# 在FDM管理的FTD上配置基于路由的VPN上的BGP

## 目录

## 简介

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

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- VPN基本知识
- FTDv上的BGP配置
- 使用FDM的经验

### 使用的组件

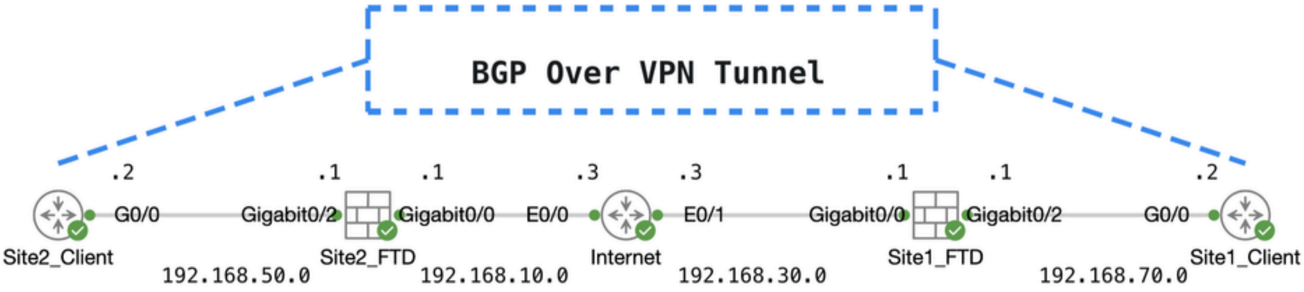
本文档中的信息基于以下软件和硬件版本：

- 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



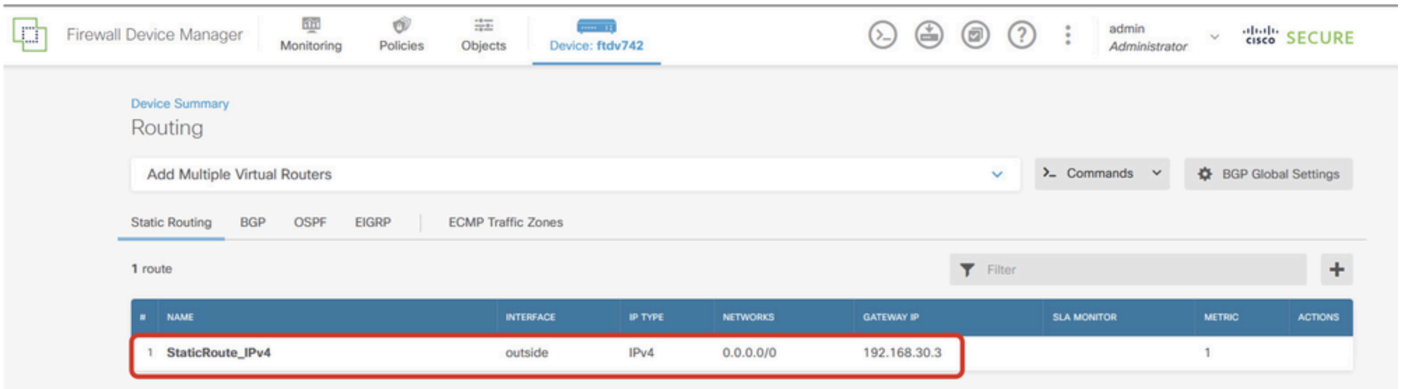
Topo

## VPN上的配置

步骤1:确保节点之间的IP互联准备就绪且稳定。FDM上的智能许可证成功注册到智能帐户。

第二步： Site1客户端的网关配置有Site1 FTD (192.168.70.1)的内部IP地址。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。

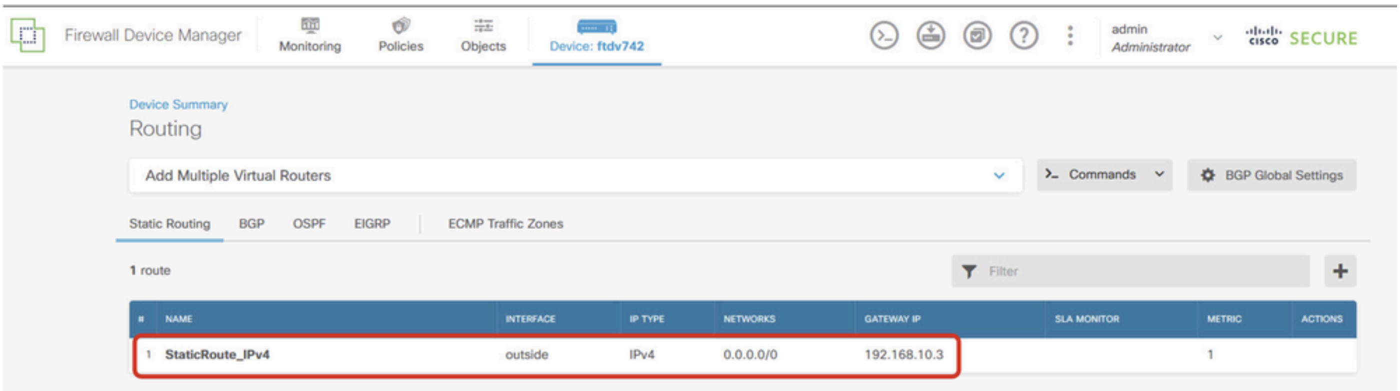
登录每个FDM的GUI。导航到Device > Routing。单击。View Configuration单击**Static Routing**选项卡以验证默认静态路由。



1 route

| # | NAME | INTERFACE | IP TYPE | NETWORKS | GATEWAY IP | SLA MONITOR | METRIC | ACTIONS |
|---|---|---|---|---|---|---|---|---|
| 1 | StaticRoute_IPv4 | outside | IPv4 | 0.0.0.0/0 | 192.168.30.3 |  | 1 |  |

站点1_FTD_网关



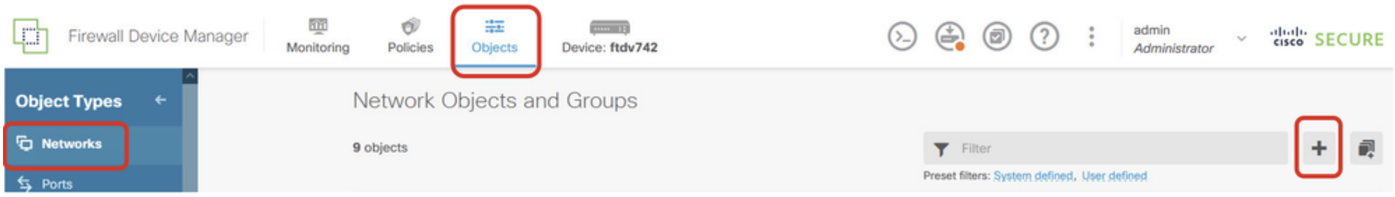
1 route

| # | NAME | INTERFACE | IP TYPE | NETWORKS | GATEWAY IP | SLA MONITOR | METRIC | ACTIONS |
|---|---|---|---|---|---|---|---|---|
| 1 | StaticRoute_IPv4 | outside | IPv4 | 0.0.0.0/0 | 192.168.10.3 |  | 1 |  |

站点2_FTD_网关

第三步：配置基于路由的站点到站点VPN。 在本示例中，首先配置Site1 FTD。

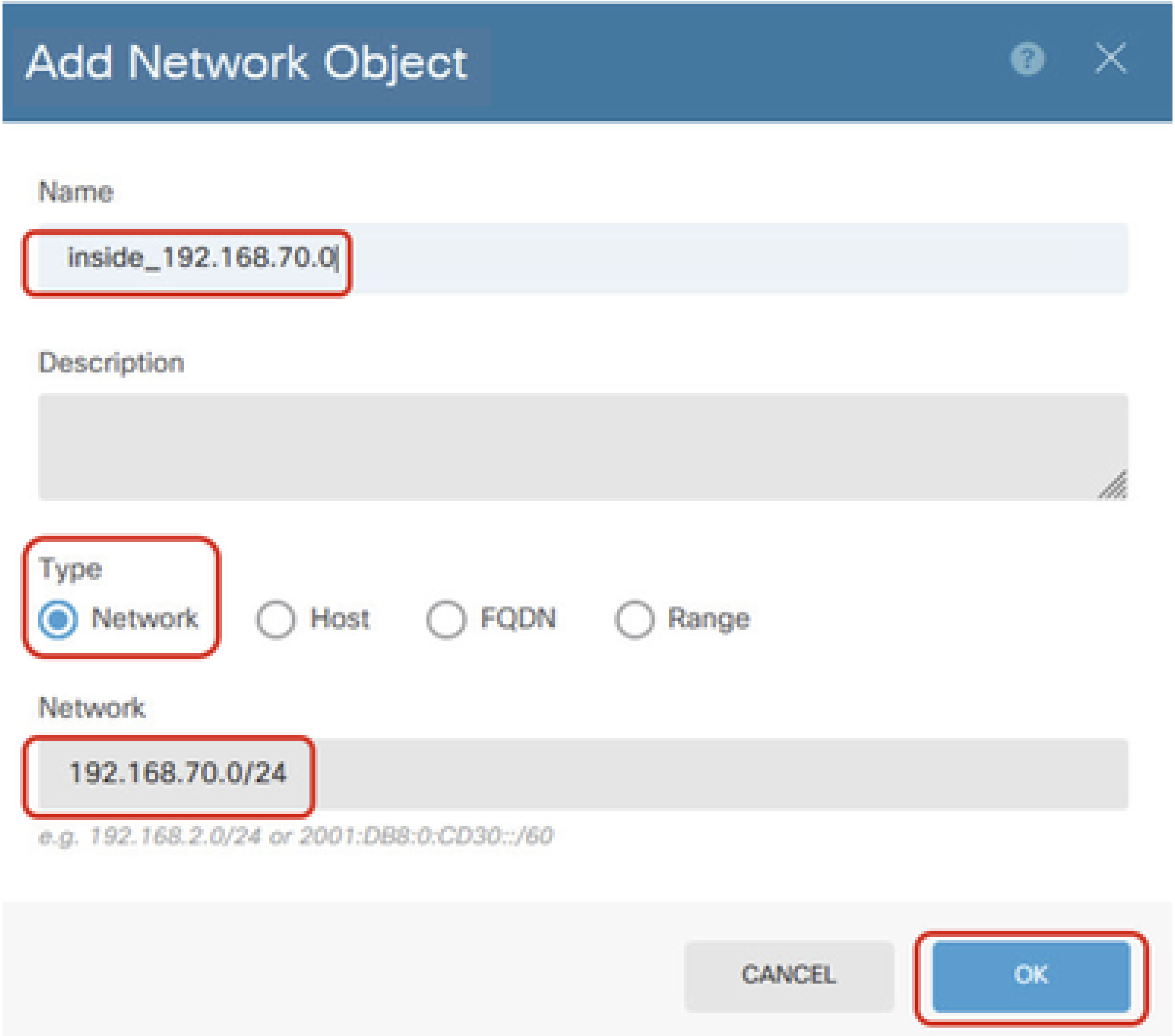
步骤 3.1 登录到Site1 FTD的FDM GUI。为Site1 FTD的内部网络创建新的网络对象。 导航至**Objects > Networks**，点击+按钮。



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
- 类型：网络
- 网络：192.168.70.0/24



