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

Contenido

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

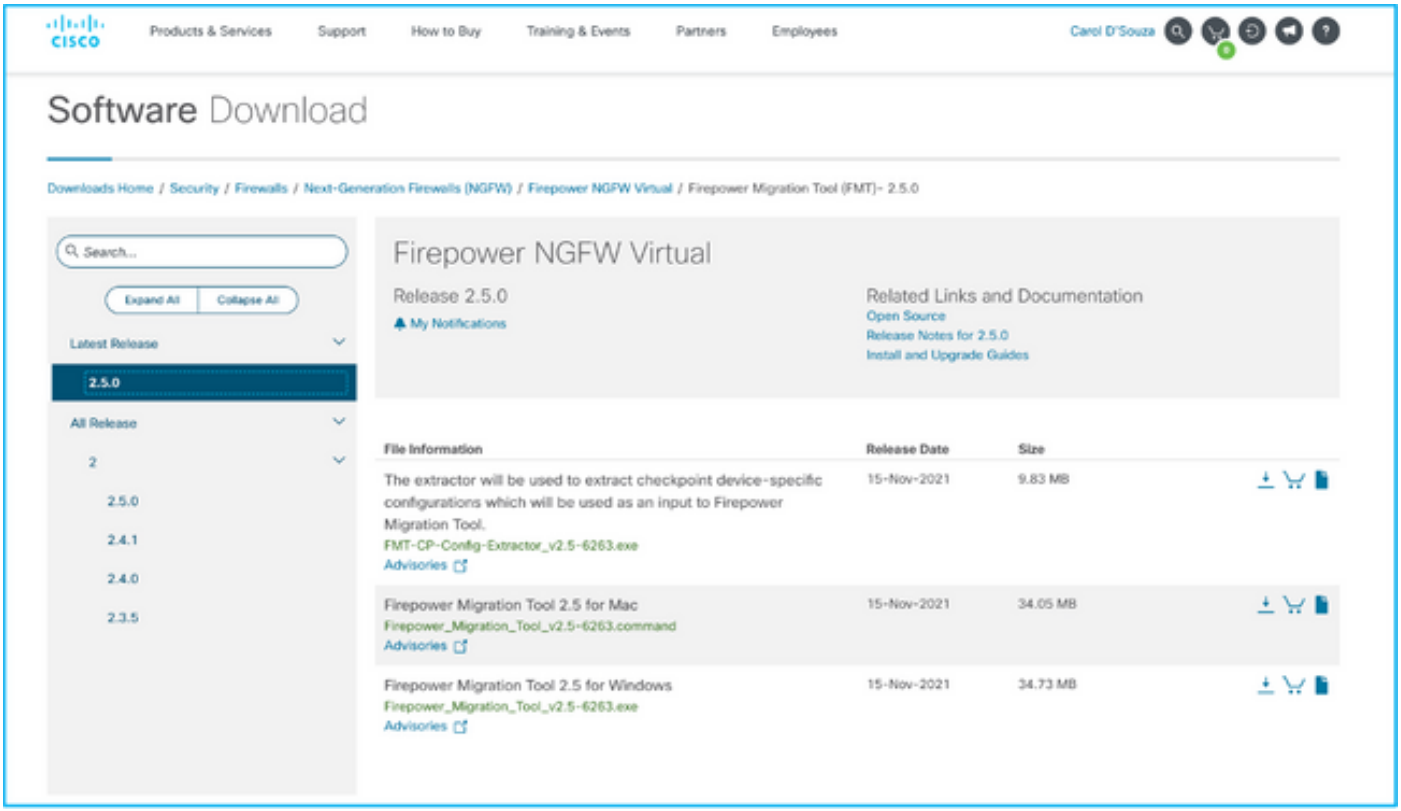
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

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.



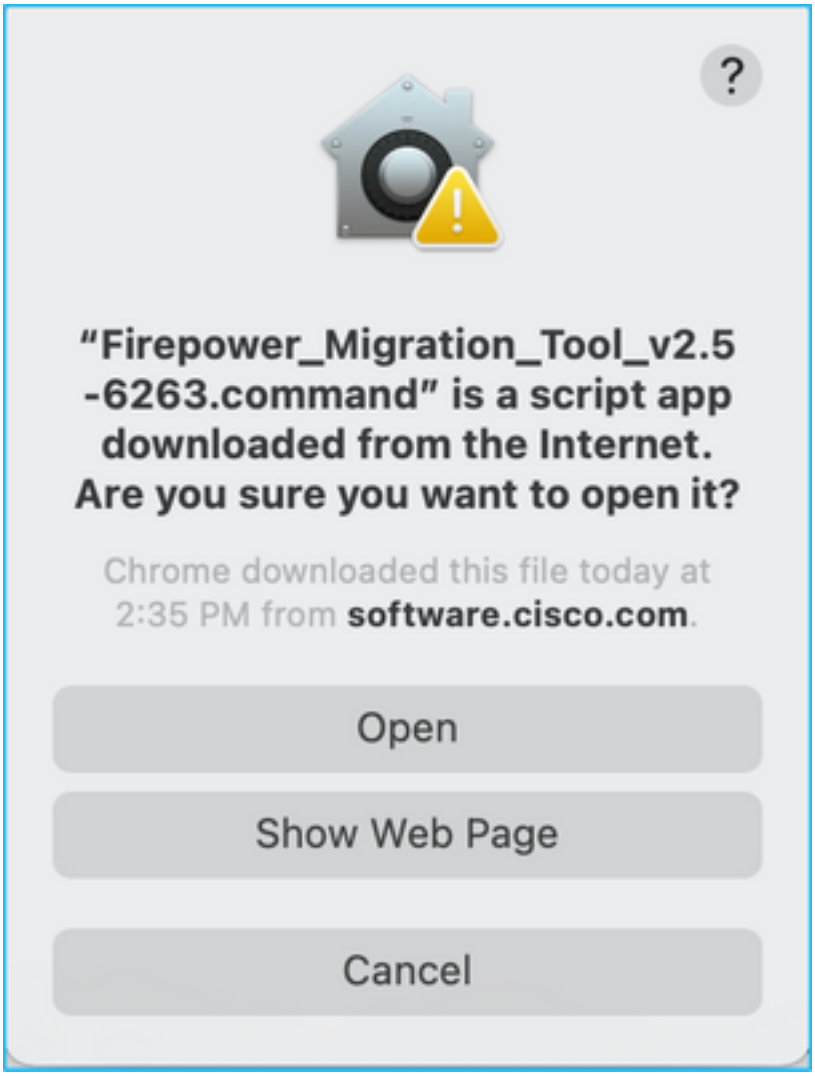
2. Revise y verifique los requisitos en la sección Pautas y limitaciones para la Herramienta de Migración de Firepower.

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.

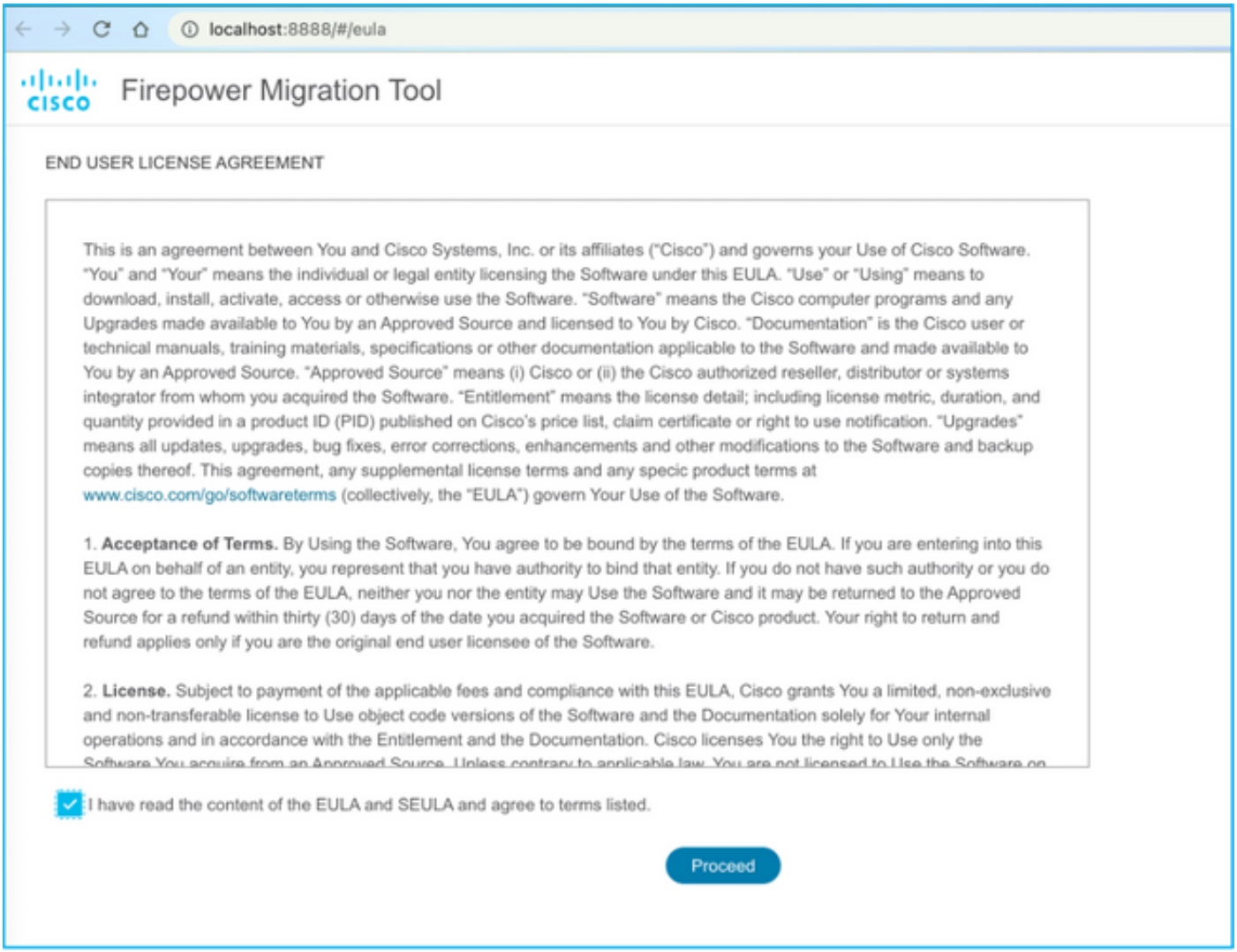
```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command

[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: homepath 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 -
```

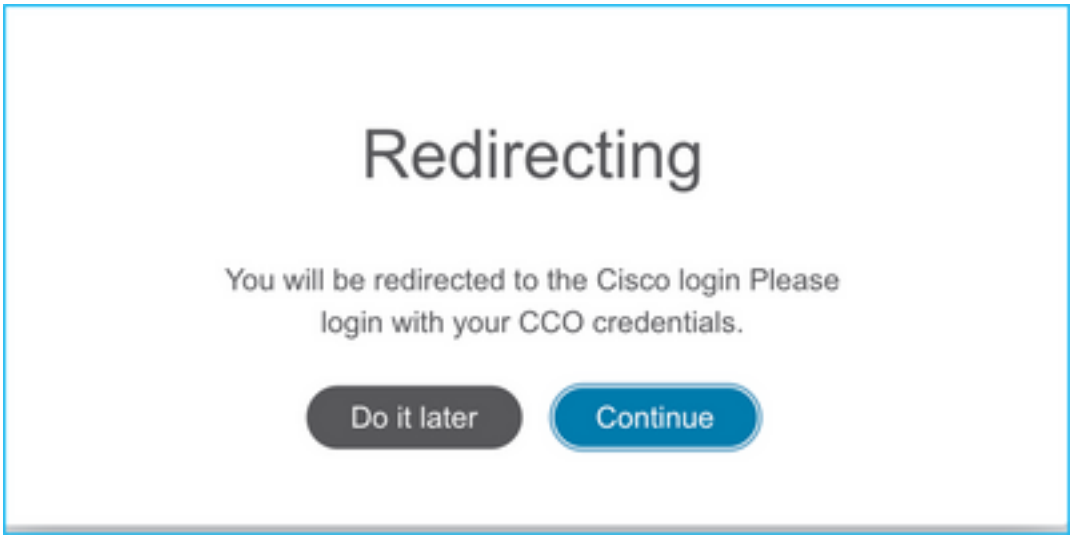
4. B Para Windows: haga doble clic en Firepower Migration Tool para iniciarla en un navegador de Google Chrome.

