Configurare una VPN basata su criteri e su route da ASA e FTD a Microsoft Azure

Sommario

Introduzione

In questo documento vengono descritti i concetti e la configurazione di una VPN tra Cisco ASA e Cisco Secure Firewall e i servizi cloud di Microsoft Azure.

Concetti

Dominio di crittografia VPN

L'intervallo di indirizzi IP IPSec consente di partecipare al tunnel VPN.Il dominio di crittografia viene definito utilizzando un selettore di traffico locale e uno remoto per specificare gli intervalli di subnet locali e remote acquisiti e crittografati da IPSec. Per definire i domini di crittografia VPN, è possibile procedere in due modi: selettori di traffico basati su route o criteri.

Basato su route:
Il dominio di crittografia è impostato in modo da consentire il traffico in entrata nel tunnel IPSec. I selettori di traffico locale e remoto di IPSec sono impostati su 0.0.0.0. Ciò significa che il traffico instradato nel tunnel IPSec viene crittografato indipendentemente dalla subnet di origine/destinazione.

Cisco Adaptive Security Appliance (ASA) supporta VPN basate su routing con uso di VTI (Virtual Tunnel Interfaces) nelle versioni 9.8 e successive.

Cisco Secure Firewall o Firepower Threat Defense (FTD) gestiti da FMC (Firepower Management Center) supportano VPN basate su route con l'utilizzo di VTI nelle versioni 6.7 e successive.

Basato su regole:

Il dominio di crittografia è impostato per crittografare solo intervalli IP specifici sia per l'origine che per la destinazione. I selettori di traffico locale e remoto basati su criteri identificano il traffico da crittografare tramite IPSec.

ASA supporta VPN basate su criteri con mappe crittografiche nella versione 8.2 e successive.

Microsoft Azure supporta selettori di traffico basati su route, criteri o route con simulatori basati su criteri. Azure attualmente limita la versione di Internet Key Exchange (IKE) che è possibile configurare in base al metodo VPN selezionato. Richieste basate su route IKEv2 e richieste basate su criteri IKEv1. Ciò significa che se si utilizza IKEv2, è necessario selezionare le route basate in Azure e l'ASA deve utilizzare una VTI, ma se l'ASA supporta solo mappe crittografiche a causa della versione del codice, è necessario configurare Azure per le route basate su selettori di traffico basati su criteri. Questa operazione viene eseguita nel portale di Azure tramite la distribuzione di script PowerShell per implementare un'opzione che Microsoft chiama UsePolicyBasedTrafficSelectors come spiegato di seguito: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps.

Per riepilogare i dati dalla prospettiva di configurazione ASA e FTD:

- Per ASA/FTD configurato con una mappa crittografica, Azure deve essere configurato per VPN basata su criteri o basata su route con UsePolicyBasedTrafficSelectors.
- Per ASA configurata con VTI, Azure deve essere configurato per VPN basata su route.
- Per FTD, ulteriori informazioni su come configurare le VTI sono disponibili qui; 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

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Per la VPN basata su route IKEv2 che utilizza VTI su ASA: Codice ASA versione 9.8(1) o successive. Azure deve essere configurato per la VPN basata su route.
- Per la VPN basata su criteri IKEv1 che utilizza la mappa crittografica su ASA e FTD: Codice ASA versione 8.2 o successiva e FTD 6.2.0 o successiva. Azure deve essere configurato per la VPN basata su criteri.
- Per la VPN basata su route IKEv2 che utilizza la mappa crittografica sull'appliance ASA con selettori del traffico basati su policy: Il codice ASA versione 8.2 o successive è configurato con una mappa crittografica. Azure deve essere configurato per la VPN basata su route con UsePolicyBasedTrafficSelectors.
- Conoscenza del CCP per la gestione e la configurazione del FTD.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Completare la procedura di configurazione. Scegliere se configurare IKEv1, route IKEv2 basata su VTI o route IKEv2 basata su selettori del traffico basati su policy (mappa crittografica su ASA).

Configurazione IKEv1 su ASA

Per una VPN IKEv1 da sito a sito da ASA ad Azure, seguire la successiva configurazione ASA. Verificare di configurare un tunnel basato su criteri nel portale di Azure. Per questo esempio, le mappe crittografiche vengono usate sull'appliance ASA.

Fare riferimento a questo documento Cisco per informazioni complete sulla configurazione di IKEv1 sull'appliance ASA.

Passaggio 1. Abilitare IKEv1 sull'interfaccia esterna.

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

Passaggio 2. Creare un criterio IKEv1 che definisca gli algoritmi o i metodi da utilizzare per l'hash, l'autenticazione, il gruppo Diffie-Hellman, la durata e la crittografia.

> **Nota:** Gli attributi IKEv1 della fase 1 elencati possono essere ricavati nel modo migliore da questo documento Microsoft pubblicamente disponibile. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

```
Cisco-ASA(config)#crypto ikev1 policy 1
Cisco-ASA(config-ikev1-policy)#authentication pre-share
Cisco-ASA(config-ikev1-policy)#encryption aes
Cisco-ASA(config-ikev1-policy)#hash sha
Cisco-ASA(config-ikev1-policy)#group 2
Cisco-ASA(config-ikev1-policy)#lifetime 28800
```

Passaggio 3. Creare un gruppo di tunnel con gli attributi IPsec e configurare l'indirizzo IP del peer e la chiave già condivisa del tunnel.

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

Passaggio 4. Creare un elenco degli accessi che definisca il traffico da crittografare e tunneling. Nell'esempio, il traffico di interesse è il traffico proveniente dal tunnel che ha origine dalla subnet 10.2.2.0 a 10.1.1.0. Può contenere più voci se tra i siti sono coinvolte più subnet.

Nelle versioni 8.4 e successive è possibile creare oggetti o gruppi di oggetti che fungono da contenitori per le reti, le subnet, gli indirizzi IP host o più oggetti. Creare due oggetti che hanno le subnet locali e remote e usarli sia per l'istruzione Crypto Access Control List (ACL) che per l'istruzione Network Address Translation (NAT).

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

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

Passaggio 5. Configurare il set di trasformazioni (TS), che deve includere la parola chiave**IKEv1**. È necessario creare un servizio di terminal identico anche sull'estremità remota.

> **Nota:** Gli attributi IKEv1 della fase 2 elencati possono essere ricavati nel modo migliore da questo documento Microsoft pubblicamente disponibile. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 6. Configurare la mappa crittografica e applicarla all'interfaccia esterna che ha i seguenti componenti:
·L'indirizzo IP del peer
·Elenco degli accessi definito contenente il traffico di interesse
·TS
·La configurazione non imposta PFS (Perfect Forward Secrecy) perché nella documentazione di Azure disponibile pubblicamente viene indicato che PFS è disabilitato per IKEv1 in Azure. Tramite questa configurazione è possibile attivare un'impostazione PFS facoltativa, che crea una nuova coppia di chiavi Diffie-Hellman utilizzate per proteggere i dati (entrambi i lati devono essere abilitati per PFS prima dell'avvio della fase 2): **crypto map outside_map 20 set pfs** .
· Le durate IPSec per la fase 2 sono basate sulla documentazione di Azure disponibile pubblicamente. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev1 transform-set myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 3600
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
102400000
Cisco-ASA(config)#crypto map outside_map interface outside
```

Passaggio 7. Verificare che il traffico VPN non sia soggetto ad altre regole NAT. Creare una regola di esenzione NAT:

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

> **Nota**: quando si utilizzano più subnet, è necessario creare gruppi di oggetti con tutte le subnet di origine e di destinazione e utilizzarli nella regola NAT.

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

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

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

Basato su route IKEv2 con VTI su codice ASA 9.8 (1) o versioni successive

Per una VPN basata su route IKEv2 da sito a sito su codice ASA, seguire questa configurazione. Verificare che Azure sia configurato per la VPN basata su route e non configurare UsePolicyBasedTrafficSelectors nel portale di Azure. Sull'appliance ASA è configurata una VTI.

Fare riferimento a questo documento Cisco per informazioni complete sulla configurazione della VTI dell'ASA.

Passaggio 1. Abilitare IKEv2 sull'interfaccia esterna:

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

Passaggio 2. Aggiungere un criterio IKEv2 fase 1.

> **Nota**: Microsoft ha pubblicato informazioni in conflitto con gli attributi di crittografia IKEv2 fase 1, integrità e durata utilizzati da Azure. Gli attributi elencati vengono forniti nel modo più efficace da questo documento Microsoft pubblicamente disponibile. In questa sezione sono visibili le informazioni che creano conflitti tra gli attributi IKEv2 di Microsoft. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 3. Aggiungere una proposta IPsec IKEv2 fase 2. Specificare i parametri di sicurezza in IPsec di crittografia **ikev2 ipsec-proposal** modalità di configurazione:

protocollo esp crittografia {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocollo integrità esp {md5 | sha-1 | csa-256 | csa-384 | csa-512 | null}

> **Nota:** Microsoft ha pubblicato informazioni in conflitto con gli attributi di crittografia IPSec di fase 2 specifici utilizzati da Azure. Gli attributi elencati vengono forniti nel modo più efficace da questo documento Microsoft pubblicamente disponibile. In questa sezione sono visibili le informazioni che creano conflitti tra gli attributi IPSec della fase 2 e quelli di Microsoft. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 4. Aggiungere un profilo IPSec che specifichi:

- Proposta IPSec fase 2 ikev2 configurata in precedenza
- Durata IPSec fase 2 (facoltativa) in secondi e/o kilobyte
- Gruppo PFS (facoltativo)

> **Nota:** Microsoft ha pubblicato informazioni in conflitto con gli attributi IPSec specifici della fase 2 e PFS utilizzati da Azure. Gli attributi elencati vengono forniti nel modo più efficace da questo documento Microsoft pubblicamente disponibile. In questa sezione sono visibili le informazioni che creano conflitti tra gli attributi IPSec della fase 2 e quelli di Microsoft. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 5. Creare un gruppo di tunnel con gli attributi IPsec e configurare l'indirizzo IP del peer e la chiave precondivisa del tunnel locale e remoto 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
```