Add Network Object

Name

inside_192.168.70.0

Description

Type

● Network ○ Host ○ FQDN ○ Range

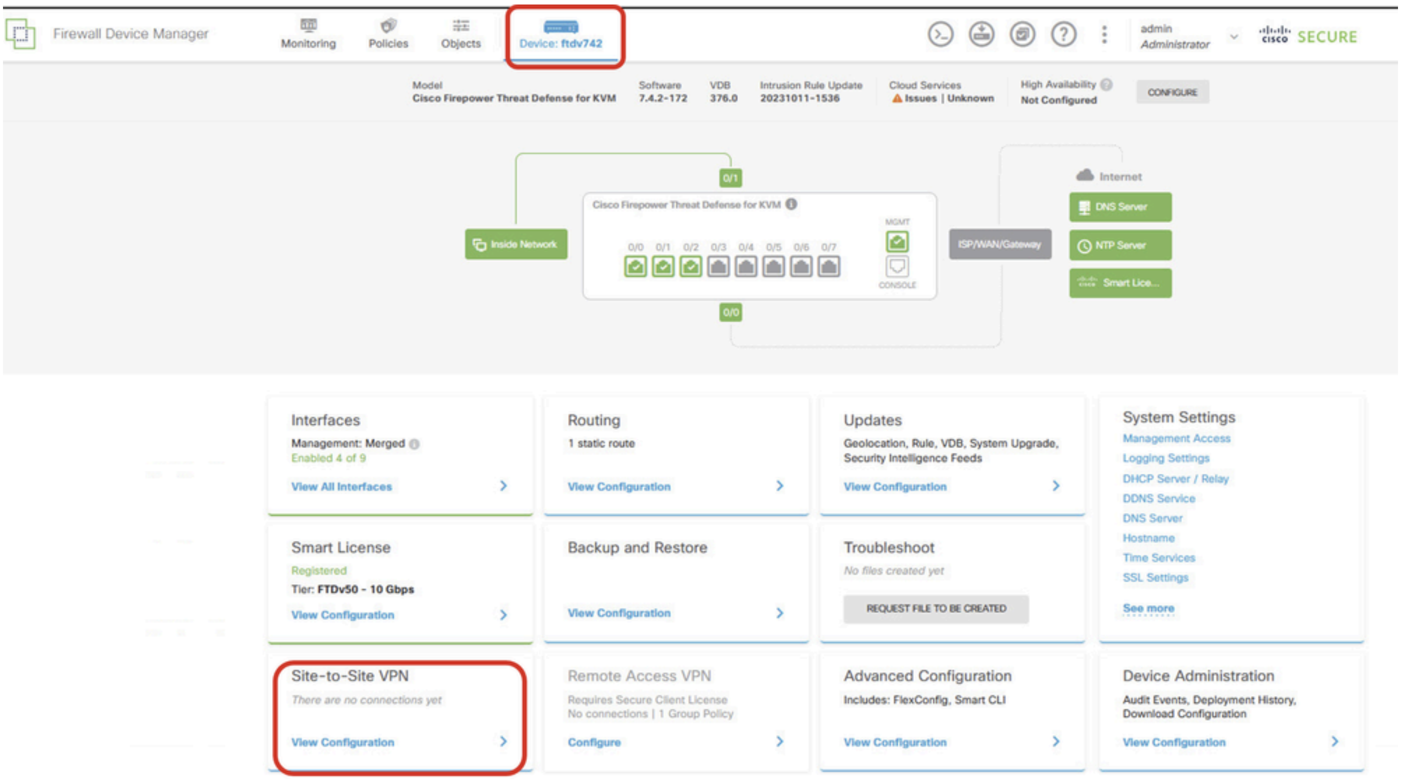
Network

192.168.70.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

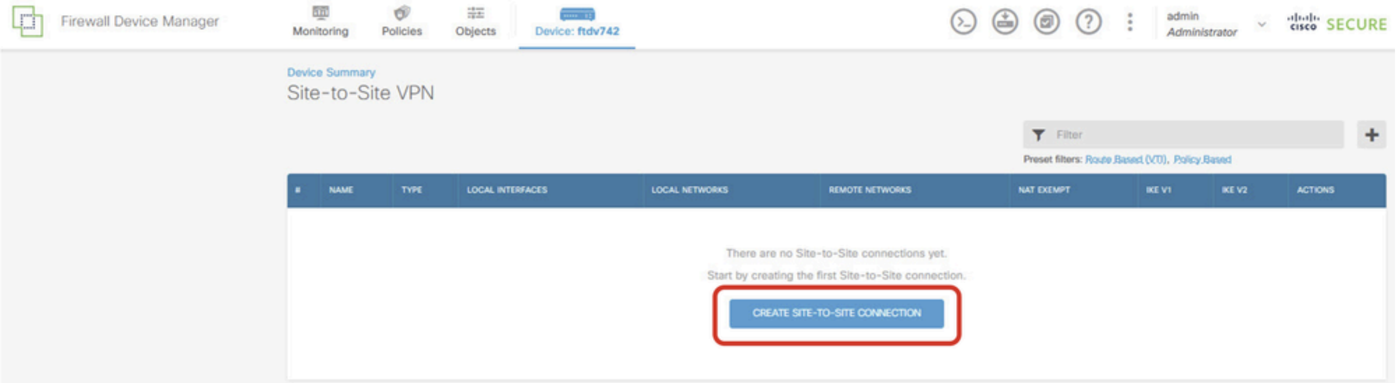
Site1_Inside_Network

步骤 3.3导航到**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**



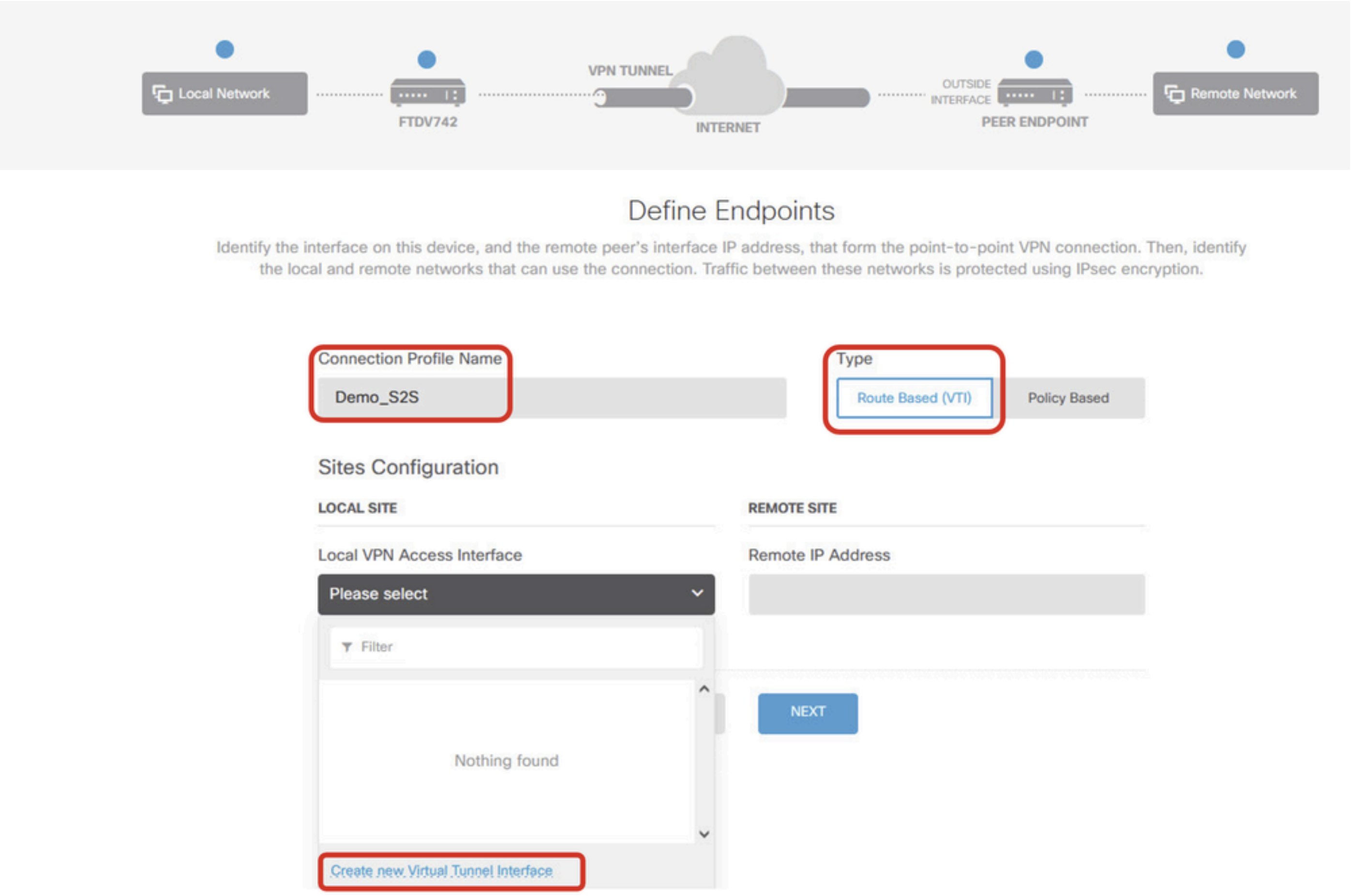
| # | NAME | TYPE | LOCAL INTERFACES | LOCAL NETWORKS | REMOTE NETWORKS | NAT EXEMPT | IKE V1 | IKE V2 | ACTIONS |
|---|---|---|---|---|---|---|---|---|---|

There are no Site-to-Site connections yet.
Start by creating the first Site-to-Site connection.

Create_Site-to-Site_Connection

步骤 3.5提供必要信息。

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



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Demo_S2S

Type: Route Based (VTI) | Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface: Please select

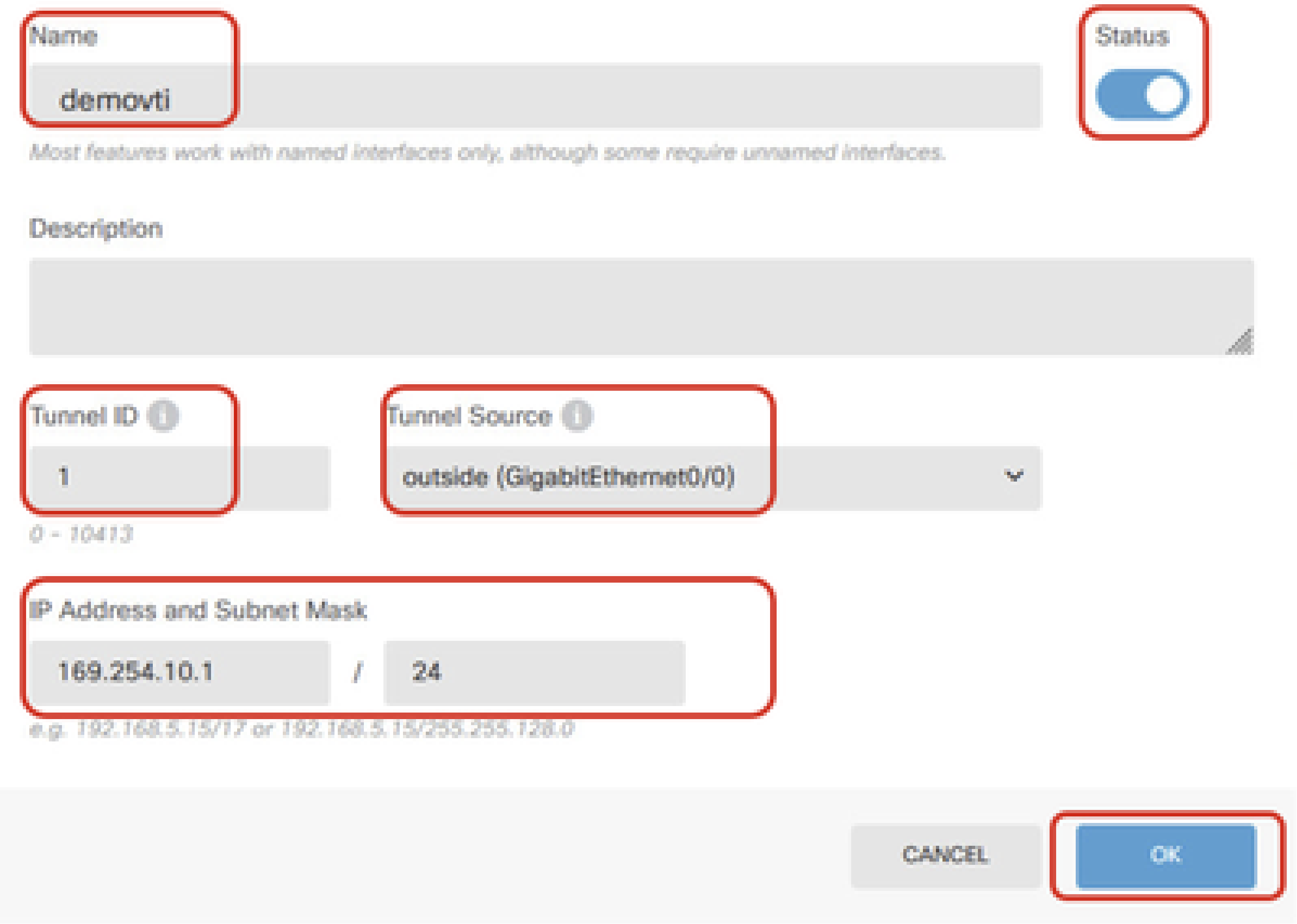
REMOTE SITE

Remote IP Address

Create_VTI_in_VPN_Wizard

步骤 3.6提供创建新VTI所需的信息。 单击 OK 按钮。

- 名称：demovti
- 隧道ID：1
- 隧道源：外部(GigabitEthernet0/0)
- IP地址和子网掩码：169.254.10.1/24
- 状态：点击滑块至“已启用”位置



Name

demovti

Most features work with named interfaces only, although some require unnamed interfaces.

Status

Description

Tunnel ID

1

0 - 10413

Tunnel Source

outside (GigabitEthernet0/0)

IP Address and Subnet Mask

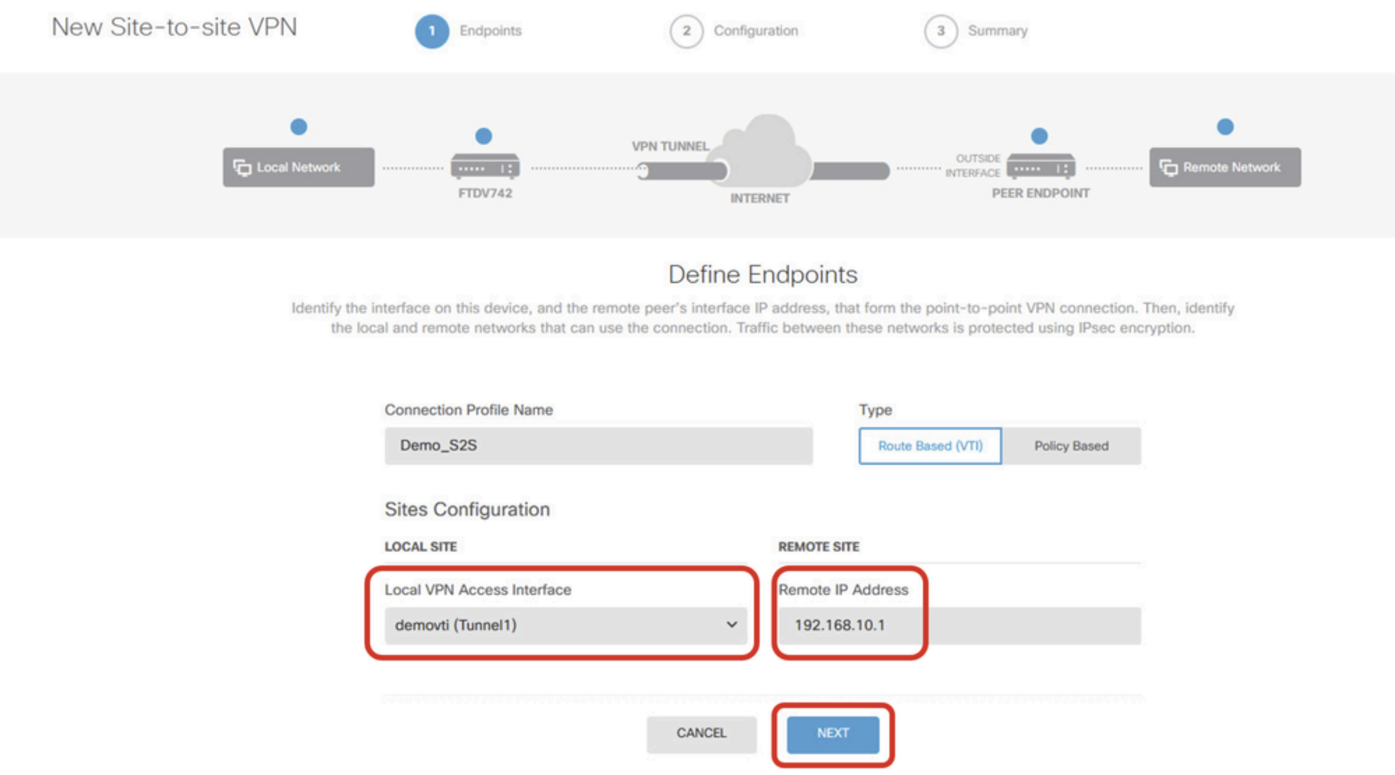
169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

创建_VTI_详细信息

步骤 3.7继续提供必要信息。 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



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Demo_S2S

Type: Route Based (VTI) | Policy Based

Sites Configuration

LOCAL SITE

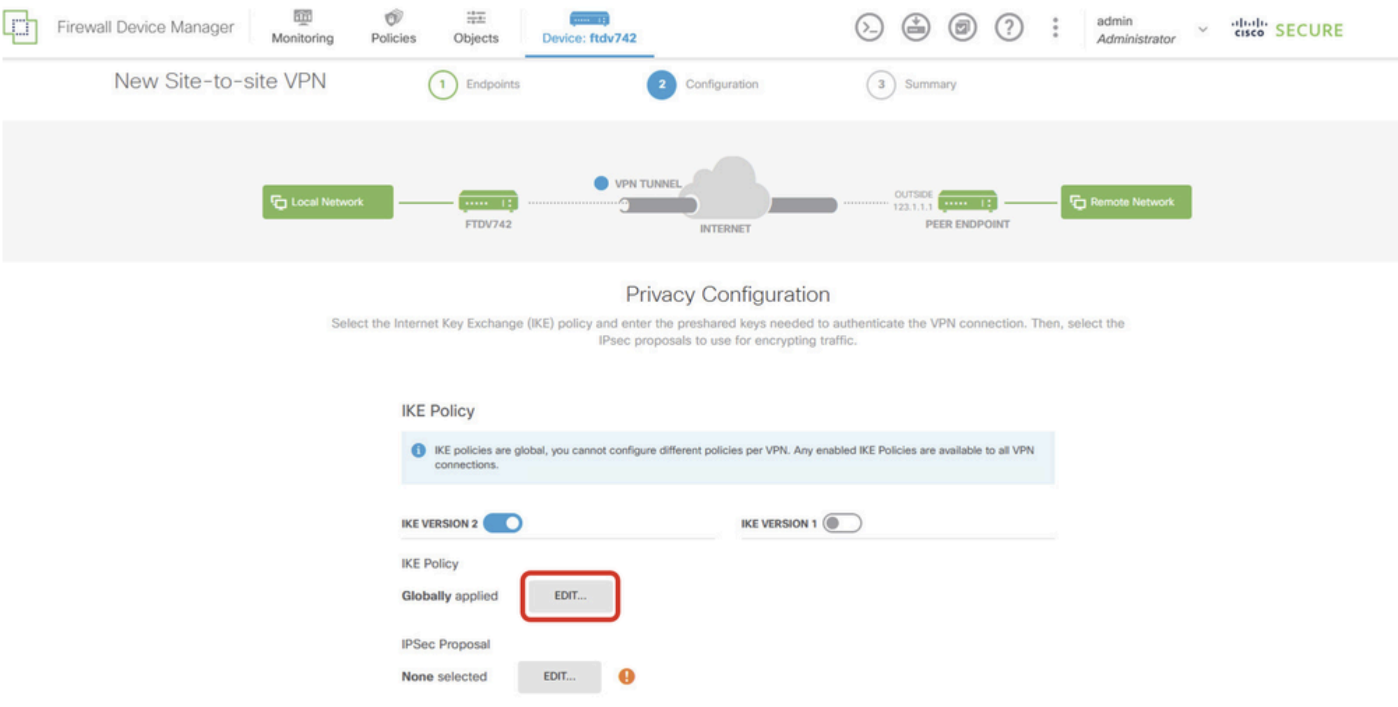
Local VPN Access Interface: demovti (Tunnel1)

REMOTE SITE

Remote IP Address: 192.168.10.1

VPN_Wizard_Endpoints_Step1

步骤 3.8导航至IKE Policy。单击 Edit 按钮。



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 (on) IKE VERSION 1 (off)

IKE Policy

Globally applied EDIT...

IPSec Proposal

None selected EDIT...

