ia – inr

icmp

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

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

Syntax Description

deny	如果条件匹配则拒绝访问。
icmp_type	（可选）ICMP 消息类型（请参阅 表 1-1）。
if_name	接口名称。
ip_address	向接口发送 ICMP 消息的主机的 IP 地址。
net_mask	要应用于主机 IP 地址的网络掩码。
permit	如果条件匹配则允许访问。

Command Default

ASA 的默认行为是允许所有 ICMP 流量到达 ASA 接口。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

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

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

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

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

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

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

下表列出了支持的 ICMP 类型值。

表 *1: ICMP* 类型和文字

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

CR_Examples

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

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

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

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

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

Related Commands

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

icmp-object

要将ICMP类型添加至ICMP对象组，请在icmp-type配置模式下使用icmp-object命令。要删除ICMP类型，请使用此命 **no**令的形式。

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

Syntax Description

icmp_type	指定ICMP类型名称或编号(0-255)。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

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

ICMP 类型号和名称包括：

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

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

CR_Examples

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

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

Related Commands

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

icmp unreachable

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

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

Syntax Description

rate-limit*rate*	设置不可达消息的速率限制，介于每秒 1 到 100 条消息之间。默认值为每秒 1 条消息。
burst-size*size*	设置突发率，介于 1 和 10 之间。发送的回复数量为突发大小，但在达到速率限制之前不会发送后续回复。

Command Default

默认的速率限制为每秒 1 条消息。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(2)	添加了此命令。

使用指南

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

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

CR_Examples

以下示例启用生存时间递减并设置 ICMP 不可达速率限制：

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

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

Related Commands

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

id-cert-issuer

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

id-cert-issuer
no id-cert-issuer

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认设置为启用（接受身份证书）。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

CR_Examples

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

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

Related Commands

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

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

id-mismatch

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

id-mismatch [**count***number***duration***seconds*] **actionlog**
id-mismatch [**count***number***duration***seconds*] **actionlog**]

Syntax Description

countnumber	发送系统消息日志之前不匹配实例的最大数量。
durationseconds	要监控的时间段（以秒为单位）。

Command Default

此命令默认禁用。如果启用该命令时未指定选项，则默认速率为 3 秒内 30。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

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

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 ID 不匹配：

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

Related Commands

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

命令	说明
policy-map	创建第 3/4 层策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

id-randomization

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

id-randomization
no id-randomization

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下已禁用。不会修改来自 DNS 查询的 DNS 标识符。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

ID 随机化有助于防御缓存毒化攻击。

CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 ID 随机化：

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

Related Commands

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

id-usage

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

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

Syntax Description

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

Command Default

该 **id-usage**命令默认为 。 **ssl-ipsec**

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

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

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

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

CR_Examples

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

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

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

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

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

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

Related Commands

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

igmp

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

igmp
no igmp

Syntax Description

此命令没有任何参数或关键字。

Command Default

已启用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令仅 **no** 形式出现在运行配置中。

CR_Examples

以下示例在所选接口上禁用 IGMP 处理：

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

Related Commands

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

igmp access-group

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

igmp access-group*acl*
no igmp access-group*acl*

Syntax Description

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

Command Default

所有组都可以通过某个接口加入。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

CR_Examples

以下示例限制了访问列表 1 允许的主机加入组的行为：

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

Related Commands

命令	说明
showigmpinterface	显示接口的组播信息。

igmp forward interface

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

igmp forward interface*if-name*
no igmp forward interface*if-name*

Syntax Description

if-name	接口的逻辑名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

在输入接口上输入此命令。此命令用于末节组播路由，不能与 PIM 同时配置。

CR_Examples

以下示例将 IGMP 主机报告从当前接口转发到指定接口：

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

Related Commands

命令	说明
showigmpinterface	显示接口的组播信息。

igmp join-group

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

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

Syntax Description

group-address	多播组的IP地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

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

CR_Examples

以下示例将所选接口配置为加入 IGMP 组 255.2.2.2：

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

Related Commands

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

igmp limit

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

igmp limit编号
no igmp limit[编号]

Syntax Description

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

Command Default

默认值为 500。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

此命令用于配置 IGMP 状态的限制。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发。

当您更改接口上具有活动加入的 IGMP 限制时，新限制不适用于现有组。仅当将新组添加到接口或 IGMP 加入计时器到期时，ASA 才会验证限制。要应用新的限制并立即生效，必须在接口上禁用并重新启用 IGMP。

