配置由單個FMC管理的FTD之間的VPN遷移

目錄

簡介

本檔案介紹將站點到站點VPN從一個FTD遷移到由同一FMC管理的另一個FTD，同時保持與路由器的VPN連線。

必要條件

需求

為有效實施遷移流程，思科建議熟悉以下主題：
· 向FMC註冊FTD:瞭解如何向Firepower管理中心(FMC)註冊Firepower威脅防禦(FTD)裝置。
· 站點到站點VPN配置：在FMC管理的FTD裝置上配置站點到站點VPN的經驗。

採用元件

本檔案以指定的軟體和硬體版本為基礎：
· Firepower威脅防禦虛擬(FTDv):運行7.3.1版的兩個例項。
· Firepower管理中心(FMC):版本7.4.0。

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。

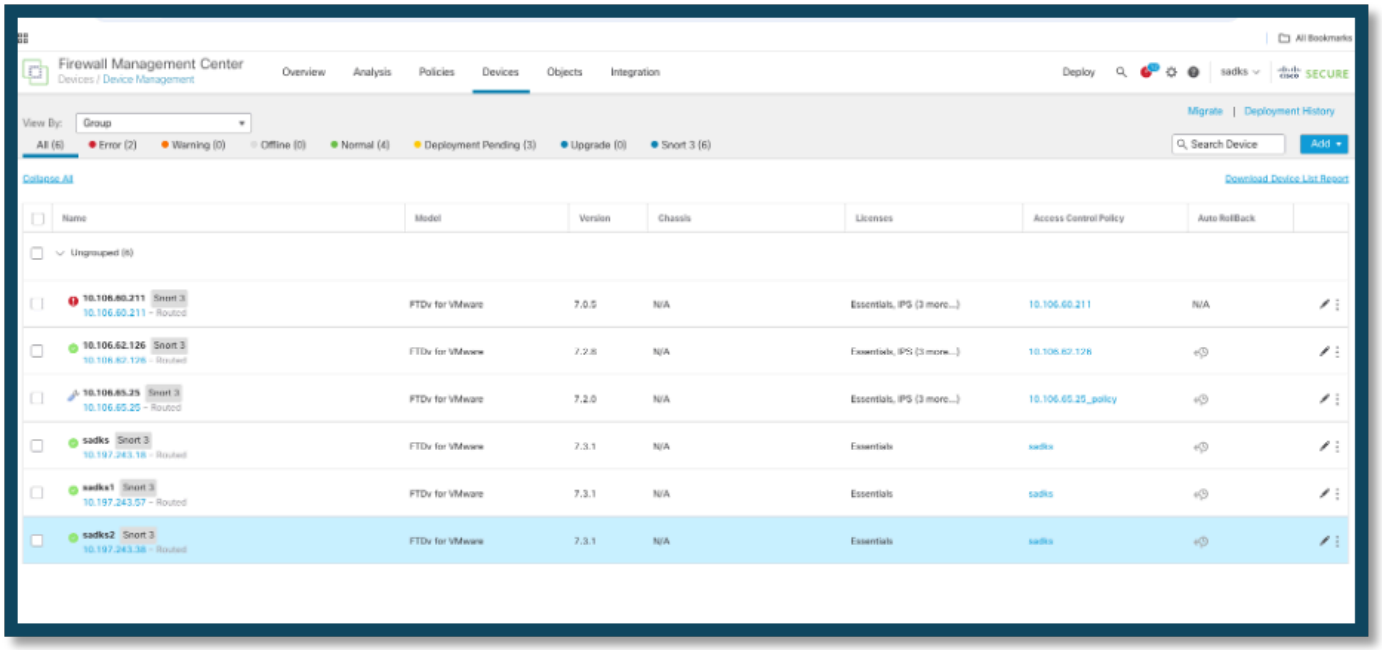
設定

程式

1.向FMC註冊新的FTD:
·首先在Firepower管理中心(FMC)的Devices > Device Management下註冊新的Firepower威脅防

