

Configuración de FTD desde el archivo de configuración ASA con la herramienta de migración de Firepower

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Errores conocidos relacionados con la herramienta de migración de Firepower](#)

[Información Relacionada](#)

Introducción

Este documento describe un ejemplo de migración de Adaptive Security Appliance (ASA) a Firepower Threat Defense (FTD) en FPR4145.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de ASA
- Conocimiento de Firepower Management Center (FMC) y FTD

Componentes Utilizados

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

- ASA versión 9.12(2)
- FTD versión 6.7.0
- FMC versión 6.7.0
- Firepower Migration Tool versión 2.5.0

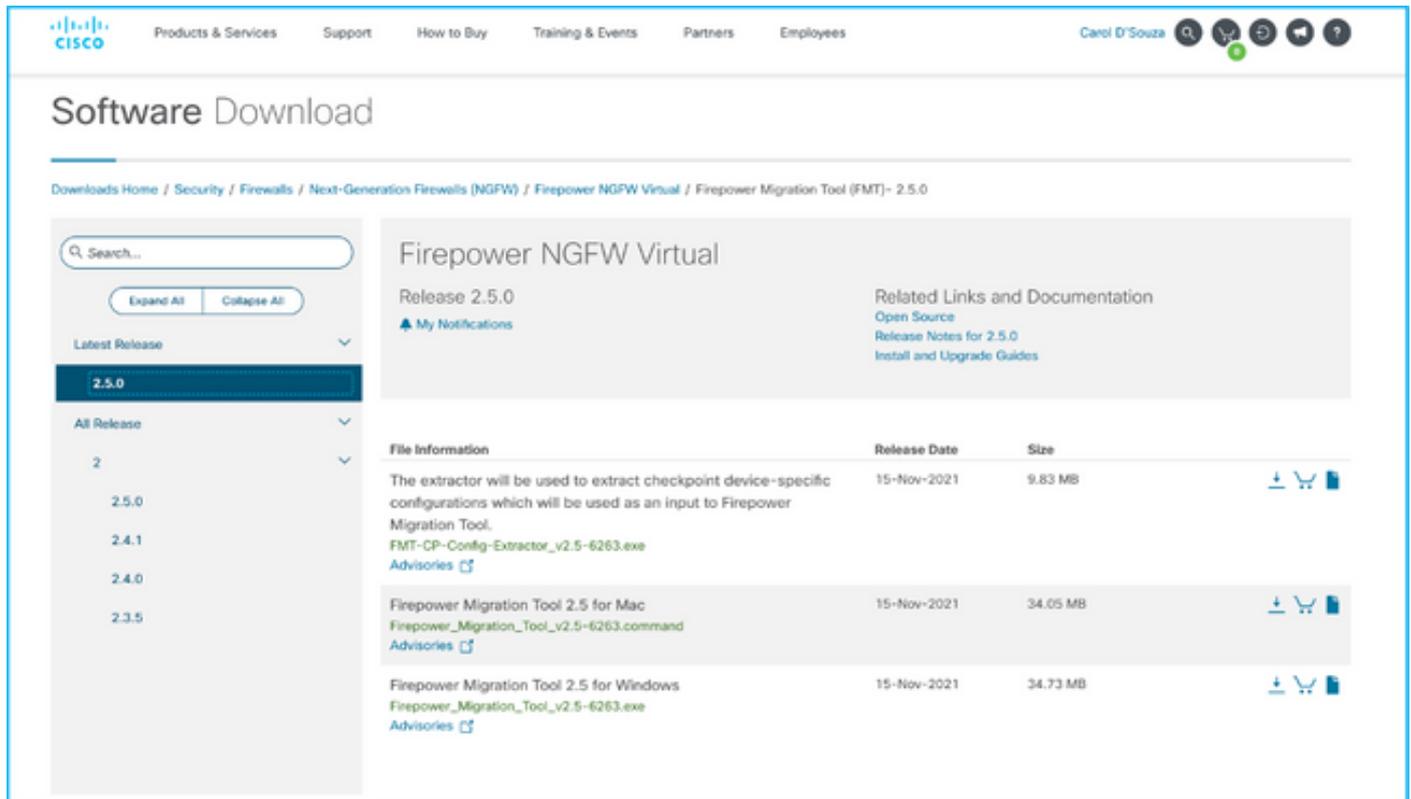
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Exportar archivo de configuración ASA en formato **.cfg** o **.txt**. FMC debe implementarse con FTD registrado en él.

Configurar

1. Descargue Firepower Migration Tool desde software.cisco.com como se muestra en la imagen.



The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual, Release 2.5.0. The page includes a search bar, navigation tabs, and a table of download links for various operating systems.

File Information	Release Date	Size	Download
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v2.5-6263.exe Advisories	15-Nov-2021	9.83 MB	Download
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command Advisories	15-Nov-2021	34.05 MB	Download
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe Advisories	15-Nov-2021	34.73 MB	Download

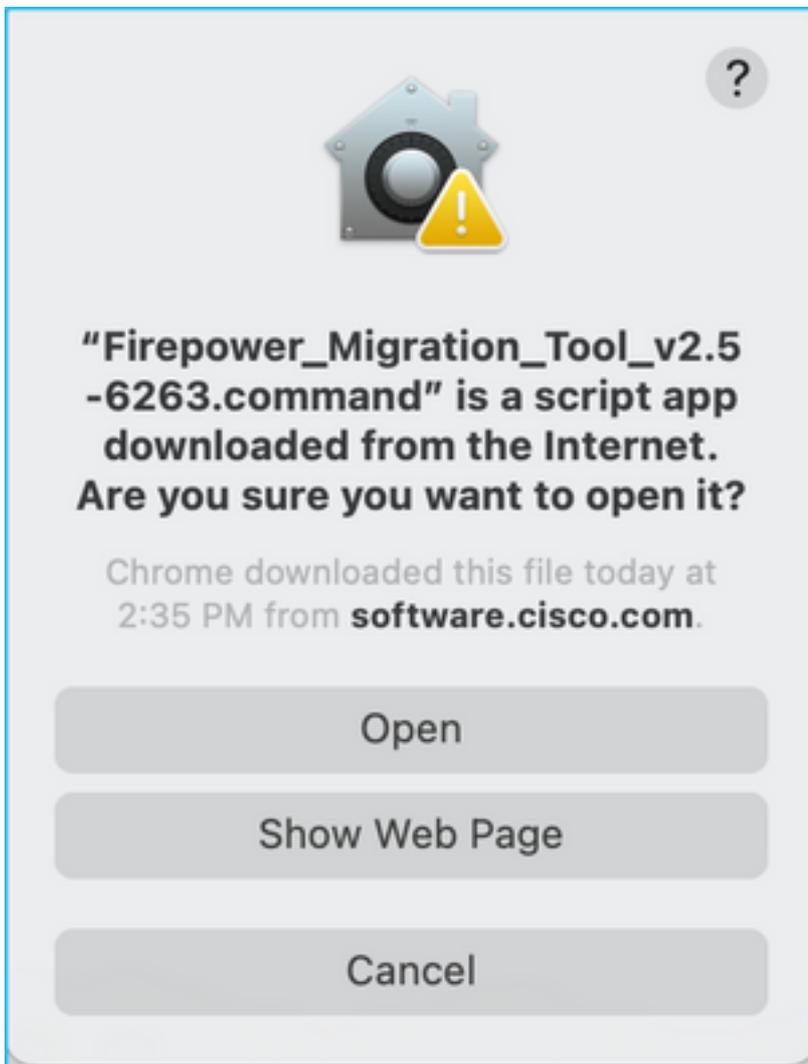
2. Revise y verifique los requisitos en la sección [Pautas y limitaciones](#) para la Herramienta de Migración de Firepower.

3. Si tiene previsto migrar un archivo de configuración de gran tamaño, configure los parámetros de suspensión para que el sistema no se suspenda durante una migración.

3.1. Para Windows, vaya a Opciones de alimentación en el Panel de control. Haga clic en **Cambiar configuración del plan** junto a su plan de energía actual. Cambiar **Ponga el ordenador a modo suspendido a Nunca**. Haga clic en **Guardar cambios**.

3.2. Para MAC, navegue hasta **Preferencias del sistema > Ahorro de energía**. Marque la casilla situada junto a para evitar que el ordenador se apague automáticamente cuando la pantalla esté apagada y arrastre el botón **Desactivar pantalla** después del control deslizante a Nunca.

Nota: Esta advertencia, el diálogo aparece cuando los usuarios de MAC intentan abrir el archivo descargado. Ignore esto y siga el paso 4 A.



