

Migre ASA a Firepower Threat Defence (FTD) mediante FMT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Antecedentes](#)

[Obtener el archivo de configuración de ASA](#)

[Exportar certificado PKI de ASA e importar a Management Center](#)

[Recuperar paquetes y perfiles de AnyConnect](#)

[Configurar](#)

[Configuration Steps:](#)

[Troubleshoot](#)

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

Introducción

Este documento describe el procedimiento para migrar Cisco Adaptive Security Appliance (ASA) a Cisco Firepower Threat Device .

Prerequisites

Requirements

Cisco recomienda que conozca Cisco Firewall Threat Defence (FTD) y Adaptive Security Appliance (ASA).

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) v7.0.1
- Dispositivo de seguridad adaptable (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defence Virtual (FTDv) v7.4.1

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:

- Cisco Adaptive Security Appliance (ASA) 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)
- Fortinet (más de 5,0)
- Palo Alto Networks (6.1+)

Antecedentes

Antes de migrar la configuración de ASA, ejecute estas actividades:

Obtener el archivo de configuración de ASA

Para migrar un dispositivo ASA, utilice el comando `show running-config` para un solo contexto, o `show tech-support` para el modo multicontexto para obtener la configuración, guárdela como un archivo `.cfg` o `.txt` y transfírela al equipo con la herramienta de migración Secure Firewall.

Exportar certificado PKI de ASA e importar a Management Center

Utilice este comando para exportar el certificado PKI a través de la CLI desde la configuración ASA de origen con las claves a un archivo PKCS12:

```
ASA(config)#crypto puede export <trust-point-name> pkcs12 <passphrase>
```

A continuación, importe el certificado PKI en un centro de gestión (Object Management PKI Objects). Para obtener más información, consulte Objetos PKI en la [Guía de configuración de Firepower Management Center](#).

Recuperar paquetes y perfiles de AnyConnect

Los perfiles de AnyConnect son opcionales y se pueden cargar a través del centro de gestión o la

herramienta de migración de Secure Firewall.

Utilice este comando para copiar el paquete requerido del ASA de origen a un servidor FTP o TFTP:

Copy <ubicación del archivo de origen:/nombre del archivo de origen> <destino>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Ejemplo de copia del paquete Anyconnect.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Ejemplo de copia de External Browser Package.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Ejemplo de copia del paquete Hostscan.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Ejemplo de copia de Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Ejemplo de copia de Data.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Ejemplo de copia del perfil de Anyconnect.

Importe los paquetes descargados en el centro de administración (Administración de objetos > VPN > Archivo AnyConnect).

a-Dap.xml y Data.xml se deben cargar en el centro de gestión desde la herramienta de migración de Secure Firewall en la sección Revisión y validación > VPN de acceso remoto > Archivo AnyConnect.

Los perfiles de b-AnyConnect se pueden cargar directamente en el centro de gestión o a través de la herramienta de migración de Secure Firewall en la sección Revisión y validación > VPN de acceso remoto > Archivo AnyConnect.

Configurar

Configuration Steps:

1.Descargar la herramienta de migración de Firepower más reciente de Cisco Software Central:

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Expand All Collapse All

Latest Release v

7.0.1

All Release v

7 v

7.0.1

7.0.0

Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

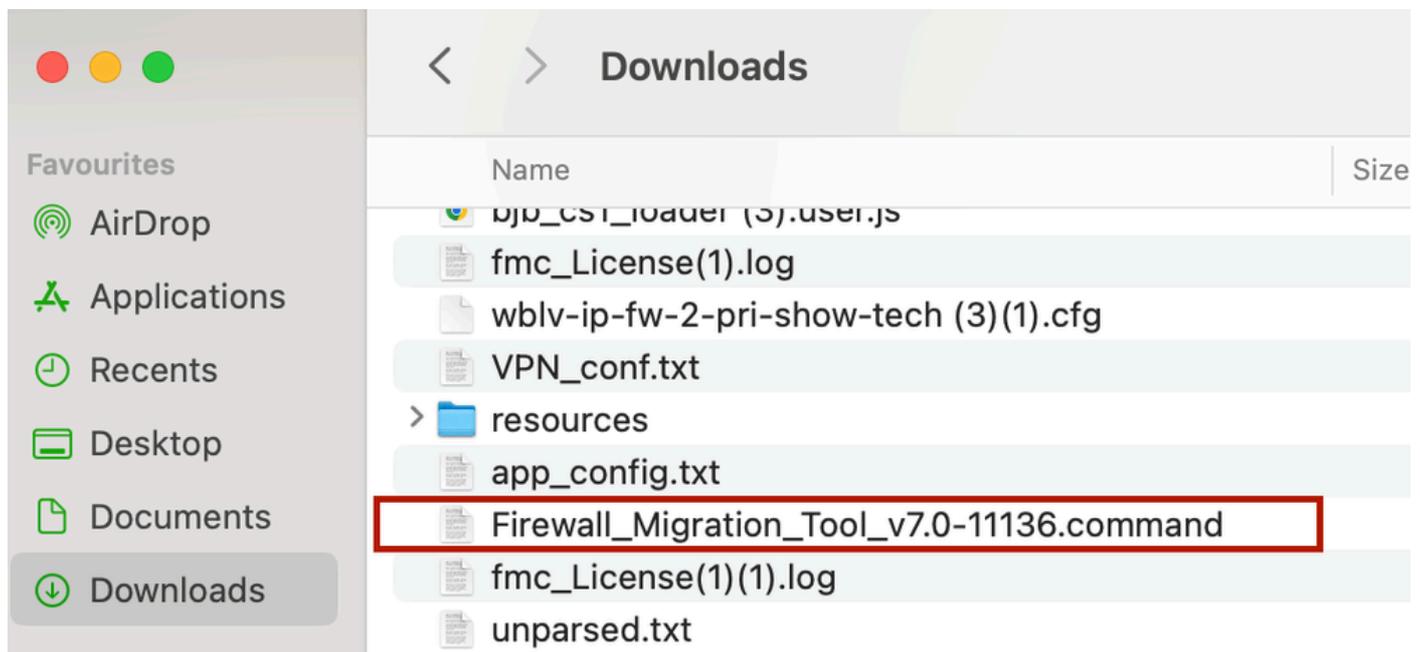
[Release Notes for 7.0.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB	↓ 🛒 📄

Descarga de software

2. Haga clic en el archivo que descargó anteriormente en el equipo.



El archivo

```
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 [INFO      | 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 : {}"
2025-01-16 16:51:41,838 [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 16:51:41] "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"
2025-01-16 16:51:46,868 [INFO     | common] > "proxies : {}"
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 -
```

Registros de la consola



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

-
3. Después de ejecutar el programa, se abre un navegador web que muestra el "Acuerdo de licencia del usuario final".
 1. Marque la casilla de verificación para aceptar los términos y condiciones.
 2. Haga clic en Proceed.

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 specific product terms at www.cisco.com/go/software/terms (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. It makes no warranty, applicable law. You are not licensed to Use the

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

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD



Extract Source Information

Any additional information explaining this



EULA

4. Inicie sesión con una cuenta CCO válida y la interfaz GUI de FMT aparecerá en el navegador web.



Security Cloud Sign On

Email

Continue

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

Or

[Other login options](#)

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

Conexión a FMT

5. Seleccione el firewall de origen que desea migrar.



Nota: Para este ejemplo, conéctese directamente al ASA.

-
7. Se muestra un resumen de la configuración encontrada en el firewall como panel. Haga clic en Siguiente.

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

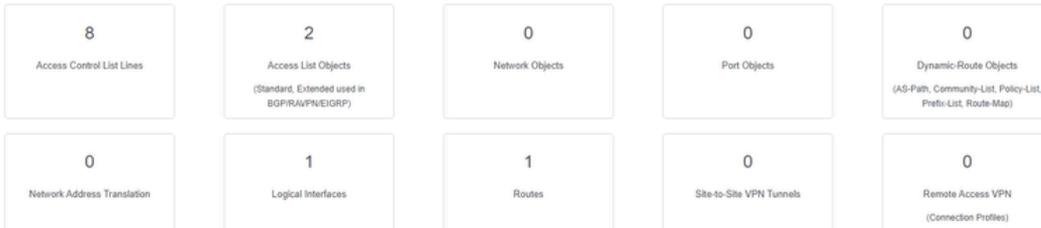
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



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

<https://cisco.com>

Back

Next

Summary

8. Seleccione el CSP objetivo que se utilizará en la migración.

Proporcione la dirección IP del FMC. Se abre una ventana emergente en la que se le solicitarán las credenciales de inicio de sesión del FMC.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

✓ Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

Back

Next

IP de FMC

9. (Opcional) Seleccione el FTD de destino que desea utilizar.