Passaggio 6. Creare una VTI che specifichi:

- Nuovo numero di interfaccia del tunnel: interface tunnel [numero]
- Nuovo nome interfaccia tunnel: nameif [nome]
- Indirizzo IP inesistente nell'interfaccia del tunnel: ip address [ip-address] [mask]
- Interfaccia di origine del tunnel in cui la VPN termina localmente: tunnel source interface [int-name]
- Indirizzo IP del gateway di Azure: destinazione del tunnel [Azure Public IP]

- Modalità IPv4 IPSec: modalità tunnel ipsec ipv4
- Profilo IPSec da utilizzare per la VTI: profilo ipsec di protezione del tunnel [nome-profilo]

```
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
```

Passaggio 7. Creare un percorso statico per indirizzare il traffico nel tunnel. Per aggiungere una route statica, immettere questo comando:
route if_name dest_ip mask gateway_ip [distance]

OSPF (Open Shortest Path First) **dest_ip** e **mask** è l'indirizzo IP per la rete di destinazione nel cloud di Azure, ad esempio 10.0.0.0/24. Il gateway_ip deve essere qualsiasi indirizzo IP (esistente o inesistente) nella subnet dell'interfaccia del tunnel, ad esempio 169.254.0.2. Lo scopo di questo gateway_ip è indirizzare il traffico nell'interfaccia del tunnel, ma il gateway IP specifico non è importante.

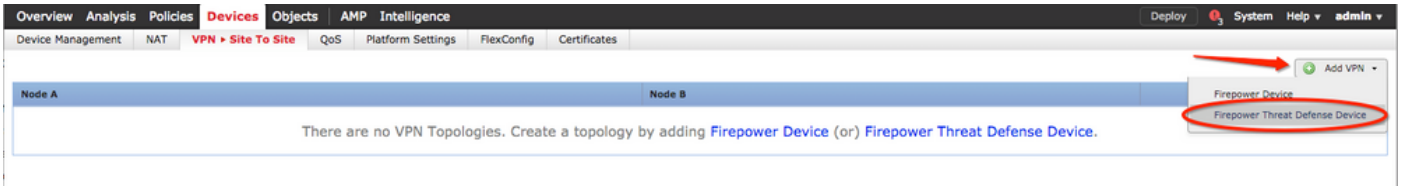
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

Configurazione IKEv1 su FTD

Per una VPN IKEv1 da sito a sito da FTD ad Azure, è necessario aver registrato in precedenza il dispositivo FTD in FMC.

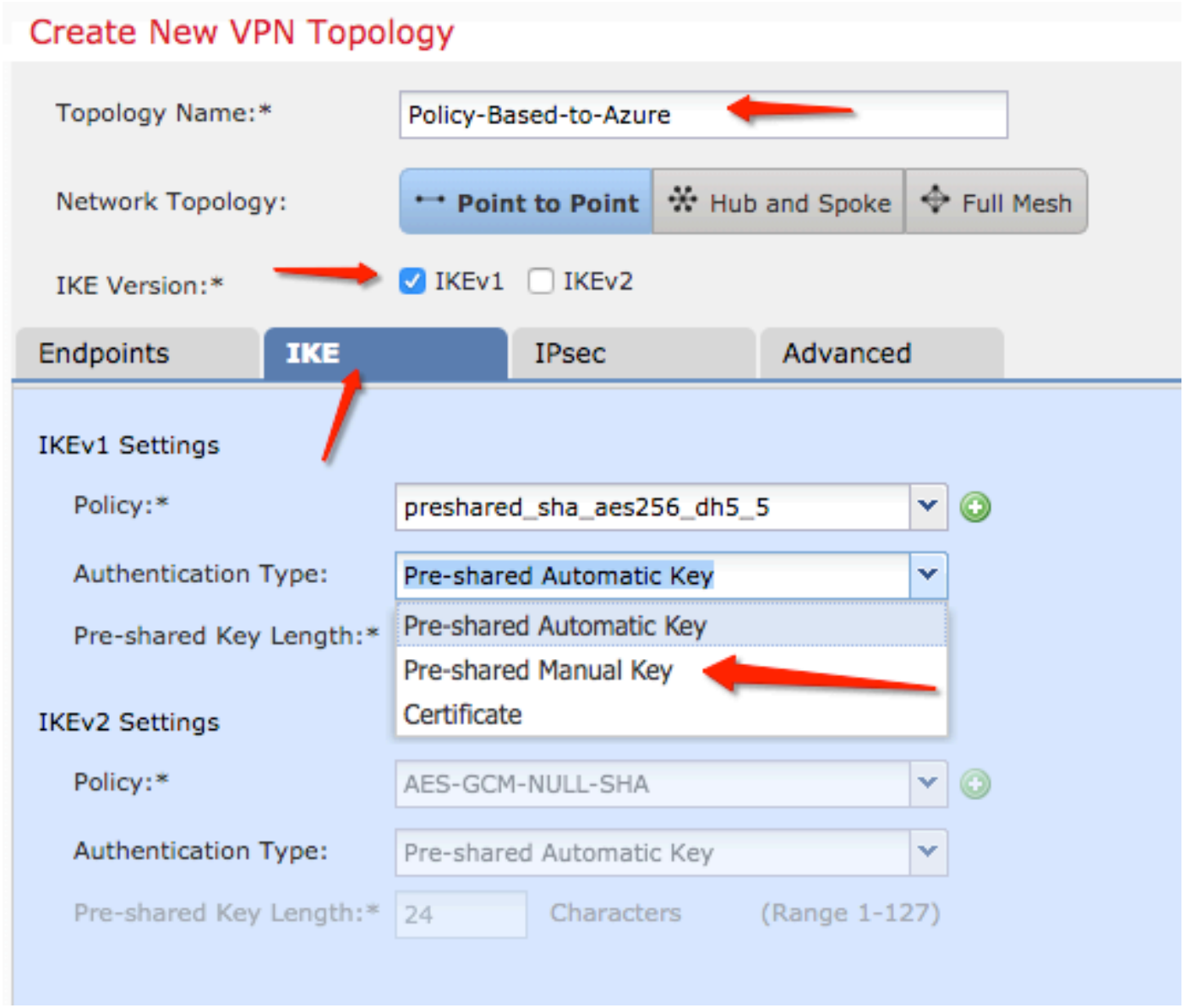
Passaggio 1. Creare un criterio da sito a sito. Passare alla **FMC dashboard > Devices > VPN > Site to Site**.

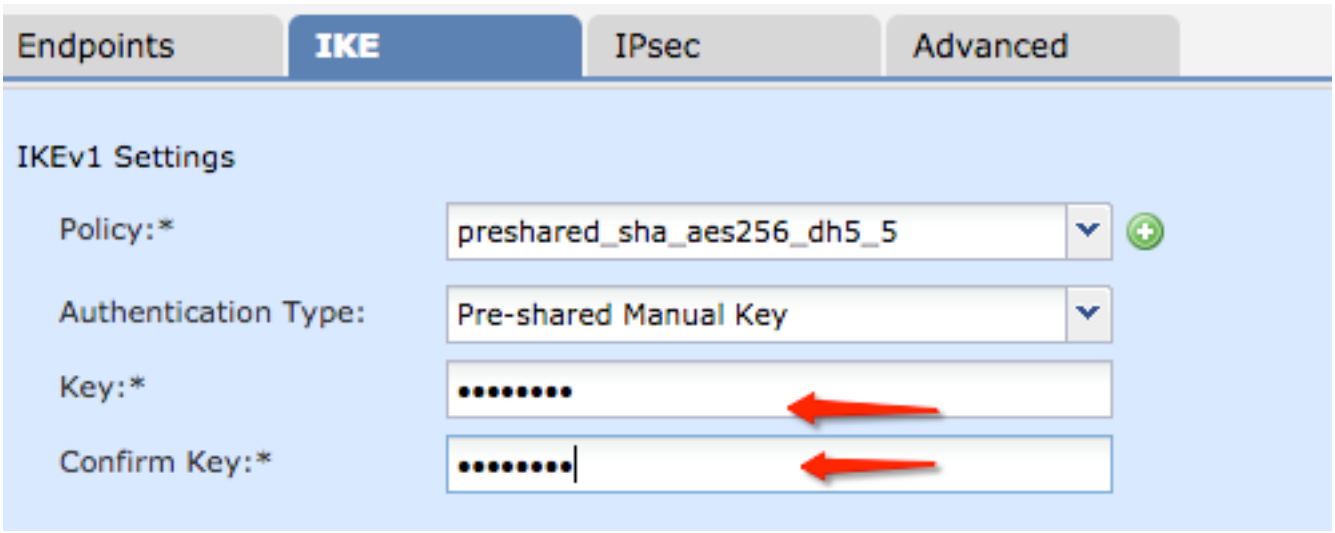
Passaggio 2. Creare un nuovo criterio. Fare clic su **Add VPN** e scegliere **Firepower Threat Defense device** .



