在FDM管理的FTD上配置基于路由的VPN上的BGP

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- VPN上的配置
- BGP上的配置

验证

故障排除

简介

本文档介绍如何在FirePower设备管理器(FDM)管理的FTDv上通过基于路由的站点到站点VPN配置BGP。

先决条件

要求

Cisco 建议您了解以下主题：

- 对VPN的基本了解
- FTDv上的BGP配置
- 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：

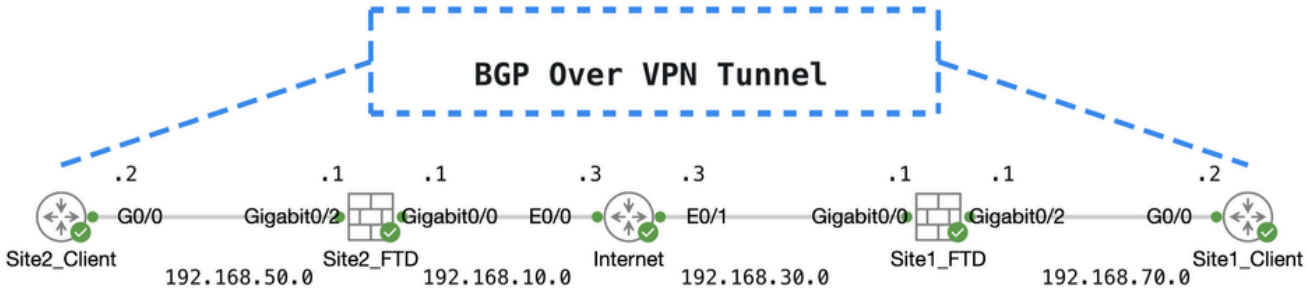
- 思科FTDv版本7.4.2

- 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。

配置

网络图



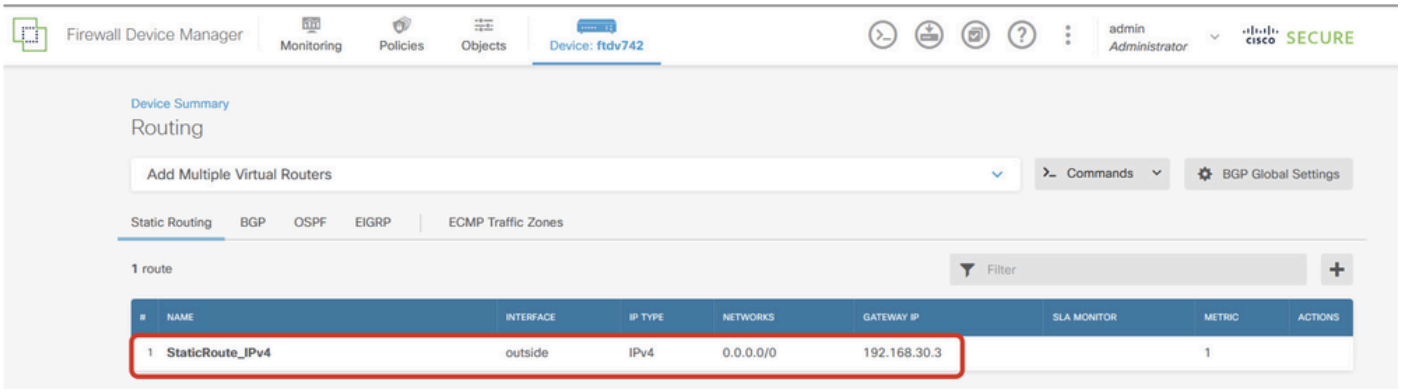
Topo

VPN上的配置

步骤1.确保节点间的IP互联已准备就绪，性能稳定。FDM上的智能许可证已成功注册到智能帐户。

步骤2.为Site1客户端的网关配置Site1 FTD的内部IP地址(192.168.70.1)。 Site2客户端的网关配置有Site2 FTD的内部IP地址(192.168.50.1)。 此外，请确保在FDM初始化后，正确配置两个FTD上的默认路由。

登录到每个FDM的GUI。导航至。Device > Routing单击。View Configuration单击选**Static Routing**项卡以检验默认静态路由。



站点1_FTD_网关



站点2_FTD_网关

步骤3.配置基于路由的站点到站点VPN。在此示例中，首先配置Site1 FTD。

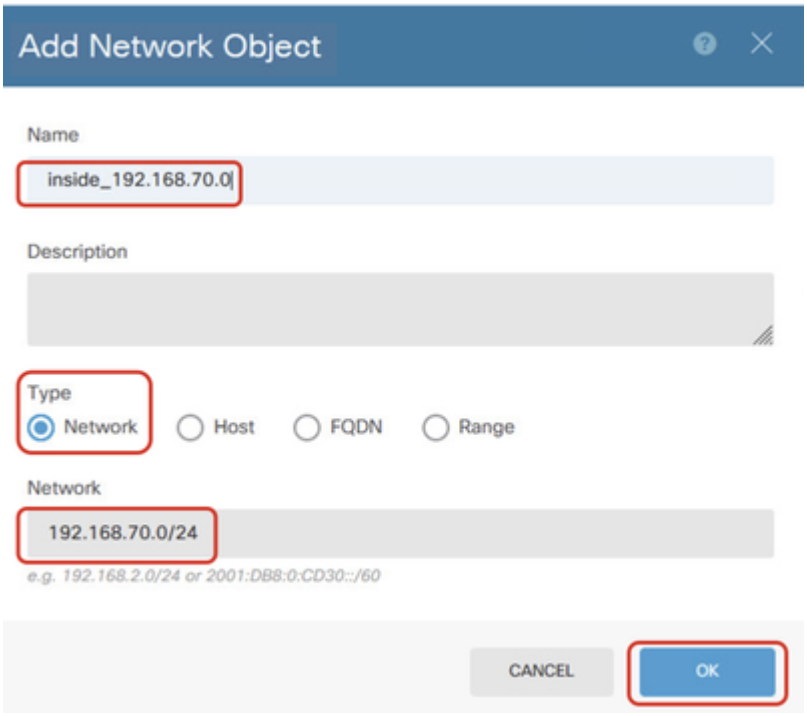
第3.1步：登录到Site1 FTD的FDM GUI。为Site1 FTD的内部网络创建新的网络对象。导航到**Objects > Networks**，单击+按钮。



