

# 使用Firepower遷移工具從ASA配置檔案配置FTD

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[與Firepower遷移工具相關的已知錯誤](#)

[相關資訊](#)

---

## 簡介

本文檔介紹自適應安全裝置(ASA)到FPR4145上的Firepower威脅防禦(FTD)遷移的示例。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ASA基礎知識
- 瞭解Firepower管理中心(FMC)和FTD

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA版本9.12(2)
- FTD版本6.7.0
- FMC版本6.7.0
- Firepower遷移工具2.5.0版

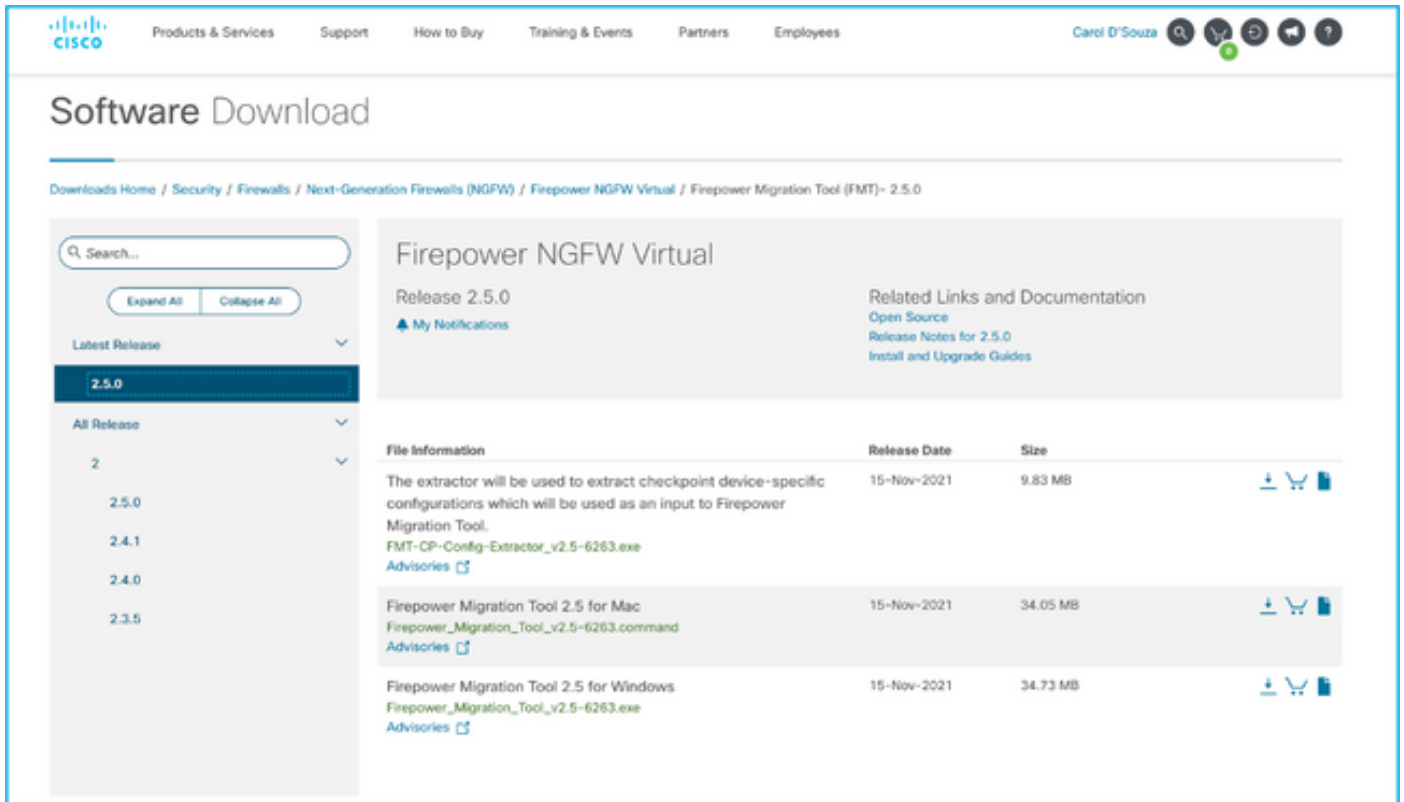
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

以或格式匯出ASA.cfg配置.txt檔案。FMC必須部署在其下註冊的FTD。

# 設定

1. 從 [software.cisco.com](https://software.cisco.com) 下載 Firepower 遷移工具，如下圖所示。



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual, Release 2.5.0. The page includes a search bar, a list of releases with 2.5.0 selected, and a table of file information.


