Configurar VPN Baseada em Rota com Rota Estática no FTD Gerenciado pelo FDM

Contents

Introdução

Este documento descreve como configurar um túnel VPN site a site baseado em rota estática em um FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica de como um túnel VPN funciona.
- Conhecimento prévio de navegação pelo Firepower Device Manager (FDM).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

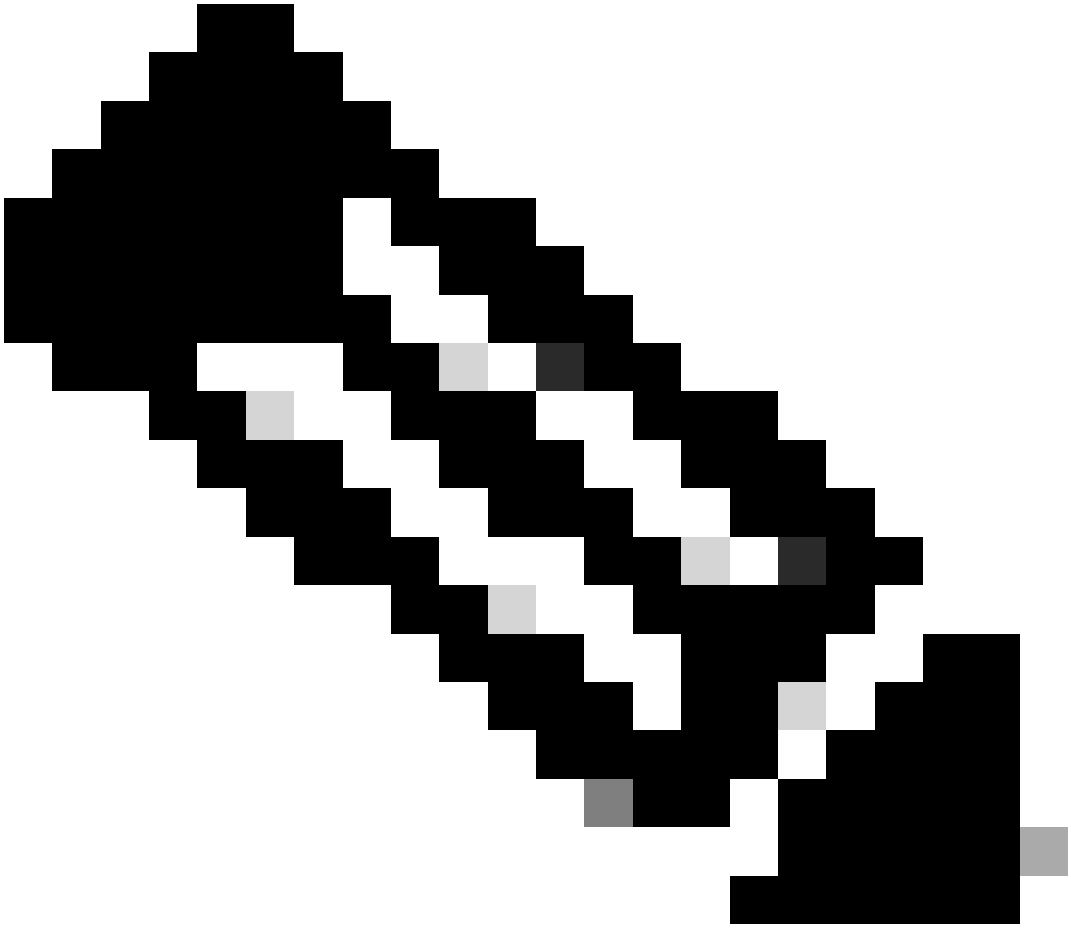
- Cisco Firepower Threat Defense (FTD) versão 7.0 gerenciado pelo Firepower Device Manager (FDM).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A VPN baseada em rota permite que a determinação do tráfego interessante seja criptografada ou enviada pelo túnel VPN, e usa o roteamento de tráfego em vez da política/lista de acesso como na VPN baseada em política ou em mapa de criptografia. O domínio de criptografia é definido para permitir qualquer tráfego que entre no túnel IPsec. Os seletores de tráfego local e remoto de IPsec são definidos como 0.0.0.0/0.0.0.0. Isso significa que qualquer tráfego roteado para o túnel IPsec é criptografado, independentemente da sub-rede de origem/destino.

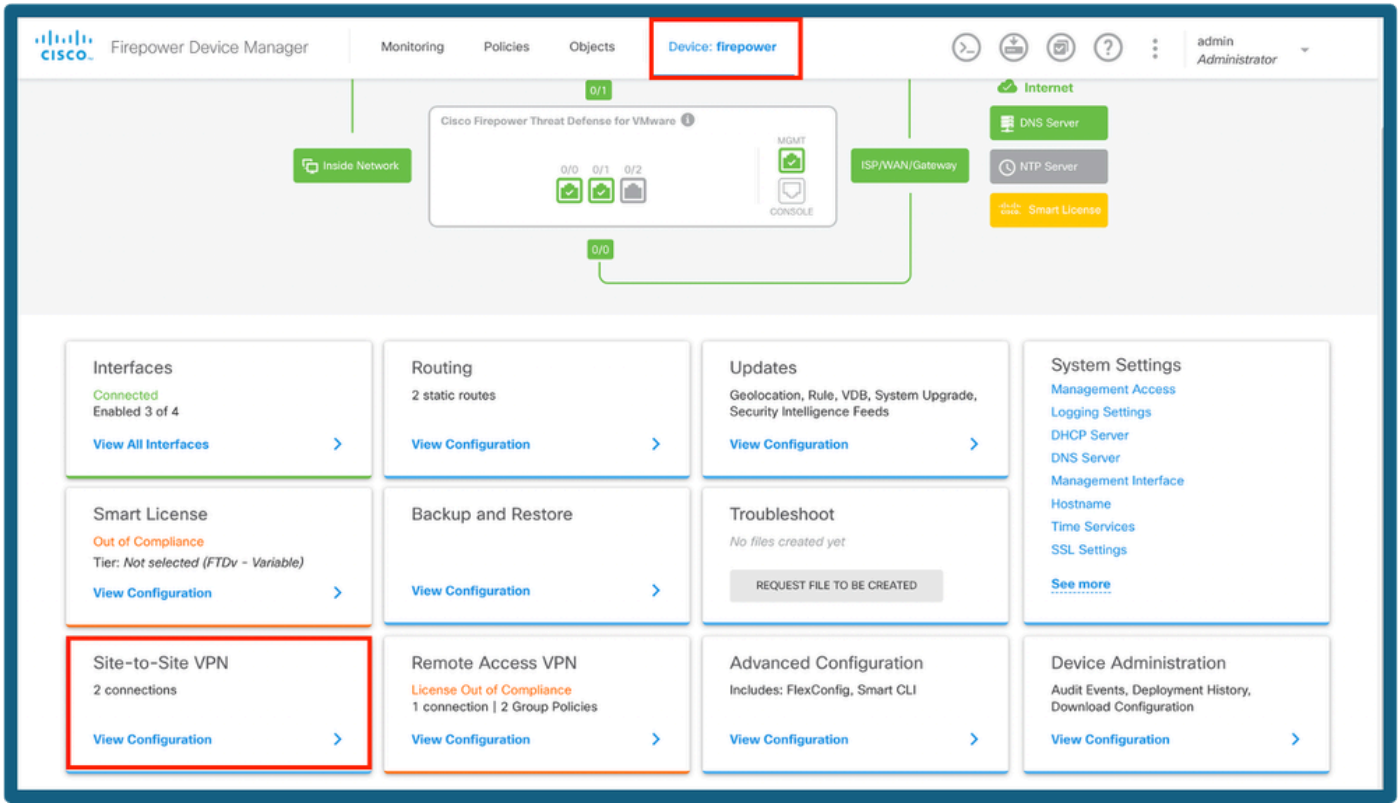
Este documento se concentra na configuração da Interface de túnel virtual estático (SVTI).



Note: Não é necessário nenhum licenciamento adicional, a VPN Baseada em Rota pode ser configurada nos Modos Licenciado e de Avaliação. Sem a conformidade com criptografia (Recursos Controlados por Exportação Habilitados), somente DES pode ser usado como um algoritmo de criptografia.

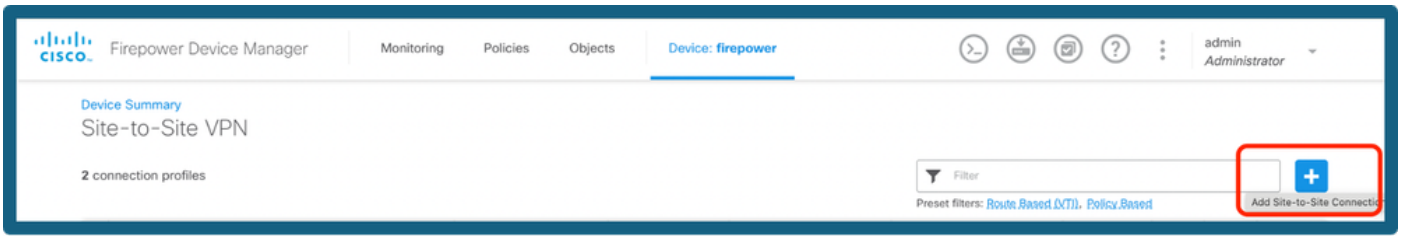
Etapas de Configuração no FDM

Etapa 1. Navegue até Device > Site To Site.



