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 transfiérala 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).

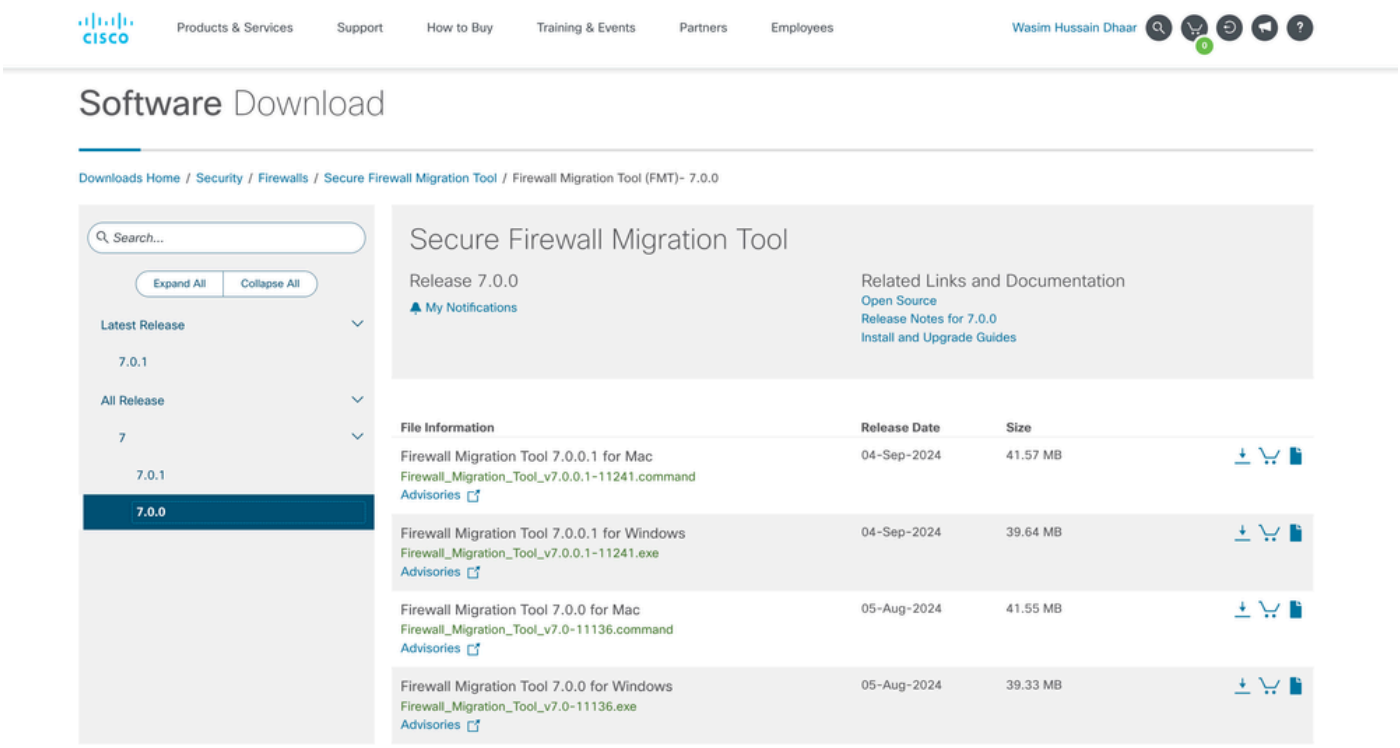
a-Dap.xml y Data.xml se deben cargar en el centro de gestión desde la herramienta de migración de Secure Firewall en la sección Revisión y validación > VPN de acceso remoto > Archivo AnyConnect.

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

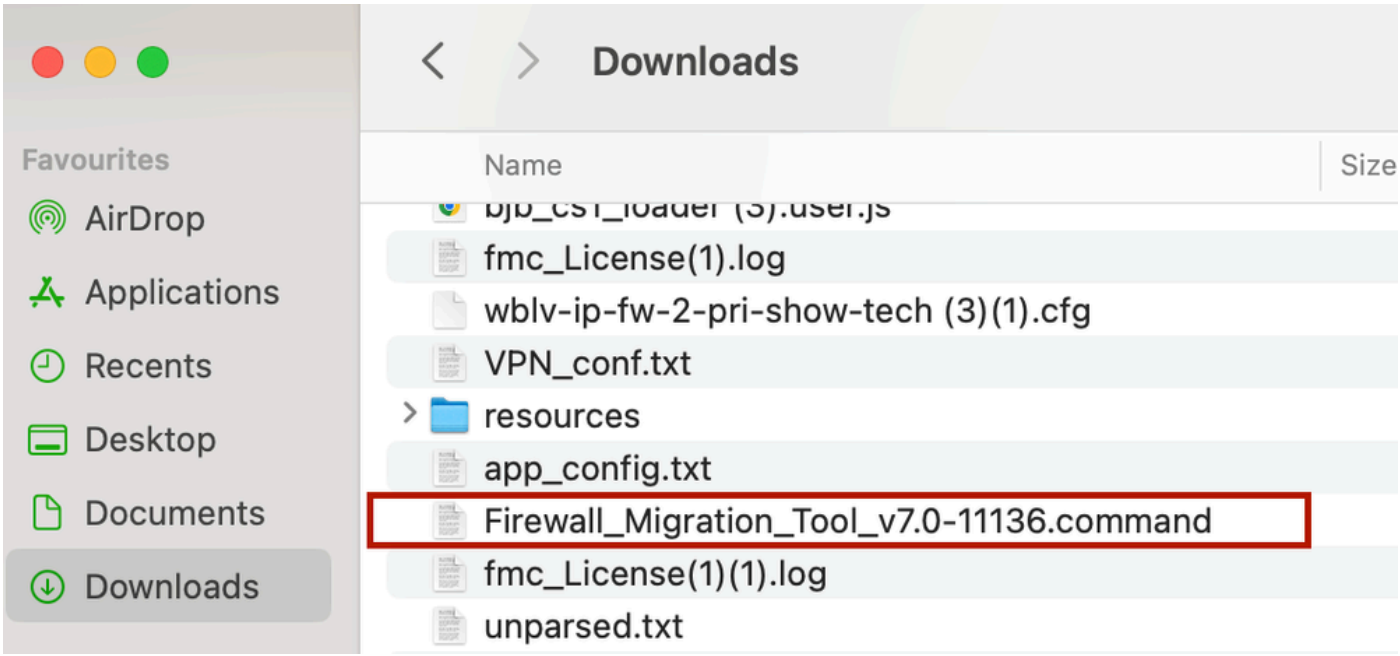
Configuration Steps:

