

Configurar VPN baseada em política e baseada em rota do ASA e do FTD para o Microsoft Azure

Contents

[Introduction](#)

[Conceitos](#)

[Domínio de criptografia VPN](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração de IKEv1 no ASA](#)

[IKEv2 baseado em rota com VTI no ASA Code 9.8 \(1\) ou posterior](#)

[Configuração de IKEv1 no FTD](#)

[IKEv2 baseado em rota com seletores de tráfego baseados em política](#)

[Verificar](#)

[Fase 1](#)

[Fase 2](#)

[Troubleshoot](#)

[IKEv1](#)

[IKEv2](#)

Introduction

Este documento descreve os conceitos e a configuração de uma VPN entre o Cisco ASA e o Cisco Secure Firewall e os Serviços em Nuvem do Microsoft Azure.

Conceitos

Domínio de criptografia VPN

O IPSec de intervalo de endereços IP permite participar do túnel VPN. O domínio de criptografia é definido com o uso de um seletor de tráfego local e seletor de tráfego remoto para especificar quais intervalos de sub-rede local e remoto são capturados e criptografados pelo IPSec. Há dois métodos para definir os domínios de criptografia VPN: seletores de tráfego baseados em rota ou em políticas.

Baseado em rota:

O domínio de criptografia é definido para permitir qualquer tráfego que entre no túnel IPSec. IPSec Os seletores de tráfego local e remoto são definidos como 0.0.0.0. Isso significa que qualquer tráfego roteado para o túnel IPSec é criptografado, independentemente da sub-rede de origem/destino.

O Cisco Adaptive Security Appliance (ASA) suporta VPN baseada em rota com o uso de interfaces de túnel virtual (VTIs) nas versões 9.8 e posteriores.

O Cisco Secure Firewall ou Firepower Threat Defense (FTD) gerenciado pelo FMC (Firepower Management Center) oferece suporte a VPN baseada em rota com o uso de VTIs nas versões 6.7 e posteriores.

Com base em políticas:

O domínio de criptografia está definido para criptografar apenas intervalos de IP específicos para origem e destino. Os seletores de tráfego local baseados em política e os seletores de tráfego remoto identificam o tráfego a ser criptografado no IPsec.

O ASA suporta VPN baseada em políticas com mapas de criptografia na versão 8.2 e posterior.

O Microsoft Azure oferece suporte a roteadores baseados em política ou roteadores com seletores de tráfego simulados baseados em política. No momento, o Azure restringe qual versão do Internet Key Exchange (IKE) você pode configurar com base no método VPN selecionado. A rota baseada requer IKEv2 e a política baseada requer IKEv1. Isso significa que, se IKEv2 for usado, a rota baseada no Azure deverá ser selecionada e o ASA deverá usar um VTI, mas se o ASA só oferecer suporte a mapas de criptografia devido à versão do código, o Azure deverá ser configurado para a rota baseada em seletores de tráfego baseados em política. Isso é realizado no portal do Azure via implantação de script do PowerShell para implementar uma opção que a Microsoft chama UsePolicyBasedTrafficSelectors como explicado aqui:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>.

Para resumir da perspectiva de configuração do ASA e do FTD:

- Para o ASA/FTD configurado com um mapa de criptografia, o Azure deve ser configurado para VPN baseada em política ou baseada em rota com UsePolicyBasedTrafficSelectors.
- Para o ASA configurado com um VTI, o Azure deve ser configurado para VPN baseada em rota.
- Para FTD, mais informações sobre como configurar VTIs podem ser encontradas aqui; 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

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Para VPN baseada em rota IKEv2 que usa VTI no ASA: Código ASA versão 9.8(1) ou posterior. (O Azure deve ser configurado para VPN baseada em rota.)
- Para VPN baseada em política IKEv1 que usa o mapa de criptografia no ASA e no FTD: Código ASA versão 8.2 ou posterior e FTD 6.2.0 ou posterior. (O Azure deve ser configurado para VPN baseada em política.)
- Para VPN baseada em rota IKEv2 que usa mapa de criptografia no ASA com seletores de tráfego baseados em política: Código ASA versão 8.2 ou posterior configurado com um mapa de criptografia. (O Azure deve ser configurado para VPN baseada em rota com

UsePolicyBasedTrafficSelectors.)

- Conhecimento do FMC para a gestão e configuração do FTD.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Conclua as etapas de configuração. Escolha entre configurar IKEv1, IKEv2 baseado em rota com VTI ou IKEv2 baseado em rota com seletores de tráfego baseados em política de uso (mapa de criptografia no ASA).

Configuração de IKEv1 no ASA

Para uma VPN IKEv1 de site a site do ASA para o Azure, siga a próxima configuração do ASA. Certifique-se de configurar um túnel baseado em política no portal do Azure. Os mapas de criptografia são usados no ASA para este exemplo.

Consulte [este documento da Cisco](#) para obter informações completas de configuração do IKEv1 no ASA.

Etapa 1. Ative o IKEv1 na interface externa.

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

Etapa 2. Crie uma política IKEv1 que defina os algoritmos/métodos a serem usados para hash, autenticação, grupo Diffie-Hellman, tempo de vida e criptografia.

Note: Os atributos IKEv1 da fase 1 listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 3. Crie um grupo de túneis sob os atributos IPsec e configure o endereço IP do peer e a chave pré-compartilhada do 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
```

Etapa 4. Criar uma lista de acesso que defina o tráfego a ser criptografado e enviado em túnel. Neste exemplo, o tráfego de interesse é o tráfego do túnel que é originado da sub-rede 10.2.2.0 para 10.1.1.0. Ele pode conter várias entradas se houver várias sub-redes envolvidas entre os sites.

Na versão 8.4 e posteriores, podem ser criados objetos ou grupos de objetos que servem de contêineres para redes, sub-redes, endereços IP de host ou vários objetos. Crie dois objetos que tenham as sub-redes local e remota e use-os para as instruções crypto Access Control List (ACL) e 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
```

Etapa 5. Configure o Transform Set (TS), que deve envolver a palavra-chave IKEv1. Um TS idêntico também deve ser criado na extremidade remota.

Note: Os atributos IKEv1 da fase 2 listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). Para obter mais esclarecimentos, entre em contato com o suporte do Microsoft Azure.

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

Etapa 6. Configure o mapa de criptografia e aplique-o à interface externa, que tem estes componentes:

- O endereço IP do par
- A lista de acesso definida que contenha o tráfego de interesse
- O TS
- A configuração não define o Perfect Forward Secrecy (PFS), pois a [documentação do Azure disponível publicamente](#) declara que o PFS está desabilitado para IKEv1 no Azure. Uma configuração PFS opcional, que cria um novo par de chaves Diffie-Hellman usadas para proteger os dados (ambos os lados devem ser habilitados para PFS antes que a Fase 2 seja ativada), pode ser habilitada através do uso desta configuração: `crypto map outside_map 20 set pfs`.
- Os tempos de vida de IPsec da fase 2 definidos são baseados na [documentação disponível publicamente no Azure](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 7. Certifique-se de que o tráfego VPN não esteja sujeito a nenhuma outra regra NAT. Crie uma regra de isenção 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
```

Observação: quando várias sub-redes são usadas, você deve criar grupos de objetos com todas as sub-redes de origem e destino e usá-las na regra 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
```

IKEv2 baseado em rota com VTI no ASA Code 9.8 (1) ou posterior

Para uma VPN baseada em rota IKEv2 de site a site no código ASA, siga esta configuração. Verifique se o Azure está configurado para VPN baseada em rota e não configure UsePolicyBasedTrafficSelectors no portal do Azure. Um VTI é configurado no ASA.

