Configurar VPN basada en políticas y basada en rutas desde ASA y FTD a Microsoft Azure

Contenido

Introducción

Este documento describe los conceptos y la configuración para una VPN entre Cisco ASA y Cisco Secure Firewall y los servicios en la nube de Microsoft Azure.

Conceptos

Dominio de cifrado VPN

El intervalo de direcciones IP IPSec permite participar en el túnel VPN. El dominio de cifrado se define mediante un selector de tráfico local y un selector de tráfico remoto para especificar los intervalos de subred local y remota que IPSec captura y cifra. Existen dos métodos para definir los dominios de cifrado VPN: selectores de tráfico basados en ruta o en políticas.

Basado en ruta:
El dominio de cifrado está configurado para permitir el tráfico que entra en el túnel IPSec. Los selectores de tráfico local y remoto de IPSec se establecen en 0.0.0.0. Esto significa que cualquier tráfico enrutado en el túnel IPSec se cifra independientemente de la subred de origen/destino.

El dispositivo de seguridad adaptable de Cisco (ASA) admite VPN basada en rutas con el uso de interfaces de túnel virtual (VTI) en las versiones 9.8 y posteriores.

Cisco Secure Firewall o Firepower Threat Defense (FTD) administrado por FMC (Firepower Management Center) admite VPN basada en ruta con el uso de VTI en las versiones 6.7 y posteriores.

Basado en políticas:

El dominio de cifrado se establece para cifrar sólo intervalos de IP específicos para el origen y el destino. Los selectores de tráfico local basados en políticas y los selectores de tráfico remoto identifican el tráfico que se va a cifrar a través de IPSec.

ASA admite VPN basada en políticas con mapas criptográficos en la versión 8.2 y posteriores.

Microsoft Azure admite selectores de tráfico basados en rutas, basados en políticas o basados en rutas simulados. Azure restringe actualmente la versión de Intercambio de claves de Internet (IKE) que puede configurar en función del método seleccionado de VPN. Basado en rutas requiere IKEv2 y basado en políticas requiere IKEv1. Esto significa que si se usa IKEv2, se debe seleccionar basado en rutas en Azure y ASA debe usar un VTI, pero si ASA sólo admite mapas criptográficos debido a la versión de código, Azure debe configurarse para basado en rutas con selectores de tráfico basados en políticas. Esto se logra en el portal de Azure a través de la implementación de scripts de PowerShell para implementar una opción que Microsoft llama a UsePolicyBasedTrafficSelectors como se explica aquí: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps.

Para resumir desde la perspectiva de la configuración de ASA y FTD:

- Para ASA/FTD configurado con un mapa criptográfico, Azure debe configurarse para VPN basada en políticas o basada en rutas con UsePolicyBasedTrafficSelectors.
- Para ASA configurado con un VTI, Azure debe configurarse para VPN basada en ruta.
- Para el FTD, se puede encontrar más información sobre cómo configurar las VTI aquí; 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

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Para VPN basada en ruta IKEv2 que utiliza VTI en ASA: Código ASA versión 9.8(1) o posterior. (Azure debe estar configurado para VPN basada en rutas.)
- Para VPN basada en políticas IKEv1 que utiliza el mapa criptográfico en ASA y FTD: Código ASA versión 8.2 o posterior y FTD 6.2.0 o posterior. (Azure debe configurarse para VPN basada en políticas.)
- Para VPN basada en rutas IKEv2 que utiliza mapa criptográfico en ASA con selectores de tráfico basados en políticas: Código ASA versión 8.2 o posterior configurado con un mapa criptográfico. (Azure debe configurarse para VPN basada en rutas con UsePolicyBasedTrafficSelectors.)
- Conocimiento de FMC para la gestión y configuración de FTD.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Complete los pasos de configuración. Elija entre configurar IKEv1, IKEv2 basado en ruta con VTI o IKEv2 basado en ruta con selectores de tráfico basado en políticas de uso (mapa criptográfico en ASA).

Configuración de IKEv1 en ASA

Para una VPN IKEv1 de sitio a sitio de ASA a Azure, siga la siguiente configuración de ASA. Asegúrese de configurar un túnel basado en directivas en el portal de Azure. Para este ejemplo, se utilizan mapas criptográficos en ASA.

Consulte este documento de Cisco para obtener información completa sobre IKEv1 en la configuración de ASA.

Paso 1. Habilite IKEv1 en la interfaz externa.

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

Paso 2. Cree una política IKEv1 que defina los algoritmos/métodos que se utilizarán para el hash, la autenticación, el grupo Diffie-Hellman, la duración y el cifrado.

> **Nota:** Los atributos IKEv1 de la fase 1 enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 3. Cree un grupo de túnel bajo los atributos IPsec y configure la dirección IP del par y la clave previamente compartida del túnel.

```
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
```

Paso 4. Cree una lista de acceso que defina el tráfico que se va a cifrar y tunelizar. En este ejemplo, el tráfico de interés es el tráfico del túnel que se origina desde la subred 10.2.2.0 a 10.1.1.0. Puede contener entradas múltiples si hay varias subredes involucradas entre los sitios.

En las versiones 8.4 y posteriores, se pueden crear objetos o grupos de objetos que sirvan como contenedores para las redes, subredes, direcciones IP de host o varios objetos. Cree dos objetos que tengan las subredes local y remota y utilícelas para las instrucciones crypto Access Control List (ACL) y 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
```

Paso 5. Configure el conjunto de transformación (TS), que debe incluir la palabra clave**IKEv1**. También se debe crear un TS idéntico en el extremo remoto.

> **Nota:** Los atributos IKEv1 de la fase 2 enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Para obtener más información, póngase en contacto con el soporte técnico de Microsoft Azure.

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

Paso 6. Configure el mapa criptográfico y aplíquelo a la interfaz externa, que tiene estos componentes:
·La dirección IP del par
·La lista de acceso definida que contiene el tráfico de interés
·El TS
·La configuración no establece Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS) ya que la documentación de Azure disponible públicamente establece que PFS está inhabilitado para IKEv1 en Azure. Una configuración PFS opcional, que crea un nuevo par de claves Diffie-Hellman que se utilizan para proteger los datos (ambos lados deben estar habilitados para PFS antes de que aparezca la fase 2), se puede habilitar mediante el uso de esta configuración: **crypto map outside_map 20 set pfs .**
· Los períodos de duración de IPSec de fase 2 se basan en la documentación de Azure disponible públicamente. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 7. Asegúrese de que el tráfico VPN no esté sujeto a ninguna otra regla NAT. Cree una regla de exención 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**: Cuando se utilizan varias subredes, debe crear grupos de objetos con todas las subredes de origen y destino y utilizarlas en la regla 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
```

Basado en ruta IKEv2 con VTI en el código ASA 9.8 (1) o posterior

Para una VPN basada en ruta IKEv2 de sitio a sitio en código ASA, siga esta configuración. Asegúrese de que Azure esté configurado para VPN basada en rutas y no configure UsePolicyBasedTrafficSelectors en el portal de Azure. Se configura un VTI en el ASA.

Consulte este documento de Cisco para obtener información completa sobre la configuración de ASA VTI.

Paso 1. Habilite IKEv2 en la interfaz externa:

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

Paso 2. Agregue una política IKEv2 fase 1.

> **Nota**: Microsoft ha publicado información que entra en conflicto con los atributos específicos de cifrado, integridad y duración de la fase 1 de IKEv2 utilizados por Azure. Los atributos enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Aquí se puede ver la información que entra en conflicto con el atributo IKEv2 de Microsoft. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 3. Agregue una propuesta IPsec de IKEv2 fase 2. Especifique los parámetros de seguridad en el IPSec de cifrado **ikev2 ipsec-proposal** modo de configuración global:

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

> **Nota:** Microsoft ha publicado información que entra en conflicto con respecto a los atributos de integridad y cifrado IPSec de fase 2 concretos utilizados por Azure. Los atributos enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Aquí se puede ver la información que entra en conflicto con el atributo IPSec de fase 2 de Microsoft. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 4. Agregue un perfil IPSec que especifique:

- La propuesta IPSec ikev2 fase 2 previamente configurada
- Duración de IPSec de fase 2 (opcional) en segundos o kilobytes
- El grupo PFS (opcional)