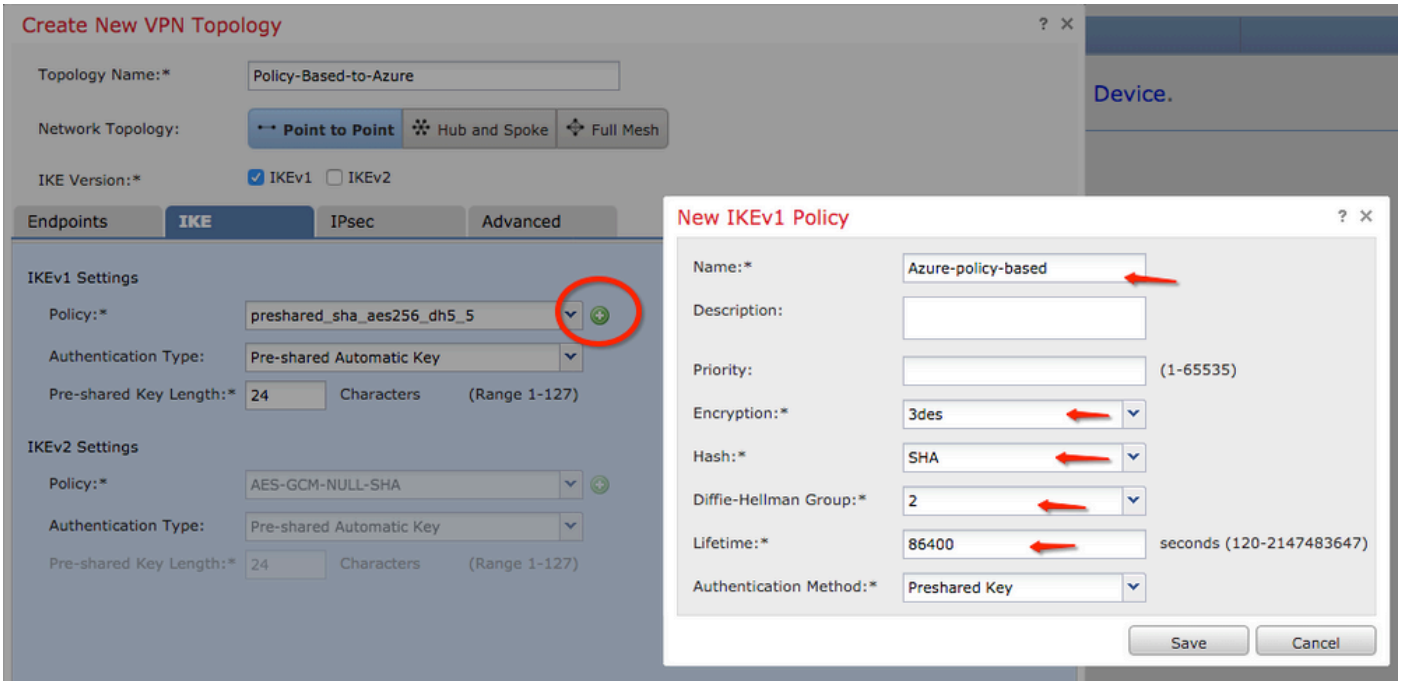
Passaggio 3. Nella **Create new VPN Topology** , specificare **Topology Name**, controllare la **IKEV1** e fare clic sul pulsante **IKE** . Ai fini di questo esempio, le chiavi già condivise vengono utilizzate come metodo di autenticazione.

Fare clic su **Authentication Type** e scegliere **Pre-shared manual key** . Digitare la chiave pre-condivisa manuale sul **Key** e**Confirm Key** campi di testo.

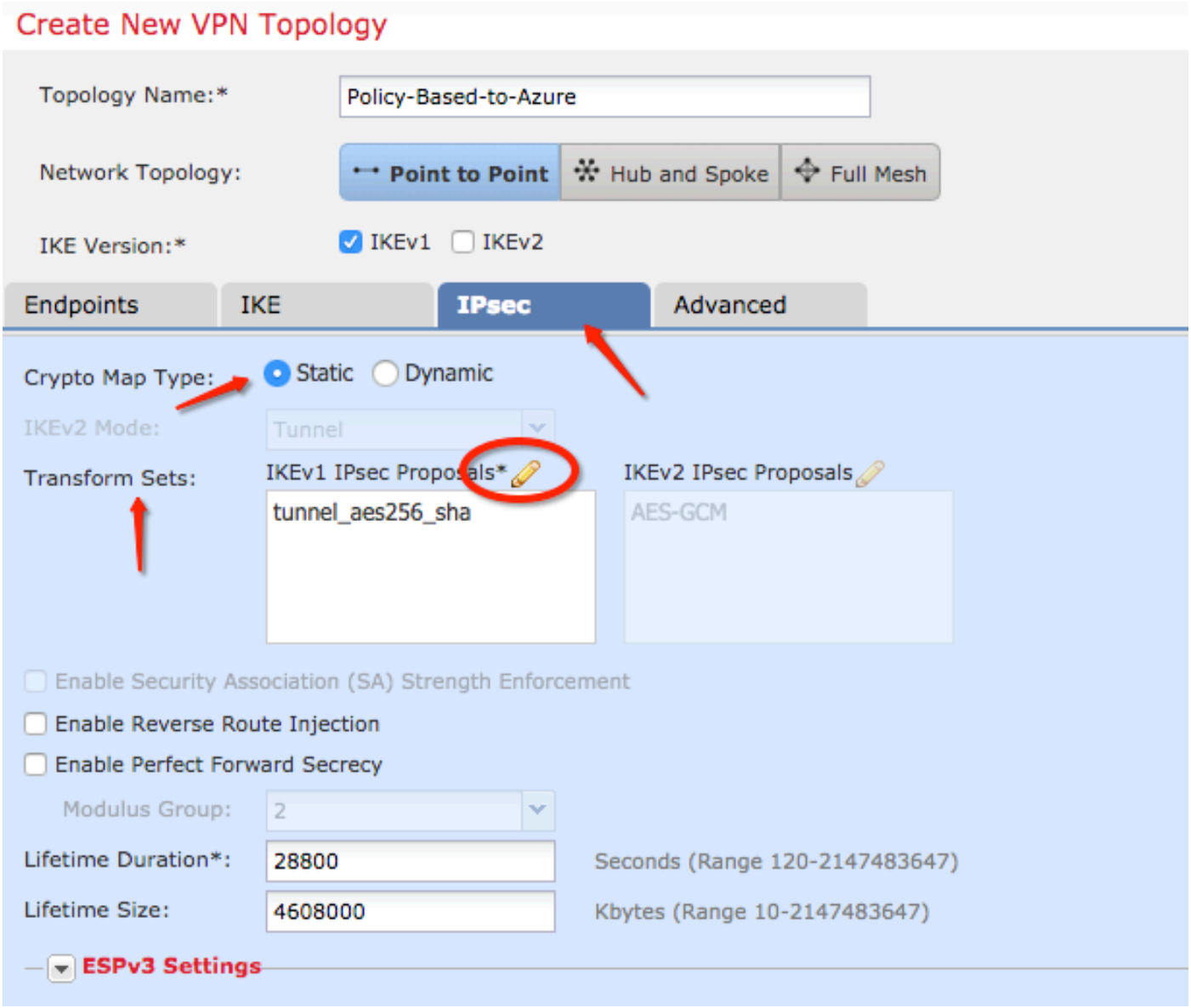




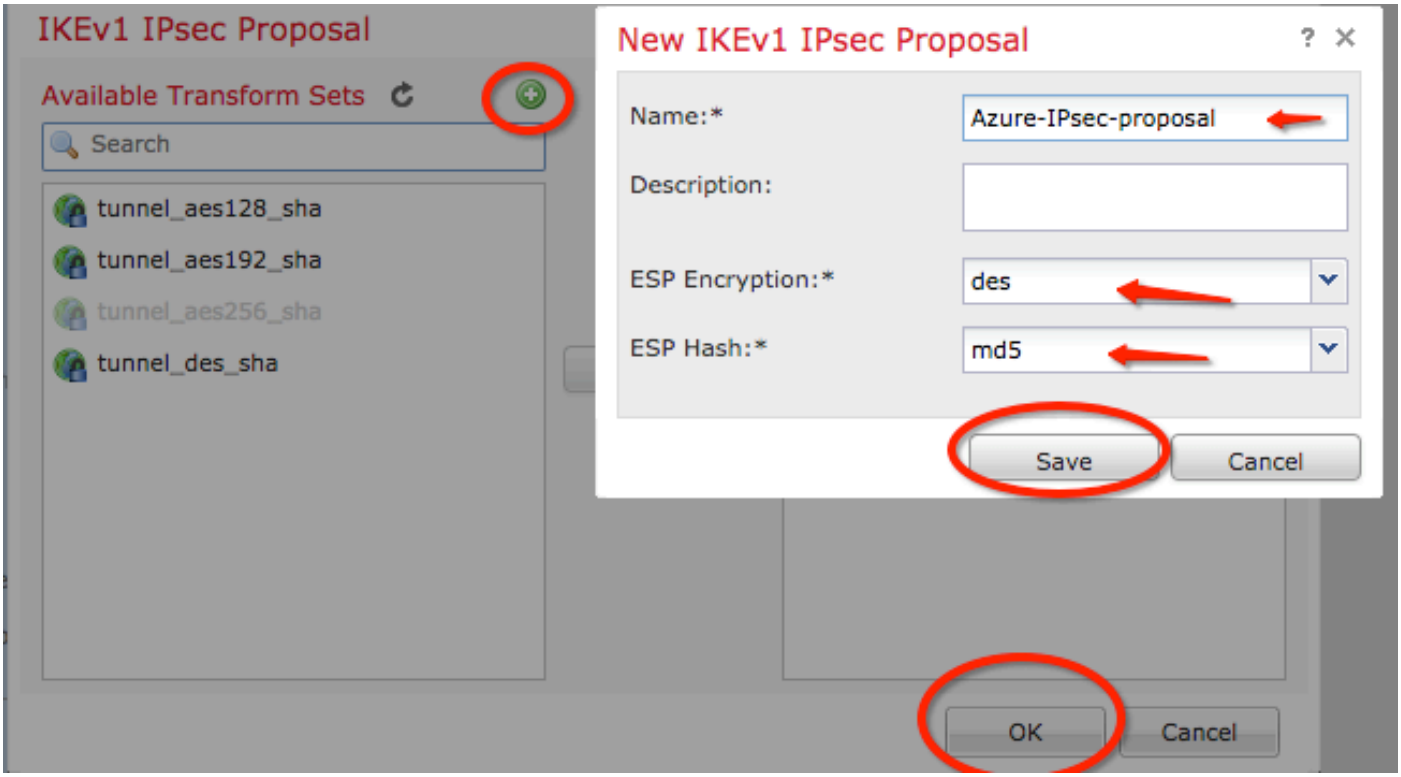
Passaggio 4. Configurare il criterio ISAKMP o i parametri della fase 1 con la creazione di un nuovo criterio. Nella stessa finestra, fare clic sul pulsante **green plus button** per aggiungere un nuovo criterio ISAKMP. Specificare il nome del criterio e scegliere i valori desiderati per Crittografia, Hash, Gruppo Diffie-Hellman, Durata e Metodo di autenticazione, quindi fare clic su **Save** .



