Configuración de la migración de VPN entre FTD gestionados por un único FMC

Contenido

Introducción

Este documento describe la migración de una VPN de sitio a sitio de un FTD a otro, administrada por el mismo FMC, mientras se mantiene la conexión VPN con el router.

Prerequisites

Requirements

Para llevar a cabo el proceso de migración de forma eficaz, Cisco recomienda familiarizarse con los temas proporcionados:
· Registro FTD con FMC: Comprensión de cómo registrar dispositivos Firepower Threat Defence (FTD) con Firepower Management Center (FMC).
· Configuración de VPN de sitio a sitio: Experiencia en la configuración de VPN de sitio a sitio en dispositivos FTD gestionados por FMC.

Componentes Utilizados

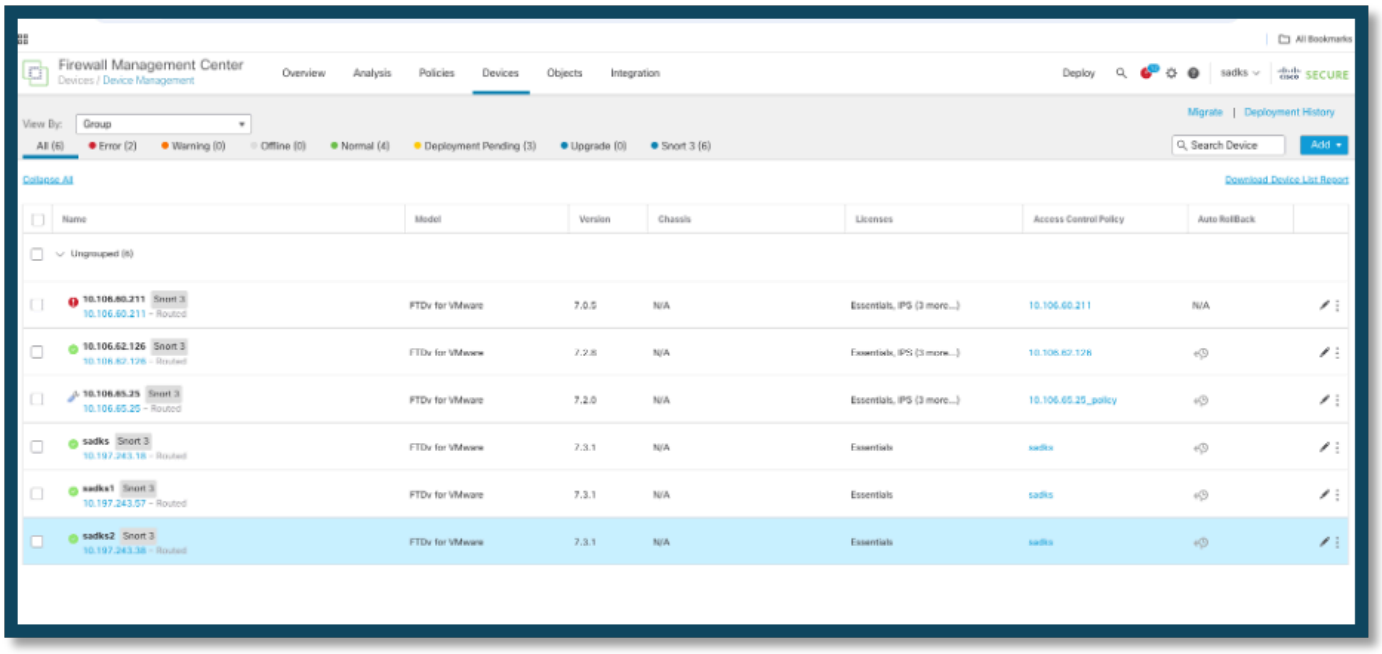
Este documento se basa en las versiones de software y hardware proporcionadas:
· Firepower Threat Defence Virtual (FTDv): Dos instancias que ejecutan la versión 7.3.1.
· FirePOWER Management Center (FMC): Versión 7.4.0.

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.

