

在FMC管理的FTD上配置基於路由的站點到站點VPN隧道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制和限制](#)

[FMC的配置步驟](#)

[驗證](#)

[在FMC GUI上](#)

[在FTD CLI上](#)

簡介

本文檔介紹如何在由Firepower管理中心管理的Firepower威脅防禦上配置基於靜態路由的站點到站點VPN隧道。

必要條件

需求

思科建議您瞭解以下主題：

- 對VPN隧道工作方式有基礎認識。
- 瞭解如何在FMC中導航。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科Firepower管理中心(FMC)版本6.7.0
- Cisco Firepower威脅防禦(FTD)版本6.7.0

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

基於路由的VPN允許確定要加密或通過VPN隧道傳送的相關流量，並且使用流量路由而不是策略/訪問清單（如基於策略或基於加密對映的VPN中所示）。加密域設定為允許任何進入IPsec隧道的流量。IPsec本地和遠端流量選擇器設定為0.0.0.0/0.0.0.0。這表示路由到IPsec通道的任何流量都會被加密，無論其來源/目的地子網為何。

本檔案將重點介紹靜態虛擬通道介面(SVTI)組態。有關安全防火牆上的動態虛擬通道介面(DVTI)組態，請參閱[本檔案](#)。


限制和限制

以下是FTD上基於路由的通道的已知限制和限制：


- 僅支援IPsec。不支援GRE。
- 僅支援IPv4介面，以及IPv4、受保護的網路或VPN負載（不支援IPv6）。
- 對VPN流量進行分類的VTI介面支援靜態路由和僅BGP動態路由協定（不支援其他協定，如OSPF、RIP等）。
- 每個介面僅支援100個VTI。
- FTD叢集上不支援VTI。
- 這些策略不支援VTI:
 - QoS
 - NAT
 - 平台設定

新VPN通道的FMC/FTD 6.7.0版不再支援這些演演算法（FMC支援所有移除的密碼以管理FTD < 6.7）：

- IKE策略不支援3DES、DES和NULL加密。
- DH組1、2和24在IKE策略和IPsec建議中不受支援。
- IKE策略不支援MD5完整性。
- IKE策略不支援PRF MD5。
- IPsec提議中不支援DES、3DES、AES-GMAC、AES-GMAC-192和AES-GMAC-256加密演算法。

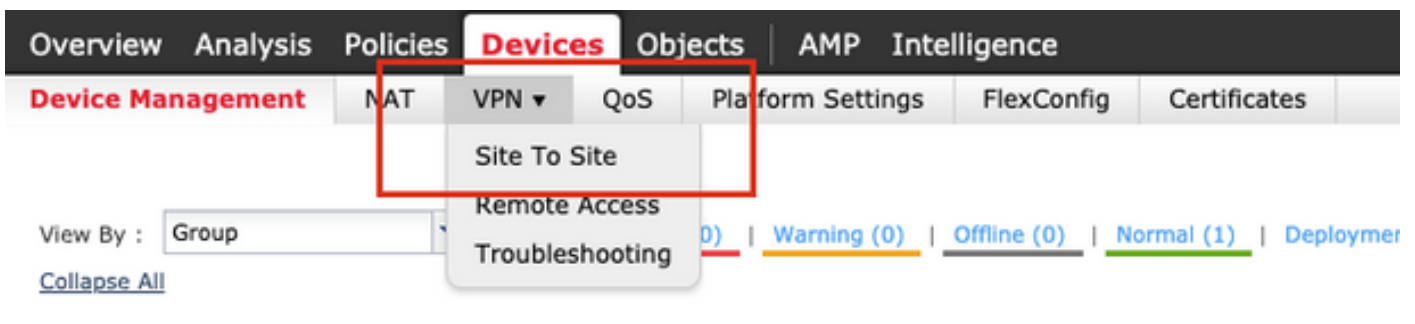
 注意：對於基於站點到站點路由和基於策略的VPN隧道，此情況適用。為了將舊版FTD從FMC升級到6.7，它會觸發預驗證檢查，警告使用者有與封鎖升級的已移除密碼相關的變更。

通過FMC 6.7管理的FTD 6.7	配置可用	站點到站點VPN隧道
全新安裝	弱密碼可用，但無法用於配置FTD 6.7裝置。	弱密碼可用，但無法用於配置FTD 6.7裝置。
升級：FTD僅配置弱密碼	從FMC 6.7 UI升級，預驗證檢查會顯示錯誤。在重新配置之前，升級被阻止。	進行FTD升級後，並假設對等點的設定未變更，則通道會終止。
升級：FTD僅設定一些弱密碼和強密碼	從FMC 6.7 UI升級，預驗證檢查會顯示錯誤。在重新配置之前，升級被阻止。	FTD升級後，假設對等點具有強密碼，然後通道重新建立。
升級：C類國家/地區（沒有強大的加密許可證）	允許DES	允許DES

