使用FMT將Paloalto遷移到Firepower威脅防禦

目錄

簡介

本文檔介紹將Paloalto防火牆遷移到Cisco Firepower威脅裝置的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower遷移工具
- Paloalto防火牆
- 安全防火牆威脅防禦(FTD)
- 思科安全防火牆管理中心(FMC)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 帶Firepower遷移工具(FMT)v7.7的Mac OS
- PAN NGFW版本8.0+
- 安全防火牆管理中心(FMCv)v7.6
- 安全防火牆威脅防禦版本7.4.2

免責聲明：本文檔中引用的網路和IP地址未與任何單個使用者、組或組織關聯。此配置專為實驗室環境而建立。

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。

概觀

本文檔的具體要求包括：

- PAN NGFW版本8.4+或更高版本
- 安全防火牆管理中心(FMCv)版本6.2.3或更高版本

防火牆遷移工具支援以下裝置清單：

- Cisco ASA(8.4+)
- 具備FPS的Cisco ASA(9.2.2+)
- 思科安全防火牆裝置管理員(7.2+)
- 檢查點(r75-r77)
- 檢查點(r80-r81)
- Fortinet(5.0+)
- Palo Alto Networks(8.0+)

背景資訊

在遷移Paloalto防火牆配置之前，請執行以下活動：

獲取Paloalto防火牆配置zip檔案

- Paloalto防火牆的版本必須是8.4+。
- 從Palo Alto防火牆匯出當前運行配置（*.xml必須採用xml格式）。
- 登入到Paloalto Firewall Cli以執行show routing route並以txt格式(*.txt)儲存輸出。
- 壓縮副檔名為*.zip的運行配置檔案(*.xml)和路由檔案(*.txt)。

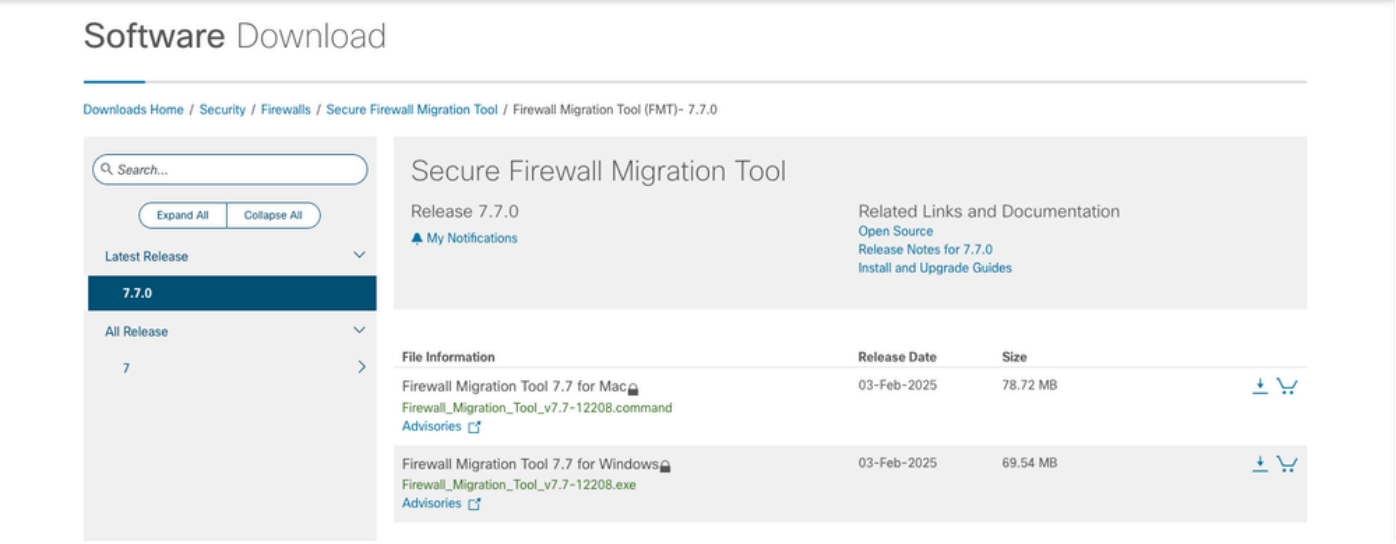
遷移前檢查清單

- 在開始遷移過程之前，確保FTD已註冊到FMC。
- 已在FMC上建立具有管理許可權的新使用者帳戶。或者可以使用現有的管理員憑據。
- 匯出的Palo Alto運行配置檔案.xml必須使用.zip副檔名進行壓縮（請按照上一節中提到的步驟操作）。
- 與Paloalto防火牆介面相比，Firepower裝置的物理或子介面或埠通道的數量必須相同或更多。

