在FDM管理的FTD上配置具有PBR的双活动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
- 配置
  - 网络图
  - VPN上的配置
    - 站点1 FTD VPN配置
    - 站点2 FTD VPN配置
  - PBR上的配置
    - 站点1 FTD PBR配置
    - 站点2 FTD PBR配置
  - SLA监控器上的配置
    - 站点1 FTD SLA监控器配置
    - 站点2 FTD SLA监控器配置
  - 静态路由配置
    - 站点1 FTD静态路由配置
    - 站点2 FTD静态路由配置
- 验证
  - ISP1和ISP2工作正常
    - VPN
    - 路由
    - SLA监控
    - Ping 测试
  - 当ISP2正常工作时，ISP1会遇到中断
    - VPN
    - 路由
    - SLA监控
    - Ping 测试
  - 当ISP1工作正常时，ISP2会遇到中断
    - VPN
    - 路由
    - SLA监控
    - Ping 测试
- 故障排除

简介

本文档介绍如何在FDM管理的FTD上使用PBR配置基于双活动路由的站点到站点VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 对VPN的基本了解
- 基本了解基于策略的路由(PBR)
- 基本了解Internet协议服务级别协议(IP SLA)
- 使用FDM的经验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTDv版本7.4.2
- 思科FDM版本7.4.2

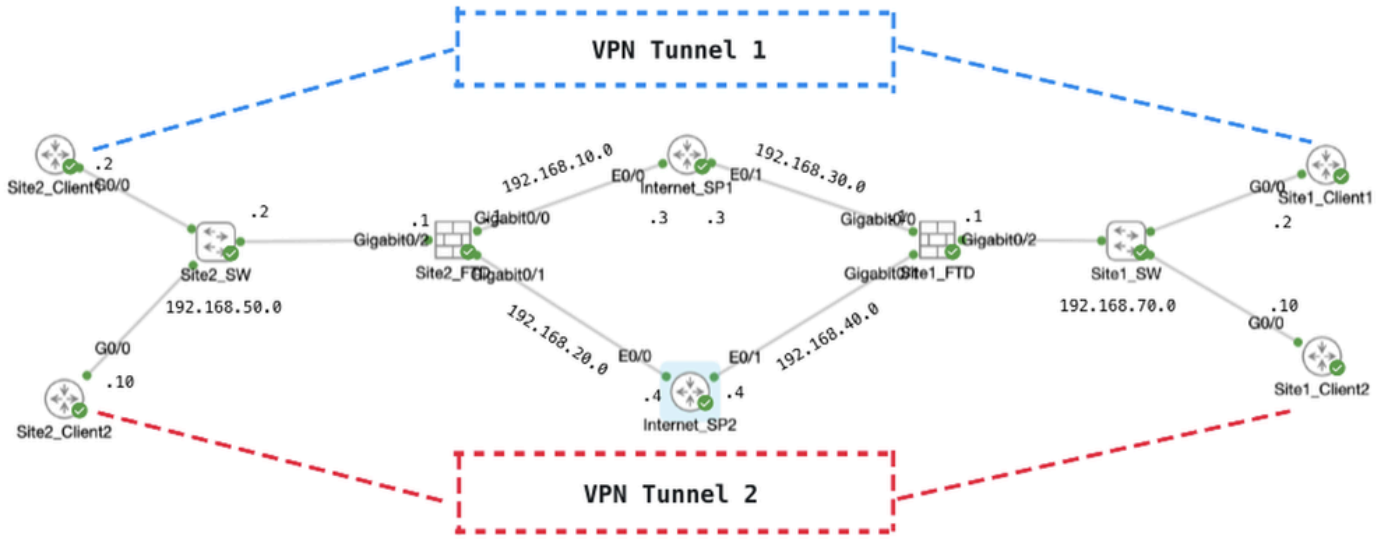
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档说明如何在FTD上配置基于双活动路由的站点到站点VPN。在本例中，站点1和站点2的FTD具有两个活动ISP连接，从而同时与两个ISP建立站点到站点VPN。默认情况下，VPN流量通过ISP1的Tunnel 1（蓝线）。 对于特定主机，流量通过ISP2上的Tunnel 2（红线）。 如果ISP1遇到中断，流量会切换到ISP2作为备份。相反，如果ISP2遇到中断，流量会切换到ISP1作为备份。本示例使用基于策略的路由(PBR)和互联网协议服务级别协议(IP SLA)来满足这些要求。

配置

网络图



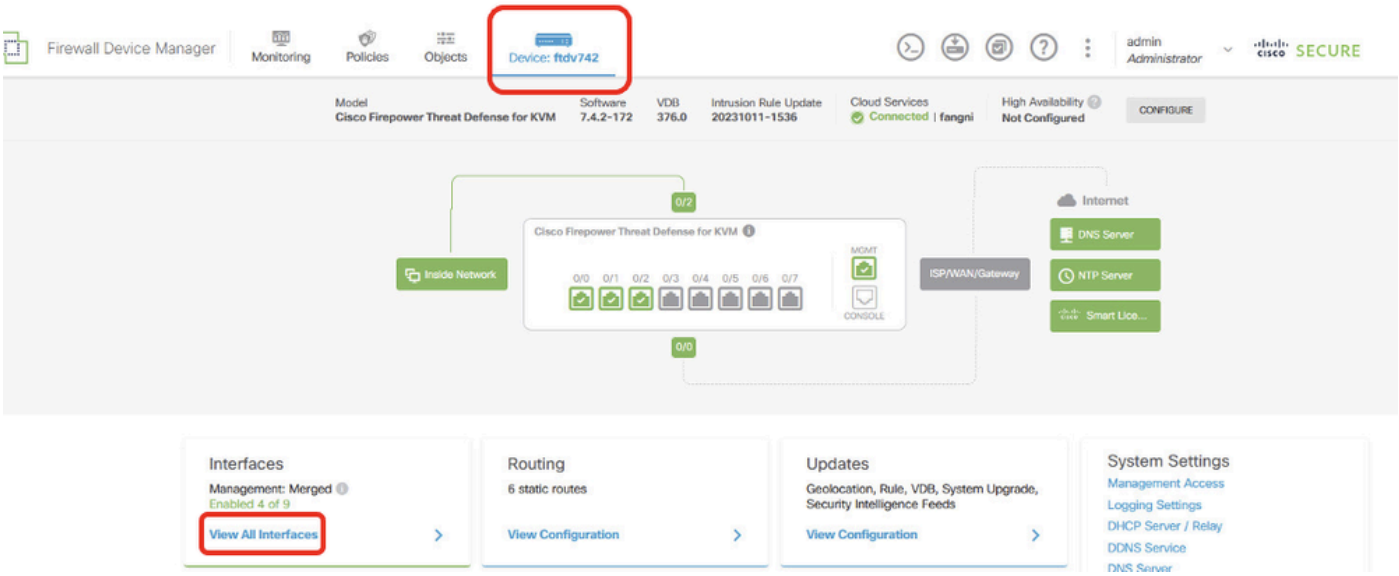
拓扑

VPN上的配置

必须确保节点之间的IP互联的初步配置已经及时完成。站点1和站点2中的客户端都使用FTD内部IP地址作为网关。

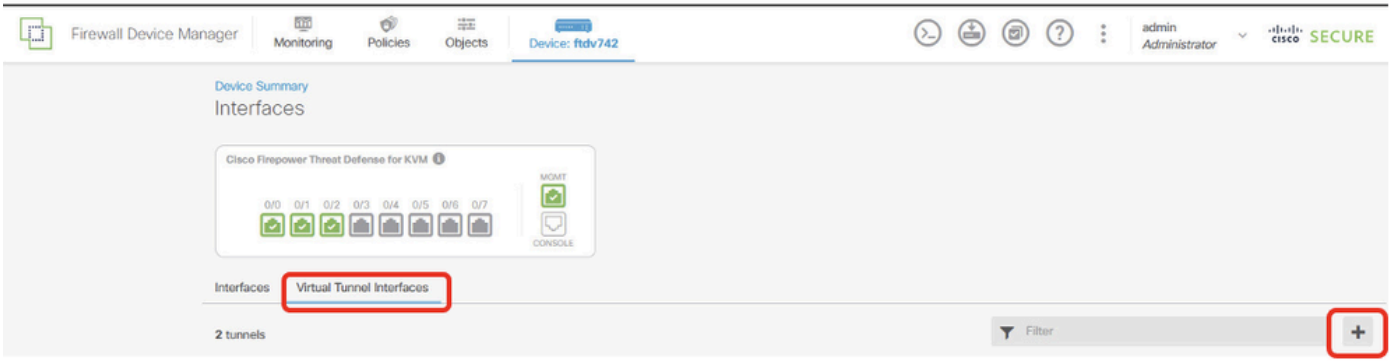
站点1 FTD VPN配置

步骤1.为ISP1和ISP2创建虚拟隧道接口。登录Site1 FTD的FDM GUI。导航到Device > Interfaces。单击查看所有接口。



Site1FTD_View_All_Interfaces

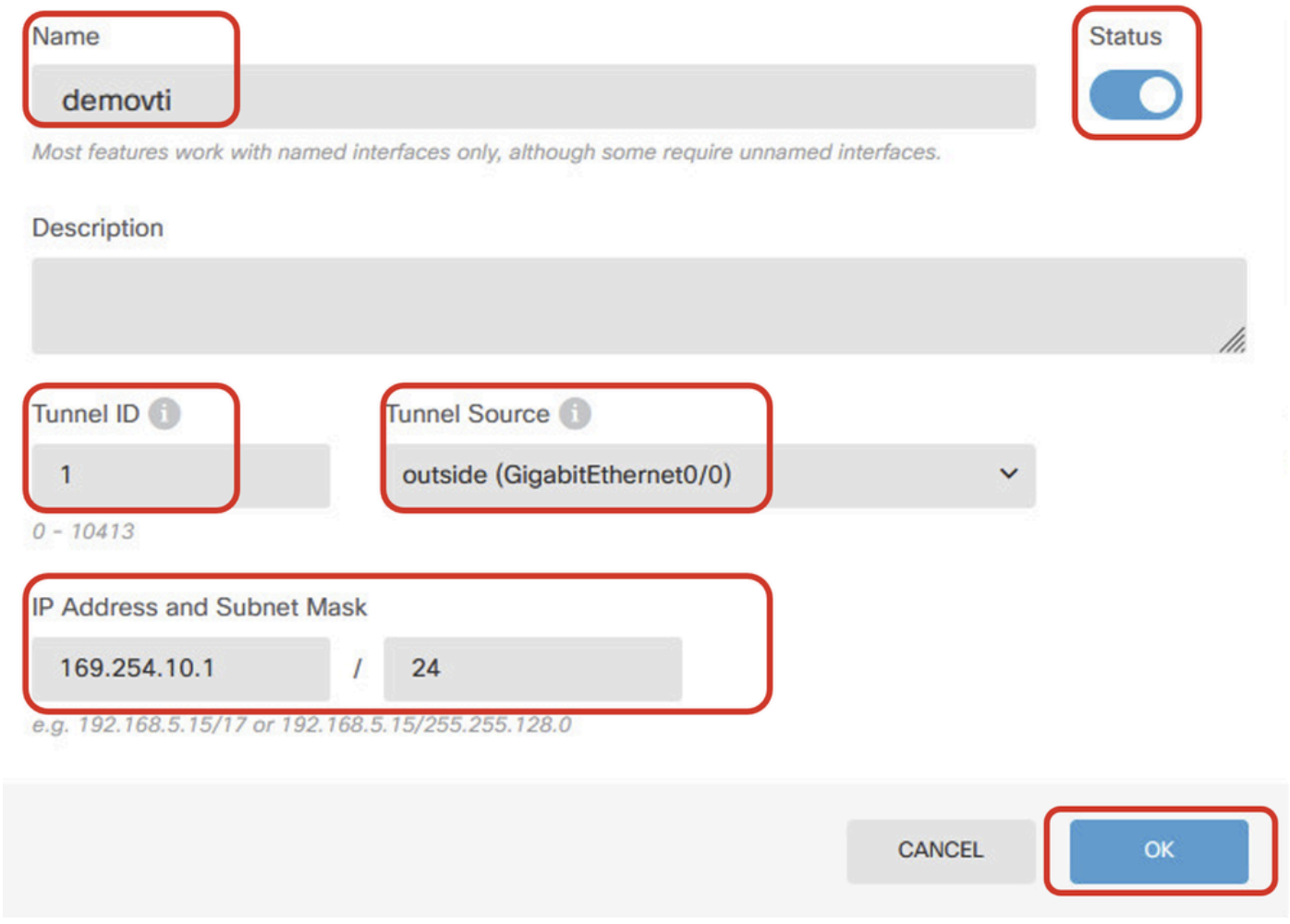
步骤2.单击Virtual Tunnel Interfaces选项卡，然后单击+按钮。



Site1FTD_Create_VTI

步骤3.提供VTI详细信息的必要信息。单击OK按钮。

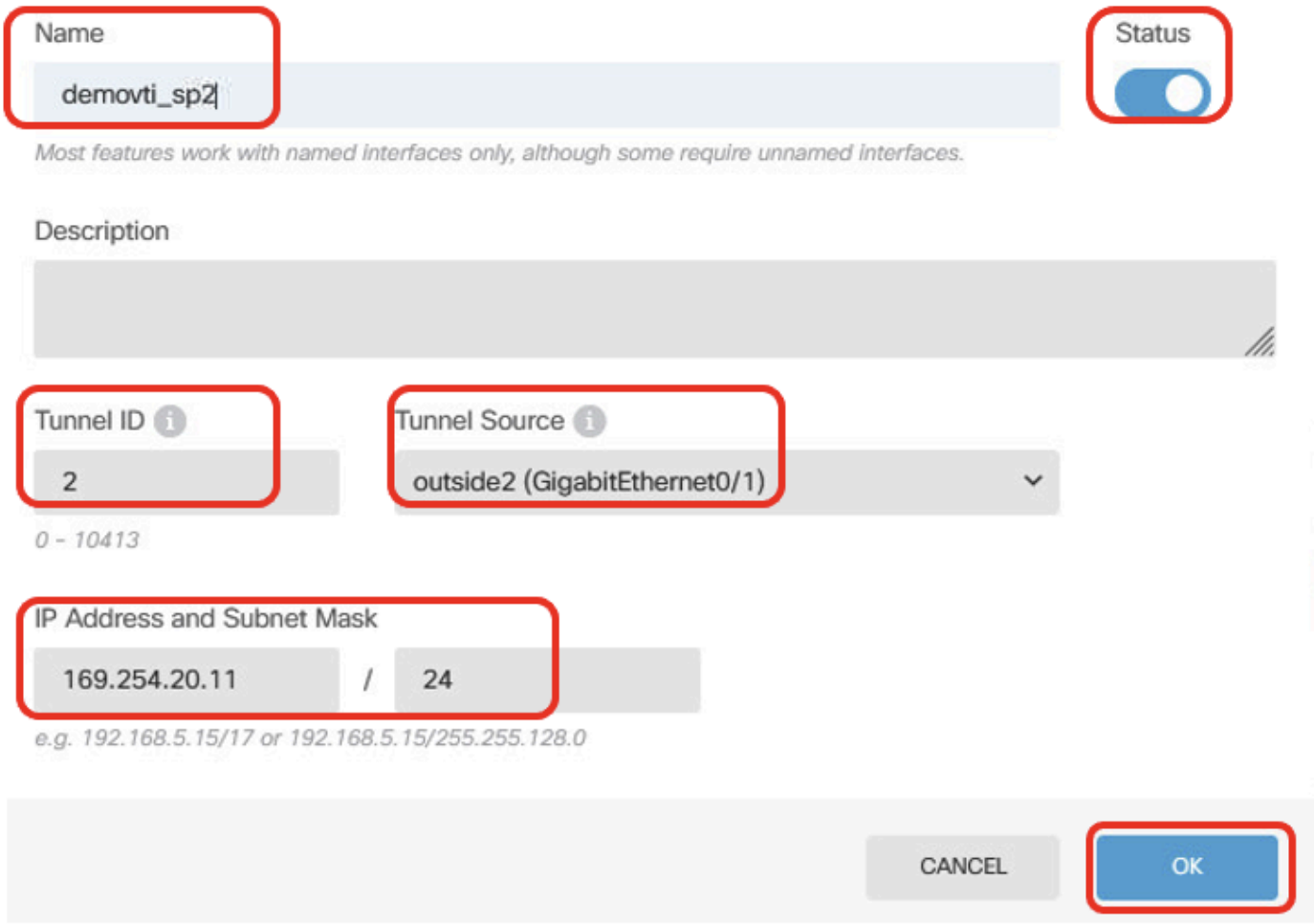
- 名称：demovti
- 隧道ID:1
- 通道来源:外部(GigabitEthernet0/0)
- IP 地址和子网掩码:169.254.10.1/24
- 状态:单击滑块到“已启用”位置



站点1FTD_VTI_详细信息_隧道1_ISP1

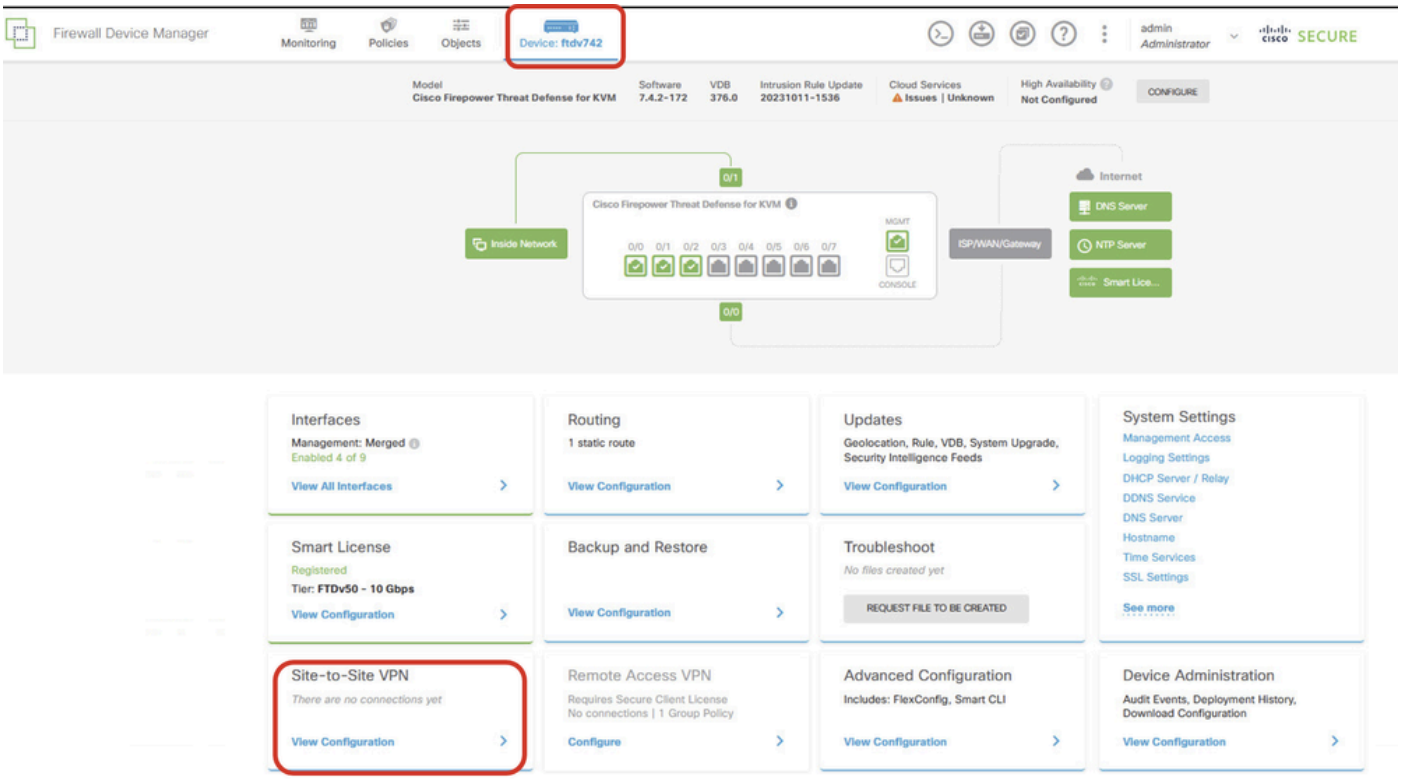
- 名称：demovti_sp2
- 隧道ID:2

- 通道来源:outside2(GigabitEthernet0/1)
- IP 地址和子网掩码:169.254.20.11/24
- 状态:单击滑块到“已启用”位置



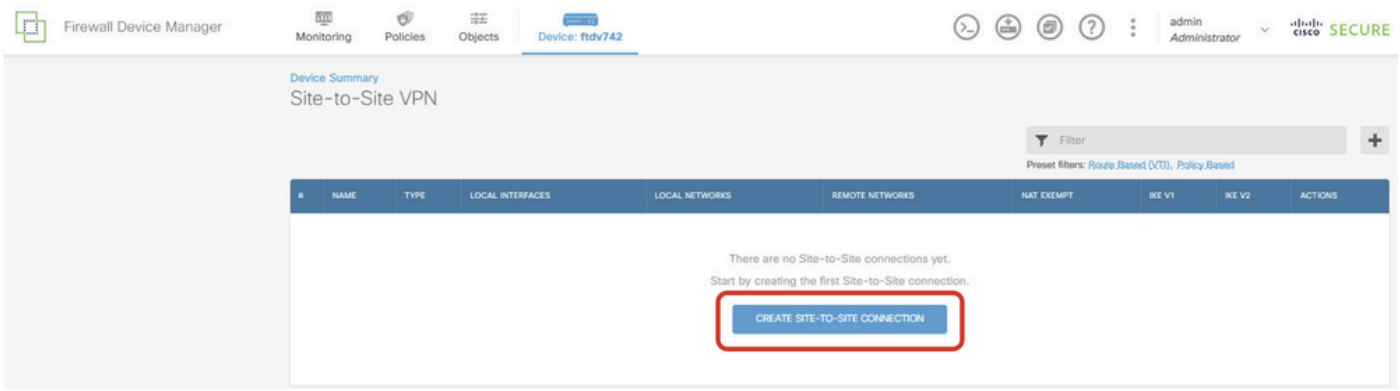
站点1FTD_VTI_详细信息_隧道2_ISP2

步骤4.导航到Device > Site-to-Site VPN。单击View Configuration按钮。



Site1FTD_View_Site2Site_VPN

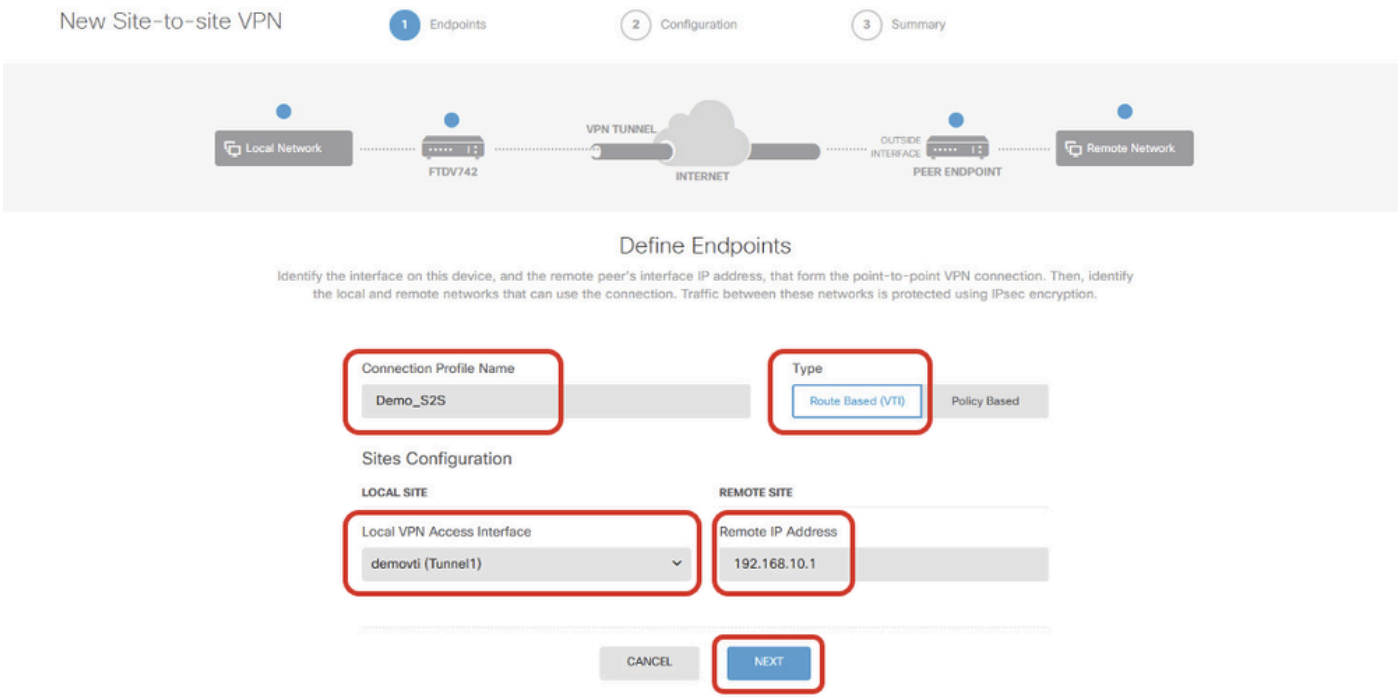
步骤5.开始通过ISP1创建新的站点到站点VPN。单击CREATE SITE-TO-SITE CONNECTION按钮，或单击+按钮。



Site1FTD_Create_Site-to-Site_Connection

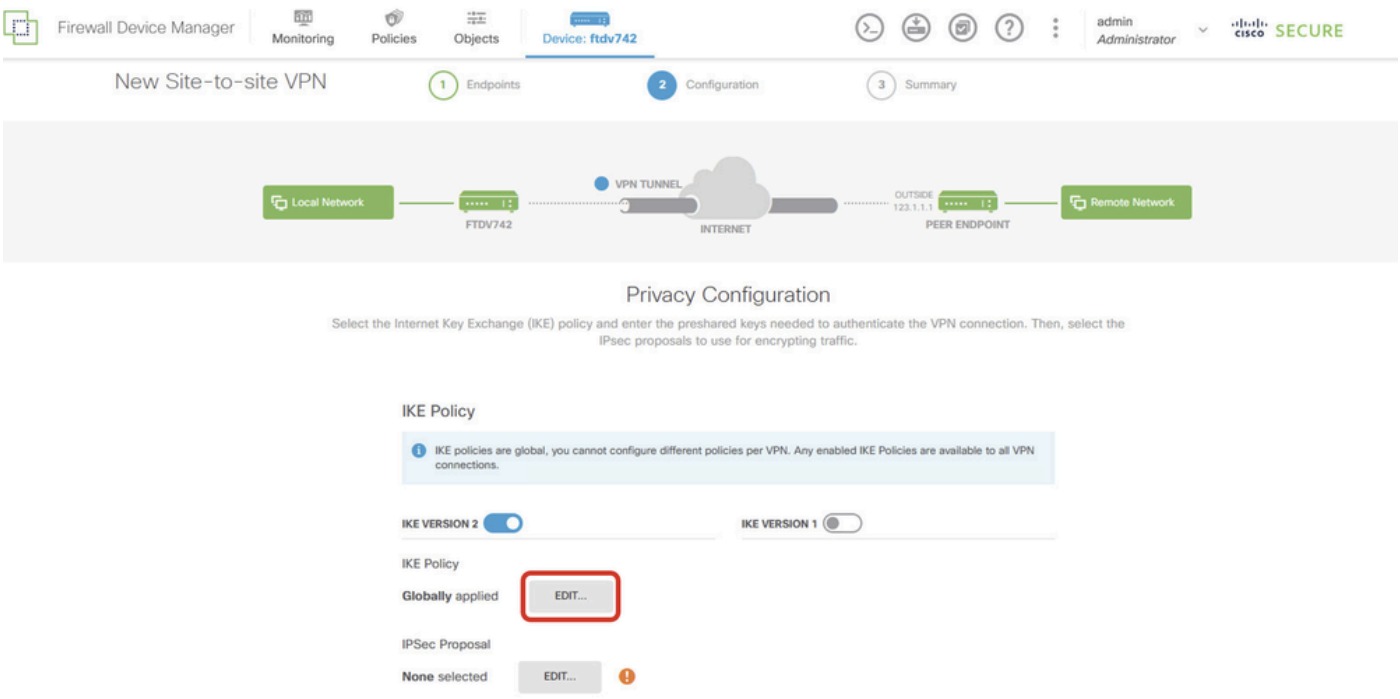
步骤5.1.提供端点的必要信息。单击NEXT按钮。

- 连接配置文件名称：Demo_S2S
- type：基于路由(VTI)
- 本地VPN访问接口：demovti（在步骤3中创建。）
- 远程 IP 地址:192.168.10.1（这是Site2 FTD ISP1 IP地址）



