Configuration VPN site à site sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit comment configurer un VPN site à site sur Firepower Threat Defense (FTD) géré par FMC.

Conditions préalables

Exigences

Vous devez avoir connaissance de ces sujets :

- Compréhension de base du VPN
- Expérience avec Firepower Management Center
- Expérience avec la ligne de commande ASA

Composants utilisés

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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 lâ€™incidence possible des commandes.

Configuration

Commencez par la configuration sur FTD avec FirePower Management Center.

Étape 1. Définissez la topologie VPN.

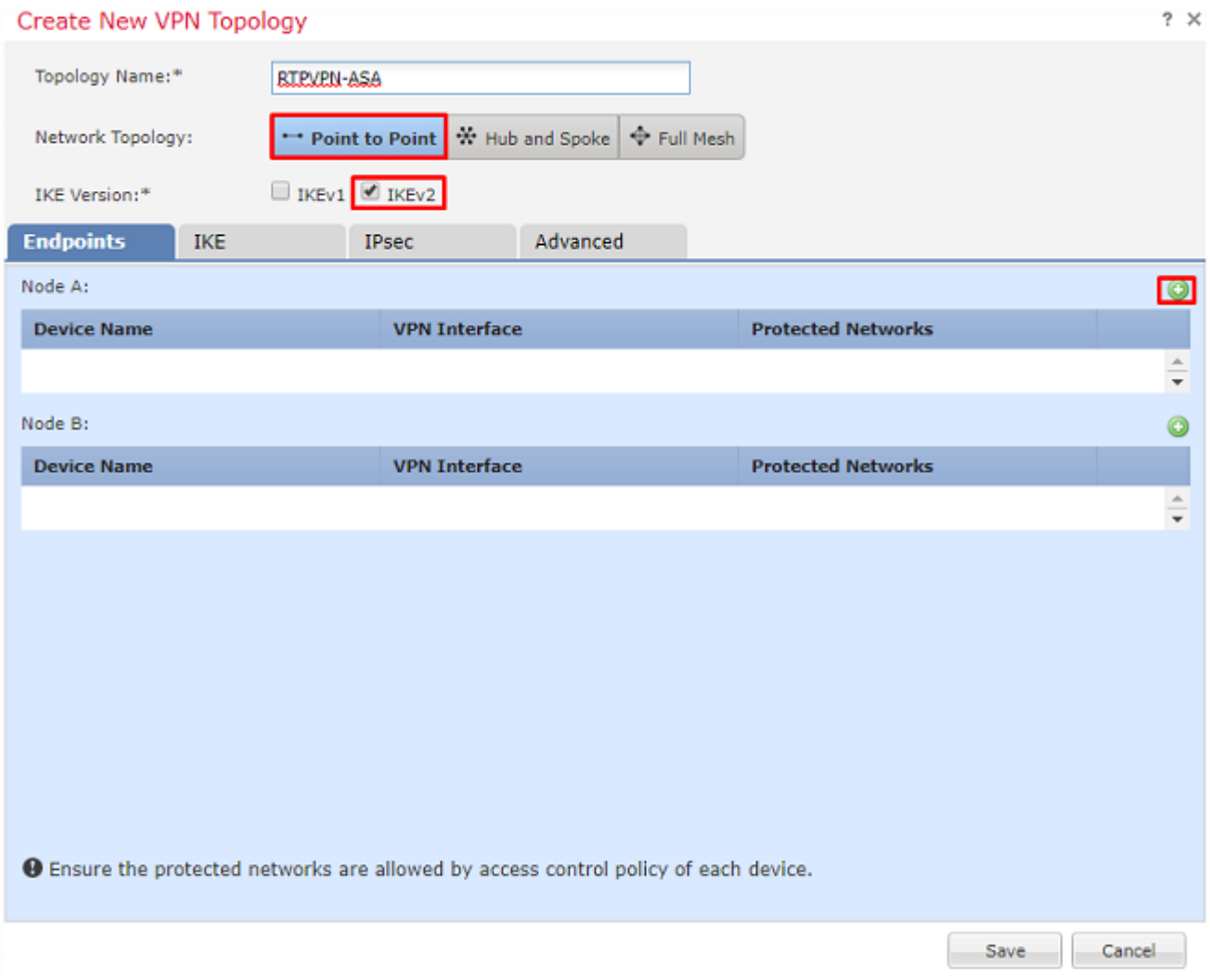
1. Accédez à **Devices > VPN > Site To Site.** Sous Add VPN**,** cliquez sur **Firepower Threat Defense Device**, comme illustré dans cette image.

2. La zone **Create New VPN Topology** s'affiche. Donnez au VPN un nom facilement identifiable.

Topologie du réseau : point à point

Version IKE : IKEv2

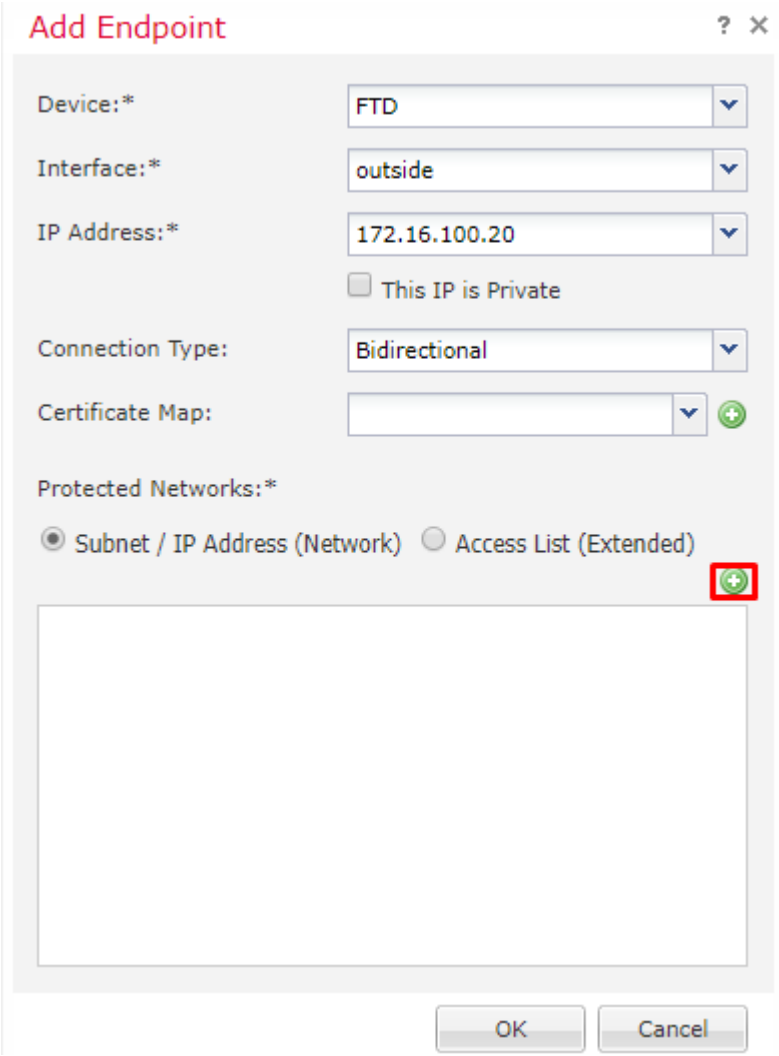
Dans cet exemple, lorsque vous sélectionnez des points d'extrémité, le noeud A est le FTD et le noeud B est l'ASA. Cliquez sur le bouton plus vert pour ajouter des périphériques à la topologie, comme illustré dans cette image.



3. Ajoutez le FTD comme premier point d'extrémité.

Choisissez l'interface sur laquelle une carte de chiffrement est placée. L'adresse IP doit être renseignée automatiquement à partir de la configuration du périphérique.

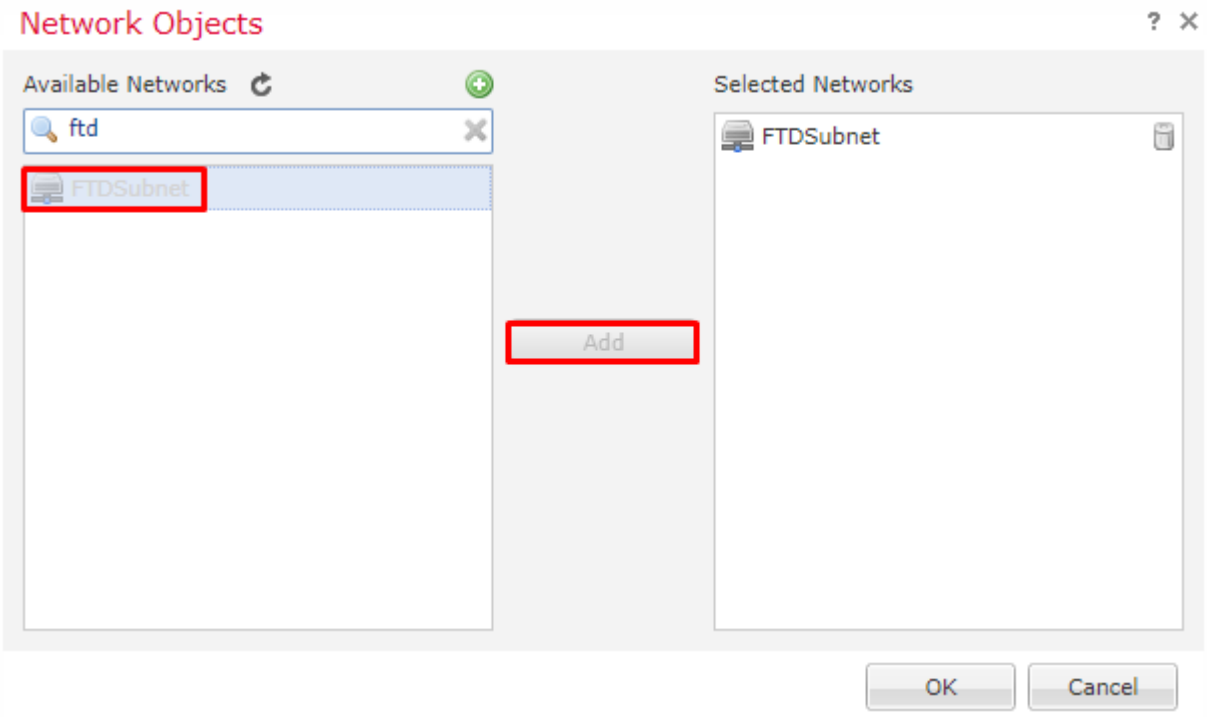
Cliquez sur le signe plus vert sous Réseaux protégés, comme illustré dans cette image, pour sélectionner les sous-réseaux qui doivent être chiffrés dans ce VPN.



