Configuration VPN site à site sur FTD géré par FMC

Contenu

Introduction

Ce document fournit un exemple de configuration pour le VPN site à site sur Firepower Threat Defense (FTD) géré par FMC.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

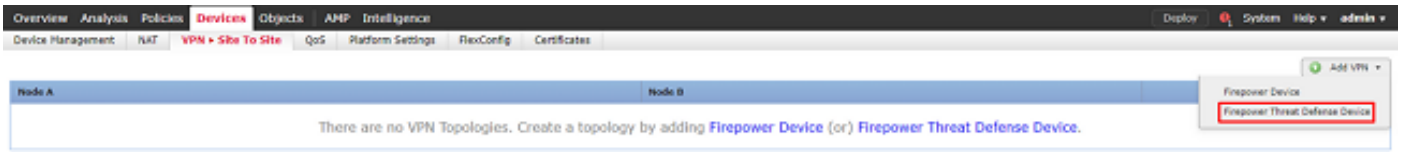
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Commencez par configurer FTD avec FirePower Management Center.

Étape 1. Définissez la topologie VPN.

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

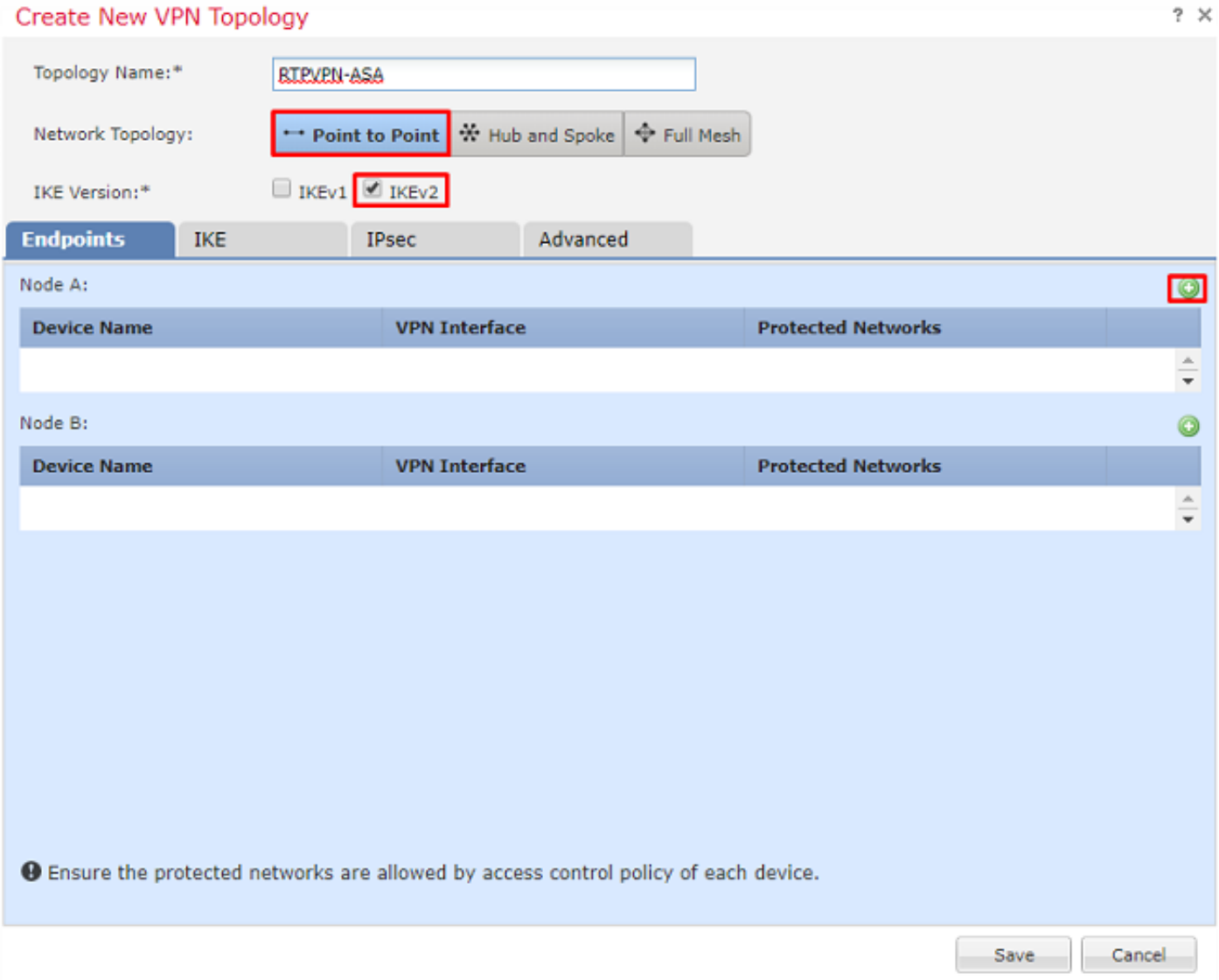


2. **La** zone **Créer une topologie VPN** apparaît. Donnez à VPN un nom facilement identifiable.

Topologie du réseau : Pointez vers Point

Version IKE : IKEv2

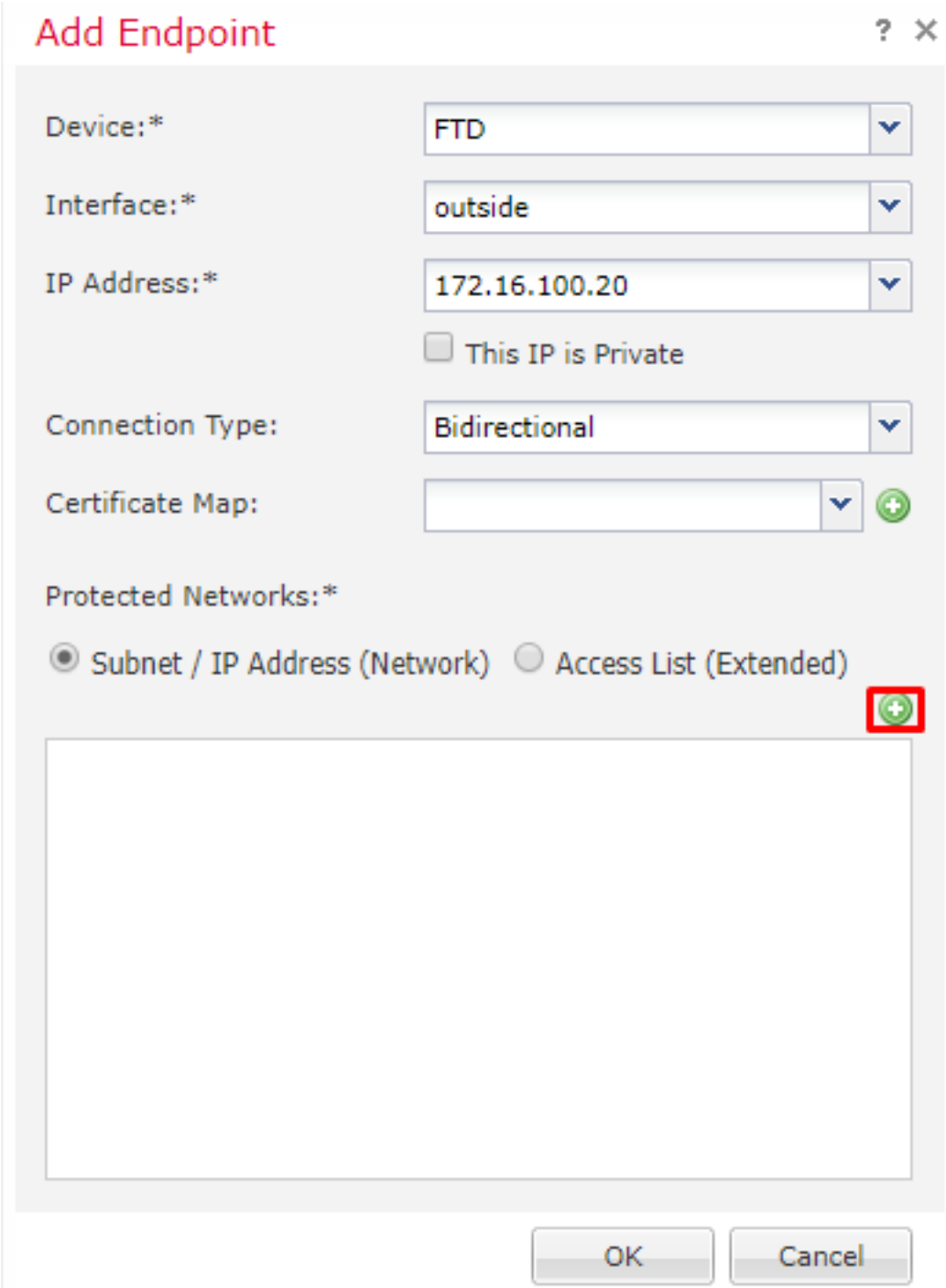
Dans cet exemple, lorsque vous sélectionnez des terminaux, le noeud A est le FTD et le noeud B est l'ASA. Cliquez sur le bouton vert plus pour ajouter des périphériques à la topologie, comme illustré dans cette image.



