Configurar ISP VTI duplo no FTD gerenciado pelo FMC

Contents

Introdução

Este documento descreve a implantação de configuração de ISP duplo usando interfaces de túnel virtual em um dispositivo FTD gerenciado pelo FMC.

Pré-requisitos

Requisitos básicos

- Uma compreensão básica de VPNs site a site seria benéfica. Esse histórico ajuda a compreender o processo de configuração do VTI, incluindo os conceitos e as configurações principais envolvidas.
- Entender os fundamentos da configuração e do gerenciamento de VTIs na plataforma Cisco Firepower é essencial. Tal inclui o conhecimento do funcionamento dos VTI no âmbito do FTD e do modo como são controlados através da interface do FMC.

Componentes Utilizados

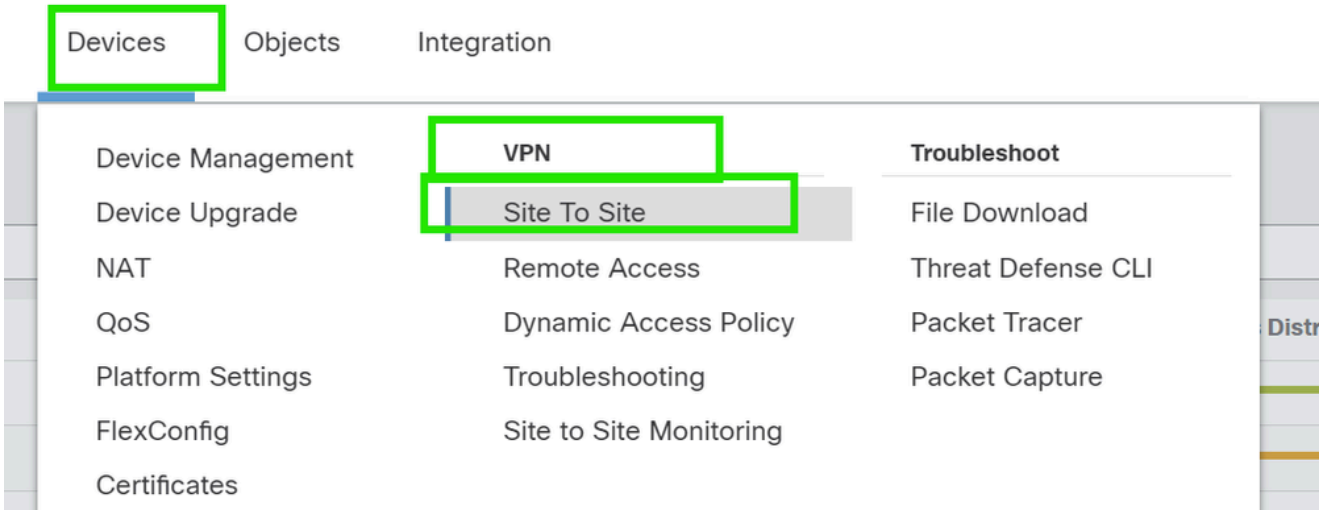
- Cisco Firepower Threat Defense (FTD) para VMware: versão 7.0.0
- Firepower Management Center (FMC): versão 7.2.4 (build 169)

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.

