IKE

配置 IKE

IKE 也称为 ISAKMP，是允许两个主机商定如何建立 IPSec 安全关联的协商协议。要为虚拟专用网络配置 ASA，您可以设置在整个系统范围内应用的全局 IKE 参数，还可以创建对等体通过协商建立 VPN 连接的 IKE 策略。

过程

步骤 1 启用 IKE， 第 1 页。

步骤 2 设置站点到站点 VPN 的 IKE 参数， 第 2 页。

步骤 3 配置 IKE 策略， 第 7 页。

启用 IKE

过程

步骤 1 要为 VPN 连接启用 IKE，请执行以下操作：

a) 在 ASDM 中，依次选择**配置 > 远程接入 VPN > 网络（客户端）接入 > 安全客户端 连接配置文件**。

b) 在 Access Interfaces 区域中，为您将将在其上使用 IKE 的接口选中 IPsec (IKEv2) Access 之下的 **Allow Access**。

步骤 2 要为站点到站点 VPN 启用 IKE，请执行以下操作：

a) 在 ASDM 中，依次选择 **Configuration > Site-to-Site VPN > Connection Profiles**。

b) 选择您想要在其上使用 IKEv1 和 IKEv2 的接口。

站点到站点 VPN 的 IKE 参数

在 ASDM 中，依次选择**配置 > 站点间 VPN > 高级 > IKE 参数**。

NAT 透明度

- 启用经由 NAT-T 的 IPsec

  经由 NAT-T 的 IPsec 允许 IPSec 对等体通过 NAT 设备建立远程访问和 LAN 到 LAN 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，但只有在必要时封装 IPSec 流量。默认情况下启用此功能。

  - ASA 可同时支持标准 IPsec、经由 TCP 的 IPsec、NAT-T 和经由 UDP 的 IPsec，具体取决于与其交换数据的客户端。
  - 同时启用 NAT-T 和经由 UDP 的 IPsec 时，NAT-T 优先。
  - 启用时，经由 TCP 的 IPsec 优先于所有其他连接方法。

  NAT-T 的 ASA 实施支持单个 NAT/PAT 设备之后的 IPSec 对等体，如下所示：

  - 一个 LAN 到 LAN 连接。
  - LAN 到 LAN 连接或多个远程访问客户端，但不是二者的混合。

  要使用 NAT-T，请执行以下操作：

  - 为用于打开端口 4500 的接口创建 ACL (Configuration > Firewall > Access Rules)。
  - 在此窗格中启用经由 NAT-T 的 IPsec。
  - 在 Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies 窗格中的 Fragmentation Policy 参数上，编辑您将用于启用 IPsec 预分片的接口。配置该项后，可以仍然允许流量通过不支持 IP 分片的 NAT 设备；它们不会阻碍支持分片的 NAT 设备的操作。

- 启用经由 TCP 的 IPsec

  对于标准 ESP 或 IKE 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，经由 TCP 的 IPsec 使得 VPN 客户端可以在其中进行操作。经由 TCP 的 IPSec 将 IKE 和 IPSec 协议同时封装在 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。此功能默认为已禁用。

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。它可在所有物理和 VLAN 接口上工作。它只是一个客户端到 ASA 功能。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。
- 启用时，经由 TCP 的 IPsec 优先于所有其他连接方法。

您可以同时在 ASA 及其连接的客户端上启用经由 TCP 的 IPsec。

您可以为您指定的最多 10 个端口启用经由 TCP 的 IPsec。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工作。其结果是，您无法再使用浏览器通过启用 IKE 的接口管理 ASA。要解决此问题，请将 HTTP/HTTPS 管理重新配置到不同的端口。

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。

发送至对等体的标识

选择对等体将在 IKE 协商期间用于标识自身的 **Identity**：

Address	使用交换 ISAKMP 标识信息的主机的 IP 地址。
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	远程对等体使用您指定的 **Key Id String** 来查找预共享密钥。
Automatic	按连接类型确定 IKE 协商： • 预共享密钥的 IP 地址 • 证书身份验证的证书 DN。

会话控制

- Disable Inbound Aggressive Mode Connections

  第 1 阶段 IKE 协商可以使用主模式或攻击性模式。两者提供相同的服务，但是攻击性模式只需要对等体之间的两次交换，而不是三次。攻击性模式速度更快，但是不为通信方提供标识保护。因此在建立于其中加密信息的安全 SA 之前，需要它们交换标识信息。此功能默认为已禁用。

- Alert Peers Before Disconnecting
  - 客户端或 LAN 到 LAN 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 到 LAN 配置中）会话即将断开，并向其传达原因。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。

