LAN 间 IPsec VPN

LAN 间 VPN 可连接不同地理位置的网络。

可以创建与思科对等体以及与符合所有相关标准的第三方对等体的 LAN 间 IPsec 连接。这些对等体可以采用内部和外部地址（使用 IPv4 和 IPv6 选址）的任意组合。

ASA 不允许通过 VPN 隧道传输 ping 以外的本地源流量。

本章介绍如何构建 LAN 间 VPN 连接。

配置摘要

本节提供本章介绍的示例 LAN 间配置的摘要。后面各节提供分步说明。

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
```

```
hostname(config-ikev2-policy)# # encryption aes
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)#  crypto ipsec ikev1 transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

在多情景模式下配置站点间 VPN

按照以下步骤在多情景模式下允许站点间支持。通过执行这些步骤，可以了解资源分配如何划分。

过程

步骤 1 如要在多情景模式下配置 VPN，请配置资源类，然后选择 VPN 许可证作为允许的资源的一部分。“为资源管理配置类”提供这些配置步骤。以下是示例配置：

```
class ctx1
 limit-resource VPN Burst Other 100
 limit-resource VPN Other 1000
```

步骤 2 配置情景并使其成为已配置的允许 VPN 许可证的类的成员。以下是示例配置：

```
context context1
 member ctx1
 allocate-interface GigabitEthernet3/0.2
 allocate-interface GigabitEthernet3/1.2
 allocate-interface Management0/0
 config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
 join-failover-group 1
```

步骤 3 配置连接配置文件、策略、加密映射等，如同对使用站点间VPN的单情景VPN配置进行配置一样。

配置接口

一个ASA至少有两个接口，在本指南中分别将它们称为外部接口和内部接口。通常，外部接口连接到公共互联网，内部接口连接到专用网络且不接受公共访问。

首先，请在ASA上配置并启用两个接口。然后，为接口分配名称、IP地址和子网掩码。或者，在安全设备上配置接口的安全级别、速度和双工操作。

注释 ASA 的外部接口地址（适用于 IPv4/IPv6）不能与专用端地址空间重叠。

过程

步骤 1 要进入接口配置模式，请在全局配置模式下输入含有要配置接口的默认名称的 **interface** 命令。在以下示例中，该接口为 ethernet0。

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

步骤 2 要设置接口的 IP 地址和子网掩码，请输入 **ip address** 命令。在以下示例中，IP 地址为 10.10.4.100，子网掩码为 255.255.0.0。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

步骤 3 要命名接口，请输入 **nameif** 命令，最多 48 个字符。设置此名称后，不能对其进行更改。在以下示例中，ethernet0 接口的名称为 outside。

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

步骤 4 要启用接口，请输入 **shutdown** 命令的 **no** 版本。默认情况下，接口处于禁用状态。

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

步骤 5 要保存更改，请输入 **write memory** 命令：

```
hostname(config-if)# write memory
hostname(config-if)#
```

步骤 6 如要配置其他接口，请使用相同程序。

在外部接口上配置 ISAKMP 策略和启用 ISAKMP

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。这包括与对等体协商 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。

通过 IKEv1 策略，可以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。

以下各节提供在接口上创建 IKEv1 和 IKEv2 策略并将其启用的操作步骤：

- 为 IKEv1 连接配置 ISAKMP 策略，第 4 页
- 为 IKEv2 连接配置 ISAKMP 策略，第 5 页

为 IKEv1 连接配置 ISAKMP 策略

要为 IKEv1 连接配置 ISAKMP 策略，请使用 **crypto ikev1 policy** 命令进入 IKEv1 策略配置模式，在此模式下可以配置 IKEv1 参数。

过程

步骤 1 进入 IPsec IKEv1 策略配置模式。例如：

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

步骤 2 设置身份验证方法。以下示例配置预共享密钥：

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

步骤 3 设置加密方法。以下示例配置：

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

步骤 4 设置 HMAC 方法。以下示例配置 SHA-1：

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

步骤 5 设置 Diffie-Hellman 群。以下示例配置组 14：

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

步骤 6 设置加密密钥生命周期。以下示例配置 43,200 秒（12 小时）：

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

步骤 7 在单情景或多情景模式下于名为 outside 的接口上启用 IKEv1：

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

步骤 8 如要保存更改，请输入 **write memory** 命令：

```
hostname(config)# write memory
hostname(config)#
```

