Configure BGP over Route-Based VPN on FTD Managed by FDM

Contents

Introduction

This document describes configuring BGP over route-based site-to-site VPN on FTDv managed by FirePower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of VPN
- BGP configurations on FTDv
- Experience with FDM

Components Used

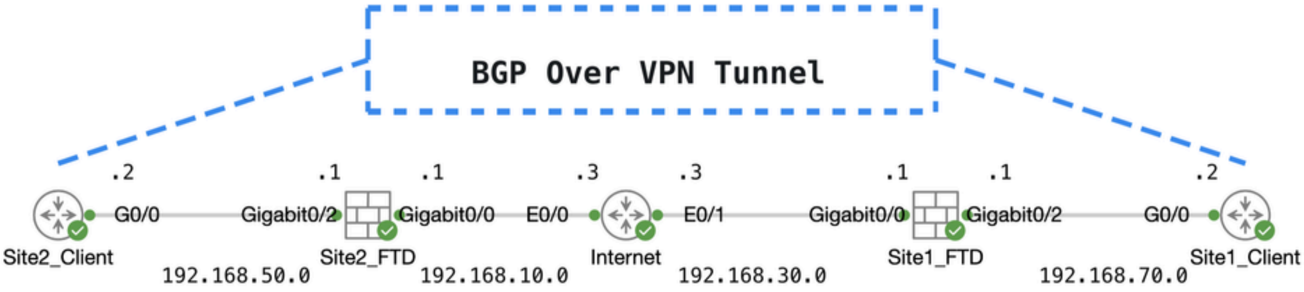
The information in this document is based on these software and hardware versions:

- Cisco FTDv version 7.4.2
- Cisco FDM version 7.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



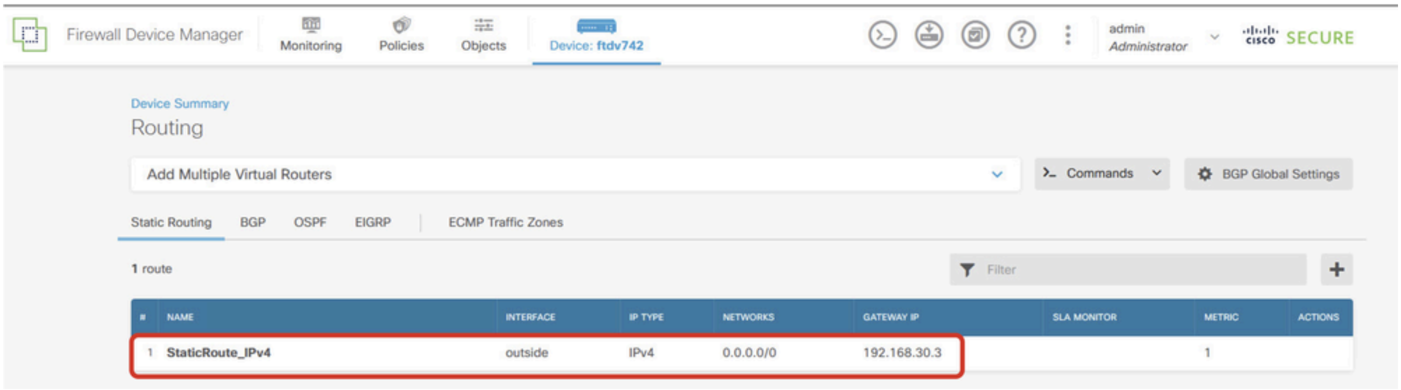
Topo

Configurations on VPN

Step 1. Ensure the IP interconnectivity between nodes is ready and stable. The smart license on FDM is registered with the smart account successfully.

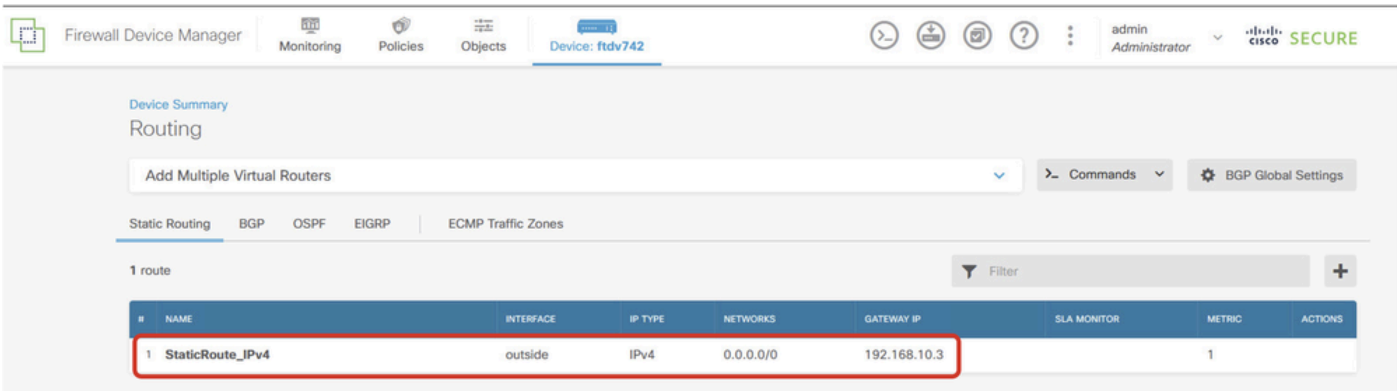
Step 2. The gateway of Site1 Client is configured with the inside IP address of Site1 FTD (192.168.70.1). The gateway of the Site2 client is configured with the inside IP address of Site2 FTD (192.168.50.1). Also, ensure the default route on both FTDs is configured correctly after FDM initialization.

Login to the GUI of each FDM. Navigate to Device > Routing . Click View Configuration . Click the **Static Routing** tab in order to verify the default static 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	

Site1_FTD_Gateway

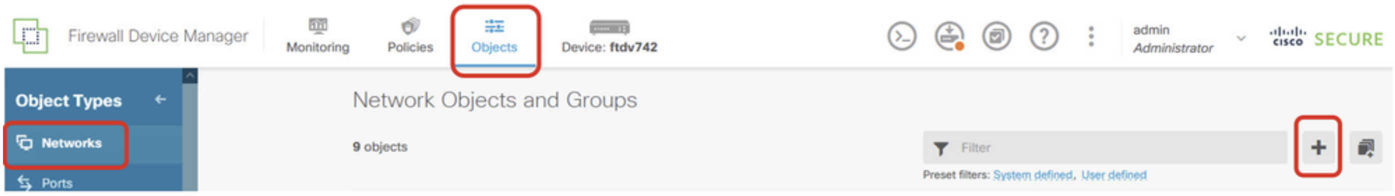


#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.10.3		1	

Site2_FTD_Gateway

Step 3. Configure route-based site-to-site VPN. In this example, first configure the Site1 FTD.

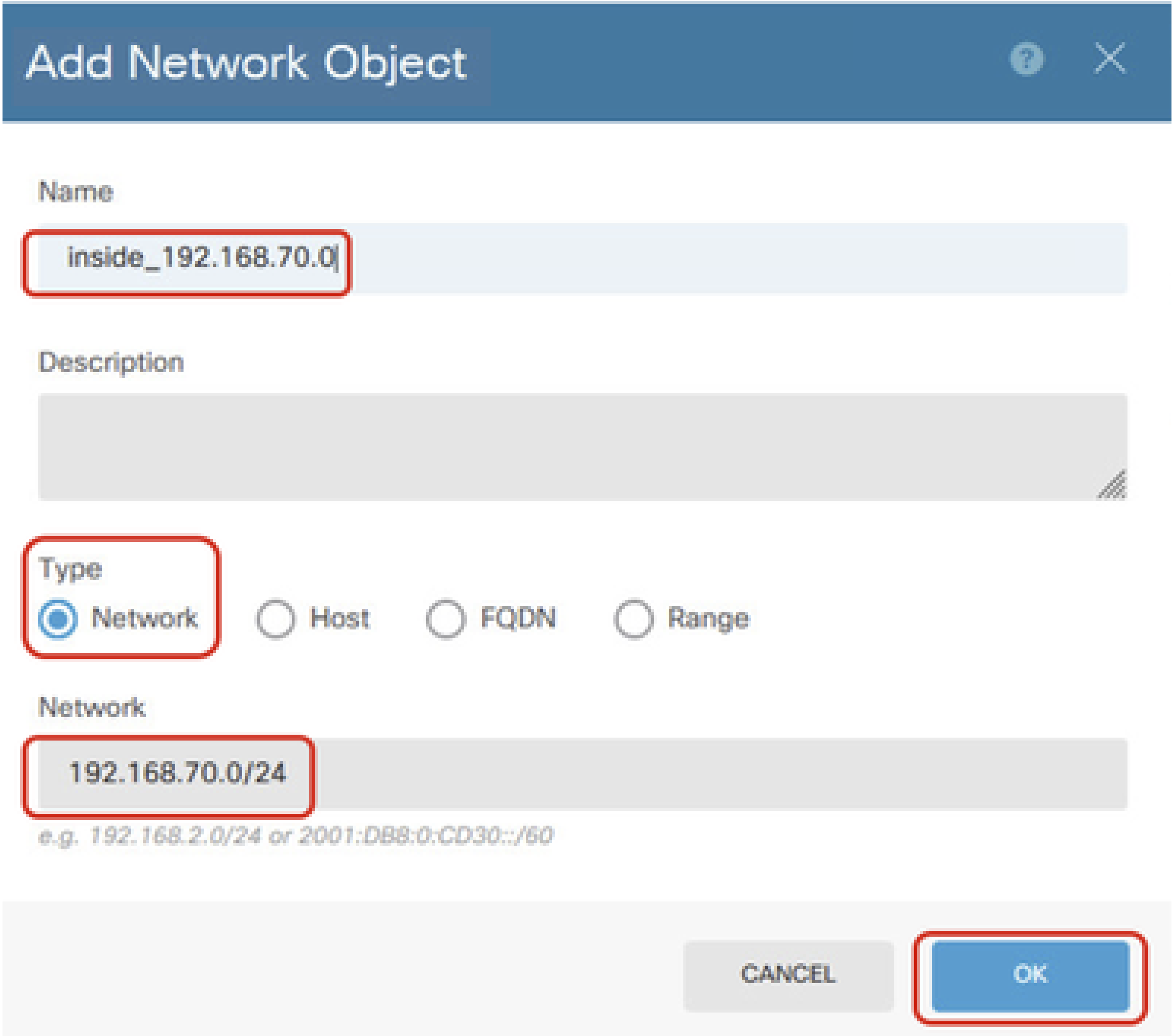
Step 3.1. Login to the FDM GUI of Site1 FTD. Create a new network object for the inside network of Site1 FTD. Navigate to **Objects** > **Networks**, click the + button.



Create_Network_Object

Step 3.2. Provide necessary information. Click the OK button.

- Name: inside_192.168.70.0
- Type: Network
- Network: 192.168.70.0/24


Add Network Object

Name

inside_192.168.70.0

Description

Type

● Network ○ Host ○ FQDN ○ Range

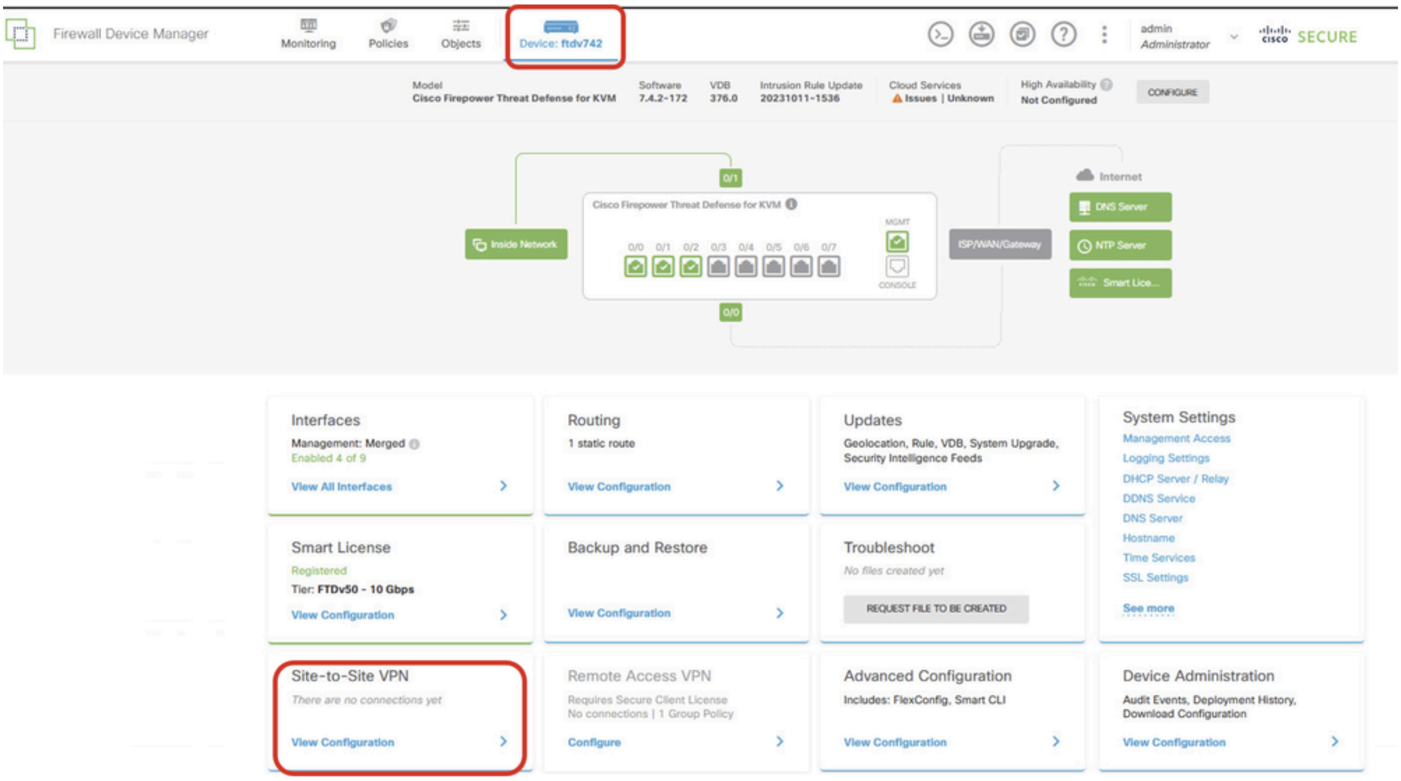
Network

192.168.70.0/24

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

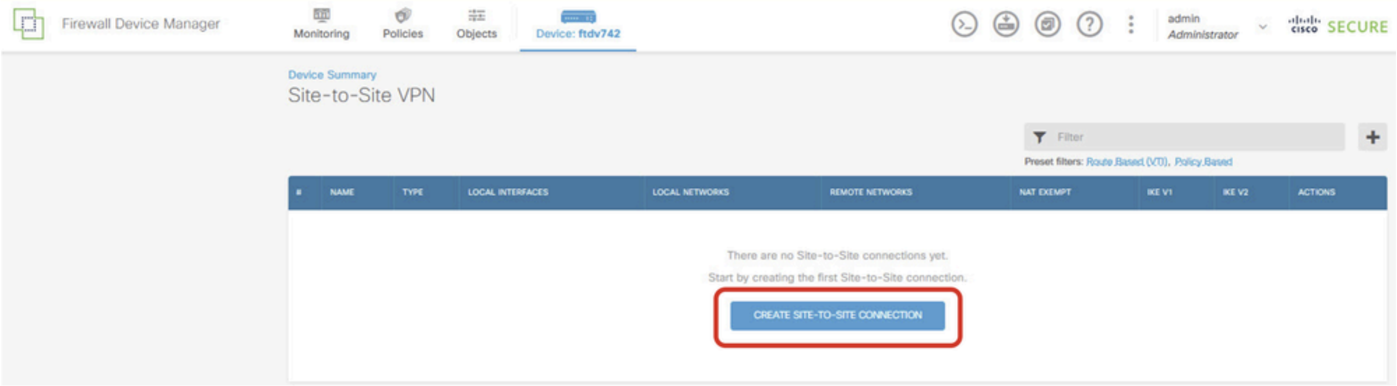
Site1_Inside_Network

Step 3.3. Navigate to **Device > Site-to-Site VPN** . Click **View Configuration** .



