Migre de Paloalto a Firepower Threat Defence mediante FMT

Contenido

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 Paloa Firewall, ejecute estas actividades:

Obtener archivo zip de configuración de firewall de Paloalto

- El firewall Paloalto 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 Paloalto 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

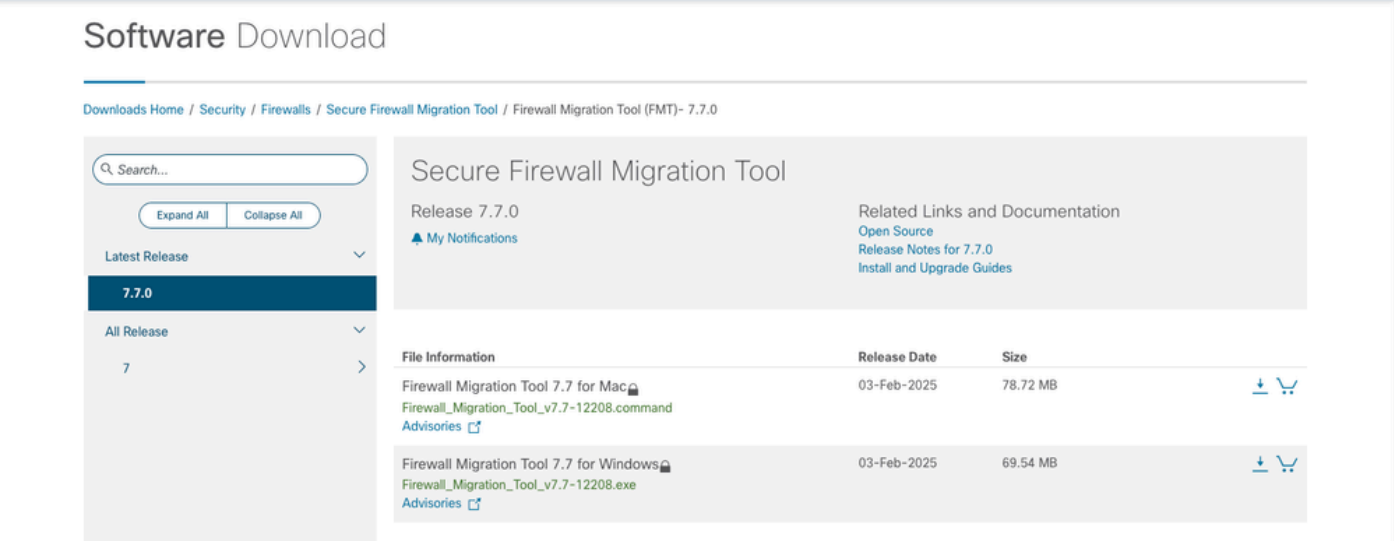
- Asegúrese de que el FTD se ha registrado en el FMC antes de comenzar el proceso de

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

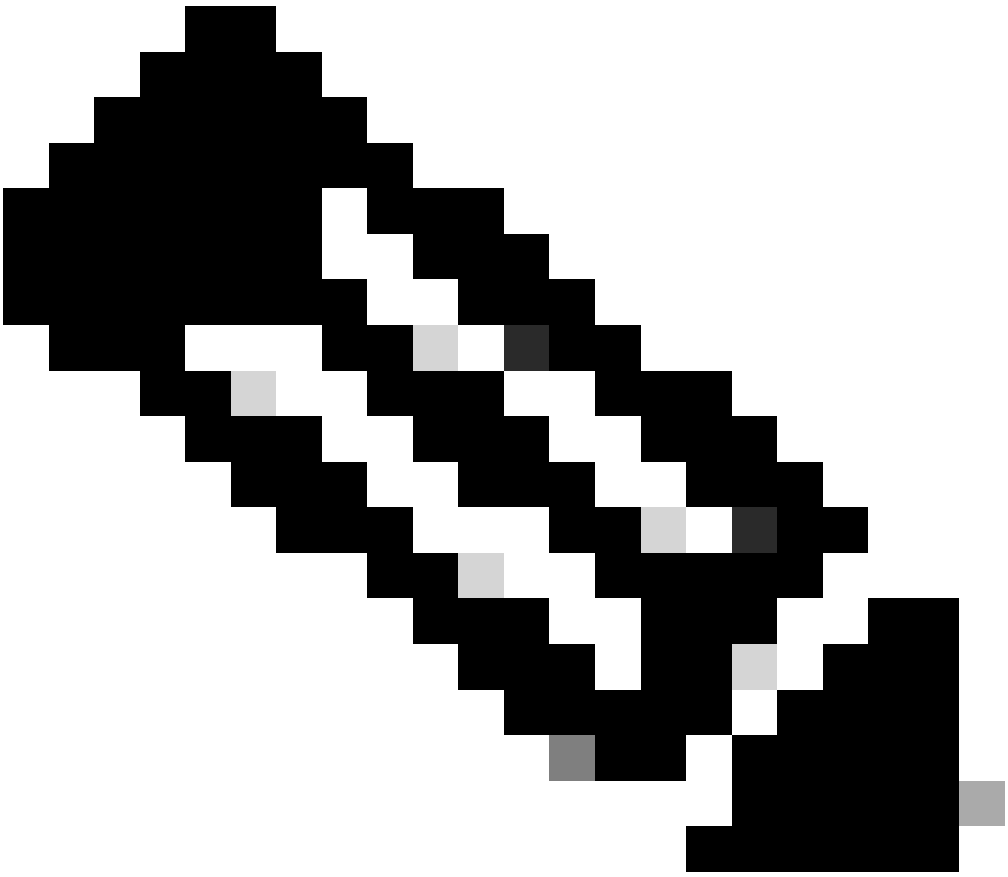
Pasos de migración

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



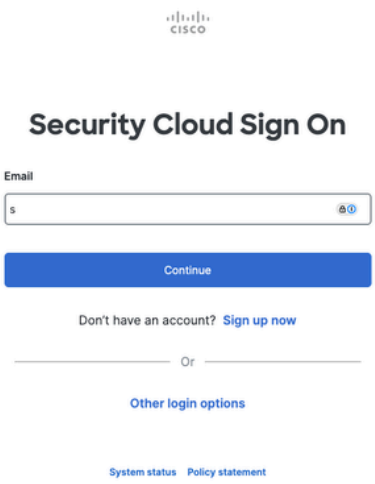
Descarga de FMT

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



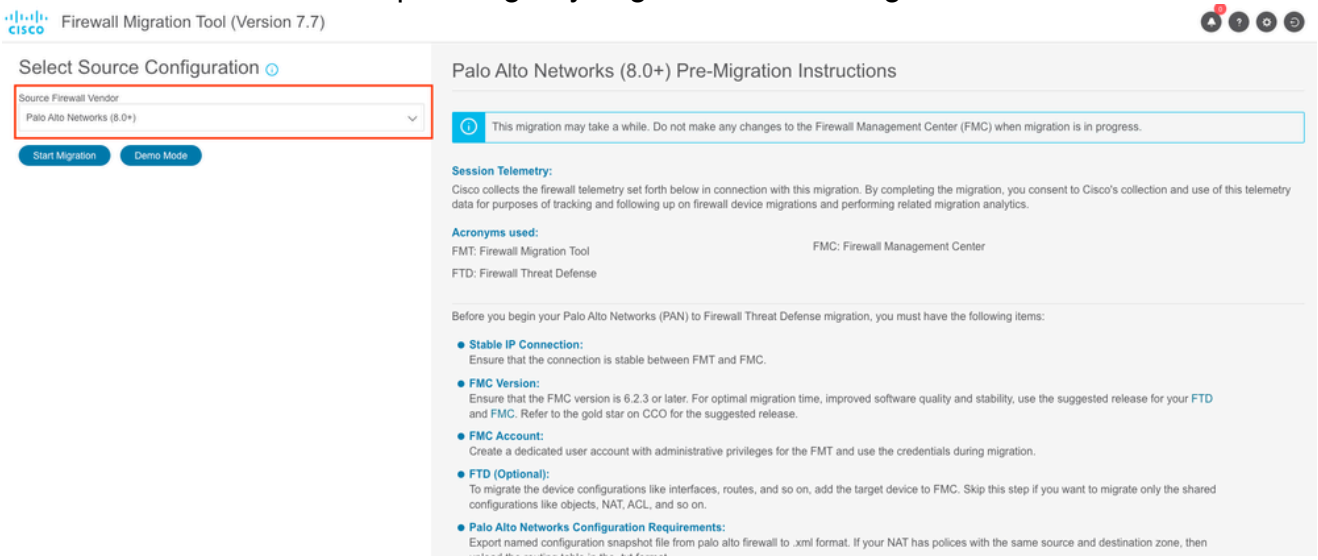
Nota: El programa se abre automáticamente y una consola genera automáticamente contenido en el directorio en el que se ejecutó el archivo.