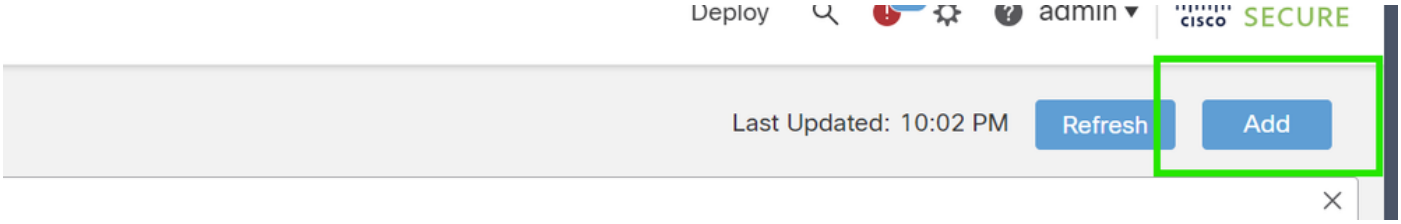
Configurações no FMC

Configuração de Topologia

1. Navegue até Devices >VPN > Site To Site.



2. Clique em Add para adicionar a topologia VPN.



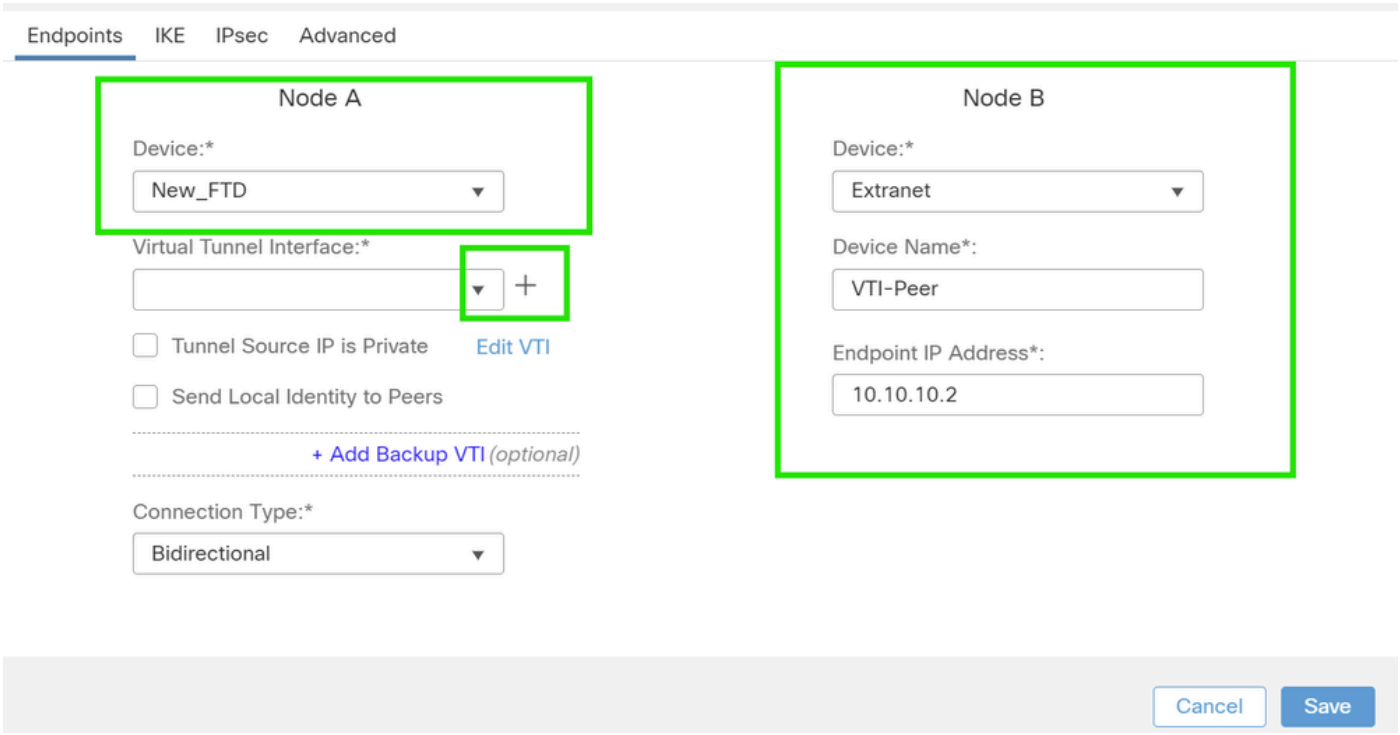
3. Dê um nome para a topologia, escolha VTI e Ponto a Ponto e selecione uma versão IKE (IKEv2 neste caso).

Configuração do endpoint

1. Escolha o dispositivo no qual o túnel precisa ser configurado.

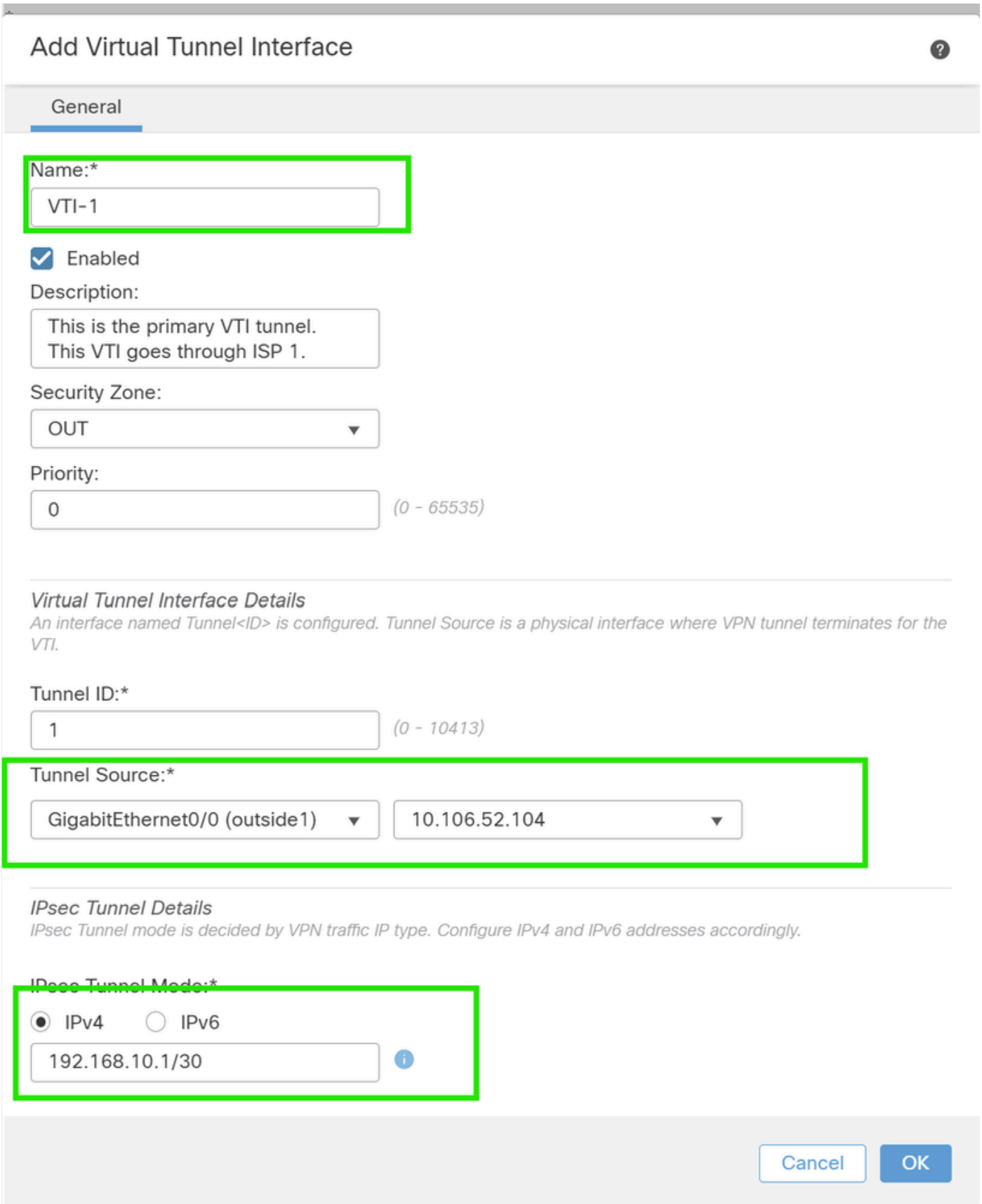
Adicione os detalhes do peer remoto.