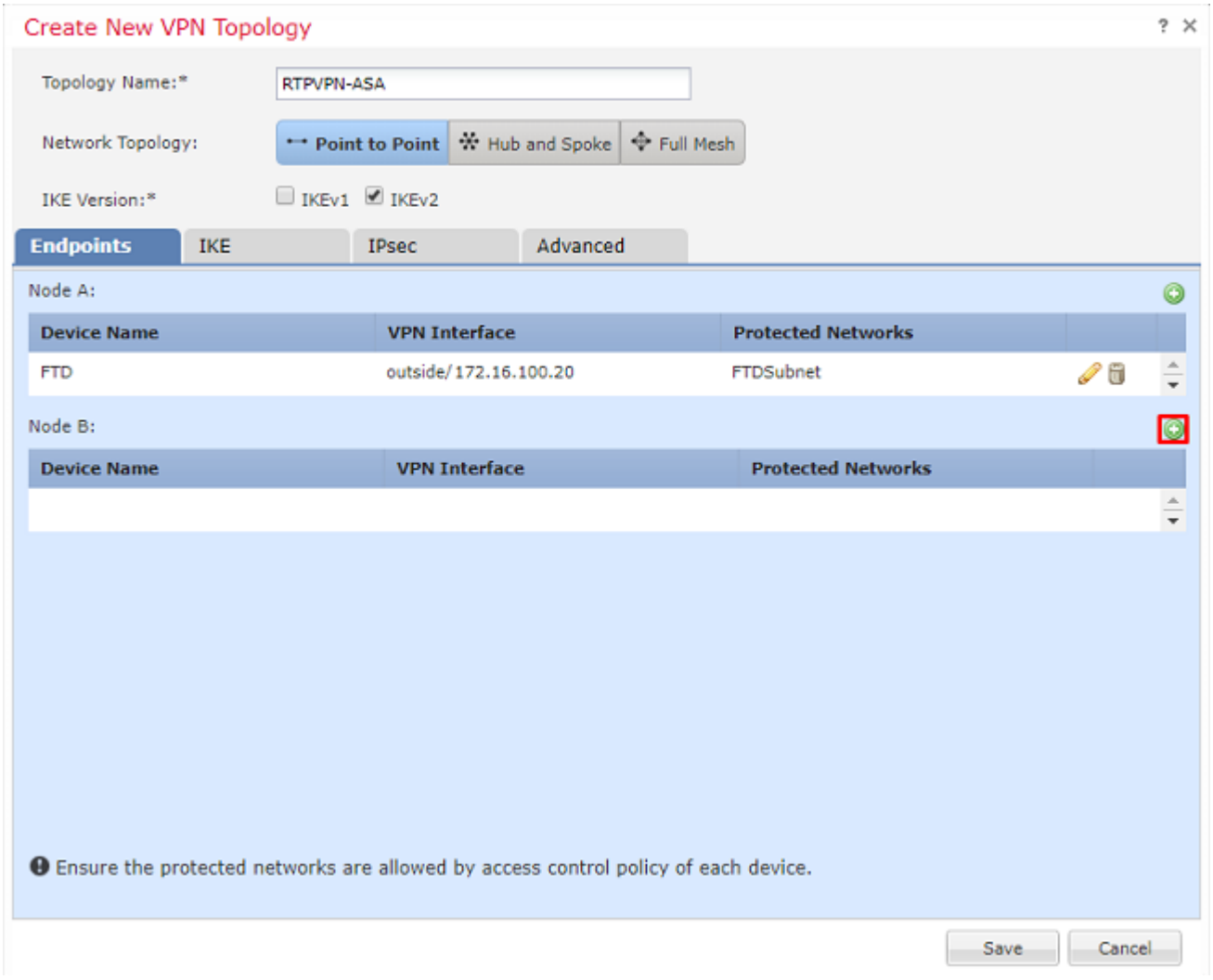
4. Cliquez sur le vert plus et un objet réseau est créé ici.

5. Ajoutez tous les sous-réseaux locaux au FTD qui doit être chiffré. Cliquez sur **Add** pour les déplacer vers les réseaux sélectionnés. Cliquez maintenant sur **OK**, comme illustré dans cette image.

FTDSubnet = 10.10.113.0/24

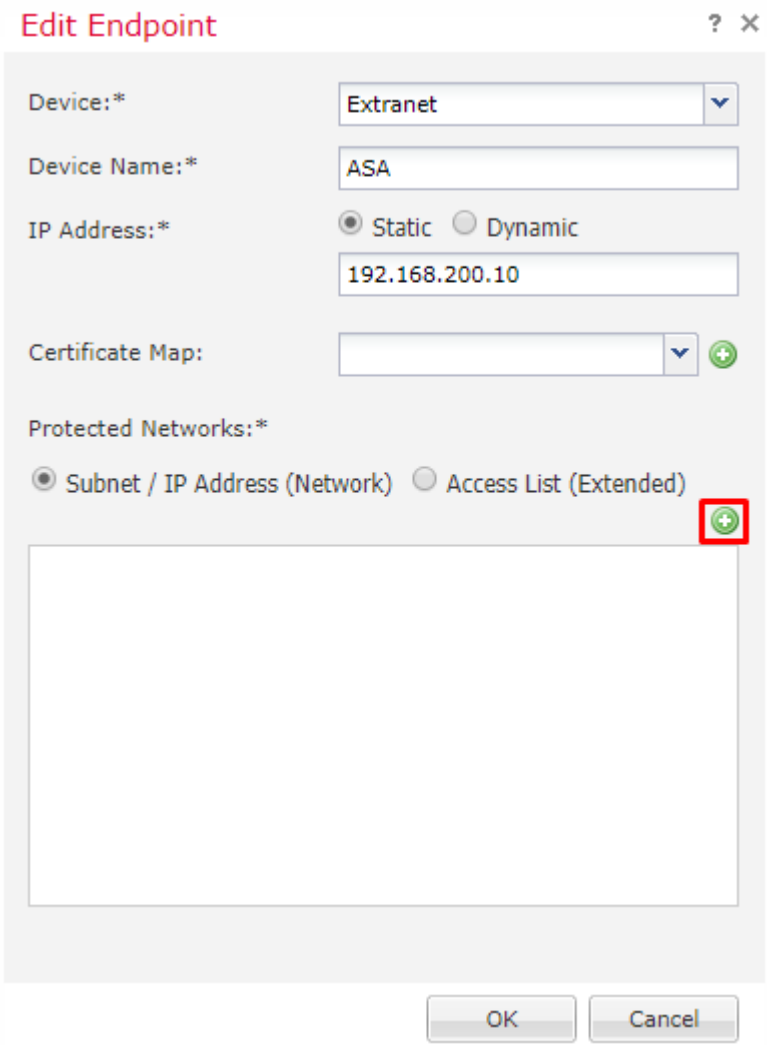


Noeud A : le point de terminaison (FTD) est terminé. Cliquez sur le signe plus vert pour le noeud B, comme illustré dans l'image.



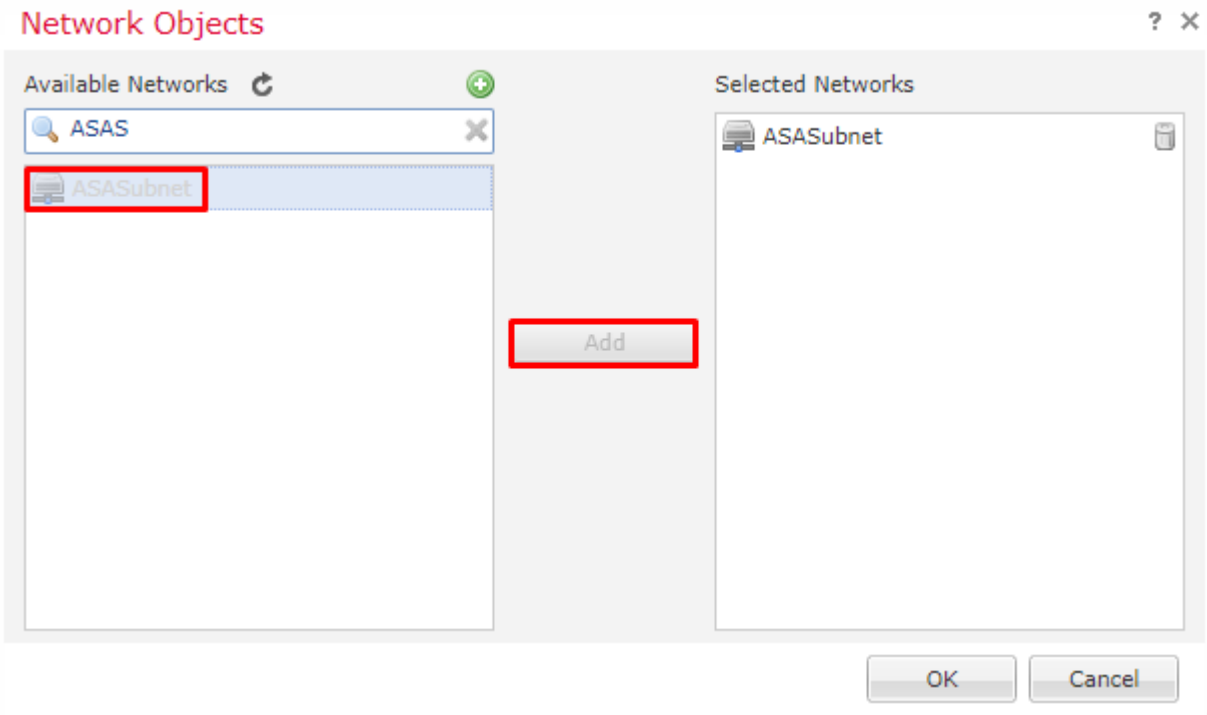
Le noeud B est un ASA. Les périphériques qui ne sont pas gérés par le FMC sont considérés comme des périphériques extranet.

6. Ajoutez un nom de périphérique et une adresse IP. Cliquez sur le signe plus vert pour ajouter des réseaux protégés, comme illustré dans l'image.



7. Comme le montre cette image, sélectionnez les **sous-réseaux ASA** qui doivent être chiffrés et ajoutez-les aux réseaux sélectionnés.