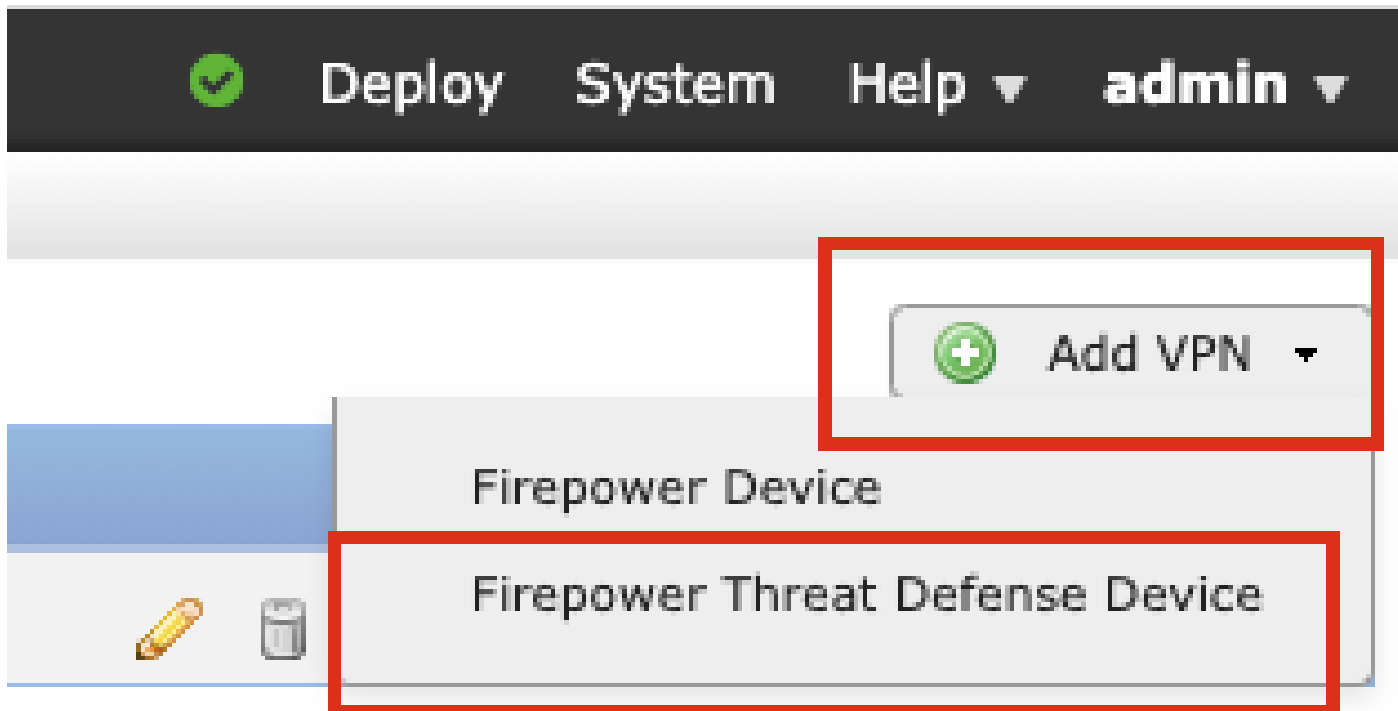
 注意：無需其他許可，可在許可模式和評估模式下配置基於路由的VPN。如果沒有加密合規（啟用匯出控制功能），只有DES可用作加密演算法。

FMC的配置步驟

步驟 1. 導航至Devices >VPN >Site To Site。



步驟 2. 按一下「Add VPN」，然後選擇「Firepower Threat Defense Device」，如下圖所示。

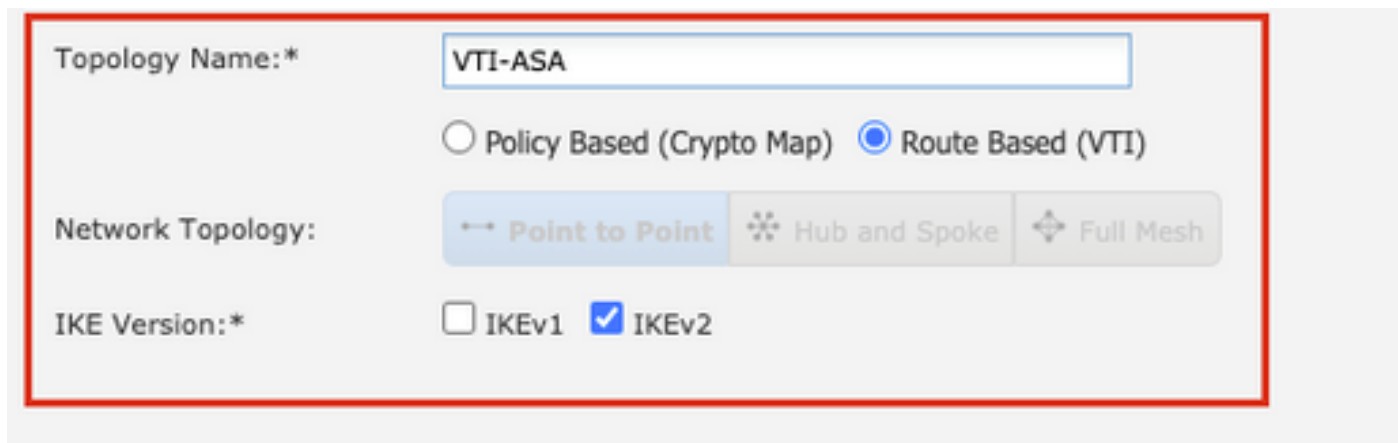


步驟 3. 提供拓撲名稱並選擇VPN型別作為基於路由(VTI)。選擇IKE版本。

在本演示中：

拓撲名稱：VTI-ASA

IKE版本：IKEv2



步驟 4. 選擇需要在其上配置隧道的Device，您可以選擇新增新的Virtual Template Interface(按一下+圖示)，或者從現有清單中選擇一個介面。

The screenshot shows a configuration page with tabs for 'Endpoints', 'IKE', 'IPsec', and 'Advanced'. The 'Endpoints' tab is active, showing two nodes: Node A and Node B. Node A's configuration includes: 'Device:*' set to 'FTD', 'Virtual Tunnel Interface:*' set to an empty field with a '+' icon, 'Tunnel Source IP is Private' unchecked, and 'Connection Type:*' set to 'Bidirectional'. Node B's configuration includes: 'Device:*' set to 'Empty', 'Virtual Tunnel Interface:*' set to an empty field with a '+' icon, 'Tunnel Source IP is Private' unchecked, and 'Connection Type:*' set to 'Bidirectional'. Below each node's configuration are fields for 'Tunnel IP Address', 'Tunnel Source Interface', and 'Tunnel Source Interface IP', all of which are currently empty.