3. Ajoutez le FTD comme premier point de terminaison.

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

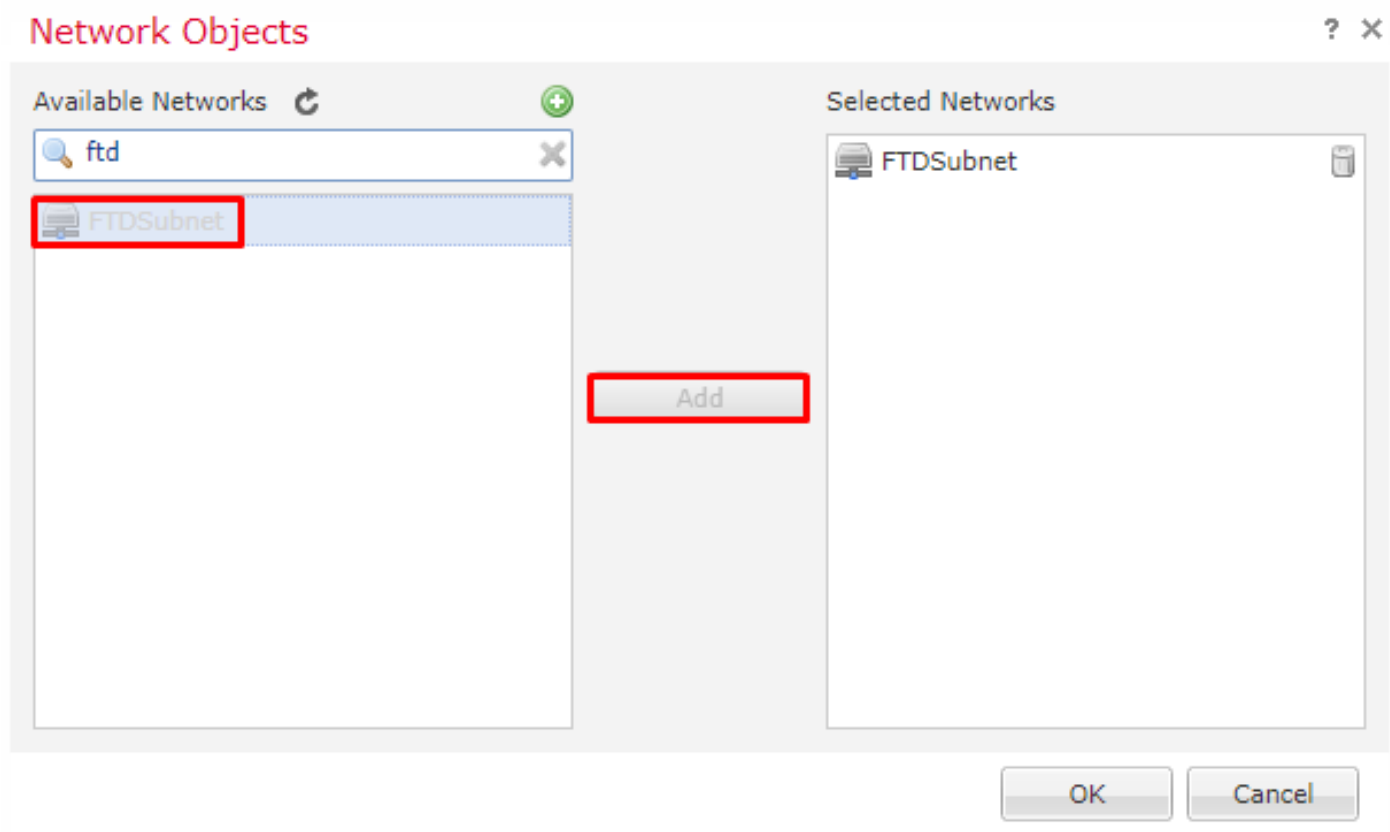
Cliquez sur le vert plus sous Réseaux protégés, comme illustré dans cette image, pour sélectionner les sous-réseaux à chiffrer dans ce VPN.



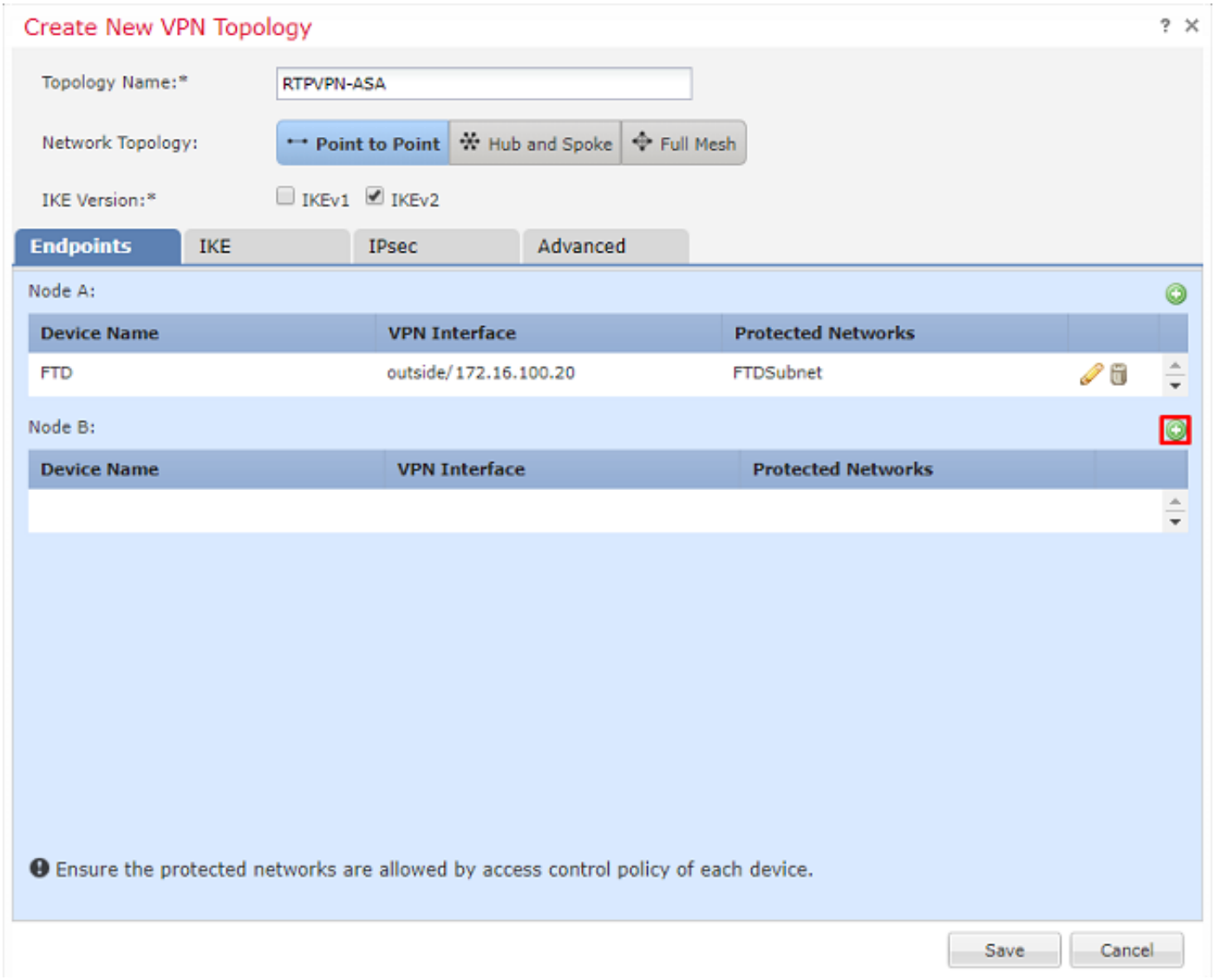
4. Cliquez sur vert plus et un objet réseau est créé ici.

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

FTDSubnet = 10.10.113.0/24

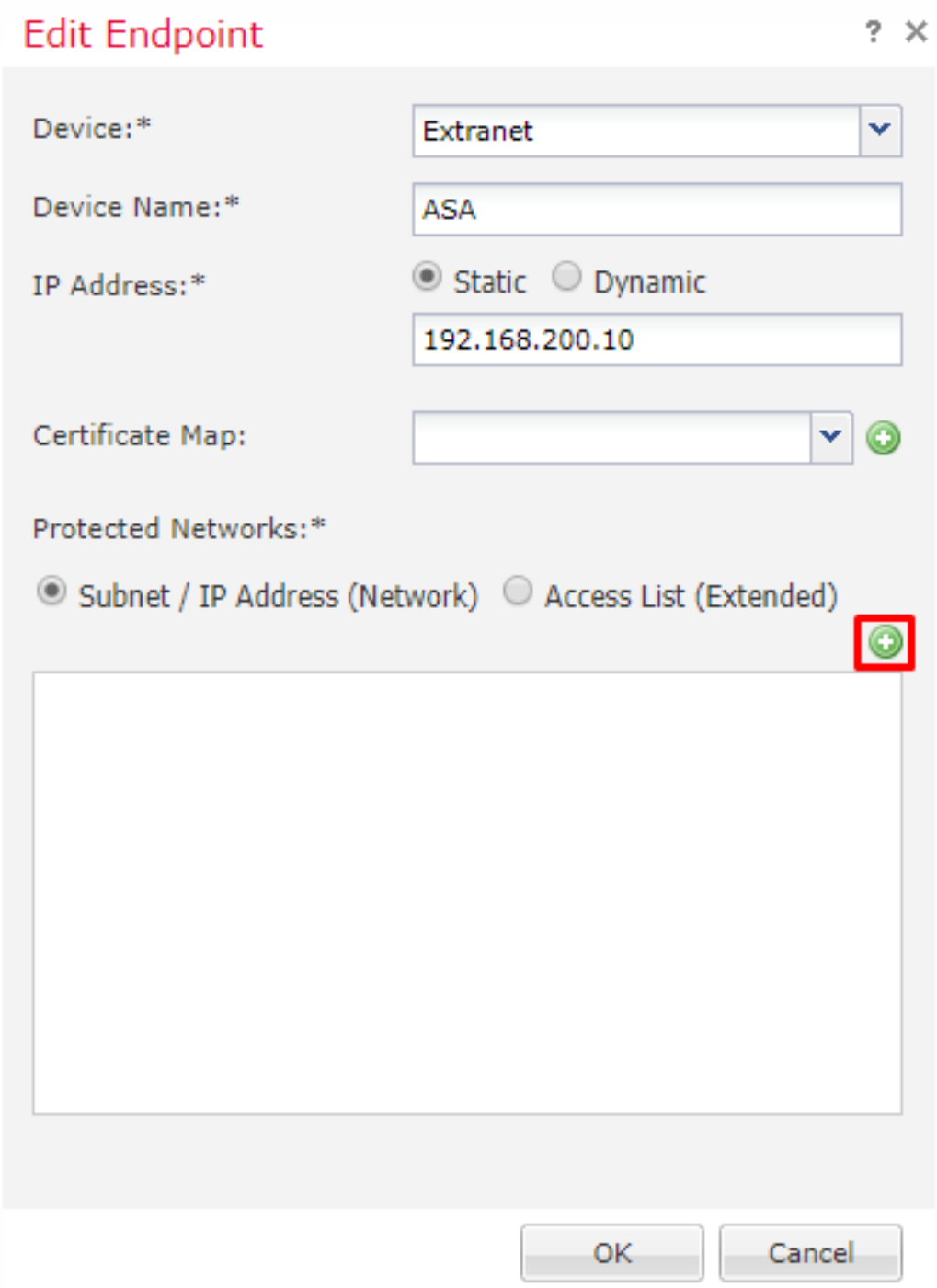


Noeud A : Le point de terminaison (FTD) est terminé. Cliquez sur le signe vert plus pour le noeud B, comme illustré dans l'image.