Create_Network_Object

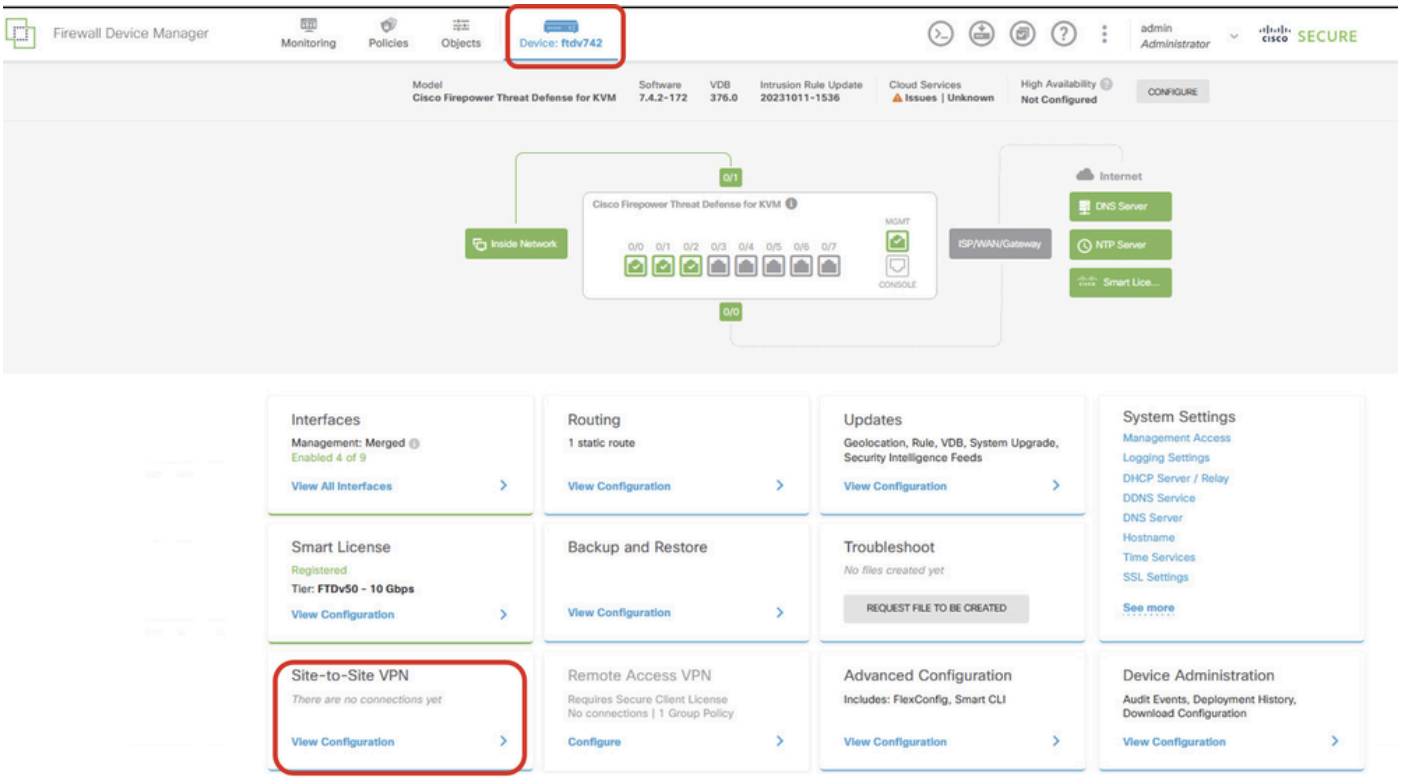
步骤3.2.提供必要信息。单击 按钮。OK

- 名称：inside_192.168.70.0
- type：网络
- 网络:192.168.70.0/24



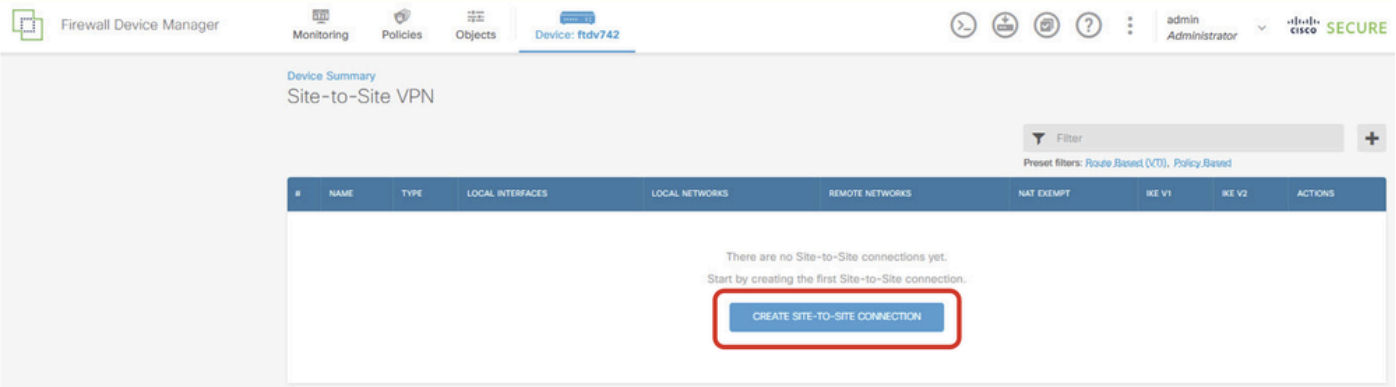
Site1_Inside_Network

第 3.3 步： 导航至 。**Device > Site-to-Site VPN**单击。**View Configuration**



查看站点到站点VPN

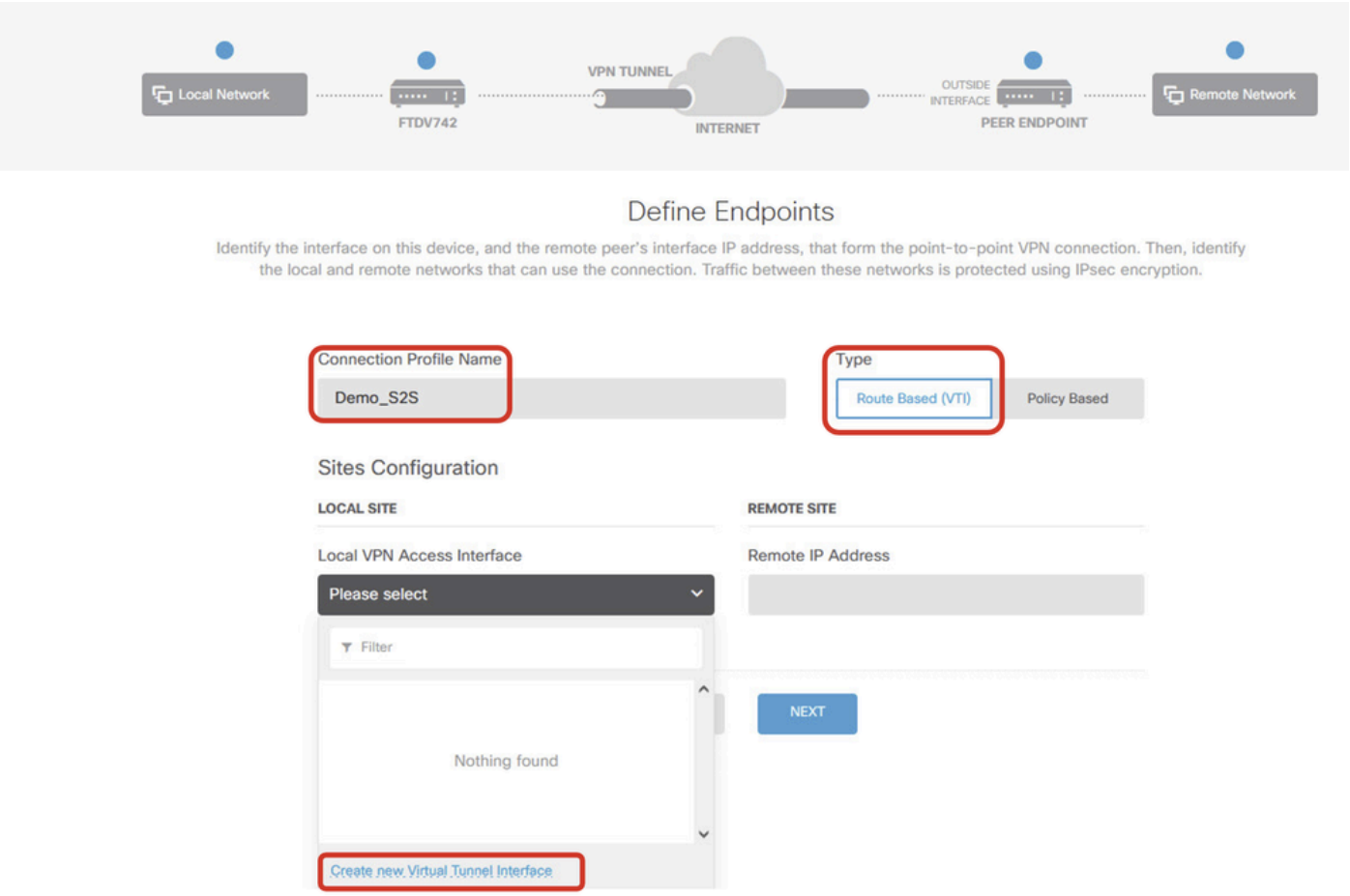
步骤3.4.开始创建新的站点到站点VPN。单击。**CREATE SITE-TO-SITE CONNECTION**



Create_Site-to-Site_Connection

步骤3.5.提供必要的信息。

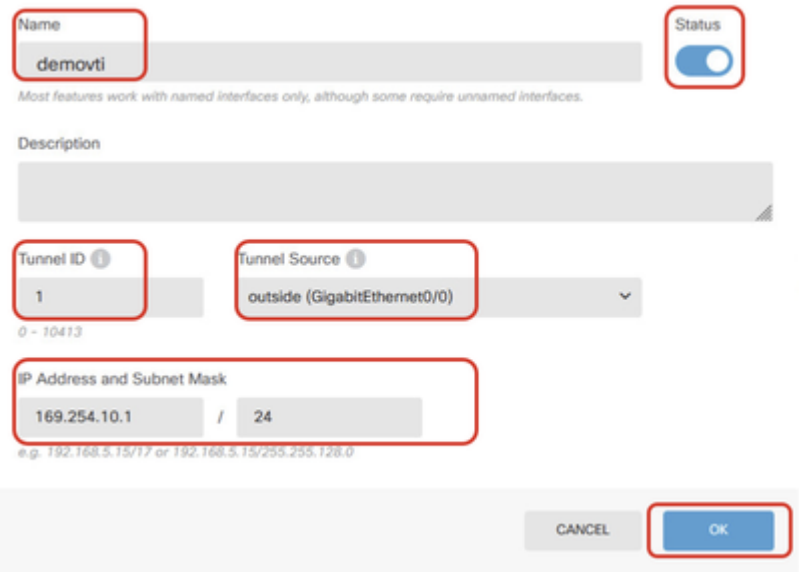
- 连接配置文件名称：Demo_S2S
- type：基于路由(VTI)
- 本地VPN访问接口：单击下拉列表，然后单击**Create new Virtual Tunnel Interface**。



Create_VTI_in_VPN_Wizard

第3.6步：提供创建新VTI所需的信息。单击OK按钮。

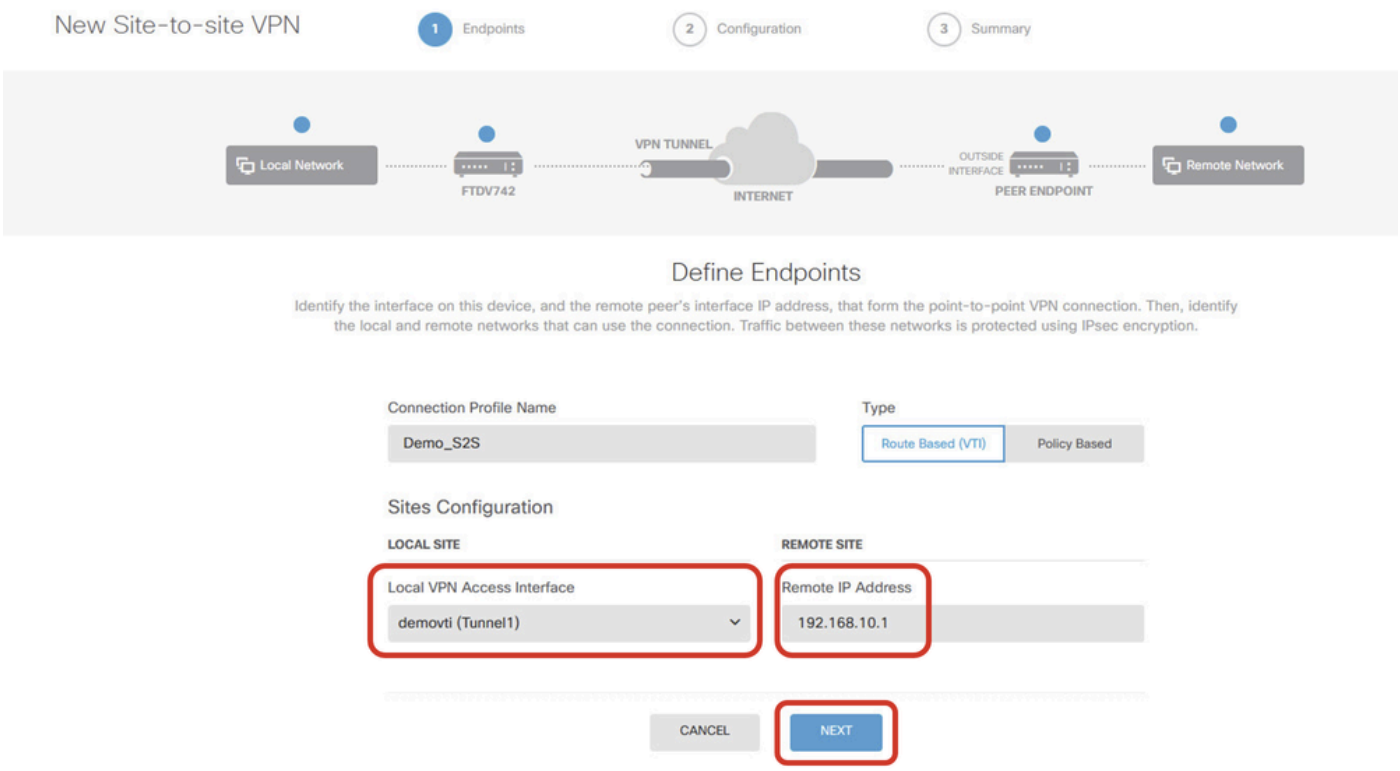
- 名称：demovti
- 隧道ID:1
- 通道来源:外部(GigabitEthernet0/0)
- IP 地址和子网掩码:169.254.10.1/24
- 状态:单击滑块到“已启用”位置



