

Migrate Paloalto to Firepower Threat Defense Using FMT

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Background Information](#)

[Obtain Paloalto Firewall Configuraton zip file](#)

[Pre-Migration Checklist](#)

[Configure](#)

[Migration Steps](#)

[Troubleshoot](#)

[Troubleshooting Secure Firewall Migration Tool](#)

[Common migration failures:](#)

[Using the Support Bundle for troubleshooting:](#)

Introduction

This document describes the procedure to migrate Paloalto Firewall to Cisco Firepower Threat Device .

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Migration tool
- Paloalto Firewall
- Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

Components Used

The information in this document is based on these software and hardware versions:

- Mac OS with Firepower Migration Tool (FMT) v7.7
- PAN NGFW version 8.0+
- Secure Firewall Management Center (FMCv) v7.6
- Secure Firewall Threat Defense version 7.4.2

Disclaimer: The networks and IP addresses referenced in this document are not associated with any individual users, groups, or organizations. This configuration has been created exclusively for use in a lab environment.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Specific requirements for this document include:

- PAN NGFW version 8.4+ or later
- Secure Firewall Management Center (FMCv) Version 6.2.3 or later

The Firewall Migration Tool supports this list of devices:

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Cisco Secure Firewall Device Manager (7.2+)
- Check Point (r75-r77)
- Check Point (r80-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

Background Information

Before you migrate your Paloalto Firewall configuration, execute these activities:

Obtain Paloalto Firewall Configuraton zip file

- Paloalto Firewall must be version 8.4+.
- Export the current running configuration from the Palo Alto firewall (*.xml must be in xml Format).
- Log in to Paloalto Firewall Cli to execute show routing route and save the ouput in txt format (*.txt).
- Compress the running configuration file (*.xml) and Routing file (*.txt) with the an extension of *.zip.

Pre-Migration Checklist

- Ensure the FTD has been registered to the FMC before beginning the migration process.
- New user account with administrative privileges has been created on the FMC. Or existing admin credentials can be used.
- Exported Palo Alto running configuration file.xml must be zipped with an extension of .zip (follow the procedure mentioned in previous section).
- Firepower device must have the same or more number of Physical or Sub-interface or Port-channels compared to Paloalto Firewall interfaces.

Configure

Migration Steps

1. **Download** the most recent Firepower Migration Tool from Cisco Software Central that is compatible to your computer:

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

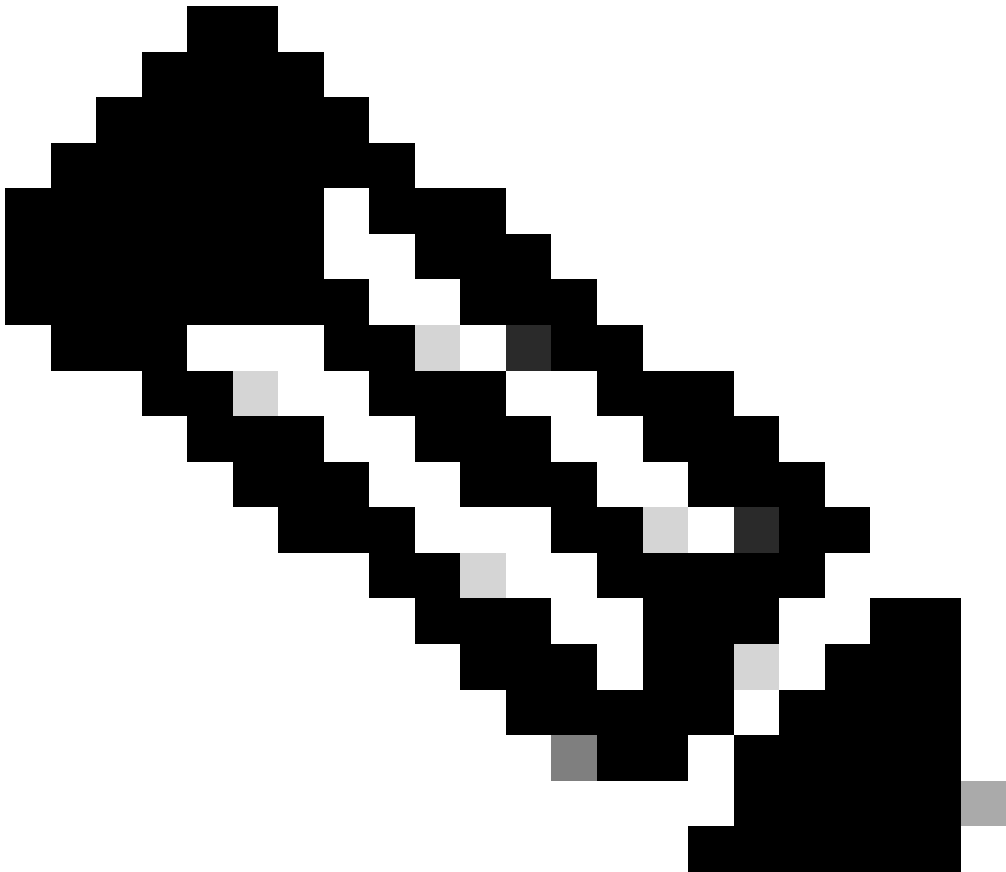
Release Notes for 7.7.0

Install and Upgrade Guides

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

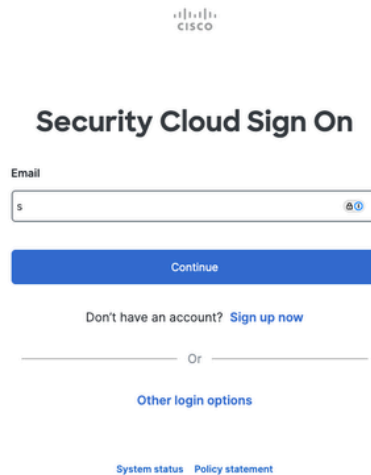
FMT Download

3. **Open** the file you previously downloaded to your computer.



Note: The program opens automatically and a console auto generates content on the directory where you ran the file.

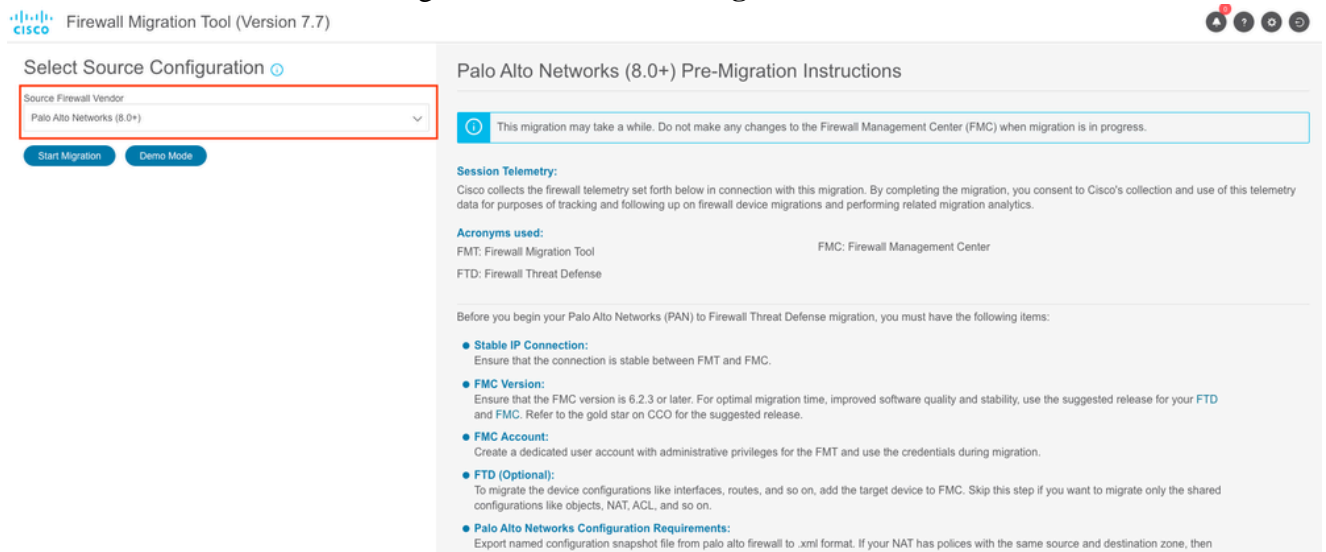
4. After you run the program, it opens a web browser that displays the **End User License Agreement**.
 1. **Select** the check box to accept terms and conditions.
 2. Click **Proceed**.
5. Log in using a valid CCO credentials in order to access FMT GUI.



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 a link: "Other login options". At the bottom are two links: "System status" and "Policy statement".

