在FMC托管FTD上配置基于路由的站点到站点VPN

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 静态VTI与动态VTI

限制和限制

- 一般VTI限制(FTD)
- 路由协议支持（7.x — 从6.7更新）
- IPv6（7.x — 从6.7更新）
- 动态VTI附加限制(7.3+)
- NAT、QoS和策略
- 弱加密算法
- 许可

FMC的配置步骤

- 实验演示值
- 步骤1.打开站点到站点VPN
- 步骤2.添加VPN拓扑
- 步骤3.拓扑名称、类型和IKE版本
- 步骤4.选择FTD设备和VTI
- 步骤5.创建静态虚拟隧道接口
- 步骤6.确认VTI创建
- 步骤7.配置对等体（节点B — 外联网）
- 步骤8. IKE选项卡 — 选择或创建IKE策略
- 步骤9.（可选）创建IKEv2策略
- 步骤10. IKE身份验证
- 步骤11. IPsec选项卡 — IPsec建议案
- 步骤12.（可选）创建IKEv2 IPsec提议
- 步骤13.选择IPsec提议
- 步骤14.完全向前保密和生命期
- 步骤15.保存VPN拓扑
- 步骤16.配置访问控制策略（必填）
- 步骤17.通过VTI添加静态路由
- 步骤18.部署配置

部署后的CLI示例

验证

从FMC GUI
从FTD CLI
故障排除快速参考
相关文档
修订历史纪录
文档应用于

简介

本文档介绍如何在由FMC管理的Cisco Secure FTD上配置基于静态路由的站点到站点VPN隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- FMC Web UI（设备、策略、部署）的导航
- 基本IPsec站点到站点VPN操作（IKE阶段1/2，隧道建立）
- FTD上的静态路由（对于基于动态路由的设计，可以选择使用BGP/OSPF/EIGRP）

使用的组件

基于路由的VPN使用虚拟隧道接口(VTI)和路由（静态或动态）而不是加密ACL来确定加密哪些流量。本文档重点介绍静态VTI(SVTI)点对点或外联网对等互联。有关可扩展的中心辐射型设计，请参阅本文结尾部分列出的相关文档中的动态VTI(DVTI)。

示例中使用的实验版本：

组件	version
Cisco Secure Firewall Management Center	7.4或更高版本（与7.6兼容的示例）

组件	version
思科安全防火墙威胁防御	7.4或更高版本（与7.6兼容的示例）

FTD 6.7上引入了基于静态VTI路由的VPN，DVTI扩展路由协议支持IPv6 VTI及更高版本，VTI规模要求FTD 7.3+/FMC 7.3+。版本特定差异在“限制和限制”部分中列出。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

基于路由的VPN（基于VTI）加密路由到隧道接口的流量。与基于策略的（加密映射）VPN不同，头端的ACL不选择唯一流量。相反，路由表会将流量定向到VTI。对于静态VTI，IPsec流量选择器实际上是任意点对点的（IPv4为0.0.0.0/0.0.0.0）。 任何路由到隧道接口的数据包都会被加密，无论其源/目标子网如何，都受对等体上的访问控制和路由限制。

基于策略的VPN仍然使用显式代理ID/加密ACL。基于路由的VPN优先用于：

- 隧道上的动态路由(BGP、OSPF、EIGRP)
- 云连接(AWS、Azure、GCP)
- 简化的加密域管理
- 从传统加密映射设计迁移

静态VTI与动态VTI

类型	使用案例	FTD最小值
静态VTI(SVTI)	点对点、外联网对等点、中心辐射型辐条	6.7
动态VTI(DVTI)	具有多个辐条的集线器（集线器上的单个虚拟模板）	7.3

本文档逐步介绍SVTI。有关使用多SA的DVTI中心辐射点，请参阅在安全防火墙上使用多SA配置DVTI（文档ID 220322。）

限制和限制

查看FMC设备配置指南 — 站点到站点VPN/VTI指南中适用于您的FMC版本的当前平台限制。除非另有说明，下一节中的摘要反映的是FMC/FTD 7.4-7.6。

一般VTI限制(FTD)

限制	详细信息
通道模式	仅IPsec。FTD上不支持基于VTI的GRE。
防火墙模式	仅在路由模式下支持VTI。
集群	FTD集群部署不支持VTI。
HA（主用/备用）	FTD HA（高可用性）对支持静态VTI。HA中通过VTI的动态路由：备用设备可能未通过主用设备IP创建的VTI隧道到达子网（相应地规划路由）。 对于HA中超过400个VTI，请将设备保持时间设置为45秒。
扩展	每台设备最多1024个静态和动态VTI(7.x)。 原始6.7文档引用了每个接口100个VTI;当前指南为每台设备1024个，确保您根据您的平台和版本进行验证。
IPSec 配置文件	最多20个唯一IPsec配置文件（静态VTI）。
sysopt connection permit-vpn	不适用于基于路由的VPN。您必须为两个方向的已解密流量配置访问控制策略(ACP)规则。
平台设置	平台设置中的SNMP或系统日志选择不支持VTI隧道接口。
远程访问 VPN	VTI接口不能用作远程访问VPN策略的网络接口。

路由协议支持（7.x — 从6.7更新）

原始FTD 6.7文档仅说明BGP。当前FTD支持通过VTI的以下路由方法：

协议	支持
静态路由	Yes
调试输出中显示“BGP	IPv4 和 IPv6
OSPF	OSPFv2和OSPFv3
EIGRP	IPv4

BGP准则:使用BGP over VTI时，请在路由配置上设置TTL跳数> 1。

ECMP:可将分支静态VTI放置在ECMP区域中，以实现负载均衡和故障切换。动态VTI不支持ECMP。

IPv6（7.x — 从6.7更新）

原始FTD 6.7文档指出仅支持IPv4，当前版本支持：

- 隧道源和VTI终端上的IPv6地址
- 组合：IPv4 over IPv4、IPv6 over IPv6、IPv4 over IPv6、IPv6 over IPv4
- 隧道源上的静态和动态IPv6地址

