int – ipu

- integrity， 第 3 页
- intercept-dhcp， 第 5 页
- interface （全局），第 7 页
- interface (vpn load-balancing)，第 10 页
- interface bvi，第 12 页
- interface loopback，第 15 页
- interface-policy，第 17 页
- interface port-channel，第 19 页
- interface redundant，第 21 页
- interface tunnel，第 23 页
- interface vlan，第 24 页
- interface vni，第 27 页
- interim-accounting-update，第 29 页
- internal-password，第 31 页
- internal-port，第 33 页
- internal-segment-id，第 35 页
- interval maximum，第 37 页
- invalid-ack，第 39 页
- ip address，第 41 页
- ip address dhcp，第 44 页
- ip address pppoe，第 46 页
- ip-address-privacy，第 48 页
- ip audit attack，第 49 页
- ip audit info，第 51 页
- ip audit interface，第 53 页
- ip audit name，第 55 页
- ip audit signature，第 57 页
- ip-client，第 62 页
- ip-comp，第 63 页

- ip local pool， 第 65 页
- ip unnumbered， 第 67 页
- ip-phone-bypass， 第 68 页
- ips， 第 70 页
- ipsec-udp， 第 73 页
- ipsec-udp-port， 第 75 页

integrity

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

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

Syntax Description

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

Command Default

默认为 **sha(**SHA 1算法）。

使用指南

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

Command Modes

下表展示可输入命令的模式：

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

Command History

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

CR_Examples

以下示例进入 IKEv2 策略配置模式并将完整性算法设置为 MD5：

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

Related Commands

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

intercept-dhcp

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

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

Syntax Description

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

Command Default

DHCP 拦截已禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局策略配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

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

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

CR_Examples

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

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

interface （全局）

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

对于物理接口（适用于除 ASASM 之外的所有型号）：

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

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

对于分配了映射名称的多情景模式：

interface*mapped_name*

Syntax Description

mapped_name	在多上下文模式下，如果使用命令分配了映射名称，则指定映射名 **allocate-interface** 称。
physical_interface	将物理接口类型、插槽和端口号指定为 *type*[*slot*/]*port*。类型和插槽/端口之间的空格是可选的。 物理接口类型包括： • **ethernet** • gigabitethernet • **tengigabitethernet** • **management** 输入类型，后跟插槽/端口，例如， **gigabitethernet0/1**。 管理接口仅用于管理流量。但是，如果需要，也可以将其用于直通流量，具体取决于您的型号（请参阅 **management-only** 命令）。 请参阅相应型号的硬件文档以确定接口类型、插槽和端口号。
subinterface	指定 1 至 4294967293 之间的整数，用于指定逻辑子接口。子接口的最大数量取决于您的 ASA 型号。子接口不适用于 ASA 5505、ASASM，也不适用于 ASA 5512-X 至 ASA 5555-X 上的管理接口。有关每个平台的最大子接口（或 VLAN）数，请参阅配置指南。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。

Command Default

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

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

接口的默认状态取决于类型和上下文模式：

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

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

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

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

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

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

CR_Examples

以下示例在单模式下配置物理接口的参数：

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

以下示例在单模式下配置子接口的参数：

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

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

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

以下示例以多上下文模式配置上下文配置的参数：

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

Related Commands

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
member-interface	将接口分配给冗余接口。
clearinterface	清除命令的计数 **showinterface**器。
showinterface	显示接口的运行时间状态和统计信息。
vlan	为子接口分配 VLAN。

interface (vpn load-balancing)

要在 VPN 负载均衡虚拟集群中为 VPN 负载均衡指定非默认公共或专用接口，请在 vpn load-balancing 模式下使用 **interface**命令。要删除接口规范并恢复为默认接口，请使用此命令的 **no** 形式。

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

Syntax Description

interface-name	要配置为 VPN 负载均衡集群的公共或专用接口的接口的名称。
lbprivate	指定此命令配置 VPN 负载均衡的专用接口。
lbpublic	指定此命令为 VPN 负载均衡配置公共接口。

Command Default

如果省略 **interface** 命令，则 **lbprivate** 接口默认为 **inside**， **lbpublic** 接口默认为 **outside**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
vpn load-balancing	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

首先，必须已使用 **vpnload-balancing**命令进入 vpn load-balancing 配置模式。

此外，之前还必须使用过 **interface**、 **ipaddress** 和 **nameif** 命令来配置和分配名称到您在此命令中指定的接口。

CR_Examples

以下是命令序列的示例，其 **vpnload-balancing** 中包括一个命令，该命令 **interface** 将集群的公共接口指定为“测试”，并将集群的私有接口恢复为默认值（内部）：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
```

```
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# nointerface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

ciscoasa(config-load-balancing)# **participate**

Related Commands

命令	说明
vpnload-balancing	进入 vpn 负载均衡配置模式。

interface bvi

要为网桥组配置网桥虚拟接口 (BVI)，请在全局配置模式下使用**interfacebvi** 命令。要删除 BVI 配置，请使用此命 **no**令的形式。

interface bvi*bridge_group_number*
no interface bvi*bridge_group_number*

Syntax Description

bridge_group_number	将网桥组编号指定为介于 1 和 100 之间的整数；对于 9.3(1) 及更高版本，范围扩大到 1 到 250 之间。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.4(1)	添加了此命令。
9.3(1)	编号范围扩大到 1 到 250，以支持 250 个 BVI。
9.6(2)	每个网桥组的最大接口数量已从 4 增加到 64。

使用指南

使用此命令可进入接口配置模式，以便为您的网桥组配置管理 IP 地址。如果不想产生安全情景开销，或者要最大限度地使用安全情景，请将接口一起组合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组的流量与其他网桥组是分离的；流量不会路由至ASA中的另一个网桥组，并且流量必须退出 ASA 后才能通过外部路由器路由回 ASA 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或AAA服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。每个情景或在单模式下至少需要一个网桥组。

每个网桥组都需要一个管理 IP 地址。ASA 使用该 IP 地址作为源自网桥组的数据包的源地址。管理 IP 地址必须与已连接网络位于同一子网上。对于 IPv4 流量，需要管理 IP 地址来传递任何流量。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。对于另一种管理方法，您可以独立于任何网桥组配置管理接口。

对于9.2及更早版本，您可以在单模式下或多模式下的每个情景配置最多8个网桥组；对于9.3(1)及更高版本，最多可以配置250个网桥组。每个网桥组可包括最多4个接口。在9.6(2)及更高版本中，您可以向一个网桥组添加最多64个接口。您不能将同一接口分配至多个网桥组。请注意，您必须至少使用 1 个网桥组；数据接口必须属于网桥组。