> **Nota:** Microsoft ha publicado información que entra en conflicto con respecto a la duración IPSec de fase 2 y los atributos PFS concretos utilizados por Azure. Los atributos enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Aquí se puede ver la información que entra en conflicto con el atributo IPSec de fase 2 de Microsoft. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 5. Cree un grupo de túnel bajo los atributos IPsec y configure la dirección IP del par y la clave previamente compartida de túnel local y 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
```

Paso 6. Cree una VTI que especifique:

- Un nuevo número de interfaz de túnel: interface tunnel [número]

- Un nuevo nombre de interfaz de túnel: nameif [nombre]
- Una dirección IP que no existe en la interfaz de túnel: ip address [ip-address] [mask]
- Interfaz de origen del túnel donde la VPN termina localmente: tunnel source interface [int-name]
- La dirección IP del gateway de Azure: tunnel destination [Azure Public IP]
- Modo IPSec IPv4: tunnel mode ipsec ipv4
- El perfil IPSec que se utilizará para esta VTI: tunnel protection ipsec profile [profile-name]

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

Paso 7. Cree una ruta estática para dirigir el tráfico al túnel. Para agregar una ruta estática, ingrese este comando:
route if_name dest_ip mask gateway_ip [distance]

dest_ip y **mask** es la dirección IP de la red de destino en la nube de Azure, por ejemplo, 10.0.0.0/24. El gateway_ip debe ser cualquier dirección IP (existente o inexistente) en la subred de la interfaz de túnel, como 169.254.0.2. El propósito de este gateway_ip es dirigir el tráfico a la interfaz de túnel, pero la IP de gateway concreta en sí no es importante.

