在FMC管理的FTD上設定路由型站台到站台VPN通道

目錄

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隧道如何工作有基本的瞭解。
- 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：

- Cisco 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允許確定要加密或透過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。這意味著路由到IPSec隧道的所有流量都會被加密，無論源/目標子網如何。

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隧道介面(DVTI)配置，請參閱此文檔。

限制和限制

以下是FTD上基於路由的隧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）。
- 為VPN分類流量的VTI介面支援靜態路由和僅BGP動態路由協定（不支援OSPF、RIP等其它協定）。
- 每個介面僅支援100個VTI。
- FTD叢集不支援VTI。
- 以下策略不支援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提議中不受支援。
- IKE策略不支援MD5完整性。
- IKE策略不支援PRF MD5。
- DES、3DES、AES-GMAC、AES-GMAC-192和AES-GMAC-256加密演算法在IPsec提議中不受支援。

注意：這對於基於站點到站點路由的VPN隧道以及基於策略的VPN隧道都適用。若要將舊版FTD從FMC升級到6.7，會觸發預先驗證檢查，警告使用者有關封鎖升級之已移除密碼的變更。

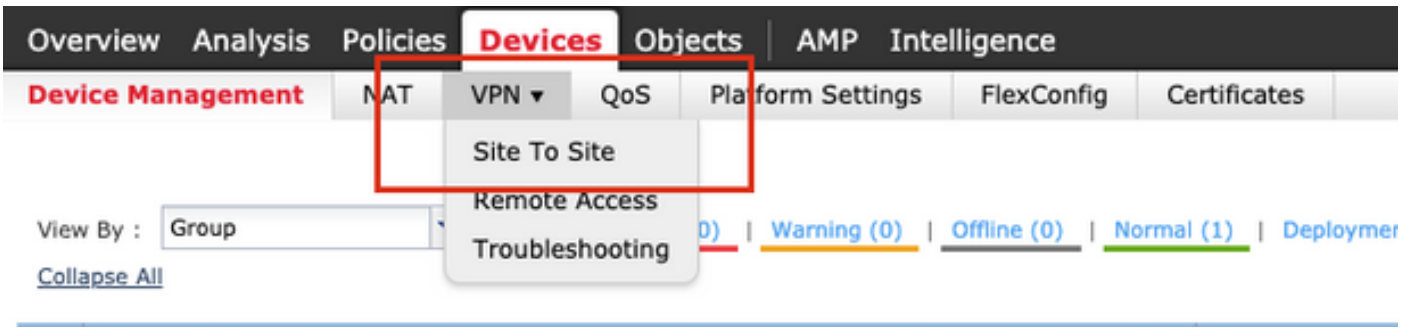
透過FMC 6.7管理的FTD 6.7	可用組態	站點到站點VPN隧道
全新安裝	弱密碼可用，但無法用於配置FTD 6.7裝置。	弱密碼可用，但無法用於配置FTD 6.7裝置。
升級：FTD僅設定弱式密碼	從FMC 6.7 UI升級，預先驗證檢查會顯示錯誤。在重新配置之前，升級會被阻止。	進行FTD升級後，並假設對等體未變更其設定，則通道會終止。
升級：FTD僅設定一些弱式密碼和某些強式密碼	從FMC 6.7 UI升級，預先驗證檢查會顯示錯誤。在重新配置之前，升級會被阻止。	FTD升級後，假設對等點具有強式密碼，然後通道重新建立。
升級：C類國家/地區（沒有強大的加密許可證）	允許DES	允許DES

.

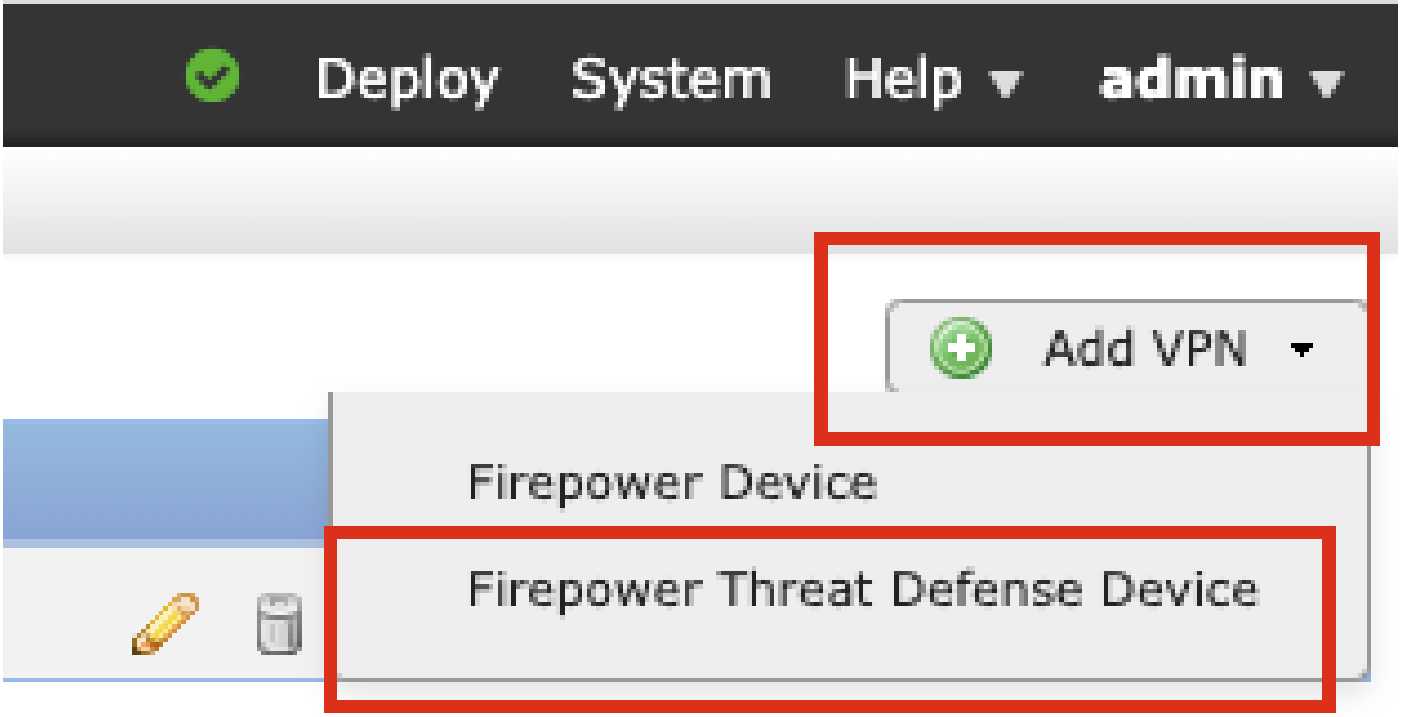
注意：不需要其他許可，可以在許可模式和評估模式下配置基於路由的VPN。 如果沒有加密規範（已啟用導出控制功能），則只有DES可用作加密演算法。

