在FDM管理的FTD上使用靜態路由配置基於路由的VPN

目錄

簡介

本檔案介紹如何在FDM管理的FTD上設定靜態路由型站對站VPN通道。

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。
- 預先瞭解通過Firepower裝置管理器(FDM)的導航。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 由Firepower裝置管理器(FDM)管理的Cisco Firepower威脅防禦(FTD)版本7.0。

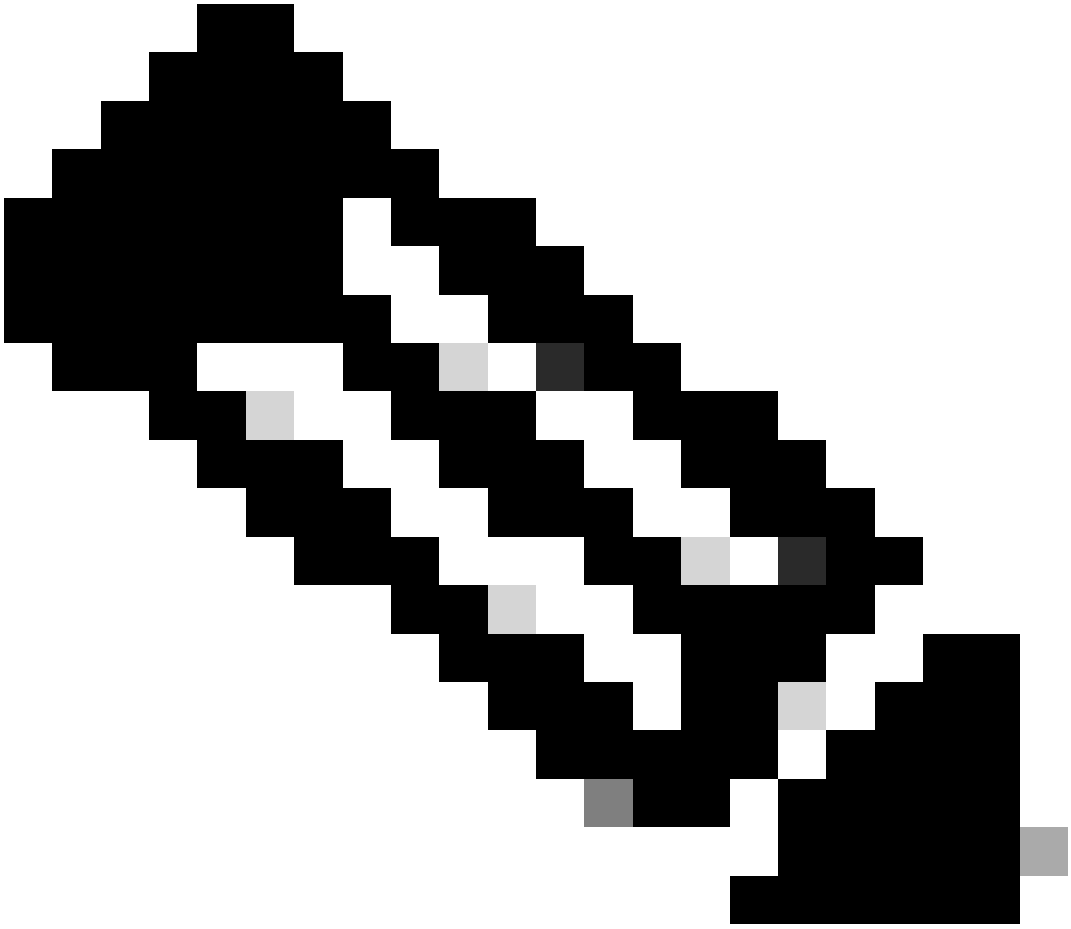
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

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。

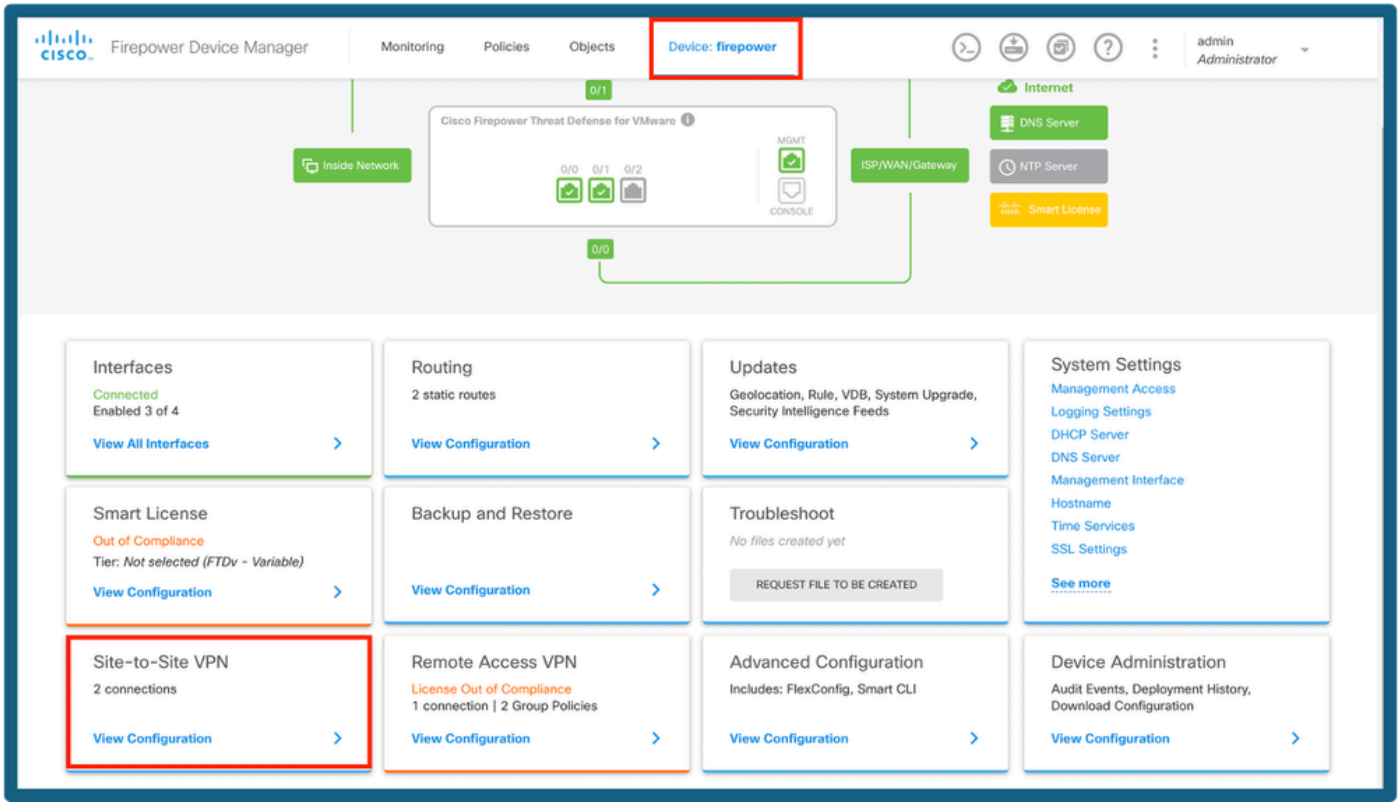
本檔案將重點介紹靜態虛擬通道介面(SVTI)組態。



附註：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。如果沒有加密合規（已啟用匯出控制功能），只有DES可用作加密演算法。

