Configuration du tunnel VPN site à site basé sur la route sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit comment configurer un tunnel VPN de site à site basé sur la route sur une défense contre les menaces Firepower gérée par un centre de gestion Firepower.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du fonctionnement d'un tunnel VPN.
- Comprendre comment naviguer dans le FMC.

Composants utilisés

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

- Cisco Firepower Management Center (FMC) version 6.7.0
- Cisco Firepower Threat Defense (FTD) version 6.7.0

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 basé sur la crypto-carte. Le domaine de chiffrement est configuré pour autoriser tout trafic entrant 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.

Limitations et restrictions

Voici les limitations et restrictions connues pour les tunnels basés sur la route sur FTD :

- Prend en charge IPsec uniquement. GRE n'est pas pris en charge.
- Aucune prise en charge de Dynamic VTI.
- Prend en charge uniquement les interfaces IPv4, ainsi que IPv4, les réseaux protégés ou les données utiles VPN (pas de prise en charge d'IPv6).
- Le routage statique et uniquement le protocole de routage dynamique BGP est pris en charge pour les interfaces VTI qui classifient le trafic pour VPN (pas de prise en charge d'autres protocoles tels qu'OSPF, RIP, etc.).
- Seules 100 interfaces VTI sont prises en charge par interface.
- VTI n'est pas pris en charge sur un cluster FTD.
- VTI n'est pas pris en charge dans ces politiques :

  · QoS
  •NAT
  · Paramètres de plate-forme

Ces algorithmes ne sont plus pris en charge sur FMC/FTD version 6.7.0 pour les nouveaux tunnels VPN (FMC prend en charge tous les chiffrements supprimés pour gérer FTD < 6.7) :

- Le chiffrement 3DES, DES et NULL n'est pas pris en charge dans la stratégie IKE.
- Les groupes DH 1, 2 et 24 ne sont pas pris en charge dans la stratégie IKE et la proposition IPsec.
- L'intégrité MD5 n'est pas prise en charge dans la stratégie IKE.
- PRF MD5 n'est pas pris en charge dans la stratégie IKE.

- Les algorithmes de chiffrement DES, 3DES, AES-GMAC, AES-GMAC-192 et AES-GMAC-256 ne sont pas pris en charge dans la proposition IPsec.

Remarque : cela est vrai pour les tunnels VPN basés sur la route de site à site ainsi que sur les politiques. Afin de mettre à niveau un FTD plus ancien vers 6.7 à partir de FMC, il déclenche un contrôle de pré-validation avertissant l'utilisateur des modifications qui concernent les chiffres supprimés qui bloquent la mise à niveau.

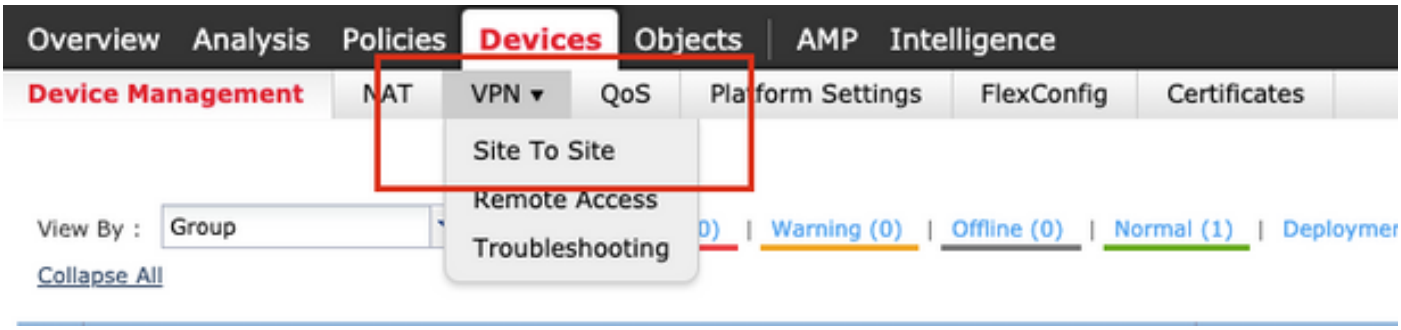
FTD 6.7 géré via FMC 6.7	Configuration disponible	Tunnel VPN de site à site
Nouvelle installation	Chiffres faibles disponibles, mais ne peuvent pas être utilisés pour configurer le périphérique FTD 6.7.	Chiffres faibles disponibles, mais ne peuvent pas être utilisés pour configurer le périphérique FTD 6.7.
Mise à niveau : FTD configuré uniquement avec des chiffrements faibles	Mise à niveau à partir de l'interface utilisateur de FMC 6.7, un contrôle de prévalidation affiche une erreur. La mise à niveau est bloquée jusqu'à la reconfiguration.	Après la mise à niveau FTD, et supposez que l'homologue n'a pas modifié ses paramètres, le tunnel est terminé.
Mise à niveau : FTD configuré uniquement avec des chiffrements faibles et certains chiffrements forts	Mise à niveau à partir de l'interface utilisateur de FMC 6.7, un contrôle de prévalidation affiche une erreur. La mise à niveau est bloquée jusqu'à la reconfiguration.	Après la mise à niveau FTD, et supposez que l'homologue a des chiffres forts, le tunnel se rétablit.
Mise à niveau : pays de classe C (ne dispose pas d'une licence de chiffrement puissante)	Autoriser DES est autorisé	Autoriser DES est autorisé

.

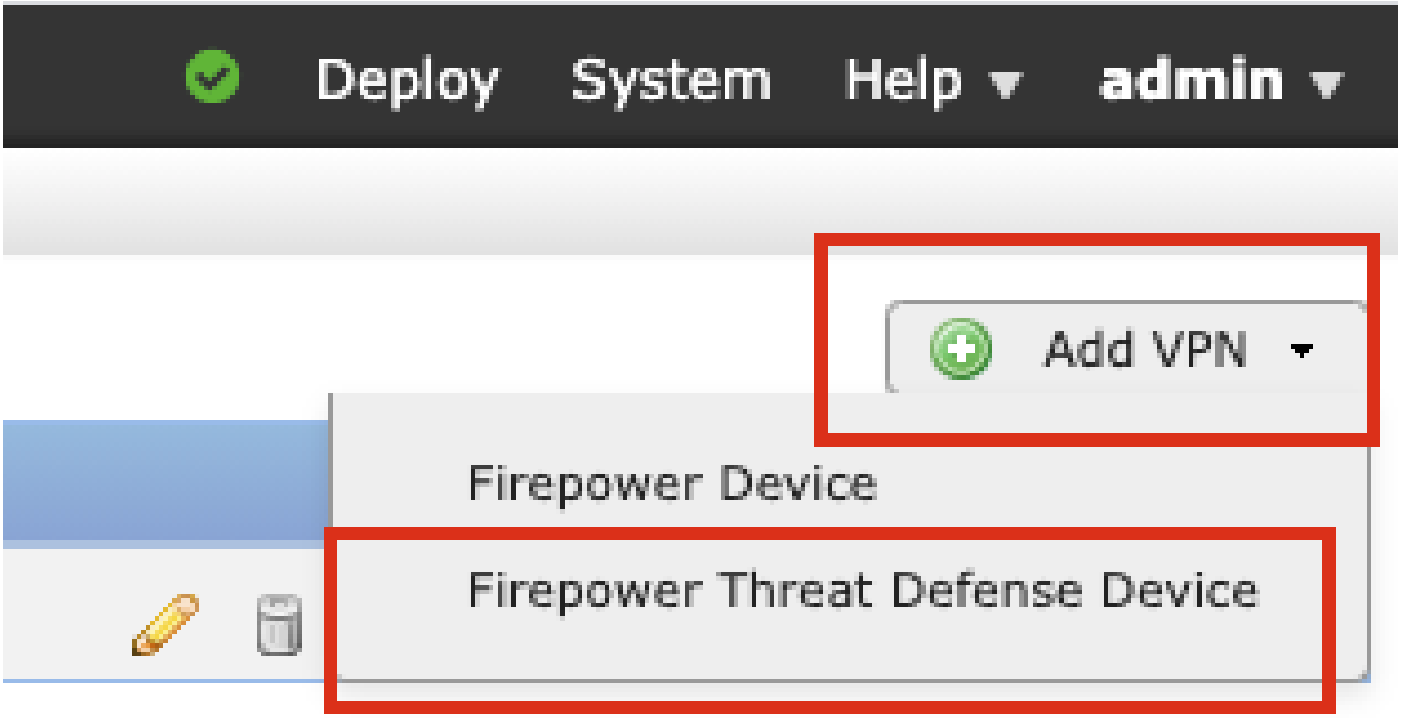
Remarque : aucune licence supplémentaire n'est nécessaire, le VPN basé sur la route peut être configuré en mode sous licence et en mode d'évaluation. Sans la conformité au chiffrement (Exportation des fonctionnalités contrôlées activée), seul DES peut être utilisé comme algorithme de chiffrement.

Étapes de configuration sur FMC

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



Étape 2. Cliquez sur Add VPN, et choisissez Firepower Threat Defense Device, comme illustré dans l'image.

