Transición perfecta: Migración de Palo Alto Firewall a Cisco FTD

Contenido

Introducción

Este documento describe el proceso de transición de un firewall de Palo Alto a un sistema Cisco FTD mediante el uso de la versión 6.0 de FMT.

Prerequisites

Requirements

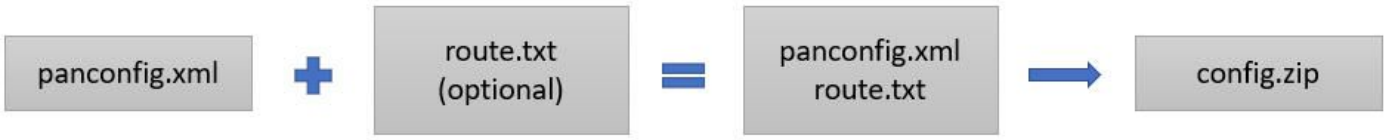
Cisco recomienda que tenga conocimiento sobre estos temas:

- Exportación de la configuración en ejecución actual desde el firewall de Palo Alto en formato XML (*.xml).
- Acceder a la CLI de Palo Alto Firewall y ejecutar el comando show routing route, luego guardar el resultado como un archivo de texto (*.txt).
- Comprimir el archivo de configuración (*.xml) y el archivo de salida de routing (*.txt) en un único archivo ZIP (*.zip).

Componentes Utilizados

La información de este documento se basa en la versión 8.4.x o posterior de Firewall de Palo Alto.

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.



Herramienta de migración de Firepower (FMT)

El FMT ayuda a los equipos de ingenieros en la transición de los firewalls de cualquier proveedor existente a los firewalls de última generación (NGFW)/Firepower Threat Defence (FTD) de Cisco. Asegúrese de utilizar la última versión de FMT, descargada desde el sitio web de Cisco.

Pauta de migración

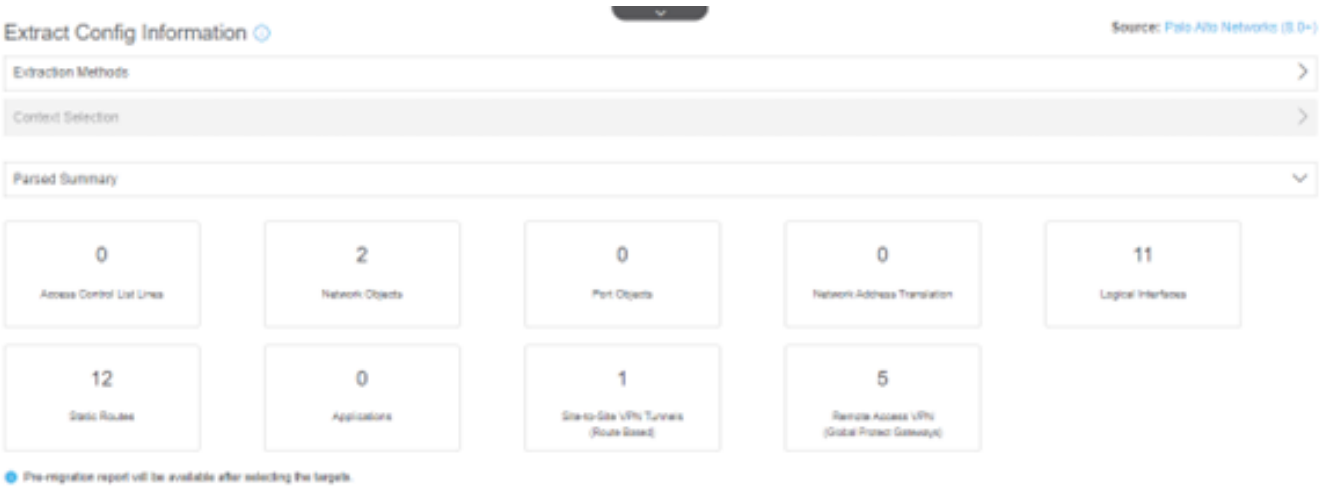
1. Lista de comprobación previa a la migración

- Asegúrese de que el FTD se ha añadido al FMC antes de comenzar el proceso de migración.
- Se ha creado una nueva cuenta de usuario con privilegios administrativos en el FMC.
- El archivo de configuración en ejecución file.xml de Palo Alto exportado debe comprimirse con la extensión .zip.
- El NGFW/FTD debe tener el mismo número de interfaces físicas, subinterfaces o canal de puerto que las interfaces de firewall de Palo Alto.