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.



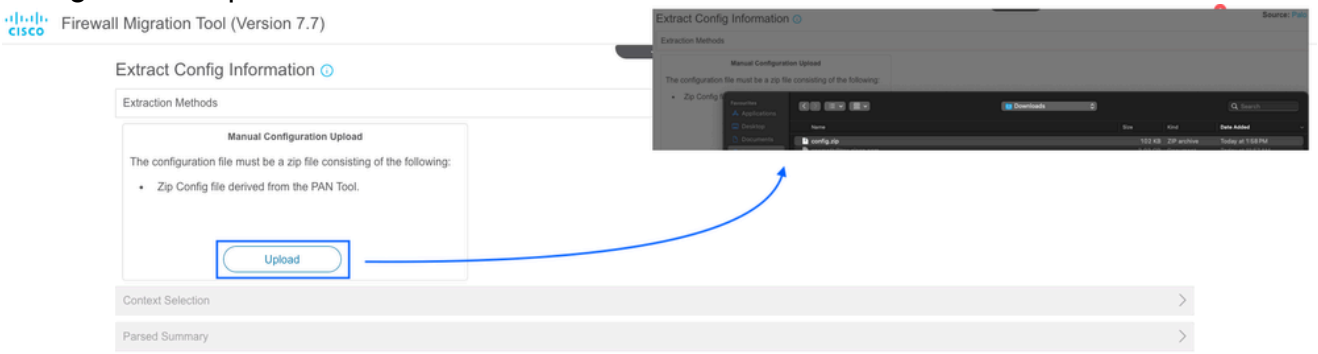
Mensaje de inicio de sesión FMT

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



GUI de FMT

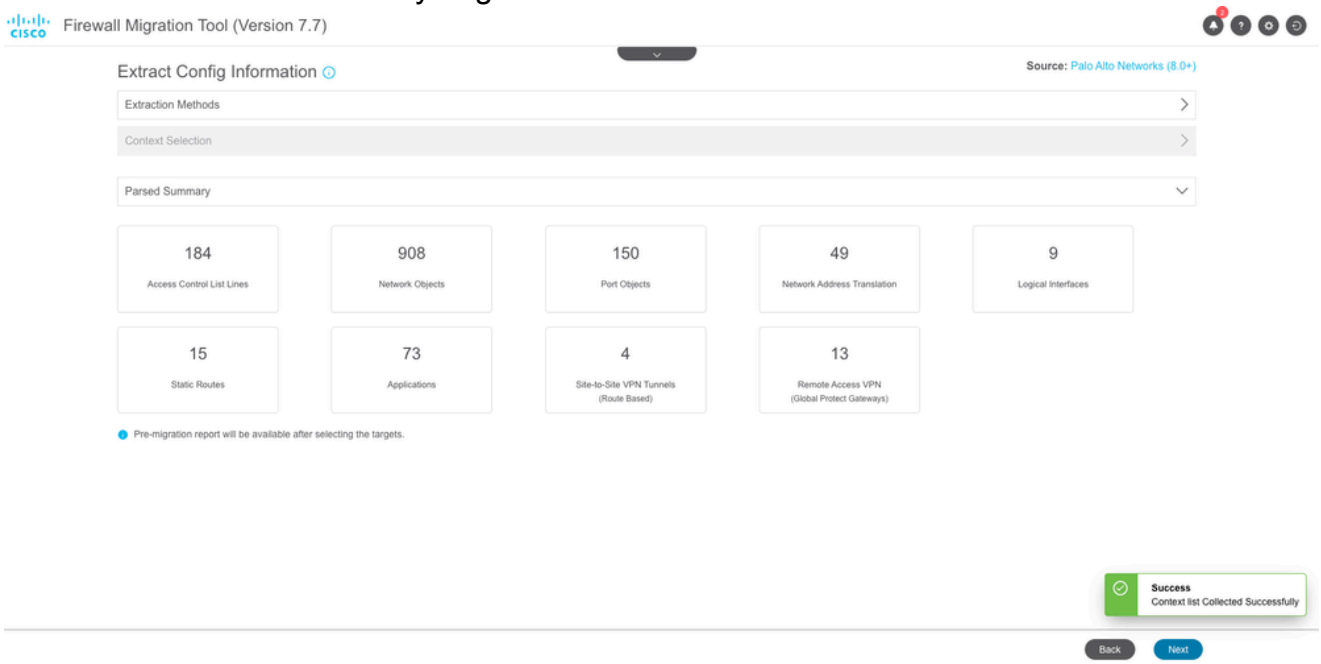
7. Ahora se muestra la sección Métodos de extracción, donde debe cargar el archivo de configuración Zip de Paloalto Firewall al FMT.



Asistente de carga de configuración

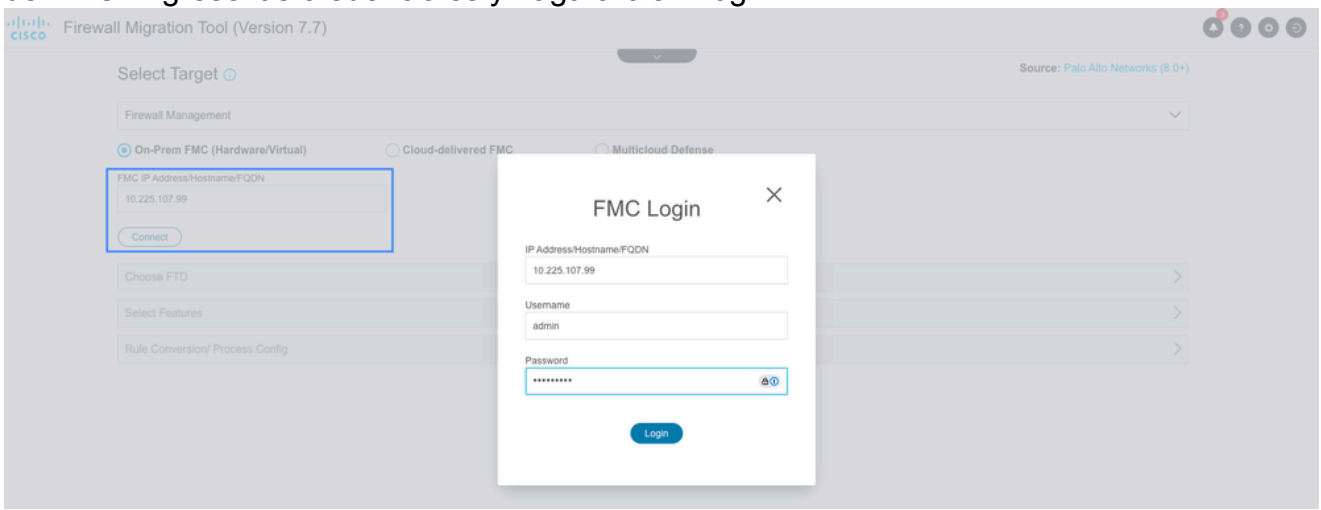
8. El resumen de configuración analizada se muestra ahora después de cargar el archivo de configuración. En el caso de VSYS, hay disponibles selecciones de VSYS independientes.

