Configuration d'un VPN basé sur des stratégies et des routes depuis ASA et FTD vers Microsoft Azure

Contenu

Introduction

Ce document décrit les concepts et la configuration d'un VPN entre Cisco ASA et Cisco Secure Firewall et Microsoft Azure Cloud Services.

Concepts

Domaine de chiffrement VPN

La plage d'adresses IP IPSec permet de participer au tunnel VPN.Le domaine de cryptage est défini à l'aide d'un sélecteur de trafic local et d'un sélecteur de trafic distant pour spécifier les plages de sous-réseaux locaux et distants qui sont capturées et cryptées par IPSec. Il existe deux méthodes pour définir les domaines de cryptage VPN : des sélecteurs de trafic basés sur des routes ou des politiques.

Basé sur la route :
Le domaine de cryptage 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. Cela signifie que tout trafic acheminé dans le tunnel IPSec est chiffré quel que soit le sous-réseau source/de destination.

Cisco Adaptive Security Appliance (ASA) prend en charge le VPN basé sur les routes avec l'utilisation d'interfaces de tunnel virtuel (VTI) dans les versions 9.8 et ultérieures.

Cisco Secure Firewall ou Firepower Threat Defense (FTD) géré par FMC (Firepower Management Center) prend en charge les VPN basés sur les routes avec l'utilisation de VTI dans les versions 6.7 et ultérieures.

Basé sur des politiques :

Le domaine de chiffrement est configuré pour chiffrer uniquement des plages IP spécifiques pour la source et la destination. Les sélecteurs de trafic local basés sur des stratégies et les sélecteurs de trafic distants identifient le trafic à chiffrer sur IPSec.

ASA prend en charge les VPN basés sur des politiques avec des crypto-cartes dans les versions 8.2 et ultérieures.

Microsoft Azure prend en charge les sélecteurs de trafic basés sur une route, une stratégie ou une route avec des sélecteurs de trafic basés sur une stratégie simulée. Azure limite actuellement la version IKE (Internet Key Exchange) que vous pouvez configurer en fonction de la méthode VPN sélectionnée. Le routage basé sur la route nécessite IKEv2 et le routage basé sur la stratégie nécessite IKEv1. Cela signifie que si IKEv2 est utilisé, alors le routage basé sur Azure doit être sélectionné et ASA doit utiliser un VTI, mais si l'ASA ne prend en charge que les crypto-cartes en raison de la version du code, alors Azure doit être configuré pour le routage basé sur la stratégie avec des sélecteurs de trafic basés sur la stratégie. Ceci est accompli dans le portail Azure via le déploiement de script PowerShell pour implémenter une option que Microsoft appelle UsePolicyBasedTrafficSectors comme expliqué ici : https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps.

Pour résumer du point de vue de la configuration ASA et FTD :

- Pour ASA/FTD configuré avec une crypto-carte, Azure doit être configuré pour un VPN basé sur une stratégie ou basé sur une route avec UsePolicyBasedTrafficSelectors.
- Pour ASA configuré avec un VPN, Azure doit être configuré pour le VPN basé sur la route.
- Pour FTD, des informations supplémentaires sur la configuration des VTI sont disponibles ici ; https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_site_to_site_vpns.html#concept_ccj_p4r_cmb

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pour le VPN basé sur la route IKEv2 qui utilise VTI sur ASA : Code ASA version 9.8(1) ou ultérieure. (Azure doit être configuré pour le VPN basé sur la route.)
- Pour le VPN basé sur des stratégies IKEv1 qui utilise la crypto-carte sur ASA et FTD : Code ASA version 8.2 ou ultérieure et FTD 6.2.0 ou ultérieure. (Azure doit être configuré pour le VPN basé sur des stratégies.)
- Pour un VPN basé sur la route IKEv2 qui utilise une crypto-carte sur ASA avec des sélecteurs de trafic basés sur des politiques : Code ASA version 8.2 ou ultérieure configuré avec une carte de chiffrement. (Azure doit être configuré pour le VPN basé sur la route avec

UsePolicyBasedTrafficSelectors.)
- Connaissance de FMC pour la gestion et la configuration FTD.

Components Used

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

- Cisco ASA
- Microsoft Azure
- FTD Cisco
- Cisco FMC

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

Exécutez les étapes de configuration. Choisissez de configurer IKEv1, IKEv2 basé sur la route avec VTI ou IKEv2 basé sur la route avec des sélecteurs de trafic basés sur la politique d'utilisation (crypto-carte sur ASA).

Configuration IKEv1 sur ASA

Pour un VPN de site à site IKEv1 d'ASA vers Azure, suivez la configuration ASA suivante. Assurez-vous de configurer un tunnel basé sur une stratégie dans le portail Azure. Les crypto-cartes sont utilisées sur ASA pour cet exemple.

Consultez ce document Cisco pour obtenir des informations complètes sur IKEv1 et la configuration ASA.

Étape 1 : activation d'IKEv1 sur l'interface externe

```
Cisco-ASA(config)#crypto ikev1 enable outside
```

Étape 2 : création d'une stratégie IKEv1 définissant les algorithmes/méthodes à utiliser pour le hachage, l'authentification, le groupe Diffie-Hellman, la durée de vie et le chiffrement

> **Note**: Les attributs IKEv1 de phase 1 répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ikev1 policy 1
Cisco-ASA(config-ikev1-policy)#authentication pre-share
Cisco-ASA(config-ikev1-policy)#encryption aes
Cisco-ASA(config-ikev1-policy)#hash sha
Cisco-ASA(config-ikev1-policy)#group 2
```

```
Cisco-ASA(config-ikev1-policy)#lifetime 28800
```

Étape 3 : création d'un groupe de tunnels sous les attributs IPsec et configuration de l'adresse IP de l'homologue et de la clé pré-partagée du tunnel

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
```

Étape 4 : création d'une liste de contrôle d'accès définissant le trafic à chiffrer et à tunnelliser Dans cet exemple, le trafic d'intérêt est le trafic du tunnel qui provient du sous-réseau 10.2.2.0 vers 10.1.1.0. Il peut contenir plusieurs entrées si plusieurs sous-réseaux sont impliqués entre les sites.

Dans les versions 8.4 et ultérieures, il est possible de créer des objets ou des groupes d'objets qui servent de conteneurs pour les réseaux, les sous-réseaux, les adresses IP d'hôte ou plusieurs objets. Créez deux objets possédant les sous-réseaux local et distant et utilisez-les pour les instructions ACL (Access Control List) et NAT (Network Address Translation).

```
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0

Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

Étape 5. Configuration du jeu de transformation (TS), qui doit impliquer le mot clé**IKEv1**. Un TS identique doit également être créé sur l'extrémité distante.

> **Note**: Les attributs IKEv1 de phase 2 répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

Étape 6. Configurez la crypto-carte et appliquez-la à l'interface externe, qui comporte les composants suivants :
·L'adresse IP de l'homologue
·La liste d'accès définie qui contient le trafic d'intérêt
·Le TS
·La configuration ne définit pas PFS (Perfect Forward Secrecy) car la documentation Azure disponible publiquement indique que PFS est désactivé pour IKEv1 dans Azure. Un paramètre optionnel de PFS, qui crée une nouvelle paire de clés Diffie-Hellman utilisées afin de protéger les données (les deux côtés doivent être activés par PFS avant que la phase 2 ne s'affiche), peut être activé via l'utilisation de cette configuration : **crypto map outside_map 20 set pfs .**
· Les durées de vie IPSec de phase 2 sont basées sur la documentation Azure disponible publiquement. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
```

```
Cisco-ASA(config)#crypto map outside_map 20 set ikev1 transform-set myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 3600
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
102400000
Cisco-ASA(config)#crypto map outside_map interface outside
```

Étape 7. Assurez-vous que le trafic VPN n'est soumis à aucune autre règle NAT. Créez une règle d'exemption NAT :

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination
static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

> **Remarque** : lorsque plusieurs sous-réseaux sont utilisés, vous devez créer des groupes d'objets avec tous les sous-réseaux source et de destination et les utiliser dans la règle NAT.

```
Cisco-ASA(config)#object-group network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object 10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.2.2.0 255.255.255.0

Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object 10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE
destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

IKEv2 basé sur la route avec VTI sur ASA Code 9.8 (1) ou ultérieur

Pour un VPN basé sur la route de site à site IKEv2 sur code ASA, suivez cette configuration. Assurez-vous qu'Azure est configuré pour le VPN basé sur la route et ne configurez pas UsePolicyBasedTrafficSelector dans le portail Azure. Une interface VTI est configurée sur l'ASA.

Consultez ce document Cisco pour obtenir des informations complètes sur la configuration ASA VTI.

Étape 1 : activation d'IKEv2 sur l'interface externe

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

Étape 2 : ajout d'une stratégie IKEv2 phase 1

> **Remarque** : Microsoft a publié des informations qui sont en conflit avec les attributs spécifiques de cryptage, d'intégrité et de durée de vie IKEv2 de phase 1 utilisés par Azure. Les attributs répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Les informations qui entrent en conflit avec l'attribut IKEv2 de Microsoft sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

Étape 3 : ajout d'une proposition IPsec IKEv2 phase 2 Spécifiez les paramètres de sécurité dans le cryptage IPsec **ikev2 ipsec-proposal** mode de configuration global:

protocole esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocole intégrité esp {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **Note**: Microsoft a publié des informations qui entrent en conflit avec les attributs de cryptage et d'intégrité IPSec de phase 2 spécifiques utilisés par Azure. Les attributs répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Les informations qui entrent en conflit avec l'attribut IPSec de phase 2 de Microsoft sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

Étape 4. Ajoutez un profil IPSec qui spécifie :

- La proposition IPSec de phase 2 ikev2 précédemment configurée
- Durée de vie IPSec de phase 2 (facultatif) en secondes et/ou kilo-octets
- Le groupe PFS (facultatif)

> **Note**: Microsoft a publié des informations qui entrent en conflit avec la durée de vie IPSec de phase 2 et les attributs PFS utilisés par Azure. Les attributs répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Les informations qui entrent en conflit avec l'attribut IPSec de phase 2 de Microsoft sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec profile PROFILE1
Cisco-ASA(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-profile)#set security-association lifetime seconds 27000
Cisco-ASA(config-ipsec-profile)#set security-association lifetime kilobytes unlimited
Cisco-ASA(config-ipsec-profile)#set pfs none
```