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

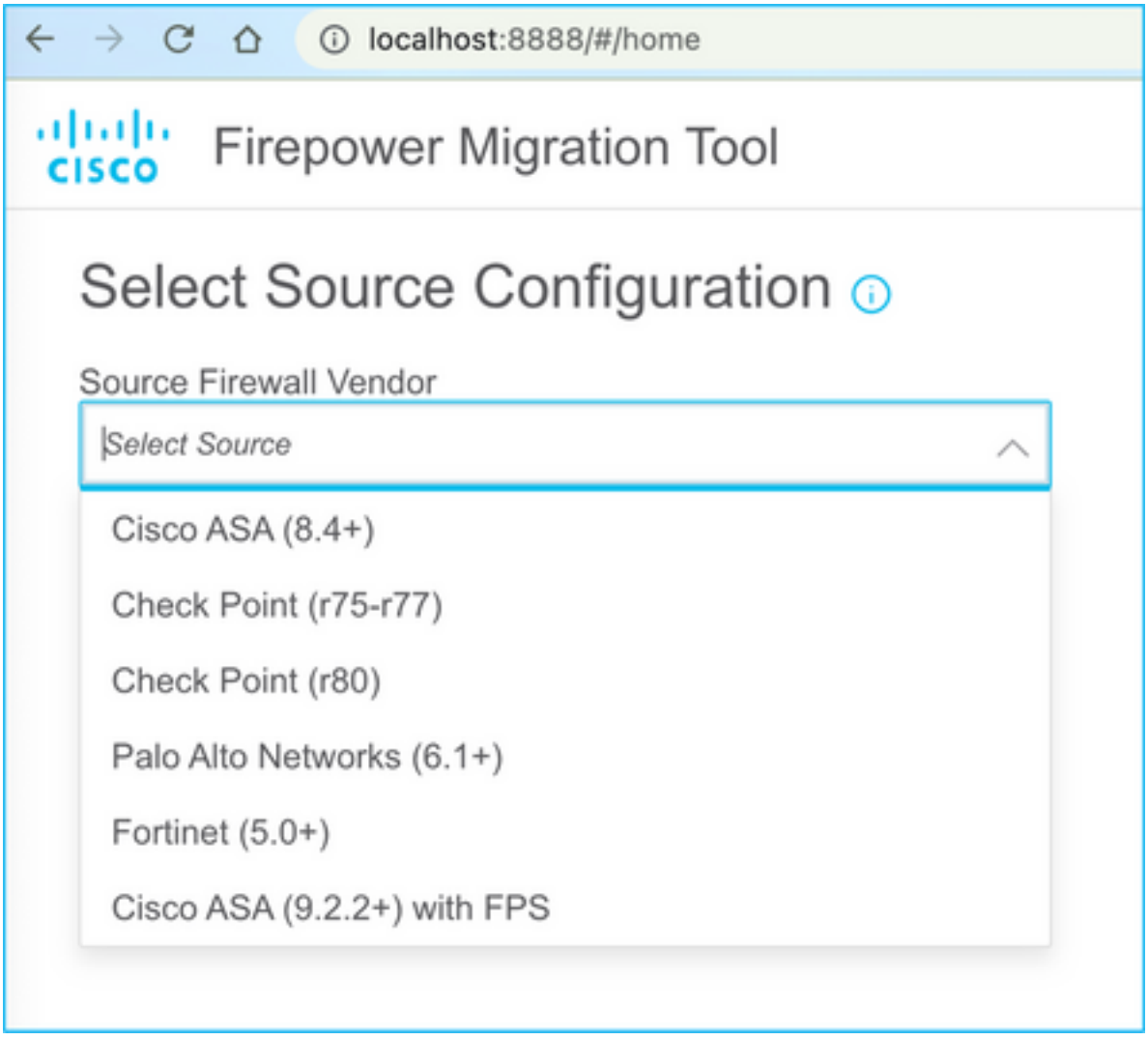


6. En la página de inicio de sesión de Firepower Migration Tool, haga clic en el enlace de inicio de sesión con CCO para iniciar sesión en su cuenta de Cisco.com con sus credenciales de inicio de sesión único.

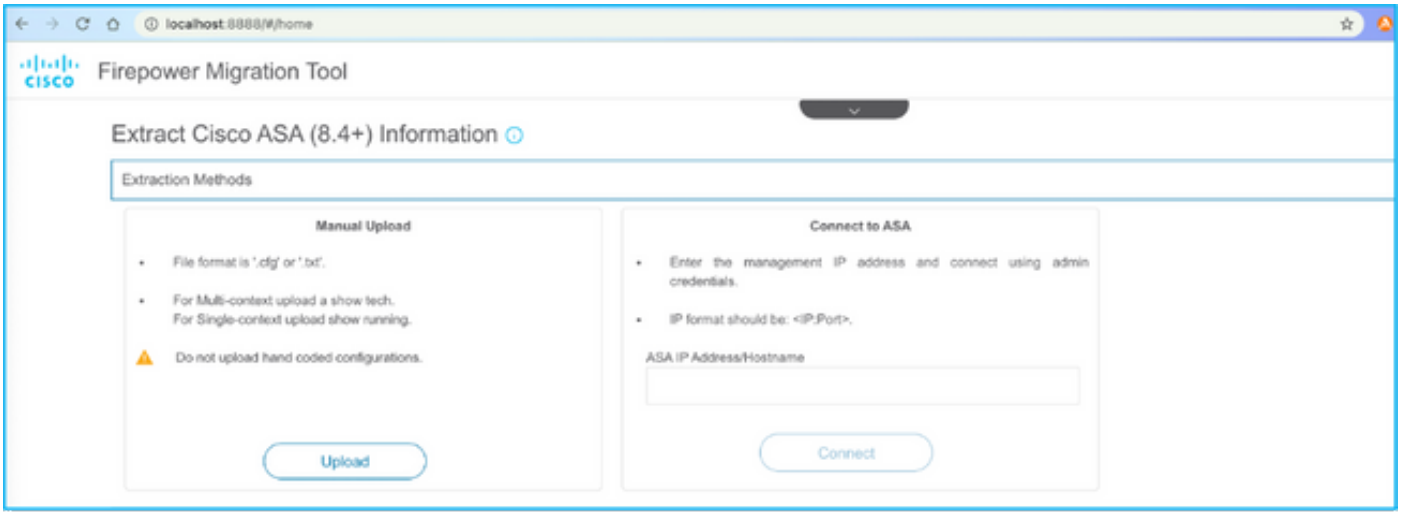
Nota: Si no tiene una cuenta de Cisco.com, créela en la página de inicio de sesión de Cisco.com. Inicie sesión con las siguientes credenciales predeterminadas: Nombre de usuario—Contraseña de administrador—Admin123.



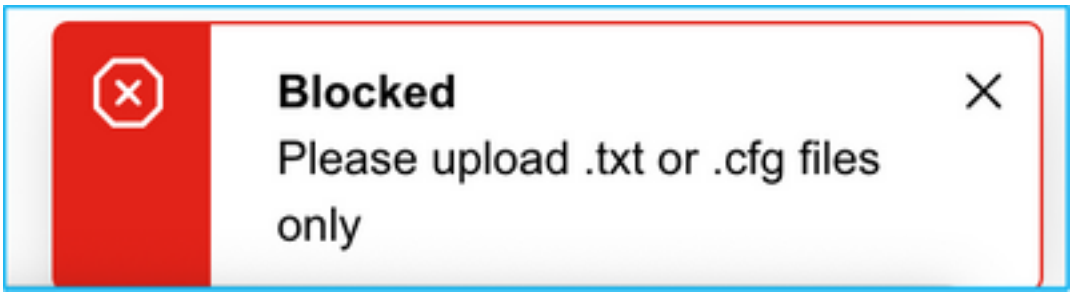
7. Seleccione la configuración de origen. En esta situación, es Cisco ASA (8.4+).

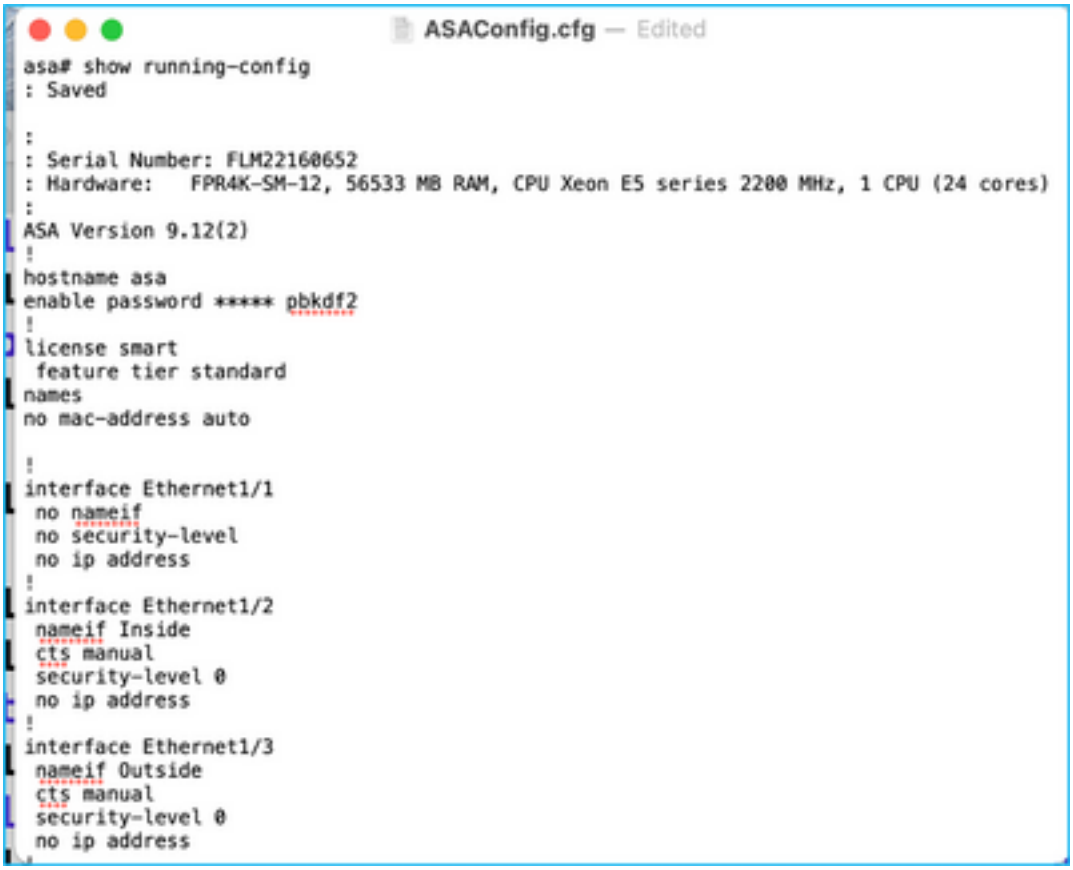


8. Seleccione Carga manual si no tiene conectividad con el ASA. De lo contrario, puede recuperar la configuración en ejecución del ASA e introducir la dirección IP de administración y los detalles de inicio de sesión. En nuestra situación, se realizó una carga manual.



