

使用FMT將ASA遷移到Firepower威脅防禦(FTD)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[背景資訊](#)

[獲取ASAConfiguration檔案](#)

[從ASA匯出PKI證書並匯入管理中心](#)

[檢索AnyConnect軟體包和配置檔案](#)

[設定](#)

[設定步驟:](#)

[疑難排解](#)

[安全防火牆遷移工具故障排除](#)

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-ss0- 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)。

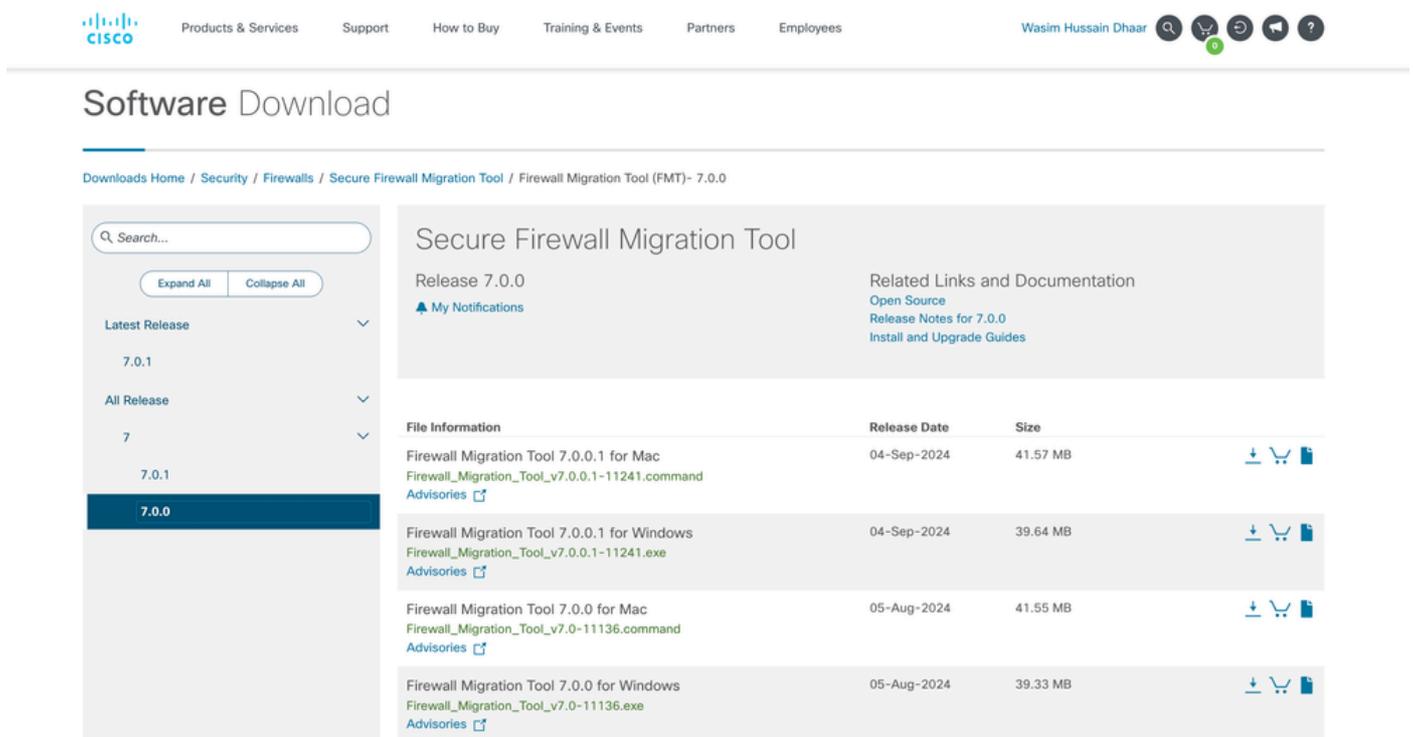
必須從Review and Validate > Remote Access VPN > AnyConnect File一節中的Secure Firewall遷移工具將-Dap.xml和Data.xml上傳到管理中心。

