Configuración de VPN basada en rutas con ruta estática en FTD administrada por FDM

Contenido

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio basado en ruta estática en un FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de cómo funciona un túnel VPN.
- Conocimientos previos sobre la navegación por Firepower Device Manager (FDM).

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

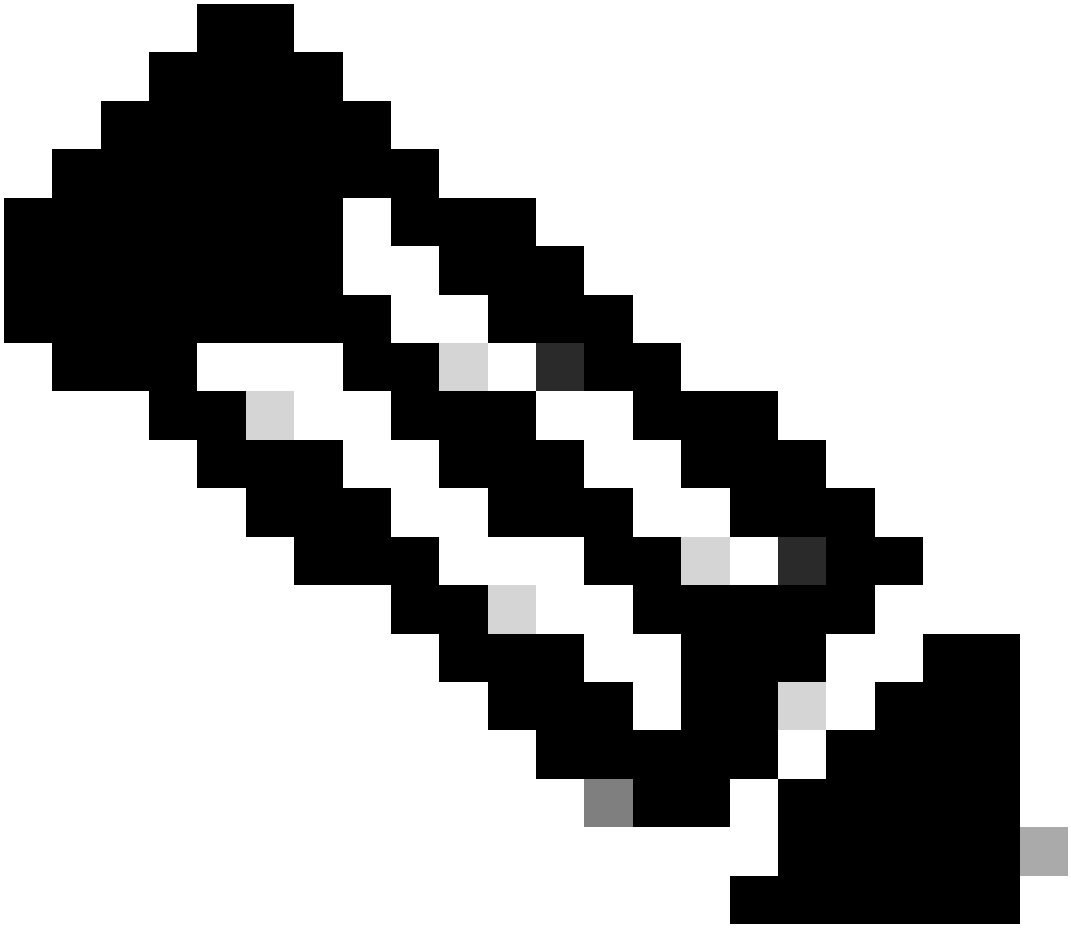
- Cisco Firepower Threat Defence (FTD) versión 7.0 gestionada por Firepower Device Manager (FDM).

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.

Antecedentes

La VPN basada en rutas permite la determinación del tráfico interesante que se va a cifrar o enviar a través del túnel VPN, y utiliza el ruteo del tráfico en lugar de la política/lista de acceso como en la VPN basada en políticas o en el mapa criptográfico. El dominio de cifrado está configurado para permitir cualquier tráfico que ingrese al túnel IPsec. Los selectores de tráfico local y remoto de IPsec se establecen en 0.0.0.0/0.0.0.0. Esto significa que cualquier tráfico enrutado en el túnel IPsec se cifra independientemente de la subred de origen/destino.

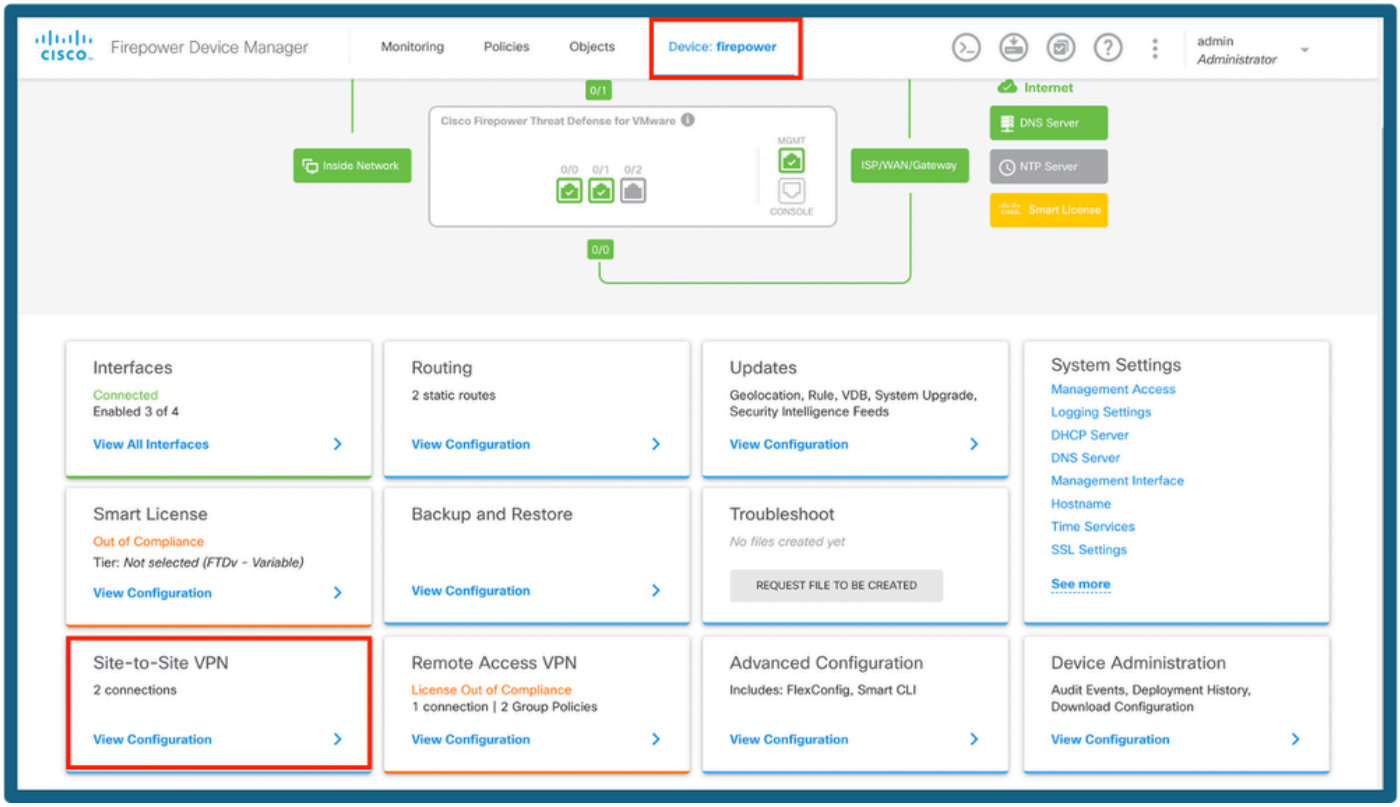
Este documento se centra en la configuración de la Interfaz de Túnel Virtual Estática (SVTI).



> Nota: No se necesitan licencias adicionales, la VPN basada en rutas se puede configurar en los modos con licencia y de evaluación. Sin cumplimiento de cifrado (funciones controladas de exportación habilitadas), sólo se puede utilizar DES como algoritmo de cifrado.

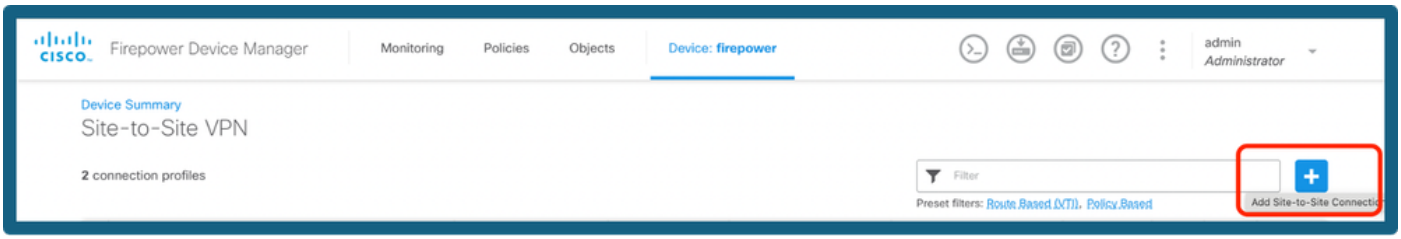
Pasos de configuración en FDM

Paso 1. Vaya a Dispositivo > Sitio a Sitio.



