在FDM管理的FTD上配置VRF感知路由型站點到站點VPN

目錄

簡介

本檔案介紹如何在FDM管理的FTD上設定VRF感知路由型站對站VPN。

必要條件

需求

思科建議您瞭解以下主題：

- 對VPN有基礎認識
- 對虛擬路由和轉送(VRF)有基礎認識
- 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 7.4.2版
- Cisco FDM版本7.4.2
- Cisco ASAv版本9.20.3

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。

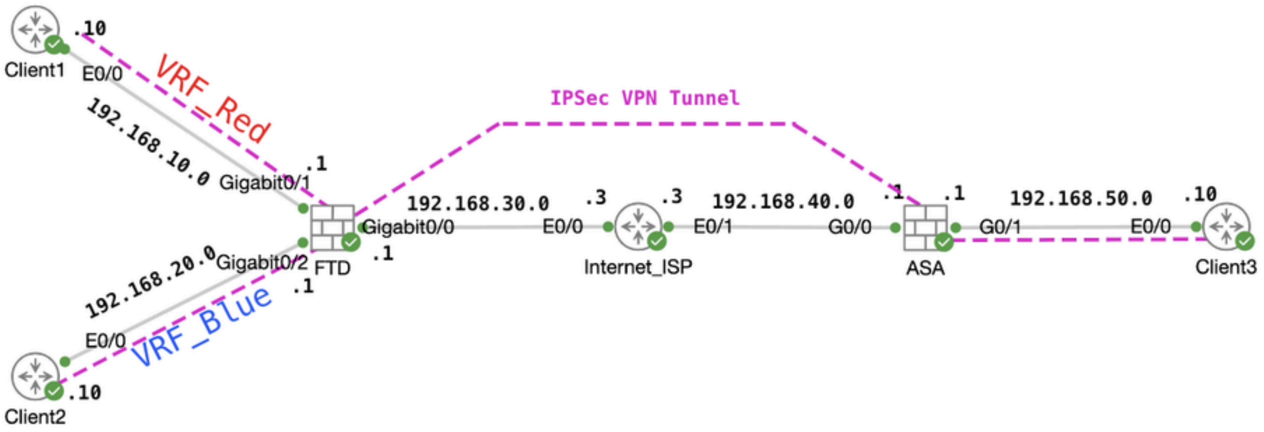
背景資訊

Firepower裝置管理器(FDM)上的虛擬路由和轉發(VRF)允許您在單個Firepower威脅防禦(FTD)裝置上建立多個隔離路由例項。每個VRF例項都作為單獨的虛擬路由器運行，具有自己的路由表，從而實現網路流量的邏輯分離，並提供增強的安全性和流量管理功能。

本文檔說明如何使用VTI配置VRF感知IPSec VPN。VRF紅色網路和VRF藍色網路位於FTD之後。VRF Red網路中的Client1和VRF Blue中的Client2將通過IPSec VPN隧道與ASA後面的客戶端3通訊。

設定

網路圖表

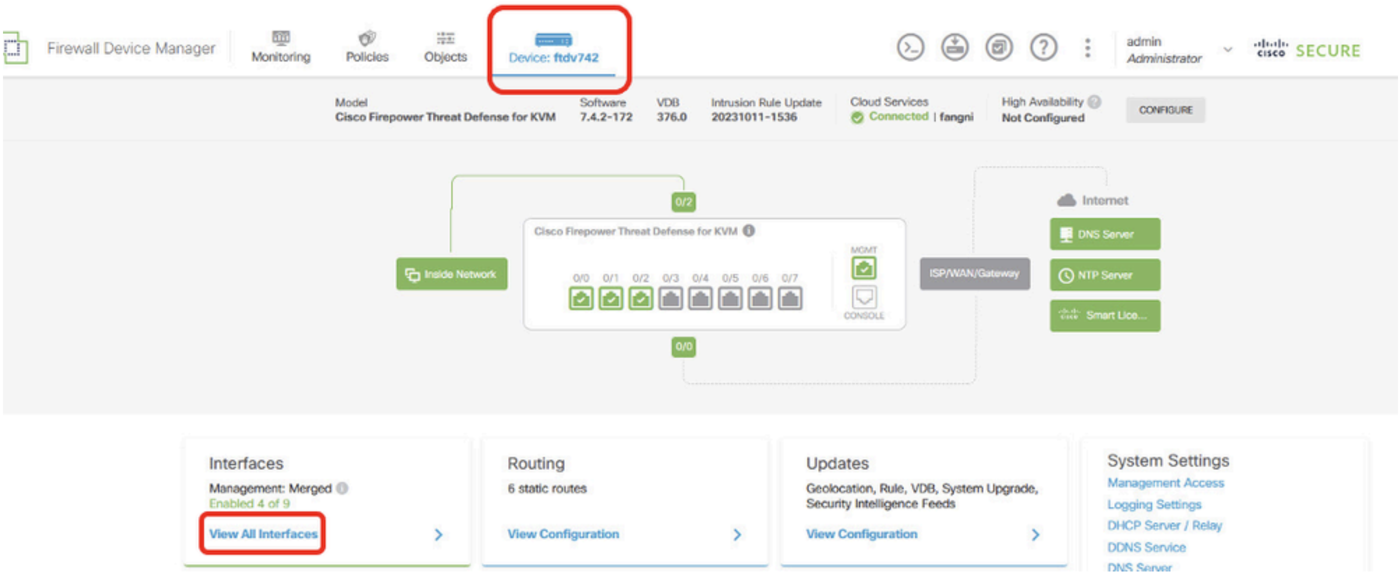


拓撲

設定FTD

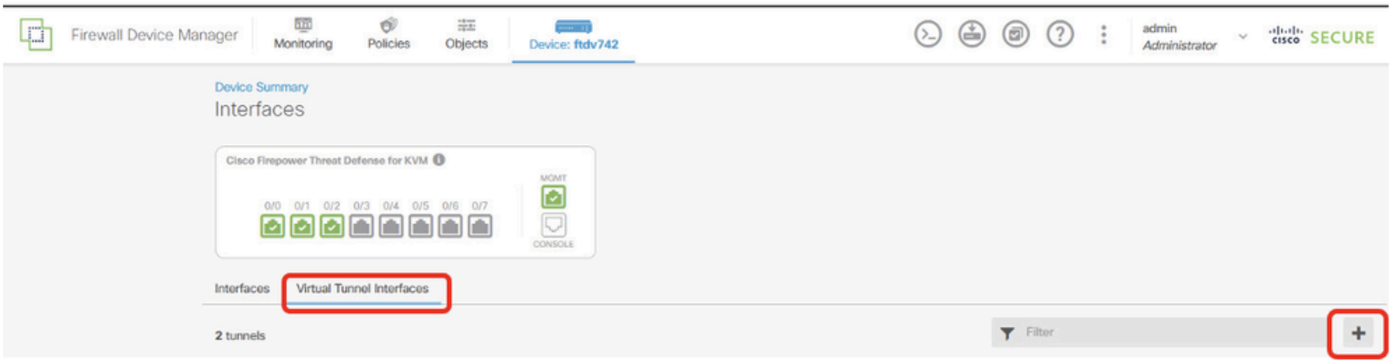
步驟1.必須確保已經完成節點之間IP互連的初步配置。Client1和Client2使用FTD Inside IP位址作為閘道。 Client3使用ASA內部IP地址作為網關。

步驟2.建立虛擬通道介面。登入FTD的FDM GUI。導航到Device > Interfaces。按一下「View All Interfaces」。



FTD_View_Interface

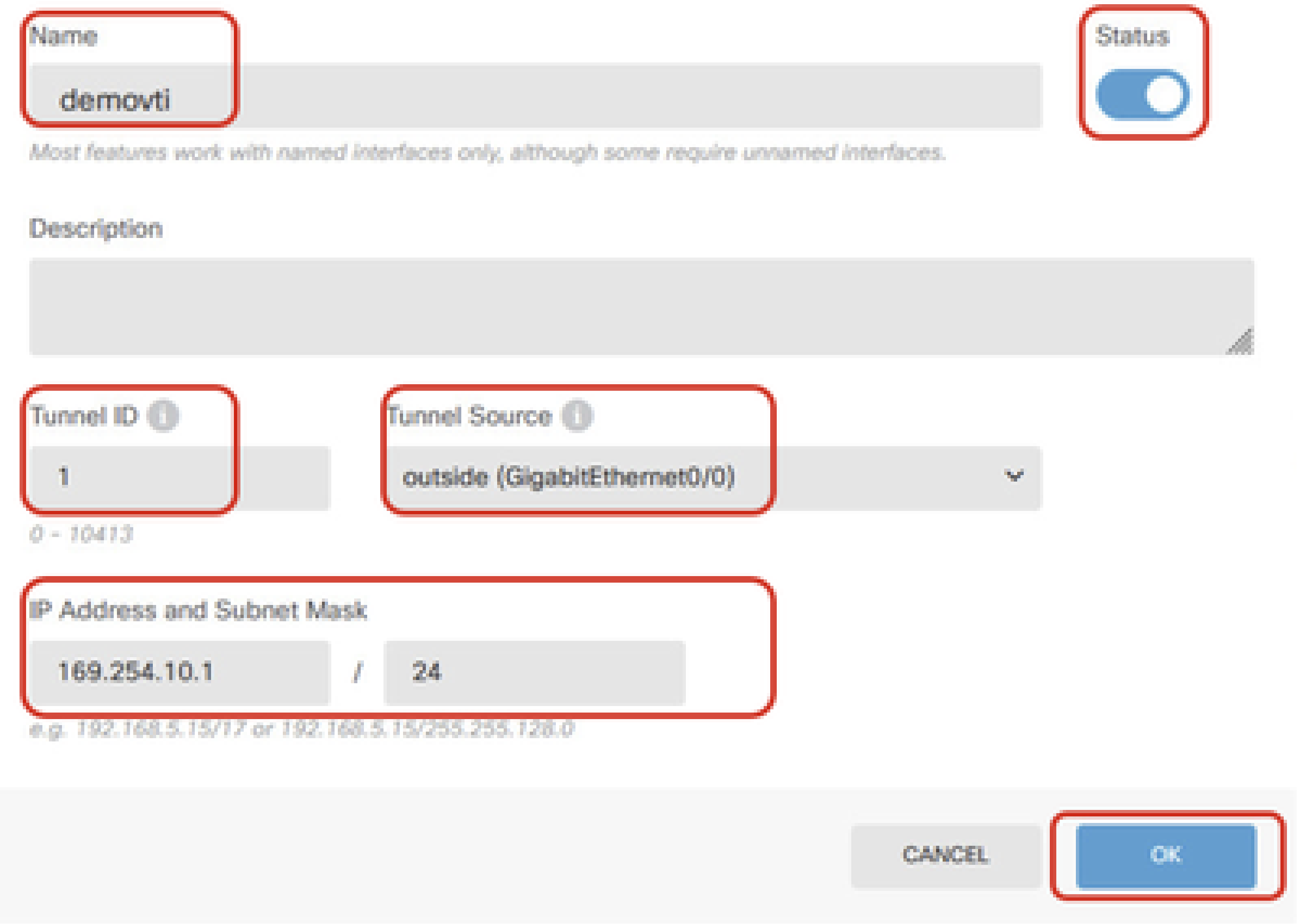
步驟2.1.按一下Virtual Tunnel Interfaces索引標籤。按一下+按鈕。



FTD_Create_VTI

步驟2.2.提供必要資訊。按一下「OK」按鈕。

- 名稱:demovti
- 通道ID:1
- 通道來源：outside(GigabitEthernet0/0)
- IP地址和子網掩碼：169.254.10.1/24
- 狀態:按一下滑塊到「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

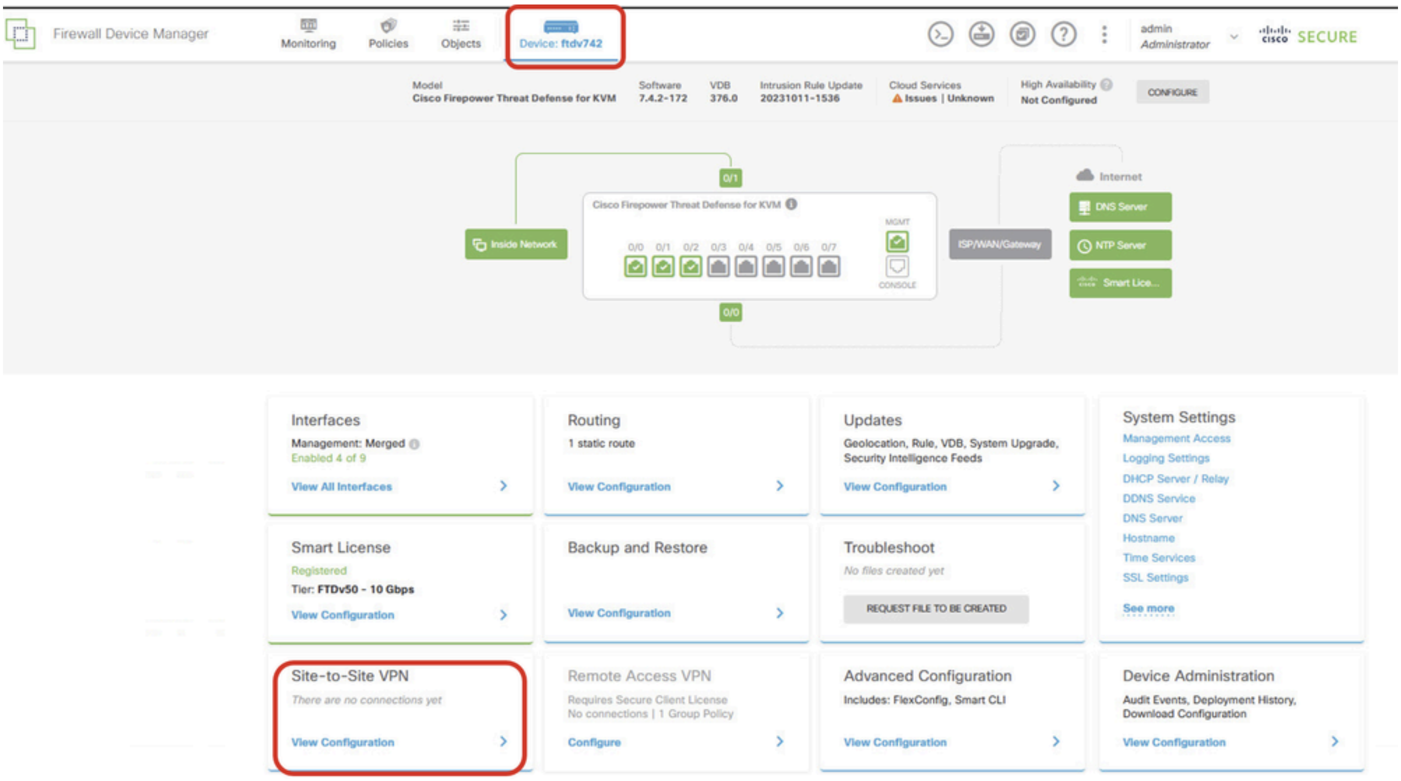
Tunnel Source: outside (GigabitEthernet0/0)