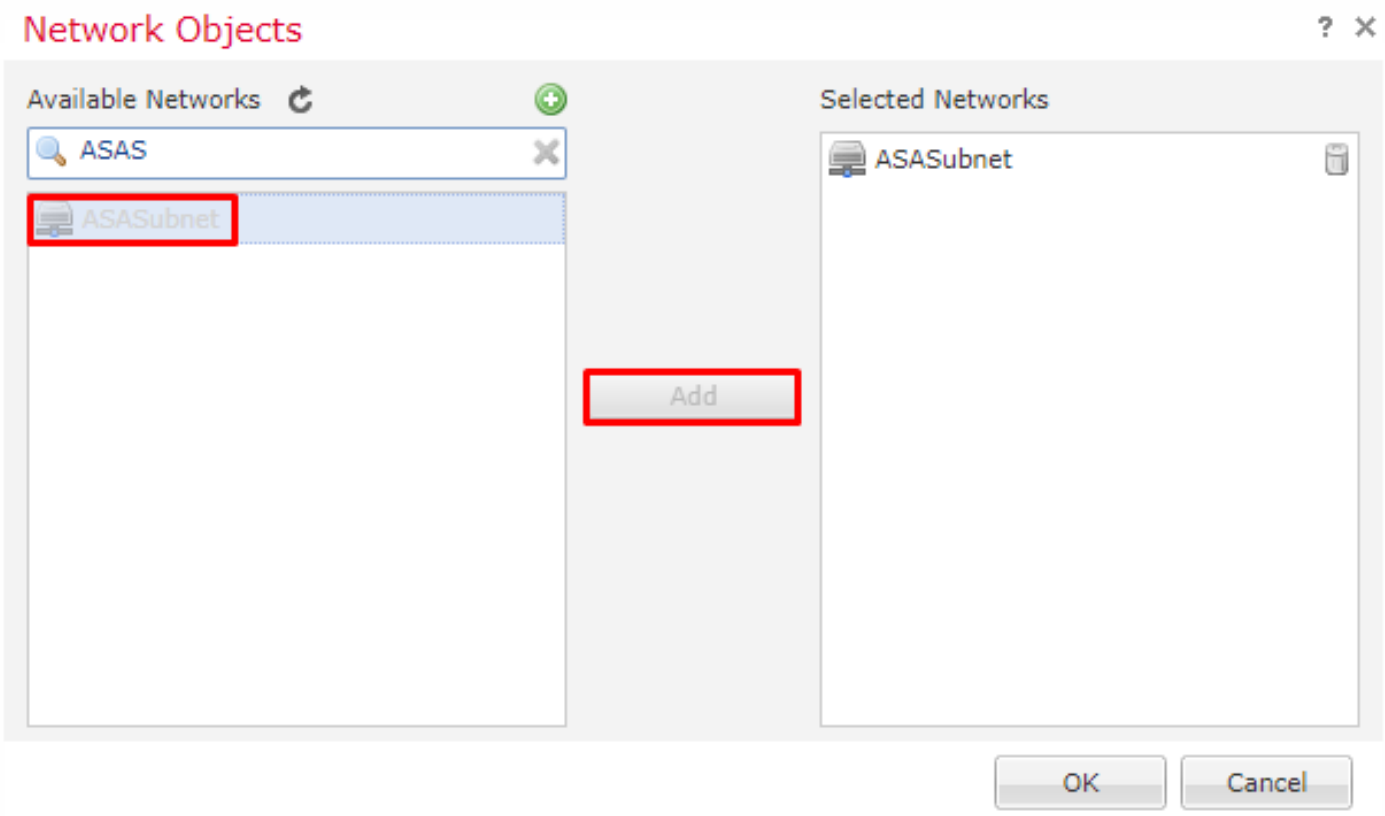
Le noeud B est un ASA. Les périphériques qui ne sont pas gérés par le FMC sont considérés comme extranet.

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



7. Comme l'illustre cette image, sélectionnez les **sous-réseaux ASA** à chiffrer et ajoutez-les aux réseaux sélectionnés.

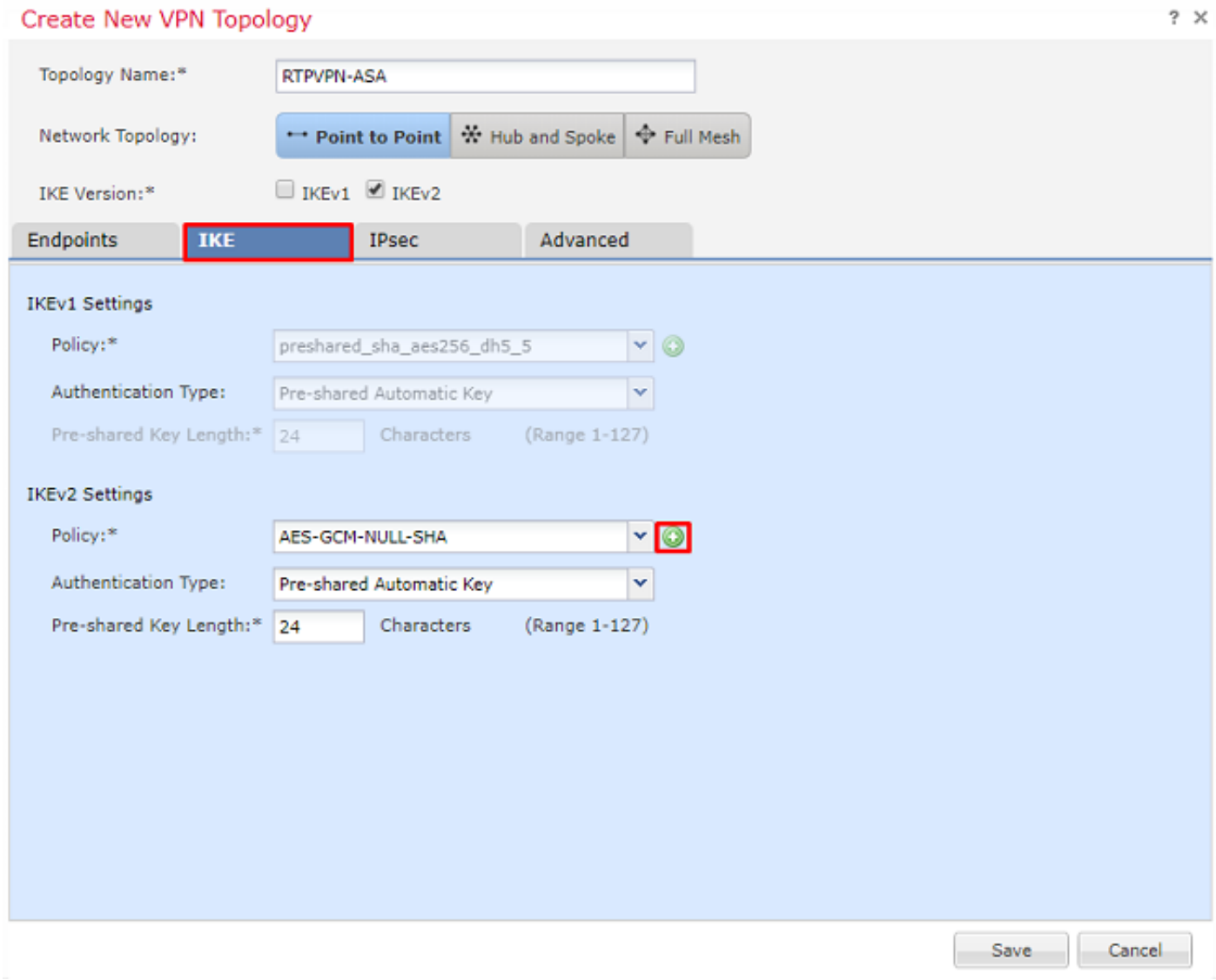
ASASubnet = 10.10.110.0/24



Étape 2. Configurez les paramètres IKE.

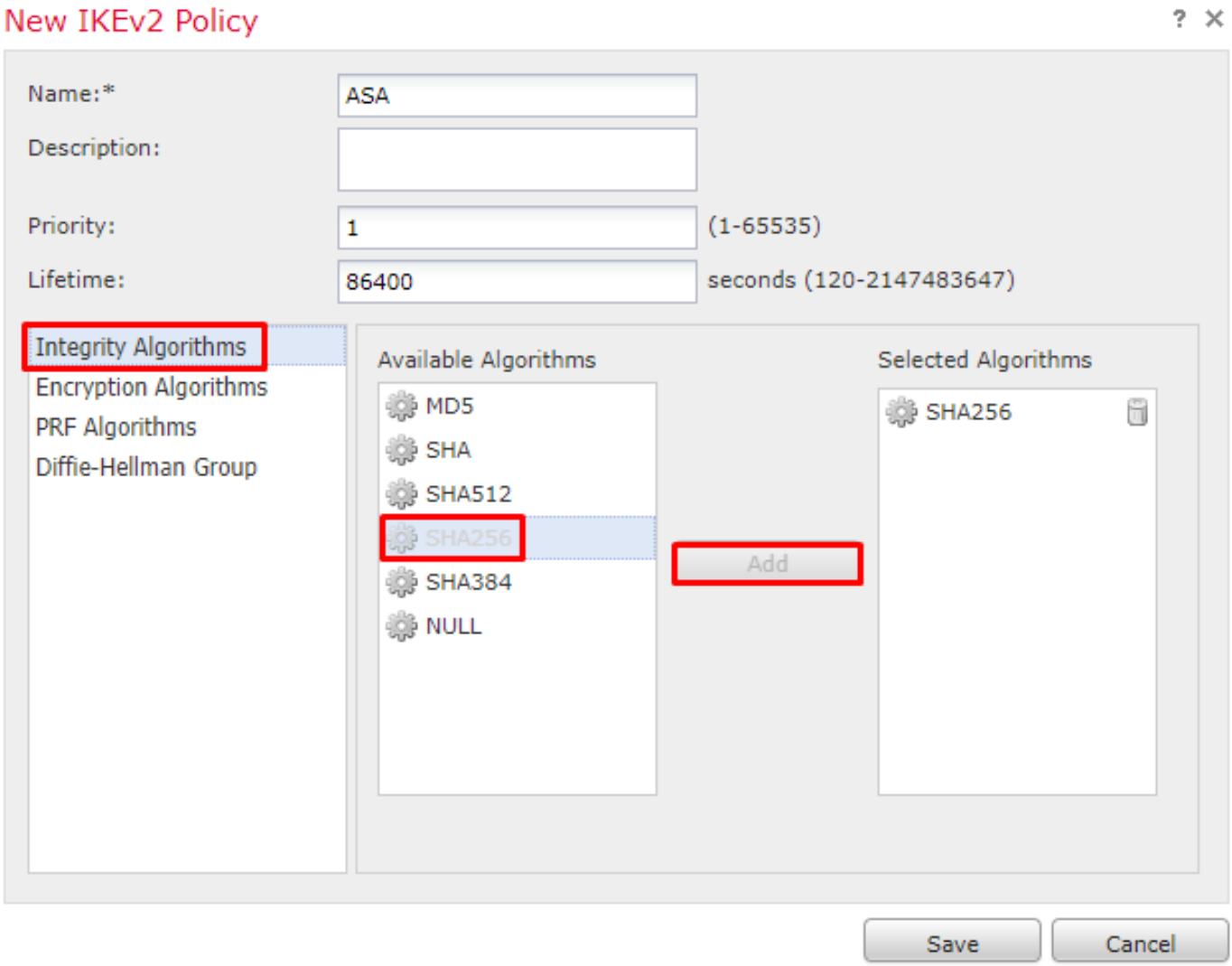
Les deux terminaux sont maintenant en place et passent par la configuration IKE/IPSEC.

