在FDM管理的FTD上使用静态路由配置基于路由的VPN

目录

简介

先决条件

- 要求
- 使用的组件
- 背景信息

FDM的配置步骤

验证

相关信息

简介

本文档介绍如何在FDM管理的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：

- 基本了解VPN隧道的工作方式。
- 预先了解通过Firepower设备管理器(FDM)的导航知识。

使用的组件

本文档中的信息基于以下软件版本：

- 由Firepower设备管理器(FDM)管理的Cisco Firepower威胁防御(FTD)版本7.0。

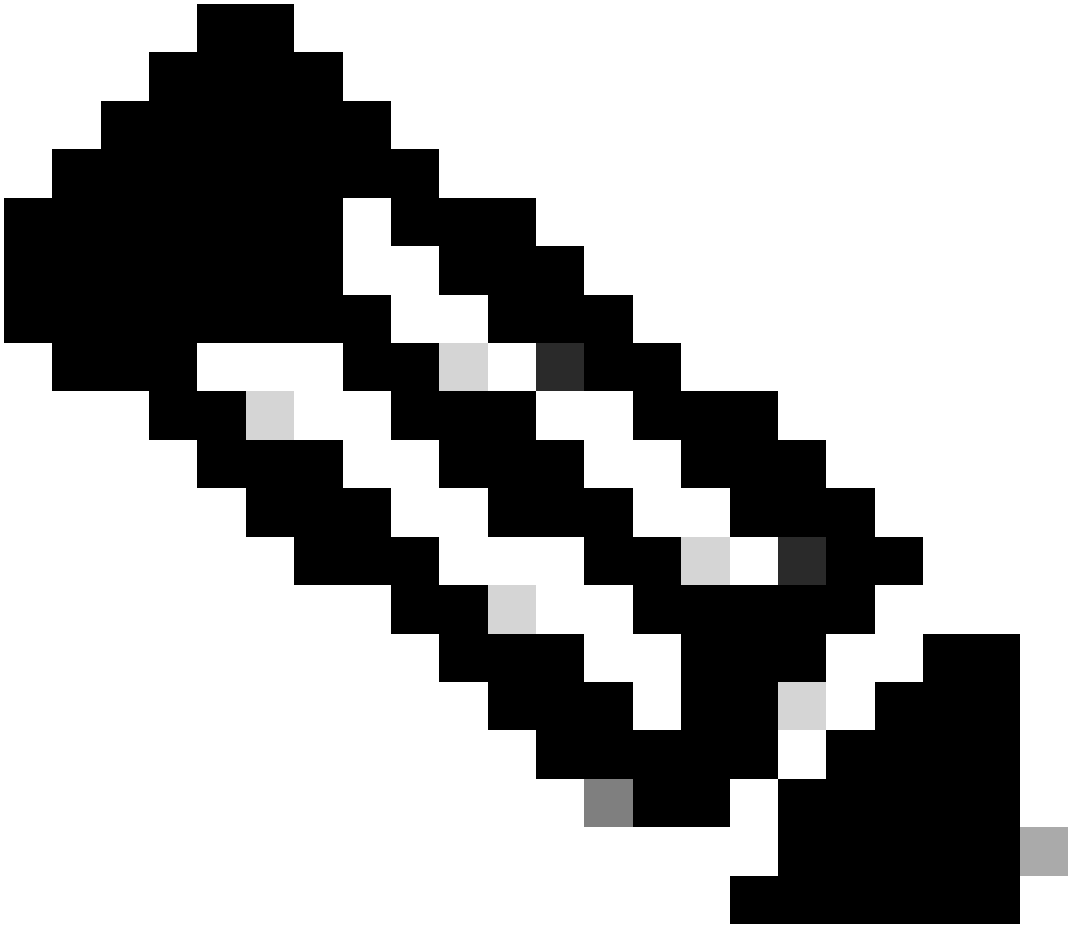
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

基于路由的VPN允许确定要加密或通过VPN隧道发送的相关流量，并且使用流量路由而不是策略/访问列表（如基于策略或基于加密映射的VPN中所示）。加密域设置为允许任何进入IPsec隧道的流量。IPsec本地和远程流量选择器设置为0.0.0.0/0.0.0.0。这意味着路由到IPsec隧道的所有流量都会被