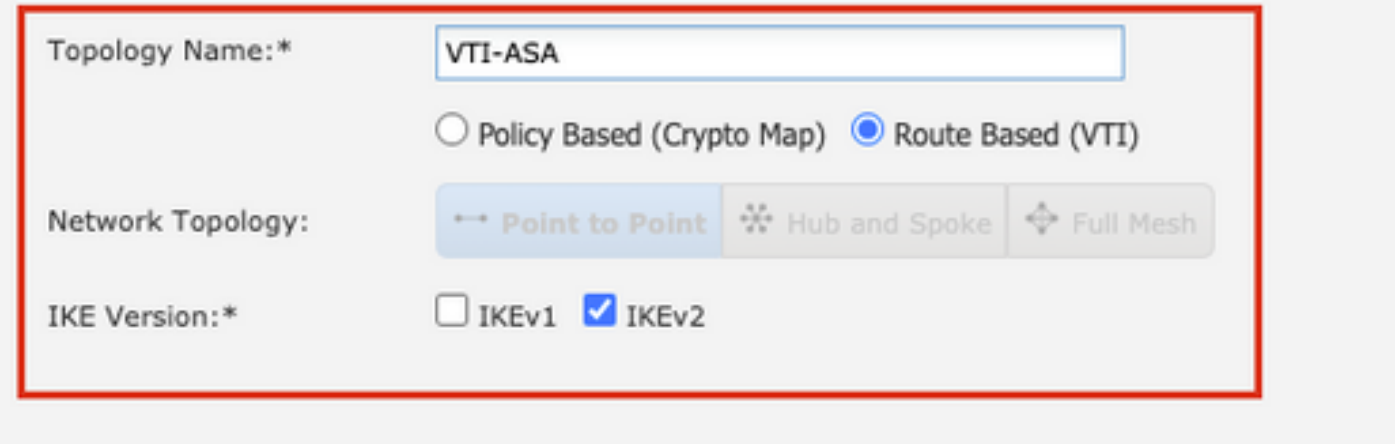


Étape 3. Indiquez un nom de topologie et sélectionnez le type de VPN comme VTI (Route Based). Sélectionnez la version IKE.

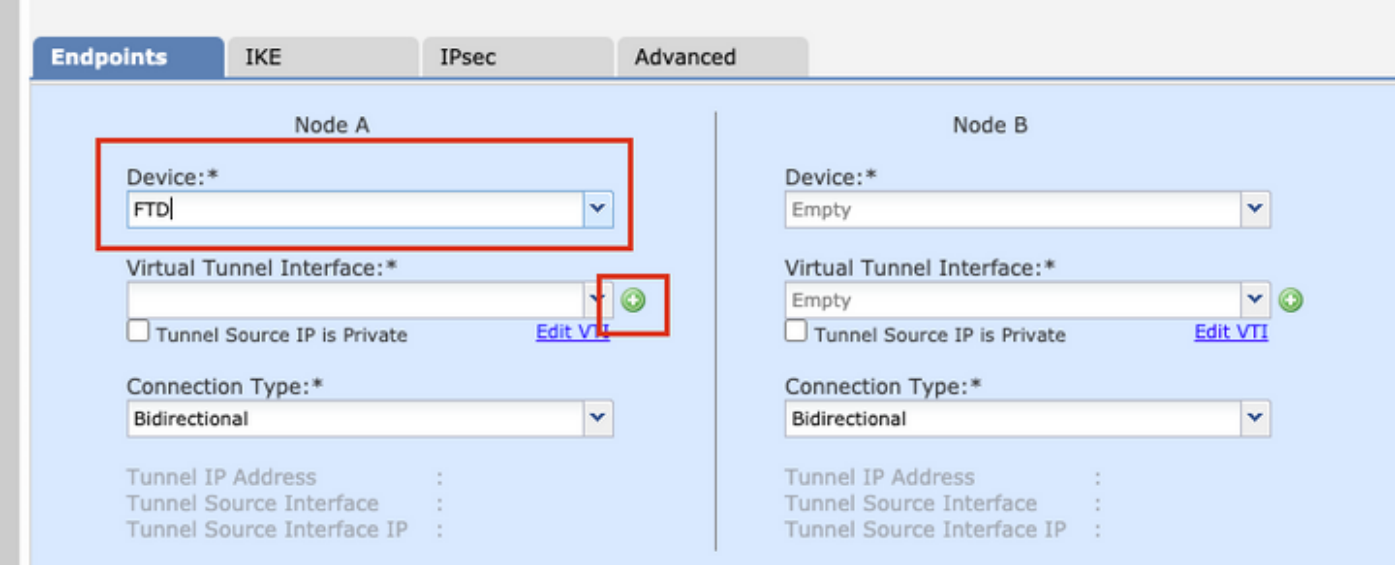
Pour les besoins de cette démonstration :

Nom de la topologie : VTI-ASA

Version IKE : IKEv2



Étape 4. Choisissez le Périphérique sur lequel le tunnel doit être configuré, Vous pouvez choisir d'ajouter une nouvelle interface de modèle virtuel (cliquez sur l'icône +), ou sélectionnez-en une dans la liste qui existe.



Étape 5. Définissez les paramètres de la nouvelle interface de tunnel virtuel. Click OK.

Pour les besoins de cette démonstration :

Nom : VTI-ASA

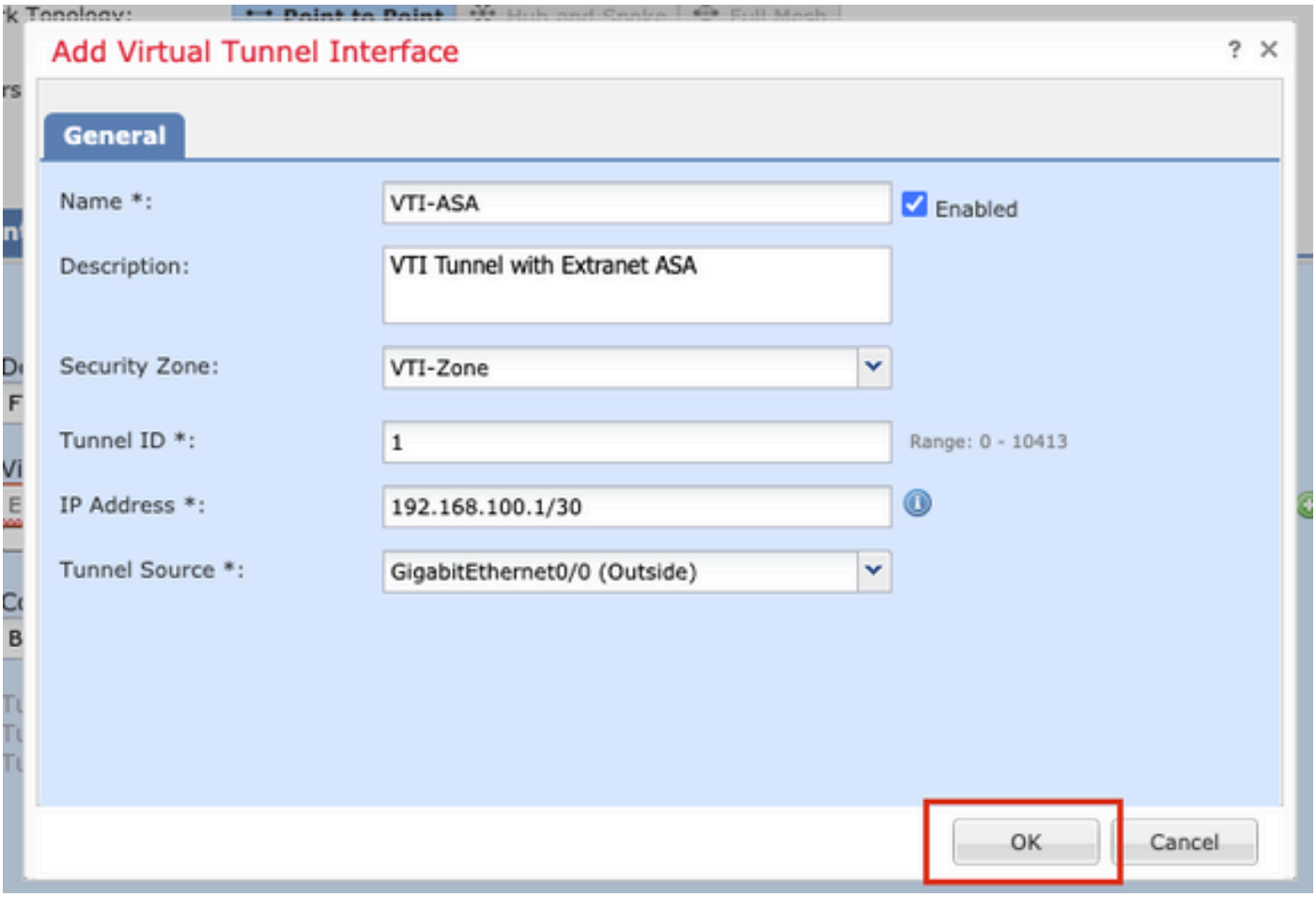
Description (en option) : tunnel VTI avec Extranet ASA