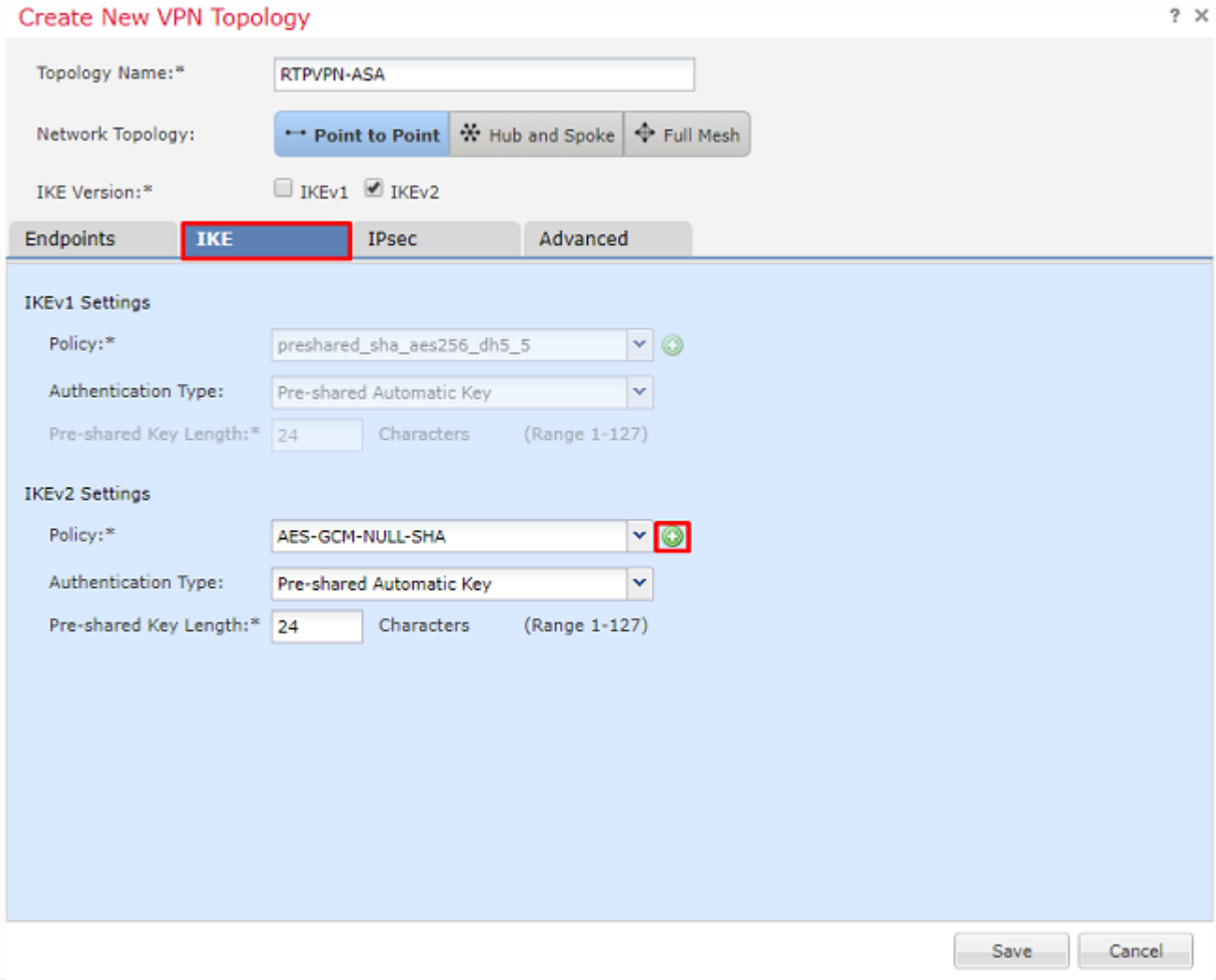
ASASubnet = 10.10.110.0/24



Étape 2. Configurer les paramètres IKE

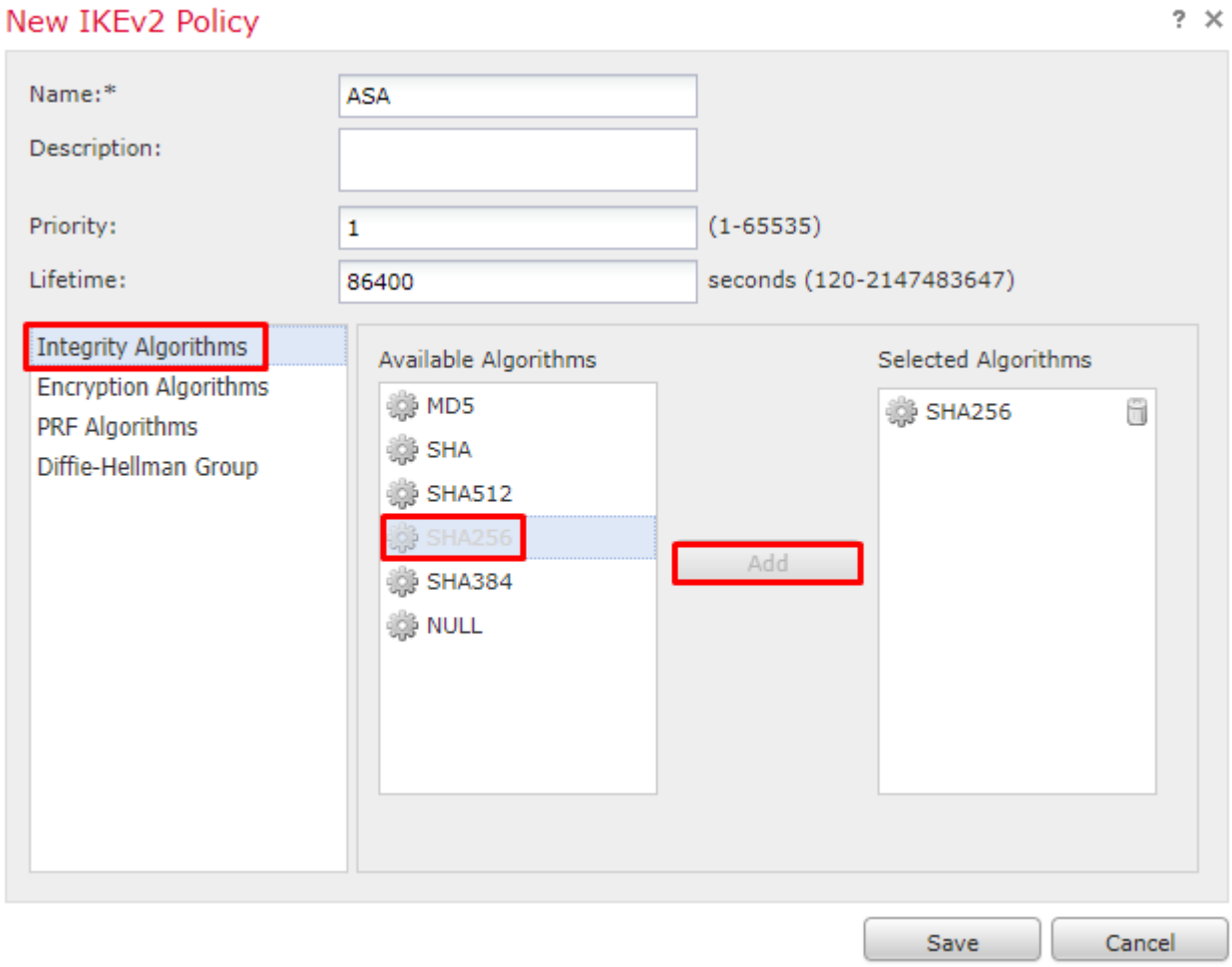
Les deux terminaux sont maintenant en place et passent par la configuration IKE/IPSEC.

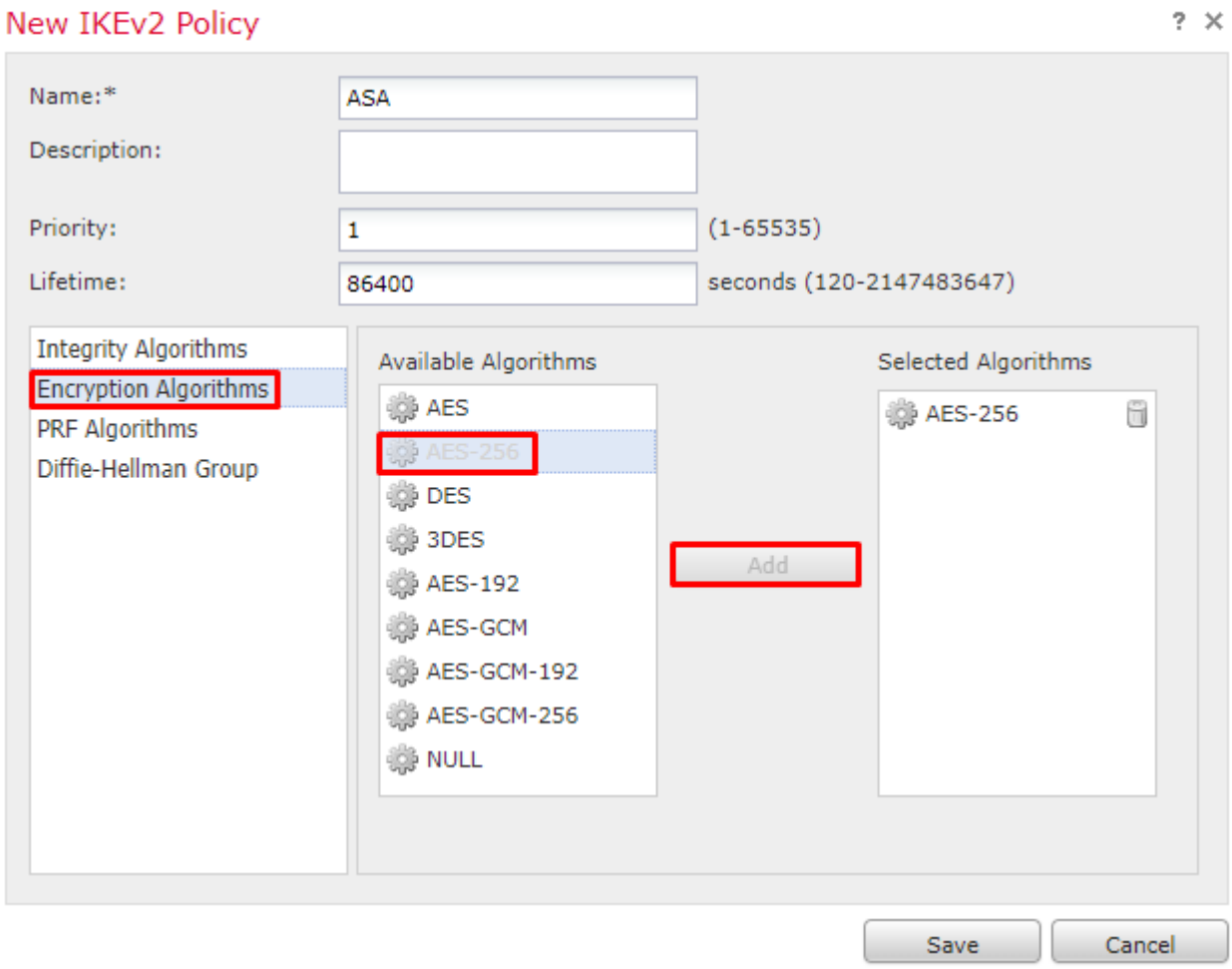
1. Sous l'onglet **IKE**, spécifiez les paramètres utilisés pour l'échange initial IKEv2. Cliquez sur le signe plus vert pour créer une nouvelle stratégie IKE, comme illustré dans l'image.

