

Migre de Paloalto a Firepower Threat Defence mediante FMT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Antecedentes](#)

[Obtener archivo zip de configuración de firewall de Paloalto](#)

[Lista de comprobación previa a la migración](#)

[Configurar](#)

[Pasos de migración](#)

[Troubleshoot](#)

[Solución de problemas de Secure Firewall Migration Tool](#)

[Fallos de migración habituales:](#)

[Uso del paquete de soporte para la resolución de problemas:](#)

Introducción

Este documento describe el procedimiento para migrar Paloalto Firewall a Cisco Firepower Threat Device .

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Herramienta de migración de Firepower
- Firewall Paloalto
- Protección frente a amenazas de firewall (FTD)
- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Mac OS con Firepower Migration Tool (FMT) v7.7
- NGFW PAN versión 8.0+
- Secure Firewall Management Center (FMCv) v7.6

- Secure Firewall Threat Defence versión 7.4.2

Descargo: Las redes y direcciones IP a las que se hace referencia en este documento no están asociadas a usuarios, grupos u organizaciones individuales. Esta configuración se ha creado exclusivamente para su uso en un entorno de laboratorio.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Los requisitos específicos para este documento incluyen:

- PAN NGFW versión 8.4+ o posterior
- Secure Firewall Management Center (FMCv) versión 6.2.3 o posterior

La herramienta de migración de firewalls admite esta lista de dispositivos:

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) con FPS
- Administrador de dispositivos de firewall seguro de Cisco (7.2+)
- Check Point (r75-r77)
- Check Point (r80-r81)
- Fortinet (más de 5,0)
- Palo Alto Networks (8.0+)

Antecedentes

Antes de migrar la configuración de Palo Alto Firewall, ejecute estas actividades:

Obtener archivo zip de configuración de firewall de Palo Alto

- El firewall Palo Alto debe ser de la versión 8.4+.
- Exporte la configuración en ejecución actual desde el firewall de Palo Alto (*.xml debe estar en formato xml).
- Inicie sesión en Palo Alto Firewall Cli para ejecutar show routing route y guardar el resultado en formato txt (*.txt).
- Comprima el archivo de configuración en ejecución (*.xml) y el archivo de enrutamiento (*.txt) con la extensión *.zip.

Lista de comprobación previa a la migración

- Asegúrese de que el FTD se ha registrado en el FMC antes de comenzar el proceso de

migración.

- Se ha creado una nueva cuenta de usuario con privilegios administrativos en el FMC. También se pueden utilizar las credenciales de administrador existentes.
- El archivo de configuración en ejecución de Palo Alto exportado.xml debe comprimirse con una extensión de .zip (siga el procedimiento mencionado en la sección anterior).
- El dispositivo Firepower debe tener el mismo número o más de interfaces físicas, subinterfaces o canales de puerto en comparación con las interfaces de firewall Paloalto.

Configurar

Pasos de migración

1. Descargue la herramienta de migración de Firepower más reciente de Cisco Software Central que sea compatible con su ordenador:

The screenshot shows the Cisco Software Central interface for downloading the Secure Firewall Migration Tool (FMT) version 7.7.0. The page title is "Software Download" and the breadcrumb trail is "Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0".

On the left, there is a search bar and a filter menu. The filter menu is set to "Latest Release" and shows "7.7.0" as the selected version, with "All Release" and "7" as other options.