加密，而不考虑源/目标子网。

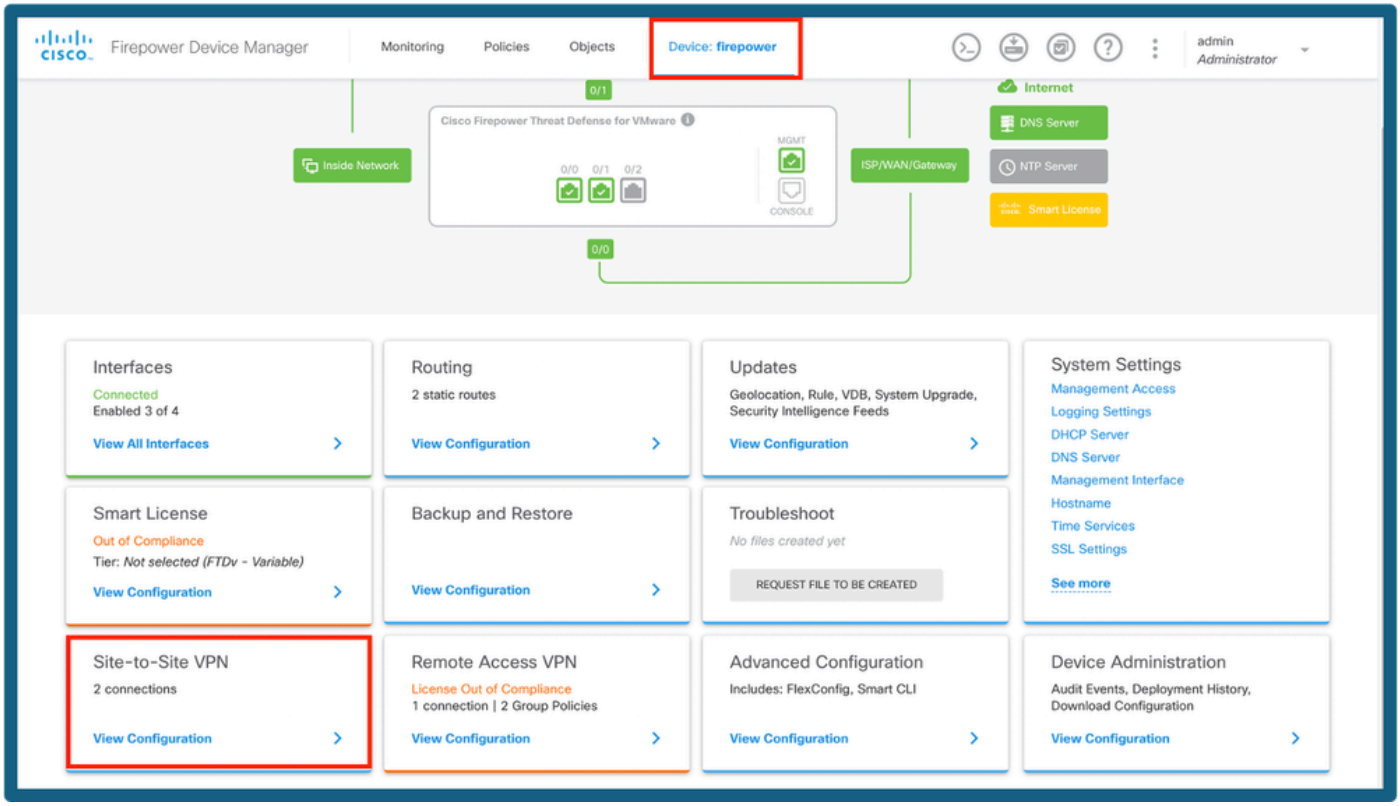
本文档重点介绍静态虚拟隧道接口(SVTI)配置。



注意：无需其他许可，可在许可模式和评估模式下配置基于路由的VPN。如果没有加密合规性（已启用导出控制功能），只有DES可用作加密算法。

FDM的配置步骤

步骤1.导航到Device > Site To Site。



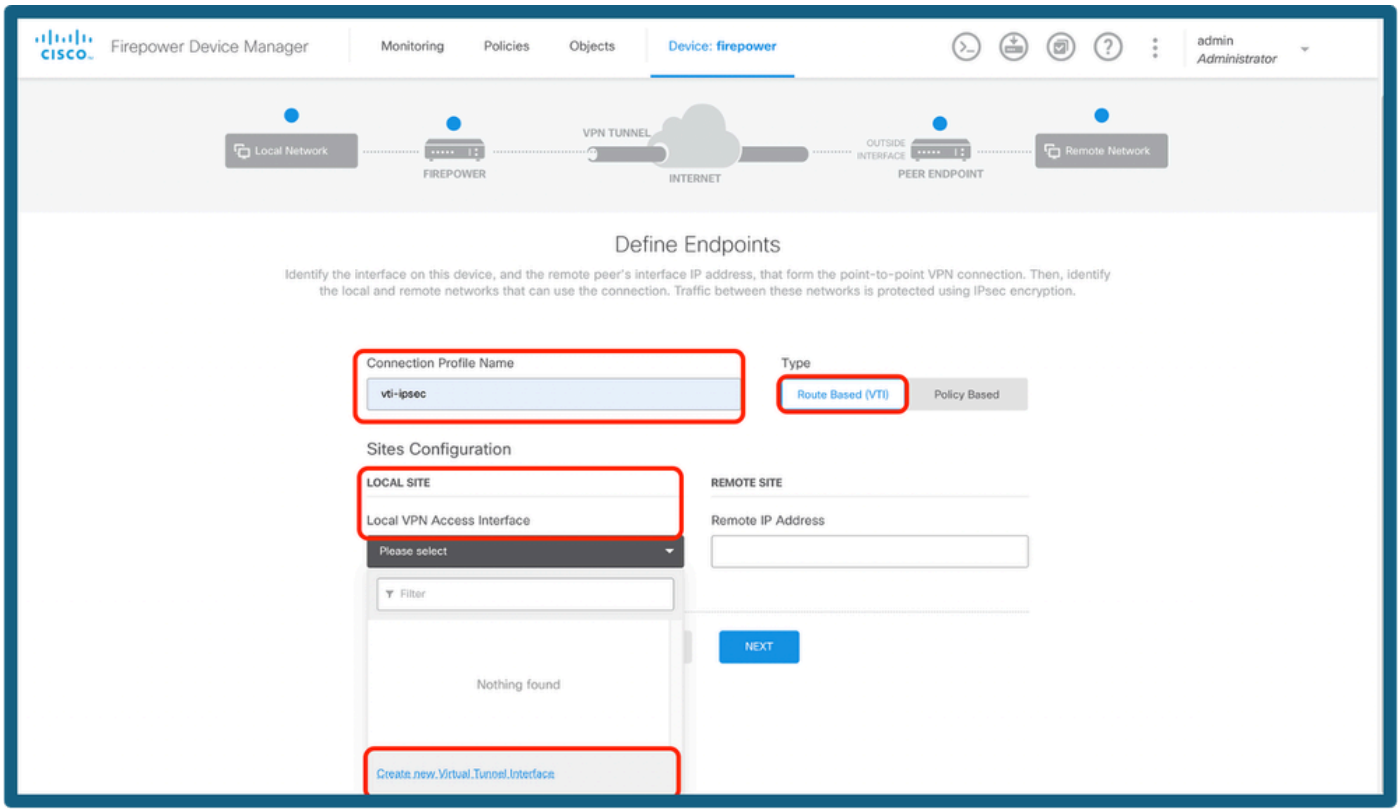
FDM仪表板

步骤2.点击+图标将新站点添加到站点连接。

添加S2S连接

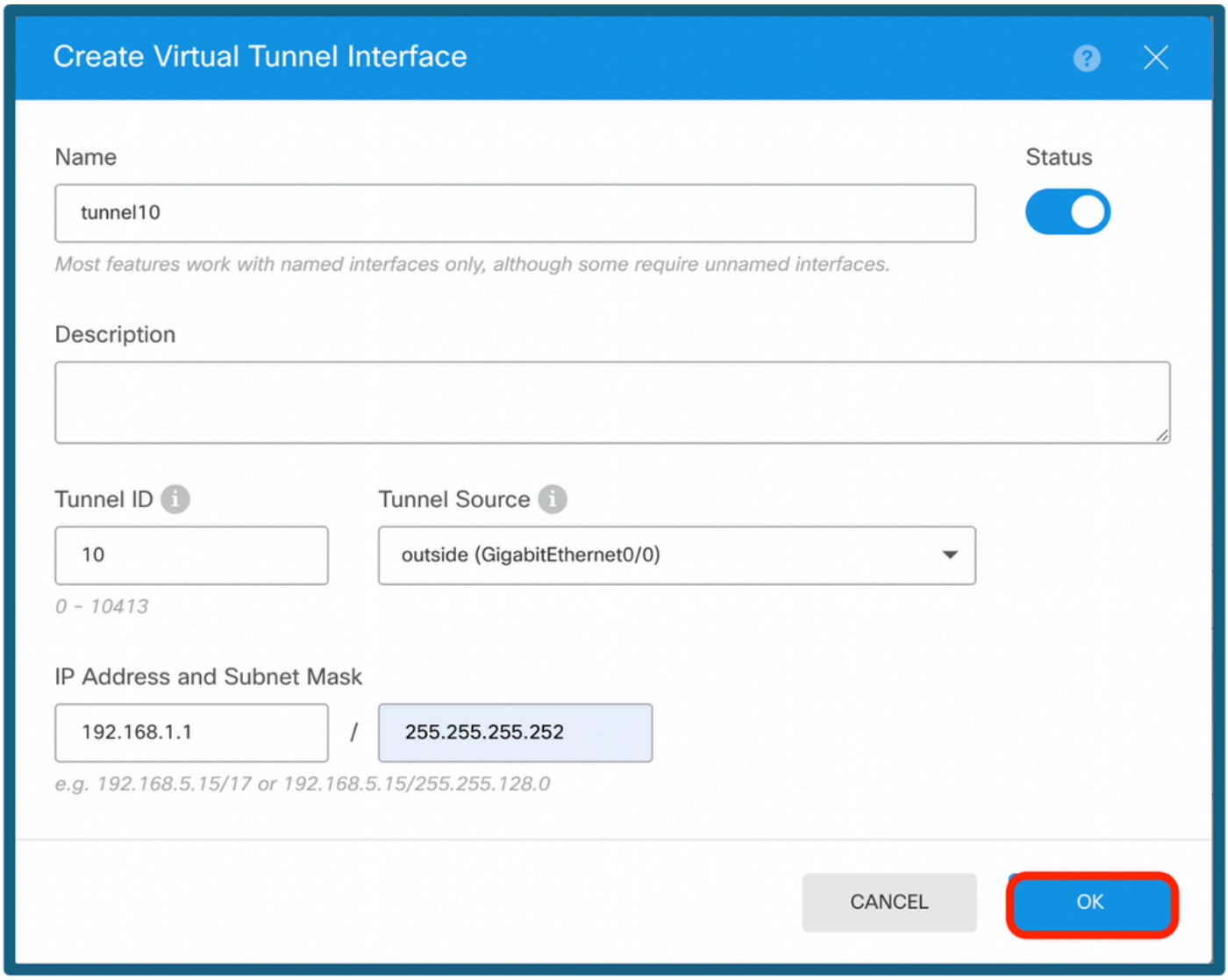
步骤3.提供拓扑名称，并选择VPN类型作为基于路由(VTI)。

单击Local VPN Access Interface，然后单击Create new Virtual Tunnel Interface或从列表中选择一个已存在的接口。



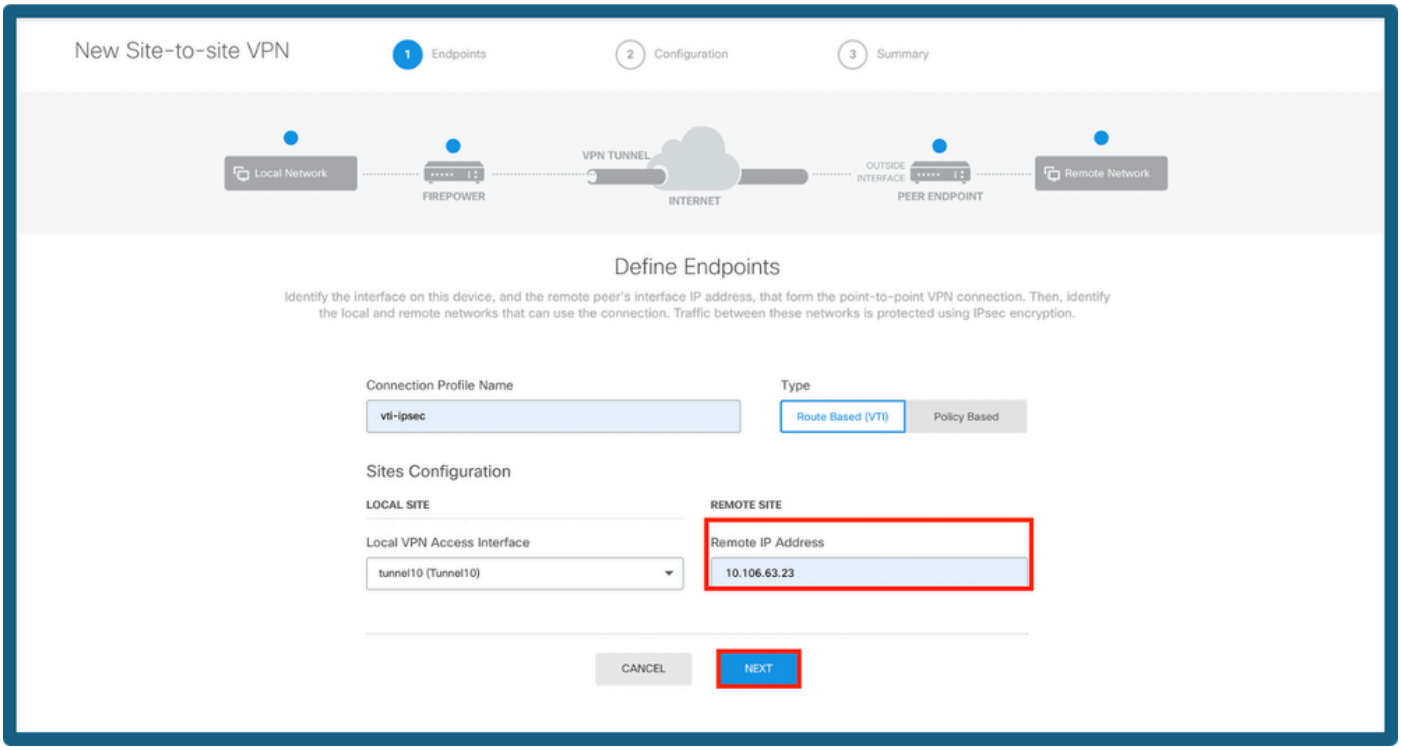
添加隧道接口

步骤4.定义新虚拟隧道接口的参数。Click OK.