設定

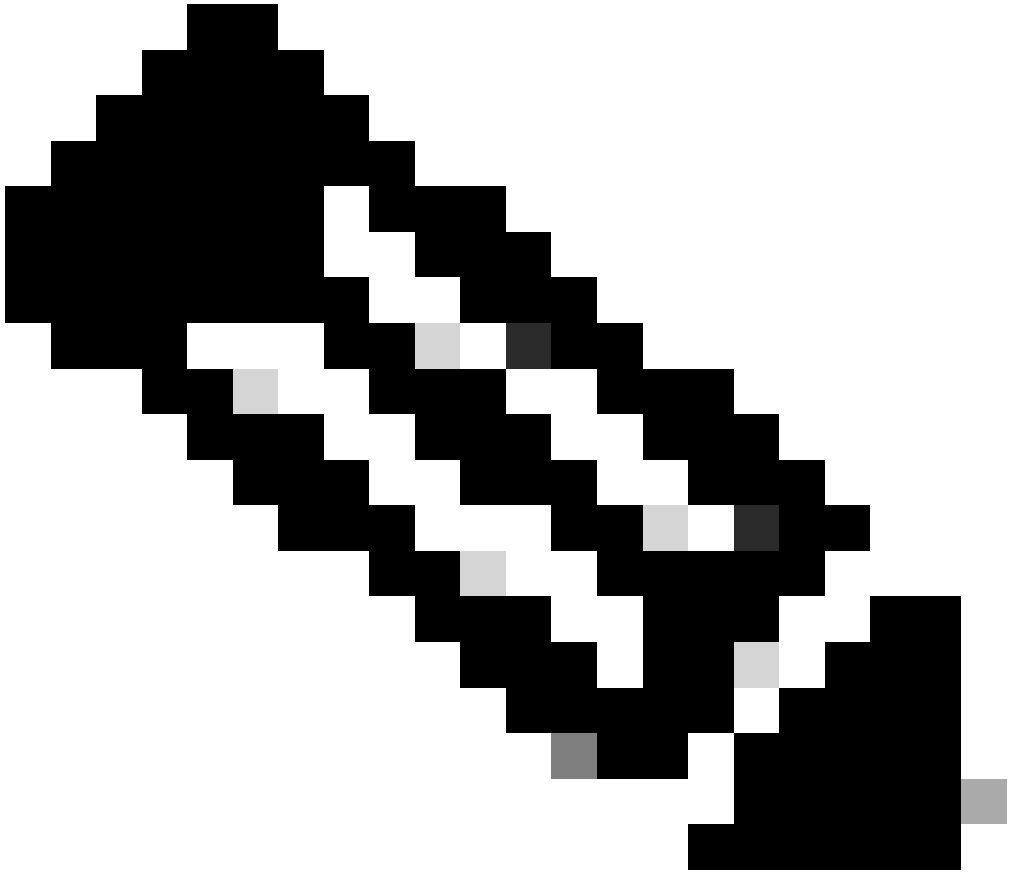
遷移步驟

1.從與您的電腦相容的思科軟體中心下載最新的Firepower遷移工具：



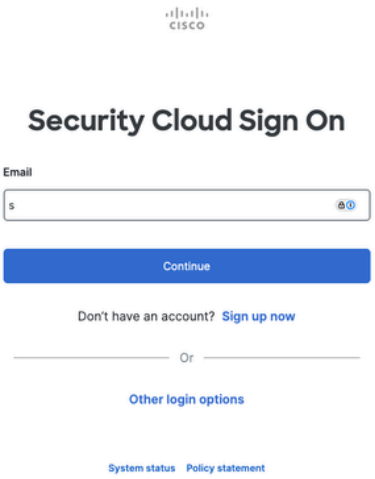
FMT下載

3. 開啟您以前下載到電腦的檔案。



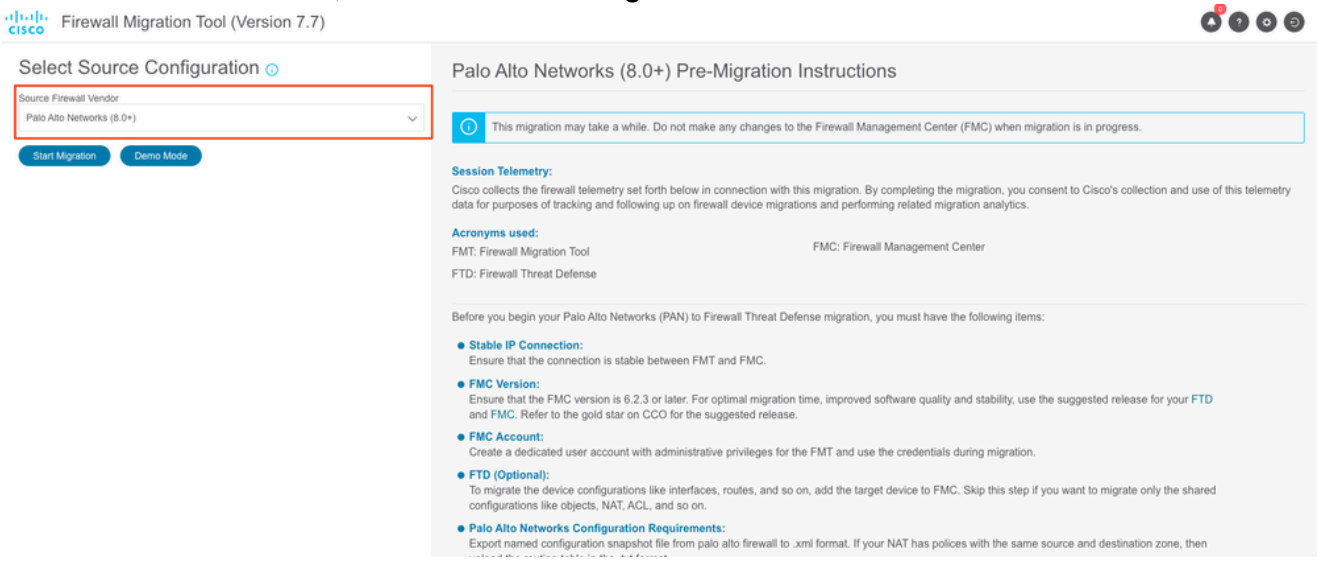
附註：該程式將自動開啟，控制檯將在運行檔案的目錄上自動生成內容。

4. 運行該程式後，它會開啟一個顯示終端使用者許可協定的Web瀏覽器。
    1. 選中此覈取方塊以接受條款和條件。
    2. 按一下「繼續」。
5. 使用有效的CCO憑證登入，以存取FMT GUI。