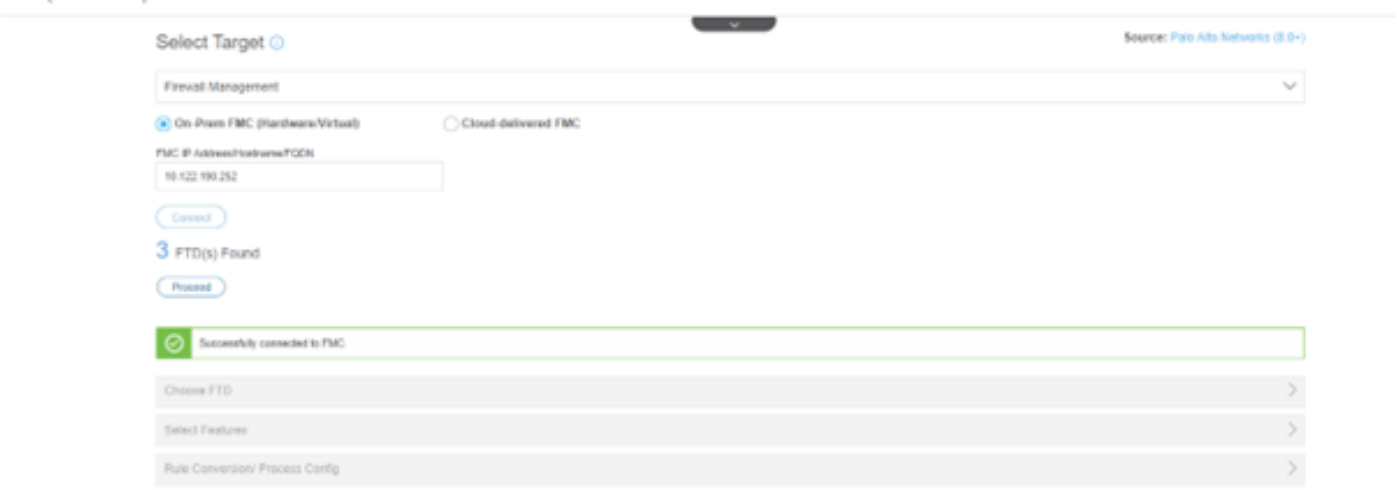
2. Uso de la herramienta de migración

- Descargue FMT tool .exe y ejecútelo como administrador.
- FMT requerirá una ID de CEC o una cuenta de usuario de Cisco para iniciar sesión.
- Post Successful login (Registro correcto) la herramienta mostrará un panel donde puede elegir el proveedor del firewall y cargar el archivo *.zip correspondiente; consulte la siguiente imagen.

- Revise atentamente las instrucciones proporcionadas en el lado derecho antes de continuar con la migración.
- Haga clic en Iniciar migración cuando esté listo para comenzar.
- Cargue el archivo *.zip guardado que contiene los parámetros de configuración del firewall de Palo Alto.
- Una vez cargado el archivo de configuración, podrá ver un resumen analizado del contenido y hacer clic en next; consulte la siguiente imagen.

