在FDM管理的FTD上，透過路由型VPN設定BGP

目錄

簡介

本檔案介紹在FirePower裝置管理員(FDM)管理的FTDv上，透過路由型站台對站台VPN設定BGP。

必要條件

需求

思科建議您瞭解以下主題：

- 對VPN的基本瞭解
- FTDv上的BGP組態
- 使用FDM的經驗

採用元件

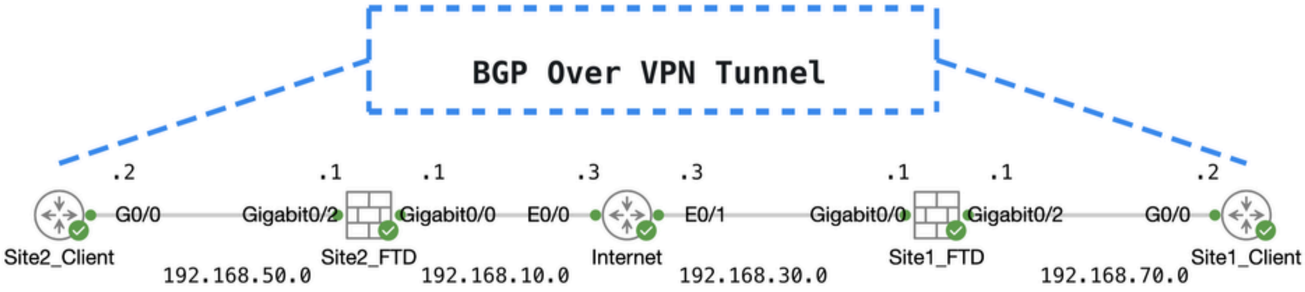
本文中的資訊係根據以下軟體和硬體版本：

- Cisco FTDv版本7.4.2
- Cisco FDM 7.4.2版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



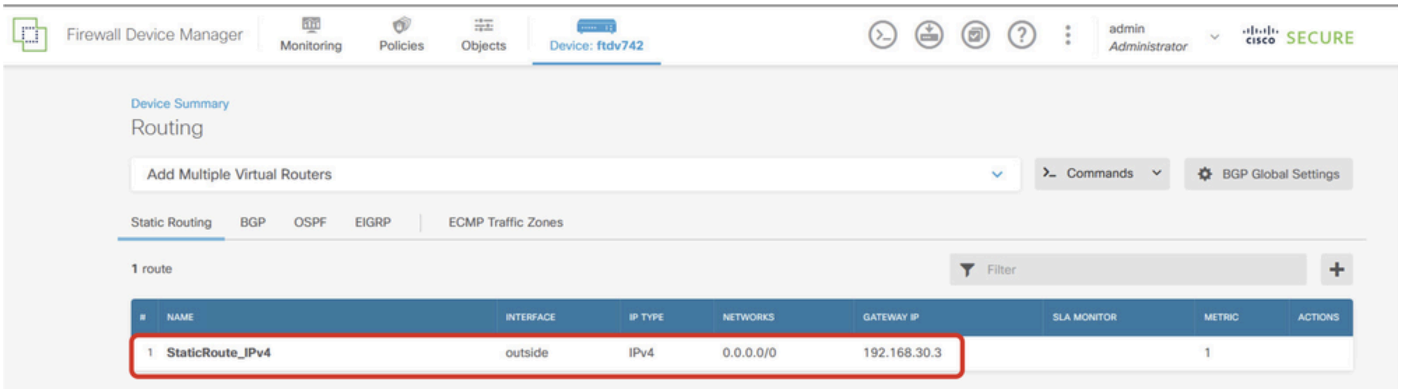
托波

VPN上的配置

步驟 1.確保節點之間的IP互連就緒且穩定。FDM上的智慧型授權已順利註冊至智慧帳戶。

步驟 2. Site1客戶端的網關配置有Site1 FTD的內部IP地址(192.168.70.1)。Site2客戶端的網關配置有Site2 FTD的內部IP地址(192.168.50.1)。此外，請確保在FDM初始化後，正確設定兩個FTD上的預設路由。

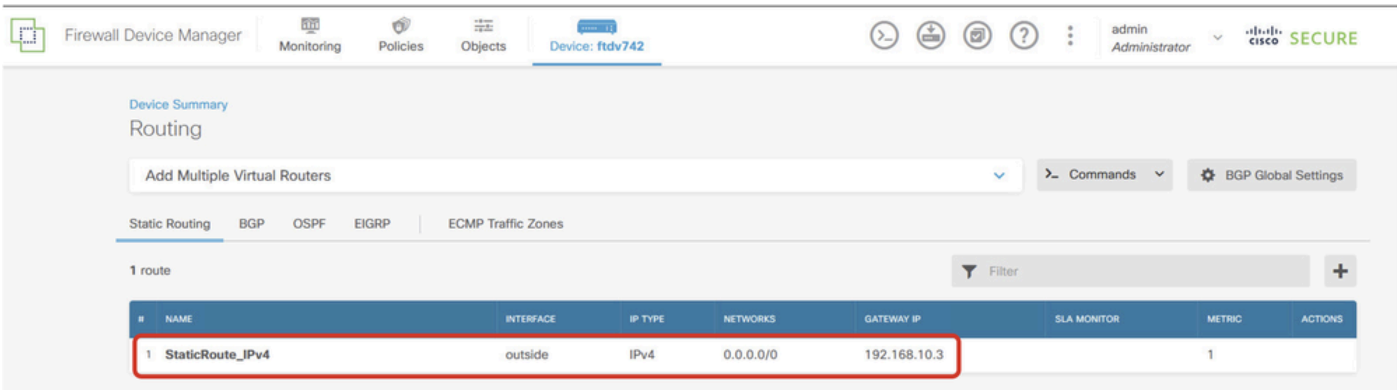
登入每個FDM的GUI。導航到Device > Routing。按一下View Configuration。按一下**Static Routing**頁籤以驗證預設靜態路由。



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	

站點1_FTD_網關



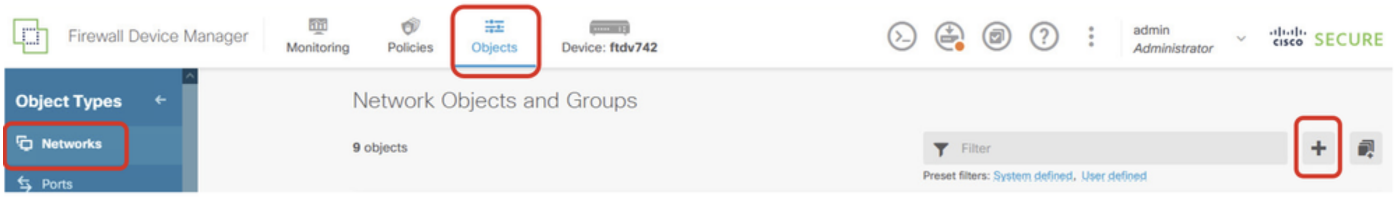
1 route

#	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	

站點2_FTD_網關

步驟 3.配置基於路由的站點到站點VPN。 在本範例中，首先設定Site1 FTD。

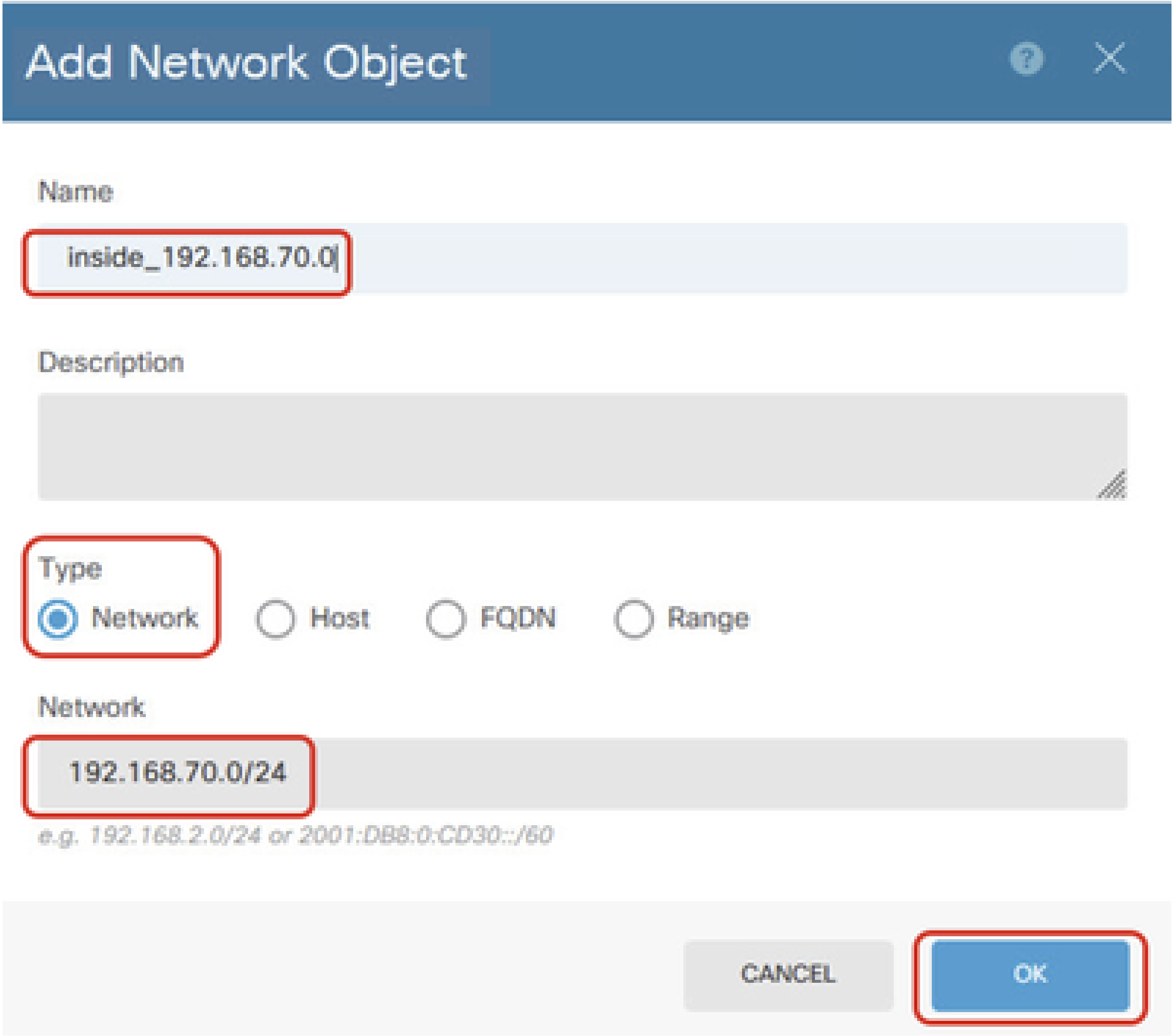
步驟 3.1. 登入Site1 FTD的FDM GUI。為Site1 FTD的內部網路建立新網路對象。 導航到**Objects** > **Networks**，按一下+按鈕。



Create_Network_Object

步驟 3.2.提供必要資訊。按一下OK 按鈕。

- 名稱：inside_192.168.70.0
- 型別：網路
- 網路：192.168.70.0/24



Name

inside_192.168.70.0

Description

Type

● Network ○ Host ○ FQDN ○ Range

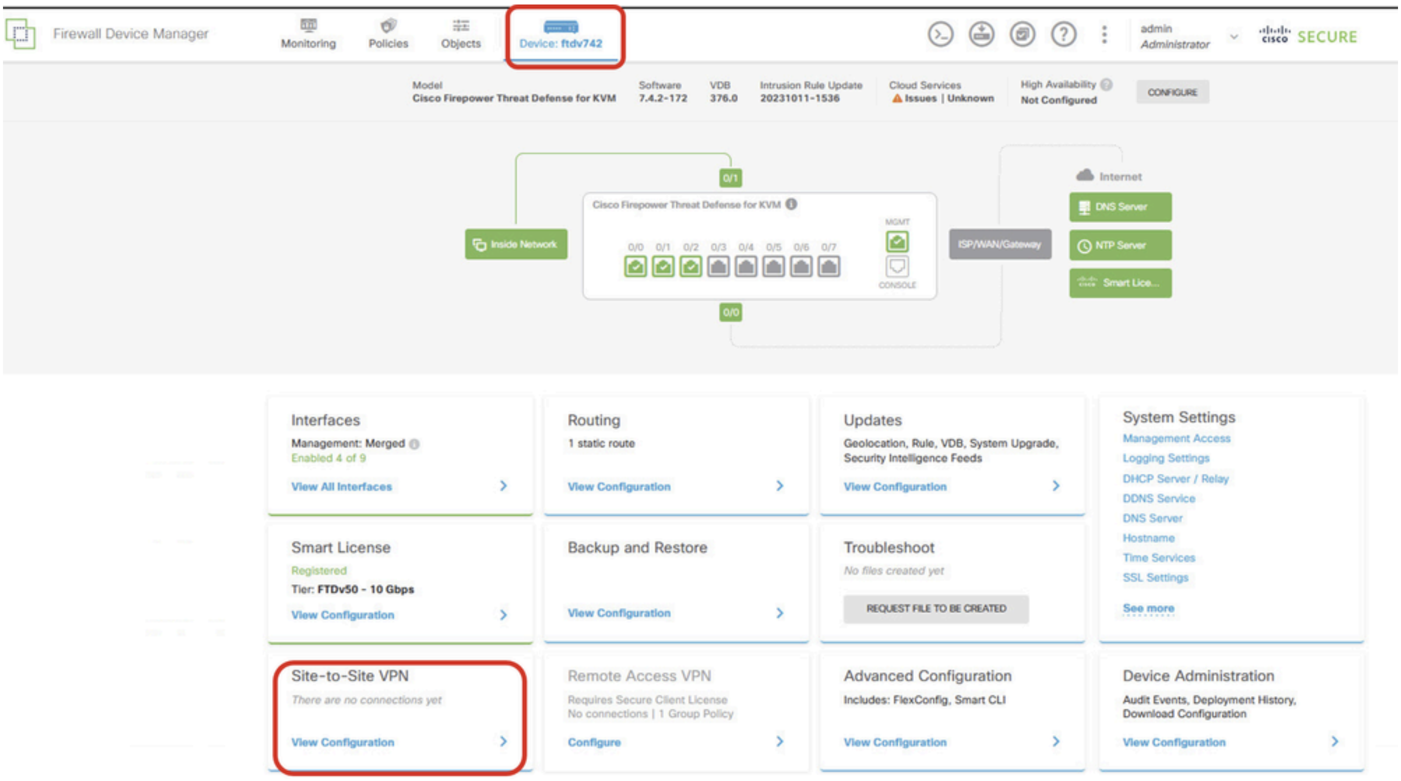
Network

192.168.70.0/24

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

站點1_內部_網路

步驟 3.3.導航到**Device > Site-to-Site VPN**。 點選**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

