為使用NAT的專用訪問配置使用安全FTD和ASA的安全訪問

目錄

簡介

本文說明如何使用網路位址轉譯設定安全存取網路通道群組。

必要條件

需求

思科建議您瞭解以下主題：

- 思科防火牆管理中心
- 思科安全防火牆威脅防禦
- Cisco Secure Access
- 思科調適型安全裝置
- 網路位址轉換

- 基於原則的路由
- 防火牆上的封包擷取

採用元件

本檔案中的資訊是根據：

- 思科防火牆管理中心7.10
- 思科安全防火牆威脅防禦7.10
- Cisco Secure Access
- 思科調適型安全裝置9.22
- 思科路由器

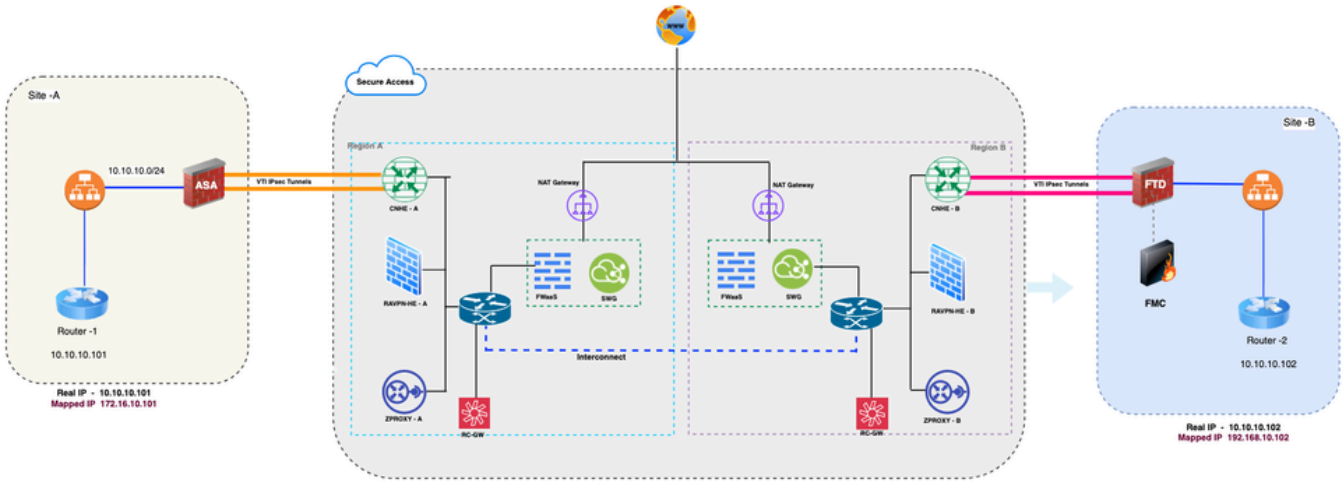
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科安全訪問提供雲原生安全服務邊緣功能，包括安全網際網路訪問(SIA)和安全私有訪問(SPA)。對於將私有應用程式訪問擴展到遠端使用者而不回程通過資料中心的組織，安全訪問使用IPsec網路隧道組(NTG)在本地網路裝置(例如思科防火牆威脅防禦(FTD)、自適應安全裝置(ASA)和思科安全訪問雲入網點(PoPs))之間建立加密隧道。

本文詳細介紹如何使用IKEv2在Cisco FTD、ASA和Cisco Secure Access之間建立基於路由的IPsec隧道，從而啟用FTD和ASA上安全訪問的網路地址轉換(NAT)和基於策略的路由(PBR)以僅引導私有訪問繫結的流量進入隧道。

網路圖表



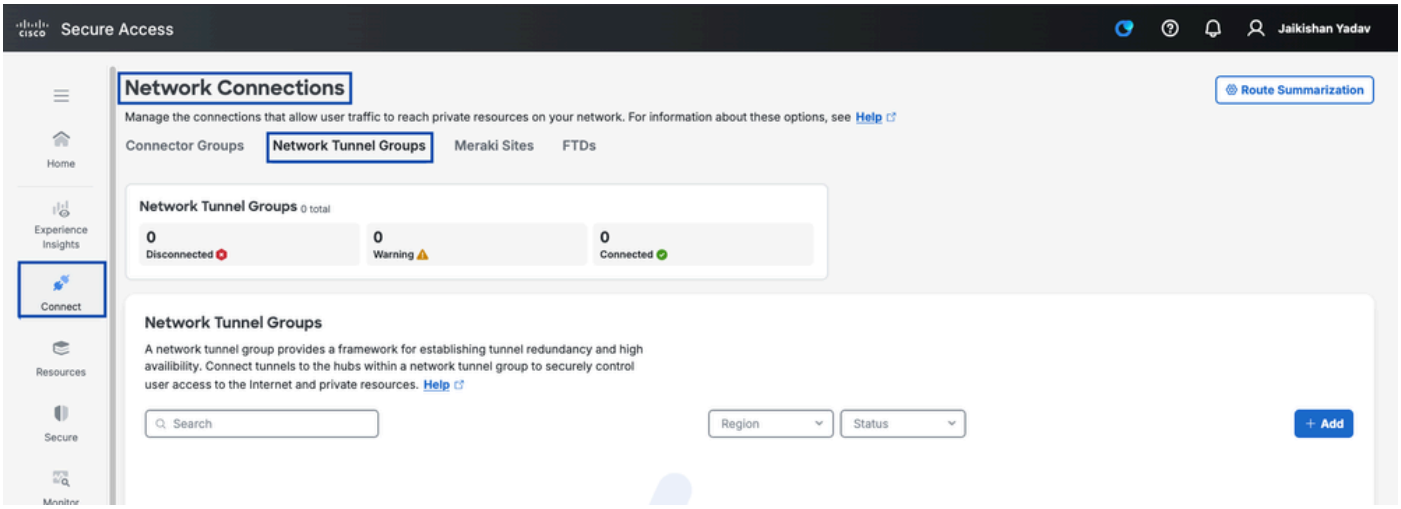
網路拓撲

設定

安全存取和安全防火牆執行緒防禦 — 含PBR的動態(BGP)路由型VPN

在安全訪問中配置網路隧道組

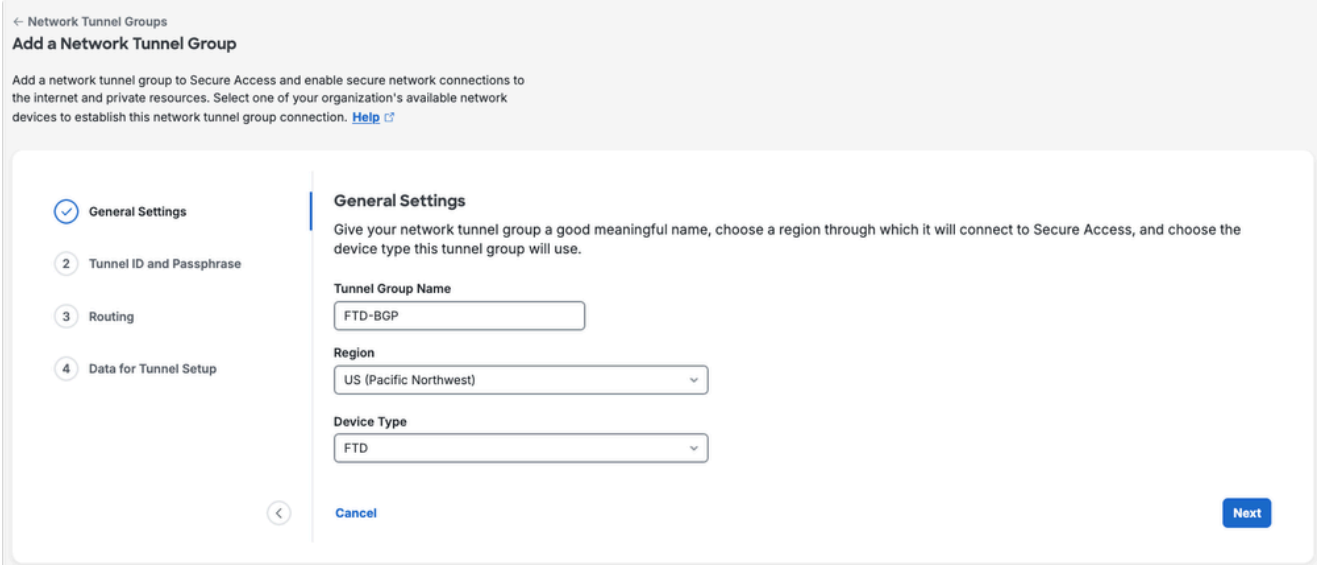
1.登入到Secure Access控制面板Secure Access
2.導覽至Connect > Network Connections > Network Tunnel Groups，然後點選+Add以配置網路隧道組