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

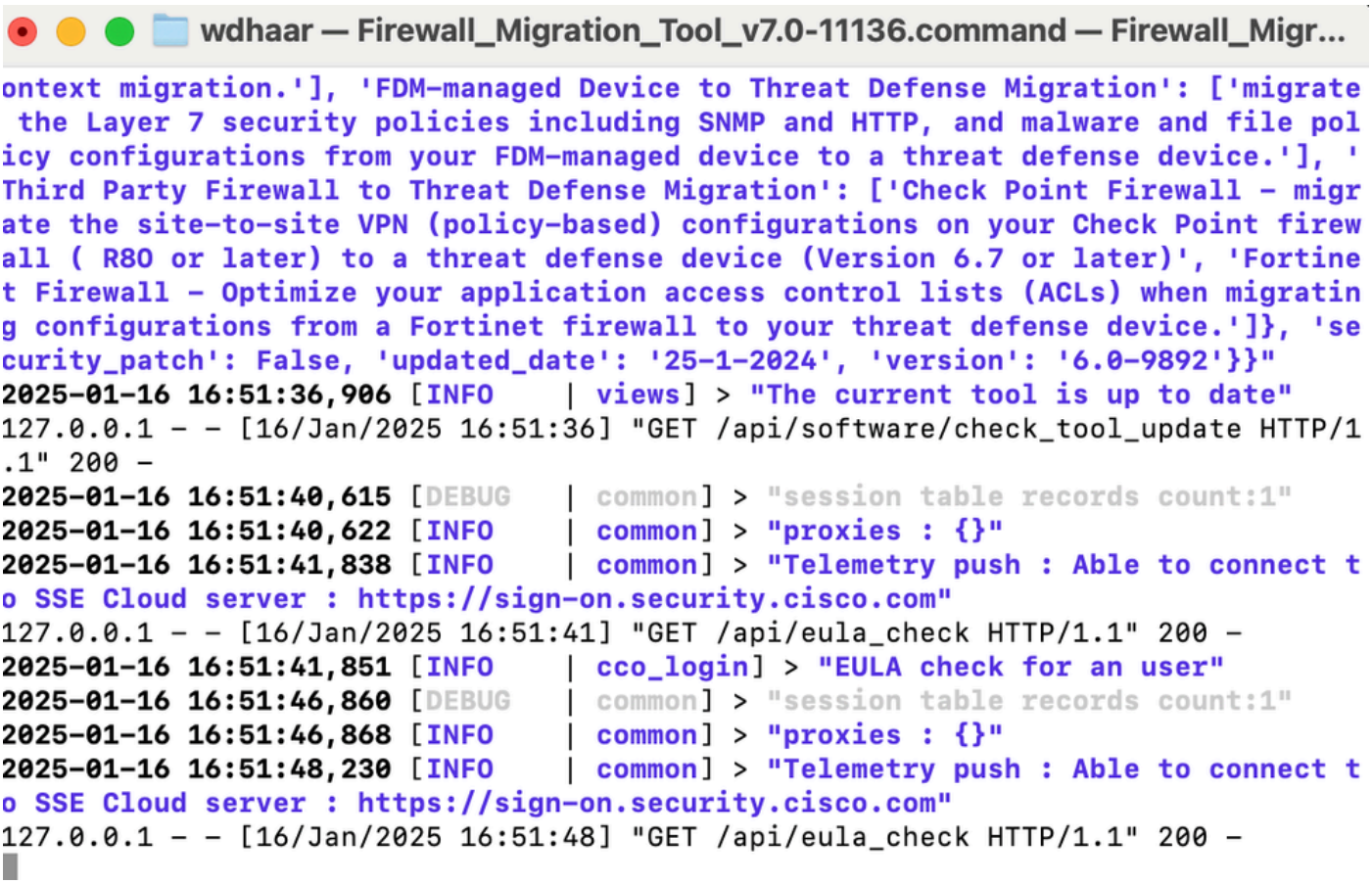


Descarga de software

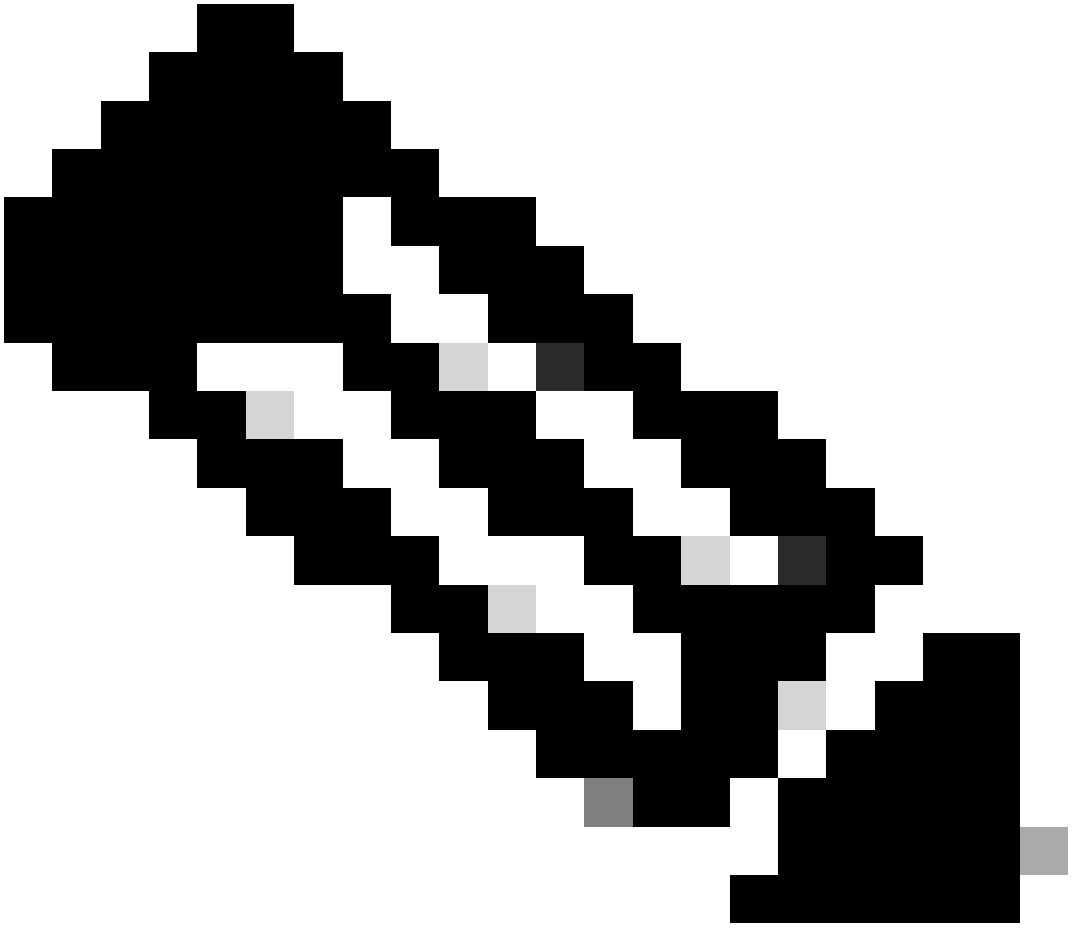
2. Haga clic en el archivo que descargó anteriormente en el equipo.



El archivo

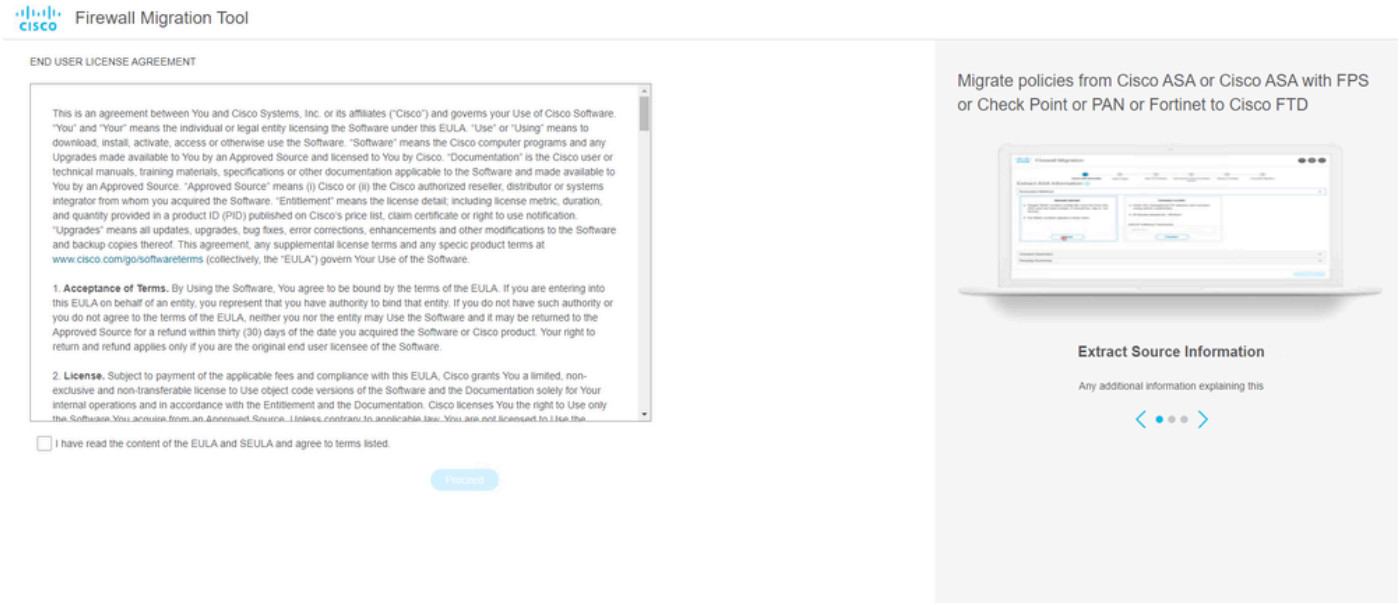


Registros de la consola



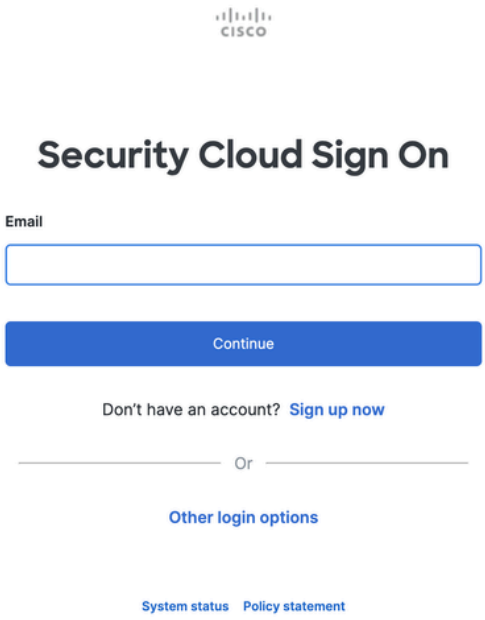
Nota: El programa se abre automáticamente y una consola genera automáticamente contenido en el directorio donde ejecutó el archivo.

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.