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

第5.2步：导航到IKE策略。单击EDIT按钮。



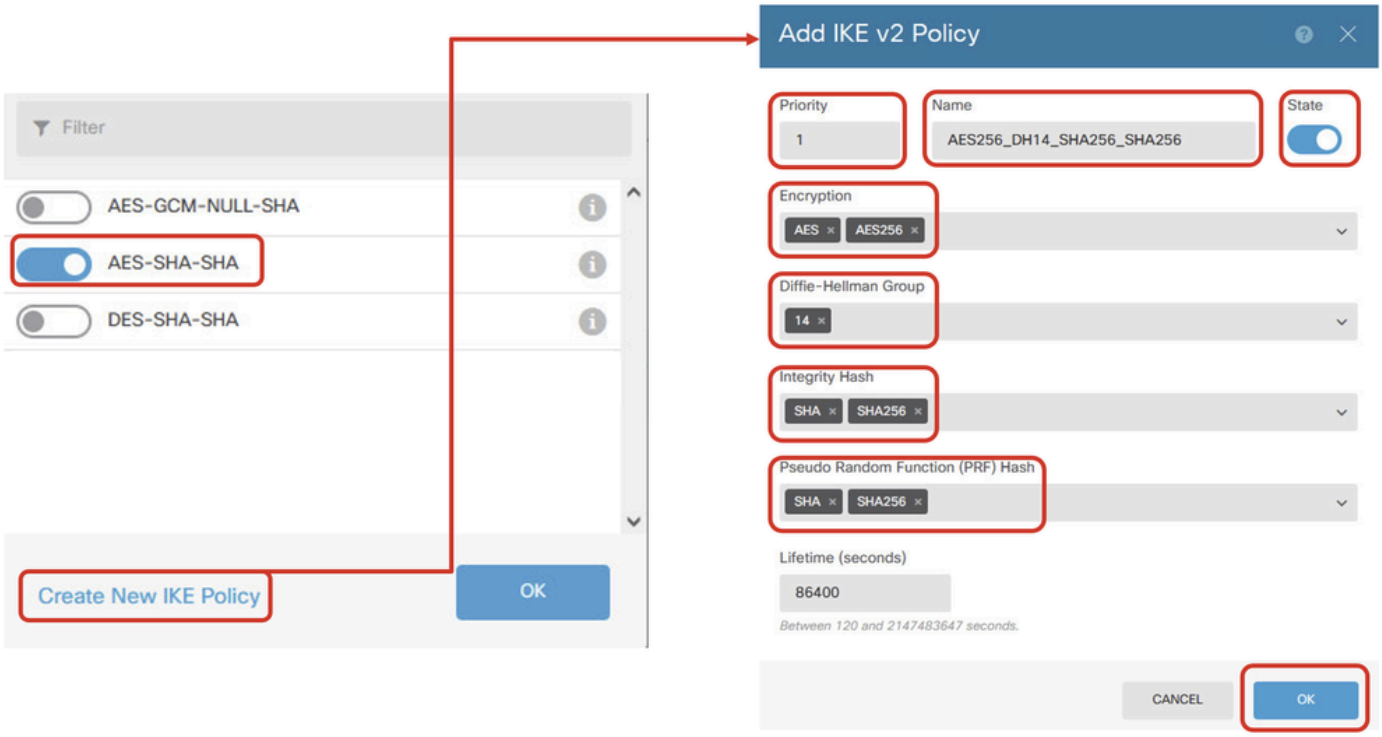
Site1FTD_Edit_IKE_Policy

第5.3步：对于IKE策略，您可以使用预定义，也可以通过点击创建新IKE策略来创建一个新策略。

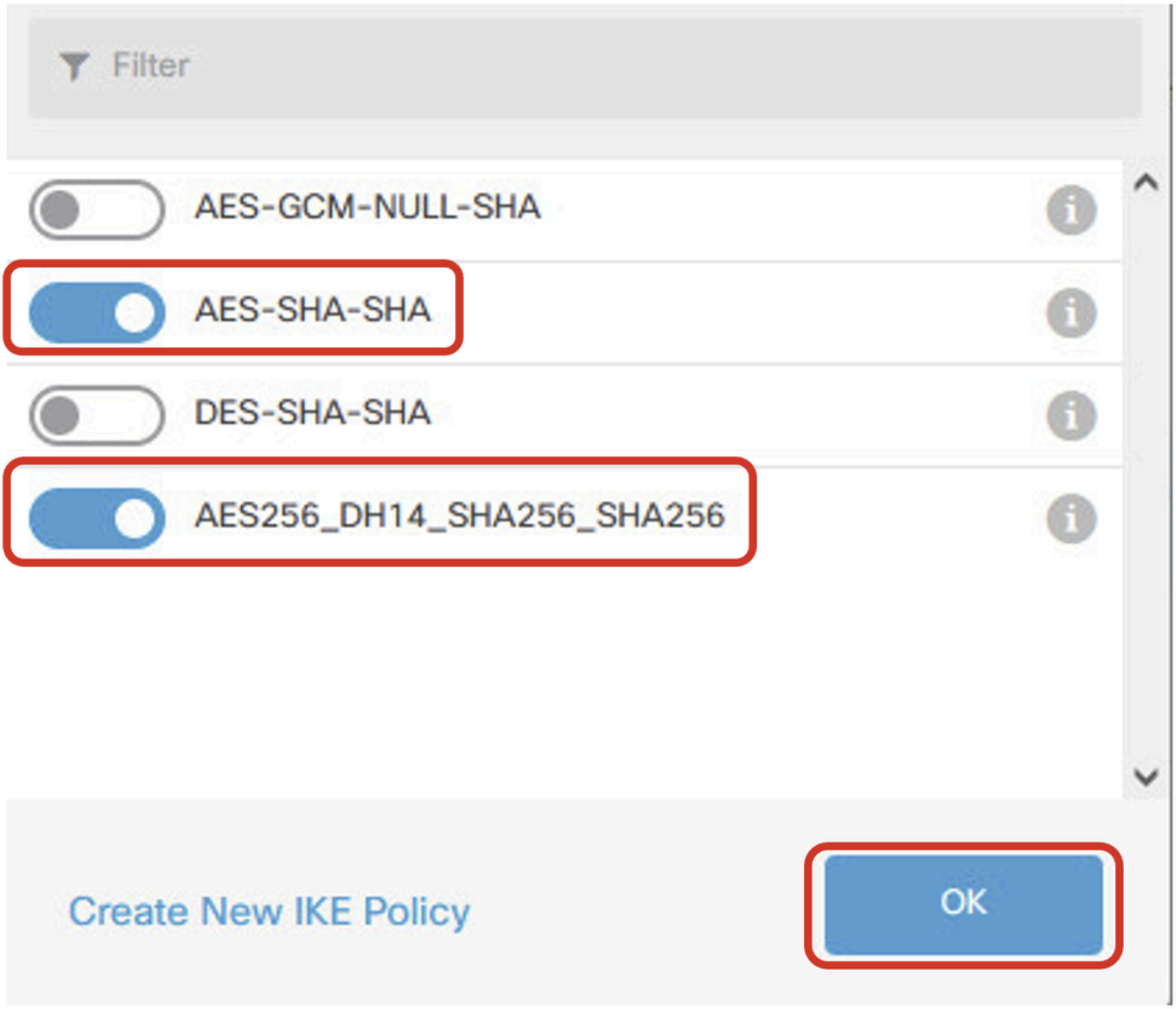
在本示例中，切换现有IKE策略AES-SHA-SHA，并创建一个新策略用于演示。单击OK按钮进行保存。

- 名称：AES256_DH14_SHA256_SHA256

- 加密 :AES、AES256
- DH Group：14
- 完整性哈希：SHA256
- PRF哈希：SHA256
- 生命期：86400 (default)

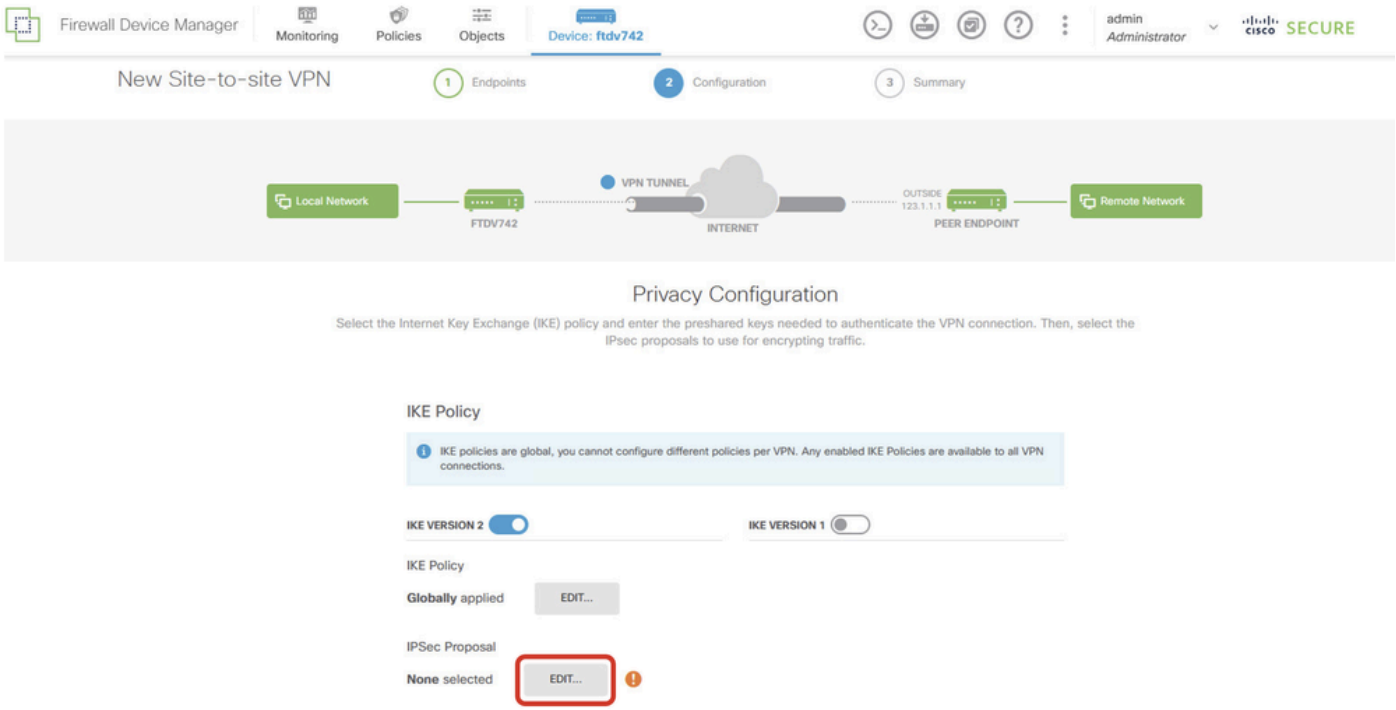


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

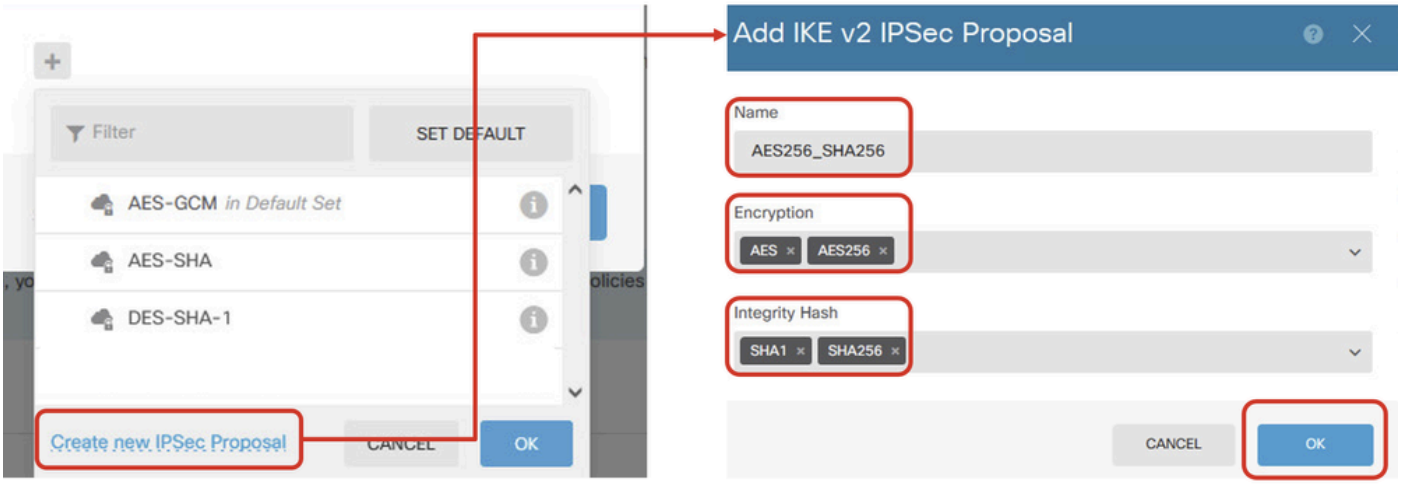
步骤5.4.导航至IPSec建议。单击EDIT按钮。



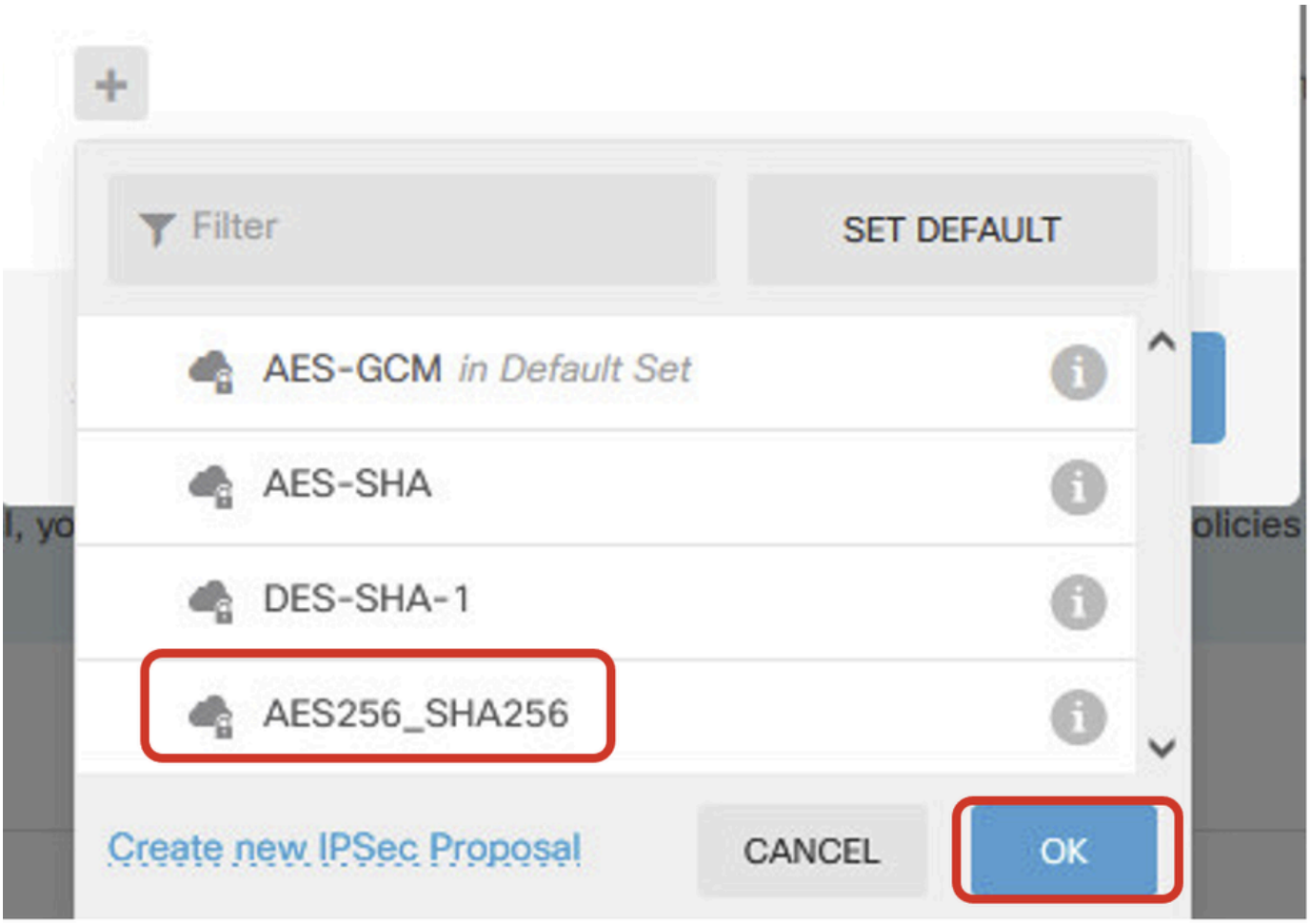
Site1FTD_Edit_IKE_Proposal

第5.5步：对于IPSec提议，您可以使用预定义，也可以通过单击创建新的IPSec提议创建一个新提议。在本示例中，为演示目的创建新示例。单击OK按钮进行保存。

- 名称：AES256_SHA256
- 加密 :AES、AES256
- 完整性哈希：SHA1、SHA256



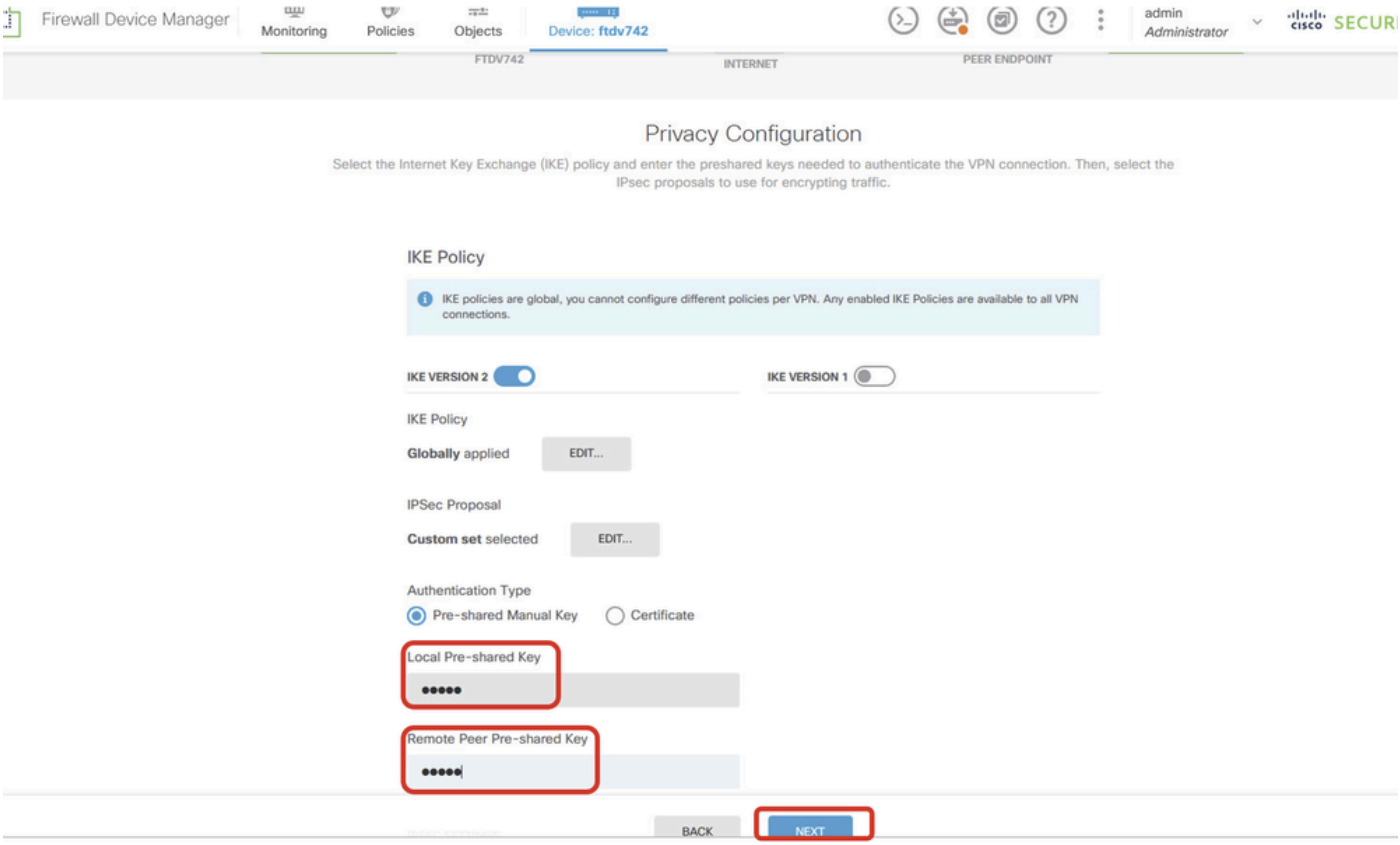
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