FMC的配置步驟

步驟 1.導航到裝置>VPN >站點到站點。



步驟 2.按一下Add VPN，然後選擇Firepower Threat Defense Device，如圖所示。

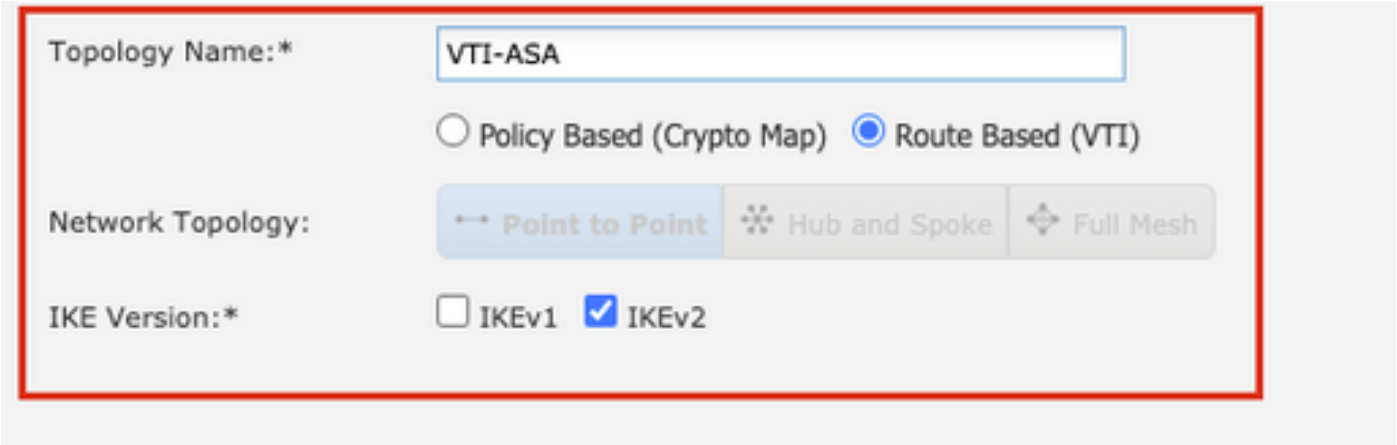


步驟 3.提供拓撲名稱並選擇基於路由(VTI)的VPN型別。選擇IKE Version。

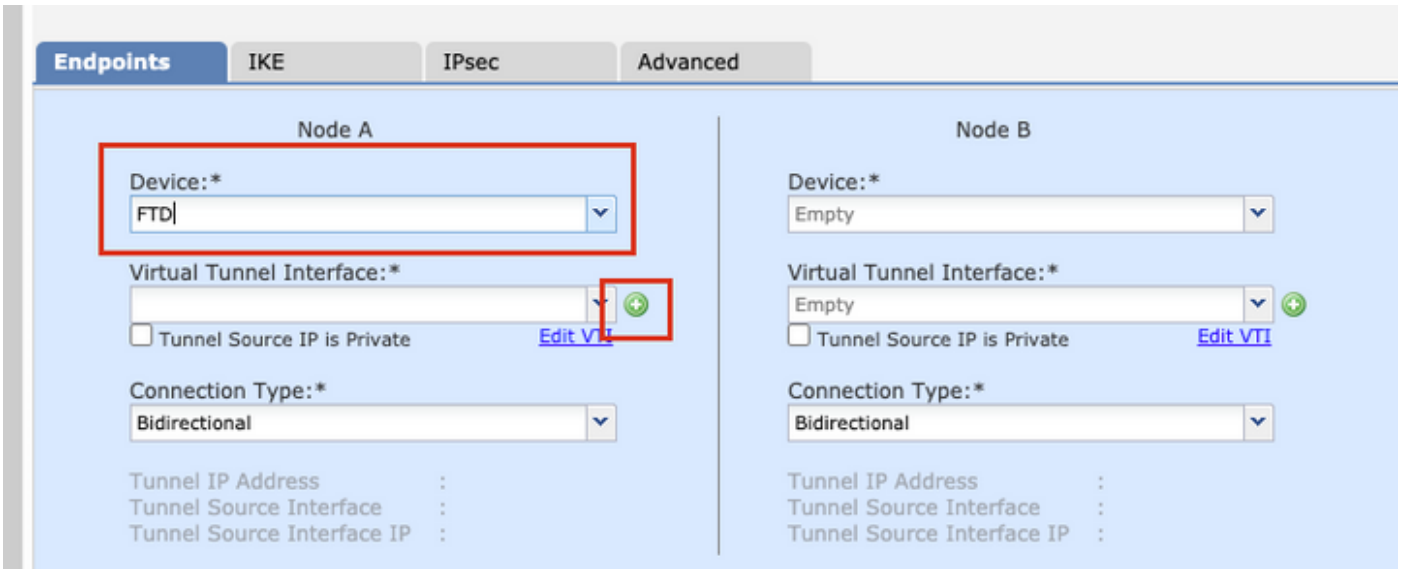
在本演示中：

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裝置，您可以選擇增加新的虛擬隧道介面(點選+圖示)，或者從清單中選擇一個已存在的介面。



