Configuración de Dual ISP VTI en FTD gestionado por FMC

Contenido

Introducción

Este documento describe la implementación de la configuración de ISP dual mediante interfaces de túnel virtual en un dispositivo FTD administrado por FMC.

Prerequisites

Requisitos básicos

- Una comprensión básica de las VPN de sitio a sitio sería beneficiosa. Estos antecedentes ayudan a comprender el proceso de configuración de VTI, incluidos los conceptos y configuraciones clave implicados.
- Es fundamental comprender los aspectos básicos de la configuración y la administración de las VTI en la plataforma Cisco Firepower. Esto incluye el conocimiento de cómo funcionan las VTI en el FTD y cómo se controlan a través de la interfaz FMC.

Componentes Utilizados

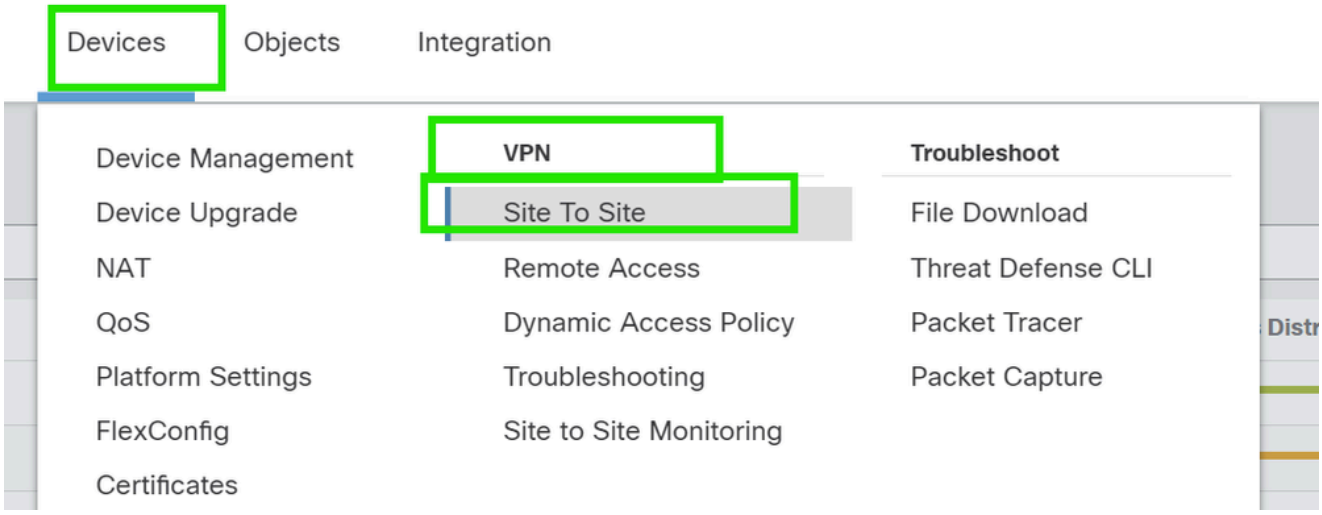
- Cisco Firepower Threat Defense (FTD) para VMware: versión 7.0.0
- Firepower Management Center (FMC): versión 7.2.4 (compilación 169)

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.