View Site-to-Site VPN

Step 3.4. Start to create a new site-to-site VPN. Click **CREATE SITE-TO-SITE CONNECTION** .



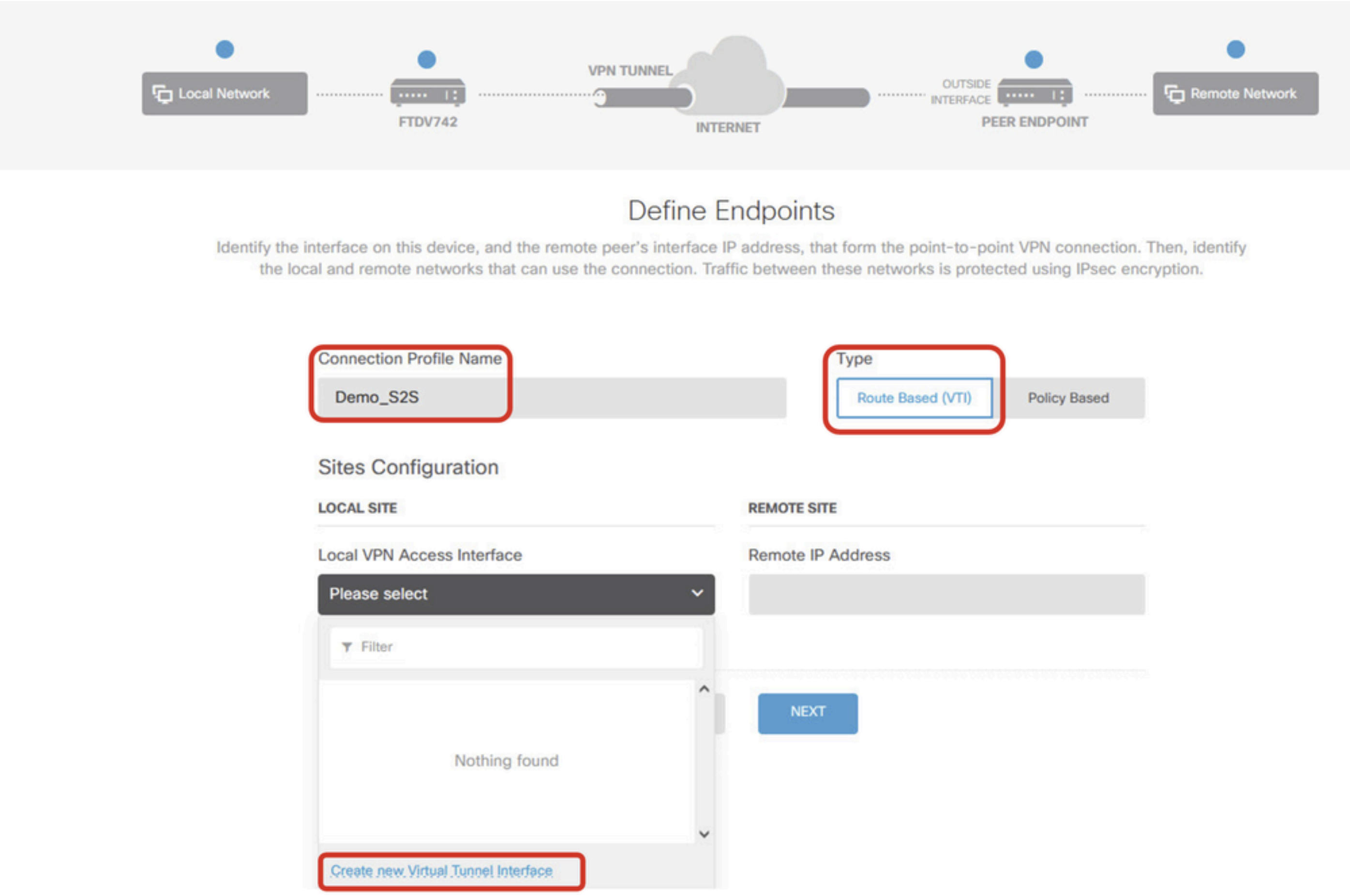
There are no Site-to-Site connections yet.

Start by creating the first Site-to-Site connection.

Create_Site-to-Site_Connection

Step 3.5. Provide the necessary information.

- Connection Profile Name: Demo_S2S
- Type: Route Based (VTI)
- Local VPN Access Interface: click the dropdown list, then click **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

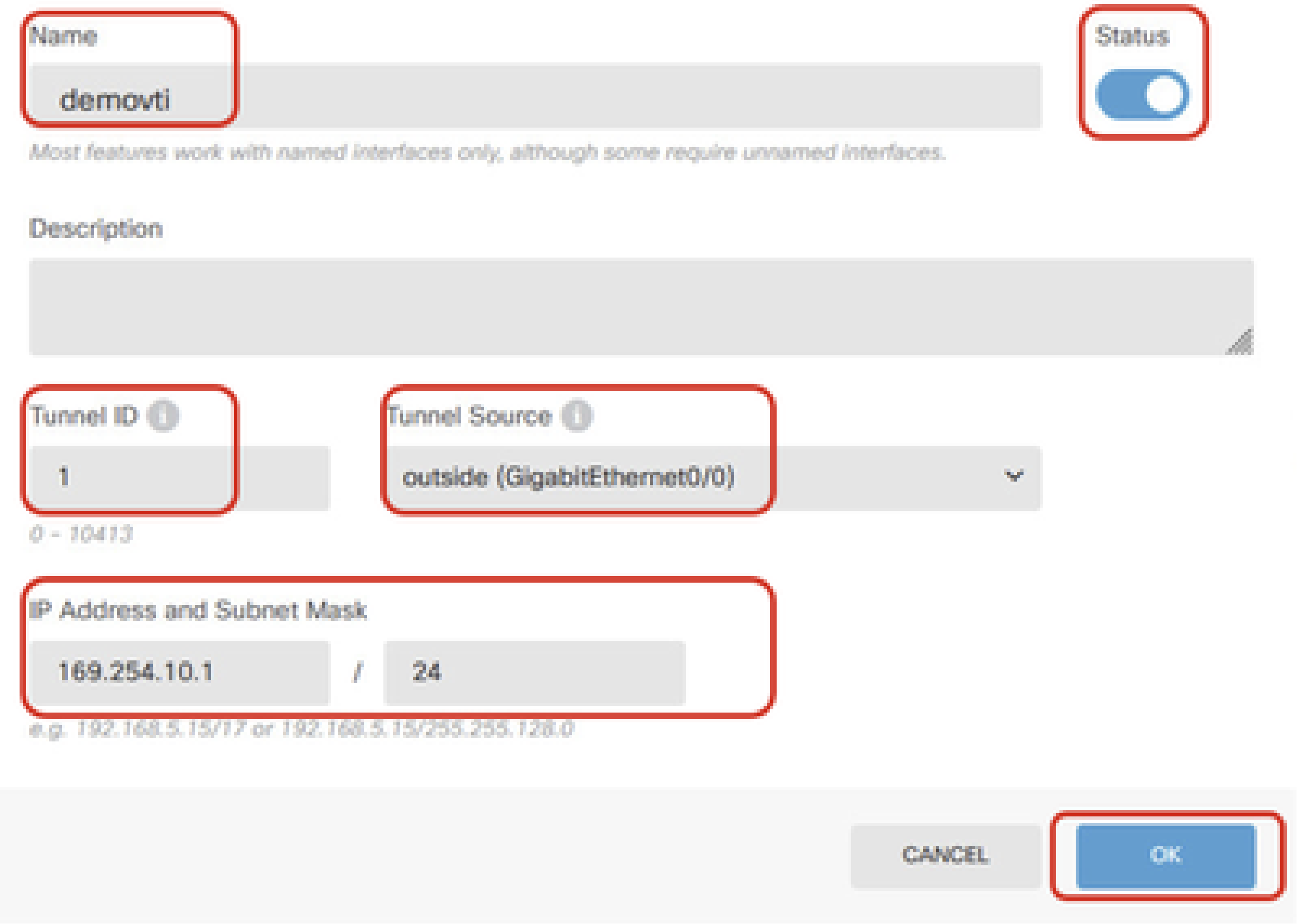
REMOTE SITE

Remote IP Address

Create_VTI_in_VPN_Wizard

Step 3.6. Provide the necessary information in order to create a new VTI. Click the **OK** button.

- Name: demovti
- Tunnel ID: 1
- Tunnel Source: outside (GigabitEthernet0/0)
- IP Address And Subnet Mask: 169.254.10.1/24
- Status: click the slider to the Enabled position



Name: demovti

Status

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

Description

Tunnel ID: 1

0 - 10413

Tunnel Source: outside (GigabitEthernet0/0)

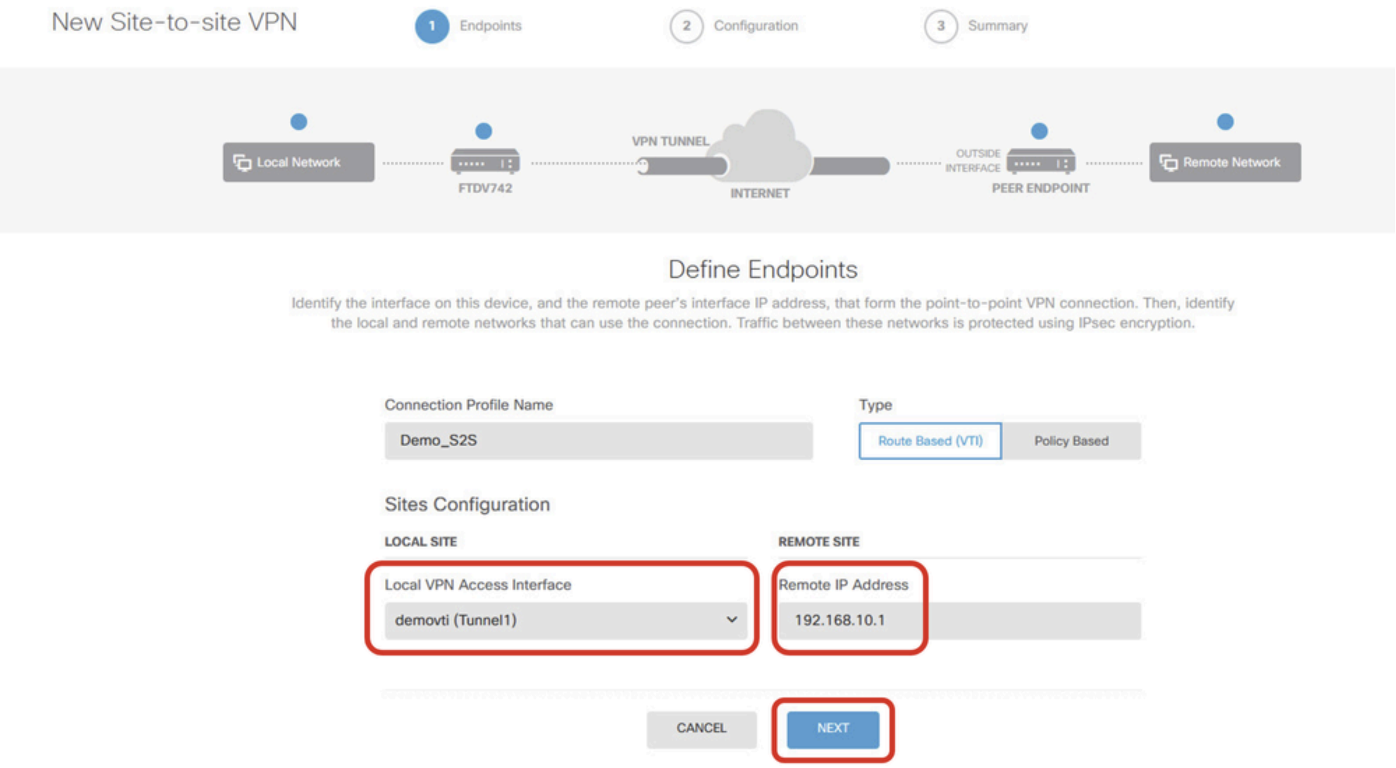
IP Address and Subnet Mask: 169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Create_VTI_Details

Step 3.7. Continue to provide the necessary information. Click the **NEXT** button.

