Seamless Transition: Migrating from Palo Alto Firewall to Cisco FTD

Contents

Introduction

This document describes the process of transitioning from a Palo Alto firewall to a Cisco FTD system by employing the FMT version 6.0.

Prerequisites

Requirements

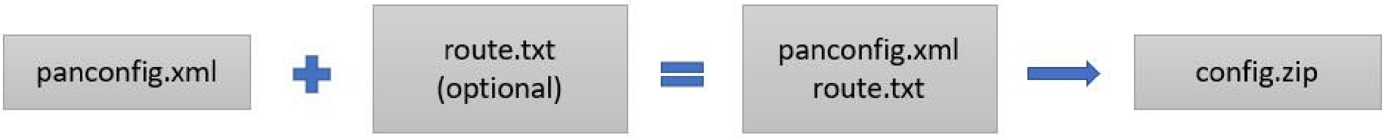
Cisco recommends that you have knowledge of these topics:

- Exporting the current running configuration from the Palo Alto firewall in XML format (***.xml**).
- Accessing the Palo Alto Firewall CLI and executing the **show routing route** command, then saving the output as a text file (***.txt**).
- Compressing both the configuration file (***.xml**) and the routing output file (***.txt**) into a single ZIP archive (***.zip**).

Components Used

The information in this document is based on Palo Alto Firewall version 8.4.x or later.

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.



panconfig.xml + route.txt (optional) = panconfig.xml route.txt → config.zip

Firepower Migration Tool (FMT)

The FMT aids engineering teams in the transition of any existing Vendor firewalls to Ciscos Next-Generation Firewall (NGFW)/Firepower Threat Defense (FTD). Ensure to operate the latest version of FMT, downloaded from the Cisco website.

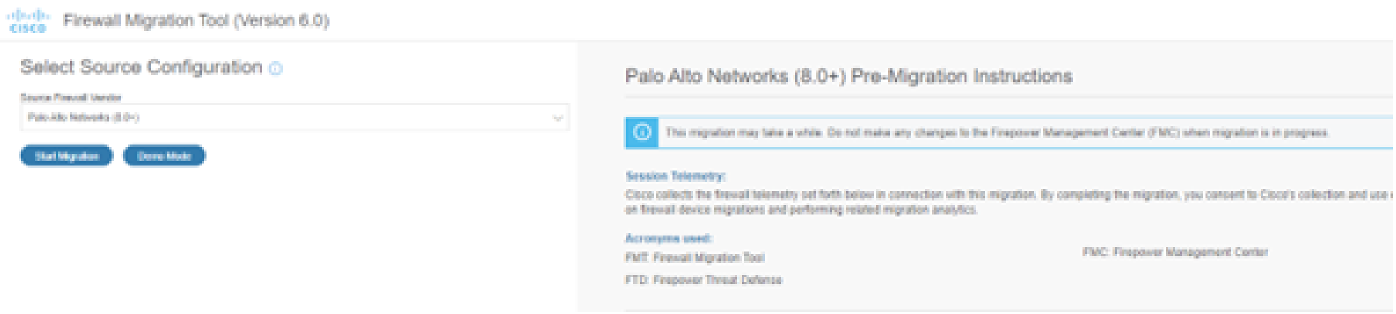
Migration Guideline

1. Pre-Migration Checklist

- Ensure the FTD has been added to the FMC before beginning the migration process.
- New user account with administrative privileges has been created on the FMC.
- Exported Palo Alto running configuration **file.xml** must be zipped with an extension of **.zip**.
- NGFW/FTD must have the same number of Physical or Sub-interface or Port-channel equals to Palo Alto Firewall interfaces.

2. Migration Tool Usage

- Download the FMT tool **.exe** and run as administrator.
- FMT will require CEC ID or cisco user account in order to log in.
- Post Successful login the tool will display a dashboard where you can choose firewall vendor and upload the corresponding ***.zip** file; refer to the next image.