Configurar

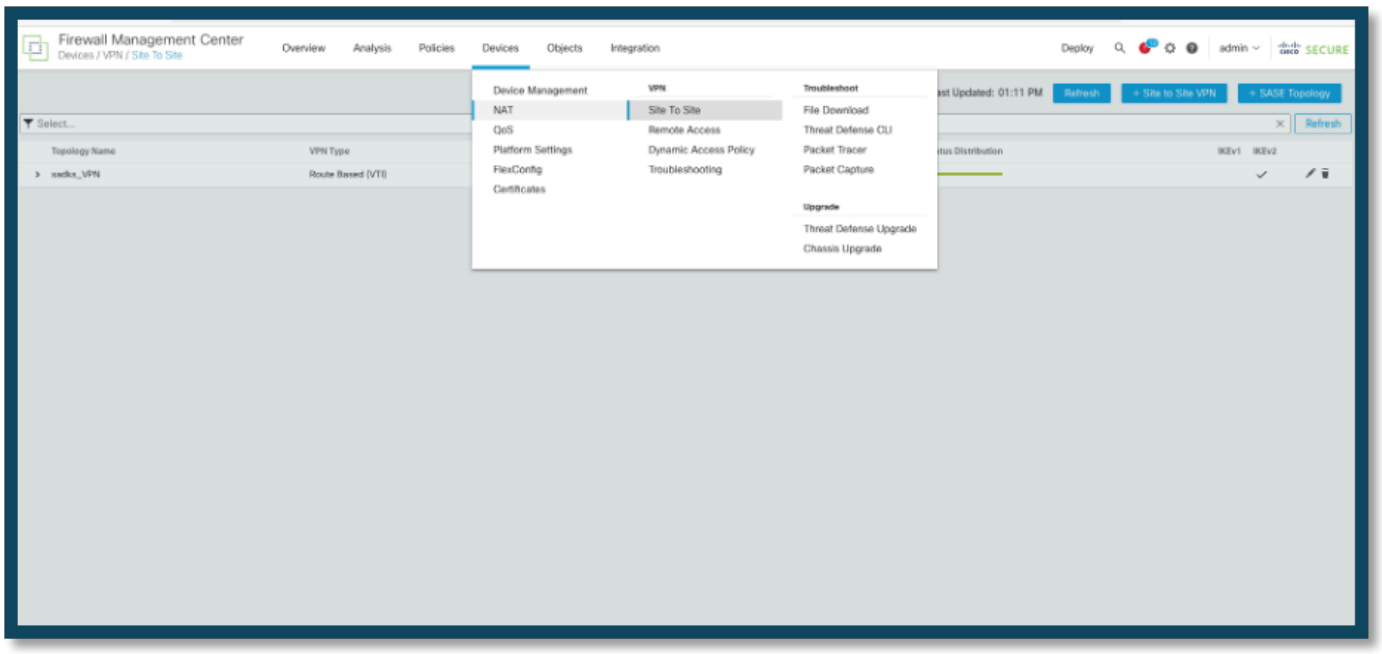
Procedimiento

1. Registrar el nuevo FTD en el CSP:
   · Empiece por registrar el nuevo dispositivo Firepower Threat Defence (FTD) en Firepower Management Center (FMC) en Dispositivos > Administración de dispositivos.
   · En este ejemplo, el nuevo dispositivo registrado se denomina "sadks2".



Nuevo FTD registrado

2. Acceda a la configuración del túnel de sitio a sitio:
   · Vaya a la configuración del túnel de sitio a sitio en Dispositivos > Sitio a sitio en la interfaz FMC.