Site-to-Site VPN
There are no connections yet
View Configuration

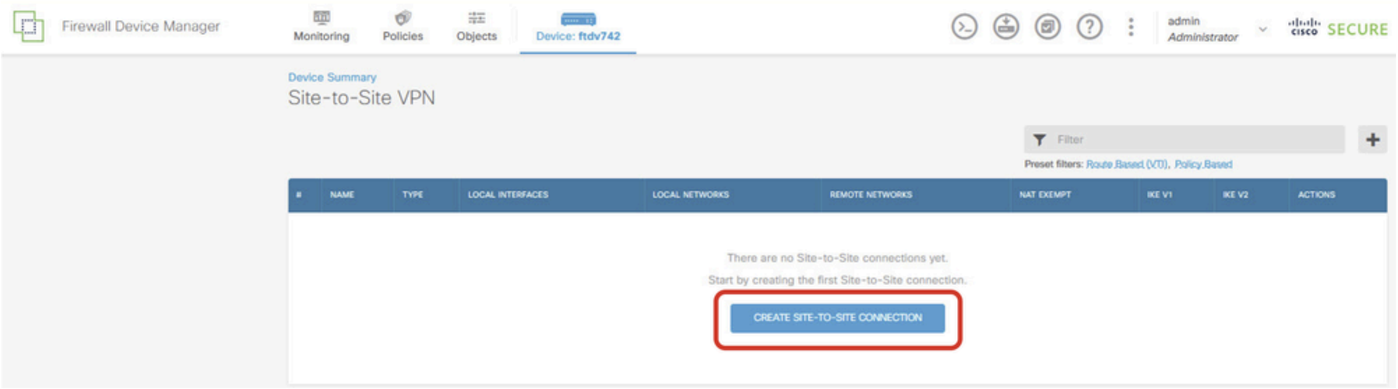
Remote Access VPN
Requires Secure Client License
No connections | 1 Group Policy
Configure

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration

Device Administration
Audit Events, Deployment History, Download Configuration
View Configuration

檢視站點到站點VPN

步驟 3.4.開始建立新的站點到站點VPN。點選**CREATE SITE-TO-SITE CONNECTION**。



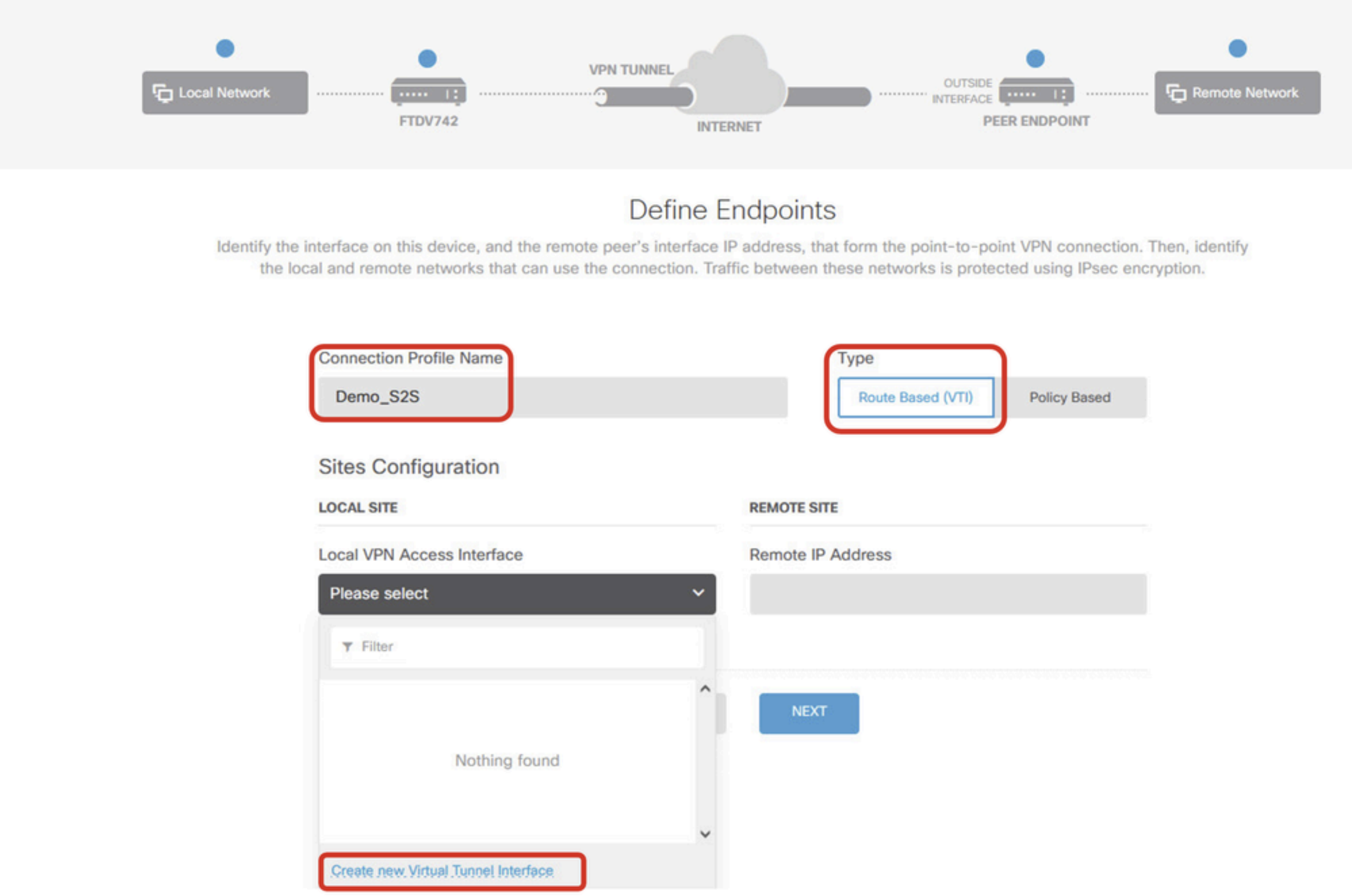
#	NAME	TYPE	LOCAL INTERFACES	LOCAL NETWORKS	REMOTE NETWORKS	NAT EXEMPT	IKE V1	IKE V2	ACTIONS

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

Create_Site-to-Site_Connection

步驟 3.5.提供必要資訊。

- 連線配置檔名稱：Demo_S2S
- 型別：基於路由(VTI)
- 本地VPN訪問介面：按一下下拉選單，然後按一下**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

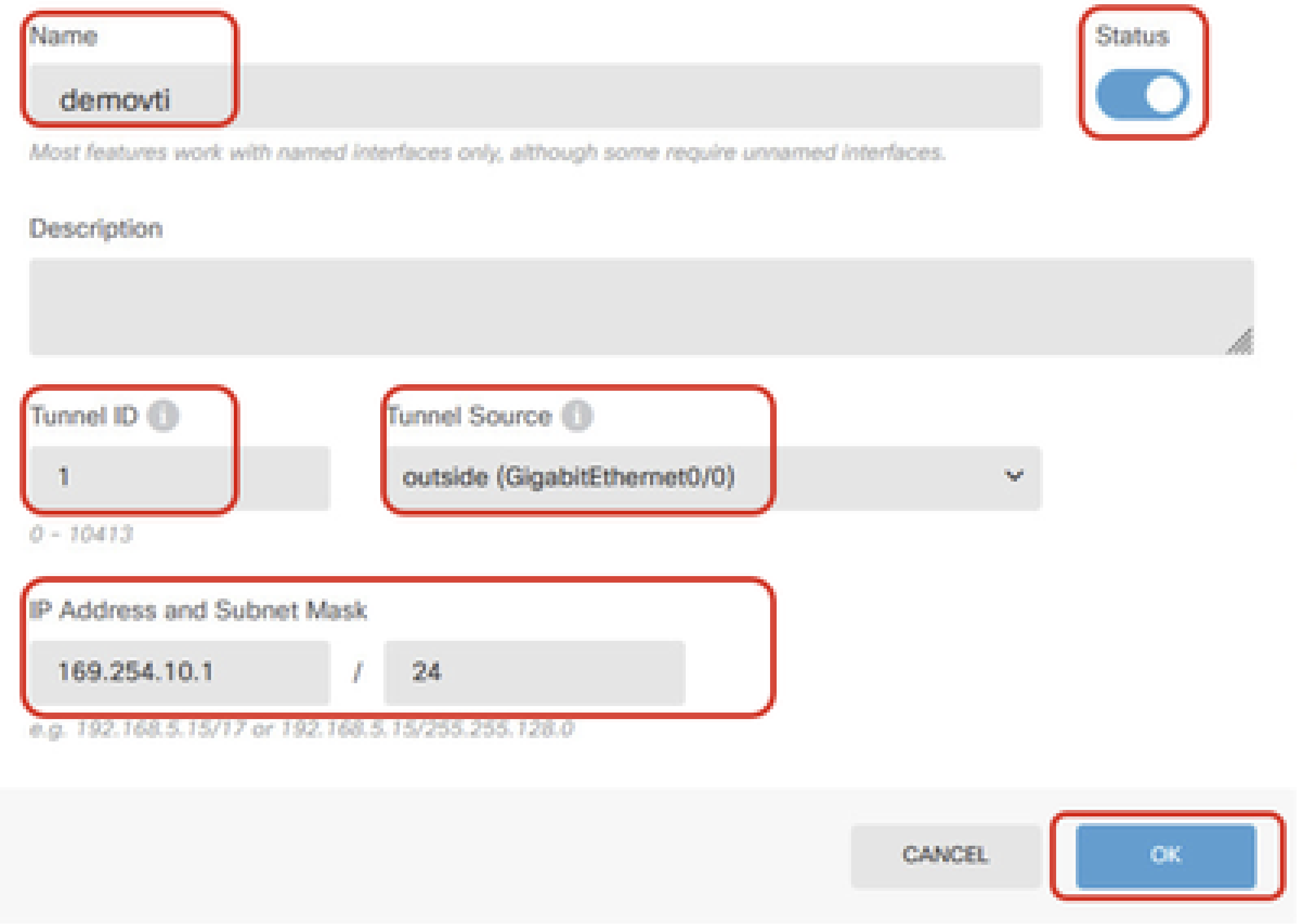
REMOTE SITE

Remote IP Address

Create_VTI_in_VPN_Wizard

步驟 3.6.提供必要資訊以建立新的VTI。 按一下OK按鈕。

- 名稱：demovti
- 通道ID：1
- 隧道源：外部(GigabitEthernet0/0)
- IP地址和子網掩碼：169.254.10.1/24
- 狀態：按一下滑杆至「已啟用」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

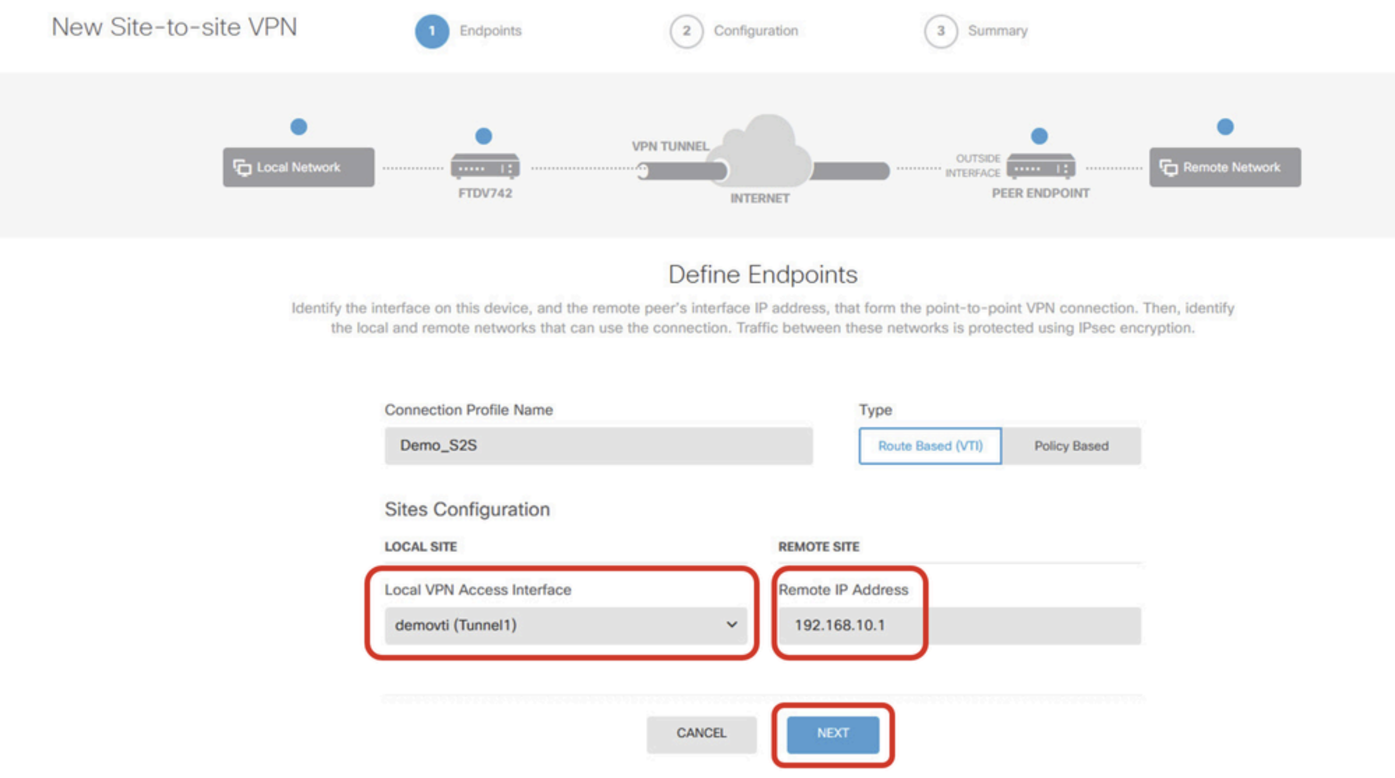
169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

建立_VTI_細節

步驟 3.7.繼續提供必要資訊。 按一下NEXT按鈕。

- 本地VPN訪問介面：demovti（在步驟3.6中建立。）
- 遠端IP地址：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)

