無縫過渡：從Palo Alto防火牆遷移到Cisco FTD

目錄

簡介

本檔案介紹使用FMT 6.0版從Palo Alto防火牆過渡到Cisco FTD系統的過程。

必要條件

需求

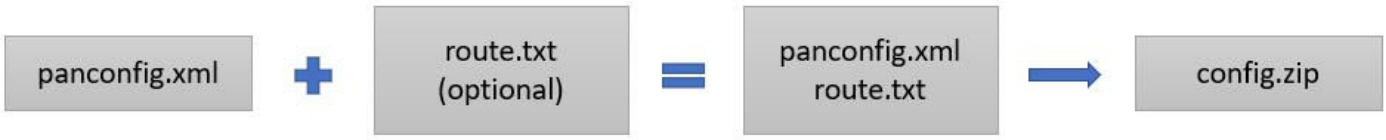
思科建議您瞭解以下主題：

- 以XML格式(*.xml)從Palo Alto防火牆匯出當前運行配置。
- 訪問Palo Alto防火牆CLI並執行show routing route命令，然後將輸出儲存為文本檔案(*.txt)。
- 將組態檔(*.xml)和路由輸出檔案(*.txt)壓縮為單個ZIP封存(*.zip)。

採用元件

本文檔中的資訊基於Palo Alto Firewall 8.4.x或更高版本。

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。



Firepower遷移工具(FMT)

FMT可幫助工程團隊完成從任何現有供應商防火牆到思科下一代防火牆(NGFW)/Firepower威脅防禦(FTD)的過渡。 確保運行從思科網站下載的最新版本的FMT。

遷移指南

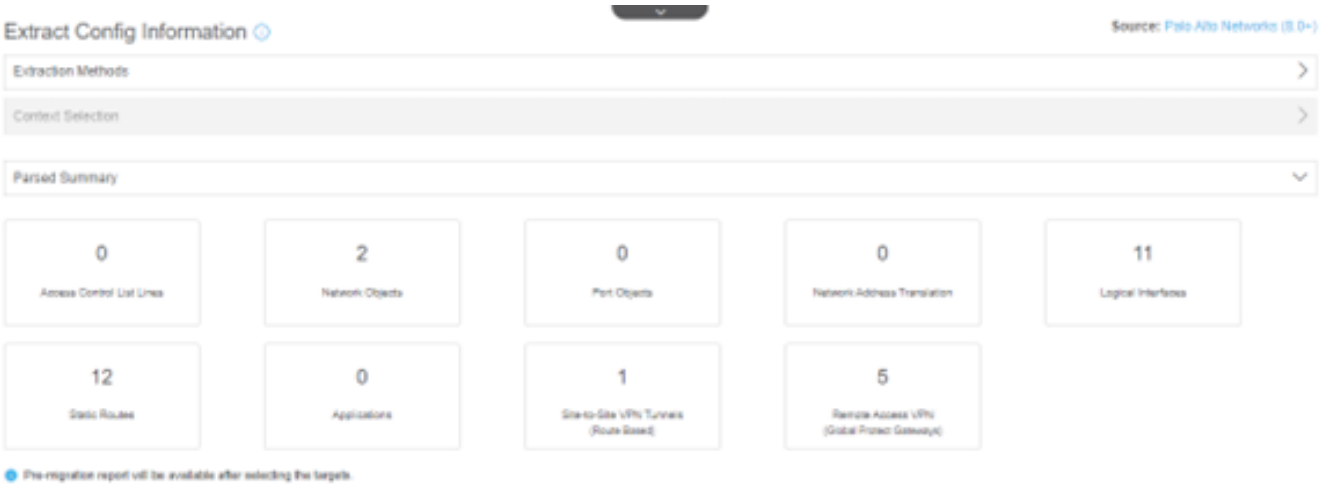
1.遷移前檢查清單

- 在開始遷移過程之前，確保FTD已新增到FMC。
- 已在FMC上建立具有管理許可權的新使用者帳戶。
- 匯出的Palo Alto運行配置檔案.xml必須使用.zip副檔名進行壓縮。
- NGFW/FTD的物理或子介面或埠通道的數量必須與Palo Alto防火牆介面相同。