Consulte [este documento da Cisco](#) para obter informações completas sobre a configuração do ASA VTI.

Etapa 1. Ativar o IKEv2 na interface externa:

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

Etapa 2. Adicionar uma política da fase 1 do IKEv2.

Observação: a Microsoft publicou informações que estão em conflito com relação aos atributos de criptografia, integridade e vida útil da fase 1 do IKEv2 específicos usados pelo Azure. Os atributos listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). As informações que entram em conflito com o atributo IKEv2 da Microsoft estão [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 3. Adicionar uma proposta de IKEv2 fase 2 do IPsec. Especifique os parâmetros de segurança no IPsec de criptografia `ikev2 ipsec-proposal` modo de configuração 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 | nulo}
protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | nulo}
```

Note: A Microsoft publicou informações conflitantes com relação aos atributos de criptografia e integridade IPsec da fase 2 específicos usados pelo Azure. Os atributos listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). As informações que entram em conflito com o atributo IPsec fase 2 da Microsoft são [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 4. Adicione um perfil IPsec que especifique:

- A proposta de IPsec da fase 2 do ikev2 configurada anteriormente
- Tempo de vida de IPsec fase 2 (opcional) em segundos e/ou kilobytes
- O grupo PFS (opcional)

Note: A Microsoft publicou informações conflitantes com relação ao tempo de vida de IPsec da fase 2 e aos atributos de PFS usados pelo Azure. Os atributos listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). As informações que entram em conflito com o atributo IPsec fase 2 da Microsoft são [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 5. Crie um grupo de túneis sob os atributos de IPsec e configure o endereço IP do peer e a chave pré-compartilhada do túnel local e remoto de 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
```

Etapa 6. Criar um VTI que especifique:

- Um novo número de interface de túnel: `interface tunnel [number]`
- Um novo nome de interface de túnel: `nameif [nome]`
- Um endereço IP não existente deve existir na interface de túnel: `ip address [endereço-ip] [máscara]`
- Interface de origem do túnel onde a VPN termina localmente: `tunnel source interface [int-name]`
- O endereço IP do gateway do Azure: destino do túnel [`IP Público do Azure`]
- Modo IPsec IPv4: `tunnel mode ipsec ipv4`
- O perfil IPsec a ser usado para este 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
```

Etapa 7. Criar uma rota estática para apontar o tráfego para o túnel. Para adicionar uma rota estática, digite este comando:

```
route if_name dest_ip mask gateway_ip [distance]
```

O `dest_ip` e `mask` é o endereço IP para a rede de destino na nuvem do Azure, por exemplo, 10.0.0.0/24. O `gateway_ip` precisa ser qualquer endereço IP (existente ou não existente) na sub-rede da interface do túnel, como 169.254.0.2. A finalidade deste `gateway_ip` é apontar o tráfego para a interface do túnel, mas o próprio IP do gateway não é importante.

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

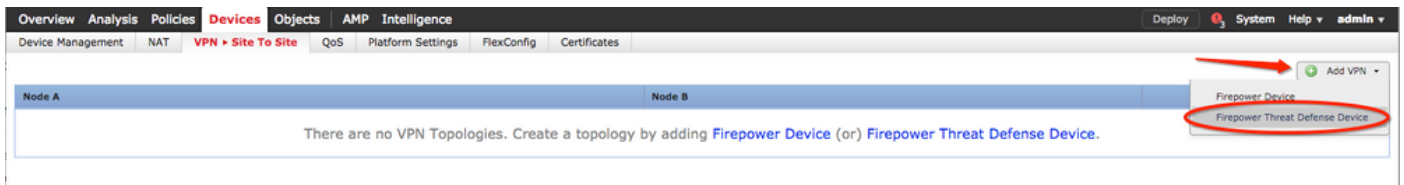
Configuração de IKEv1 no FTD

Para uma VPN IKEv1 de site a site do FTD para o Azure, você precisa ter registrado anteriormente o dispositivo FTD para o FMC.

Etapa 1. Criar uma política Site a Site. Navegue até a página **FMC dashboard > Devices > VPN > Site to Site**.

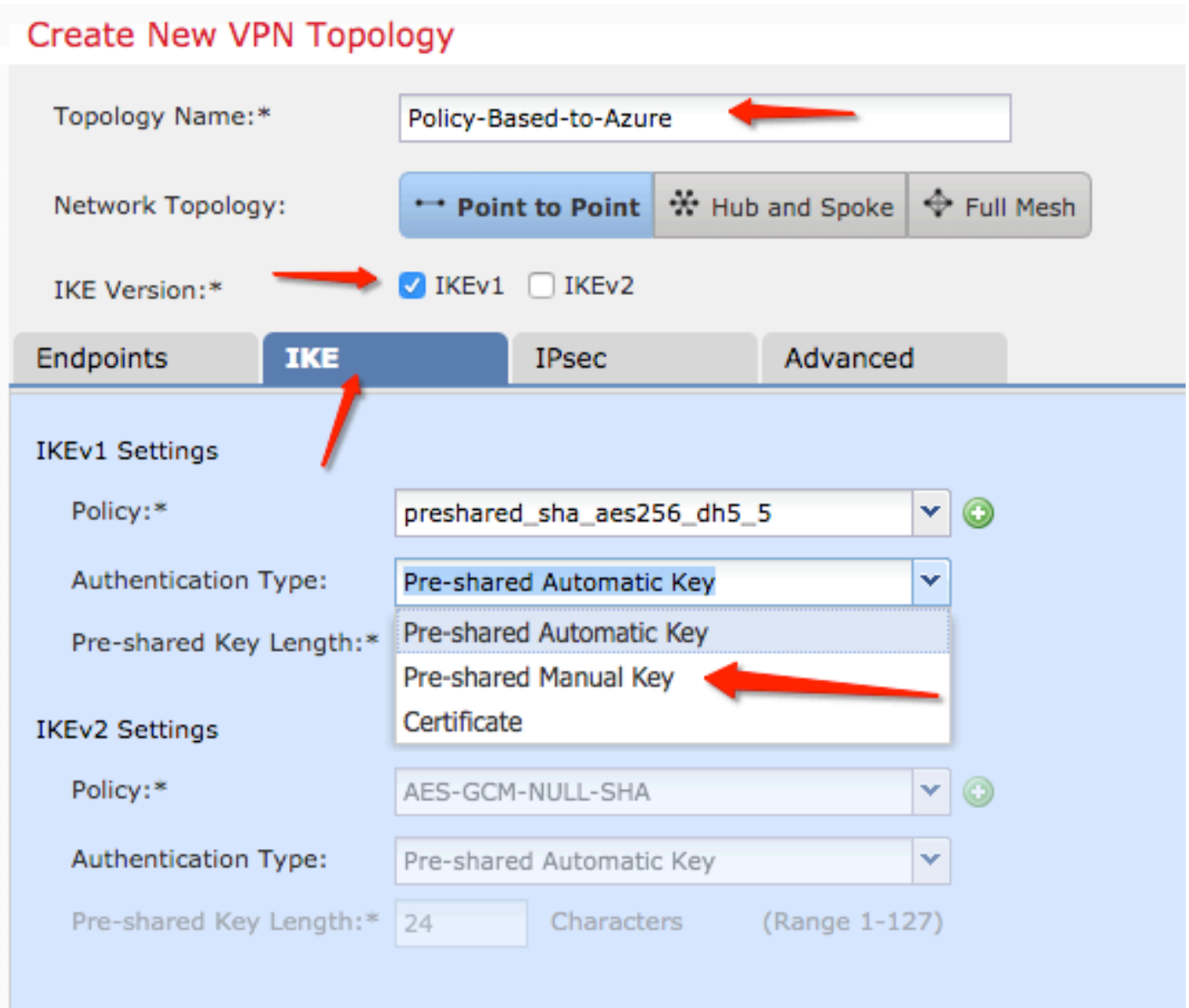


Etapa 2. Criar uma nova política. Clique no botão **Add VPN** e escolha **Firepower Threat Defense device**.



Etapa 3. No **Create new VPN Topology** , especifique seu **Topology Name**, verifique a **IKEV1** protocolo e clique no botão **IKE** guia. Neste exemplo, as chaves pré-compartilhadas são usadas como um método de autenticação.

Clique no botão **Authentication Type** e selecione **Pre-shared manual key** . Digite a chave pré-compartilhada manual no **Key** e **Confirm Key** campos de texto.



Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5 +

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Etapa 4. Configure a política ISAKMP ou os parâmetros da Fase 1 com a criação de uma nova. Na mesma janela, clique no botão **green plus button** para adicionar uma nova política de ISAKMP. Especifique o nome da política, escolha os métodos desejados de criptografia, hash, grupo Diffie-Hellman, tempo de vida e método de autenticação e clique em **Save** .

Create New VPN Topology

Topology Name:* Policy-Based-to-Azure

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5 +

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA +

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

New IKEv1 Policy

Name:* Azure-policy-based

