默认设置。定制对象包含用于具体指定门户页面的配置参数。

8.0 版软件扩展了用于配置定制的功能，新进程与之前的版本不兼容。在升级到 8.0 软件过程中，安全设备使用旧设置生成新的定制对象，以保留当前配置。此过程只发生一次，由于旧值只是新值的部分子集，因此处理过程不只是从旧格式到新格式的简单转换。

注　在升级到 8.0 版之前，仅当已在 7.2(x) 版配置文件中的适当接口上启用无客户端 SSL VPN (WebVPN) 时， 7.2 版门户定制和 URL 列表才可在 Beta 8.0 配置中运行。

示例

以下命令将删除名为 GroupB 的定制对象：

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

相关命令

命令	说明
customization	指定要用于隧道组、组或用户的定制对象。
export customization	导出定制对象。
import customization	安装定制对象。
revert webvpn all	删除所有 webvpn 相关数据 （定制、插件、转换表、 URL 列表和网络内容）。
show webvpn customization	显示 ASA 的闪存设备上目前存在的定制对象。

revert webvpn plug-in protocol

要从 ASA 的闪存设备删除插件，请在特权 EXEC 模式下输入 **revert webvpn plug-in protocol** 命令。

revert plug-in protocol *protocol*

语法说明

protocol	输入以下字符串之一： • **rdp** 远程桌面协议插件可让远程用户连接到运行 Microsoft 终端服务的计算机。 • **ssh** 安全外壳插件可让远程用户建立到远程计算机的安全信道，或者让远程用户使用 Telnet 连接到远程计算机。 • **vnc** 虚拟网络计算插件可让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。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn plug-in protocol** 命令可禁用并删除对基于 Java 的指定客户端应用的无客户端 SSL VPN 支持，而且将其从 ASA 的闪存驱动器中删除。

示例

以下命令删除 RDP 支持：

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

相关命令

命令	说明
import webvpn plug-in protocol	将指定的插件从 URL 复制到 ASA 的闪存设备。当您发出此命令时，无客户端 SSL VPN 自动支持基于 Java 的客户端应用用于将来的会话。
show import webvpn plug-in	列出 ASA 的闪存设备上存在的插件。

revert webvpn translation-table

要从 ASA 闪存删除转换表，请在特权 EXEC 模式下输入 **revert webvpn translation-table** 命令。

revert webvpn translation-table *translationdomain language*

语法说明

translationdomain	可用的转换域： • AnyConnect • PortForwarder • 横幅 • CSD • 定制 • URL 列表 • （转换来自 RDP、 SSH 和 VNC 插件的消息。）
language	指定要删除的字符编码方法。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn translation-table** 命令可禁用和删除导入的转换表，并且将其从 ASA 的闪存中删除。删除转换表会导致在适用时恢复默认设置。

示例

以下命令删除 AnyConnect 转换表 Dutch：

```
ciscoasa# revert webvpn translation-table anyconnect dutch
ciscoasa
```

相关命令

命令	说明
revert webvpn all	删除所有 webvpn 相关数据 （定制、插件、转换表、 URL 列表和网络内容）。
show webvpn translation-table	显示 ASA 的闪存设备上目前存在的转换表。

revert webvpn url-list

要从 ASA 删除 URL 列表，请在特权 EXEC 模式下输入 **revert webvpn url-list** 命令。

revert webvpn url-list template *name*

语法说明

template *name*	指定 URL 列表的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn url-list** 命令可禁用当前 URL 列表并且将其从 ASA 的闪存驱动器中删除。删除 URL 列表会导致在适用时恢复默认设置。

与 **revert webvpn url-list** 命令一起使用的模板参数指定之前配置的 URL 列表的名称。要配置此类列表，请在全局配置模式下使用 **url-list** 命令。

示例

以下命令删除 URL 列表 servers2：

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

相关命令

命令	说明
revert webvpn all	删除所有 webvpn 相关数据 （定制、插件、转换表、URL 列表和网络内容）。
show running-configuration url-list	显示当前配置的 URL 列表命令集。
url-list （WebVPN 模式）	将 WebVPN 服务器和 URL 的列表应用到特定用户或组策略。

revert webvpn webcontent

要从 ASA 闪存中的某个位置删除指定的网络对象，请在特权 EXEC 模式下输入 **revert webvpn webcontent** 命令。

revert webvpn webcontent *filename*

语法说明

filename	指定包含要删除的网络内容的闪存文件的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

使用 **revert webvpn content** 命令可禁用和删除包含网络内容的文件，以及将其从 ASA 的闪存中删除。删除网络内容会导致在适用时恢复默认设置。