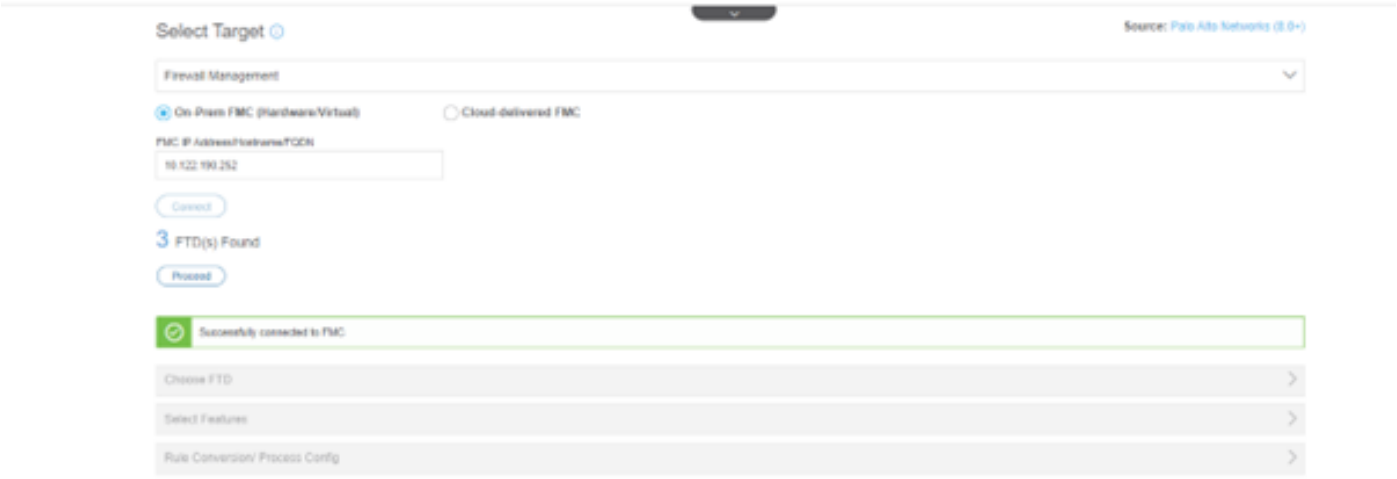
2.遷移工具使用情況

- 下載FMT工具.exe並以管理員身份運行。
- FMT需要使用CEC ID或思科使用者帳戶才能登入。
- 成功登入後，該工具將顯示一個控制面板，您可以在其中選擇防火牆供應商並上傳相應*.zip檔案；請參閱下一張圖片。

- 繼續遷移之前，請仔細閱讀右側提供的說明。
- 準備開始後，按一下Start Migration。
- 上傳包含Palo Alto防火牆配置設定的已儲存*.zip檔案。
- 上傳配置檔案後，您將能夠看到內容的分析摘要並點選next；請參閱下一個映像。