Firewall Migration Tool (Version 6.0)
Select Source Configuration
Start Migration
Demo Mode

Source Firewall Vendor: Palo Alto Networks (8.0+)

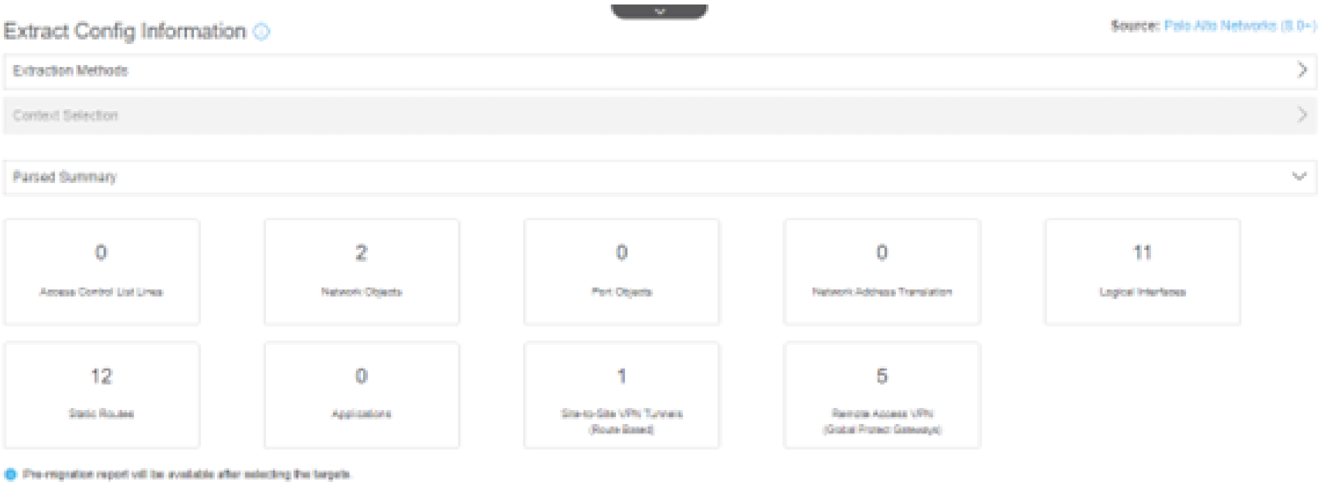
Palo Alto Networks (8.0+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firepower 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
on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool
FMC: Firepower Management Center
FTD: Firepower Threat Defense

- Review the instructions provided on the right-hand side carefully before proceeding with the migration.
- Click **Start Migration** once you are ready to begin.
- Upload the saved ***.zip** file that contains the configuration settings from your Palo Alto firewall.
- Once the configuration file is uploaded, you will be able to see a Parsed Summary of the contents and click **next**; refer to the next image.



Extract Config Information

Source: Palo Alto Networks (8.0+)