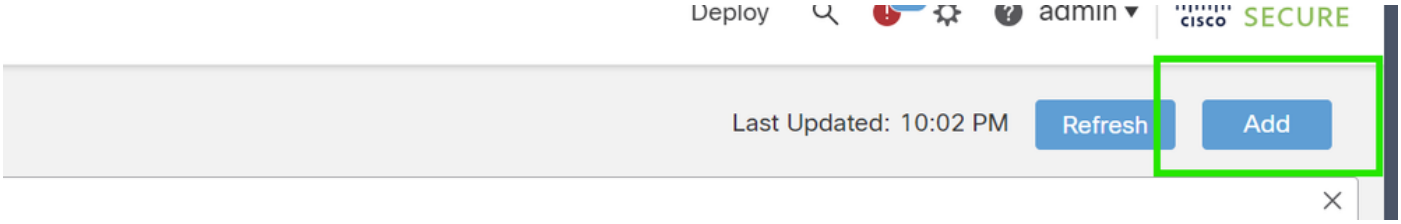
Configuraciones en FMC

Configuración de topología

1. Vaya a Devices > VPN > Site To Site.



2. Haga clic en Agregar para agregar la topología VPN.



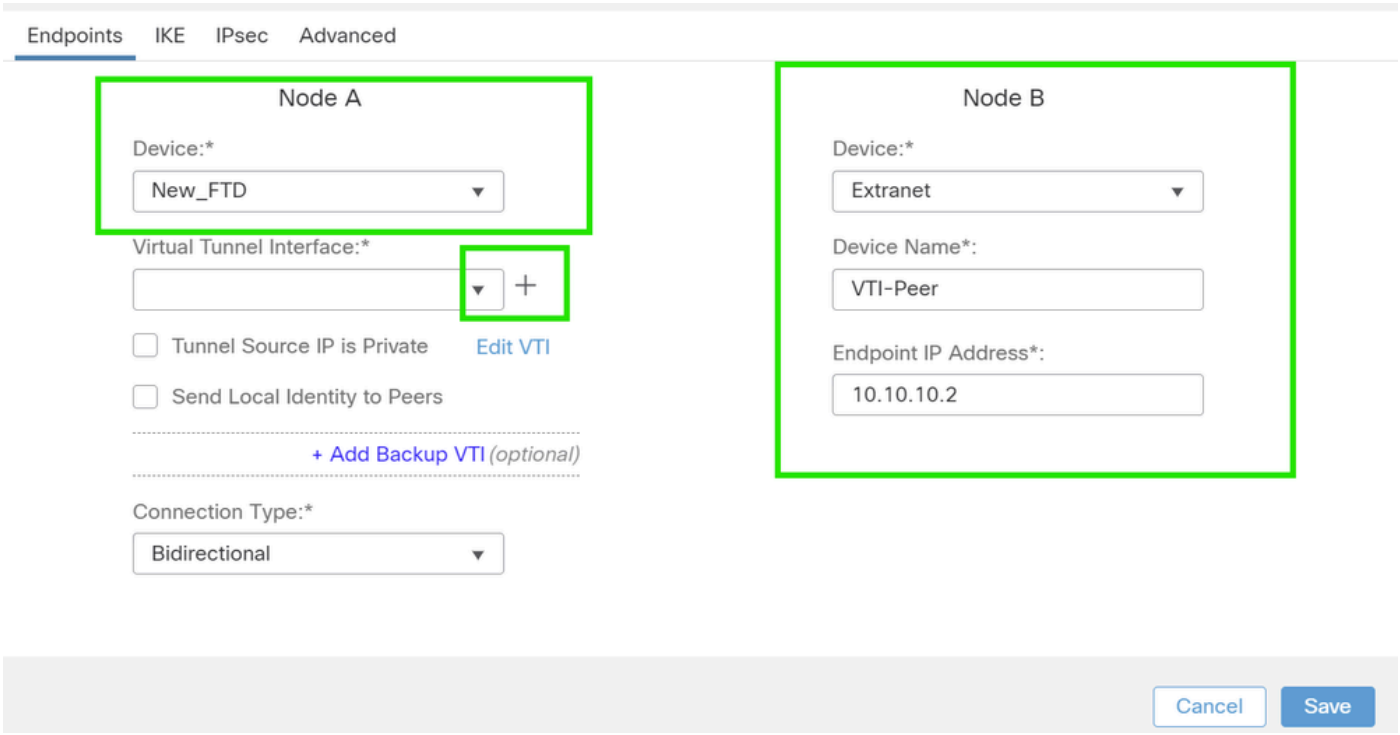
3. Dé un nombre a la topología, elija VTI y Point-to-Point, y seleccione una versión IKE (IKEv2 en este caso).

Configuración de terminales

1. Seleccione el dispositivo en el que debe configurarse el túnel.

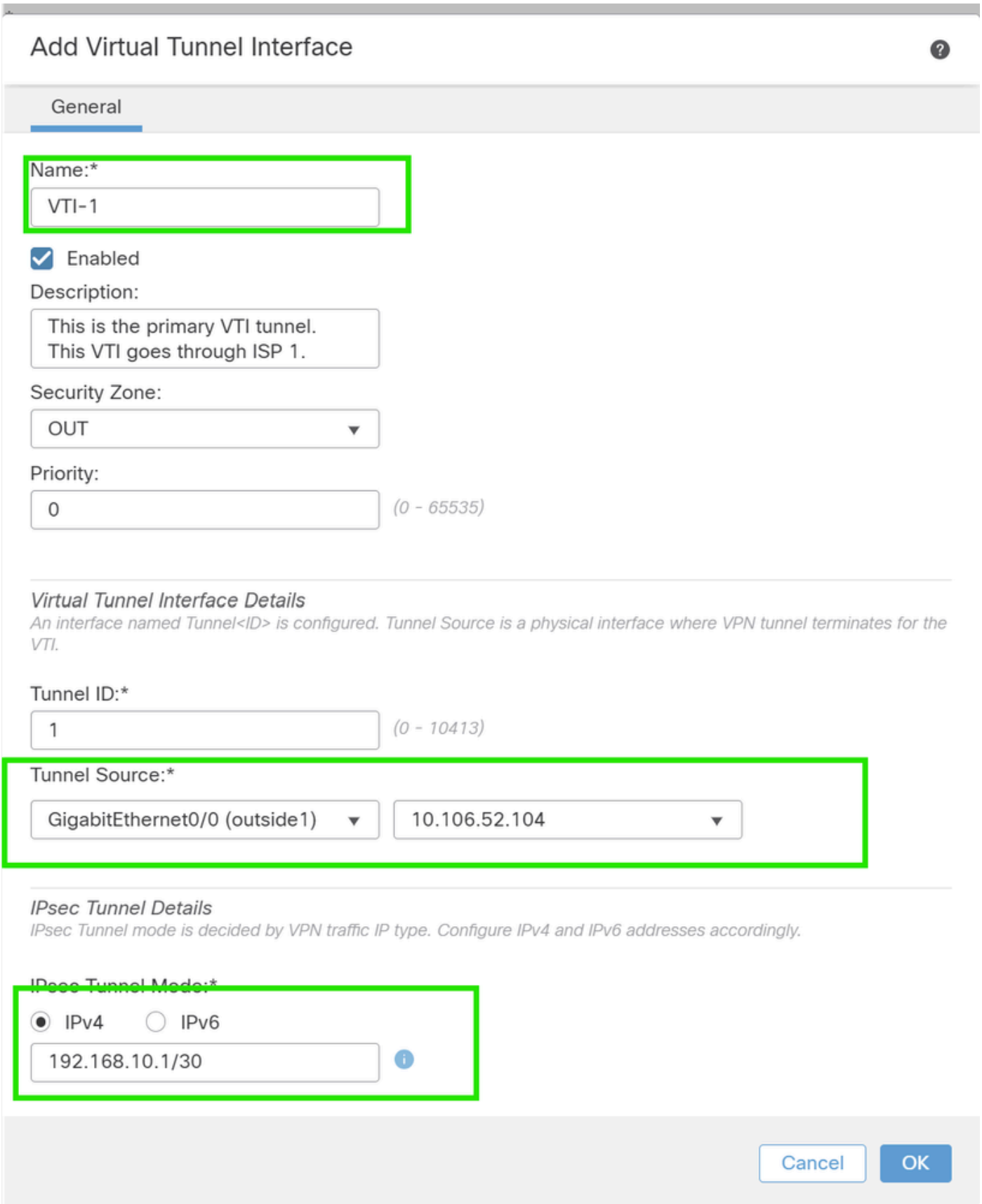
Agregue los detalles del par remoto.