Étape 5 : création d'un groupe de tunnels sous les attributs IPsec et configuration de l'adresse IP de l'homologue et de la clé prépartagée de tunnel local et distant IKEv2

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

Étape 6. Créez un VTI qui spécifie :

- Un nouveau numéro d'interface de tunnel : interface tunnel [numéro]
- Un nouveau nom d'interface de tunnel : nameif [nom]
- Une adresse IP inexistante doit exister sur l'interface du tunnel : ip address [adresse-ip] [masque]
- Interface source du tunnel où le VPN se termine localement : tunnel source interface [int-name]
- Adresse IP de la passerelle Azure : tunnel destination [Azure Public IP]
- Mode IPv4 IPSec : tunnel mode ipsec ipv4
- Profil IPSec à utiliser pour cette interface VTI : tunnel protection ipsec profile [profile-name]

```
Cisco-ASA(config)#interface tunnel 100
Cisco-ASA(config-if)#nameif vti
Cisco-ASA(config-if)#ip address 169.254.0.1 255.255.255.252
Cisco-ASA(config-if)#tunnel source interface outside
Cisco-ASA(config-if)#tunnel destination [Azure Public IP]
Cisco-ASA(config-if)#tunnel mode ipsec ipv4
Cisco-ASA(config-if)#tunnel protection ipsec profile PROFILE1
```

Étape 7 : création d'une route statique pour diriger le trafic vers le tunnel Pour ajouter une route statique, entrez la commande suivante :
route if_name dest_ip mask gateway_ip [distance]

Les **dest_ip** et **mask** est l'adresse IP pour le réseau de destination dans le cloud Azure, par exemple, 10.0.0.0/24. L'adresse ip de la passerelle doit être n'importe quelle adresse IP (existante ou inexistante) sur le sous-réseau de l'interface du tunnel, telle que 169.254.0.2. L'objectif de cette adresse ip de la passerelle est de diriger le trafic vers l'interface du tunnel, mais l'adresse IP de la passerelle en particulier n'est pas importante.

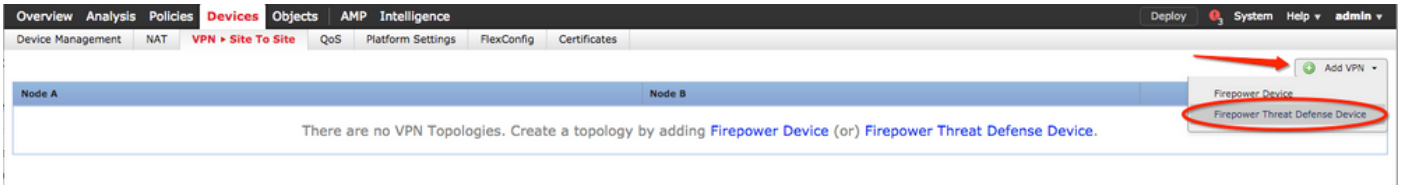
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

Configuration IKEv1 sur FTD

Pour un VPN de site à site IKEv1 de FTD à Azure, vous devez avoir préalablement enregistré le périphérique FTD sur FMC.

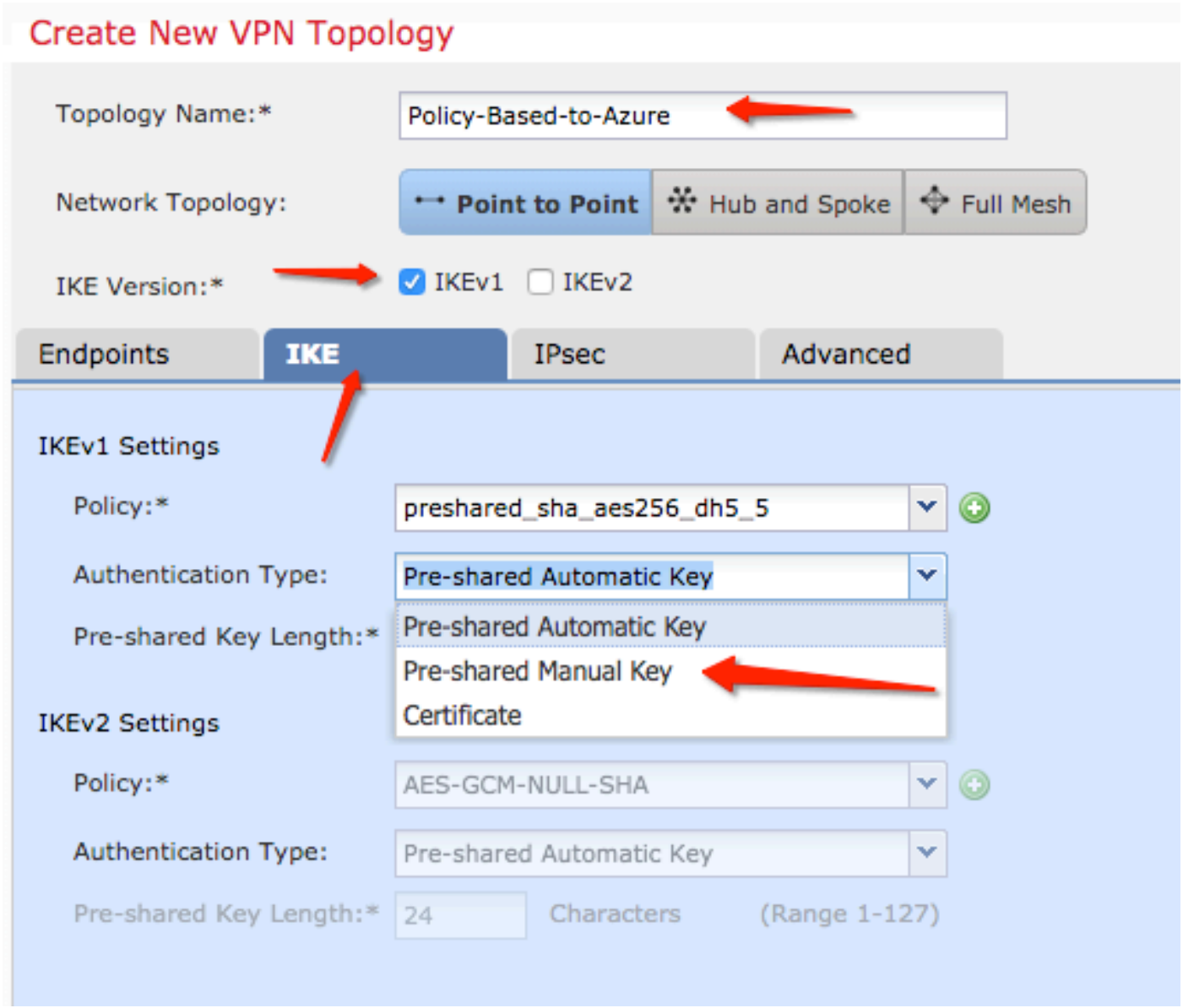
Étape 1 : création d'une stratégie de site à site Accédez à la **FMC dashboard > Devices > VPN > Site to Site**.

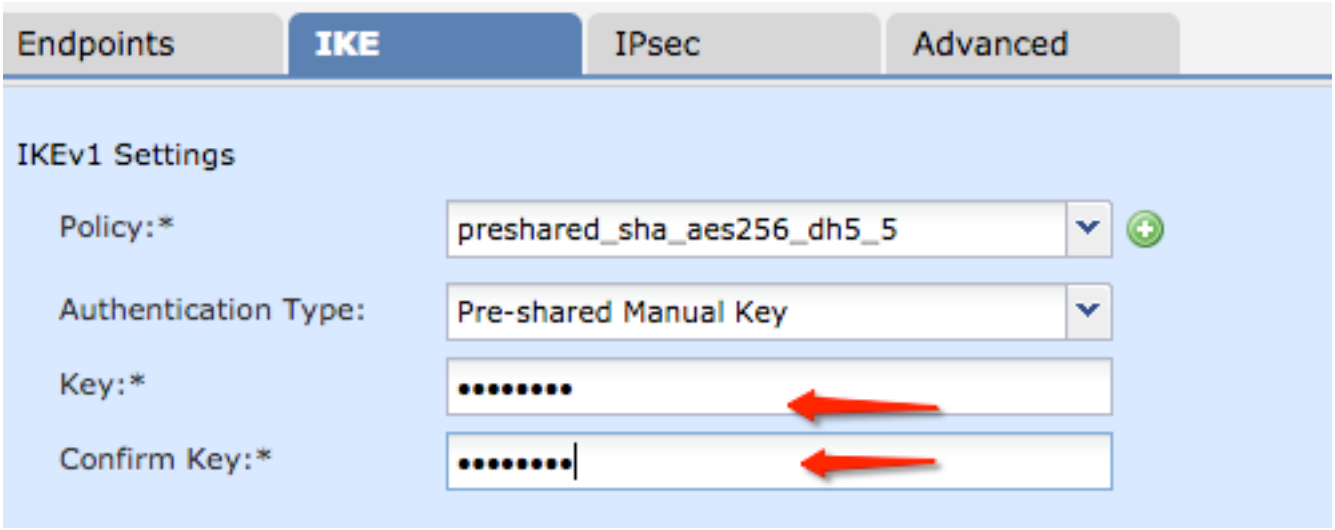
Étape 2 : création d'une nouvelle stratégie Cliquez sur le bouton **Add VPN** et choisissez l'option **Firepower Threat Defense device** .