Description:

Priority: (1-65535)

Encryption:* 3des

Hash:* SHA

Diffie-Hellman Group:* 2

Lifetime:* 86400 seconds (120-2147483647)

Authentication Method:* Preshared Key

Save Cancel

Etapa 5. Configurar a política IPsec ou os parâmetros da fase 2. Navegue até a página **IPsec** , escolha **Static** no **Crypto Map Type** caixa de seleção. Clique no botão **edit pencil ícone** da **IKEV1 IPsec Proposals** NO **Transform Sets** opção.

Create New VPN Topology

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh


IKE Version:* IKEv1 IKEv2


Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets:

IKEv1 IPsec Proposals* 

IKEv2 IPsec Proposals 

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

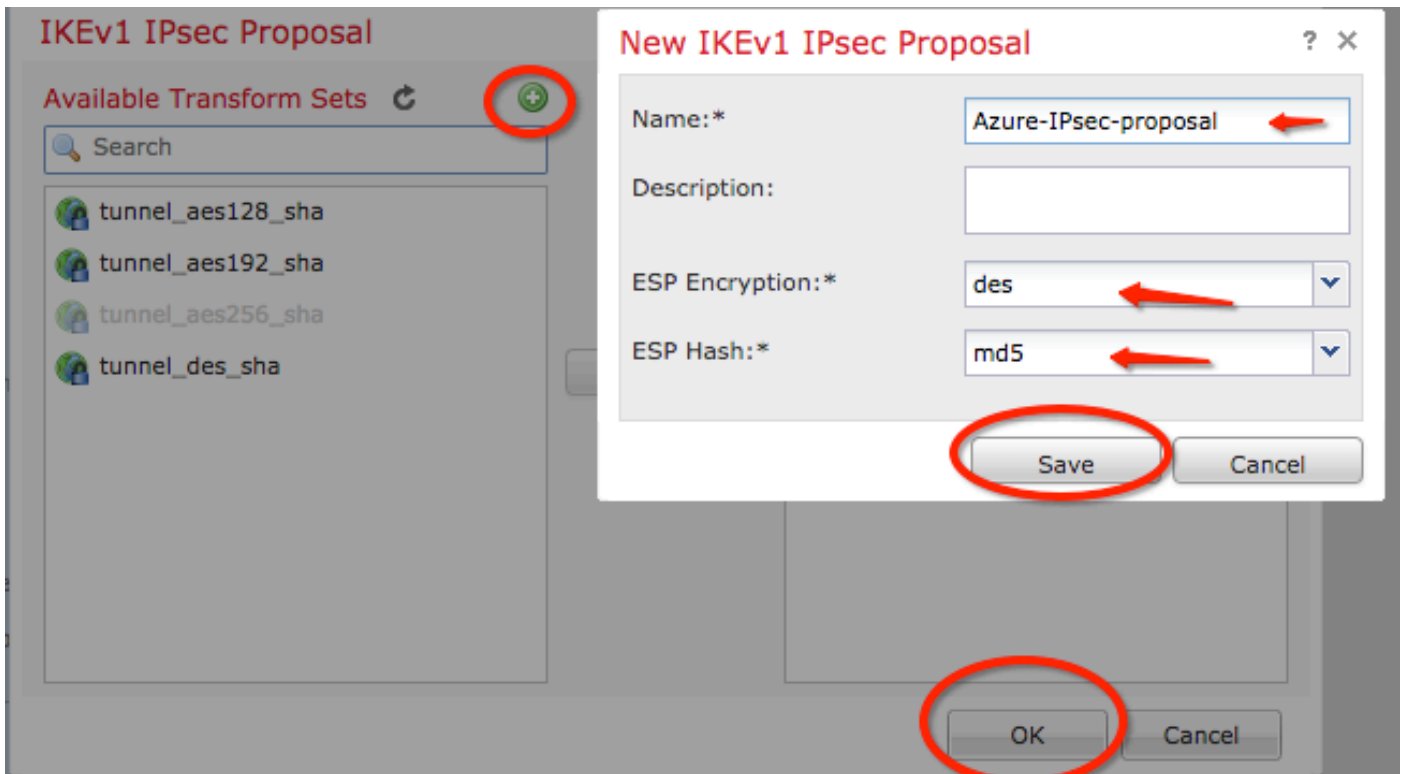
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

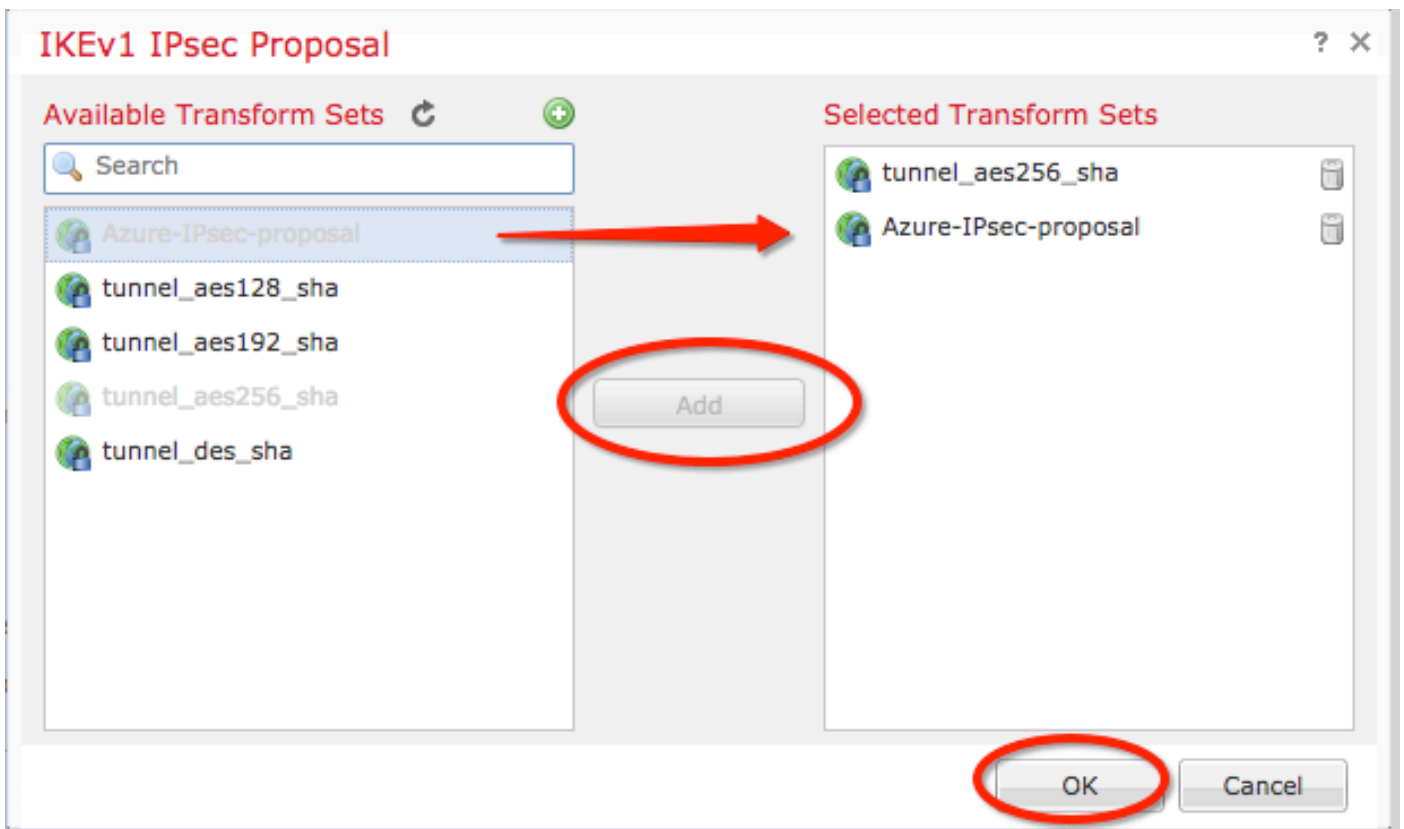
Lifetime Size: Kbytes (Range 10-2147483647)

ESPv3 Settings

Etapa 6. Criar uma nova proposta de IPsec. Na guia **IKEv1 IPsec Proposal** clique no botão **green plus button** para adicionar um novo. Especifique o nome da política e seus parâmetros desejados para os algoritmos de criptografia ESP e hash ESP e clique em **save**.



Passo 7. Na guia IKEV1 IPsec Proposal , adicione sua nova diretiva IPsec à Selected Transform Sets e clique em OK .



Etapa 8. Voltar à página IPsec configure a Duração e o Tamanho de Vida Útil desejados.

Create New VPN Topology

Topology Name:* Policy-Based-to-Azure

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

IPsec Endpoints IKE Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals* IKEv2 IPsec Proposals

tunnel_aes256_sha
Azure-IPsec-proposal

AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

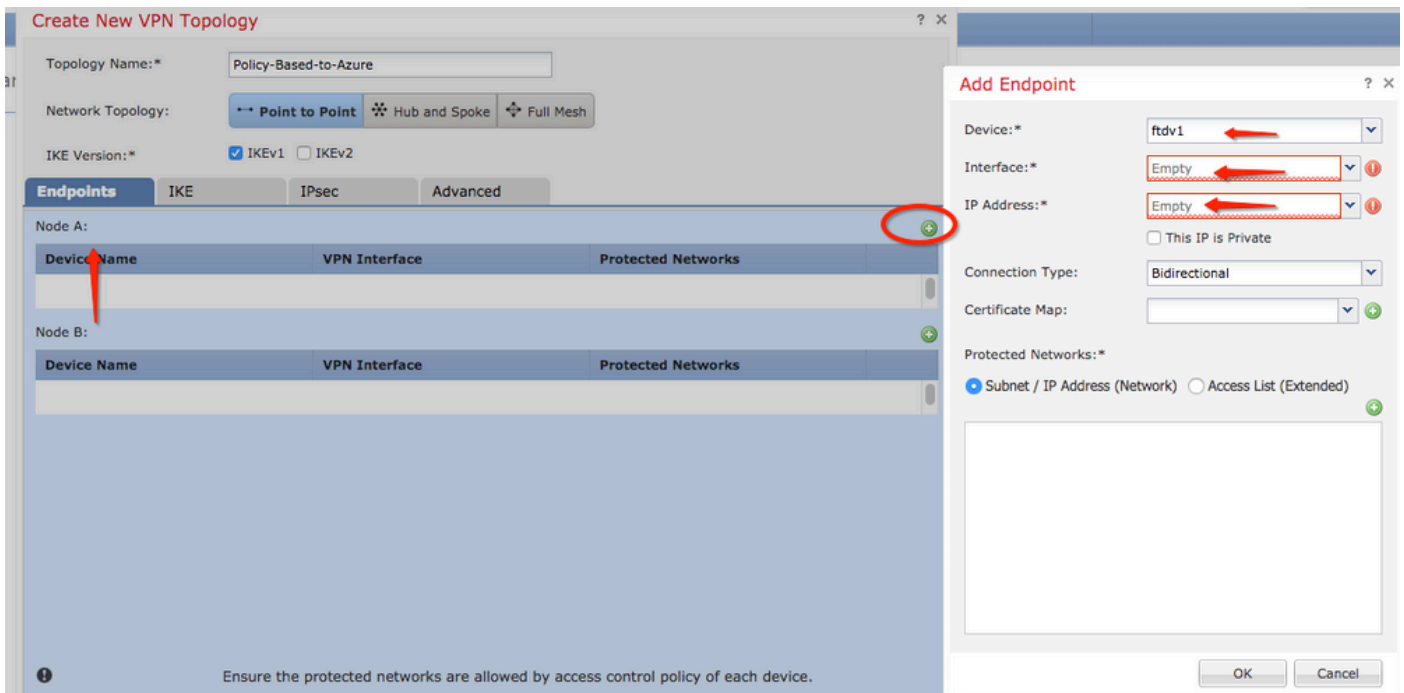
Modulus Group: 2

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

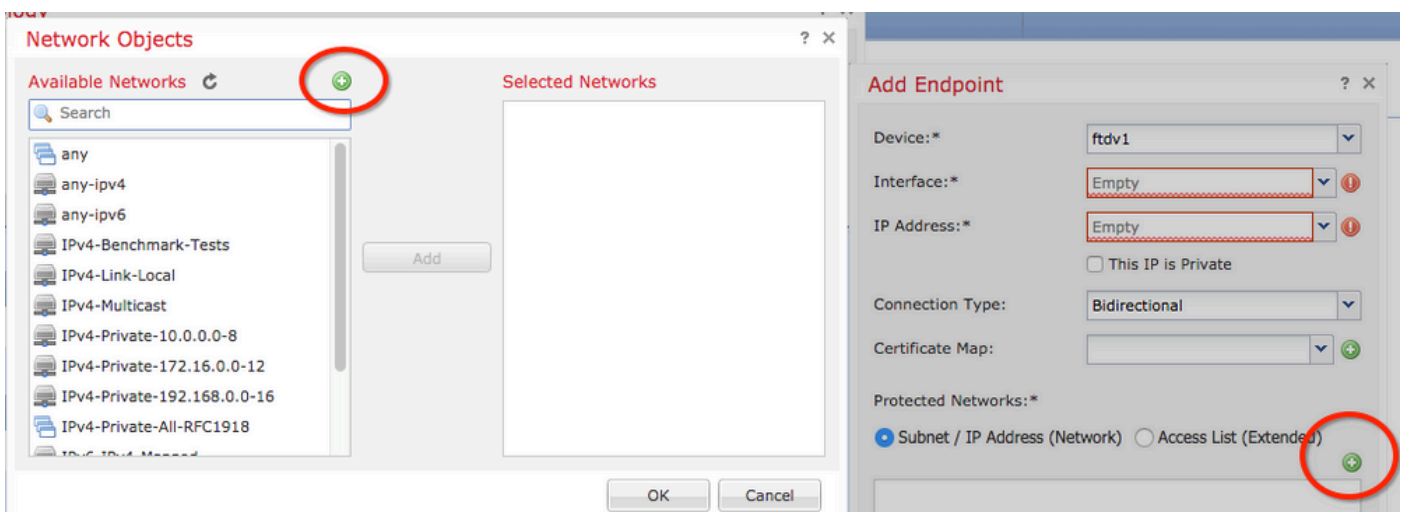
Etapa 9. Escolha o domínio de criptografia/seletores de tráfego/redes protegidas. Navegue até a página Endpoints guia. Na guia Node A clique no botão green plus button para adicionar um novo. Neste exemplo, o Nó A é usado como sub-redes locais para o FTD.



