

使用FMT將Paloalto遷移到Firepower威脅防禦

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[背景資訊](#)

[獲取Paloalto防火牆配置zip檔案](#)

[遷移前檢查清單](#)

[設定](#)

[遷移步驟](#)

[疑難排解](#)

[安全防火牆遷移工具故障排除](#)

[常見的遷移失敗：](#)

[使用支援捆綁包進行故障排除：](#)

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：

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0

Search...

Expand All Collapse All

Latest Release

7.7.0

All Release

7

Secure Firewall Migration Tool

Release 7.7.0

My Notifications

Related Links and Documentation

Open Source

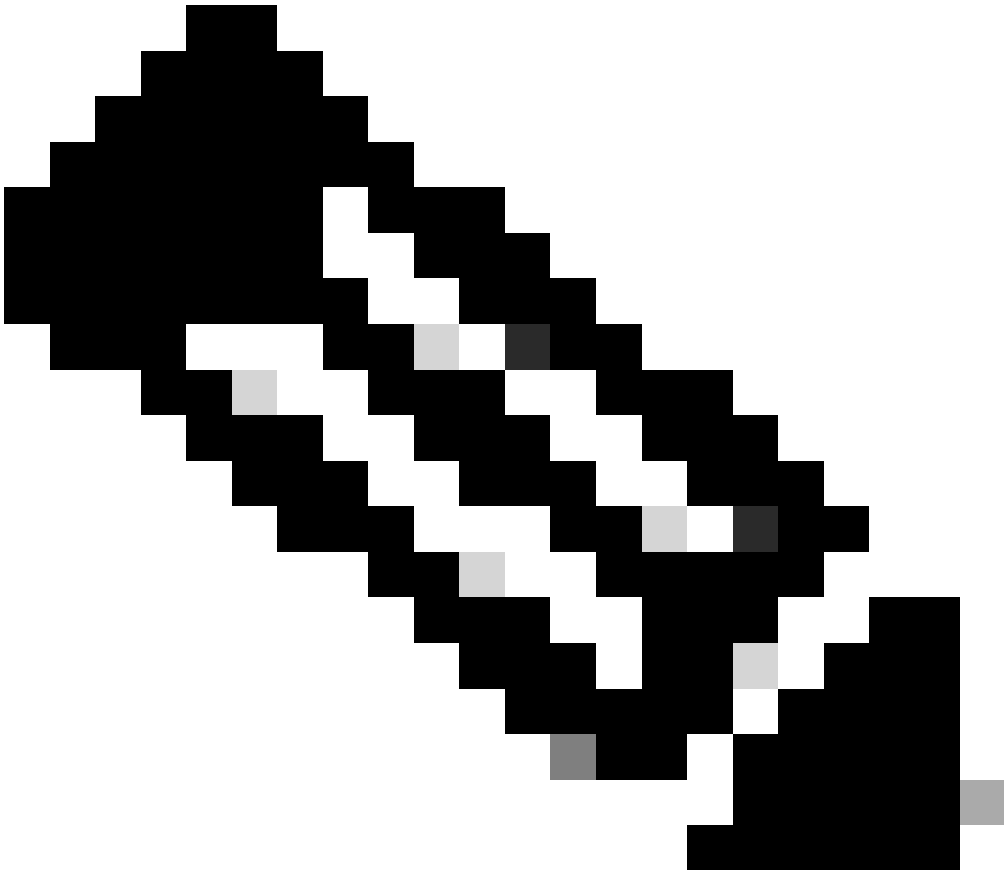
Release Notes for 7.7.0

Install and Upgrade Guides

File Information	Release Date	Size	
Firewall Migration Tool 7.7 for Mac	03-Feb-2025	78.72 MB	Download Add to Cart
Firewall_Migration_Tool_v7.7-12208.command			
Advisories			
Firewall Migration Tool 7.7 for Windows	03-Feb-2025	69.54 MB	Download Add to Cart
Firewall_Migration_Tool_v7.7-12208.exe			
Advisories			

