Virtual Tunnel Interface

本章介绍如何配置 VTI 隧道。

关于 Virtual Tunnel Interface

ASA 支持称为 Virtual Tunnel Interface (VTI) 的逻辑接口。作为策略型 VPN 的替代方案，您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。您可以使用动态或静态路由。VTI 的出口流量经加密发送至对等体，而关联的 SA 会解密 VTI 的进口流量。

使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。您不再需要跟踪所有远程子网并将其包含在加密映射访问列表中。这可以简化部署，而且静态 VTI 通过动态路由协议支持基于路由的 VPN，还能满足虚拟私有云的诸多要求。

静态 VTI

您可以使用静态 VTI 配置进行站点间连接，其中两个站点之间的隧道会始终在线。对于静态 VTI 接口，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要创建静态 VTI 接口，请参阅添加 VTI 接口，第 8 页。

动态 VTI

动态 VTI 为站点间 VPN 提供高度安全且可扩展的连接。动态 VTI 简化了大型企业中心辐射型部署的对等体配置。单个动态 VTI 可以替换中心上的多个静态 VTI 配置。您可以将新的分支添加到中心，而无需更改中心配置。动态 VTI 取代动态加密映射和用于建立隧道的动态中心辐射型方法。在管理中心，动态 VTI 仅支持中心辐射型拓扑。

动态 VTI 会使用虚拟模板来进行 IPsec 接口的动态实例化和管理。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。动态 VTI 支持多个 IPsec 安全关联，并接受分支提议的多个 IPsec 选

择器。动态 VTI 也支持动态 (DHCP) 分支。要创建动态 VTI 接口，请参阅添加动态 VTI 接口，第 11 页。

ASA 如何为 VPN 会话创建动态 VTI 隧道

1. 在 ASA 上创建虚拟模板 (**interface virtual-Template** *template_number* **type tunnel**)。

   您可以将此模板用于多个 VPN 会话。
2. 将此模板附加到隧道组。您可以将虚拟模板连接到多个隧道组。
3. 分支会向中心发起隧道请求。
4. 中心对分支进行身份验证。
5. ASA 使用虚拟模板来为与分支的 VPN 会话动态创建虚拟访问接口。
6. 中心会使用虚拟接入接口与分支建立动态 VTI 隧道。
7. 配置 IKEv2 路由集接口命令，以通告 VTI 接口 IP over IKEv2 交换。此选项可在 VTI 接口之间启用单播可访问性，以便 BGP 或路径监控通过隧道运行。
8. 在 VPN 会话结束后，隧道将断开连接，中心将删除相应的虚拟接入接口。

Virtual Tunnel Interface 准则

情景模式和集群

- 仅支持单一模式。
- 不支持集群。

防火墙模式

仅在路由模式中受支持。

BGP IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 BGP 路由。

EIGRP 支持

支持 VTI 上的 IPv4 和 IPv6 EIGRP 路由。

OSPF IPv4 和 IPv6 支持

支持 VTI 上的 IPv4 和 IPv6 OSPF 路由。

IPv6 支持

- 可以配置 IPv6 寻址的 VTI。

- VTI 的隧道源和隧道目标都可以有 IPv6 地址。
- 支持以下 VTI IP（或内部网络 IP 版本）与公共 IP 版本的组合：
  - IPv6 over IPv6
  - 基于 IPv6 的 IPv4
  - IPv4 over IPv4
  - 基于 IPv4 的 IPv6
- 仅支持将静态 IPv6 地址作为隧道源和目的地址。
- 隧道源接口可以有一个 IPv6 地址，并且您可以将该地址指定用作隧道终端。如果不指定，列表中的第一个 IPv6 全局地址会被默认用作隧道终端。
- 您可以将隧道模式指定为 IPv6。如已指定，则 IPv6 流量可以通过 VTI 进行隧道传输。但是，单个 VTI 的隧道模式可以是 IPv4 或 IPv6。

常规配置准则

- 如果在 LAN 到 VPN VPN 中使用动态加密映射和动态 VTI，则仅会出现动态 VTI 隧道。出现此问题的原因是，加密映射和动态 VTI 都尝试使用默认隧道组。