Etapa 10. Na guia **Add Endpoint** , especifique o FTD a ser usado no **Device** juntamente com a interface física e o endereço IP a serem usados.

Etapa 11. Para especificar o seletor de tráfego local, navegue até o **Protected Networks** e clique no botão **green plus button** para criar um novo objeto.

Etapa 12. No **Network Objects** clique no botão **green plus button** ao lado do **Available Networks** para criar um novo objeto seletor de tráfego local.



Etapa 13. No **New Network Object** especifique o nome do objeto e escolha adequadamente **host/rede/intervalo/FQDN**. Em seguida, clique em **save** .

New Network Object

Name:

Description:

Network: Host Range Network FQDN

Allow Overrides:

Save Cancel

Etapa 14. Adicionar o objeto ao Selected Networks no Network Objects e clique em OK . Clique em OK no Add Endpoint janela.

Network Objects

Available Networks

- local-ftd
- any
- any-ipv4
- any-ipv6
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918

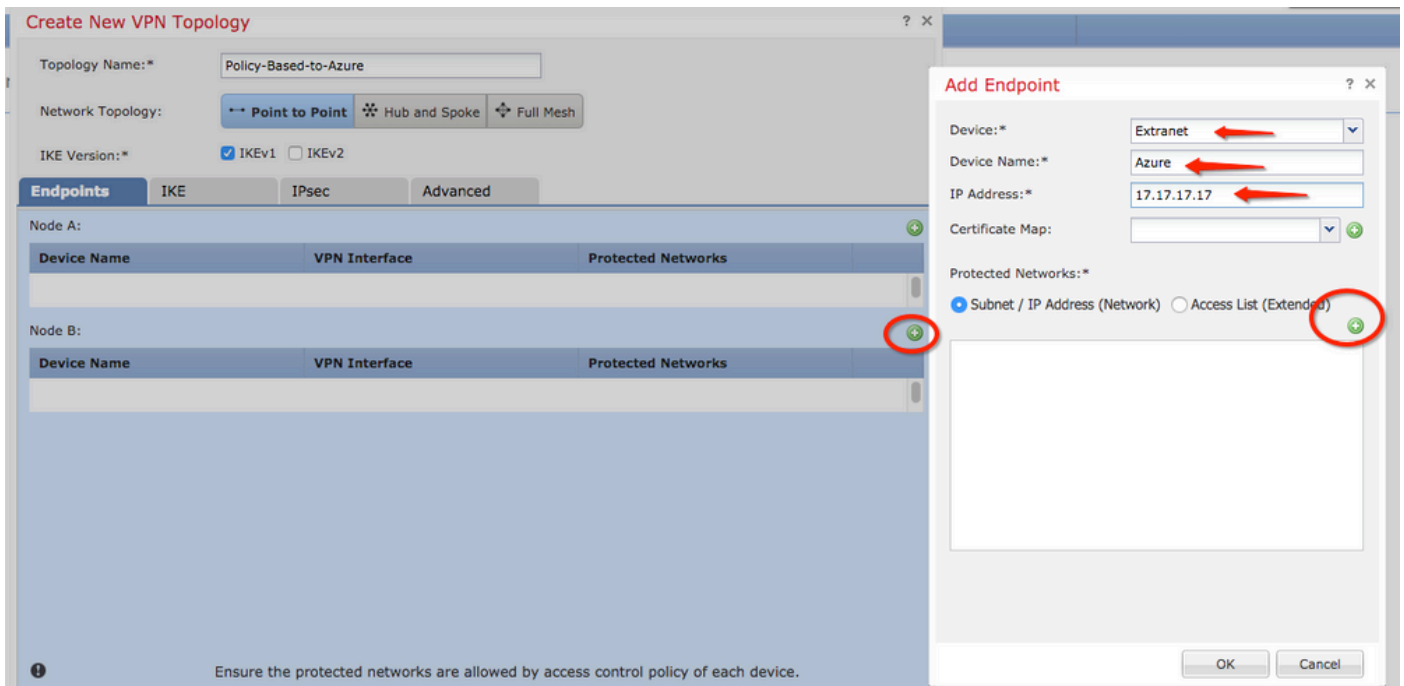
Add

Selected Networks

- local-ftd

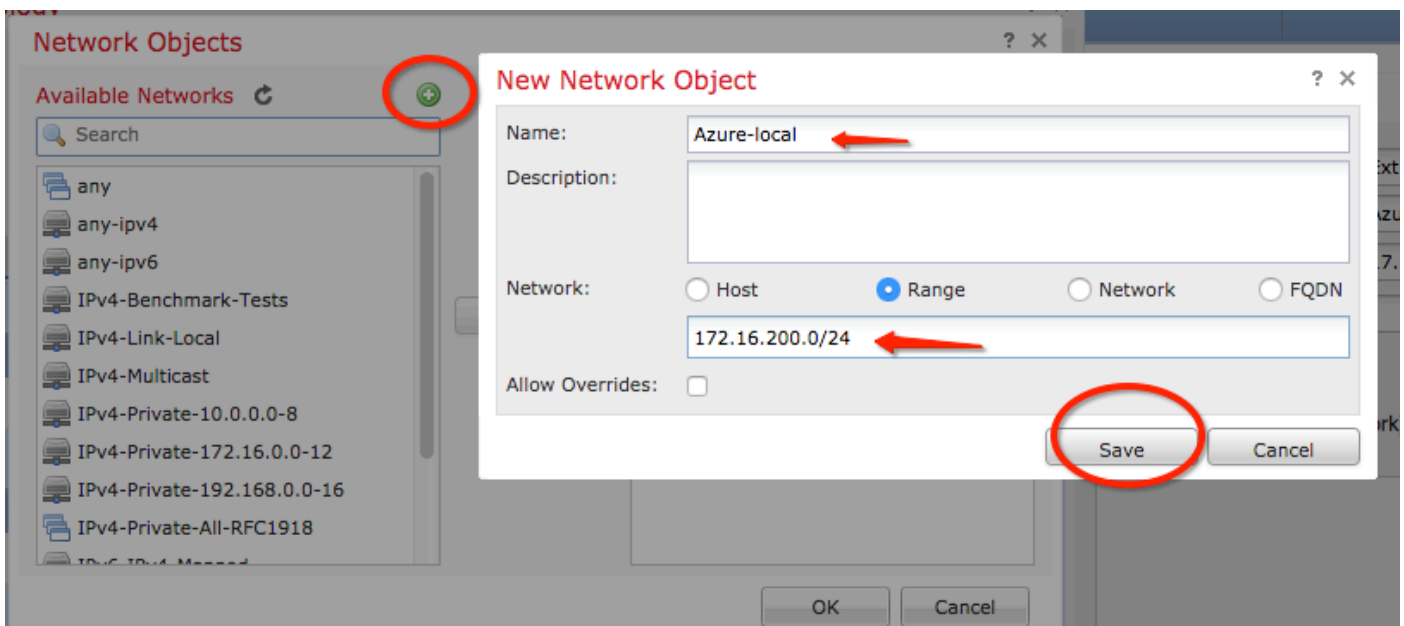
OK Cancel

Etapa 15. Defina o ponto de extremidade do Nó B, que, neste exemplo, é o ponto de extremidade do Azure. Na guia Create New VPN Topology navegue até a janela Node B e clique no botão green plus button para adicionar o seletor de tráfego de endpoint remoto. Especificar Extranet para todos os endpoints de peer da VPN que não são gerenciados pelo mesmo FMC que o Node A. Digite o nome do dispositivo (significativo localmente apenas) e seu endereço IP.

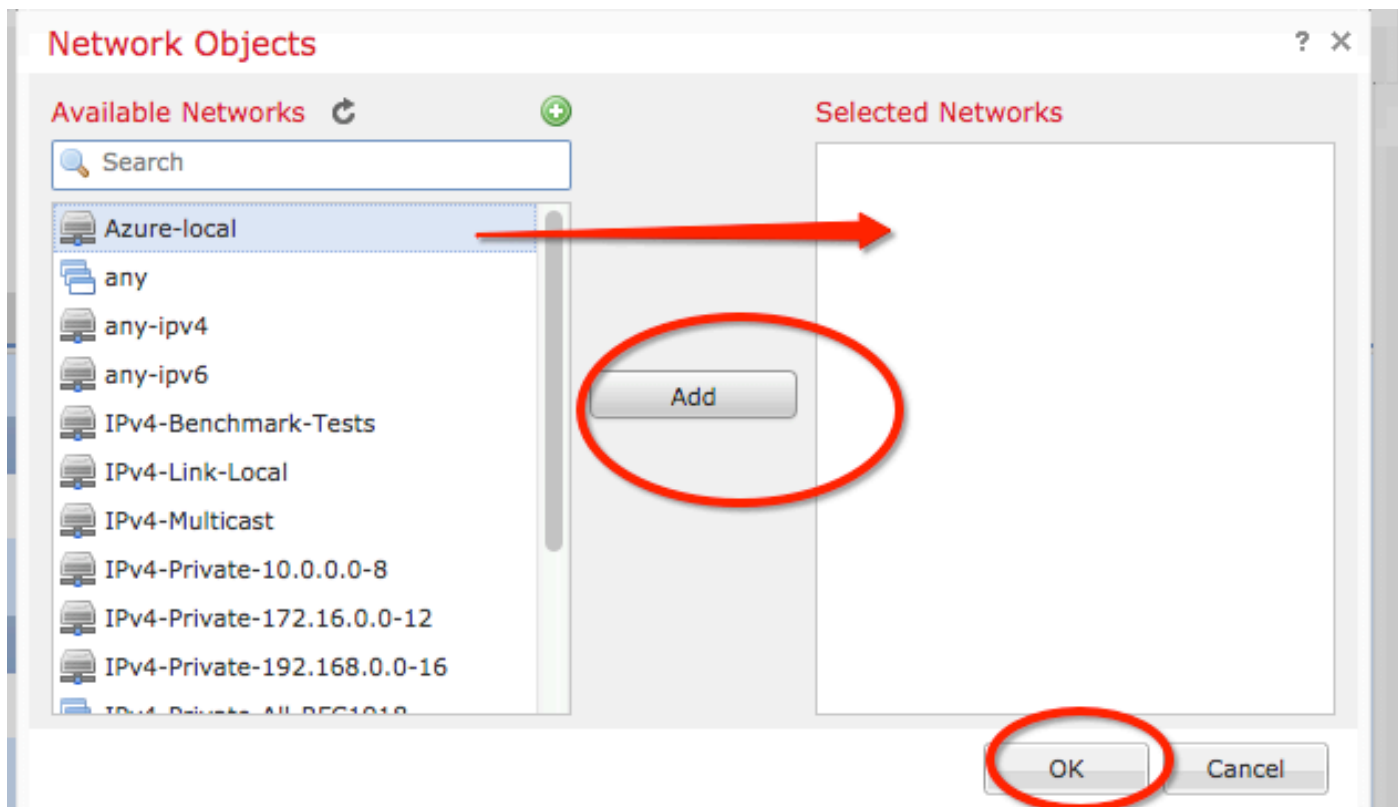


Etapa 16. Criar o objeto seletor de tráfego remoto. Navegue até a página **Protected Networks** e clique no botão **green plus button** para adicionar um novo objeto.

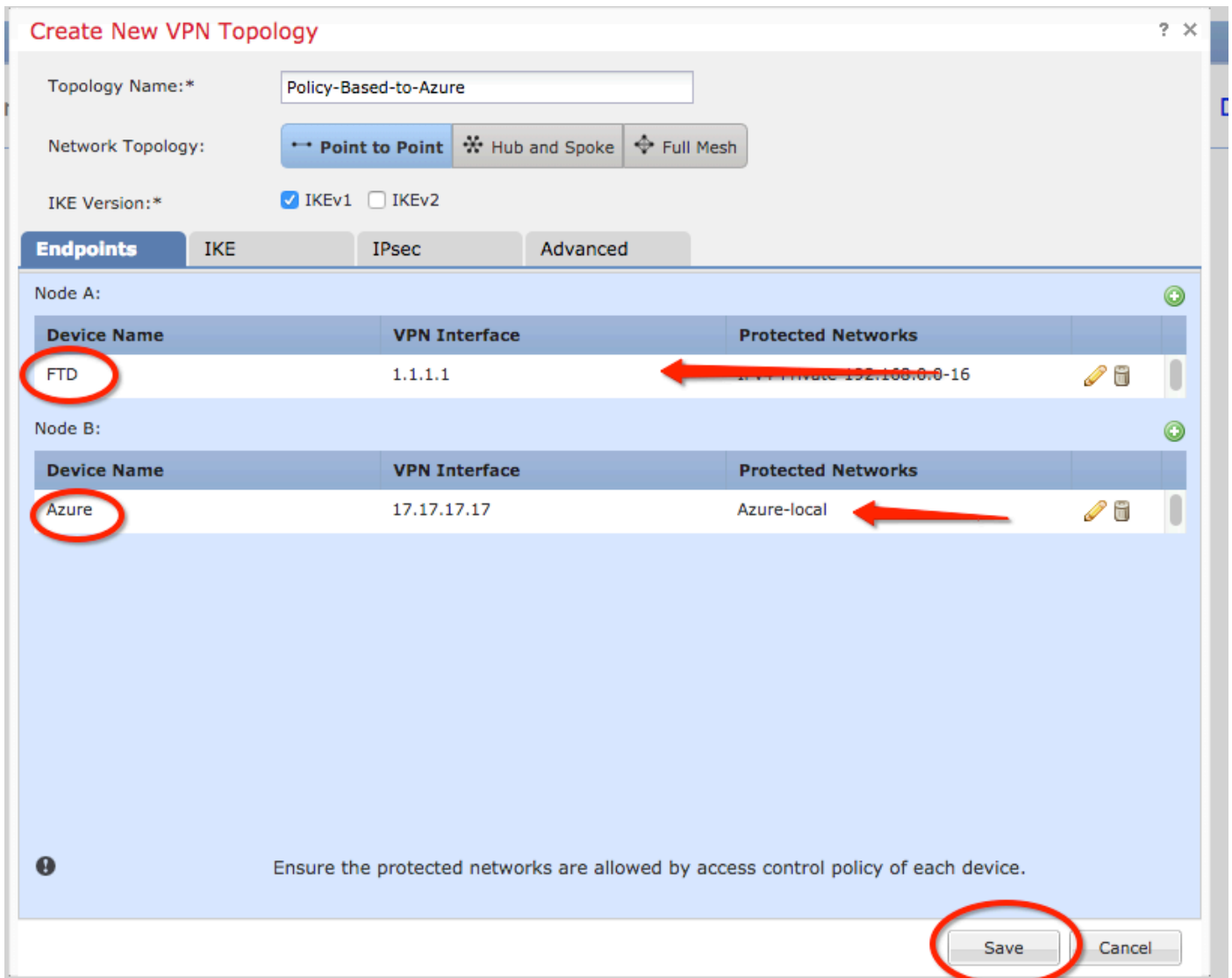
Etapa 17. No **Network Objects** clique no botão **green plus button** ao lado do **Available Networks** texto para criar um novo objeto. Na guia **New Network Object** especifique o nome do objeto e escolha adequadamente **host/intervalo/rede/FQDN** e clique em **Save**.