Painel do FDM

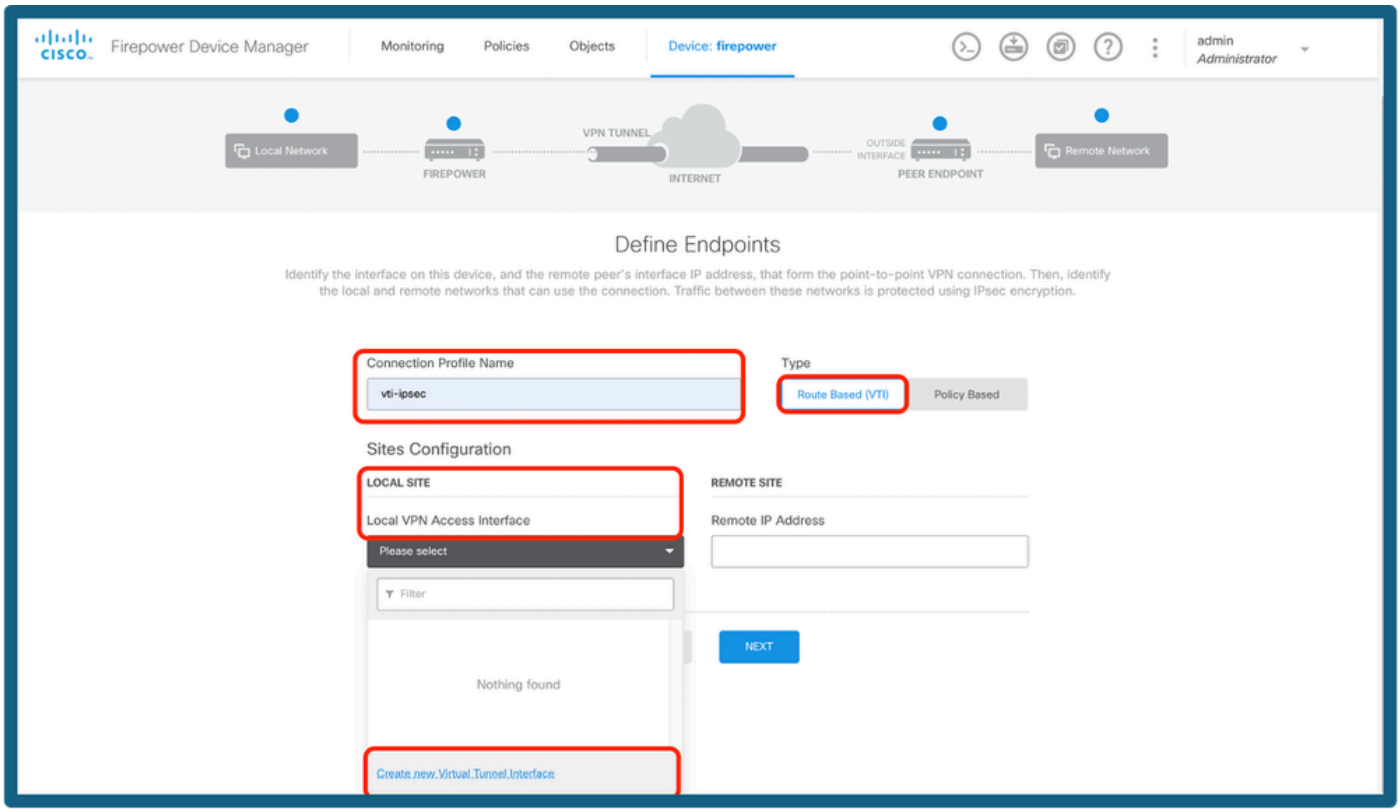
Etapa 2. Clique no ícone + para adicionar um novo site à conexão de site.



Adicionar conexão S2S

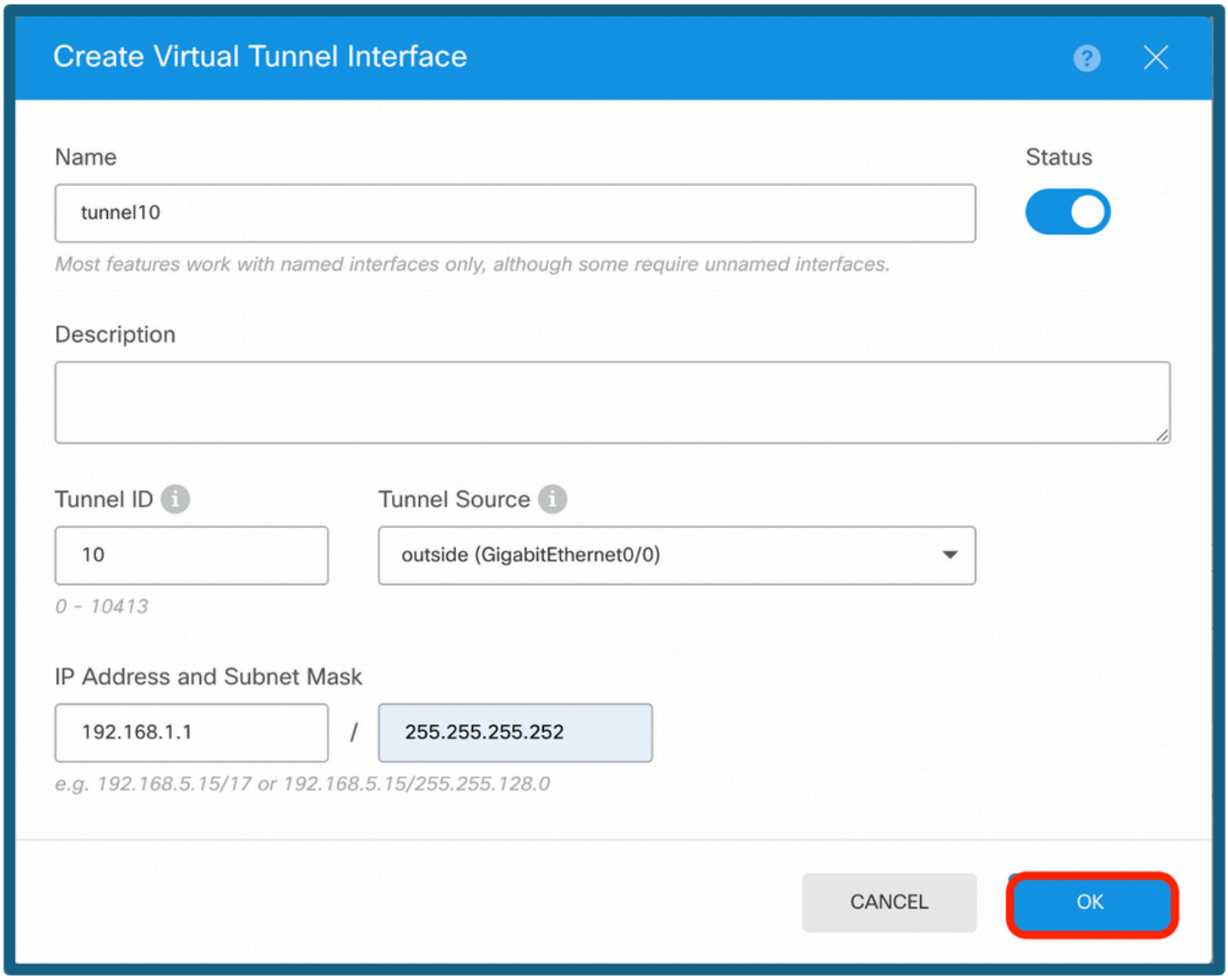
Etapa 3. Forneça um nome de topologia e selecione o tipo de VPN como baseado em rota (VTI).

Clique em Local VPN Access Interface e, em seguida, clique em Create new Virtual Tunnel Interface ou selecione um na lista existente.



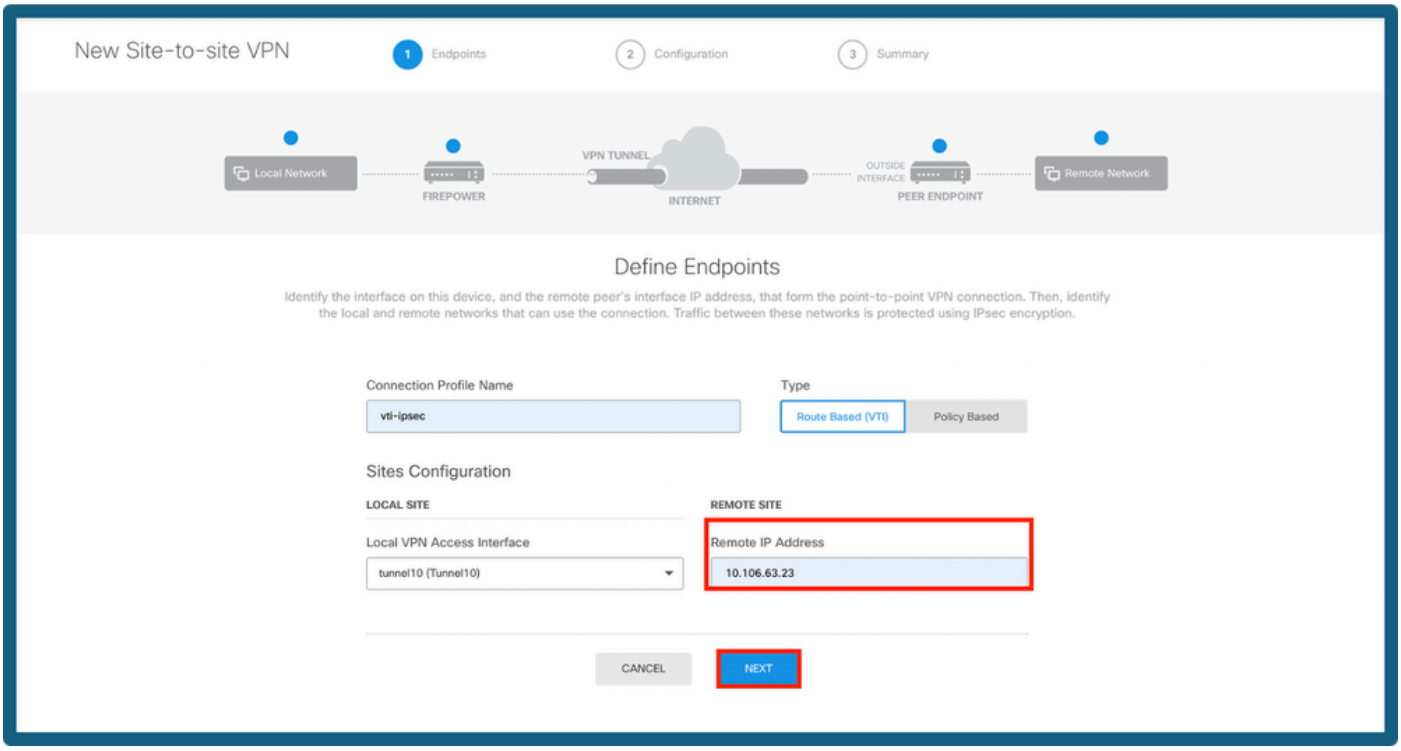
Adicionar interface de túnel

Etapa 4. Definir os parâmetros da Nova Interface de Túnel Virtual. Click OK.