安全訪問 — 網路隧道組

3.配置網路隧道組 — 常規設定

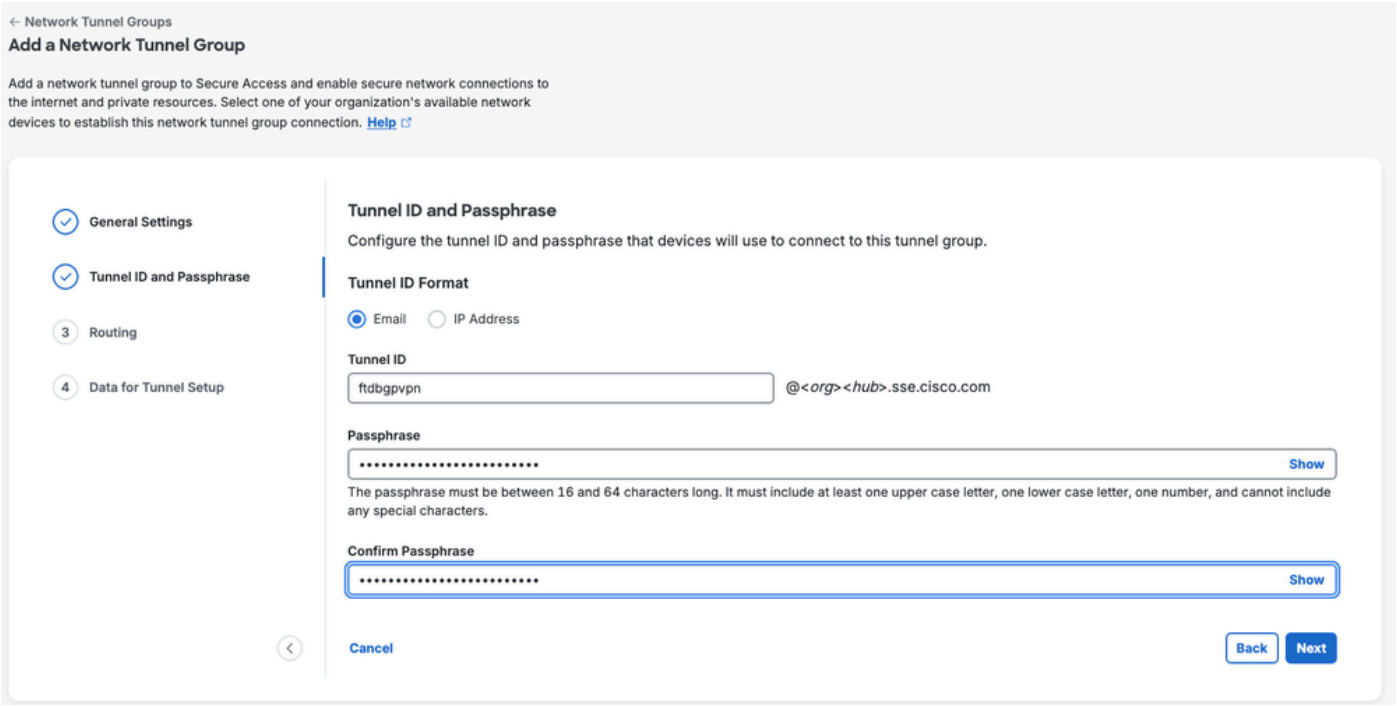
- 配置隧道組名稱、區域和設備型別
- 按一下下一步



安全訪問 — 網路隧道組常規設定

4.設定通道ID和密碼短語。

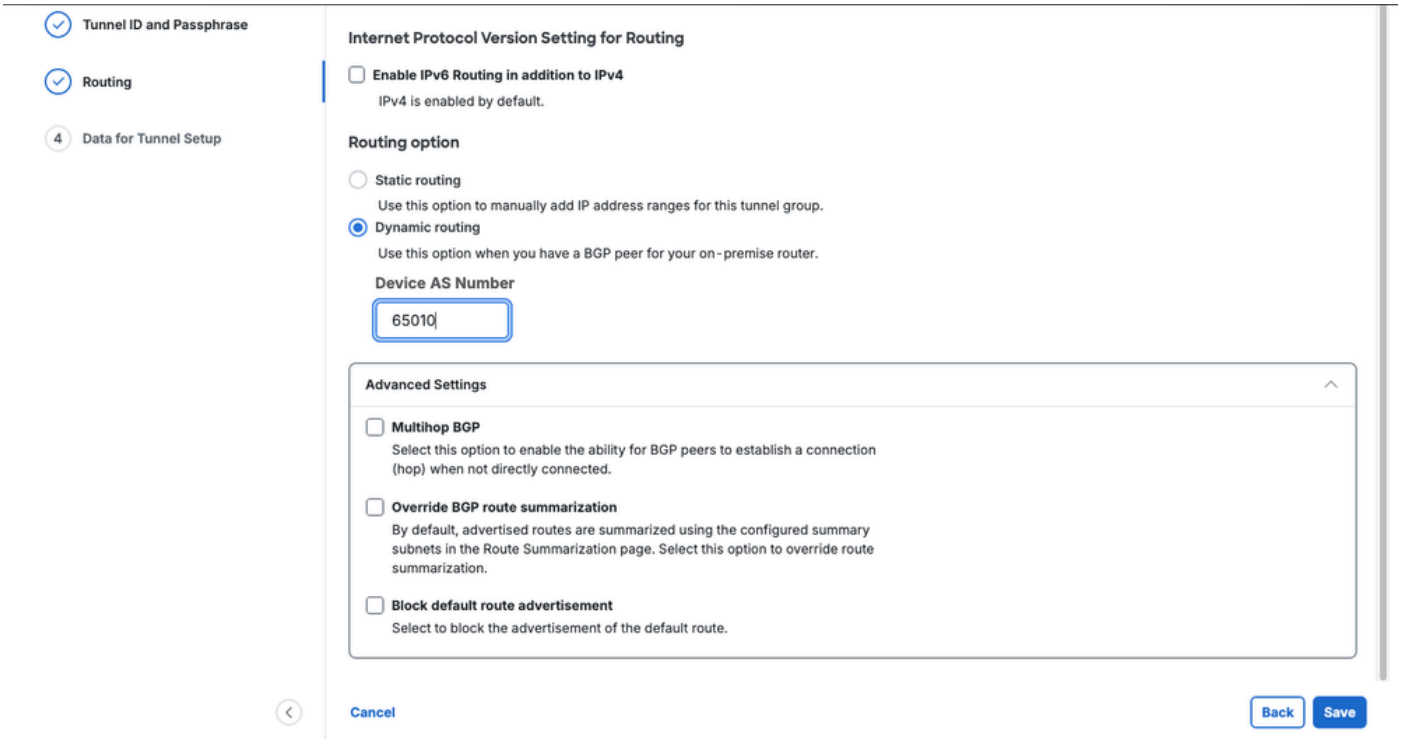
- 設定通道ID和密碼。
- 按一下「下一步」



安全存取 — 網路通道群組ID和密碼

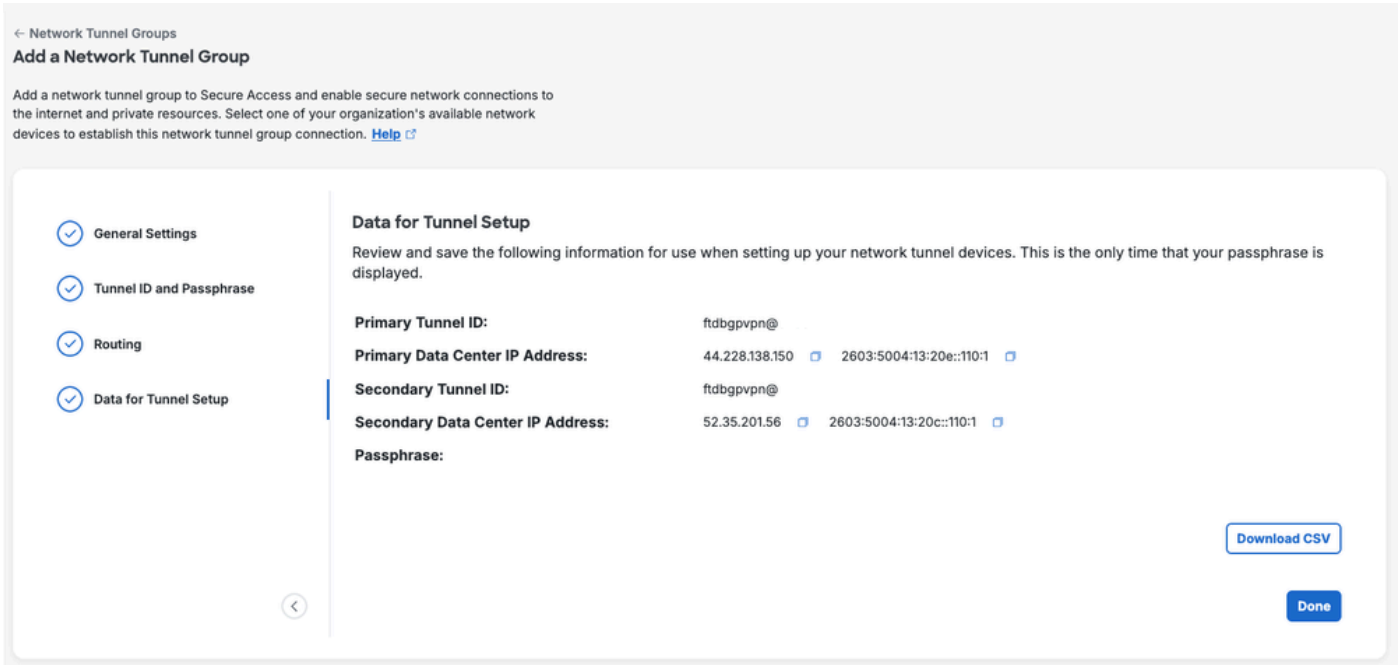
5.配置路由

- 配置裝置AS編號
- 按一下「Save」



安全存取 — 網路通道群組路由

6.儲存網路隧道組配置

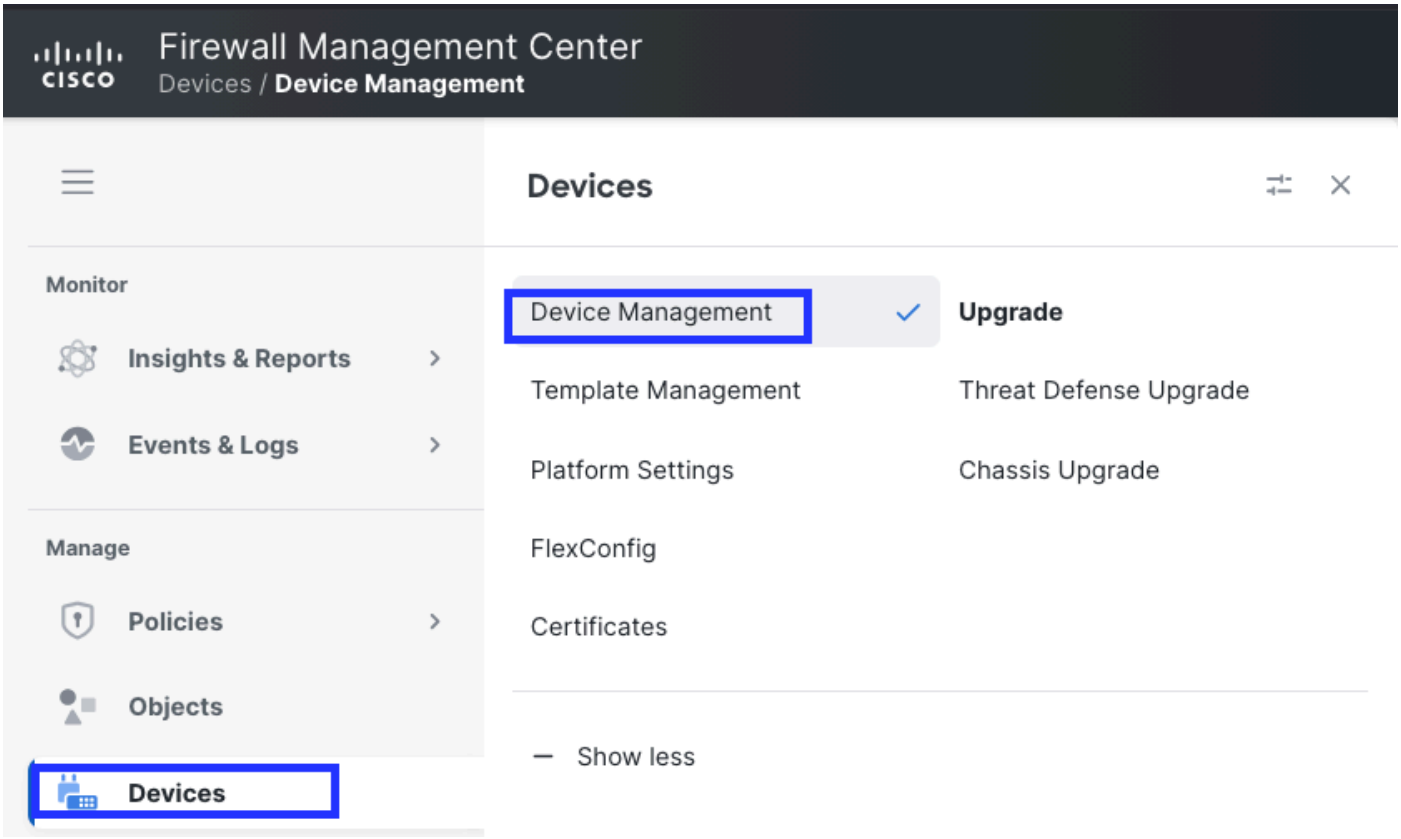


在具有PBR的安全防火牆威脅防禦(FTD)上配置基於動態路由的IPsec VPN

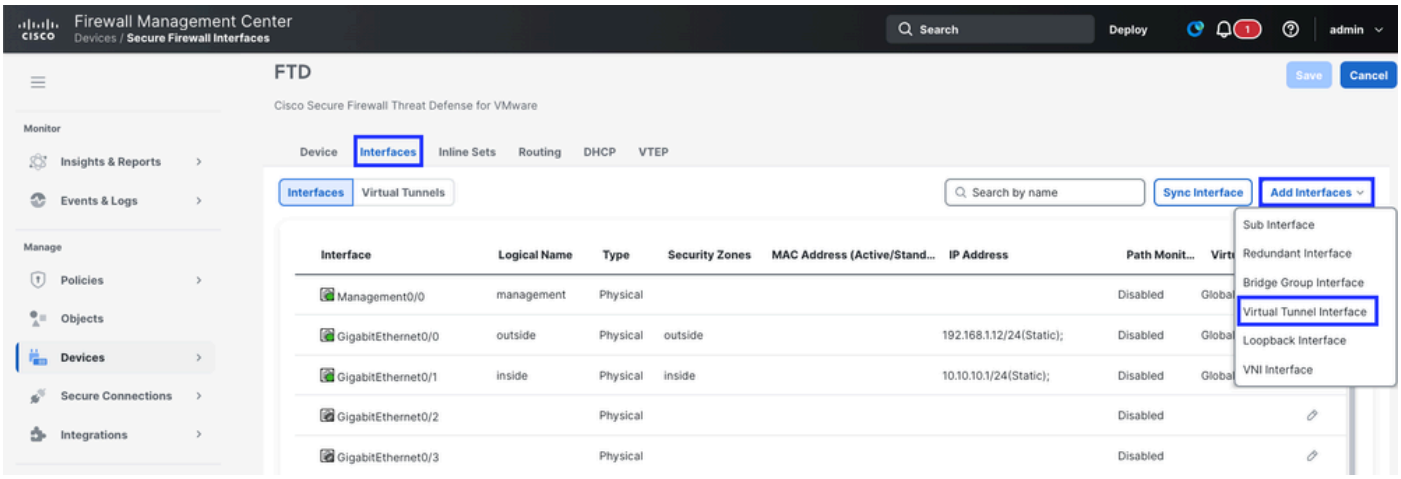
1.登入防火牆管理中心(FMC)

2.設定虛擬通道介面VTI

- 導航到Devices > Device Management



- 點選裝置旁邊的鉛筆圖示，導航至Interface部分
- 按一下Add interfaces並選擇Virtual Tunnel Interface



安全防火牆管理 — FTD VTI組態

- 設定VTI

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

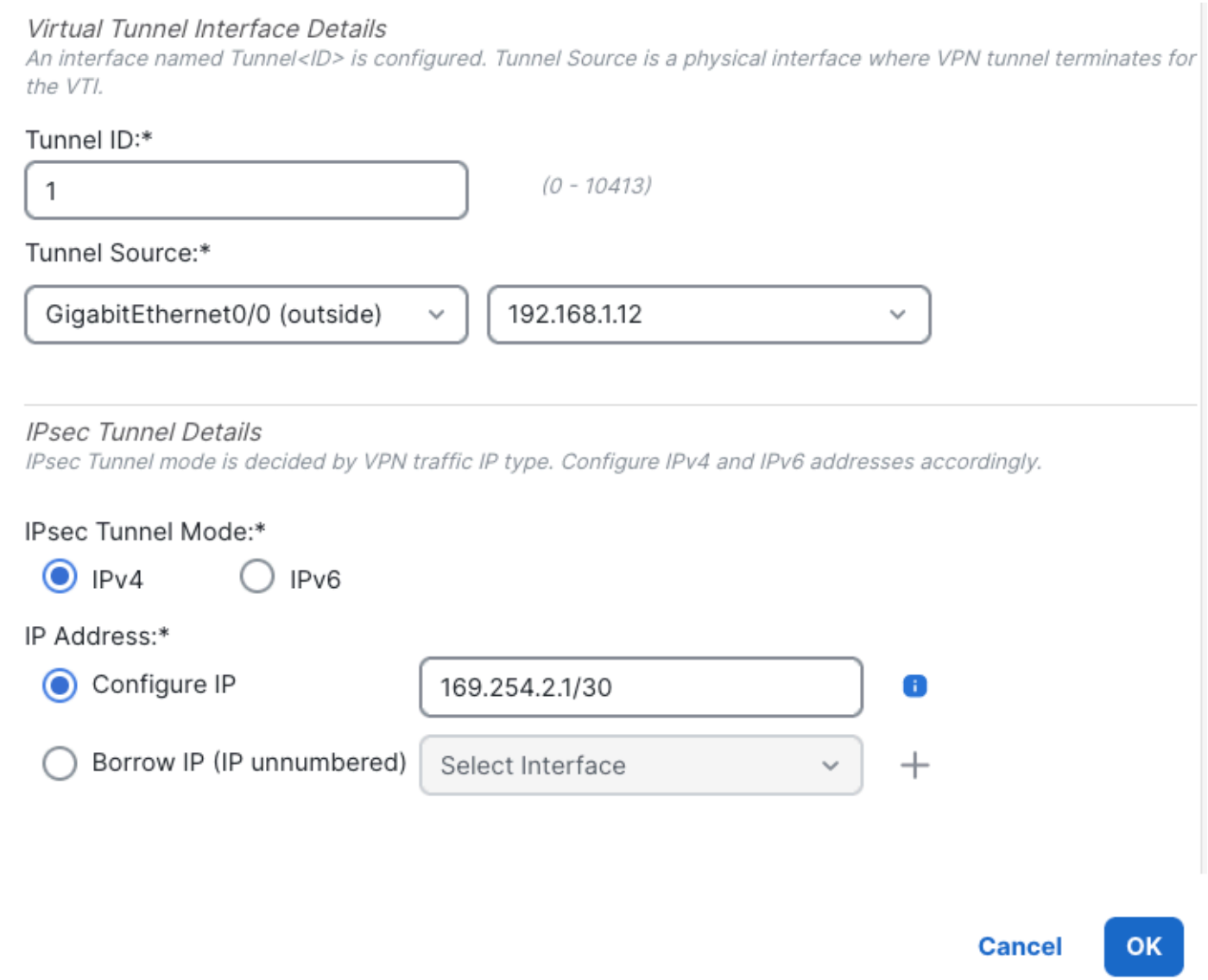
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

