

在FDM管理的FTD上使用PBR配置雙活動路由型站點到站點VPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[VPN上的配置](#)

[站點1 FTD VPN配置](#)

[站點2 FTD VPN配置](#)

[PBR上的配置](#)

[站點1 FTD PBR配置](#)

[站點2 FTD PBR配置](#)

[SLA監控器上的配置](#)

[Site1 FTD SLA監控器配置](#)

[站點2 FTD SLA監控器配置](#)

[靜態路由上的配置](#)

[站點1 FTD靜態路由配置](#)

[站點2 FTD靜態路由配置](#)

[驗證](#)

[ISP1和ISP2工作正常](#)

[VPN](#)

[路由](#)

[SLA監控](#)

[Ping測試](#)

[ISP1發生中斷，而ISP2正常工作](#)

[VPN](#)

[路由](#)

[SLA監控](#)

[Ping測試](#)

[ISP2發生中斷，而ISP1正常工作](#)

[VPN](#)

[路由](#)

[SLA監控](#)

[Ping測試](#)

[疑難排解](#)

簡介

本文說明如何在FDM管理的FTD上使用PBR配置雙活動路由型站點到站點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
- 對原則型路由(PBR)的基本瞭解
- 對網際網路通訊協定服務等級協定(IP SLA)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

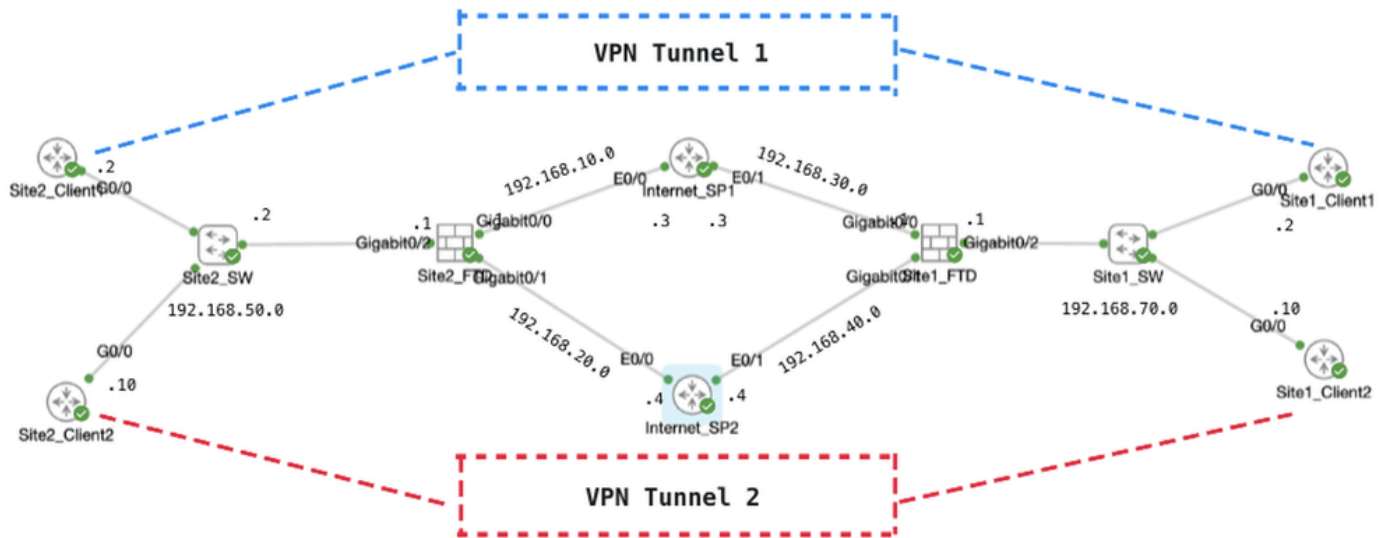
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案將說明如何在FTD上設定雙作用中路由型站對站VPN。在本例中，站點1和站點2的FTD都有兩個活動ISP連線，可同時與兩個ISP建立站點到站點VPN。預設情況下，VPN流量通過ISP1隧道1（藍線）。對於特定主機，流量通過ISP2隧道2（紅線）。如果ISP1遇到中斷，則流量會切換到ISP2作為備份。相反，如果ISP2遇到中斷，則流量會切換到ISP1作為備份。本範例中使用原則型路由(PBR)和網際網路通訊協定服務等級協定(IP SLA)來滿足這些要求。

設定

網路圖表



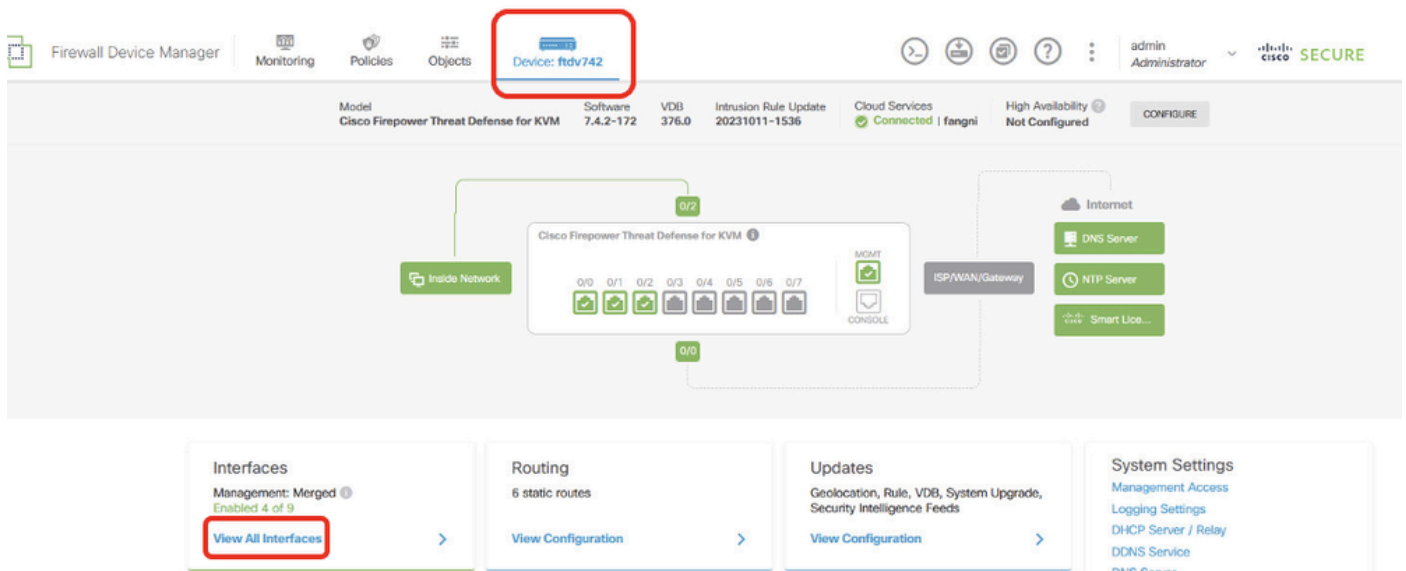
拓撲

VPN上的配置

必須確保在節點之間正確完成IP互連的初步配置。Site1和Site2中的客戶端都將FTD內部IP地址用作網關。

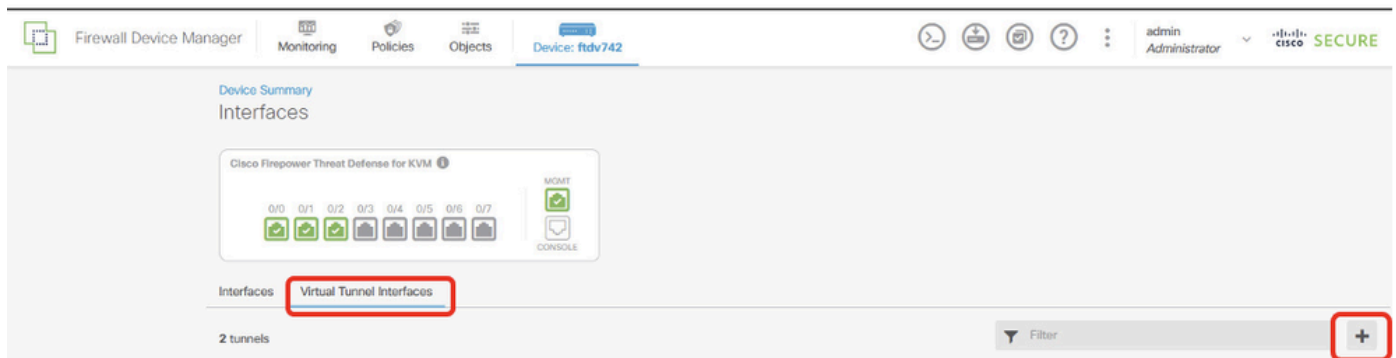
站點1 FTD VPN配置

步驟1.為ISP1和ISP2建立虛擬隧道介面。登入Site1 FTD的FDM GUI。導覽至Device > Interfaces。按一下「View All Interfaces」。



Site1FTD_View_All_Interfaces

步驟2.按一下Virtual Tunnel Interfaces頁籤，然後按一下+按鈕。



Site1FTD_Create_VTI

步驟3.提供VTI詳細資訊的必要資訊。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

Status

☒

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

Description

Tunnel ID

1

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

CANCEL **OK**

Site1FTD_VTI_Details_Tunnel1_ISP1

- 名稱:demovti_sp2
- 通道ID:2

- 通道來源：outside2(GigabitEthernet0/1)
- IP地址和子網掩碼：169.254.20.11/24
- 狀態:按一下滑塊到「已啟用」位置

Name

demovti_sp2

Status

☒

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

Description

Tunnel ID ⓘ

2

Tunnel Source ⓘ

outside2 (GigabitEthernet0/1) ▼

0 - 10413

IP Address and Subnet Mask

169.254.20.11 / 24

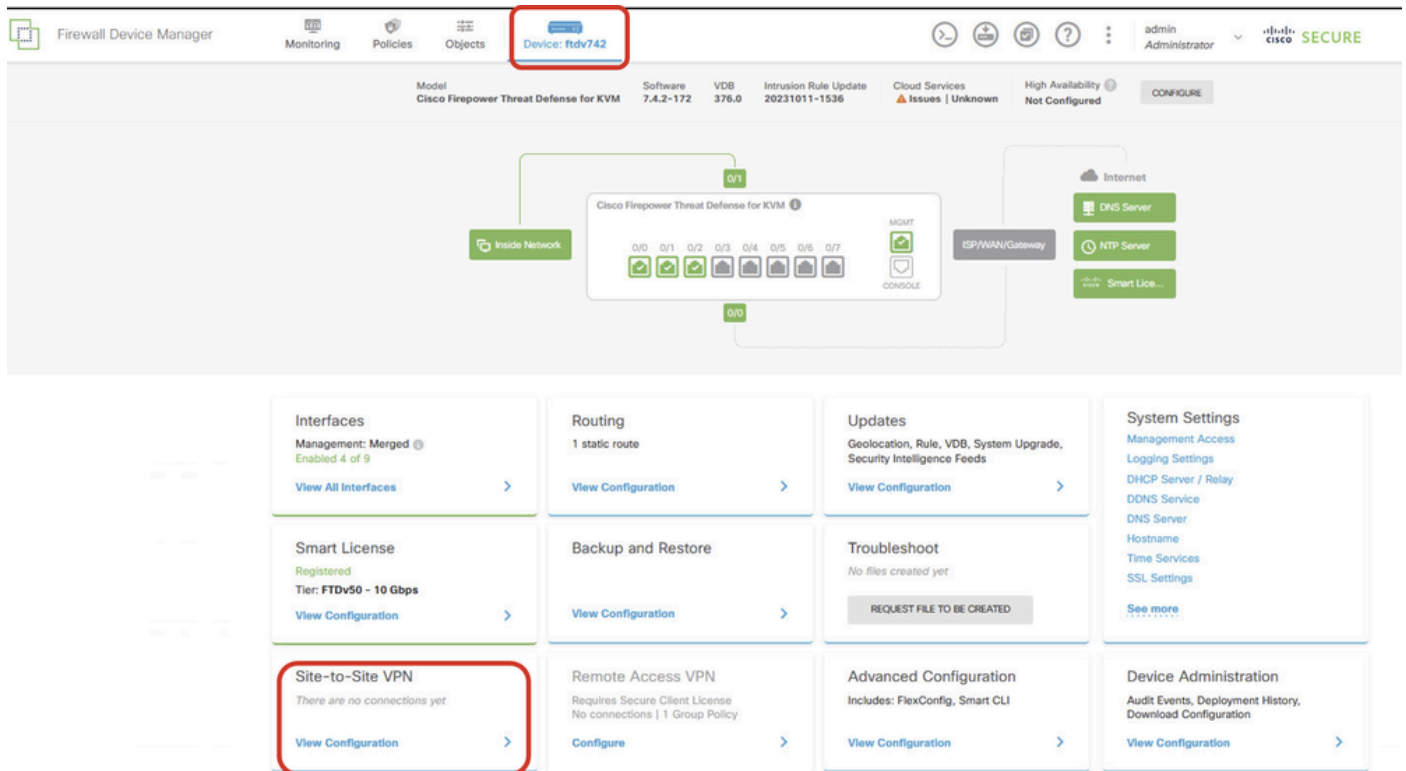
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

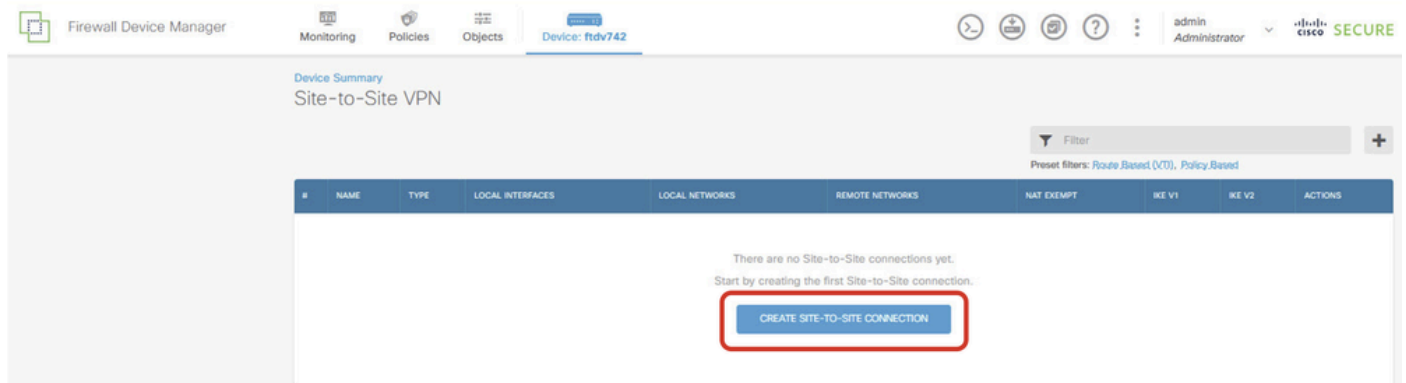
Site1FTD_VTI_Details_Tunnel2_ISP2

步驟4.導覽至Device > Site-to-Site VPN。按一下「View Configuration」按鈕。



Site1FTD_View_Site2Site_VPN

步驟5.開始通過ISP1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。



Site1FTD_Create_Site-to-Site_Connection

步驟5.1. 提供端點的必要資訊。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3中建立。)
- 遠端IP地址：192.168.10.1 (這是Site2 FTD ISP1 IP地址)

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

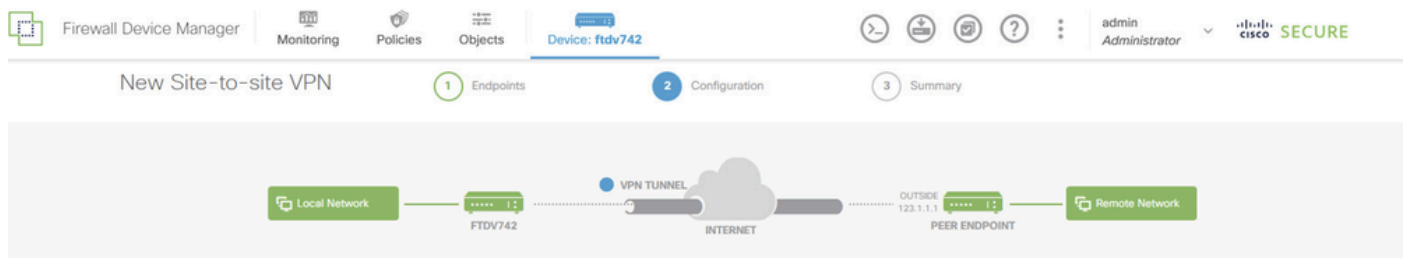
Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface: demovti (Tunnel1)	Remote IP Address: 192.168.10.1

CANCEL **NEXT**

Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

步驟5.2.導覽至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

1 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...

Site1FTD_Edit_IKE_Policy

步驟5.3.對於IKE策略，您可以使用預定義，也可以通過按一下「新建IKE策略」來創建新的IKE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按鈕以進行儲存。

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

The image shows a two-pane configuration window titled "Add IKE v2 Policy".

