使用FMT將ASA遷移到Firepower威脅防禦(FTD)

目錄

簡介

本文檔介紹將Cisco Adaptive Security Appliance(ASA)遷移到Cisco Firepower Threat Device的過程。

必要條件

需求

思科建議您瞭解思科防火牆威脅防禦(FTD)和自適應安全裝置(ASA)。

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)的Mac OS v7.0.1
- 調適型安全裝置(ASA)v9.16(1)
- 安全防火牆管理中心(FMCv)v7.4.2
- 安全防火牆威脅防禦虛擬(FTDv)v7.4.1

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：

- Cisco Adaptive Security Appliance(ASA)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)
- Fortinet(5.0+)

· Palo Alto Networks(6.1+)

背景資訊

在遷移ASA配置之前，請執行以下活動：

獲取ASA配置檔案

要遷移ASA裝置，請使用show running-config用於單情景，或使用show tech-support用於多情景模式獲取配置，將其另存為.cfg或.txt檔案，然後使用安全防火牆遷移工具將其傳輸到電腦。

從ASA匯出PKI證書並匯入管理中心

使用以下命令通過CLI將帶金鑰的PKI證書從源ASA配置匯出到PKCS12檔案：
ASA(config)#crypto ca export <trust-point-name> pkcs12 <密碼短語>
然後，將PKI證書匯入管理中心（對象管理PKI對象）。 有關詳細資訊，請參閱Firepower管理中心配置指南中的PKI對象。

檢索AnyConnect軟體包和配置檔案

AnyConnect配置檔案是可選的，可以通過管理中心或安全防火牆遷移工具上傳。

使用以下命令將所需的軟體包從源ASA複製到FTP或TFTP伺服器：

複製<原始檔位置：/源檔名> <目標>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <-----複製Anyconnect軟體包的示例。

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <-----複製外部瀏覽器軟體包的示例。

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <-----複製Hostscan包的示例。

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <-----複製Dap.xml的示例

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <復-----Data.xml的示例

----- ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <複製Anyconnect配置檔案的示例。

將下載的軟體包匯入管理中心(對象管理 > VPN > AnyConnect檔案)。

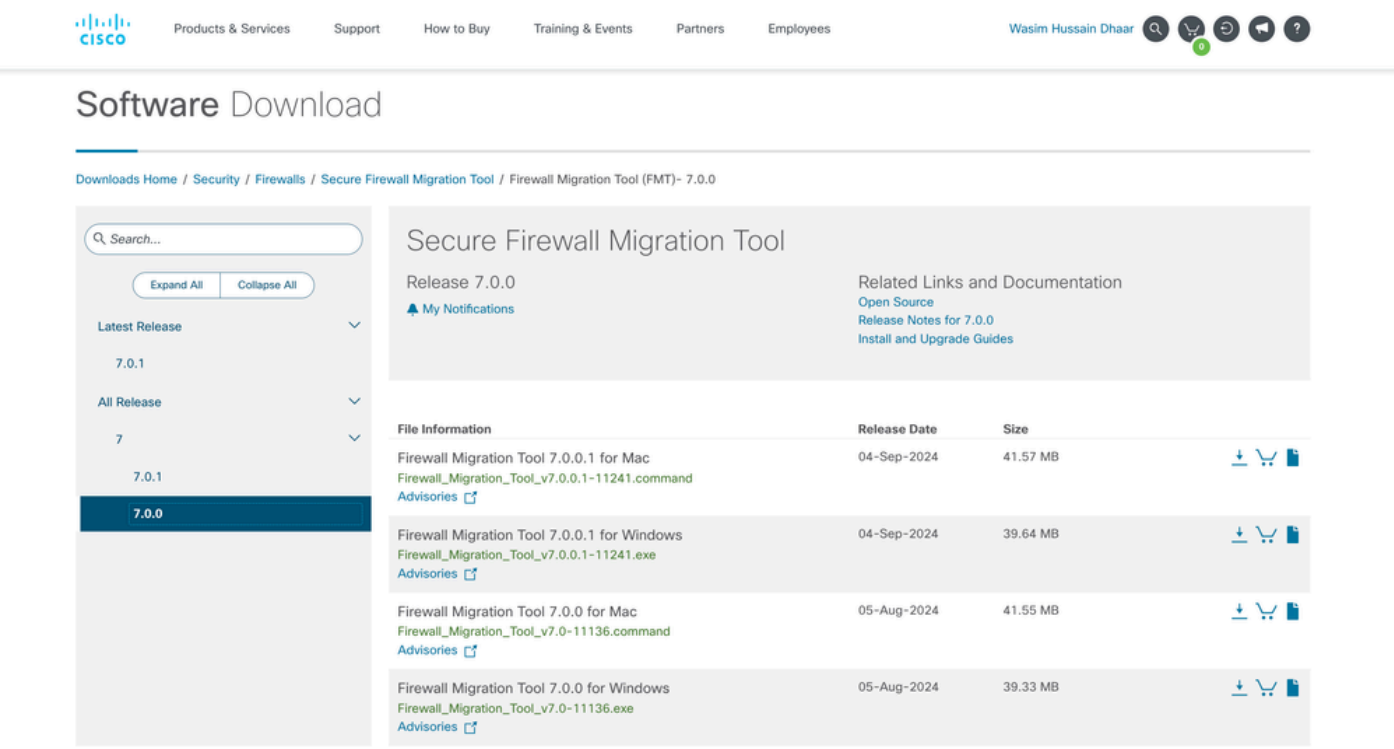
必須從Review and Validate > Remote Access VPN > AnyConnect File一節中的Secure Firewall遷移工具將-Dap.xml和Data.xml上傳到管理中心。

b-AnyConnect配置檔案可以直接上傳到管理中心，或通過稽核和驗證 > 遠端訪問VPN > AnyConnect檔案部分中的Secure Firewall遷移工具上傳。

設定

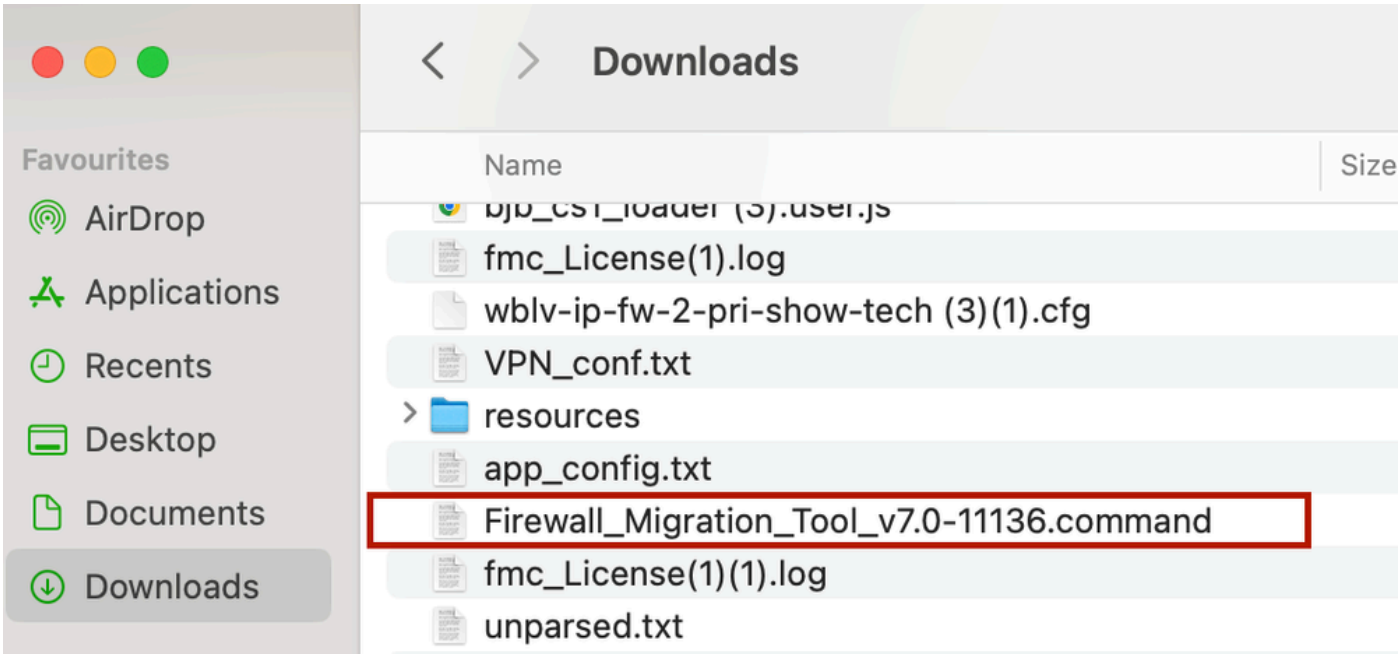
設定步驟:

