Konfigurieren eines richtlinienbasierten und routenbasierten VPN von ASA und FTD zu Microsoft Azure

Inhalt

Einleitung

In diesem Dokument werden die Konzepte und die Konfiguration für ein VPN zwischen Cisco ASA und Cisco Secure Firewall sowie Microsoft Azure Cloud Services beschrieben.

Konzepte

VPN-Verschlüsselungsdomäne

Der IP-Adressbereich IPSec ermöglicht die Teilnahme am VPN-Tunnel. Die Verschlüsselungsdomäne wird mithilfe eines lokalen Datenverkehrsselektors und eines Remote-Datenverkehrsselektors definiert, um festzulegen, welche lokalen und Remote-Subnetzbereiche von IPSec erfasst und verschlüsselt werden. Es gibt zwei Methoden zum Definieren der VPN-Verschlüsselungsdomänen: route- oder richtlinienbasierte Datenverkehrsauswahl.

Routenbasiert:
Die Verschlüsselungsdomäne ist so festgelegt, dass jeder Datenverkehr zugelassen wird, der in den IPSec-Tunnel eingeht. Die Auswahl für lokalen und Remote-Datenverkehr von IPSec ist auf 0.0.0.0 festgelegt. Dies bedeutet, dass der gesamte Datenverkehr, der in den IPSec-Tunnel geleitet wird, unabhängig vom Quell-/Ziel-Subnetz verschlüsselt wird.

Cisco Adaptive Security Appliance (ASA) unterstützt routenbasiertes VPN unter Verwendung von Virtual Tunnel Interfaces (VTIs) ab Version 9.8.

Cisco Secure Firewall oder FirePOWER Threat Defense (FTD), verwaltet von FMC (FirePOWER Management Center), unterstützt routenbasiertes VPN unter Verwendung von VTIs in Version 6.7 und höher.

Richtlinienbasiert:

Die Verschlüsselungsdomäne ist so festgelegt, dass nur bestimmte IP-Bereiche sowohl für die Quelle als auch für das Ziel verschlüsselt werden. Richtlinienbasierte lokale Datenverkehrsauswahl- und Remote-Datenverkehrsauswahl geben an, welcher Datenverkehr über IPSec verschlüsselt werden soll.

ASA unterstützt richtlinienbasiertes VPN mit Crypto Maps in Version 8.2 und höher.

Microsoft Azure unterstützt route-, richtlinienbasierte oder routenbasierte Datenverkehrsauswahl mit simulierten richtlinienbasierten Datenverkehrsselektoren. Azure schränkt derzeit die IKE-Version (Internet Key Exchange) ein, die Sie auf Basis der ausgewählten VPN-Methode konfigurieren können. Routenbasiert erfordert IKEv2, und richtlinienbasiert erfordert IKEv1. Dies bedeutet, dass bei Verwendung von IKEv2 in Azure routenbasiert ausgewählt werden muss und ASA eine VTI verwenden muss. Wenn die ASA jedoch aufgrund der Codeversion nur Kryptografiezuordnungen unterstützt, muss Azure mit richtlinienbasierten Datenverkehrsselektoren routenbasiert konfiguriert werden. Dies wird im Azure-Portal über die PowerShell-Skriptbereitstellung erreicht, um eine Option zu implementieren, die Microsoft wie folgt UsePolicyBasedTrafficSelectors aufruft: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps

Zusammenfassend aus der ASA- und FTD-Konfigurationsperspektive:

- Für ASA/FTD, die mit einer Crypto Map konfiguriert wurden, muss Azure für richtlinienbasiertes VPN oder routenbasiert mit UsePolicyBasedTrafficSelectors konfiguriert werden.
- Für ASA, die mit einem VTI konfiguriert wurde, muss Azure für ein routenbasiertes VPN konfiguriert werden.
- Weitere Informationen zur Konfiguration von VTIs für FTD finden Sie hier. 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

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Für IKEv2-Routing-basiertes VPN, das VTI auf ASA verwendet: ASA-Code Version 9.8(1) oder höher (Azure muss für routenbasiertes VPN konfiguriert sein.)
- Für IKEv1-richtlinienbasiertes VPN, das die Crypto Map auf ASA und FTD verwendet: ASA-Code Version 8.2 oder höher und FTD 6.2.0 oder höher. (Azure muss für richtlinienbasiertes VPN konfiguriert sein.)
- Für IKEv2-VPN auf Routenbasis, das Crypto Map auf ASA mit richtlinienbasierten

Datenverkehrsauswahl-Optionen verwendet: ASA-Code Version 8.2 oder höher, der mit einer Crypto Map konfiguriert wurde. (Azure muss für routenbasiertes VPN mit UsePolicyBasedTrafficSelectors konfiguriert werden.)
- Kenntnisse von FMC für FTD-Management und -Konfiguration.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

Führen Sie die Konfigurationsschritte aus. Sie können entweder IKEv1, IKEv2-Routenbasiert mit VTI oder IKEv2-Routenbasiert mit richtlinienbasierten Traffic Selectors (Crypto Map auf ASA) konfigurieren.

IKEv1-Konfiguration auf ASA

Bei einem standortübergreifenden IKEv1-VPN von ASA zu Azure befolgen Sie die nächste ASA-Konfiguration. Stellen Sie sicher, dass Sie im Azure-Portal einen richtlinienbasierten Tunnel konfigurieren. Für dieses Beispiel werden auf ASA Crypto Maps verwendet.

Weitere Informationen zur ASA-Konfiguration finden Sie in diesem Cisco Dokument.

Schritt 1: Aktivieren Sie IKEv1 auf der externen Schnittstelle.

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

Schritt 2: Erstellen Sie eine IKEv1-Richtlinie, die die Algorithmen/Methoden für Hash, Authentifizierung, Diffie-Hellman-Gruppe, Lebensdauer und Verschlüsselung definiert.

> **Anmerkung:** Die aufgelisteten IKEv1-Attribute der Phase 1 werden bestmöglich aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 3: Erstellen Sie unter den IPsec-Attributen eine Tunnelgruppe, und konfigurieren Sie die Peer-IP-Adresse und den vorinstallierten Tunnelschlüssel.

```
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
```

Schritt 4: Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden und zu tunnelnden Datenverkehr definiert. In diesem Beispiel ist der relevante Datenverkehr der Datenverkehr aus dem Tunnel, der vom Subnetz 10.2.2.0 an 10.1.1.0 stammt. Er kann mehrere Einträge enthalten, wenn zwischen den Standorten mehrere Subnetze vorhanden sind.

In Version 8.4 und höher können Objekte oder Objektgruppen erstellt werden, die als Container für Netzwerke, Subnetze, Host-IP-Adressen oder mehrere Objekte dienen. Erstellen Sie zwei Objekte mit den lokalen und den Remote-Subnetzen, und verwenden Sie sie sowohl für die Crypto Access Control List (ACL)- als auch für die Network Address Translation (NAT)-Anweisungen.

```
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
```

Schritt 5: Konfigurieren Sie den Transformationssatz (TS), der das Schlüsselwort enthalten muss**IKEv1**. Auch am Remote-Ende muss ein identischer TS erstellt werden.

> **Anmerkung:** Die aufgelisteten IKEv1-Attribute der Phase 2 werden bestmöglich aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

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

Schritt 6: Konfigurieren Sie die Crypto Map, und wenden Sie sie auf die externe Schnittstelle an, die folgende Komponenten enthält:

- Die Peer-IP-Adresse
- Die definierte Zugriffsliste, die den Datenverkehr von Interesse enthält
- TS
- In der Konfiguration wird kein Perfect Forward Secrecy (PFS) festgelegt, da in der öffentlich verfügbaren Azure-Dokumentation angegeben ist, dass PFS für IKEv1 in Azure deaktiviert ist. Eine optionale PFS-Einstellung, die ein neues Paar Diffie-Hellman-Schlüssel erstellt, die zum Schutz der Daten verwendet werden (beide Seiten müssen PFS-aktiviert sein, bevor Phase 2 aktiviert wird), kann mithilfe dieser Konfiguration aktiviert werden: **crypto map outside_map 20 set pfs** .
- Die festgelegten IPSec-Lebensdauern für Phase 2 basieren auf der öffentlich verfügbaren Azure-Dokumentation. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 7: Stellen Sie sicher, dass der VPN-Datenverkehr keiner anderen NAT-Regel unterliegt. Erstellen Sie eine NAT-Ausnahmeregelung:

```
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
```

> **Hinweis**: Wenn mehrere Subnetze verwendet werden, müssen Sie Objektgruppen mit allen Quell- und Zielsubnetzen erstellen und diese in der NAT-Regel verwenden.

```
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 Routenbasiert mit VTI auf ASA-Code 9.8 (1) oder höher

Befolgen Sie bei einem Site-to-Site IKEv2 Route Based VPN on ASA-Code die folgende Konfiguration. Stellen Sie sicher, dass Azure für routenbasiertes VPN konfiguriert ist, und konfigurieren Sie UsePolicyBasedTrafficSelectors nicht im Azure-Portal. Auf der ASA wird ein VTI konfiguriert.

Vollständige Informationen zur ASA VTI-Konfiguration finden Sie in diesem Cisco Dokument.

Schritt 1: Aktivieren Sie IKEv2 auf der externen Schnittstelle:

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

Schritt 2: Fügen Sie eine IKEv2 Phase 1-Richtlinie hinzu.

> **Hinweis**: Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten Verschlüsselungs-, Integritäts- und Lebensdauerattribute von IKEv2 Phase 1 in Konflikt stehen. Die aufgeführten Attribute werden am besten aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Die Informationen, die ein Konflikt mit dem IKEv2-Attribut von Microsoft verursachen, sind hier zu sehen. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 3: Fügen Sie einen IPsec-Vorschlag für IKEv2 Phase 2 hinzu. Geben Sie die Sicherheitsparameter in der Krypto-IPsec an. **ikev2 ipsec-proposal** Konfigurationsmodus:

Protokoll-ESP-Verschlüsselung {des | 3de | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
Protokoll-ESP-Integrität {md5 | SHA-1 | SHA-256 | SHA-384 | SHA-512 | null}

> **Anmerkung:** Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten IPSec-Verschlüsselungs- und Integritätsattribute der Phase 2 in Konflikt stehen. Die aufgeführten Attribute werden am besten aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Die Informationen, die dem IPSec-Attribut der Phase 2 von Microsoft in Konflikt stehen, sind hier zu sehen. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 4: Fügen Sie ein IPSec-Profil hinzu, das Folgendes angibt:

- Der zuvor konfigurierte IPSec-Vorschlag für ikev2 Phase 2
- IPSec-Lebensdauer der Phase 2 (optional) in Sekunden und/oder Kilobyte
- Die PFS-Gruppe (optional)

> **Anmerkung:** Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten IPSec-Lebensdauer und PFS-Attribute der Phase 2 in Konflikt stehen. Die aufgeführten Attribute werden am besten aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Die Informationen, die dem IPSec-Attribut der Phase 2 von Microsoft in Konflikt stehen, sind hier zu sehen. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 5: Erstellen Sie eine Tunnelgruppe unter den IPsec-Attributen, und konfigurieren Sie die Peer-IP-Adresse sowie den lokalen und den vorinstallierten IKEv2-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
```