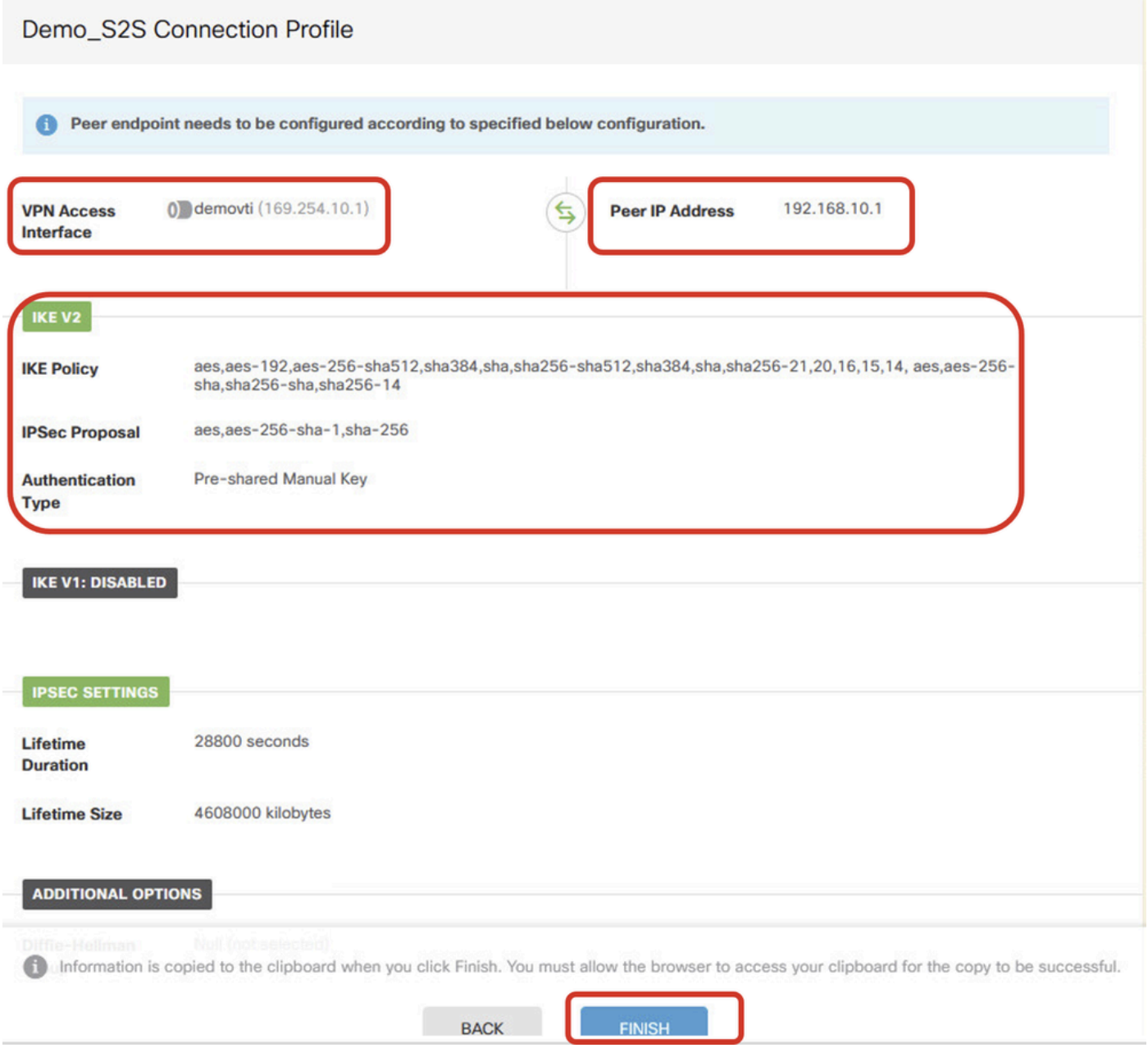
步骤5.6.向下滚动页面并配置预共享密钥。点击NEXT按钮。

记下此预共享密钥，稍后在Site2 FTD上配置它。



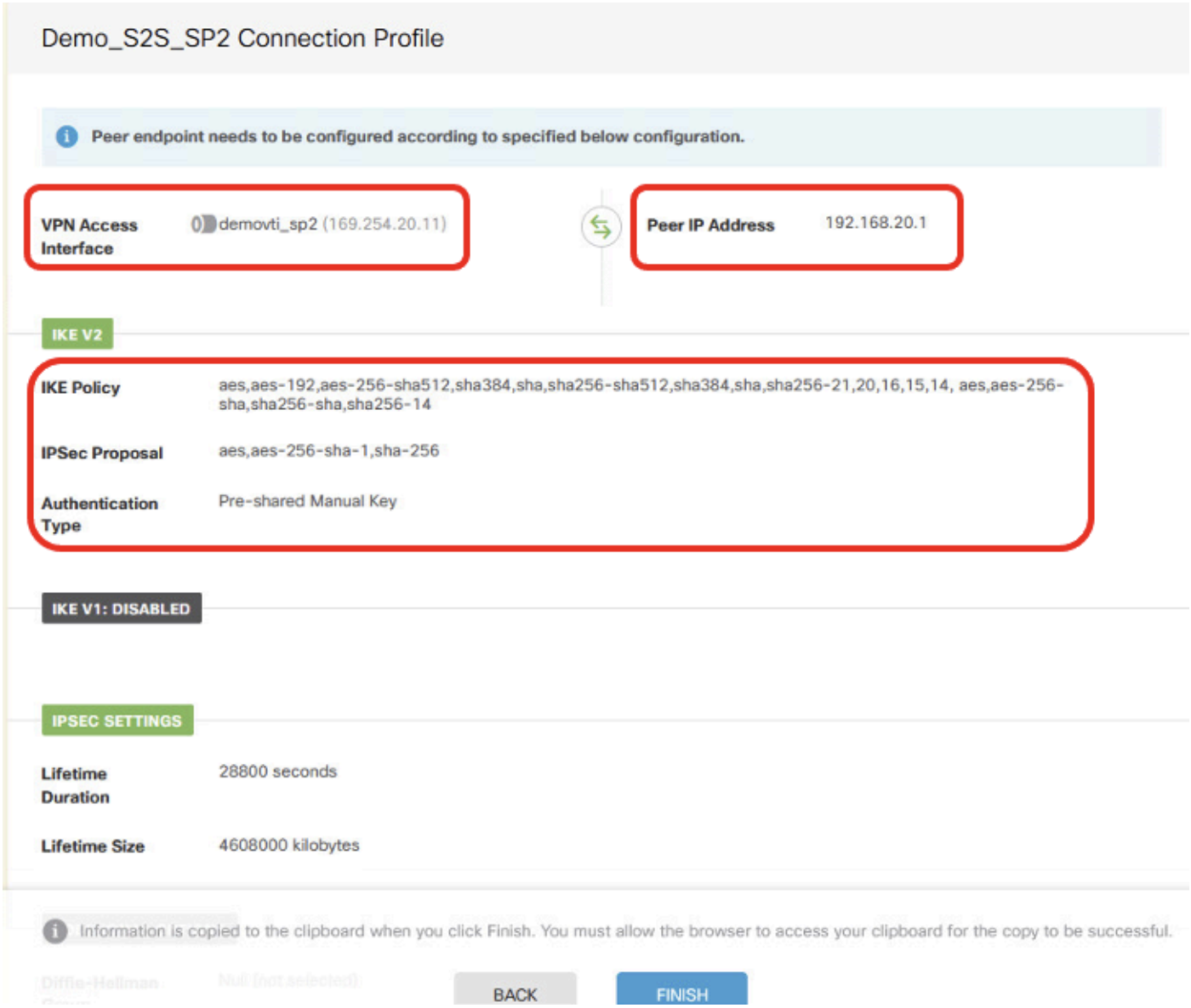
Site1FTD_Configure_Pre_Shared_Key

步骤5.7.检查VPN配置。如果需要修改任何内容，请单击BACK按钮。如果一切正常，请单击FINISH按钮。



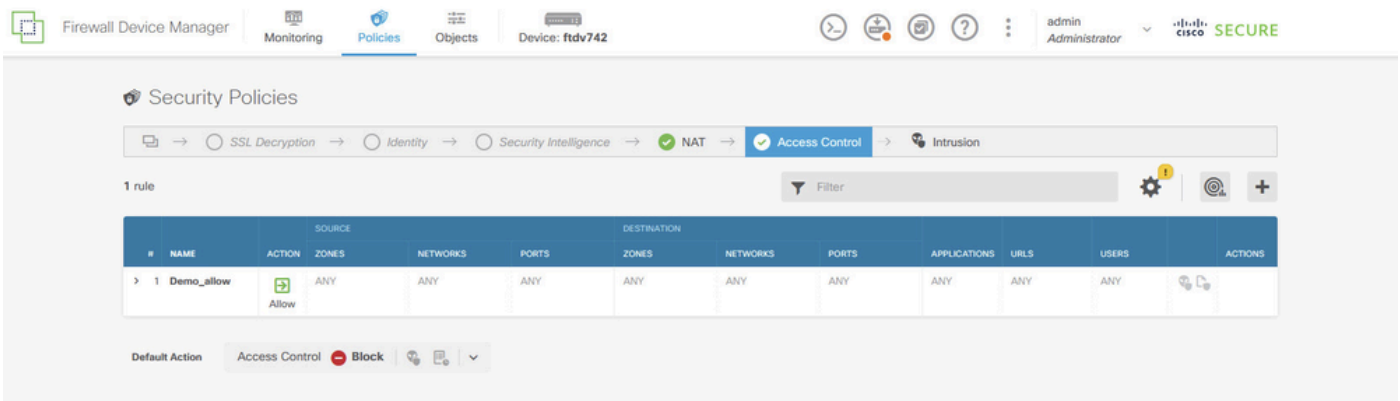
Site1FTD_ISP1_Review_VPN_Config_Summary

步骤6.重复步骤5.以通过ISP2创建新的站点到站点VPN。



Site1FTD_ISP2_Review_VPN_Config_Summary

步骤7.创建访问控制规则以允许流量通过FTD。在本示例中，允许所有内容用于演示目的。根据实际需要修改策略。



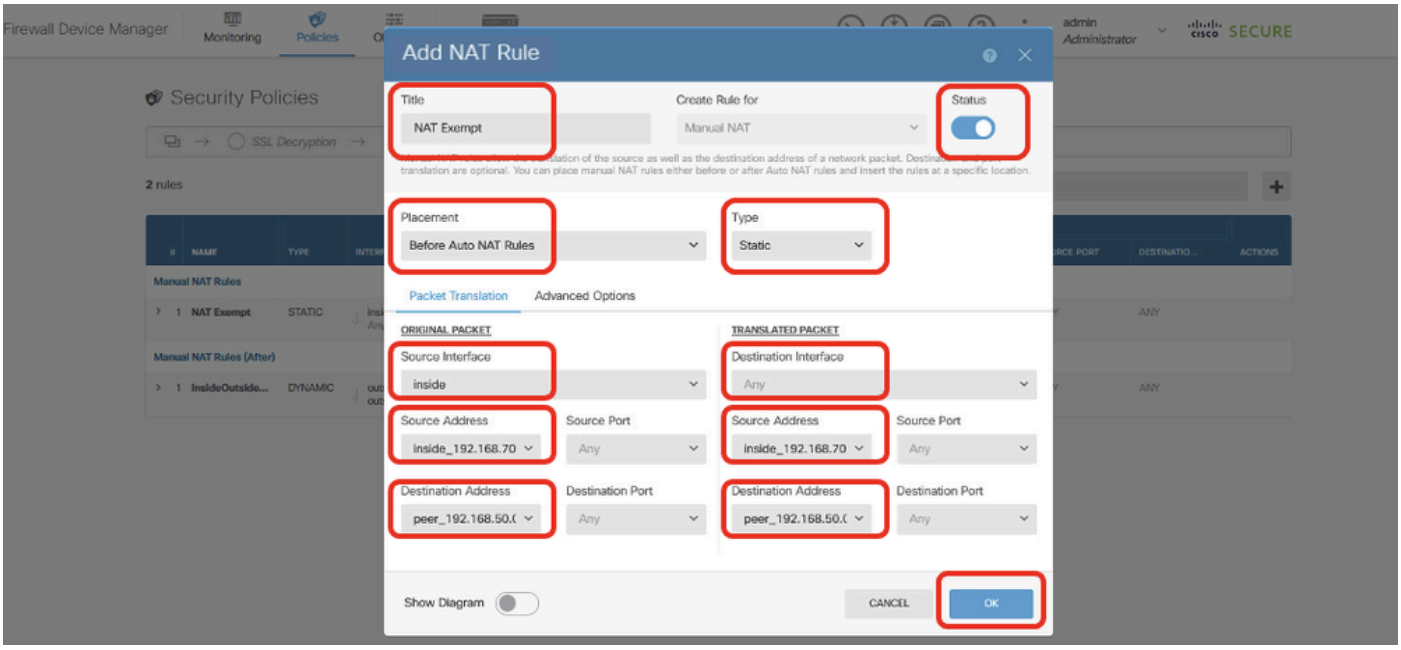
Site1FTD_Allow_Access_Control_Rule_Example

步骤8.(可选)如果为客户端配置了动态NAT以访问Internet，请在FTD上配置客户端流量的NAT免除规则。

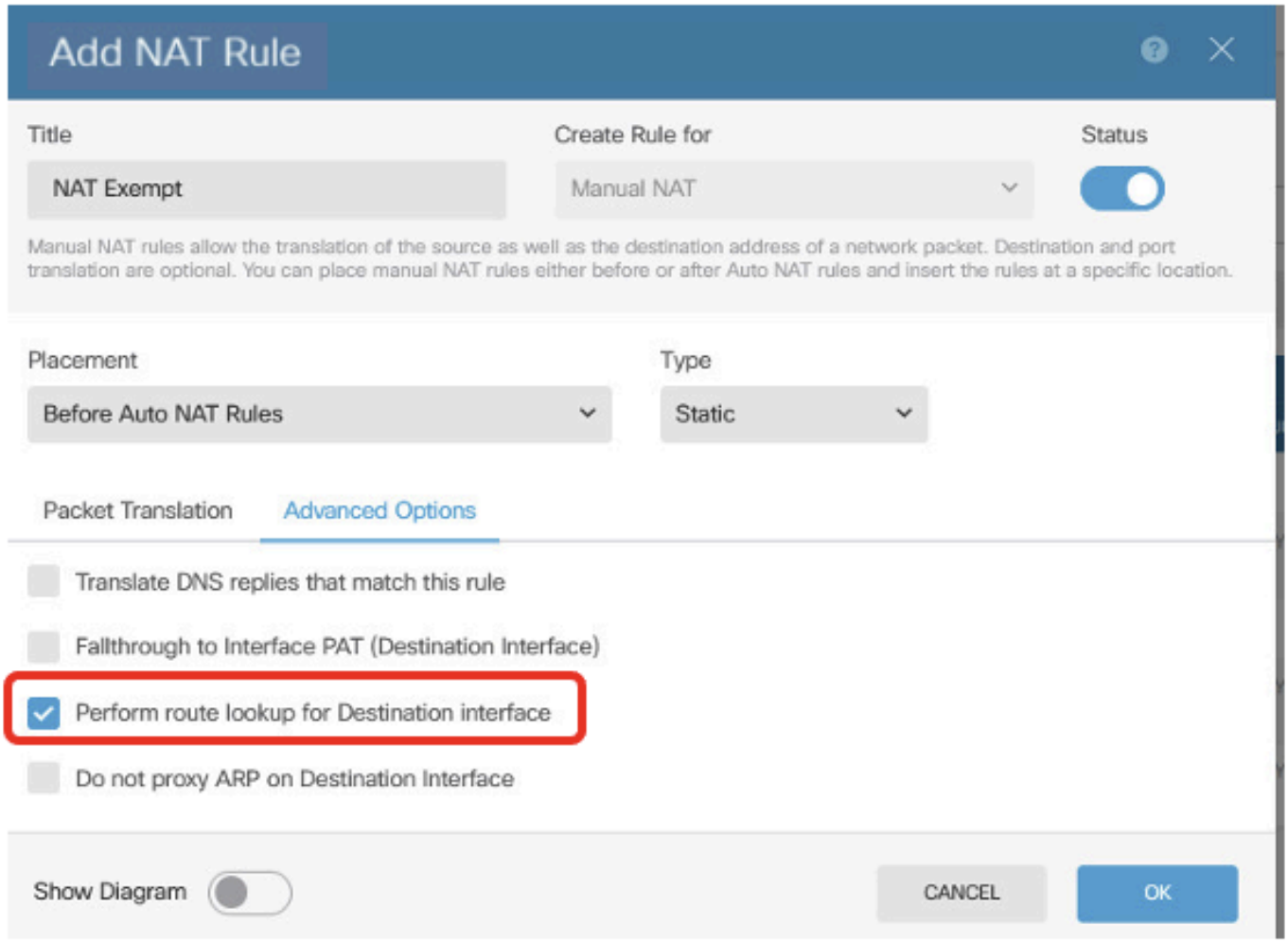
出于演示目的，本示例中为客户端配置了动态NAT以访问互联网。因此需要NAT豁免规则。

导航到Policies > NAT。单击+按钮。提供详细信息并单击OK。

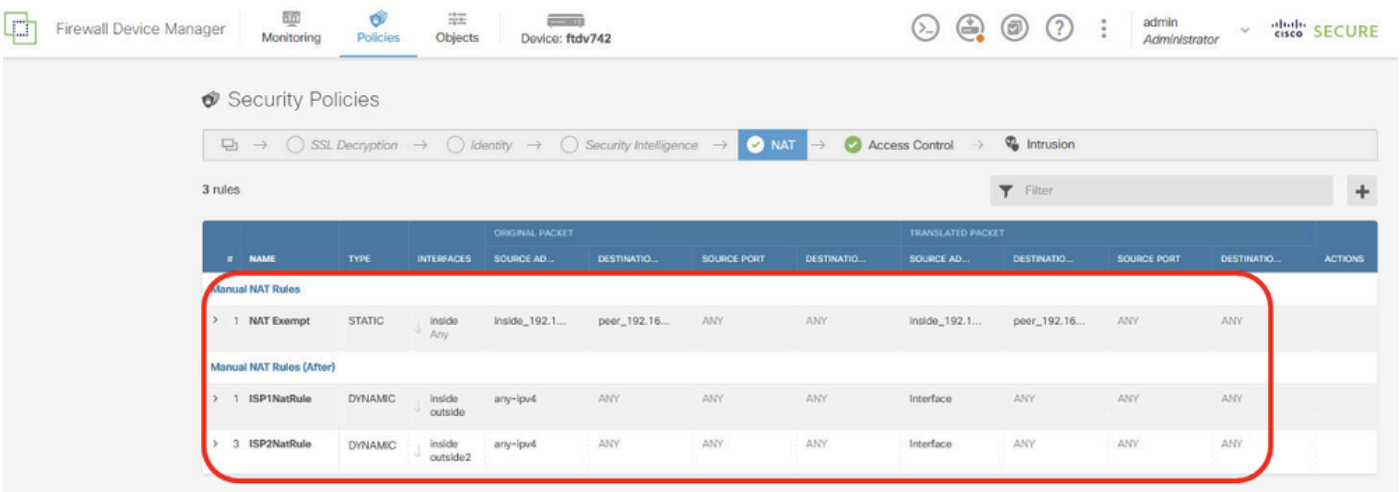
- Title:NAT免除
- 位置：在自动NAT规则之前
- type：静态
- 来源接口:内部
- 目的地：any
- 原始源地址：192.168.70.0/24
- 转换后的源地址：192.168.70.0/24
- 原始目的地址：192.168.50.0/24
- 转换后的目的地址：192.168.50.0/24
- 启用路由查找时



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



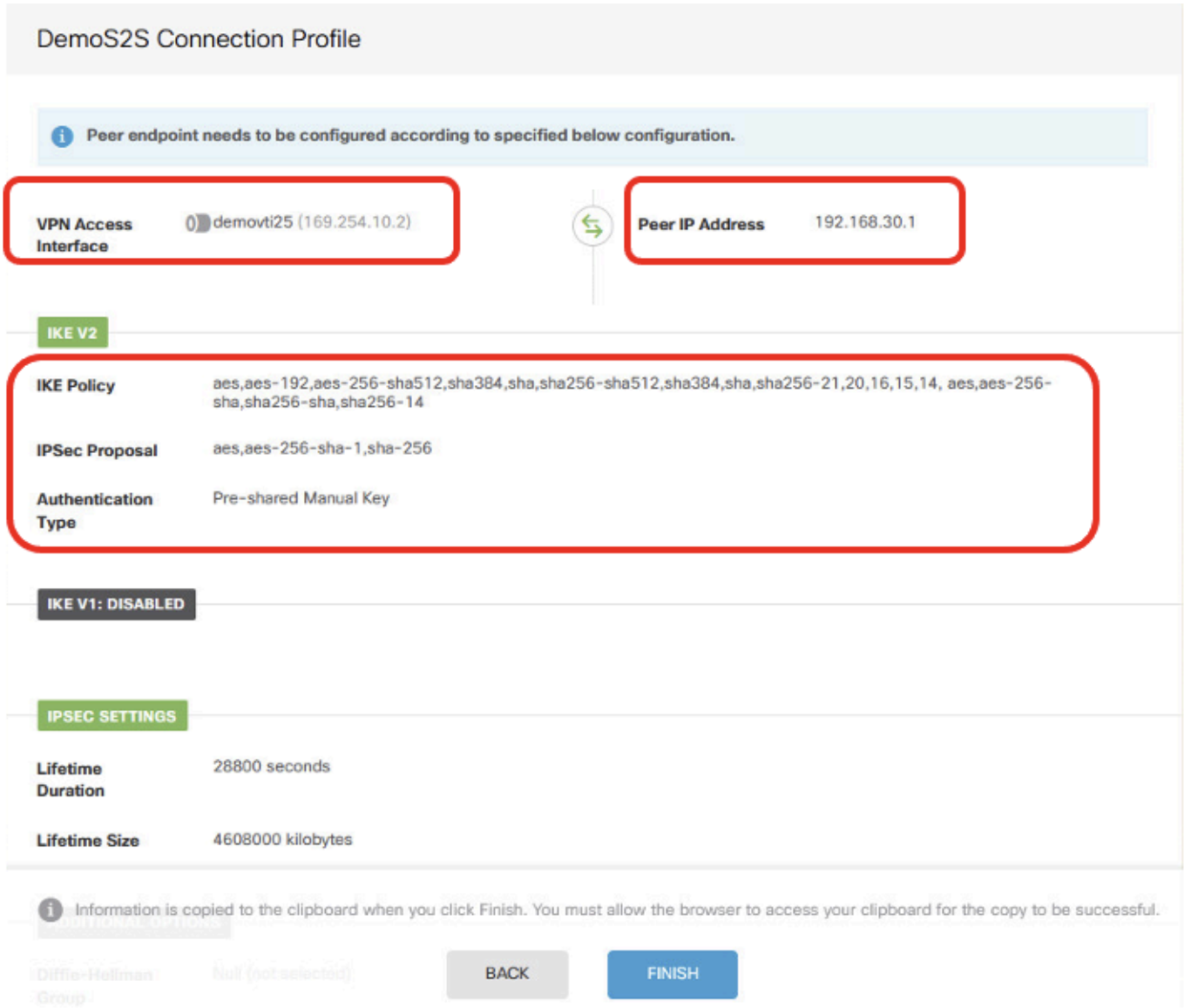
Site1FTD_Nat_Rule_Overview

步骤9.部署配置更改。

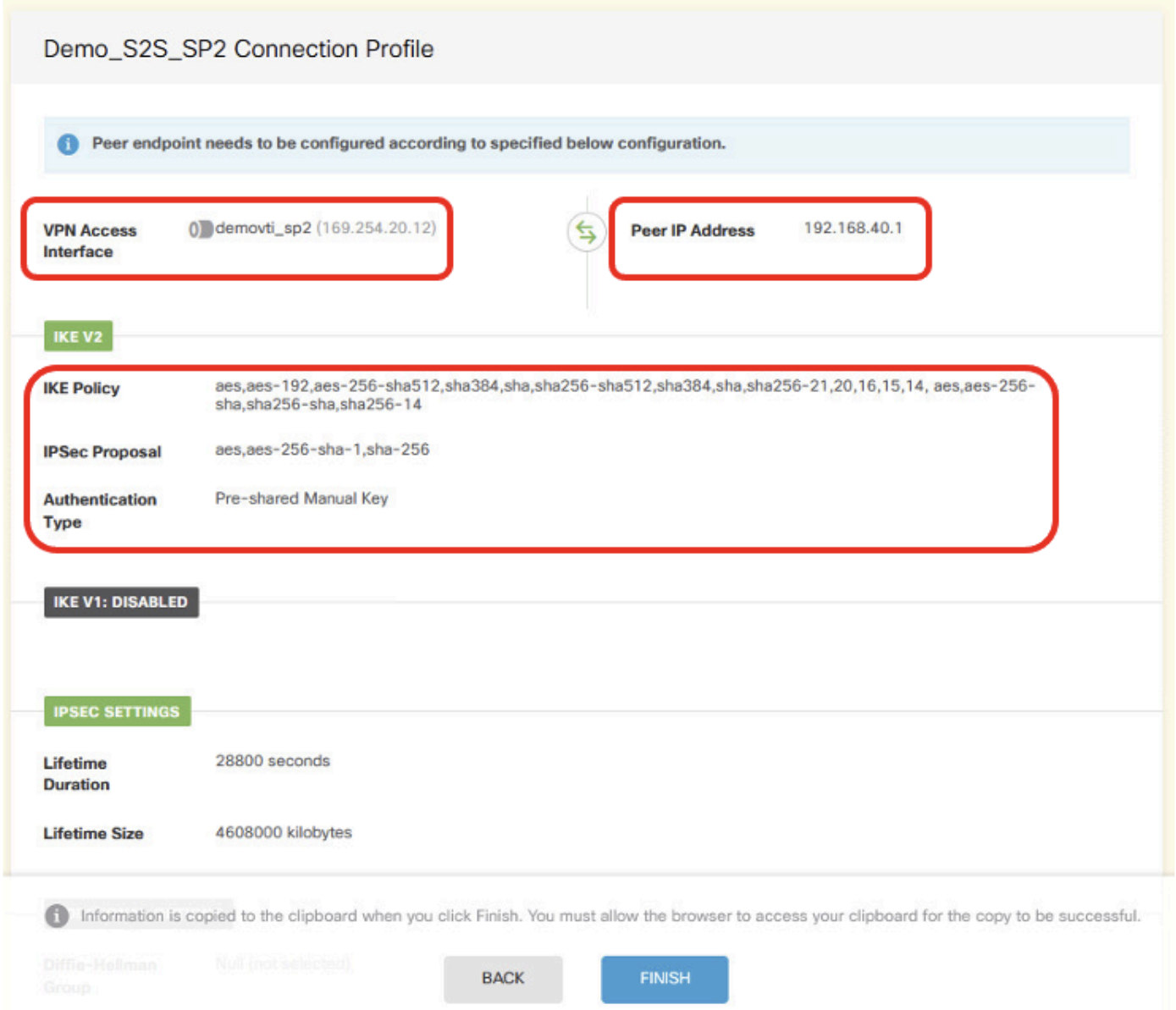
站点1FTD_部署_更改

站点2 FTD VPN配置

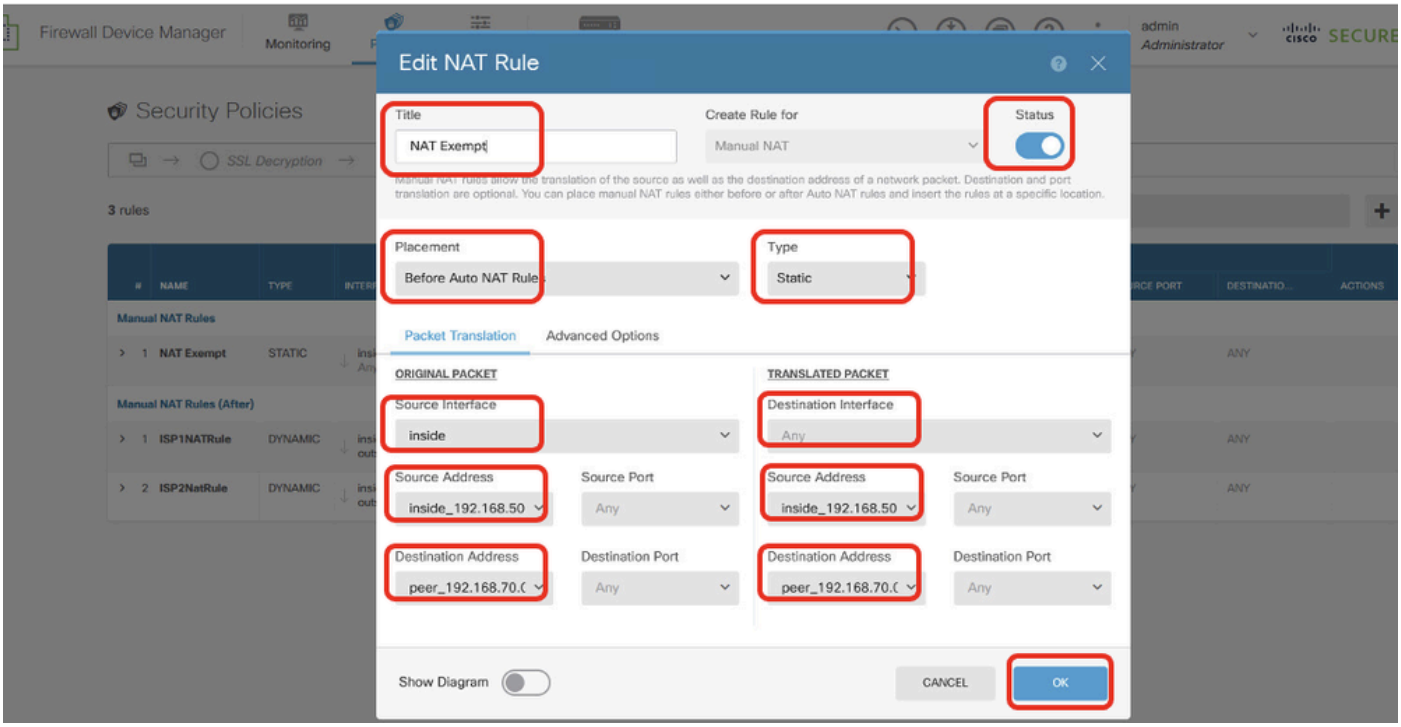
步骤10.使用站点2 FTD的相应参数重复步骤1到步骤9。



Site2FTD_ISP1_Review_VPN_Config_Summary



Site2FTD_ISP2_Review_VPN_Config_Summary

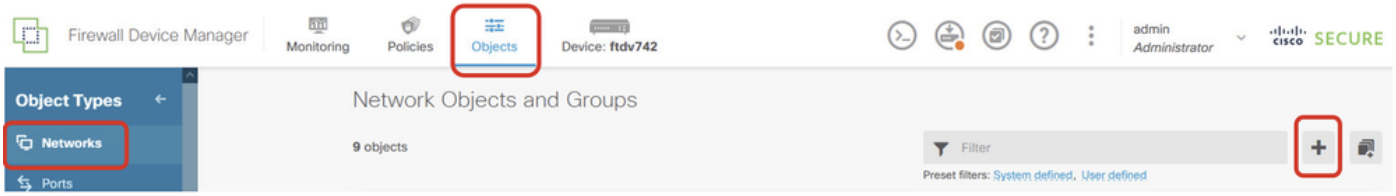


Site2FTD_Nat_Exempt_Rule

PBR上的配置

站点1 FTD PBR配置

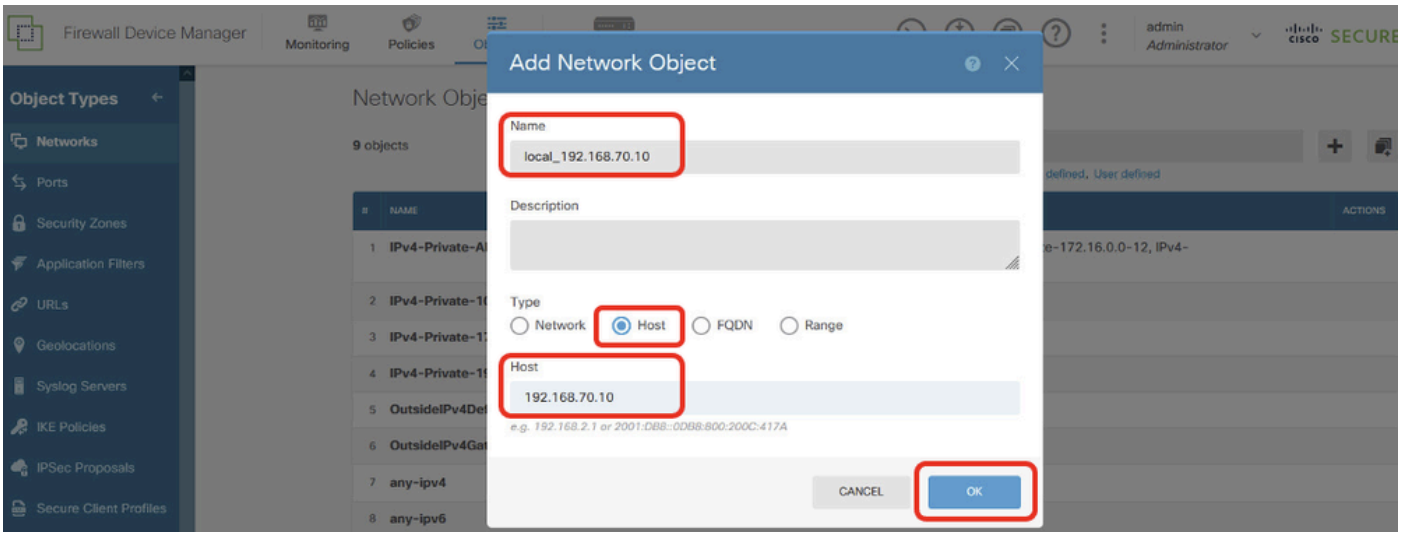
第11步：为Site1 FTD创建PBR访问列表要使用的新网络对象。导航到对象(Objects)>网络(Networks)，然后单击+按钮。