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

FTD_Create_VTI_Details

步驟3.導覽至Device > Site-to-Site VPN。按一下View Configuration按鈕。



Model: Cisco Firepower Threat Defense for KVM | Software: 7.4.2-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Issues | Unknown | High Availability: Not Configured

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 >

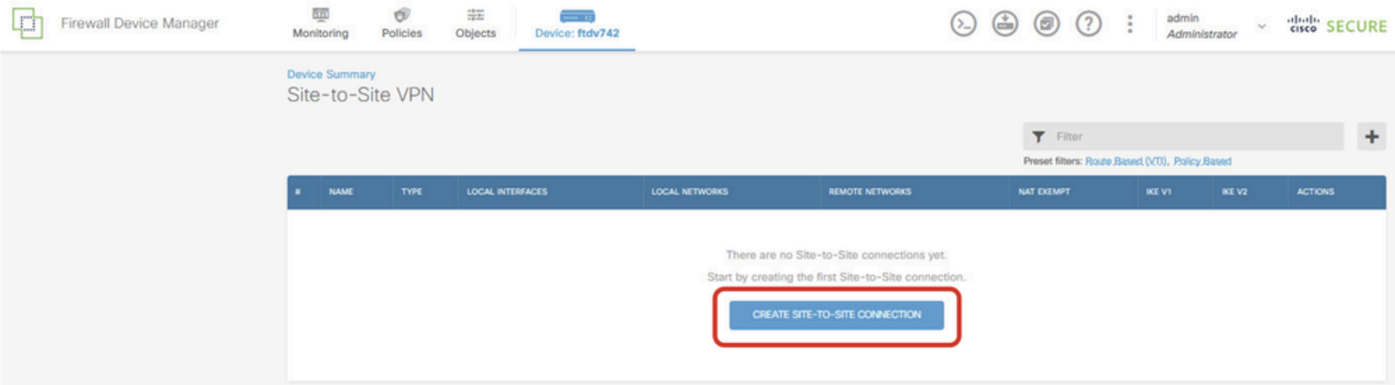
Remote Access VPN
Requires Secure Client License
No connections | 1 Group Policy
Configure >

Advanced Configuration
Includes: FlexConfig, Smart CLI
View Configuration >

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

FTD_Site-to-Site_VPN_View_Configurations

步驟3.1.開始建立新的站點到站點VPN。按一下CREATE SITE-TO-SITE CONNECTION 按鈕。或按一下+按鈕。



Device Summary

Site-to-Site VPN

Preset filters: Route Based (VTI), Policy Based

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

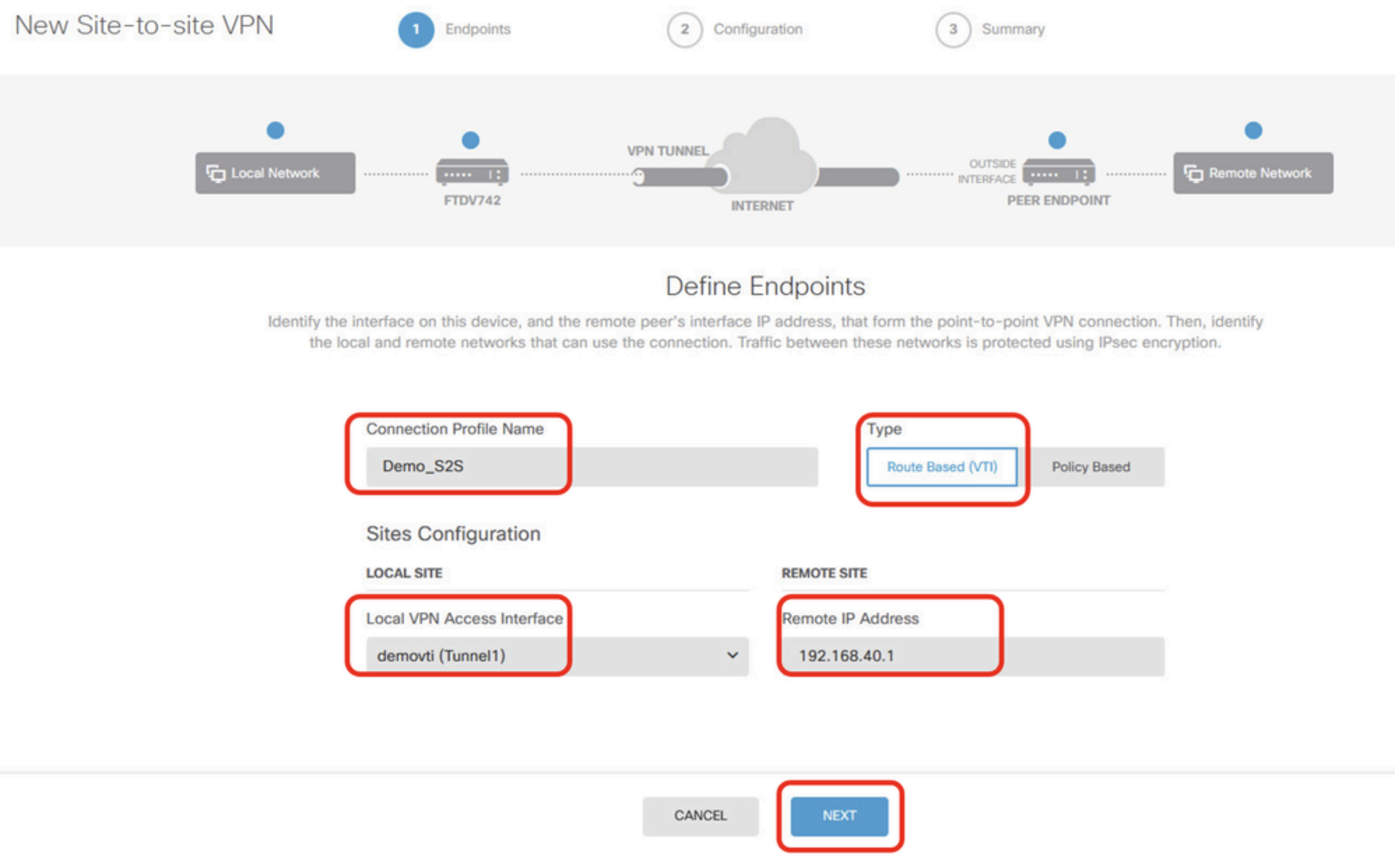
There are no Site-to-Site connections yet.

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

FTD_Create_Site2Site_Connection

步驟 3.2. 提供 必要資訊。按一下「NEXT」按鈕。

- 連線配置檔名稱：演示_S2
- Type:路由型(VTI)
- 本地VPN訪問介面：演示（在步驟2中建立）
- 遠端IP地址：192.168.40.1（這是外部IP地址的對等ASA）


New Site-to-site VPN

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

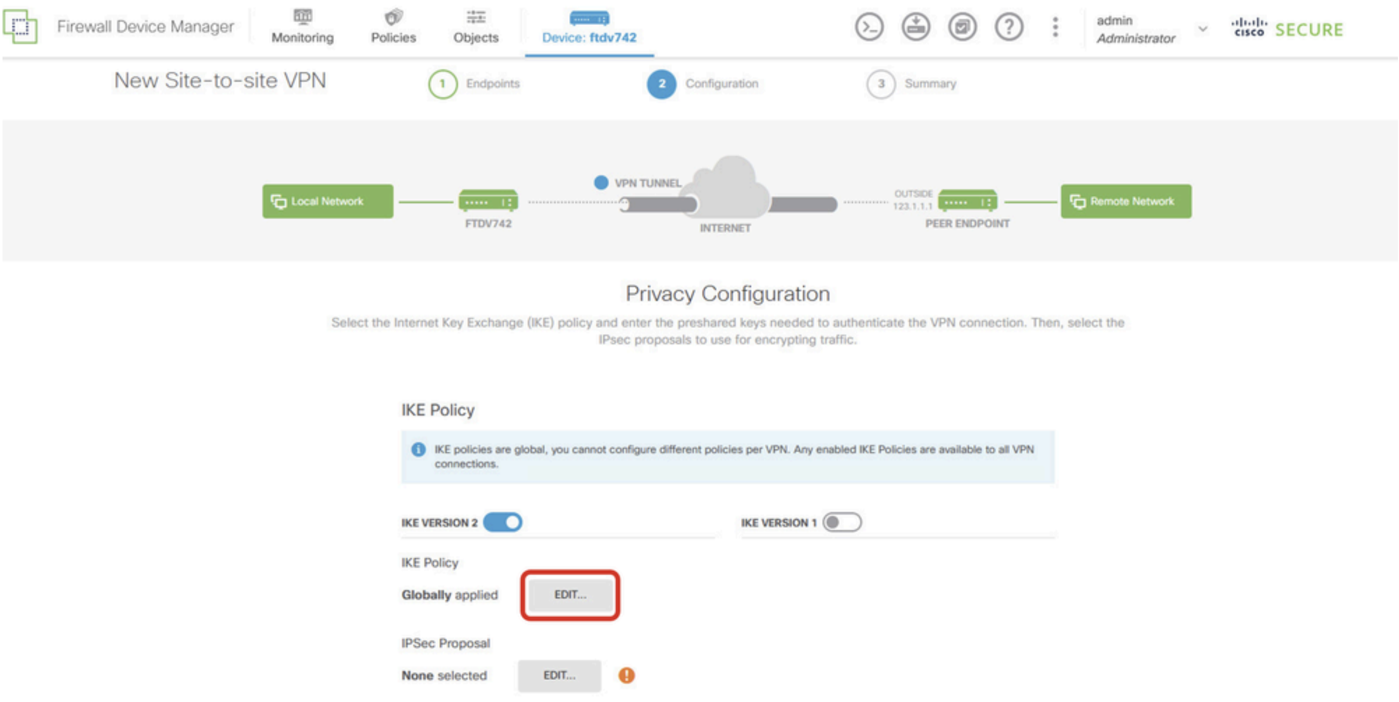
Local VPN Access Interface: demovti (Tunnel1)

REMOTE SITE

Remote IP Address: 192.168.40.1

FTD_Site-to-Site_VPN_Endpots

步驟3.3.導航到IKE Policy。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...

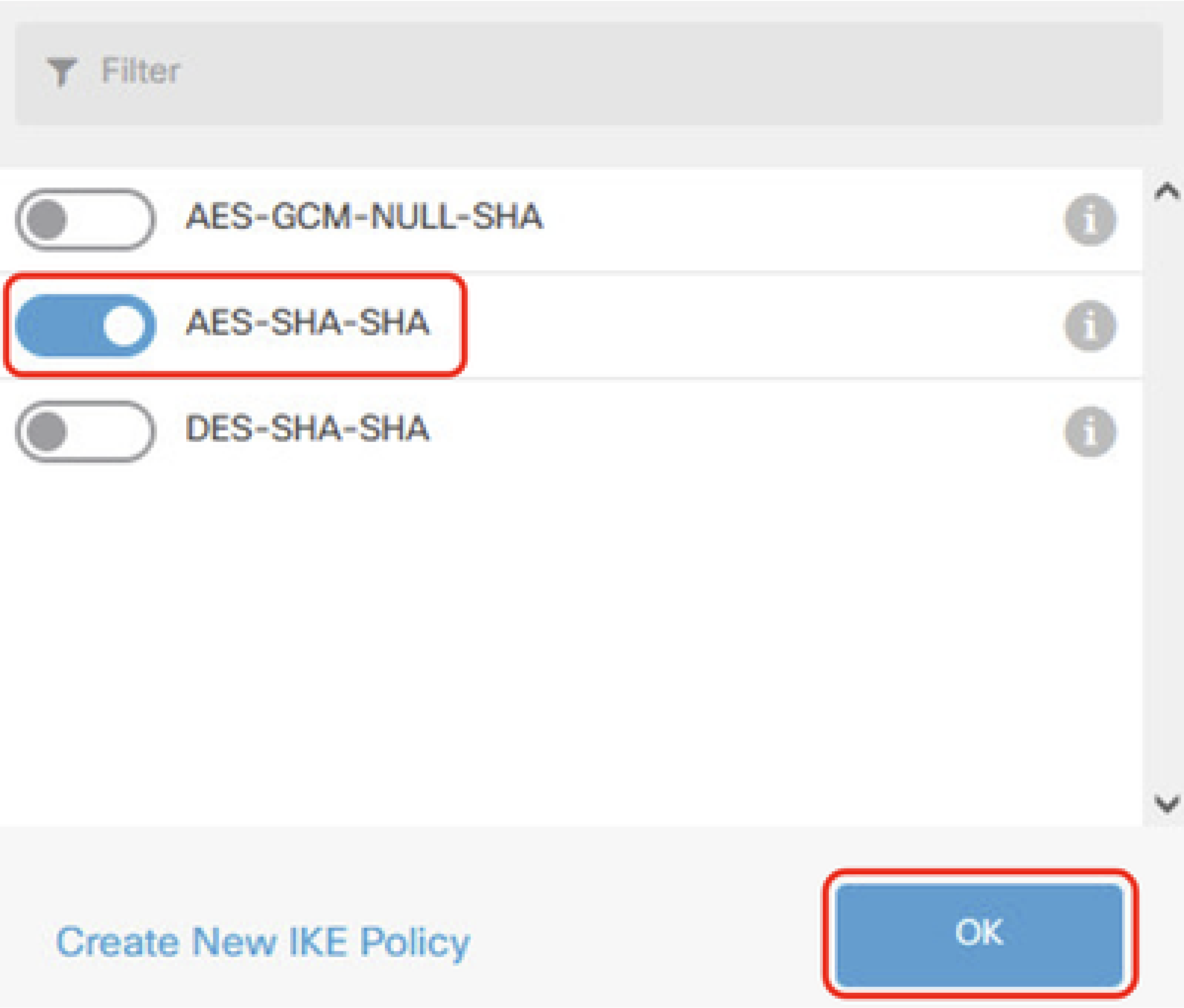
IPSec Proposal

None selected EDIT...

