IPsec 和 ISAKMP

有关隧道、IPsec 和 ISAKMP

本主题介绍用于建立虚拟专用网络 (VPN) 的互联网协议安全 (IPsec) 以及互联网安全关联和密钥管理协议 (ISAKMP) 标准。

借助隧道，可以使用互联网等公共TCP/IP网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

ASA 使用 ISAKMP 和 IPSec 隧道标准来建立和管理隧道。ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数
- 建立隧道
- 验证用户和数据
- 管理安全密钥
- 加密和解密数据
- 管理隧道中的数据传输
- 作为隧道终端或路由器管理入站和出站数据传输

ASA 可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目标。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

IPsec 概述

ASA 会将 IPsec 用于 LAN 间 VPN 连接，并提供将 IPsec 用于客户端到 LAN VPN 连接的选项。在 IPsec 术语中，对等体是一个远程访问客户端或其他安全网关。对于这两个连接类型， ASA 仅支持思科对等体。由于我们遵守 VPN 行业标准，ASA 也可以与其他供应商的对等体结合使用；但是，我们不支持这些对等体。

在建立隧道的过程中，两个对等体会协商管理身份验证、加密、封装和密钥管理的安全关联。这些协商包括两个阶段：第一个阶段，建立隧道 (IKE SA)；第二个阶段，管理该隧道内的流量 (IPsec SA)。

LAN 间 VPN 可连接不同地理位置的网络。在 IPsec LAN 间 连接中，ASA 可用作发起方或响应方。在 IPsec 客户端到 LAN 连接中，ASA 只能用作响应方。发起方会提议 SA；响应方会接受、拒绝或提出相反提议，所有这一切都根据配置的 SA 参数进行。要建立连接，两个实体都必须同意 SA。

了解 IPsec 隧道

IPsec 隧道是 ASA 在对等体之间建立的 SA 集合。SA 指定适用于敏感数据的协议和算法并指定对等体使用的密钥内容。IPSec SA 控制用户流量的实际传输。SA 是单向的，但是通常成对建立（入站和出站）。

对等体协商用于每个 SA 的设置。每个 SA 包括以下内容：

- IKEv1 转换集或 IKEv2 提议
- 加密映射
- ACL
- 隧道组
- 预分片策略

ISAKMP 和 IKE 概述

ISAKMP 是使两台主机商定如何构建 IPsec 安全关联 (SA) 的协商协议。它提供用于商定 SA 属性的格式的通用框架。此安全关联包括与对等体协商 SA 以及修改或删除 SA。ISAKMP 将协商分为两个阶段：阶段 1 和阶段 2。阶段 1 创建第一条隧道，其将保护随后的 ISAKMP 协商消息。阶段 2 创建保护数据的隧道。

IKE 使用 ISAKMP 为要使用的 IPsec 设置 SA。IKE 创建用于对对等体进行身份验证的加密密钥。

ASA 支持为旧版思科 VPN 客户端连接使用 IKEv1，还支持为 AnyConnect VPN 客户端使用 IKEv2。

要设置 ISAKMP 协商的条款，请创建 IKE 策略，其中包含以下内容：

- IKEv1 对等体必需的身份验证类型：使用证书的 RSA 签名或预共享密钥 (PSK)。
- 加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法，用于确保发送方的身份，以及确保消息在传输过程中未发生修改。

- Diffie-Hellman 群，用于确定 encryption-key-determination 算法的强度。ASA 使用此算法派生加密密钥和散列密钥。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密等所要求的密钥内容和散列运算的算法。
- 在更换加密密钥前，ASA 可使用该加密密钥的时间限制。

利用 IKEv1 策略，您要为每个参数设置一个值。对于 IKEv2，您可以为单个策略配置多个加密和身份验证类型以及多个完整性算法。ASA 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，您可以发送单个提议来传达所有允许的转换，而无需像对 IKEv1 一样发送每个允许的组合。

ASA 不支持 IKEv2 多安全关联 (SA)。ASA 当前仅接受找到的第一个 SA 上的入站 IPsec 流量。如果在任何其他 SA 上收到 IPsec 流量，则该流量将由于 `vpn-overlap-conflict` 而被丢弃。多个 IPsec SA 可能来自两个对等体之间的重复隧道，也可能来自非对称隧道。

了解 IKEv1 转换集和 IKEv2 提议

IKEv1 转换集或 IKEv2 提议是定义 ASA 如何保护数据的安全协议和算法的组合。在 IPsec SA 协商中，对等体必须标识两个对等体都一样的转换集或提议。然后ASA应用匹配的转换集或提议为该加密映射创建保护 ACL 中数据流的 SA。

利用 IKEv1 转换集，您可以为每个参数设置一个值。对于 IKEv2 提议，您可以为单个提议配置多个加密和身份验证类型以及多个完整性算法。ASA 将按照安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

如果您更改用于创建其 SA 的转换集或提议的定义，ASA 将撤销隧道。有关详细信息，请参阅清除安全关联，第 39 页。

注释 如果您清除或删除转换集或提议中的唯一元素，ASA 将自动取消其加密映射引用。

关于 IKEv2 多对等体加密映射

从 9.14(1) 版本开始，ASA IKEv2 支持多对等体加密映射 - 当隧道中的对等体关闭时，IKEv2 尝试与列表中的下一个对等体建立隧道。最多可以使用 10 个对等体地址来配置加密映射。IKEv2 上的这种多对等体支持非常有用，特别是从具有多对等体加密映射的 IKEv1 迁移时。

IKEv2 仅支持双向加密映射。因此，在双向加密映射上也配置了多个对等体，并使用相同的方法接受来自发起隧道的对等体的请求。

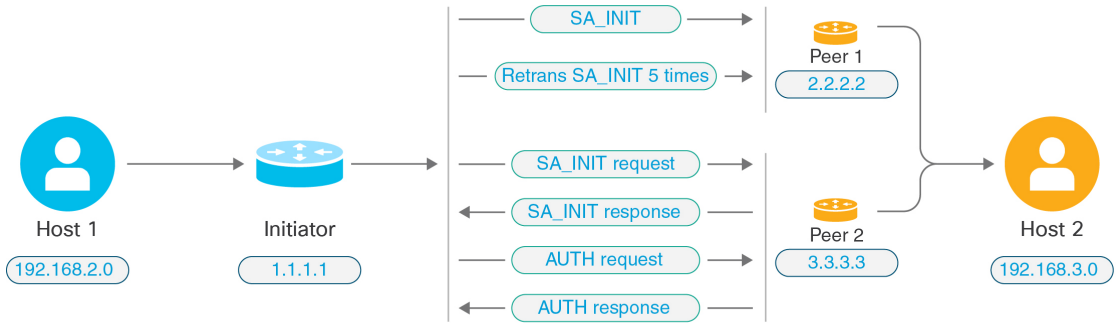
IKEv2 发起方行为

IKEv2 发起与对等体（例如 Peer1）的会话。如果对等体 1 无法访问 5 次 SA_INIT 重传，则会发送最终重传。此活动大约需要 2 分钟。

当 Peer1 发生故障时，SA_INIT 消息会被发送到 Peer2。如果 Peer2 也无法访问，则在 2 分钟后发起与 Peer3 的会话。

在加密映射的对等体列表中的所有对等体都用尽后，IKEv2 会再次从 Peer1 发起会话，直到与任何对等体建立 SA。下图描述了该行为。

图 *1:* 发起方流程



注释 发起 IKE SA 需要持续的流量，以便每次失败尝试都会移动到下一个对等体，并最终由某个可访问的对等体建立 SA。在流量中断的情况下需要手动触发，以便启动与下一个对等体的 IKE SA。

IKEv2 响应方行为

如果在加密映射中为 IKE SA 的响应方设备配置了多个对等体，则每次尝试 IKE SA 时，都会使用加密映射中的当前活动对等体的地址来验证发起方 IKE SA 的地址。

例如，如果加密映射中的当前活动对等体（用作响应方）是第一个对等体，则会从 Peer1 IP 地址发起 IKE SA。同样，如果加密映射中的当前活动对等体（用作响应方）是第二个对等体，则会从 Peer2 IP 地址发起 IKE SA。

注释 IKEv2 多对等体拓扑的响应方侧不支持对等体遍历。

加密映射更改时重置对等体索引

对加密映射所做的任何更改都会将对等体索引重置为零，并且隧道启动将从列表中的第一个对等体开始。下表提供了特定条件下的多对等体索引转换：

表 *1: SA* 之前的多对等体索引转换

SA 之前的条件	对等体索引已移动 是/否/重置
对等体无法访问	是
第 1 阶段提议不匹配	是
第 2 阶段提议不匹配	是
未收到 DPD 确认	是
身份验证阶段的流量选择器不匹配	是
身份验证失败	是
由于对等体无法访问，密钥更新失败	重置

表 *2: SA* 之后的多对等体索引转换

SA 后的条件	对等体索引已移动 是/否/重置
由于提议不匹配，密钥更新失败	重置
重新生成密钥期间流量选择器不匹配	重置
加密映射修改	重置
HA 切换	否
清除加密 IKEv2 SA	重置
清除 ipsec sa	重置
IKEv2 SA 超时	重置

IKEv2 多对等体的准则

IKEv1 和 IKEv2 协议

如果加密映射同时配置了 IKE 版本和多个对等体，则在移动到下一个对等体之前，将在两个版本的每个对等体上进行 SA 尝试。

例如，如果加密映射配置了两个对等体（例如 P1 和 P2），则会使用 IKEv2 向 P1 发起隧道，使用 IKEv1 向 P1 发起隧道，使用 IKEv2 向 P2 发起隧道，以此类推。

高可用性

具有多个对等体的加密映射会启动通往 HA 中的响应方设备的隧道。当第一台设备无法访问时，它就会移至下一台响应方设备。

发起方设备发起到响应方设备的隧道。如果主用设备发生故障，备用设备会尝试从 Peer1 IP 地址建立隧道，而不管主用设备上的 Peer2 IP 地址的加密映射如何。