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



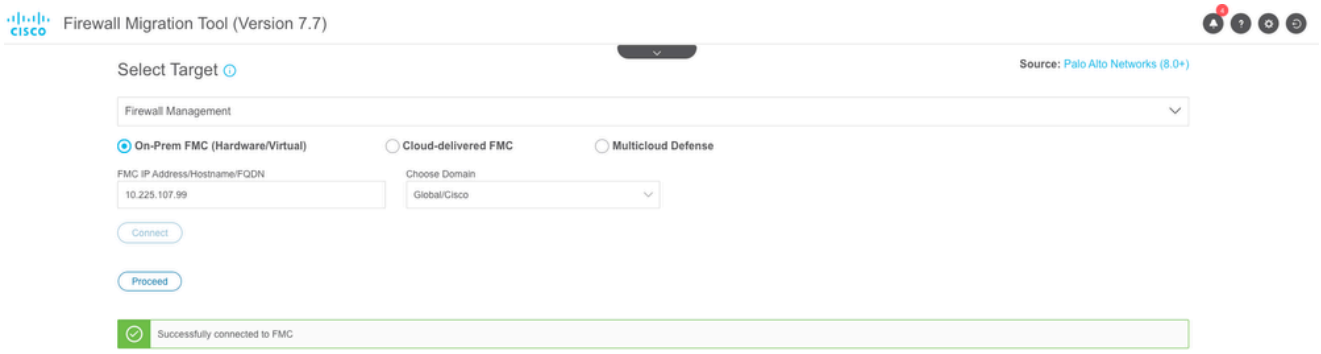
Resumen de validación de configuración

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.