FMT Login Prompt

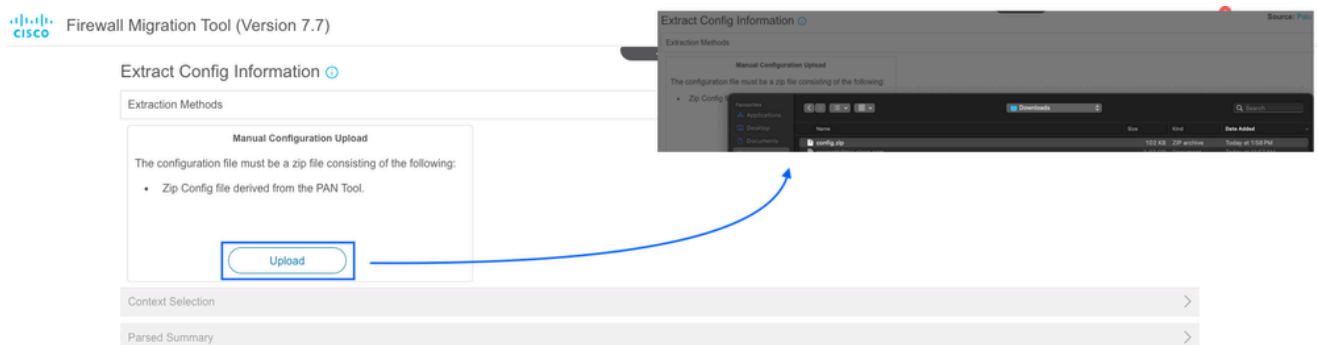
6. Select the Source Firewall to migrate and click **Start Migration**.



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 two buttons: "Start Migration" and "Demo Mode". 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 are sections for "Session Telemetry", "Acronyms used" (FMT: Firewall Migration Tool, FTD: Firewall Threat Defense, FMC: Firewall Management Center), and a list of requirements for migration.

FMT GUI

7. Extraction Methods section is now displayed, where you must **upload** the Zip configuration file from Paloalto Firewall to the FMT.



The image shows the Firewall Migration Tool (Version 7.7) interface, specifically the "Extract Config Information" section. 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 bullet point: "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 "config.zip" file in the "Downloads" folder. A blue arrow points from the "Upload" button to the "config.zip" file.

Configuration Upload Wizard

8. Parsed Configuration summary is now displayed after the configuration file is uploaded. In case of VSYS, separate VSYS selections are available. Each of them must be parsed and migrated one after another.

Validate the parsed summary and click **Next** icon.

Firewall Migration Tool (Version 7.7)

Source: Palo Alto Networks (8.0+)

Extract Config Information

Extraction Methods

Context Selection

Parsed Summary

184 Access Control List Lines	908 Network Objects	150 Port Objects	49 Network Address Translation	9 Logical Interfaces
15 Static Routes	73 Applications	4 Site-to-Site VPN Tunnels (Route Based)	13 Remote Access VPN (Global Protect Gateways)	

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

Success
Context list Collected Successfully

Back Next

Configuration Validation Summary

9. You can choose the type of FMC in this section. Provide its management IP address and click on **Connect**.

A pop up is displayed prompting for providing FMC credentials. Enter the credentials and click **Login**.

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

Connect

Choose FTD

Select Features

Rule Conversion/ Process Config

FMC Login

IP Address/Hostname/FQDN
10.225.107.99

Username
admin

Password

Login

FMC Login

10. Up on successfully connecting to FMC, you can now choose the **Domain** (if any) and click **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

Domain Selection

11. Choose the FTD to which you are going to migrate to and click **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 >

Select Target FTD

12. The tool now list out the features that are going to be migrated. Click **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