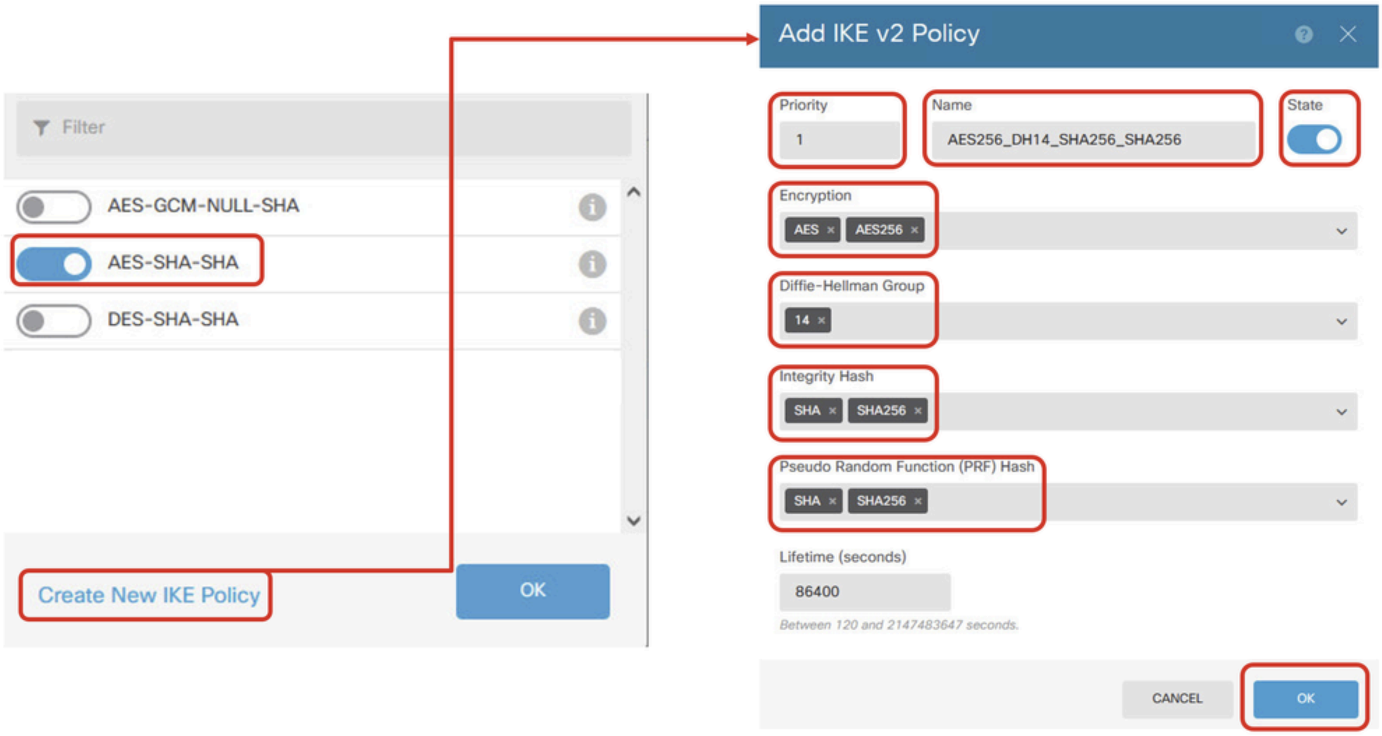
Edit_IKE_Policy

步骤 3.9 对于IKE策略，您可以使用预定义策略，也可以通过单击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按钮以保存

。

- 名称：AES256_DH14_SHA256_SHA256
- 加密：AES、AES256
- DH组：14
- 完整性哈希：SHA、SHA256
- PRF散列：SHA、SHA256
- 生存期：86400（默认值）



Priority: 1

Name: AES256_DH14_SHA256_SHA256

State: ●

Encryption: AES × AES256 ×

Diffie-Hellman Group: 14 ×

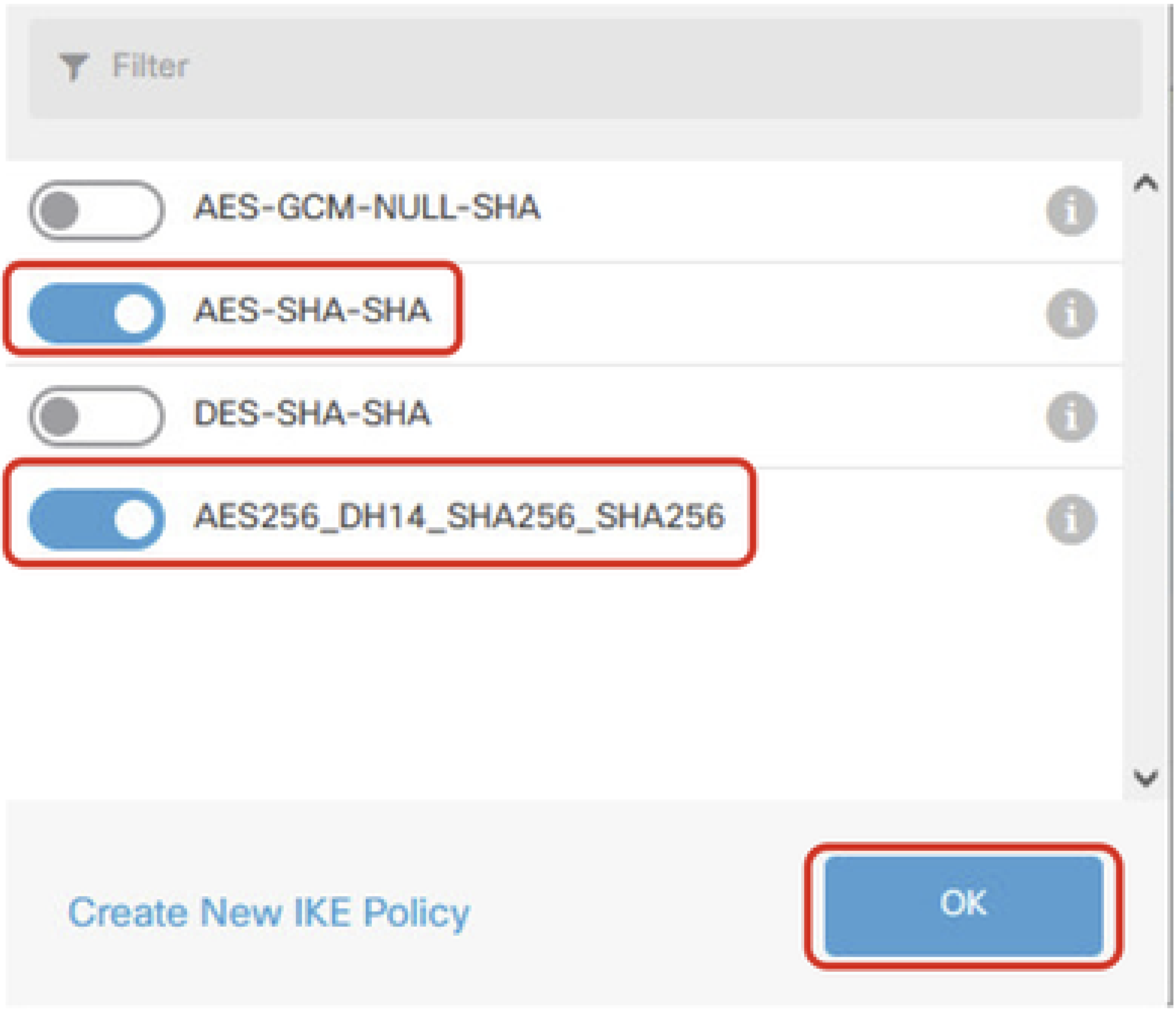
Integrity Hash: SHA × SHA256 ×

Pseudo Random Function (PRF) Hash: SHA × SHA256 ×

Lifetime (seconds): 86400

Between 120 and 2147483647 seconds.

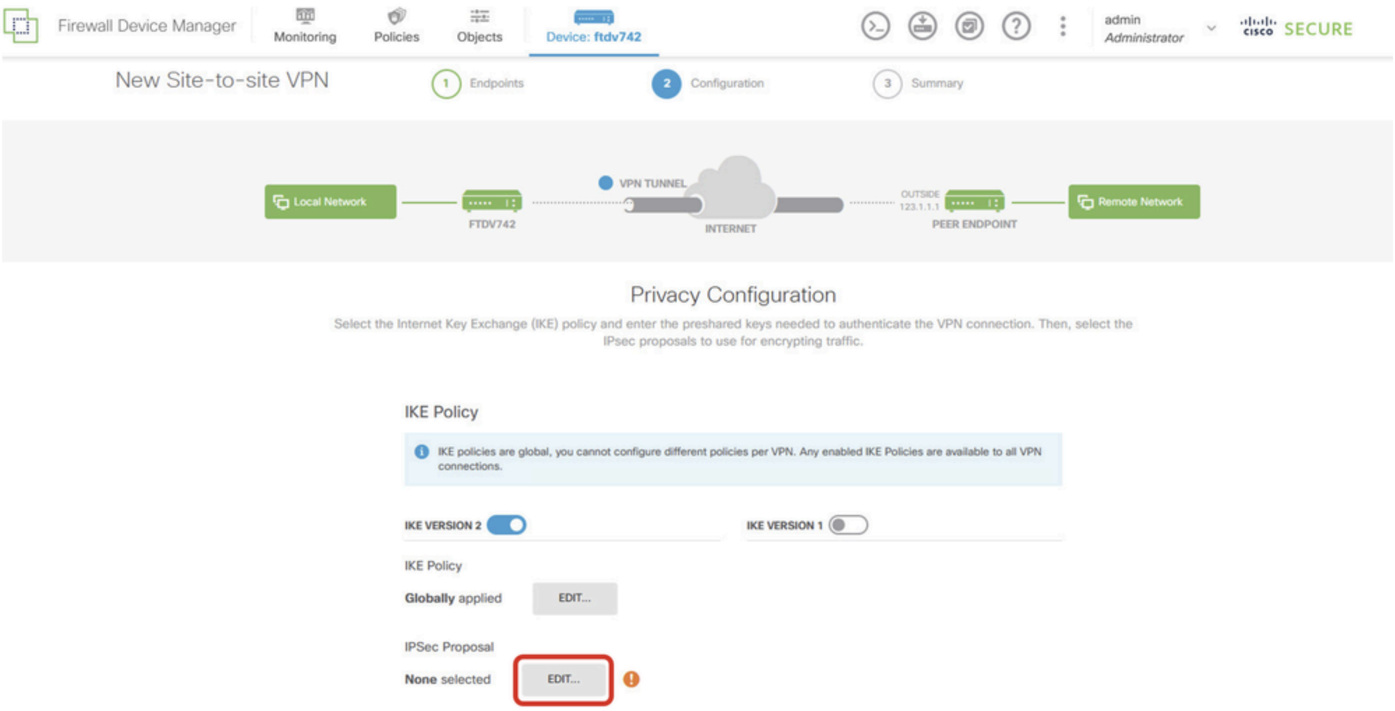
Add_New_IKE_Policy



- ○ AES-GCM-NULL-SHA
- ● AES-SHA-SHA
- ○ DES-SHA-SHA
- ● AES256_DH14_SHA256_SHA256

Enable_New_IKE_Policy

步骤 3.10 导航到IPSec提议。单击 Edit 按钮。



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ● IKE VERSION 1 ○

IKE Policy

Globally applied EDIT...

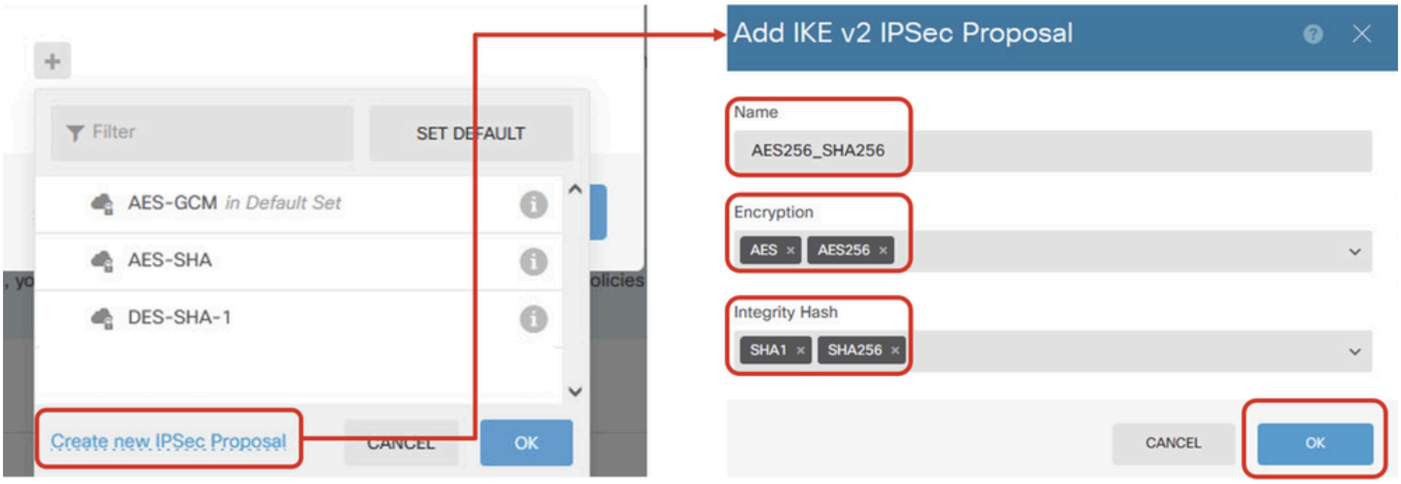
IPSec Proposal

None selected EDIT...

Edit_IKE_Proposal

步骤 3.11 对于IPSec提议，您可以使用预定义的，也可以通过单击Create new IPSec Proposal来创建一个新的。在本例中，创建一个新的用于演示目的。提供必要的信息。单击OK按钮以保存。

