Op beleid gebaseerde en routegebaseerde VPN configureren van ASA en FTD naar Microsoft Azure

Inhoud

Inleiding

In dit document worden de concepten en de configuratie beschreven voor een VPN tussen Cisco ASA en Cisco Secure Firewall en Microsoft Azure Cloud Services.

Concepten

VPN-encryptiedomein

Het IP-adressenbereik van IPSec maakt het mogelijk om deel te nemen aan de VPN-tunnel.Het coderingsdomein wordt gedefinieerd met het gebruik van een lokale verkeersselector en een externe verkeersselector om te specificeren welke lokale en externe subnetbereiken door IPSec worden opgenomen en versleuteld. Er zijn twee methoden om de VPN-coderingsdomeinen te definiëren: op route gebaseerde of beleidsgebaseerde verkeerskiezen.

Routegebaseerd:
Het coderingsdomein is ingesteld om verkeer toe te staan dat de IPSec-tunnel binnenkomt. Lokale en externe IPsec-verkeersselectors worden op 0.0.0.0 ingesteld. Dit betekent dat elk verkeer dat in de IPSec-tunnel wordt gerouteerd, wordt versleuteld ongeacht het bron-/doelsubnetbestand.

Cisco adaptieve security applicatie (ASA) ondersteunt route-gebaseerde VPN met het gebruik van Virtual Tunnel Interfaces (VTI's) in versies 9.8 en hoger.

Cisco Secure Firewall of Firepower Threat Defence (FTD), beheerd door FMC (Firepower Management Center) ondersteunt routegebaseerde VPN's met het gebruik van VTI's in versies 6.7 en hoger.

Op beleid gebaseerd:

Het coderingsdomein is ingesteld om alleen specifieke IP-bereiken voor zowel bron als bestemming te versleutelen. Op beleid gebaseerde lokale verkeersselecteurs en externe verkeersselecteurs bepalen welk verkeer via IPSec moet worden versleuteld.

ASA ondersteunt op beleid gebaseerde VPN met cryptokaarten in versie 8.2 en hoger.

Microsoft Azure ondersteunt routegebaseerde, beleidsgebaseerde of routegebaseerde selectoren met gesimuleerde beleidsgebaseerde traffic selectors. Azure beperkt momenteel welke versie van Internet Key Exchange (IKE) u kunt configureren op basis van de geselecteerde VPN-methode. Routegebaseerd vereist IKEv2 en beleidsgebaseerd vereist IKEv1. Dit betekent dat als IKEv2 wordt gebruikt, routegebaseerd in Azure moet worden geselecteerd en ASA een VTI moet gebruiken, maar als de ASA alleen cryptokaarten ondersteunt vanwege codeversie, dan moet Azure worden geconfigureerd voor routegebaseerd met beleidsgebaseerde verkeerskiezers. Dit gebeurt in het Azure-portal via PowerShell-scriptimplementatie om een optie te implementeren die Microsoft UsePolicyBased TrafficSelectors noemt, zoals hier wordt uitgelegd: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps.

Samenvattend vanuit het ASA- en FTD-configuratieperspectief:

- Voor ASA/FTD geconfigureerd met een cryptokaart, moet Azure worden geconfigureerd voor op beleid gebaseerde VPN of route-gebaseerde met UsePolicyBased TrafficSelectors.
- Voor ASA geconfigureerd met een VTI moet Azure worden geconfigureerd voor routegebaseerde VPN.
- Voor FTD is hier meer informatie te vinden over hoe VTI's te configureren; 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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Voor IKEv2 op route gebaseerde VPN die VTI op ASA gebruikt: ASA-code versie 9.8(1) of hoger. (Azure moet worden geconfigureerd voor routegebaseerde VPN.)
- Voor IKEv1 op beleid gebaseerde VPN die de cryptokaart gebruikt op ASA en FTD: ASA-codeversie 8.2 of hoger en FTD 6.2.0 of hoger. (Azure moet worden geconfigureerd voor op beleid gebaseerde VPN.)
- Voor IKEv2 op route gebaseerde VPN die crypto-kaarten gebruikt op ASA met op beleid gebaseerde traffic selectors: ASA-codeversie 8.2 of hoger geconfigureerd met een cryptokaart. (Azure moet worden geconfigureerd voor routegebaseerde VPN met

UsePolicyBased TrafficSelectors.)
- Kennis van het VCC voor FTD-beheer en -configuratie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA
- Microsoft Azure
- Cisco FTD
- Cisco VCC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Voltooi de configuratie stappen. Kies voor de configuratie van IKEv1, IKEv2-route op basis van VTI of IKEv2-route op basis van Use Policy-Based Traffic Selectors (crypto map op ASA).

IKEv1-configuratie op ASA

Voor een site-to-site IKEv1 VPN van ASA naar Azure volgt u de volgende ASA-configuratie. Zorg ervoor dat u een op beleid gebaseerde tunnel in het Azure-portal configureert. Voor ASA worden cryptokaarten gebruikt.

Raadpleeg dit Cisco-document voor volledige IKEv1 op ASA-configuratieinformatie.

Stap 1. Schakel IKEv1 in op de buiteninterface.

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

Stap 2. Maak een IKEv1-beleid dat de algoritmen/methoden definieert die moeten worden gebruikt voor de hash, authenticatie, Diffie-Hellman groep, levensduur en encryptie.

> **Opmerking:** De vermelde fase 1 IKEv1-kenmerken worden vanuit dit openbaar beschikbare Microsoft-document het best geleverd. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 3. Maak een tunnelgroep onder de IPsec-kenmerken en configureer het peer IP-adres en de

vooraf gedeelde sleutel.

```
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
```

Stap 4. Maak een toegangslijst waarin het te versleutelen en te tunnelen verkeer wordt gedefinieerd. In dit voorbeeld is het verkeer van belang het verkeer van de tunnel die afkomstig is van het 10.2.2.0-subnet naar 10.1.1.0. Het kan meerdere ingangen bevatten als er meerdere subnetten betrokken zijn tussen de sites.

In versies 8.4 en hoger kunnen objecten of groepen objecten worden gemaakt die dienen als containers voor de netwerken, subnetten, IP-adressen van de host of meerdere objecten. Maak twee objecten met de lokale en externe subnetten en gebruik deze voor zowel de crypto Access Control List (ACL) als de Network Address Translation (NAT)-verklaringen.

```
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
```

Stap 5. Configureer de transformatieset (TS), waarbij het trefwoord moet worden gebruikt**IKEv1**. Een identieke TS moet ook op het verre eind worden tot stand gebracht.

> **Opmerking:** De vermelde fase 2 IKEv1-kenmerken worden vanuit dit openbaar beschikbare Microsoft-document het best geleverd. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

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

Stap 6. Configureer de crypto-kaart en pas deze toe op de buiteninterface die de volgende componenten heeft:
·Het peer IP-adres
·De gedefinieerde toegangslijst die het relevante verkeer bevat
·Het TS
·De configuratie stelt geen Perfect Forward Secrecy (PFS) in, aangezien openbare Azure-documentatie aangeeft dat PFS is uitgeschakeld voor IKEv1 in Azure. Een optionele PFS-instelling, die een nieuw paar Diffie-Hellman-toetsen creëert die worden gebruikt om de gegevens te beschermen (beide kanten moeten PFS-ingeschakeld zijn voordat fase 2 verschijnt), kan worden ingeschakeld via het gebruik van deze configuratie: **crypto map outside_map 20 set pfs** .
· De IPSec-reeks van fase 2 is gebaseerd op openbare Azure-documentatie. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 7. Zorg ervoor dat het VPN-verkeer niet aan een andere NAT-regel wordt onderworpen. Maak een NAT-vrijstellingsregel:

```
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
```

> **Opmerking**: wanneer meerdere subnetten worden gebruikt, moet u objectgroepen maken met alle bron- en doelsubnetten en deze gebruiken in de NAT-regel.

```
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 routegebaseerd met VTI op ASA Code 9.8 (1) of hoger

Voor een site-to-site IKEv2 Route gebaseerde VPN op ASA-code, volg deze configuratie. Zorg ervoor dat Azure is geconfigureerd voor routegebaseerde VPN en configureer geen UsePolicyBased TrafficSelectors in het Azure-portal. Een VTI wordt geconfigureerd op de ASA.

Raadpleeg dit Cisco-document voor volledige ASA VTI-configuratieinformatie.

Stap 1. Schakel IKEv2 in op de buiteninterface:

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

Stap 2. Voeg een IKEv2 fase 1 beleid toe.

> **Opmerking**: Microsoft heeft informatie gepubliceerd die strijdig is met de specifieke IKEv2 fase 1-codering, integriteit en levensechte eigenschappen die door Azure worden gebruikt. De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbaar beschikbare Microsoft document. De informatie die IKEv2 attributen van Microsoft strijdig maakt is hier zichtbaar. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 3. Voeg een IKEv2 fase 2 IPsec voorstel toe. Specificeer de beveiligingsparameters in de crypto IPsec **ikev2 ipsec-proposal** configuratiemodus:

protocol esp encryptie {des | 3 dec. | AES | AES-192 | AES-256 | AES-gcm | AES-GCM-192 | AES-GCM-256 | AES-gmac | AES-gmac-192 | AES-gmac-256 | van nul
protocol ESP integriteit {md5 | sha-1 | SHA-256 | SHA-384 | SHA-512 | van nul

> **Opmerking:** Microsoft heeft informatie gepubliceerd die strijdig is met de specifieke fase 2 IPSec-encryptie en integriteitskenmerken die door Azure worden gebruikt. De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbaar beschikbare Microsoft document. De informatie die fase 2 IPSec attributen van Microsoft in strijd is is hier zichtbaar. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 4. Voeg een IPSec-profiel toe dat het volgende specificeert:

- Het eerder geconfigureerde ikev2-fase 2 IPSec-voorstel
- Fase 2 IPSec-levensduur (optioneel) in seconden en/of kilobytes
- De PFS-groep (optioneel)

> **Opmerking:** Microsoft heeft informatie gepubliceerd die strijdig is met de specifieke fase 2 IPSec-levensduur en PFS-kenmerken die door Azure worden gebruikt. De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbaar beschikbare Microsoft document. De informatie die fase 2 IPSec attributen van Microsoft in strijd is is hier zichtbaar. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 5. Maak een tunnelgroep onder de IPsec-kenmerken en configureer het peer IP-adres en de vooraf gedeelde IKEv2 lokale en externe 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)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

Stap 6. Maak een VTI die het volgende specificeert:

- Een nieuw tunnelinterfacenummer: interfacetunnel [number]
- Een nieuwe tunnelinterfacenaam: naam [name]
- Een niet-bestaand IP-adres dat op de tunnelinterface moet bestaan: IP-adres [ip-adres] [masker]
- Tunnelbroninterface waar VPN lokaal wordt afgesloten: Tunnelbroninterface [int-name]
- Het Azure-IP-adres: tunnelbestemming [Azure Public IP]
- IPSec IPv4-modus: tunnelmodus ipsec ipv4
- Het te gebruiken IPSec-profiel voor dit VTI: ipsec-profiel voor tunnelbescherming [profielnaam]