集中式集群

具有多个对等体的加密映射可以启动通往集中式集群部署中的响应方设备的隧道。如果第一台设备无法访问，它会尝试移至下一台响应方设备。

发起方设备发起到响应方设备的隧道。如果无法访问 Peer1，那么集群中的每个节点都会移动到下一个 Peer2。

分布式集群

如果配置了 IKEv2 多对等体加密映射，则不支持分布式集群。

多情景模式

在多情景模式下，多对等体行为将特定于每个情景。

调试命令

如果隧道建立失败，请启用这些命令以对问题作进一步分析。

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

以下示例是特定于 IKEv2 多对等体的调试日志，显示了对等体的转换。

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto map.
```

IPsec VPN 的许可

注释　此功能不适用于无负载加密型号。

使用 IKEv2 的 IPsec 远程访问 VPN 需要 AnyConnect Plus 或 Apex 许可证，可单独购买。使用 IKEv1 的 IPsec 远程访问 VPN 和使用 IKEv1 或 IKEv2 的 IPsec 站点间 VPN 使用 基础 许可证随附的其他 VPN 许可证。有关每个型号的最大值，请参阅思科 ASA 系列功能许可证。

IPsec VPN 准则

情景模式准则

支持单情景或多情景模式。在多情景模式下，远程访问 VPN 需要 AnyConnect Apex 许可证。尽管 ASA 未明确认可 AnyConnect Apex 许可证，但它实施 Apex 许可证的特征，例如获得平台限制许可的 AnyConnect 高级版、Secure Client 移动版、适用于思科 VPN 电话的 Secure Client 和高级终端评估。

防火墙模式指导原则

仅支持路由防火墙模式。不支持透明防火墙模式。

故障转移准则

仅在主用/备用故障转移配置中复制 IPsec VPN 会话。

其他准则

在配置 IKE 时，系统会自动保留 RADIUS UDP 端口 1645 和 1646。系统日志 713903 中记录了此预留，其中端口号显示为 27910 和 28166。该预留可确保端口不会被用于 PAT 转换。

配置 ISAKMP

配置 IKEv1 和 IKEv2 策略

IKEv1 和 IKEv2 最多分别支持 20 个 IKE 策略，每个都有不同的值集。为您创建的每个策略分别分配一个唯一的优先级。优先级数值越低，优先级就越高。

在 IKE 协商开始时，发起协商的对等体将其所有策略发送至远程对等体，然后远程对等体将尝试找到一个匹配项。远程对等体将按照优先级顺序（优先级最高的优先），将该对等体的所有策略与自身配置的各个策略进行比对，直到发现一个匹配项。

当来自两个对等体的两个策略包含相同的加密、散列、身份验证和 Diffie-Hellman 参数值时，表明存在匹配项。对于 IKEv1，远程对等体策略还必须指定一个生命周期，其值应低于或等于发起方发送的策略中的生命周期。如果生命周期不相同，ASA 将使用较短的生命周期。对于 IKEv2，各对等体之间将不协商生命周期，而是在本地进行管理，从而可以在每个对等体上单独配置其生命周期。如果不存在可接受的匹配项，IKE 将拒绝协商，并且不会建立 SA。

毫无疑问，为每个参数选择具体值时，需要在安全和性能之间进行权衡。默认值提供的安全级别足以达到大多数组织的安全要求。如果与仅支持一个参数值的对等体进行互操作，则只能选择该参数值。

您必须在每个 ISAKMP 命令中包含优先级。优先级数值唯一标识了策略并且决定着策略在 IKE 协商中的优先级。

过程

步骤 1 要创建 IKE 策略，请在单情景或多情景模式下从全局配置模式输入 **crypto** *ikev1* | *ikev2* policy 命令。提示符将显示 IKE 策略配置模式。

示例：

```
hostname(config)# crypto ikev1 policy 1
```

注释 新的 ASA 配置没有默认 IKEv1 或 IKEv2 策略。

步骤 2 指定加密算法。 默认值为 AES-128。

encryption [aes | aes-192 | aes-256]

示例：

```
hostname(config-ikev1-policy)#
encryption aes
```

步骤 3 指定散列算法。默认值为 SHA-1。

hash[sha]

示例：

```
hostname(config-ikev1-policy)#
hash sha
```

步骤 4 指定身份验证方法。默认设置为预共享密钥。

authentication[**pre-shared**]**rsa-sig**]

示例：

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

步骤 5 指定 Diffie-Hellman 群标识符。默认值是组 14。

group [14]

示例：

```
hostname(config-ikev1-policy)#
group 14
```

步骤 6 指定 SA 生命周期。默认值为 86400 秒（24 小时）。

lifetime *seconds*

示例：

此示例将其生命周期设置为 4 小时（14400 秒）：

```
hostname(config-ikev1-policy)# lifetime 14400
```

步骤 7 使用 IKE 策略关键字和值，第 9 页中提供的 IKEv1 和 IKEv2 策略关键字及其值来指定其他设置。如果您没有为特定策略参数指定值，则将应用默认值。

IKE 策略关键字和值

	关键字	含义	说明
authentication	**rsa-sig**	带有使用RSA签名算法生成的密钥的数字证书	指定 ASA 用于建立每个 IPSec 对等体身份的身份验证方法。
	pre-share（默认）	预共享密钥	预共享密钥不能在增长型网络中很好地进行扩展，但是在小型网络中更容易设置。
encryption	**aes**（默认值）	使用 128 位密钥的 AES	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。 默认值为 128 位密钥。
hash	**sha**（默认）	SHA-1（HMAC 变体）	指定用于确保数据完整性的散列算法。它可以确保数据包来自其所声明的发送方，并且在传输过程中未被修改。
group	**14**（默认值）	组 14（2048 位）	指定 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享密钥。 Diffie-Hellman 群编号越小，其执行所要求的 CPU 时间就越少。Diffie-Hellman 群编号越大，则安全性越高。 默认组是 DH 组 14
lifetime	**整数值** （86400＝默认值）	120 至 2147483647 秒	指定 SA 生命周期。默认值为 86400 秒或 24 小时。通常，此生命周期越短，ISAKMP 协商（在某种程度上）越安全。但是，此生命周期越短，ASA 设置后续 IPSec SA 的速度越快。

	关键字	含义	说明
integrity	sha（默认）	SHA-1（HMAC 变体）	指定用于确保数据完整性的散列算法。它可以确保数据包来自其所声明的发送方，并且在传输过程中未被修改。
	sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全散列算法 SHA 2。
	sha384	SHA 2，384 位摘要	指定具有 384 位摘要的安全散列算法 SHA 2。
	sha512	SHA 2，512 位摘要	指定具有 512 位摘要的安全散列算法 SHA 2。
	null		指定 AES-GCM 为加密算法时，管理员可以选择 null 作为 IKEv2 完整性算法。

	关键字	含义	说明
encryption	aes（默认值）	AES	指定保护两个 IPSec 对等体之间传输的数据的对称加密算法。 默认值为 128 位 AES。
	aesaes-192aes-256		高级加密标准支持长度为 128、192、256 位的密钥。
	aesgcmaesgcm192aesgcm256	用于 IKEv2 加密的 AES-GCM 算法选项	高级加密标准支持长度为 128、192、256 位的密钥。
policy_index			访问 IKEv2 策略子模式。
prf	sha（默认）	SHA-1（HMAC 变体）	指定伪随机函数 (PRF)，即用于生成密钥内容的算法。
	sha256	SHA 2，256 位摘要	指定具有 256 位摘要的安全散列算法 SHA 2。
	sha384	SHA 2，384 位摘要	指定具有 384 位摘要的安全散列算法 SHA 2。
	sha512	SHA 2，512 位摘要	指定具有 512 位摘要的安全散列算法 SHA 2。
priority			将策略模式扩展为支持其他 IPsec V3 功能并使 AES-GCM 和 ECDH 设置成为 Suite B 支持的一部分。
group	**1419202124**	组 14（2048 位）	指定 Diffie-Hellman 群标识符，两个 IPsec 对等体会在不相互传输该标识符的情况下，使用该标识符来派生共享密钥。 Diffie-Hellman 群编号越小，其执行所要求的 CPU 时间就越少。Diffie-Hellman 群编号越大，则安全性越高。 默认值为 (DH) 组 14
lifetime	**整数值** （86400＝默认值）	120 至 2147483647 秒	指定 SA 生命周期。默认值为 86400 秒或 24 小时。通常，此生命周期越短，ISAKMP 协商（在某种程度上）越安全。但是，此生命周期越短，ASA 设置后续 IPSec SA 的速度越快。

在外部接口上启用 IKE

您必须在终止 VPN 隧道的接口上启用 IKE。这通常是外部或公共接口。要启用 IKEv1 或 IKEv2，请在单情景或多情景模式下从全局配置模式使用 crypto [**ikev1** | **ikev2**] **enable** *interface-name* 命令。

例如：

```
hostname(config)# crypto ikev1 enable outside
```

启用或禁用 IKEv1 积极模式

阶段 1 IKEv1 协商可以使用主模式或积极模式。这两个模式提供相同的服务，但是积极模式只需在对等体之间进行两次消息交换，交换总计三条消息；而不需要进行三次消息交换，交换总计六条消息。积极模式速度更快，但是不为通信方提供标识保护。因此，对等体在建立安全 SA 之前必须交换标识信息。默认情况下启用积极模式。

注释 禁用积极模式可防止思科 VPN 客户端使用预共享密钥身份验证建立通向 ASA 的隧道。但是，它们可以使用基于证书的身份验证（也就是 ASA 或 RSA）建立隧道。

要为第 1 阶段 IKEv1 协商启用积极模式，请在单情景或多情景模式下输入以下命令：

```
hostname(config)# crypto map <map-name> seq-num set ikev1 phase1-mode aggressive <group-name>
```

要禁用积极模式，请在单情景或多情景模式下输入以下命令：

```
hostname(config)# crypto ikev1 am-disable
```

如果禁用了积极模式，然后想要恢复它，请使用此命令的 no 形式。例如：

```
hostname(config)#  no crypto ikev1 am-disable
```

配置 IKEv1 和 IKEv2 ISAKMP 对等体的 ID 方法

在 IKEv1 或 IKEv2 ISAKMP 阶段 I 协商中，对等体必须相互标识自身身份。您可以从以下选项中选择标识方法。

Address	使用交换 ISAKMP 标识信息的主机的 IP 地址。
Automatic （默认）	按连接类型确定 ISAKMP 协商： • 预共享密钥的 IP 地址。 • 证书身份验证的证书可分辨名称。
Hostname	使用交换 ISAKMP 标识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。

ASA 使用要向对等体发送的阶段 I ID。所有 VPN 场景都是如此，但主模式下 LAN 间 IKEv1 连接除外，它使用预共享密钥进行身份验证。

要更改对等标识方法，请在单情景或多情景模式下输入以下命令：

crypto isakmp identity {*address* | *hostname* | **key-id** *id-string* | **auto**}

例如，以下命令将对等标识方法设置为使用主机名：