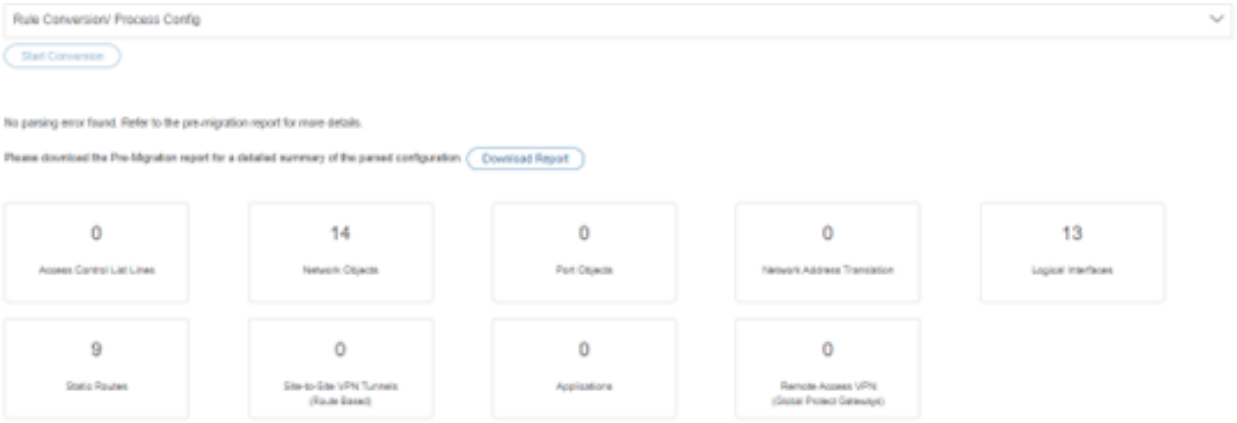


- Introduzca la dirección IP del CSP e inicie sesión.
- La herramienta buscará un FTD activo que se haya registrado en el FMC.
- Elija el FTD que desee migrar y haga clic en Proceed, como se muestra en la siguiente imagen.