注释 尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。

注释 对于单独的management接口，不可配置的桥组 (ID 301) 会自动添加至您的配置。此网桥组未包含在网桥组限制中。

注释 ASA 不支持辅助网络上的流量；仅支持与管理 IP 地址位于同一网络上的流量。

CR_Examples

以下示例包括两个桥接组，每个组有三个接口，外加一个仅管理接口：

```
interface gigabitethernet 0/0
nameif inside
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside
security-level 0
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
nameif inside
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
nameif dmz
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
```

```
interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

Related Commands

命令	说明
ace/bvi	清除桥虚拟接口配置。
bridge-group	将透明防火墙接口分组到桥接组中。
interface	配置接口。
ipaddress	设置桥组的管理IP地址。
show bridge-group	显示网桥组信息，包括成员接口和IP地址。
显示运行配置接口bvi	显示该桥组接口配置。

interface loopback

要创建环回接口，请在 **interfaceloopback** 全局配置模式下使用该命令。使用命 **no**令的形式删除环回接口。

interface loopback编号
no interface loopback*number*

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式。

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

使用指南

环回接口是一种会模拟物理接口的纯软件接口。环回接口可通过多个物理接口来访问。您只能将环回接口用于传入/传出设备的流量。

以下功能支持环回接口：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- 系统日志
- Telnet
- VTI 源接口

Command History

版本	修改
9.18(2)	添加了此命令。
9.19(1)	添加了对 VTI 的支持。

版本	修改
9.20(1)	增加了对 DNS、HTTP 和 ICMP 的支持。

CR_Examples

以下示例创建新的环回接口：

```
ciscoasa(config)# interface loopback 10
```

Related Commands

命令	说明
tunnelsourceinterface	指定用于创建 VTI 隧道的源接口。
ssh	为接口配置 SSH。
logging host	指定系统日志主机。
neighbor update-source	将接口配置为 BGP 邻居的源。
snmp-server host	指定 SNMP 服务器。
telnet	为接口配置 Telnet。

interface-policy

要指定在监控功能检测到接口故障时的故障转移策略，请在故障转移组配置模式下使用**interface-policy**命令。要恢复默认值，请使用此 **no**命令的形式。

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

Syntax Description

num	使用百分比形式时，指定 1 到 100 之间的数字，或者 1 到最大接口数。
%	（可选）指定 number *num* 是受监控接口的百分比。

Command Default

如果为设备配置了 **failoverinterface-policy** 命令，则 **interface-policyfailovergroup** 命令的默认值采用该值。如果不是，则 *num* 为 1。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

num 参数和可选的 **%** 关键字之间没有空格。

如果故障接口的数量符合配置的策略且另一台 ASA 正常运行，则此 ASA 会将自身标记为发生故障，并且可能发生故障转移（如果是主用 ASA 发生故障）。只有通过 **monitor-interface** 命令指定为监控的接口才会计入策略。

CR_Examples

以下部分示例显示了故障转移组的一种可能配置：

```
ciscoasa(config)# failover group 1

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

Related Commands

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failoverinterface-policy	配置接口监控策略。
monitor-interface	指定正在监控故障转移的接口。

interface port-channel

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

interfaceport-channel编号
no interface port-channel*number*

Syntax Description

number 指定 EtherChannel 通道组 ID，介于 1 和 48 之间。在将接口添加到通道组时，将自动创建此接口。如果尚未添加接口，则此命令会创建端口通道接口。

注释
您需要向端口通道接口添加至少一个成员接口，然后才能为其配置逻辑参数（例如名称）。

Command Default

默认情况下，端口通道接口已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

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

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

注释 ASA 5505 或 ASASM 不支持此命令。您不能将 4GE SSM 上的接口（包括 ASA 5550 上插槽 1 中的集成 4GE SSM）用作 EtherChannel 的一部分。

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例将三个接口配置为 EtherChannel 的一部分。此示例还将系统优先级设置为较高的优先级，并在 EtherChannel 分配有超过 8 个接口的情况下将千兆以太网 0/2 的优先级设置为高于其他接口。

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

interface redundant

要配置冗余接口并进入接口配置模式，请在 **interfaceredundant** 全局配置模式下使用该命令。要删除冗余接口，请使用此命 **no**令的形式。

interface redundant编号
no interface redundant*number*

Syntax Description

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

Command Default

默认情况下，冗余接口已启用。但是，要使流量通过冗余接口，还必须启用成员物理接口。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

冗余接口是将活动物理接口和备用物理接口配对（参见 **member-interface**命令）。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。

所有 ASA 配置均引用逻辑冗余接口，而不是成员物理接口。

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

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

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

注释 ASA 5505 或 ASASM 不支持此命令。

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

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

interface tunnel

要创建新的 VTI 隧道接口，请使用全 **interfacetunnel** 局配置模式下的命令。使用该命令的no形式删除VTI隧道接口。

interface tunnel编号
no interface tunnel*number*

Syntax Description

number 为隧道接口分配编号。该值可以是0-1024之间的任意值。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式。

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

Command History

版本	修改
9.7(1)	引入了此命令及其子模式。
9.16（1）	每设备支持的隧道接口数量从100增加到1024。

CR_Examples

以下示例创建新的隧道接口：

```
ciscoasa(config)# interface tunnel 10
```

Related Commands

命令	说明
tunnelsourceinterface	指定用于创建 VTI 隧道的源接口。
tunneldestination	指定 VTI 隧道目标的 IP 地址。
tunnelmode	指定将 IPsec 用于隧道保护。
tunnelprotectionipsec	指定将用于隧道保护的IPsec配置文件。

interface vlan

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

interface vlan编号
no interface vlan*number*

Syntax Description

number 指定 VLAN ID。

对于 ASA 5505，请使用介于 1 和 4090 之间的 ID。默认情况下，会在 VLAN 1 上启用 VLAN 接口 ID。

对于 ASASM，请使用介于 2 到 1000(1025 到 4094) 之间的 ID。

Command Default

默认情况下，VLAN 接口处于启用状态。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。
8.4(1)	已添加ASASM支持。

使用指南

对于 ASASM，您可以将任何 VLAN ID 添加到配置中，但只有交换机分配给 ASA 的 VLAN 才能传递流量。要查看分配给 ASA 的所有 VLAN，请使用该 **showvlan**命令。如果为尚未通过交换机分配至 ASA 的 VLAN 添加接口，则该接口将处于关闭状态。将 VLAN 分配至 ASA 时，接口将更改为启动状态。有关接口状态的 **showinterface** 更多信息，请参阅命令。

在接口配置模式下，可以分配名称、IP 地址并配置许多其他设置。

对于启用已启用接口来传递流量，请配置以下接口配置模式命令： **nameif**，对于路由模式，配置 **ipaddress**。对于 ASA 5505 交换机物理接口，请使用**switchportaccessvlan** 命令将物理接口分配给 VLAN 接口。

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

有关接口的更多信息，请参阅 CLI 配置指南。

CR_Examples

以下示例配置三个 VLAN 接口。第三个家庭接口无法将流量转发到工作接口。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

以下示例配置五个 VLAN 接口，包括使用**failoverlan** 命令单独配置的故障转移接口：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
```

```
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

Related Commands

命令	说明
allocate-interface	将接口和子接口分配至安全情景。
clearinterface	清除命令的计数 **showinterface**器。
showinterface	显示接口的运行时间状态和统计信息。

interface vni

要配置 VXLAN 网络标识符 (VNI) 接口并进入接口配置模式，请在 **interfacevni** 全局配置模式下使用该命令。要删除 VNI 接口，请使用此命 **no**令的形式。

interface vni编号
no interface vni*number*

Syntax Description

number	将 ID 设置在 1 至 10000 之间。此 ID 仅为内部接口标识符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.4(1)	添加了此命令。