```
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
```

Stap 7. Maak een statische route om verkeer in de tunnel te richten. Voer deze opdracht in om een statische route toe te voegen:
route if_name dest_ip mask gateway_ip [distance]

Het **dest_ip** en **mask** is het IP-adres voor het doelnetwerk in de Azure-cloud, bijvoorbeeld 10.0.0.0/24. De gateway_ip moet elk IP-adres zijn (bestaand of niet-bestaand) op het tunnelinterfacesubnet, zoals 169.254.0.2. Het doel van deze gateway_ip is om verkeer naar de tunnelinterface te wijzen, maar de specifieke gateway IP zelf is niet belangrijk.

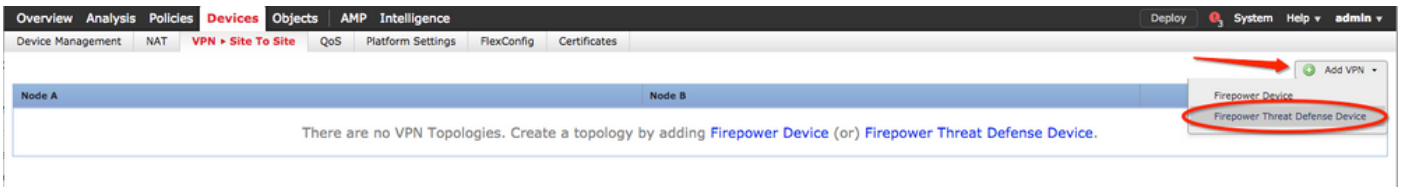
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

IKEv1-configuratie op FTD

Voor een site-to-site IKEv1 VPN van FTD naar Azure moet u het FTD-apparaat eerder bij FMC hebben geregistreerd.

Stap 1. Maak een site-to-site beleid. Naar het **FMC dashboard > Devices > VPN > Site to Site**.

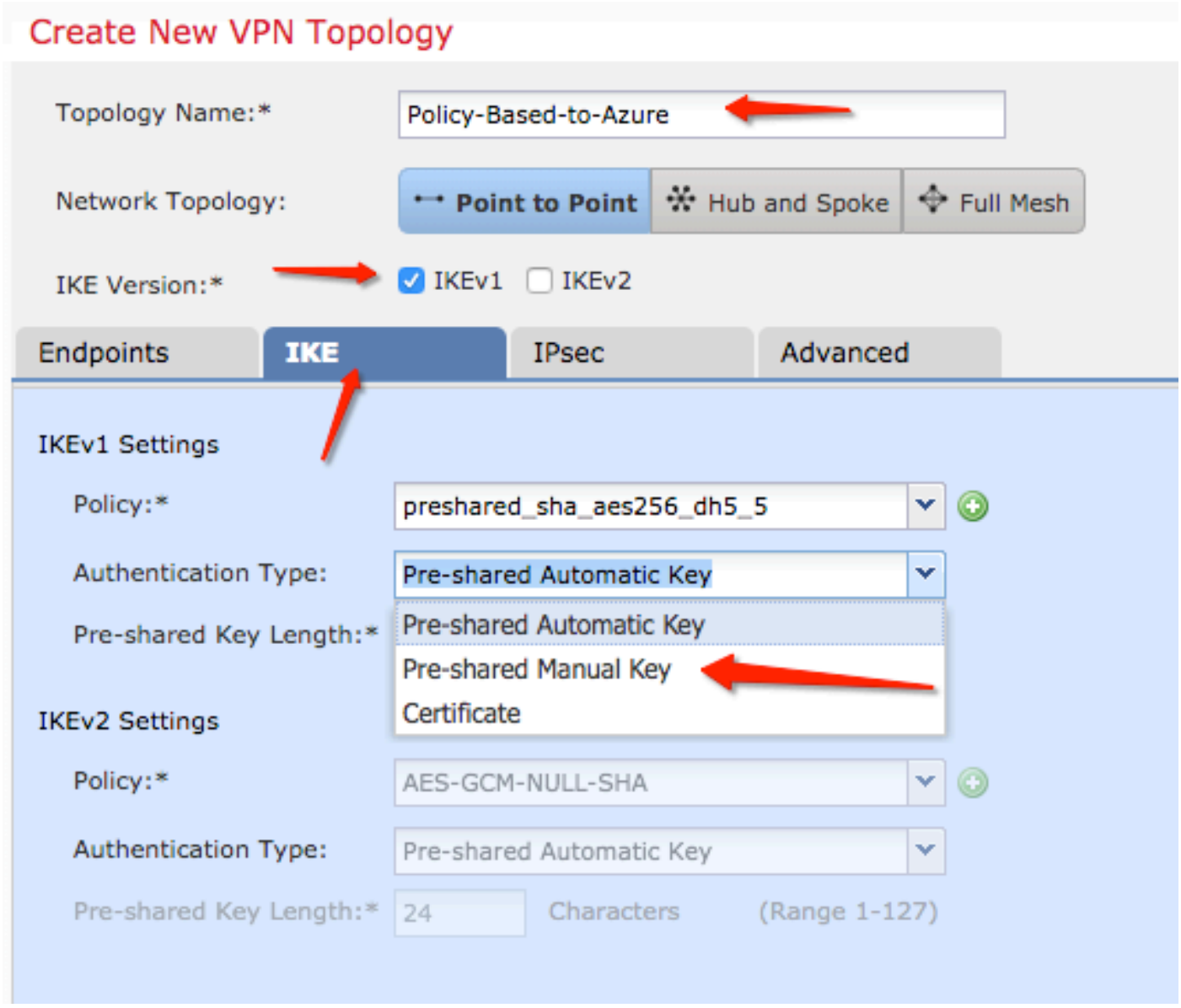
Stap 2. Maak een nieuw beleid. Klik op de **Add VPN** vervolgkeuzemenu en kies **Firepower Threat Defense device** .

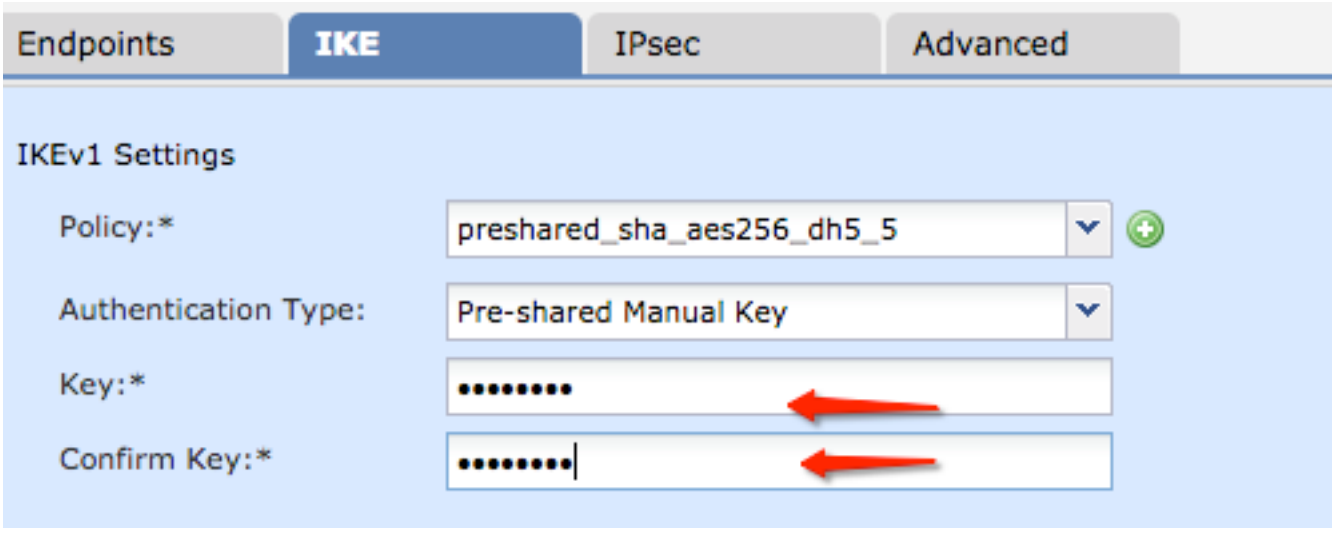


Stap 3. Op de **Create new VPN Topology** venster, geef uw **Topology Name**, controleer **IKEV1** protocol

aangevinkt en klik op de **IKE** tabblad. In dit voorbeeld worden vooraf gedeelde sleutels gebruikt als een verificatiemethode.

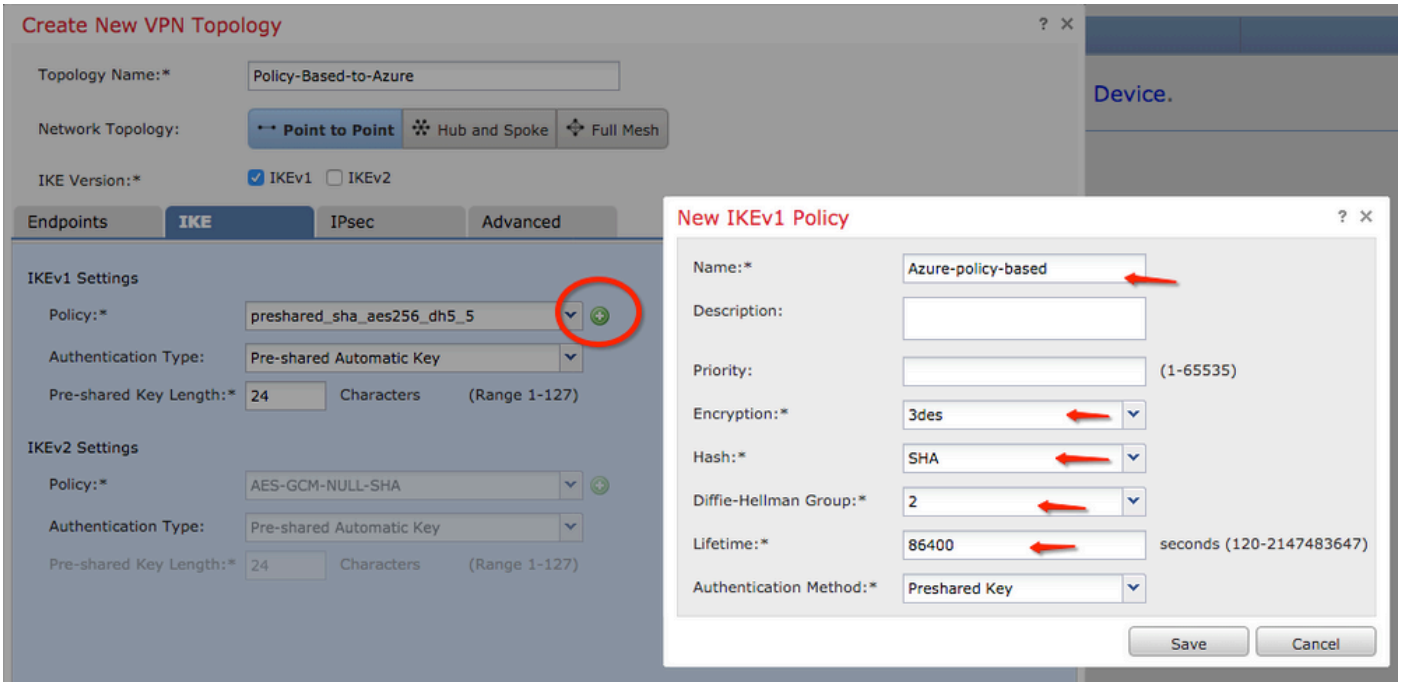
Klik op de **Authentication Type** vervolgkeuzemenu en kies **Pre-shared manual key** . Typ de handmatige vooraf gedeelde toets op de **Key** en**Confirm Key** tekstvelden.