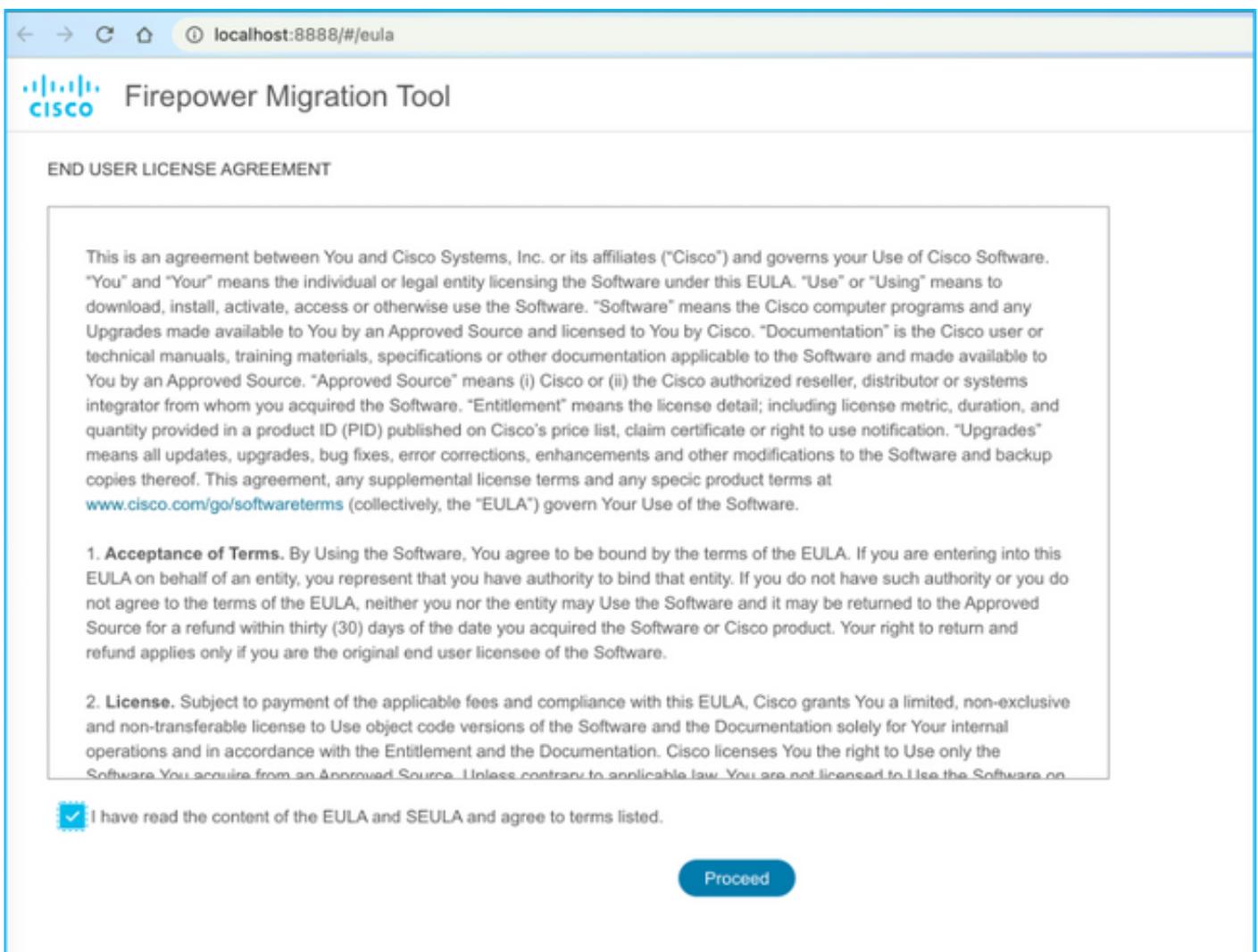
4. A. Para MAC: utilice el terminal y ejecute estos comandos.

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/  
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263  
.command  
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command  
  
[75653] PyInstaller Bootloader 3.x  
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool  
_v2.5-6263.command  
[75653] LOADER: hompath is /Users/caroldso/Downloads  
[75653] LOADER: _MEIPASS2 is NULL  
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too  
l_v2.5-6263.command  
[75653] LOADER: Cookie found at offset 0x219AE08  
[75653] LOADER: Extracting binaries  
[75653] LOADER: Executing self as child
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO      | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG     | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B Para Windows: haga doble clic en Firepower Migration Tool para iniciarla en un navegador de Google Chrome.

5. Acepte la licencia como se muestra en la imagen.



← → ↻ 🏠 ⓘ localhost:8888/#/eula

cisco Firepower Migration Tool

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 specic product terms at www.cisco.com/go/softwareterms (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.

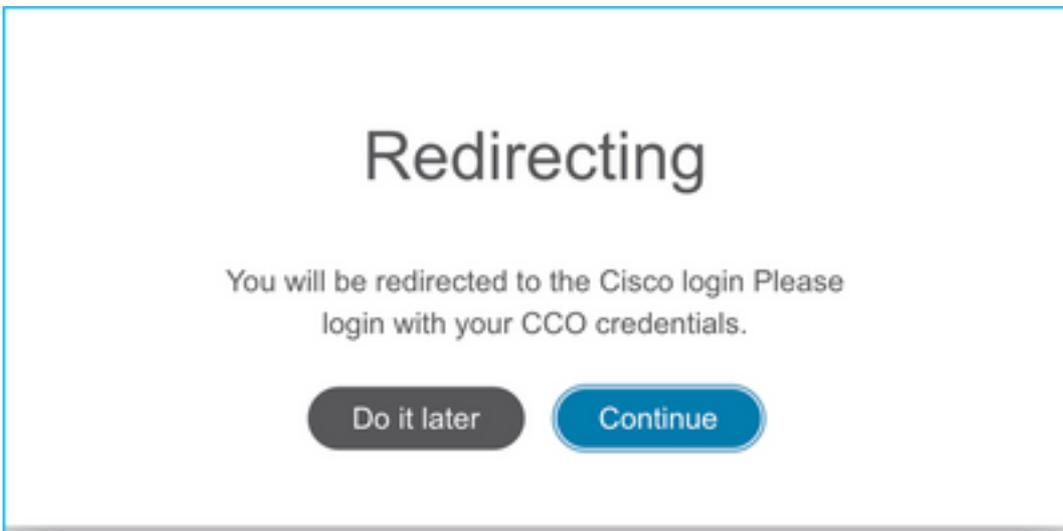
2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. Unless contrary to applicable law, You are not licensed to Use the Software on

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

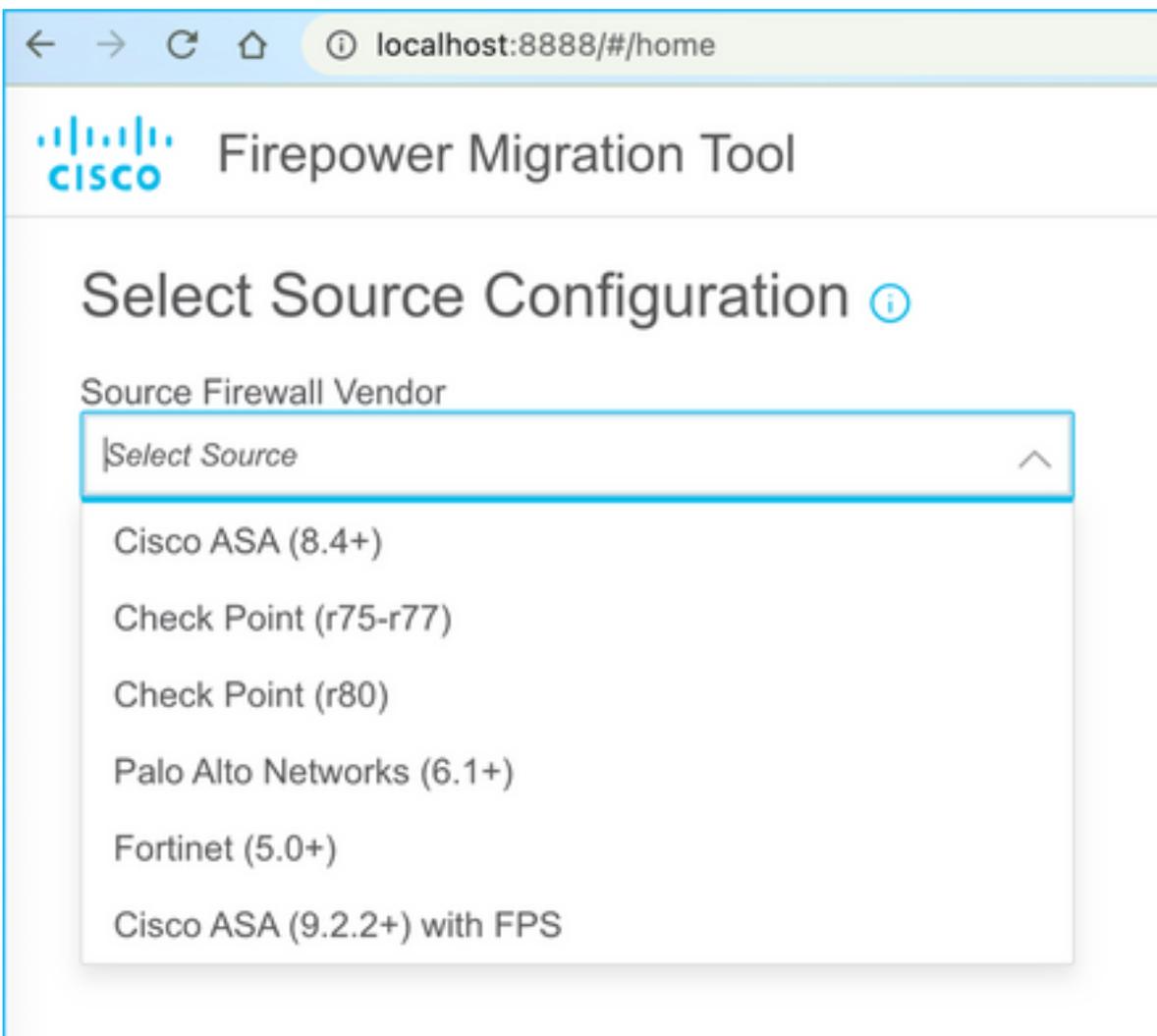
Proceed

6. En la página de inicio de sesión de Firepower Migration Tool, haga clic en el enlace de inicio de sesión con CCO para iniciar sesión en su cuenta de Cisco.com con sus credenciales de inicio de sesión único.