示例

以下命令从 ASA 闪存中删除网络内容文件 ABCLogo：

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

相关命令

命令	说明
revert webvpn all	删除所有 webvpn 相关数据 （定制、插件、转换表、 URL 列表和网络内容）。
show webvpn webcontent	显示 ASA 的闪存中当前存在的网络内容。

revocation-check

要定义是否需要对 trustpool 策略进行撤销检查，请在 crypto ca trustpool 配置模式下使用 **revocation-check** 命令。要恢复默认撤销检查方法 *none*，请使用此命令的 **no** 形式。

revocation-check {[**crl**] [**ocsp**] [**none**] }

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

语法说明

crl	指定 ASA 应使用 CRL 作为撤销检查方法。
none	指定即使所有方法都返回错误， ASA 也应将证书状态解读为有效。
ocsp	指定 ASA 应使用 OCSP 作为撤销检查方法。

默认值

默认值为 *none*。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

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

通常，CA 将其 OCSP 响应者证书的生命周期设为很短时间，以尽可能减小对其安全的影响。CA 在响应者证书中包含 ocsp-no-check 扩展，表示不需要撤销状态检查。但如果没有此扩展，该设备将尝试使用您通过此 **revocation-check** 命令为信任点配置的撤销方法检查证书撤销状态。OCSP 响应者证书如果没有 ocsp-no-check 扩展，也必须可验证，因为除非同时设置 *none* 选项来忽略状态检查，否则 OCSP 证书撤销检查将失败。

注　无论可选参数如何排列， *none* 都必须是最后使用的关键字。

ASA 将按您配置的顺序尝试各种方法，如果上一种方法返回错误 （例如服务器停机），则会尝试第二种和第三种方法，而不是查找撤销的状态。

您可以在验证信任点的客户端证书上设置撤销检查方法，还可以在验证信任点的响应者中配置不撤消检查 (**revocation-check none**)。请参阅 **match certificate** 命令查看配置示例。

如果您使用 **revocation-check crl none** 命令配置了 ASA，则当客户端连接到 ASA 时，会自动开始下载 CRL （因为它尚未缓存），然后验证该证书并完成 CRL 的下载。在此情况下，如果 CRL 未缓存， ASA 将在下载 CRL 之前验证证书。

示例

```
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)#
```

相关命令

命令	说明
crypto ca trustpool policy	进入子模式，提供定义 trustpool 策略的命令。
match certificate allow expired-certificate	管理员可以使特定证书免于到期检查。
match certificate skip revocation-check	管理员可以使特定证书免于撤销检查。

rewrite

要禁用对通过 WebVPN 连接的特定应用或流量类型进行内容重写，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，其中包含唯一标识规则的规则编号。要消除所有重写规则，请使用命令的 **no** 形式（不含规则编号）。

默认情况下， ASA 会重写或转换所有 WebVPN 流量。

rewrite order *integer* {**enable | disable**} **resource-mask** *string* [**name** *resource name*]

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

语法说明

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。
enable	将此重写规则定义为对指定流量启用内容重写的规则。
integer	设置所有配置的规则的顺序。范围是 1 到 65534。
name	（可选）标识应用规则的应用或资源的名称。
order	定义 ASA 应用规则的顺序。
resource-mask	标识适用于规则的应用或资源。
resource name	（可选）指定应用规则的应用或资源。最多 128 个字节。
string	指定要匹配的应用或资源的名称，可以包含正则表达式。您可以使用以下通配符： 指定要匹配的模式，可包含正则表达式。您可以使用以下通配符： * - 与所有内容匹配。您不能单独使用此通配符。它必须附带字母数字字符串。 ？ - 与任何单个字符匹配。 [!seq] - 与不在序列中的任何字符匹配。 [seq] - 与序列中的任何字符匹配。 最多 300 个字节。

默认值

默认为重写所有字符。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.1(1)	引入了此命令。

使用指南

ASA 对应用执行内容重写，以确保它们通过 WebVPN 连接正确呈现。某些应用不需要这种处理，例如外部公共网站。对于这些应用，可以选择关闭内容重写。

您可以使用附带 disable 选项的 rewrite 命令选择性关闭内容重写，让用户直接浏览特定网站而不通过 ASA。这类似于 IPsec VPN 连接中的拆分隧道。

您可以多次使用此命令。配置条目的顺序很重要，因为 ASA 按顺序搜索重写规则，并应用第一条匹配的规则。

示例

以下示例显示如何配置顺序号为 1 的重写规则，此规则将关闭 cisco.com 域中 URL 的内容重写：

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

相关命令

命令	说明
apcf	指定要用于特定应用的非标准规则。
proxy-bypass	配置对特定应用执行最少内容重写。

re-xauth

要规定对 IKE 密钥更新执行 IPsec 用户重新身份验证，请在 group-policy 配置模式下发出 **re-xauth enable** 命令。要禁用对 IKE 密钥更新执行用户重新身份验证，请使用 **re-xauth disable** 命令。

要从运行的配置中删除 re-xauth 属性，请使用此命令的 **no** 形式。这样可从另一个组策略继承 IKE 密钥更新的重新身份验证值。

re-xauth {**enable** [**extended**] | **disable**}

no re-xauth

语法说明

disable	对 IKE 密钥更新禁用重新身份验证
enable	对 IKE 密钥更新启用重新身份验证
extended	扩展在达到配置的 SA 的最长生命周期之前，可以重新输入身份验证凭证的时间。