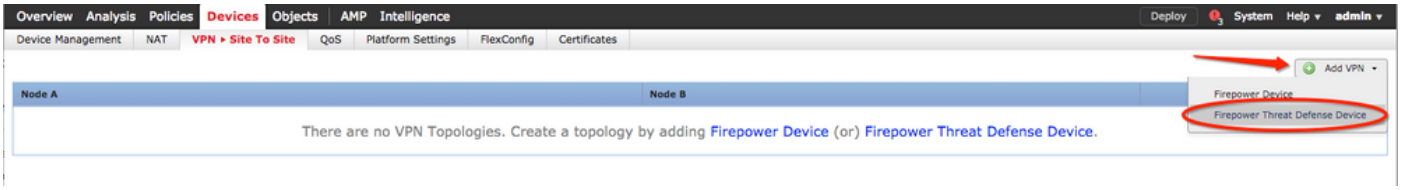
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

Configuración IKEv1 en FTD

Para una VPN IKEv1 de sitio a sitio desde FTD a Azure, debe haber registrado previamente el dispositivo FTD en FMC.

Paso 1. Crear una directiva de sitio a sitio. Vaya a la **FMC dashboard > Devices > VPN > Site to Site**.

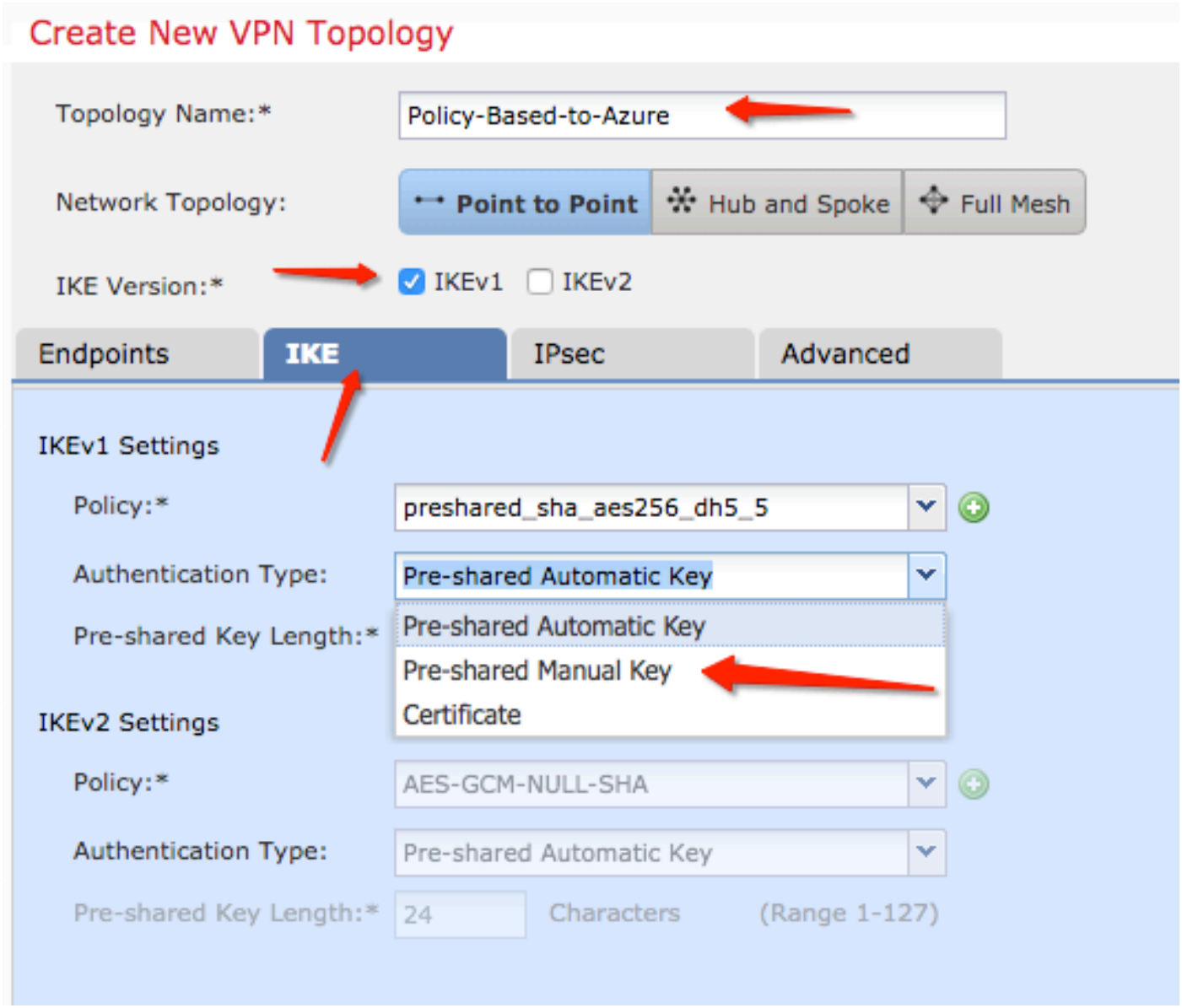
Paso 2. Cree una nueva política. Haga clic en el **Add VPN** menú desplegable y seleccione **Firepower Threat Defense device** .

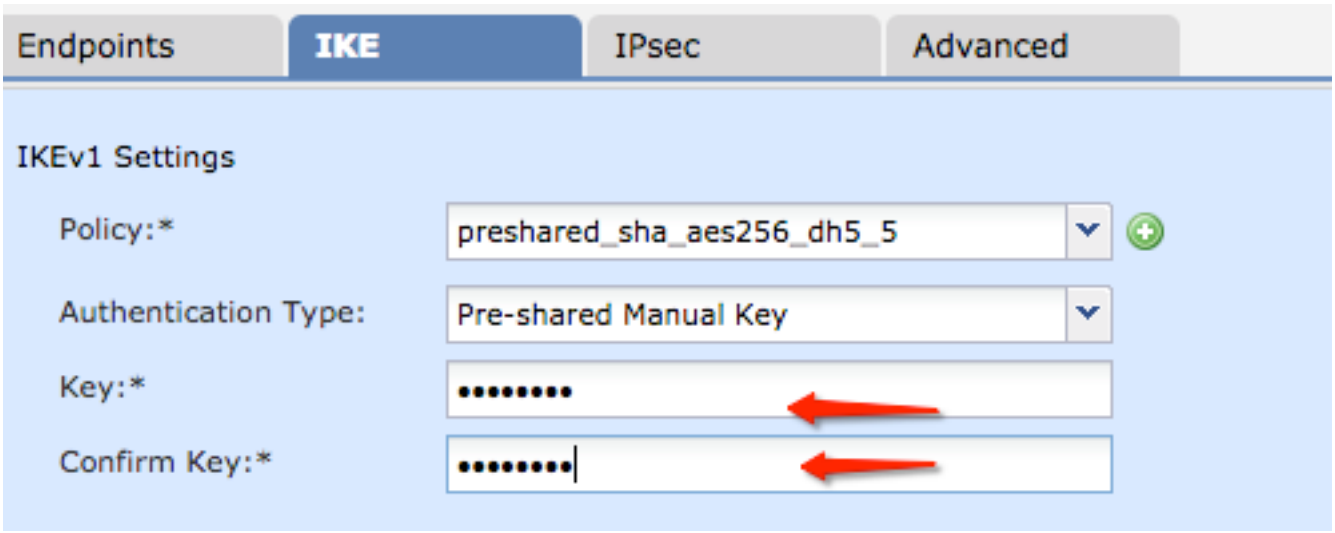


Paso 3. En el **Create new VPN Topology** , especifique su **Topology Name**, compruebe el **IKEV1** y haga clic en el botón **IKE** ficha. En este ejemplo, se utilizan claves previamente compartidas como método

de autenticación.

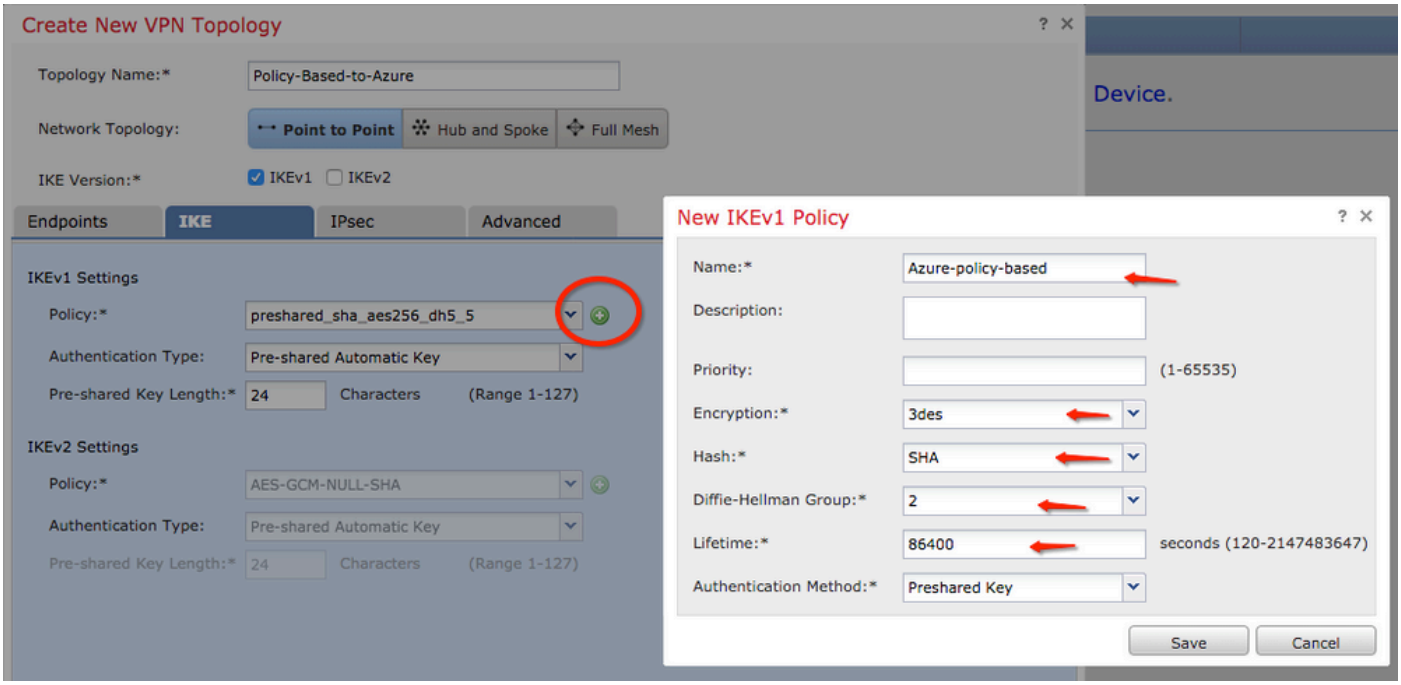
Haga clic en el **Authentication Type** menú desplegable y seleccione **Pre-shared manual key** . Escriba la clave precompartida manual en el **Key** y**Confirm Key** campos de texto.



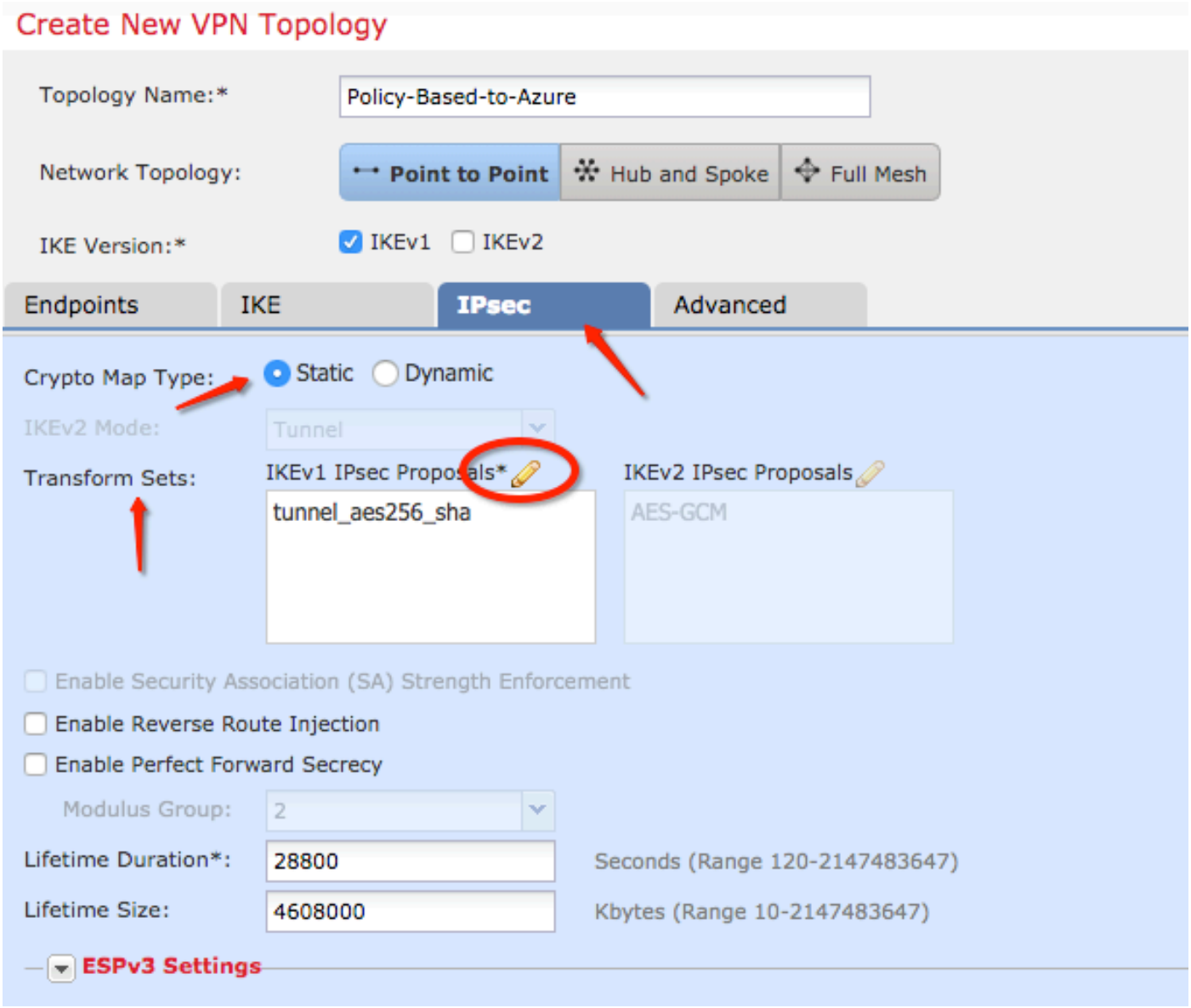


Paso 4. Configure la política ISAKMP o los parámetros de la Fase 1 con la creación de una nueva. En la misma ventana, haga clic en el botón **green plus button** para agregar una nueva política

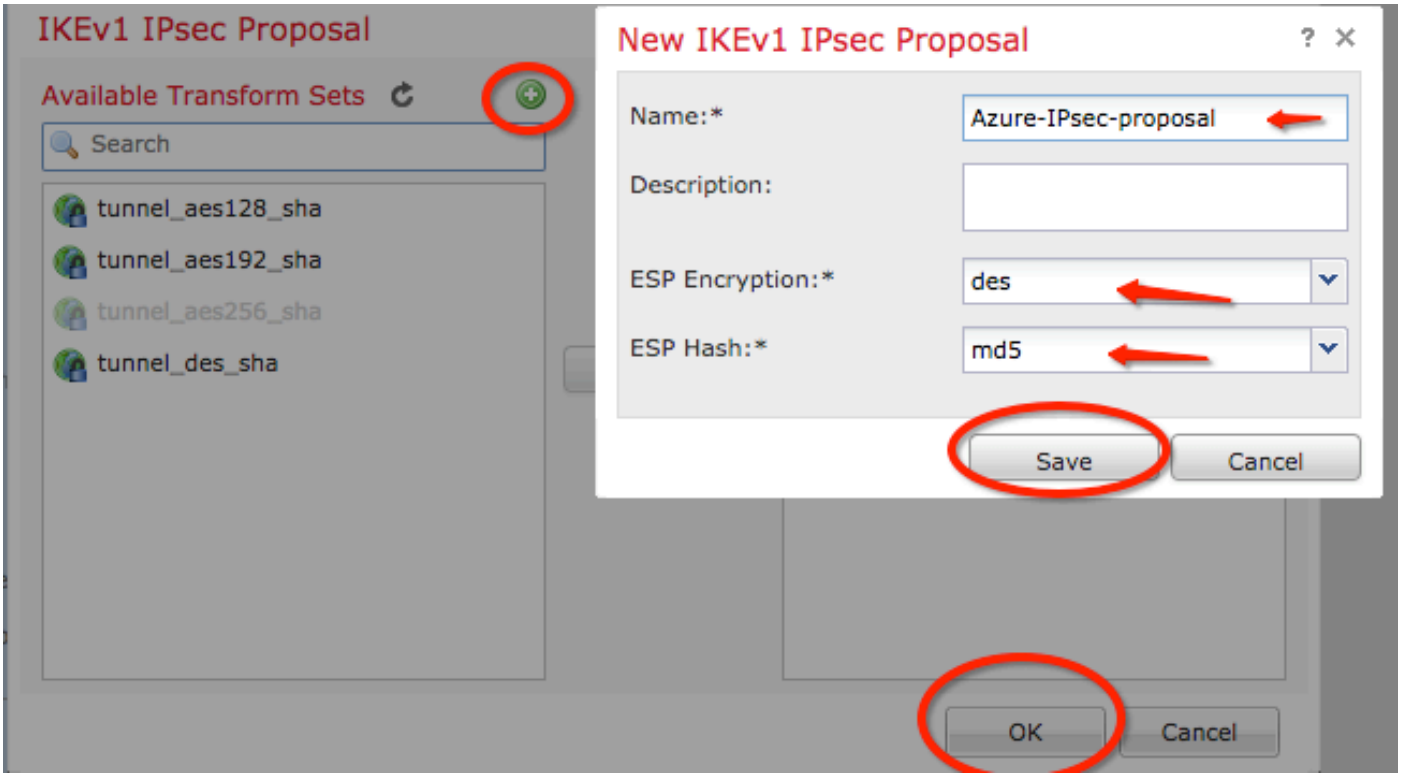
ISAKMP. Especifique el nombre de la política y elija el cifrado, hash, grupo Diffie-Hellman, duración y método de autenticación deseados, y haga clic en **Save** .



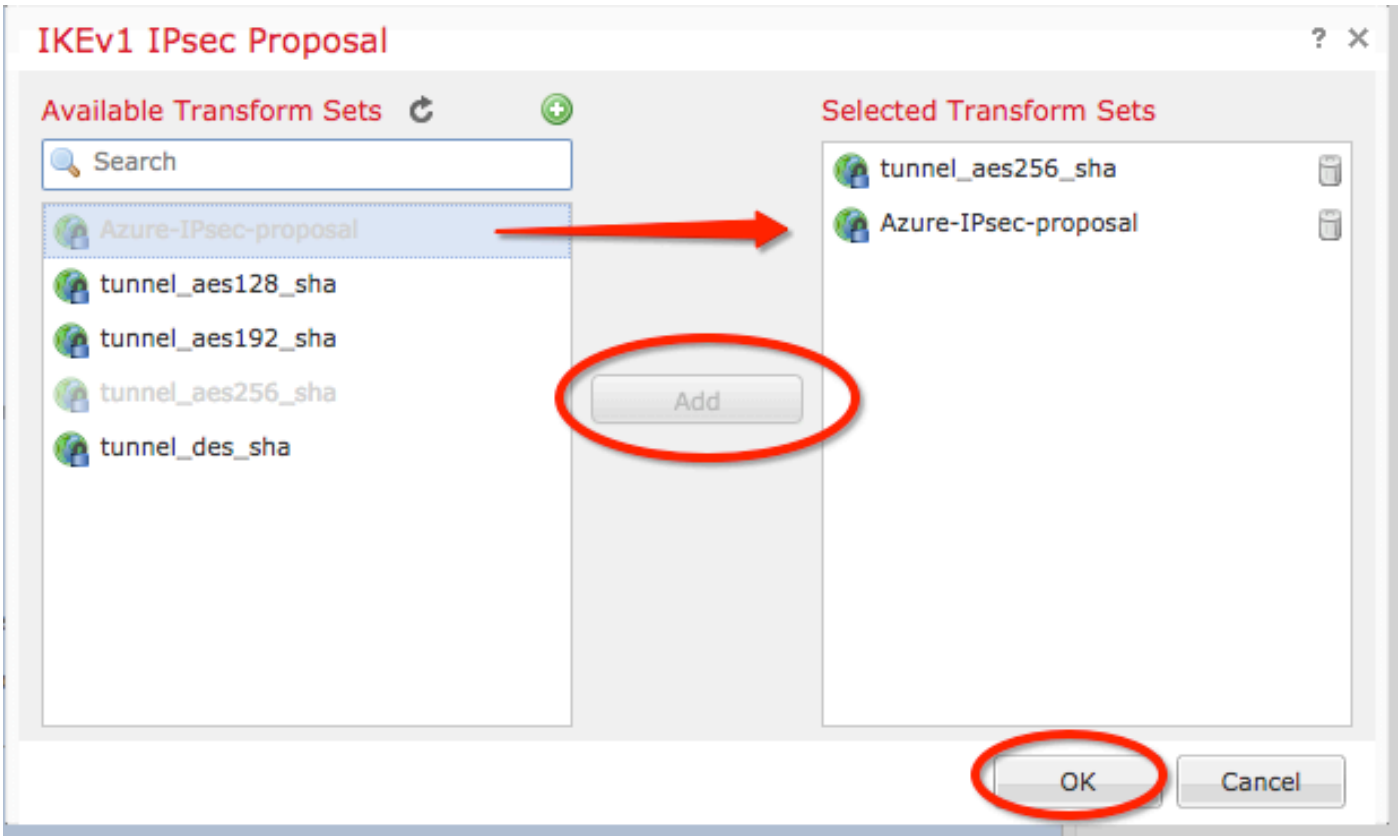
Paso 5. Configure la política IPsec o los parámetros de fase 2. Vaya a la **IPsec** ficha, elija **Static** en el **Crypto Map Type** casilla de verificación. Haga clic en el **edit pencil** del menú desplegable **IKEV1 IPsec Proposals** en el **Transform Sets** opción.