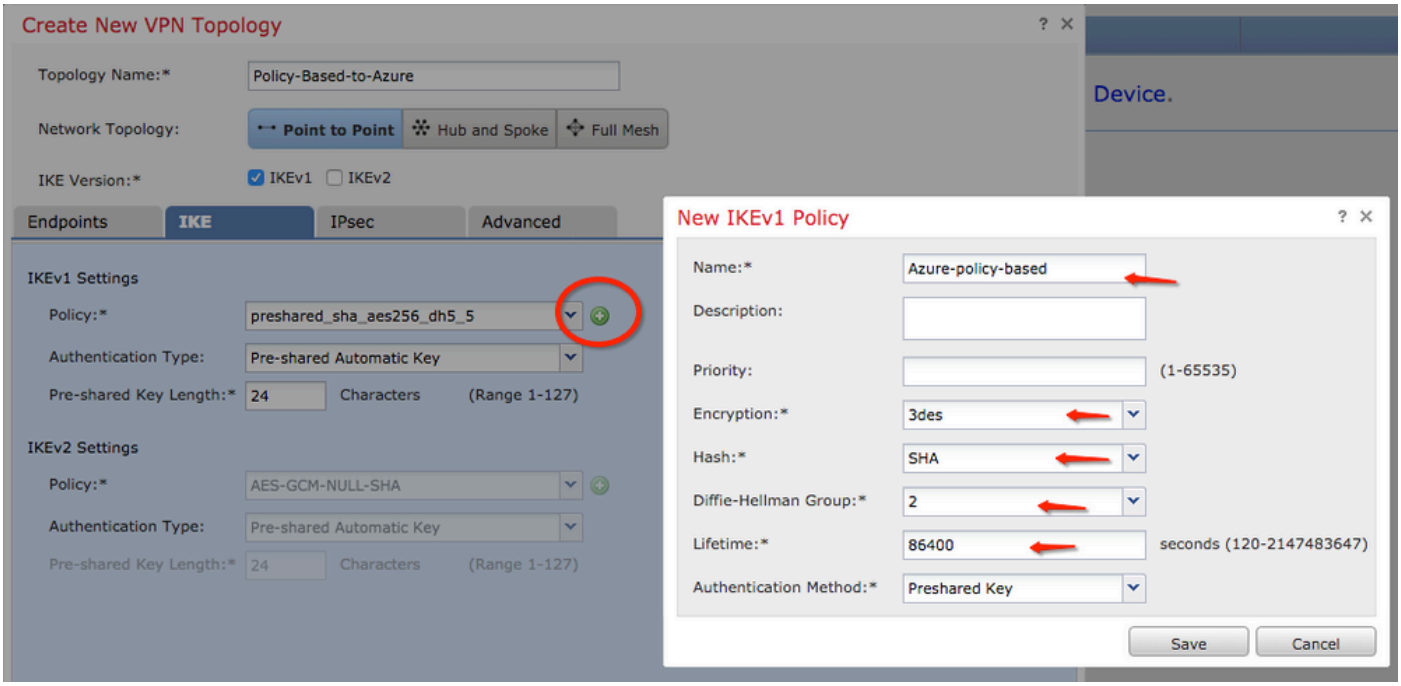
Étape 3. Sur la **Create new VPN Topology** , spécifiez votre **Topology Name**, vérifiez la **IKEV1** et cliquez sur l'option **IKE** s'affiche. Pour les besoins de cet exemple, les clés prépartagées sont utilisées comme méthode d'authentification.

Cliquez sur le bouton **Authentication Type** , puis choisissez **Pre-shared manual key** . Tapez la clé pré-partagée manuelle sur le **Key** et**Confirm Key** champs de texte.

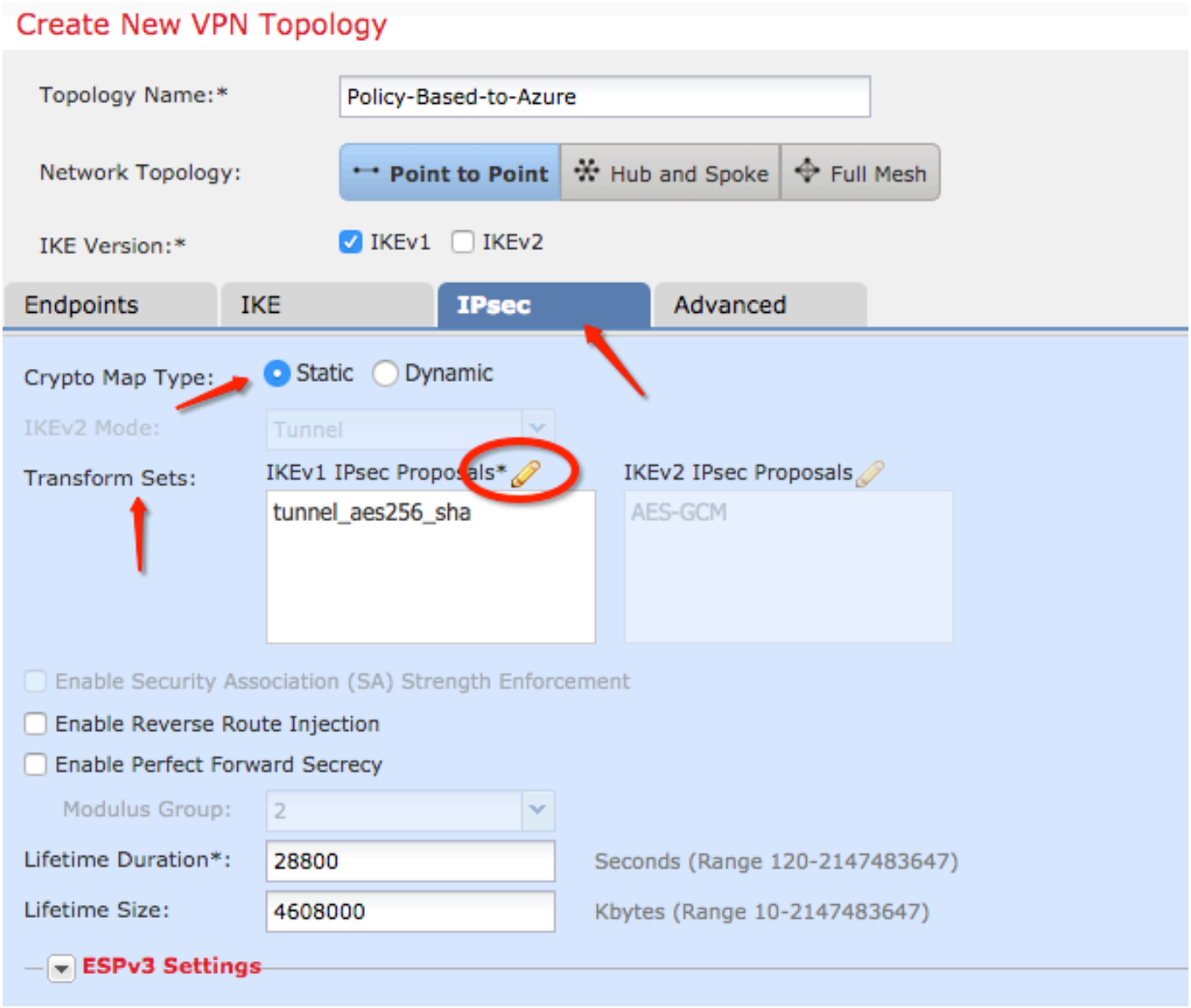




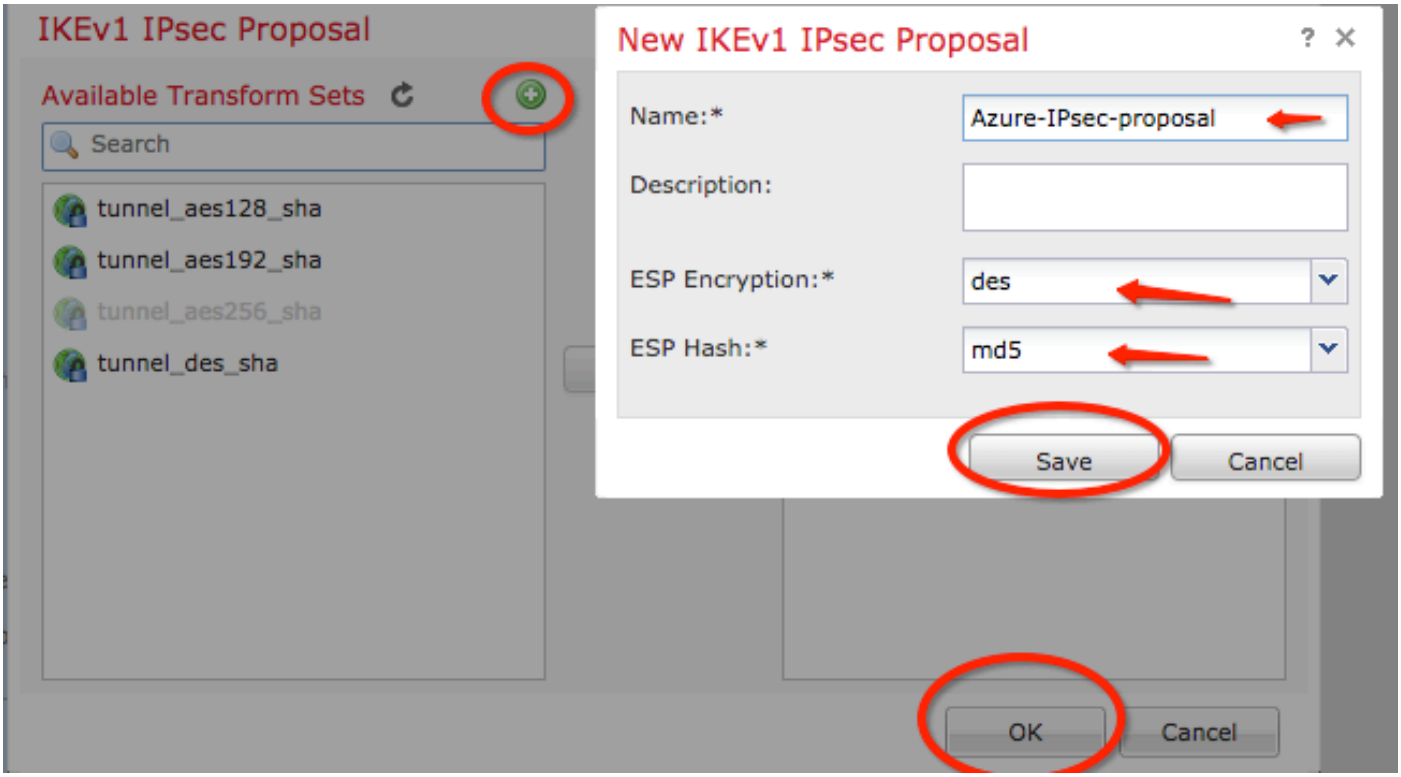
Étape 4 : configuration de la stratégie ISAKMP ou des paramètres de la phase 1 avec la création d'une nouvelle stratégie Dans la même fenêtre, cliquez sur le bouton **green plus button** pour ajouter une nouvelle stratégie ISAKMP. Spécifiez le nom de la stratégie et choisissez les méthodes de chiffrement, de hachage, de groupe Diffie-Hellman, de durée de vie et d'authentification souhaitées, puis cliquez sur **Save** .