Site1FTD_Create_Network_Object

第 11.1 步： 创建Site1 Client2 IP地址的对象。提供必要信息。单击 OK 按钮。

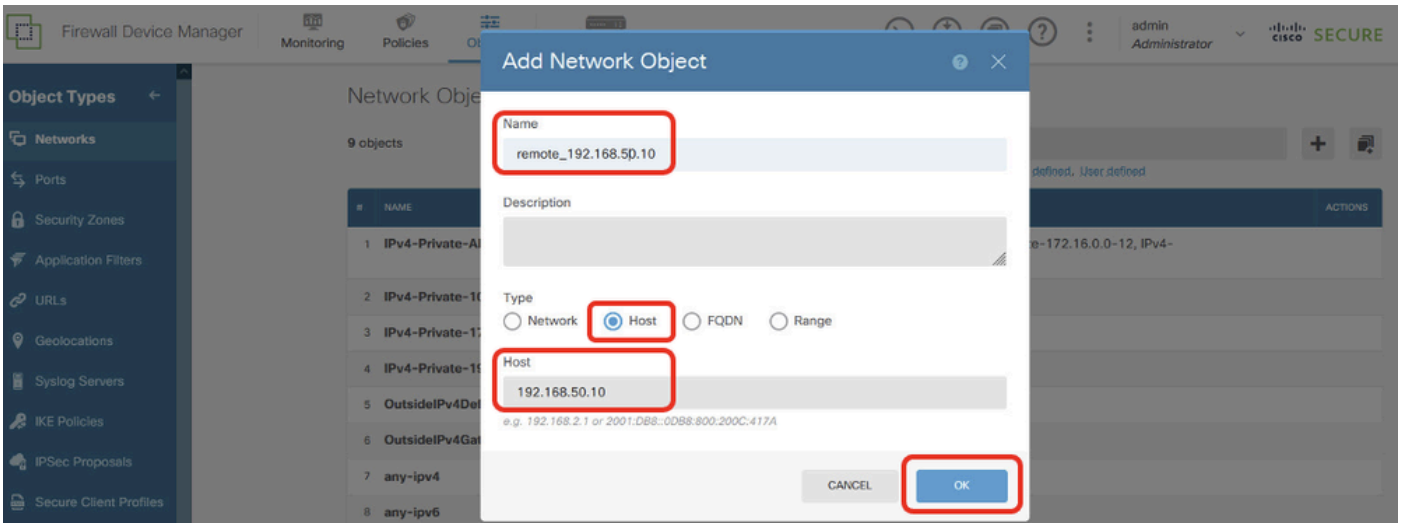
- 名称：local_192.168.70.10
- type：主机
- 主机：192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

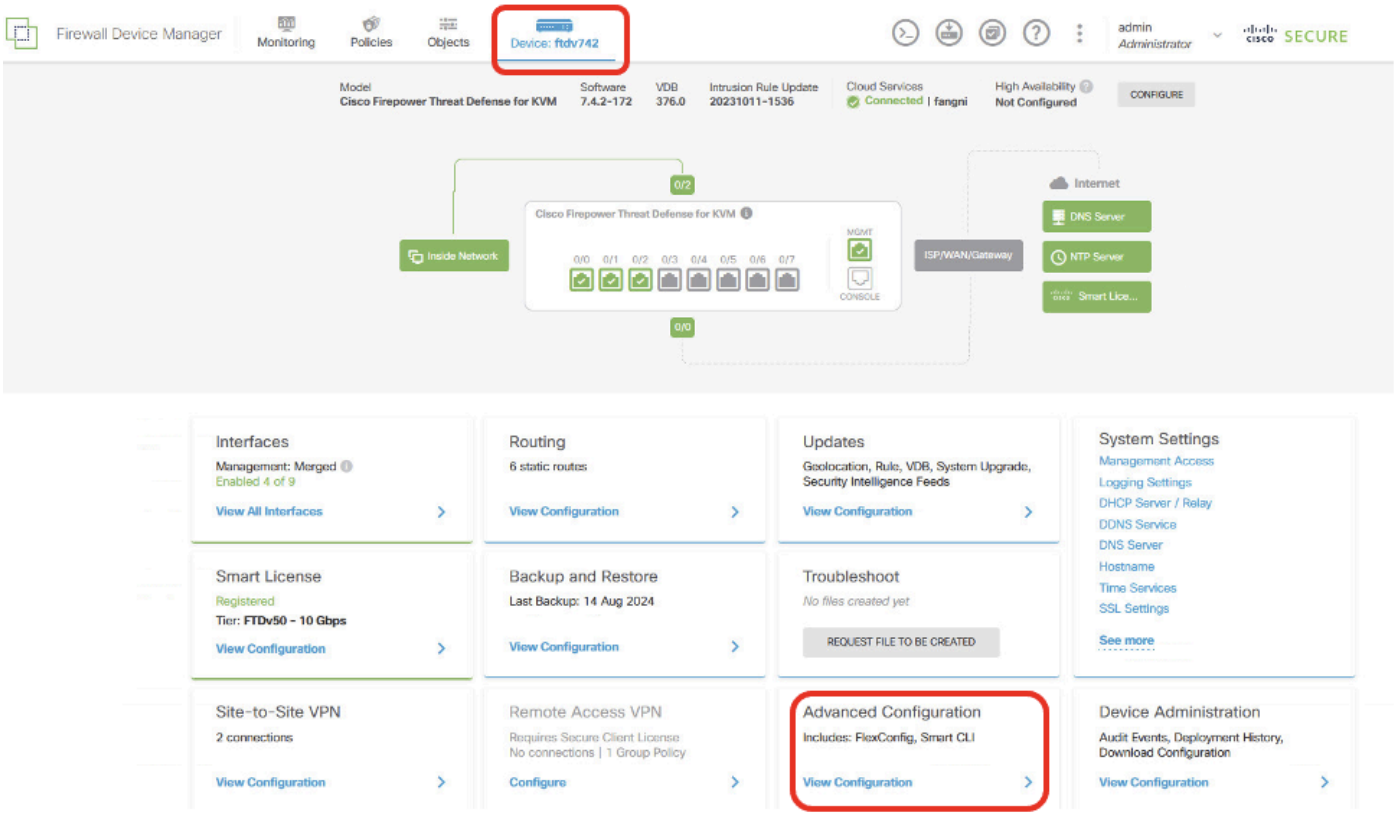
步骤11.2.创建Site2 Client2 IP地址的对象。提供必要信息。单击OK按钮。

- 名称：remote_192.168.50.10
- type：主机
- 主机：192.168.50.10



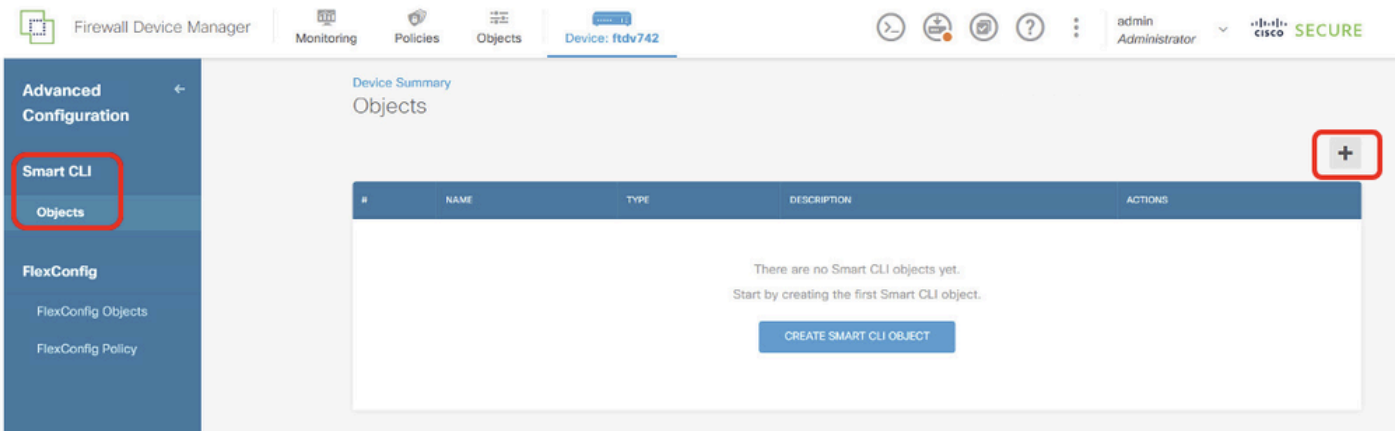
Site1FTD_PBR_RemoteObject

步骤12.为PBR创建扩展访问列表。导航到Device > Advanced Configuration。单击View Configuration。



Site1FTD_View_Advanced_Configuration

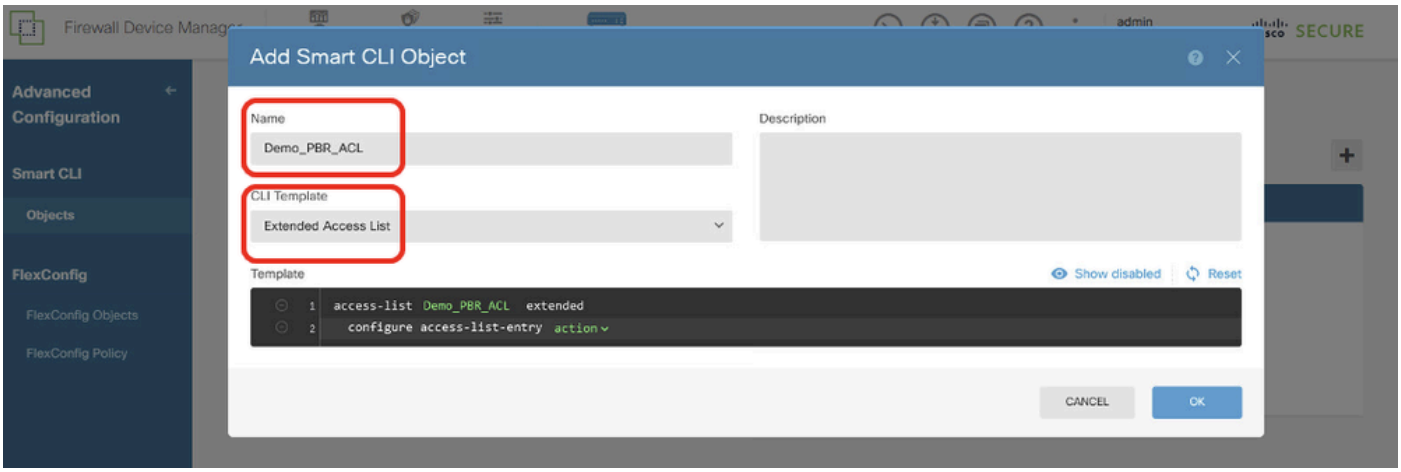
步骤12.1.导航到Smart CLI > Objects。单击+按钮。



Site1FTD_Add_SmartCLI_Object

第12.2步：输入对象的名称，然后选择CLI模板。

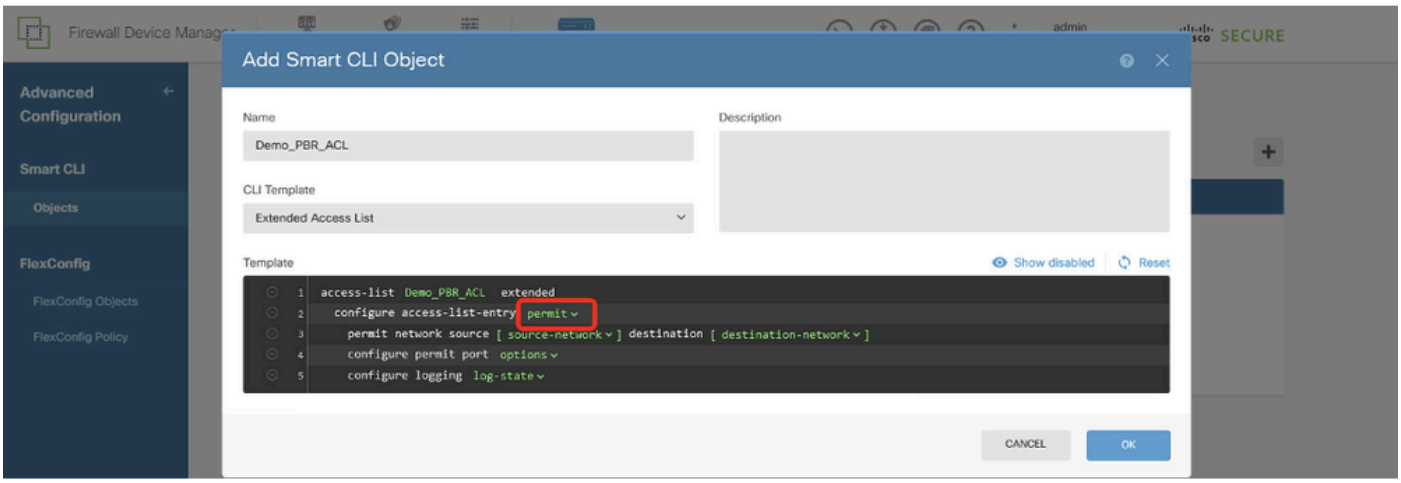
- 名称：Demo_PBR_ACL
- CLI模板：扩展访问列表



Site1FTD_Create_PBR_ACL_1

步骤12.3.导航到Template并配置。单击OK按钮进行保存。

第2行，单击action。选择 Permit。

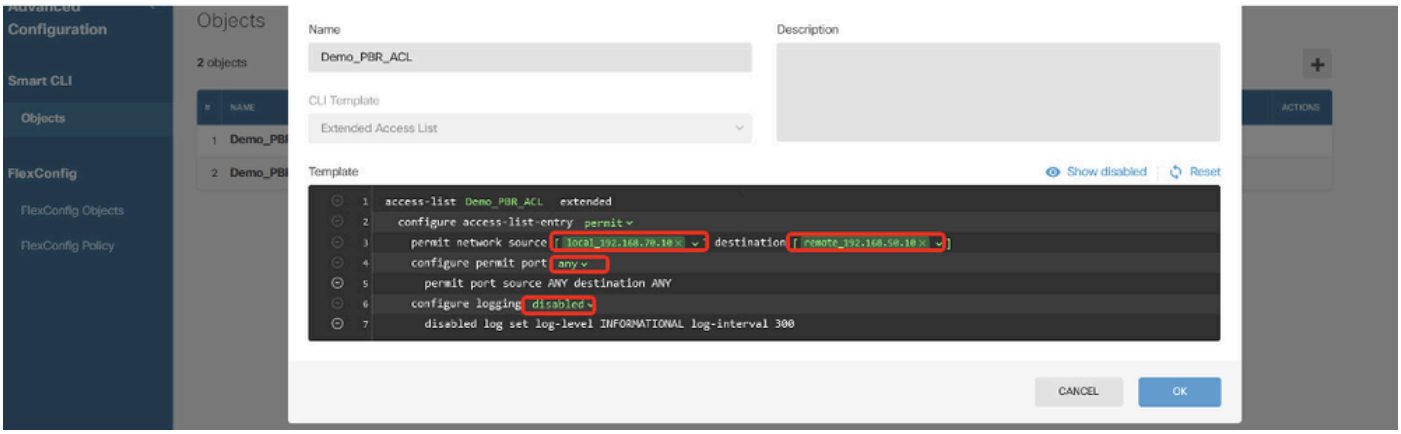


Site1FTD_Create_PBR_ACL_2

第3行，单击source-network。选择local_192.168.70.10。单击destination-network。选择remote_192.168.50.10。

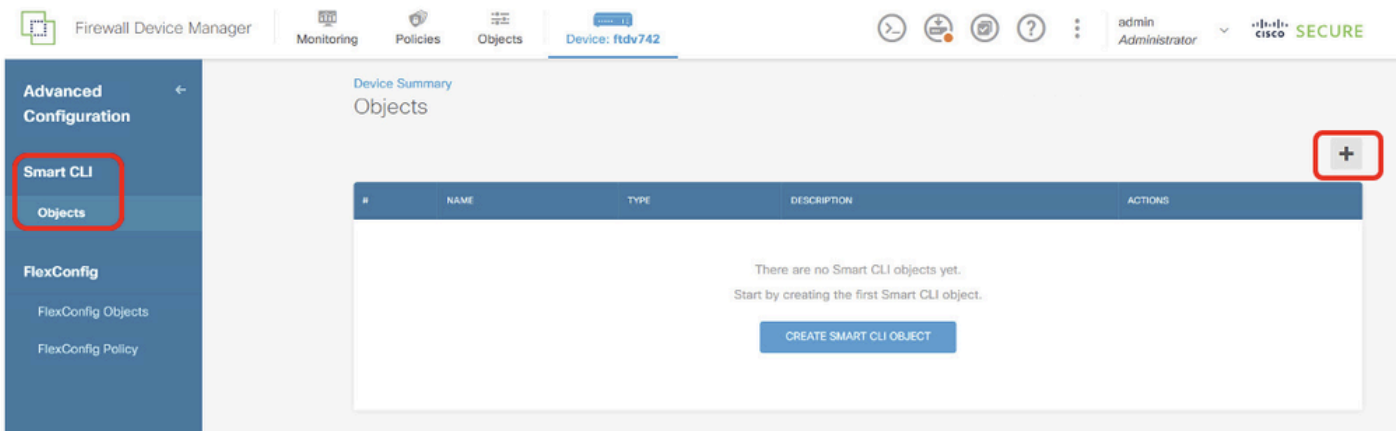
第4行，单击options并选择any。

第6行，单击log-state，然后选择disabled。



Site1FTD_Create_PBR_ACL_3

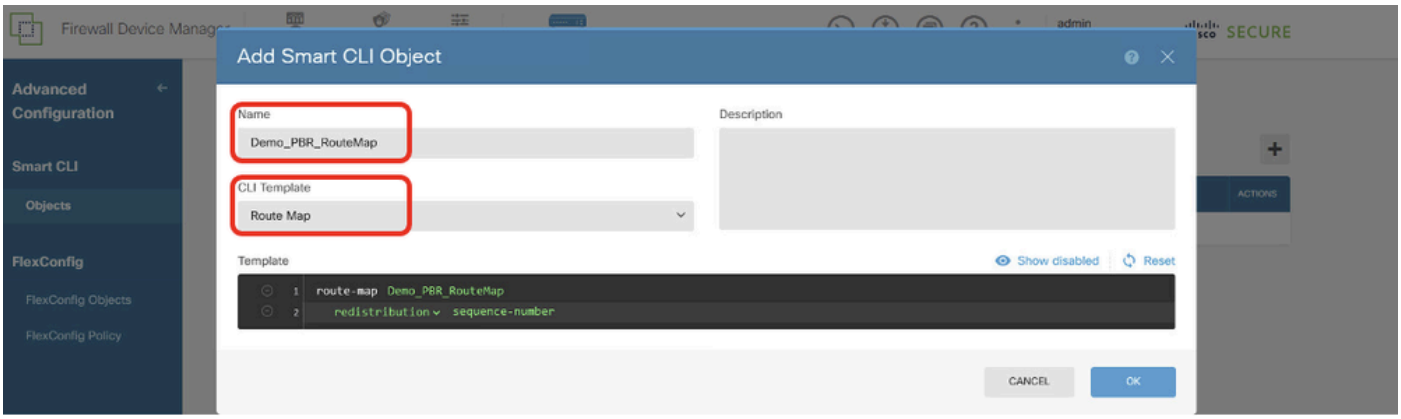
步骤13.为PBR创建路由映射。导航到设备>高级配置> Smart CLI >对象。单击+按钮。