步驟 5.定義新虛擬隧道介面的引數。按一下「OK」（確定）。

在本演示中：

名稱：VTI-ASA

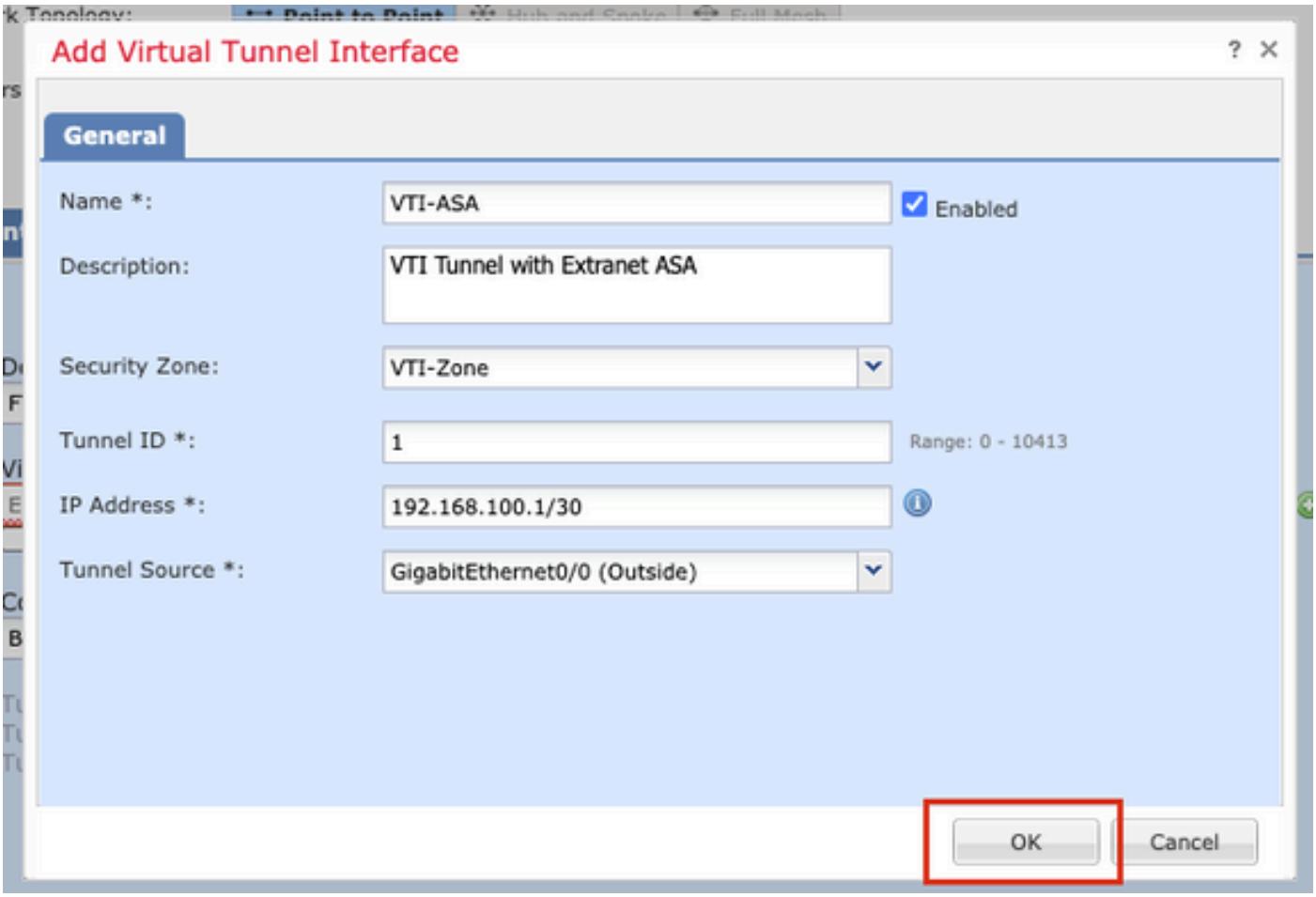
說明（可選）：VTI隧道和外聯網ASA

安全區域：VTI-Zone

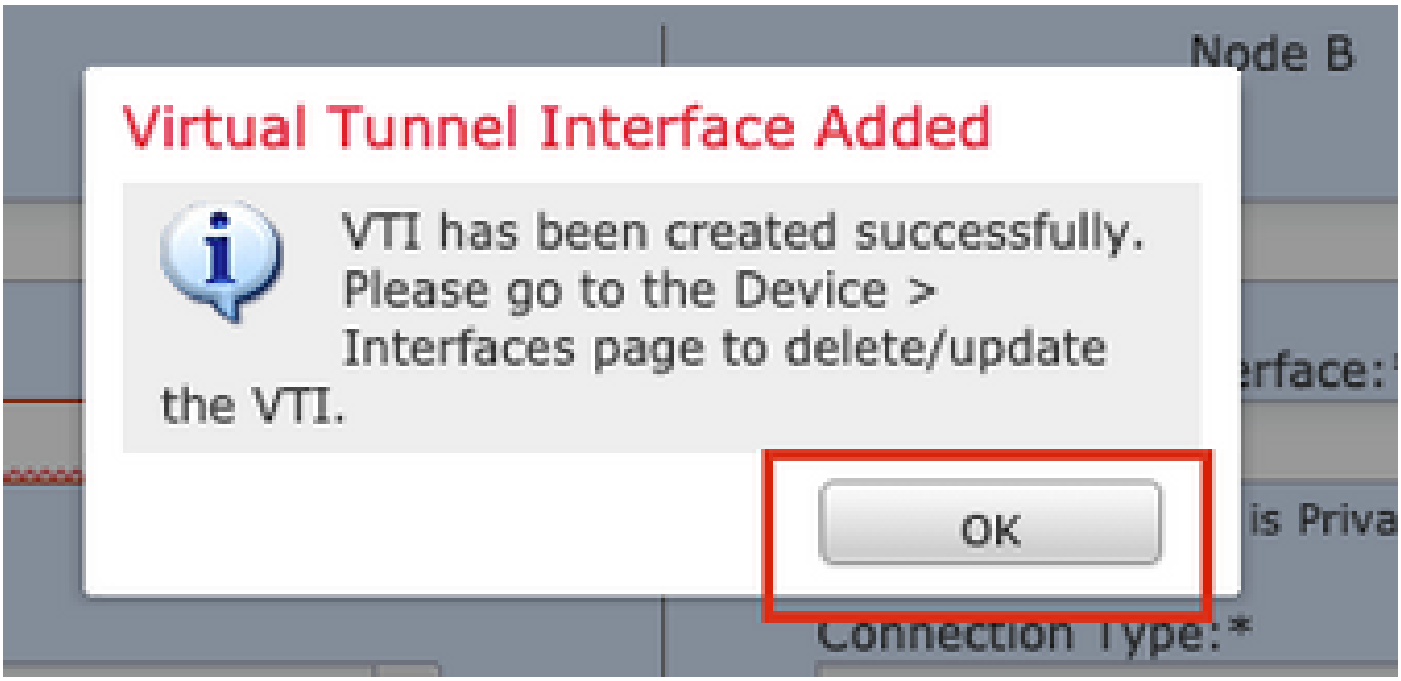
通道ID：1

IP地址：192.168.100.1/30

隧道源：GigabitEthernet0/0（外部）



步驟 6.點選彈出窗口中的OK，通知已建立新的VTI。



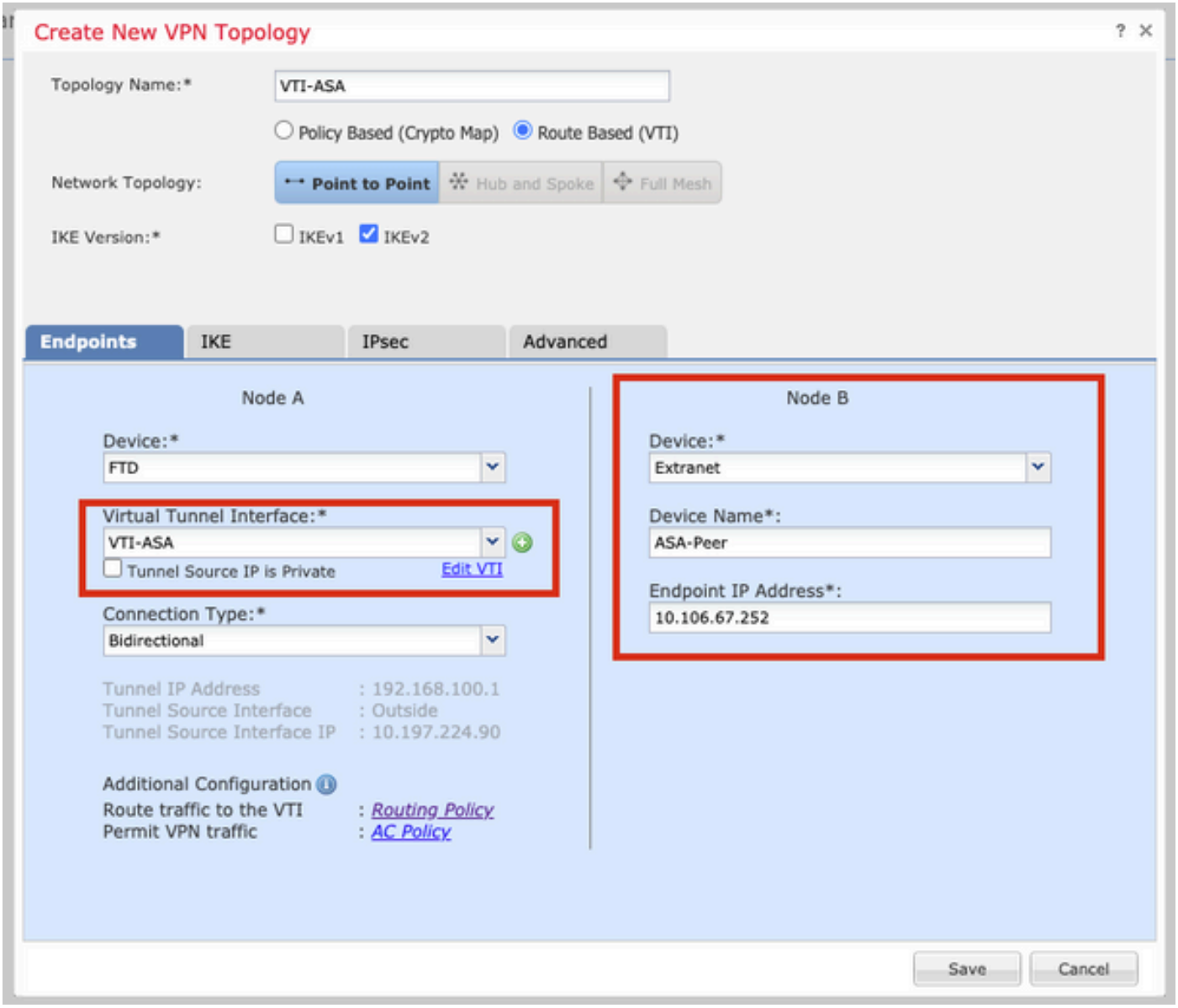
步驟 7.選擇新建立的VTI或虛擬隧道介面下存在的VTI。提供節點B（對等裝置）的資訊。