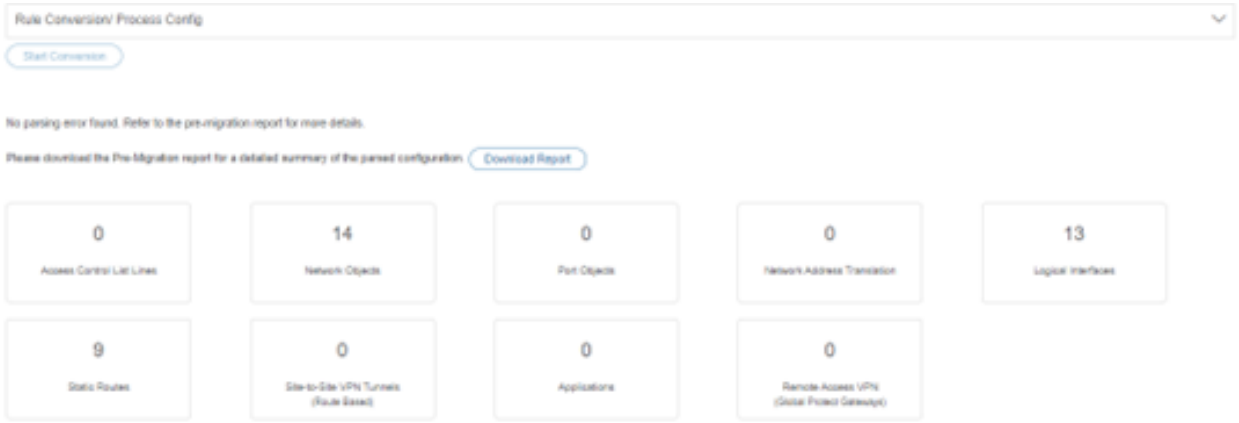
- 輸入FMC的IP地址並登入。
- 工具將搜尋已向FMC註冊的活動FTD。
- 選擇要遷移的FTD，然後按一下Proceed，如下圖所示。



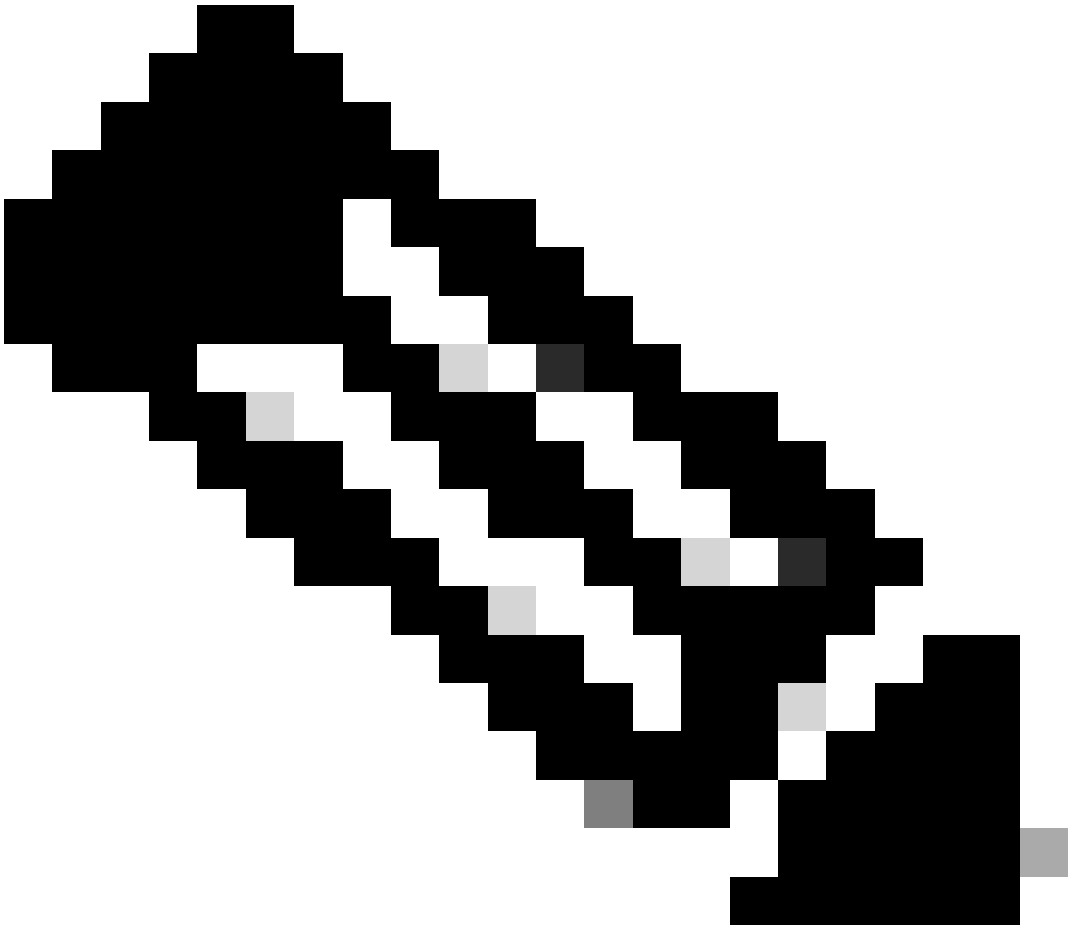
- 選擇特定功能，以便根據客戶的要求進行遷移。請注意，與FTD相比，Palo Alto防火牆具有不同的功能集。
- 按一下「Proceed」，然後參閱下一張映像以作參考。