Site1FTD_Add_SmartCLI_Object

第13.1步：输入对象的名称，然后选择CLI模板。

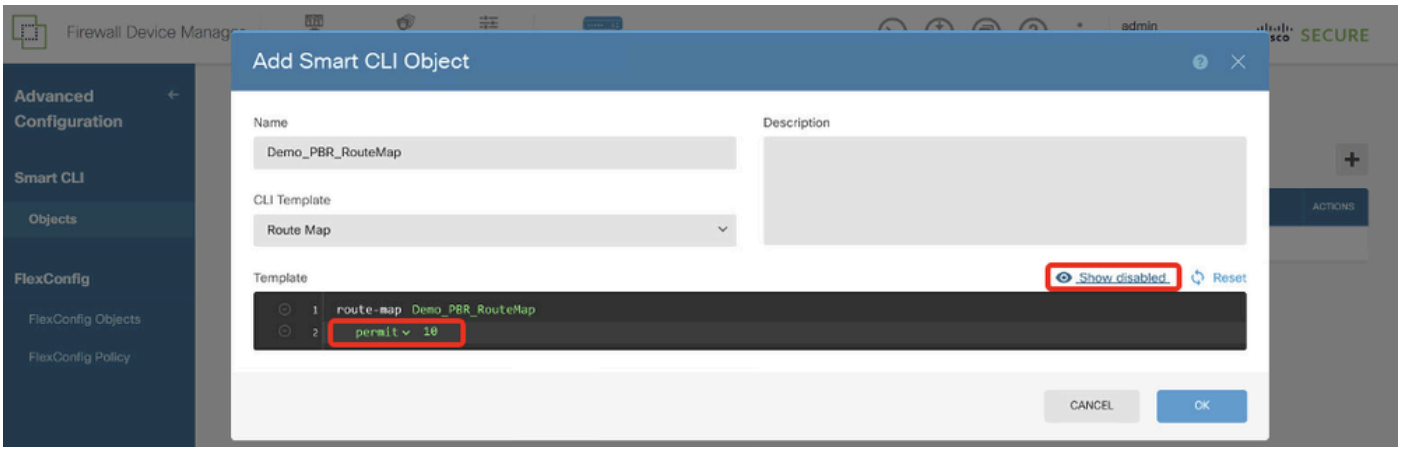
- 名称：Demo_PBR_RouteMap
- CLI模板：路由映射



Site1FTD_Create_PBR_RouteMap_1

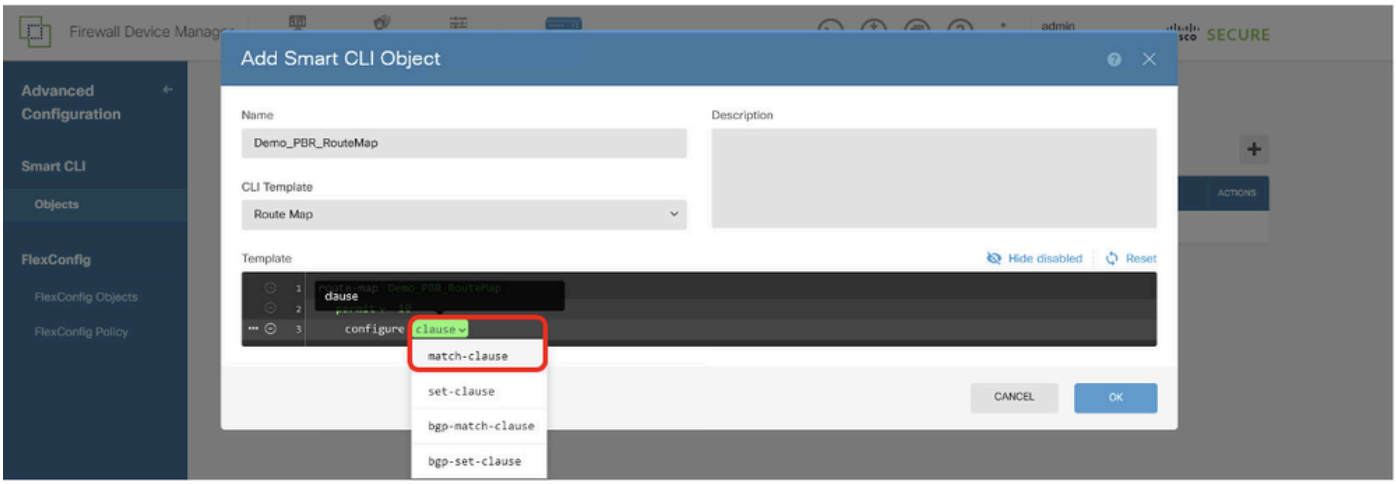
步骤13.2.导航到Template并配置。单击OK按钮保存。

第2行，单击redistribution。选择 Permit。单击sequence-number，手动输入10。单击Show disabled。



Site1FTD_Create_PBR_RouteMap_2

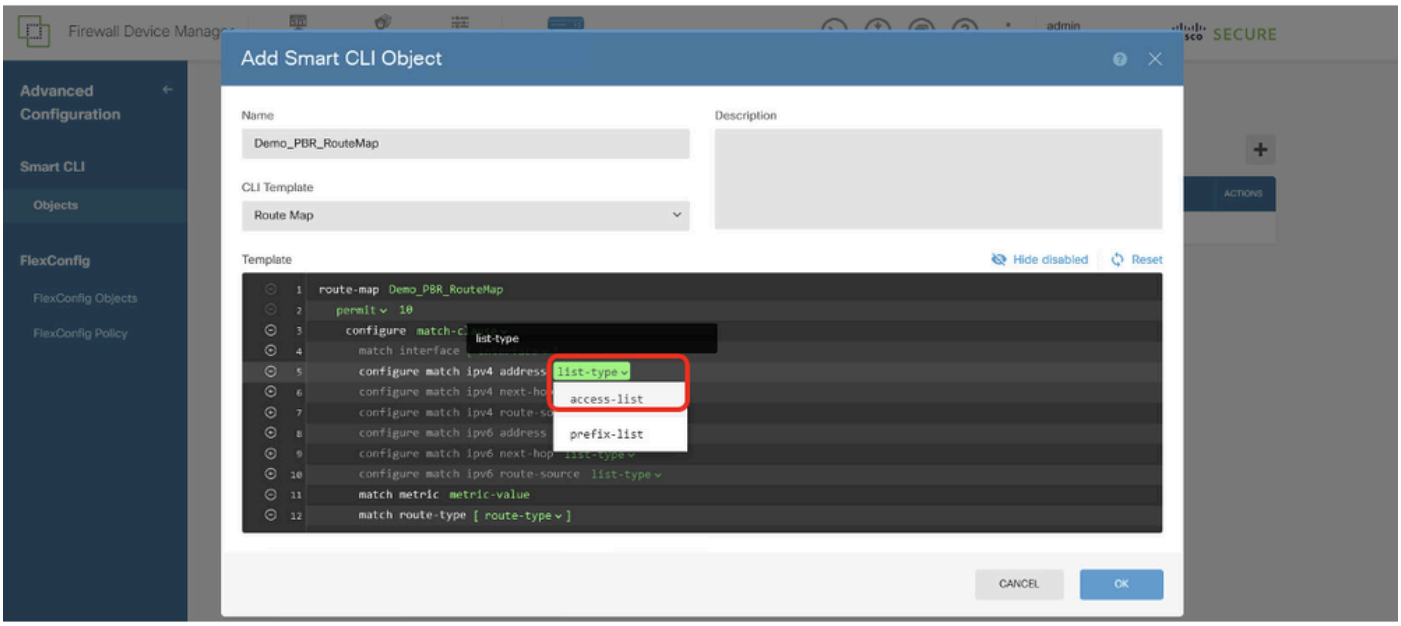
第3行，单击+以启用该行。单击clause。选择match-clause。



Site1FTD_Create_PBR_RouteMap_3

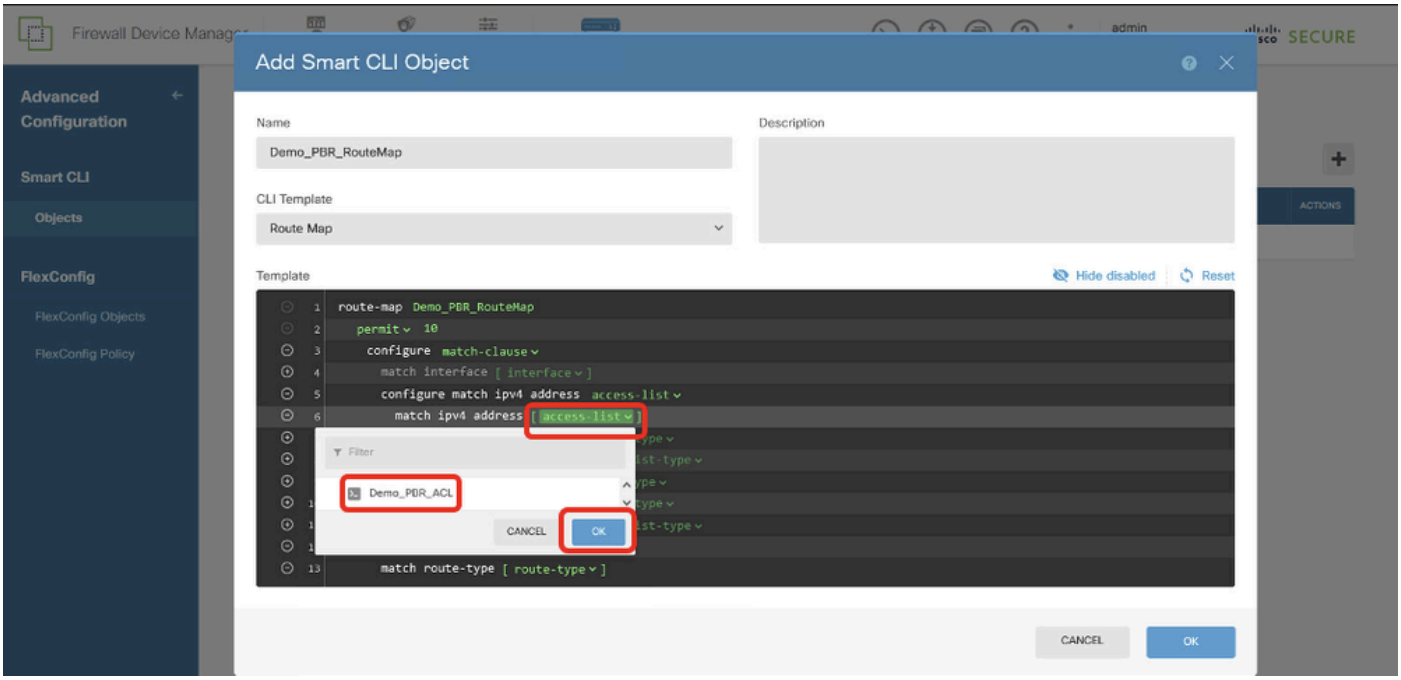
第4行，单击-禁用该行。

第5行，单击+以启用该行。单击list-type。选择access-list。



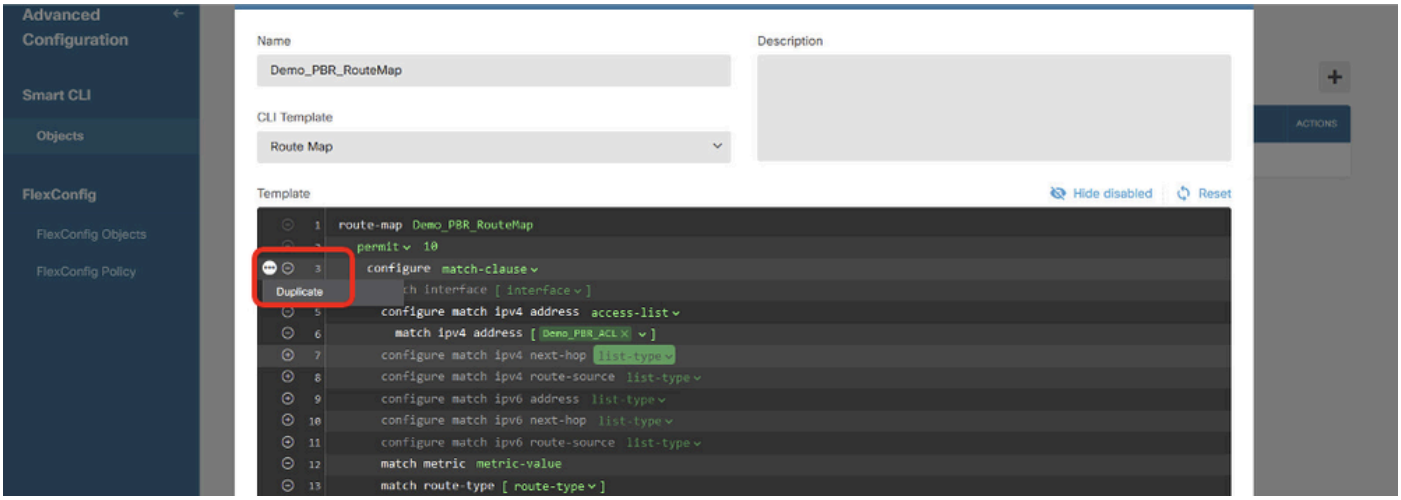
Site1FTD_Create_PBR_RouteMap_4

第6行，单击access-list。选择在步骤12中创建的ACL名称。在本例中，它是Demo_PBR_ACL。



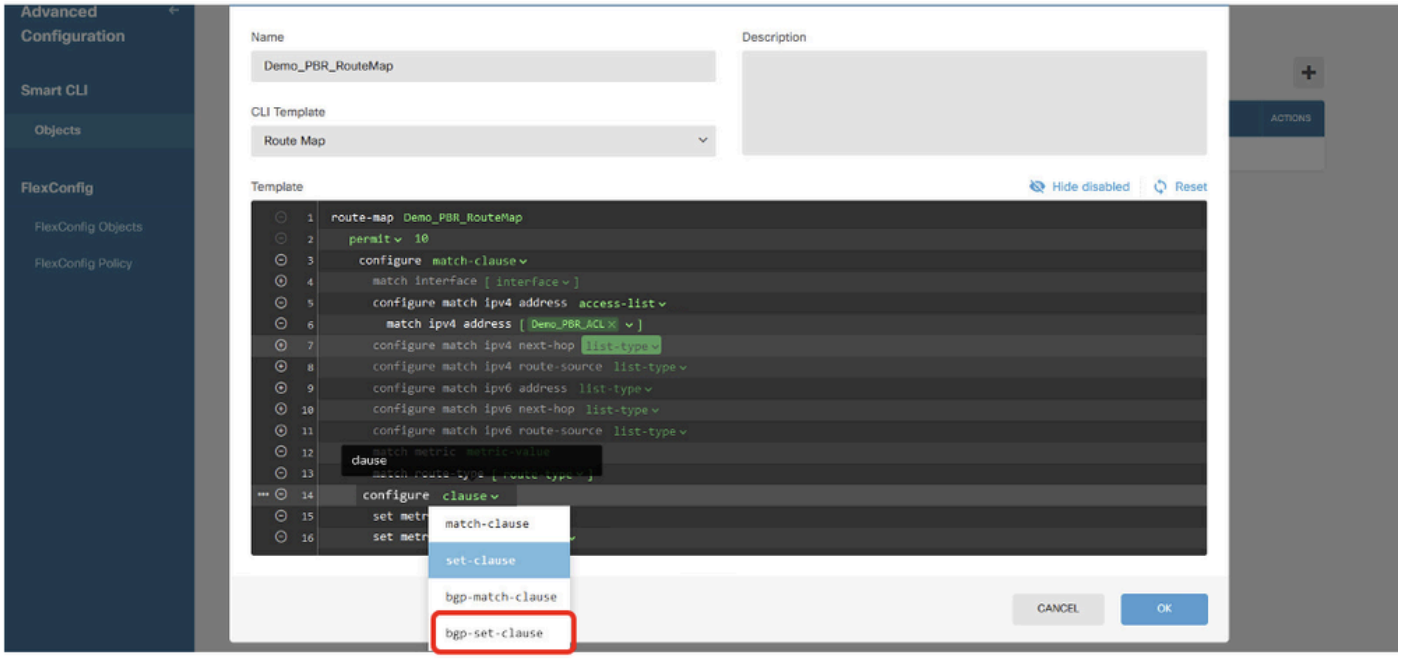
Site1FTD_Create_PBR_RouteMap_5

移回第3行。单击选项... 按钮并选择复制。



Site1FTD_Create_PBR_RouteMap_6

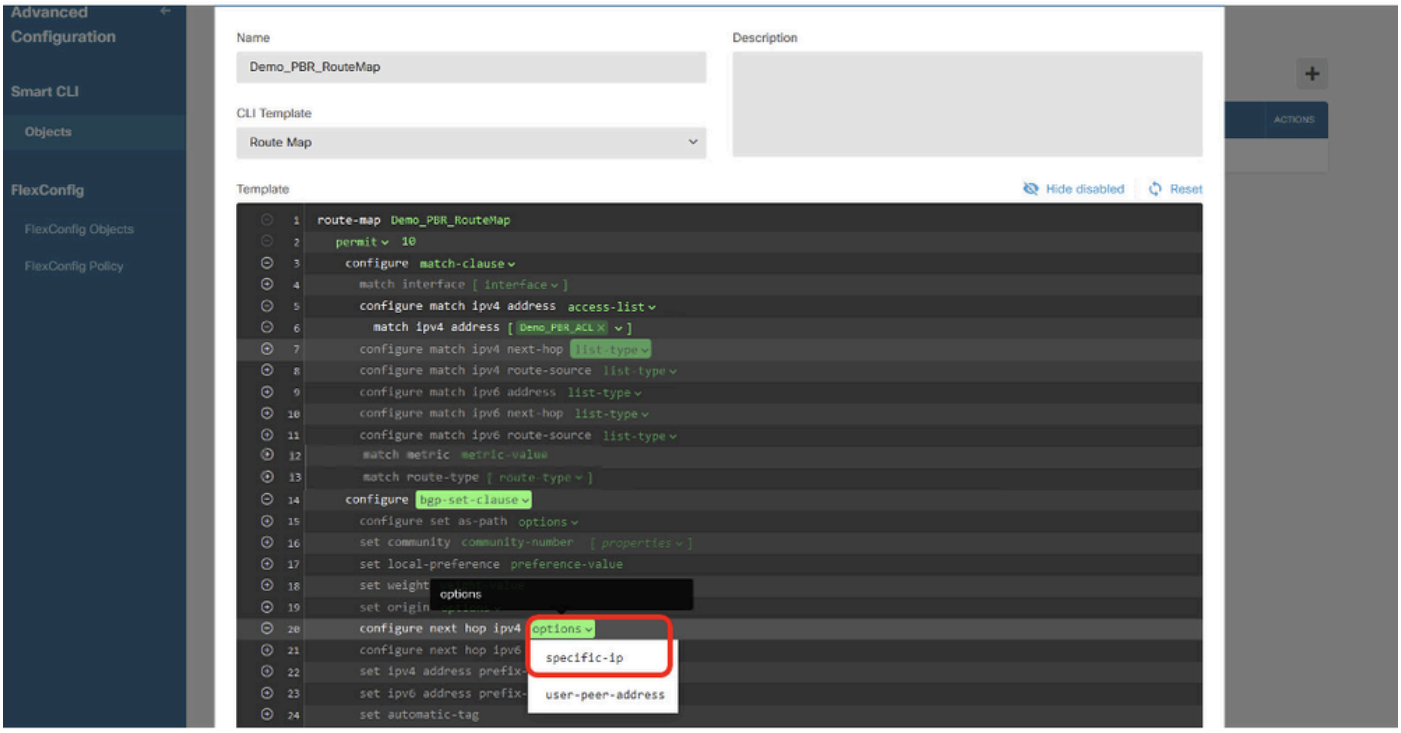
第14行，单击clause，然后选择bgp-set-clause。



Site1FTD_Create_PBR_RouteMap_7

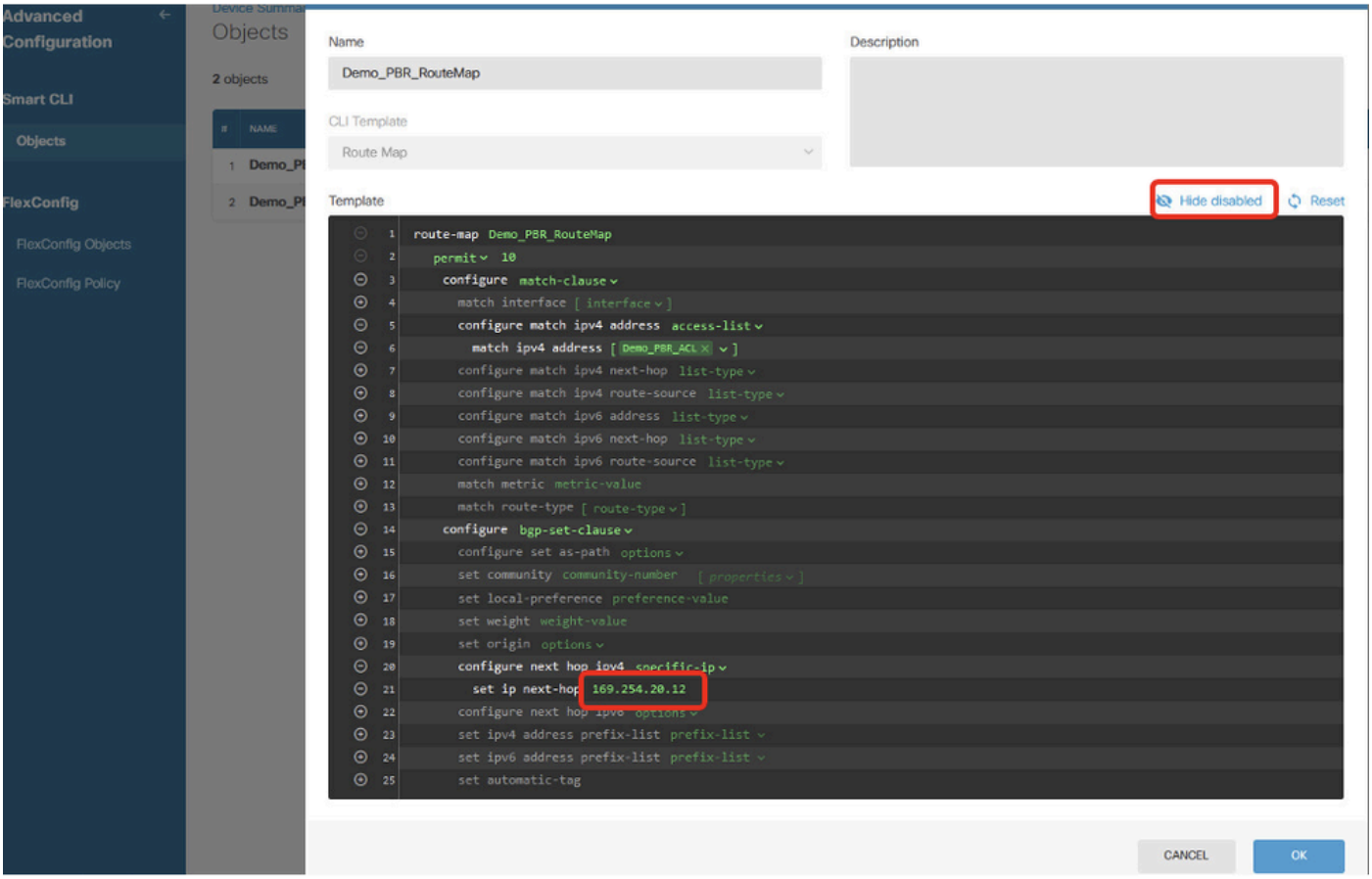
在行12、13、15、16、17、18、19、21、22、23、24中，单击按钮以禁用。

第20行，单击options并选择specific-ip。



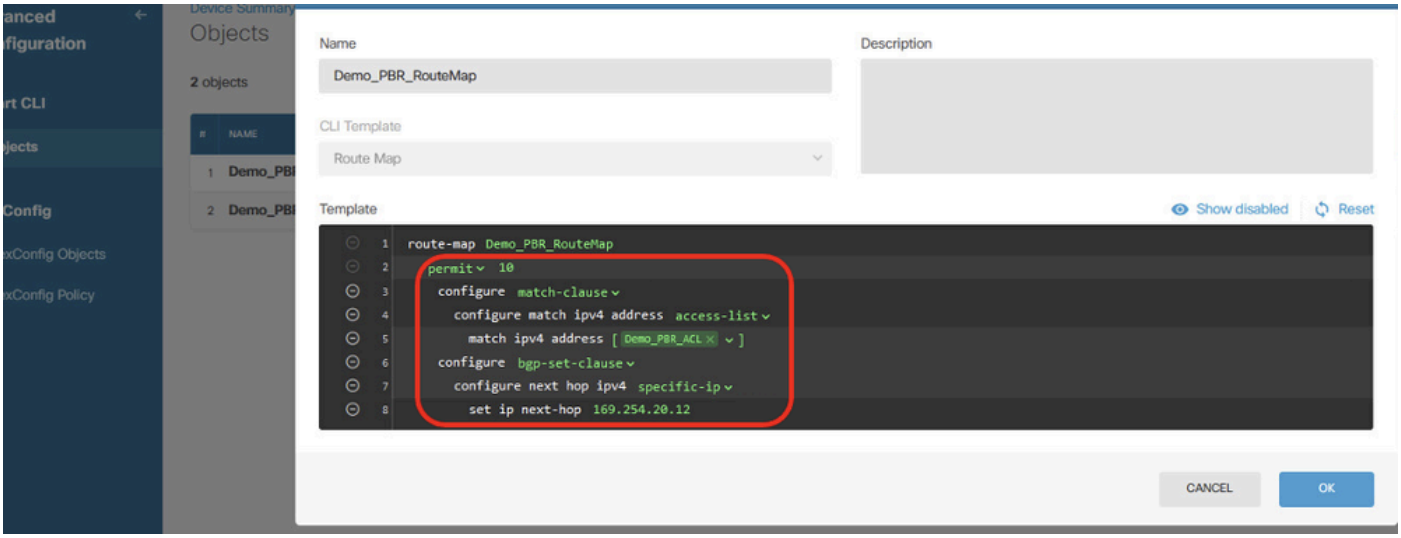
Site1FTD_Create_PBR_RouteMap_8

第21行，单击ip-address。手动输入下一跳IP地址。在本示例中，它是对等体Site2 FTD VTI tunnel2(169.254.20.12)的IP地址。 单击Hide disabled。



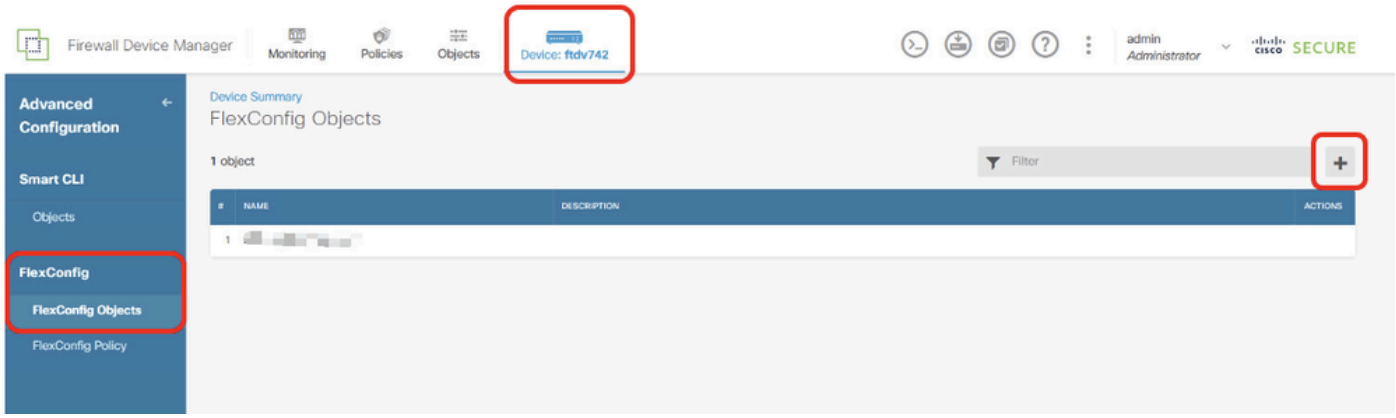
Site1FTD_Create_PBR_RouteMap_9

检查路由映射的配置。



Site1FTD_Create_PBR_RouteMap_10

步骤14.为PBR创建FlexConfig对象。导航到设备>高级配置> FlexConfig对象，然后单击+按钮。



Site1FTD_Create_PBR_FlexObj_1

步骤14.1.输入对象的名称。在本示例中，Demo_PBR_FlexObj。在模板和否定模板编辑器中，输入命令行。

- 模板：

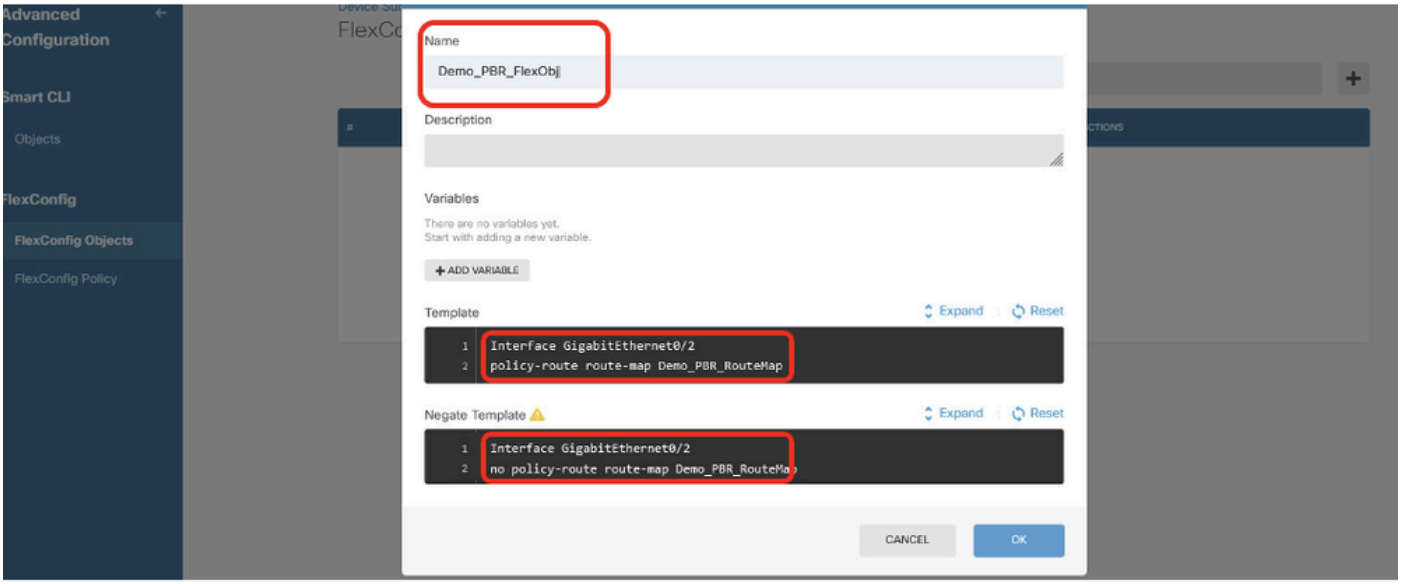
interface GigabitEthernet0/2

policy-route route-map Demo_PBR_RouteMap_Site2

- Negate模板：

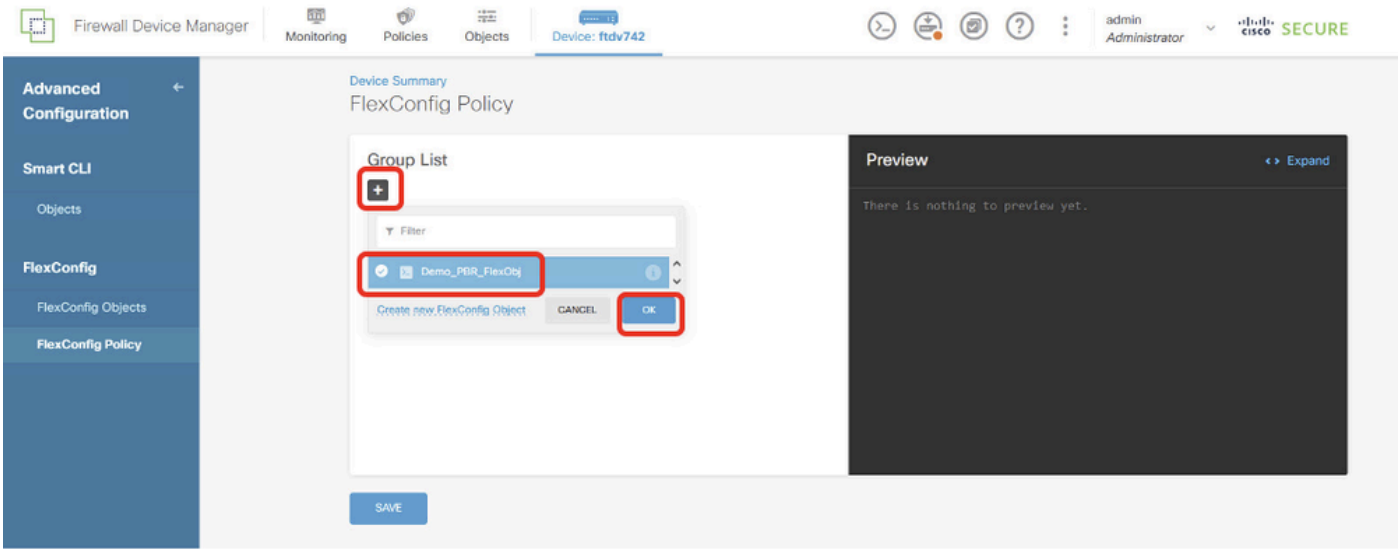
interface GigabitEthernet0/2

no policy-route route-map Demo_PBR_RouteMap_Site2



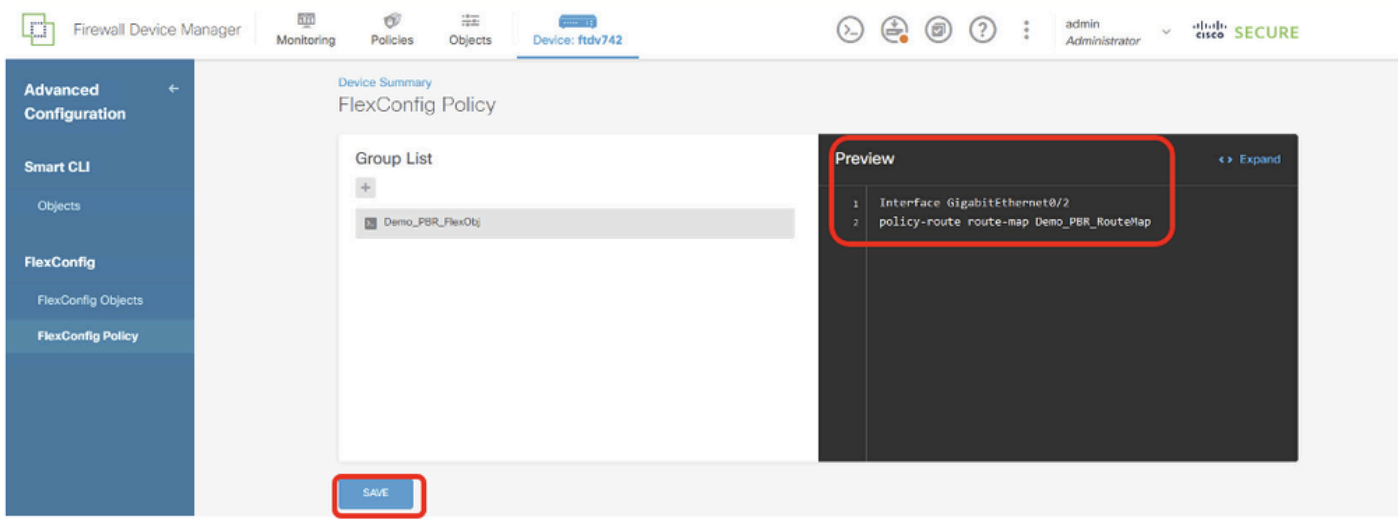
Site1FTD_Create_PBR_FlexObj_2

步骤15.为PBR创建FlexConfig策略。导航到设备>高级配置> FlexConfig策略。单击+按钮。选择在步骤14中创建的FlexConfig对象名称。单击OK按钮。



