Configurer un VPN basé sur la route avec une route statique sur FTD gérée par FDM

Table des matières

Introduction

Ce document décrit comment configurer un tunnel VPN de site à site basé sur une route statique sur un FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du fonctionnement d'un tunnel VPN.
- Connaissances préalables de la navigation dans Firepower Device Manager (FDM).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

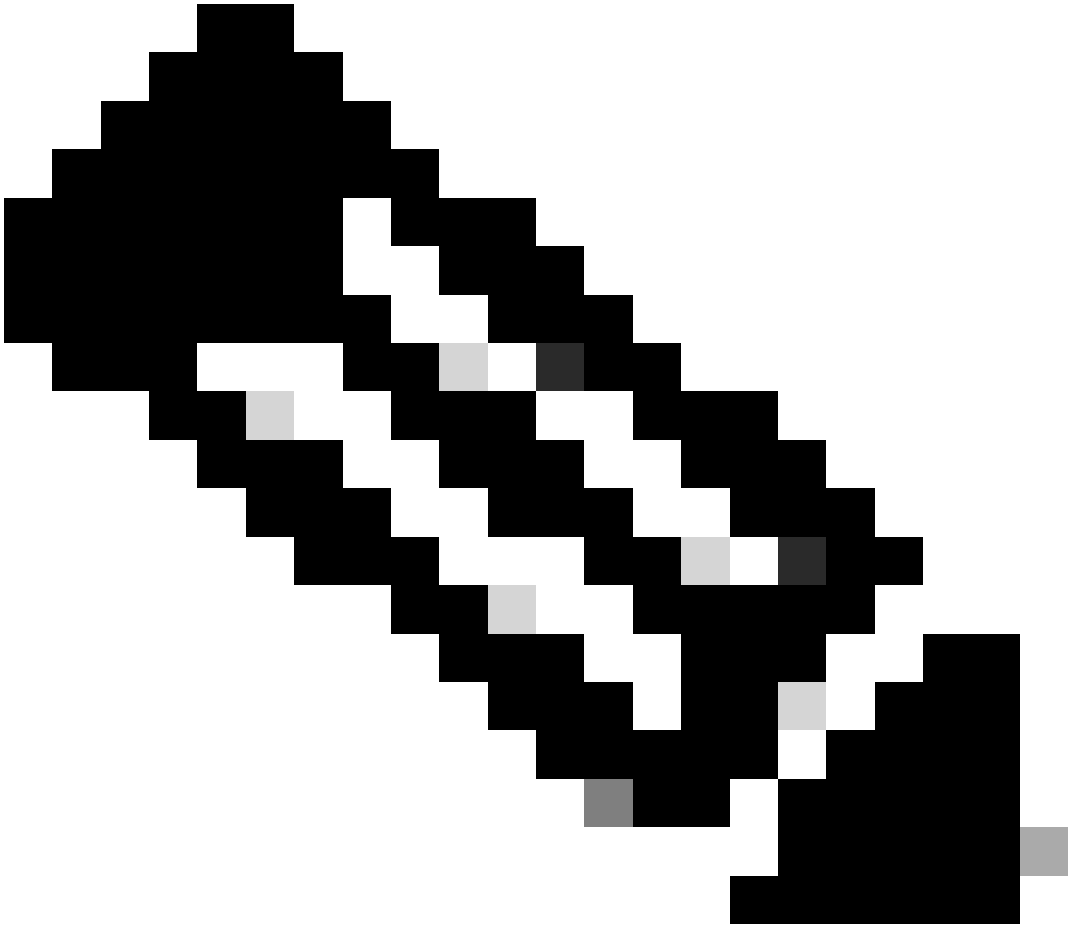
- Cisco Firepower Threat Defense (FTD) version 7.0 géré par Firepower Device Manager (FDM).

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.

Informations générales

Le VPN basé sur la route permet de déterminer le trafic intéressant à chiffrer, ou à envoyer sur le tunnel VPN, et d'utiliser le routage du trafic au lieu de la politique/liste d'accès comme dans le VPN basé sur la politique ou la crypto-carte. Le domaine de chiffrement est configuré pour autoriser tout trafic qui entre dans le tunnel IPsec. Les sélecteurs de trafic local et distant IPsec sont définis sur 0.0.0.0/0.0.0.0. Cela signifie que tout trafic acheminé dans le tunnel IPsec est chiffré quel que soit le sous-réseau source/de destination.

Ce document se concentre sur la configuration de l'interface SVTI (Static Virtual Tunnel Interface).



> Remarque : Aucune licence supplémentaire n'est nécessaire, le VPN basé sur la route peut être configuré en mode sous licence ainsi qu'en mode d'évaluation. Sans la conformité du chiffrement (fonctionnalités d'exportation contrôlée activées), seul DES peut être utilisé comme algorithme de chiffrement.

Étapes de configuration sur FDM

Étape 1. Accédez à Périphérique > Site à site.

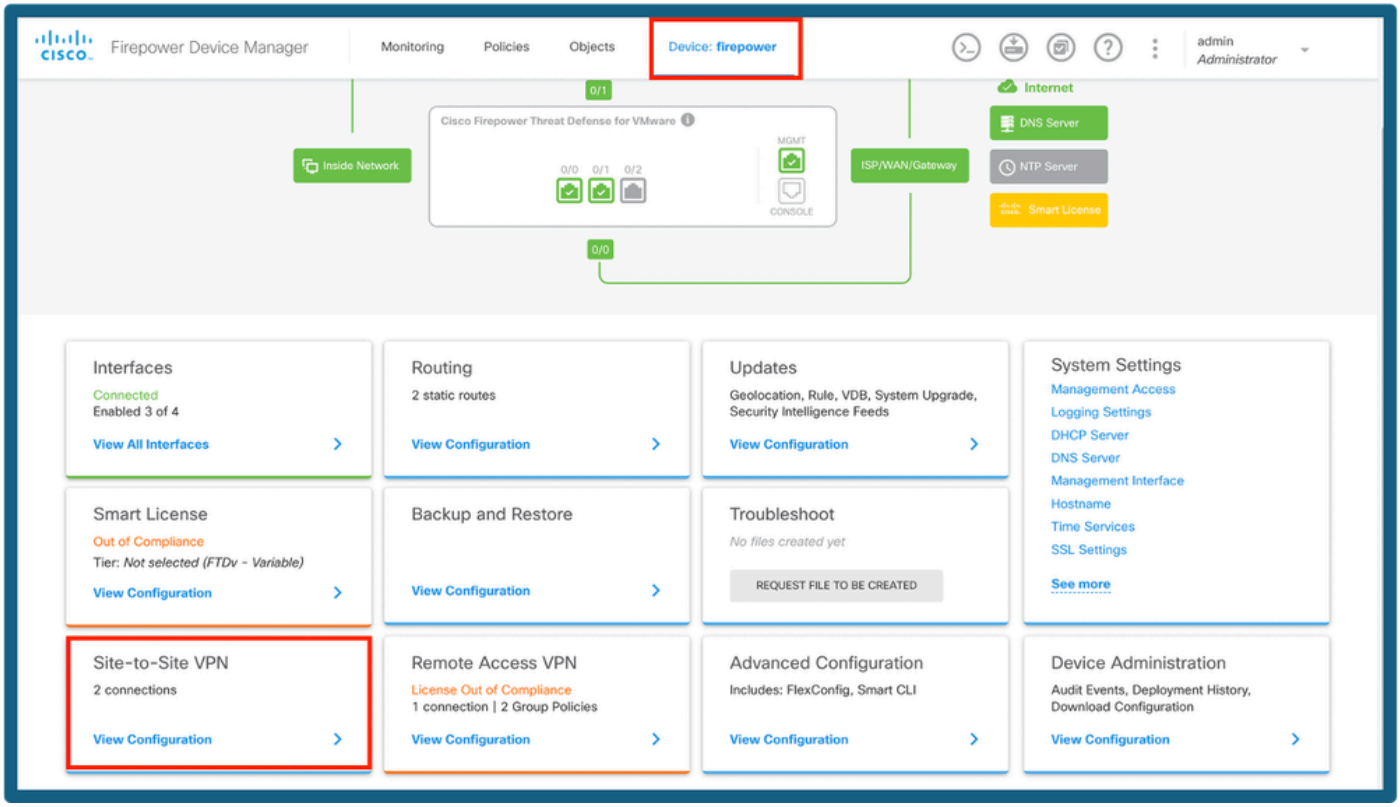
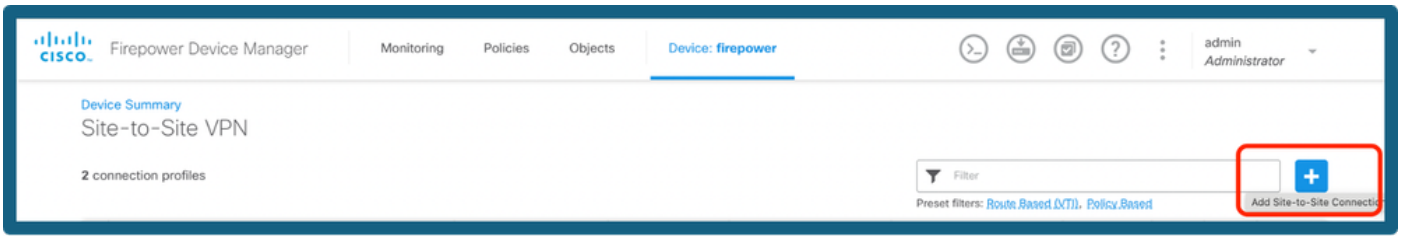