FDM的配置步驟

步驟1。導覽至Device > Site To Site。



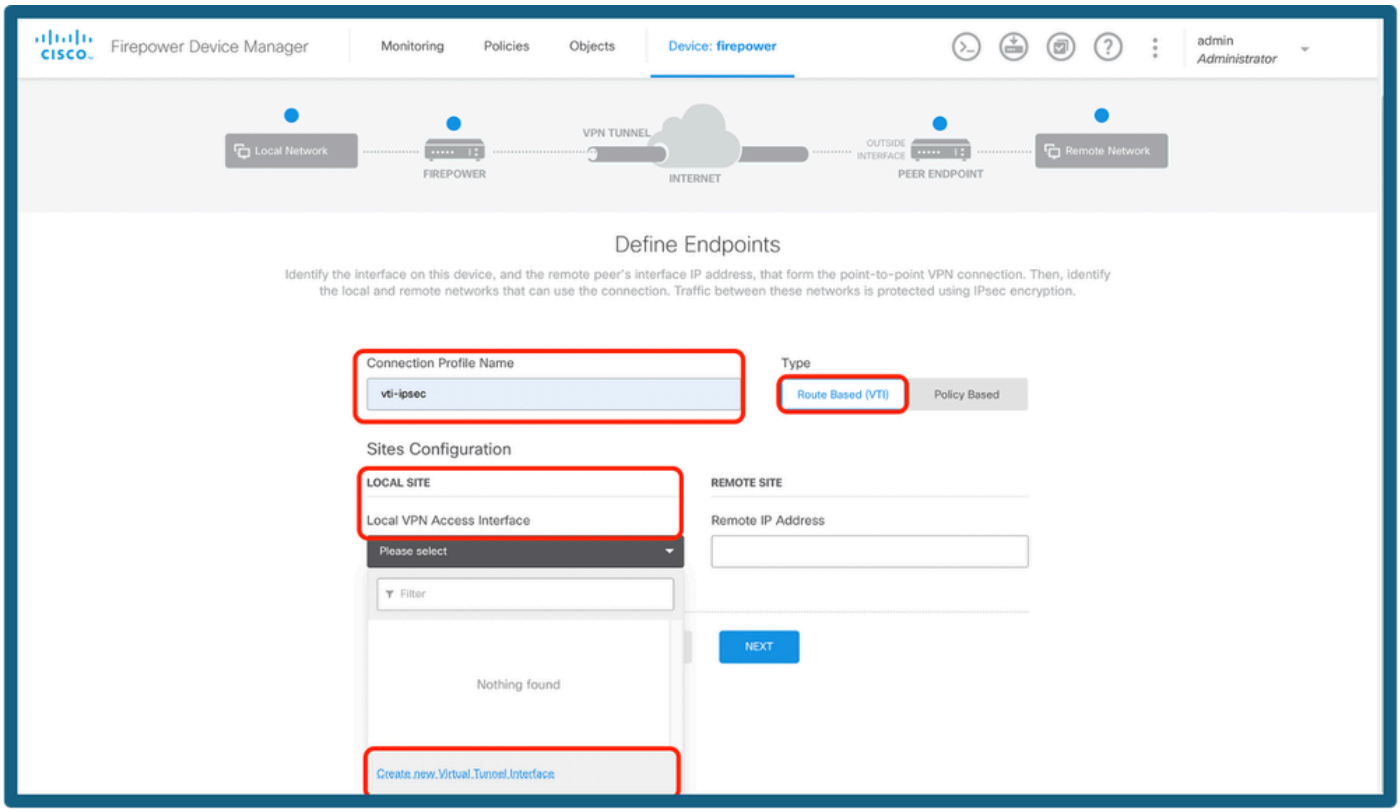
FDM儀表板

步驟2.按一下+圖示將新站點新增到站點連線。

新增S2S連線

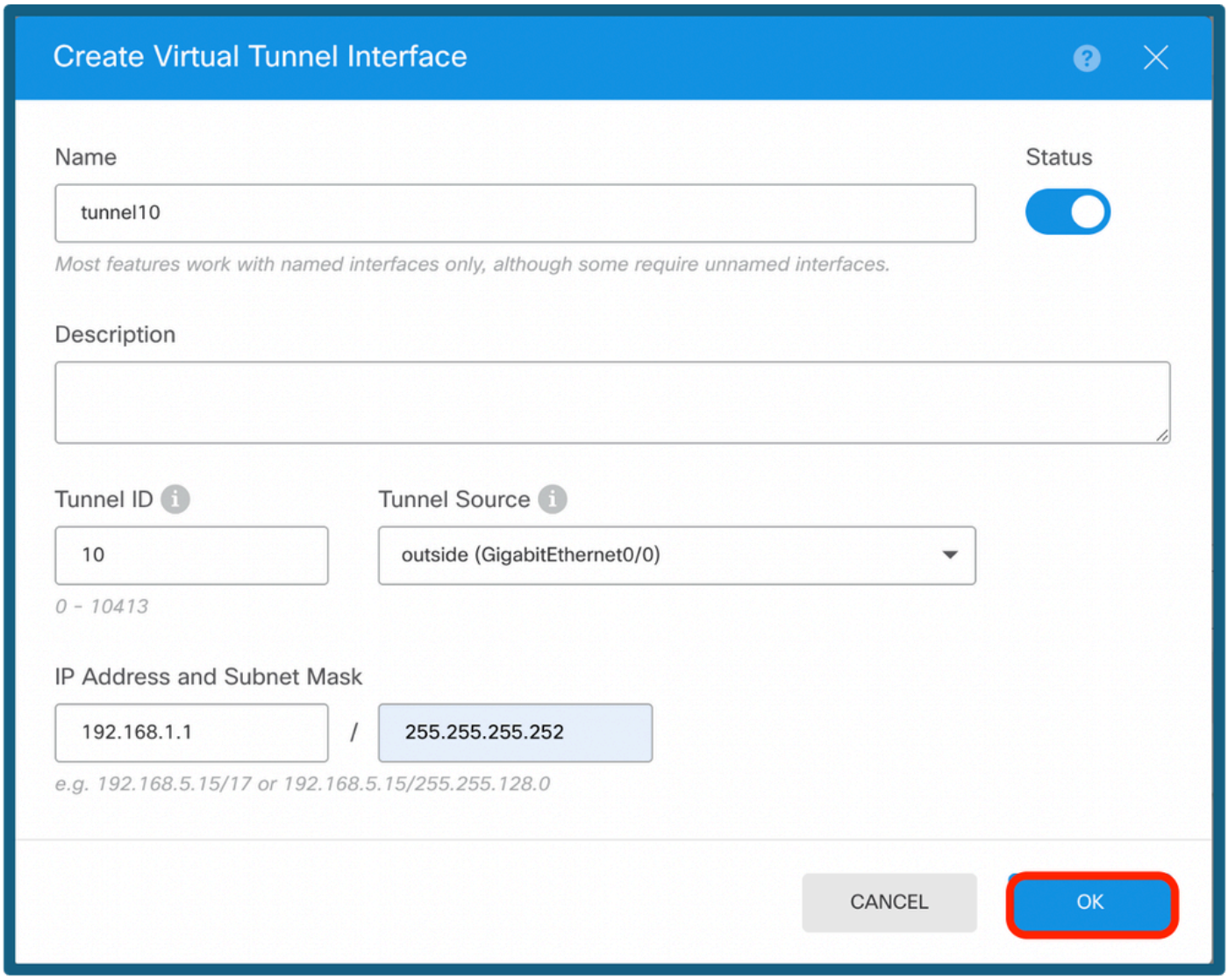
步驟3.提供拓撲名稱並選擇VPN的型別作為基於路由(VTI)。

按一下Local VPN Access Interface，然後按一下Create new Virtual Tunnel Interface或從現有清單中選擇一個。