- Local VPN Access Interface: demovti (created in Step 3.6.)
- Remote IP Address: 192.168.10.1



New Site-to-site VPN

1 Endpoints — 2 Configuration — 3 Summary

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)

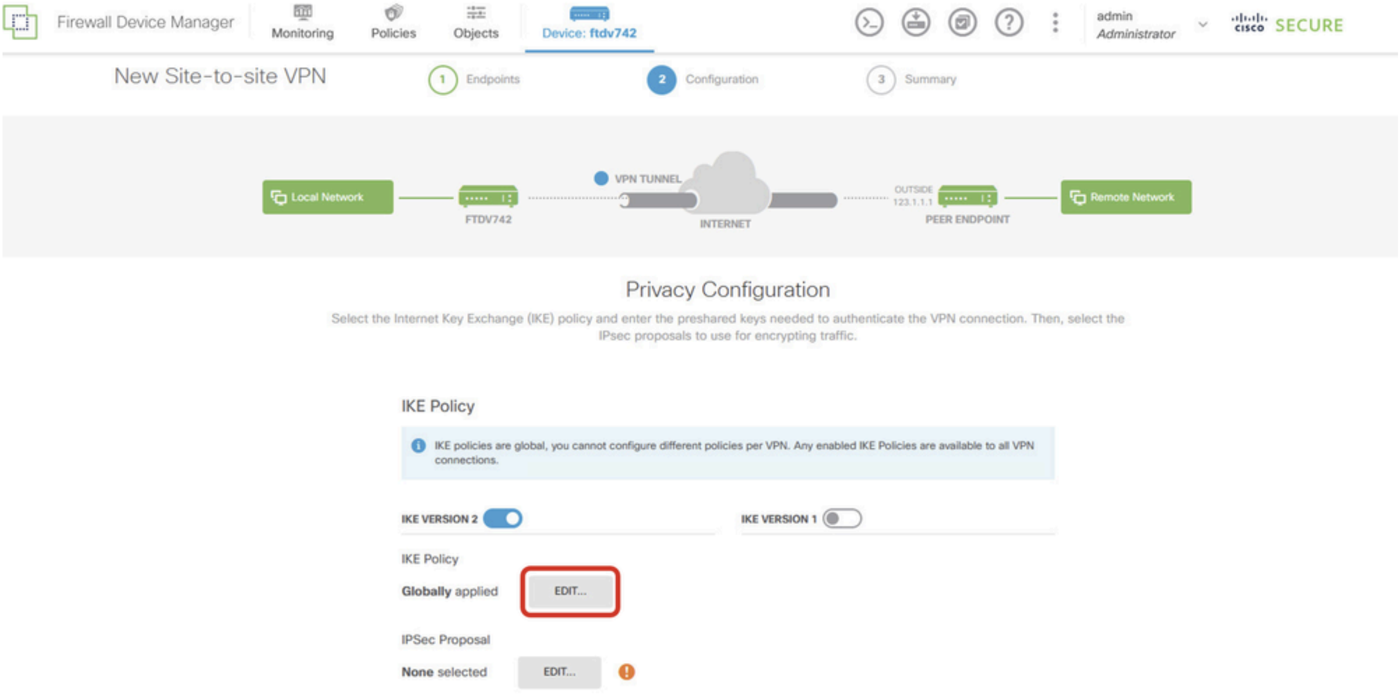
REMOTE SITE

Remote IP Address: 192.168.10.1

CANCEL NEXT

VPN_Wizard_Endpoints_Step1

Step 3.8. Navigate to IKE Policy. Click the **EDIT** button.



New Site-to-site VPN

1 Endpoints — 2 Configuration — 3 Summary

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...

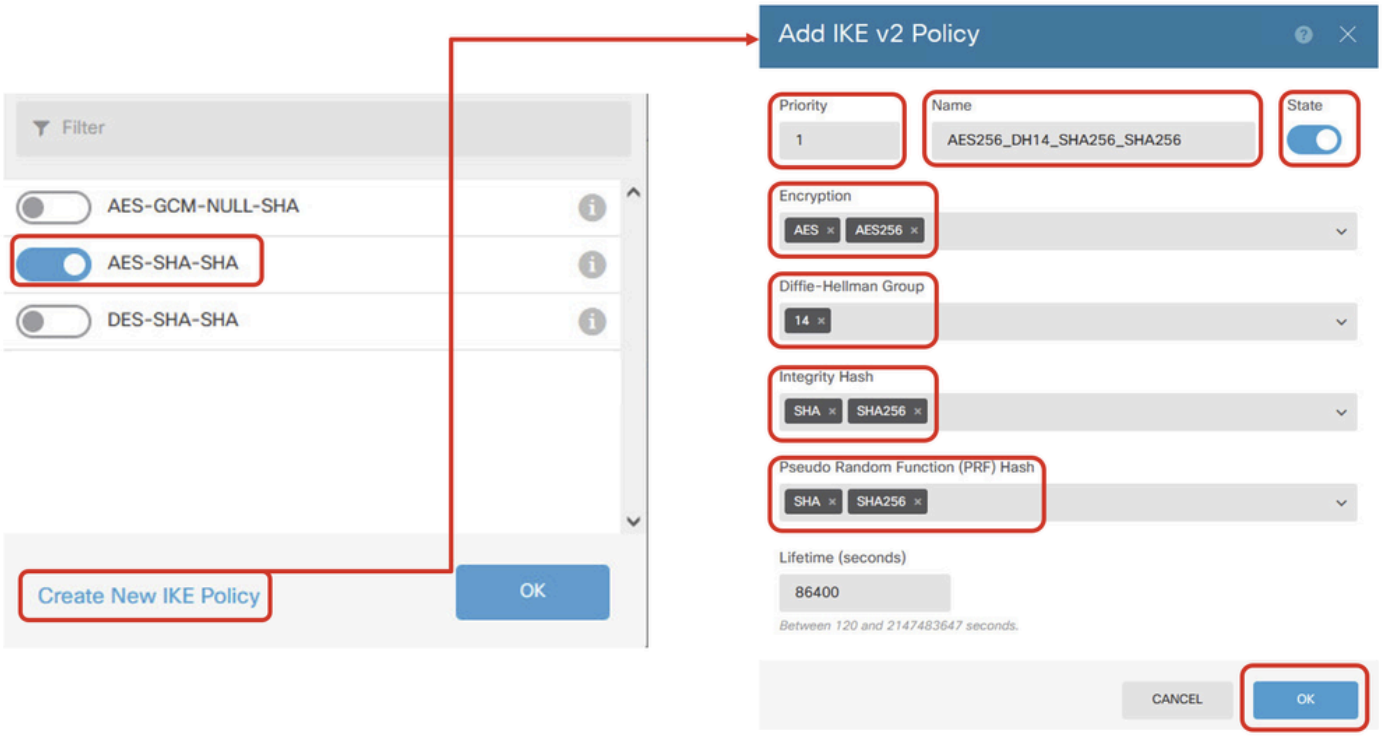
IPSec Proposal: None selected EDIT...

Edit_IKE_Policy

Step 3.9. For the IKE policy, you can use a pre-defined one or create a new one by clicking **Create New IKE Policy**.

In this example, toggle an existing IKE policy **AES-SHA-SHA** and also create a new one for demo purposes. Click the **OK** button in order to save.

- Name: AES256_DH14_SHA256_SHA256
- Encryption: AES, AES256
- DH Group: 14
- Integrity Hash: SHA, SHA256
- PRF Hash: SHA, SHA256
- Lifetime: 86400 (default)



○ AES-GCM-NULL-SHA

● AES-SHA-SHA

○ DES-SHA-SHA

Priority: 1

Name: AES256_DH14_SHA256_SHA256

State: ●

Encryption: AES × AES256 ×

Diffie-Hellman Group: 14 ×

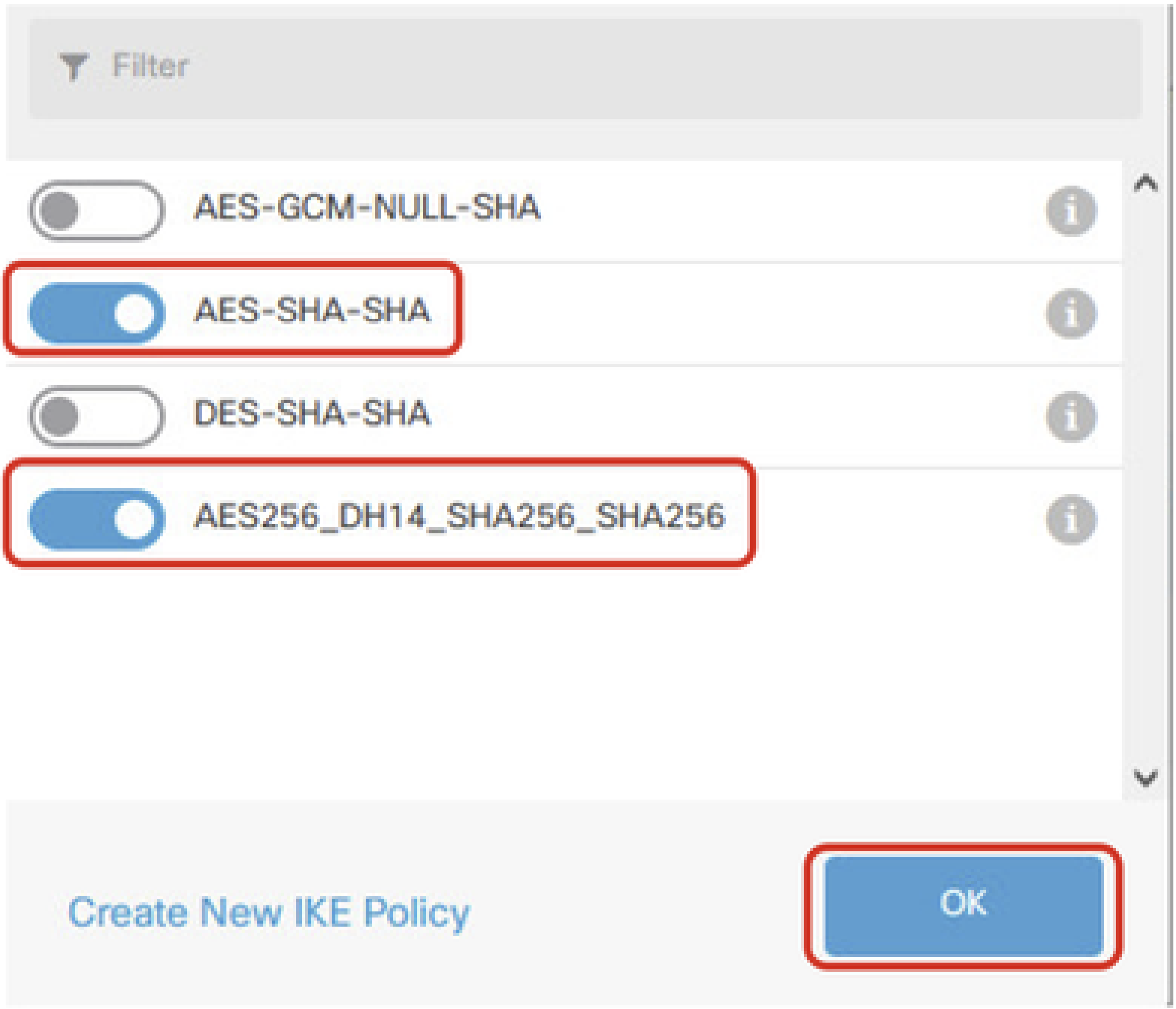
Integrity Hash: SHA × SHA256 ×

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

Lifetime (seconds): 86400

Between 120 and 2147483647 seconds.

Add_New_IKE_Policy



○ AES-GCM-NULL-SHA

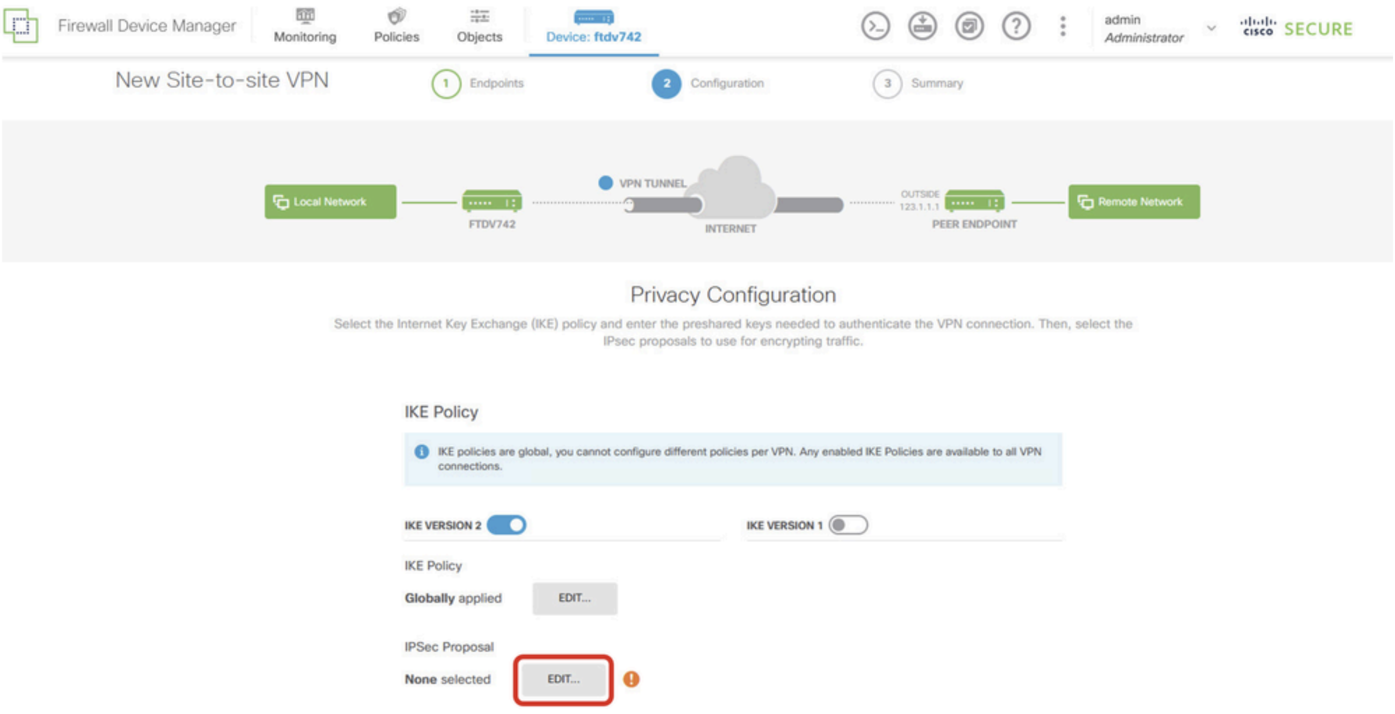
● AES-SHA-SHA

○ DES-SHA-SHA

● AES256_DH14_SHA256_SHA256

Enable_New_IKE_Policy

Step 3.10. Navigate to the IPSec Proposal. Click the **EDIT** button.