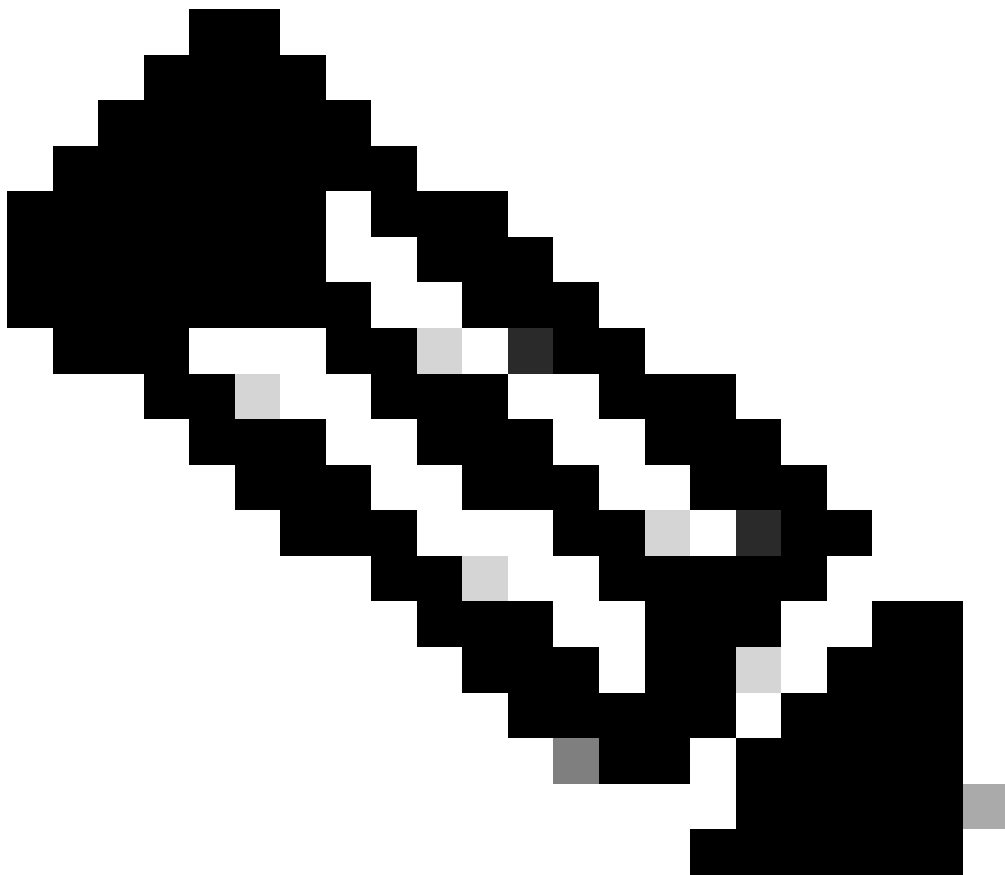
Select Features ▼

Device Configuration <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Interfaces <input checked="" type="checkbox"/> Routes <input checked="" type="checkbox"/> Site-to-Site VPN Tunnels <ul style="list-style-type: none"> <input type="checkbox"/> Policy Based (Unsupported) ? <input checked="" type="checkbox"/> Route Based (VTI) 	Shared Configuration <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Access Control <ul style="list-style-type: none"> <input type="checkbox"/> Migrate policies with Application-default as Enabled ? <input checked="" type="checkbox"/> Network Objects <input checked="" type="checkbox"/> Port Objects <input checked="" type="checkbox"/> Remote Access VPN 	Advanced Configuration <ul style="list-style-type: none"> Optimization <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Migrate Only Referenced Objects Access Control Options <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Discovered Identities ?
---	--	---

Proceed

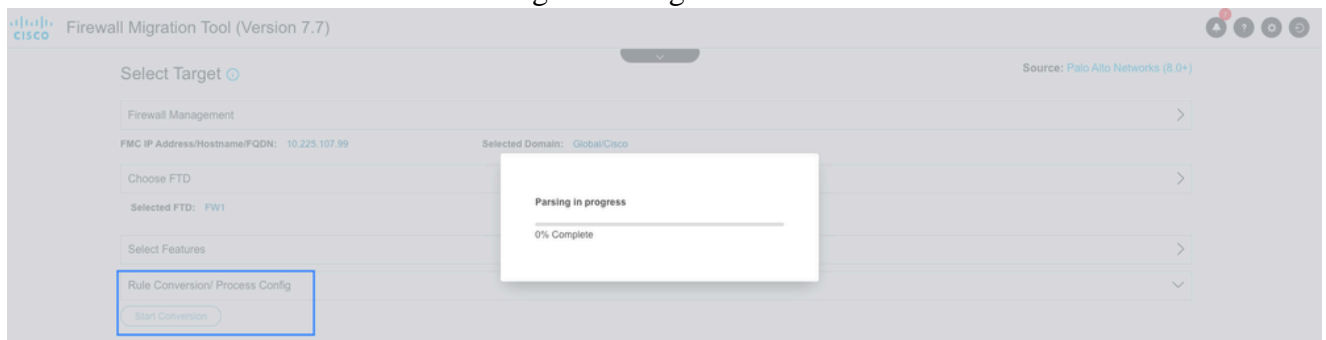
Rule Conversion/ Process Config >

Feature Selection



Note: All the features are selected by default. You can deselect any configuration which is not to be migrated.