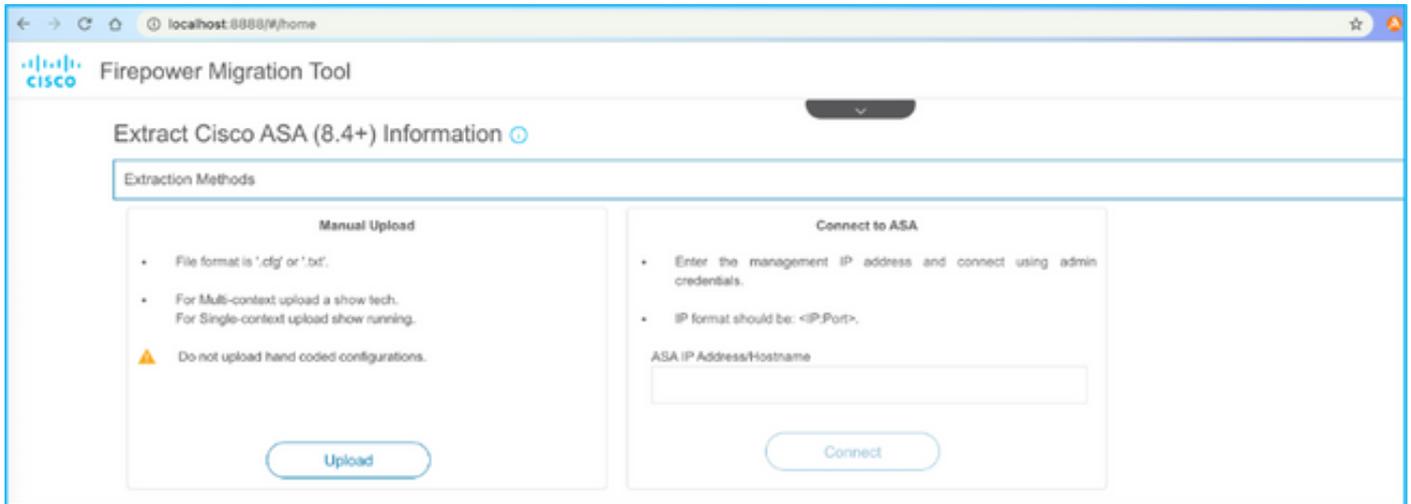
Nota: Si no tiene una cuenta de Cisco.com, créela en la página de inicio de sesión de Cisco.com. Inicie sesión con las siguientes credenciales predeterminadas: Nombre de usuario—Contraseña de administrador—Admin123.



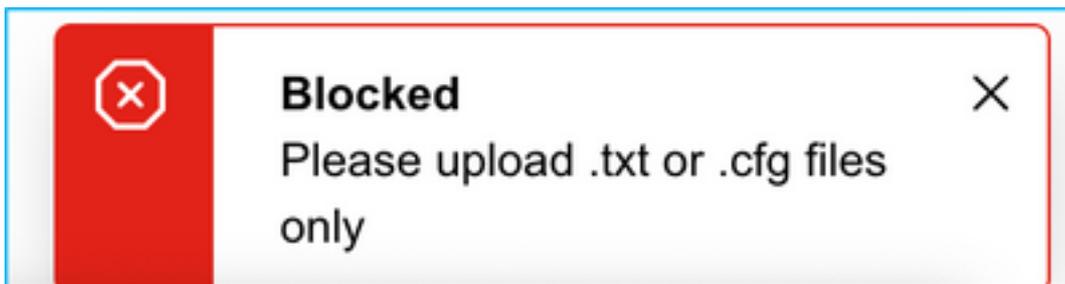
7. Seleccione la configuración de origen. En esta situación, es Cisco ASA (8.4+).



8. Seleccione Carga manual si no tiene conectividad con el ASA. De lo contrario, puede recuperar la configuración en ejecución del ASA e introducir la dirección IP de administración y los detalles de inicio de sesión. En nuestra situación, se realizó una carga manual.

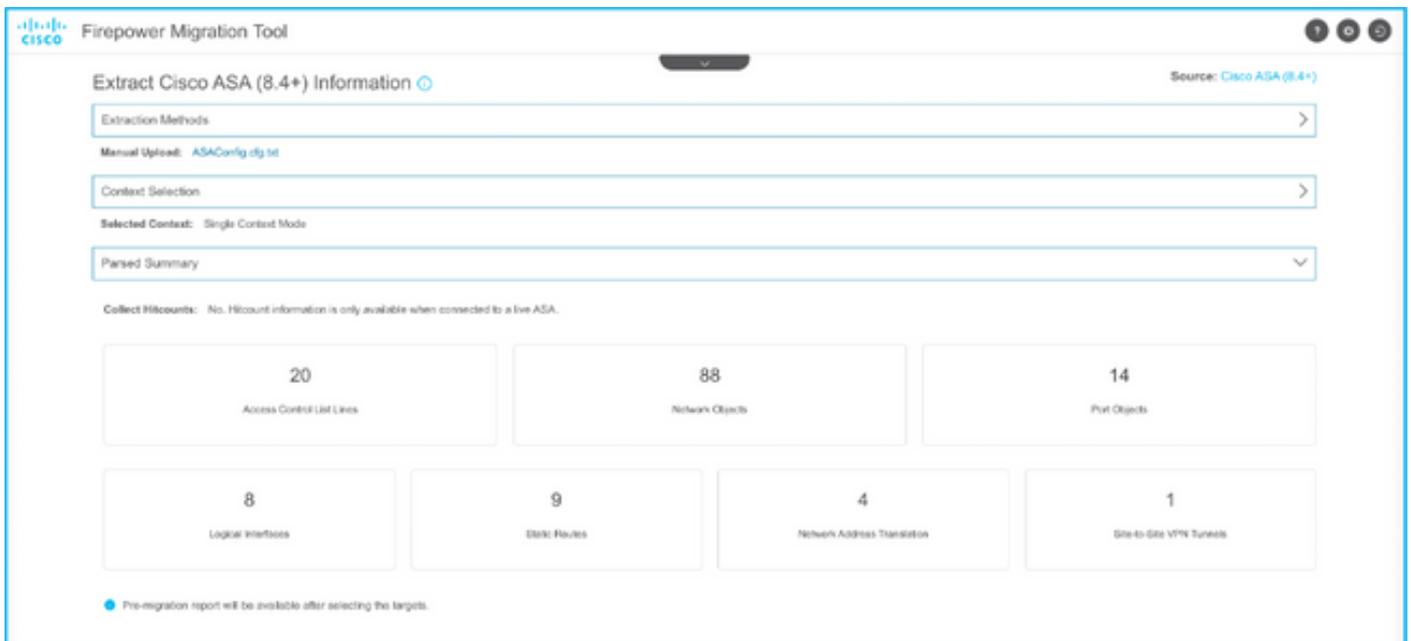


Nota: Este error aparece si el archivo no está soportado. Asegúrese de cambiar el formato a texto sin formato. (Se ha visto un error a pesar de tener la extensión .cfg).