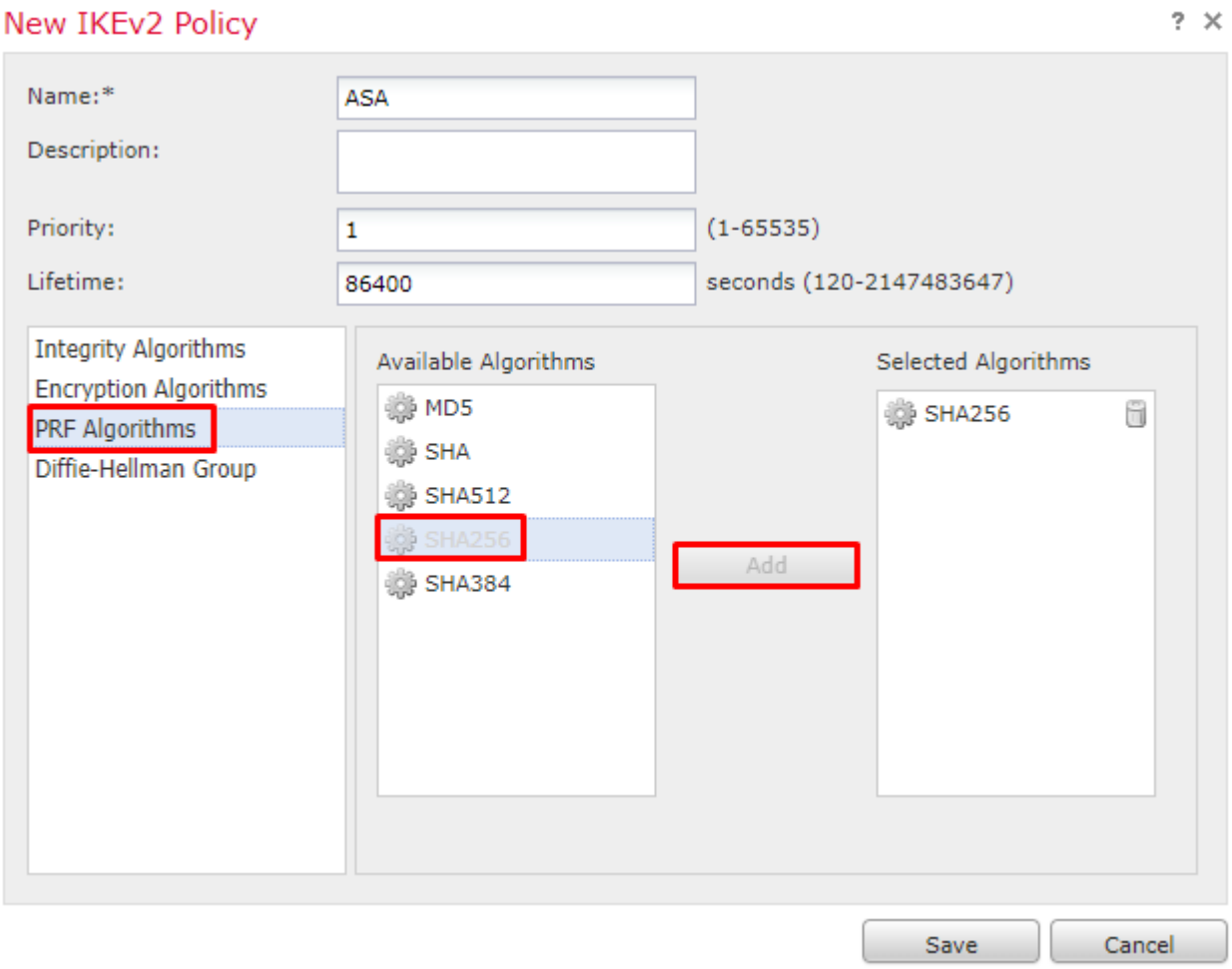


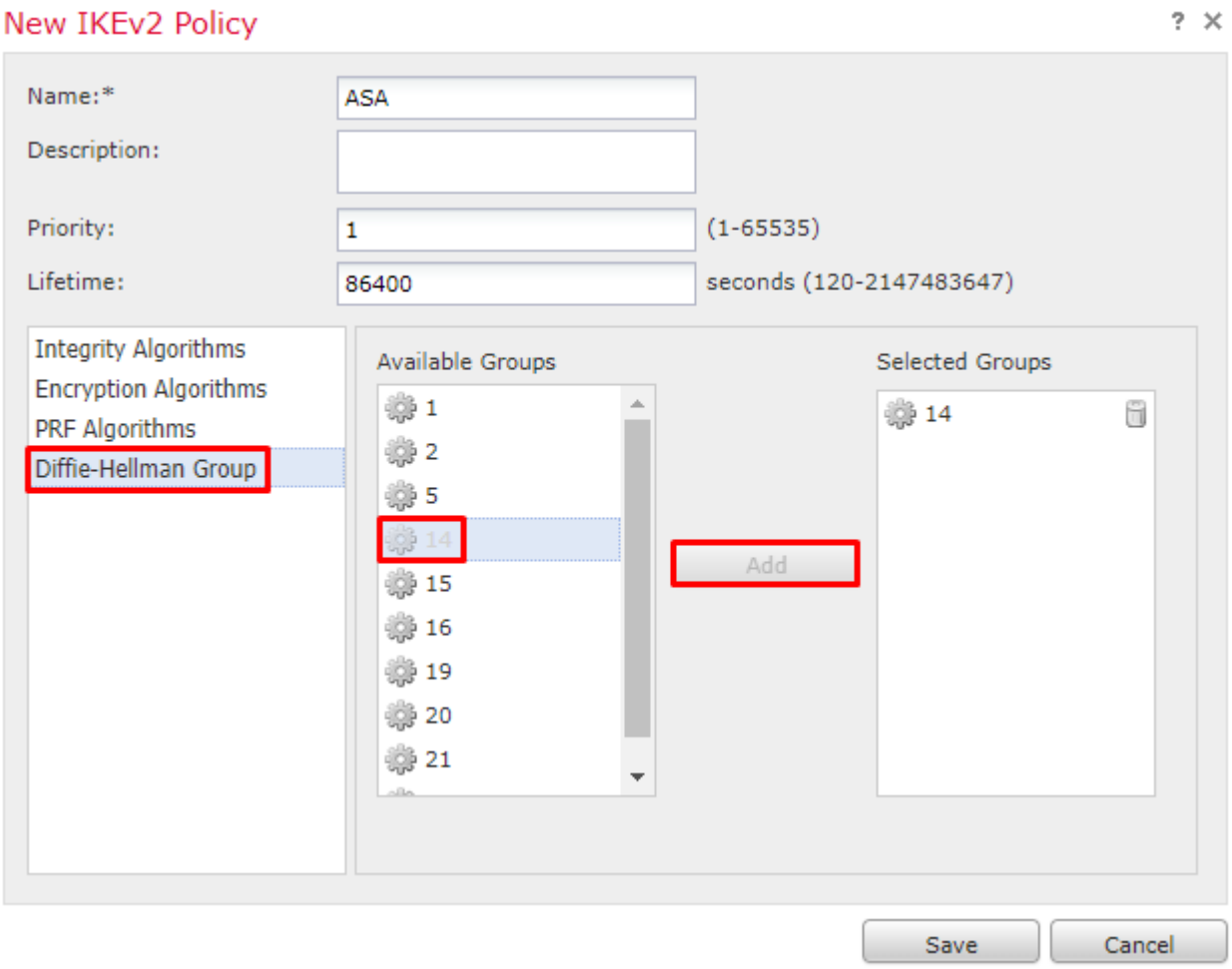
2. Dans la nouvelle stratégie IKE, spécifiez un numéro de priorité ainsi que la durée de vie de la phase 1 de la connexion. Ce document utilise ces paramètres pour l'échange initial : Integrity (SHA256), Encryption (AES-256), PRF (SHA256) et Diffie-Hellman Group (Group 14)

> **Remarque** : toutes les stratégies IKE du périphérique sont envoyées à l'homologue distant, quel que soit le contenu de la section de stratégie sélectionnée. La première stratégie IKE correspondant à l'homologue distant sera sélectionnée pour la connexion VPN. Choisissez la stratégie à envoyer en premier à l'aide du champ de priorité. La priorité 1 sera envoyée en premier.


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
NULL
Add
Selected Algorithms
SHA256
Save
Cancel