步驟 5. 定義新虛擬通道介面的引數。按一下「OK」(確定)。

在本演示中：

名稱：VTI-ASA

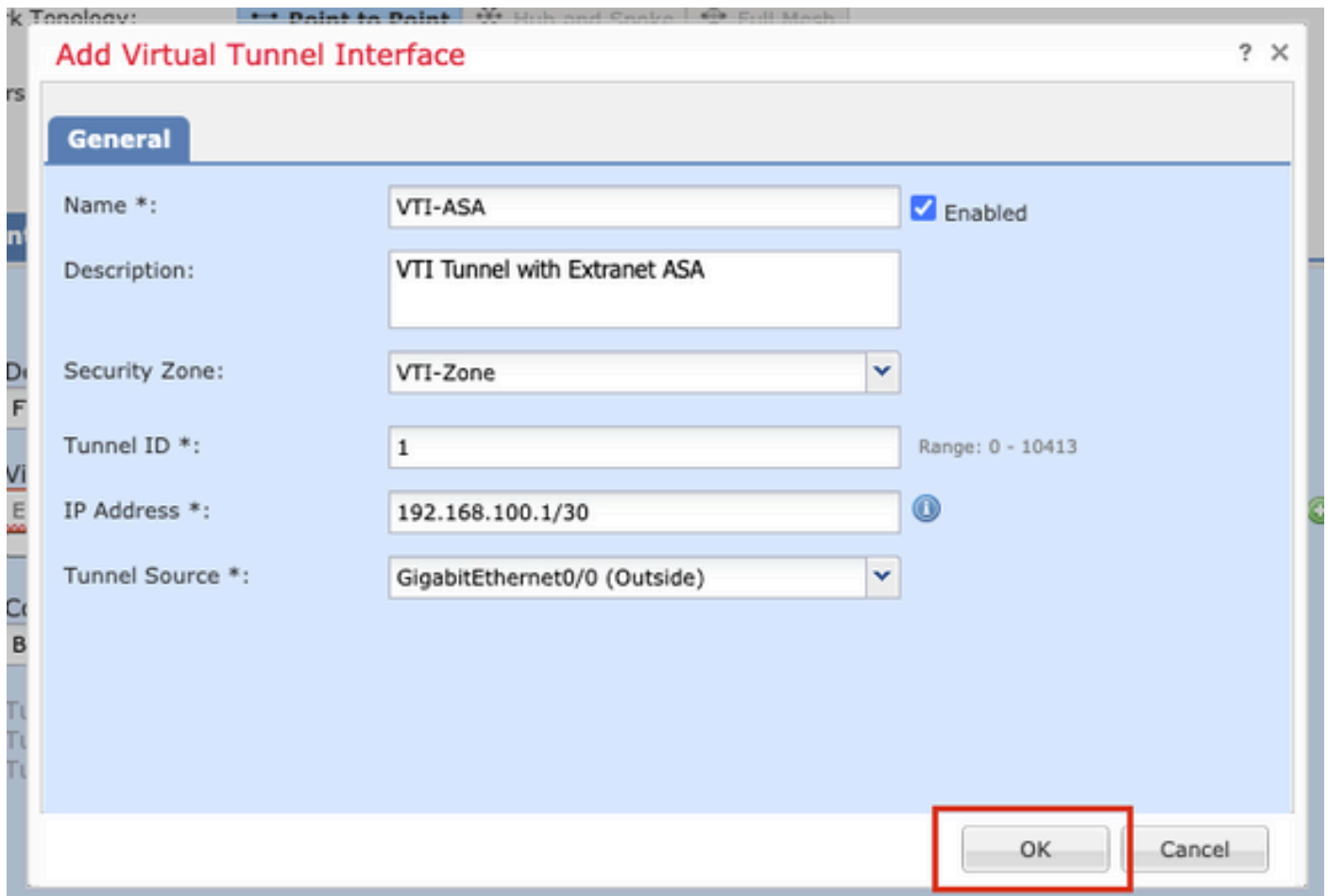
說明 (可選)：使用外網ASA的VTI隧道

安全區域：VTI-Zone

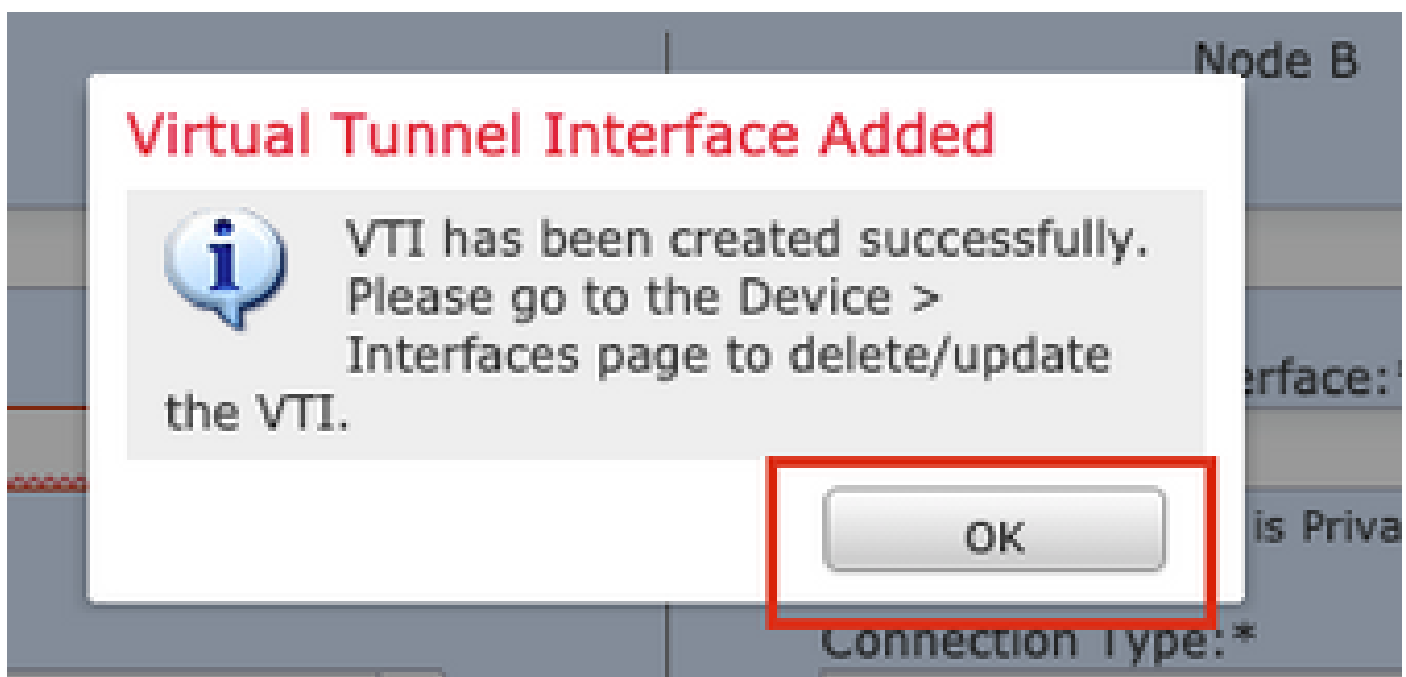
通道ID:1

IP地址：192.168.100.1/30

隧道源：GigabitEthernet0/0 (外部)