```
hostname(config)# crypto isakmp identity hostname
```

INVALID_SELECTORS 通知

如果 IPsec 系统在某个 SA 上收到入站数据包，但该数据包的报头字段与该 SA 的选择符不一致，则 IPsec 系统必须丢弃该数据包。此事件的审核日志条目包括当前日期/时间、SPI、IPsec 协议、数据包的源和目标、该数据包的任何其他可用向量值，以及来自相关SA条目的选择符值。系统会生成IKE通知 INVALID_SELECTORS 并发送到发送方（IPsec 对等体），表明收到的数据包因未能通过选择符检查而丢弃。

ASA 已在 CTM 中使用如下所示的现有系统日志对此事件进行日志记录：

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

管理员现在可以启用或禁用在SA上收到与该SA的流量选择符不匹配的入站数据包时向对等体发送IKEv2 通知。如果启用，IKEv2 通知消息的速率限制为每个 SA 每 5 秒发送一条通知消息。IKEv2 通知在 IKEv2 信息交换中发送到对等体。

配置十六进制 IKEv2 预共享密钥

您可以在本地和远程预共享密钥命令中添加关键字 *hex*，配置十六进制的 IKEv2 预共享密钥。

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

启用或禁用发送 IKE 通知

管理员可以启用或禁用在 IKEv2 IPsec VPN 连接上收到与该连接的流量选择符不匹配的入站数据包时向对等体发送 IKE 通知。默认情况下禁用发送此通知。使用以下 CLI 命令启用或禁用在对 ASDM 证书中的用户名授权时发送 IKE INVALID_SELECTORS 通知：

[**no**] **crypto ikev2 notify invalid-selectors**

执行证书身份验证时，证书中的 CN 就是用户名，并且将对本地服务器执行授权。如果检索“service-type”属性，则按前文所述进行处理。

配置 IKEv2 分片选项

在 ASA 上，可以启用或禁用 IKEv2 分片，可以指定对 IKEv2 数据包分片时的 MTU（最大传输单位），还可以由管理员使用以下命令配置首选分片方法：

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

默认情况下，启用所有 IKEv2 分片方法， IPv4 的 MTU 为 576，IPv6 的 MTU 为 1280，首选方法为 IETF 标准 RFC-7383。

在考虑以下注意事项的情况下，指定 [**mtu** <*mtu-size*>]：

- 使用的 MTU 值应包括 IP (IPv4/IPv6) 报头 + UDP 报头大小。
- 如果管理员未指定，则 IPv4 的默认 MTU 为 576，IPv6 的默认 MTU 为 1280。
- 一旦指定，则对 IPv4 和 IPv6 使用相同的 MTU。
- 有效范围介于 68 至 1500 之间。

注释 在配置 MTU 时，您必须考虑 ESP 开销。由于加密期间添加到 MTU 的 ESP 开销，数据包的大小会在加密后增加。如果收到“数据包太大”(packet too big) 错误，请确保检查 MTU 大小并配置较低的 MTU。

可将以下支持的分片方法之一配置为 IKEv2 [**preferred-method** [**ietf** | **cisco**]] 的首选分片方法：

- 基于 IETF RFC-7383 标准的 IKEv2 分片。
  - 当两个对等体都指定了协商期间的支持和首选项时，系统将使用此方法。
  - 使用此方法时，系统将在分片后执行加密，为每个 IKEv2 分片消息提供单独的保护。
- 思科专有分片。
  - 如果此方法是对等体（例如 Secure Client）提供的唯一方法，或者两个对等体都指定了协商期间的支持和首选项，则系统将使用此方法。
  - 使用此方法时，系统将在加密后执行分片。接收方对等体在收到所有分片之前，无法对消息进行解密或身份验证。
  - 此方法不能与非思科对等体实现互操作。

命令 **show running-config crypto ikev2** 将显示当前配置，**show crypto ikev2 sa detail** 将显示将分片用于 SA 时所实施的 MTU。

开始之前

- 不支持路径 MTU 发现，需要手动配置 MTU 以符合网络的需求。
- 此配置是全局配置，将影响应用该配置后所建立的后续 SA。较早的 SA 不会受到影响。禁用分片时，同样如此。
- 最多可以接收 100 个分片。

示例

- 要禁用 IKEv2 分片，请执行以下操作：

```
no crypto ikev2 fragmentation
```

- 要恢复默认操作，请执行以下操作：

```
crypto ikev2 fragmentation
```

或

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- 要将 MTU 值更改为 600，请执行以下操作：

```
crypto ikev2 fragmentation mtu 600
```

- 要恢复默认 MTU 值，请执行以下操作：

```
 no crypto ikev2 fragmentation mtu 576
```

- 要将首选分片方法更改为“思科”，请执行以下操作：

```
crypto ikev2 fragmentation preferred-method cisco
```

- 要将首选分片方法恢复为“IETF”，请执行以下操作：

```
no crypto ikev2 fragmentation preferred-method cisco
```

或

```
 crypto ikev2 fragmentation preferred-method ietf
```

AAA 身份验证和授权

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

使用用户输入的用户名/密码，对本地服务器执行 AAA 身份验证。使用同一用户名，对 *radius* 服务器执行其他授权。如果检索 *service-type* 属性，则按前文所述进行处理。

启用经由 NAT-T 的 IPsec

NAT-T 允许 IPsec 对等体通过 NAT 设备建立连接。其方法是使用端口 4500 将 IPsec 流量封装在 UDP 数据报中，从而为 NAT 设备提供端口信息。NAT-T 会自动检测所有 NAT 设备，但只有在必要时才封装 IPSec 流量。

注释 由于 Secure Client的限制，您必须启用 NAT-T，才能让 Secure Client使用 IKEv2 成功建立连接。即使客户端不在 NAT-T 设备后面，此要求也适用。

ASA 可同时支持标准 IPsec、IPsec over TCP、NAT-T 和 IPsecover UDP，具体取决于与其交换数据的客户端。

以下细分表格显示启用了各选项的连接。

选项	启用的功能	客户端位置	使用的功能
选项 1	如果已启用 NAT-T	并且客户端位于 NAT 后面，则	使用 NAT-T
		并且如果没有 NAT，则	使用本地 IPsec (ESP)
选项 2	如果已启用 IPsec over UDP	并且客户端位于 NAT 后面，则	使用 IPsec over UDP
		并且如果没有 NAT，则	使用 IPsec over UDP
选项 3	如果 NAT-T 和 IPsec over UDP 都已启用	并且客户端位于 NAT 后面，则	使用 NAT-T
		并且如果没有 NAT，则	使用 IPsec over UDP

注释 IPsec over TCP 启用时，它将优先于所有其他连接方法。

当您启用 NAT-T 时， ASA 将在所有启用 IPsec 的接口上自动打开端口 4500。

ASA 支持在 LAN 间访问网络或远程访问网络中运行（但不能同时在这两种网络中运行）的一台 NAT/PAT 设备后面部署多个 IPsec 对等体。在混合环境中，远程访问隧道将协商失败，因为所有对等体都显示来自相同的公用 IP 地址，即 NAT 设备的地址。此外，远程访问隧道在混合环境中失败的原因还包括它们通常使用和 LAN 间隧道组相同的名称（也就是 NAT 设备的 IP 地址）。这种一致性会导致在 NAT 设备后面的 LAN 间和远程访问混合网络中多个对等体之间协商失败。

如要使用 NAT-T，请在单情景或多情景模式下执行以下站点间步骤：

过程

步骤 1 输入以下命令，在 ASA 上全局启用 IPsec over NAT-T：

crypto isakmp nat-traversal *natkeepalive*

其中 natkeepalive 参数的取值范围是 10 至 3600 秒。默认值为 20 秒。

示例：

输入以下命令将启用 NAT-T 并将其生命周期值设置为一小时：

```
hostname(config)# crypto isakmp nat-traversal 3600
```

步骤 2 通过输入以下命令为 IPsec 分片策略选择加密前选项：

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。

启用 IPsec with IKEv1 over TCP

IPsec over TCP将 IKEv1 和 IPSec 协议同时封装在类 TCP 数据包内，并支持同时穿过 NAT 与 PAT 设备和防火墙的安全隧道。默认情况下会禁用此功能。对于标准 ESP 或 IKEv1 在其中无法工作，或者仅在修改现有防火墙规则的情况下才能工作的环境，IPsec/IKEv1 over TCP 使得思科 VPN 客户端可以在此环境中运行。

注释 此功能不能与基于代理的防火墙配合使用。

IPsec over TCP 可与远程访问客户端配合使用。您可以同时在 ASA 及其连接的客户端上启用 IPsec over TCP。它在 ASA 上全局启用，用于所有启用 IKEv1 的接口。它不适用于 LAN 间连接。

ASA 可同时支持标准 IPsec、IPsec over TCP、NAT 遍历和 IPsec over UDP，具体取决于与其交换数据的客户端。IPsec over TCP 启用时优先于所有其他连接方法。

您可以为您指定的最多 10 个端口启用 IPsec over TCP。如果您输入一个已知端口，例如端口 80 (HTTP) 或端口 443 (HTTPS)，系统会显示一条警告，指示与该端口关联的协议将不再用于公共接口。其结果是，您无法再使用浏览器通过公共接口管理 ASA。要解决此问题，请将 HTTP/HTTPS 管理重新配置到不同的端口。

默认端口为 10000。

您必须在客户端以及 ASA 上配置 TCP 端口。客户端配置必须包含至少一个您为 ASA 设置的端口。

要在 ASA 上为 IKEv1 全局启用 IPsec over TCP，请在单情景或多情景模式下执行以下命令：

crypto ikev1 ipsec-over-tcp [port *port 1...port0]*

本示例在端口 45 上启用 IPsec over TCP：

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

为 IKEv1 配置证书组匹配

隧道组定义用户连接条件和权限。证书组匹配允许使用用户证书的使用者 DN 或颁发者 DN 将用户与隧道组进行匹配。

注释 证书组匹配仅适用于 IKEv1 和 IKEv2 LAN 间连接。IKEv2 远程访问连接支持在隧道组的 webvpn 属性中以及在 certificate-group-map 的 webvpn 配置模式下配置的下拉组选择。

要根据证书的这些字段将用户与隧道组匹配，必须先创建定义匹配条件的规则，然后将每个规则与所需的隧道组匹配。

要创建证书映射，请使用 **use the crypto ca certificate map** 命令。要定义隧道组，请使用 tunnel-group 命令。

您还必须配置证书组匹配策略，指定从规则或从组织单位 (OU) 字段匹配组，或指定为所有证书用户使用默认组。可以使用其中任意或所有方法。

过程

步骤 1 要配置基于证书的 ISAKMP 会话向隧道组映射所遵循的策略和规则并将证书映射条目与隧道组关联，请在单情景或多情景模式下输入 tunnel-group-map 命令。

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

policy	指定用于从证书获取隧道组名称的策略。Policy 可以是以下某一项： *ike-id* - 指示如果无法根据规则查找确定隧道组或采用来自 OU 的隧道组，则基于证书的 ISAKMP 会话将根据阶段 1 ISAKMP ID 的内容映射到隧道组。 *ou* - 指示如果无法根据规则查找确定隧道组，则使用主题可分辨名称 (DN) 中 OU 的值。 *peer-ip* - 指示如果无法根据规则查找确定隧道组或采用来自 OU 的隧道组或 ike-id 方法，则使用对等体 IP 地址。 *rules* - 指示根据此命令所配置的证书映射关联，将基于证书的 ISAKMP 会话映射到隧道组。
rule index	（可选）指 **crypto ca certificate map** 命令指定的参数。有效值为 1 到 65535。

请注意下列说明：

- 您可以多次调用此命令，前提是每次调用都是唯一的，并且不多次引用映射索引。
- 规则不能超过 255 个字符。
- 您可以将多个规则分配给同一组。为此，您首先要添加规则优先级和组。然后，为每个组定义所需数量的条件语句。当将多个规则分配给同一组时，将为测试为真的第一条规则生成匹配项。
- 通过创建一条规则，您可以要求将用户分配给特定隧道组之前匹配所有条件。要求匹配所有条件等同于逻辑和运算。或者，如果要在将用户分配给特定隧道组之前要求只匹配一个条件，请为每个条件创建一条规则。要求只匹配一个条件等同于逻辑或运算。

步骤 2 指定当配置未指定隧道组时要使用的默认隧道组。

其语法为 **tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* ，其中 *rule-index* 是规则的优先级，并且 tunnel-group name 必须用于现有的隧道组。

示例

以下示例启用根据阶段 1 ISAKMP ID 的内容将基于证书的 ISAKMP 会话映射到隧道组：