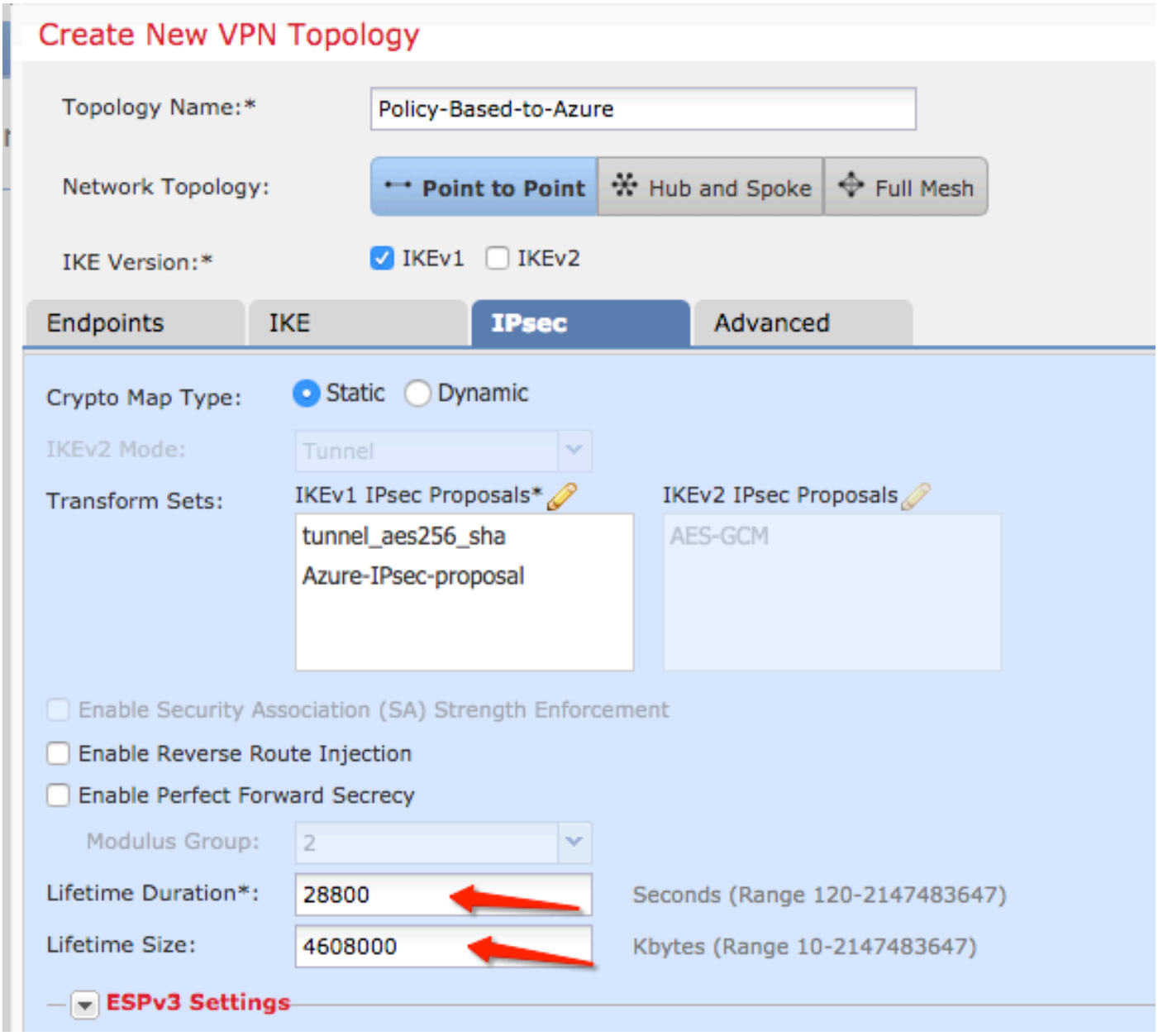
Paso 6. Cree una nueva propuesta de IPSec. En el **IKEv1 IPSec Proposal** haga clic en el botón **green plus button** para agregar uno nuevo. Especifique el nombre de la política y sus parámetros deseados para los algoritmos ESP Encryption y ESP Hash y haga clic en **Save** .



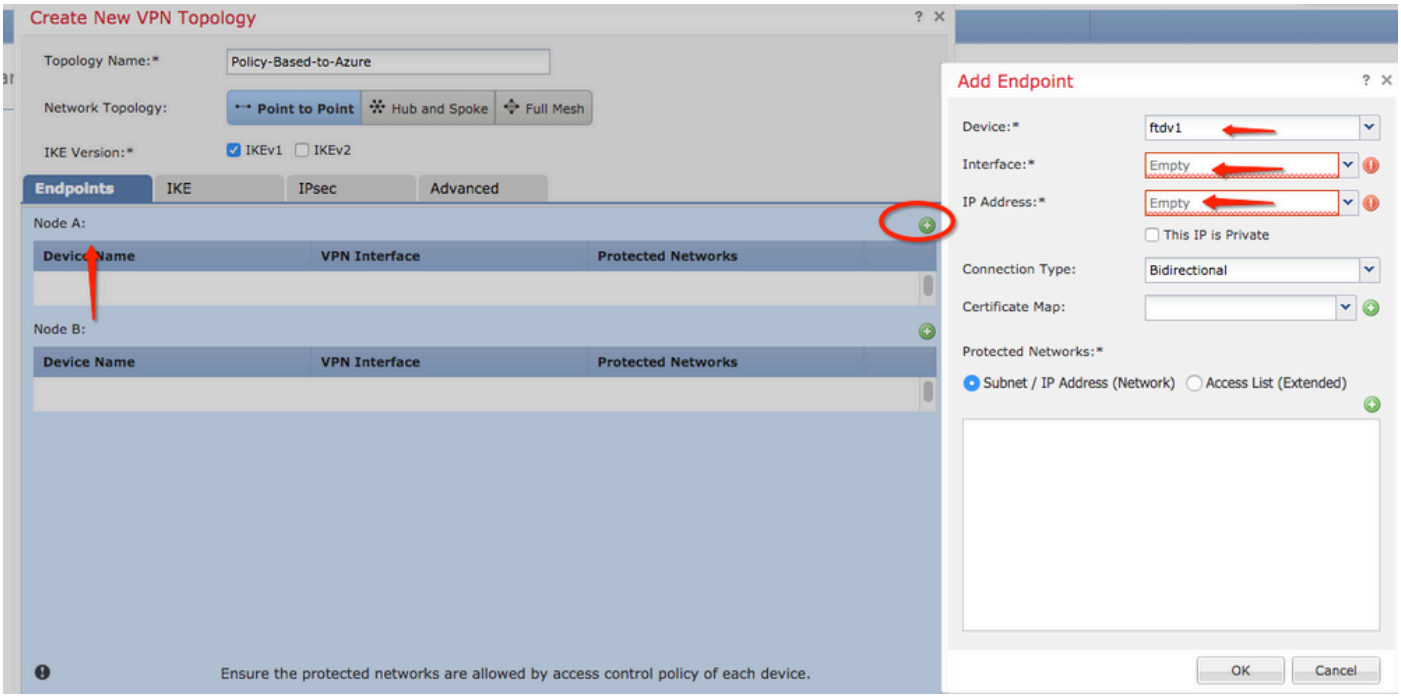
Paso 7. En el **IKEV1 IPsec Proposal** , agregue la nueva directiva IPsec a la ventana **Selected Transform Sets** y haga clic en **OK** .



Paso 8. Vuelva al **IPSec** , configure la duración y el tamaño deseados.



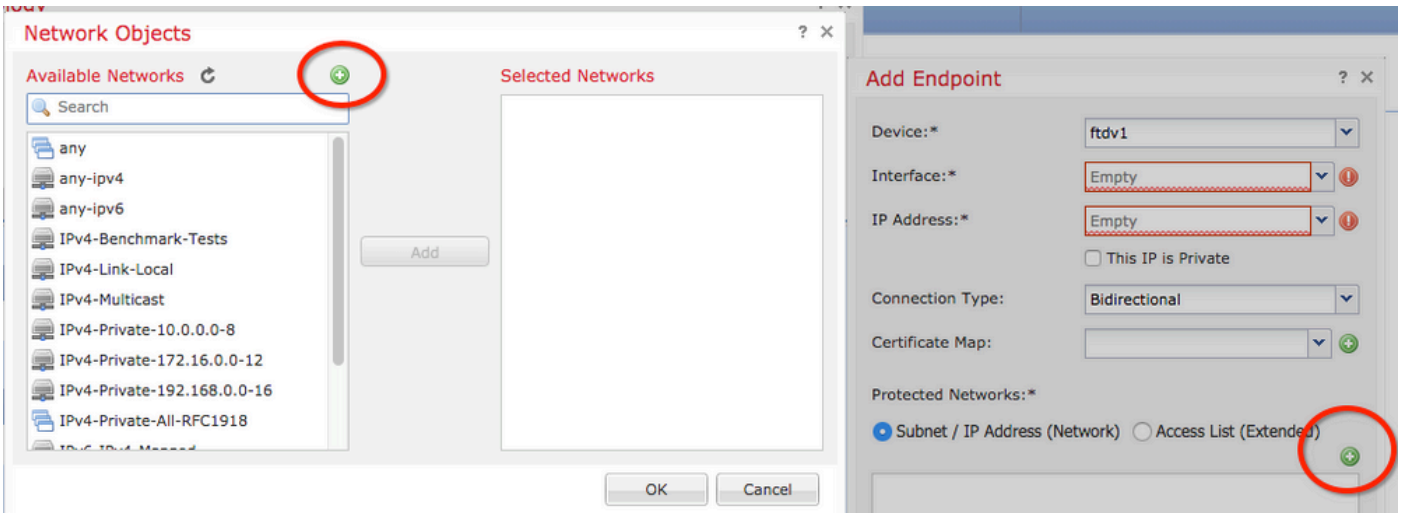
Paso 9. Elija el dominio de cifrado/selectores de tráfico/redes protegidas. Vaya a la **Endpoints** ficha. En el **Node A** haga clic en el botón **green plus button** para agregar uno nuevo. En este ejemplo, el nodo A se utiliza como subredes locales del FTD.



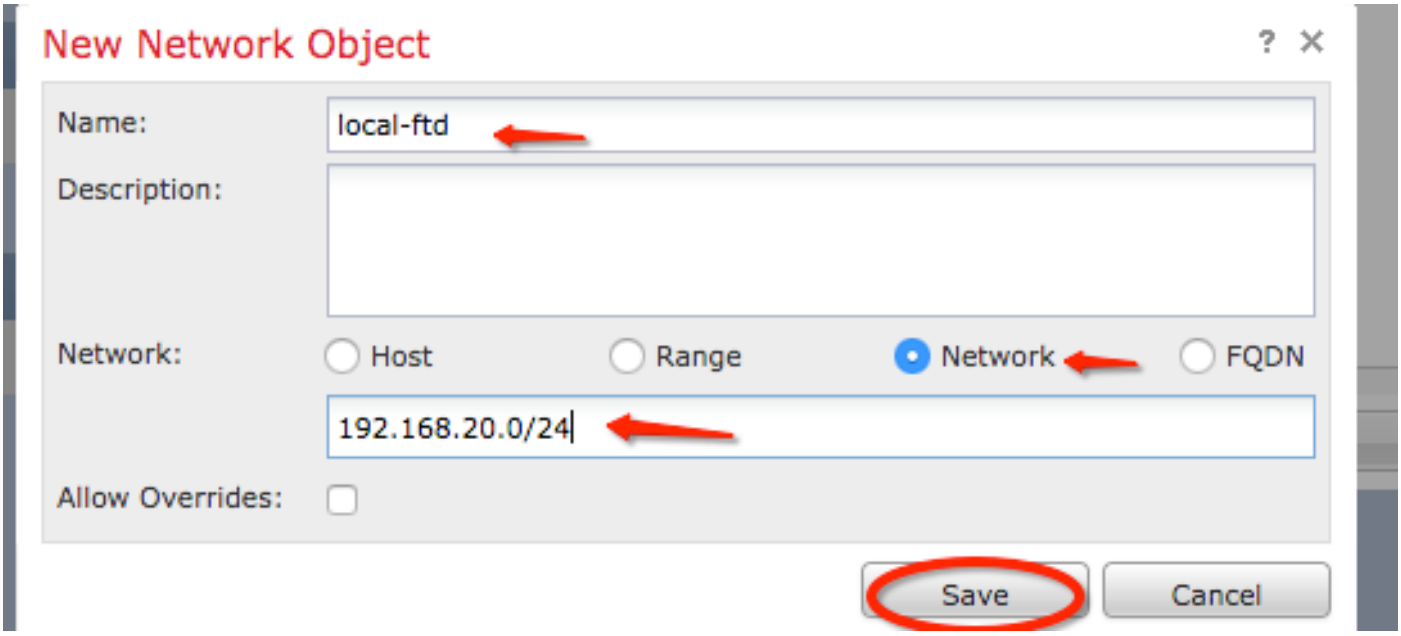
Paso 10. En el **Add Endpoint** , especifique el FTD que se utilizará en el **Device** junto con su interfaz física y la dirección IP que se utilizará.

Paso 11. Para especificar el selector de tráfico local, acceda a la **Protected Networks** y haga clic en el botón **green plus button** para crear un nuevo objeto.

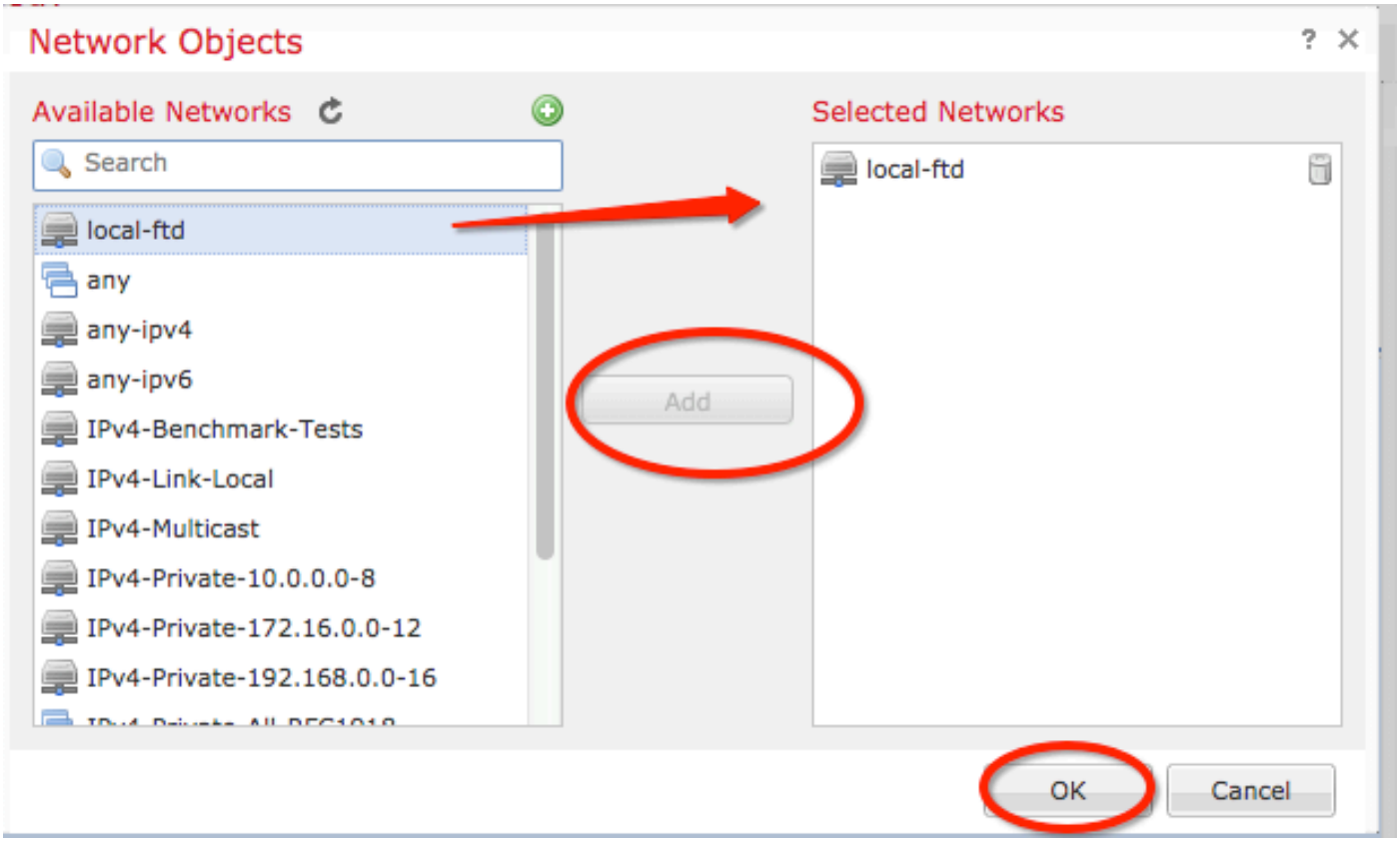
Paso 12. En el **Network Objects** haga clic en el botón **green plus button** junto a la **Available Networks** texto para crear un nuevo objeto de selector de tráfico local.



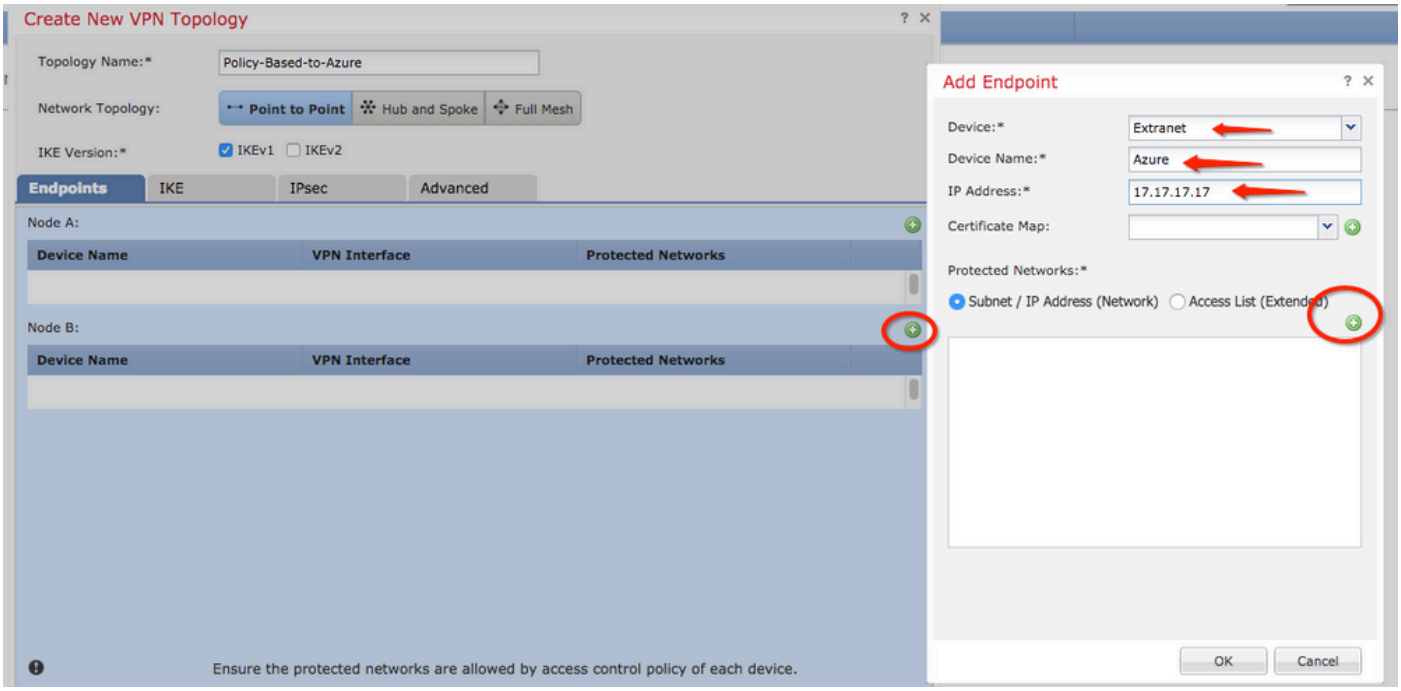