Left Pane:

- Filter: [empty]
- Policy list:
 - ☐ AES-GCM-NULL-SHA
 - ☒ AES-SHA-SHA
 - ☐ DES-SHA-SHA
- Buttons: "Create New IKE Policy" and "OK"

Right Pane:

- Priority: 1
- Name: AES256_DH14_SHA256_SHA256
- State: ☒
- Encryption: AES x AES256
- Diffie-Hellman Group: 14
- Integrity Hash: SHA x SHA256
- Pseudo Random Function (PRF) Hash: SHA x SHA256
- Lifetime (seconds): 86400
Between 120 and 2147483647 seconds.
- Buttons: "CANCEL" and "OK"

Site1FTD_Add_New_IKE_Policy

Filter

AES-GCM-NULL-SHA

i

AES-SHA-SHA

i

DES-SHA-SHA

i

AES256_DH14_SHA256_SHA256

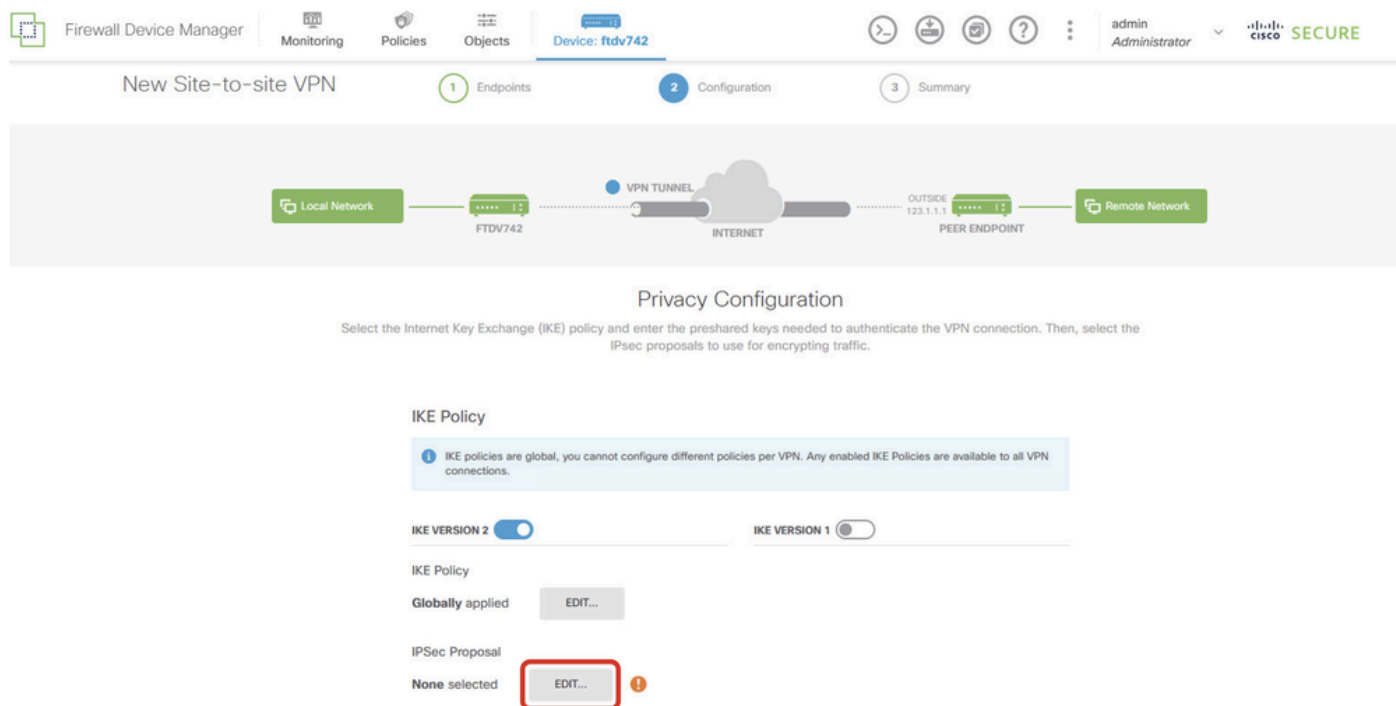
i

Create New IKE Policy

OK

Site1FTD_Enable_New_IKE_Policy

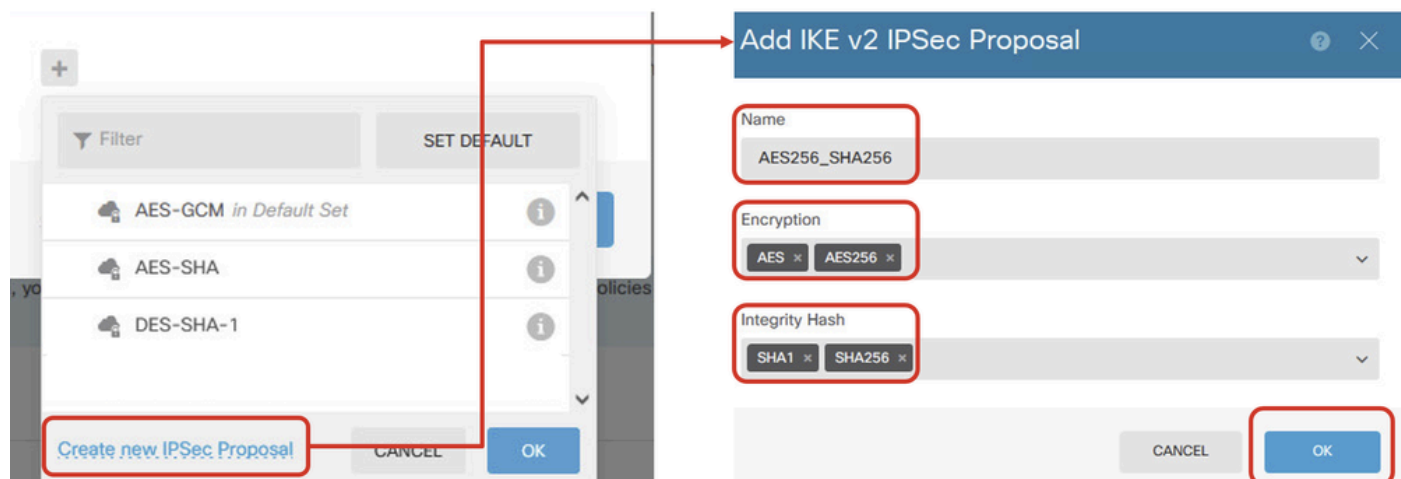
步驟5.4.導覽至IPSec建議書。按一下EDIT按鈕。



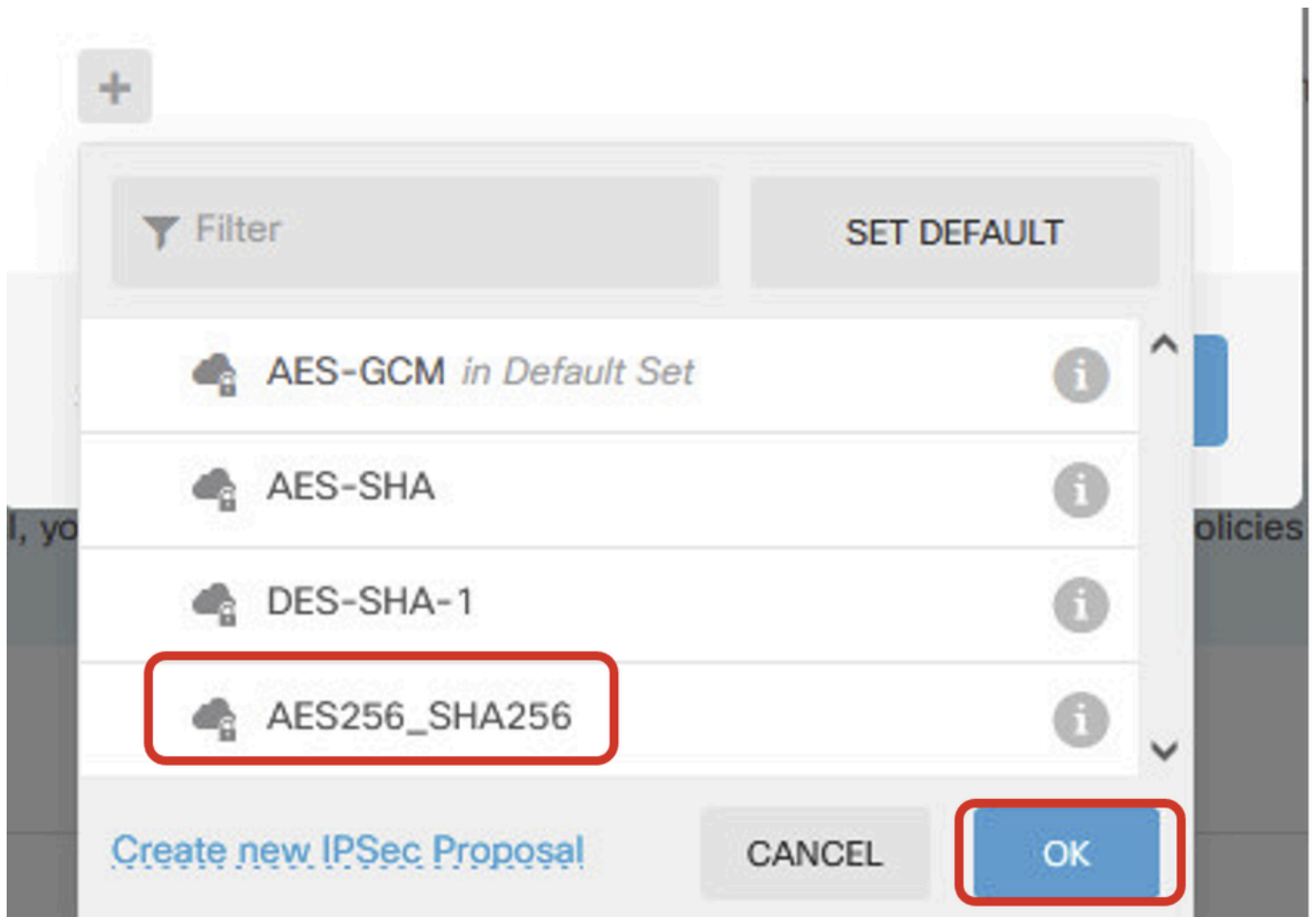
Site1FTD_Edit_IKE_Proposal

步驟5.5.對於IPSec建議，您可以使用預定義的建議或按一下建立新的IPSec建議創建新的IPSec建議。在本示例中，建立一個用於演示的新示例。按一下OK按鈕以進行儲存。

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



Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

步驟5.6.向下滾動頁面並配置預共用金鑰。按一下「下一步」按鈕。

記下此預共用金鑰，稍後在Site2 FTD上配置它。

Firewall Device Manager

MonitoringPoliciesObjects

Device: ftdv742

admin Administrator

FTDV742INTERNETPEER ENDPOINT

Privacy Configuration

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

IKE Policy

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

IKE VERSION 2

IKE VERSION 1

IKE Policy

Globally applied

EDIT...

IPSec Proposal

Custom set selected

EDIT...

Authentication Type

Pre-shared Manual Key

Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

BACK

NEXT

Site1FTD_Configure_Pre_Shared_Key

步驟5.7.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

i 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)

i 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.

BACK

FINISH

Site1FTD_ISP1_Review_VPN_Config_Summary

步驟6.重復步驟5.以便通過ISP2建立新的站點到站點VPN。

Demo_S2S_SP2 Connection Profile

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

VPN Access
Interface

demovti_sp2 (169.254.20.11)

Peer IP Address

192.168.20.1

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

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.

Diffie-Hellman

Null (not selected)

BACK

FINISH

Site1FTD_ISP2_Review_VPN_Config_Summary

步驟7.建立存取控制規則，以允許流量通過FTD。在本例中，允許所有用於演示。根據您的實際需要修改您的策略。

Firewall Device Manager

Monitoring Policies Objects Device: ftdv742

admin Administrator

SECURE

Security Policies

1 rule

Filter

#	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

Site1FTD_Allow_Access_Control_Rule_Example

步驟8.(可選)如果為客戶端配置了動態NAT以訪問網際網路，請為FTD上的客戶端流量配置NAT豁免規則。

出於演示目的，本示例中為客戶端配置了動態NAT以訪問網際網路。因此需要NAT豁免規則。

導航到Policies > NAT。按一下+按鈕。提供詳細資訊，然後按一下「OK」。

- Title:NAT免除
- 位置：自動NAT規則之前
- Type:靜態
- 源介面：INSIDE
- 目標：任意
- 原始源地址：192.168.70.0/24
- 轉換後的源地址：192.168.70.0/24
- 原始目標地址：192.168.50.0/24
- 轉換的目標地址：192.168.50.0/24
- 啟用Route-Lookup

Firewall Device Manager

Monitoring Policies

Security Policies

2 rules

Manual NAT Rules

1 NAT Exempt STATIC

Manual NAT Rules (After)

1 InsideOutside... DYNAMIC

Add NAT Rule

Title: NAT Exempt

Create Rule for: Manual NAT

Status: ☒

Placement: Before Auto NAT Rules

Type: Static

Packet Translation

Advanced Options

ORIGINAL PACKET

Source Interface: inside

Source Address: inside_192.168.70

Source Port: Any

Destination Address: peer_192.168.50

Destination Port: Any

TRANSLATED PACKET

Destination Interface: Any

Source Address: inside_192.168.70

Source Port: Any

Destination Address: peer_192.168.50

Destination Port: Any

Show Diagram: ☐

CANCEL OK

Site1FTD_Nat_Exempt_Rule

Add NAT Rule

Title

NAT Exempt

Create Rule for

Manual NAT

Status

☒

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement

Before Auto NAT Rules

Type

Static

Packet Translation

Advanced Options

☐ Translate DNS replies that match this rule

☐ Fallthrough to Interface PAT (Destination Interface)

☒ Perform route lookup for Destination interface

☐ Do not proxy ARP on Destination Interface

Show Diagram

☐

CANCEL

OK

Site1FTD_Nat_Exempt_Rule_2

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv742

admin Administrator

SECURE

Security Policies

SSL Decryption

Identity

Security Intelligence

NAT

Access Control

Intrusion

3 rules

Filter

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Manual NAT Rules												
> 1	NAT Exempt	STATIC	Inside Any	inside_192.1...	peer_192.16...	ANY	ANY	inside_192.1...	peer_192.16...	ANY	ANY	
Manual NAT Rules (After)												
> 1	ISP1NatRule	DYNAMIC	Inside outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	
> 3	ISP2NatRule	DYNAMIC	Inside outside2	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Site1FTD_Nat_Rule_Overview

步驟9.部署配置更改。



Site1FTD_Deployment_Changes

站點2 FTD VPN配置

步驟10.使用站點2 FTD的相應引數重複步驟1到步驟9。

DemoS2S Connection Profile

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

VPN Access Interface

demovti25 (169.254.10.2)

Peer IP Address

192.168.30.1

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

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.

Diffie-Hellman Group

Null (not selected)

BACK

FINISH

Site2FTD_ISP1_Review_VPN_Config_Summary

Demo_S2S_SP2 Connection Profile

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

VPN Access Interface demovti_sp2 (169.254.20.12)



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, 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

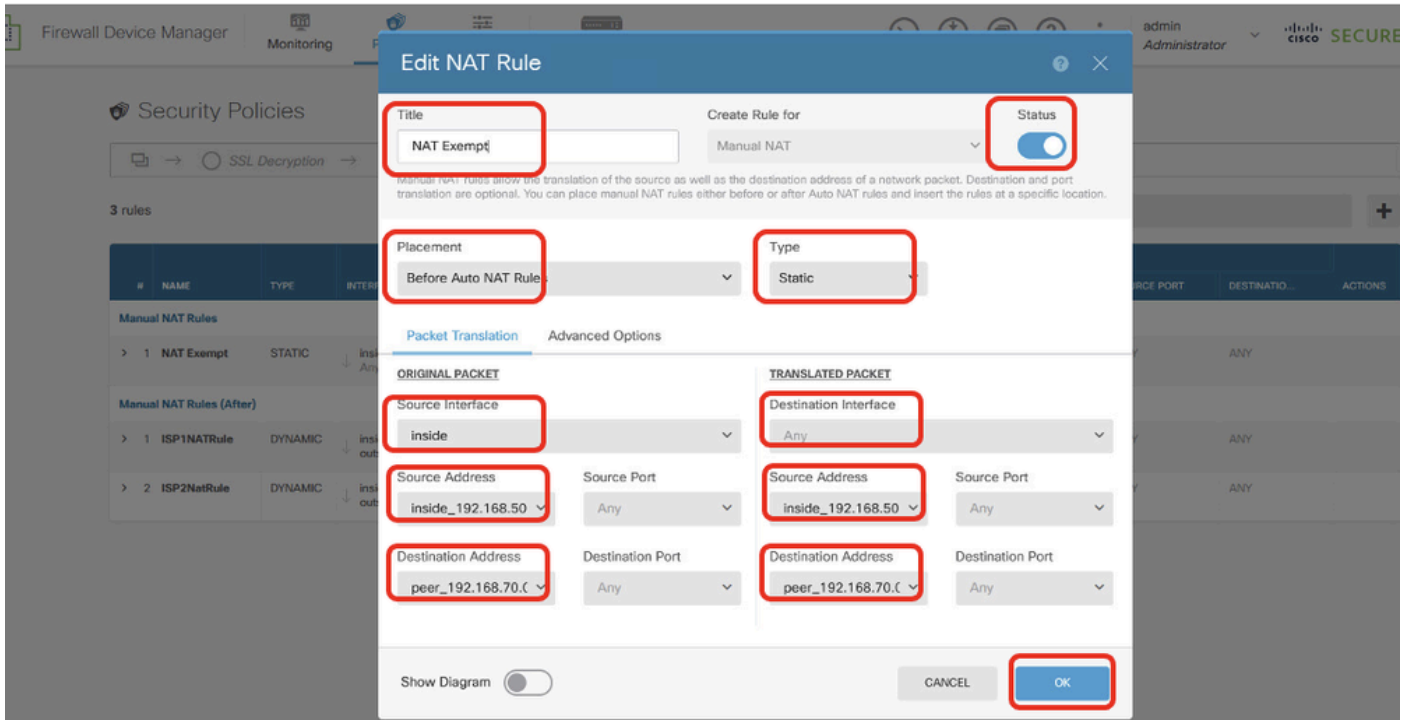
Lifetime Size 4608000 kilobytes

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.