Zone de sécurité : VTI-Zone

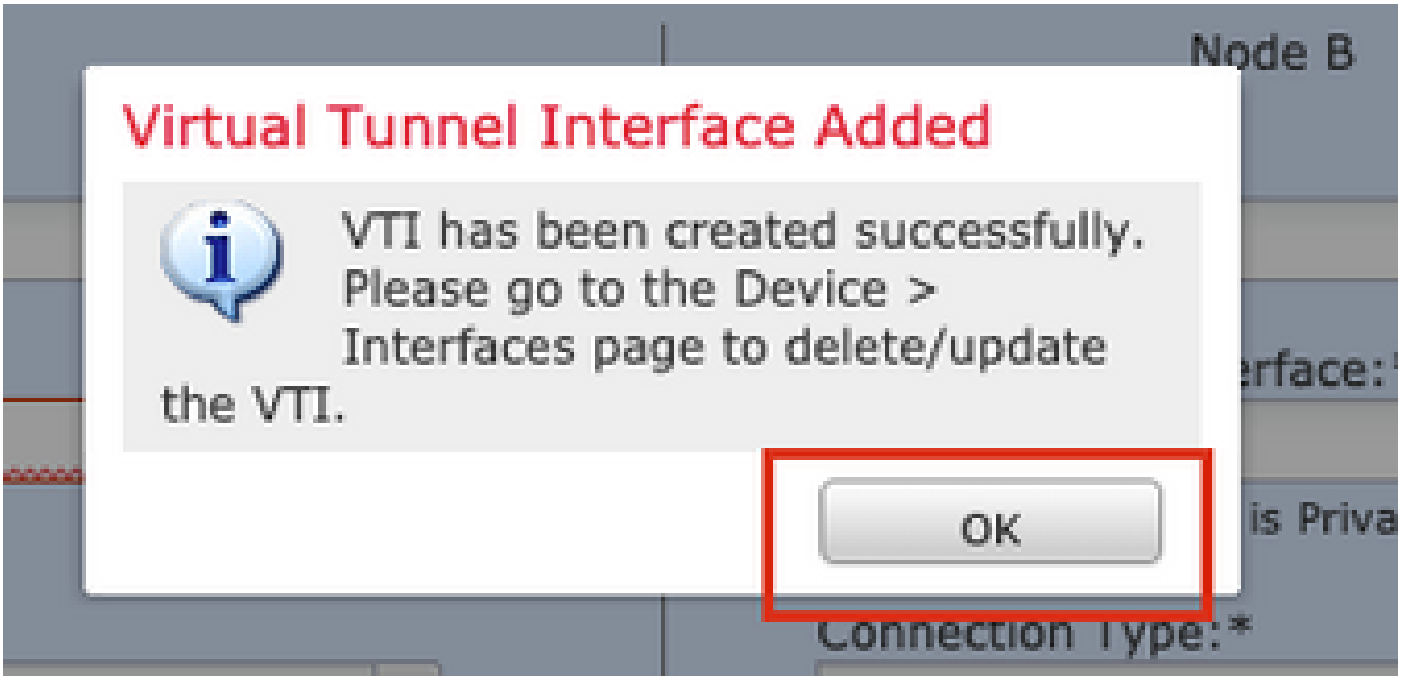
ID de tunnel : 1

Adresse IP : 192.168.100.1/30

Source du tunnel : GigabitEthernet0/0 (externe)



Étape 6. Cliquez sur OK dans la fenêtre contextuelle mentionnant que la nouvelle interface VTI a été créée.



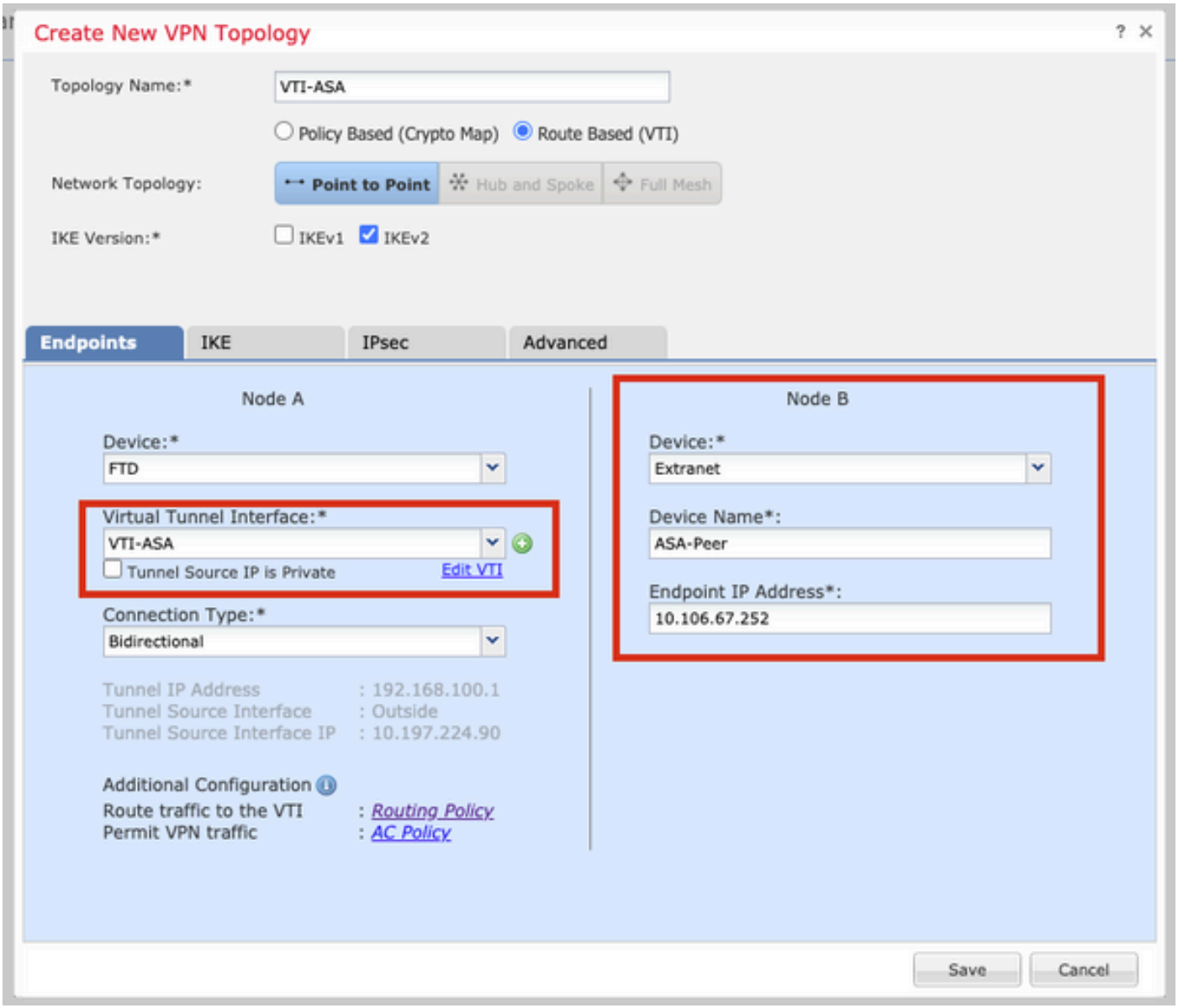
Étape 7. Sélectionnez le VTI nouvellement créé ou un VTI qui existe sous Virtual Tunnel Interface. Fournissez les informations pour le noeud B (qui est le périphérique homologue).

Pour les besoins de cette démonstration :

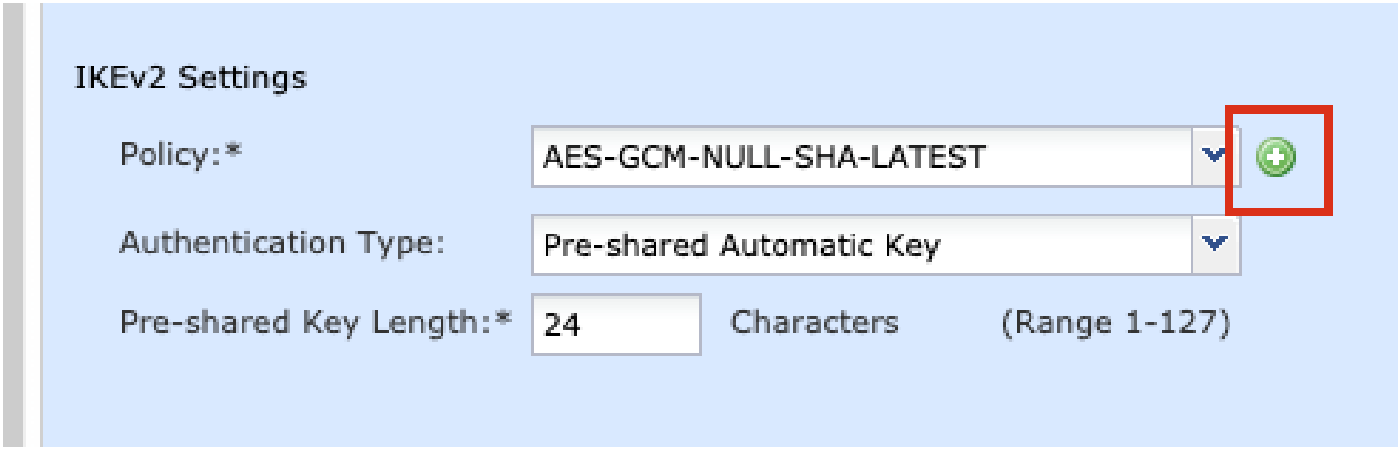
Périphérique : Extranet

Nom du périphérique : homologue ASA

Adresse IP du point d'extrémité : 10.106.67.252



Étape 8. Accédez à l'onglet IKE. Vous pouvez choisir d'utiliser une politique prédéfinie ou cliquer sur le bouton + en regard de l'onglet Politique et en créer une nouvelle.



Étape 9. (Facultatif, si vous créez une nouvelle stratégie IKEv2.) Fournissez un nom pour la stratégie et sélectionnez les algorithmes à utiliser dans la stratégie. Cliquez sur Save.