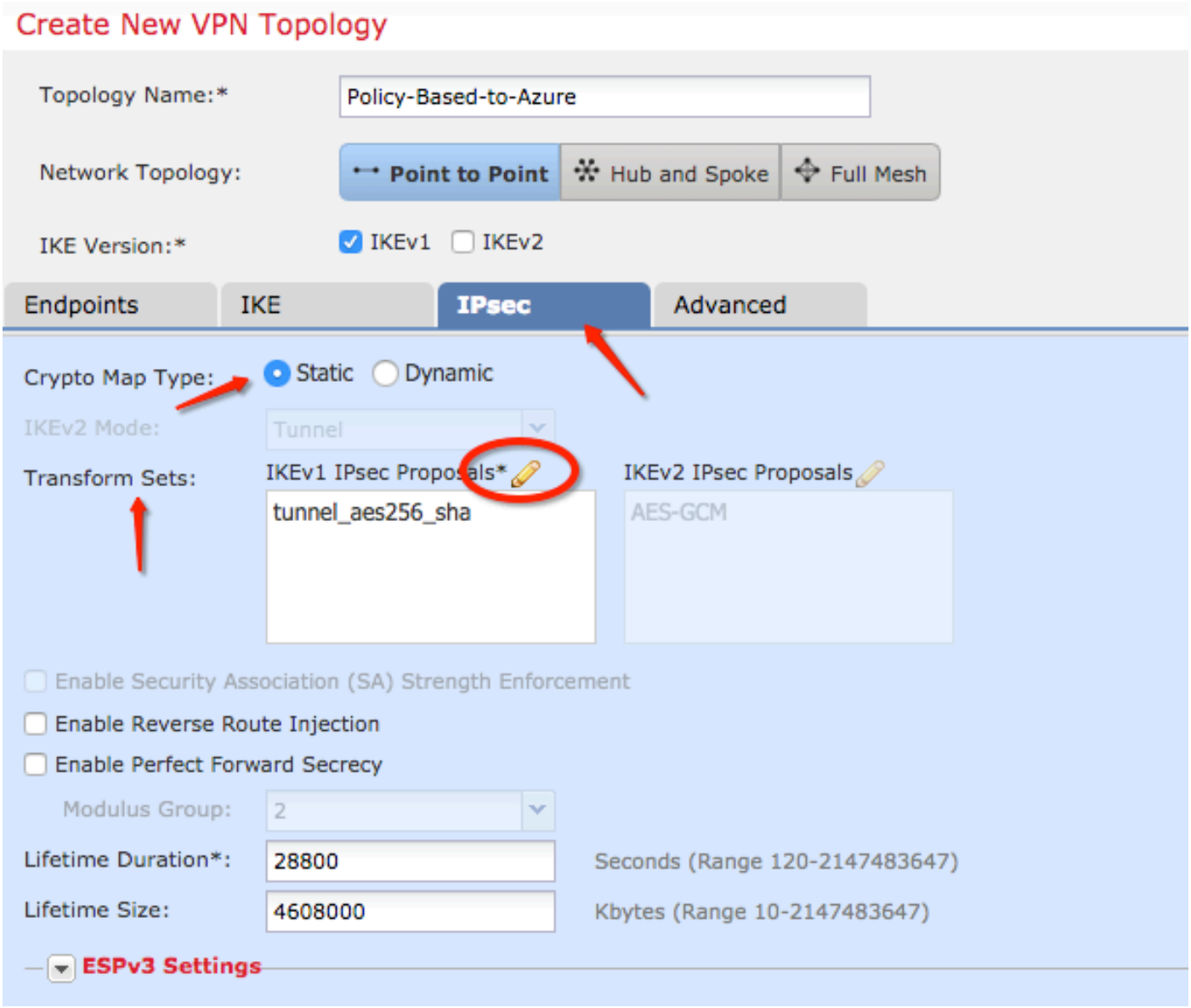


Stap 4. Configureer het ISAKMP-beleid of de parameters van fase 1 met de aanmaak van een

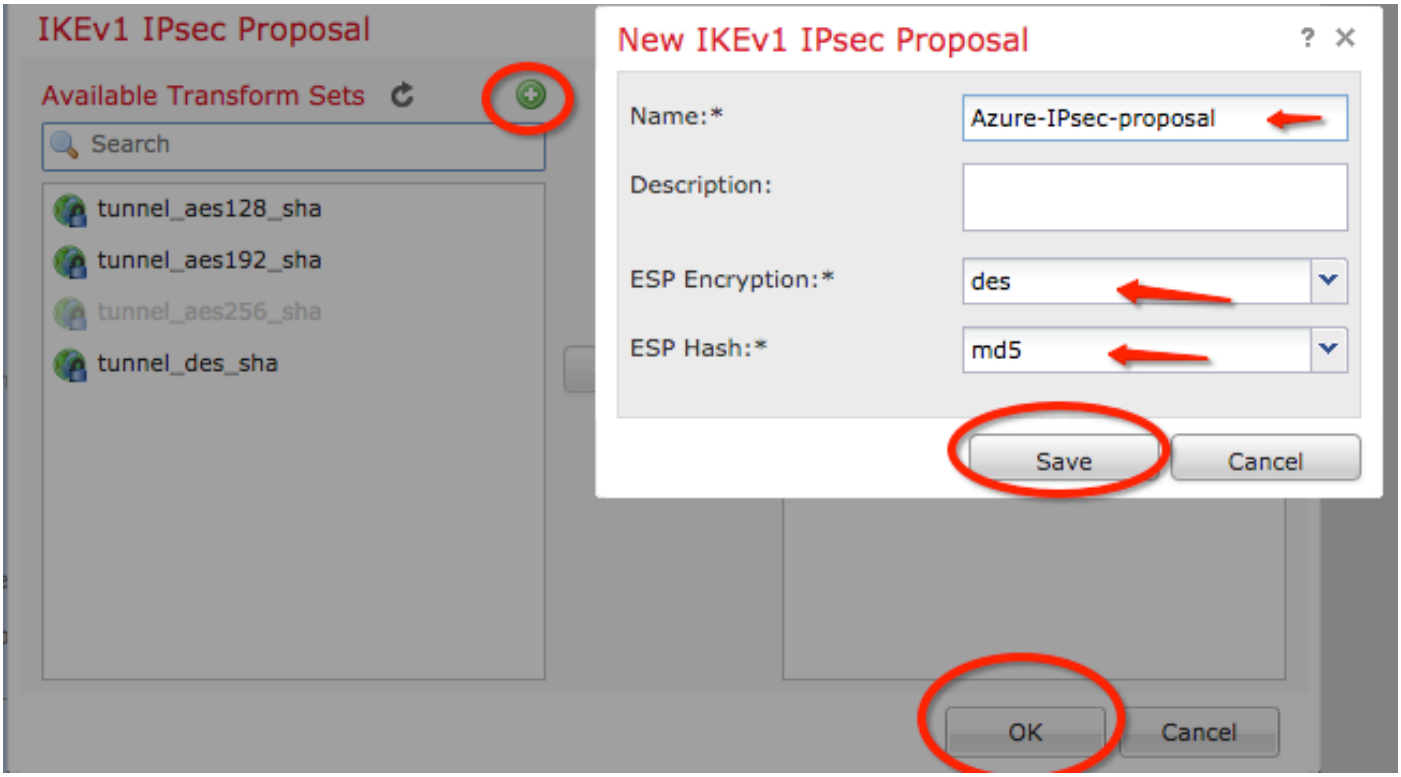
nieuwe. Klik in hetzelfde venster op de **green plus button** om een nieuw ISAKMP-beleid toe te voegen. Specificeer de naam van het beleid en kies de gewenste Encryptie, Hash, Diffie-Hellman groep, Leven en Verificatie methode, en klik **Save** .



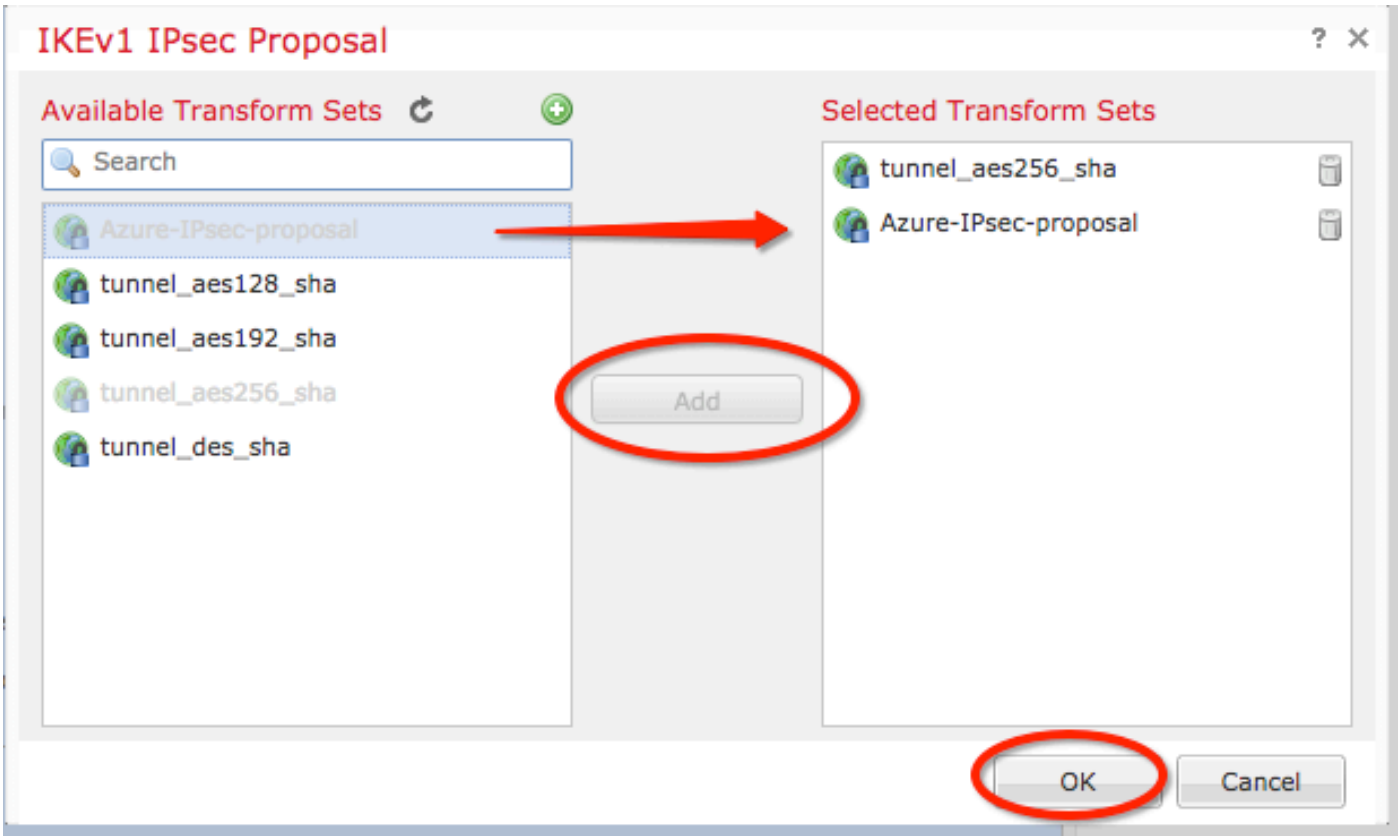
Stap 5. Configureer het IPsec-beleid of de parameters van fase 2. Naar het **IPsec** tabblad kiest u **Static** op het **Crypto Map Type** selectievakje. Klik op de **edit pencil** pictogram vanaf het **IKEV1 IPsec Proposals** op het **Transform Sets** optie.



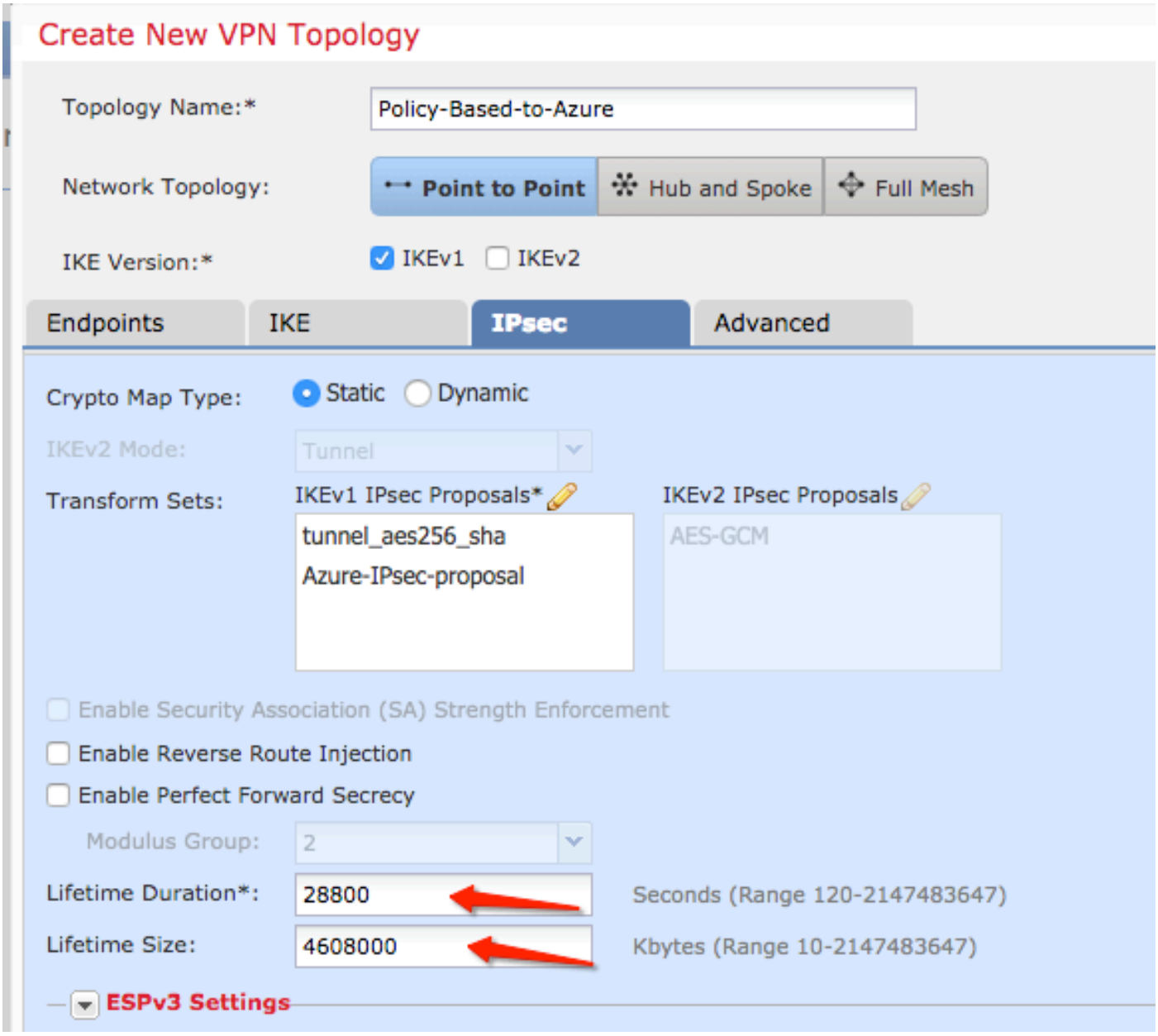
Stap 6. Maak een nieuw IPsec-voorstel. Op de **IKEv1 IPSec Proposal** klikt u op het **green plus button** om er een nieuwe toe te voegen. Specificeer de naam van het beleid en de gewenste parameters voor ESP Encryptie en ESP Hash algoritmen en klik **Save** .



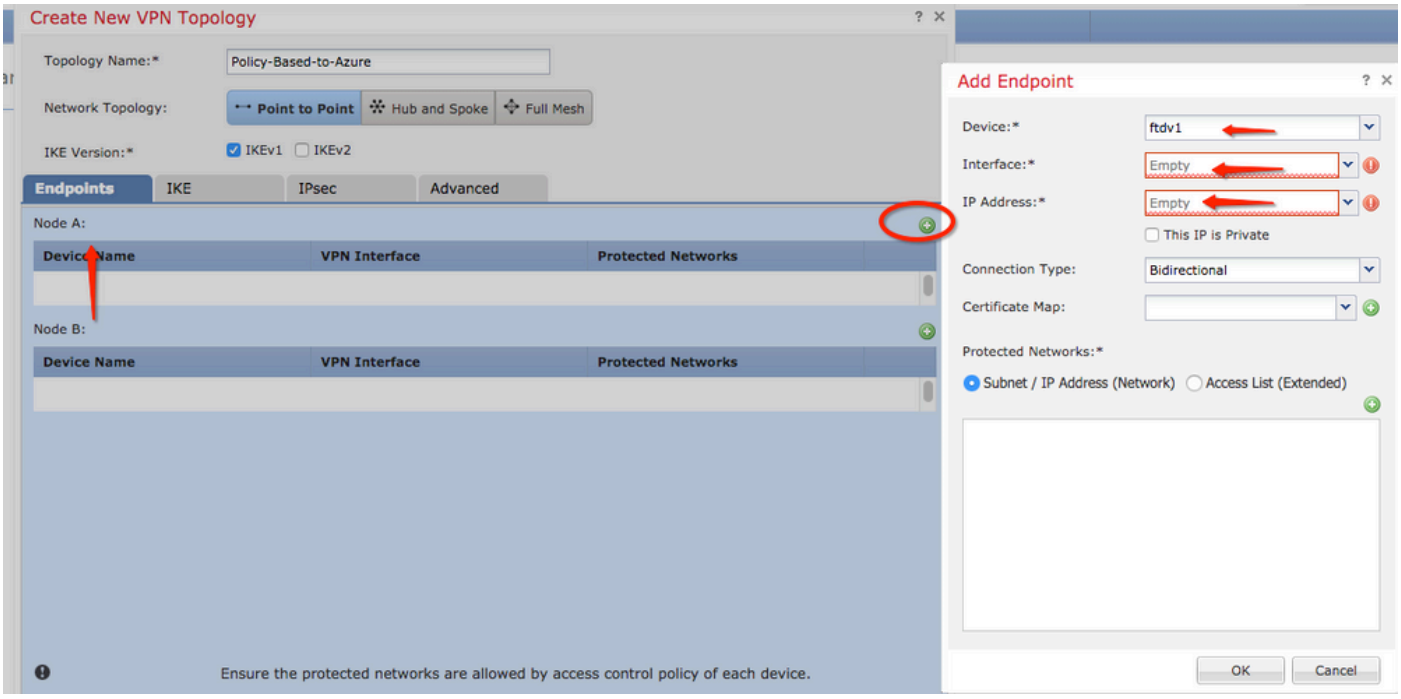
Stap 7. Op de **IKEV1 IPsec Proposal** IPsec-beleid toevoegen aan het **Selected Transform Sets** doorsnede en klik **OK** .



Stap 8. **IPSec** tabblad, de gewenste Levensduur en Grootte instellen.



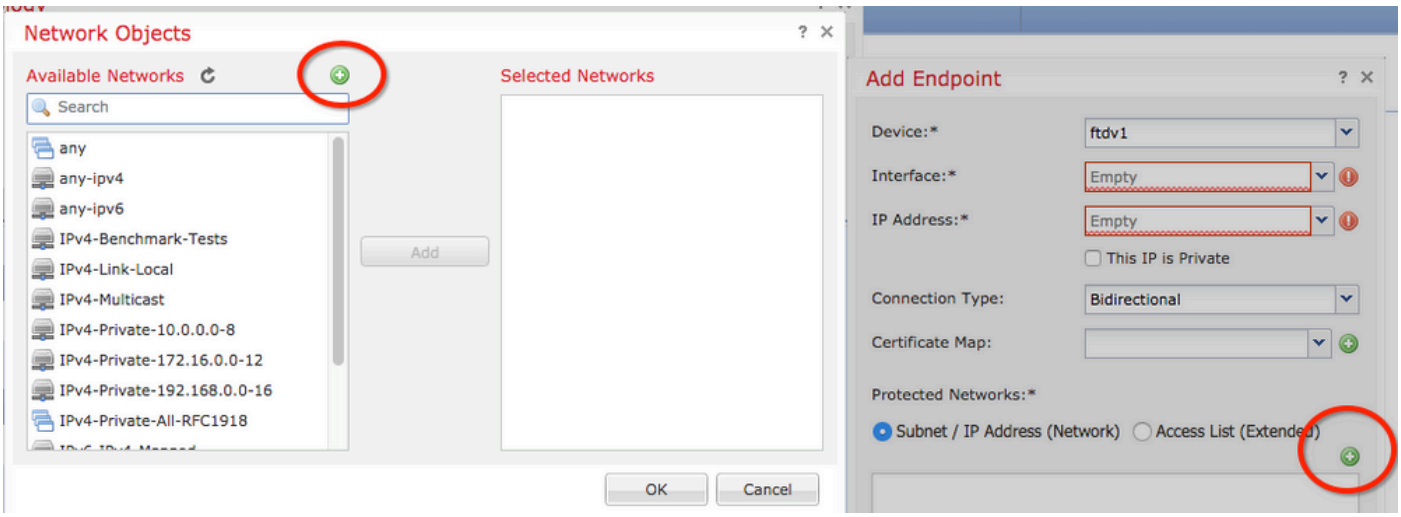
Stap 9. Kies het domein voor versleuteling/de verkeersselectors/beschermde netwerken. Naar het **Endpoints** tabblad. Op de **Node A** Klik in het gedeelte op de **green plus button** om er een nieuwe toe te voegen. In dit voorbeeld wordt knooppunt A gebruikt als lokale subnetten voor het FTD.