为 IKEv2 连接配置 ISAKMP 策略

要为 IKEv2 连接配置 ISAKMP 策略，请使用 **crypto ikev2 policy** 命令进入 IKEv2 策略配置模式，在此模式下可以配置 IKEv2 参数。

过程

步骤 1 进入 IPsec IKEv2 策略配置模式。例如：

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

步骤 2 设置加密方法。以下是配置 AES 的示例：

```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```

步骤 3 设置 Diffie-Hellman 群。以下是配置组 15 的示例：

```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```

步骤 4 设置用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF)。以下示例配置 SHA-1（HMAC 变体）：

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

步骤 5 设置加密密钥生命周期。以下示例配置 43,200 秒（12 小时）：

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

步骤 6 在名为 outside 的接口上启用 IKEv2：

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

步骤 7 如要保存更改，请输入 **write memory** 命令：

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 的多密钥交换

IKEv2 使用 Diffie-Hellman (DH) 组在发起方和响应方之间建立共享密钥。IKEv2 支持额外的密钥交换，以保护 IPsec 通信免受量子计算机的攻击。每个交换都会使用不同的 DH 组。为 SA 设置计算出的共享密钥是从每次交换派生的所有密钥的组合。IKE SA 是在 IKE 对等体之间交换多个密钥后建立的。

ASA 对多密钥交换使用七种新的转换类型：

- 额外密钥交换 1（IANA 值 6）
- 额外密钥交换 2（IANA 值 7）
- 额外密钥交换 3（IANA 值 8）
- 额外密钥交换 4（IANA 值 9）
- 额外密钥交换 5（IANA 值 10）
- 额外密钥交换 6（IANA 值 11）
- 额外密钥交换 7（IANA 值 12）

您最多可以配置七个多密钥交换。对于配置的每个额外密钥交换，您必须指定 DH 组。ASA 使用从先前交换派生的密钥来对中间密钥交换进行加密。如果发起方和响应方对等体未就DH组达成一致，则协商失败，并会向发起方发送 **NO_PROPOSAL_CHOSEN** 错误通知。您还可以将转换配置为 none。如果选择 none，则不会进行密钥交换。

对于发起方，如果为额外密钥交换 *n* 将密钥交换方法配置为 **none**：

- 响应方可以为额外密钥交换 *n* 选择 **none** 作为密钥交换方法。
- 额外密钥交换为可选。

要让提议协商成功，发起方提议中的所有转换都必须与响应方中的转换相匹配。

在以下发起方示例中：

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

响应方必须具有 additional-key-exchange 5 才能匹配提议。

如果对等体不支持额外密钥交换，则会发生以下情况：

- 如果发起方有另一个与响应方提议匹配的 IKEv2 提议，则会建立 IKEv2 SA。
- 对等体将IKE_SA_INIT交换消息中的任何额外密钥交换转换类型视为未知转换类型，并跳过这些提议。协商失败，并会向发起方发送 **NO_PROPOSAL_CHOSEN** 错误通知。

有关此功能的详细信息，请参阅 RFC 9242。

IKEv2 多密钥交换的准则和限制

- 您最多可以有七个多密钥交换。
- 您无法在后续密钥交换中使用相同的 DH 组。

对于此功能，ASA 不支持：

- IKEv1
- 传统密钥交换和基于后量子算法的密钥交换组合。
- 远程访问 VPN。只有站点间 VPN 支持 IKEv2 多密钥交换。
- 集群

为 IKEv2 配置多密钥交换

此配置为可选，如果要保护 IPsec 通信免受量子计算机攻击，则可以执行此配置。

开始之前

- 查看准则和限制。有关详细信息，请参阅IKEv2 多密钥交换的准则和限制，第 7 页。
- 配置 IKEv2 策略的加密算法、散列算法、身份验证方法和 SA 生命周期。有关详细信息，请参阅配置 IKEv1 和 IKEv2 策略。