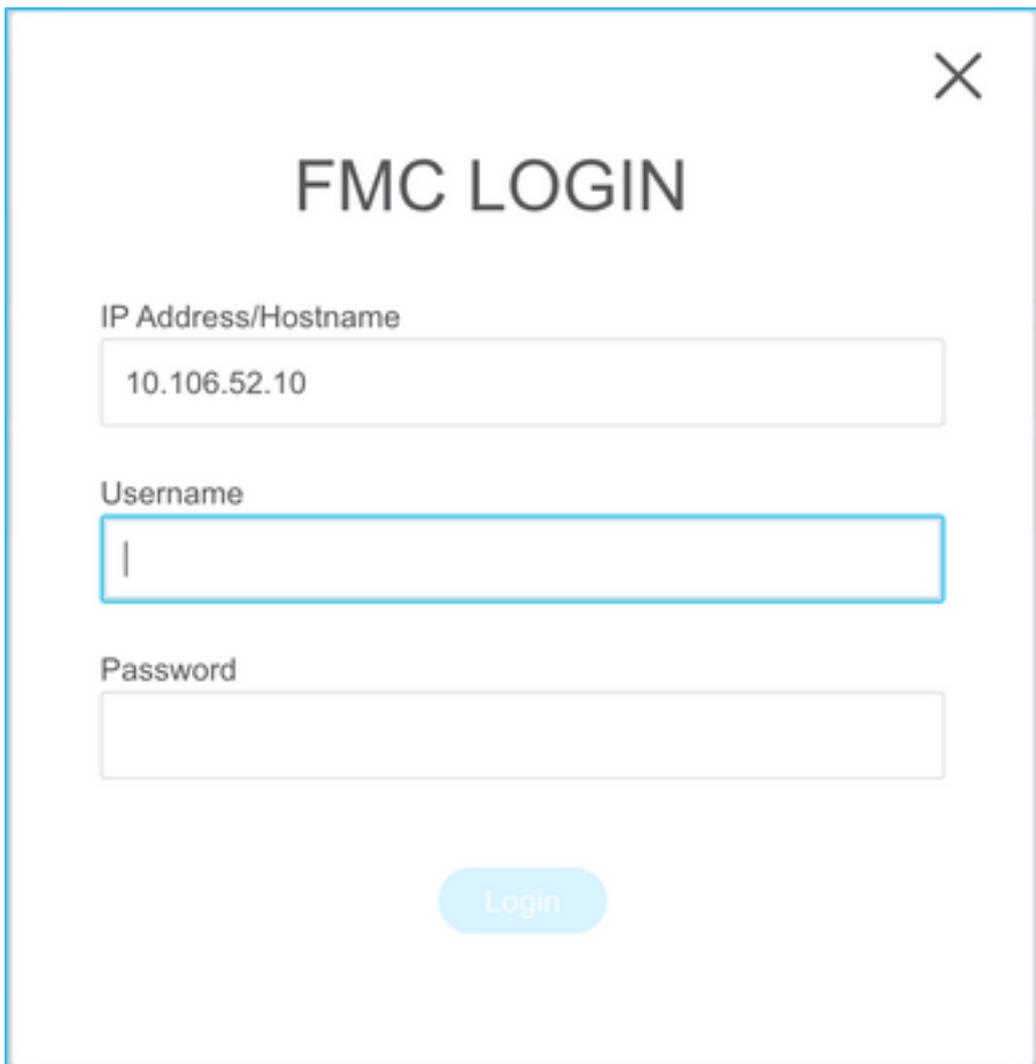
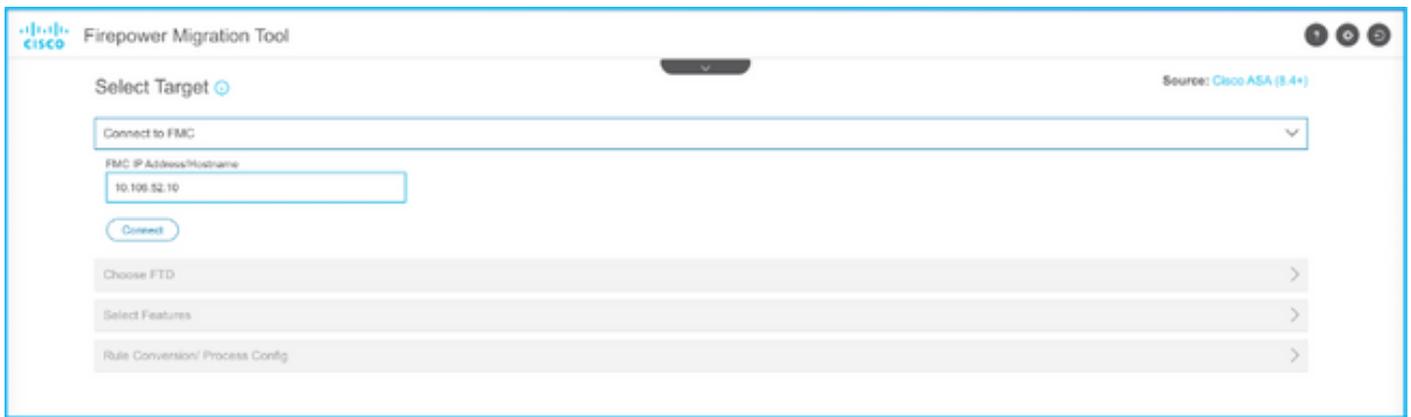


```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address auto
:
interface Ethernet1/1
no nameif
no security-level
no ip address
:
interface Ethernet1/2
nameif Inside
cts manual
security-level 0
no ip address
:
interface Ethernet1/3
nameif Outside
cts manual
security-level 0
no ip address
```

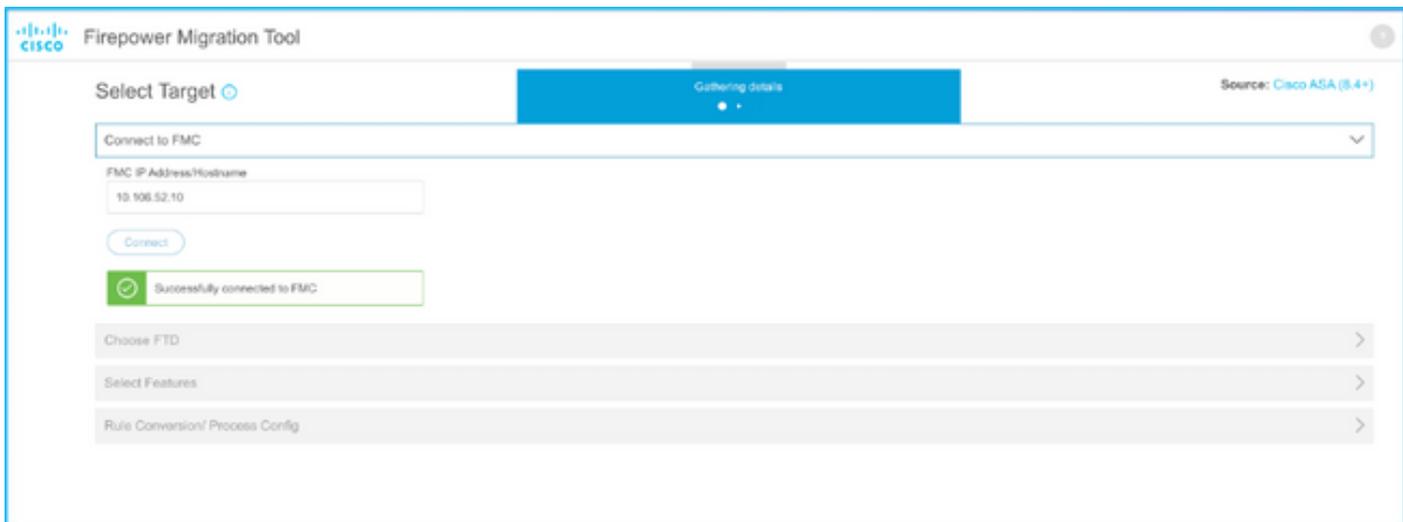
9. Después de cargar el archivo, los elementos se analizarán proporcionando un resumen como se muestra en la imagen:



10. Introduzca la IP de FMC y las credenciales de inicio de sesión a las que se migrará la configuración de ASA. Asegúrese de que la IP de FMC esté accesible desde su estación de trabajo.



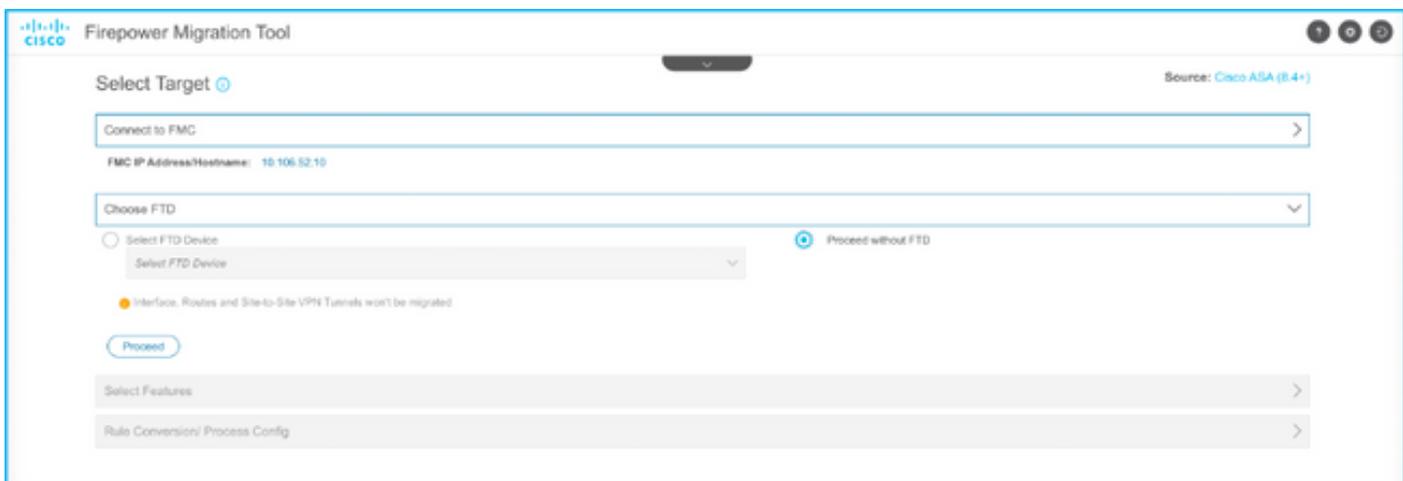
11. Una vez conectado el FMC, se mostrarán los FTD administrados que se encuentran debajo.