使用指南

您必须使用 **vtep-nve** 命令将 VNI 接口与 VTEP 源接口相关联。您还必须将 VXLAN**segment-id**。

CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并将 VNI 1 接口与其关联：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

interim-accounting-update

要为 AAA 服务器组启用 RADIUS 临时记帐更新消息的生成，请在 aaa-server group 配置模式下使用 **interim-accounting-update**命令。要禁用临时记账更新消息，请使用此命令的 **no**形式。

interim-accounting-update [**periodic** [*hours*]]
no interim-accounting-update [**periodic** [*hours*]]

Syntax Description

periodic [*hours*]	（可选）为每个配置为向相关服务器组发送会计记录的 VPN 会话启用定期生成和传输会计记录。可以选择包括发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。 将此选项用于为 ISE 身份验证更改配置的服务器组。

Command Default

默认情况下，不启用 interim-accounting-update。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.2(1)	添加了 **periodic** 关键字。

使用指南

如果使用不带 **periodic** 关键字的此命令，则 ASA 仅会在将 VPN 隧道连接添加到无客户端 VPN 会话时发送临时审计更新消息。发生此情况时，将生成记帐更新，以便将新分配的IP地址通知给RADIUS服务器。

如果要使用服务器组为远程访问 VPN 配置 ISE 授权更改，请添加 **periodic** 关键字。周期报告包括 AnyConnect 连接以及无客户端会话。

ISE 将基于其从 NAS 设备（如 ASA）收到的记帐记录，保留一个活动会话的目录。但是，如果 ISE 在 5 天内没有收到任何表明会话仍然处于活动状态（会计消息或姿态交易）的迹象，它将从其数据库中删除该会话记录。为了确保长期 VPN 连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记帐更新消息。

CR_Examples

以下示例显示如何为动态授权(CoA)更新和每小时定期记帐配置ISE服务器组。其中包括使用 ISE 配置密码身份验证的隧道组配置。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

以下示例显示如何使用ISE为本地证书验证和授权配置隧道组。在这种情况下，您将该命令包含在 **authorize-only**服务器组配置中，因为服务器组将不会用于身份验证。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

命令	说明
authorize-only	为RADIUS服务器组启用仅授权模式。
dynamic-authorization	启用RADIUS服务器组的动态授权。

internal-password

要在无客户端 SSL VPN 门户页面上显示额外的密码字段，请在 webvpn 配置模式下使用 **internal-password**命令。ASA 使用该附加密码对允许 SSO 的文件服务器的用户进行身份验证。

要禁用使用内部密码的功能，请使用此命令的 **no** 版本。

internal-passwordenable
no internal password

Syntax Description

enable	启用内部密码。

Command Default

默认设置为禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

如果启用此选项，最终用户在登录无客户端 SSL VPN 会话时将键入第二个密码。无客户端 SSL VPN 服务器使用 HTTPS 向身份验证服务器发送包含用户名和密码的 SSO 身份验证请求。如果身份验证服务器批准身份验证请求，它会向无客户端 SSL VPN 服务器返回 SSO 身份验证 cookie。ASA 会代表用户保留此 Cookie 并将其用于对用户进行身份验证，以确保受 SSO 服务器保护的域内的网站安全。

如果要求内部密码与 SSL VPN 密码不同，则内部密码功能非常有用。特别是，可以使用一次性密码对 ASA 进行身份验证，对内部站点使用其他密码。

CR_Examples

以下示例显示如何启用内部密码：

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

```
 internal password enable
ciscoasa(config-webvpn)#
```

Related Commands

命令	说明
webvpn	进入 webvpn 配置模式，在此模式下配置无客户端 SSL VPN 连接的属性。

internal-port

要为 Azure 上的 ASA Virtual 的 VNI 接口指定 VXLAN 内部端口，请在接口配置模式下使用 **internal-port** 命令。要删除端口，请使用此命 **no**令的形式。

internal-port 端口
no internal-port 端口

Syntax Description

port 将端口设置在 1024 和 65535 之间。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

命令	说明
debug vxlan	调试 VXLAN 流量。
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
external-port	设置外部 VXLAN 端口。
external-segment-id	指定 VNI 接口的 VXLAN 外部段 ID。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
internal-segment-id	指定 VNI 接口的 VXLAN 内部段 ID。
nve	指定网络虚拟化终端实例。
peer ip	手动指定对等 VTEP IP 地址。
proxy paired	将接口设置为配对代理模式。
show interface vni	显示VNI接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show nve	显示NVE接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

internal-segment-id

要为 Azure 上网关负载均衡器 (GWLB) 指定 ASA Virtual 的 VNI 接口的 VXLAN 内部网段 ID，请在接口配置模式下使用 **internal-segment-id** 命令。要删除 ID，请使用此命 **no**令的形式。

internal-segment-id *id*
no internal-segment-id *id*

Syntax Description

D 将 ID 设置在 1 至 16777215 之间。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

命令	说明
debug vxlan	调试 VXLAN 流量。

命令	说明
encapsulation vxlan	将 NVE 实例设置为 VXLAN 封装。
external-port	设置外部 VXLAN 端口。
external-segment-id	指定 VNI 接口的 VXLAN 外部段 ID。
inspect vxlan	强制遵守标准 VXLAN 报头格式。
interface vni	创建用于 VXLAN 标记的 VNI 接口。
internal-port	设置内部 VXLAN 端口。
nve	指定网络虚拟化终端实例。
peer ip	手动指定对等 VTEP IP 地址。
proxy paired	将接口设置为配对代理模式。
show interface vni	显示VNI接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
show nve	显示NVE接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlan port	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

interval maximum

如要配置 DDNS 更新方法所尝试更新的最大间隔，请在 DDNS-update-method 模式下使用 **interval**命令。要从运行配置中删除 DDNS 更新方法的间隔，请使用此命令的 **no** 形式。

天 小interval maximum时分钟 秒
天 小no interval maximum时分钟 秒

Syntax Description

天数	指定更新尝试之间的天数，范围为 0 至 364。
hours	指定更新尝试之间的间隔小时数，范围为 0 到 23。
分钟	指定更新尝试之间的分钟数，范围为 0 到 59。
seconds	指定更新尝试之间间隔的秒数，范围为 0 到 59。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

将天、小时、分钟和秒相加得到总间隔。

CR_Examples

以下示例将名为 ddns-2 的方法配置为每隔 3 分 15 秒尝试一次更新：

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

Related Commands

命令	说明
ddns	为已创建的 DDNS 方法指定 DDNS 更新方法类型。

命令	说明
ddnsupdate	将 DDNS 更新方法与 ASA 接口或 DDNS 更新主机名关联。
ddns更新方法	创建一个用于动态更新 DNS 资源记录的方法。
dhcp-clientupdatedns	配置 DHCP 客户端传递给 DHCP 服务器的更新参数。
dhcpd 更新 dns	启用 DHCP 服务器来执行 DDNS 更新。

invalid-ack

要设置具有无效 ACK 的数据包的操作，请在 tcp-map 配置模式下使用 **invalid-ack** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。此命令属于使用**setconnectionadvanced-options**命令启用的 TCP 规范化策略的一部分。

invalid-ack {**allow** | **drop**}
no invalid-ack

Syntax Description

allow	允许具有无效 ACK 的数据包。
drop	丢弃具有无效 ACK 的数据包。

Command Default

默认操作是丢弃具有无效 ACK 的数据包。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(4)/8.0(4)	添加了此命令。