默认值

禁用对 IKE 密钥更新的重新身份验证。

命令模式

下表显示可输入命令的模式：

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

命令历史

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

使用指南

IKE 密钥更新的重新身份验证仅适用于 IPsec 连接。

如果对 IKE 密钥更新启用重新身份验证，ASA 将在初始阶段 1 IKE 协商过程中提示用户输入用户名和密码，同时还在发生 IKE 密钥更新时为用户身份验证提示输入这些内容。重新身份验证可提供额外的安全。

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。使用 **extended** 关键字，用户可以重新输入身份验证凭证，直到到达配置的 SA 的最长生命周期。

要检查配置的密钥更新间隔，请在监控模式下发出 **show crypto ipsec sa** 命令，以查看安全关联生命周期（以秒为单位和以千字节数据为单位）。

注　如果连接的另一端没有用户，则重新身份验证失败。

示例

以下示例显示如何为名为 FirstGroup 的组策略启用密钥更新的重新身份验证：

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

rip send version

要指定用于在接口上发送 RIP 更新的 RIP 版本，请在接口配置模式下使用 **rip send version** 命令。要恢复默认值，请使用此命令的 **no** 形式。

rip send version {[**1**] [**2**]}

no rip send version

语法说明

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

默认值

ASA 发送 RIP 版本 1 数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

通过在接口上输入 **rip send version** 命令，您可以基于每个接口覆盖全局 RIP 发送版本设置。

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。

示例

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
```

相关命令

命令	说明
rip receive version	指定在特定接口上接收更新时要接受的 RIP 版本。
router rip	启用 RIP 路由过程并进入该进程的路由器配置模式。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rip receive version

要指定在接口上接受的 RIP 版本，请在接口配置模式下使用 **rip receive version** 命令。要恢复默认值，请使用此命令的 **no** 形式。

version {[**1**] [**2**]}

no version

语法说明

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

默认值

ASA 接受版本 1 和版本 2 数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

通过在接口上输入 **rip receive version** 命令，您可以基于每个接口覆盖全局设置。

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。

示例

以下示例将 ASA 配置为在指定接口上接收 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
```

相关命令

命令	说明
rip send version	指定从特定接口发出更新时要使用的 RIP 版本。
router rip	启用 RIP 路由过程并进入该进程的路由器配置模式。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rip authentication mode

要指定在 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 **rip authentication mode** 命令。要恢复默认身份验证方法，请使用此命令的 **no** 形式。

rip authentication mode {**text** | **md5**}

no rip authentication mode

语法说明

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）。

默认值

默认情况下使用明文身份验证。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。

使用 **show interface** 命令可在接口上查看 **rip authentication** 命令。

示例

以下示例显示在 GigabitEthernet0/3 接口上配置 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
```

相关命令

命令	说明
rip authentication key	启用 RIP 版本 2 身份验证并指定身份验证密钥。
rip receive version	指定在特定接口上接收更新时要接受的 RIP 版本。
rip send version	指定从特定接口发出更新时要使用的 RIP 版本。
show running-config interface	显示指定接口的配置命令。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rip authentication key

要启用 RIP 版本 2 数据包的身份验证并指定身份验证密钥，请在接口配置模式下使用 **rip authentication key** 命令。要禁用 RIP 版本 2 身份验证，请使用此命令的 **no** 形式。

rip authentication key [0 | 8] *string* **key_id** *id*

no rip authentication key

语法说明

0	指定将后跟未加密的密码。
8	指定将后跟加密的密码。
id	指定密钥标识值；有效值范围为 1 到 255。
key	指定要用于身份验证密钥字符串的共享密钥。密钥最多可包含 16 个字符。
string	指定未加密 （明文）的用户密码。

默认值

RIP 身份验证已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。启用邻居身份验证后，您必须确保 *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。 *key* 是最多 16 个字符的文本字符串。

使用 **show interface** 命令可在接口上查看 **rip authentication** 命令。

示例

以下示例显示在 GigabitEthernet0/3 接口上配置 RIP 身份验证：

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

相关命令

命令	说明
rip authentication mode	指定在 RIP 版本 2 数据包中使用的身份验证类型。
rip receive version	指定在特定接口上接收更新时要接受的 RIP 版本。
rip send version	指定从特定接口发出更新时要使用的 RIP 版本。
show running-config interface	显示指定接口的配置命令。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rip receive version

要指定在接口上接受的 RIP 版本，请在接口配置模式下使用 **rip receive version** 命令。要恢复默认值，请使用此命令的 **no** 形式。

version {[**1**] [**2**]}

no version

语法说明

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

默认值

ASA 接受版本 1 和版本 2 数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

通过在接口上输入 **rip receive version** 命令，您可以基于每个接口覆盖全局设置。

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。

示例

以下示例将 ASA 配置为在指定接口上接收 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
```