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

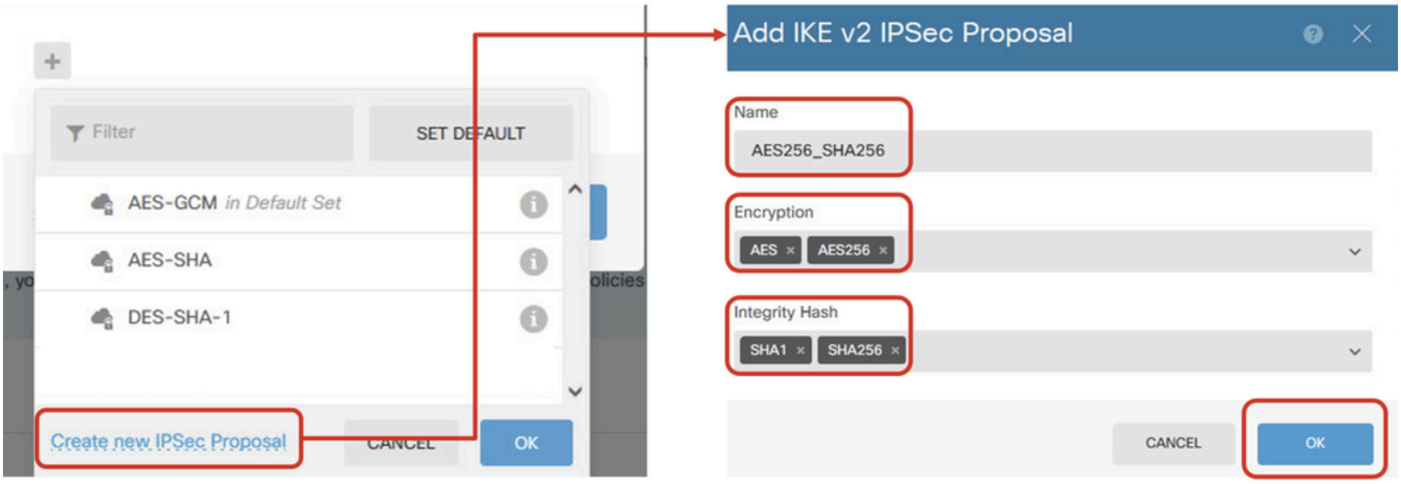
IKE Policy: **Globally** applied

IPSec Proposal: **None** selected

Edit_IKE_Proposal

Step 3.11. For the IPSec proposal, you can use a pre-defined or you can create a new one by clicking **Create new IPSec Proposal**. In this example, create a new one for demo purposes. Provide the necessary information. Click the **OK** button in order to save.

- Name: AES256_SHA256
- Encryption: AES, AES256
- Integrity Hash: SHA1, SHA256



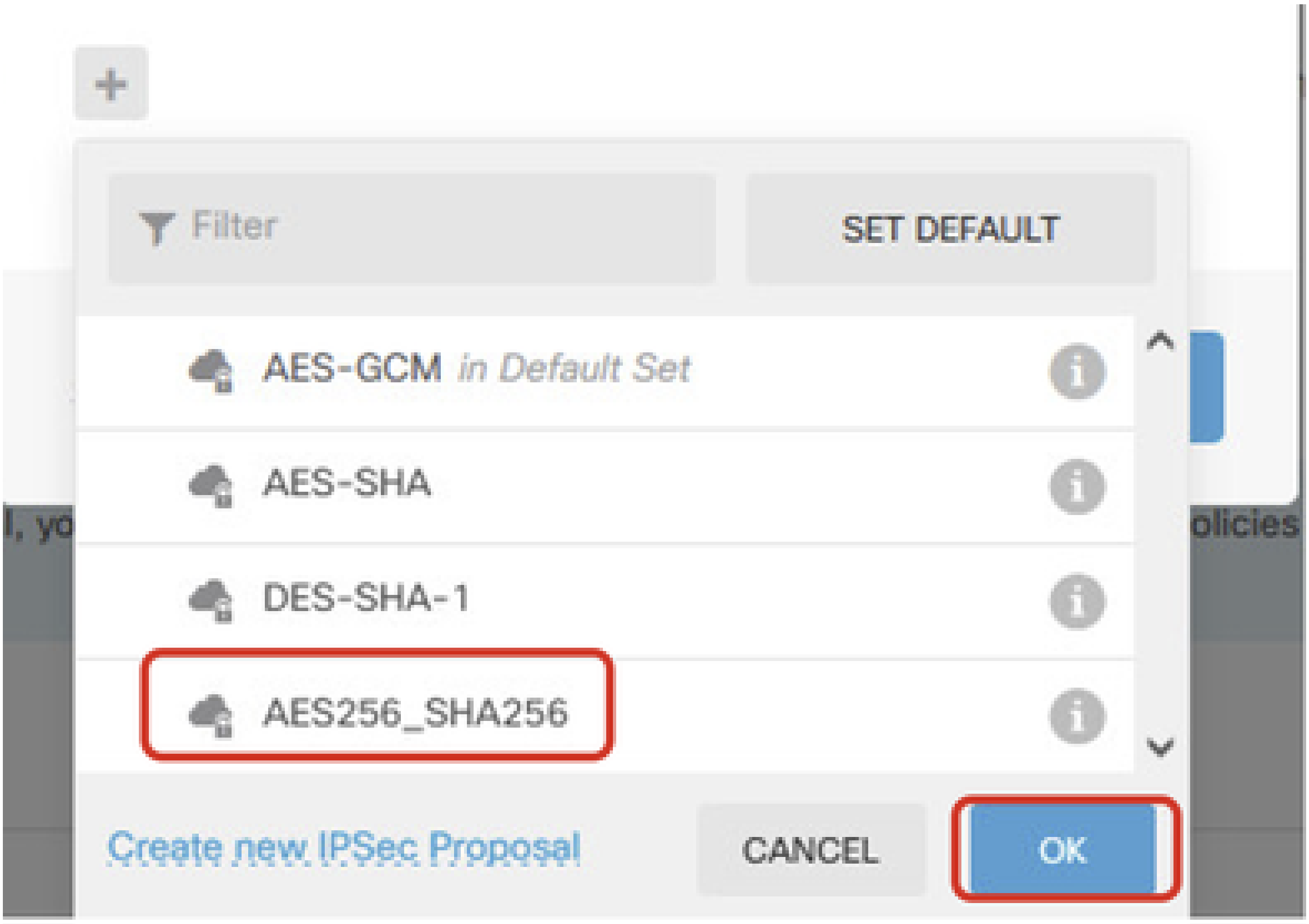
Add IKE v2 IPSec Proposal

Name: AES256_SHA256

Encryption: AES × AES256 ×

Integrity Hash: SHA1 × SHA256 ×

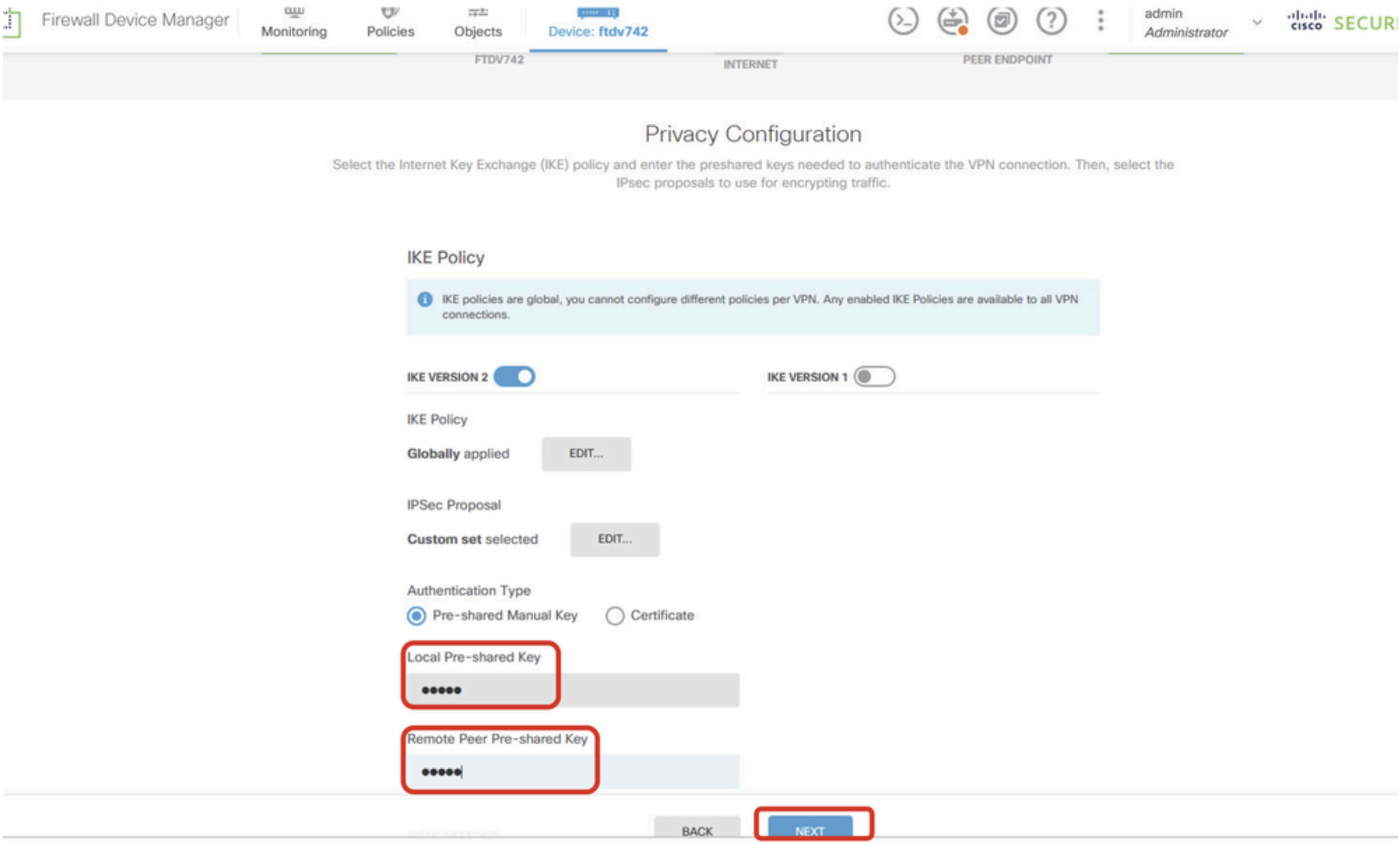
Add_New_IPSec_Proposal



Enable_New_IPSec_Proposal

Step 3.12. Configure the pre-shared key. Click the **NEXT** button.

Note down this pre-shared key and configure it on the Site2 FTD later.



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

IPSec Proposal: **Custom set** selected

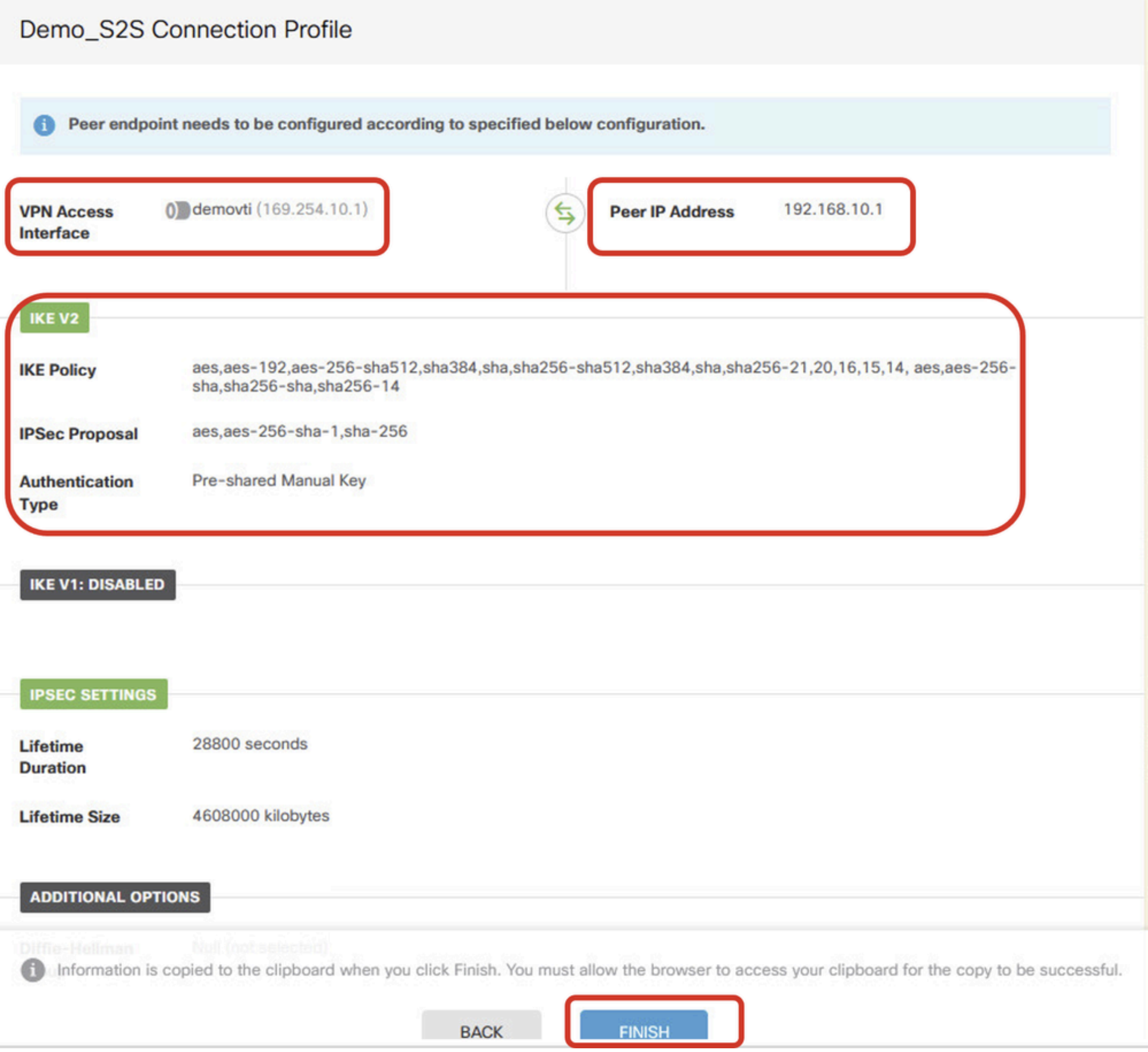
Authentication Type: ● Pre-shared Manual Key ○ Certificate

Local Pre-shared Key: ●●●●●

Remote Peer Pre-shared Key: ●●●●●

Configure_Pre_Shared_Key

Step 3.13. Review the VPN configuration. If anything needs to be modified, click the **BACK** button. If everything is good, click the **FINISH** button.