```
hostname(config)# tunnel-group-map enable ike-id
```

以下示例启用根据对等体的 IP 地址将基于证书的 ISAKMP 会话映射到隧道组：

```
hostname(config)# tunnel-group-map enable peer-ip
```

以下示例启用根据使用者可分辨名称 (DN) 中的组织单位 (OU) 映射基于证书的 ISAKMP 会话：

```
hostname(config)# tunnel-group-map enable ou
```

以下示例启用根据既定规则映射基于证书的 ISAKMP 会话：

```
hostname(config)# tunnel-group-map enable rules
```

配置 IPsec

本节介绍使用 IPsec 实施 VPN 时配置 ASA 所需执行的程序。

定义加密映射

加密映射定义在 IPsec SA 中协商的 IPSec 策略。其包括以下内容：

- 确定 IPSec 连接允许和保护的数据包的 ACL。
- 对等体标识。
- IPSec 流量的本地地址。（有关详细信息，请参阅将加密映射应用于接口 ，第 26 页。）
- 最多 11 个 IKEv1 转换集或 IKEv2 提议，用于尝试与对等体安全设置进行匹配。

一个加密映射集包括一个或多个具有相同映射名称的加密映射。在创建第一个加密映射时，就要创建加密映射集。以下站点间任务将在单情景或多情景模式下创建或添加加密映射：

crypto map *map-name seq-num* **match address** *access-list-name*

使用 access-list-name 指定 ACL ID，即长度最多为 241 个字符的字符串或整数。

提示 使用全部为大写的字母可以更轻松地在您的配置中标识 ACL ID。

您可以继续输入此命令，向加密映射集添加加密映射。在以下示例中，*mymap* 是您可能想要添加加密映射的加密映射集的名称。

crypto map mymap 10 match address 101

上面语法中显示的序号 (*seq-num*) 将具有相同名称的加密映射相互区分开。分配给加密映射的序号还决定着同一个加密映射集中该加密映射相较于其他加密映射的优先级。序号越小，优先级就越高。在您将加密映射集分配给接口之后， ASA 将按照此映射集中的加密映射评估通过该接口的所有 IP 流量，从序号最小的加密映射开始。

[no] crypto map *map_name map_index* **set pfs [group14 | group15 | group16 | group19 | group20 | group21]**

指定用于加密映射完全向前保密 (PFS) 的 ECDH 组。防止您为加密映射配置组 14 和组 24 选项（使用 IKEv1 策略时）。

[no] crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

根据此加密映射条目为任何连接启用反向路由注入 (RRI)。如果未指定为动态，则 RRI 在配置时完成并被视为静态，在配置更改或被删除之前保持不变。此外，只要为 RRI 路由配置了已存在静态路由的相同目标，现有的静态路由就会被丢弃并安装 RRI 路由。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。

如果指定为动态，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除路由。

不能使用与静态加密映射相同的名称来配置动态加密映射，反之亦然，即使其中一个加密映射实际上并未被使用。

注释 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

[no] crypto map *name priority* **set validate-icmp-errors**

或

[**no**]**crypto dynamic-map** *name priority* **set validate-icmp-errors**

指定是否为加密或动态加密映射验证传入的 ICMP 错误消息。

[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}

或

[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]

为加密或动态加密映射配置现有的不分片 (DF) 策略（安全关联级别）。

- *clear-df*—Ignores the DF bit.
- *copy-df* — 保持 DF 位。

- *set-df* — 设置和使用 DF 位。

[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

或

[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

管理员可以按照任意长度和间隔对 IPsec 安全关联启用虚拟流量机密性 (TFC) 数据包。您必须在启用 TFC 之前设置 IKEv2 IPsec 提议。

注释 启用流量保密性数据包可防止 VPN 空闲超时。

分配给加密映射的 ACL 包括具有相同 ACL 名称的所有 ACE，如以下命令语法所示：

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

在创建第一个 ACE 时就要创建 ACL。以下命令语法将创建或添加 ACL：

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

在以下示例中，ASA 对从 10.0.0.0 子网流向 10.1.1.0 子网的所有流量应用分配给加密映射的 IPSec 保护：

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

匹配数据包的加密映射确定用于 SA 协商的安全设置。如果本地 ASA 发起协商，它将使用静态加密映射中指定的策略创建发送到指定对等体的提议。如果对等体发起协商，ASA 会尝试将策略与静态加密映射匹配，如果匹配失败，则尝试匹配加密映射集中的任意动态加密映射，从而决定是接受还是拒绝对等体提议。

要使两个对等体成功建立SA，它们必须至少有一个兼容的加密映射。要兼容，加密映射必须符合以下条件：

- 加密映射必须包含兼容的加密 ACL（例如，镜像 ACL）。如果对应的对等体使用动态加密映射，则 ASA 还必须包含兼容的加密 ACL 才能应用 IPsec。
- 每个加密映射将标识另一个对等体（除非对应的对等体使用动态加密映射）。
- 加密映射至少有一个共同的转换集或提议。

一个接口只能应用一个加密映射集。如果存在以下任意情况，则在ASA上为特定接口创建多个加密映射：

- 您想让特定对等体处理不同的数据流。
- 您想要将不同的 IPSec 安全应用于不同类型的流量。

例如，创建一个加密映射并分配一个标识两个子网之间流量的 ACL，然后分配一个 IKEv1 转换集或 IKEv2 提议。创建另一个使用不同 ACL 标识另外两个子网之间流量的加密映射，并应用包含不同 VPN 参数的转换集或提议。

如果要为某个接口创建多个加密映射，请为每个映射条目指定一个确定其在加密映射集内优先级的序号 (seq-num)。

每个 ACE 包含一个 permit 或 deny 语句。下表解释应用于加密映射的 ACL 中 permit 和 deny ACE 的特殊含义。

加密映射评估结果	解决方案
匹配 ACE 中包含 permit 语句的条件	停止按照加密映射集中剩余的ACE对数据包进行进一步分析，而按照分配给该加密映射的IKEv1 转换集或IKEv2 提议中的数据包设置评估数据包安全设置。将这些安全设置与转换集或提议中的设置进行匹配之后，ASA 将应用关联的 IPsec 设置。通常对于出站流量，这意味着对数据包进行解密、身份验证和路由。
匹配 ACE 中包含 deny 语句的条件	中断按照正在评估的加密映射中剩余的 ACE 对数据包进行进一步分析，而按照下一个加密映射（具体由分配给它的下一个序号决定）中的 ACE 继续进行评估。
无法匹配加密映射集中所有受测试的 permit ACE	路由数据包，而不对其进行加密。

包含 deny 语句的 ACE 过滤掉不需要 IPSec 保护的出站流量（例如，路由协议流量）。因此，请插入初始 deny 语句来过滤不应该按照加密 ACL 中的 permit 语句进行评估的出站流量。

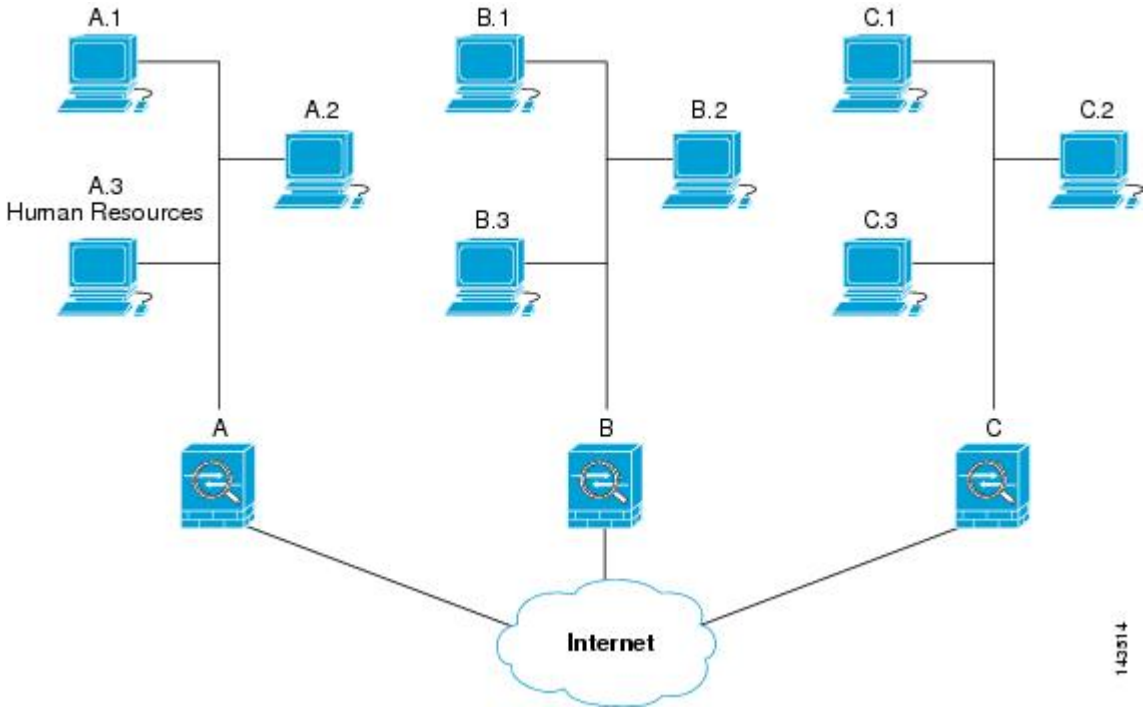
对于入站加密数据包，安全设备使用源地址和 ESP SPI 确定解密参数。安全设备解密数据包后，会将解密的数据包的内部报头与和数据包 SA 关联的 ACL 中的 permit ACE 进行比较。如果内部报头无法与代理匹配，安全设备将丢弃该数据包。如果内部报头与代理匹配，安全设备则会路由该数据包。

在比较未加密入站数据包的内部报头时，安全设备将忽略所有拒绝规则，因为它们会阻止阶段 2 SA 的建立。

注释 要将未加密的入站流量作为明文路由，请在 permit ACE 之前插入 deny ACE。ASA 在分割隧道访问列表中推送的 ACE 不能超过 28 个。

LAN 间加密映射示例

以下LAN 间网络示例中配置安全设备 A、B 和 C 的目的是允许通过隧道传送来自其中一个主机并且以其余主机中另一个主机作为目标的所有流量。但是，因为主机 A.3 的流量包含来自人力资源部门的敏感数据，所以这些流量要求采用强加密并比其他流量更频繁地重新生成密钥。因此，您需要为来自主机 A.3 的流量分配一个专用转换集。



上图中显示的和以下说明中使用的简单地址表示为假想地址。说明后面使用的是带有真实 IP 地址的示例。

要为出站流量配置安全设备 A，您要创建两个加密映射，一个用于来自主机 A.3 的流量，另一个用于来自网络 A 中其他主机的流量，如以下示例所示：

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

创建 ACL 之后，您要为每个加密映射分配一个转换集，向每个匹配的数据包应用所要求的 IPsec。

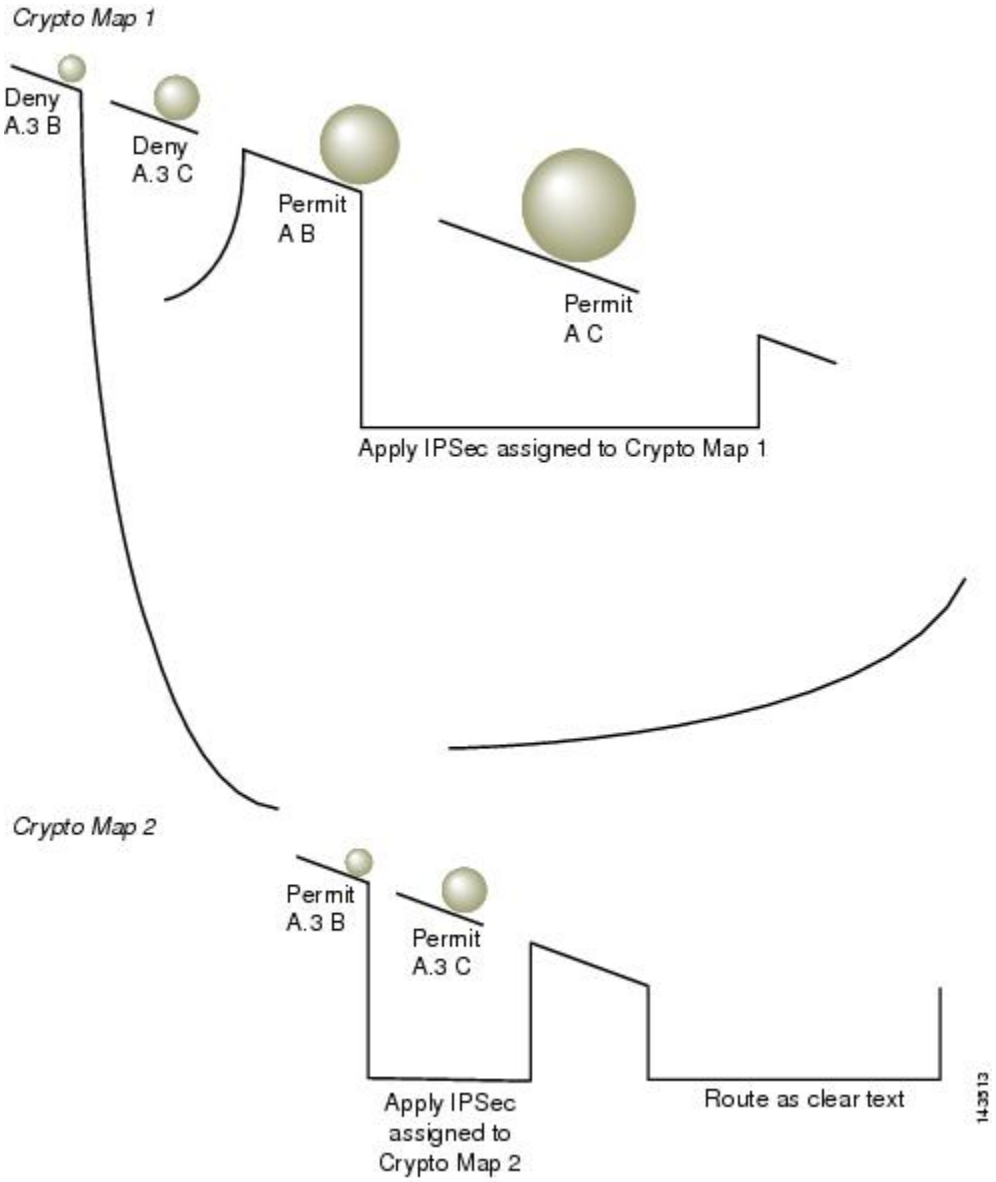
级联 ACL 涉及插入 deny ACE 以绕过按照某个 ACL 进行的评估，而按照加密映射集中的后续 ACL 继续进行评估。由于您可以将每个加密映射与不同的 IPsec 设置关联，因此您可以使用 deny ACE 将特定流量从相应加密映射中的进一步评估中排除，并且将特定流量与另一个加密映射中的 permit 语句匹配以提供或要求提供不同的安全保护。分配给加密 ACL 的序号确定其在加密映射集内评估序列中的位置。

下图显示从本示例中的概念性 ACE 创建的级联 ACL。每个符号的含义定义如下：

	加密映射集中的加密映射。
	（直线上的缺口）当数据包与 ACE 匹配时退出加密映射。

	符合一个 ACE 描述的数据包。各种尺寸的球表示与图中各个 ACE 匹配的不同数据包。尺寸的区别只代表每个数据包的源和目标的差异。
	重定向至加密映射集中的下一个加密映射。
	当数据包与 ACE 匹配或无法匹配加密映射集中的所有 permit ACE 时，做出响应。

图 *2:* 加密映射集中的级联 ***ACL***



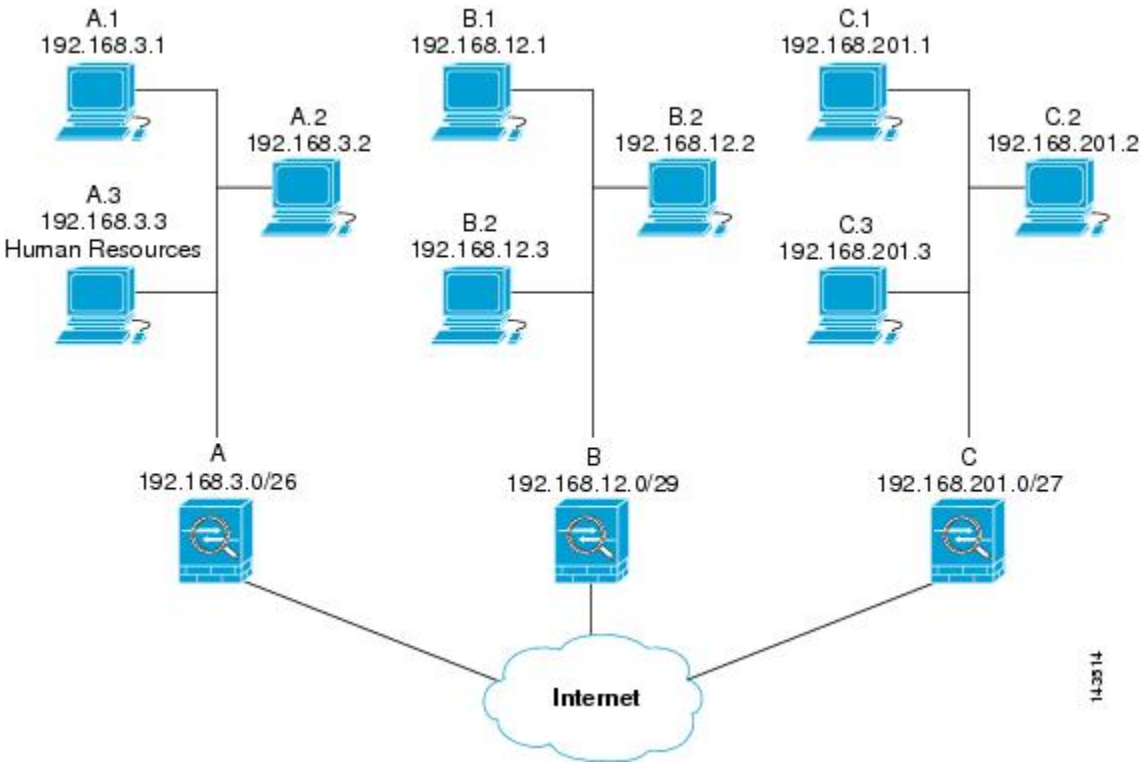
安全设备 A 评估源自主机 A.3 的数据包，直到与某个 permit ACE 匹配，然后尝试分配与加密映射关联的 IPSec 安全。但凡数据包与某个 deny ACE 匹配，ASA 将忽略加密映射中剩余的 ACE，然后按照下一个加密映射（具体由分配给它的序号决定）继续进行评估。因此在本示例中，如果安全设备 A 收到来自主机 A.3 的数据包，它会将数据包与第一个加密映射中的 deny ACE 匹配，然后按照下一个加密映射继续评估数据包。当它将数据包与该加密映射中的 permit ACE 匹配时，它会应用关联的 IPSec 安全（强加密和频繁地重新生成密钥）。

为了完成示例网络中的 ASA 配置，我们将镜像加密映射分配到 ASA B 和 C。但是，因为 ASA 在评估加密的入站流量时会忽略 deny ACE，所以我们可以忽略 deny A.3 B 和 deny A.3 C ACE 的等效镜像，并且因而忽略加密映射 2 的等效镜像。因此，没有必要在 ASA B 和 C 上配置级联 ACL。

下表显示分配给为所有三个 ASA（A、B 和 C）配置的加密映射的 ACL：

安全设备 A		**安全设备 B**		**安全设备 C**	
加密映射序号	**ACE 模式**	加密映射序号	**ACE 模式**	加密映射序号	**ACE 模式**
1	deny A.3 B	1	permit B A	1	permit C A
	deny A.3 C				
	permit A B				
	permit A C		permit B C		permit C B
2	permit A.3 B				
	permit A.3 C				

下图将此前显示的概念性地址映射至真实 IP 地址。



下表中显示的真实 ACE 可确保此网络内接受评估的所有 IPsec 数据包都获得正确的 IPsec 设置

安全设备	加密映射序号	ACE 模式	真实 ACE
A	1	deny A.3 B	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		deny A.3 C	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		permit A B	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		permit A C	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.22