在部署IPv6 VTI之前验证对等功能和FMC版本说明。

动态VTI附加限制(7.3+)

- 仅IKEv2（无IKEv1）
- FMC中的中心辐射型拓扑（建议每个拓扑使用一个中心点）
- DVTI上无ECMP、无QoS、无集群、无多实例中的VRF
- 每个设备最多1000个DVTI会话（取决于平台）
- 在大多数设计中，DVTI集线器需要环回（或借用IP）编址

NAT、QoS和策略

策略/功能	静态VTI	动态VTI
访问控制策略	必需（两个方向）	必需
NAT	在拓扑向导中可免除VPN流量；NAT规则可以应用于非VPN流量。请勿将NAT加密的IKE/ESP不正确。	相似；请参阅FMC NAT免除选项
服务质量	有限的平台支持；DVTI不支持QoS。	Not Supported
平台设置（VTI上的SNMP/系统日志）	不支持。	Not Supported

NAT/QoS/平台设置策略中“不支持”原始6.7文本VTI。当前指南：非加太协议是强制性的；VTI上的SNMP/Syslog不受支持；不支持DVTI上的QoS，请在您的版本中查询FMC以进行NAT交互。

弱加密算法

从FMC/FTD 6.7开始的新VPN隧道删除了较弱的算法。较新的版本保持强加密默认值，对于FTD 6.7+上的新隧道配置，这些算法不受支持：

IKE策略 — 新隧道不支持：

- 加密 :3DES、DES、NULL
- 完整性：MD5
- PRF:MD5
- DH组：1、2 和 24

IPsec提议 — 新隧道不支持：

ESP 加密:DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256

升级影响(6.7+):如果现有VPN策略使用删除的密码，从6.7之前的版本升级FMC管理的FTD可触发预验证检查。在升级之前，使用强算法重新配置IKE/IPsec策略。

场景	配置UI	升级后的隧道
全新安装(6.7+)	弱密码可见，但无法应用于FTD 6.7+	不适用
升级:FTD仅使用弱密码	在重新配置之前升级被阻止	如果强制隧道关闭
升级:混合弱/强密码	在重新配置之前升级被阻止	如果对等体使用强密码，则隧道可以重新建立
出口控制（C类）许可证	DES是唯一没有强加密许可证的选项	仅DES隧道

建议:使用IKEv2、AES-256、SHA-256或SHA-512和DH组19/20/21（或更高支持的组）进行新部署。

许可

在许可模式或评估模式下，基于路由的VPN不需要除基本FTD功能之外的其他许可证。如果未启用导出控制功能（强加密），在受限部署中只有DES可用作加密算法。

FMC的配置步骤

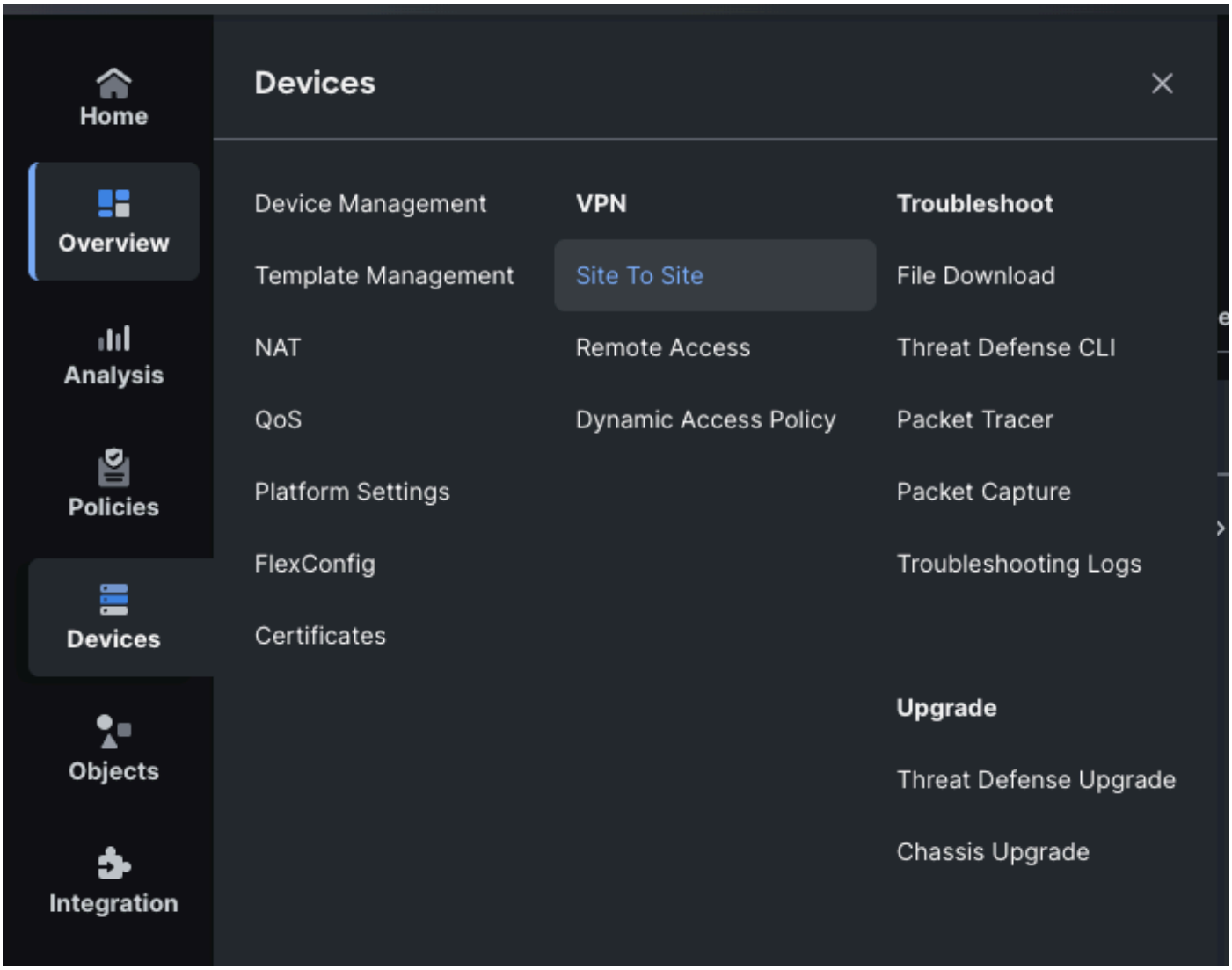
这些步骤在FTD（节点A）和外联网对等体(例如ASA（节点B）)之间的基于静态路由(VTI)站点到站点VPN中进行配置：