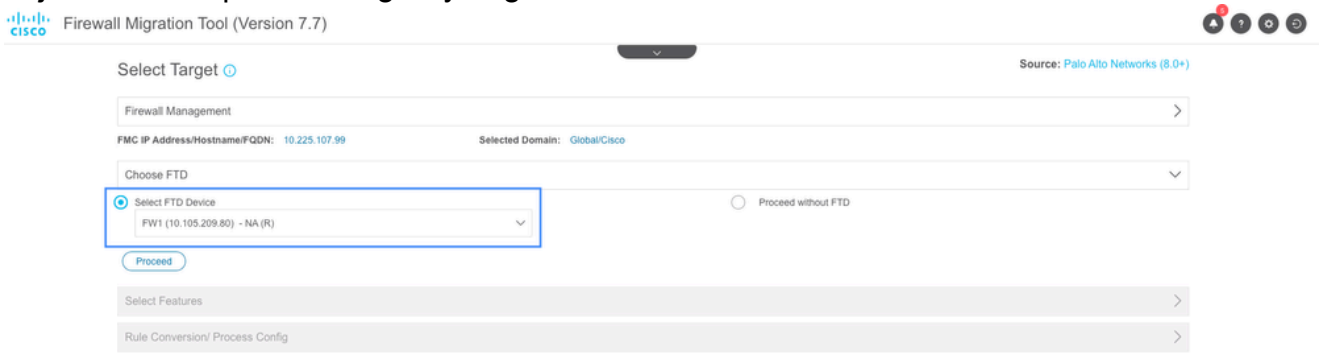
Conexión a FMC

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



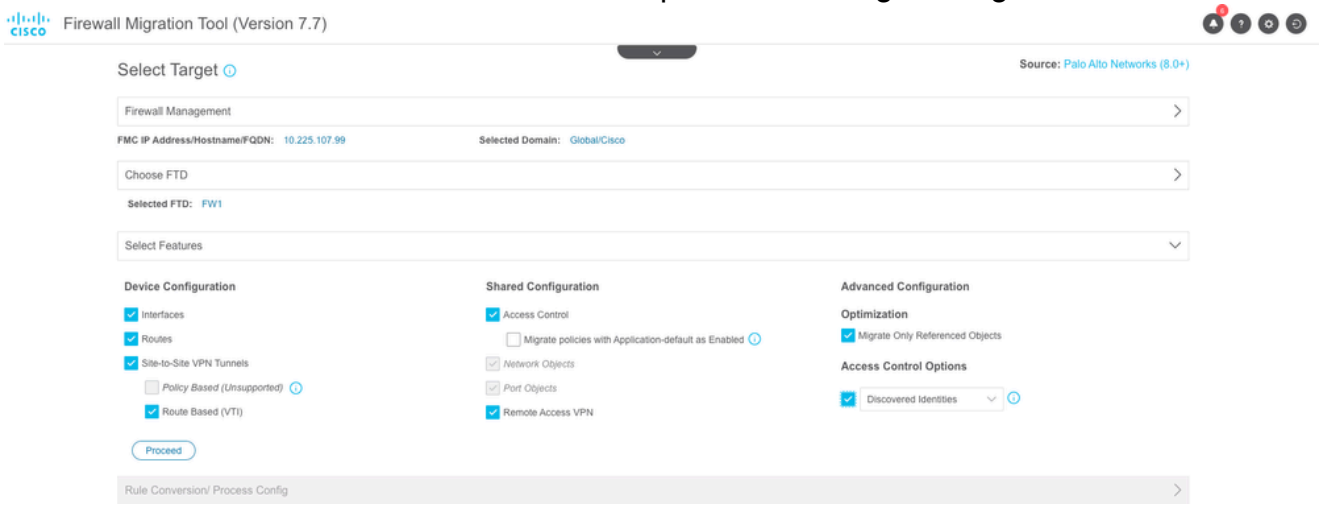
Selección de dominio

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

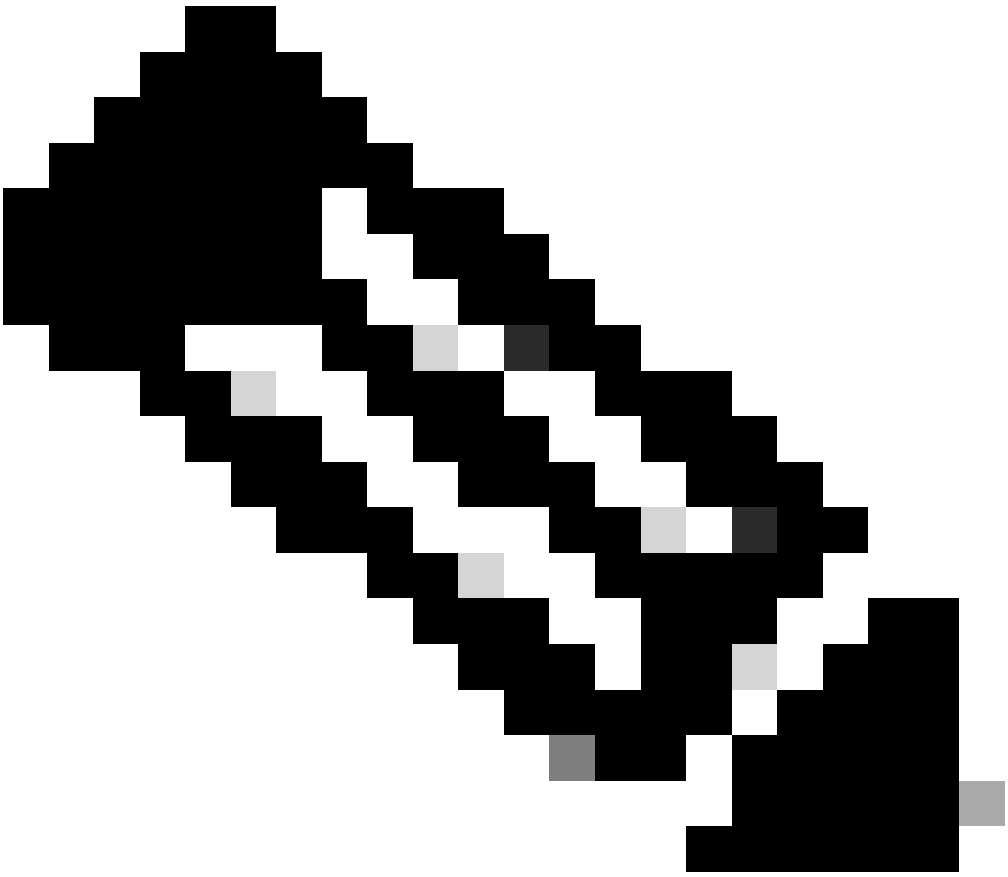


Seleccionar FTD de destino

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

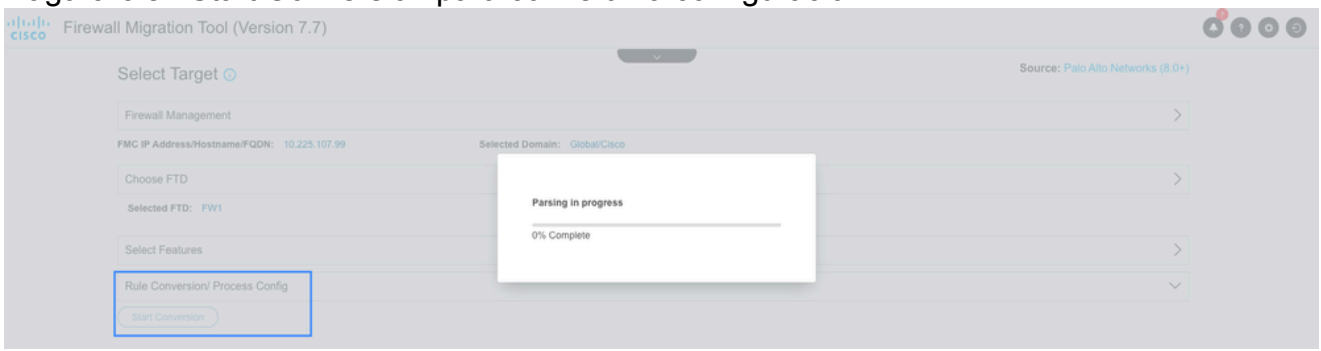


Selección de funciones



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

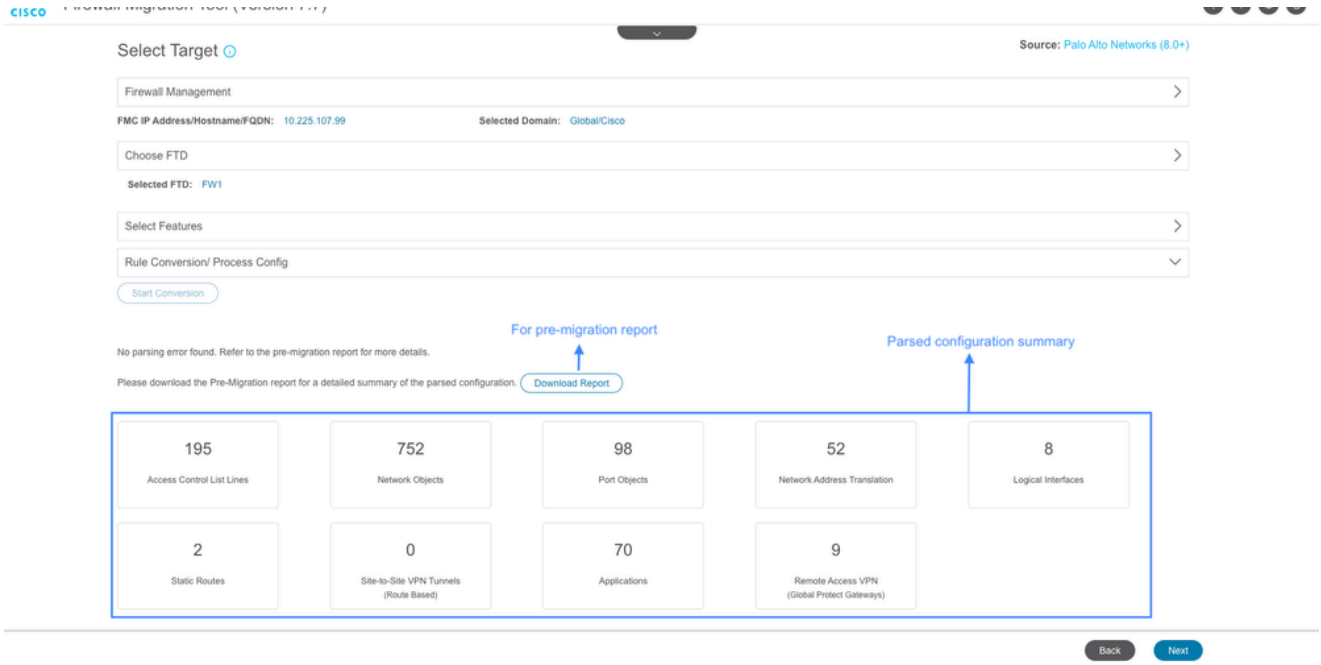
13. Haga clic en Start Conversion para convertir la configuración.



Configuración de análisis

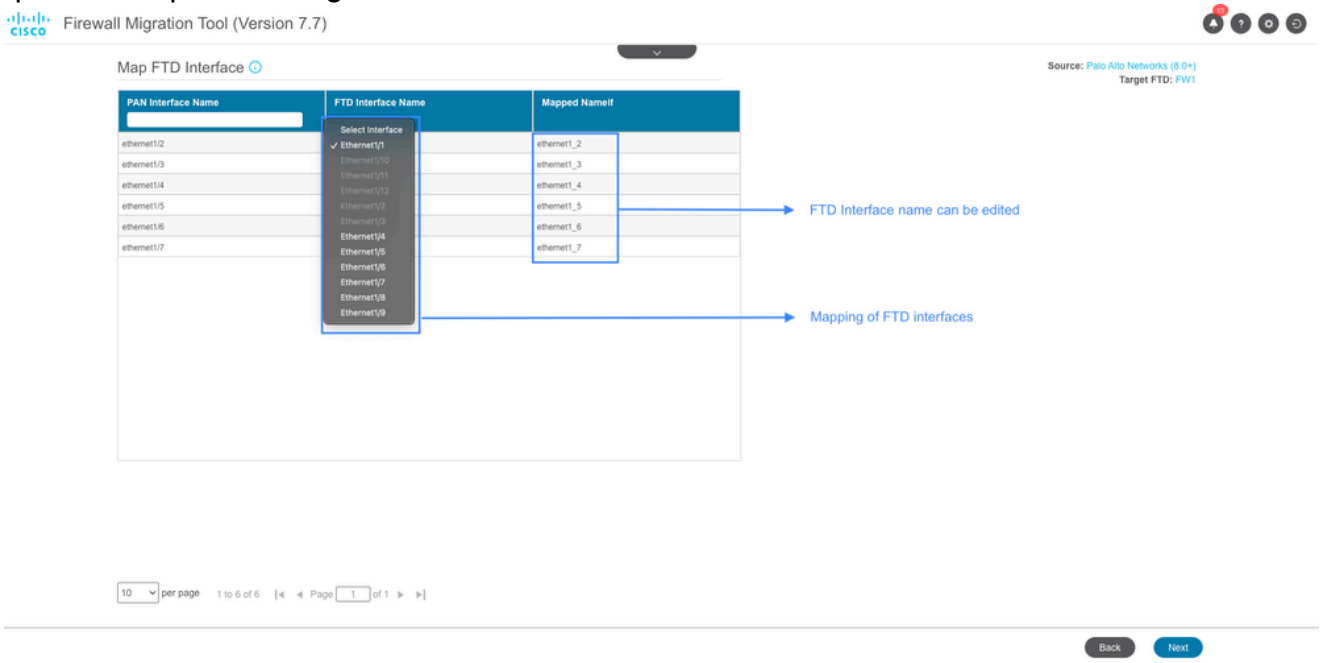
La herramienta analiza la configuración y muestra el resumen de conversión como se muestra en la imagen. También puede descargar el informe previo a la migración para validar la configuración migrada en busca de errores o advertencias, si los hubiera. Vaya a

la página siguiente haciendo clic en Next.