- FMT將根據您的選擇執行轉換。檢視「Pre-Migration Report（遷移前報告）」中的更改，然

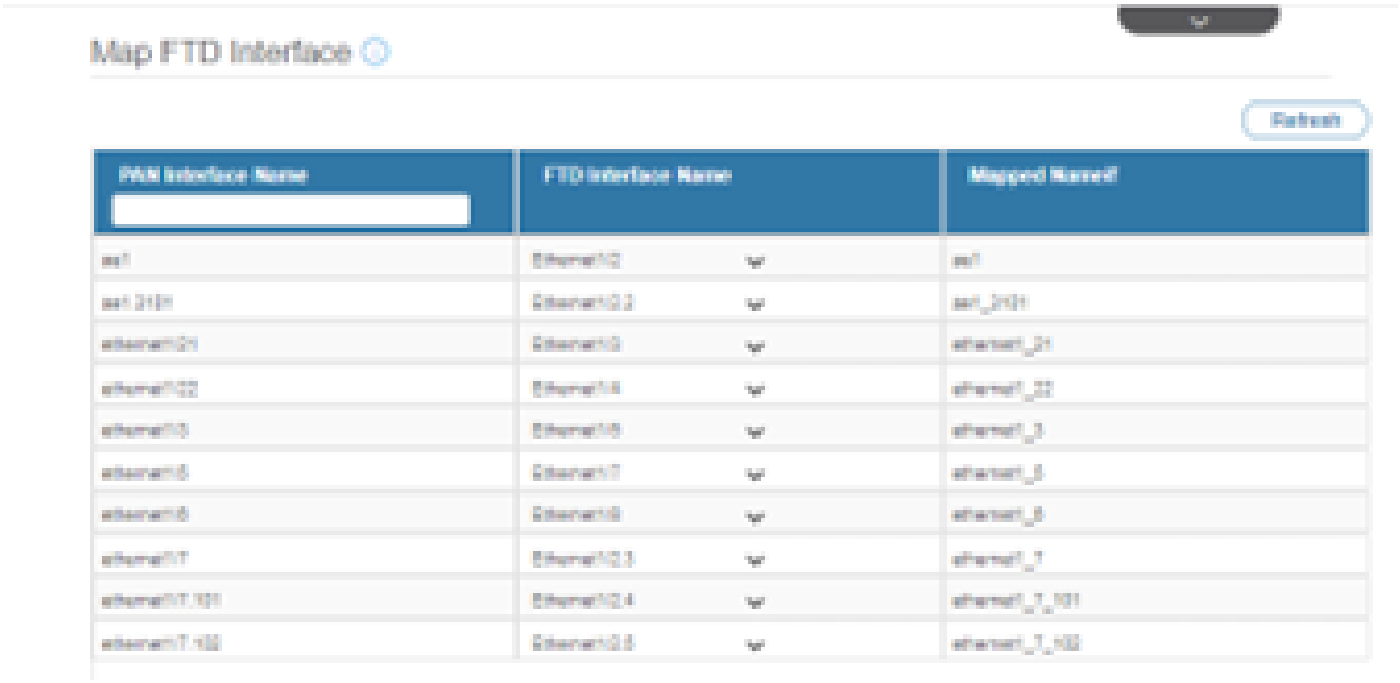