  我们的建议操作如下动作之一：
  - 将 LAN 间 VPN 迁移到动态 VTI。
  - 使用静态加密映射及其自己的隧道组。
- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 您可以将静态、BGP、OSPF 或 EIGRP IPv4 路由用于使用这种隧道接口的流量。
- 对于静态和动态 VTI，请确保不将借用 IP 接口用作任何 VTI 接口的隧道源 IP 地址。
- VTI 的 MTU 将根据底层物理接口自动设置。但是，如果在启用 VTI 后更改物理接口 MTU，则您必须禁用并重新启用 VTI 才能使用新的 MTU 设置。
- 对于动态 VTI，虚拟接入接口会从配置的隧道源接口继承 MTU。如果不指定隧道源接口，虚拟接入接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。
- 您最多可以在一台设备上配置 1024 个 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。
  - 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，如果型号支持 5510 VLAN，则隧道计数为 500 减去配置的物理接口数。
- VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目的地址之间收发数据。

- 如果必须应用 NAT，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于站点间隧道组中的 IKEv1，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，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- VTI 接口之间支持 ICMP ping。
- 如果 IKEv2 站点间 VPN 隧道的对等设备发送 IKEv2 配置请求负载，则 ASA 无法与该设备建立 IKEv2 隧道。您必须在对等设备上禁用 config-exchange 请求，ASA 才能与对等设备建立 VPN 隧道。
- 动态 VTI 支持 HA 和 IKEv2。

默认设置

- 默认情况下，通过 VTI 的所有流量都经过加密。
- 默认情况下，VTI 接口的安全级别为 0。您无法配置安全级别。

VTI 的限制

ASA 会在 VTI 解密后丢弃安全组标签 (SGT) 帧和数据包。

动态 VTI 不支持：

- ECMP 和 VRF
- 集群
- IKEv1
- QoS

对于动态 VTI，如果未指定隧道源，IKEv2 将在设备的所有接口上启用，管理专用接口和故障转移接口除外。

创建 VTI 隧道

要配置 VTI 隧道，请创建 IPsec 提议（转换集）。您需要创建引用该 IPsec 提议的 IPsec 配置文件，然后使用该 IPsec 配置文件创建 VTI 接口。使用相同 IPsec 提议和 IPsec 配置文件参数配置远程对等体。SA 协商将在所有隧道参数配置完后开始。

注释 对于同时属于两个 VPN VTI 域并且物理接口上存在 BGP 邻接关系的 ASA：

因接口运行状况检查而触发状态更改时，系统将删除物理接口中的路由，直至与新的活动对等体重新建立 BGP 邻接关系。此操作不适用于 VTI 逻辑接口。

可以在 VTI 接口上应用访问控制列表来控制通过 VTI 的流量。如要在不检查源和目标接口的 ACL 的情况下允许来自 IPsec 隧道的所有数据包，请在全局配置模式下输入 sysopt connection permit-vpn 命令。

您可以使用以下命令在不检查 ACL 的情况下允许 IPsec 流量通过 ASA：

hostname(config)# sysopt connection permit-vpn

当外部接口和 VTI 接口的安全级别为 0 时，如果您在 VTI 接口上应用了 ACL，并且尚未配置 same-security-traffic，则不会命中该接口。

要配置此功能，请在全局配置模式下使用 **same-security-traffic** 命令及其 **intra-interface** 参数。

有关详细信息，请参阅允许接口内流量 (Hairpinning)。

过程

步骤 1 添加 IPsec 提议（转换集）。

步骤 2 添加 IPsec 配置文件。

步骤 3 添加 VTI 隧道。

添加 IPsec 提议（转换集）

为了保护 VTI 隧道中的流量，需要使用转换集。转换集作为 IPsec 配置文件的一部分使用，是安全协议和算法的集合，用于保护 VPN 中的流量。

开始之前

- 可以使用预共享密钥或证书对与 VTI 关联的 IKE 会话进行身份验证。IKEv2 允许使用不对称身份验证方法和密钥。对于 IKEv1 和 IKEv2，必须在用于 VTI 的隧道组下配置预共享密钥。
- 对于使用 IKEv1 的基于证书的身份验证，必须指定要在发起方使用的信任点。对于响应方，必须在 tunnel-group 命令中配置信任点。对于 IKEv2，必须同时在发起方和响应方的 tunnel-group 命令下配置用于身份验证的信任点。

过程

添加 IKEv1 转换集或 IKEv2 IPsec 提议以建立安全关联。

要添加 IKEv1 转换集，请使用以下命令：

crypto ipsec ikev1 transform-set {*transform-set-name* | *encryption* | *authentication*}