Diffie-Hellman Group Null (not selected)

BACK

FINISH

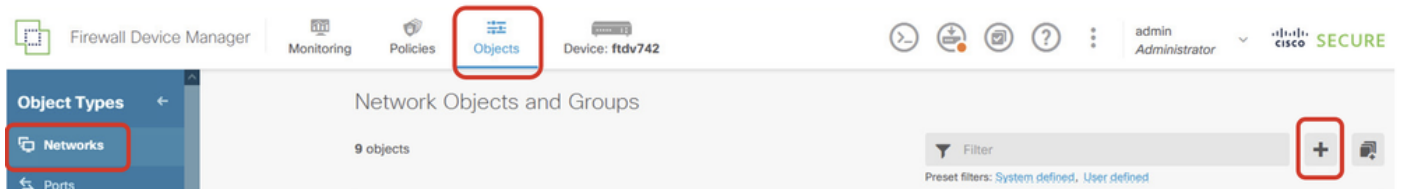


Site2FTD_Nat_Exempt_Rule

PBR上的配置

站點1 FTD PBR配置

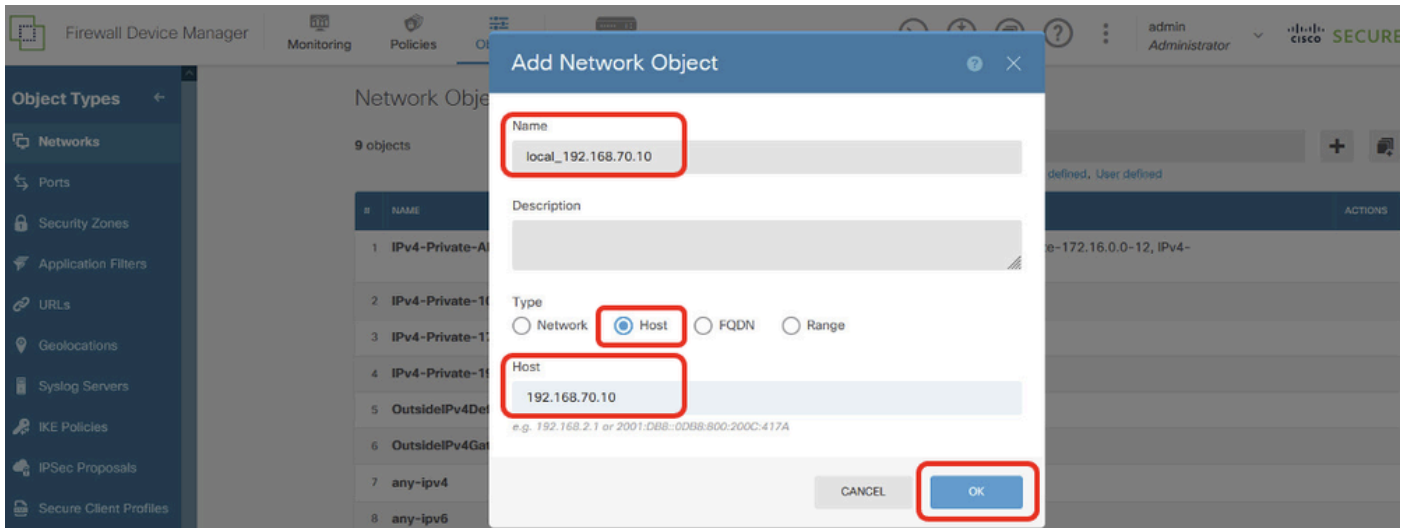
步驟11. 為Site1 FTD建立要由PBR訪問清單使用的新網路對象。導航到對象>網路，然後按一下+按鈕。



Site1FTD_Create_Network_Object

步驟 11.1. 建立Site1 Client2 IP地址的對象。提供必要資訊。按一下OK按鈕。

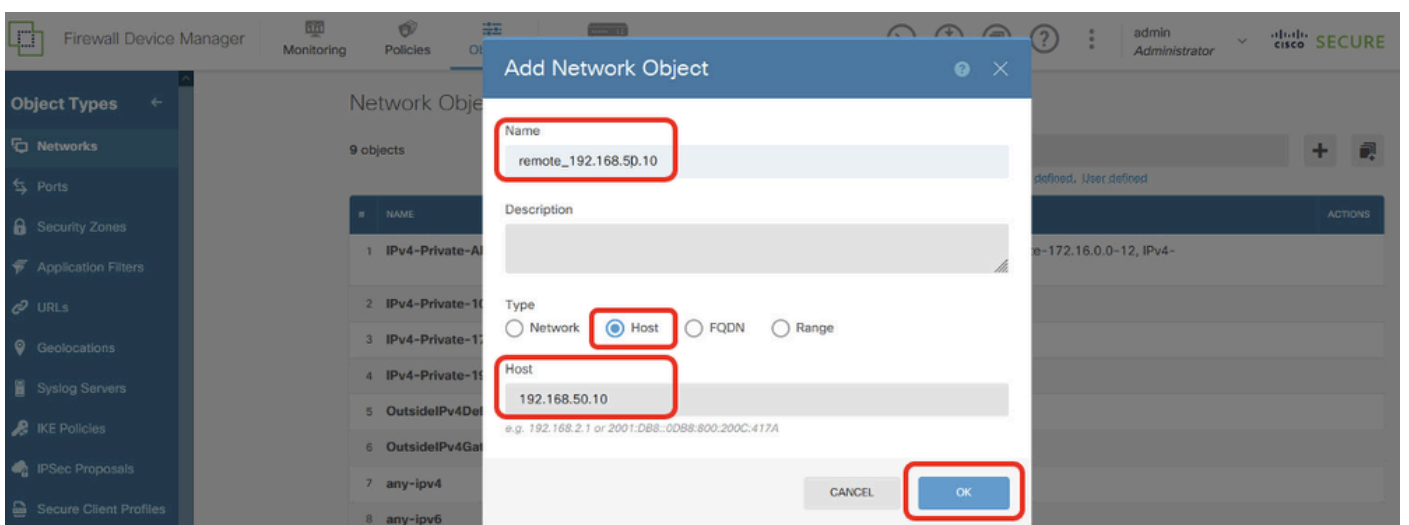
- 名稱:local_192.168.70.10
- Type:主機
- 主機 : 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

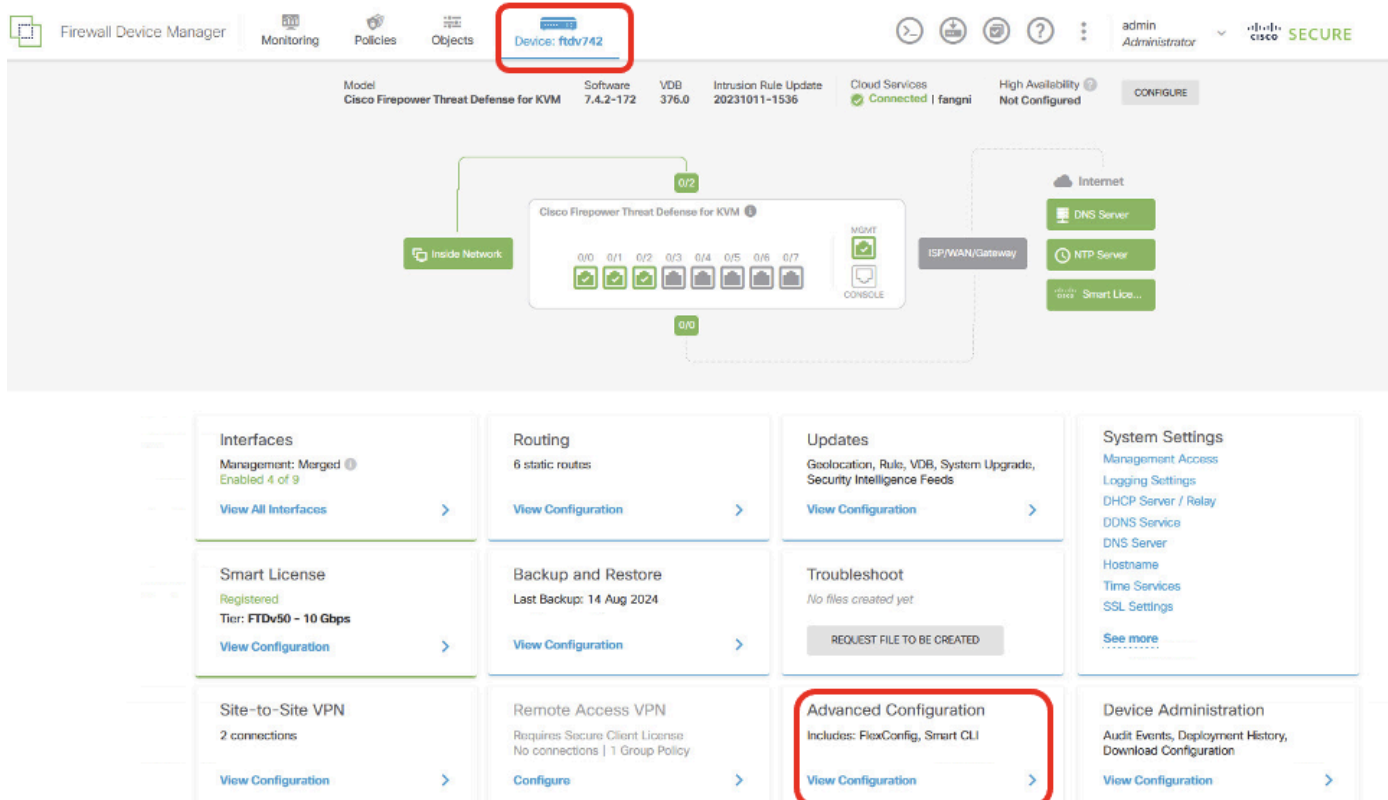
步驟11.2.建立Site2 Client2 IP地址的對象。提供必要資訊。按一下「OK」按鈕。

- 名稱:remote_192.168.50.10
- Type:主機
- 主機 : 192.168.50.10



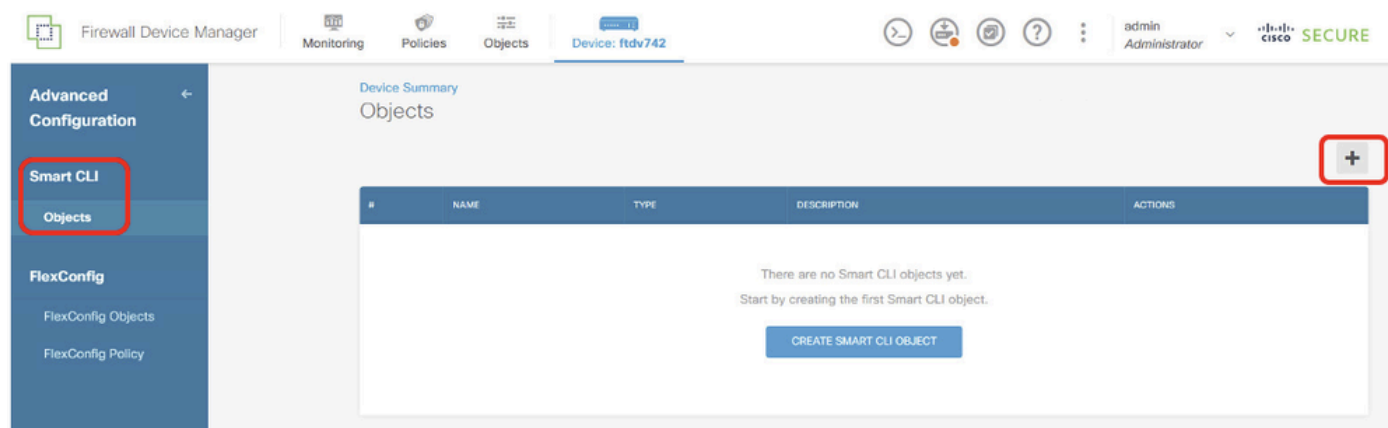
Site1FTD_PBR_RemoteObject

步驟12.為PBR建立擴展訪問清單。導覽至Device > Advanced Configuration。按一下「View Configuration」。



Site1FTD_View_Advanced_Configuration

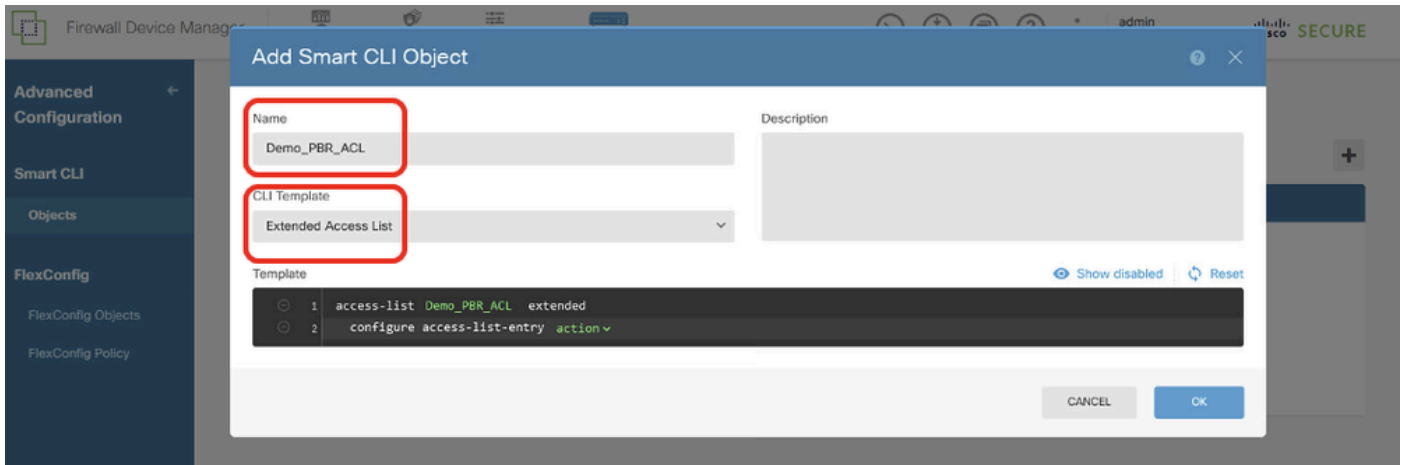
步驟12.1.導航到Smart CLI > Objects。按一下+按鈕。



Site1FTD_Add_SmartCLI_Object

步驟12.2.輸入對象的名稱，然後選擇CLI模板。

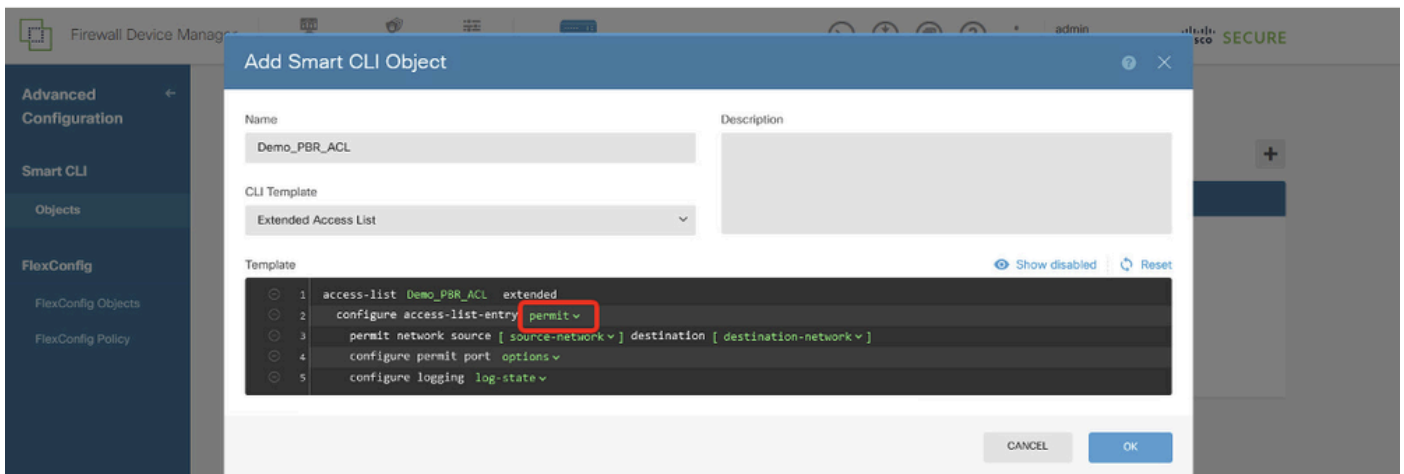
- 名稱: Demo_PBR_ACL
- CLI模板：擴展訪問清單



Site1FTD_Create_PBR_ACL_1

步驟12.3.導覽至Template並進行設定。按一下OK按鈕以進行儲存。

第2行，按一下action。選擇permit。

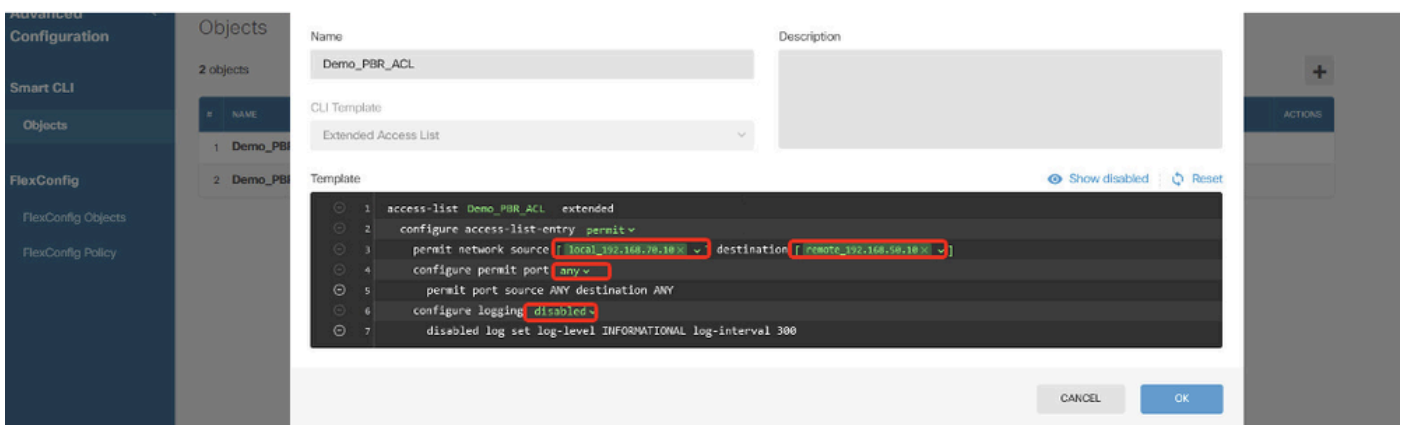


Site1FTD_Create_PBR_ACL_2

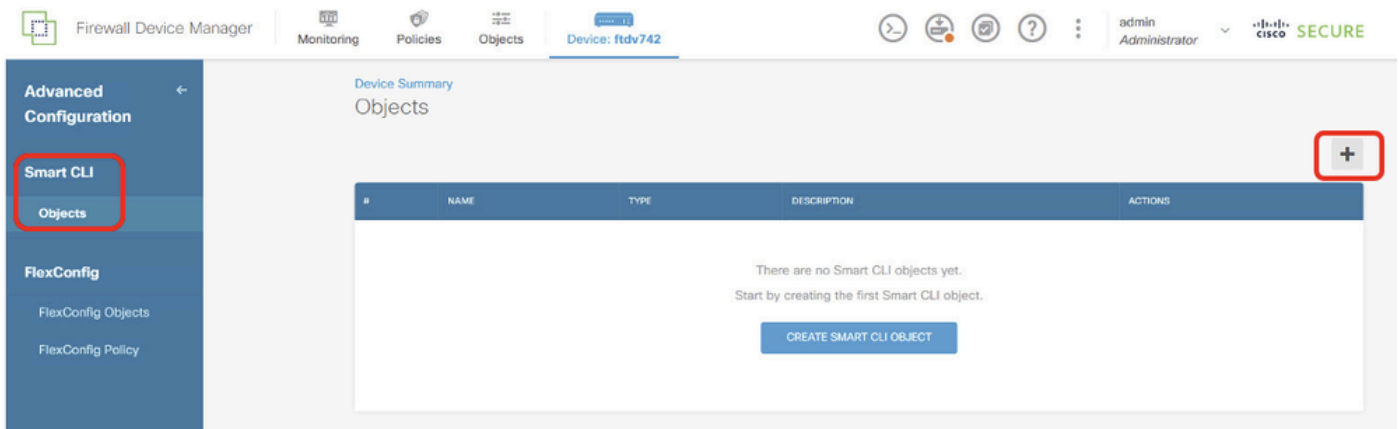
第3行，按一下source-network。選擇local_192.168.70.10。按一下destination-network。選擇remote_192.168.50.10。