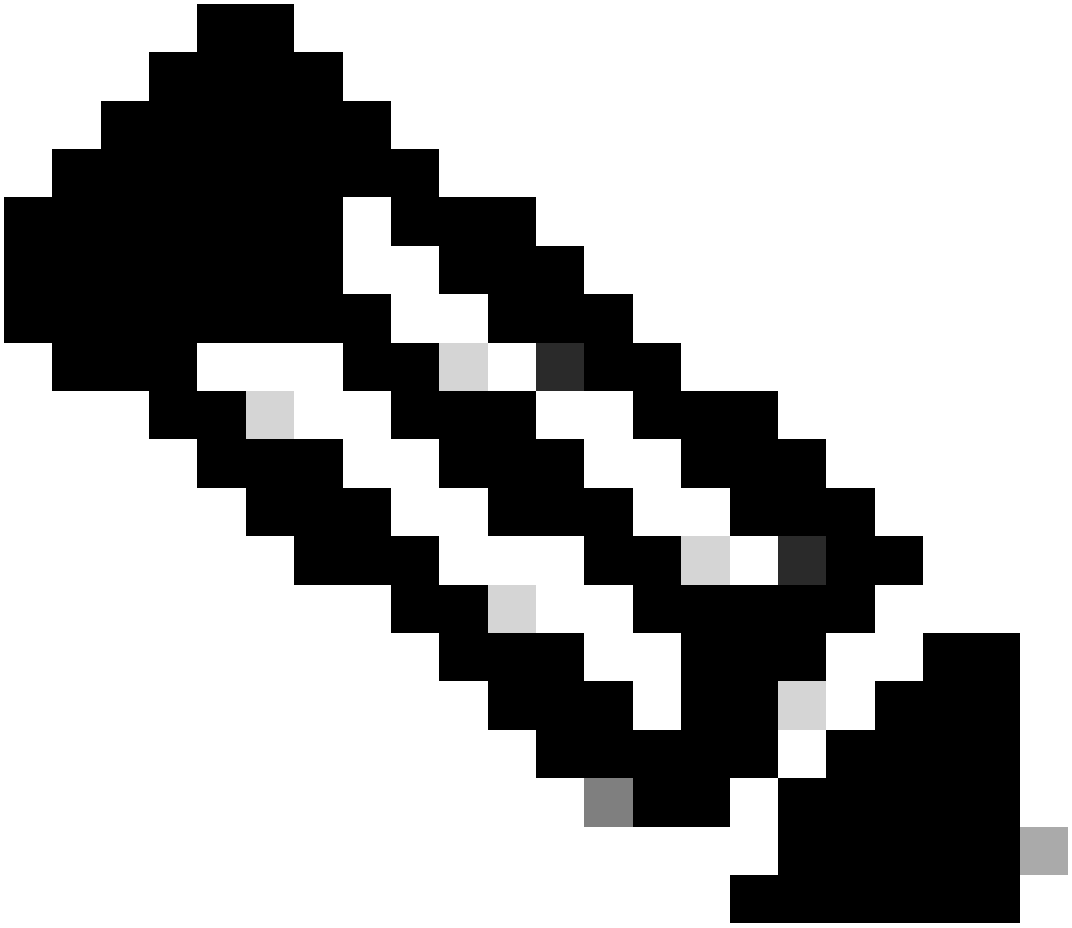


- Elija las características específicas para migrar en función de los requisitos del cliente. Tenga en cuenta que los firewalls de Palo Alto tienen un conjunto de funciones diferentes en comparación con el FTD.
- Haga clic en Proceed y consulte la siguiente imagen para referencia.

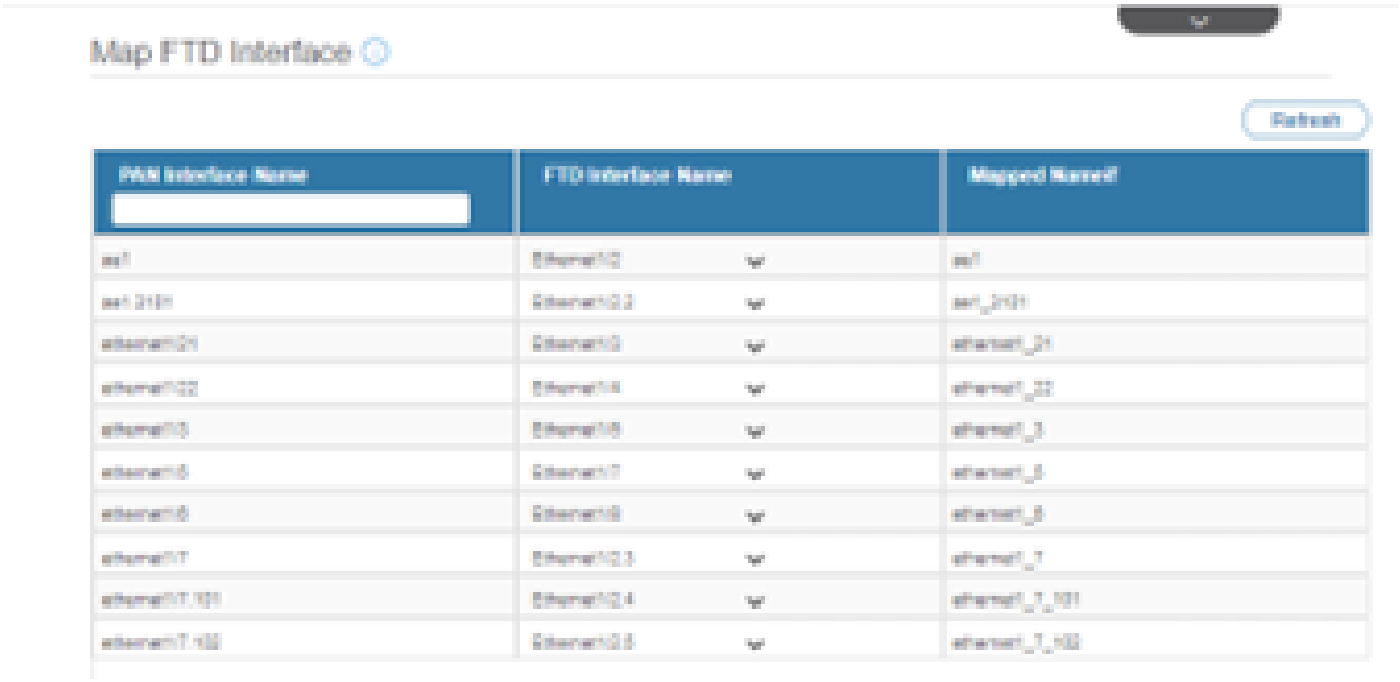
- El FMT ejecutará la conversión de acuerdo con sus selecciones. Revise los cambios en el informe anterior a la migración y, a continuación, haga clic en Continuar. Consulte la siguiente imagen para obtener ayuda.