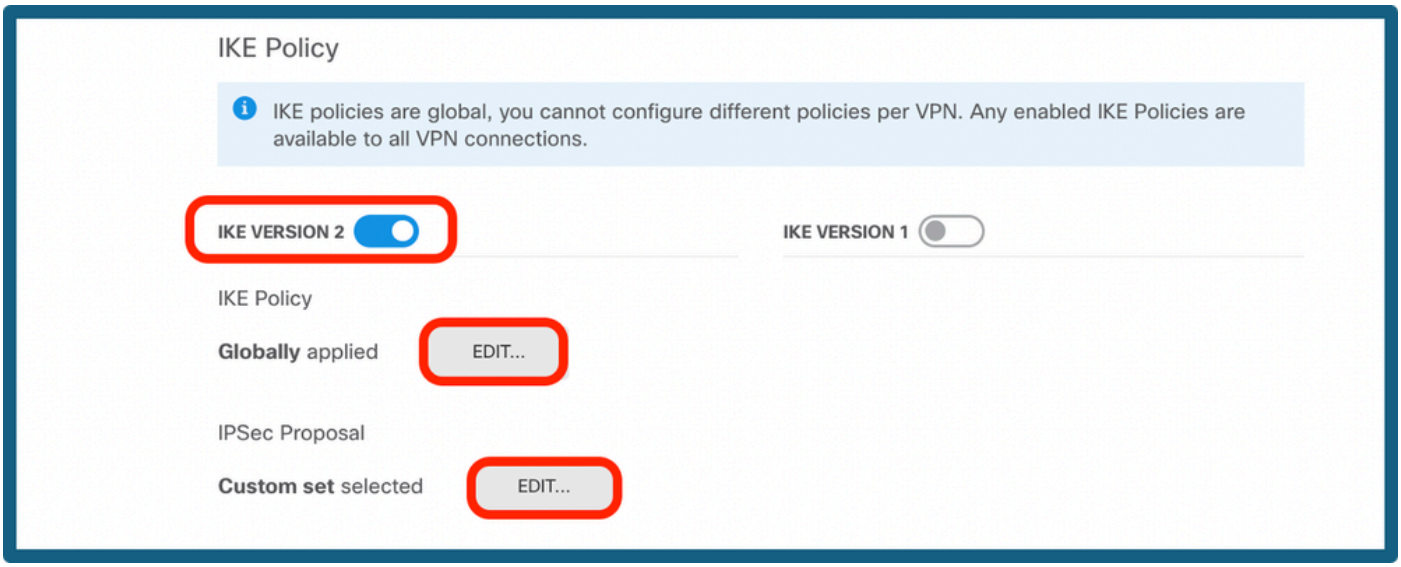
Configuração de VTI

Etapa 5. Escolha o VTI recém-criado ou um VTI que exista na Virtual Tunnel Interface.Forneça o endereço IP remoto.



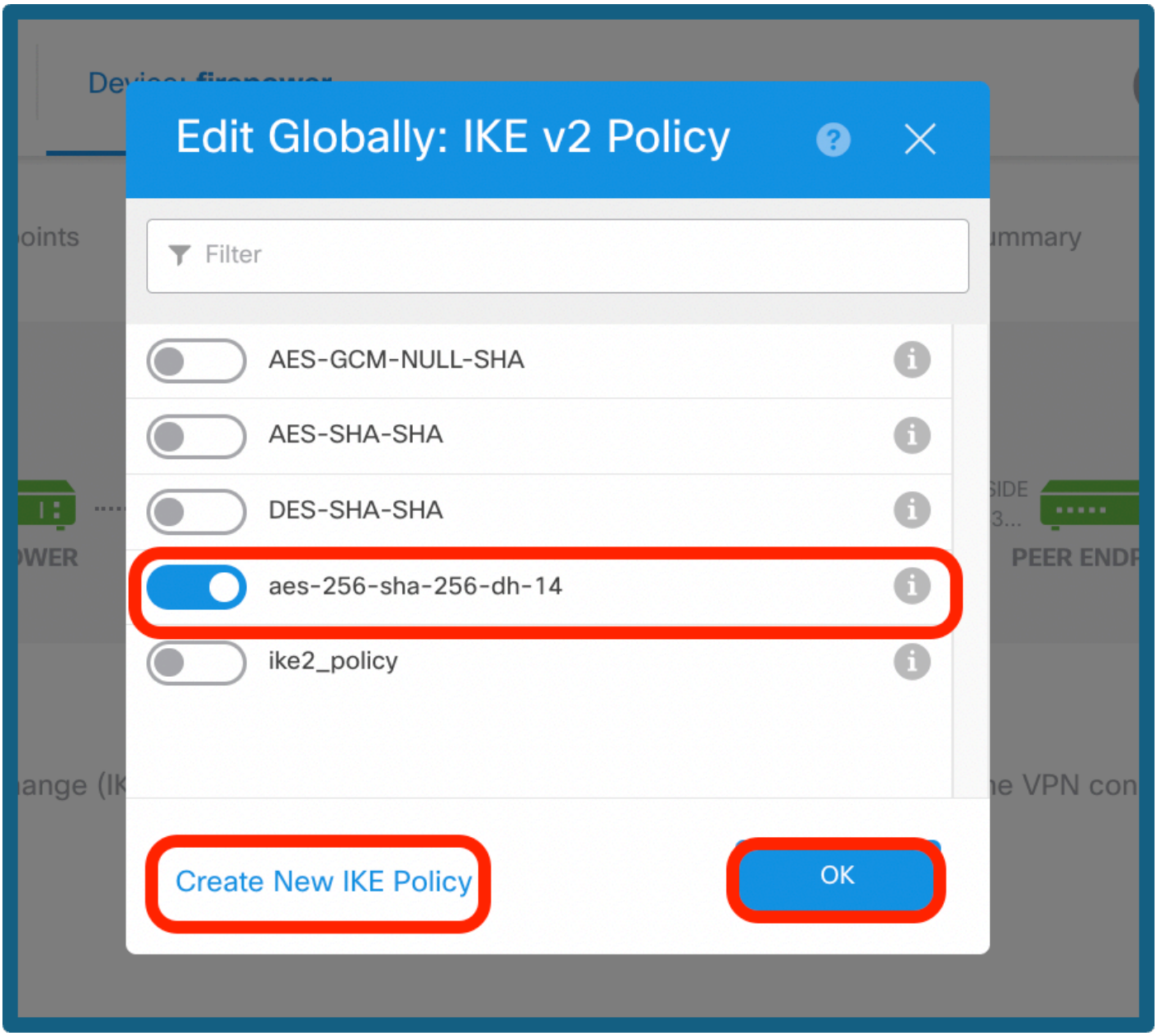
Adicionar IP do Par

Etapa 6. Escolha a versão IKE e escolha o botão Edit para definir os parâmetros IKE e IPsec como mostrado na imagem.

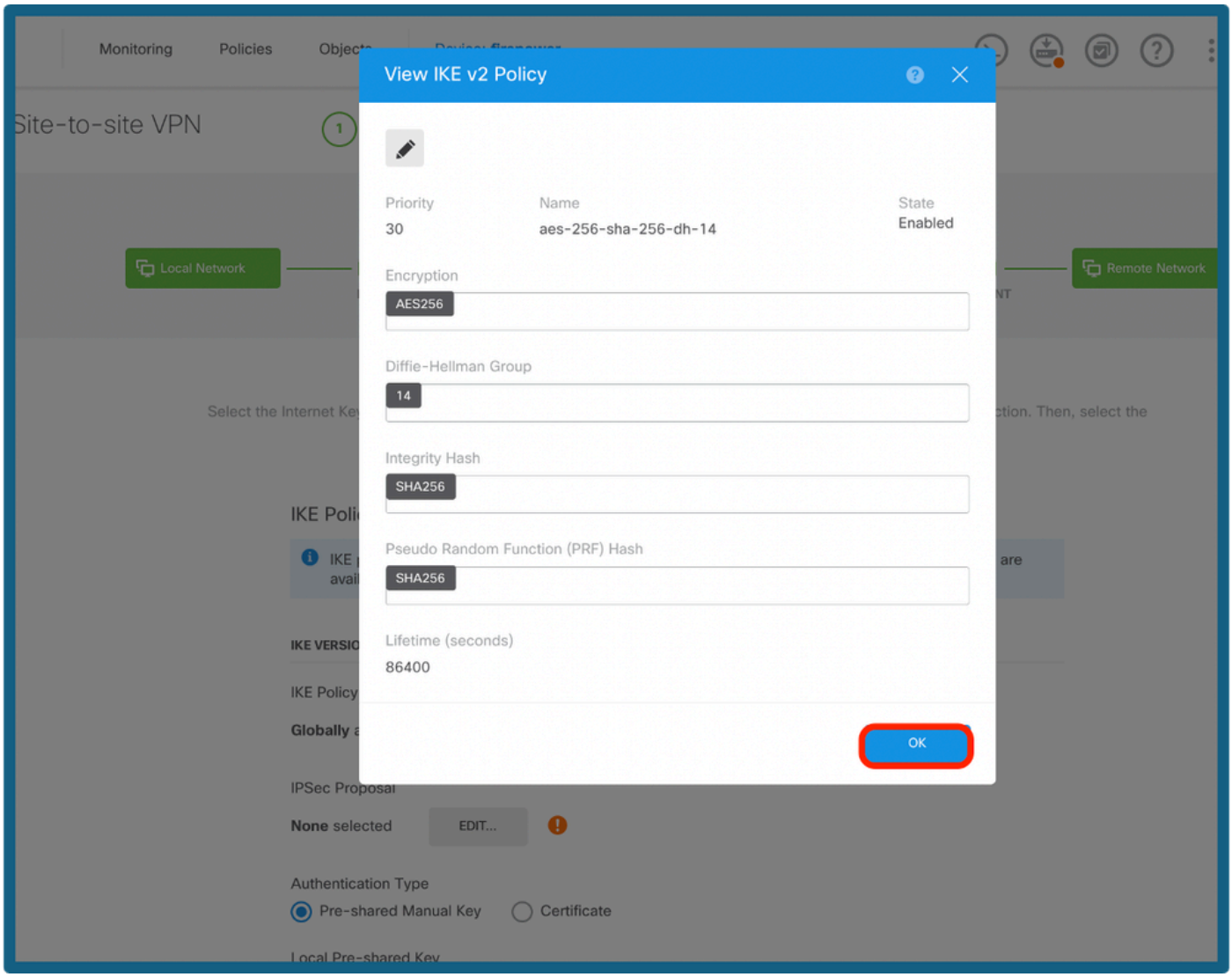


Configurar a versão do IKE

Etapa 7a. Escolha o botão IKE Policy como mostrado na imagem e clique no botão ok ou Create New IKE Policy, se você quiser criar uma nova política.