Schritt 6: Erstellen Sie einen VTI mit folgenden Angaben:

- Eine neue Tunnelschnittstellennummer: interface tunnel [Nummer]
- Neuer Name der Tunnelschnittstelle: nameEIF [Name]
- Eine auf der Tunnelschnittstelle nicht vorhandene IP-Adresse: ip address [IP-Adresse] [Maske]
- Tunnelquellenschnittstelle, bei der das VPN lokal endet: tunnel source interface [int-name]
- Die IP-Adresse des Azure-Gateways: tunnel destination [Öffentliche Azure-IP]
- IPSec-IPv4-Modus: Tunnelmodus IPsec IPv4
- Das IPSec-Profil für diesen VTI: tunnel protection ipsec-Profil [Profilname]

```
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
```

Schritt 7: Erstellen Sie eine statische Route, um Datenverkehr in den Tunnel zu leiten. Um eine statische Route hinzuzufügen, geben Sie den folgenden Befehl ein:
route if_name dest_ip mask gateway_ip [distance]

Die Fehlermeldung **dest_ip** und **mask** ist die IP-Adresse für das Zielnetzwerk in der Azure-Cloud, z. B. 10.0.0.0/24. Bei gateway_ip muss es sich um eine beliebige IP-Adresse (vorhanden oder nicht vorhanden) im Tunnelschnittstellen-Subnetz handeln, z. B. 169.254.0.2. Ziel dieses gateway_ip ist es, Datenverkehr in die Tunnelschnittstelle zu leiten, die jeweilige Gateway-IP selbst ist jedoch unwichtig.

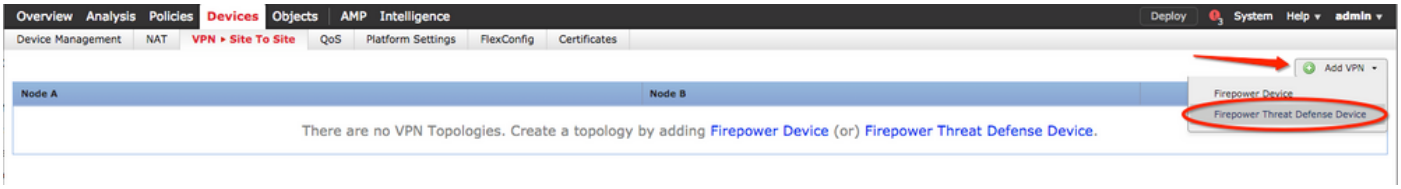
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

IKEv1-Konfiguration auf FTD

Für ein standortübergreifendes IKEv1-VPN von FTD zu Azure müssen Sie das FTD-Gerät zuvor bei FMC registriert haben.

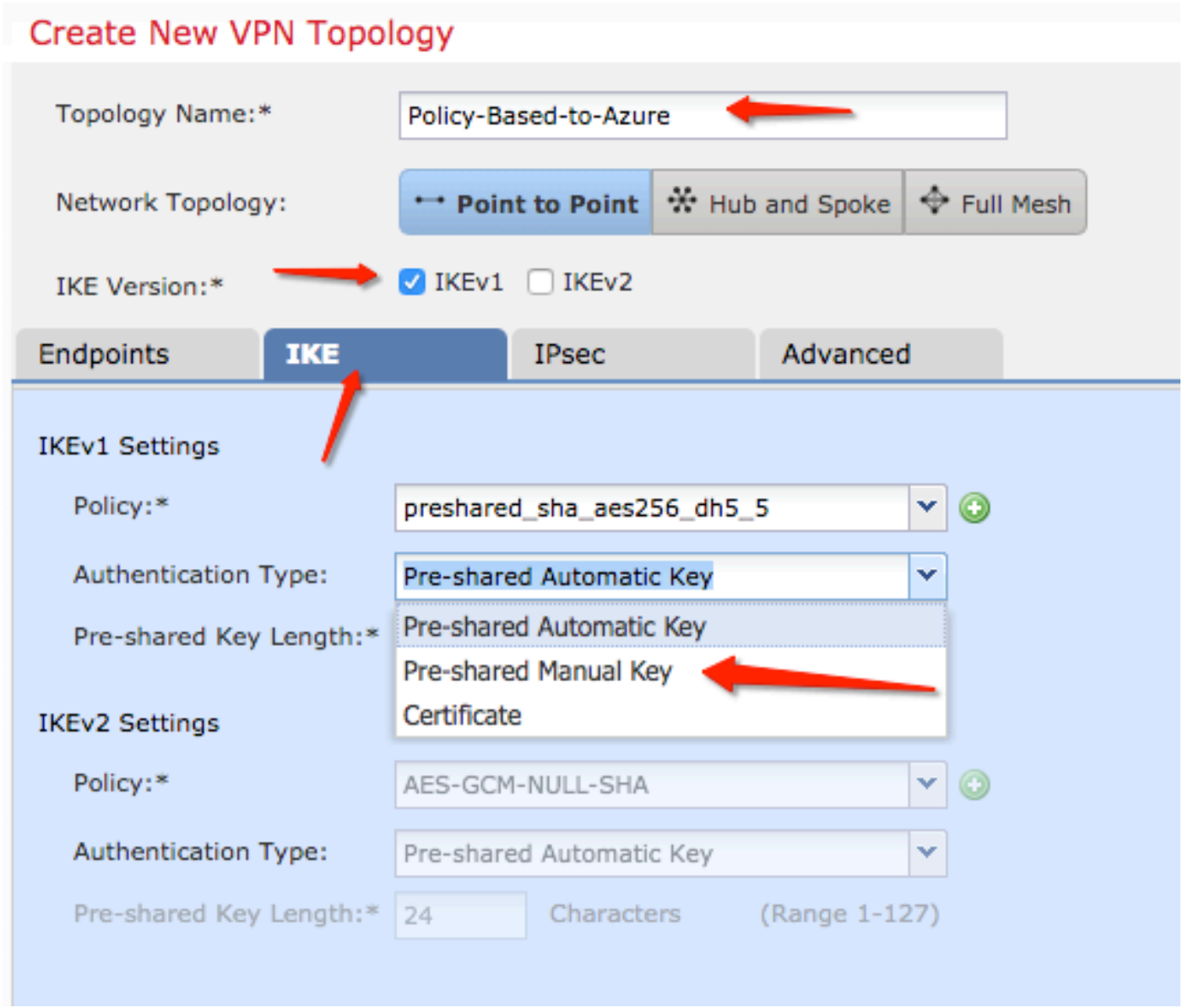
Schritt 1: Erstellen einer Site-to-Site-Richtlinie Navigieren Sie zum **FMC dashboard > Devices > VPN > Site to Site**.

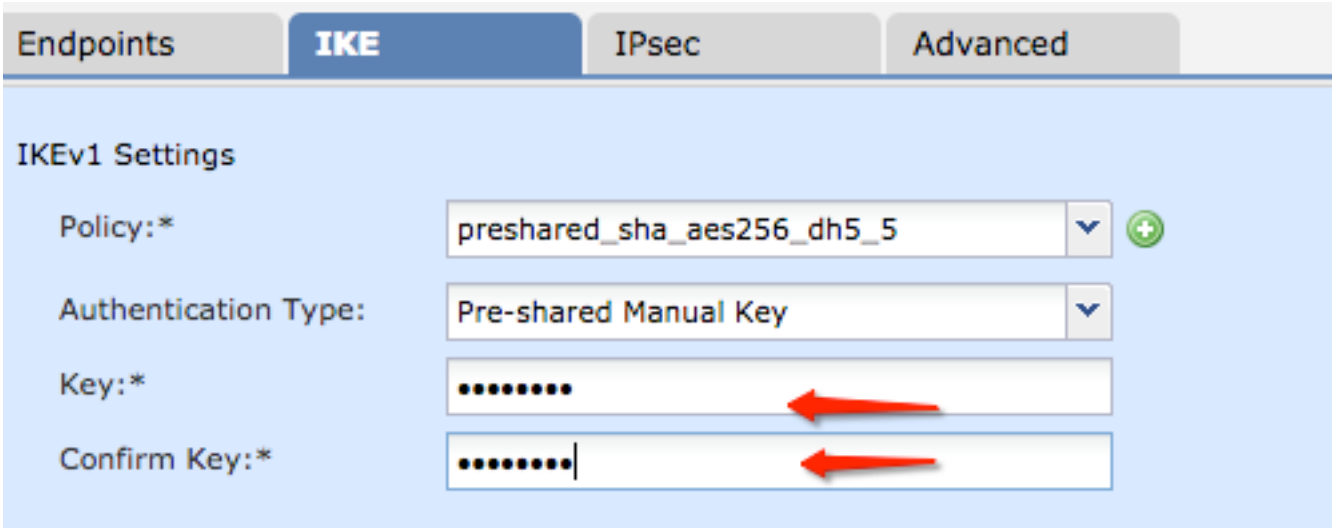
Schritt 2: Erstellen einer neuen Richtlinie Klicken Sie auf **Add VPN** Dropdown-Menü und wählen **Firepower Threat Defense device .**