过程

步骤 1 创建 IKEv2 策略。

crypto ikev2 policy *policy_index*

提示符将显示 IKEv2 策略配置模式。

示例：

```
hostname(config)# crypto ikev2 policy 1
```

步骤 2 为 IKEv2 策略配置额外的密钥交换转换。

additional-key-exchange <*1-7*>

提示符将显示 IKEv2 策略额外密钥交换配置模式。一个策略最多可以配置七个密钥交换转换。

示例：

```
hostname(config-ikev2-policy)# additional-key-exchange 1
```

步骤 3 通过为额外密钥交换转换定义一个或多个 DH 组来配置密钥交换方法。

key-exchange-method <*DH_group*>

将 DH 组指定为 14、15、16、19、20、21 或 31。您还可以将转换配置为 none。如果选择 none，则不会进行密钥交换。

示例：

```
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
```

步骤 4 重复步骤 2 和 3，为 IKEv2 策略配置多个密钥交换。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# additional-key-exchange 1
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
hostname(config-ikev2-policy)# additional-key-exchange 2
hostname(config-ikev2-policy-ake)# key-exchange-method 20 21
hostname(config-ikev2-policy)# additional-key-exchange 3
hostname(config-ikev2-policy-ake)# key-exchange-method 19 20 none
...
```

下一步做什么

确认配置。有关详细信息，请参阅验证 IKEv2 多密钥交换配置 ， 第 9 页。

验证 IKEv2 多密钥交换配置

使用以下显示命令来查看或验证 IKEv2 多密钥交换配置：

- **show running-config crypto ikev2**

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

- **show crypto ikev2 sa detail**

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548
bytes
Parent SA Extended Status:
Delete in progress: FALSE
```

```
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

创建 IKEv1 转换集

IKEv1 转换集由加密方法和身份验证方法组成。在与 ISAKMP 进行 IPsec 安全关联协商期间，对等体同意使用特定转换集来保护特定数据流。转换集对于两个对等体必须相同。

转换集保护关联的加密映射条目中指定的 ACL 的数据流。您可以在 ASA 配置中创建转换集，然后在加密映射条目或动态加密映射条目中指定最多 11 个转换集。

下表列出了有效的加密和身份验证方法。

表 *1:* 有效的加密和身份验证方法

有效加密方法	有效身份验证方法
	esp-sha-hmac（默认）
esp-aes（128 位加密）（默认）	
esp-aes-192	
esp-aes-256	
esp-null	

在通过不可信网络（例如公共互联网）连接的两个 ASA 之间，通常采用隧道模式实施 IPsec。隧道模式是默认模式，无需配置。

如要配置转换集，请在单情景或多情景模式下执行以下站点间任务：

过程

步骤 1 在全局配置模式下，输入 **crypto ipsec ikev1 transform-set** 命令。以下示例使用名称 FirstSet、esp-aes 加密 和 esp-sha-hmac 身份验证来配置转换集。语法如下：

esp-sha-hmac（默认）

crypto ipsec ikev1 transform-set *transform-set-nameencryption-method authentication-method*

```
hostname(config)#
crypto ipsec transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)#
```

步骤 2 保存更改。

```
hostname(config)# write memory
hostname(config)#
```

创建 IKEv2 提议

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。

下表列出了有效的 IKEv2 加密和身份验证方法。

表 *2:* 有效的 *IKEv2* 加密和完整性方法

有效加密方法	有效完整性方法
	sha（默认）
aes（默认）- 使用 128 位密钥的 AES。	
aes-192	
aes-256	

如要配置 IKEv2 提议，请在单情景或多情景模式下执行以下任务：

过程

步骤 1 在全局配置模式下，使用 **crypto ipsec ikev2 ipsec-proposal** 命令进入 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。在以下示例中，secure 是提议的名称：

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

步骤 2 然后，输入协议和加密类型。ESP 是唯一支持的协议。例如：

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

hostname(config-ipsec-proposal)#
```

步骤 3 输入完整性类型。例如：

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

步骤 4 保存更改。

配置 ACL

ASA 使用访问控制列表来控制网络访问。默认情况下，自适应安全设备拒绝所有流量。您需要配置允许流量的 ACL。有关详细信息，请参阅常规操作配置指南中的“有关访问控制列表的信息”。