- 您可以通过此窗格启用该功能，以便 ASA 可以发送这些警报，并传达断开的原因。

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 VPN 客户端（无需进行配置）。

- Wait for All Active Sessions to Voluntarily Terminate Before Rebooting

  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。此功能默认为已禁用。

- Number of SAs Allowed in Negotiation for IKEv1

  限制可以随时协商的 SA 的最大数量。

IKE v2 特定设置

IKE v2 可使用其他会话控制，限制打开的 SA 的数量。默认情况下，ASA 不限制打开的 SA 的数量：

- “Cookie 质询”- 使得 ASA 可以响应 SA 发起数据包，向对等设备发送 Cookie 质询。
  - “对传入 SA 进行 Cookie 质询前的百分比阈值”- ASA 允许协商的 SA 总数量的百分比，超过该百分比后，对于任何未来的 SA 协商，都会触发 Cookie 质询。范围为 0 到 100%。默认为 50%。

- Number of Allowed SAs in Negotiation - 限制可以随时协商的 SA 的最大数量。如果与 Cookie Challenge 配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。
- “允许的最大 SA 数”- 限制 ASA 上允许的 IKEv2 连接的数量。默认情况下，限制是许可证指定的最大连接数。
- Notify Invalid Selector - 当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。发送此通知默认为已禁用。

使用 IKE v2 特定设置防止 DoS 攻击

您可以配置 Cookie Challenge（这会质询传入安全关联 (SA) 的标识），或者限制打开的 SA 的数量，从而防止对于 IPsec IKEv2 连接的拒绝服务 (DoS) 攻击。默认情况下，ASA 不会限制打开的 SA 的数量，也从不对 SA 进行 Cookie 质询。您还可以限制允许的 SA 的数量，这可以停止来自协商的更多连接，从而防御 Cookie 质询功能无法抵御的内存和/或 CPU 攻击，并且保护当前的连接。

在 DoS 攻击中，当对等设备发送 SA 发起数据包并且 ASA 发送其响应但对等设备不再响应时，攻击者发起 DoS 攻击。如果对等设备持续这样做，ASA 上所有允许的 SA 请求会用尽，直到其停止响应。

启用 Cookie 质询的阈值百分比可以限制打开的 SA 协商的数量。例如，使用默认设置 50%，当 50% 的允许 SA 处于协商（打开）状态时，ASA 会对到达的任何其他 SA 发起数据包进行 Cookie 质询。

如果与**Number of SAs Allowed in Negotiation**或“允许的最大 SA 数”配合使用，可以配置低于这些限制的 Cookie 质询阈值，以便实现有效的交叉检查。

您还可以通过依次选择 Configuration > Site-to-Site VPN > Advanced > System Options，在 IPsec 层次上限制所有 SA 的生存期。