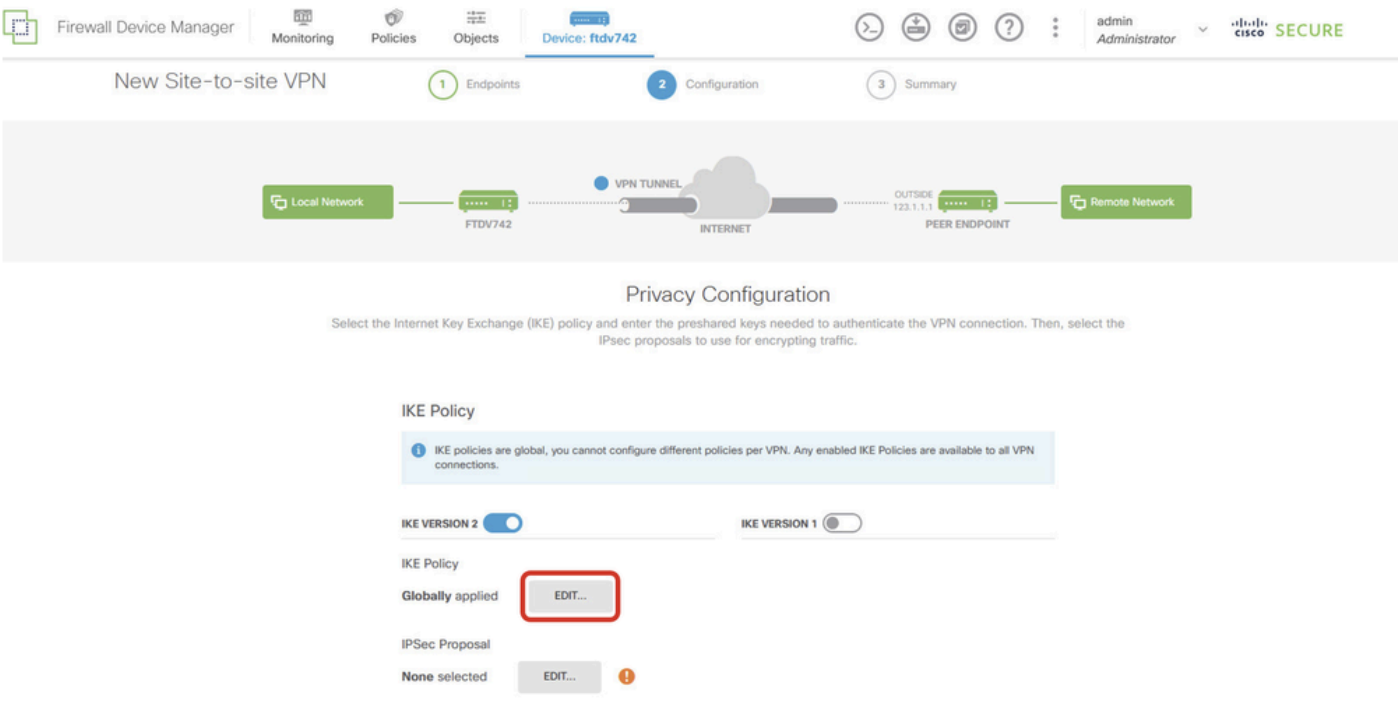
REMOTE SITE

Remote IP Address: 192.168.10.1

CANCEL NEXT

VPN_Wizard_Endpoint_Step1

步驟 3.8.導航到IKE Policy。按一下EDIT按鈕。



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

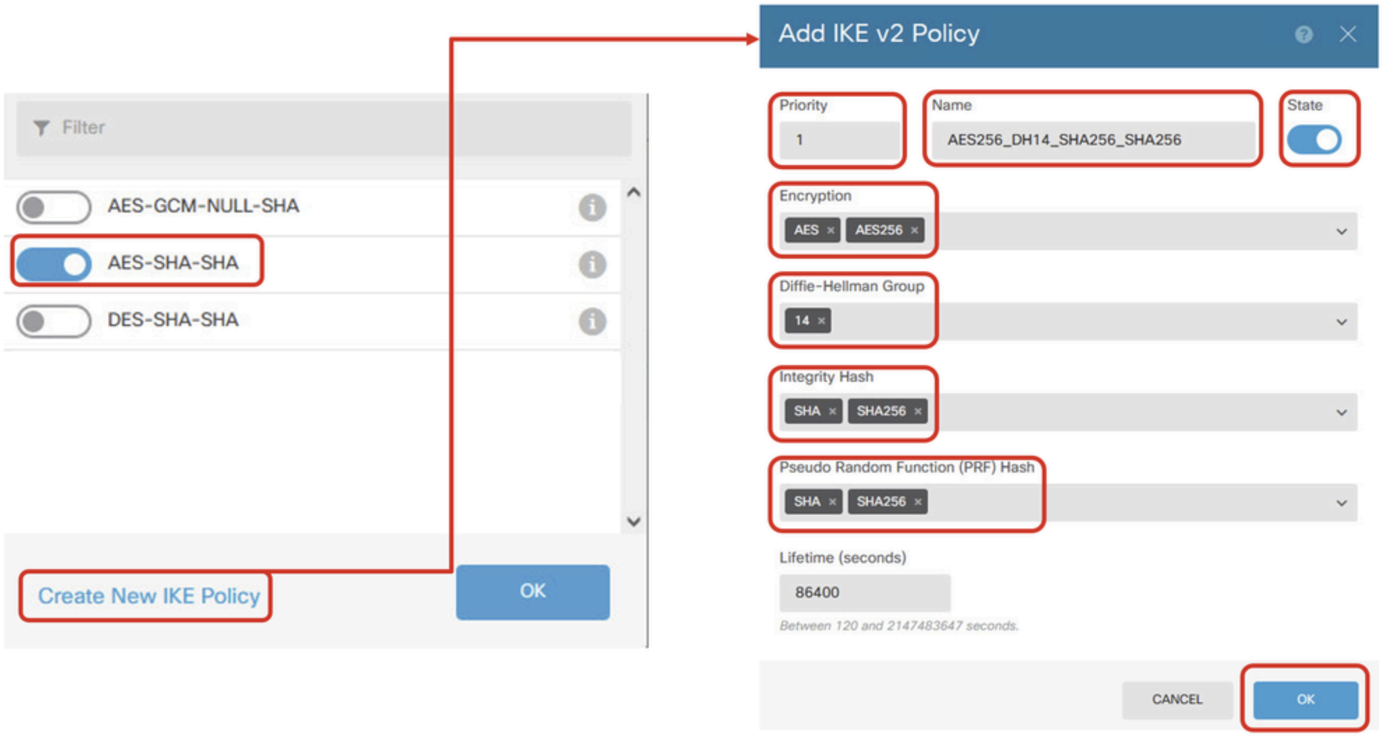
None selected EDIT...

Edit_IKE_Policy

步驟 3.9. 對於IKE策略，您可以使用預定義策略，或者按一下Create New IKE Policy建立新策略。

在本示例中，切換現有IKE策略AES-SHA-SHA，並建立一個新策略用於演示。按一下OK按鈕進行儲存。

- 名稱：AES256_DH14_SHA256_SHA256
- 加密：AES、AES256
- DH組：14
- 完整性雜湊：SHA、SHA256
- PRF雜湊：SHA、SHA256
- 存留期：86400（預設）



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 ×

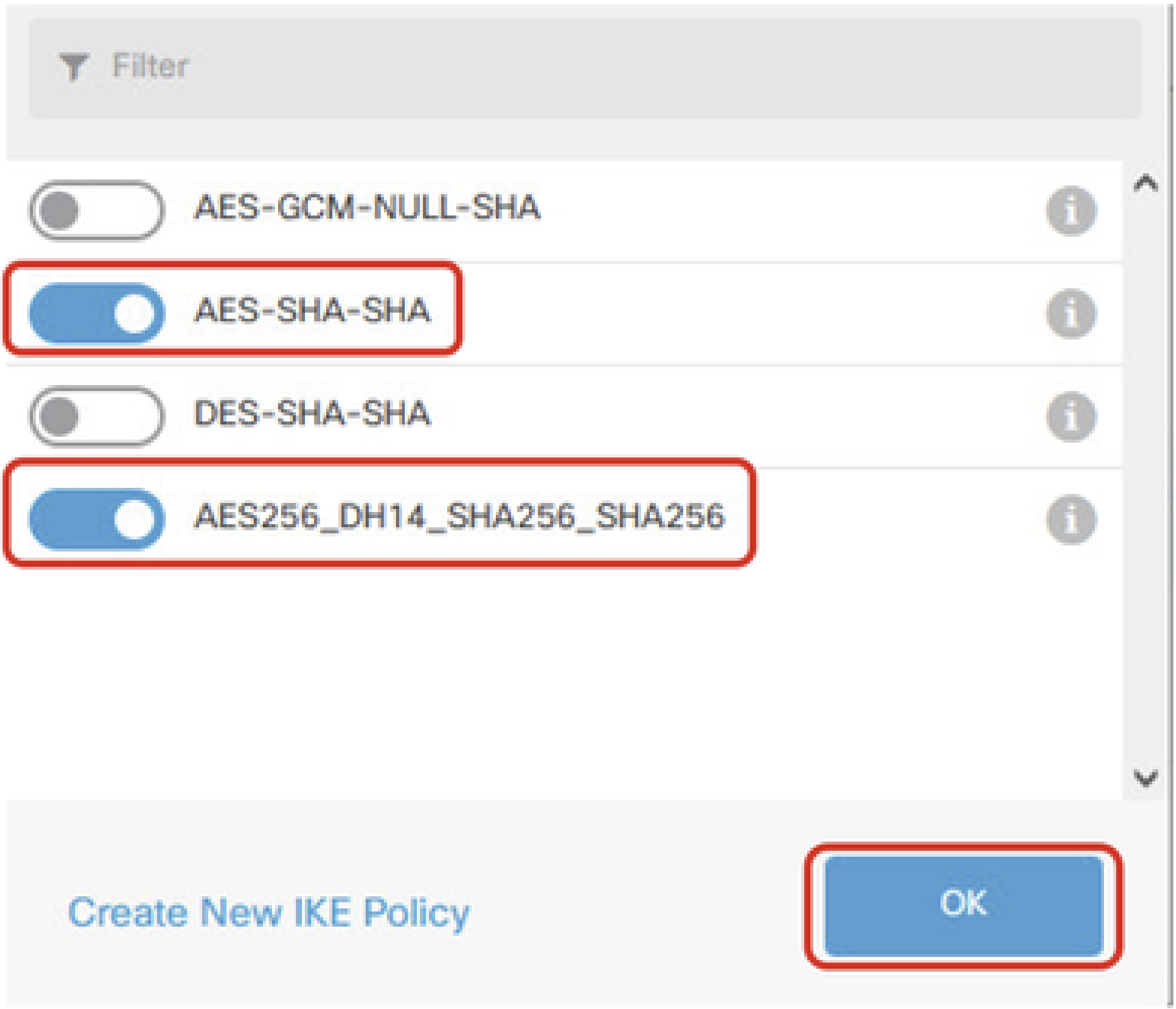
Integrity Hash
SHA × SHA256 ×

Pseudo Random Function (PRF) Hash
SHA × SHA256 ×

Lifetime (seconds)
86400

Between 120 and 2147483647 seconds.

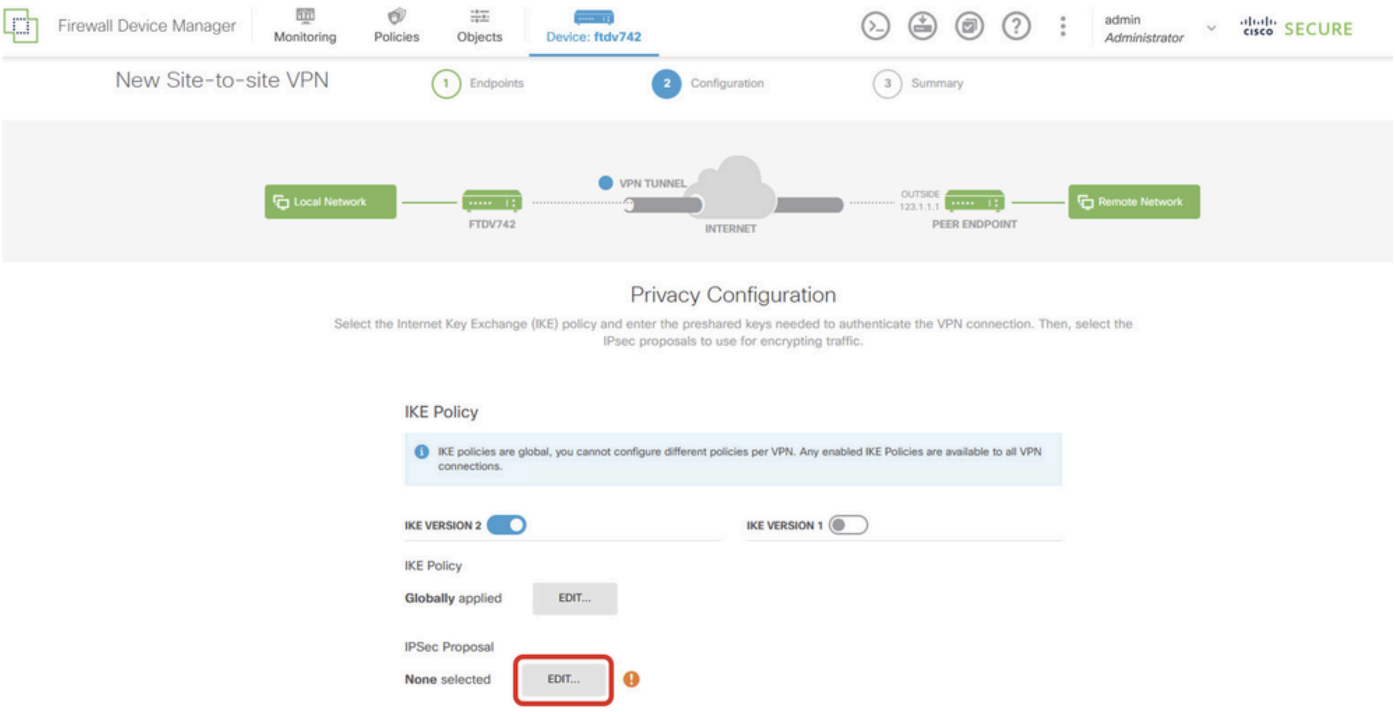
Add_New_IKE_Policy



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

啟用_新建_IKE_策略

步驟 3.10. 導航到IPSec建議。按一下EDIT按鈕。



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 ○

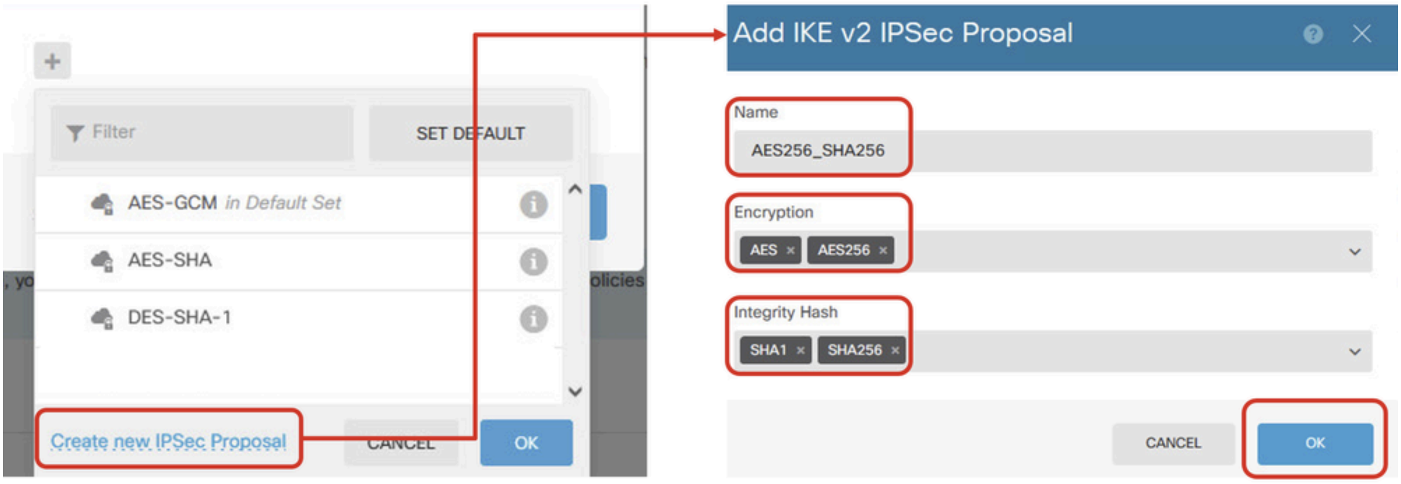
IKE Policy
Globally applied EDIT...

IPSec Proposal
None selected EDIT...