为此 LAN 间 VPN 控制连接配置的 ACL 基于源 IP 地址和转换的目标 IP 地址以及（可选）端口。配置在连接两端相互镜像的 ACL。

VPN 流量的 ACL 使用转换的地址。

注释 有关使用 VPN 过滤器配置 ACL 的详细信息，请参阅为远程访问指定 VLAN 或对组策略应用统一访问控制规则。

过程

步骤 1 输入 **access-list extended** 命令。

access-list *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

以下示例配置名为 l2l_list 的 ACL，允许来自 192.168.0.0 网络中 IP 地址的流量传送到 150.150.0.0 网络。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)#
```

步骤 2 在连接的另一端为 ASA 配置一个 ACL，对该 ACL 进行镜像。

加密映射中的 ACL 或附加到同一加密映射的两个不同加密 ACL 中定义的子网不得重叠。

在以下示例中，对等体的提示符为 hostname2。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0 192.168.0.0
 255.255.0.0
hostname(config)#
```

定义隧道组

隧道组是包含隧道连接策略的一组记录。您可以配置隧道组来标识AAA服务器，指定连接参数，以及定义默认组策略。ASA 会在内部存储隧道组。

ASA 中有两个默认隧道组：DefaultRAGroup 和 DefaultL2Lgroup，前者是默认的 IPsec 远程访问隧道组，后者是默认的 IPsec LAN 间隧道组。可以修改这些隧道组，但不能将其删除。

IKE 版本 1 和 2 之间的主要差异在于其允许的身份验证方法。IKEv1 在 VPN 两端仅允许一种类型的身份验证（即，预共享密钥或证书）。但是，IKEv2 允许分别使用本地和远程身份验证 CLI 配置不对称身份验证方法（即，对发起方使用预共享密钥身份验证，但对响应方使用证书身份验证）。因此，通过 IKEv2 可使用不对称身份验证，其中一端对一个凭证进行身份验证，另一端使用其他凭证（预共享密钥或证书）。

您也可以根据环境创建一个或多个新隧道组。如果在隧道协商过程中没有标识特定隧道组，ASA 将会使用这两个隧道组来配置远程访问隧道组和 LAN 间隧道组的默认隧道参数。

要建立基本 LAN 间连接，必须为隧道组设置两个属性：

- 将连接类型设置为 IPsec LAN 间。
- 配置 IP 地址的身份验证方法（即用于 IKEv1 和 IKEv2 的预共享密钥）。

过程

步骤 1 要将连接类型设置为 IPsec LAN 间，请输入 **tunnel-group** 命令。

语法为 **tunnel-group** *name* **type** *type*，其中 name 是分配给隧道组的名称，type 是隧道的类型。在 CLI 中输入的隧道类型为：

- **remote-access** （IPsec、SSL 和无客户端 SSL 远程访问）
- **ipsec-l2l** （IPsec LAN 间）

在以下示例中，隧道组的名称是 LAN 间对等体的 IP 地址 10.10.4.108。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

注释
仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用名称非 IP 地址的 LAN 间隧道组。

步骤 2 要将身份验证方法设置为使用预共享密钥，请进入 ipsec-attributes 模式，然后输入 **ikev1pre-shared-key** 命令以创建预共享密钥。需要在此 LAN 间连接的两个 ASA 上均使用同一预共享密钥。

密钥是 1 至 128 个字符的字母数字字符串。

在以下示例中，IKEv1 预共享密钥是 44kkaol59636jnfx：

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

步骤 3 保存更改。

```
hostname(config)# write memory
hostname(config)#
```

如要验证隧道是否启动并正常运行，请使用 **show vpn-sessiondb summary**、**show vpn-sessiondb detail l2l** 或 **show crypto ipsec sa** 命令。

创建加密映射并将其应用于接口

加密映射条目组合 IPsec 安全关联的各种元素，包括以下元素：

- IPsec 应保护的流量（在 ACL 中定义）。
- 将 IPsec 保护的流量发送到的位置（通过标识对等体）。
- 对此流量应用的 IPsec 安全性（由转换集指定）。
- IPsec 流量的本地地址（通过对接口应用加密映射进行标识）。