Você pode adicionar uma nova Interface de Modelo Virtual clicando no ícone "+" ou selecionar um na lista existente.

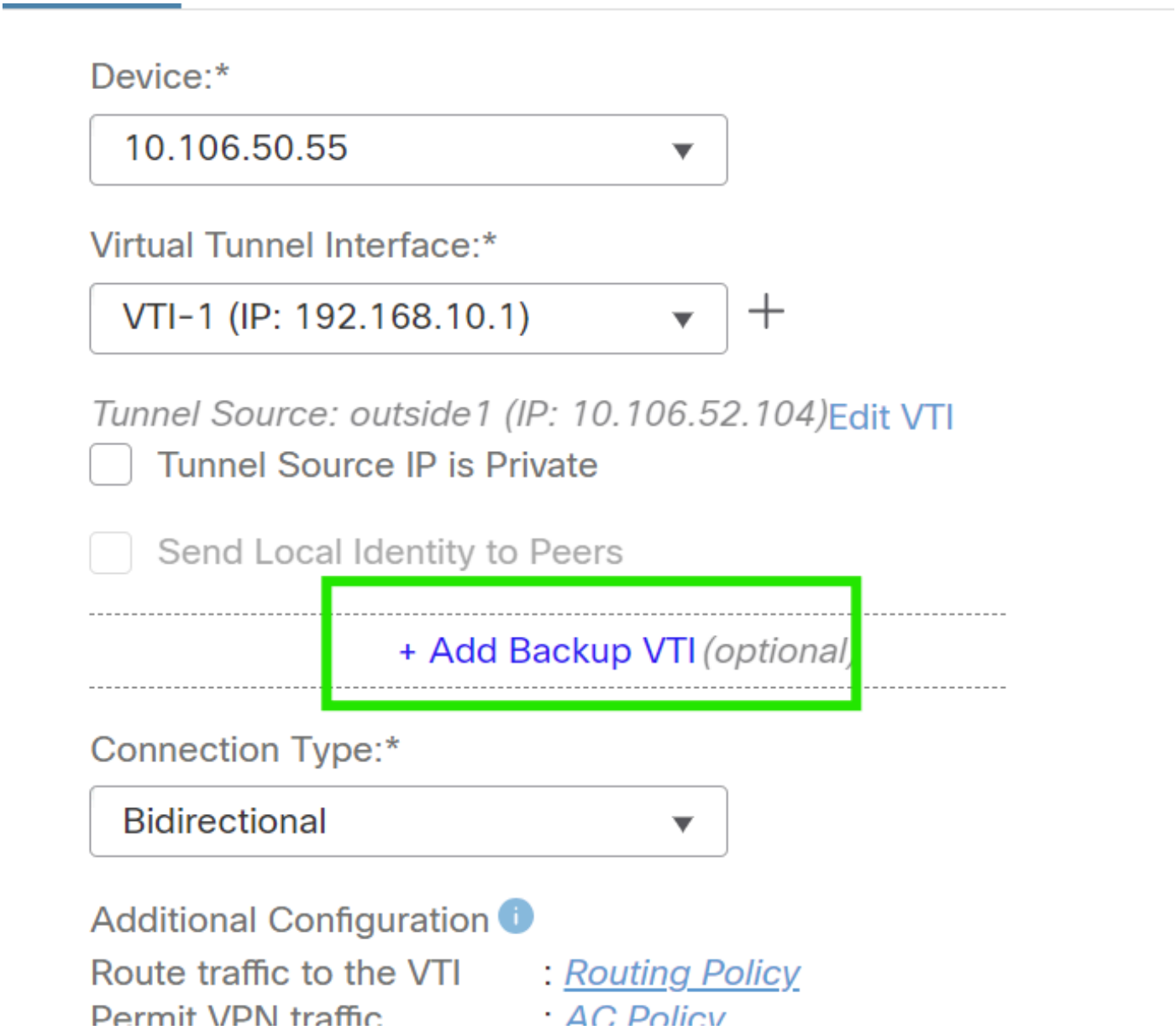


Se estiver criando uma nova interface VTI, adicione os parâmetros corretos, ative-os e clique em "OK".