Site1FTD_Create_PBR_FlexPolicy_1

步骤15.1.在预览窗口中检验命令。如果情况良好，请单击Save。



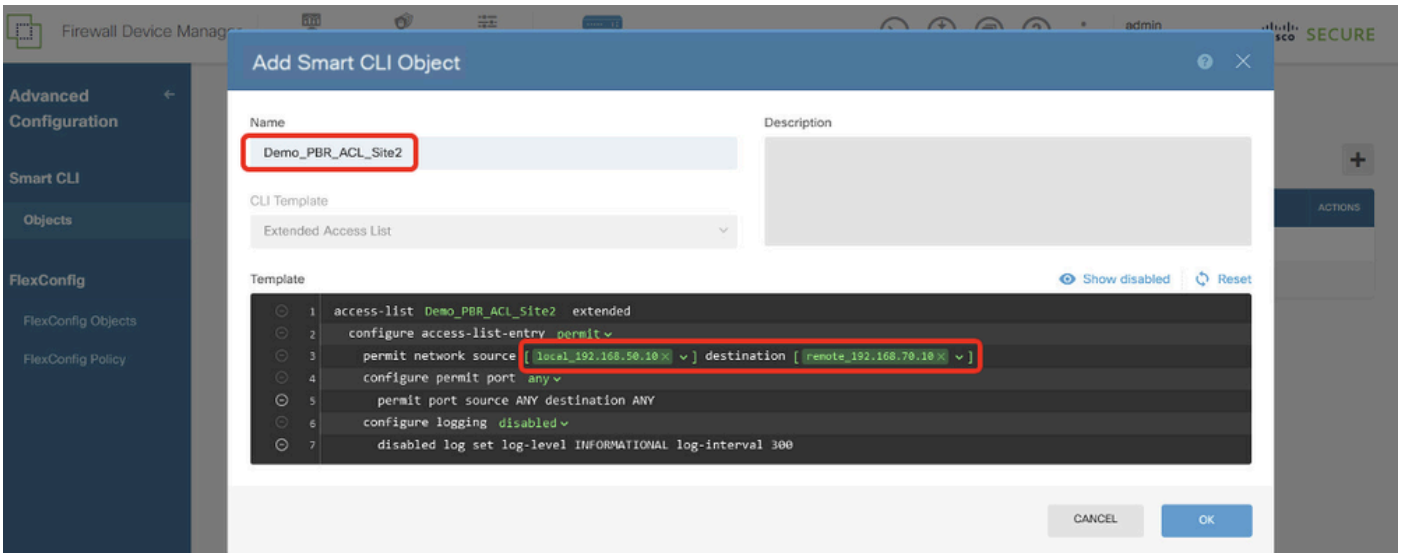
Site1FTD_Create_PBR_FlexPolicy_2

步骤16.部署配置更改。

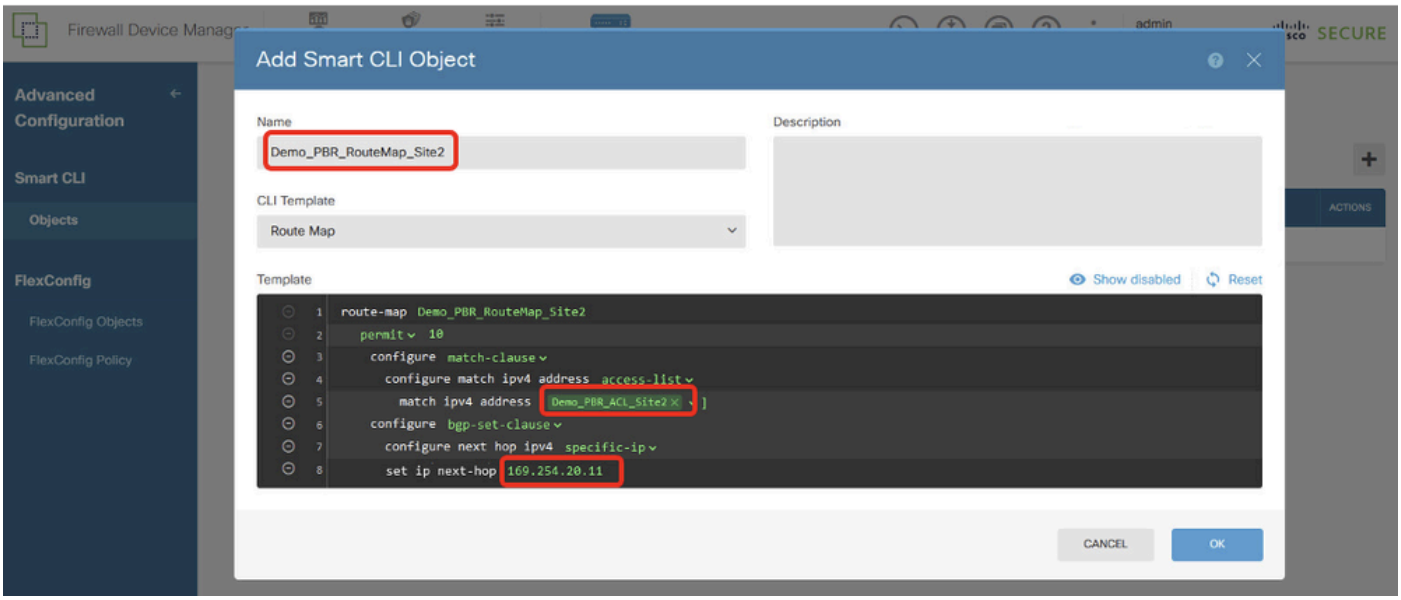
站点1FTD_部署_更改

站点2 FTD PBR配置

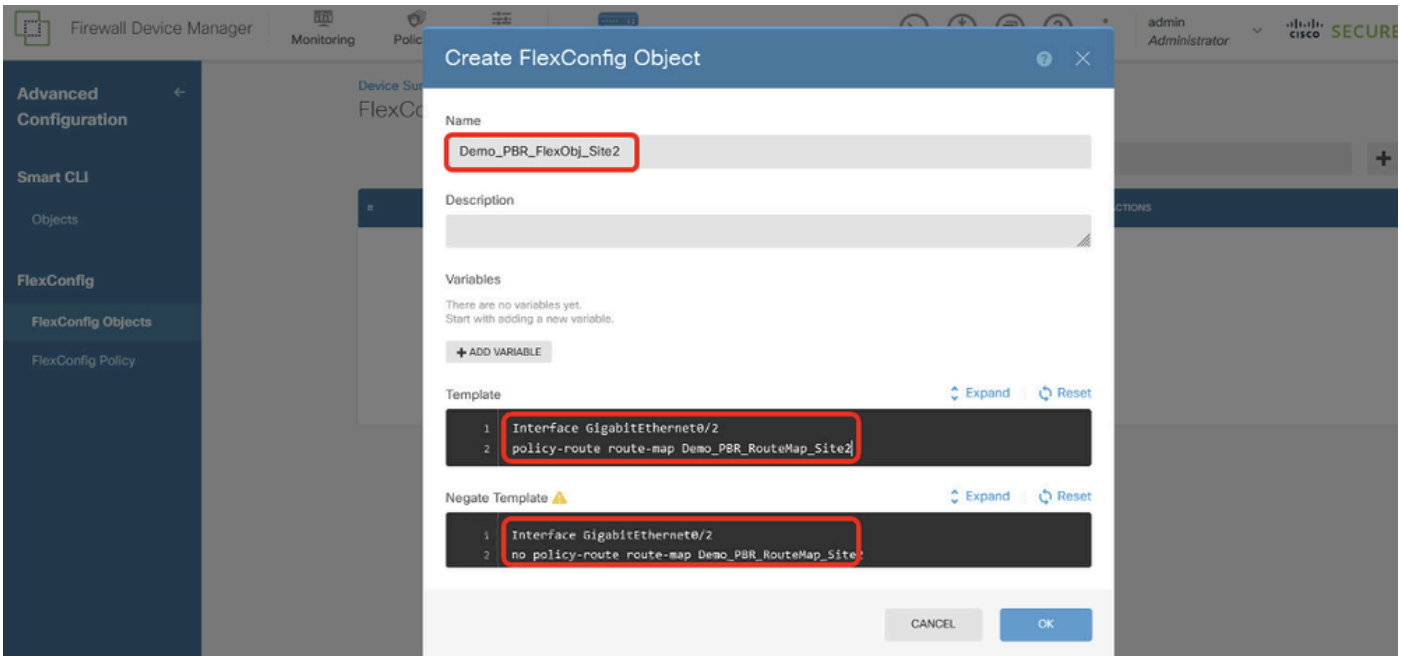
步骤17.重复步骤11到步骤16.以创建PBR并为Site2 FTD创建相应参数。



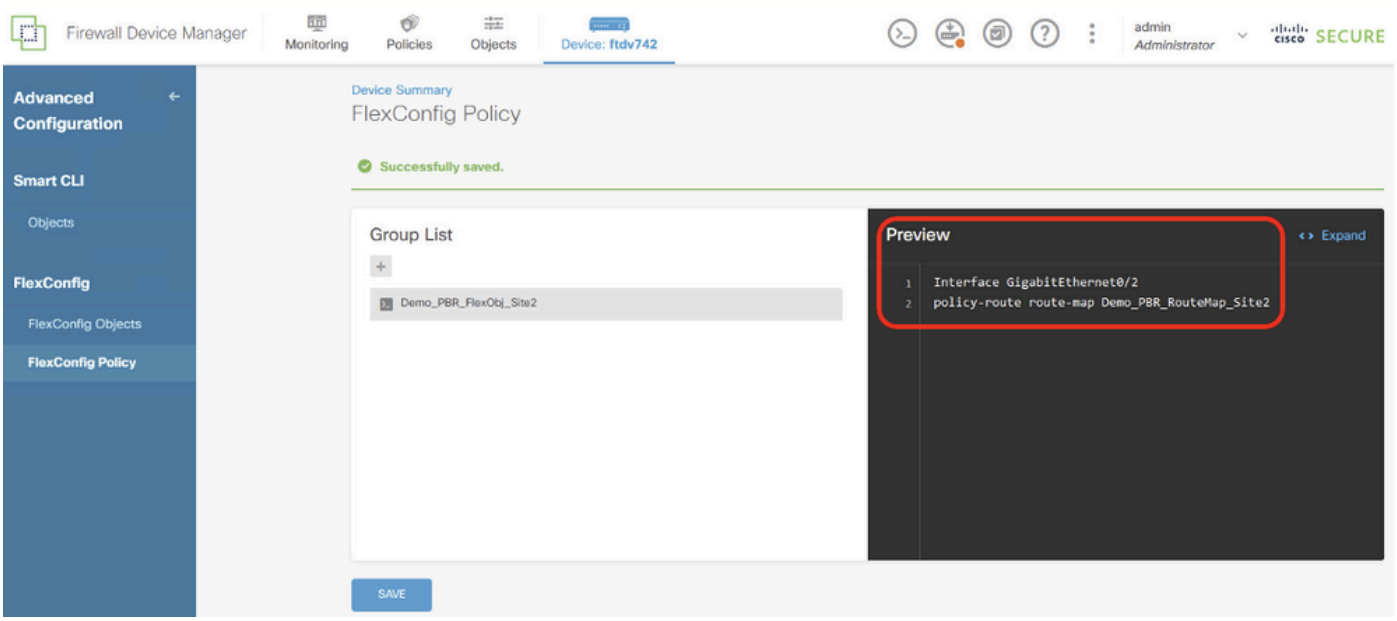
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

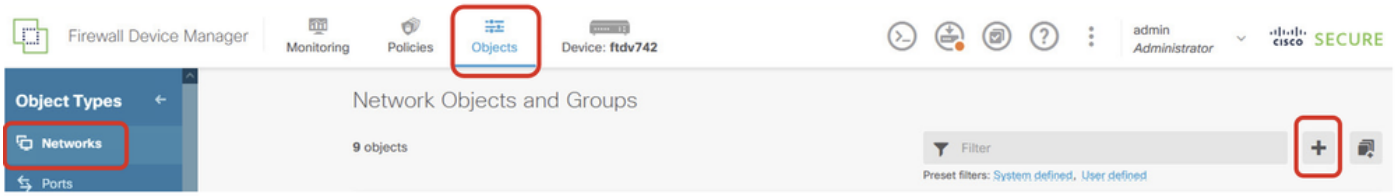


Site2FTD_Create_PBR_FlexPolicy

SLA监控器上的配置

站点1 FTD SLA监控器配置

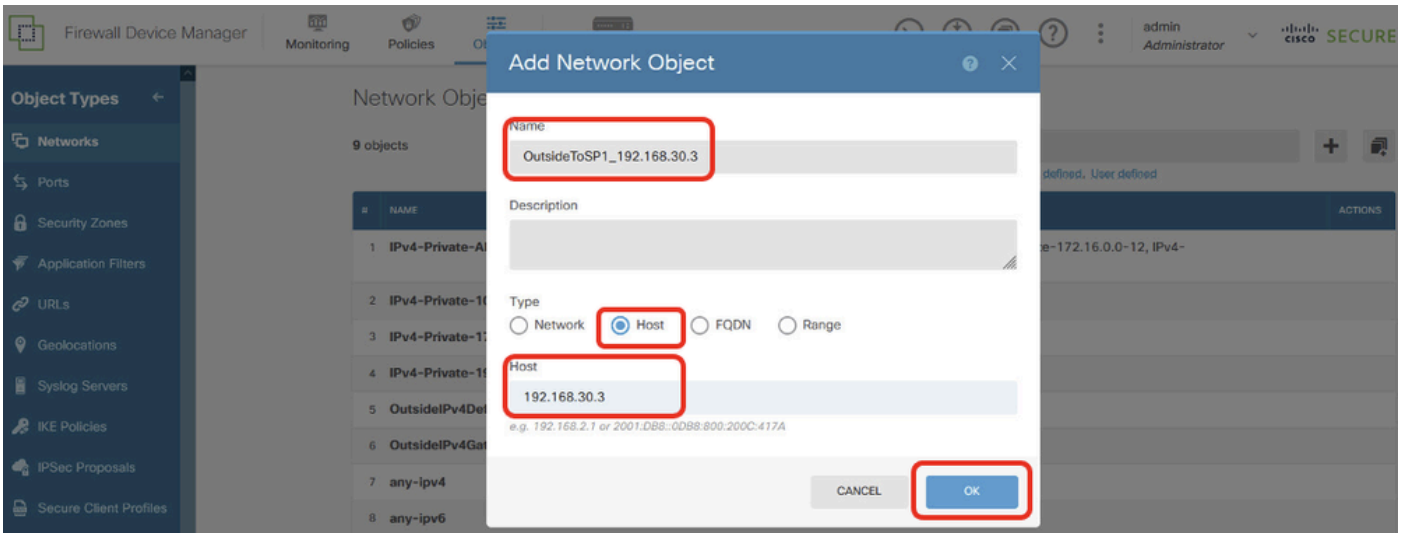
步骤18.创建要由Site1 FTD的SLA监控器使用的新网络对象。导航到Objects > Networks，然后单击+按钮。



Site1FTD_Create_Network_Object

步骤18.1.创建ISP1网关IP地址的对象。提供必要信息。单击OK按钮。

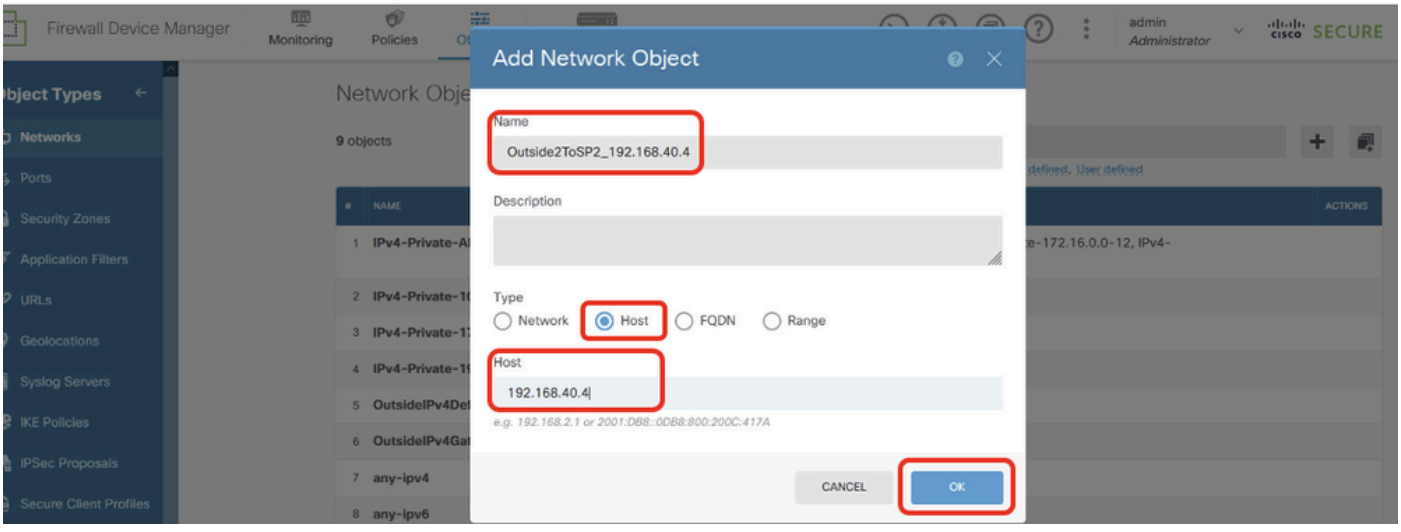
- 名称：OutsideToSP1_192.168.30.3
- type：主机
- 主机：192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

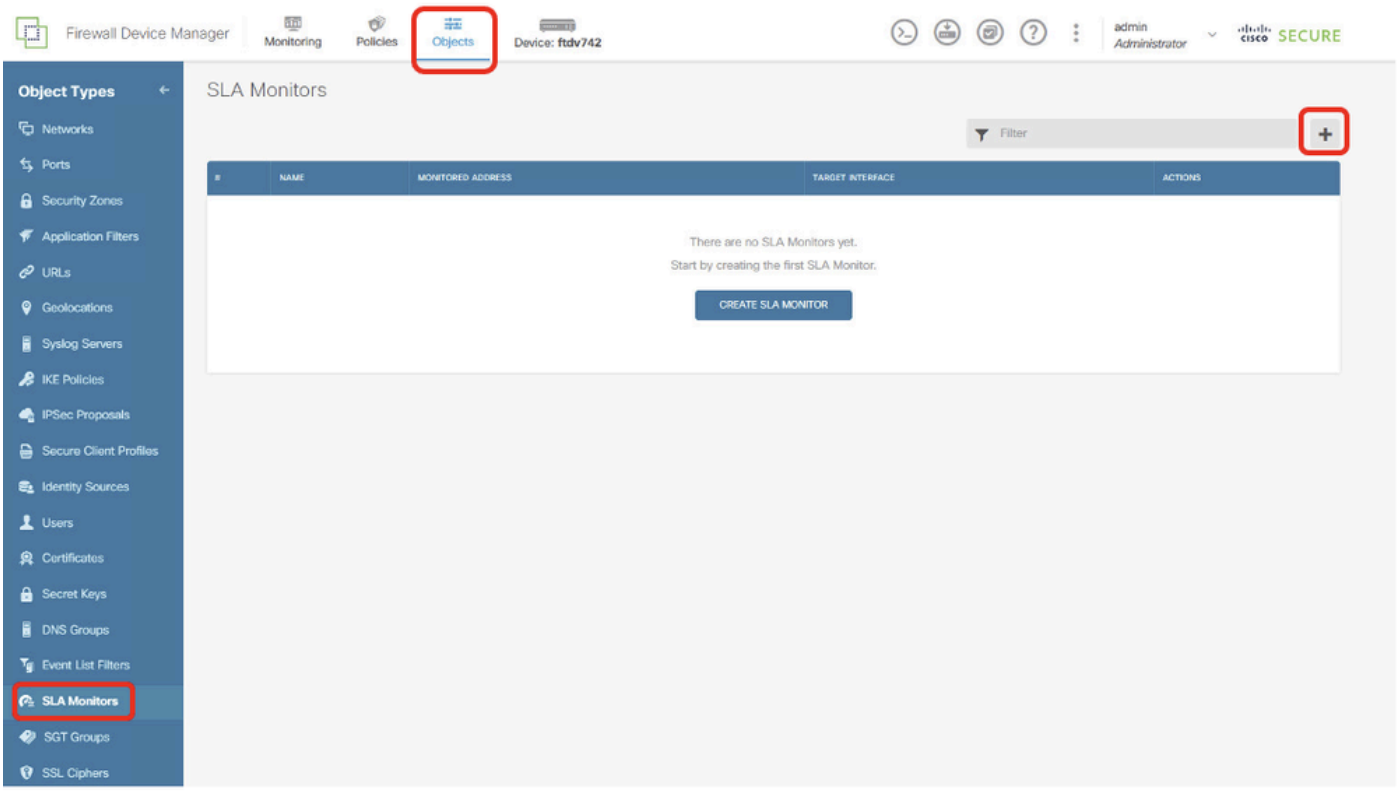
步骤18.2.创建ISP2网关IP地址的对象。提供必要信息。单击OK按钮。

- 名称：Outside2ToSP2_192.168.40.4
- type：主机
- 主机：192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

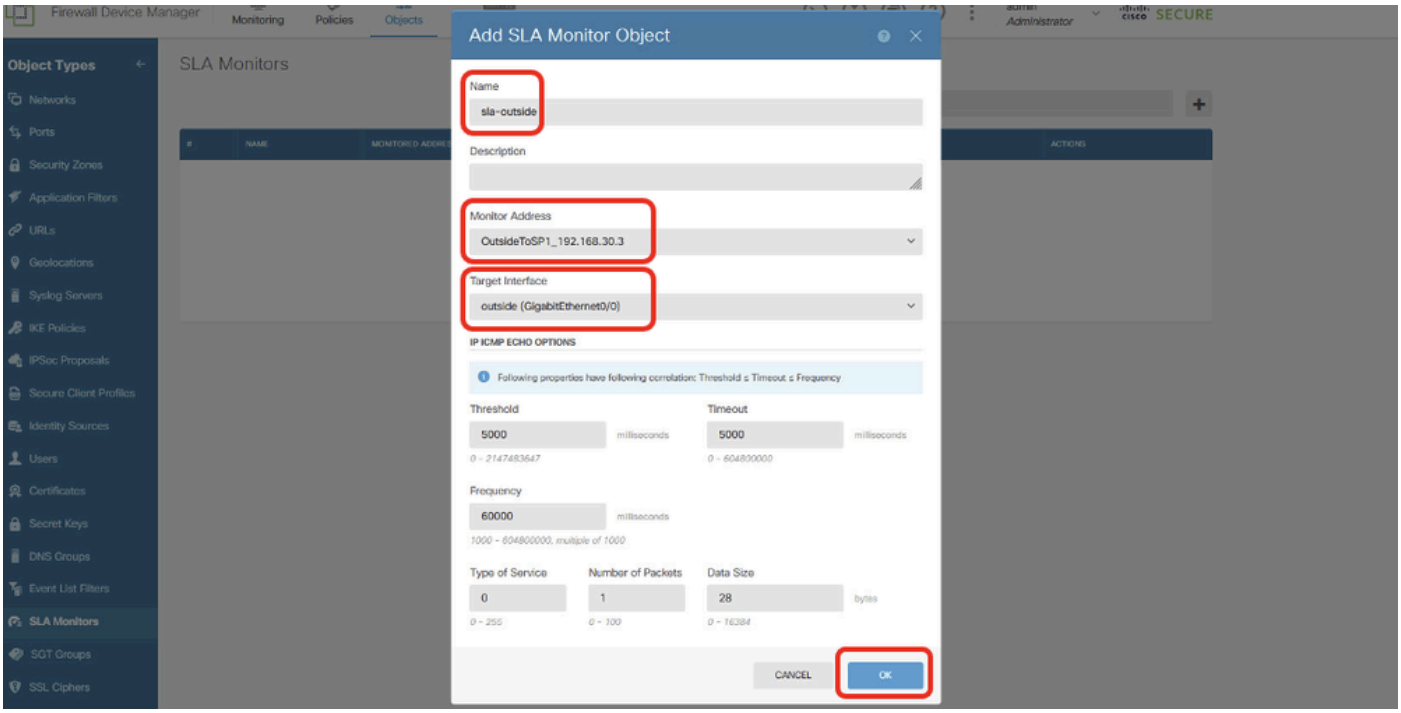
步骤19.创建SLA监控器。导航到对象>对象类型> SLA监控器。单击+按钮以创建新的SLA监控器。



Site1FTD_Create_SLAMonitor

第19.1步：在添加SLA监控器对象窗口中，为ISP1网关提供必要的信息。单击OK按钮保存。

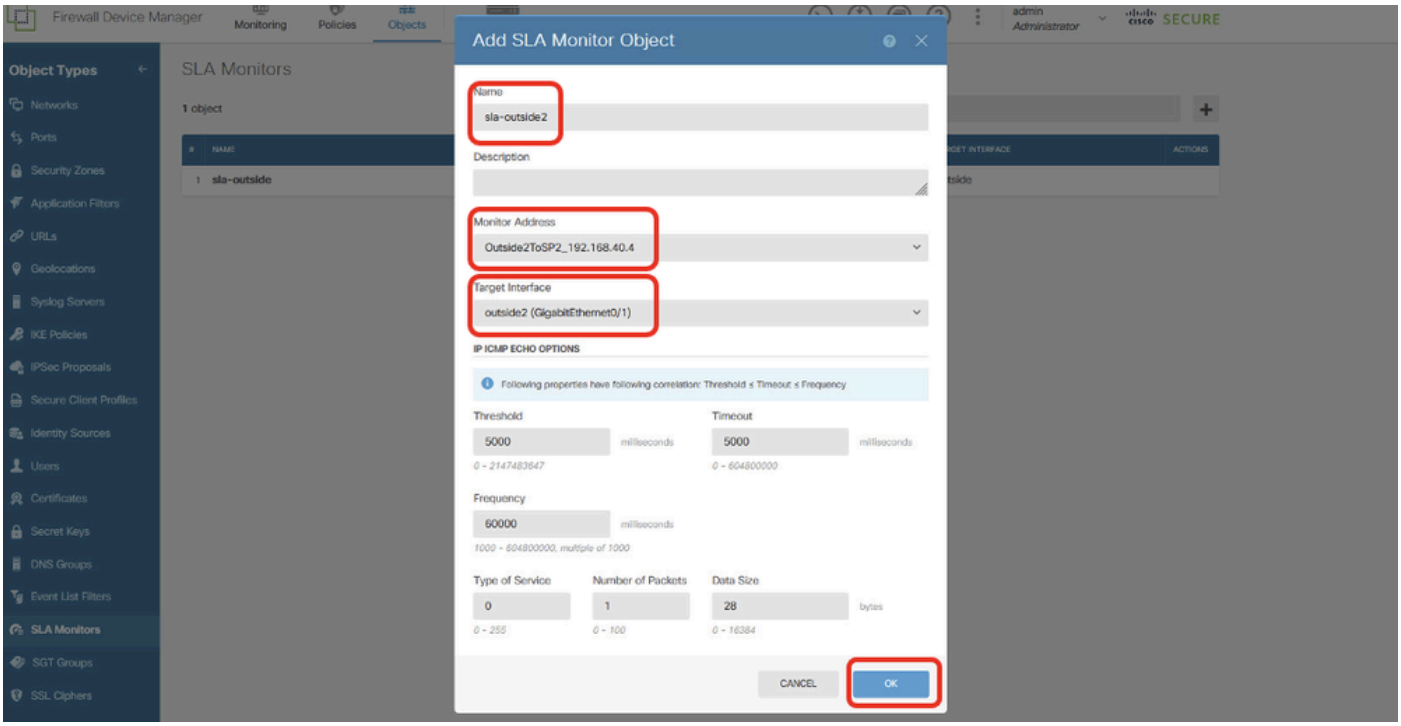
- 名称：sla-outside
- 监控器地址：OutsideToSP1_192.168.30.3
- 目标接口：outside(GigabitEthernet0/0)
- IP ICMP回应选项：默认



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

步骤19.2.继续单击+按钮为ISP2网关创建新的SLA监控器。在添加SLA监控器对象窗口中，为ISP2网关提供必要的信息。单击OK按钮保存。

- 名称：sla-outside2
- 监控器地址：Outside2ToSP2_192.168.40.4
- 目标接口：outside2(GigabitEthernet0/1)
- IP ICMP回应选项：默认