Panel de FDM

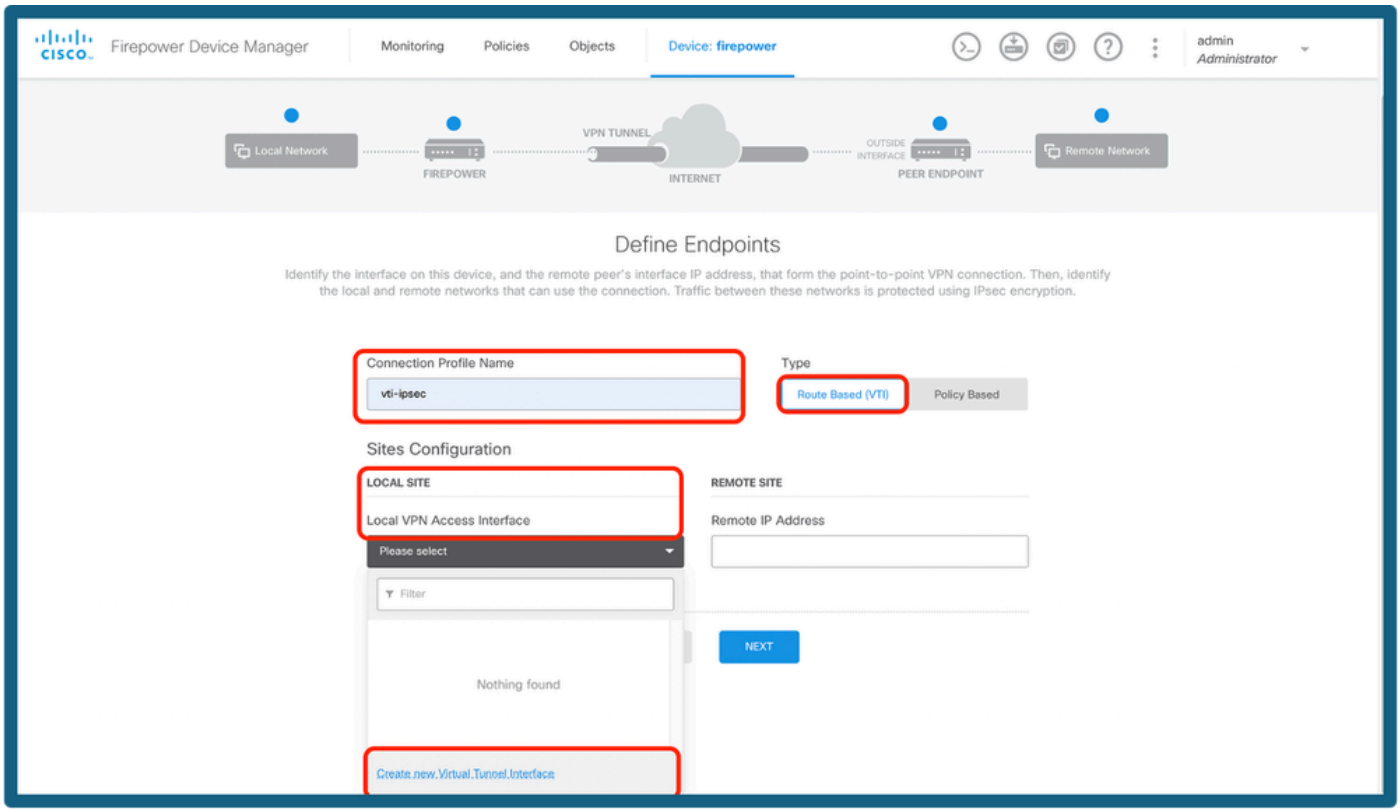
Paso 2. Haga clic en el icono + para agregar un nuevo sitio a la conexión del sitio.



Agregar una conexión S2S

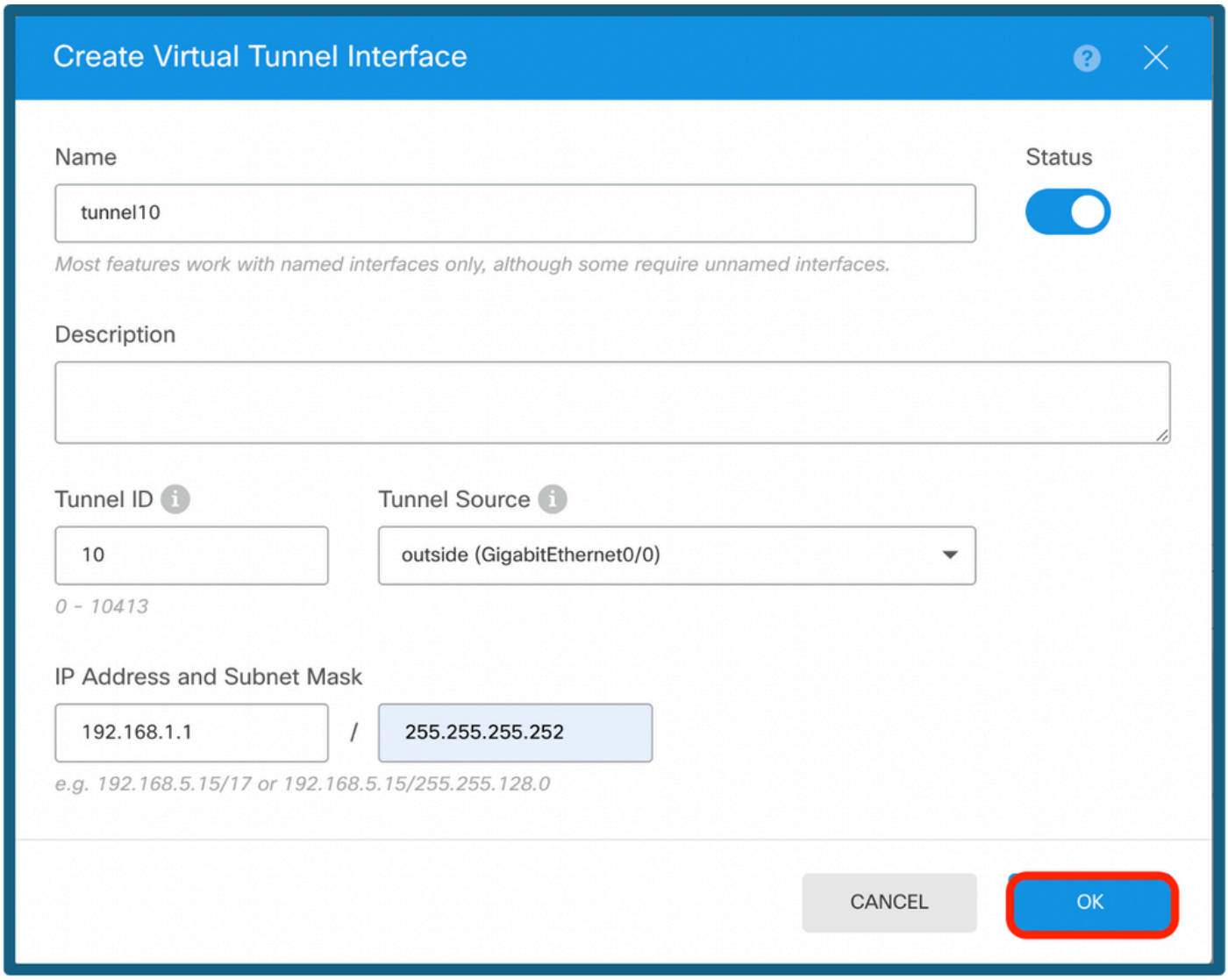
Paso 3. Proporcione un nombre de topología y seleccione el tipo de VPN como basado en ruta (VTI).

Haga clic en Local VPN Access Interface, y luego haga clic en Create new Virtual Tunnel Interface o seleccione una de la lista que existe.



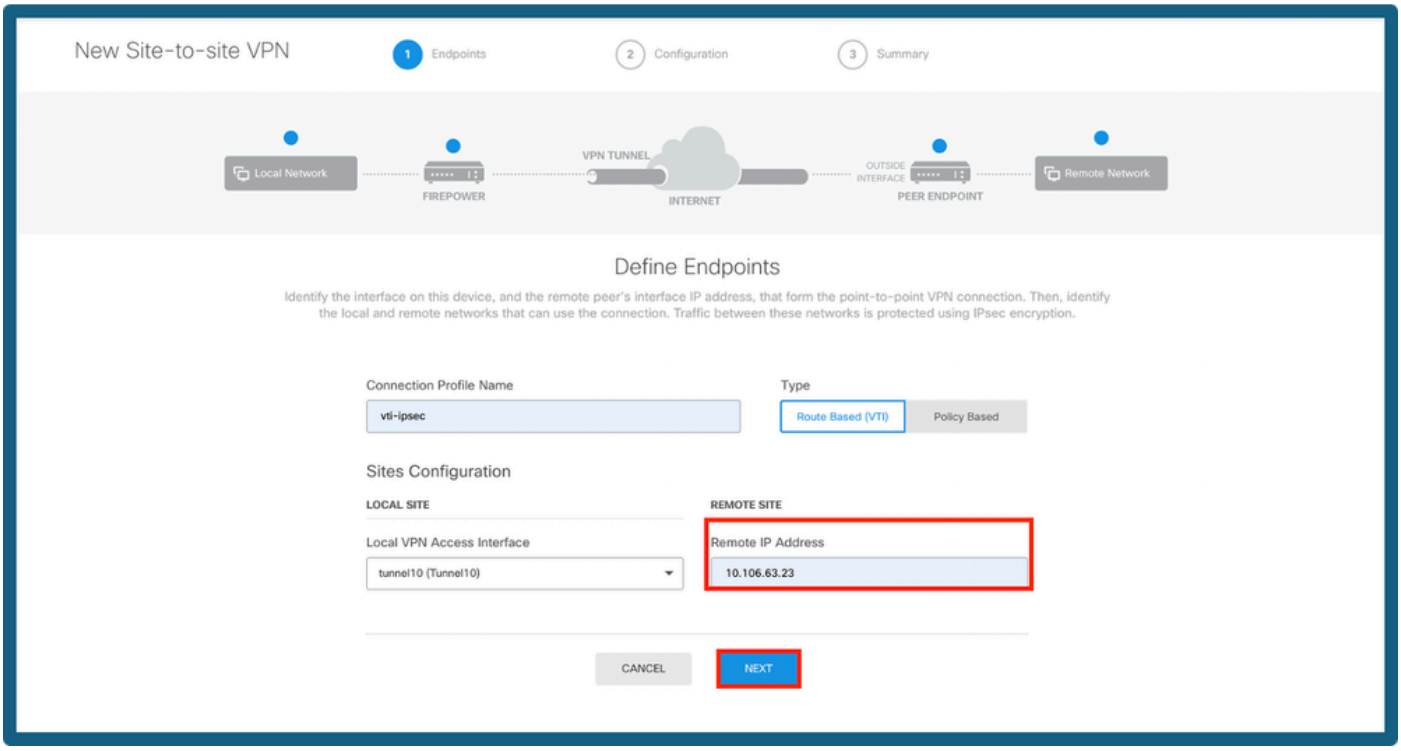
Agregar interfaz de túnel

Paso 4. Defina los parámetros de la nueva interfaz de túnel virtual. Click OK.