使用指南

要启用 TCP 规范化，请使用模块化策略框架：

1. **tcp-map**- 标识 TCP 规范化操作。
    1. **invalid-ack**— 在 tcp-map 配置模式下，可以输入**invalid-ack** 命令和许多其他命令。
2. **class-map**- 标识要对其执行 TCP 规范化的流量。
3. **policy-map**- 确定与每个类映射关联的操作。
    1. —**class**确定您想要执行操作的类映射。
    2. **setconnectionadvanced-options**- 标识您创建的 TCP 映射。
4. **service-policy**- 向接口或全局分配策略映射。

可能会在以下实例中看到无效 ACK：

- 在 TCP 连接 SYN-ACK 已接收状态下，如果已接收的 TCP 数据包的 ACK 号与正在发送的下一个 TCP 数据包的序列号不完全相同，则是无效 ACK。
- 如果已收到 TCP 数据包的 ACK 号大于发送的下一个 TCP 数据包的序列号，则为无效 ACK。

注释 对于 WAAS 连接，系统自动允许包含无效 ACK 的 TCP 数据包。

CR_Examples

以下示例将 ASA 设置为允许具有无效 ACK 的数据包：

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

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

ip address

要为接口（在路由模式下）或网桥虚拟接口 (BVI)（路由模式或透明模式）设置 IP 地址，请在接口配置模式下使用 **ipaddress** 命令。要删除 IP 地址，请使用此命 **no**令的形式。

ip address*ip_address* [掩 码] **standby***ip_address* | **cluster-pool**池名称]
no ip address [*ip_address*]

Syntax Description

cluster-pool*poolname*	（可选）对于 ASA 集群，设置 **iplocalpool** 命令定义的集群地址池。由 *ip_address* 参数定义的主集群 IP 地址仅属于当前主设备。每个集群成员都会从此池中收到一个本地 IP 地址。 您无法提前确定分配给每个单元的确切地址；要查看每个单元使用的地址，请输入 **showiplocalpool***poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。该 ID 决定了池中使用的本地 IP。
ip_address	接口的 IP 地址。
mask	（可选）IP 地址的子网掩码。如果不设置掩码，ASA 将使用 IP 地址类的默认掩码。
standby*ip_address*	（可选）对于故障转移，设置备用设备的 IP 地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	对于路由模式，此命令已从全局配置命令更改为接口配置模式命令。
8.4(1)	对于透明模式，添加了桥接组。您现在为 BVI 设置 IP 地址，而不是全局 IP 地址。
9.0(1)	添加 **cluster-pool**关键字是为了支持 ASA 集群。
9.7(1)	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。

使用指南

此命令还设置用于故障转移的备用设备地址。

多上下文模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一的子网上。在多情景模式下，如果此接口位于共享接口上，则每个 IP 地址必须唯一，但在同一子网上。如果接口是唯一的，则此 IP 地址可以在需要时由其他情景使用。

透明防火墙指南

透明防火墙不参与 IP 路由。如果要设置 BVI 地址，则只需对 ASA 进行 IP 配置。需要此地址是因为 ASA 使用此地址作为源自 ASA 的流量（例如系统消息或与 AAA 服务器的通信）的源地址。您还可以使用此地址进行远程管理访问。此地址必须与上游和下游路由器位于同一子网上。对于多情景模式，在每个情景内设置管理 IP 地址。对于包含管理接口的型号，您还可以为此接口设置 IP 地址以进行管理。

故障转移指南

备用 IP 地址必须与主 IP 地址位于同一子网。

ASA 集群指南

只有将集群接口模式配置为单个接口（**cluster-interfacemodeindividual**命令），才能为单个接口设置集群池。唯一的例外情况是仅管理接口：

- 您始终可以将仅管理接口配置为单独的接口，即使在跨网以太网通道模式下也是如此。即使在透明防火墙模式下，管理接口也可以是单独的接口。
- 在跨网以太网通道模式下，如果将管理接口配置为单独接口，则无法为管理接口启用动态路由。您必须使用静态路由。

/31 子网准则

对于路由接口，您可以在31位子网上为点对点连接配置IP地址。31位子网只包含2个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

- 31-bit Subnet and Clustering - 可以为跨区以太网通道使用 31 位子网掩码。单个 接口（包括跨区以太网通道模式下的管理 IP 地址）不支持 31 位子网。您也不能将 31 位子网用于集群控制链路。
- 31 位子网和故障转移 - 对于故障转移，当您使用 31 位子网作为 ASA 接口 IP 地址时，您无法为该接口配置备用IP地址，因为没有足够的地址。通常，用于进行故障切换的接口应有一个备用IP地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用IP地址，ASA无法执行任何网络测试；只能跟踪链路状态。对于故障切换和可选的独立状态链路（点对点连接），也可以使用 31 位子网。
- 31 位子网和管理 - 如果您有一个直接连接的管理站，则可以使用点对点连接在 ASA 上使用 SSH 或 HTTP，或者在管理站上使用 SNMP 或 Syslog。
- 31 位子网不支持的功能 - 以下功能不支持 31 位子网：

- 桥接组的 BVI 接口 - 桥接组至少需要 3 个主机地址：BVI 和连接到两个桥接组成员接口的两个主机。您必须使用 /29 子网或更小的子网。
- 组播路由

CR_Examples

以下示例设置两个接口的 IP 地址和备用地址：

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

以下示例设置网桥组 1 的管理地址和备用地址：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ipaddressdhcp	设置接口以从 DHCP 服务器获取 IP 地址。
showipaddress	显示分配给接口的 IP 地址。

ip address dhcp

要使用 DHCP 为接口获取 IP 地址，请在接口配置模式下使用**ipaddressdhcp** 命令。要为此接口禁用 DHCP 客户端，请使用此命令的 **no** 形式。

ip address dhcp [**setroute**]
no ip address dhcp

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	此命令已从全局配置命令更改为接口配置模式命令。您还可以在任何接口上启用此命令，而不是仅在外部接口上启用。

使用指南

重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入命令之前没有使用该 **noshutdown**命令启用接 **ipaddressdhcp**口，则某些 DHCP 请求可能不会被发送。

注释 ASA 将拒绝超时时间小于 32 秒的任何租用。

CR_Examples

以下示例在 Gigabitethernet0/1 接口上启用 DHCP：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ipaddress	设置该接口的 IP 地址或设置一个透明防火墙的管理 IP 地址。
showipaddressdhcp	显示从 DHCP 服务器获取的 IP 地址。

ip address pppoe

要启用 PPPoE，请在 **ipaddressppppoe**接口配置模式下使用该命令。要禁用 PPPoE，请使用此命 **no**令的形式。

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

Syntax Description

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。如果不设置掩码，ASA 将使用 IP 地址类的默认掩码。
setroute	让 ASA 使用 PPPoE 服务器提供的默认路由。如果 PPPoE 服务器不发送默认路由，则 ASA 将创建一个以访问集中器地址作为网关的默认路由。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