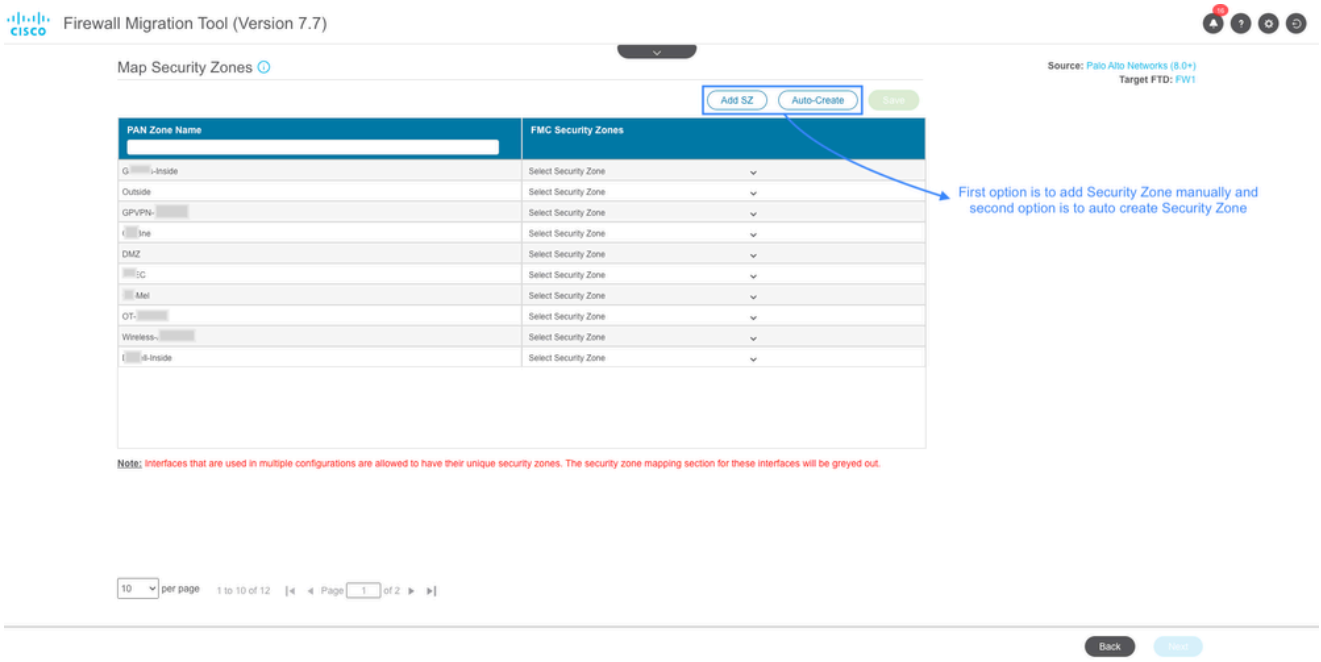
Resumen de configuración analizada

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.



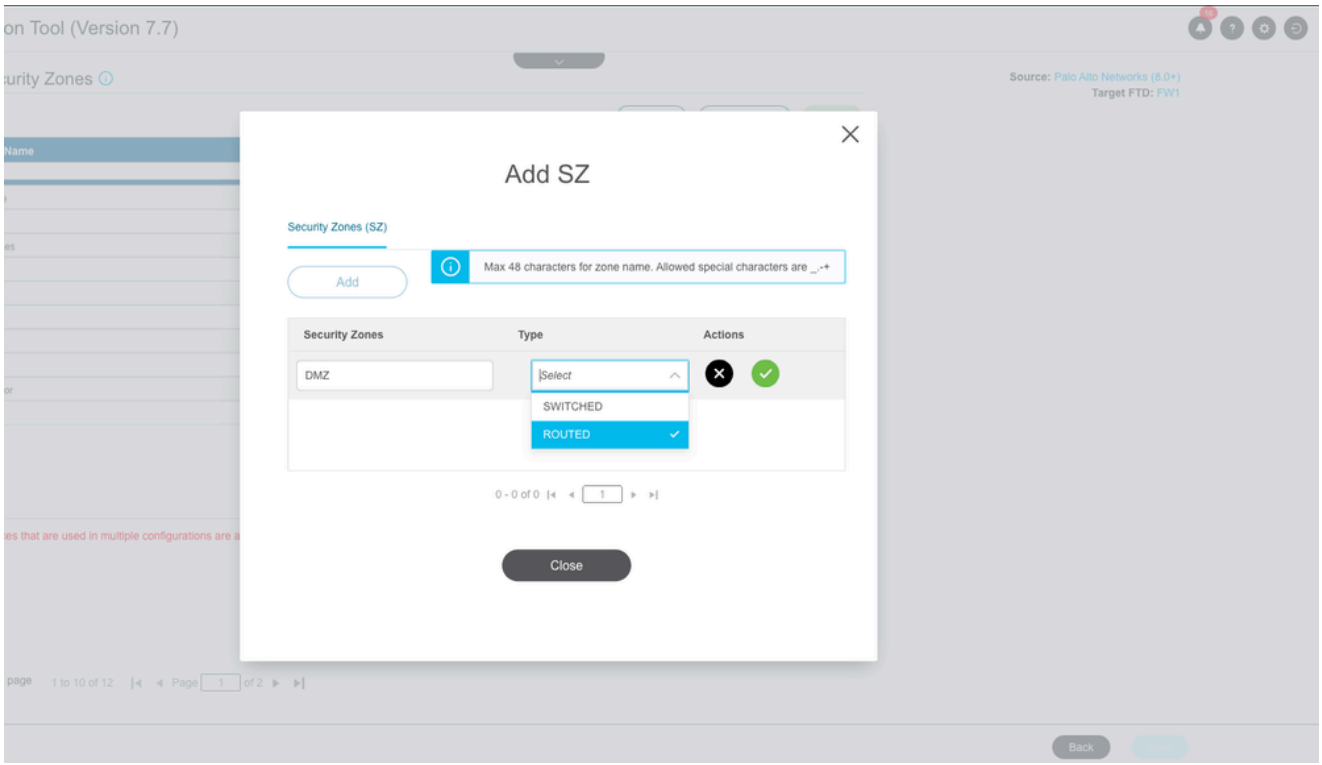
Mapeo de interfaz

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.