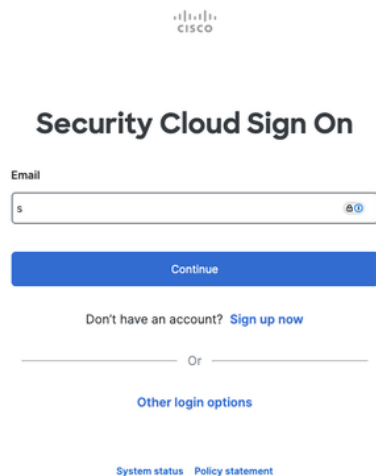
FMT下載

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。

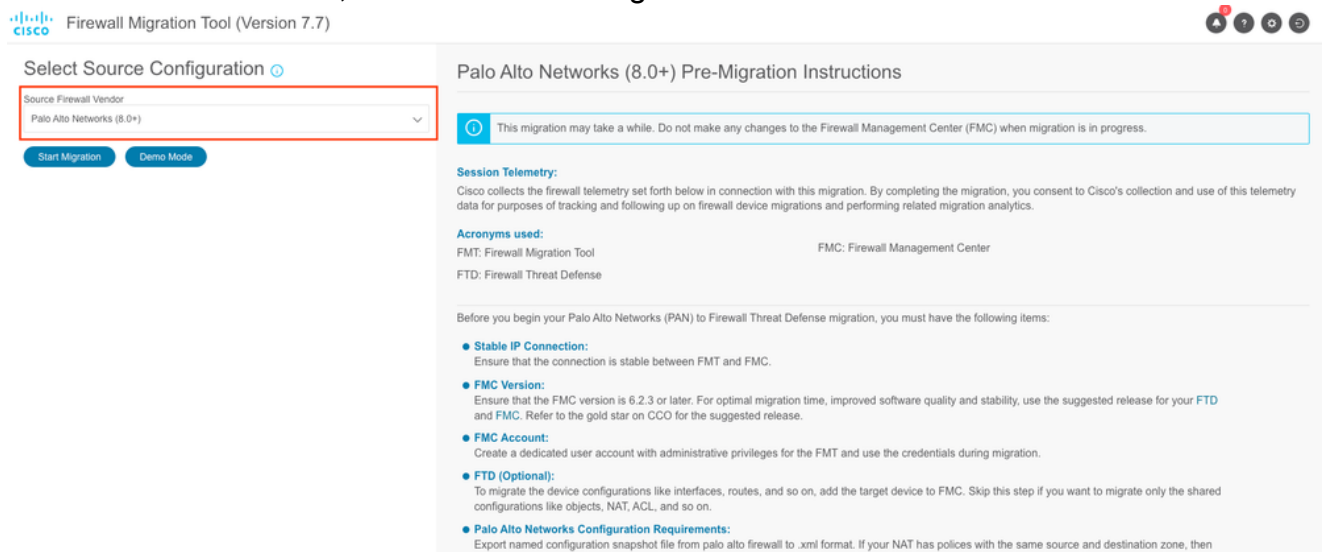
4. 運行該程式後，它會開啟一個顯示終端使用者許可協定的Web瀏覽器。
 1. 選中此覈取方塊以接受條款和條件。
 2. 按一下「繼續」。
5. 使用有效的CCO憑證登入，以存取FMT GUI。



The image shows the Cisco Security Cloud Sign On page. At the top is the Cisco logo. Below it is the title "Security Cloud Sign On". There is an "Email" input field with a dropdown arrow. Below the input field is a blue "Continue" button. Underneath the button is a link: "Don't have an account? Sign up now". Below this is a horizontal line with "Or" in the center. Under the line is the text "Other login options". At the bottom are two links: "System status" and "Policy statement".

FMT登入提示

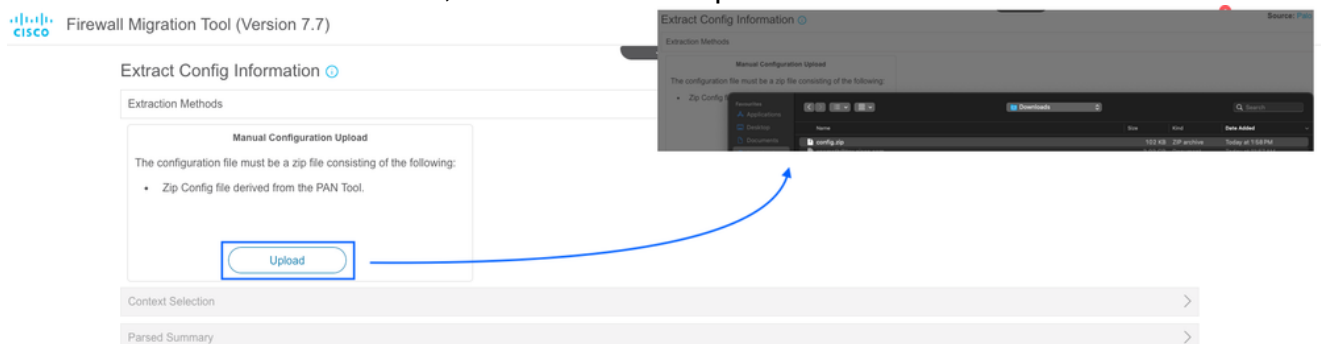
6. 選擇要遷移的源防火牆，然後按一下Start Migration。



The image shows the Firewall Migration Tool (Version 7.7) interface. On the left, under "Select Source Configuration", there is a dropdown menu for "Source Firewall Vendor" with "Palo Alto Networks (8.0+)" selected. Below this are "Start Migration" and "Demo Mode" buttons. On the right, under "Palo Alto Networks (8.0+) Pre-Migration Instructions", there is a warning box: "This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress." Below this is a "Session Telemetry" section, followed by "Acronyms used:" with definitions for FMT, FMC, and FTD. At the bottom, there is a section "Before you begin your Palo Alto Networks (PAN) to Firewall Threat Defense migration, you must have the following items:" with a list of requirements: Stable IP Connection, FMC Version, FMC Account, FTD (Optional), and Palo Alto Networks Configuration Requirements.