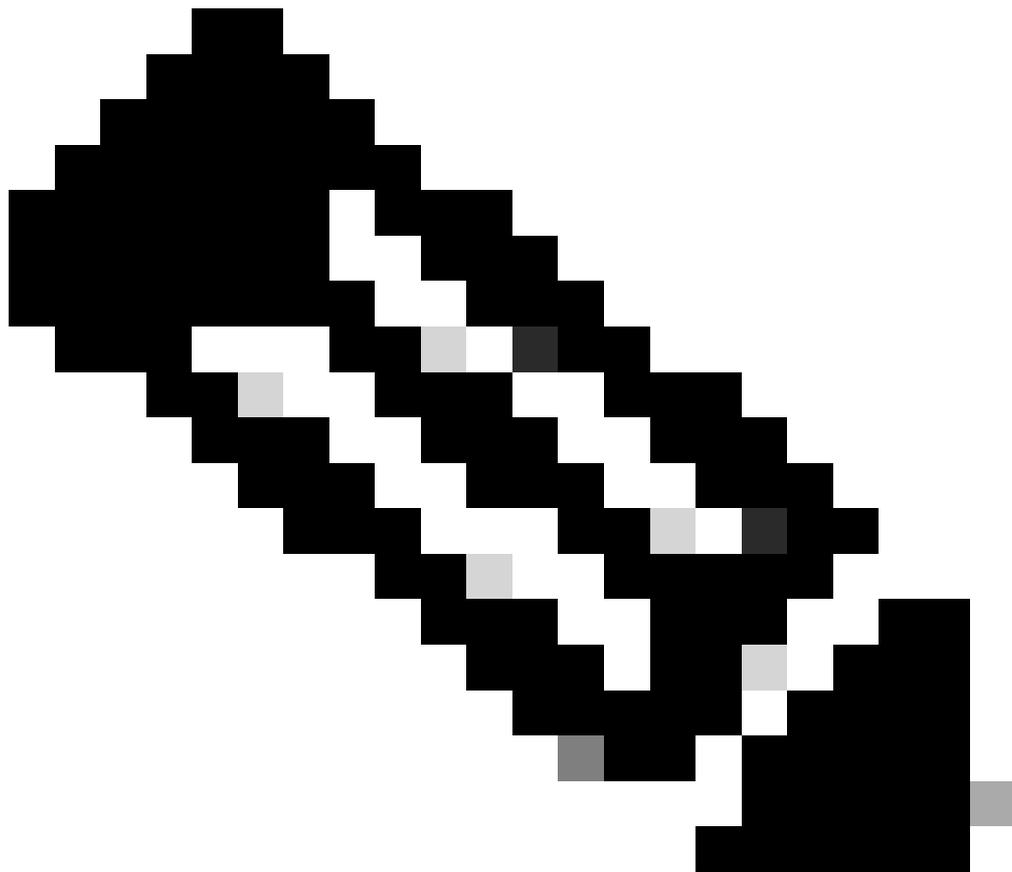
The main content area displays the "Secure Firewall Migration Tool" for "Release 7.7.0". It includes a "My Notifications" button and a section for "Related Links and Documentation" with links for "Open Source", "Release Notes for 7.7.0", and "Install and Upgrade Guides".

Below this, there is a table with the following data:

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	↓ 🛒
Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7-12208.exe Advisories	03-Feb-2025	69.54 MB	↓ 🛒

Descarga de FMT

3. Abra el archivo que descargó anteriormente en el equipo.



Nota: El programa se abre automáticamente y una consola genera automáticamente contenido en el directorio en el que se ejecutó el archivo.

-
4. Después de ejecutar el programa, se abre un navegador web que muestra el Acuerdo de licencia del usuario final.
 1. Active la casilla de verificación para aceptar los términos y condiciones.
 2. Haga clic en Continuar.
 5. Inicie sesión con credenciales de CCO válidas para acceder a la GUI de FMT.



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

Mensaje de inicio de sesión FMT

6. Seleccione Source Firewall para migrar y haga clic en Start Migration.

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor
Palo Alto Networks (8.0+)

Start Migration Demo Mode

Palo Alto Networks (8.0+) Pre-Migration Instructions

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:
FMT: Firewall Migration Tool FMC: Firewall Management Center
FTD: Firewall Threat Defense

Before you begin your Palo Alto Networks (PAN) to Firewall Threat Defense migration, you must have the following items:

- Stable IP Connection:**
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.
- Palo Alto Networks Configuration Requirements:**
Export named configuration snapshot file from palo alto firewall to .xml format. If your NAT has polices with the same source and destination zone, then

GUI de FMT

7. Ahora se muestra la sección Métodos de extracción, donde debe cargar el archivo de configuración Zip de Paloalto Firewall al FMT.

Firewall Migration Tool (Version 7.7)

Extract Config Information

Extraction Methods

Manual Configuration Upload
The configuration file must be a zip file consisting of the following:

- Zip Config file derived from the PAN Tool.