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

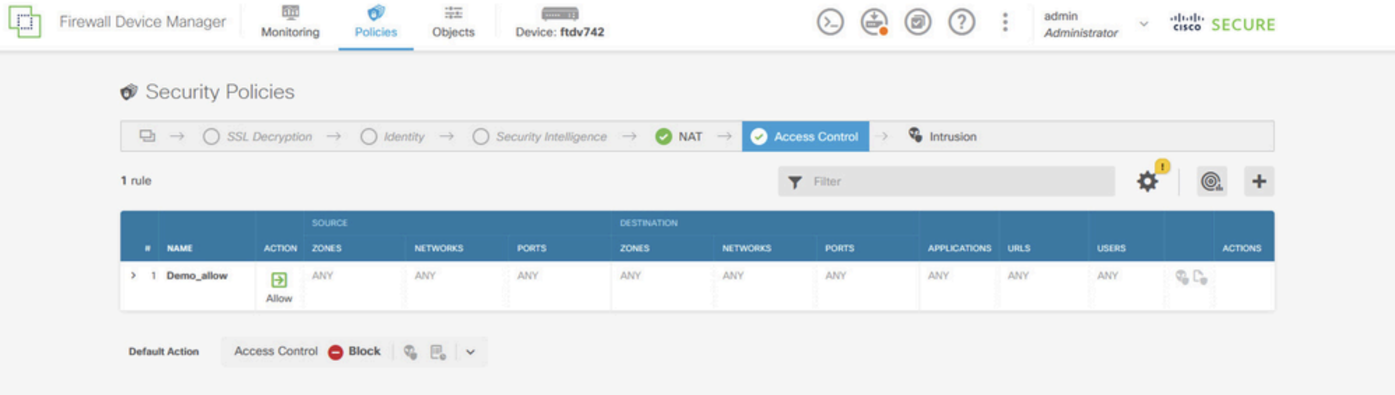
ADDITIONAL OPTIONS

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

Step 3.14. Create an Access Control rule in order to allow traffic to pass through the FTD. In this example, allow all for demo purposes. Modify your policy based on your actual needs.



1 rule

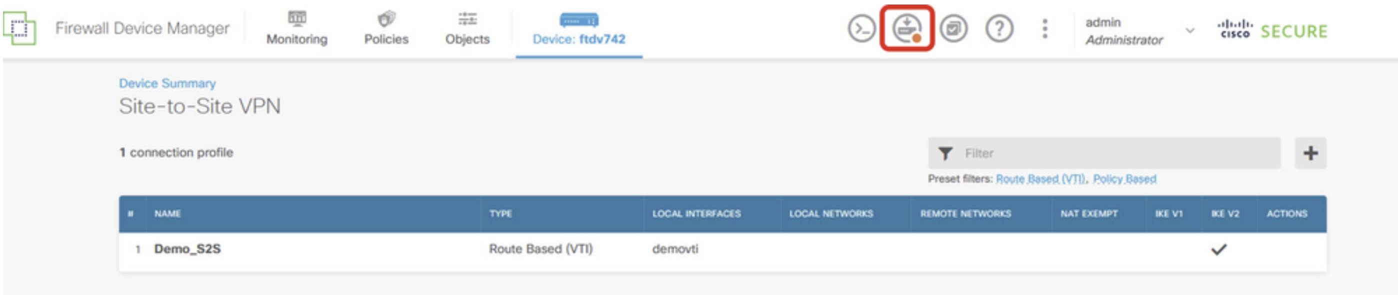
			SOURCE			DESTINATION						
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	

Default Action: Access Control Block

Access_Control_Rule_Example

Step 3.15. (Optional) Configure NAT exempt rule for the client traffic on FTD if dynamic NAT is configured for the client in order to access the internet. In this example, there is no need to configure a NAT-exempt rule because no dynamic NAT is configured on each FTD.

Step 3.16. Deploy the configuration changes.



Device Summary

Site-to-Site VPN

1 connection profile

Filter

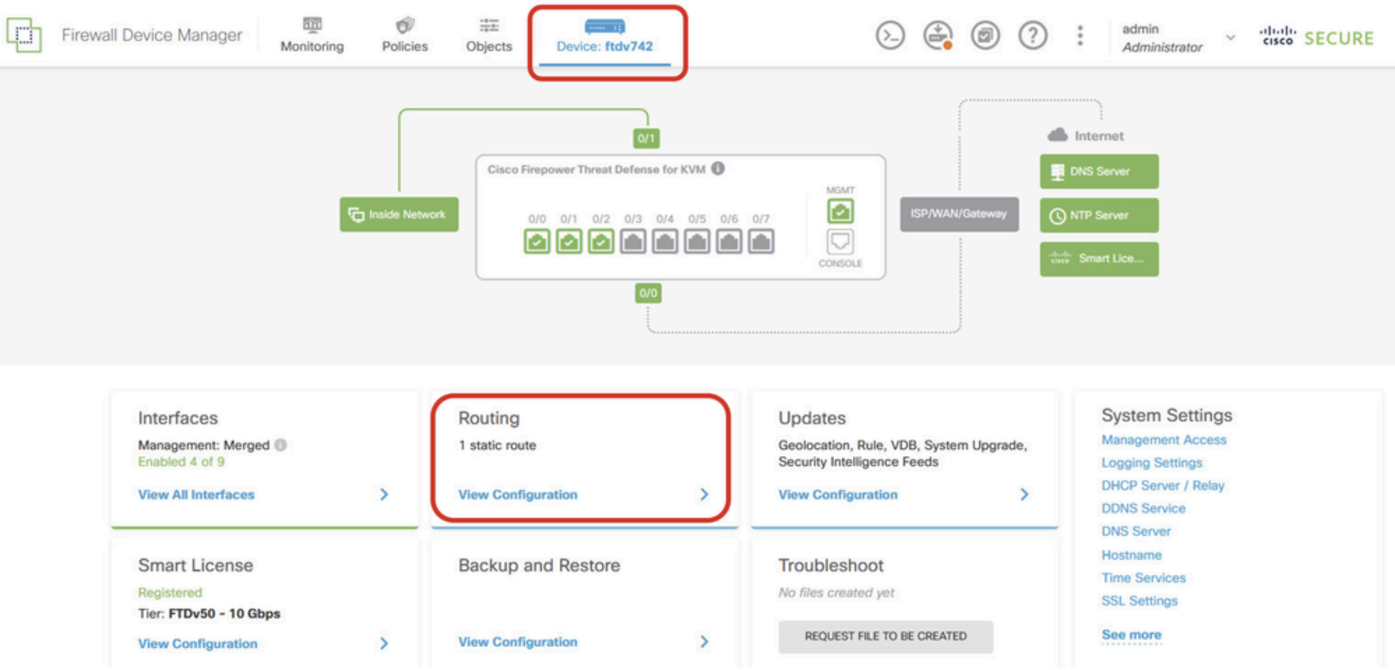
Preset filters: Route Based (VTI), Policy Based

#	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

Configurations on BGP

Step 4. Navigate to **Device** > **Routing**. Click **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

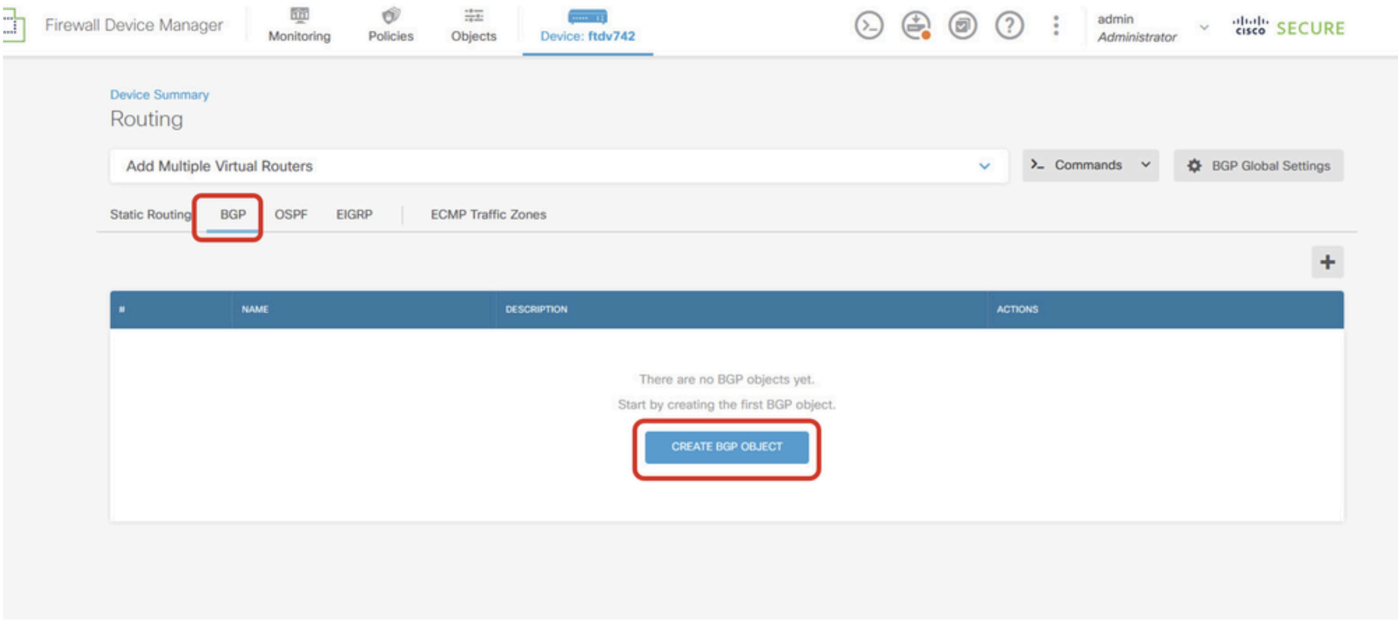
Smart License
Registered
Tier: FTDv50 - 10 Gbps
View Configuration

Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

View_Routing_Configuration

Step 5. Click the **BGP** tab and then click **CREATE BGP OBJECT**.



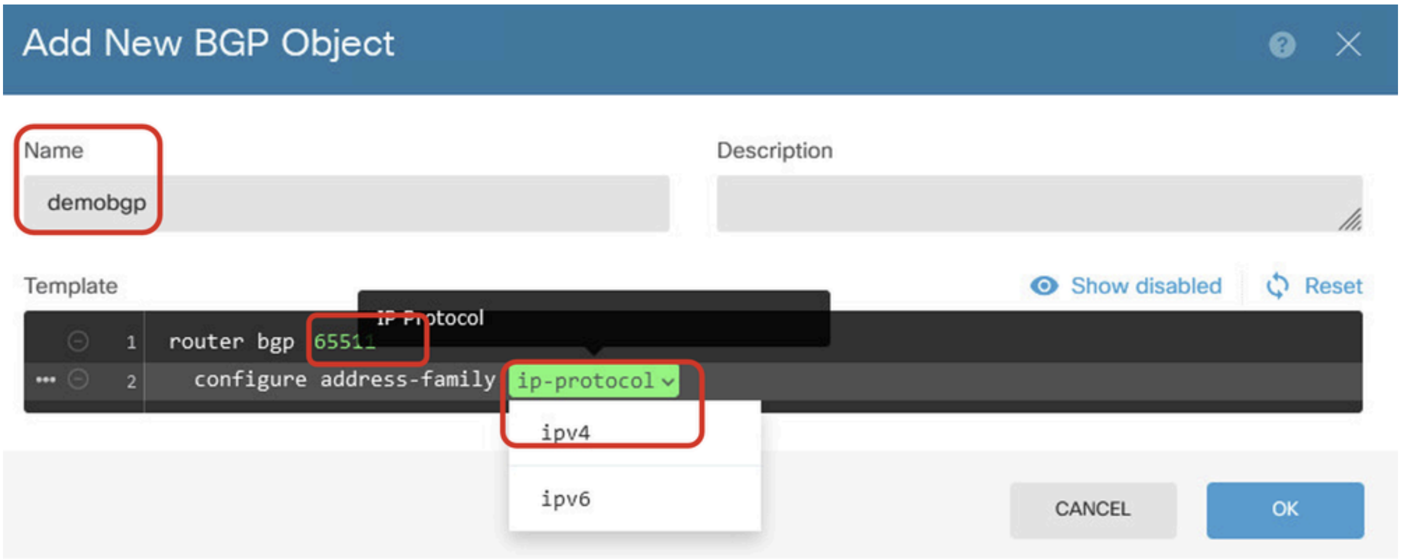
Create_BGP_Object

Step 6. Provide the name of the object. Navigate to **Template** and configure. Click the **OK** button to save.

Name: demobgp

Line 1: Configure AS number. Click **as-number**. Manual input local AS number. In this example, AS number 65511 for Site1 FTD.