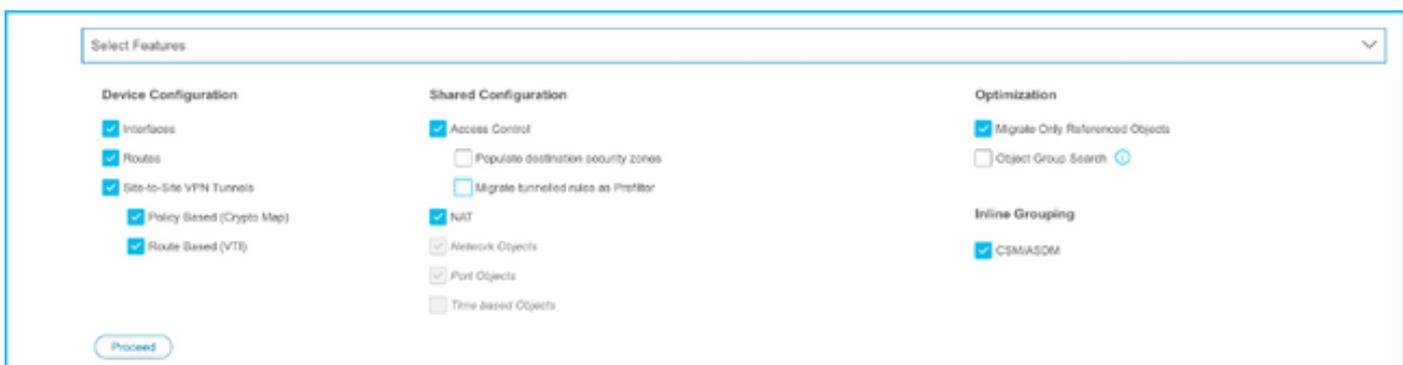
12. Elija el FTD al que desea realizar la migración de la configuración ASA.



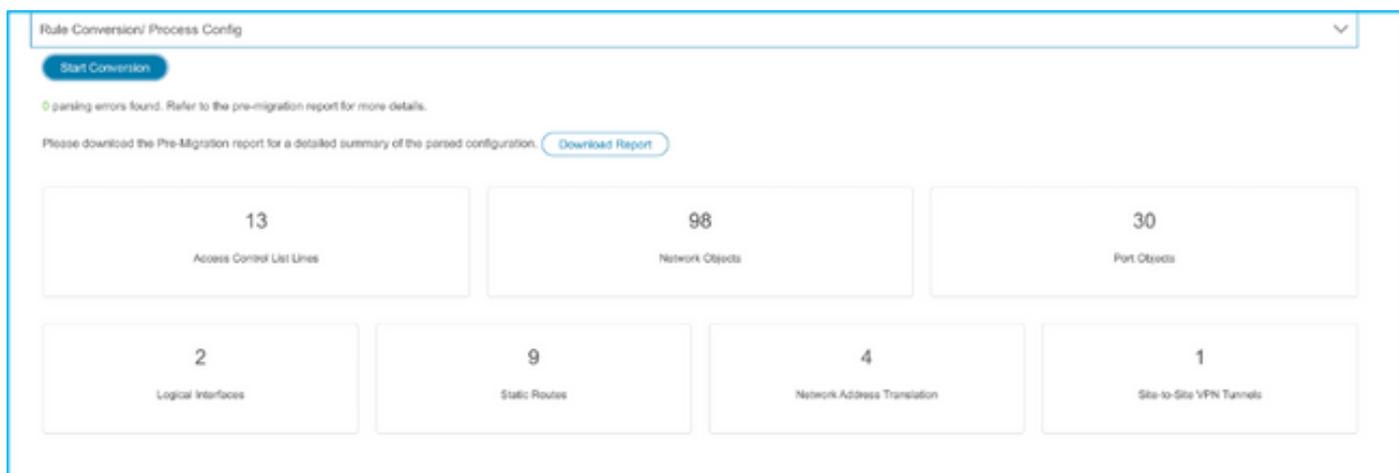
Nota: Se recomienda seleccionar el dispositivo FTD, de lo contrario las interfaces, las rutas y la configuración VPN de sitio a sitio tendrán que realizarse manualmente.



13. Seleccione las funciones que se deben migrar como se muestra en la imagen.



14. Seleccione **Iniciar conversión** para iniciar la pre-migración que rellenará los elementos pertenecientes a la configuración FTD.



The screenshot shows a web interface for 'Rule Conversion/ Process Config'. At the top, there is a 'Start Conversion' button. Below it, a message states '0 parsing errors found. Refer to the pre-migration report for more details.' and a 'Download Report' button. The main area contains seven summary cards for different configuration elements:

Configuration Element	Count
Access Control List Lines	13
Network Objects	98
Port Objects	30
Logical Interfaces	2
Static Routes	9
Network Address Translation	4
Site-to-Site VPN Tunnels	1

15. Haga clic en **Descargar informe** visto anteriormente para ver el informe previo a la migración, como se muestra en la imagen.

← → ↻ 🏠 📄 File | /Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html

CISCO Pre-Migration Report

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 reviewing the configuration 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	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

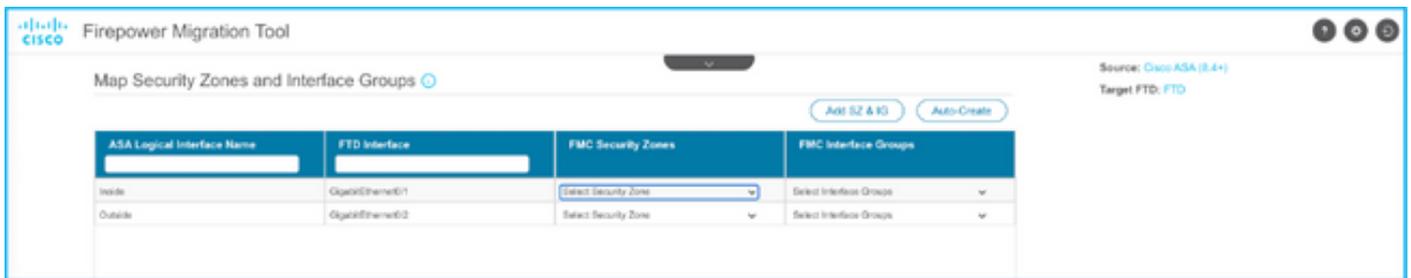
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Asigne las interfaces ASA a las interfaces FTD según se requiera, como se muestra en la imagen.

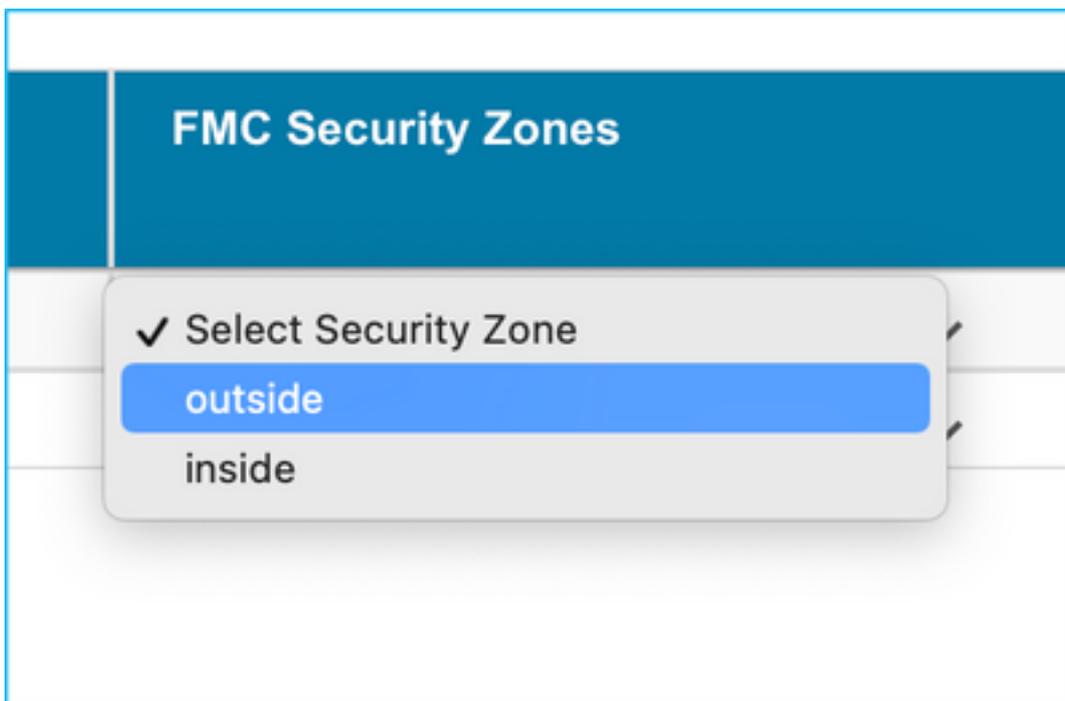
Refresh

ASA Interface Name	FTD Interface Name
<input type="text"/>	<div style="border: 1px solid gray; padding: 5px;"> Select Interface GigabitEthernet0/0 GigabitEthernet0/1 ✓ GigabitEthernet0/2 </div>
Ethernet1/2	
Ethernet1/3	