Upload

Context Selection >

Parsed Summary >

Extract Config Information

Extraction Methods

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

- Zip Config

Downloads

config.zip

Asistente de carga de configuración

8. El resumen de configuración analizada se muestra ahora después de cargar el archivo de configuración. En el caso de VSYS, hay disponibles selecciones de VSYS independientes.

Cada uno de ellos debe ser analizado y migrado uno tras otro.
Valide el resumen analizado y haga clic en el icono Next.

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

Resumen de validación de configuración

9. En esta sección puede elegir el tipo de CSP. Proporcione la dirección IP de administración y haga clic en Connect.

Aparecerá una ventana emergente en la que se le solicita que proporcione las credenciales de FMC. Ingrese las credenciales y haga clic en 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

Conexión a FMC

10. Una vez que se haya conectado correctamente a FMC, ahora puede elegir el dominio (si lo hubiera) y hacer clic en Proceed.

Select Target ⓘ Source: Palo Alto Networks (8.0+)

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

Selección de dominio

11. Elija el FTD al que va a migrar y haga clic en Proceed.

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 ⌵

Select FTD Device
 Proceed without FTD

FW1 (10.105.209.80) - NA (R) ⌵

[Proceed](#)

Select Features ➤

Rule Conversion/ Process Config ➤

Seleccionar FTD de destino

12. La herramienta ahora enumera las funciones que se van a migrar. Haga clic en Proceed.

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

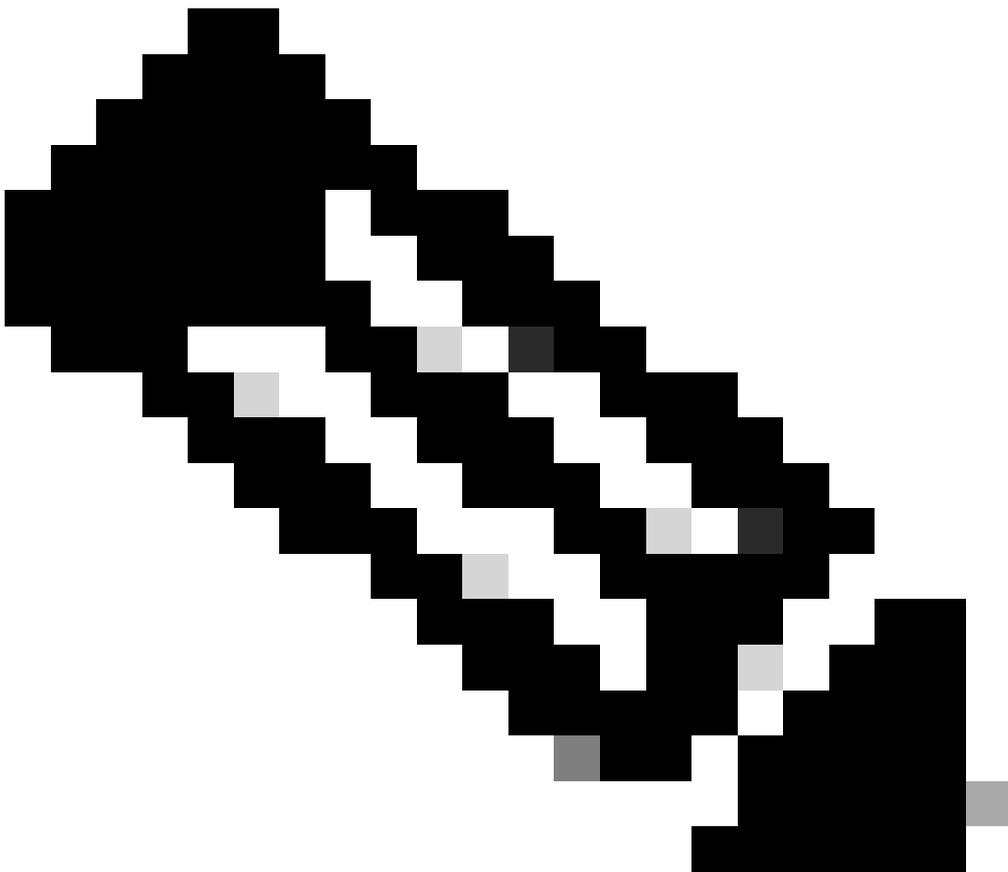
Select Features ⌵

<p>Device Configuration</p> <p><input checked="" type="checkbox"/> Interfaces</p> <p><input checked="" type="checkbox"/> Routes</p> <p><input checked="" type="checkbox"/> Site-to-Site VPN Tunnels</p> <p><input type="checkbox"/> Policy Based (Unsupported) ⓘ</p> <p><input checked="" type="checkbox"/> Route Based (VTI)</p>	<p>Shared Configuration</p> <p><input checked="" type="checkbox"/> Access