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。

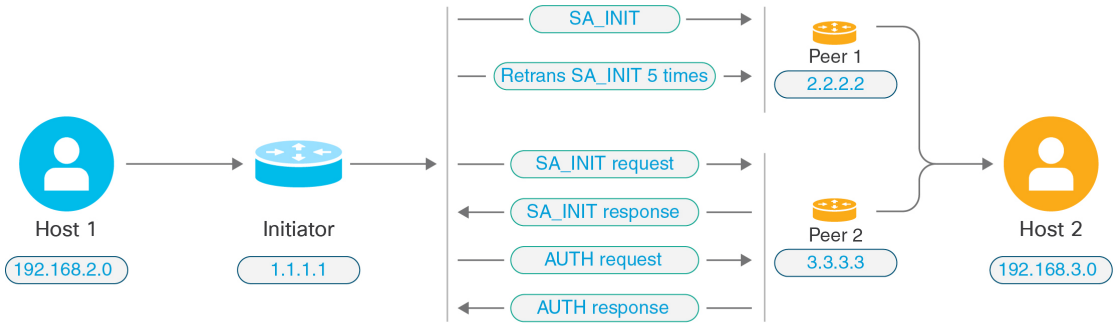
IKEv2 发起方行为

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.
```

IKE 策略

Configuration > Site-to-Site VPN > Advanced > IKE Policies

使用该窗格可通过 Add 添加、通过 Edit 编辑或通过 Delete 删除 IKEv1 和 IKEv2 策略。

要设置 IKE 协商条款，您可以创建一个或多个 IKE 策略，包括以下内容：

- 唯一优先级（1 至 65543，其中 1 为最高优先级）。
- 身份验证方法，用于确保对等体的身份。
- 加密方法，用于保护数据并确保隐私。
- HMAC 方法，用于确保发送方身份，以及确保消息在传输过程中未被修改。
- Diffie-Hellman 群，用于确立 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。
- ASA 在更换加密密钥前可使用该加密密钥的时长限制。

每个 IKE 协商分为两个部分，分别称为第 1 阶段和第 2 阶段。第 1 阶段创建第一条隧道，用于保护后来的 IKE 协商消息。第 2 阶段创建用于保护数据的隧道。

对于 IKEv1，您只能为一个参数启用一个设置。对于 IKEv2，每个提议对于加密、D-H 群、完整性哈希和 PRF 哈希可具有多个设置。

如果您未配置任何 IKE 策略，ASA 会使用默认策略，默认策略始终会被设为最低优先级，它包含有每个参数的默认值。如果您没有为特定参数指定值，则默认值生效。

当 IKE 协商开始时，发起协商的对等体将其所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。

如果 IKE 策略具有相同的加密、哈希、身份验证和 Diffie-Hellman 值，而且 SA 生存期小于或等于发送的策略中的生存期，则它们之间存在匹配。如果生存期不同，则会应用较短的生存期（来自远程对等体）。如果不存在匹配，IKE 将拒绝协商，并且不会建立 IKE SA。

字段

- IKEv1 Policies - 显示每个配置的 IKE 策略的参数设置。
  - Priority # - 显示此策略的优先级。
  - Encryption - 显示加密方法。
  - Hash - 显示散列算法。
  - D-H Group - 显示 Diffie-Hellman 群。
  - Authentication - 显示身份验证方式。
  - Lifetime (secs) - 显示以秒为单位的 SA 生存期。
- IKEv2 Policies - 显示每个配置的 IKEv2 策略的参数设置。
  - Priority # - 显示此策略的优先级。
  - Encryption - 显示加密方法。
  - Integrity Hash - 显示散列算法。

- PRF Hash - 显示伪随机功能 (PRF) 散列算法。
- D-H Group - 显示 Diffie-Hellman 群。
- Lifetime (secs) - 显示以秒为单位的 SA 生存期。

添加或编辑 IKEv1 策略

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKE Policy

Priority # - 键入一个数值，以便设置 IKE 策略的优先级。取值范围为 1 至 65535，其中 1 为最高优先级。

Encryption - 选择一个加密方法。这是保护在两个 IPSec 对等体之间传输的数据的对称加密方法。选项如下：

des	56 位 DES-CBC。安全性较低，但速度比备选提议快。默认值。
3des	168 位三重 DES。
aes	128 位 AES。
aes-192	192 位 AES。
aes-256	256 位 AES。

Hash - 选择确保数据完整性的散列算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。

sha	SHA-1	默认值为 SHA-1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对MD5的成功（但非常困难）攻击；然而，IKE使用的HMAC 变体可防止此类攻击。
md5	MD5	

“身份验证”- 选择 ASA 用于建立每个 IPSec 对等体标识的身份验证方法。对于增长型网络，预共享密钥不能很好地进行扩展，但是在小型网络中更容易设置。选项如下：

pre-share	预共享密钥。
rsa-sig	使用 RSA 签名算法生成的带密钥的数字证书。

D-H Group - 选择 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机密。

1	群 1（768 位）	群 2（1024 位 Diffie - Hellman）执行所需的 CPU 时间较少，但安全性要低于群 1 或 5。
2	群 2（1024 位）	
5	群 5（1536 位）	

14	组 14（2048 位）	默认 Diffie-Hellman 组为 Group 14（2048 位 Diffie-Hellman）

Lifetime (secs) - 为 SA 生存期选择 Unlimited 或输入一个整数。默认值为 86400 秒或 24 小时。生命期越长，ASA 设置未来 IPsec 安全关联的速度就越慢。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）。建议接受默认值。

Time Measure - 选择时间度量值。ASA 接受以下值：

120 - 86,400 秒
2 - 1440 分钟
1 - 24 小时
1 天

添加或编辑 IKEv2 策略

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy

Priority # - 键入一个数值，以便设置 IKEv2 策略的优先级。取值范围为 1 至 65535，其中 1 为最高优先级。

Encryption - 选择一个加密方法。这是保护在两个 IPSec 对等体之间传输的数据的对称加密方法。选项如下：

des	为 ESP 指定 56 位 DES-CBC 加密。
3des	（默认）为 ESP 指定三重 DES 加密算法。