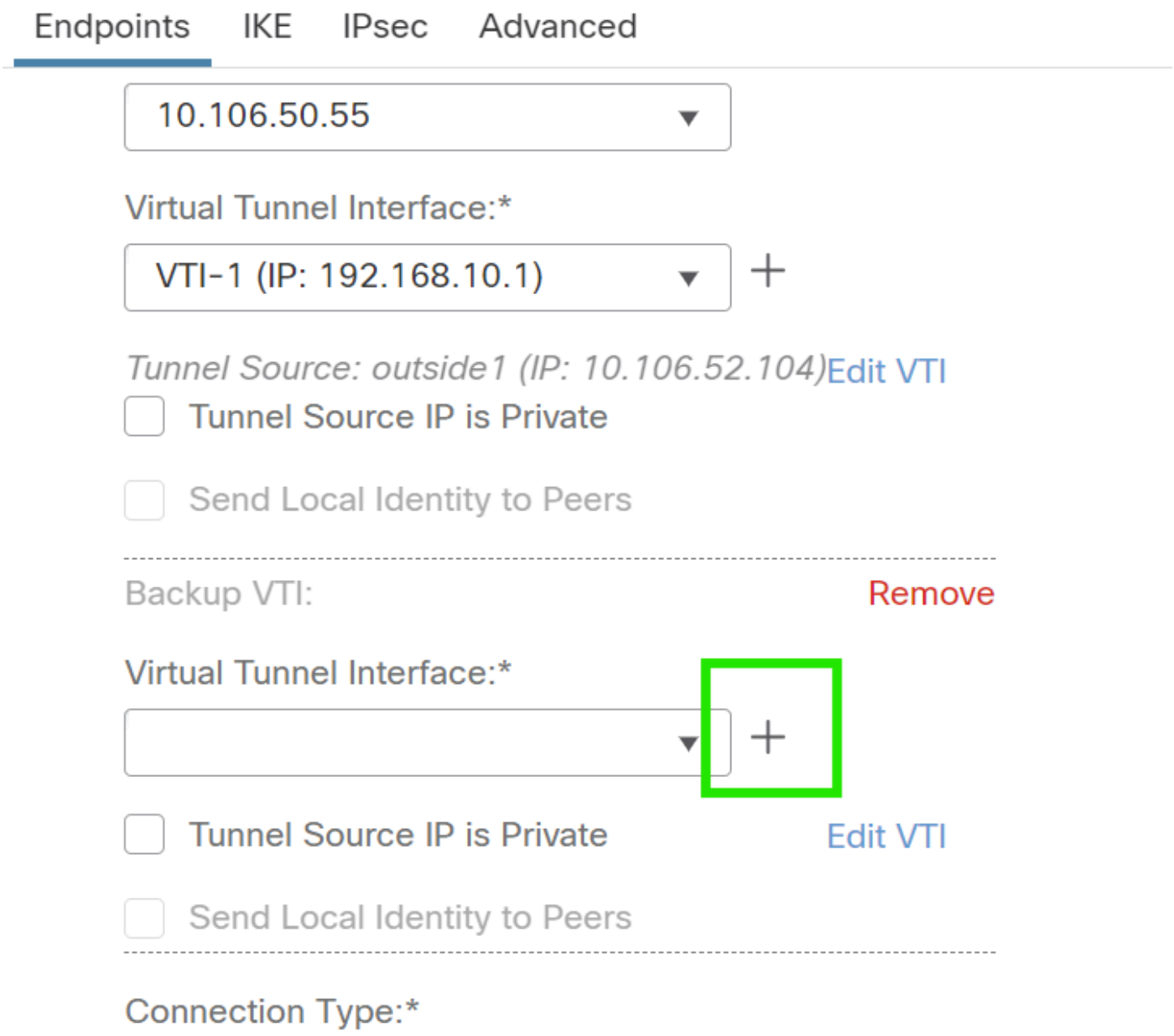
OBSERVAÇÃO: este se torna o VTI principal.