Etapa 18. Voltar à página **Network Objects**, adicione seu novo objeto remoto à **Selected Networks** e clique em **OK**. Clique em **OK** no **Add Endpoint** janela.



Etapa 19. Na guia **Create New VPN Topology** você pode ver agora os dois nós com seus seletores de tráfego/redes protegidas corretos. Clique em **save** .



Etapa 20. No painel do FMC, clique em **Deploy** no painel superior direito, escolha o dispositivo FTD e clique em **Deploy** .

Etapa 21. Na interface de linha de comando, a configuração da VPN é igual à dos dispositivos ASA.

IKEv2 baseado em rota com seletores de tráfego baseados em política

Para uma VPN IKEv2 de site a site no ASA com mapas de criptografia, siga esta configuração. Verifique se o Azure está configurado para VPN baseada em rota e UsePolicyBasedTrafficSelectors deve ser configurado no portal do Azure por meio do uso do PowerShell.

[Este documento](#) da Microsoft descreve a configuração de UsePolicyBasedTrafficSelectors em conjunto com o modo VPN do Azure baseado em rota. Sem a conclusão desta etapa, o ASA com mapas de criptografia não estabelece a conexão devido a uma incompatibilidade nos seletores de tráfego recebidos do Azure.

Consulte [este documento da Cisco](#) para obter informações completas sobre o ASA IKEv2 com informações de configuração de mapa de criptografia.

Etapa 1. Ativar o IKEv2 na interface externa:

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

Etapa 2. Adicionar uma política da fase 1 do IKEv2.

Observação: a Microsoft publicou informações que estão em conflito com relação aos atributos de criptografia, integridade e vida útil da fase 1 do IKEv2 específicos usados pelo Azure. Os atributos listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). As informações de atributo IKEv2 da Microsoft que estão em conflito são [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 3. Crie um grupo de túneis sob os atributos IPsec e configure o endereço IP do peer e a chave pré-compartilhada do túnel local 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
```