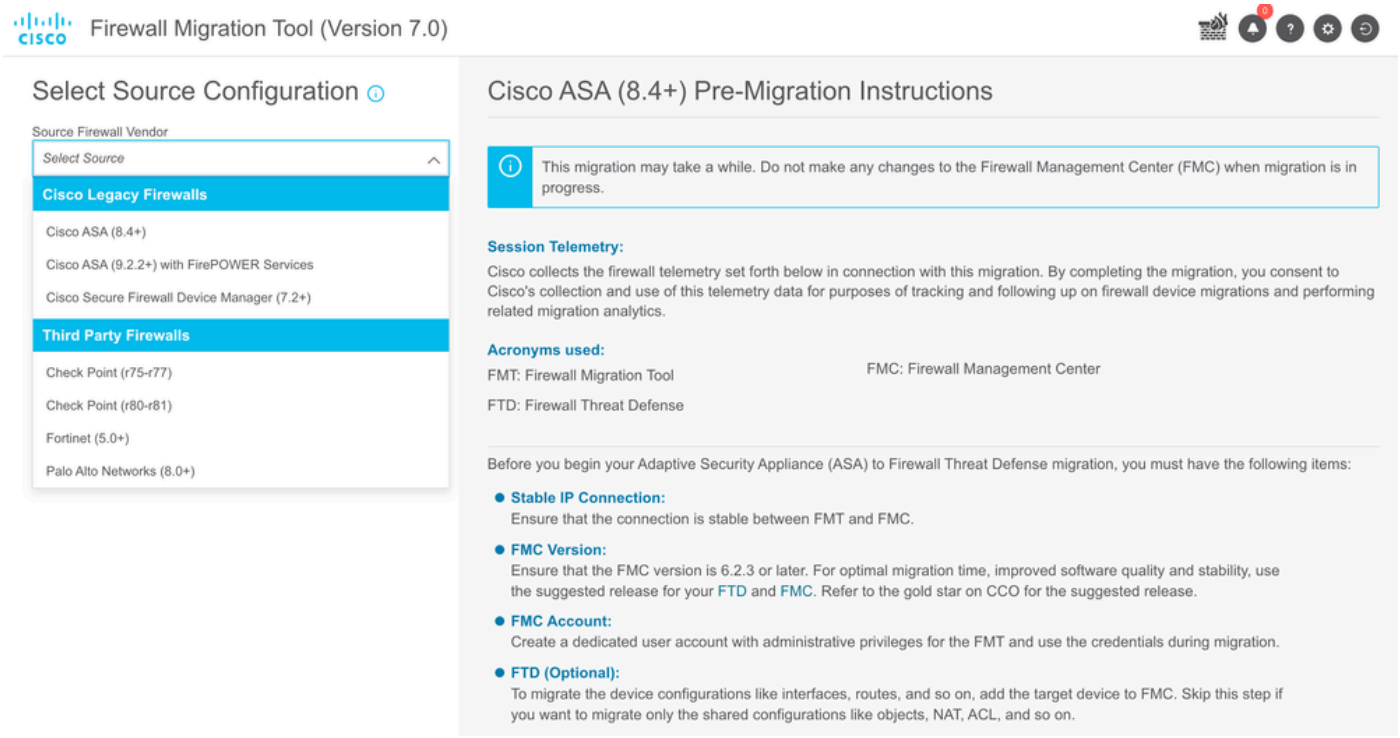
EULA

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



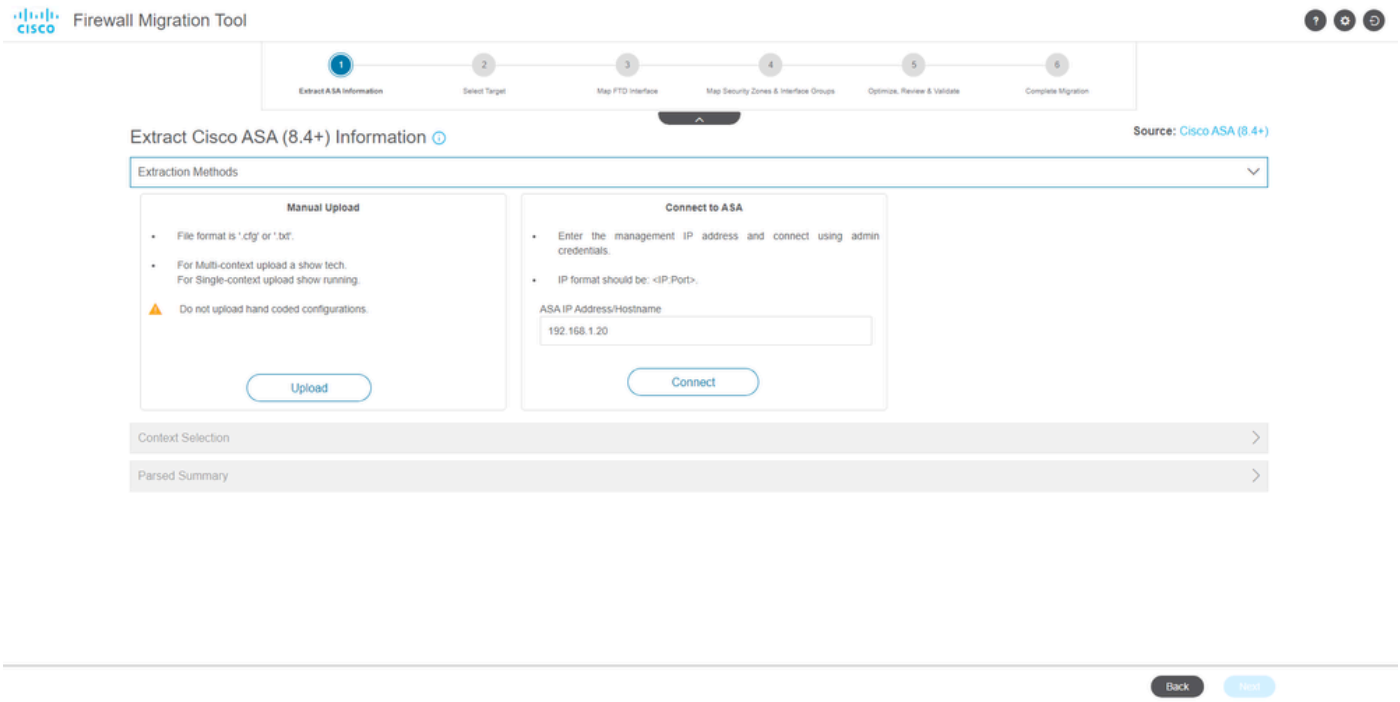
Conexión a FMT

5. Seleccione el firewall de origen que desea migrar.

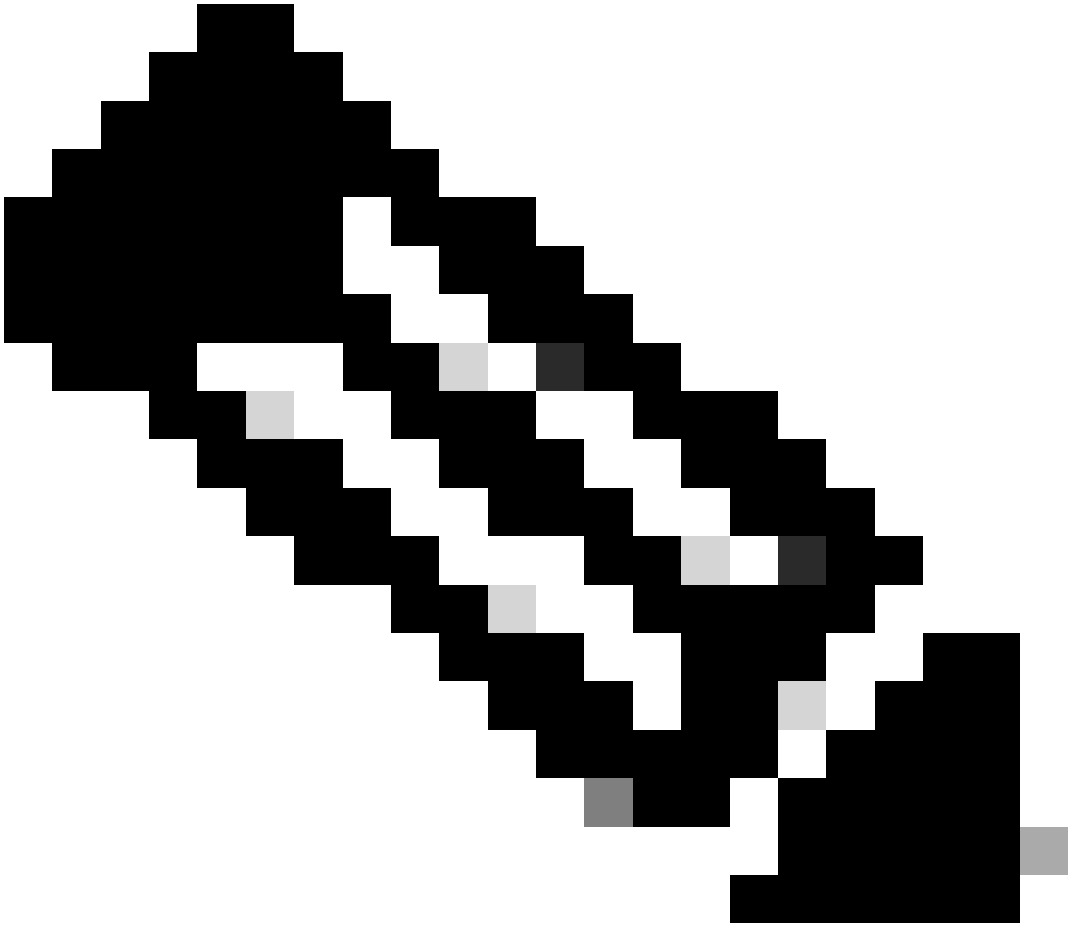


Firewall de origen

6. Seleccione el método de extracción que se utilizará para obtener la configuración.
    1. La carga manual requiere que cargue el **Running Config** archivo del ASA en formato ".cfg" o ".txt".
    2. Conéctese al ASA para extraer las configuraciones directamente del firewall.