17. Asigne zonas de seguridad y grupos de interfaz a las interfaces FTD.



A. Si FMC tiene zonas de seguridad y grupos de interfaz ya creados, puede seleccionarlos según sea necesario:



B Si hay necesidad de crear zonas de seguridad y un grupo de interfaces, haga clic en **Agregar SZ e IG** como se muestra en la imagen.

✕

Add SZ & IG

Security Zones (SZ) Interface Groups (IG)

Add

iMax 48 characters for Interface Group name. Allowed special characters are _.-+

Interface Groups	Type	Actions
<input style="width: 100%;" type="text" value="Inside"/>	ROUTED	✕ ✓

0 - 0 of 0 |< < > >|

Close

C. De lo contrario, puede optar por la opción **Creación automática** que creará zonas de seguridad y grupos de interfaz con el nombre **ASA Logical interface_sz** y **ASA Logical interface_ig** respectivamente.

Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to ASA interfaces

Security Zones Interface Groups

Cancel

Auto-Create



Firepower Migration Tool

Map Security Zones and Interface Groups ⓘ

Add SZ & IG

Auto-Create

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	inside	Inside_ig (A)
Outside	GigabitEthernet0/2	outside	Outside_ig (A)

18. Revise y valide cada uno de los elementos FTD creados. Las alertas se ven en rojo como se muestra en la imagen.



Firepower Migration Tool

Optimize, Review and Validate Configuration ⓘ

Source: Cisco ASA (8.4+)

Target FTD: FTD

Access Control NAT Network Objects Port Objects Interfaces Routes VPN Objects Site-to-Site VPN Tunnels ⓘ

ADP Pre-Filter

Select all 13 entries

Selected: 0 / 13

Apply

Cancel

Search

#	Name	SOURCE				DESTINATION				State	Action	ACE Count
		Zone	Network	Port	Zone	Network	Port					
<input type="checkbox"/>	1	Outside_access_in_01	outside	any	ANY	ANY			✓	Allow	1	
<input type="checkbox"/>	2	Outside_access_in_02	outside	any	ANY				✓	Allow	1	
<input type="checkbox"/>	3	Outside_access_in_03	outside	any	ANY				✓	Allow	2	
<input type="checkbox"/>	4	Outside_access_in_04	outside	any	ANY				✓	Allow	4	
<input type="checkbox"/>	5	Outside_access_in_05	outside	any	ANY				✓	Allow	3	
<input type="checkbox"/>	6	Outside_access_in_06	outside	any	ANY				✓	Allow	2	
<input type="checkbox"/>	7	Outside_access_in_07	outside	any	ANY				✓	Allow	3	
<input type="checkbox"/>	8	Outside_access_in_08	outside	any	ANY				✓	Allow	1	
<input type="checkbox"/>	9	Outside_access_in_09	outside	any	ANY				✓	Allow	8	
<input type="checkbox"/>	10	Outside_access_in_10	outside	any	ANY				✓	Allow	7	
<input type="checkbox"/>	11	Outside_access_in_11	outside	any	ANY				✓	Allow	2	
<input type="checkbox"/>	12	Outside_access_in_12	outside	any	ANY				✓	Allow	1	

50 perpage 1 to 13 of 13 | Page 1 of 1

Update the Pre-Shared Key (PSK) Certificate column highlighted in yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration. For additional help, click here.

Optimize ACL (RM)

19. Las acciones de migración se pueden seleccionar como se muestra en la imagen si desea editar alguna regla. Las funciones de FTD de agregar archivos y la política IPS se pueden realizar en este paso.

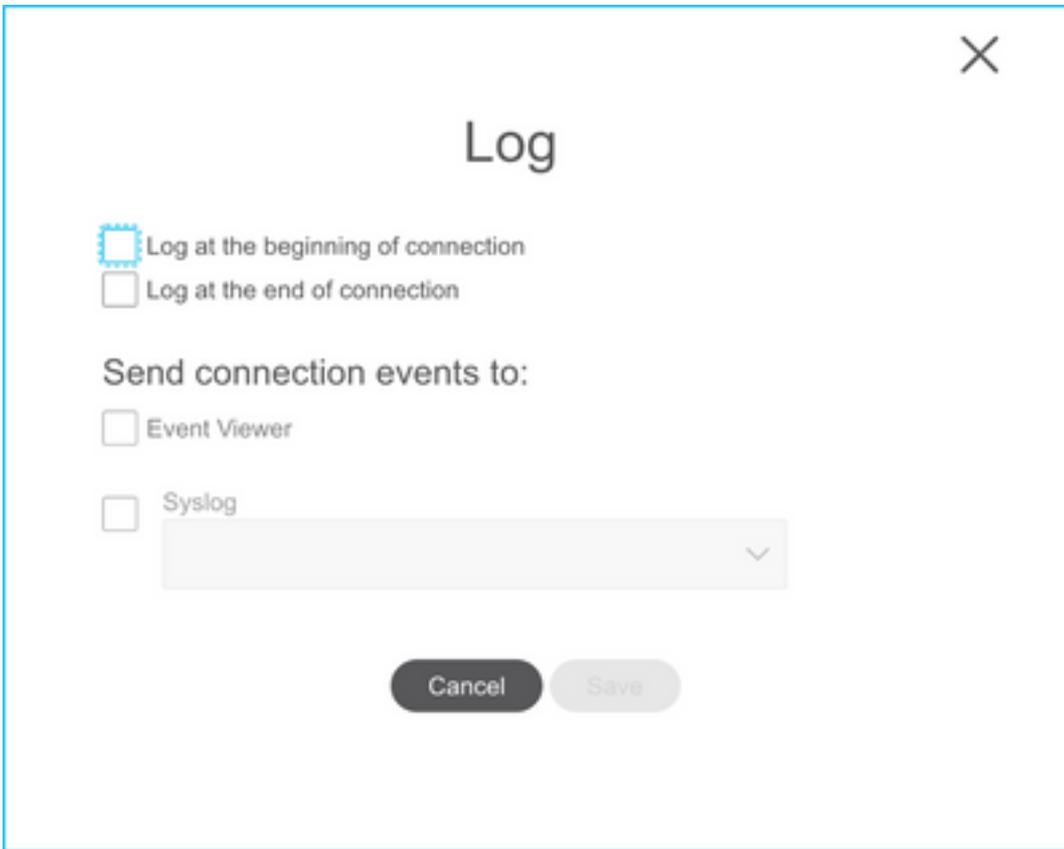
The screenshot shows the 'ACP' configuration page with a 'Pre-filter' button. A checkbox labeled 'Select all 13 entries' is checked, and 'Selected: 13 / 13' is displayed. An 'Actions' dropdown menu is open, showing 'MIGRATION ACTIONS' (Do not migrate) and 'RULE ACTIONS' (File Policy, IPS Policy, Log, Rule Action). Below the menu is a table with columns for selection, ID, Name, and Source.

<input checked="" type="checkbox"/>	#	Name	SOURCE
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	
<input checked="" type="checkbox"/>	2	Outside_access_in_#2	
<input checked="" type="checkbox"/>	3	Outside_access_in_#3	
<input checked="" type="checkbox"/>	4	Outside_access_in_#4	
<input checked="" type="checkbox"/>	5	Outside_access_in_#5	
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside any

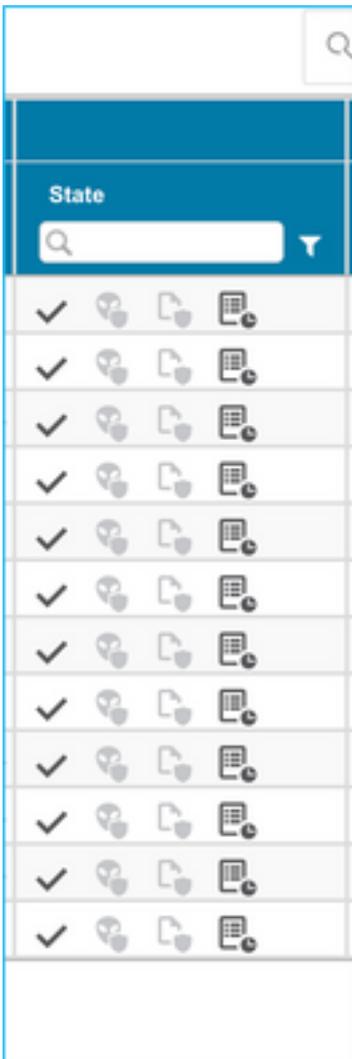
Nota: Si las políticas de archivos ya existen en el FMC, se rellenarían como se muestra en la imagen. Lo mismo se aplica a las políticas IPS junto con las políticas predeterminadas.