Paso 13. En el **New Network Object** , especifique el nombre del objeto y elija en consecuencia host/red/rango/FQDN. A continuación, haga clic en **Save** .



Paso 14. Agregue el objeto al **Selected Networks** en la sección **Network Objects** y haga clic en **OK** . Haga clic **OK** en el **Add Endpoint** ventana.

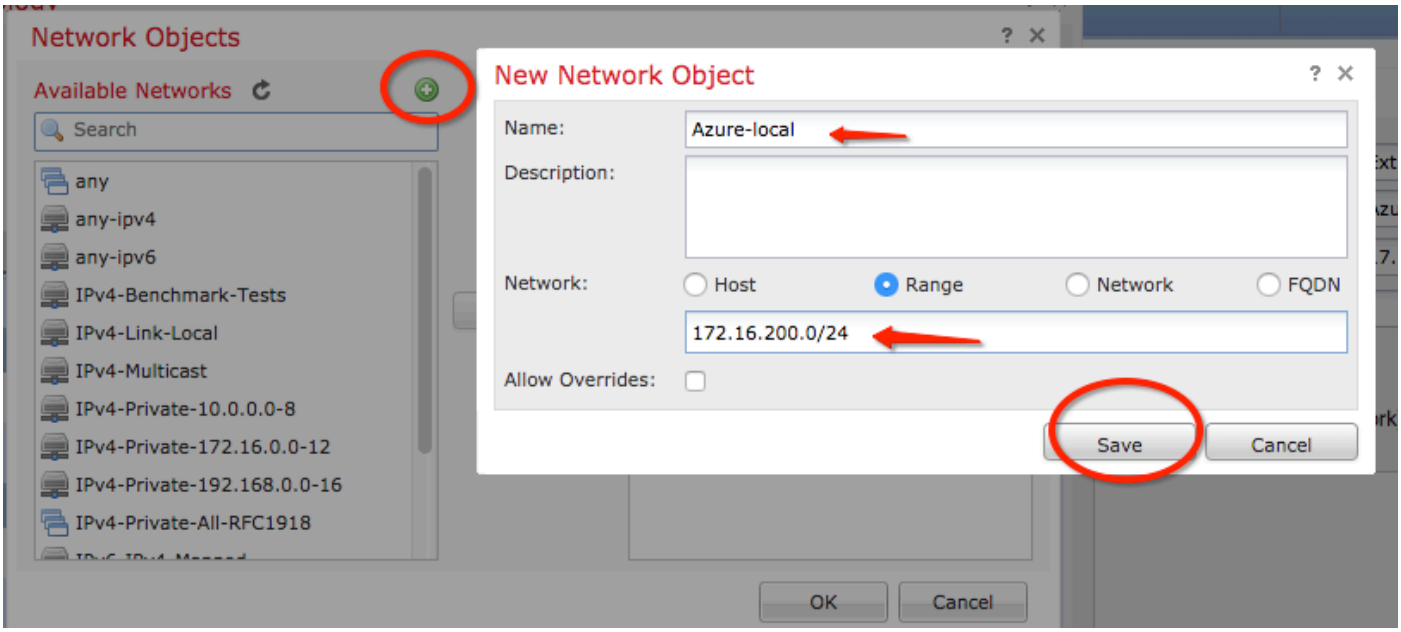


Paso 15. Defina el extremo del nodo B, que en este ejemplo es el extremo de Azure. En el **Create New VPN Topology** ventana, acceda a la **Node B** y haga clic en el botón **green plus button** para agregar el selector de tráfico de terminal remoto. Especificar **Extranet** para todos los puntos finales de peer VPN que no estén gestionados por la misma FMC que el nodo A. Escriba el nombre del dispositivo (sólo significativo a nivel local) y su dirección IP.

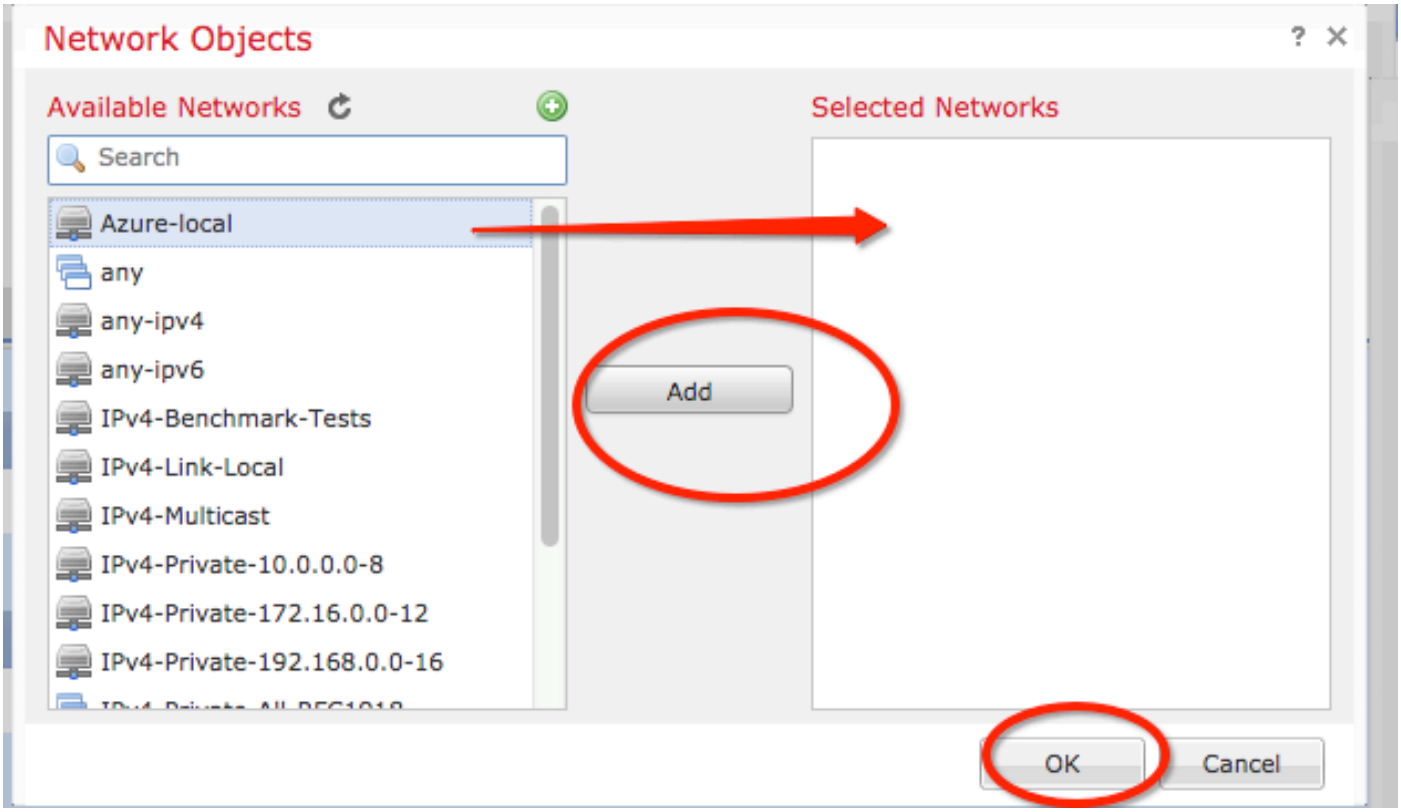


Paso 16. Cree el objeto selector de tráfico remoto. Vaya a la **Protected Networks** y haga clic en el botón **green plus button** para agregar un nuevo objeto.

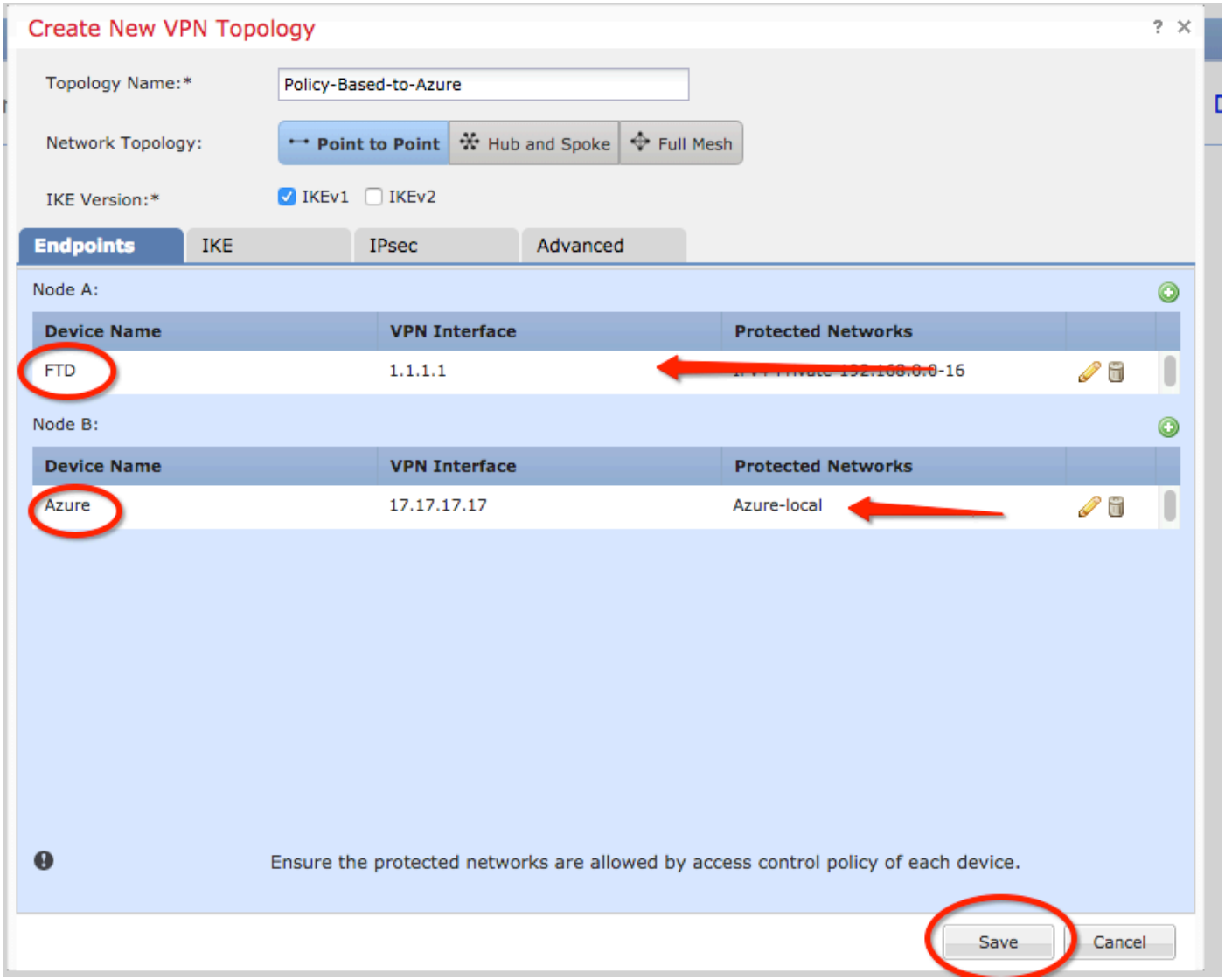
Paso 17. En el **Network Objects** haga clic en el botón **green plus button** junto a la **Available Networks** texto para crear un nuevo objeto. En el **New Network Object** , especifique el nombre del objeto, elija el host/intervalo/red/FQDN y haga clic en **Save** .



Paso 18. De nuevo en el **Network Objects** , agregue el nuevo objeto remoto a la ventana **Selected Networks** y haga clic en **OK** . Haga clic **Ok** en el **Add Endpoint** ventana.



Paso 19. En el **Create New VPN Topology** puede ver ahora ambos nodos con sus selectores de tráfico correctos/redes protegidas. Haga clic **Save** .



Paso 20. En el panel del CSP, haga clic en **Deploy** en el panel superior derecho, seleccione el dispositivo FTD y haga clic en **Deploy** .