Pour les besoins de cette démonstration :

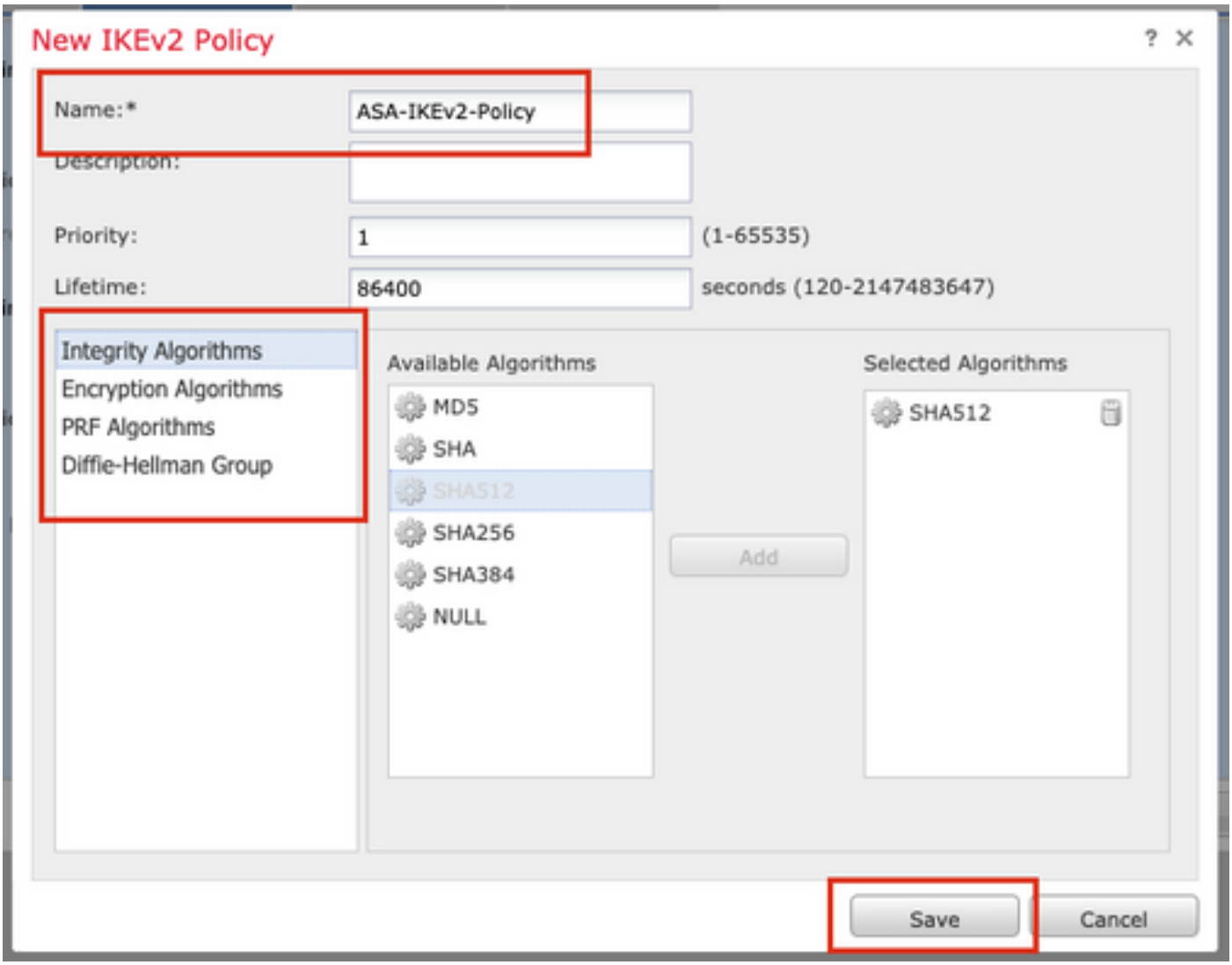
Nom : ASA-IKEv2-Policy

Algorithmes d'intégrité : SHA-512

Algorithmes de chiffrement : AES-256

Algorithmes PRF : SHA-512

Diffie-Hellman Groupe : 21



Étape 10. Choisissez la politique nouvellement créée ou la politique qui existe. Sélectionnez le type d'authentification. Si une clé manuelle pré-partagée est utilisée, fournissez la clé dans les zones Key et Confirm Key.

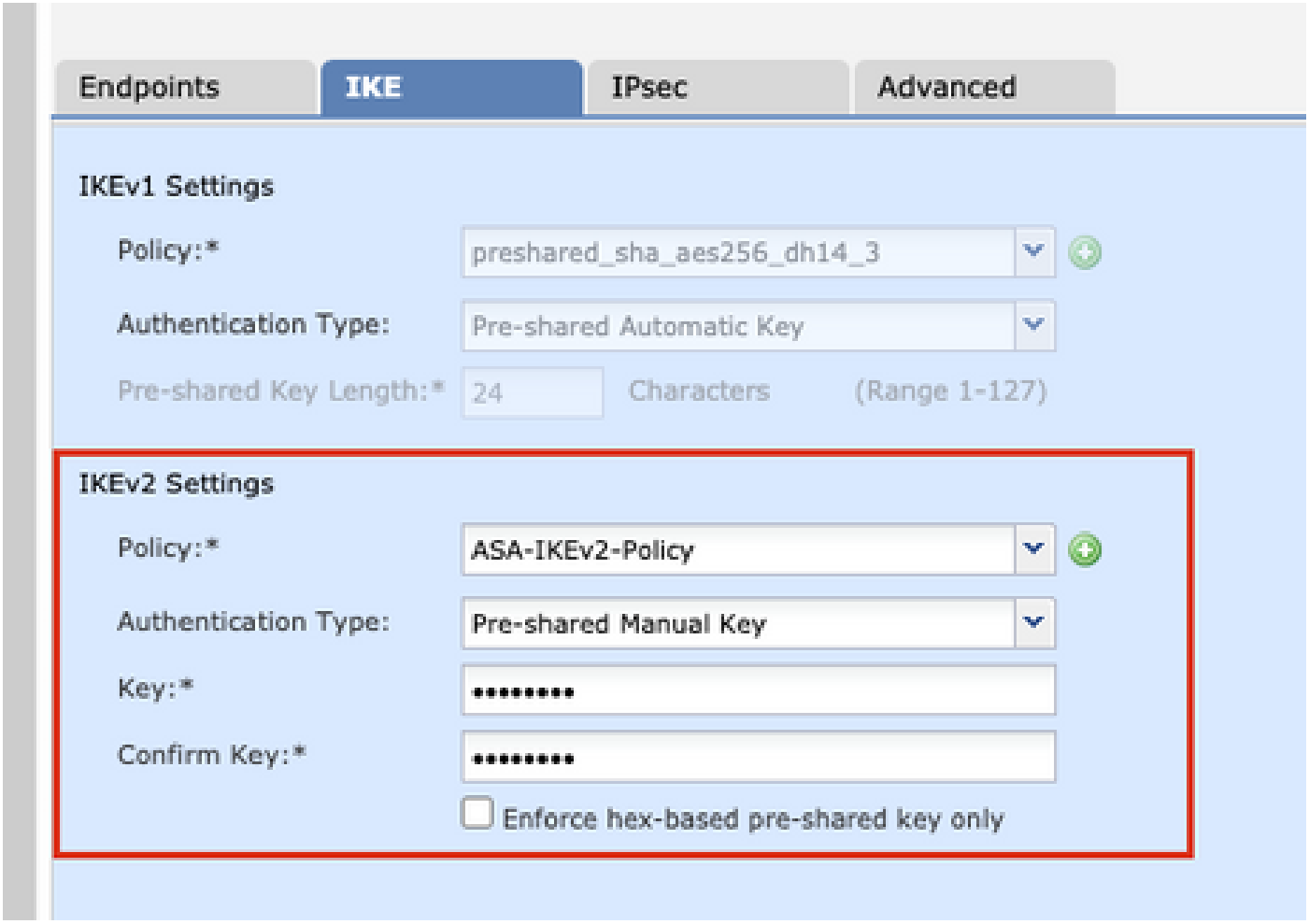
Pour les besoins de cette démonstration :

Stratégie : ASA-IKEv2-Policy

Type d'authentification : clé manuelle pré-partagée

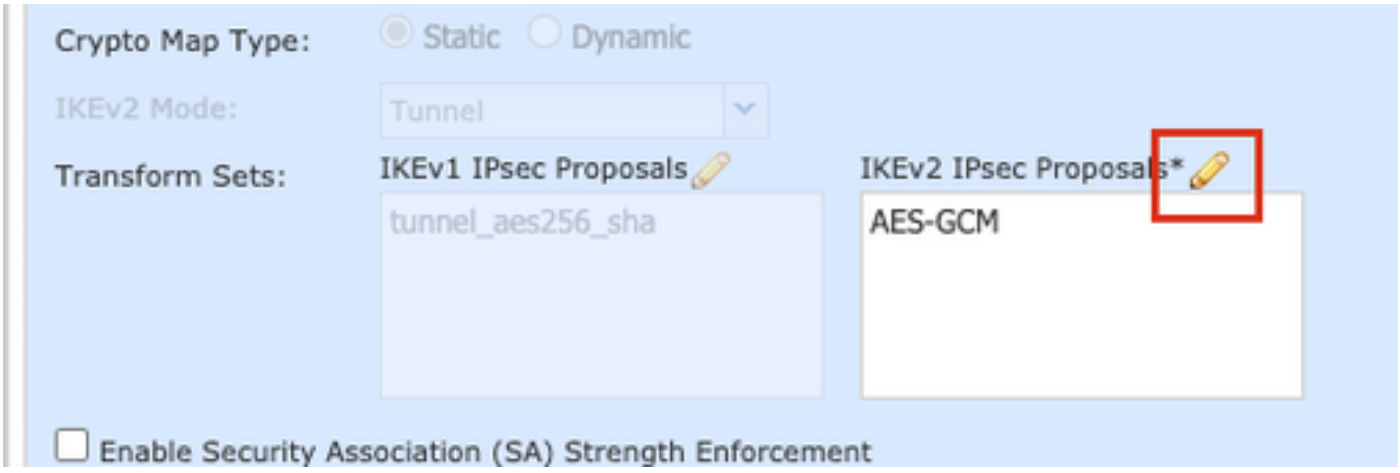
Clé : cisco123

Confirmer la clé : cisco123



Remarque : si les deux terminaux sont enregistrés sur le même FMC, l'option Pre-shared Automatic Key (Clé automatique pré-partagée) peut également être utilisée.