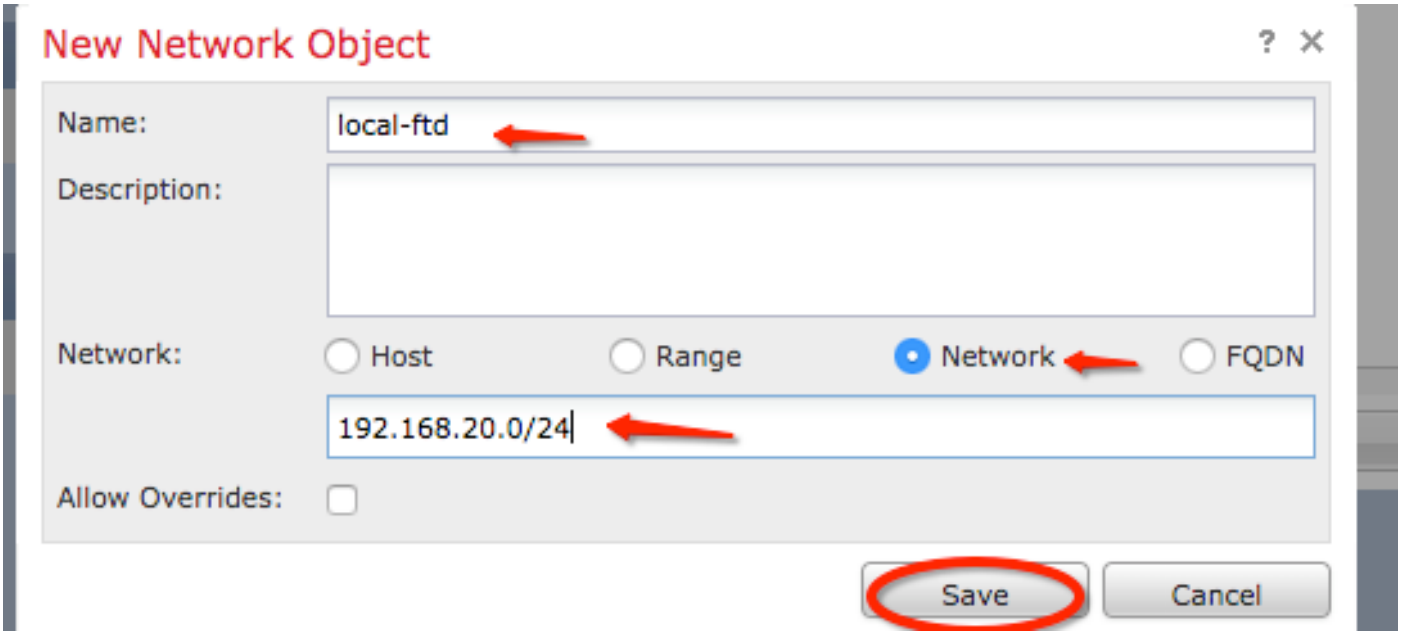
Stap 10. Op de **Add Endpoint** het FTD-venster dat moet worden gebruikt op het **Device** drop-down samen met zijn fysieke interface en IP adres aan gebruik.

Stap 1. Om de lokale verkeerskiezer te specificeren, navigeer naar de **Protected Networks** en klik op de **green plus button** om een nieuw object te maken.

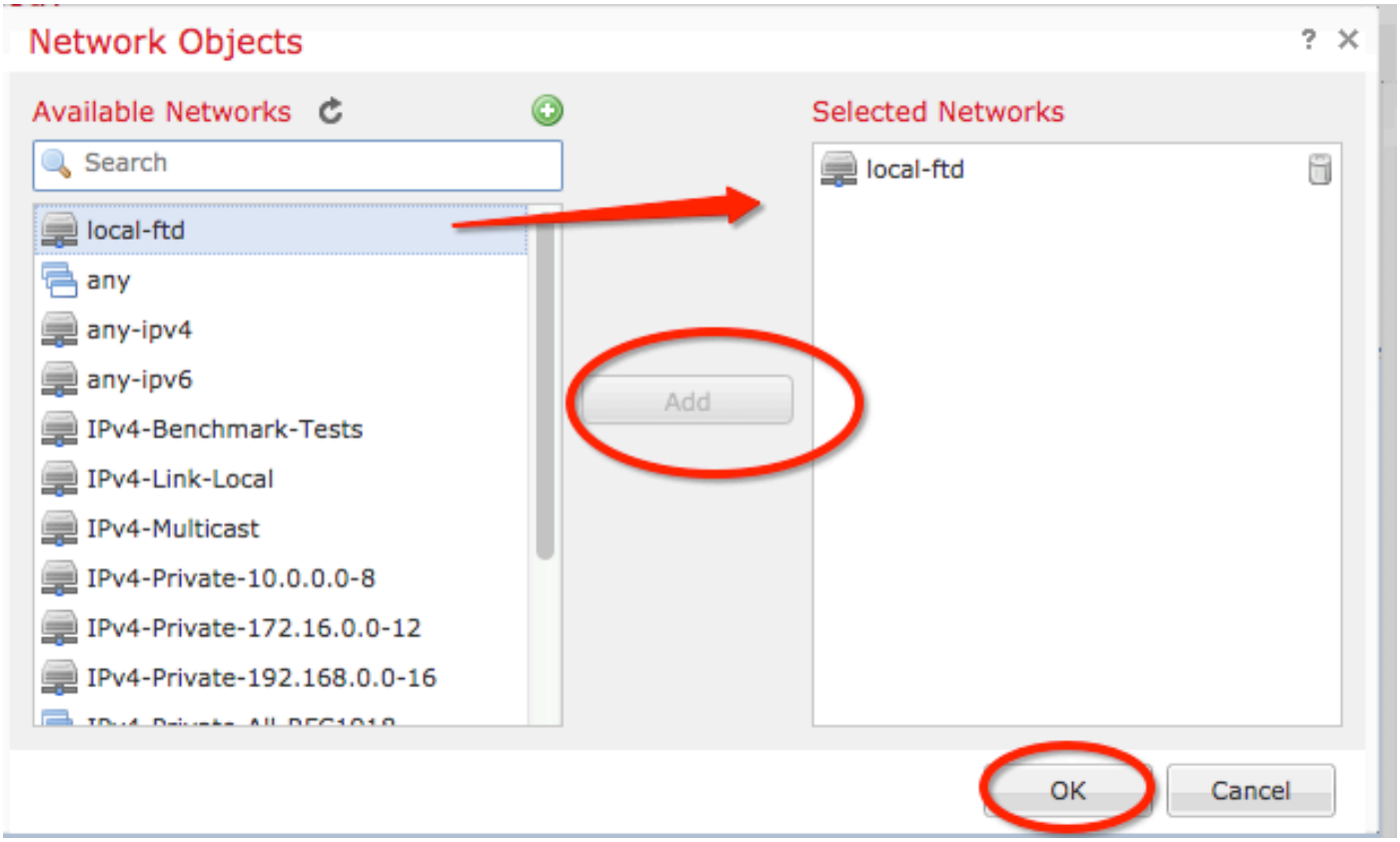
Stap 12. Op de **Network Objects** klik op het **green plus button** naast de **Available Networks** tekst om een nieuw lokaal object voor verkeersselectie te maken.



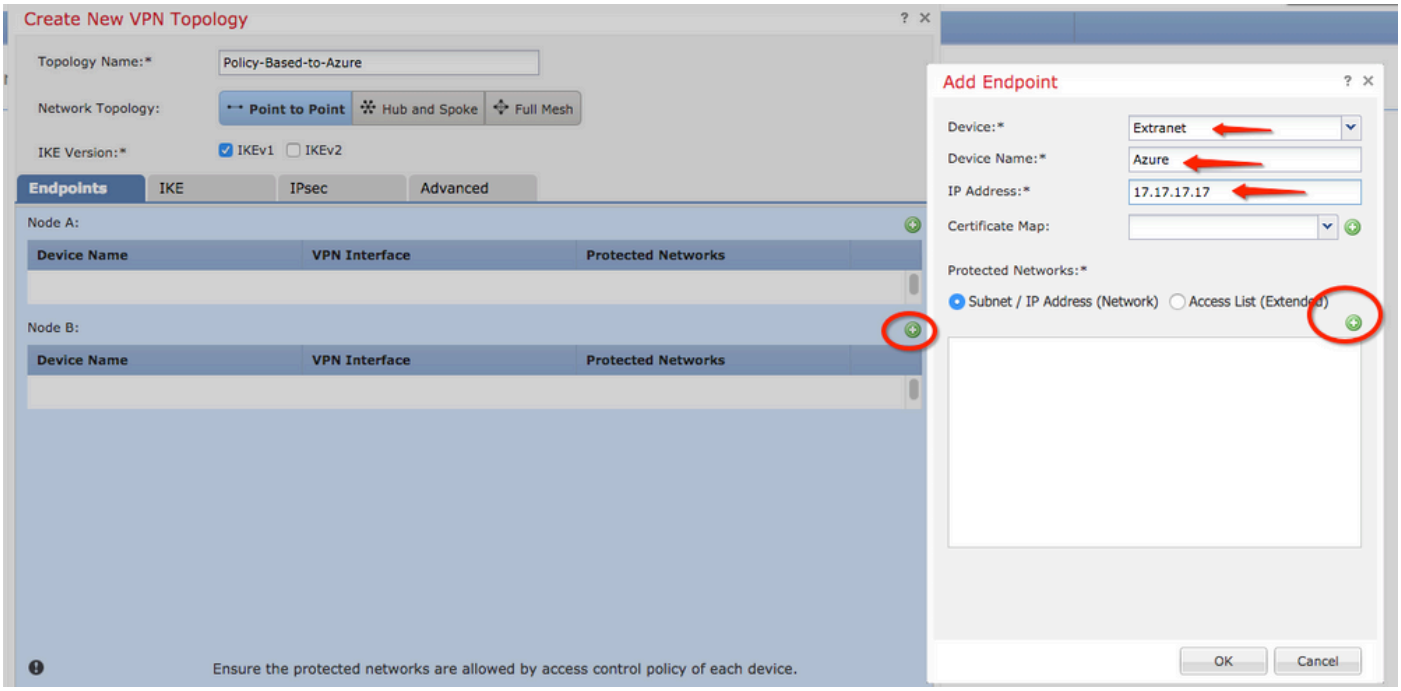
Stap 13. Op de **New Network Object** venster, specificeer de naam van het object en kies dienovereenkomstig host/netwerk/bereik/FQDN. Klik vervolgens op **Save** .



Stap 14. Voeg het object toe aan de **Selected Networks** het gedeelte over het **Network Objects** venster en klik **OK** . Klik **OK** op het **Add Endpoint** venster.

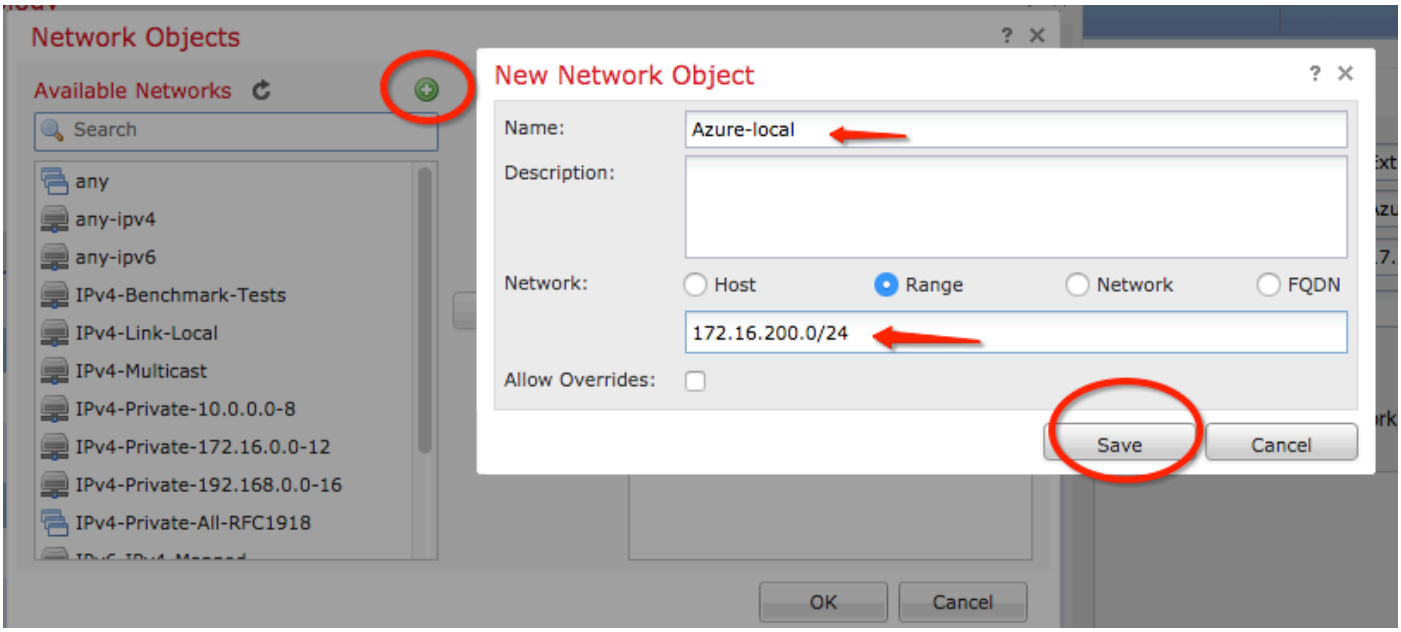


Stap 15. Bepaal het knooppunt B-eindpunt, dat in dit voorbeeld het Azure-eindpunt is. Op de **Create New VPN Topology** venster, navigeer naar het **Node B** sectie en klik op de **green plus button** om de functie voor extern endpointverkeer toe te voegen. Opgeven **Extranet** voor alle VPN-peer-endpoints die niet door hetzelfde VCC als knooppunt A worden beheerd. Typ de naam van het apparaat (alleen lokaal belangrijk) en het IP-adres.

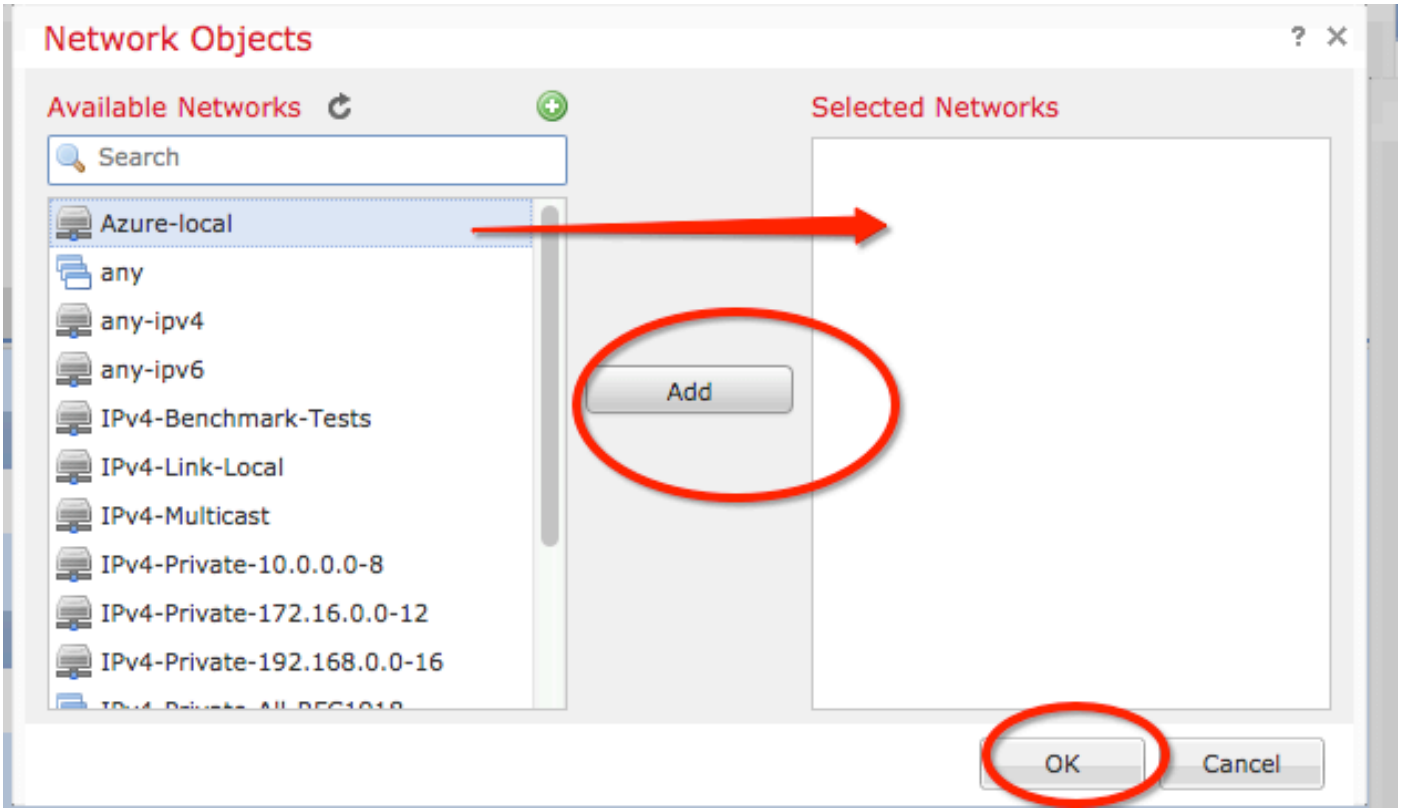