1.下載 思科軟體中心最新的Firepower遷移工具：

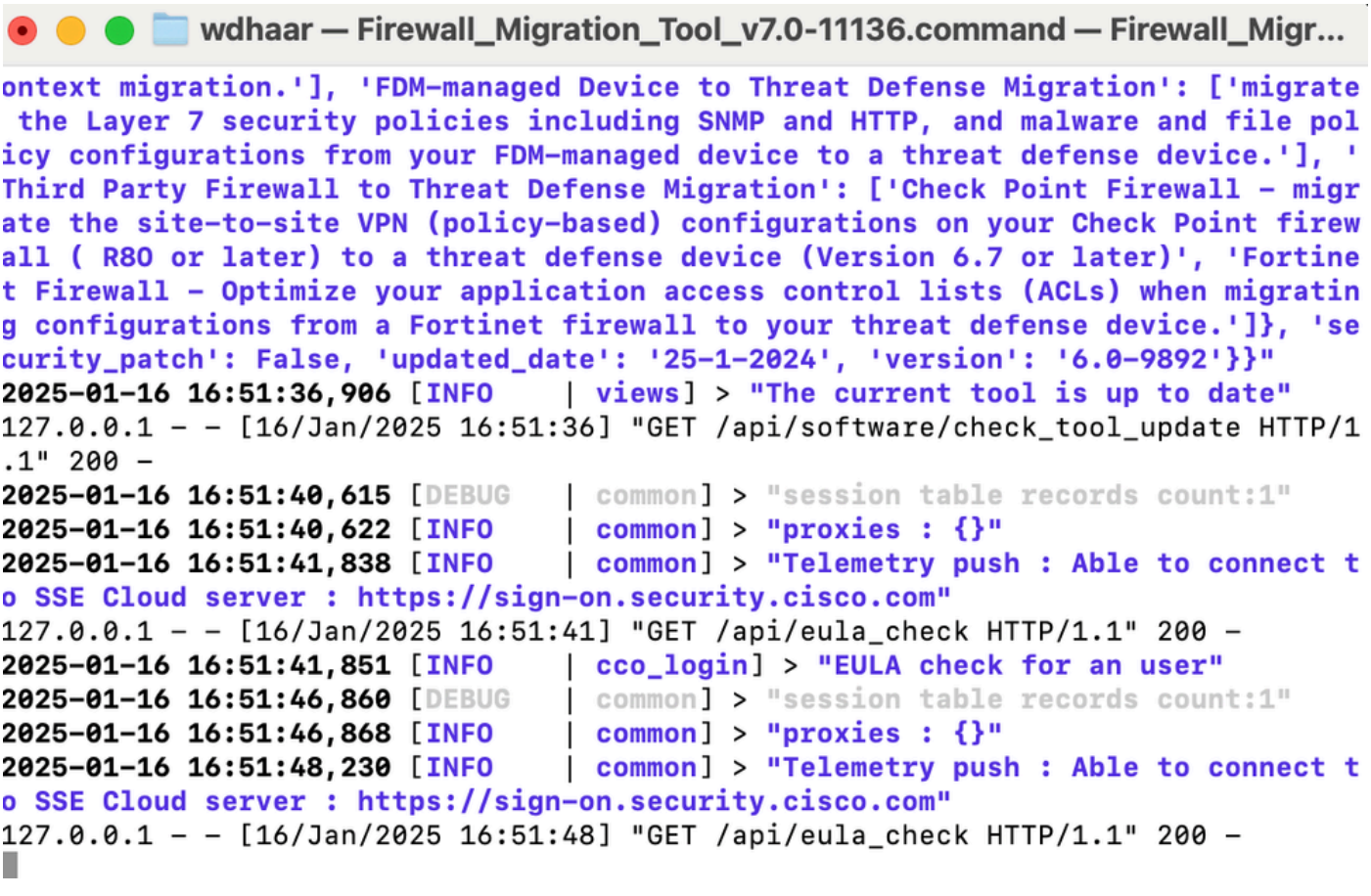


軟體下載

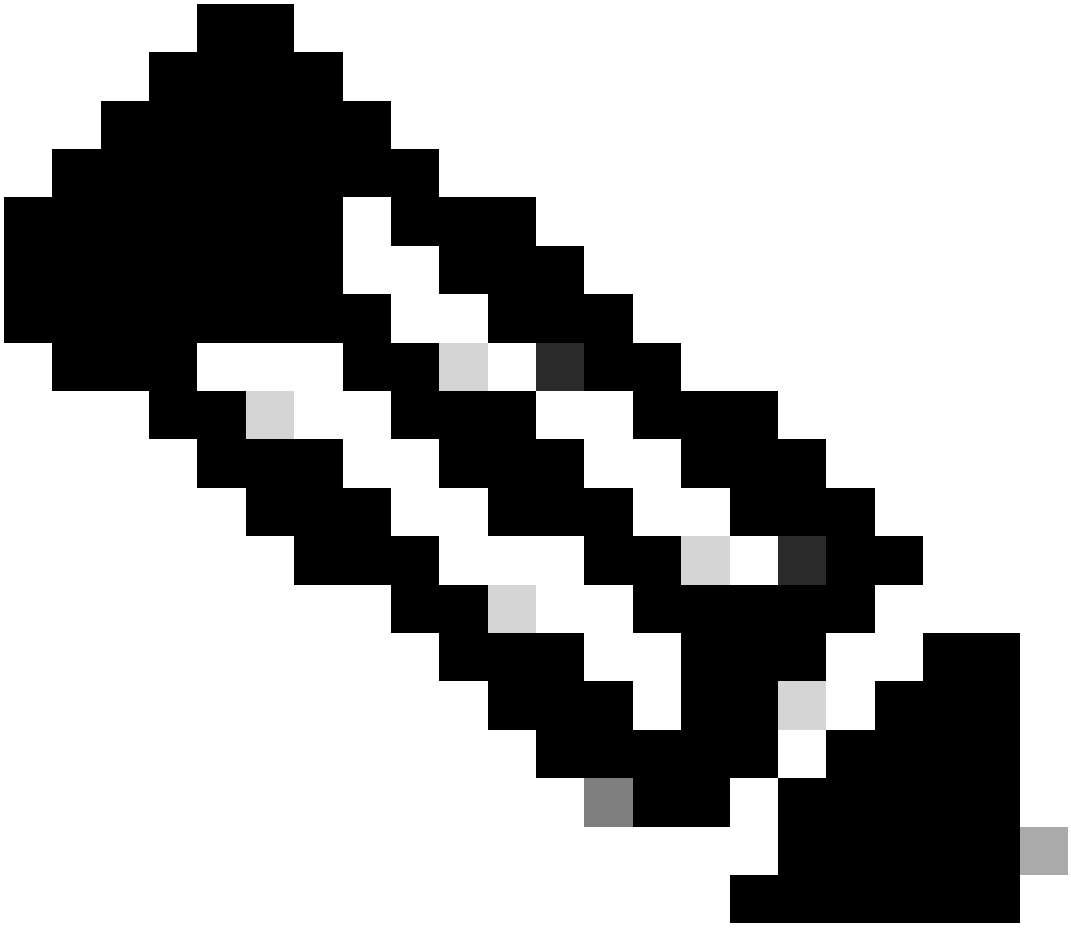
2. 按一下您以前下載到您電腦的檔案。


Downloads
Favourites
AirDrop
Applications
Recents
Desktop
Documents
Downloads
Name
Size
fmc_License(1).log
wblv-ip-fw-2-pri-show-tech (3)(1).cfg
VPN_conf.txt
resources
app_config.txt
Firewall_Migration_Tool_v7.0-11136.command
fmc_License(1)(1).log
unparsed.txt

檔案

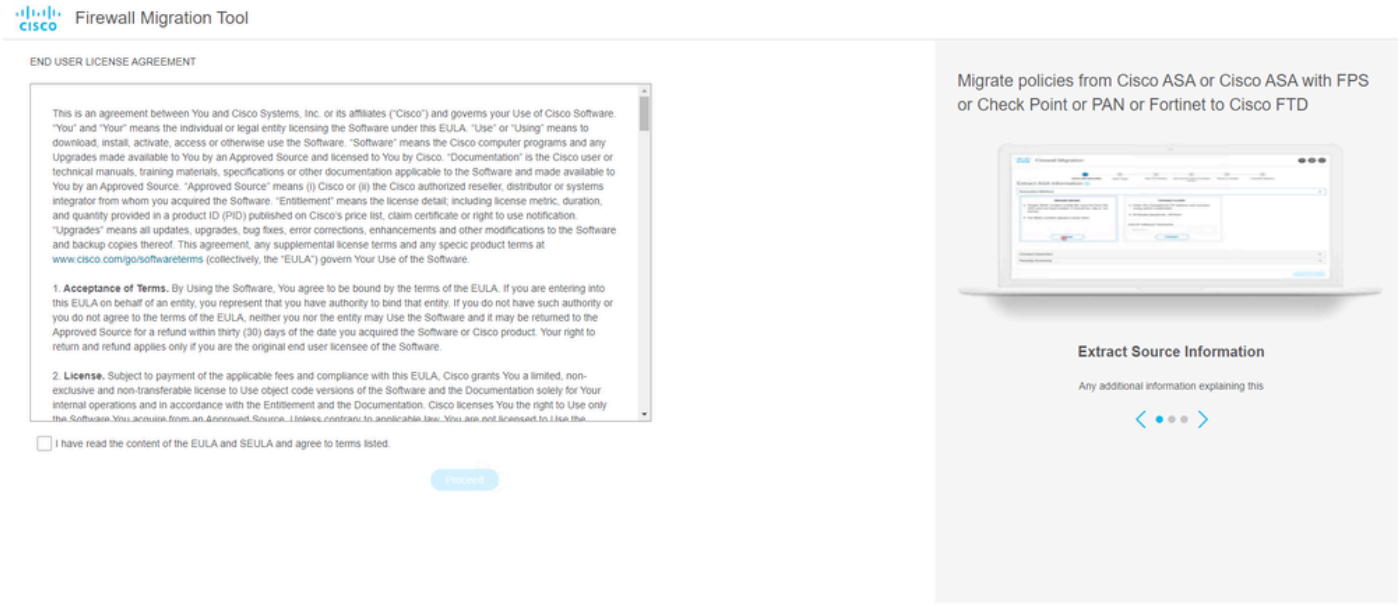

wdhaar — Firewall_Migration_Tool_v7.0-11136.command — Firewall_Migr...
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device.'], 'Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall (R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortinet Firewall - Optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.']}, 'security_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1.1" 200 -
2025-01-16 16:51:40,615 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -

控制檯日誌



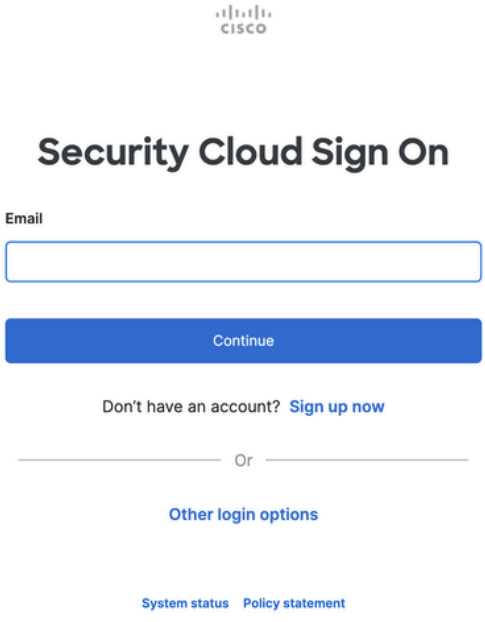
附註：該程式會自動開啟，控制檯會在您運行檔案的目錄上自動生成內容。

3. 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. 選中此覈取方塊接受條款和條件。
    2. 按一下「繼續」。



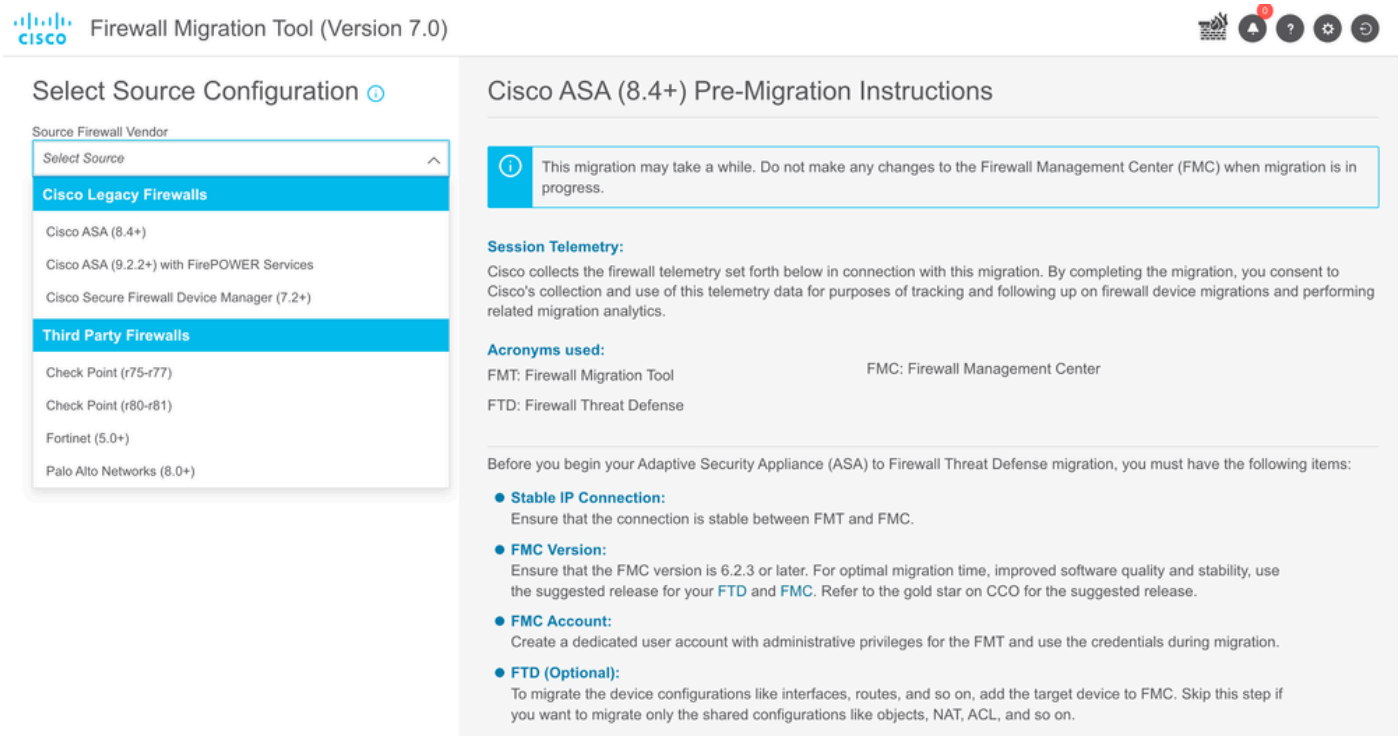
EULA

4. 使用有效的CCO帳戶登入，並且FMT GUI介面顯示在Web瀏覽器上。



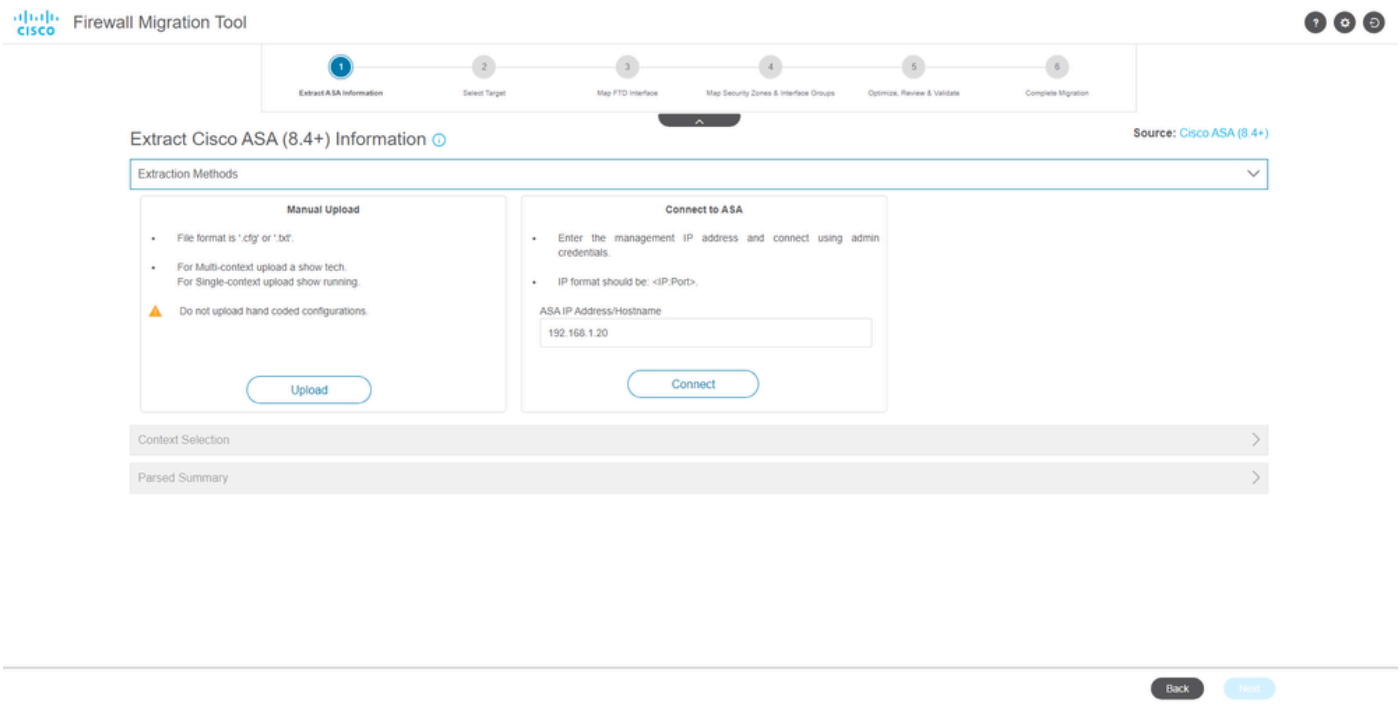
FMT登入

5. 選擇要遷移的源防火牆。

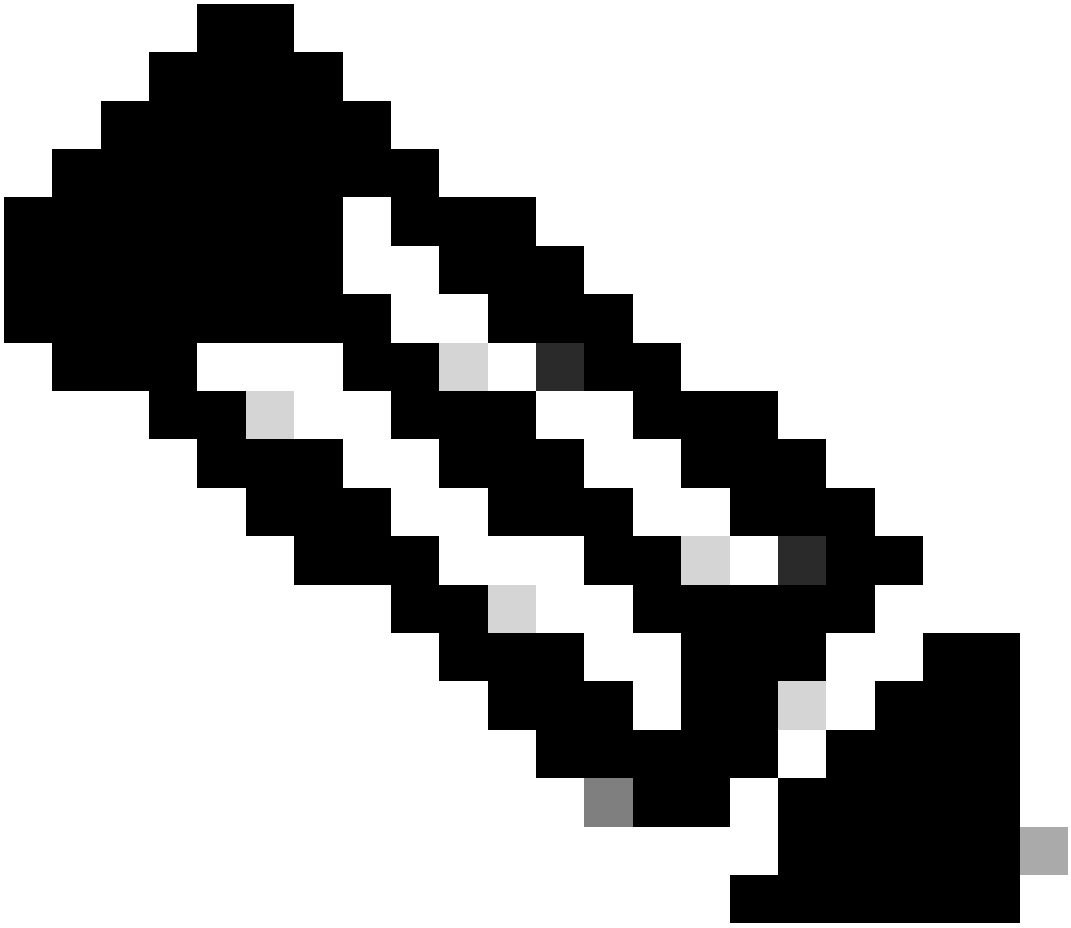


來源防火牆

6. 選擇用於獲取配置的提取方法。
    1. 手動上傳要求**Running Config**您以「.cfg」或「.txt」格式上傳ASA檔案。
    2. 連線到ASA以直接從防火牆提取配置。