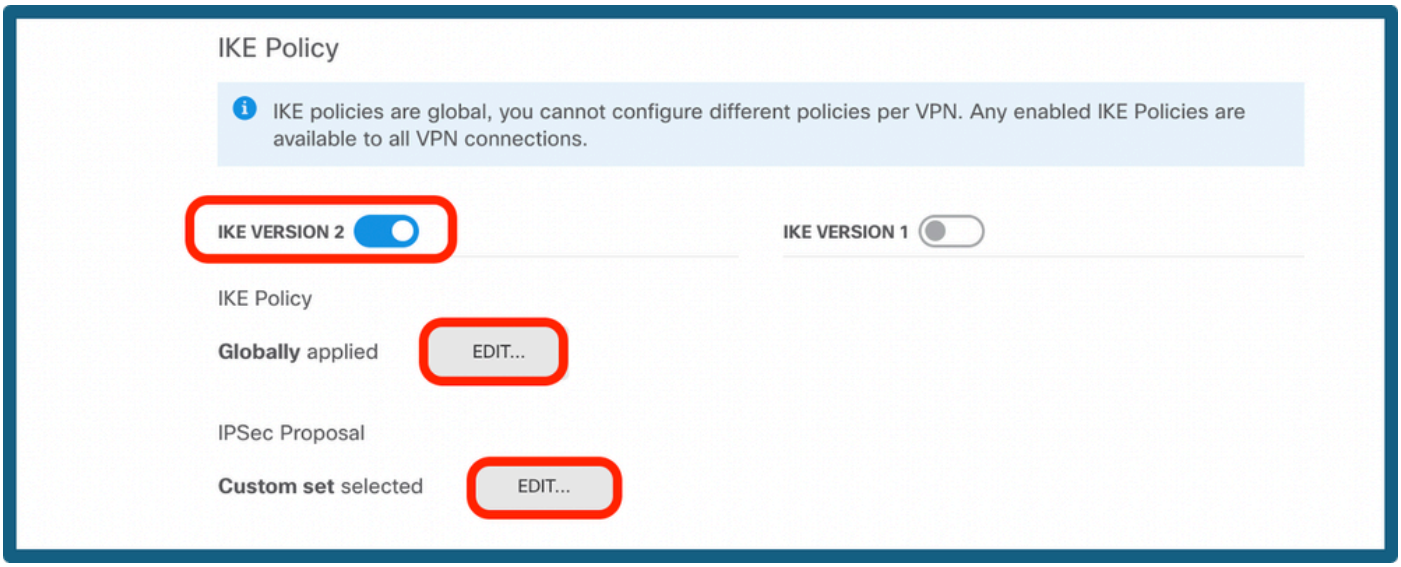
Configuración de VTI

Paso 5. Elija el VTI recién creado o un VTI que exista en la interfaz de túnel virtual. Proporcione la dirección IP remota.



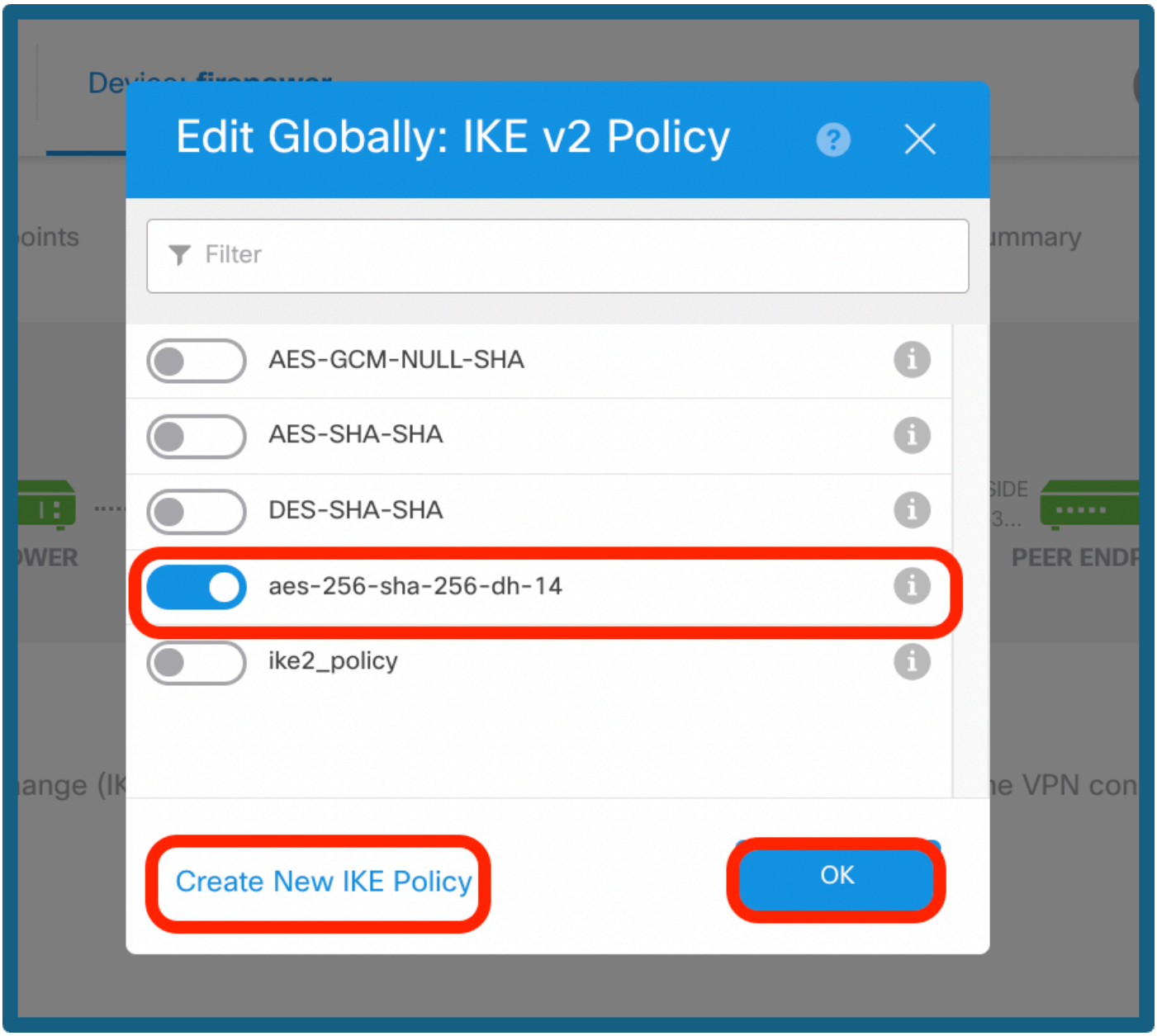
Agregar IP de par

Paso 6. Elija la Versión IKE y elija el botón Editar para establecer los parámetros IKE e IPsec como se muestra en la imagen.

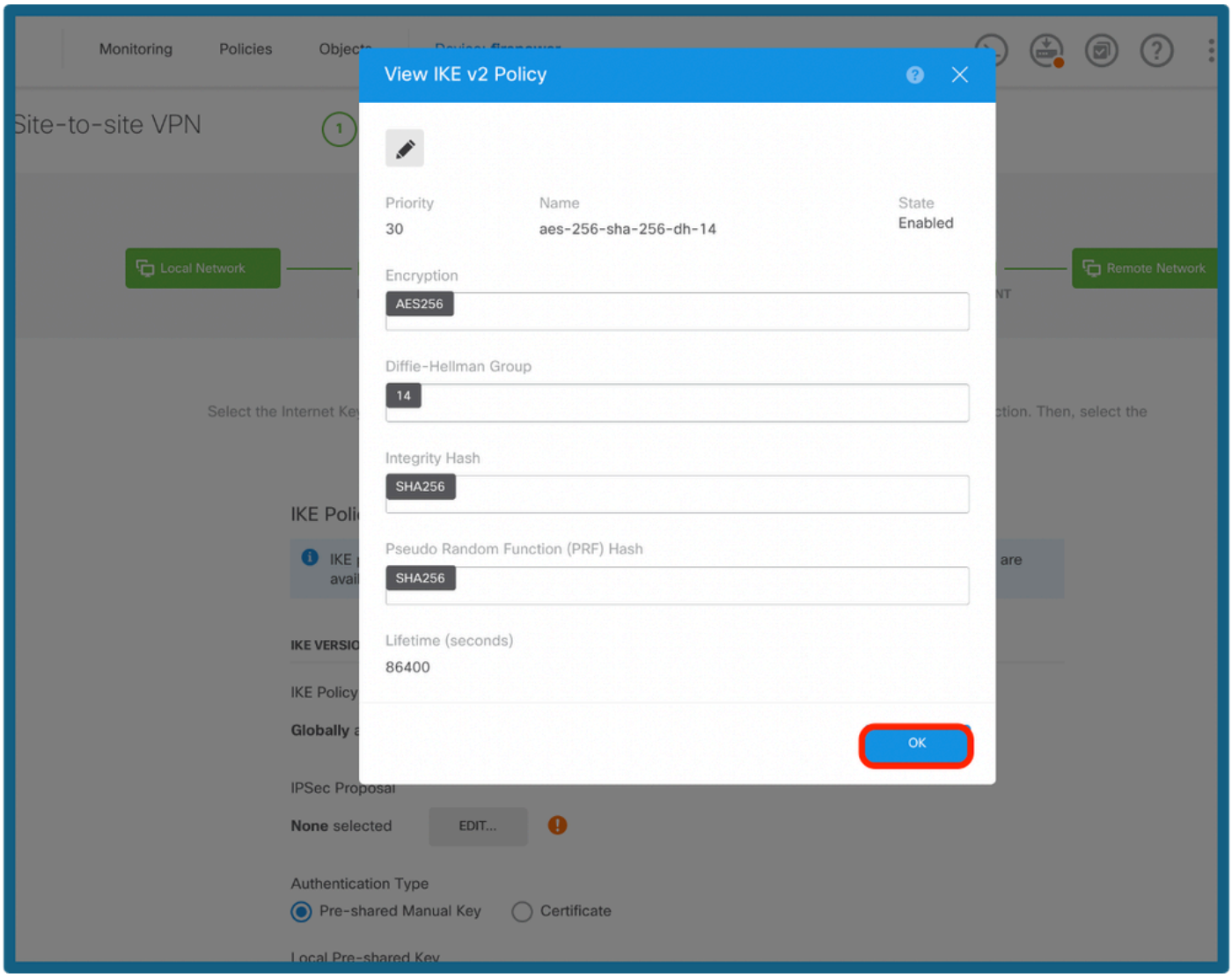


Configurar la versión IKE

Paso 7a. Elija el botón IKE Policy como se muestra en la imagen y haga clic en el botón ok o en Create New IKE Policy, si desea crear una nueva política.