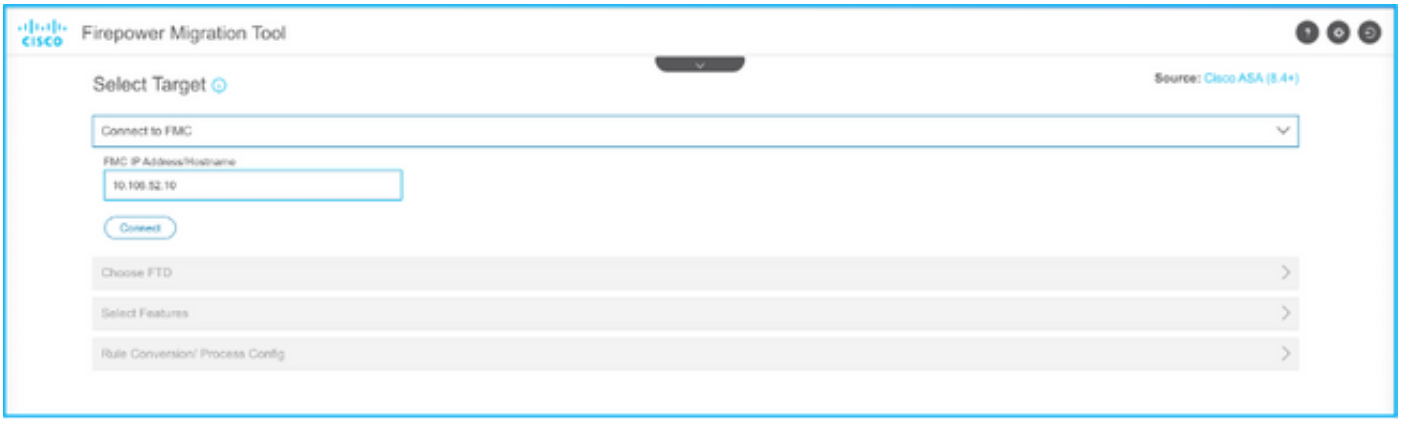
Nota: Este error aparece si el archivo no está soportado. Asegúrese de cambiar el formato a texto sin formato. (Se ha visto un error a pesar de tener la extensión .cfg).



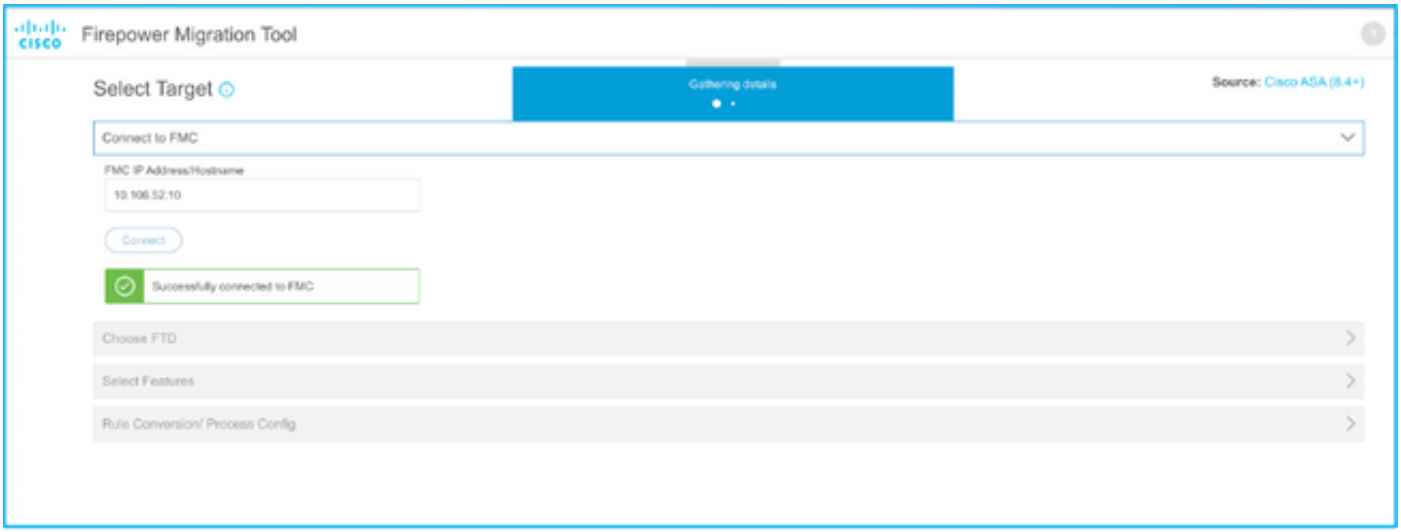


9. Después de cargar el archivo, los elementos se analizarán proporcionando un resumen como se muestra en la imagen:

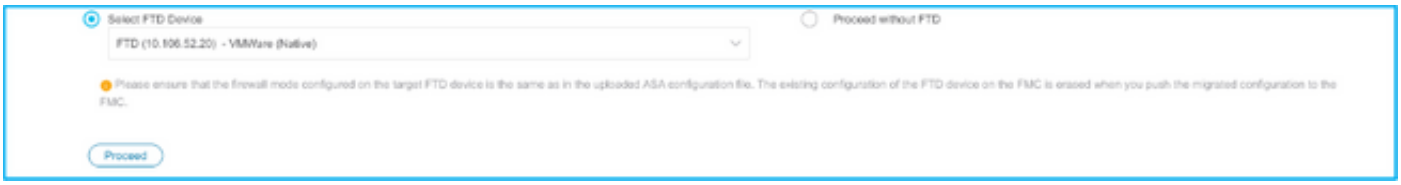
10. Introduzca la IP de FMC y las credenciales de inicio de sesión a las que se migrará la configuración de ASA. Asegúrese de que la IP de FMC esté accesible desde su estación de trabajo.



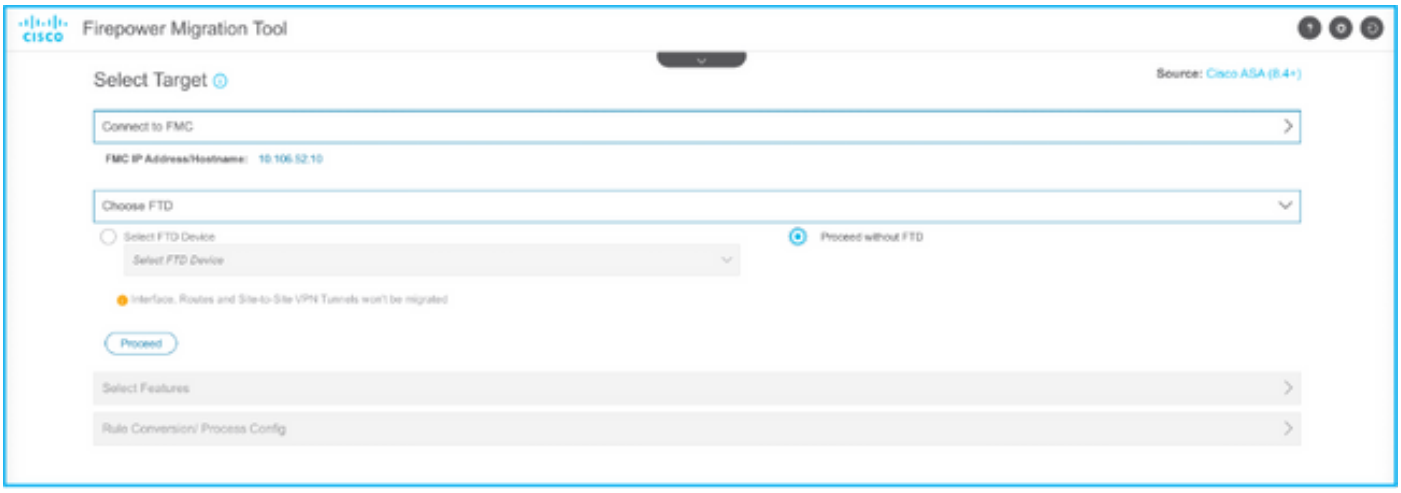
11. Una vez conectado el FMC, se mostrarán los FTD administrados que se encuentran debajo.



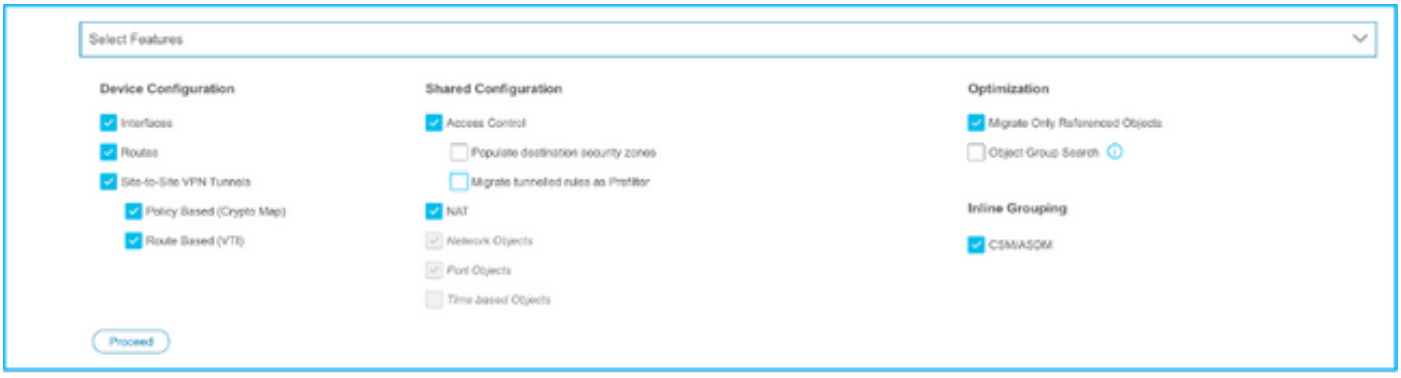
12. Elija el FTD al que desea realizar la migración de la configuración ASA.