3. Clique em "+ ". Add Backup VIT" (Adicionar VIT de backup) para adicionar um VIT secundário.

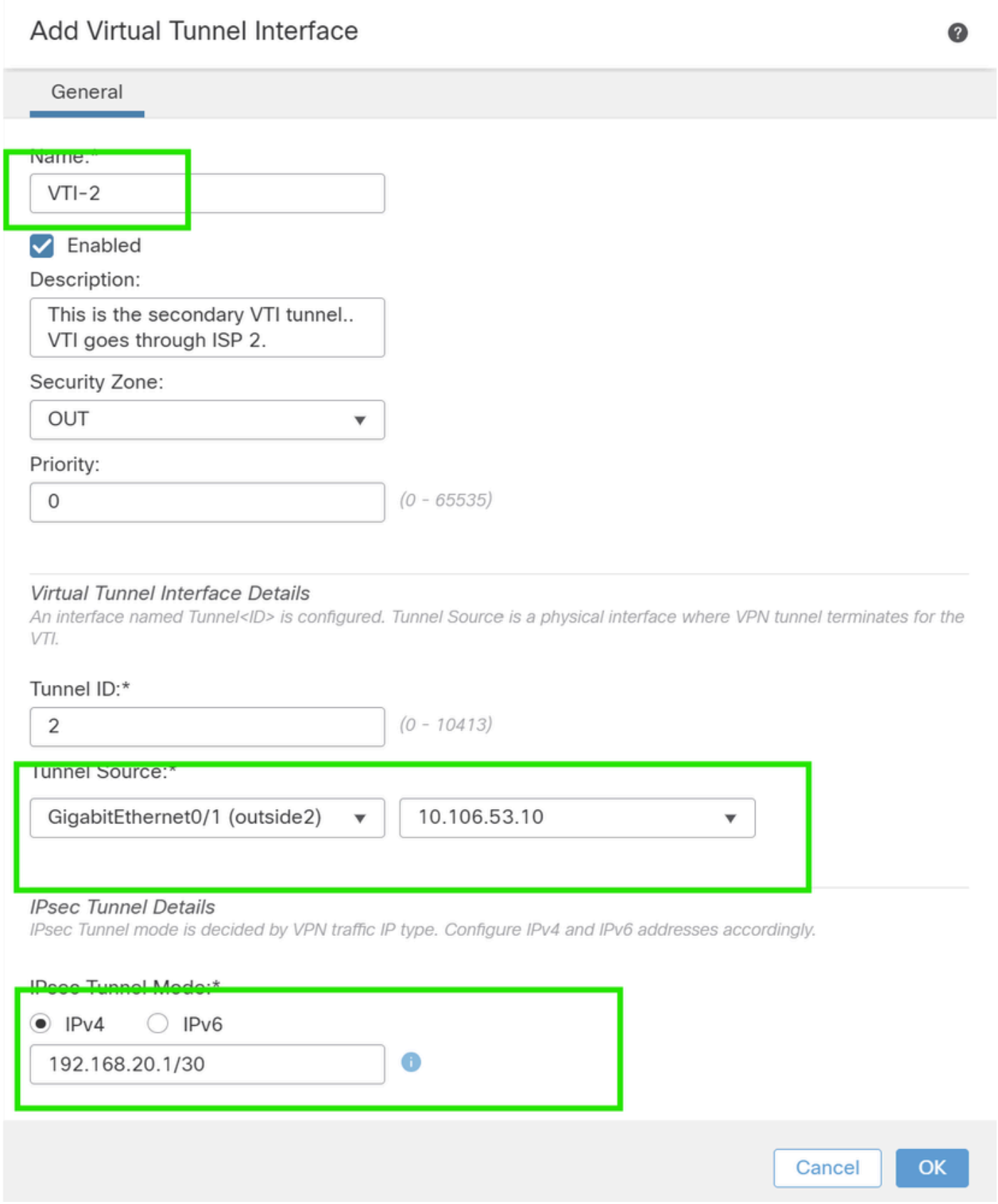


4. Clique em "+" para adicionar parâmetro para VTI secundário (se ainda não estiver configurado).



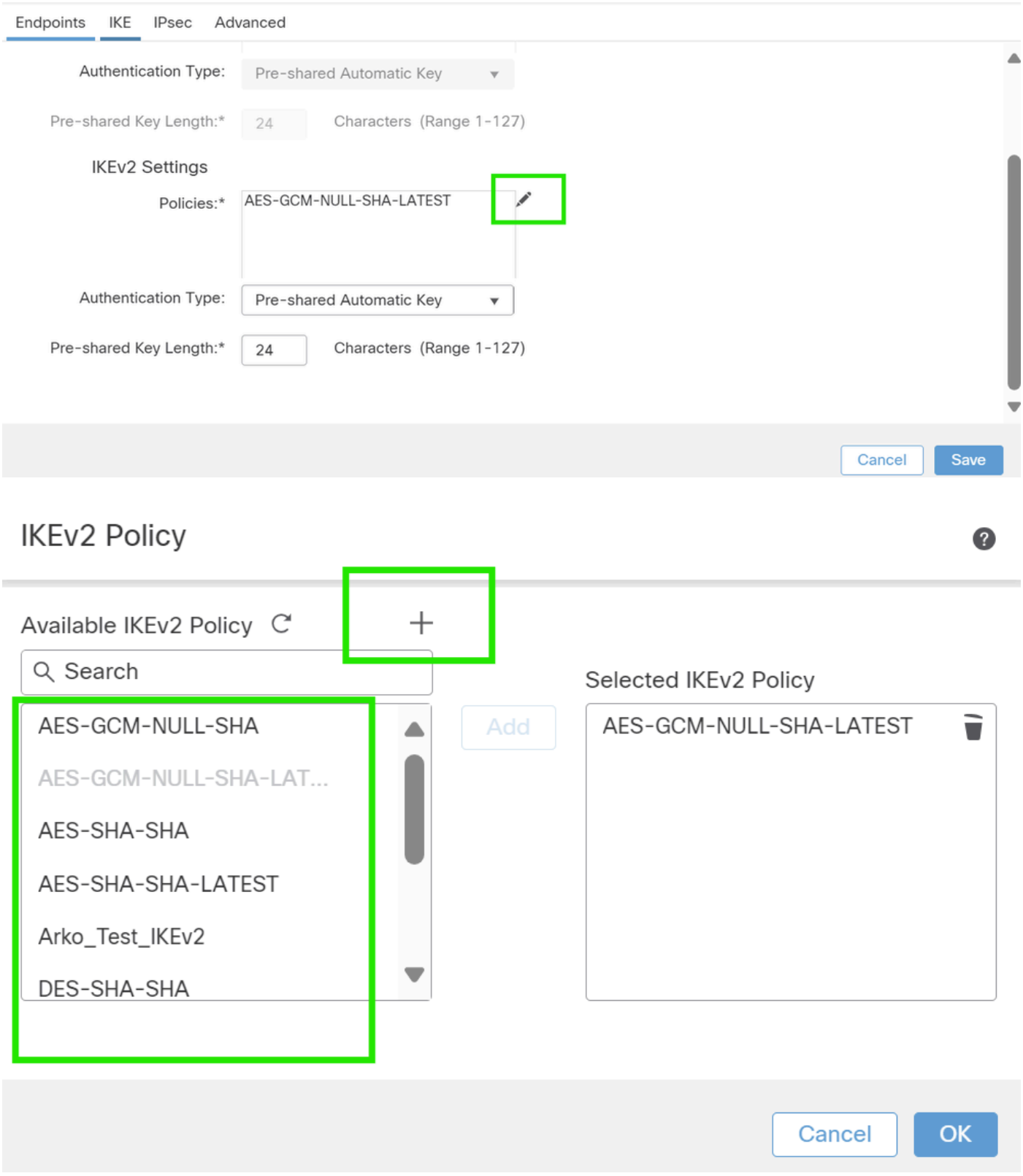
5. Se estiver criando uma nova interface VTI, adicione os parâmetros corretos, ative-os e clique em "OK".