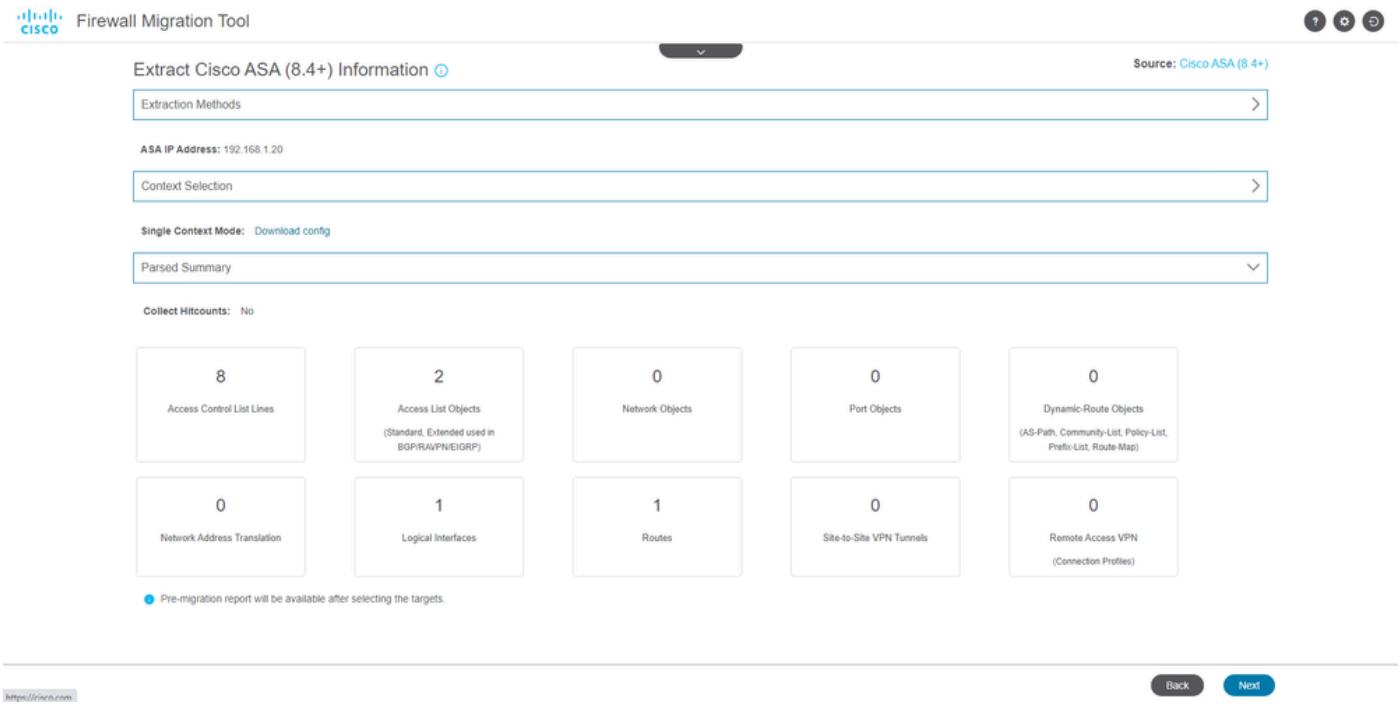


Extracción



Nota: Para este ejemplo, conéctese directamente al ASA.

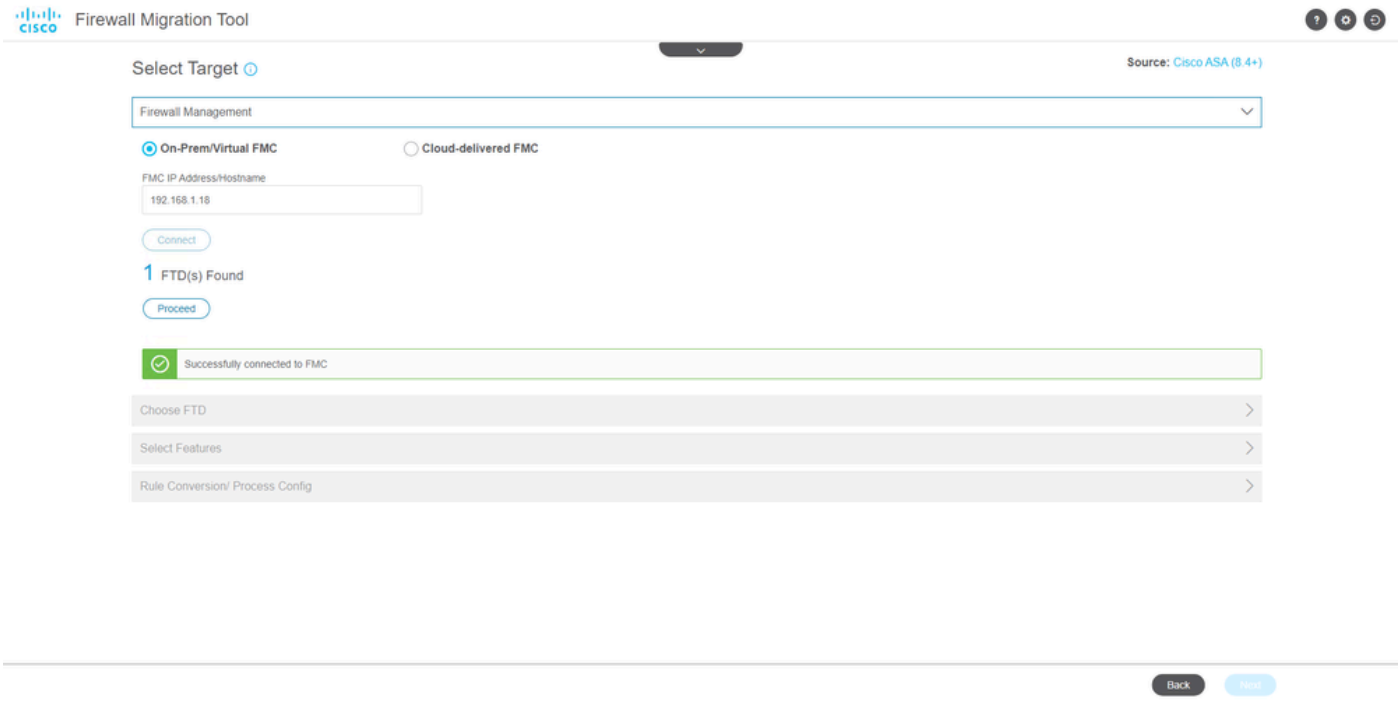
7. Se muestra un resumen de la configuración encontrada en el firewall como panel. Haga clic en Siguiente.



Summary

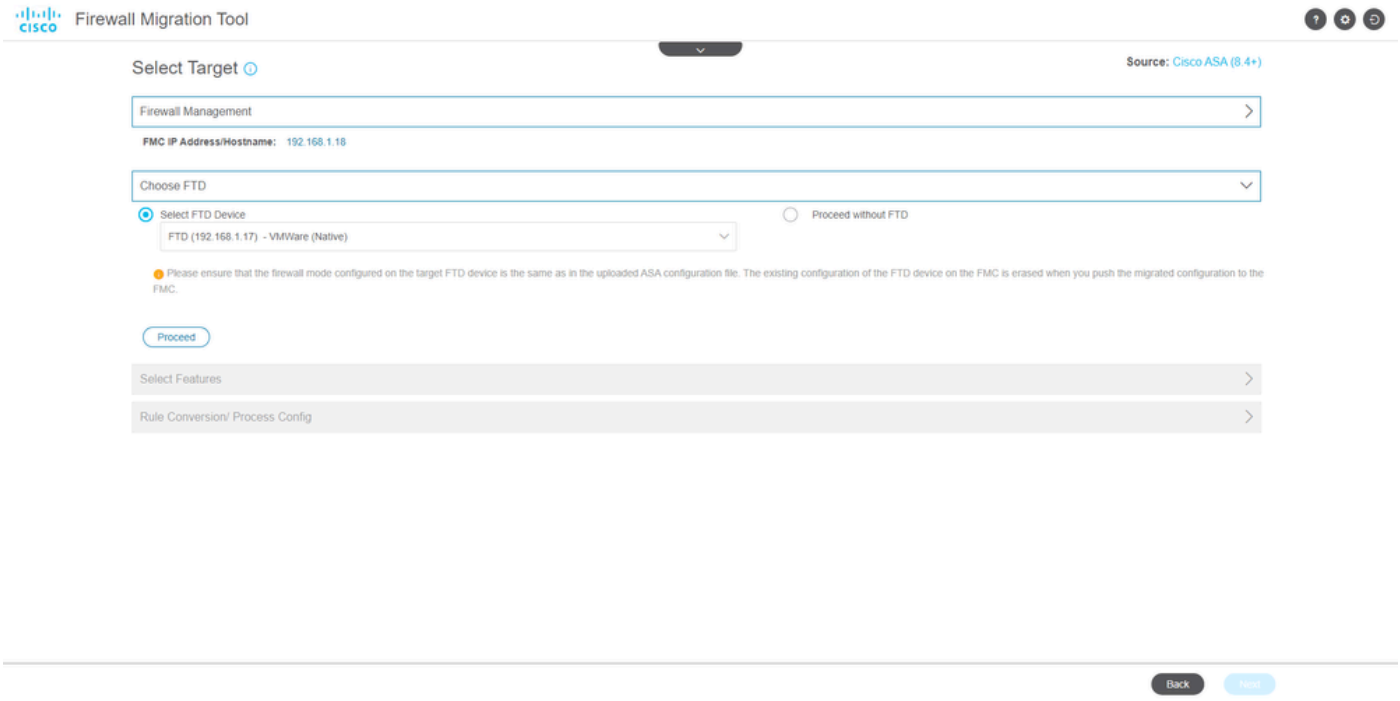
8. Seleccione el CSP objetivo que se utilizará en la migración.