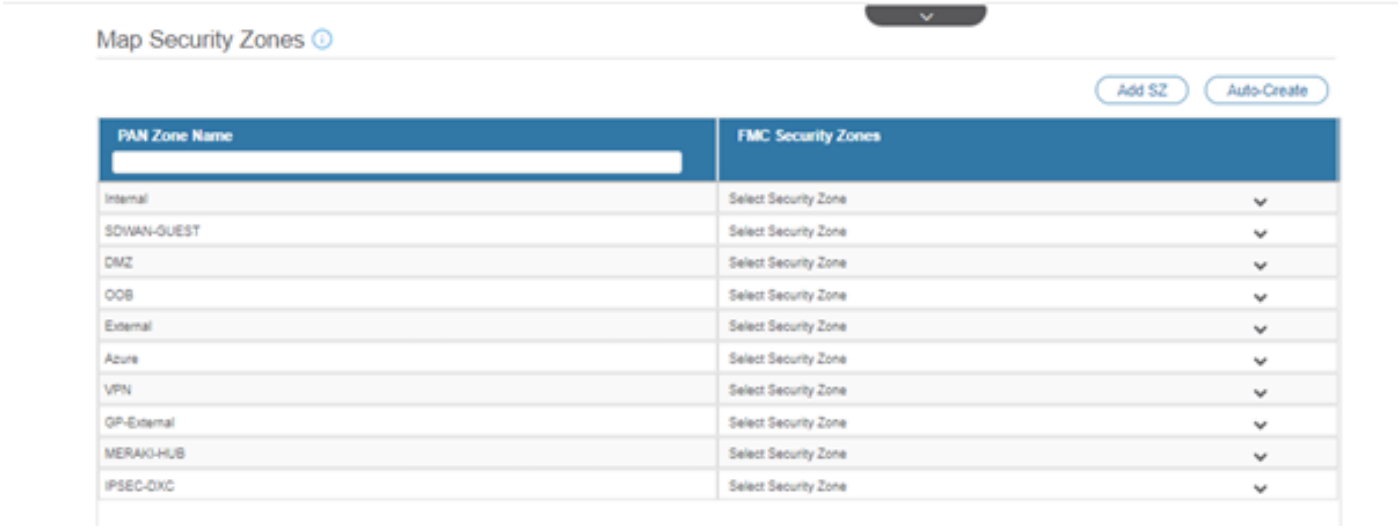
  - Asigne las interfaces del firewall de Palo Alto a las del FTD. Consulte la siguiente imagen para obtener más información.



Nota: El NGFW/FTD debe tener el mismo número de interfaces físicas, subinterfaces o Port-channel que las interfaces de firewall de Palo Alto, incluidas las subinterfaces.