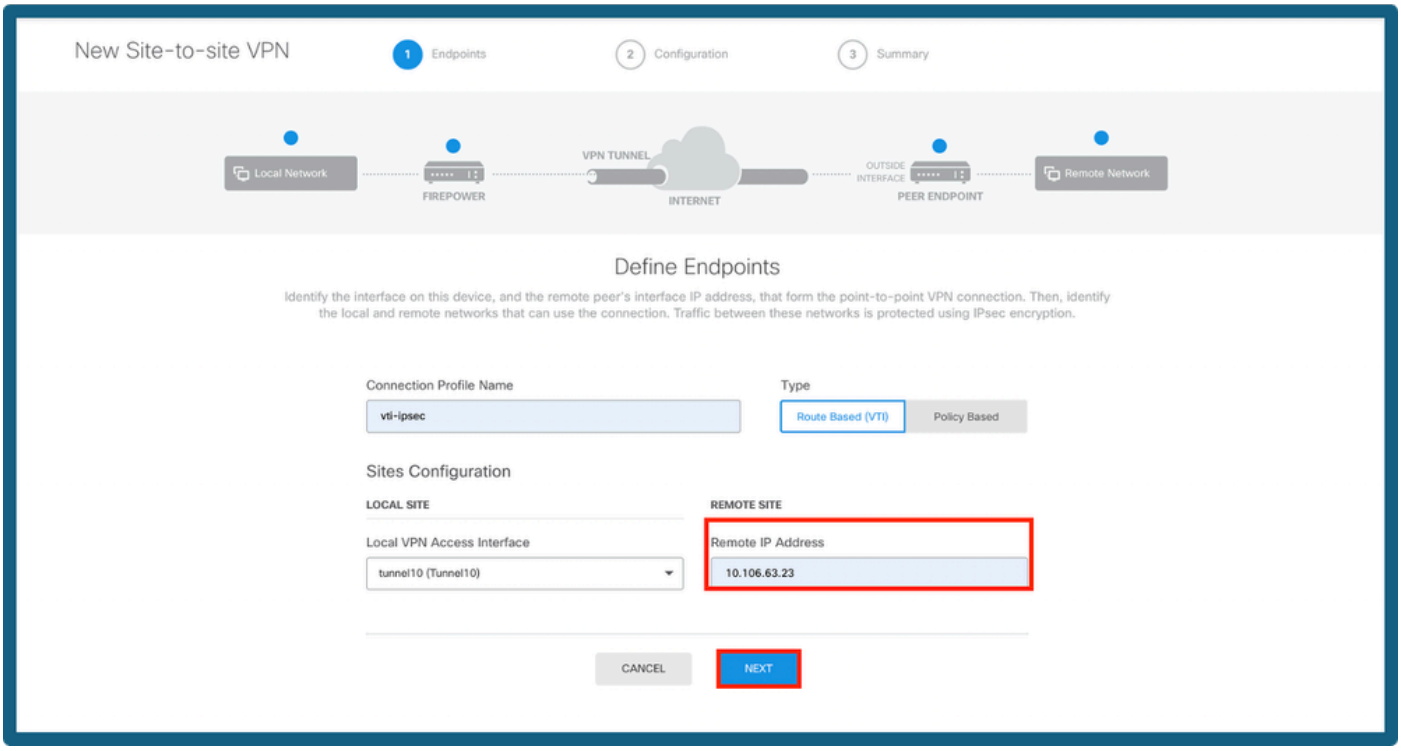
新增隧道介面

步驟4.定義新虛擬通道介面的引數。按一下「OK」（確定）。



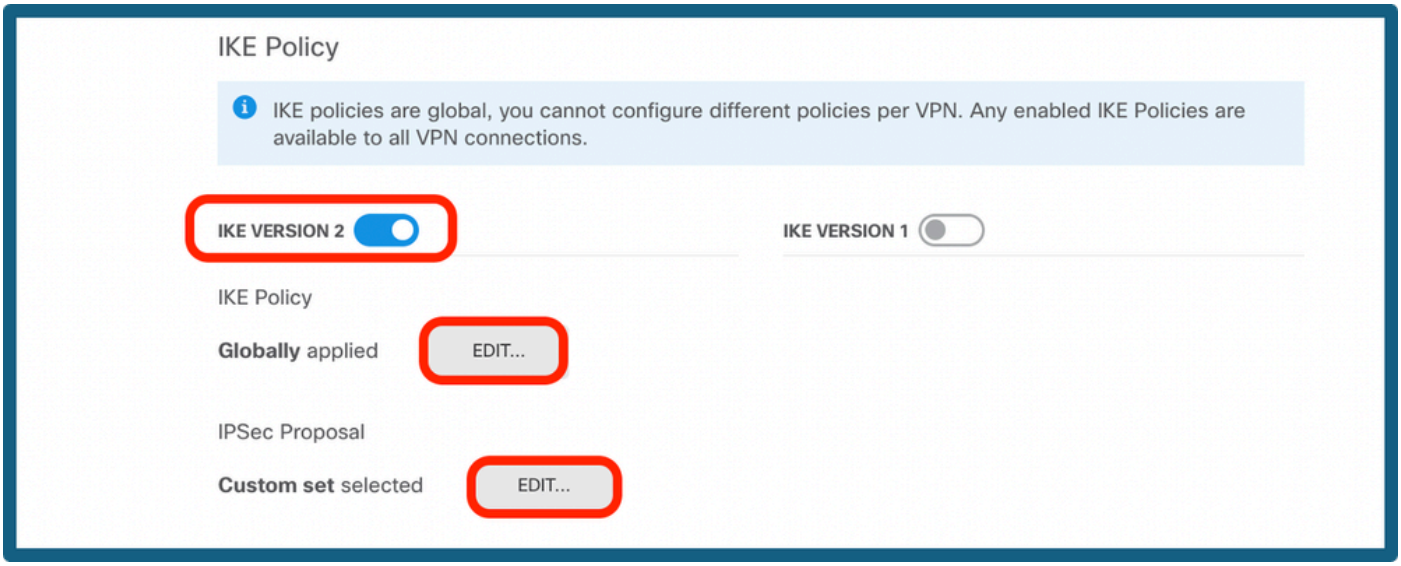
VTI配置

步驟5.選擇新建立的VTI或虛擬通道介面下存在的VTI。提供遠端IP地址。



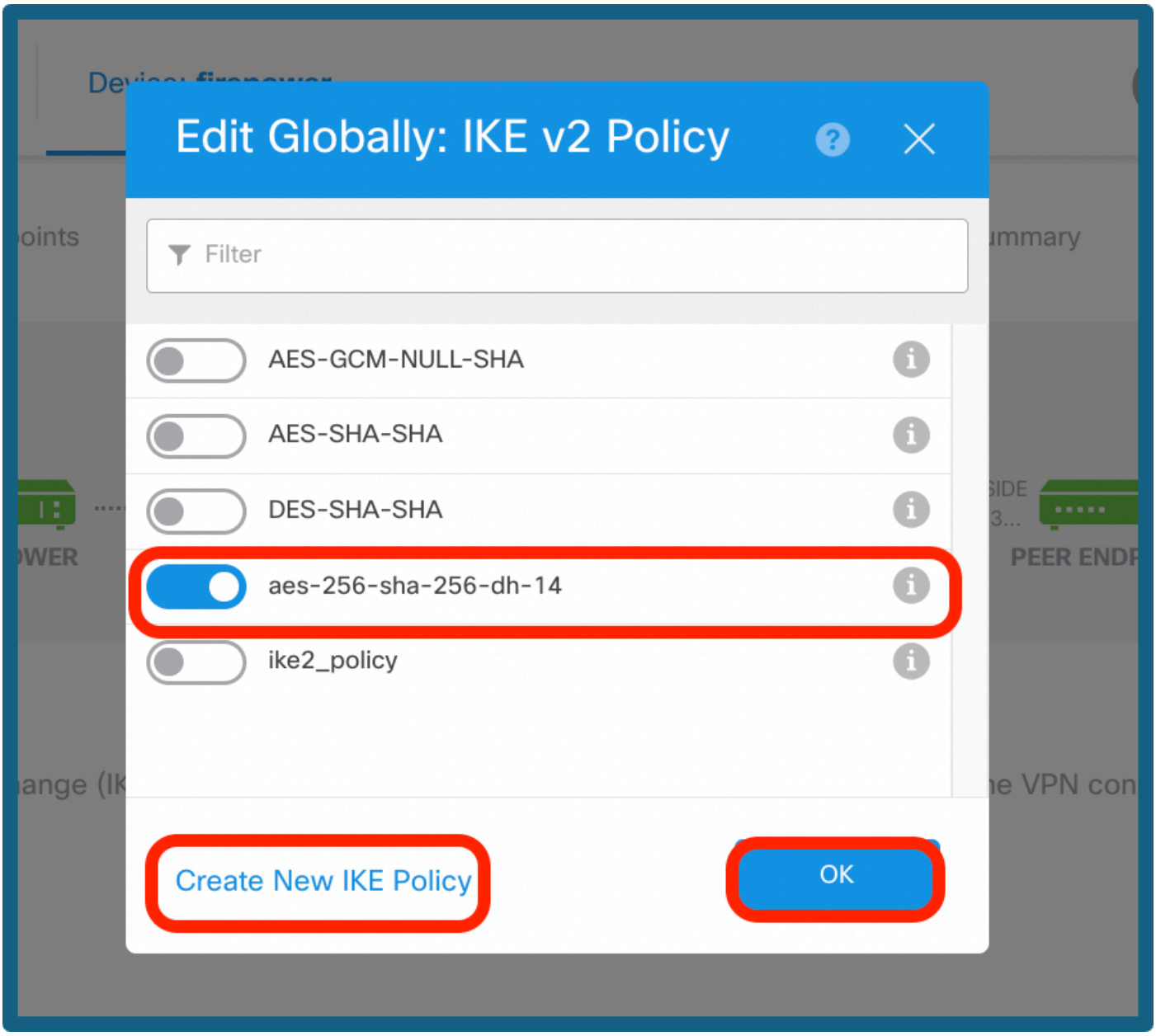
新增對等IP

步驟6.選擇IKE版本，然後選擇Edit按鈕以設定IKE和IPsec引數，如下圖所示。

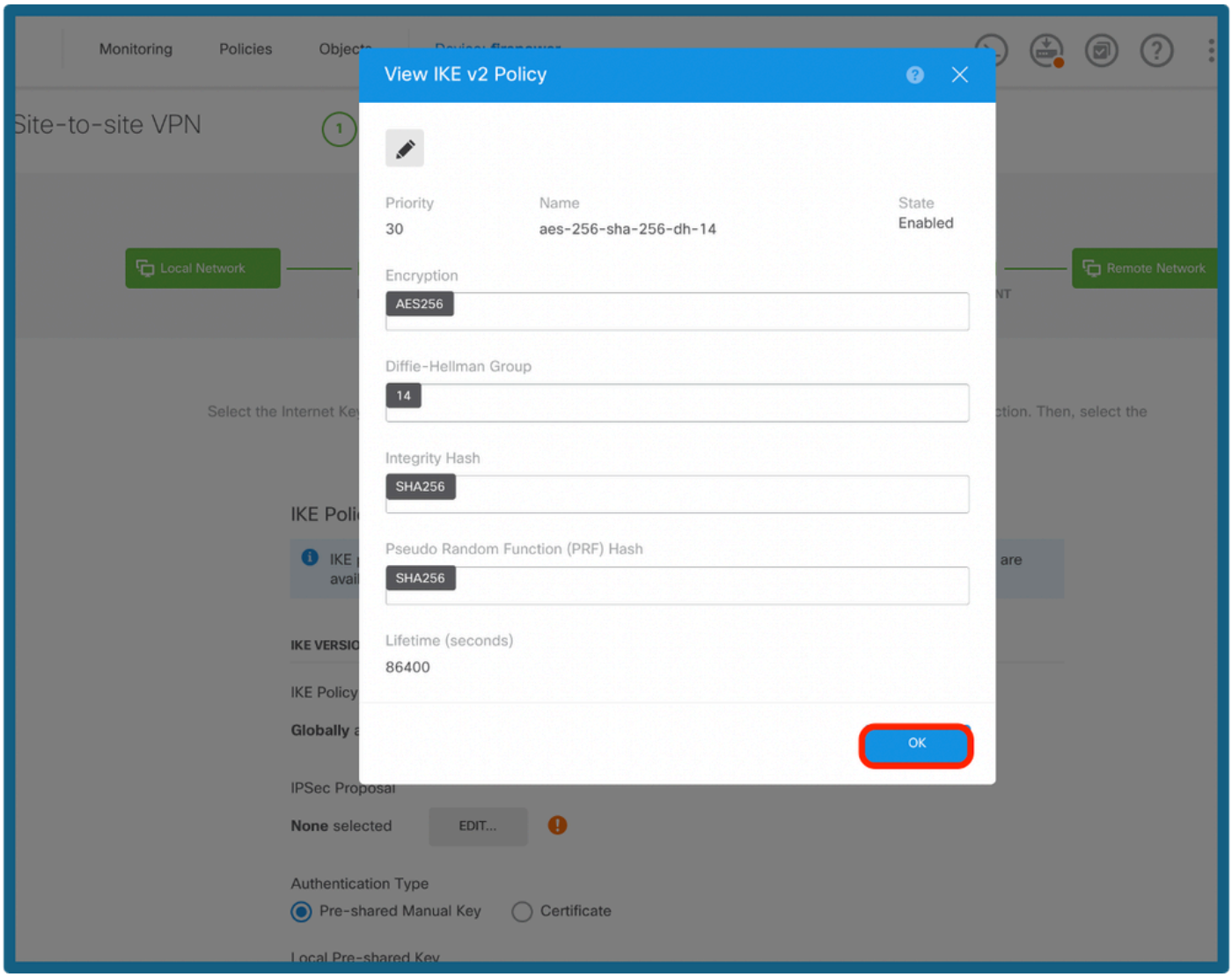


配置IKE版本

步驟7a.選擇IKE Policy按鈕（如圖所示），然後按一下ok按鈕或Create New IKE Policy（如果要建立新策略）。

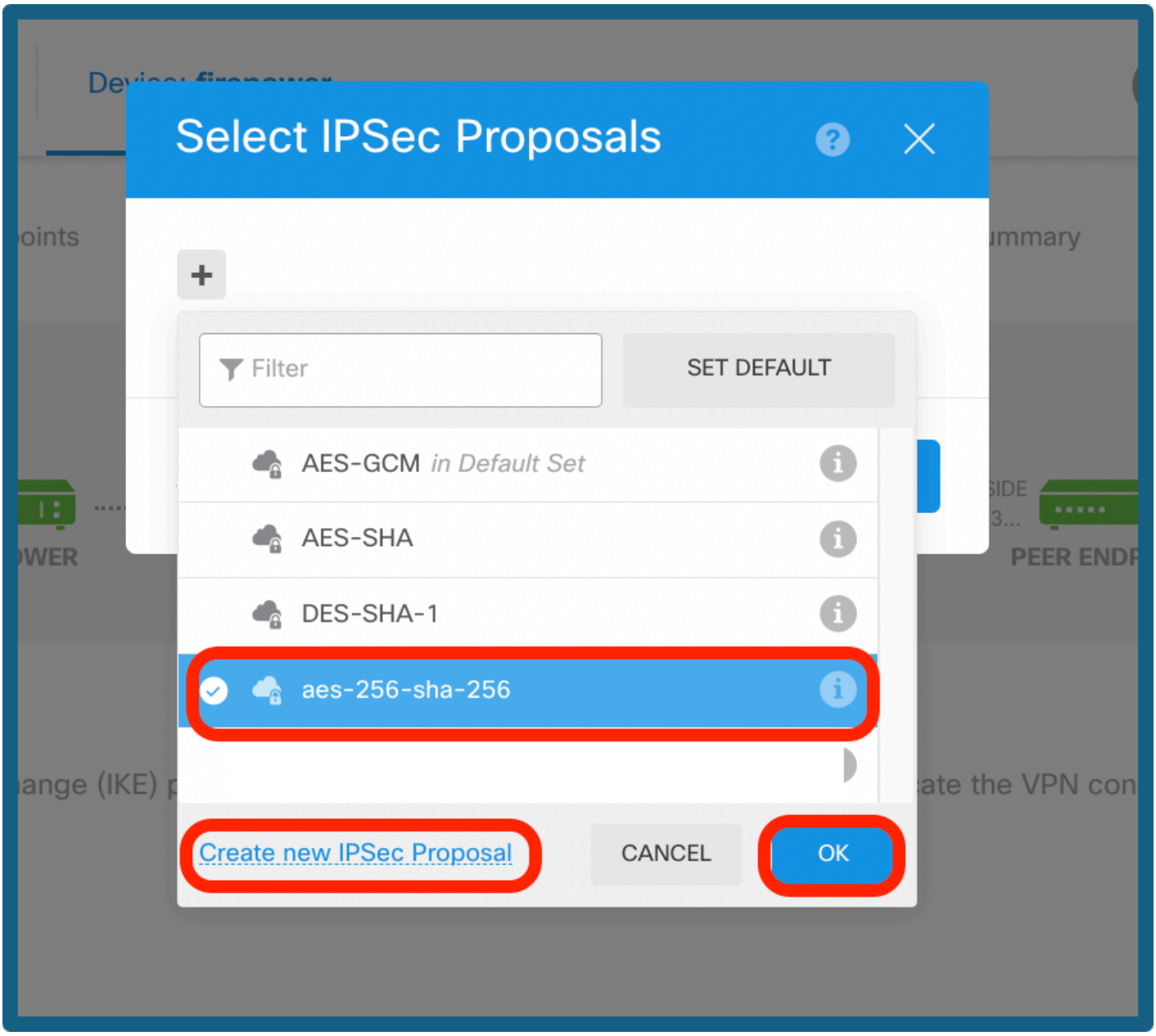

Edit Globally: IKE v2 Policy
Filter
AES-GCM-NULL-SHA
AES-SHA-SHA
DES-SHA-SHA
aes-256-sha-256-dh-14
ike2_policy
Create New IKE Policy
OK