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。

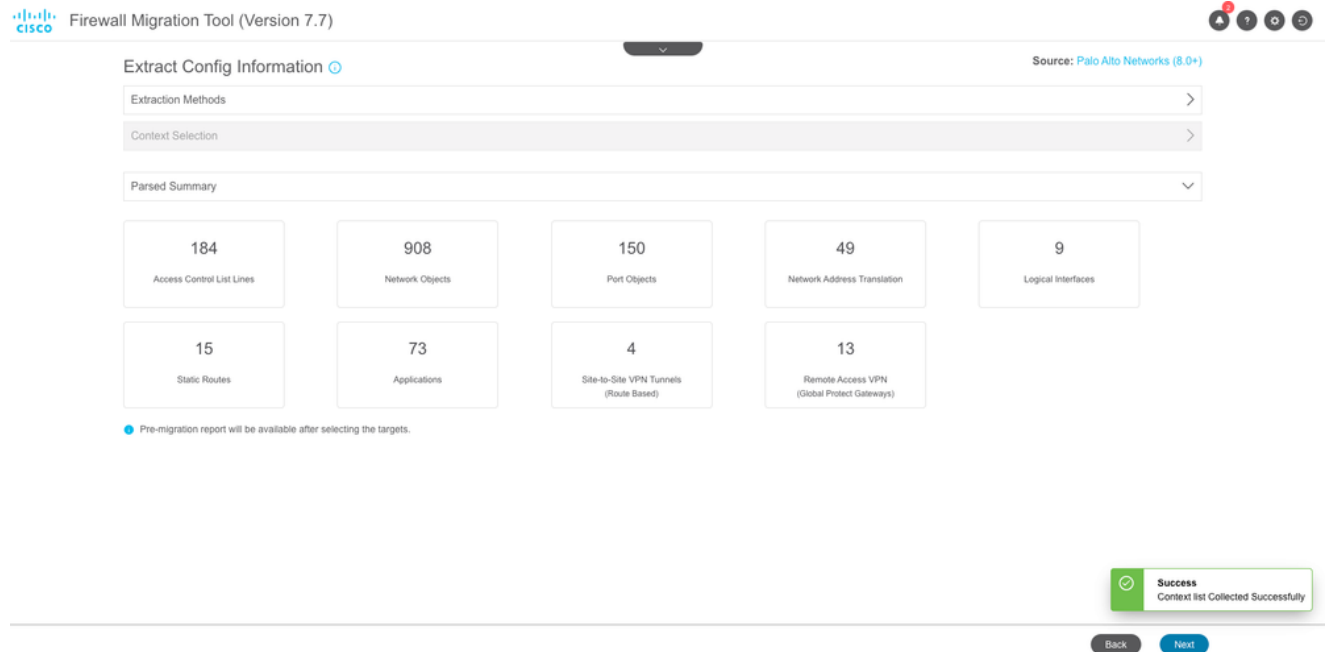


The image shows the Firewall Migration Tool (Version 7.7) "Extract Config Information" screen. It has a tabbed interface with "Extract Config Information" selected. Under "Extraction Methods", there is a "Manual Configuration Upload" section. It states: "The configuration file must be a zip file consisting of the following:" followed by a list item: "Zip Config file derived from the PAN Tool." Below this is an "Upload" button. To the right, there is a screenshot of a file explorer showing a "Downloads" folder with a file named "config.zip". A blue arrow points from the "Upload" button to the "config.zip" file.

配置上載嚮導

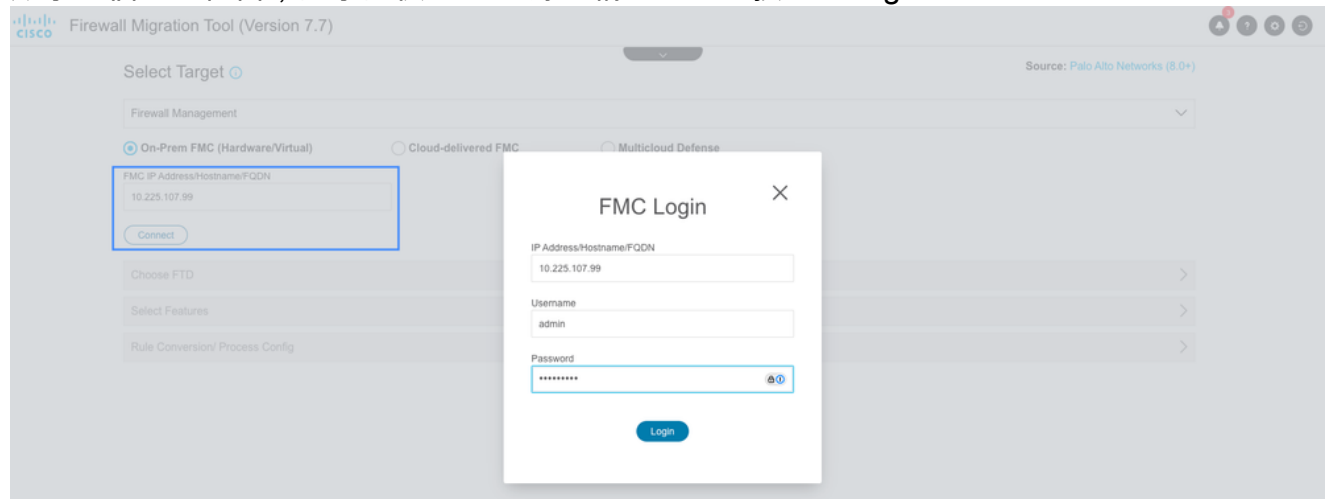
8. 上載配置檔案後，將顯示已分析的配置摘要。對於VSYS，可使用單獨的VSYS選擇。必須逐個分析並遷移它們。