Étape 11. Accédez à l'onglet IPsec. Vous pouvez choisir d'utiliser une proposition IKEv2 IPsec prédéfinie ou d'en créer une nouvelle. Cliquez sur le bouton Modifier en regard de l'onglet IKEv2 IPsec Proposal.



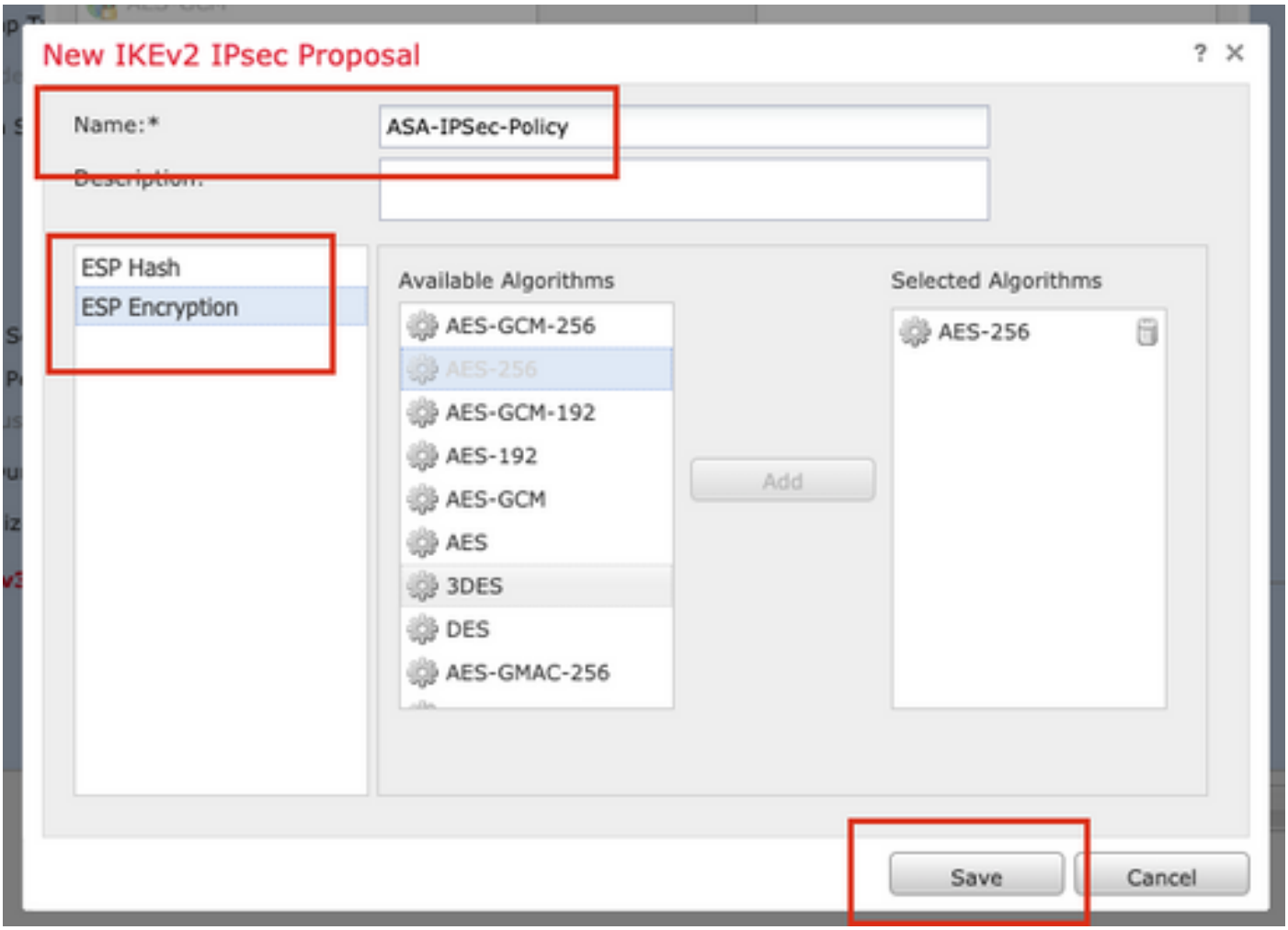
Étape 12. (Facultatif, si vous créez une nouvelle proposition IKEv2 IPsec.) Saisissez un nom pour la proposition et sélectionnez les algorithmes à utiliser dans la proposition. Cliquez sur Save.

Pour les besoins de cette démonstration :

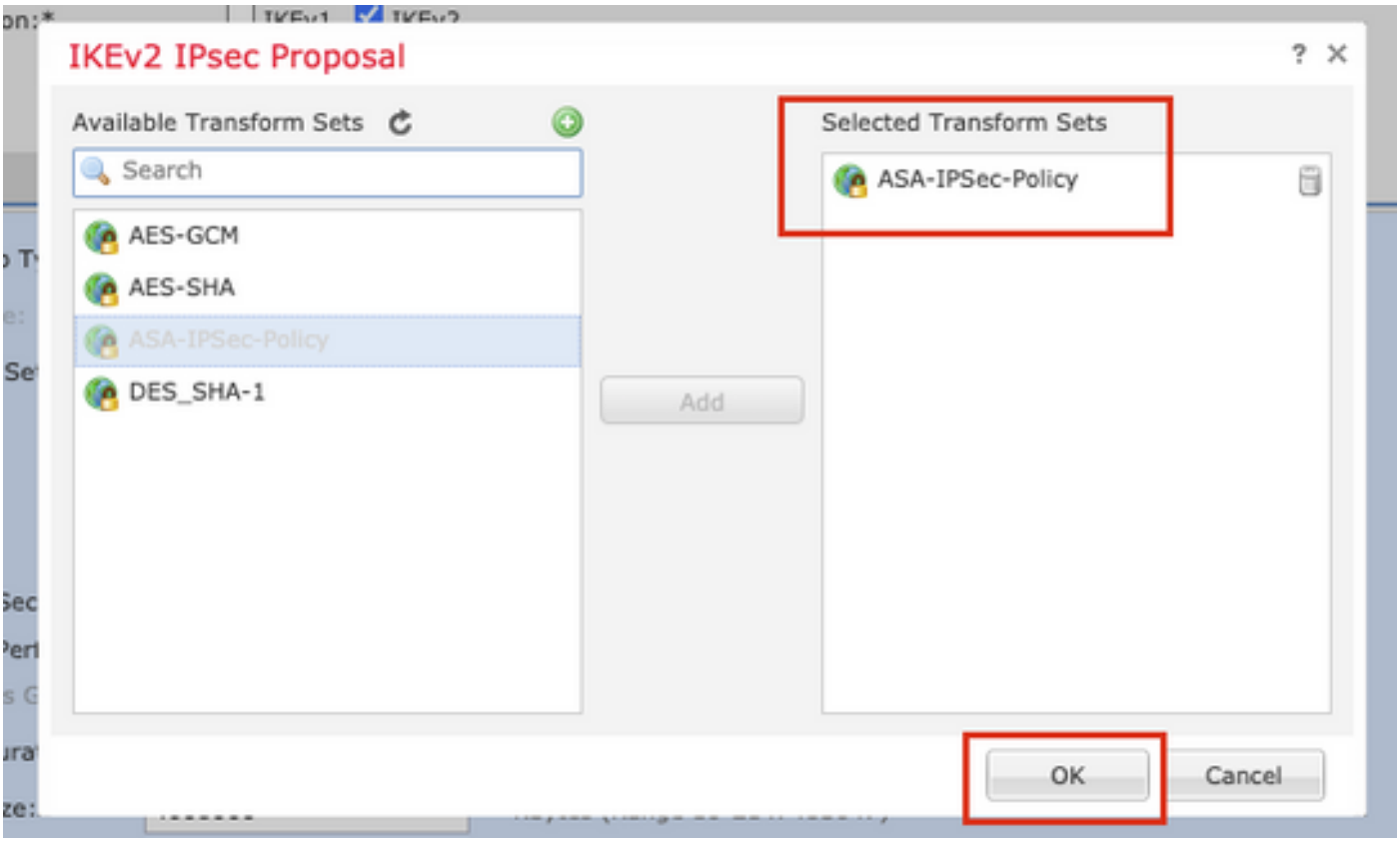
Nom : ASA-IPSec-Policy

Hachage ESP : SHA-512

Cryptage ESP : AES-256



Étape 13. Choisissez la nouvelle proposition ou la nouvelle proposition qui existe dans la liste des propositions disponibles. Click OK.