步驟 6. 點選彈出視窗中的OK，提示已建立新VTI。



步驟 7. 選擇新建立的VTI或虛擬隧道介面下存在的VTI。提供節點B（對等裝置）的資訊。

在本演示中：

裝置：Extranet

裝置名稱：ASA-Peer

終端IP地址：10.106.67.252

Create New VPN Topology

Topology Name:* VTI-ASA

Policy Based (Crypto Map) Route Based (VTI)

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:* FTD

Virtual Tunnel Interface:* VTI-ASA Tunnel Source IP is Private [Edit VTI](#)

Connection Type:* Bidirectional

Tunnel IP Address : 192.168.100.1
Tunnel Source Interface : Outside
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B

Device:* Extranet

Device Name*: ASA-Peer

Endpoint IP Address*: 10.106.67.252

Save Cancel

步驟 8. 導航到IKE頁籤。您可以選擇使用預定義的Policy，或按一下Policy頁籤旁邊的+按鈕並建立一個新策略。

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA-LATEST

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

步驟9. (可選 , 如果建立新的IKEv2策略。) 為策略提供名稱 , 並選擇要在策略中使用的演算法。按一下「Save」。

在本演示中 :

名稱 : ASA-IKEv2-Policy

完整性演算法 : SHA-512

加密演算法 : AES-256

PRF演算法 : SHA-512

Diffie-Hellman組 : 21

The screenshot shows the 'New IKEv2 Policy' configuration window. The 'Name' field is set to 'ASA-IKEv2-Policy'. The 'Priority' is 1 and 'Lifetime' is 86400 seconds. Under 'Integrity Algorithms', 'SHA512' is selected in the 'Available Algorithms' list and moved to the 'Selected Algorithms' list. The 'Save' button is highlighted.

步驟 10. 選擇新建立的策略或現有的Policy。選擇Authentication Type。如果使用預共用手動金鑰 , 請在金鑰和確認金鑰框中提供金鑰。

在本演示中 :

策略 : ASA-IKEv2-Policy

身份驗證型別：預共用手動金鑰

主要：cisco123

確認金鑰：cisco123

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3 [v] [+]

Authentication Type: Pre-shared Automatic Key [v]

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings


Policy:* ASA-IKEv2-Policy [v] [+]

Authentication Type: Pre-shared Manual Key [v]

Key:* *****

Confirm Key:* *****

Enforce hex-based pre-shared key only


 注意：如果兩個終端在同一個FMC上註冊，則還可以使用預共用自動金鑰選項。

步驟 11. 導航到IPsec選項卡。您可以選擇使用預定義的IKEv2 IPsec建議或建立一個新的IKEv2 IPsec建議。點選IKEv2 IPsec Proposal選項卡旁的Edit按鈕。


Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel [v]

Transform Sets:

IKEv1 IPsec Proposals 

tunnel_aes256_sha

IKEv2 IPsec Proposals* 

AES-GCM

Enable Security Association (SA) Strength Enforcement

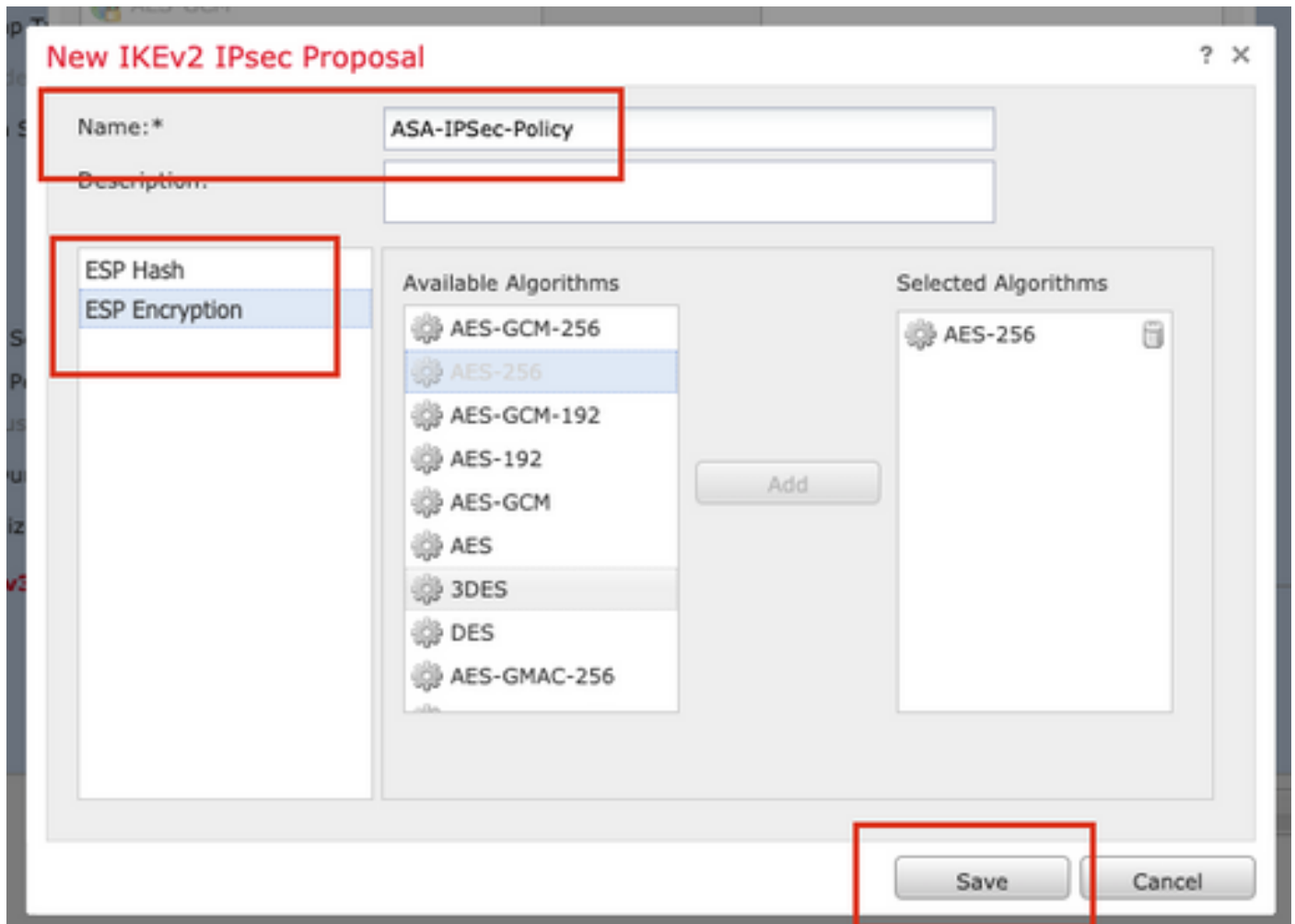
步驟12. (可選，如果建立新的IKEv2 IPsec提議。) 提供建議書的名稱，並選擇建議書中要使用的演算法。按一下「Save」。

