Configuration de deux interfaces VTI ISP sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit le déploiement d'une configuration ISP double à l'aide d'interfaces de tunnel virtuel sur un périphérique FTD géré par FMC.

Conditions préalables

Exigences de base

- Une compréhension fondamentale des VPN de site à site serait bénéfique. Cette formation vous aide à comprendre le processus de configuration de VTI, y compris les principaux concepts et configurations impliqués.
- Il est essentiel de comprendre les principes fondamentaux de la configuration et de la gestion des interfaces VTI sur la plate-forme Cisco Firepower. Cela inclut la connaissance du fonctionnement des interfaces VTI dans le FTD et de la manière dont elles sont contrôlées via l'interface FMC.

Composants utilisés

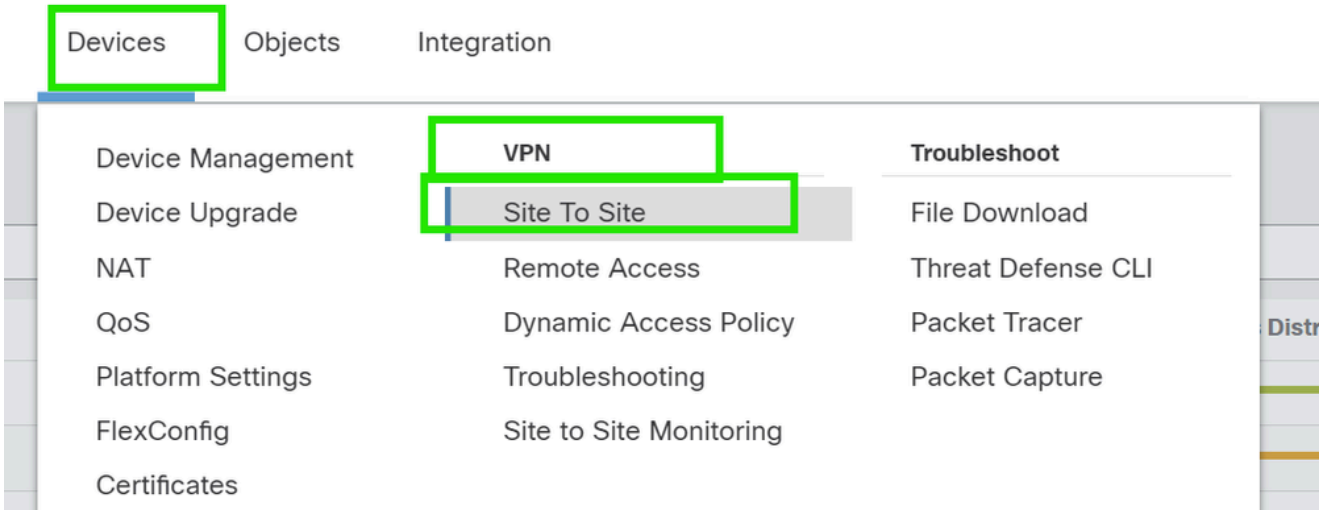
- Cisco Firepower Threat Defense (FTD) pour VMware : version 7.0.0
- Firepower Management Center (FMC) : version 7.2.4 (build 169)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