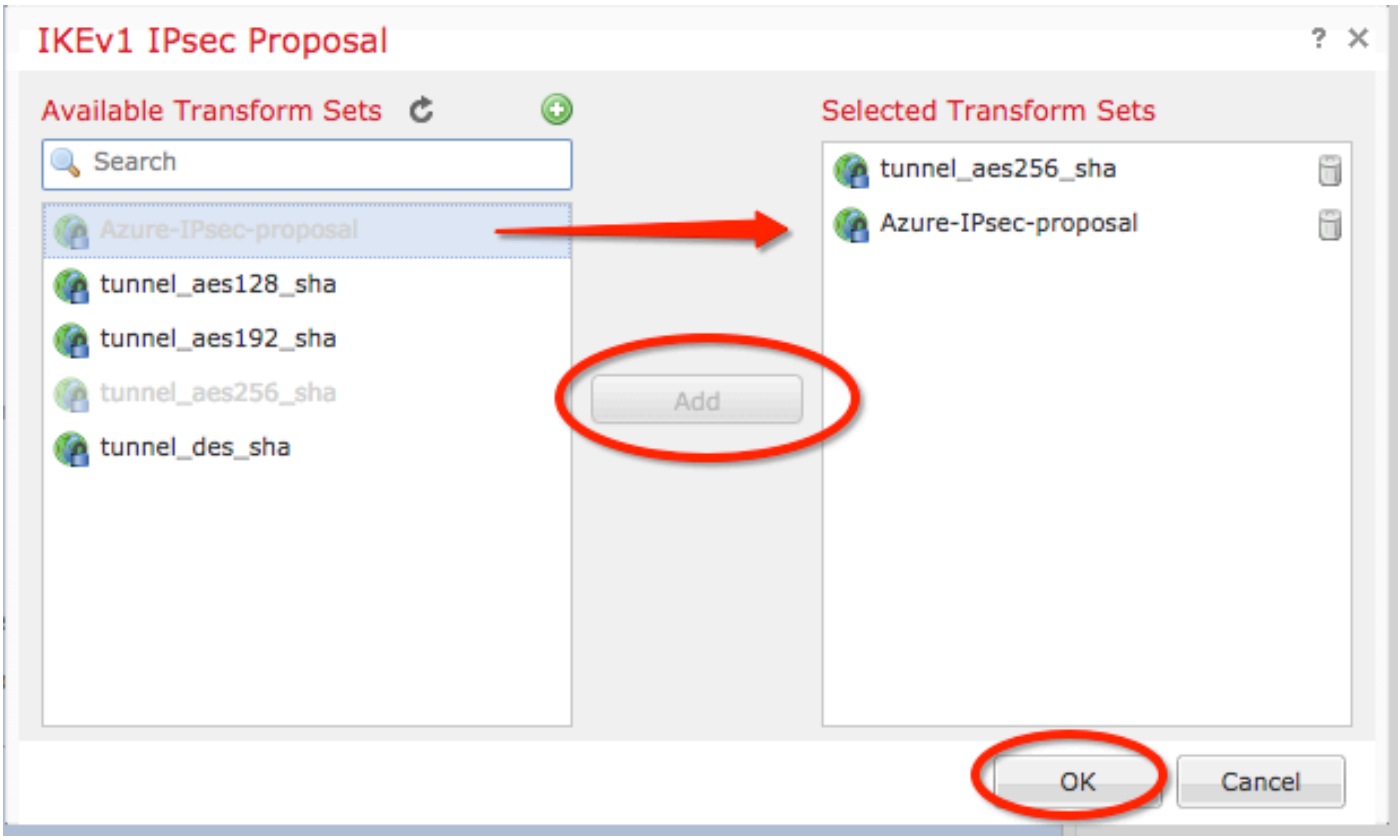
Étape 5 : configuration de la stratégie IPsec ou des paramètres de phase 2 Accédez à la **IPsec** , sélectionnez **Static** sur la **Crypto Map Type** pour une description. Cliquez sur le bouton **edit pencil** dans la barre **IKEV1 IPsec Proposals** à la **Transform Sets** option.



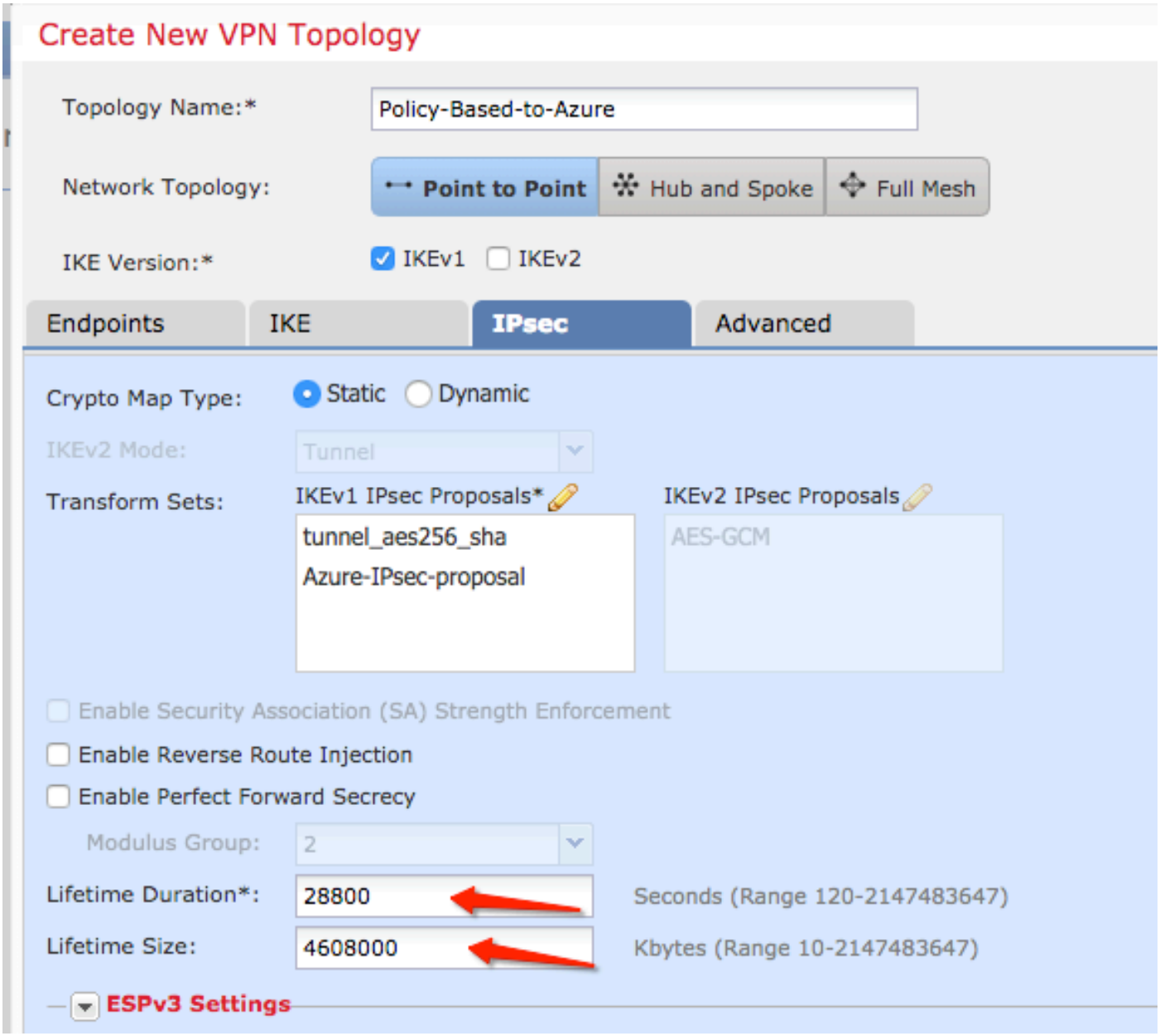
Étape 6. Créer une nouvelle proposition IPsec Sur le **IKEv1 IPSec Proposal** , cliquez sur l'icône **green plus button** pour en ajouter un nouveau. Spécifiez le nom de la stratégie et ses paramètres souhaités pour le chiffrement ESP et les algorithmes de hachage ESP, puis cliquez sur **Save** .