在本演示中：

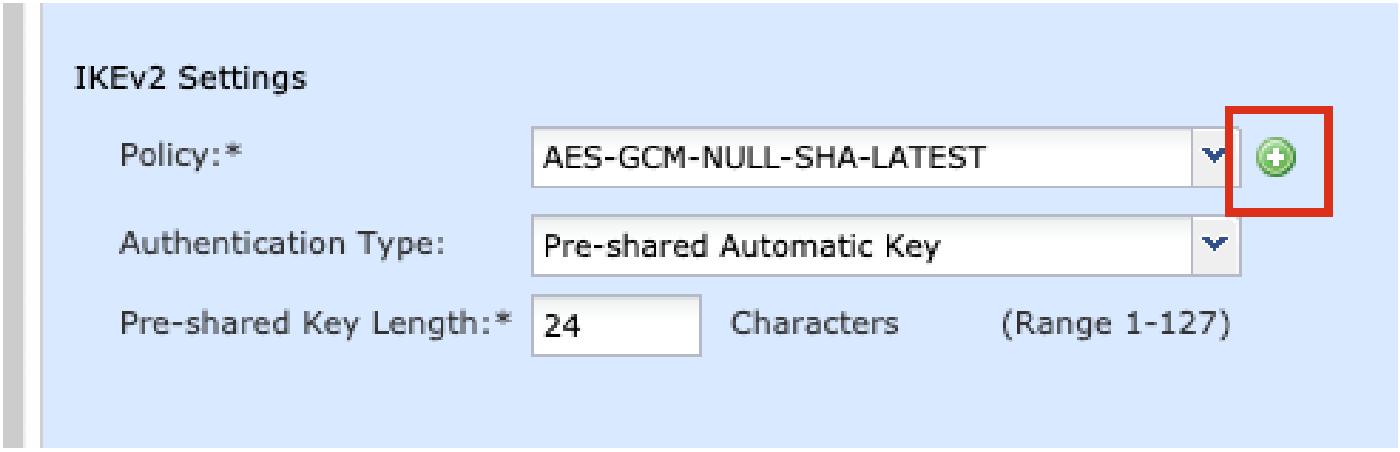
裝置：Extranet

裝置名稱：ASA-Peer

終端IP地址：10.106.67.252



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



第9步：（如果建立新的IKEv2策略，則可選。）為策略提供名稱並選擇要用於策略的演算法。按一下Save。

在本演示中：

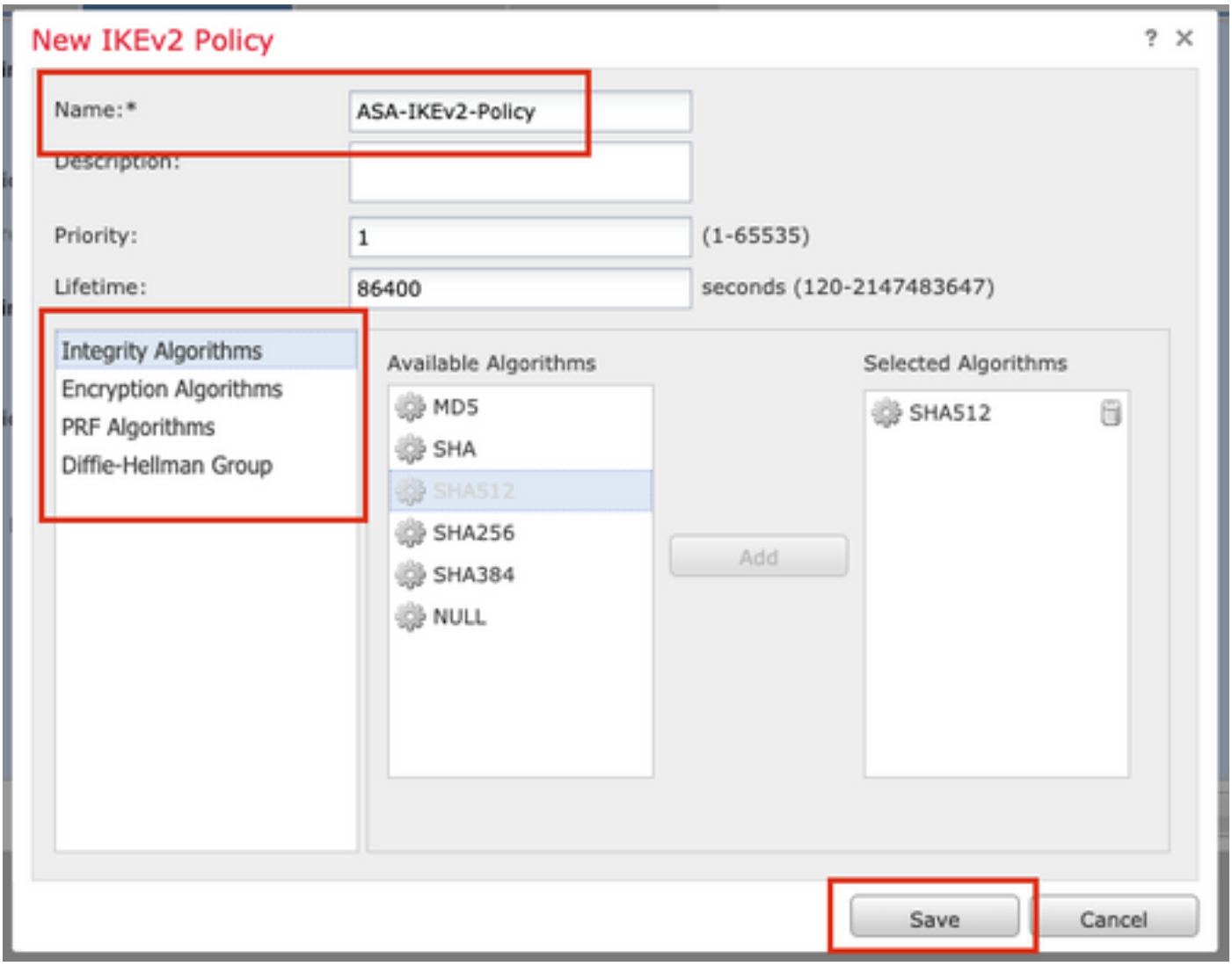
名稱：ASA-IKEv2-Policy

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



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。