FTD_Edit_IKE_Policy

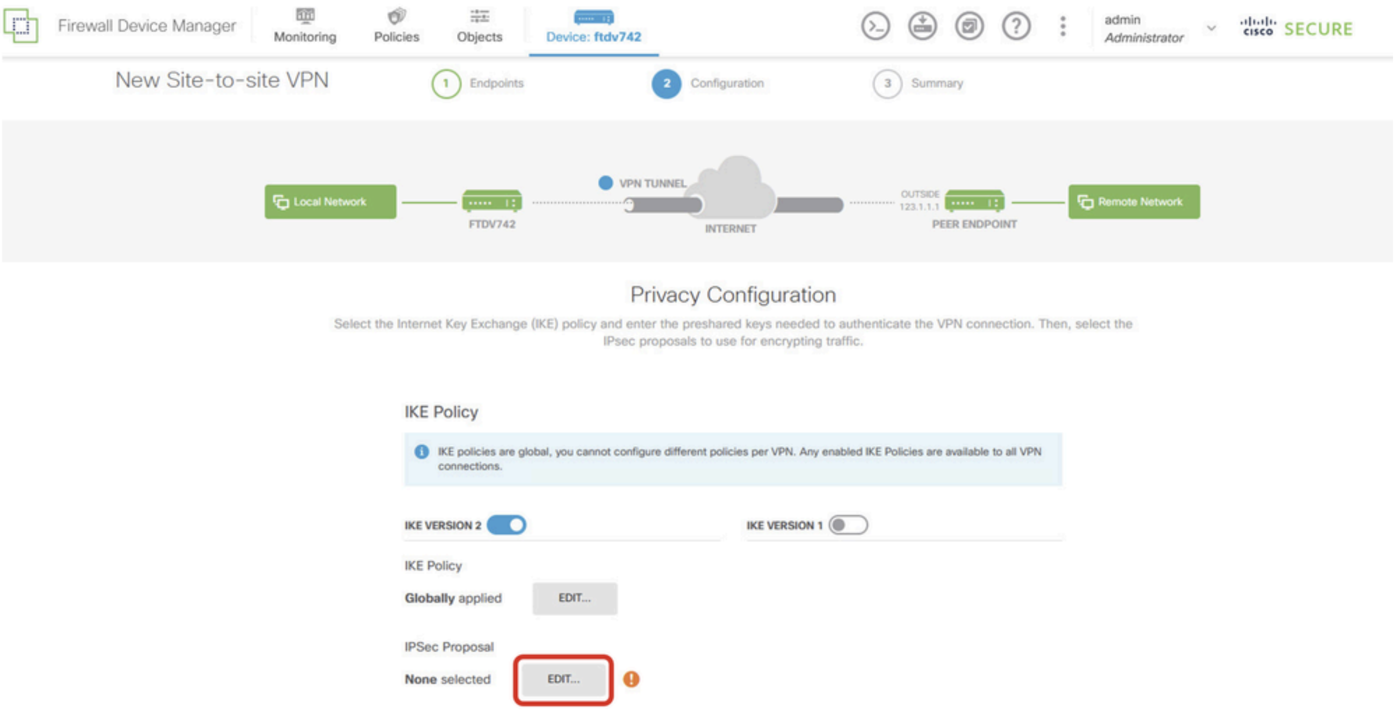
步驟 3.4. 對於IKE策略，可以使用預定義，也可以通過按一下 建立新的IKE策略 .

在本示例中，切換現有IKE策略名稱AES-SHA-SHA。按一下OK按鈕進行儲存。



FTD_Enable_IKE_Policy

步驟3.5.導航至IPSec建議書。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...

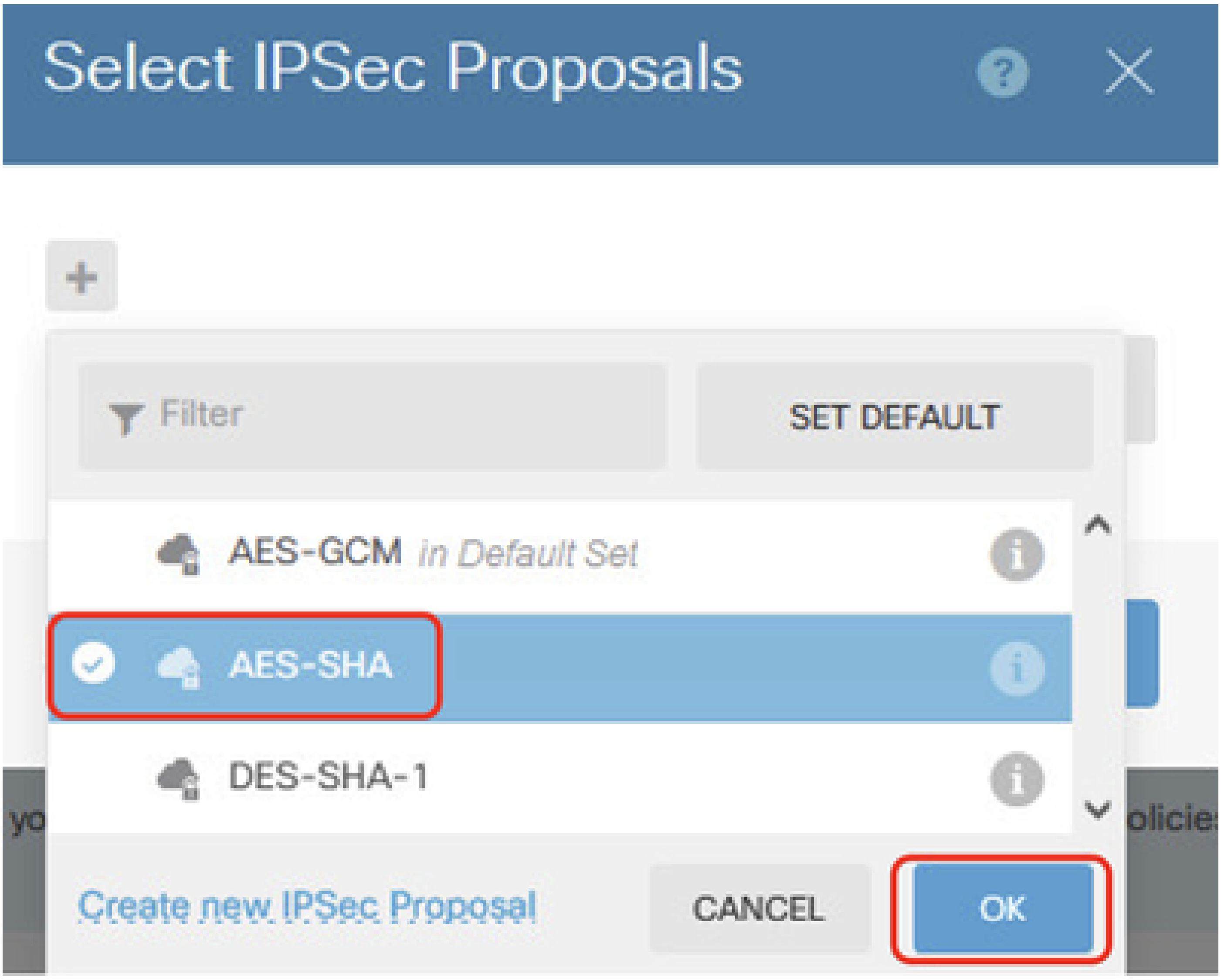
IPSec Proposal

None selected EDIT...

FTD_Edit_IPSec_Proposal

步驟3.6.對於IPSec建議，您可以使用預定義，也可以通過按一下建立新IPSec建議建立一個新IPSec建議。

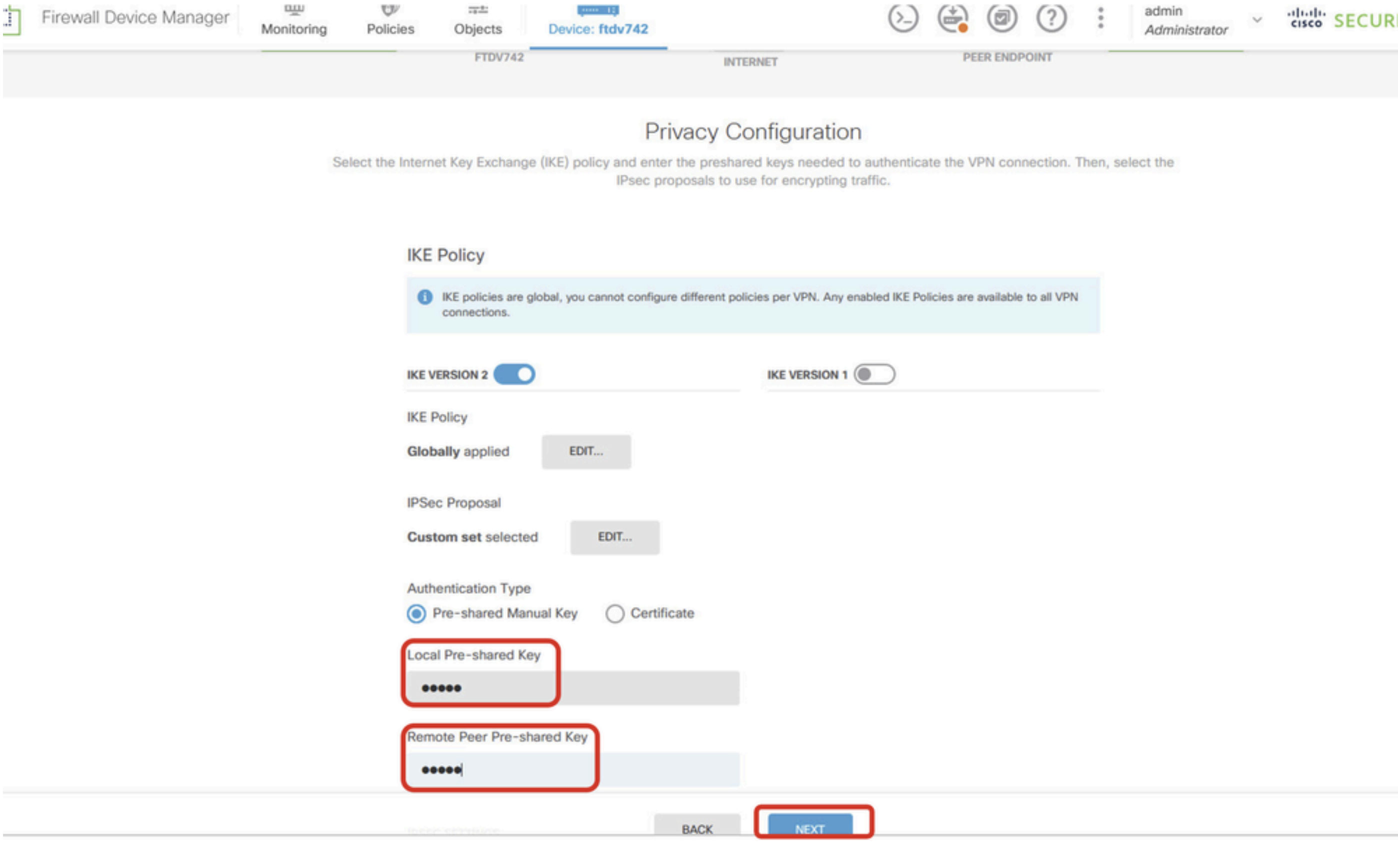
在本示例中，切換現有IPSec建議名稱AES-SHA。按一下 確定 按鈕儲存。



FTD_Enable_IPSec_Proposal

步驟3.7.向下滾動頁面並配置預共用金鑰。按一下「NEXT」按鈕。

請記下此預共用金鑰，稍後在ASA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...