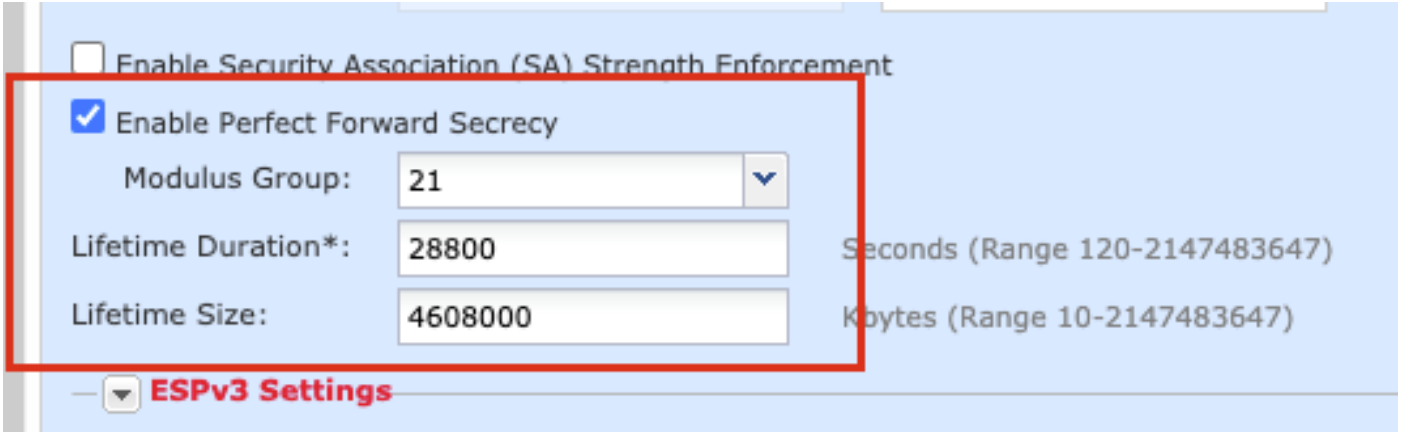
Étape 14. (Facultatif) Sélectionnez les paramètres Perfect Forward Secrecy. Configurez la durée de vie et la taille de vie d'IPsec.

Pour les besoins de cette démonstration :

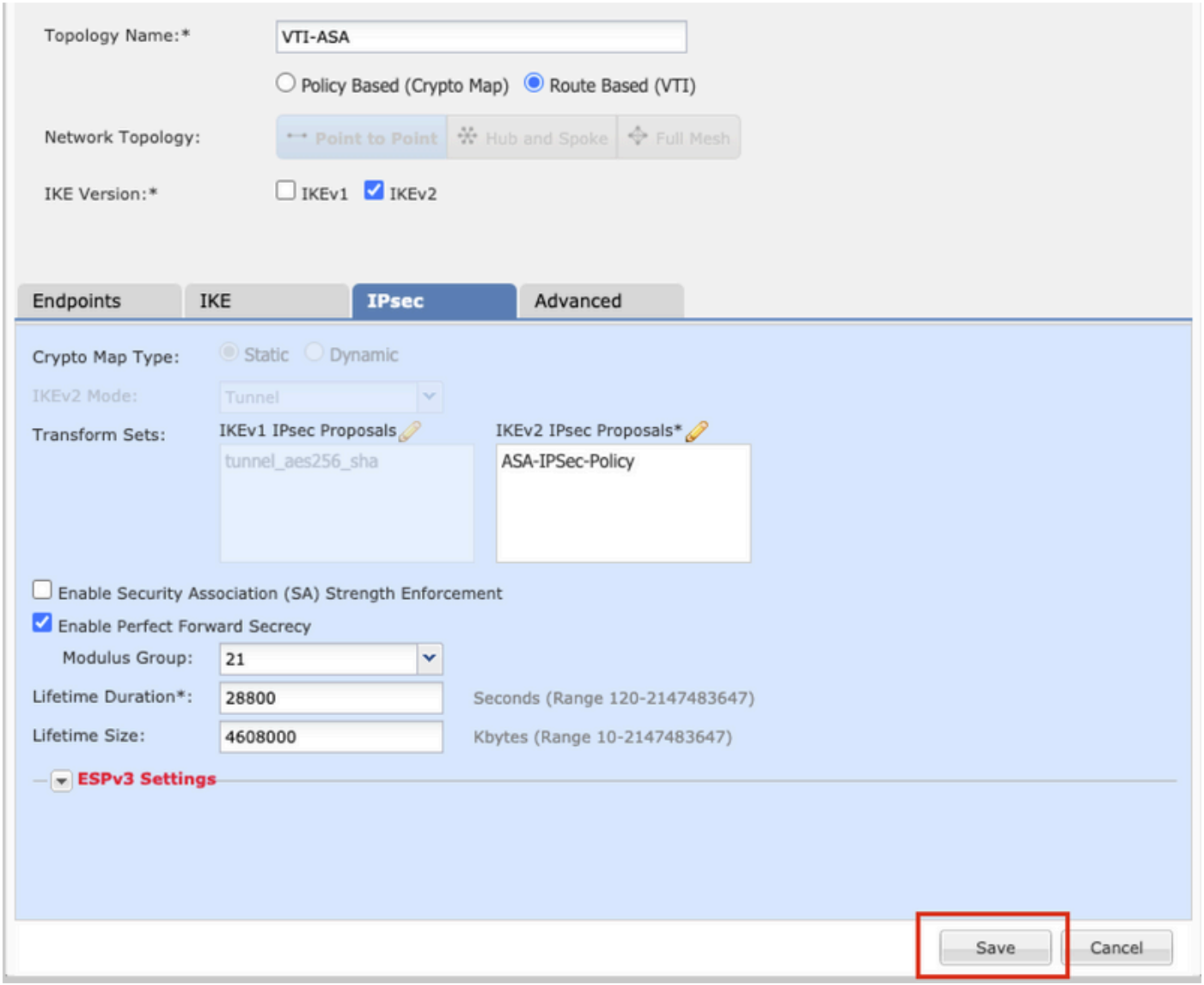
Secret direct parfait : Groupe de modules 21

Durée de vie : 28800 (par défaut)

Durée de vie : 4608000 (par défaut)



Étape 15. Vérifiez les paramètres configurés. Cliquez sur Save, comme illustré dans cette image.



Étape 16. (Facultatif) Configurez la stratégie NAT. Accédez à Devices > NAT. Sélectionnez la stratégie NAT affectée à ce FTD.

Fournissez les Objets d'interface source et les Objets d'interface de destination dans l'onglet Objets d'interface.

Fournissez la source d'origine, la destination d'origine, la source traduite, la destination traduite dans l'onglet Traduction. Click OK.

Pour les besoins de cette démonstration :

Objets d'interface source : dans la zone

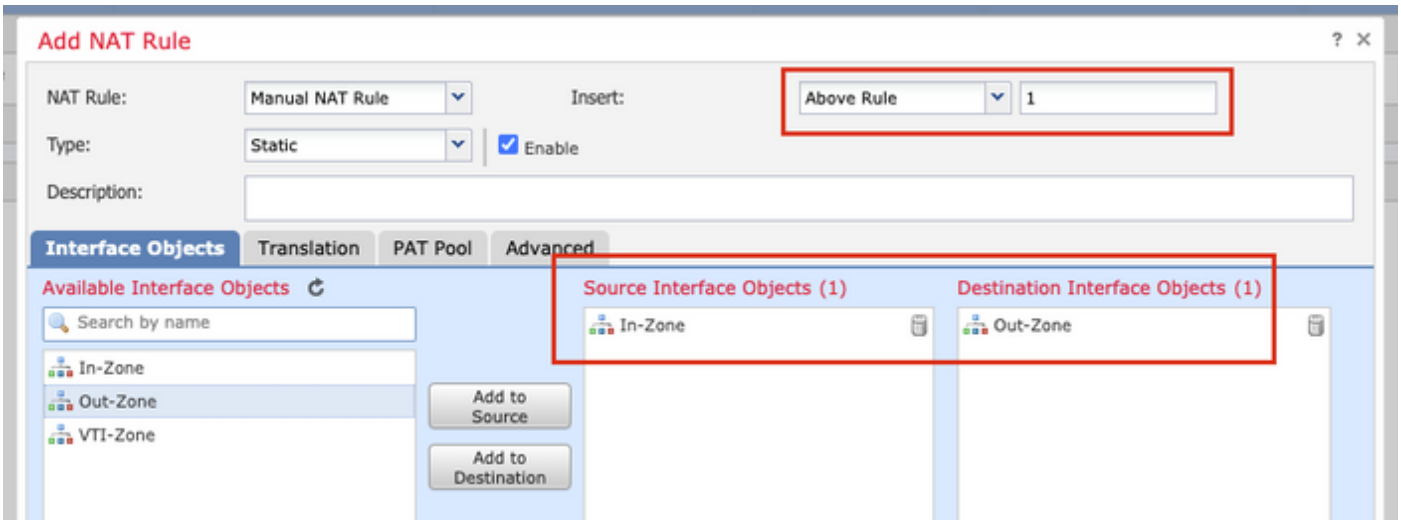
Objets d'interface de destination : zone de sortie

