Configuration d'un VPN basé sur la stratégie et la route depuis ASA et FTD vers MS Azure

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Concepts
  - Domaine de cryptage VPN

Configurer

- Configuration IKEv1 sur ASA
- IKEv2 basé sur la route avec VTI sur le code ASA 9.8 (1) ou ultérieur
- Configuration IKEv1 sur FTD
- IKEv2 basé sur la route avec des sélecteurs de trafic basés sur des politiques

Vérifier

- Phase 1
- Phase 2

Dépannage

- IKEv1
- IKEv2

Introduction

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

Conditions préalables

Exigences

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 crypto-carte (Azure doit être configuré pour le VPN basé sur la route avec UsePolicyBasedTrafficSectors.)
- Connaissance de FMC pour la gestion et la configuration FTD.

Composants utilisés

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

- Périphérique FTD Cisco
- Cisco FMC
- Microsoft Azure
- Cisco ASAv exécutant ASA 9.18.4.22

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

Concepts

Domaine de cryptage VPN

La plage d'adresses IP avec IPSec lui permet de participer au tunnel VPN. Le domaine de cryptage est défini à l'aide d'un sélecteur de trafic local et de trafic distant pour spécifier quelles plages de sous-réseaux local et distant sont capturées et cryptées par IPSec.

Voici deux méthodes pour définir les domaines de cryptage VPN : sélecteurs de trafic basés sur la route ou sur 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 Firepower Management Center (FMC) 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 d'Internet Key Exchange (IKE) que vous pouvez configurer en fonction de la méthode VPN sélectionnée. La version basée sur la route nécessite IKEv2 et la version basée sur la stratégie requiert IKEv1. Si IKEv2 est utilisé, la version basée sur la route dans Azure doit être sélectionnée et ASA doit utiliser un VTI.

Si l'ASA ne prend en charge que les crypto-cartes en raison de la version du code, Azure doit être configuré pour les sélecteurs de trafic basés sur la route 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 UsePolicyBasedTrafficSelector, à laquelle vous pouvez vous référer : Connecter une passerelle VPN à plusieurs périphériques VPN basés sur des stratégies sur site.

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

- Pour ASA configuré avec un VTI, Azure doit être configuré pour le VPN basé sur la route.

- Pour FTD, des informations supplémentaires sur la façon de configurer les VTI peuvent être trouvées ici ; Guide de configuration de Firepower Management Center, Version 6.7
- 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.

Configurer

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, implémentez 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.

Référence Configurez les tunnels site à site IKEv1 IPsec avec l'ASDM ou l'interface de ligne de commande sur ASAv pour obtenir des informations complètes sur IKEv1 sur la configuration ASA.

---

1. Activez IKEv1 sur l'interface externe.

<#root>

```
Cisco-ASA(config)#

crypto ikev1 enable outside
```

---

2. Créez une stratégie IKEv1 qui définit les algorithmes/méthodes à utiliser pour le hachage, l'authentification, le groupe Diffie-Hellman, la durée de vie et le chiffrement.

Remarque : Les attributs IKEv1 de phase 1 répertoriés proviennent de périphériques VPN et de paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
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 14

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

lifetime 28800

---

3. Créez un groupe de tunnels sous les attributs IPsec et configurez l'adresse IP de l'homologue et la clé pré-partagée du tunnel.

<#root>

```
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
```

---

4. Créez une liste d’accès qui définit le trafic à chiffrer et à tunnelliser.

Dans cet exemple, le trafic d'intérêt provient du tunnel provenant 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).

<#root>

```
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
```

---

5. Configurez le Transform Set (TS), qui doit impliquer le mot clé IKEv1. Un TS identique doit également être créé sur l'extrémité distante.

Remarque : Les attributs IKEv1 de phase 2 répertoriés peuvent être référencés à partir des périphériques VPN et des paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
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 :

- Le TS.
- Adresse IP de l'homologue.
- La liste d'accès définie qui contient le trafic d'intérêt.
- La configuration ne définit pas PFS (Perfect Forward Secrecy). Les périphériques VPN et les paramètres IPsec/IKE pour les connexions de passerelle VPN site à site indiquent que PFS est désactivé pour IKEv1 dans Azure.

Un paramètre PFS facultatif crée une nouvelle paire de clés Diffie-Hellman qui est utilisée pour protéger les données (les deux côtés doivent être compatibles PFS avant que la phase 2 ne s'affiche). Ce paramètre peut être activé en exécutant cette commande : crypto map outside_map 20 set pfs.

- Les durées de vie IPSec de phase 2 sont définies en fonction des périphériques VPN et des paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
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
```

---

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

<#root>

```
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
```

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.

<#root>

```
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_DESTINA
```

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

Pour un VPN basé sur la route de site à site IKEv2 sur code ASA, utilisez 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.

Référence CLI Book 3 : Guide de configuration de l'interface de ligne de commande VPN de la gamme Cisco ASA, 9.8 pour des informations complètes sur la configuration ASA VTI.

---

1. Activez IKEv2 sur l’interface externe :

```
<#root>
```

```
Cisco-ASA(config)#

crypto ikev2 enable outside
```

---

2. Ajoutez une stratégie IKEv2 phase 1.

Remarque : Microsoft a publié des informations qui entrent en conflit avec les attributs spécifiques de cryptage, d'intégrité et de durée de vie IKEv2 Phase 1 utilisés par Azure. Les attributs répertoriés proviennent des périphériques VPN et des paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Les informations qui entrent en conflit avec l'attribut IKEv2 de Microsoft sont Sample Configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
Cisco-ASA(config)#

crypto ikev2 policy 1

Cisco-ASA(config-ikev2-policy)#

encryption aes-256

Cisco-ASA(config-ikev2-policy)#

integrity sha256

Cisco-ASA(config-ikev2-policy)#

group 14

Cisco-ASA(config-ikev2-policy)#

lifetime seconds 28800
```

---

3. Ajoutez 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 entrent en conflit avec les attributs de cryptage et d'intégrité IPSec de phase 2 spécifiques utilisés par Azure. Les attributs répertoriés proviennent des périphériques VPN et des paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Les informations qui entrent en conflit avec l'attribut IPSec de la phase 2 de Microsoft sont Exemple de configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
Cisco-ASA(config)#

crypto ipsec ikev2 ipsec-proposal SET1


Cisco-ASA(config-ipsec-proposal)#

protocol esp encryption aes-256


Cisco-ASA(config-ipsec-proposal)#

protocol esp integrity sha-256
```

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)

Remarque : 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 issus des offres IKE Quick Mode Security Association (IKE Quick Mode SA) VPN basées sur la route. Les informations qui entrent en conflit avec l'attribut IPSec de la phase 2 de Microsoft sont Exemple de configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
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
```

---

5. Créez un groupe de tunnels sous les attributs IPsec et configurez l'adresse IP de l'homologue et la clé pré-partagée de tunnel local et distant IKEv2 :

```
<#root>
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
```

---

6. Créez une 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]

<#root>

```
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
```

---

7. Créez une route statique pour diriger le trafic vers le tunnel. Pour ajouter une route statique, exécutez cette commande :

route if_name dest_ip mask ip_passerelle [distance]

Le dest_ip et le mask est l'adresse IP pour le réseau de destination dans le cloud Azure, par exemple, 10.0.0.0/24. Le gateway_ip doit être n'importe quelle adresse IP (existante ou inexistante) sur le sous-réseau de l'interface de tunnel, telle que 169.254.0.2. Le but de ce gateway_ip est de pointer le trafic dans l'interface de tunnel, cependant, l'adresse IP de passerelle particulière elle-même n'est pas importante.