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.

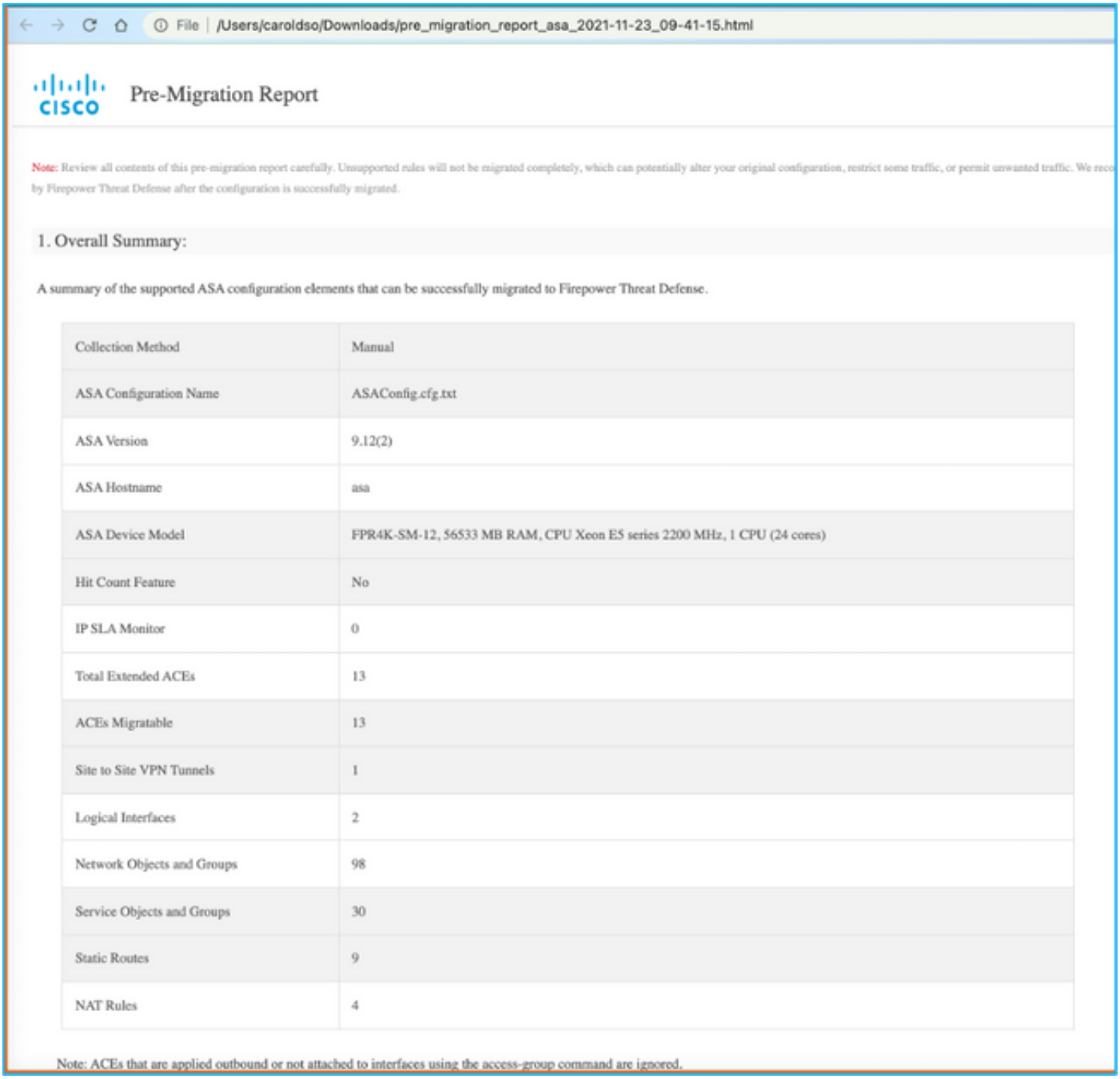


13. Seleccione las funciones que se deben migrar como se muestra en la imagen.



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

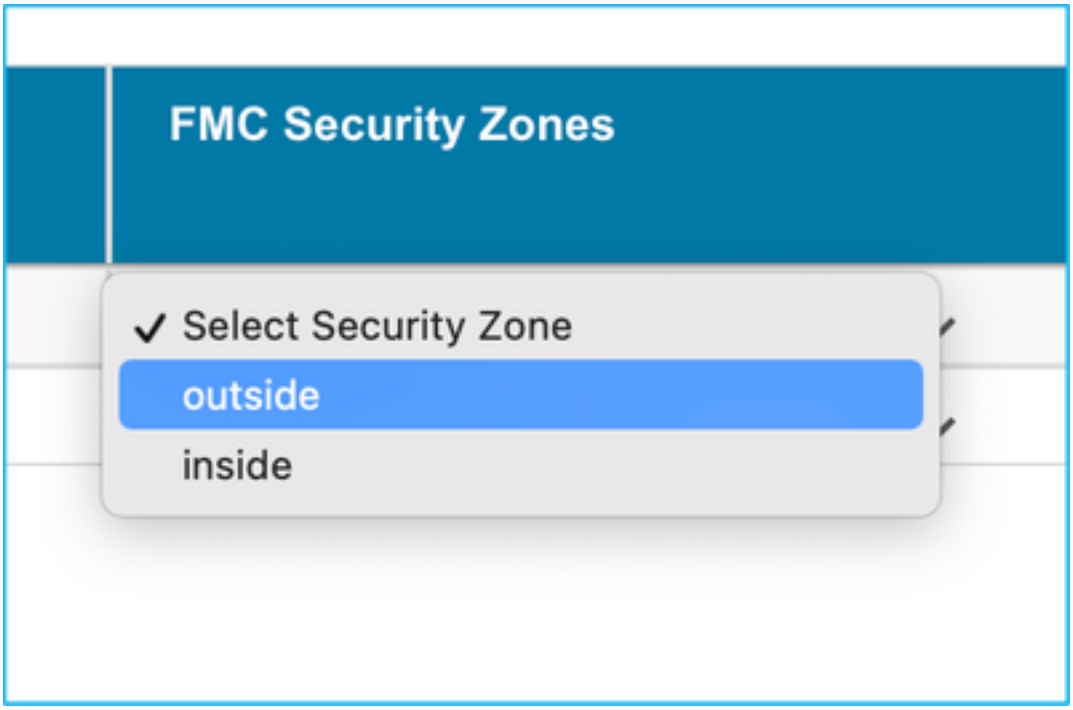
15. Haga clic en **Descargar informe** visto anteriormente para ver el informe previo a la migración, como se muestra en la imagen.



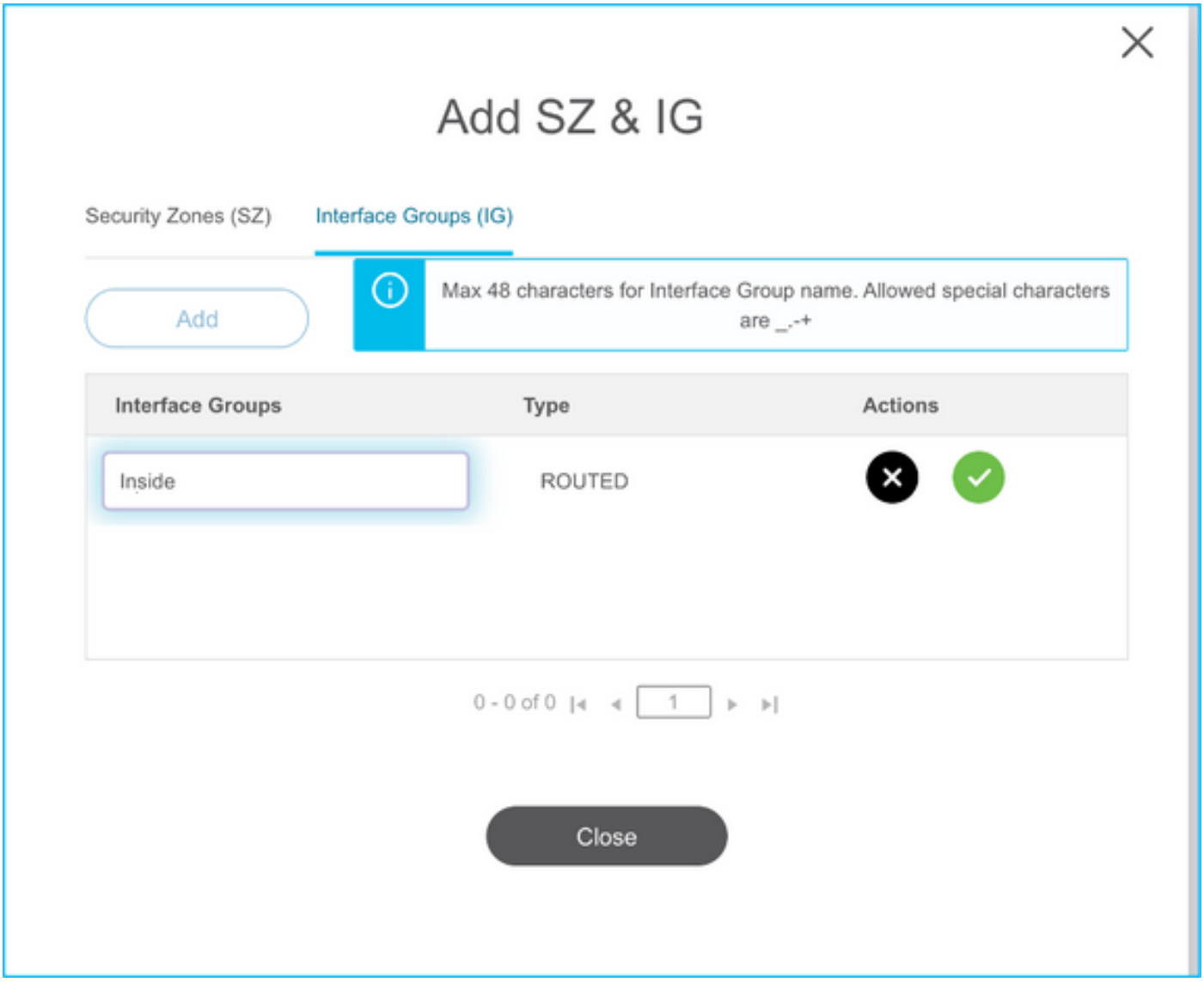
16. Asigne las interfaces ASA a las interfaces FTD según se requiera, como se muestra en la imagen.