第4行，按一下options並選擇any。

第6行，按一下log-state 並選擇disabled。

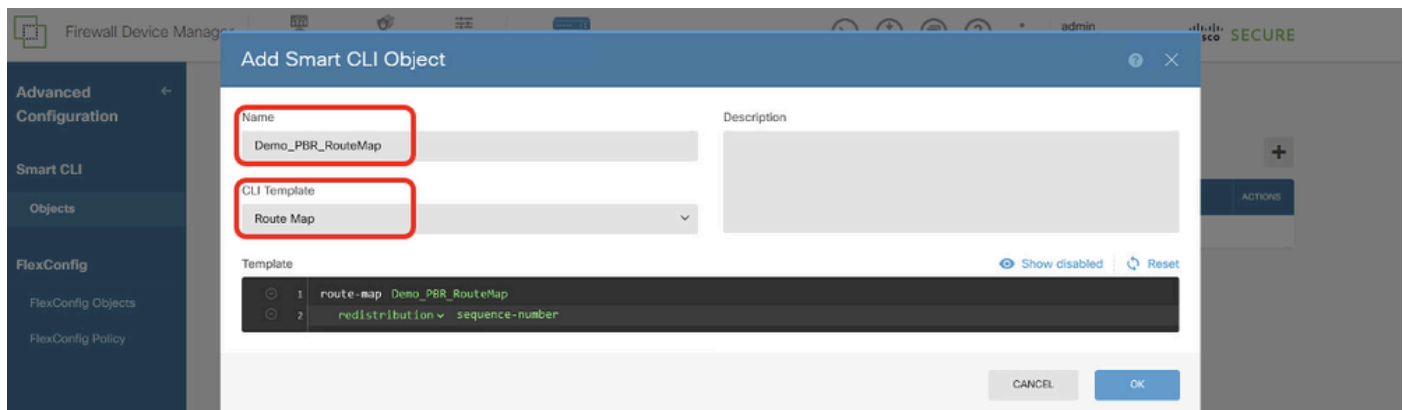


步驟13.為PBR建立路由對映。導航到Device > Advanced Configuration > Smart CLI > Objects。按一下+按鈕。



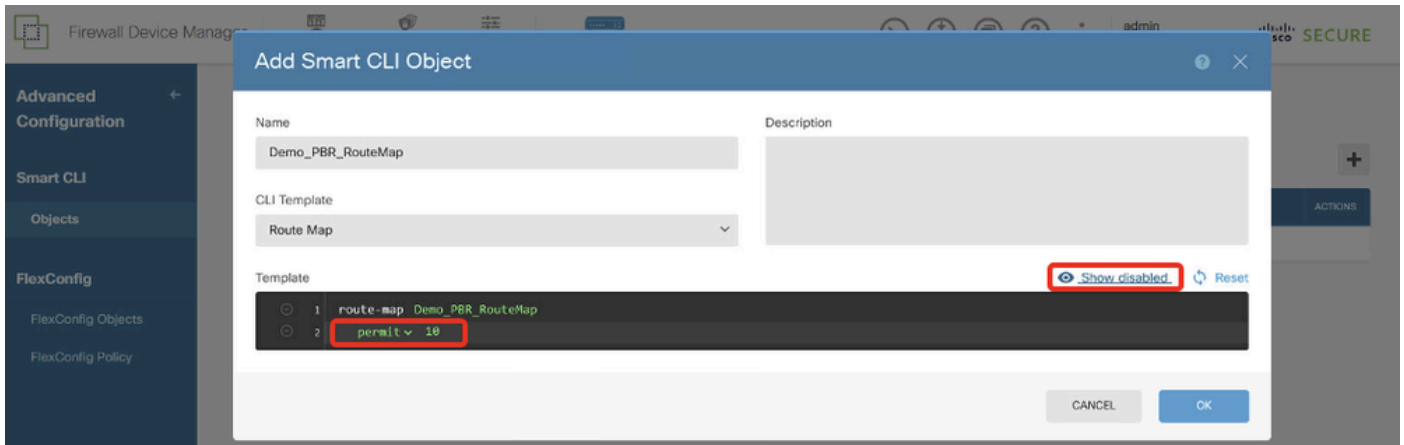
步驟13.1.輸入對象的名稱，然後選擇CLI模板。

- 名稱: Demo_PBR_RouteMap
- CLI模板：路由對映



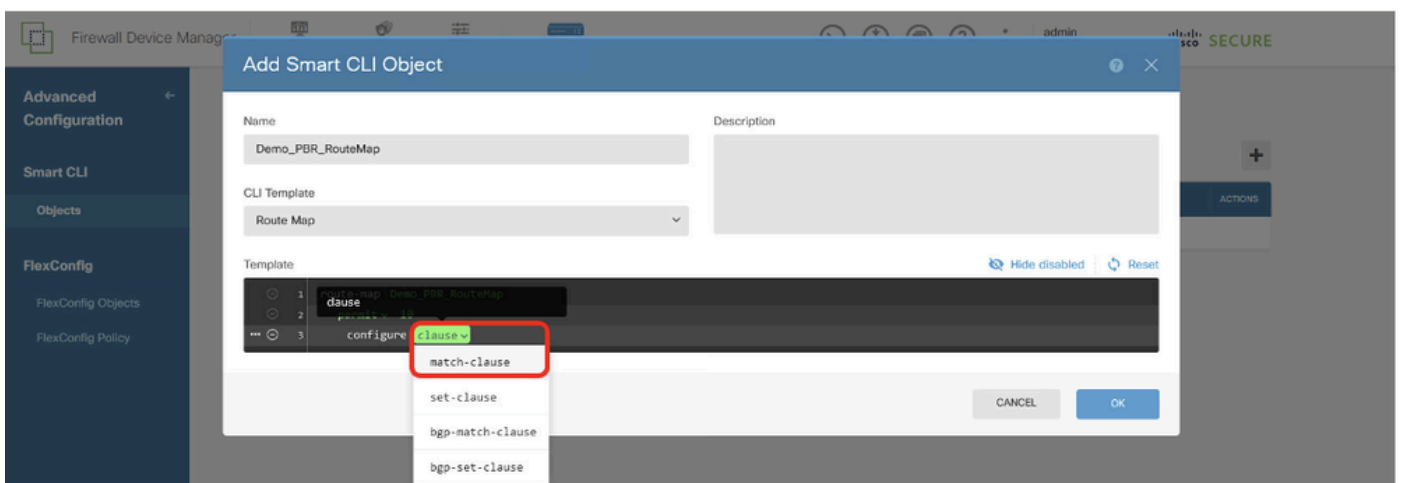
步驟13.2.導覽至Template並進行設定。按一下OK按鈕進行儲存。

第2行，按一下redistribution。選擇permit。按一下「sequence-number, manual input 10」。按一下「Show disabled」。



Site1FTD_Create_PBR_RouteMap_2

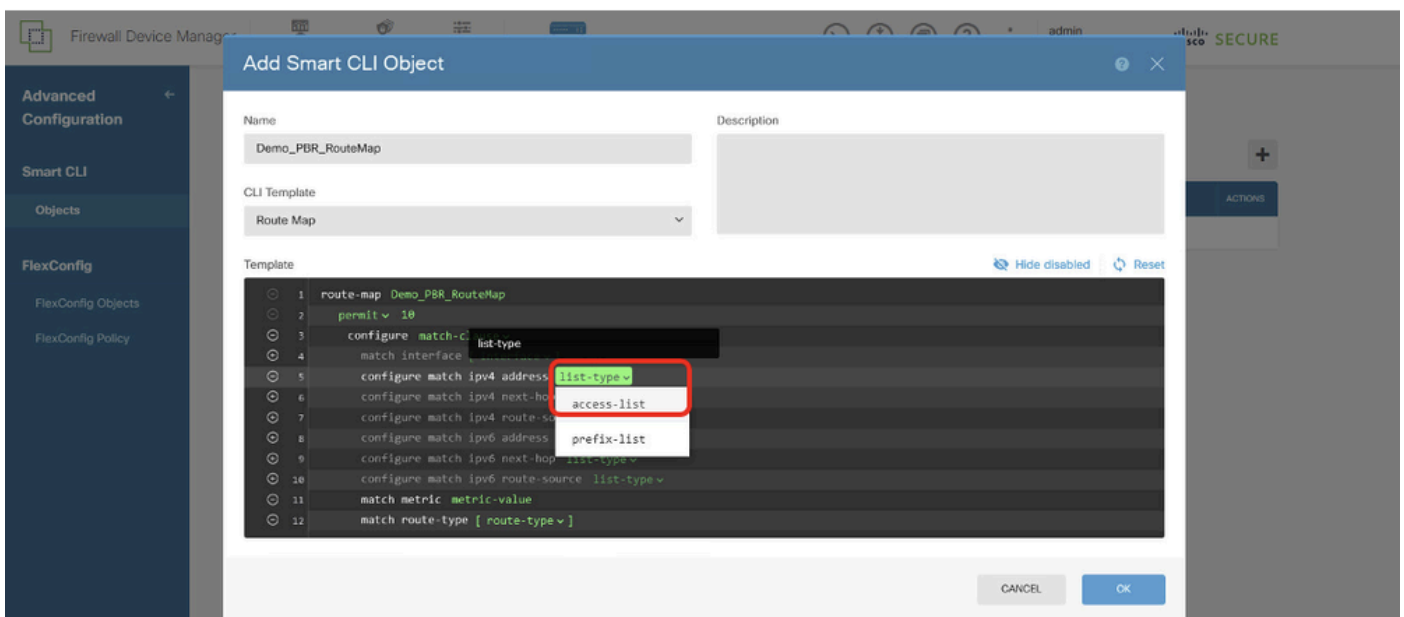
第3行，按一下+ 啟用該行。按一下clause。選擇match-clause。



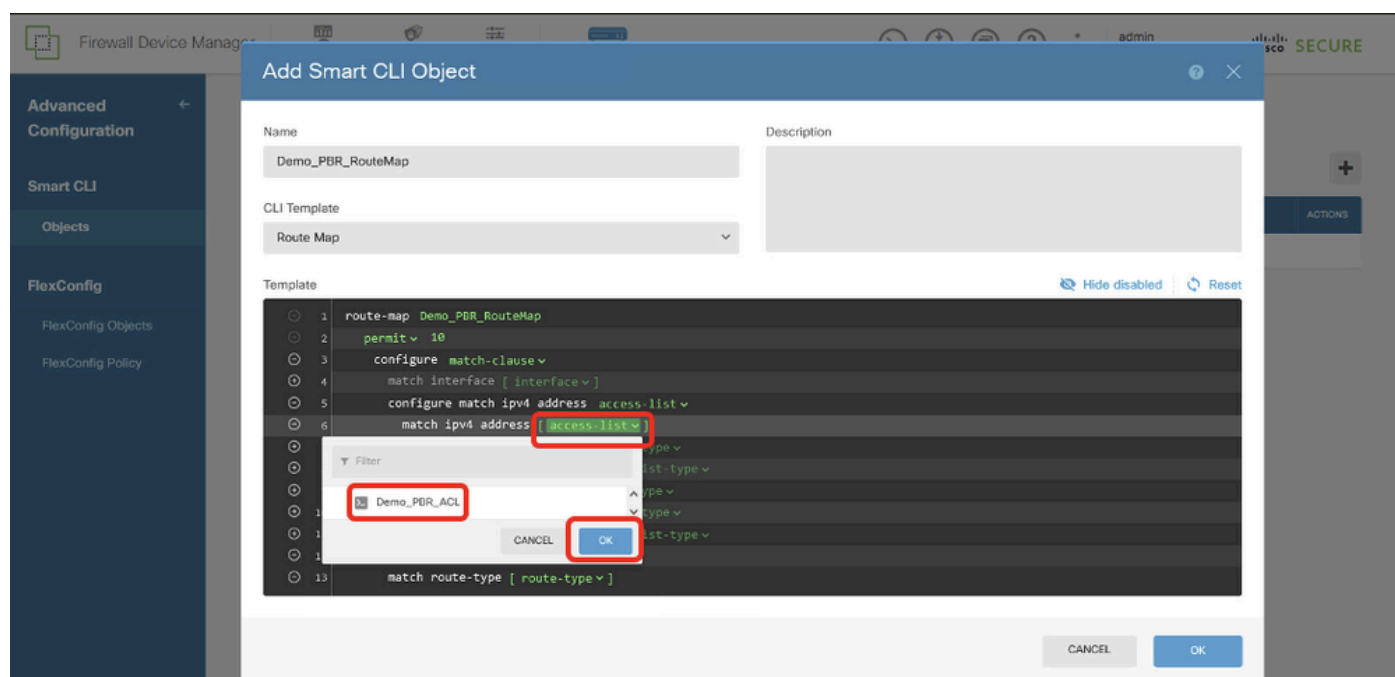
Site1FTD_Create_PBR_RouteMap_3

第4行，按一下-禁用該行。

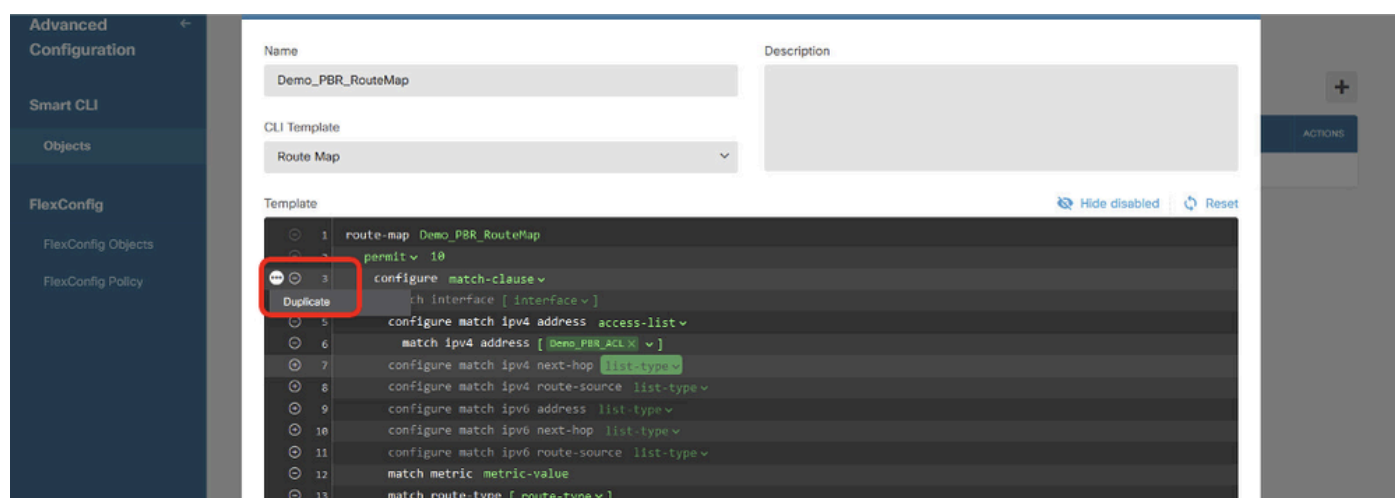
第5行，按一下+啟用該行。按一下「list-type」。選擇access-list。



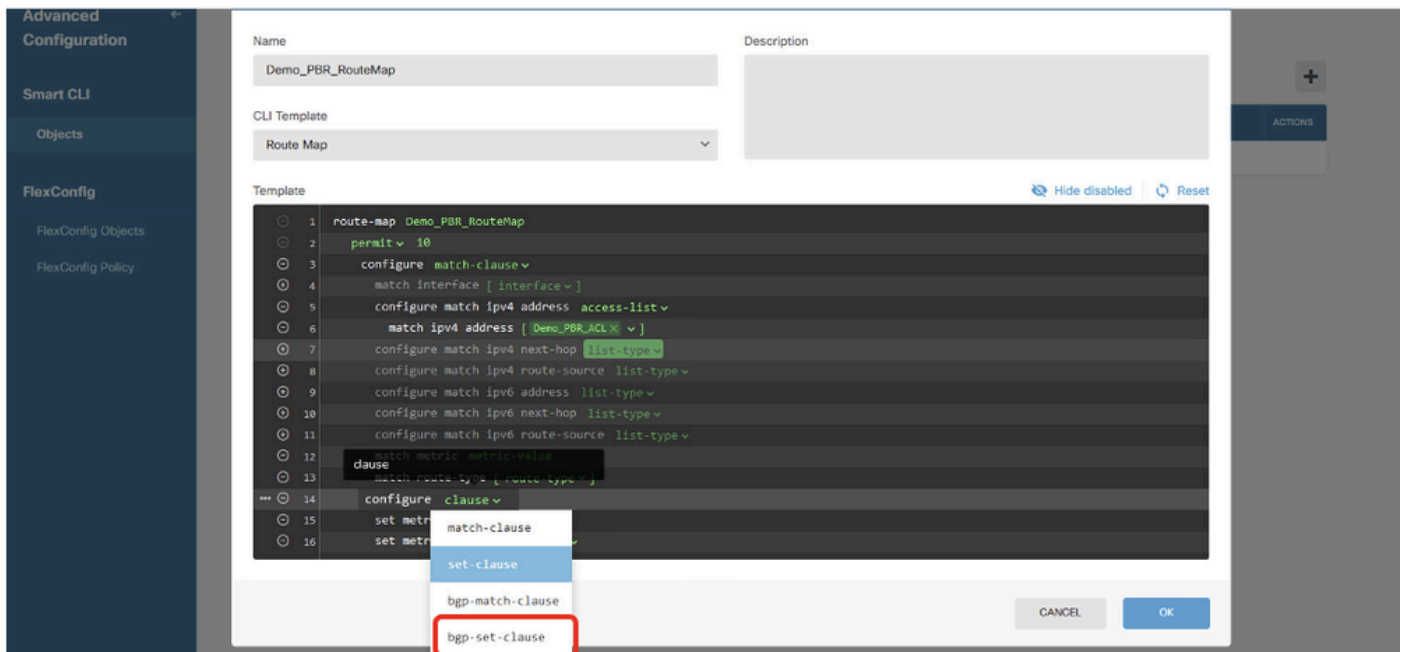
第6行，按一下access-list。選擇在步驟12中建立的ACL名稱。在本例中，它是Demo_PBR_ACL。