<#root>

```
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.

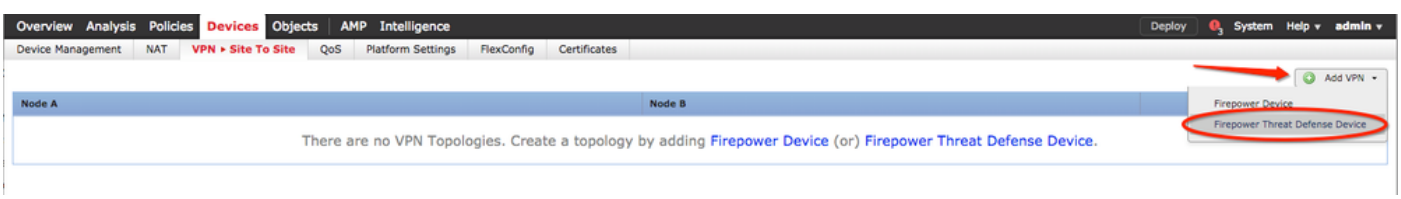
---

1. Créez une stratégie de site à site. Accédez au tableau de bord FMC > Devices > VPN > Site to Site.



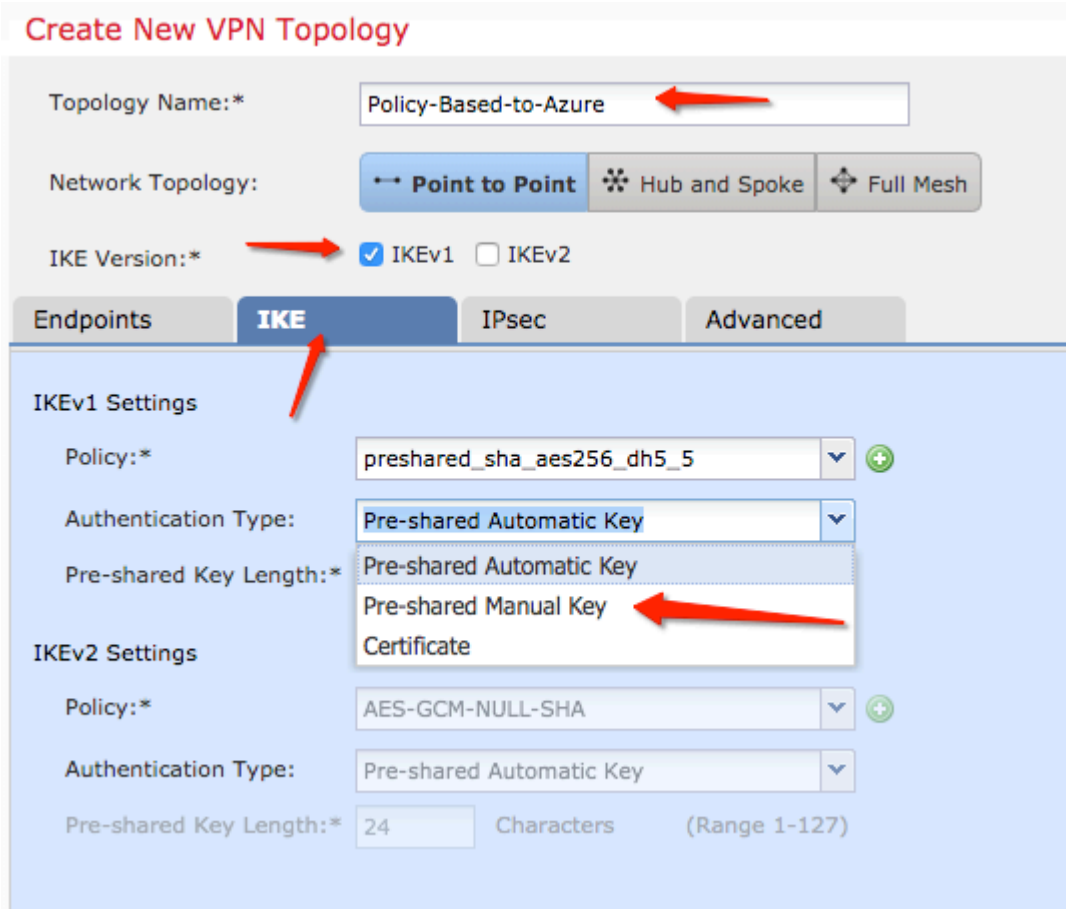
---

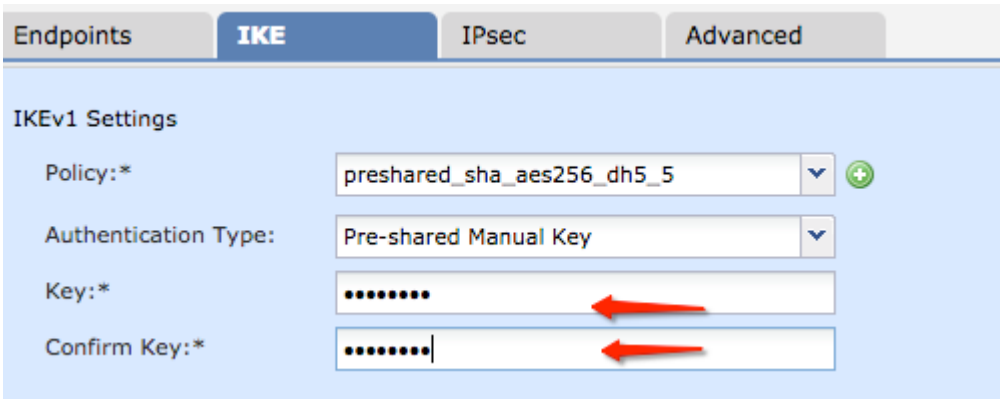
2. Créez une nouvelle stratégie. Cliquez sur le menu déroulant Add VPN et choisissez Firepower Threat Defense Device.



---

3. Dans la fenêtre Create new VPN Topology, spécifiez votre nom de topologie, cochez la case du protocole IKEV1 et cliquez sur l'onglet IKE. Dans cet exemple, les clés prépartagées sont utilisées comme méthode d'authentification. Cliquez sur le menu déroulant Authentication Type et choisissez Pre-shared Manual Key. Tapez la clé pré-partagée manuelle dans les champs de texte Clé et Confirmer la clé.

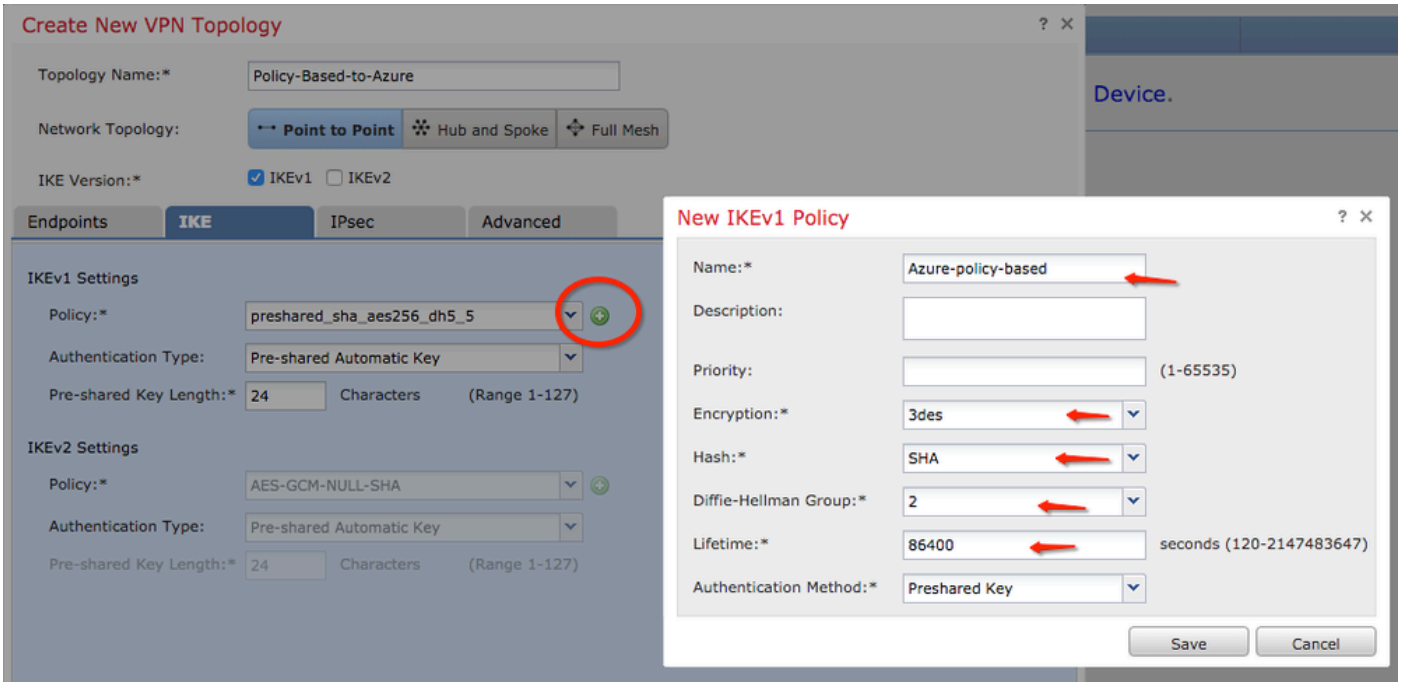




---

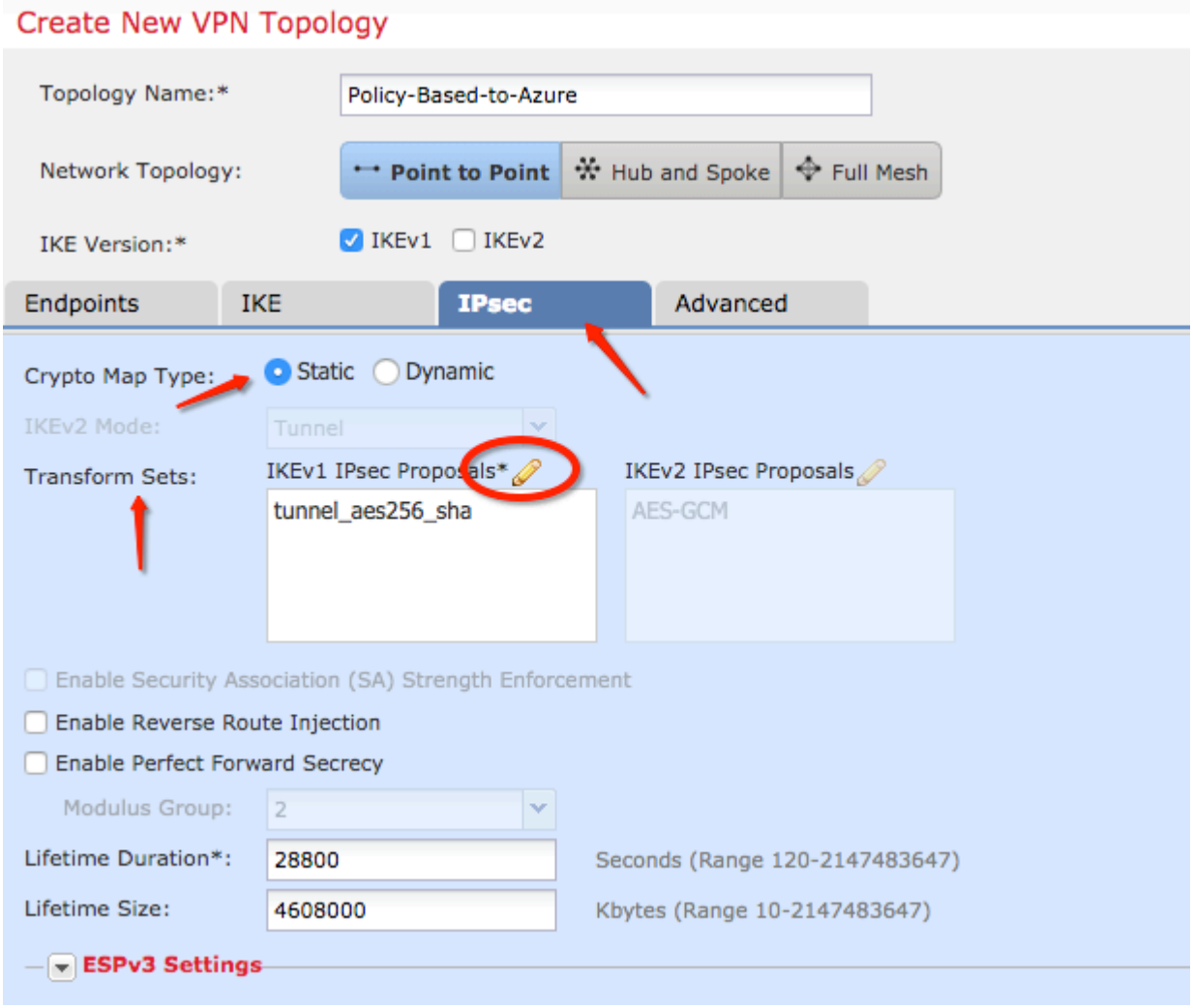