PPPoE 将以太网和 PPP 两个广泛接受的标准结合在一起，可提供将 IP 地址分配至客户端系统的身份验证方法。ISP 部署 PPPoE 的原因在于，PPPoE 支持使用其现有远程访问基础设施进行高速宽带访问，同时也更加便于客户使用。

在使用 PPPoE 设置 IP 地址之前，配置 **vpdn** 命令以设置用户名、密码和身份验证协议。如果在多个接口上启用此命令（例如通往 ISP 的备份链路），则如有必要，可以使用 pppPoE client vpdn group 命令将每个接口分配到不同的 VPDN 组。

最大传输单位 (MTU) 大小会自动设置为 1492 字节，这是允许在以太网帧内进行 PPPoE 传输的正确值。

重新输入此命令以重置并重新启动 PPPoE 会话。

不能与 **ipaddress** 命令或 **ipaddressdhcp** 命令同时设置此命令。

CR_Examples

以下示例在 Gigabitethernet 0/1 接口上启用 PPPoE：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

以下示例手动设置 PPPoE 接口的 IP 地址：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

Related Commands

命令	说明
interface	配置接口并进入接口配置模式。
ip address	设置接口的 IP 地址。
pppoe 客户端 vpdn 组	将此接口分配给特定 VPDN 组。
show ip address pppoe	显示从 PPPoE 服务器获取的 IP 地址。
vpdn group	创建 vpdn 组并配置 PPPoE 客户端设置。

ip-address-privacy

要启用 IP 地址隐私，请在参数配置模式下使用 **ip-address-privacy**命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此**no** 命令的形式。

ip-address-privacy
no ip-address-privacy

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

以下示例显示如何在 SIP 检测策略映射中启用 SIP IP 地址隐私：

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

Related Commands

命令	说明
policy-maptypeinspect	创建检查策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

ip audit attack

要为匹配攻击签名的数据包设置默认操作，请在全局配置模式下使用**ipauditattack** 命令。要恢复默认操作（重置连接），请使用此命令的 **no**形式。

ip audit attack[**action**[**alarm**][**drop**][**reset**]]
no ip audit attack

Syntax Description

action	（可选）指定您正在定义一组默认操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果您未输入 **action** 关键字，ASA 会假定您已输入该关键字，并且 **action** 关键字会显示在配置中。
alarm	（默认）生成一条系统消息，显示数据包与签名匹配。
drop	（可选）丢弃数据包。
reset	（可选）丢弃数据包并关闭连接。

Command Default

默认操作是发送 并发出警报。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您可以指定多个操作，或不指定任何操作。使用 **ipauditname** 命令配置审核策略时，可以覆盖使用此命令设置的操作。如果不在 **ipauditname** 命令中指定操作，则使用使用此命令设置的操作。

有关签名列表，请参阅 **ipauditsignature** 命令。

CR_Examples

以下示例将匹配攻击签名的数据包的默认操作设置为“警报”和“重置”。内部接口的审核策略会将此默认设置覆盖为仅警报，而外部接口的策略使用通过 **ipauditattack** 命令设置的审核策略。

```
ciscoasa(config)# ip audit attack action alarm reset
```

```
ciscoasa(config)# ip audit name insidepolicy attack action alarm
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

命令	说明
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauditsignature	禁用签名。
showrunning-configipauditattack	显示命令的 **ipauditattack**配置。

ip audit info

要为匹配信息签名的数据包设置默认操作，请在全局配置模式下使用**ipauditinfo**命令。要恢复默认操作（生成警报），请使用此命令的 **no**形式。您可以指定多个操作，或不指定任何操作。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit info

Syntax Description

action	（可选）指定您正在定义一组默认操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果您未输入 **action** 关键字，ASA 会假定您已输入该关键字，并且 **action** 关键字会显示在配置中。
alarm	（默认）生成一条系统消息，显示数据包与签名匹配。
drop	（可选）丢弃数据包。
reset	（可选）丢弃数据包并关闭连接。

Command Default

默认操作是生成警报。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

使用 **ipauditname** 命令配置审核策略时，可以覆盖使用此命令设置的操作。如果不在 **ipauditname**命令中指定操作，则使用使用此命令设置的操作。

有关签名列表，请参阅 **ipauditsignature** 命令。

CR_Examples

以下示例将与信息性签名匹配的数据包的默认操作设置为警报和重置。内部接口的审核策略将将此默认设置覆盖为警报和丢弃，而外部接口的策略使用通过 **ipauditinfo**命令设置的默认设置。

```
ciscoasa(config)# ip audit info action alarm reset
```

```
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauditsignature	禁用签名。
showrunning-configipauditinfo	显示命令的 **ipauditinfo** 配置。

ip audit interface

要将审核策略分配到接口，请在全局配置模式下使用 **ipauditinterface**命令。要从接口中删除策略，请使用此命 **no**令的形式。

ip audit interface*interface_namepolicy_name*
no ip audit interface*interface_namepolicy_name*

Syntax Description

interface_name	指定接口名称。
policy_name	使用 **ipauditname** 命令添加的策略的名称。您可以向每个接口分配信息策略和攻击策略。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例将审核策略应用于内部和外部接口：

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。

命令	说明
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
ipauditsignature	禁用签名。
showrunning-configipauditinterface	显示命令的 **ipauditinterface**配置。

ip audit name

要创建命名的审核策略来标识在数据包与预定义的攻击签名或信息签名匹配时要采取的操作，请在全局配置模式下使用 **ipauditname** 命令。要删除该策略，请使用此命 **no**令的形式。

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

Syntax Description

action	（可选）指定您正在定义一组操作。如果此关键字后面不传任何操作，则 ASA 将不执行任何操作。如果不输入 **action** 关键字，则 ASA 使用 **ipauditattack** 和 **ipauditinfo**命令设置的默认操作。
alarm	（可选）生成一条系统消息，显示数据包与签名匹配。
attack	为攻击签名创建审核策略；则该数据包可能是网络攻击的一部分，例如 DoS 攻击或非法 FTP 命令。
drop	（可选）丢弃数据包。
info	为信息签名创建审核策略；该数据包当前并未攻击您的网络，但可能是信息收集活动的一部分，例如端口扫描。
name	设置策略的名称。
reset	（可选）丢弃数据包并关闭连接。

Command Default

如果不使用**ipauditattack**和**ipauditinfo** 命令更改默认操作，则针对攻击签名和信息签名的默认操作是生成警报。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

签名是与已知攻击模式匹配的活动。例如，存在与 DoS 攻击匹配的签名。要应用策略，请使用 **ipauditinterface** 命令将其分配到接口。您可以向每个接口分配信息策略和攻击策略。

有关签名列表，请参阅**ipauditsignature** 命令。

如果流量与签名匹配，并且您要针对该流量执行操作，请使用 **shun** 命令防止来自违规主机的新连接，并禁止来自任何现有连接的数据包。

CR_Examples

以下示例设置内部接口的审核策略，以针对攻击和信息签名生成警报，而外部接口的策略重置攻击连接：

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditsignature	禁用签名。
shun	阻止具有特定源和目标地址的数据包。

ip audit signature

要禁用审核策略的签名，请在全局配置模式下使用 **ipauditsignature**命令。要重新启用签名，请使用此命令的 **no** 形式。

ip audit signature*signature_number***disable**
no ip audit signature签名编号

Syntax Description

disable	禁用签名。
签名编号	指定要禁用的签名编号。有关支持的签名列表，请参阅表 3-1 。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果合法流量持续匹配签名，并且您愿意冒着禁用签名的风险来避免大量警报，则您可能需要禁用签名。表 3-1 列出了支持的签名和系统消息编号。