Etapa 4. Criar uma lista de acesso que defina o tráfego a ser criptografado e enviado em túnel. Neste exemplo, o tráfego de interesse é o tráfego do túnel que é originado da sub-rede 10.2.2.0 para 10.1.1.0. Ele pode conter várias entradas se houver várias sub-redes envolvidas entre os sites.

Na versão 8.4 e posteriores, podem ser criados objetos ou grupos de objetos que servem de contêineres para redes, sub-redes, endereços IP de host ou vários objetos. Crie dois objetos que tenham as sub-redes local e remota e use-os para as instruções 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
```

Etapa 5. Adicionar uma proposta de IKEv2 fase 2 do IPsec. Especifique os parâmetros de segurança no modo de configuração de criptografia ikev2 ipsec-proposal do IPsec:

```
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 | nulo}
```

protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | nulo}

Observação: a Microsoft publicou informações que estão em conflito com relação aos atributos de criptografia e integridade IPsec da fase 2 específicos usados pelo Azure. Os atributos listados recebem o melhor esforço [deste documento da Microsoft disponível publicamente](#). As informações de atributo IPsec da fase 2 da Microsoft que estiverem em conflito são [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 6. Configure um mapa de criptografia e aplique-o à interface externa, que contém estes componentes:

- O endereço IP do par
- A lista de acesso definida que contenha o tráfego de interesse
- A proposta IKEv2 fase 2 IPsec
- O tempo de vida do IPsec da fase 2 em segundos
- Uma configuração opcional de PFS (Perfect Forward Secrecy), que cria um novo par de chaves Diffie-Hellman usadas para proteger os dados (ambos os lados devem ser habilitados para PFS, antes que a Fase 2 seja iniciada)

A Microsoft publicou informações conflitantes com relação ao tempo de vida de IPsec da fase 2 e aos atributos de PFS usados pelo Azure.

Os atributos listados recebem o melhor esforço da [este documento da Microsoft disponível publicamente](#).

As informações de atributo IPsec da fase 2 da Microsoft que estiverem em conflito são [visíveis aqui](#). Para obter mais esclarecimentos, entre em contato com o suporte do 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
```