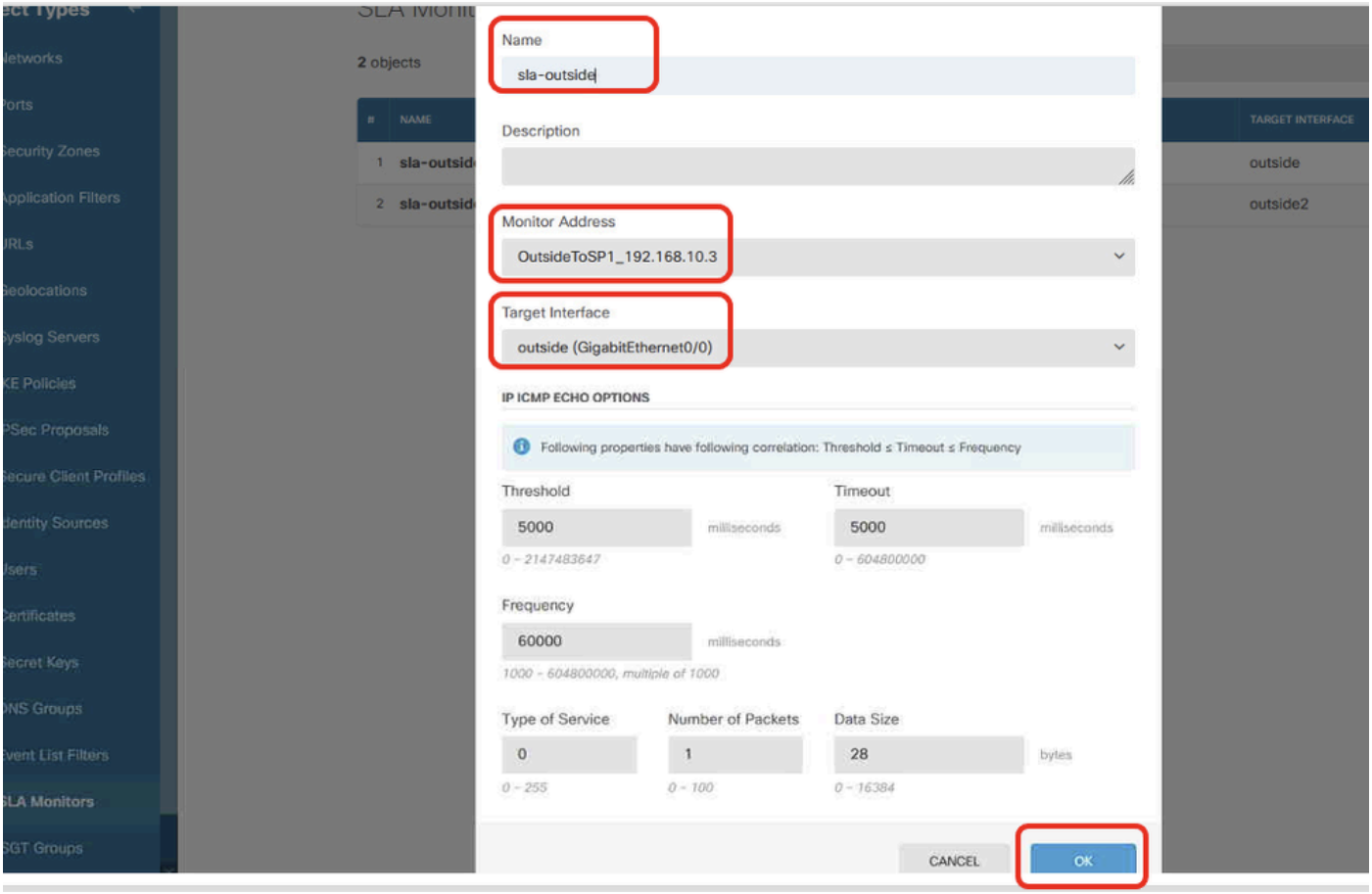
Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

步骤20.部署配置更改。

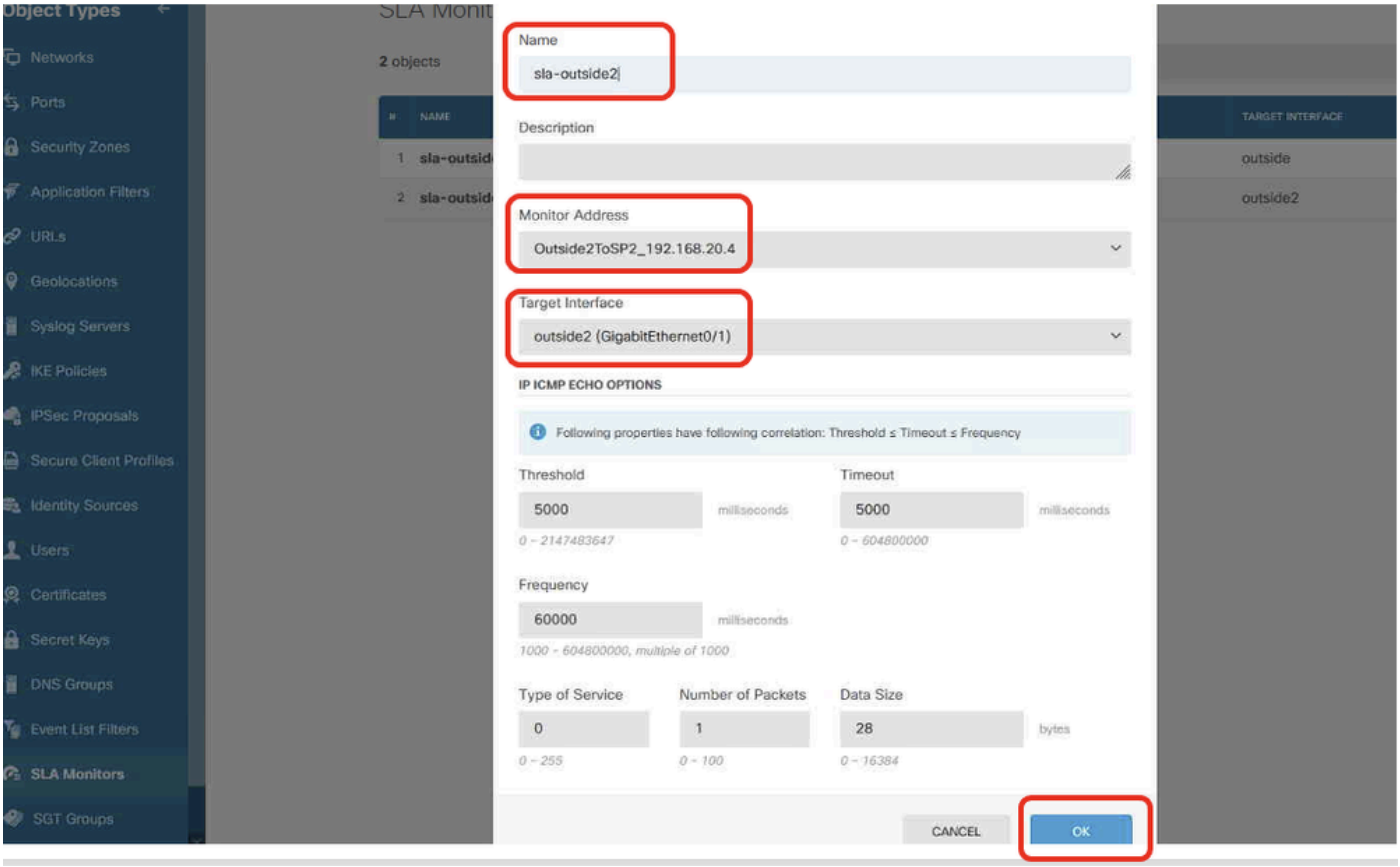
站点1FTD_部署_更改

站点2 FTD SLA监控器配置

步骤21.重复步骤18.到步骤20.使用站点2 FTD上的相应参数创建SLA监控器。



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

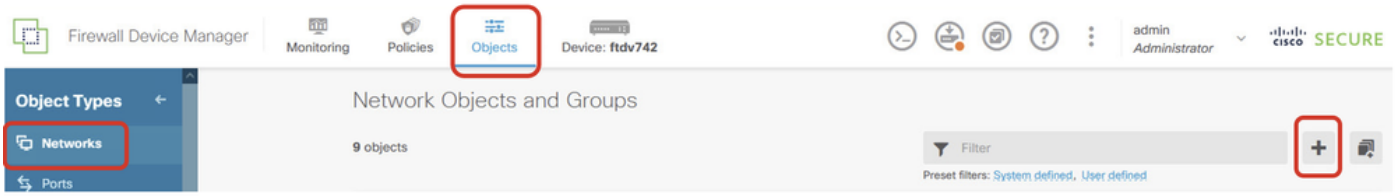


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

静态路由配置

站点1 FTD静态路由配置

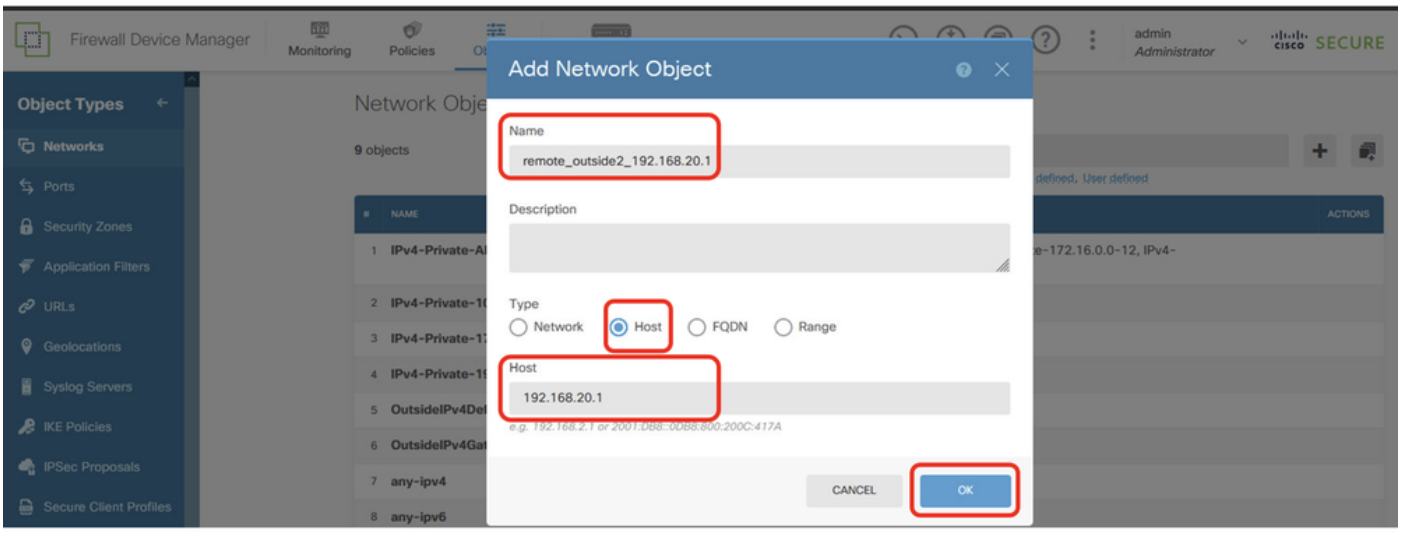
步骤22.创建要由Site1 FTD的静态路由使用的新网络对象。导航到对象>网络，单击+按钮。



Site1FTD_Create_Obj

步骤22.1.为对等体Site2 FTD的outside2 IP地址创建对象。提供必要信息。单击OK按钮。

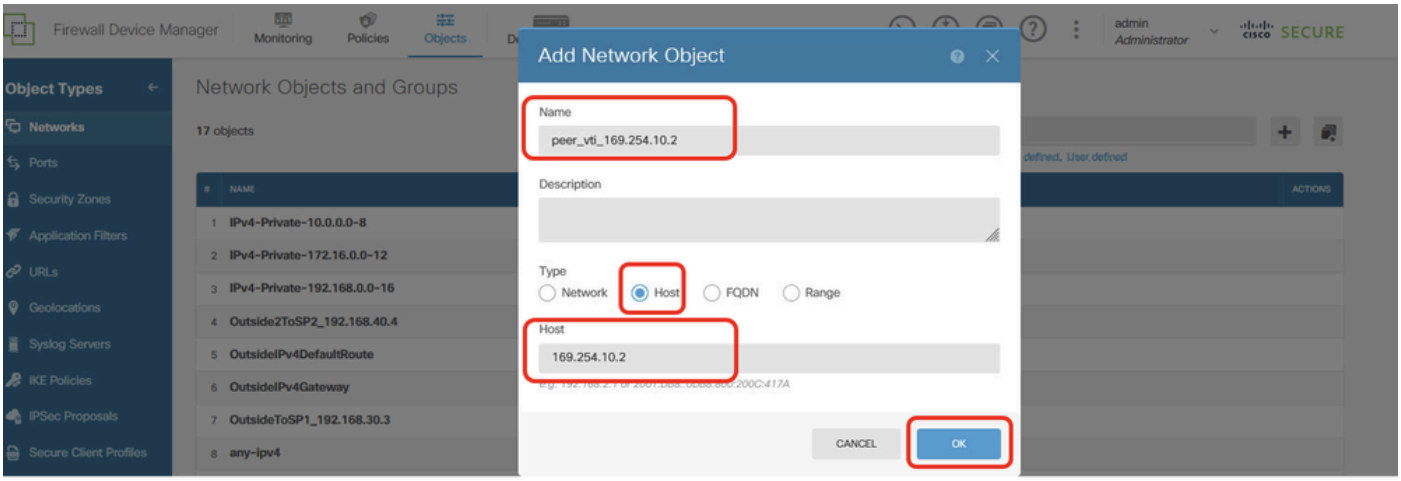
- 名称：remote_outside2_192.168.20.1
- type：主机
- 网络:192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

步骤22.2.为对等体Site2 FTD的VTI Tunnel1 IP地址创建对象。提供必要信息。单击OK按钮。

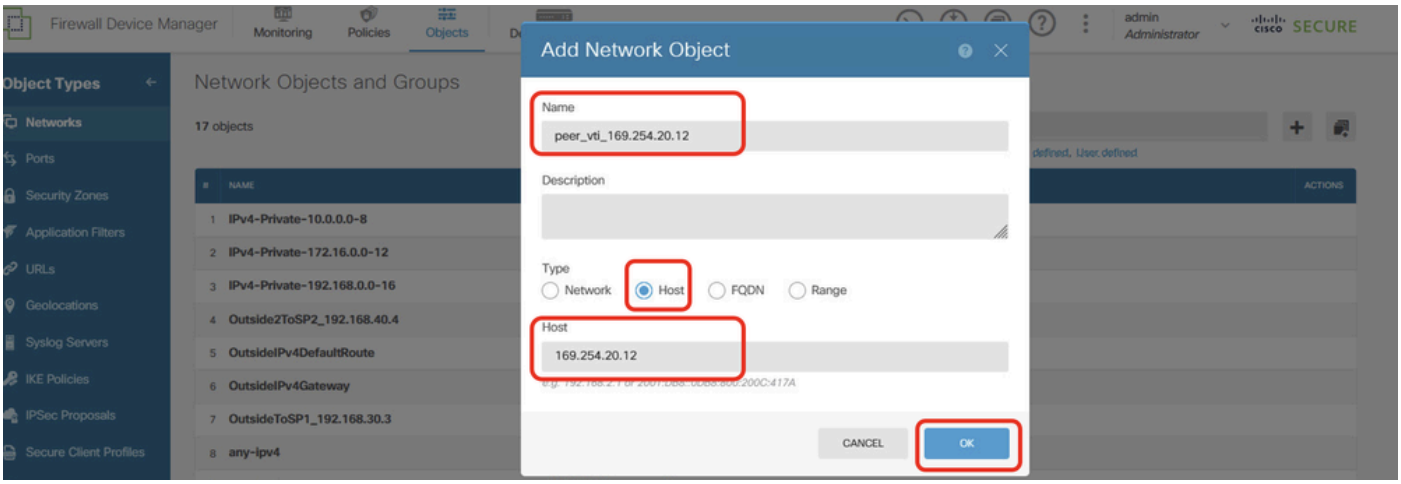
- 名称：peer_vti_169.254.10.2
- type：主机
- 网络：169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

步骤22.3.为对等体Site2 FTD的VTI Tunnel2 IP地址创建对象。提供必要信息。单击OK按钮。

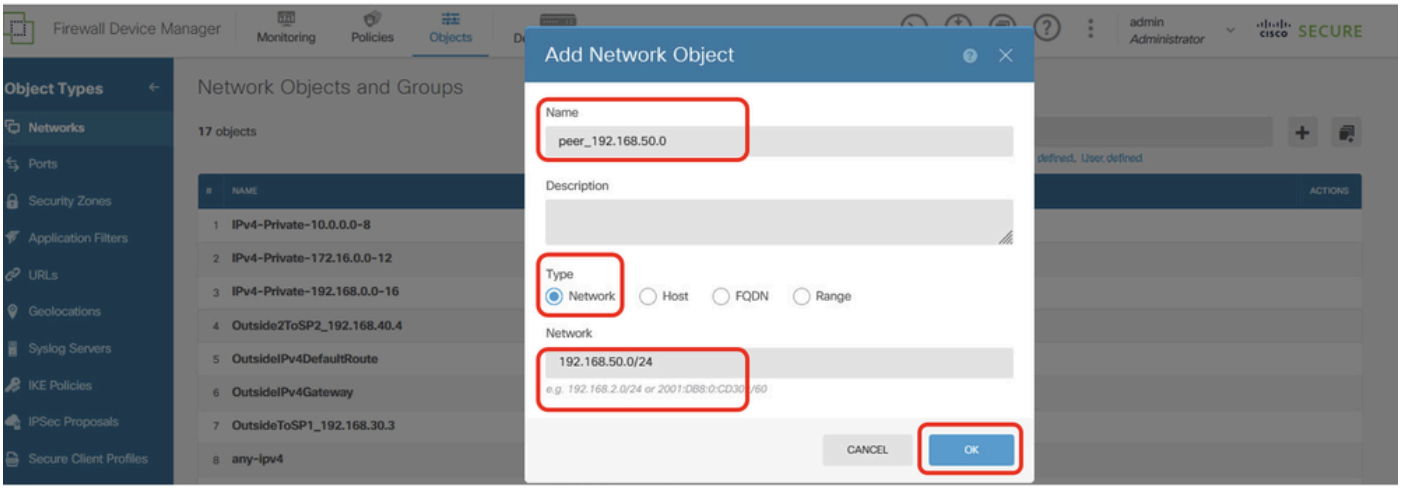
- 名称：peer_vti_169.254.20.12
- type：主机
- 网络：169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

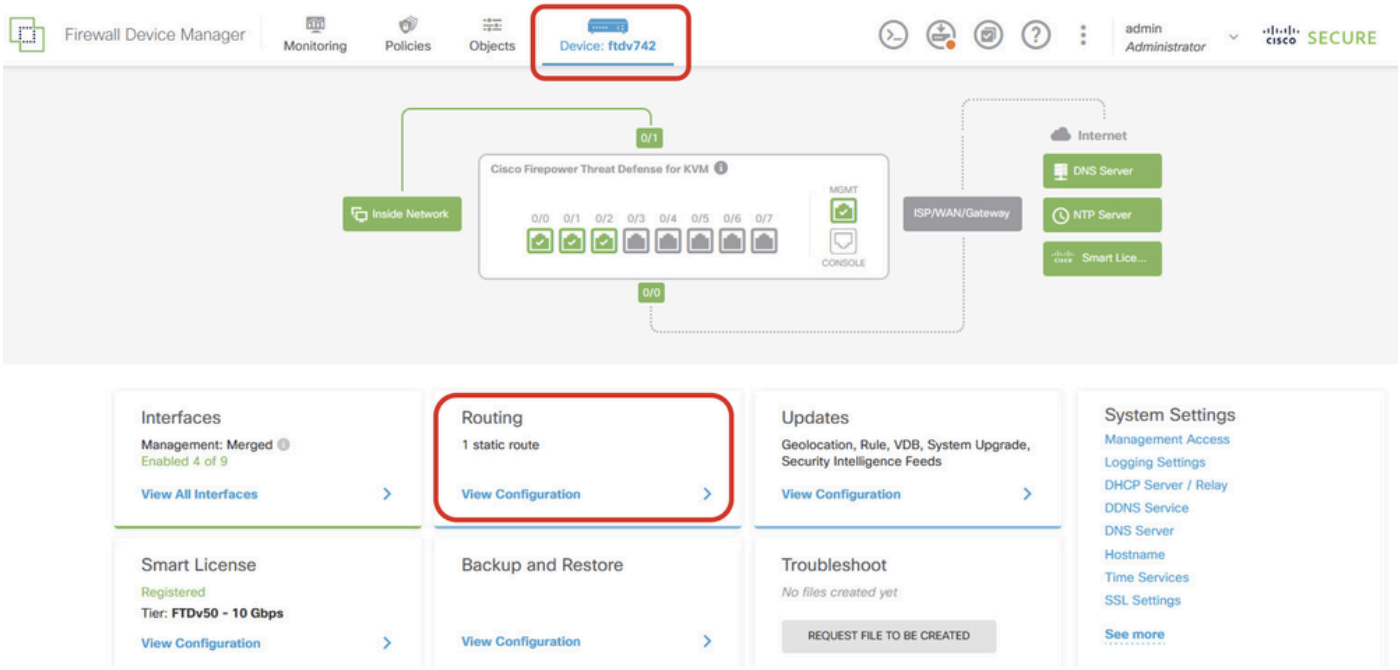
步骤22.4.为对等体Site2 FTD的内部网络创建对象。提供必要信息。单击OK按钮。

- 名称：peer_192.168.50.0
- type：网络
- 网络：192.168.50.0/24

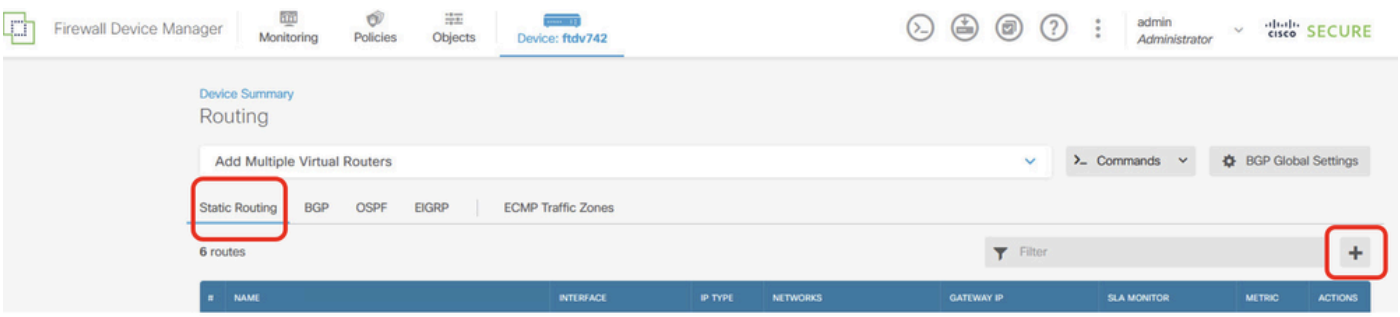


Site1FTD_Create_NetObj_StaticRoute_4

步骤23.导航到设备>路由。单击View Configuration。单击静态路由选项卡。单击+按钮添加新的静态路由。



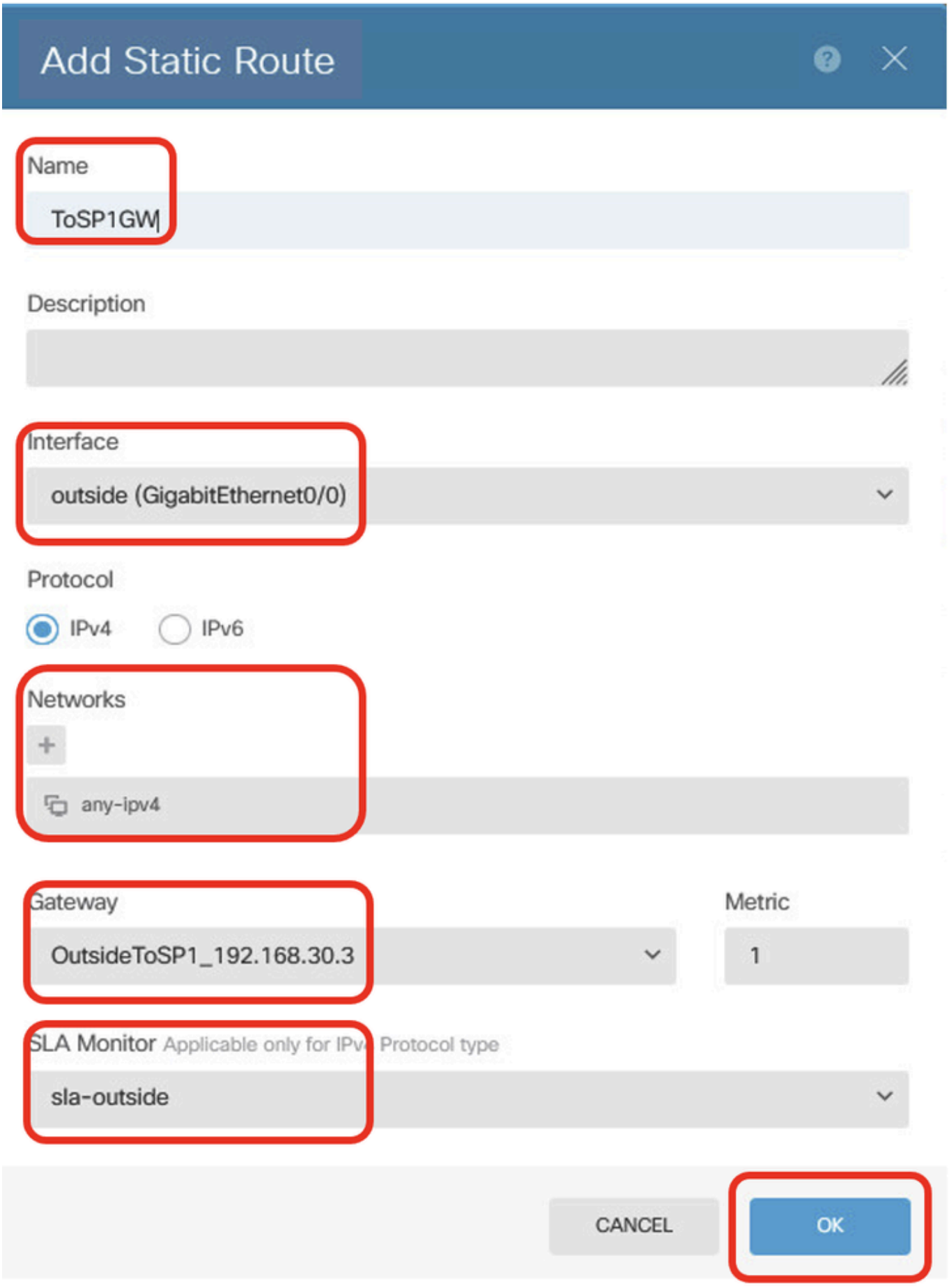
Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

步骤23.1.使用具有SLA监控的ISP1网关创建默认路由。如果ISP1网关出现中断，流量会通过ISP2切换到备用默认路由。一旦ISP1恢复，流量将恢复为使用ISP1。请提供必要的信息。单击OK按钮保存。