選擇IKE策略

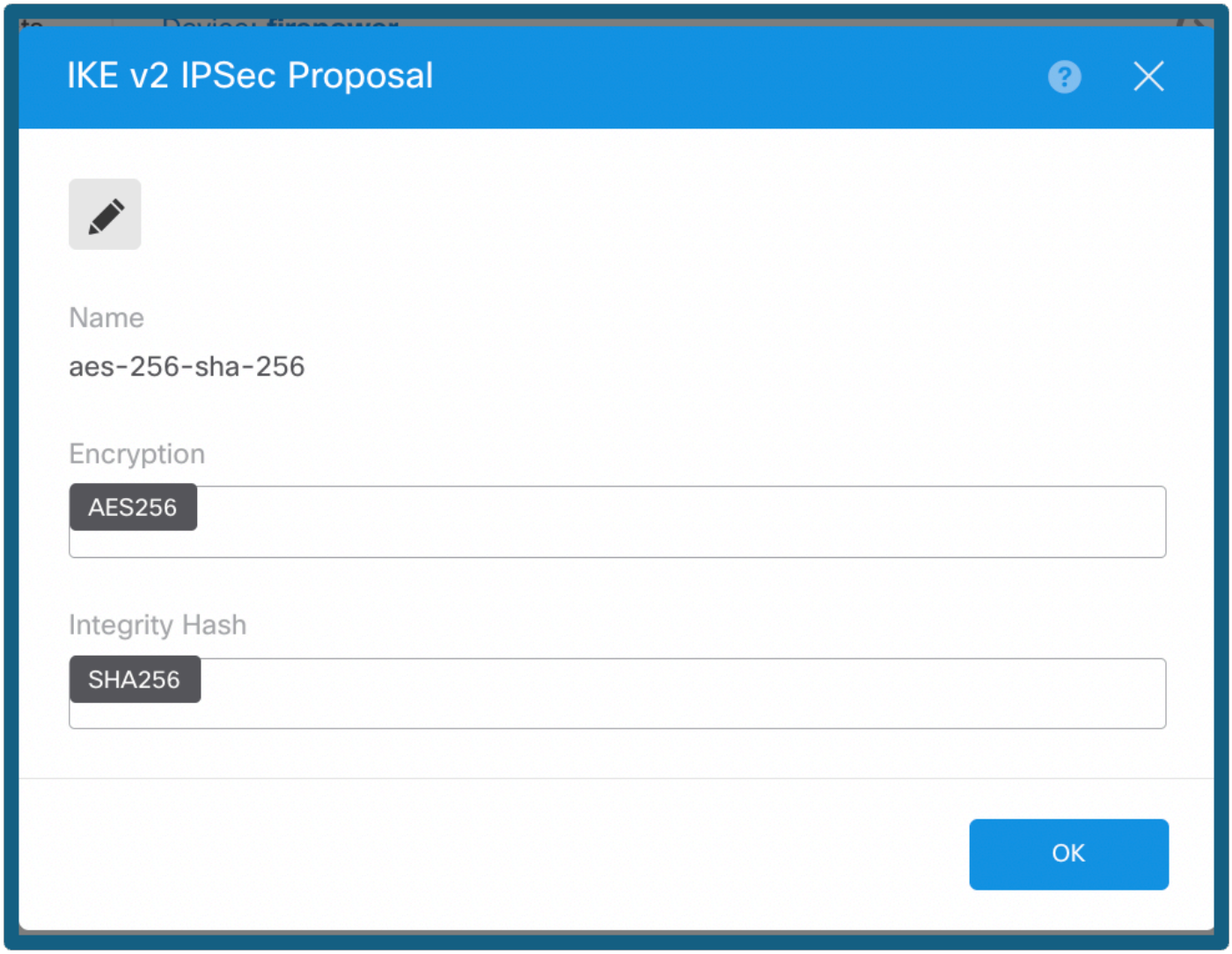


IKE策略的配置

第7b步：選擇IPSec Policy按鈕（如圖所示），然後按一下ok按鈕或Create New IPsec Proposal（如果要建立新提議）。


Select IPSec Proposals
Filter
SET DEFAULT
AES-GCM in Default Set
AES-SHA
DES-SHA-1
aes-256-sha-256
Create new IPSec Proposal
CANCEL
OK