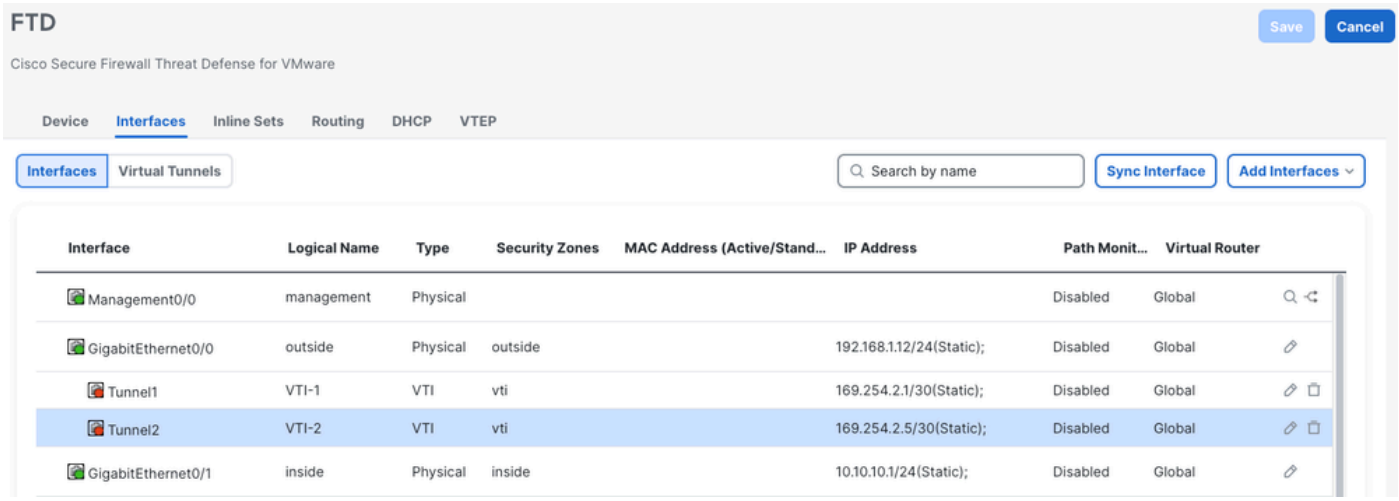
Tunnel ID:*

1 *(0 - 10413)*

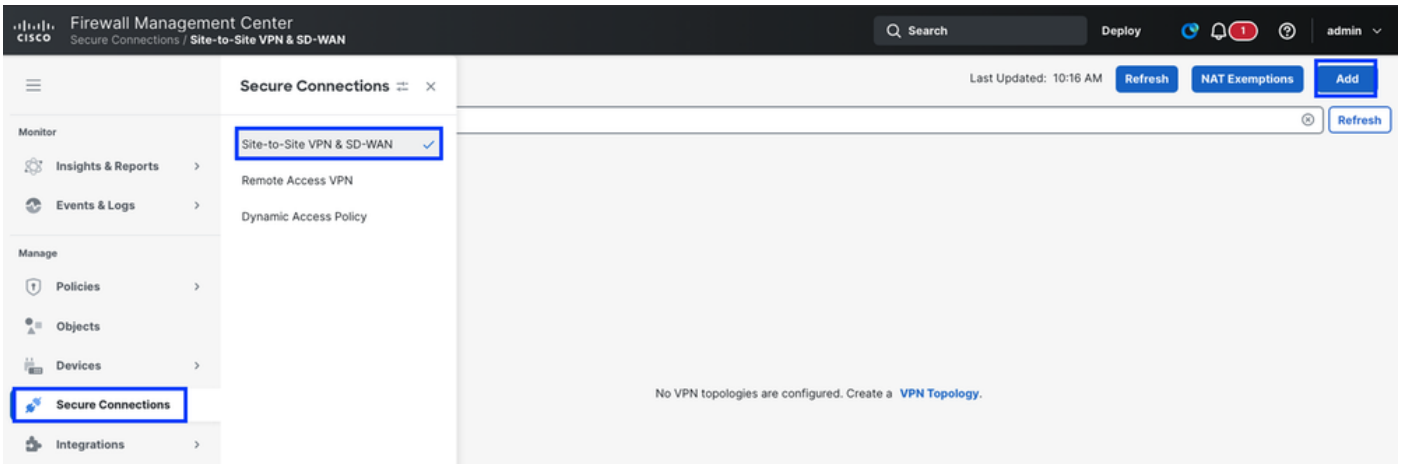


安全防火牆管理 — FTD VTI組態

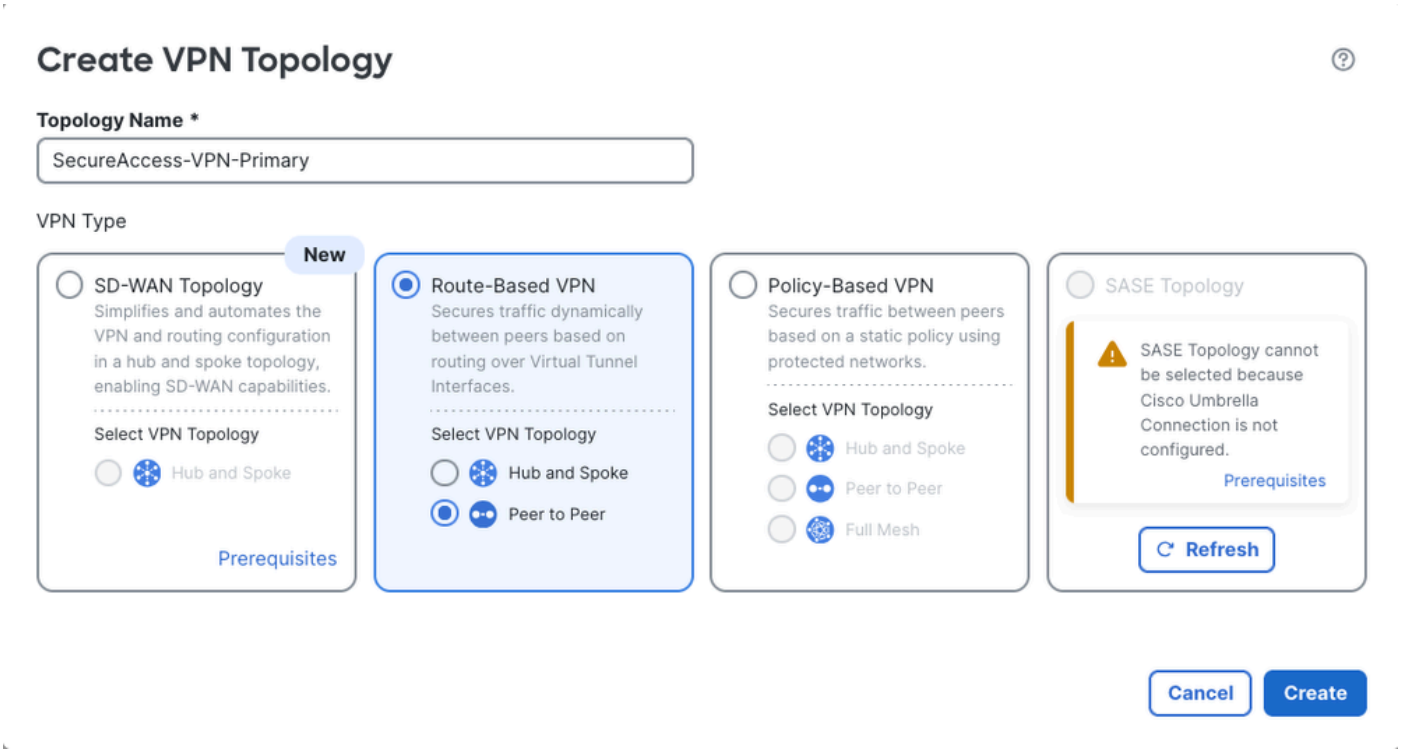
- 為具有安全訪問的輔助IPsec VPN配置VTI-2



3.導航到Secure Connections > Site-to-Site VPN & SD-WAN，然後點選Add以配置VPN

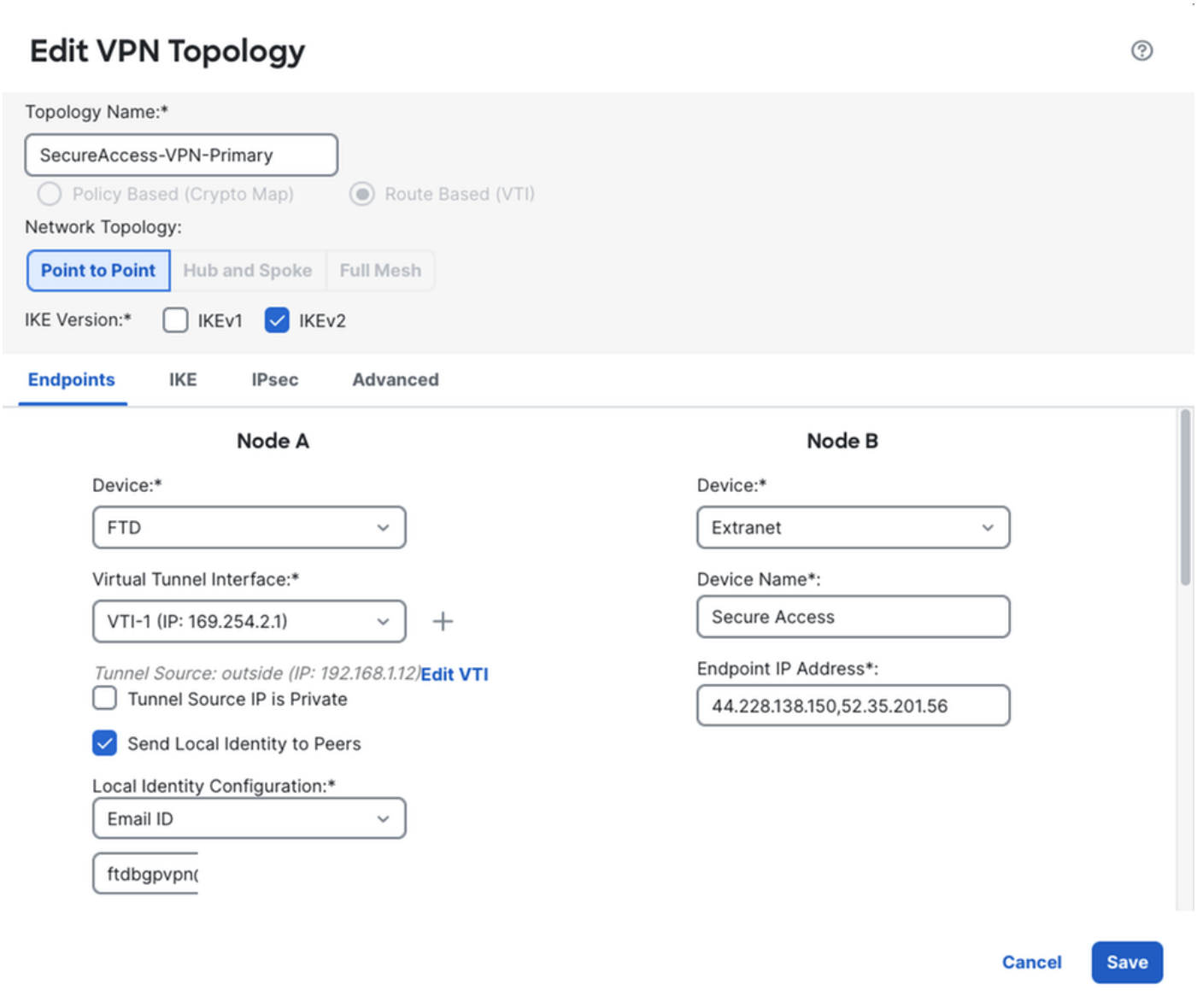


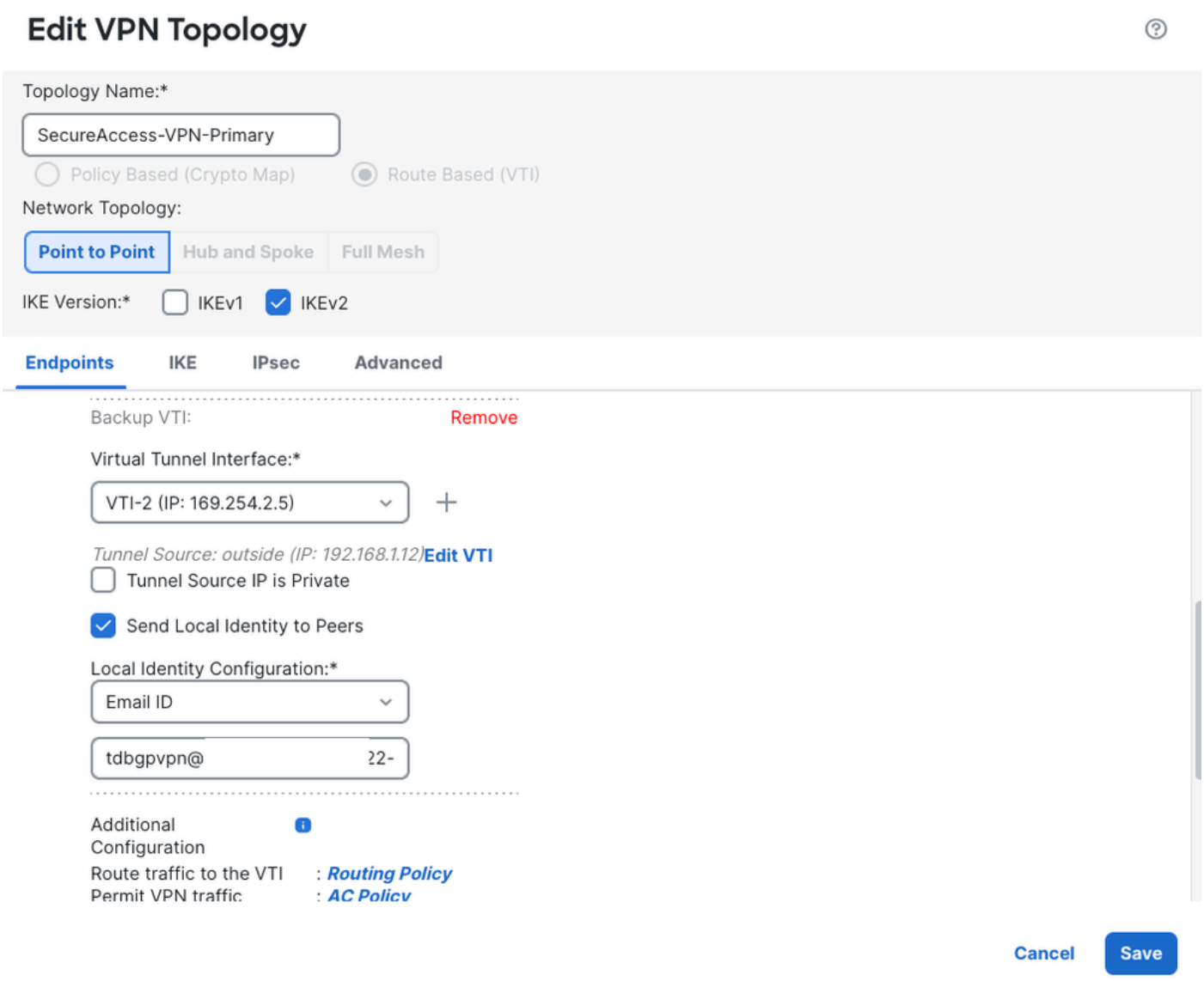
- 建立VPN拓撲



- 在安全訪問上配置網路隧道組的步驟6中，獲取主資料中心和輔助資料中心的隧道ID和IP地址。

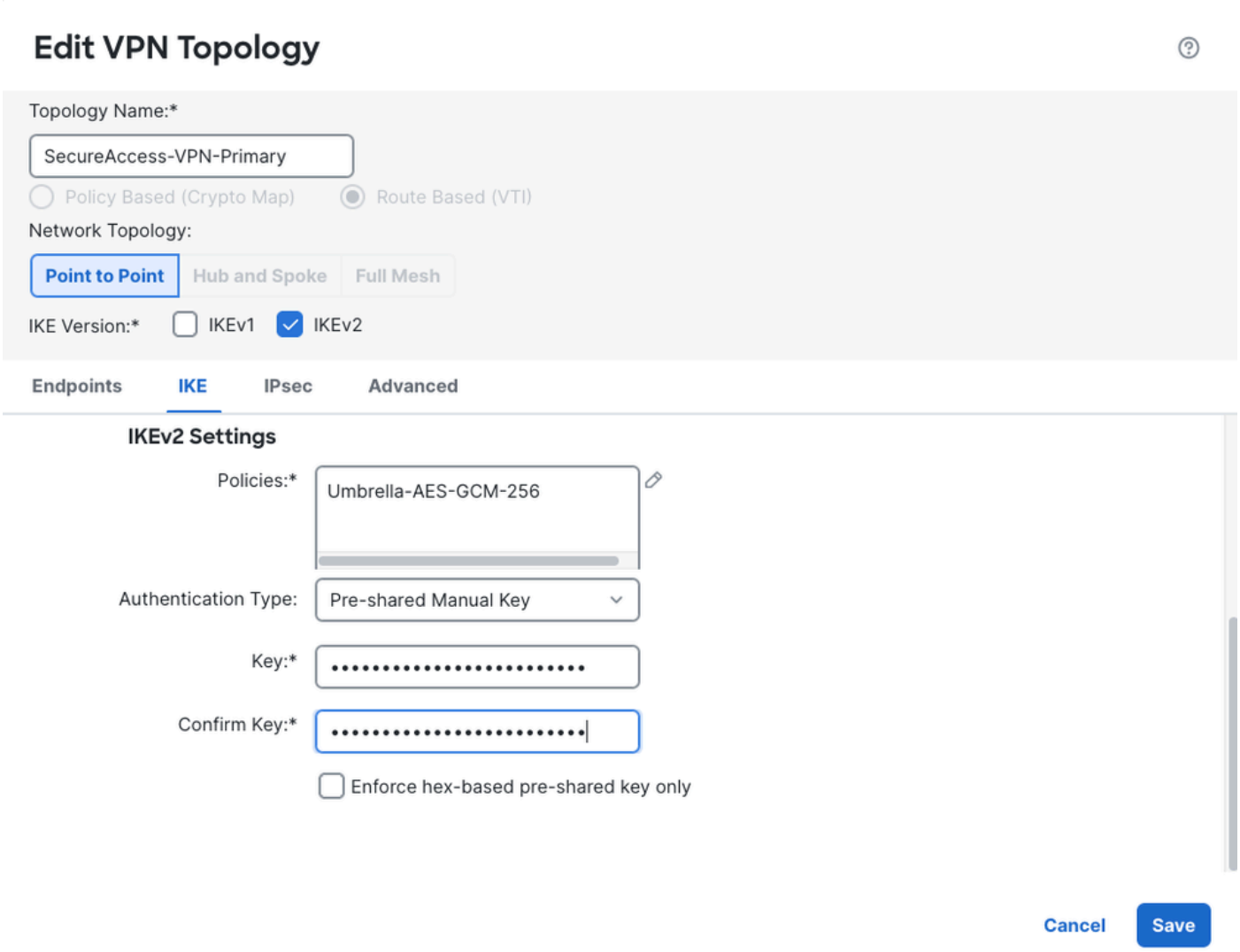
- 點選「端點」
- 在節點A下，點選裝置並選擇您的FTD裝置
- 點選Virtual Tunnel Interface並選擇上一步中建立的第一個VTI介面
- 點選Send Local Identity to Peers選項並選擇Email ID，輸入主隧道ID（從Configure Network Tunnel Group on Secure Access下的「儲存網路隧道組配置」中）
- 在Node B下，按一下Device（裝置），然後選擇Extranet
- 點選Device Name（裝置名稱），並為其指定名稱
- 點選Endpoint IP Addresses（終端IP地址），然後輸入安全訪問主和輔助IP地址（以逗號分隔）(在Configure Network Tunnel Group on Secure Access（在安全訪問中配置網路隧道組）下的Save Network Tunnel Group Configuration（儲存網路隧道組配置））