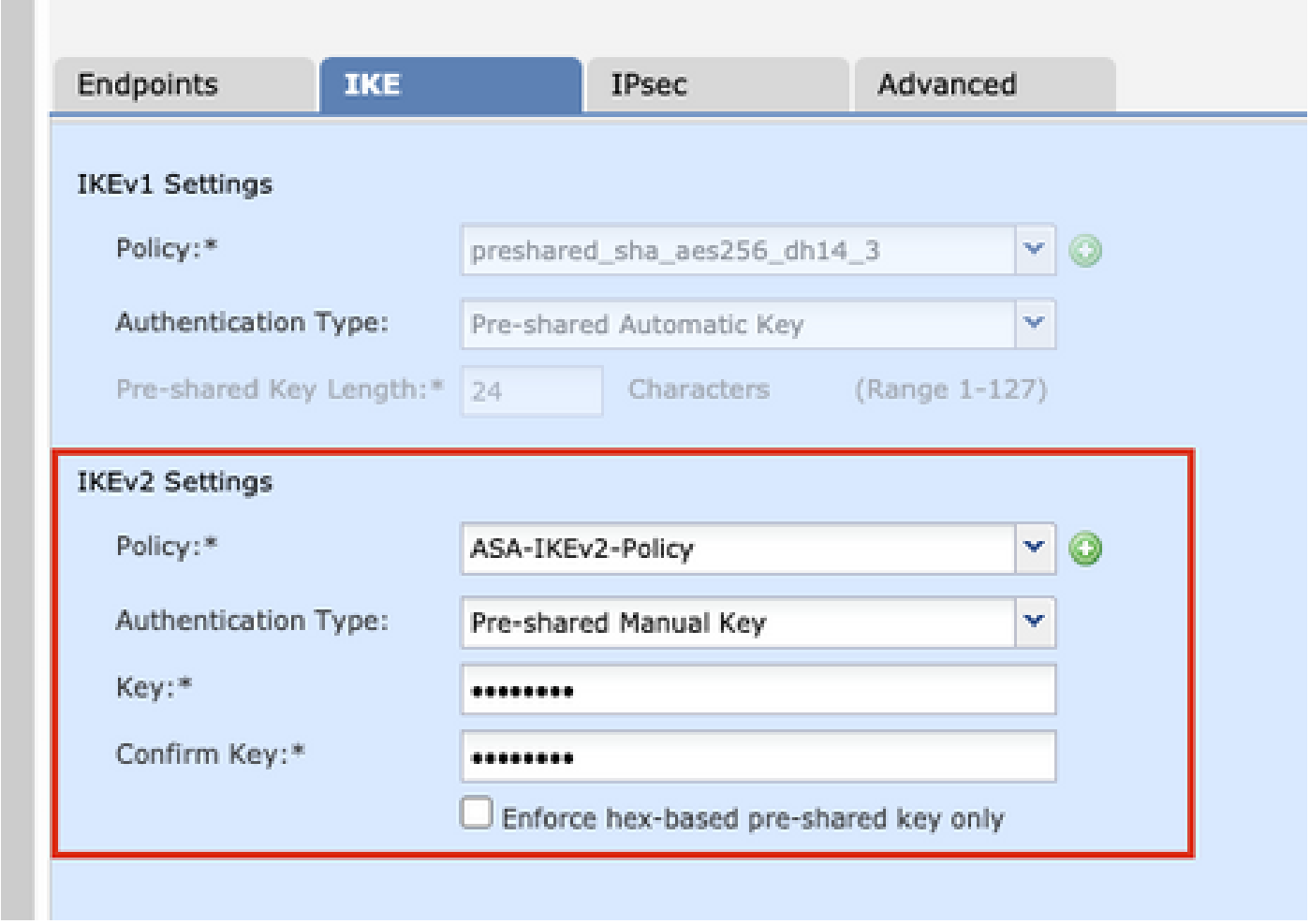
在本演示中：

策略：ASA-IKEv2-Policy

驗證型別：預先共用手動金鑰

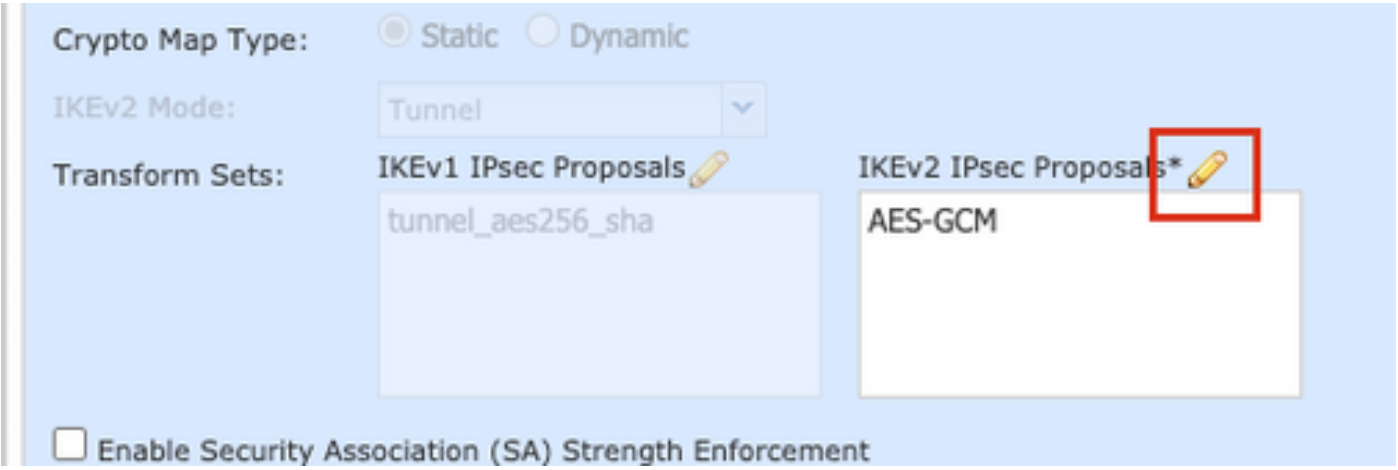
金鑰：cisco123

確認金鑰：cisco123



注意：如果兩個終端在同一FMC上註冊，還可以使用預共用自動金鑰選項。

步驟 11.導航到IPsec頁籤。 您可以選擇使用預定義的IKEv2 IPsec建議或建立新建議。點選IKEv2 IPsec Proposal頁籤旁的Edit按鈕。



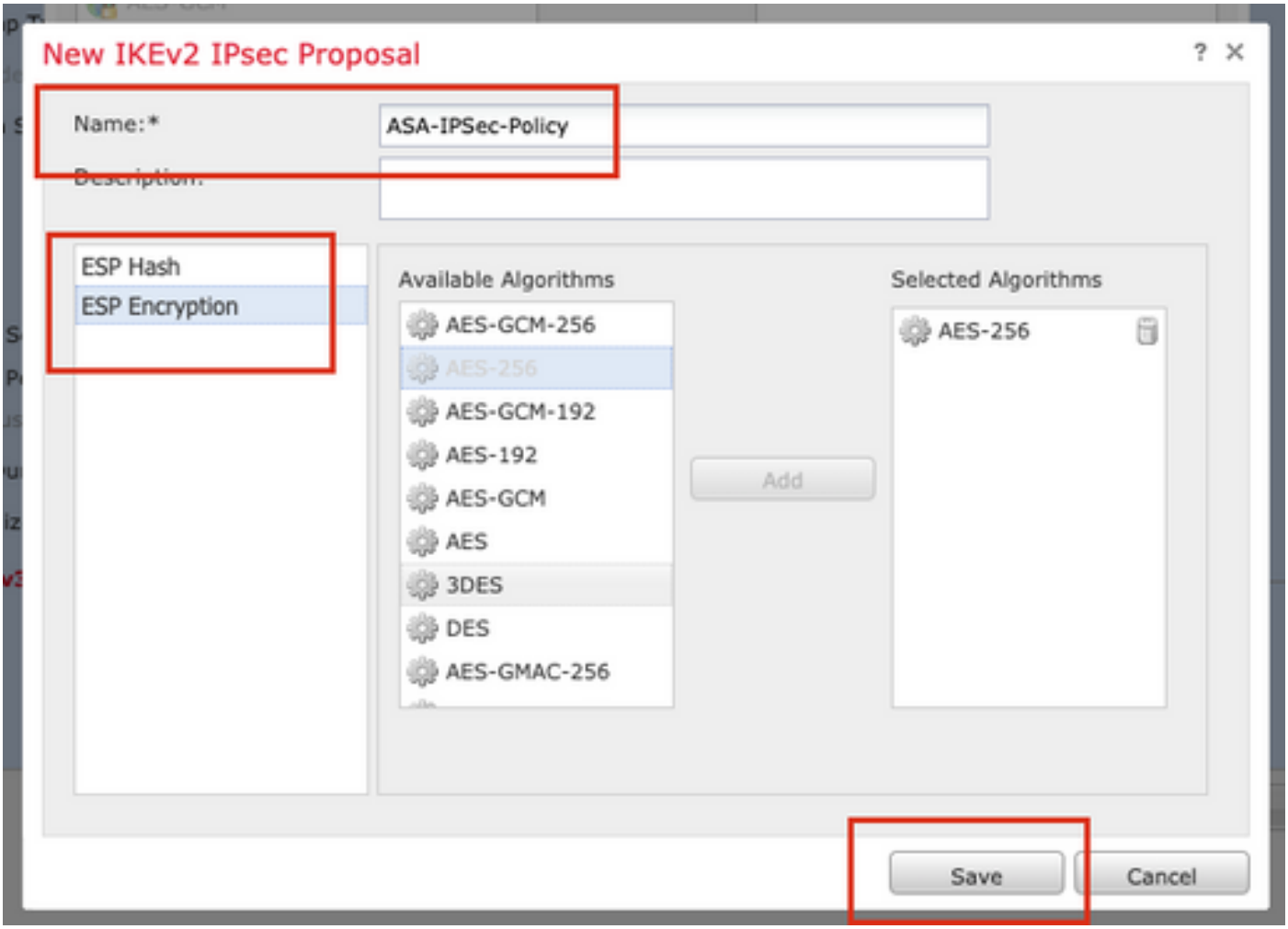
第12步：（可選，如果您建立新的IKEv2 IPsec提議。）為建議提供名稱，並選擇建議中所用的演算法。按一下Save。

