Configurar VPN site a site no FTD gerenciado pelo FDM

Contents

Introduction

Este documento descreve como configurar a VPN site a site no Firepower Threat Defense (FTD) gerenciado pelo FirePower Device Manager (FDM).

Contribuído por Cameron Schaeffer, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica da VPN
- Experiência com FDN
- Experiência com a linha de comando Adaptive Security Appliance (ASA)

Componentes Utilizados

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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.

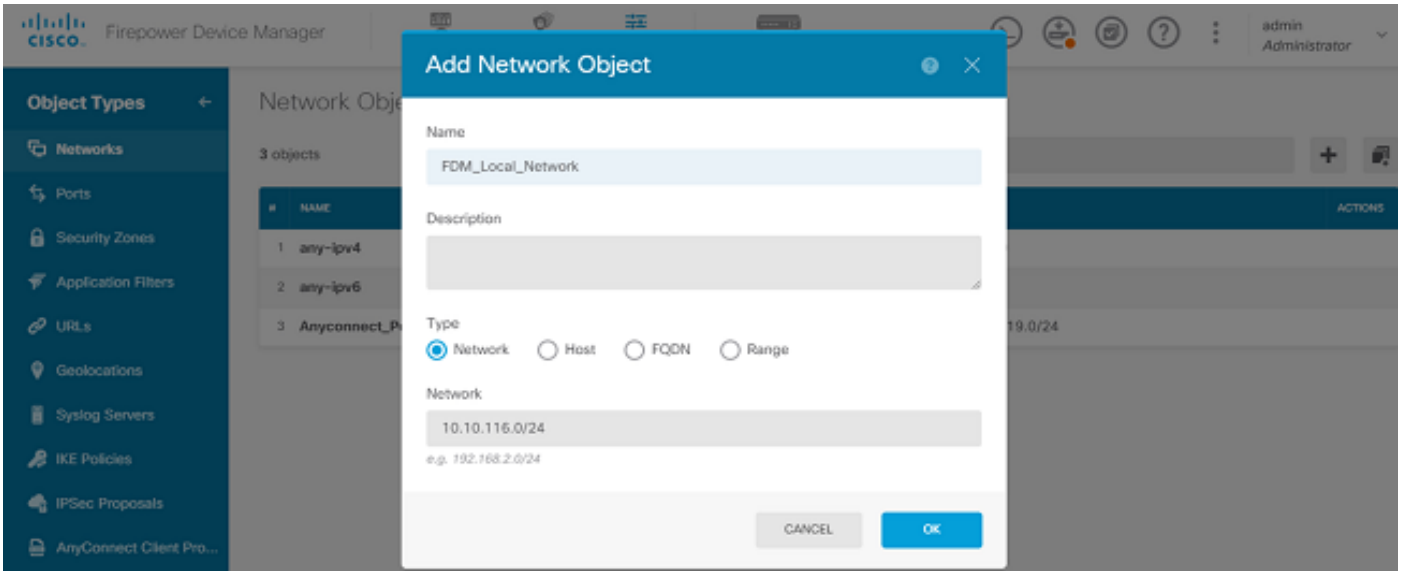
Configurar

Comece com a configuração no FTD com FDM.