Tableau de bord FDM

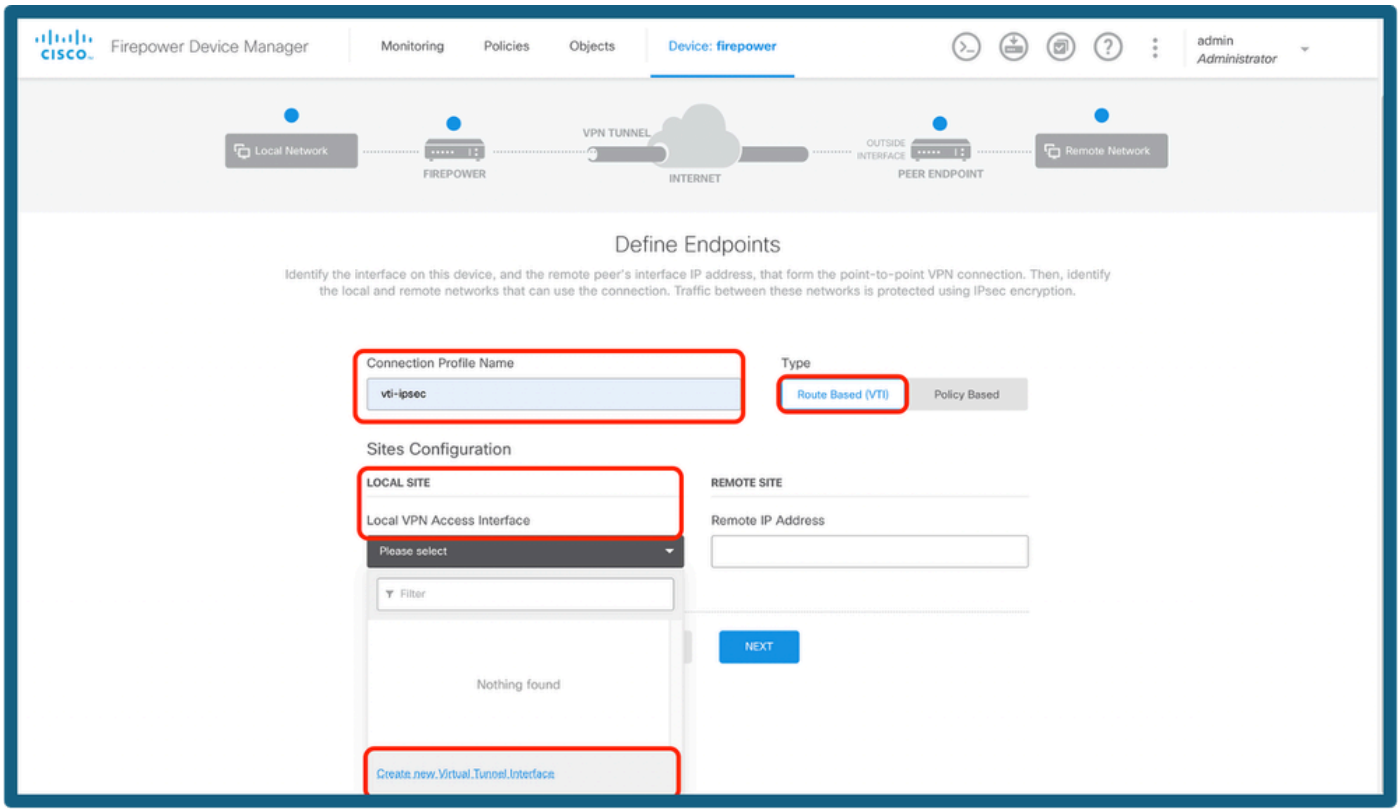
Étape 2. Cliquez sur l'icône + pour ajouter une connexion de site à site.



Ajouter une connexion S2S

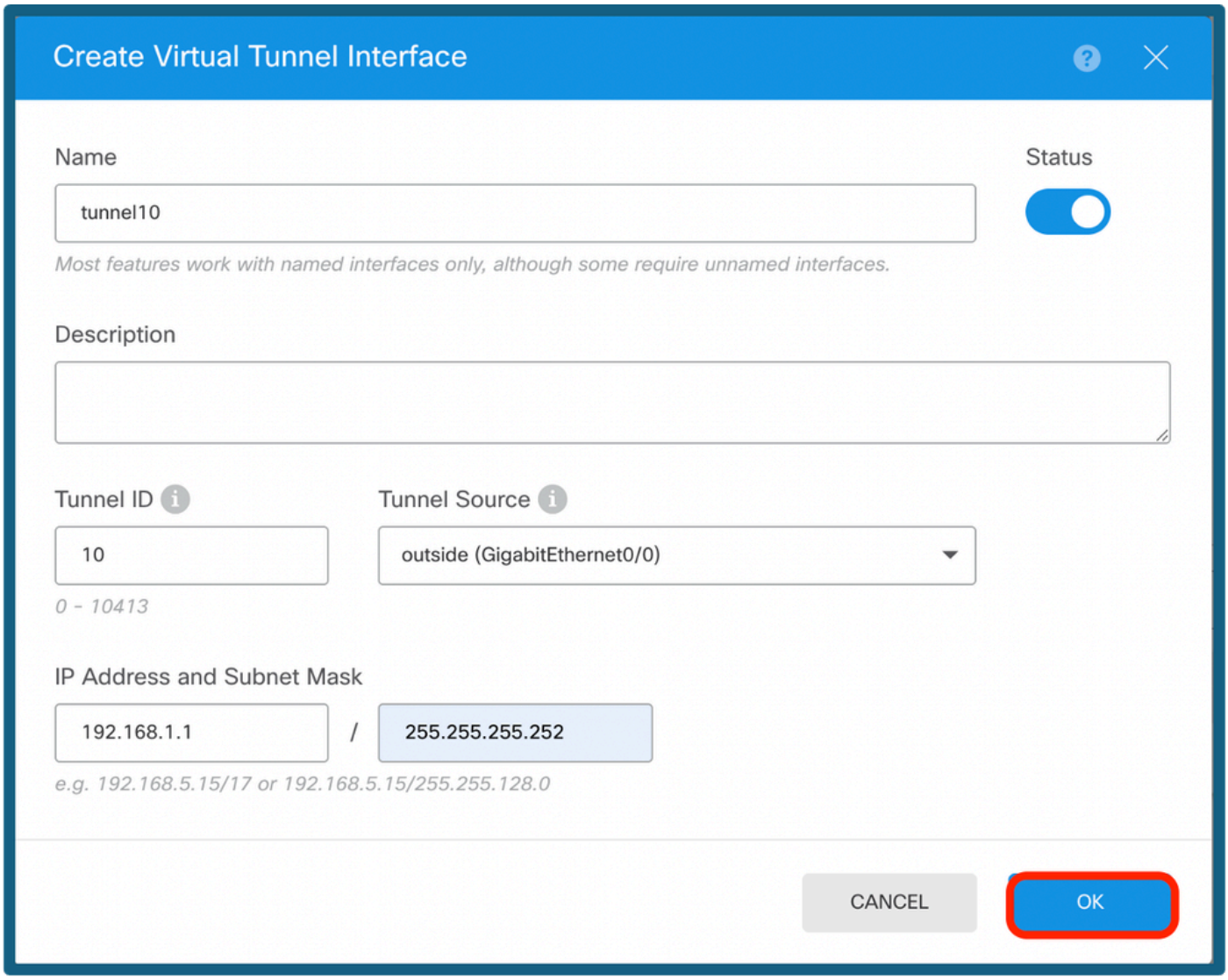
Étape 3. Fournissez un nom de topologie et sélectionnez le type de VPN comme VTI (Route Based).

Cliquez sur Local VPN Access Interface, puis cliquez sur Create new Virtual Tunnel Interface ou sélectionnez-en une dans la liste qui existe.



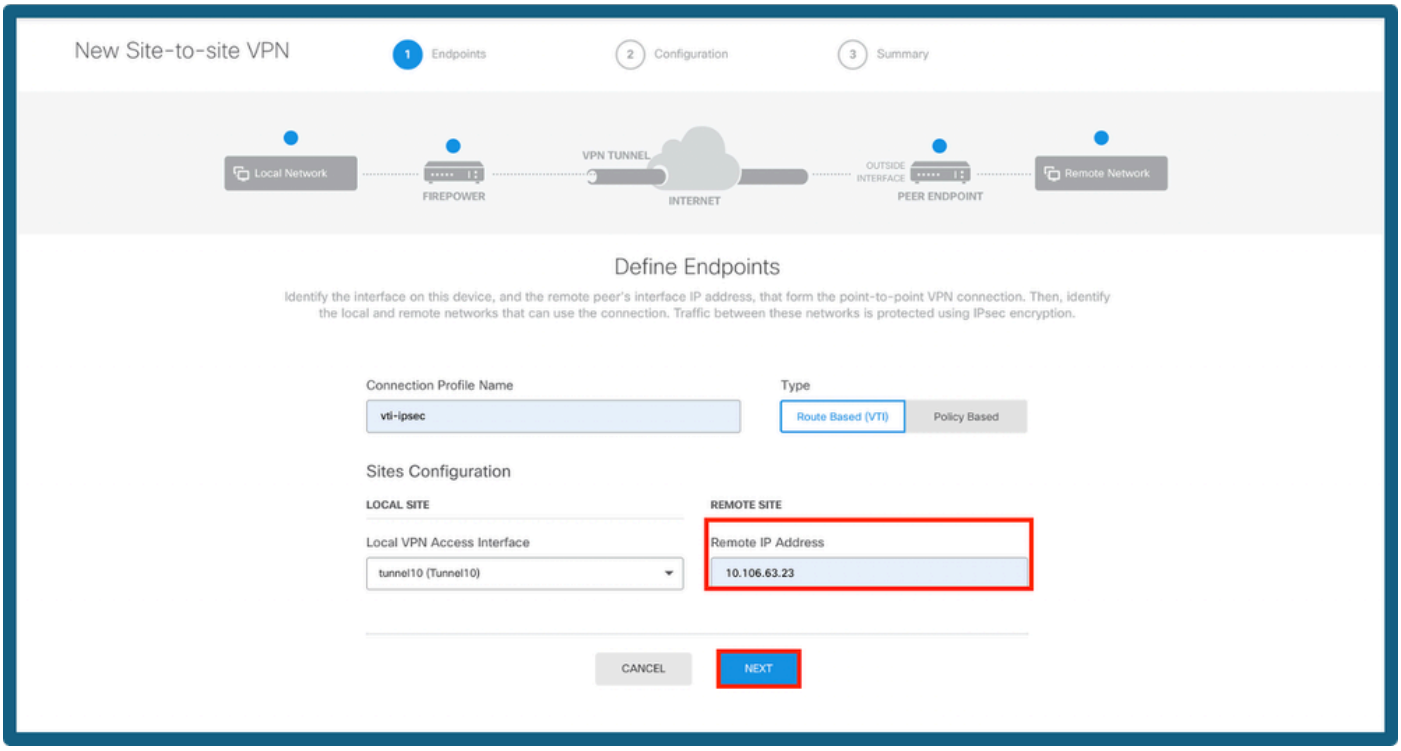
Ajouter une interface de tunnel

Étape 4 : définition des paramètres de la nouvelle interface de tunnel virtuel Click OK.