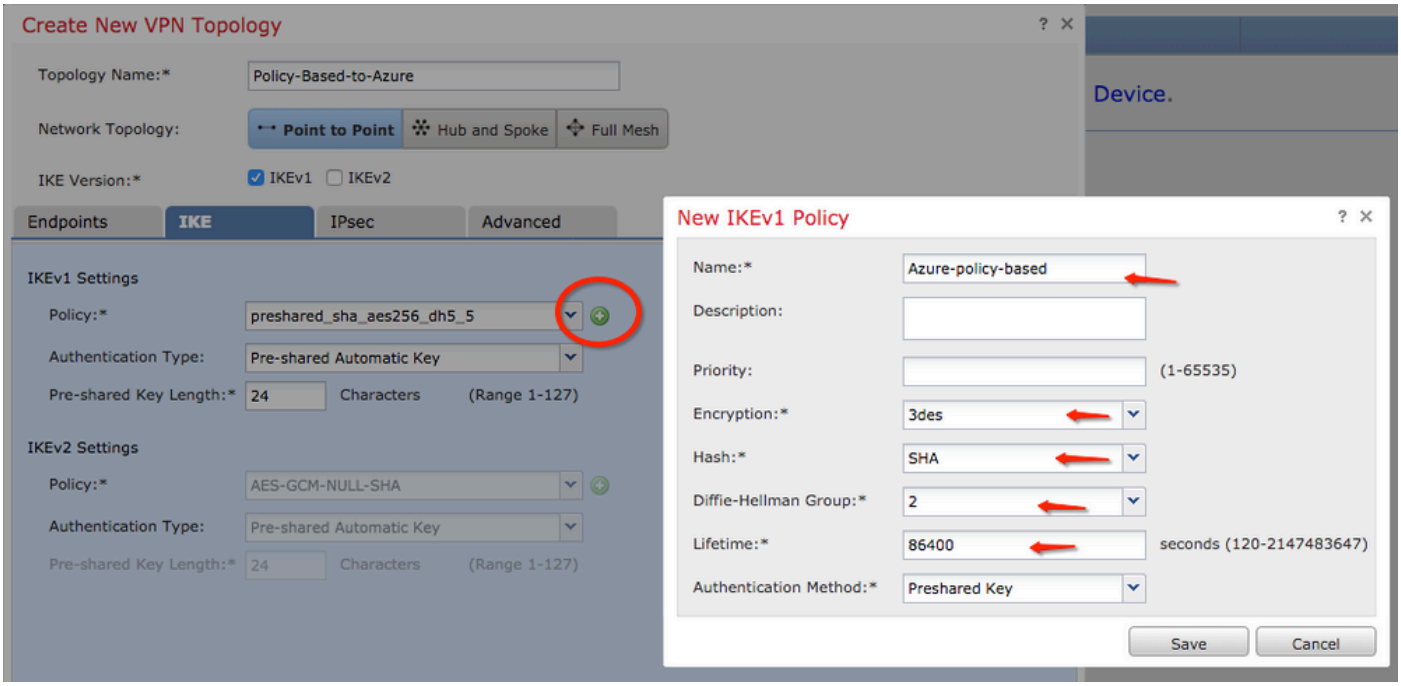
Schritt 3: Auf der **Create new VPN Topology** Fenster, geben Sie Ihre **Topology Name**, überprüfen Sie die **IKEV1** Protokoll-Checkbox und klicken Sie auf **IKE** aus. Für dieses Beispiel werden vorinstallierte Schlüssel als Authentifizierungsmethode verwendet.

Klicken Sie auf **Authentication Type** und wählen Sie **Pre-shared manual key** . Geben Sie den manuellen Pre-Shared Key auf der **Key** und**Confirm Key** Textfelder.

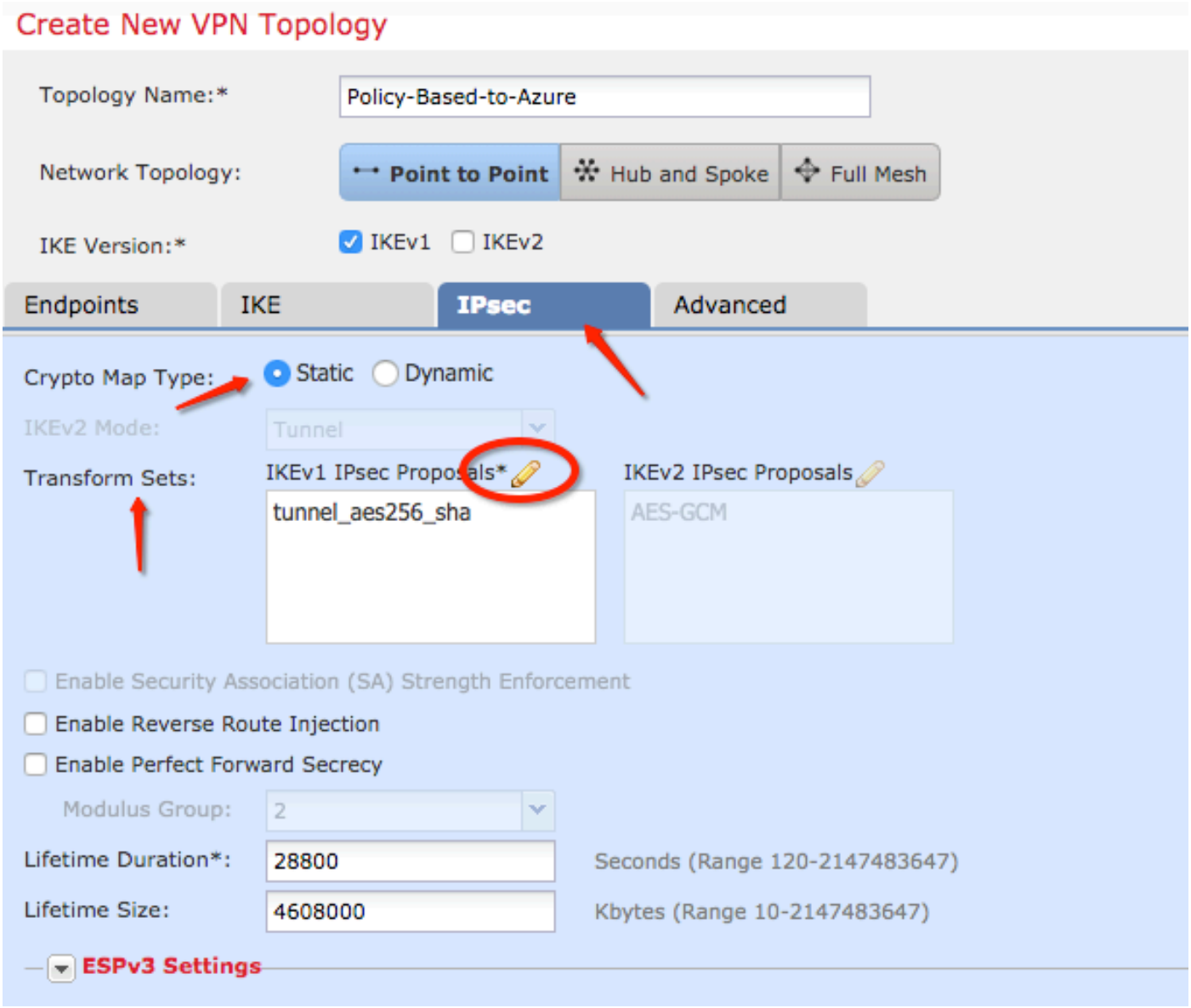




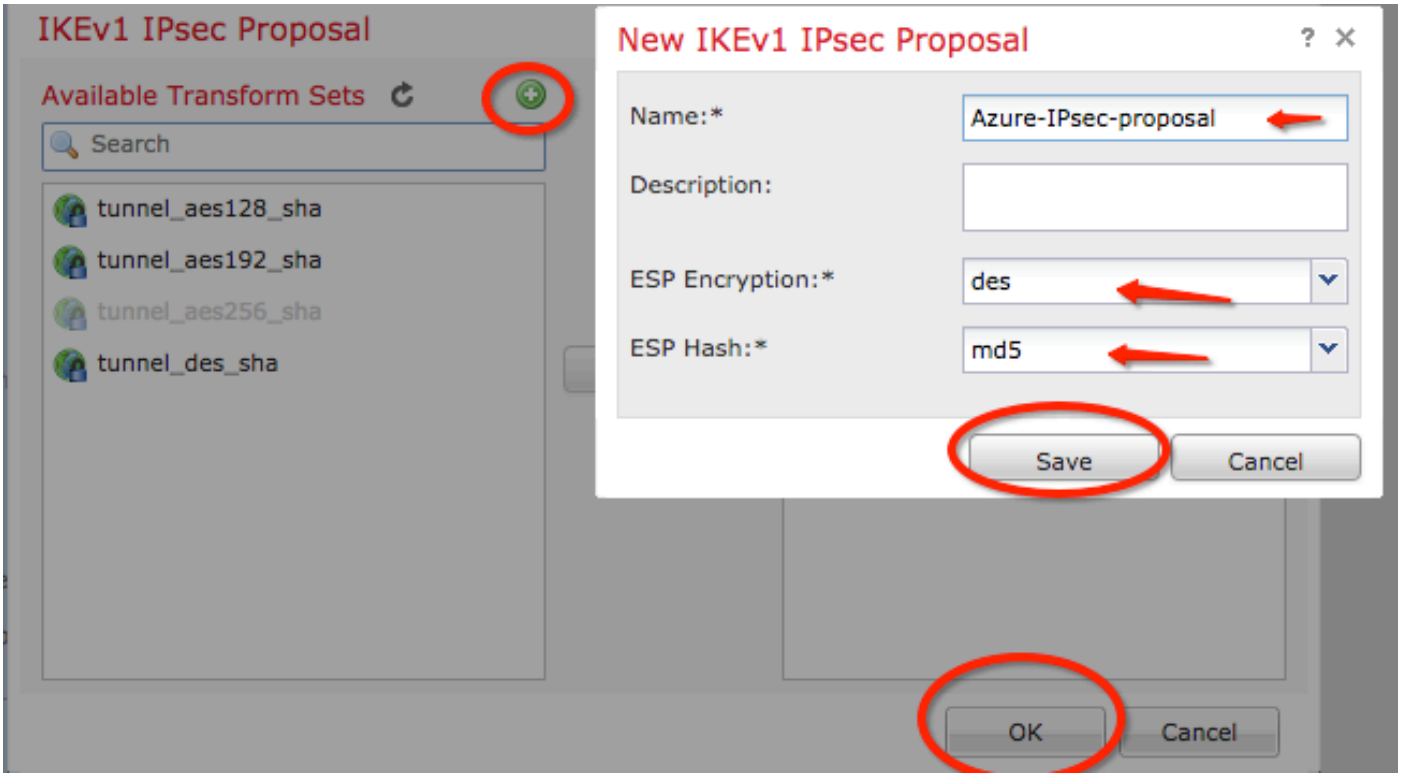
Schritt 4: Konfigurieren Sie die ISAKMP-Richtlinie oder die Parameter für Phase 1, indem Sie eine neue erstellen. Klicken Sie im gleichen Fenster auf das **green plus button** um eine neue ISAKMP-Richtlinie hinzuzufügen. Geben Sie den Namen der Richtlinie an, wählen Sie die gewünschte Verschlüsselung, Hash, Diffie-Hellman-Gruppe, Lebensdauer und Authentifizierungsmethode aus, und klicken Sie auf **Save** .



