is – iz

isakmp am-disable（已弃用）

要禁用入站积极模式连接，请在全局配置模式下使用**isakmpam-disable** 命令。要启用入站积极模式连接，请使用此命令的 **no** 形式。

isakmp am-disable
no isakmp am-disable

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值为启用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmpam-disable** 命令取而代之。

CR_Examples

以下示例在全局配置模式下禁用入站积极模式连接：

```
ciscoasa(config)# isakmp am-disable
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp disconnect-notify (已弃用)

要启用向对等体发送断开连接通知，请在全局配置模式下使用**isakmpdisconnect-notify** 命令。要禁用断开连接通知，请使用此命 **no**令的形式。

isakmp disconnect-notify
no isakmp disconnect-notify

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认值为禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmpdisconnect-notify** 命令取而代之。

CR_Examples

以下示例在全局配置模式下输入，启用向对等体发送断开连接通知：

```
ciscoasa(config)# isakmp disconnect-notify
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp enable（已弃用）

要在IPsec对等体与ASA通信的接口上启用ISAKMP协商，请在全局配置模式下使用该**isakmpenable**命令。要在接口上禁用 ISAKMP，请使用此**no**命令的形式。

isakmp enable*interface-name*
no isakmp enable*interface-name*

Syntax Description

interface-name	指定启用或禁用ISAKMP协商的接口名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该**cryptoisakmpenable**命令取而代之。

CR_Examples

以下示例在全局配置模式下输入了如何在内部接口上禁用 ISAKMP：

```
ciscoasa(config)# no isakmp enableinside
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除IKE运行时间SA数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp identity (已弃用)

如要设置发送至对等体的第 2 阶段 ID，请在全局配置模式下使用**isakmpidentity** 命令。要恢复默认设置，请使用此命 **no**令的形式。

isakmp identity { **address** | **hostname** | **key-id***key-id-string* | **auto** }
no isakmp identity { **address** | **hostname** | **key-id***key-id-string* | **auto** }

Syntax Description

address	使用交换 ISAKMP 身份信息的主机的 IP 地址。
auto	通过连接类型确定 ISKMP 协商；预共享密钥的 IP 地址或证书认证的证书 DN。
hostname	使用交换 ISAKMP 身份信息的主机的完全限定域名（默认）。此名称包含主机名和域名。
key-id*key_id_string*	指定远程对等体用于查找预共享密钥的字符串。

Command Default

默认 ISAKMP 身份是 **isakmpidentityhostname** 命令。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmpidentity** 命令取而代之。

CR_Examples

以下示例进入全局配置模式，根据连接类型在接口上启用 ISAKMP 协商，以便与 IPSec 对等体进行通信：

```
ciscoasa(config)# isakmp identity auto
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。

命令	说明
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp ipsec-over-tcp (已弃用)

要启用 IPsec over TCP，请在全局配置模式下使用**isakmpipsec-over-tcp** 命令。要禁用 TCP 上的 IPsec，请使用此命 **no**令的形式。

isakmp ipsec-over-tcp [**port***port1...port10*]
no isakmp ipsec-over-tcp [**port***port1...port10*]

Syntax Description

port*port1...port10*	（可选）指定设备在其上接受 IPsec over TCP 连接的端口。您最多可以列出 10 个端口。端口号可以在 1-65535 范围内。默认端口号为 10000。

Command Default

默认值为禁用。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。 **cryptoisakmpipsec-over-tcp** 命令将取代它。

CR_Examples

此示例以全局配置模式输入，在端口 45 上启用 TCP 上的 IPsec：

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp keepalive

要配置 IKE 保持连接，请在 **isakmpkeepalive** 隧道组 ipsec-attributes 配置模式下使用该命令。要使用默认阈值和重试值将保持连接参数恢复为已启用，请使用此命令的 **no** 形式。

isakmp keepalive [**threshold***seconds* | 无限] [**retry**秒] [**disable**]
no isakmp keepalive [**threshold***seconds* | 无限] [**retry**秒] [**disable**]

Syntax Description

disable	禁用 IKE 保持连接处理（默认情况下处于启用状态）。
无限	ASA 从不启动保持连接监控。
retry秒	指定未收到保持连接响应后重试的间隔（秒）。范围是2-10秒。默认值为 2 秒。
threshold 秒	指定对等方在开始保持连接监控之前可以空闲的秒数。范围是 10-3600 秒。LAN 间组的默认值为 10 秒，远程访问组的默认值为 300 秒。