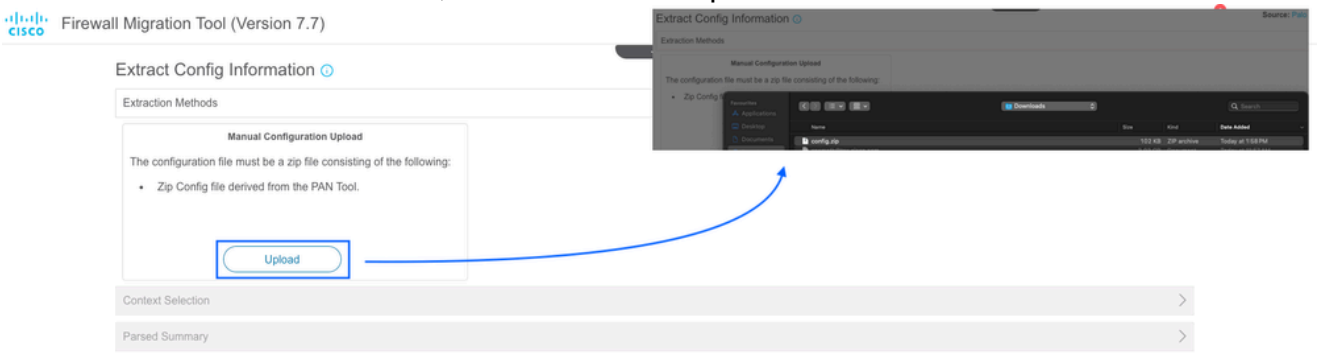
FMT登入提示

6. 選擇要遷移的源防火牆，然後按一下Start Migration。



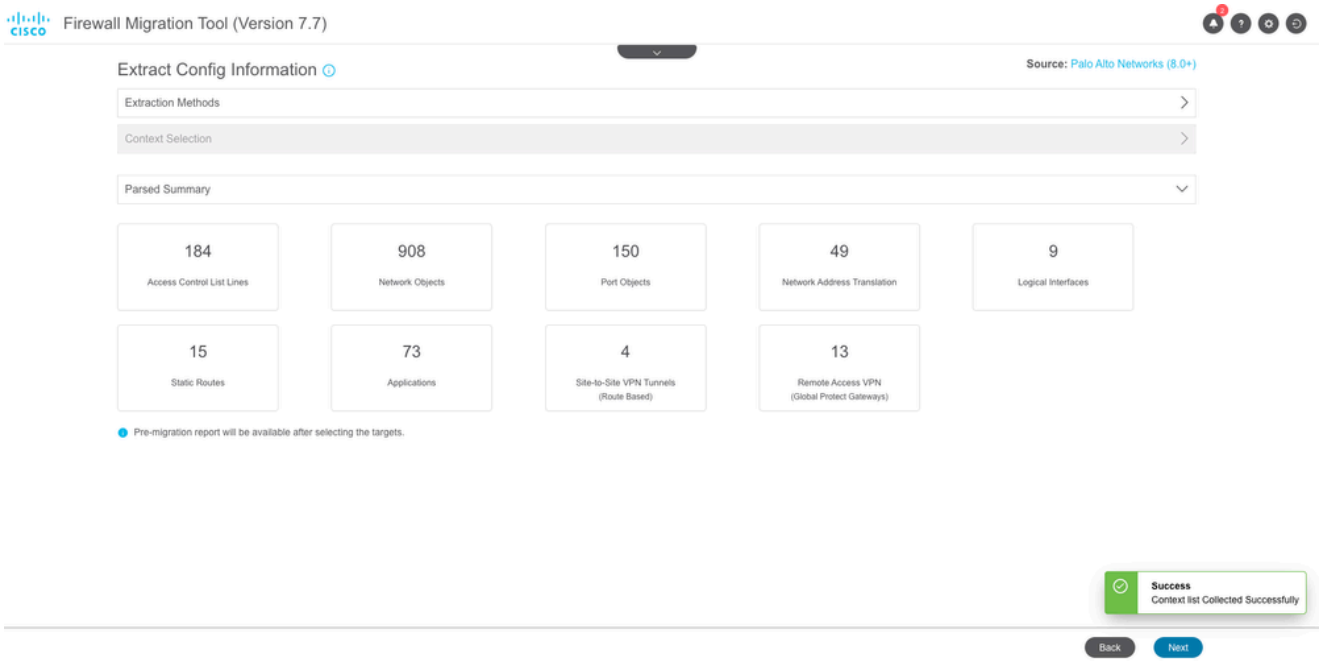
FMT GUI

7. 此時將顯示「提取方法」部分，您必須在其中將Zip配置檔案從Paloalto防火牆上傳到FMT。



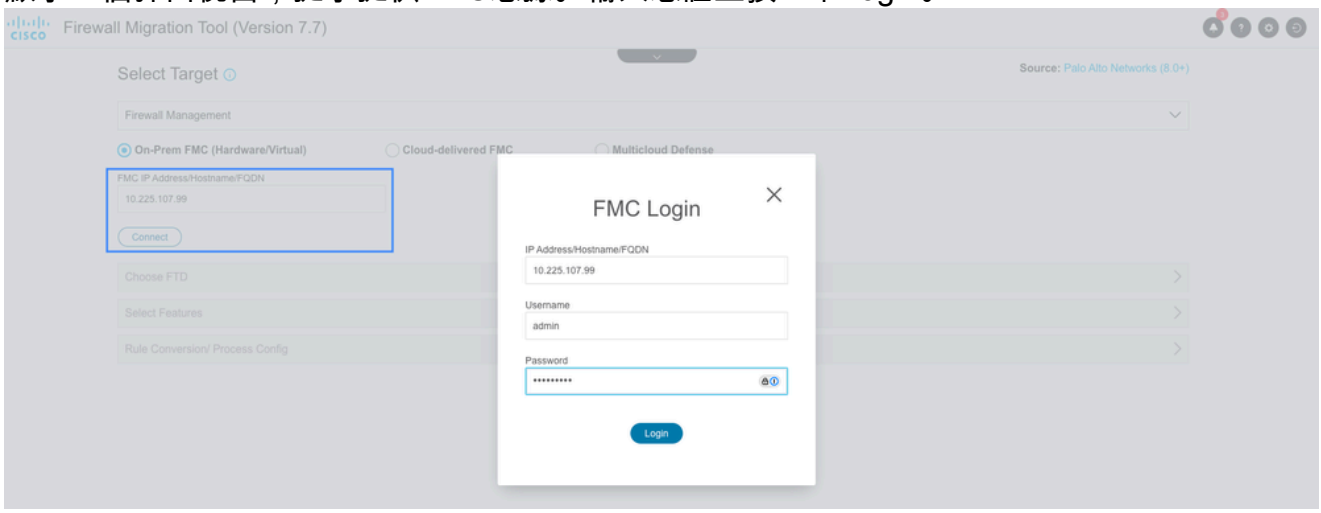
配置上載嚮導

8. 上載配置檔案後，將顯示已分析的配置摘要。對於VSYS，可使用單獨的VSYS選擇。必須逐個分析並遷移它們。
驗證已分析的摘要並點選下一步圖示。



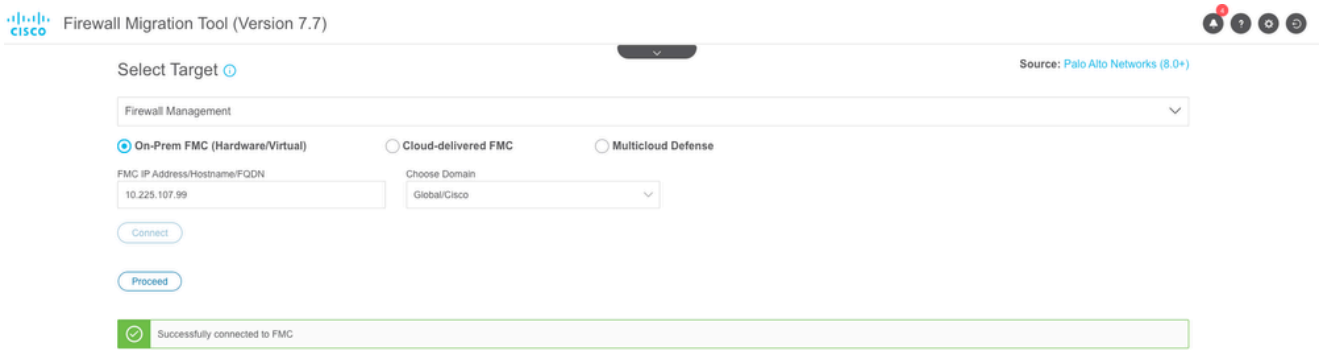
配置驗證摘要

9. 您可以在此部分選擇FMC的型別。提供其管理IP地址，然後按一下Connect。
顯示一個彈出視窗，提示提供FMC憑據。輸入憑證並按一下Login。



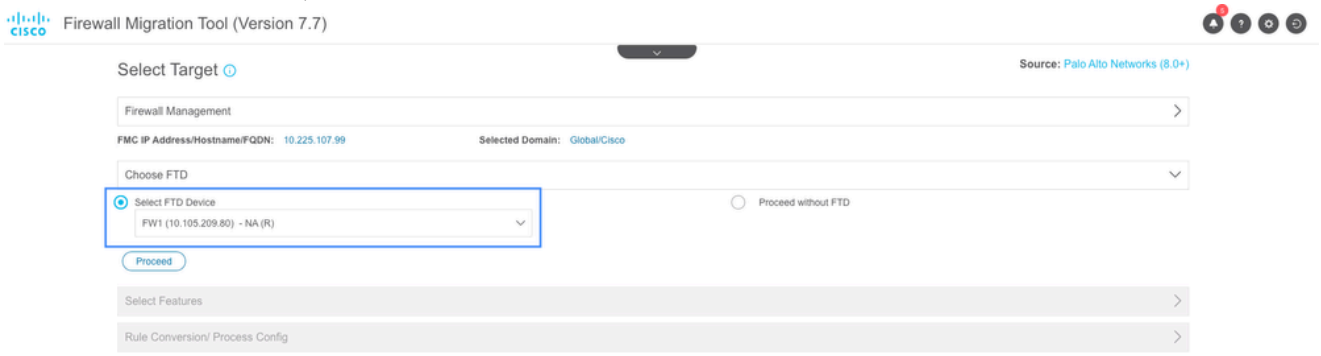