Puede agregar una nueva interfaz de plantilla virtual haciendo clic en el icono "+" o seleccionar una de la lista existente.

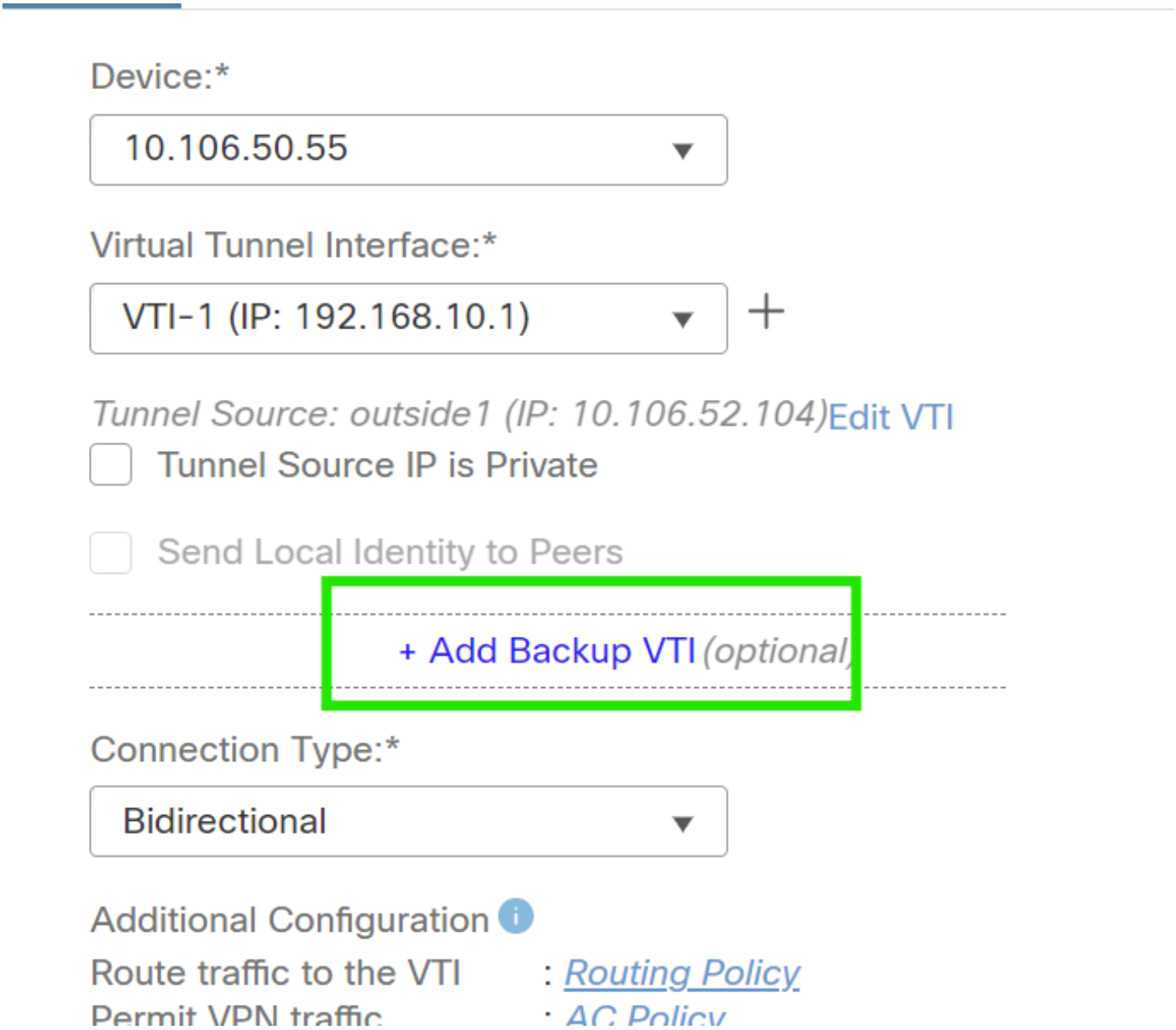


Si está creando una nueva interfaz VTI, agregue los parámetros correctos, habilítela y haga clic en "Aceptar".