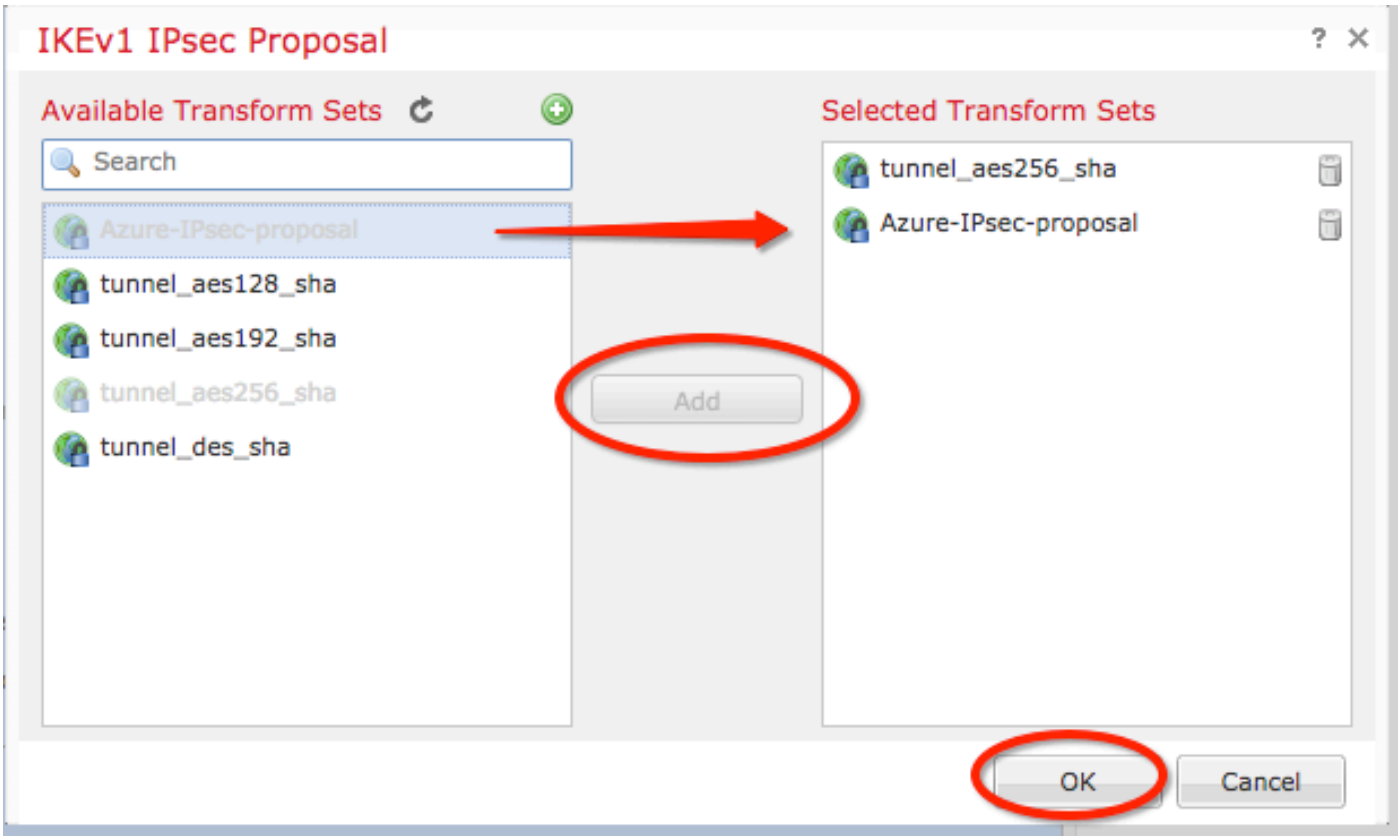
Passaggio 5. Configurare il criterio IPSec o i parametri della fase 2. Passare alla **IPsec** , scegliere **Static** sul **Crypto Map Type** casella di controllo. Fare clic sul pulsante **edit pencil** dall'elenco **IKEV1 IPsec Proposals** al **Transform Sets** opzione.



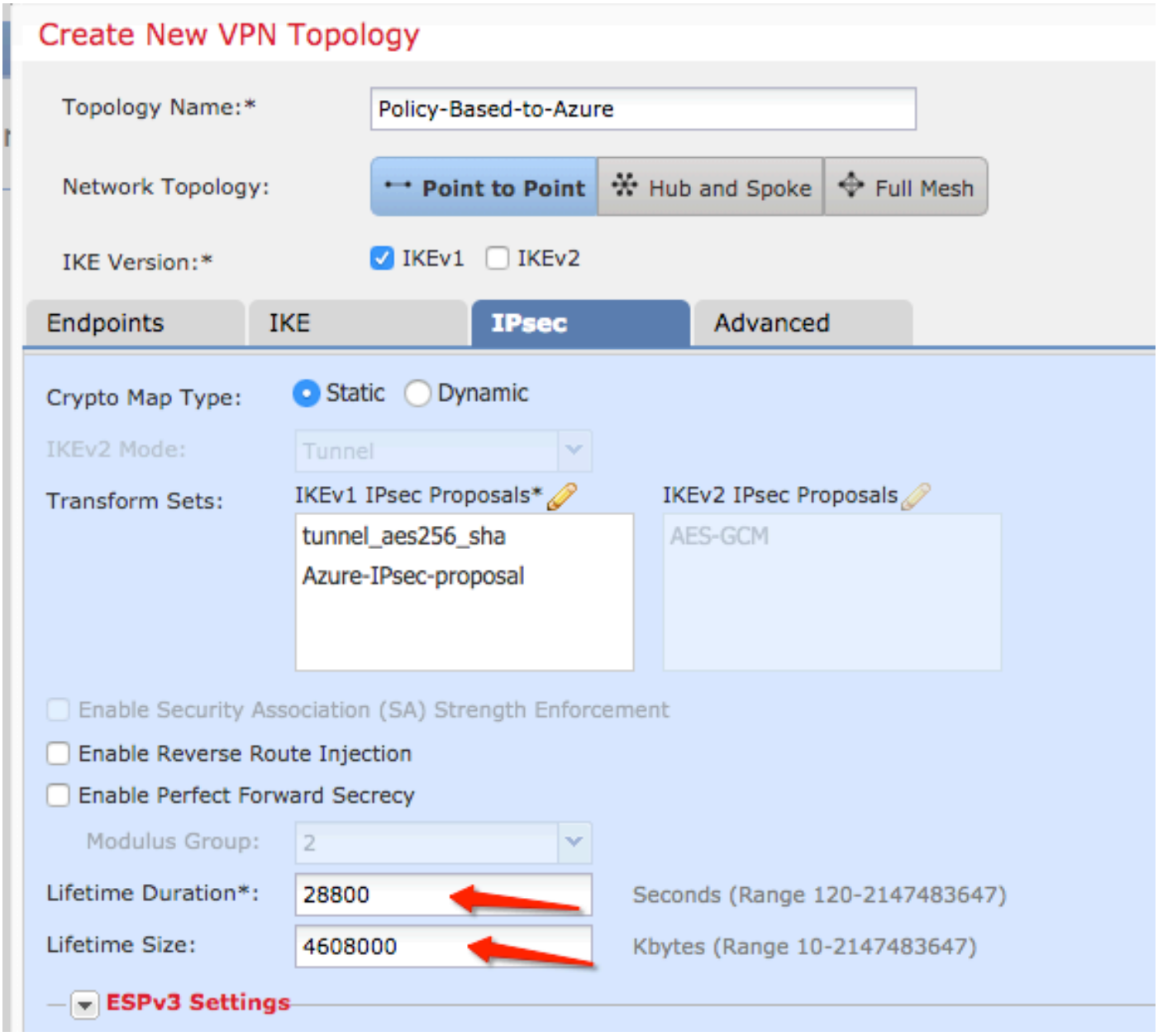
Passaggio 6. Creare una nuova proposta IPSec. Nella scheda **IKEv1 IPSec Proposal** fare clic sul pulsante **green plus button** per aggiungerne uno nuovo. Specificare il nome del criterio e i relativi parametri desiderati per gli algoritmi di crittografia ESP ed ESP Hash e fare clic su **Save** .