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

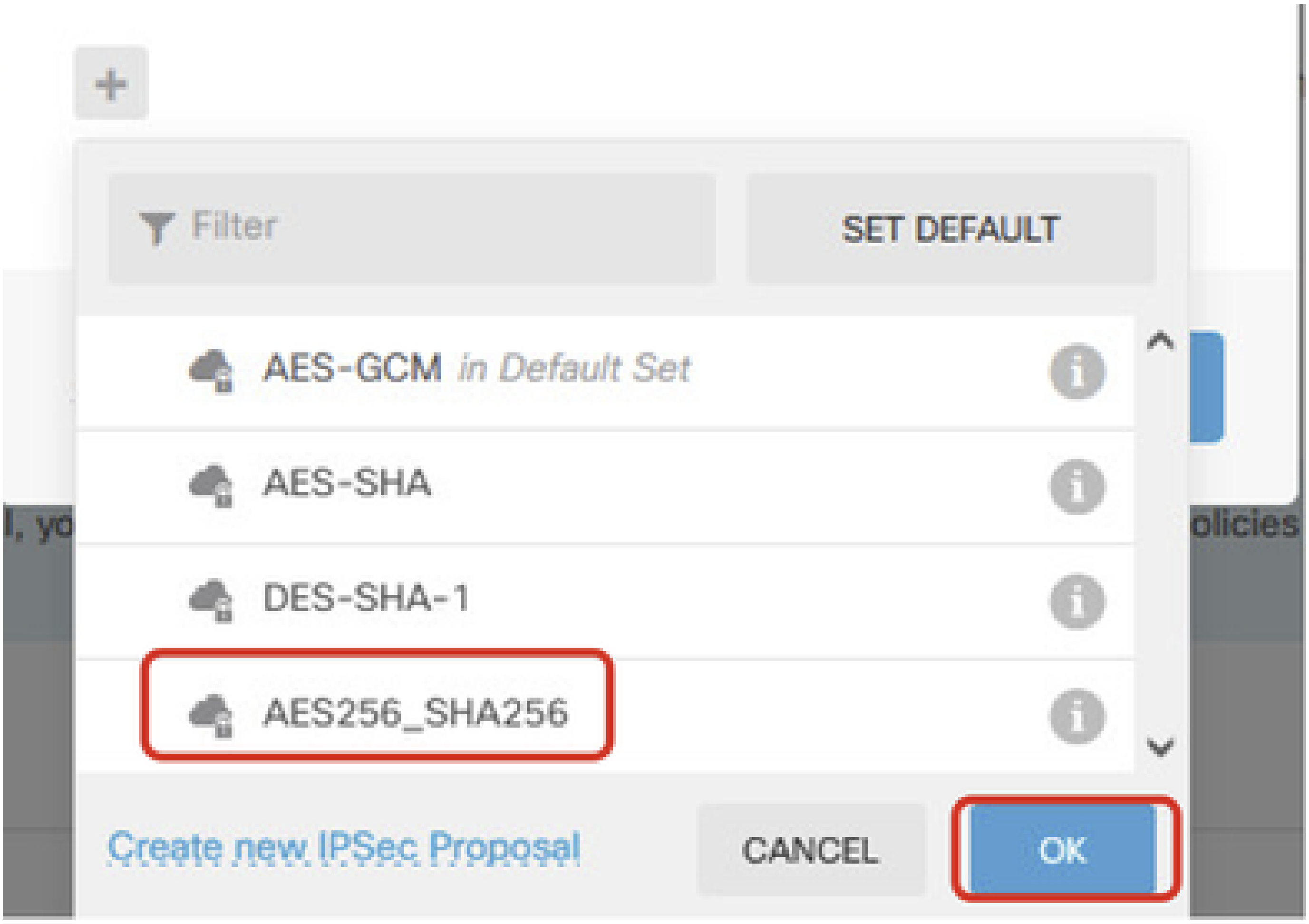


Name: AES256_SHA256

Encryption: AES × AES256 ×

Integrity Hash: SHA1 × SHA256 ×

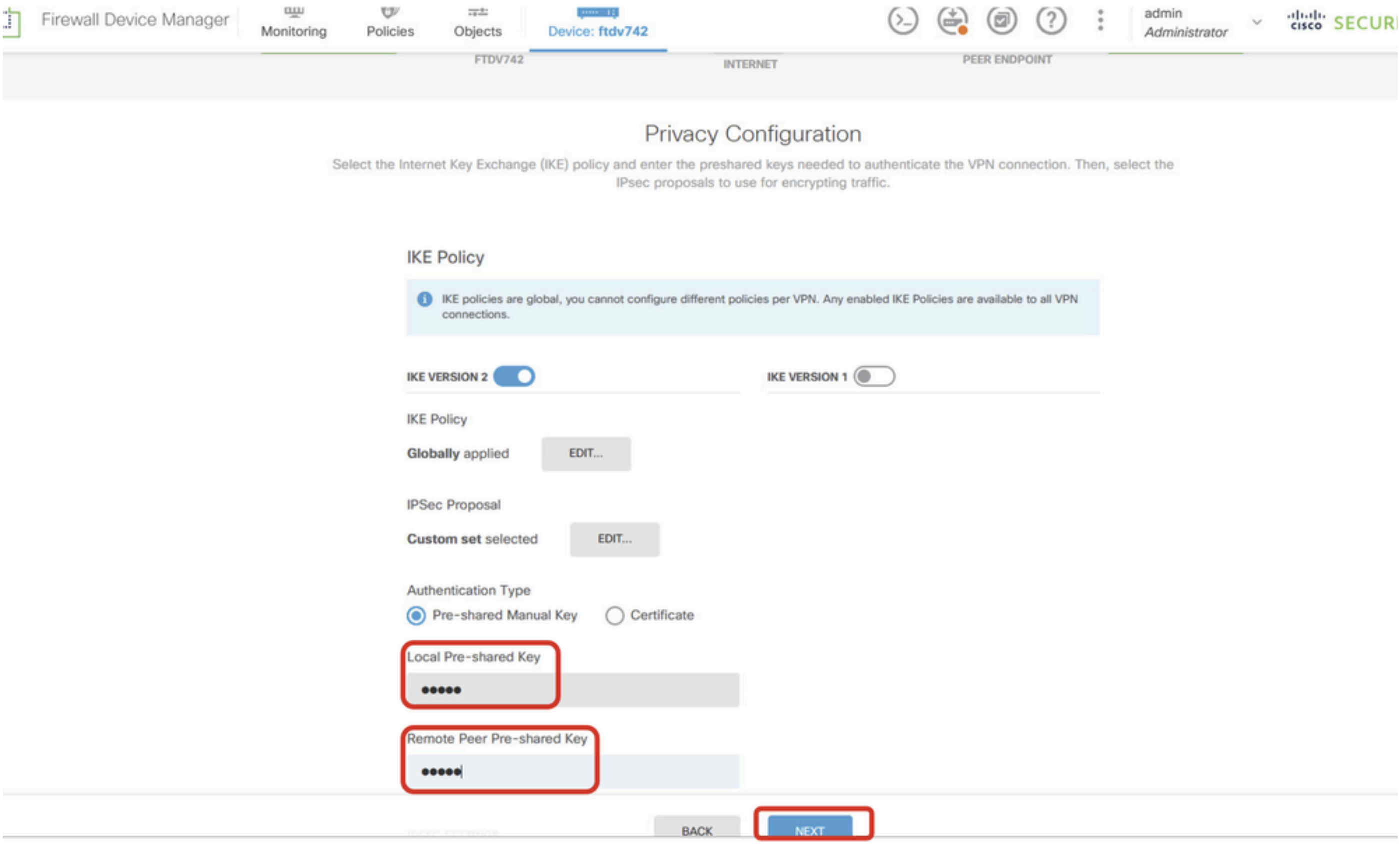
Add_New_IPSec_Proposal



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上配置它。



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ● IKE VERSION 1 ○

IKE Policy
**Globally** applied EDIT...

IPSec Proposal
**Custom set** selected EDIT...

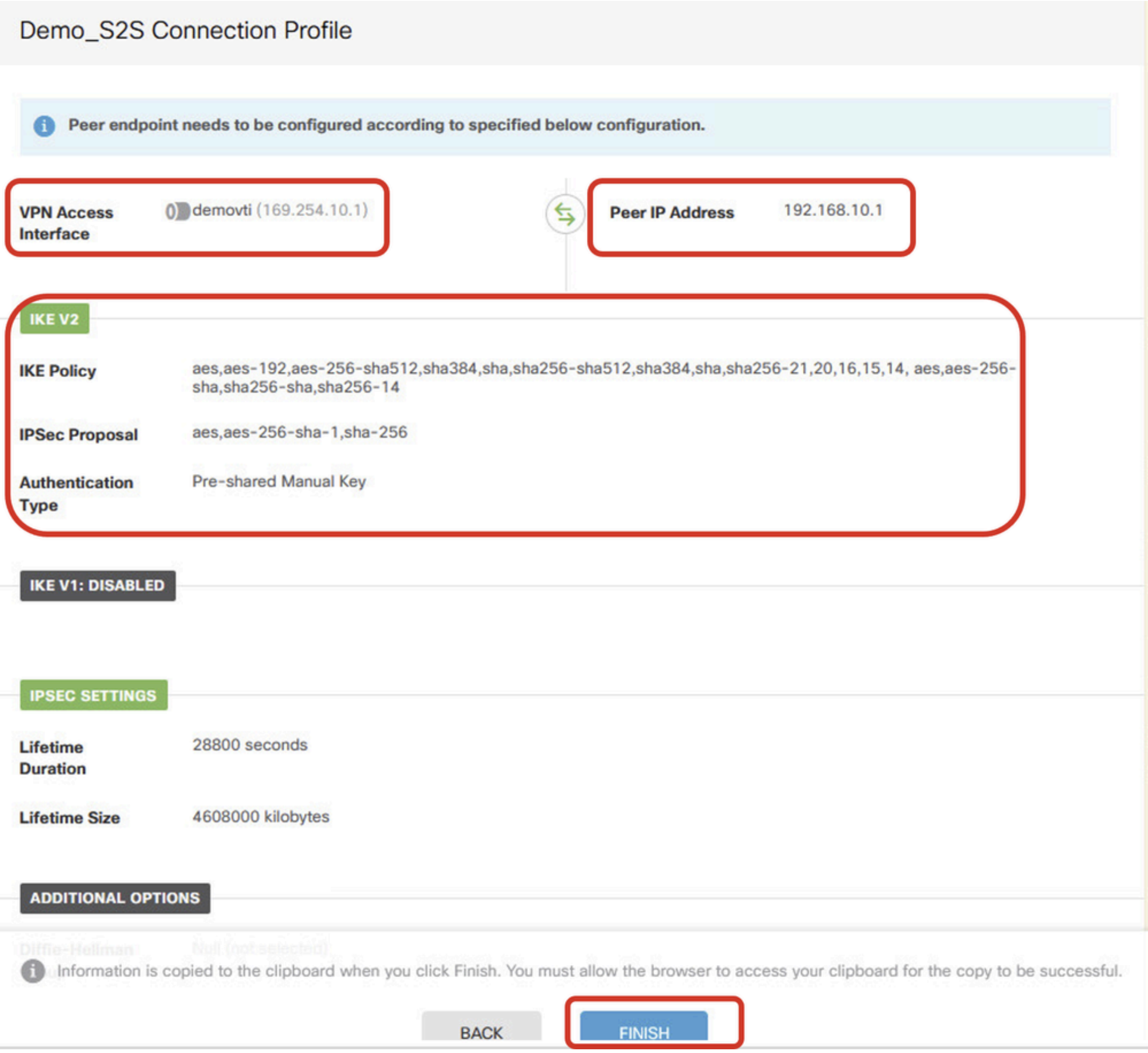
Authentication Type
● Pre-shared Manual Key ○ Certificate

Local Pre-shared Key
●●●●●

Remote Peer Pre-shared Key
●●●●●

Configure_Preshared_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。



Demo_S2S Connection Profile

Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface: demovti (169.254.10.1)

Peer IP Address: 192.168.10.1

IKE V2

IKE Policy: aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal: aes,aes-256-sha-1,sha-256

Authentication Type: Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration: 28800 seconds

Lifetime Size: 4608000 kilobytes

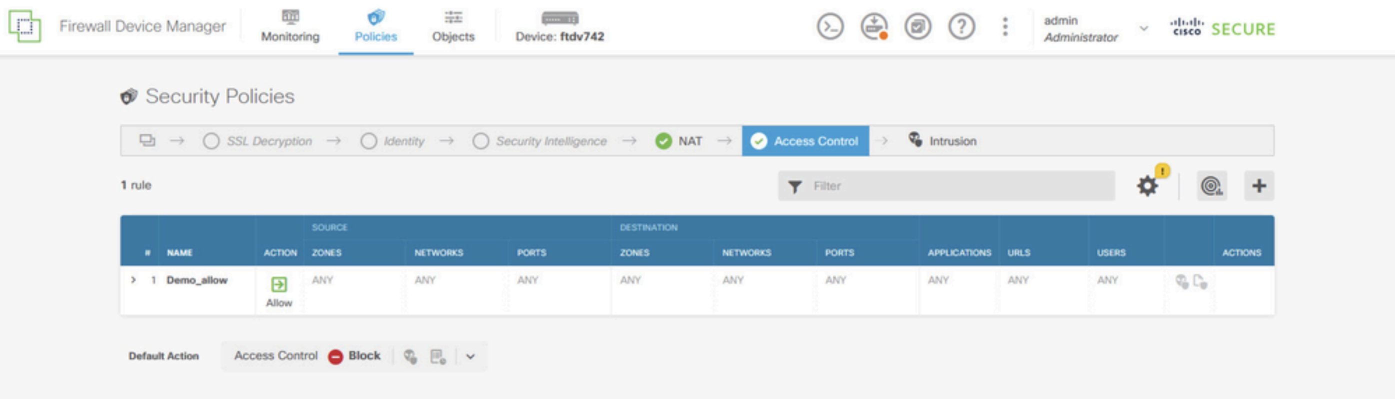
ADDITIONAL OPTIONS

Diffie-Hellman: Null (not selected)

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

VPN_Wizard_Complete

步骤 3.14创建访问控制规则以允许流量通过FTD。在本例中，为了演示目的，全部允许。 根据实际需求修改策略。



1 rule

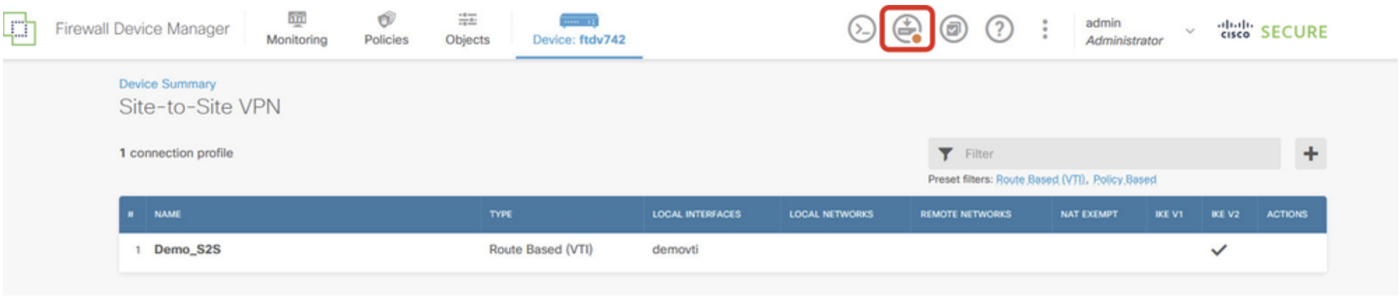
| | | | SOURCE | | | DESTINATION | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | NAME | ACTION | ZONES | NETWORKS | PORTS | ZONES | NETWORKS | PORTS | APPLICATIONS | URLS | USERS | ACTIONS |
| 1 | Demo_allow | Allow | ANY | ANY | ANY | ANY | ANY | ANY | ANY | ANY | ANY | |

Default Action: Access Control ● Block

Access_Control_Rule_Sample

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上配置客户端流量的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。



Device Summary

Site-to-Site VPN

1 connection profile

Filter

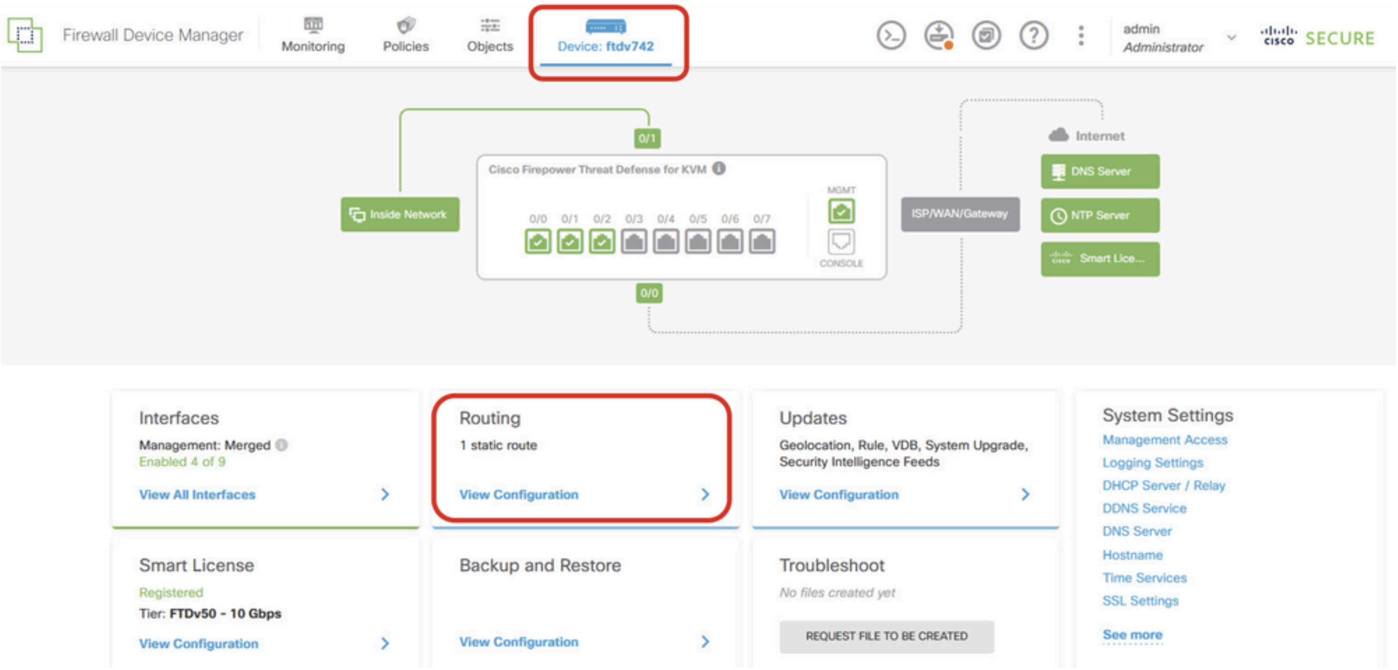
Preset filters: Route Based (VTI), Policy Based

| # | NAME | TYPE | LOCAL INTERFACES | LOCAL NETWORKS | REMOTE NETWORKS | NAT EXEMPT | IKE V1 | IKE V2 | ACTIONS |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Demo_S2S | Route Based (VTI) | demovti | | | | | ✓ | |

Deploy_VPN_Configuration

## BGP上的配置

第四步： 导航到设备>路由。单击View Configuration。



Interfaces
Management: Merged
Enabled 4 of 9
View All Interfaces >

Routing
1 static route
View Configuration >

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration >

System Settings
Management Access
Logging Settings
DHCP Server / Relay
DDNS Service
DNS Server
Hostname
Time Services
SSL Settings
See more