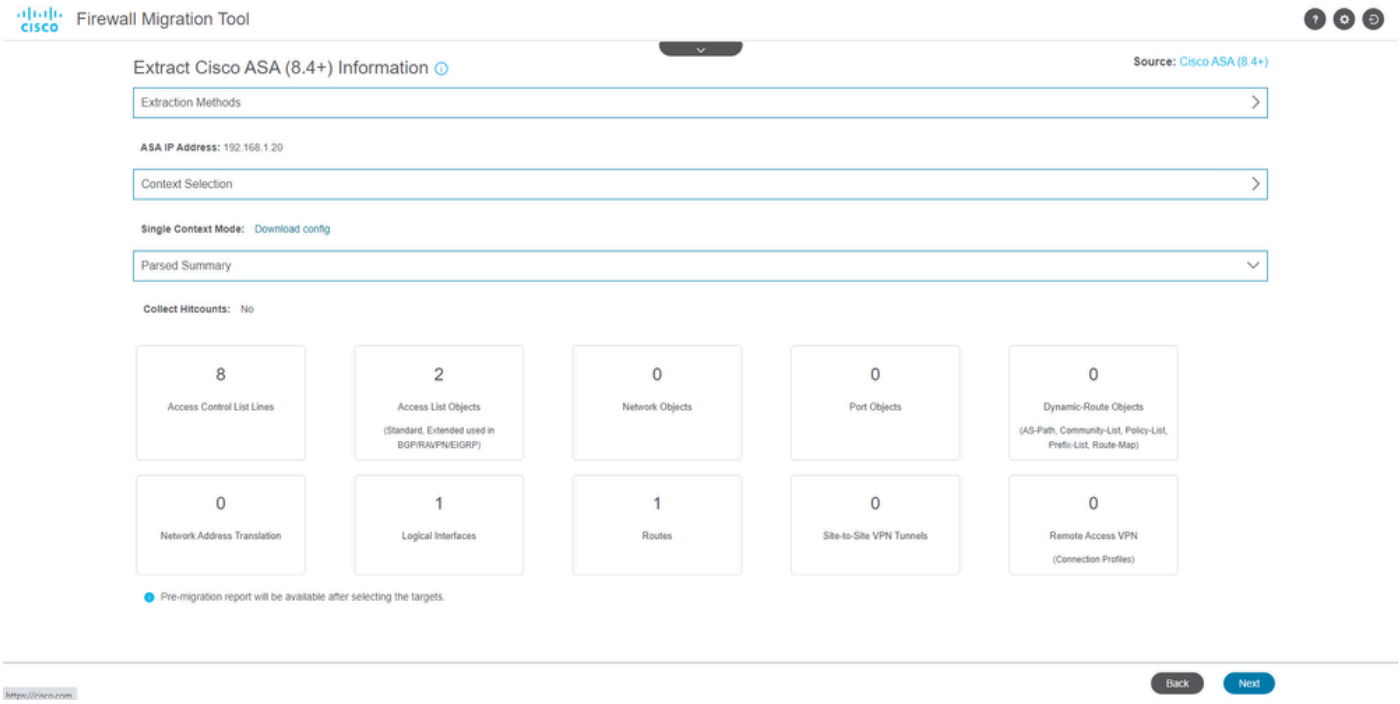


提取



附註：在本示例中，直接連線到ASA。

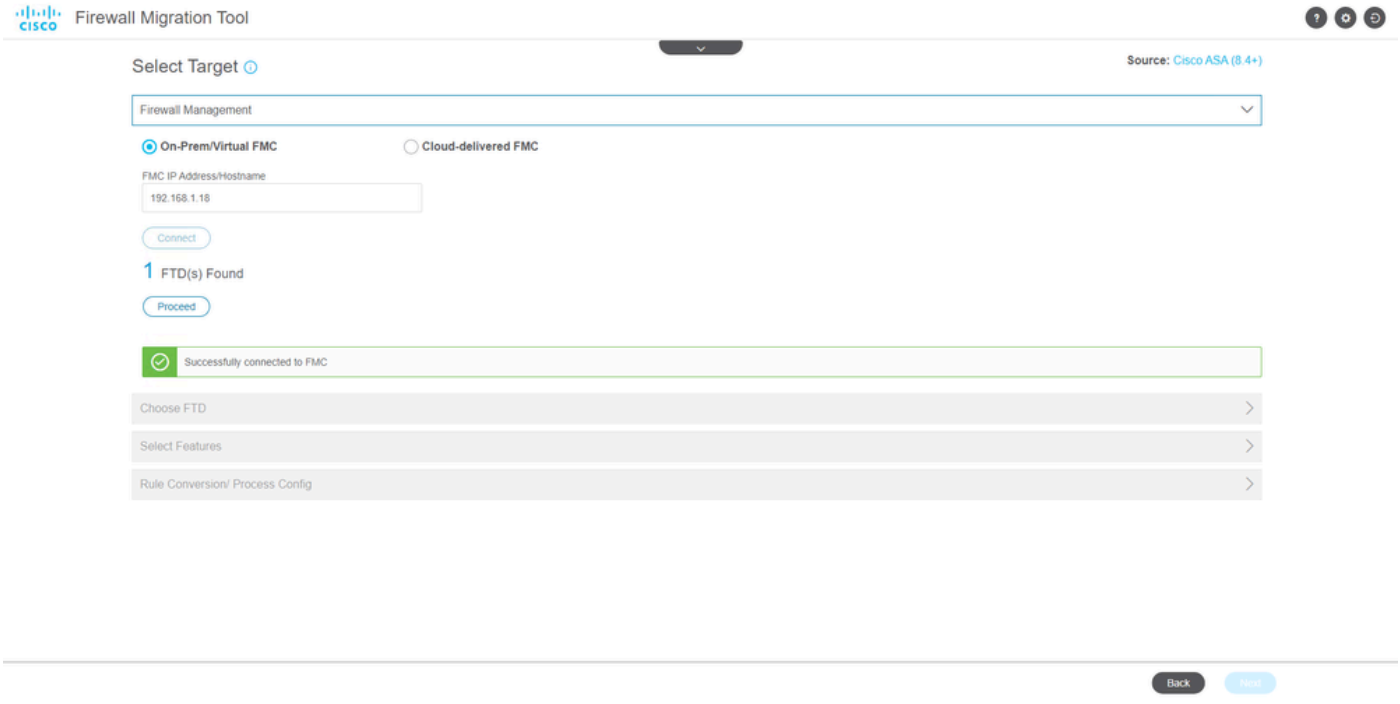
7. 在防火牆上找到的配置摘要顯示為儀表板，請單擊「下一步」。



摘要

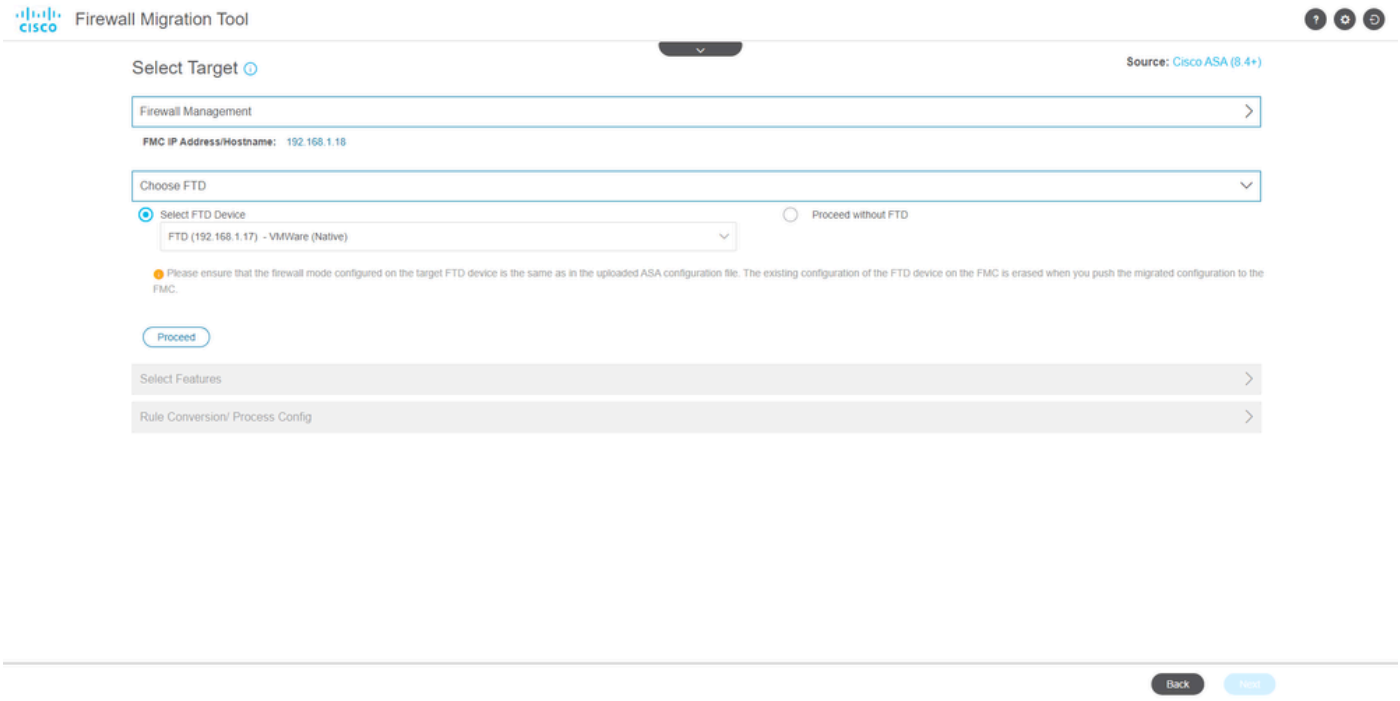