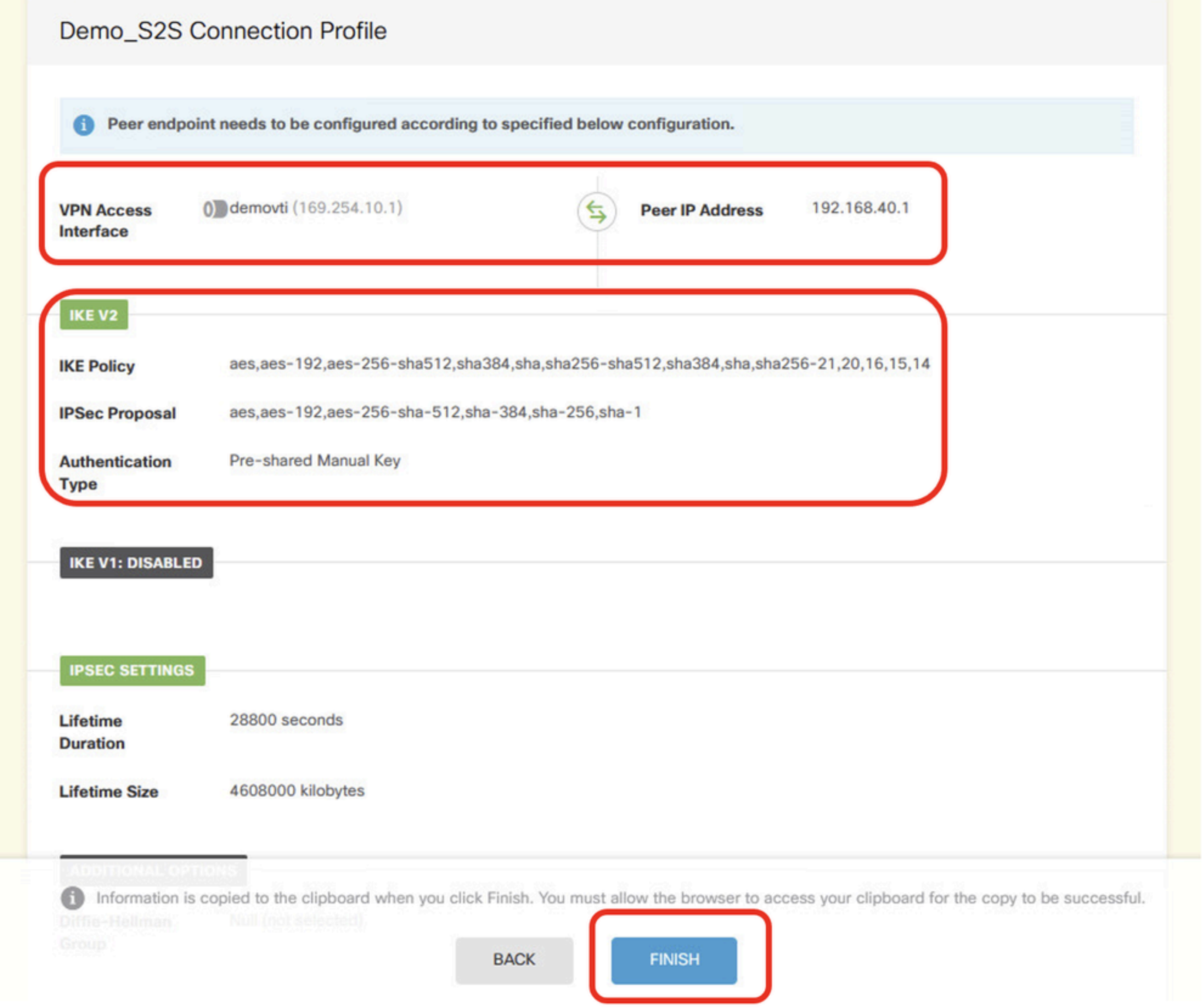
Authentication Type
● Pre-shared Manual Key ○ Certificate

Local Pre-shared Key
●●●●●

Remote Peer Pre-shared Key
●●●●●

FTD_Configure_Pre_Shared_Key

步驟3.8.檢查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	192.168.40.1

IKE V2

IKE Policy	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14
IPSec Proposal	aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1
Authentication Type	Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration	28800 seconds
Lifetime Size	4608000 kilobytes

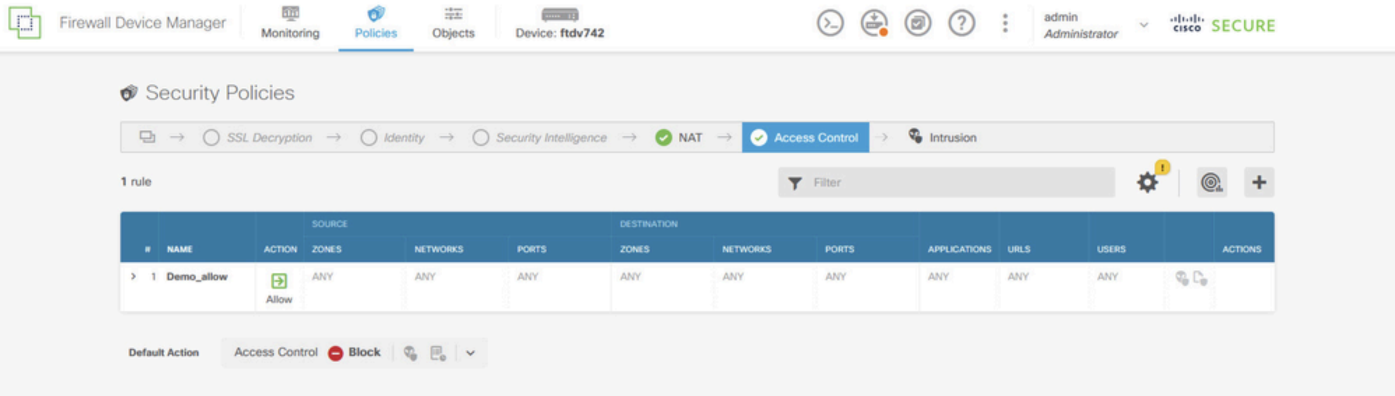
ADDITIONAL OPTIONS

Diffie-Hellman Group	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.

FTD_Review_VPN_Configuration

步驟3.9.建立存取控制規則，允許流量通過FTD。在本例中，允許所有用於演示。請根據您的實際需要修改您的策略。



Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

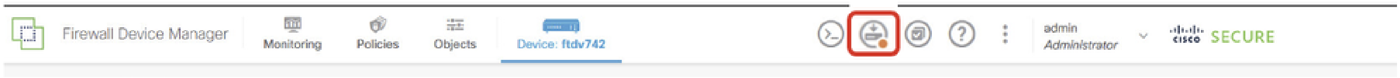
			SOURCE			DESTINATION						
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	

Default Action Access Control Block

FTD_ACP_範例

步驟3.10。（可選）如果為客戶端訪問網際網路配置了動態NAT，請為FTD上的客戶端流量配置NAT豁免規則。在本示例中，不需要配置NAT免除規則，因為FTD上未配置動態NAT。