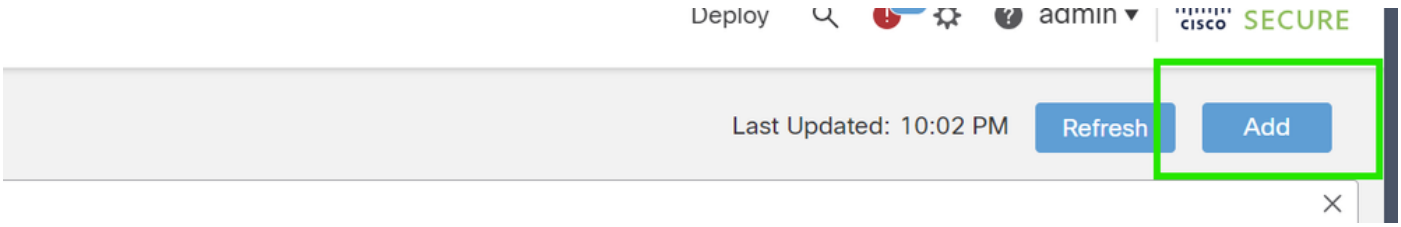
Configurations sur FMC

Configuration topologique

1. Accédez à Périphériques > VPN > Site à site.



2. Cliquez sur Add pour ajouter une topologie VPN.



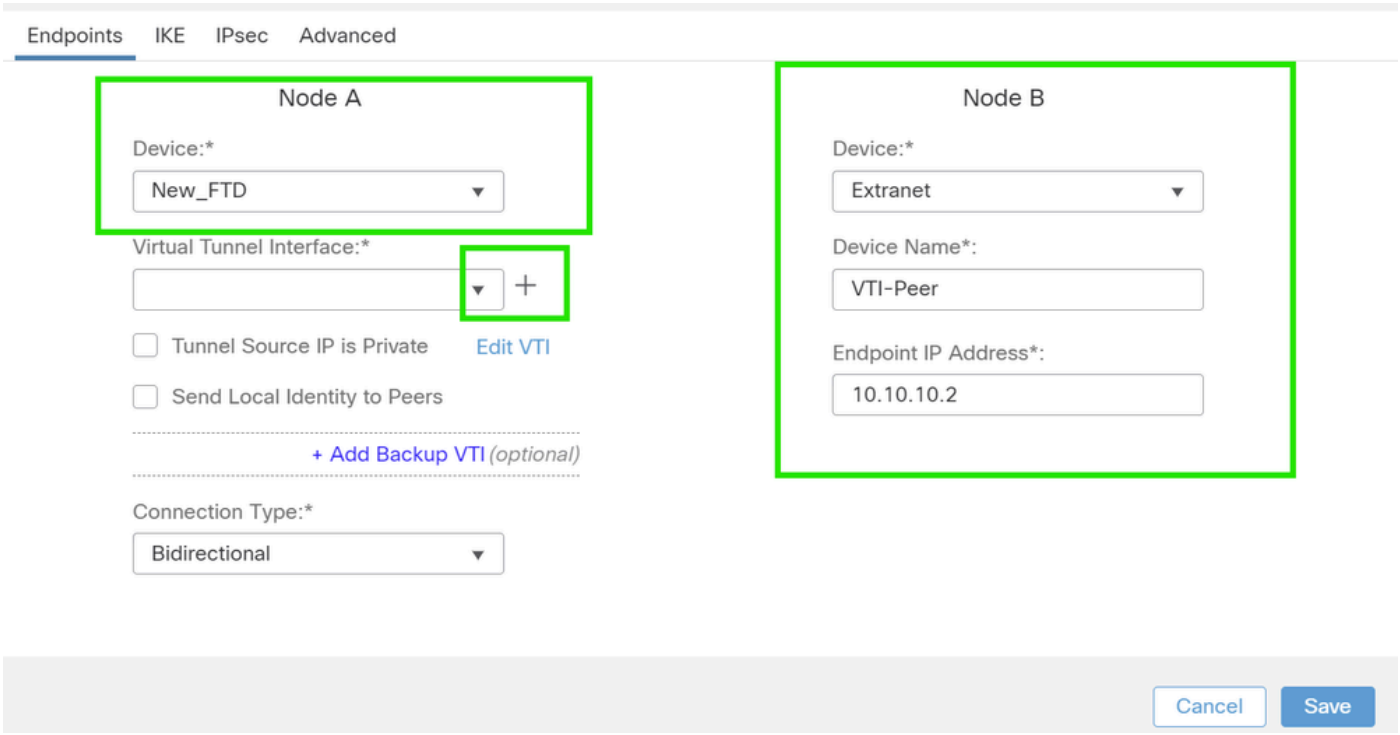
3. Donnez un nom à la topologie, choisissez VTI et Point-to-Point, puis sélectionnez une version IKE (IKEv2 dans ce cas).

Configuration des terminaux

1. Choisissez le périphérique sur lequel le tunnel doit être configuré.

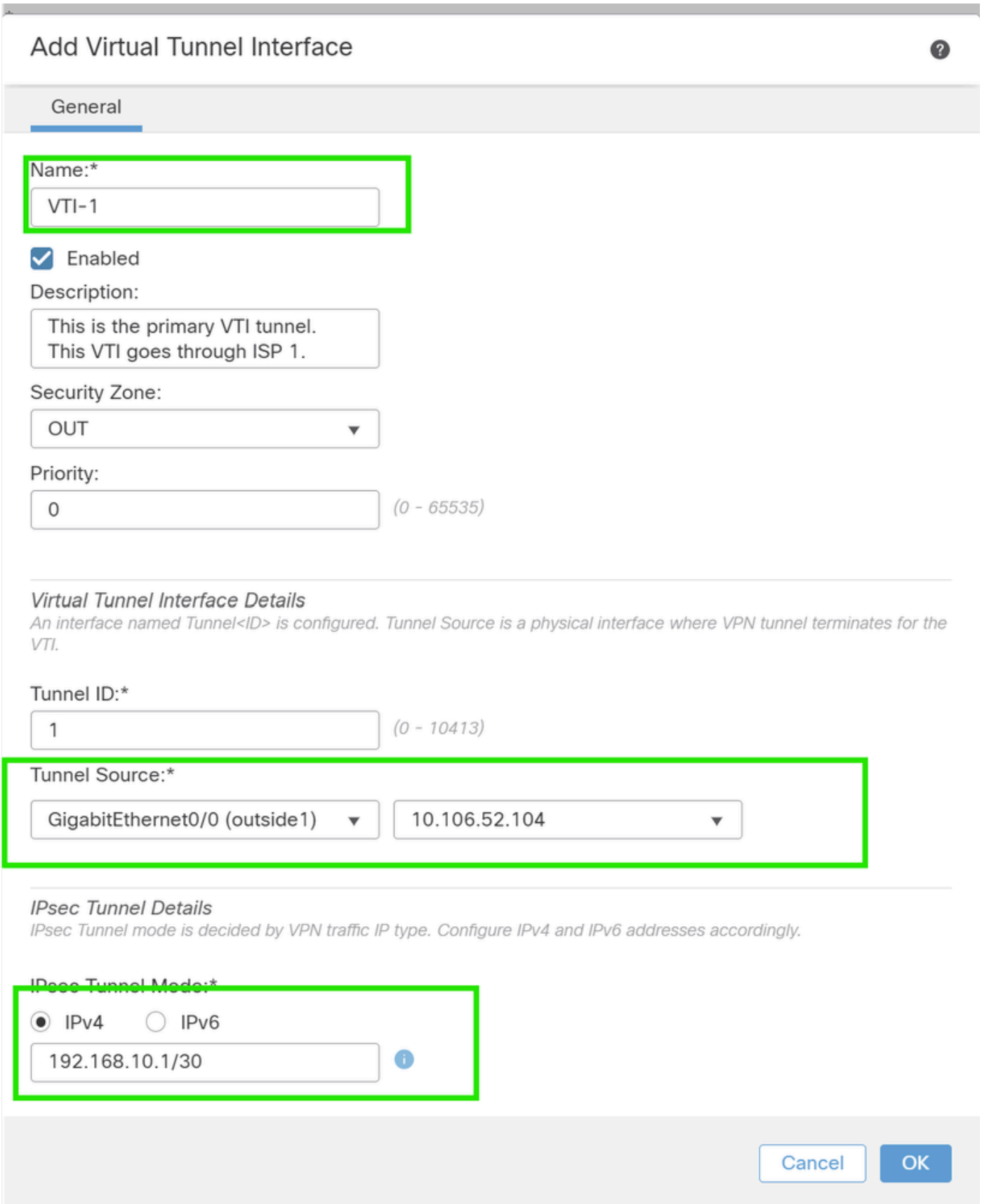
Ajoutez les détails de l'homologue distant.