4. Configurez la stratégie ISAKMP ou les paramètres de la phase 1 avec la création d'une nouvelle stratégie. Dans la même fenêtre, cliquez sur le bouton + vert pour ajouter une nouvelle stratégie ISAKMP. Spécifiez le nom de la stratégie et choisissez le cryptage, le hachage, le

groupe Diffie-Hellman, la durée de vie et la méthode d'authentification souhaités, puis cliquez sur Enregistrer.



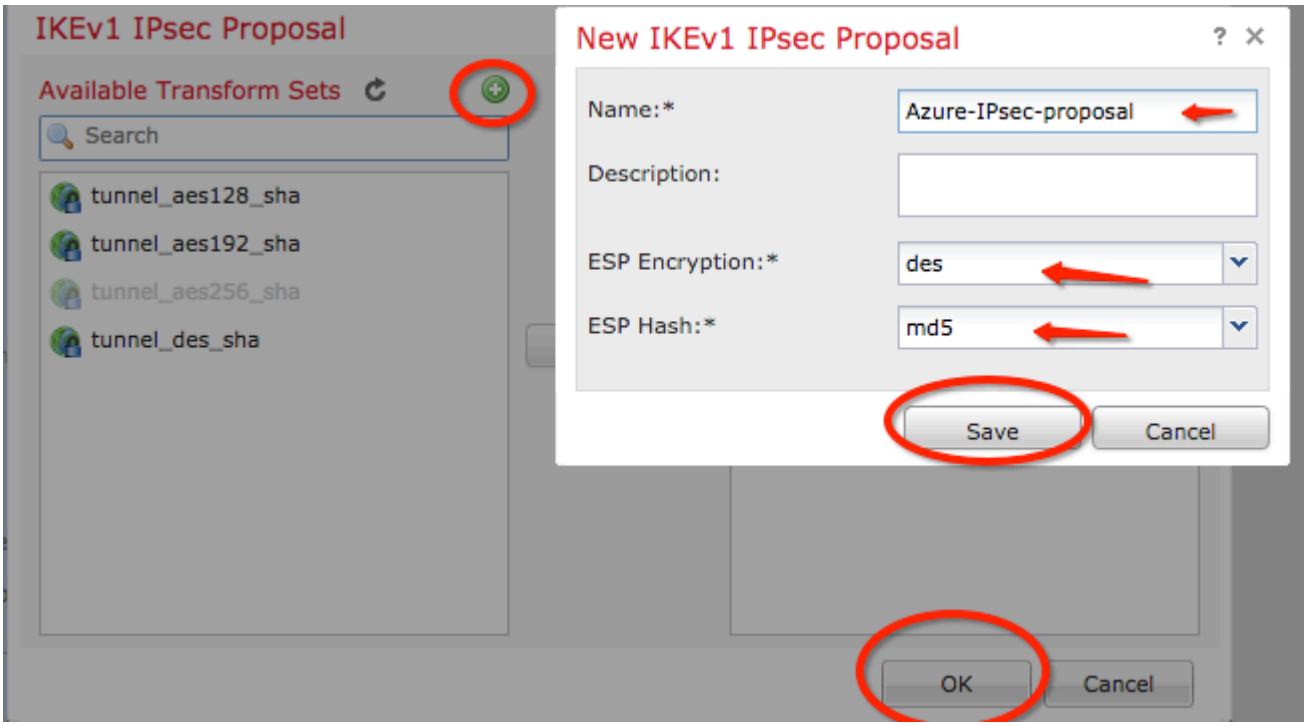
---

5. Configurez la stratégie IPsec ou les paramètres de phase 2. Accédez à l'onglet IPsec, choisissez Static sur la case à cocher Crypto Map Type. Cliquez sur l'icône de modification du crayon dans la section IKEV1 IPsec Proposal de l'option Transform Sets.



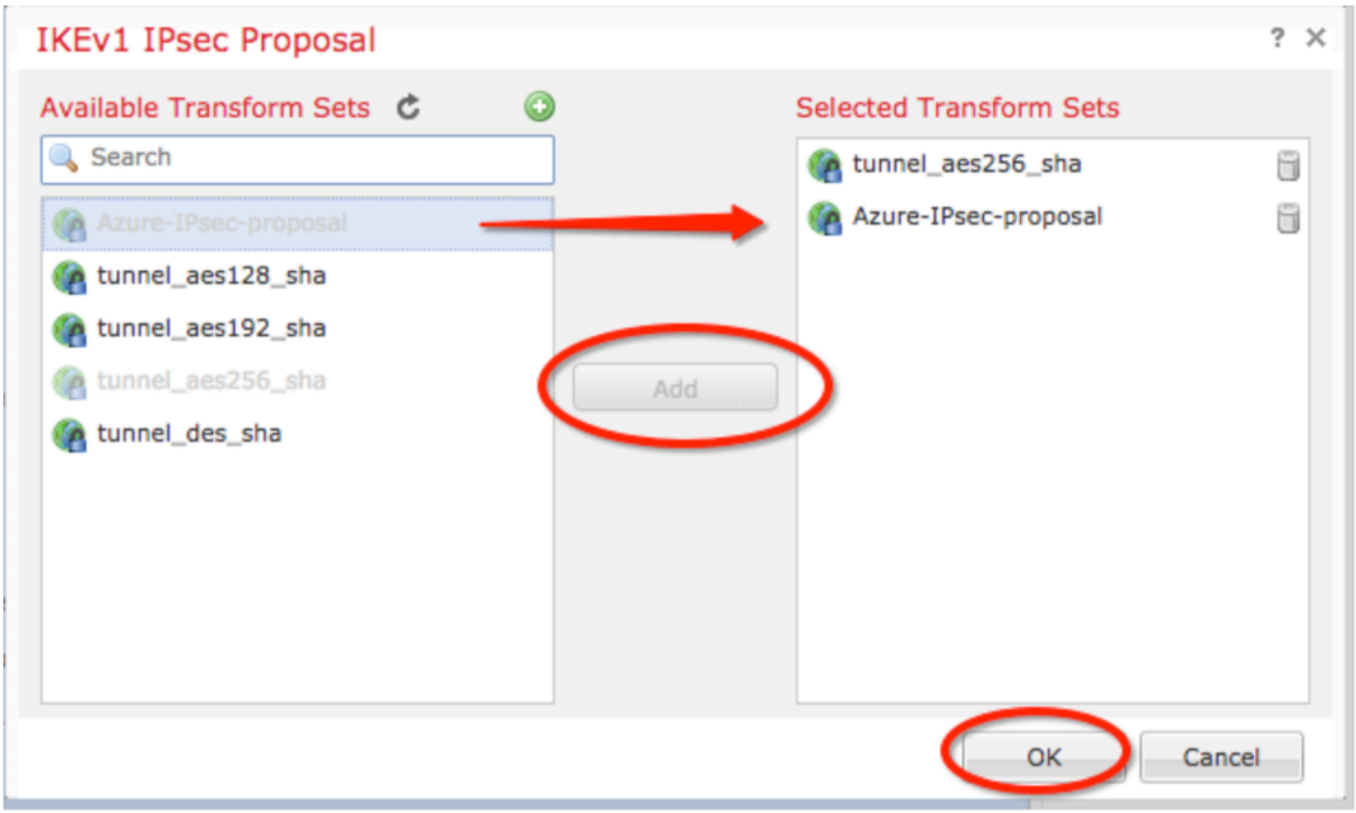
---

6. Créez une nouvelle proposition IPsec. Dans la fenêtre IKEv1 IPSec Proposal, cliquez sur le bouton + vert 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 Enregistrer.