在本演示中：

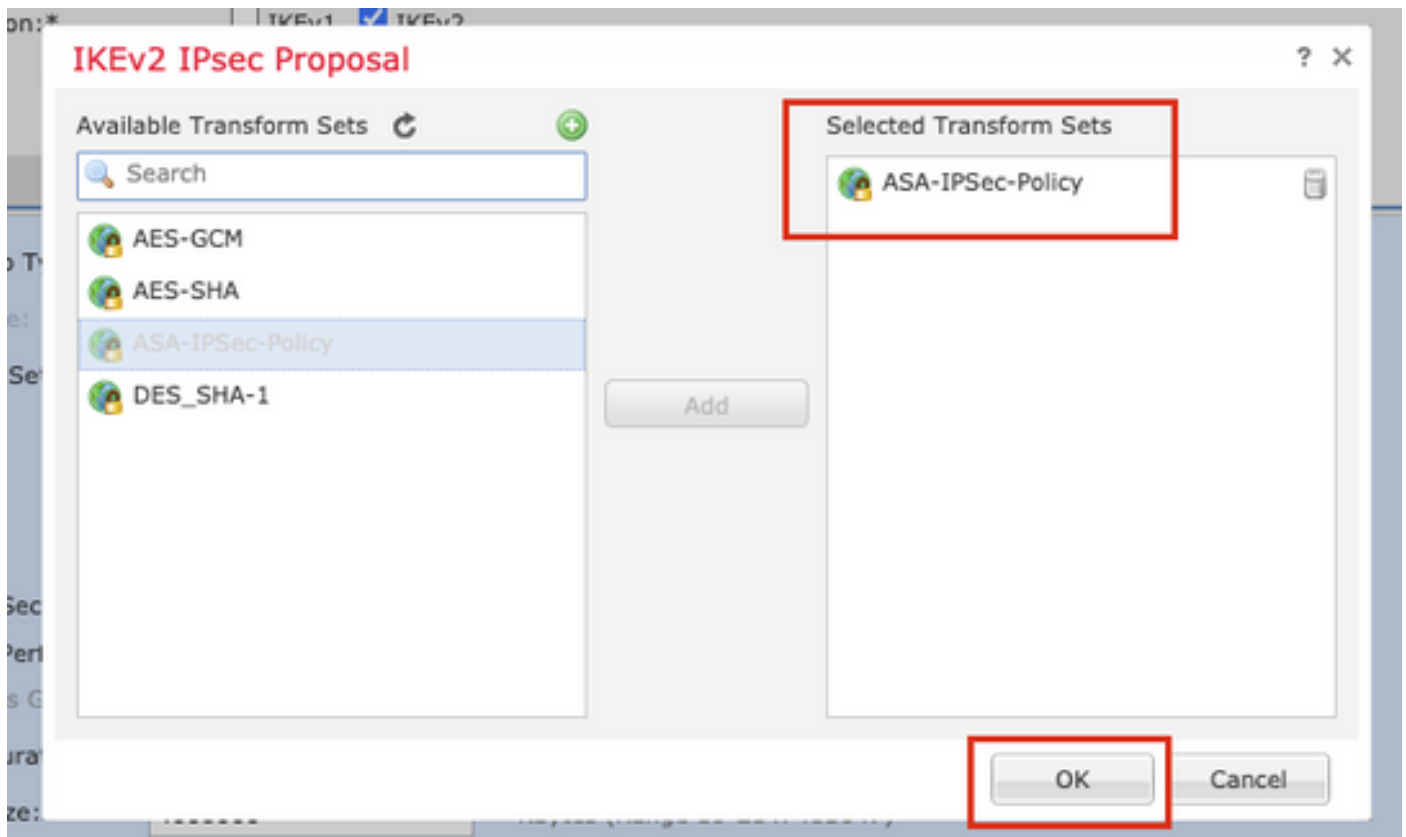
名稱：ASA-IPSec-Policy

ESP雜湊：SHA-512

ESP加密：AES-256



步驟 13. 從可用提案清單中選擇新建立的提案或提案。按一下「OK」(確定)。



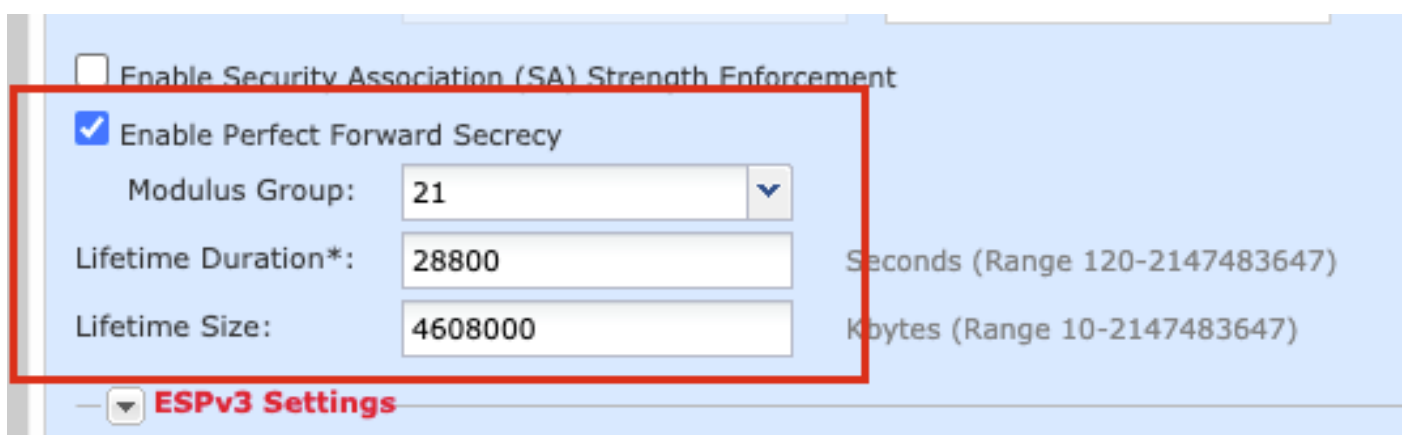
步驟14。(可選)選擇Perfect Forward Secrecy設定。配置IPsec生存期和生存期大小。

在本演示中：

完全前向保密：模群21

生存時間：28800 (預設)

生存期大小：4608000 (預設值)



步驟 15.檢查配置的設定。按一下「Save」，如下圖所示。

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets: **IKEv1 IPsec Proposals** **IKEv2 IPsec Proposals***