OBSERVAÇÃO: este se torna o VTI secundário.

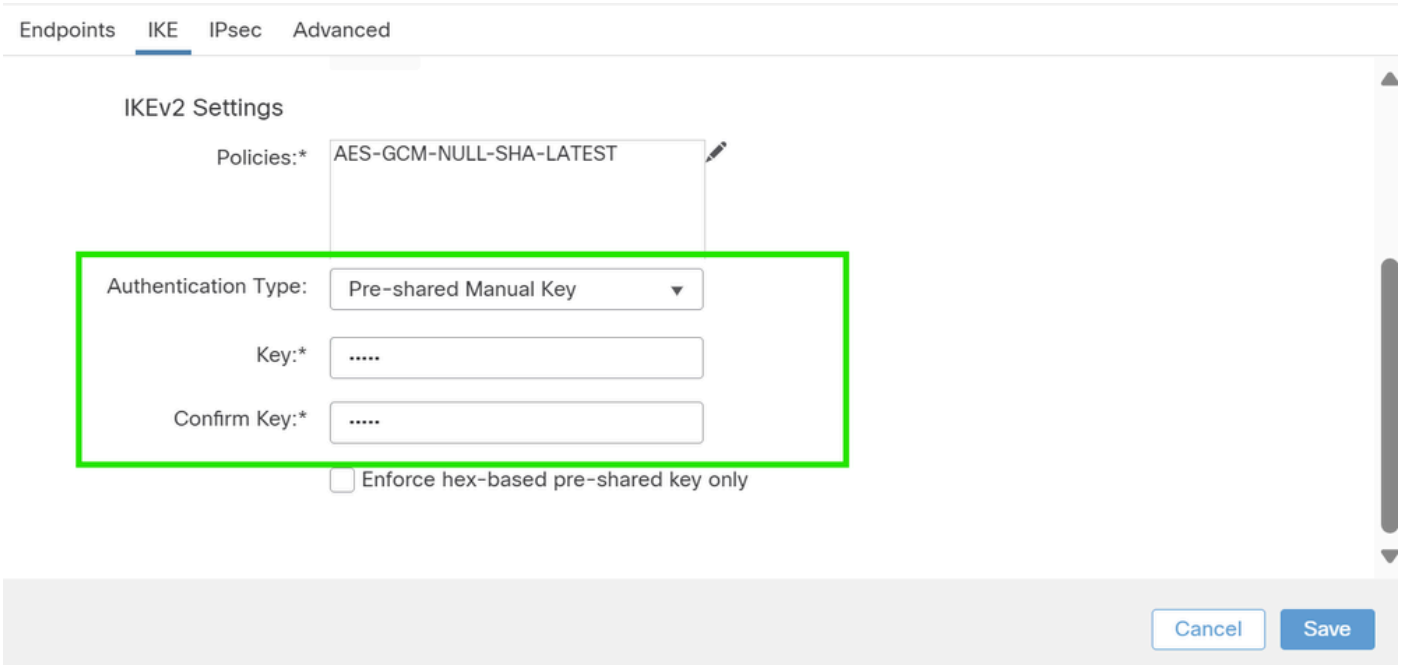


configuração de IKE

1. Navegue até a guia IKE. Você pode optar por usar uma política predefinida ou clicar no botão de lápis ao lado da guia Política para criar uma nova ou selecionar outra política disponível com base em sua exigência.