Command Default

远程访问组的默认值为阈值 300 秒，重试时间为 2 秒。

对于 LAN 间组，默认阈值为 10 秒，重试时间为 2 秒。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在每个隧道组中，默认启用 IKE 保持连接以及默认阈值和重试值。您可以仅将此属性应用于 IPsec 远程访问类型和 IPsec LAN 间隧道组类型。

CR_Examples

以下示例在 tunnel-group ipsec-attributes 配置模式下进入，配置 IKE DPD，将阈值确定为 15，并为 IP 地址为 209.165.200.225 的 IPsec LAN 间隧道组指定重试间隔为 10：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
```

```
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
clear-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。

isakmp nat-traversal（已弃用）

要全局启用 NAT 穿越，请在全局配置模式下检查 ISAKMP 是否已启用（可以使用命令启用 **isakmpenable**它），然后使用该 **isakmpnat-traversal**命令。如果已启用 NAT 遍历，则可以使用此命令的 **no**形式禁用它。

isakmp nat-traversal*natkeepalive*
no isakmp nat-traversal*natkeepalive*

Syntax Description

natkeepalive	设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

Command Default

默认情况下，NAT 穿越（**isakmpnat-traversal** 命令）是禁用的。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmpnat-traversal** 命令取而代之。

使用指南

许多使用 IPsec 的网络都使用网络地址转换 (NAT)，包括端口地址转换 (PAT)，但存在许多不兼容性，导致 IPsec 数据包无法成功通过 NAT 设备。NAT 遍历使 ESP 数据包能够穿过一个或多个 NAT 设备。

ASA 支持 NAT 遍历，如 IETF“IPsec 数据包的 UDP 封装”(UDP Encapsulation of IPsec Packets) 草案第 2 版和第 3 版所述（详见 http://www.ietf.org/html.charters/ipsec-charter.html ）和 NAT 遍历动态和静态加密映射均支持。

此命令将在 ASA 上全局启用 NAT-T。要在加密映射条目中禁用，请使用 **cryptomapsetnat-t-disable** 命令。

CR_Examples

以下示例在全局配置模式下启用 ISAKMP，然后启用 NAT 遍历，间隔为 30 秒：

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy authentication

要在 IKE 策略中指定身份验证方法，请在全局配置模式下使用**isakmppolicyauthentication** 命令。要删除 ISAKMP 身份验证方法，请使用 **clearconfigure**命令。

优先事项**isakmp policyauthentication** {**crack** | **pre-share** | **rsa-sig**}

Syntax Description

crack	指定 IKE 认证加密密钥质询/响应 (CRACK) 作为认证方法。
pre-share	指定预共享密钥作为身份验证方法。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
rsa-sig	指定 RSA 签名作为身份验证方法。 RSA 签名为 IKE 协商提供不可否认性。这意味着您可以向第三方证明您是否与对等体进行了 IKE 协商。

Command Default

默认 ISAKMP 策略身份验证是 **pre-share** 选项。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

IKE 策略定义一组用于 IKE 协商的参数。如果指定 RSA 签名，则必须配置 ASA 及其对等体，从证书颁发机构 (CA) 获取证书。如果指定预共享密钥，则必须在 ASA 及其对等体中单独配置这些预共享密钥。

CR_Examples

以下示例在全局配置模式下设置要在优先级编号为 40 的 IKE 策略中使用的 RSA 签名身份验证方法：

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy encryption（已弃用）

要指定要在 IKE 策略中使用的加密算法，请在全局配置模式下使用 **isakmppolicyencryption** 命令。要将加密算法重置为默认值，请使用此命令的 **no**形式。

isakmp policy*priority***encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}
no isakmp policy*priority***encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

Syntax Description

3des	指定在 IKE 策略中使用三重 DES 加密算法。
aes	指定要在 IKE 策略中使用的加密算法是具有 128 位密钥的 AES。
aes-192	指定要在 IKE 策略中使用的加密算法是具有 192 位密钥的 AES。
aes-256	指定要在 IKE 策略中使用的加密算法是具有 256 位密钥的 AES。
des	指定要在 IKE 策略中使用的加密算法为 56 位 DES-CBC。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