Stap 16. Maak het object van de afstandsbediening. Naar het **Protected Networks** sectie en klik op de **green plus button** om een nieuw object toe te voegen.

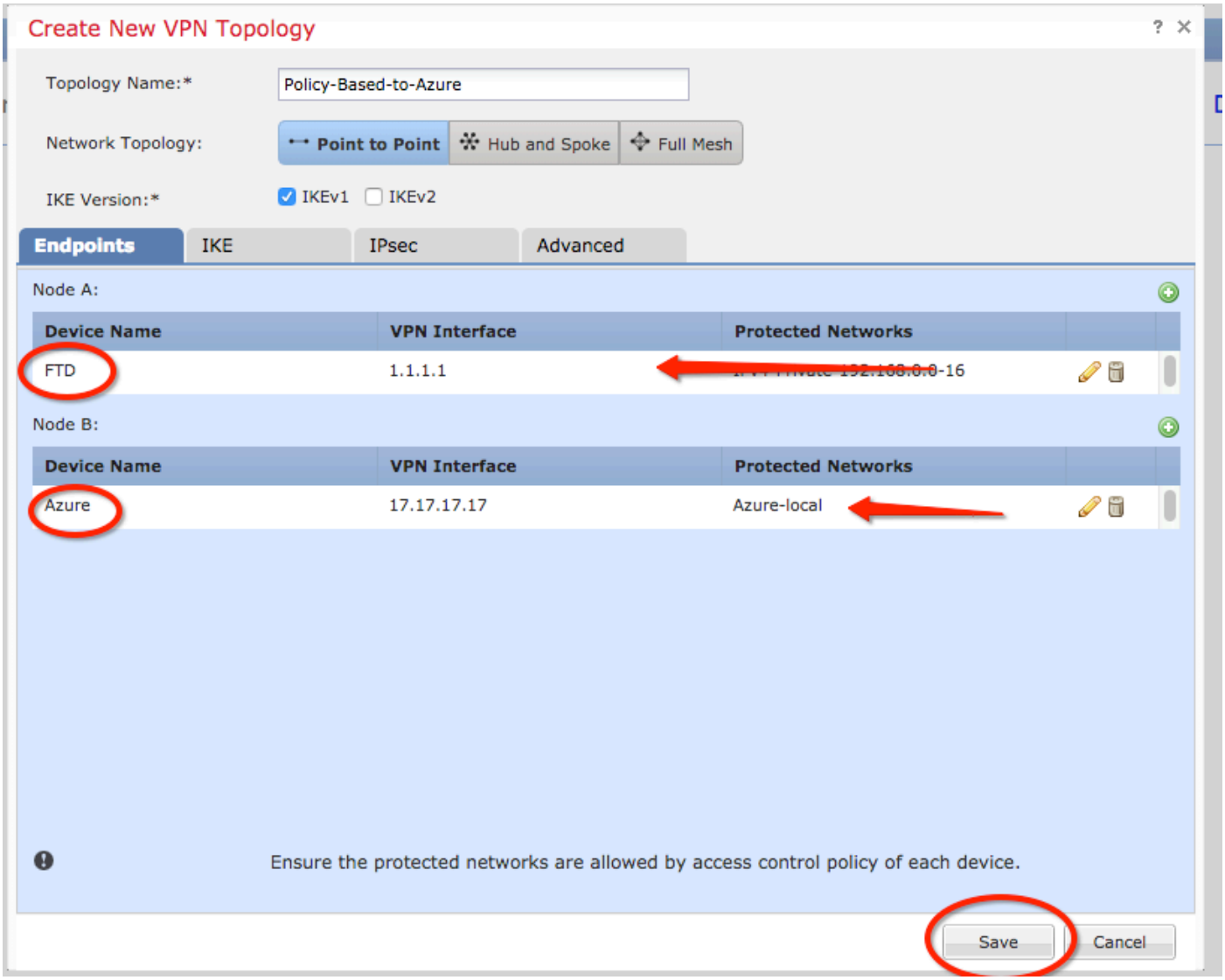
Stap 17. Op de **Network Objects** klik op het **green plus button** naast de **Available Networks** tekst om een nieuw object te maken. Op de **New Network Object** venster, geef de naam van het object op en kies dienovereenkomstig host/bereik/netwerk/FQDN en klik op **Save** .



Stap 18. **Network Objects** venster, uw nieuwe externe object aan het **Selected Networks** doorsnede en klik **OK** . Klik **Ok** op het **Add Endpoint** venster.



Stap 19. Op de **Create New VPN Topology** u kunt nu beide knooppunten zien met hun juiste verkeersselecteurs/beschermde netwerken. Klik **Save** .



Stap 20. Klik op het FMC-dashboard **Deploy** kies in het rechter bovenvenster het FTD-apparaat en klik vervolgens op **Deploy** .

Stap 21. Op de opdrachtregelinterface ziet de VPN-configuratie er hetzelfde uit als die voor ASA-apparaten.

IKEv2-routegebaseerd met op beleid gebaseerde verkeersselectors

Voor een site-to-site IKEv2 VPN op ASA met cryptokaarten, volg deze configuratie. Zorg ervoor dat Azure is geconfigureerd voor routegebaseerde VPN en UsePolicyBased TrafficSelectors moeten worden geconfigureerd in het Azure-portal met behulp van PowerShell.

In dit document van Microsoft wordt de configuratie van UsePolicyBased TrafficSelectors beschreven in combinatie met de routegebaseerde Azure VPN-modus. Zonder afronding van deze stap, ASA met cryptokaarten slaagt er niet in de verbinding tot stand te brengen door een mismatch in de van Azure ontvangen verkeersselectors.