Paso 21. En la interfaz de línea de comandos, la configuración de VPN tiene el mismo aspecto que la de los dispositivos ASA.

Basado en ruta IKEv2 con selectores de tráfico basados en políticas

Para una VPN IKEv2 de sitio a sitio en ASA con mapas criptográficos, siga esta configuración. Asegúrese de que Azure esté configurado para VPN basada en rutas y de que UsePolicyBasedTrafficSelectors se deba configurar en el portal de Azure mediante el uso de PowerShell.

Este documento de Microsoft describe la configuración de UsePolicyBasedTrafficSelectors junto con el modo VPN de Azure basado en ruta. Sin la finalización de este paso, ASA con mapas criptográficos no puede establecer la conexión debido a una discordancia en los selectores de tráfico recibidos de Azure.

Consulte este documento de Cisco para obtener información completa sobre ASA IKEv2 con información de configuración de mapa criptográfico.

Paso 1. Habilite IKEv2 en la interfaz externa:

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

Paso 2. Agregue una política IKEv2 fase 1.

> **Nota**: Microsoft ha publicado información que entra en conflicto con los atributos específicos de cifrado, integridad y duración de la fase 1 de IKEv2 utilizados por Azure. Los atributos enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Aquí se puede ver la información de atributos IKEv2 de Microsoft que está en conflicto. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 3. Cree un grupo de túnel bajo los atributos IPsec y configure la dirección IP del par y la clave previamente compartida de túnel local y 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
```