示例：

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

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-md5-hmac — 使用 MD5/HMAC-128 作为散列算法。
- esp-sha-hmac — 使用 SHA/HMAC-160 作为散列算法。
- esp-none — 不进行 HMAC 身份验证。

添加 IKEv2 IPsec 提议。

注释
对于 IOS 平台，请在 IKEv2 配置文件配置模式下使用 **no config-exchange request** 命令来禁用配置交换选项。有关详细信息，请参阅http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280。

- 指定 IPsec 提议名称：

  crypto ipsec ikev2 ipsec-proposal *IPsec proposal name*

示例：

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- 在 crypto IPsec ikev2 ipsec-proposal 配置模式下指定安全参数：

  protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} | integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}

示例：

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

添加 IPsec 配置文件

IPsec 配置文件包含其引用的 IPsec 提议或转换集中所需的安全协议和算法。这能够确保两个站点间 VIT VPN 对等体之间存在安全的逻辑通信路径。

过程

步骤 1 设置配置文件名称：

crypto ipsec profile *name*

示例：

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

步骤 2 设置 IKEv1 或 IKEv2 提议。可以选择 IKEv1 转换集或 IKEv2 IPsec 提议。

a) 设置 IKEv1 转换集。

- 要设置 IKEv1 提议，请在 crypto ipsec profile 命令子模式下输入以下命令：

  set ikev1 transform set *set_name*

  在本示例中，SET1 是先前创建的 IKEv1 提议集。

  ```
  ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
  ```

b) 设置 IKEv2 提议。

- 要设置 IKEv2 提议，请在 crypto ipsec profile 命令子模式下输入以下命令：

  set ikev2 ipsec-proposal *IPsec_proposal_name*

  在本示例中，SET1 是先前创建的 IKEv2 IPsec 提议。

  ```
  ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
  ```

步骤 3 （可选）指定安全关联的持续时间：

set security-association lifetime { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

示例：

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

步骤 4 （可选）将 VTI 隧道端部配置为仅用作响应方：

responder-only

- 可以将 VTI 隧道的一端配置为仅用作响应方。仅响应方端不会发起隧道或重新生成密钥。
- 如果使用的是 IKEv2，请设置安全关联生命周期的持续时间，此值应大于发起方端的 IPsec 配置文件中的生命周期值。这是为了方便发起方端成功地重新生成密钥，并确保隧道保持活动状态。
- 如果使用的是 IKEv1，IOS 应始终处于仅响应方模式，这是因为 IOS 不支持连续通道模式。ASA 将成为会话发起方并重新生成密钥。

- 如果发起方端的重新生成密钥配置未知，请删除仅响应方模式以便双向建立SA，或在仅响应方端配置无限 IPsec 生命周期值以防止到期。

步骤 5 （可选）指定 PFS 组。完美前向保密 (PFS) 为每个加密交换生成唯一会话密钥。此唯一会话密钥可保护交换免于后续解密。要配置 PFS，必须选择在生成 PFS 会话密钥时要使用的 Diffie-Hellman 密钥导出算法。该密钥导出算法将生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上的 Diffie-Hellman 组必须匹配。

set pfs { **group14** }

示例：

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

步骤 6 （可选）指定用于定义发起 VTI 隧道连接时要使用的证书的信任点。

set trustpoint *name*

示例：

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

步骤 7 （可选）为此 IPsec 配置文件启用反向路由注入 (RRI)，并将反向路由设置为动态。

set reverse-route [dynamic]

示例：

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

添加 VTI 接口

要创建新 VTI 接口并建立 VTI 隧道，请执行以下步骤：

注释 实施IP SLA，确保当活动隧道中的路由器不可用时，隧道仍保持活动状态。请参阅《ASA 常规操作配置指南》(http://www.cisco.com/go/asa-config) 中的“配置静态路由跟踪”。

过程

步骤 1 创建新的隧道接口：

interface tunnel *tunnel_interface_number*

指定 0 到 10413 范围内的隧道 ID。最多可支持 10413 个 VTI 接口。

示例：

```
ciscoasa(config)#interface tunnel 100
```

步骤 2 输入 VTI 接口的名称。

在 **interface tunnel** 命令子模式下输入以下命令：

nameif *interface name*

示例：

```
ciscoasa(config-if)#nameif vti
```

步骤 3 输入 VTI 接口的 IP 地址。

ip address *IP addressmask*

示例：

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

步骤 4 输入虚拟模板继承的接口的 IPv4 或 IPv6 地址。

您还可以选择物理接口或设备上配置的环回接口。从虚拟模板克隆的所有虚拟访问接口都将具有相同的 IP 地址。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