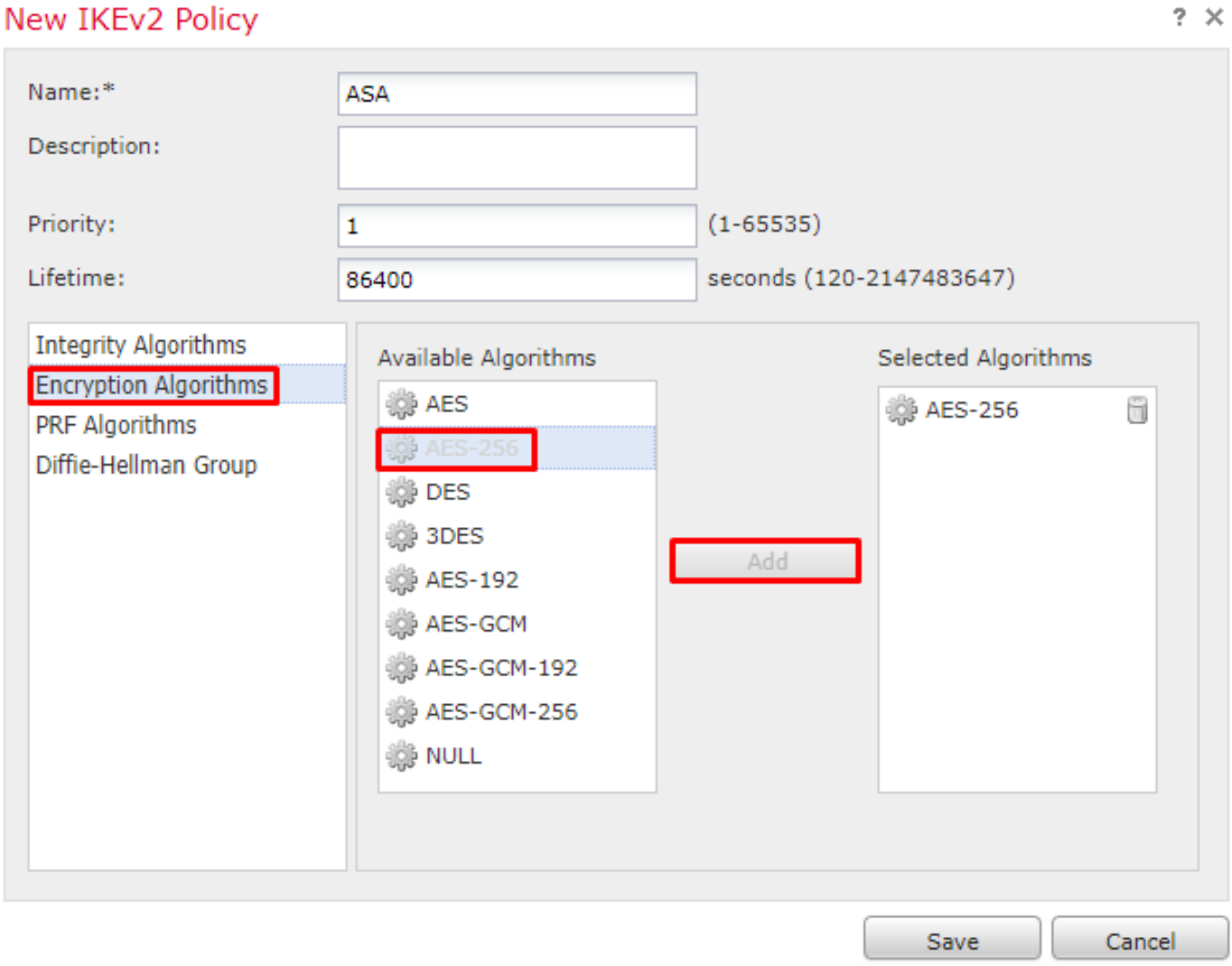
1. Sous l'onglet **IKE**, spécifiez les paramètres utilisés pour l'échange initial IKEv2. Cliquez sur le vert plus pour créer une nouvelle stratégie IKE, comme l'illustre l'image.

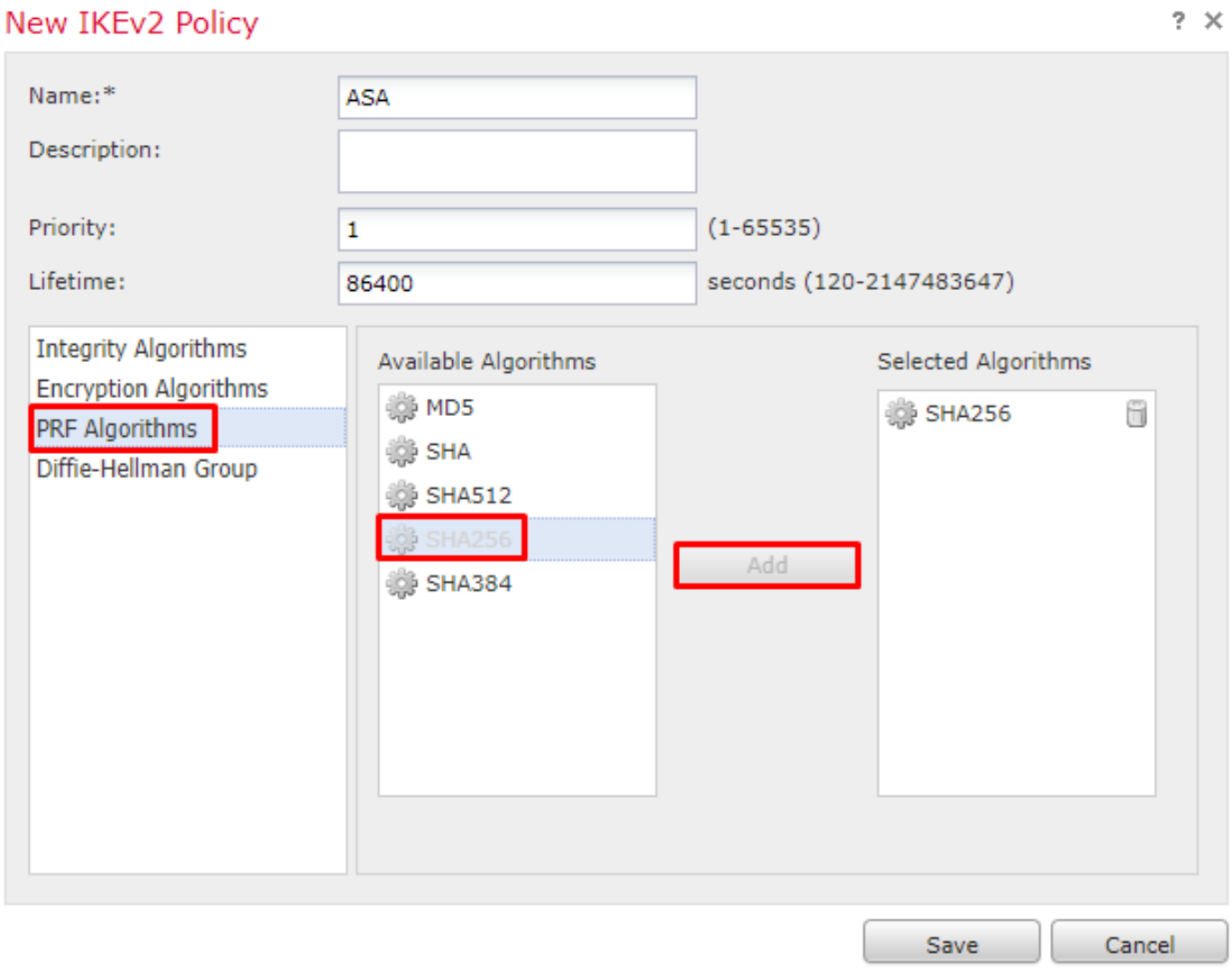


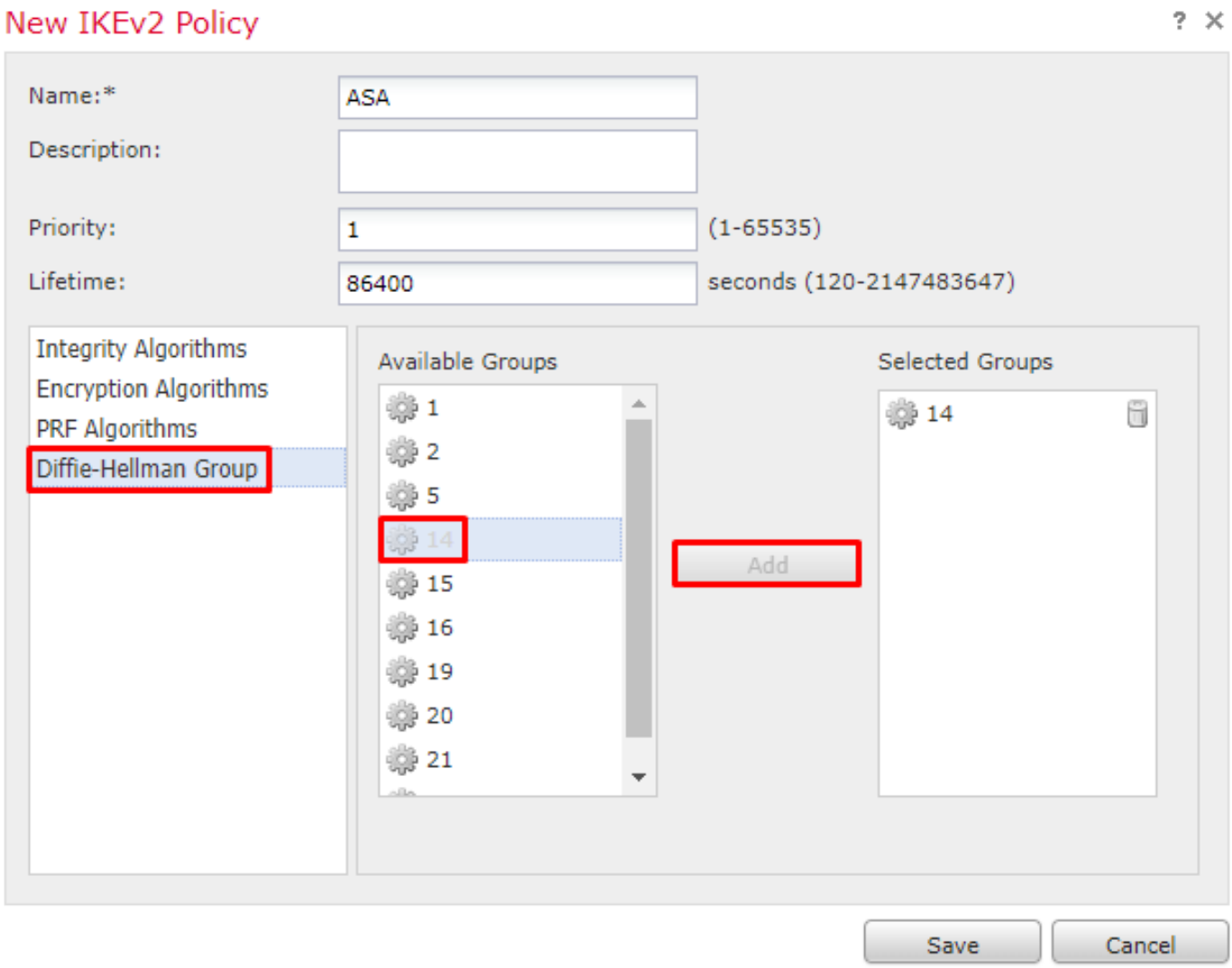
2. Dans la nouvelle stratégie IKE, spécifiez un numéro de priorité ainsi que la durée de vie de la phase 1 de la connexion. Ce document utilise ces paramètres pour l'échange initial : Integrity (SHA256), Encryption (AES-256), PRF (SHA256) et Diffie-Hellman Group (Groupe 14)