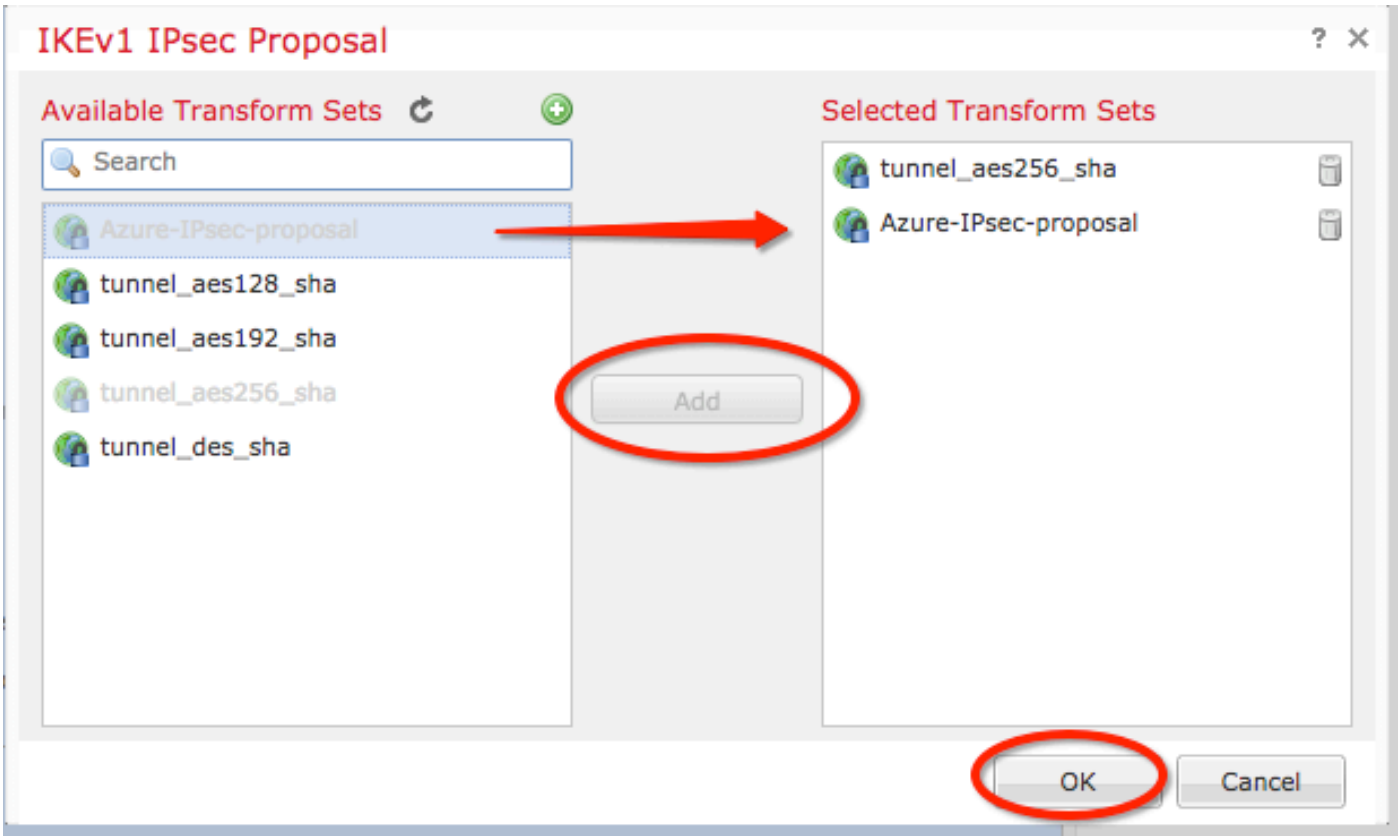
Schritt 5: Konfigurieren der IPsec-Richtlinie oder der Parameter für Phase 2 Navigieren Sie zum **IPsec** Registerkarte auswählen **Static** auf der **Crypto Map Type** Kontrollkästchen. Klicken Sie auf **edit pencil** des **IKEV1 IPsec Proposals** am **Transform Sets** Option.



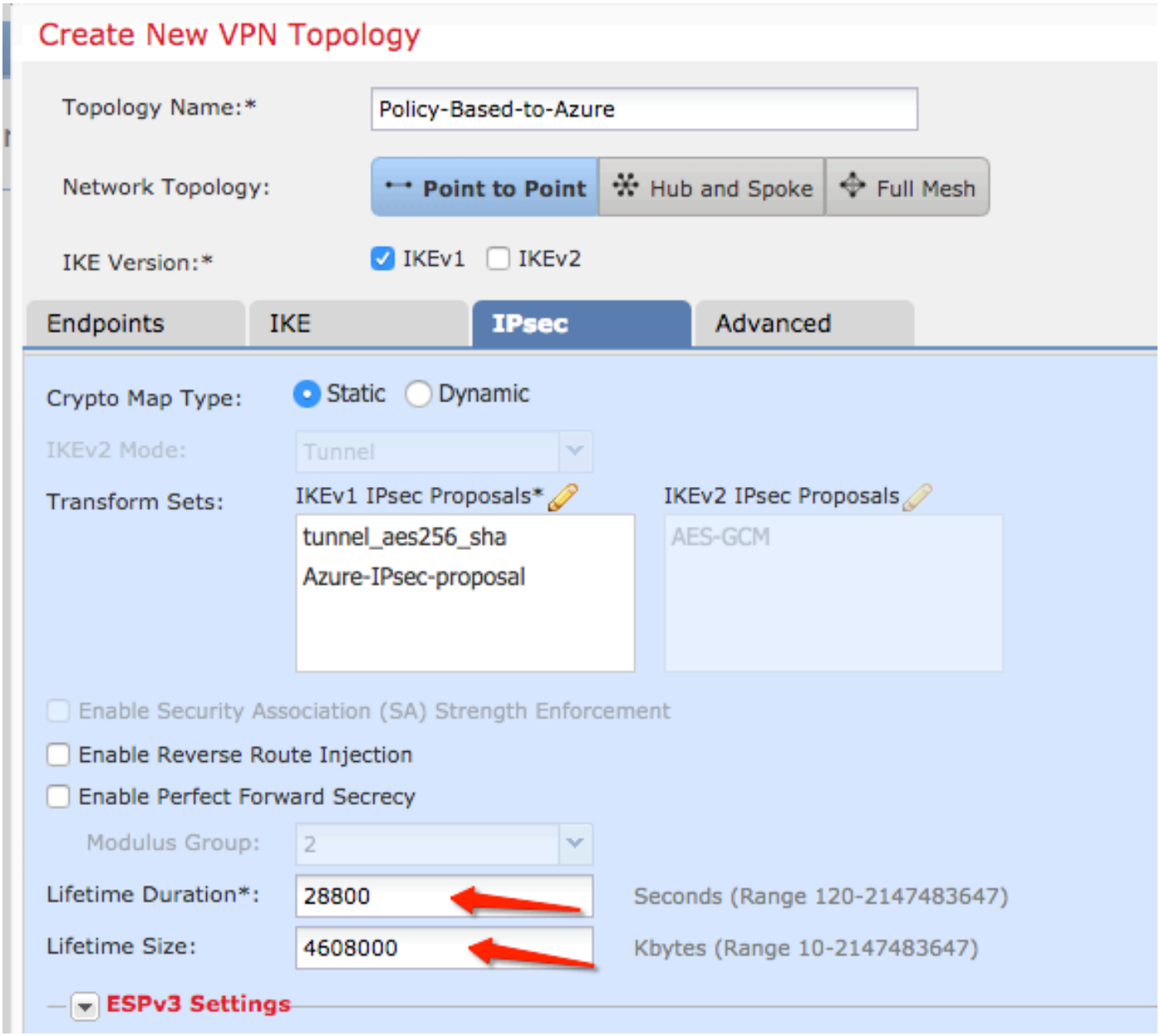
Schritt 6: Erstellen Sie ein neues IPsec-Angebot. Auf dem **IKEv1 IPSec Proposal** auf das **green plus button** um eine neue hinzuzufügen. Geben Sie den Namen der Richtlinie und die gewünschten Parameter für die ESP-Verschlüsselung und die ESP-Hash-Algorithmen an, und klicken Sie auf **Save** .