Extraction Methods

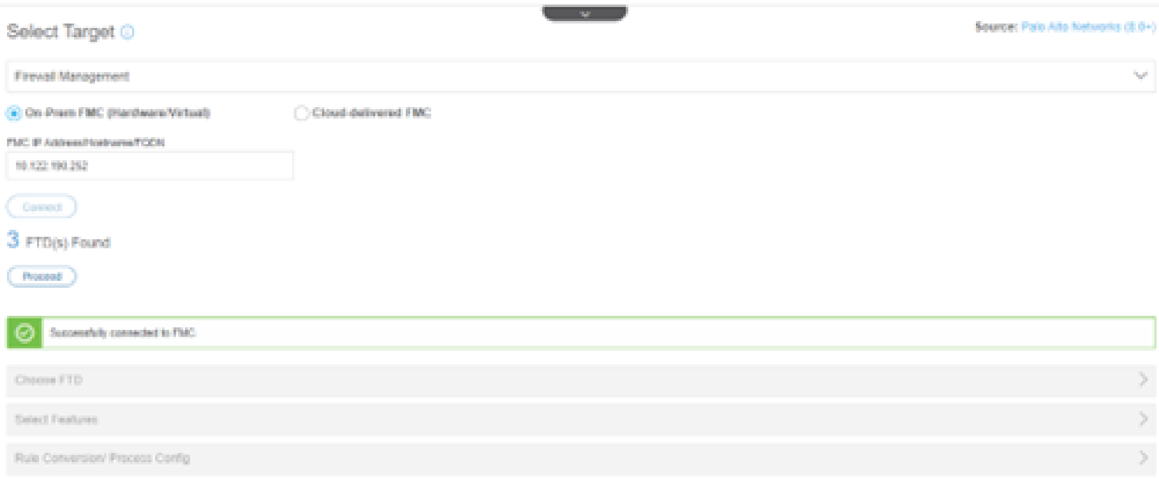
Context Selection

Parsed Summary

0 Access Control List Lines	2 Network Objects	0 Port Objects	0 Network Address Translation	11 Logical Interfaces
12 Static Routes	0 Applications	1 Site-to-Site VPN Tunnels (Route Based)	5 Remote Access VPN (Global Protect Gateways)	

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

- Enter the IP address of the FMC and log in.
- The tool will search for an active FTD that has been registered with the FMC.
- Choose the FTD you like to migrate and click **Proceed**, as shown in the next image.



Select Target

Source: Palo Alto Networks (8.0+)

Firewall Management

● On-Prem FMC (Hardware/Virtual) ○ Cloud-delivered FMC

FMC IP Address/Hostname/FQDN

10.122.190.252

3 FTD(s) Found

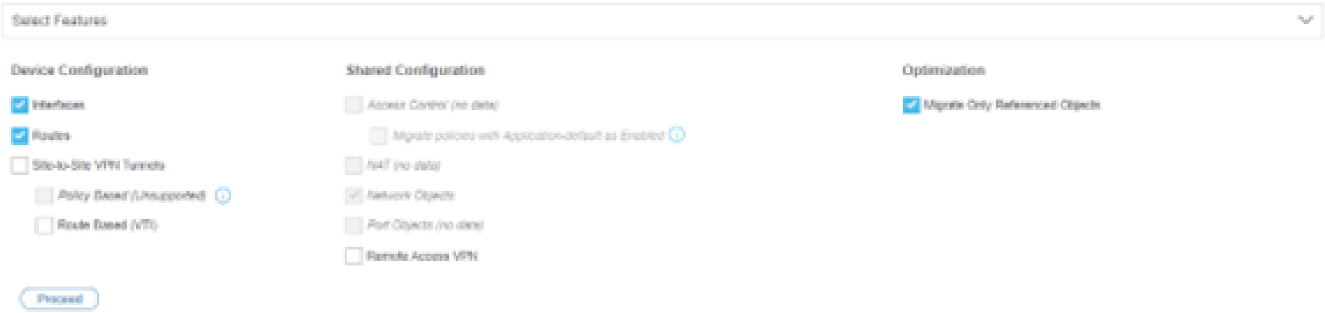
Successfully connected to FMC

Choose FTD

Select Features

Rule Conversion/ Process Config

- Choose the specific features in order to migrate based on the requirements of the customer. Note that Palo Alto firewalls have a different feature set compared to FTD.
- Click **Proceed** and consult the next image for reference.



Select Features

Device Configuration

☑ Interfaces

☑ Routes

□ Site-to-Site VPN Tunnels

□ Policy Based (Unsupported)

□ Route Based (VTI)

Shared Configuration

□ Access Control (no data)

□ Migrate policies with Application-default as Enabled

□ NAT (no data)