aes	为 ESP 指定带有 128 位密钥加密的 AES。
aes-192	为 ESP 指定带有 192 位密钥加密的 AES。
aes-256	为 ESP 指定带有 256 位密钥加密的 AES。
aes-gcm	指定 AES-GCM/GMAC 128 位支持，以确保对称加密和完整性。
aes-gcm-192	指定 AES-GCM/GMAC 192 位支持，以确保对称加密和完整性。
aes-gcm-256	指定 AES-GCM/GMAC 256 位支持，以确保对称加密和完整性。
NULL	表示不加密。

D-H Group - 选择 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机密。

1	群 1（768 位）	默认情况下，群 2（1024 位 Diffie - Hellman）执行所需的 CPU 时间较少，但安全性要低于群 2 或 5。
2	群 2（1024 位）	

5	群 5（1536 位）	
14	群 14	
19	群 19	
20	群 20	
21	群 21	
24	群 24	

Integrity Hash - 选择确保 ESP 协议的数据完整性的散列算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。

sha	SHA 1	默认值为 SHA 1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对MD5的成功（但非常困难）攻击；然而，IKE使用的HMAC 变体可防止此类攻击。
md5	MD5	
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-bit digest**	指定具有 384 位摘要的安全散列算法 SHA 2。
sha512	**SHA 2, 512-bit digest**	指定具有 512 位摘要的安全散列算法 SHA 2。
null		表示将 AES-GCM 或 AES-GMAC 配置为加密算法。如果 AES-GCM 已被配置为加密算法，对于完整性算法您必须选择 null。

Pseudo-Random Function (PRF) - 对于在 SA 中使用的所有加密算法，指定用于构建密钥内容的 PRF。

sha	SHA-1	默认值为 SHA-1。MD5 的摘要较小，被认为速度比 SHA-1 稍快。已发生过针对MD5的成功（但非常困难）攻击；然而，IKE使用的HMAC 变体可防止此类攻击。
md5	MD5	
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。

Lifetime (secs) - 为 SA 生存期选择 Unlimited 或输入一个整数。默认值为 86400 秒或 24 小时。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）。建议接受默认值。

ASA 接受以下值：

120 - 86,400 秒
2 - 1440 分钟

1 - 24 小时
1 天

配置 IPsec

ASA 会将 IPsec 用于 LAN 到 LAN 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”是指远程访问客户端或其他安全网关。ASA 支持与思科对等体（IPv4 或 IPv6），以及符合所有相关标准的第三方对等体的 LAN 到 LAN IPsec 连接。

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。这些协商涉及两个阶段：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。

ASA 支持以下 IPSec 属性：

- 主模式用于使用数字证书进行身份验证时的协商第一阶段 ISAKMP 安全关联
- 攻击性模式用于使用预共享密钥进行身份验证时的协商第一阶段 ISAKMP 安全关联 (SA)
- 身份验证算法：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 身份验证模式：
  - 预共享密钥
  - X.509 数字认证
- 加密算法：
  - AES -128、-192 和 -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 扩展身份验证 (XAuth)
- 模式配置（也称为 ISAKMP 配置方法）
- 隧道封装模式

- 使用 LZS 的 IP 压缩 (IPCOMP)

过程

步骤 1 配置 加密映射，第 13 页。

步骤 2 配置 IPsec 预分片策略，第 20 页。

步骤 3 配置 IPsec 提议（转换集），第 22 页。

加密映射

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

此窗格显示当前配置的加密映射，该映射在 IPSec 规则中定义。您可以在此处添加、编辑、删除和上移、下移、剪切、复制和粘贴 IPsec 规则。

注释 您无法编辑、删除或复制隐式规则。使用动态隧道策略配置时，ASA 会隐式接受远程客户端的流量选择提议。您可以通过提供特定的流量选择来将其覆盖。

此外，您还可以通过选择接口、源、目标、目标服务或规则查询，选择是或包含，并输入筛选参数，从而通过 **Find** 来查找规则（过滤规则的显示）。点击 ... 可以启动一个浏览对话框，该对话框会显示您可以选择的所有现有条目。使用 **Diagram** 以图示形式显示规则。

IPSec 规则指定以下字段：

- Type: Priority - 显示规则类型（静态或动态）及其优先级。
- Traffic Selection
  - # - 指示规则编号。
  - Source - 指示流量发送至 Remote Side Host/Network 列中所列 IP 地址时，遵从此规则的 IP 地址。在详细信息模式（请查看 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，例如 inside:any，其中 any 意味着内部接口上的任意主机都会受该规则影响。
  - Destination - 列出当流量发自 Security Appliance Side Host/Network 列中所列 IP 地址时，遵从此规则的 IP 地址。在详细信息模式（请查看 Show Detail 按钮）下，地址列可能包含带 any 一词的接口名称，如 outside:any。其中 any 意味着外部接口上的任意主机都会受该规则影响。同样也是在详细信息模式下，地址列可能包含用方括号括起来的 IP 地址，例如 [209.165.201.1-209.165.201.30]。这些地址都是转换后的地址。当内部主机连接至外部主机时，ASA 会将内部主机的地址映射至地址池中的地址。主机创建出站连接后，ASA 会保持该地址映射。此地址映射结构称为 xlate，会在内存中保留一段时间。