Raadpleeg dit Cisco-document voor volledige ASA IKEv2 met configuratieinformatie over crypto-kaarten.

Stap 1. Schakel IKEv2 in op de buiteninterface:

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

Stap 2. Voeg een IKEv2 fase 1 beleid toe.

> **Opmerking**: Microsoft heeft informatie gepubliceerd die strijdig is met de specifieke IKEv2 fase 1-codering, integriteit en levensechte eigenschappen die door Azure worden gebruikt. De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbaar beschikbare Microsoft document. IKEv2 attributen informatie van Microsoft dat conflicten is hier zichtbaar. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 3. Maak een tunnelgroep onder de IPsec-kenmerken en configureer het peer IP-adres en de vooraf gedeelde IKEv2 lokale en externe 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)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

Stap 4. Maak een toegangslijst waarin het te versleutelen en te tunnelen verkeer wordt gedefinieerd. In dit voorbeeld is het verkeer van belang het verkeer van de tunnel die afkomstig is van het 10.2.2.0-subnet naar 10.1.1.0. Het kan meerdere ingangen bevatten als er meerdere subnetten betrokken zijn tussen de sites.

In versies 8.4 en hoger kunnen objecten of groepen objecten worden gemaakt die dienen als containers voor de netwerken, subnetten, IP-adressen van de host of meerdere objecten. Maak twee objecten met de lokale en externe subnetten en gebruik deze voor zowel de crypto ACL als de NAT-instructies.