相关命令

命令	说明
rip send version	指定从特定接口发出更新时要使用的 RIP 版本。
router rip	启用 RIP 路由过程并进入该进程的路由器配置模式。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rip send version

要指定用于在接口上发送 RIP 更新的 RIP 版本，请在接口配置模式下使用 **rip send version** 命令。要恢复默认值，请使用此命令的 **no** 形式。

rip send version {[**1**] [**2**]}

no rip send version

语法说明

1	指定 RIP 版本 1。
2	指定 RIP 版本 2。

默认值

ASA 发送 RIP 版本 1 数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

通过在接口上输入 **rip send version** 命令，您可以基于每个接口覆盖全局 RIP 发送版本设置。

如果您指定 RIP 版本 2，则可以启用邻居身份验证和使用基于 MD5 的加密来对 RIP 更新进行身份验证。

示例

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
```

相关命令

命令	说明
rip receive version	指定在特定接口上接收更新时要接受的 RIP 版本。
router rip	启用 RIP 路由过程并进入该进程的路由器配置模式。
version	指定 ASA 在全局范围内使用的 RIP 版本。

rmdir

要删除现有目录，请在特权 EXEC 模式下使用 **rmdir** 命令。

rmdir [/noconfirm] [disk0: | disk1: | flash:]*path*

语法说明

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

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式。

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

如果该目录不为空，则 **rmdir** 命令将失败。

示例

以下示例显示如何删除名为 “test” 的现有目录：

```
ciscoasa# rmdir test
```

相关命令

命令	说明
dir	显示目录内容。
mkdir	创建新目录。
pwd	显示当前工作目录。
show file	显示关于文件系统的信息。

route

要输入指定接口的静态或默认路由，请在全局配置模式下使用 **route** 命令。要从指定接口删除路由，请使用此命令的 **no** 形式。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

语法说明

gateway_ip	指定网关路由器的 IP 地址 （此路由的下一跃点地址）。 **注**　*gateway_ip* 参数在透明模式下是可选的。
interface_name	指定用于路由流量的内部或外部网络接口名称。
ip_address	指定内部或外部网络 IP 地址。
metric	（可选）指定此路由的管理距离。有效值范围为 1 到 255。默认值为 1。
netmask	指定要应用于 *ip_address* 的网络掩码。
track *number*	（可选）将跟踪条目与此路由关联。有效值为从 1 到 500。 **注**　**track** 选项仅在单一路由模式下可用。
tunneled	指定该路由作为 VPN 流量的默认隧道网关。

默认值

metric 默认值为 1。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
7.2(1)	添加了 **track** *number* 值。

使用指南

使用 **route** 命令可输入接口的默认或静态路由。要输入默认路由，请将 *ip_address* 和 *netmask* 设置为 **0.0.0.0**，或使用缩短形式 **0**。保存后，使用 **route** 命令输入的所有路由都存储在配置中。

除了标准默认路由以外，您可以定义用于隧道流量的单独默认路由。使用 **tunneled** 选项创建默认路由后，来自 ASA 上终止隧道的所有流量 （无法使用已获知或静态路由进行路由）都将发送到此路由。对于来自隧道的新兴流量，此路由将覆盖任何其他已配置或已获知的默认路由。

以下限制适用于具有 **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 (**ip verify reverse-path**)。在隧道路由的传出接口上启用 uRPF 将导致会话失败。
- 请勿在隧道路由的传出接口上启用 TCP 拦截，因为会话将会失败。
- 请勿将 VoIP 检查引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS 检查引擎或 DCE RPC 检查引擎与隧道路由一起使用。这些检查引擎将忽略隧道路由。

您无法通过 **tunneled** 选项定义多个默认路由；不支持对隧道流量使用 ECMP。

创建静态路由以访问与任何接口上的路由器外部连接的网络。例如， ASA 采用以下静态 **route** 命令，通过 192.168.1.5 路由器发送目标为 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 CONNECT 路由。使用 **clear route** 或 **clear configure route** 命令时不会删除此条目。

如果 **route** 命令使用 ASA 上接口之一的 IP 地址作为网关 IP 地址，则 ASA 将对数据包中的目标 IP 地址执行 ARP 命令而不是对网关 IP 地址执行 ARPing 命令。

示例

以下示例显示如何为外部接口指定一条默认 **route** 命令：

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

以下示例显示如何添加这些静态 **route** 命令以提供对网络的访问权限：