> **Note**: Toutes les stratégies IKE du périphérique sont envoyées à l'homologue distant, quelle que soit la section de stratégie sélectionnée. La première stratégie IKE appariée par l'homologue distant sera sélectionnée pour la connexion VPN. Choisissez la stratégie qui est envoyée 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

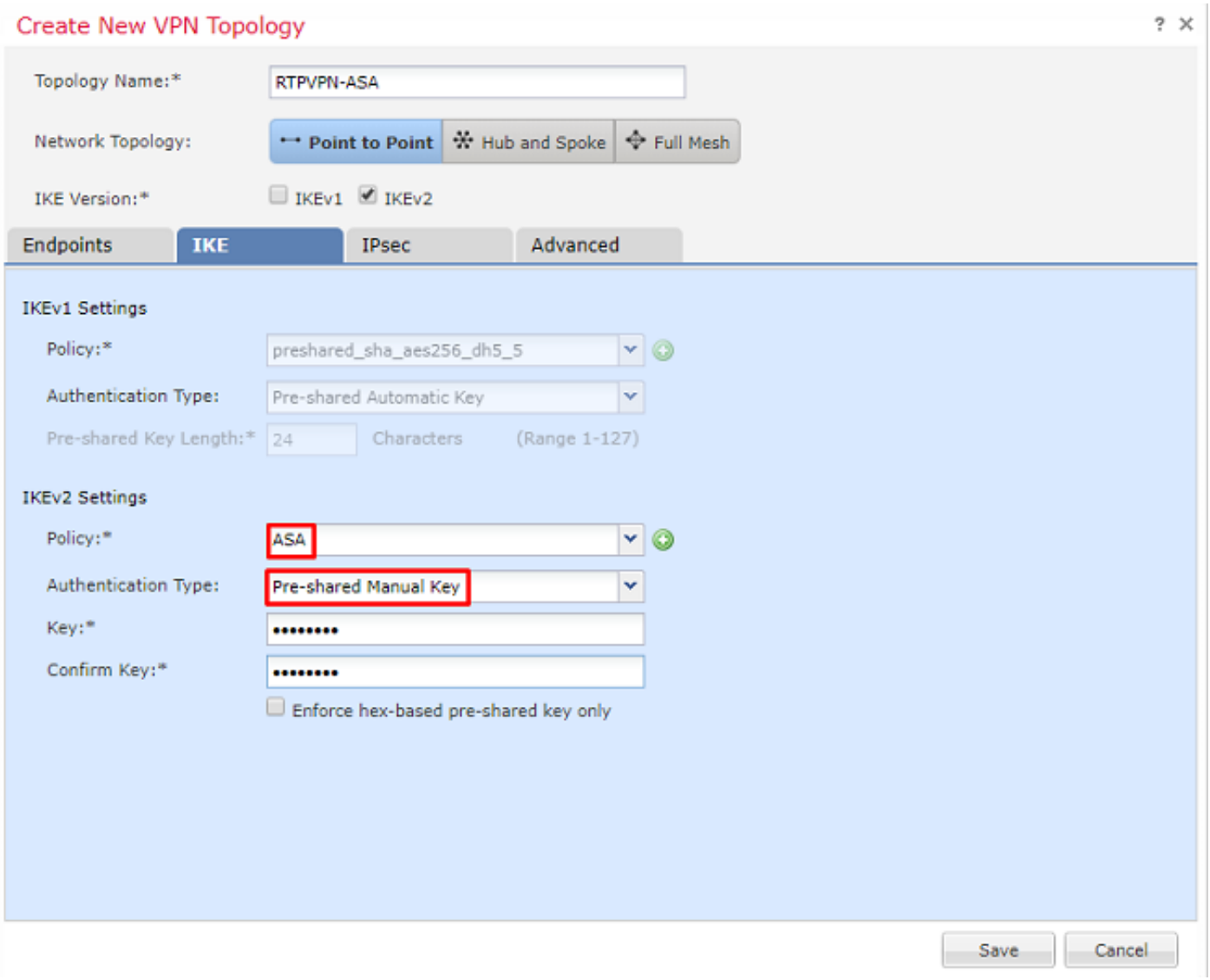

New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256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



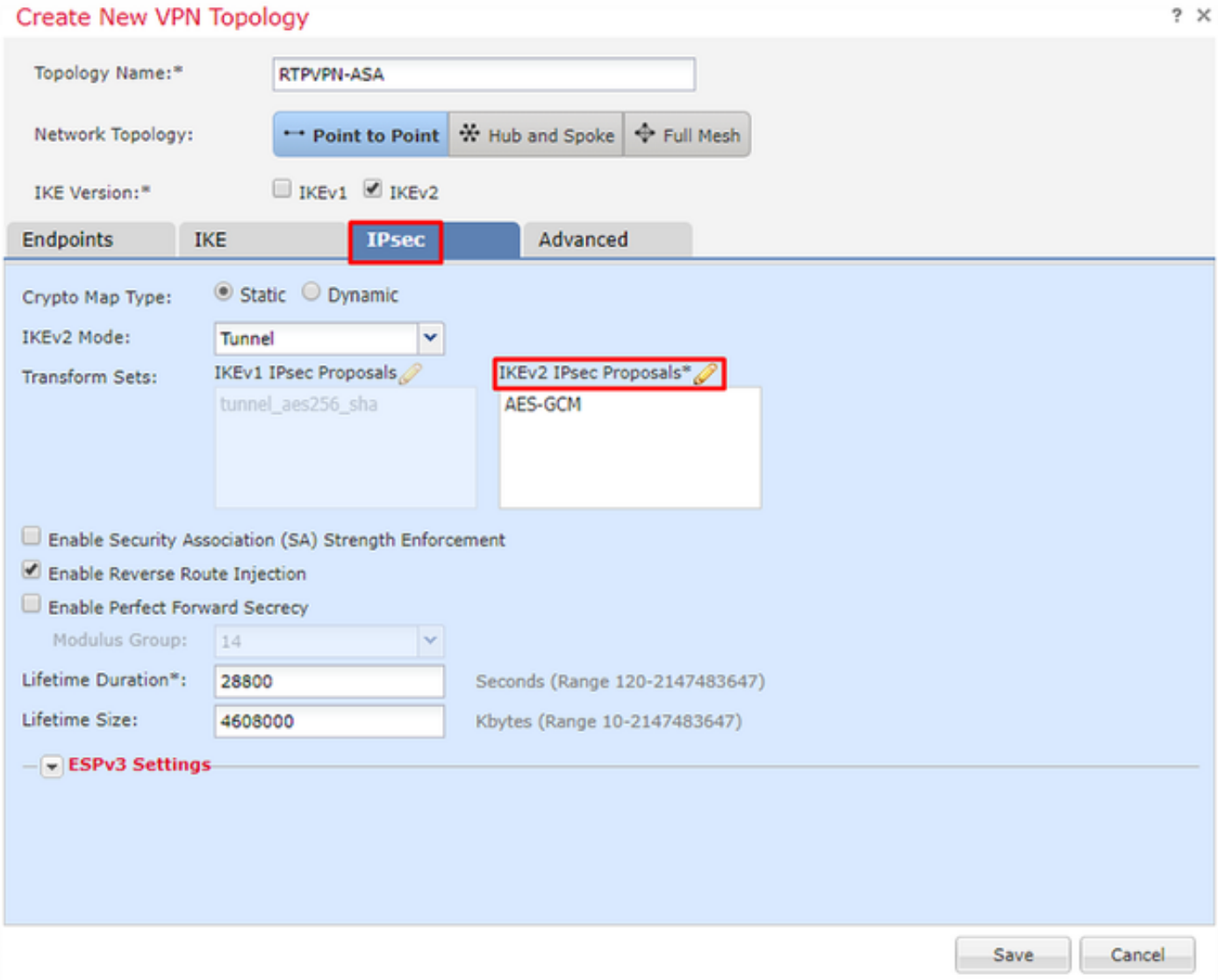
3. Une fois les paramètres ajoutés, sélectionnez cette stratégie et choisissez le **type d'authentification**.

4. Choisissez **le** manuel **à clé partagée**. Pour ce document, le PSK cisco123 est utilisé.



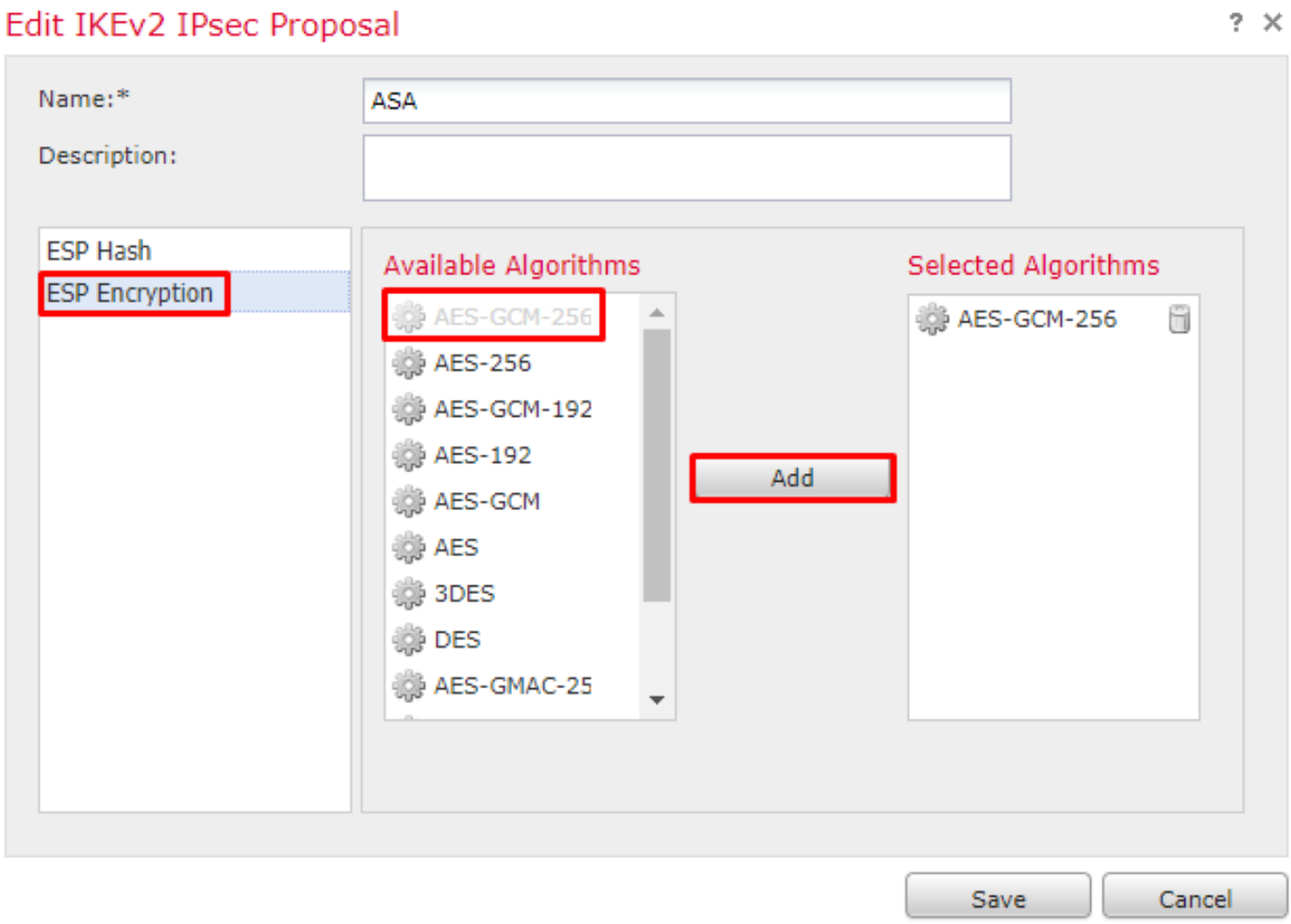
Étape 3. Configurez les paramètres IPsec.