Control</p> <p><input type="checkbox"/> Migrate policies with Application-default as Enabled ⓘ</p> <p><input checked="" type="checkbox"/> Network Objects</p> <p><input checked="" type="checkbox"/> Port Objects</p> <p><input checked="" type="checkbox"/> Remote Access VPN</p>	<p>Advanced Configuration</p> <p>Optimization</p> <p><input checked="" type="checkbox"/> Migrate Only Referenced Objects</p> <p>Access Control Options</p> <p><input checked="" type="checkbox"/> Discovered Identities ⌵ ⓘ</p>
---	--	--

[Proceed](#)

Rule Conversion/ Process Config ➤

Selección de funciones



Nota: Todas las funciones están seleccionadas de forma predeterminada. Puede anular la selección de cualquier configuración que no se vaya a migrar.

13. Haga clic en Start Conversion para convertir la configuración.



Configuración de análisis

La herramienta analiza la configuración y muestra el resumen de conversión como se muestra en la imagen. También puede descargar el informe previo a la migración para validar la configuración migrada en busca de errores o advertencias, si los hubiera. Vaya a

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

Back Next

Resumen de configuración analizada

14. Puede definir la asignación de interfaz de Paloalto a FTD, así como editar el nombre de interfaz de cada interfaz en la sección Asignación de interfaz. Haga clic en Next después de que se complete la Asignación de interfaz.

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	✓ Ethernet1/1	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

Mapeo de interfaz

15. Puede Agregar la Zona de Seguridad manualmente para cada interfaz o Crear Automáticamente en la sección Asignar la Zona de Seguridad . Haga clic en Next después de crear y asignar zonas de seguridad.

Map Security Zones

PAN Zone Name	FMC Security Zones
G...-Inside	Select Security Zone
Outside	Select Security Zone
GP/PA-	Select Security Zone
I...Ine	Select Security Zone
DMZ	Select Security Zone
I...C	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
I...-Inside	Select Security Zone