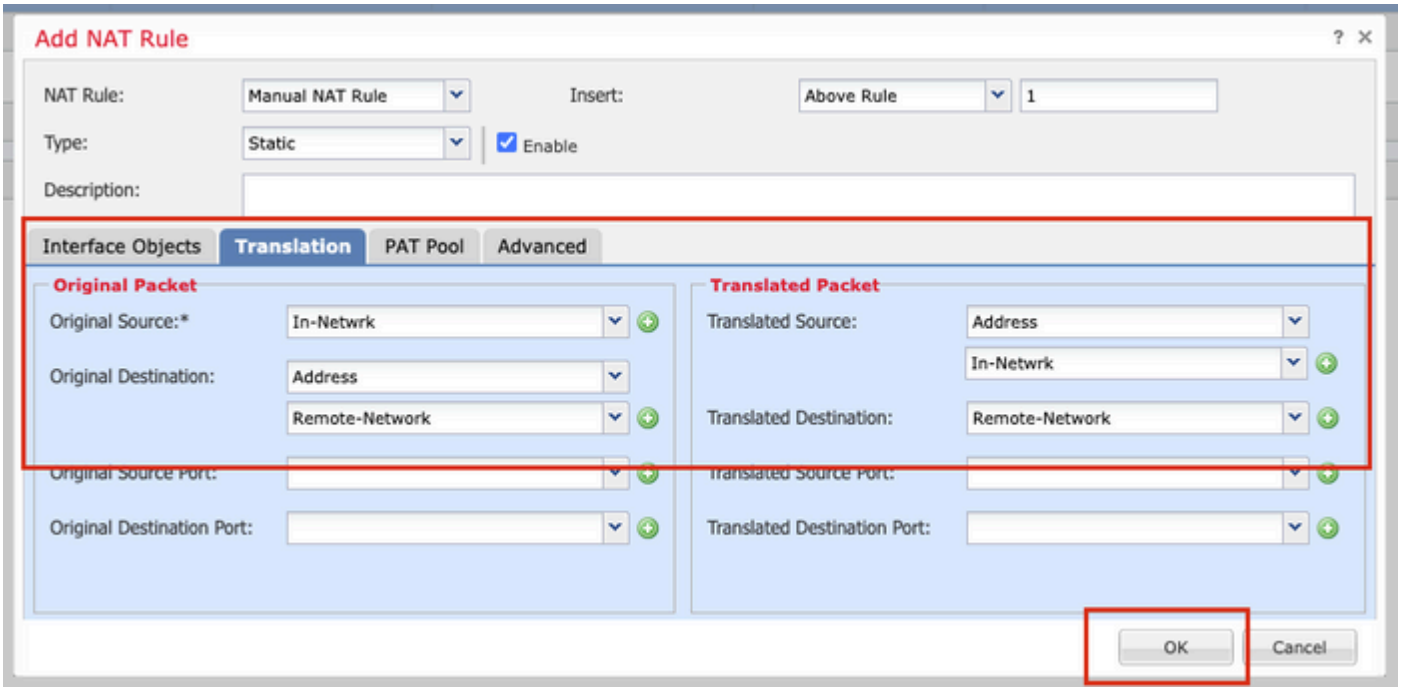
Source d'origine : In-Network

Destination d'origine : Remote-Network

Source traduite : In-Network

Destination traduite : Réseau distant





Remarque : assurez-vous que l'exemption NAT statique pour le tunnel site à site est ajoutée en plus des règles NAT/PAT dynamiques.

Étape 17. Configurez la stratégie de contrôle d'accès. Accédez à Politiques > Contrôle d'accès > Contrôle d'accès. Modifiez la stratégie appliquée au FTD.

Remarque : sysopt connection permit-vpn ne fonctionne pas avec les tunnels VPN basés sur la route. Les règles de contrôle d'accès doivent être configurées pour les zones IN-> OUT et OUT -> IN.

Indiquez les zones source et de destination dans l'onglet Zones.

Fournissez les réseaux source, réseaux de destination dans l'onglet Réseaux. Cliquez sur Add.

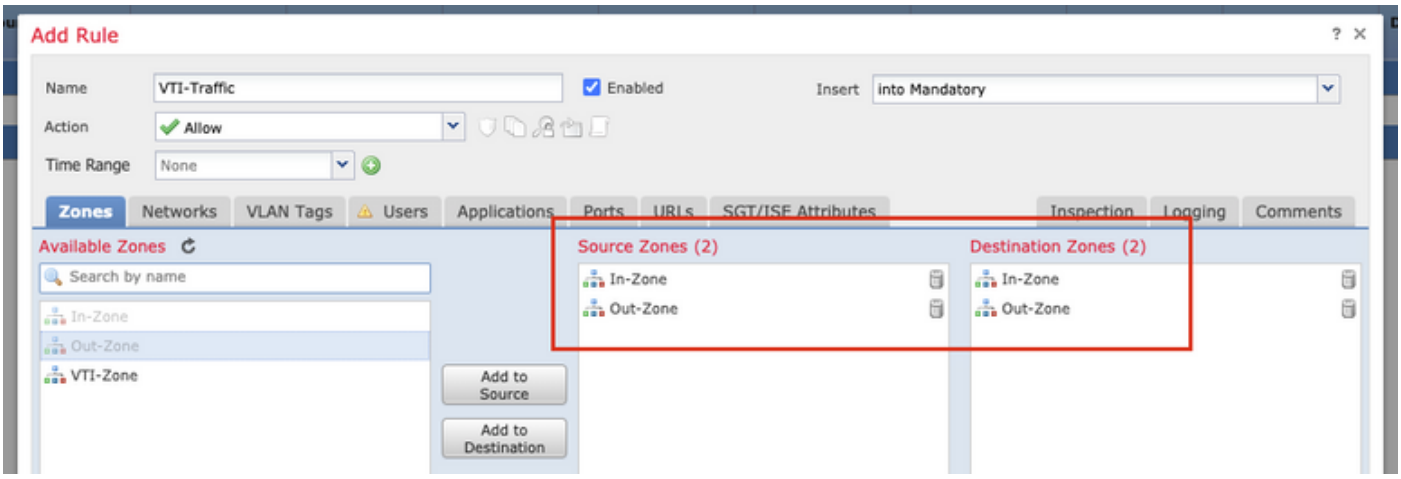
Pour les besoins de cette démonstration :

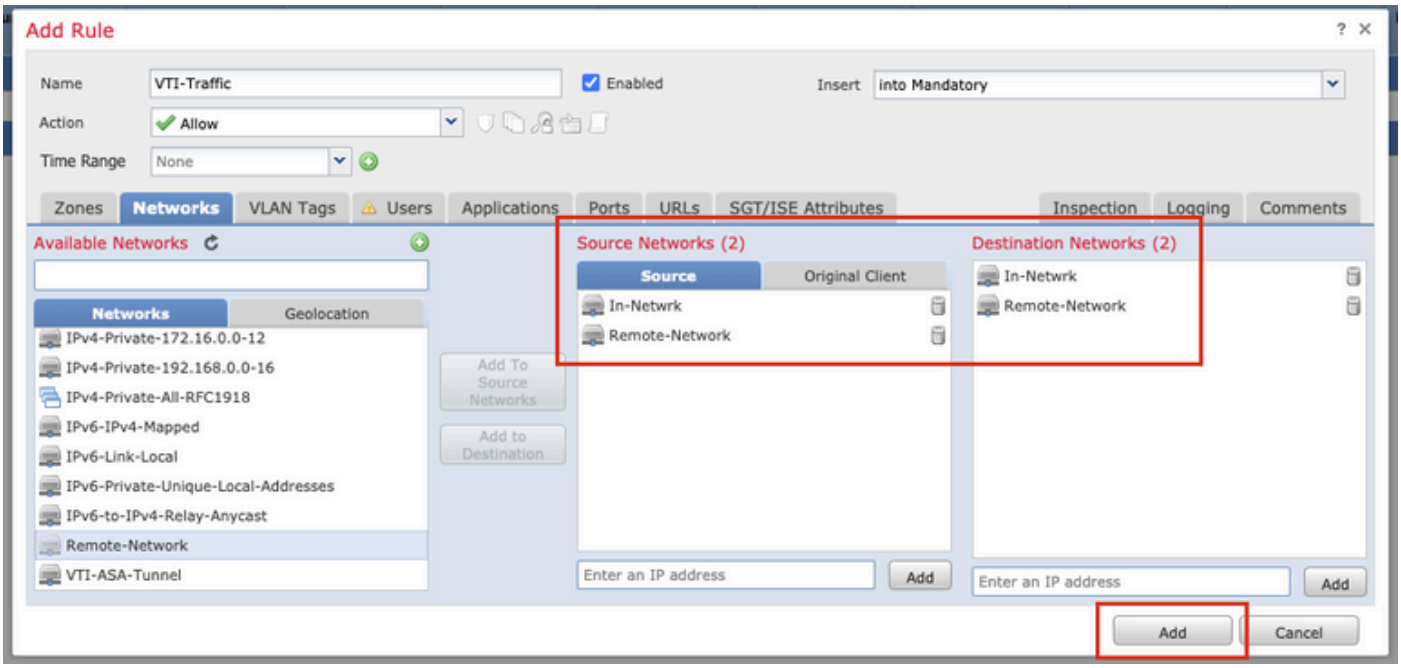
Zones source : In-Zone et Out-Zone

Zones de destination : zone de sortie et zone d'entrée

Réseaux sources : réseau interne et réseau distant

Réseaux de destination : réseau distant et réseau interne





Étape 18. Ajoutez le routage sur le tunnel VTI. Accédez à Périphériques > Gestion des périphériques. Modifiez le périphérique sur lequel le tunnel VTI est configuré.

Accédez à Static Route sous l'onglet Routing. Cliquez sur Add Route.