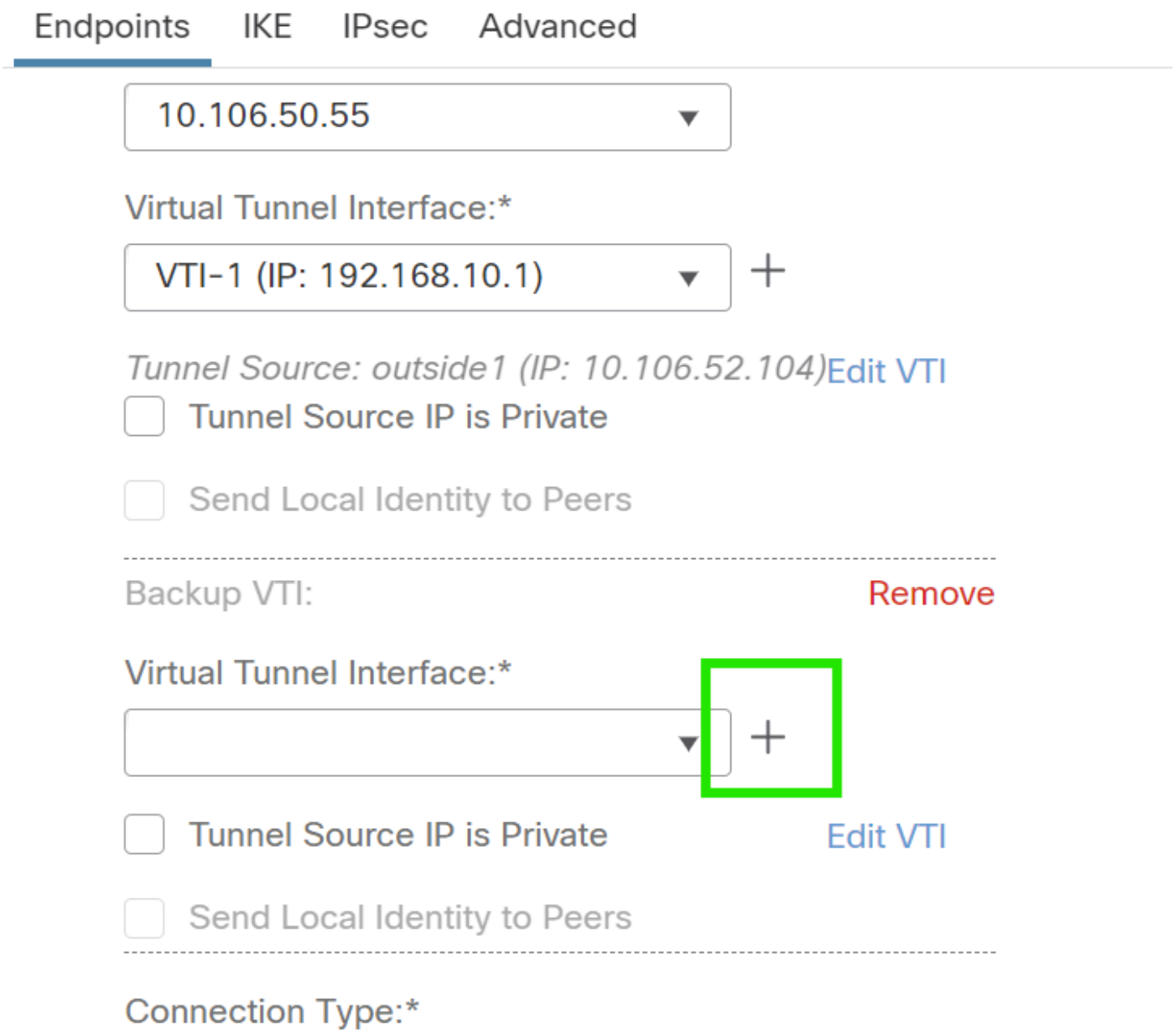
NOTA: Se convierte en la VTI principal.