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

步驟 16. 配置訪問控制策略。導覽至Policies > Access Control > Access Control。編輯應用於FTD的策略。

 注意：sysopt connection permit-vpn不適用於基於路由的VPN隧道。需要為IN-> OUT區域和OUT -> IN區域配置訪問控制規則。

在Zones頁籤中提供Source Zones和Destination Zones。

在Networks 選項卡中提供Source Networks和Destination Networks。按一下「Add」。

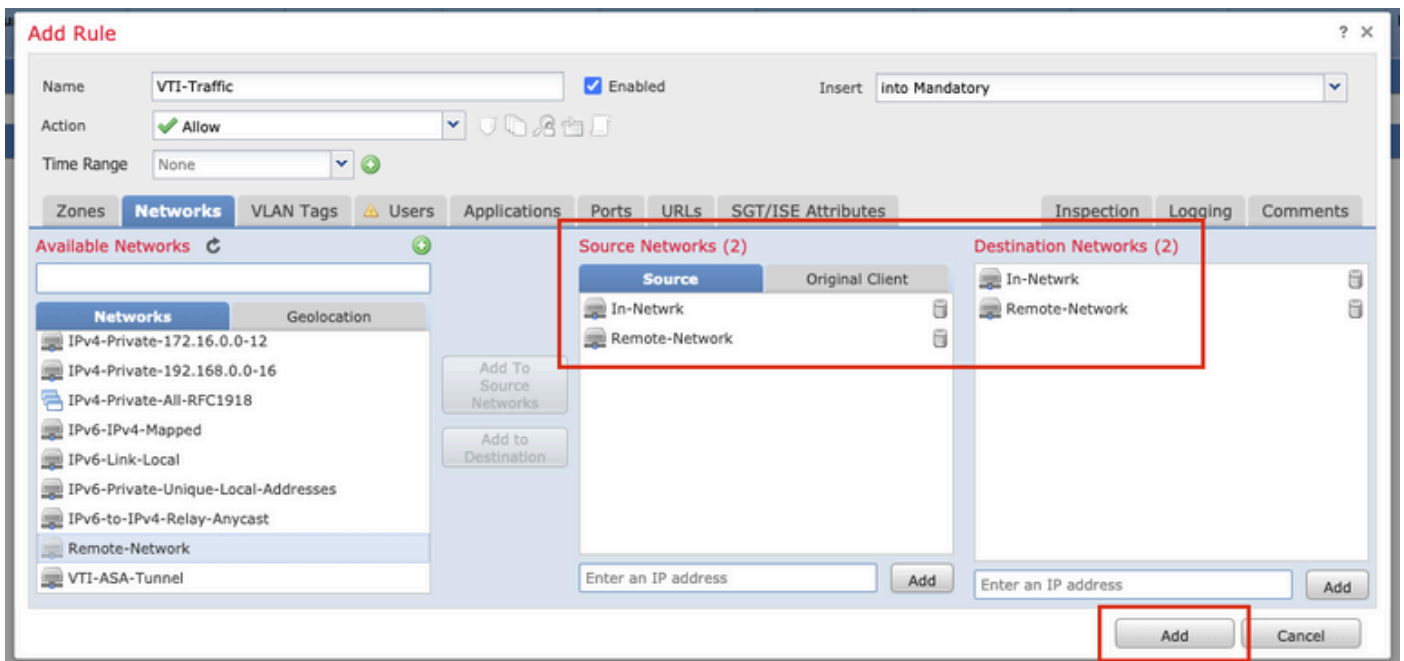
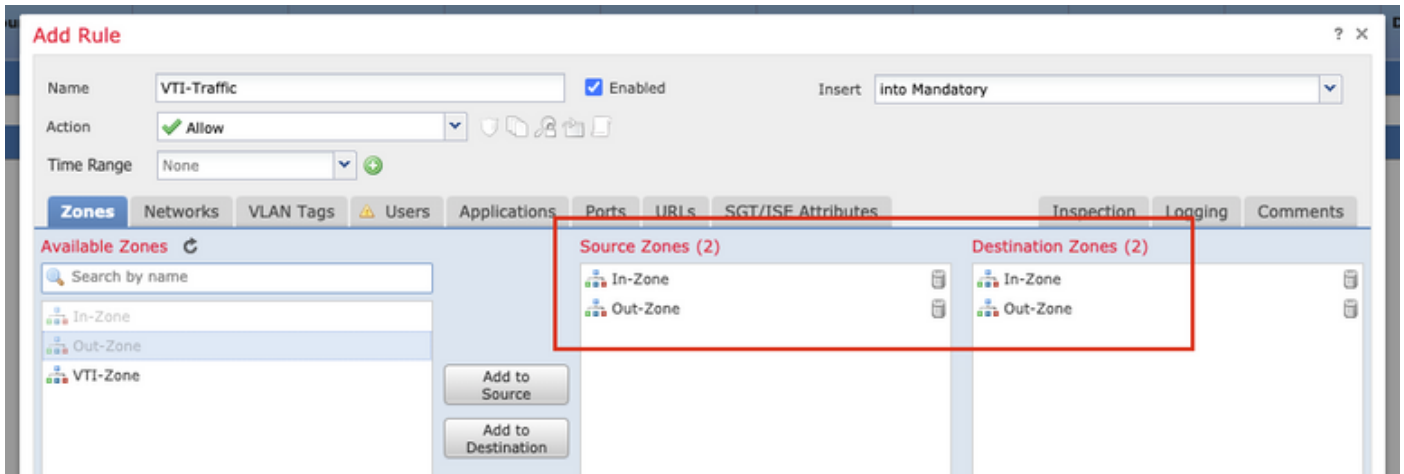
在本演示中：