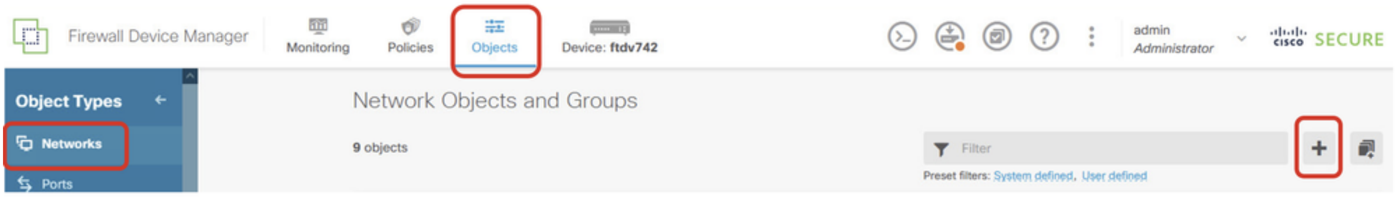
步驟3.11.部署配置更改。



FTD_Deployment_Change

步驟4.配置虛擬路由器。

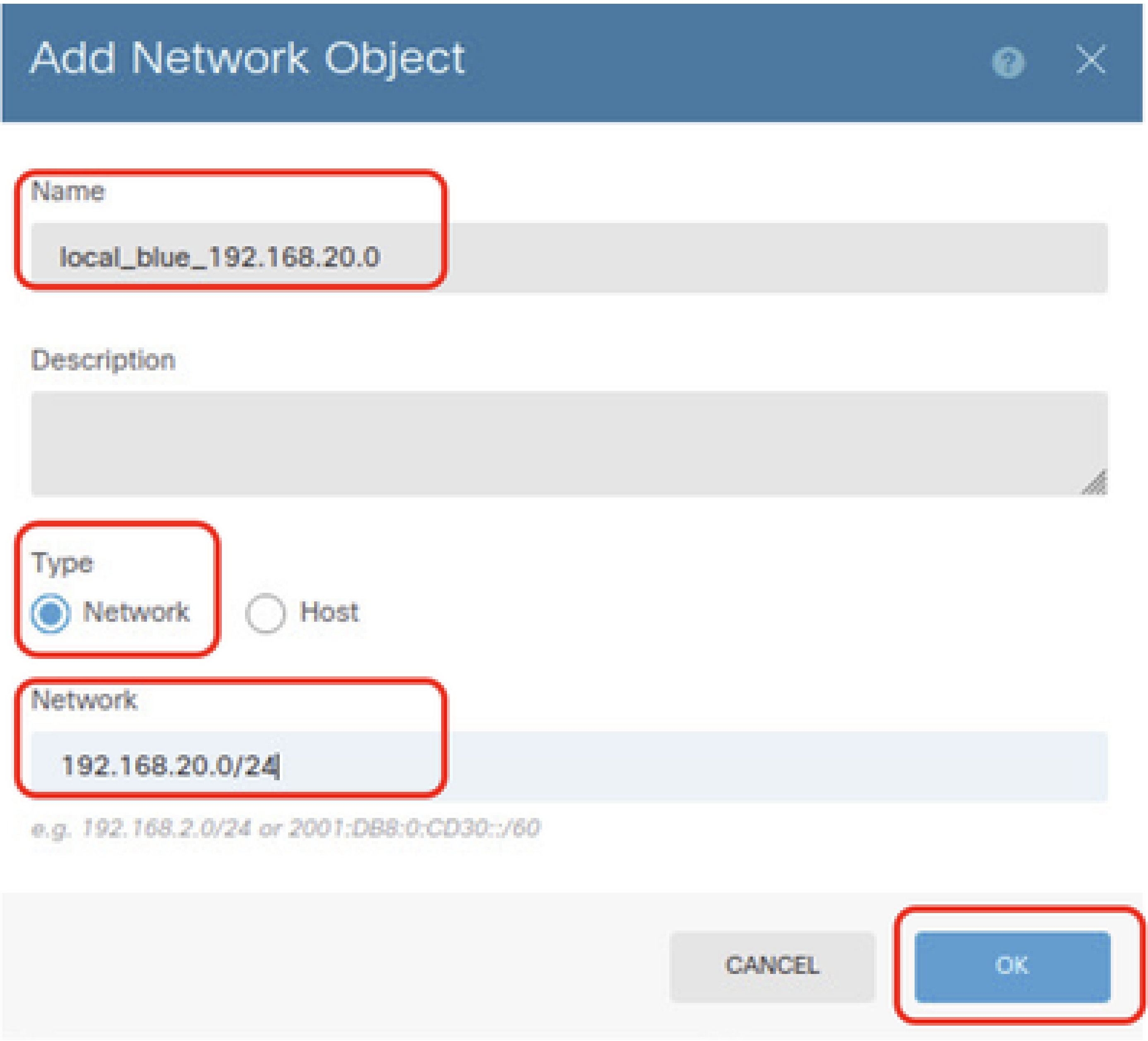
步驟4.1.為靜態路由建立網路對象。導航到對象>網路，單擊+按鈕。



FTD_Create_NetObjects

步驟4.2.提供每個網路對象的必要資訊。按一下「OK」按鈕。

- 名稱:local_blue_192.168.20.0
- Type:網路
- 網路：192.168.20.0/24


Add Network Object

Name

local_blue_192.168.20.0

Description

Type

● Network ○ Host

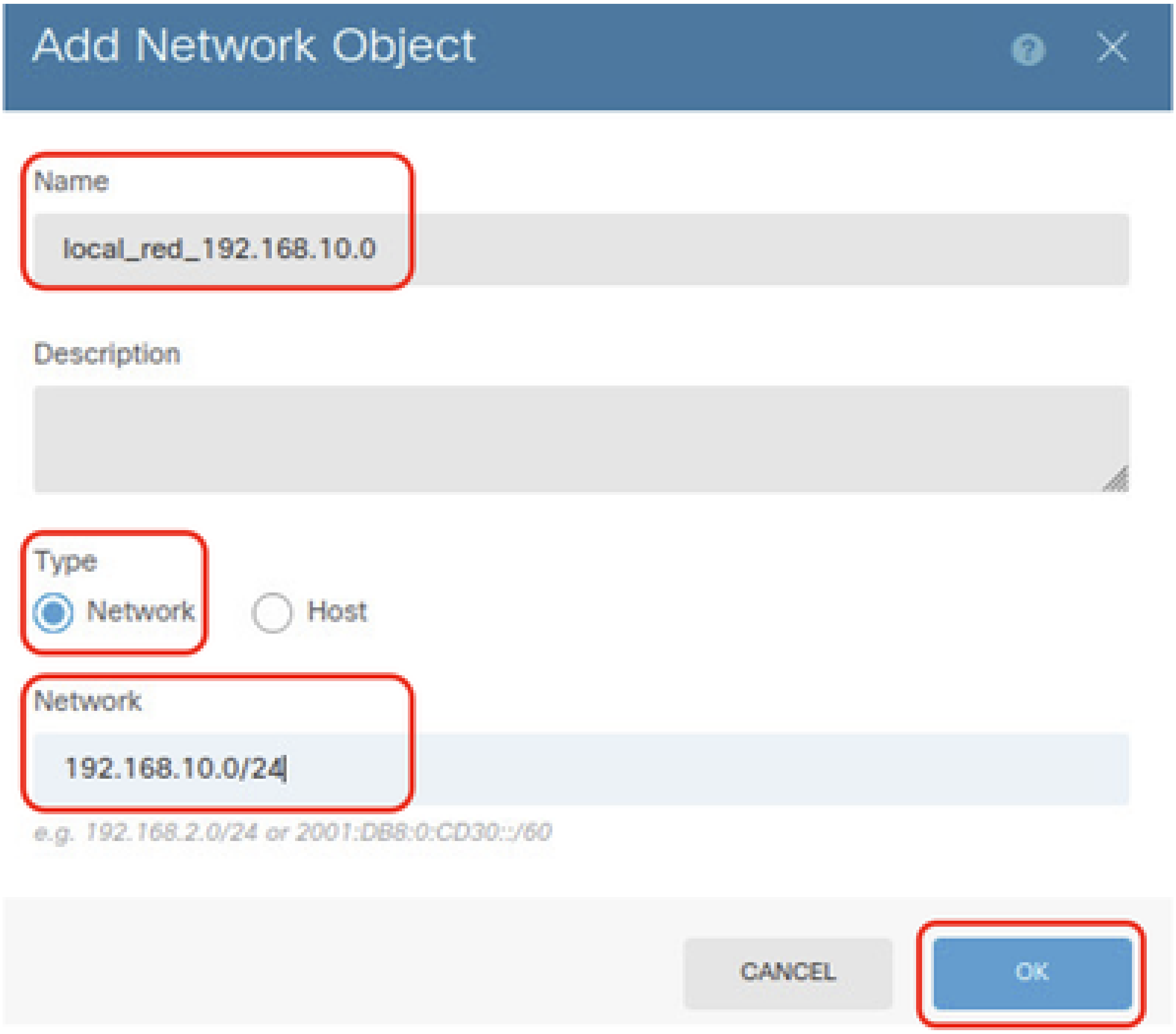
Network

192.168.20.0/24

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

FTD_VRF_Blue_Network

- 名稱:local_red_192.168.10.0
- Type:網路
- 網路：192.168.10.0/24



Add Network Object

Name

local_red_192.168.10.0

Description

Type

● Network ○ Host

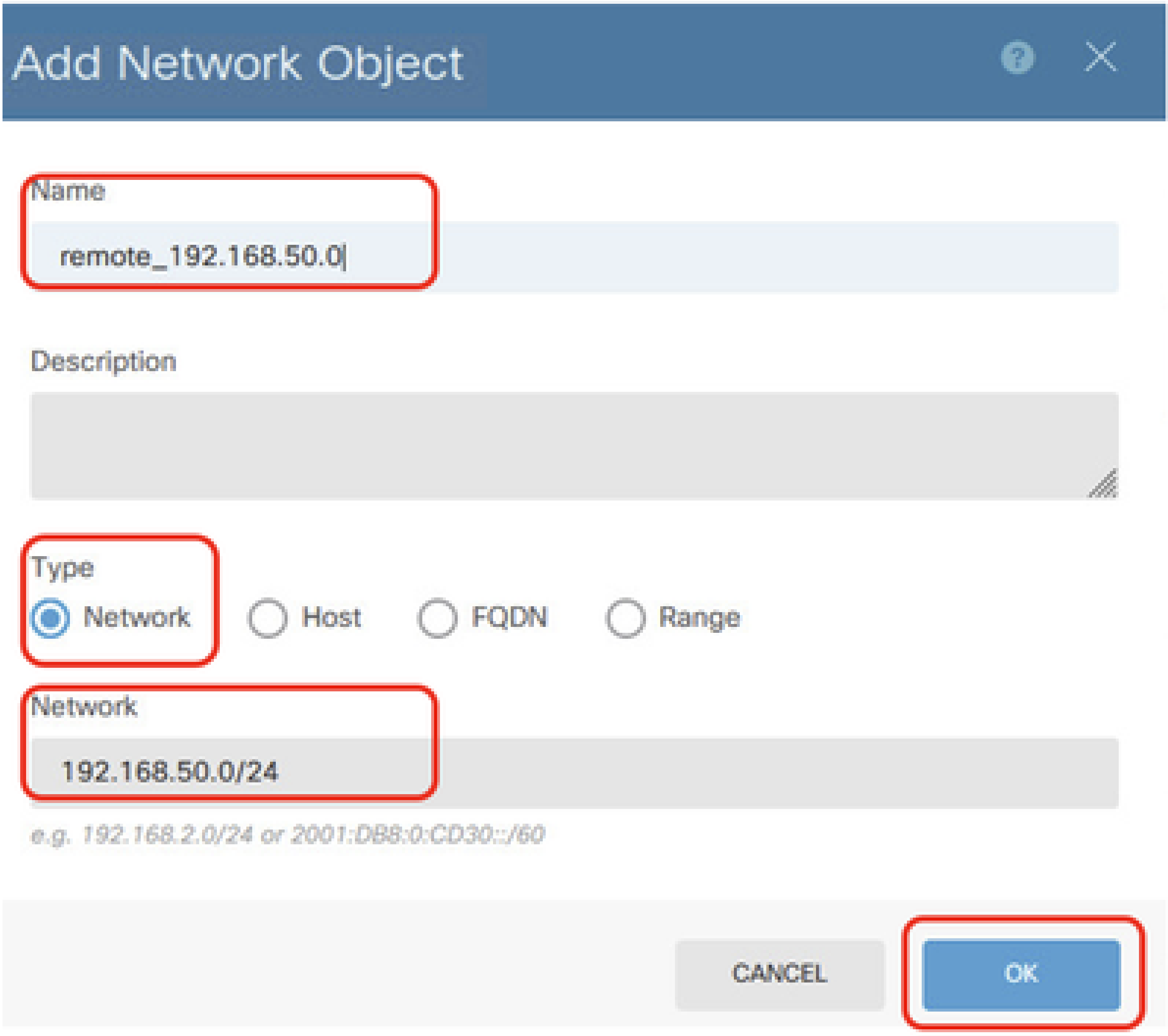
Network

192.168.10.0/24

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

FTD_VRF_Red_Network

- 名稱:remote_192.168.50.0
- Type:網路
- 網路：192.168.50.0/24



Name

remote_192.168.50.0

Description

Type

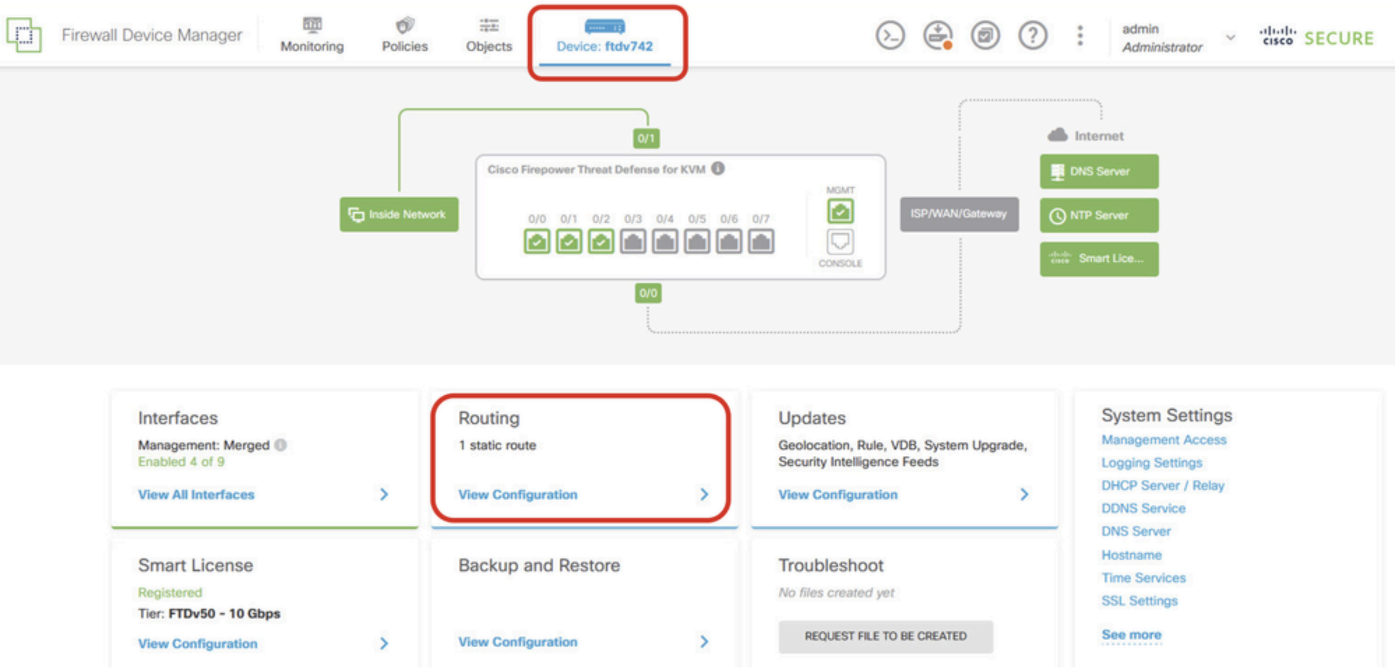
● Network ○ Host ○ FQDN ○ Range

Network

192.168.50.0/24

FTD_Remote_Network

步驟4.3.建立第一個虛擬路由器。導覽至Device > Routing。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

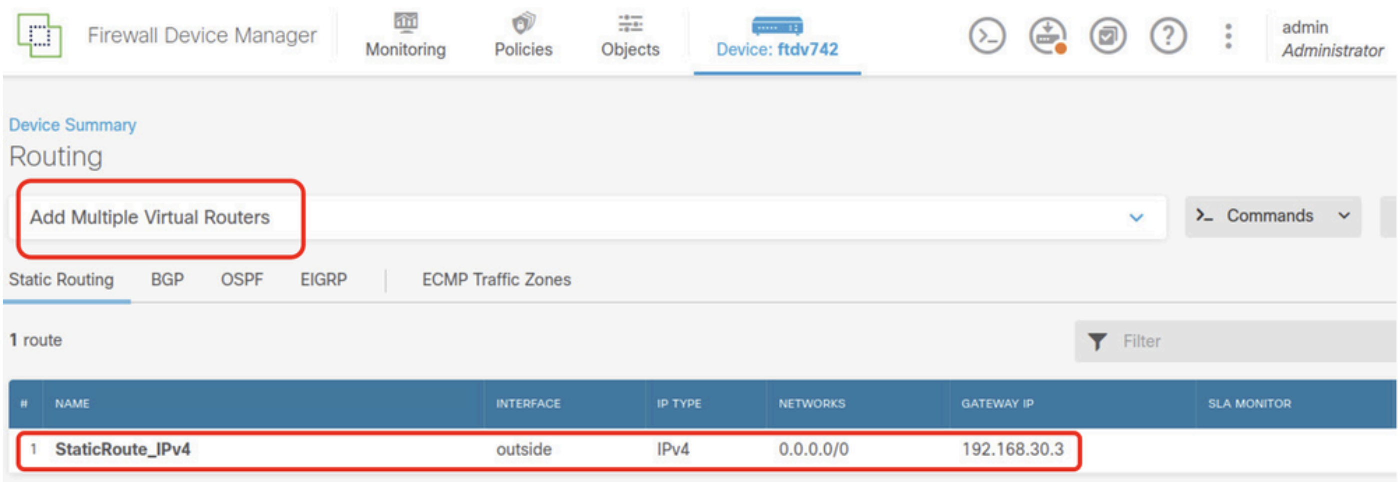
Backup and Restore
View Configuration

Troubleshoot
No files created yet
REQUEST FILE TO BE CREATED

FTD_View_Routing_Configuration

步驟4.4.按一下Add Multiple Virtual Routers。

附註：在FDM初始化期間，已配置通過外部介面的靜態路由。如果您沒有此功能，請手動進行配置。



Routing

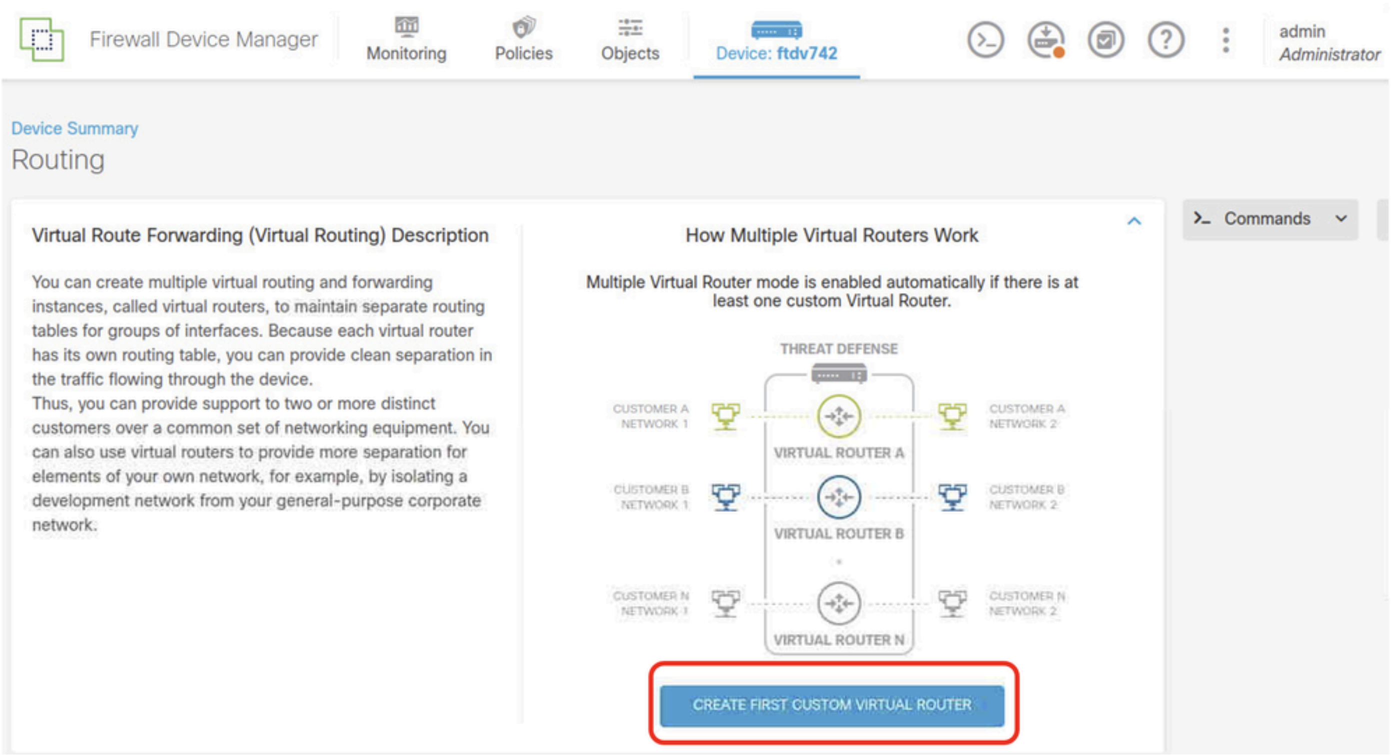
Add Multiple Virtual Routers

1 route

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

FTD_Add_First_Virtual_Router1

步驟4.5.按一下CREATE FIRST CUSTOM VIRTUAL ROUTER。



Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.
Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