File Information	Release Date	Size
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v2.5-6263.exe <a href="#">Advisories</a>	15-Nov-2021	9.83 MB
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command <a href="#">Advisories</a>	15-Nov-2021	34.05 MB
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe <a href="#">Advisories</a>	15-Nov-2021	34.73 MB

2. 檢視並驗證 Firepower 遷移工具部分的要求。

3. 如果計畫遷移大型配置檔案，請配置休眠設定，以便系統在遷移推送期間不進入休眠狀態。

3.1. 對於 Windows，導航到「控制面板」中的電源選項。按一下當前電源計畫旁邊的 Change Plan Settings，然後將 Put the computer to sleep 切換為 Never。按一下「Save Changes」。

3.2. 對於 MAC，請導航至系統首選項 > 節能程式。勾選「Prevent the Computer from Reading Automatically when the display is off (顯示器關閉時防止電腦自動休眠)」旁邊的框，然後將「Turn Display Off after (在滑動條後關閉顯示器)」拖到「Never (從不)」。

 **注意：**當 MAC 使用者嘗試開啟下載的檔案時，此警告對話方塊將彈出。忽略此問題並遵循步驟 4.1。



**“Firepower\_Migration\_Tool\_v2.5-6263.command” is a script app downloaded from the Internet. Are you sure you want to open it?**

Chrome downloaded this file today at 2:35 PM from **software.cisco.com**.

Open

Show Web Page

Cancel

4.1.對於MAC — 使用terminal並運行以下命令：

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command


[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: hompath is /Users/caroldso/Downloads
[75653] LOADER: _MEIPASS2 is NULL
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
l_v2.5-6263.command
[75653] LOADER: Cookie found at offset 0x219AE08
[75653] LOADER: Extracting binaries
[75653] LOADER: Executing self as child
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4.2.對於Windows — 按兩下Firepower遷移工具，以便在Google Chrome瀏覽器中啟動該工具。

5.接受許可證，如下圖所示：

← → ↻ 🏠 ⓘ localhost:8888/#/eula

 Firepower Migration Tool

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 specic product terms at [www.cisco.com/go/softwareterms](http://www.cisco.com/go/softwareterms) (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. Unless contrary to applicable law, You are not licensed to Use the Software on

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

[Proceed](#)

6.在Firepower遷移工具的登入頁面上，按一下使用Cisco Connection Online(CCO)連結登入，以便使用單點登入憑證登入到Cisco.com帳戶。