```
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 操作将默认路由安装到外部接口上的 10.1.1.1 网关。SLA 操作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
```

相关命令

命令	说明
clear configure route	删除静态配置的 **route** 命令。
clear route	删除通过动态路由协议 （如 RIP）获知的路由。
show route	显示路由信息。
show running-config route	显示配置的路由。

route-map

要定义在不同路由协议之间重分布路由的条件，或启用策略路由，请在全局配置模式下使用 **route-map** 命令或在 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。

route-map *name* [**permit** | **deny**] [*sequence number*]

no route-map *name* [**permit** | **deny**] [*sequence number*]

语法说明

name	定义有意义的路由映射名称。重分布路由器配置命令使用此名称来引用此路由映射。多个路由映射可以共享相同的名称。
permit	（可选）如果满足此路由映射的匹配条件，并且指定了 **permit** 关键字，则该路由如设置操作所控制进行重分布。如果是策略路由，则数据包进行策略路由。 如果不满足匹配条件，并指定了 **permit** 关键字，则测试具有相同映射标记的下一个路由映射。如果路由没有通过共享相同名称的路由映射组的匹配条件，则不会通过该设置重分布。 **permit** 关键字为默认值。
deny	（可选）如果满足路由映射的匹配条件，并且指定了 **deny** 关键字，则路由不会重分布。如果是策略路由，则数据包不会进行策略路由，并且不会检查共享相同映射标记名称的其他路由映射。如果数据包没有进行策略路由，则使用正常的转发算法。
sequence-number	（可选）表示新路由映射在已采用相同名称配置的路由映射列表中的位置。如果通过此命令的 no 形式指定，应删除路由映射的位置。

默认值

没有默认值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。

使用指南

使用路由映射重分布路由

使用 **route-map** 全局配置命令以及 match 和 set route-map 配置命令可定义在不同路由协议之间重分布路由的条件。每条 **route-map** 命令都有关联的 match 和 set 命令列表。match 命令指定匹配条件 - 允许当前 route-map 命令重分布的条件。 set 命令指定设置操作 - 在满足 match 命令实施的条件时要执行的特定重分布操作。 **no route-map** 命令删除路由映射。

match 路由映射配置命令有多种格式。可以按任何顺序指定 match 命令，并且所有 match 命令都必须 “ 通过 ” 才可使路由根据 set 命令指定的设置操作重分布。 match 命令的 no 形式可删除指定的匹配条件。

当您想要详细控制路由如何在路由过程之间重分布时，使用路由映射。目标路由协议是您通过路由器全局配置命令指定的协议。源路由协议是您通过重分布路由器配置命令指定的协议。有关如何配置路由映射的示例，请参阅 “ 示例 ” 部分。

当您通过路由映射传递路由时，一个路由映射可以有多个部分。不匹配至少一个与 route-map 命令相关的匹配子句的任何路由都会被忽略；也就是说，该路由将不会通告出站路由映射，并且将不接受入站路由映射。如果想要只修改部分数据，则必须配置第二个路由映射部分，并指定显式匹配。

sequence-number 参数的工作原理如下：

1. 如果没有采用路由映射名称定义的条目，则通过将 sequence-number 参数设置为 10 创建条目。
2. 如果只有一个采用路由映射名称定义的条目，则该条目成为以下 route-map 命令的默认条目。该条目的 sequence-number 参数将保持不变。
3. 如果采用路由映射名称定义了多个条目，则输出错误消息，指出需要 sequence-number 参数。
4. 如果指定了 **no route-map name** 命令 （不带 sequence-number 参数），则删除整个路由映射。

示例

以下示例显示如何将跃点数等于 1 的路由重分布到 OSPF 中。ASA 将这些路由作为度量为 5 和度量类型为 Type 1 （类型 1）的外部 LSA 重分布：

```
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
```

以下示例显示如何采用配置的度量值将 10.1.1.0 静态路由重分布到 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
```

相关命令

命令	说明
redistribute	将路由从一个路由域重分布到另一个路由域。
route	创建接口的静态或默认路由。
router	进入指定协议的路由器配置模式。

route null0

静态 null0 路由用于将不想要或不需要的流量转发到黑洞。空接口 null0 用于创建黑洞。在全局配置模式下使用 **route null0** 命令为不需要的目标创建静态路由。此静态路由配置指向空接口。

要删除静态 null0 路由，请使用此命令的 **no** 形式。

route null0 *ip_address*

no route null0 *ip_address*

语法说明

ip_address	指定内部或外部网络 IP 地址。

默认值

默认情况下，静态 null 0 路由已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

静态路由针对不需要的目标创建，并且静态路由配置指向空接口。目标地址与黑洞静态路由最佳匹配的任何流量都将自动丢弃。与 ACL 不同，静态 null0 路由不会导致任何性能下降。