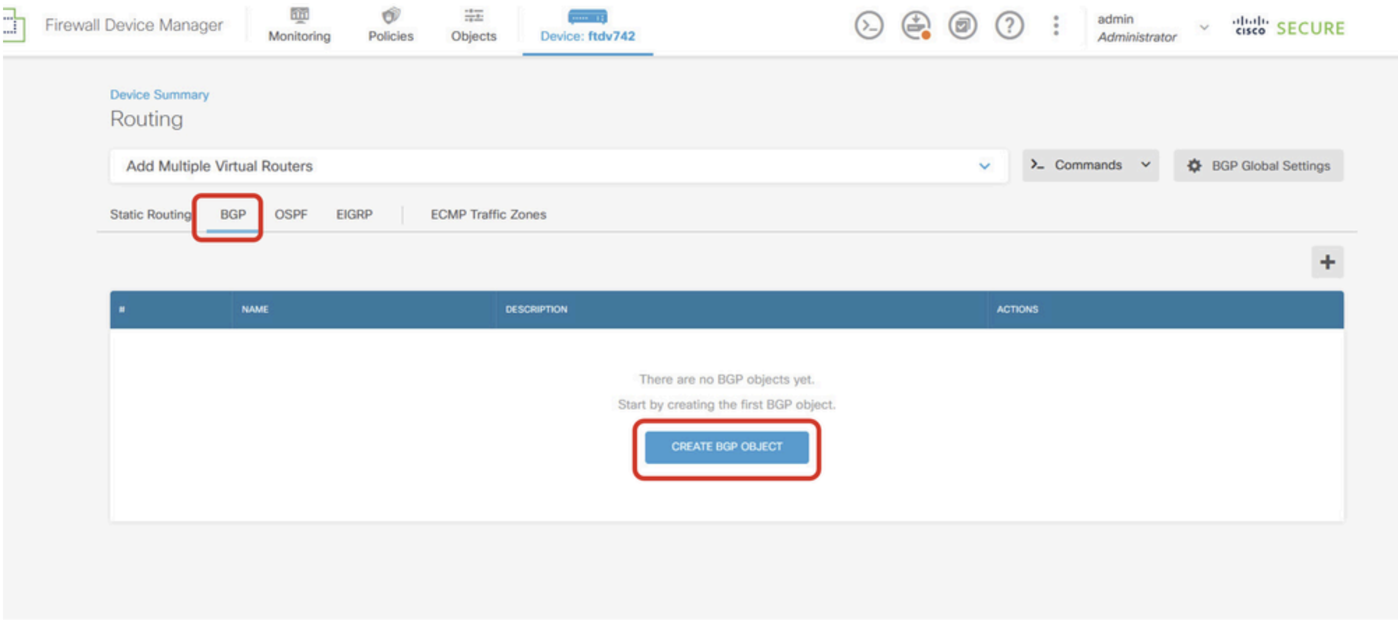
Smart License
Registered
Tier: FTDv50 - 10 Gbps
View Configuration >

Backup and Restore
View Configuration >

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

View_Routing_Configuration

第五步：单击BGP选项卡，然后单击CREATE BGP OBJECT。



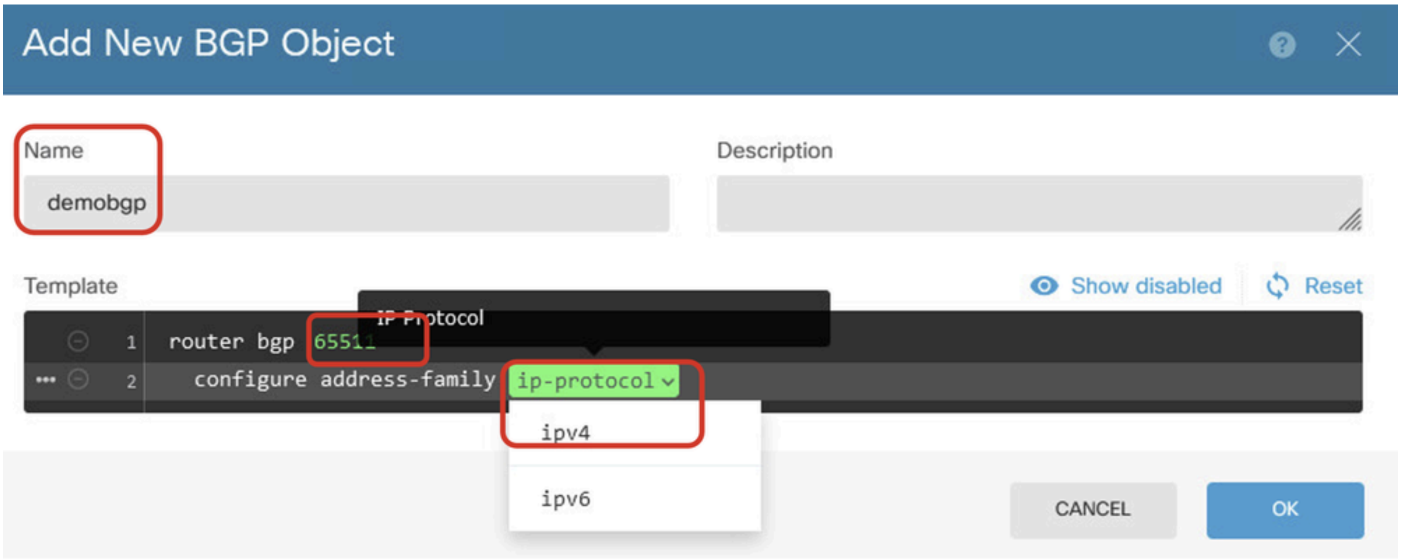
Create_BGP_Object

第六步：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编号。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。

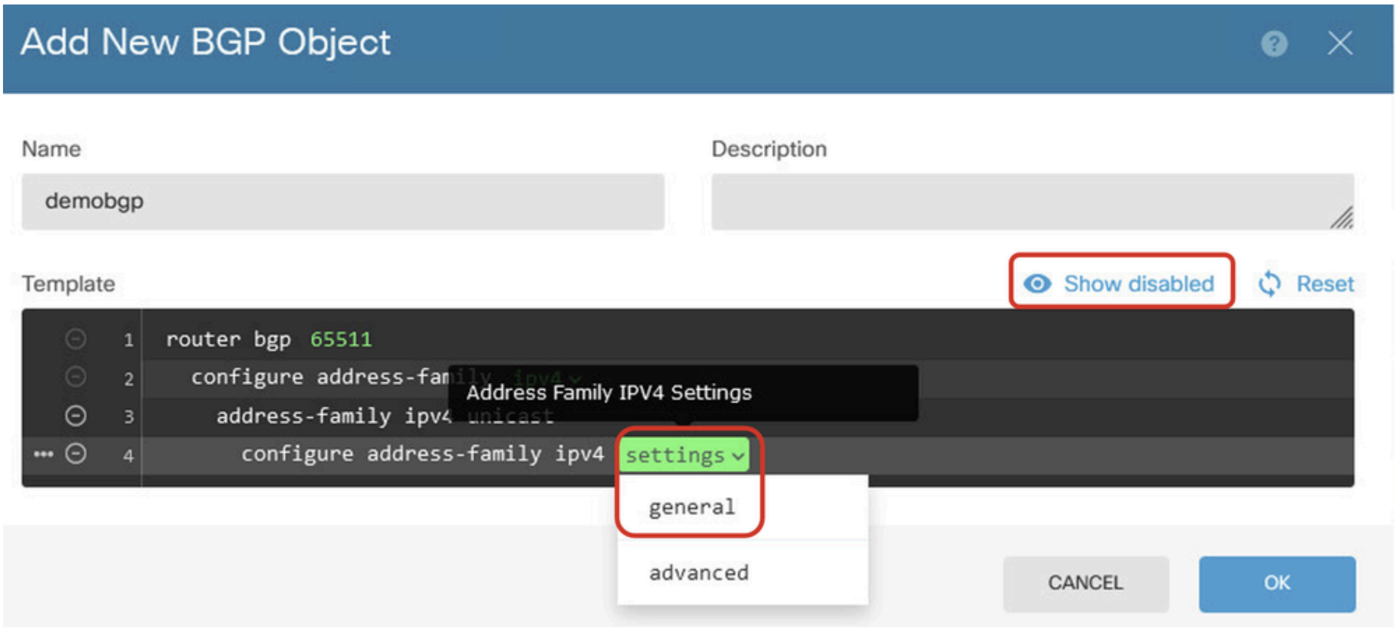


Name: demobgp

```
router bgp 65511
  configure address-family ip-protocol
```

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。



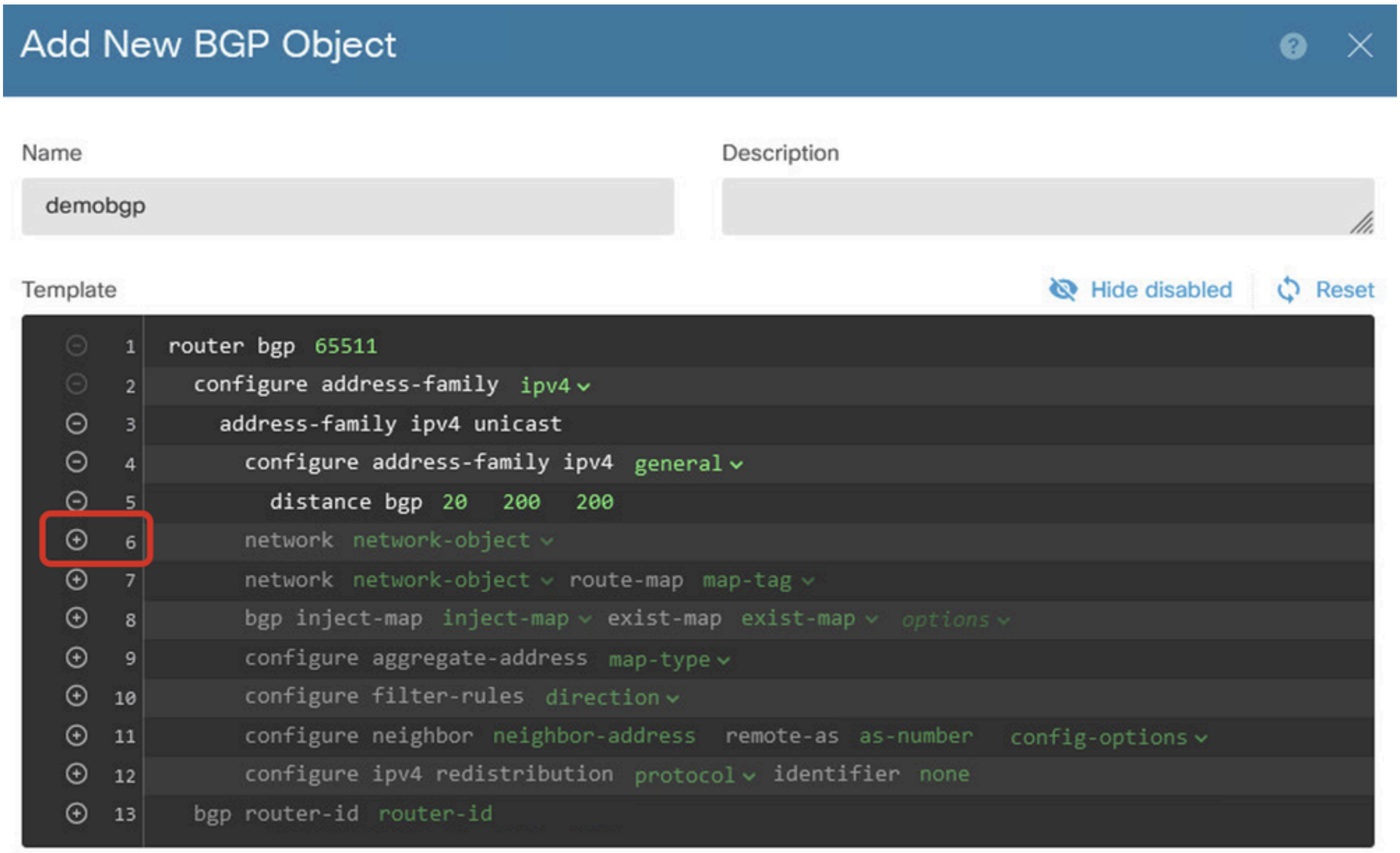
Name: demobgp

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 settings
```

settings:
- general
- advanced

Create_BGP_Object_AddressSetting

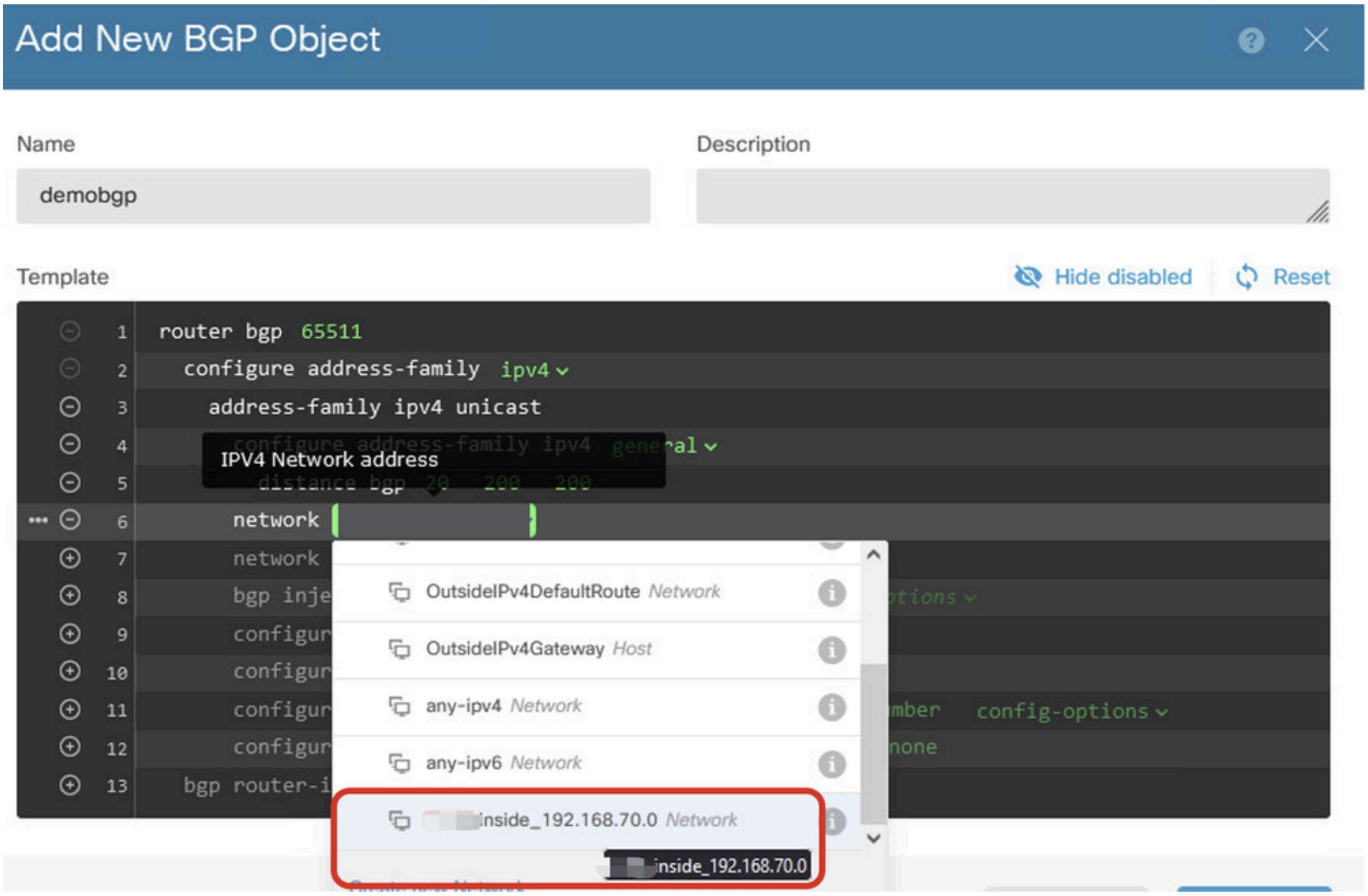
第6行：点击+图标可允许该行配置BGP网络。单击network-object。您可以查看现有可用对象并选择一个。在本示例中，选择对象name inside_192.168.70.0（在步骤3.2中创建）。



Name: demobgp

```
1  router bgp 65511
2    configure address-family ipv4
3      address-family ipv4 unicast
4        configure address-family ipv4 general
5          distance bgp 20 200 200
6        network network-object
7        network network-object route-map map-tag
8        bgp inject-map inject-map exist-map exist-map options
9        configure aggregate-address map-type
10       configure filter-rules direction
11       configure neighbor neighbor-address remote-as as-number config-options
12       configure ipv4 redistribution protocol identifier none
13   bgp router-id router-id
```

Create_BGP_Object_Add_Network



Name: demobgp

Description:

Template