 **注意：**如果您沒有Cisco.com帳戶，請在Cisco.com登入頁面上建立。使用以下預設憑據登入：使用者名稱 — admin和密碼 — Admin123。

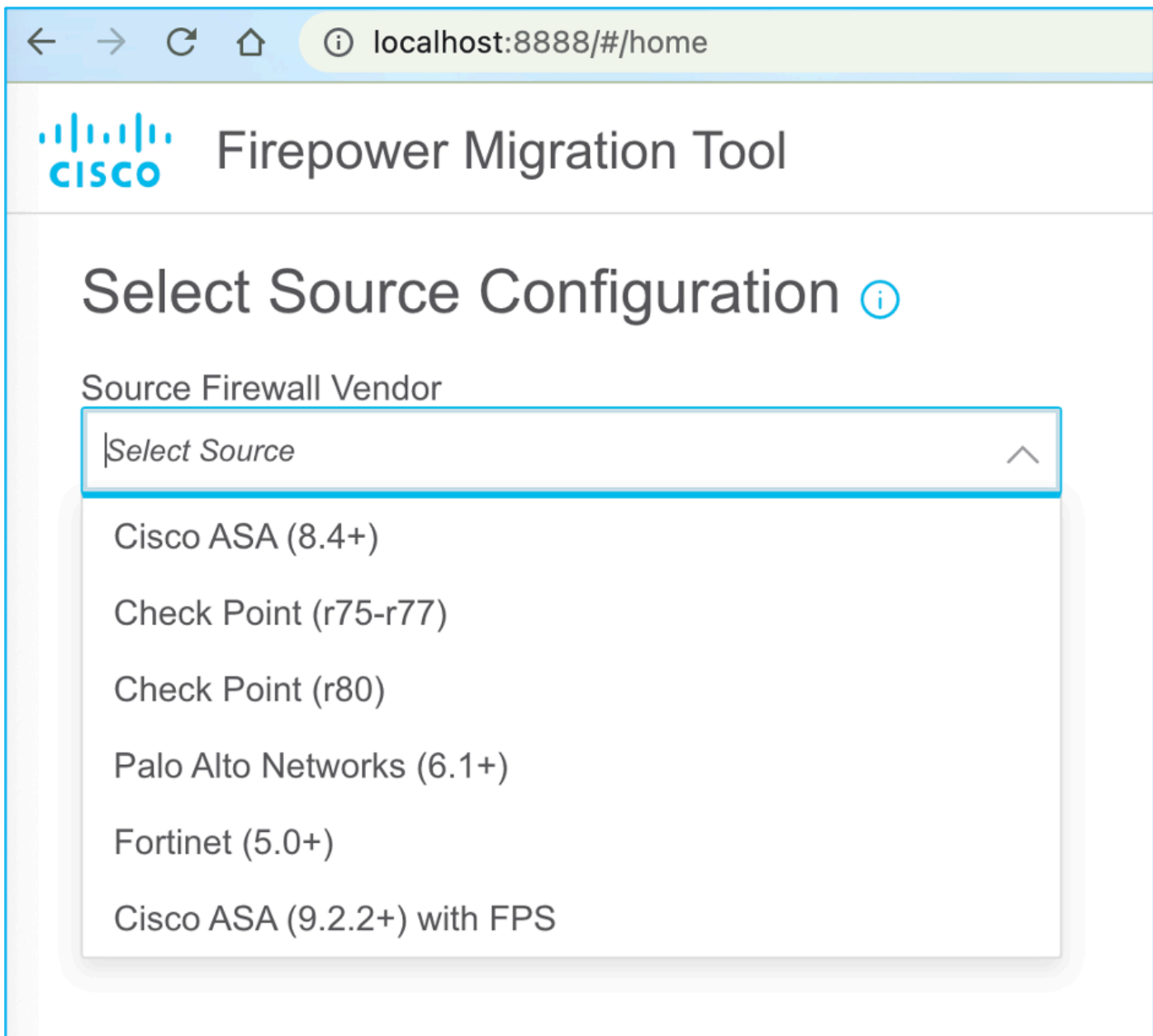
# Redirecting

You will be redirected to the Cisco login. Please login with your CCO credentials.