3. Haga clic en "+ ". Add Backup VIT" para agregar un VIT secundario.

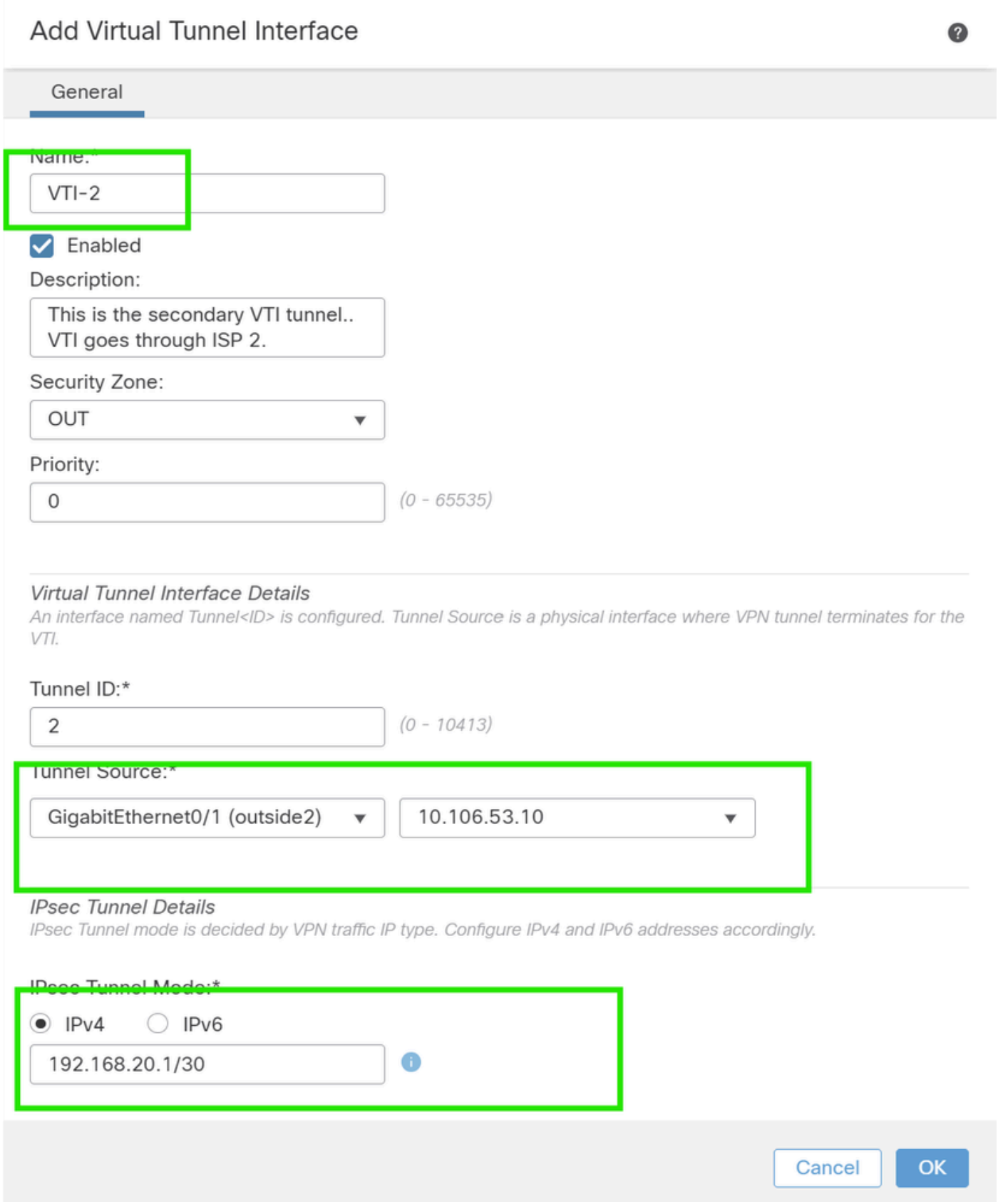


4. Haga clic en "+" para agregar un parámetro para VTI secundario (si no está ya configurado).



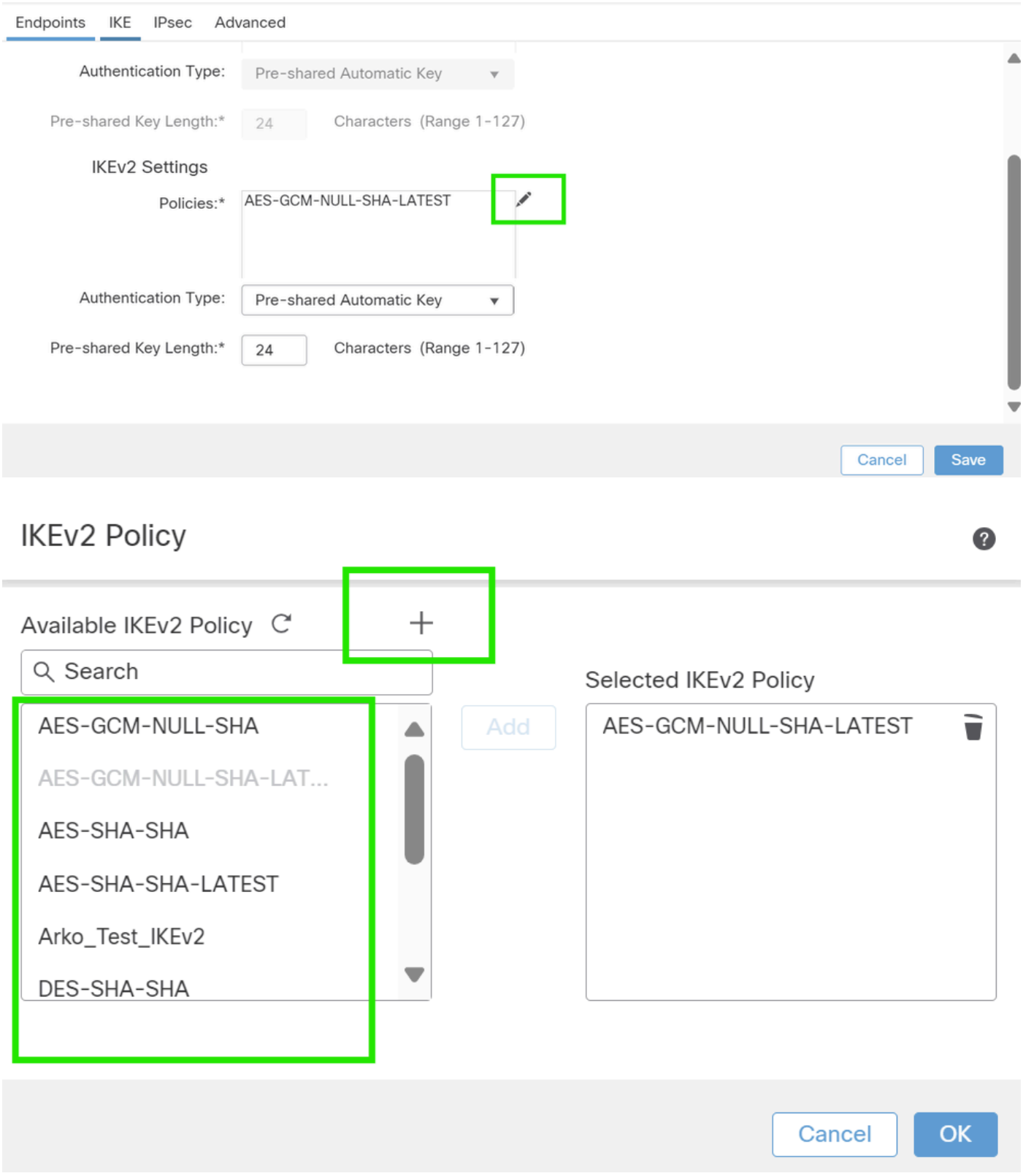
5. Si está creando una nueva interfaz VTI, agregue los parámetros correctos, actívela y haga clic en "Aceptar".