	2	permit A.3 B	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		permit A.3 C	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.22
B	不需要	permit B A	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		permit B C	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.2
C	不需要	permit C A	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.19
		permit C B	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.2

您可以应用示例网络中所示的推理，通过使用级联 ACL 将不同安全设置分配给受 ASA 保护的不同主机或子网。

注释 默认情况下，ASA 不支持目的地与其所进入的接口相同的 IPsec 流量。这种类型流量的名称包括 U-turn、hub-and-spoke 和 hairpinning。但是，您可以插入允许流量往返网络的 ACE，从而将 IPsec 配置为支持 U-turn 流量。例如，要在安全设备 B 上支持 U-turn 流量，请将概念性“permit B B”ACE 添加到 ACL1 中。实际 ACE 如下所示：**permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

设置公钥基础设施 (PKI) 密钥

您必须设置公钥基础设施 (PKI)，管理员才可以在生成或归零密钥对时选择 Suite B ECDSA 算法：

开始之前

如果将加密映射配置为使用 RSA 或 ECDSA 信任点进行身份验证，您首先必须生成密钥集。然后您可以创建信任点并在隧道组配置中引用它。

过程

步骤 1 在生成密钥对时选择 Suite B ECDSA 算法：

crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]

步骤 2 在归零密钥对时选择 Suite B ECDSA 算法：

crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]

将加密映射应用于接口

您必须为 IPSec 流量经过的每个接口分配加密映射集。ASA 在所有接口上都支持 IPsec。向接口分配加密映射集将命令 ASA 按照该加密映射集评估所有流量并在连接或 SA 协商期间使用指定的策略。

将加密映射分配给接口还将初始化运行时数据结构，例如 SA 数据库和安全策略数据库。将修改过的加密映射重新分配给该接口会将运行时数据结构与加密映射配置重新同步。此外，通过使用新序号添加新的对等体和重新分配加密映射不会中断现有连接。

使用接口 ACL

默认情况下，ASA 允许 IPSec 数据包绕过接口 ACL。如果要将接口 ACL 应用于 IPsec 流量，请使用 **no** 形式的 **sysopt connection permit-vpn** 命令。

与传出接口绑定的加密映射 ACL 将允许或拒绝 IPSec 数据包通过 VPN 隧道。IPsec 对从 IPSec 隧道到达的数据包进行身份验证和解密，并使其按照与隧道关联的 ACL 接受评估。

ACL 定义要保护的 IP 流量。例如，您可以创建 ACL 以保护两个子网或两台主机之间的所有 IP 流量。（这些 ACL 类似于用于 **access-group** 命令的 ACL。但是，用于 **access-group** 命令时，ACL 确定在接口上转发或阻止哪些流量。）

在分配给加密映射之前，ACL 不特定于 IPsec。每个加密映射都引用 ACL，如果某数据包与其中一个 ACL 中的 permit 匹配，则加密映射还确定应用于此数据包的 IPSec 属性。

分配给 IPsec 加密映射的 ACL 有四个主要功能：

- 选择 IPsec 将保护的出站流量（允许 = 保护）。
- 为在没有建立 SA 的情况下进行的数据传送触发 ISAKMP 协商。
- 处理入站流量，以便过滤出并丢弃原本应受 IPsec 保护的流量。
- 在处理来自对等体的 IKE 协商时，确定是否接受对于 IPSec SA 的请求。（协商仅适用于 **ipsec-isakmp crypto map** 条目。）对等体必须允许与 **ipsec-isakmp crypto map** 命令条目关联的数据流，才能确保在协商期间被接受。

注释 如果删除 ACL 中的唯一元素，ASA 也将删除关联的加密映射。

如果修改一个或多个加密映射当前引用的 ACL，请使用 **crypto map interface** 命令重新初始化运行时 SA 数据库。有关详细信息，请参阅 **crypto map** 命令。

对于您在本地对等体上定义的静态加密映射的每个指定加密 ACL，我们建议您在远程对等体上定义一个“镜像”加密 ACL。加密映射还应支持共同的转换并将其他系统称为对等体。这将确保两个对等体正确处理 IPsec。

注释 每个静态加密映射必须定义一个 ACL 和一个 IPSec 对等体。如果任何一个缺失，加密映射都不完整并且 ASA 将丢弃尚未与之前的完整加密映射匹配的任何流量。使用 **show conf** 命令确保每个加密映射都是完整的。要修复某个不完整的加密映射，请删除该加密映射，添加缺少的条目，然后重新应用它。

加密 ACL 不支持重复或重叠的条目。

我们建议不要使用 **any** 关键字在加密 ACL 中指定源或目标地址，因为会造成一些问题。我们强烈建议不要使用 **permit any any** 命令语句，因为它会执行以下操作：

- 保护所有出站流量，包括发送到相应的加密映射中指定对等体的所有受保护流量。
- 要求保护所有入站流量。

在这种情况下，ASA 将自动丢弃缺少 IPSec 保护的所有入站数据包。

确保定义要保护哪些数据包。如果将 **any** 关键字用于 **permit** 语句，请在其前面加上一系列 **deny** 语句来过滤掉您不想要保护的流量，否则其将进入 **permit** 语句。

注释 配置了 **no sysopt connection permit-vpn** 时，尽管在外部接口上有访问组（调用 deny ip any any access-list），系统仍会允许来自客户端的解密直通流量。

如果用户想要使用 **no sysopt permit** 命令结合外部接口上的访问控制列表 (ACL) 来控制通过站点间或远程访问 VPN 对受保护网络进行的访问，则无法成功进行控制。

在这种情况下，启用管理访问内部接口时，不应用ACL，用户仍然可以使用SSH连接到安全设备。流向内部网络上的主机的流量将被ACL正确地阻拦，但是无法阻止流向内部接口的解密直通流量。

ssh 和 **http** 命令具有比 ACL 更高的优先级。换句话说，要拒绝从 VPN 会话流向设备的 SSH、Telnet 或 ICMP 流量，应使用 **ssh**、**telnet** 和 **icmp** 命令，这些命令将拒绝应该添加的本地 IP 池。

不管流量是入站还是出站流量，ASA 都将按照分配给接口的 ACL 评估流量。按照以下步骤将 IPsec 分配到接口上：

过程

步骤 1 创建用于 Ipsec 的 ACL。

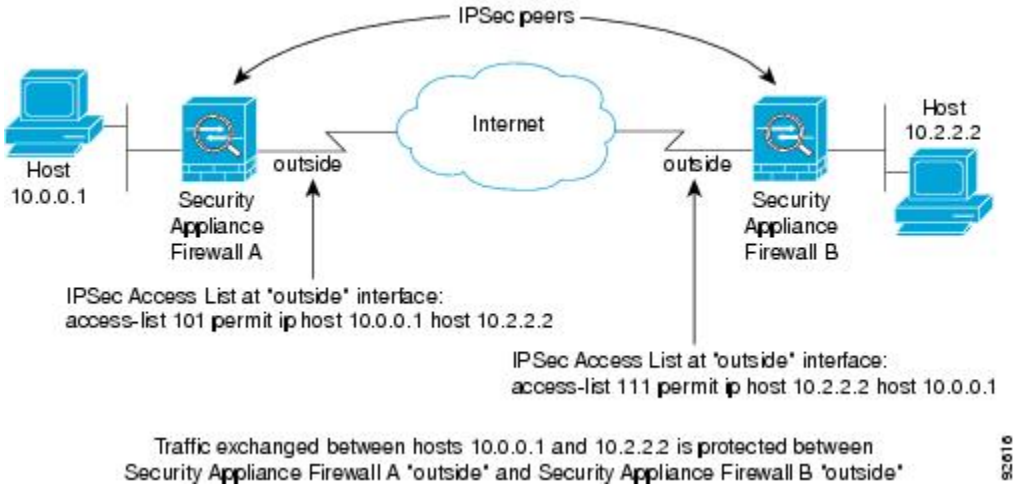
步骤 2 将列表映射到一个或多个使用同一个加密映射名称的加密映射。

步骤 3 将 IKEv1 转换集或 IKEv2 提议映射到加密映射，从而向数据流应用 IPsec。

步骤 4 通过将加密映射共用的加密映射名称分配到接口，以加密映射集的形式应用全部加密映射。

示例

在本示例中，数据退出 ASA A 上的外部接口，流向主机 10.2.2.2 时，IPsec 保护将应用于主机 10.0.0.1 和主机 10.2.2.2 之间的流量。



ASA A 评估从主机 10.0.0.1 到主机 10.2.2.2 的流量，如下所示：

- 源 = 主机 10.0.0.1
- 目标 = 主机 10.2.2.2

ASA A 也评估从主机 10.2.2.2 到主机 10.0.0.1 的流量，如下所示：

- 源 = 主机 10.2.2.2
- 目标 = 主机 10.0.0.1

与接受评估的数据包匹配的第一条 permit 语句确定 IPsec SA 的范围。

更改 IPsec SA 生命周期

协商新的 IPsec SA 时，您可以更改 ASA 使用的全局生命周期值。您可以为特定加密映射覆盖这些全局生命周期值。

IPSec SA 使用派生的共享密钥。密钥是 SA 的组成部分；密钥一起超时就要求刷新密钥。每个 SA 都有两个生命周期：计时生命周期和流量生命周期。SA 将在各个生命周期之后到期，然后对等体将开始协商新的 SA。默认生命周期是 28,800 秒（八小时）和 4,608,000 千字节（一个小时内每秒钟 10 兆字节）。

如果您更改全局生命周期，ASA 将丢弃隧道。它将在随后建立 SA 的协商中使用新值。

如果加密映射没有配置生命周期值并且 ASA 请求使用新的 SA，它会将现有 SA 中使用的全局生命周期值插入到发送至对等体的请求中。当对等体收到协商请求时，它会使用对等体提议的生命周期值和本地配置的生命周期值这二者中较小的值作为新 SA 的生命周期。

对等体将在超出现有 SA 的生命周期阈值之前协商一个新 SA，确保在现有 SA 过期时已经准备好新 SA。当现有 SA 剩余生命周期只有大约 5% 至 15% 时，对等体将协商一个新的 SA。

注释 我们建议您在站点间 IKEv2 隧道的任一端配置不同的安全关联计时器，以避免重新生成密钥冲突。

更改 VPN 路由

默认情况下，按数据包邻接关系查找针对外部 ESP 数据包执行；不会对通过 IPsec 隧道发送的数据包执行查找。

在某些网络拓扑中，路由更新更改了内部数据包的路径，但本地 IPsec 隧道仍正常运行时，通过隧道的数据包可能无法正确路由，且无法到达其目的地。

要避免此情况，请对 IPsec 内部数据包启用按数据包路由查找功能。

开始之前

为避免这些查找产生任何性能影响，默认情况下禁用此功能。此功能仅在需要时启用。

过程

请对 IPsec 内部数据包启用按数据包路由查找功能。

[**no**] [**crypto**] **ipsec inner-routing-lookup**

注释 此命令在配置后仅适用于非 VTI 隧道。

示例

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

创建静态加密映射

要使用静态加密映射创建基本 IPSec 配置，请执行以下步骤：

过程

步骤 1 要创建 ACL 以定义要保护的流量，请输入以下命令：

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

其中 *access-list-name* 指定 ACL ID，即一个最长为 241 个字符的字符串或整数。*destination-netmask* 和 *source-netmask* 指定 IPv4 网络地址和子网掩码。在本例中，**permit** 关键字将使匹配指定条件的所有流量受加密保护。

示例：

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

步骤 2 要配置定义如何保护流量的 IKEv1 转换集，请输入以下命令：

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

Encryption 指定使用哪个加密方法保护 IPsec 数据流：

- esp-aes — 使用带 128 位密钥的 AES。
- esp-aes-192 — 使用带 192 位密钥的 AES。
- esp-aes-256 — 使用带 256 位密钥的 AES。\
- esp-null — 不加密。

Authentication 指定使用哪个加密方法保护 IPsec 数据流。

- esp-sha-hmac — 使用 SHA/HMAC-160 作为散列算法。
- esp-none — 不进行 HMAC 身份验证。

示例：

在本示例中，myset1 和 myset2 以及 aes_set 是转换集的名称。

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-aes esp-sha-hmac
hostname(config)#
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

步骤 3 要配置同时定义如何保护流量的 IKEv2 提议，请输入以下命令：

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

proposal tag 是 IKEv2 IPsec 提议的名称，即一个 1 至 64 个字符的字符串。

创建提议，然后进入 ipsec 提议配置模式，在此模式下可以为提议指定多个加密和完整性类型。

示例：

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

在本例中，secure 是提议的名称。输入协议和加密类型：