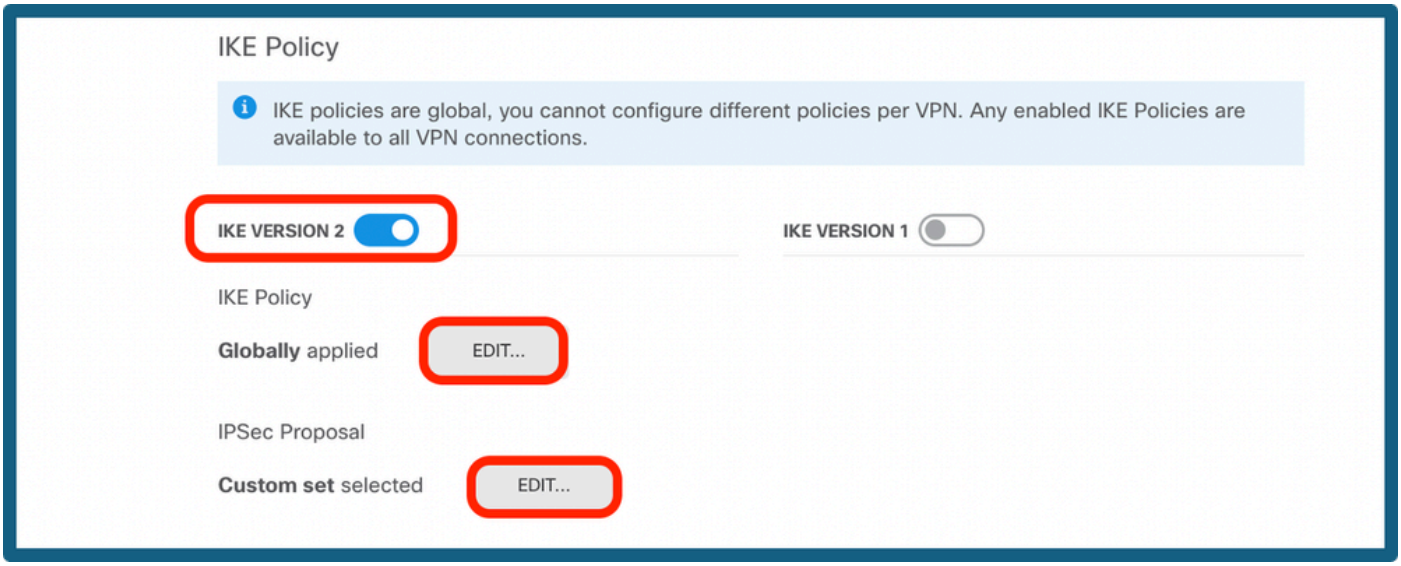
VTI配置

步骤5.选择新创建的VTI或虚拟隧道接口下存在的VTI。提供远程IP地址。



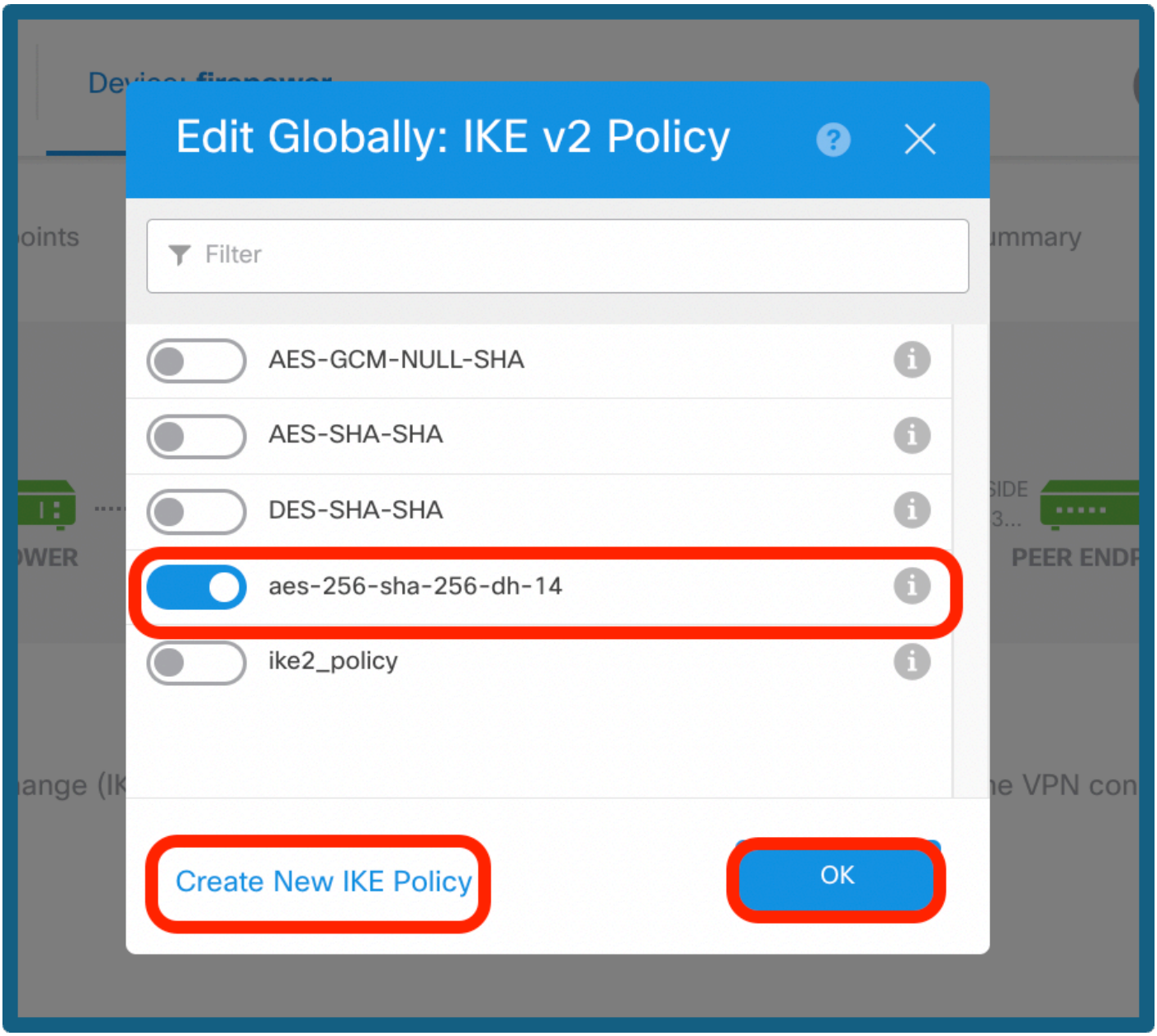
添加对等IP

步骤6.选择IKE Version，然后选择Edit按钮以设置IKE和IPsec参数，如图所示。

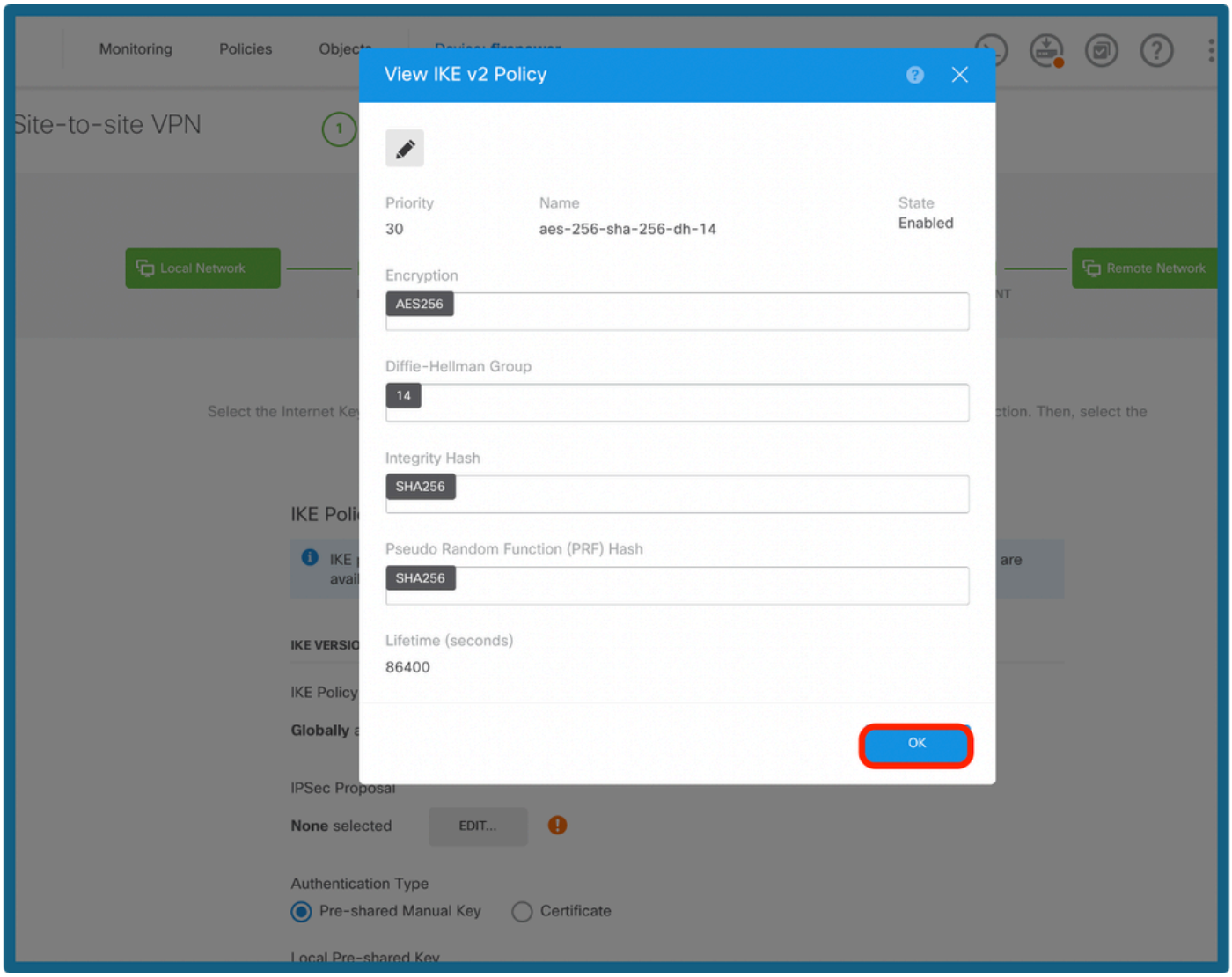


配置IKE版本

步骤7a.选择IKE Policy按钮（如图所示），然后单击ok按钮或Create New IKE Policy（如果要创建新策略）。

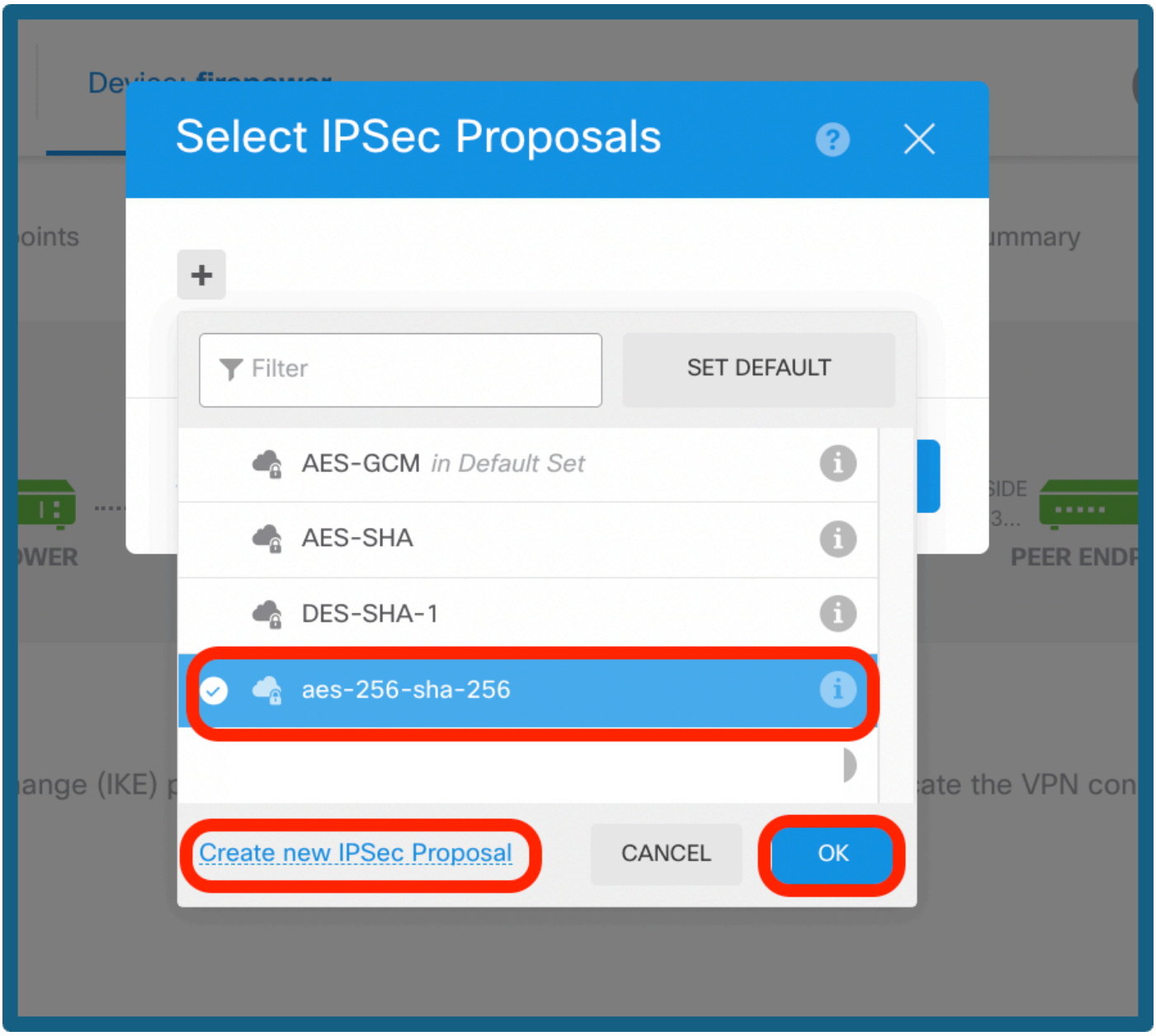

Edit Globally: IKE v2 Policy