为使 IPsec 成功，两个对等体均必须包含具有兼容配置的加密映射条目。为使两个加密映射条目兼容，它们必须至少符合以下条件：

- 加密映射条目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，则对等体的加密 ACL 必须“允许”ASA 加密 ACL 中的条目。
- 加密映射条目必须各自标识另一个对等体（除非对应的对等体使用动态加密映射）。
- 加密映射条目必须至少有一个共同的转换集。

如果为给定接口创建多个加密映射条目，请使用每个条目的序号 (seq-num) 将其排名：seq-num 越低，优先级越高。在设置有加密映射的接口上，ASA 先按照优先级较高的映射条目评估流量。

如果反向路由注入 (RRI) 被应用于加密映射，则该映射对于 ASA 上的一个接口必须是唯一的。换而言之，同一加密映射不能被应用于多个接口。如果将多个加密映射应用于多个接口，则可能无法正确清除路由。如果多个接口需要加密映射，则每个路由都必须使用唯一定义的映射。

如果存在以下任意情况，请为给定接口创建多个加密映射条目：

- 不同对等体处理不同数据流。
- 您想要将不同的 IPSec 安全应用于不同类型的流量（面向相同或不同的对等体），例如您希望对一组子网之间的流量进行身份验证，而对另一组子网之间的流量同时进行身份验证和加密。

在此情况下，请在两个单独的 ACL 中定义不同类型的流量，并为每个加密 ACL 创建单独的加密映射条目。

在多个接口上应用加密映射

对于双 ISP，您可以将加密映射应用于 ASA 上的外部接口和备份接口。在使用此配置时，仅发起选项不可用。如果需要此冗余，则您必须使用 Virtual Tunnel Interface (VTI)。

在多个接口上使用加密映射时：

- 您必须有路由协议或路由跟踪。
- 确保远程端也使用路由协议。
- 您必须为同一个加密映射谨慎选择多个接口，因为ASA 允许来自具有较低首选路由的接口上的远程站点的连接。

如要在全局配置模式下创建加密映射并将其应用于外部接口，请在单情景或多情景模式下执行以下步骤：

过程

步骤 1 要将 ACL 分配到加密映射条目，请输入 **crypto map match address** 命令。

语法为 **crypto map** map-name seq-num **match address** aclname。在以下示例中，映射名称为 abcmap，序号为 1，ACL 名称为 **l2l_list**。

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

步骤 2 要标识 IPsec 连接的对等体，请输入 **crypto map set peer** 命令。

语法为 **crypto map** map-name seq-num **set peer** {ip_address1 | hostname1}[... ip_address10 | hostname10]。在以下示例中，对等体名称为 10.10.4.108。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

步骤 3 要为加密映射条目指定 IKEv1 转换集，请输入 **crypto map ikev1 set transform-set** 命令。

语法为 **crypto map** map-name seq-num **ikev1 set transform-set** transform-set-name。在以下示例中，转换集名称为 FirstSet。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

步骤 4 如要为加密映射条目指定 IKEv2 提议，请输入 crypto map ikev2 set ipsec-proposal 命令：

语法为 **crypto map** map-name seq-num set **ikev2 ipsec-proposal proposal-name**。在以下示例中，提议名称为 secure。

通过 **crypto map** 命令，可以为单个映射索引指定多个 IPsec 提议。在该情况下，多个提议会在协商过程中传输到 IKEv2 对等体，并且提议的顺序由管理员在加密映射条目排序时确定。

注释
如果 IPsec 提议中存在组合模式 (AES-GCM/GMAC) 和普通模式（所有其他类型）算法，则无法将单个提议发送到对等体。在此情况下必须具有至少两个提议，一个用于组合模式算法，另一个用于普通模式算法。

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

将加密映射应用于接口

您必须对 IPsec 流量经过的每个接口应用加密映射集。ASA 在所有接口上都支持 IPsec。对接口应用加密映射集将命令 ASA 按照该加密映射集评估所有接口流量，并在连接或安全关联协商期间使用指定的策略。

将加密映射绑定到接口还会初始化运行时数据结构，例如安全关联数据库和安全策略数据库。今后以任何方式修改加密映射时，ASA 都会自动将更改应用于运行配置。它将断开任何现有连接，并在应用新的加密映射后重新建立这些连接。