  - Service - 指定此规则指定的服务和协议（TCP、UDP、ICMP 或 IP）。
  - Action - 指定 IPsec 规则类型（保护或不保护）。

- Transform Set - 显示此规则的转换集。
- Peer - 标识 IPSec 对等体。
- PFS - 显示此规则的完全向前保密设置。
- NAT-T Enabled - 指示是否为此策略启用 NAT 遍历。
- “启用反向路由”- 指示是否为此策略启用反向路由注入 (RRI)。RRI 在配置时完成并被视为静态的，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。
  - “动态”- 如果指定动态 RRI，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 RRI。

注释 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

- Connection Type -（仅对静态隧道策略有意义。）将此策略的连接类型标识为双向、仅发出或仅应答。
- SA Lifetime - 显示该规则的 SA 生存期。
- CA Certificate - 显示该策略的 CA 证书。这仅适用于静态连接。
- IKE Negotiation Mode - 显示 IKE 协商是使用主模式还是攻击性模式。
- Description -（可选）指定此规则的简要说明。对于现有规则，这是您在添加该规则时键入的说明。隐式规则包括以下说明：“Implicit rule”。要编辑除隐式规则之外的任意规则的说明，请右键点击此列，并选择 Edit Description 或双击此列。
- Enable Anti-replay window size - 设置防重放窗口大小，该值为 64 的倍数，介于 64 至 1028 之间。在采用流量整形的分层 QoS 策略中，优先级排队的一个副作用（请参阅 "Rule Actions > QoS Tab"）是数据包的重新排序。对于 IPSec 数据包，未处于防重放窗口内的错序数据包，会生成警告系统日志消息。在进行优先级排队的情况下，这些警告会变成错误警报。配置防重放窗口大小可以帮助您避免可能的错误警报。
- “启用 IPsec 内部路由查找”- 默认情况下，不会对通过 IPsec 隧道发送的数据包执行查找，仅对外部 ESP 数据包执行按数据包邻接关系查找。在某些网络拓扑中，当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。

创建或编辑 IPSec 规则隧道策略（加密映射）- Basic 选项卡

请使用此窗格为 IPsec 规则定义新的隧道策略。在您点击 **OK** 后，您在此处定义的值会显示在 IPsec Rules 表中。默认情况下，所有规则一旦显示在 IPsec Rules 表中，就会立即启用。

Tunnel Policy 窗格允许您定义用于协商 IPSec（第 2 阶段）安全关联 (SA) 的隧道策略。ASDM 可捕获您的配置编辑，但不会将其保存至运行配置，直至您点击 **Apply**。

每个隧道策略都必须指定一个转换集，并确定其应用至的安全设备接口。转换集可标识执行 IPSec 加密和解密运算的加密和散列算法。由于不是每个 IPSec 对等体都支持相同的算法，您可能想要指定一些策略，并为每个策略分配优先级。然后，安全设备会与远程 IPsec 对等体协商，以便商定两个对等体都支持的转换集。

隧道策略可以是 *static* 或 *dynamic*。静态隧道策略可以标识一个或多个，您的安全设备允许与其进行 IPsec 连接的 IPsec 对等体或子网。无论是您的安全设备发起连接，还是您的安全设备接收来自远程主机的连接请求，都可以使用静态策略。静态策略会要求您输入标识允许的主机或网络所需的信息。

对于被允许发起与安全设备的连接的远程主机，如果您无法或不想提供这些远程主机的相关信息，可以使用动态隧道策略。如果您仅将安全设备用作与远程 VPN 中央站点设备相关的 VPN 客户端，则不需要配置任何动态隧道策略。允许远程访问客户端，通过充当 VPN 中央站点设备的安全设备，发起与您的网络的连接时，动态隧道策略最为有用。远程访问客户端拥有动态分配的 IP 地址，或者您不想为大量的远程访问客户端配置单独的策略时，动态隧道策略非常有用。

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Basic

- Interface - 选择此策略应用至的接口的名称。
- Policy Type - 选择此隧道策略的类型（静态或动态）。
- Priority - 输入此策略的优先级。
- IKE Proposals (Transform Sets) - 指定 IKEv1 和 IKEv2 IPsec 提议：
  - IKEv1 IPsec Proposal - 为策略选择提议（转换集），然后点击 **Add** 将其移至活动转换集列表。点击 **Move Up** 或 **Move Down**，以便重新排列列表框中的提议。您最多可向加密映射条目或动态加密映射条目，添加 11 个提议。
  - IKEv2 IPsec Proposal - 为策略选择提议（转换集），然后点击 **Add** 将其移至活动转换集列表。点击 **Move Up** 或 **Move Down**，以便重新排列列表框中的提议。您最多可向加密映射条目或动态加密映射条目，添加 11 个提议。
- Peer Settings - 对于动态加密映射条目可选 - 配置此策略的对等体设置。
  - Connection Type -（仅对静态隧道策略有意义。）选择双向、仅发出或仅应答，以便指定此策略的连接类型。对于 LAN 到 LAN 连接，请选择双向或仅应答（而非仅发出）。对于 LAN 到 LAN 冗余，请选择仅应答。如果您选择仅发出，可以指定最多 10 个冗余对等体。对于单向，您可以指定仅发出或仅应答，二者均不会默认启用。
  - IP Address of Peer to Be Added - 输入您将要添加的 IPSec 对等体的 IP 地址。从 9.14(1) 开始，ASA 支持 IKEv2 中的多个对等体。您最多可以向加密映射中添加 10 个对等体。