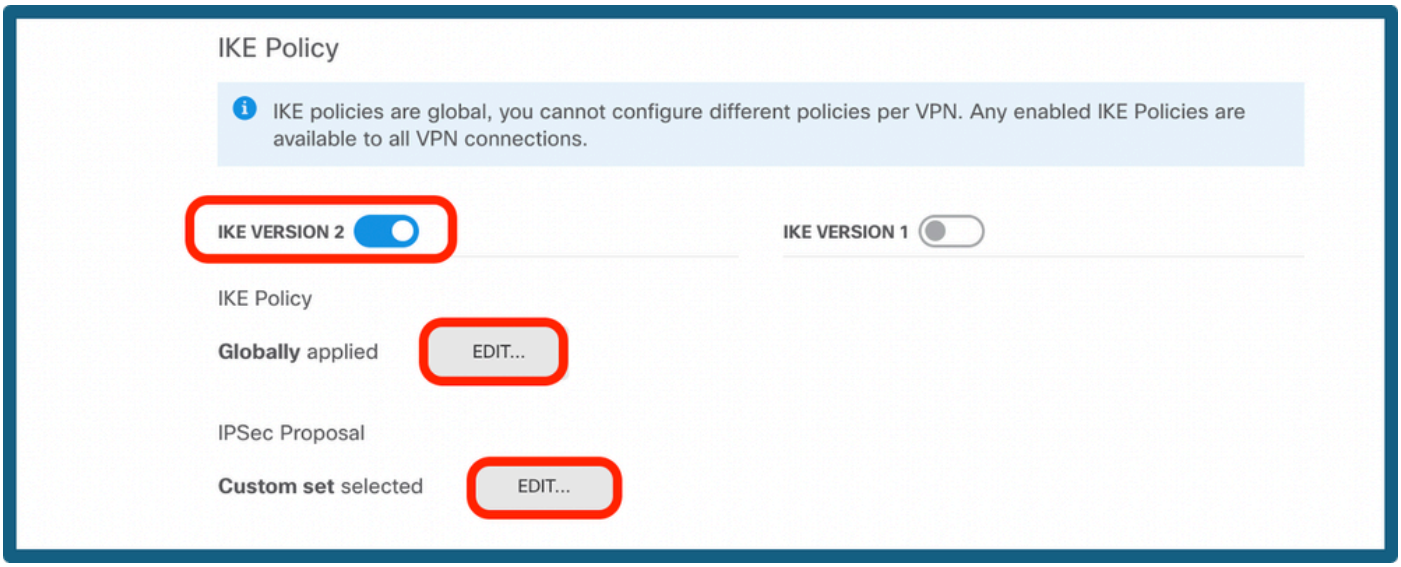
Configuration VTI

Étape 5. Choisissez le VTI nouvellement créé ou un VTI qui existe sous Virtual Tunnel Interface.Fournissez l'adresse IP distante.



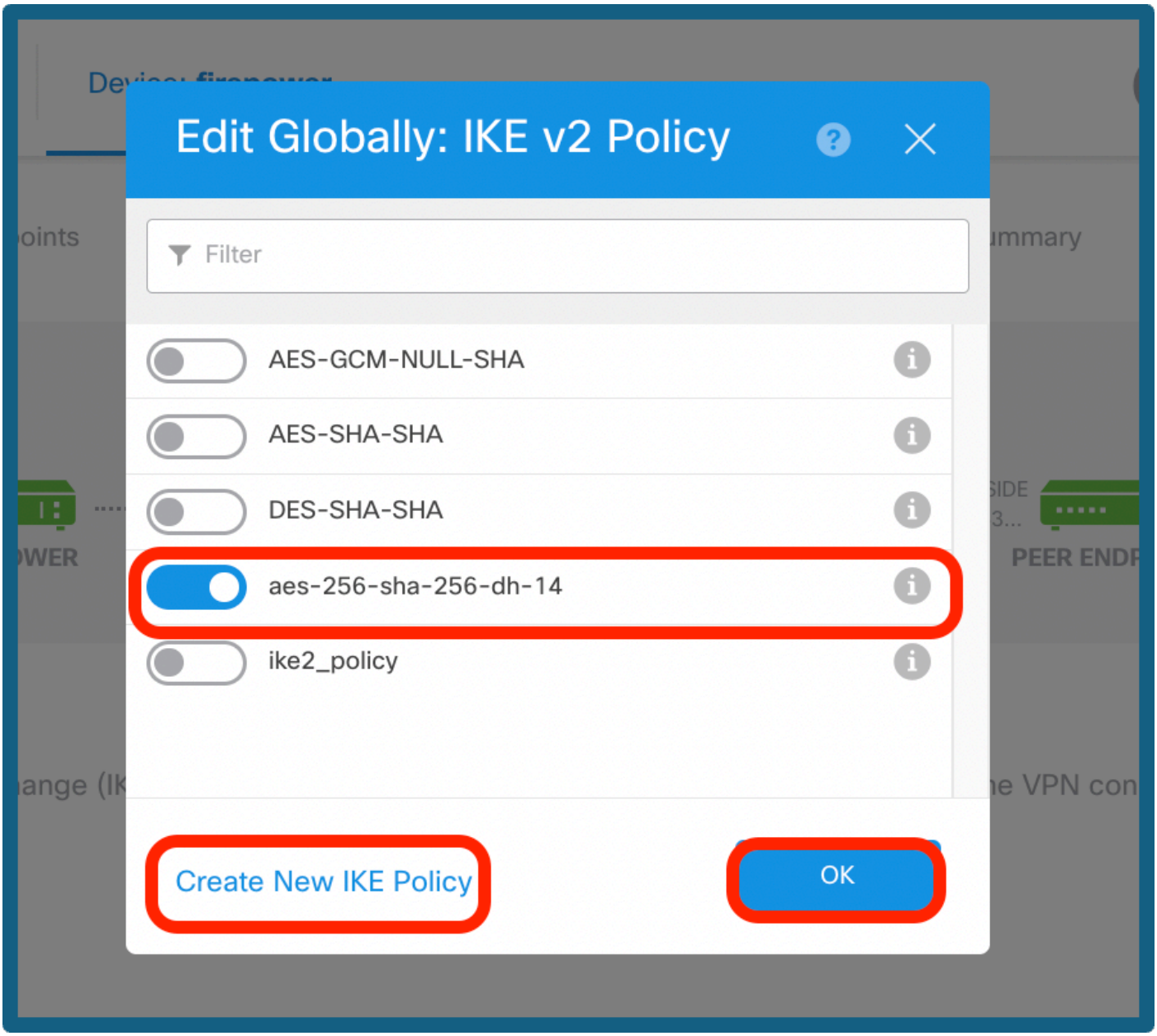
Ajouter une adresse IP homologue

Étape 6. Choisissez la version IKE et choisissez le bouton Edit pour définir les paramètres IKE et IPsec comme indiqué dans l'image.

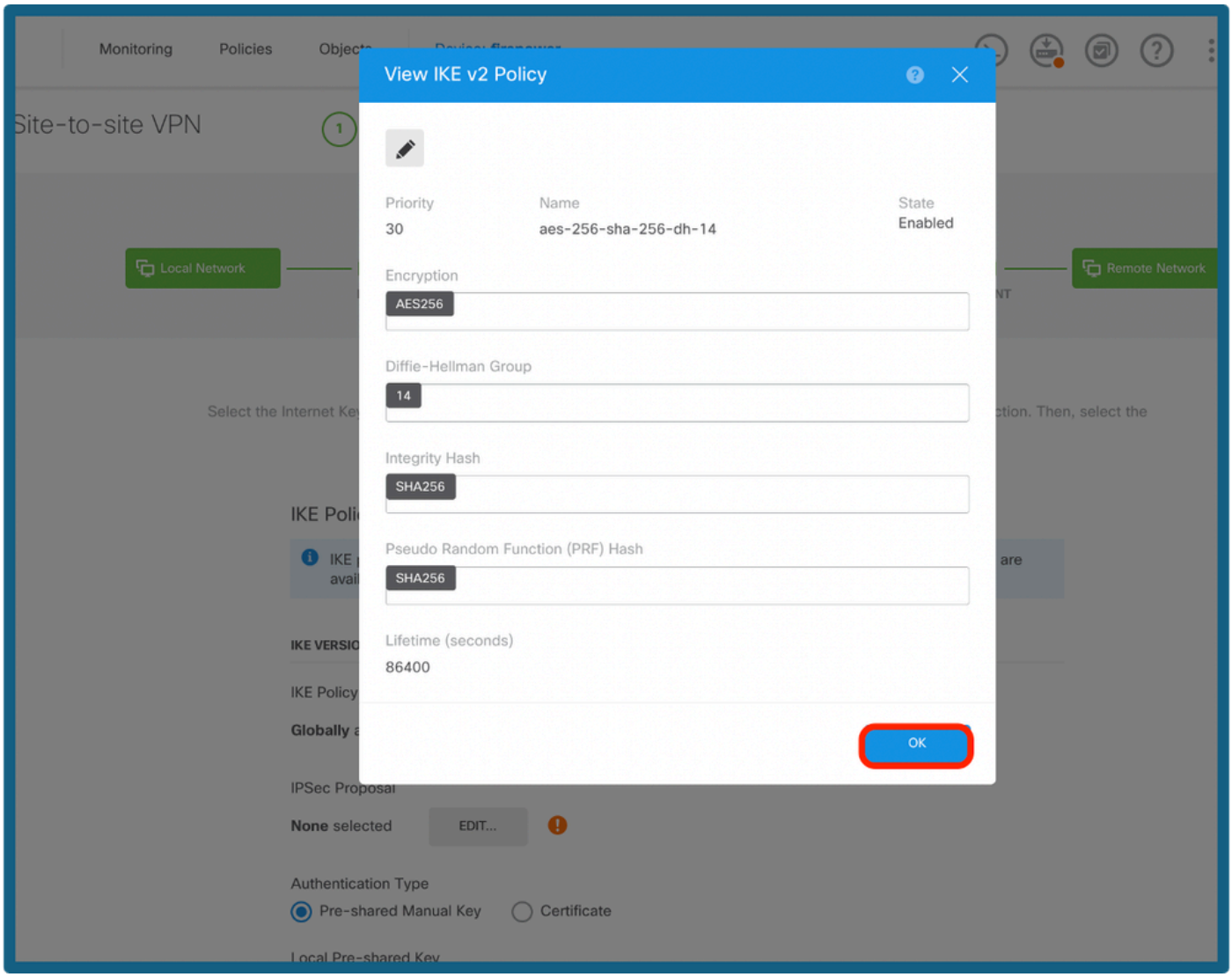


Configuration de la version IKE

Étape 7a. Choisissez le bouton IKE Policy comme illustré dans l'image et cliquez sur le bouton ok ou sur Create New IKE Policy, si vous souhaitez créer une nouvelle stratégie.