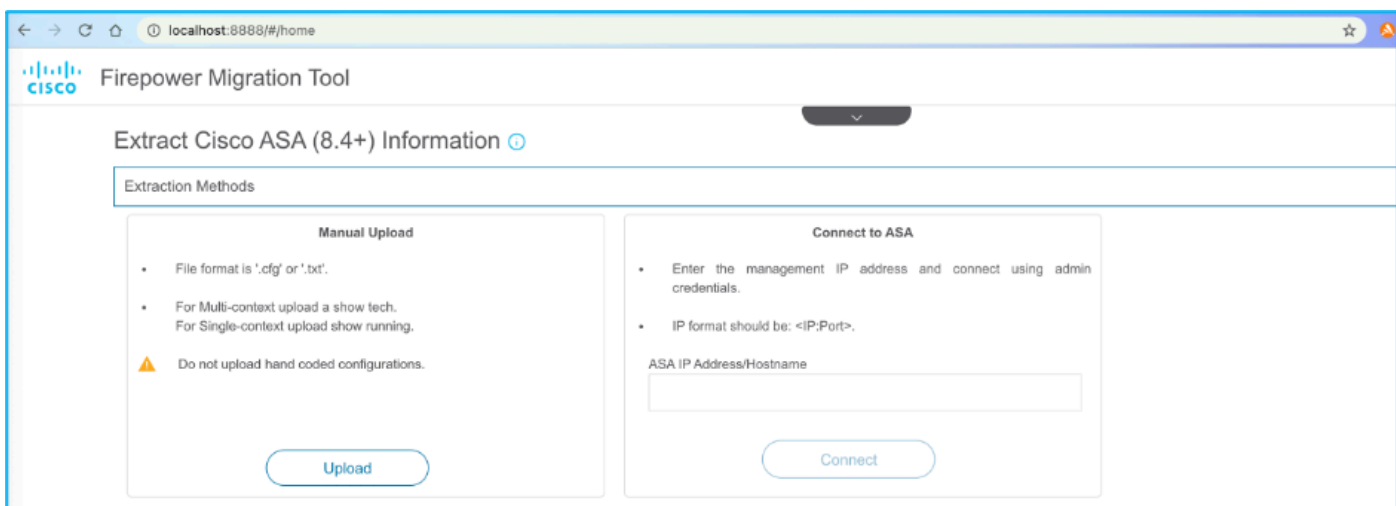
Do it later

Continue

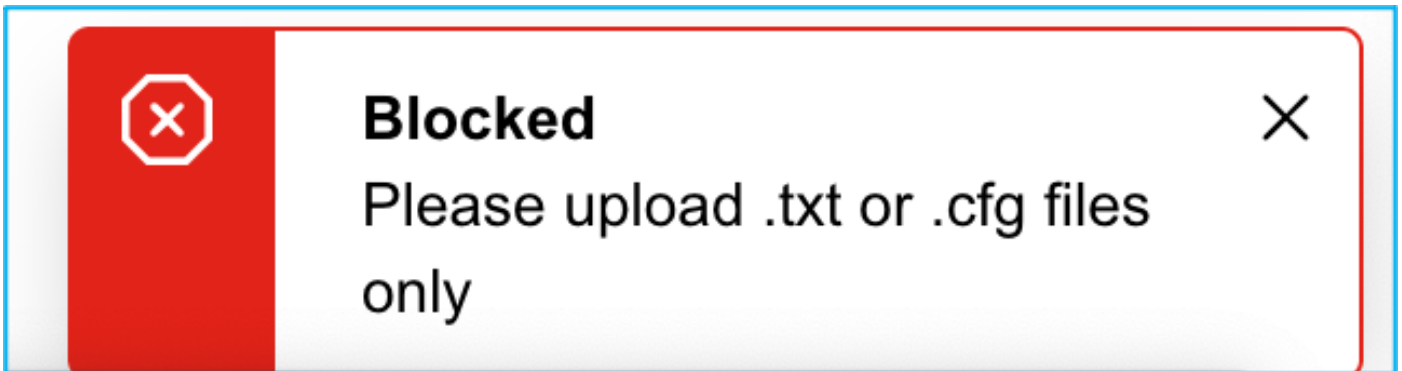
7.選擇來源配置。在此方案中，它是Cisco ASA(8.4+)。



8.如果您沒有到ASA的連線，請選擇Manual Upload。否則，您可以從ASA檢索運行配置，並輸入管理IP和登入詳細資訊。在此案例中，已執行手動上傳。



✎ 註：如果檔案不受支援，則會出現此錯誤。確保將格式更改為純文字檔案。(儘管具有擴展，但仍會出現.cfg錯誤。)



```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
!
hostname asa
enable password ***** pbkdf2
!
license smart
  feature tier standard
names
no mac-address auto

!
interface Ethernet1/1
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/2
  nameif Inside
  cts manual
  security-level 0
  no ip address
!
interface Ethernet1/3
  nameif Outside
  cts manual
  security-level 0
  no ip address
```

9.上傳檔案後，系統會分析元素，提供摘要，如下圖所示：



Firepower Migration Tool

Extract Cisco ASA (8.4+) Information Source: Cisco ASA (8.4+)

Extraction Methods >

Manual Upload: ASAConfig.cfg.txt

Context Selection >

Selected Context: Single Context Mode

Parsed Summary >

Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

20 Access Control List Lines	88 Network Objects	14 Port Objects	
8 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

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

10. 輸入要將ASA配置遷移到的FMC IP和登入憑證。確保可從工作站訪問FMC IP。

Firepower Migration Tool

Select Target Source: Cisco ASA (8.4+)