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：

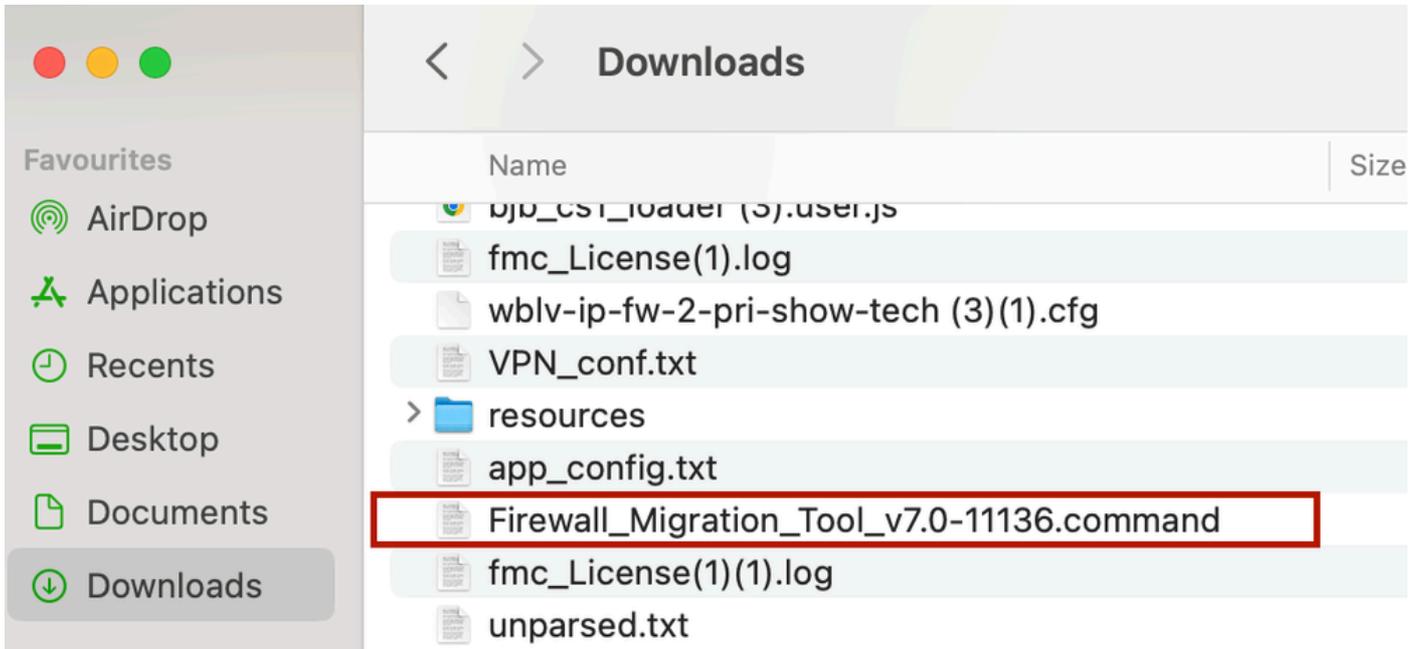


The screenshot shows the Cisco Software Download page for the Secure Firewall Migration Tool (FMT) 7.0.0. The page includes a search bar, navigation tabs (Products & Services, Support, How to Buy, Training & Events, Partners, Employees), and a user profile (Wasim Hussain Dhaar). The main content area displays the tool's release information and a table of download links.