後按一下Proceed。請參見下一張影象以獲取指導。



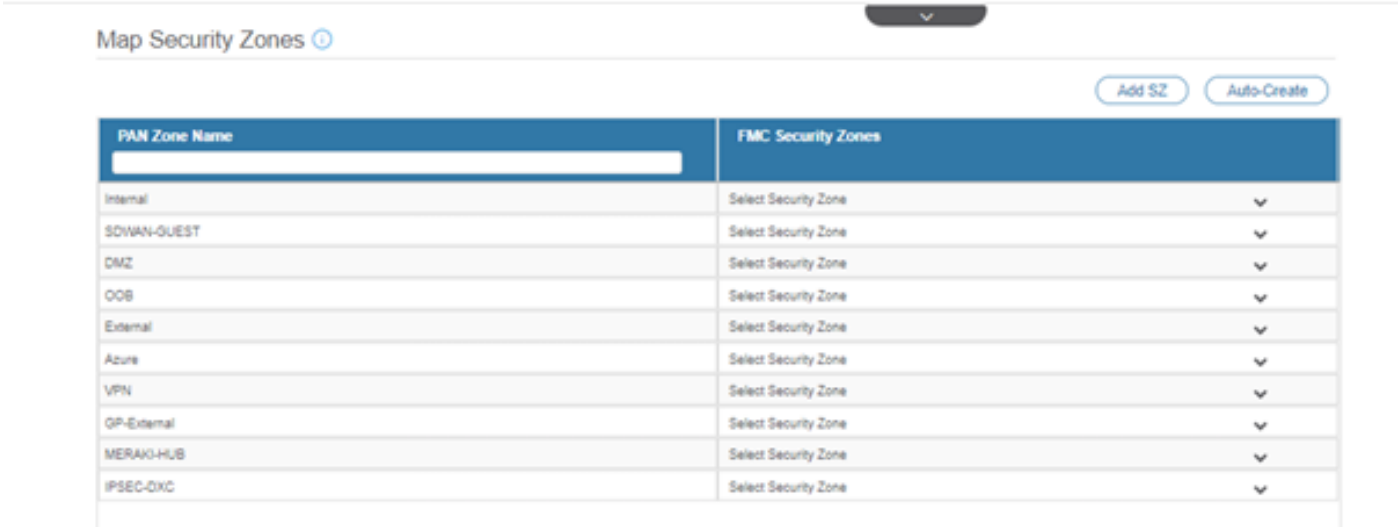
- 將Palo Alto防火牆的介面對映到FTD上的介面。有關詳細資訊，請參閱下一張圖片。