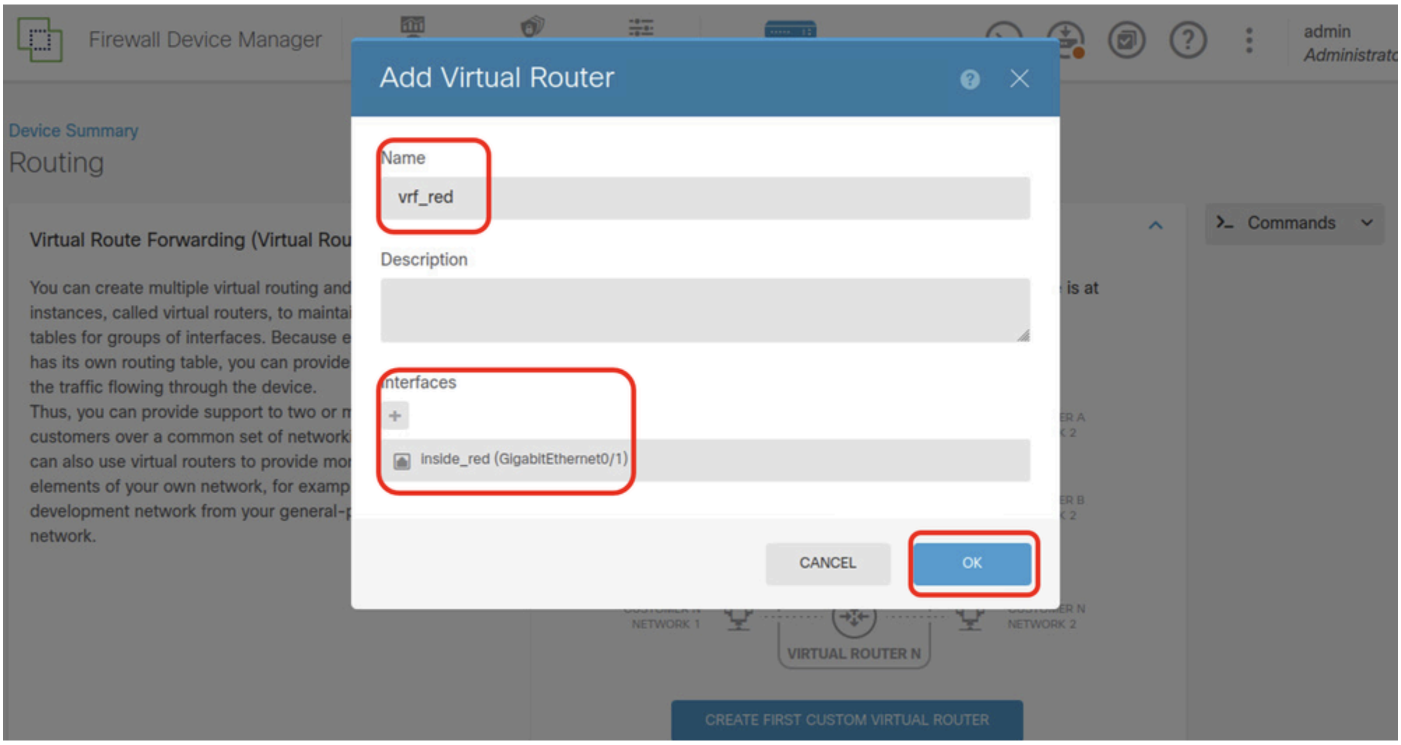
How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

FTD_Add_First_Virtual_Router2

步驟4.6.提供第一個虛擬路由器的必要資訊。按一下「OK」按鈕。首次建立虛擬路由器後，將自動顯示vrf名稱Global。

- 名稱:vrf_red
- 介面：inside_red(GigabitEthernet0/1)



Name
vrf_red

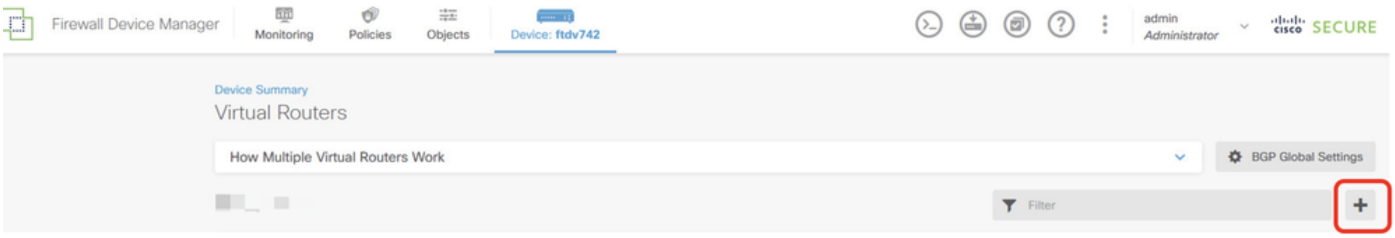
Description

Interfaces
inside_red (GigabitEthernet0/1)

FTD_Add_First_Virtual_Router3

步驟4.7.建立第二個虛擬路由器。導航到Device > Routing。按一下「View Configuration」。按一

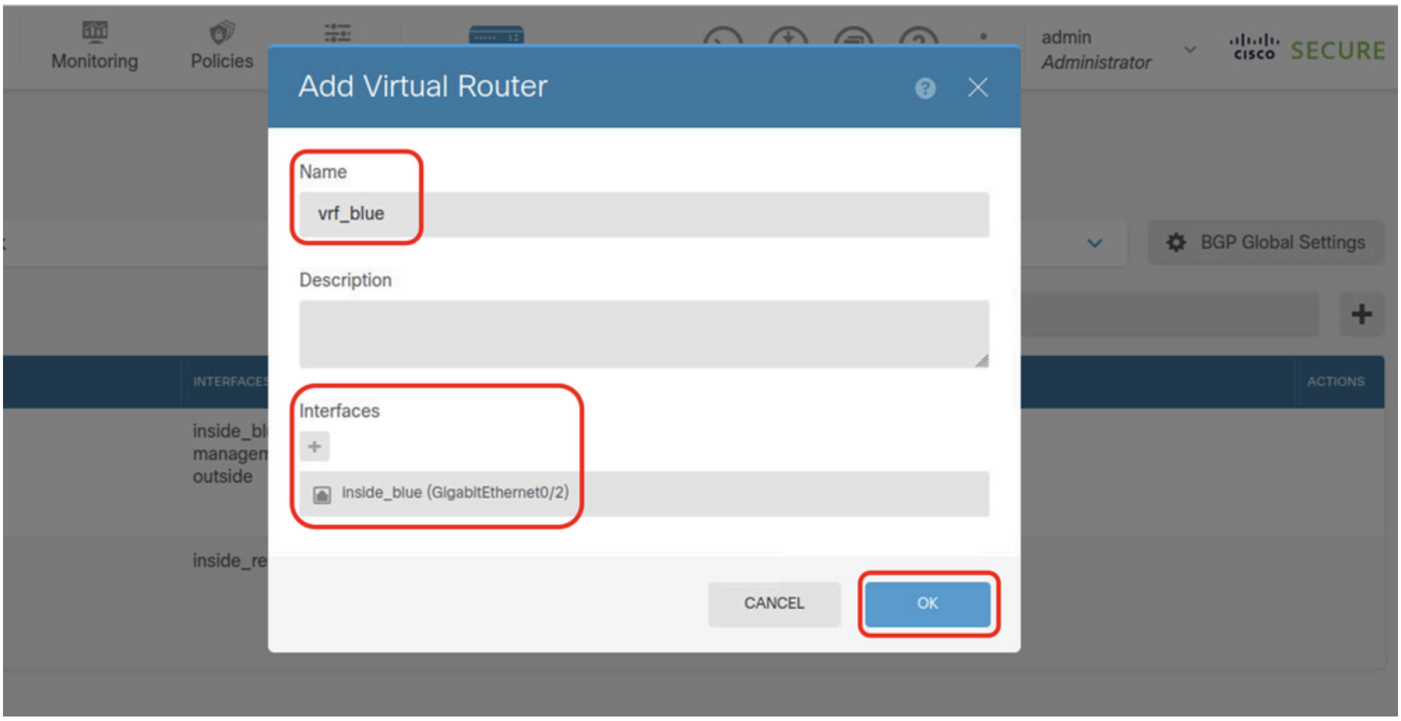
下+按鈕。



FTD_Add_Second_Virtual_Router

步驟4.8.提供第二台虛擬路由器的必要資訊。按一下OK按鈕

- 名稱:vrf_blue
- 介面：inside_blue(GigabitEthernet0/2)


Add Virtual Router

Name: vrf_blue

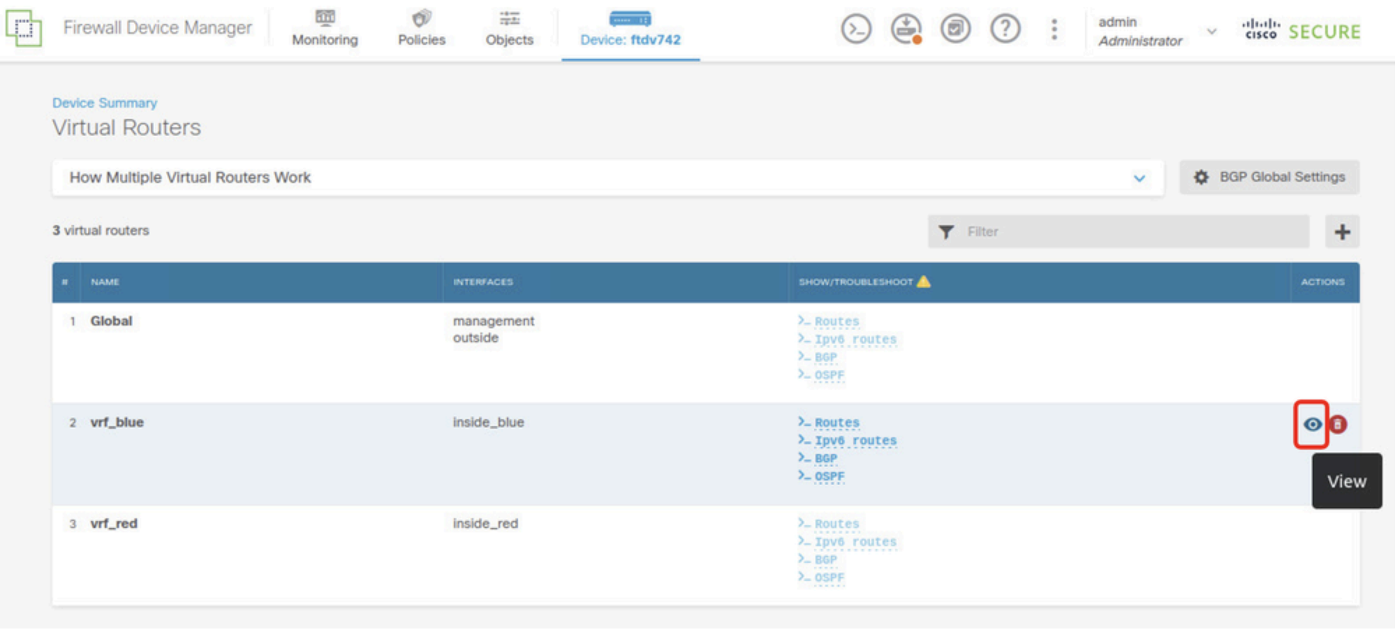
Description

Interfaces: inside_blue (GigabitEthernet0/2)

FTD_Add_Second_Virtual_Router2

步驟5.建立從vrf_blue到Global的路由洩漏。此路由允許192.168.20.0/24網路上的端點啟動將穿越站點到站點VPN隧道的連接。在本示例中，遠端終端正在保護192.168.50.0/24網路。