Filter
AES-GCM-NULL-SHA
AES-SHA-SHA
DES-SHA-SHA
aes-256-sha-256-dh-14
ike2_policy
Create New IKE Policy
OK

选择IKE策略

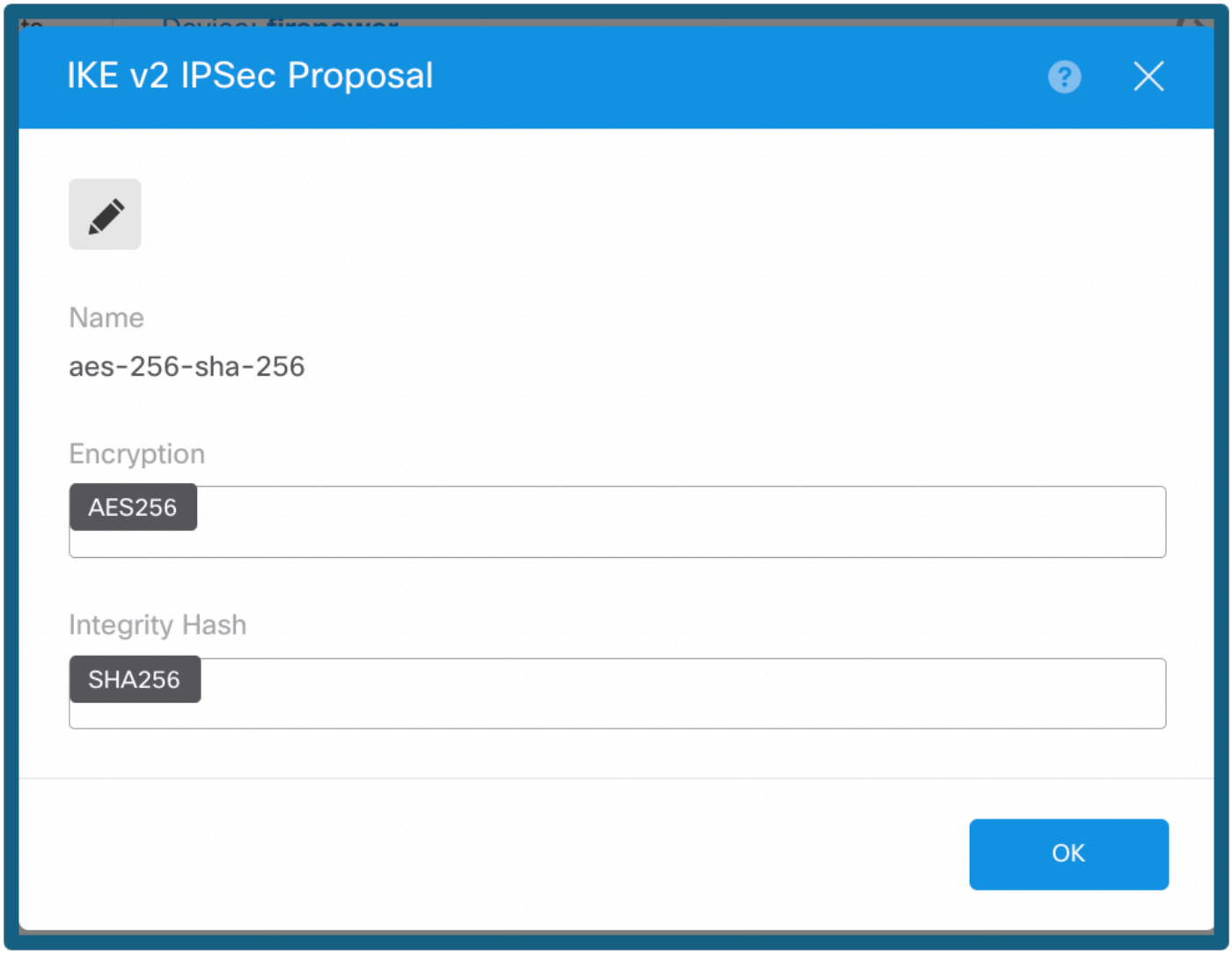


IKE策略的配置

步骤7b.选择IPSec Policy按钮（如图所示），然后单击ok按钮或Create New IPsec Proposal（如果您想要创建新提议）。


Select IPSec Proposals
Filter
SET DEFAULT
AES-GCM in Default Set
AES-SHA
DES-SHA-1
aes-256-sha-256
Create new IPSec Proposal
CANCEL
OK