Command Default

默认 ISAKMP 策略加密为 **3des**。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmppolicyencryption** 命令取而代之。

CR_Examples

以下示例在全局配置模式下将 128 位密钥 AES 加密设置为要在优先级编号为 25 的 IKE 策略中使用的算法：

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

以下示例在全局配置模式下设置要在优先级数字为 40 的 IKE 策略中使用的 3DES 算法：

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy group（已弃用）

要为 IKE 策略指定 Diffie-Hellman 组，请在全局配置模式下使用**isakmppolicygroup**命令。要将 Diffie-Hellman 组标识符重置为默认值，请使用此命令的**no** 形式。

isakmp policy*priority***group** {**1** | **2** | **5**}
no isakmp policy*priority***group**

Syntax Description

group1	指定在 IKE 策略中使用 768 位 Diffie-Hellman 组。这是默认值。
group2	指定在 IKE 策略中使用 1024 位 Diffie-Hellman 组 2。
group5	指定在 IKE 策略中使用 1536 位 Diffie-Hellman 组 5。
priority	唯一标识 Internet 密钥交换 (IKE) 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。

Command Default

默认为组 2。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。已添加组 7 。
7.2(1)	此命令已弃用。该 **cryptoisakmppolicygroup** 命令取而代之。

使用指南

IKE 策略定义在 IKE 协商期间使用的一组参数。

有三个组选项：768 位（DH 组 1）、1024 位（DH 组 2）和 1536 位（DH 组 5）。1024 位和 1536 位 Diffie-Hellman 组可提供更强的安全性，但需要更多的 CPU 时间来执行。

注释 思科 VPN 客户端版本 3.x 或更高版本需要使用 ISAKMP 策略才能配置 DH 组 2。（如果已配置 DH 组 1，则思科 VPN 客户端无法连接。）AES 支持仅在许可用于 VPN-3DES 的 ASA 上可用。由于 AES 提供的密钥较大，ISAKMP 协商应该使用 Diffie-Hellman (DH) 组 5，而不是组 1 或组 2。这是使用 **isakmppolicyprioritygroup5** 命令完成的。

CR_Examples

以下示例在全局配置模式下输入，设置组 2（1024 位 Diffie Hellman）以用于优先级编号为 40 的 IKE 策略：

```
ciscoasa(config)# isakmp policy 40 group   2
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy hash（已弃用）

要为 IKE 策略指定散列算法，请在全局配置模式下使用 **isakmppolicyhash**命令。要将散列算法重置为 SHA-1 的默认值，请使用此命令的 **no** 形式。

isakmp policy*priority***hash** {**md5** | **sha**}
no isakmp policy*priority***hash**

Syntax Description

md5	指定在 IKE 策略中使用 MD5（HMAC 变体）作为散列算法。
priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
sha	指定将 SHA-1（HMAC 变体）用作 IKE 策略中的散列算法。

Command Default

默认散列算法是 SHA-1。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。**cryptoisakmppolicyhash**命令将取代它。

使用指南

IKE 策略定义在 IKE 协商期间使用的一组参数。

有两个散列算法选项：SHA-1 和 MD5。MD5 的摘要较小，被认为速度比 SHA-1 稍快。

CR_Examples

以下示例在全局配置模式下输入，指定在 IKE 策略中使用 MD5 散列算法，优先级数字为 40：

```
ciscoasa(config)# isakmp policy 40 hash    md5
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。

命令	说明
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp policy lifetime（已弃用）

如要指定 IKE 安全关联到期前的生命周期，请在全局配置模式下使用**isakmppolicylifetime**命令。要将安全关联生命周期重置为默认值 86,400 秒（一天），请使用此命令的 **no** 形式。

isakmp policy*priority***lifetime***seconds*
no isakmp policy*priority***lifetime**

Syntax Description

priority	唯一标识 IKE 策略并为该策略分配优先级。请使用一个介于 1 到 65,534 之间的整数，1 表示最高优先级，65534 表示最低优先级。
seconds	指定每个安全关联在到期前应存在的秒数。要建议有限生命周期，请使用 120 到 2147483647 秒之间的整数。要设置无限生命周期，请使用 0 秒。

Command Default

默认值为 86,400 秒（一天）。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmppolicylifetime** 命令取而代之。