Edit_IKE_Proposal

步驟 3.11. 對於IPSec提議，您可以使用預定義或者按一下建立新的IPSec提議建立一個新提議。在此範例中，建立用於示範的新範例。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱：AES256_SHA256
- 加密：AES、AES256
- 完整性雜湊：SHA1、SHA256



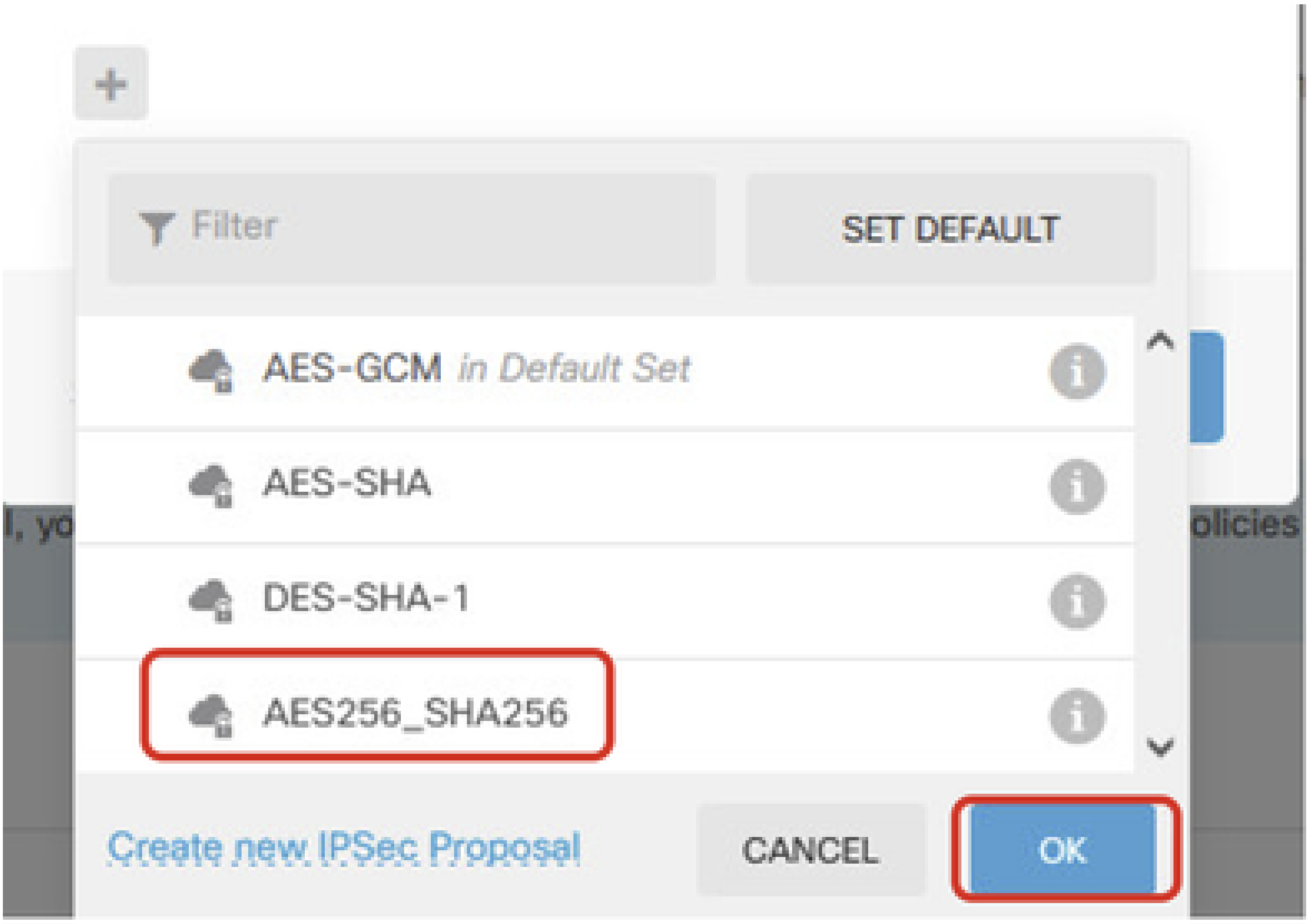
Add IKE v2 IPSec Proposal

Name: AES256_SHA256

Encryption: AES × AES256 ×

Integrity Hash: SHA1 × SHA256 ×

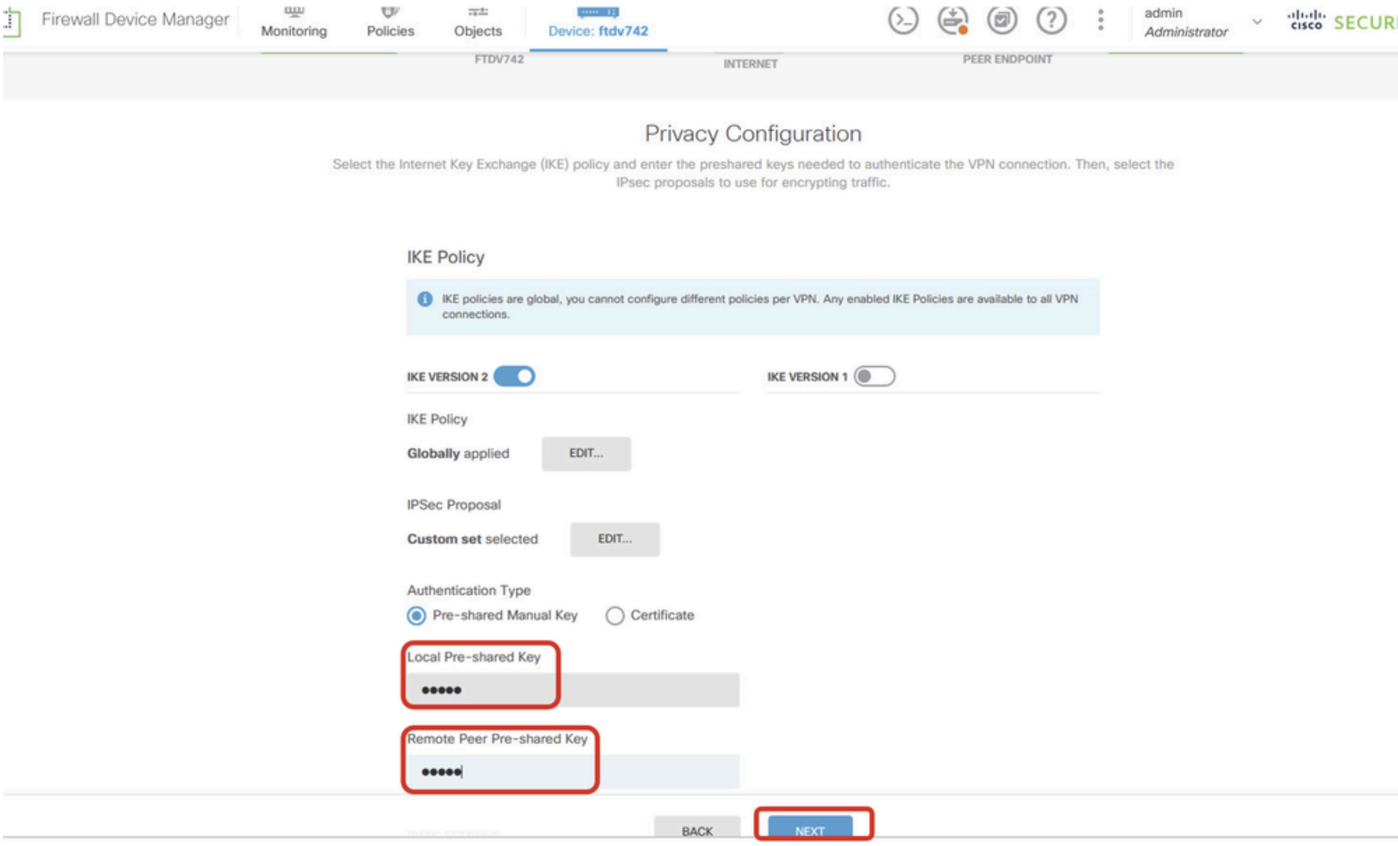
增加_新建_IPSec_提議



啟用_新建_IPSec_提議

步驟 3.12.配置預共用金鑰。按一下NEXT按鈕。

記下這個預共用金鑰，稍後在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 (on) IKE VERSION 1 (off)

IKE Policy

Globally applied EDIT...

IPSec Proposal

Custom set selected EDIT...

Authentication Type

● Pre-shared Manual Key ○ Certificate

Local Pre-shared Key

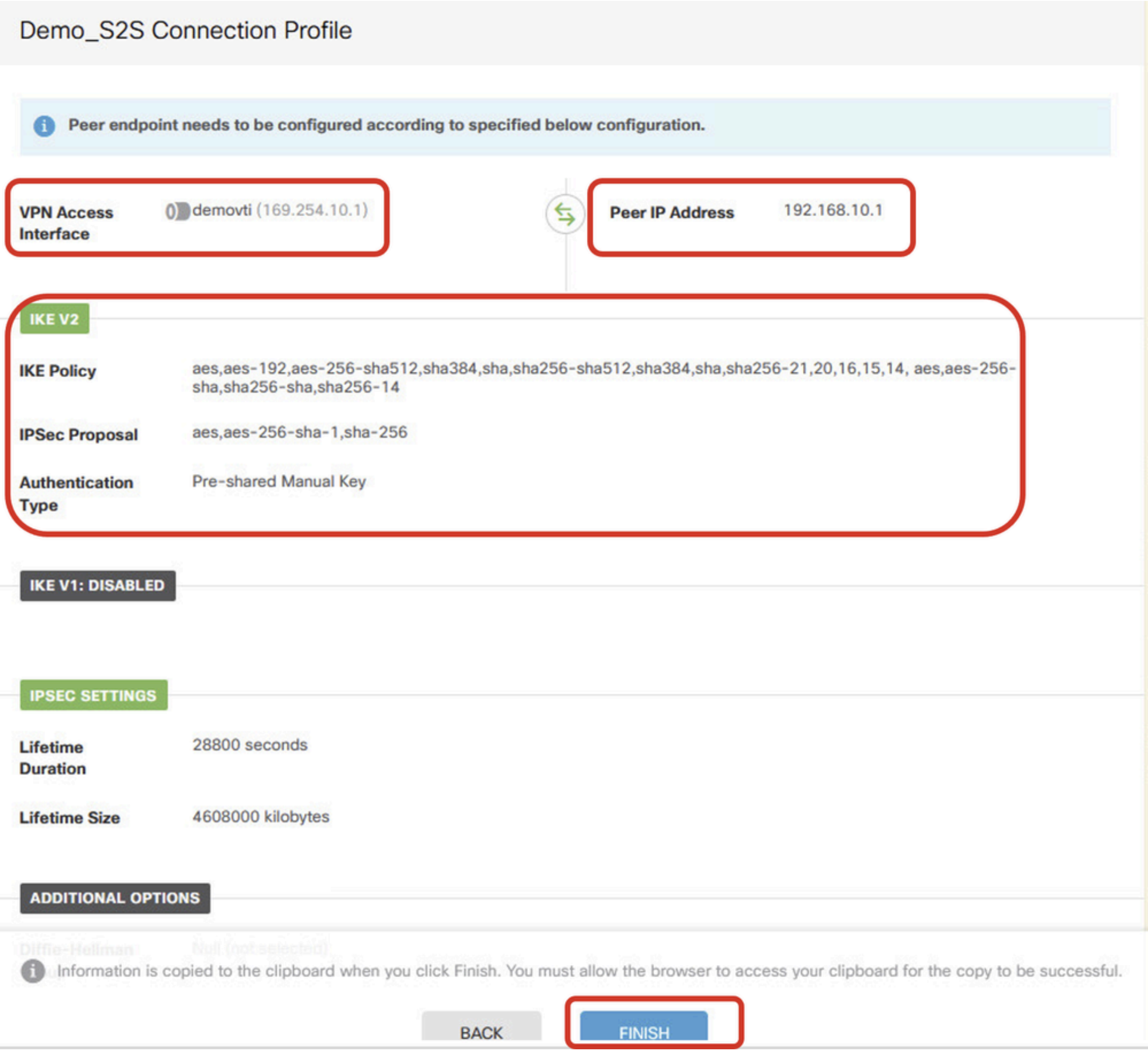
●●●●●

Remote Peer Pre-shared Key

●●●●●

Configure_Pre_Shared_Key

步驟 3.13.檢視VPN配置。如果需要修改任何內容，請按一下BACK按鈕。如果一切正常，請按一下FINISH按鈕。



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

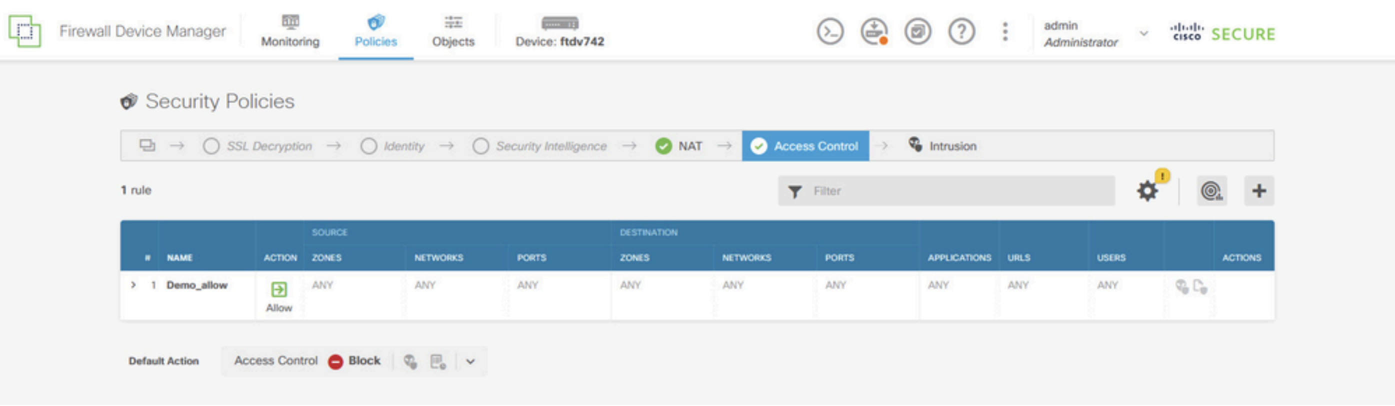
ADDITIONAL OPTIONS

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

步驟 3.14.建立存取控制規則，以允許流量透過FTD。在本例中，允許全部用於演示目的。 根據您的實際需求修改策略。



1 rule

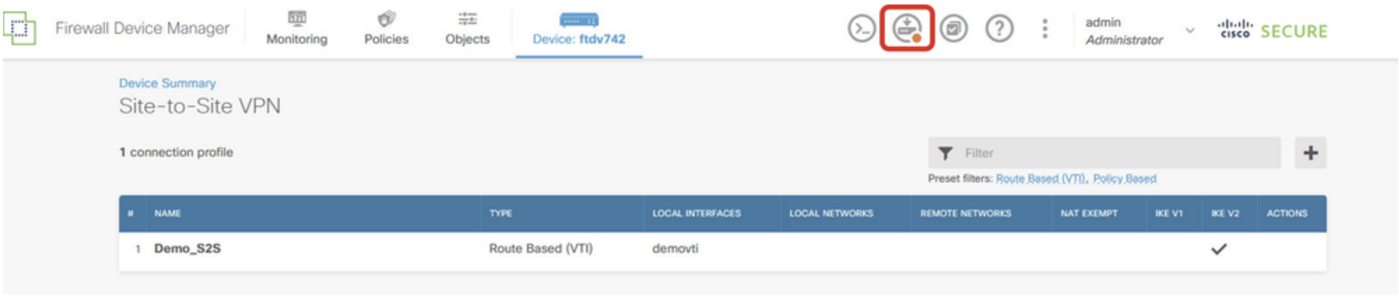
			SOURCE			DESTINATION						
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	