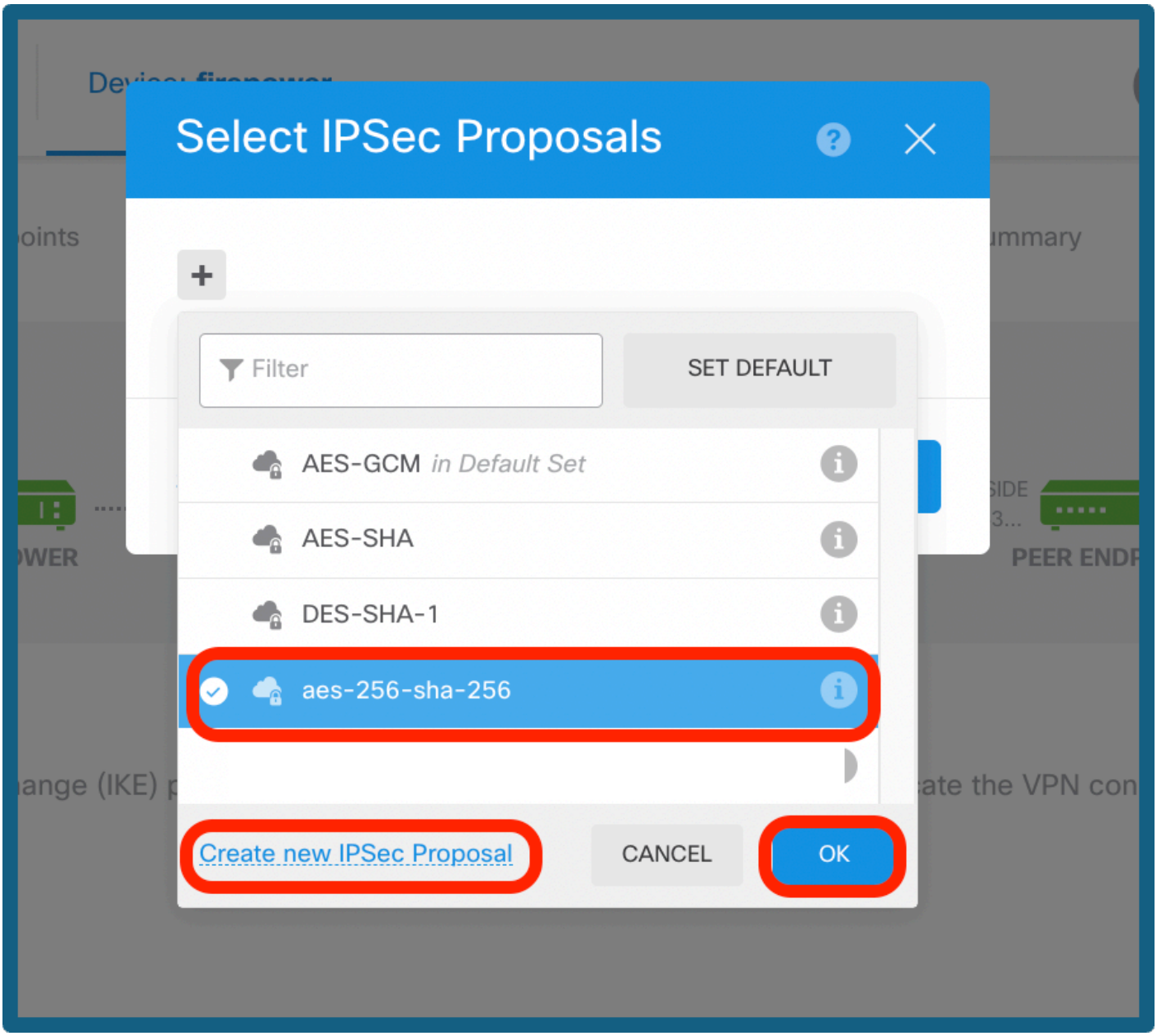


Elija la política IKE

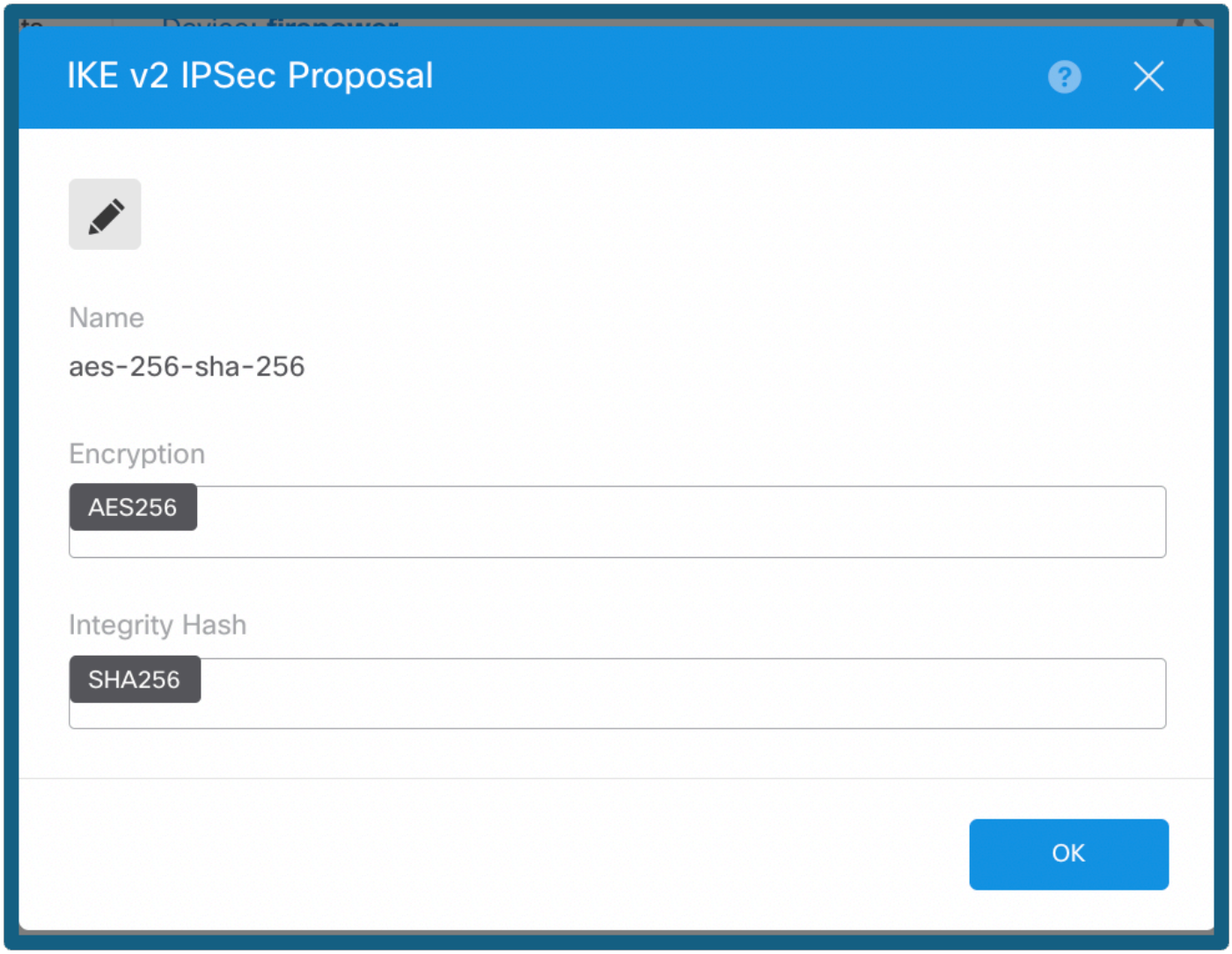


Configuración de la política IKE

Paso 7b. Elija el botón IPSec Policy como se muestra en la imagen y haga clic en el botón ok o en Create New IPsec Propuesta, si desea crear una nueva propuesta.