- 點選Add Backup VTI
- 點選Virtual Tunnel Interface並選擇上一步中建立的第二個VTI介面
- 點選Send Local Identity to Peers選項並選擇Email ID，輸入輔助隧道ID（從Configure Network Tunnel Group on Secure Access下的「儲存網路隧道組配置」中）
- 點選Save





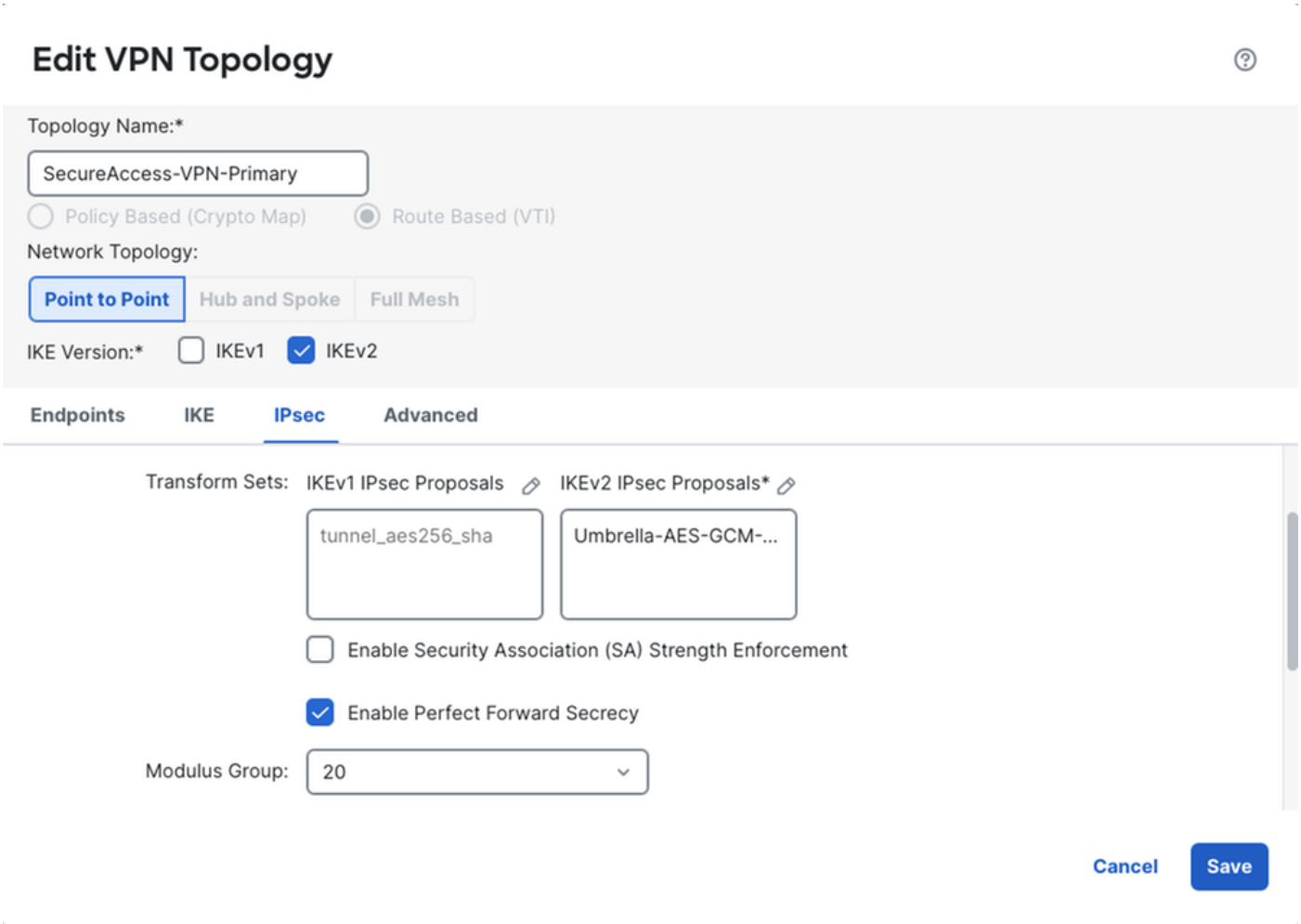
安全FTD - VPN端點組態

- 根據支援的IPsec引數配置IKEv2設定
  - 選擇Policies as Umbrella-AES-GCM-256
  - 選擇Authentication Type as Pre-Shared Manual Key



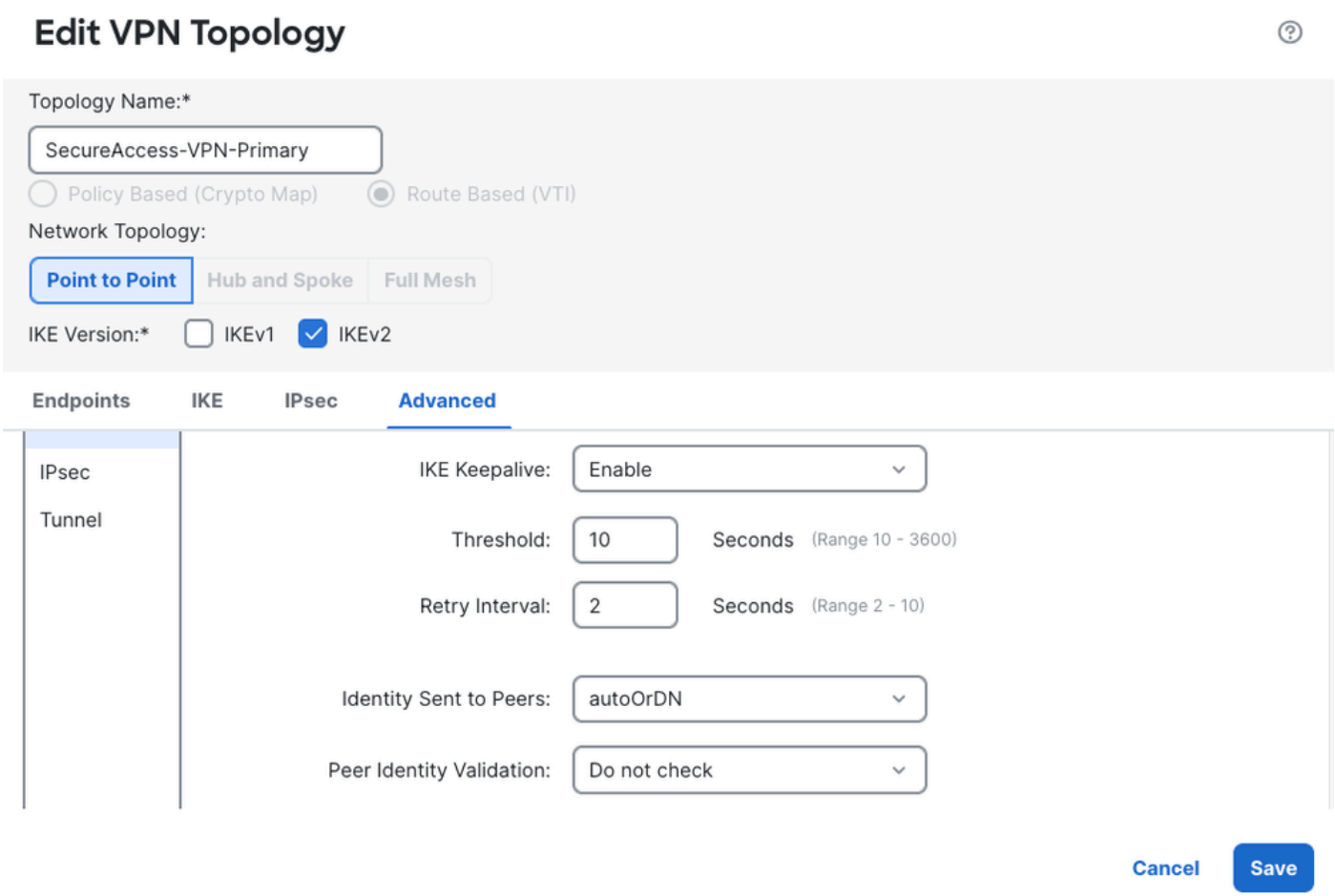
安全FTD - VPN IKE設定

- 配置IPsec設定
  - 選擇IKEv2 IPsec Proposals作為Umbrella-AES-GCM-256
  - 啟用PFS作為選擇模陣列作為20



安全FTD - VPN IPsec設定

- 高級設定
- 按一下「Save」



安全FTD - VPN高級設定

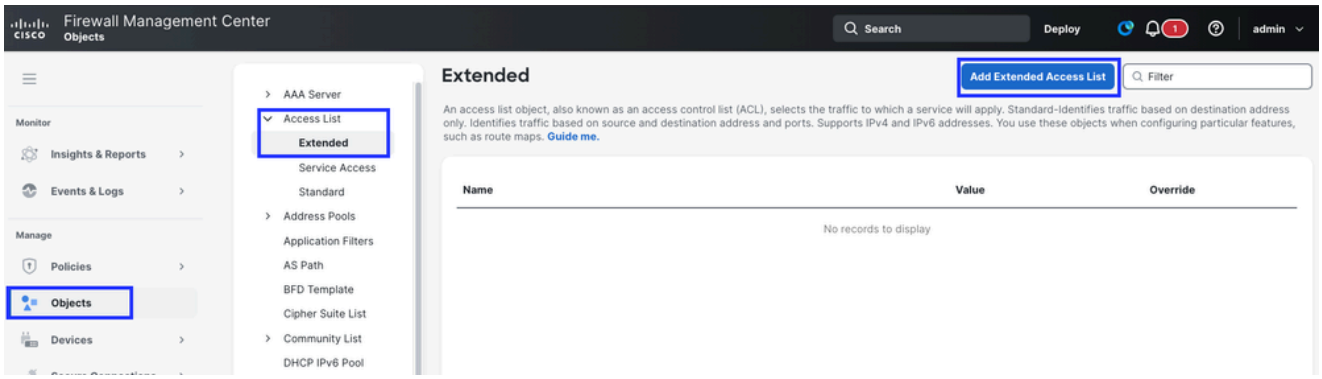
FTD原則型路由

在傳統路由中，資料包根據目的IP地址進行路由。在基於目的地的路由系統中更改特定流量的路由很困難。基於策略的路由(PBR)擴展並補充了路由協定提供的機制，讓您能夠更好地控制路由。

PBR允許您設定IP優先順序。此功能也允許您為特定流量（例如透過高成本連結的優先流量）指定路徑。使用PBR，您可以根據目標網路以外的標準（如源埠、目標地址、目標埠、協定、應用程式或這些對象的組合）來定義路由。如需詳細資訊，請參閱基於原則的路由