```
hostname(config-ipsec-proposal)# protocol esp encryption aes
```

示例：

此命令用于选择是使用 AES-GCM 算法还是 AES-GMAC 算法：

[**no**] **protocol esp encryption** [**aes| aes-192 | aes-256 | aes-gcm| aes-gcm-192 | aes-gcm-256| null]**

如果选择 SHA-2 或 null，则必须选择使用哪个算法作为 IPsec 完整性算法。如果将 AES-GCM/GMAC 配置为加密算法，则必须选择 null 完整性算法：

[**no**] **protocol esp integrity** [**sha-1** | **sha-256** | **sha-384** | **sha-512** | **null**]

注释　如果已将 AES-GCM/GMAC 配置为加密算法，则必须选择 null 完整性算法：可以将 SHA-256 用于完整性和 PRF 以建立 IKEv2 隧道，但是也可以将其用于 ESP 完整性保护。

步骤 4　（可选）管理员可以启用路径最大传输单元 (PMTU) 老化并设置将 PMTU 值重置为其原始值的时间间隔。

[**no**] **crypto ipsec security-association pmtu-aging** *reset-interval*

步骤 5　要创建加密映射，请使用单情景或多情景模式执行以下站点间步骤：

a) 将 ACL 分配到加密映射：

crypto map *map-name seq-num* **match address** *access-list-name*

加密映射集是一系列加密映射条目，每个条目使用不同的序号 (*seq-num)*，但使用相同的映射名称。使用 *access-list-name* 指定 ACL ID，即长度最多为 241 个字符的字符串或整数。在以下示例中，mymap 是加密映射集的名称。此映射集序号为 10，此序号用于排列一个加密映射集内多个条目的优先级。序号越小，优先级就越高。

示例：

在本示例中，名称为 101 的 ACL 将分配给加密映射 mymap。