FMC登入

10. 成功連線到FMC後，您現在可以選擇Domain（如果有），然後點選Proceed。



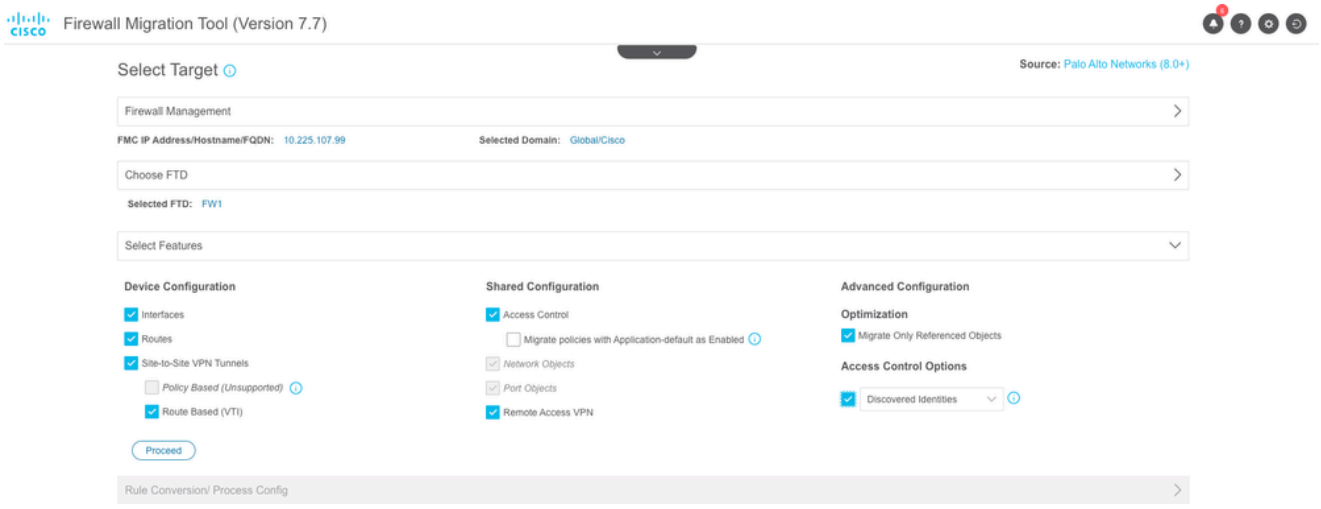
域選擇

11. 選擇要遷移到的FTD，然後按一下Proceed。



選擇目標FTD

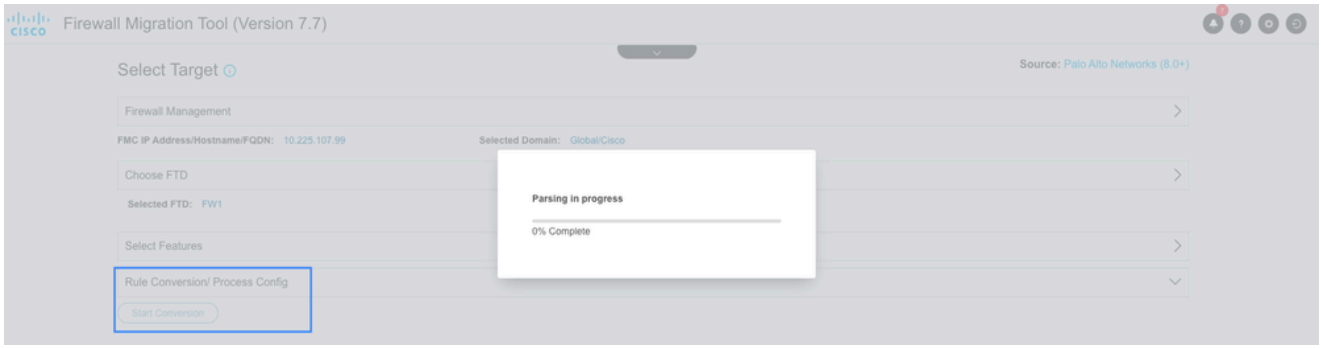
12. 該工具現在列出了要遷移的功能。按一下「Proceed」。



功能選擇

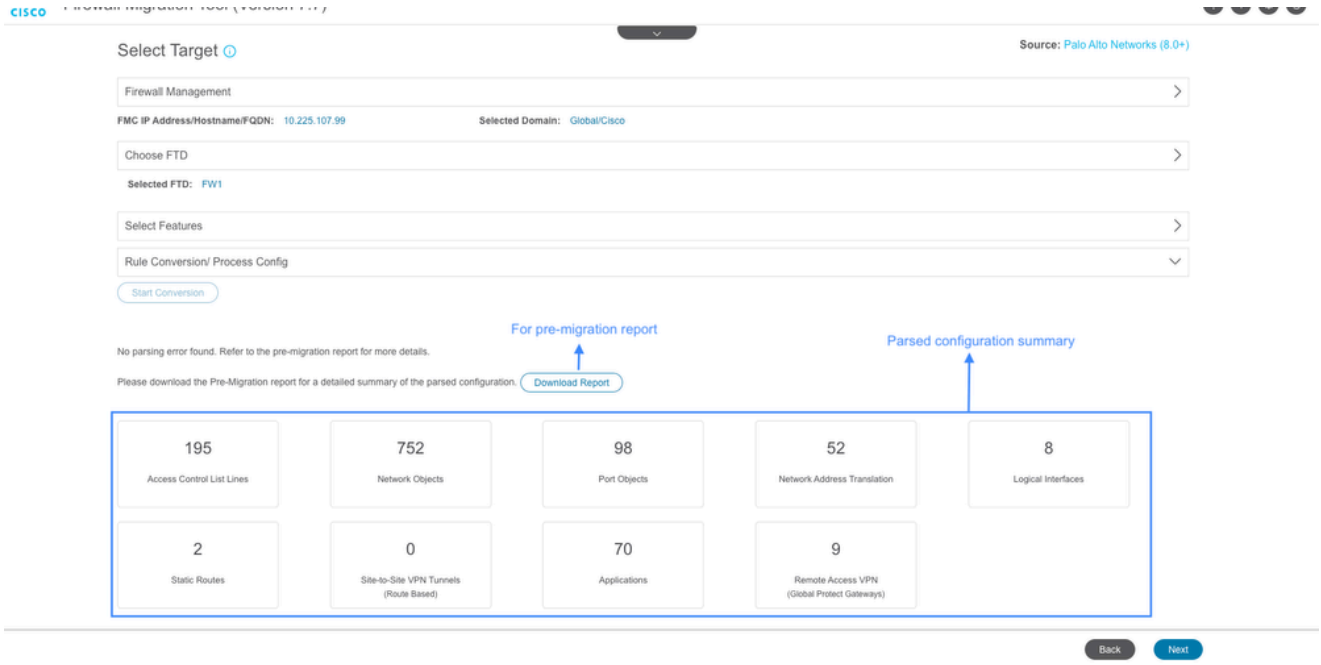
附註：預設情況下，所有特徵都將被選取。您可以取消選擇任何不遷移的配置。

13. 按一下Start Conversion轉換配置。



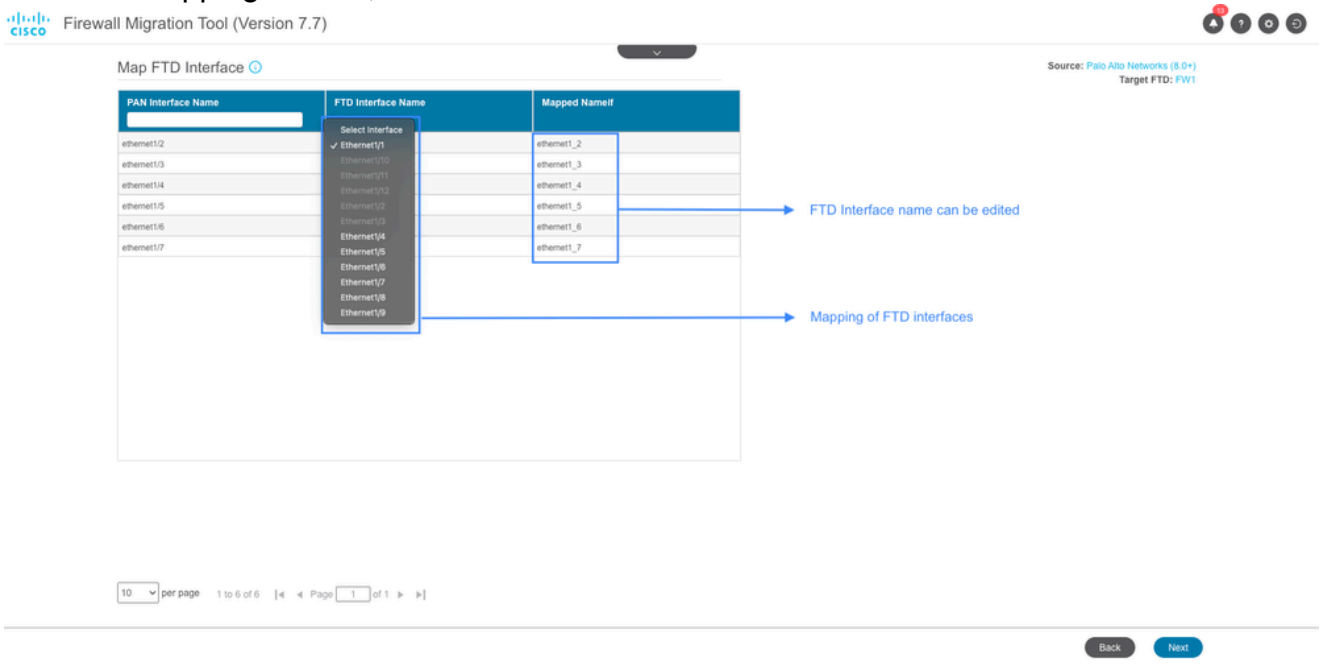
正在分析配置

該工具將分析配置並顯示轉換摘要，如下圖所示。您還可以下載遷移前報告，以驗證遷移的配置是否有任何Errors或Warnings（如果有）。 按一下下一步導航到下一頁。