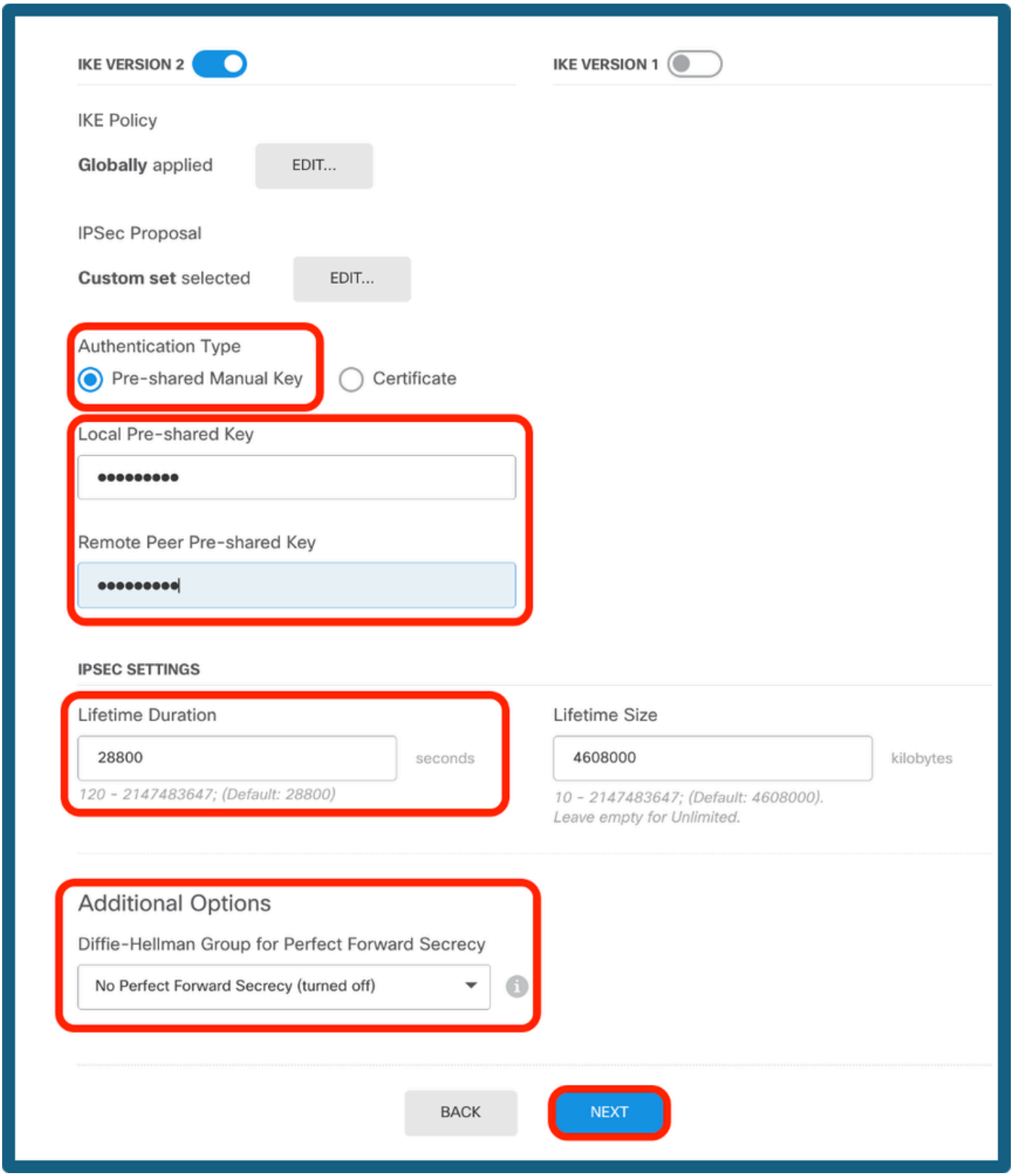
选择IPsec提议



IPsec建议书的配置

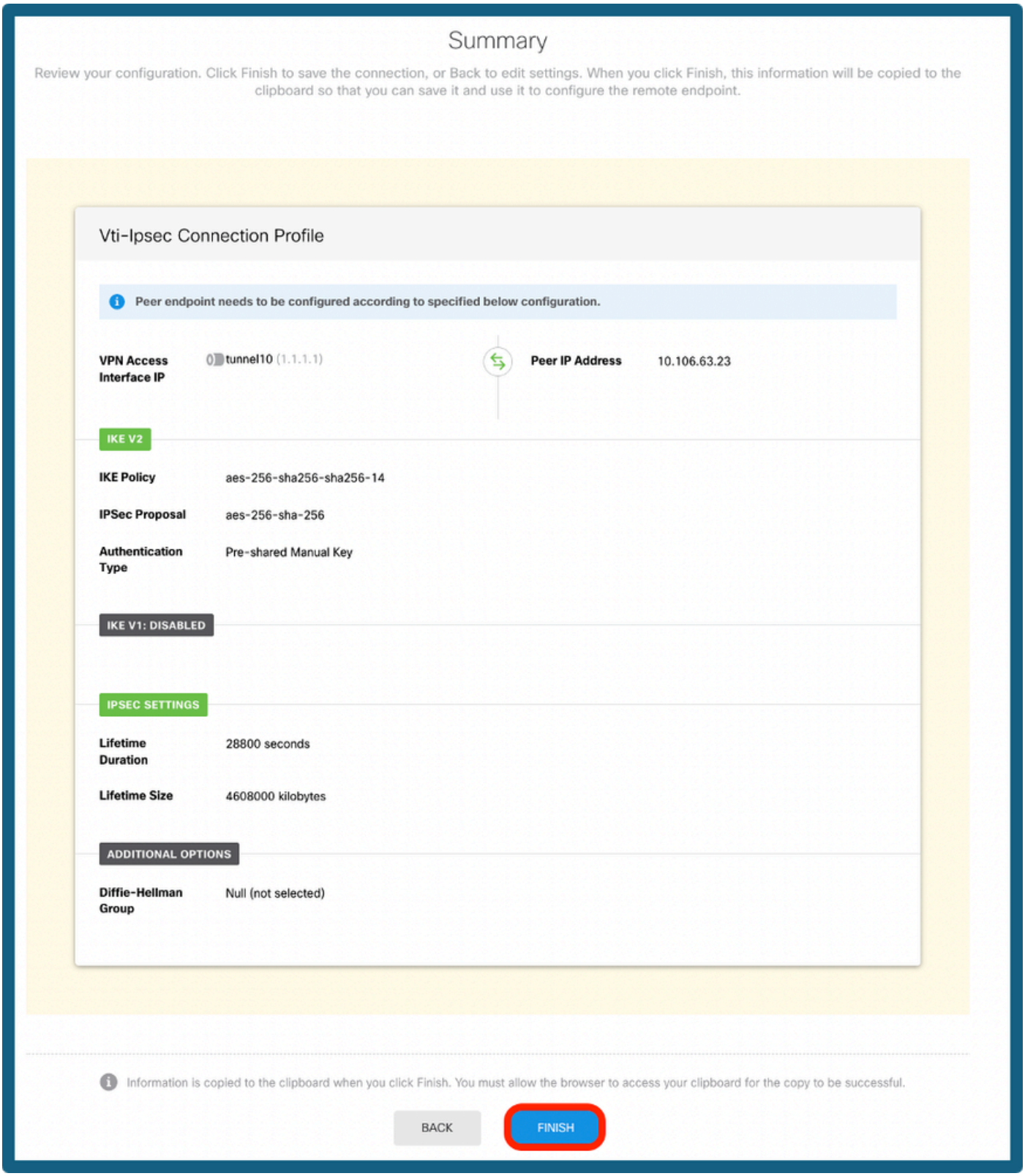
步骤8a.选择身份验证类型。如果使用预共享手动密钥，请提供Local和Remote预共享密钥。