- Enable Perfect Forwarding Secrecy - 选中此项，以便启用此策略的完全向前保密功能。PFS 是一个加密概念，其中每个新密钥都与任何先前密钥无关。在 IPsec 协商中，除非您指定完全向前保密，否则第 2 阶段的密钥会基于第 1 阶段的密钥。
- “Diffie-Hellman 群”- 当您启用 PFS 时，还必须选择 ASA 用于生成会话密钥的 Diffie-Hellman 群。选项如下：

- Group 1 (768-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 1 来生成 IPsec 会话密钥，其中素数和生成元均为 768 位。此选项更加安全，但需要更多的处理开销。
- Group 2 (1024-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 2 来生成 IPsec 会话密钥，其中素数和生成元均为 1024 位。此选项比群 1 更加安全，但需要更多的处理开销。
- Group 5 (1536-bits) = 使用完全向前保密功能，并且使用 Diffie-Hellman 群 5 来生成 IPsec 会话密钥，其中素数和生成元均为 1536 位。此选项比群 2 更加安全，但需要更多的处理开销。
- Group 14 (2048-bits) = 使用完全向前保密功能，并将 Diffie-Hellman 群 14 用于 IKEv2。
- Group 19 = 使用完全向前保密功能，并将 Diffie-Hellman 群 19 用于 IKEv2，以便支持 ECDH。
- Group 20 = 使用完全向前保密功能，并将 Diffie-Hellman 群 20 用于 IKEv2，以便支持 ECDH。
- Group 21 = 使用完全向前保密功能，并将 Diffie-Hellman 群 21 用于 IKEv2，以便支持 ECDH。
- Group 24 = 使用完全向前保密功能，并将 Diffie-Hellman 群 24 用于 IKEv2。

创建或编辑 IPSec 规则隧道策略（加密映射） - Advanced 选项卡

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced

- Enable NAT-T - 启用此策略的 NAT 遍历 (NAT-T)。
- Enable Reverse Route Injection - 启用此策略的反向路由注入。如果您为远程 VPN 客户端或 LAN 到 LAN 会话运行 ASA 或路由信息协议 (RIP)，反向路由注入 (RRI) 会被用于填充运行动态路由协议（如开放最短路径优先 [OSPF] 或增强型内部网关路由协议 [EIGRP]）的内部路由器的路由表。RRI 在配置时完成并被视为静态的，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。
  - “动态” - 如果指定动态 RRI，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 RRI。通常，RRI 路由用于启动隧道（如果尚无隧道），并且需要对流量加密。在支持动态 RRI 的情况下，隧道建立之前并不存在路由。因此，配置了动态 RRI 的 ASA 通常只会用作响应方。

注释 动态 RRI 仅适用于基于 IKEv2 的静态加密映射。

- Security Association Lifetime Settings - 配置安全关联 (SA) 的持续时间。此参数指定 IPsec SA 密钥生存期的度量方式，即 IPsec SA 过期并必须用新的密钥重新协商前，它可以持续的时长。
  - Time - 根据小时 (hh)、分钟 (mm) 和秒 (ss) 指定 SA 生存期。

- Traffic Volume - 根据流量的千字节数定义 SA 生存期。输入负载数据的千字节数量，IPsec SA 在达到该数量后到期。最小值为 100 KB，默认值为 10000 KB，最大值为 2147483647 KB。

- Static Type Only Settings - 指定静态隧道策略的参数。
  - Device Certificate - 选择要使用的证书。如果您选择 None (Use Preshared Keys) 之外的选项，此设置为默认值。您选择 None 之外的选项时，Send CA certificate chain 复选框处于活动状态。
  - Send CA certificate chain - 启用整个信任点链的传输。
  - IKE Negotiation Mode - 选择 IKE 协商模式、主模式或攻击性模式。此参数可以设置交换密钥信息和设置 SA 的模式。它设置该协商的发起方使用的模式；响应方会自动协商。攻击性模式速度较快，使用的数据包较少，交换次数较少，但是它不会保护通信方的身份。主模式速度较慢，使用的数据包较多，交换次数较多，但是它会保护通信方的身份。此模式更安全，并且是默认选择。如果选择 Aggressive，则 Diffie-Hellman Group 列表会激活。
  - Diffie-Hellman Group - 选择要应用的 Diffie-Hellman 群。选择如下：群 1（768 位）、群 2（1024 位）或群 5（1536 位）。

- ESP v3 - 指定是否为加密和动态加密映射验证传入 ICMP 错误消息，设置每安全关联策略，或者启用流量数据包：
  - Validate incoming ICMP error messages - 选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的那些 ICMP 错误消息。
  - Enable Do Not Fragment (DF) policy - 定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位。选择如下选项之一：

    Clear DF bit - 忽略 DF 位。

    Copy DF bit - 保持 DF 位。

    Set DF bit - 设置并使用 DF 位。
  - Enable Traffic Flow Confidentiality (TFC) packets - 启用虚拟 TFC 数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。