表 *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 选项 - 错误选项列表	信息	在收到 IP 数据报时触发，其中 IP 数据报报头中的 IP 选项列表不完整或格式错误。IP 选项列表包含一个或多个执行各种网络管理或调试任务的选项。
1001	400001	IP 选项 - 记录数据包路由	信息	在收到 IP 数据报，而该数据报的 IP 选项列表包括选项 7（记录数据包路由）时触发。

签名 ID	消息编号	签名标题	签名类型	说明
1002	400002	IP 选项 - 时间戳	信息	在收到IP数据报，而该数据报的IP选项列表包括选项4（时间戳）时触发。
1003	400003	IP 选项 - 安全	信息	在收到IP数据报，而该数据报的IP选项列表包括选项2（安全选项）时触发。
1004	400004	IP 选项 - 松散源路由	信息	在收到IP数据报，且该数据报的IP选项列表包括选项3（松散源路由）时触发。
1005	400005	IP 选项 - SATNET ID	信息	在收到 IP 数据报，其中该数据报的 IP 选项列表包括选项 8（SATNET 数据流标识符）时触发。
1006	400006	IP 选项 - 严格源路由	信息	在收到 IP 数据报，而其中该数据报的 IP 选项列表包括选项 2（严格源路由）时触发。
1100	400007	IP 分段攻击	攻击	当收到任何 IP 数据报且在偏移字段中指示偏移值小于 5 但大于 0 时触发。
1102	400008	不可能的 IP 数据包	攻击	当源地址等于目标地址的 IP 数据包到达时触发。此签名可以捕获所谓的LAND 攻击 (Land Attack)。
1103	400009	IP 重叠分片数 (Teardrop)	攻击	当同一 IP 数据报中包含的两个分段具有偏移量（表明它们在数据报中共享定位）时触发。这可能意味着分片 A 正在被分片 B 完全覆盖，或者分片 A 正在被分片 B 部分覆盖。某些操作系统无法正确处理以这种方式重叠的分片，可能会引发异常或以其他不良方式运行接收重叠分段，这就是 Teardrop 攻击创建 DoS 的方式。
2000	400010	ICMP 回应应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 0（回应应答）的 IP 数据报时触发。
2001	400011	ICMP 主机不可达	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 3（主机不可达）的 IP 数据报时触发。
2002	400012	ICMP 源抑制	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 4（源抑制）的 IP 数据报时触发。
2003	400013	ICMP 重定向	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 5（重定向）的 IP 数据报时触发。
1 月	400014	ICMP 回应请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 8（回应请求）的 IP 数据报时触发。
2005	400015	数据报的 ICMP 超时	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 11（数据报超时）的 IP 数据报时触发。

签名 ID	消息编号	签名标题	签名类型	说明
2006	400016	数据报上的 ICMP 参数问题	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 12（数据报上的参数问题）的 IP 数据报时触发。
2007	400017	ICMP 时间戳请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 13 (时间戳请求) 的 IP 数据报时触发。
2008	400018	ICMP 时间戳应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 14（时间戳应答）的 IP 数据报时触发。
2009	400019	ICMP 信息请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 15（信息请求）的 IP 数据报时触发。
2010	400020	ICMP 信息应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 16（ICMP 信息应答）的 IP 数据报时触发。
2011	400021	ICMP 地址掩码请求	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 17（地址掩码请求）的 IP 数据报时触发。
2012	400022	ICMP 地址掩码应答	信息	收到 IP 报头的协议字段设置为 1 (ICMP) 且 ICMP 报头中的类型字段设置为 18（地址掩码应答）的 IP 数据报时触发。
2150	400023	分段的 ICMP 流量	攻击	当收到 IP 报头的协议字段设置为 1 (ICMP) 的 IP 数据报并且更多分片标志设置为 1 (ICMP) 或者偏移字段中指示有偏移时触发。
2151	400024	大 ICMP 流量	攻击	收到 IP 报头的协议字段设置为 1 (ICMP) 且 IP 长度大于 1024 的 IP 数据报时触发。
2154	400025	死亡之 Ping 攻击	攻击	当收到 IP 报头的协议字段设置为 1 (ICMP)、最后分片位已设置，并且 (IP 偏移量 * 8) + (IP 数据长度) → 65535 也就是说，IP 偏移量（表示此分段在原始数据包中的起始位置，以 8 字节为单位）加上数据包其余部分就大于 IP 数据包的最大大小。
3040	400026	TCP NULL 标志	攻击	当单个未设置 SYN、FIN、ACK 或 RST 标志的 TCP 数据包已发送到特定主机时触发。
3041	400027	TCP SYN+FIN 标志	攻击	当设置了 SYN 和 FIN 标志并将其发送到特定主机的单个 TCP 数据包时触发。
3042	400028	仅 TCP FIN 标志	攻击	当单个孤立 TCP FIN 数据包发送到特定主机上的特权端口（端口号小于 1024）时触发。
3153	400029	指定了不正确的 FTP 地址	Informational	在发出地址与请求主机不同的端口命令时触发。

签名 ID	消息编号	签名标题	签名类型	说明
3154	400030	指定了不正确的 FTP 端口	Informational	在发出的 port 命令指定的数据端口为 1024 或 65535 时触发。
4050	400031	UDP 炸弹攻击	攻击	当指定的 UDP 长度小于指定的 IP 长度时触发。这种格式错误的数据包类型与拒绝服务尝试相关。
4051	400032	UDP Snork 攻击	攻击	当检测到源端口为 135、7 或 19 且目的端口为 135 的 UDP 数据包时触发。
4052	400033	UDP Chargen DoS 攻击	攻击	当检测到源端口为 7 且目的端口为 19 的 UDP 数据包时触发此签名。
6050	400034	DNS HINFO 请求	信息	在尝试从 DNS 服务器访问 HINFO 记录时触发。
6051	400035	DNS 区域传输	信息	在正常 DNS 区域传输上触发，其中源端口为 53。
6052	400036	来自高端口的 DNS 区域传输	信息	在非法 DNS 区域传输（其中源端口不等于 53）时触发。
6053	400037	所有记录的 DNS 请求	信息	触发所有记录的 DNS 请求。
6100	400038	RPC 端口注册	信息	当尝试在目标主机上注册新的 RPC 服务时触发。
6101	400039	RPC 端口取消注册	信息	当尝试在目标主机上注销现有的 RPC 服务时触发。
6102	400040	RPC 转储	信息	当向目标主机发出 RPC 转储请求时触发。
6103	400041	通过代理发送的 RPC 请求	攻击	当向目标主机的端口映射器发送代理的 RPC 请求时触发。
6150	400042	ypserv（YP 服务器后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 服务器后台守护程序 (ypserv) 端口的请求时触发。
6151	400043	ypserv（YP 绑定后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 绑定后台守护程序 (ypbind) 端口的请求时触发。
6152	400044	yppasswdd（YP 密码后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 密码后台守护程序 (yppasswdd) 端口的请求时触发。
6153	400045	ypupdated（YP 更新后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 更新后台守护程序 (ypupdated) 端口的请求时触发。
6154	400046	ypxfrd（YP 传输后台守护程序）端口映射请求	信息	当向端口映射程序发出 YP 传输后台守护程序 (ypxfrd) 端口的请求时触发。
6155	400047	mountd（装载后台守护程序）端口映射请求	信息	当向端口映射程序发出安装后台守护程序 (mountd) 端口的请求时触发。
6175	400048	rexd（远程执行后台守护程序）端口映射请求	信息	当向端口映射程序请求远程执行后台守护程序 (rexd) 端口时触发。