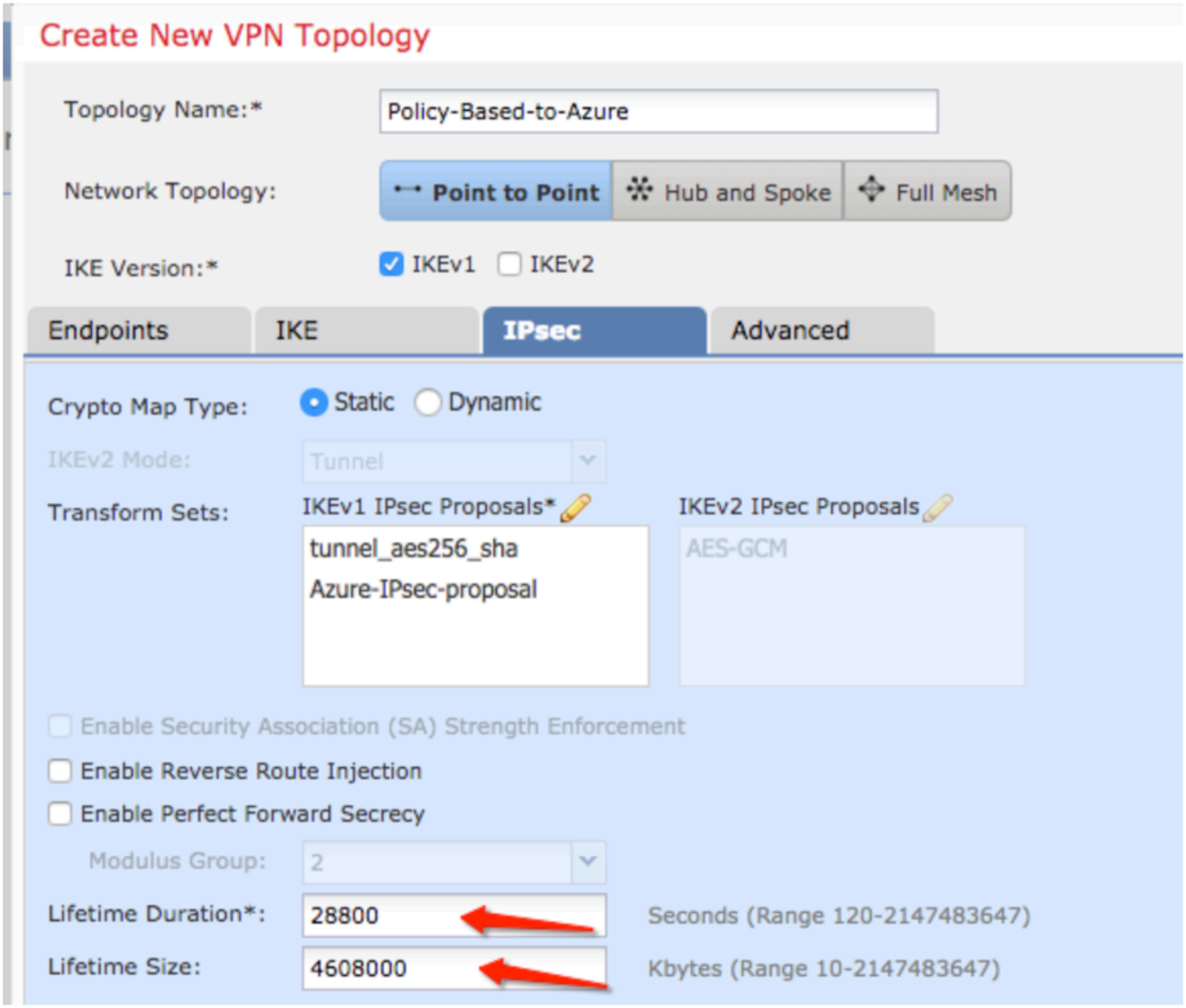
---

7. Dans la fenêtre IKEV1 IPsec Proposal, ajoutez votre nouvelle stratégie IPsec à la section Selected Transform Sets et cliquez sur OK.



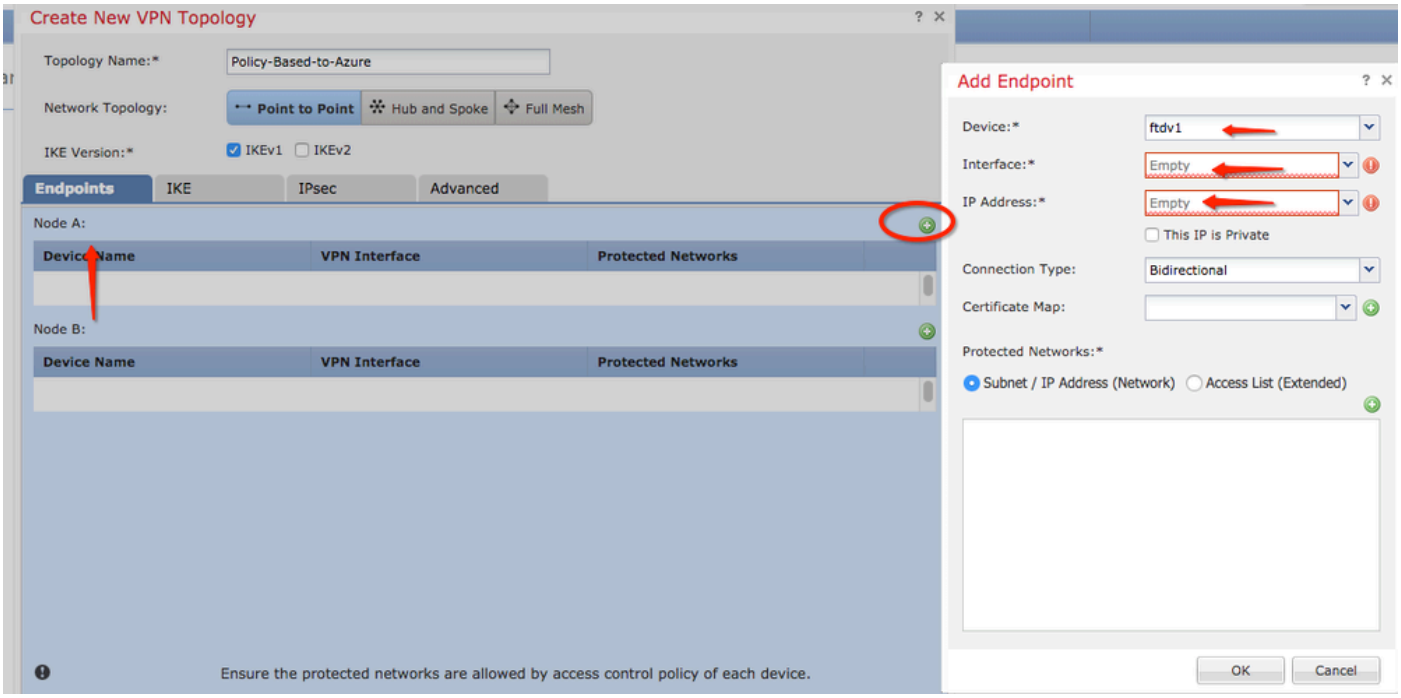
---

8. Dans l'onglet IPSec, configurez la durée de vie et la taille souhaitées.



---

9. Sélectionnez le domaine de cryptage/les sélecteurs de trafic/les réseaux protégés. Accédez à l'onglet Endpoints. Sur le noeud A, cliquez sur**green + button**pour en ajouter un nouveau. Dans cet exemple, le noeud A est utilisé comme sous-réseaux locaux vers le FTD.



---

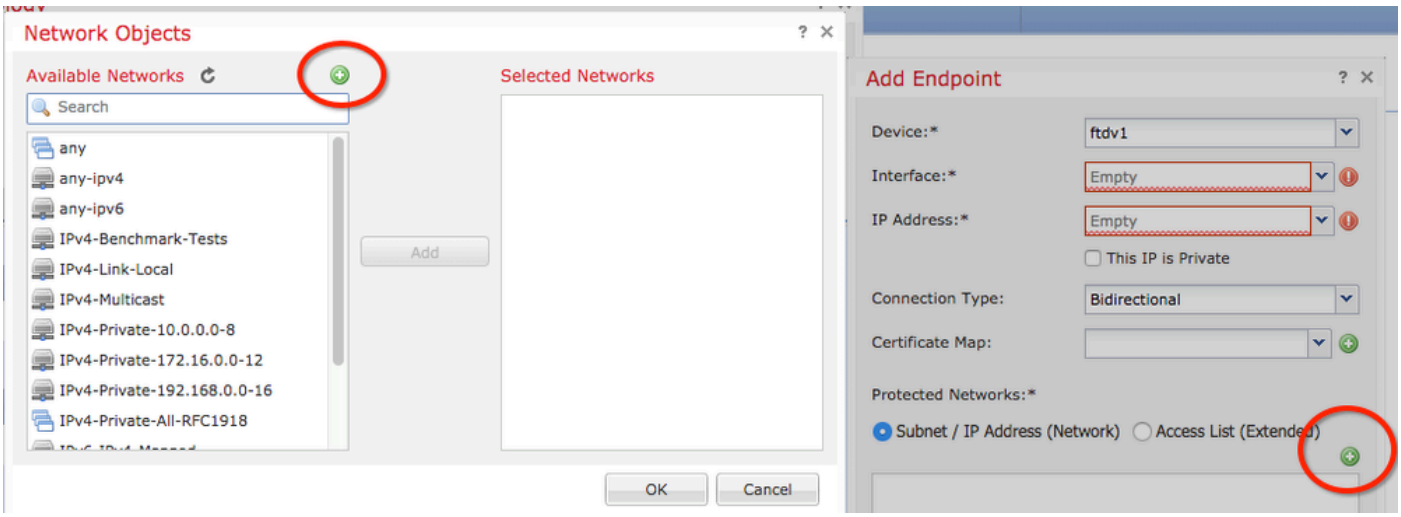
10. Dans la fenêtre Add Endpoint, spécifiez le FTD à utiliser dans la liste déroulante Device avec son interface physique et son adresse IP à utiliser.

---

11. Pour spécifier le sélecteur de trafic local, accédez à l'option Protected Networks, puis cliquez sur le bouton + vert pour créer un nouvel objet.