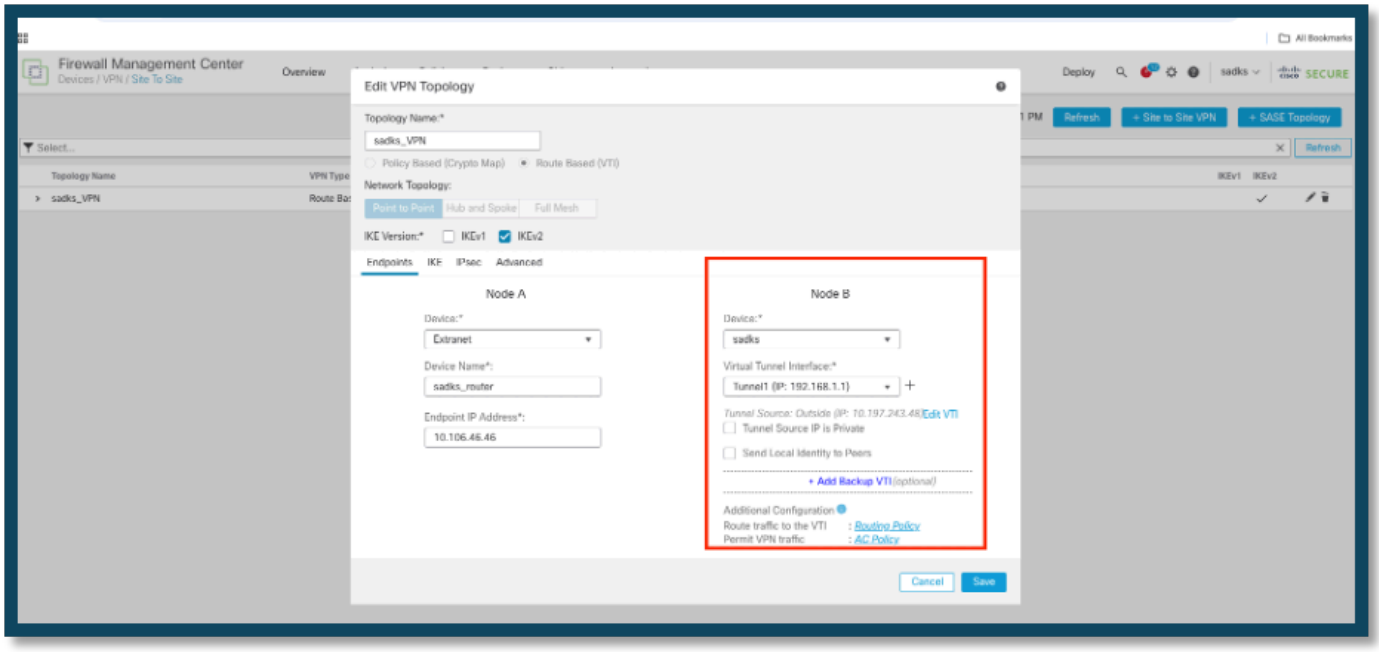


Vaya a Configuración de VPN

3. Modifique la configuración VPN:

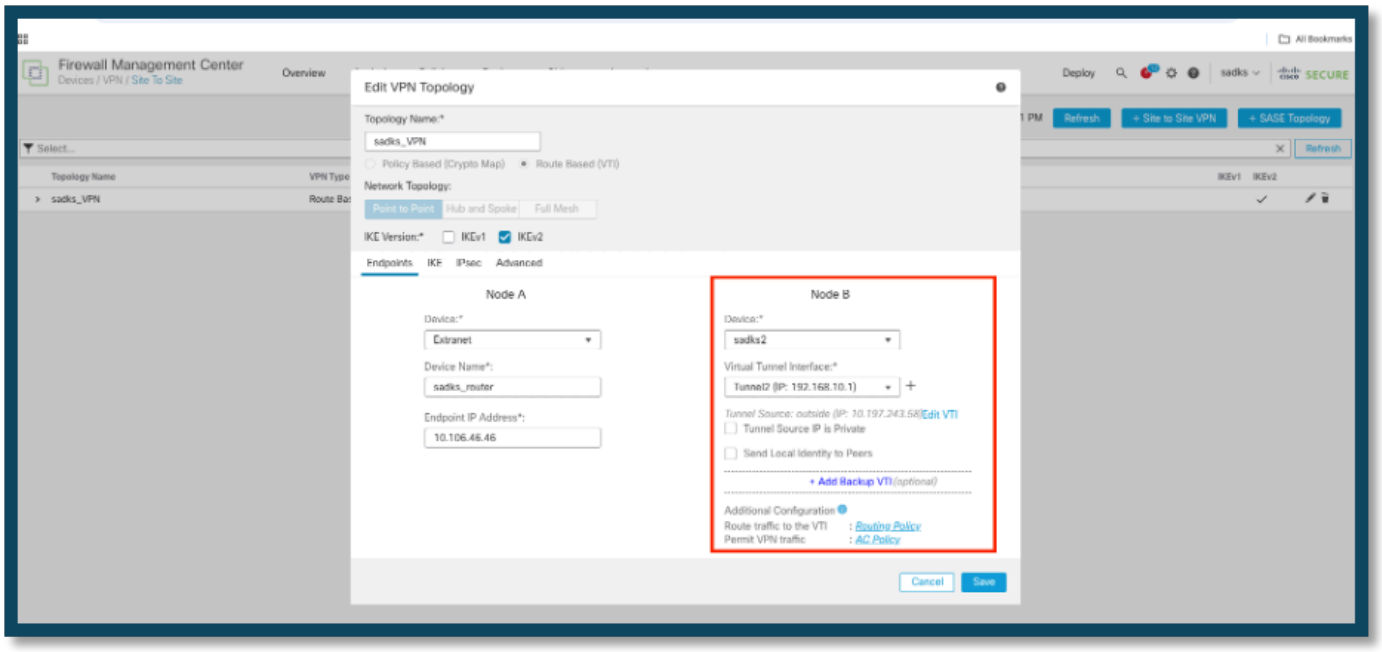
· Seleccione la configuración de VPN que desea actualizar.

•Ejemplo: En esta situación, la configuración VPN implica un dispositivo FTD y un router. Aquí, el Nodo B representa el dispositivo FTD, y la configuración se ha actualizado para cambiar la asociación del dispositivo de "sadks" a "sadks2".