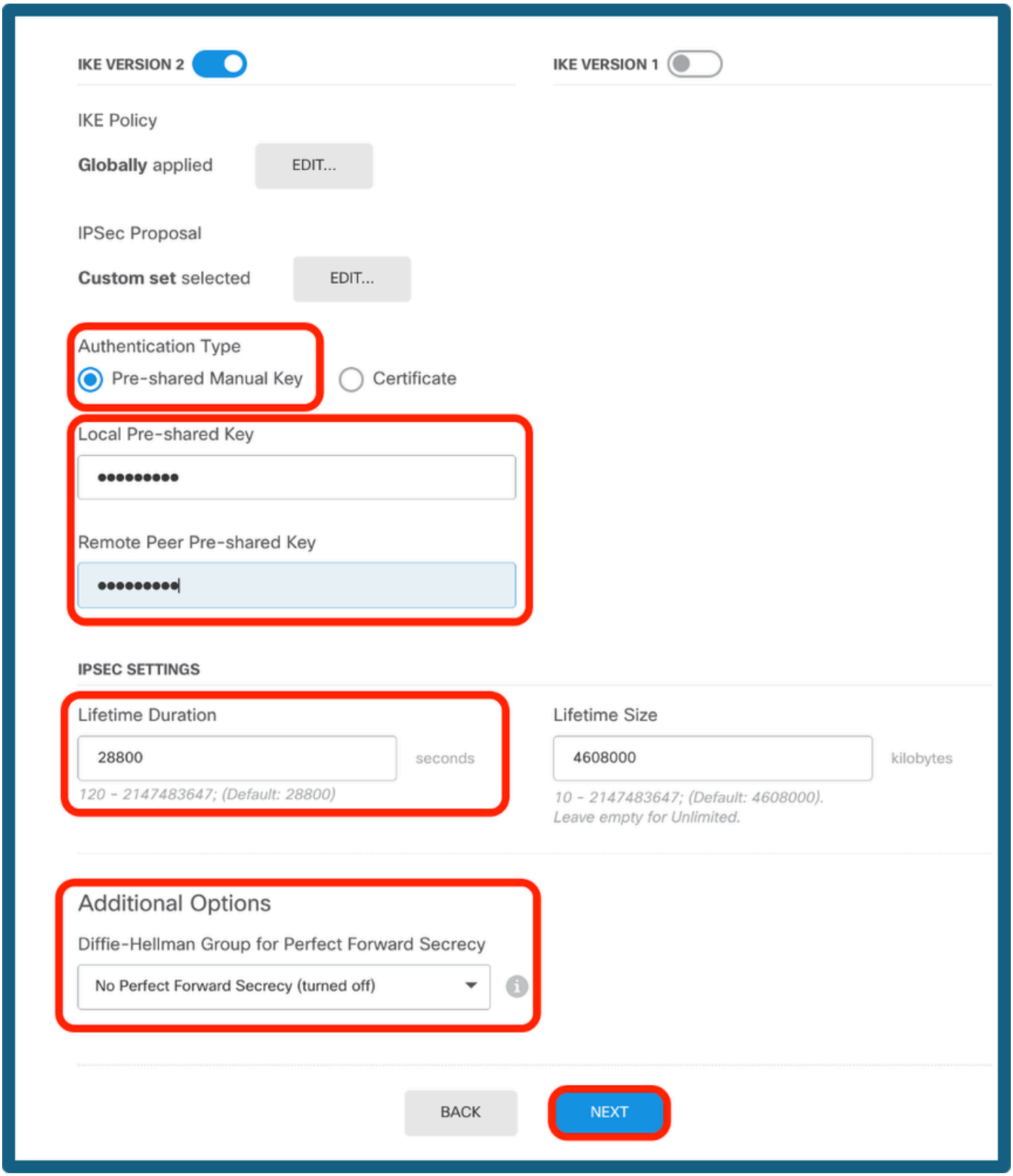
選擇IPsec方案



IPsec提議配置

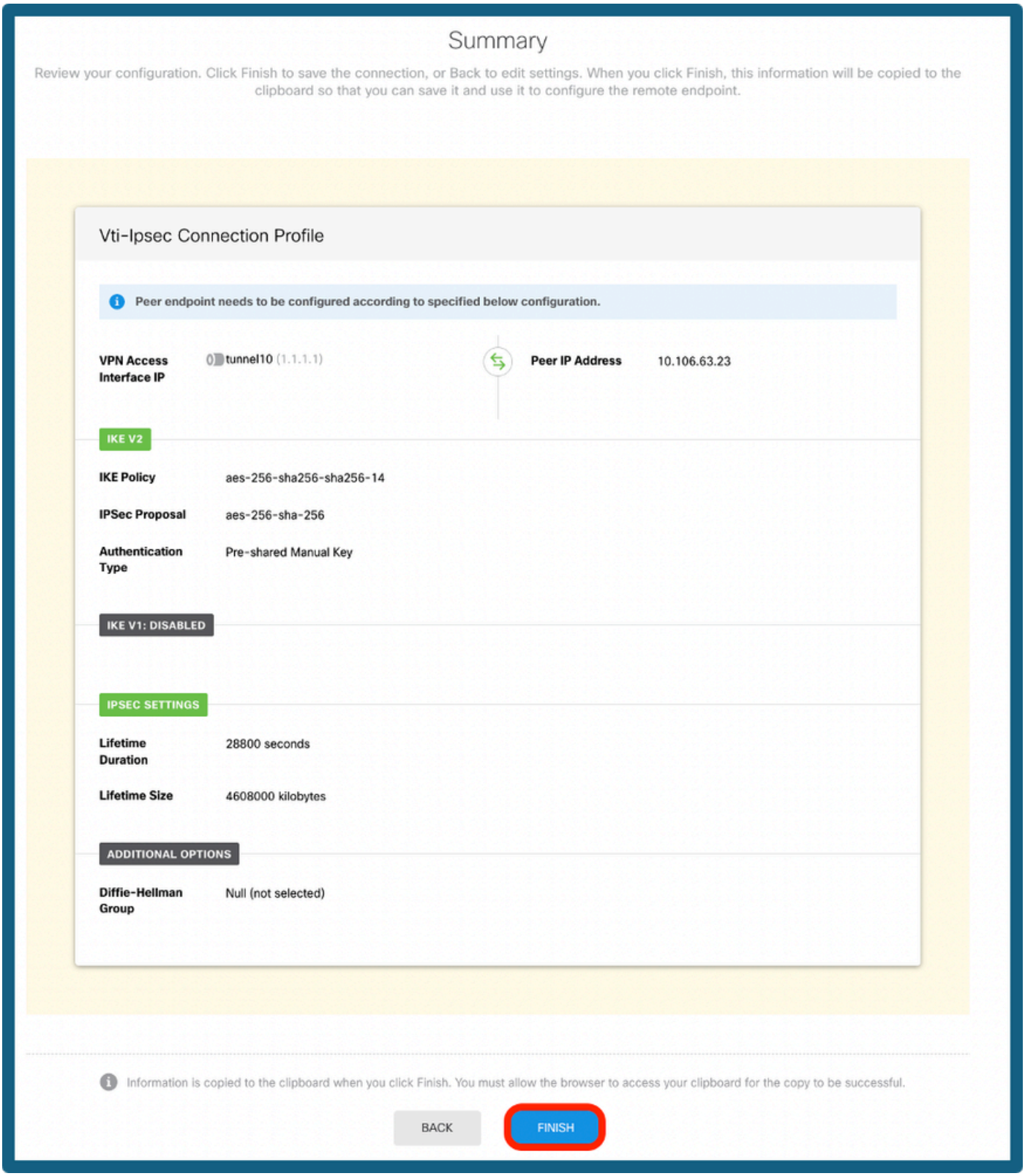
步驟8a.選擇Authentication Type。如果使用預共用手動金鑰，請提供本地和遠端預共用金鑰。

