使用FMT將ASA遷移到Firepower威脅防禦(FTD)

目錄
<u>必要條件</u>
採用元件
概觀
<u>背景資訊</u>
獲取ASA配置檔案
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
<u>設定</u>
<u>設定步驟:</u>
<u>疑難排解</u>
<u>安全防火牆遷移工具故障排除</u>

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。 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<u>Firepower管理中心</u> 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:

CISCO Products & Service	ces Support	How to Buy	Training & Events	Partners	Employees		Wasim Hussain Dhaa	" ଷ ଷ୍ଟୃତ ପ ଡ
Software Do	wnload							
Downloads Home / Security / Fire	walls / Secure Fire	wall Migration Tool /	Firewall Migration Tool (F	FMT)- 7.0.0				
Q. Search Expand All Collaps Latest Release 7.0.1	e All	Secure Release 7.0.	Firewall Mig	ration T	- 00l	Related Links Open Source Release Notes for 7 Install and Upgrade	and Documentation 7.0.0 Guides	
All Release	~	Eile Information				Polosso Date	Cize	
7 7.0.1	~	Firewall Migration Firewall_Migration_ Advisories	n Tool 7.0.0.1 for Mac Tool_v7.0.0.1-11241.co	mmand		04-Sep-2024	41.57 MB	±₩∎
7.0.0		Firewall Migration Firewall_Migration_ Advisories	n Tool 7.0.0.1 for Wind Tool_v7.0.0.1-11241.ex	dows e		04-Sep-2024	39.64 MB	± ∵ ∎
		Firewall Migration Firewall_Migration_ Advisories	n Tool 7.0.0 for Mac Tool_v7.0-11136.comm	and		05-Aug-2024	41.55 MB	± \; ∎
		Firewall Migration Firewall_Migration_ Advisories	n Tool 7.0.0 for Windo Tool_v7.0-11136.exe	ws		05-Aug-2024	39.33 MB	±∵≓∎