附註：NGFW/FTD必須具有與包括子介面的Palo Alto防火牆介面相同的物理或子介面數量或埠通道數量。



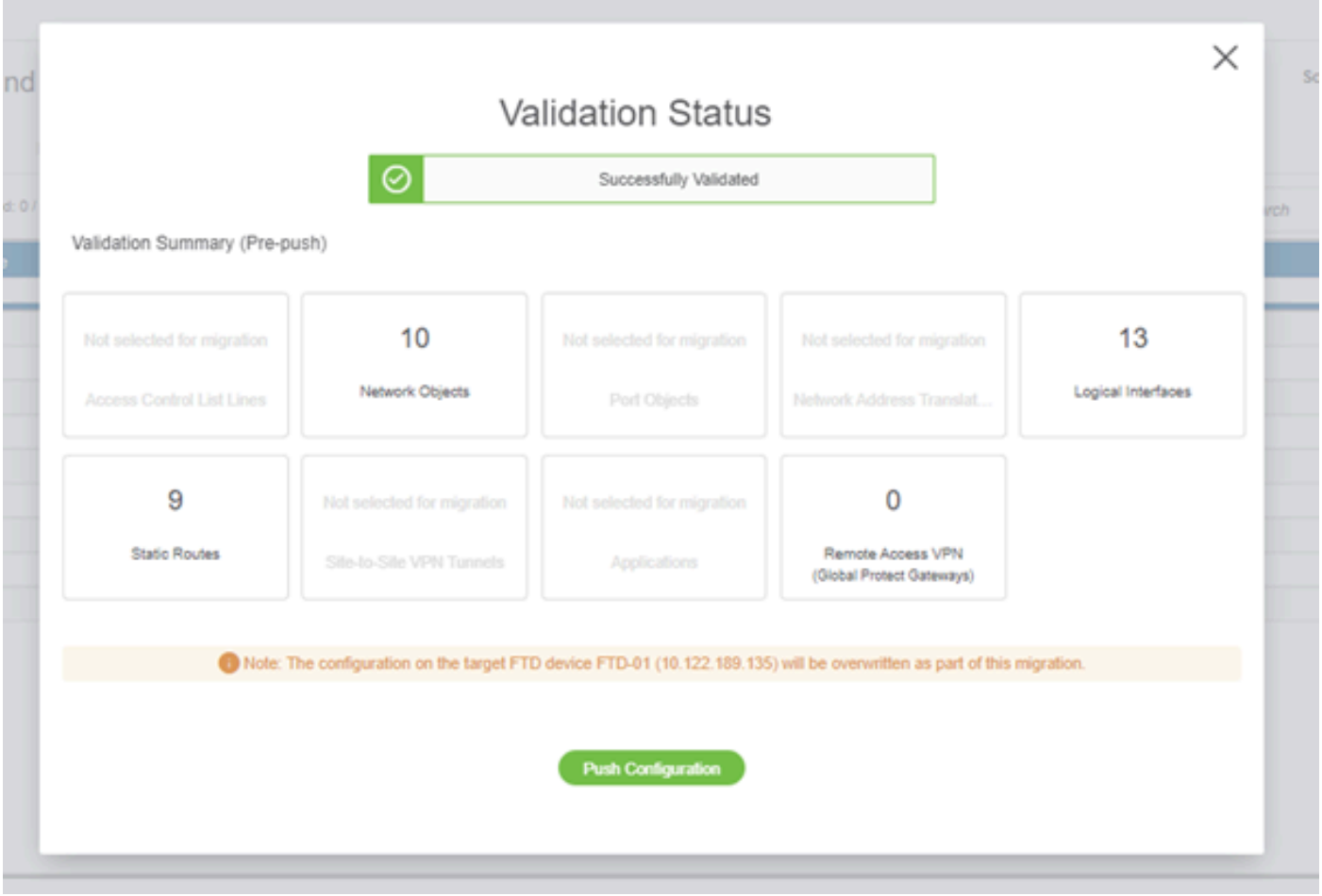
- 確定Zones的對映，可以手動完成，也可以使用Auto-create功能完成。要進行視覺化，請參閱下一張影象。