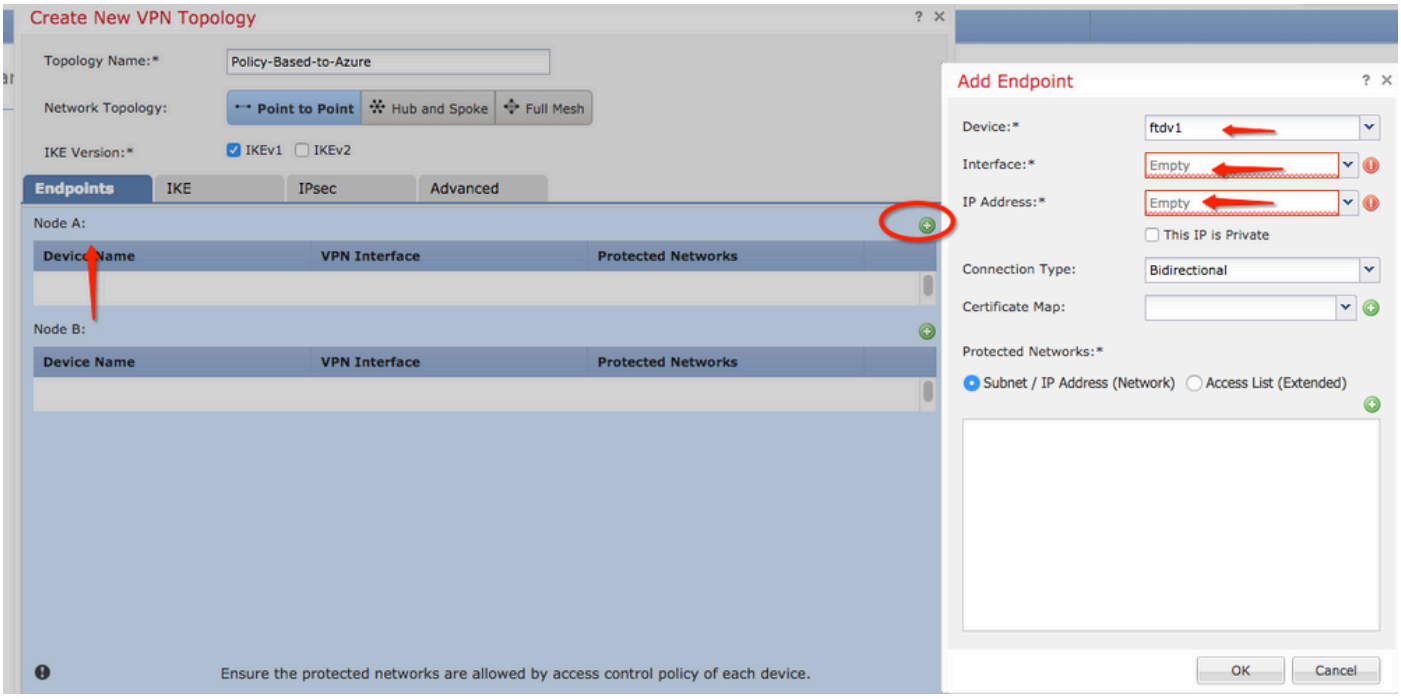
Étape 7. Sur le **IKEV1 IPsec Proposal** , ajoutez votre nouvelle stratégie IPsec à la **Selected Transform Sets** et cliquez sur **OK** .



Étape 8. Revenez à la **IPSec** , configurez la durée de vie et la taille souhaitées.



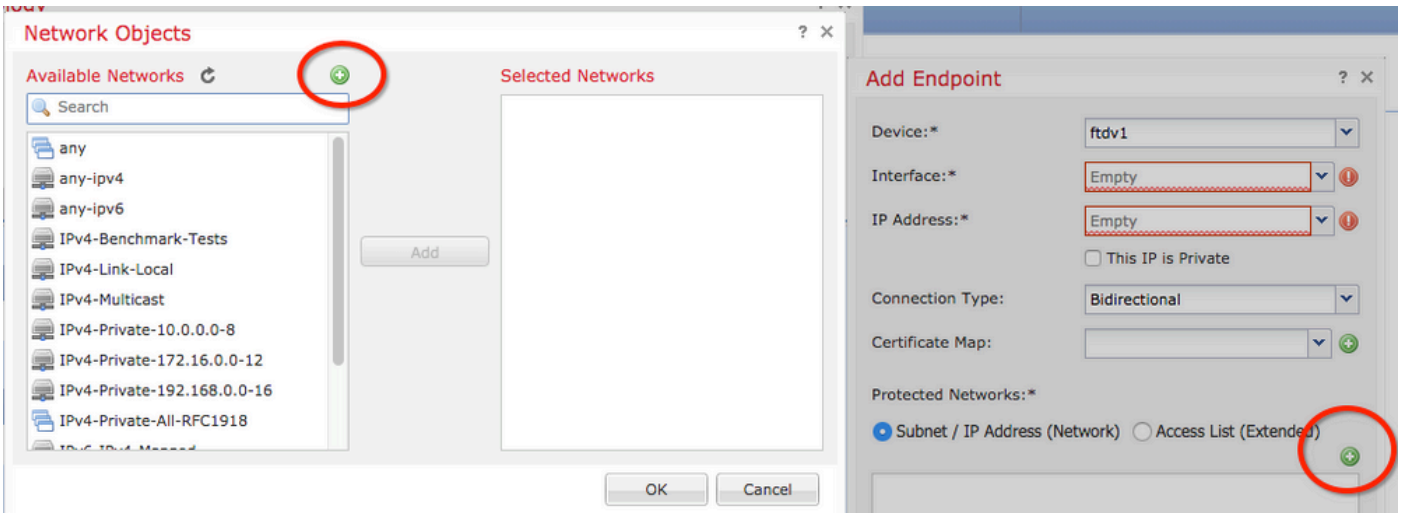
Étape 9. Choisissez le domaine de cryptage/les sélecteurs de trafic/les réseaux protégés. Accédez à la **Endpoints** s'affiche. Sur le **Node A** section cliquez sur le bouton **green plus button** pour en ajouter un nouveau. Dans cet exemple, le noeud A est utilisé comme sous-réseaux locaux vers le FTD.



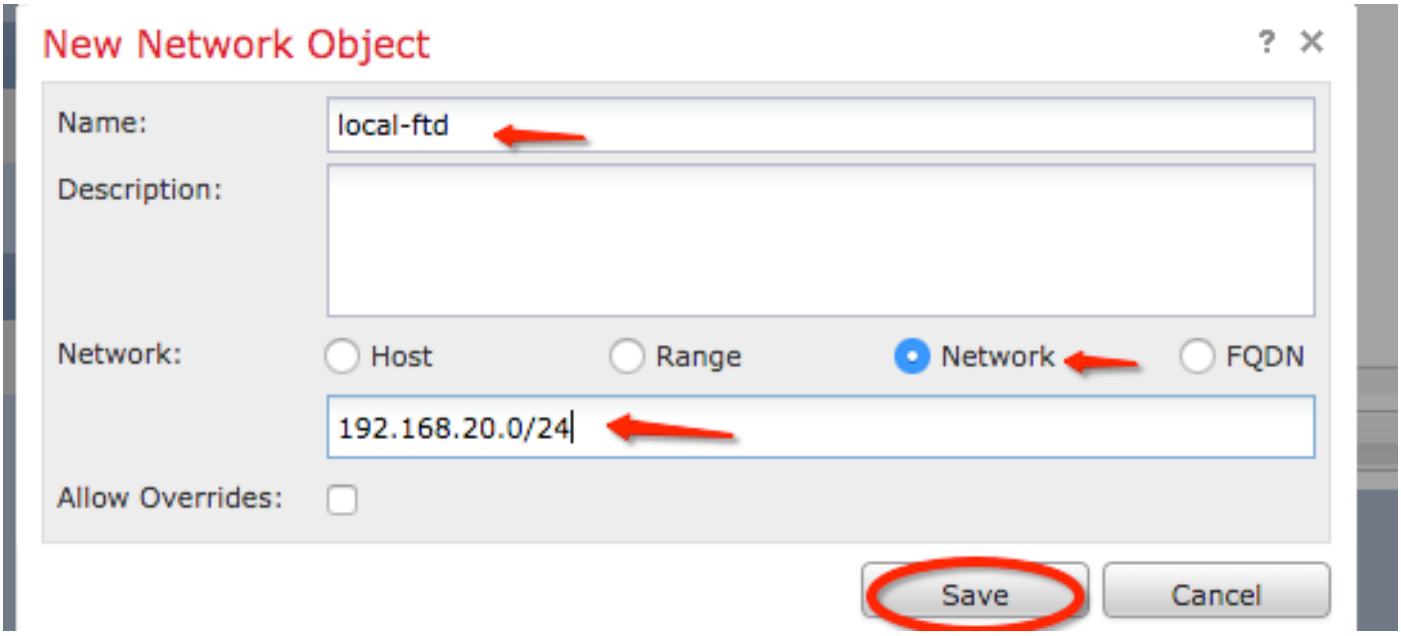
Étape 10. Sur la **Add Endpoint** , spécifiez le FTD à utiliser sur la **Device** , ainsi que son interface physique et son adresse IP à utiliser.

Étape 11. Pour spécifier le sélecteur de trafic local, accédez à la page **Protected Networks** et cliquez sur l'option **green plus button** pour créer un objet.