NOTA: Se convierte en la VTI secundaria.

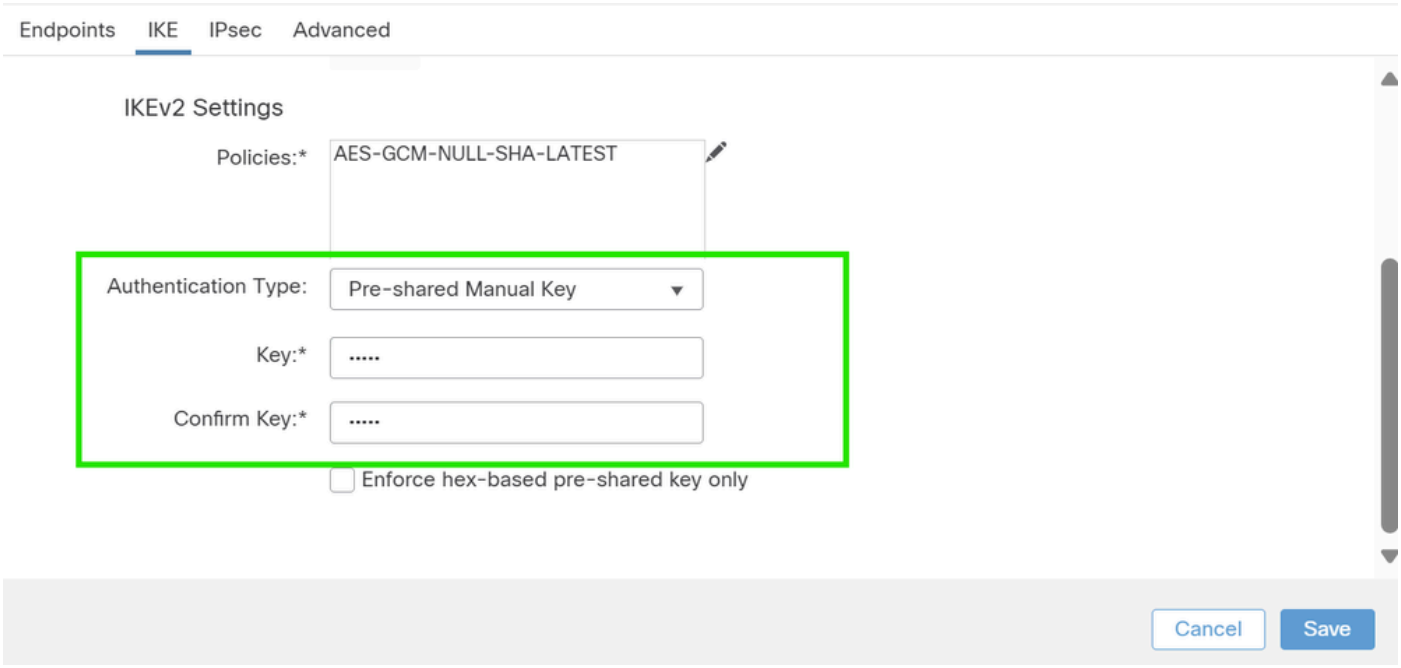


configuración IKE

1. Acceda a la pestaña IKE. Si lo desea, puede utilizar una directiva predefinida; de lo contrario, haga clic en el botón de lápiz situado junto a la ficha Directiva para crear una nueva directiva o seleccione otra directiva disponible en función de sus necesidades.