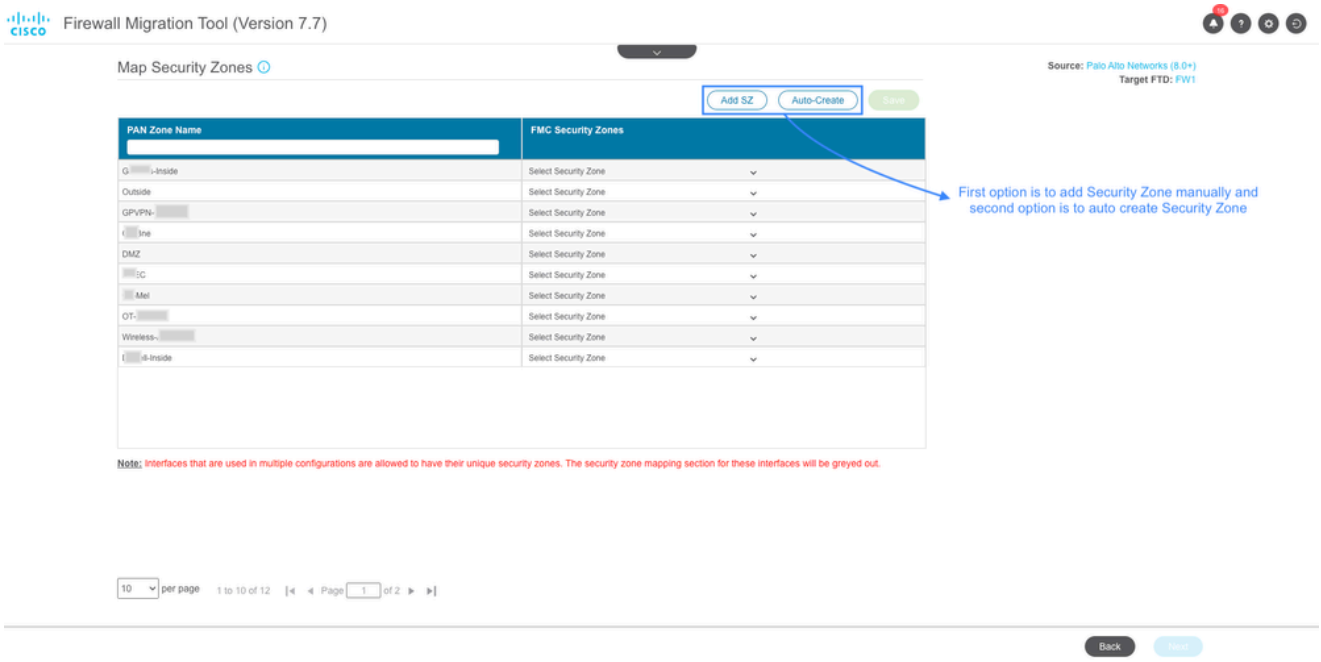
分析的配置摘要

14. 您可以在Interface Mapping部分定義Paloalto到FTD介面對映以及編輯每個介面的介面名稱。Interface Mapping完成後，按一下Next。