Vous pouvez ajouter une nouvelle interface de modèle virtuel en cliquant sur l'icône "+" ou en sélectionner une dans la liste existante.

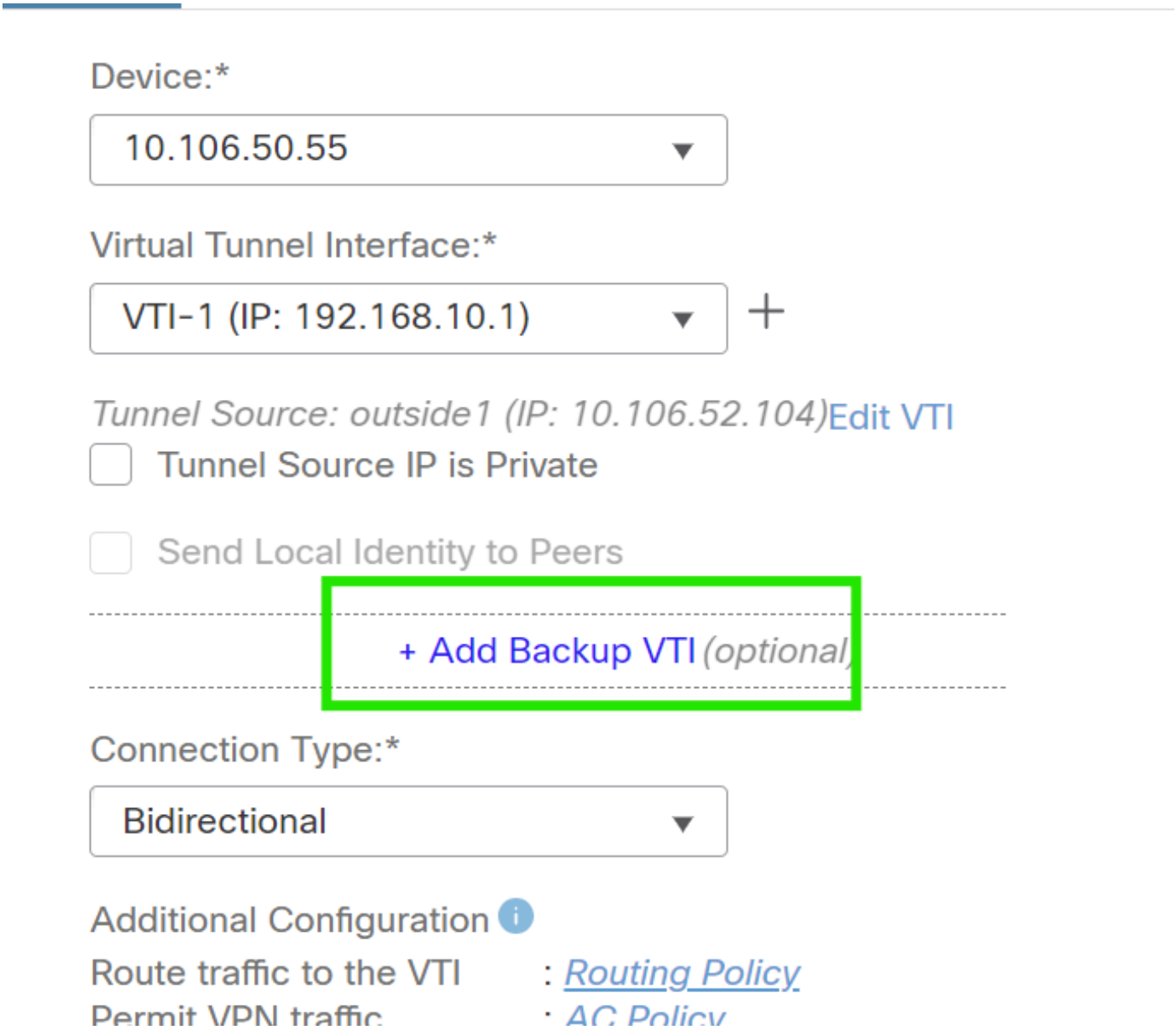


Si vous créez une nouvelle interface VTI, ajoutez les paramètres appropriés, activez-la et cliquez sur « OK ».