Add SZ Auto-Create Save

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

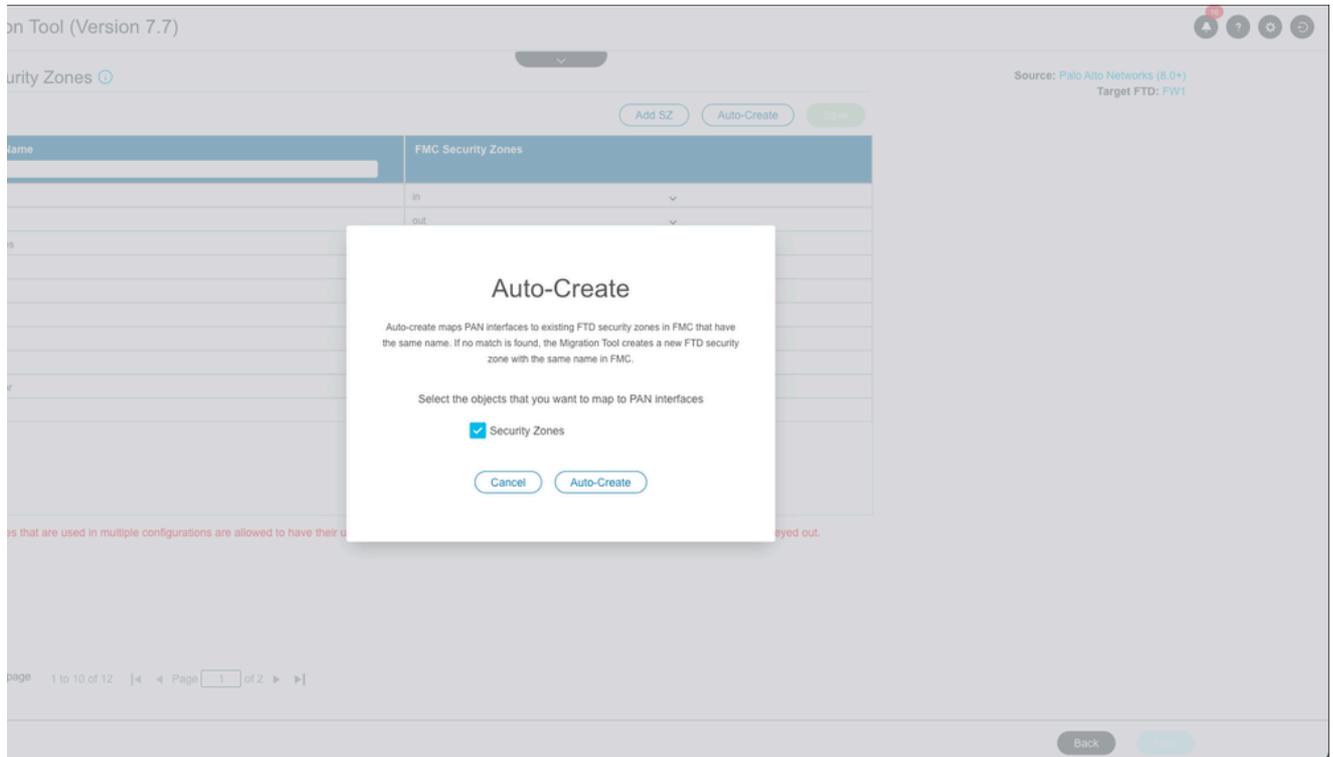
Creación de zonas de seguridad

Creación manual de zonas de seguridad:

The screenshot shows a modal window titled "Add SZ" with a close button (X) in the top right. Below the title, there is a "Security Zones (SZ)" section with an "Add" button and a character limit warning: "Max 48 characters for zone name. Allowed special characters are _-+*". The main form has three columns: "Security Zones" with a text input containing "DMZ", "Type" with a dropdown menu showing "ROUTED" selected, and "Actions" with a red 'X' and a green checkmark. At the bottom, there is a "Close" button and a pagination indicator "0 - 0 of 0 | Page 1 of 2".