如要将已配置的加密映射应用于外部接口，请执行以下步骤：

过程

步骤 1 输入 **crypto map interface** 命令。语法为 **crypto map** map-name **interface** interface-name。

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

步骤 2 保存更改。

```
hostname(config)# write memory
hostname(config)#
```

动态站点间 VPN 概述

在动态站点间 VPN 中，环回接口用作 VPN 隧道的源和目标。您可以使用这些接口在安全网关之间移动站点到站点对等体，而无需更新对等体。当环回地址通过路由协议传播时，ASA 会将流量从远程对等体无缝重定向到新的安全网关集群，而无需更改对等体上的配置。

注释 此功能不适用于评估许可证。

在动态站点间 VPN 中使用环回接口的优势

- 冗余：在物理链路或接口发生故障期间，由于环回接口仍可通过多个物理接口访问，因此 VPN 连接保持存在。在集群中，如果具有环回接口的节点发生故障，则接口和会话将转移到备用节点。
- 动态环回地址重新分配：将环回地址重新分配给其他安全网关集群期间会保留 VPN 连接，而无需更改远程对等体。
- 动态路径选择 (Dynamic Path Selection)：当路由协议动态选择站点之间的最佳路径时，VPN 连接会得到优化，从而提高性能和可靠性。

使用具有环回接口的动态 VPN 的前提条件

一般前提条件

此功能受以下支持：

- Cisco Secure Firewall 4200 系列版本 9.24.1
- 第 2 层集群
- 与动态加密映射附加的静态加密映射。

许可证前提条件

此功能需要许可证：

- 具有强加密的基础许可证。
- 分布式 VPN 模式的运营商许可证。

使用环回接口配置动态站点间 VPN

开始之前

确保您查看 使用具有环回接口的动态 VPN 的前提条件，第 17 页。

过程

步骤 1 使用 **interface** 命令配置外部接口：

a) 使用 **nameif** 命令配置环回接口的名称。
b) 使用 security-level 命令配置 **安全级别** 。
c) 使用 **ip address** 命令来配置接口的 IP 地址。

示例：

```
hostname(config)# interface ethernet0/0
hostname(config-if)#nameif outside
hostname(config-if)#security-level 0
hostname(config-if)#ip address 192.0.2.17 255.255.255.0
```

步骤 2 使用 **interface** 命令配置第 2 层环回接口：

a) 使用 **description** 命令配置说明。
b) 使用 **nameif** 命令配置环回接口的名称。
c) 使用 **ip address** 命令来配置环回接口的 IP 地址。

示例：

```
hostname(config)# interface Loopback2
hostname(config-if)#description Loopback to terminate Group 2
hostname(config-if)#nameif LB2
hostname(config-if)#ip address 209.165.201.1 255.255.255.252
```

步骤 3 使用 **crypto ipsec ikev2 ipsec-proposal** *proposal tag* 命令配置 IKEv2 IPsec 提议：

a) 使用 **description** 命令配置说明。
b) 使用 **protocol esp encryption** 命令配置加密协议。
c) 使用 **protocol esp integrity** 命令配置加密和完整性协议。

示例：

```
hostname(config)#crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
hostname(config-ipsec-proposal)#protocol esp encryption aes
hostname(config-ipsec-proposal)#protocol esp integrity sha-256
```

步骤 4 使用 **crypto ikev2 policy** *policy_index*命令配置 IKEv2 策略：

a) 使用 **protocol esp encryption** 命令配置加密协议。
b) 使用 **protocol esp integrity** 命令配置加密和完整性协议。
c) 使用 **group** 命令来配置 Diffie-Hellman 群。
d) 使用 **prf** 命令配置伪随机函数 (PRF) 该伪随机函数用作导出密钥材料和 IKEv2 隧道加密所需的哈希操作的算法。
e) 使用 **生命周期** 命令配置加密钥的生命周期。

示例：

```
hostname(config)#crypto ikev2 policy 1
hostname(config-ikev2-policy)#protocol esp encryption aes-256
hostname(config-ikev2-policy)#protocol esp integrity sha
hostname(config-ikev2-policy)#group 5
hostname(config-ikev2-policy)#prf sha
hostname(config-ikev2-policy)#lifetime seconds 86400
```