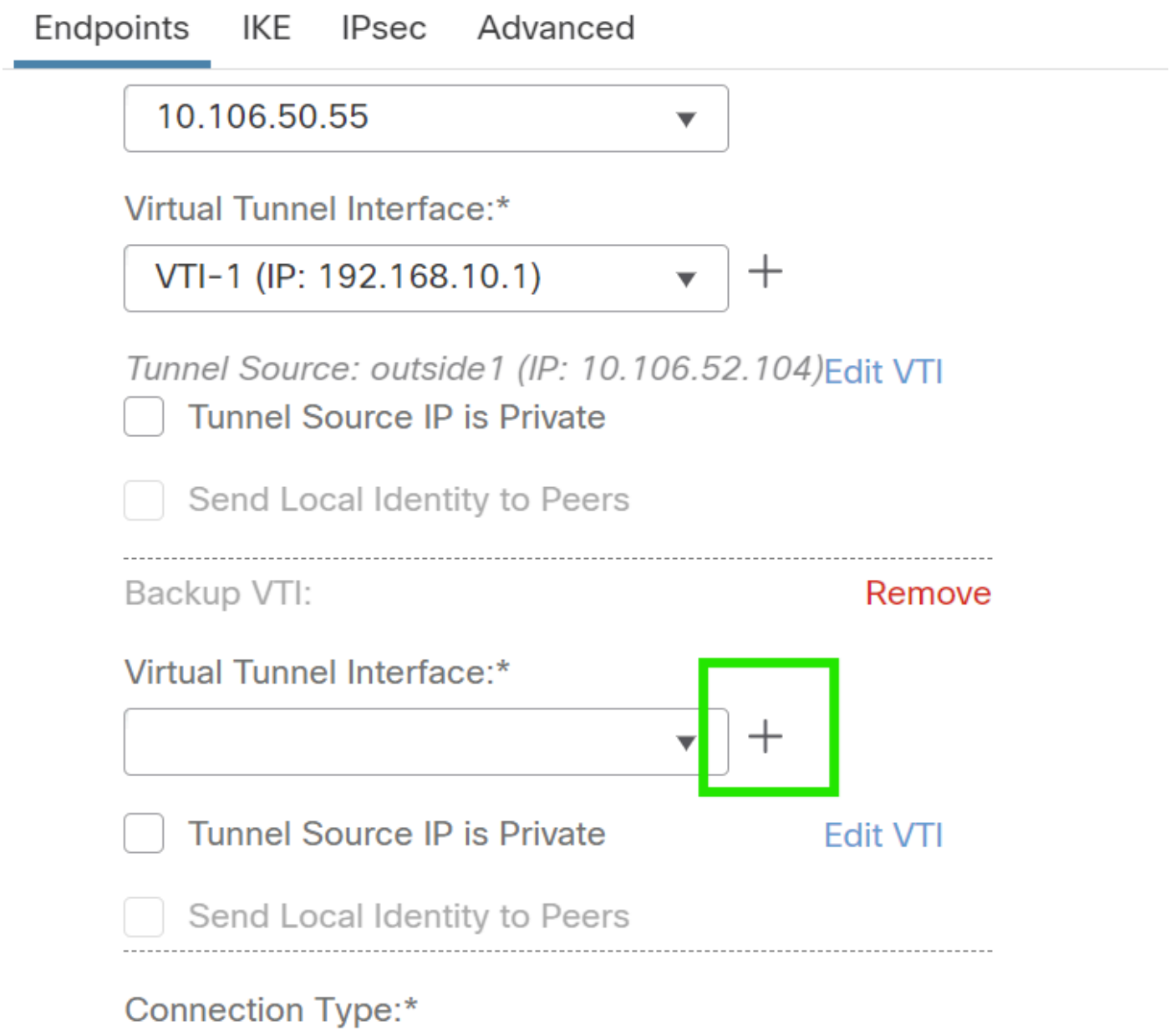
REMARQUE : il s'agit de la VTI principale.