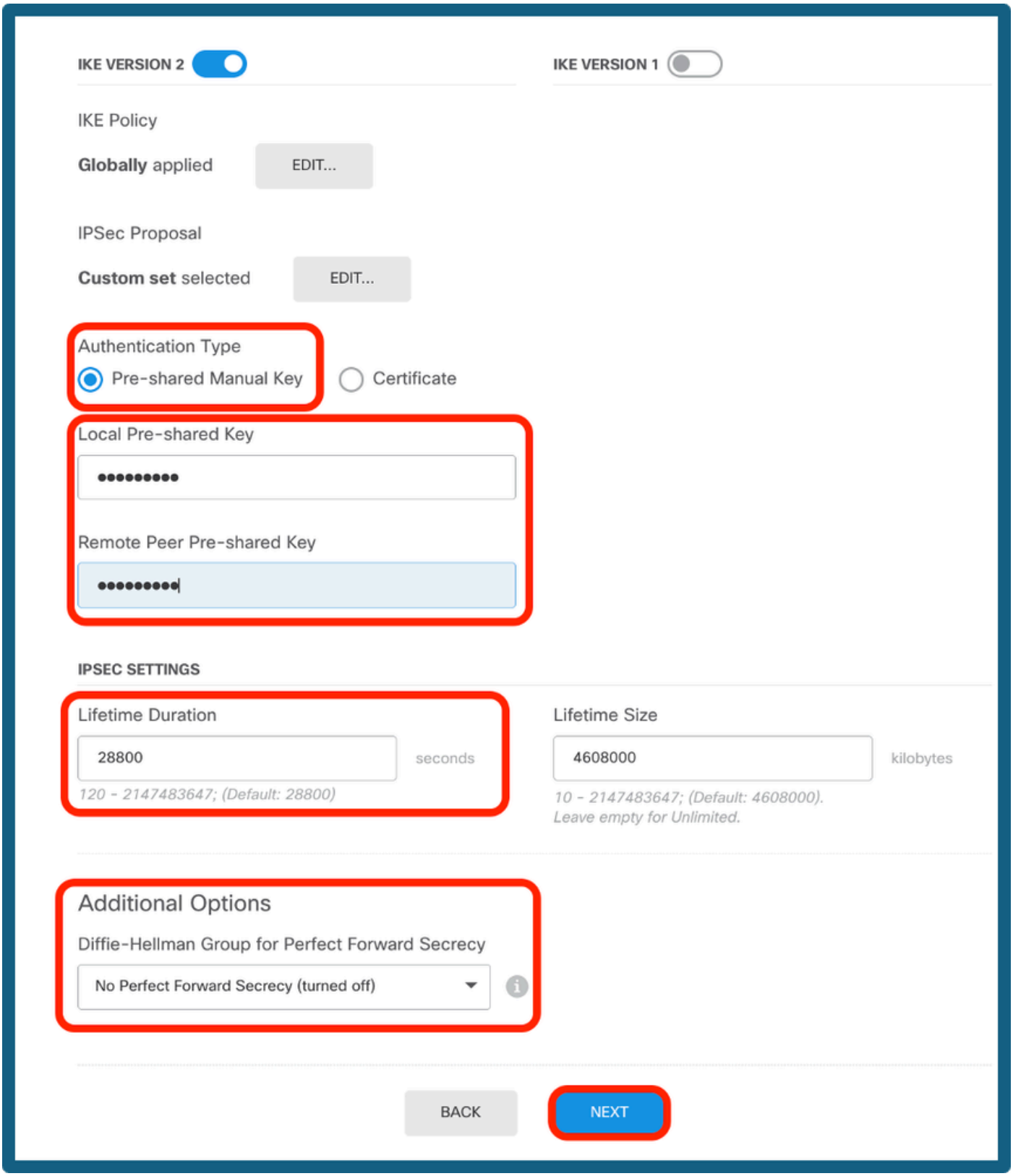
Seleccionar propuesta de IPsec



Configuración de la propuesta de IPsec

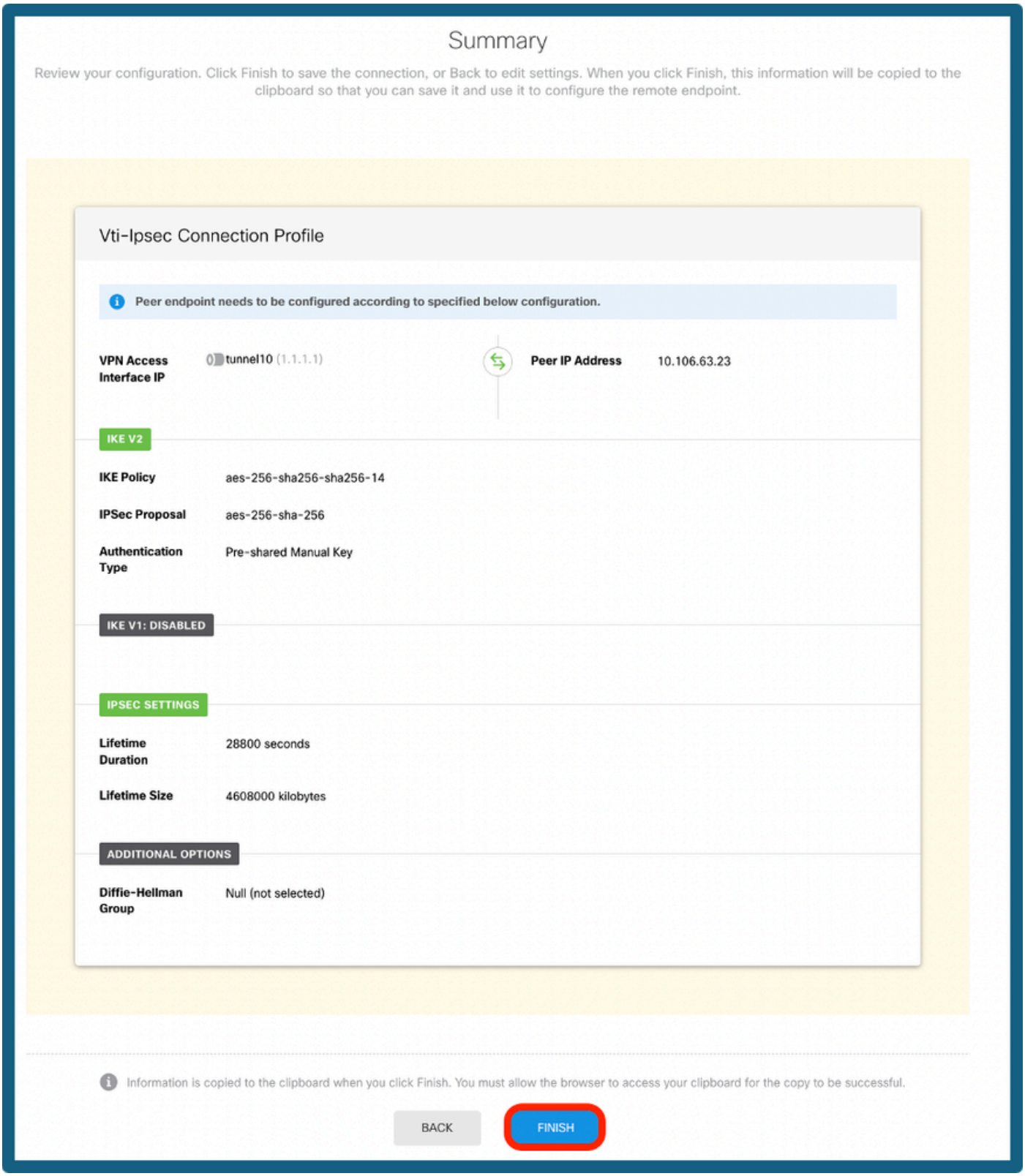
Paso 8a. Seleccione el Tipo de autenticación. Si se utiliza una clave manual previamente compartida, proporcione la clave previamente compartida local y remota.

Paso 8b. (Opcional) Elija la configuración Perfect Forward Secrecy. Configure IPSec Lifetime Duration and Lifetime Size y, a continuación, haga clic en Next (Siguiente).



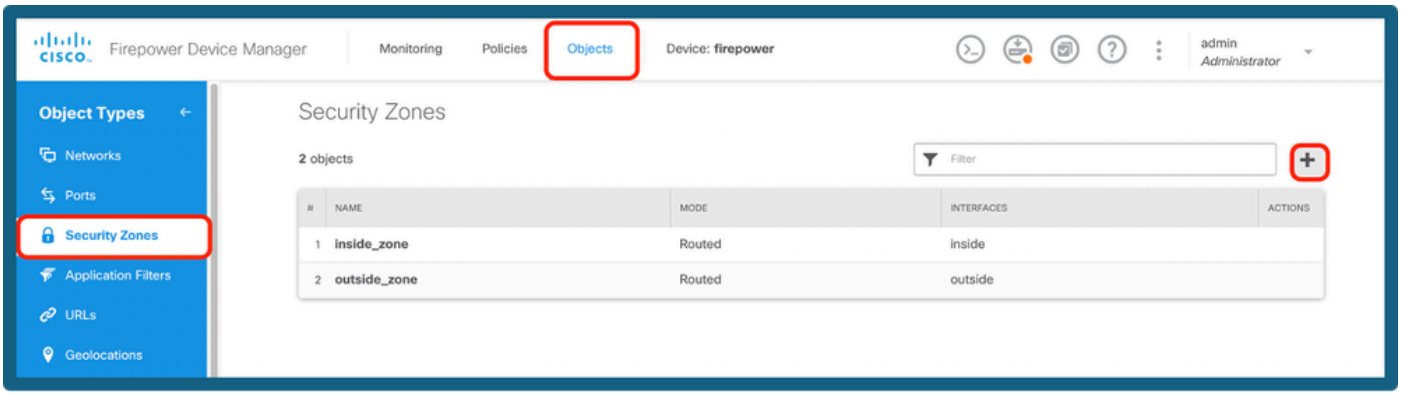
PSK y configuración de por vida

Paso 9. Revise la configuración y haga clic en Finish.



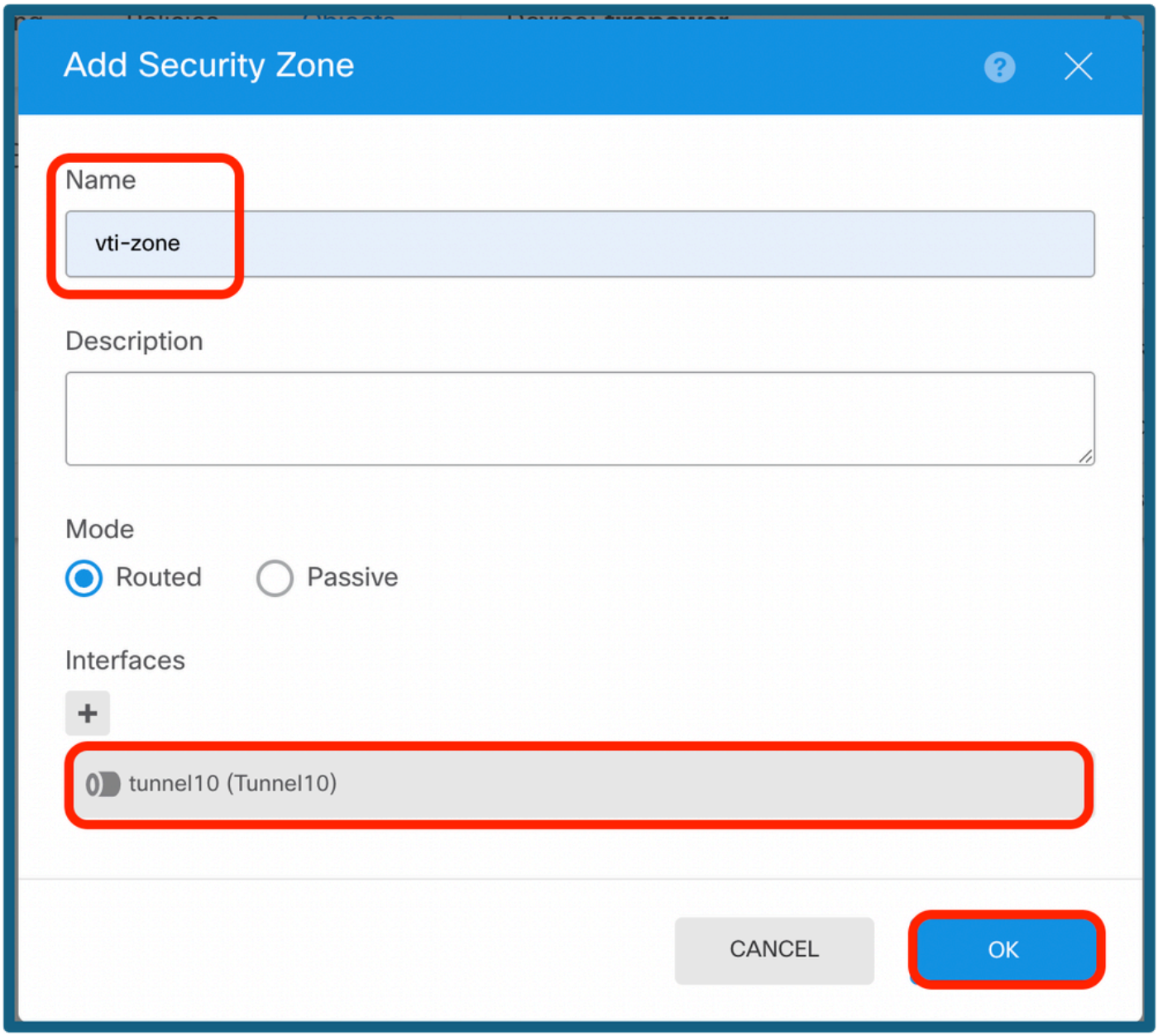
Resumen de la configuración

Paso 10a. Navegue hasta Objetos > Zonas de seguridad y luego haga clic en el icono +.



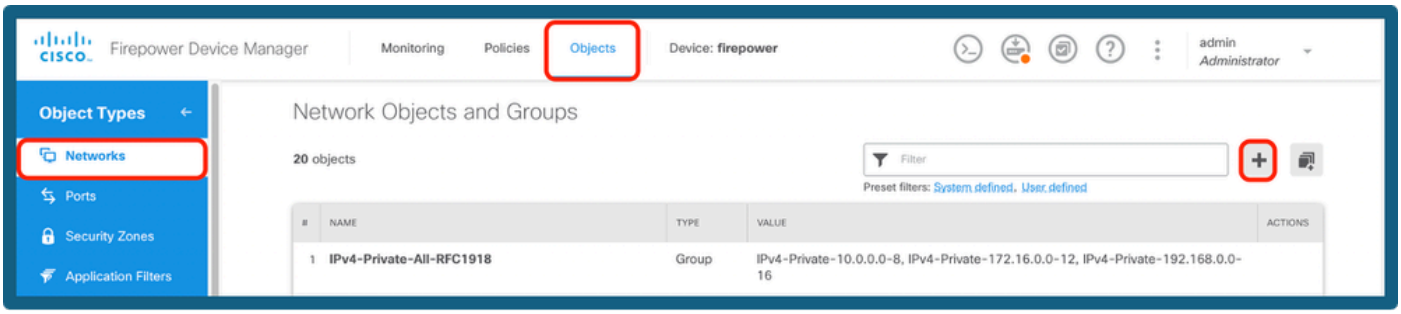
Agregar una zona de seguridad

Paso 10b. Cree una zona y seleccione la interfaz VTI como se muestra a continuación.