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。

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target ⓘ

Firewall Management

☒ On-Prem FMC (Hardware/Virtual) ☐ Cloud-delivered FMC ☐ Multicloud Defense

FMC IP Address/Hostname/FQDN: 10.225.107.99

Choose Domain: Global/Cisco

Connect

Proceed

Successfully connected to FMC

域選擇

11. 選擇要遷移到的FTD，然後按一下Proceed。

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target ⓘ

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

☒ Select FTD Device ☐ Proceed without FTD

FW1 (10.105.209.80) - NA (R)

Proceed

Select Features

Rule Conversion/ Process Config

選擇目標FTD

12. 該工具現在列出了要遷移的功能。按一下「Proceed」。

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target ⓘ

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

Selected FTD: FW1

Select Features

Device Configuration

- ☒ Interfaces
- ☒ Routes
- ☒ Site-to-Site VPN Tunnels
- ☐ Policy Based (Unsupported) ⓘ
- ☒ Route Based (VTI)

Shared Configuration

- ☒ Access Control
- ☐ Migrate policies with Application-default as Enabled ⓘ
- ☒ Network Objects
- ☒ Port Objects
- ☒ Remote Access VPN

Advanced Configuration

Optimization

- ☒ Migrate Only Referenced Objects

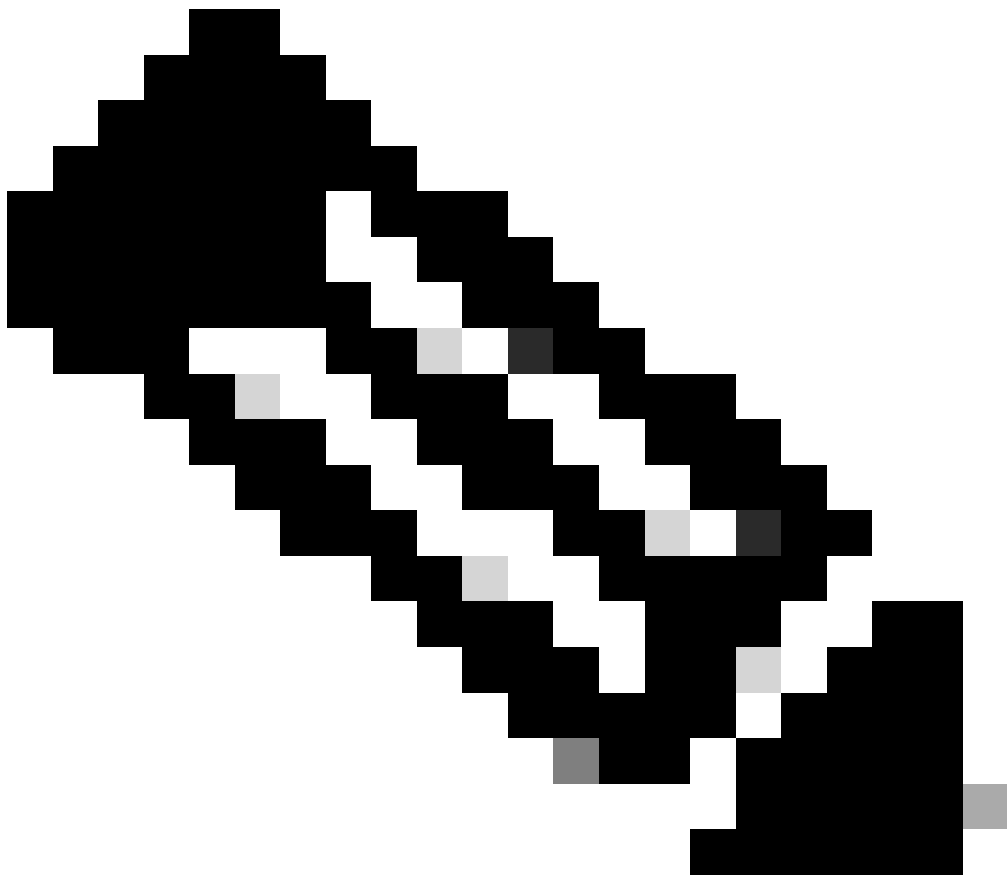
Access Control Options

- ☒ Discovered Identities ⓘ

Proceed

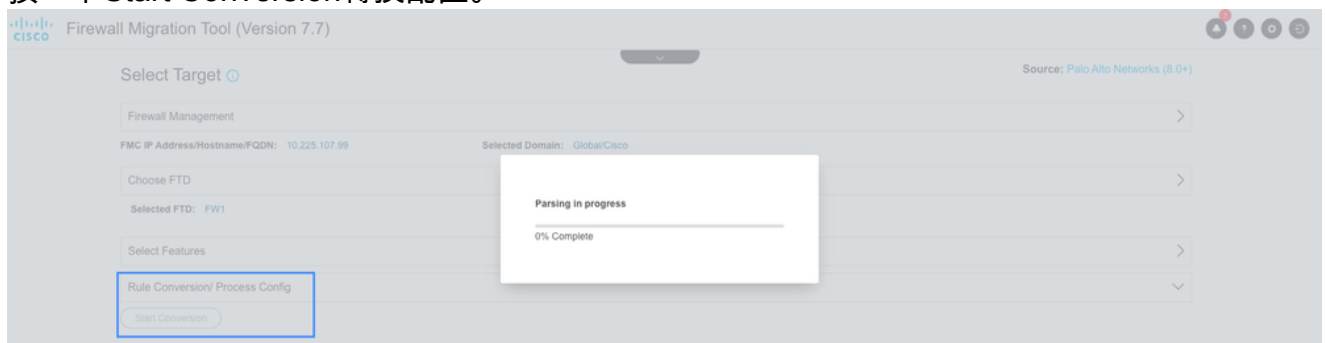
Rule Conversion/ Process Config

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。

Select Target Source: Palo Alto Networks (8.0+)

Firewall Management >

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD >

Selected FTD: FW1

Select Features >