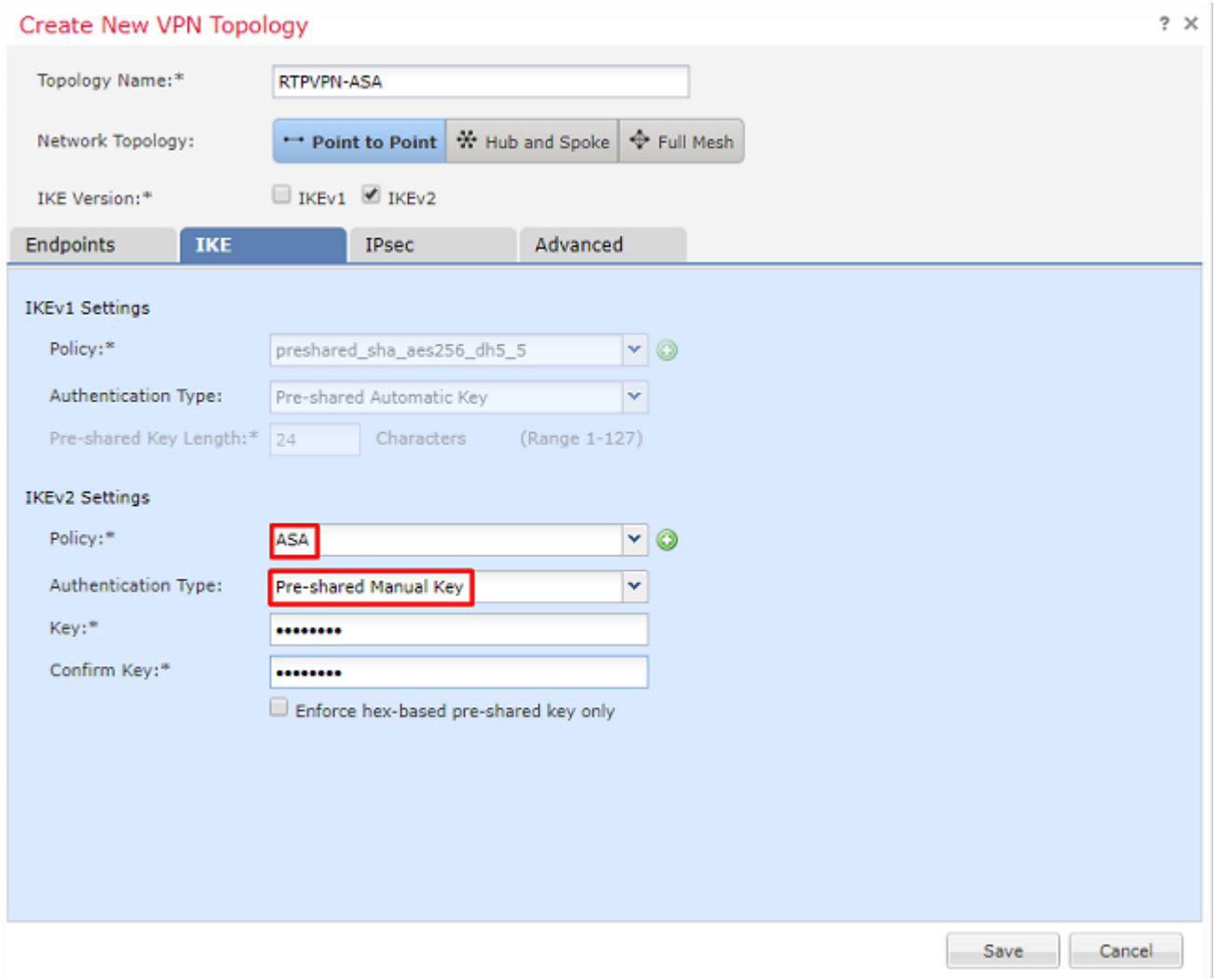

New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
Add
Selected Algorithms
SHA256
Save
Cancel



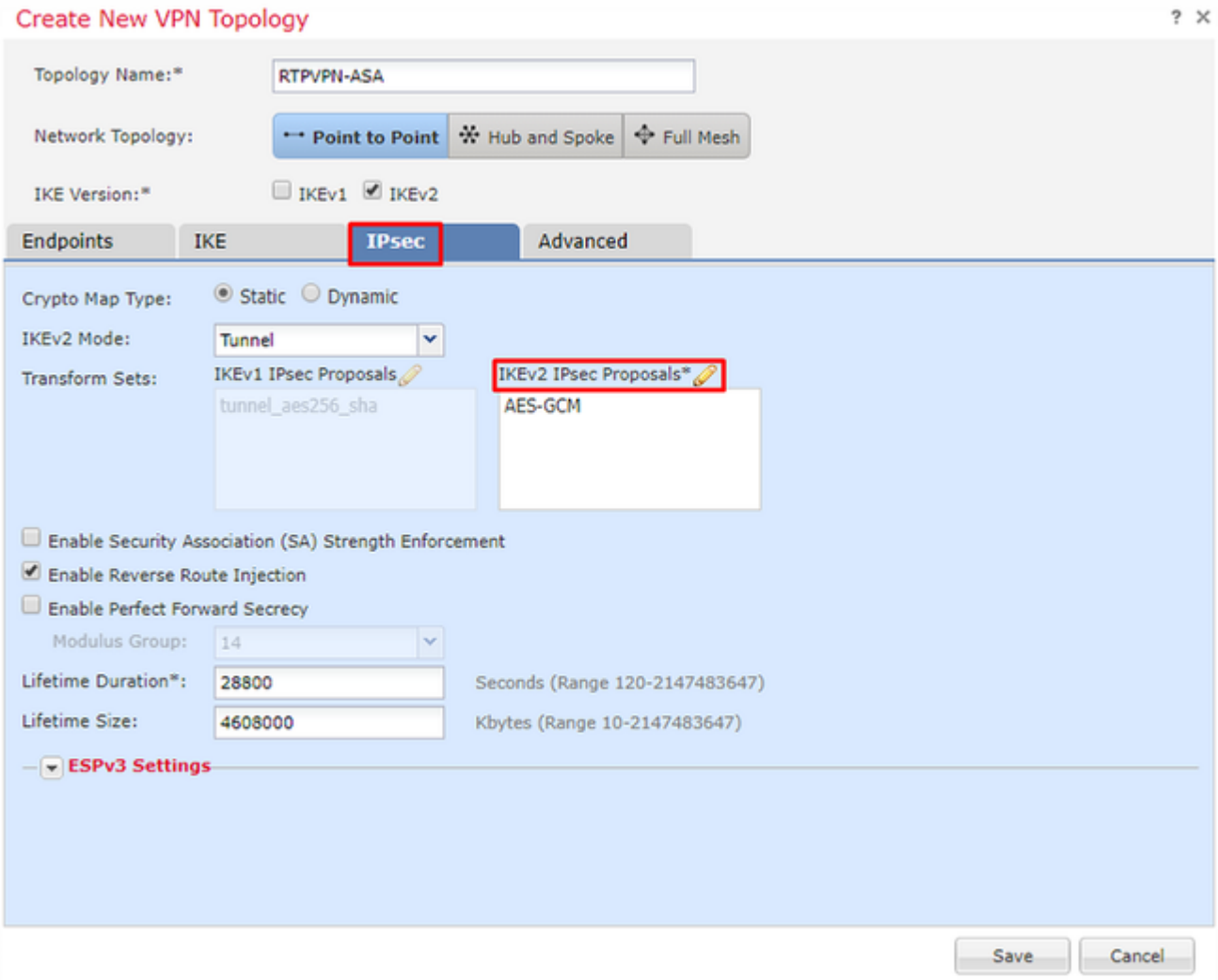
3. Une fois les paramètres ajoutés, sélectionnez cette stratégie et choisissez le **type d'authentification**.

4. Sélectionnez **pre-shared-key** manual. Pour ce document, le PSK cisco123 est utilisé.



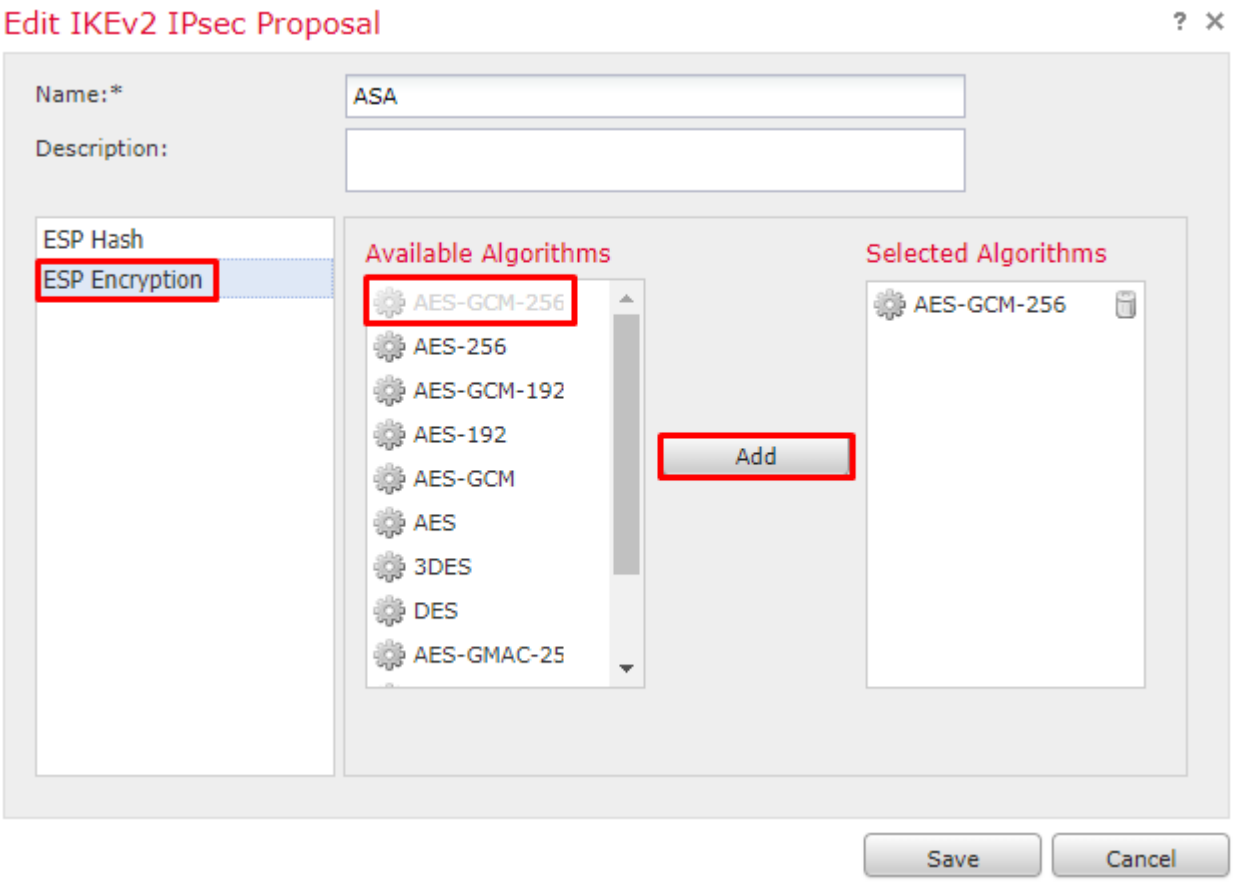
Étape 3. Configurer les paramètres IPsec

1. Sous **IPsec,** cliquez sur le crayon pour modifier le jeu de transformation et créer une nouvelle proposition IPsec, comme illustré dans cette image.