13. Click on **Start Conversion** for converting the configuration.



Parsing Configuration

The Tool Parses the configuration and display the conversion summary as shown in the image. You can also download the **Pre-Migration Report** for validating the migrated configuration for any **Errors** or **Warnings**, if any. Navigate to next page by clicking **Next**.

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](#)

Parsed Configuration Summary

14. You can define Paloalto to FTD interface mapping as well as edit interface name for each interface in the Interface Mapping Section. Click **Next** after the **Interface Mapping** is completed.

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

PAN Interface Name	FTD Interface Name	Mapped NameIf
ethernet1/2	Select Interface	ethernet1_2
ethernet1/3	✓ Ethernet1/1	ethernet1_3
ethernet1/4	Ethernet1/10	ethernet1_4
ethernet1/5	Ethernet1/11	ethernet1_5
ethernet1/6	Ethernet1/12	ethernet1_6
ethernet1/7	Ethernet1/13	ethernet1_7
	Ethernet1/14	
	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](#)

Interface Mapping

15. You can either **Add the Security Zone** manually for each interfaces or **Auto Create** it in Map the Security Zone section . Click **Next** after creating and mapping Security Zones.

Map Security Zones

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

Add SZ

Auto-Create

Save

PAN Zone Name	FMC Security Zones
G-Inside	Select Security Zone
Outside	Select Security Zone
GPVFN-	Select Security Zone
I-Inte	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

First option is to add Security Zone manually and second option is to auto create 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

Security Zone Creation

Manual Creation of Security Zones:

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 _-+*

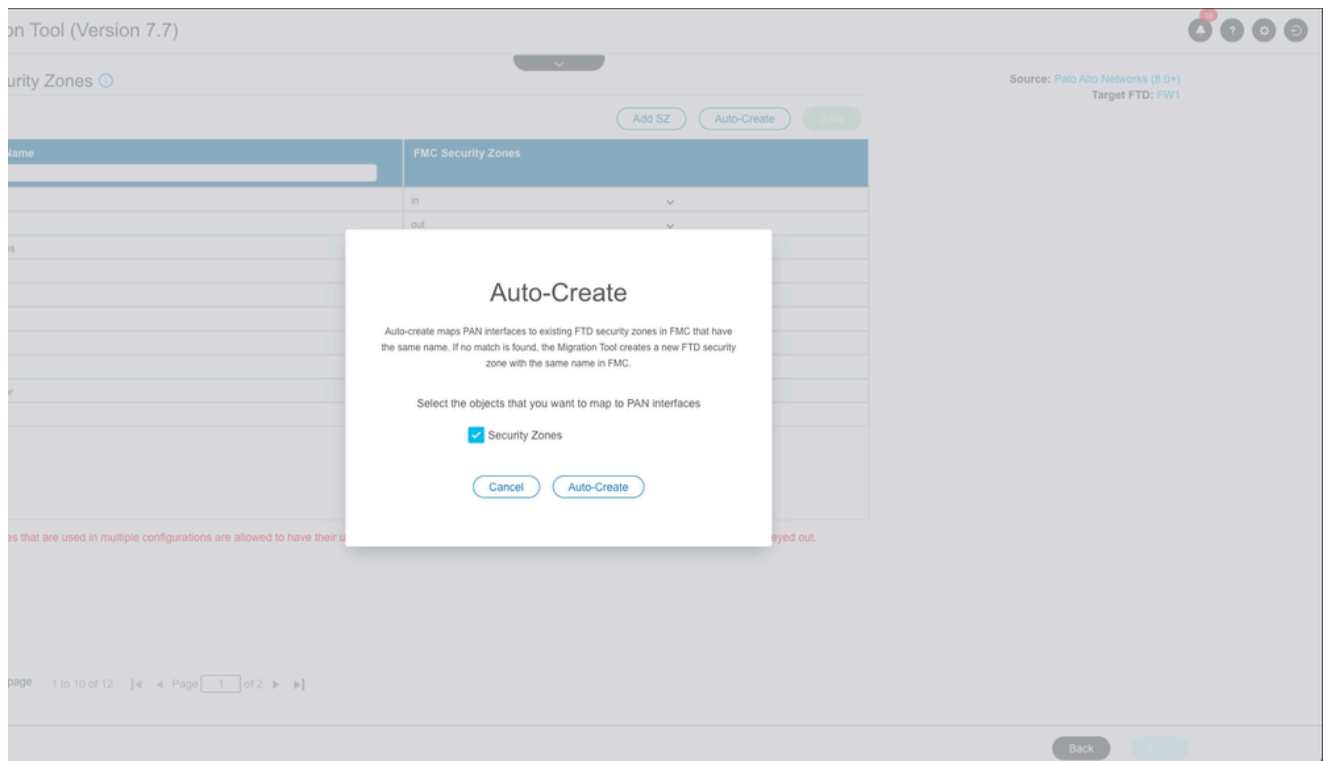
Security Zones	Type	Actions
DMZ	Select	
	SWITCHED	
	ROUTED	