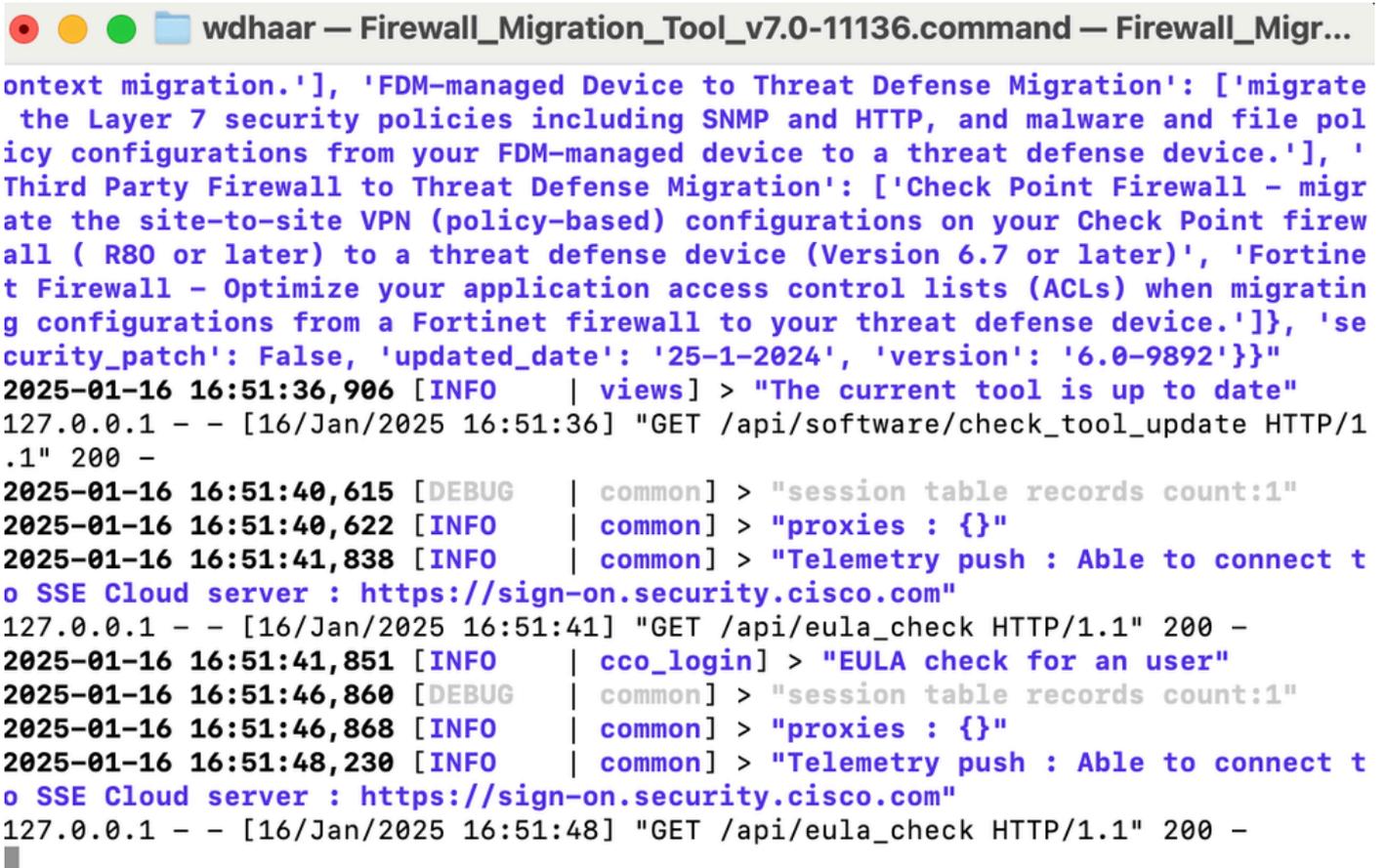
File Information	Release Date	Size	Download
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB	Download Add to Cart Bookmark
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB	Download Add to Cart Bookmark
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB	Download Add to Cart Bookmark
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB	Download Add to Cart Bookmark

軟體下載

2. 按一下您以前下載到您電腦的檔案。



檔案



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」。

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/software/terms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. It makes no warranty, in any applicable law. You are not licensed to Use the

I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD



Extract Source Information

Any additional information explaining this



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。



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

FMT登入

5. 選擇要遷移的源防火牆。



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」。

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

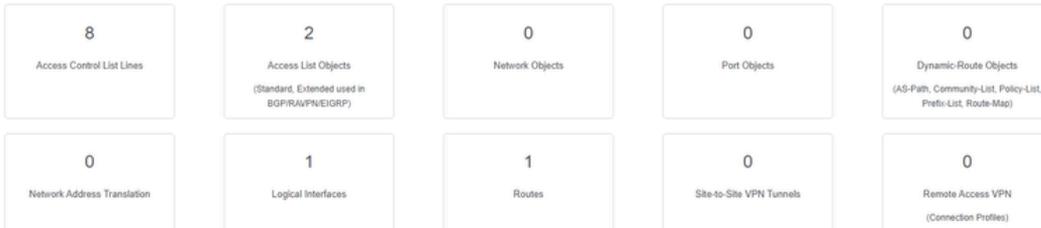
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary ▾

Collect Hitcounts: No



● Pre-migration report will be available after selecting the targets.

https://cisco.com

Back

Next

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。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management ▾

 On-Prem/Virtual FMC

 Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

✔ Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

Back

Next

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

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Select FTD Device

FTD (192.168.1.17) - VMWare (Native)

Proceed without FTD

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features

Rule Conversion/ Process Config

Back

Next

目標FTD

10. 選擇要遷移的配置，螢幕截圖上顯示選項。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Device Configuration

 Interfaces Routes Static BGP EIGRP Site-to-Site VPN Tunnels (no data) Policy Based (Crypto Map) Route Based (VTI)

Shared Configuration

 Access Control Populate destination security zones

Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.