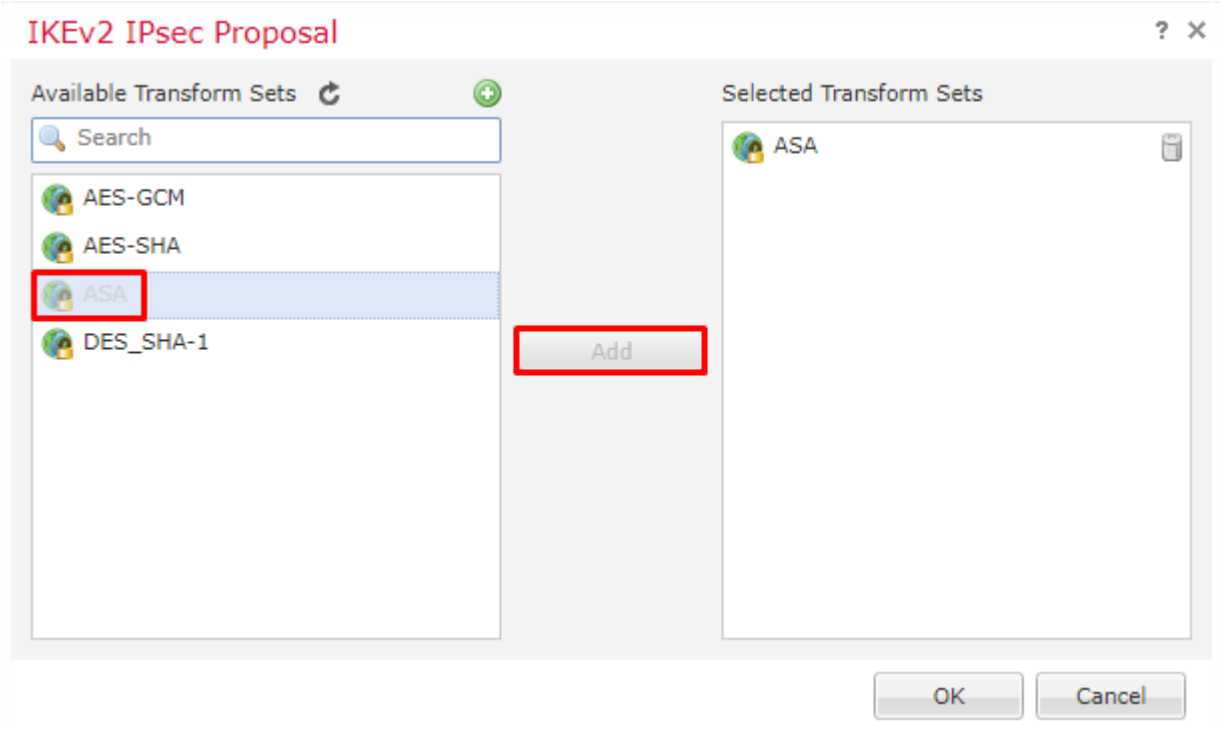


2. Afin de créer une nouvelle proposition IKEv2 IPsec, cliquez sur le plus vert et entrez les paramètres de phase 2.

Sélectionnez **ESP Encryption > AES-GCM-256**. Lorsque l'algorithme GCM est utilisé pour le chiffrement, un algorithme de hachage n'est pas nécessaire. Avec GCM, la fonction de hachage est intégrée.

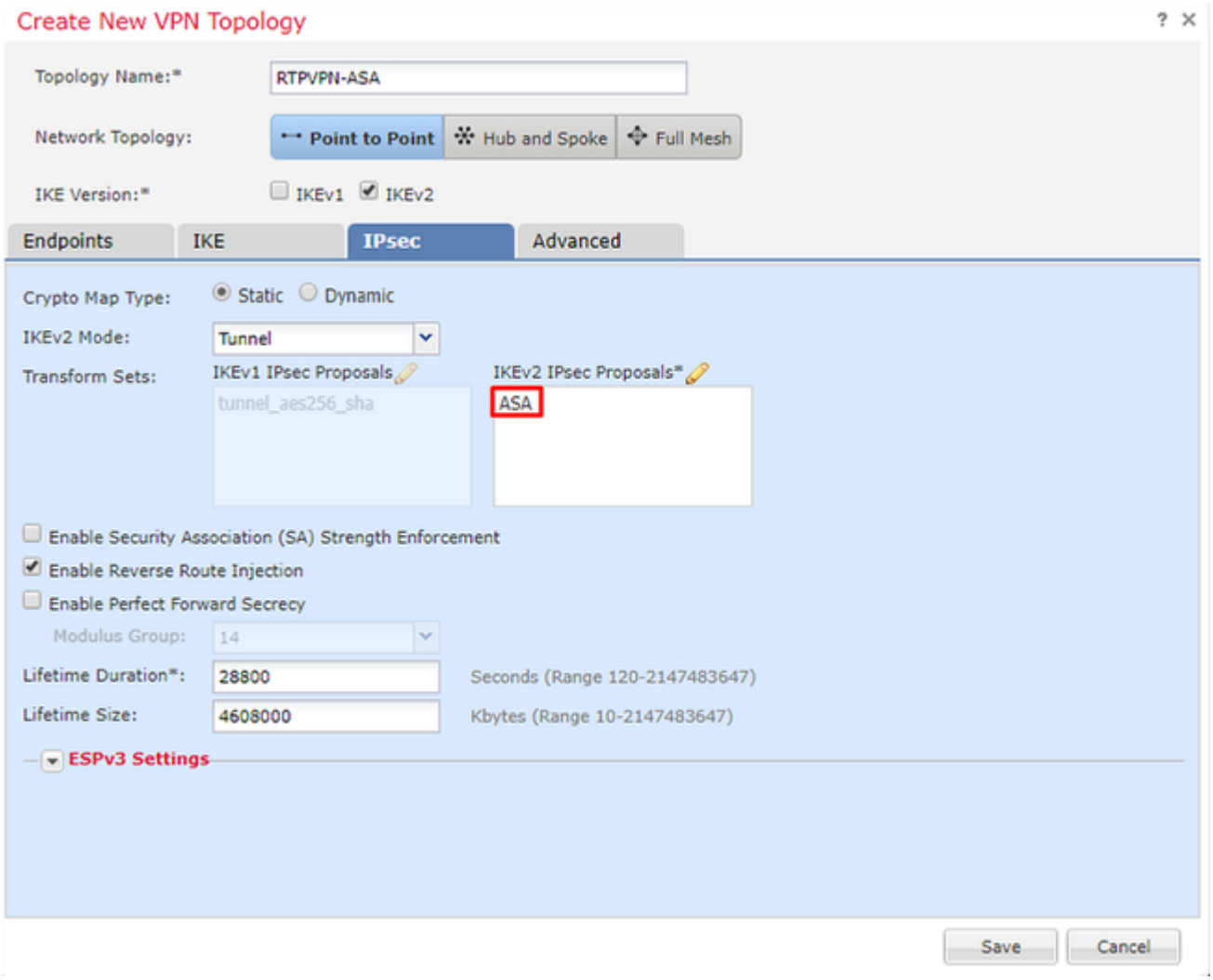


3. Une fois la nouvelle proposition IPsec créée, ajoutez-la aux jeux de transformation sélectionnés.



La proposition IPsec nouvellement sélectionnée est désormais répertoriée sous Propositions IPsec IKEv2.

Si nécessaire, la durée de vie de la phase 2 et le PFS peuvent être modifiés ici. Dans cet exemple, la durée de vie est définie par défaut et PFS est désactivé.

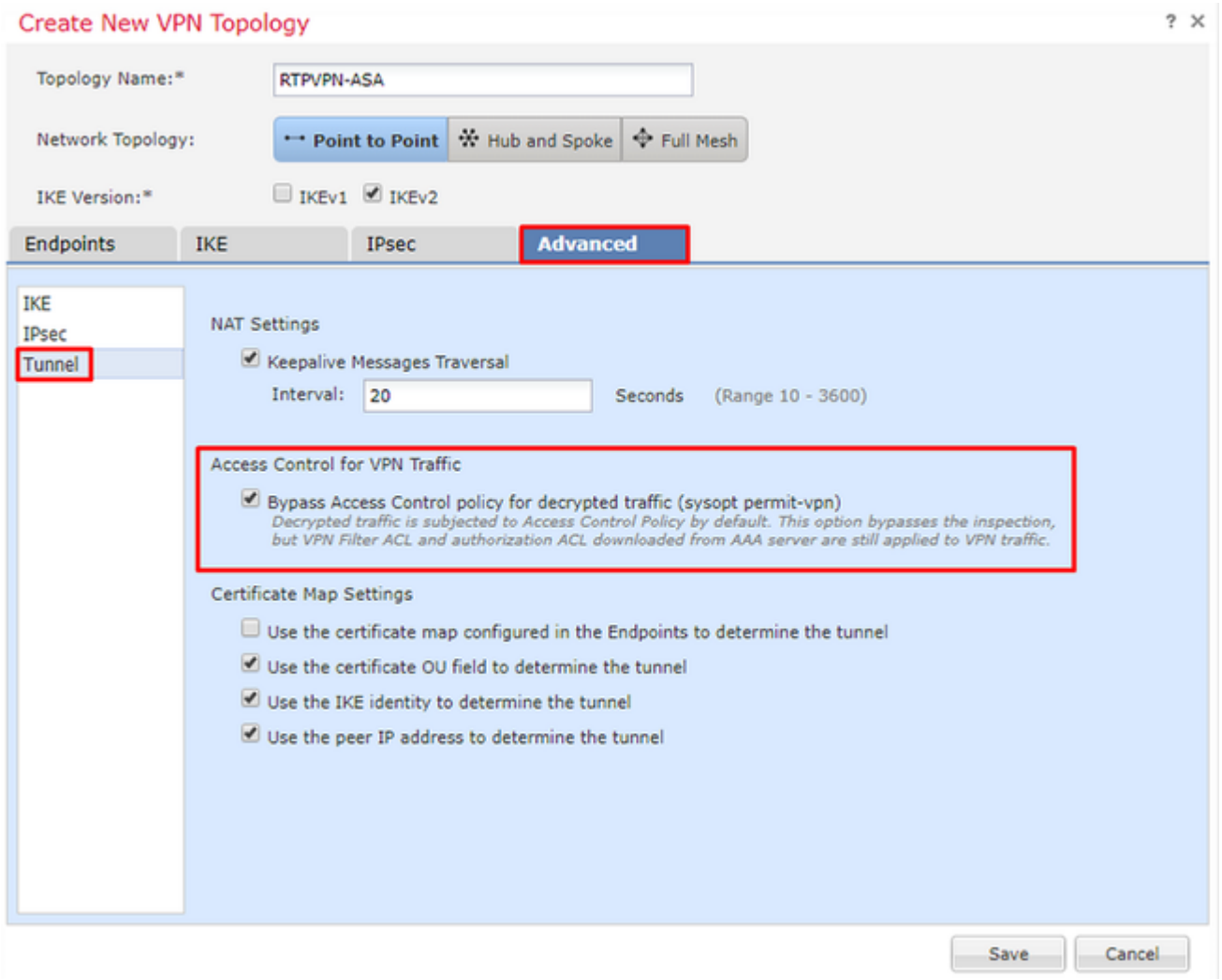


Facultatif : vous devez renseigner l'option Ignorer le contrôle d'accès ou Créer une stratégie de contrôle d'accès.

Étape 4. Contourner le contrôle d'accès.

En option, **sysopt permit-vpn** peut être activé sous **Advanced > Tunnel**.