- 分配應用程式阻止配置檔案。由於這是沒有應用程式對映的實驗室裝置，您可以繼續使用預設設定。按一下「Next」，然後參閱提供的映像。

- 根據需要最佳化ACL、對象、介面和路由。由於這是使用最少配置的實驗設定，您可以繼續使用預設選項。然後按一下Validate，參照下一個影象。

- 成功驗證後，配置即可部署到目標FTD。請參見下一個影象以瞭解進一步的說明。



- 推送配置會將遷移的配置儲存在FMC中，並將自動部署到FTD。
- 如果在遷移期間發生任何問題，請隨意開啟TAC案例以獲得進一步幫助。

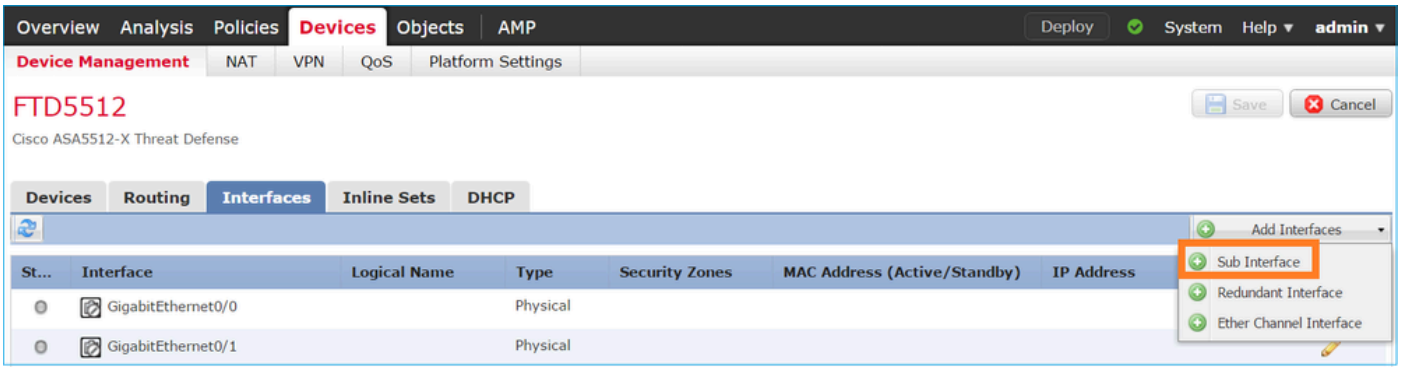
3.遷移後驗證

- 驗證FTD和FMC上的組態。
- 測試裝置ACL、策略、連線和其他高級功能。
- 在執行任何更改之前建立回退點。
- 在生產環境中投入使用之前，先在實驗室環境中測試遷移。

已知的問題

1. FTD上缺少介面

- 登入Palo Alto CLI並執行show interface all。您必須擁有等於或大於FTD中的介面數量。
- 通過FMC GUI建立相同或更多的介面 — 子介面、埠通道或物理介面。
- 導覽至FMC GUI Device > Device Management，然後按一下將建立所需介面的FTD。在Interface部分下，從右角下拉選單中選擇Create Sub-interface/BVI，然後建立介面並關聯相應的介面。儲存配置並同步到裝置。



- 通過執行Show interface ip brief檢查是否在FTD上建立了介面，然後繼續遷移介面對映。

2.路由表

- 通過執行Show routing route或Show routing route summary檢驗Palo Alto防火牆上的路由表。
- 在將路由遷移到FTD之前，請驗證該表，並根據專案需要選擇所需的路由。
- 通過Show route all和show route summary驗證FTD中的相同路由表。

3.最佳化

- 最佳化對象面板呈灰色顯示，有時必須在FMC中建立手動對象並對其進行對映。若要在FTD中檢視對象，請使用Show Running |在對象和Palo Alto中，使用Show address <object name>。
- 應用程式遷移需要在遷移之前對Palo Alto防火牆進行稽核，FTD具有專用的IPS裝置或者您可以在FTD中啟用該功能，以便您根據客戶要求計畫應用程式遷移任務。
- Palo Alto防火牆的NAT配置必須通過show running nat-policy進行驗證，並且您必須在FTD中具有自定義NAT策略，該策略可在FTD中通過Show Running nat檢視。

結論

藉助FMT，Palo Alto防火牆已成功遷移至思科FTD。在FTD上執行遷移後發生任何問題，以及進行疑難排解，請進一步開啟TAC案例。

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）。