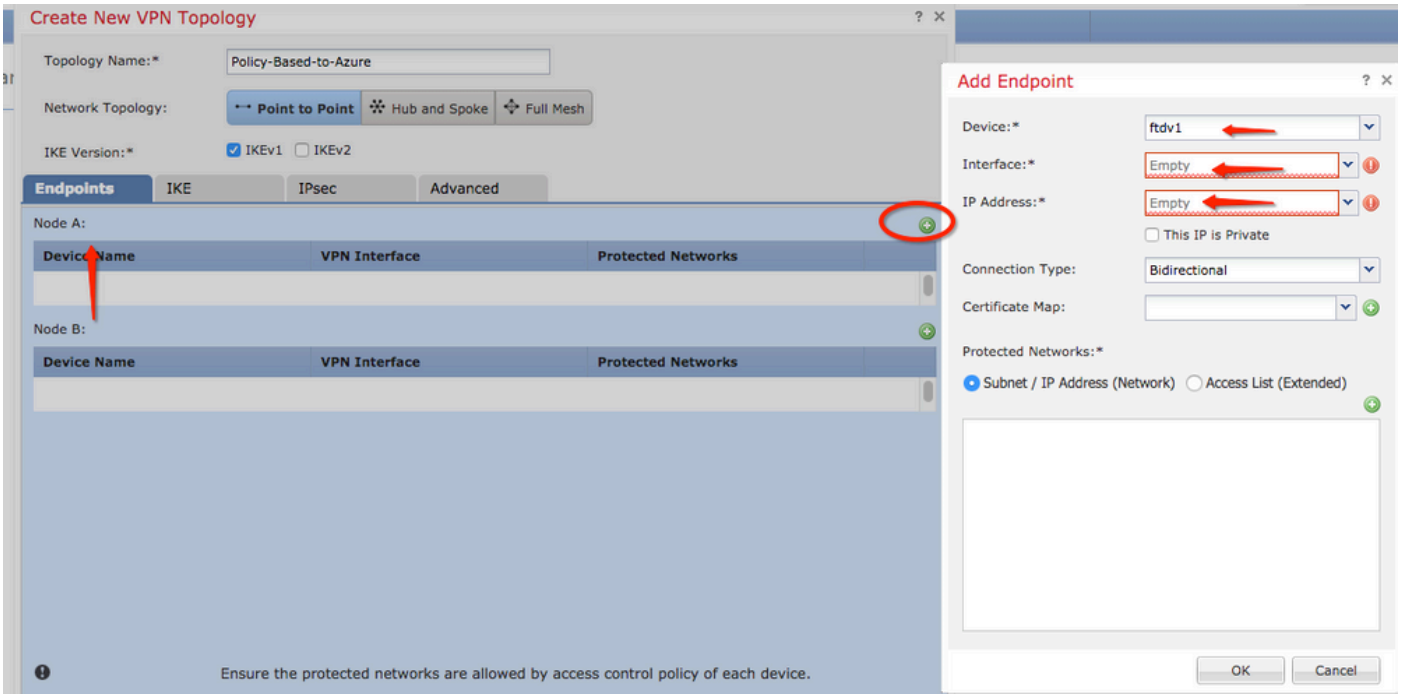
Passaggio 7. Nella scheda **IKEV1 IPsec Proposal** aggiungere il nuovo criterio IPSec alla finestra di dialogo **Selected Transform Sets** e fare clic su **OK** .



Passaggio 8. Tornare alla **IPSec** configurare la durata e le dimensioni desiderate.



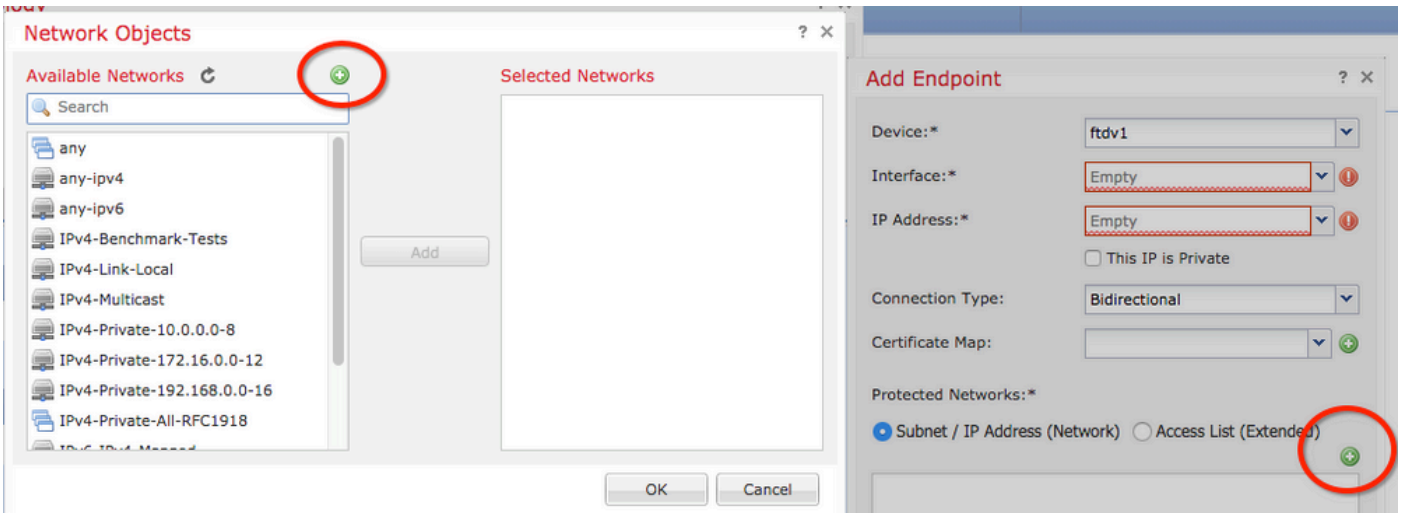
Passaggio 9. Selezionare il dominio di crittografia/selettori traffico/reti protette. Passare alla **Endpoints** . Nella scheda **Node A** fare clic sul pulsante **green plus button** per aggiungerne uno nuovo. In questo esempio il nodo A viene usato come subnet locali dell'FTD.



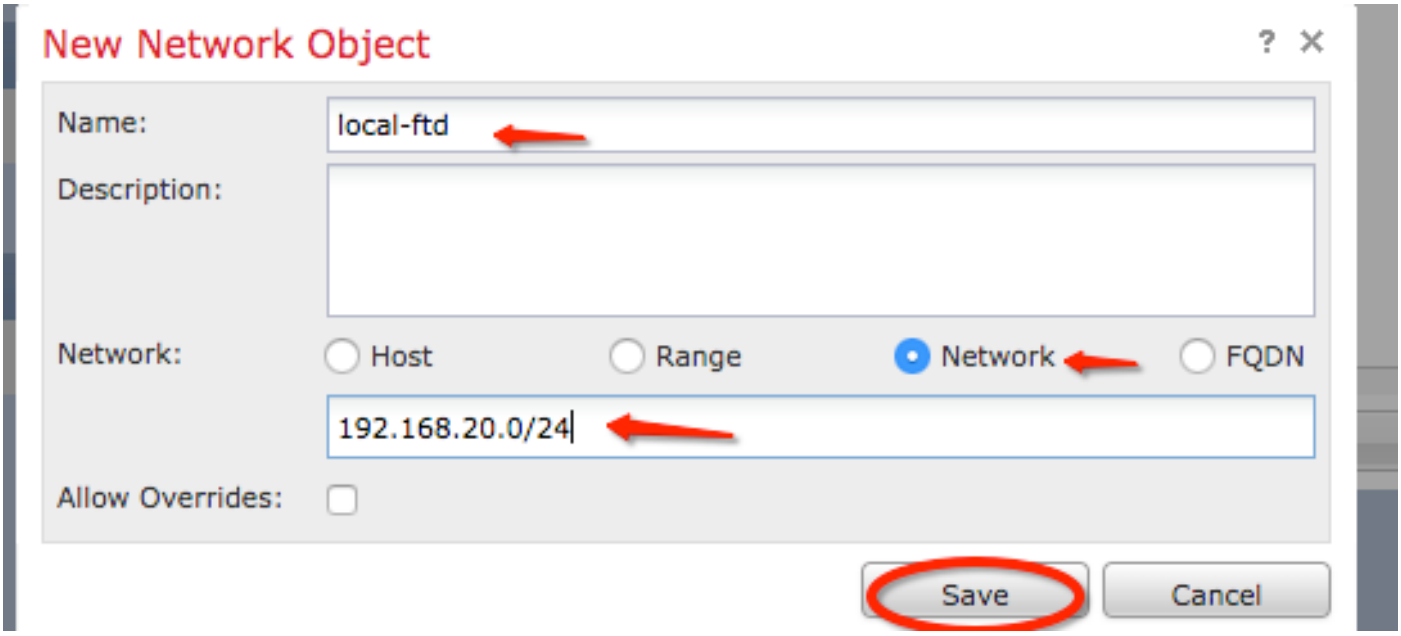
Passaggio 10. Nella **Add Endpoint** , specificare l'FTD da utilizzare **Device** insieme all'interfaccia fisica e all'indirizzo IP da utilizzare.