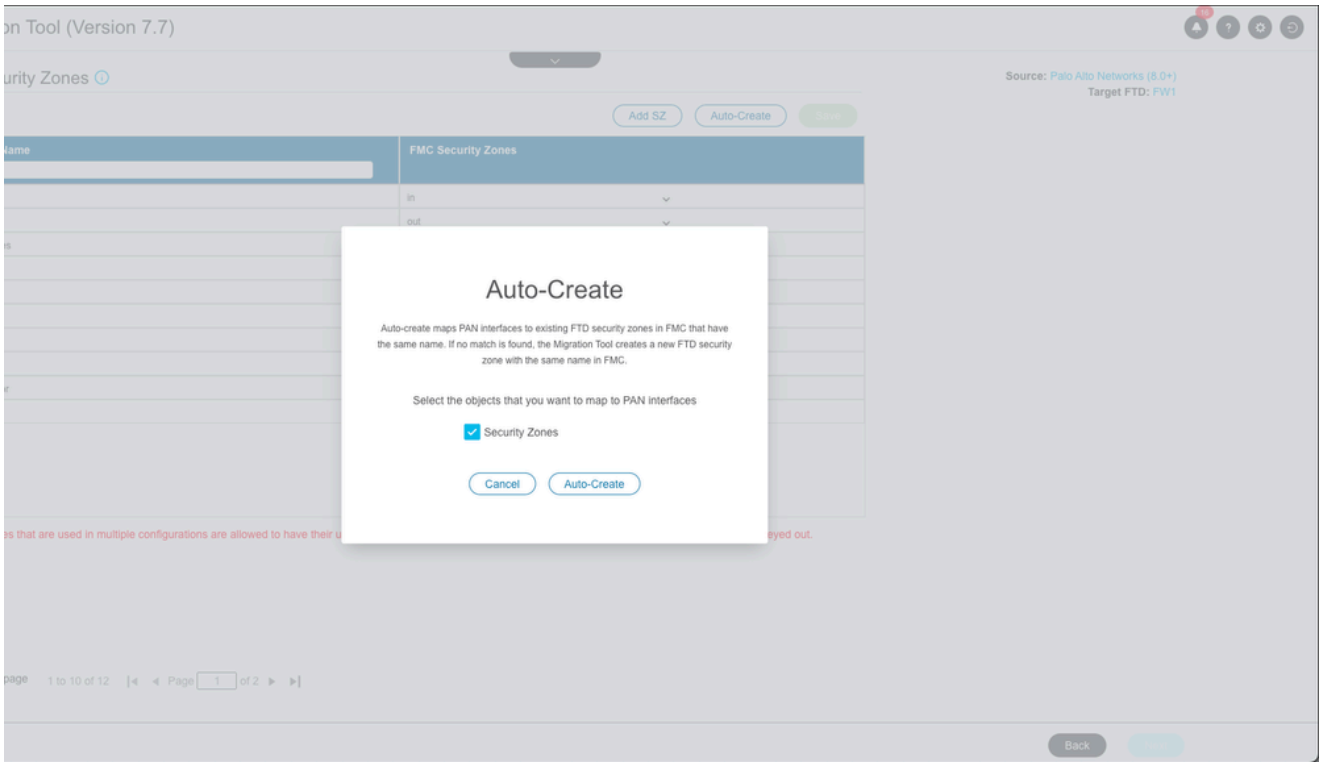
Creación de zonas de seguridad

Creación manual de zonas de seguridad:



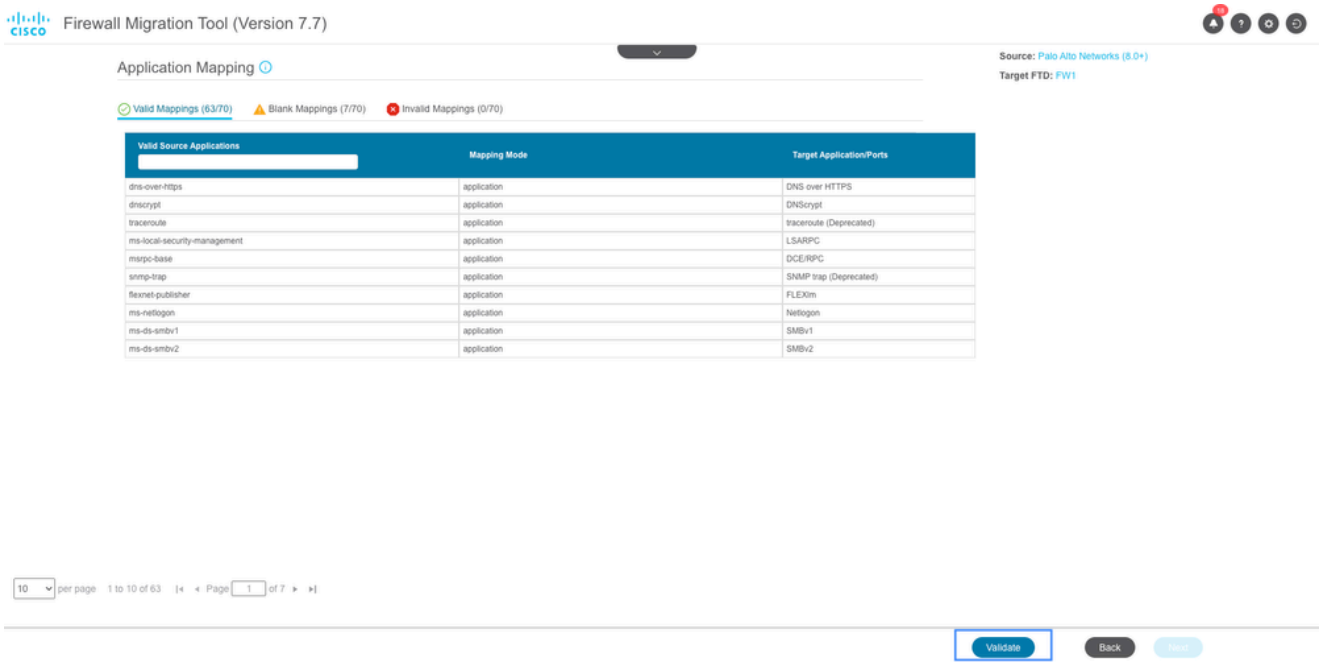
Creación manual de zonas de seguridad

Creación automática de zonas de seguridad:

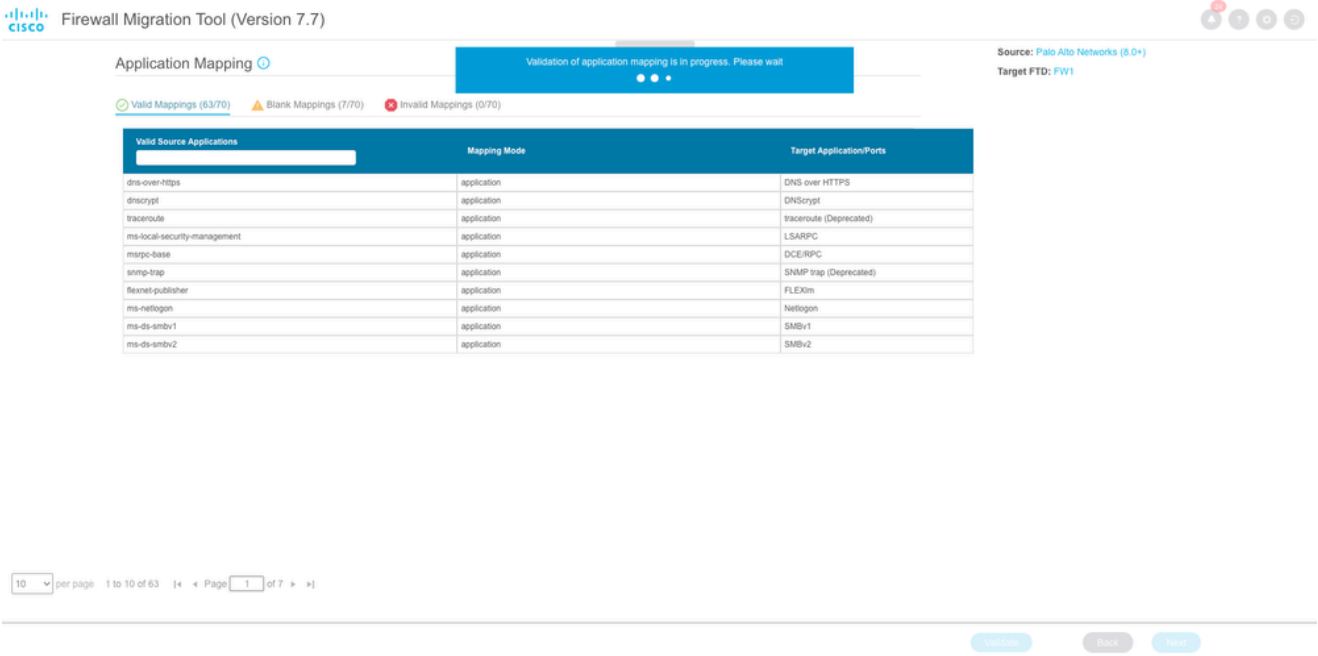


Creación automática de zonas de seguridad

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



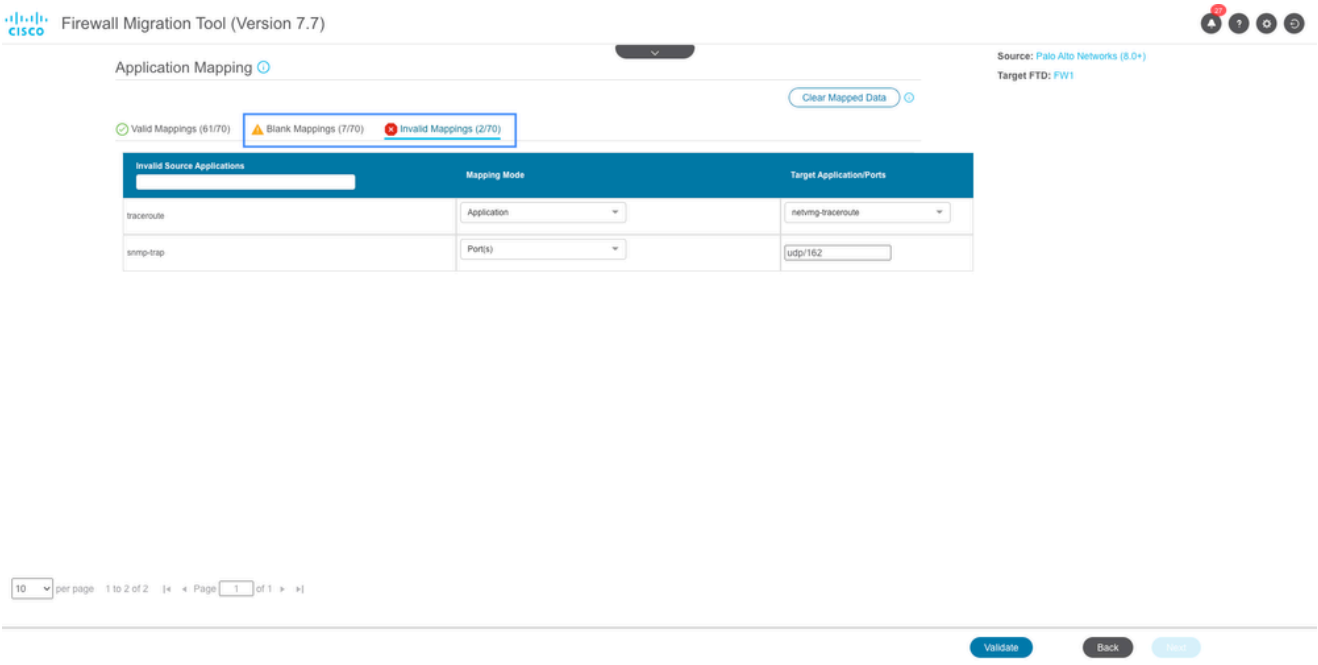
Asignación de aplicaciones



Validación de asignación de aplicaciones

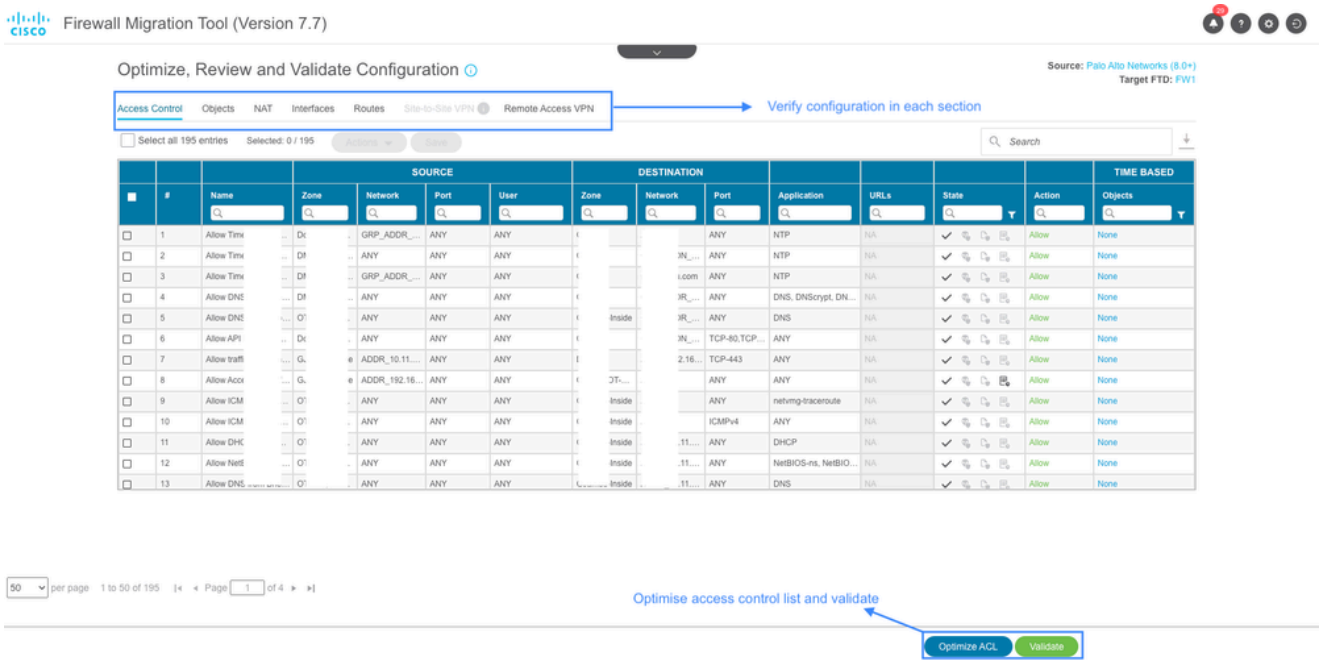
Tras la validación, FMT muestra las asignaciones en blanco y no válidas. Las asignaciones no válidas deben corregirse antes de continuar y la corrección de asignaciones en blanco es opcional.

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.