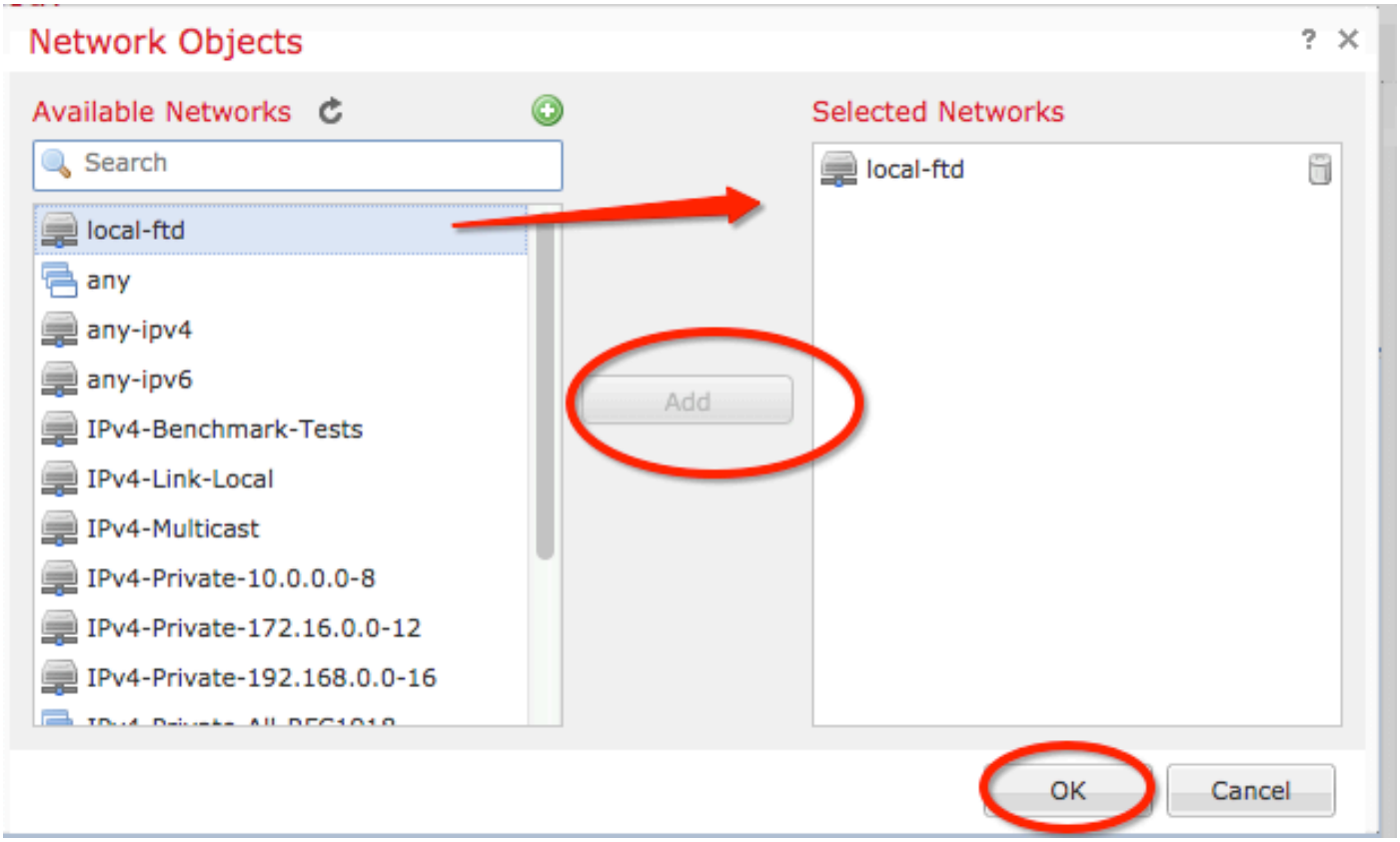
Étape 12. Dans la **Network Objects** , cliquez sur le bouton **green plus button** à côté de la **Available Networks** pour créer un nouvel objet sélecteur de trafic local.



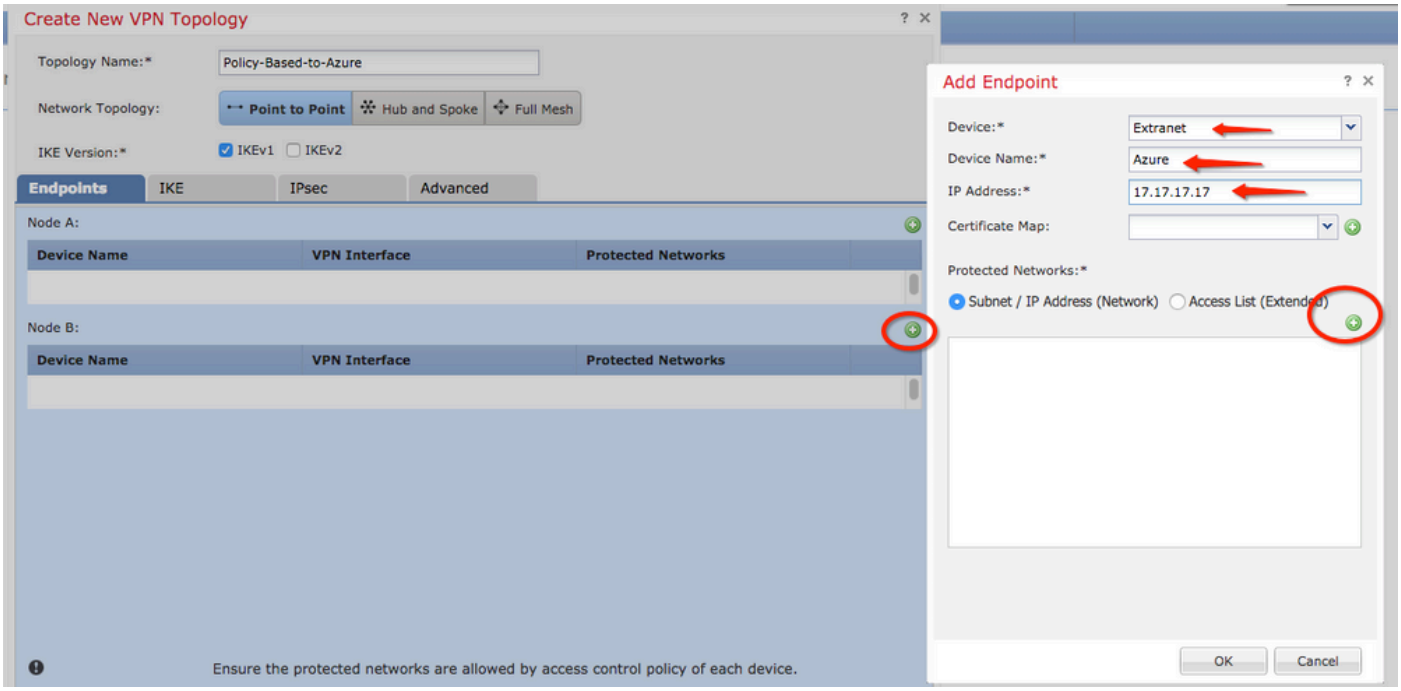
Étape 13. Dans la **New Network Object** , spécifiez le nom de l'objet et choisissez hôte/réseau/plage/FQDN. Ensuite, cliquez sur **Save** .



Étape 14. Ajouter l'objet à la **Selected Networks** section sur le **Network Objects** et cliquez sur **OK** . Cliquer **OK** sur la **Add Endpoint** s'affiche.

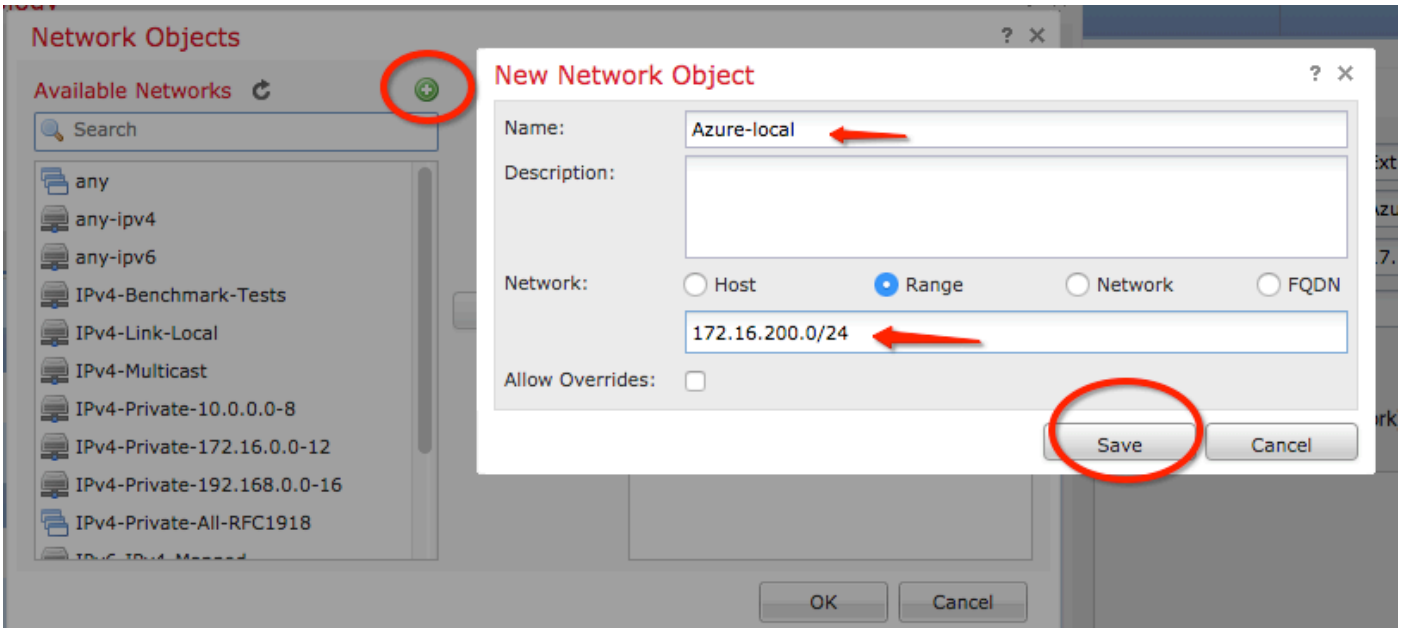


Étape 15. Définissez le point de terminaison du noeud B, qui dans cet exemple est le point de terminaison Azure. Sur le **Create New VPN Topology** , accédez à la fenêtre **Node B** et cliquez sur le bouton **green plus button** pour ajouter le sélecteur de trafic du terminal distant. Spécifier **Extranet** pour tous les terminaux homologues VPN qui ne sont pas gérés par le même FMC que le noeud A. Tapez le nom du périphérique (significatif localement uniquement) et son adresse IP.