移回第3行。按一下選項... 按鈕並選擇複製。



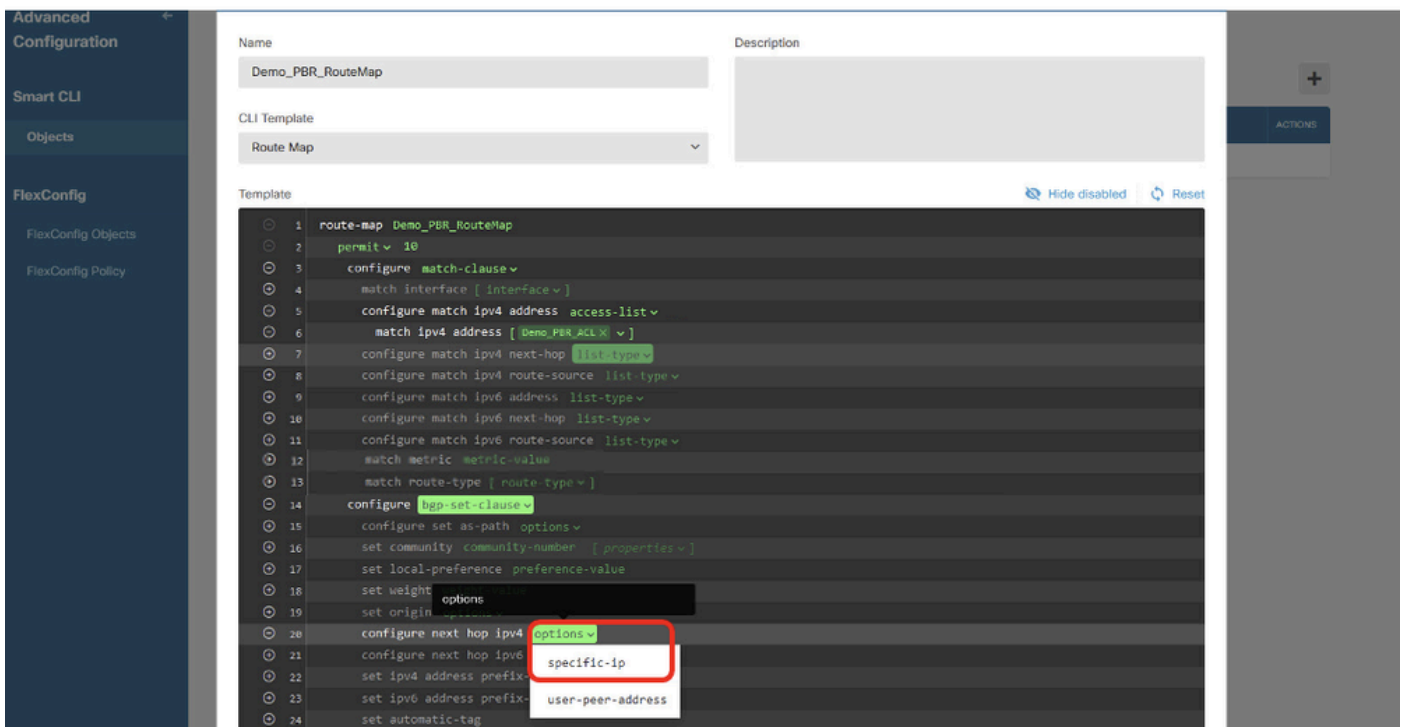
在第14行中，按一下clause並選擇bgp-set-clause。



Site1FTD_Create_PBR_RouteMap_7

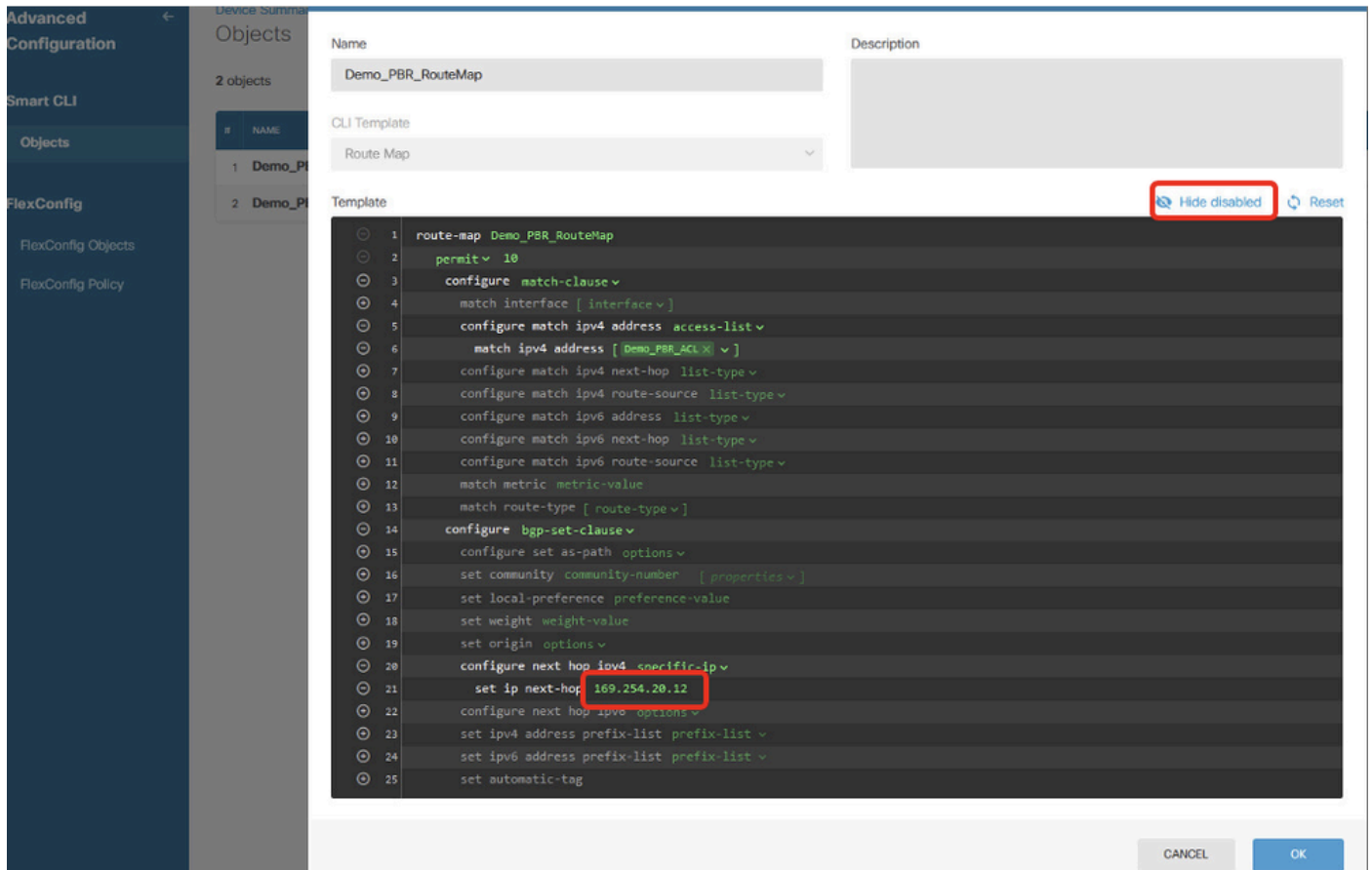
在行12、13、15、16、17、18、19、21、22、23、24中，按一下按鈕以禁用。

第20行，按一下options並選擇specific-ip。



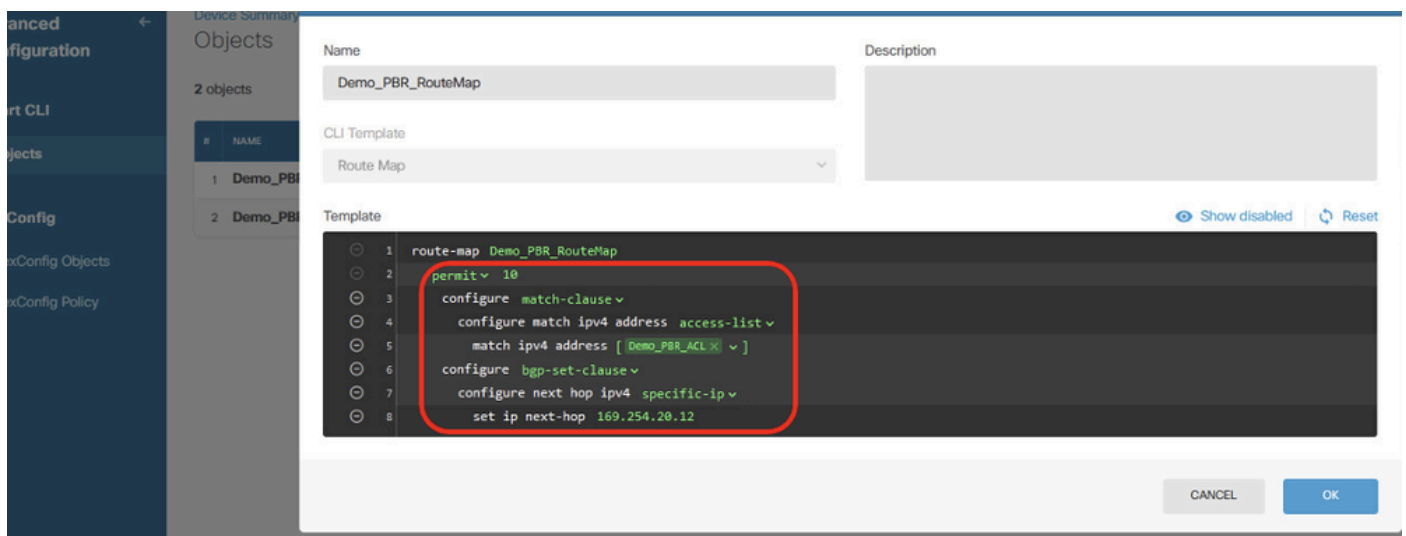
Site1FTD_Create_PBR_RouteMap_8

第21行，按一下ip-address。手動輸入下一跳IP地址。在本範例中，這是對等點Site2 FTD VTI通道2(169.254.20.12)的IP位址。按一下Hide disabled。



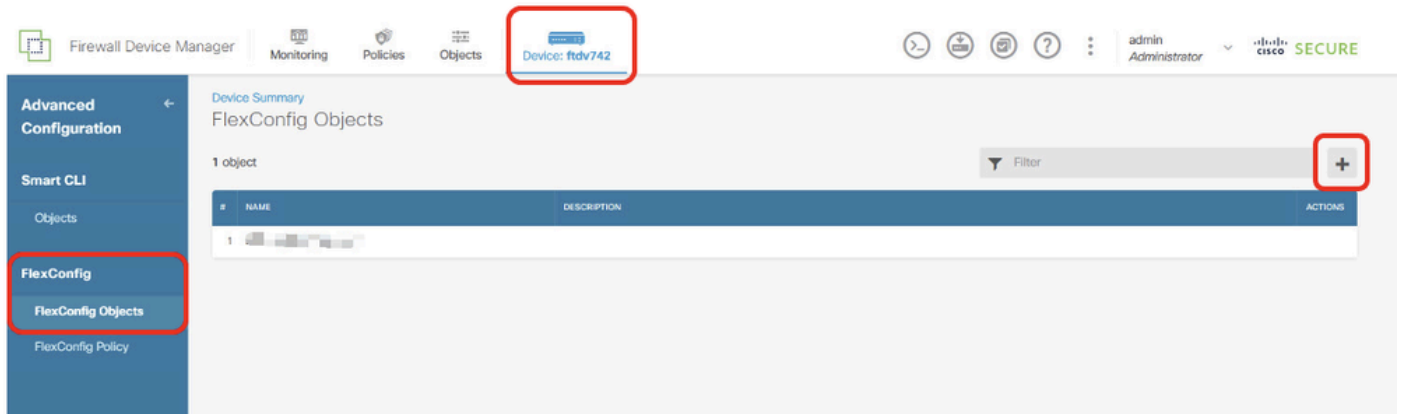
Site1FTD_Create_PBR_RouteMap_9

檢查路由對映的配置。



Site1FTD_Create_PBR_RouteMap_10

步驟14.為PBR建立FlexConfig對象。導航到Device > Advanced Configuration > FlexConfig Objects，然後點選+按鈕。



Site1FTD_Create_PBR_FlexObj_1

步驟14.1.輸入對象的名稱。在本例中，Demo_PBR_FlexObj。在Template和Negate Template編輯器中輸入命令列。

- 模板：

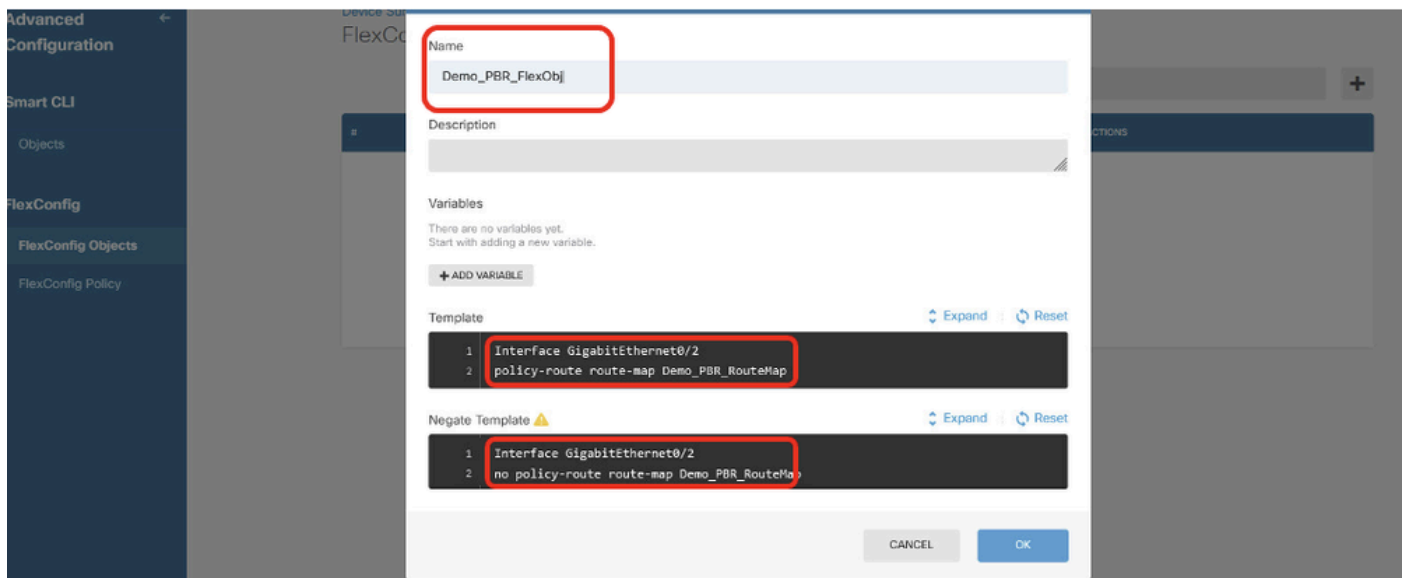
```
interface GigabitEthernet0/2
```

```
policy-route route-map Demo_PBR_RouteMap_Site2
```

- 否定模板：

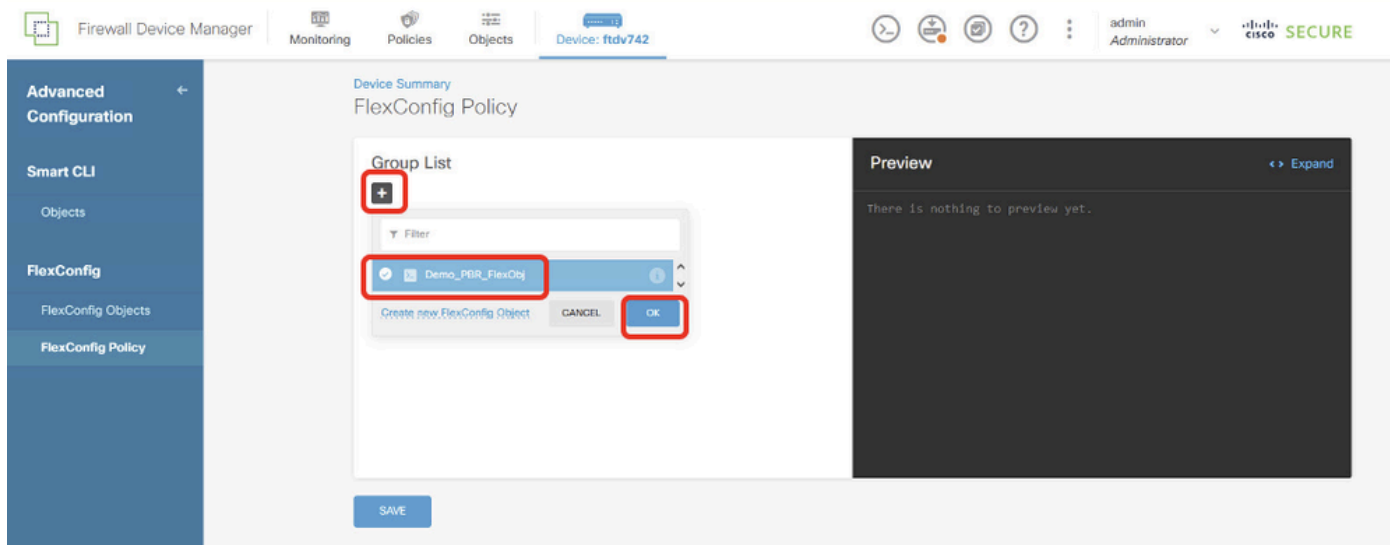
```
interface GigabitEthernet0/2
```

```
no policy-route route-map Demo_PBR_RouteMap_Site2
```