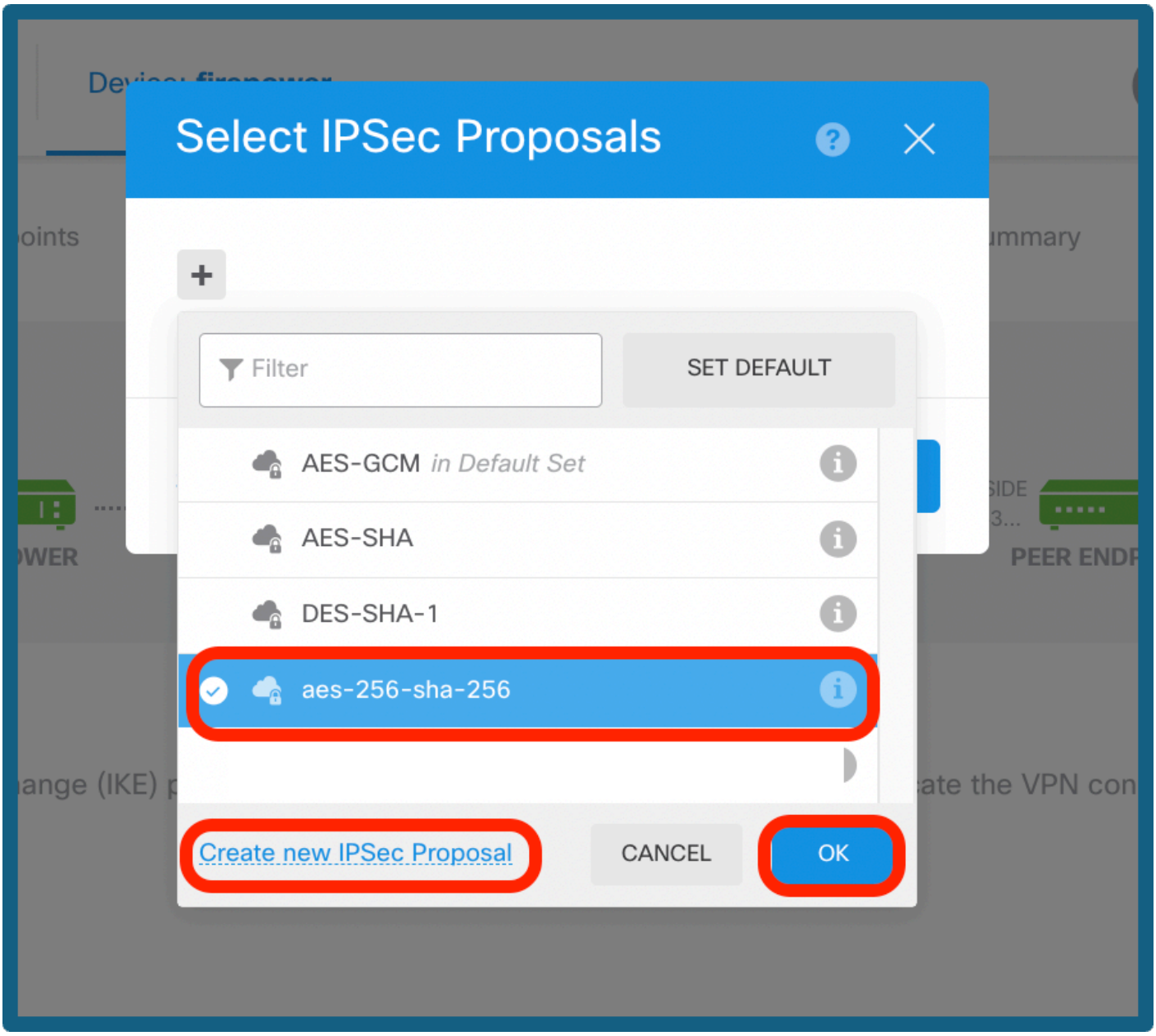


Choisir une stratégie IKE

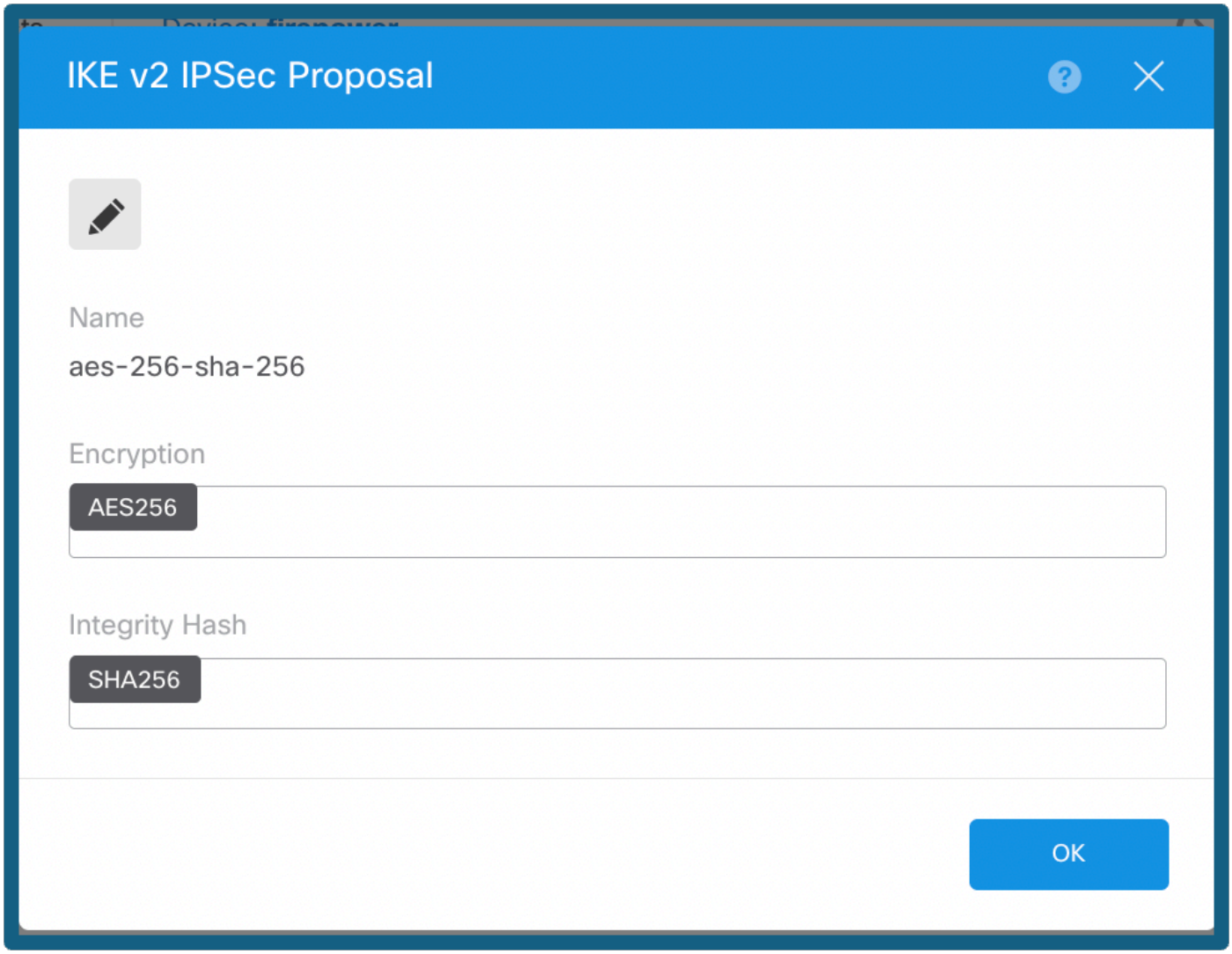


Configuration de la stratégie IKE

Étape 7b. Choisissez le bouton IPSec Policy comme indiqué dans l'image et cliquez sur le bouton ok ou sur Create New IPsec Proposal, si vous souhaitez créer une nouvelle proposition.