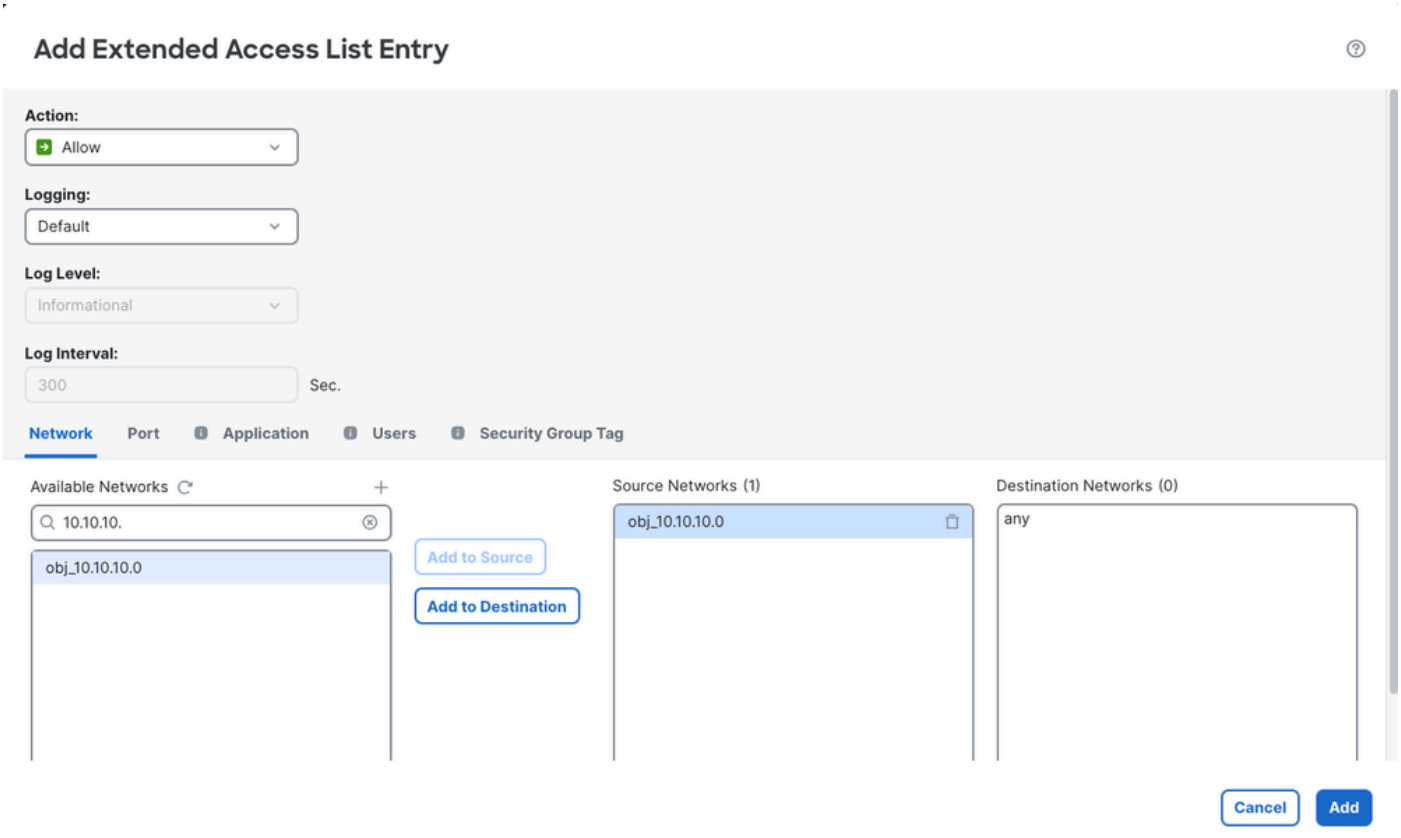
1.配置訪問清單

- 導航到對象>訪問清單>擴展
- 按一下Add Extended Access List

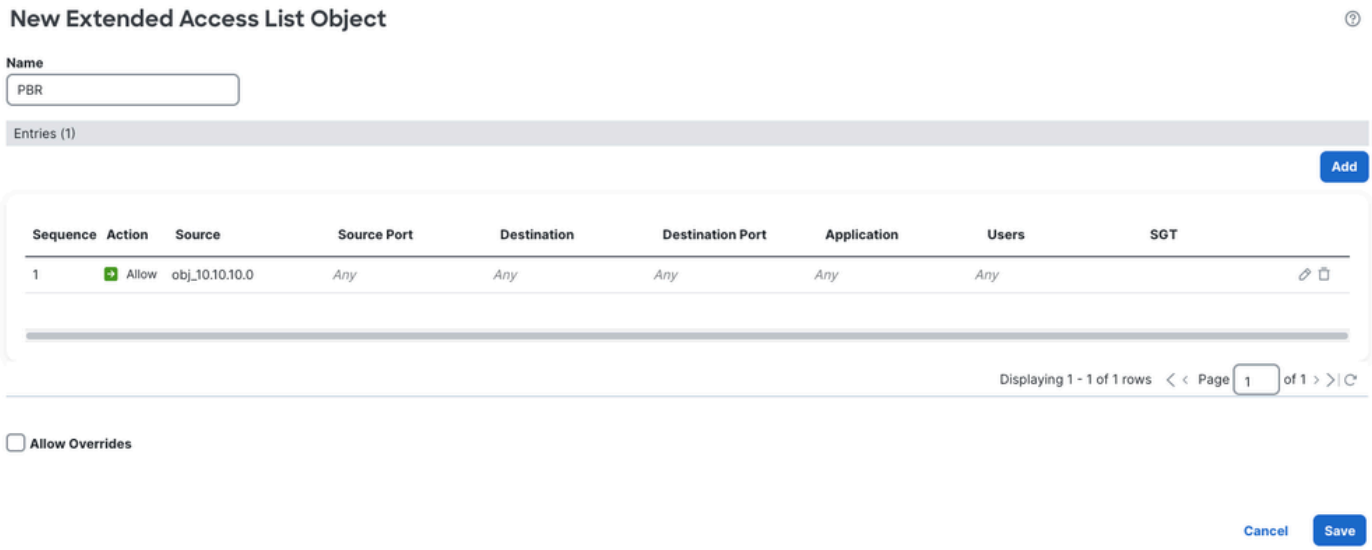


安全FTD — 擴充存取清單

- 提供訪問清單名稱
- 定義操作
  - 允許. — 定義的流量將傳送到IPsec隧道
  - 阻止 — 流量將繞過來自IPsec隧道的流量
  - 將根據序列號（從低到高）匹配規則
  - 按一下Add
  - 按一下「Save」