☑ Network Objects

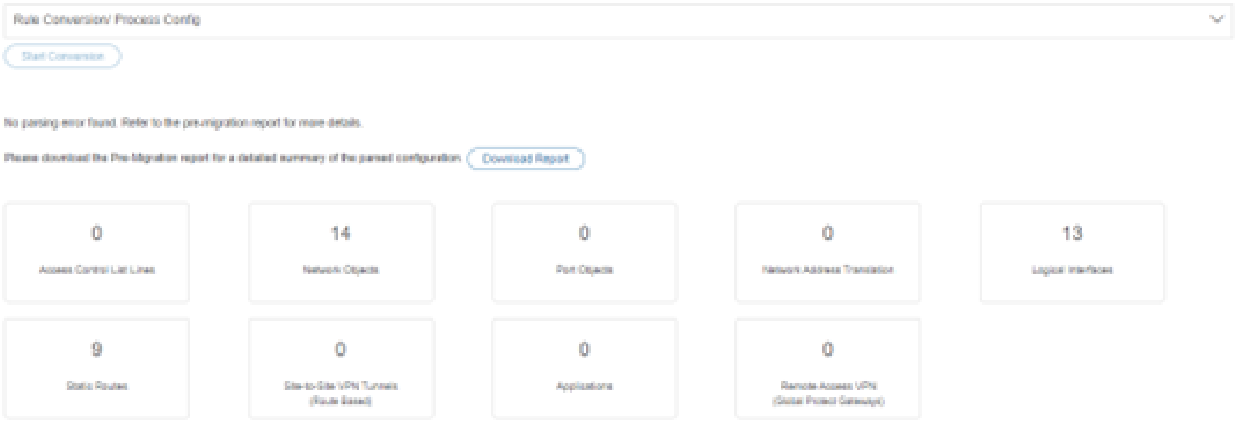
□ Port Objects (no data)

□ Remote Access VPN

Optimization

☑ Migrate Only Referenced Objects

- The FMT will execute the conversion according to your selections. Review the changes in the Pre-Migration Report, then click **Proceed**. See the next image for guidance.



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.