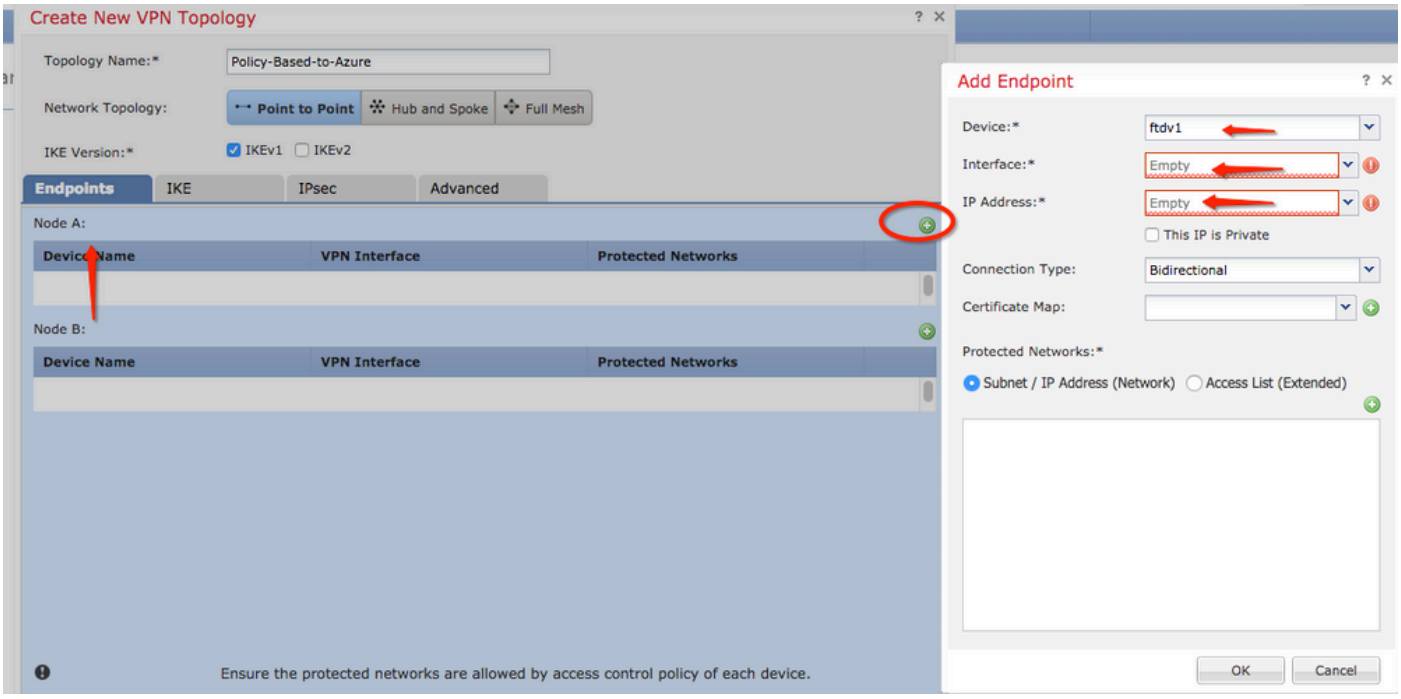
Schritt 7. Auf dem **IKEV1 IPsec Proposal** wird die neue IPsec-Richtlinie dem **Selected Transform Sets** Abschnitt und klicken Sie auf **OK** .



Schritt 8: Zurück zum **IPSec** konfigurieren Sie die gewünschte Lebensdauer und Größe.



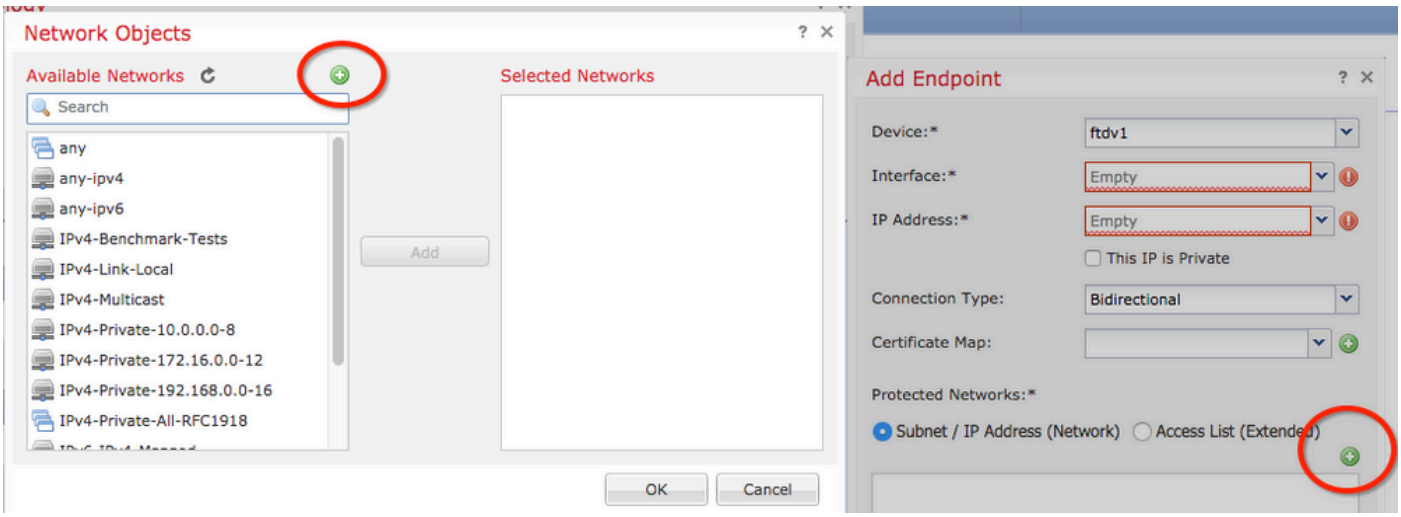
Schritt 9: Wählen Sie die Verschlüsselungsdomäne/Datenverkehrsauswahl/Geschützte Netzwerke aus. Navigieren Sie zum **Endpoints** aus. Auf dem **Node A** Abschnitt klicken Sie auf **green plus button** um eine neue hinzuzufügen. In diesem Beispiel wird Knoten A als lokale Subnetze des FTD verwendet.



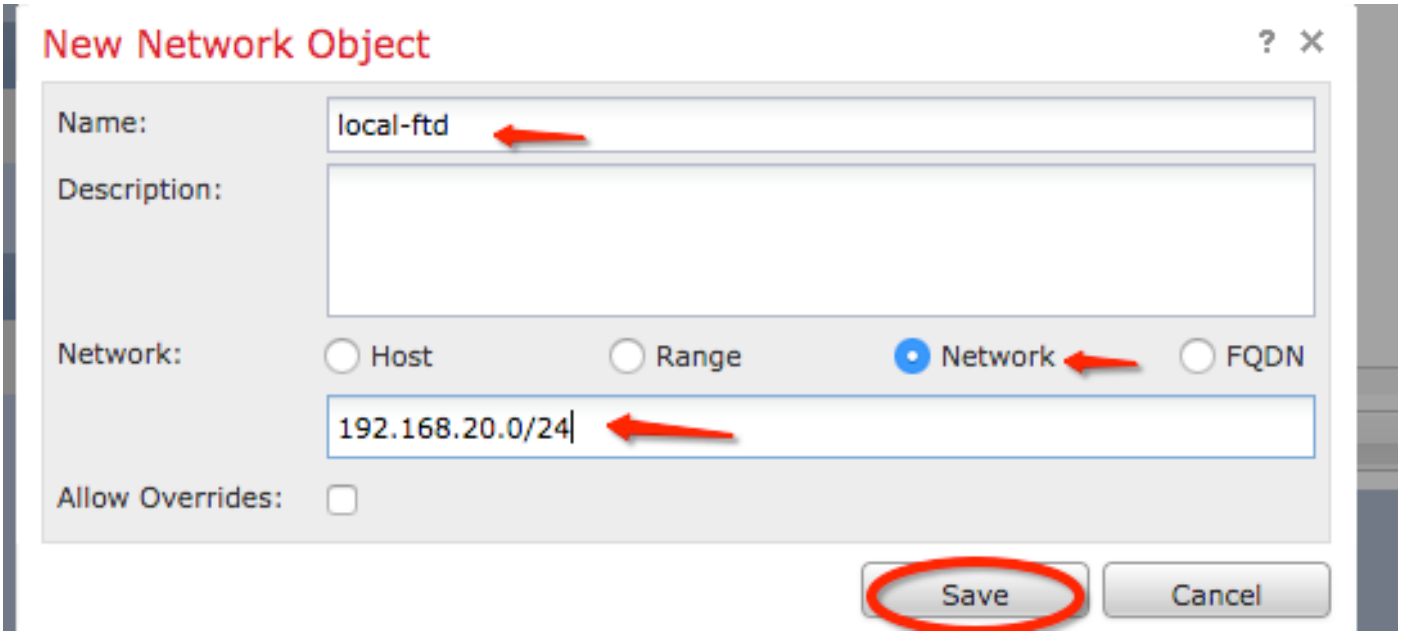
Schritt 10. Auf der **Add Endpoint** das FTD, das auf dem **Device** zusammen mit der physischen Schnittstelle und der zu verwendenden IP-Adresse.

Schritt 11: Navigieren Sie zum Selektor für den lokalen Datenverkehr **Protected Networks** und klicke auf den **green plus button** um ein neues Objekt zu erstellen.