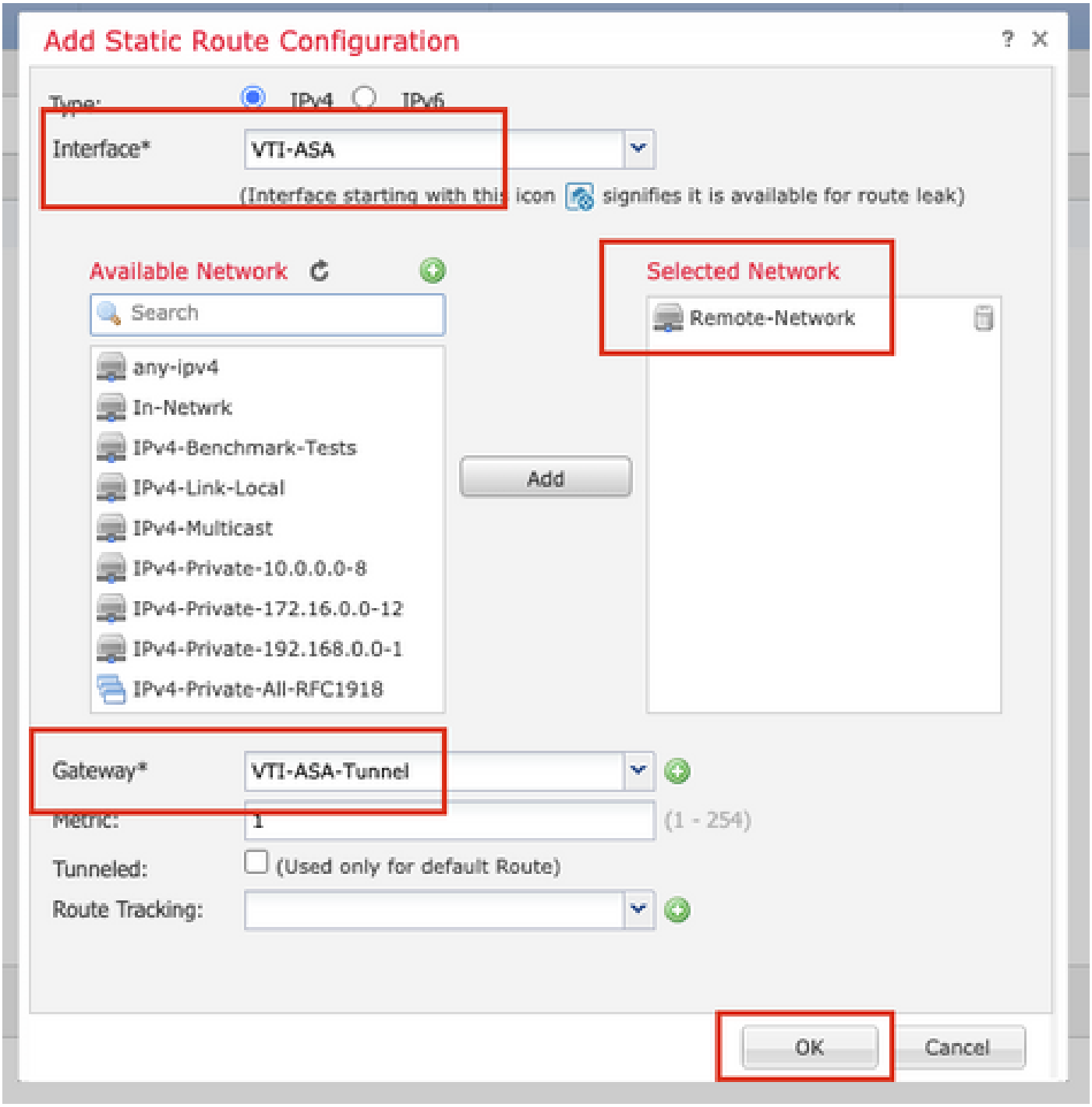
Fournissez l'interface, choisissez le réseau, fournissez la passerelle. Click OK.

Pour les besoins de cette démonstration :

Interface : VTI-ASA

Réseau : réseau distant

Passerelle : tunnel VTI-ASA



Étape 19. Accédez à Déployer > Déploiement. Choisissez le FTD vers lequel la configuration doit être déployée et cliquez sur Deploy.

Configuration envoyée à l'interface de ligne de commande FTD après un déploiement réussi :

<#root>

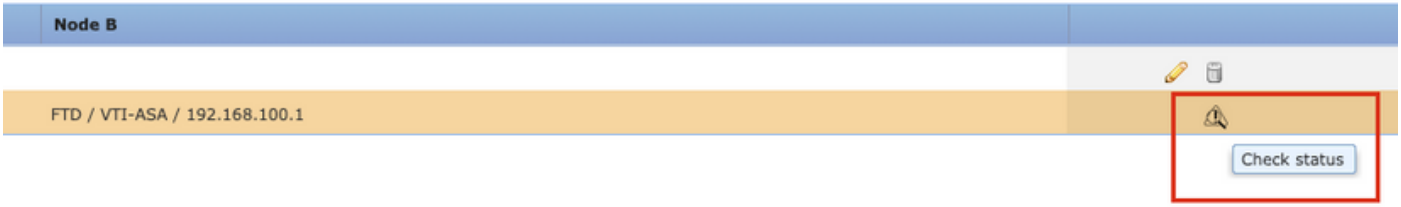
```
crypto ikev2 policy 1


 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 enable Outside


crypto ipsec ikev2 ipsec-proposal CSM_IP_1


 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1


 set ikev2 ipsec-proposal CSM_IP_1
 set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****


interface Tunnel1


 description VTI Tunnel with Extranet ASA

 nameif VTI-ASA


 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4

 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

Vérifier

À partir de FMC GUI

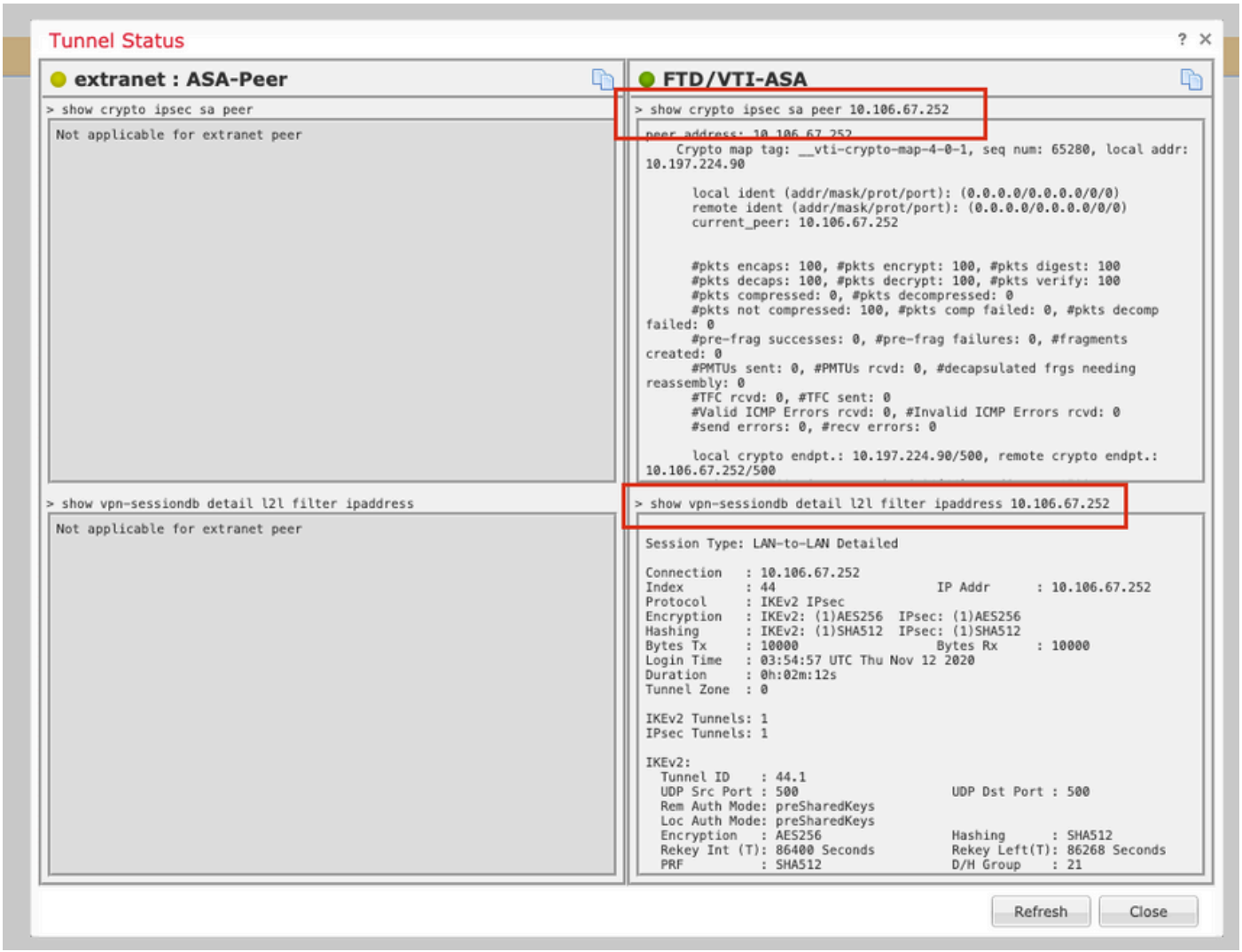
Cliquez sur l'option Check Status pour surveiller l'état en direct du tunnel VPN à partir de

l'interface utilisateur graphique elle-même



Cela inclut les commandes suivantes, extraites de l'interface de ligne de commande FTD :

- show crypto ipsec sa peer <Adresse IP homologue>
- show vpn-sessiondb detail l2l filter ipaddress <Adresse IP homologue>



À partir de FTD CLI

Ces commandes peuvent être utilisées à partir de l'interface de ligne de commande FTD pour afficher la configuration et l'état des tunnels VPN.

```
show running-config crypto
show running-config nat
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail l2l
```

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.