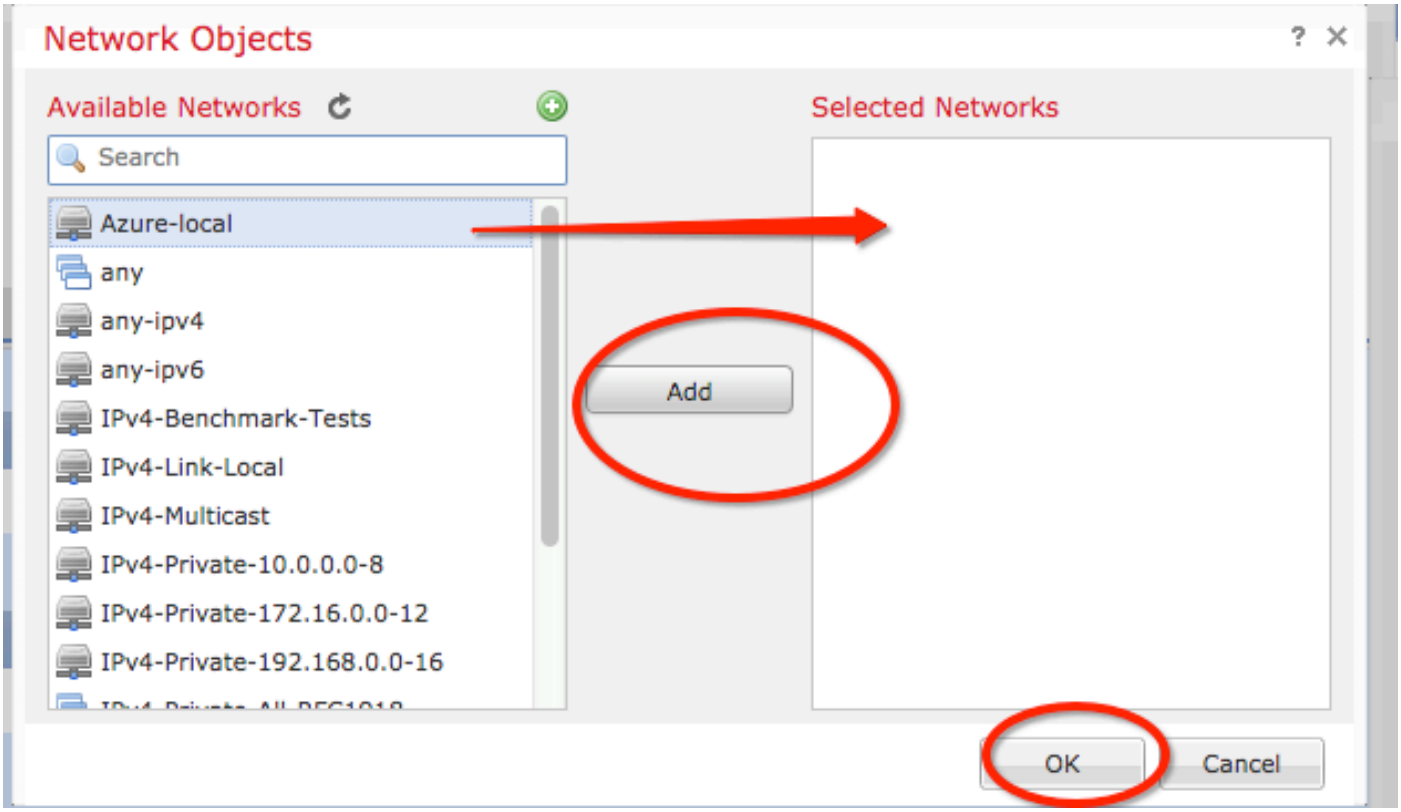


Étape 16. Créez l'objet de sélecteur de trafic distant. Accédez à la **Protected Networks** et cliquez sur le bouton **green plus button** pour ajouter un nouvel objet.

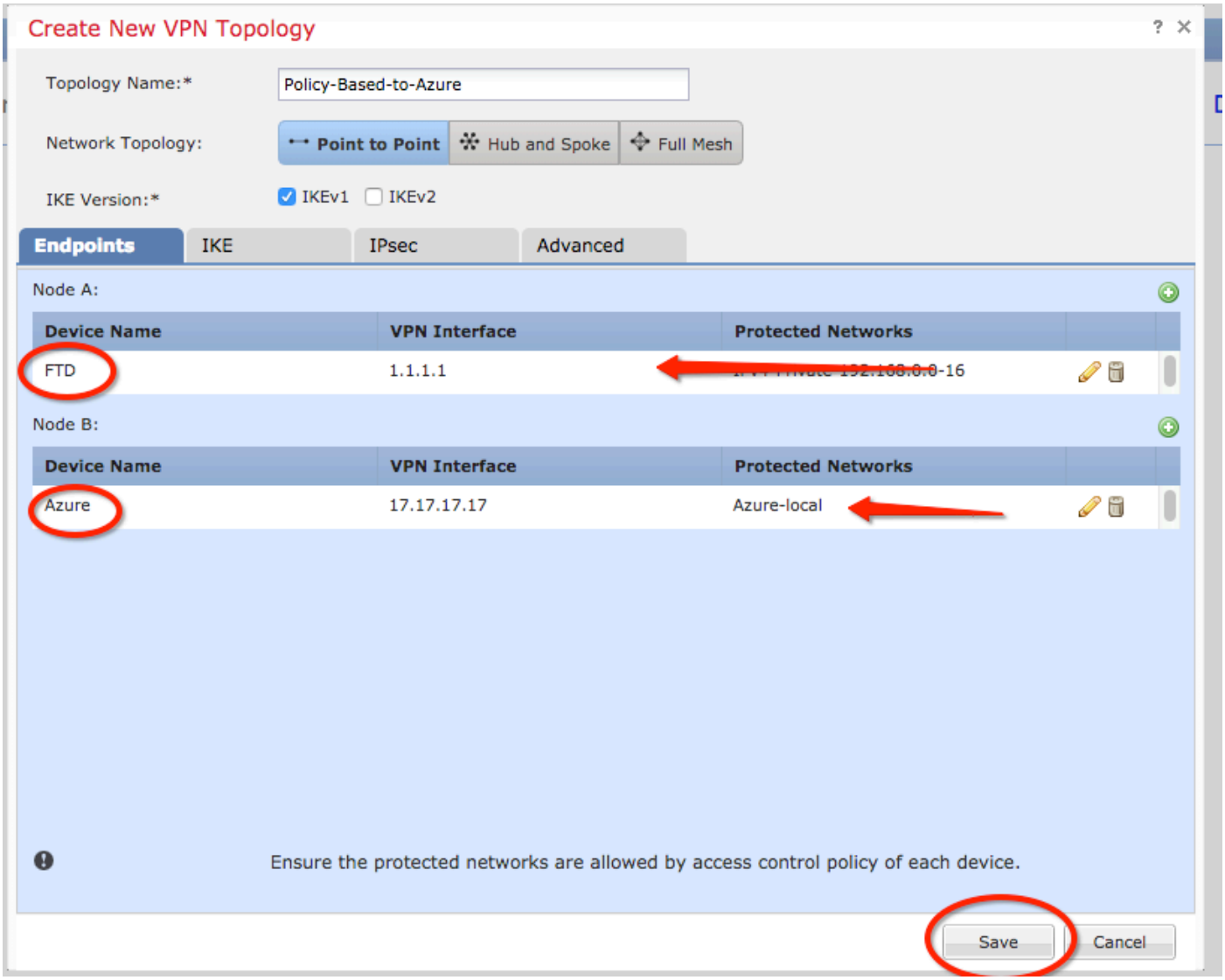
Étape 17. Dans la **Network Objects** , cliquez sur le bouton **green plus button** à côté de la **Available Networks** pour créer un nouvel objet. Sur le **New Network Object** , spécifiez le nom de l'objet et choisissez hôte/plage/réseau/FQDN, puis cliquez sur **Save** .



Étape 18. Retour sur le **Network Objects** , ajoutez votre nouvel objet distant à la **Selected Networks** et cliquez sur **OK** . Cliquer **Ok** sur la **Add Endpoint** s'affiche.



Étape 19. Dans la **Create New VPN Topology** vous pouvez maintenant voir les deux noeuds avec leurs sélecteurs de trafic/réseaux protégés corrects. Cliquer **Save** .



Étape 20. Sur le tableau de bord FMC, cliquez sur **Deploy** dans le volet supérieur droit, sélectionnez le périphérique FTD, puis cliquez sur **Deploy** .

Étape 21. Sur l'interface de ligne de commande, la configuration VPN est identique à celle des périphériques ASA.

IKEv2 basé sur la route avec des sélecteurs de trafic basés sur des politiques

Pour un VPN de site à site IKEv2 sur ASA avec crypto-cartes, suivez cette configuration. Assurez-vous qu'Azure est configuré pour le VPN basé sur la route et que UsePolicyBasedTrafficSelector doit être configuré dans le portail Azure à l'aide de PowerShell.

Ce document de Microsoft décrit la configuration de UsePolicyBasedTrafficSelector en conjonction avec le mode VPN Azure basé sur la route. Sans la réalisation de cette étape, ASA avec crypto-cartes ne parvient pas à établir la connexion en raison d'une non-correspondance dans les sélecteurs de trafic reçus d'Azure.

Référez-vous à ce document Cisco pour obtenir des informations complètes sur la configuration ASA IKEv2 avec crypto-carte.

Étape 1 : activation d'IKEv2 sur l'interface externe

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

Étape 2 : ajout d'une stratégie IKEv2 phase 1

> **Remarque** : Microsoft a publié des informations qui sont en conflit avec les attributs spécifiques de cryptage, d'intégrité et de durée de vie IKEv2 de phase 1 utilisés par Azure. Les attributs répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Les informations d'attribut IKEv2 de Microsoft relatives aux conflits sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

Étape 3 : création d'un groupe de tunnels sous les attributs IPsec et configuration de l'adresse IP de l'homologue et de la clé prépartagée de tunnel local et distant IKEv2

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

Étape 4 : création d'une liste de contrôle d'accès définissant le trafic à chiffrer et à tunnelliser Dans cet exemple, le trafic d'intérêt est le trafic du tunnel qui provient du sous-réseau 10.2.2.0 vers 10.1.1.0. Il peut contenir plusieurs entrées si plusieurs sous-réseaux sont impliqués entre les sites.