The 'File Policy' dialog box has a title bar with a close button (X). Below the title is a search field labeled 'Select File Policy *'. A dropdown menu is open, showing 'eicar' and 'None' as options. At the bottom are 'Cancel' and 'Select' buttons.

La configuración del registro se puede realizar para las reglas requeridas. La configuración del servidor Syslog existente en el FMC se puede seleccionar en esta etapa.

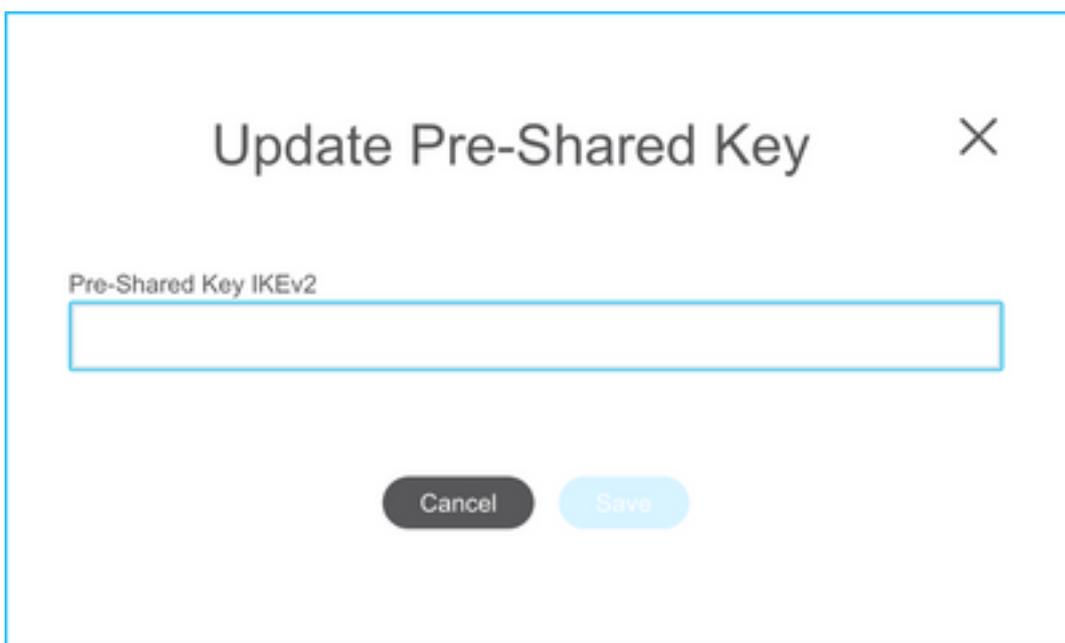
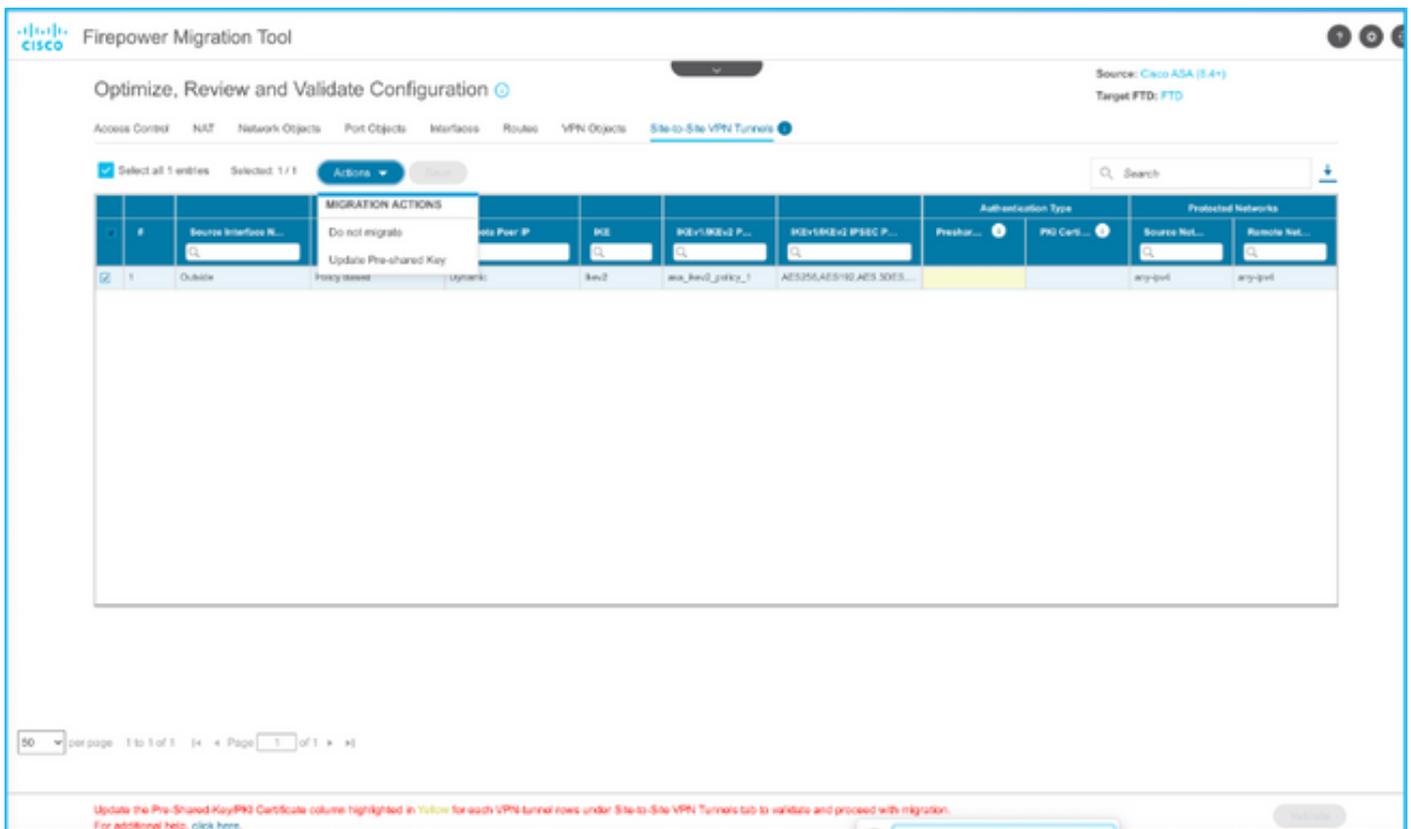


Las acciones de regla seleccionadas se resaltarán en consecuencia para cada regla.

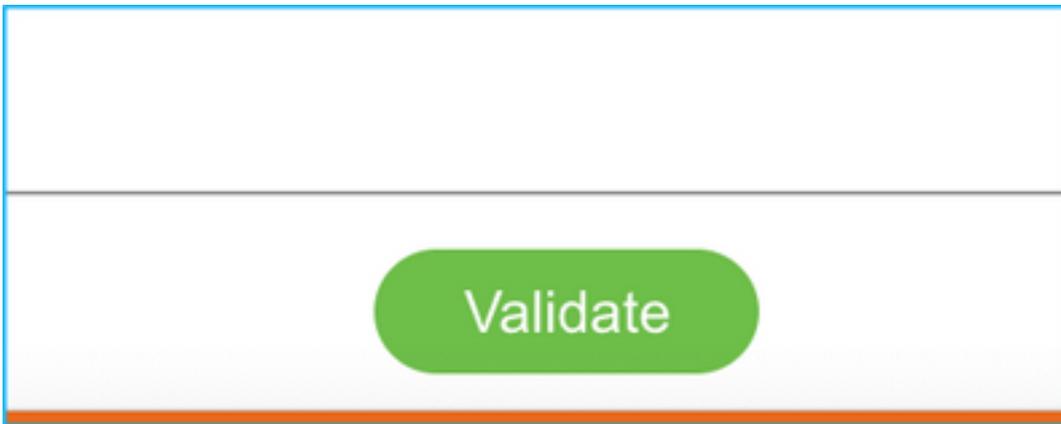


20. Del mismo modo, NAT, objeto de red, objetos de puerto, interfaces, rutas, objetos VPN, túneles VPN de sitio a sitio y otros elementos según su configuración se pueden revisar paso a paso.