CR_Examples

以下示例将接口上的 IGMP 状态数量限制为 250：

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

Related Commands

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

igmp query-interval

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

igmp query-interval秒
no igmp query-interval秒

Syntax Description

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

Command Default

默认查询间隔为125秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

LAN 的指定路由器是发送 IGMP 主机查询消息的唯一路由器：

- 对于 IGMP 版本 1，系统将根据 LAN 上运行的组播路由协议选择指定路由器。
- 对于 IGMP 版本 2，指定路由器是子网上 IP 地址最低的组播路由器。

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

⚠

注意 更改此值可能会严重影响组播转发。

CR_Examples

以下示例将 IGMP 查询间隔更改为 120 秒：

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

Related Commands

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

igmp query-max-response-time

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

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

Syntax Description

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

Command Default

10秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

此命令仅在 IGMP 版本 2 或 3 运行时有效。

此命令用于控制路由器删除组之前，响应方可以响应 IGMP 查询消息的时间段。

CR_Examples

以下示例将最大查询响应时间更改为 8 秒：

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

Related Commands

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

igmp query-timeout

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

igmpquery-timeout*seconds*
no igmpquery-timeout秒

Syntax Description

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

Command Default

默认查询间隔为255秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令需要 IGMP 版本 2 或 3。

CR_Examples

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

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

Related Commands

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

igmp static-group

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

igmp static-group*group*
no igmp static-group*group*

Syntax Description

group	IP 多播组地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

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

CR_Examples

以下示例将所选接口添加到组播组 239.100.100.101：

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

Related Commands

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

igmp 版本

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

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

Syntax Description

1	IGMP 版本 1。
2	IGMP 版本 2。

Command Default

IGMP 版本 2。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

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

CR_Examples

以下示例将所选接口配置为使用 IGMP 版本 1：

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

Related Commands

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

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

ignore-ipsec-keyusage (已弃用)

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

ignore-ipsec-keyusage
no ignore-ipsec-keyusage

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

CR_Examples

以下示例显示如何忽略密钥使用检查的结果：

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

Related Commands

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

ignore lsa mospf

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

ignore lsa mospf
no ignore lsa mospf

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

不支持类型 6 MOSPF 数据包。

CR_Examples

以下示例导致 LSA 类型 6 MOSPF 数据包被忽略：

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

Related Commands

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

ignore-lsp-errors

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

ignore-lsp-errors
no ignore-lsp-errors

Syntax Description

此命令没有任何参数或关键字。

Command Default

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

稳定性

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

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

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

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

CR_Examples

以下示例指示路由器忽略具有内部校验和的链路状态数据包

错误：

ciscoasa(config)# **routerisis**

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

Related Commands

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

命令	说明
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routepriorityhigh	为 IS-IS IP 前缀分配高优先级。

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

ignore-ssl-keyusage (已弃用)

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

ignore-ssl-keyusage
no ignore-ssl-keyusage

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

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

CR_Examples

以下示例显示如何忽略密钥使用检查的结果：

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

Related Commands

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

ike-retry-count

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

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

Syntax Description

none 指定不允许重试。

value 指定思科 AnyConnect VPN 客户端在初始连接失败后要执行的最大连接重试次数（1-10 次）。

Command Default

允许重试的默认次数为 3 次。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令

使用指南

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

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

CR_Examples

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

```
ciscoasa
```

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

以下示例将用户名财务的 IKE 重试计数设置为 9：

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

Related Commands

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

ikev1 pre-shared-key

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

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

Syntax Description

key	指定介于 1 到 128 个字符之间的字母数字密钥。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

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

使用指南

您可以将此属性应用于所有 IPsec tunnel-group 类型。

CR_Examples

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

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

Related Commands

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

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

ikev1 trust-point

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

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

Syntax Description

trust-point-name	指定要使用的信任点的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
隧道组 ipsec 属性	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.4(1)	命令名称已从 trust-point 更改为 ikev1 trust-point。

使用指南

您可以将此属性应用于所有 IPsec 隧道组类型。

CR_Examples

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

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

Related Commands

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

ikev1 user-authentication

要在 IKE 期间配置混合身份验证，请在 tunnel-group ipsec-attributes 配置模式下使用 **ikev1user-authentication** 命令。要禁用混合身份验证，请使用此命 **no**令的形式。

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

Syntax Description

hybrid	指定 IKE 期间使用混合 XAUTH 身份验证。
interface	（可选）指定在其上配置用户身份验证方法的接口。
none	在 IKE 期间禁用用户身份验证。
xauth	指定 XAUTH，也称为扩展用户身份验证。