Default Action Access Control Block

Access_Control_Rule_Example

步驟3.15. （可選）如果為客戶端配置了動態NAT以訪問網際網路，請在FTD上為客戶端流量配置NAT免除規則。在本範例中，不需要設定NAT豁免規則，因為每個FTD上都沒有設定動態NAT。

步驟 3.16.部署配置更改。



Device Summary

Site-to-Site VPN

1 connection profile

Filter

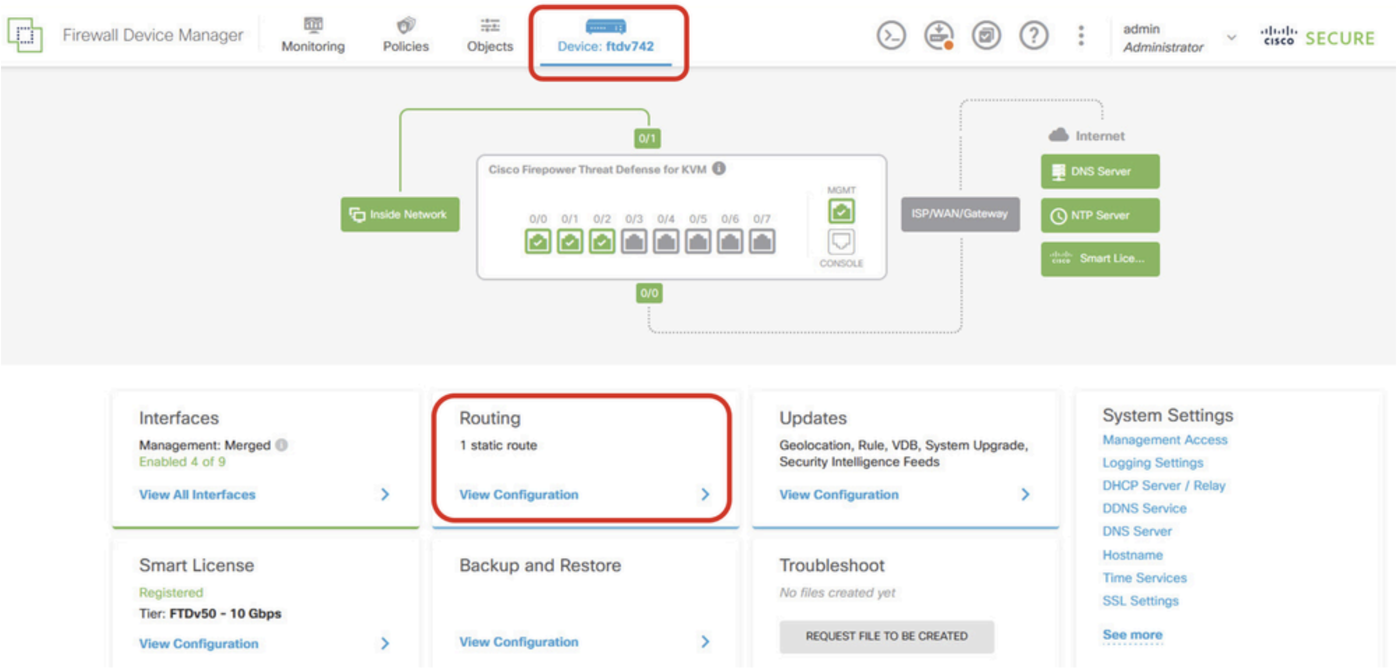
Preset filters: Route Based (VTI), Policy Based

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

部署_VPN_配置

BGP上的配置

步驟 4. 導航到裝置>路由。按一下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

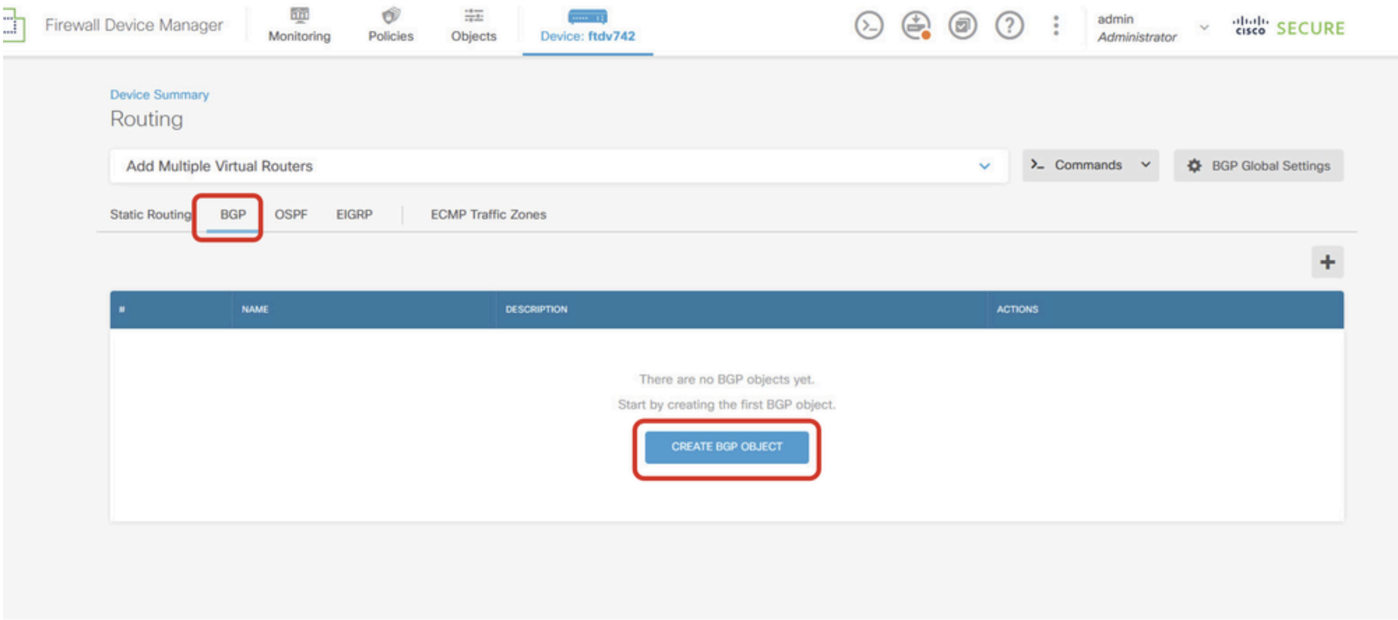
Smart License
Registered
Tier: FTDv50 - 10 Gbps
View Configuration

Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

檢視_路由_組態

步驟 5.按一下BGP頁籤，然後按一下CREATE BGP OBJECT。



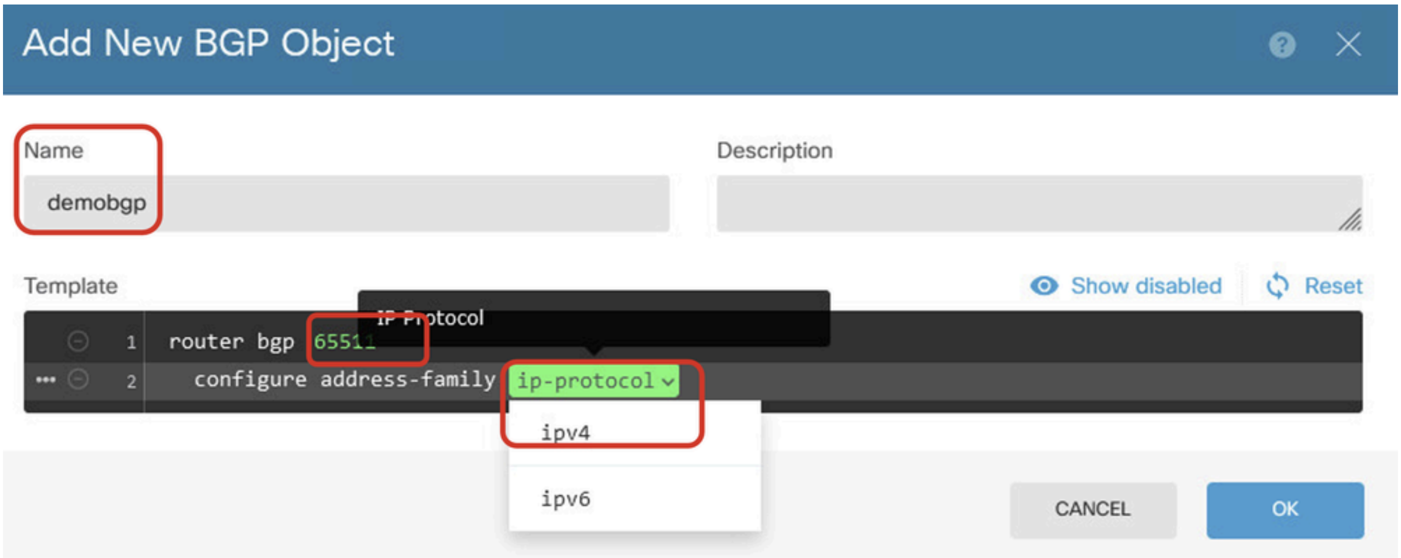
Create_BGP_Object

步驟 6.提供物件的名稱。 導航到模板並進行配置。按一下OK按鈕進行儲存。

名稱：demobgp

第1行：配置AS編號。按一下as-number。手動輸入本地AS編號。在本例中，Site1 FTD的AS編號65511。

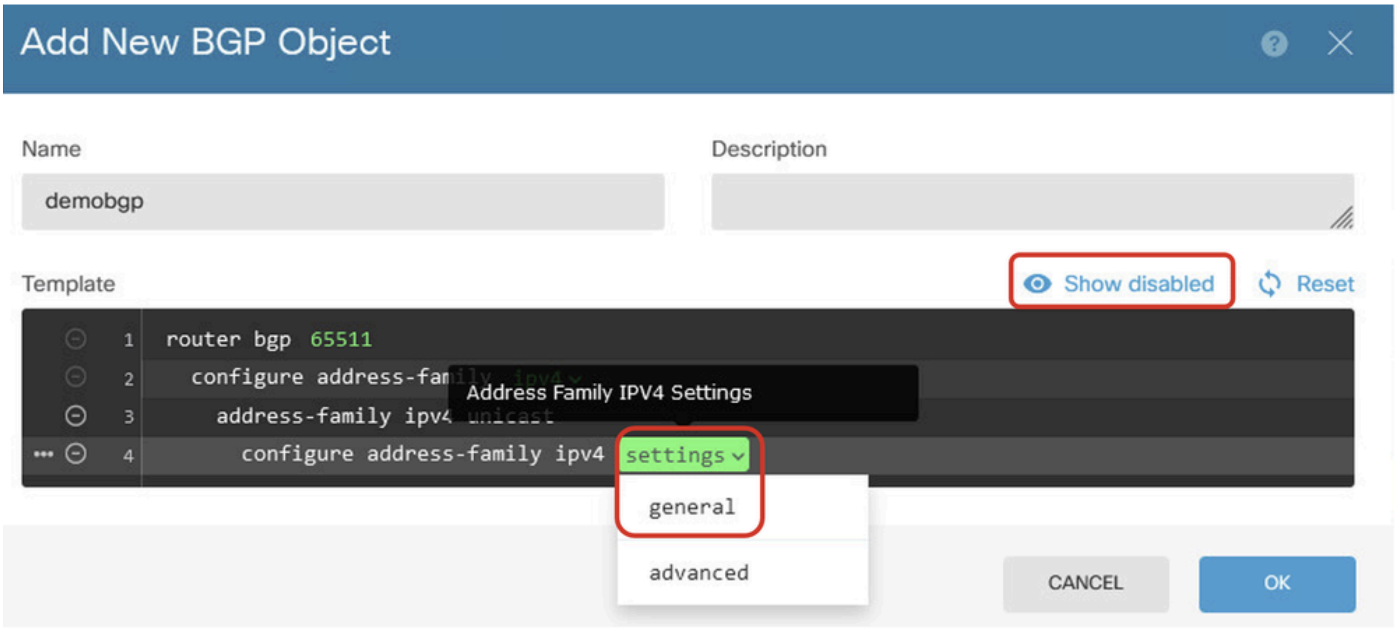
第2行：配置IP協定。按一下ip-protocol。選擇ipv4。



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

Create_BGP_Object_ASNumber_Protocol

第4行：配置更多設定。按一下settings，選擇general，然後按一下Show disabled。



Add New BGP Object

Name: demobgp

Description:

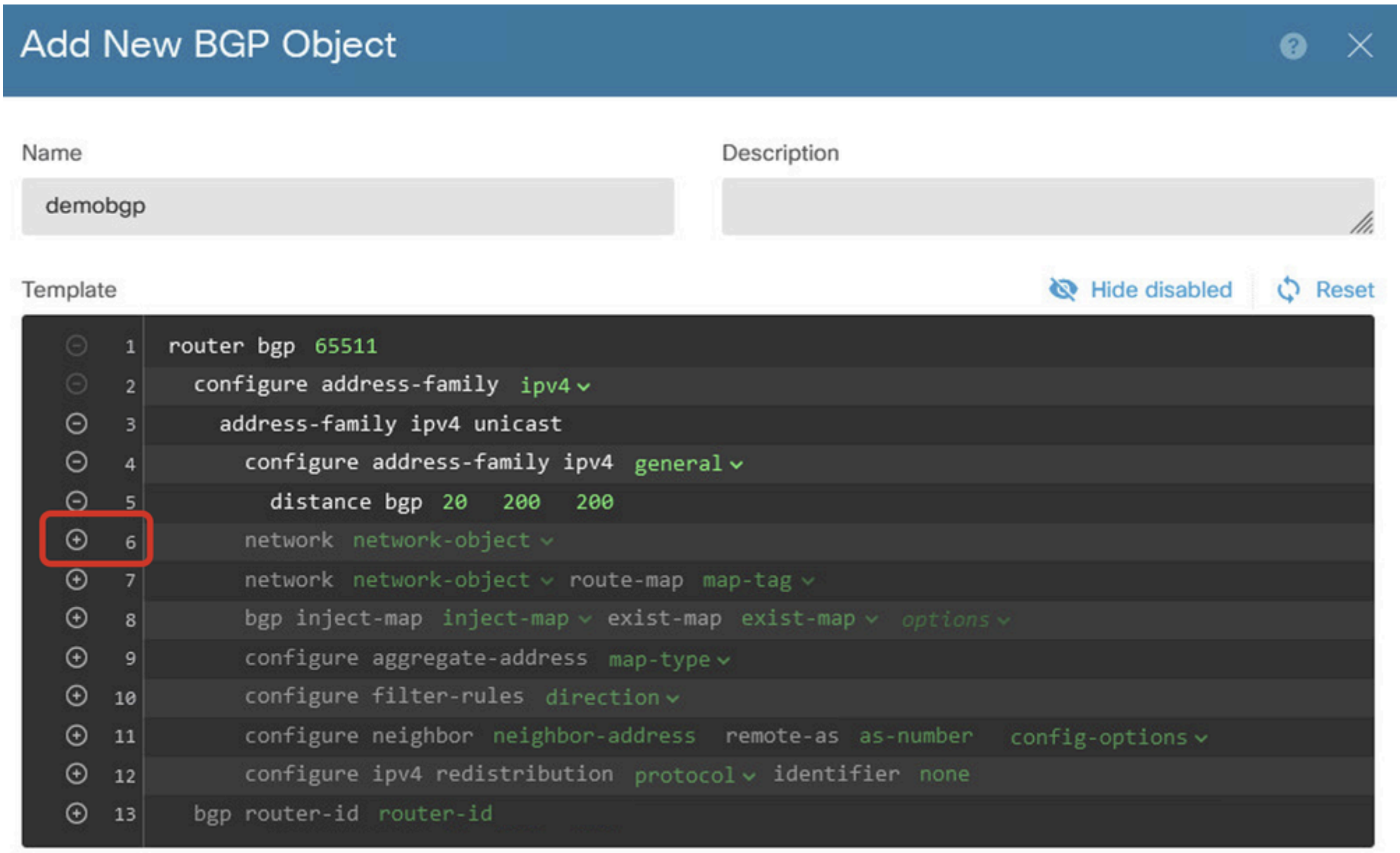
Template — Show disabled — Reset

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

Address Family IPV4 Settings

Create_BGP_Object_AddressSetting

第6行：點選+圖示可允許該行配置BGP網路。按一下network-object。您可以檢視現有的可用物件，然後選擇一個物件。在本示例中，選擇對象name inside_192.168.70.0（在步驟3.2中建立）。