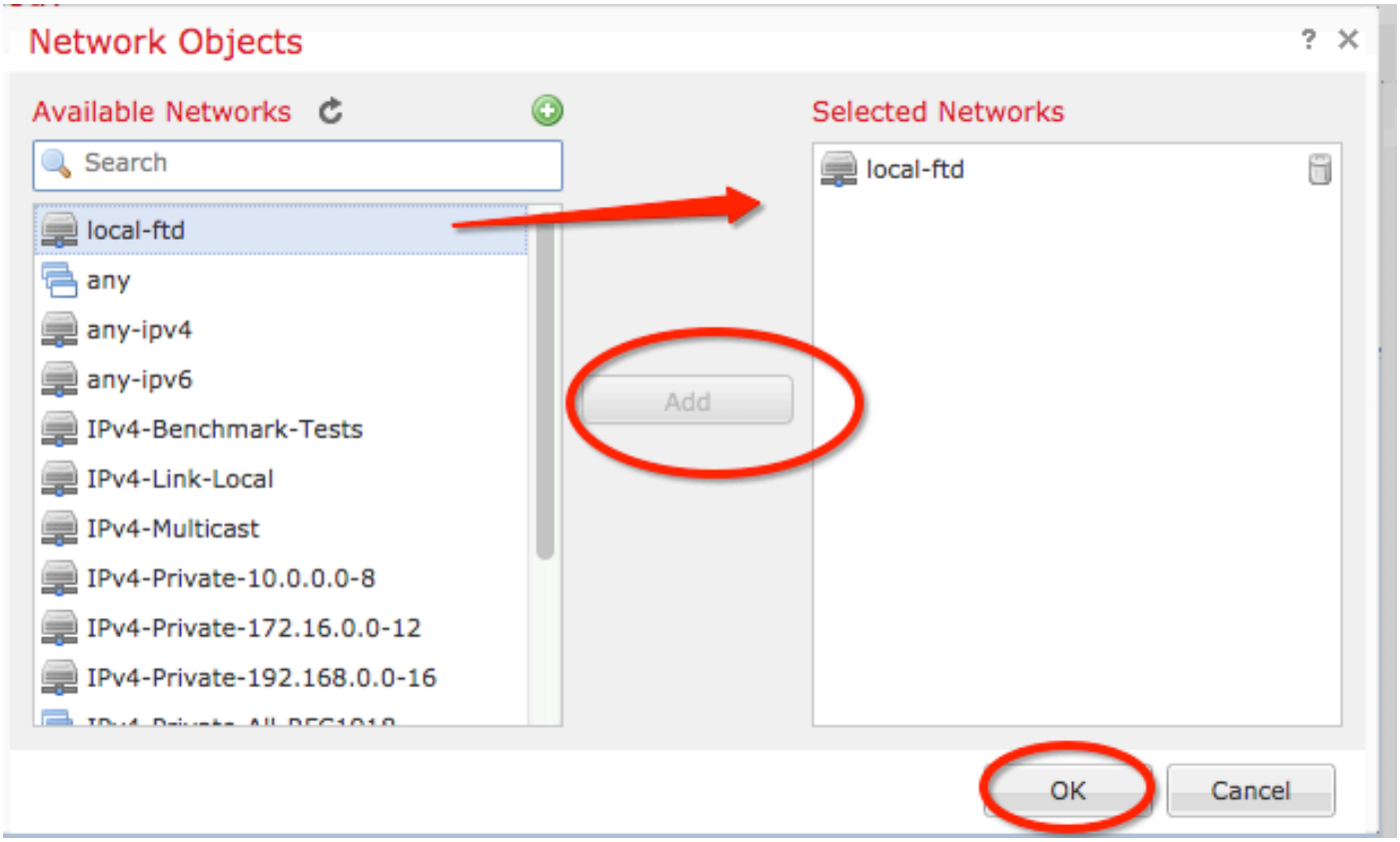
Schritt 12: Auf der **Network Objects** auf das **green plus button** neben dem **Available Networks** Text, um ein neues lokales Datenverkehrsselektionsobjekt zu erstellen.



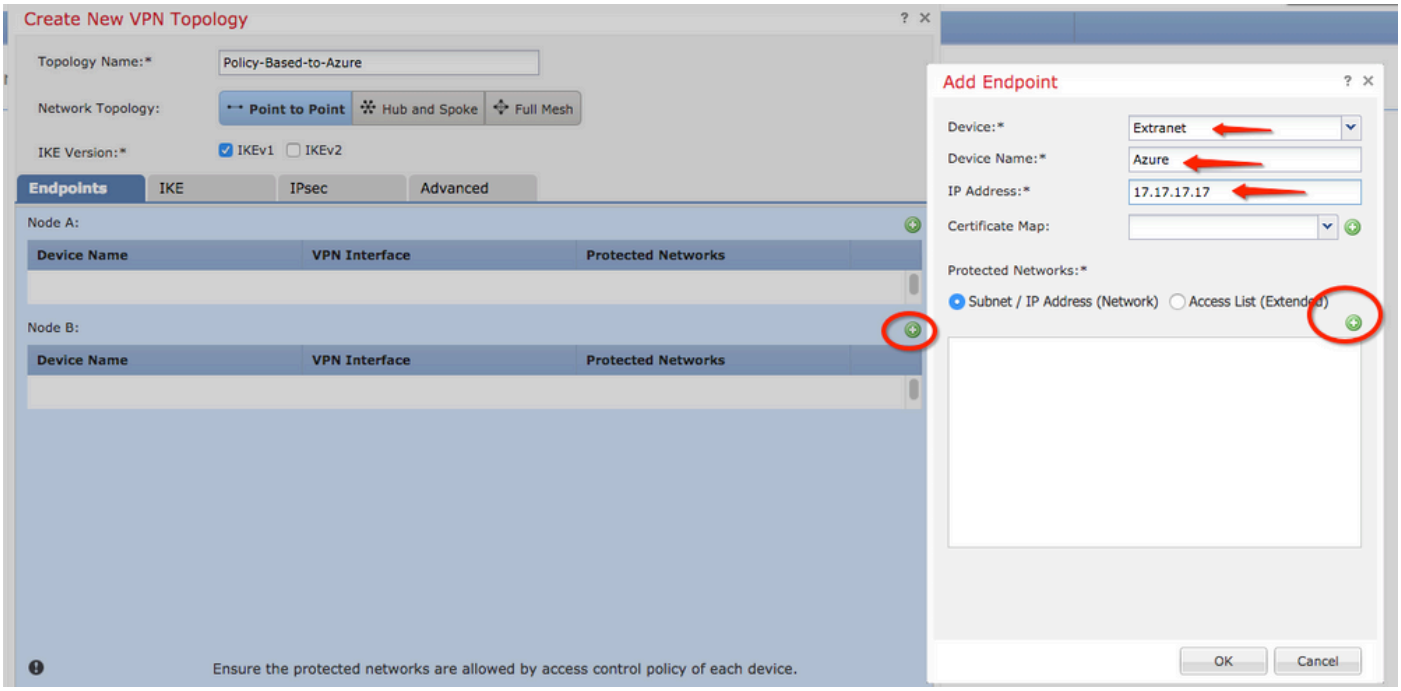
Schritt 13: Auf der **New Network Object** den Namen des Objekts an und wählen Sie entsprechend Host/Netzwerk/Bereich/FQDN. Klicken Sie anschließend auf **Save** .



Schritt 14: Fügen Sie das Objekt der **Selected Networks** Abschnitt über **Network Objects** und klicke auf **OK** . Klicken Sie auf **OK** auf der **Add Endpoint** angezeigt.

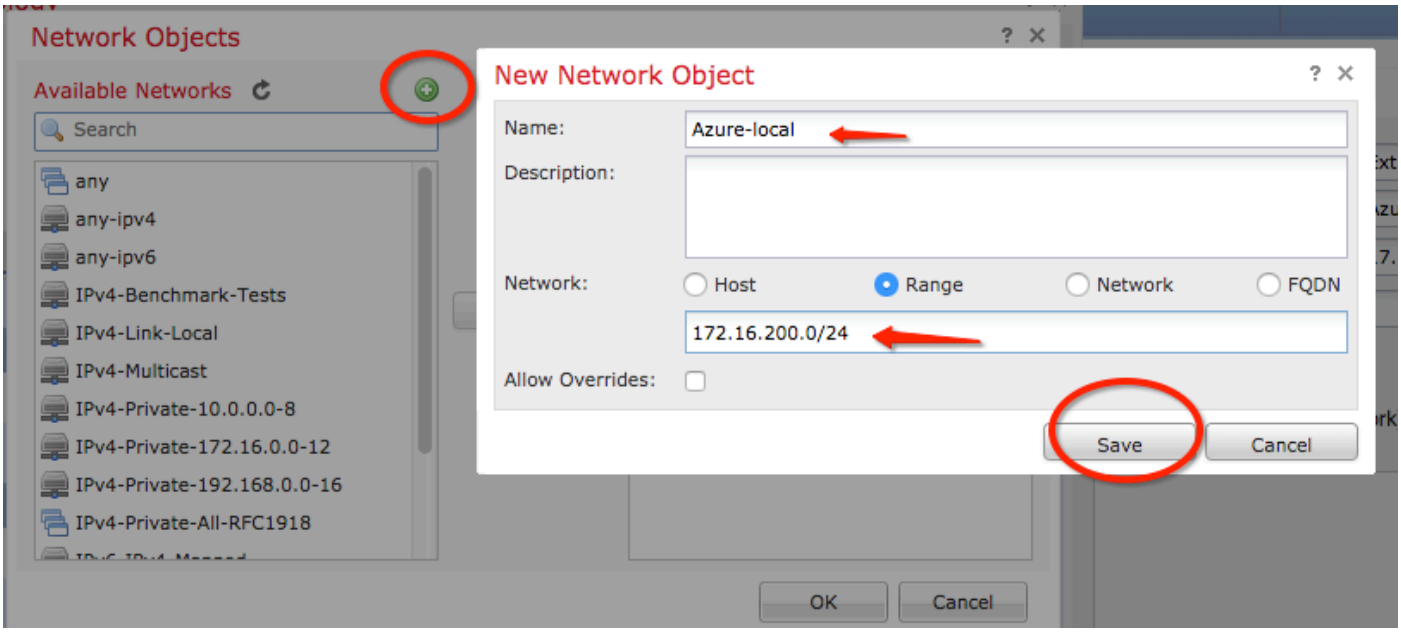


Schritt 15: Definieren Sie den Endpunkt von Knoten B, der in diesem Beispiel der Azure-Endpunkt ist. Auf dem **Create New VPN Topology** Fenster, navigieren Sie zum **Node B** und klicken Sie auf **green plus button** um den Selektor für den Datenverkehr von Remote-Endpunkten hinzuzufügen. Angeben **Extranet** für alle VPN-Peer-Endpunkte, die nicht vom gleichen FMC wie Knoten A verwaltet werden. Geben Sie den Namen des Geräts (nur lokal bedeutsam) und seine IP-Adresse ein.