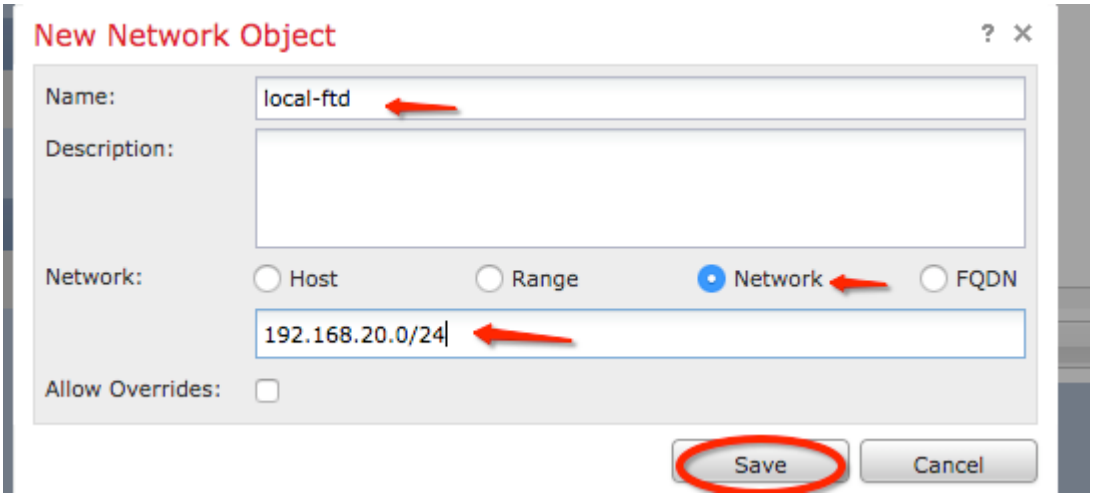
---

12. Dans la fenêtre Objets réseau, cliquez sur le bouton + vert en regard du texte Réseaux disponibles pour créer un nouvel objet sélecteur de trafic local.



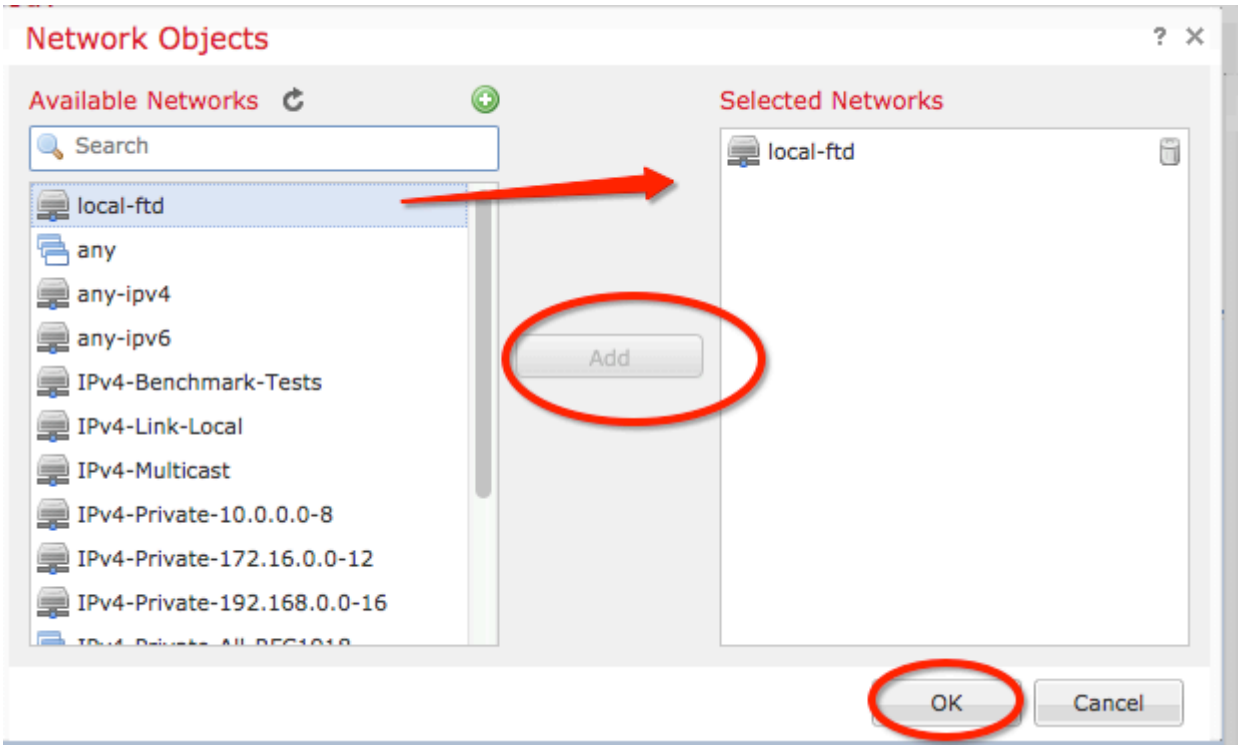
---

13. Dans la fenêtre Nouvel objet réseau, indiquez le nom de l'objet et choisissez-le en conséquence ; hôte/réseau/plage/nom de domaine complet. Cliquez ensuite sur Enregistrer.



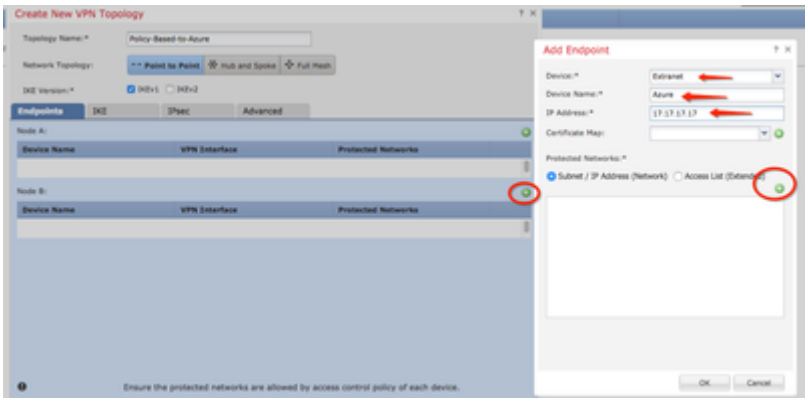
---

14. Ajoutez l'objet à la section Réseaux sélectionnés de la fenêtre Objets réseau et cliquez sur OK. Cliquez sur OK dans la fenêtre Ajouter un point de terminaison.



---

15. Définissez le noeud B qui, dans cet exemple, est le point de terminaison Azure. Dans la fenêtre Create New VPN Topology, accédez à la section Node B et cliquez sur le bouton vert + pour ajouter le sélecteur de trafic du point d'extrémité distant. Spécifiez 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.