步骤 5 创建动态加密映射

a) 使用 **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set ikev2 ipsec-proposal** *transform-set-name1* 命令配置动态加密映射并为该映射指定 IKEv2 转换集。

b) 使用 **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set reverse-route** 命令根据此加密映射条目为任何连接启用反向路由注入。

示例：

```
hostname(config)#crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
hostname(config)#crypto dynamic-map dmap 1 set reverse-route
```

步骤 6 配置静态加密映射：

a) 使用 **crypto map** *map-name sequence-num* **ipsec-isakmp dynamic** *dynamic-map-name* 命令将动态加密映射集添加到静态加密映射集中。

b) 使用 **crypto map** *map-name* **interface** *loopback_interface* 命令将静态加密映射应用到环回接口。

示例：

```
hostname(config)#crypto map vpn 1 ipsec-isakmp dynamic dmap
hostname(config)#crypto map vpn interface LB2
```

步骤 7 配置默认 LAN 间隧道组：

a) 使用 **tunnel-group DefaultL2LGroup ipsec-attributes** 命令配置默认 LAN 到 LAN 隧道组的 IPsec IKEv2 属性。

b) 使用 **ikev2 remote-authentication pre-shared-key** *key* 命令配置用于对远程对等体进行身份验证的预共享密钥 (PSK)。

c) 使用 **ikev2 local-authentication pre-shared-key** *key* 命令配置用于对本地设备进行身份验证的预共享密钥。

示例：

```
hostname(config)#tunnel-group DefaultL2LGroup ipsec-attributes
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key ****
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key ****
```

步骤 8 在环回接口上使用 **crypto ikev2 enable** *loopback_interface* 命令启用 IKEv2：

示例：

```
hostname(config)#crypto ikev2 enable LB2
```

步骤 9 配置路由协议以通告环回接口。

示例：

配置 OSPF 示例:

```
hostname(config)#router ospf 1
hostname(config-router)#network 203.0.113.0 255.255.255.0 area 0
hostname(config-router)#network 209.165.201.1 255.255.255.252 area 0
hostname(config-router)#log-adj-changes
hostname(config-router)#redistribute connected

hostname(config)#interface outside
hostname(config-interface)#ospf cost 1
hostname(config-interface)#ospf message-digest-key 1 md5 *****
hostname(config-interface)#ospf authentication message-digest
```

验证动态站点间 IPsec VPN 配置。

使用以下显示命令来验证动态站点间 VPN（使用环回接口）配置：

显示 vpn-sessiondb

```
asa-node2/data-node# show vpn-sessiondb det l2l

Session Type: LAN-to-LAN Detailed

Connection   : DefaultL2LGroup
Index        : 399                    IP Addr      : <Peer-IP>
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv2: (1)SHA256  IPsec: (1)SHA256
Bytes Tx     : 58680                  Bytes Rx     : 86152
Login Time   : 09:59:41 EDT Tue Apr 8 2025
Duration     : 0h:01m:21s
Session State: Cluster Owner (backup is asa-node1)

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 399.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES128                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86319 Seconds
  PRF          : SHA256                 D/H Group    : 14
  Filter Name  : trace

IPsec:
  Tunnel ID    : 399.2
  Local Addr   : 209.165.201.1 255.255.255.0/0/0
  Remote Addr  : 192.0.2.20 255.255.255.0/0/0
  Encryption   : AES128                 Hashing      : SHA256
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28715 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 58680                  Bytes Rx     : 86152
  Pkts Tx      : 978
```

显示 crypto ikev2

```
asa-node2/data-node# show crypto ikev2 sa
IKEv2 SAs:
Session-id:399, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                         Remote
fvrf/ivrf     Status         Role
   724781 209.165.201.1/500           192.0.2.20/500
Global/Global      READY    RESPONDER

   ...
```

show crypto ipsec sa

```
asa-node2/data-node# show crypto ipsec sa

interface: LB2
```

验证动态站点间 IPsec VPN 配置。

```
 Crypto map tag: dyn-loop1, seq num: 65535, local addr: 209.165.201.1
...
```

验证动态站点间 **IPsec VPN** 配置。

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。