使用指南

当 IKE 开始协商时，它会设法就其自身会话的安全参数达成一致。然后，每个对等体上的安全关联都会引用商定的参数。对等体将保留安全关联，直到生命周期到期。在安全关联到期之前，后续IKE 协商可以使用它，这可以节省设置新的IPsec 安全关联的时间。对等体将在当前安全关联到期之前协商新的安全关联。

生命期越长，ASA 设置未来 IPsec 安全关联的速度就越快。加密强度大到足以确保安全性，无需使用非常快的再生密钥时间（大约每隔几分钟再生一次）。建议您接受默认值，但如果对等体未提议生命周期，则可以指定无限生命周期。

注释 如果 IKE 安全关联设置为无限生命周期，但对等体提议有限生命周期，则使用对等体协商的有限生命周期。

CR_Examples

以下示例在全局配置模式下输入，在优先级编号为 40 的 IKE 策略中将 IKE 安全关联的生命周期设置为 50,4000 秒（14 小时）：

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

以下示例在全局配置模式下将 IKE 安全关联设置为无限生命周期。

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

Related Commands

clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isakmp reload-wait (已弃用)

要允许等待所有活动会话自行终止后再重新启动 ASA，请在全局配置模式下使用**isakmpreload-wait** 命令。要禁用等待活动会话终止并重新启动 ASA，请使用此命令的 **no** 形式。

isakmp reload-wait
no isakmp reload-wait

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	此命令已弃用。该 **cryptoisakmpreload-wait** 命令取而代之。

CR_Examples

以下示例在全局配置模式下输入，指示 ASA 等待所有活动会话终止后再重新启动：

```
ciscoasa(config)# isakmp reload-wait
```

Related Commands

命令	说明
clearconfigureisakmp	清除所有 ISAKMP 配置。
clearconfigureisakmppolicy	清除所有 ISAKMP 策略配置。
clearisakmpsa	清除 IKE 运行时间 SA 数据库。
showrunning-configisakmp	显示所有活动配置。

isis priority

要配置接口上指定 ASA 的优先级，请在接口 isis 配置模式下使用 **isispriority** 命令。要重置默认优先级，请使用此命 **no**令的形式。

isis priority*number-value* [**level-1** | **level-2**]
no isis priority [**level-1** | **level-2**]

Syntax Description

number-value	设置路由器的优先级。范围为 0 到 127。
level-1	（可选）单独设置 1 级的优先级。
level-2	（可选）单独设置 2 级的优先级。

Command Default

默认值为 64。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令设置用于确定 LAN 上的哪个 ASA 将成为指定路由器或 DIS 的优先级。优先级将在呼叫数据包中通告。优先级最高的 ASA 将成为 DIS。

注释 在 IS-IS 中，没有指定备份的路由器。将优先级设置为 0 将降低此系统成为 DIS 的几率，但不会阻止其成为 DIS。如果具有更高优先级的 ASA 上线，它将接管当前 DIS 的角色。在优先级相等的情况下，最高 MAC 地址将打破平衡。

CR_Examples

以下示例展示通过将优先级设置为 80 提供优先级的第 1 级路由。此 ASA 现在更有可能成为 DIS：

```
ciscoasa(config)#
interface GigabitEthernet0/0
```

```
ciscoasa(config-if)#
isis priority 80 level-1
```

Related Commands

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

命令	说明
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
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。

命令	说明
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis protocol shutdown

要禁用 IS-IS 协议，以使其无法在指定接口上形成邻接关系，并将该接口的 IP 地址放入 ASA 生成的 LSP 中，请在接口 isis 配置模式下使用该 **isisprotocolshutdown**命令。要重新启用 IS-IS 协议，请使用此命 **no**令的形式。

isis protocol shutdown
no isis protocol shutdown

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令将使您能为指定接口禁用 IS-IS 协议，而不会删除配置参数。对于配置了该命令的接口，IS-IS 协议不会形成任何邻接关系，并且该接口的 IP 地址会放入 ASA 生成的 LSP 中。如果您不希望 IS-IS 在 **protocolshutdown**任何接口上形成任何邻接关系并清除 IS-IS LSP 数据库，请使用该命令。

CR_Examples

以下示例在千兆以太网 0/0 上禁用 IS-IS 协议：

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis protocol shutdown
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