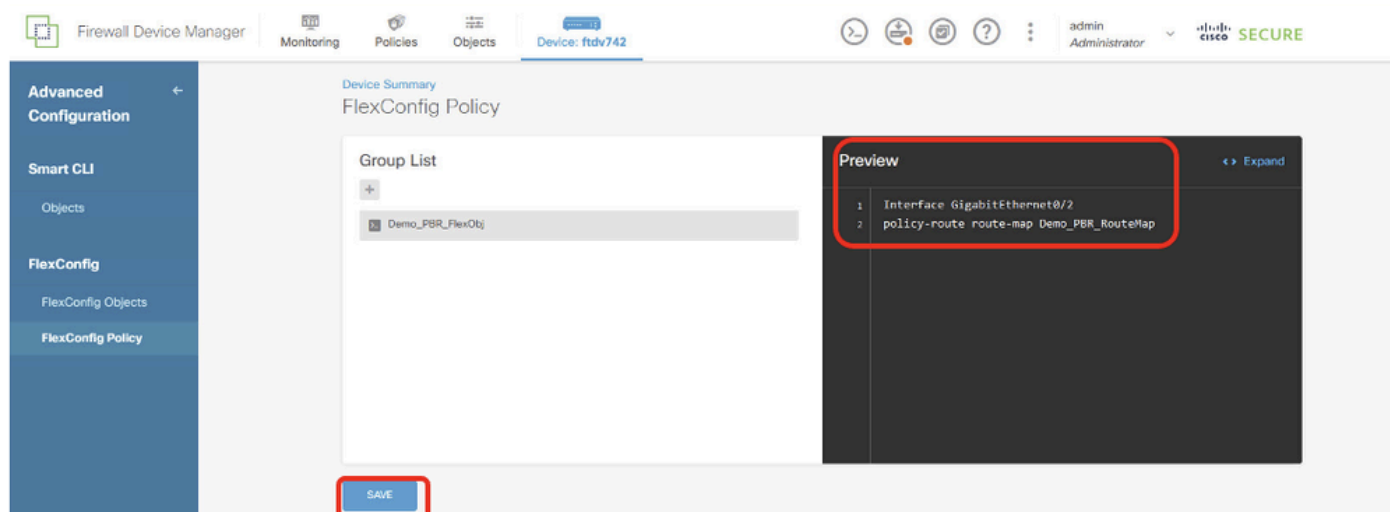
Site1FTD_Create_PBR_FlexObj_2

步驟15.為PBR建立FlexConfig策略。導航到Device > Advanced Configuration > FlexConfig Policy。按一下+按鈕。選擇在步驟14中建立的FlexConfig對象名稱。按一下OK按鈕。



Site1FTD_Create_PBR_FlexPolicy_1

步驟15.1.在預覽視窗中檢驗命令。如果條件良好，請按一下Save。



Site1FTD_Create_PBR_FlexPolicy_2

步驟16.部署配置更改。



Site1FTD_Deployment_Changes

站點2 FTD PBR配置

步驟17.重複步驟11至步驟16.以便使用站點2 FTD的相應引數建立PBR。

Firewall Device Manager

Add Smart CLI Object

Name: **Demo_PBR_ACL_Site2**

Description:

CLI Template: Extended Access List

Template:

```

1 access-list Demo_PBR_ACL_Site2 extended
2 configure access-list-entry permit
3 permit network source [ local_192.168.56.10 % ] destination [ remote_192.168.79.10 % ]
4 configure permit port any
5 permit port source ANY destination ANY
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300

```

[Show disabled](#) [Reset](#)

[CANCEL](#) [OK](#)

Site2FTD_Create_PBR_ACL

Firewall Device Manager

Add Smart CLI Object

Name: **Demo_PBR_RouteMap_Site2**

Description:

CLI Template: Route Map

Template:

```

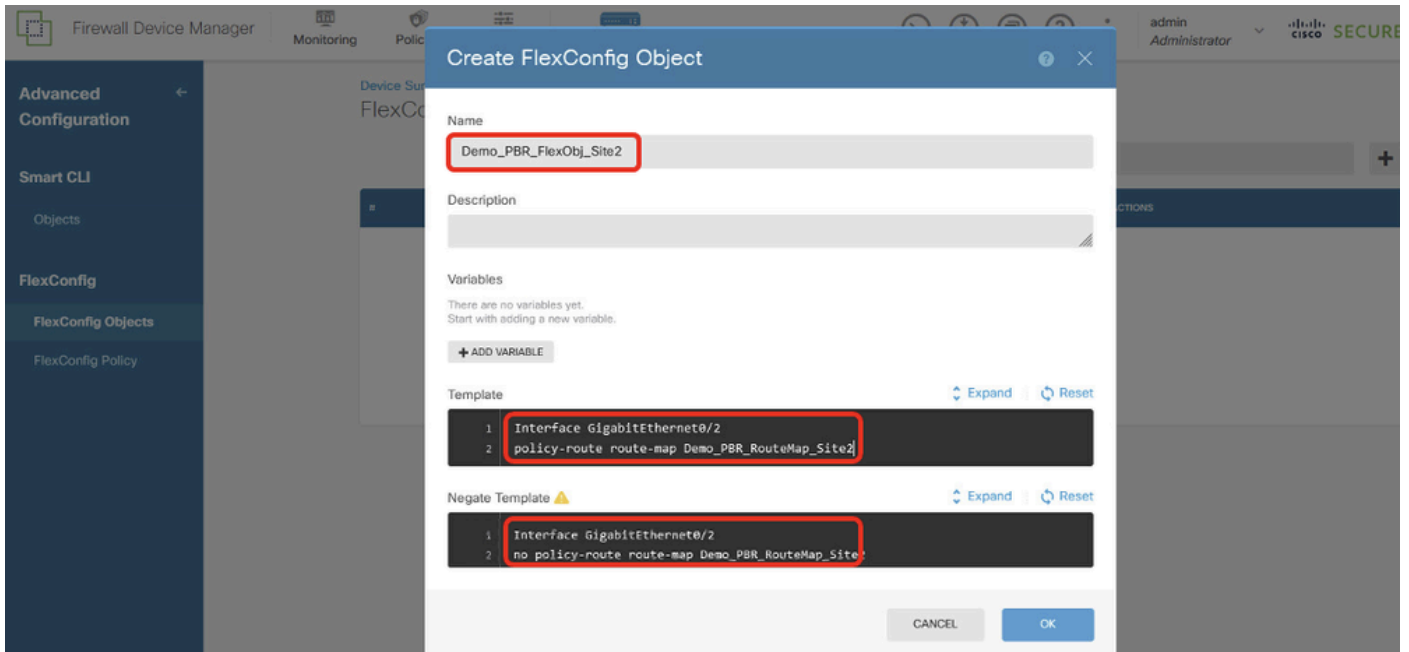
1 route-map Demo_PBR_RouteMap_Site2
2 permit 10
3 configure match-clause
4 configure match ipv4 address access-list
5 match ipv4 address [ Demo_PBR_ACL_Site2 % ]
6 configure bgp-set-clause
7 configure next hop ipv4 specific-ip
8 set ip next-hop 169.254.20.11

```

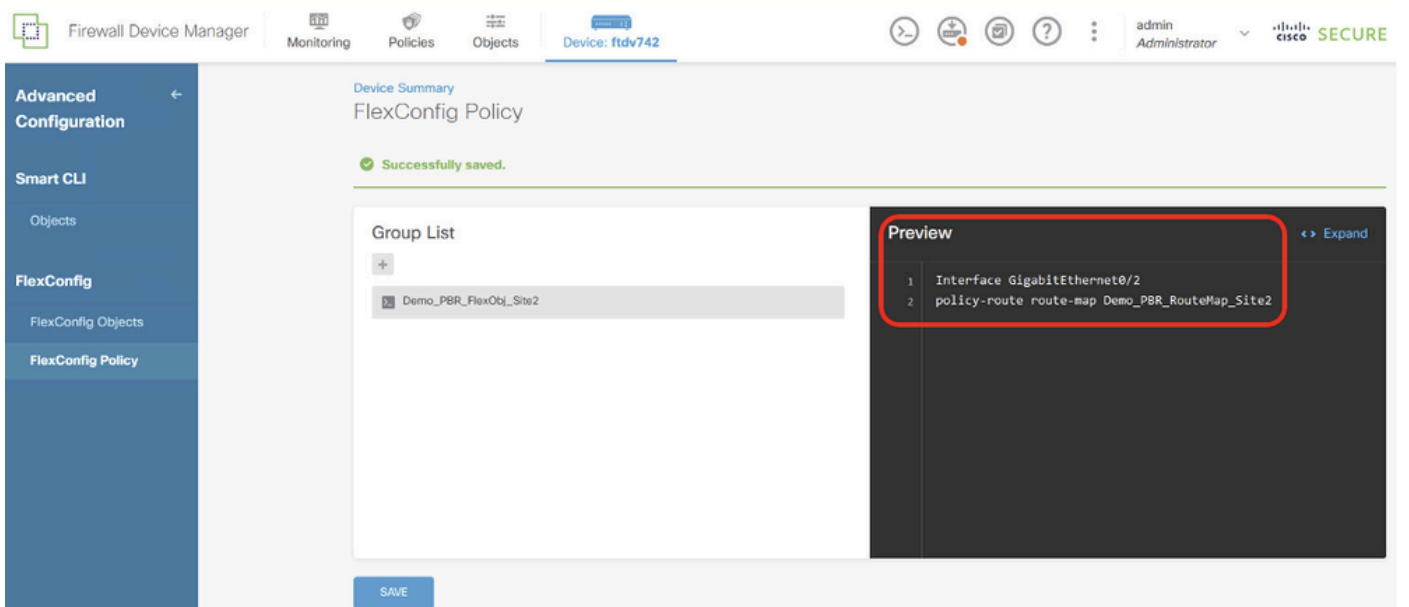
[Show disabled](#) [Reset](#)

[CANCEL](#) [OK](#)

Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

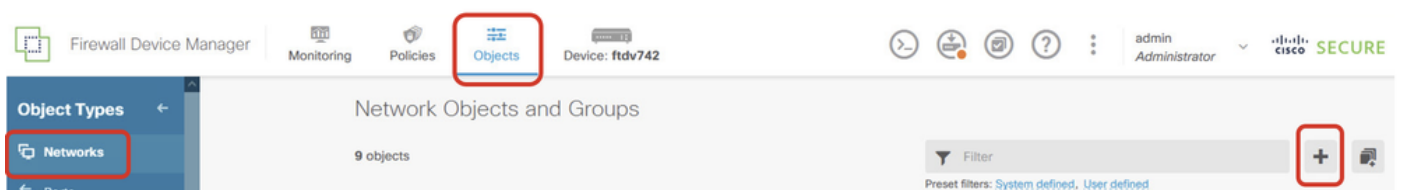


Site2FTD_Create_PBR_FlexPolicy

SLA監控器上的配置

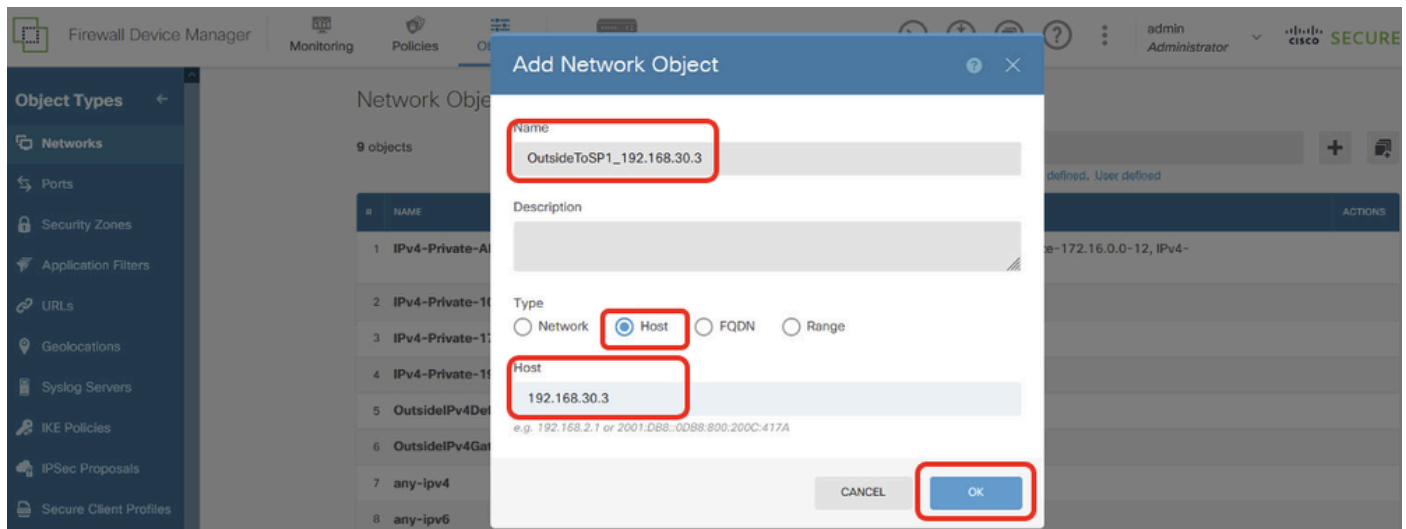
Site1 FTD SLA監控器配置

步驟18.為Site1 FTD的SLA監控器建立新的網路對象。導航到對象>網路，單擊+按鈕。



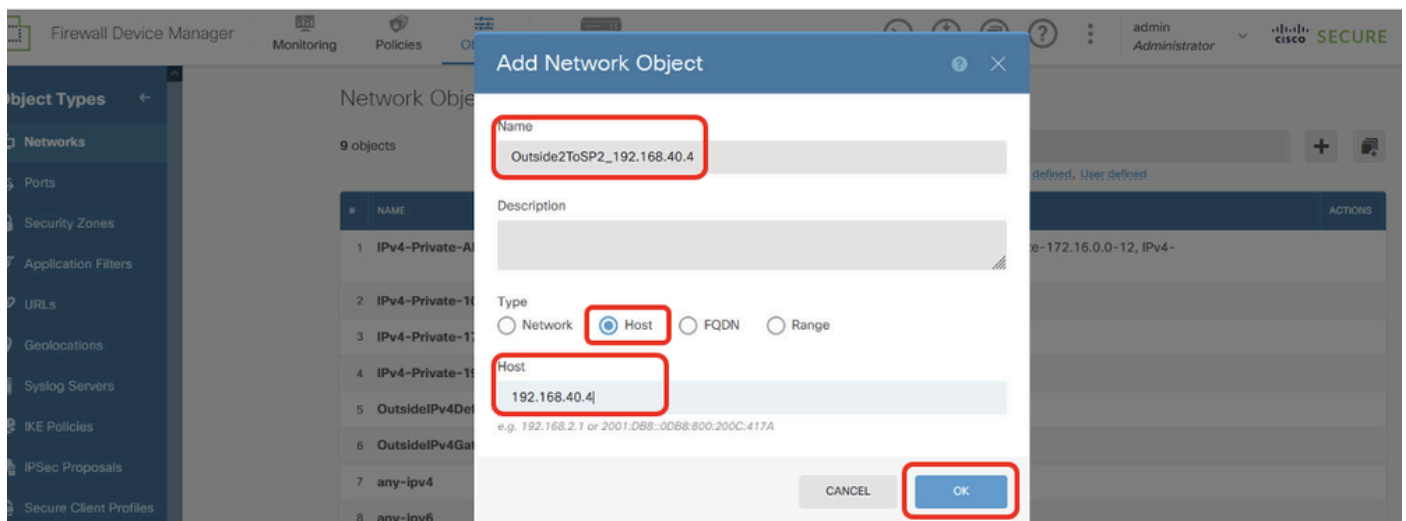
步驟18.1.為ISP1網關IP地址建立對象。提供必要資訊。按一下「OK」按鈕。

- 名稱:OutsideToSP1_192.168.30.3
- Type:主機
- 主機：192.168.30.3



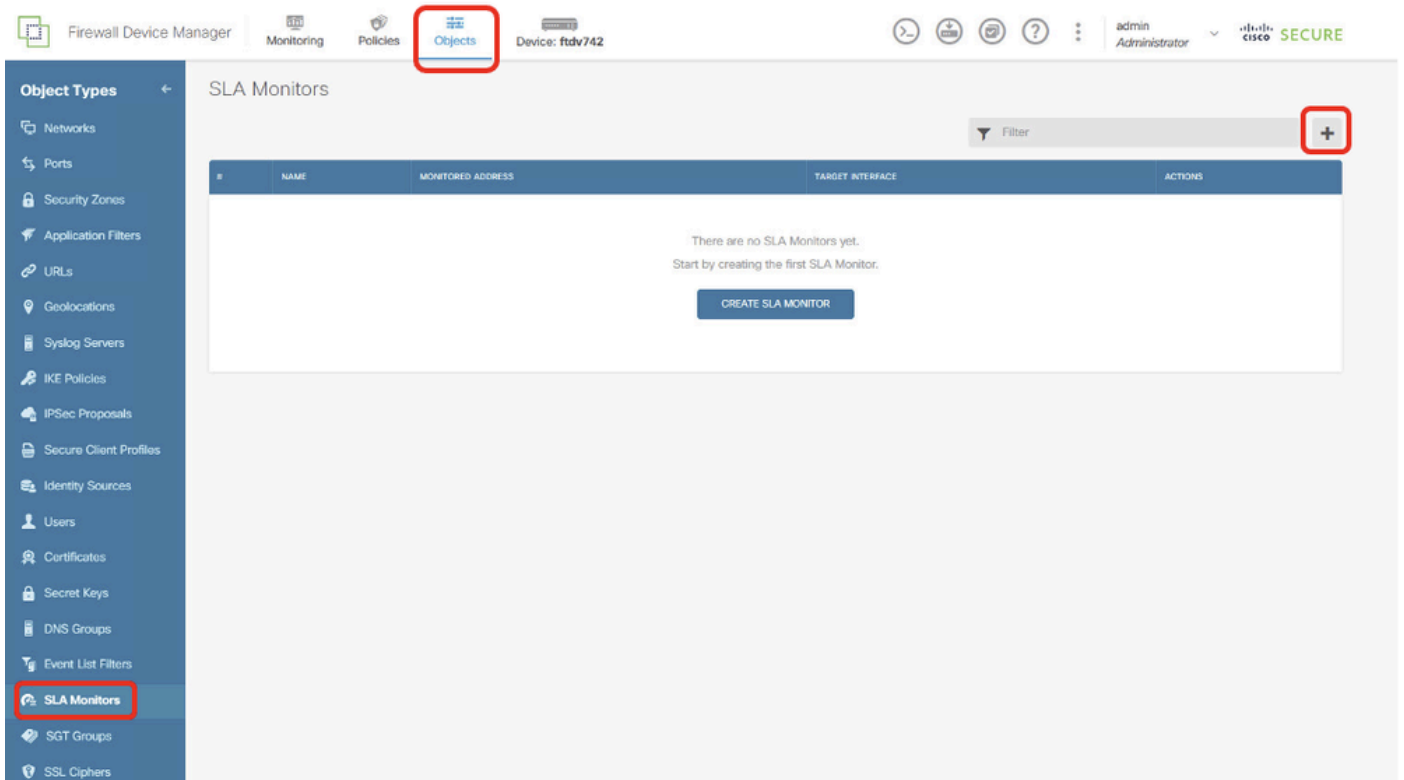
步驟18.2.為ISP2網關IP地址建立對象。提供必要資訊。按一下「OK」按鈕。