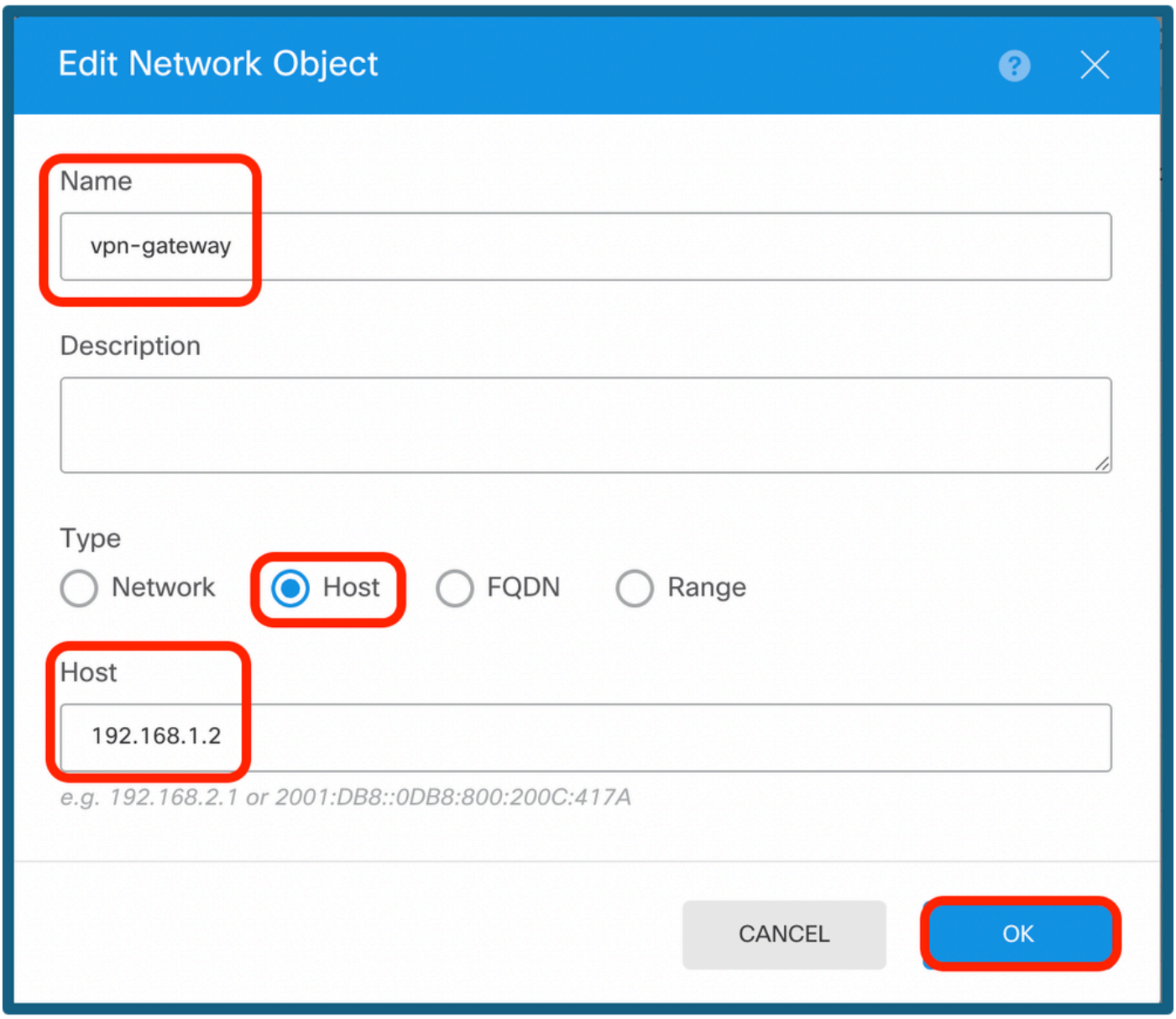
Configuración de la zona de seguridad

Paso 11a. Navegue hasta Objetos > Redes, haga clic en el icono +.



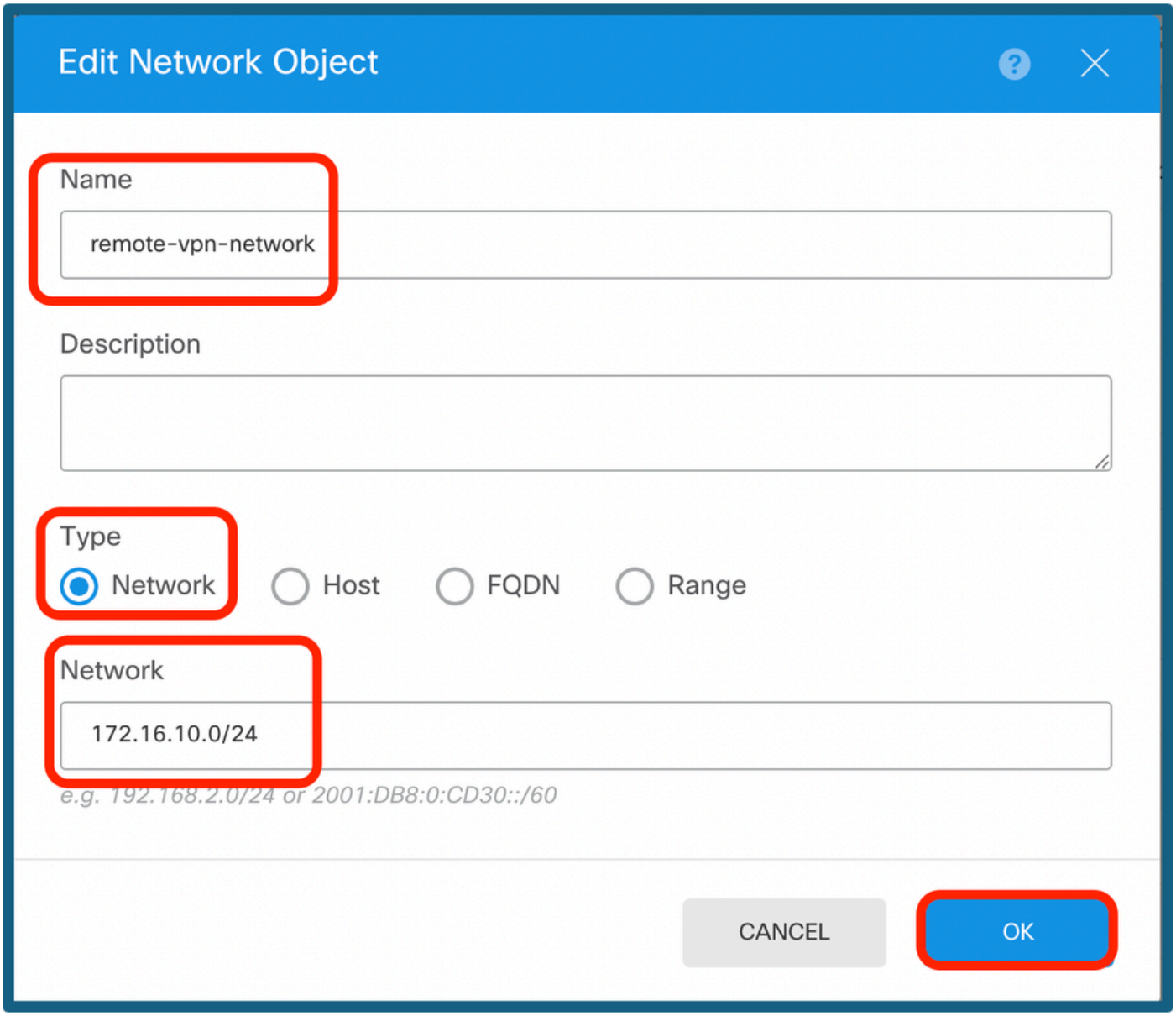
Agregar objetos de red

Paso 11b. Agregue un objeto host y cree una gateway con IP de túnel del extremo del par.

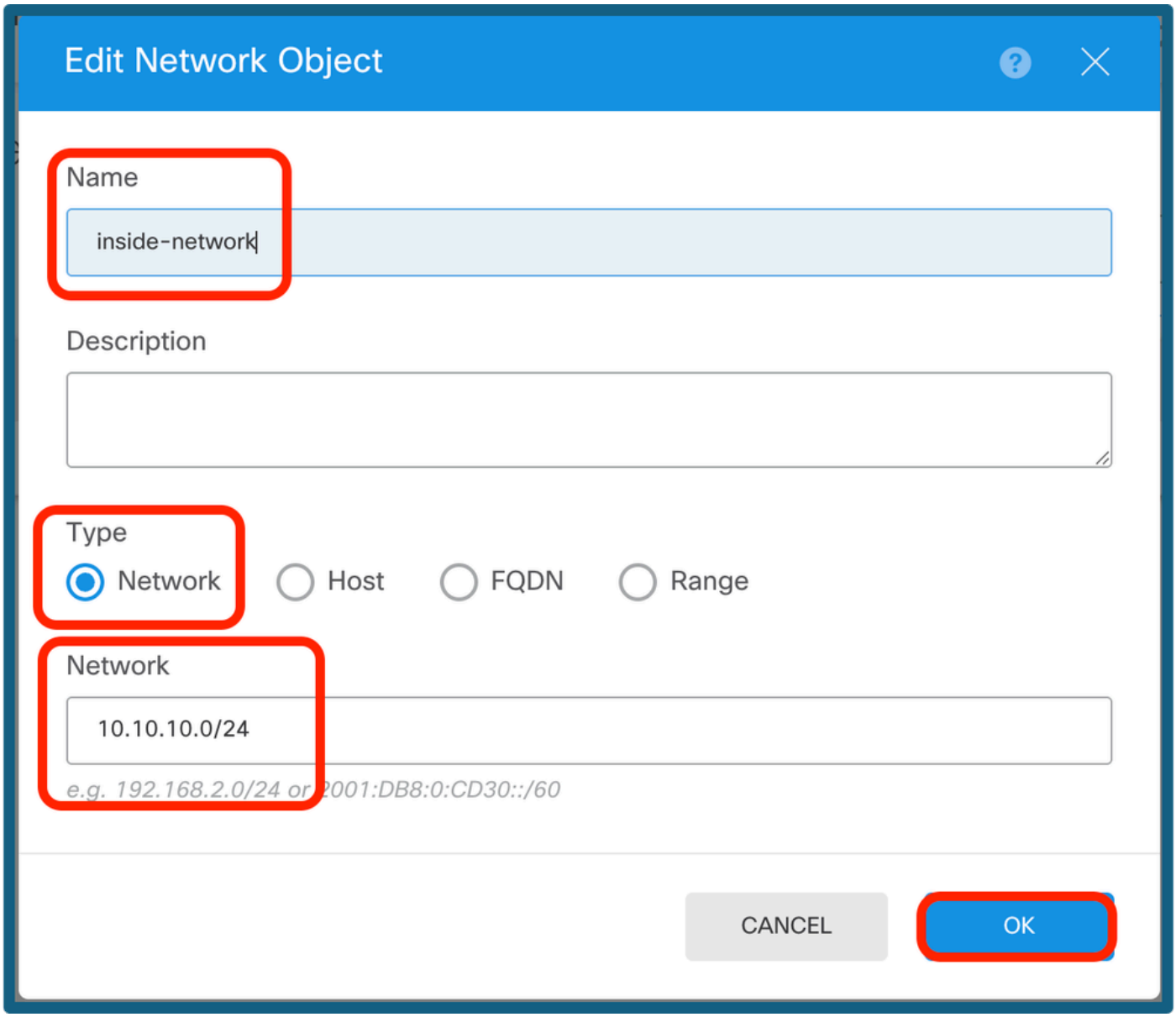


Configurar puerta de enlace VPN

Paso 11c. Agregue la subred remota y la subred local.