创建_VTI_详细信息

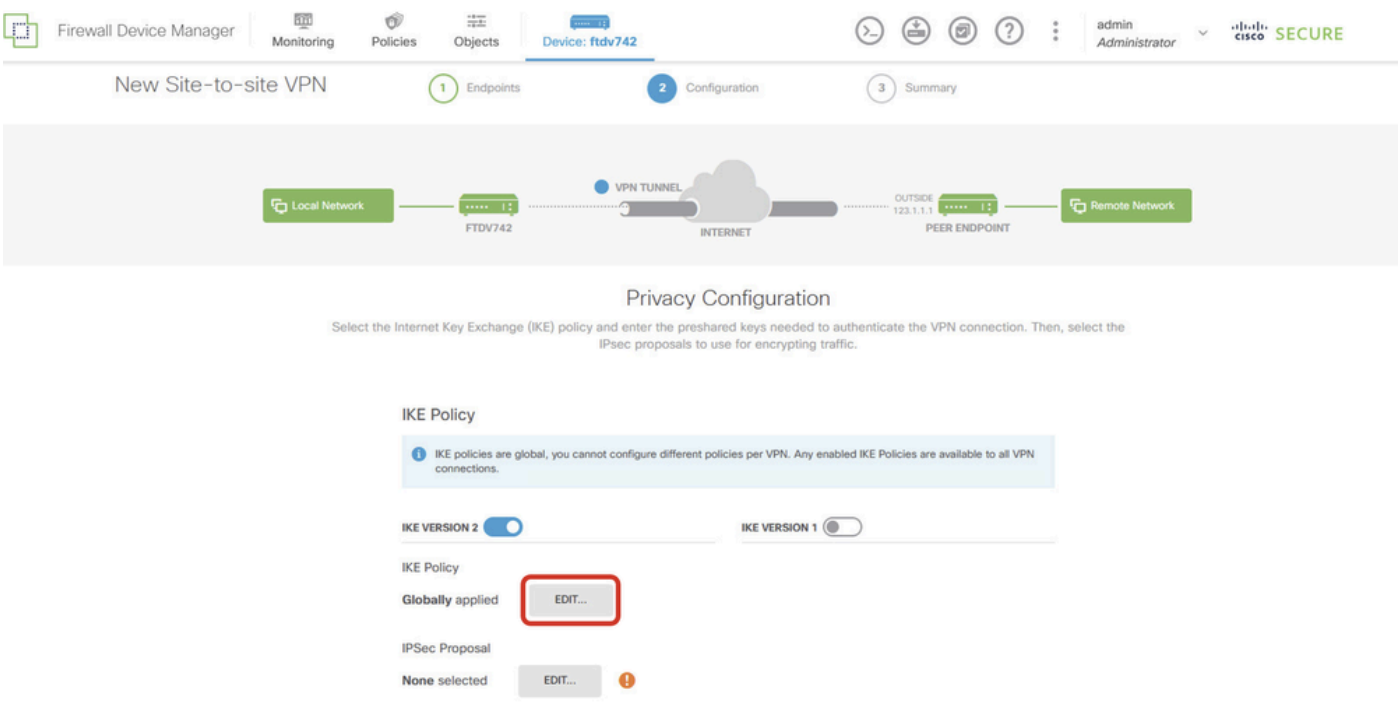
步骤3.7.继续提供必要的信息。单击NEXT按钮。

- 本地VPN访问接口：demovti（在步骤3.6中创建。）
- 远程 IP 地址:192.168.10.1



VPN_Wizard_Endpoints_Step1

第3.8步：导航到IKE Policy。单击 Edit 按钮。



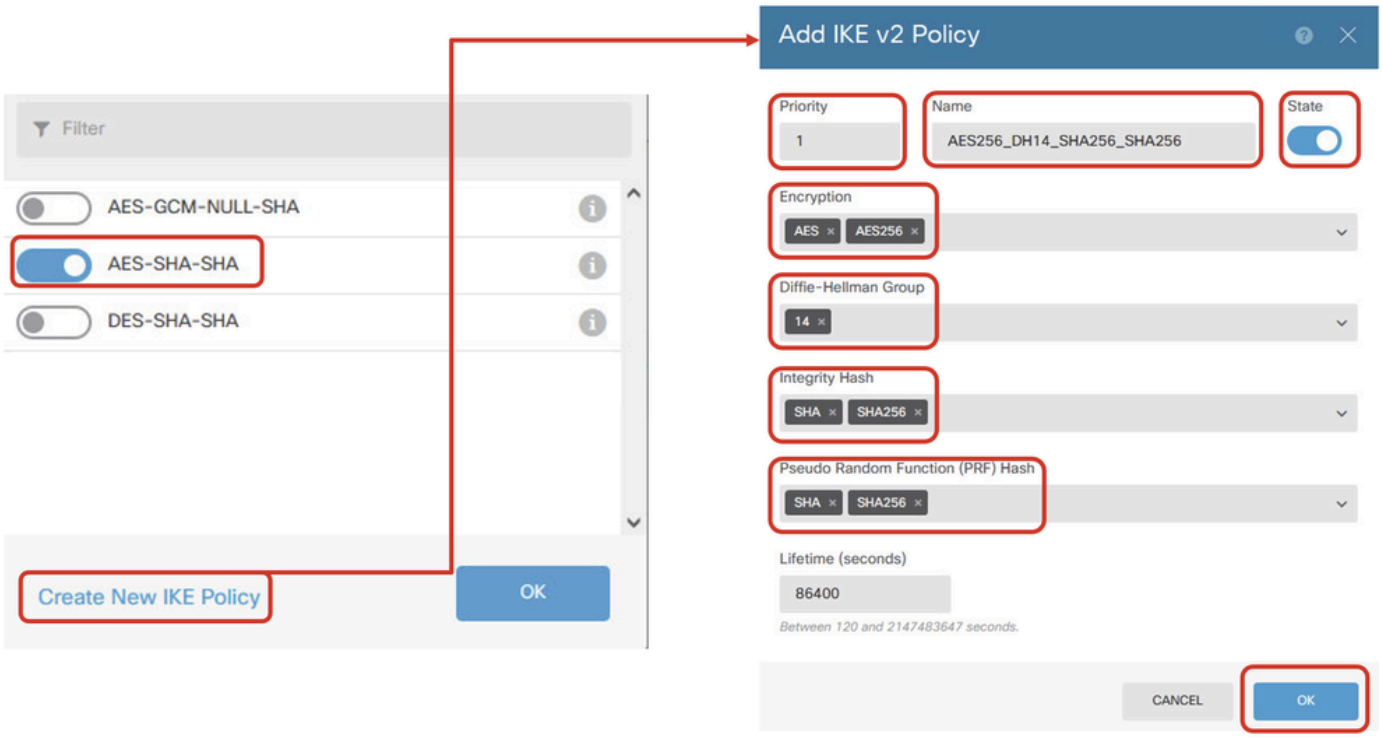
Edit_IKE_Policy

第3.9步：对于IKE策略，可以使用预定义策略，也可以通过点击Create New IKE Policy创建新策略

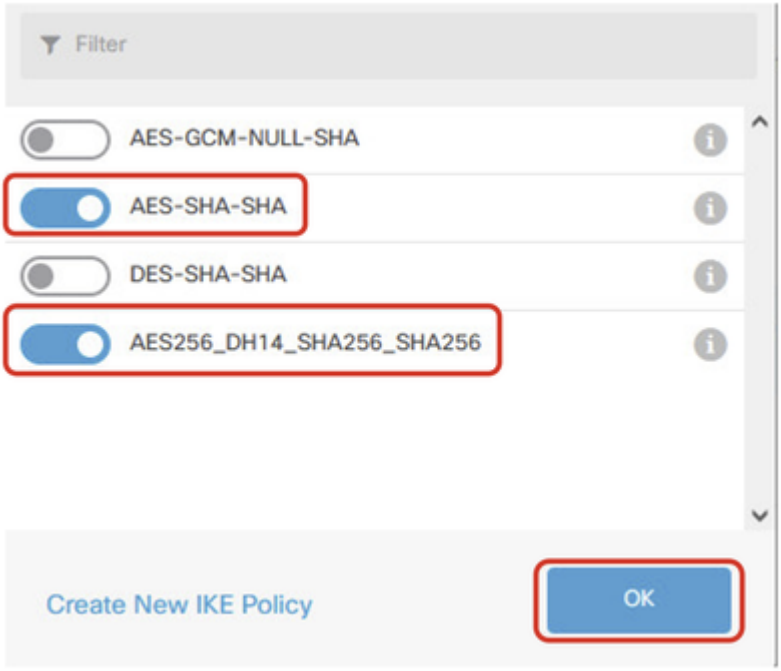
。

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)

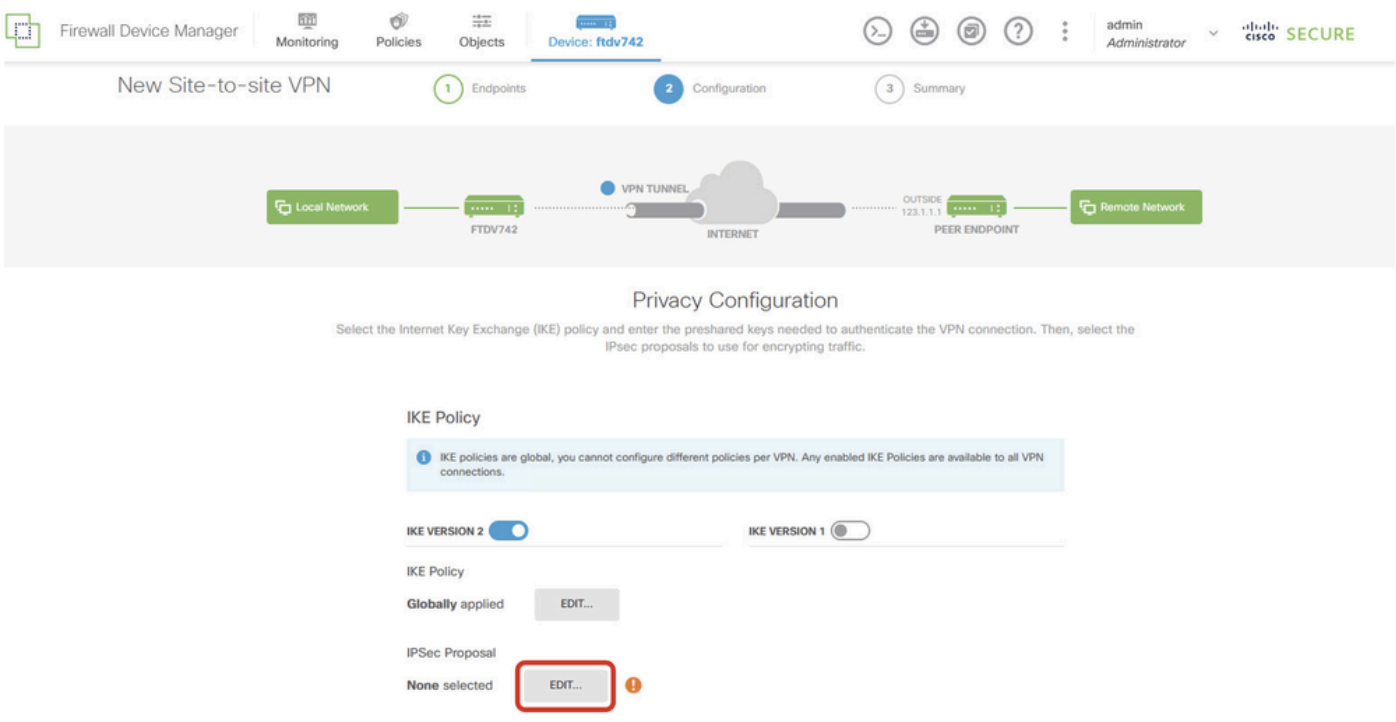


Add_New_IKE_Policy



Enable_New_IKE_Policy

步骤3.10.导航至IPSec建议。单击 Edit 按钮。

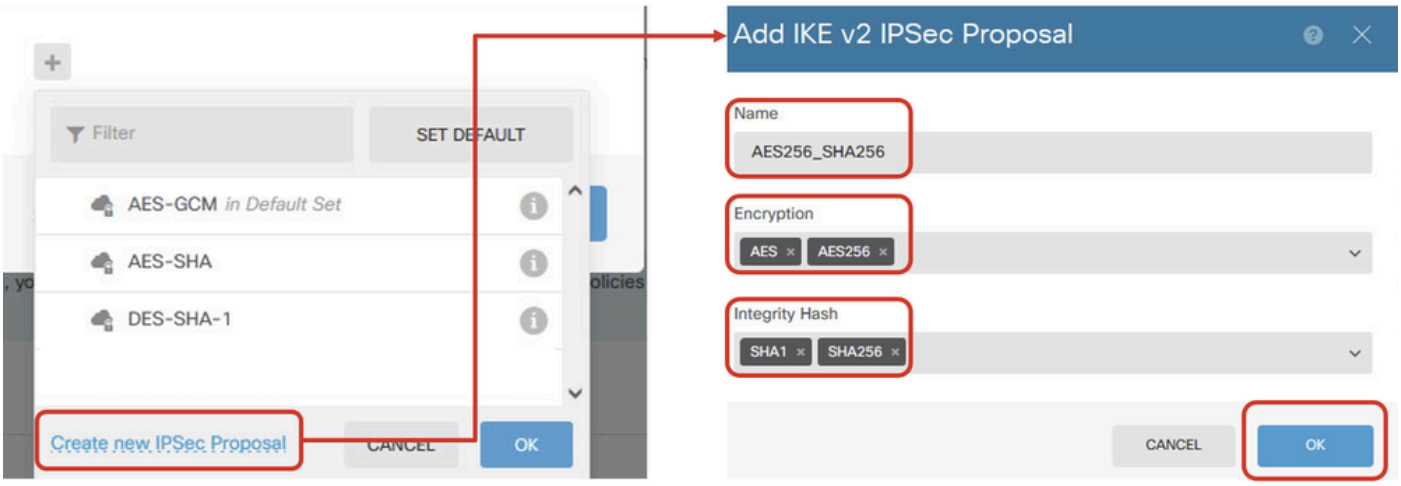


Edit_IKE_Proposal

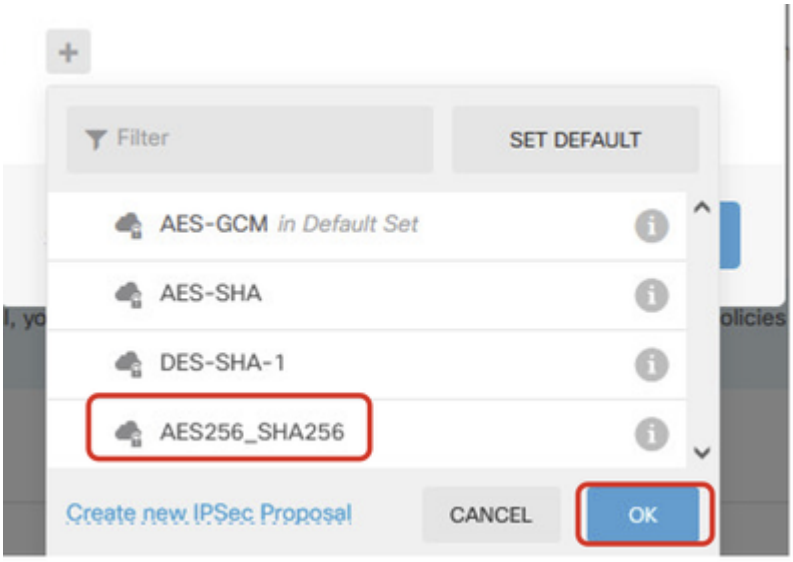
第3.11步：对于IPSec提议，您可以使用预定义，也可以通过点击创建新的IPSec提议创建新提议。在本例中，创建新一个用于演示目的。提供必要的信息。单击OK按钮进行保存。