Dans les versions 8.4 et ultérieures, il est possible de créer des objets ou des groupes d'objets qui servent de conteneurs pour les réseaux, les sous-réseaux, les adresses IP d'hôte ou plusieurs objets. Créez deux objets ayant les sous-réseaux local et distant et utilisez-les pour la liste de contrôle d'accès de chiffrement et les instructions NAT.

```
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0

Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

Étape 5 : ajout d'une proposition IPsec IKEv2 phase 2 Spécifiez les paramètres de sécurité dans le mode de configuration crypto IPsec ikev2 ipsec-proposition :

protocole esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocole intégrité esp {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **Remarque** : Microsoft a publié des informations qui sont en conflit avec les attributs de cryptage et d'intégrité IPSec de phase 2 spécifiques utilisés par Azure. Les attributs répertoriés sont fournis au mieux à partir de ce document Microsoft accessible au public. Les informations d'attribut IPSec de la phase 2 de Microsoft indiquant des conflits sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

Étape 6. Configurer une carte de chiffrement et l'appliquer à l'interface externe, qui contient les composants suivants :
·L'adresse IP de l'homologue
·La liste d'accès définie qui contient le trafic d'intérêt
·Proposition IPSec phase 2 IKEv2
· Durée de vie IPSec de phase 2 en secondes
·Un paramètre optionnel PFS (Perfect Forward Secrecy), qui crée une nouvelle paire de clés Diffie-Hellman utilisées afin de protéger les données (les deux côtés doivent être compatibles PFS avant que la phase 2 n'apparaisse)

Microsoft a publié des informations qui sont en conflit avec les attributs spécifiques de durée de vie IPSec de phase 2 et PFS utilisés par Azure.

Les attributs répertoriés sont fournis au mieux par ce document Microsoft accessible au public.

Les informations d'attribut IPSec de la phase 2 de Microsoft indiquant des conflits sont visibles ici. Pour plus d'informations, contactez le support technique Microsoft Azure.

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev2 ipsec-proposal myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 27000
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
unlimited
Cisco-ASA(config)#crypto map outside_map 20 set pfs none
Cisco-ASA(config)#crypto map outside_map interface outside
```

Étape 8. Assurez-vous que le trafic VPN n'est soumis à aucune autre règle NAT. Créez une règle d'exemption NAT :

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination
static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

> **Remarque** : lorsque plusieurs sous-réseaux sont utilisés, vous devez créer des groupes d'objets avec tous les sous-réseaux source et de destination et les utiliser dans la règle NAT.

```
Cisco-ASA(config)#object-group  network 10.x.x.x_SOURCE
```

```
Cisco-ASA(config-network-object-group)#network-object  10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object  10.2.2.0 255.255.255.0

Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object  10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object  10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE
destination static 10.x.x.x_DESTINATION  10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

Vérification

Une fois que vous avez terminé la configuration sur ASA et la passerelle Azure, Azure lance le tunnel VPN. Vous pouvez vérifier que le tunnel se construit correctement avec ces commandes :

Phase 1

Vérifiez que l'association de sécurité de phase 1 a été créée :

IKEv2

Ensuite, une association de sécurité IKEv2 est créée à partir de l'interface externe locale IP 192.168.1.2 sur le port UDP 500, vers l'adresse IP de destination distante 192.168.2.2. Il existe également une SA enfant valide créée pour le trafic chiffré à transmettre.

```
Cisco-ASA# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44615, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
Status         Role
  3208253 192.168.1.2/500                                 192.168.2.2/500
READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/142 sec
*-->Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x9b60edc5/0x8e7a2e12
```

Ici, une SA IKEv1 construite avec ASA comme initiateur pour homologue IP 192.168.2.2 avec une durée de vie restante de 86388 secondes est affichée.

```
Cisco-ASA# sh crypto ikev1 sa detail

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.2.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : aes             Hash    : SHA
    Auth    : preshared       Lifetime: 86400
    Lifetime Remaining: 86388
```

Phase 2

Vérifiez que l'association de sécurité IPSec de phase 2 a été créée avec **show crypto ipsec sa peer [peer-ip]** .

```
Cisco-ASA# show crypto ipsec sa peer 192.168.2.2
peer address: 192.168.2.2
Crypto map tag: outside, seq num: 10, local addr: 192.168.1.2

access-list VPN extended permit ip 192.168.0.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.2.2


#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.2/500, remote crypto endpt.: 192.168.2.2/500
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8E7A2E12
current inbound spi : 9B60EDC5

inbound esp sas:
spi: 0x9B60EDC5 (2606820805)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (4193279/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:
spi: 0x8E7A2E12 (2390371858)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (3962879/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Quatre paquets sont envoyés et quatre sont reçus via l'association de sécurité IPSec sans erreur. Un SA entrant avec SPI 0x9B60EDC5 et un SA sortant avec SPI 0x8E7A2E12 sont installés comme prévu.

Vous pouvez également vérifier que les données traversent le tunnel en vérifiant **vpn-sessiondb l2l**

entrées :

```
Cisco-ASA#show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection : 192.168.2.2
Index : 44615 IP Addr : 192.168.2.2
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 18:32:54 UTC Tue Mar 13 2018
Duration : 0h:05m:22s
```

Octets Tx : et octets Rx : affiche les compteurs de données envoyés et reçus sur l'association de sécurité IPSec.

Dépannage

Étape 1. Vérifiez que le trafic pour le VPN est reçu par ASA sur l'interface interne destinée au réseau privé Azure. Pour tester, vous pouvez configurer une requête ping continue à partir d'un client interne et configurer une capture de paquets sur ASA pour vérifier qu'elle est reçue :

capture [cap-name] interface [if-name] match [protocol] [src-ip] [src-mask] [dest-ip] [dest-mask]

show capture [cap-name]

```
Cisco-ASA#capture inside interface inside match ip host [local-host] host [remote-host]
Cisco-ASA#show capture inside

2 packets captured

   1: 18:50:42.835863       192.168.0.2 > 192.168.3.2: icmp: echo request
   2: 18:50:42.839128       192.168.3.2 > 192.168.0.2: icmp: echo reply
2 packets shown
```

Si le trafic de réponse d'Azure est détecté, le VPN est correctement construit et envoie/reçoit le trafic.

Si le trafic source est absent, vérifiez que votre expéditeur achemine correctement vers l'ASA.

Si le trafic source est détecté mais que le trafic de réponse d'Azure est absent, poursuivez la vérification.

Étape 2. Vérifiez que le trafic reçu sur l'interface interne ASA est correctement traité par ASA et acheminé vers le VPN :

Pour simuler une requête d'écho ICMP :
packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip] detail

Les instructions d'utilisation complètes de Packet Tracer sont disponibles ici :
https://community.cisco.com:443/t5/security-knowledge-base/troubleshooting-access-problems-using-packet-tracer/ta-p/3114976

```
Cisco-ASA# packet-tracer input inside icmp 192.168.0.2 8 0 192.168.3.2 detail

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19afb0a0, priority=13, domain=capture, deny=false
        hits=3, user_data=0x7f6c19afb9b0, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000
        input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c195971f0, priority=1, domain=permit, deny=false
        hits=32, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=inside, output_ifc=any

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.1 using egress ifc  outside

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19250290, priority=0, domain=nat-per-session, deny=true
        hits=41, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1987c120, priority=0, domain=inspect-ip-options, deny=true
        hits=26, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any
```

```
Phase: 6
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19a60280, priority=70, domain=qos-per-class, deny=false
        hits=30, user_data=0x7f6c19a5c030, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1983ab50, priority=66, domain=inspect-icmp-error, deny=false
        hits=27, user_data=0x7f6c1987afc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f6c19afe1a0, priority=70, domain=encrypt, deny=false
        hits=2, user_data=0x13134, cs_id=0x7f6c19349670, reverse, flags=0x0, protocol=0
        src ip/id=192.168.0.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.3.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=outside

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 43, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_encrypt
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
```

```
output-status: up
output-line-status: up
Action: allow
```

Notez que la NAT exempte le trafic (aucune traduction n'est prise en compte). Vérifiez qu'aucune traduction NAT ne se produit sur le trafic VPN.

Vérifiez également la **output-interface** est correct : il doit s'agir de l'interface physique où la carte de chiffrement est appliquée ou de l'interface de tunnel virtuel.

Assurez-vous qu'aucune suppression de liste d'accès n'est visible.

Si la phase VPN affiche **ENCRYPT: ALLOW** , le tunnel est déjà construit et vous pouvez voir IPSec SA installé avec des encaps.

Étape 2.1. Si **ENCRYPT: ALLOW** vu dans packet-tracer.

Vérifiez que l'association de sécurité IPsec est installée et chiffre le trafic à l'aide de **show crypto ipsec sa** .

Vous pouvez effectuer une capture sur l'interface externe pour vérifier que les paquets chiffrés sont envoyés depuis ASA et que les réponses chiffrées sont reçues d'Azure.

Étape 2.2. Si **ENCRYPT:DROP** vu dans packet-tracer.

Le tunnel VPN n'est pas encore établi mais est en négociation. Il s'agit d'une condition attendue lorsque vous activez le tunnel pour la première fois. Exécutez les débogages pour afficher le processus de négociation de tunnel et identifier où et si une défaillance se produit.

Tout d'abord, vérifiez que la version correcte d'IKE est déclenchée et que le processus ike-common ne présente aucune erreur pertinente :

```
Cisco-ASA#debug crypto ike-common 255

Cisco-ASA# Mar 13 18:58:14 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE message to
IKEv1.  Map Tag = outside.  Map Sequence Number = 10.
```

Si aucune sortie de débogage ike-common n'est vue lorsque le trafic VPN est initié, cela signifie que le trafic est abandonné avant d'atteindre le processus crypto ou que crypto ikev1/ikev2 n'est pas activé sur le boîtier. Vérifiez à nouveau la configuration du chiffrement et les abandons de paquets.

Si les débogages ike-common montrent que le processus de chiffrement est déclenché, déboguez la version configurée d'IKE pour afficher les messages de négociation de tunnel et identifier où l'échec se produit dans la construction de tunnel avec Azure.

IKEv1

La procédure de débogage et l'analyse complètes de ikev1 sont disponibles ici.

```
Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127
```

IKEv2

La procédure de débogage ikev2 complète et l'analyse sont disponibles ici.

```
Cisco-ASA#debug crypto ikev2 platform 127
Cisco-ASA#debug crypto ikev2 protocol 127
Cisco-ASA#debug crypto ipsec 127
```

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.