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.



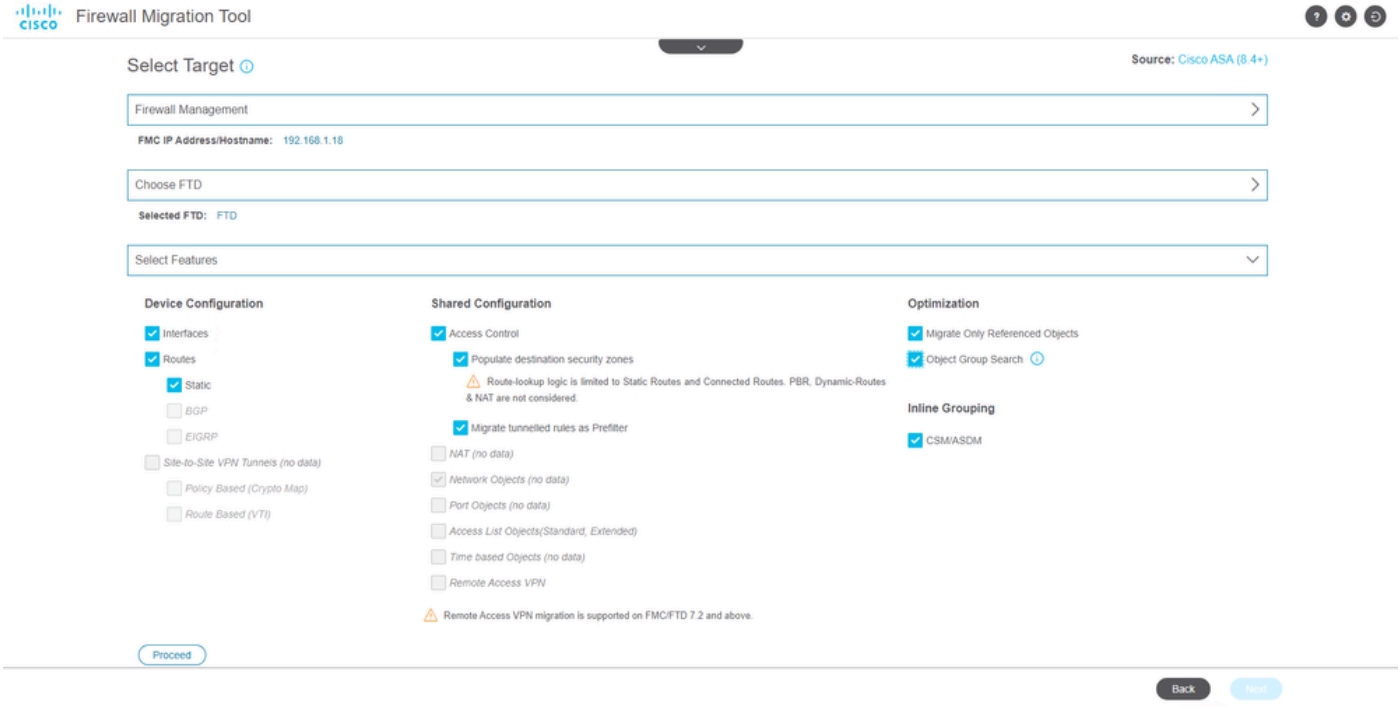
IP de FMC

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



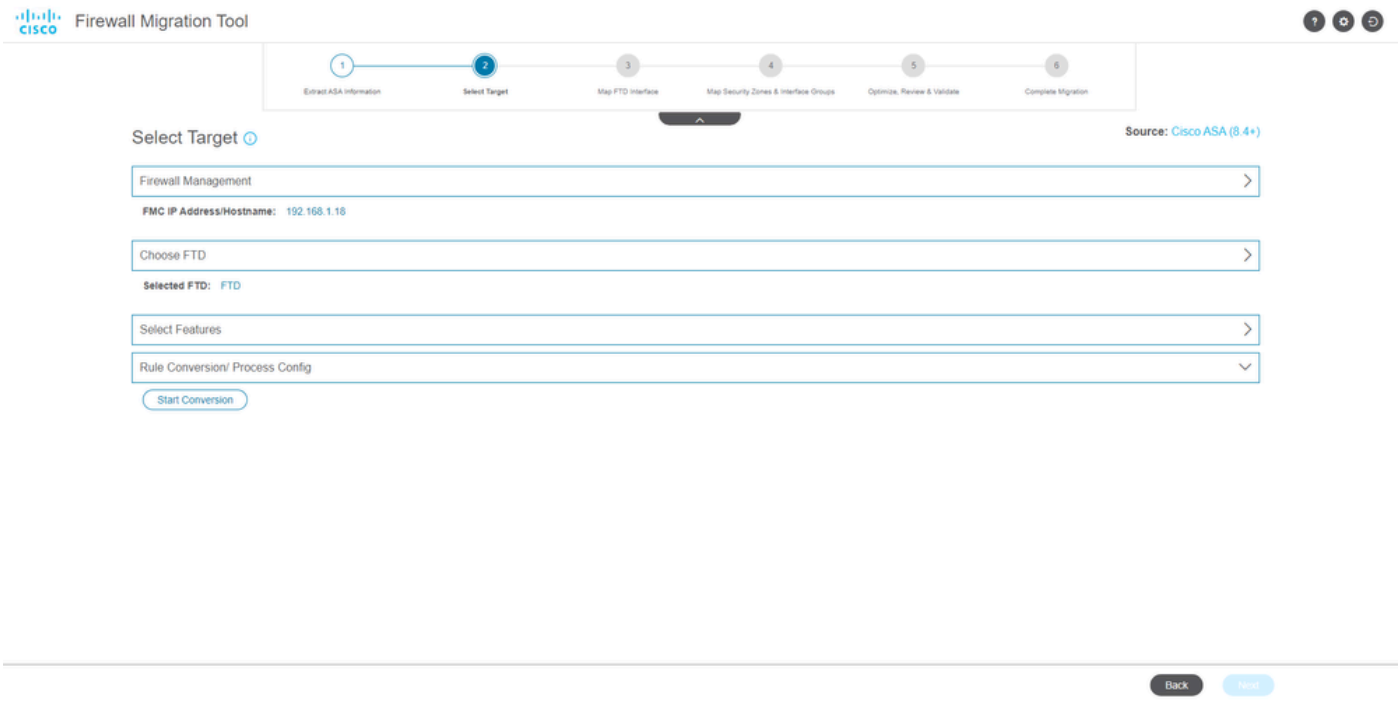
FTD objetivo

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



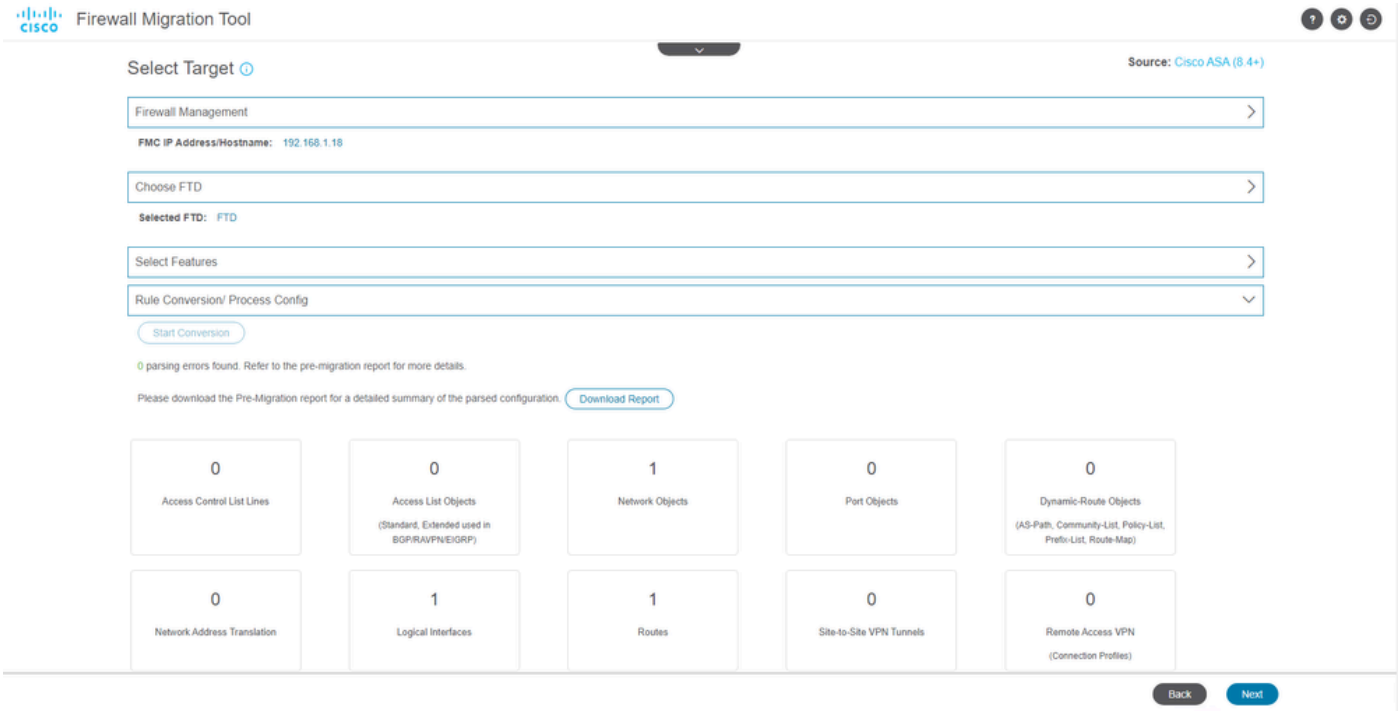
Configuraciones

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



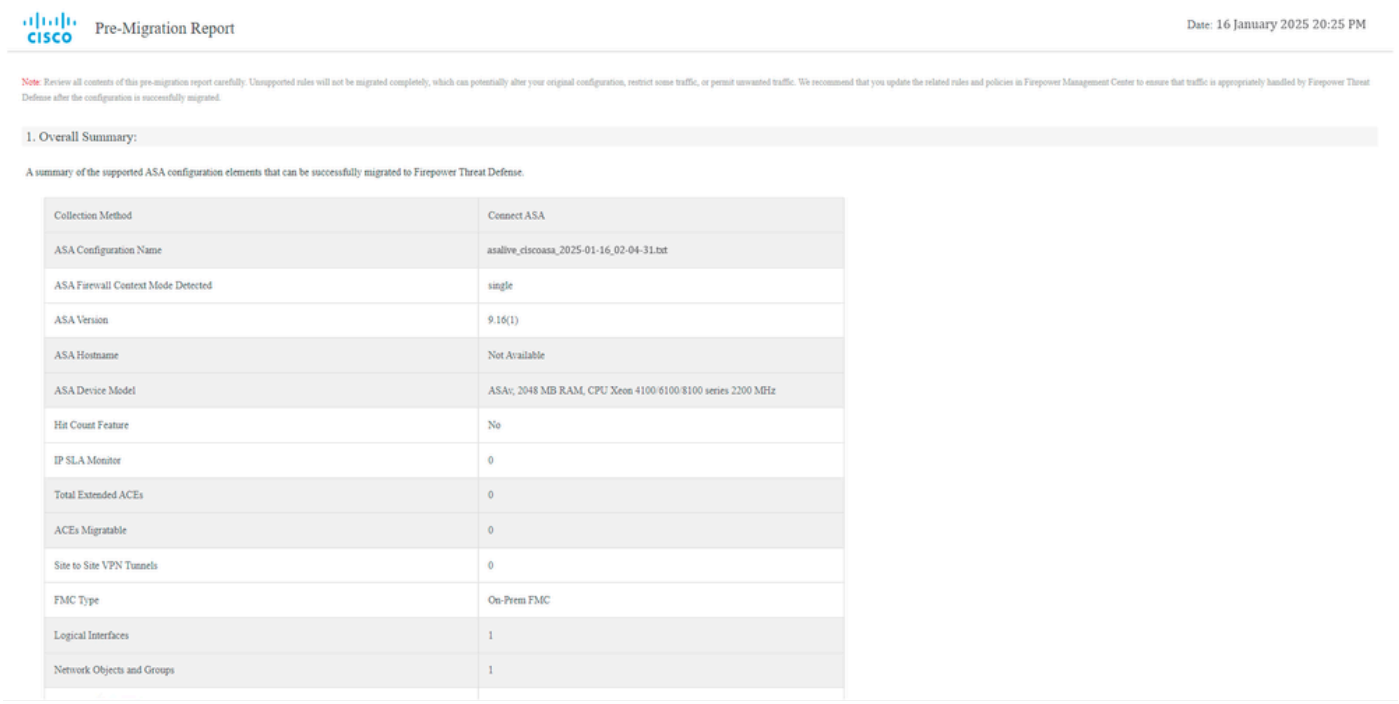
Iniciar conversión