0 Access Control List Lines

14 Network Objects

0 Port Objects

0 Network Address Translation

13 Logical Interfaces

9 Static Routes

0 Site-to-Site VPN Tunnels (Route Based)

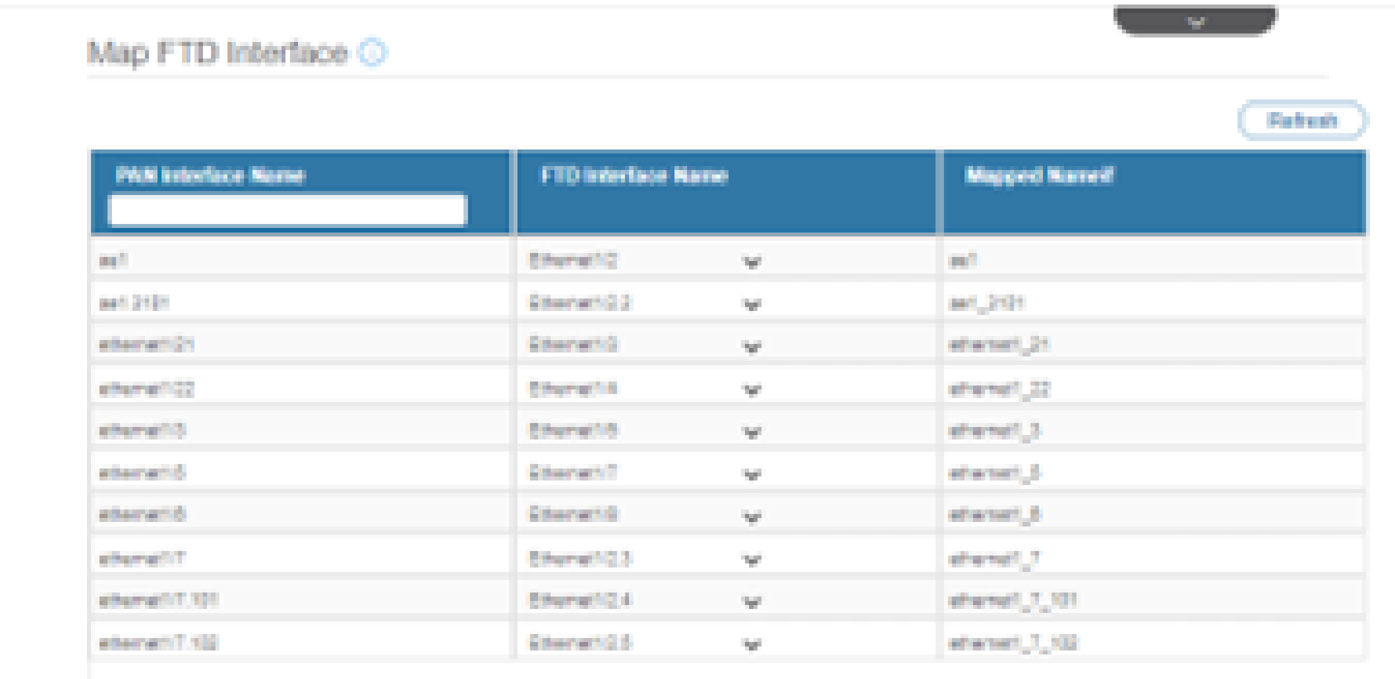
0 Applications

0 Remote Access VPN (Global Protect Gateways)

- Map the interfaces from the Palo Alto firewall to those on the FTD. Refer to the next image for details.

Note: NGFW/FTD must have same number of Physical or Sub-interface or Port-channel equals to

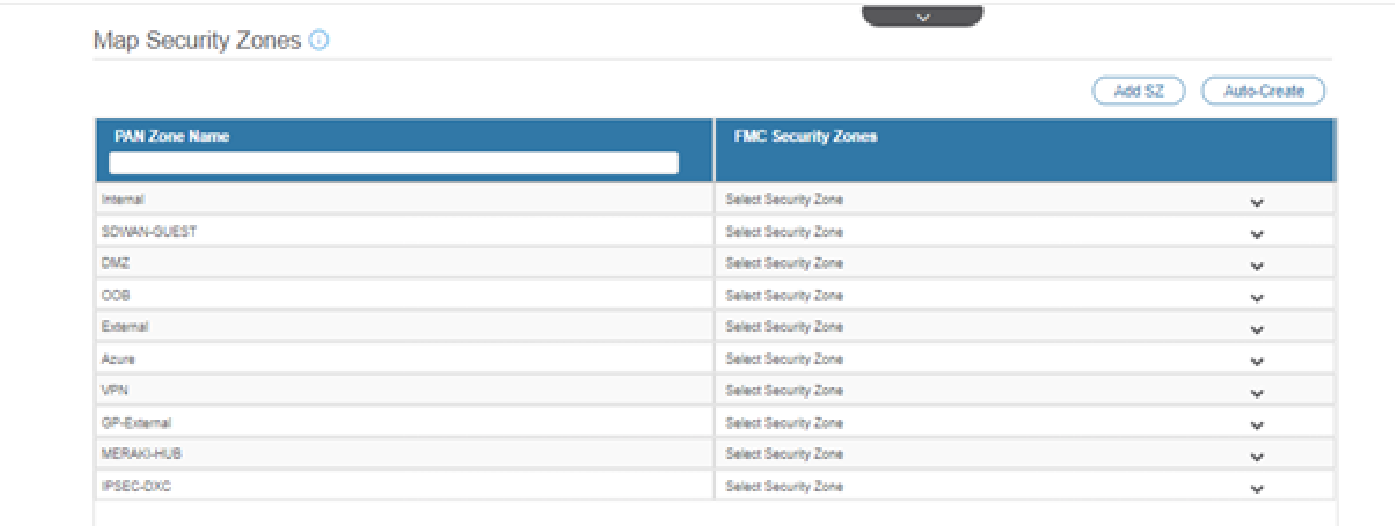
Palo Alto Firewall interfaces including Sub-interfaces.



Map FTD Interface

PAN Interface Name	FTD Interface Name	Mapped Name#
ae1	Ethernet1/2	ae1
ae1.2101	Ethernet1/2.2	ae1_2101
ethernet1/21	Ethernet1/3	ethernet1_21
ethernet1/22	Ethernet1/4	ethernet1_22
ethernet1/3	Ethernet1/5	ethernet1_3
ethernet1/5	Ethernet1/7	ethernet1_5
ethernet1/6	Ethernet1/6	ethernet1_6
ethernet1/7	Ethernet1/2.3	ethernet1_7
ethernet1/7.101	Ethernet1/2.4	ethernet1_7_101
ethernet1/7.102	Ethernet1/2.5	ethernet1_7_102