源區域：內區域和外區域

目標區域：區外和區內

源網路：內聯網和遠端網路

目標網路：遠端網路和內聯網



步驟 17.透過VTI通道新增路由。導覽至Devices > Device Management。編輯VTI隧道配置所在的裝置。

導覽至Routing 索引標籤下的Static Route。按一下Add Route。

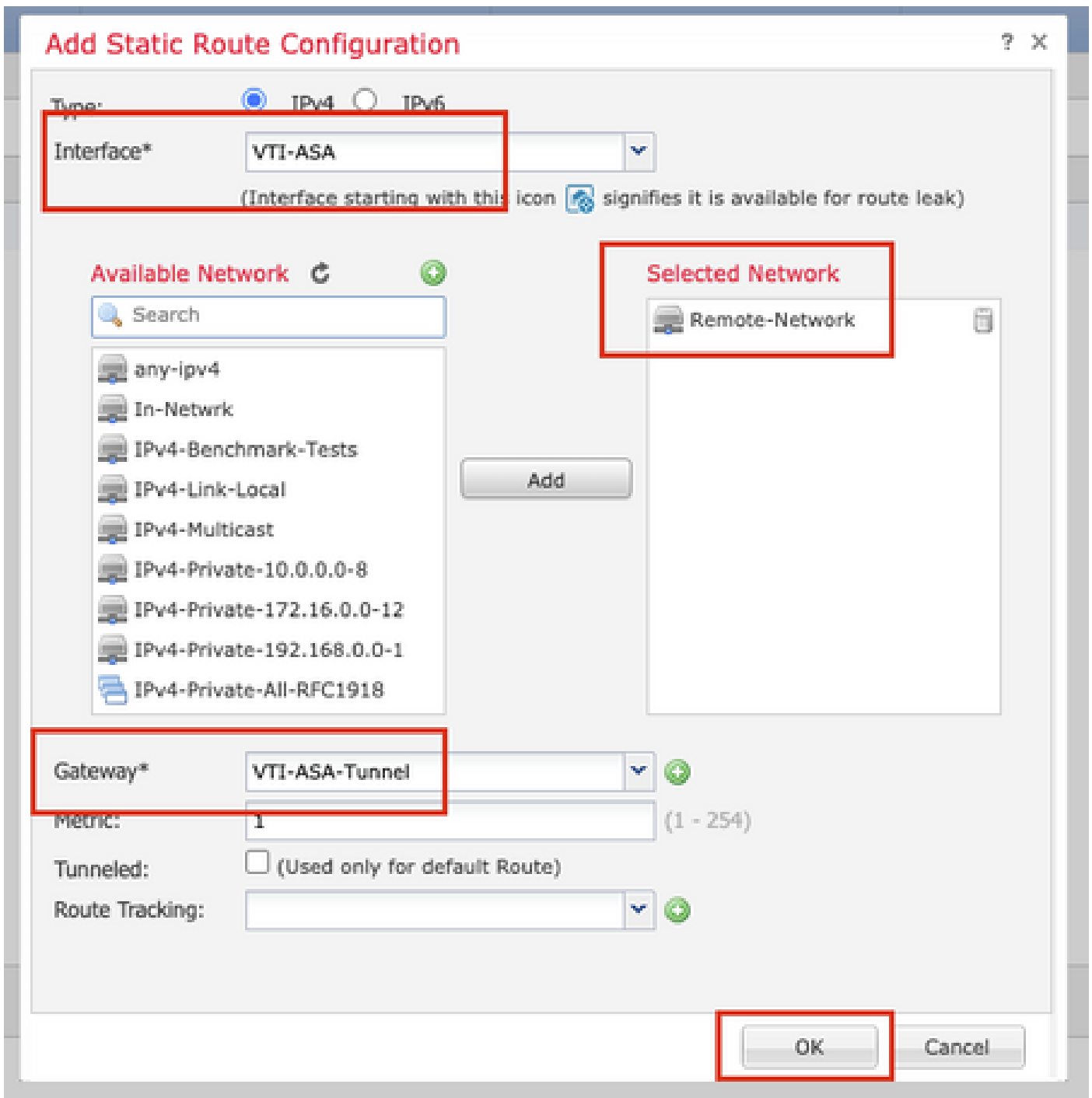
提供Interface，選擇Network，提供Gateway。按一下「OK」（確定）。