Command Default

默认身份验证方法是 XAUTH 或扩展用户身份验证。默认值为所有接口。

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

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。
8.4(1)	命令名称从 isakmp **ikev1-user-authentication**更改为 **ikev1user-authentication.**

使用指南

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

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

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

交换类型为主模式时，IPsec 混合 RSA 身份验证类型会被拒绝。

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

CR_Examples

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

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

Related Commands

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

ikev2 local-authentication

要为 IKEv2 LAN 间连接指定本地身份验证，请在 tunnel-group ipsec-attributes 配置模式下使用 **ikev2local-authentication**命令。要返回默认值，请使用此**no**命令形式。

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

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.4(1)	添加了此命令。
9.3(2)	添加了使用 EAP 的远程身份验证。
9.4(1)	添加了 hex 和 hex string 关键字。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

您只能为本地身份验证配置一个身份验证选项。

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

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

CR_Examples

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

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

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

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key XYZX
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Related Commands

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

ikev2 mobike-rrc

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

ikev2 mobike-rrc
no ikev2 mobike-rrc

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

摩拜单车“永远在线”。此命令用于为 Mobike 连接启用 RRC。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.8(1)	添加了此命令。

使用指南

此命令仅适用于 IPsec IKEv2 RA VPN 隧道组。

CR_Examples

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

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

Related Commands

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

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

ikev2 remote-authentication

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

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

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.4(1)	添加了此命令。
9.3(2)	添加了 **eap** 和 **query-identity** 关键字。
9.4(1)	添加了 hex 和 hex-string 关键字。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

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

您可以为远程身份验证配置多个身份验证选项。

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

CR_Examples

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

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

以下命令显示 EAP 身份验证请求被拒绝：

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

Related Commands

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

ikev2 rsa-sig-hash

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

ikev2rsa-sig-hashsha1
no ikev2rsa-sig-hashsha1

Syntax Description

sha1	使用 SHA-1 散列函数对 IKEv2 身份验证负载签名。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.12(1)	添加了此命令。

使用指南

该命令仅适用于 IPsec IKEv2 LAN 间隧道组。

CR_Examples

以下命令使用 SHA-1 函数对 IKEv2 身份验证负载签名：

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

Related Commands

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

im

要启用 SIP 即时消息，请在参数配置模式下使用 **im**命令（此模式可从策略映射配置模式访问）。要禁用此功能，请使用此**no** 命令的形式。

im
noim

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.2(1)	添加了此命令。

CR_Examples

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

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

Related Commands

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

imap4s (已弃用)

注释 此命令的最后支持版本是 9.5(1)。

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

imap4s
no imap4s

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
9.5(2)	此命令已弃用。

使用指南

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

CR_Examples

以下示例显示如何进入 IMAP4S 配置模式：

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

Related Commands

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

imi-traffic-descriptor

要定义在具有 IP 选项检查的数据包头中出现 IMI 流量描述符 (IMITD) 选项时的操作，请在 **imi-traffic-descriptor** 参数配置模式下使用该命令。要禁用此功能，请使用此**no** 命令的形式。

imi-traffic-descriptoraction { **allow** | **clear** }
no imi-traffic-descriptoraction { **allow** | **clear** }

Syntax Description

allow	允许包含 IMI 流量描述符 IP 选项的数据包。
clear	从数据包头中删除 IMI 流量描述符选项，然后允许数据包。

Command Default

默认情况下，IP 选项检查会丢弃包含 IMI 流量描述符 IP 选项的数据包。

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

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.5(1)	添加了此命令。

使用指南

此命令可配置的 IP 选项检查策略映射中。

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

CR_Examples

以下示例展示如何在策略映射中设置 IP 选项检查的操作：

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# imi-traffic-descriptor action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。

命令	说明
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

import

要在前缀委派客户端接口上将ASA从DHCPv6服务器获取的一个或多个参数提供给无状态地址自动配置 (SLAAC) 客户端，请在 ipv6 dhcp 池配置模式下使用 **import**命令。要删除参数，请使用此命 **no** 令的形式。

import{ [**dns-server**] [**domain-name**] [**nisaddress**] [**nisdomain-name**] [**nispaddress**] [**nispdomain-name**] [**sipaddress**] [**sipdomain-name**] [**sntpaddress**] }
no
import{ [**dns-server**] [**domain-name**] [**nisaddress**] [**nisdomain-name**] [**nispaddress**] [**nispdomain-name**] [**sipaddress**] [**sipdomain-name**] [**sntpaddress**] }