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

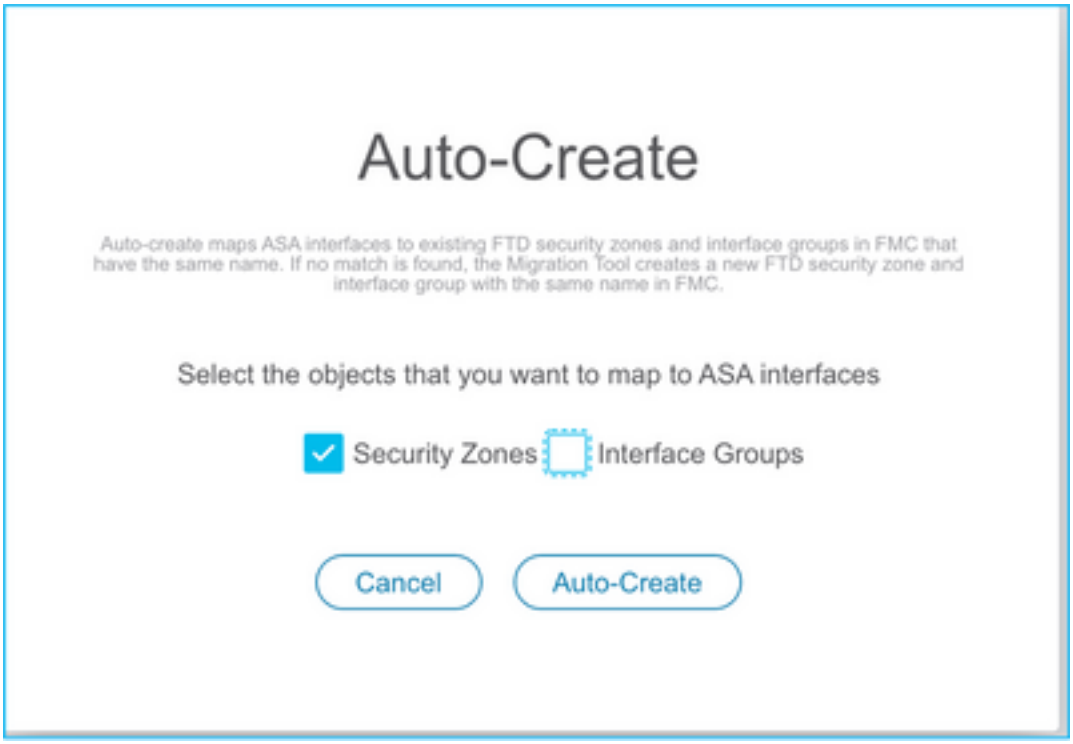
A. Si FMC tiene zonas de seguridad y grupos de interfaz ya creados, puede seleccionarlos según sea necesario:



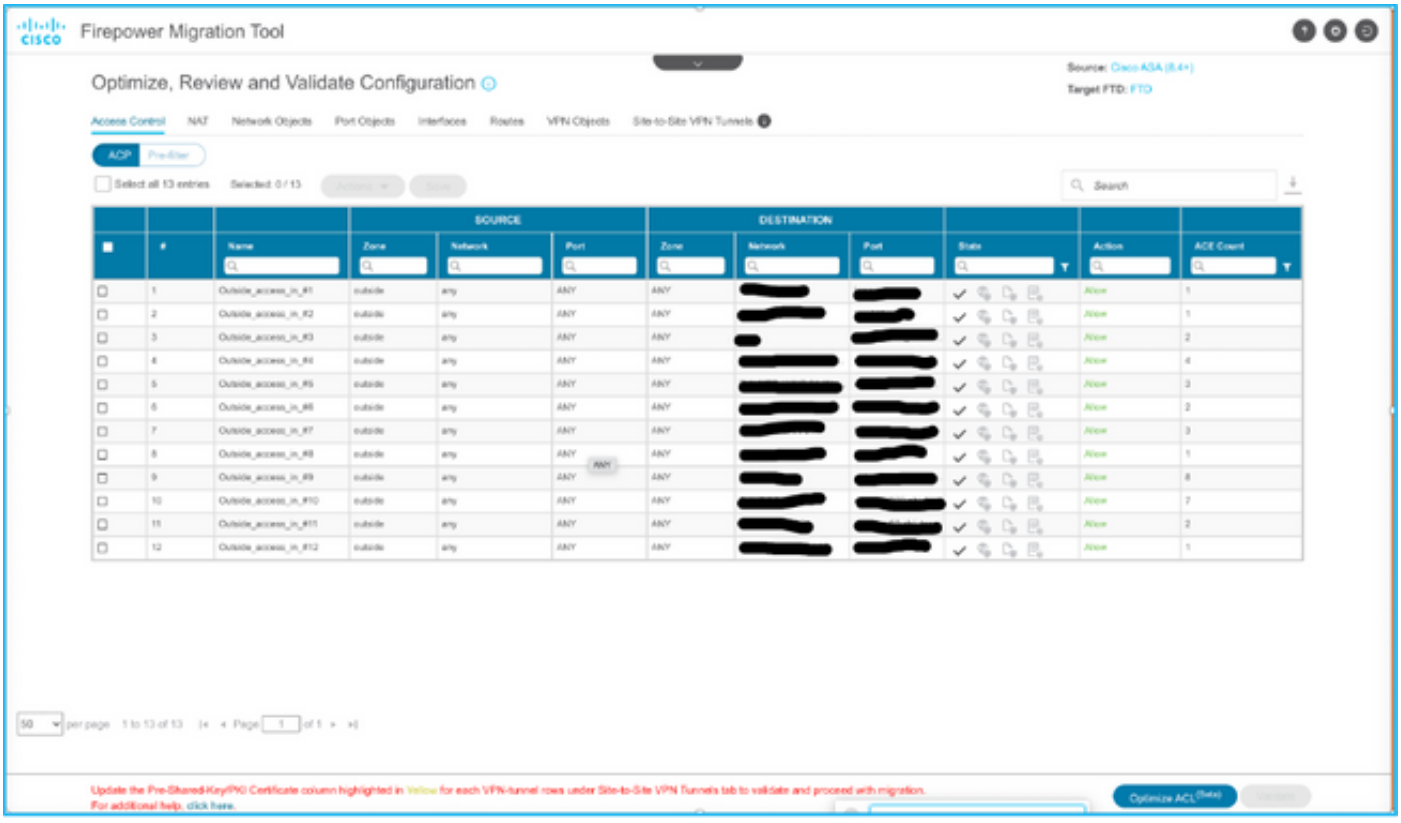
B Si hay necesidad de crear zonas de seguridad y un grupo de interfaces, haga clic en **Agregar SZ e IG** como se muestra en la imagen.



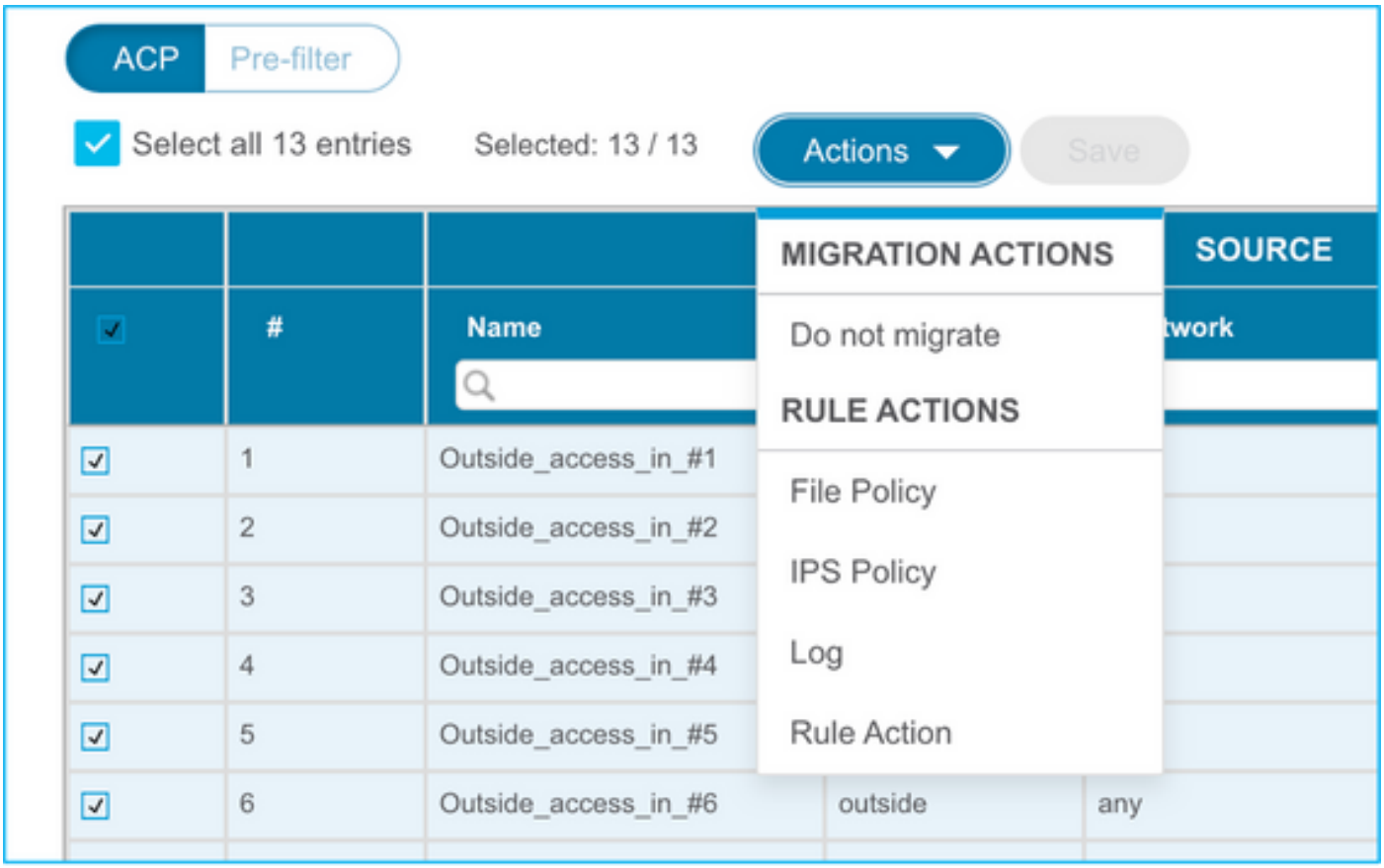
C. De lo contrario, puede optar por la opción **Creación automática** que creará zonas de seguridad y grupos de interfaz con el nombre **ASA Logical interface_sz** y **ASA Logical interface_ig** respectivamente.