```
 1  router bgp 65511
 2    configure address-family ipv4
 3      address-family ipv4 unicast
 4        configure address-family ipv4 general
 5          distance bgp 20 200 200
 6        network
 7        network
 8        bgp inje                                     ptions
 9        configur
10        configur
11        configur                                     mber   config-options
12        configur                                     none
13    bgp router-i
```

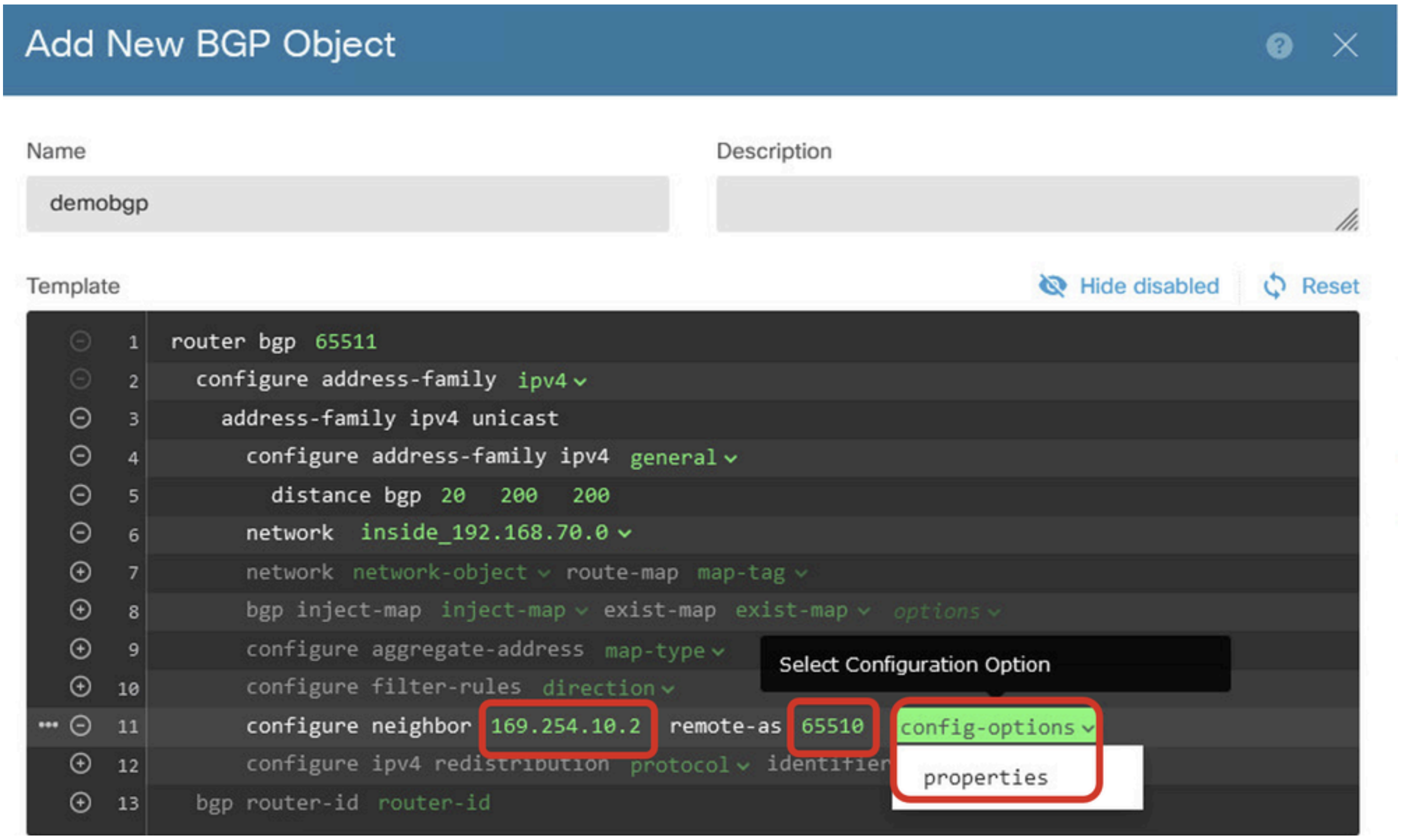
IPV4 Network address

- OutsideIPv4DefaultRoute *Network*
- OutsideIPv4Gateway *Host*
- any-ipv4 *Network*
- any-ipv6 *Network*
- [redacted]inside_192.168.70.0 *Network*

[redacted]inside_192.168.70.0

Create_BGP_Object_Add_Network2

第11行：点击+图标可启用该行以配置BGP邻居相关信息。单击neighbor-address，然后手动输入对等体BGP邻居地址。在本示例中，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用于站点2FTD。单击config-options 并选择properties。



Add New BGP Object

Name: demobgp

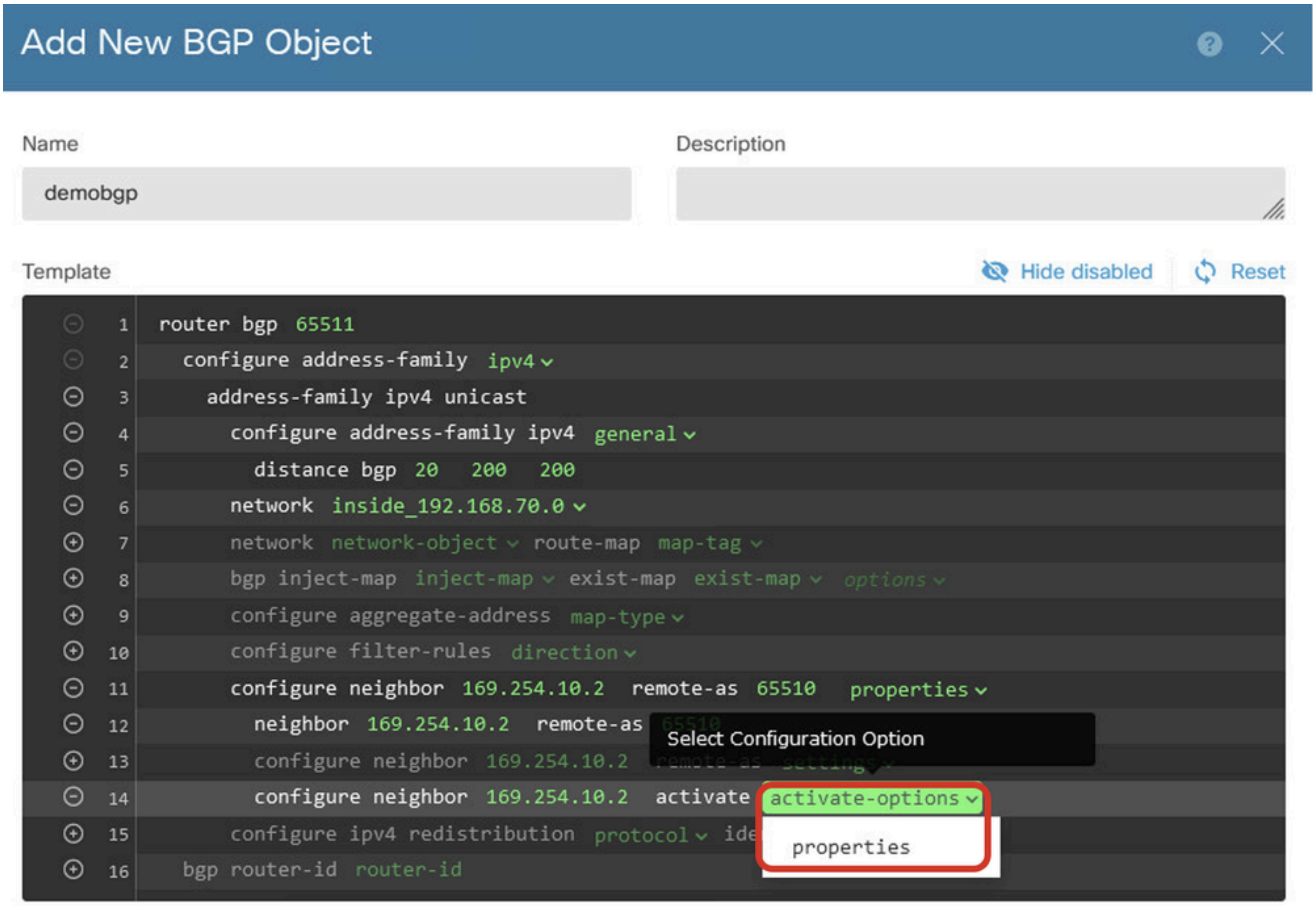
Description:

Template

```
1   router bgp  65511
2     configure address-family  ipv4
3       address-family ipv4 unicast
4         configure address-family ipv4  general
5           distance bgp  20   200   200
6         network  inside_192.168.70.0
7         network  network-object  route-map  map-tag
8         bgp inject-map  inject-map  exist-map  exist-map  options
9         configure aggregate-address  map-type
10        configure filter-rules  direction
11        configure neighbor  169.254.10.2  remote-as  65510  config-options
12        configure ipv4 redistribution  protocol  identifier
13    bgp router-id  router-id
```

Create_BGP_Object_NeighborSetting

第14行：单击+图标可启用该行以配置邻居的某些属性。单击activate-options并选择properties。



Add New BGP Object

Name: demobgp

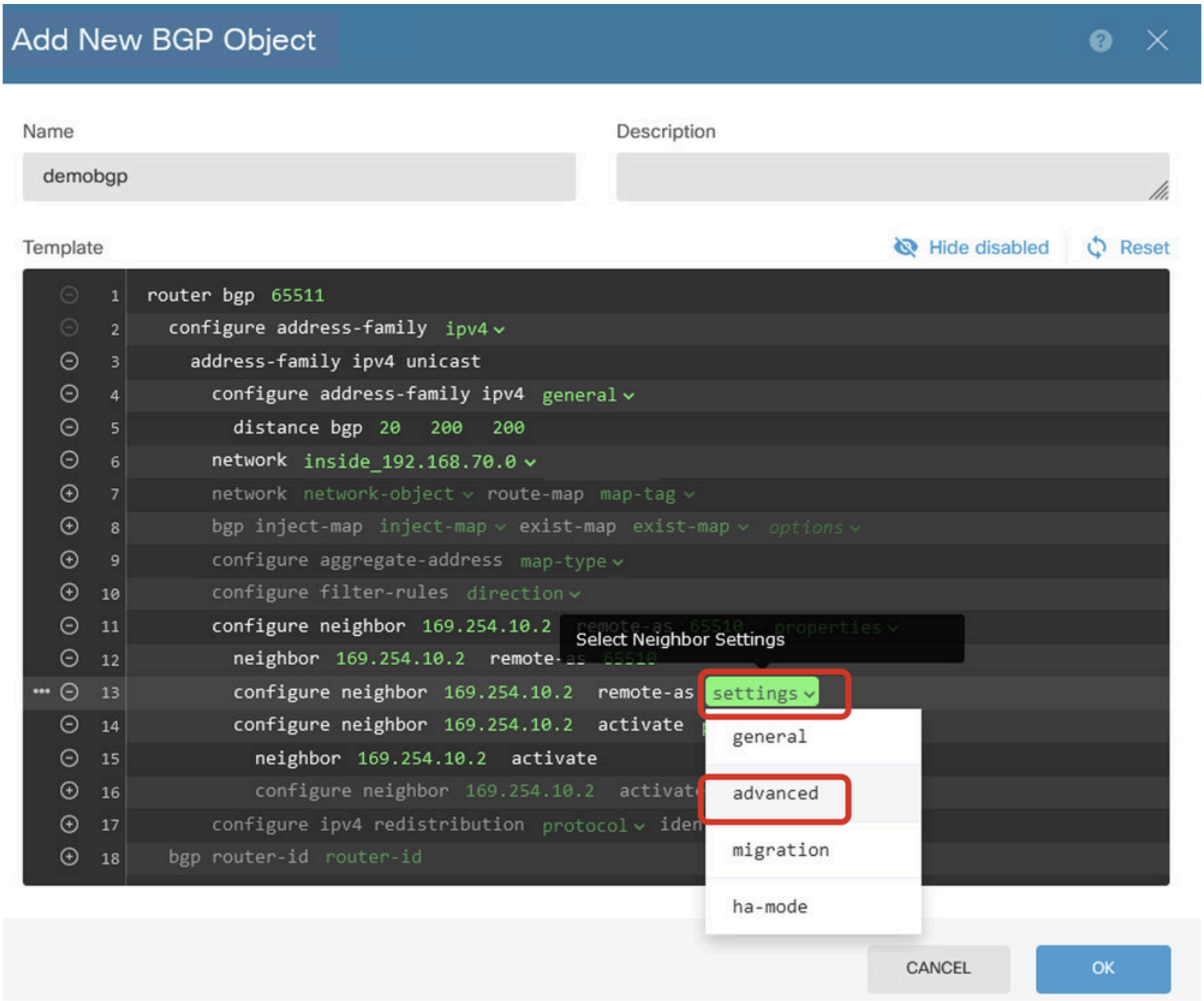
Description:

Template

```
1   router bgp  65511
2     configure address-family  ipv4
3       address-family ipv4 unicast
4         configure address-family ipv4  general
5           distance bgp  20   200   200
6         network  inside_192.168.70.0
7         network  network-object  route-map  map-tag
8         bgp inject-map  inject-map  exist-map  exist-map  options
9         configure aggregate-address  map-type
10        configure filter-rules  direction
11        configure neighbor  169.254.10.2  remote-as  65510  properties
12          neighbor  169.254.10.2  remote-as  65510
13          configure neighbor  169.254.10.2  remote-as  settings
14          configure neighbor  169.254.10.2  activate  activate-options
15        configure ipv4 redistribution  protocol  ide
16    bgp router-id  router-id
```

Create_BGP_Object_NeighborSetting_Properties

第13行：点击+图标可让行显示高级选项。单击设置并选择高级。



Add New BGP Object

Name: demobgp

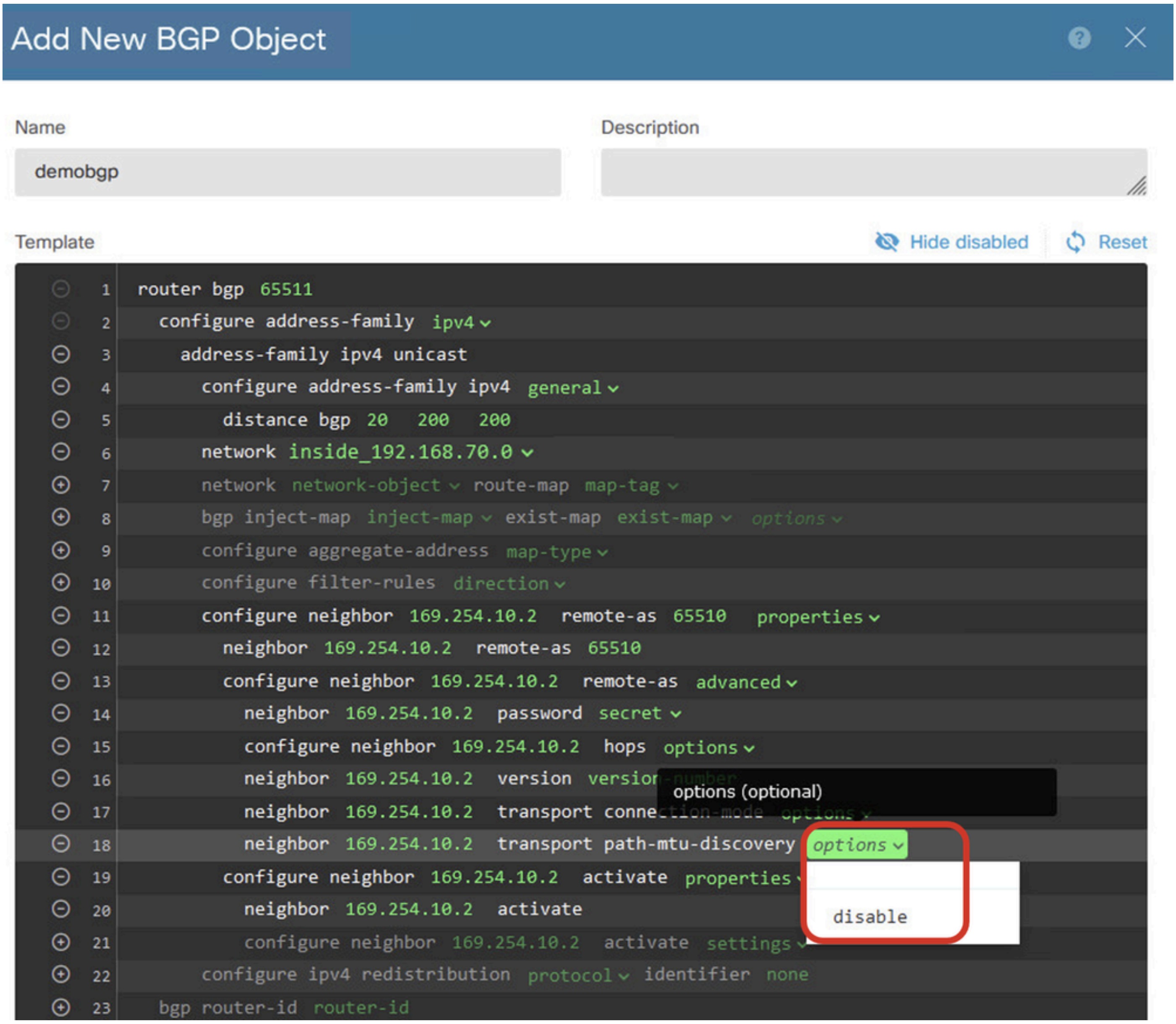
Description:

Template