Paso 4. Cree una lista de acceso que defina el tráfico que se va a cifrar y tunelizar. En este ejemplo, el tráfico de interés es el tráfico del túnel que se origina desde la subred 10.2.2.0 a 10.1.1.0. Puede contener entradas múltiples si hay varias subredes involucradas entre los sitios.

En las versiones 8.4 y posteriores, se pueden crear objetos o grupos de objetos que sirvan como contenedores para las redes, subredes, direcciones IP de host o varios objetos. Cree dos objetos que tengan las subredes local y remota y utilícelos tanto para la ACL crypto como para las sentencias 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
```

Paso 5. Agregue una propuesta IPsec de fase 2 de IKEv2. Especifique los parámetros de seguridad en el modo de configuración crypto IPsec ikev2 ipsec-offer:

protocol esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}

protocol esp integration {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **Nota**: Microsoft ha publicado información que entra en conflicto con los atributos de integridad y cifrado IPSec de fase 2 concretos utilizados por Azure. Los atributos enumerados se proporcionan en el mejor esfuerzo de este documento de Microsoft disponible públicamente. Aquí se puede ver la información de atributos IPSec de fase 2 de Microsoft que entra en conflicto. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 6. Configure un mapa criptográfico y aplíquelo a la interfaz externa, que contiene estos componentes:
·La dirección IP del par
·La lista de acceso definida que contiene el tráfico de interés
·La propuesta IPSec de fase 2 de IKEv2
· Duración de IPSec de fase 2 en segundos
·Un parámetro opcional de Confidencialidad directa perfecta (PFS), que crea un nuevo par de claves Diffie-Hellman que se utilizan para proteger los datos (ambos extremos deben estar habilitados para PFS antes de que aparezca la fase 2)

Microsoft ha publicado información que entra en conflicto con respecto a la duración de IPSec de fase 2 y los atributos PFS concretos utilizados por Azure.

Los atributos enumerados se proporcionan con el mejor esfuerzo de este documento de Microsoft disponible públicamente.

Aquí se puede ver la información de atributos IPSec de fase 2 de Microsoft que entra en conflicto. Para obtener más información, póngase en contacto con el soporte técnico de 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
```