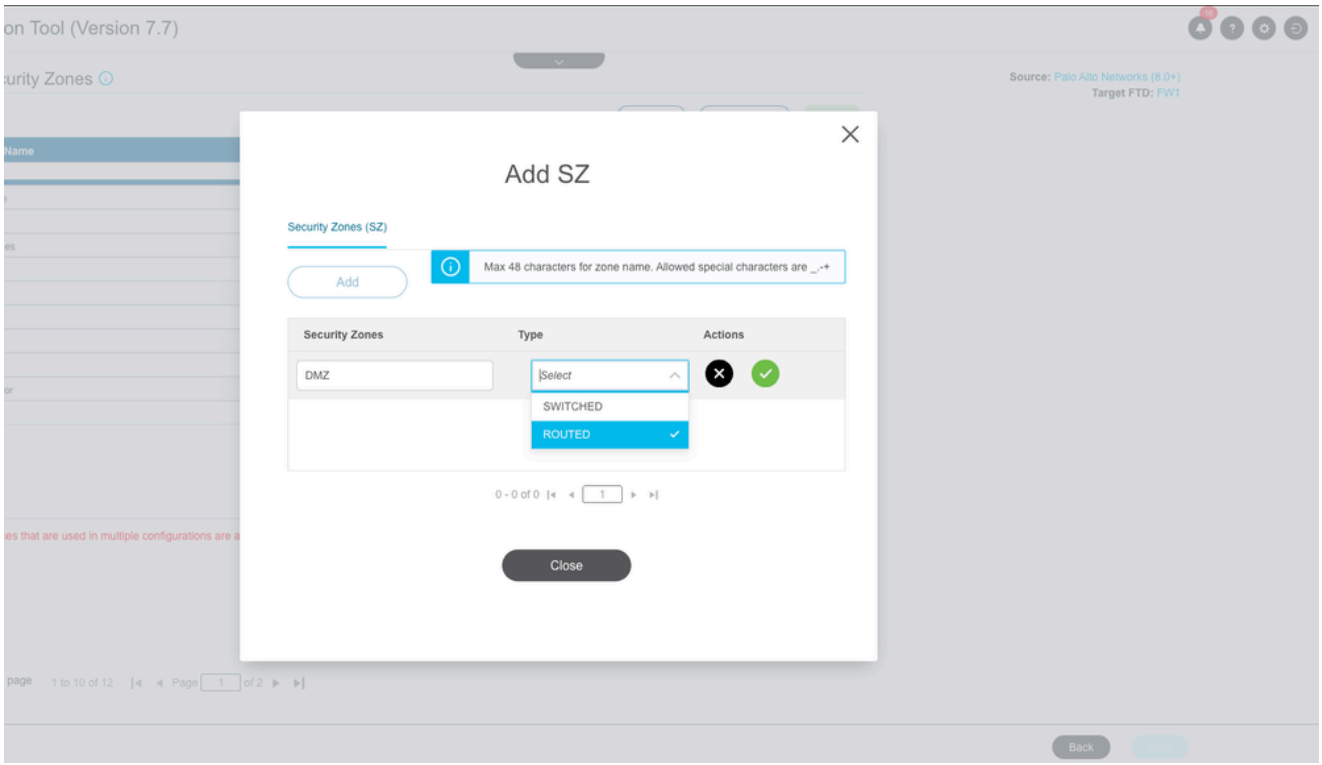
介面對應

15. 您可以手動為每個介面新增安全區域，也可以在對映安全區域部分中自動建立安全區域。建立和對映安全區域後，按一下下一步。



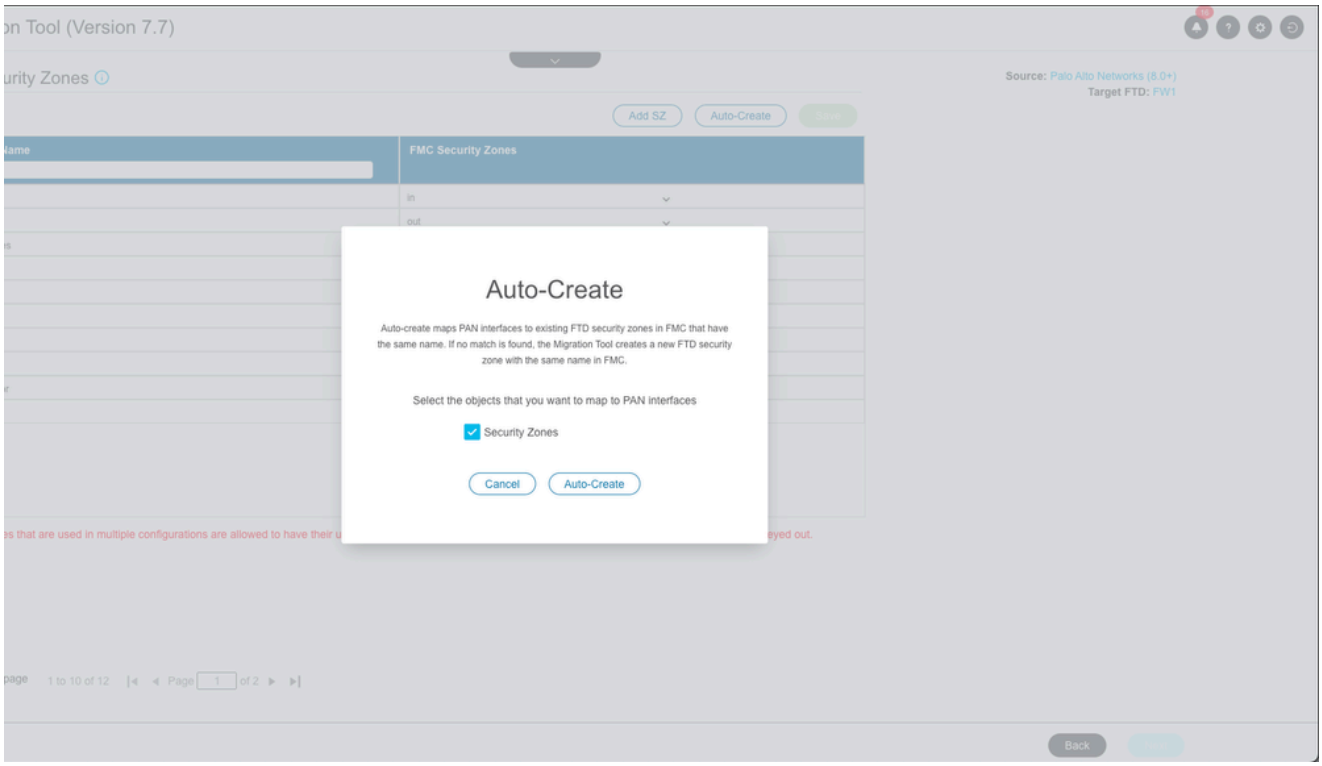
安全區域建立

手動建立安全區域：



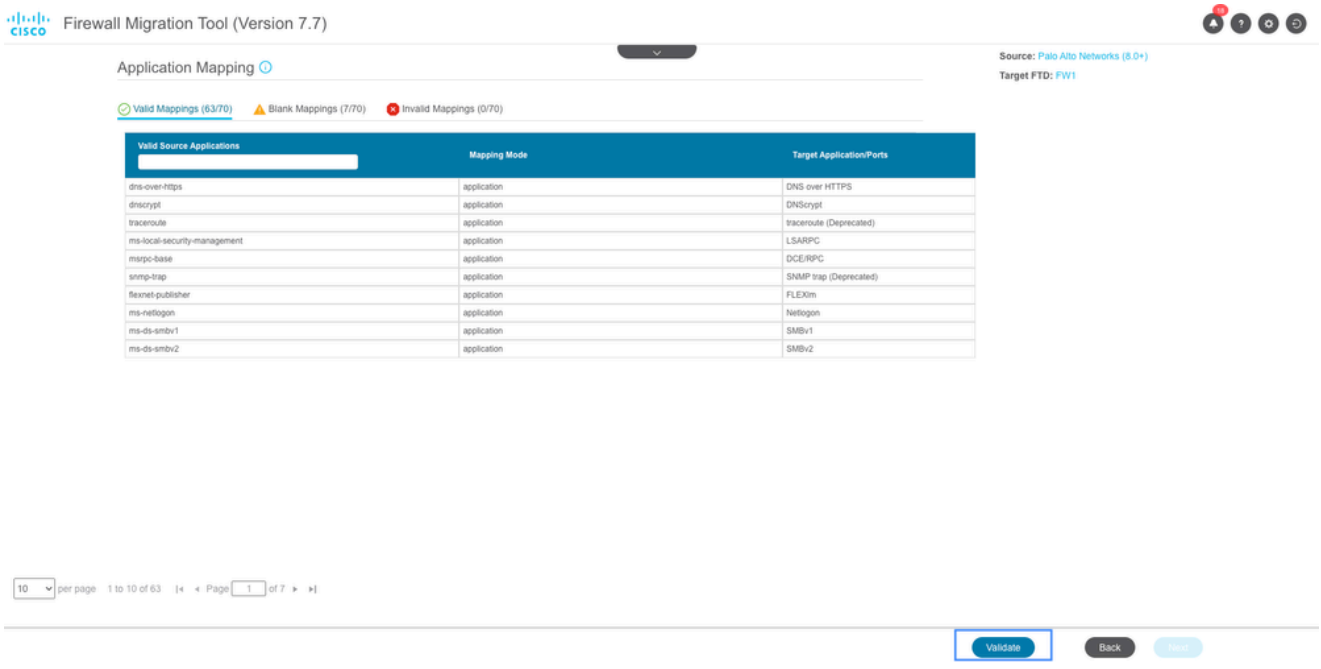
手動建立安全區域

自動建立安全區域：