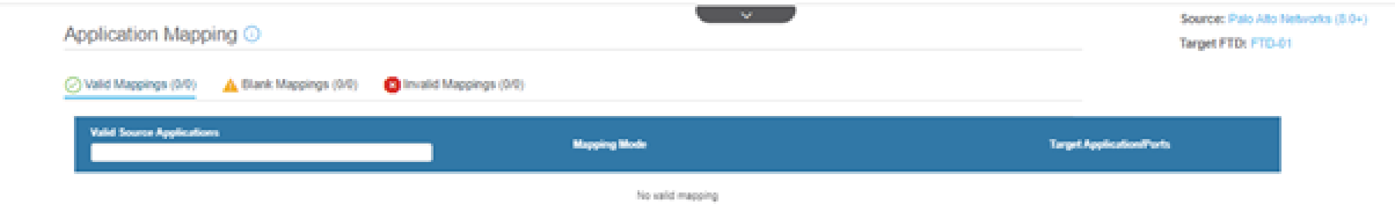
- Determine the mapping for Zones, which can either be done manually or by using the Auto-create feature. For visualization, refer to the next image.



Map Security Zones

PAN Zone Name	FMC Security Zones
Internal	Select Security Zone
SDWAN-GUEST	Select Security Zone
DMZ	Select Security Zone
OOB	Select Security Zone
External	Select Security Zone
Azure	Select Security Zone
VPN	Select Security Zone
GP-External	Select Security Zone
MERAKI-HUB	Select Security Zone
IPSEC-DXC	Select Security Zone

- Assign your application blocking profile. As this is a lab device without application mapping, you can continue with the default settings can be continued. Click **Next**, and refer to the image provided.



Application Mapping

Source: Palo Alto Networks (8.0+)

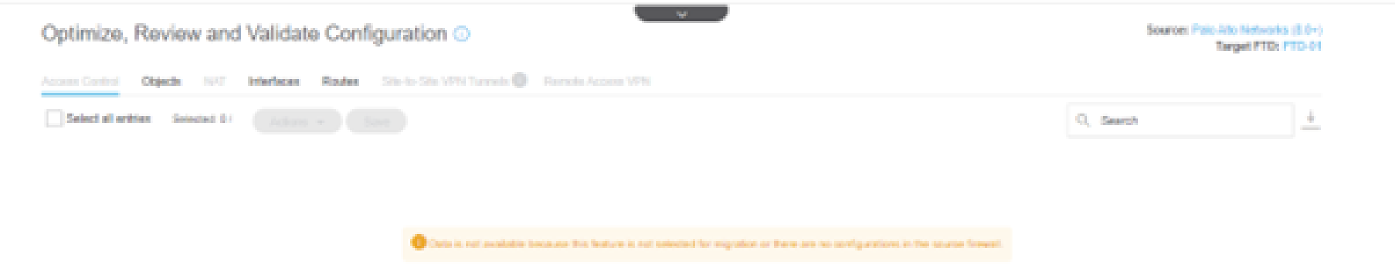
Target FTD: FTD-01

Valid Mappings (0/0) | Blank Mappings (0/0) | Invalid Mappings (0/0)

Valid Source Applications	Mapping Mode	Target Application/Ports

No valid mapping

- Optimize ACLs, objects, interfaces, and routes as needed. Since this is a lab setup with minimal configurations, you can proceed with the default options. Then click **Validate**, referencing the next image.