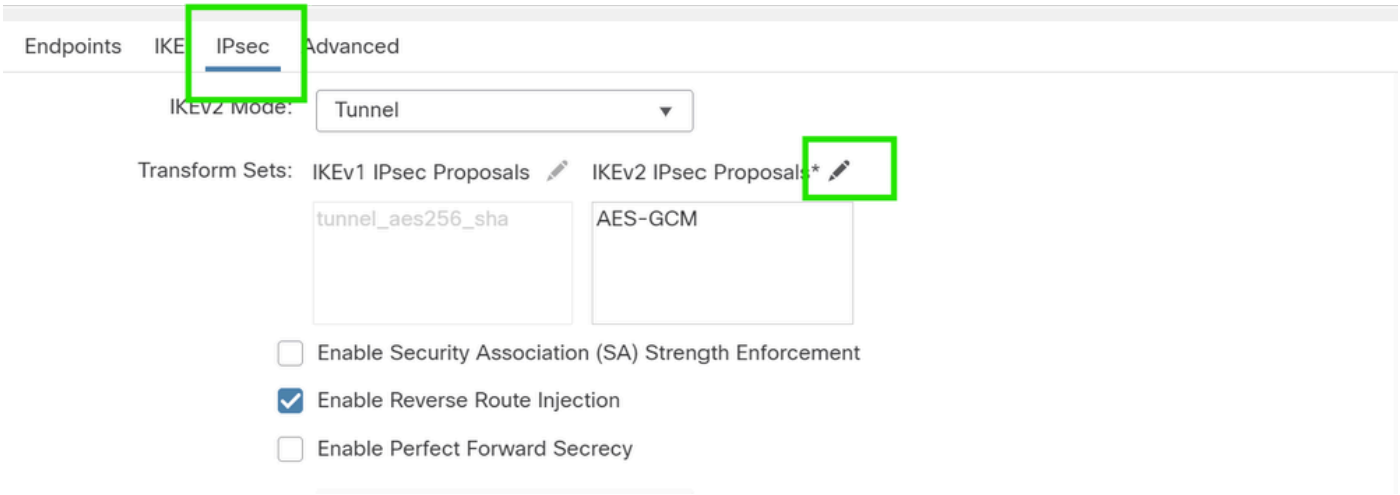


2. Selecione o Tipo de autenticação. Se uma chave manual pré-compartilhada for usada, forneça a chave nas caixas Key e Confirm Key.



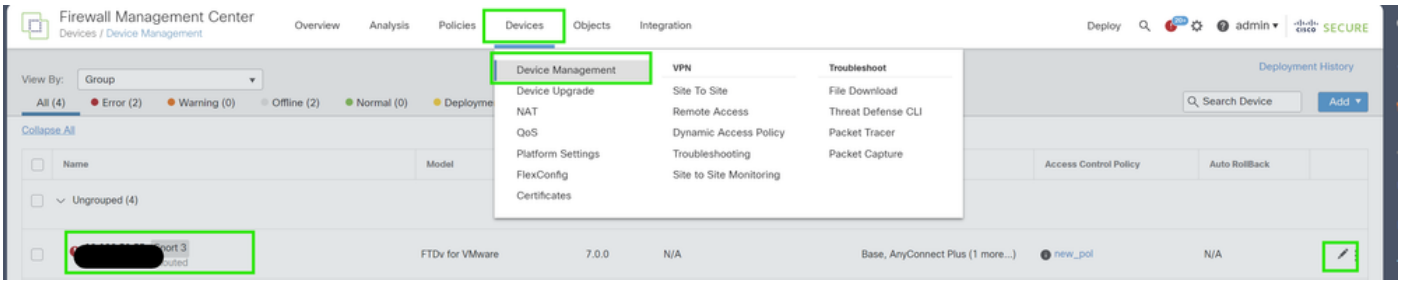
configuração de IPsec

Navegue até a guia IPsec. Você pode optar por usar uma proposta predefinida clicando no botão do lápis ao lado da guia de proposta para criar uma nova proposta ou selecionar outra proposta disponível com base em sua necessidade.