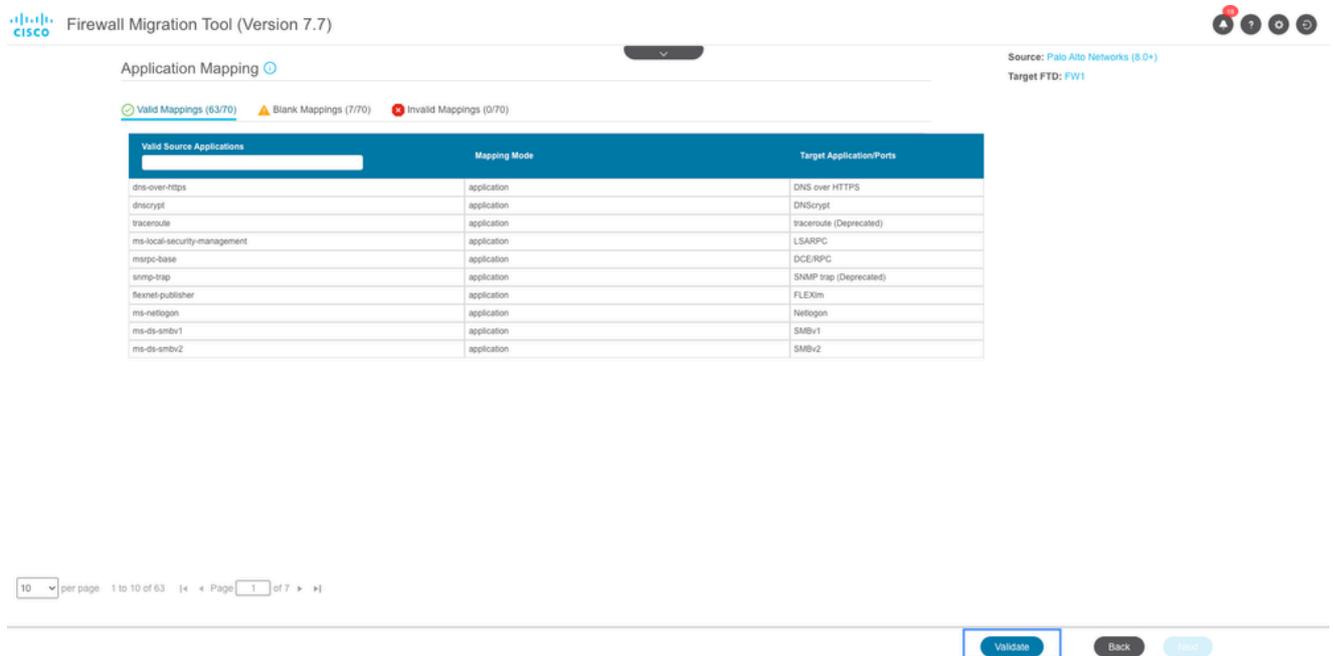
Creación manual de zonas de seguridad

Creación automática de zonas de seguridad:



Creación automática de zonas de seguridad

16. Ahora puede pasar a la sección Asignación de aplicaciones. Haga clic en el botón Validar para validar la asignación de la aplicación.



Asignación de aplicaciones

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-securitymanagement	application	LSARPC
mrpc-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXim
ms-netlogon	application	Netlogon
ms-ds-smbv1	application	SMBv1
ms-ds-smbv2	application	SMBv2

10 per page 1 to 10 of 63 | Page 1 of 7

Validate Back Next

Validación de asignación de aplicaciones

Tras la validación, FMT muestra las asignaciones en blanco y no válidas. Las asignaciones no válidas deben corregirse antes de continuar y la corrección de asignaciones en blanco es opcional.

Haga clic en Validar una vez más para validar las asignaciones corregidas. Haga clic en Next después de que la validación se haya realizado correctamente.

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 | Page 1 of 1

Validate Back Next

Asignación de aplicación en blanco e no válida

- Si es necesario, se puede optimizar la ACL en la siguiente sección. Revise la configuración en cada sección, como Control de acceso, Objetos, NAT, Interfaces, Rutas y VPN de acceso remoto. Haga clic en Validar después de revisar las configuraciones.

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

#	Name	SOURCE					DESTINATION					Application	URLs	State	Action	TIME BASED
		Zone	Network	Port	User	Zone	Network	Port								
1	Allow Tm...	Dc	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None			
2	Allow Tm...	Df	ANY	ANY	ANY			ANY	NTP	NA	✓	Allow	None			
3	Allow Tm...	Df	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None			
4	Allow DNS	Df	ANY	ANY	ANY			ANY	DNS, DNSCrypt, DN...	NA	✓	Allow	None			
5	Allow DNS	O	ANY	ANY	ANY	Inside		ANY	DNS	NA	✓	Allow	None			
6	Allow API	Dc	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	ANY	NA	✓	Allow	None		
9	Allow ICM	O	ANY	ANY	ANY	Inside		ANY	netmg-traceroute	NA	✓	Allow	None			
10	Allow ICM	O	ANY	ANY	ANY	Inside		ICMPv4	ANY	NA	✓	Allow	None			
11	Allow DHC	O	ANY	ANY	ANY	Inside		ANY	DHCP	NA	✓	Allow	None			
12	Allow NetE	O	ANY	ANY	ANY	Inside		ANY	NetBIOS-ns, NetBIO...	NA	✓	Allow	None			
13	Allow DNS	O	ANY	ANY	ANY	Inside		ANY	DNS	NA	✓	Allow	None			

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

Optimize access control list and validate

Optimize ACL Validate

Validación de configuración

18. Se muestra un resumen de validación después de que la validación se haya completado correctamente. Haga clic en Push Configuration para enviar la configuración al FMC de destino.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