3. Cliquez sur "+ ". Add Backup VIT" pour ajouter une VIT secondaire.

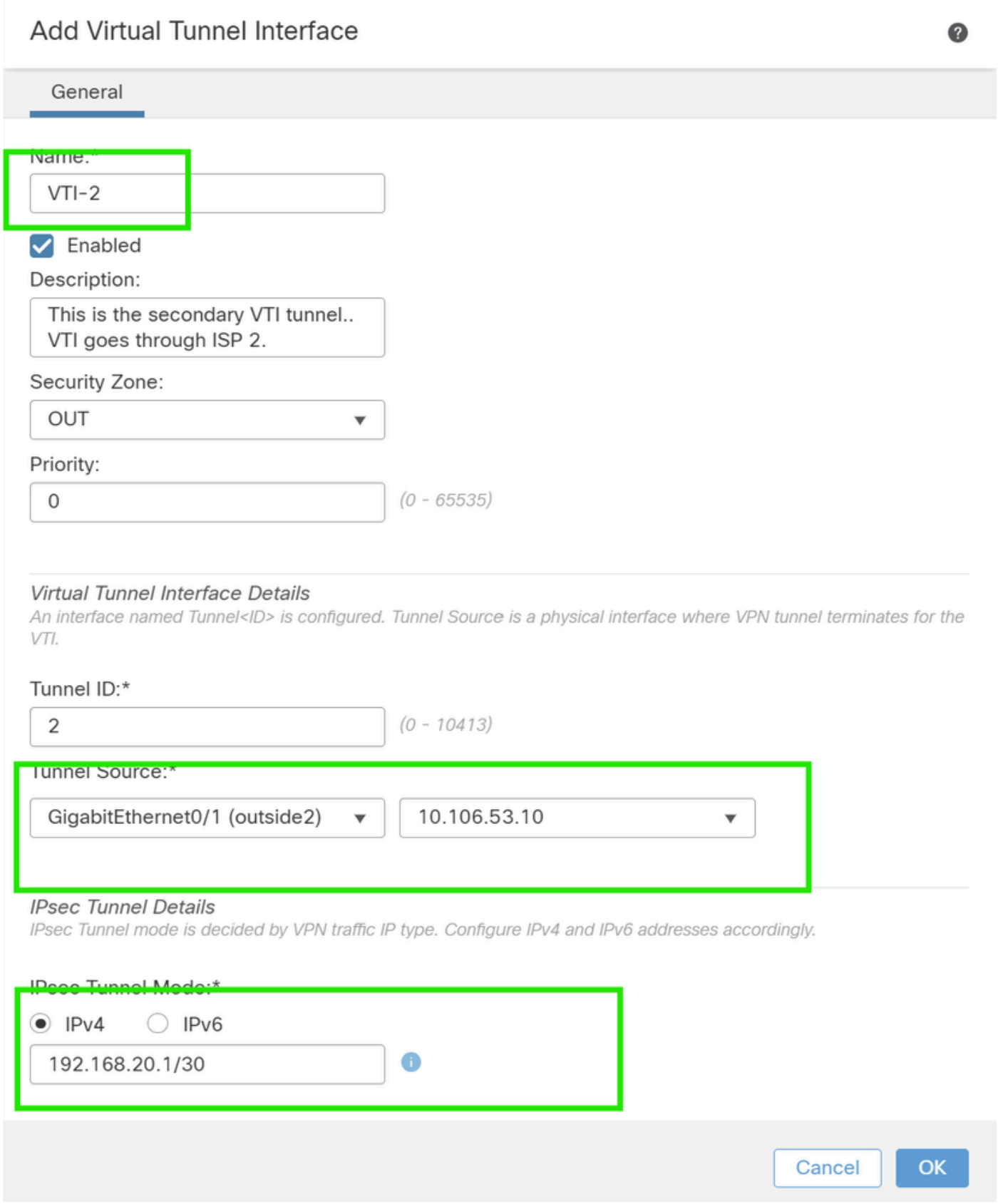


4. Cliquez sur "+" pour ajouter un paramètre pour le VTI secondaire (s'il n'est pas déjà configuré).



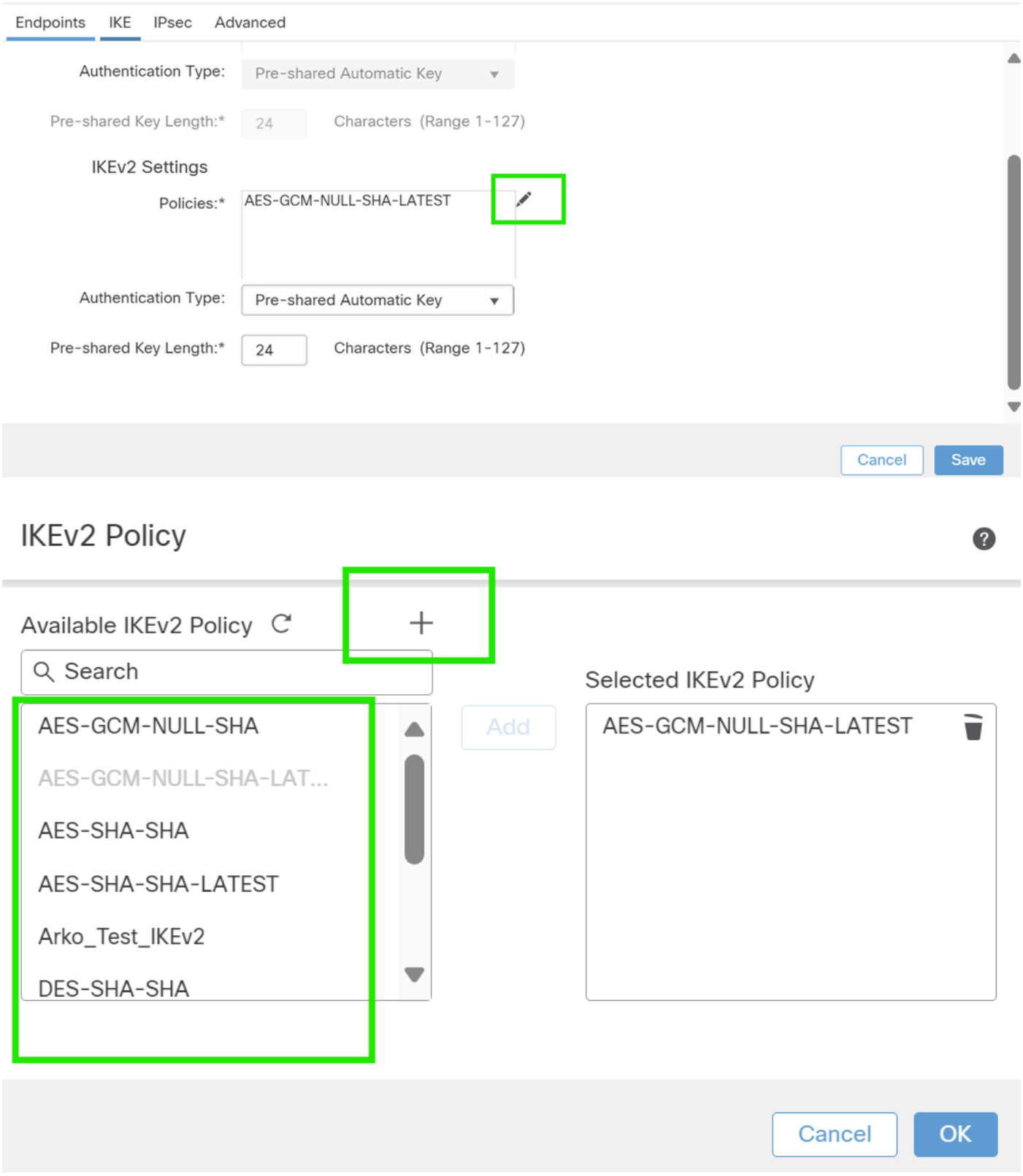
5. Si vous créez une nouvelle interface VTI, ajoutez les paramètres appropriés, activez-la et cliquez sur « OK ».