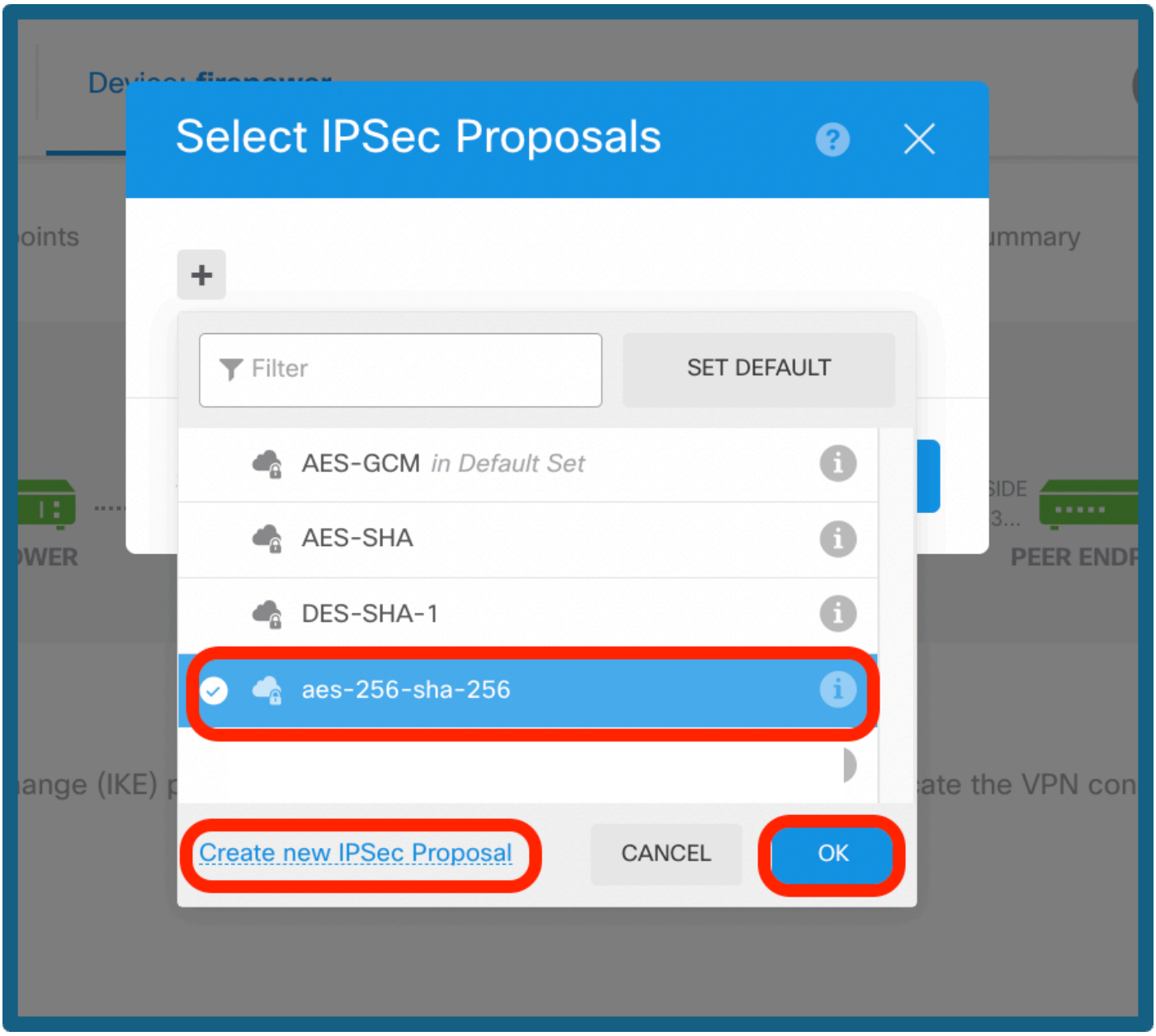


Escolher Política IKE

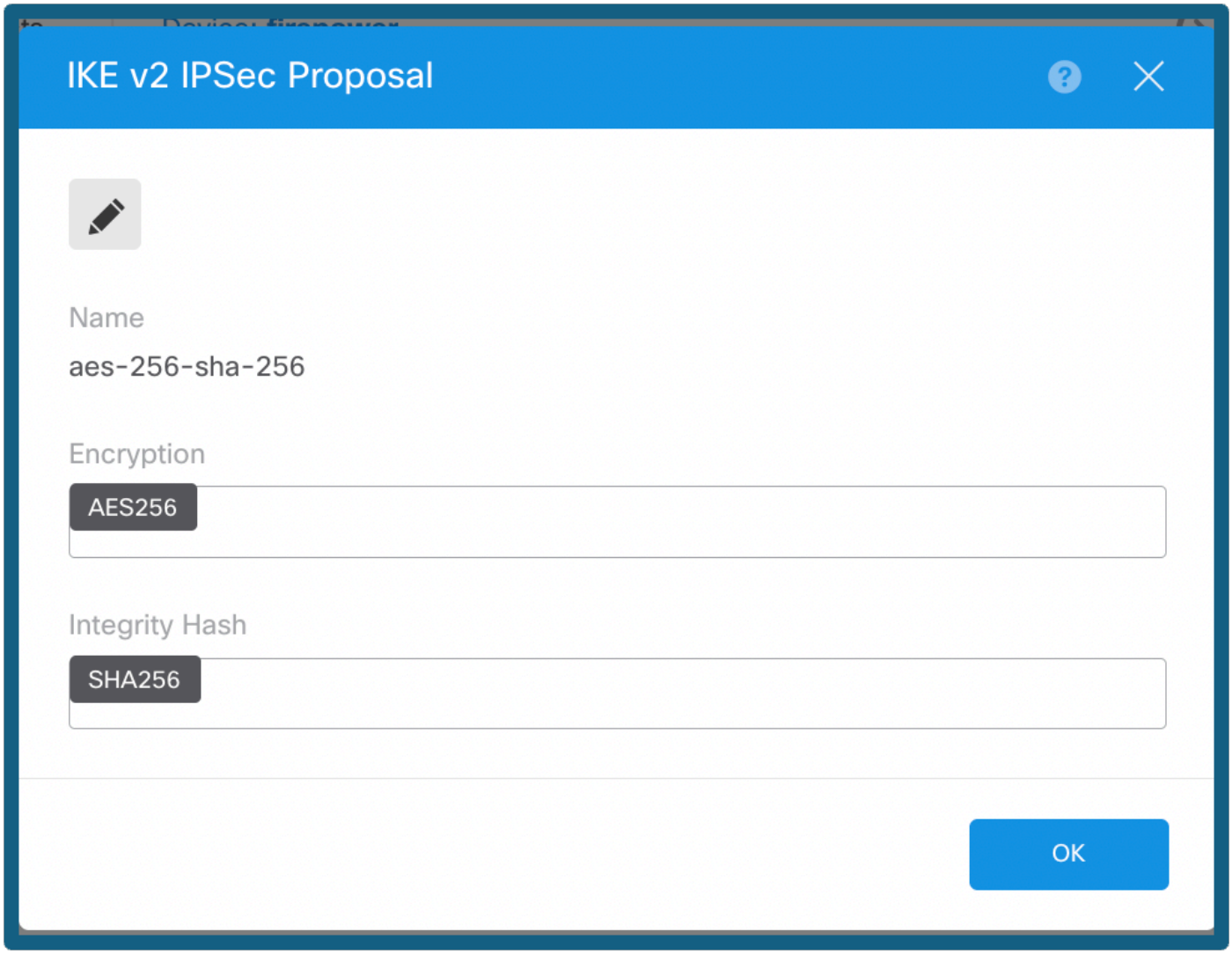


Configuração da política IKE

Etapa 7b. Escolha o botão IPSec Policy como mostrado na imagem e clique no botão ok ou Create New IPsec Proposal, se você quiser criar uma nova proposta.