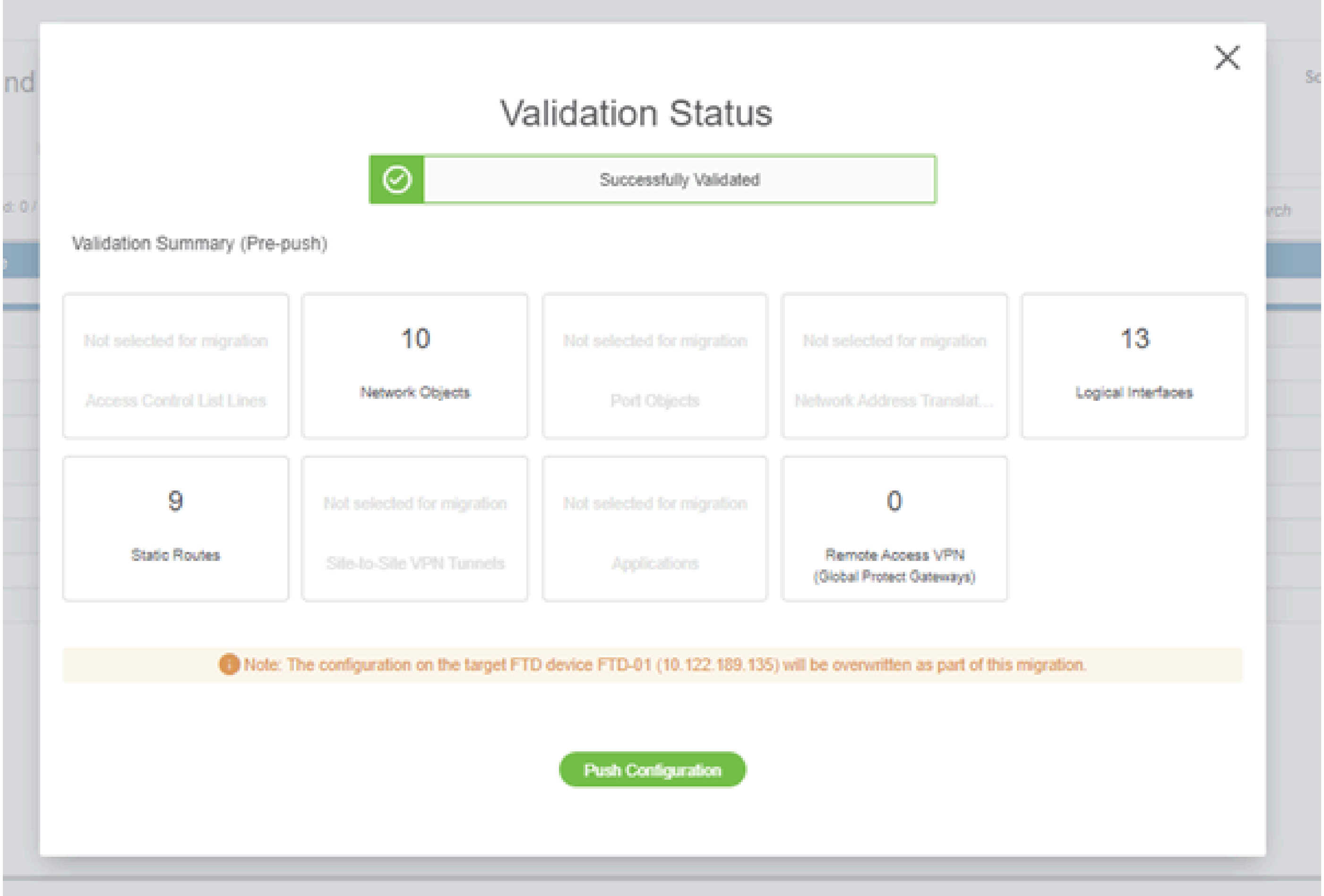
Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)

Target FTD: FTD-01

Data is not available because this feature is not selected for migration or there are no configurations in the source firewall.

- Following successful validation, the configuration is ready to be deployed to the targeted FTD. See the next image for further instructions.



Validation Status

Successfully Validated

Validation Summary (Pre-push)

Not selected for migration
Access Control List Lines

10
Network Objects

Not selected for migration
Port Objects

Not selected for migration
Network Address Translat...

13
Logical Interfaces

9
Static Routes

Not selected for migration
Site-to-Site VPN Tunnels

Not selected for migration
Applications

0
Remote Access VPN
(Global Protect Gateways)

Note: The configuration on the target FTD device FTD-01 (10.122.189.135) will be overwritten as part of this migration.