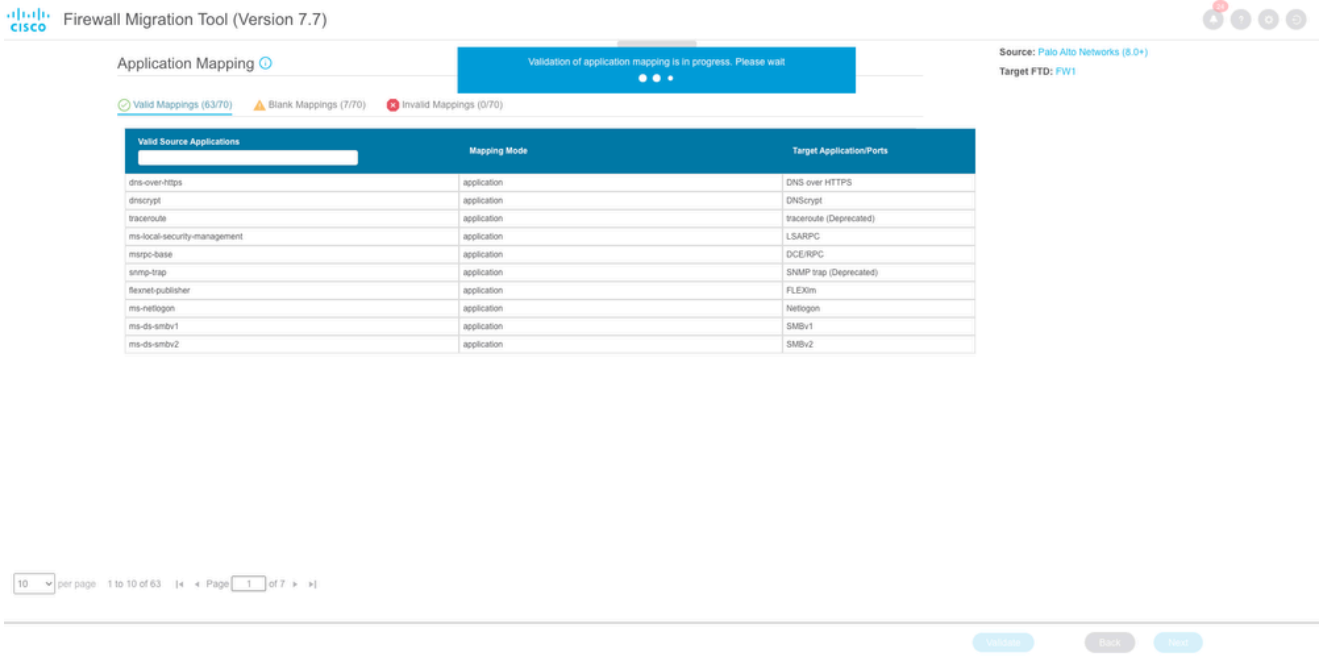


自動安全區域建立

16. 現在，您可以轉到「應用程式對映」部分。按一下驗證按鈕驗證應用程式對映。



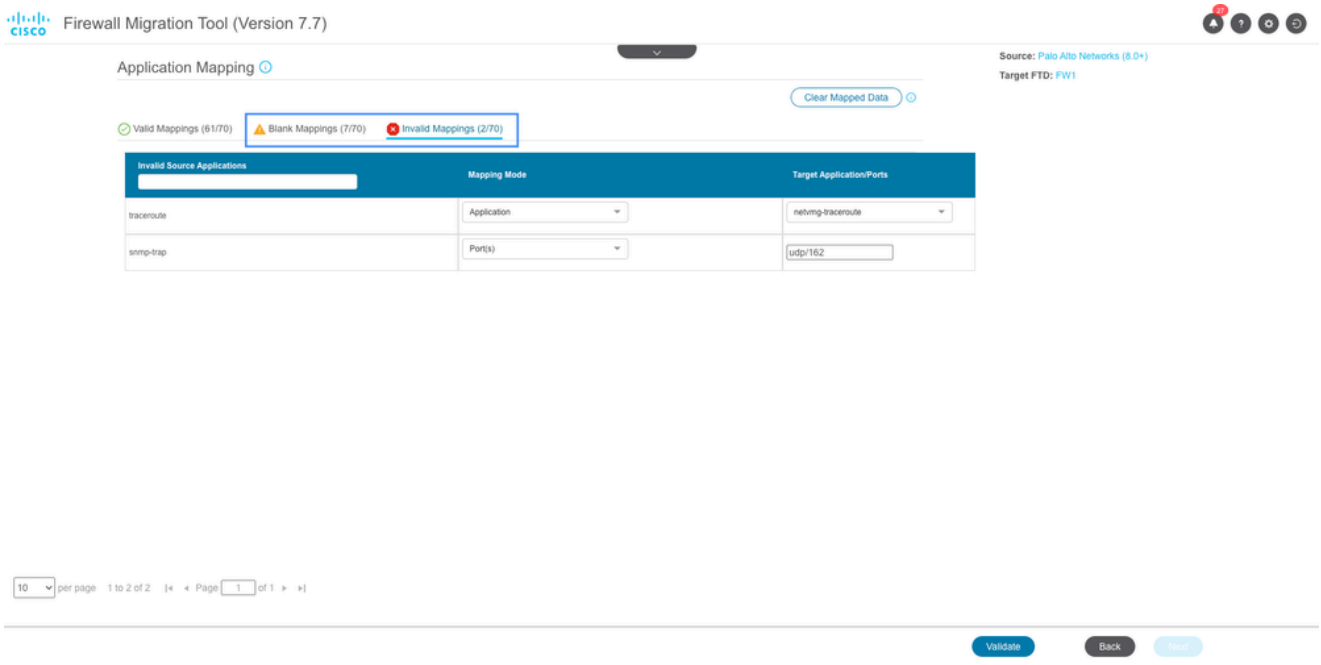
應用程式對映



應用程式對映驗證

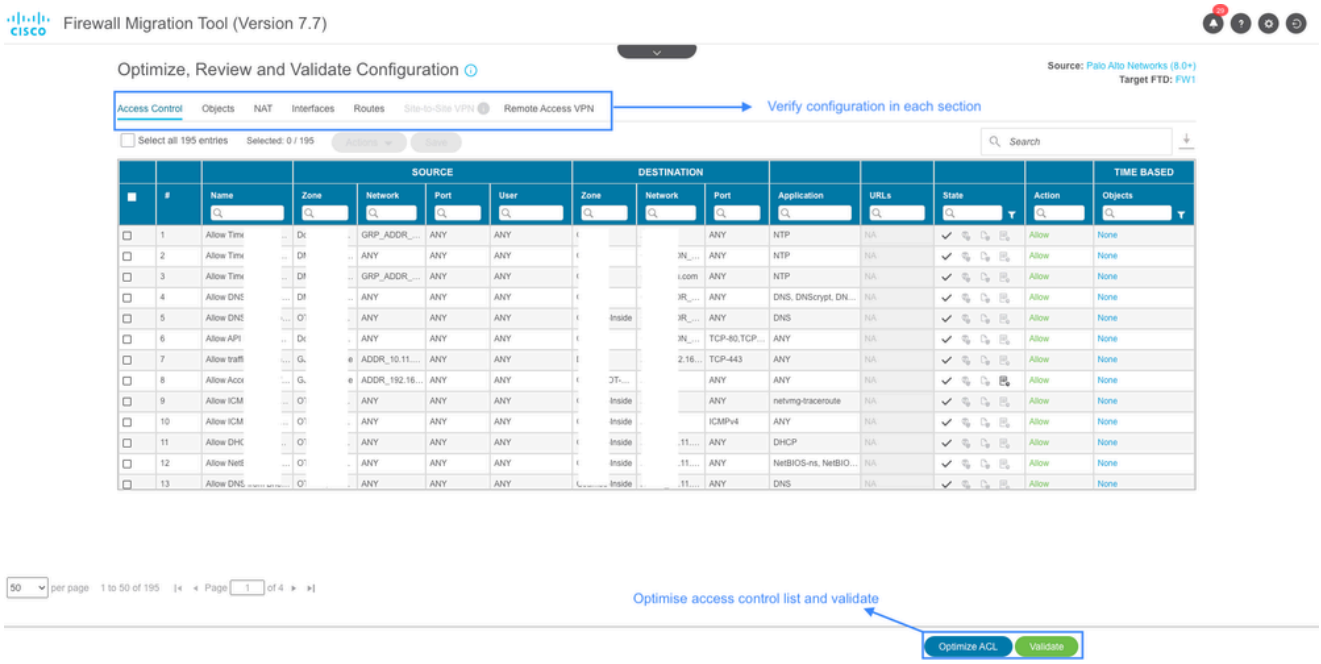
驗證後，FMT將列出空白和無效對映。在繼續進一步之前必須更正無效對映，並且更正空對映是可選的。