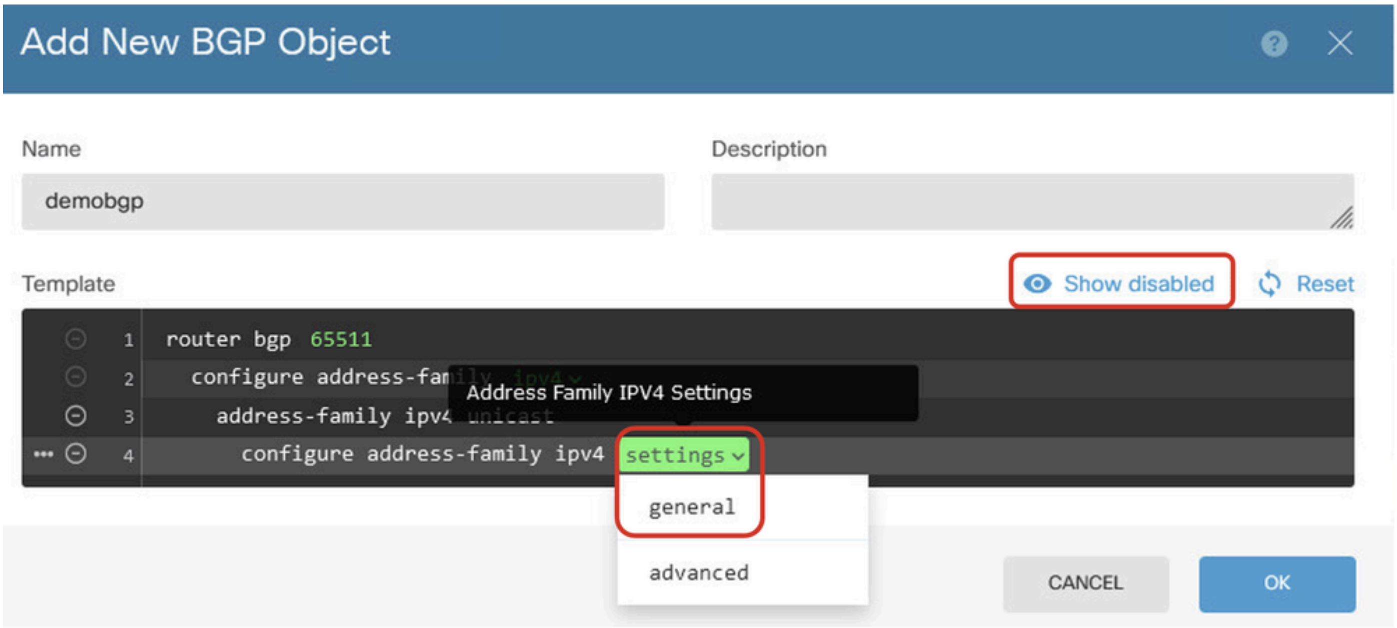
Line 2: Configure IP protocol. Click **ip-protocol**. Select **ipv4**.



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

Create_BGP_Object_ASNumber_Protocol

Line 4: Configure more settings. Click **settings**, choose **general**, and then click **Show disabled**.



Name: demobgp

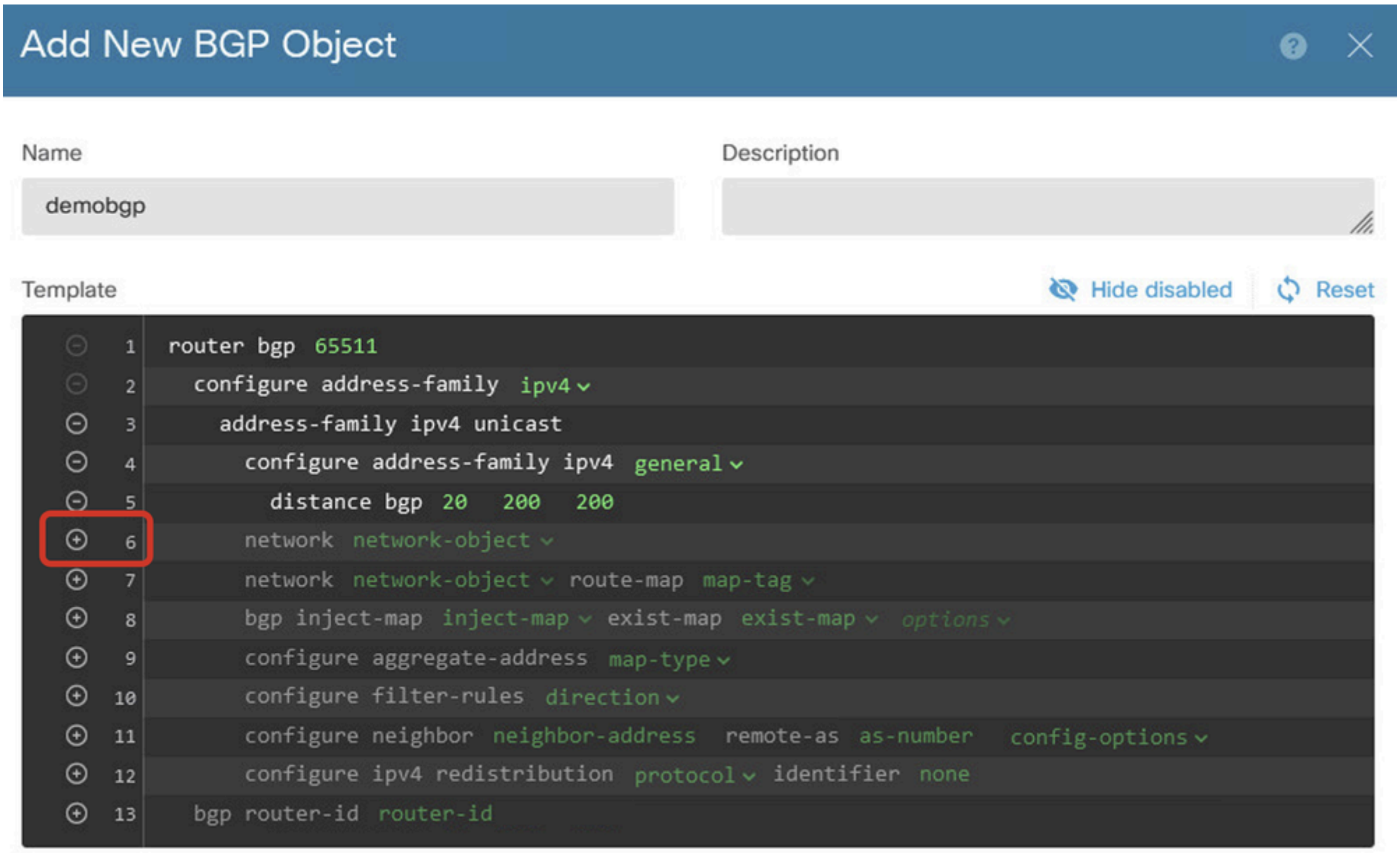
Description:

Template

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

Create_BGP_Object_AddressSetting

Line 6: Click the + icon in order to enable the line to configure the BGP network. Click **network-object**. You can see the existing available objects and choose one. In this example, choose the object name **inside_192.168.70.0** (created in Step 3.2.).



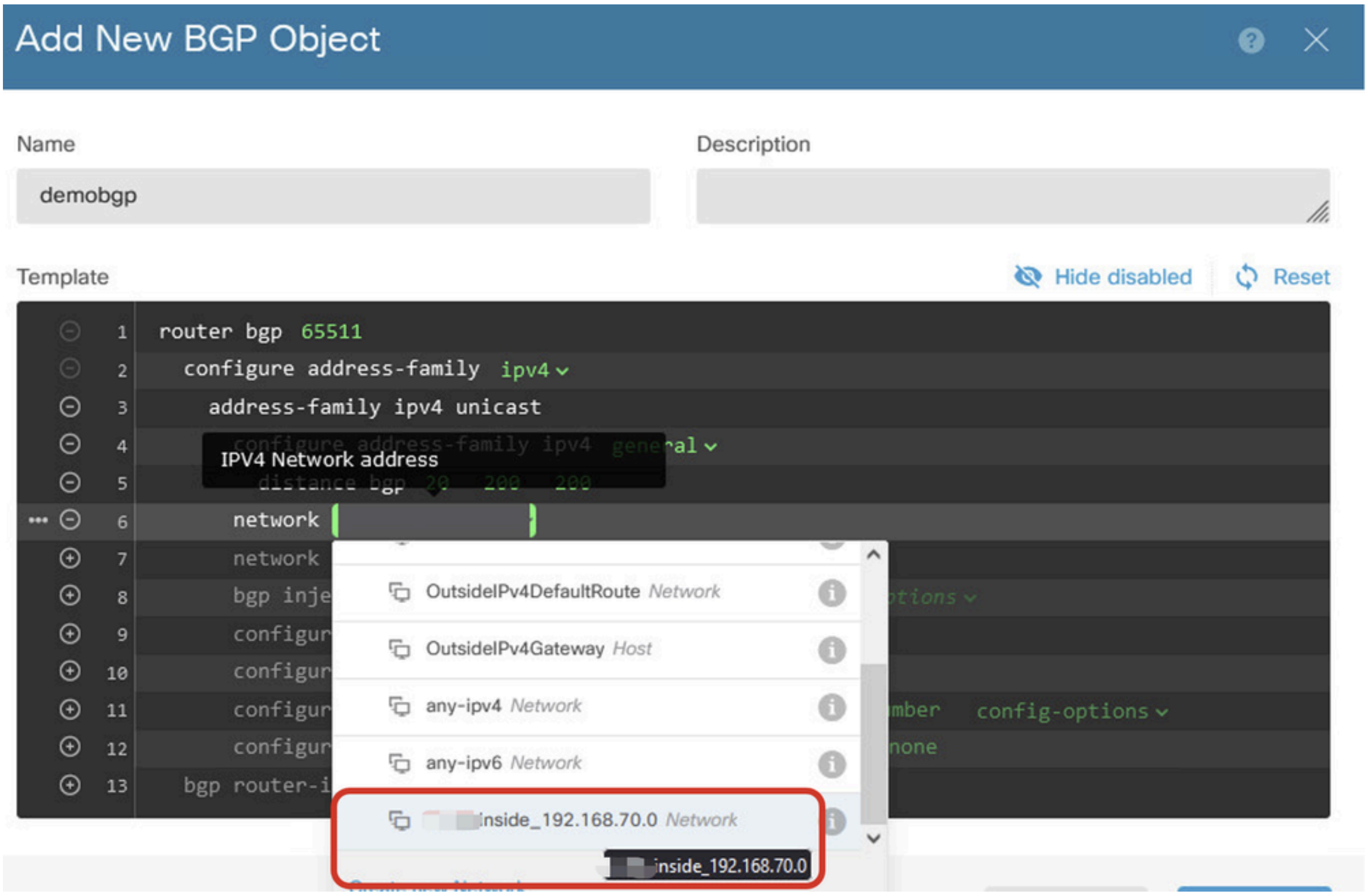
Name: demobgp

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 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

```
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                                        tions
9        configur
10       configur
11       configur                                   mber  config-options
12       configur                                   none
13     bgp router-i
```

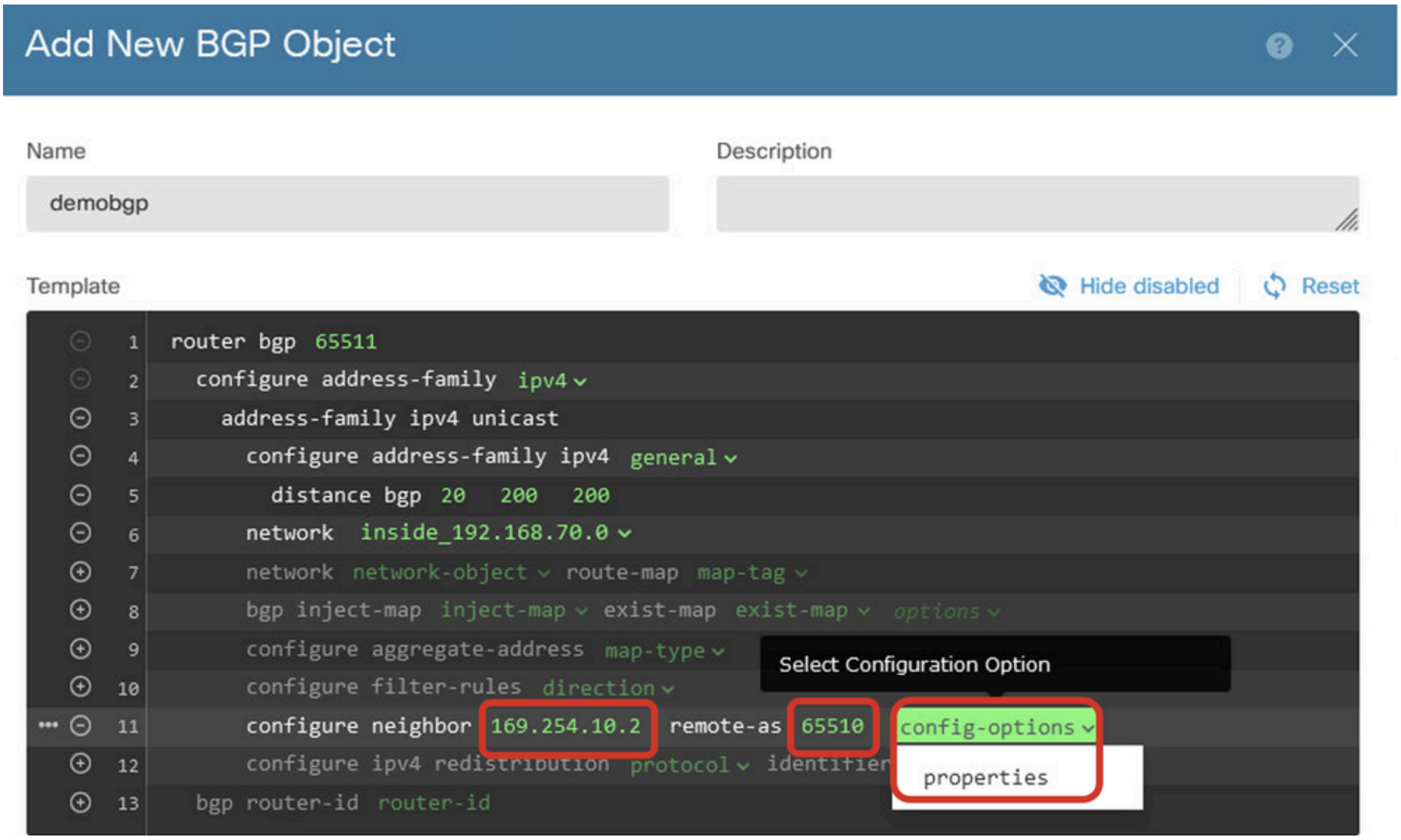
IPV4 Network address

- 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

Line 11: Click the + icon in order to enable the line to configure the BGP neighbor-related information. Click **neighbor-address**, and manually input the peer BGP neighbor address. In this example, it is 169.254.10.2 (VTI IP address of Site2 FTD). Click **as-number**, and manually input the peer AS number. In this example, 65510 is for Site2 FTD. Click **config-options** and choose **properties**.