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

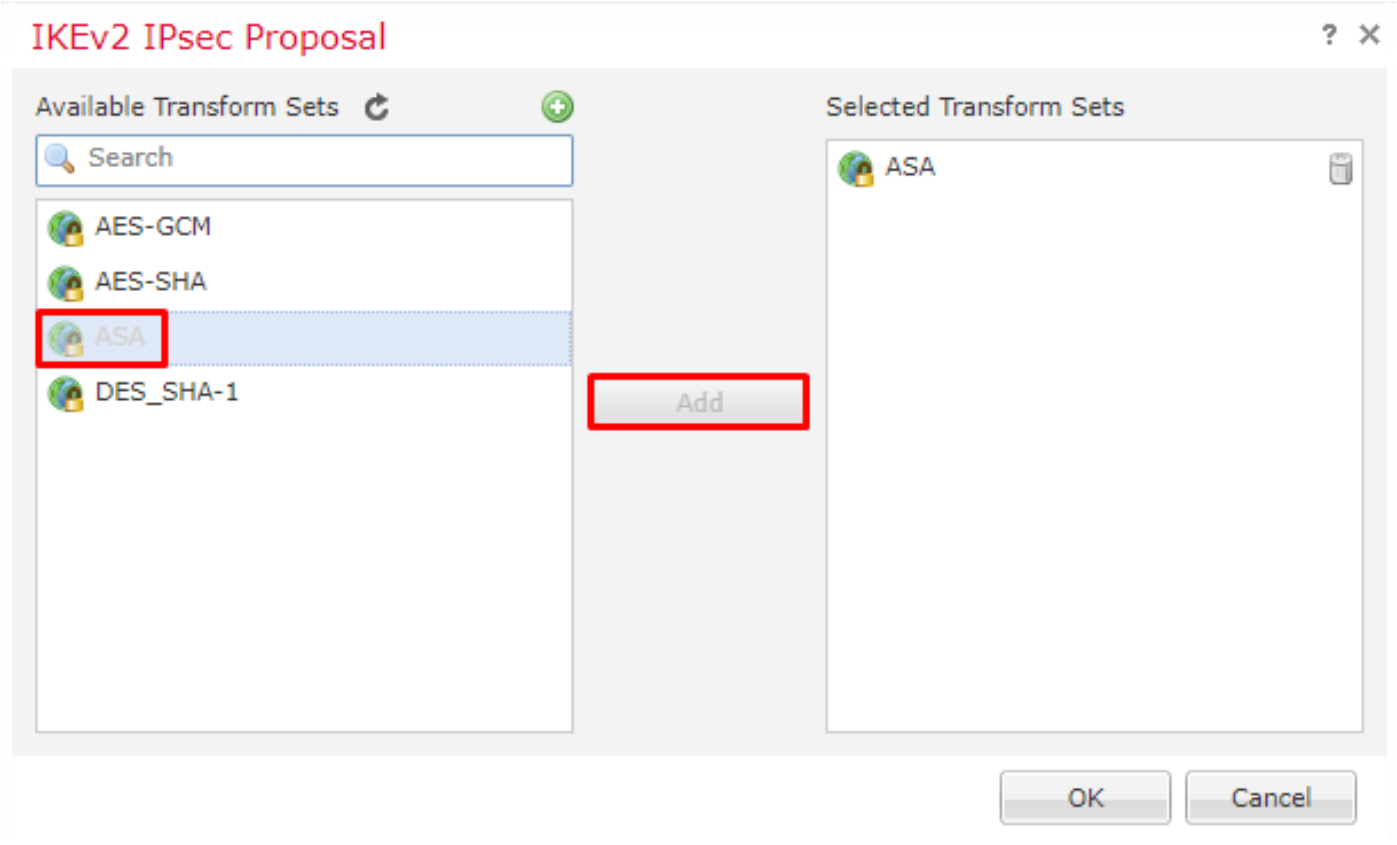


2. Afin de créer une proposition IPsec IKEv2, cliquez sur le vert plus et entrez les paramètres de phase 2.

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



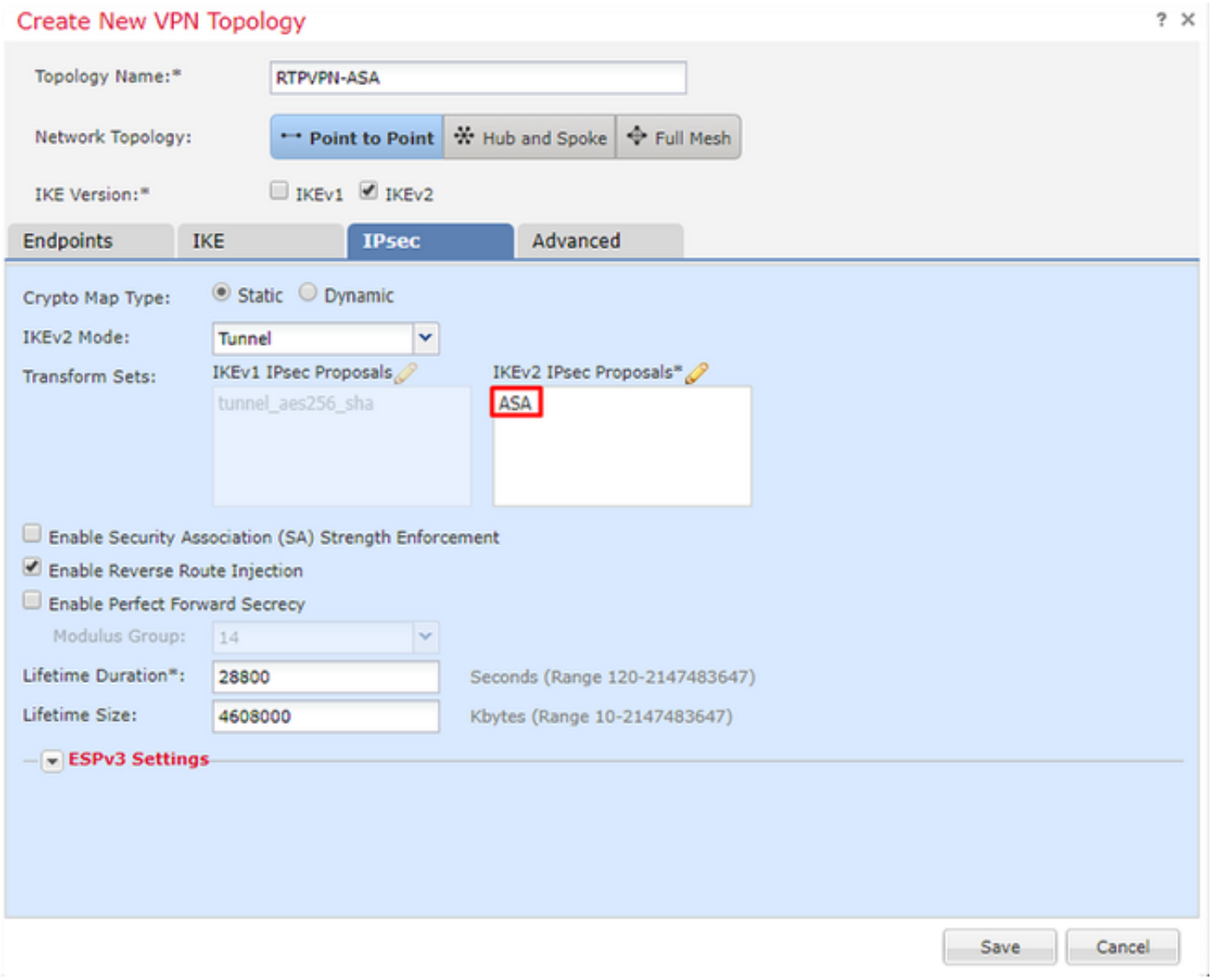
3. Une fois la nouvelle proposition IPsec créée, ajoutez-la aux jeux de transformation sélectionnés.



La proposition IPsec nouvellement sélectionnée est maintenant répertoriée dans les 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 sera définie par défaut et PFS désactivé.