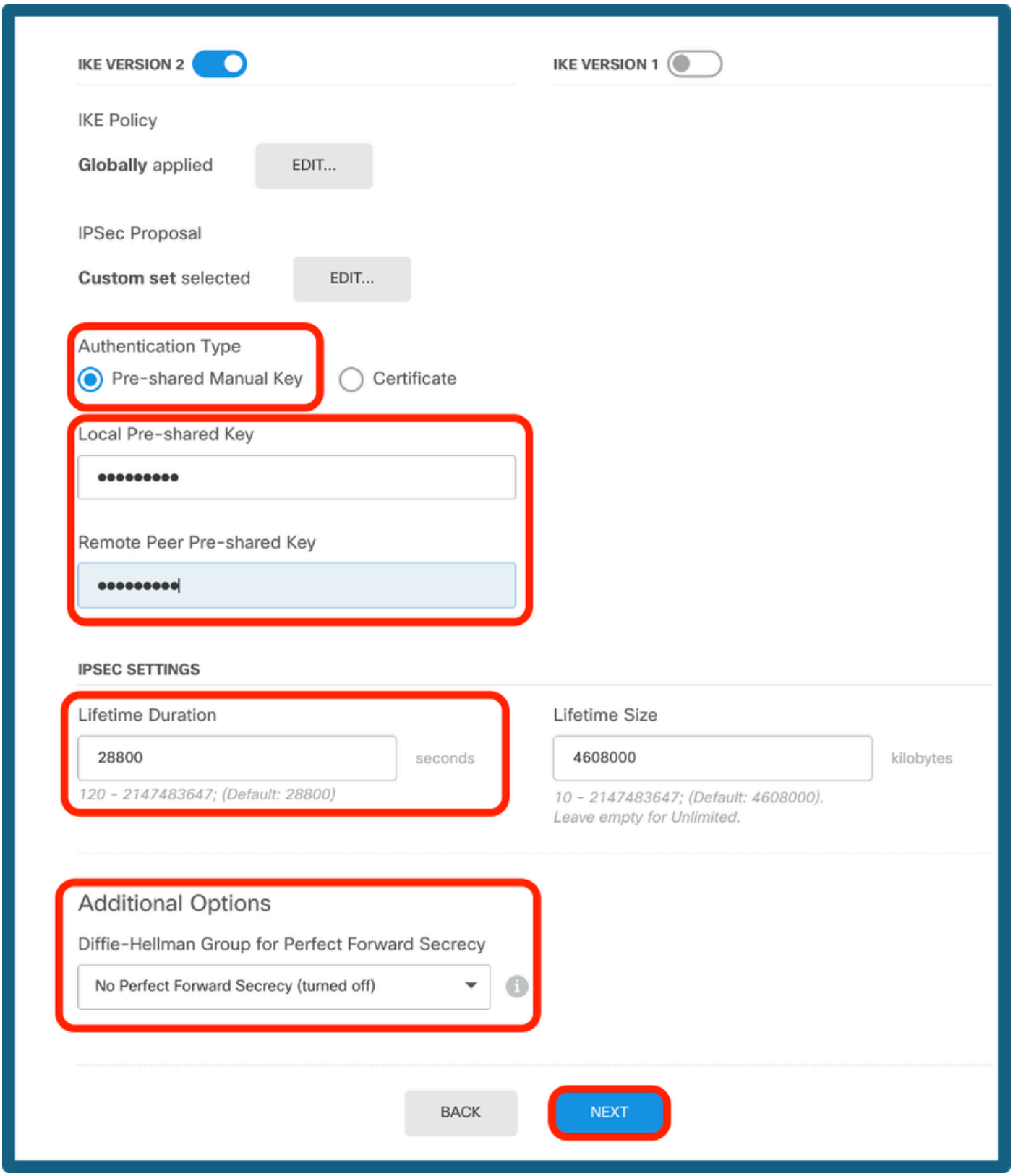
Selecionar Proposta IPsec



Configuração da proposta de IPsec

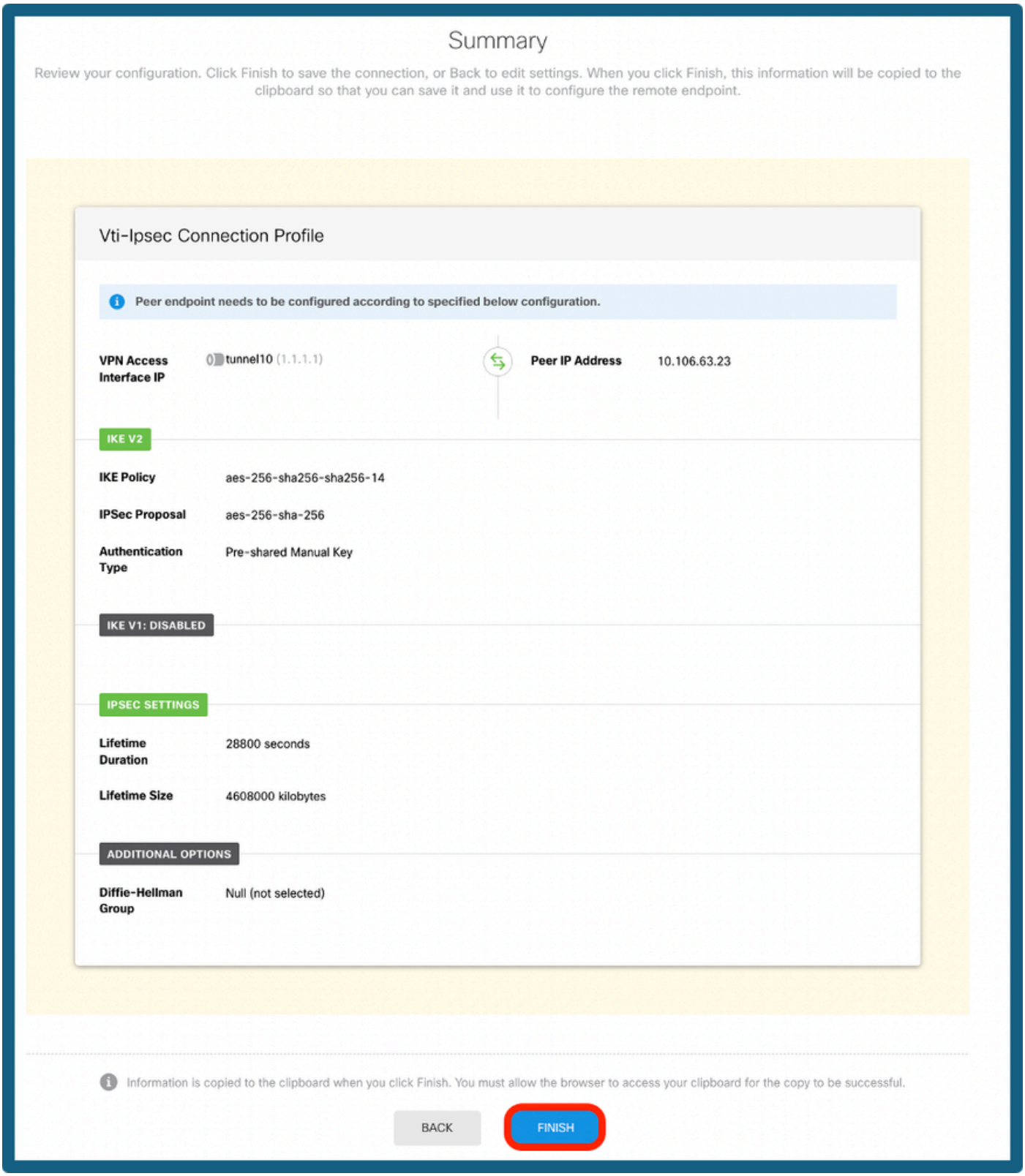
Etapa 8a. Selecione o Tipo de autenticação. Se Pre-shared Manual Key for usado, forneça a chave pré-compartilhada Local e Remote.

Etapa 8b. (Opcional) Escolha as configurações de Perfect Forward Secrecy. Configure IPsec Lifetime Duration and Lifetime Size e clique em Next.



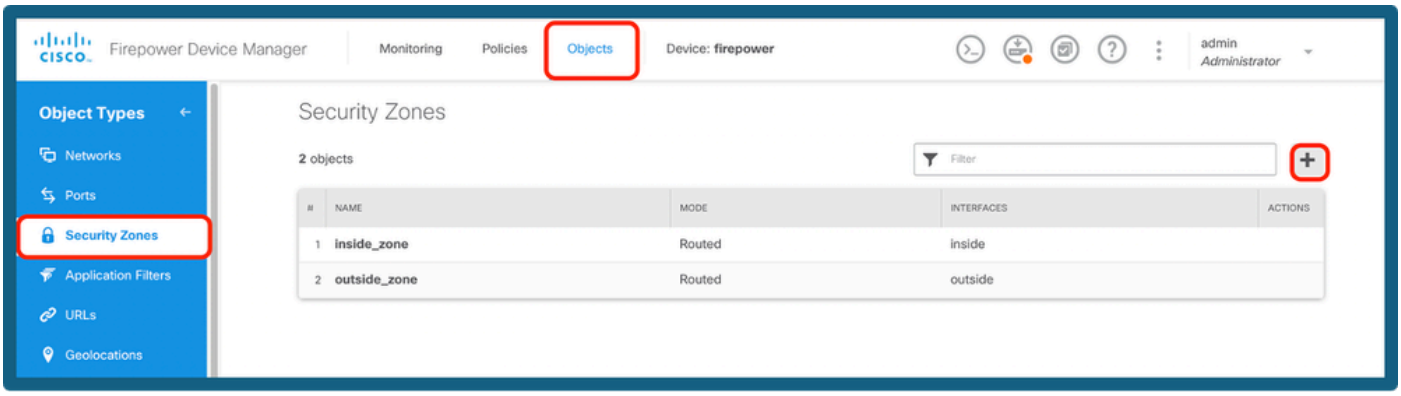
PSK e configuração vitalícia

Etapa 9. Revise a configuração e clique em Finish.



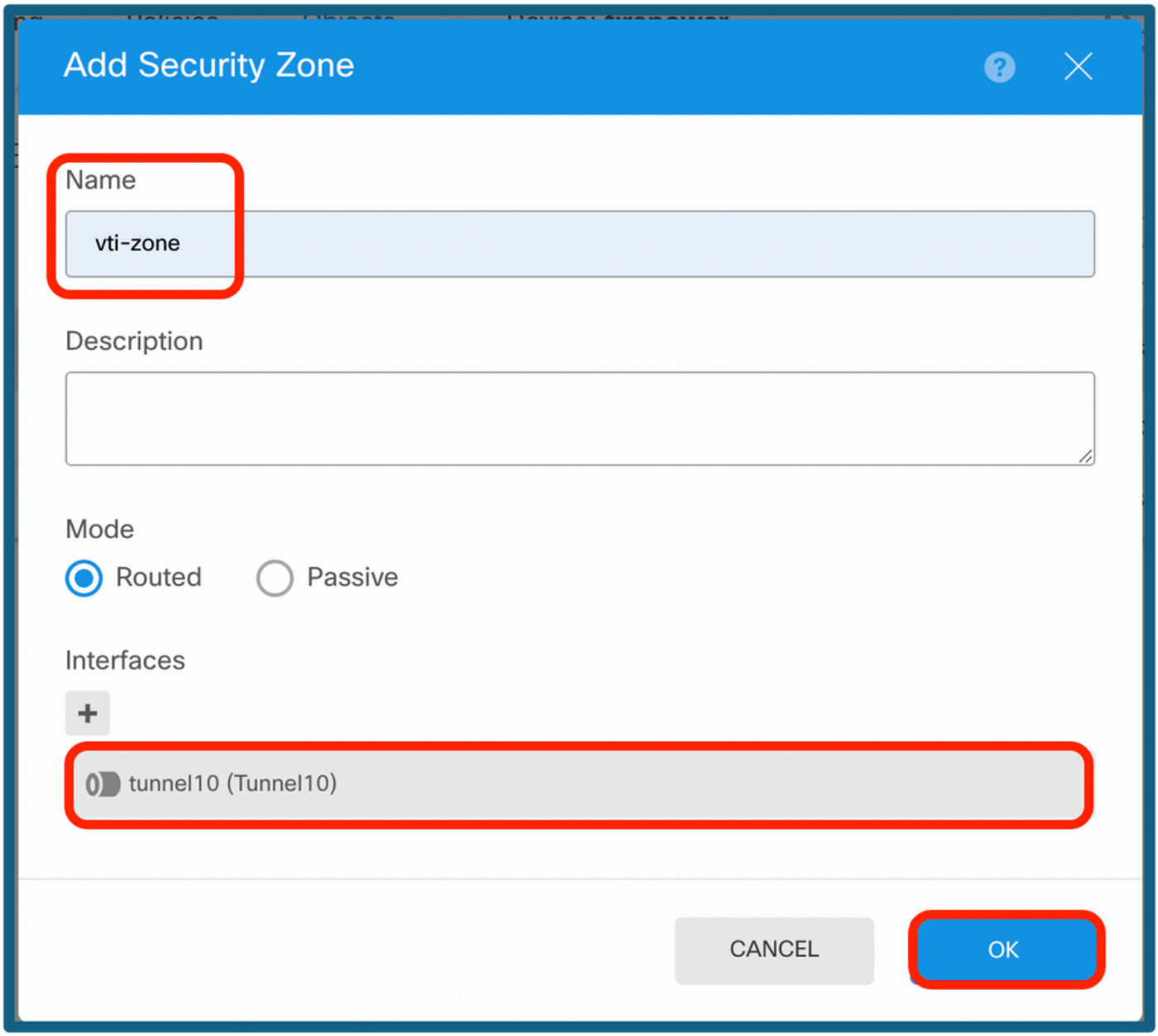
Resumo da configuração

Etapa 10a. Navegue até Objetos > Zonas de segurança e clique no ícone +.



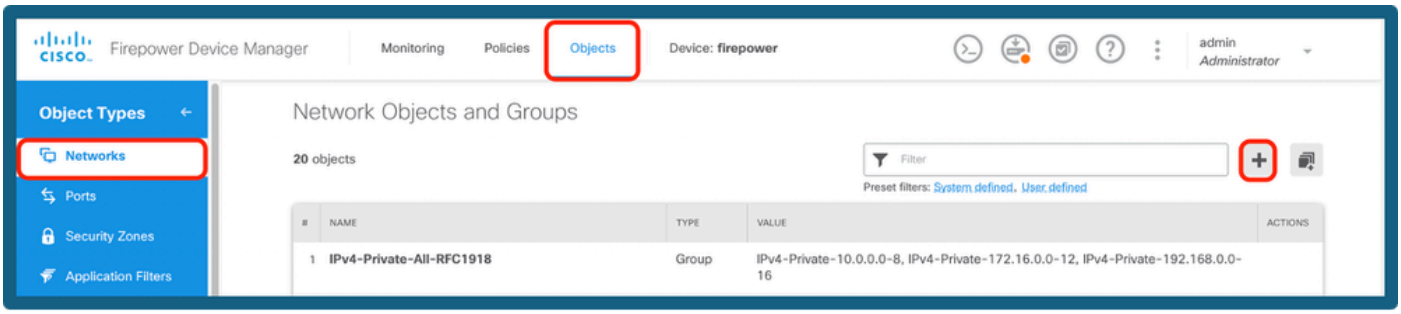
Adicionar uma zona de segurança

Etapa 10b. Crie uma região e selecione a interface VTI como mostrado abaixo.