步驟8b.（可選）選擇完全向前保密設定。配置IPsec Lifetime Duration and Lifetime Size，然後按一下next。



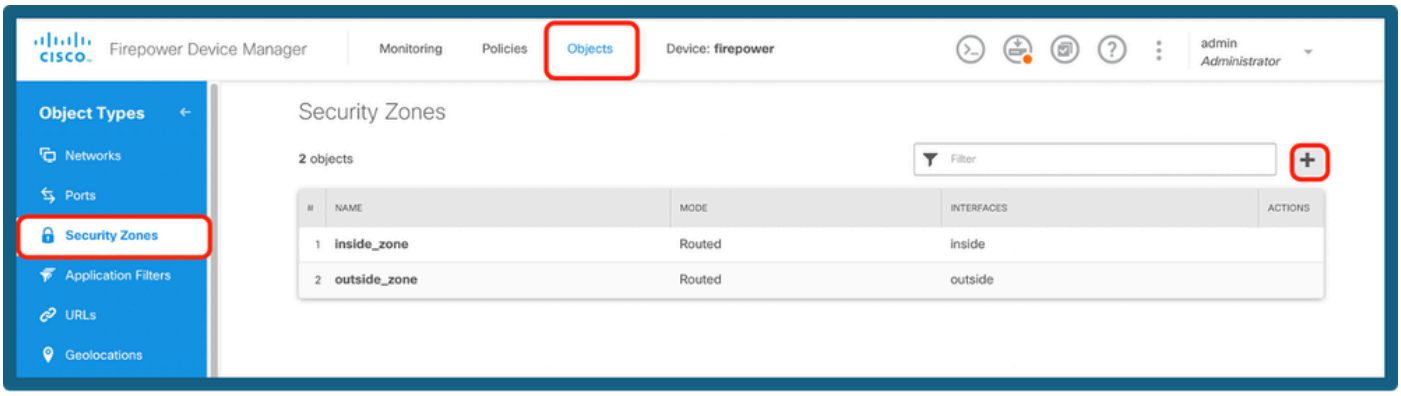
PSK和生存期配置

步驟9.檢查配置並按一下Finish。



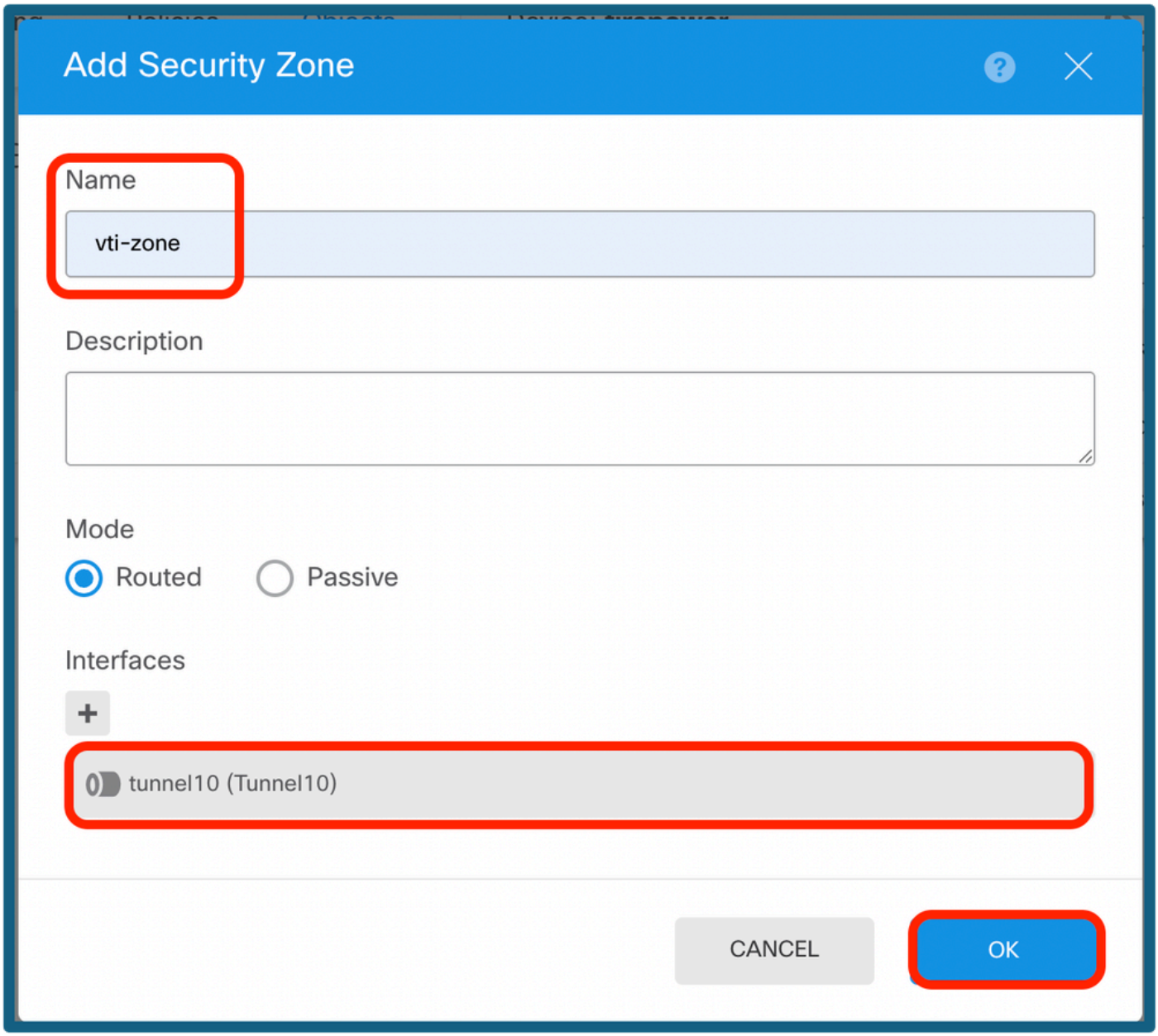
配置摘要

步驟10a。導航到Objects > Security Zones，然後按一下+圖示。



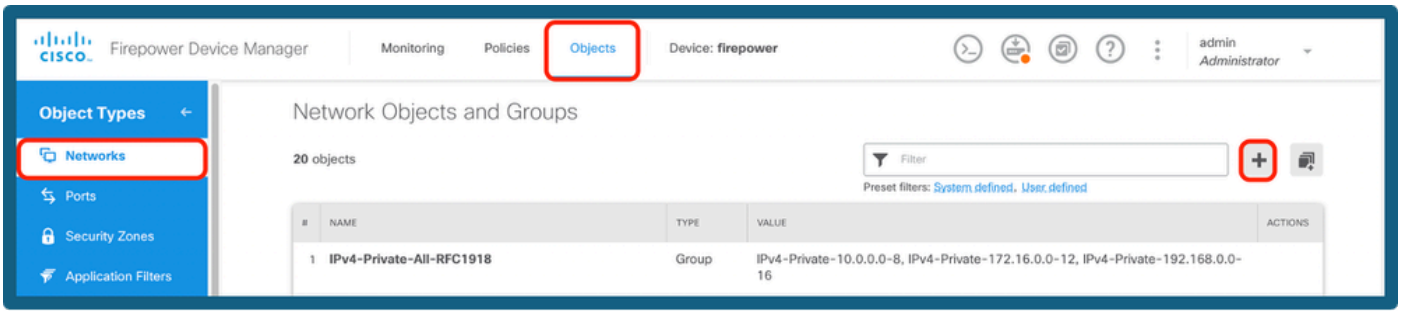
新增安全區域

步驟10b。建立一個區域，然後選擇VTI介面，如下所示。



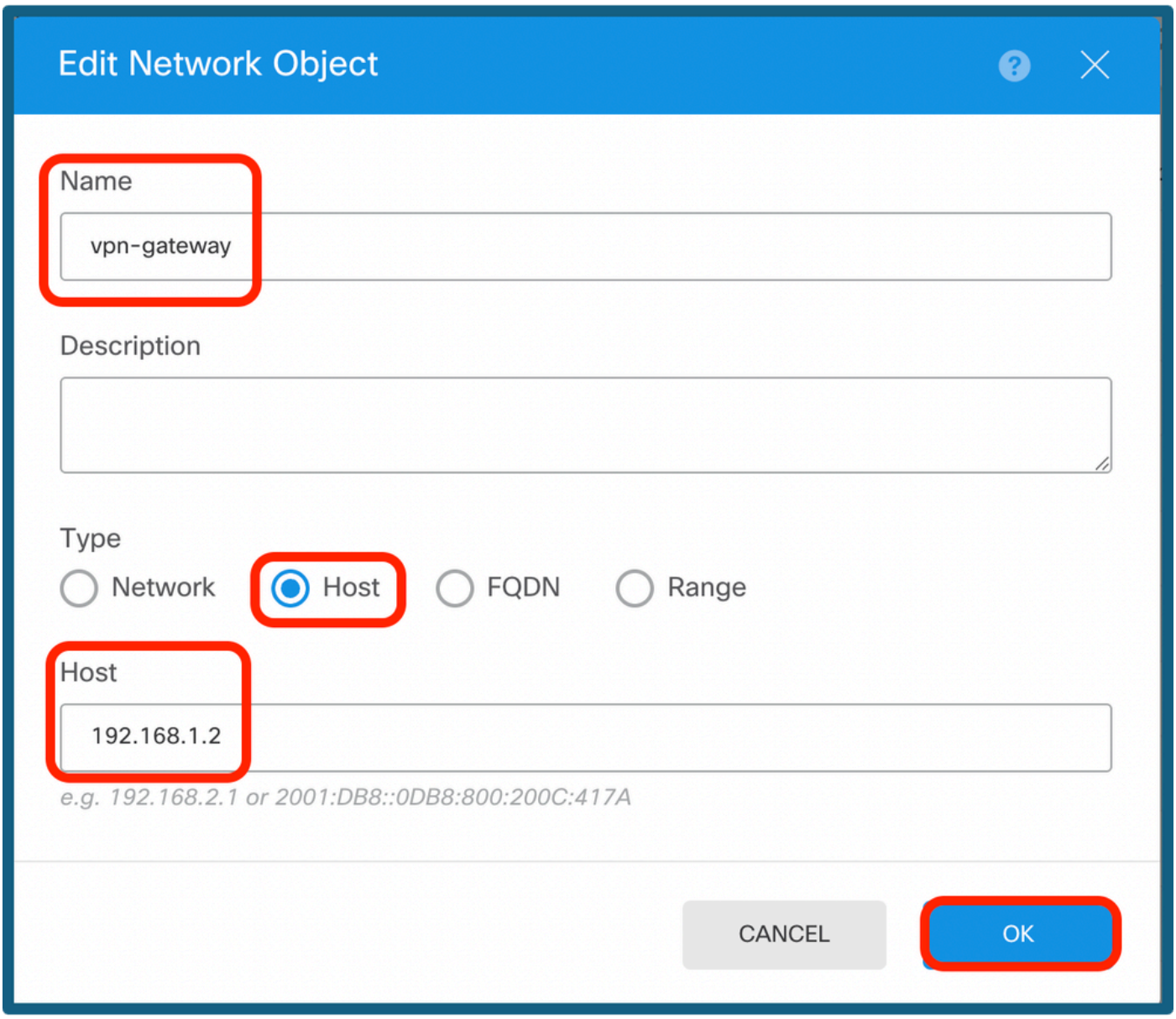
安全區域配置