Cela supprime la possibilité d'utiliser la politique de contrôle d'accès pour inspecter le trafic provenant des utilisateurs. Les filtres VPN ou les listes de contrôle dâ€™accès téléchargeables peuvent toujours être utilisés pour filtrer le trafic utilisateur. Il s'agit d'une commande globale qui s'appliquera à tous les VPN si cette case est cochée.

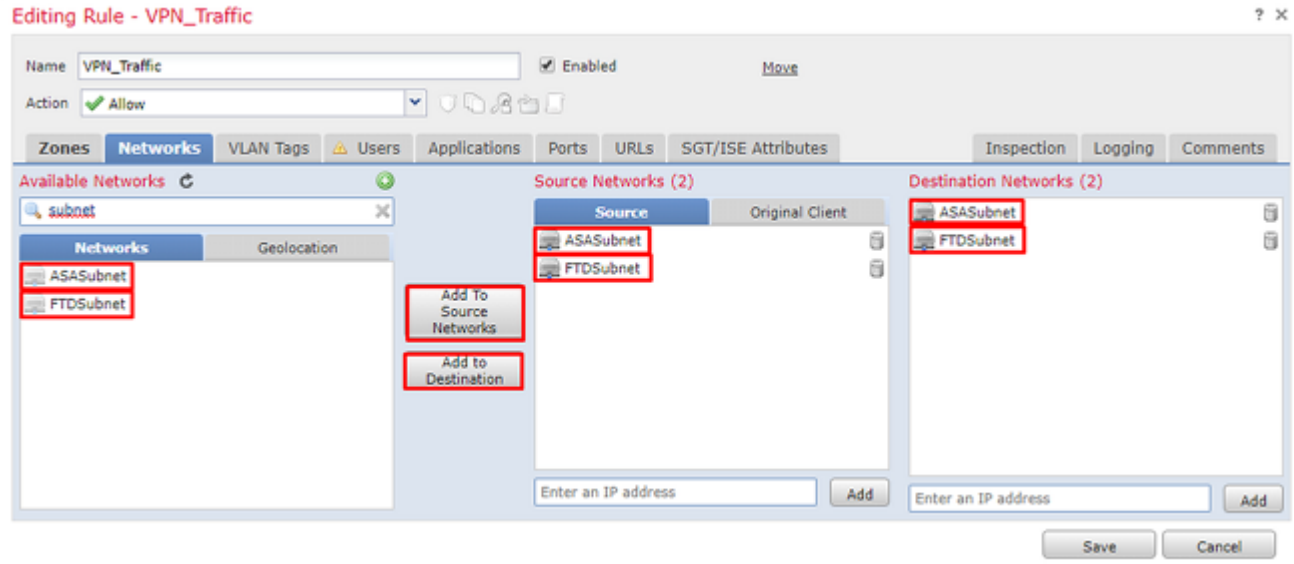


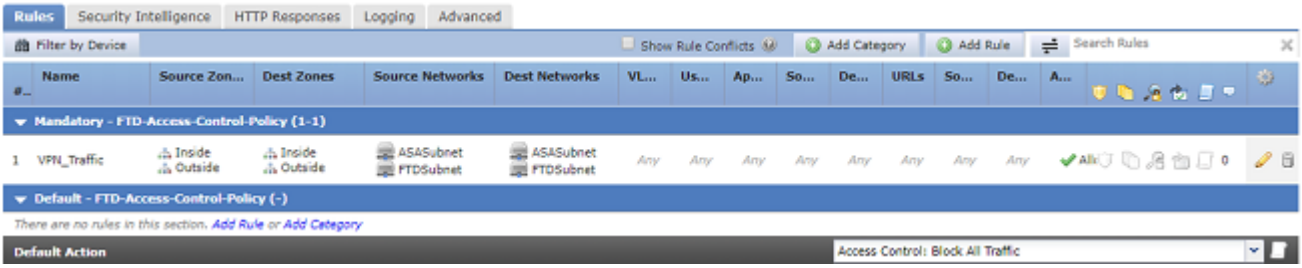
Si **sysopt permit-vpn** n'est pas activé alors une politique de contrôle d'accès doit être créée pour permettre le trafic VPN à travers le périphérique FTD. Si **sysopt permit-vpn** est activé, sautez la création d'une stratégie de contrôle d'accès.

Étape 5. Créez une politique de contrôle d'accès.

Sous Access Control Policies, accédez à **Policies > Access Control > Access Control** et sélectionnez la politique qui cible le périphérique FTD. Afin d'ajouter une règle, cliquez sur **Add Rule**, comme montré dans l'image ici.

Le trafic doit être autorisé du réseau interne vers le réseau externe et du réseau externe vers le réseau interne. Créez une règle pour les deux ou deux règles pour les séparer. Dans cet exemple, une règle est créée pour effectuer les deux opérations.

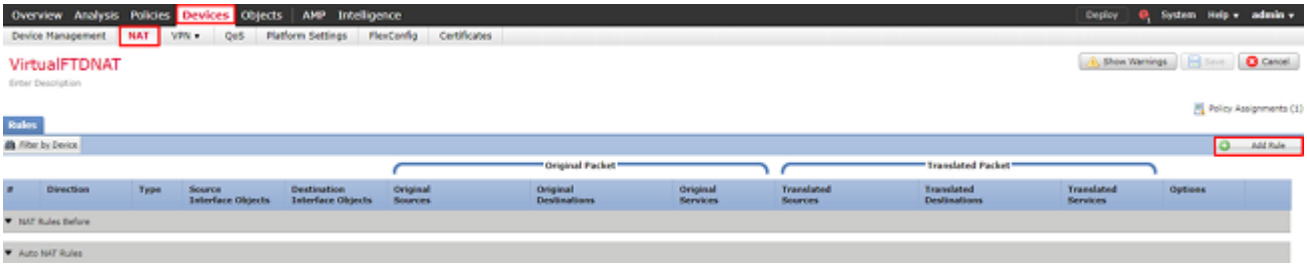




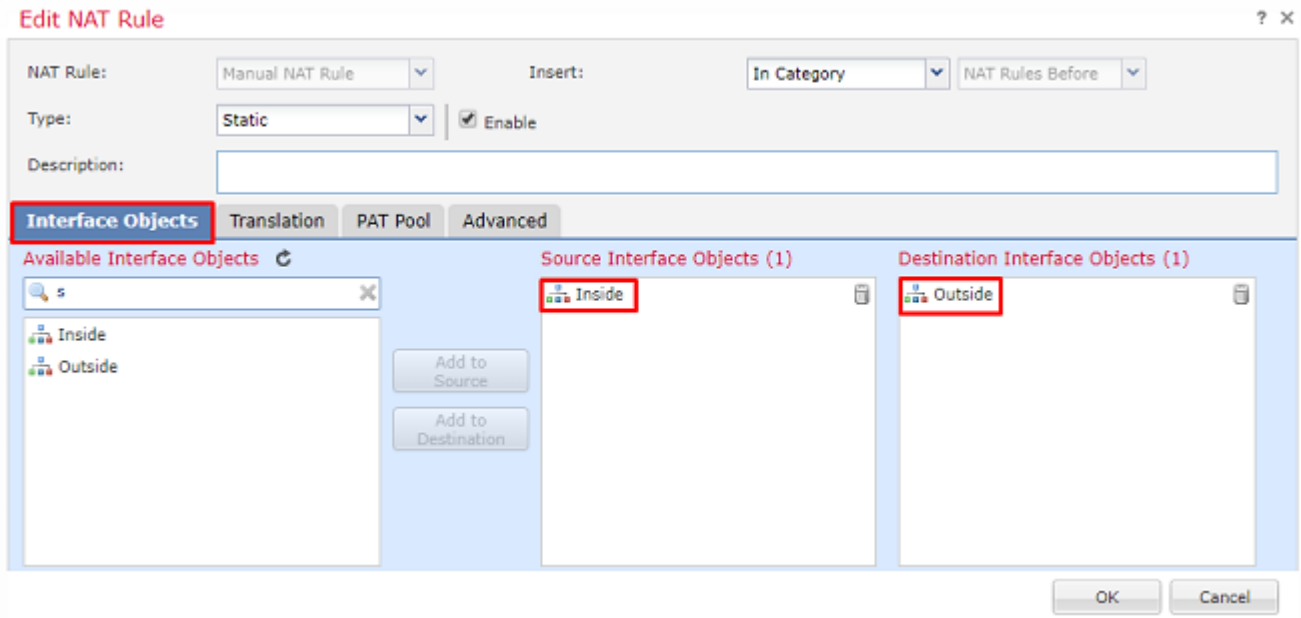
Étape 6. Configurez l'exemption NAT.

Configurez une instruction d'exemption NAT pour le trafic VPN. Une exemption NAT doit être en place pour empêcher le trafic VPN d'atteindre une autre instruction NAT et de traduire incorrectement le trafic VPN.

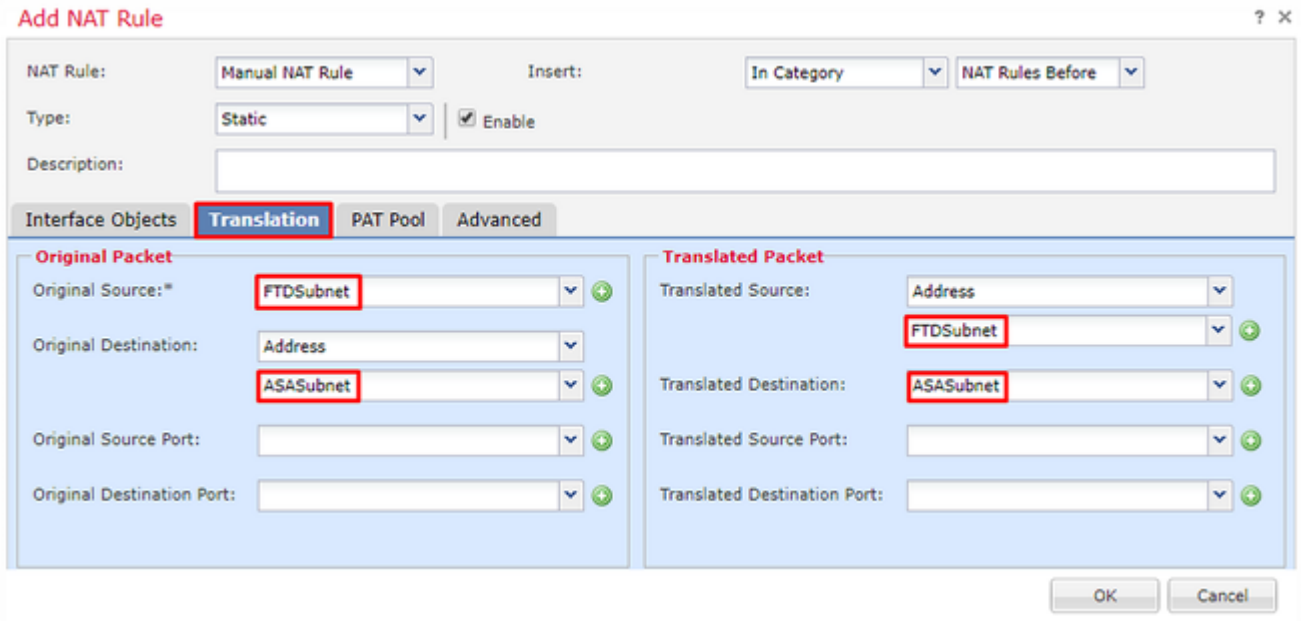
1. Accédez à **Périphériques > NAT**, sélectionnez la politique NAT qui cible le FTD. Créez une nouvelle règle lorsque vous cliquez sur le bouton **Ajouter une règle**.