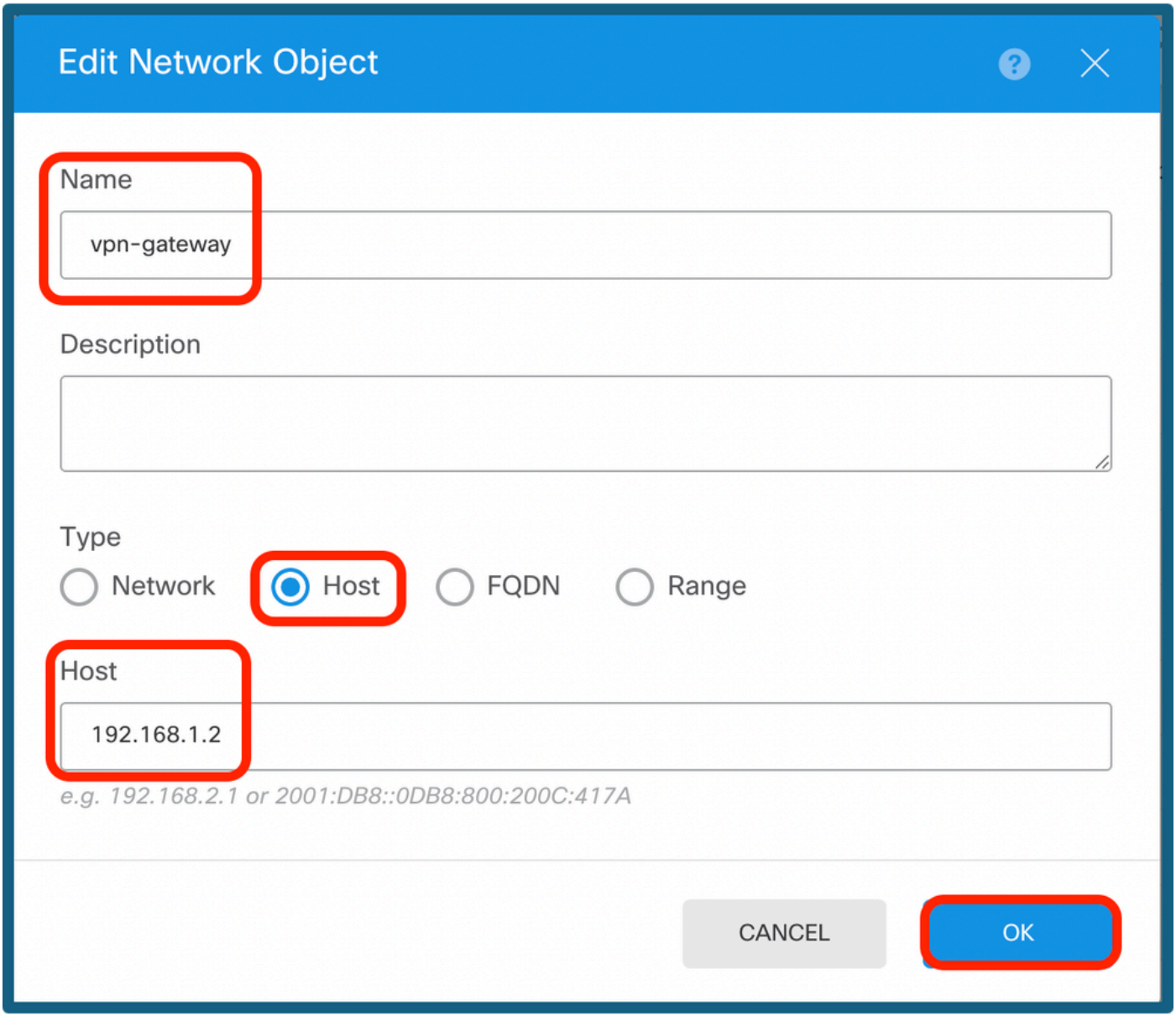
Configuração da zona de segurança

Etapa 11a. Navegue até Objetos > Redes, clique no ícone +.



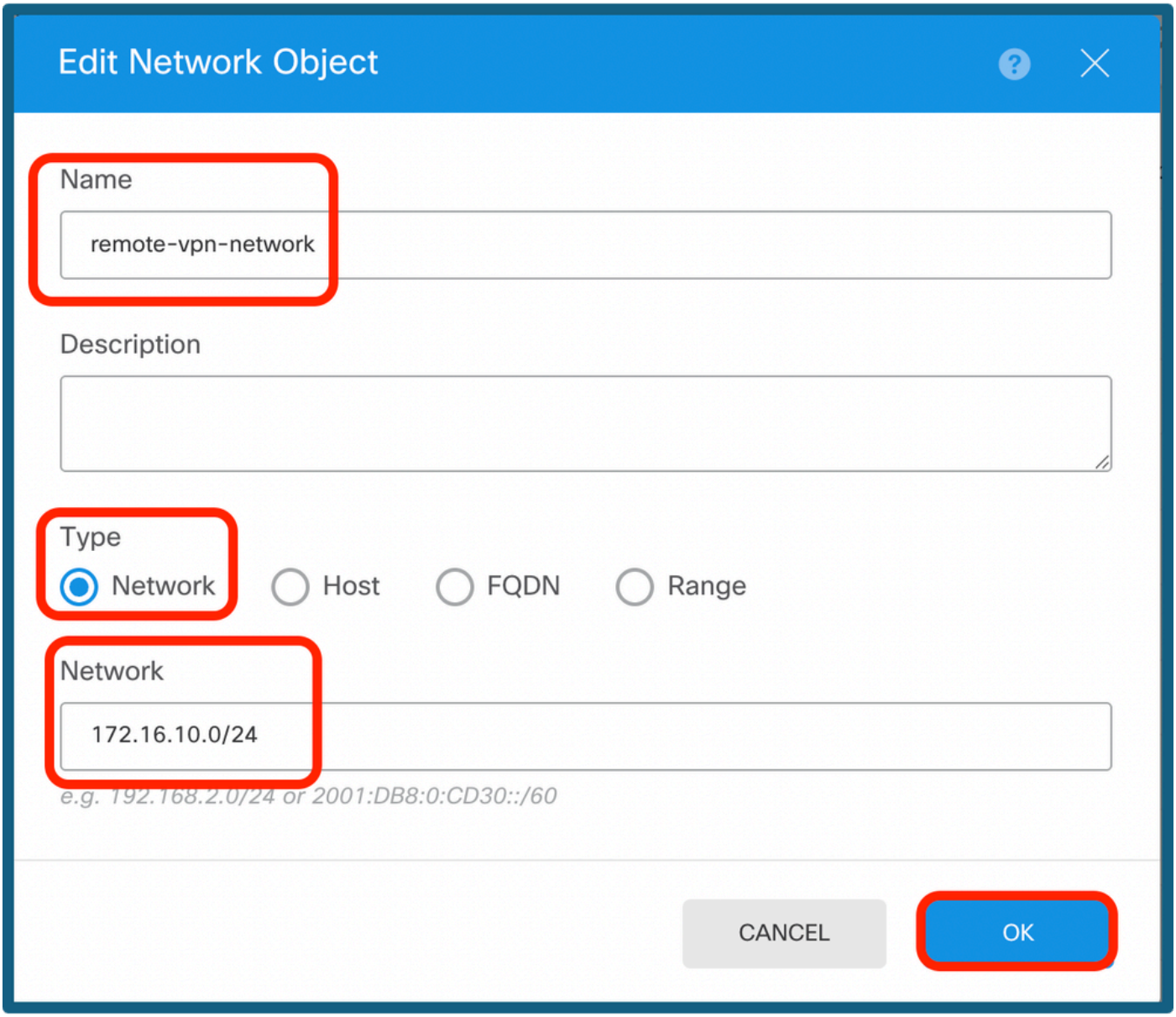
Adicionar objetos de rede

Etapa 11b. Adicione um objeto de host e crie um gateway com o ip de túnel da extremidade do peer.

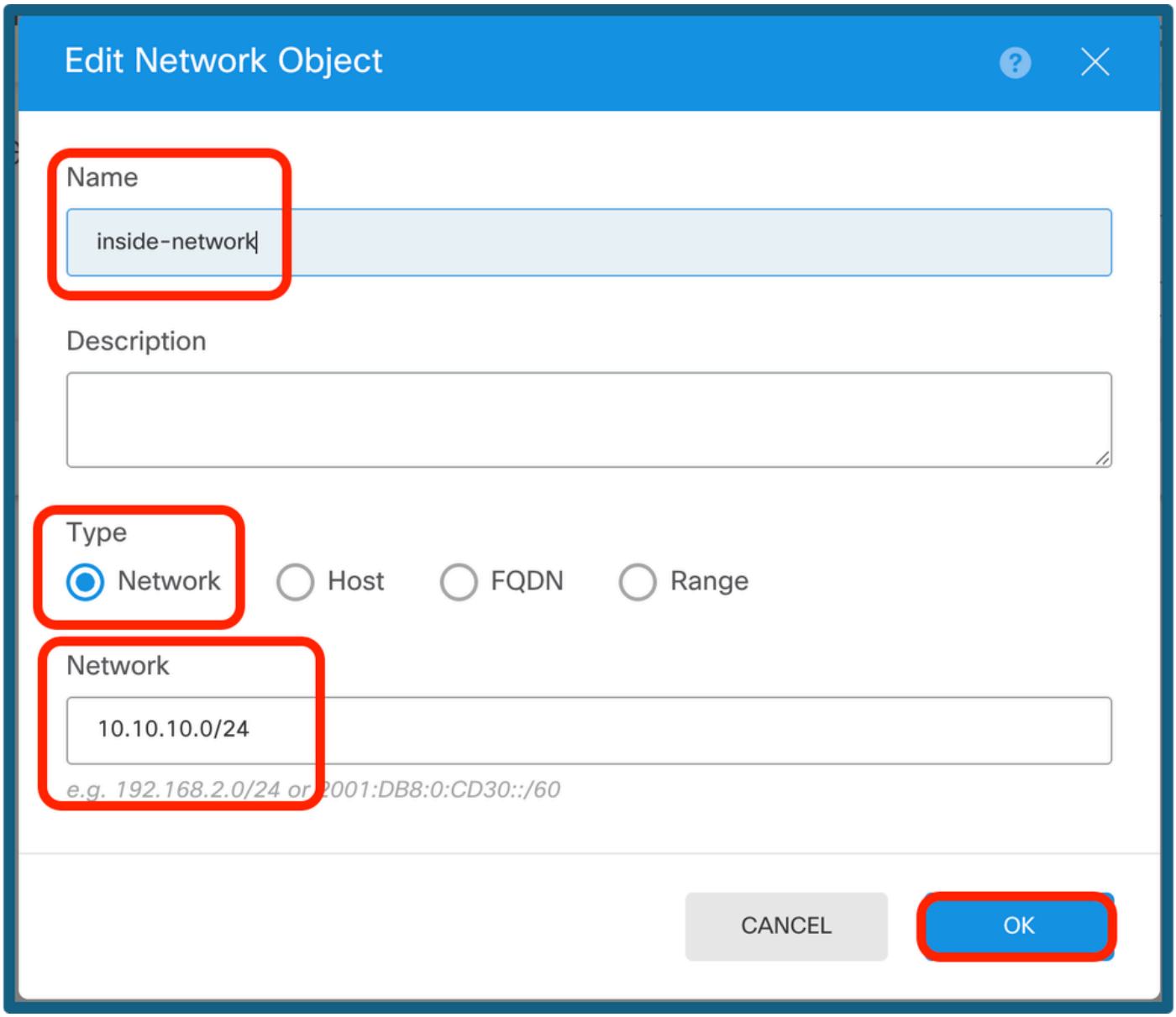


Configurar o gateway VPN

Etapa 11c. Adicione a sub-rede remota e a sub-rede local.