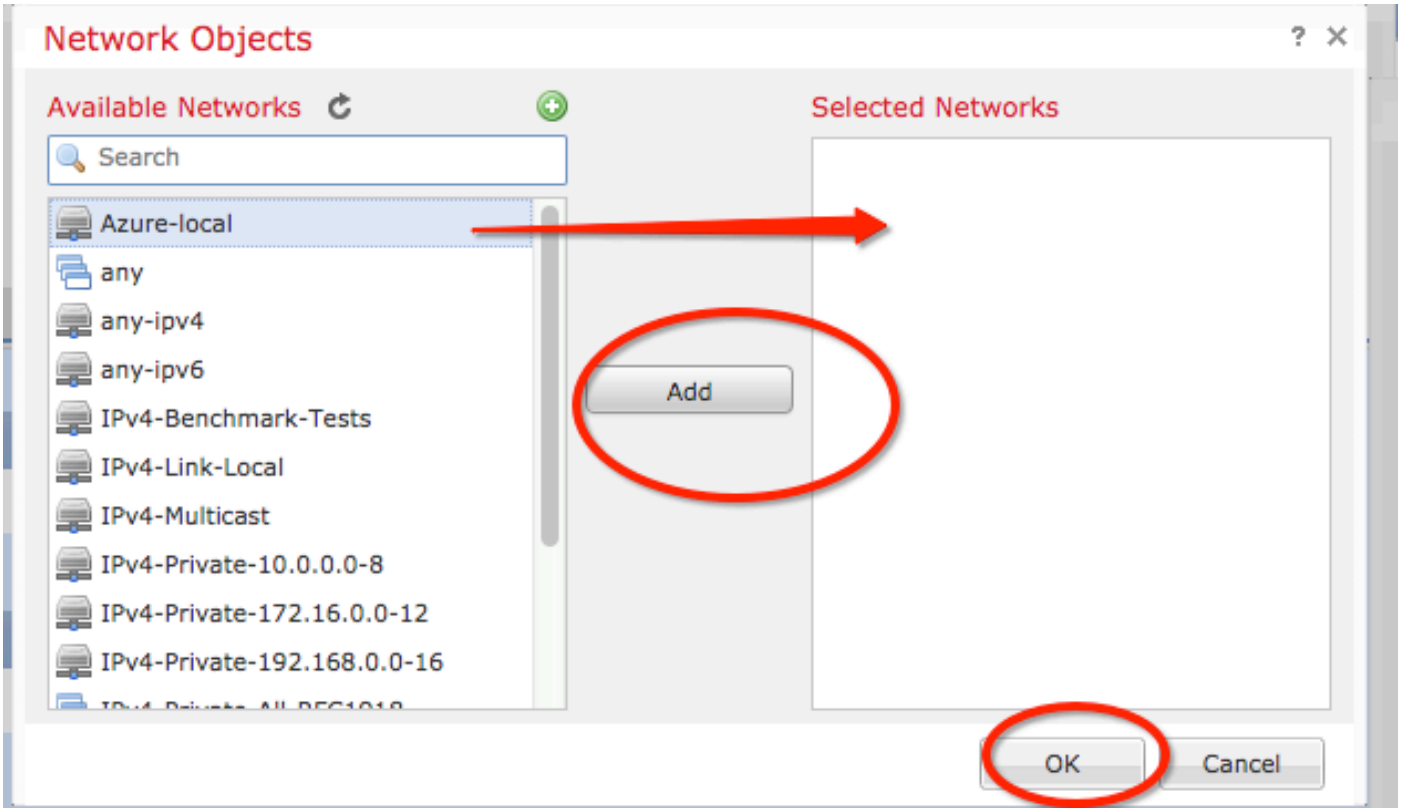


Schritt 16: Erstellen Sie das Remote-Datenverkehrsselektionsobjekt. Navigieren Sie zum **Protected Networks** und klicke auf das **green plus button** um ein neues Objekt hinzuzufügen.

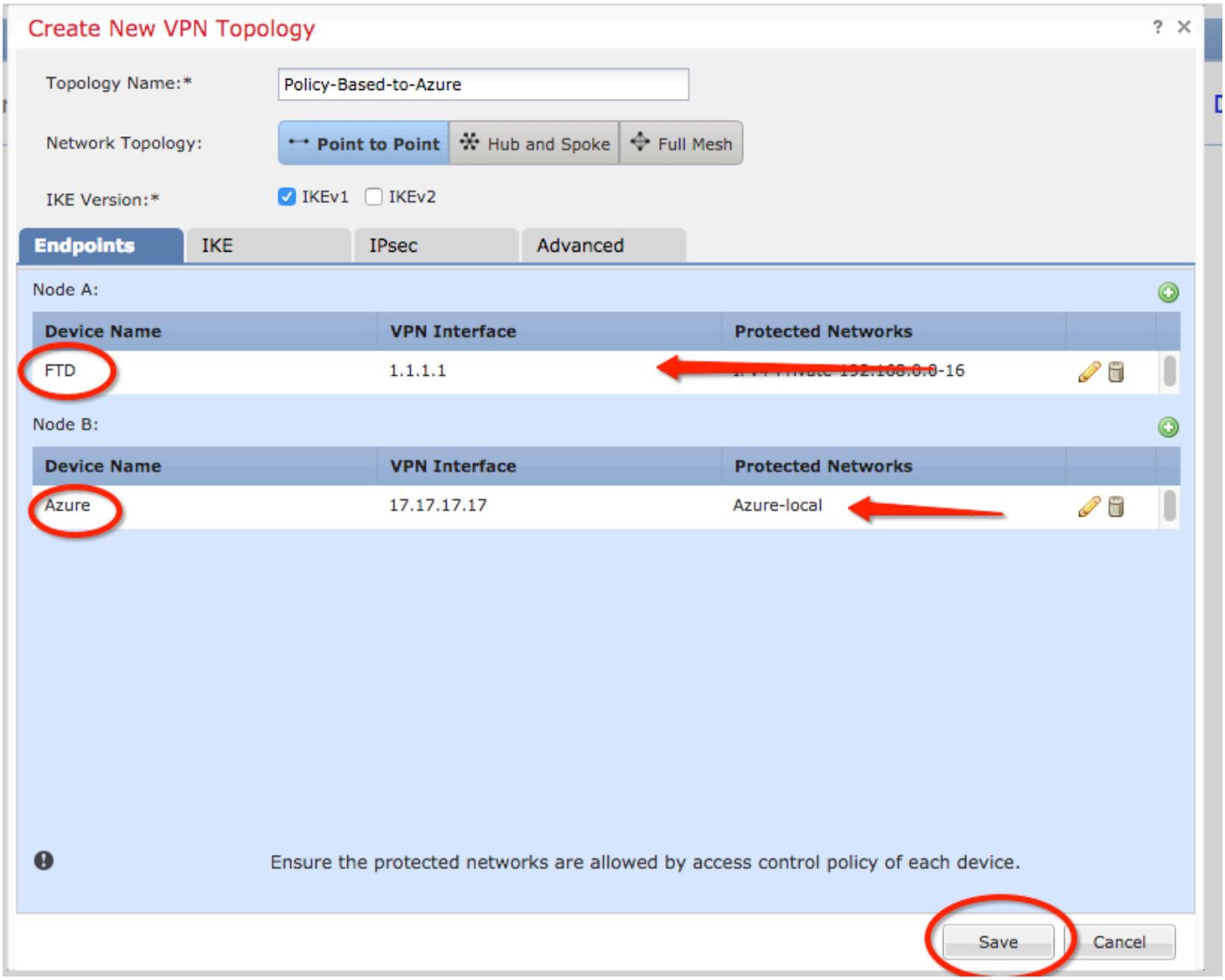
Schritt 17. Auf der **Network Objects** auf das **green plus button** neben dem **Available Networks** Text, um ein neues Objekt zu erstellen. Auf dem **New Network Object** angezeigt, geben Sie den Namen des Objekts an und wählen Sie dementsprechend Host/Bereich/Netzwerk/FQDN aus, und klicken Sie auf **Save** .



Schritt 18. Zurück zum **Network Objects** das neue Remoteobjekt dem **Selected Networks** Abschnitt und klicken Sie auf **OK** . Klicken Sie auf **Ok** auf der **Add Endpoint** angezeigt.



Schritt 19. Auf der **Create New VPN Topology** können Sie nun beide Knoten mit ihren richtigen Traffic Selektoren/geschützten Netzwerken sehen. Klicken Sie auf **Save** .



Schritt 20: Klicken Sie im FMC-Dashboard auf **Deploy** im rechten oberen Fensterbereich das FTD-Gerät auswählen und auf **Deploy** .

Schritt 21: Auf der Kommandozeile ähnelt die VPN-Konfiguration der Konfiguration für ASA-Geräte.

IKEv2-Routenbasiert mit richtlinienbasierten Datenverkehrs-Auswahlhilfen

Bei einem Site-to-Site IKEv2 VPN auf ASA mit Crypto Maps befolgen Sie diese Konfiguration. Stellen Sie sicher, dass Azure für routenbasiertes VPN konfiguriert ist, und UsePolicyBasedTrafficSelectors müssen mithilfe von PowerShell im Azure-Portal konfiguriert werden.