```
1  router bgp 65511
2    configure address-family ipv4
3      address-family ipv4 unicast
4        configure address-family ipv4 general
5          distance bgp 20  200  200
6        network inside_192.168.70.0
7        network network-object route-map map-tag
8        bgp inject-map inject-map exist-map exist-map options
9        configure aggregate-address map-type
10       configure filter-rules direction
11       configure neighbor 169.254.10.2 remote-as 65510 properties
12         neighbor 169.254.10.2 remote-as 65510
13         configure neighbor 169.254.10.2 remote-as settings
14         configure neighbor 169.254.10.2 activate p
15           neighbor 169.254.10.2 activate
16           configure neighbor 169.254.10.2 activat
17       configure ipv4 redistribution protocol iden
18   bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties_Advanced

第18行：点击选项并选择禁用以禁用路径MTU发现。



Name: demobgp

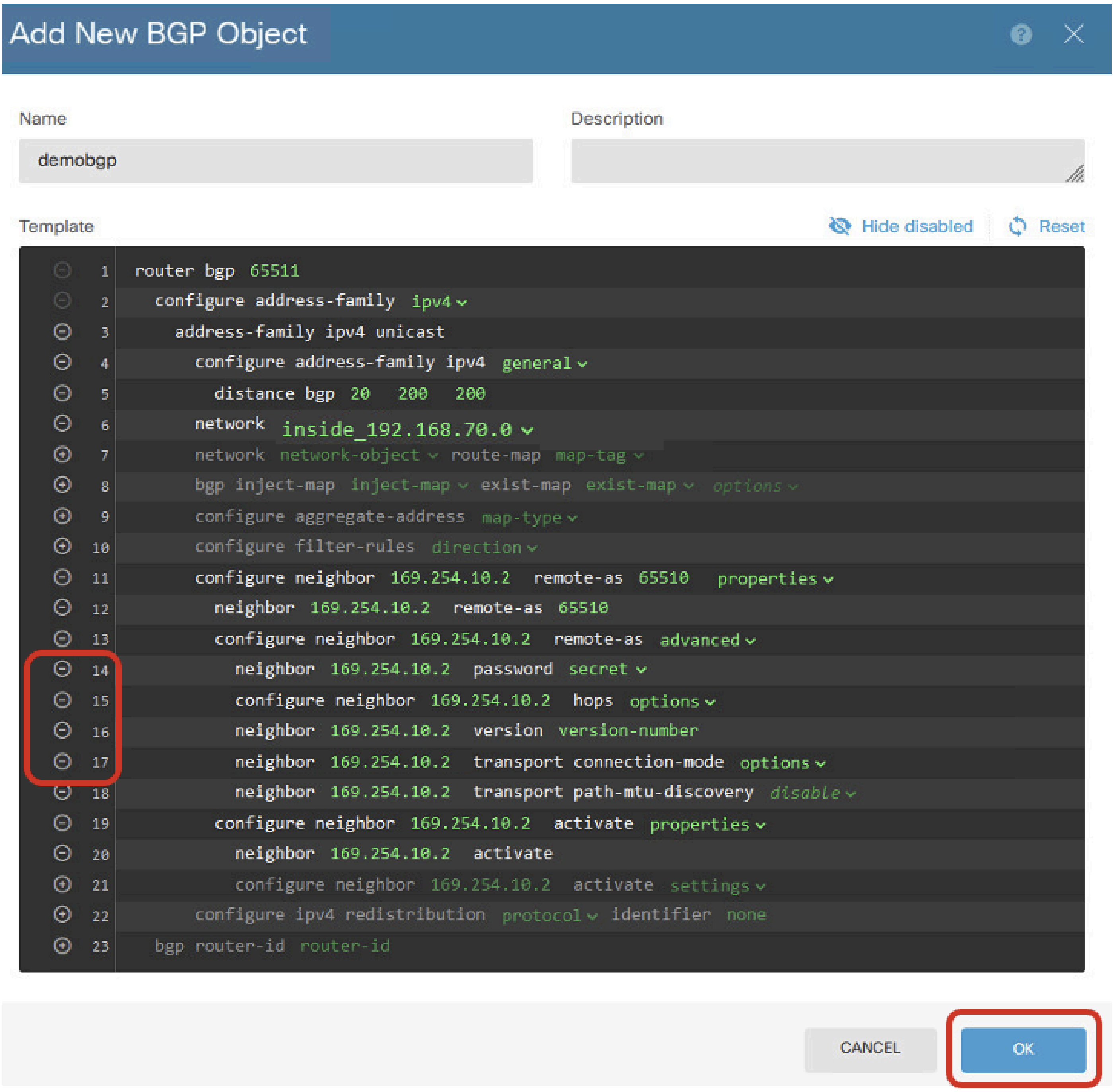
Description:

Template

```
1  router bgp 65511
2    configure address-family ipv4
3      address-family ipv4 unicast
4        configure address-family ipv4 general
5          distance bgp 20 200 200
6        network inside_192.168.70.0
7        network network-object route-map map-tag
8        bgp inject-map inject-map exist-map exist-map options
9        configure aggregate-address map-type
10       configure filter-rules direction
11       configure neighbor 169.254.10.2 remote-as 65510 properties
12         neighbor 169.254.10.2 remote-as 65510
13         configure neighbor 169.254.10.2 remote-as advanced
14           neighbor 169.254.10.2 password secret
15           configure neighbor 169.254.10.2 hops options
16           neighbor 169.254.10.2 version version-number
17           neighbor 169.254.10.2 transport connection-mode options
18           neighbor 169.254.10.2 transport path-mtu-discovery options
19         configure neighbor 169.254.10.2 activate properties
20           neighbor 169.254.10.2 activate
21           configure neighbor 169.254.10.2 activate settings
22       configure ipv4 redistribution protocol identifier none
23   bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

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



Name: demobgp

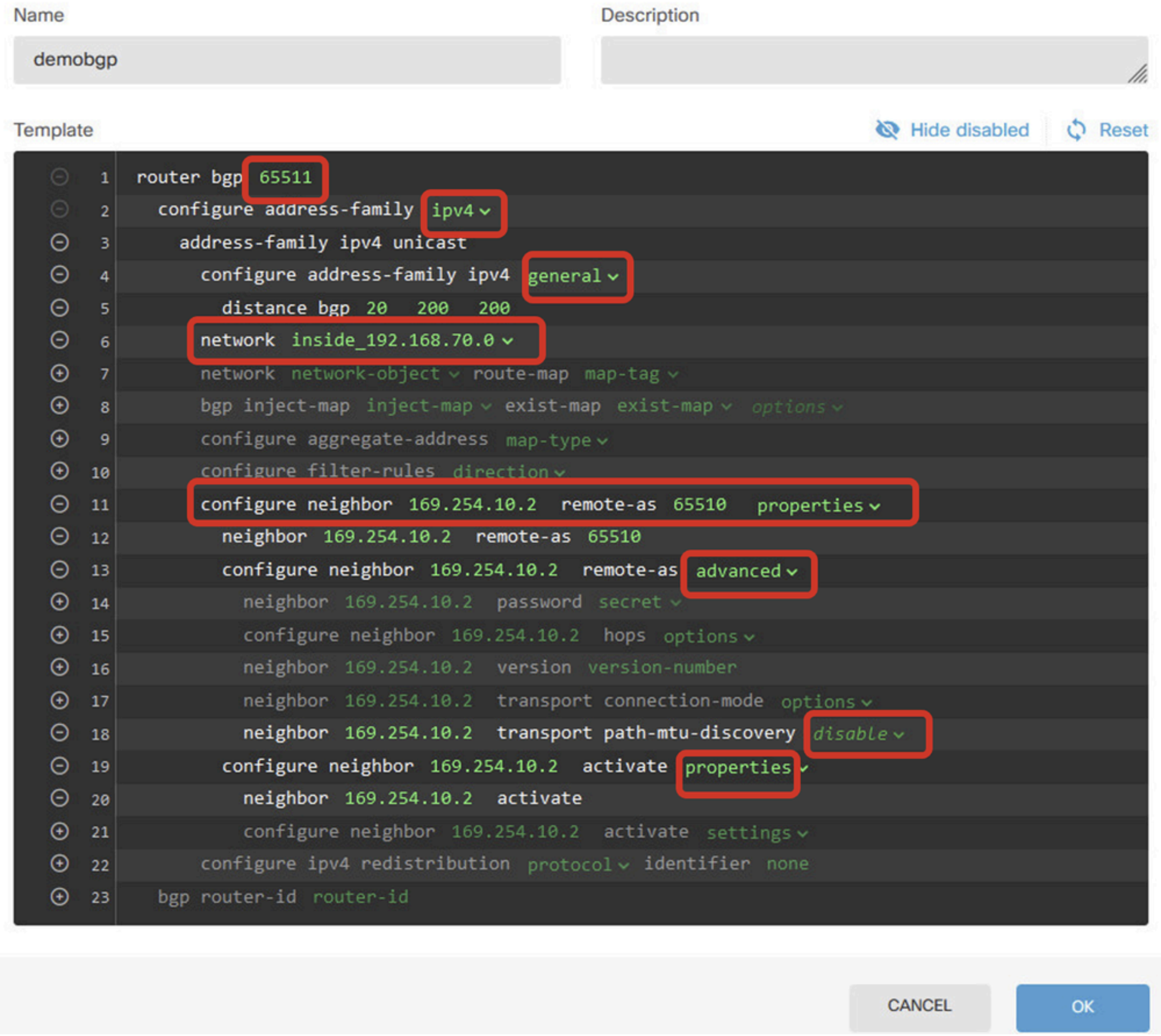
Description:

Template

```
router bgp 65511
  configure address-family ipv4
    address-family ipv4 unicast
      configure address-family ipv4 general
        distance bgp 20 200 200
      network inside_192.168.70.0
      network network-object route-map map-tag
      bgp inject-map inject-map exist-map exist-map options
      configure aggregate-address map-type
      configure filter-rules direction
      configure neighbor 169.254.10.2 remote-as 65510 properties
        neighbor 169.254.10.2 remote-as 65510
        configure neighbor 169.254.10.2 remote-as advanced
          neighbor 169.254.10.2 password secret
          configure neighbor 169.254.10.2 hops options
          neighbor 169.254.10.2 version version-number
          neighbor 169.254.10.2 transport connection-mode options
          neighbor 169.254.10.2 transport path-mtu-discovery disable
        configure neighbor 169.254.10.2 activate properties
          neighbor 169.254.10.2 activate
          configure neighbor 169.254.10.2 activate settings
      configure ipv4 redistribution protocol identifier none
  bgp router-id router-id
```

Create_BGP_Object_DisableLines

以下是此示例中的BGP设置的概述。您可以根据实际需求配置其他BGP设置。



Name

demobgp

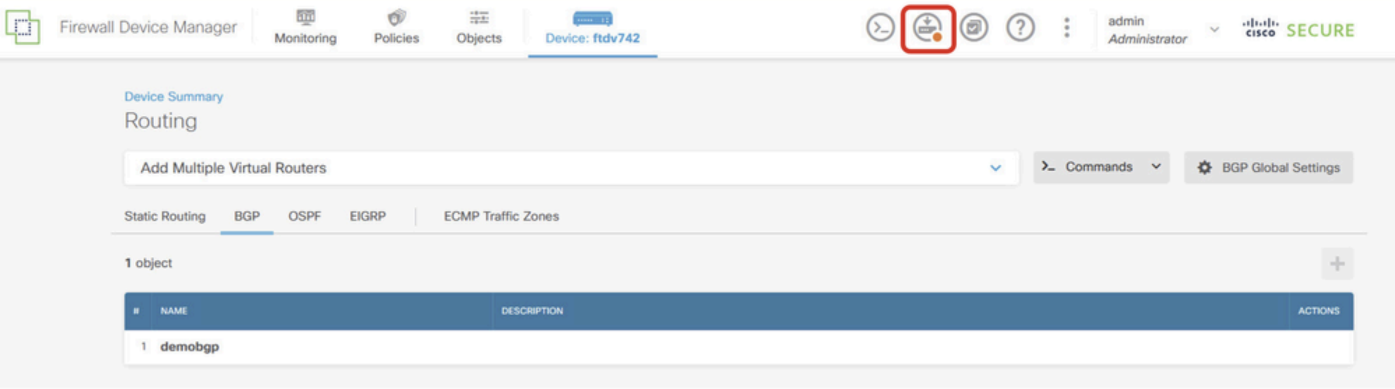
Description

Template