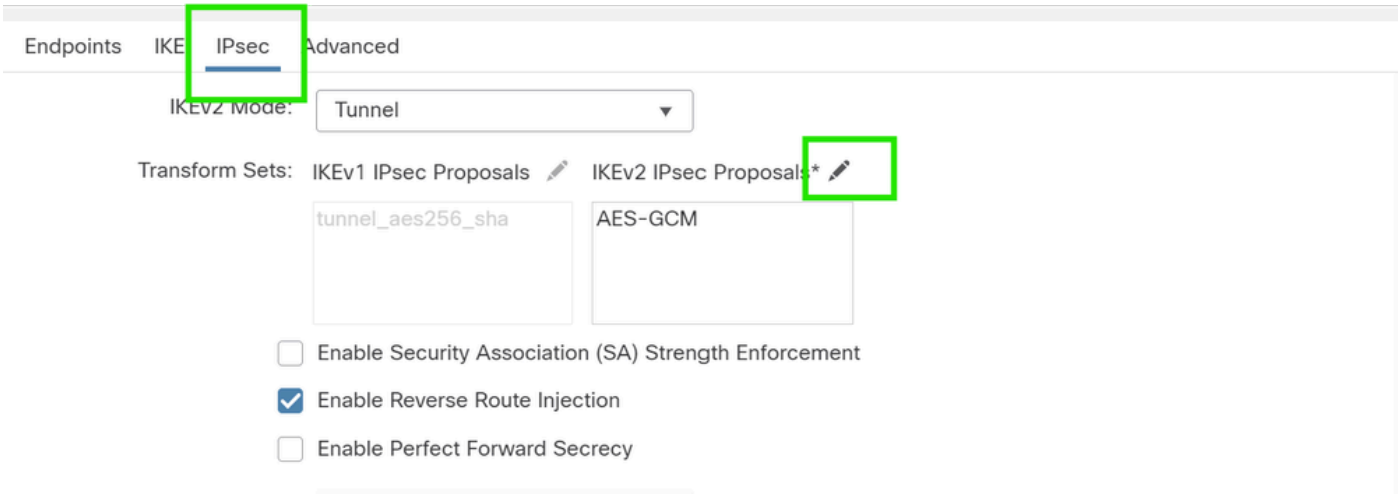


2. Seleccione el tipo de autenticación. Si se utiliza una clave manual previamente compartida, especifíquela en los cuadros Key (Clave) y Confirm Key (Confirmar clave).



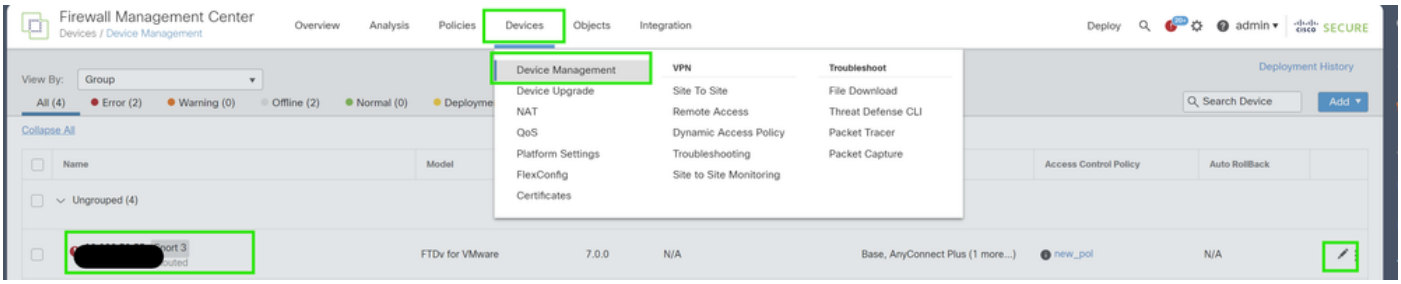
configuración de IPsec

Vaya a la ficha IPsec. Puede optar por utilizar una propuesta predefinida haciendo clic en el botón de lápiz situado junto a la ficha de propuesta para crear una nueva propuesta o seleccionar otra propuesta disponible en función de sus necesidades.