Push Configuration

- The Push Configuration will save the migrated configurations in FMC and will be deployed to the FTD automatically.
- In case of any issue while migrating, feel free to open a TAC case for further assistance.

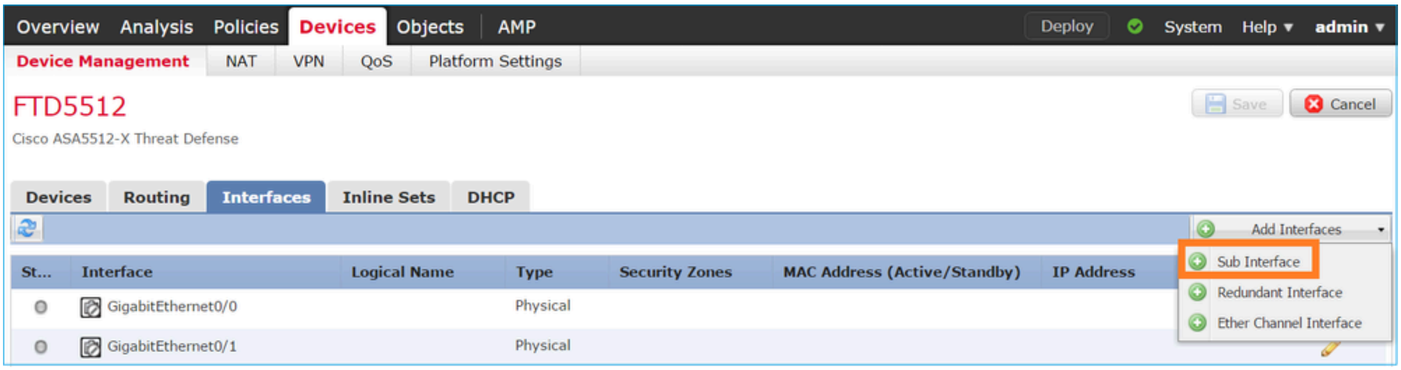
3. Post - Migration Validation

- Validating the configuration on the FTD and FMC.
- Testing the device ACLs, Policy, Connectivity, and other Advanced features.
- Create a rollback point before performing any changes.
- Testing the migration in the lab environment before Go-Live in the Production environment.

Known Issues

1. Missing Interfaces on FTD

- Login to Palo Alto CLI and execute the **show interface all**. You must have equal or more than the number of interfaces in FTD.
- Create the equal or more number of interfaces - either sub-interface, Port-channel, or Physical interface via FMC GUI.
- Navigate to **FMC GUI Device** > **Device Management**, click the FTD in which the required interface is to be created. Under Interface section, from the right corner dropdown menu choose **Create Sub-interface/BVI** accordingly and create the interface and associate corresponding interfaces. Save the configuration and sync to the device.



FTD5512

Cisco ASA5512-X Threat Defense

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
○	GigabitEthernet0/0		Physical			
○	GigabitEthernet0/1		Physical			

- Verify that interfaces are created on FTD by executing **Show interface ip brief** and proceed with migration for interface mapping.

2. Routing Table

- Verify the routing table on Palo Alto firewall by executing Show routing route or Show routing route summary.
- Before migrating the routes to FTD, verify the table and choose the required routes as per the project need.
- Vaildate the same routing table in the FTD by Show route all and show route summary.

3. Optimize

- Optimizing objects panel greyed out, sometimes you must create a manual object in FMC and map it. In order to view the object in **FTD**, use **Show Running | in objects** and in Palo Alto, use **Show address <object name>**.
- Application Migration requires an Audit of Palo Alto firewall before the migration, FTD has dedicated IPS device or you can enable the feature in FTD so you need to plan the application migration task as per customer requirement.
- NAT Configuration of Palo Alto firewall must be verified by **show running nat-policy** and you must have a custom NAT policy in FTD, which can be viewed in FTD by **Show Running nat**.

Conclusion

The Palo Alto firewall has been successfully migrated to Cisco FTD with the help of FMT. In case of any issue post migration on FTD and for troubleshooting further open a TAC case.