REMARQUE : devient la VTI secondaire.

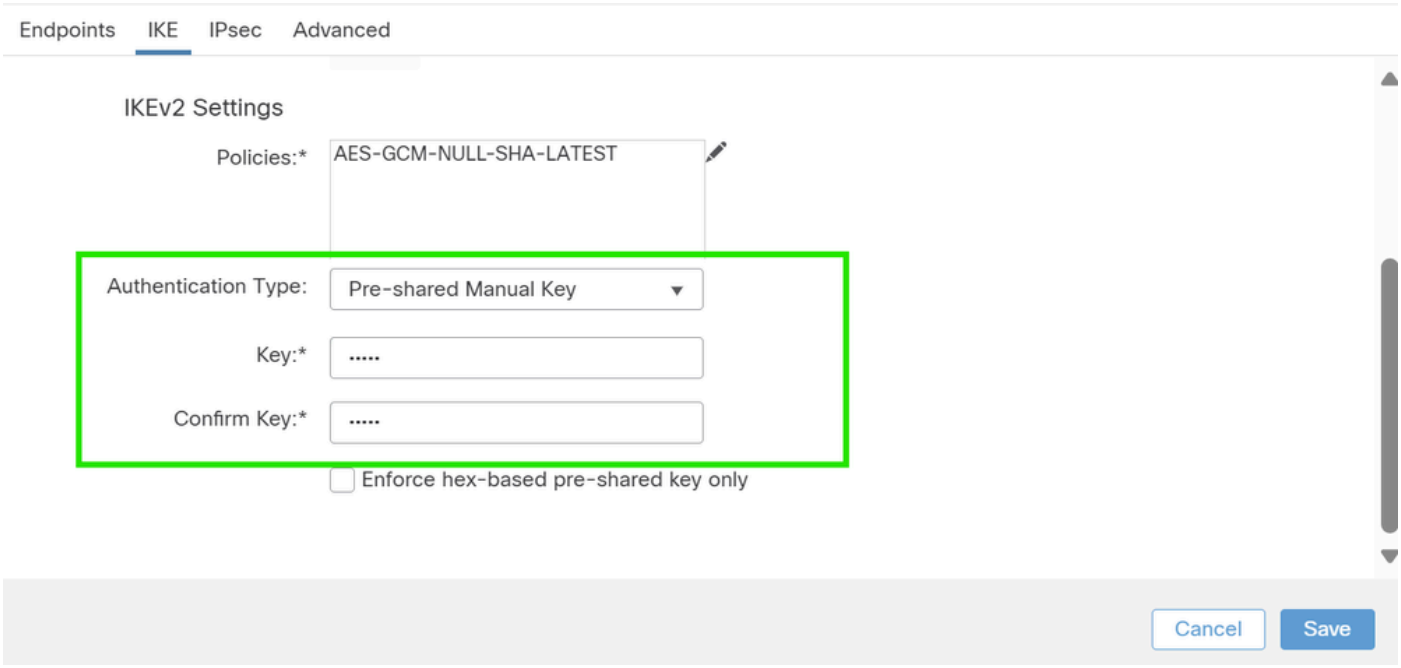


Configuration IKE

1. Accédez à l'onglet IKE. Vous pouvez choisir d'utiliser une stratégie prédéfinie ou cliquer sur le bouton représentant un crayon en regard de l'onglet Stratégie pour en créer une nouvelle ou sélectionner une autre stratégie disponible en fonction de vos besoins.