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.



Descargar informe

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



Pre-Migration Report

Date: 16 January 2025 20:25 PM

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.

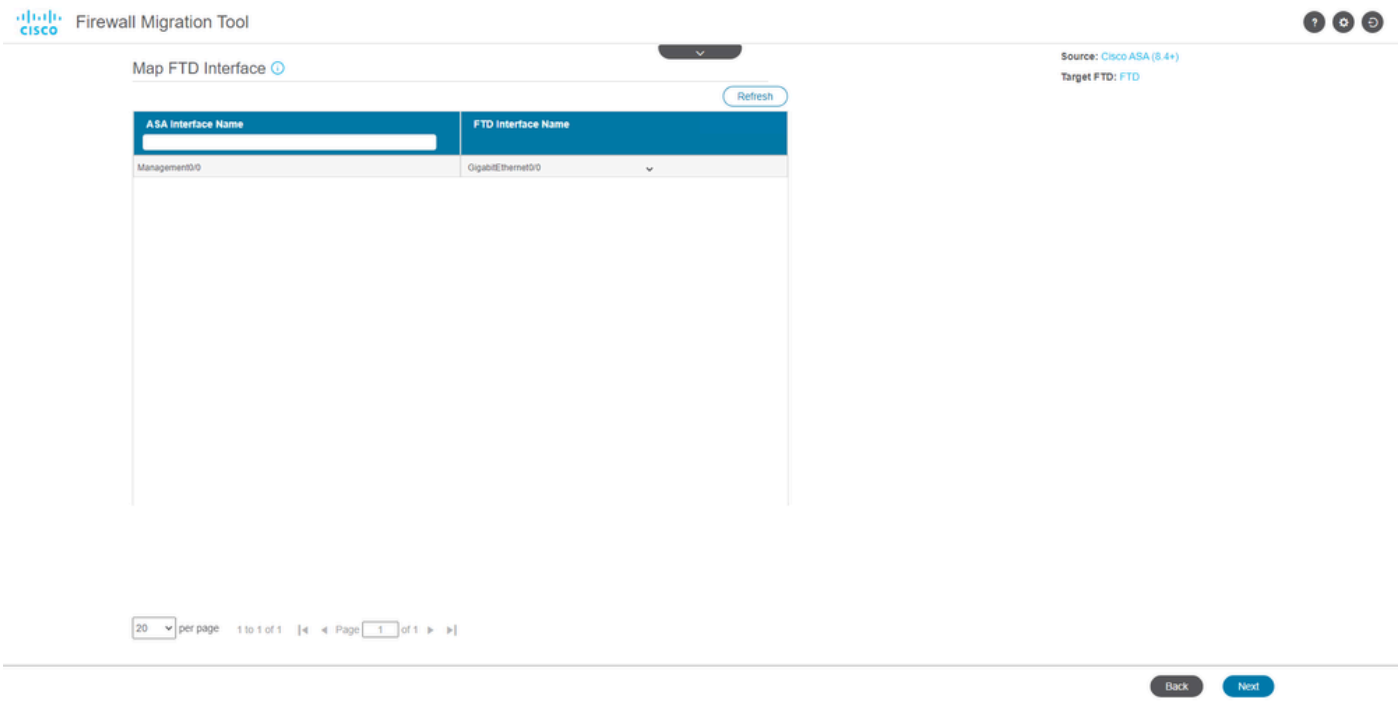
1. Overall Summary:

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	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit 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