在本演示中：

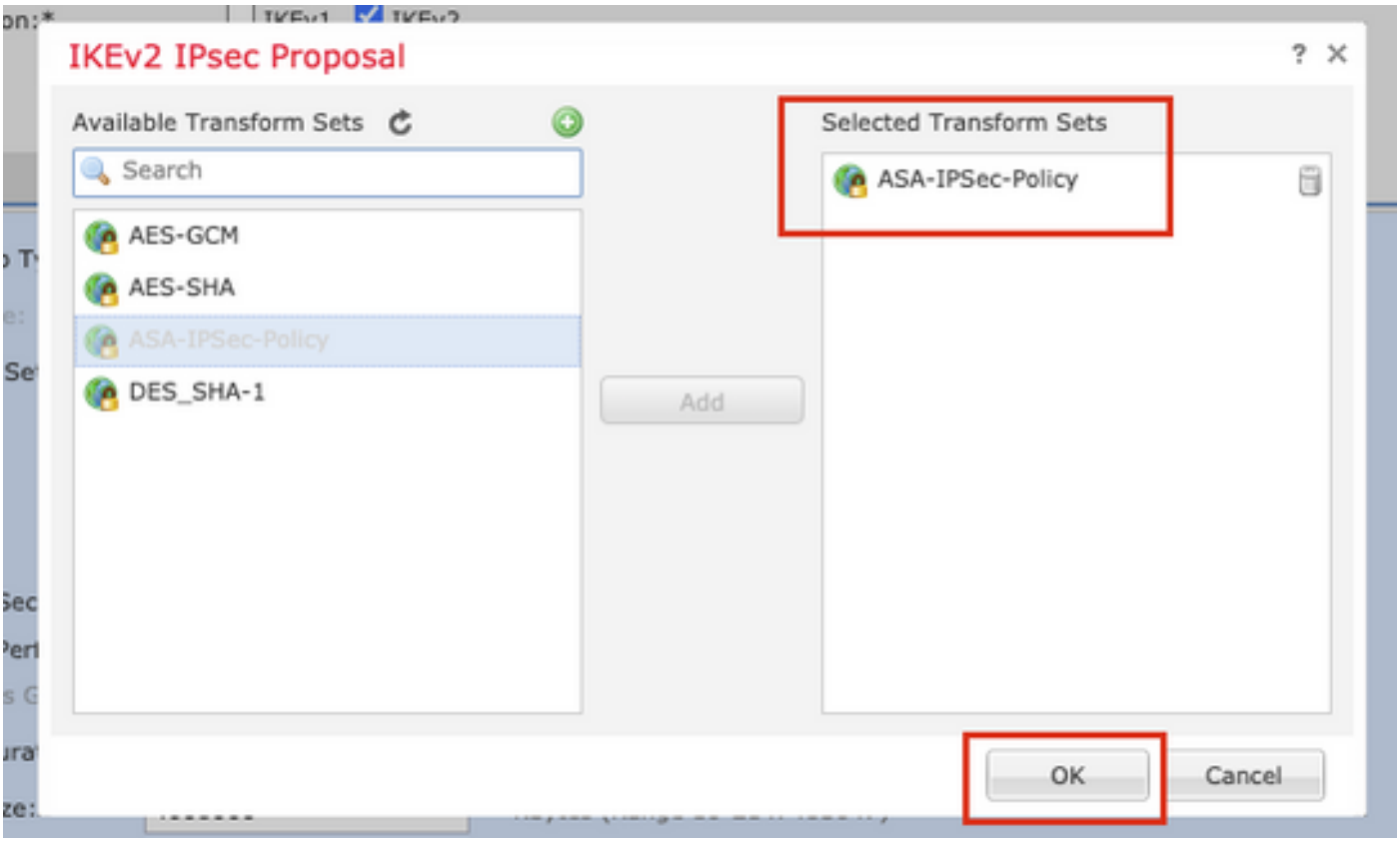
名稱：ASA-IPSec-Policy

ESP雜湊：SHA-512

ESP加密：AES-256



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



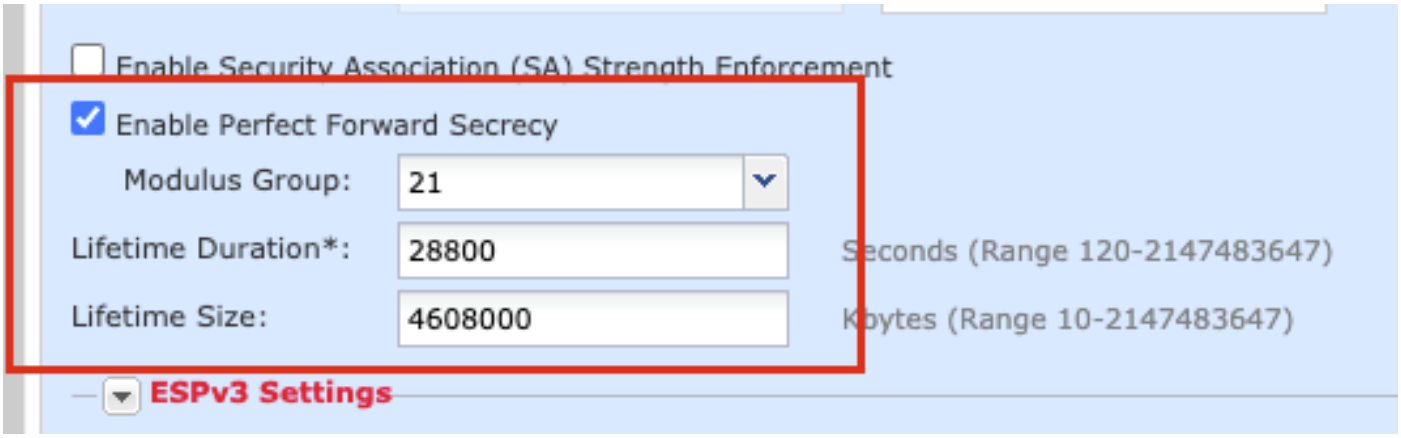
步驟14.（選擇性）選擇「完全向前保密」設定。配置IPSec生存期持續時間和生存期大小。