Add New BGP Object

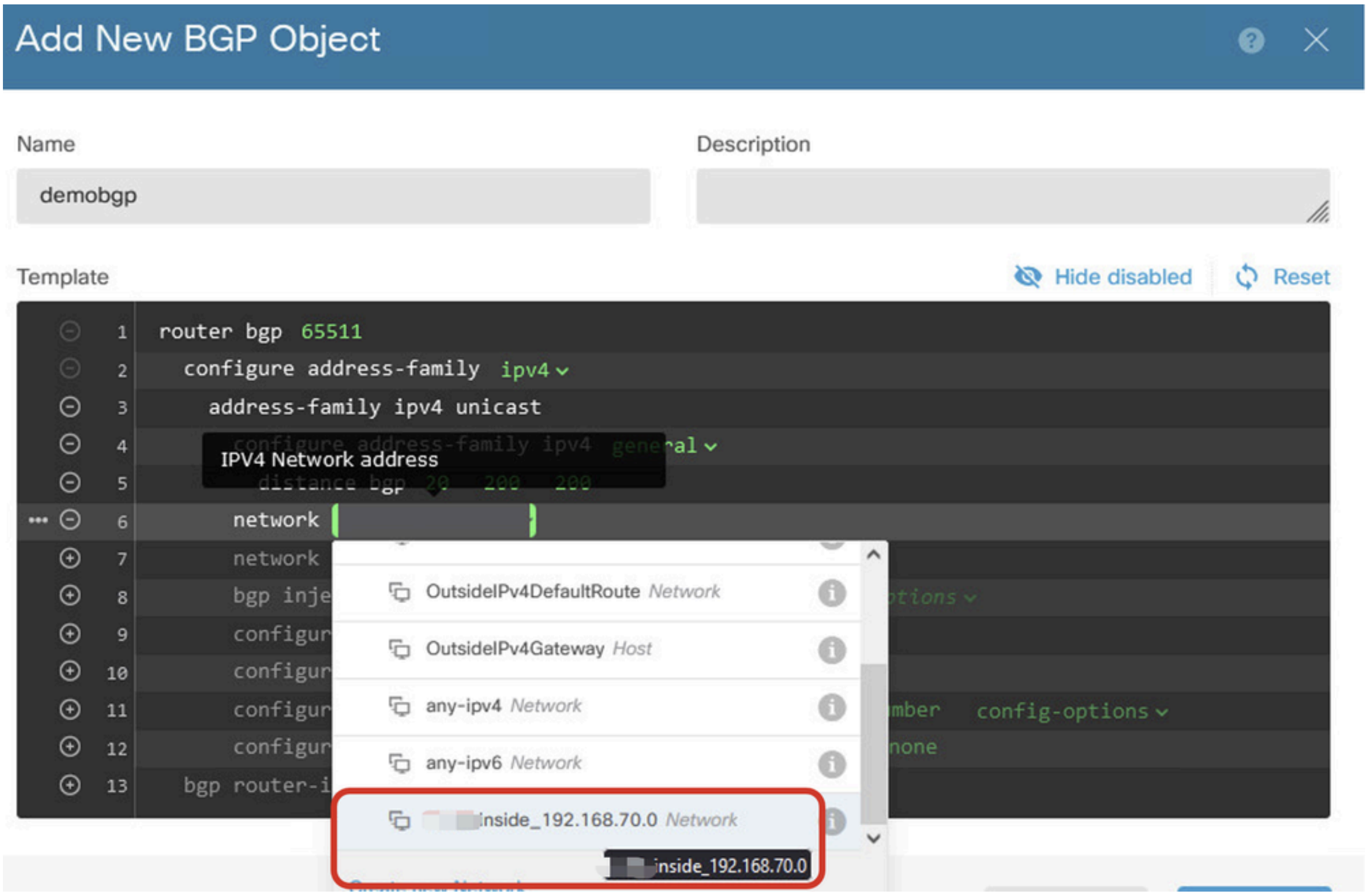
Name: demobgp

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 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



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
7        network
8        bgp inje                                   ptions
9        configur
10       configur
11       configur                                   mber  config-options
12       configur                                   none
13     bgp router-i
```

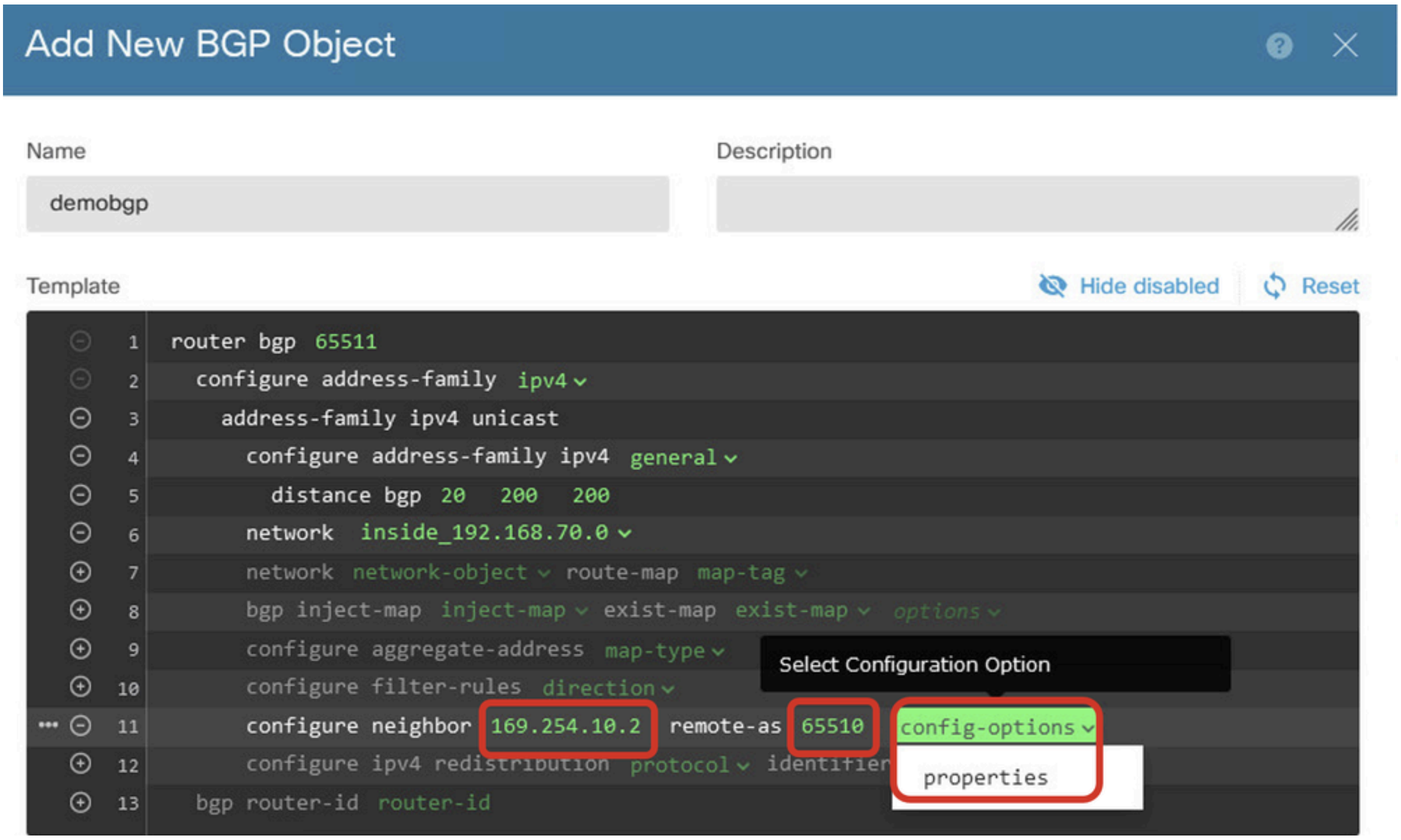
IPV4 Network address

- 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：點選+圖示可允許該行配置BGP鄰居相關資訊。按一下neighbor-address，然後手動輸入對等體BGP鄰居地址。在本例中，它是169.254.10.2（站點2 FTD的VTI IP地址）。按一下as-number，然後手動輸入對等體AS編號。在本例中，65510用於站點2 FTD。按一下config-options並選擇properties。



Name: demobgp

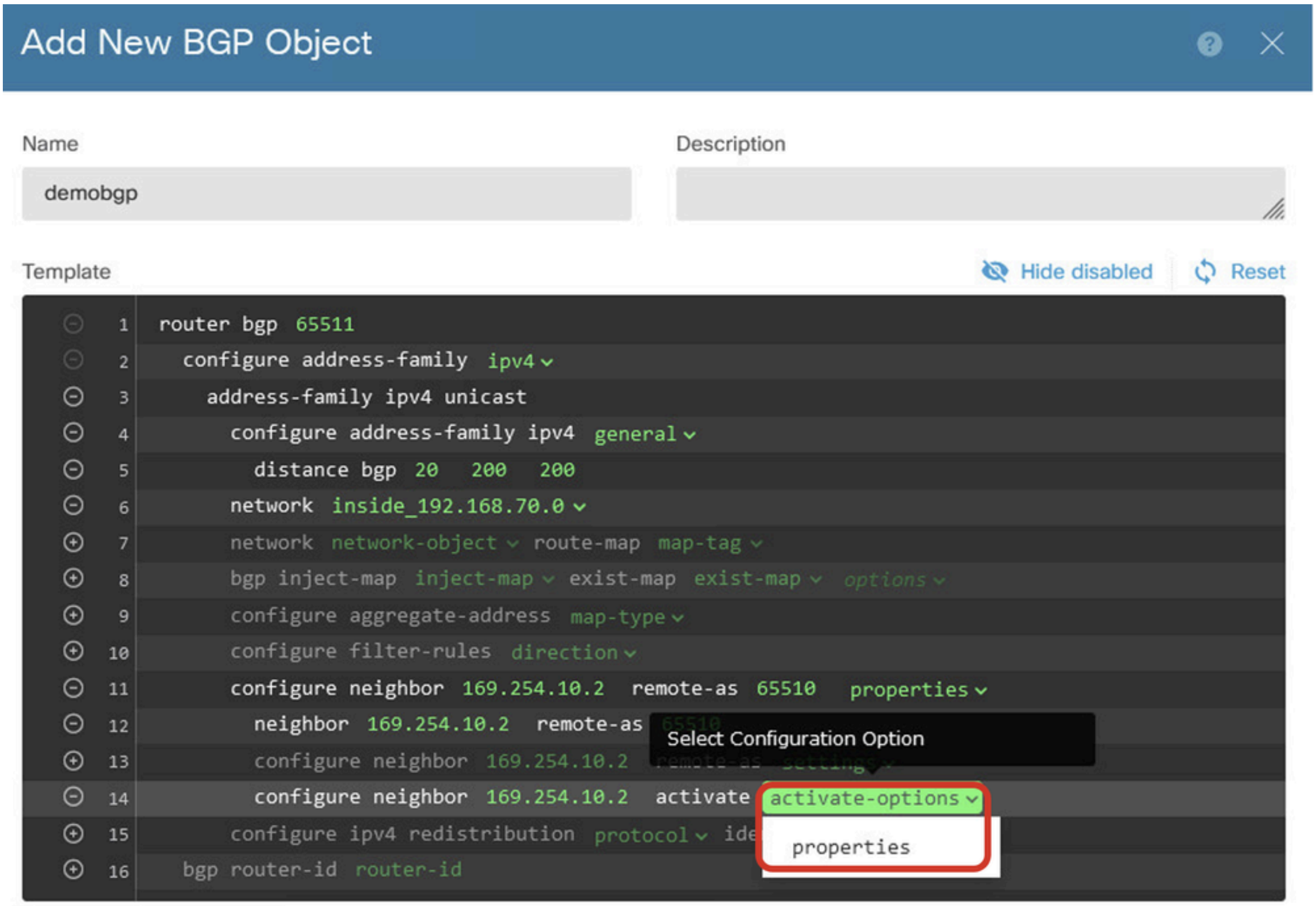
Description:

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：點選+圖示以啟用該行以配置鄰居的某些屬性。按一下activate-options並選擇properties。



Name: demobgp

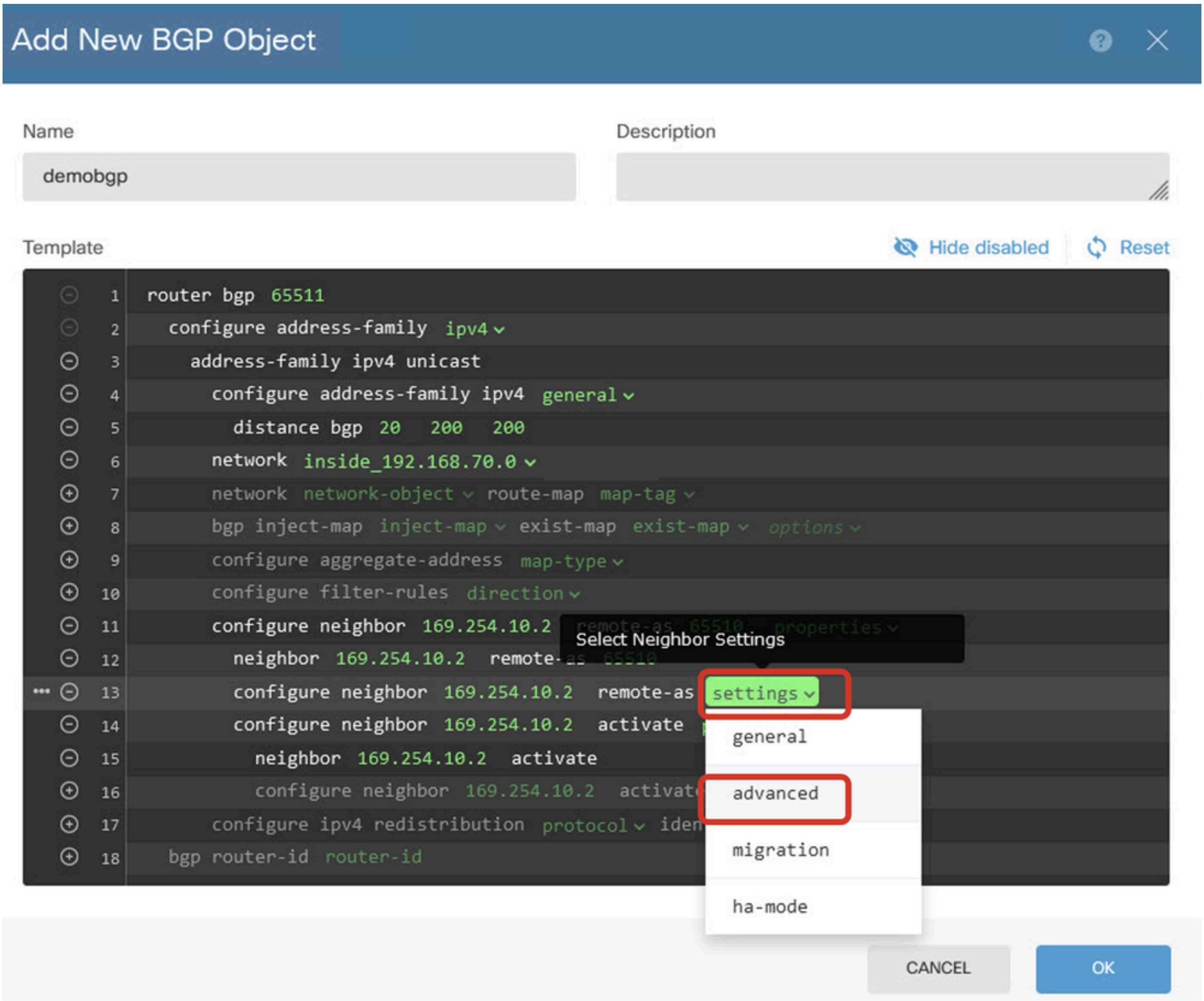
Description:

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：點選+圖示以顯示該行的高級選項。按一下設定並選擇高級。



Add New BGP Object

Name: demobgp

Description:

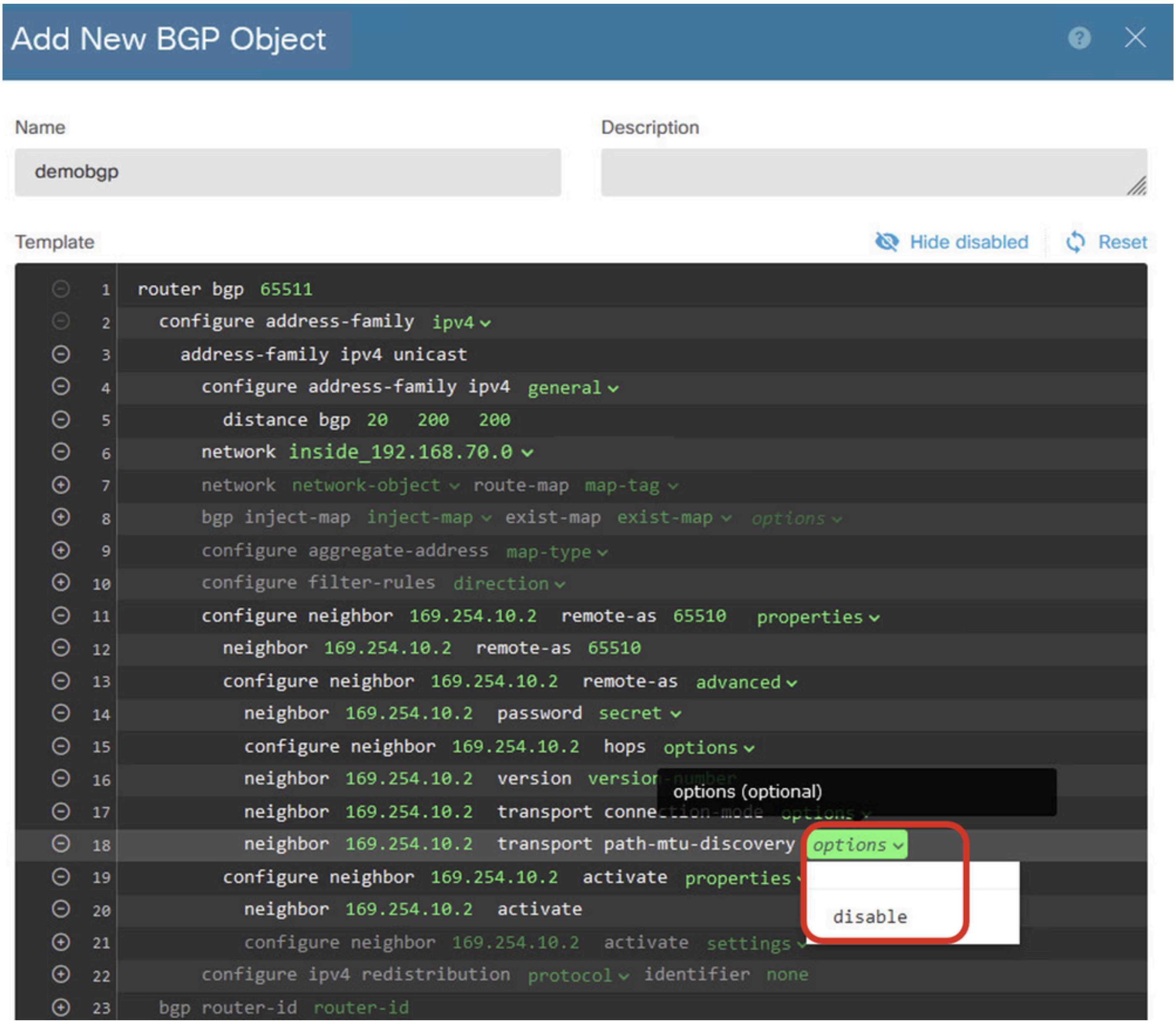
Template