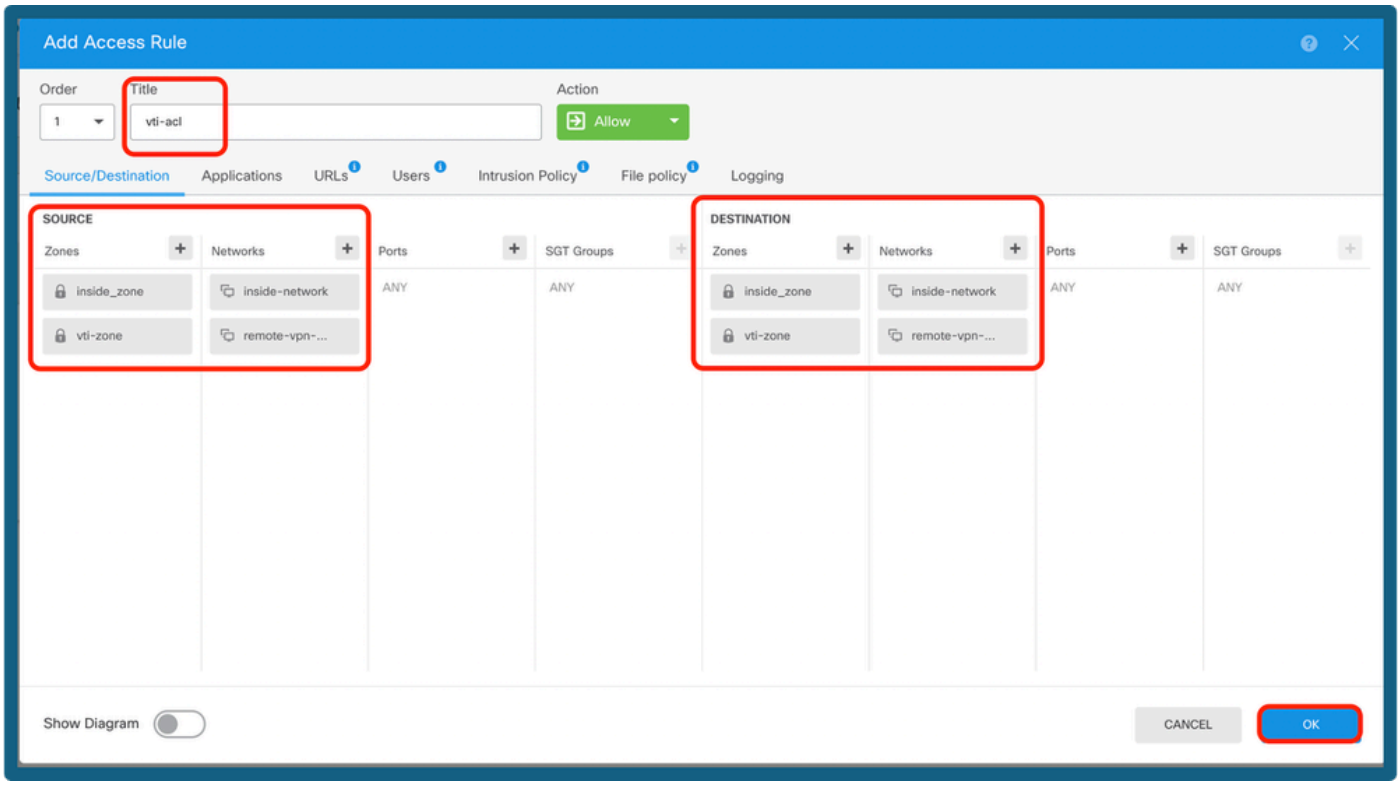


Configuración de IP remota



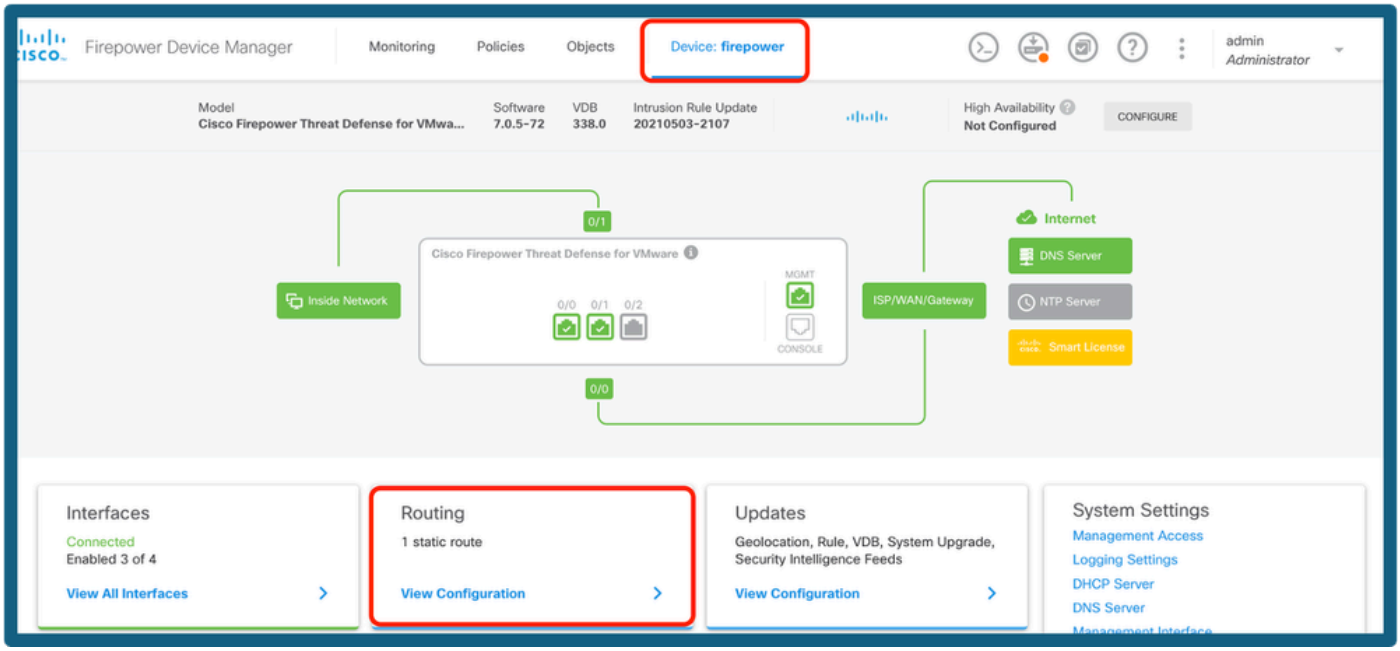
Configuración de IP local

Paso 12. Navegue hasta Dispositivo > Políticas, y configure la Política de Control de Acceso.



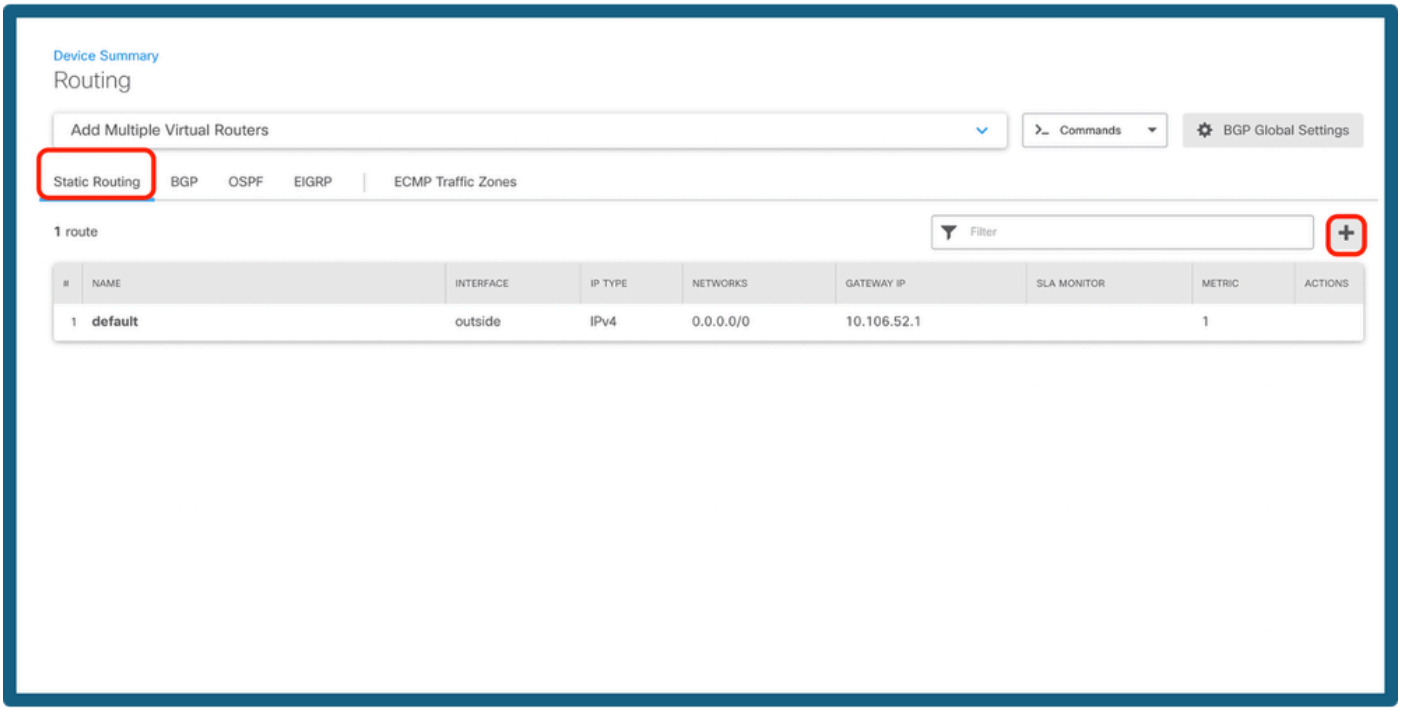
Agregar política de control de acceso

Paso 13a. Agregue el ruteo sobre el túnel VTI. Vaya a Device > Routing.