Rule Conversion/ Process Config ▾

[Start Conversion](#)

No parsing error 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](#)

For pre-migration report

Parsed configuration summary

195 Access Control List Lines	752 Network Objects	98 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	70 Applications	9 Remote Access VPN (Global Protect Gateways)	

[Back](#) [Next](#)

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。

Map FTD Interface Source: Palo Alto Networks (8.0+)
Target FTD: FW1

PAN Interface Name	FTD Interface Name	Mapped Name
ethernet1/2	Select Interface	ethernet1_2
ethernet1/3	ethernet1/10	ethernet1_3
ethernet1/4	ethernet1/11	ethernet1_4
ethernet1/5	ethernet1/12	ethernet1_5
ethernet1/6	ethernet1/13	ethernet1_6
ethernet1/7	ethernet1/14	ethernet1_7
	ethernet1/15	
	ethernet1/16	
	ethernet1/17	
	ethernet1/18	
	ethernet1/19	

FTD Interface name can be edited

Mapping of FTD interfaces

10 per page 1 to 6 of 6 Page 1 of 1

[Back](#) [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。

Map Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

PAN Zone Name	FMC Security Zones
G-Inside	Select Security Zone
Outside	Select Security Zone
GP-VPN-	Select Security Zone
I-Inside	Select Security Zone
DMZ	Select Security Zone
SC	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
I-Inside	Select Security Zone

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be grayed out.

10 per page 1 to 10 of 12 |< Page 1 of 2 >|

Back

Next

安全區域建立

手動建立安全區域：

on Tool (Version 7.7)

Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Add SZ

Security Zones (SZ)