实验演示值

参数	价值
拓扑名称	VTI-ASA
IKE版本	IKEv2
VTI名称	VTI-ASA
VTI区域	VTI区域
隧道ID	1
VTI IP(FTD)	192.168.100.1/30
通道来源	GigabitEthernet0/0（外部）
对等设备	外网ASA
对等体名称	ASA对等体
对等端点IP	10.106.67.252
IKE策略名称	ASA-IKEv2-Policy
IPsec建议名称	ASA-IPSec-Policy
PSK（仅实验室）	（在生产中使用强键）

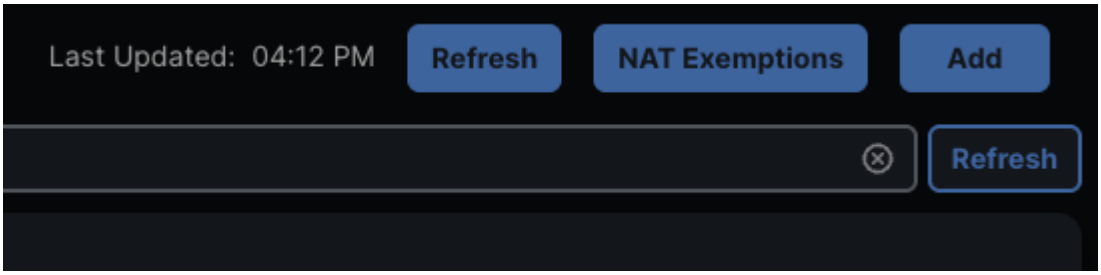
步骤1.打开站点到站点VPN

1. 导航到设备> VPN > 站点到站点



步骤2.添加VPN拓扑

1. 单击Add VPN，然后选择Firewall Threat Defense Device（或Secure Firewall Threat Defense Device，具体取决于FMC UI版本。）