Passaggio 11. Per specificare il selettore di traffico locale, passare alla **Protected Networks** e fare clic sul pulsante **green plus button** per creare un nuovo oggetto.

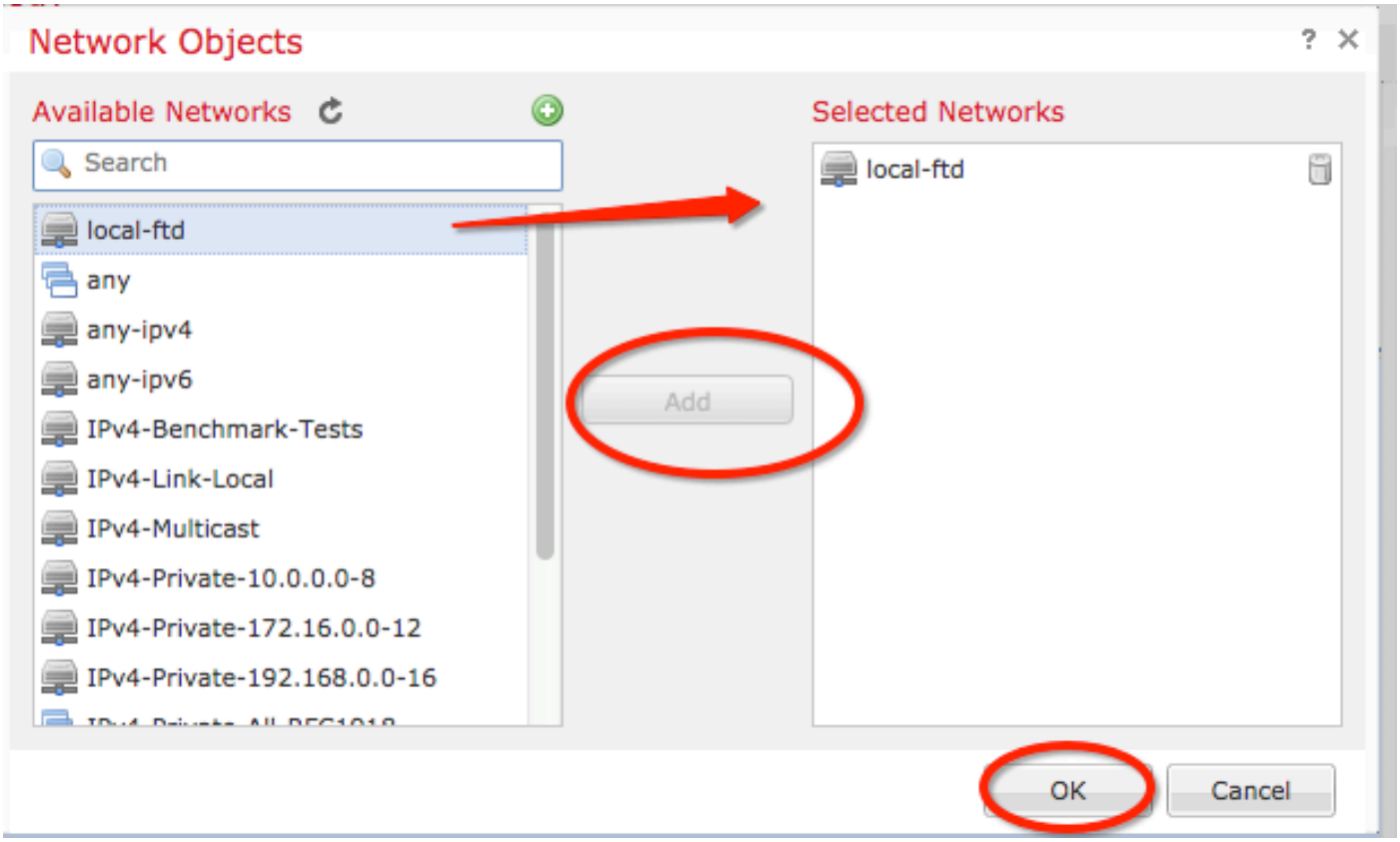
Passaggio 12. Nella **Network Objects** fare clic sul pulsante **green plus button** accanto al **Available Networks** testo per creare un nuovo oggetto selettore traffico locale.



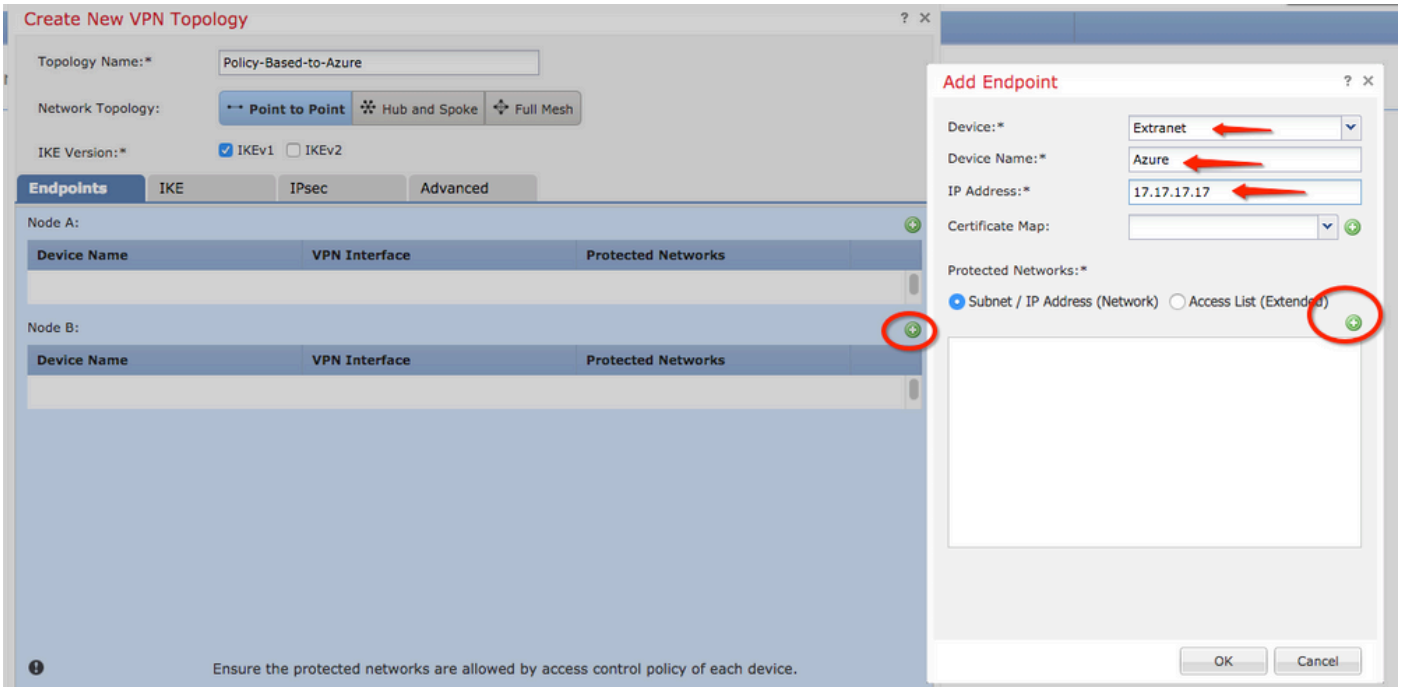
Passaggio 13. Nella **New Network Object** specificare il nome dell'oggetto e scegliere di conseguenza host/rete/intervallo/FQDN. Quindi fai clic su **Save** .



Passaggio 14. Aggiungere l'oggetto al **Selected Networks** sezione sulla **Network Objects** e fare clic su **OK** . Clic **OK** sul **Add Endpoint** finestra.