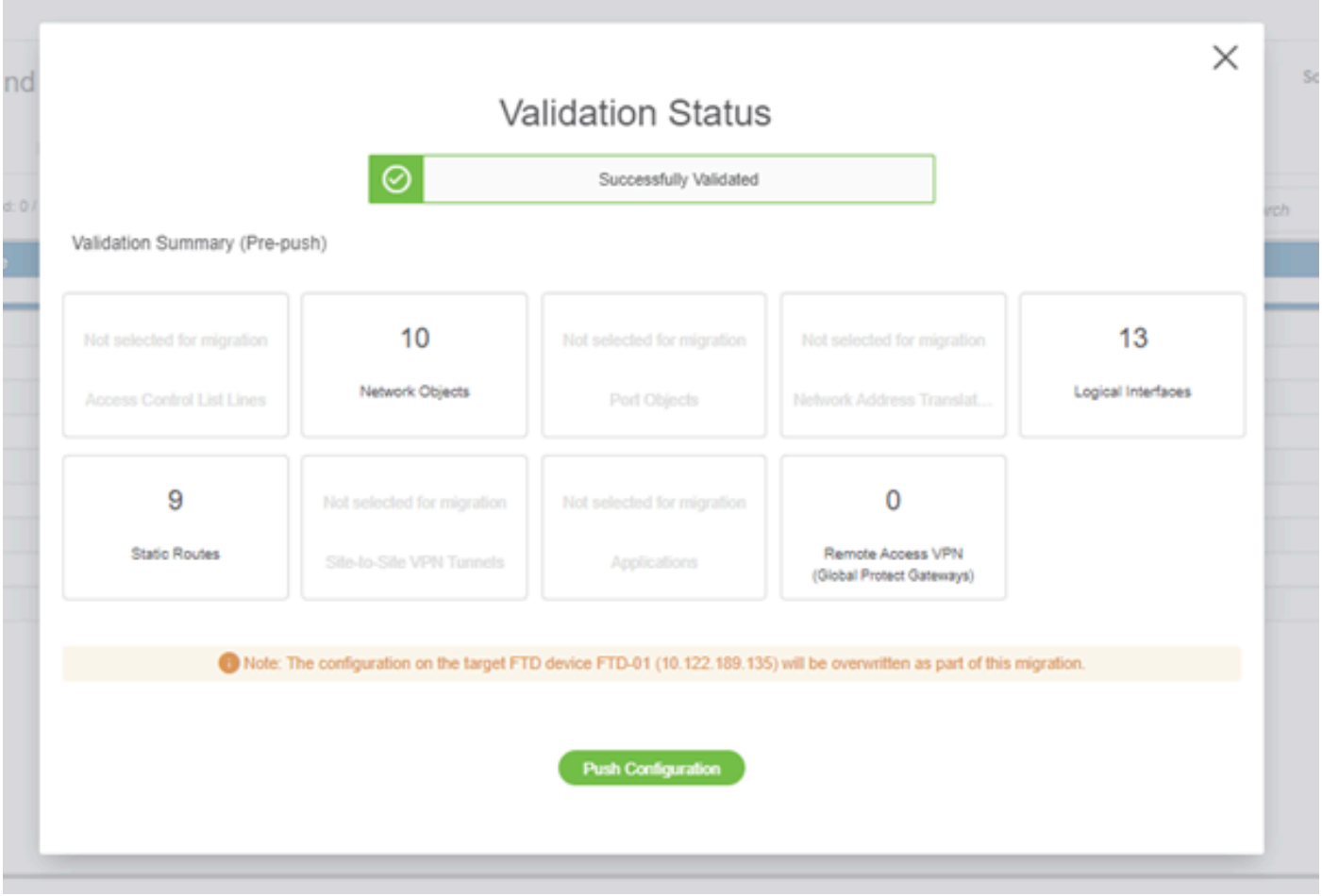
- Determine la asignación de zonas, que se puede realizar manualmente o mediante la función de creación automática. Para la visualización, consulte la siguiente imagen.



- Asigne su perfil de bloqueo de aplicaciones. Dado que se trata de un dispositivo de laboratorio sin asignación de aplicaciones, puede continuar con la configuración predeterminada. Haga clic en Next y consulte la imagen proporcionada.

- Optimice las ACL, los objetos, las interfaces y las rutas según sea necesario. Dado que se trata de una configuración de laboratorio con configuraciones mínimas, puede continuar con las opciones predeterminadas. A continuación, haga clic en Validar, haciendo referencia a la siguiente imagen.

- Una vez validada correctamente, la configuración está lista para implementarse en el FTD de destino. Consulte la siguiente imagen para obtener más instrucciones.



- La configuración de inserción guardará las configuraciones migradas en FMC y se implementará en el FTD automáticamente.
- En caso de que surja algún problema durante la migración, no dude en abrir un caso del TAC para obtener más asistencia.