 Migrate tunnelled rules as Prefilter NAT (no data) Network Objects (no data) Port Objects (no data) Access List Objects(Standard, Extended) Time based Objects (no data) Remote Access VPN

Remote Access VPN migration is supported on FMC/FTD 7.2 and above.

Optimization

 Migrate Only Referenced Objects Object Group Search

Inline Grouping

 CSM/ASDM

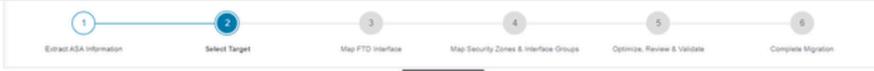
Proceed

Back

Next

組態

11.開始將配置從ASA轉換為FTD。



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

開始轉換

- 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。
- 您也可以單Download Report擊接收要遷移的配置摘要。

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

0	0	1	0	0
Access Control List Lines	Access List Objects (Standard, Extended used in BGPRAVP/NEIGRP)	Network Objects	Port Objects	Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0	1	1	0	0
Network Address Translation	Logical Interfaces	Routes	Site-to-Site VPN Tunnels	Remote Access VPN (Connection Profiles)

Back Next

下載報告

遷移前報告示例，如下圖所示：

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	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 MHz
Hat 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

Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 Page 1 of 1

Back Next

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：



Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

10 per page 1 to 1 of 1 Page 1 of 1

Back Next

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。



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN

Access List Objects **Network Objects** Port Objects VPN Objects Dynamic-Route Objects

Select all 1 entries Selected: 0 / 1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 Page 1 of 1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration.

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。

Validation Status

Successfully Validated

Validation Summary (Pre-push)

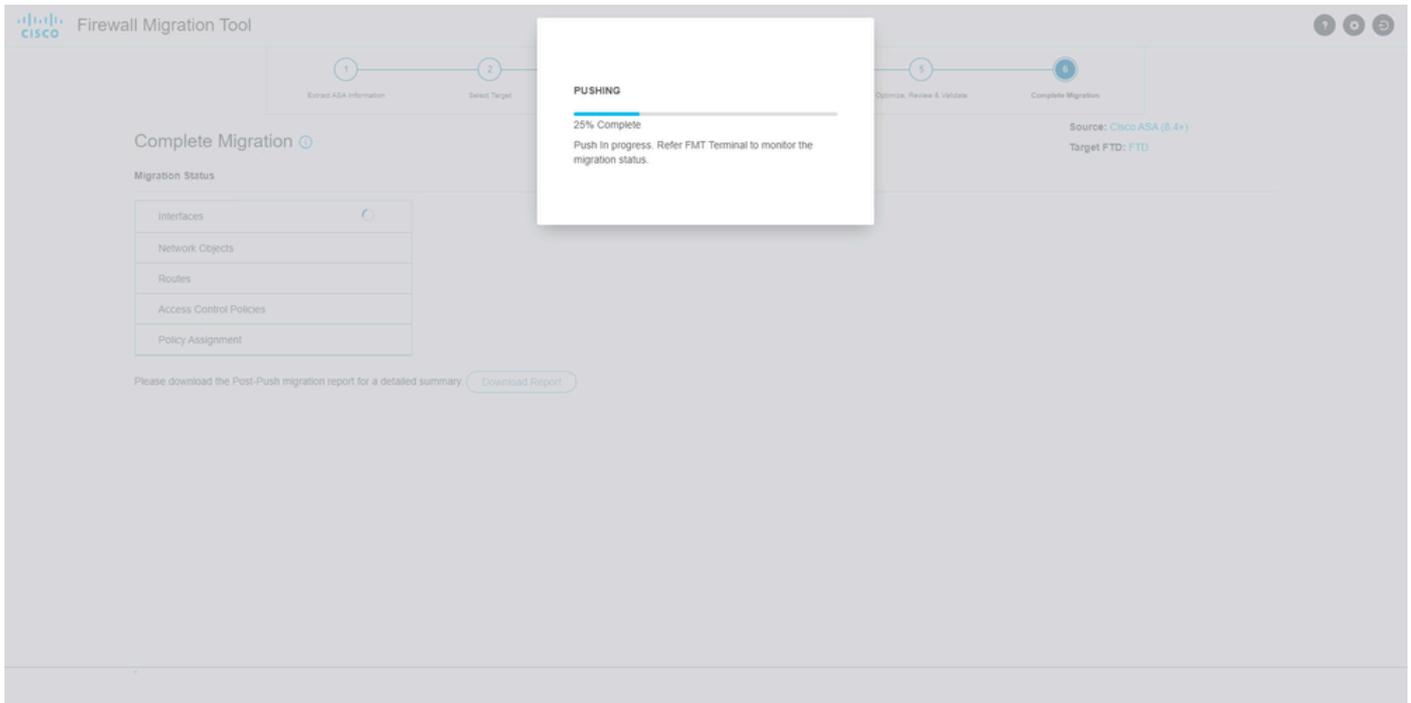
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