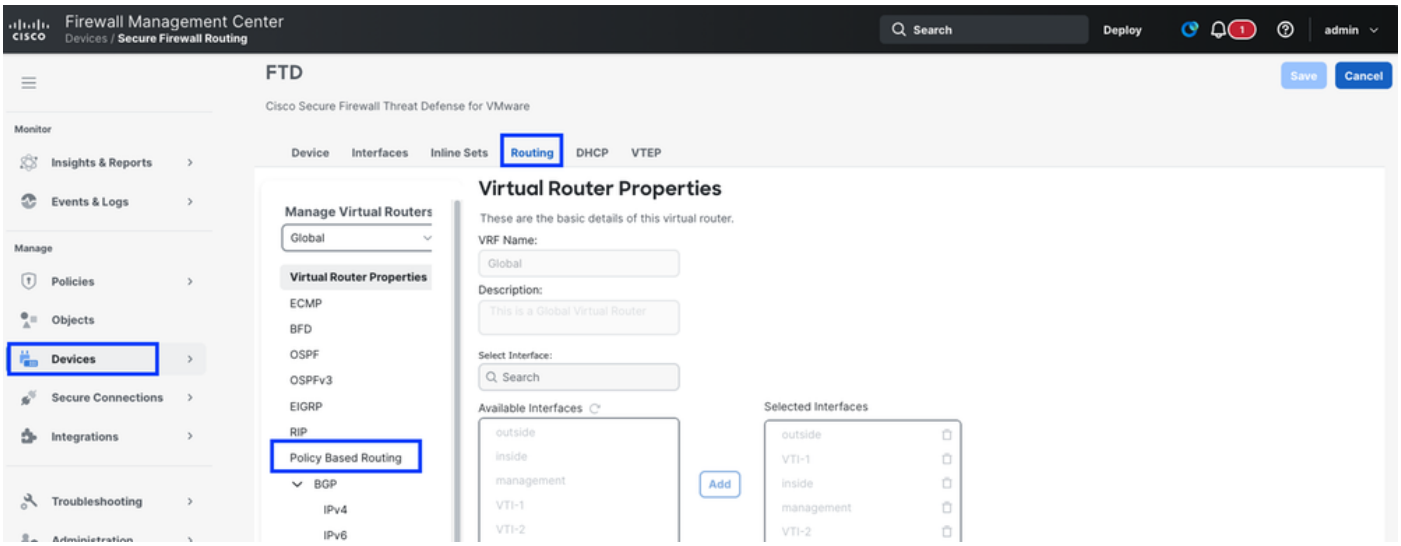
安全FTD — 擴充存取清單



安全FTD — 擴充存取清單

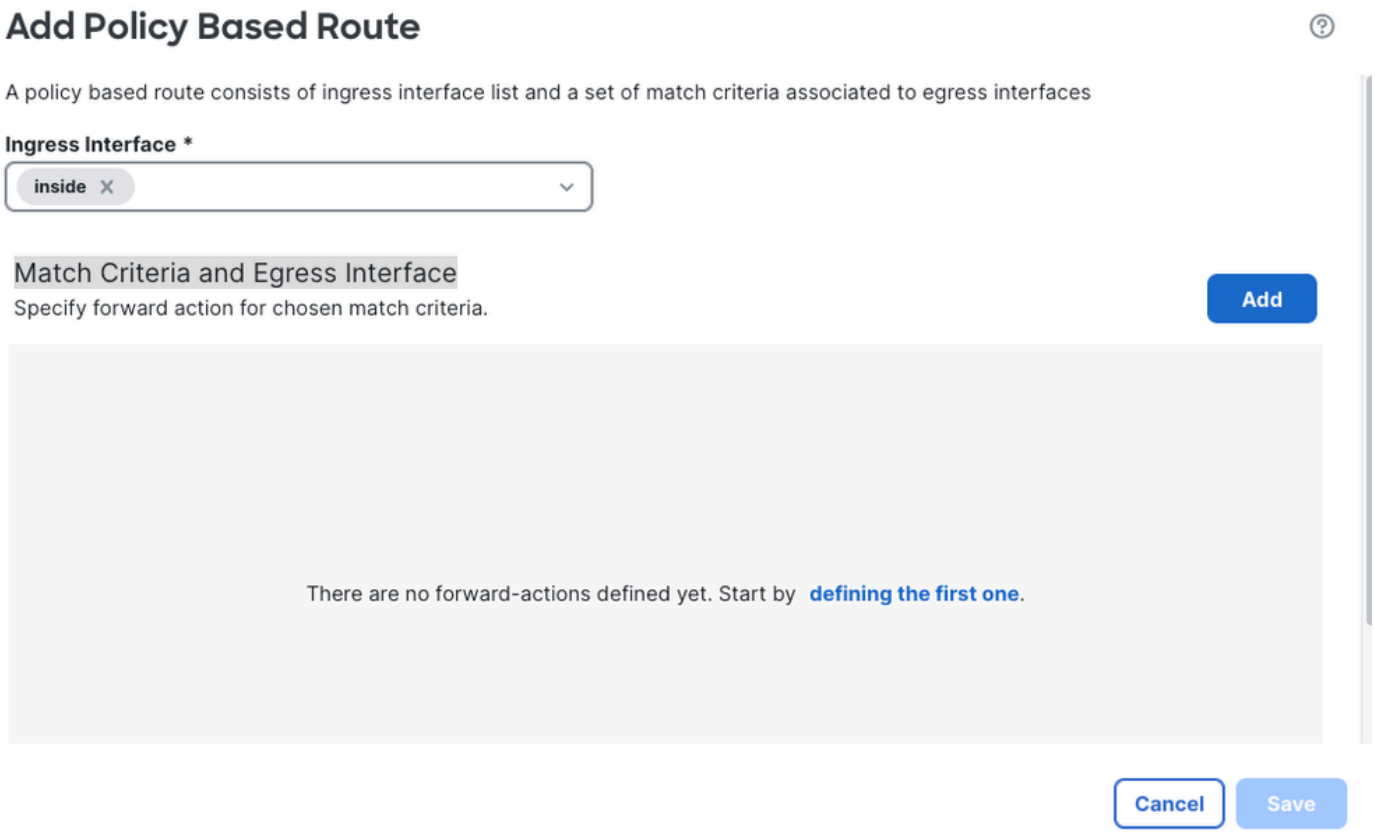
2.配置基於策略的路由

- 導覽至Devices > Device Management > FTD > Routing



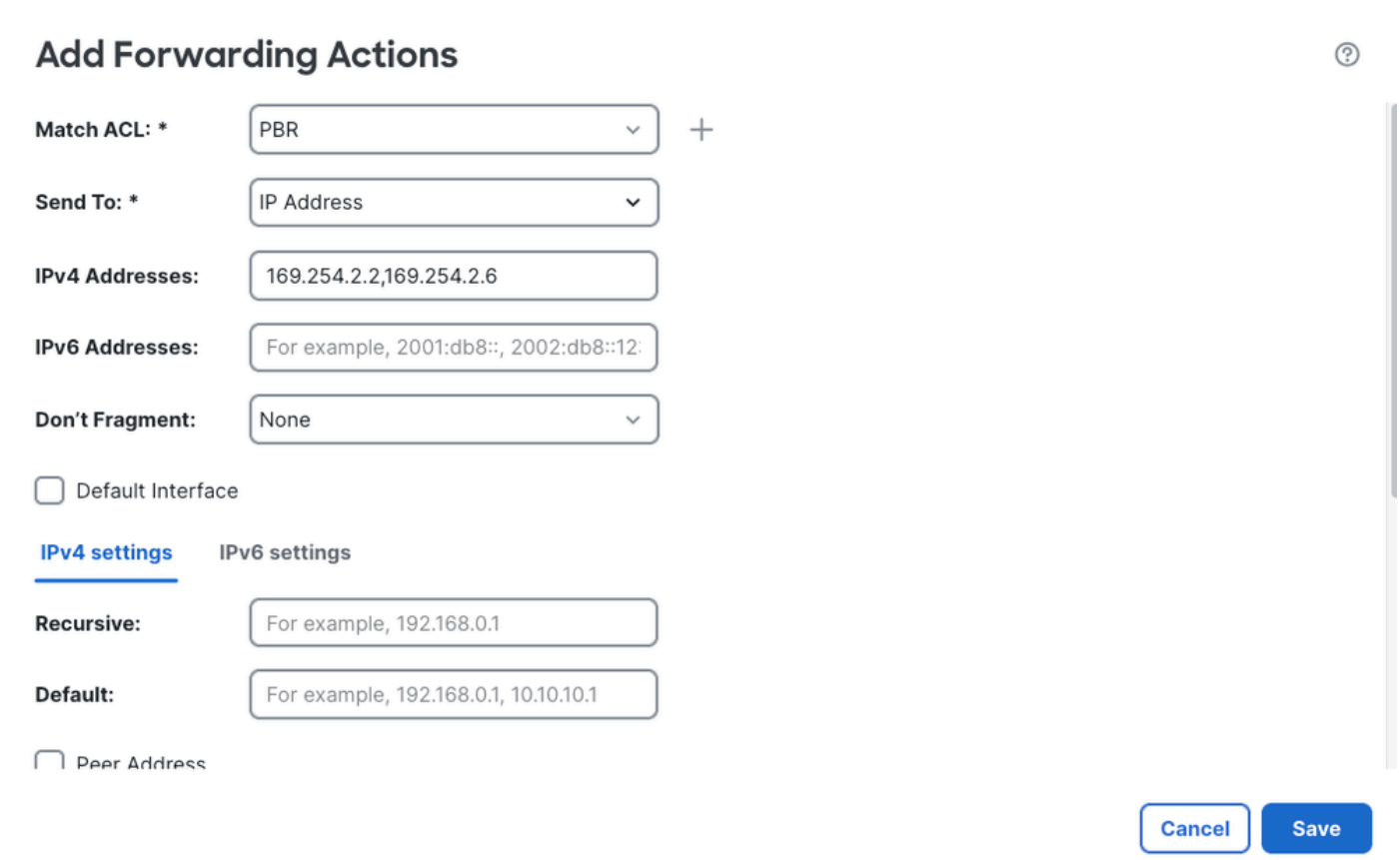
安全FTD — 基於原則的路由

- 點選Add
- 為我們在訪問清單中定義的子網選擇Ingress Interface - Ingress interface

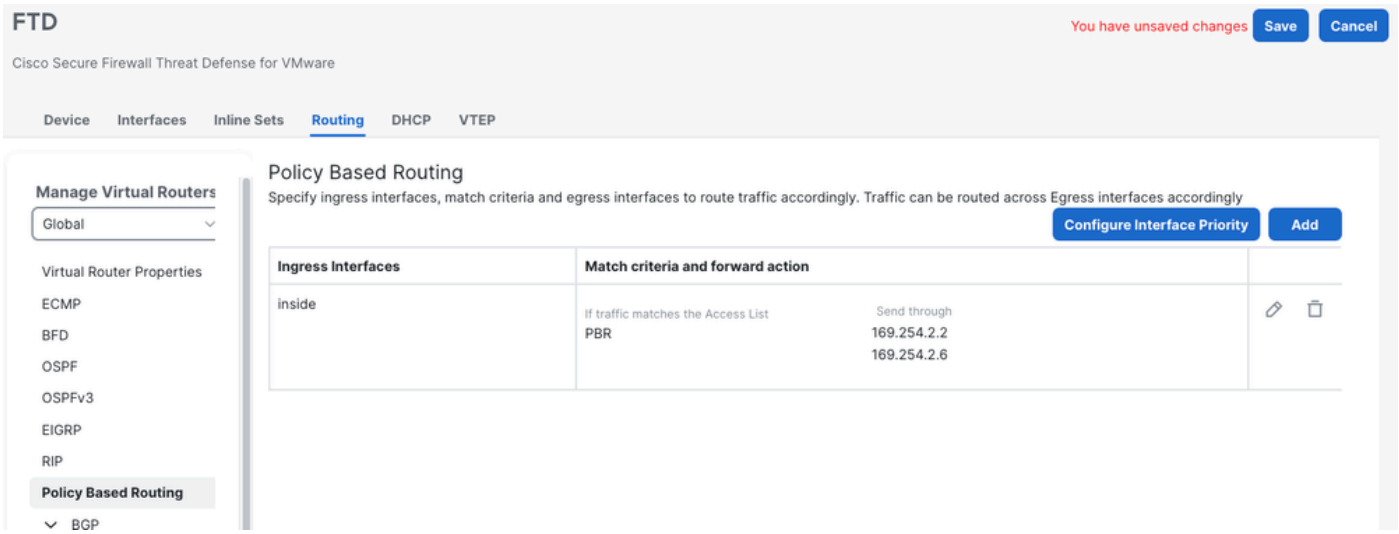


安全FTD — 基於原則的路由

- 定義匹配條件和輸出介面
  - 按一下Add
  - 選擇Match ACL
  - 選擇Send to as IP address
  - 新增下一跳IP地址。- VTI介面IP地址為。169.254.2.130和。169.254.2.5/30。因此，VTI-1和VTI-2的下一跳IP地址將是169.254.2.2和。169.254.2.6
  - 按一下Save



安全FTD — 基於原則的路由

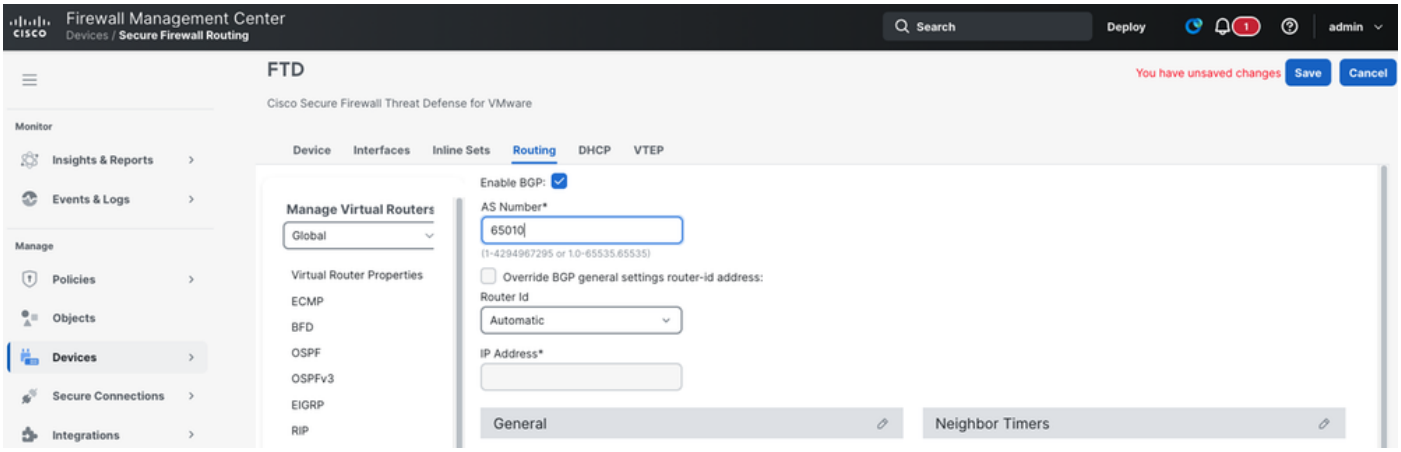


安全FTD — 基於原則的路由

設定FTD上的BGP

1.啟用BGP

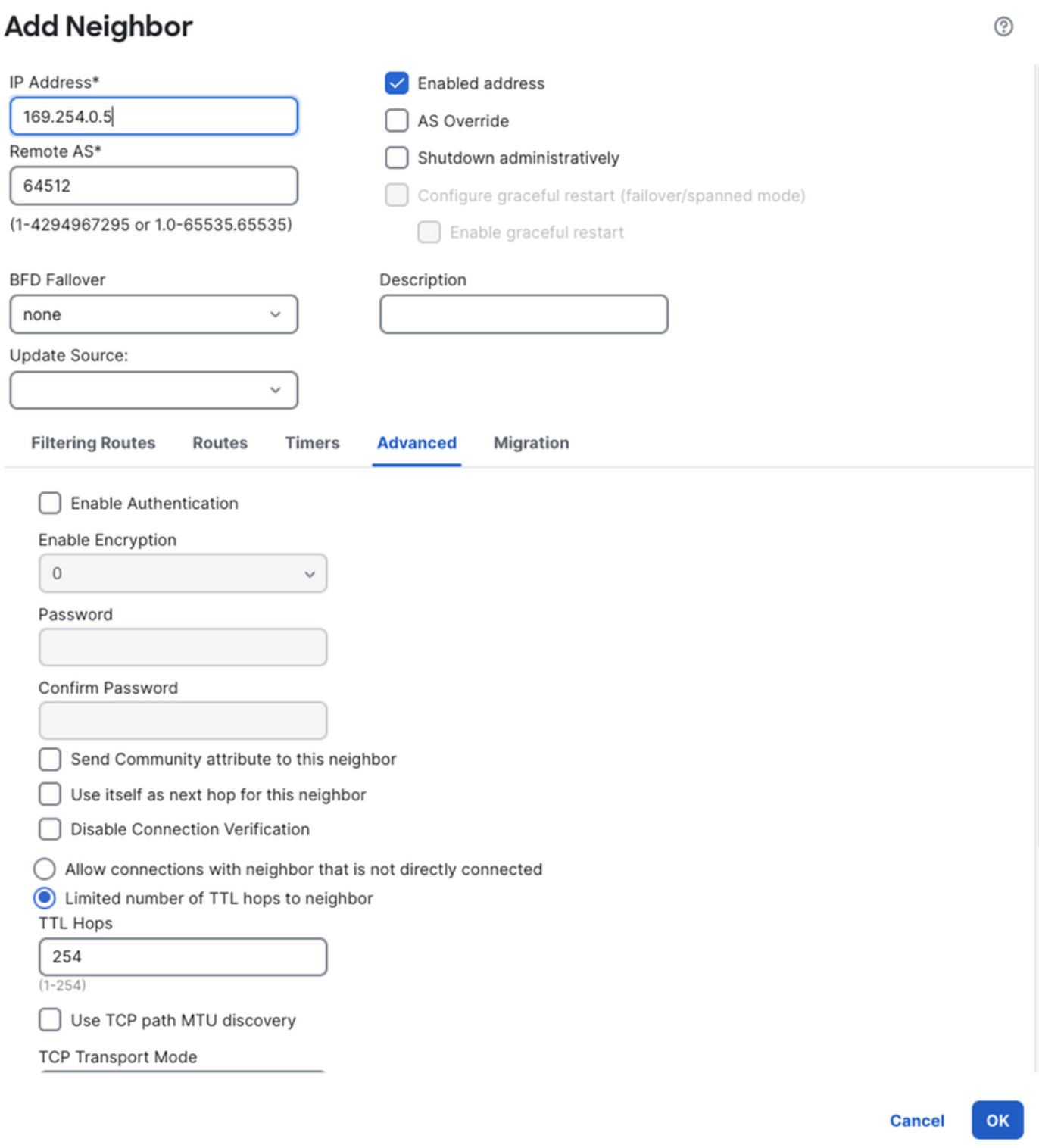
- 導覽至Devices > Device Management > FTD > Routing > General Settings > BGP
- 啟用BGP並新增AS編號（FTD本地AS編號）
- 按一下「Save」