- 名称：AES256_SHA256

- 加密 :AES、AES256
- 完整性哈希：SHA1、SHA256



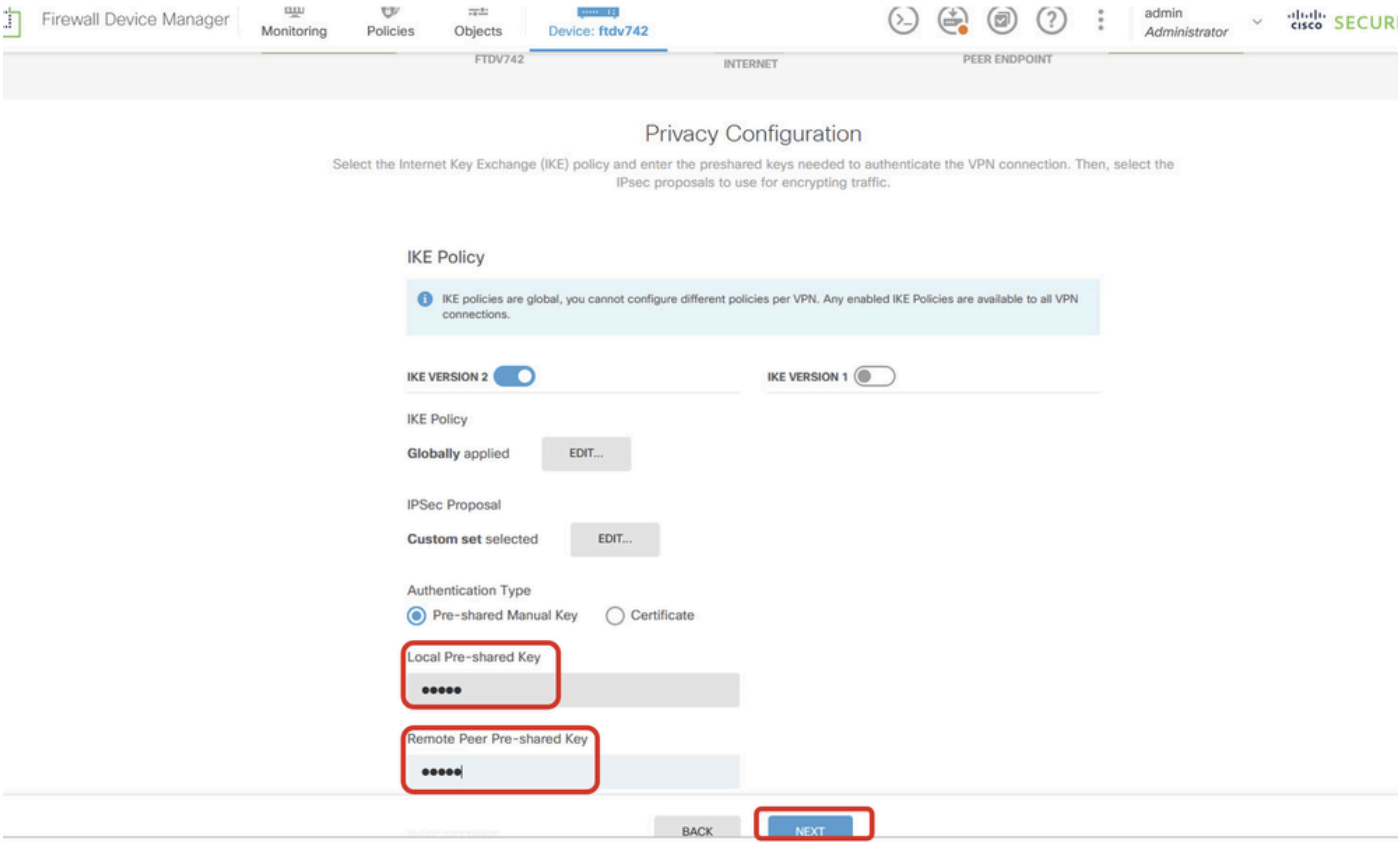
Add_New_IPSec_Proposal



Enable_New_IPSec_Proposal

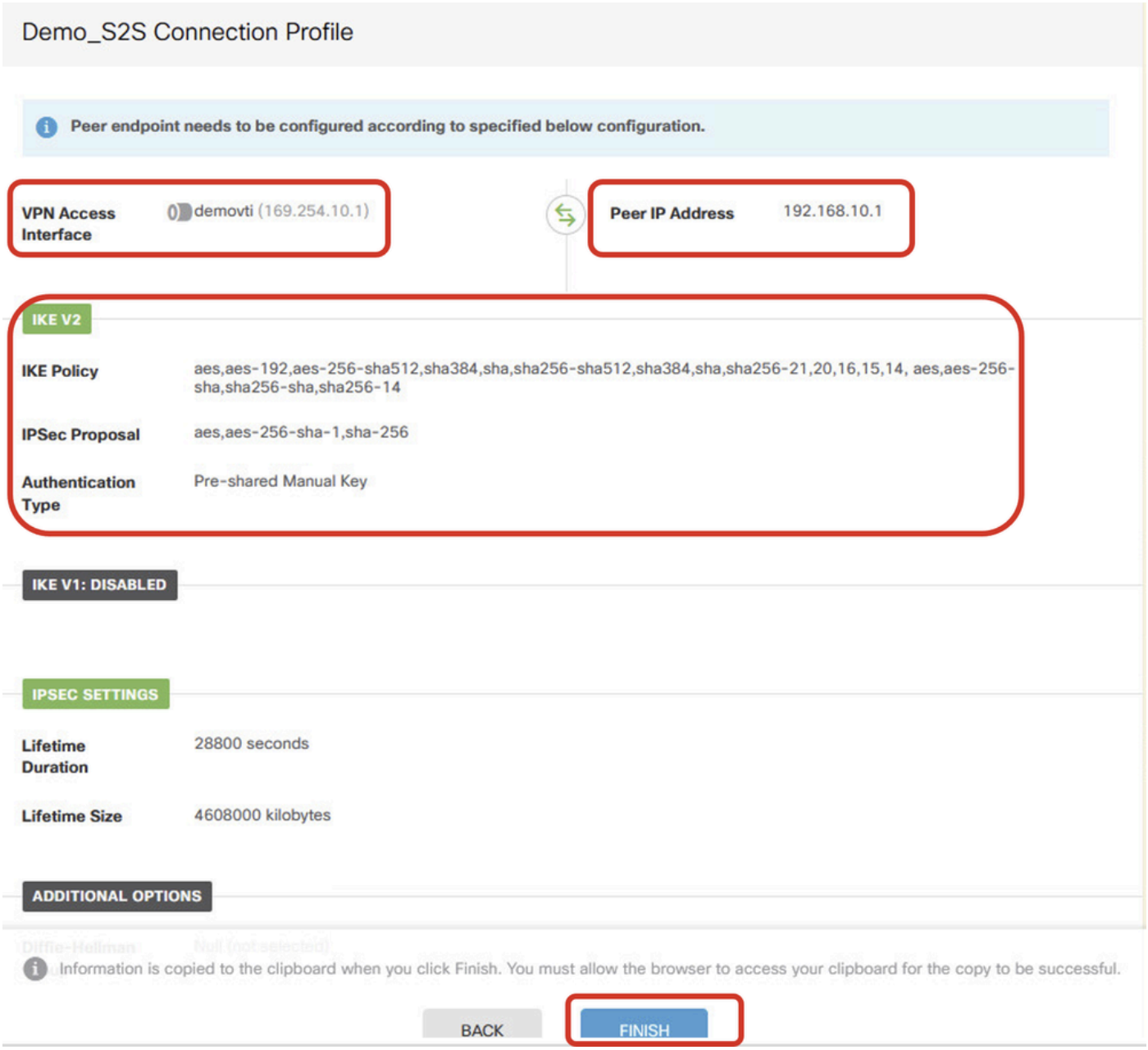
步骤3.12.配置预共享密钥。单击 Next 按钮。

记下此预共享密钥，稍后在Site2 FTD上配置该密钥。



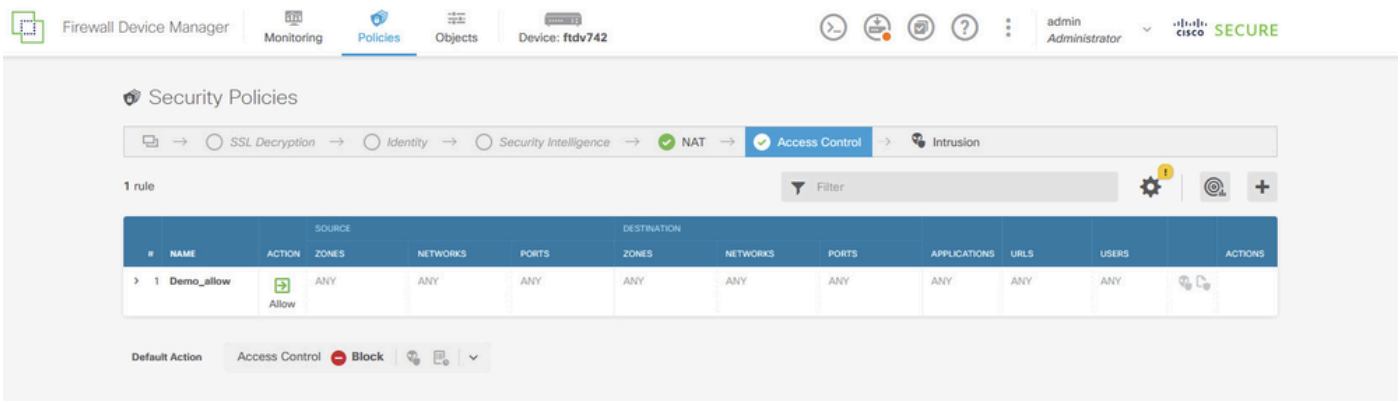
Configure_Pre_Shared_Key

步骤3.13.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。



VPN_Wizard_Complete

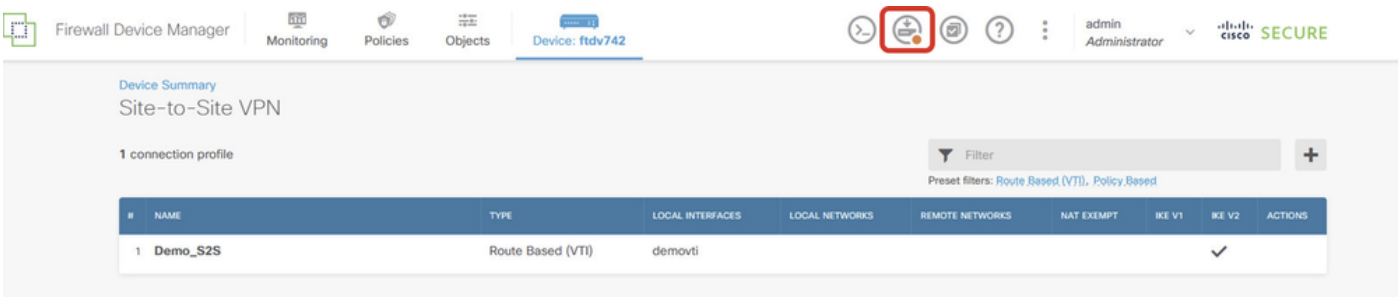
步骤3.14.创建访问控制规则，以允许流量通过FTD。在本示例中，允许所有内容用于演示目的。根据实际需要修改策略。



Access_Control_Rule_Instance

第3.15步（可选）如果为客户端配置了动态NAT以访问互联网，请在FTD上为客户端流量配置NAT豁免规则。在本示例中，无需配置NAT免除规则，因为每个FTD上均未配置动态NAT。