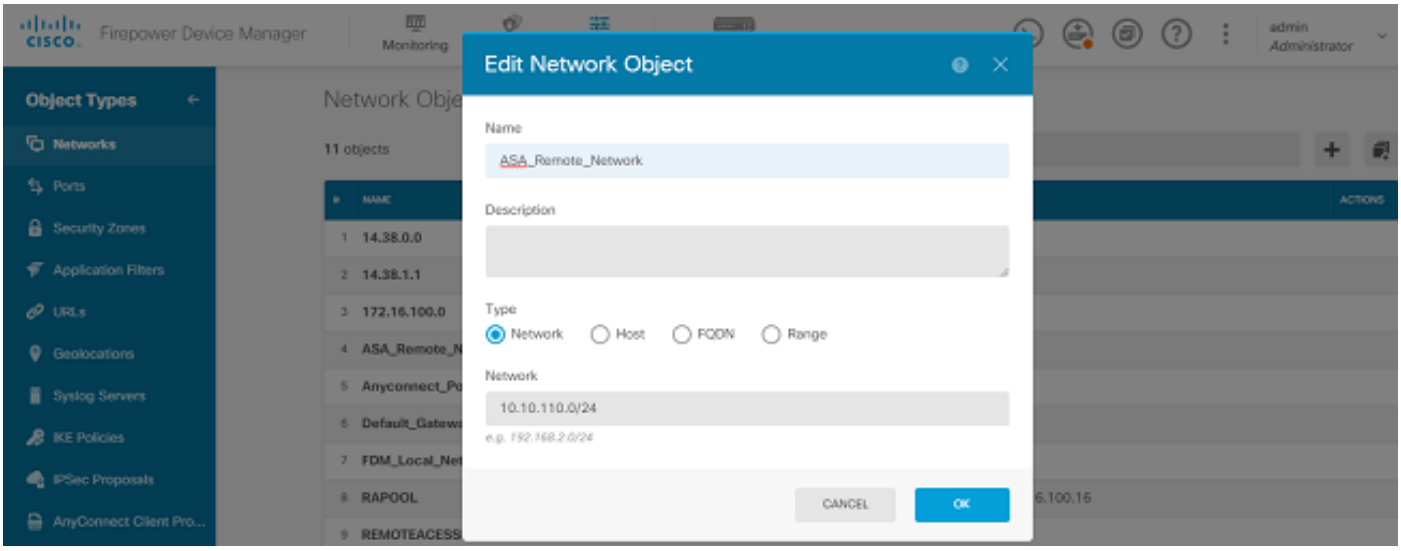
Definir redes protegidas

Navegue até **Objetos > Redes > Adicionar nova rede**.

Configurar objetos para redes LAN a partir da GUI do FDM. Crie um objeto para a rede local atrás do dispositivo FDM, como mostrado na imagem.



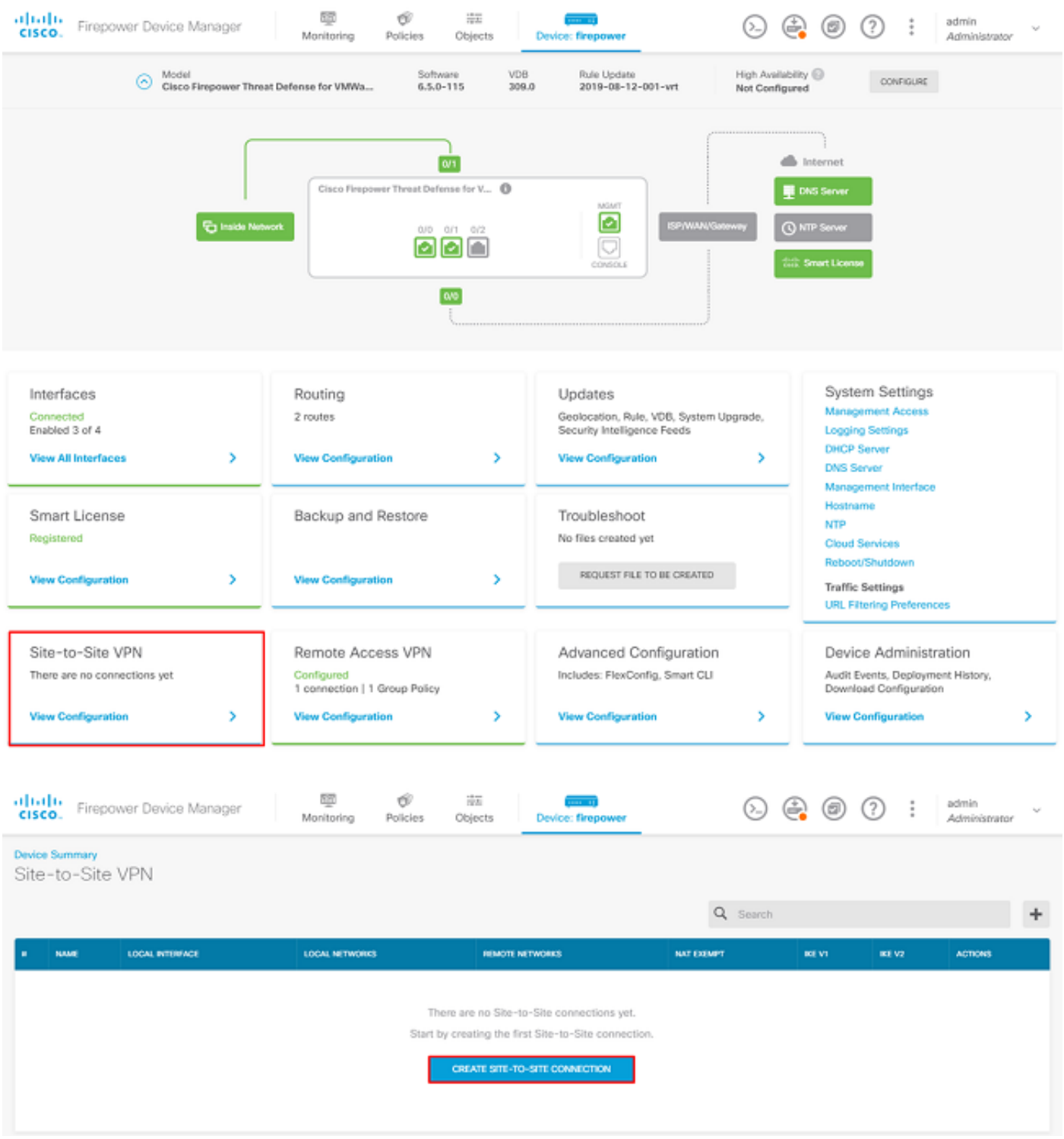
Crie um objeto para a rede remota atrás do dispositivo ASA como mostrado na imagem.