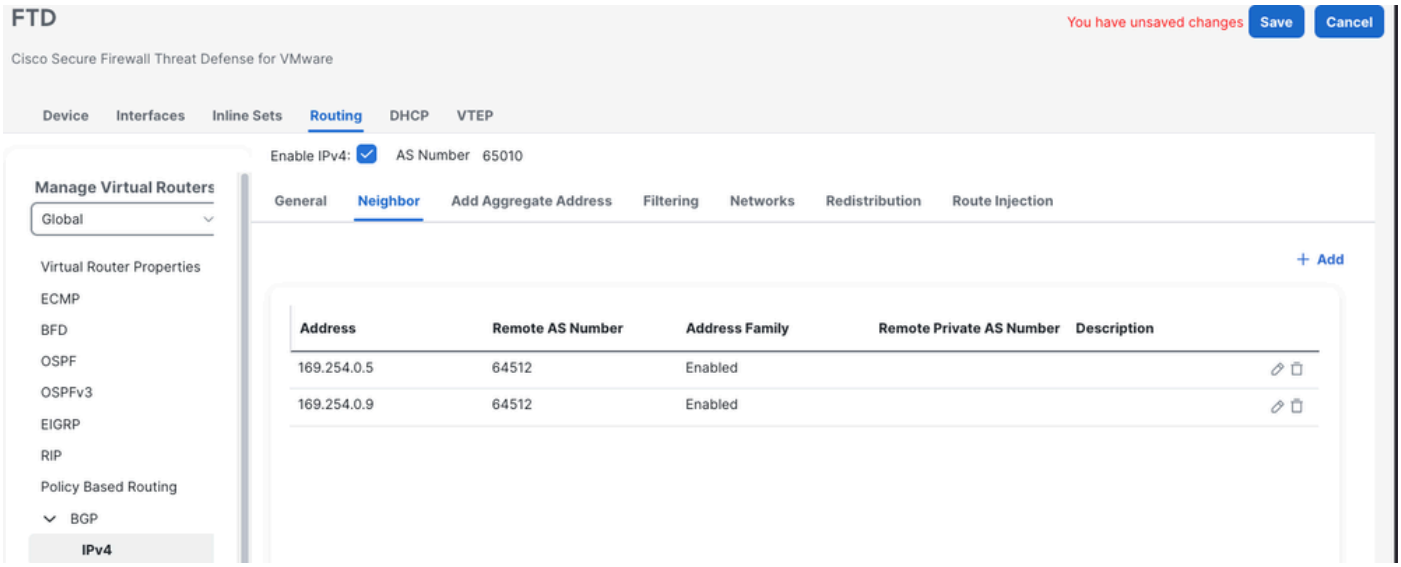
安全FTD - BGP路由

- 導覽至BGP > IPv4

2.新增BGP Neighbor — 安全訪問BGP對等體是169.254.0.5和。169.254.0.9


Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK

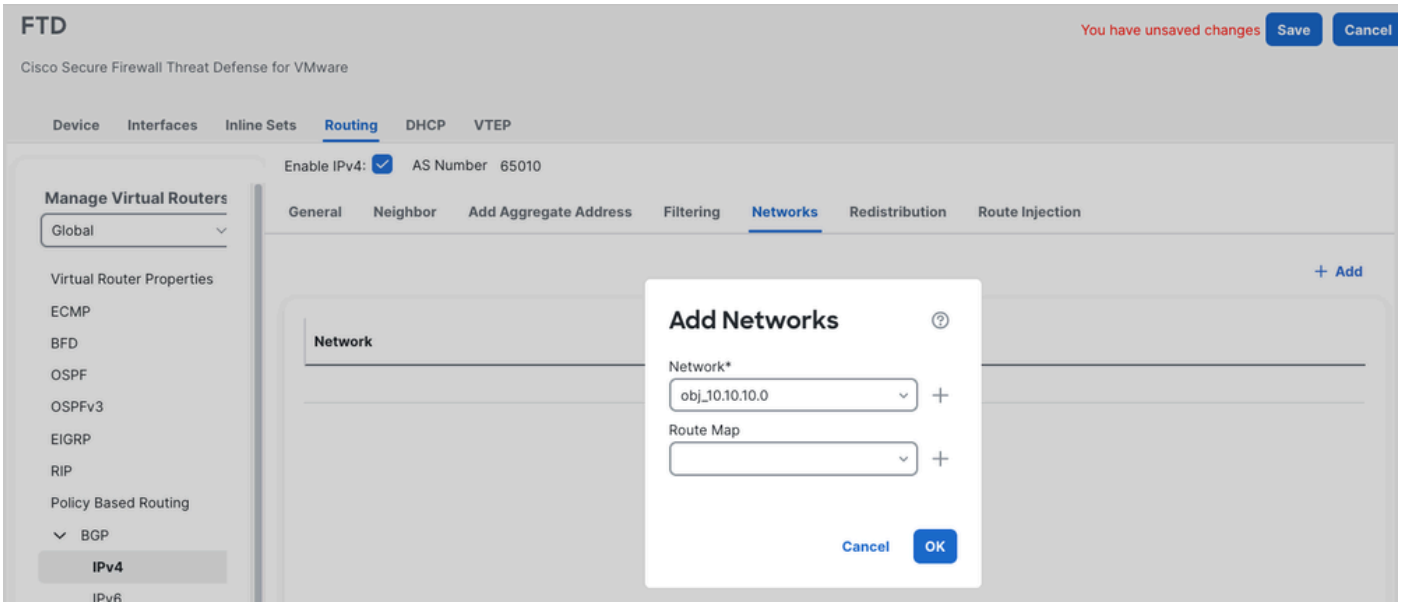
安全FTD - BGP路由



安全FTD - BGP路由

3.新增網路 — 需要通告到安全訪問的網路

- 按一下「OK」

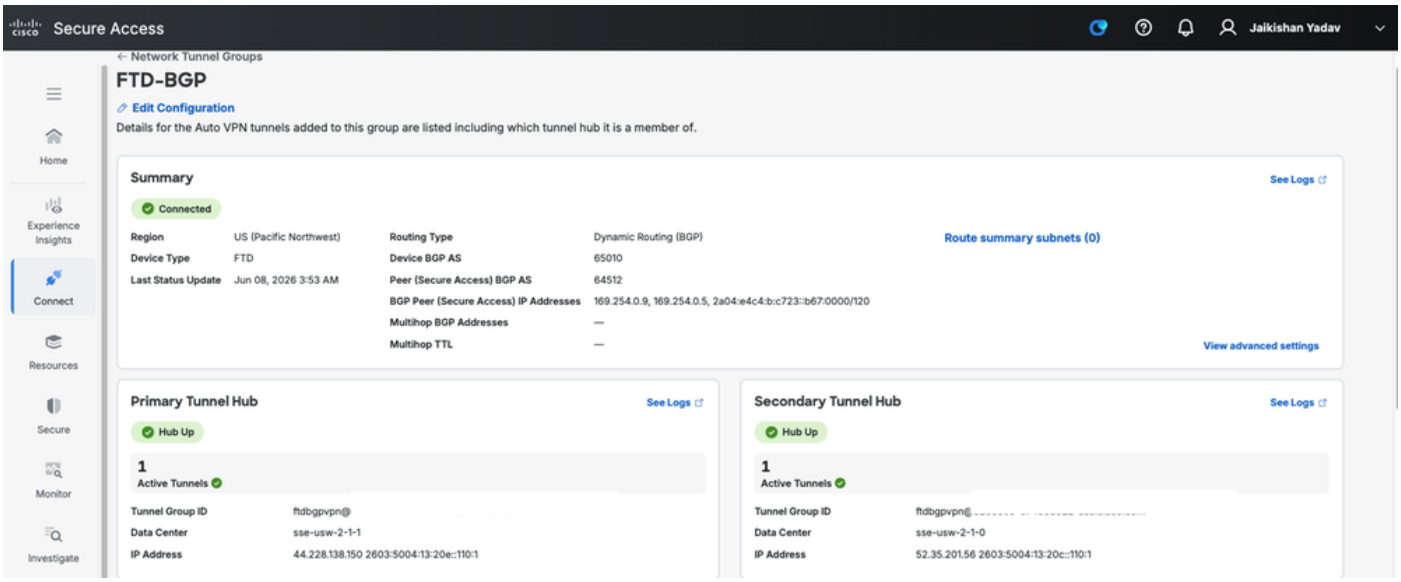


安全FTD - BGP路由

- 儲存並部署更改

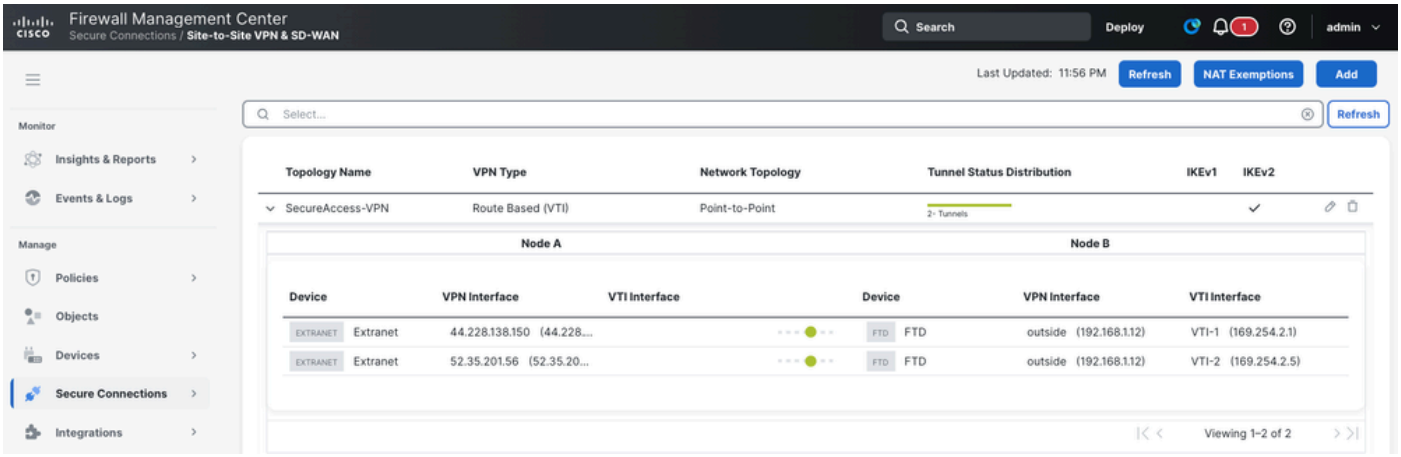
驗證通道狀態

論安全訪問



安全FTD - IPsec通道狀態

關於FMC

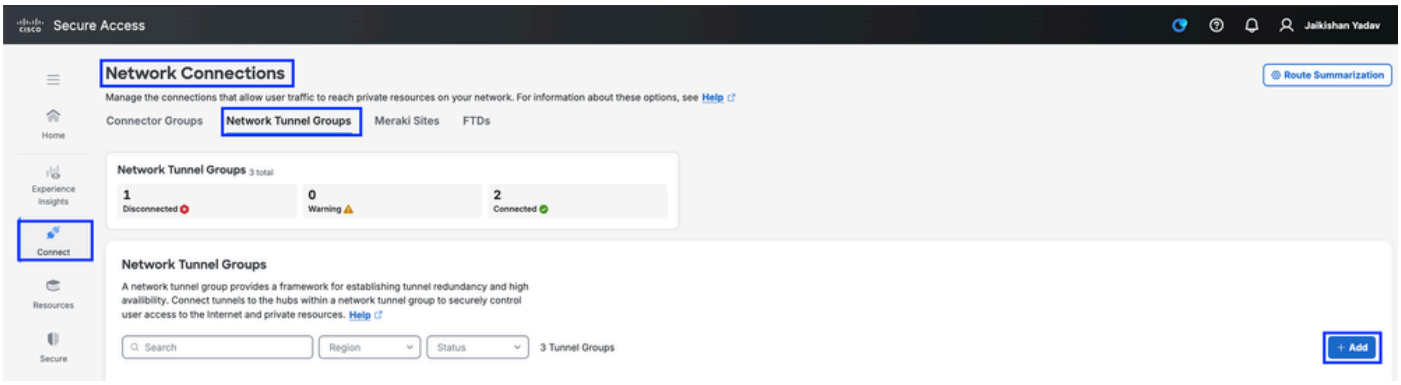


安全FMC - IPsec通道狀態

在帶PBR的自適應安全裝置(ASA)上配置基於靜態路由的IPsec VPN

安全訪問上的VPN配置

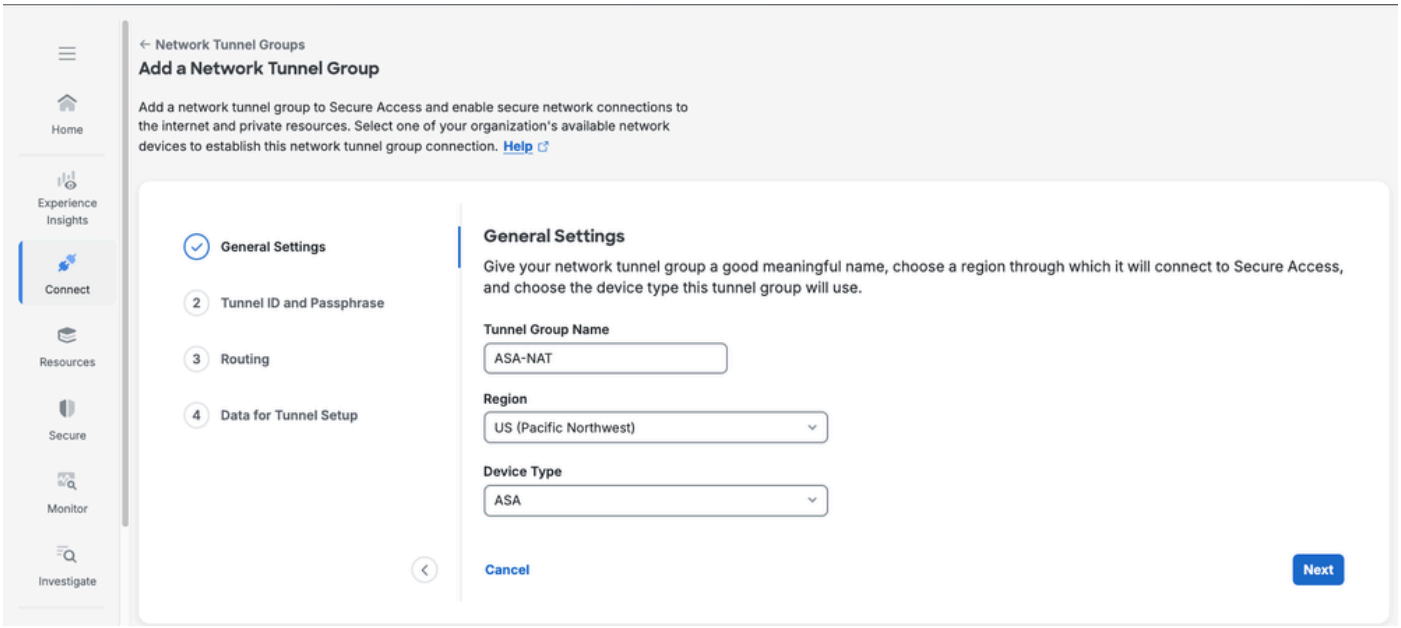
1.登入到Secure Access控制面板Secure Access
2.導覽至Connect > Network Connections > Network Tunnel Groups，然後點選+Add以配置網路隧道組