```
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
```

Stap 5. Voeg een IKEv2 fase 2 IPsec voorstel toe. Specificeer de beveiligingsparameters in de configuratiemodus crypto IPsec ikev2 ipsec-voorstel:

protocol esp encryptie {des | 3 dec. | AES | AES-192 | AES-256 | AES-gcm | AES-GCM-192 | AES-GCM-256 | AES-gmac | AES-gmac-192 | AES-gmac-256 | van nul
protocol ESP integriteit {md5 | sha-1 | SHA-256 | SHA-384 | SHA-512 | van nul

Opmerking: Microsoft heeft informatie gepubliceerd die conflicteert met de specifieke fase 2 IPSec-encryptie en integriteitskenmerken die door Azure worden gebruikt. De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbaar beschikbare Microsoft document. Fase 2 IPSec kent hier informatie van Microsoft toe die conflicten veroorzaakt. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 6. Configureer een crypto-kaart en pas deze toe op de buiteninterface die deze componenten bevat:
·Het peer IP-adres
·De gedefinieerde toegangslijst die het relevante verkeer bevat
·Het voorstel voor IKEv2 fase 2 IPSec
· De fase 2 IPSec-levensduur in seconden
·Een optionele Perfect Forward Secrecy (PFS)-instelling, die een nieuw paar Diffie-Hellman-toetsen maakt die worden gebruikt om de gegevens te beschermen (beide kanten moeten PFS-ingeschakeld zijn voordat fase 2 verschijnt)

Microsoft heeft informatie gepubliceerd die strijdig is met de specifieke fase 2 IPSec-levensduur en PFS-kenmerken die door Azure worden gebruikt.

De vermelde eigenschappen worden geleverd met de beste inspanning van dit openbare Microsoft-document.

Fase 2 IPSec kent hier informatie van Microsoft toe die conflicten veroorzaakt. Neem voor meer informatie contact op met Microsoft Azure-ondersteuning.