示例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

步骤 5 指定隧道源接口。

tunnel source interface *interface_name*

源接口可以是物理接口或环回接口。

示例：

```
ciscoasa(config-if)#tunnel source interface outside
```

步骤 6 指定隧道目标 IP 地址。

tunnel destination *ip_address*

示例：

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

步骤 7 使用隧道模式 IPsec IPv4 配置隧道。

tunnel mode ipsec *ipv4*

示例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

步骤 8 将 IPsec 配置文件分配给隧道。

tunnel protection ipsec *IPsec profile*

示例：

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

步骤 9 为静态 VTI 接口分配一个流量选择器。

tunnel protection policy *acl_name*

访问列表可以包含单个或多个列表选择器。如果不配置此命令，静态 VTI 接口将默认建议使用任意到任意选择器。

示例：

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225 255.255.255.224
 any
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

示例

ASA 与 IOS 设备之间的 VTI 隧道（采用 IKEv2）配置示例：

```
ASA□

crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 □ 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]


IOS□

!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 □ 21
!
```

```
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
 ip address 10.10.10.0 255.255.255.254
 tunnel mode ipsec ipv4
 tunnel source [router-interface]
 tunnel destination [asa-ip-address]
 tunnel protection ipsec profile asa-vti
!
```

添加动态 VTI 接口

要为动态 VTI 创建虚拟模板，请执行以下操作：

注释 实施 IP SLA，确保当活动隧道中的路由器不可用时，隧道仍保持活动状态。请参阅《ASA 常规操作配置指南》中的“配置静态路由跟踪”，地址是：http://www.cisco.com/go/asa-config。

开始之前

确保您已配置 IPsec 配置文件和 IP 未编号接口。

过程

步骤 1 创建新的虚拟模板：

interface virtual-Template *template_number* **type tunnel**

template_number 是虚拟模板的唯一编号。范围为 1 到 10413。

接口模板不得处于关闭状态。以下是虚拟模板的必填参数：

- 接口名称
- 隧道 IPsec 模式

- 隧道 IPsec 配置文件

示例：

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

步骤 2 指定动态 VTI 虚拟模板接口的名称。

在 **interface** 配置模式下输入以下命令：

nameif *interface_name*

ASA 会动态创建虚拟访问接口为 <*Virtual_Template_name*>_va<*n*>。例如，如果虚拟模板的名称为 dVTI101，则虚拟访问接口将为 dVTI101_va1、dVTI101_va2，以此类推。如果要修改虚拟模板，必须使用 **shutdown** 命令来关闭虚拟模板。

示例：

```
ciscoasa(config-if)#nameif dVTI101
```

步骤 3 配置虚拟模板继承的接口的 IPv4 或 IPv6 地址。

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

虚拟模板可以继承设备上配置的任何物理接口的 IP 地址或环回地址。从虚拟模板克隆的所有虚拟访问接口都将具有相同的 IP 地址。

示例：

```
ciscoasa(config-if)#ip unnumbered loopback1
```

步骤 4 （可选）指定隧道源接口。

tunnel source interface *interface_name*

源接口可以是物理接口或环回接口。

ASA 仅接受来自配置为隧道源 IP 地址的接口的 VPN 会话请求。如果没有指定该接口，ASA 将接受从任何接口接收的 VPN 会话请求。虚拟访问接口会从配置的隧道源接口继承 MTU。如果没有启用上述选项，虚拟访问接口将从源接口继承 MTU，而 ASA 会从该接口接受 VPN 会话请求。