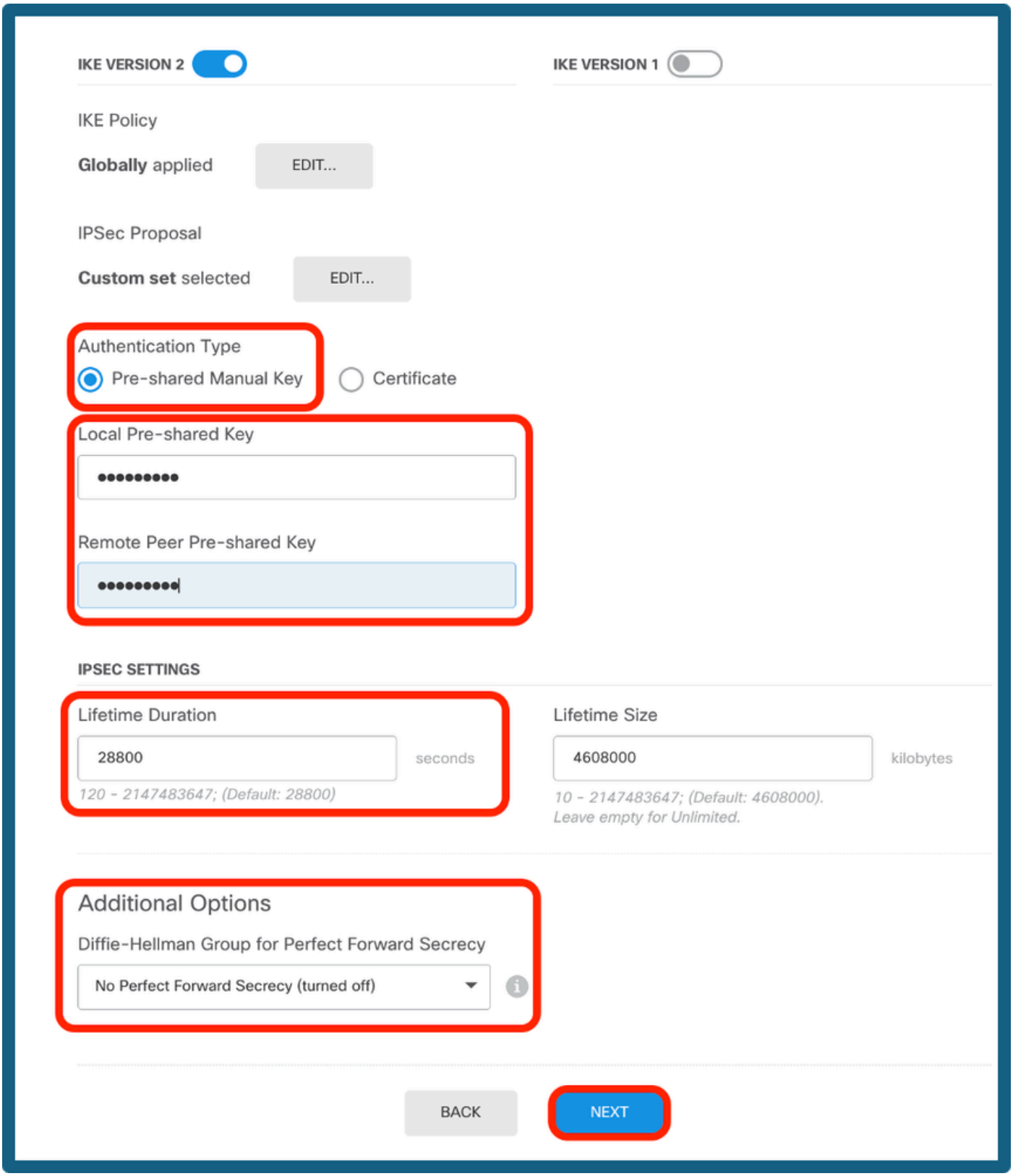
Sélectionner une proposition IPsec



Configuration de la proposition IPsec

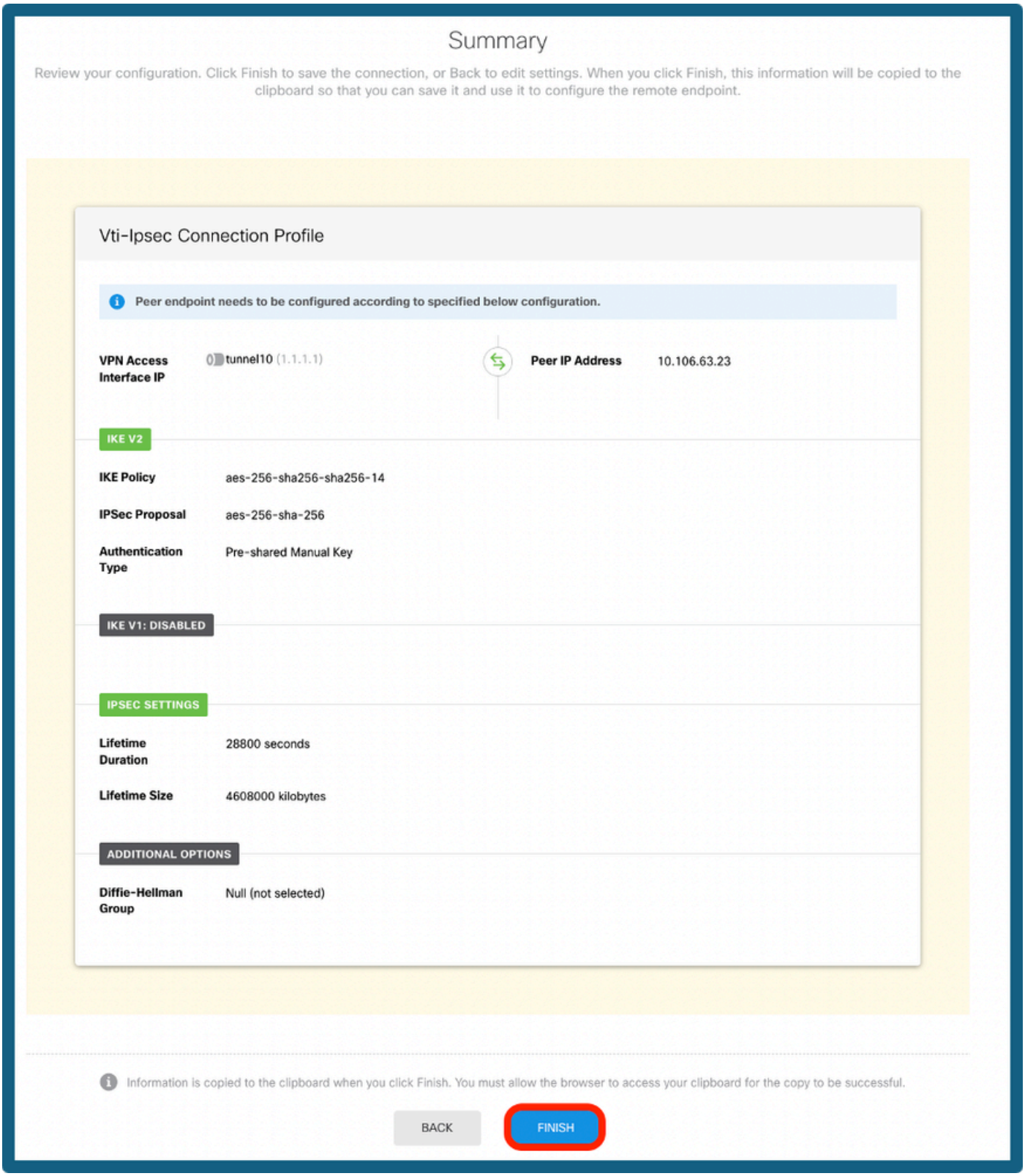
Étape 8a. Sélectionnez le type d'authentification. Si vous utilisez une clé manuelle pré-partagée, fournissez la clé pré-partagée locale et distante.

Étape 8b. (Facultatif) Sélectionnez les paramètres Perfect Forward Secrecy. Configurez la durée de vie et la taille de vie d'IPsec, puis cliquez sur Suivant.



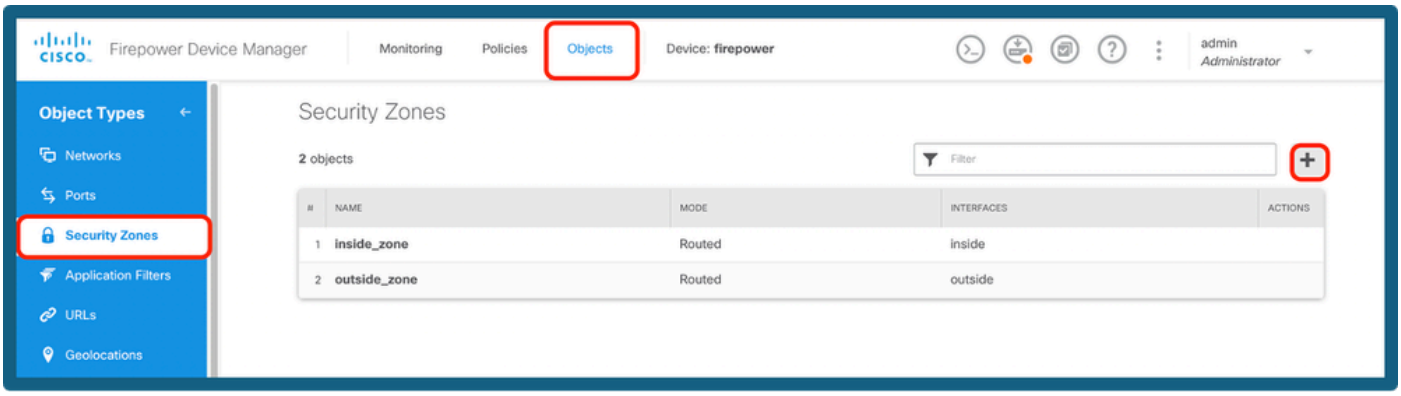
PSK et configuration à vie

Étape 9. Vérifiez la configuration et cliquez sur Finish.



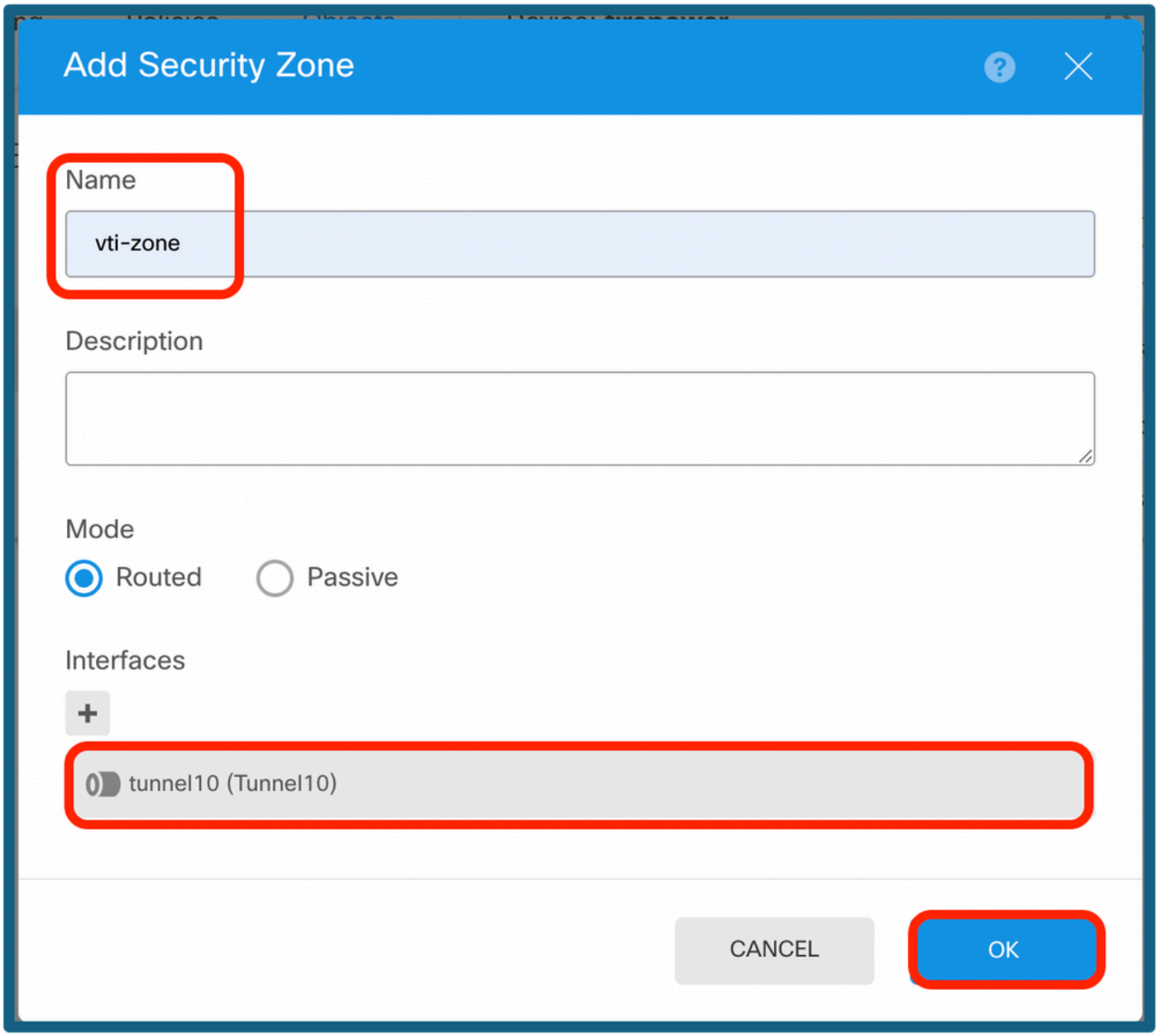
Résumé de la configuration

Étape 10a. Accédez à Objets > Zones de sécurité, puis cliquez sur l'icône +.



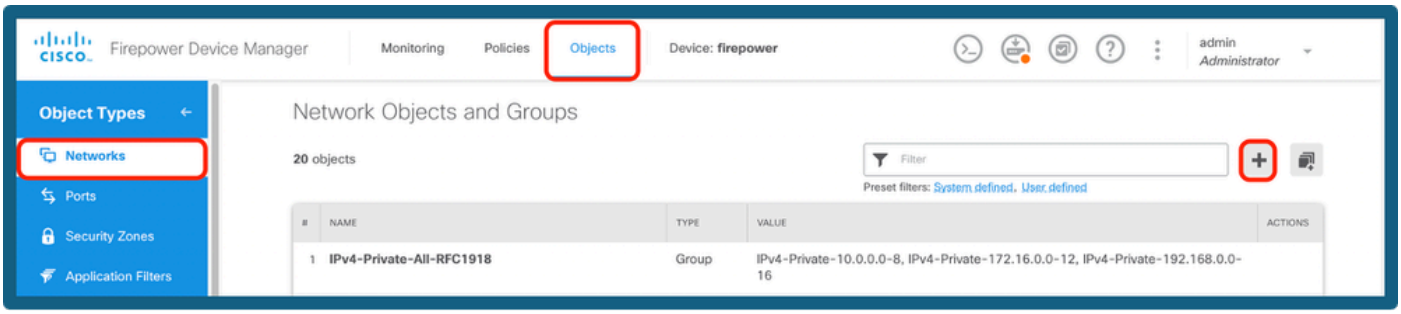
Ajouter une zone de sécurité

Étape 10b. Créez une zone et sélectionnez l'interface VTI comme indiqué ci-dessous.