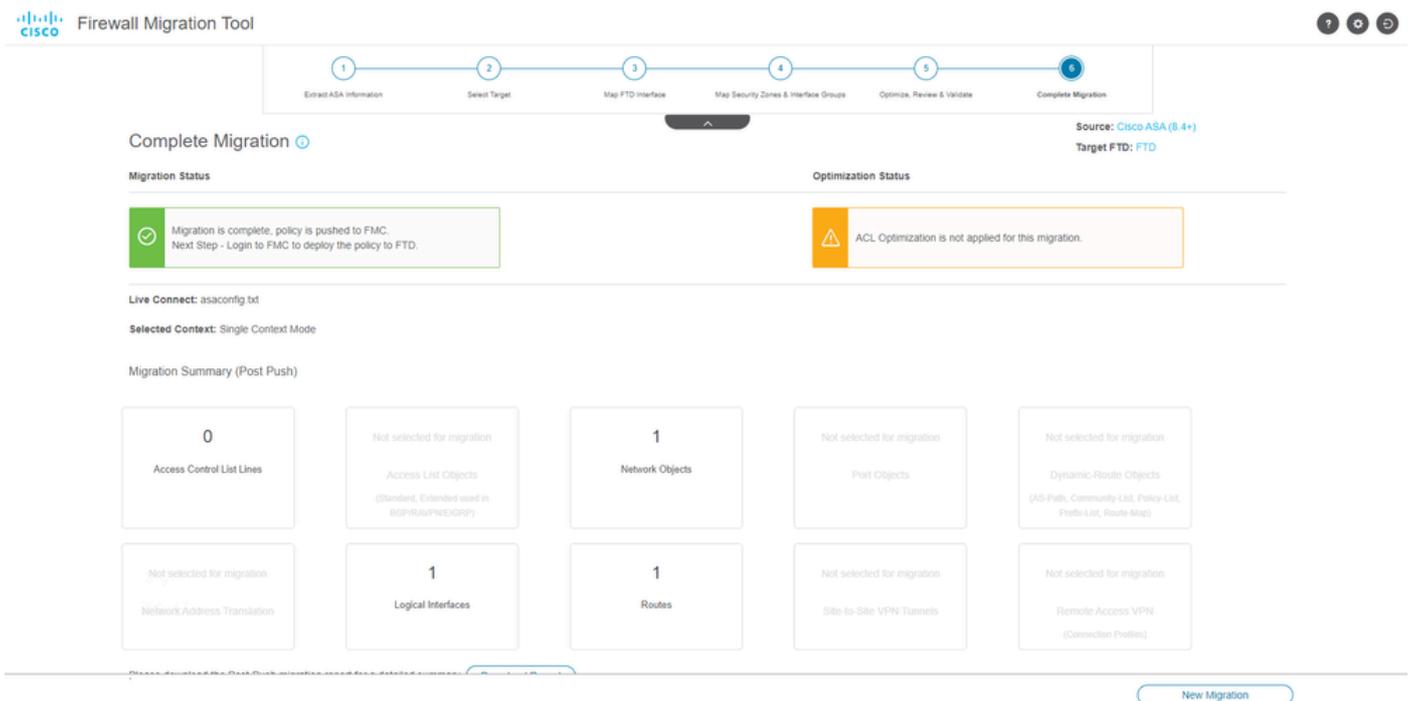
驗證

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）。