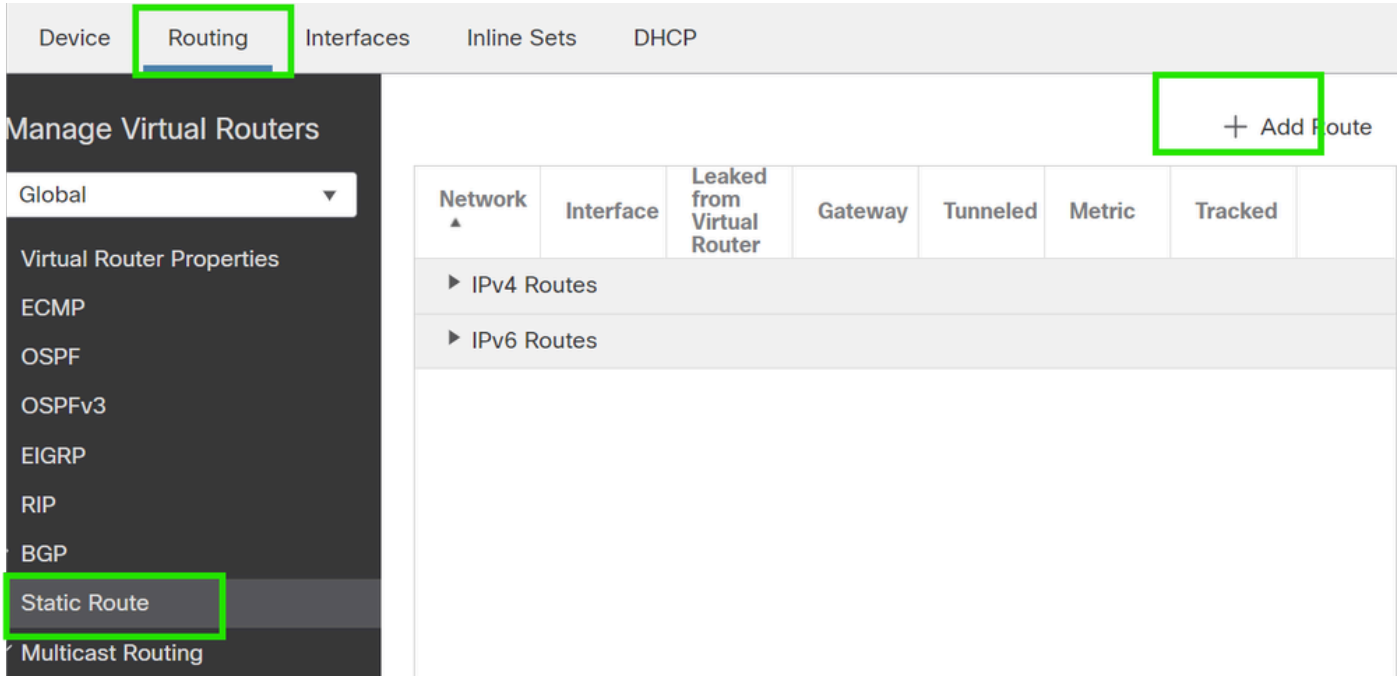
Configuración de Ruteo

1. Vaya a Device > Device Management y haga clic en el icono del lápiz para editar el dispositivo (FTD).



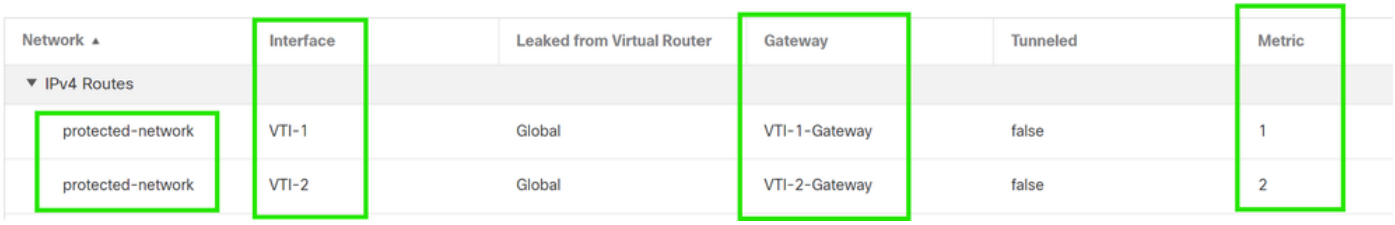
2. Vaya a Routing > Static Route (Enrutamiento > Ruta estática) y haga clic en el botón "+" para agregar una ruta al VTI principal y secundario.

NOTA: Puede configurar el método de routing adecuado para que el tráfico pase a través de la interfaz de túnel. En este caso, se han utilizado rutas estáticas.



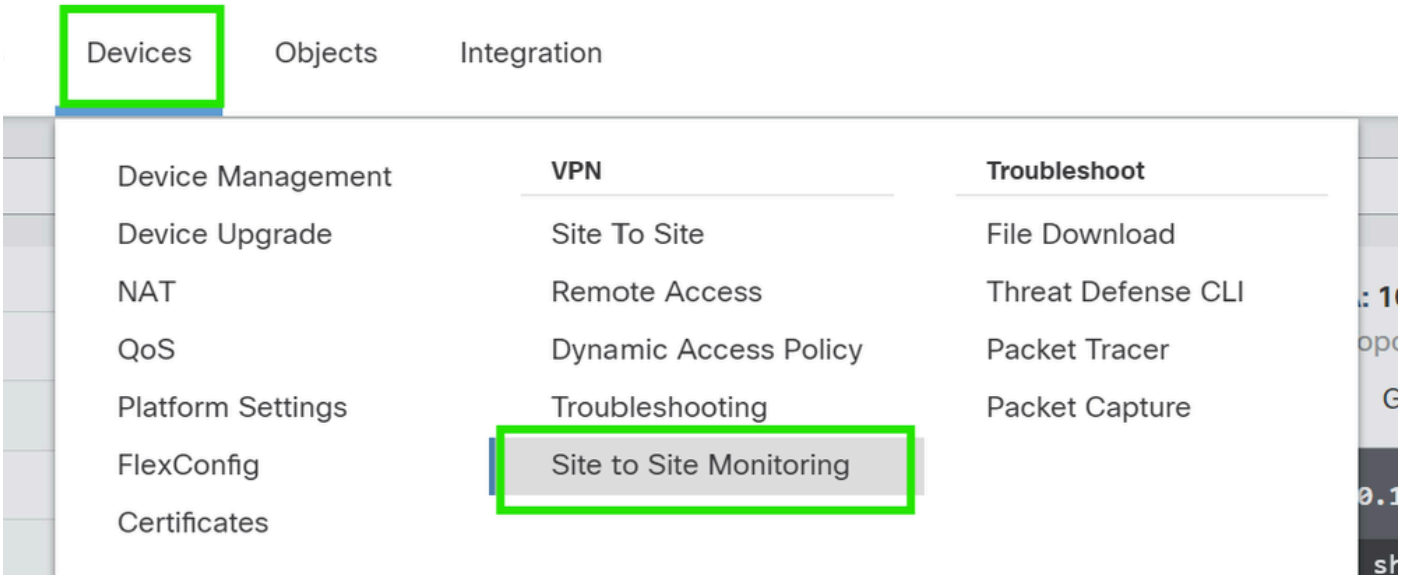
3. Agregue dos rutas para su red protegida y establezca un valor AD más alto (en este caso, 2) para la ruta secundaria.

La primera ruta utiliza la interfaz VTI-1 y la segunda la interfaz VTI-2.

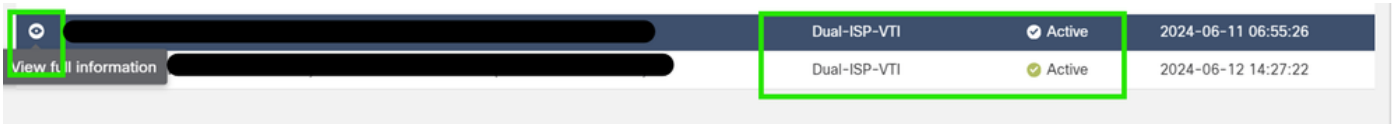


Verificación

1. Vaya a Dispositivos > VPN > Supervisión de sitio a sitio .



2. Haga clic en el ojo para ver más detalles sobre el estado del túnel.



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).