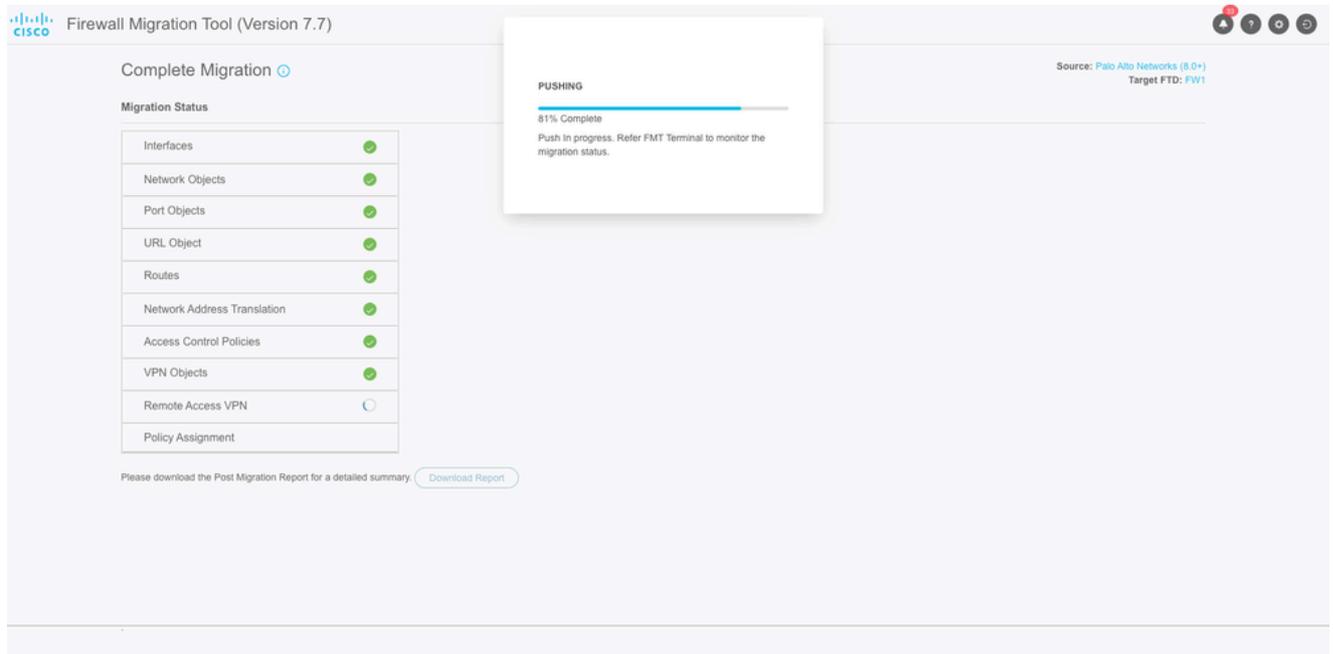
195	752	100	52	8
Access Control List Lines	Network Objects	Port Objects	Network Address Translation	Logical Interfaces
2	0	62	9	
Static Routes	Site-to-Site VPN Tunnels (Route Based)	Applications	Remote Access VPN (Global Protect Gateways)	