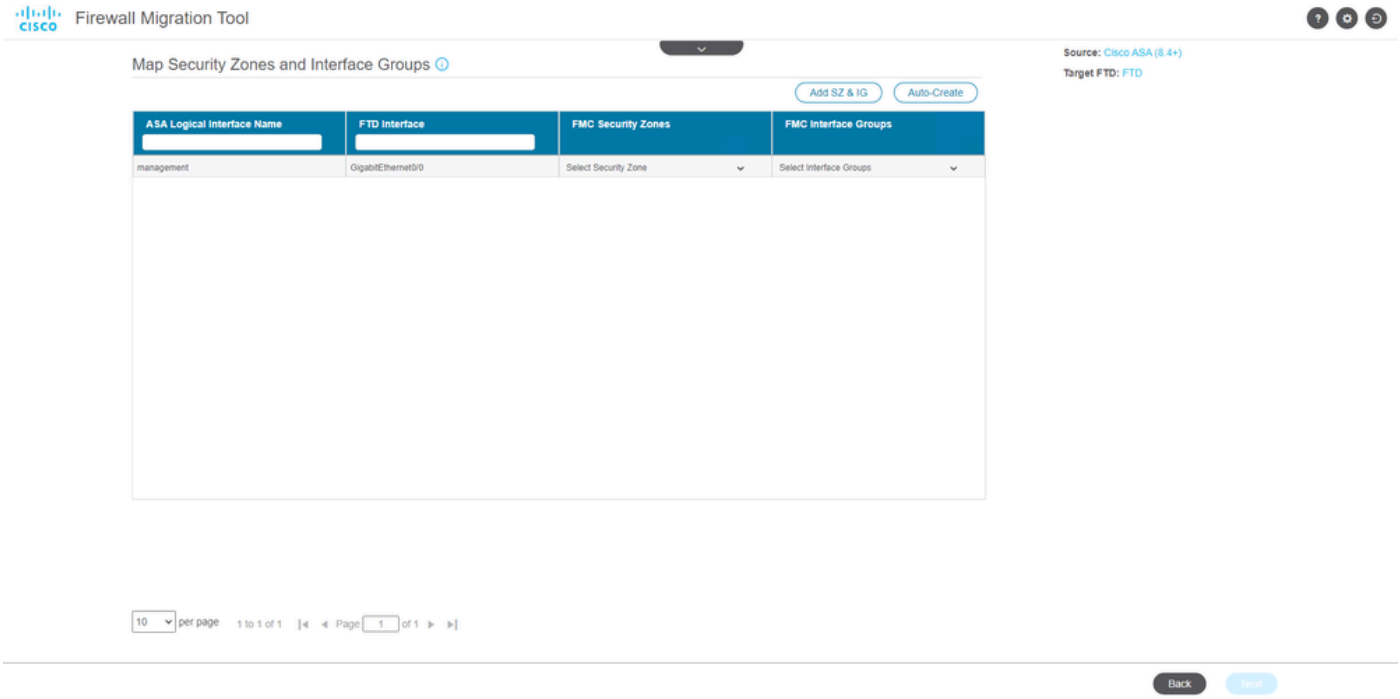
Informe previo a la migración

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



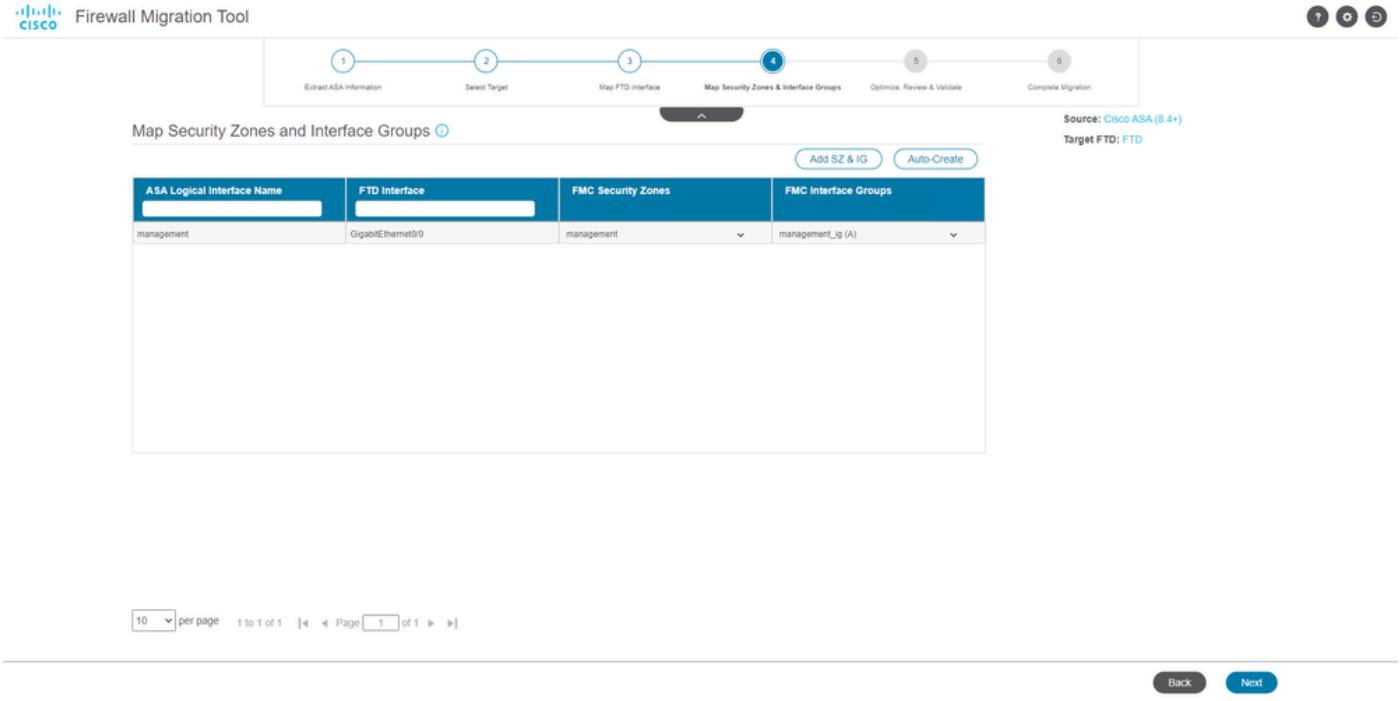
Interfaces de mapa

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



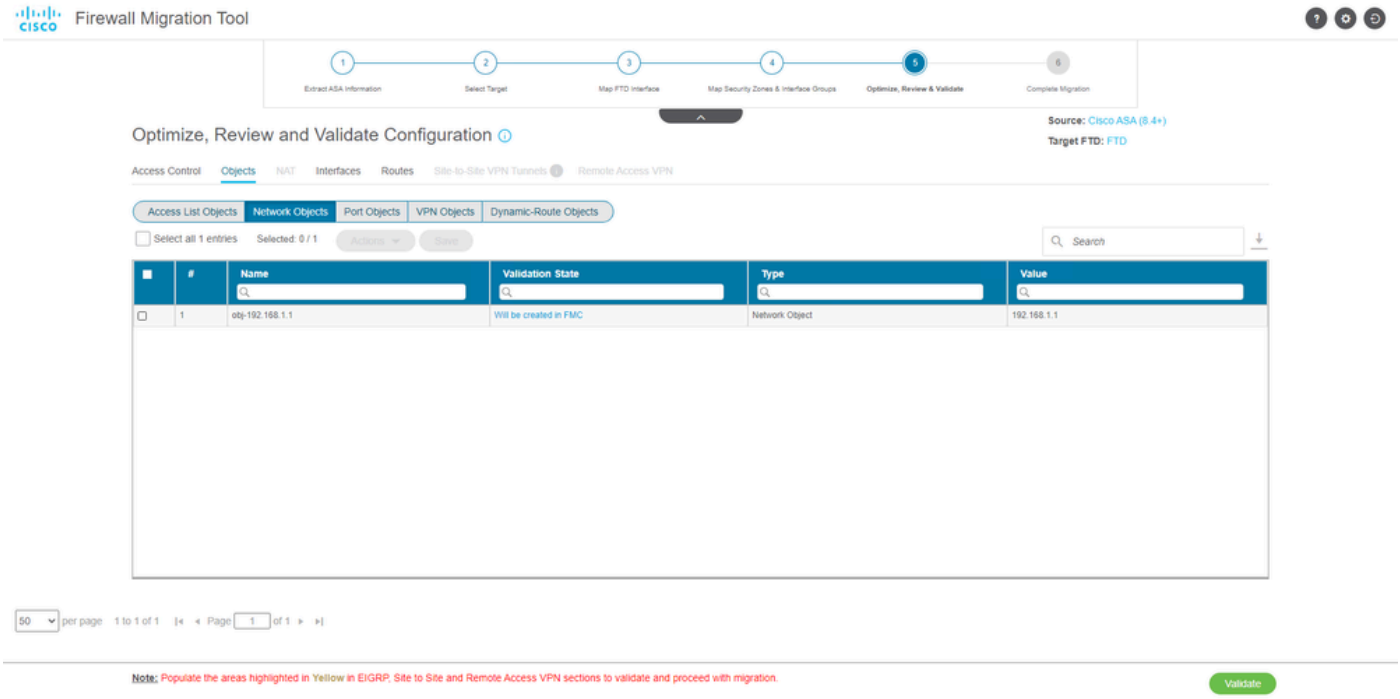
Zonas de seguridad y grupos de interfaces