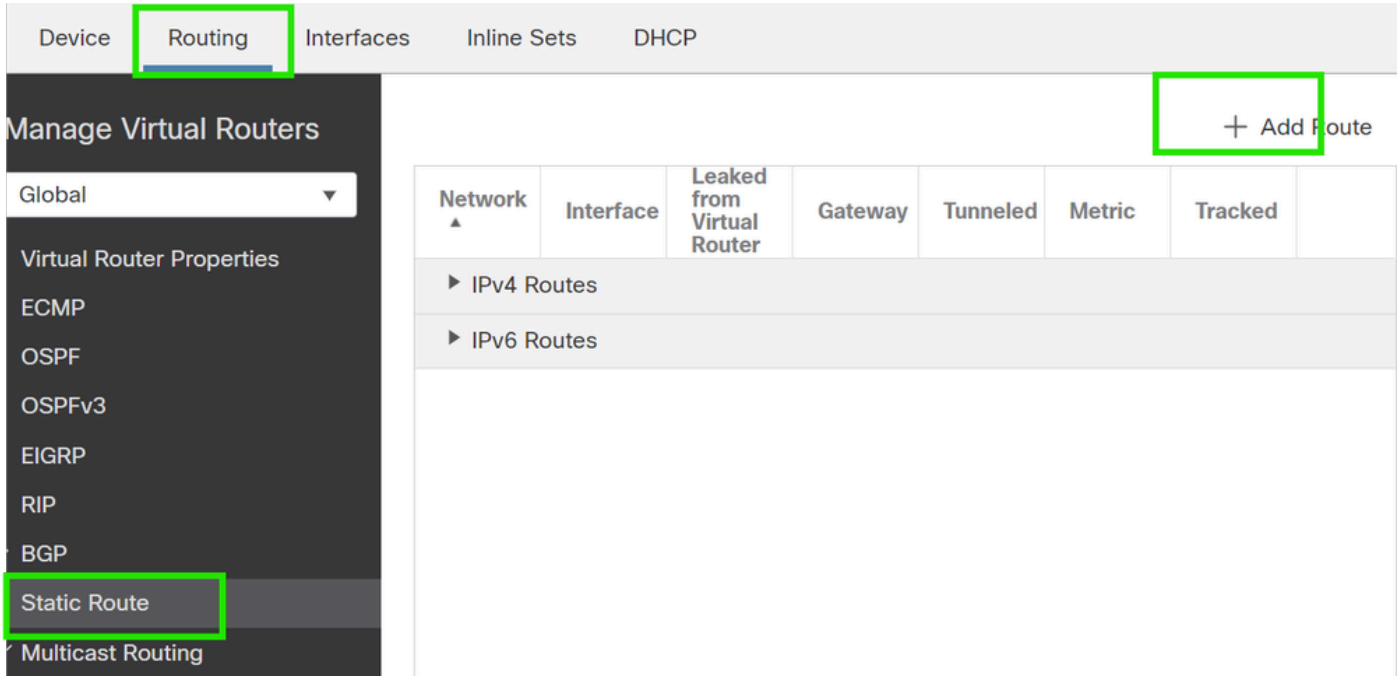
Configuração de roteamento

1. Vá para Device > Device Management e clique no ícone do lápis para editar o dispositivo (FTD).



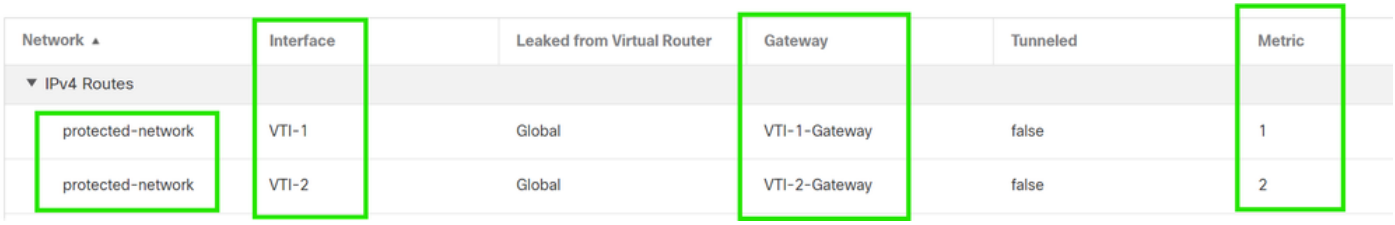
2. Vá para Roteamento > Rota estática e clique no botão "+" para adicionar uma rota ao VTI primário e secundário.

OBSERVAÇÃO: você pode configurar o método de roteamento apropriado para que o tráfego passe pela interface de túnel. Nesse caso, foram usadas rotas estáticas.



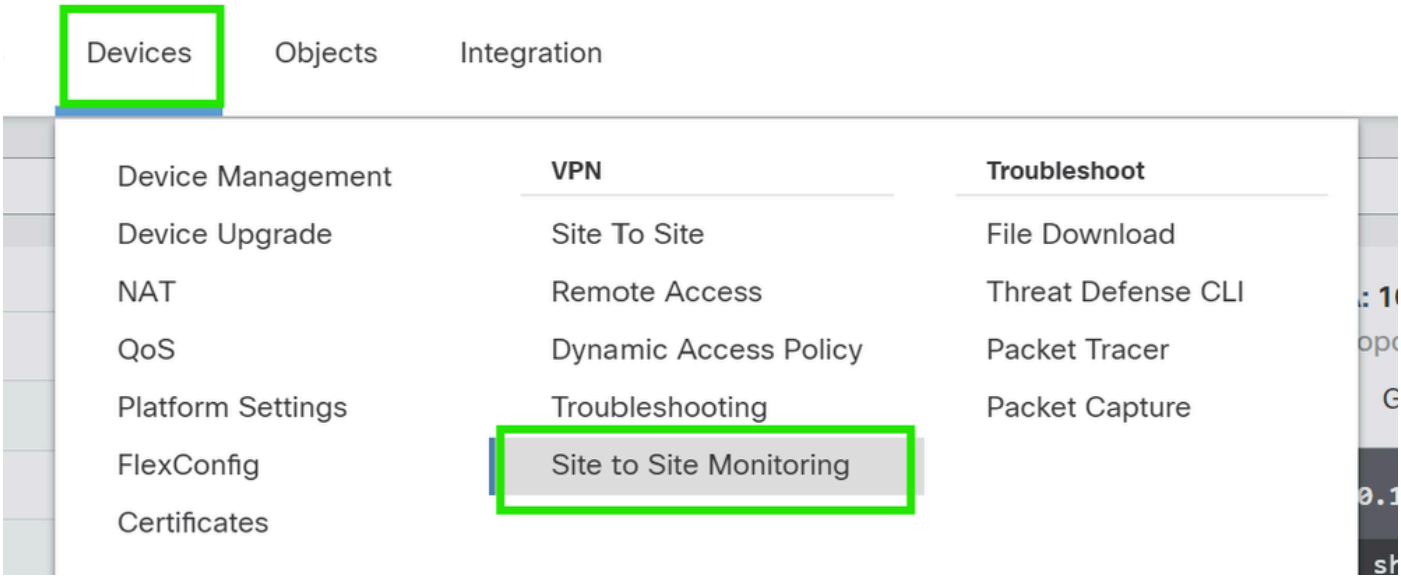
3. Adicione duas rotas para sua rede protegida e defina um valor AD mais alto (neste caso, 2) para a rota secundária.

A primeira rota usa a interface VTI-1 e a segunda usa a interface VTI-2.

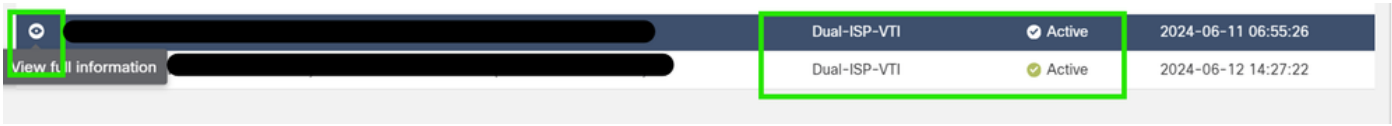


Verificar

1. Vá para Devices > VPN > Site to Site Monitoring .



2. Clique no olho para verificar mais detalhes sobre o status do túnel.



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.