在本演示中：

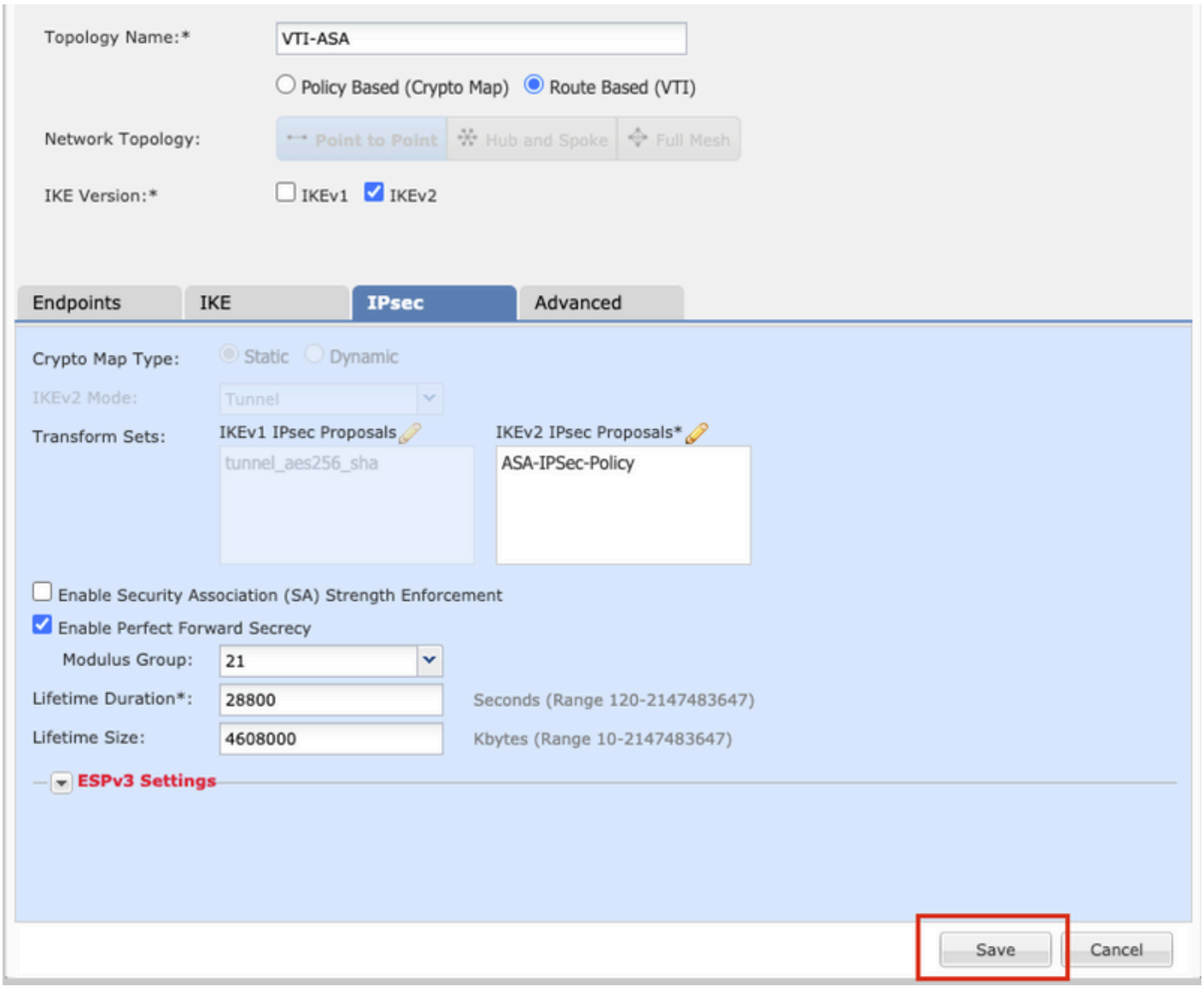
完全正向保密：模陣列21

存留期期間：28800（預設）

存留時間大小： 4608000（預設）



步驟 15.檢查配置的設定。按一下Save，如下圖所示。



步驟 16.配置訪問控制策略。導航到策略>訪問控制>訪問控制。編輯套用至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。