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

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
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。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis retransmit-interval

要配置每个 IS-IS LSP 的重新传输之间的时间量，请在接口 isis 配置模式下使用 **isisretransmit-interval** 命令。要恢复默认值，请使用此命 **no**令的形式。

isis retransmit-interval秒
no isis retransmit-interval秒

Syntax Description

秒（可选）每个 LSP 重新传输之间的时间。数字应该大于已连接网络上任意两个路由器之间的预计往返延迟。范围为 0 到 65535。

Command Default

默认值为 5。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

请确保保守地设置 *seconds* 参数，否则可能会导致不必要的重新传输。此命令对 LAN（多点）接口没有影响。

CR_Examples

以下示例将 GigabitEthernet 0/0 配置为大型串行线路的每 60 秒重新传输每个 IS-IS LSP：

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-interval 60
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

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

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
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。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

isis retransmit-throttle-interval

要配置接口上每个 IS-IS LSP 的重新传输之间的时间量，请在接口 isis 配置模式下使用 **isisretransmit-throttle-interval** 命令。要恢复默认值，请使用此命 **no**令的形式。

isis retransmit-throttle-interval*milliseconds*
no isis retransmit-throttle-interval

Syntax Description

毫秒	（可选）接口上 LSP 重传之间的最小延迟。范围为 0 到 65535。

Command Default

延迟由 **isislsp-interval** 命令确定。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

在包含很多 LSP 和很多接口的大型网络中，作为控制 LSP 重新传输流量的一种方式，此命令可能非常有效。此命令可以控制可在接口上重新发送 LSP 的速率。

该命令不同于接口上发送 LSP 的速率（由命令控 **isislsp-interval**制）和单个 LSP 重传之间的周期（由命令控 **isisretransmit-interval**制）。您可以组合使用这些命令，以控制从一个 ASA 到其邻居的路由流量的提供负载。

CR_Examples

以下示例配置 GigabitEthernet 0/0 以将 LSP 重新传输的速率限制为每 300 毫秒一次：

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-throttle-interval 300
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。

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

命令	说明
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
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。
routerisis	启用 IS-IS 路由。

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

isis tag

当将某个 IP 前缀放入 IS-IS LSP 时，要在该接口配置的 IP 地址上设置标签，请在 **isistag**接口 isis 配置模式下使用该命令。要停止标记 IP 地址，请使用此命 **no**令的形式。

isis tag*tag-number*
no isis tag*tag-number*

Syntax Description

tag-number	用作 IS-IS 路由标签的数字。范围为 1 到 4294967295。

Command Default

没有与为接口配置的 IP 地址关联的路由标记。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

直到使用标签时，才会对设置该标签的路由进行操作，例如，重新分发路由或汇总路由。配置此命令将触发 ASA 生成新的 LSP，因为标签是数据包中新的信息片段。

CR_Examples

以下示例将 GigabitEthernet 0/0 配置为具有标记 100：

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis tag 100
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。

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

命令	说明
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
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。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。

命令	说明
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

is-type

要配置 IS-IS 路由进程实例的路由级别，请在路由器 isis 配置模式下使用 **is-type** 命令。要重置默认值，请使用此命 **no**令的形式。

isis type [**level-1** | **level 1-2** | **level-2-only**
no isis type [**level-1** | **level 1-2** | **level-2-only**

Syntax Description

level-1	（可选）表示区域内路由。此 ASA 仅了解其区域内的目的地。2 级（区域间）路由由最近的 1-2 级 ASA 执行。
level-1-2	（可选）ASA 同时执行 1 级和 2 级路由。此 ASA 运行两个路由进程实例。它有一个用于区域内目的地（1 级路由）的链路状态数据包数据库 (LSDB)，并运行最短路径优先 (SPF) 计算来发现区域拓扑。它还具有另一个 LSDB，其中包含所有其他骨干网（第 2 级）路由器的链路状态数据包 (LSP)，并运行另一个 SPF 计算来发现骨干网的拓扑以及所有其他区域的存在。
level-2-only	（可选）表示区域间路由。此 ASA 是主干网的一部分，并且不与其所在区域内的仅限 1 级的 ASA 进行通信。