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



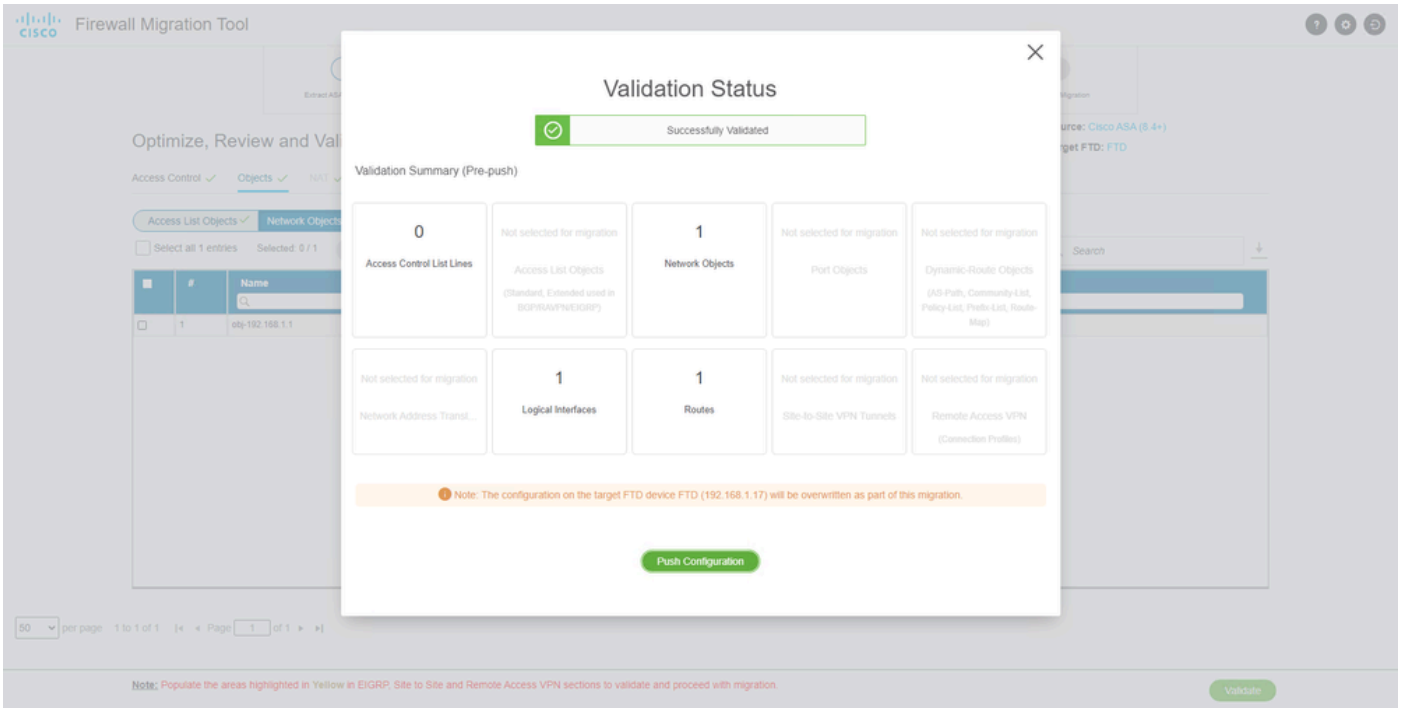
Herramienta de creación automática

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 enValidate.



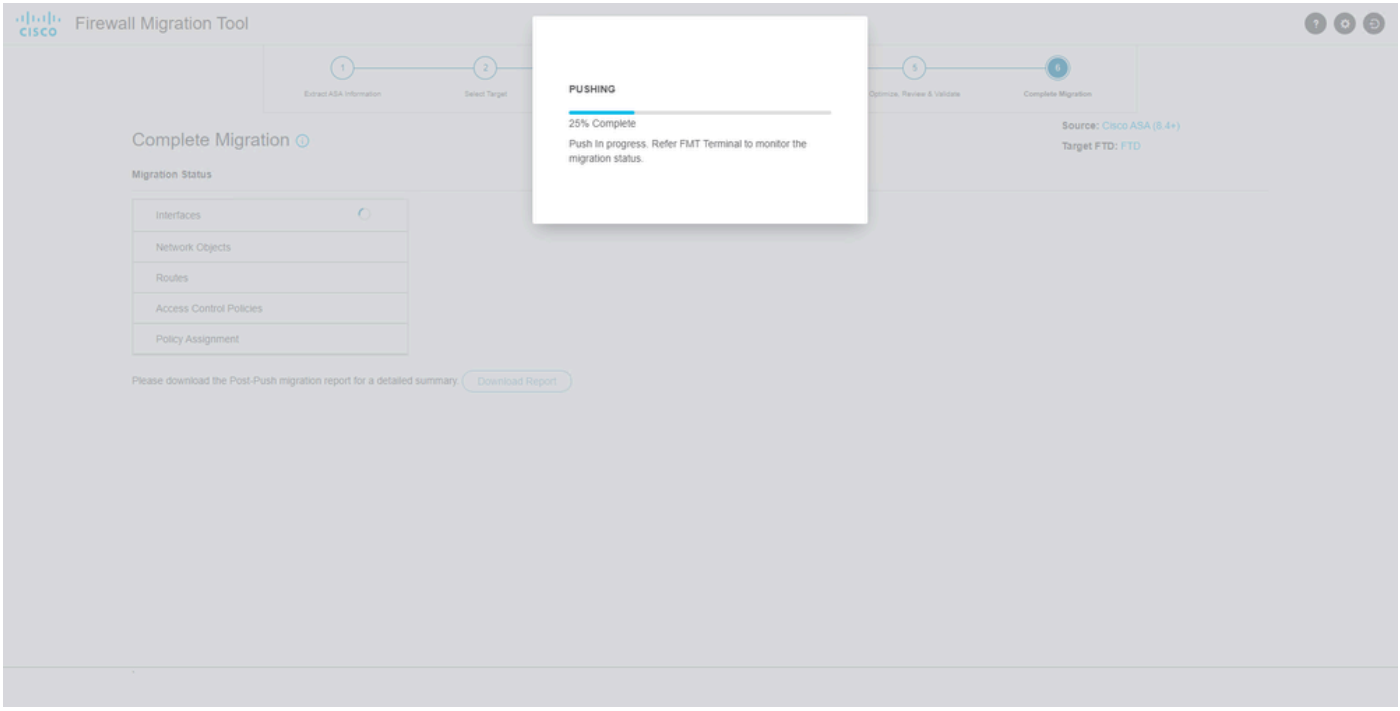
Revisar y validar

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



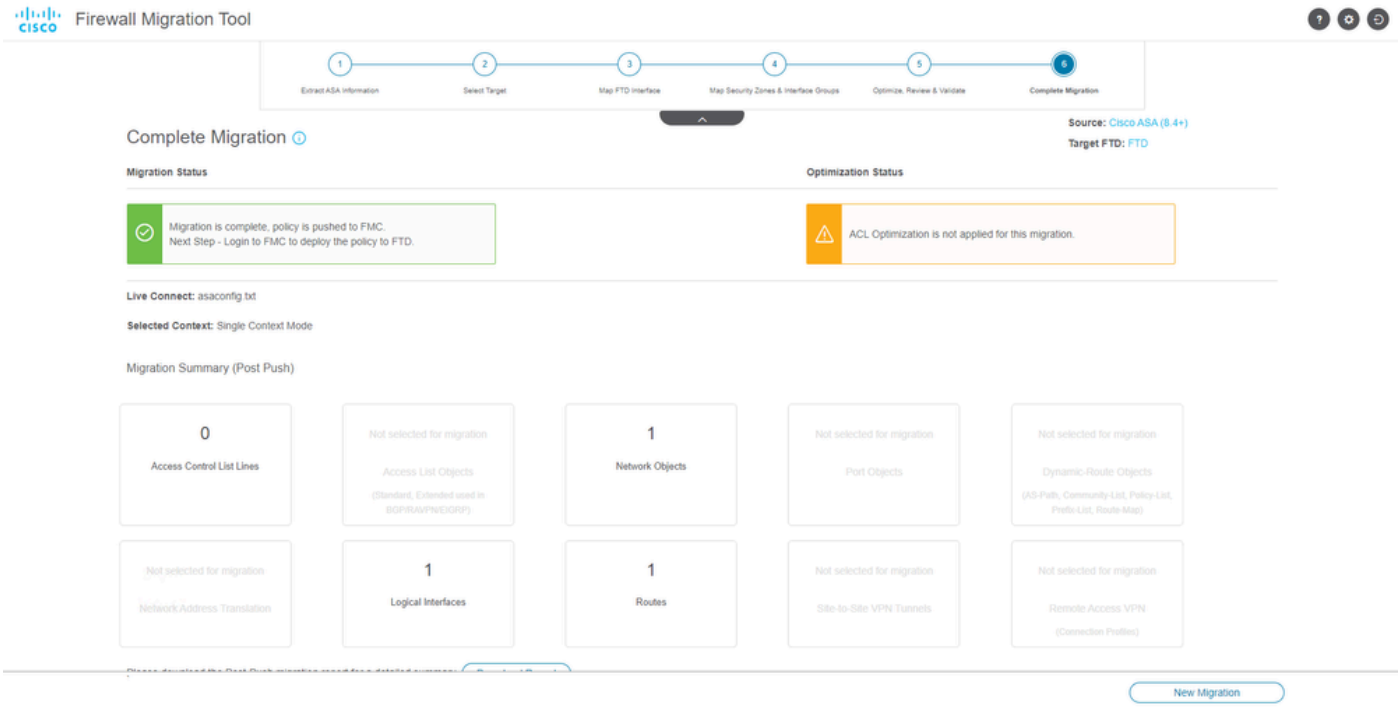
Validación

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 laDeploypestaña.

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).