Connect to FMC >

FMC IP Address/Hostname  
10.108.52.10

Connect

Choose FTD >

Select Features >

Rule Conversion/ Process Config >



# FMC LOGIN

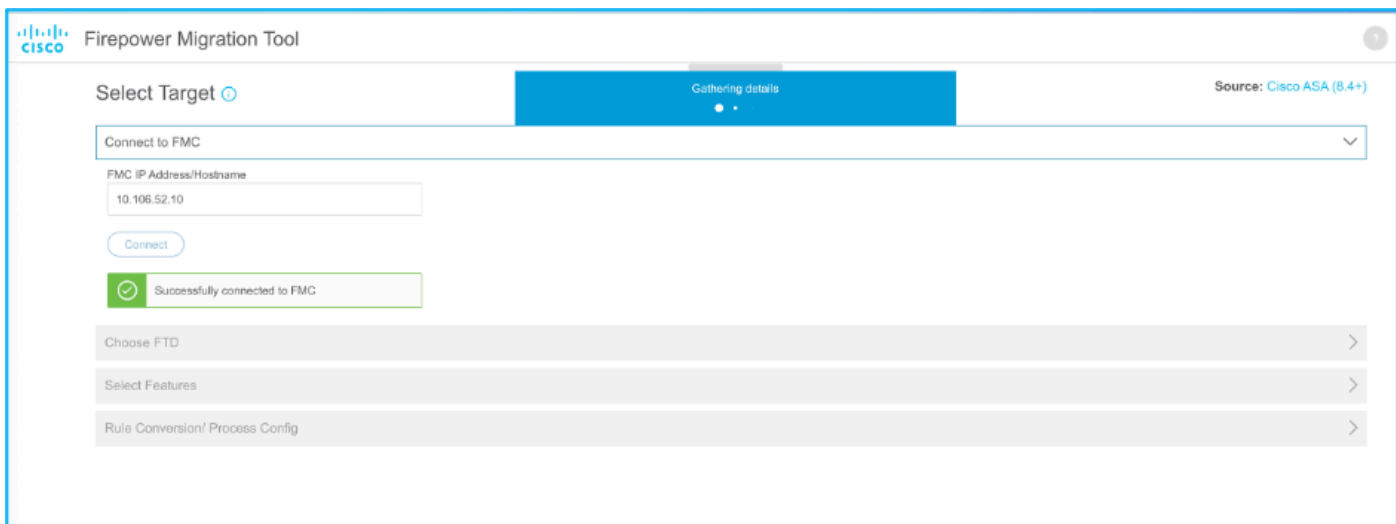
IP Address/Hostname

Username

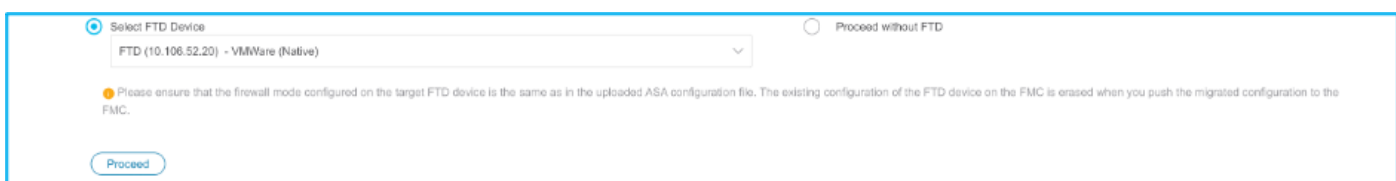
Password

Login

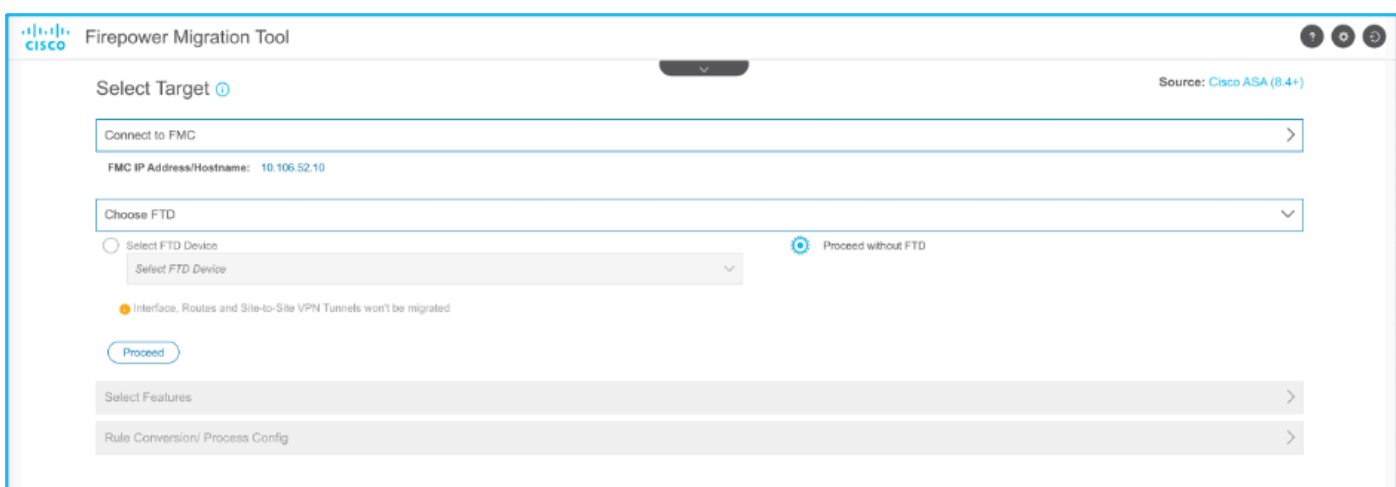
11.連線FMC後，其下方的託管FTD會顯示。



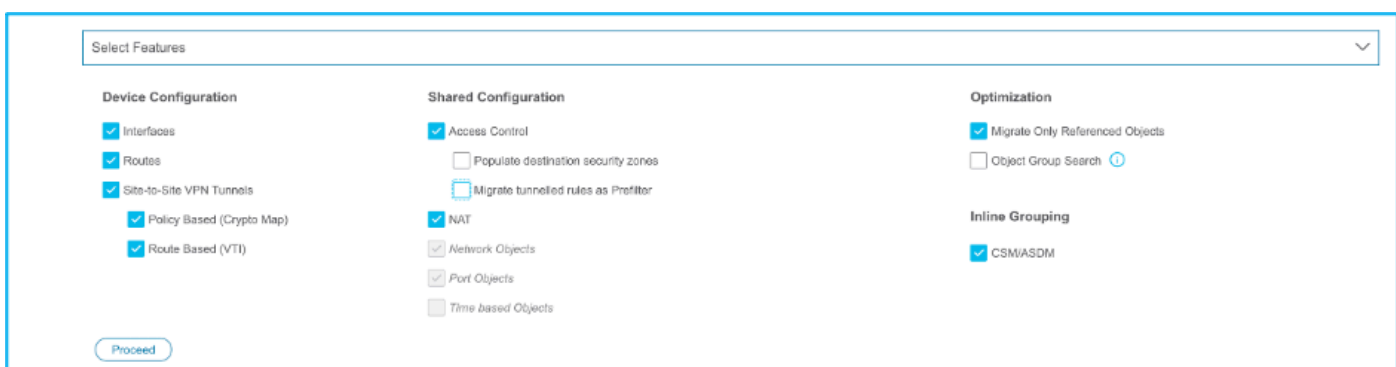
12. 選擇要執行ASA配置遷移到的FTD。



註：建議選擇FTD裝置，否則介面、路由和站點到站點VPN配置必須手動完成。



13. 選擇需要遷移的功能，如下圖所示：



14.選擇開始轉換，以啟動預遷移，預遷移將填充與FTD配置有關的要素。

The screenshot shows a web interface for 'Rule Conversion/ Process Config'. At the top, there is a 'Start Conversion' button. Below it, a message states '0 parsing errors found. Refer to the pre-migration report for more details.' A 'Download Report' button is also present. The main area displays a summary of configuration elements in seven boxes:

Element	Count
Access Control List Lines	13
Network Objects	98
Port Objects	30
Logical Interfaces	2
Static Routes	9
Network Address Translation	4
Site-to-Site VPN Tunnels	1

15.按一下Download Report ( 先前出現 )，檢視遷移前報告，如下圖所示：

← → ↻ 🏠 ⓘ File | /Users/caroldso/Downloads/pre\_migration\_report\_asa\_2021-11-23\_09-41-15.html

**CISCO** Pre-Migration Report

**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 reviewing the configuration 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	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

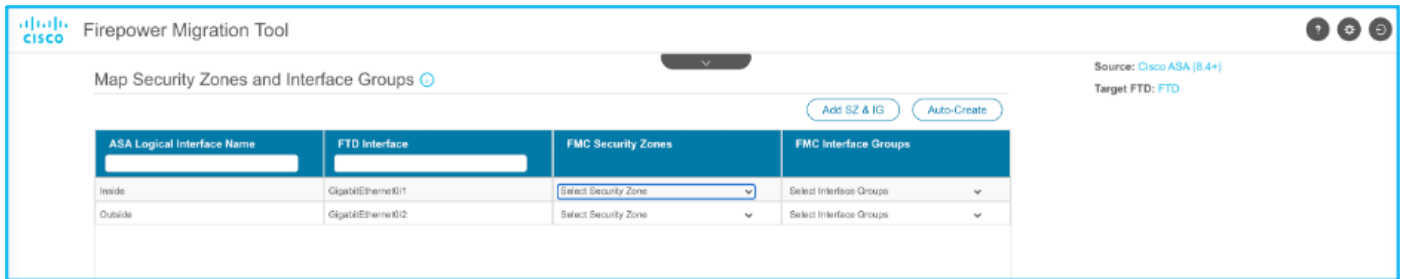
**Note:** ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. 根據需要將ASA介面對映到FTD介面，如下圖所示：