安全訪問 — 網路隧道組

3.配置網路隧道組 — 常規設定

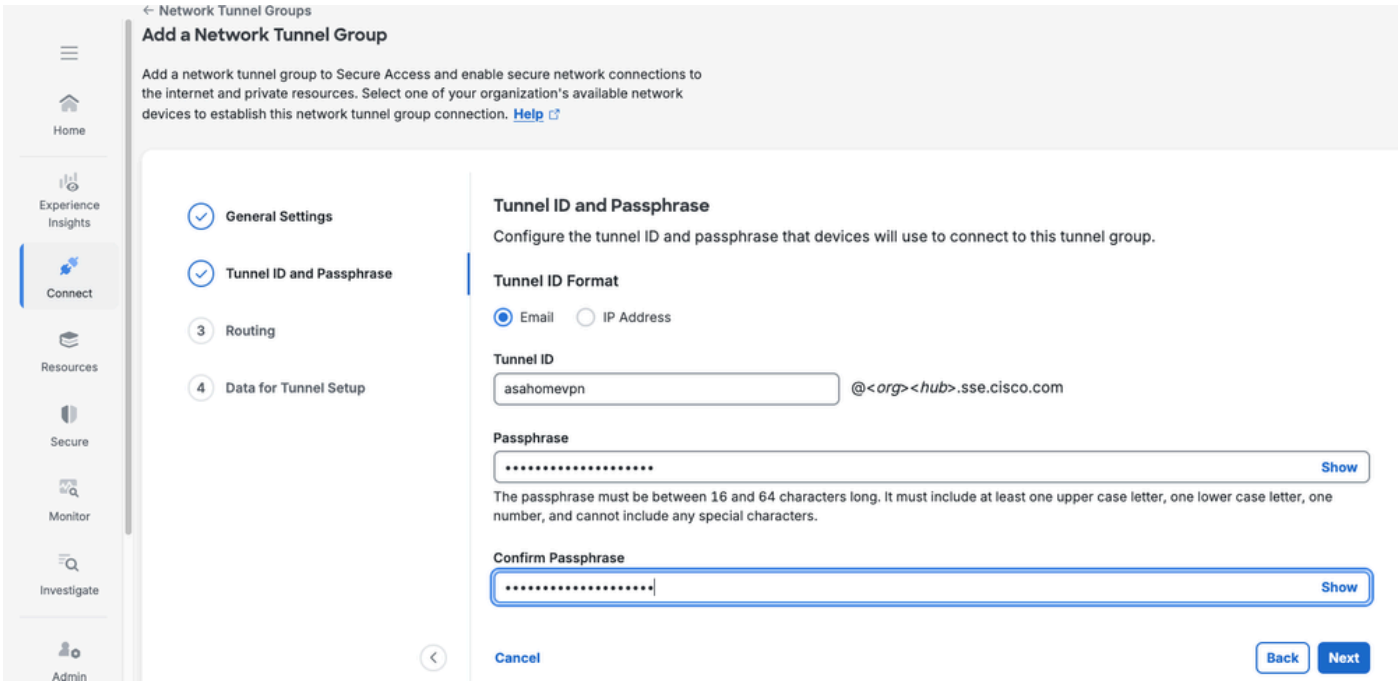
- 配置隧道組名稱、區域和設備型別
- 按一下下一步



安全訪問 — 網路隧道組常規設定

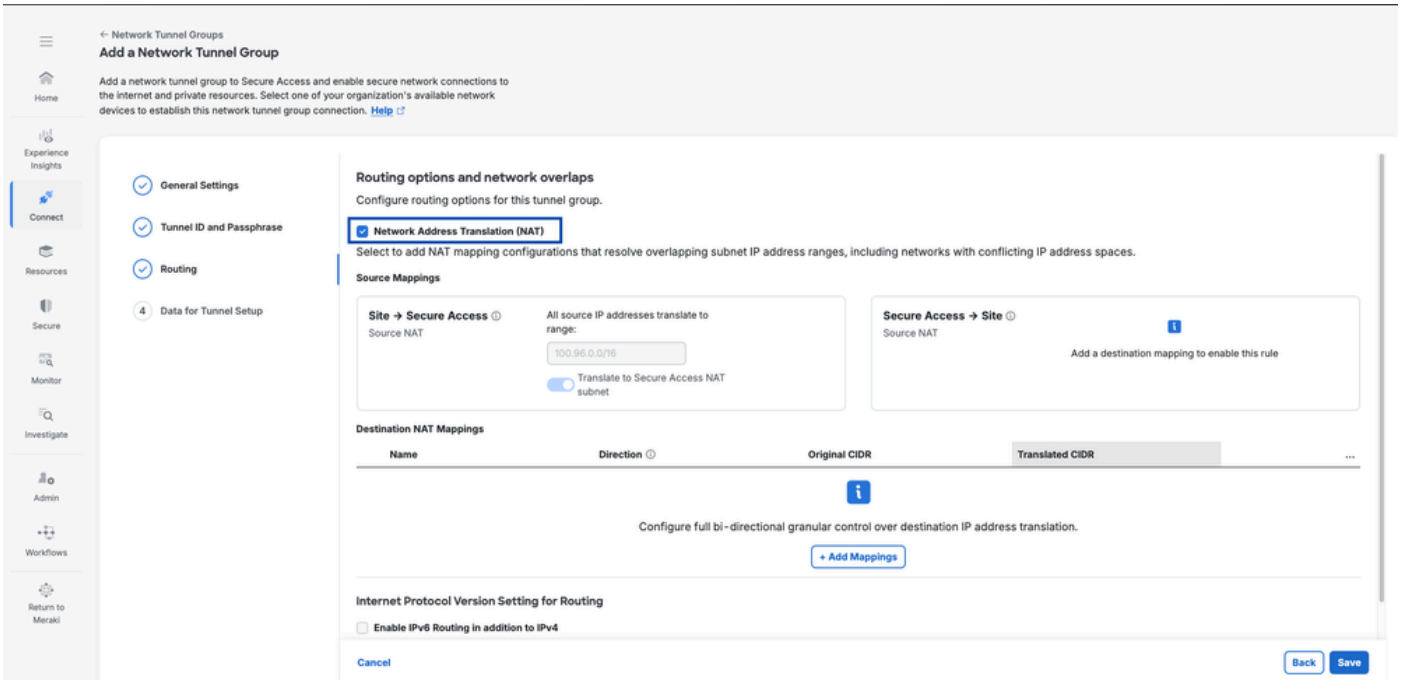
4.設定通道ID和密碼短語。

- 設定通道ID和密碼。
- 按一下「下一步」



安全訪問 — 網路隧道組

5.啟用網路地址轉換(NAT)

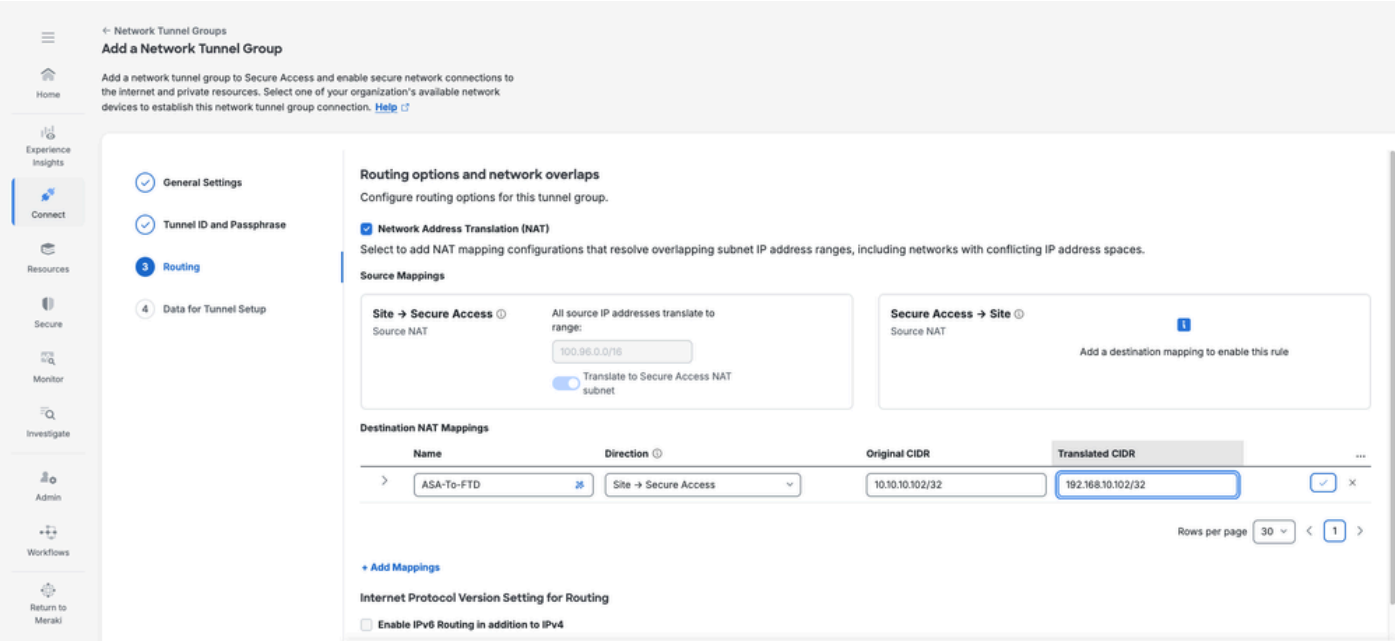


安全訪問 — 網路隧道組NAT設定

6.新增目標NAT對映

流程1 — 路由器1到路由器2（站點到安全訪問）

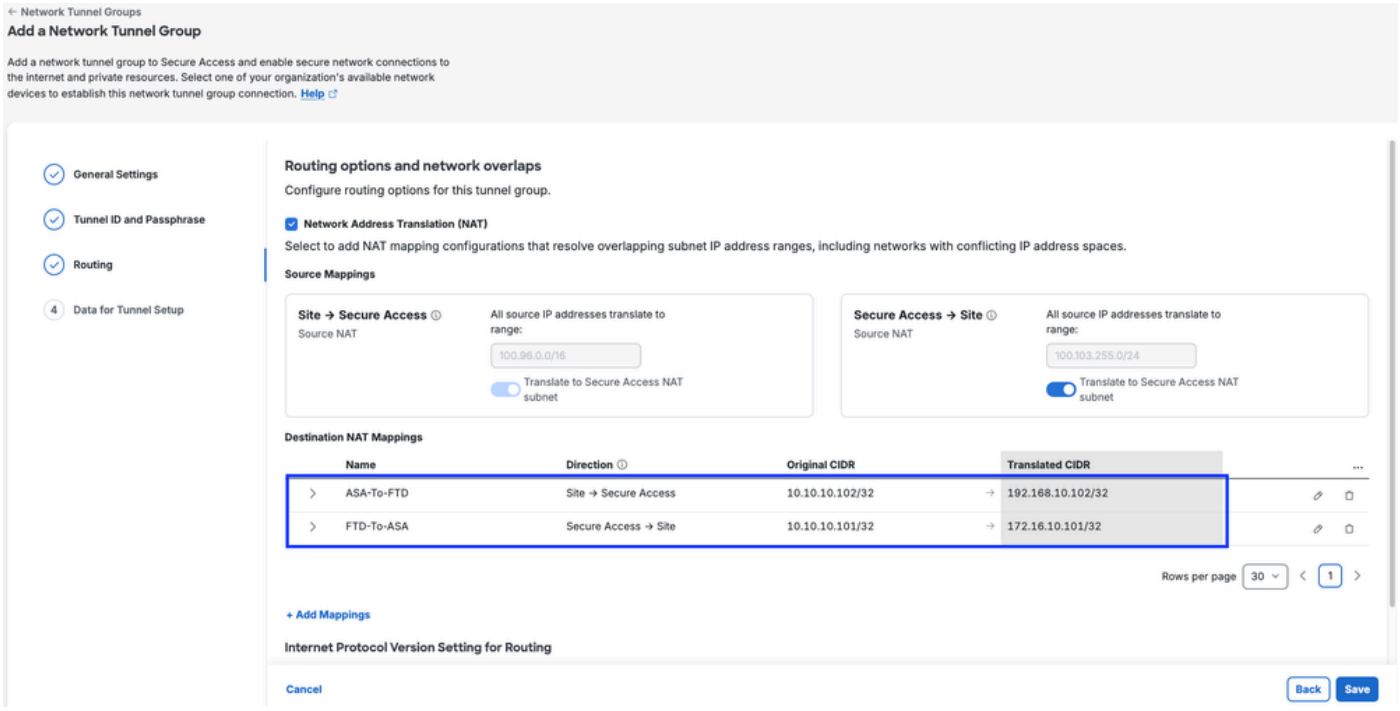
流程2 — 路由器2到路由器1（站點安全訪問）



安全訪問 — 網路隧道組NAT設定

注意：啟用NAT時，BGP不可用。此外，在客戶邊緣裝置上配置靜態VPN

提示：請始終記住ping已轉換的IP。
轉換後的IP將進入轉換後的CIDR，而實際IP將進入原始CIDR。



安全訪問 — 網路隧道組NAT設定

按一下 儲存

提示：對於從「站點A」到「站點B」的流量，從CNHE-1的視點方向是「站點 — > SecureAccess」

對於從「站點B」到「站點A」的流量，從CNHE-1的角度方向是「SecureAccess -> Site」

ASA上的VPN配置

1.登入ASA CLI，進入啟用模式並驗證通向Internet的基本IP連線

ASA# sh ip
系統IP地址：
介面名稱IP位址子網路遮罩方法
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0手冊
GigabitEthernet0/1 inside 10.10.1 255.255.255.0手冊

當前IP地址：
介面名稱IP位址子網路遮罩方法
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0手冊
GigabitEthernet0/1 inside 10.10.1 255.255.255.0手冊

ASA# ping 8.8.8.8
鍵入要中止的轉義序列。
正在向8.8.8.8傳送5個100位元組ICMP響應，超時為2秒：
!!!!!
成功率為100%(5/5)，往返最小/平均/最大= 20/28/30毫秒
ASA#

2.配置IKEv2策略並在外部介面上啟用IKEv2

crypto ikev2 policy 10
加密aes-gcm-256
完整性null
組19
lifetime seconds 86400
crypto ikev2 enable outside

3.配置IPSec建議

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary
protocol esp encryption aes-gcm-256

4.配置IPsec配置檔案

crypto ipsec profile csa-profile-primary
set ikev2 ipsec-proposal Ipsec-Proposal-primary
set ikev2 local-identity email-id <primary tunnel-id>

5.配置組策略，並在屬性下啟用IKEv2協定。

group-policy csa-policy-primary internal
group-policy csa-policy-primary attributes
vpn-tunnel-protocol ikev2

6.配置隧道組。

tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary
tunnel-group 44.228.138.150 ipsec-attributes

ikev2 remote-authentication pre-shared-key <pre-shared-key>
ikev2 local-authentication pre-shared-key <pre-shared-key>

7.設定虛擬通道介面(VTI)

- Nameif可以是您的選擇
- 分配給VTI的IP地址不得與ASA上的任何其他介面重疊
- 通道源可以是防火牆的外部介面
- 隧道目標必須為資料中心IP地址

interface Tunnel1
nameif VTI-1
IP 網址 169.254.2.1 255.255.255.252
隧道源介面外部
隧道目標44.228.138.150
通道模式ipsec ipv4
通道保護ipsec設定檔csa-profile-primary

8.配置路由，使到對映IP地址或子網的流量在VTI介面內路由。下一跳需要在VTI範圍內通過IP進行。

route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5.（適用於基於網際網路的RAVPN池或CGNAT流量）

或

路由VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

基於原則的路由

1.訪問清單

access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any

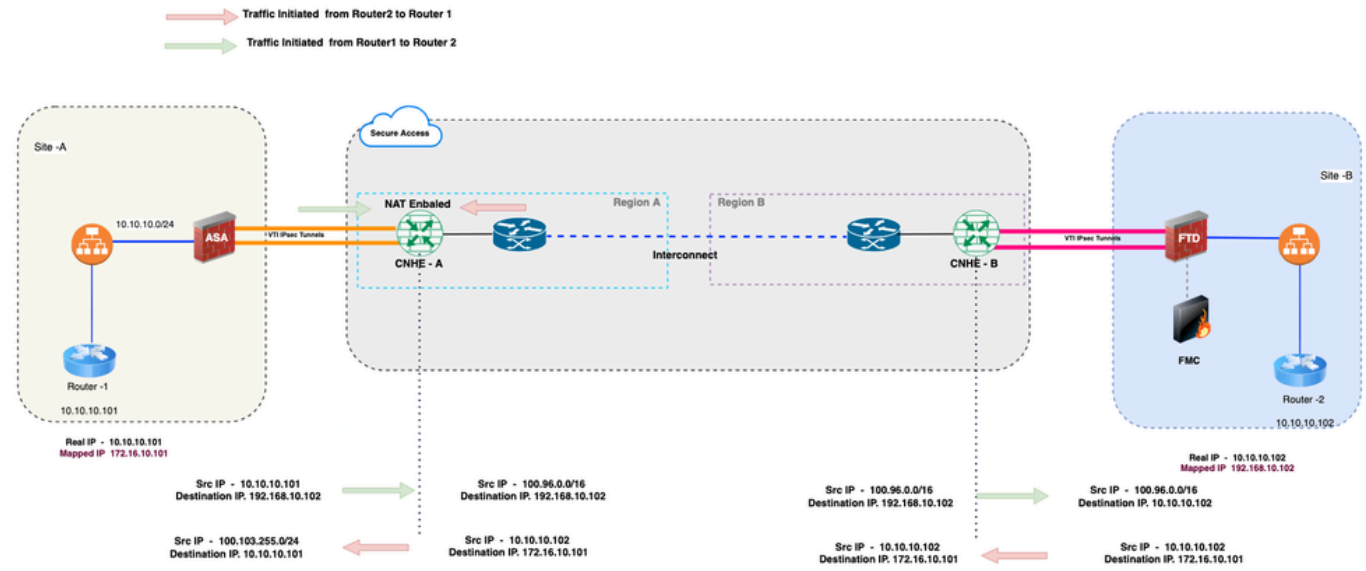
2.路由對映

route-map RM-CSA permit 10
match ip address PBR
set ip next-hop 169.254.2.2 169.254.2.6

3.將路由對映應用於輸入介面

interface GigabitEthernet0/1
nameif inside
安全級別100
ip address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA

驗證



路由器介面和GW可達性狀態

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

測試1 - Router2 —> Router1。- Ping測試

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

ASA上的資料包捕獲（本地FW）

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

FTD上的封包擷取（遠端防火牆）

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

測試2. - Router 2 —> Router 1 ping測試

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

FTD封包擷取（本機防火牆）

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

ASA資料包捕獲（遠端FW）

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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）。