軟體下載

2. 按一下您以前下載到您電腦的檔案。



```
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 pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortine
t Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']}, 'se
curity_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INF0 | 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 : {}"
                                 common] > "Telemetry push : Able to connect t
2025-01-16 16:51:41,838 [INFO
o 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"
                                 common] > "proxies : {}"
2025-01-16 16:51:46,868 [INFO
2025-01-16 16:51:48,230 [INFO
                                 common] > "Telemetry push : Able to connect t
o 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Proceed(繼續)。



CISCO Firewall Migration Tool

END USER LICENSE AGREEMENT



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 ontions
	Sustam status - Policy statement

FMT登入

5. 選擇要遷移的源防火牆。





Select Source Configuration ()

Select Source	^
Cisco Legacy Firewalls	
Cisco ASA (8.4+)	
Cisco ASA (9.2.2+) with FirePOWER Services	
Cisco Secure Firewall Device Manager (7.2+)	
Third Party Firewalls	
Check Point (r75-r77)	
Check Point (r80-r81)	
Fortinet (5.0+)	
Dala Alta Naturarke (8.0+)	

Cisco ASA (8.4+) Pre-Migration Instructions

(i) This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.

Session Telemetry:

Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:

FMC: Firewall Management Center

Before you begin your Adaptive Security Appliance (ASA) to Firewall Threat Defense migration, you must have the following items:

Stable IP Connection:

FMT: Firewall Migration Tool FTD: Firewall Threat Defense

Ensure that the connection is stable between FMT and FMC.

• FMC Version:

Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.

- FMC Account:
 - Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.

• FTD (Optional):

To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.

來源防火牆

6. 選擇用於獲取配置的提取方法。

- 1. 手動上傳要求您以Running Config「.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。

cisco F	Firewall Migration Tool								000
		1 Extract A SA Information	2 Select Target	3 Map PTD Interface	4 Map Security Zones & Interface Oroups	5 Optimize, Review & Validate	6 Complete Migration		
	Extract Cisco AS	SA (8.4+) Information	0		<u>^</u>			Source: Cisco ASA (8.4+)	
	Extraction Methods							~	
	File format is '.ctg' For Multi-context For Single-context Do not upload har	Manual Upload or '.txt'. upload a show tech. tupload show running. Ind coded configurations. Upload		Cor . Enter the management credentials. . IP format should be: <ip pc<br="">ASA IP Address/Hostname 192.168.1.20 C</ip>	IP address and connect using rtb,	admin			
	Context Selection							>	
	Parsed Summary							>	

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,請按一下下一步。

CISCO Firewall Migration Tool

00

P Address: 192.168.1.20										
P Address: 192.168.1.20										
ext Selection										
Single Context Mode: Download config										
ed Summary										
et Hitcounts: No										
8	2	0	0	0						
Access Control List Lines	Access List Objects	Network Objects	Port Objects	Dynamic-Route Objects						
	(Standard, Extended used in BGP/RAVPN/EIGRP)			(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)						
0	1	1	0	0						
abunda Addasan Yanashalina	-	Protec	Charles City UDAL Y-march	Damala Associ 1/041						
enrork Address Transation	cogcar interaces	Routes	Sile-to-Sile YPN Tunnels	(Connection Profiles)						
etwork Address Translation	Logical Interfaces	Routes	Site-to-Site VPN Tunnels	Remote Access VPN (Connection Profiles)						

摘要

https://cisco.com

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。

cisco Firewa	I Migration Tool		000
	Select Target 🕢	ource: Cisco ASA (8.4+)	
	Firewall Management	~	
	On-Prem/Virtual FMC Cloud-delivered FMC FMC IP Address/Hostname 192.163.1.18 Connect FTD(s) Found Froceed		
	Successfully connected to FMC		
	Choose FTD	>	
	Select Features	>	
	Rule Conversion/ Process Config	>	

■∞ ■ 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

Back Next

diada cisco	Firewa	all Migration Tool	
		Select Target ()	Cisco ASA (8.4+)
		Firewall Management	>
		FMC IP Address/Hostname: 192.168.1.18	
		Choose FTD	\sim
		Select FTD Device FTD (192:156:1.17) - VM/Ware (Native) V	
		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 migrate FMC.	ed configuration to the
		Proceed	
		Select Features	>
		Rule Conversion/ Process Config	>

目標FTD

10. 選擇要遷移的配置,螢幕截圖上顯示選項。

cisco	Firewa	all Migration Tool			000
		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	Shared Configuration	Optimization	
		Interfaces	Control	Migrate Only Referenced Objects	
		Routes	Populate destination security zones	Object Group Search 🕕	
		Static	Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.	Inline Grouping	
		Elepp	 Migrate tunnelled rules as Prefilter 		
		Cito In Site UDM Tunnale (no data)	NAT (no data)	CSM/ASDM	
		Bolicy Based (Counts Man)	Vetwork Objects (no data)		
		Porty based (07)	Port Objects (no data)		