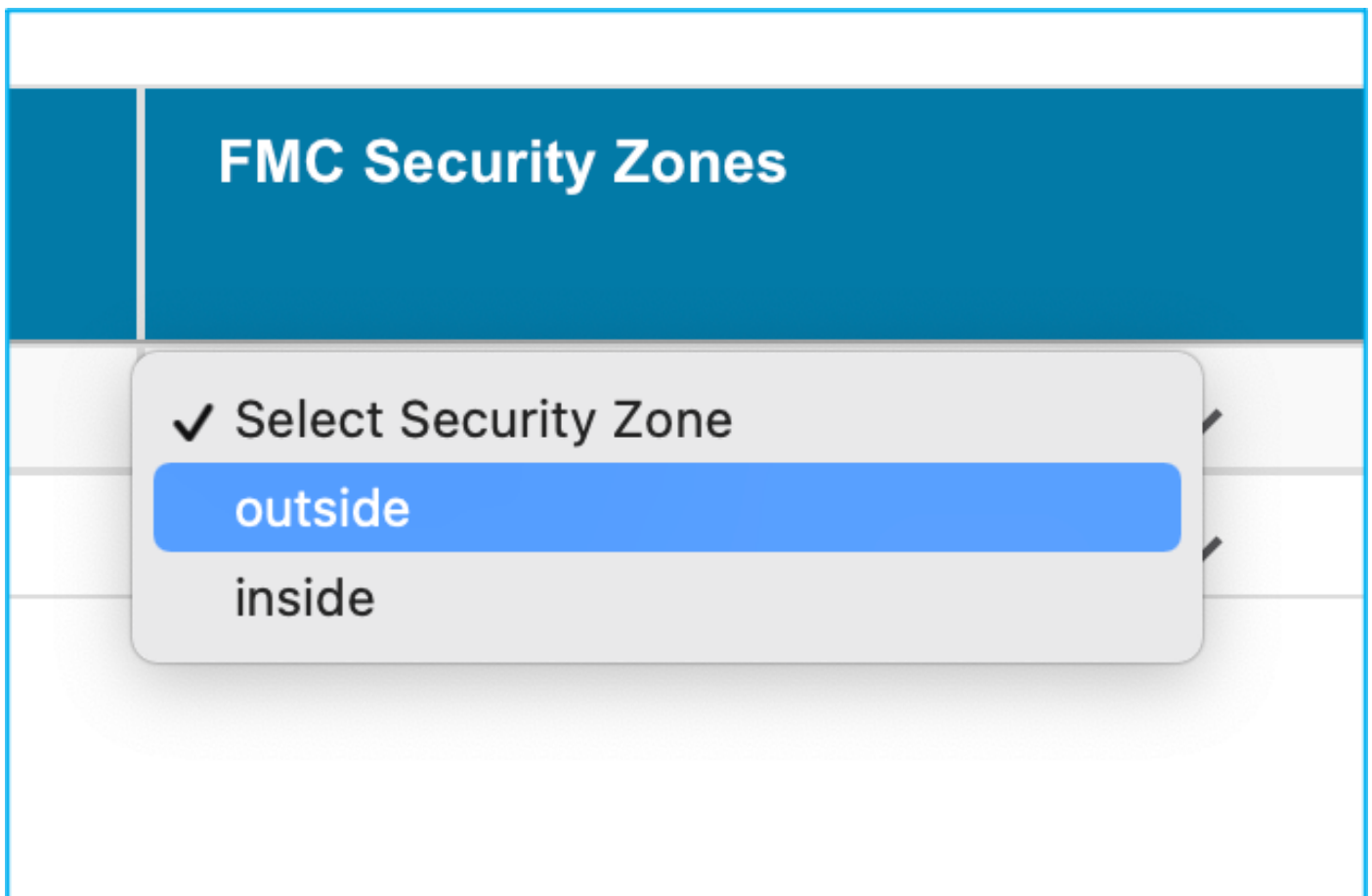
Refresh

ASA Interface Name	FTD Interface Name
<input type="text"/>	Select Interface
Ethernet1/2	GigabitEthernet0/0
Ethernet1/3	GigabitEthernet0/1
	✓ GigabitEthernet0/2

17. 將安全區域和介面組分配給FTD介面。



17.1. 如果FMC已建立安全區域和介面組，則可以根據需要選擇它們：



17.2. 如果需要建立安全區域和介面組，請按一下Add SZ & IG，如下圖所示：

✕

## Add SZ & IG

Security Zones (SZ)Interface Groups (IG)