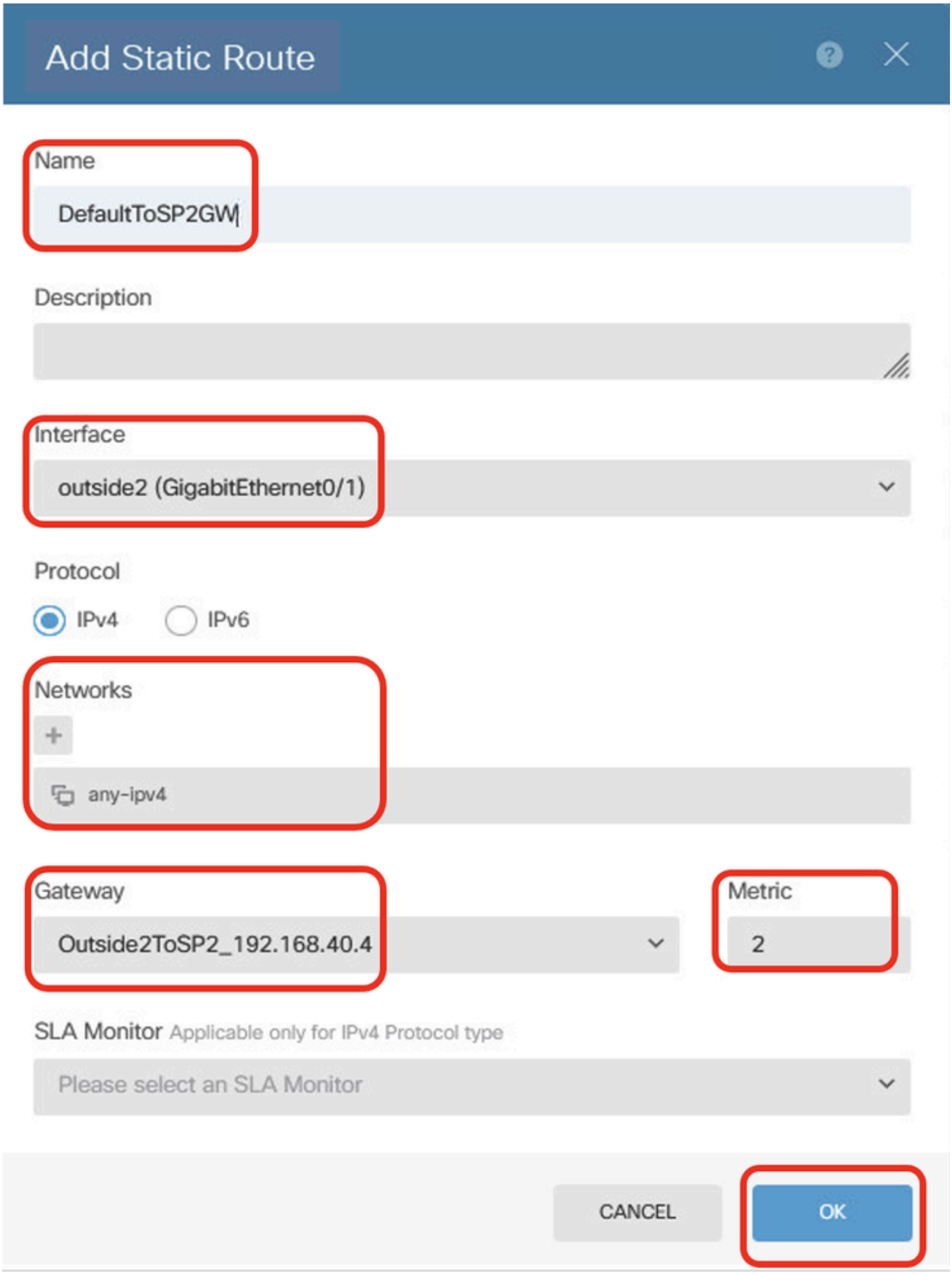
- 名称：ToSP1GW
- 接口:outside(GigabitEthernet0/0)
- 协议：IPv4
- 网络：any-ipv4
- 网关：OutsideToSP1_192.168.30.3
- 度量:1
- SLA监控：sla-outside



Site1FTD_Create_StaticRoute_1

步骤23.2.通过网关ISP2网关创建备用默认路由。指标必须大于1。在本例中，指标为2。请提供必要信息。单击OK按钮保存。

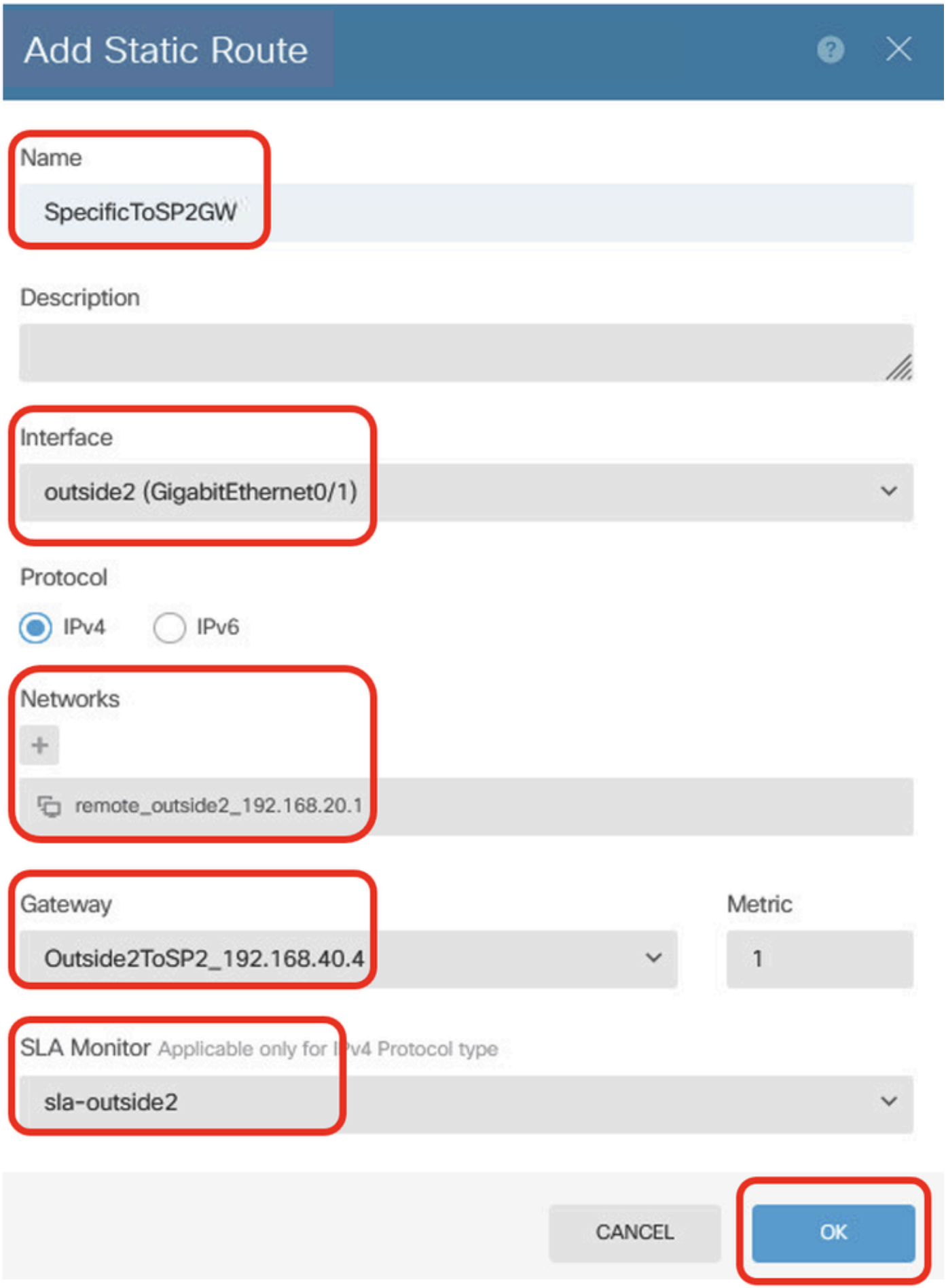
- 名称：DefaultToSP2GW
- 接口:outside2(GigabitEthernet0/1)
- 协议：IPv4
- 网络：any-ipv4
- 网关：Outside2ToSP2_192.168.40.4
- 度量:2



Site1FTD_Create_StaticRoute_2

第23.3步：通过ISP2网关创建到对等体Site2 FTD的outside2 IP地址的静态路由（具有SLA监控），用于与Site2 FTD的outside2建立VPN。提供必要的信息。单击OK按钮保存。

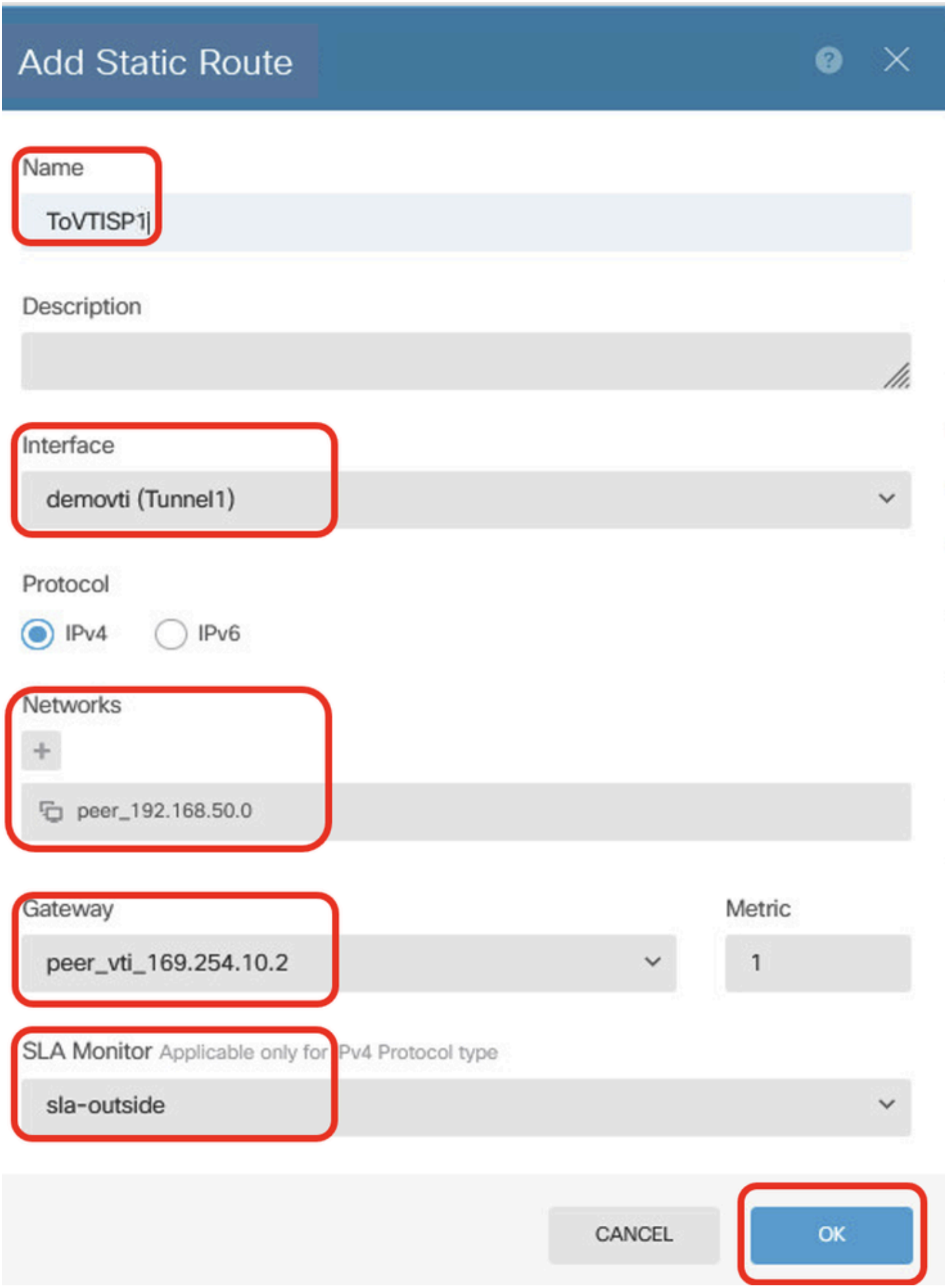
- 名称：SpecificToSP2GW
- 接口:outside2(GigabitEthernet0/1)
- 协议：IPv4
- 网络：remote_outside2_192.168.20.1
- 网关：Outside2ToSP2_192.168.40.4
- 度量:1
- SLA监控：sla-outside2



Site1FTD_Create_StaticRoute_3

第23.4步：创建通往对等体Site2 FTD的内部网络的目标流量的静态路由（通过Site2 FTD的对等VTI隧道1作为网关），并使用SLA监控来加密通过隧道1的客户端流量。如果ISP1网关遇到中断，VPN流量将切换到ISP2的VTI隧道2。一旦ISP1恢复，流量将恢复到ISP1的VTI隧道1。请提供必要信息。单击OK按钮保存。

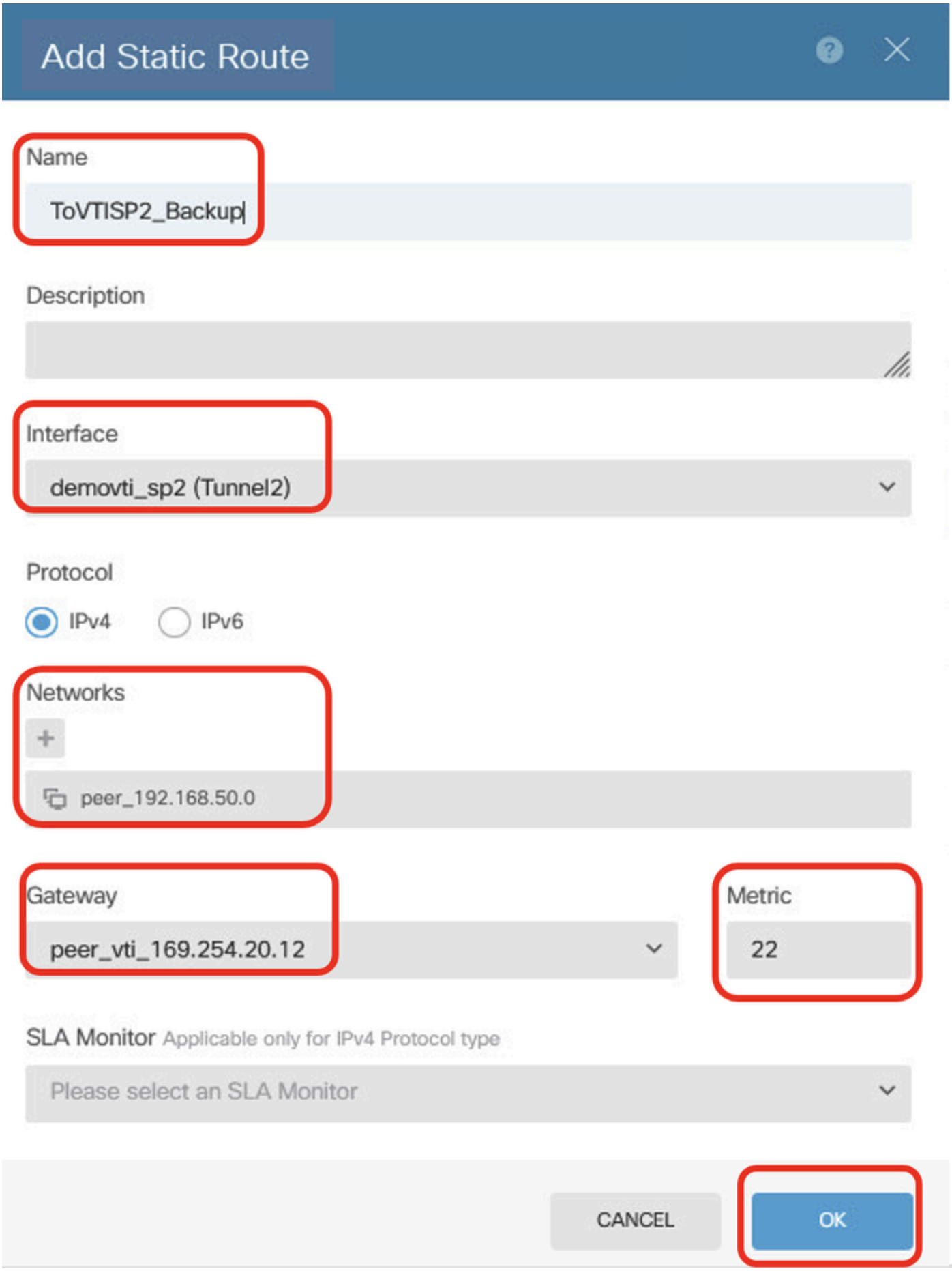
- 名称：ToVTISP1
- 接口:demovti(Tunnel1)
- 协议：IPv4
- 网络：peer_192.168.50.0
- 网关：peer_vti_169.254.10.2
- 度量:1
- SLA监控：sla-outside



Site1FTD_Create_StaticRoute_4

步骤23.5.创建备用静态路由，通过Site2 FTD的对等VTI隧道2作为网关将目标流量发送到对等体Site2 FTD的内部网络，用于通过隧道2加密客户端流量。将度量设置为大于1的值。在本示例中，度量为22。提供必需的信息。单击OK按钮保存。

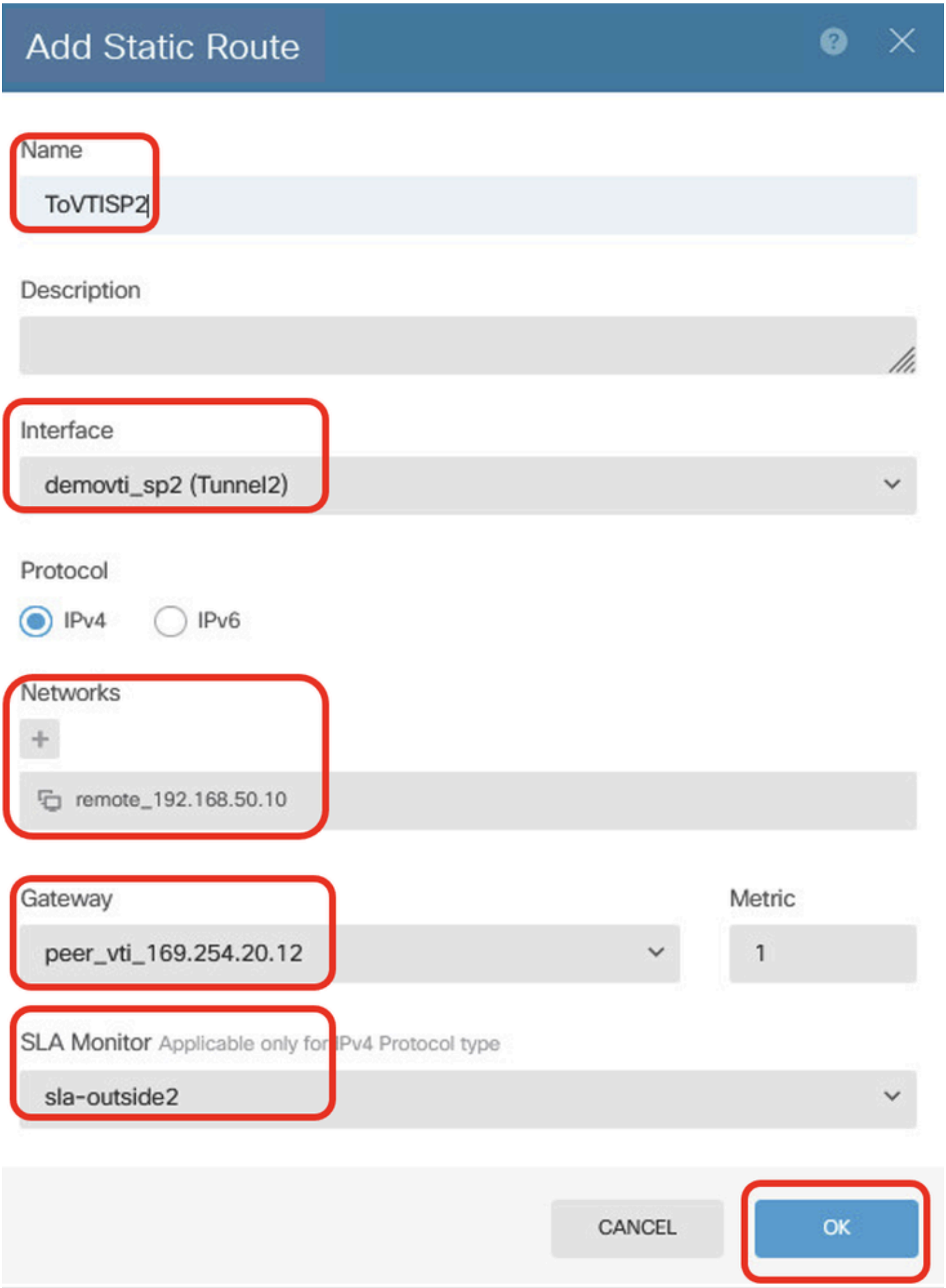
- 名称：ToVTISP2_Backup
- 接口:demovti_sp2(Tunnel2)
- 协议：IPv4
- 网络：peer_192.168.50.0
- 网关：peer_vti_169.254.20.12
- 度量:22



Site1FTD_Create_StaticRoute_5

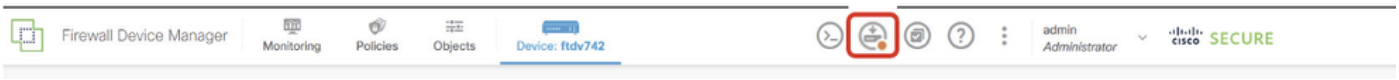
步骤23.6.为PBR流量创建静态路由。通过Site2 FTD的对等VTI隧道2作为网关发往Site2 Client2的目标流量，具有SLA监控。请提供必要信息。单击OK按钮保存。

- 名称：ToVTISP2
- 接口:demovti_sp2(Tunnel2)
- 协议：IPv4
- 网络：remote_192.168.50.10
- 网关：peer_vti_169.254.20.12
- 度量:1
- SLA监控：sla-outside2



Site1FTD_Create_StaticRoute_6

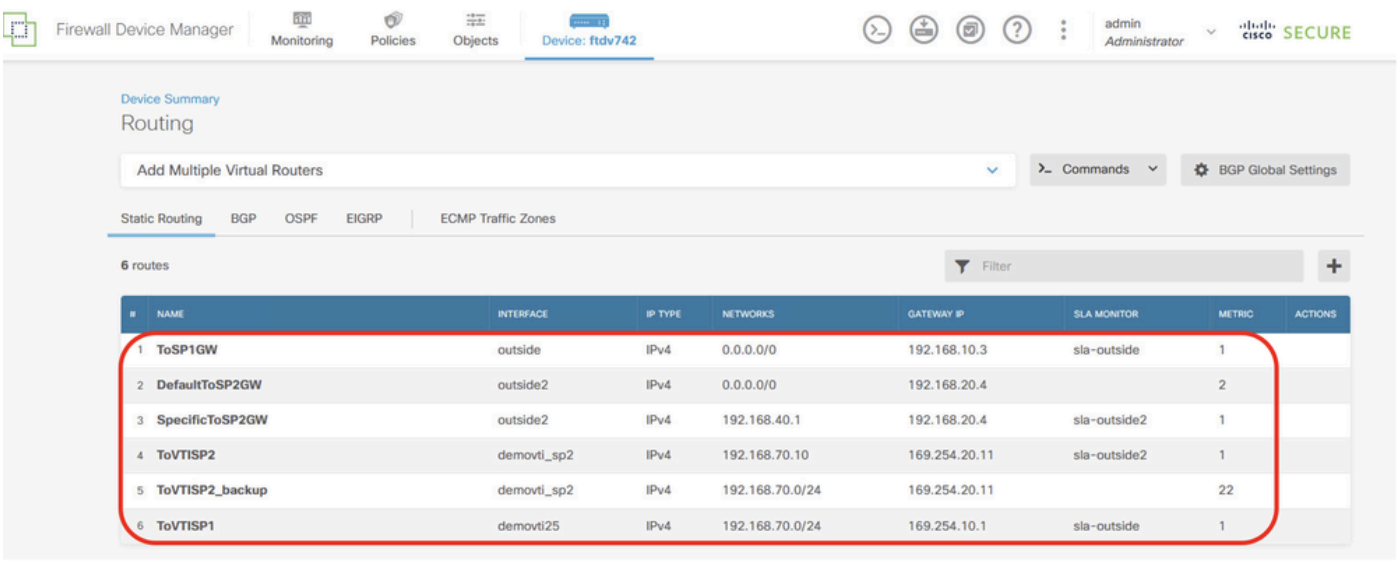
步骤24.部署配置更改。



站点1FTD_部署_更改

站点2 FTD静态路由配置

步骤25.重复步骤22到24以创建静态路由，其中包含Site2 FTD的相应参数。



Site2FTD_Create_StaticRoute

验证

使用本部分可确认配置能否正常运行。通过控制台或SSH导航至Site1 FTD和Site2 FTD的CLI。

ISP1和ISP2工作正常

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549
```

```
IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d
```

```
// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
499259237 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607
```

路由

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA监控

```
// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
```

```
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
```

```
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
// Site2 FTD:

ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Ping 测试

场景1. Site1 Client1 ping Site2 Client1。

在ping之前，请检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD.

在本示例中，Tunnel1显示1497个数据包用于封装，1498个数据包用于解封。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
```

```
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1成功ping Site2 Client1。

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD after ping successfully。

在本示例中，隧道1显示用于封装的1502个数据包和用于解封的1503个数据包，两个计数器增加5个数据包，匹配5个ping回应请求。这表明Site1 Client1到Site2 Client1的ping操作是通过ISP1 Tunnel 1路由的。Tunnel 2显示封装或解封计数器没有增加，从而确认没有用于此流量。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

场景2. Site1 Client2 ping Site2 Client2。

在ping之前，请检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD.

在本示例中，Tunnel2显示21个数据包用于封装，20个数据包用于解封。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2成功ping Site2 Client2。

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/39/87 ms
```

检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD after ping successfully。

在本示例中，隧道2显示用于封装的26个数据包和用于解封的25个数据包，两个计数器增加5个数据包，匹配5个ping回应请求。这表示通过ISP2隧道2将Site1 Client2 ping Site2 Client2。隧道1显示封装或解封计数器没有增加，从而确认没有用于此流量。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

当ISP2正常工作时，ISP1会遇到中断

在本例中，手动关闭ISP1的接口E0/1，模拟ISP1发生中断。

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Tunnel1发生故障。只有Tunnel2与IKEV2 SA处于活动状态。

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500                    C
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500                    G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

路由

在路由表中，备用路由将生效。

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA监控

在Site1 FTD上，SLA监控器显示ISP1的条目编号为855903900 timeout（目标地址为192.168.30.3）。

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
```

```
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping 测试

在ping之前，请检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD.

在本示例中，Tunnel2显示36个数据包用于封装，35个数据包用于解封。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1成功ping Site2 Client1。

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2成功ping Site2 Client2。

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/56/87 ms
```

检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD afsuccessfully ping。

在本示例中，隧道2显示用于封装的46个数据包和用于解封的45个数据包，两个计数器增加10个数据包，匹配10个ping回应请求。这表示ping数据包通过ISP2隧道2路由。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
```

```
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

当ISP1工作正常时，ISP2会遇到中断

在本例中，手动关闭ISP2的接口E0/1，以模拟ISP2发生中断。

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

Tunnel2发生故障。只有Tunnel1与IKEV2 SA处于活动状态。

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc



// Site2 FTD:
```

```
ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

路由

在路由表中，与ISP2相关的路由不适用于PBR流量。

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:
```

```
ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

SLA监控

在Site1 FTD上，SLA监控器显示ISP2的条目编号为188426425 timeout（目标地址为192.168.40.4）。

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
```

```
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping 测试

在ping之前，请检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD.

在本示例中，隧道1显示用于封装的74个数据包，以及用于解封的73个数据包。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1成功ping Site2 Client1。

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2成功ping Site2 Client2。

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/58/143 ms
```

检查show crypto ipsec sa的计数器 | inc interface:|encap|decap on Site1 FTD after ping successfully。

在本示例中，隧道1显示用于封装的84个数据包和用于解封的83个数据包，两个计数器均增加10个数据包，匹配10个ping回应请求。这表示ping数据包通过ISP1隧道1路由。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

您可以使用这些debug命令对VPN部分进行故障排除。

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

您可以使用这些debug命令对PBR部分进行故障排除。

```
debug policy-route
```

您可以使用这些debug命令对SLA Monitor部分进行故障排除。

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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）。