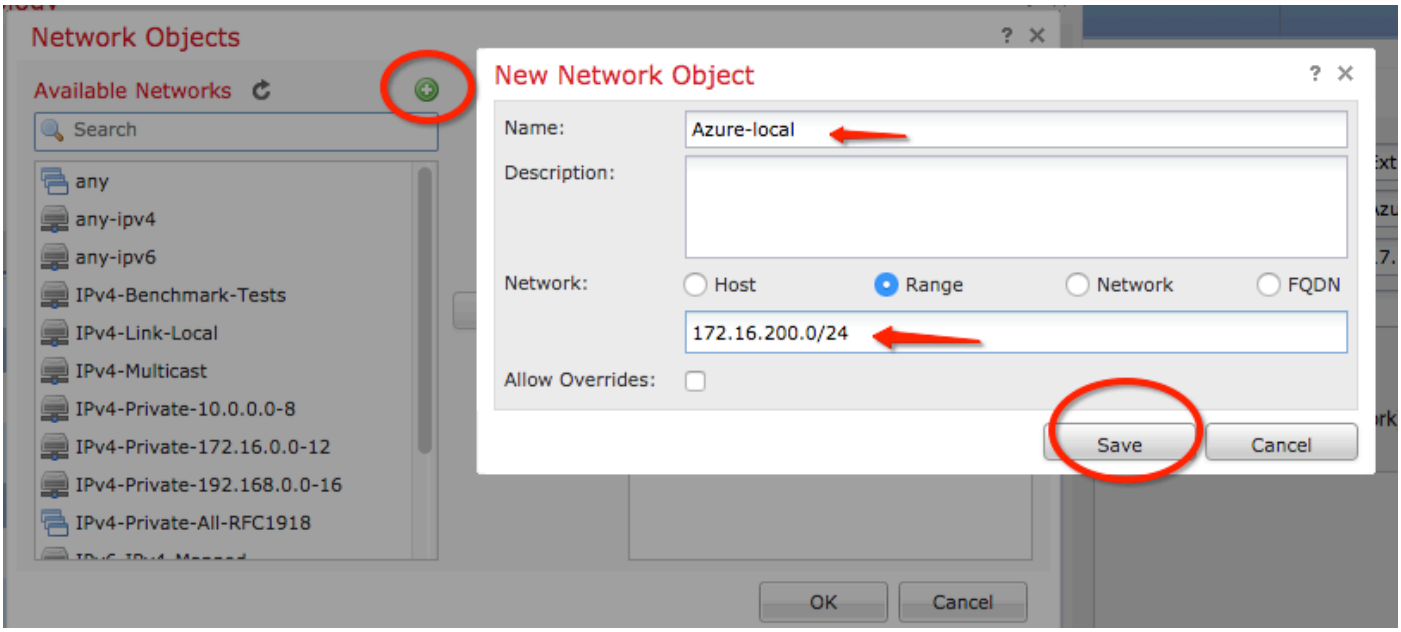


Passaggio 15. Definire l'endpoint del nodo B, che in questo esempio è l'endpoint di Azure. Nella scheda **Create New VPN Topology** , passare alla **Node B** e fare clic sul pulsante **green plus button** per aggiungere lo strumento di selezione del traffico dell'endpoint remoto. Specificare **Extranet** per tutti gli endpoint peer VPN non gestiti dallo stesso FMC del nodo A. Digitare il nome del dispositivo (solo significativo a livello locale) e il relativo indirizzo IP.

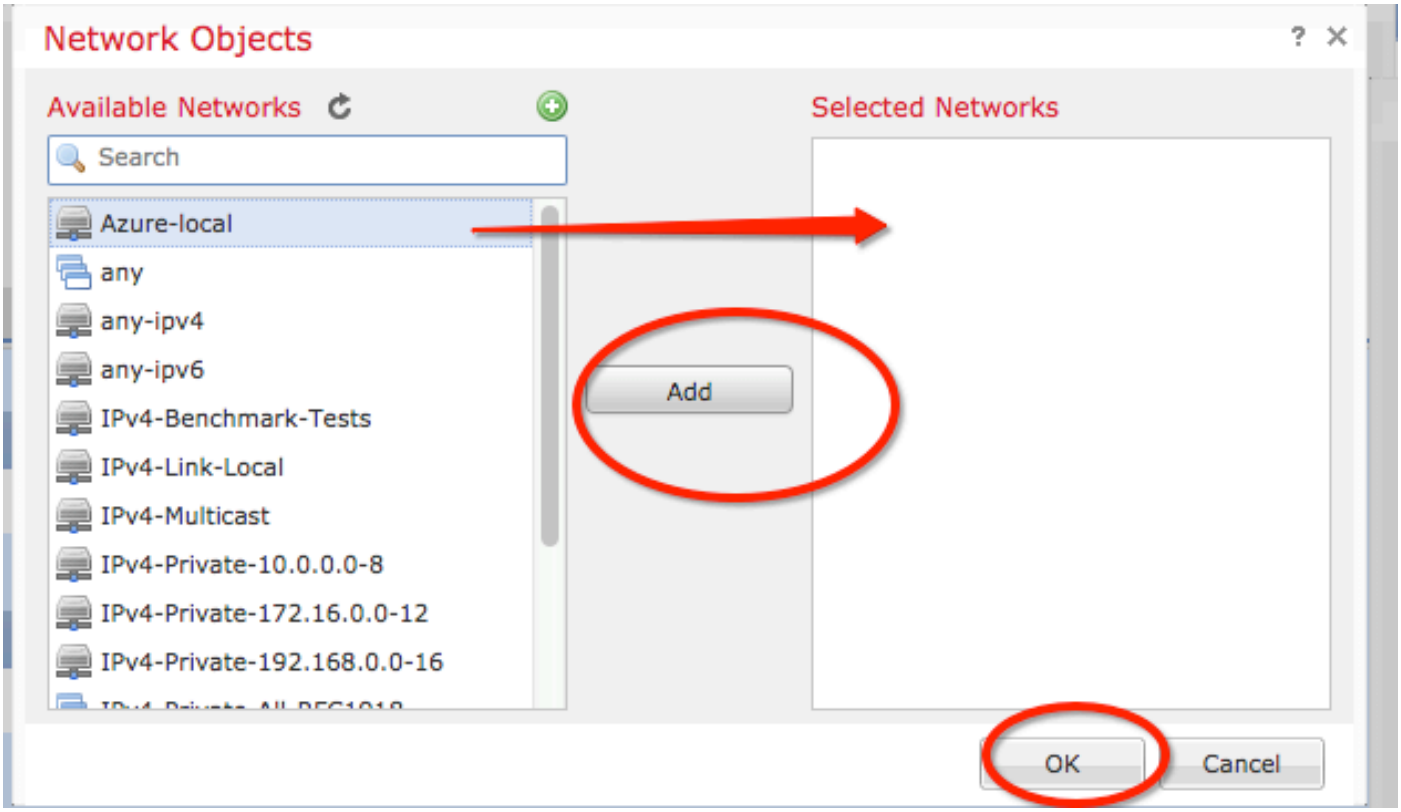


Passaggio 16. Creare l'oggetto selettore traffico remoto. Passare alla **Protected Networks** e fare clic sul pulsante **green plus button** per aggiungere un nuovo oggetto.

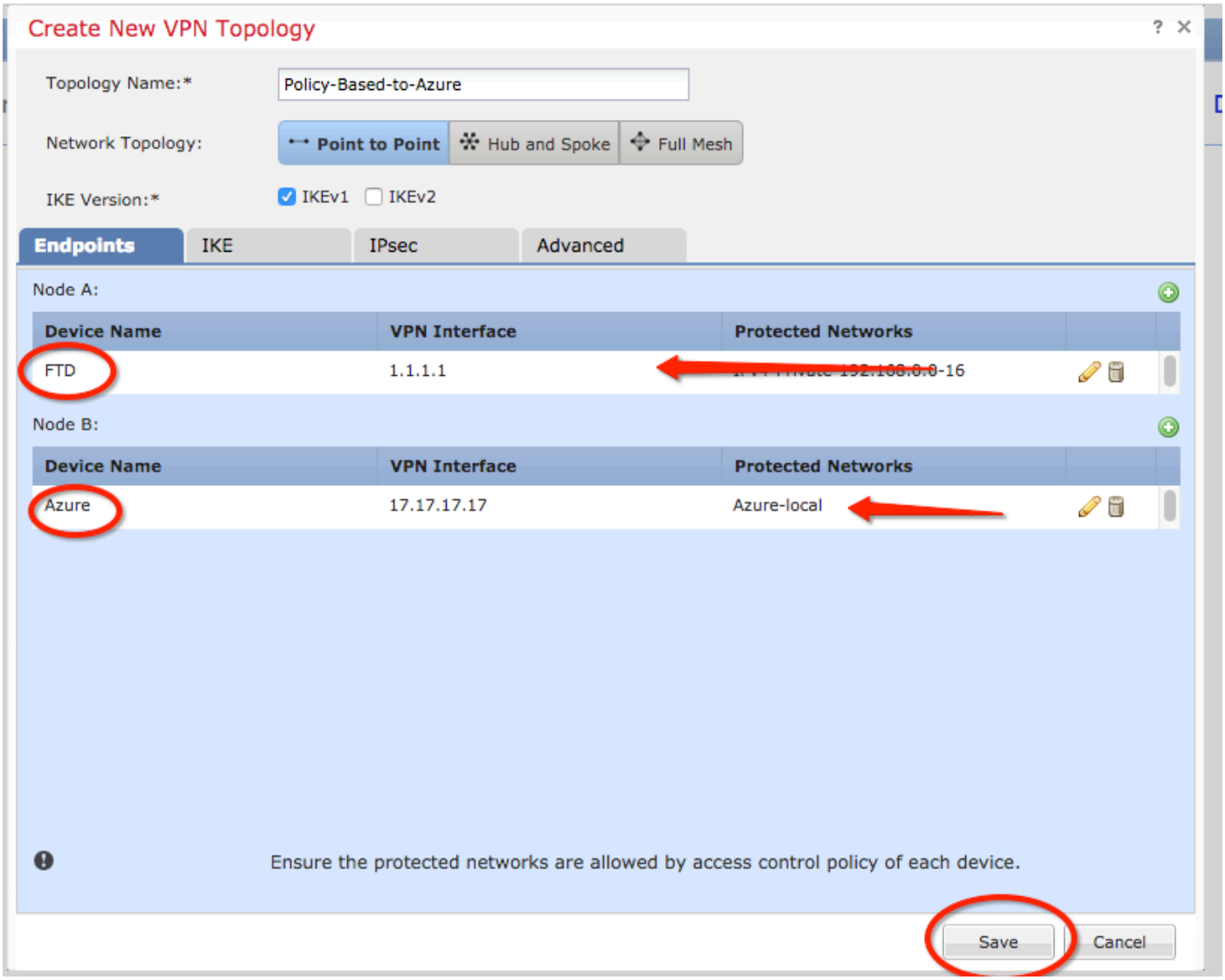
Passaggio 17. Nella **Network Objects** fare clic sul pulsante **green plus button** accanto al **Available Networks** testo per creare un nuovo oggetto. Nella scheda **New Network Object** specificare il nome dell'oggetto e scegliere di conseguenza host/intervallo/rete/FQDN e fare clic su **Save** .