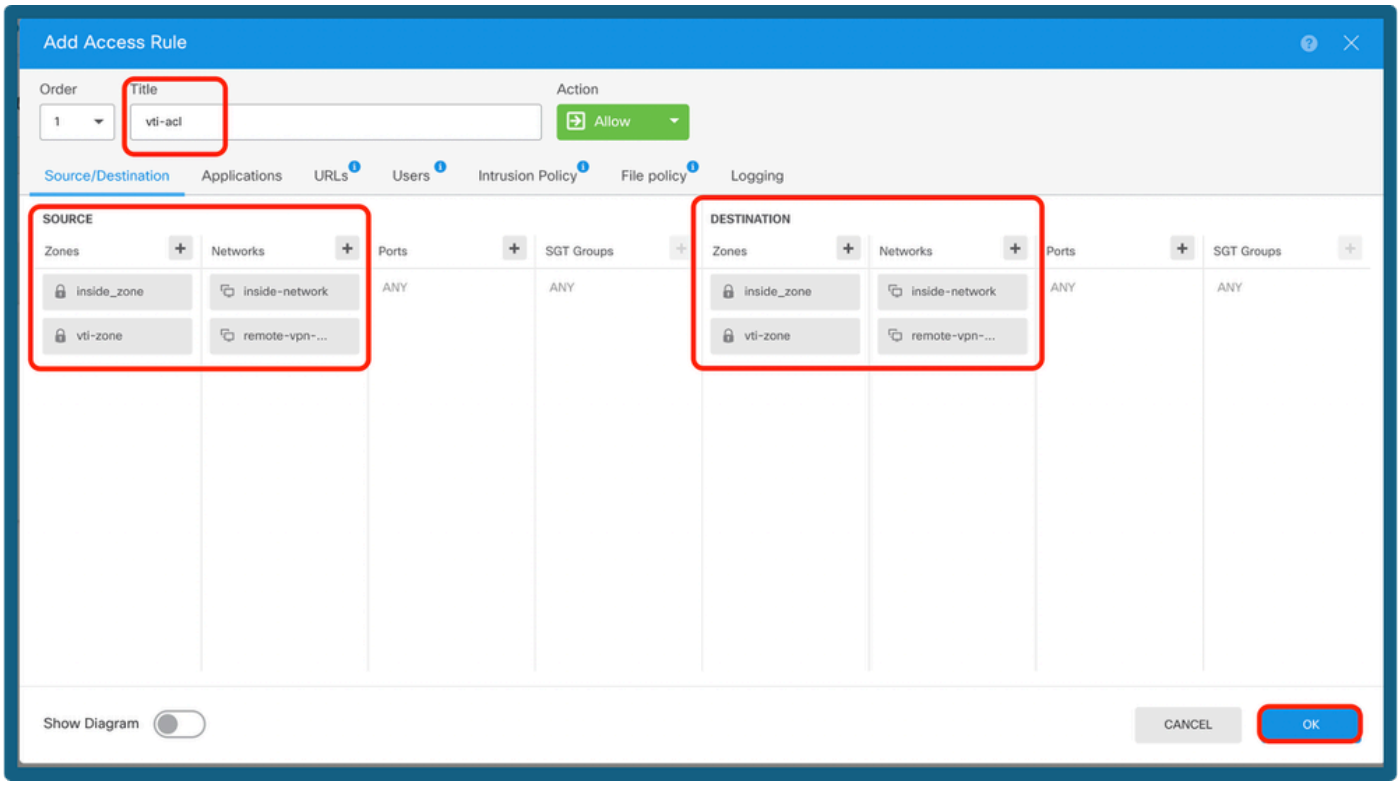


Configuração de IP remoto



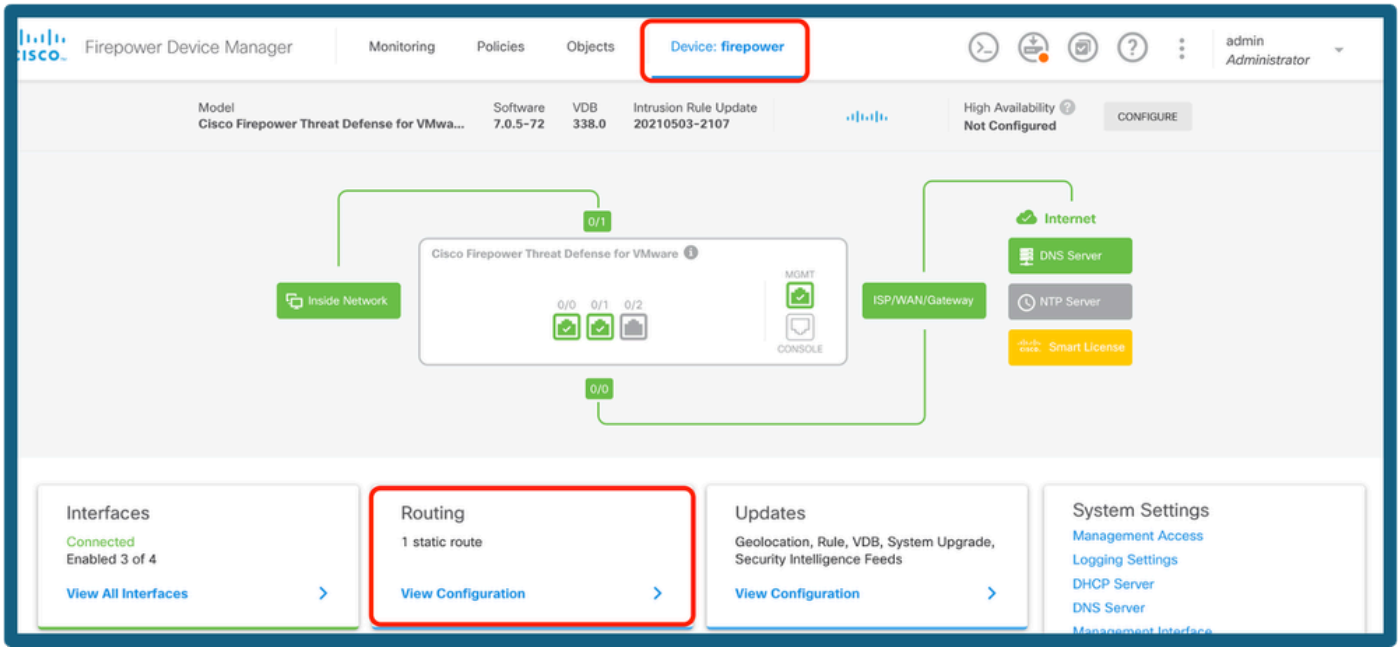
Configuração de IP local

Etapa 12. Navegue até Device > Policies e configure a Access Control Policy.



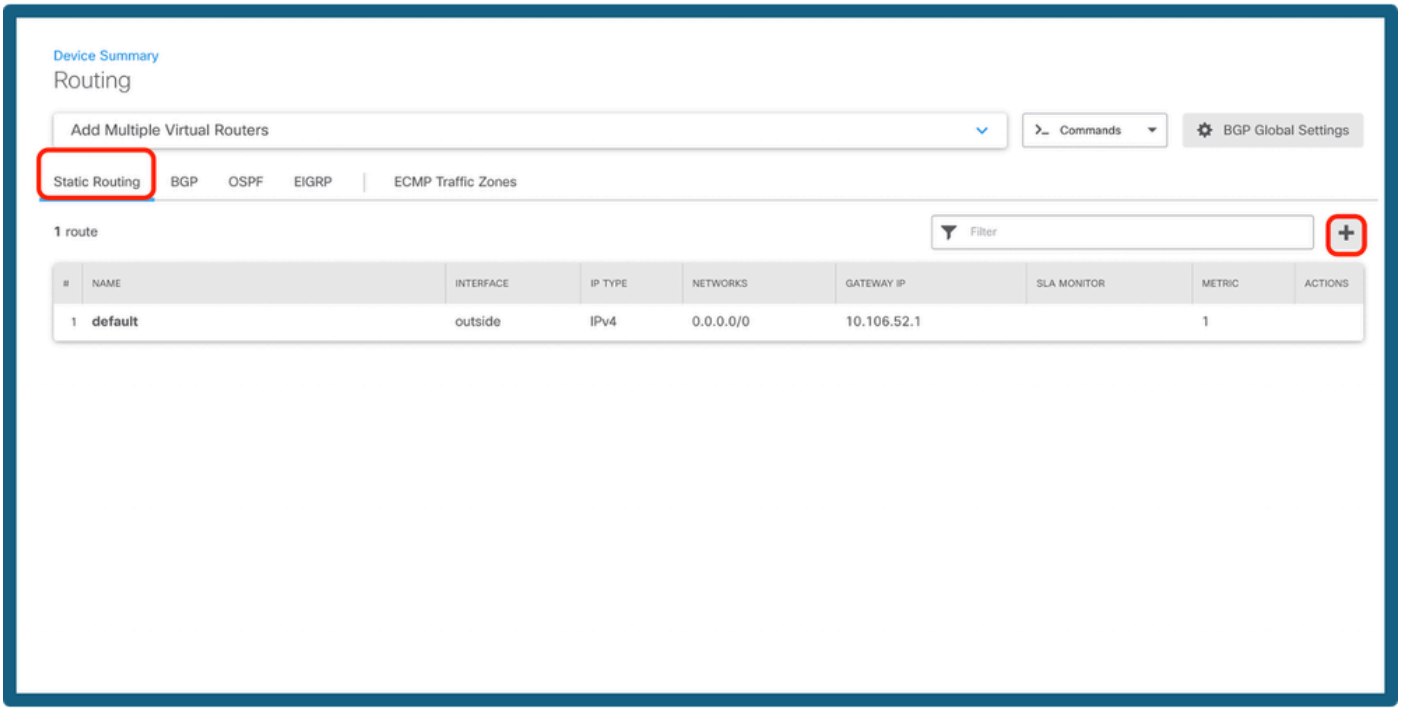
Adicionar Política de Controle de Acesso

Etapa 13a. Adicione o roteamento sobre o túnel VTI. Navegue até Device > Routing.