Add Max 48 characters for zone name. Allowed special characters are _-+*

Security Zones	Type	Actions
DMZ	Select	
	SWITCHED	
	ROUTED	

0 - 0 of 0 |< 1 >|

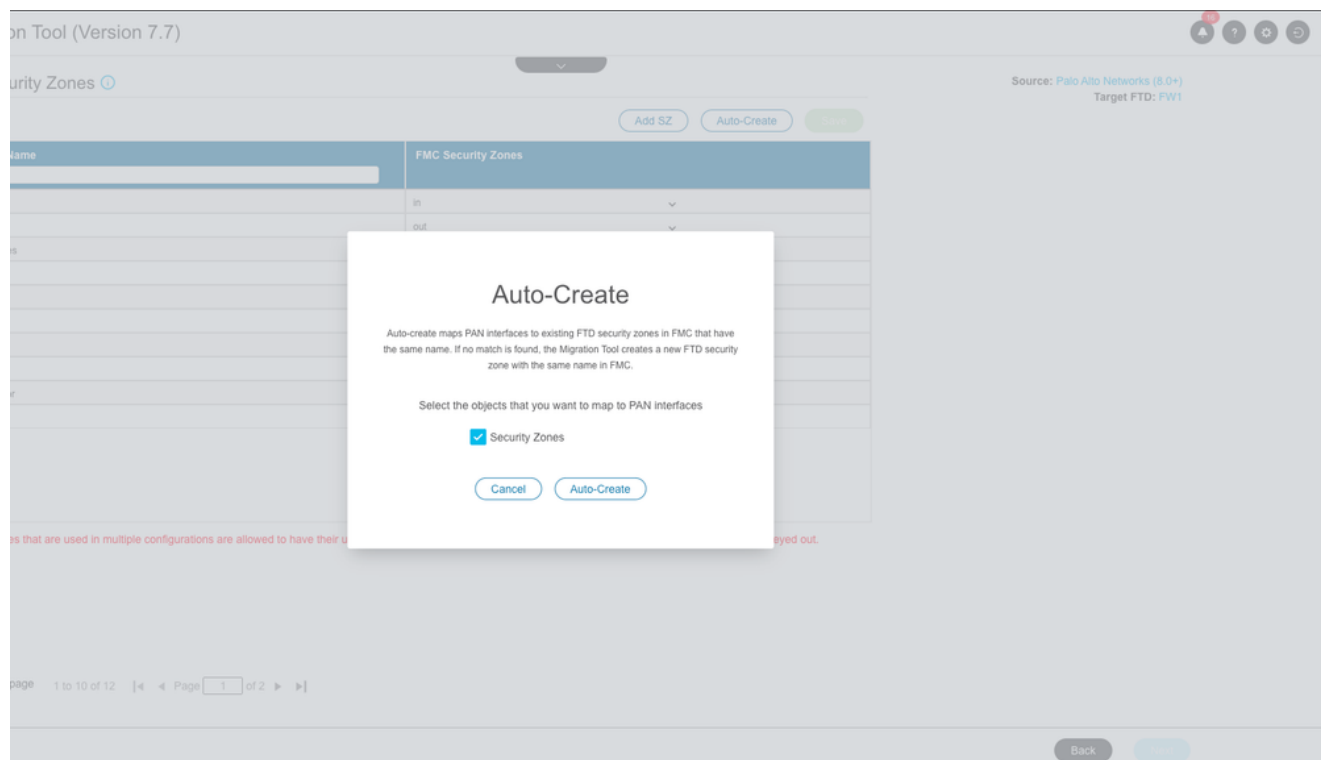
Close

page 1 to 10 of 12 |< Page 1 of 2 >|

Back

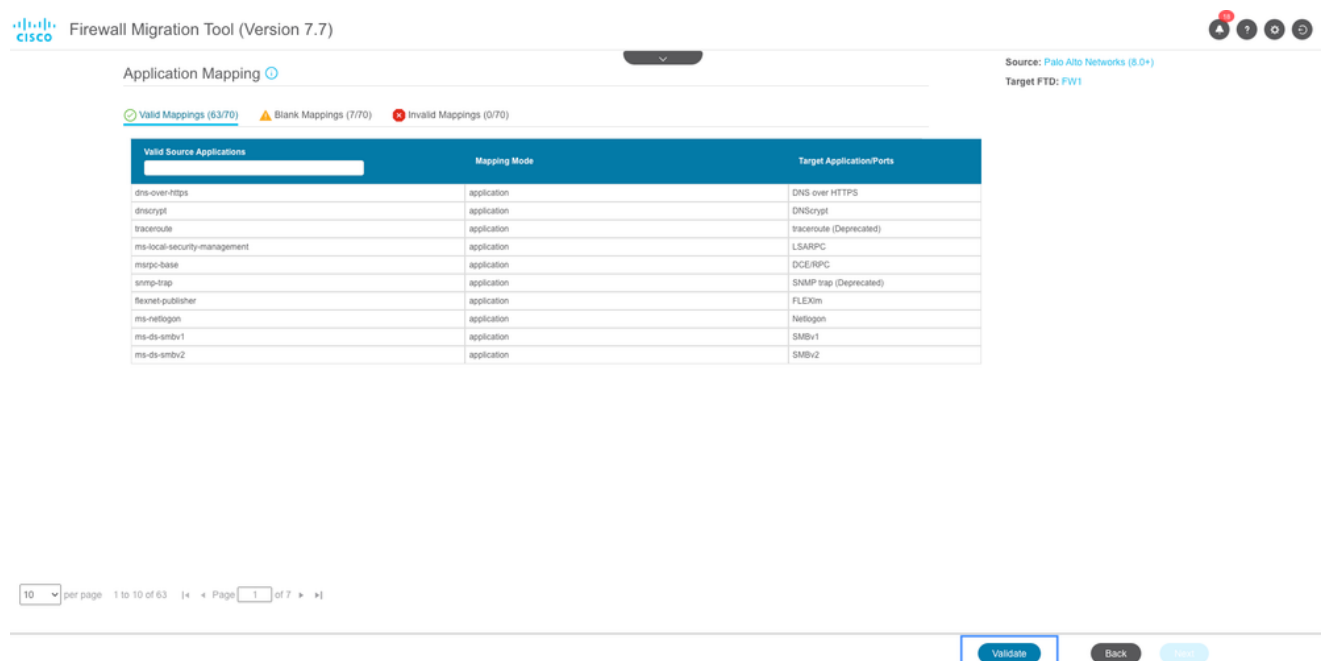
手動建立安全區域

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

Firewall Migration Tool (Version 7.7)