Configurar VPN site a site

Navegue para **VPN site a site > Criar conexão site a site**.

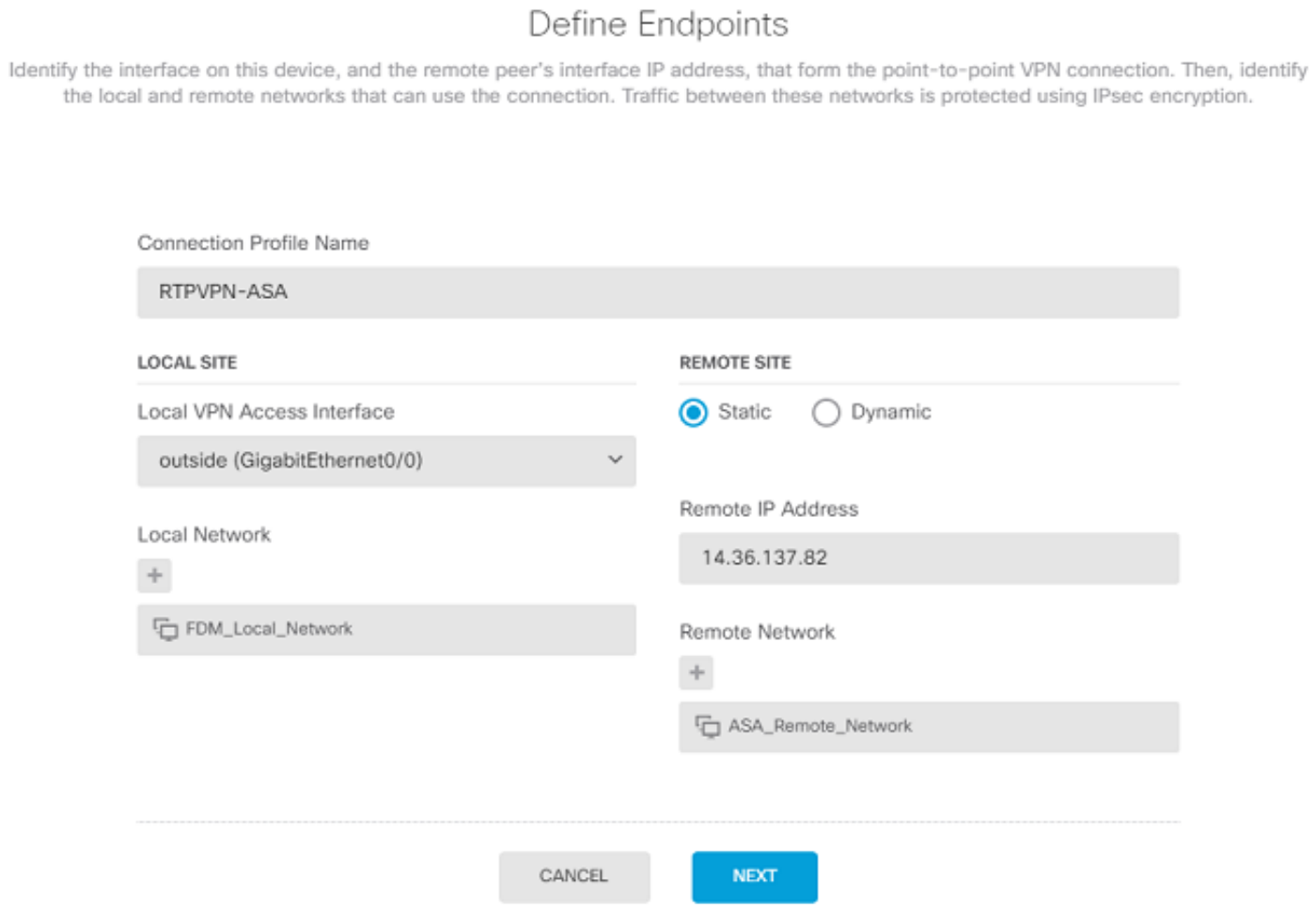
Navegue pelo assistente Site-to-Site no FDM, conforme mostrado na imagem.