1. Si decide migrar a un FTD, seleccione el FTD que desea utilizar.

2. Si no desea utilizar un FTD, puede rellenar la casilla de verificación Proceed without FTD

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Select FTD Device

FTD (192.168.1.17) - VMWare (Native) v

 Proceed without FTD

⚠️ 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 migrated configuration to the FMC.

Proceed

Select Features >

Rule Conversion/ Process Config >

Back

Next

FTD objetivo

10. Seleccione las configuraciones que desea migrar; las opciones se muestran en las capturas de pantalla.

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

- Interfaces
- Routes
 - Static
 - BGP
 - EIGRP
- Site-to-Site VPN Tunnels (no data)
- Policy Based (Crypto Map)
- Route Based (VTI)

Shared Configuration

- Access Control
 - Populate destination security zones
 - ⚠️ Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.
 - Migrate tunnelled rules as Prefilter
- NAT (no data)
- Network Objects (no data)
- Port Objects (no data)
- 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.

Optimization

- Migrate Only Referenced Objects
- Object Group Search

Inline Grouping

- CSM/ASDM

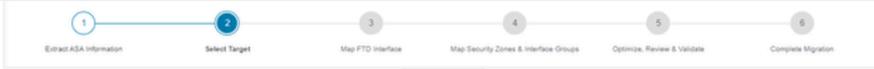
Proceed

Back

Next

Configuraciones

11. Inicie la conversión de las configuraciones de ASA a FTD.



Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

Rule Conversion/ Process Config >

Start Conversion

Back Next

Iniciar conversión

12. Una vez finalizada la conversión, se muestra un panel con el resumen de los objetos que se van a migrar (limitado a la compatibilidad).

1. Si lo desea, puede hacer clic **Download Report** para recibir un resumen de las configuraciones que se van a migrar.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

Rule 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 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVP/VEIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network-Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

Back Next

Descargar informe

Ejemplo de informe previo a la migración, como se muestra en la imagen:

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 that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled 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	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)
ASA Hostname	Not Available
ASA Device Model	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 MHz
Hat 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

Informe previo a la migración

13. Asigne las interfaces ASA con las interfaces FTD en la herramienta de migración.

The screenshot shows the 'Map FTD Interface' configuration screen in the Cisco Firewall Migration Tool. The interface includes a table with two columns: 'ASA Interface Name' and 'FTD Interface Name'. The first entry in the table is 'Management0/0' under the ASA column and 'GigabitEthernet0/0' under the FTD column. The table is currently empty of other entries. At the top right, it indicates 'Source: Cisco ASA (8.4+)' and 'Target FTD: FTD'. Navigation buttons for 'Back' and 'Next' are located at the bottom right, and a 'Refresh' button is positioned above the table.

Interfaces de mapa

14. Crear las zonas de seguridad y los grupos de interfaces para las interfaces en el FTD

Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 |< < Page 1 of 1 >>|

Back Next

Zonas de seguridad y grupos de interfaces

La herramienta crea automáticamente las zonas de seguridad (SZ) y los grupos de interfaz (IG), tal y como se muestra en la imagen:



Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_lg (A)

10 per page 1 to 1 of 1 |< < Page 1 of 1 >>|

Back Next

Herramienta de creación automática

15. Revise y valide las configuraciones que se van a migrar en la herramienta de migración.
 1. Si ya ha terminado de revisar y optimizar las configuraciones, haga clic en `Validate`.