步骤8b.（可选）选择完全向前保密设置。配置IPsec Lifetime Duration and Lifetime Size，然后单击next。



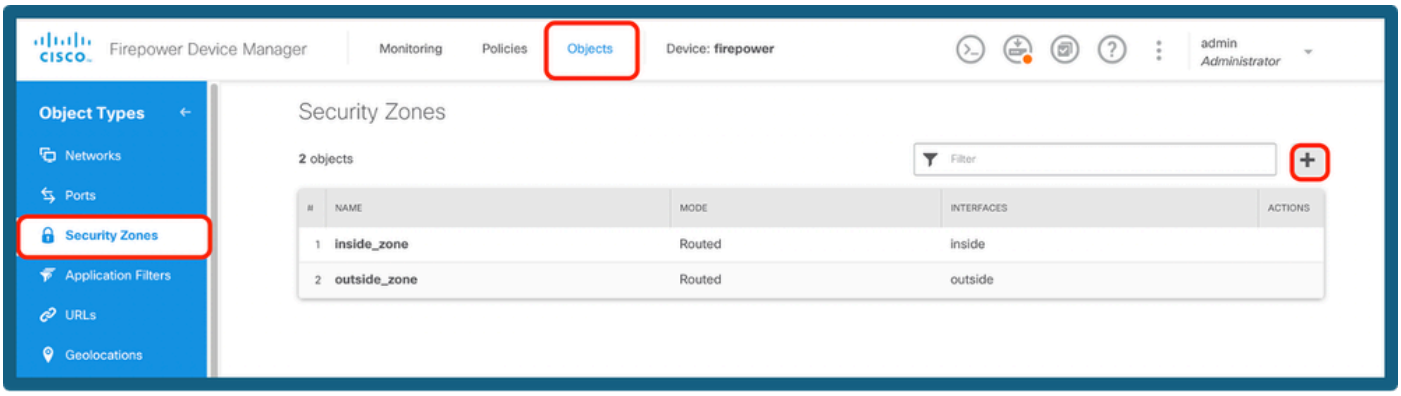
PSK和生命周期配置

步骤9.检查配置，然后单击Finish。



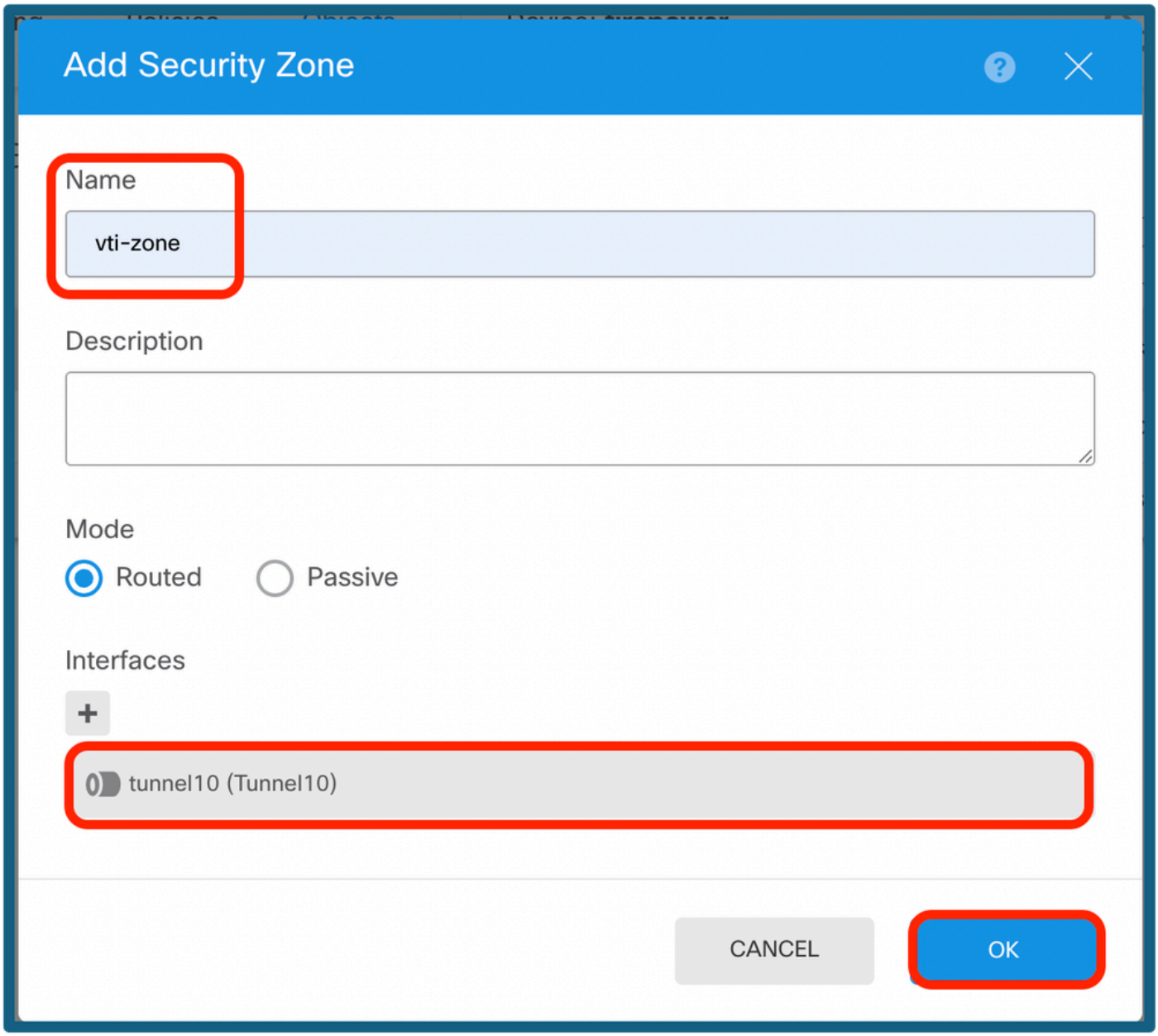
配置汇总

步骤10a.导航到对象>安全区域，然后单击+图标。



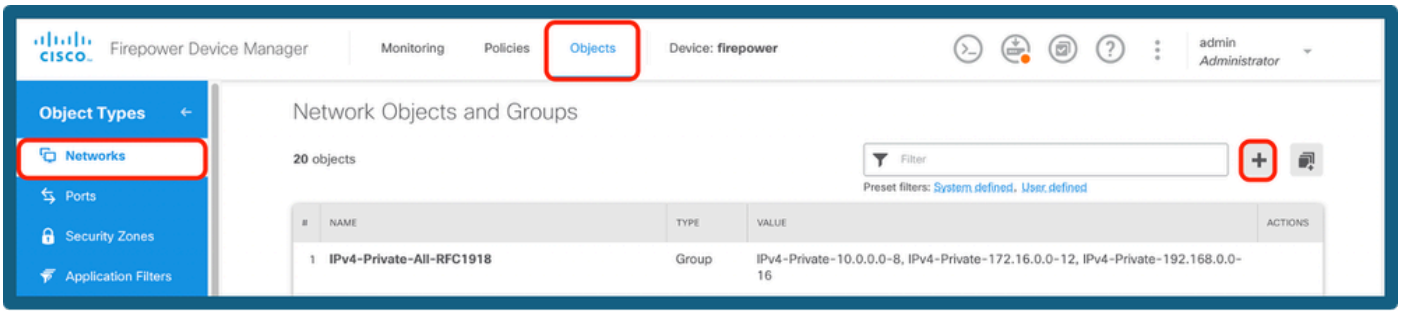
添加安全区域

步骤10b.创建一个区域，然后选择VTI接口，如下所示。



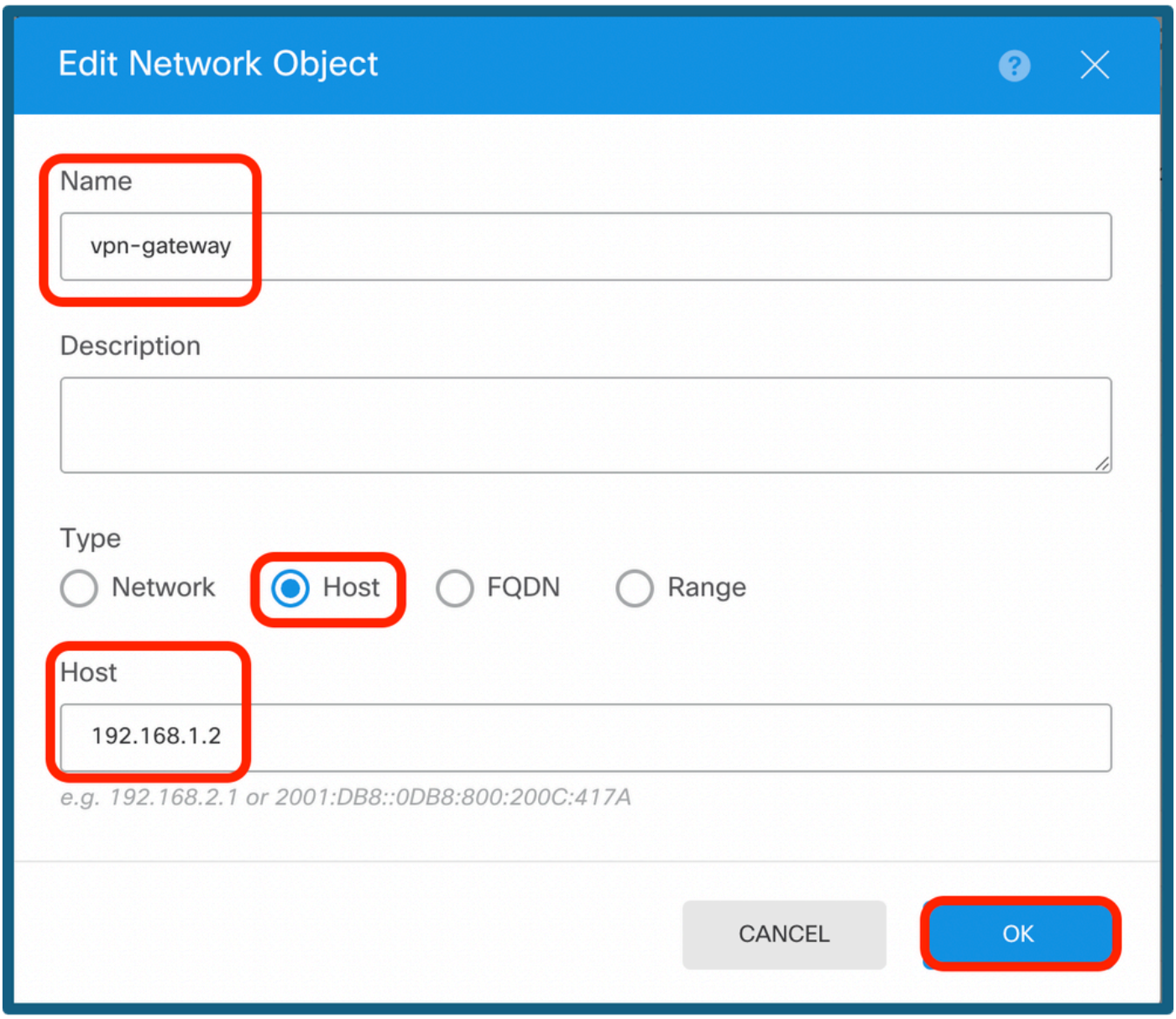
安全区域配置

步骤11a.导航到对象>网络，单击+图标。