Add

i

Max 48 characters for Interface Group name. Allowed special characters are \_.-+

Interface Groups	Type	Actions
<input style="width: 100%; border: 1px solid #ccc;" type="text" value="Inside"/>	ROUTED	<span style="background-color: black; color: white; border-radius: 50%; padding: 5px 10px; display: inline-block;">✕</span> <span style="background-color: #28a745; color: white; border-radius: 50%; padding: 5px 10px; display: inline-block;">✓</span>

0 - 0 of 0 |< < > >|

Close

17.3. 否則，您可以繼續使用Auto-Create選項，該選項將分別建立名為ASA logical interface\_sz和ASA logical interface\_ig的安全區域和介面組。

# Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to ASA interfaces

Security Zones  Interface Groups

Cancel

Auto-Create

 Firepower Migration Tool

Map Security Zones and Interface Groups ⓘ

[Add SZ & IG](#) [Auto-Create](#)

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	inside ▼	Inside_jg (A) ▼
Outside	GigabitEthernet0/2	outside ▼	Outside_jg (A) ▼

18. 審查並驗證所建立的每個FTD要素。警報以紅色顯示，如下圖所示：



Firepower Migration Tool

Optimize, Review and Validate Configuration

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

Access Control NAT Network Objects Port Objects Interfaces Routes VPN Objects Site-to-Site VPN Tunnels

ACP Pre-filter

Select all 13 entries Selected: 0 / 13 Actions Save

Search

#	Name	SOURCE			DESTINATION			State	Action	ACE Count
		Zone	Network	Port	Zone	Network	Port			
<input type="checkbox"/>	1	Outside_access_in_#1	outside	any	ANY	ANY			Allow	1
<input type="checkbox"/>	2	Outside_access_in_#2	outside	any	ANY	ANY			Allow	1
<input type="checkbox"/>	3	Outside_access_in_#3	outside	any	ANY	ANY			Allow	2
<input type="checkbox"/>	4	Outside_access_in_#4	outside	any	ANY	ANY			Allow	4
<input type="checkbox"/>	5	Outside_access_in_#5	outside	any	ANY	ANY			Allow	3
<input type="checkbox"/>	6	Outside_access_in_#6	outside	any	ANY	ANY			Allow	2
<input type="checkbox"/>	7	Outside_access_in_#7	outside	any	ANY	ANY			Allow	3
<input type="checkbox"/>	8	Outside_access_in_#8	outside	any	ANY	ANY			Allow	1
<input type="checkbox"/>	9	Outside_access_in_#9	outside	any	ANY	ANY			Allow	8
<input type="checkbox"/>	10	Outside_access_in_#10	outside	any	ANY	ANY			Allow	7
<input type="checkbox"/>	11	Outside_access_in_#11	outside	any	ANY	ANY			Allow	2
<input type="checkbox"/>	12	Outside_access_in_#12	outside	any	ANY	ANY			Allow	1

50 per page 1 to 13 of 13 Page 1 of 1

Update the Pre-Shared-Key/PG Certificate column highlighted in Yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration. For additional help, click here.

Optimize ACL (Beta) Validate


19. 如果要編輯任何規則，可以選擇遷移操作，如下圖所示。在此步驟中，可以完成新增檔案和IPS策略的FTD功能。


ACP Pre-filter

Select all 13 entries Selected: 13 / 13 Actions Save

#	Name	MIGRATION ACTIONS			SOURCE
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	Do not migrate		
<input checked="" type="checkbox"/>	2	Outside_access_in_#2	RULE ACTIONS		
<input checked="" type="checkbox"/>	3	Outside_access_in_#3	File Policy		
<input checked="" type="checkbox"/>	4	Outside_access_in_#4	IPS Policy		
<input checked="" type="checkbox"/>	5	Outside_access_in_#5	Log		
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside	any	

註：如果FMC中已存在檔案策略，則會填充它們，如下圖所示。對於IPS策略以及預設策略

 , 情況也是如此。



## File Policy

Select File Policy \*

eicar  
None

Cancel

Select

可以完成所需規則的日誌配置。在此階段，可以選擇FMC上現有的Syslog伺服器配置。



# Log

Log at the beginning of connection

Log at the end of connection

## Send connection events to:

Event Viewer

Syslog

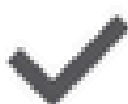
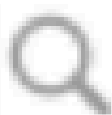
Cancel

Save

所選擇的規則操作會針對每個規則相應加亮。



## State



## 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）。