8.選擇要用於遷移的目標FMC。

提供FMC的IP。它會開啟一個彈出視窗，提示您輸入FMC的登入憑證。



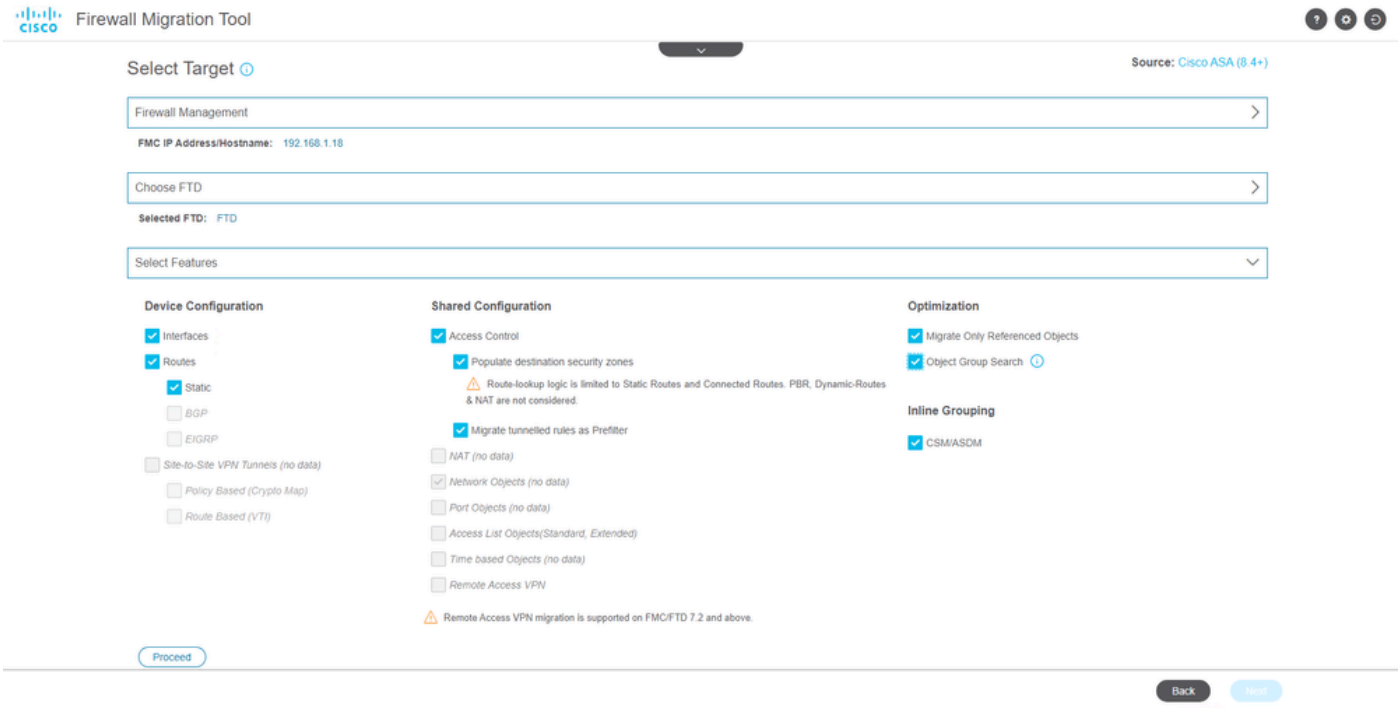
FMC IP

9. （可選）選擇要使用的目標FTD。
    1. 如果您選擇移轉到FTD，請選擇要使用的FTD。
    2. 如果您不想使用FTD，可以填寫此覈取方塊Proceed without FTD