Optimize, Review and Validate Configuration

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

Access Control | **Objects** | NAT | Interfaces | Routes | Site-to-Site VPN Tunnels | Remote Access VPN

Access List Objects | **Network Objects** | Port Objects | VPN Objects | Dynamic-Route Objects

Select all 1 entries Selected: 0 / 1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

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

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

Validate

Revisar y validar

16. Si el estado de validación es correcto, envíe las configuraciones a los dispositivos de destino.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

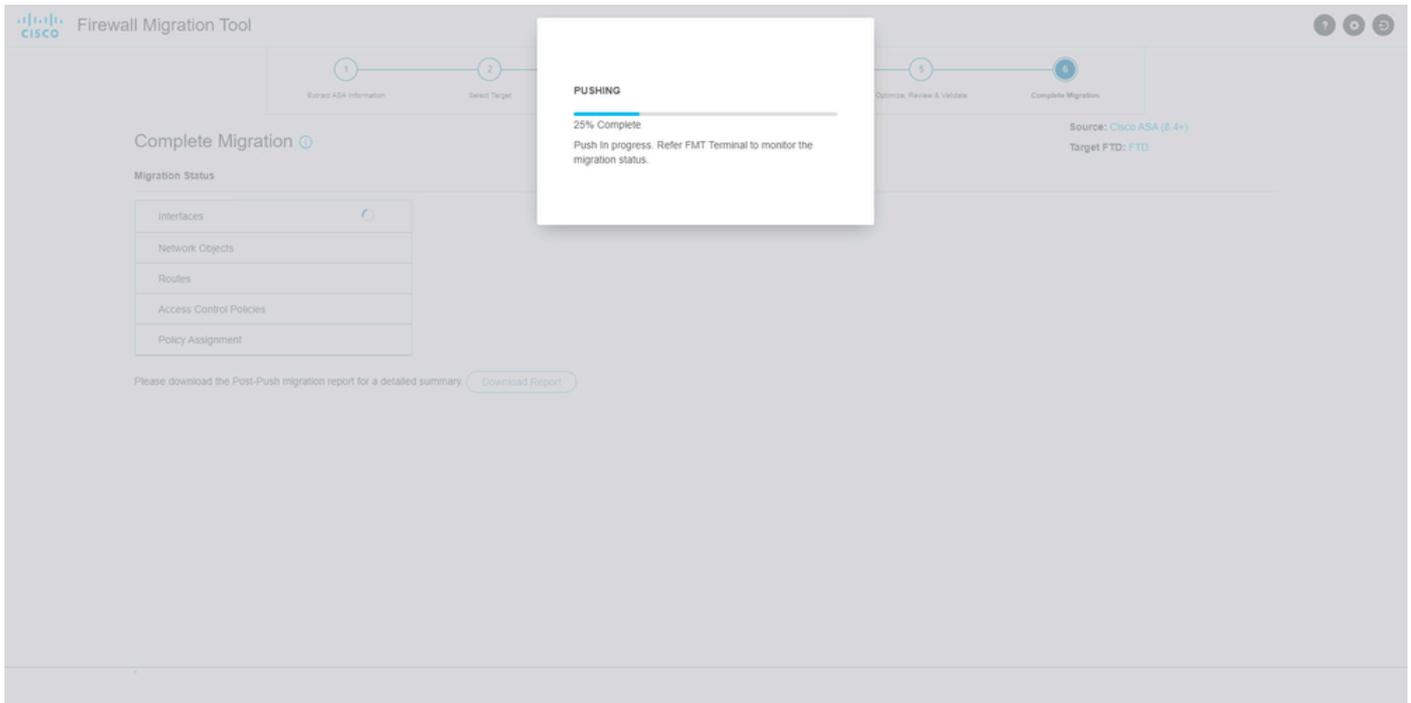
0	Not selected for migration Access Control List Lines Access List Objects (Standard, Extended used in BGP/RAV/EIGRP)	1	Not selected for migration Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)	