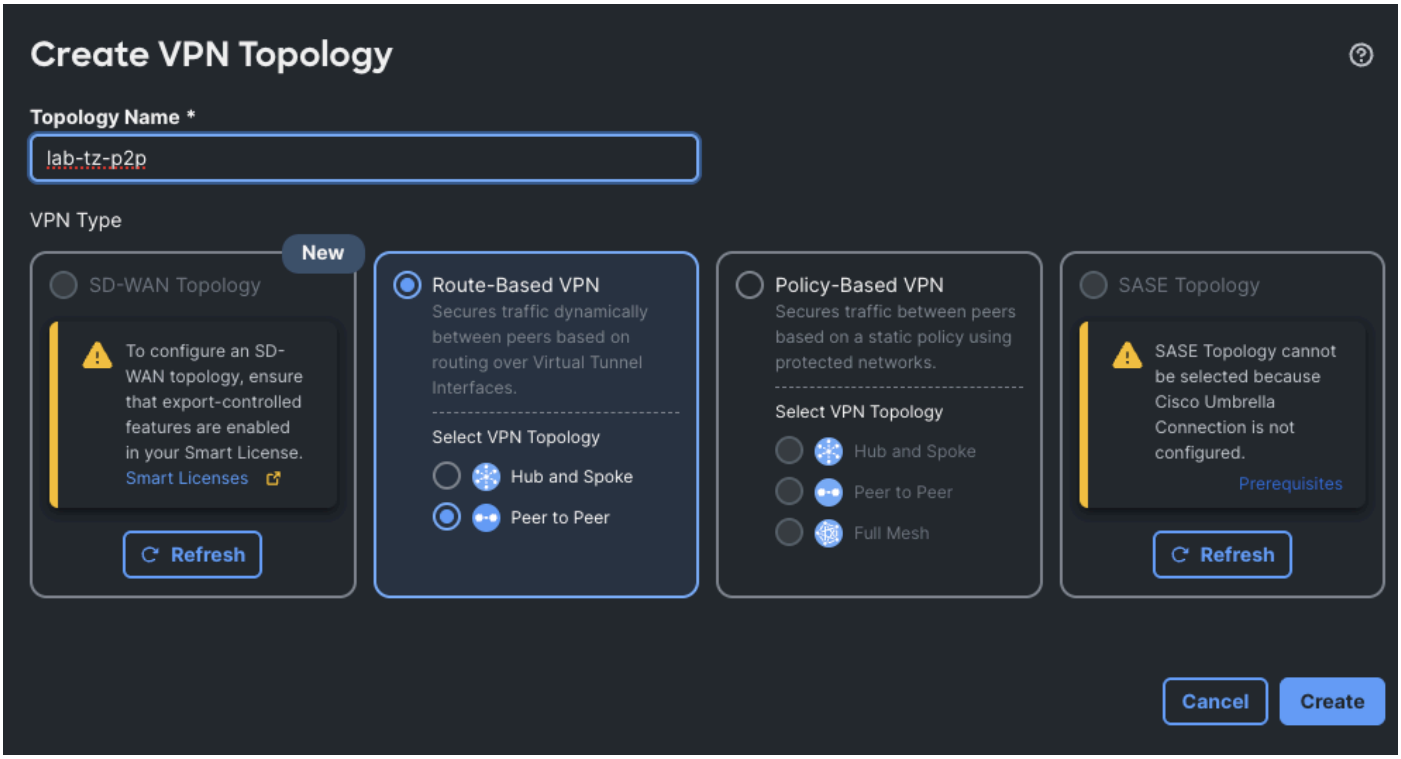


步骤3.拓扑名称、类型和IKE版本

1. 提供拓扑名称并选择VPN类型Route Based(VTI)。 选择IKE Version(推荐：IKEv2。)

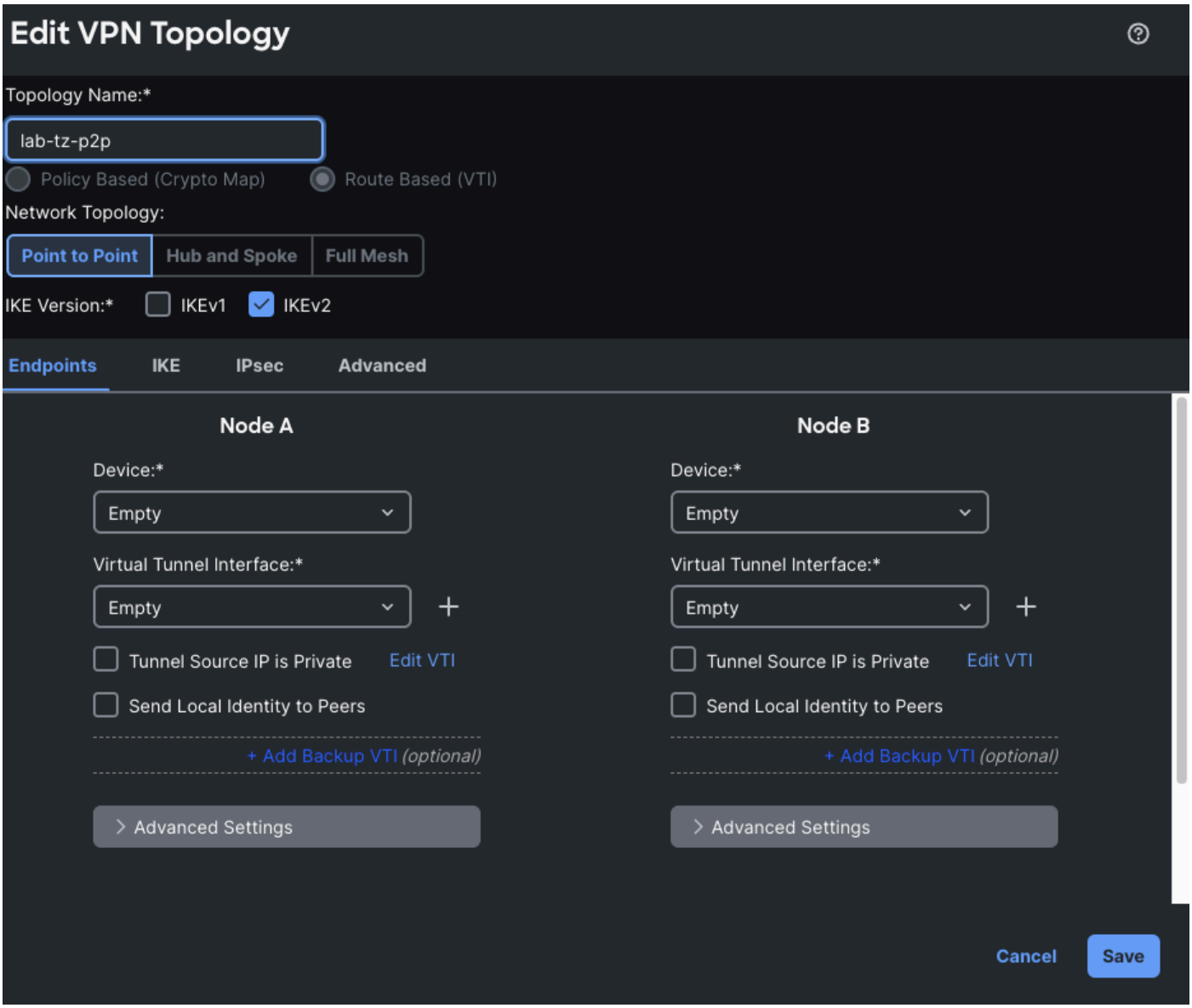
- 拓扑名称：VTI-ASA
- type：基于路由(VTI)
- IKE版本：IKEv2