```
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
```

Select Neighbor Settings

Create_BGP_Object_NeighborSetting_Properties_Advanced

第18行：點選選項並選擇停用以停用路徑MTU發現。



Add New BGP Object

Name: demobgp

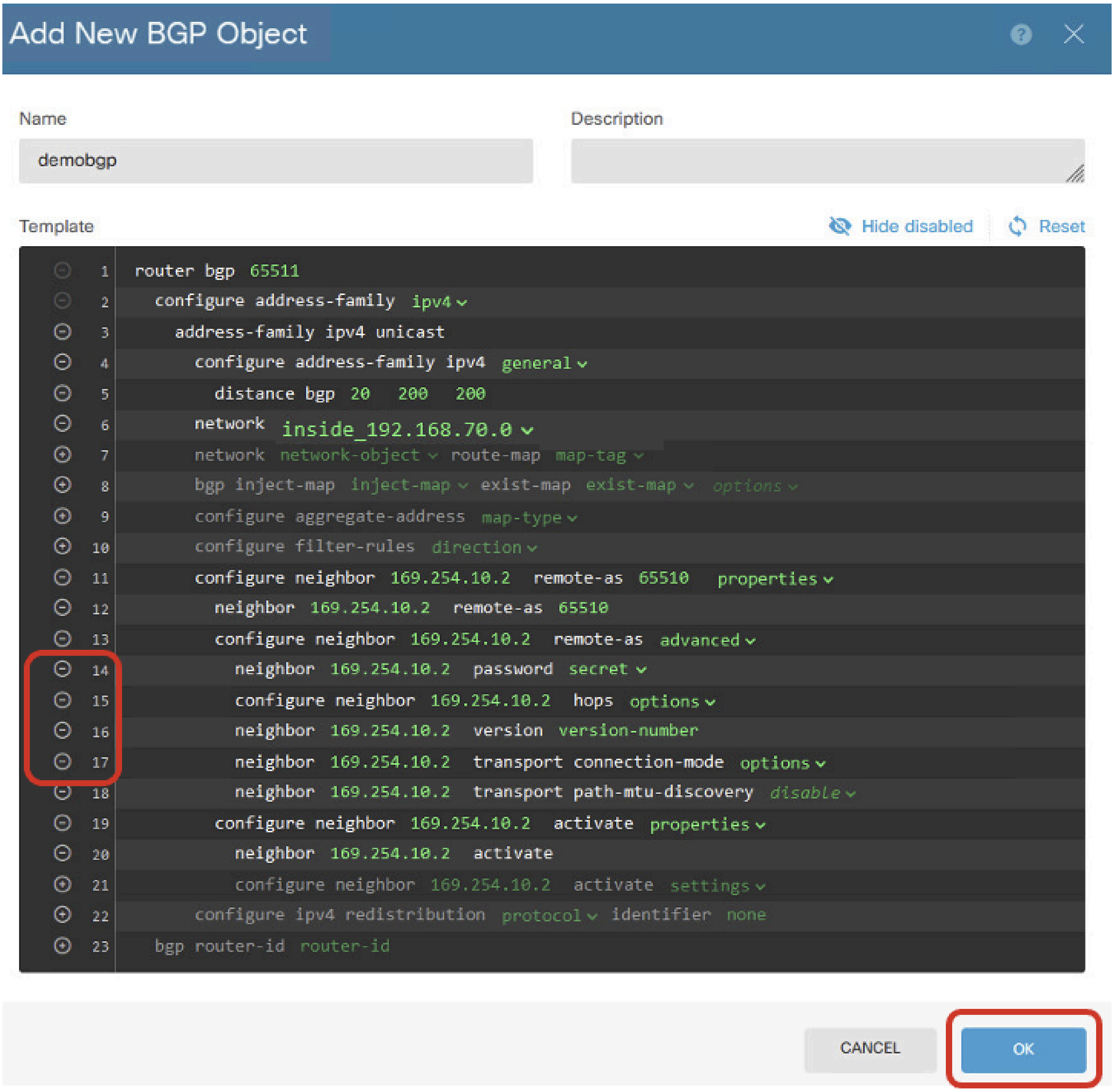
Description:

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 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

明細行14、15、16、17：按一下-按鈕以停用明細行。然後，按一下OK按鈕以儲存BGP對象。



Add New BGP Object

Name: demobgp

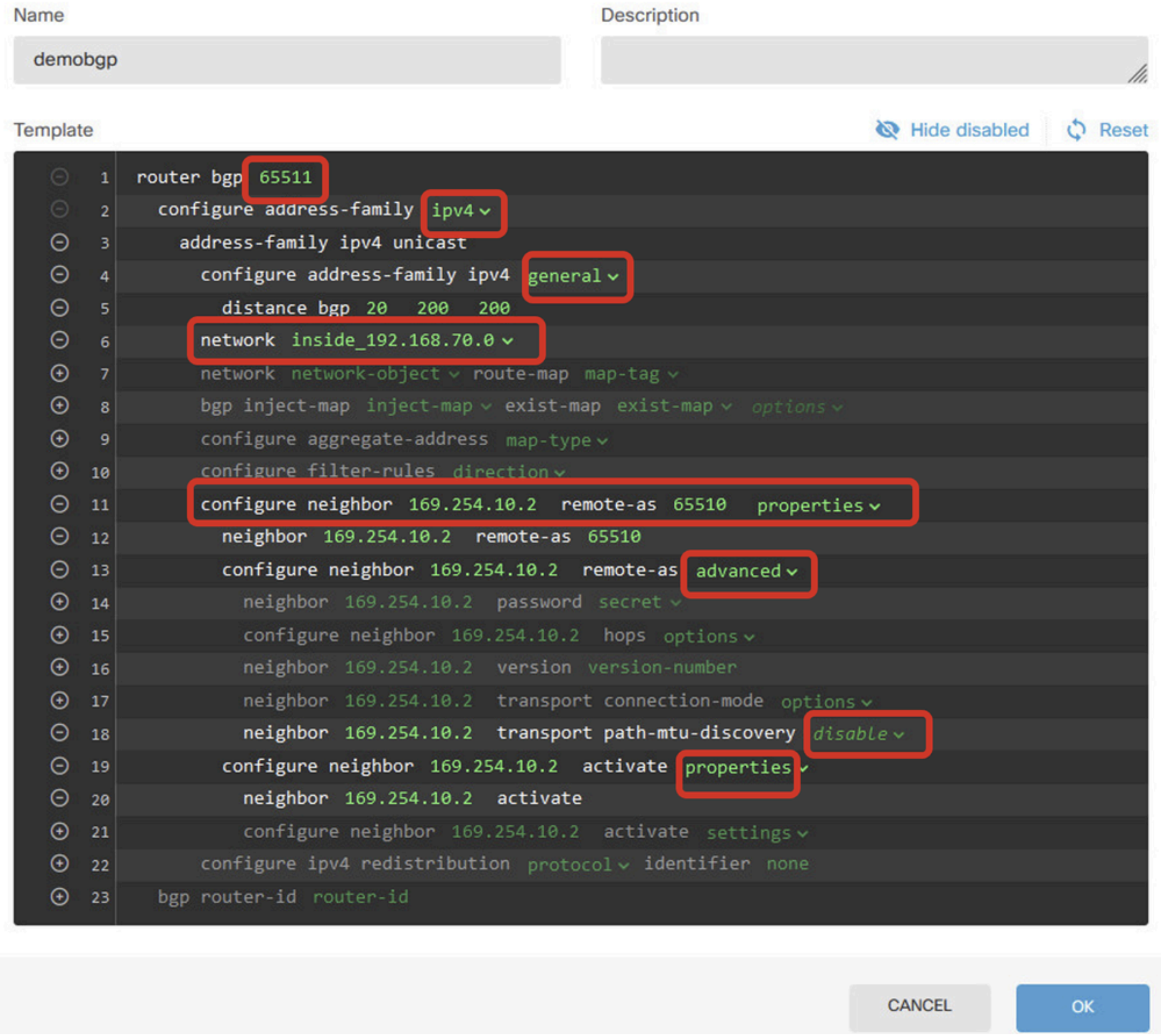
Description:

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_DisableLine

以下是此範例中BGP設定的概觀。您可以根據實際需求配置其他BGP設定。



Name: demobgp

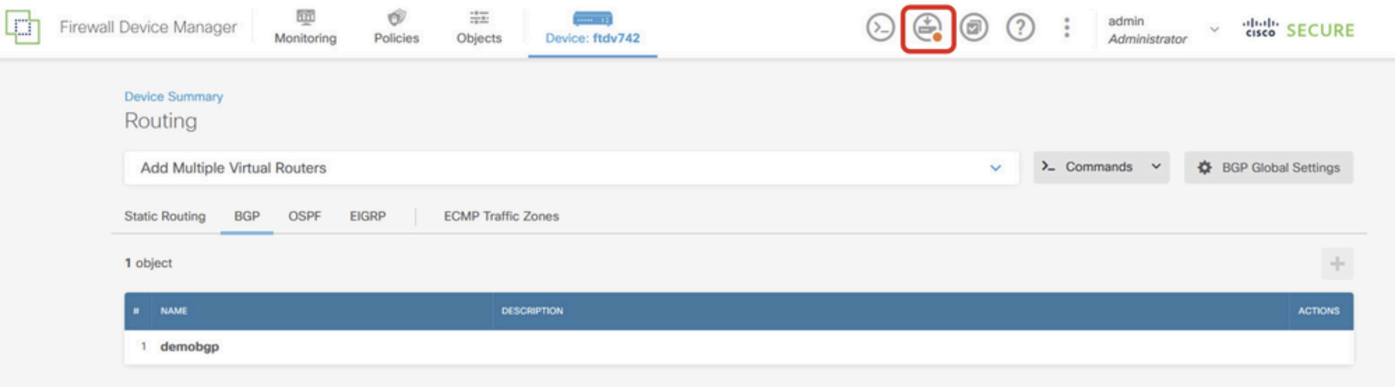
Description:

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

步驟 7.部署BGP配置更改。



1 object

#	NAME	DESCRIPTION	ACTIONS
1	demobgp		

部署_BGP_配置

步驟 8.現在，Site1 FTD的配置已完成。

若要設定Site2 FTD VPN和BGP，請對Site2 FTD的對應引數重複步驟3.到步驟7。

Site1 FTD和Site2 FTD在CLI中的配置概述。

站點1 FTD	站點2 FTD
NGFW版本7.4.2 interface GigabitEthernet0/0 nameif outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside 安全性層級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 隧道源介面外部 隧道目標192.168.10.1 通道模式ipsec ipv4 通道保護ipsec設定檔ipsec_profile|e4084d322d 對象網路OutsideIPv4網關 主機192.168.30.3 object network inside_192.168.70.0 子網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 | 任何ifc內268435457任何rule-id268435457事件日誌兩者之外的acSvcg-inter any ifc 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	NGFW版本7.4.2 interface GigabitEthernet0/0 nameif outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside 安全性層級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 隧道源介面外部 隧道目標192.168.30.1 通道模式ipsec ipv4 通道保護ipsec設定檔ipsec_profile|e4084d322d 對象網路OutsideIPv4網關 主機192.168.10.3 object network inside_192.168.50.0 子網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 | 任何ifc內268435457任何rule-id268435457事件日誌兩者之外的acSvcg-inter any ifc 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-