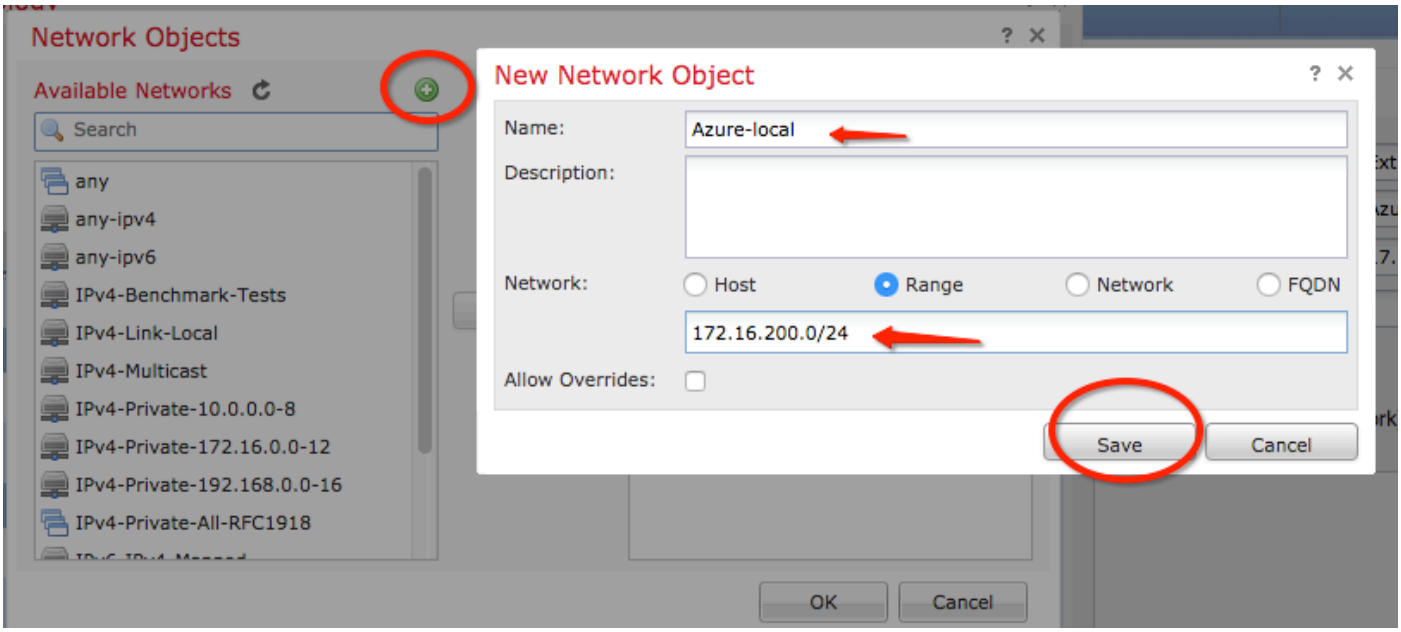


---

16. Créez l'objet de sélecteur de trafic distant. Accédez à la section Réseaux protégés et cliquez sur le bouton + vert pour ajouter un nouvel objet.

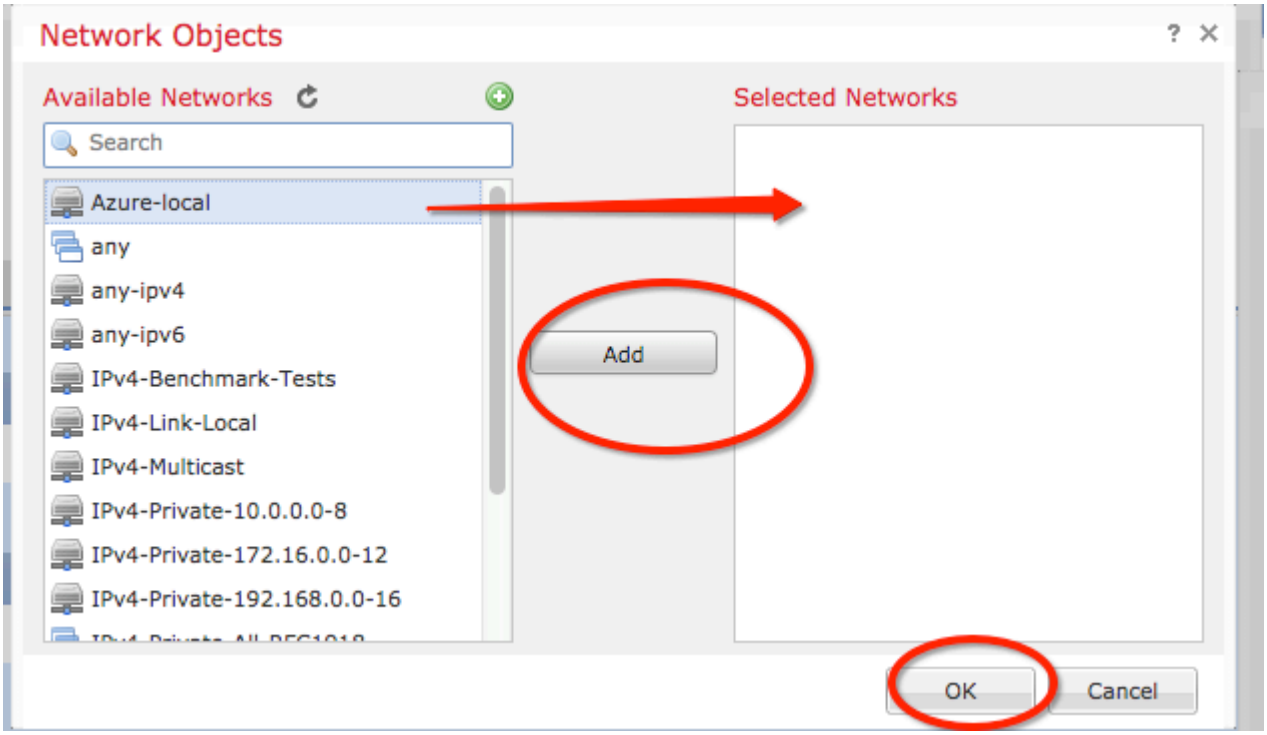
---

17. Dans la fenêtre Objets réseau, cliquez sur le bouton + vert en regard du texte Réseaux disponibles pour créer un nouvel objet. Dans la fenêtre Nouvel objet réseau, spécifiez le nom de l'objet et choisissez en conséquence ; host/range/network/FQDN et cliquez sur Enregistrer.



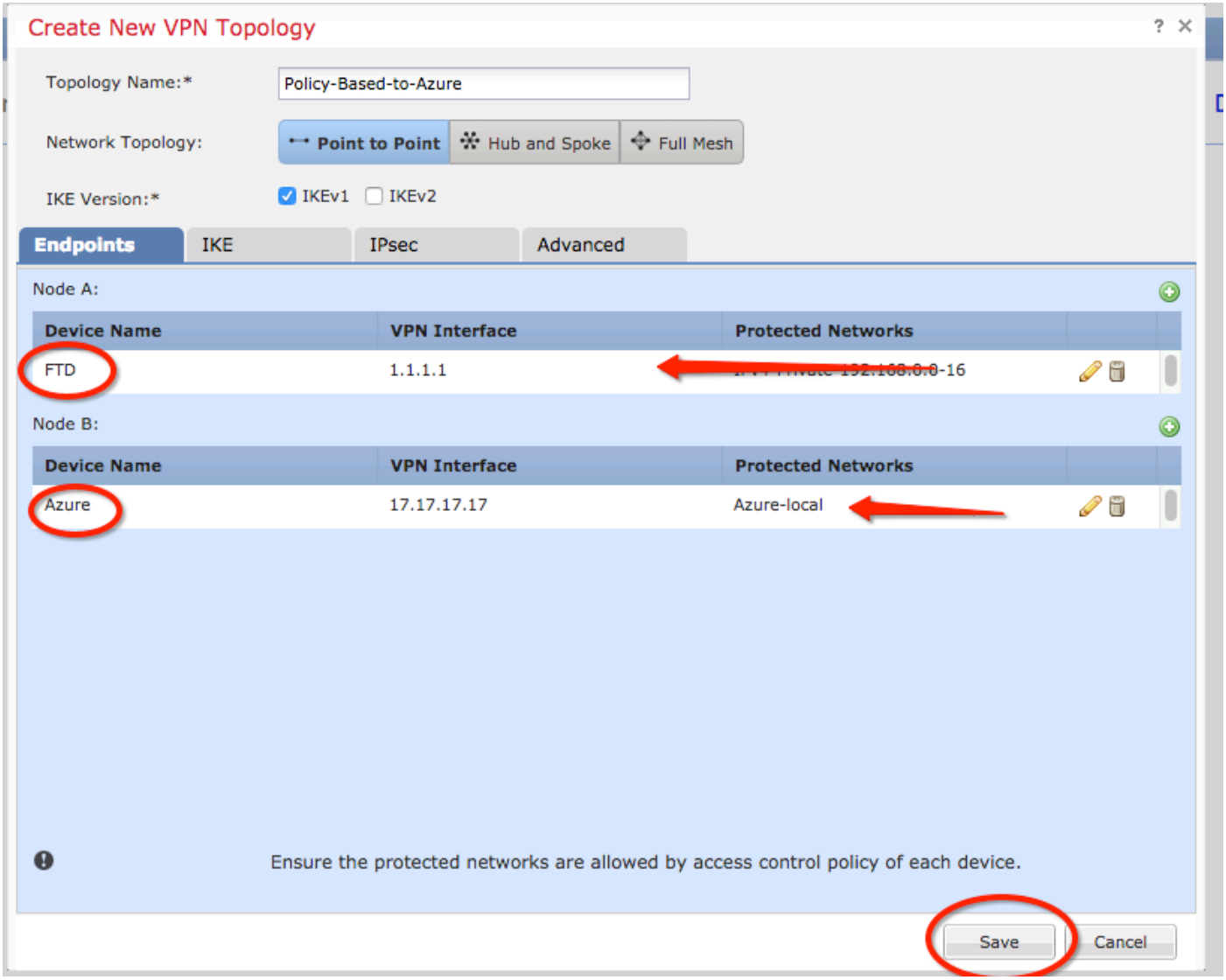
---

18. Dans la fenêtre Objets réseau, ajoutez votre nouvel objet distant à la section Réseaux sélectionnés et cliquez sur OK. Cliquez sur OK dans la fenêtre Ajouter un point de terminaison.



---

19. Dans la fenêtre Create New VPN Topology, vous pouvez voir maintenant les deux noeuds avec leurs sélecteurs de trafic/réseaux protégés corrects. Cliquez sur Save.



---

20. Dans le tableau de bord FMC, cliquez sur Déployer dans le volet supérieur droit, choisissez le périphérique FTD, puis cliquez sur Déployer.

---

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, utilisez 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.

Connect a VPN Gateway to Multiple On-premises Policy-based VPN Devices from Microsoft décrit la configuration de UsePolicyBasedTrafficSelectors en conjonction avec le mode VPN Azure basé sur les routes. Sans l'achèvement 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.

Référence CLI Book 3 : Guide de configuration de l'interface de ligne de commande VPN de la gamme Cisco ASA, 9.8 pour ASA IKEv2 complet avec informations de configuration de crypto-carte.

---

1. Activez IKEv2 sur l'interface externe :