注意：IKEv1不支持符合CC/UCAPL标准的设备。思科建议对新设计使用IKEv2。



步骤4.选择FTD设备和VTI

1. 为节点A选择FTD Device。
2. 添加新的虚拟隧道接口（点击+）或选择现有VTI。对于中心上使用DVTI的中心辐射型，中心使用动态VTI。



步骤5.创建静态虚拟隧道接口

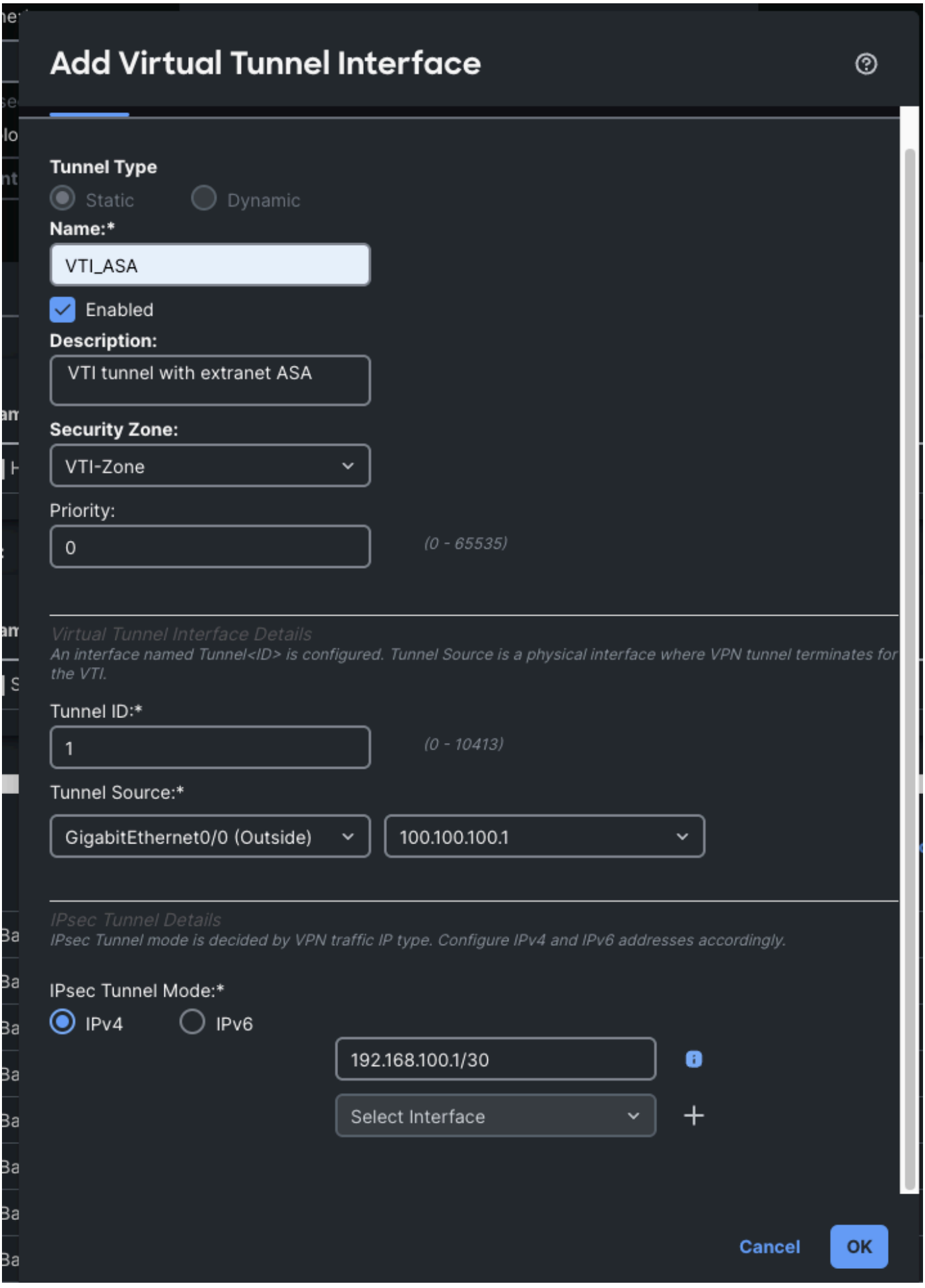
1. 定义新的VTI参数，然后单击OK。

字段	示例
名称	VTI-ASA
描述	带外网ASA的VTI隧道
安全区域	VTI区域

字段	示例
隧道ID	1
IP Address	192.168.100.1/30
通道来源	GigabitEthernet0/0（外部）
通道模式	ipsec ipv4

2.

- 将VTI分配到ACP规则中使用的专用安全区域。
- 对于IPv6，请选择适当的隧道模式和编址(7.x)。
- 请勿使用借用IP接口作为隧道源地址。


Add Virtual Tunnel Interface
Tunnel Type
Static
Dynamic
Name:*
VTI_ASA
Enabled
Description:
VTI tunnel with extranet ASA
Security Zone:
VTI-Zone
Priority:
0
(0 - 65535)
Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.
Tunnel ID:*
1
(0 - 10413)
Tunnel Source:*
GigabitEthernet0/0 (Outside)
100.100.100.1
IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.
IPsec Tunnel Mode:*
IPv4
IPv6
192.168.100.1/30
Select Interface
Cancel
OK

步骤6.确认VTI创建

1. 在确认已创建VTI时单击OK。

步骤7.配置对等体（节点B — 外联网）

1. 选择在步骤5中创建的VTI。配置节点B（对等体）：

字段	示例
设备类型	外联网
设备名	ASA对等体
终端IP地址	10.106.67.252

2.为每个对等体后面的子网配置受保护网络。受保护网络定义可以使用VPN的流量；基于路由的VPN仍然需要指向VTI的路由。

可选(7.x):