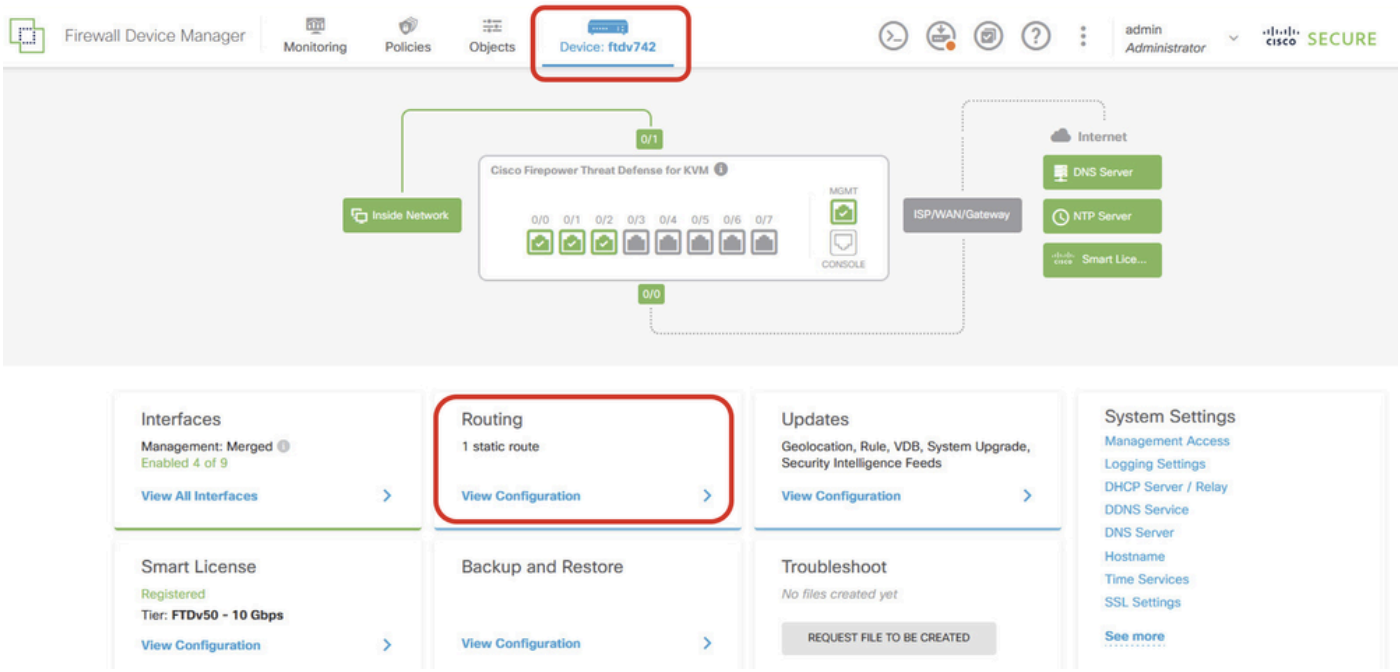
步骤3.16.部署配置更改。



部署VPN配置

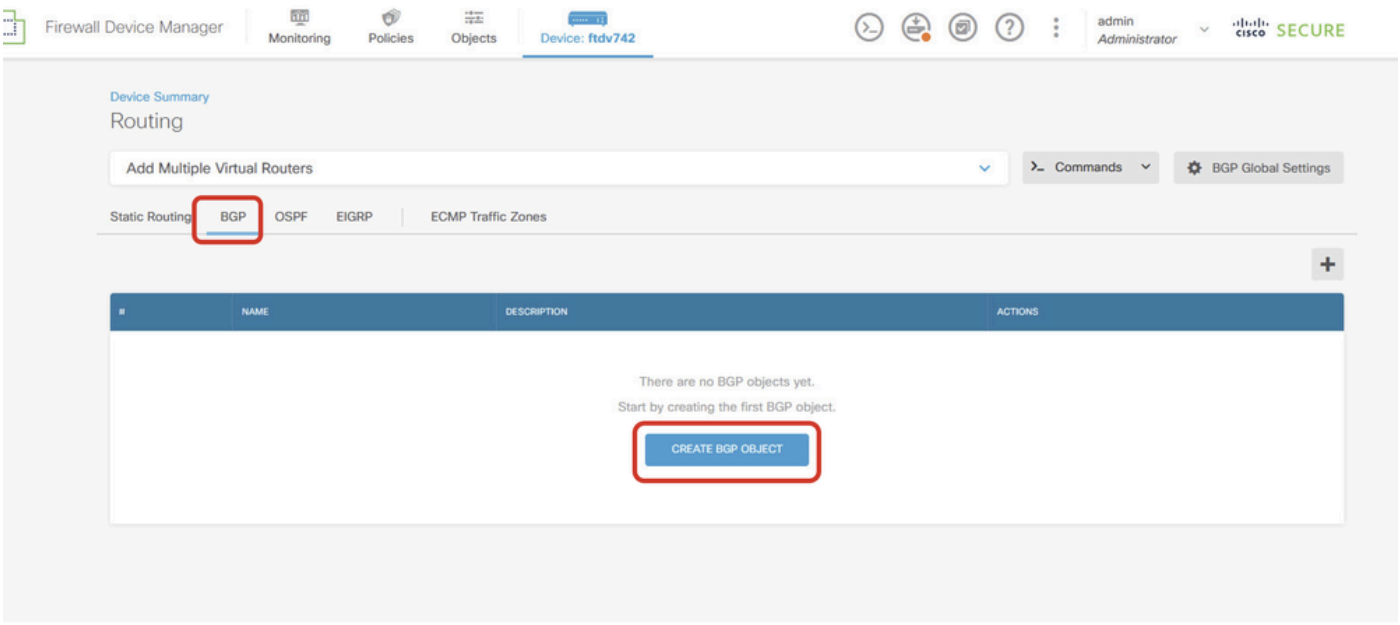
BGP上的配置

步骤4.导航到设备>路由。单击View Configuration。



View_Routing_Configuration

步骤5.单击BGP选项卡，然后单击CREATE BGP OBJECT。



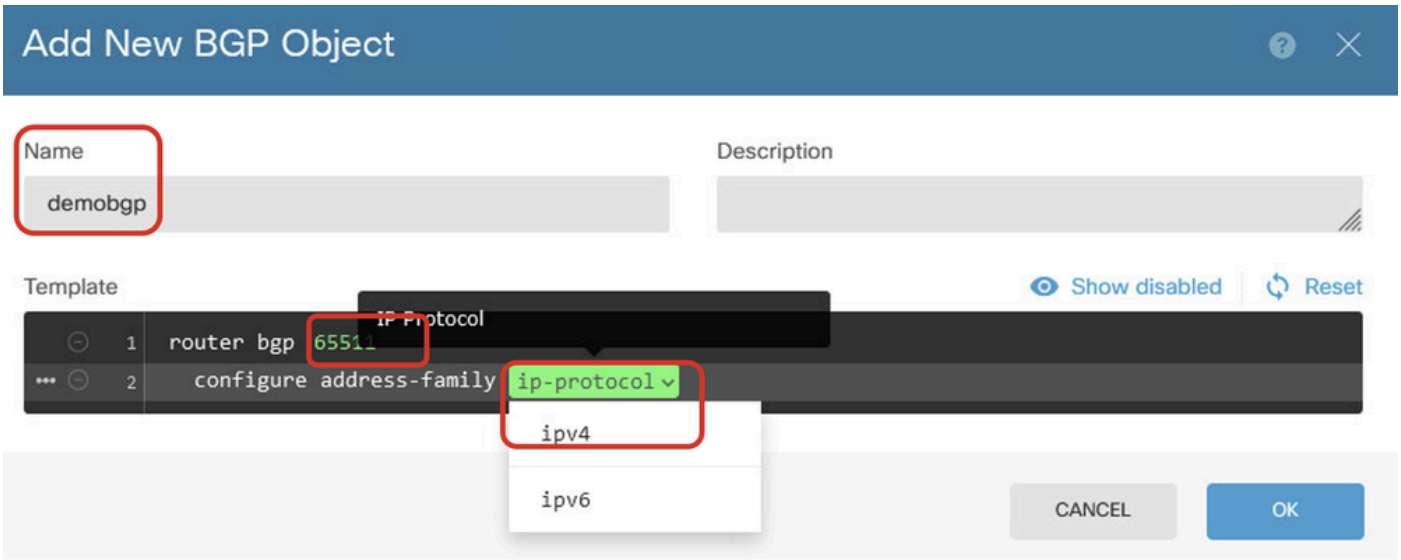
Create_BGP_Object

步骤6.提供对象的名称。导航到模板并进行配置。单击OK按钮保存。

名称：demobgp

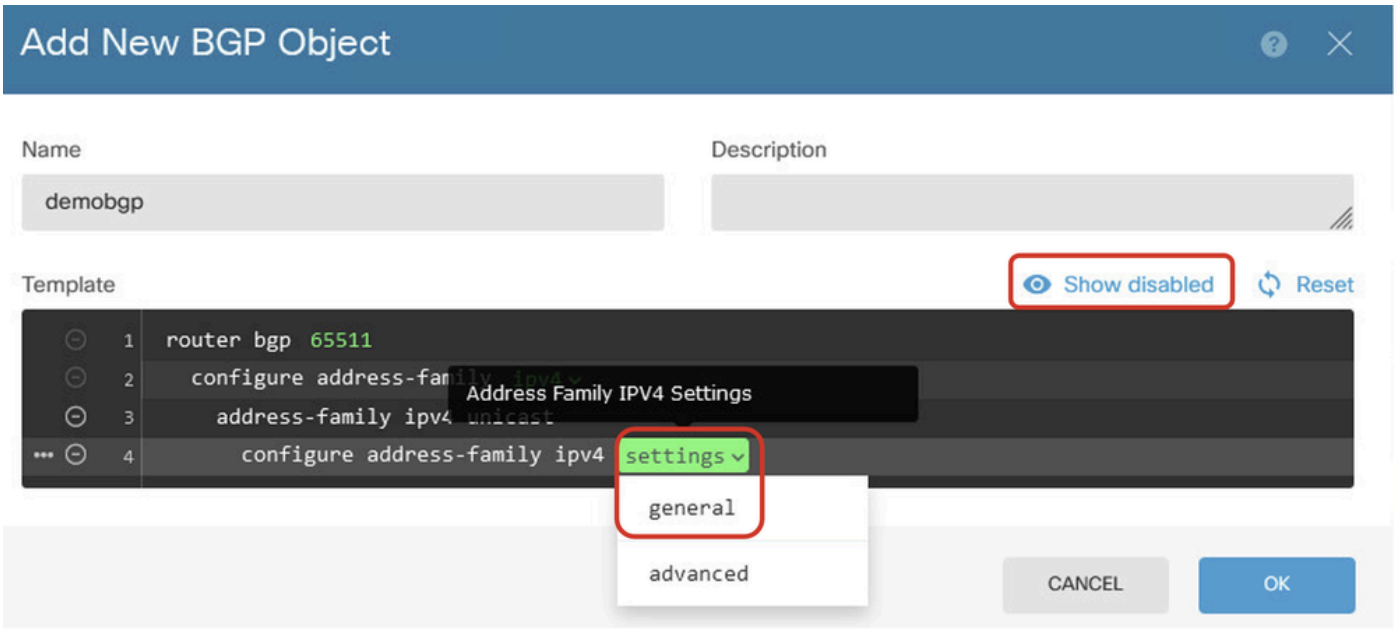
第 1 行:配置AS编号。单击as-number。手动输入本地AS number。在本示例中，Site1 FTD的AS编号65511。

第 2 行:配置IP协议。单击ip-protocol。选择ipv4。



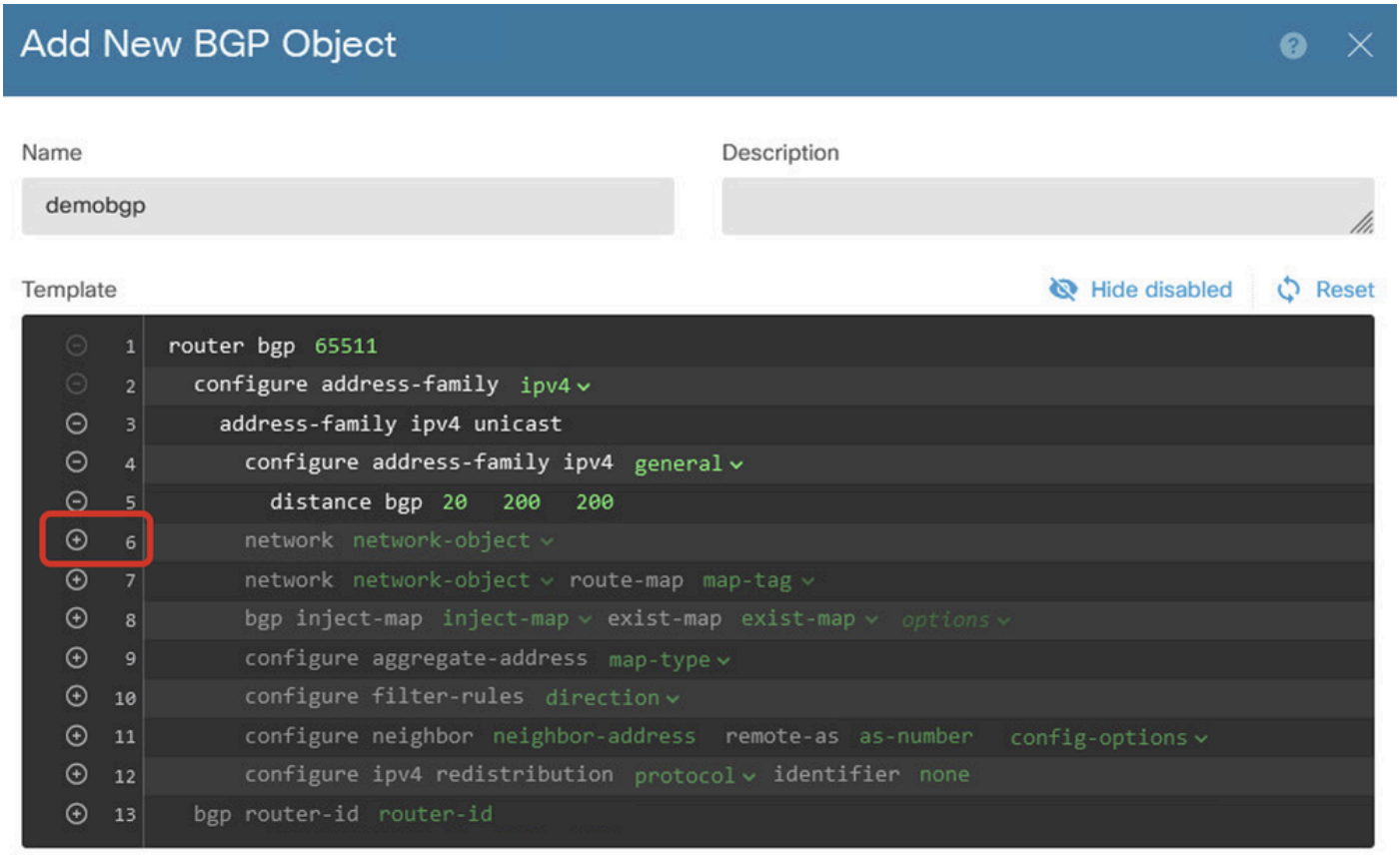
Create_BGP_Object_ASNumber_Protocol

第 4 行:配置更多设置。单击settings，选择general，然后单击Show disabled。

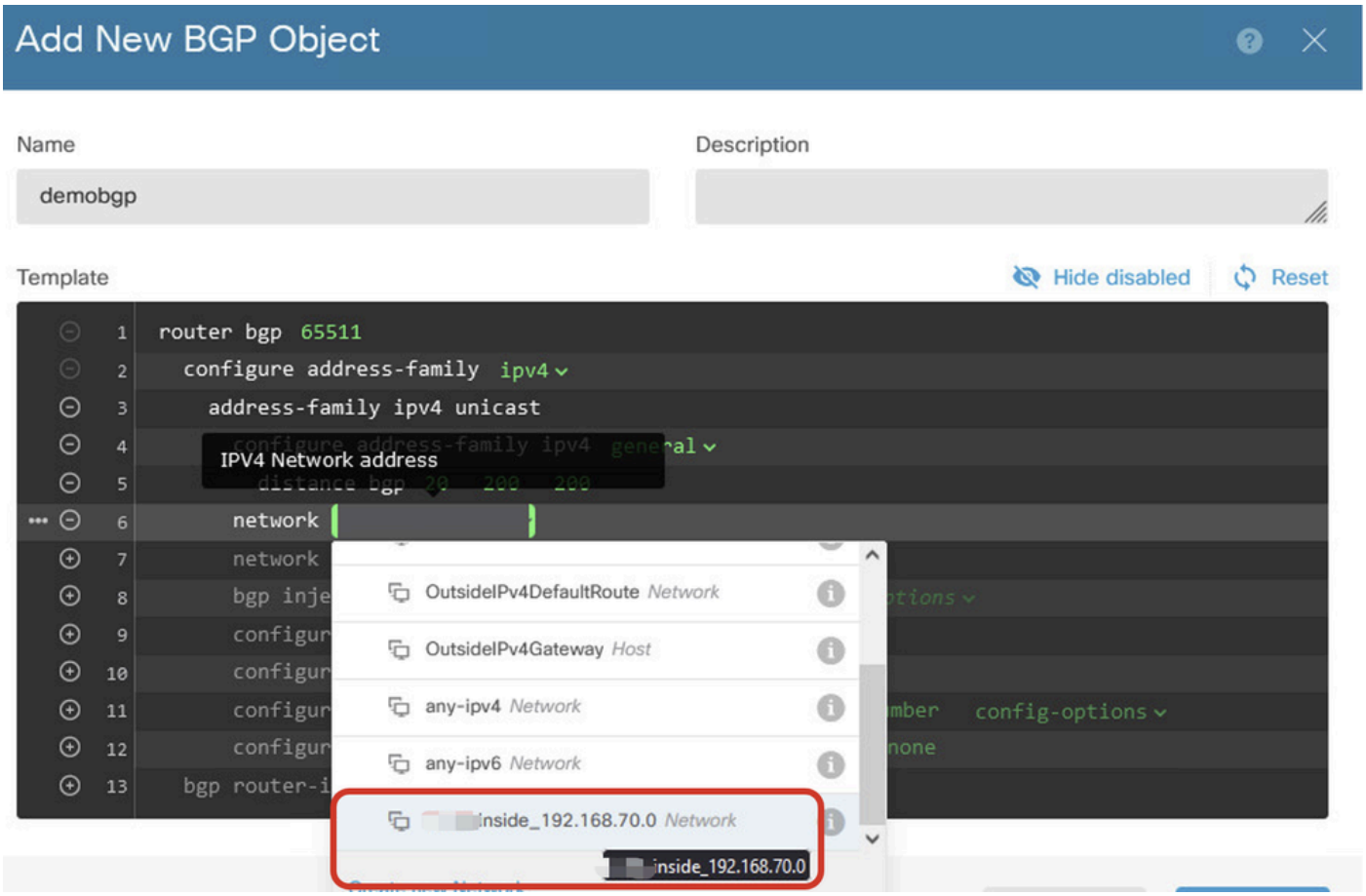


Create_BGP_Object_AddressSetting

第 6 行:单击+图标以启用线路来配置BGP网络。单击network-object。您可以查看现有可用对象并选择一个。在本示例中，选择对象name inside_192.168.70.0（在步骤3.2中创建）。