Paso 8. Asegúrese de que el tráfico VPN no esté sujeto a ninguna otra regla NAT. Cree una regla de exención 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**: Cuando se utilizan varias subredes, debe crear grupos de objetos con todas las subredes de origen y destino y utilizarlas en la regla 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
```

Verificación

Después de completar la configuración tanto en ASA como en el gateway de Azure, Azure inicia el túnel VPN. Puede verificar que el túnel se genera correctamente con estos comandos:

Fase 1

Verifique que se haya creado la fase 1 Security Association (SA):

IKEv2

A continuación, se muestra una SA IKEv2 construida desde la interfaz externa local IP 192.168.1.2 en el puerto UDP 500 hasta la IP de destino remoto 192.168.2.2. También existe una SA secundaria válida creada para que el tráfico cifrado fluya a través de ella.

```
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
```

Aquí, se muestra una SA IKEv1 construida con ASA como iniciador para igualar IP 192.168.2.2 con una vida útil restante de 86388 segundos.

```
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

Compruebe que la asociación de seguridad IPSec de fase 2 se ha creado 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
```

Se envían cuatro paquetes y se reciben cuatro a través de IPSec SA sin errores. Una SA entrante con SPI 0x9B60EDC5 y una SA saliente con SPI 0x8E7A2E12 se instalan según lo esperado.

También puede verificar que los datos pasan a través del túnel a través de una comprobación del **vpn-sessiondb l2l** entradas:

```
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: y Bytes Rx: show sent and received data counters over the IPSec SA.

Troubleshoot

Paso 1. Verifique que ASA reciba el tráfico para la VPN en la interfaz interna destinada a la red privada de Azure. Para probar, puede configurar un ping continuo desde un cliente interno y configurar una captura de paquetes en ASA para verificar que se reciba:

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

show capture [cap-name]

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

2 packets captured

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

Si se ve el tráfico de respuesta de Azure, la VPN se genera correctamente y envía/recibe tráfico.

Si el tráfico de origen está ausente, verifique que su remitente esté ruteando correctamente al ASA.

Si se ve tráfico de origen pero no hay tráfico de respuesta de Azure, continúe para verificar por qué.

Paso 2. Verifique que el tráfico recibido en la interfaz interna de ASA sea procesado correctamente por ASA y enrutado en la VPN:

Para simular una solicitud de eco ICMP:
packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8.0 [azure-host-ip] detail

Las pautas de uso completas del rastreador de paquetes se pueden encontrar aquí:
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
```

Tenga en cuenta que la NAT exime el tráfico (no se aplica ninguna traducción). Verifique que no se produzca ninguna traducción NAT en el tráfico VPN.

Además, compruebe el **output-interface** es correcto: debe ser la interfaz física en la que se aplica el mapa criptográfico o la interfaz de túnel virtual.

Asegúrese de que no se vean caídas de la lista de acceso.

Si se muestra la fase VPN **ENCRYPT: ALLOW** , el túnel ya está construido y puede ver IPSec SA instalado con encaps.

Paso 2.1. Si **ENCRYPT: ALLOW** visto en packet-tracer.

Verifique que la SA IPSec esté instalada y cifre el tráfico con el uso de **show crypto ipsec sa** .

Puede realizar una captura en la interfaz externa para comprobar que se envían paquetes cifrados desde ASA y que se reciben respuestas cifradas desde Azure.

Paso 2.2. Si **ENCRYPT:DROP** visto en packet-tracer.

El túnel VPN aún no se ha establecido pero está en negociación. Se trata de una condición esperada cuando se activa por primera vez el túnel. Ejecute debugs para ver el proceso de negociación de túnel e identificar dónde y si ocurre una falla.

En primer lugar, verifique que se active la versión correcta de IKE y que el proceso ike-common no muestre errores relevantes:

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

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

Si no se ve ningún resultado de depuración ike-common cuando se inicia el tráfico VPN, esto significa que el tráfico se descarta antes de que llegue al proceso crypto o que crypto ikev1/ikev2 no esté habilitado en el cuadro. Vuelva a comprobar la configuración criptográfica y las caídas de paquetes.

Si los debugs ike-common muestran que se activa el proceso crypto, depure la versión configurada de IKE para ver los mensajes de negociación de túnel e identificar dónde ocurre la falla en la construcción de túnel con Azure.

IKEv1

El procedimiento de depuración y análisis completo de ikev1 se puede encontrar aquí.

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

IKEv2

El procedimiento de depuración y análisis completo de ikev2 se puede encontrar aquí.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).