導覽至Device > Routing。按一下檢視配置。按一下檢視圖示 在虛擬路由器vrf_blue的操作單元格中。

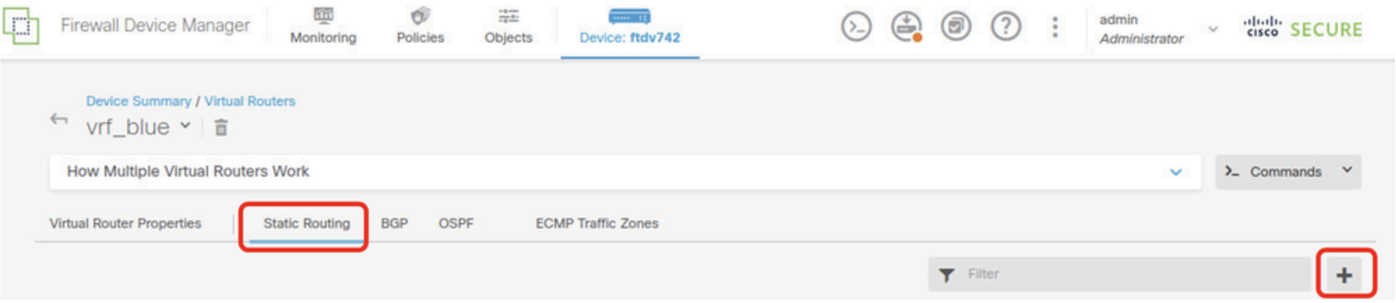


3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	Routes Ipv6 routes BGP OSPF	
2	vrf_blue	inside_blue	Routes Ipv6 routes BGP OSPF	
3	vrf_red	inside_red	Routes Ipv6 routes BGP OSPF	

FTD_View_VRF_Blue

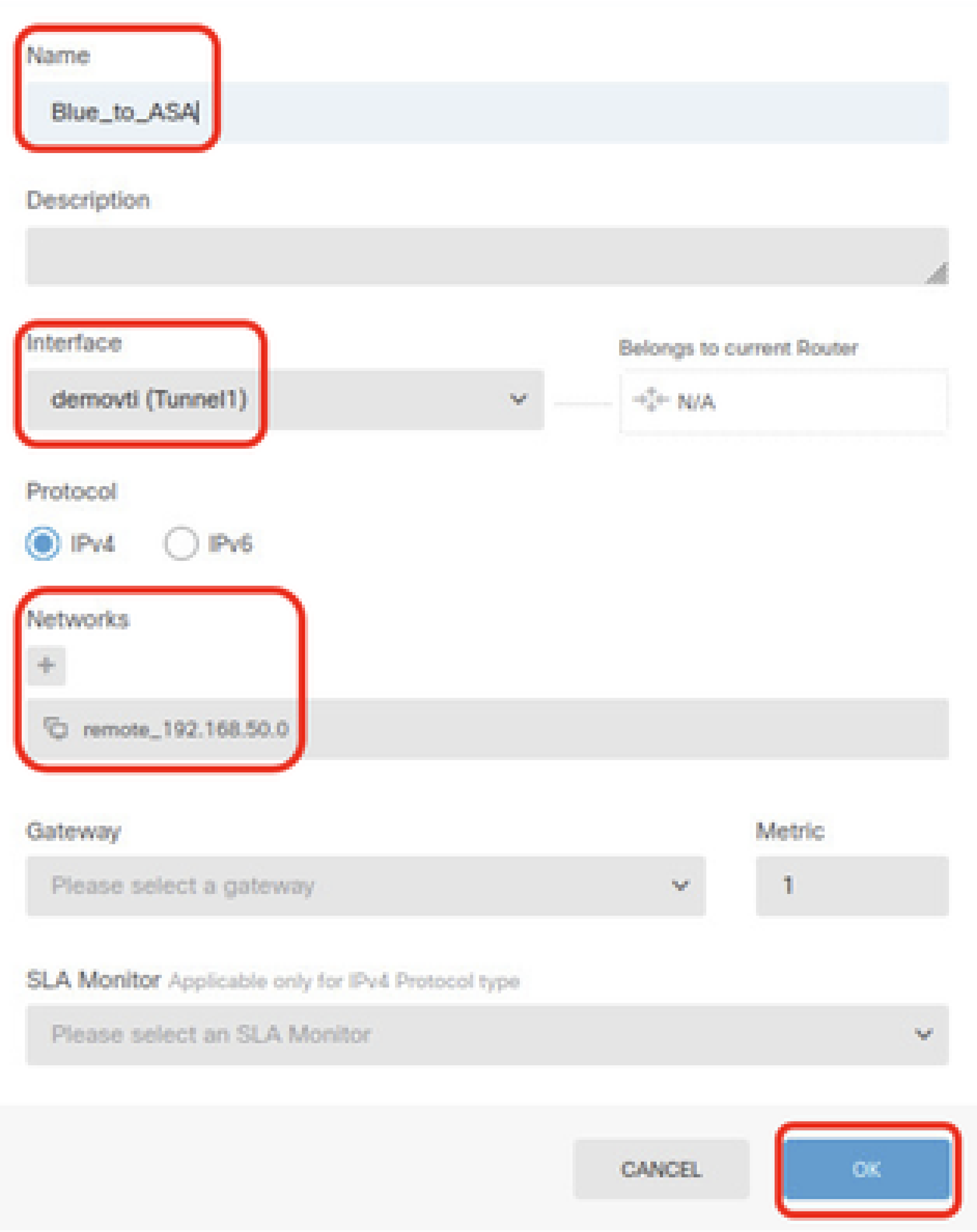
步驟5.1.按一下Static Routing 索引標籤。按一下+按鈕。



FTD_Create_Static_Route_VRF_Blue

步驟5.2.提供必要資訊。按一下「OK」按鈕。

- 名稱:Blue_to_ASA
- Interface:demovti(Tunnel1)
- 網路：remote_192.168.50.0
- 網關：將此項留空。



Name: Blue_to_ASA

Description:

Interface: demovti (Tunnel1)

Belongs to current Router: N/A

Protocol: ● IPv4 ○ IPv6

Networks: remote_192.168.50.0

Gateway: Please select a gateway

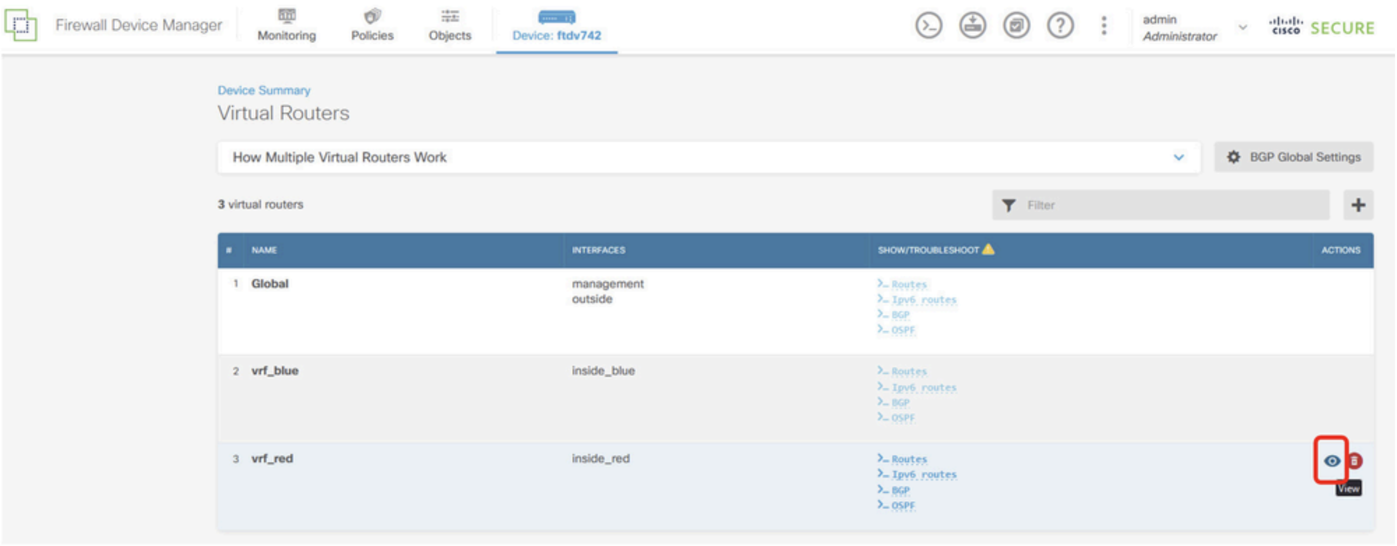
Metric: 1

SLA Monitor Applicable only for IPv4 Protocol type: Please select an SLA Monitor

FTD_Create_Static_Route_VRF_Blue_Details

步驟6.建立從vrf_red到Global的路由洩漏。此路由允許192.168.10.0/24網路上的端點啟動將穿越站點到站點VPN隧道的連接。在本示例中，遠端終端正在保護192.168.50.0/24網路。

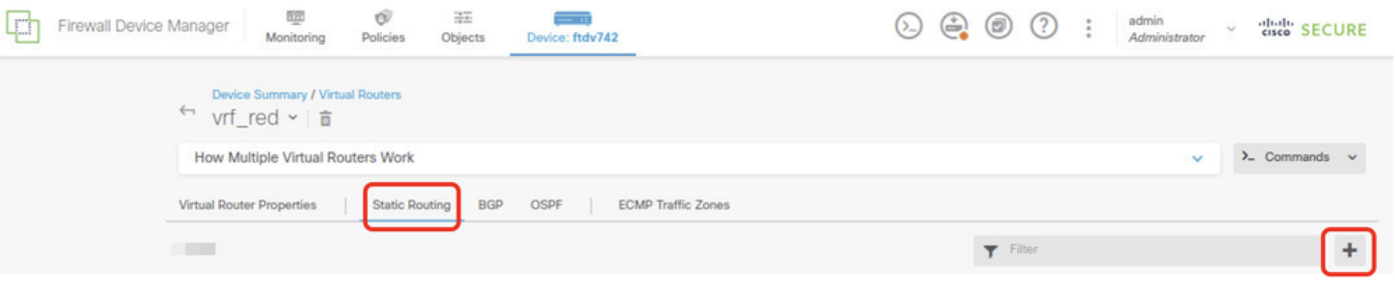
導覽至Device > Routing。按一下檢視配置。按一下檢視圖示 虛擬路由器vrf_red的操作單元。



#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	>_ Routes >_ Ipv6 routes >_ BGP >_ OSPF	
2	vrf_blue	inside_blue	>_ Routes >_ Ipv6 routes >_ BGP >_ OSPF	
3	vrf_red	inside_red	>_ Routes >_ Ipv6 routes >_ BGP >_ OSPF	

FTD_View_VRF_Red

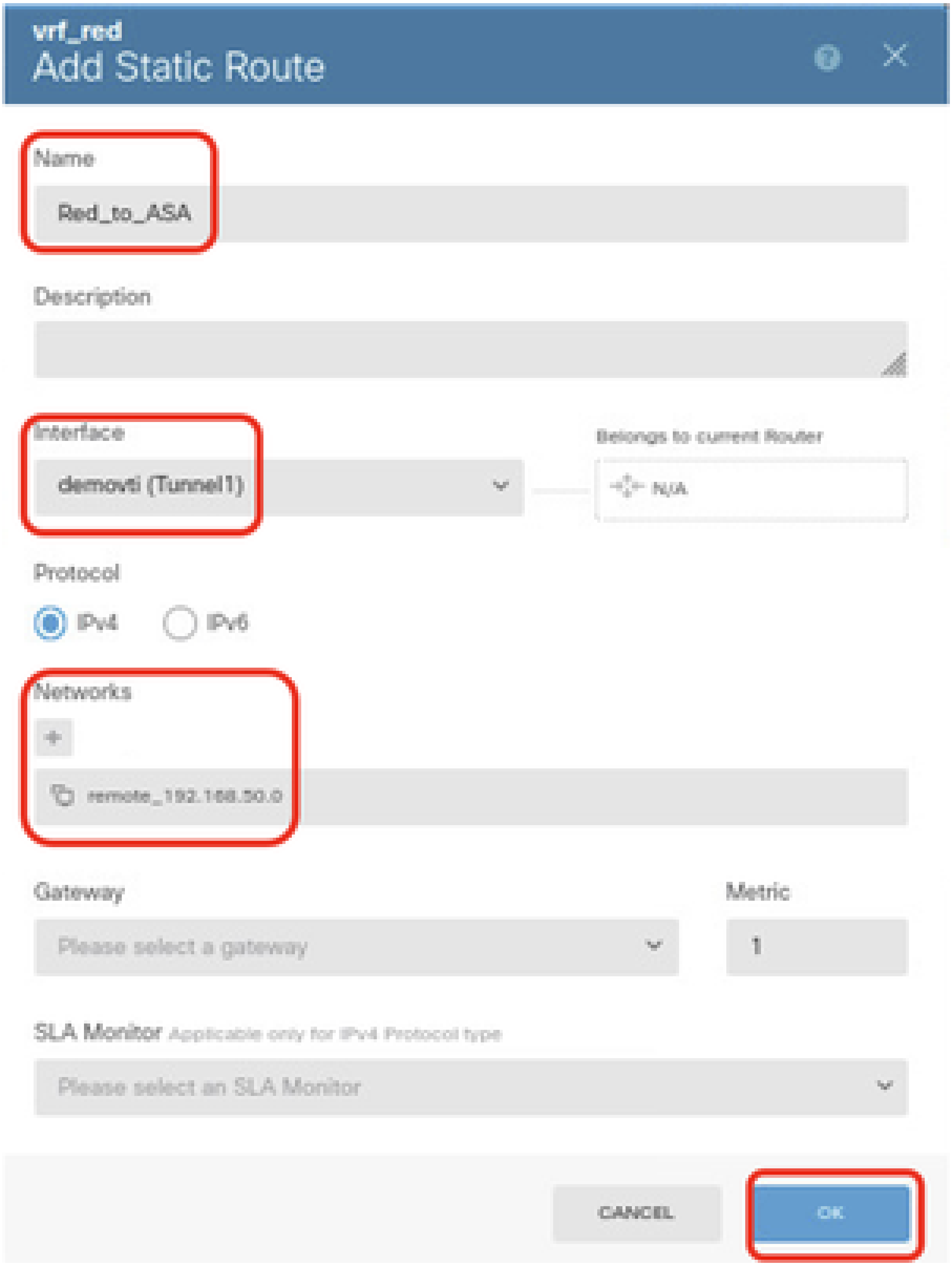
步驟6.1.按一下靜態路由頁籤。按一下+按鈕。



FTD_Create_Static_Route_VRF_Red

步驟6.2.提供必要資訊。按一下「OK」按鈕。

- 名稱:Red_to_ASA
- Interface:demovti(Tunnel1)
- 網路：remote_192.168.50.0
- 網關：將此項留空。



vrf_red

Add Static Route

Name: Red_to_ASA

Description:

Interface: demovti (Tunnel1)

Belongs to current Router: N/A

Protocol: ● IPv4 ○ IPv6

Networks: remote_192.168.50.0

Gateway: Please select a gateway

Metric: 1

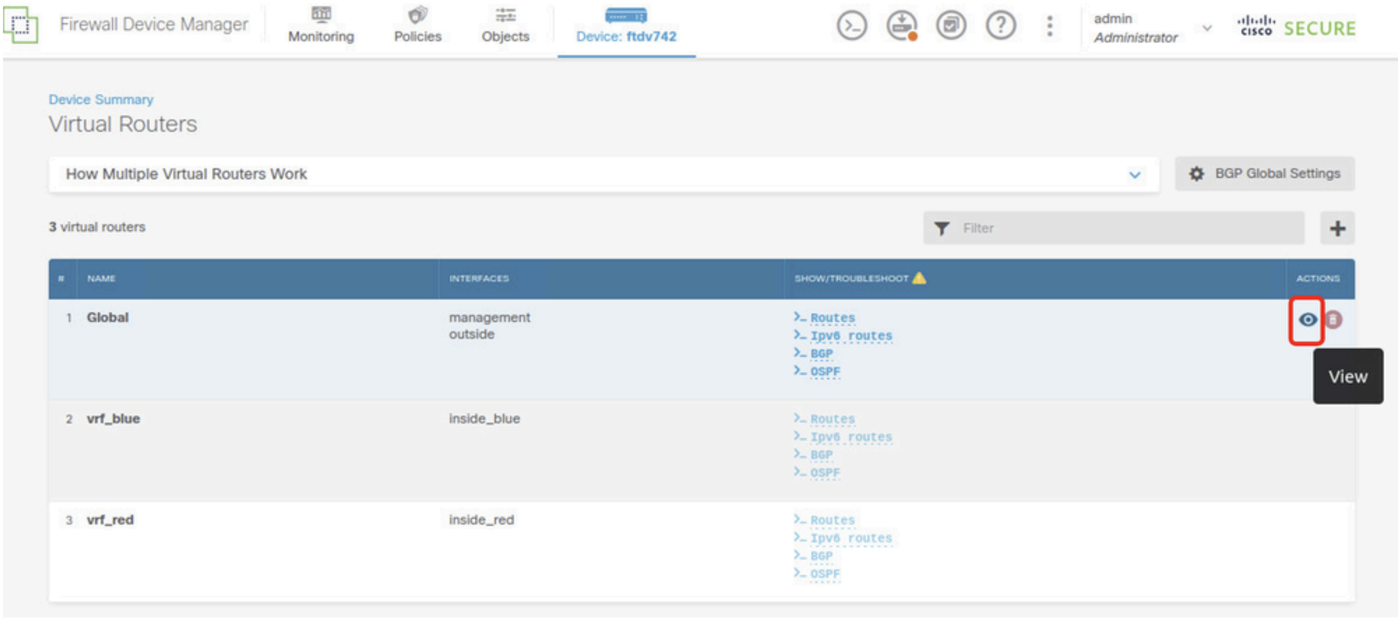
SLA Monitor Applicable only for IPv4 Protocol type: Please select an SLA Monitor

FTD_Create_Static_Route_VRF_Red_Details

步驟7.建立從全域性路由器到虛擬路由器的路由洩漏。這些路由允許受站點到站點VPN的遠端終端保護的終端訪問vrf_red虛擬路由器中的192.168.10.0/24網路和vrf_blue虛擬路由器中的

192.168.20.0/24網路。

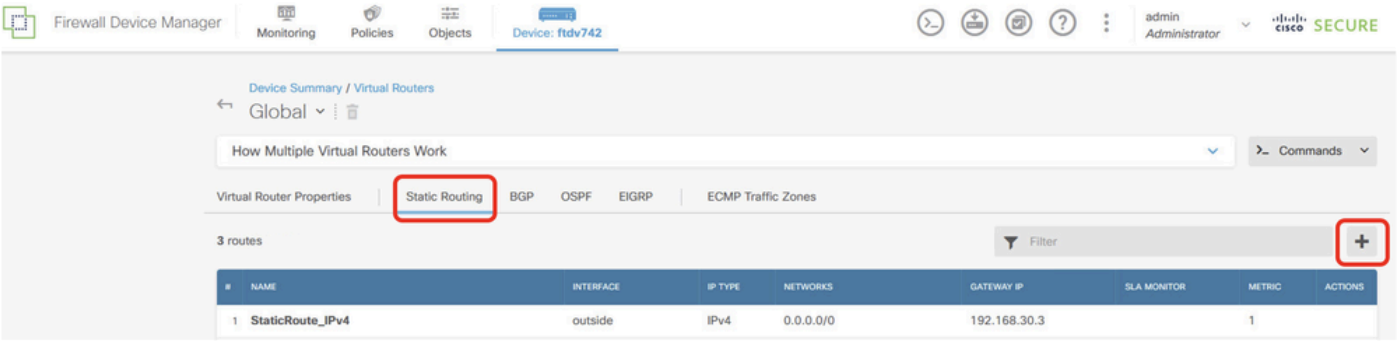
導覽至Device > Routing。按一下檢視配置。按一下全域性虛擬路由器的「操作」單元格中的檢視圖示。



#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	Routes Ipv6 routes BGP OSPF	
2	vrf_blue	inside_blue	Routes Ipv6 routes BGP OSPF	
3	vrf_red	inside_red	Routes Ipv6 routes BGP OSPF	

FTD_View_VRF_Global

步驟7.1.按一下靜態路由頁籤。按一下+按鈕。

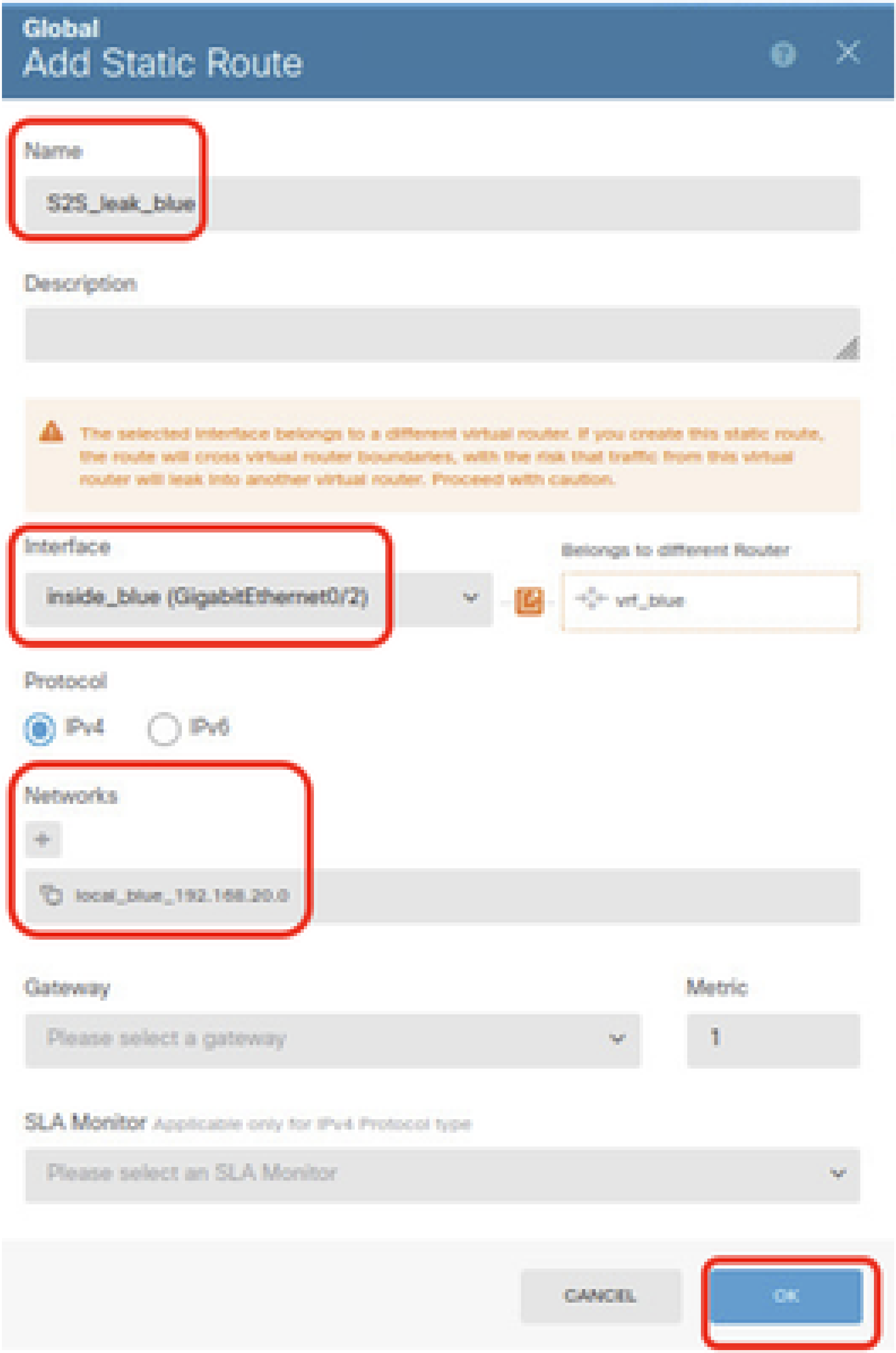


#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

FTD_Create_Static_Route_VRF_Global

步驟7.2.提供必要資訊。按一下「OK」按鈕。

- 名稱:S2S_leak_blue
- 介面：inside_blue(GigabitEthernet0/2)
- 網路：local_blue_192.168.20.0
- 網關：將此項留空。



```
 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
```

步驟10.建立一個IKEv2 ipsec建議案，定義在FTD上設定的相同引數。

<#root>

```
crypto ipsec ikev2 ipsec-proposal

AES-SHA

 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

步驟11.建立 ipsec配置檔案，引用 第10步中建立的IPSec-proposal。

<#root>

```
crypto ipsec profile

demo_ipsec_profile

 set ikev2 ipsec-proposal

AES-SHA

 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 28800
```

步驟12.建立允許IKEv2協定的組策略。

<#root>

```
group-policy

demo_gp_192.168.30.1

 internal
group-policy demo_gp_192.168.30.1 attributes
 vpn-tunnel-protocol ikev2
```

步驟13.參照步驟12中建立的組策略，為對等FTD建立隧道組，並指定 使用FTD設定相同的預先共用金鑰（在步驟3.7中建立）。

<#root>

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
 default-group-policy
```

demo_gp_192.168.30.1

```
tunnel-group 192.168.30.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

步驟14.在外部介面上啟用IKEv2。

```
crypto ikev2 enable outside
```

步驟15.建立虛擬通道。

<#root>

```
interface Tunnel1
 nameif demovti_asa
 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
```

demo_ipsec_profile

步驟16.建立靜態路由。

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

驗證

使用本節內容，確認您的組態是否正常運作。

步驟1。透過主控台或SSH導覽至FTD和ASA的CLI，透過show crypto ikev2 sa和show crypto ipsec sa指令，驗證階段1和階段2的VPN狀態。

FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv742#
ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                               Remote
 32157565 192.168.30.1/500                                    192.168.40.1/500                       G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83

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: 192.168.40.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #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.: 192.168.40.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: A493CC83
      current inbound spi : 4CF55637

    inbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16867)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4285440/16867)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                               Remote                                  
 26025779 192.168.40.1/500                                    192.168.30.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1

      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: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #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.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
      current inbound spi : A493CC83

    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4101120/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

步驟2.驗證FTD上VRF和Global的路由。

```
ftdv742# show route

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

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
SI       192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI       192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside


ftdv742# show route vrf vrf_blue


Routing Table: vrf_blue
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 not set

C        192.168.20.0 255.255.255.0 is directly connected, inside_blue
```

```
L        192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti


ftdv742# show route vrf vrf_red



Routing Table: vrf_red
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 not set

C        192.168.10.0 255.255.255.0 is directly connected, inside_red
L        192.168.10.1 255.255.255.255 is directly connected, inside_red
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

步驟3.檢驗ping測試。

ping之前，請檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on FTD。

在本範例中，Tunnel1顯示用於封裝和解除封裝的30個封包。

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1成功ping Client3。

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

Client2成功ping Client3。

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

檢查計數器 show crypto ipsec sa | inc interface:|encap|decap ping成功後，在FTD上執行。

在本範例中，Tunnel1在成功ping之後顯示封裝和解除封裝的40個封包。此外，兩個計數器都增加了10個資料包，與10個ping回應請求匹配，表明該ping流量成功通過IPSec隧道。

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
      #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

可以使用這些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
```

您可以使用這些debug命令對路由部分進行故障排除。

```
debug ip routing
```

參考

思科安全防火牆裝置管理器配置指南7.4版

Cisco安全防火牆ASA VPN CLI配置指南，9.20

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）。