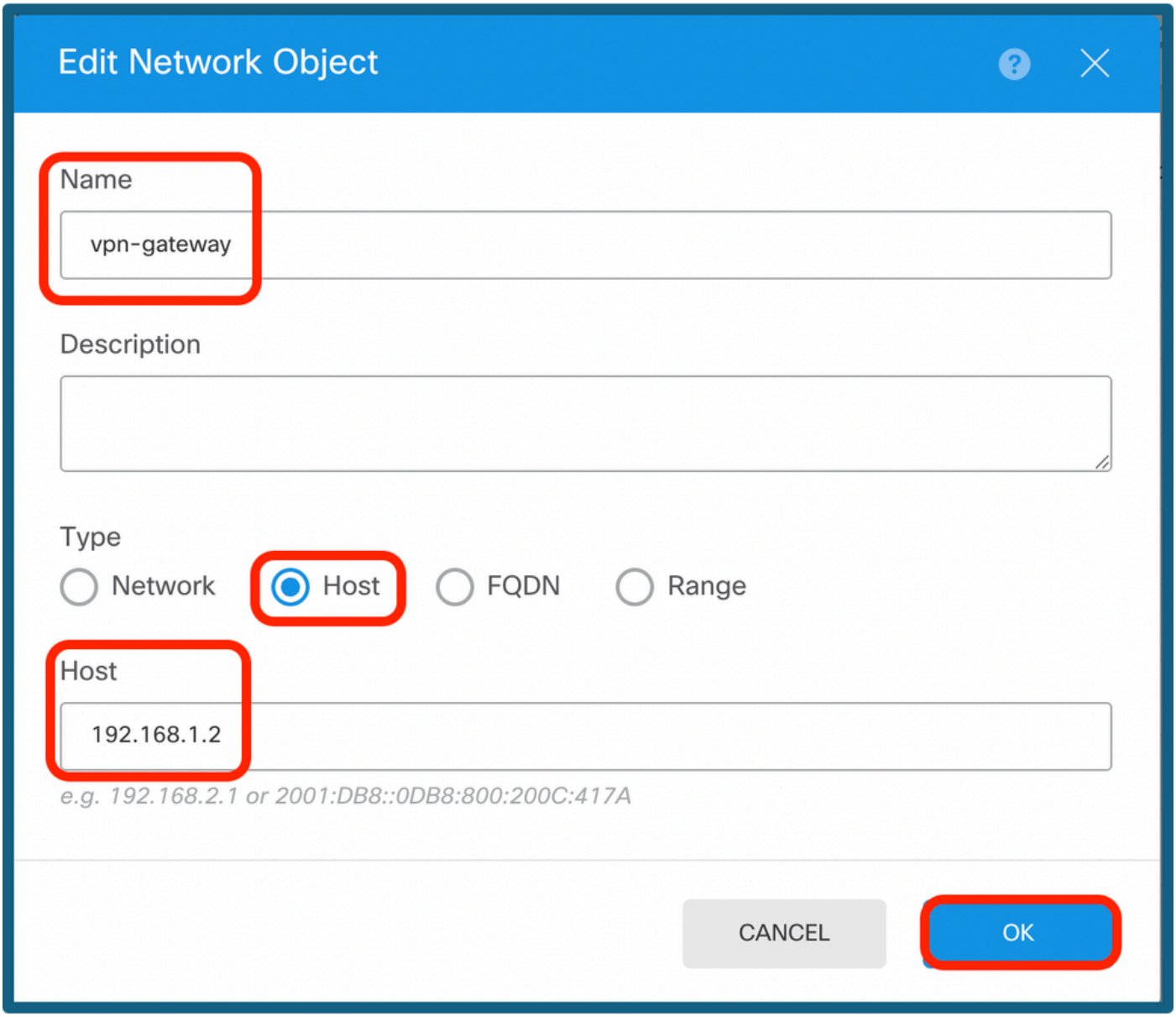
Configuration de la zone de sécurité

Étape 11a. Accédez à Objets > Réseaux, cliquez sur l'icône +.



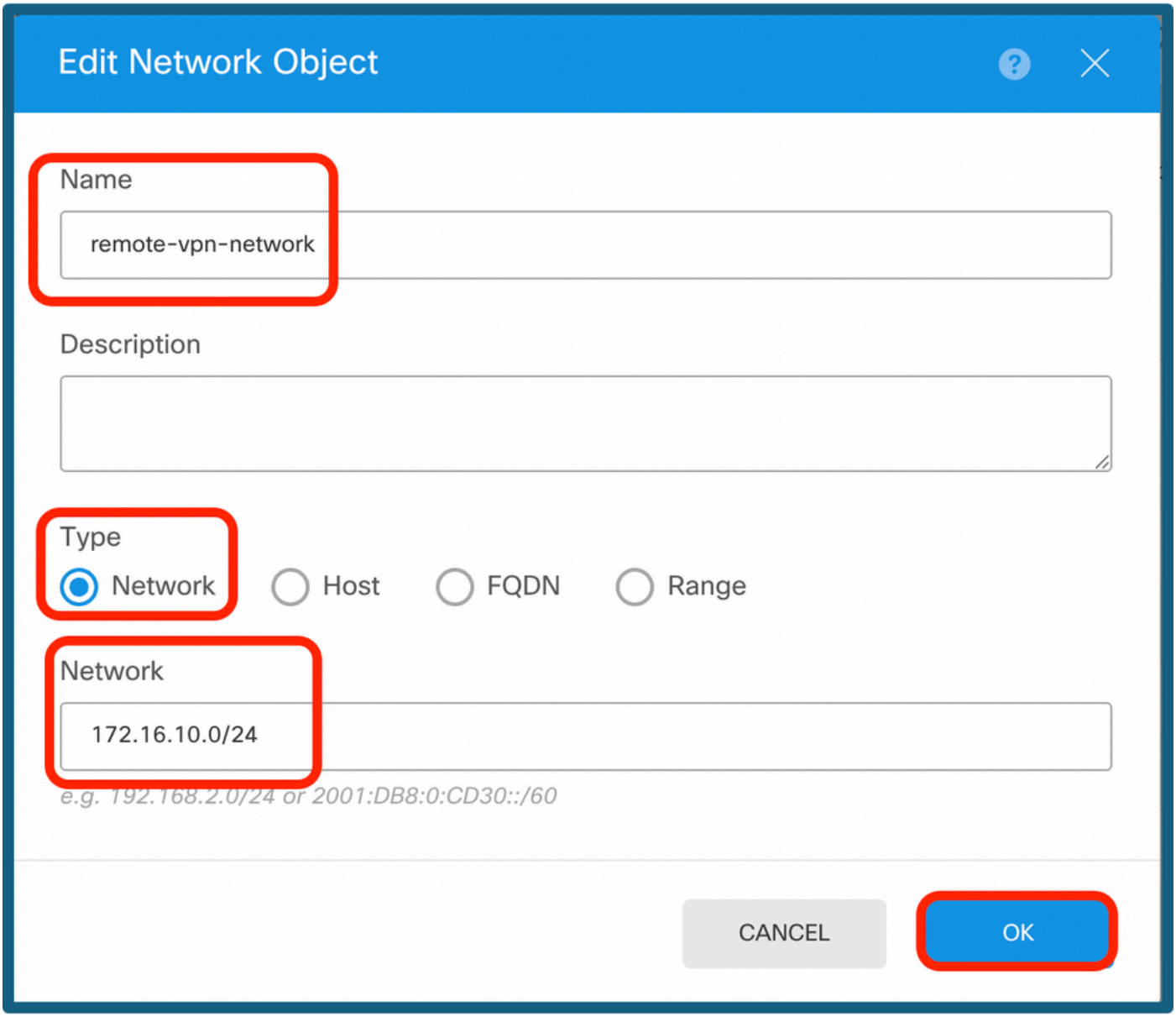
Ajouter des objets réseau

Étape 11b. Ajoutez un objet hôte et créez une passerelle avec l'adresse IP du tunnel de l'homologue.

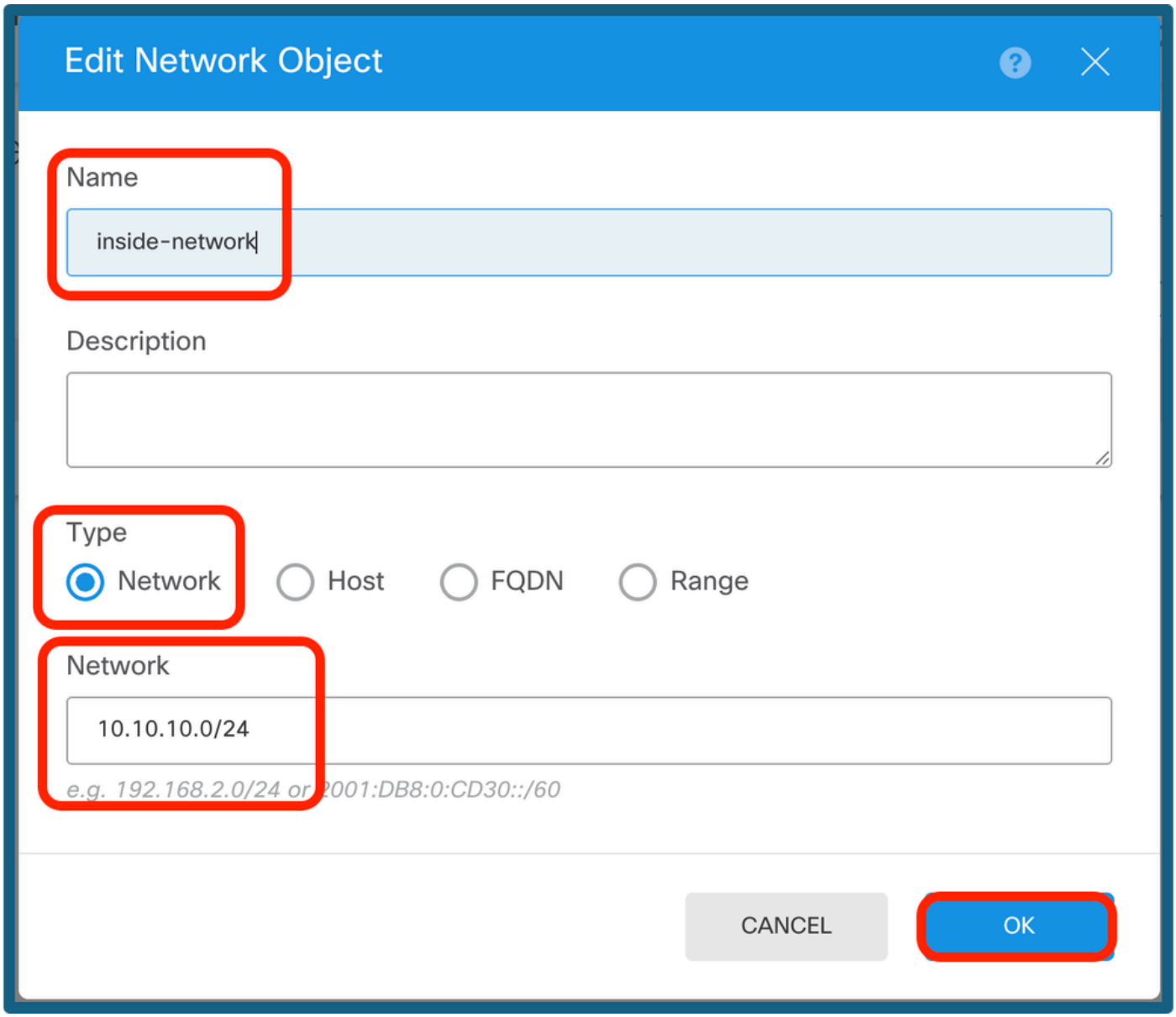


Configurer la passerelle VPN

Étape 11c. Ajoutez le sous-réseau distant et le sous-réseau local.