静态 null0 路由配置用于防止路由环路。 BGP 利用静态 null0 配置进行远程触发黑洞路由。

示例

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
```

router-alert

要定义具有 IP 选项检查的数据包中出现 Router Alert （路由器警报） IP 选项时的操作，请在参数配置模式下使用 **router-alert** 命令。要禁用此功能，请使用此命令的 **no** 形式。

router-alert action {allow | clear}

no router-alert action {allow | clear}

语法说明

allow	指示 ASA 允许包含 Router Alert （路由器警报） IP 选项的数据包通过。
clear	指示 ASA 从数据包清除 Router Alert （路由器警报） IP 选项，然后允许该数据包通过。

默认值

默认情况下， IP 选项检查丢弃包含 Router Alert （路由器警报） IP 选项的数据包。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(2)	引入了此命令。

使用指南

此命令可在 IP 选项检查策略映射中进行配置。

您可以配置 IP 选项检查以控制允许哪些具有特定 IP 选项的 IP 数据包通过 ASA。配置此检查将指示 ASA 允许数据包通过，或清除指定的 IP 选项后允许该数据包通过。

路由器警报 (RTRALT) 或 IP 选项 20 通知中转路由器检查该数据包的内容，即使数据包的目标并非该路由器。此检查在实施 RSVP 时十分有用，类似的协议需要沿着数据包交付路径从路由器中进行相对较复杂的处理。

示例

以下示例显示如何在策略映射中设置用于协议违反行为的操作：

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

相关命令

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

router-id

要使用固定路由器 ID，请在路由器配置模式下 （适用于 OSPFv2）或在 IPv6 路由器配置模式下（适用于 OSPFv3）使用 **router-id** 命令。要将 OSPF 重置为使用以前的路由器 ID 行为，请使用此命令的 **no** 形式。

router-id *id*

no router-id [*id*]

语法说明

id	以 IP 地址格式指定路由器 ID。

默认值

如果没有指定，则使用 ASA 上最高级别的 IP 地址作为路由器 ID。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
8.0(2)	此命令的处理顺序已更改。该命令现在会在 OSPFv2 配置中的 **network** 命令之前进行处理。
9.0(1)	支持多情景模式和 OSPFv3。

使用指南

默认情况下，ASA 使用 OSPF 配置中的 **network** 命令所涵盖接口上最高级别的 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：要使用特定的路由器 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 路由域内必须唯一。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 配置中应先输入 **router-id** 命令，然后再输入 **network** 命令。这可以防止与通过 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，如果所有设备接收相同的路由器 ID，则您需要配置 **router-id** *id* 命令或将路由器 ID 留空。

示例

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)#
```

相关命令

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

router-id cluster-pool

要指定第 3 层集群部署的路由器 ID 集群池，请在路由器配置模式下 （适用于 OSPFv2）或在 IPv6 路由器配置模式下 （适用于 OSPFv3）使用 **router-id cluster-pool** 命令。

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

语法说明

cluster-pool	配置第 3 层集群后，允许配置 IP 地址池。
hostname | A.B.C.D	指定此 OSPF 进程的 OSPF 路由器 ID。
ip_pool	指定 IP 地址池的名称。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.0(1)	引入了此命令。

使用指南

路由器 ID 在集群中的 OSPFv2 或 OSPFv3 路由域内必须唯一。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，如果所有设备接收相同的路由器 ID，则您需要配置 **router-id** *id* 命令或将路由器 ID 留空。

配置第 3 层集群接口后，每个设备必须有唯一的接口 IP 地址。要确保每个设备有唯一的接口 IP 地址，您可以使用 **router-id cluster-pool** 命令配置 OSPFv2 或 OSPFv3 的本地 IP 地址池。

示例

以下示例显示为 OSPFv2 配置第 3 层集群后如何配置 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
```

以下示例显示为 OSPFv3 配置第 3 层集群后如何配置 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
```

相关命令

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

router bgp

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

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

语法说明

autonomous-system-number	向其他 BGP 路由器标识本路由器并标记沿途所传递路由信息的自主系统编号。编号在从 1 到 65535 的范围内。

默认值

默认情况下，未启用任何 BGP 路由过程。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
9.2(1)	引入了此命令。

使用指南

此命令可设置分布式路由核心，用于自动保证路由信息在自主系统之间的无环路交换。

在 2009 年 1 月以前，分配给公司的 BGP 自主系统编号是范围为 1 到 65535 的 2 个八进制数字，如 RFC 4271 的*边界网关协议 4 (BGP-4)* 中所规定。

由于自主系统编号需求的增加，互联网编号授权委员会 (IANA) 将分配范围为 65536 到 4294967295 的四个八进制自主系统编号。

RFC 5396 的*自主系统 (AS) 编号的文本表示*部分记录了表示自主系统编号的三种方法。思科已实施以下两种方法：

- Asplain - 十进制数值表示法，其中 2 个字节和 4 个字节的自主系统编号均通过其十进制数值表示。例如， 65526 是 2 个字节的自主系统编号，而 234567 是 4 个字节的自主系统编号。
- Asdot - 自主系统点表示法，其中 2 个字节的自主系统编号通过其十进制数值表示，而 4 个字节的自主系统编号通过点表示法来表示。例如， 65526 是 2 个字节的自主系统编号，而 1.169031 是 4 个字节的自主系统编号 （这是 234567 十进制数值的点表示法）。