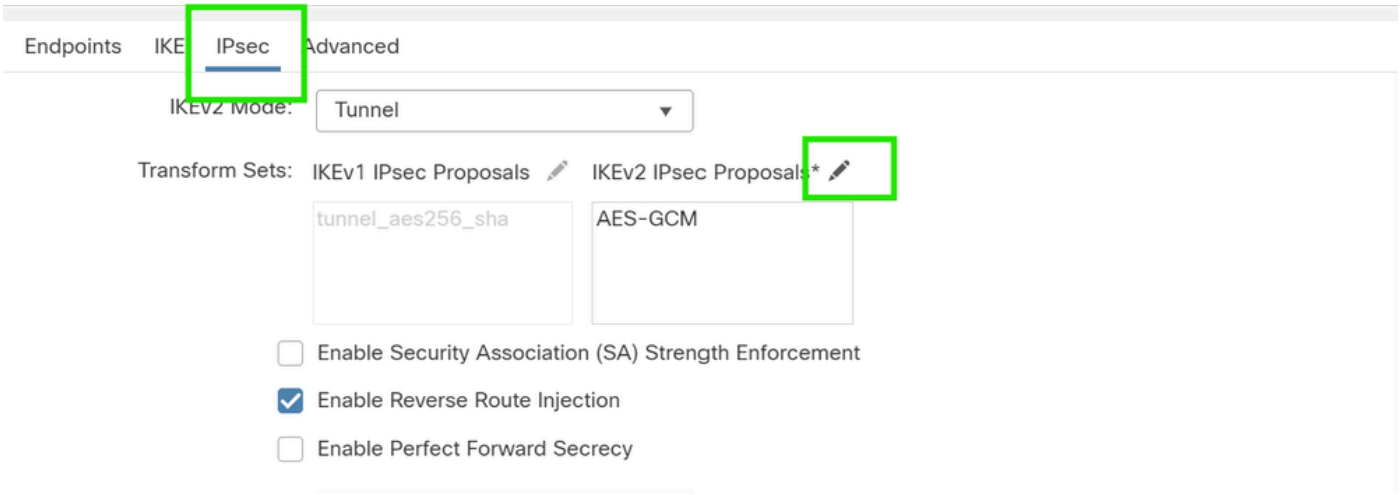


2. Sélectionnez le type d'authentification. Si une clé manuelle pré-partagée est utilisée, fournissez-la dans les zones Clé et Confirmer la clé.



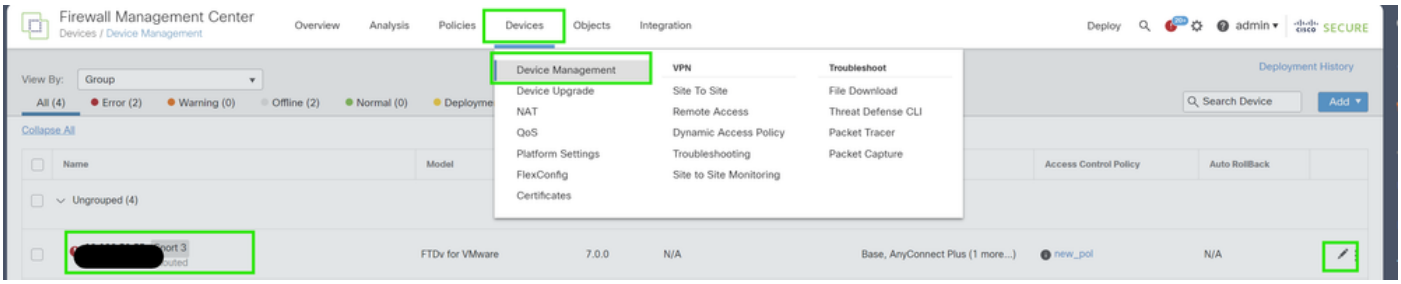
Configuration IPsec

Accédez à l'onglet IPsec. Vous pouvez choisir d'utiliser une proposition prédéfinie en cliquant sur le bouton crayon situé en regard de l'onglet Proposition pour en créer une nouvelle ou en sélectionner une autre en fonction de vos besoins.