注释 在启用 TFC 之前，您必须先在 Tunnel Policy (Crypto Map) Basic 选项卡上设置 IKE v2 IPsec 提议。

可以使用 Burst、Payload Size 和 Timeout 参数生成穿过指定 SA 的随机长度的数据包。

创建或编辑 IPSec 规则流量选择选项卡

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Traffic Selection

此窗口允许您定义要保护（允许）或不保护（拒绝）哪些流量。

- Action - 指定此规则要采取的操作。选项为保护和不保护。
- Source - 指定源主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。点击 ⋯ 可启动包含以下字段的 Browse Source 对话框：
  - Add/Edit - 选择 IP 地址或网络对象组，以便添加更多源地址或组。
  - Delete - 点击此项可删除条目。
  - Filter - 输入 IP 地址，以便过滤显示的结果。
  - Name - 指示后面的参数指定源主机或网络的名称。
  - IP Address - 指示后面的参数指定源主机或网络的接口、IP 地址和子网掩码。
  - Netmask - 选择应用于该 IP 地址的标准子网掩码。此参数在您选择 IP Address 选项按钮时显示。
  - Description - 输入说明。
  - Selected Source - 点击 **Source**，以便将选定条目作为源包含。
- Destination - 指定目标主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。点击 ... 以启动包含以下字段的 Browse Destination 对话框：
  - Add/Edit - 选择 IP 地址或网络对象组，以便添加更多目标地址或组。
  - Delete - 点击此项可删除条目。
  - Filter - 输入 IP 地址，以便过滤显示的结果。
  - Name - 指示后面的参数指定目标主机或网络的名称。
  - IP Address - 指示后面的参数指定目标主机或网络的接口、IP 地址和子网掩码。
  - Netmask - 选择应用于该 IP 地址的标准子网掩码。此参数在您选择 IP Address 选项按钮时显示。
  - Description - 输入说明。
  - Selected Destination - 点击 **Destination**，以便包含作为目标的选定条目。
- Service - 输入一个服务，或者点击 ... 以便启动 Browse Service 对话框，在该对话框中，您可以从服务列表选择服务。
- Destination - 输入 Traffic Selection 条目的说明。
- More Options
  - Enable Rule - 点击此复选框可启用此规则。
  - Source Service - 输入一个服务或点击 **...** 以便启动 Browse Service 对话框，您可以在其中从服务列表选择服务。

- Time Range - 定义此规则应用的时间范围。
- Group - 表示后面的参数指定源主机或网络的接口和组名称。
- Interface - 选择 IP 地址的接口名称。此参数在您选择 IP Address 选项按钮时显示。
- IP Address - 指定此策略应用至的接口的 IP 地址。此参数在您选择 IP Address 选项按钮时显示。
- Destination - 指定源或目标主机或网络的 IP 地址、网络对象组或接口 IP 地址。规则不能将相同地址同时用作源和目标。对于这些字段中的任一字段，点击 **...**，以便启动包含以下字段的 Browse 对话框：
- Name - 选择用作源或目标主机或网络的接口名称。此参数在您选择 Name 选项按钮时显示。这是与此选项关联的唯一参数。
- Interface - 选择 IP 地址的接口名称。此参数在您点击 Group 选项按钮时显示。
- Group - 为源或目标主机或网络，选择指定接口上的组的名称。如果此列表中没有条目，您可以输入现有组的名称。此参数在您点击 Group 选项按钮时显示。

- **Protocol and Service** - 指定与此规则相关的协议和服务参数。

注释 “Any - any”IPsec 规则不会被允许。此类规则会阻止设备及其对等体支持多个 LAN 到 LAN 隧道。

- TCP - 指定此规则适用于 TCP 连接。此选项还会显示 Source Port and Destination Port 分组框。
- UDP - 指定此规则适用于 UDP 连接。此选项还会显示 Source Port and Destination Port 分组框。
- ICMP - 指定此规则适用于 ICMP 连接。此选项还会显示 ICMP Type 分组框。
- IP - 指定此规则适用于 IP 连接。此选项还会显示 IP Protocol 分组框。
- Manage Service Groups - 显示 Manage Service Groups 窗格，在此窗格上，您可以添加、编辑或删除一组 TCP/UDP 服务/端口。
- Source Port and Destination Port - 包含 TCP 或 UDP 端口参数，具体取决于您在 Protocol and Service 分组框中选择的选项按钮。
- Service - 指示您正为个别服务指定参数。指定应用过滤器时要使用的服务名称和布尔操作符。
- Boolean operator (unlabeled) - 列出用于匹配服务框指定服务的布尔条件（等于、不等于、大于、小于或范围）。
- Service (unlabeled) - 标识要匹配的服务（例如 https、kerberos 或 any）。如果您指定了范围服务运算符，此参数会变成两个框，您可以在其中输入范围的起始值和结束值。

- ... - 显示一个服务列表，您可在其中选择要显示在 Service 框中的服务。
- Service Group - 指示您要为源端口指定服务组的名称。
- Service (unlabeled) - 选择要使用的服务组。
- ICMP Type - 指定要使用的 ICMP 类型。默认值为 any。点击 ⋯ 按钮可显示可用类型列表。

- Options
  - Time Range - 指定现有时间范围的名称，或者创建新的范围。
  - ... - 显示 Add Time Range 窗格，您可以在该窗格上定义新的时间范围。