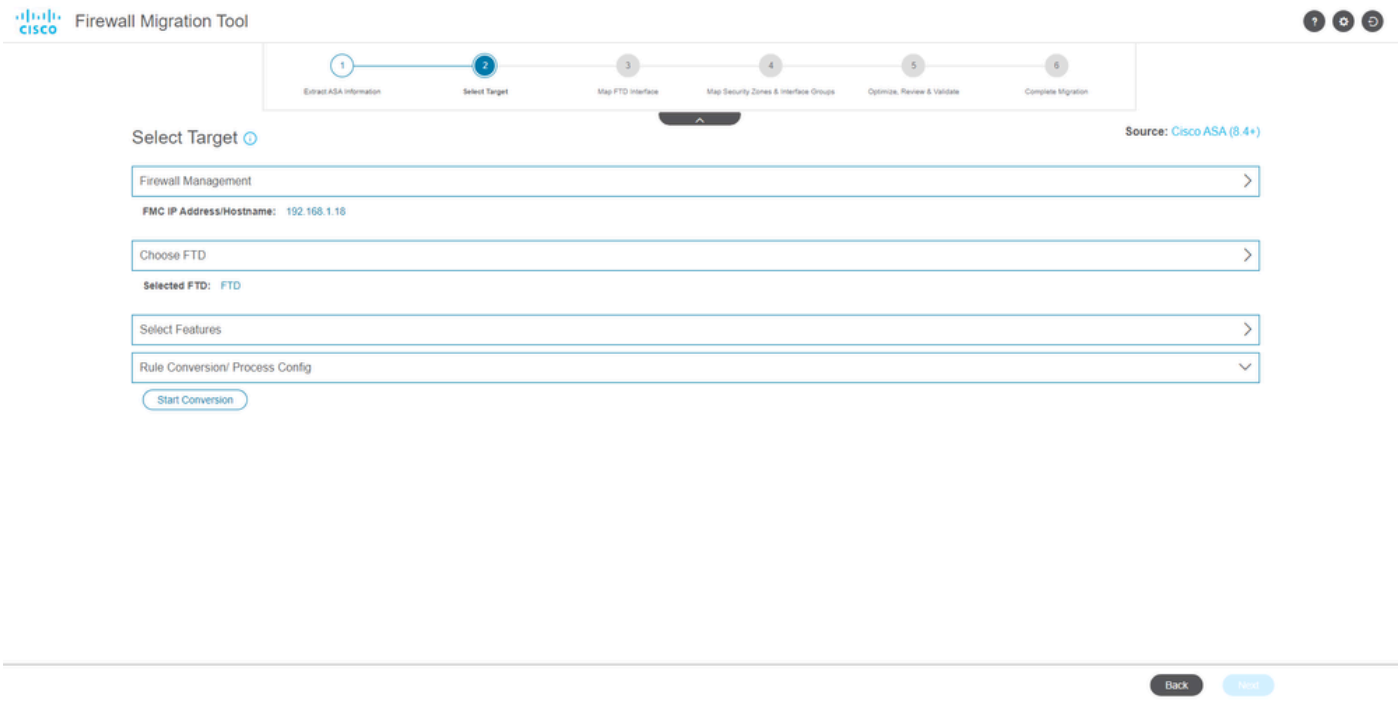
目標FTD

10. 選擇要遷移的配置，螢幕截圖上顯示選項。



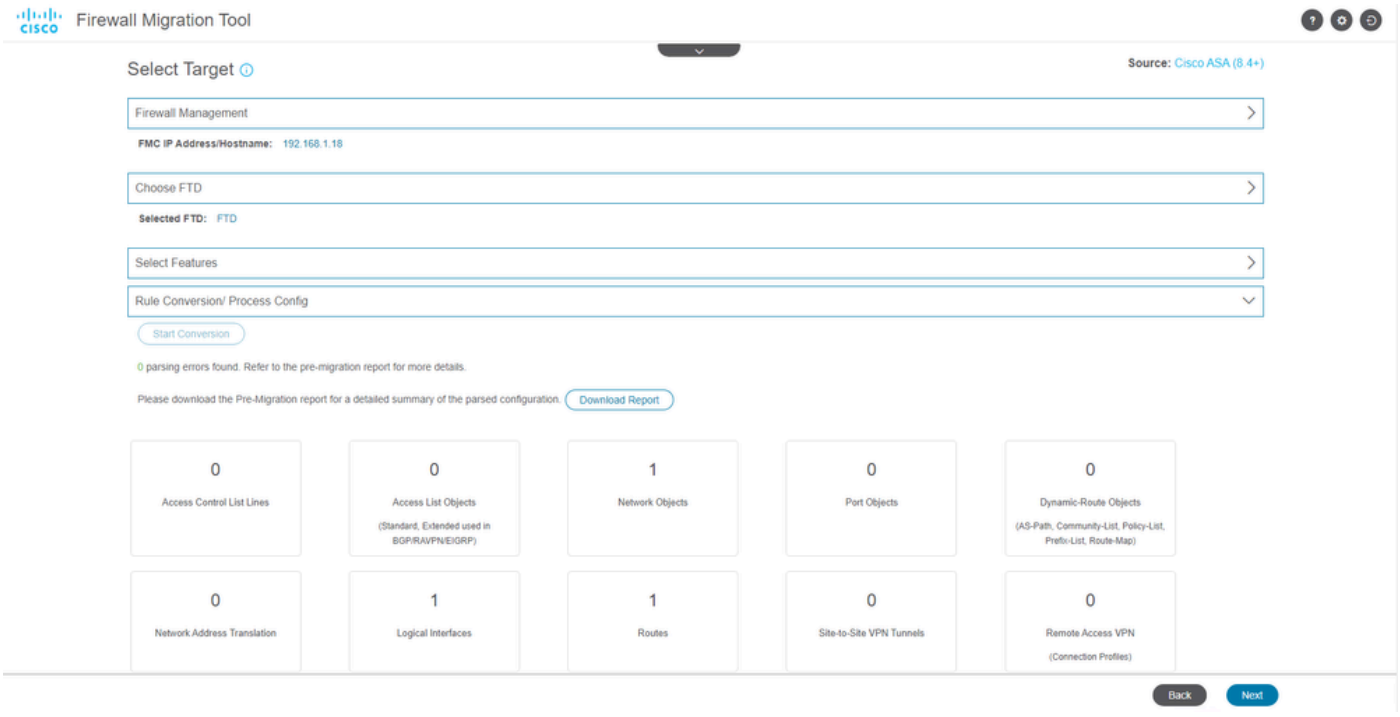
組態

11.開始將配置從ASA轉換為FTD。



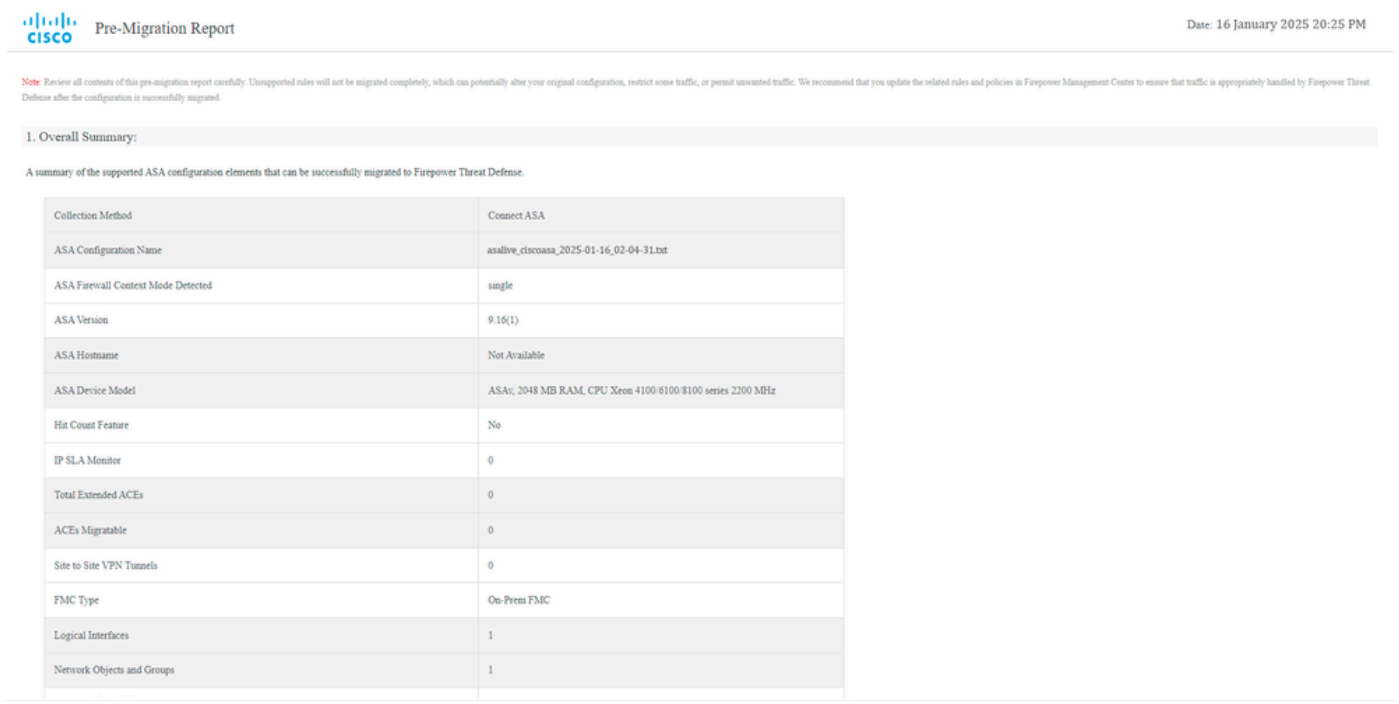
開始轉換

12. 轉換完成後，它會顯示一個儀表板，其中包含要遷移的對象（僅限於相容性）的摘要。
    1. 您也可以單**Download Report**擊接收要遷移的配置摘要。



下載報告

遷移前報告示例，如下圖所示：



Pre-Migration Report

Date: 16 January 2025 20:25 PM

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

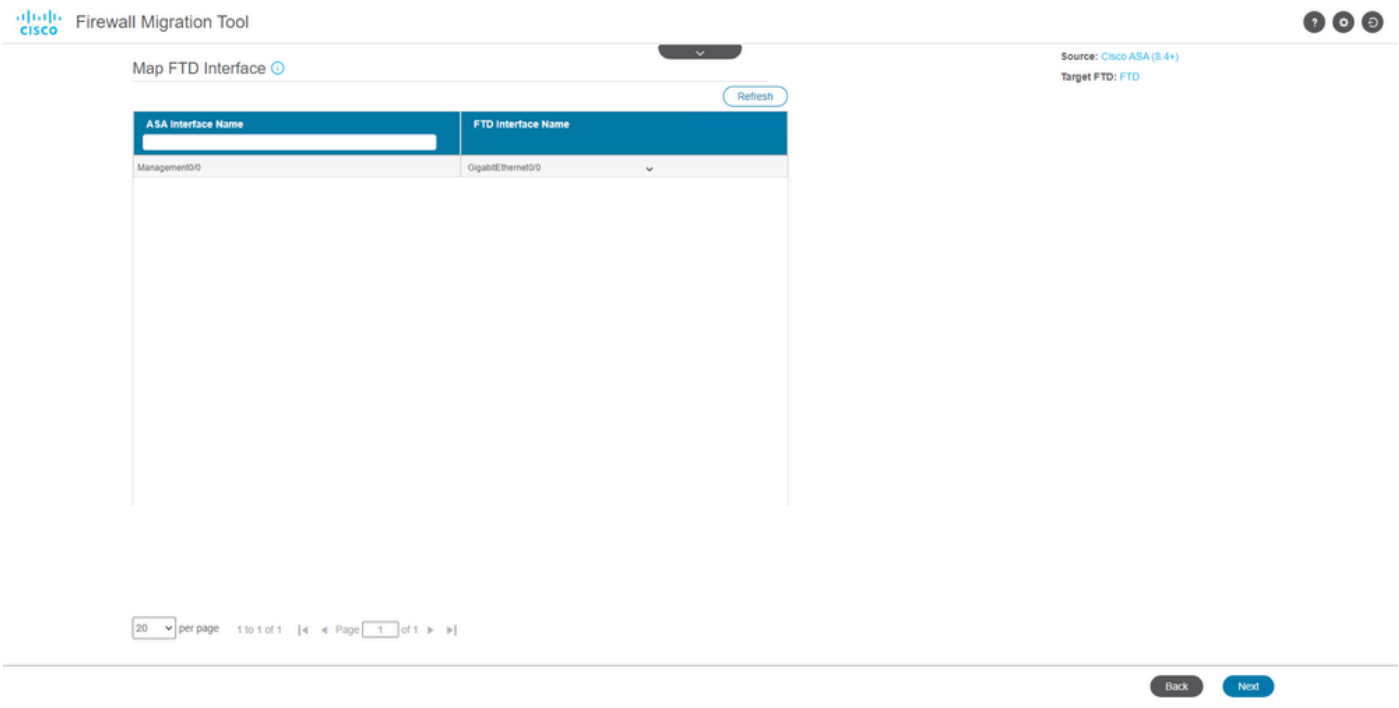
1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2025-01-16_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