Application Mapping

Validation of application mapping is in progress. Please wait

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Valid Mappings (63/70)

Blank Mappings (7/70)

Invalid Mappings (0/70)

Valid Source Applications	Mapping Mode	Target Application/Ports
dns-over-https	application	DNS over HTTPS
dnscrypt	application	DNScrypt
traceroute	application	traceroute (Deprecated)
ms-local-security-management	application	LSARPC
mrpc-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXlm
ms-netlogon	application	Netlogon
ms-ds-smbv1	application	SMBv1
ms-ds-smbv2	application	SMBv2

10

per page1 to 10 of 63

< >

Page 1 of 7

< >

Validate

Back

Next

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。

Firewall Migration Tool (Version 7.7)

Application Mapping

Clear Mapped Data

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Valid Mappings (61/70)

Blank Mappings (7/70)

Invalid Mappings (2/70)

Invalid Source Applications	Mapping Mode	Target Application/Ports
traceroute	Application	netmp-traceroute
snmp-trap	Port(s)	udp/162

10

per page1 to 2 of 2

< >

Page 1 of 1

< >

Validate

Back

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。

Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

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

Select all 195 entries Selected: 0 / 195

Verify configuration in each section

1

Allow Tm...

Dt

GRP_ADDR...

ANY

ANY

ANY

NTP

NA

✓

Allow

None

2

Allow Tm...

Dt

ANY

ANY

ANY

ANY

NTP

NA

✓

Allow

None

3

Allow Tm...

Dt

GRP_ADDR...

ANY

ANY

ANY

NTP

NA

✓

Allow

None

4

Allow DNS

Dt

ANY

ANY

ANY

ANY

DNS, DNSCrypt, DN...

NA

✓

Allow

None

5

Allow DNS

Ot

ANY

ANY

ANY

Inside

ANY

DNS

NA

✓

Allow

None

6

Allow API

Dt

ANY

ANY

ANY

ANY

TCP-80, TCP...

NA

✓

Allow

None

7

Allow traffi

G...

ADDR_10.11...

ANY

ANY

2.16...

TCP-443

ANY

NA

✓

Allow

None

8

Allow Acco

G...

ADDR_192.16...

ANY

ANY

DT...

ANY

ANY

NA

✓

Allow

None

9

Allow ICM

Ot

ANY

ANY

ANY

Inside

ANY

netmg-traceroute

NA

✓

Allow

None

10

Allow ICM

Ot

ANY

ANY

ANY

Inside

ANY

ICMPv4

NA

✓

Allow

None

11

Allow DHCP

Ot

ANY

ANY

ANY

Inside

.11...

DHCP

ANY

✓

Allow

None

12

Allow NetB

Ot

ANY

ANY

ANY

Inside

.11...

NetBIOS-ns, NetBIO...

ANY

✓

Allow

None

13

Allow DNS

Ot

ANY

ANY

ANY

Inside

.11...

DNS

ANY

✓

Allow

None

50 per page 1 to 50 of 195 Page 1 of 4

Optimise access control list and validate

Optimize ACL 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。

Optimize, Review and Validate Configuration

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

Select all 195 entries Selected: 0 / 195

Validation Status

Successfully Validated

Validation Summary (Pre-push)

195 Access Control List Lines	752 Network Objects	100 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	62 Applications	9 Remote Access VPN (Global Protect Gateways)	