步驟11a.導航到Objects > Networks，按一下+圖示。



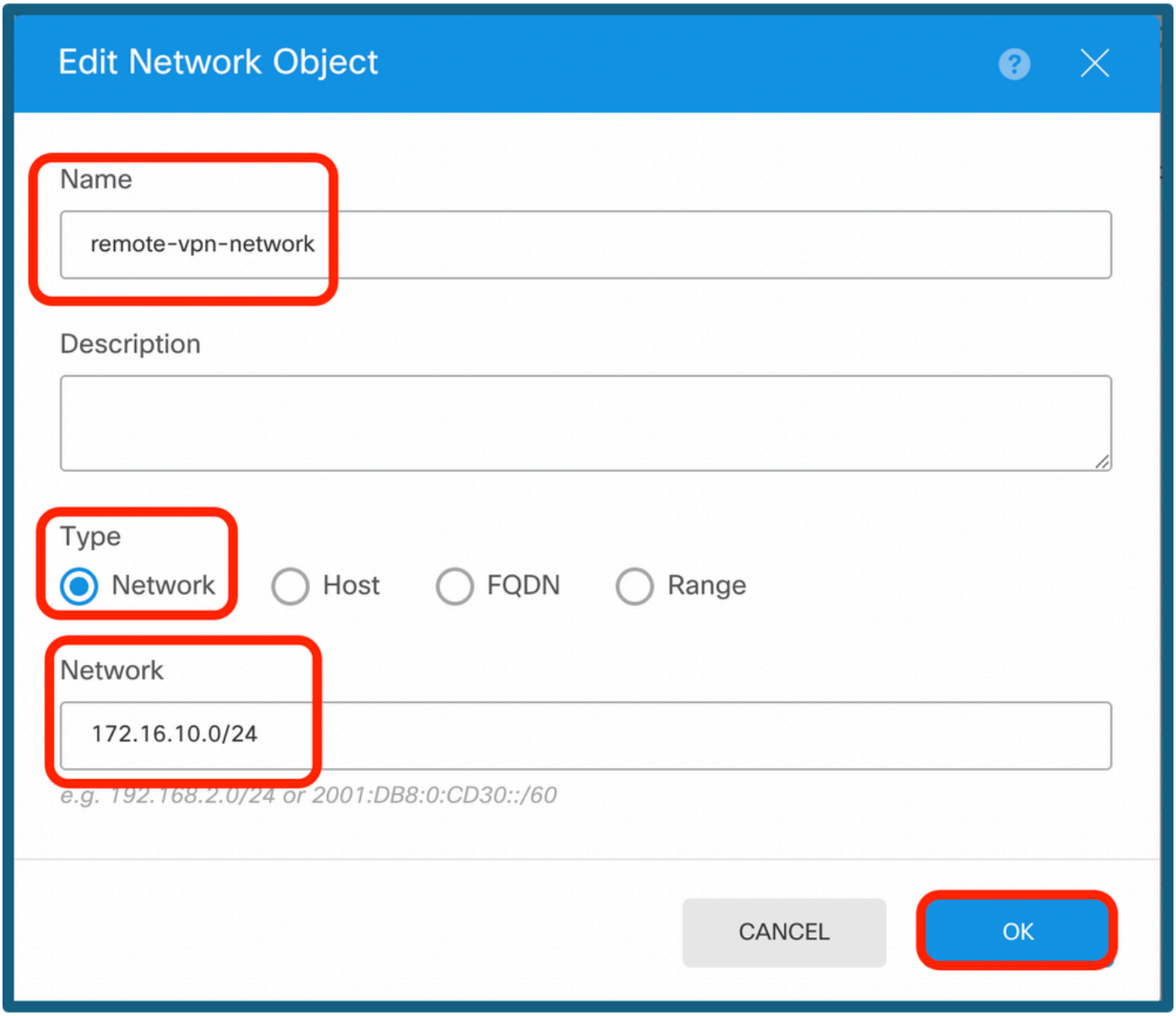
新增網路對象

步驟11b。新增host對象，並使用對等端的隧道ip建立網關。

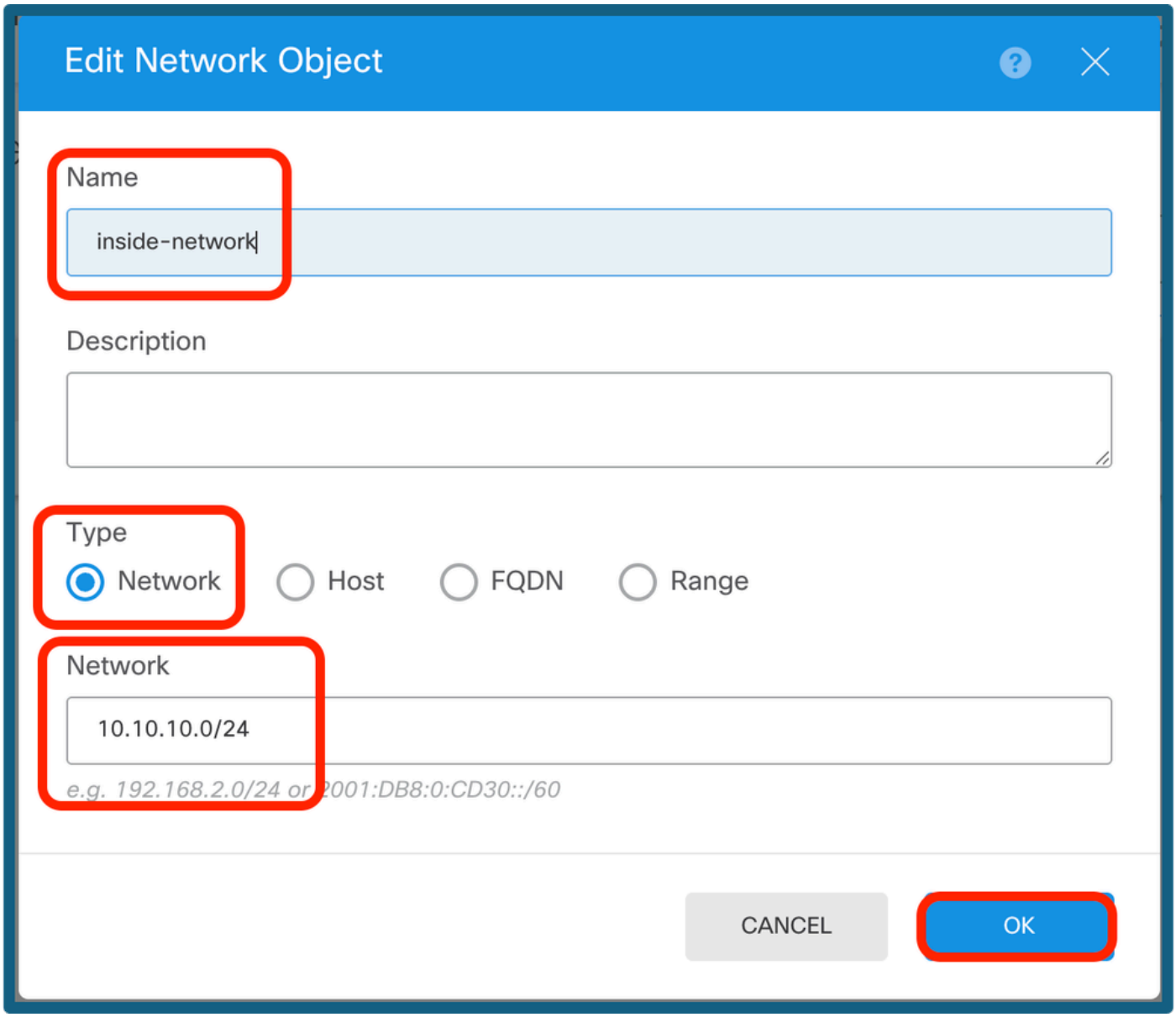


配置VPN網關

步驟11c.新增遠端子網和本地子網。

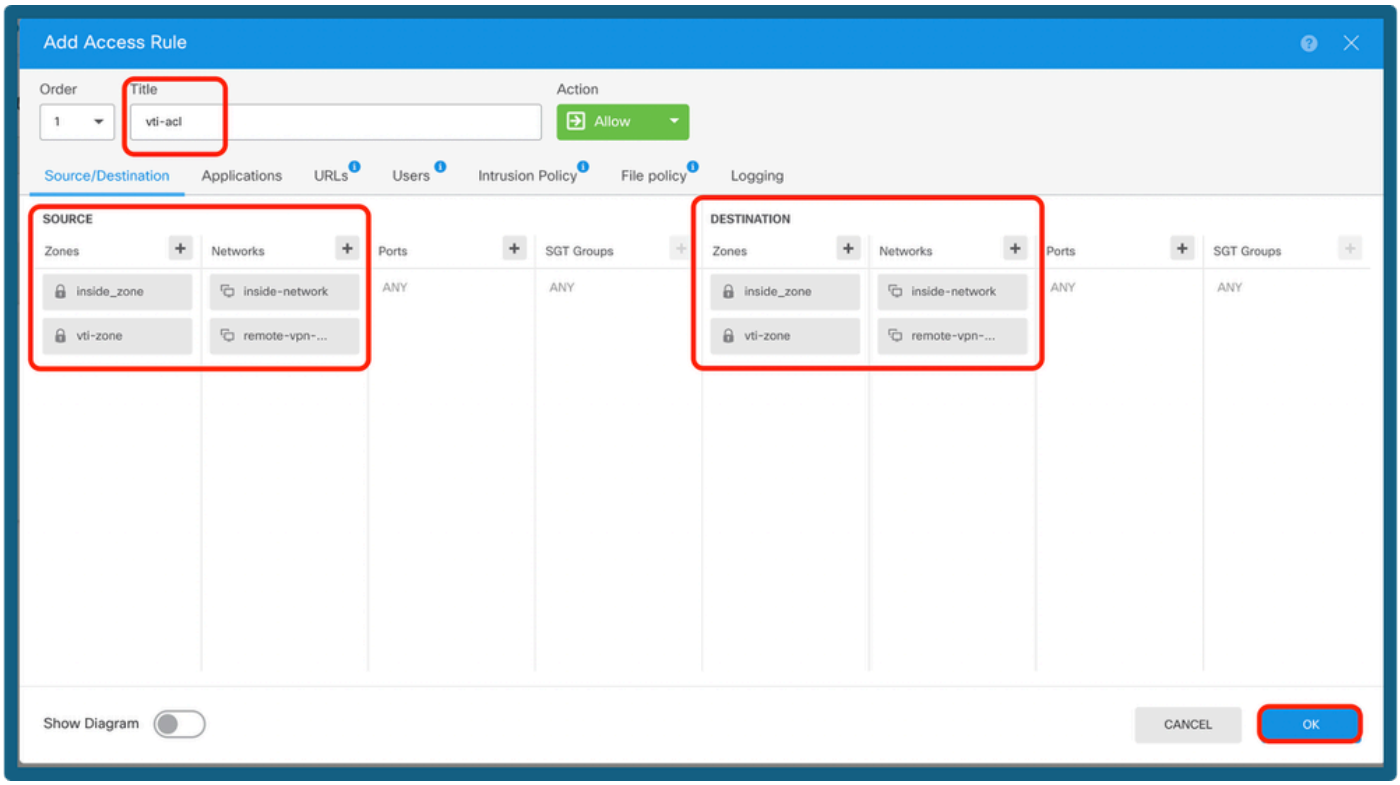

Edit Network Object
Name
remote-vpn-network
Description
Type
Network
Host
FQDN
Range
Network
172.16.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60
CANCEL
OK