0 - 0 of 0 |< 1 >|

Close

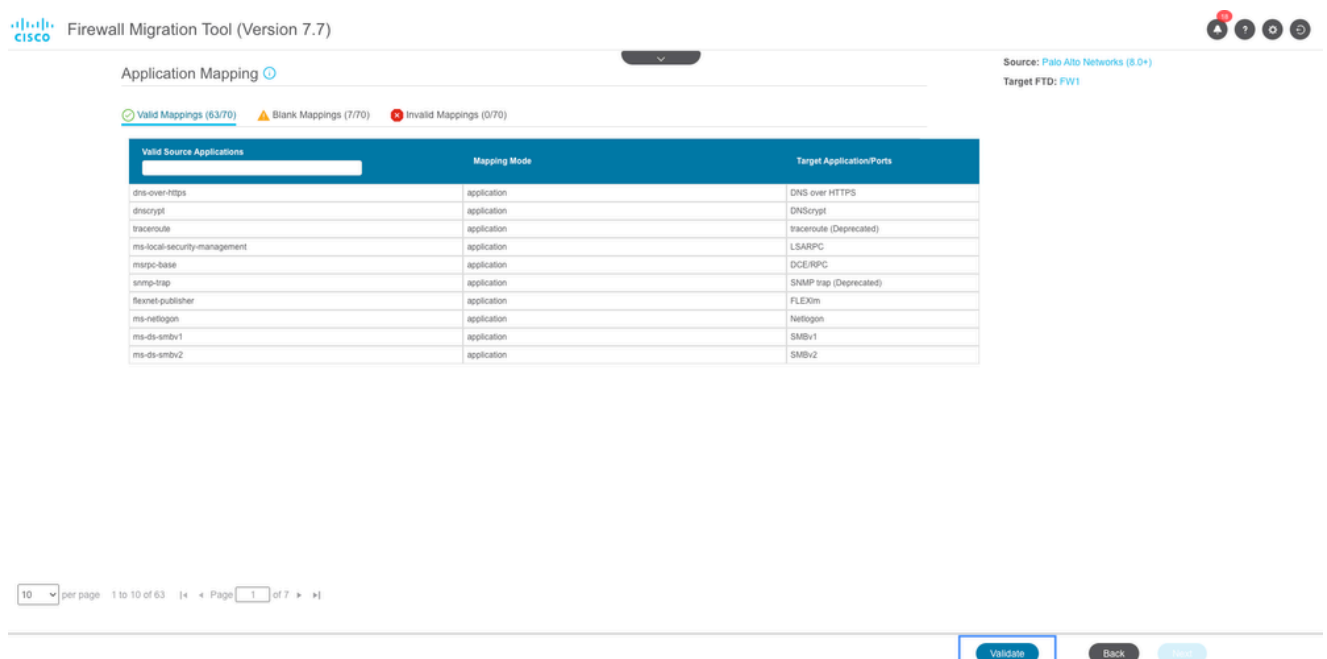
Manual Security Zone Creation

Auto Create Security Zones:



Auto Security Zone Creation

- You can now move on to Application Mapping section. Click on **Validate** button to validate the application mapping.



Application Mapping

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 page 1 to 10 of 63
1 of 7

Validate Back Next

Application Mapping Validation

Upon validation, FMT lists the Blank and invalid Mappings. **Invalid Mappings** must be corrected before proceeding further and correcting **Blank mappings** are optional.

Click **Validate** once again to validate the corrected mappings. Click **Next** after the validation is succeeded.

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	netmg-traceroute
snmp-trap	Port(s)	udp/162

10 per page 1 to 2 of 2
1 of 1

Validate Back Next

Blank & Invalid Application Mapping

- ACL can be optimized in the next section, if required. Review the configuration in each section such as Access control, Objects, NAT, Interfaces, Routes, and Remote Access VPN. Click on **Validate** after reveiwing the configurations.