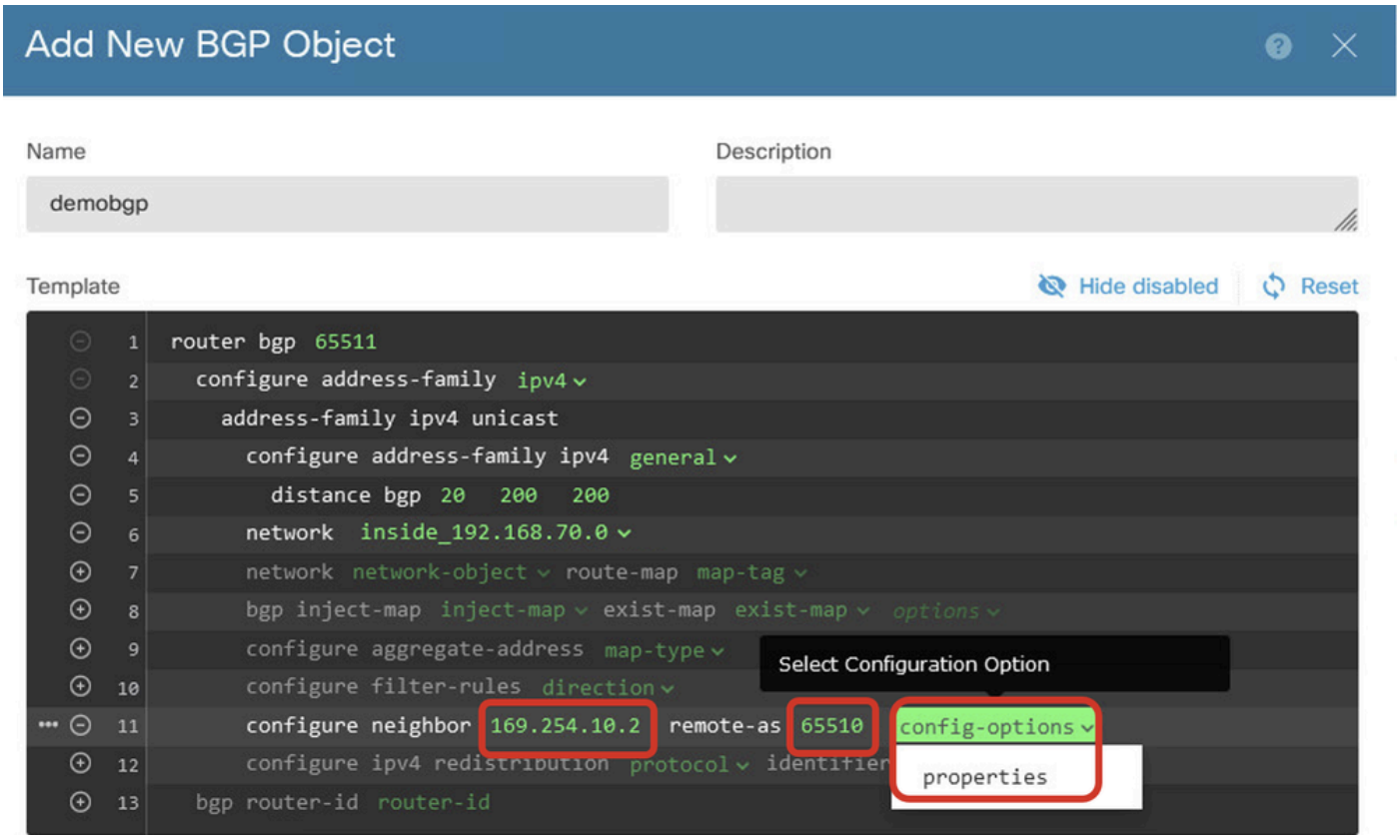


Create_BGP_Object_Add_Network



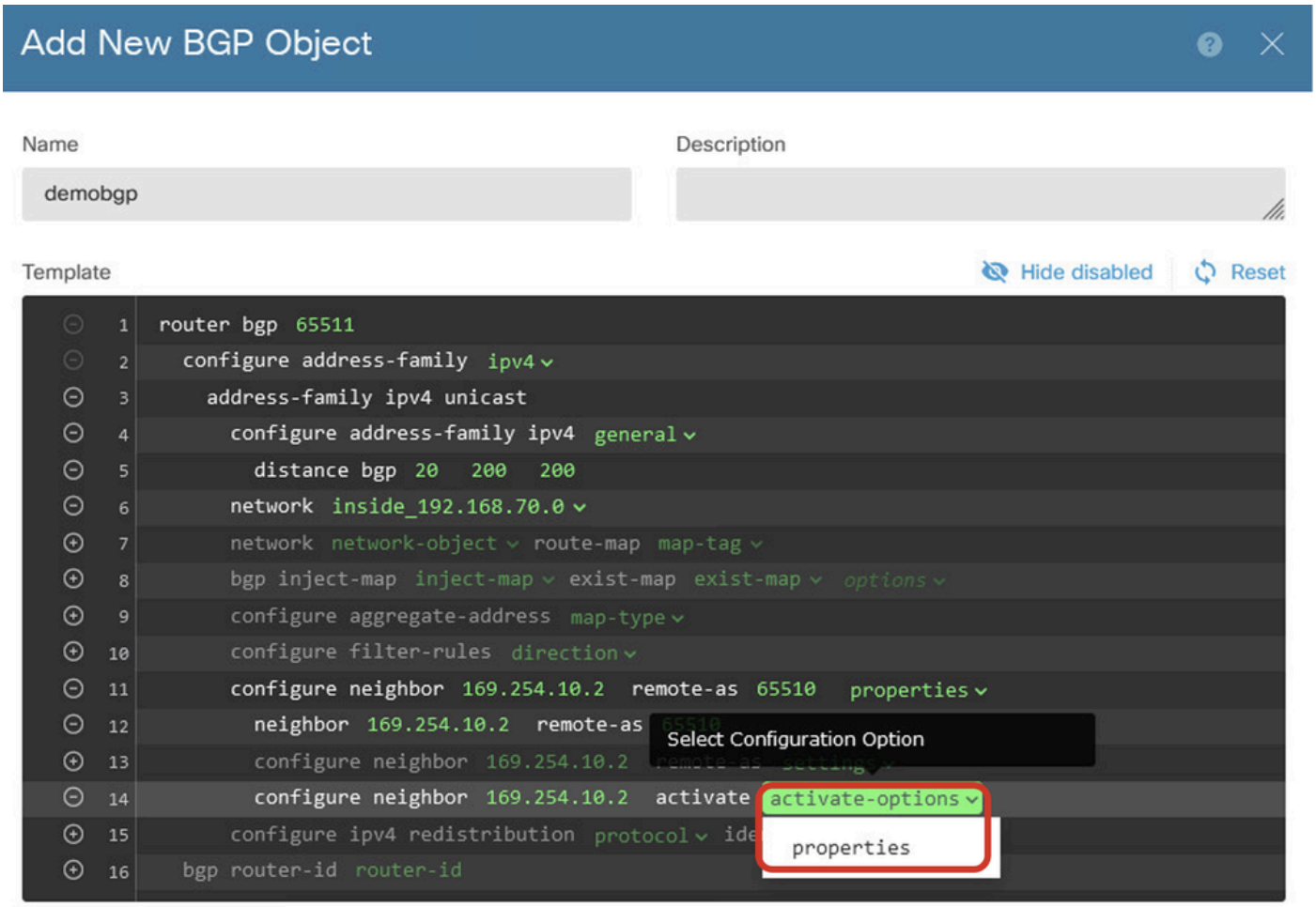
Create_BGP_Object_Add_Network2

第 11 行:单击+图标可启用线路以配置BGP邻居相关信息。单击neighbor-address，并手动输入peerBGPneighboraddress。在本例中，它是169.254.10.2（Site2 FTD的VTI IP地址）。 单击as-number，然后手动输入对等体AS编号。在本示例中，65510用于Site2 FTD。单击config-options并选择properties。