```
<#root>

Cisco-ASA(config)#

crypto ikev2 enable outside
```

---

2. Ajoutez une stratégie IKEv2 Phase 1.

Remarque : Microsoft a publié des informations qui entrent en conflit avec les attributs de chiffrement, d'intégrité et de durée de vie IKEv2 Phase 1 utilisés par Azure. Les attributs répertoriés proviennent des périphériques VPN et des paramètres IPsec/IKE pour les connexions de passerelle VPN site à site. Les informations d'attribut IKEv2 de Microsoft qui entrent en conflit sont un exemple de configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

```
<#root>

Cisco-ASA(config)#

crypto ikev2 policy 1


Cisco-ASA(config-ikev2-policy)#

encryption aes-256

Cisco-ASA(config-ikev2-policy)#

integrity sha256
```

```
Cisco-ASA(config-ikev2-policy)#

group 14

Cisco-ASA(config-ikev2-policy)#

lifetime seconds 28800
```

---

3. Créez un groupe de tunnels sous les attributs IPsec et configurez l’adresse IP de l’homologue et la clé pré-partagée de tunnel local et distant IKEv2 :

<#root>

```
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
```

---

4. Créez une liste d’accès qui définit 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.

<#root>

```
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
```

---

5. Ajoutez 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 entrent en conflit avec les attributs de cryptage et d'intégrité IPSec de phase 2 utilisés par Azure. Les attributs répertoriés sont issus des offres IKE Quick Mode Security Association (IKE Quick Mode SA) VPN basées sur la route. Les informations d'attribut IPSec de la phase 2 de Microsoft qui entrent en conflit sont Exemple de configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
Cisco-ASA(config)#

crypto ipsec ikev2 ipsec-proposal SET1


Cisco-ASA(config-ipsec-proposal)#

protocol esp encryption aes-256


Cisco-ASA(config-ipsec-proposal)#

protocol esp integrity sha-256
```

---

6. Configurez une carte de chiffrement et appliquez-la à l'interface externe, qui contient les composants suivants :

· 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 pour protéger les données (les deux côtés doivent être compatibles PFS avant que la phase 2 n'apparaisse).

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 issus des offres IKE Quick Mode Security Association (IKE Quick Mode SA) VPN basées sur la route.

Les informations d'attribut IPSec de la phase 2 de Microsoft qui entrent en conflit sont Exemple de configuration : Périphérique Cisco ASA (IKEv2/sans BGP). Pour plus d'informations, contactez le support technique Microsoft Azure.

<#root>

```
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
```

---

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

```
<#root>
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
```



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.

```
<#root>
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
```

Vérifier

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 (SA) de phase 1 a été créée :

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 association de sécurité enfant valide conçue pour le trafic chiffré à transmettre.

<#root>

```
    Cisco-ASA#

 show crypto ikev2 sa


IKEv2 SAs:

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

Tunnel-id Local                                                 Remote
  3208253 192.168.1.2/500                                       192.168.2.2/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, 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
```

Dans cet exemple, la SA IKEv1 est construite avec ASA comme initiateur pour homologue IP 192.168.2.2 avec une durée de vie restante de 86388 secondes :

<#root>

```
    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 est créée avec show crypto ipsec sa peer [peer-ip] :

<#root>

```
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-sha256-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-sha256-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 IPSec SA sans erreur. Une association de sécurité entrante avec SPI 0x9B60EDC5 et une association de sécurité sortante avec SPI 0x8E7A2E12 sont installées comme prévu.

Vous pouvez également vérifier que les données passent sur le tunnel en vérifiant les entrées vpn-sessiondb l2l :

<#root>

```
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)SHA256 IPsec: (1)SHA256
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

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]

<#root>

```
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, continuez à en vérifier la raison.

---

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

---

Reportez-vous aux directives d'utilisation complètes de Packet Tracer Troubleshooting Access Problems Using Packet-Tracer

<#root>

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=0x7f6c192502900, 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
```

La NAT exempte le trafic (aucune traduction n'entre en vigueur). Vérifiez qu'aucune traduction NAT n'a lieu sur le trafic VPN. Vérifiez également que l'interface de sortie est correcte, qu'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'il n'y a aucune suppression de liste d'accès vue. Si la phase VPN affiche ENCRYPT: ALLOW, le tunnel est déjà construit et vous pouvez voir IPSec SA installé avec des encaps.

2.1. Si ENCRYPT : ALLOW apparaît dans le traceur de paquets.

- Vérifiez que la SA IPsec est installée et chiffre le trafic à l'aide de la commande show crypto ipsec sa.
- Vous pouvez effectuer une capture sur l'interface externe pour vérifier que les paquets chiffrés sont envoyés à partir d'ASA et que les réponses chiffrées sont reçues d'Azure.

2.2. Si ENCRYPT:DROP est vu dans packet-tracer.

- Le tunnel VPN n'est pas encore établi, mais il est en négociation. Il s'agit d'une condition

attendue lors de la première activation du tunnel. Exécutez les débogages pour afficher le processus de négociation de tunnel et identifier où et si une défaillance se produit.

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

<#root>

```
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.
```

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

Référez-vous à la procédure de débogage complète ikev1 et à l'analyse : Dépannage des débogages ASA IPsec et IKE (mode principal IKEv1) TechNote.

<#root>

```
Cisco-ASA#
```

debug crypto ikev1 127

```
Cisco-ASA#
```

debug crypto ipsec 127

IKEv2

Reportez-vous à la procédure de débogage complète ikev2 et à l'analyse : Use ASA IKEv2 Debugs for Site-to-Site VPN with PSKs

<#root>

```
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.