签名 ID	消息编号	签名标题	签名类型	说明
6180	400049	rexd（远程执行后台守护程序）尝试	信息	当调用 rexd 程序时触发。远程执行后台守护程序是负责远程执行程序的服务器。这可能表示有人试图未经授权访问系统资源。
6190	400050	statd 缓冲区溢出	攻击	发送大型 statd 请求时触发。这可能是试图使缓冲区溢出并获得对系统资源的访问权限。

CR_Examples

以下示例禁用签名 6100：

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

Related Commands

命令	说明
ipauditattack	为与攻击签名匹配的数据包设置默认操作。
ipauditinfo	为与信息签名匹配的数据包设置默认操作。
ipauditinterface	将审核策略分配到接口。
ipauditname	创建命名审核策略，该策略标识在数据包与攻击签名或信息签名匹配时要采取的操作。
showrunning-configipauditsignature	显示命令的 **ipauditsignature** 配置。

ip-client

要允许 FXOS 发起管理流量并将其发送出 Firepower 2100 ASA 数据接口，请在全局配置模式下使用 **ip-client**命令。要禁用流量启动，请使用此命 **no**令的形式。

ip-client*interface_name*
no ip-client*interface_name*

Syntax Description

interface_name	指定 FXOS 可以通过其发送管理流量的接口名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.8(2)	我们添加了此命令。

使用指南

您可以在 ASA 数据接口上启用 FXOS 管理流量启动，例如，这对于 SNMP 陷阱或 NTP 和 DNS 服务器访问是必需的。有关传入管理流量，请参阅 **fxospermit**命令。

在 FXOS 配置中，请确保默认网关设置为 0.0.0.0，即将 ASA 设置为网关。请参阅 FXOS **setout-of-band** 命令。

CR_Examples

以下命令允许通过外部接口发起 FXOS 流量：

```
ciscoasa(config)# ip-client outside
```

Related Commands

命令	说明
connectfxos	从 ASA CLI 连接到 FXOS CLI。
fxospermit	允许在 ASA 数据接口上进行 FXOS 管理访问。
fxosport	设置 FXOS 管理访问端口。

ip-comp

要启用 LZS IP 压缩，请在 **ip-compenable**策略组配置模式下使用该命令。要禁用 IP 压缩，请使用该命 **ip-compdisable**令。**ip-comp**要从运行配置中删除属性，请使用此命令的 **no**形式。

ip-comp {**enable** | **disable**}
no ip-comp

Syntax Description

disable	禁用 IP 压缩。
enable	启用 IP 压缩。

Command Default

禁用 IP 压缩。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命 **no**令的形式允许从另一个组策略继承值。启用数据压缩可能会加快使用调制解调器连接的远程拨入用户的数据传输速率。

⚠

注意 数据压缩会增加每个用户会话的内存要求和 CPU 利用率，从而降低 ASA 的整体吞吐量。为此，建议仅对使用调制解调器连接的远程用户启用数据压缩。设计特定于调制解调器用户的组策略并仅对其启用压缩。

如果终端生成 IP 压缩流量，您应禁用 IP 压缩，以防止数据包解压缩不当。如果在特定 LAN 上启用了 LAN 间隧道，则主机 A 尝试将 IP 压缩数据从隧道的一端传递到另一端时，将无法与主机 B 进行通信。

注释 启用 **ip-comp** 命令并为“before-encryption”配置 IPsec 分片时，无法使用 IPsec 压缩（ip-comp_option 和 pre-encryption）。发送到加密芯片的 IP 报头会被模糊处理（由于压缩），导致加密芯片在处理提供的出站数据包时生成错误。您还可以检查您的 MTU 级别，以确保它是一个较小的值（例如 600 字节）。

CR_Examples

以下示例显示如何为名为“FirstGroup”的组策略启用 IP 压缩：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```

ip local pool

要配置 IP 地址池，请在**iplocalpool**全局配置模式下使用该命令。EXTE 要删除地址池，请使用此命**no**令的形式。

池名称ip local pool第一个地址最后一个地址 [**mask**掩 码]
no ip local pool*poolname*

Syntax Description

第一个地址	指定 IP 地址范围的起始地址。
最后一个地址	指定 IP 地址范围中的最后一个地址。
mask*mask*	（可选）指定地址池的子网掩码。不能使用 255.255.255.254 (/31) 或 255.255.255.255 (/32) 子网掩码。
poolname	指定IP地址池的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
9.0(1)	已在**ipaddress**命令中添加集群池的 IP 本地池，以支持 ASA 集群。

使用指南

当分配给 VPN 客户端的 IP 地址属于非标准网络时，您必须提供掩码值，如果使用默认掩码，数据可能会被错误路由。这种情况的一个典型例子是本地 IP 地址池包含 10.10.10.0/255.255.255.0 地址，因为默认情况下这是 A 类网络。当 VPN 客户端需要通过不同的接口访问 10 个网络内的不同子网时，这可能会导致一些路由问题。例如，如果可以通过接口 2 使用地址 10.10.100.1/255.255.255.0 的打印机，但 10.10.10.0 网络通过 VPN 隧道可用，因此使用接口 1，VPN 客户端可能会混淆该将数据路由到何处打印机的数据包。10.10.10.0 和 10.10.100.0 子网都属于 10.0.0.0 A 类网络，因此打印机数据可能通过 VPN 隧道发送。

CR_Examples

以下示例配置名为 firstpool 的 IP 地址池。起始地址为 10.20.30.40，结束地址为 10.20.30.50。网络掩码为 255.255.255.0。