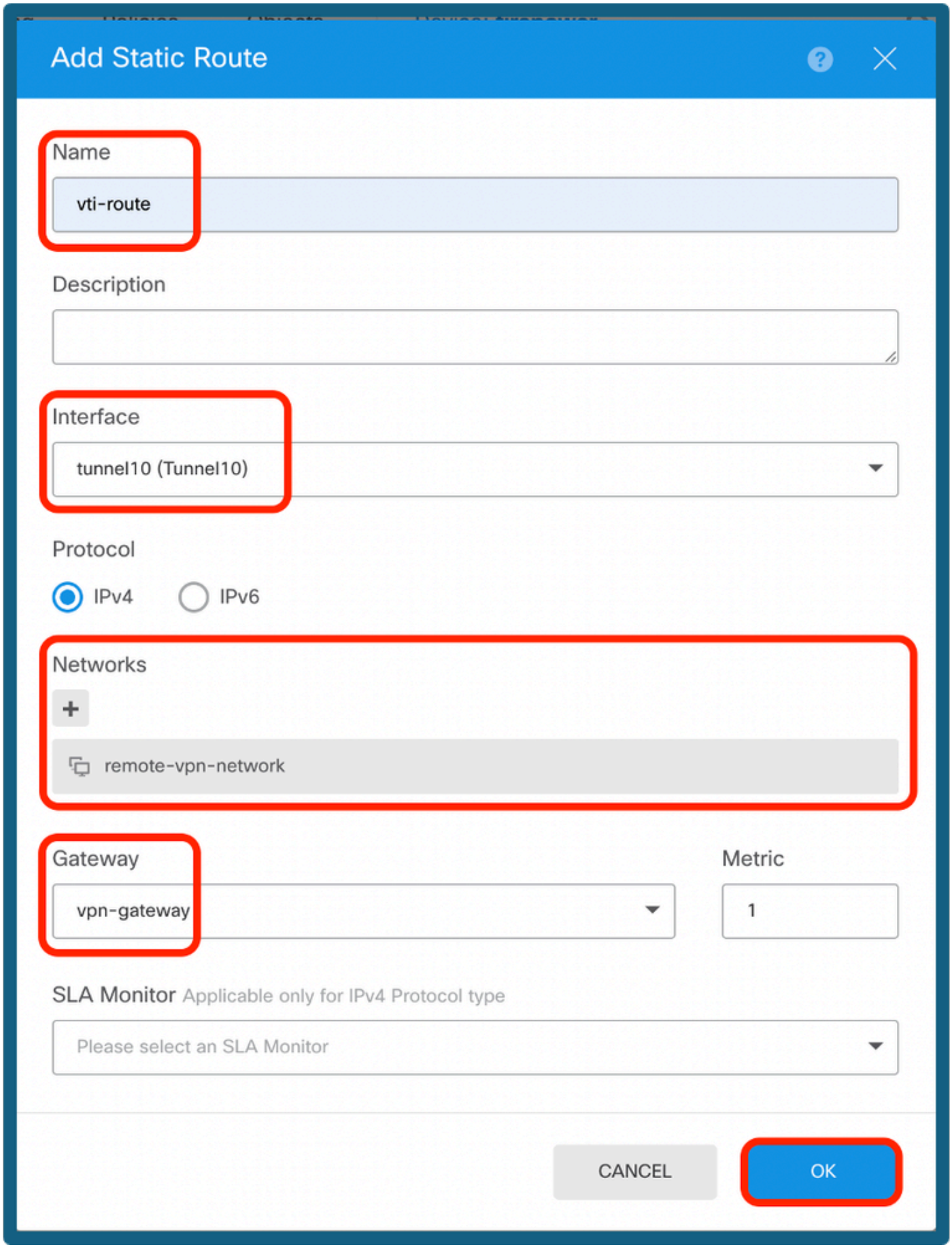
Selecionar Roteamento

Etapa 13b. Navegue até Static Route na guia Routing. Clique no ícone +.



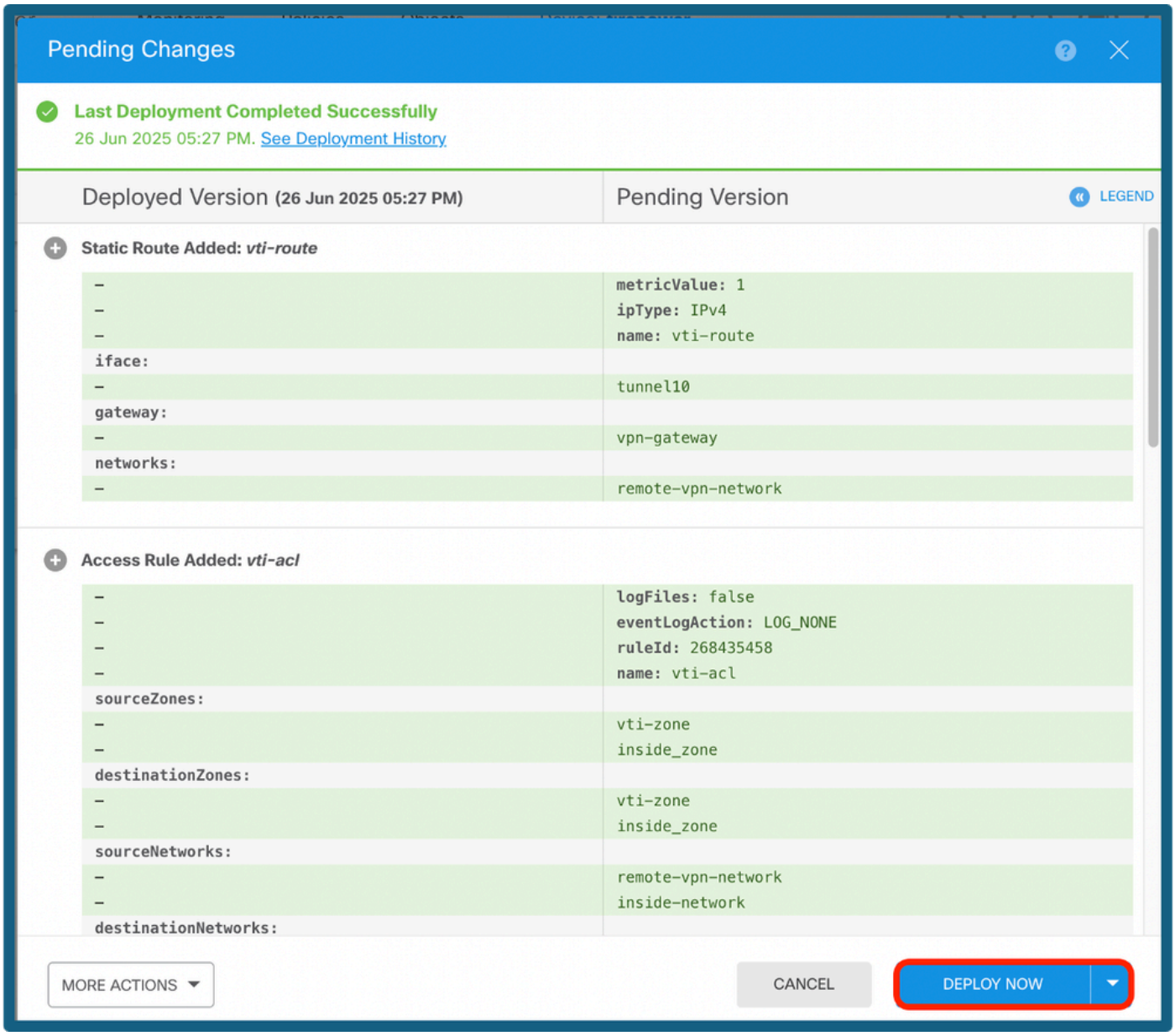
Adicionar rota

Etapa 13c. Forneça a interface, escolha a rede, forneça o gateway. Click OK.



Configurar a rota estática

Etapa 14. Navegue até Implantar. Revise as alterações e clique em Implantar agora.

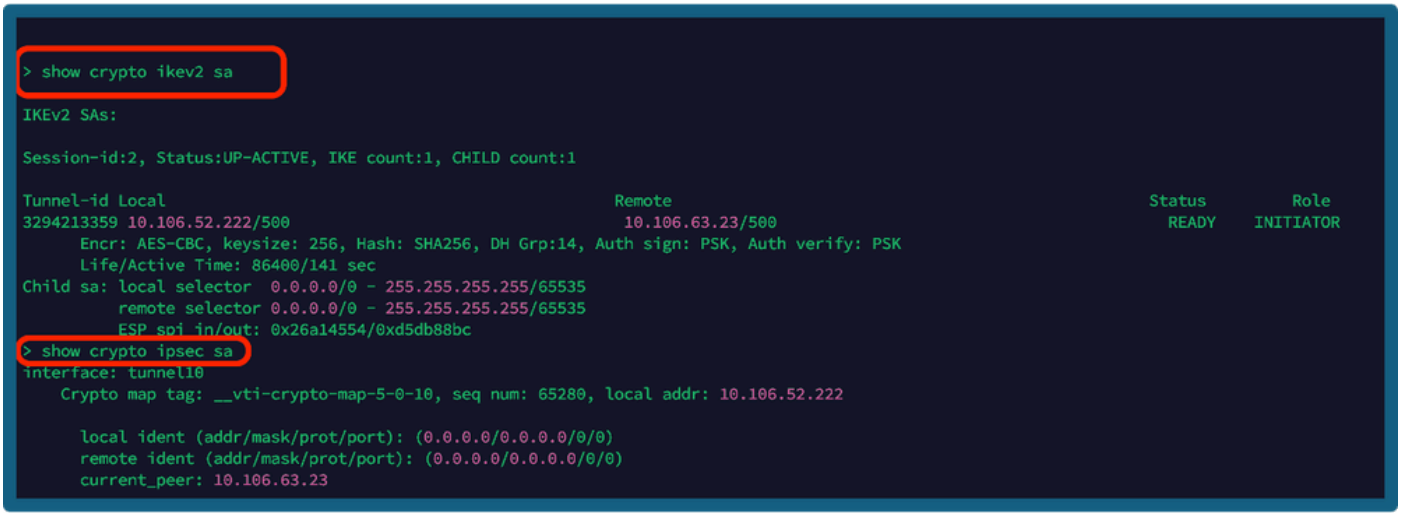


Implantar a configuração

Verificar

Quando a implantação estiver concluída, você poderá verificar o status do túnel na CLI usando os comandos:

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



comandos show

Informações Relacionadas

Para obter mais informações sobre VPNs Site a Site no FTD gerenciado pelo FDM, você pode encontrar o guia de configuração completo aqui:

FTD Gerenciado pelo Guia de Configuração do FDM

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.