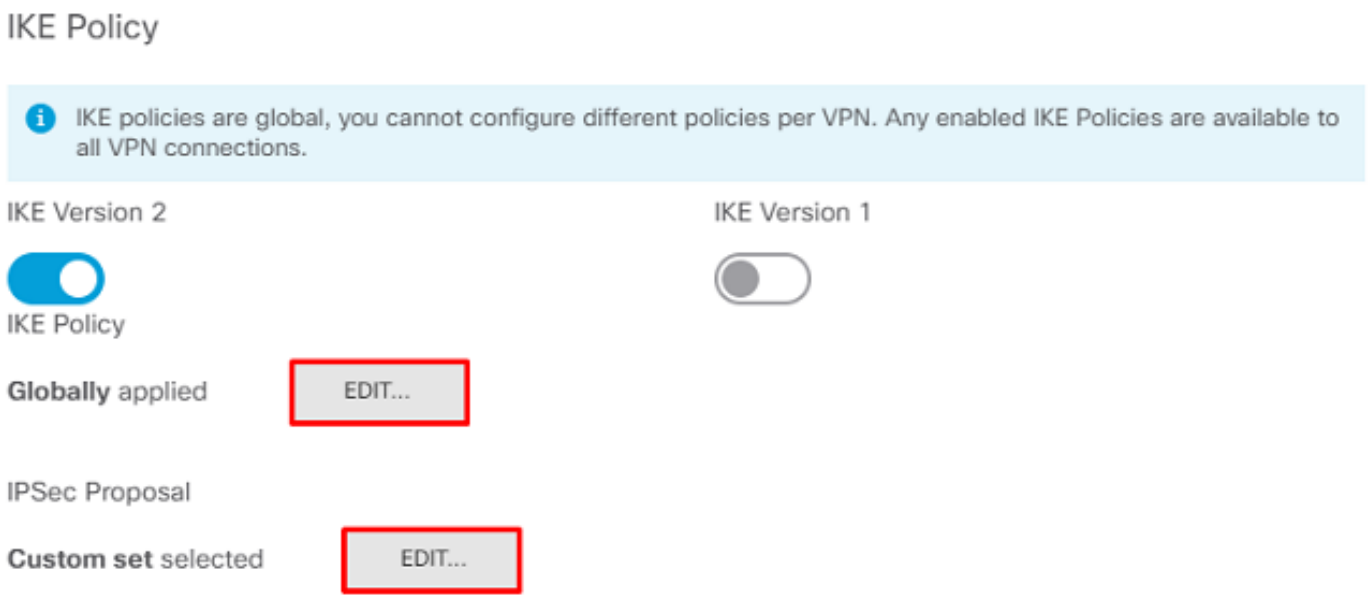
Forneça à conexão Site-to-Site um nome de perfil de conexão que seja facilmente identificável.

Selecione a interface externa correta para o FTD e, em seguida, selecione a rede local que precisará ser criptografada através da VPN site a site.

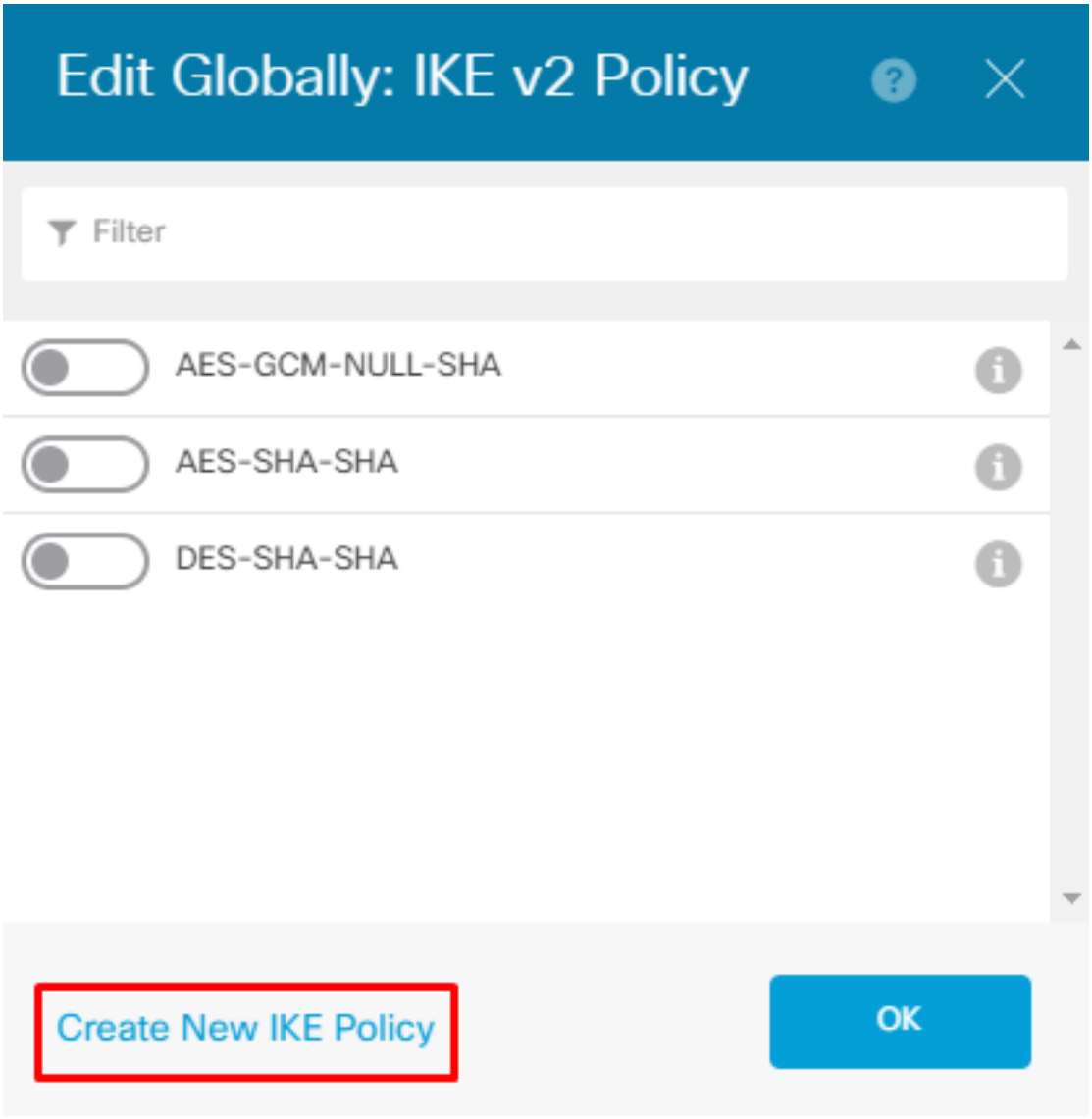
Defina a interface pública do peer remoto. Em seguida, selecione a rede dos peers remotos que serão criptografados através da VPN site a site, como mostrado na imagem.