```
router bgp 65511
  configure address-family ipv4
    address-family ipv4 unicast
      configure address-family ipv4 general
        distance bgp 20 200 200
      network inside_192.168.70.0
      network network-object route-map map-tag
      bgp inject-map inject-map exist-map exist-map options
      configure aggregate-address map-type
      configure filter-rules direction
      configure neighbor 169.254.10.2 remote-as 65510 properties
        neighbor 169.254.10.2 remote-as 65510
        configure neighbor 169.254.10.2 remote-as advanced
          neighbor 169.254.10.2 password secret
          configure neighbor 169.254.10.2 hops options
          neighbor 169.254.10.2 version version-number
          neighbor 169.254.10.2 transport connection-mode options
          neighbor 169.254.10.2 transport path-mtu-discovery disable
        configure neighbor 169.254.10.2 activate properties
          neighbor 169.254.10.2 activate
          configure neighbor 169.254.10.2 activate settings
      configure ipv4 redistribution protocol identifier none
  bgp router-id router-id
```

Create_BGP_Object_Final_Overview

步骤 7.部署BGP配置更改。



Device Summary

Routing

Add Multiple Virtual Routers

1 object

| # | NAME | DESCRIPTION | ACTIONS |
|---|---|---|---|
| 1 | demobgp | | |

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参数重复第3步到第7步。

CLI中Site1 FTD和Site2 FTD的配置概述。

| 站点1 FTD | 站点2 FTD |
|---|---|
| NGFW版本7.4.2<br><br>interface GigabitEthernet0/0<br>nameif outside<br>cts manual（cts手册）<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>security-level 0<br>ip address 192.168.30.1 255.255.255.0<br><br>interface GigabitEthernet0/2<br>nameif内部<br>security-level 0<br>ip address 192.168.70.1 255.255.255.0<br><br>interface Tunnel1<br>nameif demovti<br>ip address 169.254.10.1 255.255.255.0<br>隧道源接口外部<br>隧道目标192.168.10.1<br>隧道模式ipsec ipv4<br>隧道保护ipsec配置文件ipsec_profile\|e4084d322d<br><br>对象网络外部IPv4网关<br>host 192.168.30.3<br>object network inside_192.168.70.0<br>子网地址为192.168.70.0 255.255.255.0<br><br>access-group NGFW_ONBOX_ACL global<br>access-list NGFW_ONBOX_ACL remark rule-id 268435457：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 268435457： L5规则：Inside_Outside_Rule<br>access-list NGFW_ONBOX_ACL advanced trust object-group \|acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both<br>access-list NGFW_ONBOX_ACL remark rule-id 268435458：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 268435458： L5规则：Demo_allow | NGFW版本7.4.2<br><br>interface GigabitEthernet0/0<br>nameif outside<br>cts manual（cts手册）<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>security-level 0<br>ip address 192.168.10.1 255.255.255.0<br><br>interface GigabitEthernet0/2<br>nameif内部<br>security-level 0<br>ip address 192.168.50.1 255.255.255.0<br><br>interface Tunnel1<br>nameif demovti25<br>ip address 169.254.10.2 255.255.255.0<br>隧道源接口外部<br>隧道目标192.168.30.1<br>隧道模式ipsec ipv4<br>隧道保护ipsec配置文件ipsec_profile\|e4084d322d<br><br>对象网络外部IPv4网关<br>host 192.168.10.3<br>object network inside_192.168.50.0<br>子网地址为192.168.50.0 255.255.255.0<br><br>access-group NGFW_ONBOX_ACL global<br>access-list NGFW_ONBOX_ACL remark rule-id 268435457：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 268435457： L5规则：Inside_Outside_Rule<br>access-list NGFW_ONBOX_ACL advanced trust object-group \|acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both<br>access-list NGFW_ONBOX_ACL remark rule-id 268435458：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 268435458： L5规则：Demo_allow<br>access-list NGFW_ONBOX_ACL advanced permit object- |

| | |
|---|---|
| access-list NGFW_ONBOX_ACL advanced permit object-group \|acSvcg-268435458 any any rule-id 268435458 event-log both<br>access-list NGFW_ONBOX_ACL remark rule-id 1：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 1： L5规则：默认操作规则<br>access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1<br><br>router bgp 65511<br>bgp log-neighbor-changes<br>bgp router-id vrf auto-assign<br>address-family ipv4 unicast<br>neighbor 169.254.10.2 remote-as 65510<br>邻居169.254.10.2 transport path-mtu-discovery disable<br>neighbor 169.254.10.2 activate<br>network 192.168.70.0<br>no auto-summary<br>无同步<br>exit-address-family<br><br>route outside 0.0.0.0 0.0.0.0 192.168.30.3 1<br><br>crypto ipsec ikev2 ipsec-proposal AES256_SHA256<br>protocol esp encryption aes-256 aes<br>protocol esp integrity sha-256 sha-1<br><br>crypto ipsec profile ipsec_profile\|e4084d322d<br>set ikev2 ipsec-proposal AES256_SHA256<br>set security-association lifetime kilobytes 4608000<br>set security-association lifetime seconds 28800<br><br>crypto ipsec security-association pmtu-aging infinite<br><br>crypto ikev2 policy 1<br>加密aes-256 aes<br>integrity sha256 sha<br>第 14 组<br>prf sha256 sha<br>lifetime seconds 86400<br><br>crypto ikev2 policy 20<br>加密aes-256 aes-192 aes<br>integrity sha512 sha384 sha256 sha<br>第21组20 16 15 14<br>prf sha512 sha384 sha256 sha | group \|acSvcg-268435458 any any rule-id 268435458 event-log both<br>access-list NGFW_ONBOX_ACL remark rule-id 1：访问策略：NGFW_Access_Policy<br>access-list NGFW_ONBOX_ACL remark rule-id 1： L5规则：默认操作规则<br>access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1<br><br>router bgp 65510<br>bgp log-neighbor-changes<br>bgp router-id vrf auto-assign<br>address-family ipv4 unicast<br>neighbor 169.254.10.1 remote-as 65511<br>邻居169.254.10.1 transport path-mtu-discovery disable<br>neighbor 169.254.10.1 activate<br>network 192.168.50.0<br>no auto-summary<br>无同步<br>exit-address-family<br><br>route outside 0.0.0.0 0.0.0.0 192.168.10.3 1<br><br>crypto ipsec ikev2 ipsec-proposal AES256_SHA256<br>protocol esp encryption aes-256 aes<br>protocol esp integrity sha-256 sha-1<br><br>crypto ipsec profile ipsec_profile\|e4084d322d<br>set ikev2 ipsec-proposal AES256_SHA256<br>set security-association lifetime kilobytes 4608000<br>set security-association lifetime seconds 28800<br><br>crypto ipsec security-association pmtu-aging infinite<br><br>crypto ikev2 policy 1<br>加密aes-256 aes<br>integrity sha256 sha<br>第 14 组<br>prf sha256 sha<br>lifetime seconds 86400<br><br>crypto ikev2 policy 20<br>加密aes-256 aes-192 aes<br>integrity sha512 sha384 sha256 sha<br>第21组20 16 15 14<br>prf sha512 sha384 sha256 sha<br>lifetime seconds 86400 |

<table>
<tr>
<td>lifetime seconds 86400<br><br>crypto ikev2 enable outside<br><br>组策略 |s2sGP|192.168.10.1内部<br>组策略 |s2sGP|192.168.10.1属性<br>vpn-tunnel-protocol ikev2<br><br>tunnel-group 192.168.10.1 type ipsec-l2l<br>tunnel-group 192.168.10.1 general-attributes<br>default-group-policy |s2sGP|192.168.10.1<br><br>隧道组192.168.10.1 ipsec属性<br>ikev2 remote-authentication pre-shared-key *****<br>ikev2 local-authentication pre-shared-key *****</td>
<td>crypto ikev2 enable outside<br><br>组策略 |s2sGP|192.168.30.1内部<br>组策略 |s2sGP|192.168.30.1属性<br>vpn-tunnel-protocol ikev2<br><br>tunnel-group 192.168.30.1 type ipsec-l2l<br>tunnel-group 192.168.30.1 general-attributes<br>default-group-policy |s2sGP|192.168.30.1<br><br>隧道组192.168.30.1 ipsec属性<br>ikev2 remote-authentication pre-shared-key *****<br>ikev2 local-authentication pre-shared-key *****</td>
</tr>
</table>

# 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，以通过命令show crypto ikev2 sa和show crypto ipsec sa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<br>IKEv2 SA：<br>Session-id：134， Status：UP-ACTIVE， IKE count：1， CHILD count：1<br>隧道ID本地远程fvrf/ivrf状态角色<br>563984431 192.168.30.1/500 192.168.10.1/500全局/全球就绪型响应器<br>Encr：AES-CBC，密钥大小：256，散列：SHA256，DH组：14，身份验证签名：PSK，身份验证验证：PSK<br>寿命/活动时间：86400/5145秒<br>子sa：本地选择器0.0.0.0/0 - 255.255.255.255/65535<br>远程选择器0.0.0.0/0 - 255.255.255.255/65535<br>ESP spi输入/输出： 0xf0c4239d/0xb7b5b38b | ftdv742# show crypto ikev2 sa<br>IKEv2 SA：<br>Session-id：13， Status：UP-ACTIVE， IKE count：1， CHILD count：1<br>隧道ID本地远程fvrf/ivrf状态角色<br>339797985 192.168.10.1/500 192.168.30.1/500全局/全局就绪发起程序<br>Encr：AES-CBC，密钥大小：256，散列：SHA256，DH组：14，身份验证签名：PSK，身份验证验证：PSK<br>寿命/活动时间：86400/74099秒<br>子sa：本地选择器0.0.0.0/0 - 255.255.255.255/65535<br>远程选择器0.0.0.0/0 - 255.255.255.255/65535<br>ESP spi输入/输出：0xb7b5b38b/0xf0c4239d |

| | |
|---|---|
| ftdv742# show crypto ipsec sa<br><br>界面：demovti<br>加密映射标记：__vti-crypto-map-Tunnel1-0-1，序列号：65280，本地地址：192.168.30.1<br><br>受保护的vrf (ivrf)：全球<br>本地ident（地址/掩码/端口）：(0.0.0.0/0.0.0.0/0/0)<br>远程ident （地址/掩码/端口）：(0.0.0.0/0.0.0.0/0/0)<br>current_peer： 192.168.10.1<br><br>#pkts encaps： 5720，#pkts encrypt：5720，#pkts digest： 5720<br>#pkts decap：5717，#pkts decrypt：5717，#pkts verify：5717<br>#pkts压缩：0，#pkts解压缩：0<br>#pkts未压缩： 5720，#pkts comp失败：0，#pkts decomp失败： 0<br>#pre-frag成功：0，#pre-frag失败：0，#fragments已创建：0<br>发送#PMTUs：0，#PMTUs rcvd：0，需要重组的#decapsulated frg：0<br>#TFC rcvd：0，#TFC发送：0<br>#Valid ICMP错误rcvd：0，#Invalid ICMP错误rcvd：0<br>#send错误： 0，#recv错误： 0<br><br>本地加密终端：192.168.30.1/500，远程加密终端：192.168.10.1/500<br>路径mtu 1500、ipsec开销78(44)、媒体mtu 1500<br>PMTU剩余时间（秒）：0，DF策略：copy-df<br>ICMP错误验证：禁用，TFC数据包：禁用<br>当前出站spi：B7B5B38B<br>当前入站spi：F0C4239D<br><br>入站esp sa：<br>spi：0xF0C4239D (4039386013)<br>SA状态：活动<br>转换：esp-aes-256 esp-sha-256-hmac无压缩<br>使用中的设置={L2L， Tunnel， IKEv2， VTI，}<br>插槽：0，conn_id：266，加密映射：__vti-crypto-map-Tunnel1-0-1<br>sa计时：剩余密钥生存期（kB/秒）：(4285389/3722)<br>IV大小：16字节 | ftdv742# show crypto ipsec sa<br><br>接口：demovti25<br>加密映射标记：__vti-crypto-map-Tunnel1-0-1，序列号：65280，本地地址：192.168.10.1<br><br>受保护的vrf (ivrf)：全球<br>本地ident（地址/掩码/端口）：(0.0.0.0/0.0.0.0/0/0)<br>远程ident （地址/掩码/端口）：(0.0.0.0/0.0.0.0/0/0)<br>current_peer： 192.168.30.1<br><br>#pkts encaps： 5721、#pkts encrypt： 5721、#pkts digest： 5721<br>#pkts decap：5721，#pkts decrypt：5721，#pkts verify：5721<br>#pkts压缩：0，#pkts解压缩：0<br>#pkts未压缩： 5721，#pkts comp失败：0，#pkts decomp失败： 0<br>#pre-frag成功：0，#pre-frag失败：0，#fragments已创建：0<br>发送#PMTUs：0，#PMTUs rcvd：0，需要重组的#decapsulated frg：0<br>#TFC rcvd：0，#TFC发送：0<br>#Valid ICMP错误rcvd：0，#Invalid ICMP错误rcvd：0<br>#send错误： 0，#recv错误： 0<br><br>本地加密终端：192.168.10.1/500，远程加密终端：192.168.30.1/500<br>路径mtu 1500、ipsec开销78(44)、媒体mtu 1500<br>PMTU剩余时间（秒）：0，DF策略：copy-df<br>ICMP错误验证：禁用，TFC数据包：禁用<br>当前出站spi：F0C4239D<br>当前入站spi：B7B5B38B<br><br>入站esp sa：<br>spi：0xB7B5B38B (3082138507)<br>SA状态：活动<br>转换：esp-aes-256 esp-sha-256-hmac无压缩<br>使用中的设置={L2L， Tunnel， IKEv2， VTI，}<br>插槽：0，conn_id：160，加密映射：__vti-crypto-map-Tunnel1-0-1<br>sa计时：剩余密钥生存期（kB/秒）：(3962829/3626)<br>IV大小：16字节 |

| | |
|---|---|
| 重播检测支持：Y<br>反重播位图：<br>0xFFFFFFFF 0xFFFFFFFF<br>出站esp sa：<br>spi：0xB7B5B38B (3082138507)<br>SA状态：活动<br>转换：esp-aes-256 esp-sha-256-hmac无压缩<br>使用中的设置={L2L， Tunnel， IKEv2， VTI， }<br>插槽：0，conn_id：266，加密映射：__vti-crypto-map-Tunnel1-0-1<br>sa计时：剩余密钥生存期（kB/秒）：(4147149/3722)<br>IV大小：16字节<br>重播检测支持：Y<br>反重播位图：<br>0x00000000 0x00000001 | 重播检测支持：Y<br>反重播位图：<br>0xFFFFFFFF 0xFFFFFFFF<br>出站esp sa：<br>spi：0xF0C4239D (4039386013)<br>SA状态：活动<br>转换：esp-aes-256 esp-sha-256-hmac无压缩<br>使用中的设置={L2L， Tunnel， IKEv2， VTI， }<br>插槽：0，conn_id：160，加密映射：__vti-crypto-map-Tunnel1-0-1<br>sa计时：剩余密钥生存期（kB/秒）：(4101069/3626)<br>IV大小：16字节<br>重播检测支持：Y<br>反重播位图：<br>0x00000000 0x00000001 |

第二步： 使用命令show bgp neighbors和show route bgp通过控制台或SSH导航到每个FTD的CLI以验证BGP状态。

| 站点1 FTD | 站点2 FTD |
|---|---|
| ftdv742# show bgp neighbors<br><br>BGP邻居是169.254.10.2，vrf single_vf，远程AS 65510，外部链路<br>BGP版本4，远程路由器ID 192.168.50.1<br>BGP状态=已建立，持续1d20h<br>上次读取时间为00:00:25，上次写入时间为00:00:45，保持时间为180，保持连接间隔为60秒<br>邻居会话：<br>1个活动，不支持多会话（已禁用）<br>邻居功能：<br>路由刷新：已通告和已接收（新）<br>四组八位组的ASN功能：已通告和已接收<br>地址系列IPv4单播：通告和接收<br>多会话功能：<br>邮件统计信息：<br>InQ深度为0<br>OutQ深度为0<br><br>发送的Rcvd<br>打开：1 1<br>通知：0 0<br>更新： 2 2 | ftdv742# show bgp neighbors<br><br>BGP邻居是169.254.10.1，vrf single_vf，远程AS 65511，外部链路<br>BGP版本4，远程路由器ID 192.168.70.1<br>BGP状态=已建立，持续1d20h<br>上次读取时间为00:00:11，上次写入时间为00:00:52，保持时间为180，保持连接间隔为60秒<br>邻居会话：<br>1个活动，不支持多会话（已禁用）<br>邻居功能：<br>路由刷新：已通告和已接收（新）<br>四组八位组的ASN功能：已通告和已接收<br>地址系列IPv4单播：通告和接收<br>多会话功能：<br>邮件统计信息：<br>InQ深度为0<br>OutQ深度为0<br><br>发送的Rcvd<br>打开：1 1<br>通知：0 0<br>更新： 2 2 |

| | |
|---|---|
| Keepalive： 2423 2427<br>路由刷新：0 0<br>合计：2426 2430<br>通告运行之间的默认最短时间为30秒<br><br>对于地址系列：IPv4单播<br>会话：169.254.10.2<br>BGP表版本3，邻居版本3/0<br>输出队列大小：0<br>索引1<br>1个更新组成员<br>发送的Rcvd<br>前缀活动：---- ----<br>当前前缀：1 1（消耗80字节）<br>前缀总数：1 1<br>隐式撤回： 0 0<br>显式撤消： 0 0<br>用作最佳路径：不适用1<br>用作多路径：n/a 0<br><br>出站入站<br>本地策略拒绝的前缀：-------- -------<br>来自此对等设备的最佳路径：1 n/a<br>合计：1 0<br>发送的更新中的NLRI数：最大1，最小0<br><br>启用了地址跟踪，RIB确实具有到169.254.10.2的路由<br>已建立连接1；已丢弃0<br>上次重置从不<br>传输(tcp) path-mtu-discovery已禁用<br>Graceful-Restart已禁用 | Keepalive： 2424 2421<br>路由刷新：0 0<br>合计：2427 2424<br>通告运行之间的默认最短时间为30秒<br><br>对于地址系列：IPv4单播<br>会话：169.254.10.1<br>BGP表版本9，邻居版本9/0<br>输出队列大小：0<br>索引4<br>4个更新组成员<br>发送的Rcvd<br>前缀活动：---- ----<br>当前前缀：1 1（消耗80字节）<br>前缀总数：1 1<br>隐式撤回： 0 0<br>显式撤消： 0 0<br>用作最佳路径：不适用1<br>用作多路径：n/a 0<br><br>出站入站<br>本地策略拒绝的前缀：-------- -------<br>来自此对等设备的最佳路径：1 n/a<br>合计：1 0<br>发送的更新中的NLRI数：最大1，最小0<br><br>启用了地址跟踪，RIB确实具有到169.254.10.1的路由<br>已建立连接4；已丢弃3<br>上次重置1d21h，由于会话1的接口摆动<br>传输(tcp) path-mtu-discovery已禁用<br>Graceful-Restart已禁用 |
| ftdv742# show route bgp<br><br>代码：L -本地，C -已连接，S -静态，R - RIP，M -移动，B - BGP<br>D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area<br>N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2<br>E1 - OSPF外部类型1，E2 - OSPF外部类型2，V - VPN<br>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2<br>ia - IS-IS inter area, * - candidate default, U - | ftdv742# show route bgp<br><br>代码：L -本地，C -已连接，S -静态，R - RIP，M -移动，B - BGP<br>D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area<br>N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2<br>E1 - OSPF外部类型1，E2 - OSPF外部类型2，V - VPN<br>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2<br>ia - IS-IS inter area, * - candidate default, U - |

| | |
|---|---|
| per-user static route<br>o - ODR，P -定期下载的静态路由，+ -复制路由<br>SI -静态InterVRF、BI - BGP InterVRF<br>Gateway of last resort is 192.168.30.3 to network 0.0.0.0<br>B 192.168.50.0 255.255.255.0 [20/0]（通过 169.254.10.2,1d20h） | per-user static route<br>o - ODR，P -定期下载的静态路由，+ -复制路由<br>SI -静态InterVRF、BI - BGP InterVRF<br>Gateway of last resort is 192.168.10.3 to network 0.0.0.0<br>B 192.168.70.0 255.255.255.0 [20/0]（通过 169.254.10.1,1d20h） |

第三步：Site1客户端和Site2客户端相互之间成功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
```

站点2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。

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
```

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>
```