		There have a trip	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.		
		Proceed			
				Back	

組態

11.開始將配置從ASA轉換為FTD。

Firewall Migration Tool

	Extract ASA Information	2 Select Target	3 Map FTD Interface	4 Map Security Zones & Interface Groups	5 Optimize, Review & Validate	6 Complete Migration	
Select Target 💿				<u>^</u>			Source: Cisco ASA (8.4+)
Firewall Management							>
FMC IP Address/Hostname	к 192.168.1.18						
Choose FTD							>
Selected FTD: FTD							
Select Features							>
Rule Conversion/ Process	s Config						~
Start Conversion							

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. 您可以選擇Download Report按一下以接收要遷移的配置的摘要。

Select Target 🕔			Source: Cisco ASA (
Firewall Management							
FMC IP Address/Hostname: 192.168.1.18							
Choose FTD							
Selected FTD: FTD	elected FTD: FTD						
elect Features							
lule 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	Network Objects	Port Objects	Dynamic-Route Objects			
	(Standard, Extended used in BGP/RAVPN/EIGRP)			(AS-Path, Community-List, Policy-List, Pretto-List, Route-Map)			
0	1	1	0	0			

下載報告

遷移前報告示例,如下圖所示:

Back Next



CISCO Pre-Migration Report

Back Next

Note: Review all contents of this pre-migration report or Defense after the configuration is successfully migrated traffic is anoronriately has

1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepo

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)
ASAHostname	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。

Map FTD Interface () Source: Claco ASA (6.4+) Target FTD: FTD	
NIGELFICEFIC	
Refresh	
ASA Interface Name FTD Interface Name	
Management0/0 GigablEthemet0/0 v	
20 v perpage 1to1of1 4 4 Page 1 of1 ▶ ▶	

對映介面

14. 為FTD上的介面建立安全區域和介面群組



Back Next

Back Next

Map Security Zones and In	nterface Groups 🕕	, v	
			Add SZ & IG Auto-C
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	✓ Select interface Groups

10 v per page 1 to 1 of 1 4 4 Page 1 of 1 + +

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:

cisco	Firewall Migration Tool									000
		1 Extract ASA Information	2 Select Target	3 Map FTD Interface	Map Security Zone	& Interface Groups	5 Optimize, Review & Validate	6 Complete Migration		
	Map Security Zone	s and Interface Groups	s ()		^	(Add SZ & I	G Auto-Create	Source: Cisco A Target FTD: FTD	3A (8.4+)	
	ASA Logical Interface Na	me FTD Interface		FMC Security Zones		FMC Interface C	proups			
	management	GigabitEthernet0/0		management	~	management_ig (A)	~			

10 v per page 1 to 1 of 1 4 4 Page 1 of 1 > >

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檢視和最佳化,請按一下validate。



	date Configuration ()		Target FTD: FTD
Access Control Objects NAT Interfac	Ces Routes Site-to-Site VPN Tunnels Remote Access VPP		
Select all 1 entries Selected: 0 / 1	Actions - Sive		Q. Search
Name	Validation State	Туре	Value
0 1 obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1
00j-192.168.1.1	vini be created in FMC	reework object	192.108.1.1

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

審閱和驗證

16. 如果驗證狀態成功,將配置推送到目標裝置。

cisco Firewall Migration Tool							009
Optimize, Review and Val		Va Ø	alidation Statu	S	×	Vegation urce: Clisco ASA (8.4+) get FTD: FTD	
Access Control V Objects V NAT V Access List Objects Network Objects Select all 1 entries Selected 0/1	Validation Summary (Pre-	push) Not selected for migration Access List Objects (Standard, Extended used in	1 Network Objects			Search	1
1 06-192.166.1.1		BOPRIVEPORIP)	1 Routes				
	😗 Note: T	he configuration on the target F	TD device FTD (192.168.1.17) Push Configuration	will be overwritten as part of th	is migration.		
50 v per page 1 to 1 of 1 + 4 Page 1 of 1 + 4 Note: Populate the areas highlighted in Yellow	in EIGRP, Site to Site and Rem	ote Access VPN sections to val	idate and proceed with migrati	on			adato

驗證

通過遷移工具推送的配置示例,如下圖所示:

Validate

Firewall Migration Tool				000
Complete Migra Migration Status	Extract ALA Information	PUSHING 25% Complete Push In progress. Refer FMT Terminal to monitor the migration status.	3 Continues, Review & Valuation Sources: Clisco ASA (8.4+) Target FTD: FTD	
Interfaces	0			
Network Objects				
Access Control Policie				
Please download the Post-P	ush migration report for a detailed summary Download Re			

推送

成功遷移的示例,如下圖所示:

diada cisco	Firewall Migration Tool					000
	0	1 2 tract ASA information Select Target	3 Map FTD Interface Map Secu	4 5	Complete Migration	
	Complete Migration ()				Source: Cisco ASA (8.4+) Target FTD: FTD	
	Migration Status			Optimization Status		
	Migration is complete, policy is Next Step - Login to FMC to de	pushed to FMC. ploy the policy to FTD.		ACL Optimization is not appl	ied for this migration.	
	Live Connect: asaconfig.bd Selected Context: Single Context Mode	•				
	Migration Summary (Post Push)					
	0		1			
	Access Control List Lines		Network Objects			
		1	1			
		Logical Interfaces	Routes			
	Planet data also dike Park Park adarbit				New Migration	\supset

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. 導航到選項卡Deploy。
- 3. 選擇要將配置推送到防火牆的部署。

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)。