Na próxima página, selecione o botão **Editar** para definir os parâmetros do Internet Key Exchange (IKE) como mostrado na imagem.

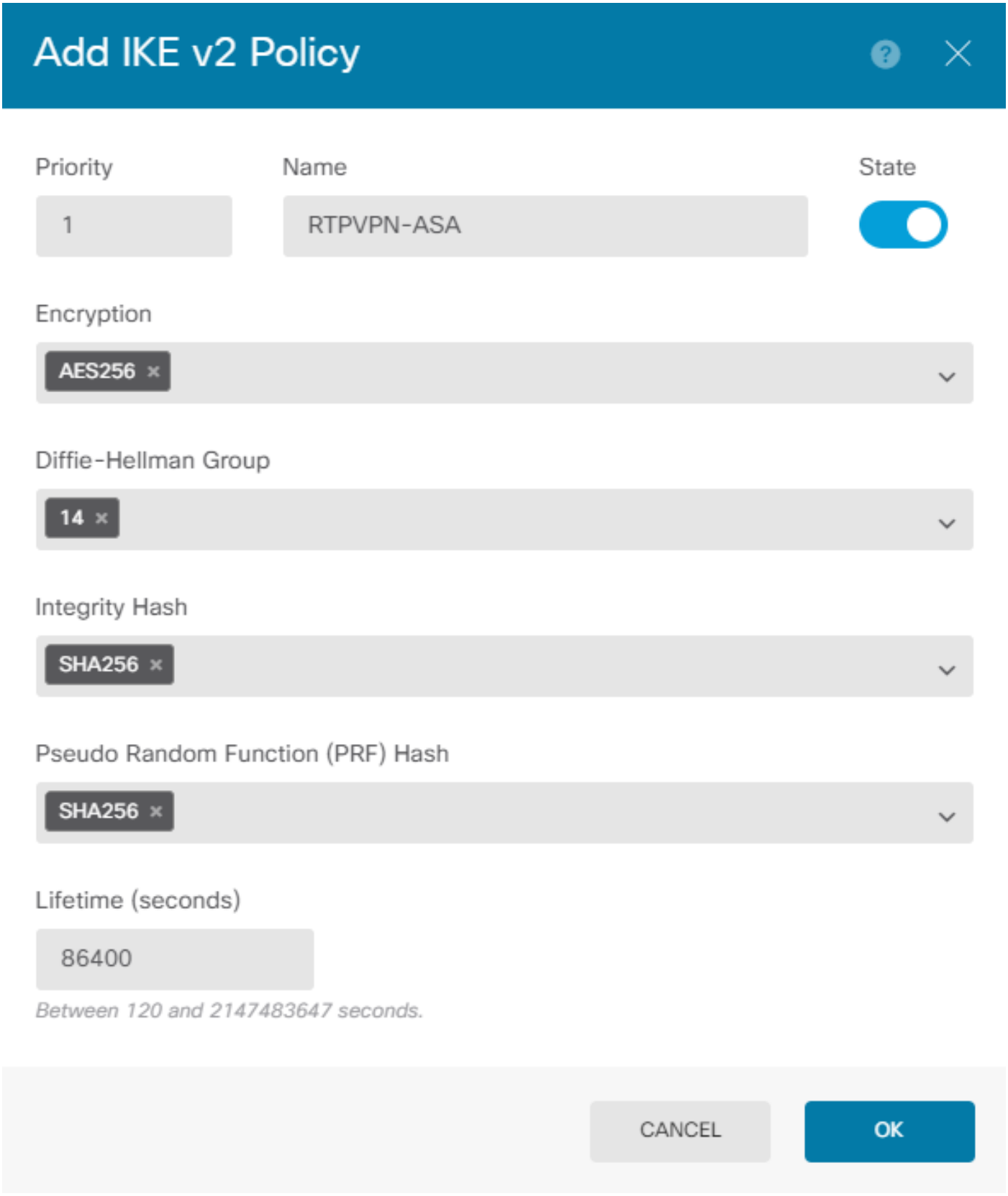


Selecione o botão **Create New IKE Policy** conforme mostrado na imagem.