3. Validación posterior a la migración

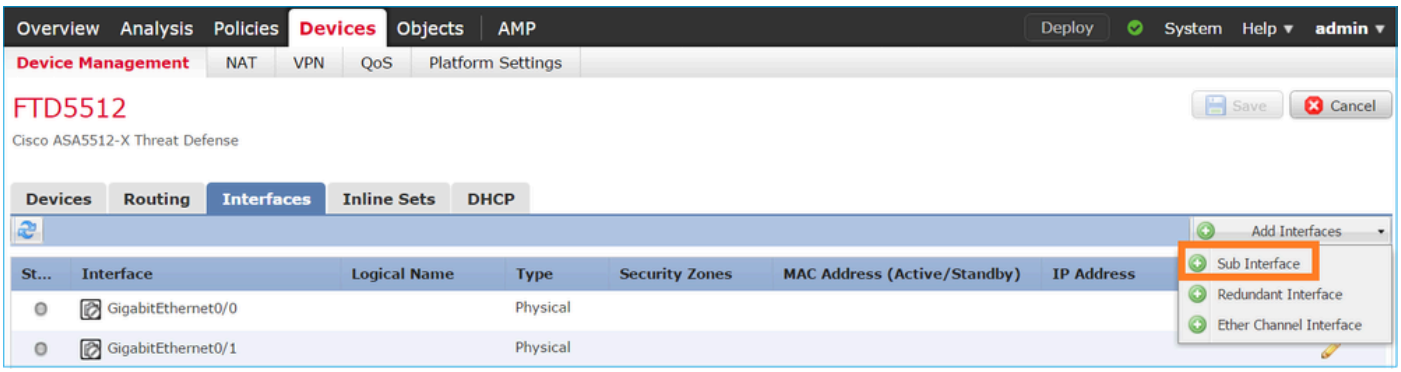
- Validación de la configuración en el FTD y el FMC.
- Prueba de las ACL del dispositivo, la política, la conectividad y otras funciones avanzadas.
- Cree un punto de reversión antes de realizar ningún cambio.
- Prueba de la migración en el entorno de laboratorio antes del lanzamiento en el entorno de producción.

Problemas conocidos

1. Interfaces faltantes en FTD

- Inicie sesión en Palo Alto CLI y ejecute el comando show interface all. Debe tener igual o más que el número de interfaces en FTD.
- Cree un número igual o superior de interfaces: subinterfaz, canal de puerto o interfaz física mediante la GUI de FMC.
- Navegue hasta Dispositivo GUI de FMC > Administración de dispositivos, haga clic en el FTD en el que se creará la interfaz requerida. En la sección Interfaz, en el menú

desplegable de la esquina derecha, elija Create Sub-interface/BVI en consecuencia y cree la interfaz y asocie las interfaces correspondientes. Guarde la configuración y sincronice con el dispositivo.



- Verifique que las interfaces se crean en FTD ejecutando Show interface ip brief y continúe con la migración para la asignación de interfaz.

2. Tabla de enrutamiento

- Verifique la tabla de ruteo en el firewall de Palo Alto ejecutando Show routing route o Show routing summary.
- Antes de migrar las rutas a FTD, verifique la tabla y elija las rutas requeridas según las necesidades del proyecto.
- Valide la misma tabla de ruteo en el FTD por Show route all y show route summary.

3. Optimizar

- El panel de optimización de objetos está atenuado; en ocasiones, debe crear un objeto manual en FMC y asignarlo. Para ver el objeto en FTD, utilice Show Running | en objetos y en Palo Alto, utilice Mostrar dirección <nombre de objeto>.
- La migración de aplicaciones requiere una auditoría del firewall de Palo Alto antes de la migración, FTD tiene un dispositivo IPS dedicado o puede habilitar la función en FTD para que tenga que planificar la tarea de migración de aplicaciones según los requisitos del cliente.
- La configuración NAT del firewall de Palo Alto se debe verificar mediante show running nat-policy y debe tener una política NAT personalizada en FTD, que se puede ver en FTD mediante Show Running nat.

Conclusión

El firewall de Palo Alto se ha migrado correctamente al FTD de Cisco con la ayuda del FMT. En caso de cualquier problema posterior a la migración en FTD y para la resolución de problemas, abra un caso TAC.

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).