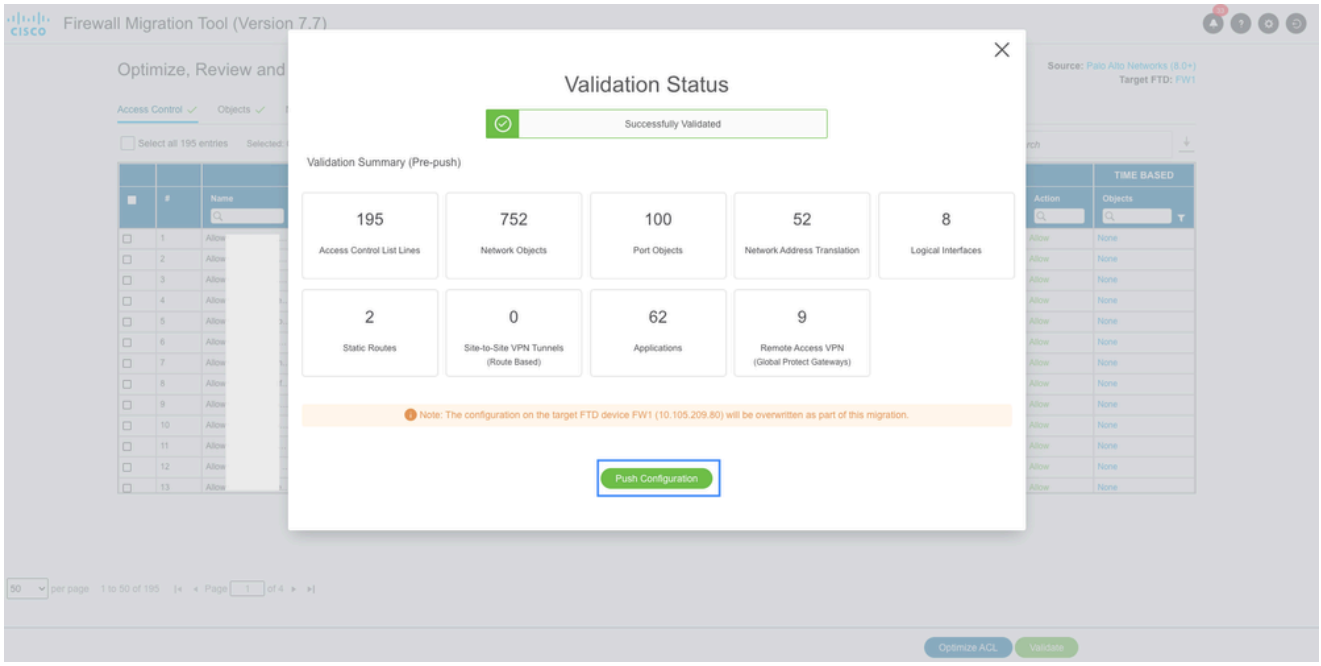
Asignación de aplicación en blanco e no válida

17. 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.



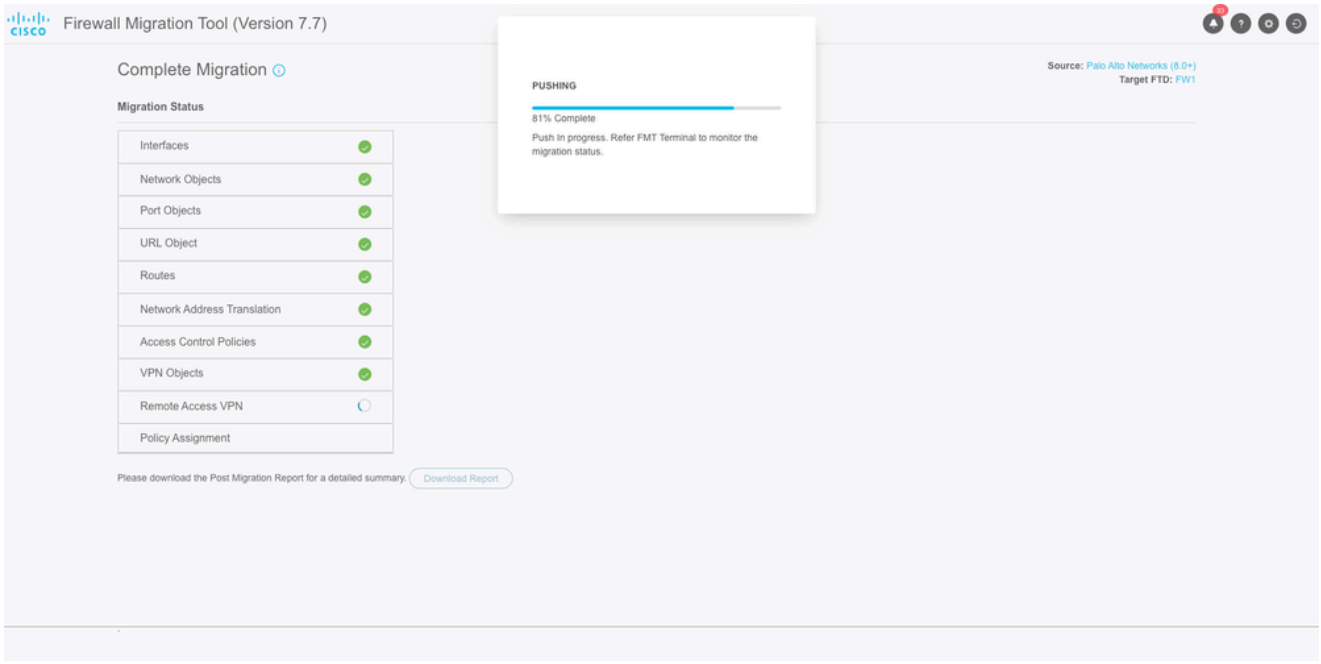
Validación de configuración

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.



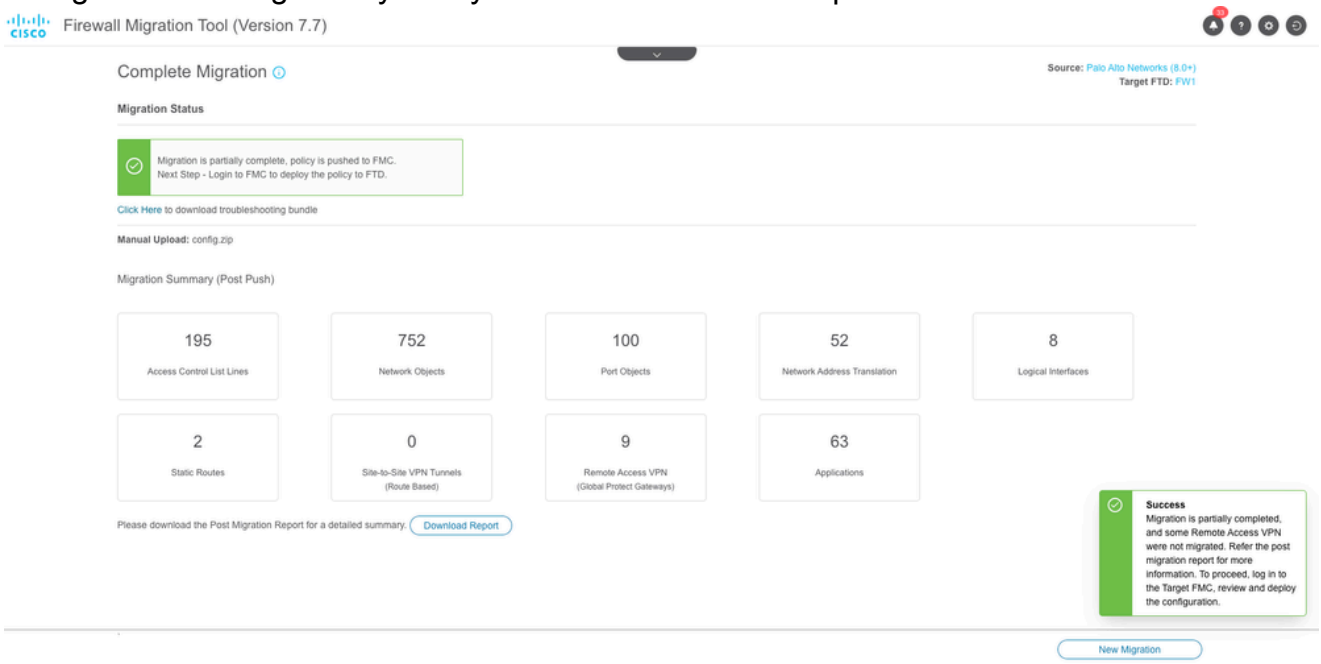
Resumen de validación de configuración

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).