有关表示自主系统编号的第三种方法的详细信息，请参阅 RFC 5396。

示例

以下示例显示如何配置自主系统编号为 100 的 BGP 进程：

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

相关命令

命令	说明
show route bgp	显示路由表。
show bgp summary	显示所有边界网关协议 (BGP) 连接的状态

router eigrp

要启动 EIGRP 路由过程并配置该进程的参数，请在全局配置模式下使用 **router eigrp** 命令。要禁用 EIGRP 路由，请使用此命令的 **no** 形式。

router eigrp *as-number*

no router eigrp *as-number*

语法说明

as-number	标识到其他 EIGRP 路由器的路由的自主系统编号。它还用于标记路由信息。有效值为从 1 到 65535。

默认值

EIGRP 路由已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.0(2)	引入了此命令。

使用指南

router eigrp 命令创建一个 EIGRP 路由过程或进入现有 EIGRP 路由过程的路由器配置模式。您只能在 ASA 上创建一个 EIGRP 路由过程。

使用以下路由器配置模式命令以配置 EIGRP 路由过程：

- **auto-summary** - 启用 / 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。
- **default-metric** - 定义重分布到 EIGRP 路 由进程中的路由的默认度量。
- **distance eigrp** - 配置内部和外部 EIGRP 路由的管理距离。
- **distribute-list** - 过滤路由更新中接收和发送的网络。
- **eigrp log-neighbor-changes** - 启用 / 禁用记录邻居状态变化。
- **eigrp log-neighbor-warnings** - 启用 / 禁用记录邻居警告消息。
- **eigrp router-id** - 创建固定路由器 ID。
- **eigrp stub** - 配置 ASA 用于末节 EIGRP 路由。
- **neighbor** - 静态定义 EIGRP 邻居。
- **network** - 配置参与 EIGRP 路由过程的网络。

- **passive-interface** - 配置充当被动接口的接口。
- **redistribute** - 将来自其他路由过程的路由重分布到 EIGRP 中。

使用以下接口配置模式命令配置接口特定的 EIGRP 参数：

- **authentication key eigrp** - 定义用于 EIGRP 消息身份验证的身份验证密钥。
- **authentication mode eigrp** - 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-interval eigrp** - 更改从接口发出 EIGRP 问候数据包的间隔。
- **hold-time eigrp** - 更改 ASA 通告的保持时间。
- **split-horizon eigrp** - 在接口上启用 / 禁用 EIGRP 水平拆分。
- **summary-address eigrp** - 手动定义汇总地址。

示例

以下示例显示如何进入自主系统编号为 100 的 EIGRP 路由过程的配置模式：

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

相关命令

命令	说明
clear configure eigrp	从运行的配置中清除 EIGRP 路由器配置模式命令。
show running-config router eigrp	显示运行的配置中的 EIGRP 路由器配置模式命令。

router ospf

要启动 OSPF 路由过程并配置此进程的参数，请在全局配置模式下使用 **router ospf** 命令。要禁用 OSPF 路由，请使用此命令的 **no** 形式。

router ospf *pid*

no router ospf *pid*

语法说明

pid	内部使用的 OSPF 路由过程标识参数；有效值为 1 到 65535。*pid* 无需匹配其他路由器上的 OSPF 进程 ID。

默认值

OSPF 路由已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.0(1)	引入了此命令。
9.0(1)	支持多情景模式。

使用指南

router ospf 命令是 ASA 上运行的 OSPF 路由过程的全局配置命令。输入 **router ospf** 命令后，命令提示符将显示为 (config-router)#，表示您处于路由器配置模式下。

使用 **no router ospf** 命令时，无需指定可选的参数，除非其提供了必要的信息。**no router ospf** 命令终止通过其 *pid* 指定的 OSPF 路由进程。您可在 ASA 上本地分配 *pid*。您必须为每个 OSPF 路由过程分配唯一的值。

router ospf 命令与以下 OSPF 特定命令一起使用以配置 OSPF 路由过程：

- **area** - 配置常规的 OSPF 区域。
- **compatible rfc1583** - 恢复用于根据 RFC 1583 计算汇总路由成本的方法。
- **default-information originate** - 在 OSPF 路由域中生成默认的外部路由。
- **distance** - 根据路由类型定义 OSPF 路由管理距离。
- **ignore** - 当路由器收到类型 6 组播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制系统日志消息发送。
- **log-adj-changes** - 配置路由器以在 OSPF 邻居启动或关闭时发送系统日志消息。
- **neighbor** - 指定邻居路由器。用于允许在 VPN 隧道上建立邻接关系。

- **network** - 定义用于运行 OSPF 的接口及这些接口的区域 ID。
- **redistribute** - 根据指定的参数配置在不同路由域之间重分布路由。
- **router-id** - 创建固定路由器 ID。
- **summary-address** - 创建 OSPF 的汇聚地址。
- **timer lsa arrival** - 定义两次接受来自 OSPF 邻居的相同链路状态通告 (LSA) 之间的最短间隔（以毫秒为单位）。
- **timer pacing flood** - 定义泛洪队列中 LSA 两次更新之间的最短间隔 （以毫秒为单位）。
- **timer pacing lsa-group** - 定义刷新或最大化寿命的 LSA 组之间的间隔 （以秒为单位）。
- **timer pacing retransmission** - 定义两次邻居重新传输之间的最短间隔 （以毫秒为单位）。
- **timer throttle lsa** - 定义生成第一次出现的 LSA 的延迟 （以毫秒为单位）。
- **timer throttle spf** - 定义接收 SPF 计算变化之间的延迟 （以毫秒为单位）。