- 如果对等体之间存在NAT设备，则启用NAT穿越。
- 在拓扑向导中免除NAT的VPN流量（如果需要）。
- 当对等体需要VTI IP进行路由时，向对等体发送虚拟隧道接口IP（与BGP/OSPF通用）。

步骤8. IKE选项卡 — 选择或创建IKE策略

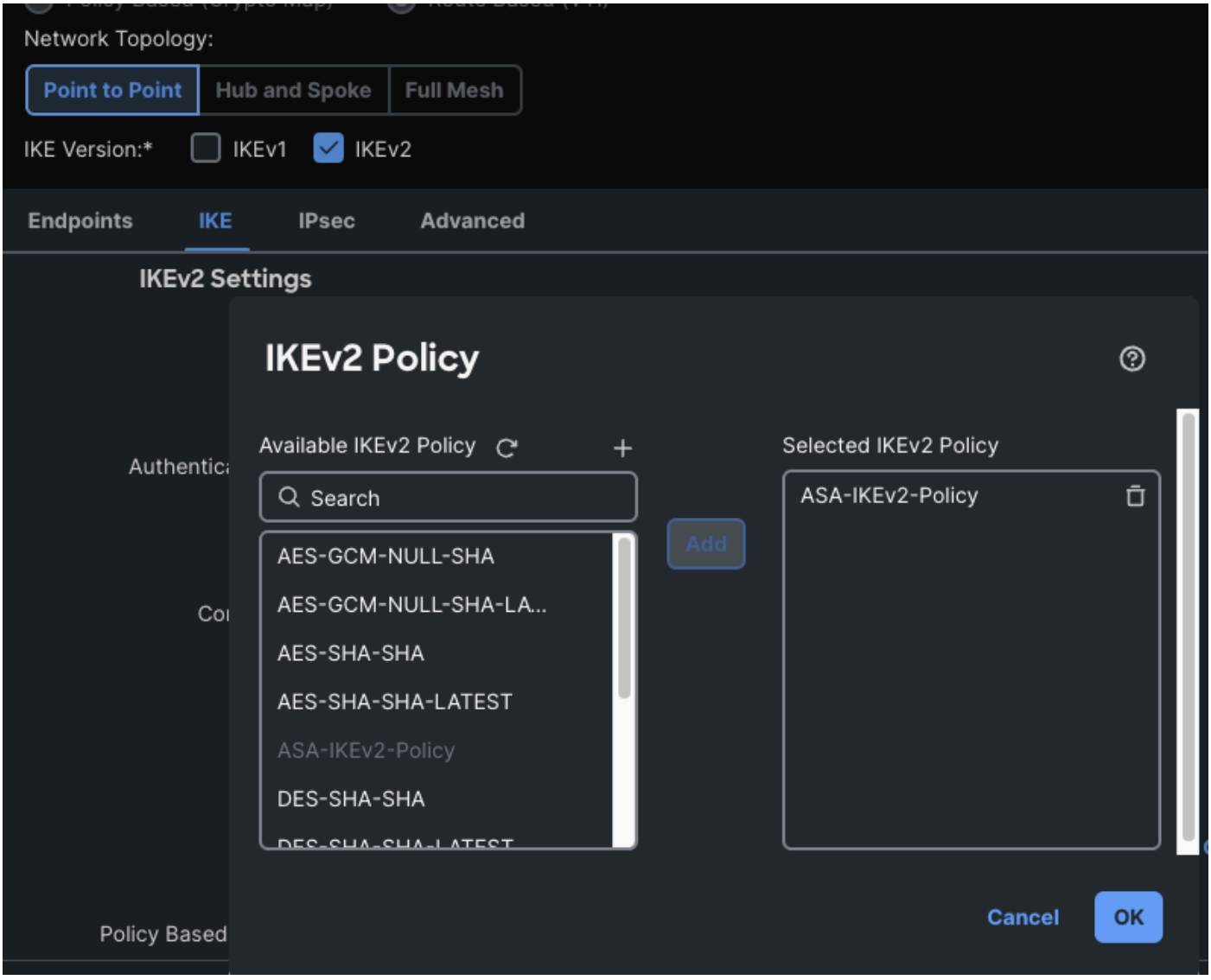
1. 打开IKE选项卡并选择现有IKEv2策略，或单击+以创建一个新策略。

步骤9.（可选）创建IKEv2策略

字段	推荐示例
名称	ASA-IKEv2-Policy
完整性	SHA-512（或SHA-256）
加密	AES-256
PRF	SHA-512（或SHA-256）
DH组	21个（或每个策略为19/20个）

---

1. Click Save.



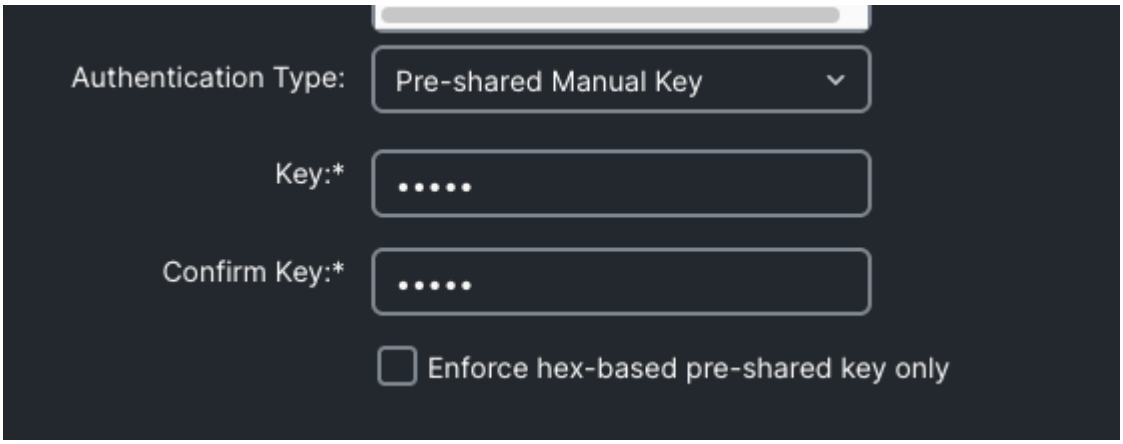
步骤10. IKE身份验证

1. 选择IKE策略。选择Authentication Type:

- 预共享手动密钥:输入并确认密钥(仅限实验/演示；在生产中使用强大的PSK。)
- 预共享自动密钥：当两个终端由同一FMC管理时可用。
- 证书：用于基于PKI的身份验证。

示例（实验）:

- Policy（策略）：ASA-IKEv2-Policy
- 身份验证:预共享手动密钥



步骤11. IPsec选项卡 — IPsec建议案

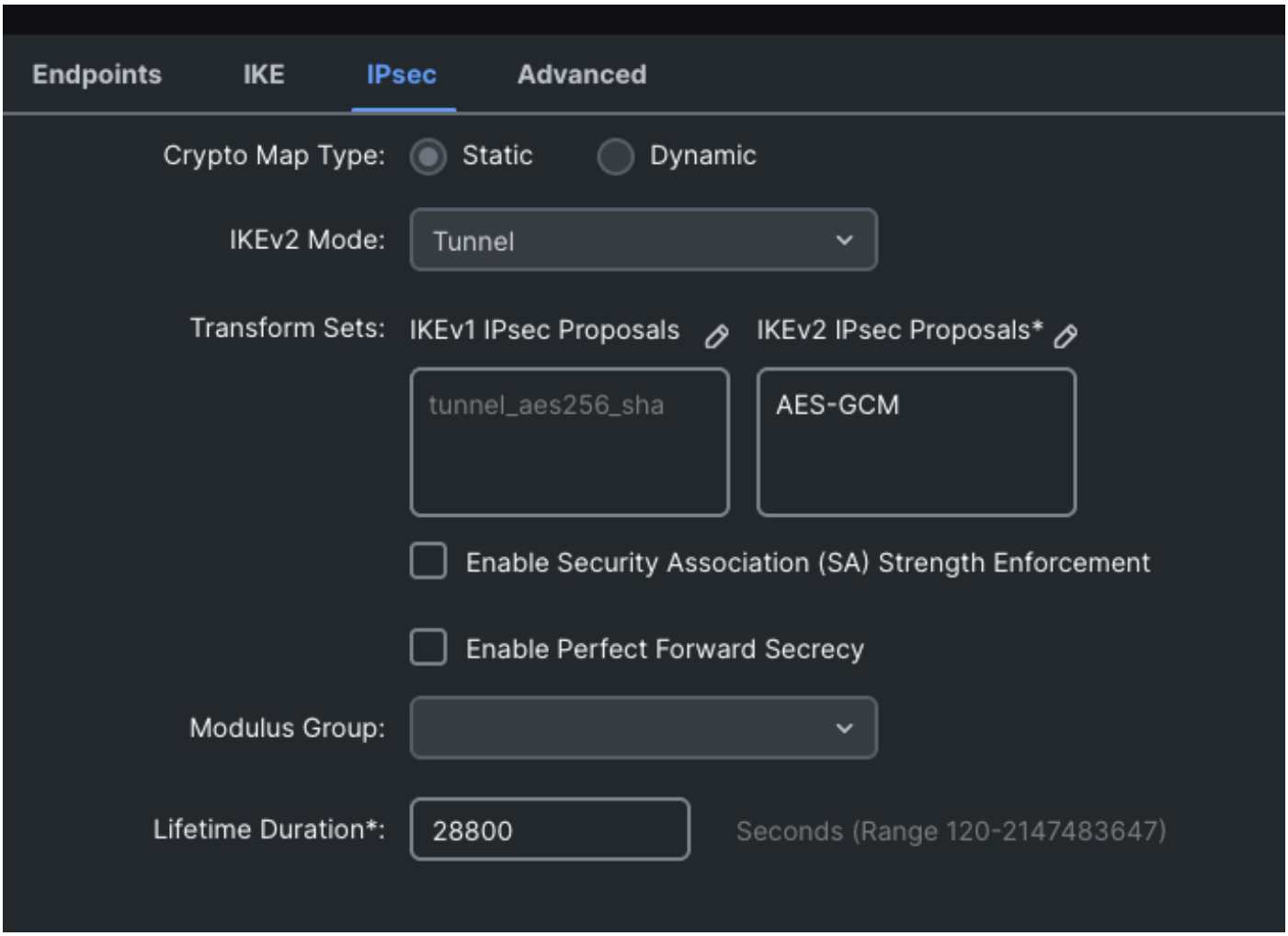
1. 打开IPsec选项卡。选择或创建IKEv2 IPsec Proposal（单击Edit或+）。