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

Verify configuration in each section

Select all 195 entries Selected: 0 / 195

#	Name	Zone	SOURCE			Zone	DESTINATION		Port	Application	URLs	State	Action	TIME BASED
			Network	Port	User		Network	Port						
1	Allow Time	Dt	GRP_ADDR...	ANY	ANY			ANY	NTP	NA		✓	Allow	None
2	Allow Time	Dt	ANY	ANY	ANY			ANY	NTP	NA		✓	Allow	None
3	Allow Time	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			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			ANY	ANY	NA		✓	Allow	None
9	Allow ICM	Ot	ANY	ANY	ANY			ANY	netmg-traceroute	NA		✓	Allow	None
10	Allow ICM	Ot	ANY	ANY	ANY			ANY	ICMPv4	ANY	NA	✓	Allow	None
11	Allow DHCP	Ot	ANY	ANY	ANY			ANY	DHCP	NA		✓	Allow	None
12	Allow NetB	Ot	ANY	ANY	ANY			ANY	NetBIOS-ns, NetBIO...	NA		✓	Allow	None
13	Allow DNS	Ot	ANY	ANY	ANY			ANY	DNS	NA		✓	Allow	None

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

Optimise access control list and validate

Optimize ACL Validate

Configuration Validation

18. A validation summary is displayed after the validation is successfully completed. Click **Push Configuration** to push the configuration to the targeted FMC.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

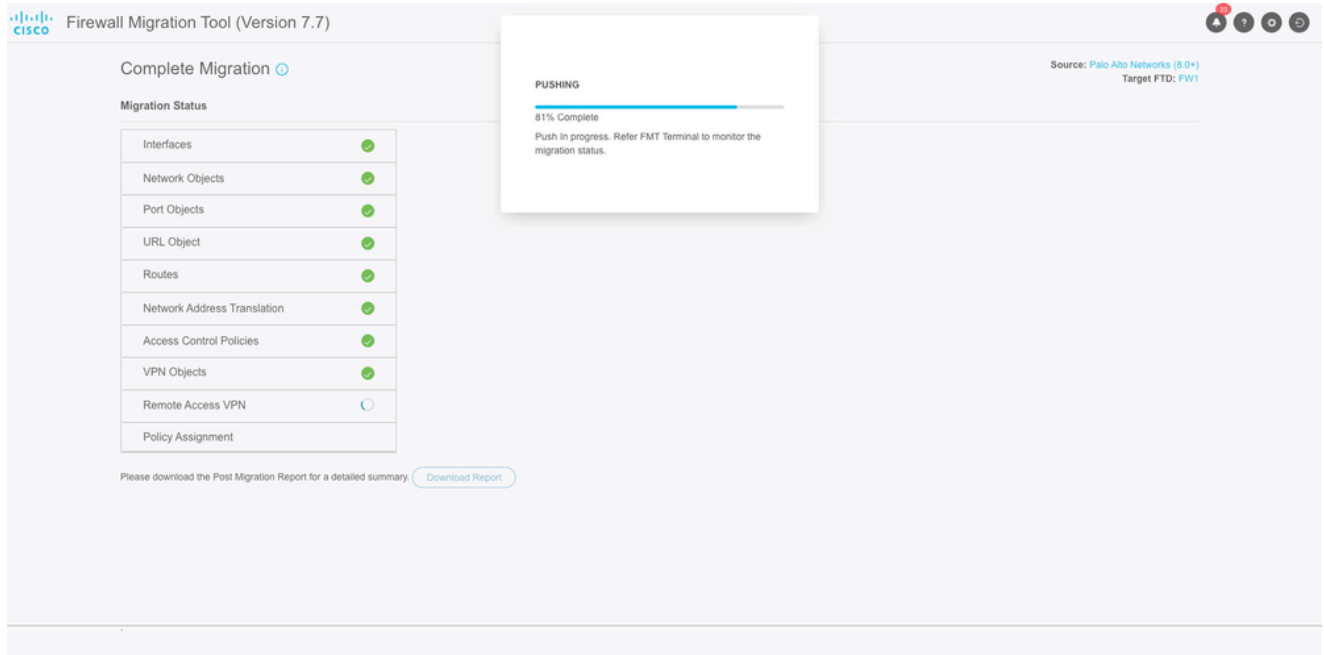
195 Access Control List Lines	752 Network Objects	100 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	62 Applications	9 Remote Access VPN (Global Protect Gateways)	