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

命令	说明
clearconfigureiplocalpool	删除所有 IP 本地池。
showrunning-configiplocalpool	显示 IP 池配置。要指定特定 IP 地址池，请在 命令中包含名称。

ip unnumbered

要从接口（例如，环回接口）借用或继承 IP 地址，请在接口配置模式下使用 **ipunnumbered** 命令。要停止从接口继承 IP 地址，请使用此命令的 **no**形式。

ipunnumbered*interface-name*
no ip unnumbered

Syntax Description

interface-name	指定要继承 IP 地址的接口的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南

ip unnumbered 命令用于将所选接口的 IP 地址继承为当前接口的地址。

CR_Examples

以下示例从环回接口借用 IP 地址：

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ip unnumbered loopback1
```

Related Commands

命令	说明
ipv6unnumbered*interface-name*	继承指定接口的 IPv6 地址。
interfaceloopback环回编号	创建环回接口。

ip-phone-bypass

要启用 IP 电话绕行，请在 group-policy 配置模式下使用 **ip-phone-bypassenable**命令。要从运行配置中删除 IP 电话绕行属性，请使用此命令的 **no** 形式。

ip-phone-bypass { **enable** | **disable** }
no ip-phone-bypass

Syntax Description

disable	禁用 IP 电话绕行。
enable	启用 IP 电话绕行。

Command Default

IP 电话旁路已禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

要禁用 IP 电话绕行，请使用 **ip-phone-bypassdisable**命令。此命令选项的 **no**形式允许从另一个组策略继承“IP 电话旁路”的值。

通过 IP 电话绕行，硬件客户端背后的 IP 电话可以在不执行用户身份验证过程的情况下进行连接。如果启用，安全设备身份验证仍然生效。

仅当启用用户身份验证时，才需要配置 IP 电话绕行。

您还需要配置 **mac-exempt**选项以避免客户端进行身份验证。请参阅命 **vpnclientmac-exempt**令以了解更多信息。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用 IP 电话旁路：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

Related Commands

命令	说明
user-authentication	要求硬件客户端后面的用户在连接之前向ASA证明自己的身份。

ips

要将流量从 ASA 转移到 AIP SSM 进行检查，请在类配置模式下使用 **ips**命令。要删除此命令，请使用此命 **no**令的形式。

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]
no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

Syntax Description

fail-close	如果 AIP SSM 失败，则阻止流量。
fail-open	如果 AIP SSM 失败，则允许流量。
inline	将数据包定向到 AIP SSM；数据包可能由于 IPS 操作而被丢弃。
promiscuous	为 AIP SSM 复制数据包； AIP SSM 无法丢弃原始数据包。
sensor {*sensor_name* | *mapped_name* }	设置此流量的虚拟传感器名称。如果您在 AIP SSM（使用 6.0 或更高版本）上使用虚拟传感器，则可以使用此参数指定传感器名称。要查看可用的传感器名称，请输入 **ips...sensor?** 命令。系统将列出可用的传感器。您也可以使用该 **showips**命令。 如果在ASA上使用多情景模式，则只能指定已分配到该情景的传感器（请参阅**allocate-ips**命令）。使用 *mapped_name* 参数（如果已在情景中配置）。 如果未指定传感器名称，则流量使用默认传感器。在多情景模式下，您可以为情景指定默认传感器。在单模式下，或者如果未在多模式下指定默认传感器，则流量将使用在 AIP SSM 上设置的默认传感器。 如果输入 AIP SSM 中尚不存在的名称，则会出现错误，命令也会被拒绝。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

ASA 5500 系列支持 AIP SSM，该 SSM 运行高级 IPS 软件，可提供主动、功能齐全的入侵防御服务，以在恶意流量（包括蠕虫和网络病毒）影响您的网络之前将其阻止。在 ASA 上配置 **ips** 命令之前或之后，请在 AIP SSM 上配置安全策略。您可以从 ASA 连接到 AIP SSM（在 **session** 命令），也可以在其管理接口上使用 SSH 或 Telnet 直接连接到 AIP SSM。或者，您可以使用 ASDM。有关配置 AIP SSM 的详细信息，请参阅使用命令行界面配置 Cisco 入侵防御系统传感器。

要配置 **ips** 命令，您必须首先配置 **class-map**命令、 **policy-map** 命令和 **class** 命令。

AIP SSM 运行与 ASA 不同的应用程序。但是，会将其集成到 ASA 流量中。除管理接口外，AIP SSM 本身不包含任何外部接口。当您在 ASA 上对流量类应用 **ips** 命令时，流量将按以下方式流经 ASA 和 AIP SSM：

1. 流量进入 ASA。
2. 应用防火墙策略。
3. 通过背板将流量发送到 AIP SSM（使用 **inline** 关键字；有关仅将流量副本发送到 AIP SSM 的信息，请参阅 **promiscuous** 关键字）。
4. AIP SSM 将其安全策略应用于流量，并采取适当的措施。
5. 有效流量通过背板发送回 ASA；AIP SSM 可能会根据其安全策略阻止某些流量，并且不会传递这些流量。
6. 系统将应用 VPN 策略（如果已配置）。
7. 流量退出 ASA。

CR_Examples

以下示例将所有 IP 流量转移到混杂模式下的 AIP SSM，并在 AIP SSM 卡因任何原因而失败时阻止所有 IP 流量：

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

以下示例将以内联模式将发往 10.1.1.0 网络和 10.2.1.0 网络的所有 IP 流量转移到 AIP SSM，并且如果 AIP SSM 卡因任何原因出现故障，则允许所有流量通过。对于 my-ips-class 流量，使用 sensor1； my-ips-class2 流量使用 sensor2。

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

Related Commands

命令	说明
allocate-ips	将虚拟传感器分配给安全情景。
class	指定要用于流量分类的类映射。
class-map	识别要在策略映射中使用的流量。
policy-map	配置策略；即流量类与一个或多个操作的关联。
showrunning-configpolicy-map	显示所有当前策略图配置。

ipsec-udp

要启用 UDP 上的 IPsec，请在 **ipsec-udpenable** 策略组配置模式下使用该命令。要从当前组策略中删除 IPsec over UDP 属性，请使用此命令的 **no**形式。

ipsec-udp {**enable** | **disable**}
no ipsec-udp

Syntax Description

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

Command Default

UDP 上的 IPsec 已禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令的 **no**形式允许从另一个组策略继承 IPsec over UDP 的值。

IPsec over UDP（有时称为 IPsec through NAT）允许 Cisco VPN 客户端或硬件客户端通过 UDP 连接到运行 NAT 的 ASA。

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

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

Cisco VPN 客户端还必须配置为使用 IPsec over UDP（默认情况下配置为使用它）。VPN 3002 无需配置即可使用 IPsec over UDP。

IPsec over UDP 是专有的，仅适用于远程访问连接，并且需要模式配置，这意味着 ASA 在协商 SA 时与客户端交换配置参数。

使用 IPsec over UDP 可能会略微降低系统性能。

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

CR_Examples

以下示例显示如何为名为FirstGroup 的策略组配置 IPsec over UDP：

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

Related Commands

命令	说明
ipsec-udp-port	指定 ASA 侦听 UDP 流量的端口。

ipsec-udp-port

要为 IPsec over UDP 设置 UDP 端口号，请在 group-policy 配置模式下使用 **ipsec-udp-port**命令。要禁用 UDP 端口，请使用此命 **no**令的形式。

ipsec-udp-port*port*
noipsec-udp-port

Syntax Description

port	使用 4001 至 49151 范围内的整数标识 UDP 端口号。

Command Default

默认端口为 10000。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

在 IPsec 协商中，ASA 会侦听配置的端口并转发该端口的 UDP 流量，即使其他过滤规则丢弃 UDP 流量。

可以配置多个组策略来启用此功能，并且每个组策略可以使用不同的端口号。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略将 IPsec UDP 端口设置为端口 4025：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

命令	说明
ipsec-udp	允许 Cisco VPN 客户端或硬件客户端通过 UDP 连接到运行 NAT 的 ASA。

当地语言翻译版本说明

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