步骤12.（可选）创建IKEv2 IPsec提议

字段	推荐示例
名称	ASA-IPSec-Policy

字段	推荐示例
ESP散列	SHA-512（或SHA-256）
ESP 加密	AES-256

1. Click Save.



步骤13.选择IPsec提议

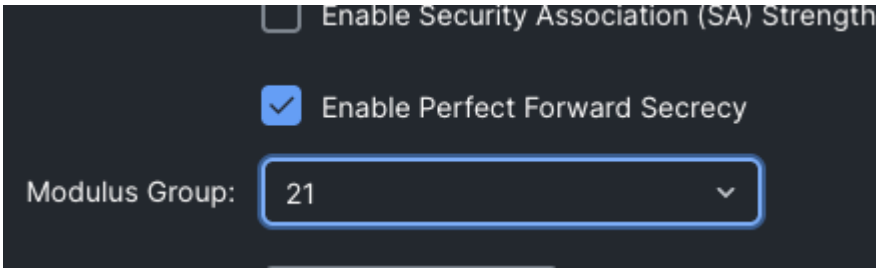
1. 选择建议书，然后单击OK。

步骤14.完全向前保密和生命期

1. 配置可选PFS和生存期：

字段	示例
完全转发安全性	第 21 组
生存期	28800秒（默认）
生存期大小	4608000 KB（默认）

2.调整以匹配对等体要求和组织加密标准。



步骤15.保存VPN拓扑

查看摘要并点击保存。

步骤16.配置访问控制策略（必填）

1. 导航至策略> 访问控制> 访问控制。编辑应用于FTD的策略。

注意：sysopt connection permit-vpn — 已解密VPN流量的旁路访问控制策略不适用于基于路由的VPN。为两个方向经过VTI区域的流量配置显式Allow规则。下表提供了创建规则示例。

方向	源区域	目标区域	源网络	目标网络
Internal → Remote	区域内	VTI-Zone（或Out-Zone）	网络内	远程网络
远程→内部	VTI区域	区域内	远程网络	网络内

2.调整区域名称以匹配您的设计。完全连接需要双向规则。

步骤17.通过VTI添加静态路由

1. 导航到设备> 设备管理。编辑FTD设备。
2. 打开路由 > 静态路由。单击Add Route。

字段	示例
接口	VTI-ASA
网络	远程网络
网关	192.168.100.2（对等VTI IP）

3.使用对等隧道IP作为网关，除非您的设计使用通过VTI可到达的另一个下一跳。

4.对于动态路由，请在VTI上配置BGP、OSPF或EIGRP，而不是（或附加于）静态路由。

5. ECMP（可选，7.x）:将多个静态VTI放在ECMP区域中并配置ECMP静态路由以实现负载共享。

步骤18.部署配置

1. 导航到部署> 部署（或部署> 部署管理器，具体取决于FMC版本）。 选择FTD并单击Deploy。在验证之前等待成功部署。

部署后的CLI示例

成功部署后，FTD CLI配置类似于：

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****

interface Tunnel1
 description VTI Tunnel with Extranet ASA
 nameif VTI-ASA
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

实际对象名称和策略编号因FMC部署而异。

验证

从FMC GUI

1. 打开Devices > VPN > Site To Site，然后选择拓扑。
2. 使用Check Status或站点到站点监控控制面板查看隧道状态。



注意：FMC VPN隧道状态无法在所有版本上实时更新（记录的时间间隔为几分钟）。 使用CLI确认GUI是否显示模糊状态。等效CLI检查（FMC可以运行这些检查以了解状态）。

```
show crypto ipsec sa peer
```

```
show vpn-sessiondb detail l2l filter ipaddress
```

从FTD CLI

```
show running-config crypto
show running-config interface Tunnel
show running-config route
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show crypto ipsec sa peer
```

```
show vpn-sessiondb detail l2l
show vpn-sessiondb detail l2l filter ipaddress
```

对于仍在使用IKEv1的传统对等体：

```
show crypto ikev1 sa detailed
```

路由验证：

```
show route
show bgp summary
show ospfv3 neighbor
```

用适合您配置的路由协议的命令替换这些命令。

故障排除快速参考

症状	共同原因	操作
IKE失败	PSK不匹配，UDP 500/4500被阻止，密码不匹配	将IKE策略/建议与对等项进行比较；检验NAT-T
IPsec开启，无流量	缺少ACP规则	为VTI区域双向添加允许规则
IPsec开启，无流量	静态路由缺失或错误	检验通过VTI到远程受保护网络的路由
FMC升级后隧道关闭	删除弱密码	使用AES-256/SHA-256+重新配置IKE/IPsec
BGP不通过VTI对等	TTL/安全区域	设置TTL跃点> 1;检验VTI IP连通性
GUI显示关闭，CLI显示	FMC状态刷新延迟	使用CLI;如果过时，则重新部署

相关文档

- 在FMC管理的FTD上配置基于路由的站点到站点VPN隧道(Cisco.com) — 文档ID 216276
- 在安全防火墙上使用多SA配置DVTI — 文档ID 220322
- FMC 7.6设备配置指南 — 站点到站点VPN
- DVTI使用案例 — 使用OSPF/BGP集中星型
- 虚拟隧道接口准则（防御协调器/FMC）
- 配置ASA/AnyConnect动态拆分隧道（FQDN路由概念参考）

修订历史纪录

修订版	日期	备注
7.0	2026年7月28日	全面实质性更新：安全防火墙品牌、7.x限制（OSPF/EIGRP/IPv6/1024 VTI规模）、DVTI交叉链路、ACP重点、更正的拼写错误、扩展的验证/故障排除
6.0	2024年9月24日	更新的简介和格式(Cisco.com)
5.0	2024年6月27日	限制和DVTI参考更新(Cisco.com)
1.0	2020年11月23日	首次公开发布

文档应用于

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)
- 基于静态路由的站点到站点VPN(SVTI)
- 外联网对等体（ASA、第三方IPsec设备）

不包括:FTD集群VTI、GRE隧道或完整DVTI中心辐射型过程（请参阅文档ID 220322。）

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。