```
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：訪問策略：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 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
鄰居169.254.10.2啟用
網路192.168.70.0
no auto-summary
無同步
exit-address-family

0.0.0.0 0.0.0.0 192.168.30.3 1外部的路由

crypto ipsec ikev2 ipsec-proposal AES256_SHA256
協定esp加密aes-256 aes
協定esp完整性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
完整性sha256 sha
群組14
prf sha256 sha
lifetime seconds 86400

crypto ikev2 policy 20
加密aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
組21 20 16 15 14
prf sha512 sha384 sha256 sha
```

```
group |acSvcg-268435458 any any rule-id 268435458 event-log both
access-list NGFW_ONBOX_ACL remark rule-id 1：訪問策略：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 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
鄰居169.254.10.1啟用
網路192.168.50.0
no auto-summary
無同步
exit-address-family

0.0.0.0 0.0.0.0 192.168.10.3 1外部的路由

crypto ipsec ikev2 ipsec-proposal AES256_SHA256
協定esp加密aes-256 aes
協定esp完整性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
完整性sha256 sha
群組14
prf sha256 sha
lifetime seconds 86400

crypto ikev2 policy 20
加密aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
組21 20 16 15 14
prf sha512 sha384 sha256 sha
lifetime seconds 86400
```

lifetime seconds 86400 crypto ikev2 enable outside 組策略 |s2sGP|192.168.10.1內部 組策略 |s2sGP|192.168.10.1屬性 vpn隧道協定ikev2 tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1一般屬性 default-group-policy |s2sGP|192.168.10.1 隧道組192.168.10.1 ipsec屬性 ikev2遠端身份驗證預共用金鑰***** ikev2本地身份驗證預共用金鑰*****	crypto ikev2 enable outside 組策略 |s2sGP|192.168.30.1內部 組策略 |s2sGP|192.168.30.1屬性 vpn隧道協定ikev2 tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1一般屬性 default-group-policy |s2sGP|192.168.30.1 隧道組192.168.30.1 ipsec屬性 ikev2遠端身份驗證預共用金鑰***** ikev2本地身份驗證預共用金鑰*****

驗證

使用本節內容，確認您的組態是否正常運作。

步驟 1.透過控制檯或SSH導航到每個FTD的CLI，透過show crypto ikev2 sa和show crypto ipsec sa命令驗證階段1和階段2的VPN狀態。

站點1 FTD	站點2 FTD
ftdv742# show crypto ikev2 sa IKEv2 SA： Session-id：134， Status：UP-ACTIVE， IKE count：1， CHILD count：1 隧道ID本地遠端fvrf/ivrf狀態角色 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER 加密：AES-CBC，金鑰大小：256，雜湊：SHA256，DH組：14，身份驗證簽名：PSK，身份驗證驗證：PSK 壽命/活動時間：86400/5145秒 子sa：本地選擇器0.0.0.0/0 - 255.255.255.255/65535 遠端選擇器0.0.0.0/0 - 255.255.255.255/65535 ESP spi輸入/輸出： 0xf0c4239d/0xb7b5b38b	ftdv742# show crypto ikev2 sa IKEv2 SA： Session-id：13， Status：UP-ACTIVE， IKE count：1， CHILD count：1 隧道ID本地遠端fvrf/ivrf狀態角色 339797985 192.168.10.1/500 192.168.30.1/500全局/全局就緒啟動器 加密：AES-CBC，金鑰大小：256，雜湊：SHA256，DH組：14，身份驗證簽名：PSK，身份驗證驗證：PSK 壽命/活動時間：86400/74099秒 子sa：本地選擇器0.0.0.0/0 - 255.255.255.255/65535 遠端選擇器0.0.0.0/0 - 255.255.255.255/65535 ESP spi輸入/輸出： 0xb7b5b38b/0xf0c4239d

ftdv742# show crypto ipsec sa 介面：demovti 　加密對映標籤： __vti-crypto-map-Tunnel1-0-1、seq num： 65280、local addr：192.168.30.1 受保護的vrf (ivrf)：全球 本地ident (addr/mask/prot/port)：(0.0.0.0/0.0.0.0/0/0) 遠端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 decap： 5717，#pkts decrypt：5717，#pkts verify： 5717 #pkts壓縮：0，#pkts解壓縮：0 未#pkts壓縮： 5720，#pkts comp失敗：0，#pkts解壓縮失敗： 0 #pre-frag成功：0，#pre-frag失敗：0，#fragments建立：0 已傳送#PMTUs：0，#PMTUs rcvd：0，需要重組的#decapsulated frgs：0 #TFC rcvd：0，#TFC傳送：0 #Valid ICMP錯誤rcvd：0，#Invalid ICMP錯誤rcvd：0 #send錯誤： 0，#recv錯誤： 0 本地加密端點： 192.168.30.1/500，遠端加密端點： 192.168.10.1/500 路徑mtu 1500，ipsec開銷78(44)，媒體mtu 1500 剩餘PMTU時間（秒）：0，DF策略：copy-df ICMP錯誤驗證：已停用，TFC資料包：已停用 當前出站spi：B7B5B38B 當前入站spi：F0C4239D 入站esp sa： spi： 0xF0C4239D (4039386013) SA狀態：活動 轉換：esp-aes-256 esp-sha-256-hmac無壓縮 使用中的設定={L2L，隧道，IKEv2，VTI，} 插槽：0，conn_id：266，加密對映：__vti-crypto-map-Tunnel1-0-1 sa計時：剩餘金鑰存留期（kB/秒）：(4285389/3722)	ftdv742# show crypto ipsec sa 介面：demovti25 　加密對映標籤： __vti-crypto-map-Tunnel1-0-1，序列號為65280，本地地址：192.168.10.1 受保護的vrf (ivrf)：全球 本地ident (addr/mask/prot/port)：(0.0.0.0/0.0.0.0/0/0) 遠端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 decap：5721，#pkts decrypt：5721，#pkts verify：5721 #pkts壓縮：0，#pkts解壓縮：0 #pkts未壓縮： 5721，#pkts comp失敗：0，#pkts解壓縮失敗： 0 #pre-frag成功：0，#pre-frag失敗：0，#fragments建立：0 已傳送#PMTUs：0，#PMTUs rcvd：0，需要重組的#decapsulated frgs：0 #TFC rcvd：0，#TFC傳送：0 #Valid ICMP錯誤rcvd：0，#Invalid ICMP錯誤rcvd：0 #send錯誤： 0，#recv錯誤： 0 本地加密端點： 192.168.10.1/500，遠端加密端點： 192.168.30.1/500 路徑mtu 1500，ipsec開銷78(44)，媒體mtu 1500 剩餘PMTU時間（秒）：0，DF策略：copy-df ICMP錯誤驗證：已停用，TFC資料包：已停用 當前出站spi：F0C4239D 當前入站spi：B7B5B38B 入站esp sa： spi： 0xB7B5B38B (3082138507) SA狀態：活動 轉換：esp-aes-256 esp-sha-256-hmac無壓縮 使用中的設定={L2L，隧道，IKEv2，VTI，} 插槽：0，conn_id：160，加密對映：__vti-crypto-map-Tunnel1-0-1 sa計時：剩餘金鑰存留期（kB/秒）：(3962829/3626) IV大小：16位元組

IV大小：16位元組 重新執行偵測支援：Y 防重播點陣圖： 0xFFFFFFFF 0xFFFFFF 出站esp sa： spi： 0xB7B5B38B (3082138507) SA狀態：活動 轉換：esp-aes-256 esp-sha-256-hmac無壓縮 使用中的設定={L2L，隧道，IKEv2，VTI，} 插槽：0，conn_id：266，加密對映：__vti-crypto-map-Tunnel1-0-1 sa計時：剩餘金鑰存留期（kB/秒）： (4147149/3722) IV大小：16位元組 重新執行偵測支援：Y 防重播點陣圖： 0x00000000 0x00000001	重新執行偵測支援：Y 防重播點陣圖： 0xFFFFFFFF 0xFFFFFF 出站esp sa： spi： 0xF0C4239D (4039386013) SA狀態：活動 轉換：esp-aes-256 esp-sha-256-hmac無壓縮 使用中的設定={L2L，隧道，IKEv2，VTI，} 插槽：0，conn_id：160，加密對映：__vti-crypto-map-Tunnel1-0-1 sa計時：剩餘金鑰存留期（kB/秒）： (4101069/3626) IV大小：16位元組 重新執行偵測支援：Y 防重播點陣圖： 0x00000000 0x00000001

步驟 2. 使用命令show bgp neighbors和show route bgp透過控制檯或SSH導航到每個FTD的CLI以驗證BGP狀態。

站點1 FTD	站點2 FTD
ftdv742# show bgp neighbors BGP鄰居是169.254.10.2，vrf single_vf，遠端AS 65510，外部鏈路 BGP版本4，遠端路由器ID 192.168.50.1 BGP狀態=已建立，持續1d20h 上次讀取00:00:25，上次寫入00:00:45，保持時間為180，保持連線間隔為60秒 鄰居會話： 1個使用中，不支援多重作業階段（停用） 鄰居功能： 路由刷新：已通告和已接收（新） 四八位組ASN功能：已通告和已接收 地址系列IPv4單播：已通告和接收 多會話功能： 訊息統計資料： InQ深度為0 OutQ深度為0 傳送的Rcvd 開啟：1 1 通知：0 0 更新： 2 2	ftdv742# show bgp neighbors BGP鄰居是169.254.10.1，vrf single_vf，遠端AS 65511，外部鏈路 BGP版本4，遠端路由器ID 192.168.70.1 BGP狀態=已建立，持續1d20h 上次讀取00:00:11，上次寫入00:00:52，保持時間為180，保持連線間隔為60秒 鄰居會話： 1個使用中，不支援多重作業階段（停用） 鄰居功能： 路由刷新：已通告和已接收（新） 四八位組ASN功能：已通告和已接收 地址系列IPv4單播：已通告和接收 多會話功能： 訊息統計資料： InQ深度為0 OutQ深度為0 傳送的Rcvd 開啟：1 1 通知：0 0 更新： 2 2

Keepalive： 2423 2427 路由刷新：0 0 合計：2426 2430 通告運行之間的預設最短時間為30秒 對於地址系列：IPv4單播 會話：169.254.10.2 BGP表版本3，鄰居版本3/0 輸出隊列大小： 0 索引1 1個更新組成員 傳送的Rcvd 字首活動：---- ---- 當前字首：1 1（使用80位元組） 字首總數：1 1 隱含撤銷： 0 0 明確撤銷：0 0 用作bestpath：n/a 1 用作多重路徑：n/a 0 出站入站 本地策略拒絕的字首： -------- ------- 來自此對等體的最佳路徑：1 n/a 合計：1 0 傳送的更新中的NLRI數：最大1，最小0 已啟用地址跟蹤，RIB確實具有到169.254.10.2的路由 已建立連線1；已丟棄0 上次重設永不 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart已停用	Keepalive： 2424 2421 路由刷新：0 0 合計：2427 2424 通告運行之間的預設最短時間為30秒 對於地址系列：IPv4單播 會話：169.254.10.1 BGP表版本9，鄰居版本9/0 輸出隊列大小： 0 索引4 4個更新組成員 傳送的Rcvd 字首活動：---- ---- 當前字首：1 1（使用80位元組） 字首總數：1 1 隱含撤銷： 0 0 明確撤銷：0 0 用作bestpath：n/a 1 用作多重路徑：n/a 0 出站入站 本地策略拒絕的字首： -------- ------- 來自此對等體的最佳路徑：1 n/a 合計：1 0 傳送的更新中的NLRI數：最大1，最小0 已啟用地址跟蹤，RIB確實具有到169.254.10.1的路由 已建立連線4；已丟棄3 上次重置1d21h，由於會話1的介面抖動 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart已停用
ftdv742# show route bgp 代碼：L -本地，C -已連線，S -靜態，R -RIP，M -移動，B - BGP D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF區域間 N1 - OSPF NSSA外部型別1，N2 - OSPF NSSA外部型別2 E1 - OSPF外部型別1、E2 - OSPF外部型別2、V - VPN i - IS-IS， su - IS-IS摘要， L1 - IS-IS級別1， L2 - IS-IS級別2 ia - IS-IS內部區域， * -候選預設值， U -每使用	ftdv742# show route bgp 代碼：L -本地，C -已連線，S -靜態，R -RIP，M -移動，B - BGP D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF區域間 N1 - OSPF NSSA外部型別1，N2 - OSPF NSSA外部型別2 E1 - OSPF外部型別1、E2 - OSPF外部型別2、V - VPN i - IS-IS， su - IS-IS摘要， L1 - IS-IS級別1， L2 - IS-IS級別2 ia - IS-IS內部區域， * -候選預設值， U -每使用

者靜態路由 o - ODR， P -定期下載的靜態路由， + -複製路由 SI -靜態InterVRF、BI - BGP InterVRF 最後選用網關是192.168.30.3到網路0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0]（透過169.254.10.2,1d20h）	者靜態路由 o - ODR， P -定期下載的靜態路由， + -複製路由 SI -靜態InterVRF、BI - BGP InterVRF 最後選用網關是192.168.10.3到網路0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0]（透過169.254.10.1,1d20h）

步驟 3.Site1客戶端和Site2客戶端相互之間成功ping通。

站點1客戶端：

```
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
```

站點2客戶端：

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

可使用這些debug命令對VPN部分進行故障排除。

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

可使用這些debug命令排除BGP部分故障。

```
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>
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。