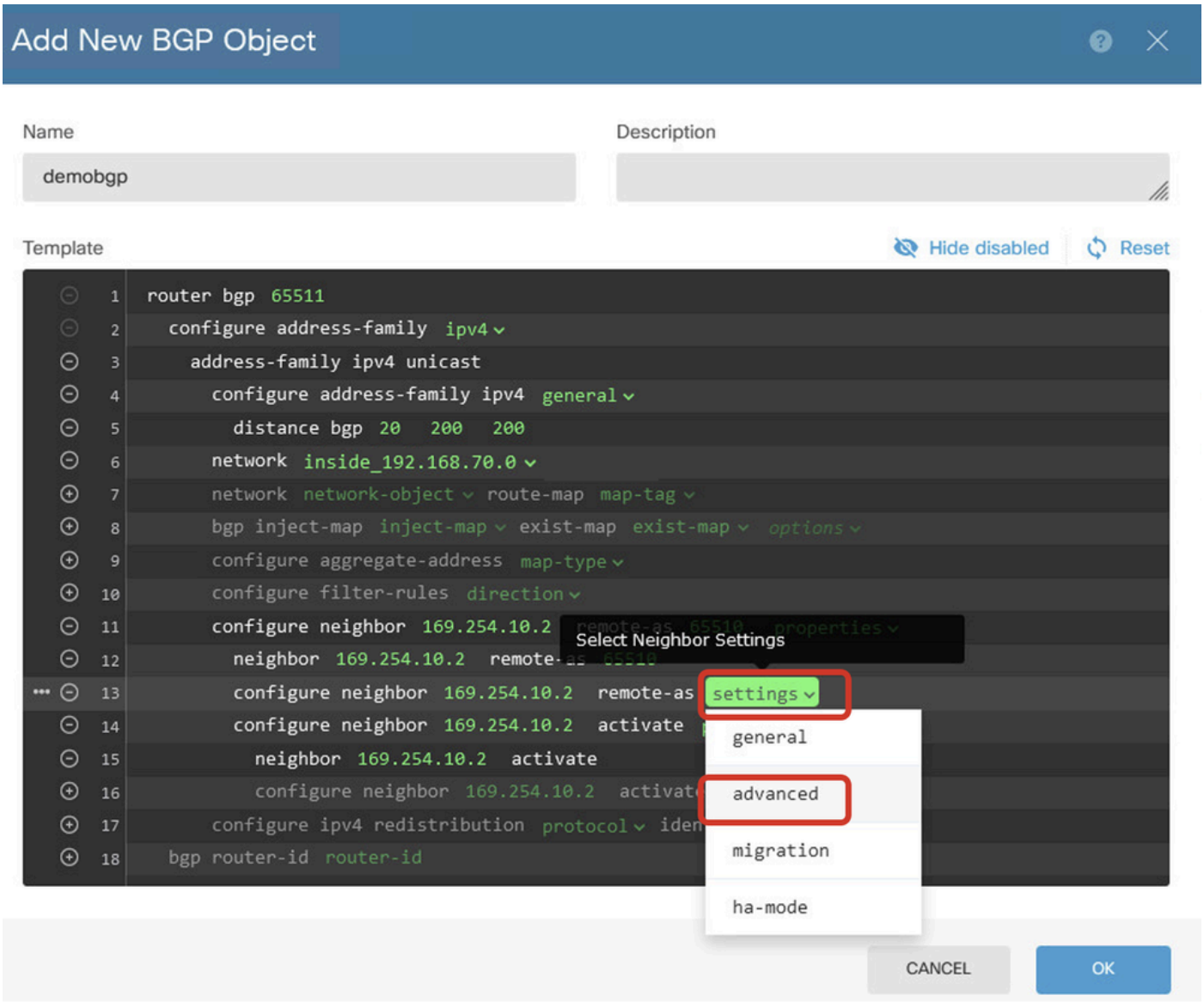
Create_BGP_Object_NeighborSetting

第 14 行:单击+图标，使线路能够配置邻居的某些属性。单击activate-options并选择properties。



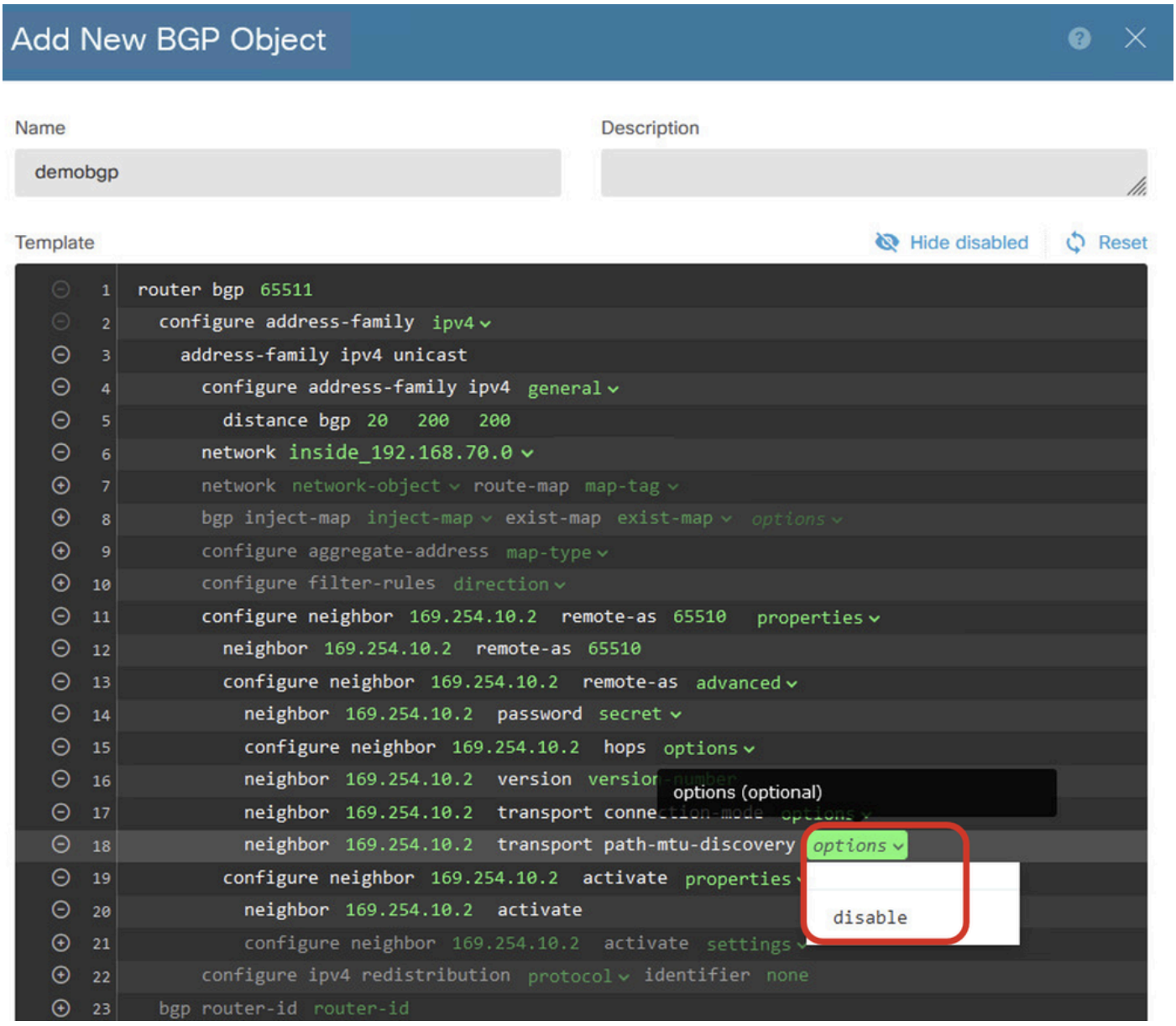
Create_BGP_Object_NeighborSetting_Properties

第 13 行:单击+图标可让行显示高级选项。单击settings并选择advanced。



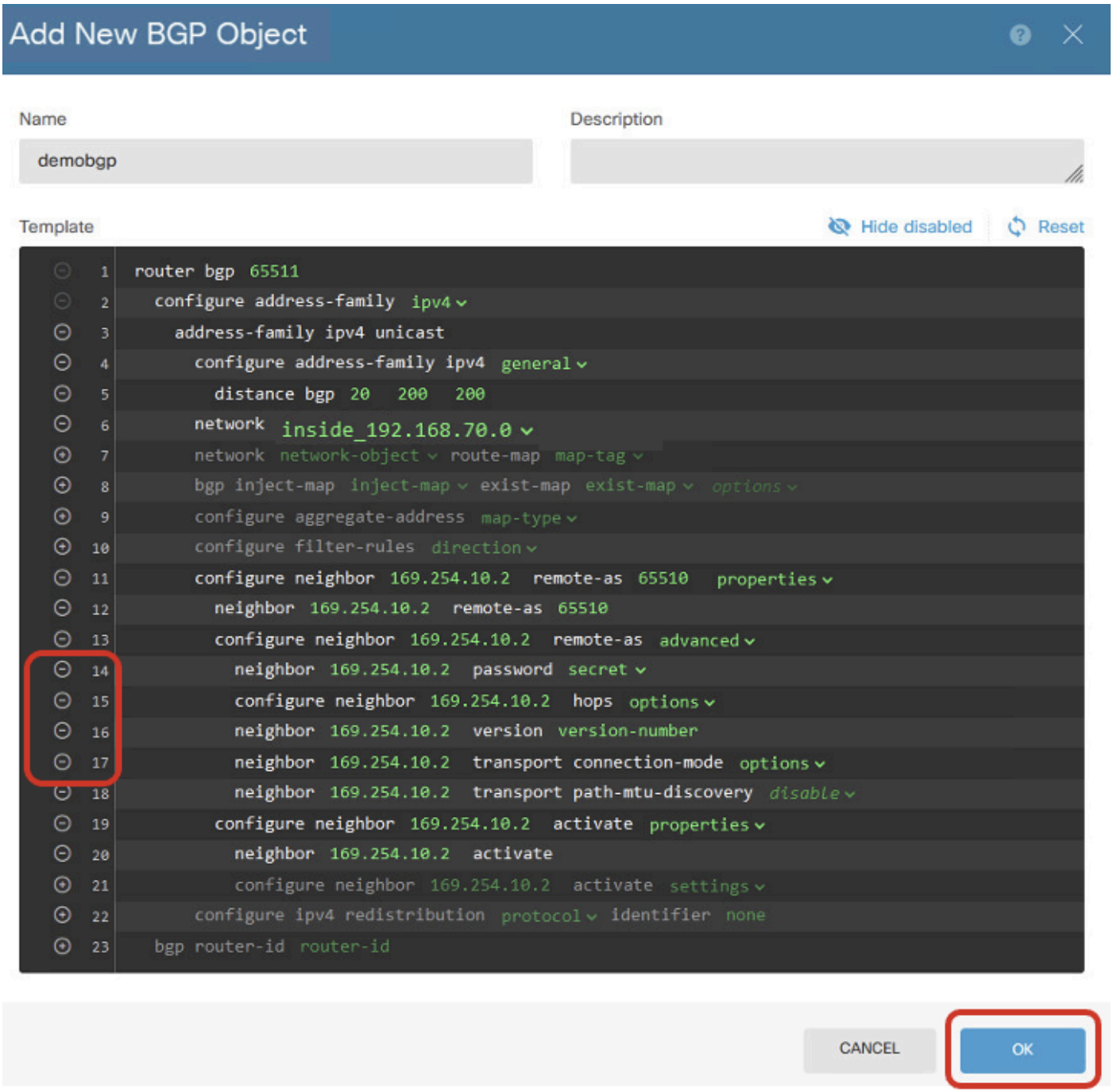
Create_BGP_Object_NeighborSetting_Properties_Advanced

第 18 行:单击options并选择disable以禁用路径MTU发现。



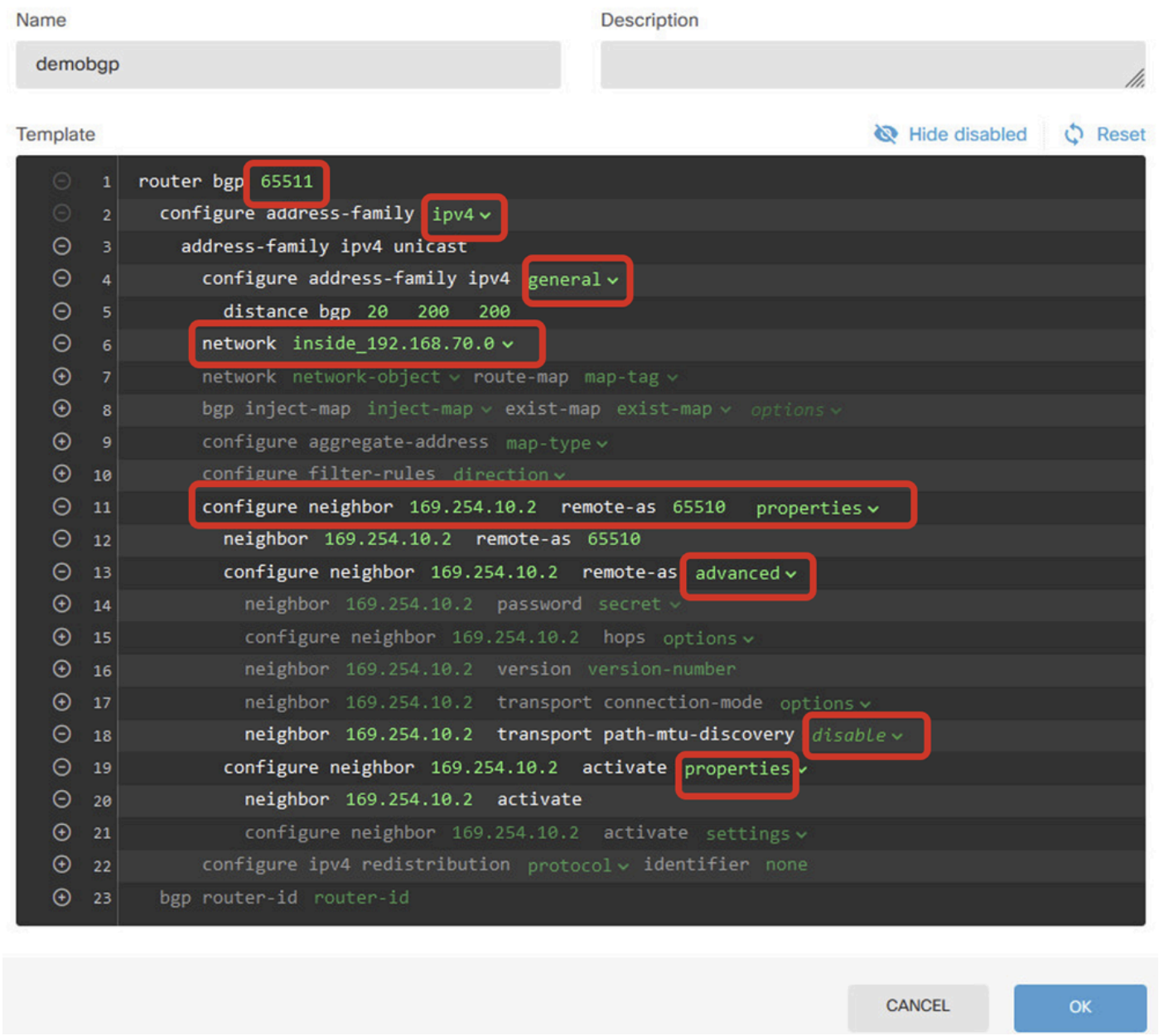
Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

线路14、15、16、17:单击-按钮以禁用这些行。然后，单击OK按钮保存BGP对象。



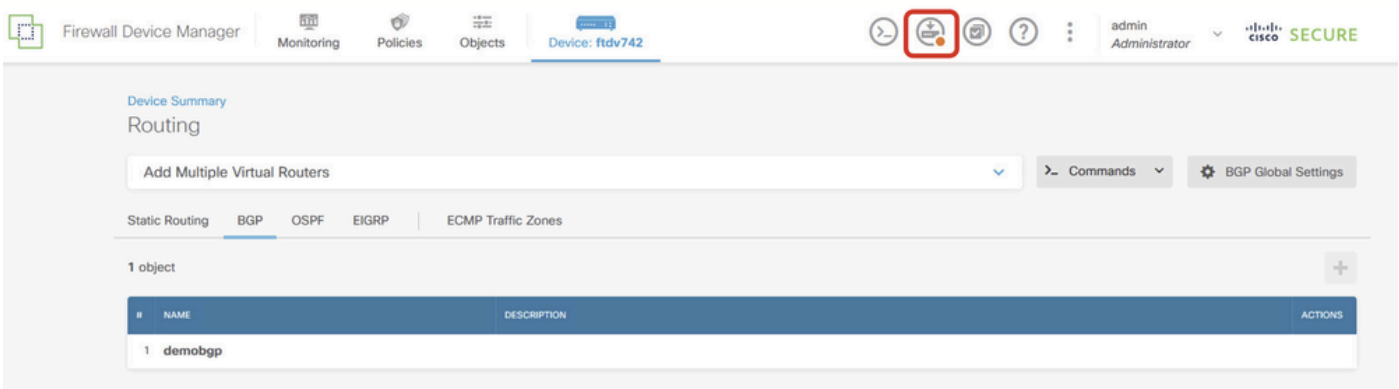
Create_BGP_Object_DisableLine

本示例概述了BGP设置。您可以根据实际需求配置其他BGP设置。



Create_BGP_Object_Final_Overview

步骤7.部署BGP配置更改。



部署_BGP_配置

步骤8.现在，Site1 FTD的配置已完成。

要配置Site2 FTD VPN和BGP，请使用相应的Site2 FTD参数重复步骤3.到步骤7.。

Site1 FTD和Site2 FTD在CLI中的配置概述。

站点1 FTD	站点2 FTD
NGFW版本7.4.2 interface GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag 策略静态sgt已禁用，受信任 安全级别0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside 安全级别0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 隧道源接口外部 隧道目标192.168.10.1 隧道模式IPSec IPv4 隧道保护ipsec profile ipsec_profile|e4084d322d 对象网络外部IPv4网关 host 192.168.30.3 object network inside_192.168.70.0 子网192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457:L5规则：Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id	NGFW版本7.4.2 interface GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag 策略静态sgt已禁用，受信任 安全级别0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside 安全级别0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 隧道源接口外部 隧道目标192.168.30.1 隧道模式IPSec IPv4 隧道保护ipsec profile ipsec_profile|e4084d322d 对象网络外部IPv4网关 host 192.168.10.3 object network inside_192.168.50.0 子网192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457:L5规则：Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id