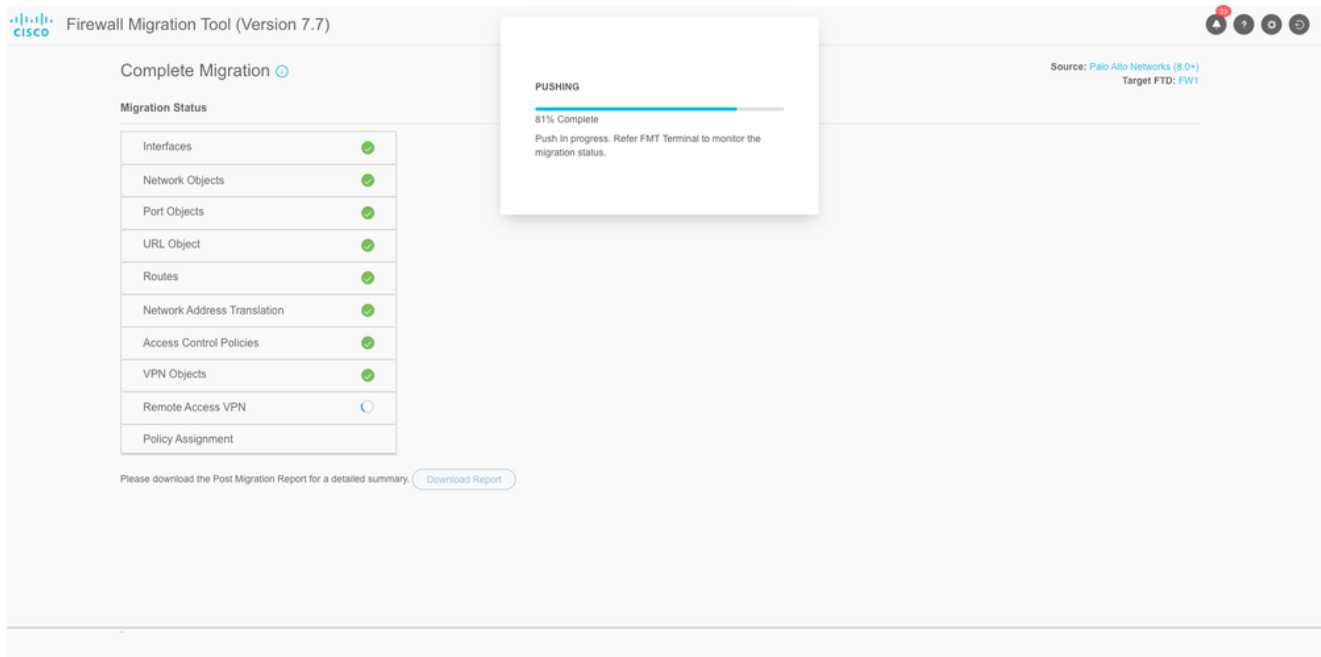
Note: The configuration on the target FTD device FW1 (10.105.209.80) will be overwritten as part of this migration.

Push Configuration

Optimize ACL Validate

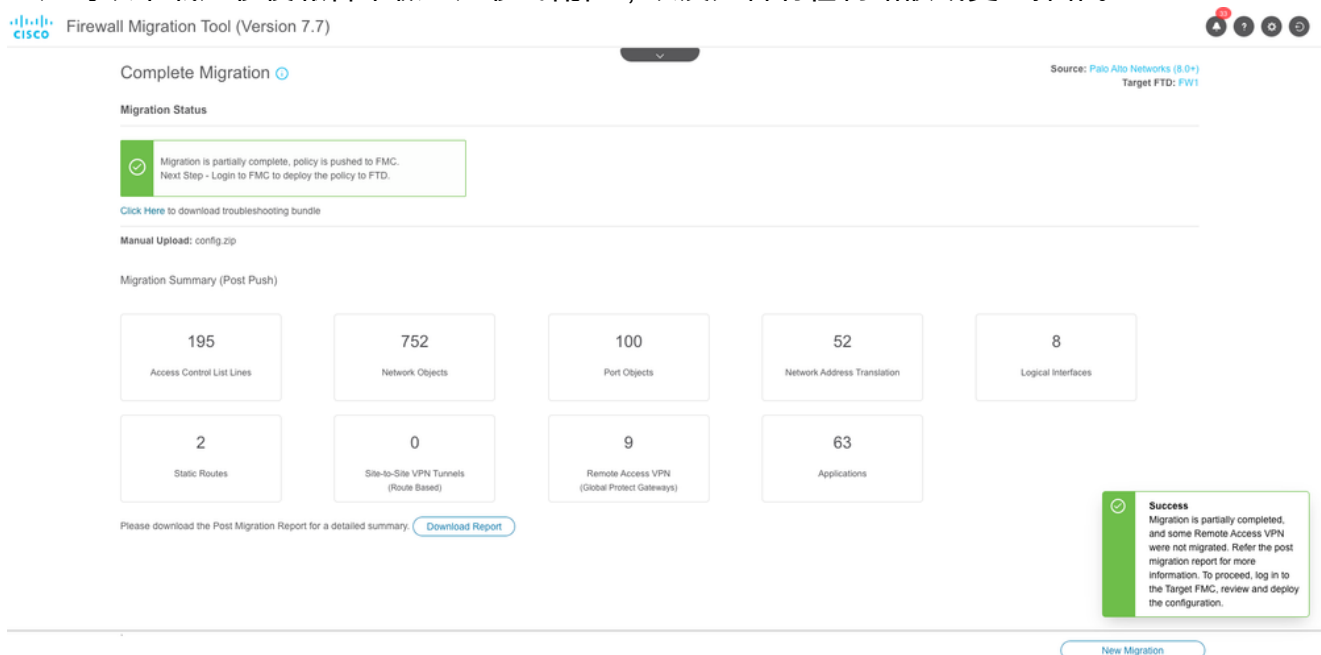
配置驗證摘要

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）。