禦(FTD)裝置。

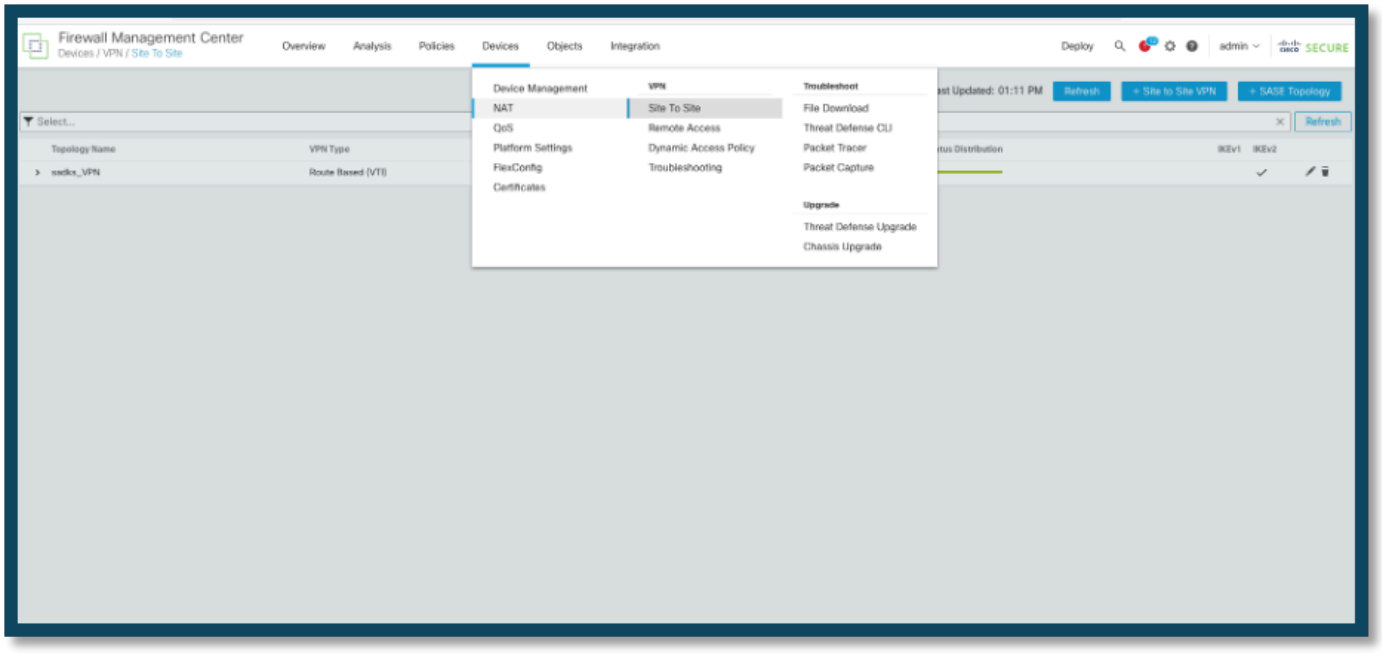
·在本示例中，註冊的新裝置命名為「sadks2」。



已註冊的新的FTD

2. 訪問站點到站點隧道配置：

·轉到FMC介面中的Devices > Site to Site，導航到站點到站點隧道設定。

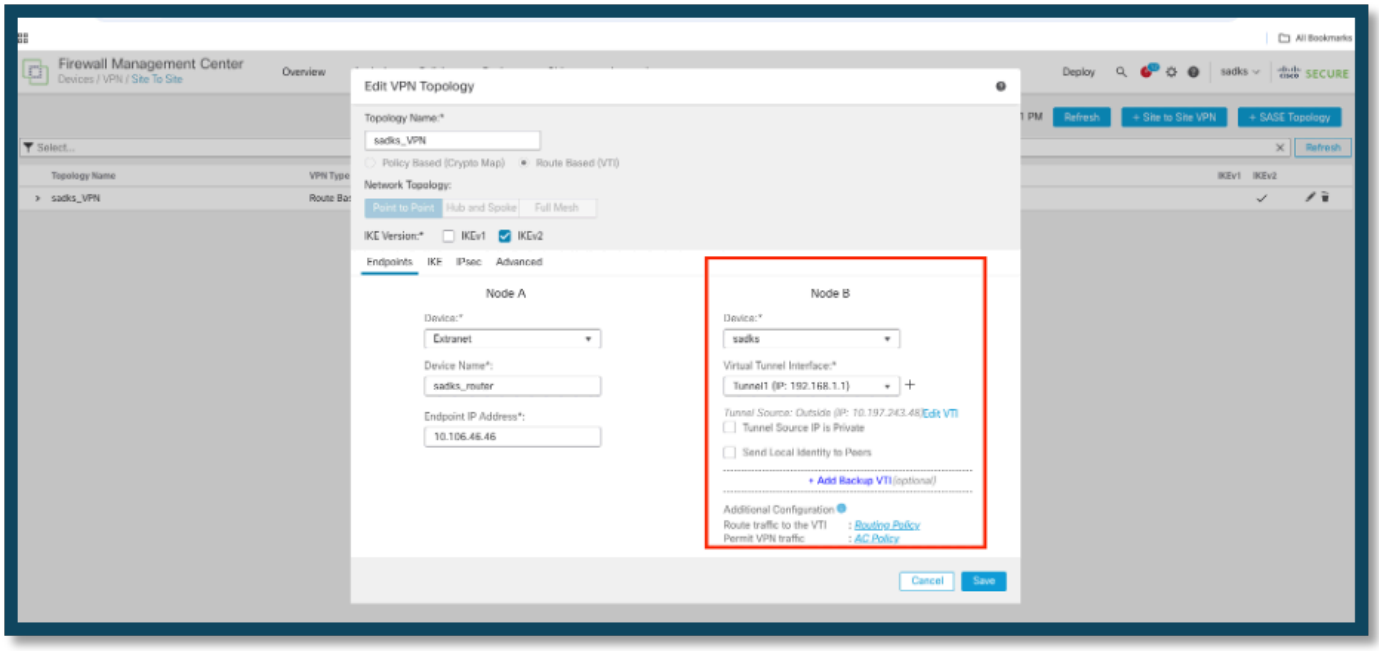


導航到VPN配置

3. 修改VPN配置：

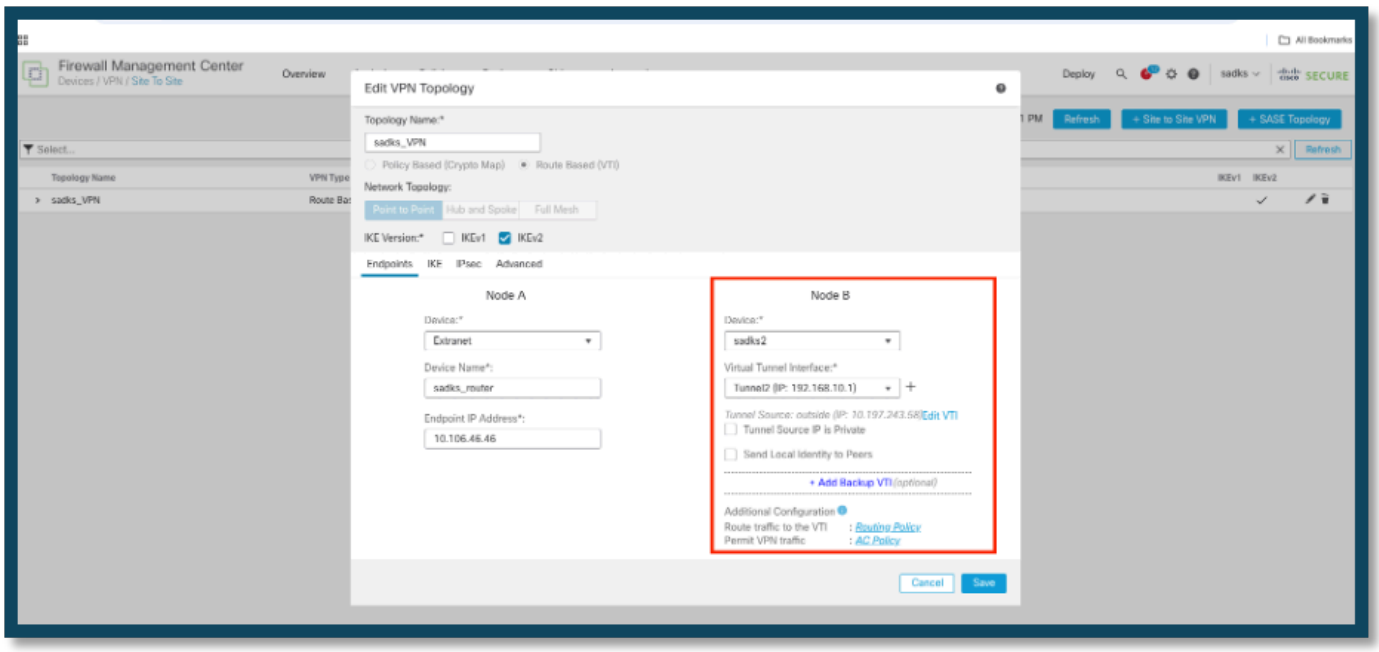
·選擇要更新的VPN配置。

•範例：在此案例中，VPN組態涉及FTD裝置及路由器。此處，節點B代表FTD裝置，且組態已更新，以將裝置關聯從「sadks」變更為「sadks2」。