示例：

```
ciscoasa(config-if)#tunnel source interface outside1
```

步骤 5 将隧道保护模式指定为 IPv4 或 IPv6。

tunnel mode ipsec {**ipv4** | **ipv6**}

示例：

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

步骤 6 将 IPsec 配置文件分配给隧道。

tunnel protection ipsec profile *ipsec_profile*

此 IPsec 配置文件会配置协商交换所需的 IPSec/IKE 参数。

示例：

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

步骤 7 将虚拟模板附加到隧道组。

tunnel-group *tunnel_group_name* **type** *type*

tunnel-group *tunnel_group_name* **ipsec-attributes**

virtual-template *template_number*

您可以将同一虚拟模板连接到多个隧道组。ASA 会使用虚拟模板来为每个 VPN 会话创建单独的虚拟访问接口。

示例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

步骤 8 为隧道组启用动态路由。

tunnel-group *tunnel_group_name* **ipsec-attributes**

ikev2 route accept any

ikev2 route set interface

ikev2 route accept any 命令允许 ASA 接受在 IKEv2 交换期间收到的任何隧道接口 IP 地址。 默认情况下，此选项处于已启用状态。

ikev2 route set interface 命令允许 ASA 在 IKEv2 交换期间发送隧道接口 IP 地址。 此选项可在 VTI 接口之间启用单播可访问性，以便 BGP 通过隧道运行。

使用 BGP/OSPF/EIGRP 为隧道组启用动态路由。在配置虚拟模板后，您必须配置路由策略，以便通过 VTI 隧道来路由设备之间的动态 VTI 流量。您还必须配置访问控制规则以允许已加密的流量。

示例：

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

Virtual Tunnel Interface 的功能历史记录

功能名称	版本	功能信息
动态 Virtual Tunnel Interface 支持	9.19(1)	您可以创建动态 VTI 并使用它在中心辐射型拓扑配置基于路由的站点间 VPN。动态 VTI 简化了大型企业中心辐射型部署的对等体配置。单个动态 VTI 可以替换中心上的多个静态 VTI 配置。您可以将新的分支添加到中心，而无需更改中心配置。 新增/修改的命令：**interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy**

功能名称	版本	功能信息
OSPF IPv4 和 IPv6 支持	9.19(1)	支持 VTI 上的 OSPF IPv4 和 IPv6 路由协议。
EIGRP 支持	9.19(1)	支持 VTI 上的 EIGRP IPv4 和 IPv6 路由协议。
静态和动态 VTI 的环回接口支持	9.19(1)	现在，您可以将环回接口设置为 VTI 的源接口。还添加了支持以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。 新增/修改的命令：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**
本地隧道 ID 支持	9.17(1)	ASA 支持唯一本地隧道 ID，它允许 ASA 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。 新增/修改的命令： **local-identity-from-cryptomap** 、
在静态 VTI 上支持 IPv6	9.16（1）	ASA 在 Virtual Tunnel Interface (VTI) 配置中支持 IPv6 地址。 VTI 隧道源接口可以具有 IPv6 地址，您可以将其配置为用作隧道终端。如果隧道源接口有多个 IPv6 地址，您可以指定要使用的地址，否则默认使用列表中的第一个 IPv6 全局地址。 隧道模式可以是 IPv4 或 IPv6，但必须与 VTI 上配置的 IP 地址类型相同，隧道才能处于活动状态。IPv6 地址可以分配给 VTI 中的隧道源或隧道目标接口。 新增/修改的命令：**tunnel source interface**、**tunnel destination**、**tunnel mode**
支持每个设备 1024 个 VTI 接口	9.16（1）	要在设备上配置的最大VTI数量已从 100 增加到 1024。 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，ASA 5510 支持 100 个VLAN，隧道计数为 100 减去配置的物理接口数。 新增/修改的命令：无
VTI 上的 DHCP 中继服务器支持	9.14(1)	ASA 允许将 VTI 接口配置为 DHCP 中继服务器连接接口。 修改了以下命令：**dhcprelay server** *ip_address vti_ifc_name*。
VTI 中支持 IKEv2、基于证书的身份验证和 ACL	9.8.(1)	Virtual Tunnel Interface (VTI) 现在支持 BGP（静态 VTI）。现在可在独立和高可用性模式下使用 IKEv2。可以通过在 IPsec 配置文件中设置信任点来使用基于证书的身份验证。还可以使用 access-group 命令，将 VTI 上的访问列表应用于过滤进口流量。 在 IPsec 配置文件配置模式下引入了以下命令：**set trustpoint**。
Virtual Tunnel Interface (VTI) 支持	9.7.(1)	使用新的逻辑接口（称为 Virtual Tunnel Interface (VTI)）可增强 ASA，该接口用于向对等体表示 VPN 隧道。这可通过将 IPSec 配置文件连接到隧道的每一端，为基于 VPN 的路由提供支持。使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。 引入了以下命令：**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。

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。