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

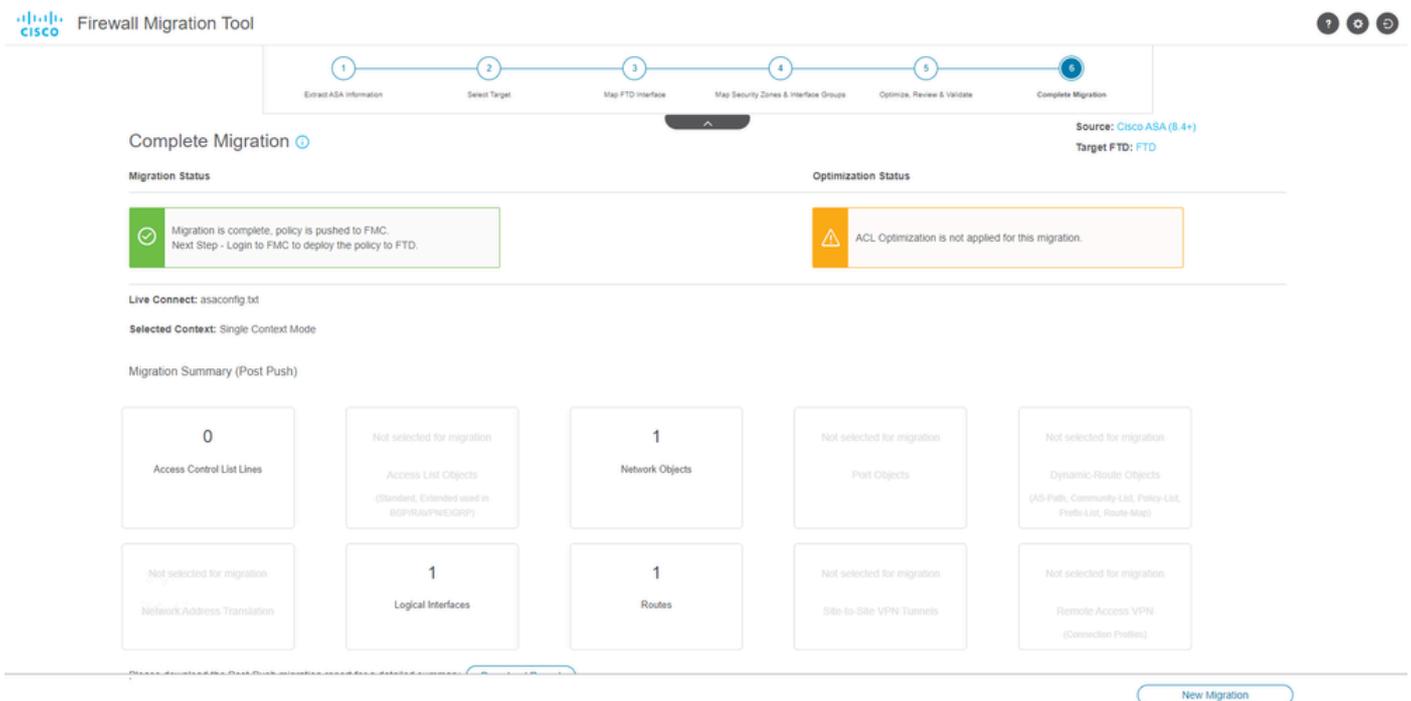
Validación

Ejemplo de configuración introducida a través de la herramienta de migración, como se muestra en la imagen:



Empujar

Ejemplo de migración correcta, como se muestra en la imagen:



Migración correcta

(Opcional) Si ha seleccionado migrar la configuración a un FTD, se requiere una implementación para transferir la configuración disponible del FMC al firewall.

Para implementar la configuración:

1. Inicie sesión en la GUI de FMC.
2. Vaya a la `Deploy` pestaña.

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

Troubleshoot

Solución de problemas de Secure Firewall Migration Tool

- Fallos de migración comunes:
 - Caracteres desconocidos o no válidos en el archivo de configuración ASA.
 - Elementos de configuración faltantes o incompletos.
 - Problemas de conectividad de red o latencia.
- Problemas durante la carga del archivo de configuración de ASA o envío de la configuración al centro de administración.
- Los problemas comunes incluyen:
- Uso de Support Bundle 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.
- La herramienta le permite descargar un paquete de soporte para archivos de registro, bases de datos y archivos de configuración.
- Pasos para descargar:
- Para obtener más ayuda:

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).