Nota: Se notificará a la alerta, como se muestra en la imagen, para actualizar la clave previamente compartida, ya que no se copia en el archivo de configuración de ASA. Seleccione **Acciones > Actualizar clave precompartida** para introducir el valor.



21. Por último, haga clic en el icono **Validar** situado en la parte inferior derecha de la pantalla, como se muestra en la imagen.



22. Una vez que la validación se haya realizado correctamente, haga clic en **Push Configuration** como se muestra en la imagen.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

13 Access Control List Lines	37 Network Objects	14 Port Objects	
2 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

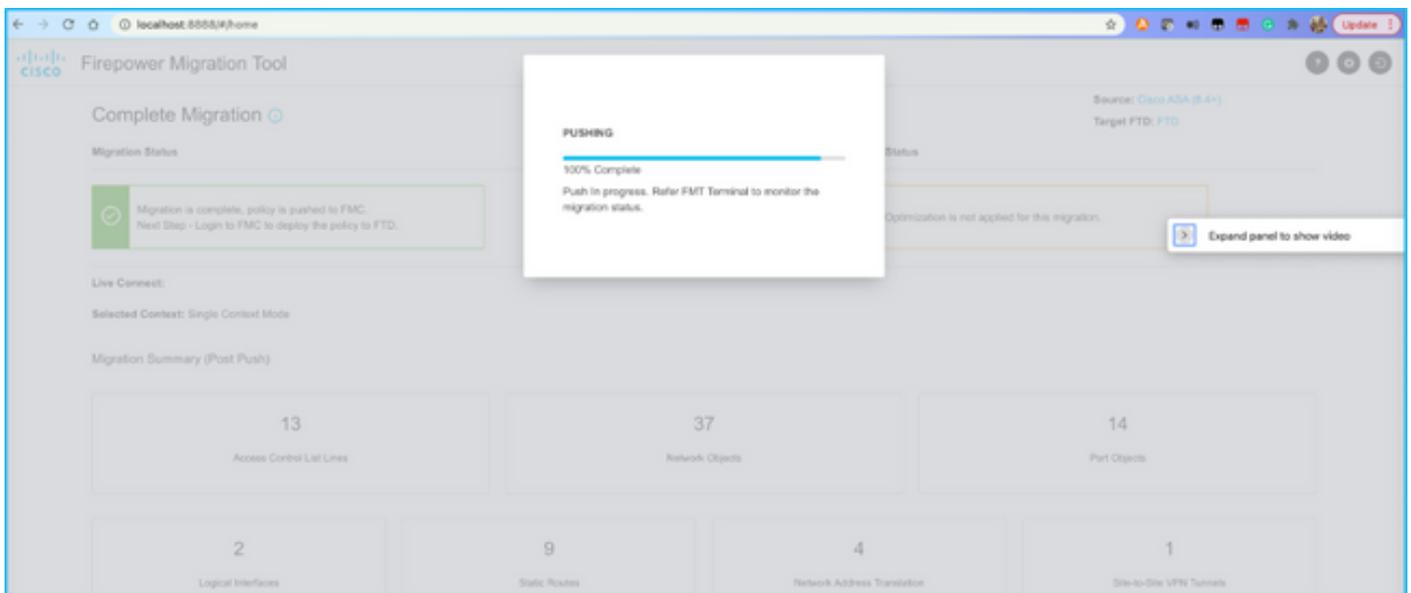
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

PUSHING

0% Complete

Push In progress. Refer FMT Terminal to monitor the migration status.



23. Una vez que la migración se ha realizado correctamente, el mensaje que se mostrará se muestra en la imagen.

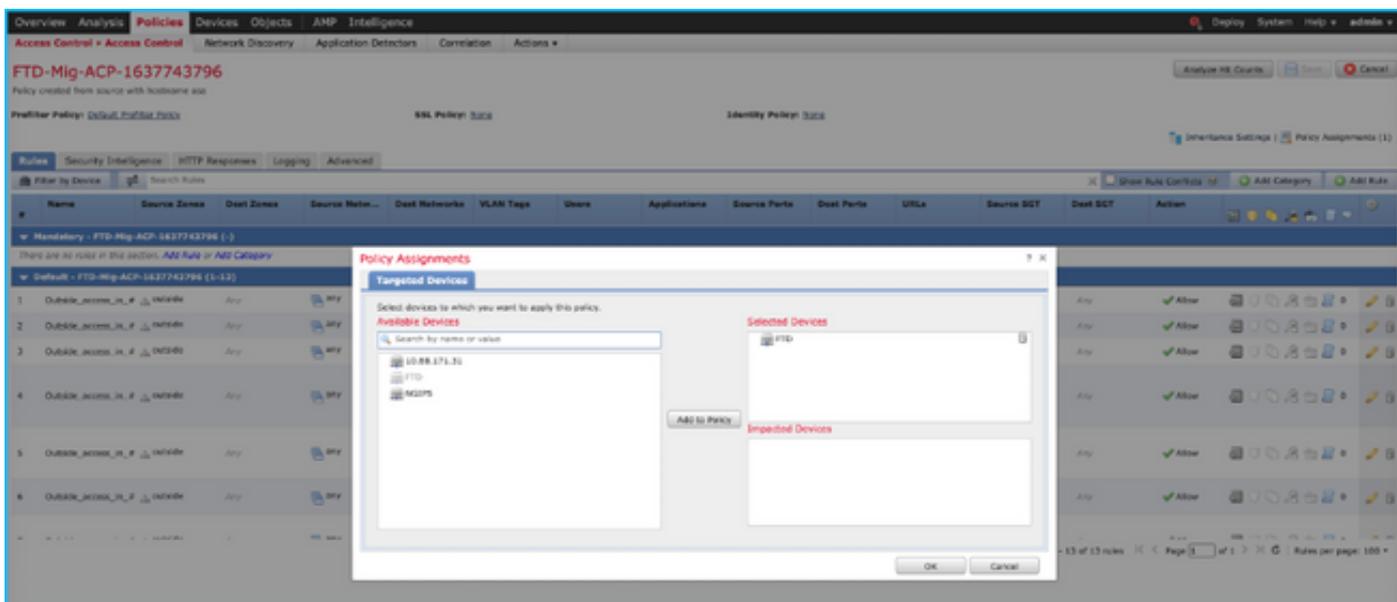
Nota: Si la migración no se realiza correctamente, haga clic en **Descargar informe** para ver el informe posterior a la migración.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

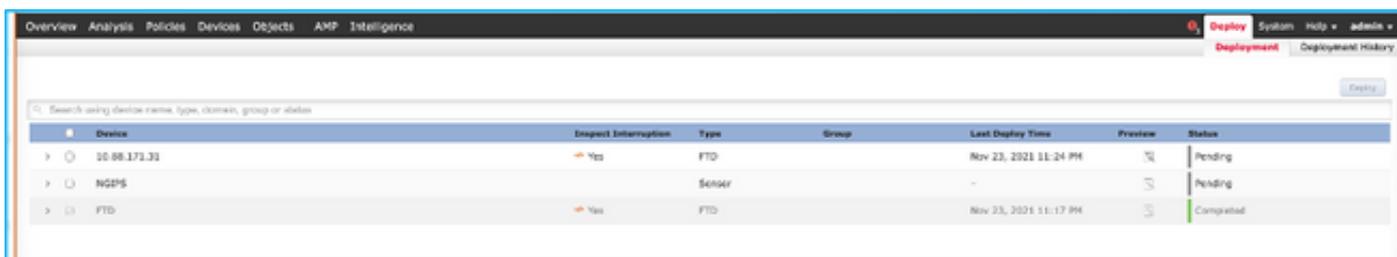
Validación en el FMC.

1. Navegue hasta **Políticas > Control de acceso > Directiva de control de acceso > Asignación de política** para confirmar que el FTD seleccionado se rellena.



Nota: La política de control de acceso de migración tendría un nombre con el prefijo **FTD-Mig-ACP**. Si no se ha seleccionado ningún FTD en el paso 2.8, el FTD debe seleccionarse en el FMC.

2. Empuje la política al FTD. Navegue hasta **Implementar > Implementación > Nombre FTD > Implementar** como se muestra en la imagen.



Errores conocidos relacionados con la herramienta de migración de Firepower

- Id. de error de Cisco [CSCwa56374](#) - La herramienta FMT se cuelga en la página de asignación de zona con error con uso de memoria alto
- Id. de error de Cisco [CSCvz88730](#): falla de inserción de interfaz para el tipo de interfaz de administración de canal de puerto FTD
- Id. de error de Cisco [CSCvx21986](#) - Migración de canal de puerto a plataforma de destino - No se soporta FTD virtual
- Id. de bug Cisco [CSCvy63003](#) - La herramienta de migración debe inhabilitar la función de interfaz si FTD ya forma parte del clúster
- Id. de error de Cisco [CSCvx08199](#) - La ACL debe dividirse cuando la referencia de la aplicación es superior a 50

Información Relacionada

- [Migración del firewall ASA a la defensa frente a amenazas con la herramienta de migración](#)

del firewall

- Soporte Técnico y Documentación - Cisco Systems