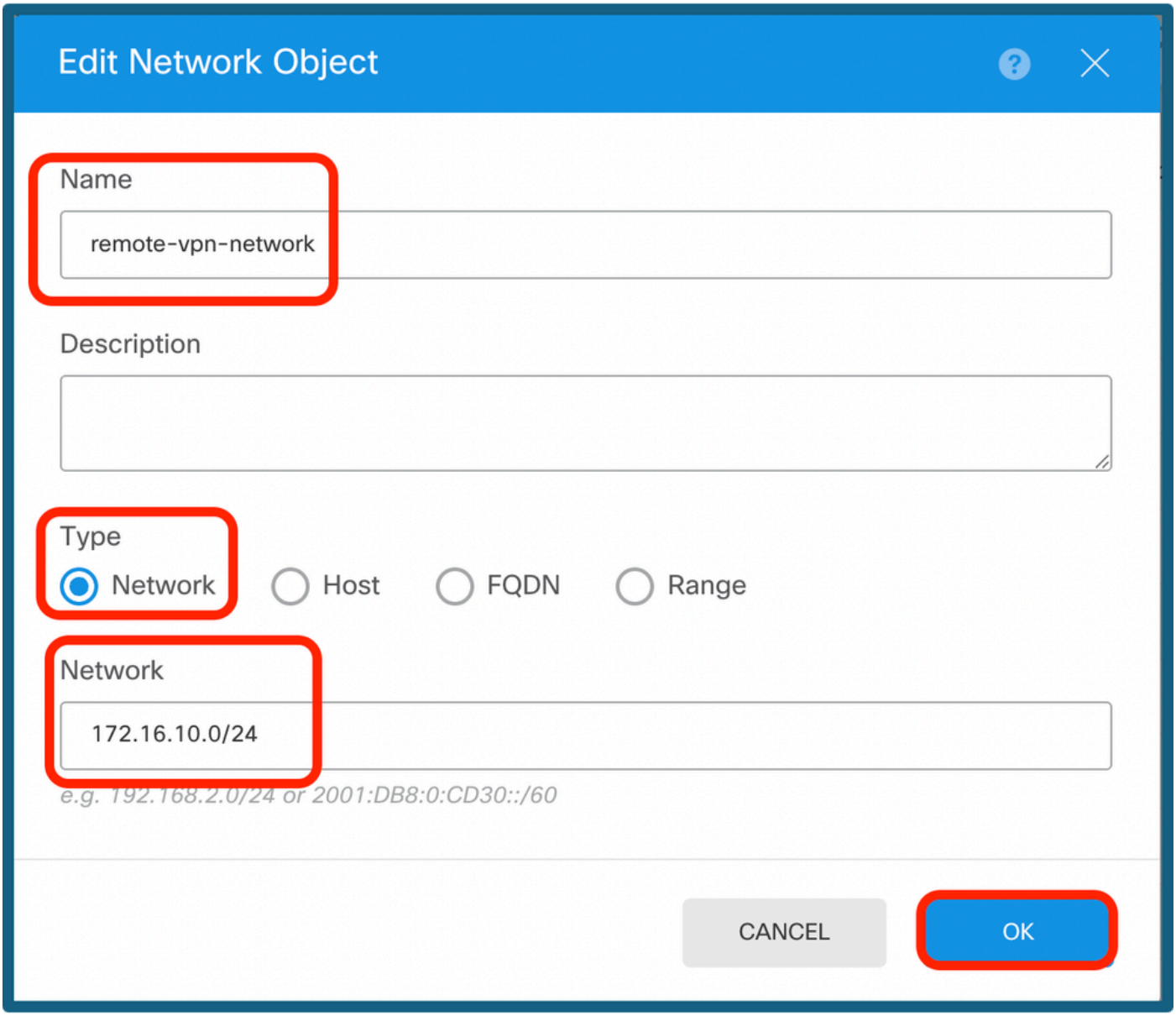
添加网络对象

步骤11b.添加一个host对象，并使用对等端的tunnel ip创建网关。

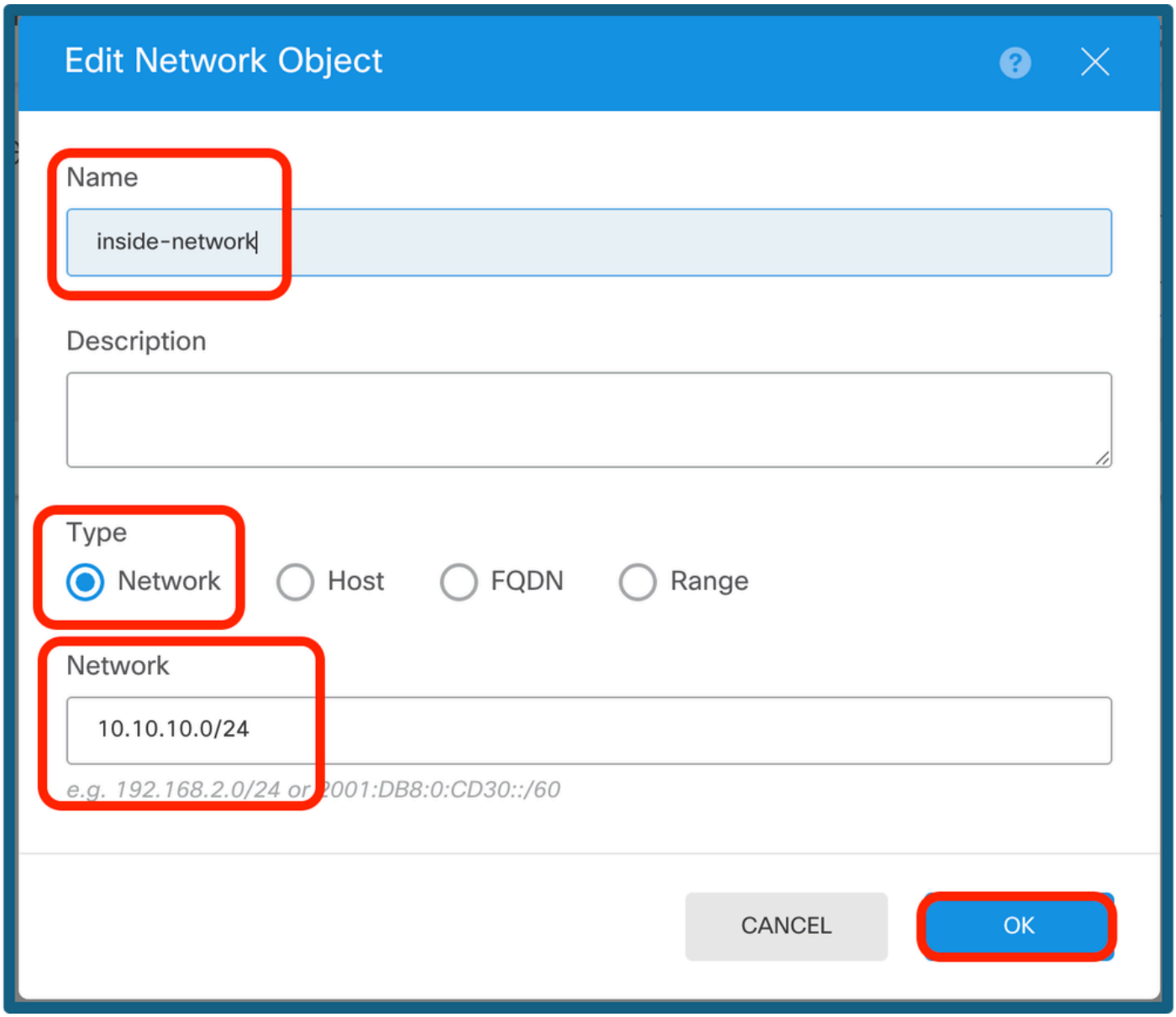


配置VPN网关

步骤11c.添加远程子网和本地子网。

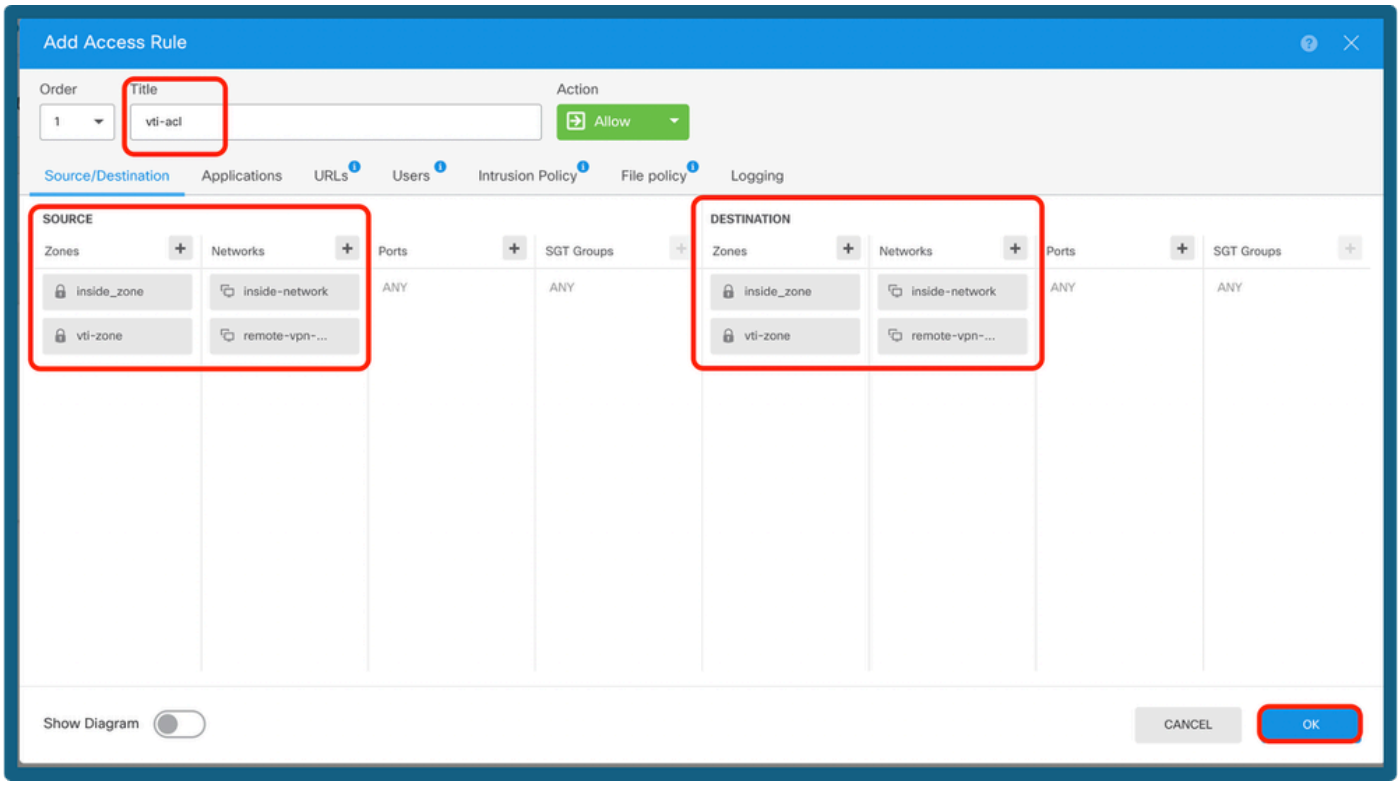

Edit Network Object
Name
remote-vpn-network
Description
Type
Network
Host
FQDN
Range
Network
172.16.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60
CANCEL
OK