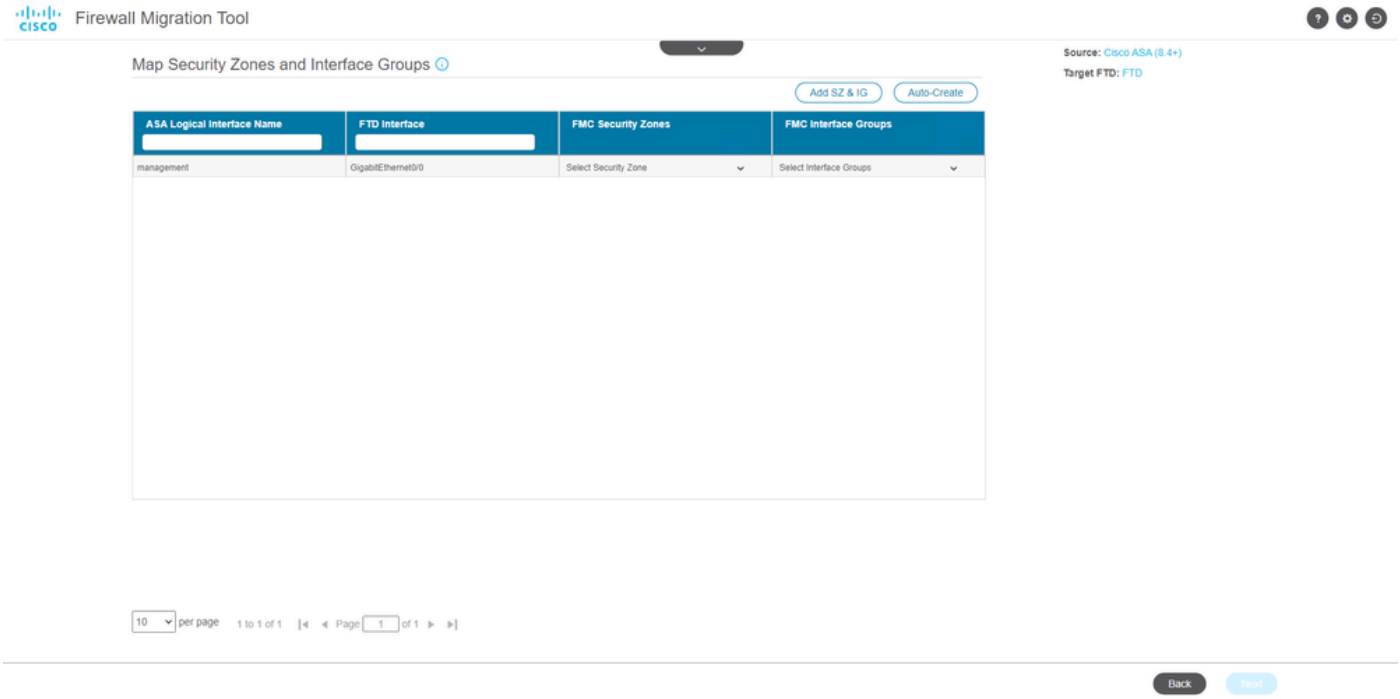
遷移前報告

13.將ASA介面與遷移工具上的FTD介面對映。



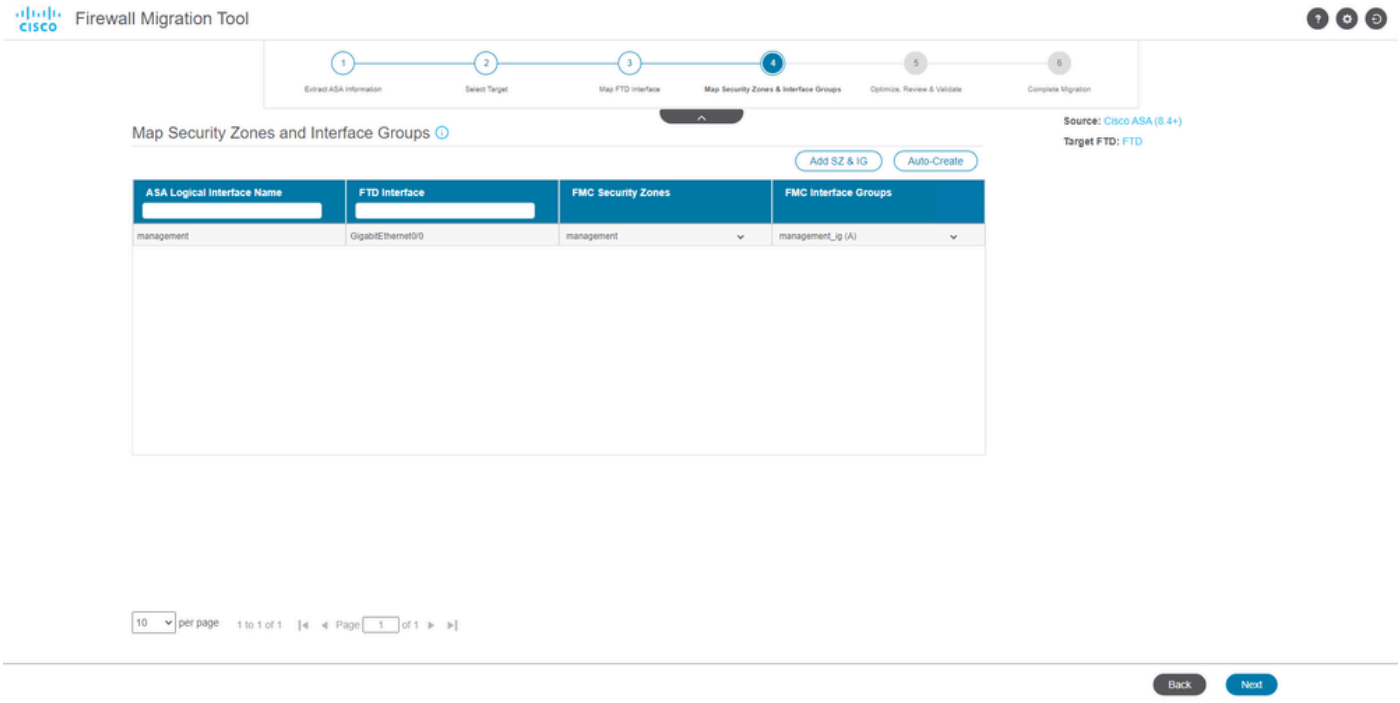
對映介面

14. 為FTD上的介面建立安全區域和介面群組



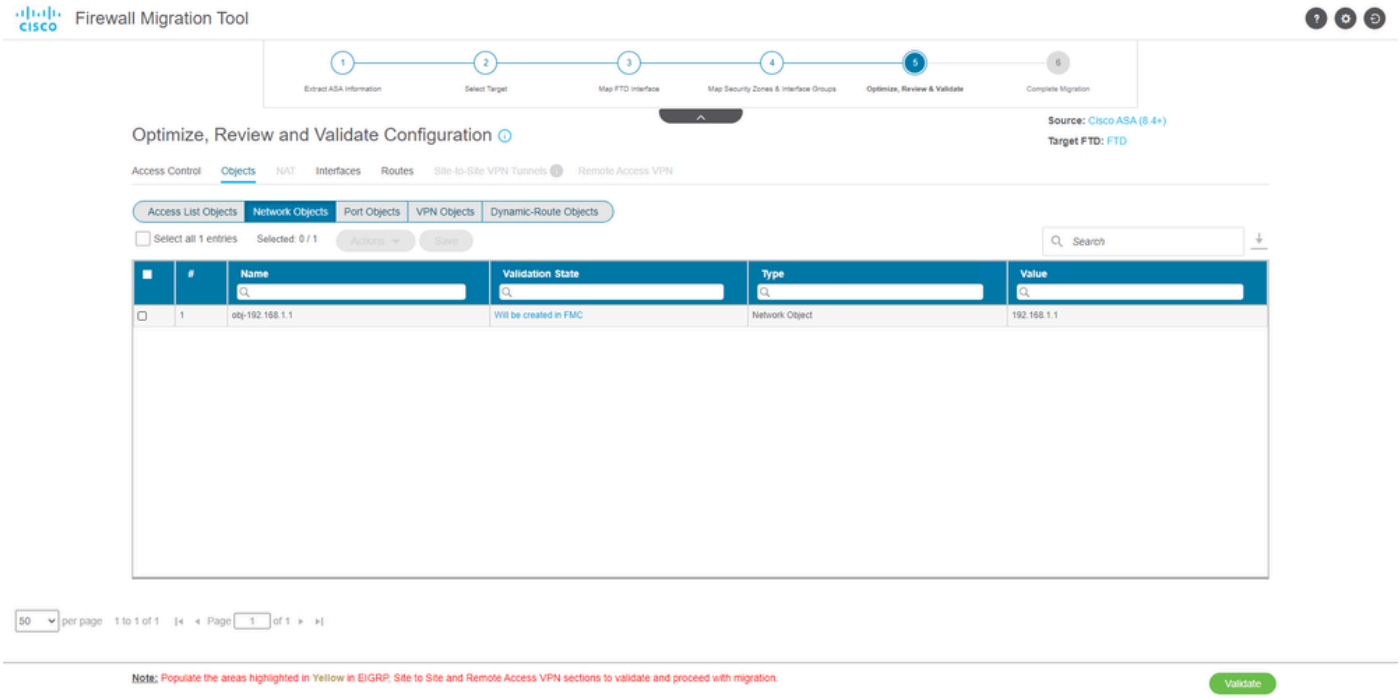
安全區域和介面組

安全區域(SZ)和介面組(IG)由工具自動建立，如下圖所示：



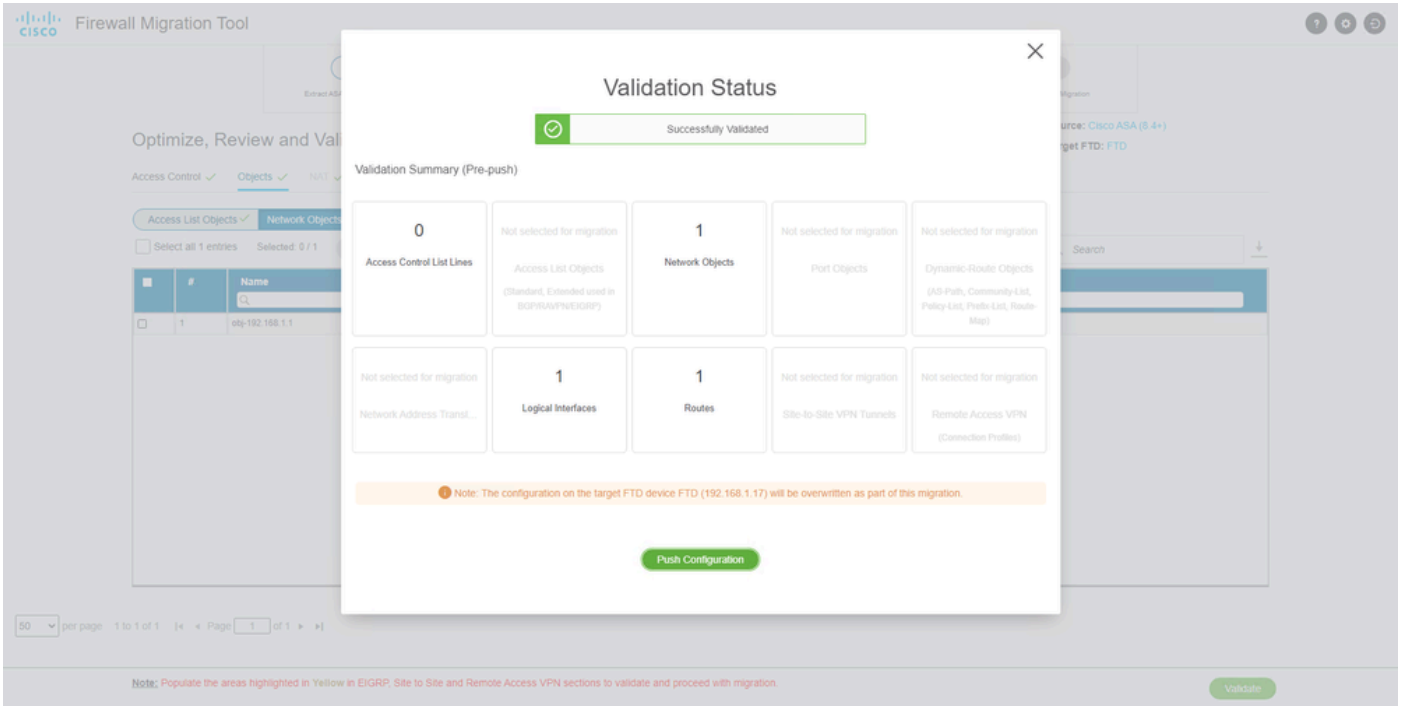
自動建立工具

15. 檢視並驗證要在遷移工具上遷移的配置。
    1. 如果您已完成配置的複查和最佳化，請按一下Validate。



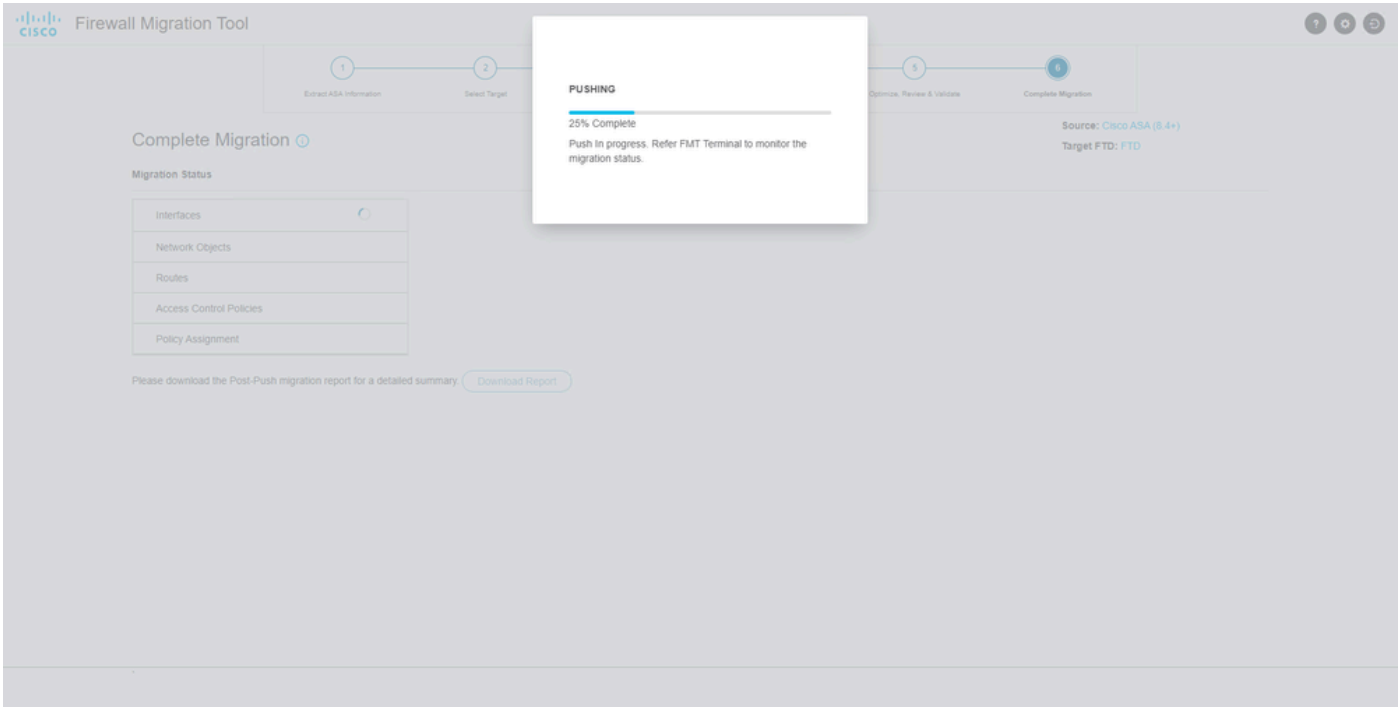
審閱和驗證

16. 如果驗證狀態成功，將配置推送到目標裝置。



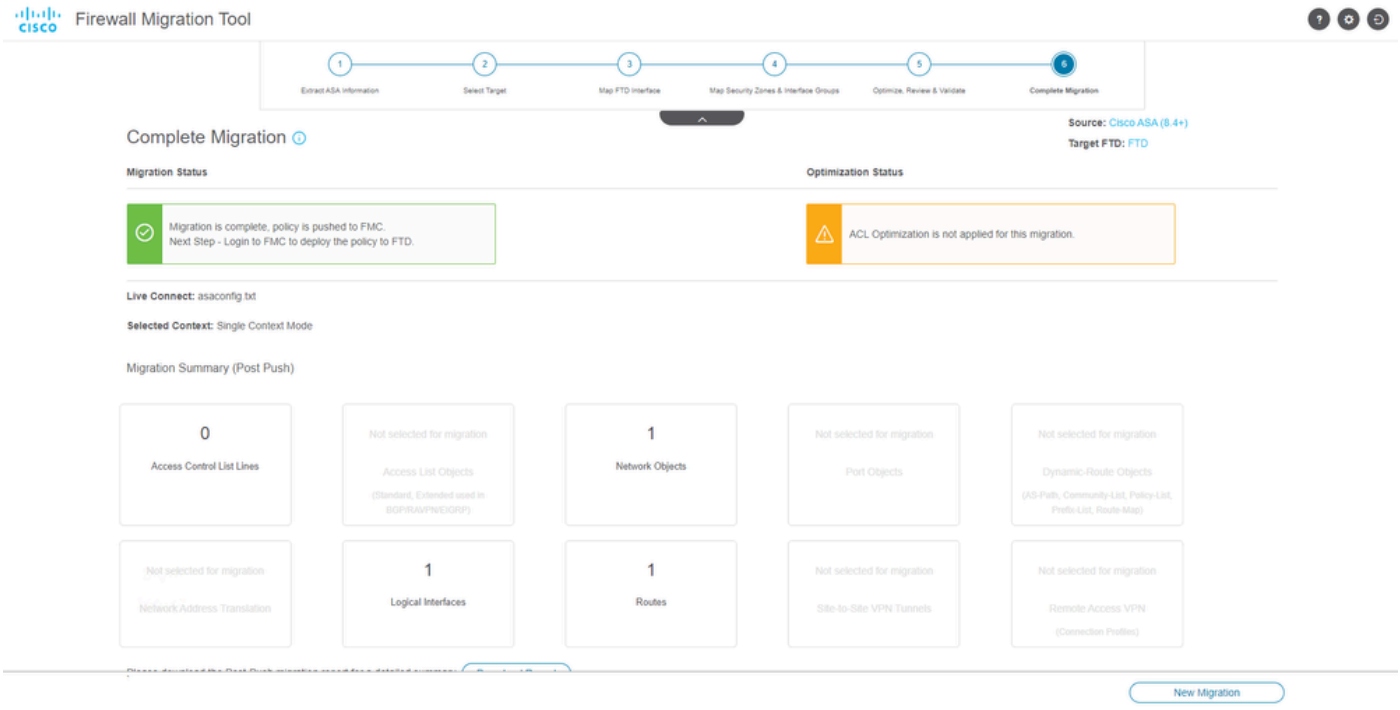
驗證

通過遷移工具推送的配置示例，如下圖所示：



推送

成功遷移的示例，如下圖所示：



成功遷移

（選用）如果選擇將組態移轉到FTD，則需要部署將可用組態從FMC推送到防火牆。

若要部署組態：

1. 登入到FMC GUI。
2. 導航到Deploy頁籤。
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

- 常見遷移失敗:
  - ASA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。
  - ASA配置檔案上傳或將配置推送到管理中心時出現問題。
  - 常見問題包括：
- 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檔案和資料庫檔案。
  - 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。
  - 該工具允許您下載日誌檔案、資料庫和配置檔案的支援捆綁包。
  - 下載步驟：
  - 如需進一步支援：

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）。