```
crypto map mymap 10 match address 101
```

b) 指定可以向其转发受 IPSec 保护的流量的对等体：

crypto map *map_name sequence number***set peer** *ip_address1 [ip_address2] [...]*

示例：

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA 设置 SA，其中对等体分配的 IP 地址为 192.168.1.100。

注释　从 9.14(1) 开始，ASA 支持 IKEv2 加密映射中的多个对等体。您最多可以向列表中添加 10 个对等体。

c) 指定此加密映射允许哪些 IKEv1 转换集或 IKEv2 提议。按照优先级顺序列出多个转换集或提议（优先级高的优先）。您可以使用以下两个命令之一，在加密映射中最多指定 11 个转换集或提议：

crypto map *map-name seq-num* **set ikev1 transform-set** *transform-set-name1 [transform-set-name2, …transform-set-name11*]

或

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

Proposal-name1 和 *proposal-name11* 指定用于 IKEv2 的一个或多个 IPsec 提议名称。每个加密映射条目支持最多 11 个提议。

示例：

在 IKEv1 的本示例中，流量与 ACL 101 匹配时，SA 可以使用 myset1（第一优先级）或 myset2（第二优先级），具体取决于哪个转换集与对等体的转换集匹配。

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

d) （可选）对于 IKEv2，请指定将 ESP 加密和身份验证应用于隧道的**mode**。此字段确定原始 IP 数据包的哪个部分已应用 ESP。

crypto map *map-name seq-num* **set ikev2 mode** [**transport | tunnel | transport-require**]

- **隧道模式** -（默认）封装模式将为隧道模式。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），从而隐藏最终的源地址和目的地址。整个原始 IP 数据报经过加密，成为新 IP 数据包中的负载。

  此模式允许路由器等网络设备用作 IPsec 代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。

  隧道模式的主要优势是不需要修改终端系统即可获得 IPsec 的优势。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

- **传输模式** - 封装模式将为传输模式，且可选择在对等体不支持时回退到隧道模式。在传输模式下，仅加密 IP 负载，原始 IP 报头保持不变。

  此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。

- **传输必要** - 封装模式将为仅传输模式，不允许回退到隧道模式。

其中，**tunnel**封装模式是默认模式；**transport**封装模式是传输模式，如果对等体不支持，可以回退到隧道模式；**transport-require**封装模式仅实施传输模式。

注释 不建议将传输模式用于远程访问 VPN。

例如，封装模式的协商如下所示：

- 如果发起方提议传输模式而响应方以隧道模式响应，发起人将回退到隧道模式。
- 如果发起方提议隧道模式而响应方以传输模式响应，响应方不会回退到隧道模式。
- 如果发起方提议隧道模式而响应方为传输必要模式，则响应方将发送“没有选择提议”。
- 同样，如果发起方为传输必要模式而响应方为隧道模式，响应方将发送“没有选择建议”。

e) （可选）如果想要覆盖全局生命周期，请为加密映射指定 SA 生命周期。

crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

Map-name 指定加密映射集的名称。*Seq-num* 指定您分配给加密映射条目的序号。您可以基于时间或传输的数据设置两个生命周期。但是，所传输数据的生命周期仅适用于站点间 VPN，不适用于远程访问 VPN。

示例：

此示例将加密映射 mymap 10 的计时生命周期缩短至 2700 秒（45 分钟）。基于流量的生命周期未更改。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

f) （可选）指定在为此加密映射请求新的 SA 时 IPsec 要求完全向前保密，或在从对等体接收的请求中要求 PFS：

crypto map *map_name seq-num* **set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]

示例：

此示例要求在为加密映射 mymap 10 协商新 SA 时提供 PFS。ASA 在新 SA 中使用 2048 位 Diffie-Hellman 素数模数群。

```
crypto map mymap 10 set pfs group14
```

g) （可选）根据此加密映射条目为任何连接启用反向路由注入 (RRI)。

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

如果未指定为动态，则 RRI 在配置时完成并被视为静态，在配置更改或被删除之前保持不变。ASA 可自动将静态路由添加到路由表中，并向其使用 OSPF 的专用网络或边界路由器通告这些路由。如果将任何源/目标 (0.0.0.0/0.0.0.0) 指定为受保护网络，请勿启用 RRI，否则会影响使用默认路由的流量。

如果指定为动态，则在成功建立 IPsec 安全关联 (SA) 时创建 RRI 并在删除 IPsec SA 后删除路由。

注释　　动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

示例：

```
crypto map mymap 10 set reverse-route dynamic
```

步骤 6 将加密映射集应用于评估 IPSec 流量的接口：

crypto map *map-name* **interface** *interface-name*

Map-name 指定加密映射集的名称。*Interface-name* 指定要在其上启用或禁用 ISAKMP IKEv1 协商的接口的名称。

示例：

在本示例中，ASA 按照加密映射 mymap 评估通过外部接口的流量，确定其是否需要保护。