Add New BGP Object

Name: demobgp

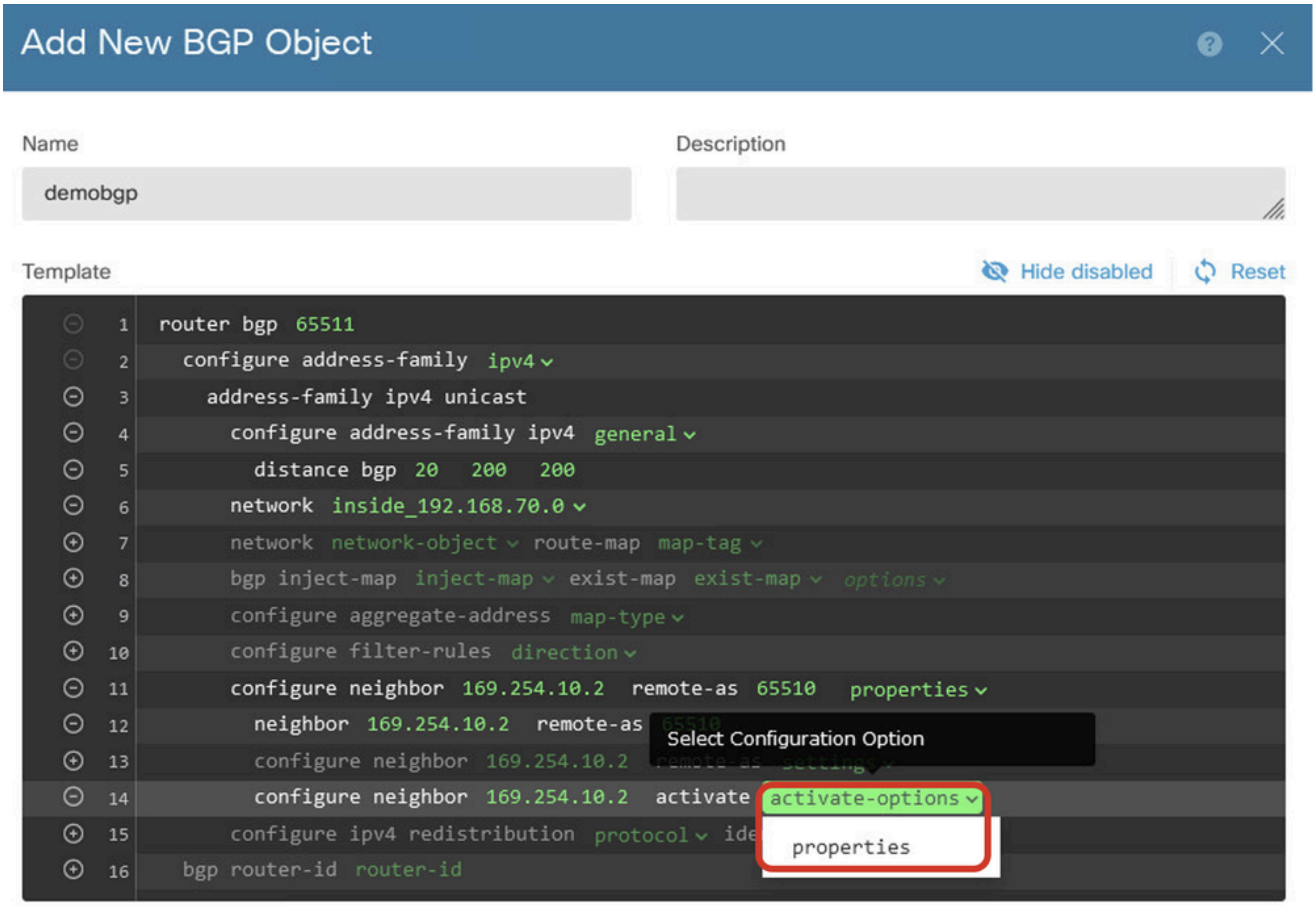
Description:

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

Line 14: Click the + icon in order to enable the line to configure some properties of the neighbor. Click **activate-options** and choose **properties**.



Add New BGP Object

Name: demobgp

Description:

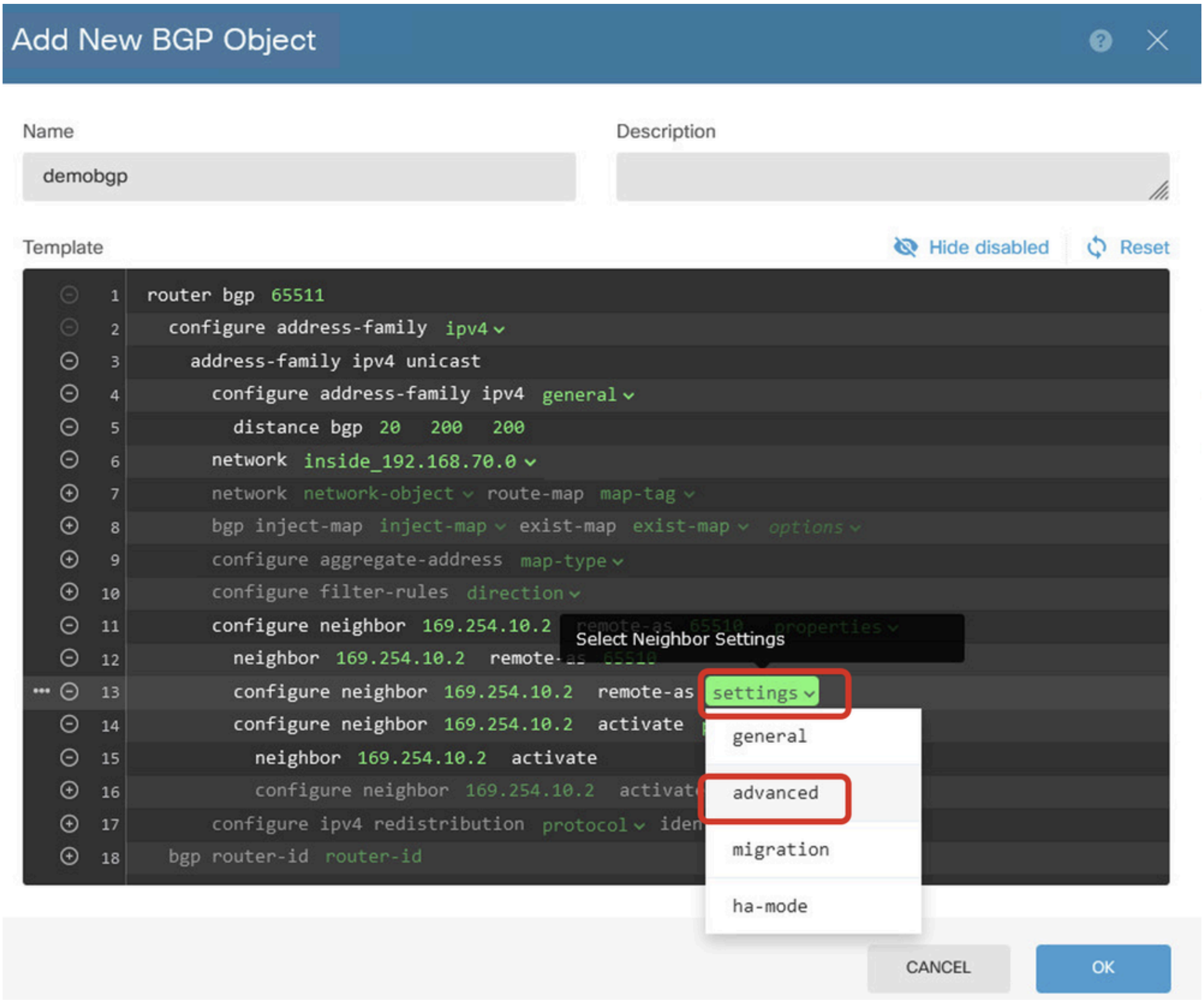
Template

Hide disabled Reset

```
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

Line 13: Click the + icon in order to enable the line to show advanced options. Click **settings** and choose **advanced**.



Add New BGP Object

Name: demobgp

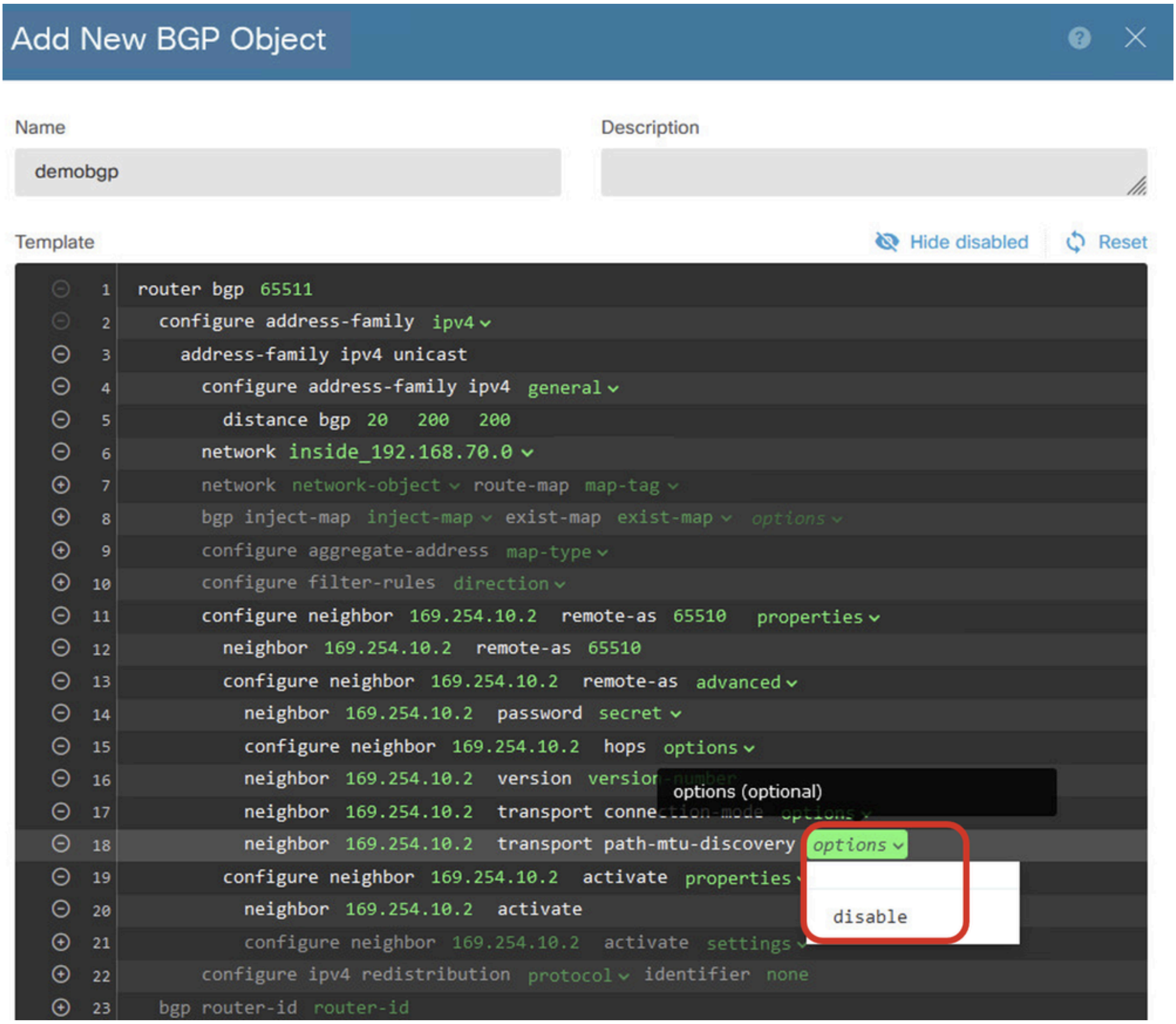
Description:

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
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

Line 18: Click **options** and choose **disable** in order to disable path MTU discovery.



Name: demobgp

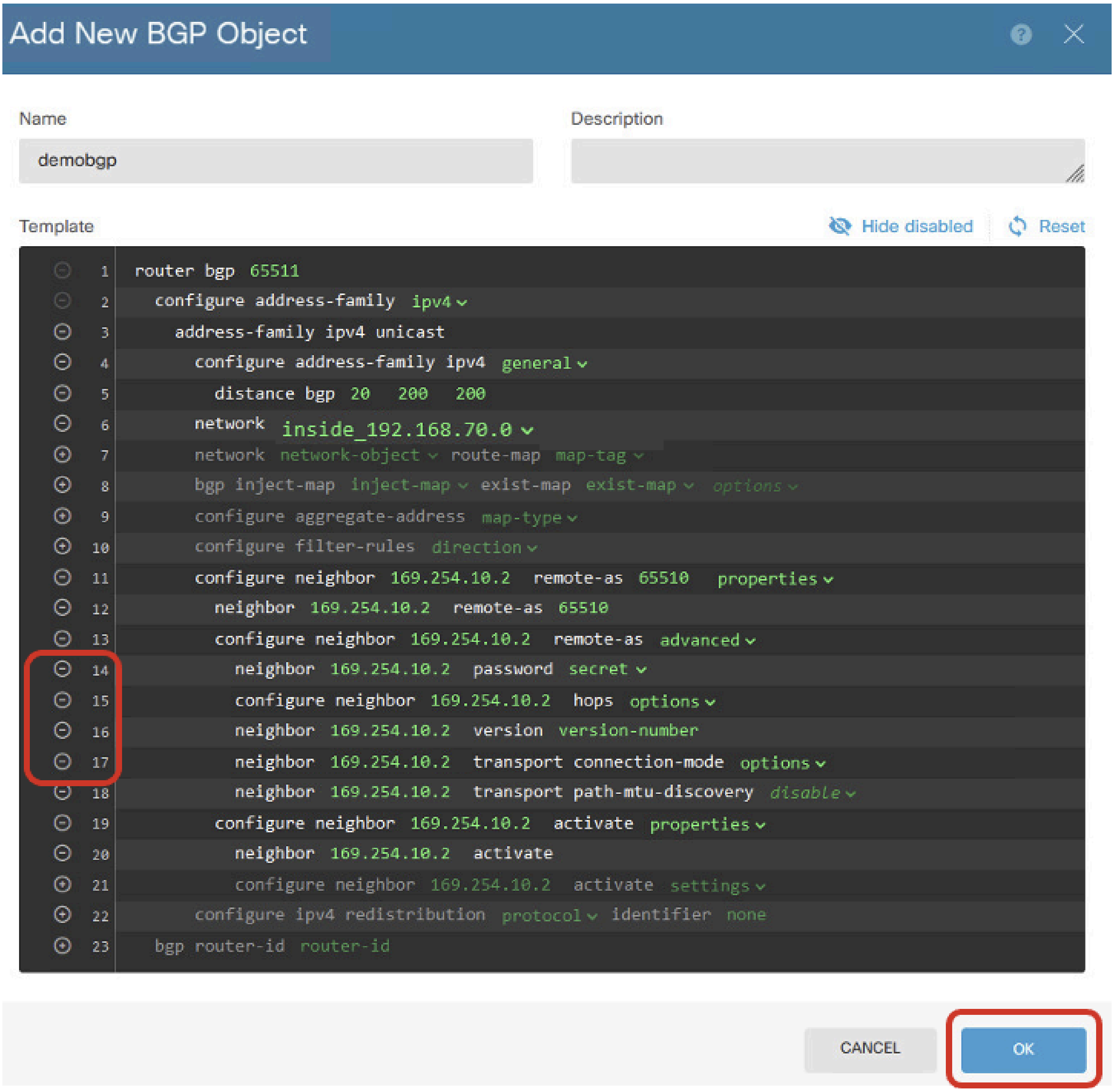
Description:

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

Line 14, 15, 16, 17: Click the **-** button in order to disable the lines. Then, click the **OK** button to save the BGP object.



Add New BGP Object

Name: demobgp

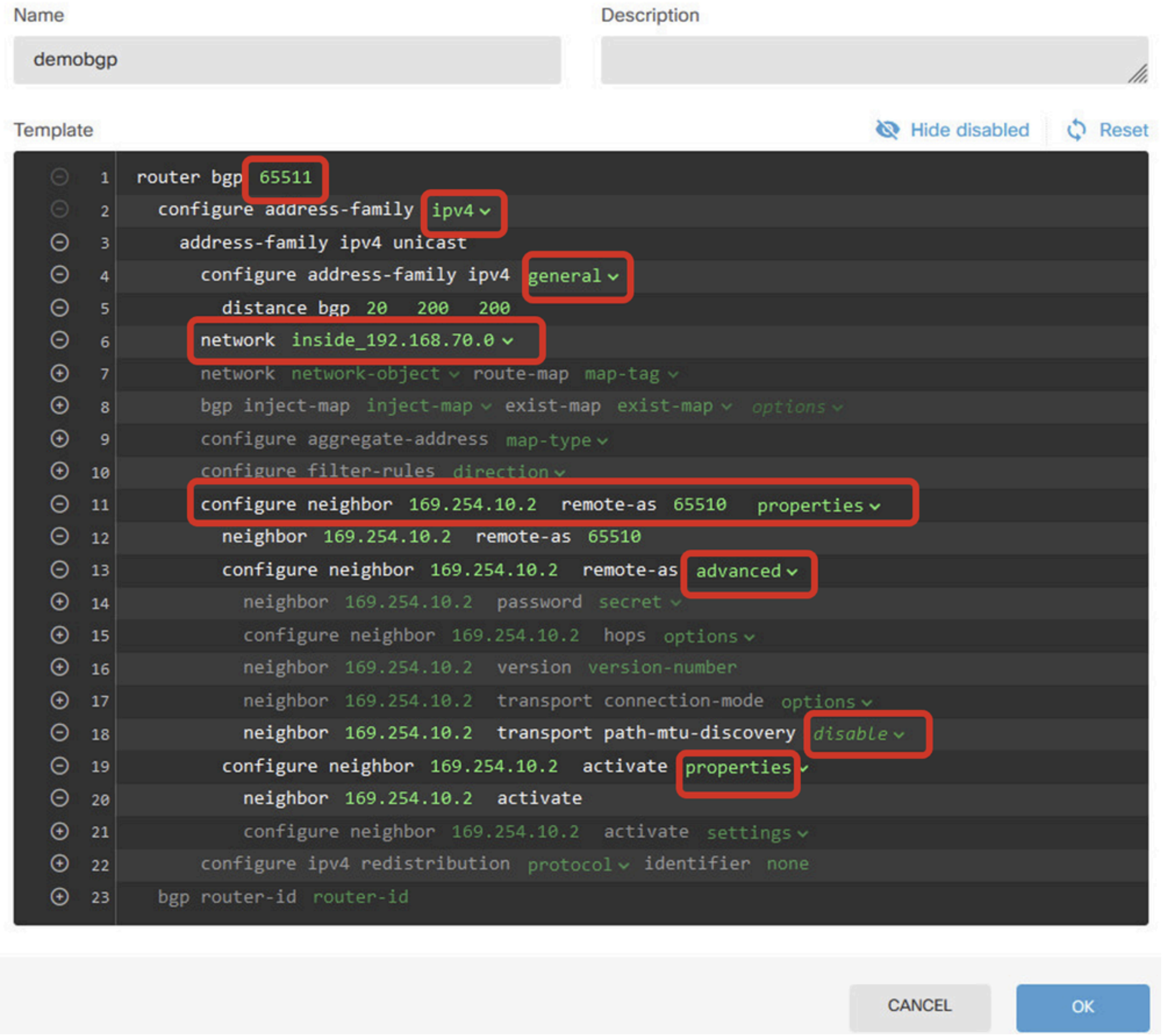
Description:

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

This is an overview of the BGP setting in this example. You can configure the other BGP settings based on your actual needs.



Name: demobgp

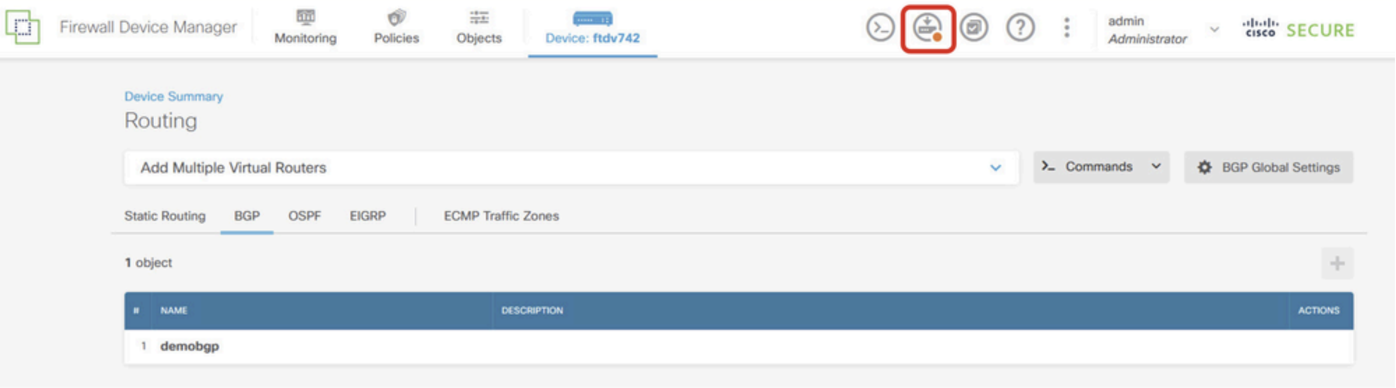
Description:

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

Step 7. Deploy the BGP configuration changes.



#	NAME	DESCRIPTION	ACTIONS
1	demobgp		

Deploy_BGP_Configuration

Step 8. Now the configuration for Site1 FTD is completed.

In order to configure Site2 FTD VPN and BGP, repeat Step 3. to Step 7. with corresponding parameters of Site2 FTD.

Configuration overview of Site1 FTD and Site2 FTD in CLI.

Site1 FTD	Site2 FTD
NGFW Version 7.4.2 interface GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 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 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d object network OutsideIPv4Gateway host 192.168.30.3 object network inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: 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: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	NGFW Version 7.4.2 interface GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 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 tunnel source interface outside tunnel destination 192.168.30.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d object network OutsideIPv4Gateway host 192.168.10.3 object network inside_192.168.50.0 subnet 192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: 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: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any

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 neighbor 169.254.10.2 activate network 192.168.70.0 no auto-summary no synchronization exit-address-family route 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 encryption aes-256 aes integrity sha256 sha group 14 prf sha256 sha lifetime seconds 86400 crypto ikev2 policy 20 encryption aes-256 aes-192 aes integrity sha512 sha384 sha256 sha group 21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside group-policy |s2sGP|192.168.10.1 internal group-policy |s2sGP|192.168.10.1 attributes vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1 general-attributes 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 *****	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 neighbor 169.254.10.1 activate network 192.168.50.0 no auto-summary no synchronization exit-address-family route 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 encryption aes-256 aes integrity sha256 sha group 14 prf sha256 sha lifetime seconds 86400 crypto ikev2 policy 20 encryption aes-256 aes-192 aes integrity sha512 sha384 sha256 sha group 21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside group-policy |s2sGP|192.168.30.1 internal group-policy |s2sGP|192.168.30.1 attributes vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1 general-attributes 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 *****

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Navigate to the CLI of each FTD via console or SSH in order to verify the VPN status of phase 1 and phase 2 through the commands **show crypto ikev2 sa** and **show crypto ipsec sa**.

Site1 FTD	Site2 FTD
ftdv742# **show crypto ikev2 sa** IKEv2 SAs: 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 Global/Global READY RESPONDER Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/5145 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: 0xf0c4239d/0xb7b5b38b	ftdv742# **show crypto ikev2 sa** IKEv2 SAs: 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 Global/Global READY INITIATOR Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/74099 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: 0xb7b5b38b/0xf0c4239d
ftdv742# **show crypto ipsec sa** interface: demovti Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1 #pkts encaps: 5720, #pkts encrypt: 5720, #pkts digest: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verify: 5717 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 5720, #pkts comp failed: 0,	ftdv742# **show crypto ipsec sa** interface: demovti25 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.10.1 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1 #pkts encaps: 5721, #pkts encrypt: 5721, #pkts digest: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verify: 5721 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 5721, #pkts comp failed: 0,

#pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.10.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: B7B5B38B current inbound spi : F0C4239D inbound esp sas: spi: 0xF0C4239D (4039386013) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4285389/3722) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0xB7B5B38B (3082138507) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4147149/3722) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001	#pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.168.10.1/500, remote crypto endpt.: 192.168.30.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: F0C4239D current inbound spi : B7B5B38B inbound esp sas: spi: 0xB7B5B38B (3082138507) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (3962829/3626) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0xF0C4239D (4039386013) SA State: active transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (kB/sec): (4101069/3626) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001

Step 2. Navigate to the CLI of each FTD via console or SSH in order to verify the BGP status using the commands **show bgp neighbors** and **show route bgp**.

Site1 FTD	Site2 FTD

```
ftdv742# show bgp neighbors

BGP neighbor is 169.254.10.2, vrf single_vf, remote
AS 65510, external link
BGP version 4, remote router ID 192.168.50.1
BGP state = Established, up for 1d20h
Last read 00:00:25, last write 00:00:45, hold time is
180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multisession capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multisession Capability:
Message statistics:
InQ depth is 0
OutQ depth is 0

Sent Rcvd
Opens:  1 1
Notifications: 0 0
Updates: 2 2
Keepalives: 2423 2427
Route Refresh: 0 0
Total: 2426 2430
Default minimum time between advertisement runs is
30 seconds

For address family: IPv4 Unicast
Session: 169.254.10.2
BGP table version 3, neighbor version 3/0
Output queue size : 0
Index 1
1 update-group member
Sent Rcvd
Prefix activity: ---- ----
Prefixes Current: 1 1 (Consumes 80 bytes)
Prefixes Total: 1 1
Implicit Withdraw: 0 0
Explicit Withdraw: 0 0
Used as bestpath: n/a 1
Used as multipath: n/a 0

Outbound Inbound
Local Policy Denied Prefixes: -------- -------
Bestpath from this peer: 1 n/a
Total: 1 0
Number of NLRIs in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a
route to 169.254.10.2
Connections established 1; dropped 0
Last reset never
```

```
ftdv742# show bgp neighbors

BGP neighbor is 169.254.10.1, vrf single_vf, remote
AS 65511, external link
BGP version 4, remote router ID 192.168.70.1
BGP state = Established, up for 1d20h
Last read 00:00:11, last write 00:00:52, hold time is
180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multisession capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multisession Capability:
Message statistics:
InQ depth is 0
OutQ depth is 0

Sent Rcvd
Opens: 1 1
Notifications: 0 0
Updates: 2 2
Keepalives: 2424 2421
Route Refresh: 0 0
Total: 2427 2424
Default minimum time between advertisement runs is
30 seconds

For address family: IPv4 Unicast
Session: 169.254.10.1
BGP table version 9, neighbor version 9/0
Output queue size : 0
Index 4
4 update-group member
Sent Rcvd
Prefix activity: ---- ----
Prefixes Current: 1 1 (Consumes 80 bytes)
Prefixes Total: 1 1
Implicit Withdraw: 0 0
Explicit Withdraw: 0 0
Used as bestpath: n/a 1
Used as multipath: n/a 0

Outbound Inbound
Local Policy Denied Prefixes: -------- -------
Bestpath from this peer: 1 n/a
Total: 1 0
Number of NLRIs in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a
route to 169.254.10.1
Connections established 4; dropped 3
Last reset 1d21h, due to Interface flap of session 1
```

Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled	Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled
ftdv742# **show route bgp** 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 B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h	ftdv742# **show route bgp** 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 B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h

Step 3. Site1 Client and Site2 Client ping each other successfully.

Site1 Client:

```
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 Client:

```
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
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

You can use those debug commands in order to troubleshoot the VPN section.

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

You can use those debug commands in order to troubleshoot the BGP section.

```
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>
```