  - Please enter the description below (optional) - 为您提供空间，以便输入规则的简要描述。

IPsec 预分片策略

Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies

当隧道流量通过公用接口时，IPsec 预分片策略指定如何处理超过最大传输单位 (MTU) 设置的数据包。此功能为处理 ASA 和客户端之间的路由器或 NAT 设备拒绝或丢弃 IP 分片的情况提供了方法。例如，假设客户端要从 ASA 后面的 FTP 服务器进行 FTP 获取，并且 FTP 服务器在公共接口上传输的数据包在封装后会超过 ASA 的 MTU 大小。此时，选择的选项将决定 ASA 如何处理这些数据包。预分片策略适用于从 ASA 公共接口发出的所有流量。

ASA 会封装所有的隧道数据包。封装后，ASA 会先将超过 MTU 设置的数据包分片，然后通过公共接口传输它们。此为默认策略。此选项适用于允许分片数据包不受阻碍地通过隧道的情况。对于FTP示例，大型数据包会被封装，然后在IP层分片。中间设备可能会丢弃片段，或只是使片段错序。负载均衡设备可能会引入错序的片段。

当您启用预分片时，ASA 会先对超过 MTU 设置的隧道数据包进行分片，然后将其封装。如果这些数据包上的 DF 位已设置，ASA 会清除 DF 位，将数据包分片，然后将其封装。此操作会创建两个离开公用接口的独立未分片 IP 数据包，并且通过将片段转换为需要在对等体站点重组的完整数据包，将这些数据包成功传输至对等体站点。在我们的示例中，ASA 通过清除 DF 位覆盖 MTU 和允许分片。

注释 在任意接口上更改 MTU 或预分片选项都会拆解所有现有连接例如，如果 100 活动隧道在公用接口上终止，并且您在外部接口上更改MTU或预分片选项，则公用接口上的所有活动隧道都会被丢弃。

使用该窗格，可以为在父窗格上选定的接口查看或通过 **Edit** 编辑现有 IPsec 预分片策略和不分片 (DF) 位策略。

字段

- Interface - 标识选定接口。您不能使用此对话框更改该参数。

- Enable IPsec pre-fragmentation - 启用或禁用 IPsec 预分片。ASA 会先对超过 MTU 设置的隧道数据包进行分片，然后将其封装。如果这些数据包上的 DF 位已设置，ASA 会清除 DF 位，将数据包分片，然后将其封装。此操作会创建两个离开公用接口的独立未分片 IP 数据包，并且通过将片段转换为需要在对等体站点重组的完整数据包，将这些数据包成功传输至对等体站点。
- DF Bit Setting Policy - 不分片位策略：Copy、Clear 或 Set。

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），还可以由管理员在以下屏幕上配置首选分片方法：

配置 > 站点间 VPN > 高级 > IKE 参数

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：

- 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 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。

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。

过程

步骤 1 在 ASDM 中，依次转到**配置** > **站点间 VPN** > **高级** > **IKE 参数**。

步骤 2 选择或取消选择**启用分片 (Enable fragmentation)** 字段。

步骤 3 指定**分片 MTU** 大小。

步骤 4 指定**首选分片方法**。

IPsec 提议（转换集）

Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets)

转换是一组在数据流上完成的操作，目的是提供数据身份验证、数据保密性和数据压缩。例如，采用 3DES 加密和 HMAC-MD5 身份验证算法 (ESP-3DES-MD5) 的 ESP 协议就是一种转换。

使用此窗格可以查看、通过 **Add** 添加、通过 **Edit** 编辑或通过 **Delete** 删除下述 IKEv1 和 IKEv2 转换集。每个表均显示所配置的转换集的名称和详细信息。

IKEv1 IPsec 提议（转换集）

- **模式** - 应用 ESP 加密和身份验证的模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。
  - **隧道模式** -（默认）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** - 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。
- **ESP 加密** - 转换集的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据身份验证和防重放服务。ESP 会封装将要保护的数据。

- **ESP 身份验证** - 转换集的 ESP 身份验证算法。

IKEv2 IPsec 提议

- **模式** - 应用 ESP 加密和身份验证的模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。
  - **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。

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”。

- **加密** - 显示 IKEv2 IPsec 提议的封装安全协议 (ESP) 加密算法。ESP 可提供数据隐私服务、可选的数据身份验证和防重放服务。ESP 会封装将要保护的数据。
- **完整性散列** - 显示确保 ESP 协议的数据完整性的散列算法。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。它可以确保数据包来自您认为的发送方，并且在传输过程中未被修改。如果 AES-GCM/GMAC 已被配置为加密算法，对于完整性算法您必须选择 null。

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。