```
crypto map mymap interface outside
```

创建动态加密映射

动态加密映射是未配置任何参数的加密映射。该映射可作为一个策略模板，其中缺失的参数将在以后根据 IPsec 协商的结果动态获取，以匹配对等体要求。如果尚未在静态加密映射中确定对等体的 IP 地址，ASA 将应用动态加密映射以便对等体协商隧道。这种情况发生于以下类型的对等体中：

- 具有动态分配的公用 IP 地址的对等体。

  LAN 间和远程访问对等体都可以使用 DHCP 获取公用 IP 地址。ASA 只使用此地址启动隧道。

- 具有动态分配的专用 IP 地址的对等体。

  请求远程访问隧道的对等体通常具有由头端分配的专用IP地址。通常，LAN间隧道具有预定的专用网络集，用于配置静态映射，进而用于建立 IPsec SA。

作为配置静态加密映射的管理员，您可能不知道动态分配的IP地址（通过DHCP或其他方法），而且您可能不知道其他客户端的专用 IP 地址（无论它们如何分配）。VPN 客户端通常没有静态 IP 地址；这些客户端需要动态加密映射来支持 IPsec 协商。例如，头端在 IKE 协商期间向思科 VPN 客户端分配 IP 地址，然后客户端使用该 IP 地址来协商 IPSec SA。

注释 动态加密映射只需要 **transform-set** 参数。

动态加密映射可以简化 IPSec 配置，我们建议在并非总是能够预先确定对等体的网络中使用动态加密映射。对于思科 VPN 客户端（例如移动用户）和获取动态分配的 IP 地址的路由器，请使用动态加密映射。

提示 在动态加密映射中将 **any** 关键字用于 **permit** 条目时，请小心。如果此 **permit** 条目包含的流量可能包含组播或广播流量，请将适用于相应地址范围的 **deny** 条目插入 ACL 中。记住为网络和子网广播流量以及 IPsec 不应保护的任何其他流量插入 **deny** 条目。

动态加密映射只适用于和发起连接的远程对等体协商 SA。ASA 不能使用动态加密映射向远程对等体发起连接。使用动态加密映射时，如果出站流量匹配 ACL 中的 permit 条目并且尚不存在对应的 SA ，则 ASA 将丢弃该流量。

加密映射集可以包括动态加密映射。动态加密映射集应是加密映射集中优先级最低的加密映射（即它们应该具有最高序列号），以便ASA先评估其他加密映射。只有在其他（静态）映射条目不匹配时，它才会检查动态加密映射集。

与静态加密映射集类似，动态加密映射集也包括具有相同动态映射名称的所有动态加密映射。动态序号将区分动态加密映射集中的动态加密映射。如果您配置动态加密映射，请插入 permit ACL，为加密 ACL 标识 IPSec 对等体的数据流。否则，ASA 将接受对等体提议的所有数据流标识。

⚠

注意 对于要通过隧道传送到使用动态加密映射集配置的ASA接口的流量，请勿对其分配模块默认路由。要标识应通过隧道传送的流量，请将 ACL 添加到动态加密映射。配置与远程访问隧道关联的 ACL 时，请小心标识合适的地址池。仅在隧道启用后使用反向路由注入安装路由。

使用单情景或多情景模式创建一个动态映射条目。您可以在一个加密映射集中同时包含静态和动态映射条目。

过程

步骤 1 （可选） 将 ACL 分配给动态加密映射：

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *access-list-name*

这将确定应保护和不应保护哪些流量。*Dynamic-map-name* 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。

示例：

在本示例中，ACL 101 已分配给动态加密映射 dyn1。映射序号为 10。

```
crypto dynamic-map dyn1 10 match address 101
```

步骤 2 指定此动态加密映射允许哪些 IKEv1 转换集或 IKEv2 提议。使用该命令为 IKEv1 转换集或 IKEv2 提议按照优先级顺序列出多个转换集或提议（优先级高的优先）：

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1*, [*transform-set-name2*, ···*transform-set-name9*]

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2*, ··· *proposal-name11*]

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。*transform-set-name* 是当前创建或修改的转换集的名称。*proposal-name* 为 IKEv2 指定一个或多个 IPsec 提议的名称。

示例：

在 IKEv1 的本示例中，流量与 ACL 101 匹配时，SA 可以使用 myset1（第一优先级）或 myset2（第二优先级），具体取决于哪个转换集与对等体的转换集匹配。

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

步骤 3 （可选） 如果您想要覆盖全局生命周期值，请为动态加密映射条目指定 SA 生命周期：

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。您可以基于时间或传输的数据设置两个生命周期。但是，所传输数据的生命周期仅适用于站点间 VPN，不适用于远程访问 VPN。

示例：

此示例将动态加密映射 dyn1 10 的计时生命周期缩短至 2700 秒（45 分钟）。基于时间的生命周期未更改。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

步骤 4 （可选）指定在为此动态加密映射请求新的 SA 时 IPsec 要求 PFS，或应该在从对等体接收的请求中要求 PFS：

crypto dynamic-map *dynamic-map-name dynamic-seq-num***set pfs**[**group14**|**group15**|**group16**|**group19**|**group20**|**group21**]

Dynamic-map-name 指定引用已有动态加密映射的加密映射条目的名称。*Dynamic-seq-num* 指定与动态加密映射条目对应的序号。

示例：

```
crypto dynamic-map dyn1 10 set pfs group14
```

步骤 5 将动态加密映射集添加到静态加密映射集中。

请确保将引用动态映射的加密映射设置为加密映射集中优先级最低的条目（序号最高）。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Map-name 指定加密映射集的名称。*Dynamic-map-name* 指定引用已有动态加密映射的加密映射条目的名称。

示例：

```
crypto map  mymap 200 ipsec-isakmp dynamic dyn1
```

提供站点间冗余

您可以使用加密映射定义多个 IKEv1 对等体，以提供冗余。此配置对于站点间 VPN 非常有用。IKEv2 不支持此功能。

如果一个对等体失败，ASA 将与下一个和加密映射关联的对等体建立隧道。它会将数据发送到已与其协商成功的对等体，并且该对等体将成为活动对等体。活动对等体是 ASA 始终首先尝试后续协商的对等体，直到协商失败为止。此时 ASA 将继续与下一个对等体协商。当与加密映射关联的所有对等体都失败时，ASA 将循环返回第一个对等体。

管理 IPsec VPN

查看 IPsec 配置

您可以在单情景或多情景模式下输入这些命令，用于查看有关 IPSec 配置的信息。

表 *3:* 用于查看 *IPSec* 配置信息的命令

show running-configuration crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。
show running-config crypto ipsec	显示完整的 IPsec 配置。
show running-config crypto isakmp	显示完整的 ISAKMP 配置。
show running-config crypto map	显示完整的加密映射配置。
show running-config crypto dynamic-map	显示动态加密映射配置。
show all crypto map	显示所有配置参数，包括使用默认值的那些配置参数。
show crypto ikev2 sa detail	在加密统计信息中显示 Suite B 算法支持。
show crypto ipsec sa	在单情景或多情景模式下显示 Suite B 算法支持和 ESPv3 IPsec 输出。
show ipsec stats	在单情景或多情景模式下显示有关 IPsec 子系统的信息。TFC 数据包以及收到的有效和无效 ICMP 错误中都会显示 ESPv3 统计信息。

等待活动会话终止再重新启动

您可以安排 ASA 仅当所有活动会话都已自行终止后，才重新启动。默认情况下会禁用此功能。

使用 **reload** 命令重新启动 ASA。如果设置了 **reload-wait** 命令，则可以使用 **reload quick** 命令覆盖 **reload-wait** 设置。**reload** 和 **reload-wait** 命令适用于特权 EXEC 模式，这两个命令都不包含 **isakmp** 前缀。

过程

要启用等待所有活动会话自行终止后ASA再重新启动的功能，请在单情景或多情景模式下执行以下站点间任务：

crypto isakmp reload-wait

示例：

```
hostname(config)# crypto isakmp reload-wait
```

断开连接前向对等体发出警报

远程访问或 LAN 间会话可能出于某些原因丢失，例如：ASA 关闭或重新启动、会话空闲超时、超过最大连接时间或管理员切断。

ASA 可以通知合格的对等体（在 LAN 间配置或 VPN 客户端中）会话即将断开。收到此警报的对等体或客户端会对该原因进行解码，并将其显示在事件日志或弹出窗格中。默认情况下会禁用此功能。

合格客户端和对等体包括以下项：

- 已启用警报的安全设备
- 运行 4.0 或更高版本软件的思科 VPN 客户端（无需进行配置）

要启用用于IPSec对等体的断开通知，请在单情景或多情景模式下输入 **crypto isakmp disconnect-notify** 命令。

清除安全关联

有一些配置更改只有在随后的 SA 的协商过程中才生效。如果要让新的设置立即生效，请清除现有 SA 以使用已更改的配置重新建立它们。如果 ASA 正在处理 IPSec 流量，请只清除配置更改所影响的那部分 SA 数据库。对于大规模更改，或 ASA 正在处理少量 IPSec 流量时，请推迟执行清除整个 SA 数据库的时间。

下表列出了可以在单情景或多情景模式下输入用以清除和重新初始化 IPsec SA 的命令。

表 *4:* 清除和重新初始化 *IPSec SA* 的命令

clear configure crypto	删除整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。
clear configure crypto ca trustpoint	删除所有信任点。
clear configure crypto dynamic-map	删除所有动态加密映射。包括用于删除特定动态加密映射的关键字。
clear configure crypto map	删除所有加密映射。包括用于删除特定加密映射的关键字。
clear configure crypto isakmp	删除整个 ISAKMP 配置。
clear configure crypto isakmp policy	删除所有 ISAKMP 策略或特定策略。
clear crypto isakmp sa	删除整个 ISAKMP SA 数据库。

清除加密映射配置

clear configure crypto 命令包括可用于删除加密配置的元素的参数，这些配置包括 IPsec、加密映射、动态加密映射、CA 信任点、所有证书、证书映射配置和 ISAKMP。

请注意，如果输入不带参数的 **clear configure crypto** 命令，则将删除整个加密配置，包括所有证书。

有关详细信息，请参阅《*Cisco Secure Firewall ASA* 系列命令参考》中的 **clear configure crypto** 命令。

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。