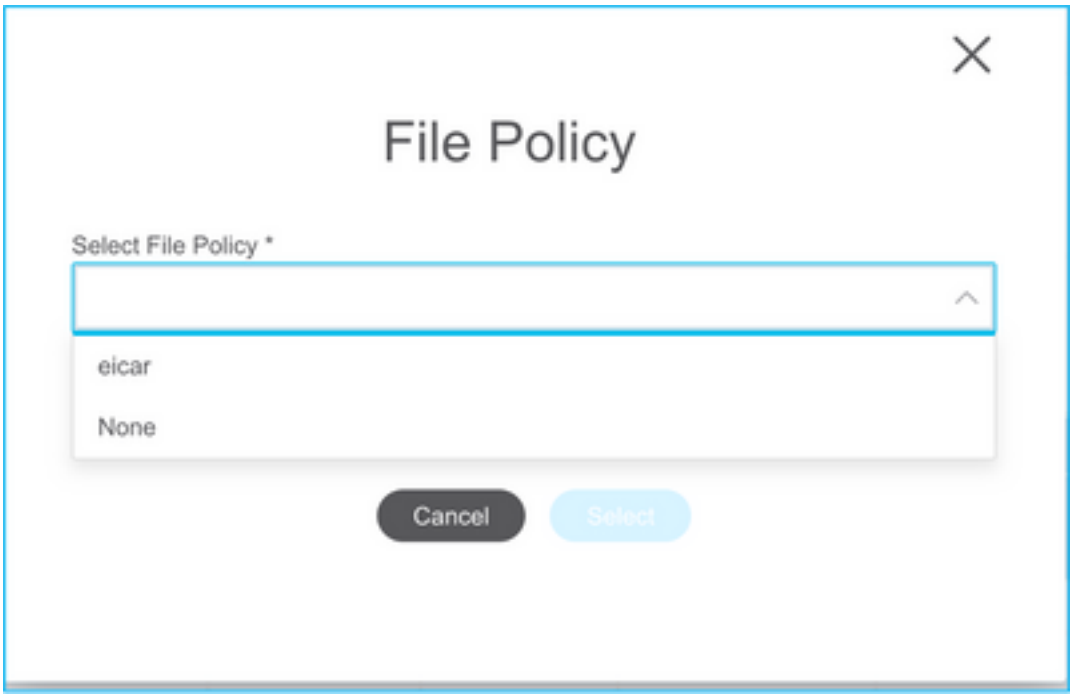
18. Revise y valide cada uno de los elementos FTD creados. Las alertas se ven en rojo como se muestra en la imagen.



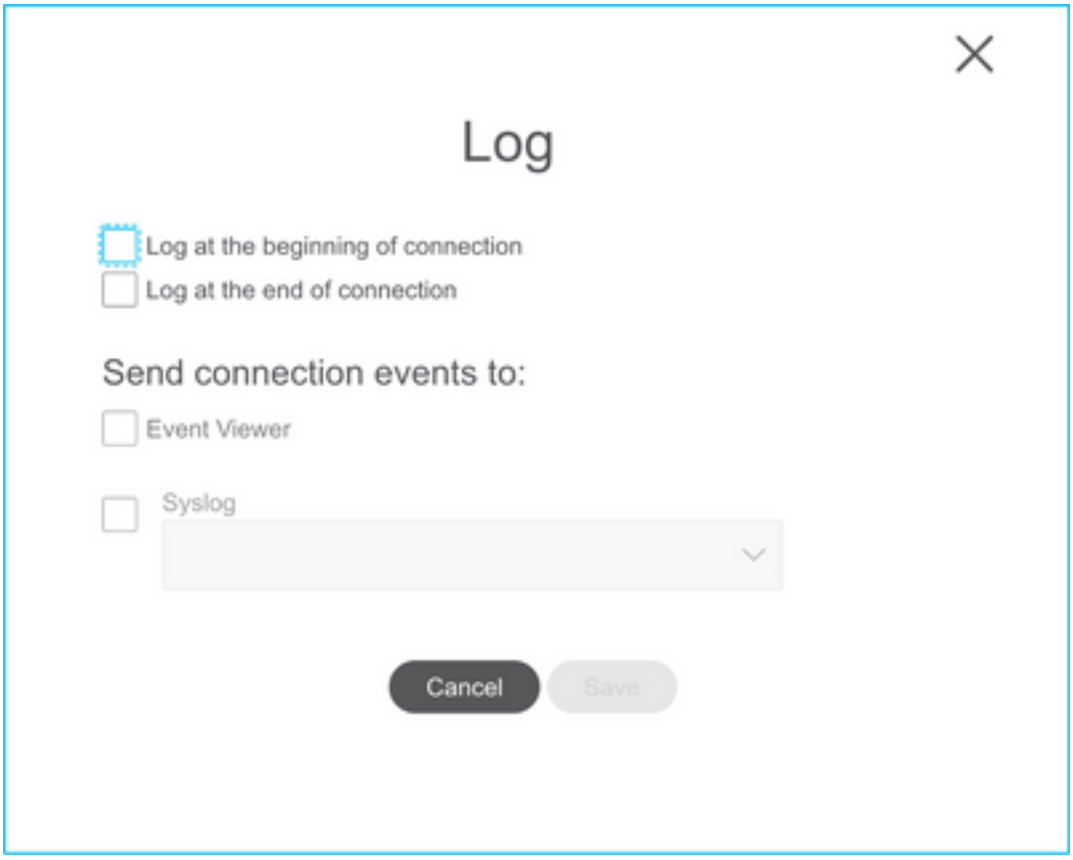
19. Las acciones de migración se pueden seleccionar como se muestra en la imagen si desea editar alguna regla. Las funciones de FTD de agregar archivos y la política IPS se pueden realizar en este paso.



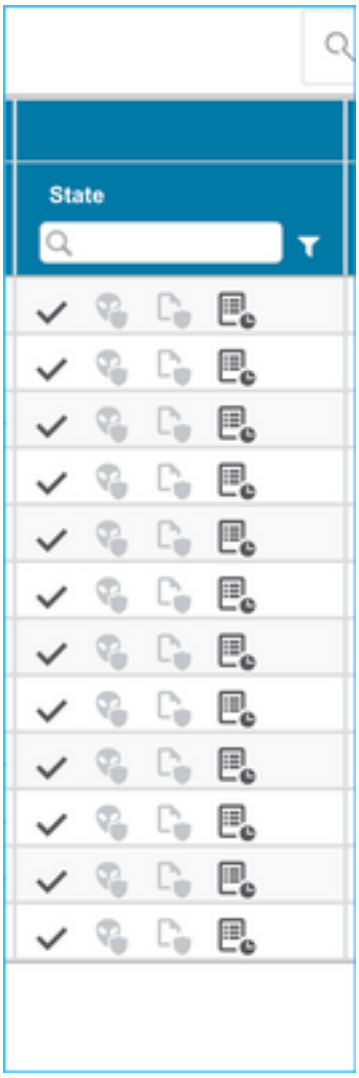
Nota: Si las políticas de archivos ya existen en el FMC, se rellenarían como se muestra en la imagen. Lo mismo se aplica a las políticas IPS junto con las políticas predeterminadas.



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.