Dispositivo FTD antiguo

A



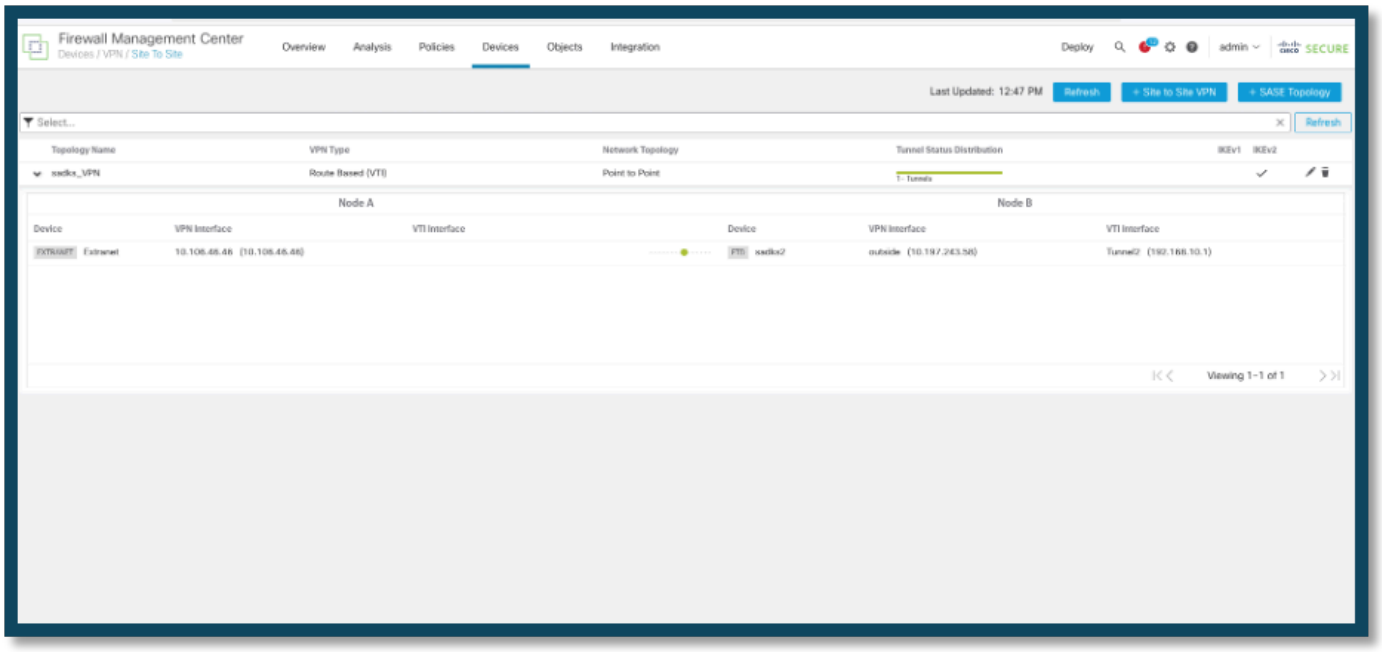
Nuevo dispositivo FTD

4. Guarde e implemente la configuración:

· Después de realizar los cambios necesarios, guarde la configuración e impleméntelo para activar las actualizaciones.

Verificación

El túnel aparece una vez implementado.



Estado del túnel

Troubleshoot

Problemas de conectividad inicial

Al crear una VPN, hay dos partes que negocian el túnel. Por lo tanto, es mejor obtener ambos lados de la conversación cuando resuelve cualquier tipo de falla de túnel. Una guía detallada sobre cómo depurar túneles IKEv2 se puede encontrar aquí: Cómo depurar VPN IKEv2

La causa más común de fallas de túnel es un problema de conectividad. La mejor manera de determinar esto es tomar capturas de paquetes en el dispositivo. Utilice este comando para tomar capturas de paquetes en el dispositivo:

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

Una vez que la captura esté en su lugar, intente enviar tráfico a través de la VPN y verifique si hay tráfico bidireccional en la captura de paquetes.

Revise la captura de paquetes con este comando:

<#root>

```
show cap capout
```

Problemas Específicos Del Tráfico

Los problemas comunes de tráfico que experimenta son:

- Problemas de ruteo detrás del FTD: la red interna no puede rutear paquetes de vuelta a las direcciones IP asignadas y a los clientes VPN.
- Listas de control de acceso que bloquean el tráfico.
- Traducción de direcciones de red que no se omite para el tráfico VPN.

Para obtener más información sobre las VPN en el FTD gestionado por FMC, puede encontrar la guía de configuración completa aquí: Guía de configuración de FTD administrada por FMC

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).