Syntax Description

dns-server	导入域名服务器 (DNS) 服务器的 IP 地址。
domain-name	导入域名。
nisaddress	导入网络信息服务 (NIS) 服务器 IP 地址。
nisdomain-name	导入 NIS 域名。
nispaddress	导入 Network Information Service Plus (NIS+) 服务器 IP 地址。
nispdomain-name	导入 NIS+ 域名。
sipaddress	导入 会话初始协议 (SIP) 服务器 IP 地址。
sipdomain-name	导入 SIP 域名。
sntpaddress	导入简单网络时间协议 (SNTP) 服务器 IP 地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

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

入的参数；但是手动配置的参数与使用 **import** 命令配置的参数不能相同。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

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

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

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。

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

import webvpn AnyConnect-customization

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

importwebvpnAnyConnect-customization type {**binary** | **resource** | **transform**} **platform** {**linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile**} **name** *name* {*URL* | **stdin** {*num_chars data* | 数据 **quit**}}

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

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

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

Related Commands

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

import webvpn customization

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

import webvpn customization名称*URL*

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

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

导入自定义对象时，ASA 会执行以下操作：

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

CR_Examples

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

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

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

Related Commands

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

import webvpn mst-translation

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

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

Syntax Description

language*language*	翻译语言。
stdin {*num_charsdata*|*data***quit**}	指定将从标准输入提供数据。如果未指定字符数，则从标准输入读取的数据应进行 base64 编码，后跟“\nquit\n”。
URL	XML 自定义对象源的远程路径。最大数量为 255 个字符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

此文件可以转换 AnyConnect 安装程序。

Related Commands

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

import webvpn plug-in protocol

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

import webvpn plug-in protocol*protocolURL*

Syntax Description

protocol

- **rdp**—远程用户可通过远程桌面协议插件连接到运行 Microsoft 终端服务的计算机。思科重新分发此插件，无需任何更改。包含原始文件的网站为 http://properjavardp.sourceforge.net/ 。
- **ssh,telnet**—安全外壳插件使远程用户能够建立与远程计算机的安全通道，或者使远程用户能够使用 Telnet 连接到远程计算机。思科重新分发此插件，无需任何更改。包含原始文件的网站为 http://javassh.org/ 。

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

- **vnc**—虚拟网络计算插件允许远程用户使用显示器、键盘和鼠标来查看和控制打开了远程桌面共享的计算机。思科重新分发此插件，无需任何更改。包含原始文件的网站为 http://www.tightvnc.com/ 。

URL　插件源的远程路径。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

在安装插件之前，请执行以下操作：

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

在导入插件时，ASA 执行以下操作：

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

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

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

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

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

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

CR_Examples

以下命令为 RDP 添加无客户端 SSL VPN 支持：

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

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

以下命令为 SSH 和 Telnet 添加无客户端 SSL VPN 支持：

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

以下命令为 VNC 添加无客户端 SSL VPN 支持：

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

Related Commands

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

import webvpn translation-table

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

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

Syntax Description

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

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

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

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

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

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

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

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

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

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

CR_Examples

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

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

Related Commands

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

import webvpn url-list

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

import webvpn url-list名称*URL*

Syntax Description

name	标识 URL 列表的名称。最大数量为 64 个字符。
URL	URL 列表源的远程路径。最大数量为 255 个字符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权执行模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

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

导入 URL 列表时，ASA 会执行以下操作：

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

CR_Examples

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

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

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

Related Commands

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

import webvpn webcontent

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

目标**import webvpn webcontent**网址源网址

Syntax Description

destinationurl	**TheURLtoexportto**. 最大数量为 255 个字符。
sourceurl	内容所在的 ASA 闪存中的 URL。最大数量为 64 个字符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

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

导入到 URL 路径为 /+CSCOE+/ 的内容仅对授权用户可见。

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

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

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

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

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

下表显示了向可选插件无客户端应用显示的帮助内容的 URL 和屏幕区域：

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

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

CR_Examples

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

```
ciscoasa# import webvpn webcontent /+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* 从位于 209.165.200.225 的 tftp 服务器导入到将应用访问帮助内容存储在闪存中的 URL。URL 包含英语语言的缩写 *en* ：

```
ciscoasa# import webvpn webcontent /+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#
```

Related Commands

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

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。