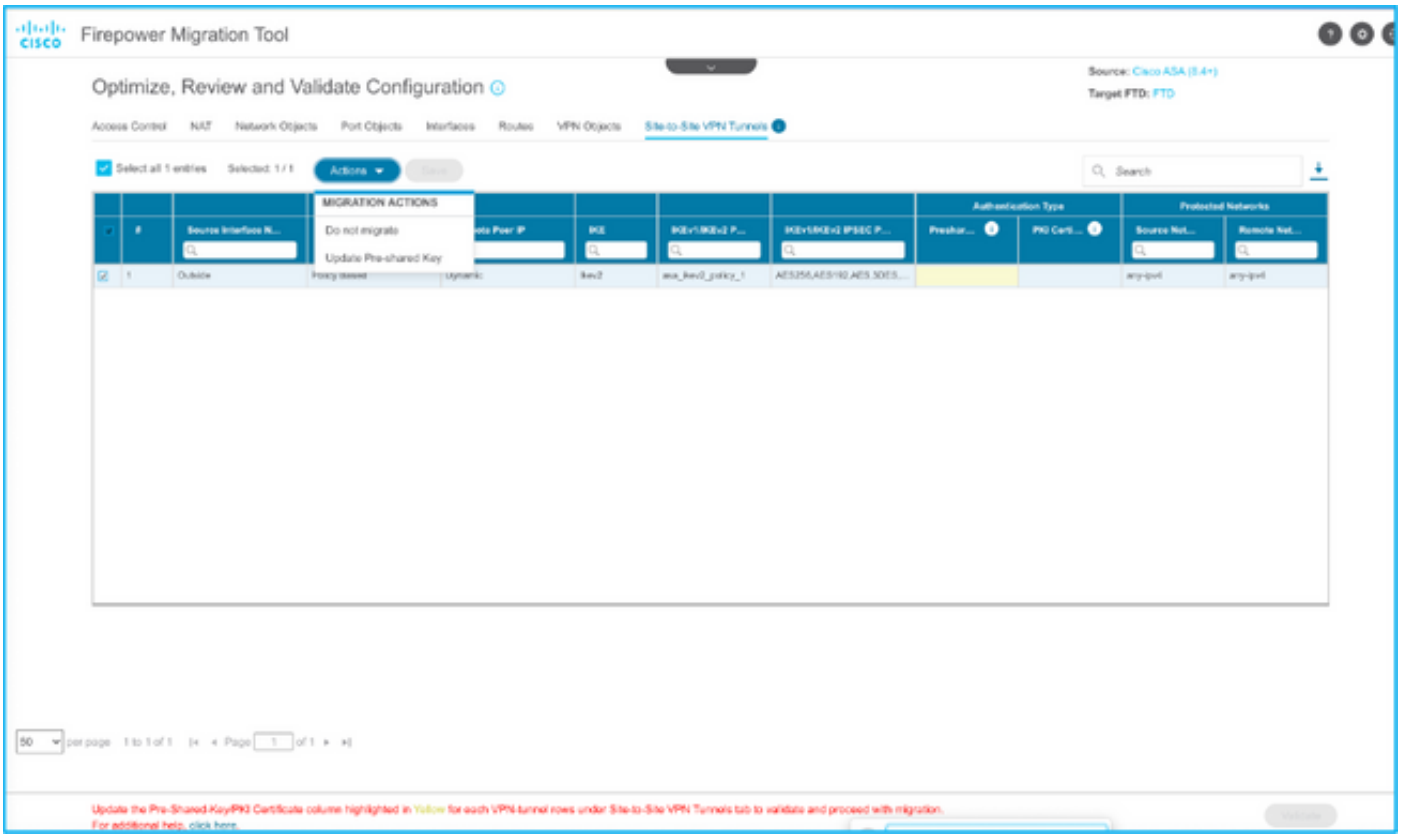


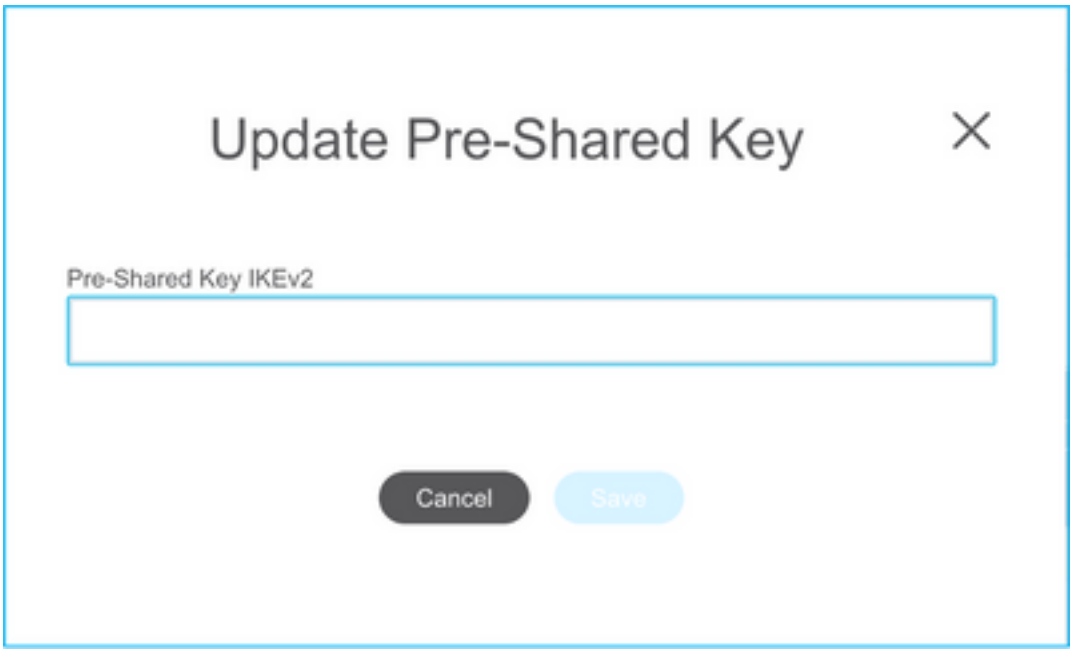
Las acciones de regla seleccionadas se resaltarán en consecuencia para cada regla.



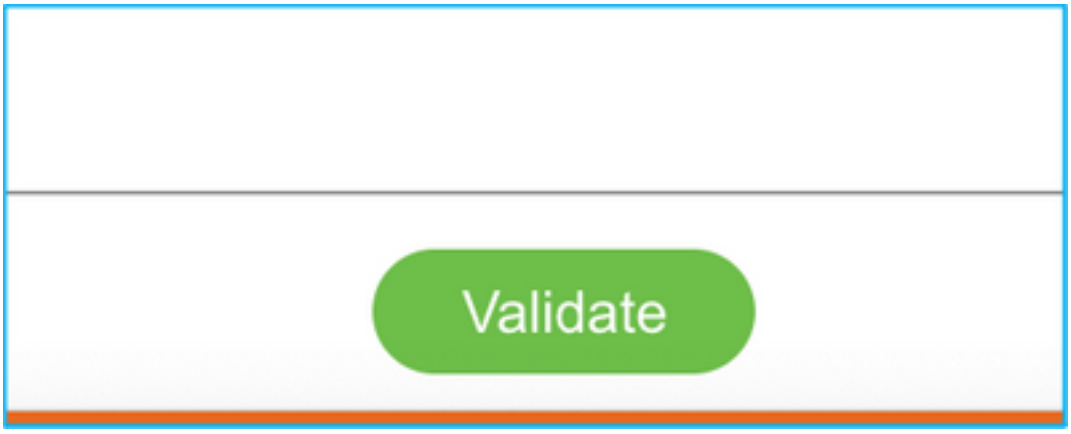
20. Del mismo modo, NAT, objeto de red, objetos de puerto, interfaces, rutas, objetos VPN, túneles VPN de sitio a sitio y otros elementos según su configuración se pueden revisar paso a paso.

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.

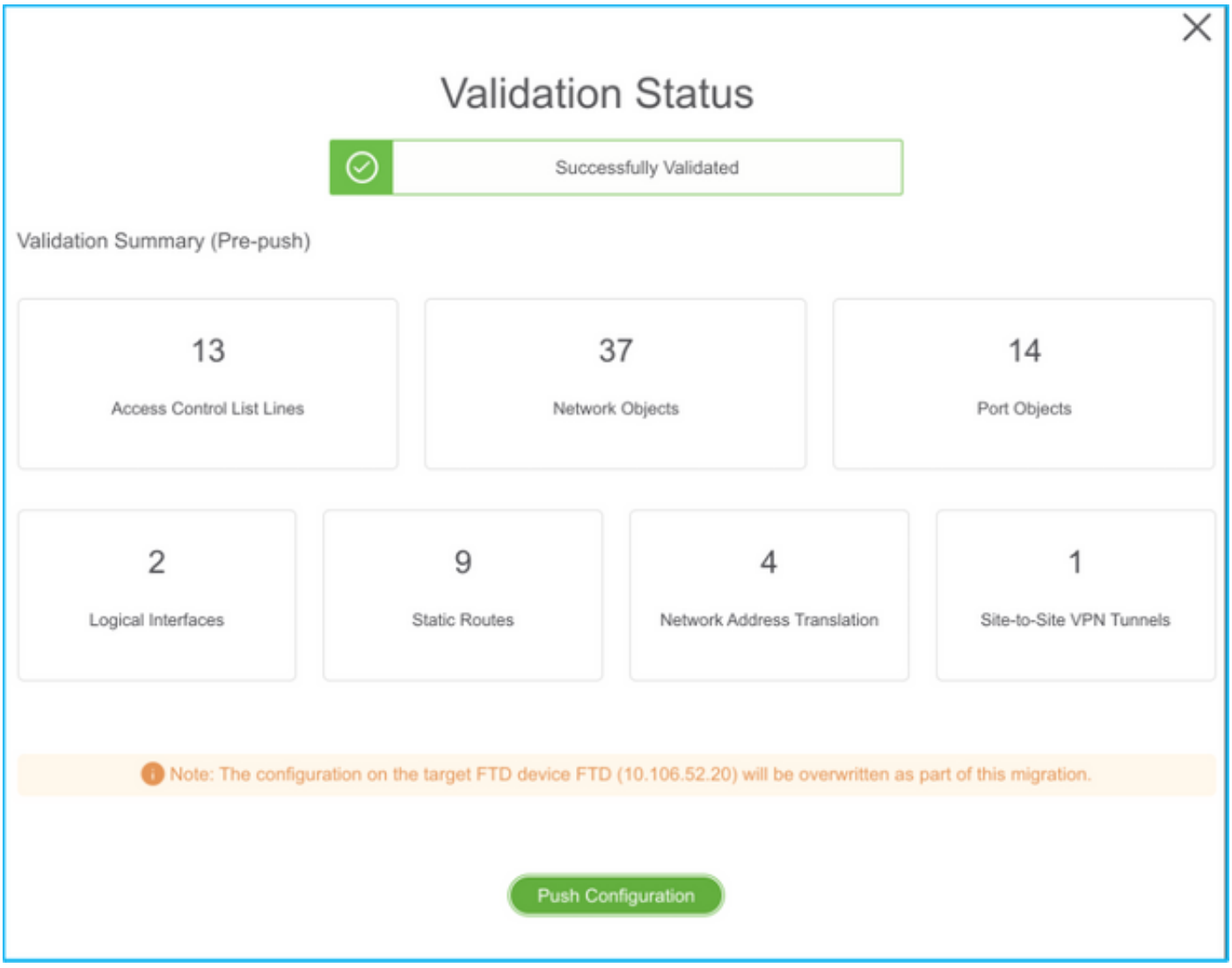


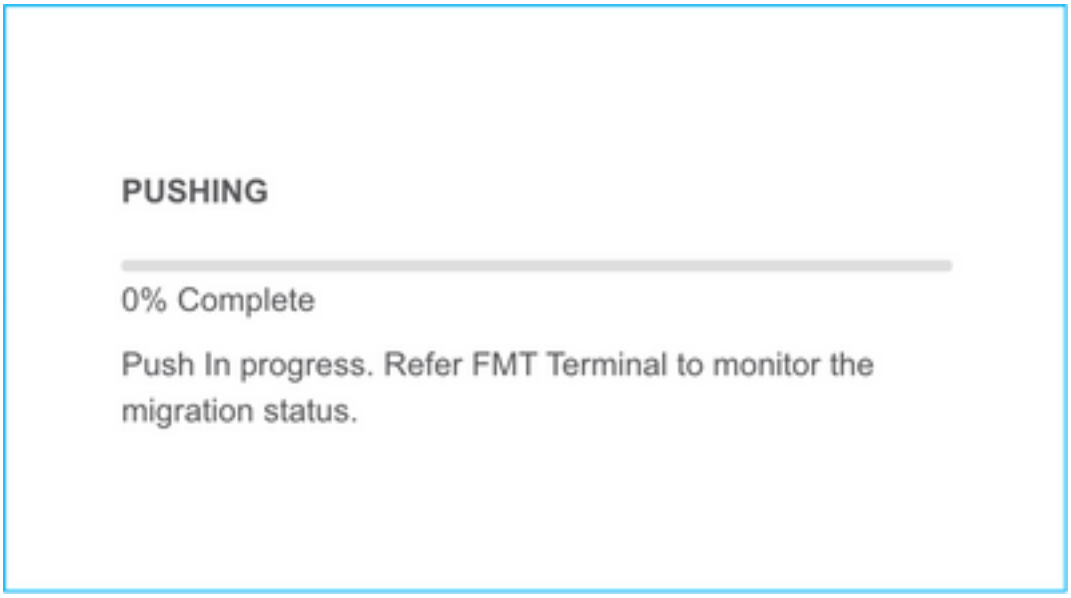


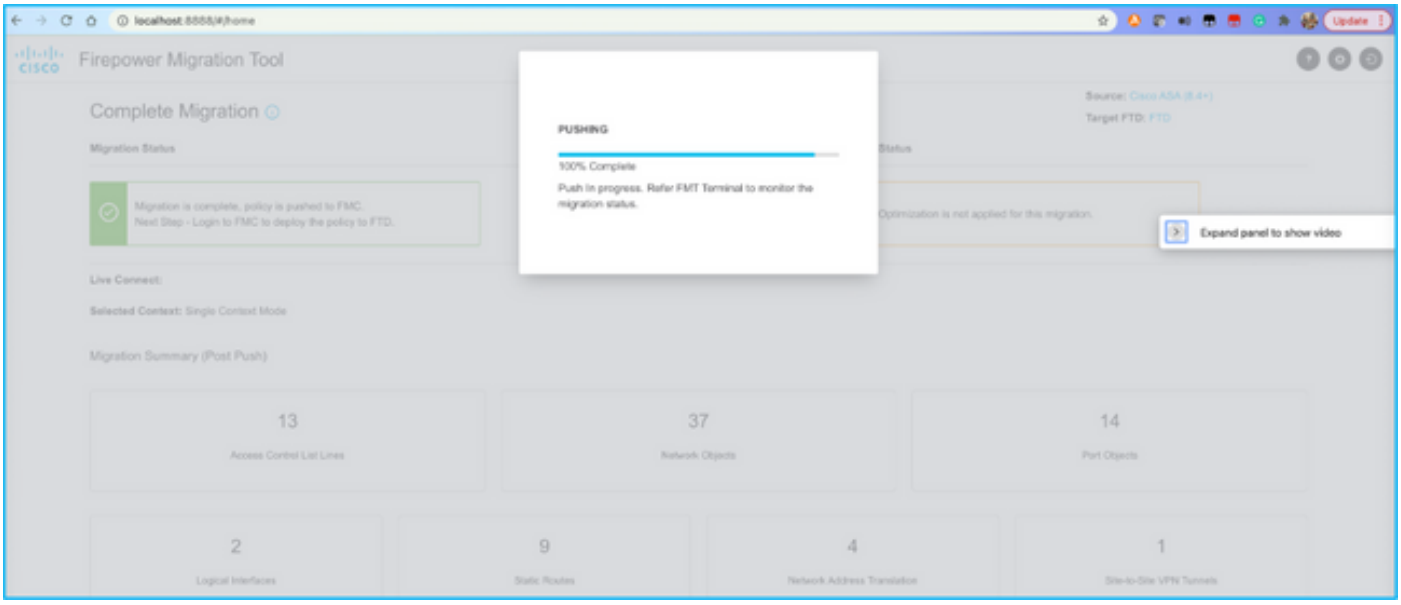
21. Por último, haga clic en el icono **Validar** situado en la parte inferior derecha de la pantalla, como se muestra en la imagen.