Passaggio 18. Tornare alla **Network Objects** aggiungere il nuovo oggetto remoto alla finestra **Selected Networks** e fare clic su **OK** . Clic **Ok** sul **Add Endpoint** finestra.



Passaggio 19. Nella **Create New VPN Topology** è ora possibile visualizzare entrambi i nodi con i relativi selettori di traffico/reti protette corretti. Clic **Save** .



Passaggio 20. Nel dashboard del CCP fare clic su **Deploy** nel riquadro superiore destro, scegliere il dispositivo FTD e fare clic su **Deploy** .

Passaggio 21. Sull'interfaccia della riga di comando, la configurazione VPN ha lo stesso aspetto di quella dei dispositivi ASA.

IKEv2 Basato su route con selettori del traffico basati su policy

Per una VPN IKEv2 da sito a sito su ASA con mappe crittografiche, seguire questa configurazione. Verificare che Azure sia configurato per la VPN basata su route e che UsePolicyBasedTrafficSelectors sia configurato nel portale di Azure tramite PowerShell.

In questo documento di Microsoft viene descritta la configurazione di UsePolicyBasedTrafficSelectors in combinazione con la modalità VPN di Azure basata su route. Senza completare questo passaggio, ASA con mappe crittografiche non riesce a stabilire la connessione a causa di una mancata corrispondenza nei selettori di traffico ricevuti da Azure.

Fare riferimento a questo documento Cisco per le informazioni di configurazione complete di ASA IKEv2 con mappa crittografica.

Passaggio 1. Abilitare IKEv2 sull'interfaccia esterna:

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

Passaggio 2. Aggiungere un criterio IKEv2 fase 1.

> **Nota**: Microsoft ha pubblicato informazioni in conflitto con gli attributi di crittografia IKEv2 fase 1, integrità e durata utilizzati da Azure. Gli attributi elencati vengono forniti nel modo più efficace da questo documento Microsoft pubblicamente disponibile. In questa sezione vengono visualizzate le informazioni sugli attributi IKEv2 fornite da Microsoft relative ai conflitti. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 3. Creare un gruppo di tunnel con gli attributi IPsec e configurare l'indirizzo IP del peer e la chiave precondivisa del tunnel locale e remoto 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
```

Passaggio 4. Creare un elenco degli accessi che definisca il traffico da crittografare e tunneling. Nell'esempio, il traffico di interesse è il traffico proveniente dal tunnel che ha origine dalla subnet 10.2.2.0 a 10.1.1.0. Può contenere più voci se tra i siti sono coinvolte più subnet.

Nelle versioni 8.4 e successive è possibile creare oggetti o gruppi di oggetti che fungono da contenitori per le reti, le subnet, gli indirizzi IP host o più oggetti. Creare due oggetti che hanno le subnet locali e remote e usarli per le istruzioni crypto ACL e NAT.

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

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

Passaggio 5. Aggiungere una proposta IPsec IKEv2 fase 2. Specificare i parametri di sicurezza nella modalità di configurazione della proposta IPSec IKEV2 di crittografia:

protocollo esp crittografia {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocollo integrità esp {md5 | sha-1 | csa-256 | csa-384 | csa-512 | null}

> **Nota**: Microsoft ha pubblicato informazioni in conflitto con gli attributi di integrità e crittografia IPSec di fase 2 specifici utilizzati da Azure. Gli attributi elencati vengono forniti nel modo più efficace da questo documento Microsoft pubblicamente disponibile. In questa fase sono visibili le informazioni sugli attributi IPSec di fase 2 fornite da Microsoft relative ai conflitti. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 6. Configurare una mappa crittografica e applicarla all'interfaccia esterna, che contiene i seguenti componenti:
·L'indirizzo IP del peer
·Elenco degli accessi definito contenente il traffico di interesse
·Proposta IPSec fase 2 IKEv2
· Durata IPSec fase 2 in secondi
·Impostazione PFS (Perfect Forward Secrecy) opzionale, che crea una nuova coppia di chiavi Diffie-Hellman utilizzate per proteggere i dati (entrambi i lati devono essere abilitati PFS prima dell'attivazione della Fase 2)

Microsoft ha pubblicato informazioni in conflitto con gli attributi IPSec e PFS specifici della fase 2 utilizzati da Azure.

Gli attributi elencati vengono forniti nel modo più efficace questo documento Microsoft disponibile pubblicamente.

In questa fase sono visibili le informazioni sugli attributi IPSec di fase 2 fornite da Microsoft relative ai conflitti. Per ulteriori informazioni, contattare il supporto tecnico di Microsoft Azure.

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

Passaggio 8. Verificare che il traffico VPN non sia soggetto ad altre regole NAT. Creare una regola di esenzione NAT:

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

> **Nota**: quando si utilizzano più subnet, è necessario creare gruppi di oggetti con tutte le subnet di origine e di destinazione e utilizzarli nella regola NAT.

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

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

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

Verifica

Dopo aver completato la configurazione sia su ASA che sul gateway di Azure, Azure avvia il tunnel VPN. È possibile verificare che il tunnel venga compilato correttamente con questi comandi:

Fase 1

Verificare che la fase 1 dell'associazione di sicurezza sia stata creata:

IKEv2

Quindi, viene mostrata una SA IKEv2 costruita dall'interfaccia esterna locale IP 192.168.1.2 sulla porta UDP 500, alla destinazione remota IP 192.168.2.2. È inoltre presente un'associazione di protezione figlio valida creata per il flusso del traffico crittografato.

```
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
```

Qui viene mostrata una SA IKEv1 costruita con ASA come iniziatore per peer IP 192.168.2.2 con una durata residua di 86388 secondi.

```
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

Verificare che l'associazione di protezione IPSec per la fase 2 sia stata creata con **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
```

Quattro pacchetti vengono inviati e quattro ricevuti tramite l'associazione di protezione IPSec senza errori. Una SA in entrata con SPI 0x9B60EDC5 e una SA in uscita con SPI 0x8E7A2E12 sono installate come previsto.

Èinoltre possibile verificare che i dati passino attraverso il tunnel tramite una verifica della **vpn-sessiondb l2l** voci:

```
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
```

Byte Tx: e Byte Rx: visualizzare i contatori dei dati inviati e ricevuti tramite l'associazione di protezione IPSec.

Risoluzione dei problemi

Passaggio 1. Verificare che il traffico per la VPN venga ricevuto dall'ASA sull'interfaccia interna destinata alla rete privata di Azure. Per verificare, è possibile configurare un ping continuo da un client interno e configurare l'acquisizione di un pacchetto sull'appliance ASA per verificare che venga ricevuto:

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
```

Se viene rilevato il traffico di risposta da Azure, la VPN viene creata correttamente e invia/riceve il traffico.

Se il traffico di origine è assente, verificare che il mittente esegua correttamente il routing all'ASA.

Se il traffico di origine viene rilevato ma il traffico di risposta da Azure è assente, continuare per verificare il motivo.

Passaggio 2. Verificare che il traffico ricevuto sull'interfaccia ASA interna sia elaborato correttamente dall'ASA e instradato alla VPN:

Per simulare una richiesta echo ICMP:
input packet-tracer [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip] detail

Le linee guida complete sull'utilizzo di packet-tracer sono disponibili qui:
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
```
Notare che il NAT esenta il traffico (nessuna traduzione ha effetto). Verificare che non si verifichi alcuna conversione NAT sul traffico VPN.

Verificare inoltre **output-interface** è corretta - deve essere l'interfaccia fisica su cui viene applicata la mappa crittografica o l'interfaccia del tunnel virtuale.

Accertarsi che non vi siano perdite nell'elenco degli accessi.

Se la fase VPN mostra **ENCRYPT: ALLOW** , il tunnel è già stato creato ed è possibile vedere l'associazione di protezione IPSec installata con incapsulamenti.

Passaggio 2.1. Se **ENCRYPT: ALLOW** visto in packet-tracer.

Verificare che l'associazione di sicurezza IPsec sia installata e crittografi il traffico con l'utilizzo di **show crypto ipsec sa** .

Èpossibile eseguire un'acquisizione sull'interfaccia esterna per verificare che i pacchetti crittografati vengano inviati da ASA e che le risposte crittografate vengano ricevute da Azure.

Passaggio 2.2. Se **ENCRYPT:DROP** visto in packet-tracer.

Il tunnel VPN non è ancora stato stabilito ma è in fase di negoziazione. Questa è una condizione prevista quando si attiva il tunnel per la prima volta. Eseguire i debug per visualizzare il processo di negoziazione del tunnel e identificare dove e se si verifica un errore.

Verificare innanzitutto che sia attivata la versione corretta di IKE e che il processo ike-common non presenti errori rilevanti:

```
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.
```
Se non viene rilevato alcun output di debug ike-common all'avvio del traffico VPN, il traffico viene interrotto prima che raggiunga il processo di crittografia o il protocollo crypto ikev1/ikev2 non è abilitato sulla confezione. Verificare la configurazione della crittografia e le perdite di pacchetti.

Se durante i debug comuni di IKE viene visualizzato l'avvio del processo di crittografia, eseguire il debug della versione configurata di IKE per visualizzare i messaggi di negoziazione del tunnel e identificare la posizione in cui si è verificato l'errore durante la generazione del tunnel con Azure.

IKEv1

Qui è possibile consultare la procedura di debug e l'analisi complete di ikev1.

```
Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127
```
IKEv2

Qui sono disponibili la procedura di debug e l'analisi complete di ikev2.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).