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

Push Configuration

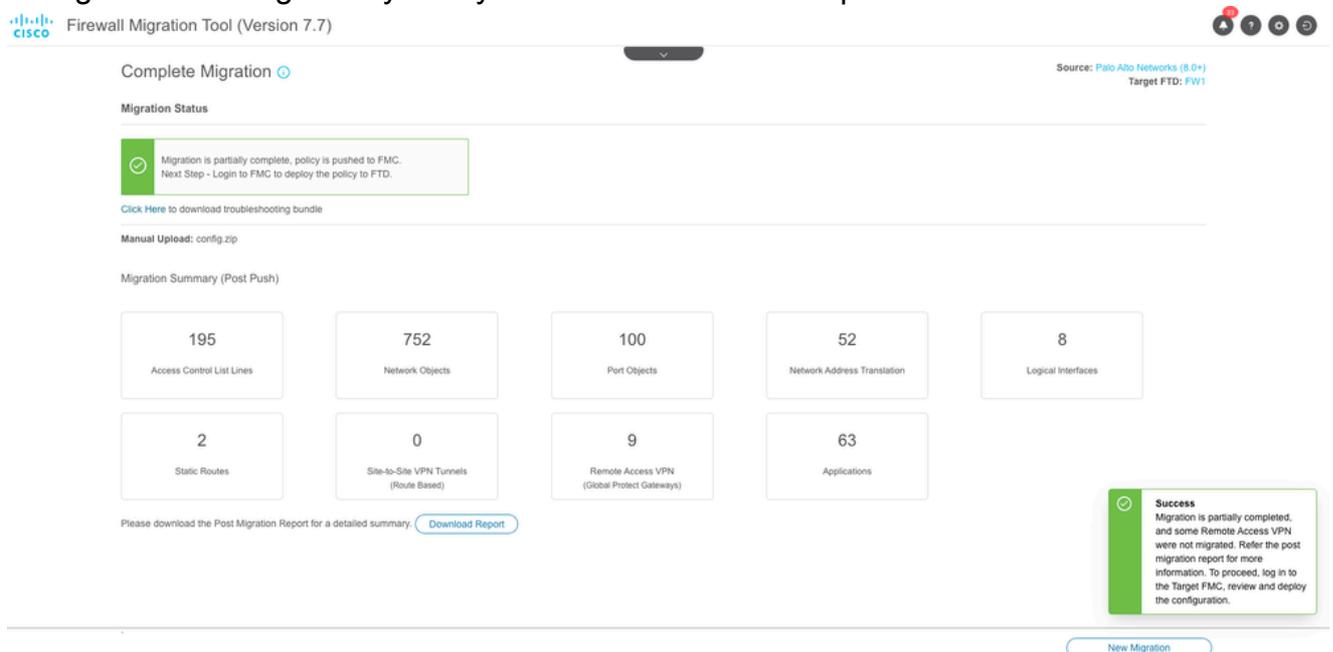
Resumen de validación de configuración

19. El progreso de la transferencia de la configuración a FMC se puede ver ahora en la sección Estado de la migración. También puede utilizar la ventana de terminal FMT para monitorear el estado de la migración.



Estado de migración

20. La herramienta mostrará un resumen de la migración cuando la migración se haya realizado correctamente. También muestra las configuraciones migradas parcialmente, si las hubiera. Por ejemplo, la configuración de VPN de acceso remoto en este escenario debido a la falta del paquete de cliente seguro. También puede descargar el informe posterior a la migración para revisar las configuraciones migradas y si hay errores o correcciones que deban realizarse.



Resumen de migración correcta

21. El último paso es revisar la configuración migrada desde FMC e implementar la configuración en FTD.
- Para implementar la configuración:
1. Inicie sesión en la GUI de FMC.
 2. Vaya a la pestaña Deploy.

3. Seleccione la implementación para enviar la configuración al firewall.
4. Haga clic en Deploy.

Troubleshoot

Solución de problemas de Secure Firewall Migration Tool

Fallos de migración habituales:

- Caracteres desconocidos o no válidos en el archivo de configuración de PaloAlto.
- Elementos de configuración faltantes o incompletos.
- Problemas de conectividad de red o latencia.
- Problemas durante la carga del archivo de configuración de PaloAlto o al enviar la configuración al FMC.

Uso del paquete de soporte para la resolución de problemas:

- En la pantalla "Complete Migration" (Migración completa), haga clic en el botón Support.
- Seleccione Support Bundle y elija los archivos de configuración que desea descargar.
- Los archivos de registro y de base de datos están seleccionados de forma predeterminada.
- Haga clic en Descargar para obtener un archivo .zip.
- Extraiga el archivo .zip para ver los registros, la base de datos y los archivos de configuración.
- Haga clic en Enviar correo electrónico para enviar los detalles del fallo al equipo técnico.
- Adjunte el paquete de soporte en su correo electrónico.
- Haga clic en Visitar la página del TAC para crear un caso del TAC de Cisco para obtener asistencia.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).