Command Default

在常规 IS-IS 配置中，ASA 作为第 1 级（区域内部）和第 2 级（区域间）路由器。

在多区域 IS-IS 配置中，配置 IS-IS 路由进程的第一个实例默认情况下是第 1-2 级（区域内部和区域间）路由器。配置的 IS-IS 进程的其余实例默认情况下是第 1 级路由器。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

我们强烈建议您配置 IS-IS 路由进程的类型。如果要配置多区域 IS-IS，则必须配置路由器类型，或允许默认情况下配置路由器。默认情况下，使用 **routerisis** 命令配置的 IS-IS 路由进程的第一个实例是 1-2 级路由器。

如果网络中只有一个区域，则无需同时运行 1 级和 2 级路由算法。如果 IS-IS 用于无连接网络服务 (CLNS) 路由（并且只有一个区域），则在任何地方都必须仅使用第 1 级。如果 IS-IS 仅用于 IP 路由

（并且只有一个区域），则只能在任何位置运行第 2 级。在 1-2 级区域存在之后添加的区域，默认情况下是 1 级区域。

如果已为 1-2 级（IS-IS 路由进程的第一个实例的默认设置）配置路由器实例，则可以使用 **is-type** 命令删除区域的 2 级（区域间）路由。您还可以使用 **is-type** 命令为区域配置 2 级路由。

CR_Examples

以下示例指定区域路由器：

```
ciscoasa#
router isis
ciscoasa(config-router)#
is-type level-2-only
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型

命令	说明
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。

命令	说明
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

issuer (Deprecated)

注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定向 SAML 类型 SSO 服务器发送断言的安全设备，请在 webvpn-sso-saml 配置模式下对该特定 SAML 类型使用 **issuer**命令。要删除发行者名称，请使用此命 **no**令的形式。

issuer*identifier*
no issuer [*identifier*]

Syntax Description

identifier 指定安全设备名称，通常是设备的主机名。标识符必须少于 65 个字母数字字符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
8.0(2)	添加了此命令。
9.5(2)	此命令已弃用。

使用指南

SSO 支持仅适用于 WebVPN，让用户无需多次输入用户名和密码即可访问不同服务器上的不同安全服务。ASA 目前支持 SAML POST 类型的 SSO 服务器和 SiteMinder 类型的 SSO 服务器。

此命令仅适用于 SAML 类型的 SSO 服务器。

CR_Examples

以下示例指定名为 asa1.example.com 的安全设备的颁发者名称：

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

Related Commands

命令	说明
assertion-consumer-url	指定安全设备用于联系 SAML 类型 SSO 服务器断言消费者服务的 URL。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
showwebvpnsso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息。
sso-server	创建单点登录服务器。
信任点	指定包含用于对 SAML 类型浏览器断言进行签名的证书的信任点名称。

issuer-name

要指定所有已颁发证书的颁发者名称 DN，请在本地证书颁发机构 (CA) 服务器配置模式下使用 **issuer-name**命令。要从证书颁发机构证书中删除使用者 DN，请使用此命令的 **no** 形式。

issuer-name*DN-string*
no issuer-name*DN-string*

Syntax Description

DN-string	指定证书的可分辨名称，也是自签名CA证书的主体名称DN。使用逗号分隔属性-值对。在任何包含逗号的值两边插入引号。发行人名称必须少于 500 个字母数字字符。

Command Default

默认颁发者名称为 cn=*hostame.domain*-name，例如 cn=asa.example.com。

Command Modes

下表展示可输入命令的模式：

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

Command History

版本	修改
7.3(1)	添加了此命令。
8.0(2)	添加了对引号的支持，以保留*DN*字符串 值中的逗号。

使用指南

该命令指定由本地CA服务器创建的任何证书上显示的颁发者名称。如果希望颁发者名称与默认CA名称不同，请使用此可选命令。

注释 通过发出 **noshutdown** 命令启用 CA 服务器并生成证书后，无法更改此颁发者名称配置。

CR_Examples

以下示例配置证书身份验证：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc.”
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
crypto ca server	提供对ca服务器配置模式命令的访问，这些命令允许您配置和管理本地CA。
keysize	指定证书注册时生成的公钥和私钥的大小。
lifetime	指定 CA 证书和颁发的证书的有效期。
showcryptocaserver	显示本地 CA 的特征。
showcryptocaservercert-db	显示本地 CA 服务器证书。

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。