Etapa 8. Certifique-se de que o tráfego VPN não esteja sujeito a nenhuma outra regra NAT. Crie uma regra de isenção 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
```

Observação: quando várias sub-redes são usadas, você deve criar grupos de objetos com todas as sub-redes de origem e destino e usá-las na regra 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

```

Verificar

Após concluir a configuração no ASA e no gateway do Azure, o Azure inicia o túnel VPN. Você pode verificar se o túnel é construído corretamente com estes comandos:

Fase 1

Verifique se a SA (Security Association, associação de segurança) da fase 1 foi criada:

IKEv2

Em seguida, uma SA IKEv2 criada a partir do IP 192.168.1.2 da interface externa local na porta UDP 500 para o IP de destino remoto 192.168.2.2 é exibida. Há também uma SA filha válida criada para que o tráfego criptografado flua.

```

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

```

Aqui, uma IKEv1 SA construída com o ASA como o iniciador para peer IP 192.168.2.2 com um tempo de vida restante de 86388 segundos é mostrada.

```

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

Verifique se a associação de segurança IPsec fase 2 foi criada com `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
```

Quatro pacotes são enviados e quatro são recebidos pelo SA IPsec sem erros. Uma AS de entrada com SPI 0x9B60EDC5 e uma SA de saída com SPI 0x8E7A2E12 são instaladas conforme esperado.

Você também pode verificar se os dados passam pelo túnel através de uma verificação do `vpn-sessiondb I2I` entradas:

```
Cisco-ASA#show vpn-sessiondb I2I
```

```
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: e Bytes Rx: show sent and received data counters over the IPsec SA (mostrar contadores de dados enviados e recebidos via SA IPsec).

Troubleshoot

Etapa 1. Verifique se o tráfego para a VPN é recebido pelo ASA na interface interna destinada à rede privada do Azure. Para testar, você pode configurar um ping contínuo de um cliente interno e configurar uma captura de pacote no ASA para verificar se foi recebida:

```
capture [nome-cap] interface [nome-if] match [protocolo] [ip-src] [máscara-src] [ip-dest] [máscara-dest]
```

```
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 o tráfego de resposta do Azure for visto, a VPN será criada corretamente e enviará/receberá tráfego.

Se o tráfego de origem estiver ausente, verifique se o remetente está roteando corretamente para o ASA.

Se o tráfego de origem for visto, mas o tráfego de resposta do Azure estiver ausente, continue para verificar o motivo.

Etapa 2. Verificar se o tráfego recebido na interface interna do ASA é processado corretamente pelo ASA e roteado para a VPN:

Para simular uma solicitação de eco ICMP:

```
packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip] detail
```

As diretrizes completas de utilização do packet tracer podem ser encontradas aqui:

<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=0x7f6c19afela0, 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
```

Observe que o NAT isenta o tráfego (nenhuma conversão entra em vigor). Verifique se nenhuma conversão de NAT ocorre no tráfego VPN.

Verifique também o `output-interface` está correto - deve ser a interface física onde o mapa de criptografia é aplicado ou a interface de túnel virtual.

Certifique-se de que não sejam vistas quedas de listas de acesso.

Se a fase VPN mostrar `ENCRYPT: ALLOW`, o túnel já está construído e você pode ver IPsec SA instalado com encapsulamentos.

Etapa 2.1. Se `ENCRYPT: ALLOW` visto no packet-tracer.

Verifique se o SA do IPsec está instalado e criptografa o tráfego com o uso de `show crypto ipsec sa`.

Você pode executar uma captura na interface externa para verificar se os pacotes criptografados são enviados do ASA e se as respostas criptografadas são recebidas do Azure.

Etapa 2.2. Se `ENCRYPT:DROP` visto no packet-tracer.

O túnel VPN ainda não está estabelecido, mas está em negociação. Essa é uma condição esperada quando você ativa o túnel pela primeira vez. Execute depurações para visualizar o processo de negociação do túnel e identificar onde e se uma falha ocorre.

Primeiro, verifique se a versão correta do IKE é acionada e se o processo `ike-common` não mostra erros 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.
```

Se nenhuma saída de depuração `ike-common` for vista quando o tráfego VPN é iniciado, isso significa que o tráfego é descartado antes de alcançar o processo de criptografia ou `ikev1/ikev2` de criptografia não está habilitado na caixa. Verifique novamente a configuração de criptografia e as quedas de pacotes.

Se as depurações `ike-common` mostrarem que o processo de criptografia é disparado, depure a versão configurada do IKE para exibir mensagens de negociação de túnel e identificar onde a falha ocorre na criação do túnel com o Azure.

IKEv1

O procedimento completo de depuração e análise de `ikev1` pode ser encontrado [aqui](#).

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

IKEv2

O procedimento de depuração e análise ikev2 completo podem ser encontrados [aqui](#).

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

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

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.