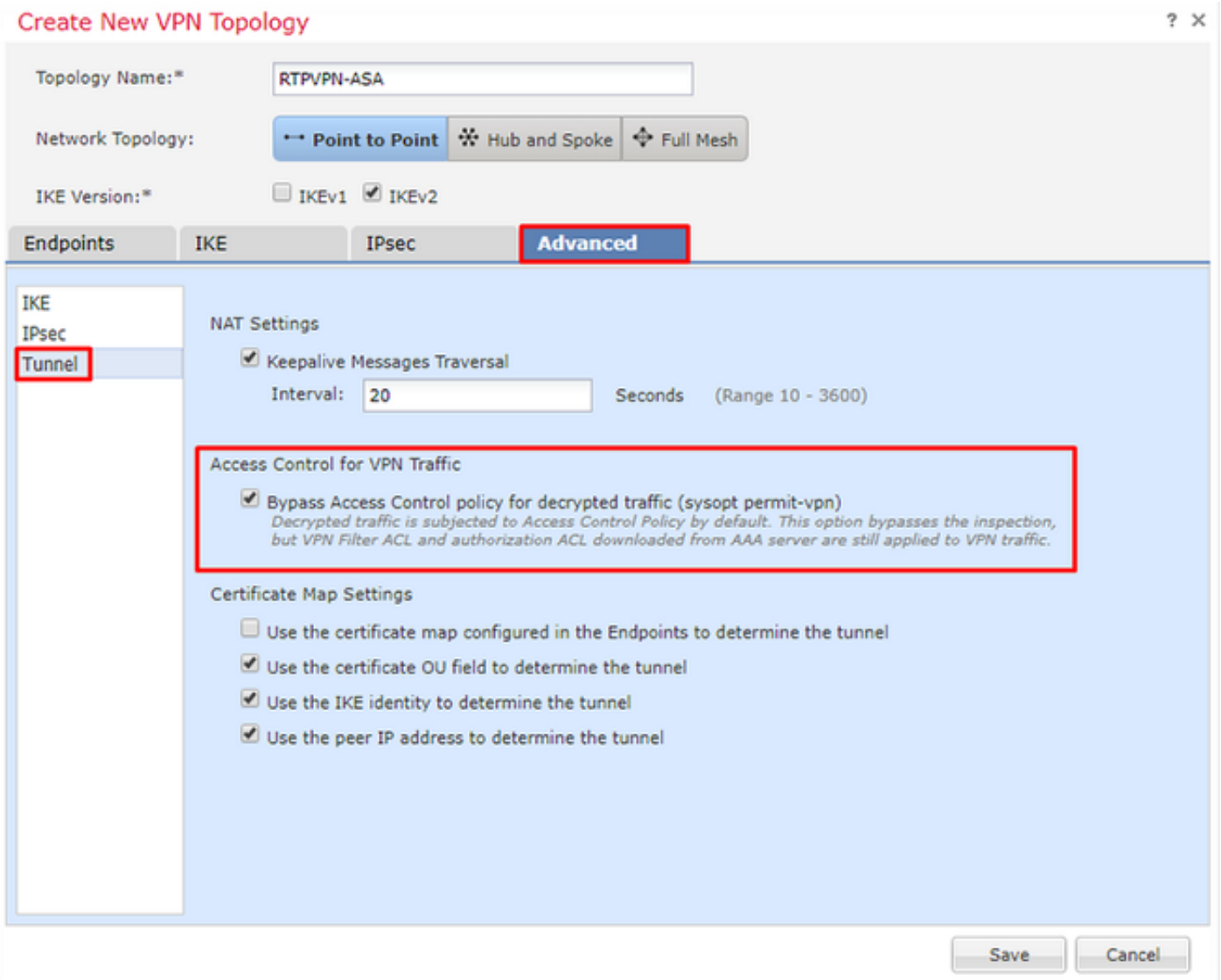


Facultatif : vous devez remplir l'option Ignorer le contrôle d'accès ou Créer une stratégie de contrôle d'accès.

Étape 4. Contourner le contrôle d'accès.

Le cas échéant, **sysopt permit-vpn** peut être activé sous **Advanced > Tunnel**.

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

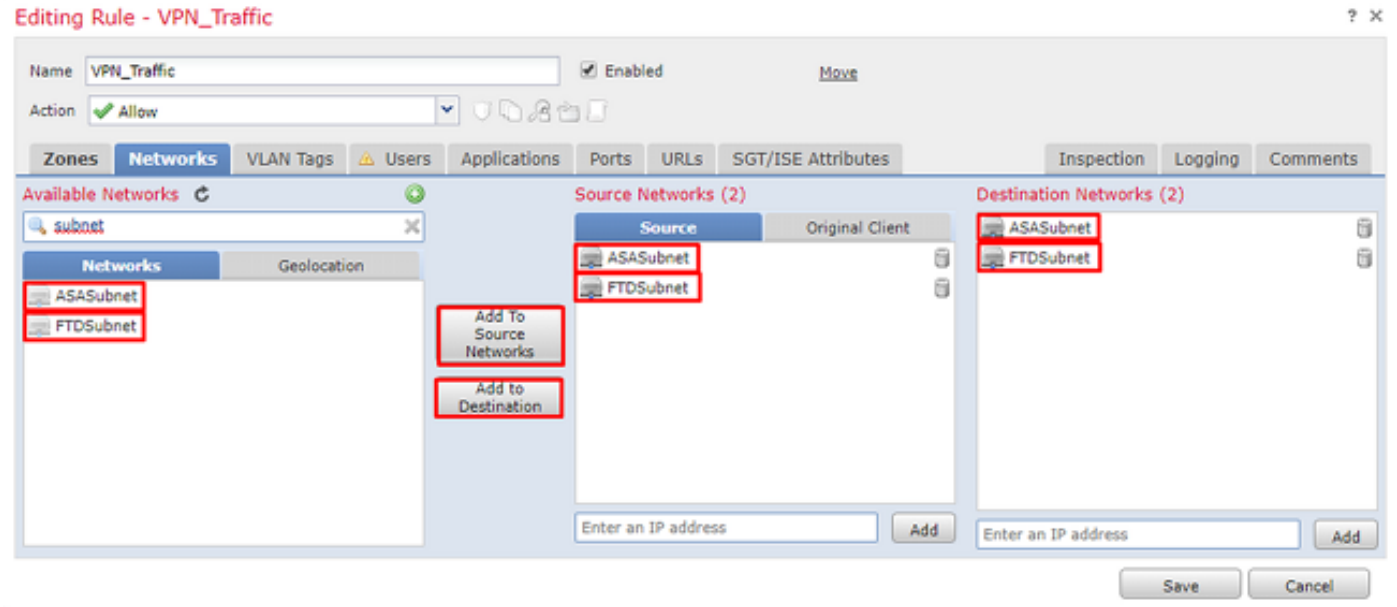


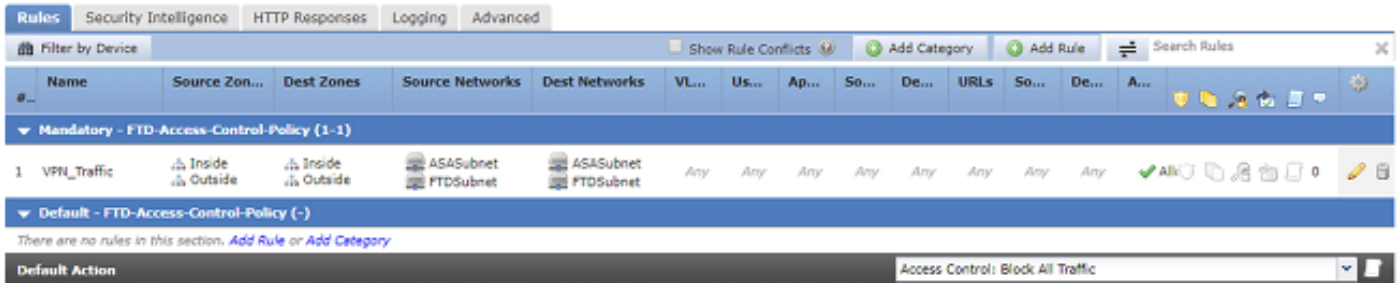
Si **sysopt permit-vpn** n'est pas activé, une stratégie de contrôle d'accès doit être créée pour autoriser le trafic VPN via le périphérique FTD. Si **sysopt permit-vpn** est activé, ignorez la création d'une stratégie de contrôle d'accès.

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

Sous Politiques de contrôle d'accès, accédez à **Politiques > Contrôle d'accès > Contrôle d'accès** et sélectionnez la Stratégie qui cible le périphérique FTD. Afin d'ajouter une règle, cliquez sur **Ajouter une règle**, comme indiqué 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 créez deux règles pour les séparer. Dans cet exemple, une règle est créée pour effectuer les deux.

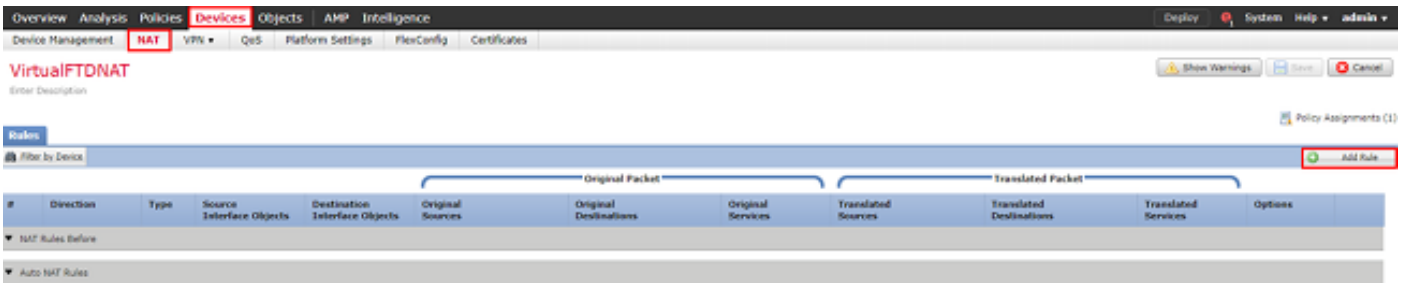




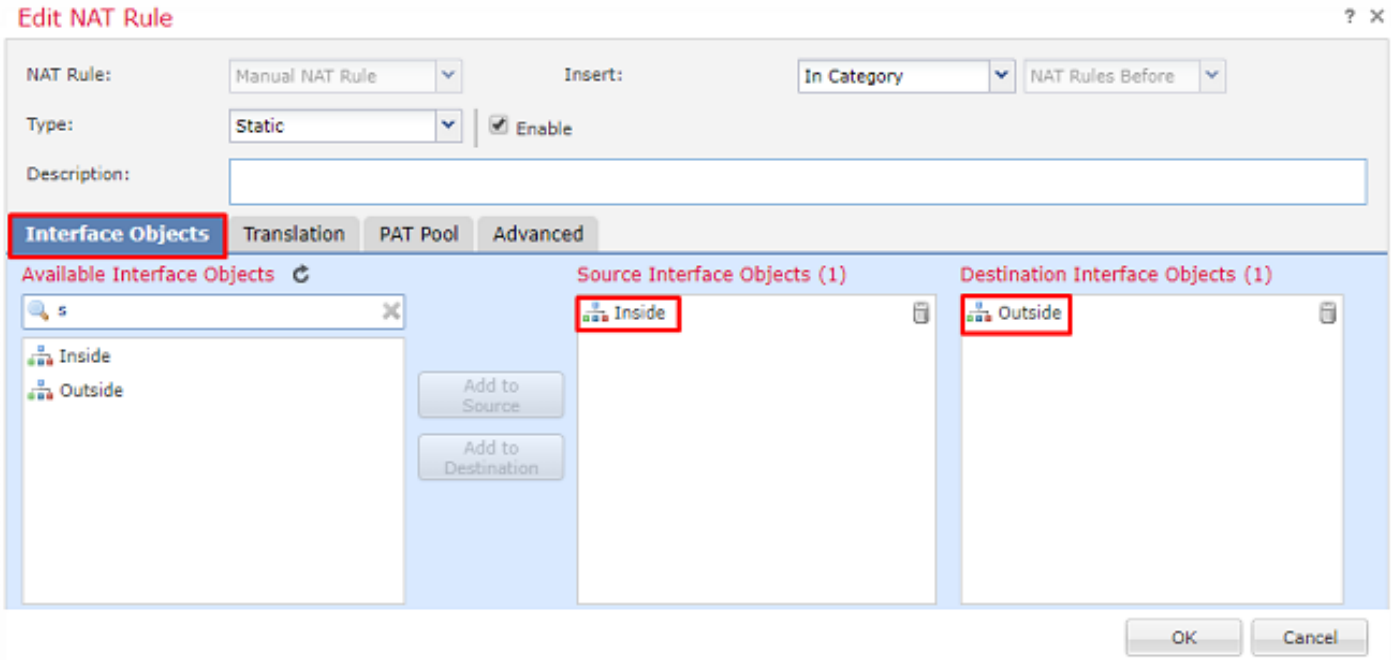
Étape 6. Configurez l'exemption NAT.