In diesem Dokument von Microsoft wird die Konfiguration von UsePolicyBasedTrafficSelectors in Verbindung mit dem routenbasierten Azure VPN-Modus beschrieben. Ohne Abschluss dieses Schrittes kann die ASA mit Crypto Maps die Verbindung aufgrund einer Diskrepanz in den von Azure empfangenen Datenverkehrs-Selektoren nicht herstellen.

Weitere Informationen zur ASA IKEv2 mit Konfigurationsdaten für die Crypto Map finden Sie in diesem Cisco Dokument.

Schritt 1: Aktivieren Sie IKEv2 auf der externen Schnittstelle:

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

Schritt 2: Fügen Sie eine IKEv2 Phase 1-Richtlinie hinzu.

> **Hinweis**: Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten Verschlüsselungs-, Integritäts- und Lebensdauerattribute von IKEv2 Phase 1 in Konflikt stehen. Die aufgeführten Attribute werden am besten aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Hier sind Informationen zu IKEv2-Attributen von Microsoft zu Konflikten sichtbar. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 3: Erstellen Sie eine Tunnelgruppe unter den IPsec-Attributen, und konfigurieren Sie die Peer-IP-Adresse sowie den lokalen und Remote-Tunnel-Pre-Shared Key für 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
```

Schritt 4: Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden und zu tunnelnden Datenverkehr definiert. In diesem Beispiel ist der relevante Datenverkehr der Datenverkehr aus dem Tunnel, der vom Subnetz 10.2.2.0 an 10.1.1.0 stammt. Er kann mehrere Einträge enthalten, wenn zwischen den Standorten mehrere Subnetze vorhanden sind.

In Version 8.4 und höher können Objekte oder Objektgruppen erstellt werden, die als Container für Netzwerke, Subnetze, Host-IP-Adressen oder mehrere Objekte dienen. Erstellen Sie zwei Objekte mit den lokalen und den Remote-Subnetzen, und verwenden Sie sie sowohl für die Crypto ACL- als auch für die NAT-Anweisungen.

```
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
```

Schritt 5: Fügen Sie einen IPsec-Vorschlag für IKEv2 Phase 2 hinzu. Geben Sie die Sicherheitsparameter im Konfigurationsmodus crypto IPsec ikev2 ipsec-offer an:

Protokoll-ESP-Verschlüsselung {des | 3de | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 |

aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
Protokoll-ESP-Integrität {md5 | SHA-1 | SHA-256 | SHA-384 | SHA-512 | null}

> **Hinweis**: Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten IPSec-Verschlüsselungs- und Integritätsattribute für Phase 2 in Konflikt stehen. Die aufgeführten Attribute werden am besten aus diesem öffentlich verfügbaren Microsoft-Dokument bereitgestellt. Die in Konflikt stehenden IPSec-Attributinformationen der Phase 2 von Microsoft sind hier sichtbar. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 6: Konfigurieren Sie eine Crypto Map, und wenden Sie diese auf die externe Schnittstelle an, die folgende Komponenten enthält:

- Die Peer-IP-Adresse
- Die definierte Zugriffsliste, die den Datenverkehr von Interesse enthält
- Der Vorschlag für IKEv2 Phase 2 IPSec
- IPSec-Lebensdauer in Sekunden
- Eine optionale PFS-Einstellung (Perfect Forward Secrecy), die ein neues Paar Diffie-Hellman-Schlüssel erstellt, die zum Schutz der Daten verwendet werden (beide Seiten müssen PFS-fähig sein, bevor Phase 2 gestartet wird)

Microsoft hat Informationen veröffentlicht, die in Bezug auf die von Azure verwendeten IPSec-Lebensdauer und PFS-Attribute der Phase 2 in Konflikt stehen.

Die aufgelisteten Attribute enthalten die besten Dieses öffentlich verfügbare Microsoft-Dokument.

Die in Konflikt stehenden IPSec-Attributinformationen der Phase 2 von Microsoft sind hier sichtbar. Weitere Informationen erhalten Sie vom Microsoft Azure-Support.

```
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
```

Schritt 8: Stellen Sie sicher, dass der VPN-Datenverkehr keiner anderen NAT-Regel unterliegt. Erstellen Sie eine NAT-Ausnahmeregelung:

```
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
```

> **Hinweis**: Wenn mehrere Subnetze verwendet werden, müssen Sie Objektgruppen mit allen Quell- und Zielsubnetzen erstellen und diese in der NAT-Regel verwenden.

```
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
```

Überprüfung

Nachdem Sie die Konfiguration auf ASA und Azure-Gateway abgeschlossen haben, initiiert Azure den VPN-Tunnel. Mit den folgenden Befehlen können Sie überprüfen, ob der Tunnel korrekt erstellt wurde:

Phase 1

Überprüfen Sie, ob die Security Association (SA) für Phase 1 erstellt wurde:

IKEv2

Als Nächstes wird eine IKEv2 SA angezeigt, die von der lokalen externen Schnittstelle IP 192.168.1.2 auf dem UDP-Port 500 zur Remote-Ziel-IP 192.168.2.2 erstellt wurde. Darüber hinaus gibt es eine gültige untergeordnete SA, die für den Fluss des verschlüsselten Datenverkehrs erstellt wurde.

```
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 wird eine IKEv1 SA mit ASA als Initiator für Peer-IP 192.168.2.2 mit einer Restlebensdauer von 86388 Sekunden angezeigt.

```
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

Überprüfen Sie, ob die IPSec-Sicherheitszuordnung für Phase 2 mit **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 Pakete werden fehlerfrei gesendet und vier über die IPSec SA empfangen. Eine eingehende

SA mit SPI 0x9B60EDC5 und eine ausgehende SA mit SPI 0x8E7A2E12 werden erwartungsgemäß installiert.

Sie können auch überprüfen, ob die Daten über den Tunnel übertragen werden, indem Sie die **vpn-sessiondb l2l** Einträge:

```
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
```

Bytes Tx: und Bytes Rx: zeigt Zähler für gesendete und empfangene Daten über die IPSec-SA an.

Fehlerbehebung

Schritt 1: Überprüfen Sie, ob der Datenverkehr für das VPN von der ASA an der internen Schnittstelle empfangen wird, die für das private Azure-Netzwerk bestimmt ist. Zum Testen können Sie einen kontinuierlichen Ping von einem internen Client konfigurieren und eine Paketerfassung auf ASA konfigurieren, um zu überprüfen, ob dieser empfangen wird:

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
```

Wenn Antwortdatenverkehr von Azure erkannt wird, wird das VPN ordnungsgemäß erstellt und sendet/empfängt Datenverkehr.

Wenn kein Quelldatenverkehr vorhanden ist, überprüfen Sie, ob der Absender die richtige Weiterleitung an die ASA ist.

Wenn Quelldatenverkehr erkannt wird, aber kein Antwortdatenverkehr von Azure vorhanden ist, fahren Sie mit der Überprüfung der Ursache fort.

Schritt 2: Vergewissern Sie sich, dass der über die ASA-interne Schnittstelle empfangene Datenverkehr von der ASA ordnungsgemäß verarbeitet und in das VPN geroutet wird:

So simulieren Sie eine ICMP-Echoanfrage:

packet-tracer input [Name der internen Schnittstelle] icmp [inside-host-ip] 8 0 [azure-host-ip] detail

Die vollständigen Richtlinien zur Packet-Tracer-Verwendung finden Sie hier: 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
```

Beachten Sie, dass die NAT den Datenverkehr ausnimmt (keine Übersetzung wird wirksam). Vergewissern Sie sich, dass für den VPN-Datenverkehr keine NAT-Übersetzung durchgeführt wird.

Überprüfen Sie außerdem **output-interface** richtig: Dies muss entweder die physische Schnittstelle sein, auf die die Crypto Map angewendet wird, oder die virtuelle Tunnelschnittstelle.

Stellen Sie sicher, dass keine Zugriffslisten-Drops erkannt werden.

Wenn die VPN-Phase **ENCRYPT: ALLOW** , der Tunnel ist bereits gebaut und Sie können sehen, IPSec SA mit encaps installiert.

Schritt 2.1. Falls **ENCRYPT: ALLOW** in Packet-Tracer angezeigt.

Überprüfen Sie, ob IPsec SA installiert ist, und verschlüsseln Sie den Datenverkehr mit **show crypto ipsec sa** .

Sie können eine Erfassung an der externen Schnittstelle durchführen, um sicherzustellen, dass verschlüsselte Pakete von ASA gesendet und verschlüsselte Antworten von Azure empfangen werden.

Schritt 2.2. Falls **ENCRYPT:DROP** in Packet-Tracer angezeigt.

Der VPN-Tunnel ist noch nicht eingerichtet, wird aber verhandelt. Dies ist ein erwarteter Zustand, wenn Sie den Tunnel zum ersten Mal hochfahren. Führen Sie Debugs aus, um den Tunnelaushandlungsprozess anzuzeigen und festzustellen, wo und ob ein Fehler auftritt.

Stellen Sie zunächst sicher, dass die richtige Version von IKE ausgelöst wird und der IKE-Prozess keine relevanten Fehler aufweist:

```
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.
```

Wenn bei der Initiierung von VPN-Datenverkehr keine ike-common-Debug-Ausgabe erkannt wird, bedeutet dies, dass Datenverkehr verworfen wird, bevor er den Crypto-Prozess erreicht, oder crypto ikev1/ikev2 ist auf dem Gerät nicht aktiviert. Überprüfen Sie die Verschlüsselungskonfiguration und Paketverluste.

Wenn typische Debugs zeigen, dass der Kryptografieprozess ausgelöst wird, debuggen Sie die von IKE konfigurierte Version, um Tunnelaushandlungsmeldungen anzuzeigen und festzustellen, wo der Fehler beim Tunnelaufbau mit Azure auftritt.

IKEv1

Vollständige ikev1 Debug Prozedur und Analyse finden Sie hier.

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

IKEv2

Vollständige ikev2 Debug Prozedur und Analyse finden Sie hier.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.