示例

以下示例显示如何进入编号为 5 的 OSPF 路由过程的配置模式：

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

相关命令

命令	说明
clear configure router	从运行的配置中清除 OSPF 路由器命令。
show running-config router ospf	显示运行的配置中的 OSPF 路由器命令。

router rip

要启动 RIP 路由过程并配置该进程的参数，请在全局配置模式下使用 **router rip** 命令。要禁用 RIP 路由过程，请使用此命令的 **no** 形式。

router rip

no router rip

语法说明

此命令没有任何参数或关键字。

默认值

RIP 路由已禁用。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

使用指南

router rip 命令是用于配置 ASA 上的 RIP 路由过程的全局配置命令。您只能在 ASA 上配置一个 RIP 路由过程。 **no router rip** 命令终止 RIP 路由过程并删除该进程的所有路由器配置。

输入 **router rip** 命令后，命令提示符将更改为 ciscoasa(config-router)#，表示您处于路由器配置模式下。

router rip 命令与以下路由器配置命令一起使用以配置 RIP 路由过程：

- **auto-summary** - 启用 / 禁用路由自动汇总。
- **default-information originate** - 分布默认路由。
- **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** - 在路由过程中添加 / 删除接口。
- **passive-interface** - 将特定接口设置为被动模式。
- **redistribute** - 将来自其他路由过程的路由重分布到 RIP 路由过程中。
- **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，基于每个接口配置 RIP 属性：

- **rip authentication key** - 设置身份验证密钥。
- **rip authentication mode** - 设置 RIP 版本 2 使用的身份验证类型。
- **rip send version** - 设置用于从接口发出更新的 RIP 版本。这将覆盖在全局路由器配置模式下设置的版本 （如果有）。
- **rip receive version** - 设置接口接受的 RIP 版本。这将覆盖在全局路由器配置模式下设置的版本 （如果有）。

RIP 在透明模式下不支持。默认情况下， ASA 拒绝所有 RIP 广播和组播数据包。要允许在透明模式下通过 ASA 操作传递这些 RIP 消息，您必须定义访问列表条目以允许此流量。例如，要允许 RIP 版本 2 流量通过 ASA，请创建访问列表条目，如下所示：

```
ciscoasa(config)# access-list myriplist extended permit ip any host 224.0.0.9
```

要允许 RIP 版本 1 广播，请创建访问列表条目，如下所示：

```
ciscoasa(config)# access-list myriplist extended permit udp any any eq rip
```

使用 **access-group** 命令将这些访问列表条目应用到相应的接口。

您可以在 ASA 上同时启用 RIP 和 OSPF 路由。

示例

以下示例显示如何进入编号为 5 的 OSPF 路由过程的配置模式：

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

相关命令

命令	说明
clear configure router rip	从运行的配置中清除 RIP 路由器命令。
show running-config router rip	显示运行的配置中的 RIP 路由器命令。

rtp-conformance

要检查针孔上流动的 RTP 数据包的 H.323 和 SIP 协议合规性，请在参数配置模式下使用 **rtp-conformance** 命令。要禁用此功能，请使用此命令的 **no** 形式。

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

语法说明

enforce-payloadtype	根据信令交换将负载类型强制设为音频 / 视频。

默认值

没有默认行为或值。

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
7.2(1)	引入了此命令。

示例

以下示例显示如何检查针孔上流动的 RTP 数据包 H.323 呼叫的协议合规性：

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

相关命令

命令	说明
class	在策略映射中标识类映射名称。
class-map type inspect	创建检查类映射以匹配特定于应用的流量。
debug rtp	显示与 H.323 和 SIP 检查关联的 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。
show running-config policy-map	显示所有当前的策略映射配置。

rtp-min-port rtp-max-port

要配置电话代理功能的 rtp-min-port 和 rtp-max-port 限制，请在 phone-proxy 配置模式下使用 **rtp-min-port** *port1* **rtp-max-port** *port2* 命令。

要从电话代理配置中取消 rtp-min-port 和 rtp-max-port 限制，请使用此命令的 **no** 形式。

rtp-min-port *port1* **rtp-maxport** *port2*

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

语法说明

port1	指定媒体终端点 RTP 端口范围的最小值，其中 *port1* 可为 1024 到 16384 的值。
port2	指定媒体终端点 RTP 端口范围的最大值，其中 *port2* 可为 32767 到 65535 的值。

默认值

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

命令模式

下表显示可输入命令的模式：

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

命令历史

版本	修改
8.2(1)	引入了此命令。

使用指南

当您需要扩展电话代理支持的呼叫数量时，配置媒体终端点的 RTP 端口范围。

示例

以下示例显示使用**媒体终端地址**命令指定用于媒体连接的 IP 地址：

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

相关命令

命令	说明
phone-proxy	配置电话代理实例。