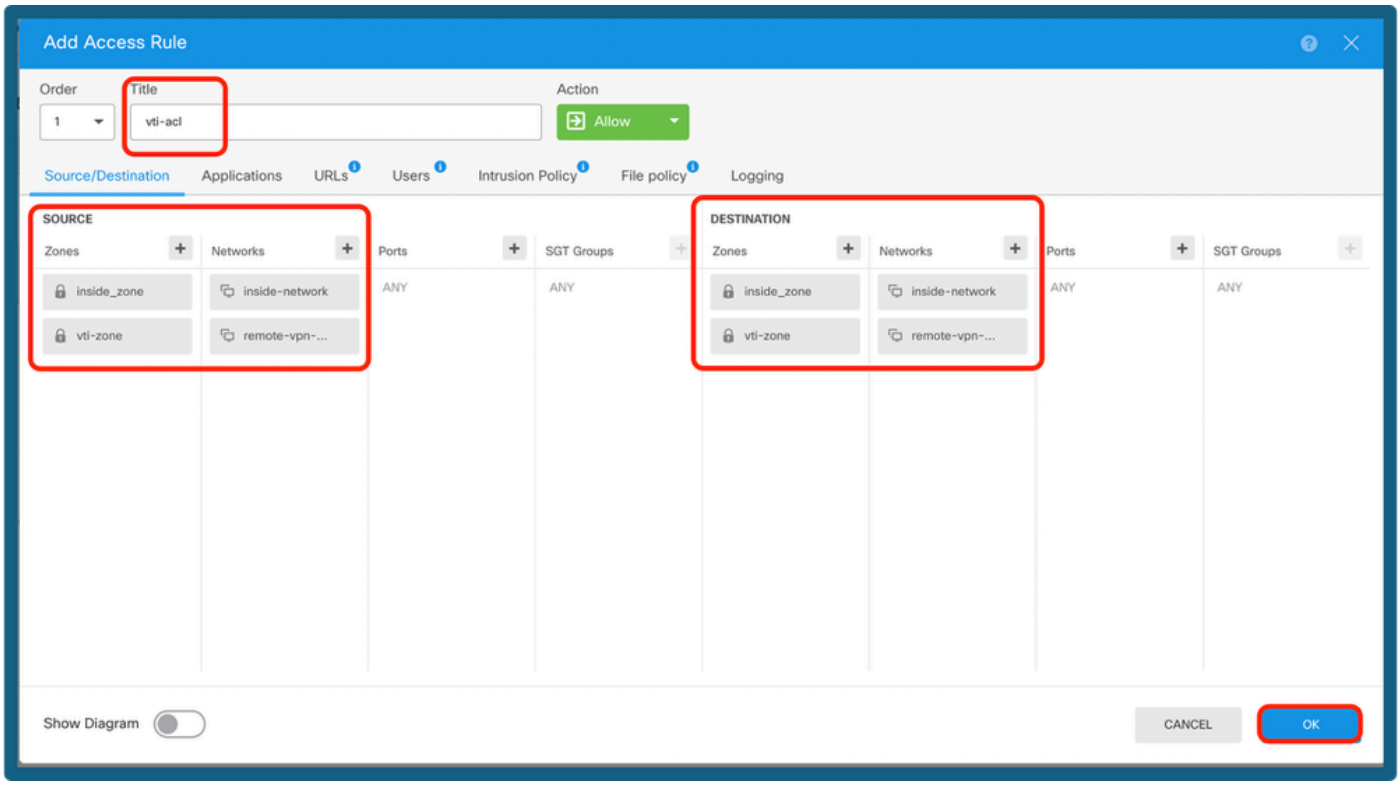


Configuration IP distante



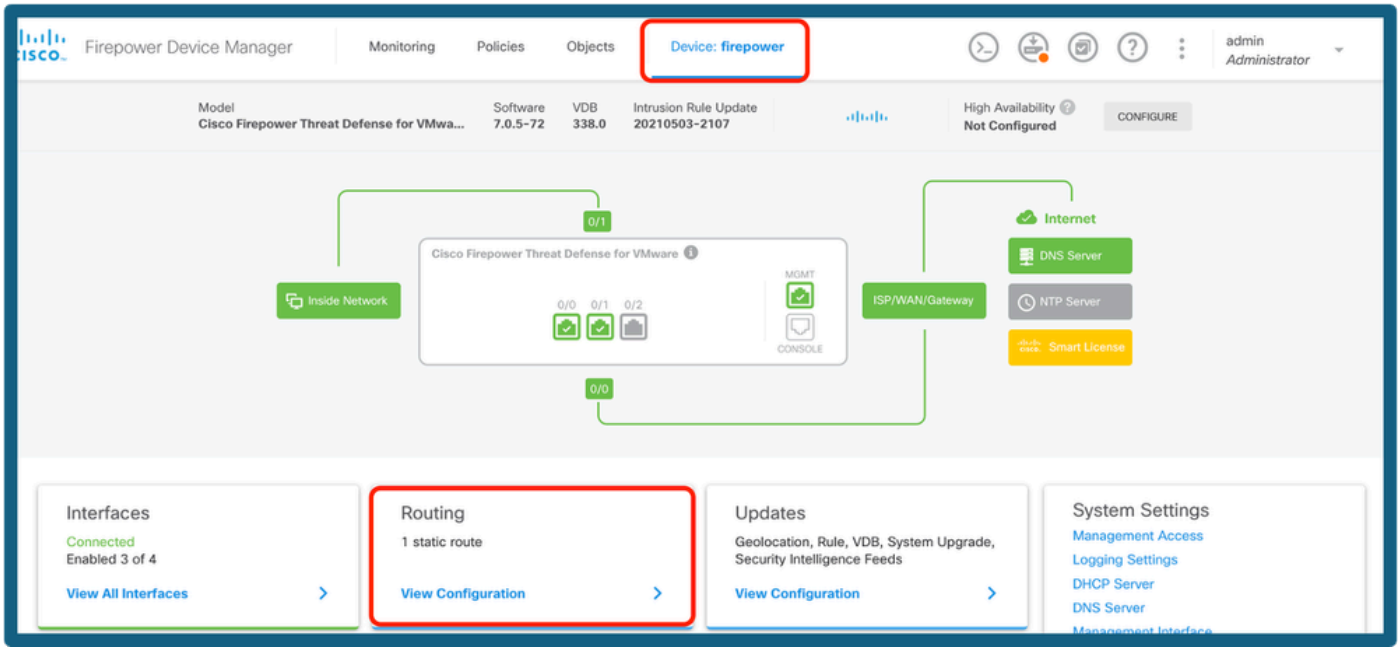
Configuration IP locale

Étape 12. Accédez à Device > Policies et configurez la politique de contrôle d'accès.



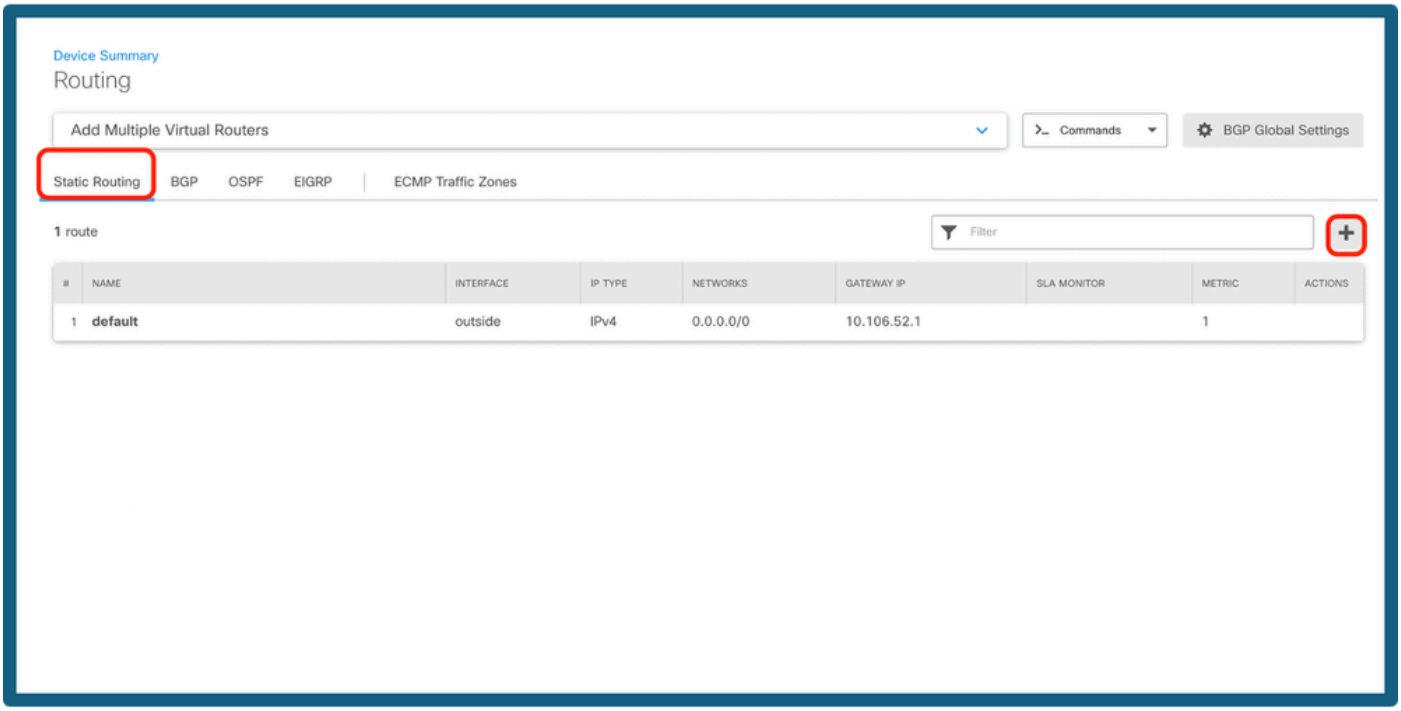
Ajouter une stratégie de contrôle d'accès

Étape 13a. Ajoutez le routage sur le tunnel VTI. Accédez à Device > Routing.