遠端IP配置



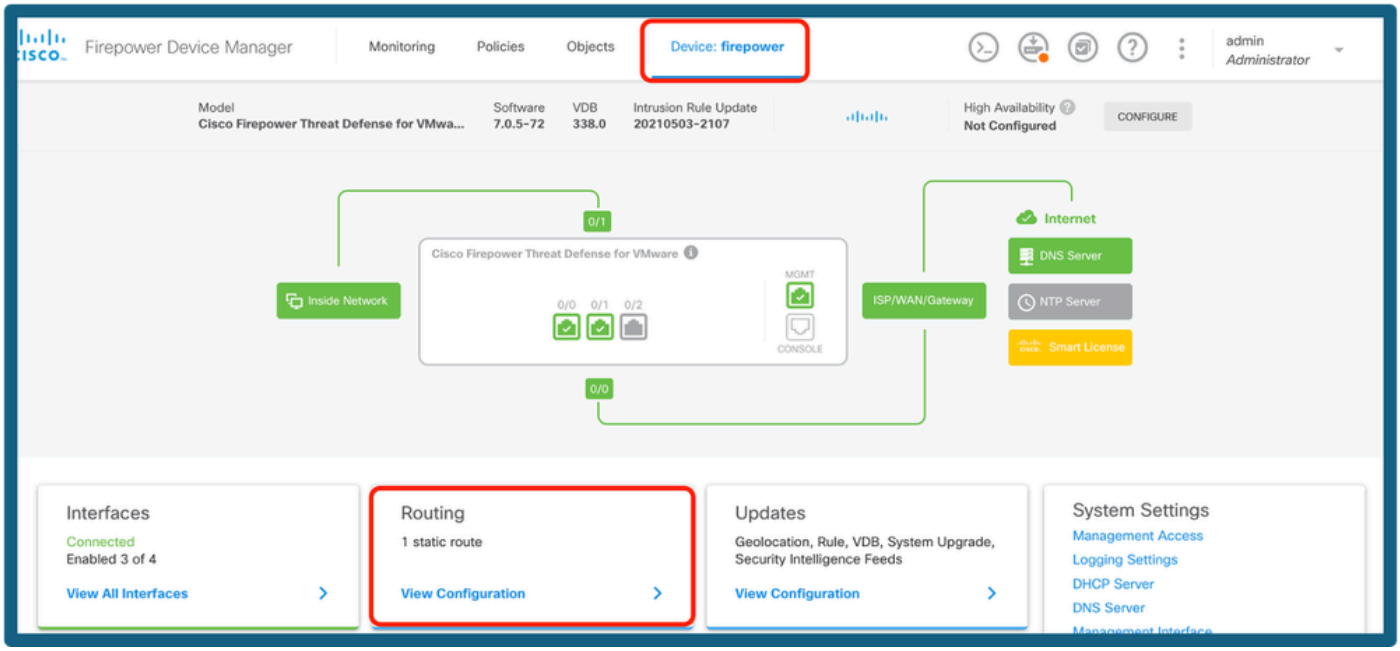
本地IP配置

步驟12.導航到Device > Policies，然後配置Access Control Policy。



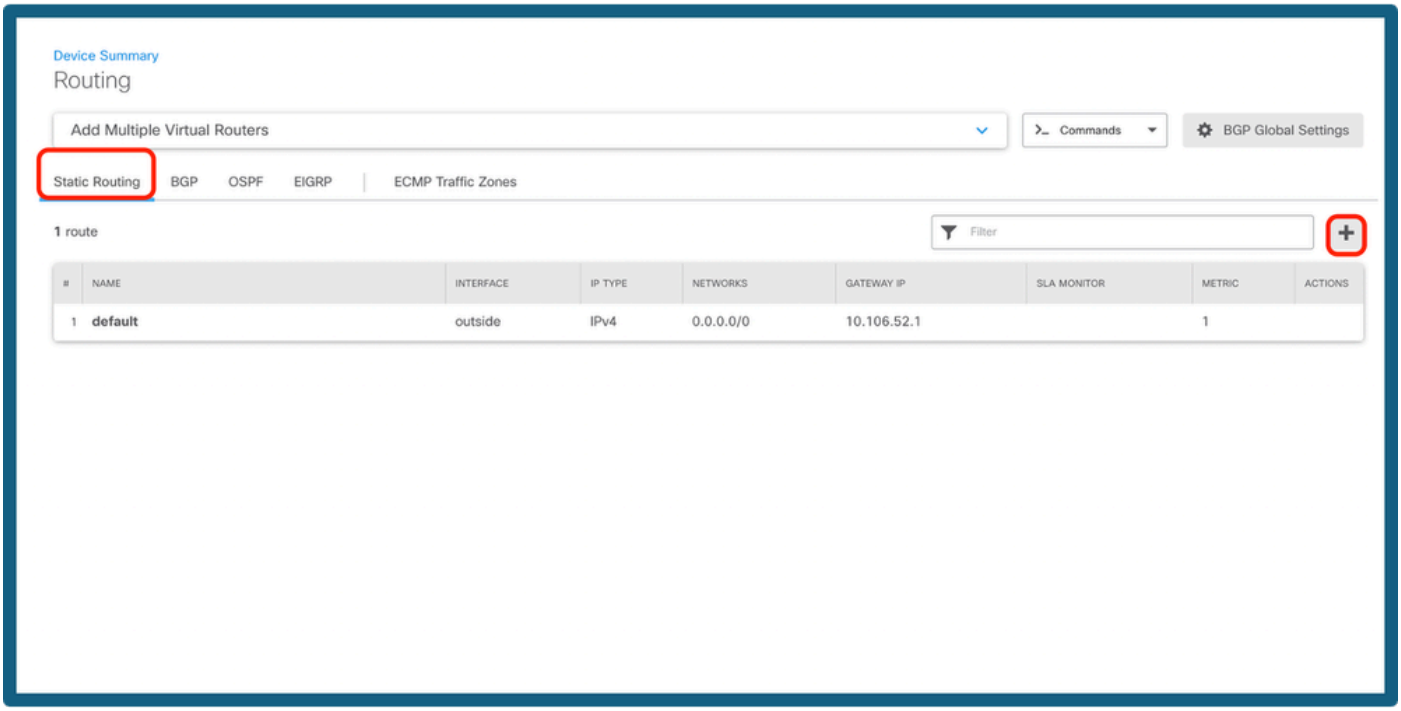
新增訪問控制策略

步驟13a.透過VTI通道新增路由。導覽至Device > Routing。



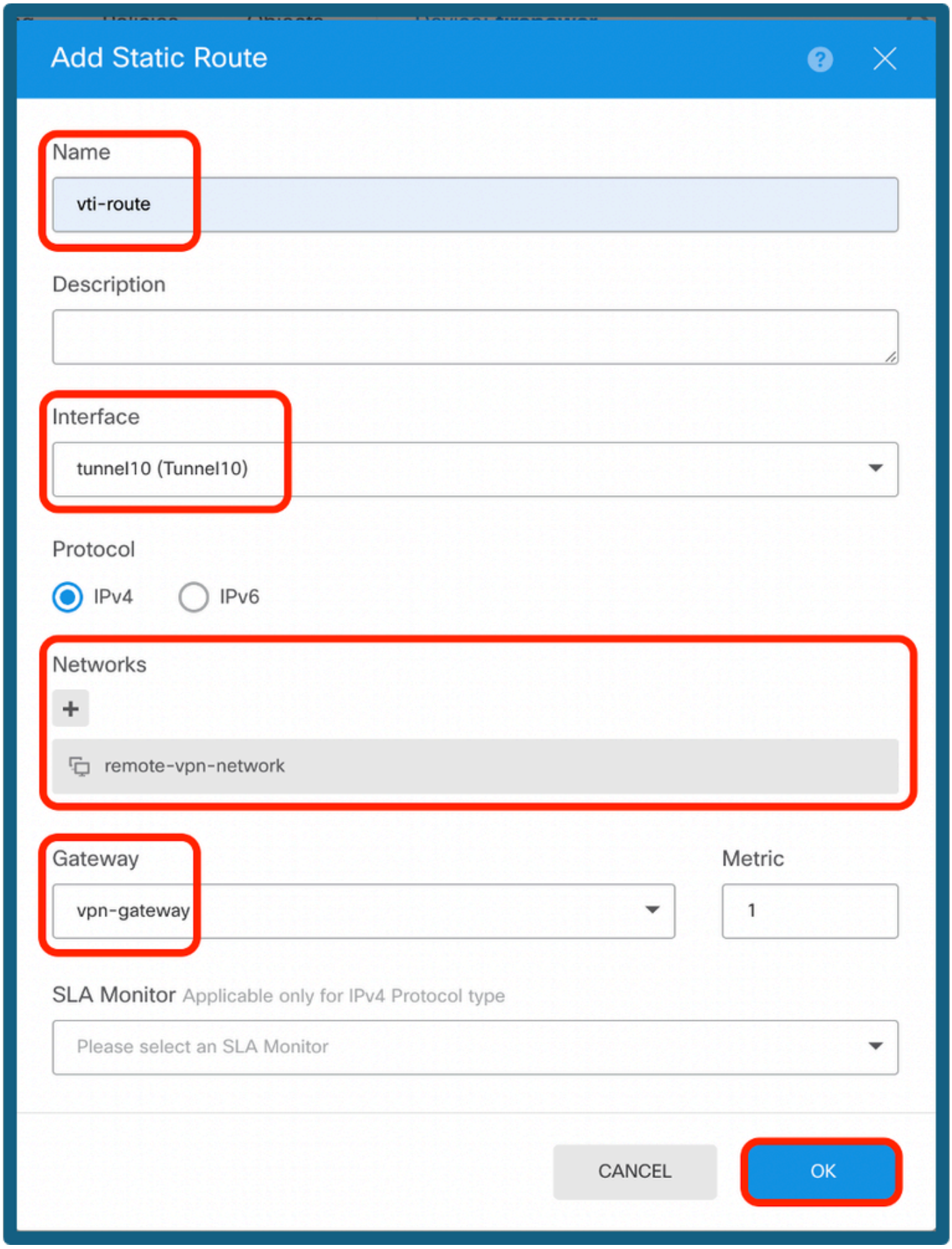
選擇工藝路線

步驟13b。導覽至Routing 索引標籤下的Static Route。按一下+圖示。



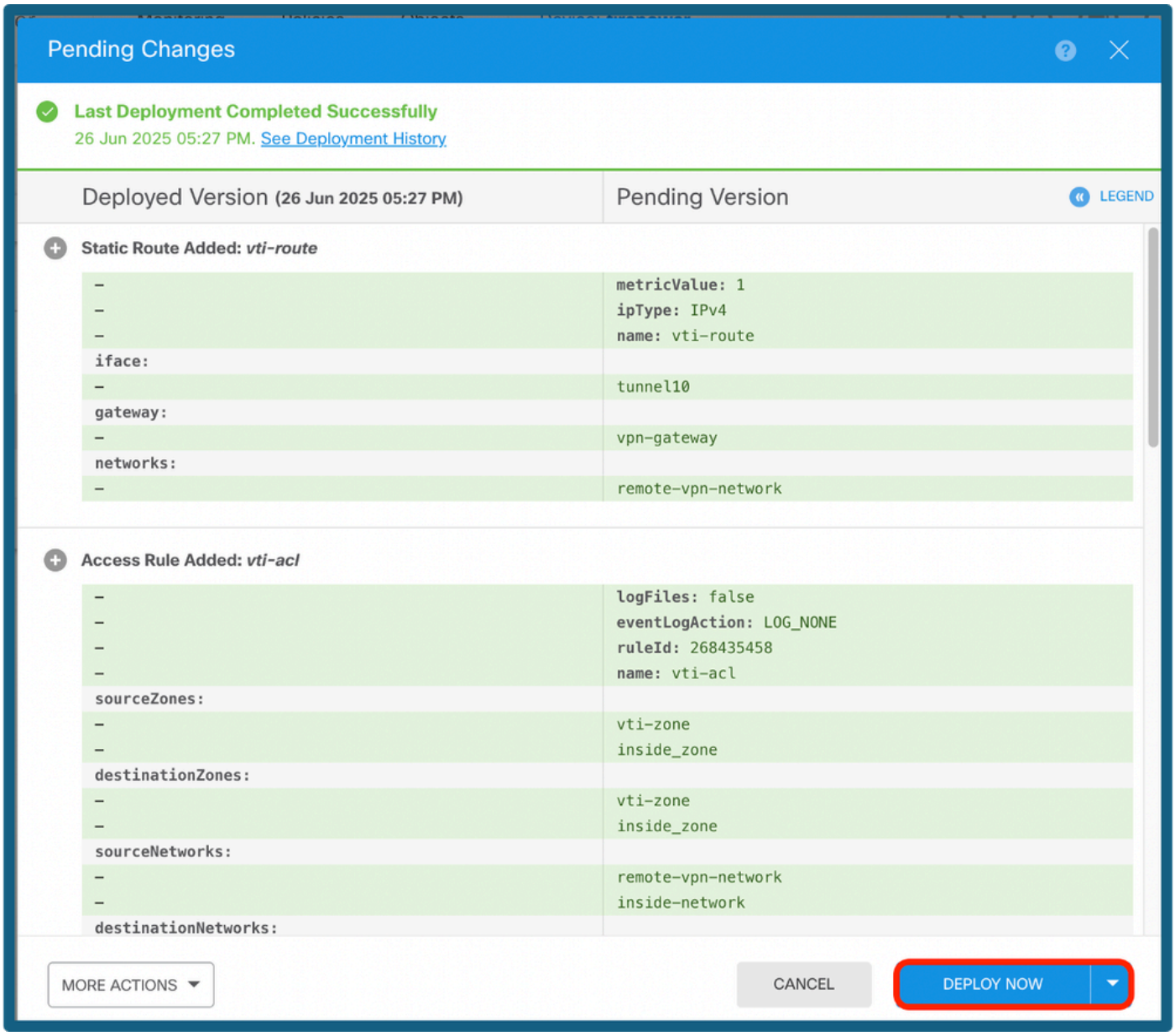
新增路由

步驟13c.提供Interface，選擇Network，提供Gateway。按一下「OK」（確定）。



配置靜態路由

步驟14.導覽至Deploy。檢視更改，然後按一下Deploy Now。

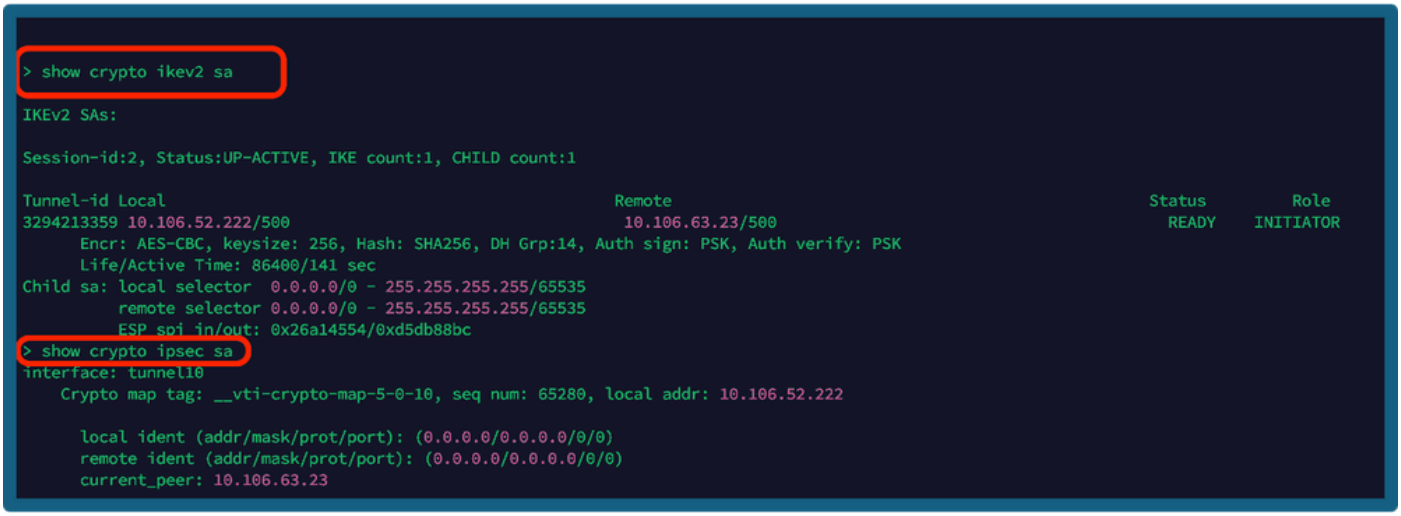


部署配置

驗證

部署完成後，可以使用以下命令在CLI上驗證隧道狀態：

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>



顯示命令

相關資訊

有關由FDM管理的FTD上的站點到站點VPN的詳細資訊，可在此處找到完整的配置指南：

FDM管理的FTD配置指南

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）。