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

Push Configuration

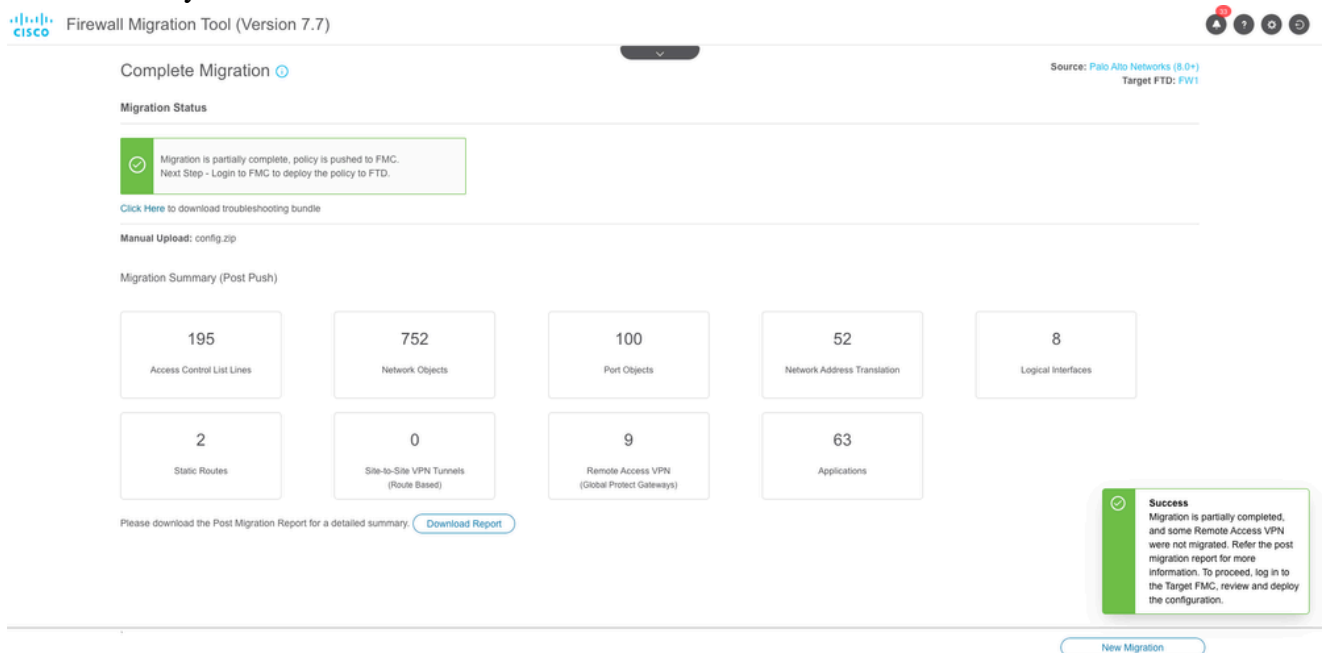
Configuration Validation Summary

19. Progress of configuration push to FMC is now visible in the Migration Status Section. You can use the **FMT terminal window** for monitoring the migration status as well.



Migration Status

20. A Migration Summary is displayed by the tool up on successful migration. It also lists out partially migrated configurations, if any. For example, Remote access VPN configuration in this scenario due to missing Secure Client Package.
- You can also download the **Post Migration Report** to review the migrated configurations as well as if there are any errors or corrections that are to be made.



Successful Migration Summary

21. The last step is to review the migrated configuration from FMC and **Deploy** the configuration to FTD. In order to deploy the configuration:
1. Log in to the FMC GUI.
 2. Navigate to the **Deploy** tab.
 3. Select the deployment to push configuration to the firewall.
 4. Click **Deploy**.

Troubleshoot

Troubleshooting Secure Firewall Migration Tool

Common migration failures:

- Unknown or invalid characters in the PaloAlto configuration file.
- Missing or incomplete configuration elements.
- Network connectivity issues or latency.
- Issues during PaloAlto configuration file upload or while pushing configuration to the FMC.

Using the Support Bundle for troubleshooting:

- On the "Complete Migration" screen, click the **Support** button.
- Select **Support Bundle** and choose the configuration files to download.
- **Log and DB** files are selected by default.
- Click **Download** to get a .zip file.
- Extract the .zip to view logs, DB, and configuration files.
- Click **Email us** to send failure details to the technical team.
- Attach the support bundle in your email.
- Click **Visit TAC page** to create a Cisco TAC case for assistance.