再次按一下Validate以驗證已更正的對映。驗證成功後按一下Next。



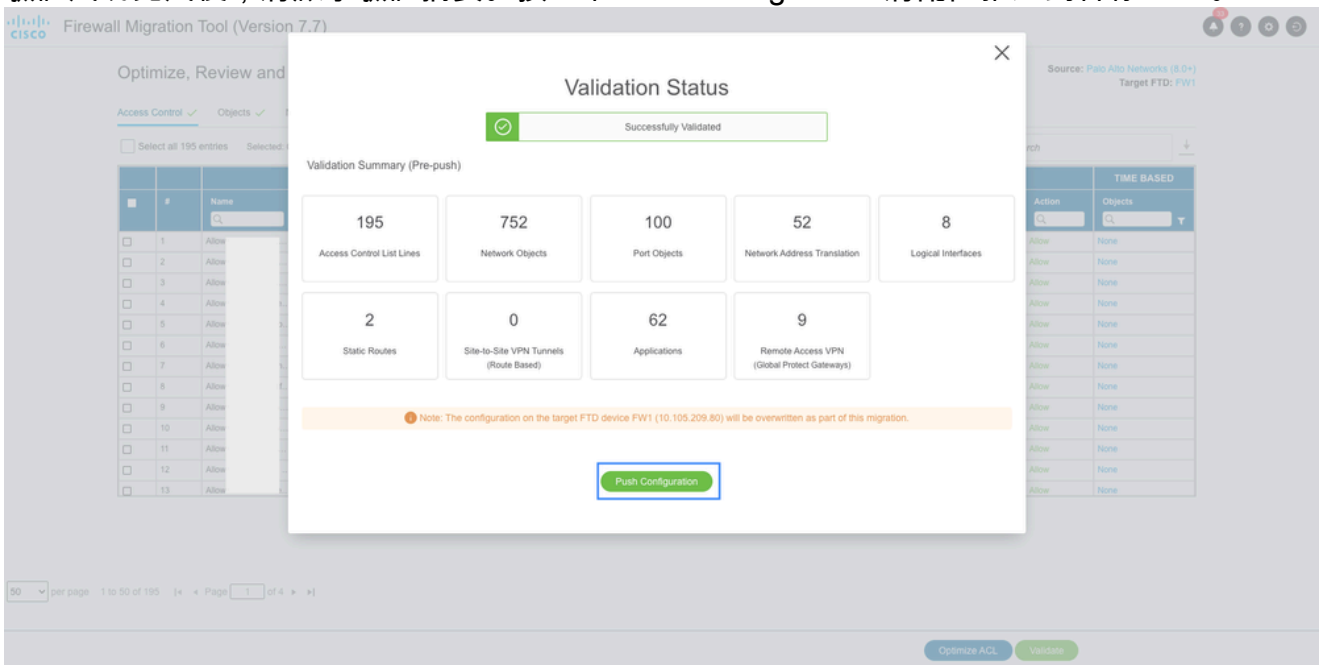
空白和無效的應用程式對映

17. 如果需要，可以在下一節中最佳化ACL。檢視每個部分中的配置，如訪問控制、對象、NAT、介面、路由和遠端訪問VPN。檢視配置後按一下Validate。



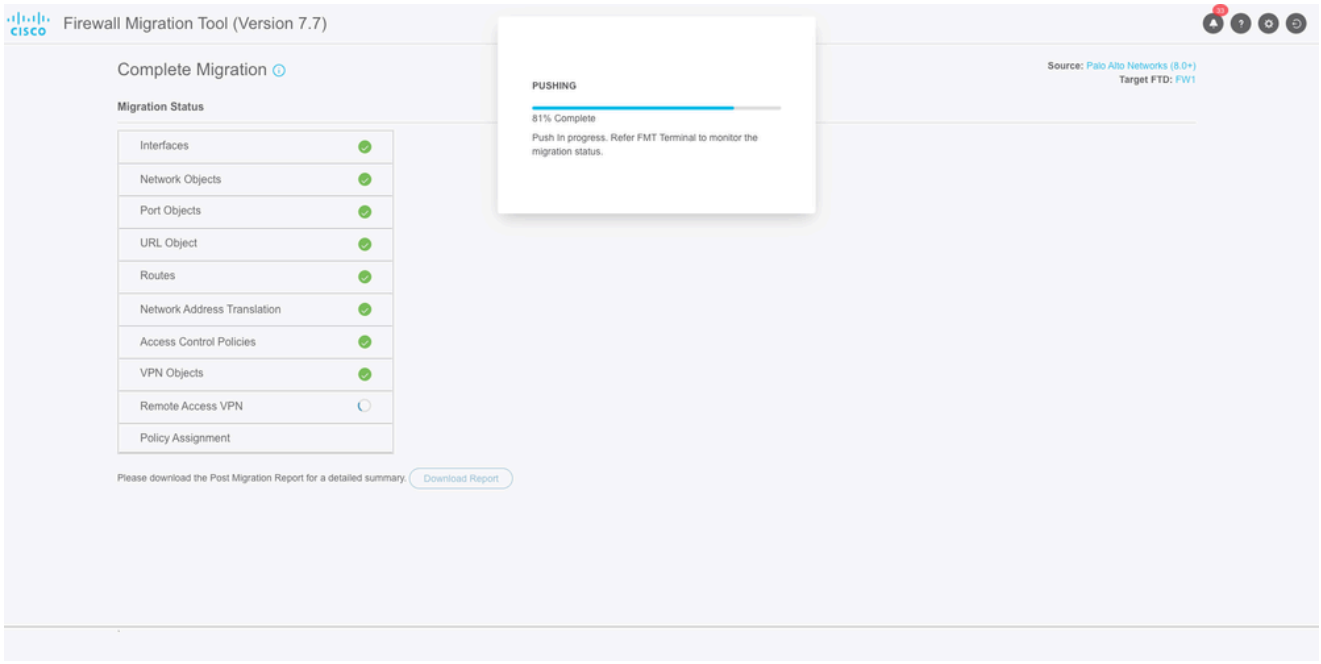
組態驗證

18. 驗證成功完成後，將顯示驗證摘要。按一下Push Configuration將配置推送到目標FMC。



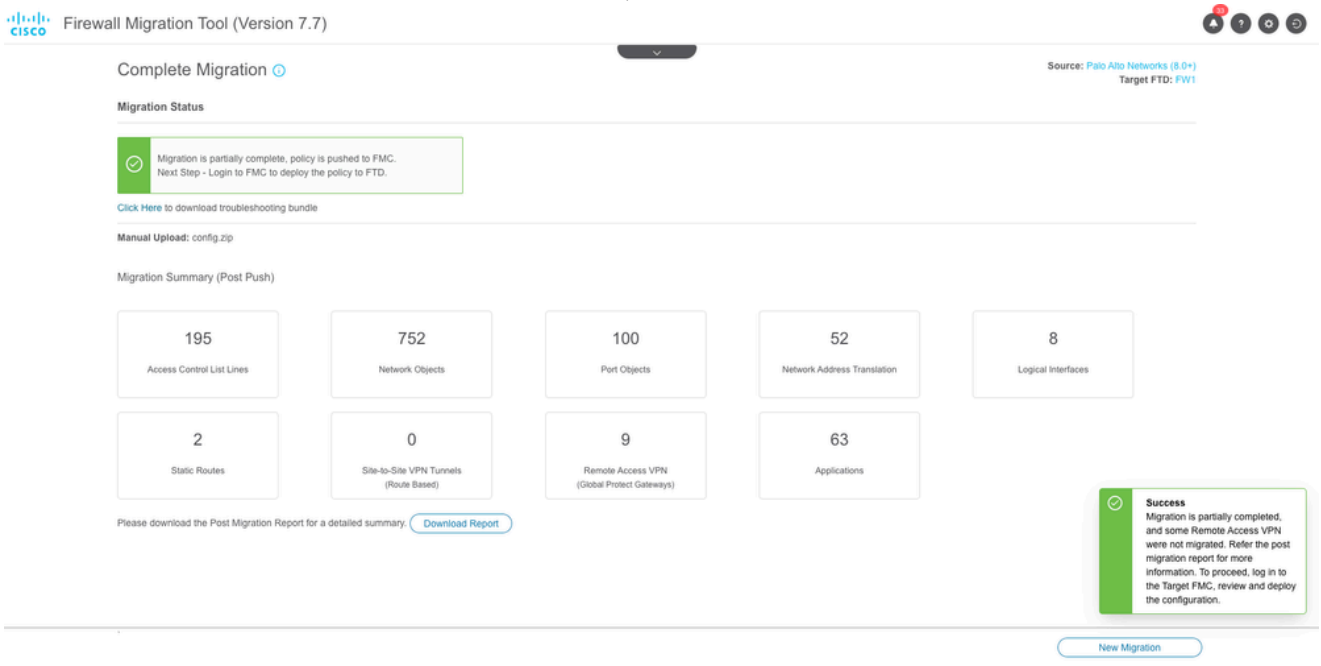
配置驗證摘要

19. 現在，向FMC推送配置的進度顯示在「遷移狀態」部分中。您也可以使用FMT終端視窗監控遷移狀態。



遷移狀態

20. 遷移成功後，該工具將顯示遷移摘要。其中還列出了部分遷移的配置（如果有）。例如，由於缺少安全客戶端軟體包，在此場景中配置遠端訪問VPN。
    您還可以下載遷移後報告來檢查遷移的配置，以及是否有任何錯誤或更正操作。



成功遷移摘要

21. 最後一步是檢視從FMC遷移的組態和將組態部署到FTD。
    若要部署組態：
    1. 登入到FMC GUI。
    2. 導覽至Deploy索引標籤。
    3. 選擇要將配置推送到防火牆的部署。
    4. 按一下「Deploy」。

疑難排解

安全防火牆遷移工具故障排除

常見的遷移失敗：

- PaloAlto配置檔案中未知或無效的字元。
- 配置元素缺失或不完整。
- 網路連線問題或延遲。
- 在PaloAlto配置檔案上傳期間或將配置推送到FMC時出現問題。

使用支援捆綁包進行故障排除：

- 在「Complete Migration」螢幕上，按一下Support按鈕。
- 選擇「Support Bundle」，然後選擇要下載的配置檔案。
- 預設情況下會選擇日誌和資料庫檔案。
- 按一下「Download」以取得.zip檔案。
- 解壓縮.zip以檢視日誌、資料庫和配置檔案。
- 按一下Email us，將故障詳細資訊傳送給技術團隊。
- 在電子郵件中附加支援捆綁包。
- 按一下Visit TAC page以建立Cisco TAC案例以取得協助。

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）。