268435458:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:L5规则：Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1:L5规则：DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1 router bgp 65511 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 169.254.10.2 remote-as 65510 neighbor 169.254.10.2 transport path-mtu-discovery disable 邻居169.254.10.2激活 network 192.168.70.0 no auto-summary 无同步 exit-address-family outside 0.0.0.0 0.0.0.0 192.168.30.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 protocol esp encryption aes-256 aes protocol esp integrity sha-256 sha-1 crypto ipsec profile ipsec_profile|e4084d322d set ikev2 ipsec-proposal AES256_SHA256 set security-association lifetime kilobytes 4608000 set security-association lifetime seconds 28800 crypto ipsec security-association pmtu-aging infinite crypto ikev2 policy 1 加密aes-256 aes integrity sha256 sha 第 14 组 prf sha256 sha lifetime seconds 86400 crypto ikev2 policy 20 加密aes-256 aes-192 aes	268435458:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:L5规则：Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1:访问策略:NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1:L5规则：DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1 router bgp 65510 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 169.254.10.1 remote-as 65511 neighbor 169.254.10.1 transport path-mtu-discovery disable 邻居169.254.10.1激活 network 192.168.50.0 no auto-summary 无同步 exit-address-family outside 0.0.0.0 0.0.0.0 192.168.10.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 protocol esp encryption aes-256 aes protocol esp integrity sha-256 sha-1 crypto ipsec profile ipsec_profile|e4084d322d set ikev2 ipsec-proposal AES256_SHA256 set security-association lifetime kilobytes 4608000 set security-association lifetime seconds 28800 crypto ipsec security-association pmtu-aging infinite crypto ikev2 policy 1 加密aes-256 aes integrity sha256 sha 第 14 组 prf sha256 sha lifetime seconds 86400 crypto ikev2 policy 20 加密aes-256 aes-192 aes

integrity sha512 sha384 sha256 sha 21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside 组策略 |s2sGP|192.168.10.1内部 组策略 |s2sGP|192.168.10.1属性 vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l 隧道组192.168.10.1常规属性 default-group-policy |s2sGP|192.168.10.1 tunnel-group 192.168.10.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****	integrity sha512 sha384 sha256 sha 21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside 组策略 |s2sGP|192.168.30.1内部 组策略 |s2sGP|192.168.30.1属性 vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l 隧道组192.168.30.1常规属性 default-group-policy |s2sGP|192.168.30.1 tunnel-group 192.168.30.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****

验证

使用本部分可确认配置能否正常运行。

步骤1.通过控制台或SSH导航到每个FTD的CLI，以便通过show crypto ikev2 sa和show crypto ipsec sa命令验证第1阶段和第2阶段的VPN状态。

站点1 FTD	站点2 FTD
ftdv742# show crypto ikev2 sa IKEv2 SA: Session-id:134, Status:UP-ACTIVE， IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status Role 563984431 192.168.30.1/500 192.168.10.1/500全球/全球就绪型响应器 加密：AES-CBC，密钥大小：256，哈希：SHA256,DH组：14，身份验证符号：PSK，身份验证验证：PSK 寿命/活动时间：86400/5145 秒 子sa:本地选择器0.0.0.0/0 -	ftdv742# show crypto ikev2 sa IKEv2 SA: Session-id:13, Status:UP-ACTIVE， IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status Role 339797985 192.168.10.1/500 192.168.30.1/500全局/全局就绪启动器 加密：AES-CBC，密钥大小：256，哈希：SHA256,DH组：14，身份验证符号：PSK，身份验证验证：PSK 寿命/活动时间：86400/74099 秒 子sa:本地选择器0.0.0.0/0 - 255.255.255.255/65535 远程选择器0.0.0.0/0 - 255.255.255.255/65535 ESP spi输入/输出：0xb7b5b38b/0xf0c4239d

255.255.255.255/65535 远程选择器0.0.0.0/0 - 255.255.255.255/65535 ESP spi输入/输出：0xf0c4239d/0xb7b5b38b	
ftdv742# show crypto ipsec sa 接口:demovti 加密映射标记：__vti-crypto-map-Tunnel1-0-1, seq num:65280，本地地址：192.168.30.1 受保护的VRF(IVRF):全局 本地 ident(addr/mask/prot/port):(0.0.0.0/0.0.0.0/0/0） 远程 ident(addr/mask/prot/port):(0.0.0.0/0.0.0.0/0/0） current_peer:192.168.10.1 #pkts封装：5720,#pkts encrypt:5720,#pkts摘要：5720 #pkts decap:5717,#pkts解密：5717,#pkts验证：5717 #pkts压缩：0，已#pkts压缩：0 #pkts未压缩：5720,#pkts成失败：0,#pkts解失败：0 #pre-frag成功：0,#pre-frag故障：0，已 #fragments建：0 #PMTUs发送：0,#PMTUs rcvd:0，需 #decapsulated重组的frg:0 #TFC rcvd:0，已#TFC送：0 #Valid ICMP错误rcvd:0,#Invalid ICMP错误rcvd:0 #send错误：0,#recv错：0 本地加密端点：192.168.30.1/500，远程加密端点：192.168.10.1/500 路径mtu 1500、ipsec开销78(44)、媒体mtu 1500 PMTU剩余时间（秒）：0,DF策略：copy-df ICMP错误验证：已禁用，TFC数据包：禁用 当前出站spi:B7B5B38B 当前入站spi:F0C4239D 入站esp sas: spi:0xF0C4239D(4039386013) SA状态：主用 转型:esp-aes-256 esp-sha-256-hmac无压缩 使用中的设置={L2L，隧道，IKEv2,VTI， }	ftdv742# show crypto ipsec sa 接口:demovti25 加密映射标记：__vti-crypto-map-Tunnel1-0-1, seq num:65280，本地地址：192.168.10.1 受保护的VRF(IVRF):全局 本地 ident(addr/mask/prot/port):(0.0.0.0/0.0.0.0/0/0） 远程 ident(addr/mask/prot/port):(0.0.0.0/0.0.0.0/0/0） current_peer:192.168.30.1 #pkts封装：5721,#pkts encrypt:5721,#pkts文摘：5721 #pkts decap:5721,#pkts解：5721,#pkts验证：5721 #pkts压缩：0，已#pkts压缩：0 #pkts未压缩：5721,#pkts组件失败：0,#pkts解失败：0 #pre-frag成功：0,#pre-frag故障：0，已 #fragments建：0 #PMTUs发送：0,#PMTUs rcvd:0，需 #decapsulated重组的frg:0 #TFC rcvd:0，已#TFC送：0 #Valid ICMP错误rcvd:0,#Invalid ICMP错误rcvd:0 #send错误：0,#recv错：0 本地加密端点：192.168.10.1/500，远程加密端点：192.168.30.1/500 路径mtu 1500、ipsec开销78(44)、媒体mtu 1500 PMTU剩余时间（秒）：0,DF策略：copy-df ICMP错误验证：已禁用，TFC数据包：禁用 当前出站spi:F0C4239D 当前入站spi:B7B5B38B 入站esp sas: spi:0xB7B5B38B(3082138507) SA状态：主用 转型:esp-aes-256 esp-sha-256-hmac无压缩 使用中的设置={L2L，隧道，IKEv2,VTI， }

插槽:0,conn_id:266，加密映射：__vti-crypto-map-Tunnel1-0-1 sa计时：剩余密钥生存时间（千字节/秒）：(4285389/3722） IV大小：16 bytes 重播检测支持：Y 反重播位图： 0xFFFFFFFF 0xFFFFFFFF 出站esp sas: spi:0xB7B5B38B(3082138507) SA状态：主用 转型:esp-aes-256 esp-sha-256-hmac无压缩 使用中的设置={L2L，隧道，IKEv2,VTI，} 插槽:0,conn_id:266，加密映射：__vti-crypto-map-Tunnel1-0-1 sa计时：剩余密钥生存时间（千字节/秒）：(4147149/3722） IV大小：16 bytes 重播检测支持：Y 反重播位图： 0x00000000 0x00000001	插槽:0,conn_id:160，加密映射：__vti-crypto-map-Tunnel1-0-1 sa计时：剩余密钥生存时间（千字节/秒）：(3962829/3626） IV大小：16 bytes 重播检测支持：Y 反重播位图： 0xFFFFFFFF 0xFFFFFFFF 出站esp sas: spi:0xF0C4239D(4039386013) SA状态：主用 转型:esp-aes-256 esp-sha-256-hmac无压缩 使用中的设置={L2L，隧道，IKEv2,VTI，} 插槽:0,conn_id:160，加密映射：__vti-crypto-map-Tunnel1-0-1 sa计时：剩余密钥生存时间（千字节/秒）：(4101069/3626） IV大小：16 bytes 重播检测支持：Y 反重播位图： 0x00000000 0x00000001

步骤2.通过控制台或SSH导航到每个FTD的CLI，以便使用show bgp neighbors和show route bgp命令验证BGP状态。

站点1 FTD	站点2 FTD
ftdv742# show bgp neighbors BGP邻居为169.254.10.2,vrf single_vf，远程AS 65510，外部链路 BGP版本4，远程路由器ID 192.168.50.1 BGP状态=已建立，持续1d20h 上次读取00:00:25，上次写入00:00:45，保持时间为180，保持连接间隔为60秒 邻居会话： 1个活动，不支持多会话（禁用） 邻居功能： 路由刷新：通告和接收（新） 四组二进制八位数的ASN功能：通告和接收 地址系列IPv4单播：通告和接收 多会话功能： 消息统计信息： InQ深度为0 OutQ深度为0	ftdv742# show bgp neighbors BGP邻居为169.254.10.1,vrf single_vf，远程AS 65511，外部链路 BGP版本4，远程路由器ID 192.168.70.1 BGP状态=已建立，持续1d20h 上次读取00:00:11，上次写入00:00:52，保持时间为180，保持连接间隔为60秒 邻居会话： 1个活动，不支持多会话（禁用） 邻居功能： 路由刷新：通告和接收（新） 四组二进制八位数的ASN功能：通告和接收 地址系列IPv4单播：通告和接收 多会话功能： 消息统计信息： InQ深度为0 OutQ深度为0

发送的Rcvd 打开： 1 1 通知：0 0 更新：2 2 保持连接：2423 2427 路由刷新：0 0 总数:2426 2430 通告运行之间的默认最短时间为30秒 对于地址系列：IPv4单播 会话：169.254.10.2 BGP表版本3，邻居版本3/0 输出队列大小：0 索引1 1个更新组成员 发送的Rcvd 前缀活动：---- ---- 当前前缀：1 1（消耗80字节） 前缀总数：1 1 隐式撤消：0 0 显式撤消：0 0 用作最佳路径：不适用1 用作多路径：不适用0 出站入站 本地策略拒绝的前缀：-------- ------- 来自此对等体的最佳路径：1不适用 总数:1 0 发送的更新中的NLRI数：最大1，最小0 地址跟踪已启用，RIB确实有到169.254.10.2的路由 已建立连接1;已丢弃0 上次重置从不 Transport(tcp)path-mtu-discovery is disabled Graceful-Restart已禁用	发送的Rcvd 打开：1 1 通知：0 0 更新：2 2 保持连接：2424 2421 路由刷新：0 0 总数:2427 2424 通告运行之间的默认最短时间为30秒 对于地址系列：IPv4单播 会话：169.254.10.1 BGP表版本9，邻居版本9/0 输出队列大小：0 索引4 4个更新组成员 发送的Rcvd 前缀活动：---- ---- 当前前缀：1 1（消耗80字节） 前缀总数：1 1 隐式撤消：0 0 显式撤消：0 0 用作最佳路径：不适用1 用作多路径：不适用0 出站入站 本地策略拒绝的前缀：-------- ------- 来自此对等体的最佳路径：1不适用 总数:1 0 发送的更新中的NLRI数：最大1，最小0 启用地址跟踪，RIB确实有到169.254.10.1的路由 建立连接4;丢弃3 上次重置1d21h，由于会话1的接口抖动 Transport(tcp)path-mtu-discovery is disabled Graceful-Restart已禁用
ftdv742# show route bgp 代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，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外部类型1、E2 - OSPF外部类型2、V	ftdv742# show route bgp 代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，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外部类型1、E2 - OSPF外部类型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 — 定期下载的静态路由，+ — 复制路由 SI — 静态InterVRF、BI - BGP InterVRF Gateway of last resort is 192.168.30.3 to network 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0]（通过169.254.10.2,1d20h）	- 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 — 定期下载的静态路由，+ — 复制路由 SI — 静态InterVRF、BI - BGP InterVRF Gateway of last resort is 192.168.10.3 to network 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0]（通过169.254.10.1,1d20h）

步骤3. Site1客户端和Site2客户端成功彼此ping通。

站点1客户端：

```
Site1_Client#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 = 31/56/90 ms
```

Site2客户端：

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

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BGP部分进行故障排除。

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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）。