- 名稱:Outside2ToSP2_192.168.40.4
- Type:主機
- 主機：192.168.40.4



步驟19.建立SLA監控器。導航到對象>對象型別> SLA監控器。按一下+按鈕以建立新的SLA監控器。

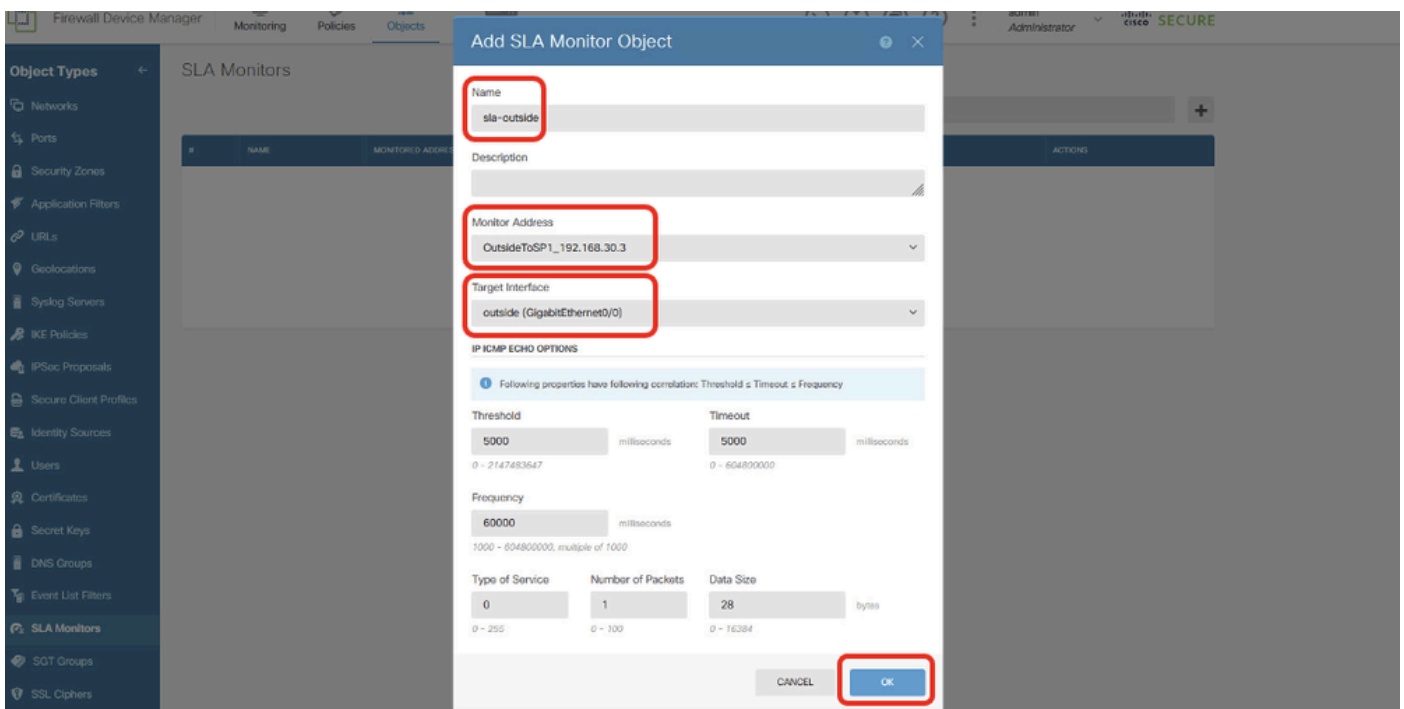
。



Site1FTD_Create_SLAMonitor

步驟19.1.在新增SLA監控對象視窗中，為ISP1網關提供必要的資訊。按一下OK按鈕進行儲存。

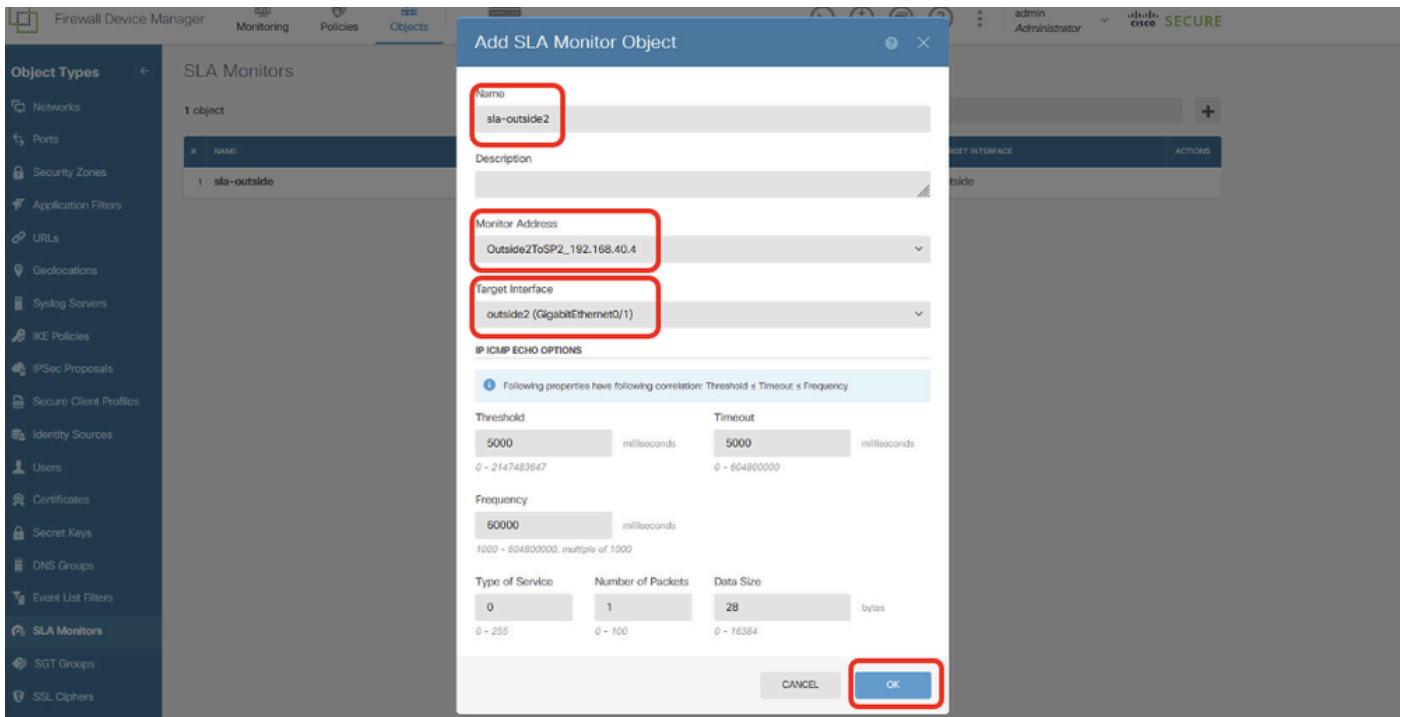
- 名稱:sla-outside
- 監控器地址：OutsideToSP1_192.168.30.3
- 目標介面：outside(GigabitEthernet0/0)
- IP ICMP ECHO選項：預設



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

步驟19.2.繼續按一下+按鈕為ISP2網關建立新的SLA監控器。在新增SLA監控對象視窗中，為ISP2網關提供必要的資訊。按一下OK按鈕進行儲存。

- 名稱:sla-outside2
- 監控器地址：Outside2ToSP2_192.168.40.4
- 目標介面：outside2(GigabitEthernet0/1)
- IP ICMP ECHO選項：預設



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

步驟20.部署配置更改。



Site1FTD_Deployment_Changes

站點2 FTD SLA監控器配置

步驟21.重複步驟18。到步驟20。使用站點2 FTD上的相應引數建立SLA監控器。

Object Types

SLA Monitor

2 objects

#	NAME
1	sla-outside1
2	sla-outside2

Name: sla-outside1

Description:

Monitor Address: OutsideToSP1_192.168.10.3

Target Interface: outside (GigabitEthernet0/0)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold: 5000 milliseconds (0 - 2147483647)

Timeout: 5000 milliseconds (0 - 604800000)

Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)

Type of Service: 0 (0 - 255)

Number of Packets: 1 (0 - 100)

Data Size: 28 bytes (0 - 16384)

CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

Object Types

SLA Monitor

2 objects

#	NAME
1	sla-outside1
2	sla-outside2

Name: sla-outside2

Description:

Monitor Address: Outside2ToSP2_192.168.20.4

Target Interface: outside2 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold: 5000 milliseconds (0 - 2147483647)

Timeout: 5000 milliseconds (0 - 604800000)

Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)

Type of Service: 0 (0 - 255)

Number of Packets: 1 (0 - 100)

Data Size: 28 bytes (0 - 16384)

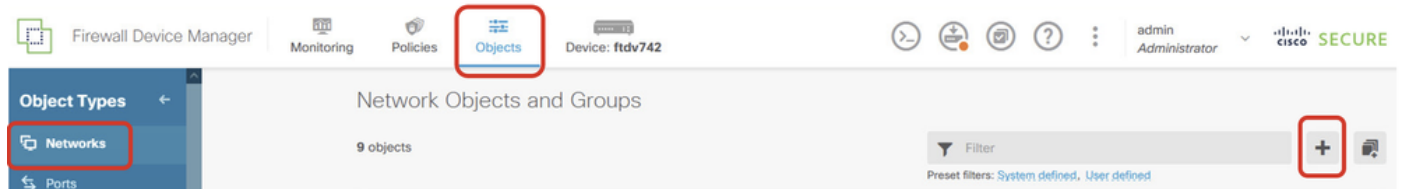
CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

靜態路由上的配置

站點1 FTD靜態路由配置

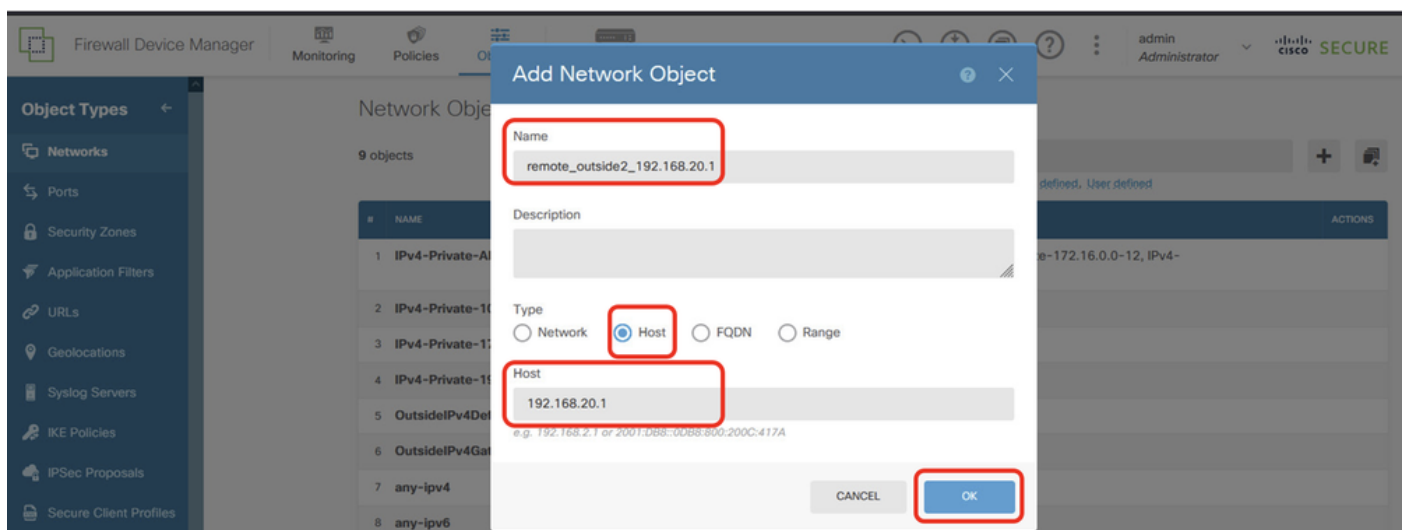
步驟22.為Site1 FTD建立將由靜態路由使用的新網路對象。導航到Objects > Networks，單擊+按鈕。



Site1FTD_Create_Obj

步驟22.1.為對等Site2 FTD的outside2 IP地址建立對象。提供必要資訊。按一下「OK」按鈕。

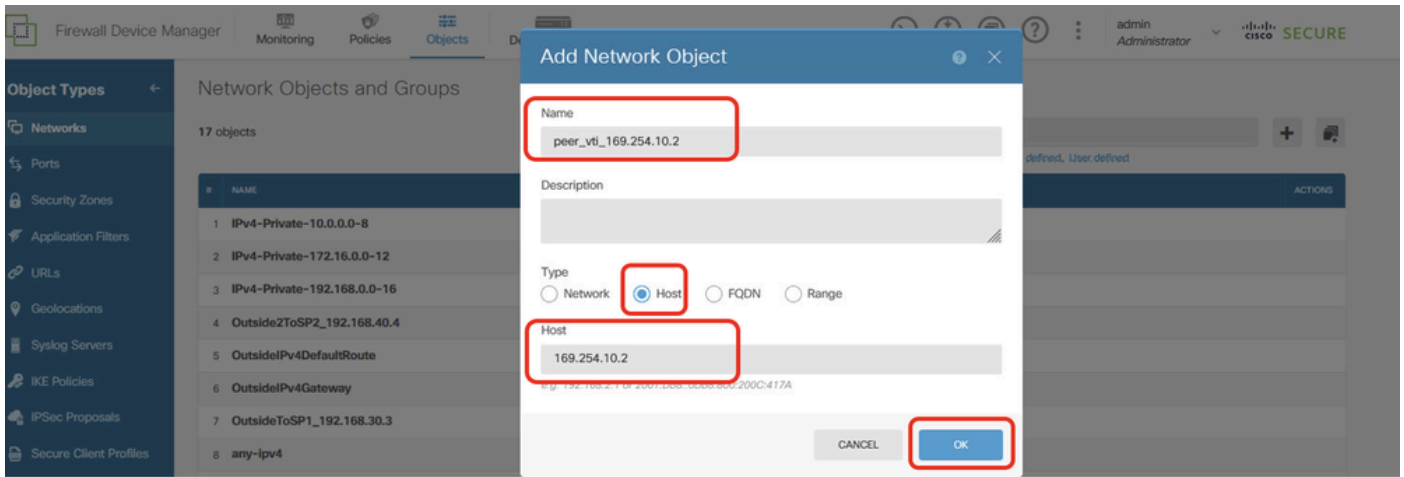
- 名稱:remote_outside2_192.168.20.1
- Type:主機
- 網路：192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

步驟22.2.為對等點Site2 FTD的VTI Tunnel1 IP位址建立對象。提供必要資訊。按一下「OK」按鈕。

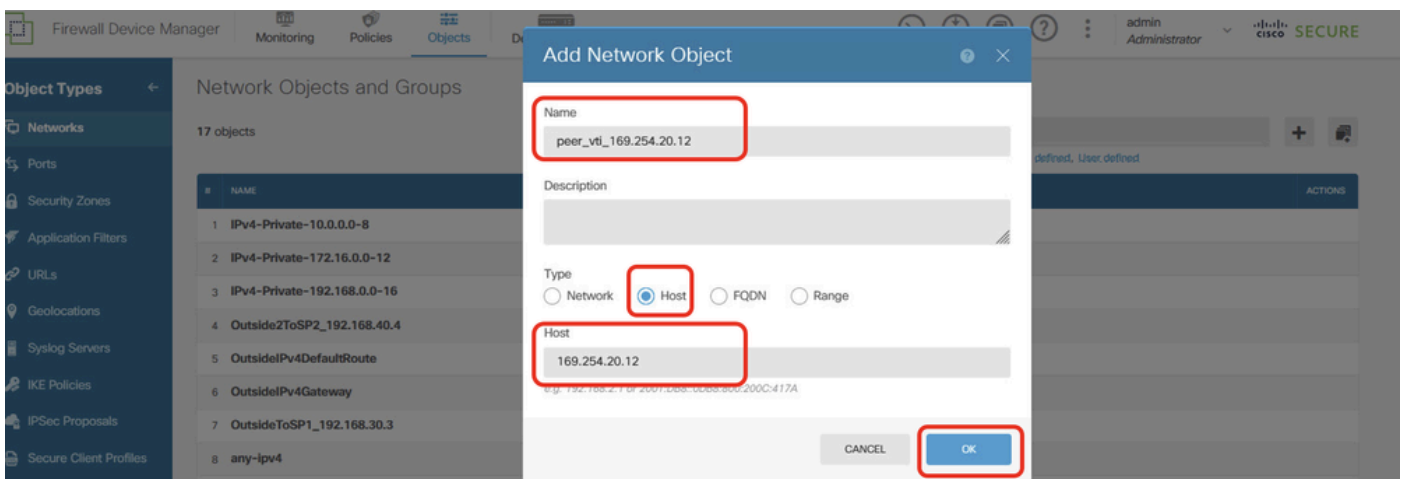
- 名稱:peer_vti_169.254.10.2
- Type:主機
- 網路：169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

步驟22.3.為對等點Site2 FTD的VTI隧道2 IP地址建立對象。提供必要資訊。按一下「OK」按鈕。

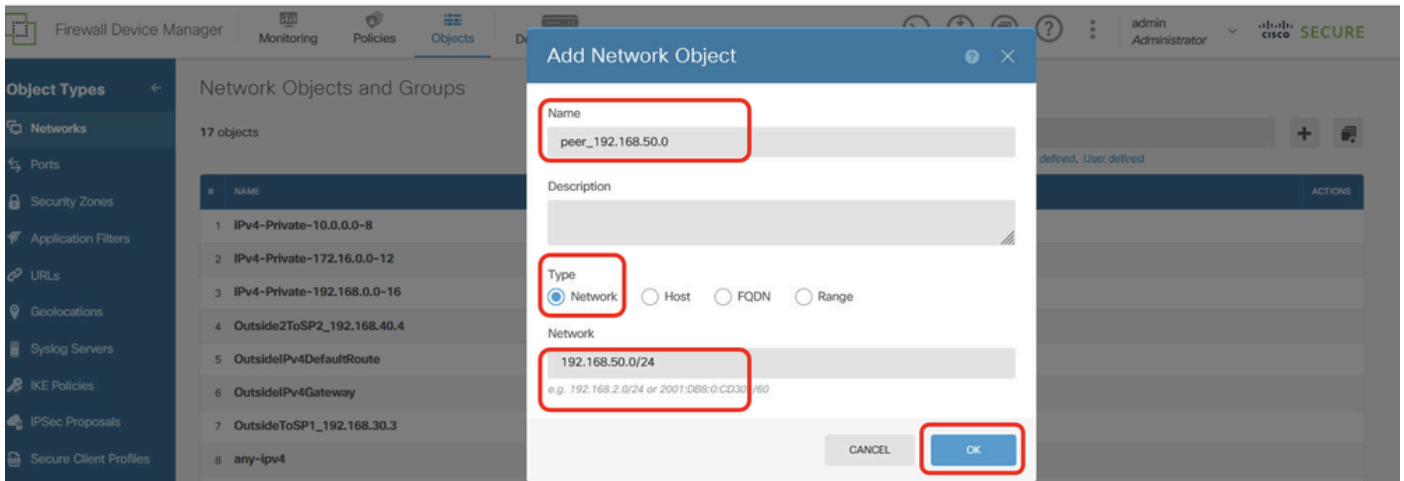
- 名稱:peer_vti_169.254.20.12
- Type:主機
- 網路 : 169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