Configurez une instruction NAT Exemption pour le trafic VPN. L'exemption NAT doit être en place pour empêcher le trafic VPN d'accéder à une autre instruction NAT et de traduire le trafic VPN de manière incorrecte.

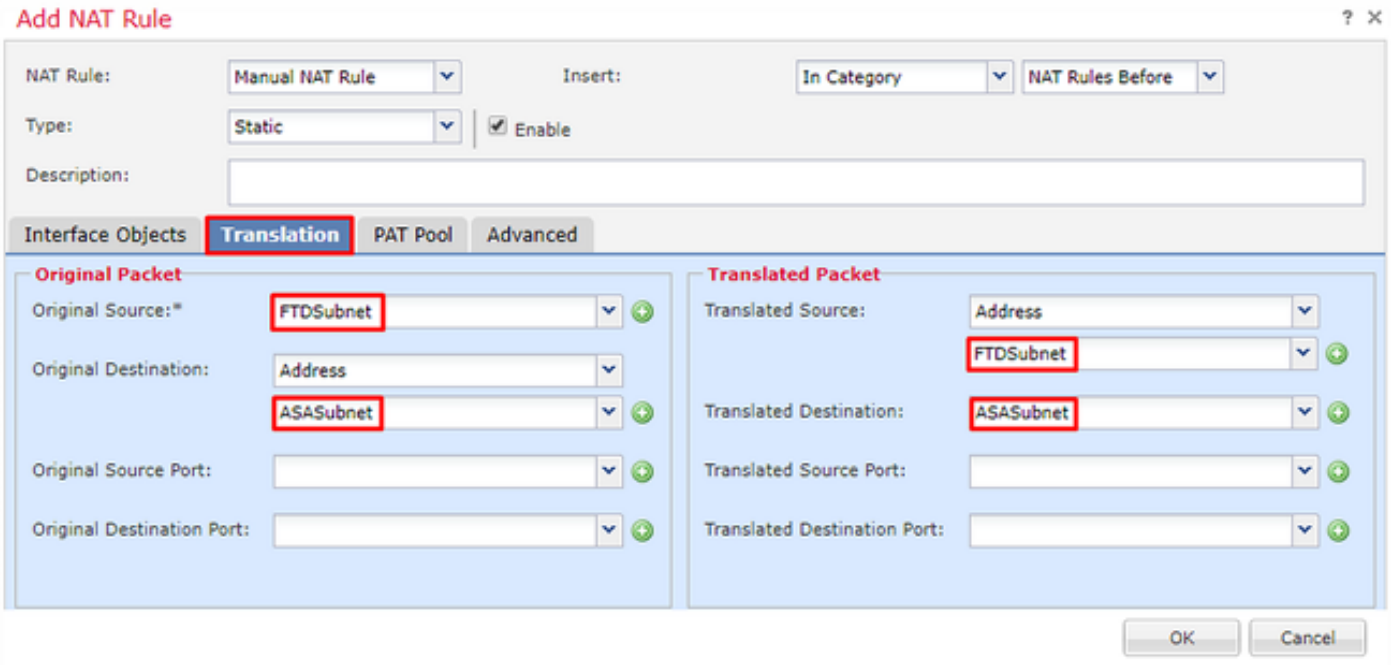
1. Accédez à **Périphériques > NAT**, sélectionnez la stratégie NAT qui cible le FTD. Créez une nouvelle règle lorsque vous cliquez sur le bouton **Ajouter une règle**.



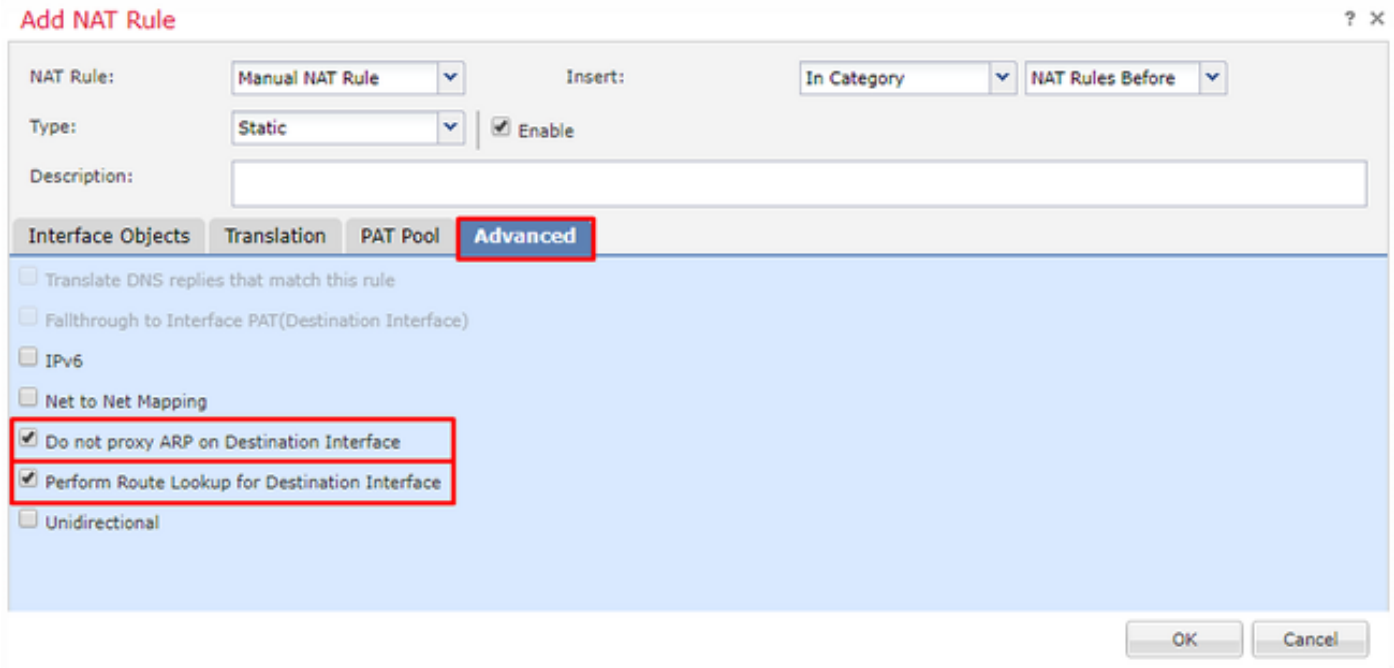
2. Créez une nouvelle règle NAT manuelle statique. Référez-vous aux interfaces internes et externes.



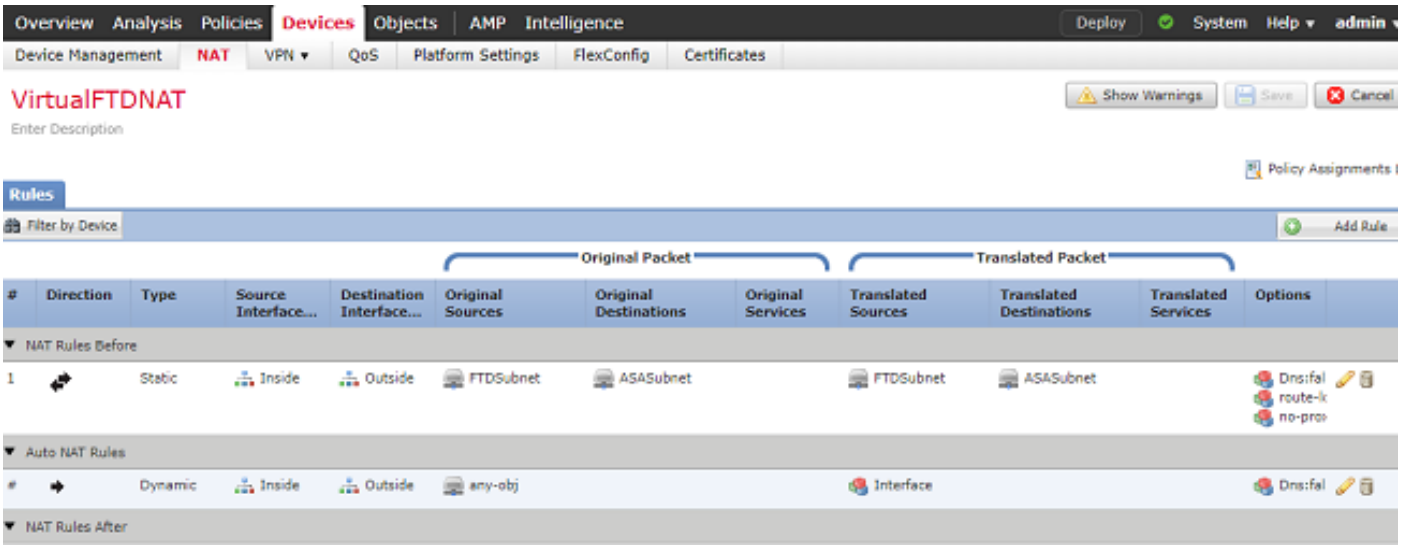
3. Sous l'onglet **Traduction** et sélectionnez les sous-réseaux source et de destination. Comme il s'agit d'une règle d'exemption NAT, faites de la source/destination d'origine et de la source/destination traduite la même, comme illustré dans cette image :



4. Enfin, passez à l'onglet **Avancé** 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 et déployez-la sur le FTD.

Étape 7. Configurez 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. Référez-vous 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 d'accès qui définit 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 référençant les algorithmes spécifiés sur le FTD :

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

7. Créez une entrée de carte de chiffrement 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 d'exemption NAT qui empêchera le trafic VPN d'être NATED par le pare-feu :

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet
no-proxy-arp route-lookup
```

Vérification

> **Note**: Pour le moment, 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 CSCvh77603.

Tentative de lancement 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 s'active. La première fois que la commande est exécutée, le tunnel VPN est désactivé, de sorte que la commande packet-tracer échouera avec VPN encrypt DROP. N'utilisez pas l'adresse IP interne du pare-feu comme adresse IP source dans Packet Tracer, 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-arp route-lookup
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 outside object-group FMC_INLINE_dst_rule_268436483 rule-id 268436483
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-arp route-lookup
```

```
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
```

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

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

Afficher crypto ikev2 sa

```
> show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local
Remote                                                Status         Role
 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 initiale

Lors de la création d'un VPN, il y a deux parties qui négocient le tunnel. Par conséquent, il est préférable d'obtenir les deux côtés de la conversation lorsque vous dépannez un type de défaillance de tunnel. Un guide détaillé sur le débogage des tunnels IKEv2 est disponible ici : Comment déboguer les VPN IKEv2

La cause la plus courante des pannes de tunnel est un problème de connectivité. Le meilleur moyen de le déterminer est de capturer des paquets sur le périphérique. Utilisez cette commande pour capturer des 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 du 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 courants de trafic que vous rencontrez sont les suivants :

- Problèmes de routage derrière le FTD : réseau interne incapable de router les paquets vers les adresses IP et les clients VPN affectés.
- Les listes de contrôle d'accès bloquent 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 : Guide de configuration FTD géré par FMC