舊FTD裝置

變更為



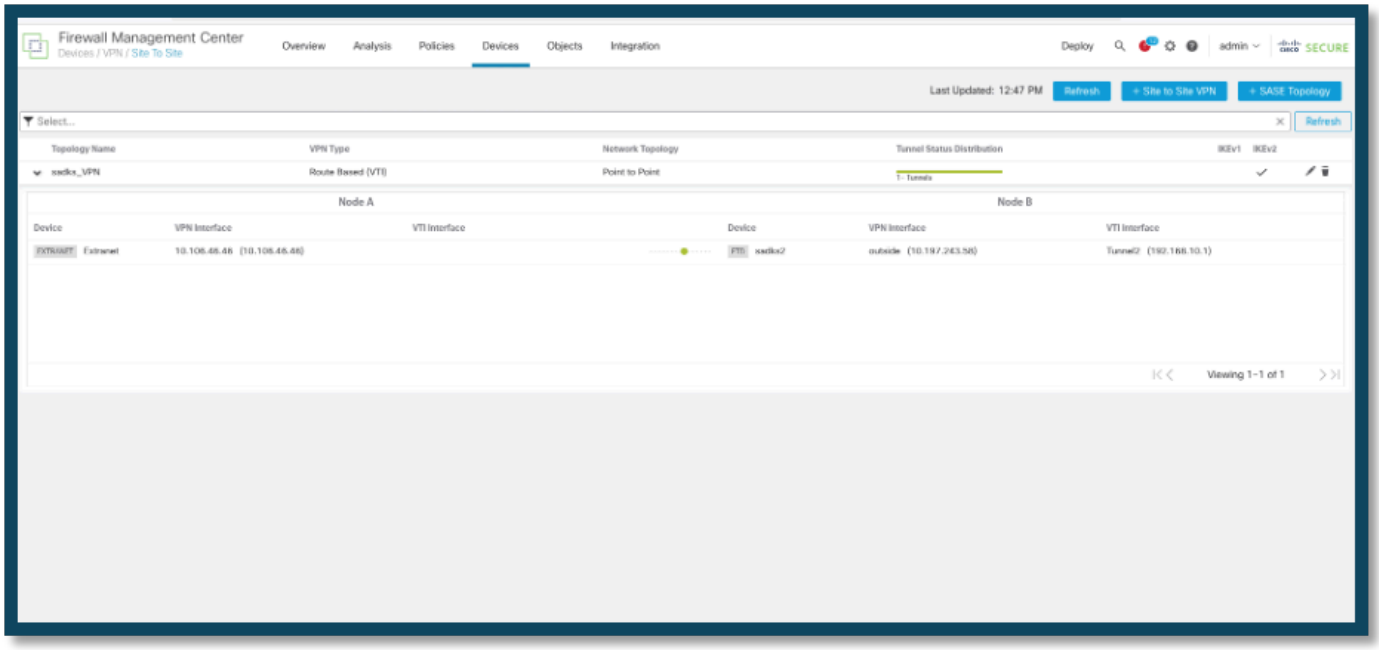
新FTD裝置

4. 儲存並部署組態：

·進行必要的更改後，儲存配置並進行部署以啟用更新。

驗證

隧道一旦部署就啟動。



通道狀態

疑難排解

初始連線問題

構建VPN時，雙方會協商隧道。因此，當您排除任何型別的隧道故障時，最好獲得會話的兩端。有關如何調試IKEv2隧道的詳細指南可以在此處找到：如何調試IKEv2 VPN

通道故障的最常見原因是連線問題。確定這一點的最佳方式是在裝置上捕獲資料包。使用此命令在裝置上捕獲資料包：

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

捕獲到位後，嘗試通過VPN傳送流量，並在資料包捕獲中檢查雙向流量。

使用以下命令檢視封包擷取：

<#root>

show cap capout

流量特定的問題

您遇到的常見流量問題包括：

- FTD背後的路由問題 — 內部網路無法將封包路由回指派的IP位址和VPN使用者端。
- 訪問控制清單阻止流量。
- VPN流量不會繞過網路地址轉換。

有關FMC管理的FTD上的VPN的詳細資訊，可在此處找到完整的配置指南：由FMC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）。