在網路頁籤中輸入源網路和目標網路。按一下Add。

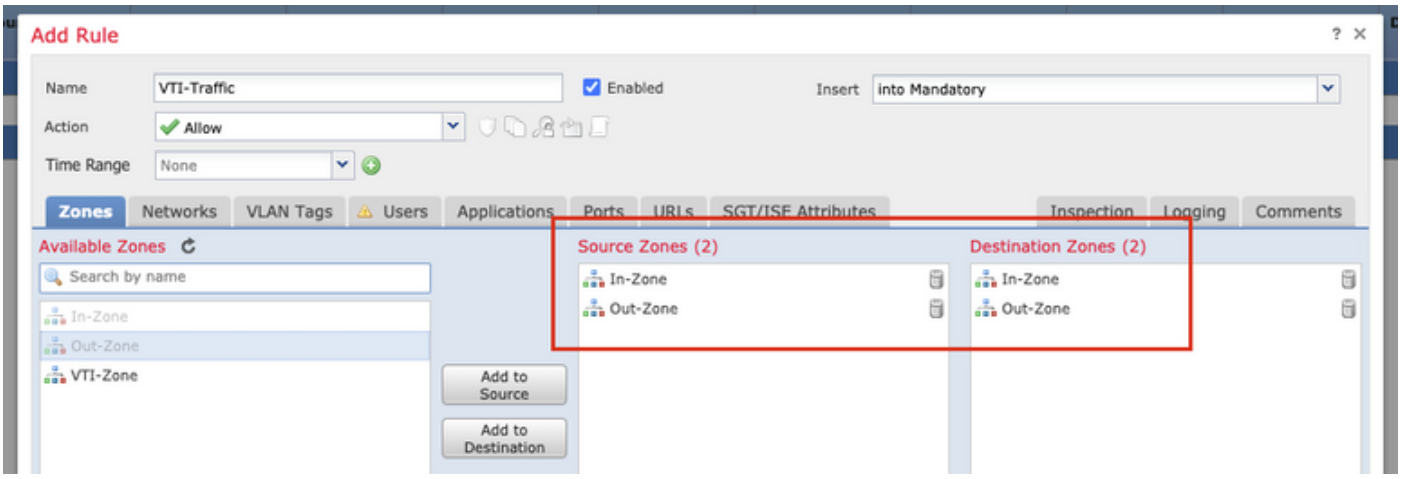
在本演示中：

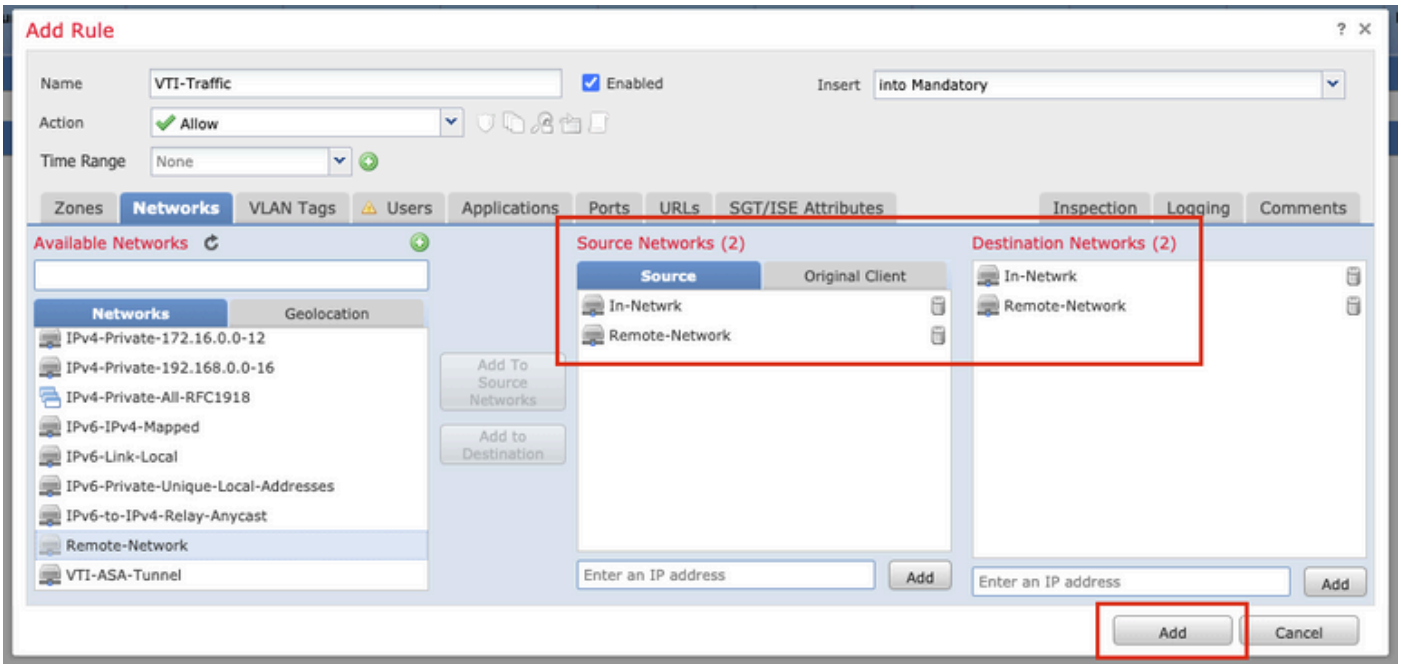
來源區域：區域內與區外

目標區域：區域外和區域內

源網路：內聯網和遠端網路

目的網路：遠端網路和內聯網





步驟 17.透過VTI隧道增加路由。導航到裝置>裝置管理。編輯配置VTI隧道的裝置。

導航到Routing 頁籤下的Static Route。按一下Add Route。

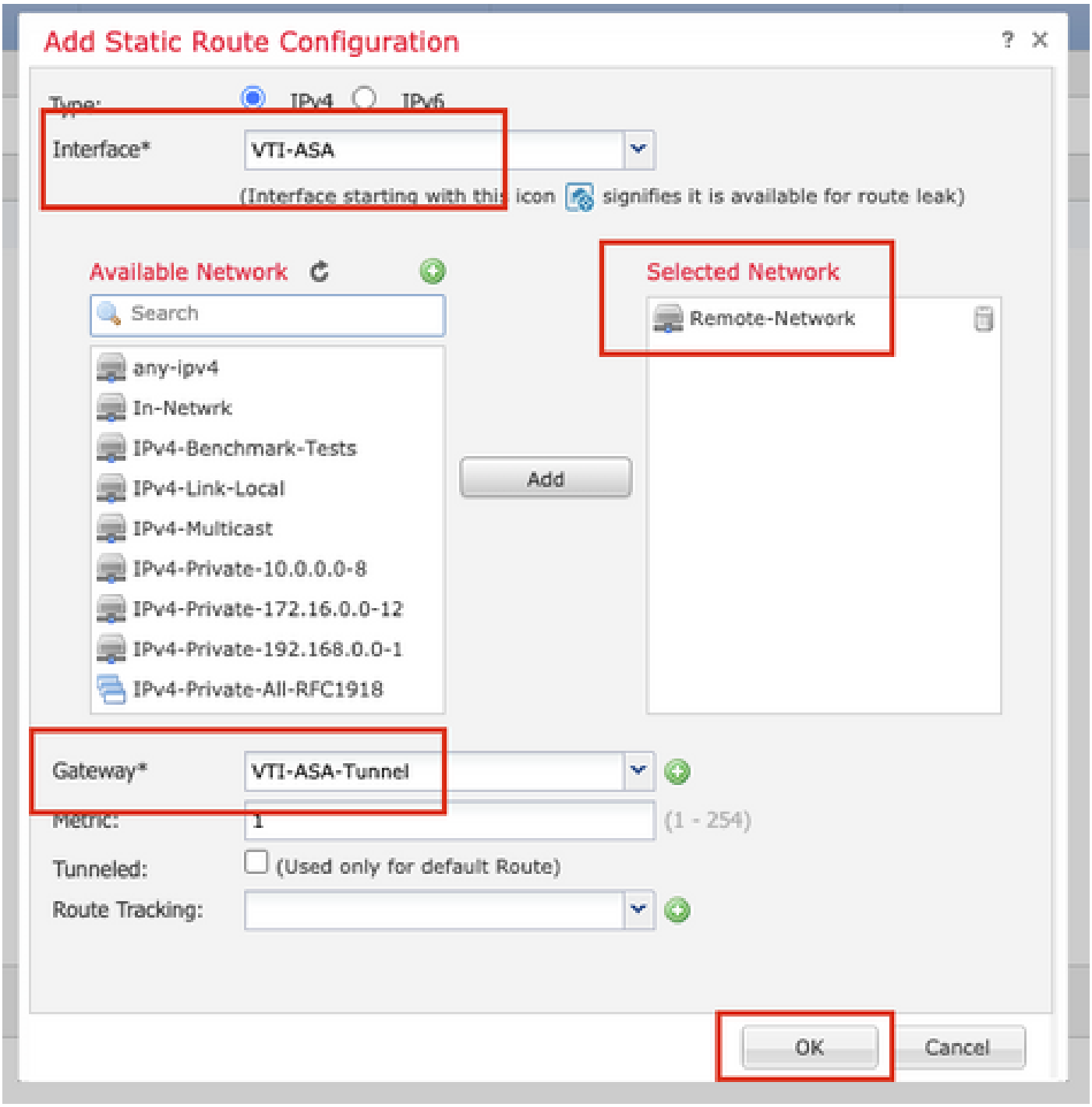
提供介面，選擇網路，提供網關。按一下「OK」（確定）。

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。選擇需要將配置部署到的FTD，然後按一下Deploy。

成功部署後，組態已推送到FTD CLI：

<#root>

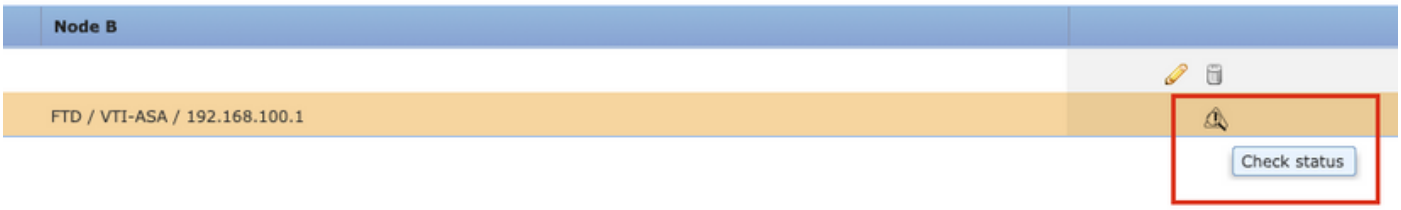
```
crypto ikev2 policy 1


 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

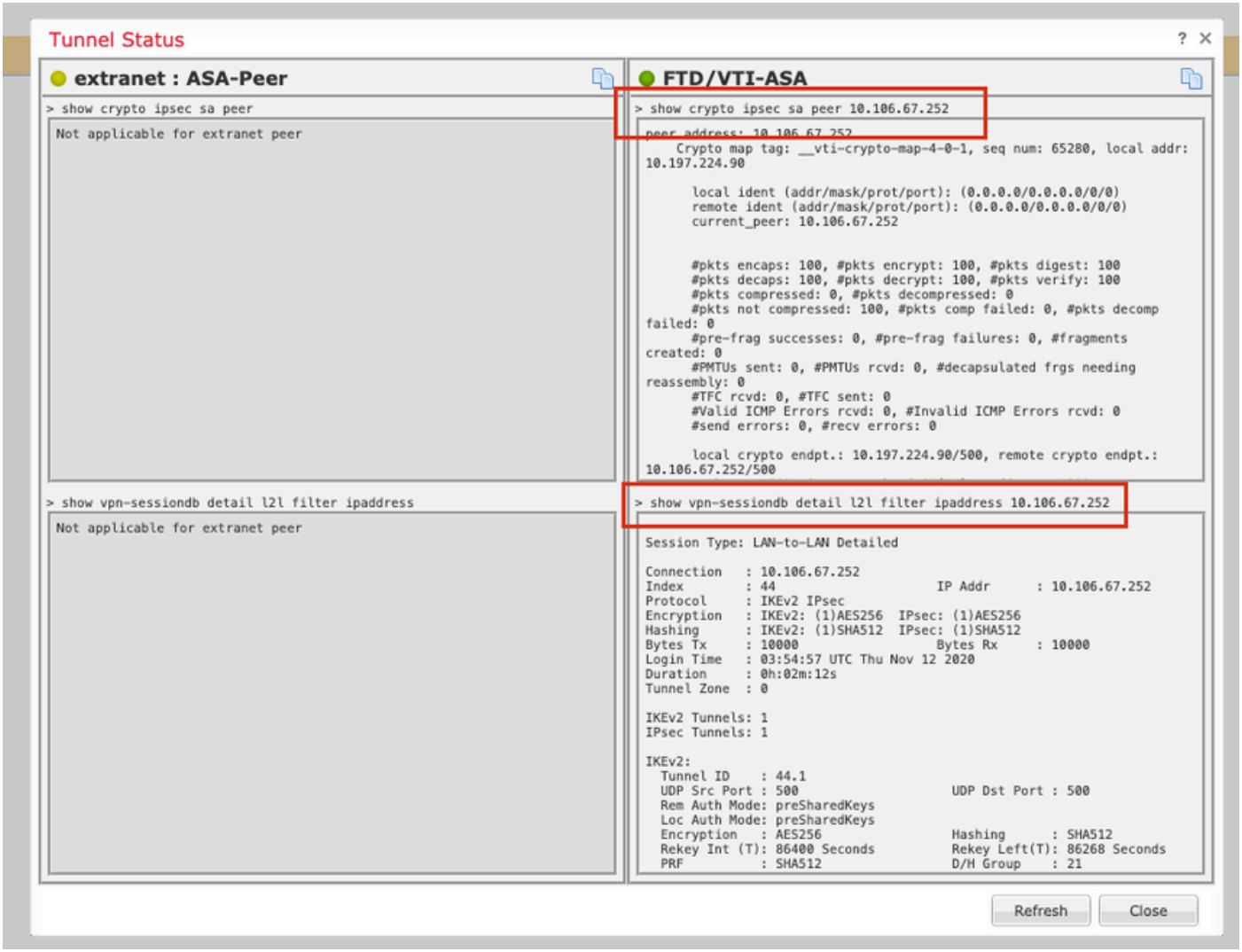
從FMC GUI

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取得的以下命令：

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



從FTD CLI

這些命令可從FTD CLI中使用，以檢視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 l2l
```