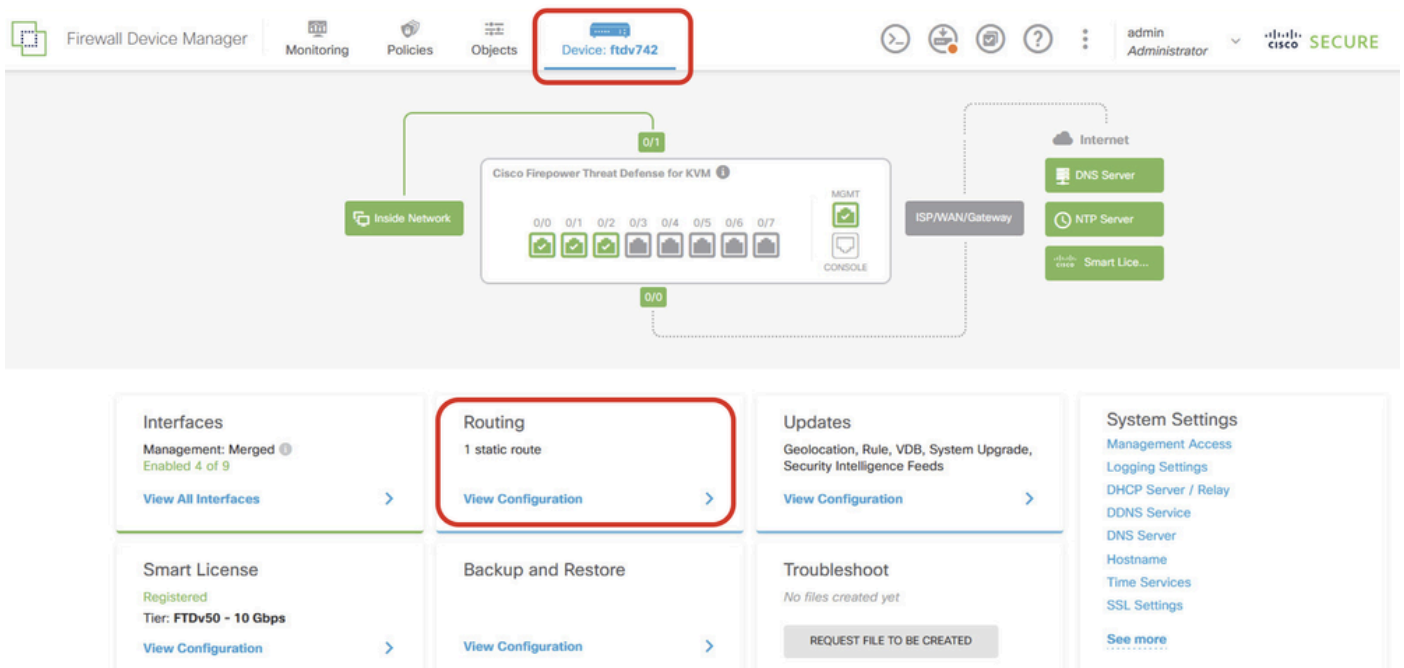
步驟22.4.為對等體Site2 FTD的內部網路建立對象。提供必要資訊。按一下「OK」按鈕。

- 名稱:peer_192.168.50.0
- Type:網路
- 網路 : 192.168.50.0/24

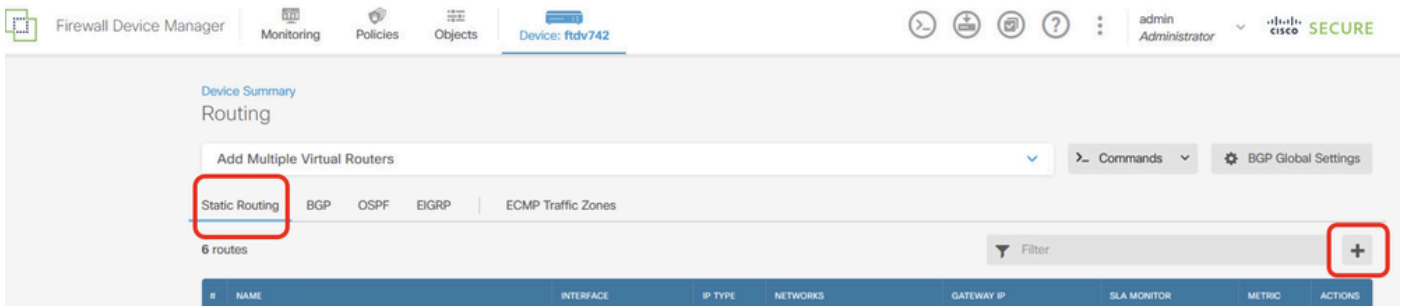


Site1FTD_Create_NetObj_StaticRoute_4

步驟23.導覽至Device > Routing。按一下「View Configuration」。按一下Static Routing頁籤。按一下+按鈕新增新的靜態路由。



Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

步驟23.1.使用具有SLA監控的ISP1網關建立預設路由。如果ISP1網關發生中斷，流量會通過ISP2切換到備用預設路由。ISP1恢復後，流量會恢復為使用ISP1。請提供必要的資訊。按一下

OK按鈕進行儲存。

- 名稱:到SP1GW
- Interface:outside(GigabitEthernet0/0)
- 通訊協定：IPv4
- 網路：any-ipv4
- 網關：OutsideToSP1_192.168.30.3
- 指標：1
- SLA監控：sla-outside

Add Static Route



Name

ToSP1GW

Description

Interface

outside (GigabitEthernet0/0)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

OutsideToSP1_192.168.30.3

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

步驟23.2.通過網關ISP2網關建立備用預設路由。指標必須大於1。在本例中，指標為2。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱:DefaultToSP2GW
- Interface:outside2(GigabitEthernet0/1)
- 通訊協定：IPv4
- 網路：any-ipv4
- 網關：Outside2ToSP2_192.168.40.4
- 指標：2

Add Static Route



Name

DefaultToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

Outside2ToSP2_192.168.40.4

Metric

2

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

步驟23.3.為通過ISP2網關且具有SLA監控的對等Site2 FTD的outside2 IP地址的目標流量建立靜態路由，用於與Site2 FTD的outside2建立VPN。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱:SpecificToSP2GW
- Interface:outside2(GigabitEthernet0/1)
- 通訊協定：IPv4
- 網路：remote_outside2_192.168.20.1
- 網關：Outside2ToSP2_192.168.40.4
- 指標：1
- SLA監控：sla-outside2

Add Static Route



Name

SpecificToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



remote_outside2_192.168.20.1

Gateway

Outside2ToSP2_192.168.40.4

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

步驟23.4.為通過站點2 FTD的對等VTI隧道1作為網關到達對等Site2 FTD的內部網路的目的地流量建立靜態路由，並使用SLA監控來加密通過隧道1的客戶端流量。如果ISP1網關遇到中斷，VPN流量會切換到ISP2的VTI隧道2。一旦ISP1恢復，流量將恢復到ISP1的VTI隧道1。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱:ToVTISP1
- Interface:demovti(Tunnel1)
- 通訊協定：IPv4
- 網路：peer_192.168.50.0
- 網關：peer_vti_169.254.10.2
- 指標：1
- SLA監控：sla-outside

Add Static Route



Name

ToVTISP1

Description

Interface

demovti (Tunnel1)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.10.2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

步驟23.5.為通過站點2 FTD的對等VTI隧道2作為網關到達對等站點2 FTD的內部網路的目標流量建立備份靜態路由，用於通過隧道2加密客戶端流量。將度量設定為大於1的值。在本示例中，度量為22。請提供必要信息。按一下OK按鈕進行儲存。

- 名稱:ToVTISP2_Backup
- Interface:demovti_sp2 (隧道2)
- 通訊協定：IPv4
- 網路：peer_192.168.50.0
- 網關：peer_vti_169.254.20.12
- 指標：22

Add Static Route



Name

ToVTISP2_Backup

Description

Interface

demovti_sp2 (Tunnel2)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.20.12

Metric

22

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

步驟23.6.為PBR流量建立靜態路由。通過Site2 FTD的對等VTI隧道2作為網關，通過SLA監控到Site2客戶端2的目標流量。請提供必要資訊。按一下OK按鈕進行儲存。

- 名稱:ToVTISP2
- Interface:demovti_sp2 (隧道2)
- 通訊協定：IPv4
- 網路：remote_192.168.50.10
- 網關：peer_vti_169.254.20.12
- 指標：1
- SLA監控：sla-outside2

Add Static Route



Name

ToVTISP2

Description

Interface

demovti_sp2 (Tunnel2)

Protocol

☒ IPv4

☐ IPv6

Networks



remote_192.168.50.10

Gateway

peer_vti_169.254.20.12

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

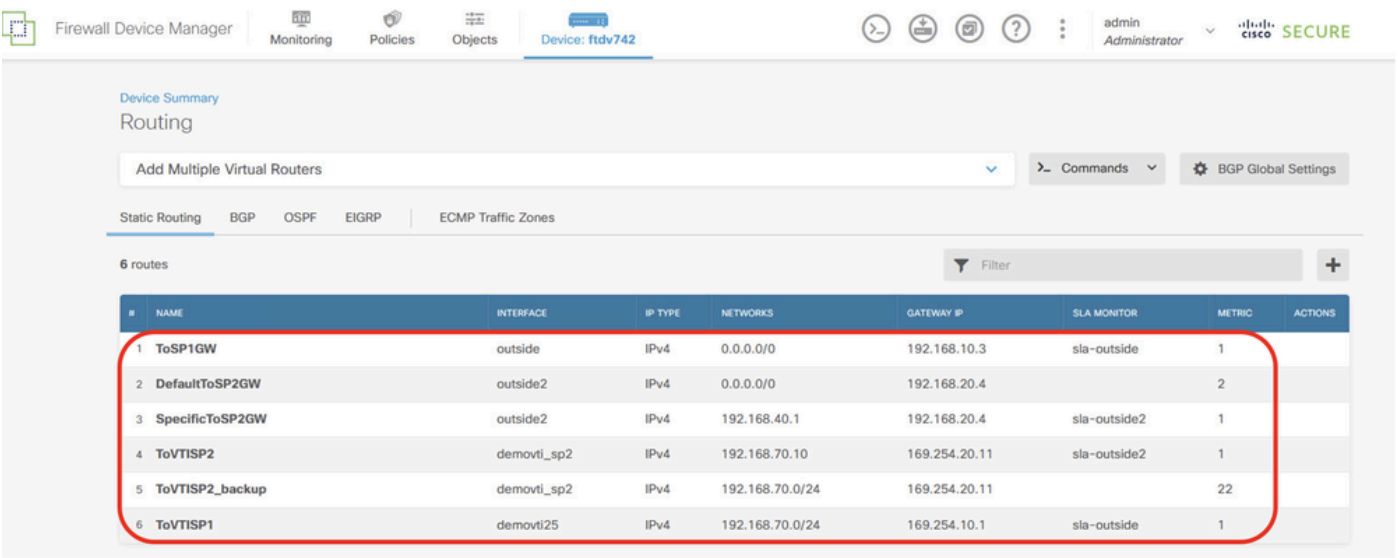
步驟24.部署配置更改。



Site1FTD_Deployment_Changes

站點2 FTD靜態路由配置

步驟25.重複步驟22到24，為Site2 FTD建立具有相應引數的靜態路由。



Site2FTD_Create_StaticRoute

驗證

使用本節內容，確認您的組態是否正常運作。透過主控台或SSH導覽至Site1 FTD和Site2 FTD的CLI。

ISP1和ISP2工作正常

VPN

//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1072332533 192.168.30.1/500	192.168.10.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
1045734377	192.168.40.1/500	192.168.20.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK		
Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d		

// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
499259237	192.168.10.1/500	192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK		
Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247		

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
477599833	192.168.20.1/500	192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK		
Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607		

路由

// Site1 FTD:

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
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S       192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA監控

// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II

Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024

Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

// Site2 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active

Enhanced History:

```
ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

```
Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Ping測試

場景1. Site1客戶端1 ping Site2客戶端1。

ping之前，請檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD。

在本範例中，Tunnel1顯示用於封裝的1497封包和用於解除封裝的1498封包。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
    #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
```

```
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1客戶端1成功ping Site2客戶端1。

```
Site1_Client1#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 = 10/97/227 ms
```

檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD after successfully。

在本範例中，通道1顯示用於封裝的1502封包和用於解除封裝的1503封包，兩個計數器增加5封包，與5個ping回應要求相符。這表示從Site1 Client1到Site2 Client1的ping是通過ISP1隧道1路由的。通道2顯示封裝或解除封裝計數器沒有增加，從而確認沒有用於此流量。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
    #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
    #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

場景2. Site1客戶端2 ping Site2客戶端2。

ping之前，請檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD。

在本範例中，Tunnel2顯示用於封裝的21個封包和用於解除封裝的20個封包。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1客戶端2成功ping Site2客戶端2。

```
Site1_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 = 4/39/87 ms
```

檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD after successfully。

在本範例中，通道2顯示26個封包進行封裝，25個封包進行解除封裝，兩個計數器增加5個封包，與5個ping回應要求相符。這表示Site1 Client2對Site2 Client2的ping是透過ISP2通道2路由的。通道1沒有顯示封裝或解除封裝計數器的增加，這確認沒有將此流量使用。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1發生中斷，而ISP2正常工作

在本示例中，手動關閉ISP1的介面E0/1以模擬ISP1遇到中斷。

```
Internet_SP1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Tunnel1發生故障。只有Tunnel2與IKEV2 SA一起處於活動狀態。

```
// Site1 FTD:
```

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel   MAC address N/A, MTU 1500
  IP address 169.254.10.1, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside   IP address: 192.168.30.1
  Destination IP address: 192.168.10.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4   IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local                                     Remote
1045734377 192.168.40.1/500                          192.168.20.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d
```

// Site2 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel   MAC address N/A, MTU 1500
  IP address 169.254.10.2, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside   IP address: 192.168.10.1
  Destination IP address: 192.168.30.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4   IPsec profile: ipsec_profile|e4084d322d
ftdv742#
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local                                     Remote
477599833 192.168.20.1/500                          192.168.40.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

路由

在路由表中，备份路由将生效。

// Site1 FTD:

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 192.168.40.4 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S       192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```


SLA監控

在Site1 FTD上，SLA監控器顯示ISP1的條目編號和超時（目標地址為192.168.30.3）855903900。

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000
```

```
Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

ftdv742# show track

Track 1

```
Response Time Reporter 855903900 reachability
Reachability is Down
7 changes, last change 00:11:03
Latest operation return code: Timeout
Tracked by:
  STATIC-IP-ROUTING 0
```

Track 2

```
Response Time Reporter 188426425 reachability
Reachability is Up
4 changes, last change 13:15:11
Latest operation return code: OK
Latest RTT (millisecs) 140
Tracked by:
  STATIC-IP-ROUTING 0
```

Ping測試

ping之前，請檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD。

在本範例中，Tunnel2顯示用於封裝的36個封包和用於解除封裝的35個封包。

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
    #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1客戶端1成功ping Site2客戶端1。

```
Site1_Client1#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 = 22/133/253 ms
```

Site1客戶端2成功ping Site2客戶端2。

```
Site1_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 = 34/56/87 ms
```

檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD afsuccessfully。

在本範例中，通道2顯示46個封包進行封裝，45個封包進行解除封裝，兩個計數器增加10個封包，與10個ping回應要求相符。這表示已透過ISP2通道2路由ping封包。

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
    #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP2發生中斷，而ISP1工作正常

在本示例中，手動關閉ISP2上的介面E0/1以模擬ISP2遇到中斷。

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

隧道2倒塌了。只有Tunnel1與IKEV2 SA一起處於活動狀態。

// Site1 FTD:

```
ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.20.11, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside2    IP address: 192.168.40.1
  Destination IP address: 192.168.20.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
1375077093	192.168.30.1/500	192.168.10.1/500
	Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
	Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc	

// Site2 FTD:

```
ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.20.12, subnet mask 255.255.255.0
Tunnel Interface Information:
```

```
Source interface: outside2    IP address: 192.168.20.1
Destination IP address: 192.168.40.1
IPsec MTU Overhead : 0
Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1025640731 192.168.10.1/500 192.168.30.1/500
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

路由

在路由表中，與ISP2相關的路由因PBR流量而消失。

// Site1 FTD:

```
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
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
C     192.168.40.0 255.255.255.0 is directly connected, outside2
L     192.168.40.1 255.255.255.255 is directly connected, outside2
S     192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C     192.168.70.0 255.255.255.0 is directly connected, inside
L     192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

```
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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

SLA監控

在Site1 FTD上，SLA監控器顯示ISP2的條目編號和超時（目標地址為192.168.40.4）188426425。

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

```
Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
```

Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10 RTTMin: 10 RTTMax: 10
NumOfRTT: 1 RTTSum: 10 RTTSum2: 100

ftdv742# show track

Track 1

Response Time Reporter 855903900 reachability
Reachability is Up
8 changes, last change 00:14:37
Latest operation return code: OK
Latest RTT (milliseconds) 60
Tracked by:
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 188426425 reachability
Reachability is Down
5 changes, last change 00:09:30
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0

Ping測試

ping之前，請檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD。

在本範例中，通道1顯示用於封裝的74個封包和用於解除封裝的73個封包。

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
    #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1客戶端1成功ping Site2客戶端1。

```
Site1_Client1#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 = 30/158/255 ms
```

Site1客戶端2成功ping Site2客戶端2。

```
Site1_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 = 6/58/143 ms
```

檢查show crypto ipsec sa的計數器 | inc interface:|encap|decap on Site1 FTD after successfully。

在本範例中，通道1顯示84個封包進行封裝，83個封包進行解除封裝，兩個計數器增加10個封包，與10個ping回應要求相符。這表示ping封包是透過ISP1通道1路由。

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
    #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
    #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。

您可以使用這些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PBR部分進行故障排除。

```
debug policy-route
```

您可以使用這些debug命令對SLA監控器部分進行故障排除。

```
ftdv742# debug sla monitor ?
error   Output IP SLA Monitor Error Messages
trace   Output IP SLA Monitor Trace Messages
```

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）。