在本演示中：

介面：VTI-ASA

網路：遠端網路

網關：VTI-ASA — 隧道



步驟 18. 導航到部署>部署。選擇需要將組態部署到的FTD，然後按一下Deploy。

成功部署後配置推送到FTD CLI:

```
<#root>
```

```
crypto ikev2 policy 1
```

```
  encryption aes-256
  integrity sha512
  group 21
  prf sha512
  lifetime seconds 86400
crypto ikev2 enable Outside
```

```

crypto ipsec ikev2 ipsec-proposal CSM_IP_1

protocol esp encryption aes-256
protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1

set ikev2 ipsec-proposal CSM_IP_1
set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****

interface Tunnel1

description VTI Tunnel with Extranet ASA

nameif VTI-ASA

ip address 192.168.100.1 255.255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4

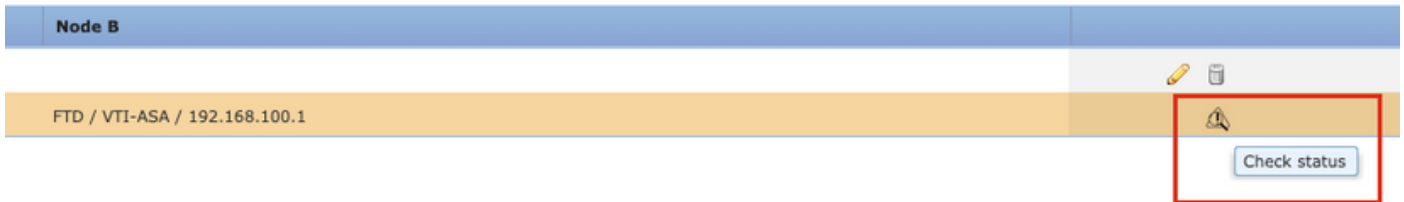
tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

```

驗證

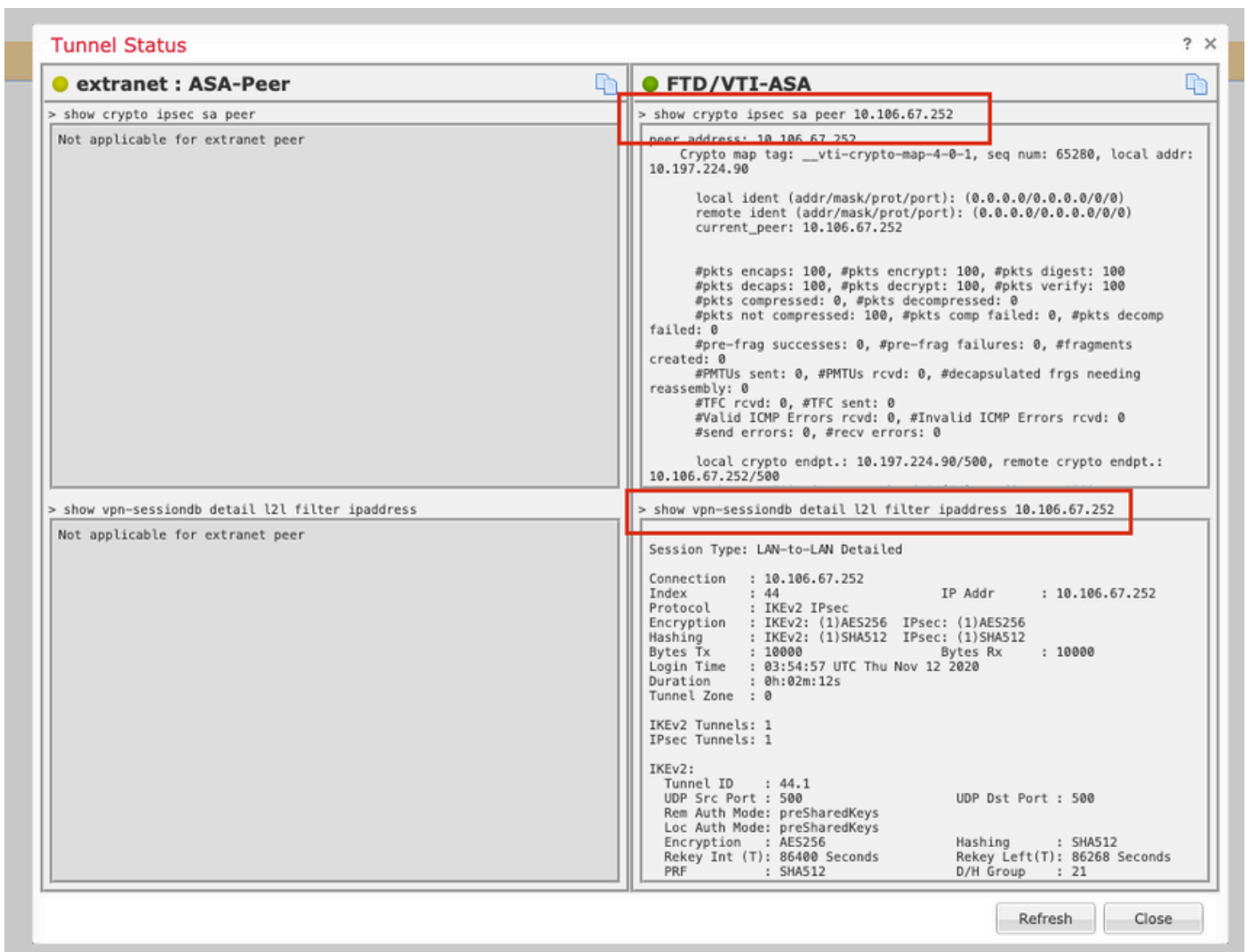
在FMC GUI上

按一下Check Status選項以從GUI本身監控VPN隧道的即時狀態



其中包括從FTD CLI獲取的以下命令：

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>



在FTD CLI上

可從FTD CLI使用這些命令來檢視VPN通道的組態和狀態。

```
show running-config crypto
show running-config nat
show running-config route
```



```
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail 121
```

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）。