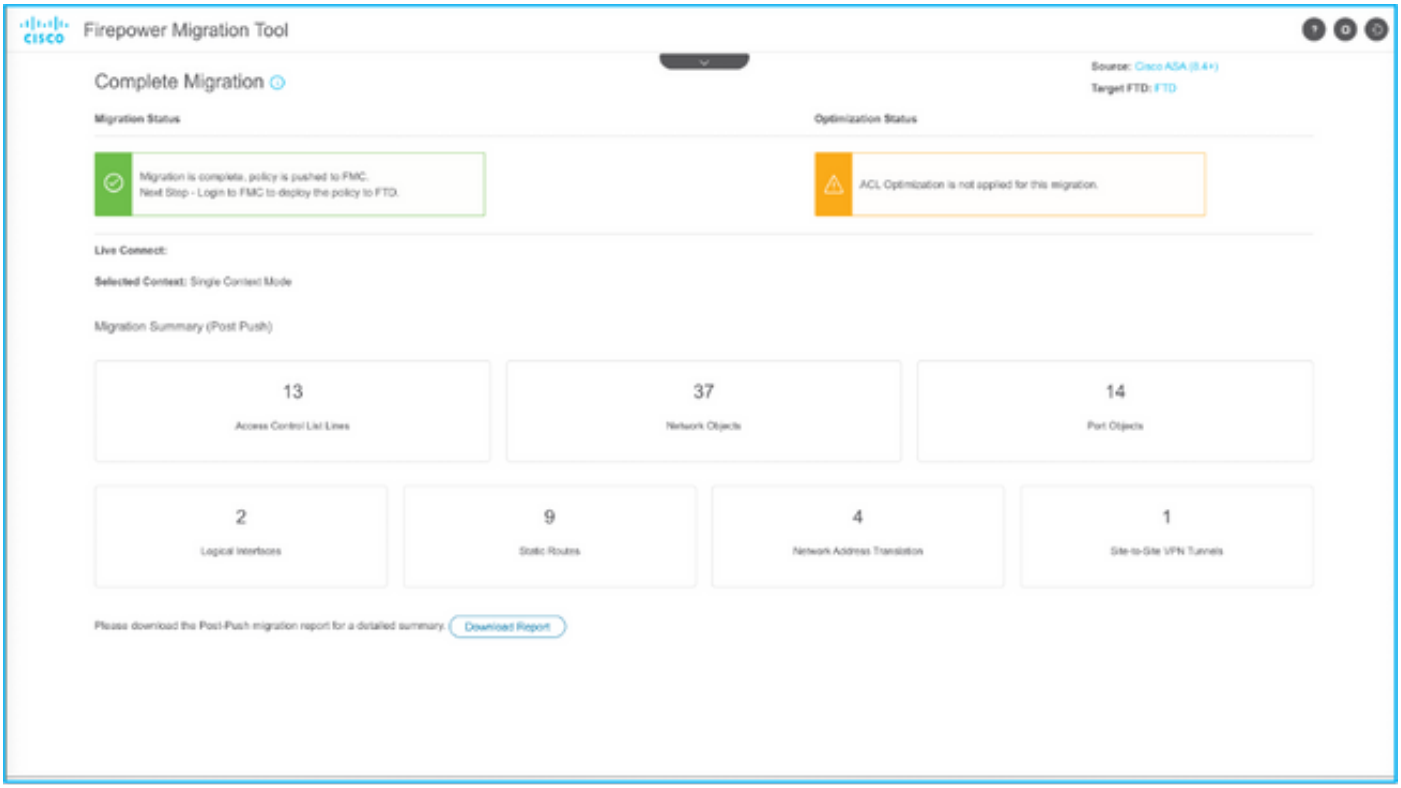
22. Una vez que la validación se haya realizado correctamente, haga clic en **Push Configuration** como se muestra en la imagen.



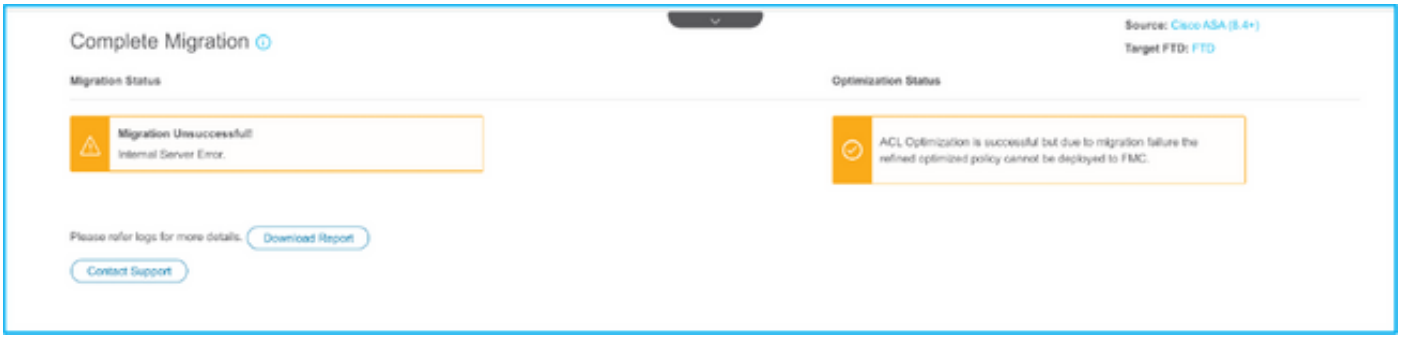




23. Una vez que la migración se ha realizado correctamente, el mensaje que se mostrará se muestra en la imagen.



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

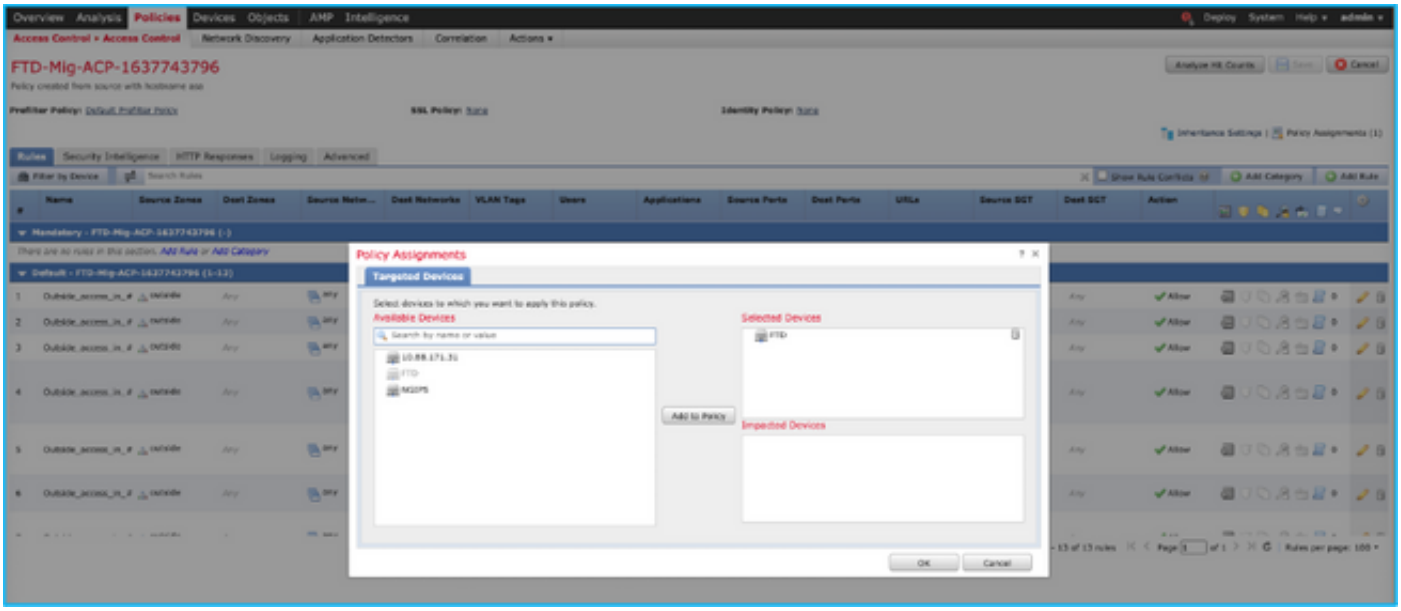


Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

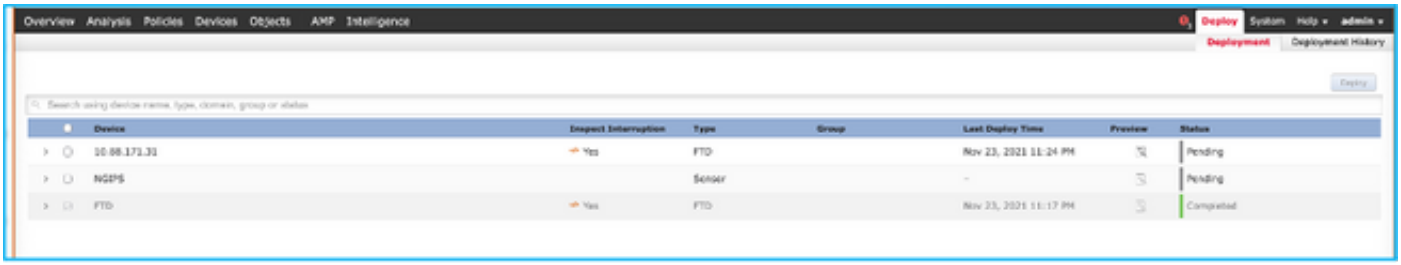
Validación en el FMC.

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