远程IP配置



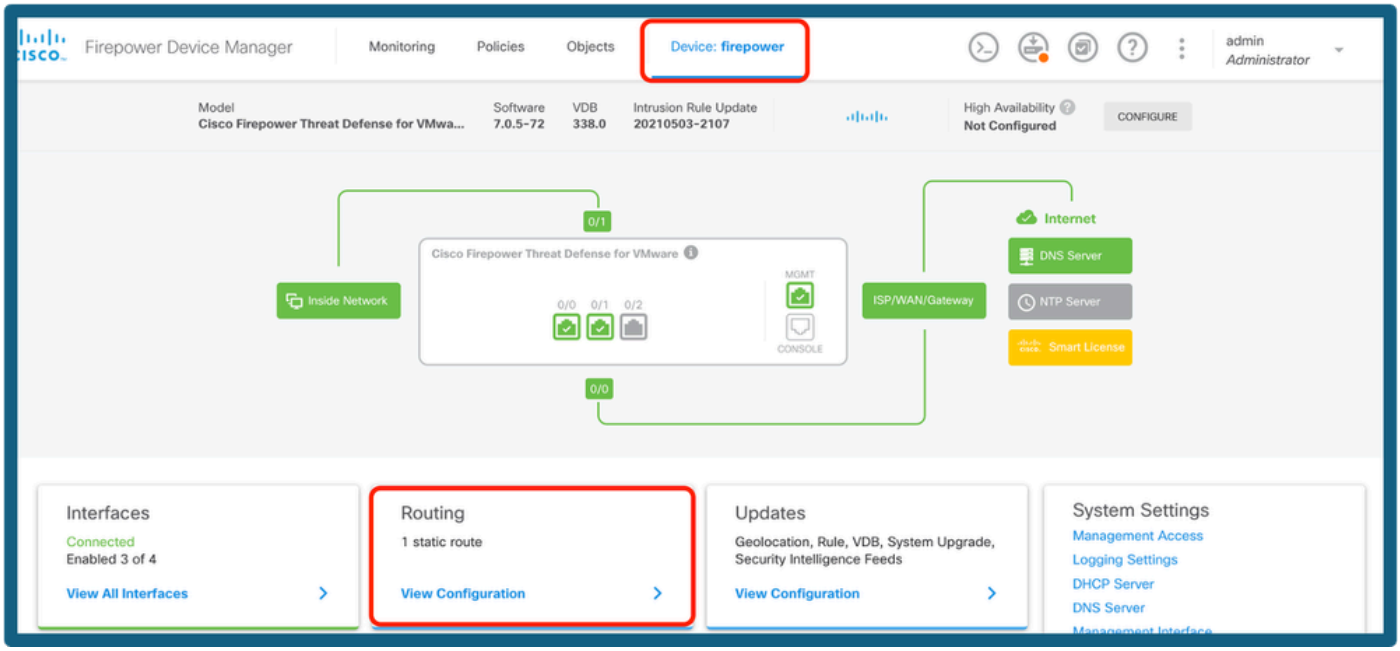
本地IP配置

步骤12.导航到Device > Policies，然后配置Access Control Policy。



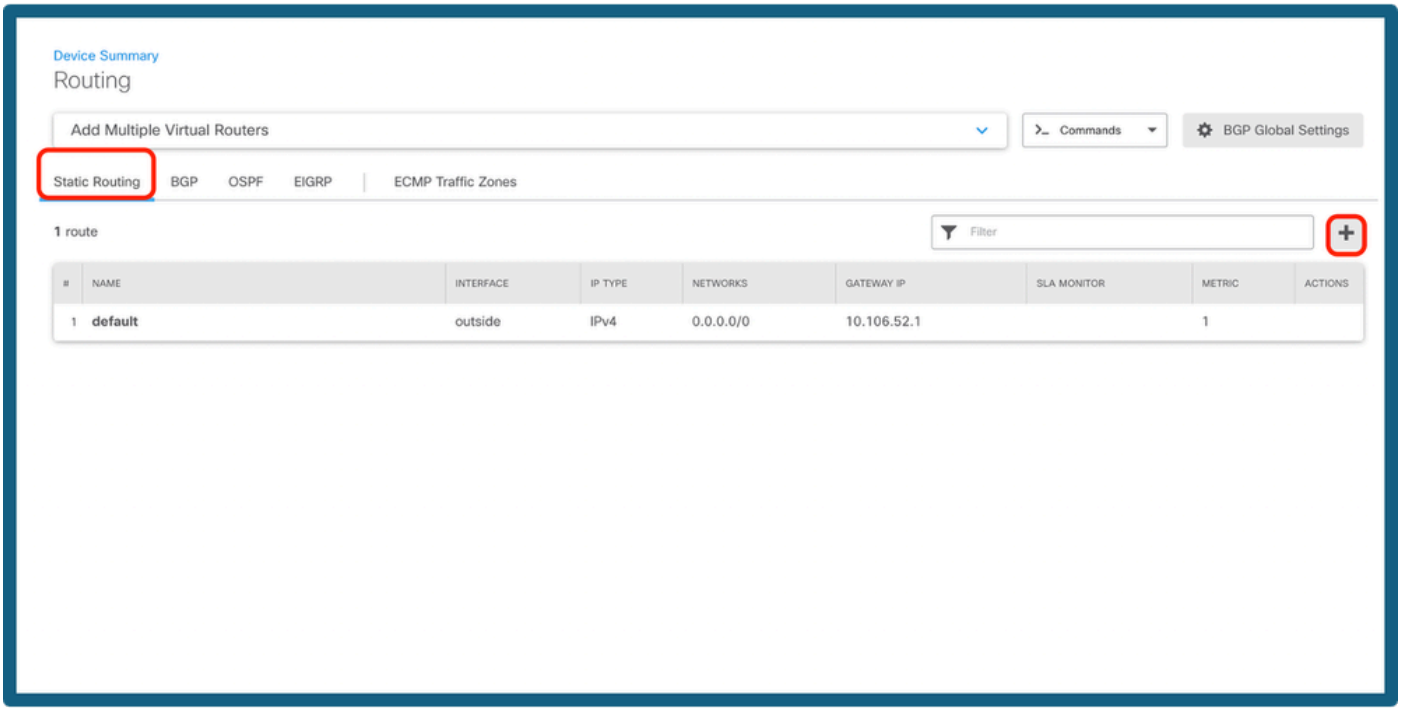
添加访问控制策略

步骤13a.添加通过VTI隧道的路由。导航到Device > Routing。



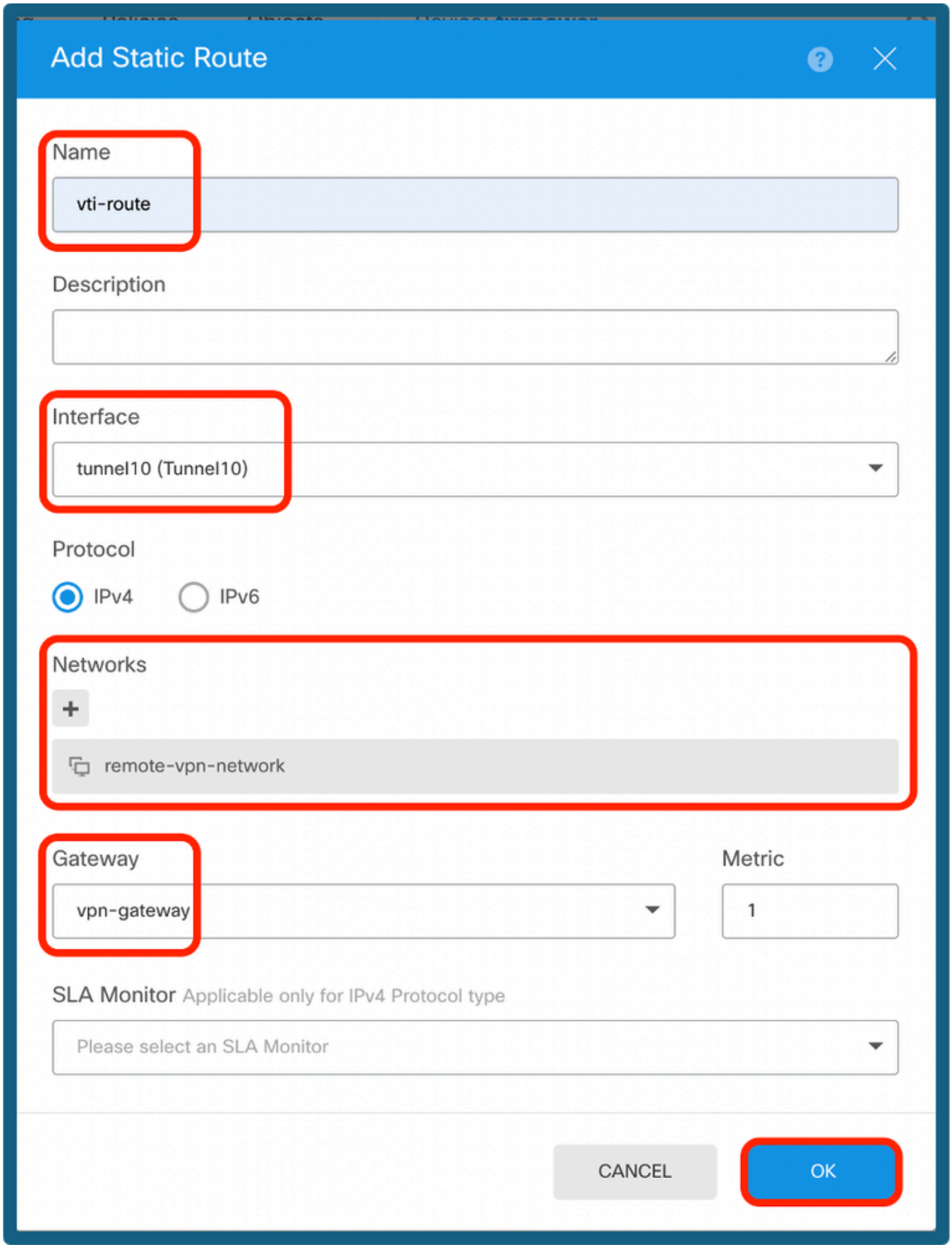
选择路由

步骤13b.导航到路由选项卡下的静态路由。单击+图标。



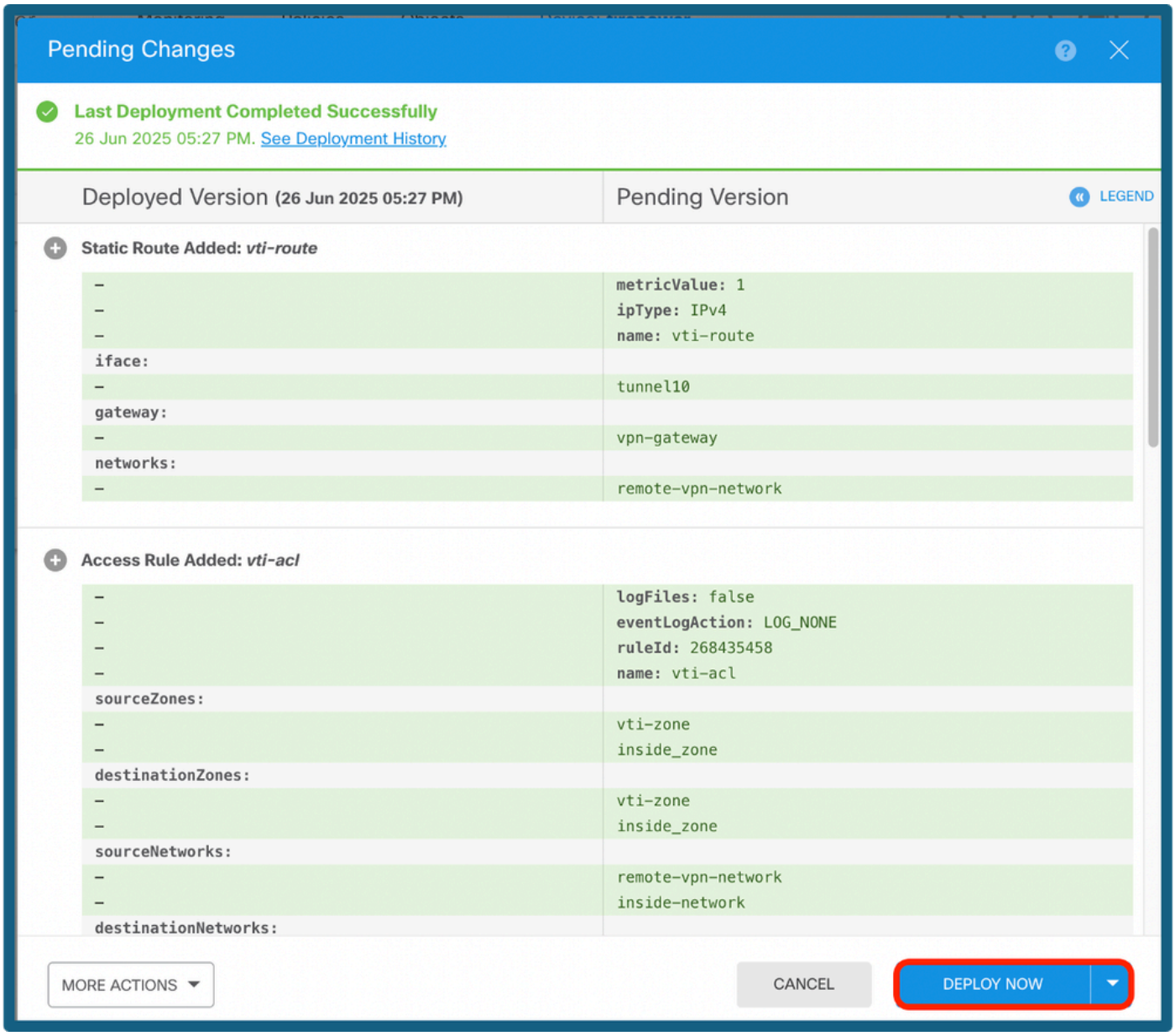
添加路由

步骤13c.提供接口，选择网络，提供网关。Click OK.



配置静态路由

步骤14.导航到部署。查看更改，然后单击Deploy Now。



部署配置

验证

部署完成后，可以使用以下命令验证CLI上的隧道状态：

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>

```
> show crypto ikev2 sa
IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  Status         Role
3294213359 10.106.52.222/500                      10.106.63.23/500                        READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/141 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x26a14554/0xd5db88bc
> show crypto ipsec sa
interface: tunnel10
    Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 10.106.63.23
```

显示命令

相关信息

有关由FDM管理的FTD上的站点到站点VPN的详细信息，可在此处找到完整的配置指南：

FDM管理的FTD配置指南

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）。