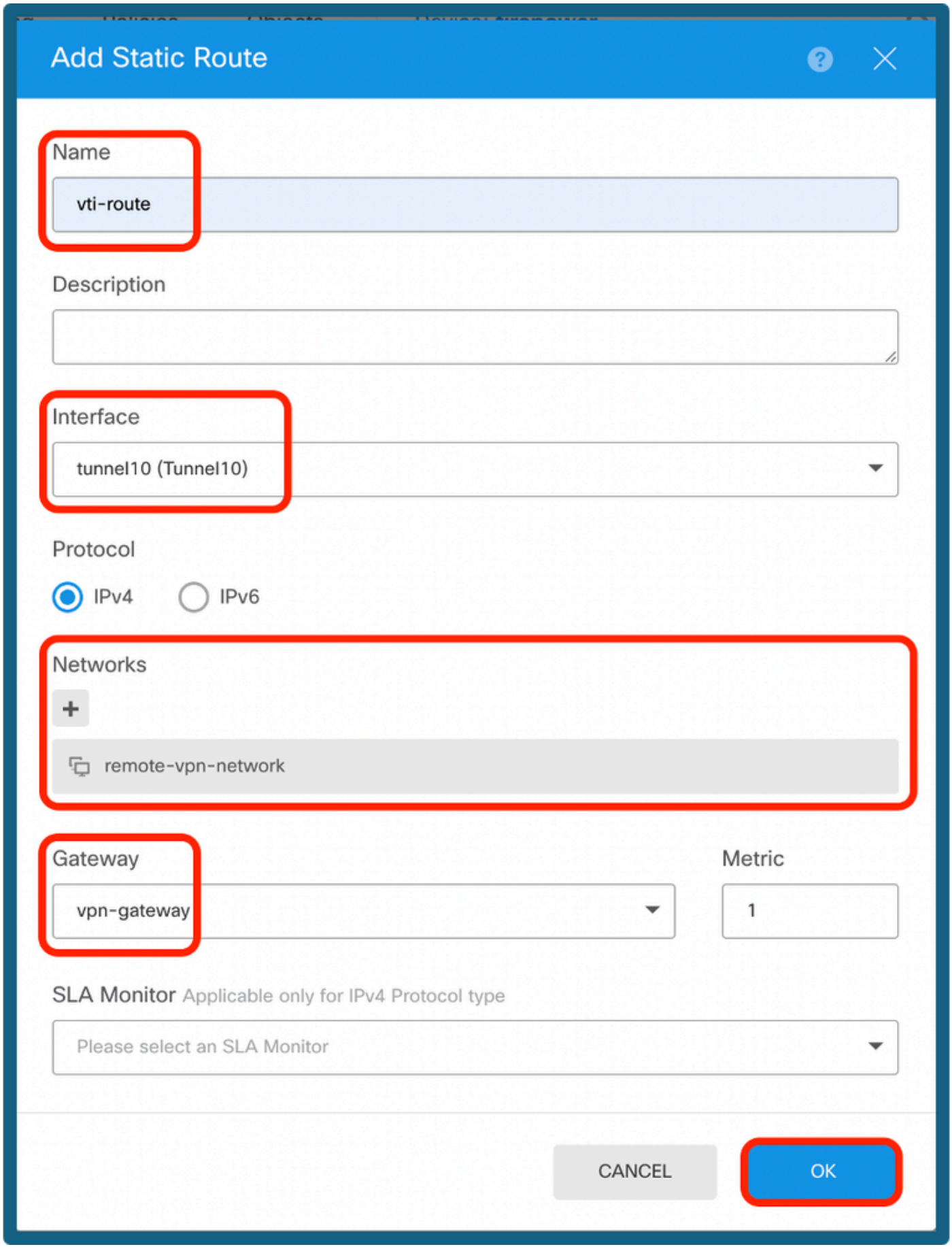
Sélectionner le routage

Étape 13b. Accédez à Static Route sous l'onglet Routing. Cliquez sur l'icône +.



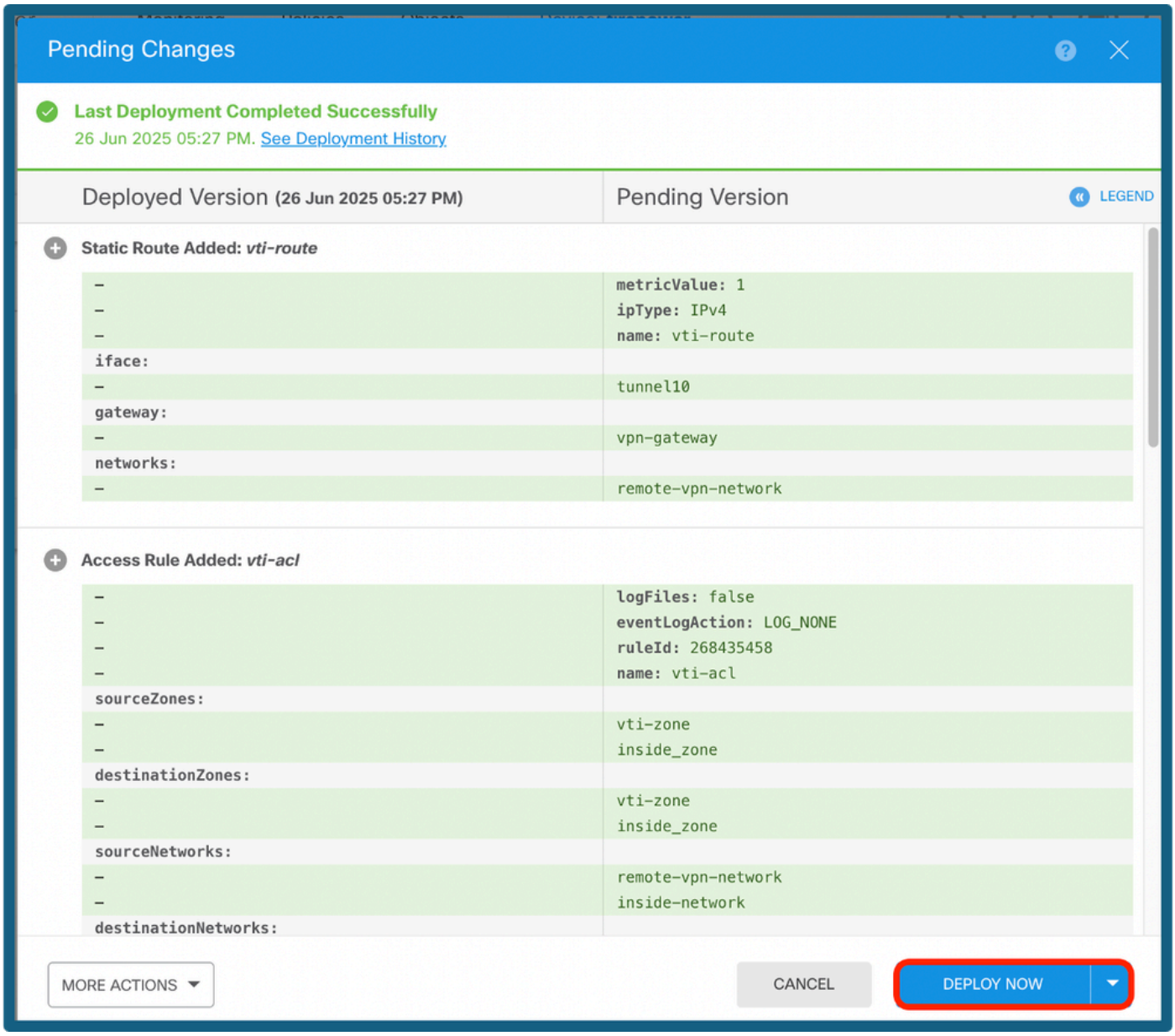
Ajouter une route

Étape 13c. Fournissez l'interface, choisissez le réseau, fournissez la passerelle. Click OK.



Configurer la route statique

Étape 14. Accédez à Déployer. Vérifiez les modifications, puis cliquez sur Déployer maintenant.

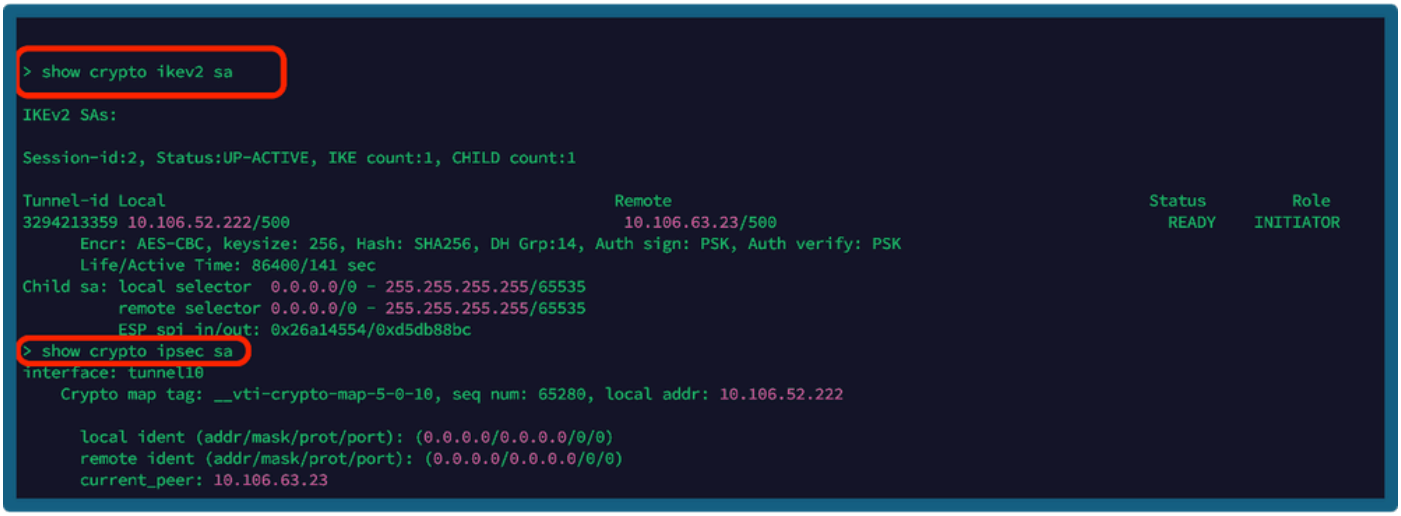


Déployer la configuration

Vérifier

Une fois le déploiement terminé, vous pouvez vérifier l'état du tunnel sur l'interface de ligne de commande en utilisant les commandes suivantes :

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



Commandes show

Informations connexes

Pour plus d'informations sur les VPN de site à site sur le FTD géré par FDM, vous pouvez trouver le guide de configuration complet ici :

Guide de configuration FTD géré par FDM

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.