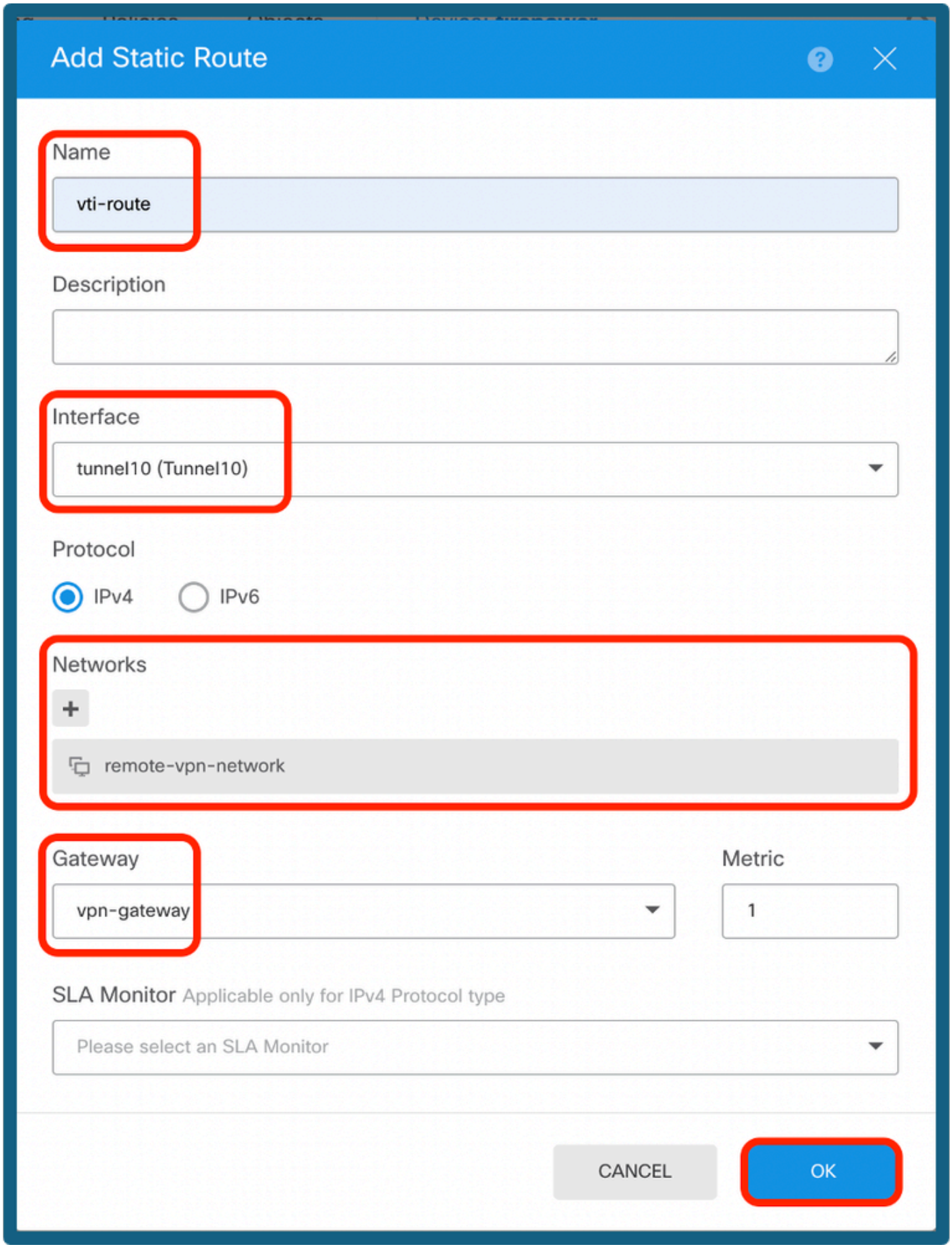
Seleccionar enrutamiento

Paso 13b. Vaya a Static Route en la pestaña Routing. Haga clic en el icono +.



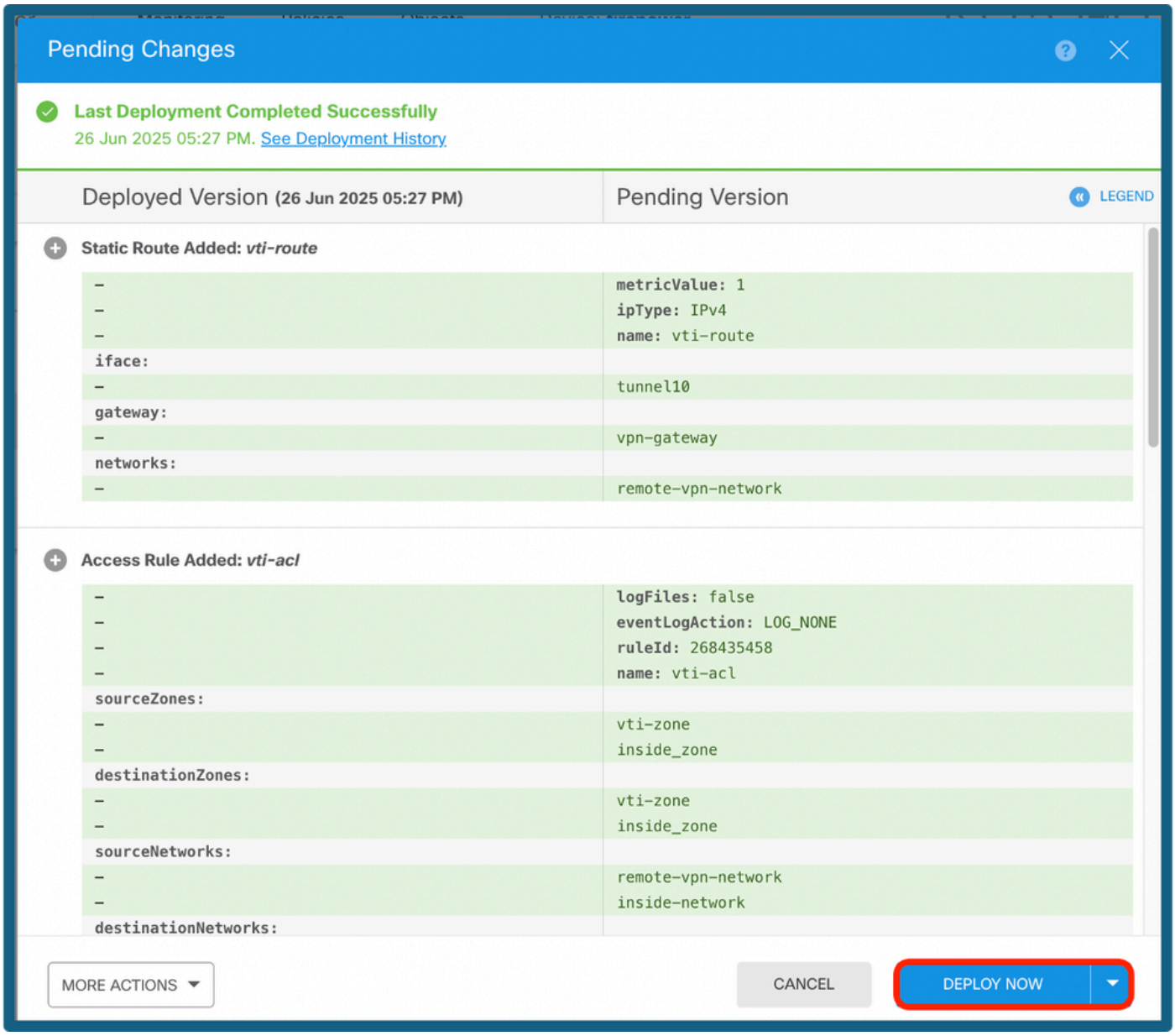
Agregar ruta

Paso 13c. Proporcione la interfaz, elija la red, proporcione la puerta de enlace. Click OK.



Configurar ruta estática

Paso 14. Vaya a Desplegar. Revise los cambios y, a continuación, haga clic en Deploy Now.

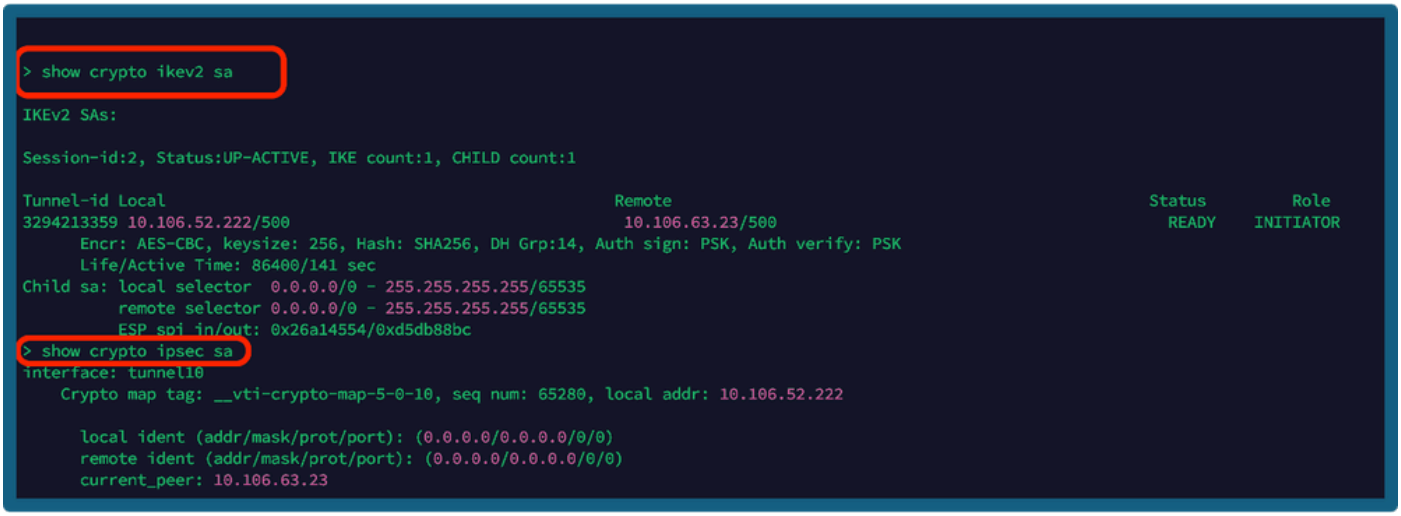


Implementación de la configuración

Verificación

Una vez completada la implementación, puede verificar el estado del túnel en la CLI mediante los siguientes comandos:

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>



Comandos show

Información Relacionada

Para obtener más información sobre las VPN de sitio a sitio en el FTD gestionado por FDM, puede encontrar la guía de configuración completa aquí:

Guía de configuración de FDM Administrado por FDM

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).