```
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
```

Stap 8. Zorg ervoor dat het VPN-verkeer niet aan een andere NAT-regel wordt onderworpen. Maak een NAT-vrijstellingsregel:

```
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
```

Opmerking: wanneer meerdere subnetten worden gebruikt, moet u objectgroepen maken met alle bron- en doelsubnetten en deze gebruiken in de NAT-regel.

```
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
```

Verifiëren

Nadat u de configuratie op zowel ASA als de Azure-gateway hebt voltooid, start Azure de VPN-tunnel. U kunt verifiëren dat de tunnel correct met deze bevelen bouwt:

Fase 1

Controleer of fase 1 Security Association (SA) is gebouwd:

IKEv2

Vervolgens wordt een IKEv2 SA weergegeven die is gebouwd van een lokale externe interface IP 192.168.1.2 op UDP-poort 500, naar een externe bestemming IP 192.168.2.2. Er is ook een geldig kind SA gebouwd voor gecodeerd verkeer om over te stromen.

```
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
```

Hier wordt een IKEv1 SA met ASA als initiator gebouwd om IP 192.168.2.2 met een resterende levensduur van 86388 seconden te vergelijken weergegeven.

```
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
```

Fase 2

Verifieer de fase 2 IPSec security associatie is gebouwd met **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
```

Vier pakketten worden verzonden en vier worden ontvangen over IPSec SA zonder fouten. Eén inkomende SA met SPI 0x9B60EDC5 en één uitgaande SA met SPI 0x8E7A2E12 zijn geïnstalleerd zoals verwacht.

U kunt ook verifiëren dat gegevens via een controle van de **vpn-sessiondb l2l** boekingen:

```
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
```

Tekst bytes: en bytes Rx: toon verzonden en ontvangen tellers over IPSec SA.

Problemen oplossen

Stap 1. Controleer dat het verkeer voor VPN door ASA wordt ontvangen op de binneninterface die voor het privé-netwerk van Azure is bestemd. Om te testen kunt u een continue ping vanuit een interne client configureren en een pakketopname op ASA configureren om te controleren of deze wordt ontvangen:

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

Opname [cap-name] tonen

```
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
```

Als antwoordverkeer van Azure wordt gezien, dan wordt VPN correct gebouwd en verstuurt/ontvangt verkeer.

Als er geen bronverkeer is, controleert u of uw afzender correct naar de ASA routeert.

Als er bronverkeer wordt gezien maar het antwoordverkeer van Azure ontbreekt, ga dan verder om te verifiëren waarom.

Stap 2. Controleer dat het verkeer dat op ASA binnenkant-interface wordt ontvangen, correct door ASA wordt verwerkt en in VPN wordt verstuurd:

U kunt als volgt een ICMP-echoverzoek simuleren:
Packet-tracer invoer [inside-interface-name] icmp [inside-host-ip] 8.0 [azure-host-ip] detail

De volledige pakket-tracer gebruiksrichtlijnen kunnen hier worden gevonden:
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
```

Merk op dat NAT verkeer vrijstelt (geen vertaling wordt van kracht). Controleer of er geen NAT-vertaling optreedt in het VPN-verkeer.

Controleer ook het volgende: **output-interface** correct is - het moet of de fysieke interface zijn waar de crypto kaart wordt toegepast of de virtuele tunnelinterface.

Zorg ervoor dat er geen toegangslijsten worden weergegeven.

Als de VPN-fase **ENCRYPT: ALLOW** , de tunnel reeds gebouwd is en u kunt IPSec SA zien geïnstalleerd met encaps.

Stap 2.1. Indien **ENCRYPT: ALLOW** gezien in pakkettracer.

Controleer of IPsec SA is geïnstalleerd en versleutelt verkeer met het gebruik van **show crypto ipsec sa** .

U kunt een opname uitvoeren op de buiteninterface om te verifiëren dat versleutelde pakketten worden verzonden van ASA en versleutelde antwoorden worden ontvangen van Azure.

Stap 2.2. Indien **ENCRYPT:DROP** gezien in pakkettracer.

VPN-tunnel is nog niet tot stand gebracht, maar is in onderhandeling. Dit is een verwachte voorwaarde wanneer u eerst de tunnel omhoog brengt. De looppas zuivert om het proces van de tunnelonderhandeling te bekijken en te identificeren waar en als een mislukking voorkomt.

Controleer eerst of de juiste versie van IKE is geactiveerd en dat het proces van IKE geen relevante fouten vertoont:

```
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.
```

Als er geen ike-common debug-uitvoer wordt gezien wanneer VPN-verkeer wordt gestart, betekent dit dat verkeer wordt gedropt voordat het het crypto-proces bereikt of dat crypto ikev1/ikev2 niet op het vak is ingeschakeld. Controleer de crypto-configuratie en de pakketdrops.

Als ike-common debugs laat zien dat het cryptoproces wordt geactiveerd, debug dan de door IKE geconfigureerde versie om tunnelonderhandelingsberichten te bekijken en identificeer waar de fout optreedt in tunnelbouw met Azure.

IKEv1-software

Volledige ikev1 debug procedure en analyse kan hier gevonden worden.

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

IKEv2

Volledige ikev2 debug procedure en analyse kan hier gevonden worden.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.