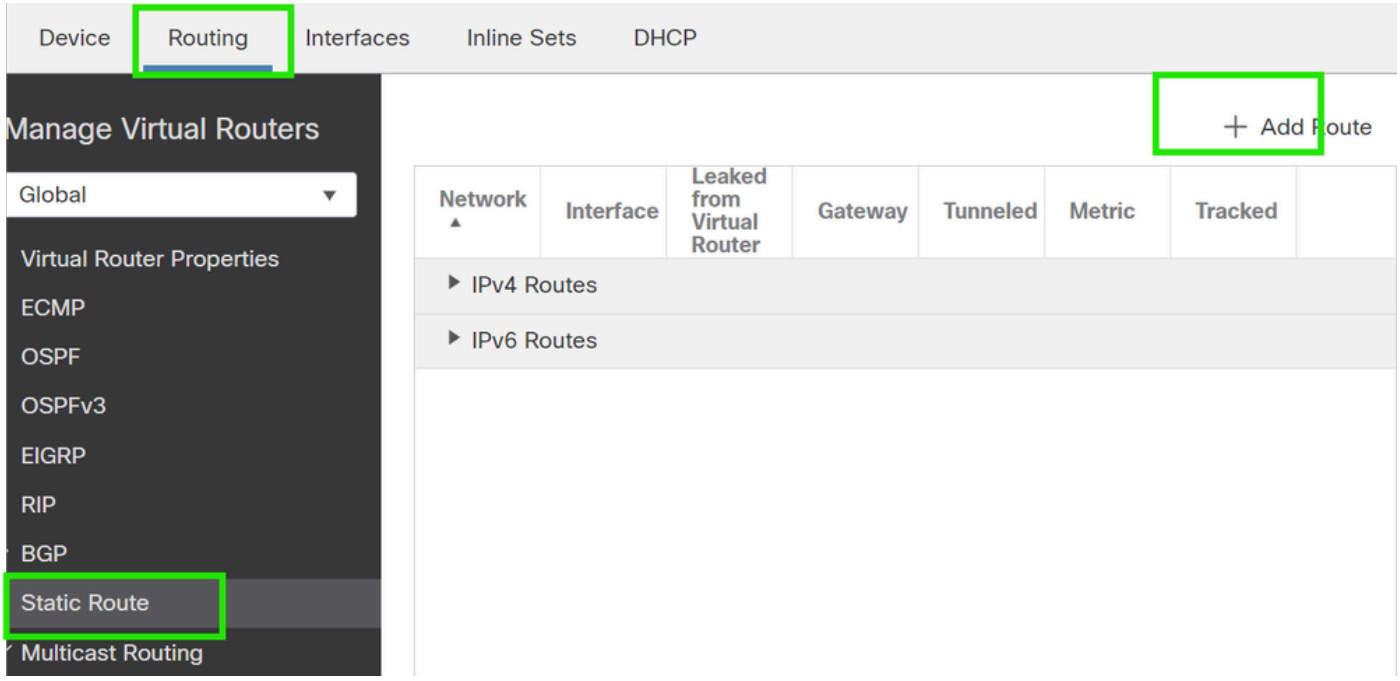
Configuration du routage

1. Accédez à Device > Device Management et cliquez sur l'icône du crayon pour modifier le périphérique (FTD).



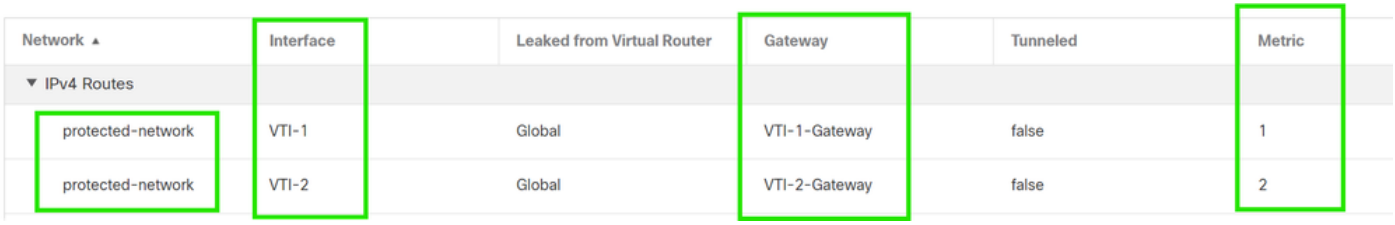
2. Accédez à Routing > Static Route et cliquez sur le bouton "+" pour ajouter une route à l'interface VTI principale et secondaire.

REMARQUE : Vous pouvez configurer la méthode de routage appropriée pour que votre trafic passe par l'interface du tunnel. Dans ce cas, des routes statiques ont été utilisées.



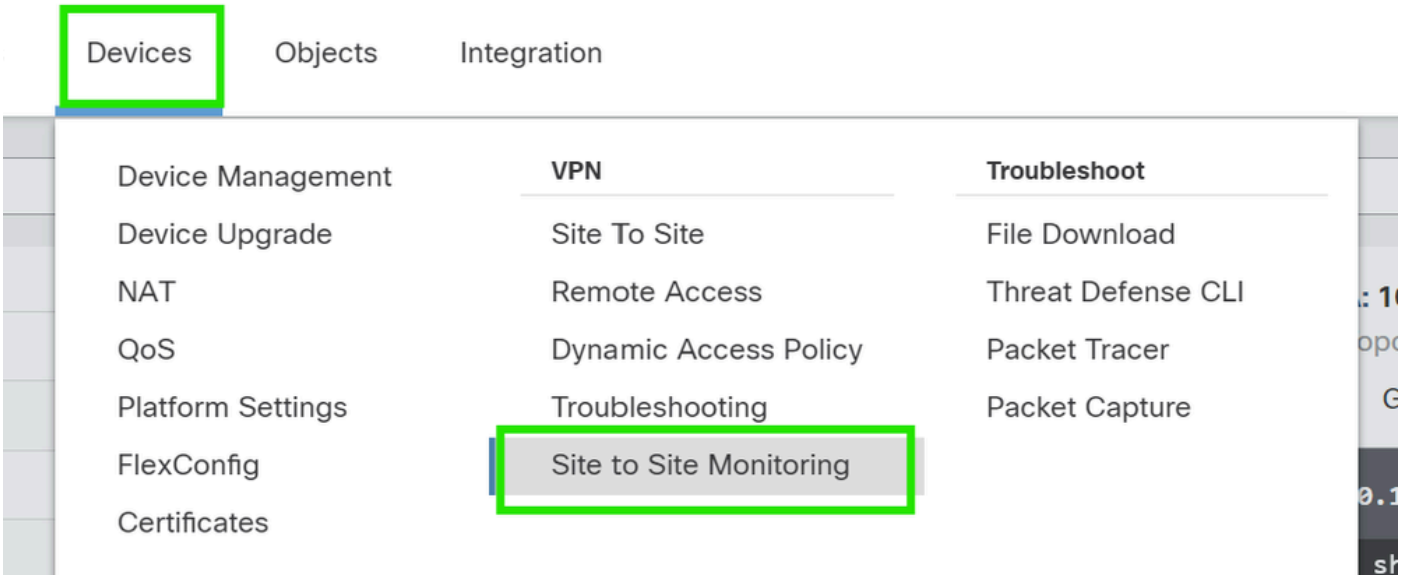
3. Ajoutez deux routes pour votre réseau protégé et définissez une valeur de distance administrative plus élevée (dans ce cas 2) pour la route secondaire.

La première route utilise l'interface VTI-1 et la seconde l'interface VTI-2.

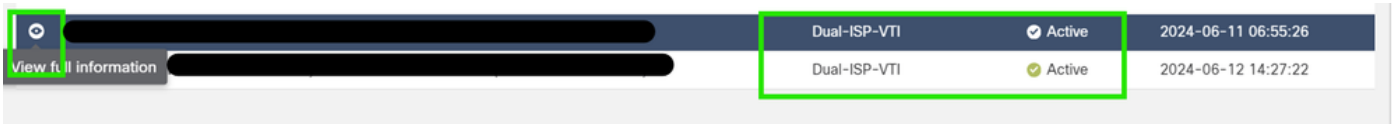


Vérifier

1. Accédez à Devices > VPN > Site to Site Monitoring .



2. Cliquez sur l'oeil pour vérifier plus de détails sur l'état du tunnel.



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.