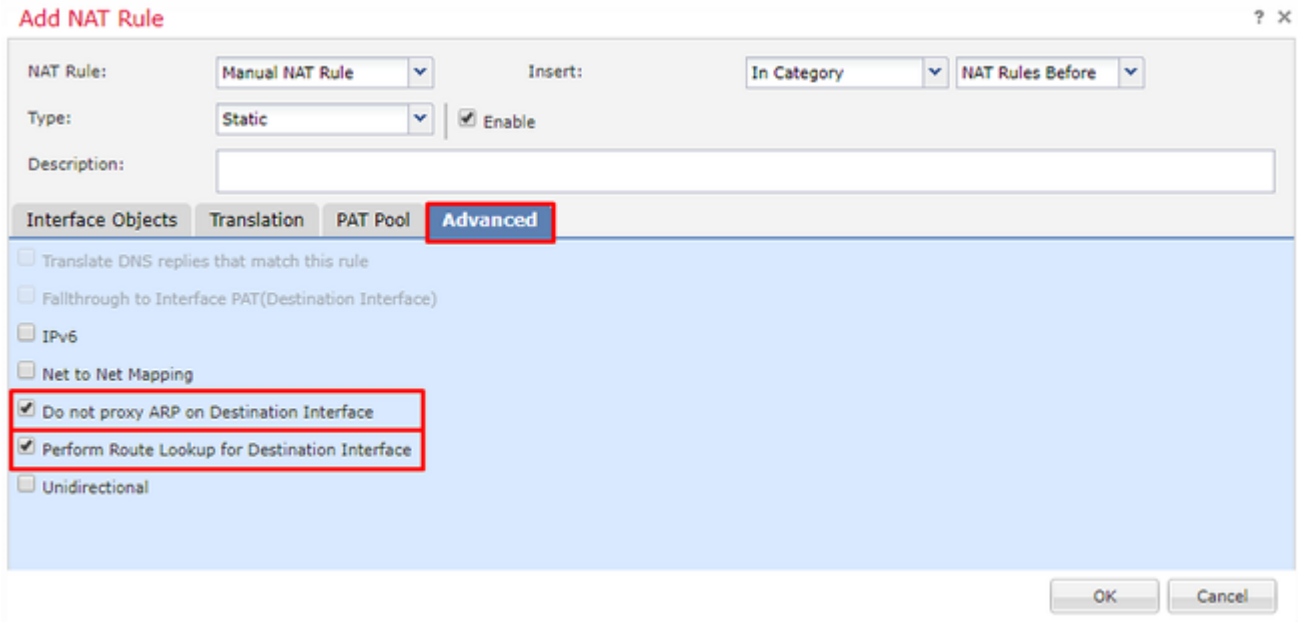
2. Créez une nouvelle règle NAT statique manuelle. Référencez les interfaces interne et externe.



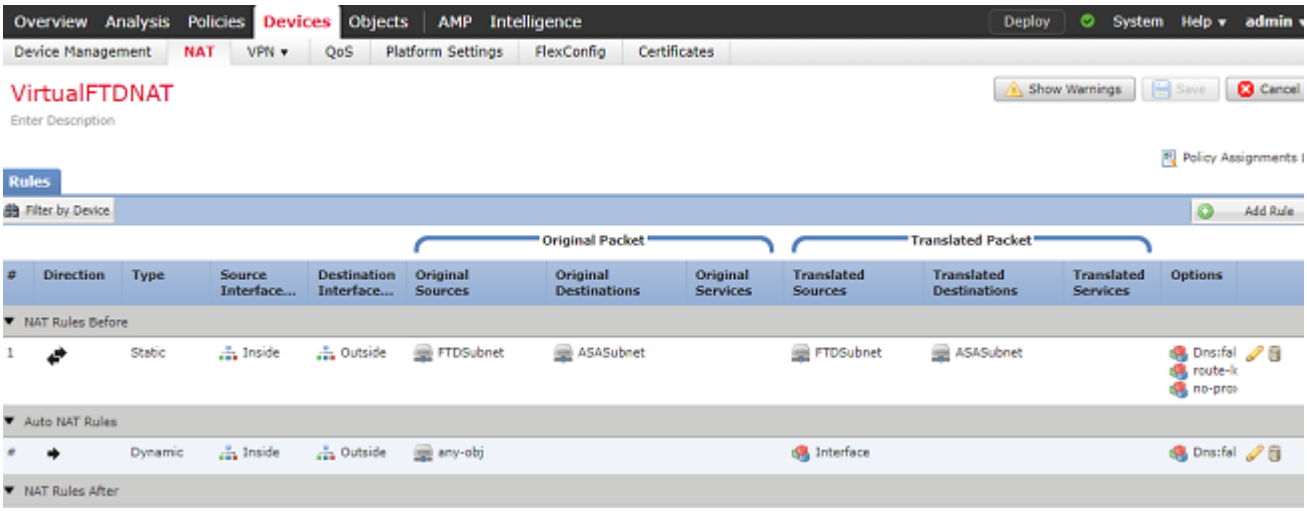
3. Sous l'onglet **Traduction**, sélectionnez les sous-réseaux source et de destination. Comme il s'agit d'une règle d'exemption NAT, faites en sorte que la source/destination d'origine et la source/destination traduite soient identiques, comme illustré dans cette image :



4. Enfin, passez à l'onglet **Advanced** et activez no-proxy-arp et route-lookup.



5. Enregistrez cette règle et examinez les résultats finaux dans la liste NAT.



6. Une fois la configuration terminée, enregistrez-la et déployez-la sur le FTD.

Étape 7. Configurer l'ASA.

1. Activez IKEv2 sur l'interface externe de l'ASA :

```
Crypto ikev2 enable outside
```

2. Créez la stratégie IKEv2 qui définit les mêmes paramètres configurés sur le FTD :

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
```

```
 Lifetime seconds 86400
```

3. Créez une stratégie de groupe autorisant le protocole ikev2 :

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
 Vpn-tunnel-protocol ikev2
```

4. Créez un groupe de tunnels pour l'adresse IP publique FTD homologue. Faites référence à la stratégie de groupe et spécifiez la clé pré-partagée :

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco123
 ikev2 remote-authentication pre-shared-key cisco123
```

5. Créez une liste de contrôle dâ€™accès définissant le trafic à chiffrer : (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSubnet
 Subnet 10.10.113.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Créez une proposition ipsec ikev2 faisant référence aux algorithmes spécifiés sur le FTD :

```
Crypto ipsec ikev2 ipsec-proposal FTD
 Protocol esp encryption aes-gcm-256
```

7. Créez une entrée de crypto-carte qui lie la configuration :

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. Créez une instruction dâ€™exemption NAT qui empêchera le trafic VPN dâ€™être NATTED par le

pare-feu :

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-p
```

Vérifier

> **Remarque** : actuellement, il n'y a aucun moyen de vérifier l'état du tunnel VPN à partir du FMC. Il existe une demande d'amélioration pour cette fonctionnalité CSCvh7603.

Tentative d'initialisation du trafic via le tunnel VPN. Avec l'accès à la ligne de commande de l'ASA ou du FTD, cela peut être fait avec la commande packet tracer. Lorsque vous utilisez la commande packet-tracer pour activer le tunnel VPN, vous devez l'exécuter deux fois pour vérifier que le tunnel est activé. La première fois que la commande est émise, le tunnel VPN est arrêté, donc la commande packet-tracer échouera avec VPN encrypt DROP. N'utilisez pas l'adresse IP interne du pare-feu comme adresse IP source dans le traceur de paquets, car cela échouera toujours.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc out
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: Inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Pour surveiller l'état du tunnel, accédez à l'interface de ligne de commande du FTD ou de l'ASA.

À partir de l'interface de ligne de commande FTD, vérifiez les phases 1 et 2 à l'aide de cette commande :

Show crypto ikev2 sa

<#root>

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
  9528731 172.16.100.20/500                              192.168.200.10/500

 READY

   INITIATOR
```

```
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/118 sec
Child sa: local selector
```

10.10.113.0/0 - 10.10.113.255/65535

```
          remote selector
```

10.10.110.0/0 - 10.10.110.255/65535

```
          ESP spi in/out:
```

0x66be357d/0xb74c8753

Dépannage et débogage

Problèmes de connectivité initiaux

Lors de la construction d'un VPN, deux parties négocient le tunnel. Par conséquent, il est préférable d'obtenir les deux côtés de la conversation lorsque vous dépannez tout type de défaillance de tunnel. Un guide détaillé sur la façon de déboguer les tunnels IKEv2 peut être trouvé ici : Comment déboguer les VPN IKEv2

La cause la plus fréquente des pannes de tunnel est un problème de connectivité. La meilleure façon de déterminer ceci est de prendre des captures de paquets sur le périphérique. Utilisez cette commande pour effectuer des captures de paquets sur le périphérique :

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Une fois la capture en place, essayez d'envoyer le trafic sur le VPN et vérifiez le trafic bidirectionnel dans la capture de paquets.

Examinez la capture de paquets avec cette commande :

show cap capout

```
firepower# show cap capout

4 packets captured

   1: 11:51:12.059628       172.16.100.20.500 > 192.168.200.10.500:  udp 690
   2: 11:51:12.065243       192.168.200.10.500 > 172.16.100.20.500:  udp 619
   3: 11:51:12.066692       172.16.100.20.500 > 192.168.200.10.500:  udp 288
   4: 11:51:12.069835       192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

Problèmes spécifiques au trafic

Les problèmes de trafic courants que vous rencontrez sont les suivants :

- Problèmes de routage derrière le FTD : le réseau interne ne peut pas router les paquets vers les adresses IP et les clients VPN attribués.
- Listes de contrôle d'accès bloquant le trafic.
- Traduction d'adresses réseau non contournée pour le trafic VPN.

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

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.