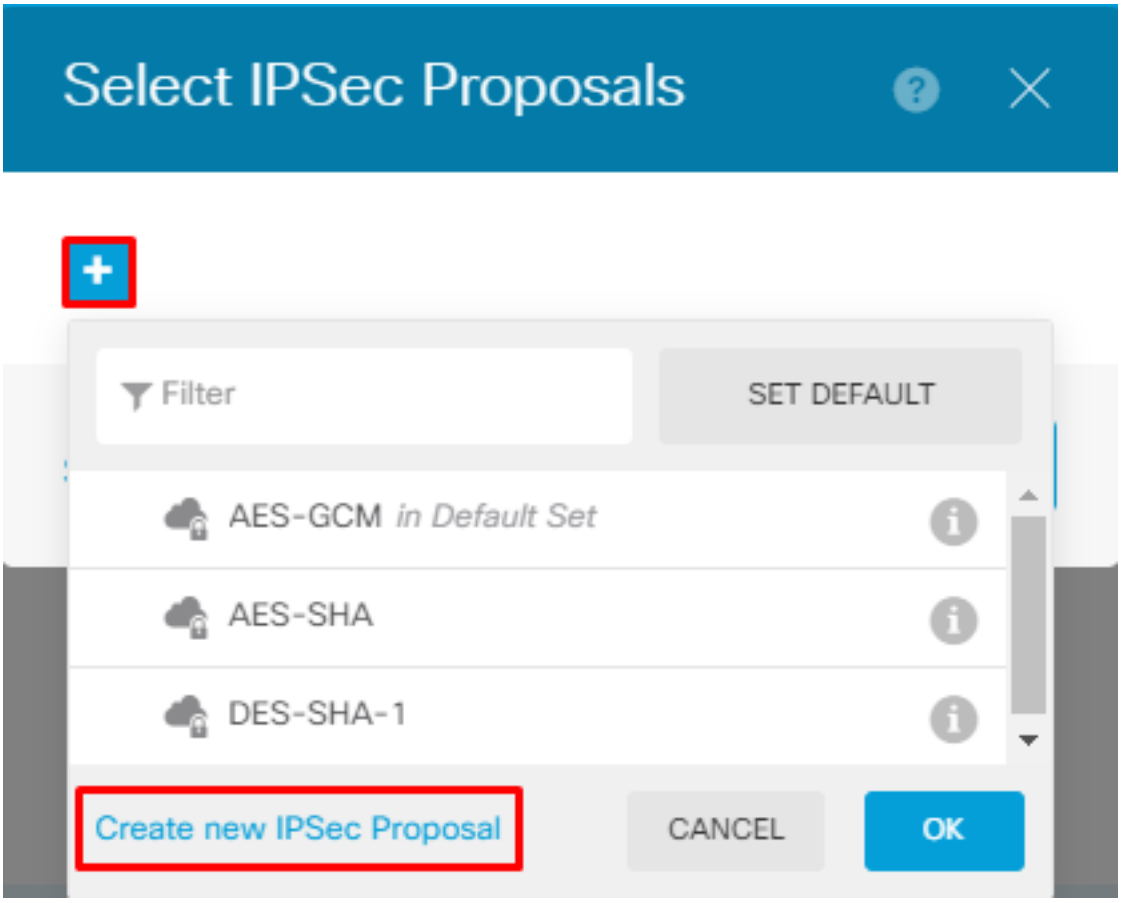


Este guia usa estes parâmetros para a troca inicial de IKEv2:

Criptografia AES-256
Integridade SHA256
Grupo DH 14
PRF SHA256



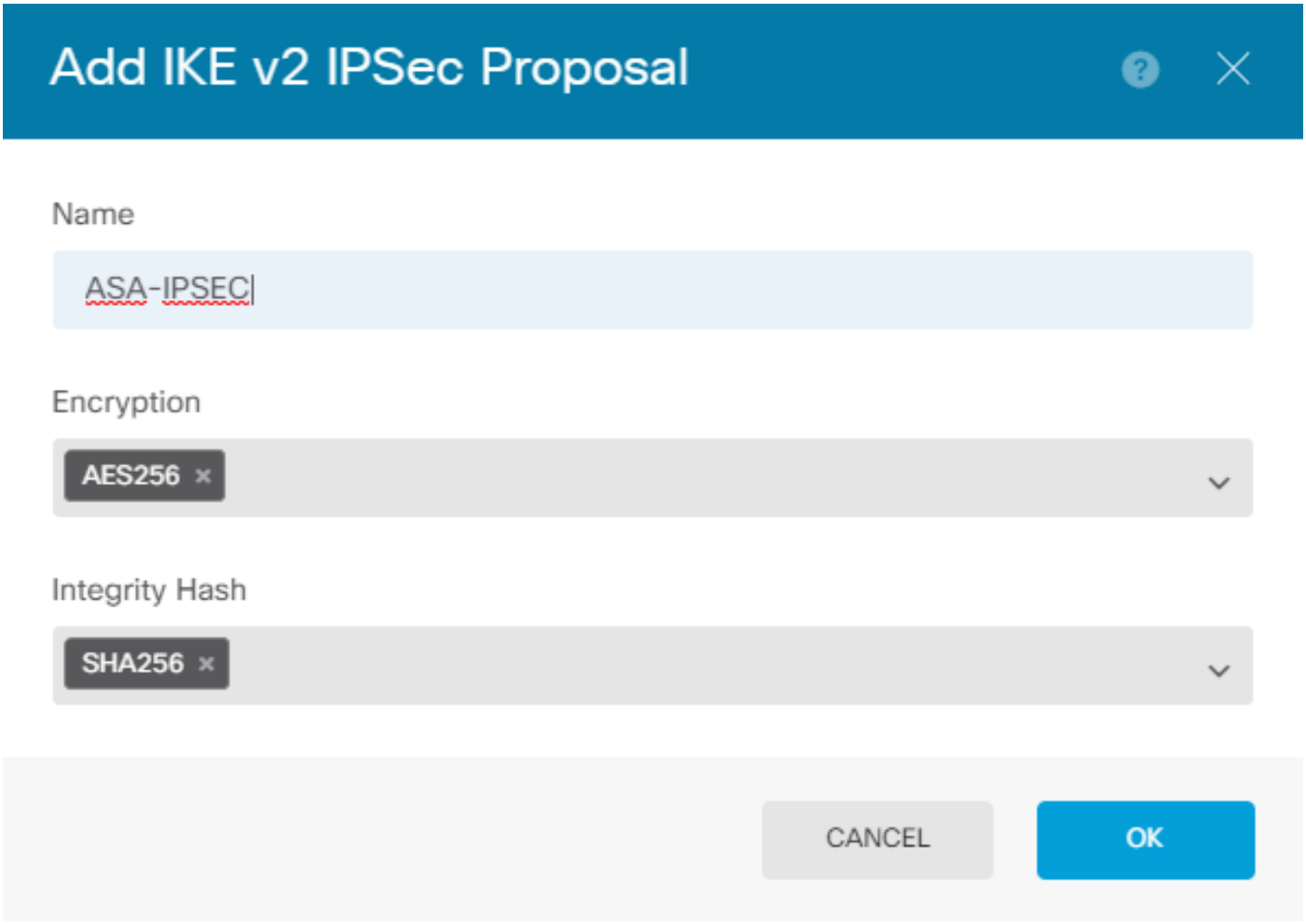
Depois de voltar à página principal, selecione o botão **Editar** para a Proposta de IPSec. Crie uma nova proposta de IPSec como mostrado na imagem.



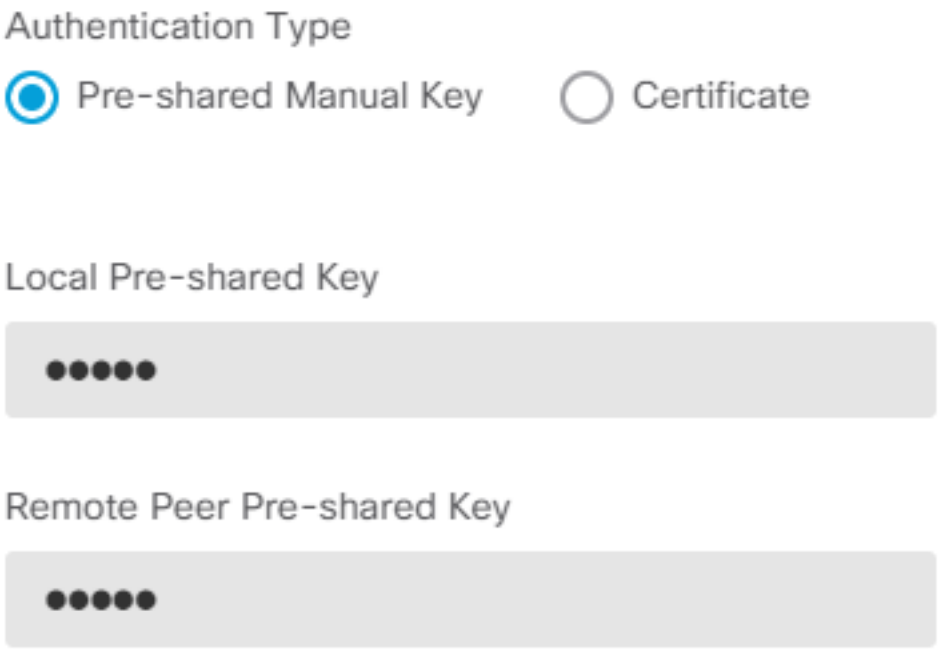
Este guia usará estes parâmetros para IPSec:

Criptografia AES-256

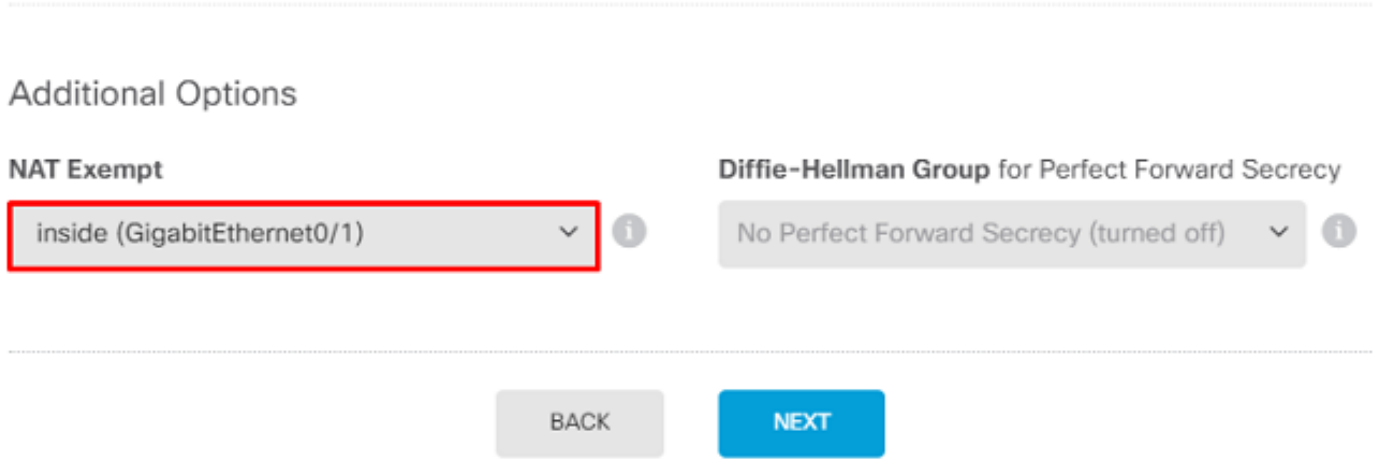
Integridade SHA256



Defina a autenticação como chave pré-compartilhada e insira a chave pré-compartilhada (PSK) que será usada em ambas as extremidades. Neste guia, a PSK da Cisco é usada conforme mostrado na imagem.



Defina a interface NAT Isenta interna. Se houver várias interfaces internas que serão usadas, uma regra de isenção de NAT manual precisará ser criada em **Políticas > NAT**.



Na página final, um resumo da conexão Site-to-Site é exibido. Verifique se os endereços IP corretos estão selecionados e se os parâmetros de criptografia corretos serão usados e pressione o botão Concluir. Implante a nova VPN site a site.

A configuração do ASA será concluída com o uso da CLI.

Configuração do ASA

1. Ative o IKEv2 na interface externa do ASA:

```
Crypto ikev2 enable outside
```

2. Crie a Política IKEv2 que define os mesmos parâmetros configurados no FTD:

```
Crypto ikev2 policy 1
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
Lifetime seconds 86400
```

3. Crie uma política de grupo que permita o protocolo IKEv2:

```
Group-policy FDM_GP internal
Group-policy FDM_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Crie um grupo de túnel para o endereço IP público FTD par. Consulte a política de grupo e especifique a chave pré-compartilhada:

```
Tunnel-group 172.16.100.10 type ipsec-l2l
```

```
Tunnel-group 172.16.100.10 general-attributes
Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco
ikev2 remote-authentication pre-shared-key cisco
```

5. Crie uma lista de acesso que defina o tráfego a ser criptografado: (FTDSubnet 10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
Subnet 10.10.116.0 255.255.255.0
Object network ASASubnet
Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Crie uma proposta IPsec IKEv2 que faça referência aos algoritmos especificados no FTD:

```
Crypto ipsec ikev2 ipsec-proposal FDM
Protocol esp encryption aes-256
Protocol esp integrity sha-256
```

7. Crie uma entrada de mapa de criptografia que conecte a configuração:

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Crie uma declaração de isenção de NAT que impedirá que o tráfego VPN seja NATTED pelo firewall:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Tente iniciar o tráfego através do túnel VPN. Com acesso à linha de comando do ASA ou FTD, isso pode ser feito com o comando packet tracer. Quando você usa o comando packet-tracer para ativar o túnel VPN, ele deve ser executado duas vezes para verificar se o túnel está ativado. Na primeira vez que o comando é emitido, o túnel VPN está inoperante, de modo que o comando packet-tracer falha com o DROP criptografado de VPN. Não use o endereço IP interno do firewall como o endereço IP origem no packet-tracer, pois isso sempre falhará.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
```

```
Additional Information:


firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971
|s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 destination static
|s2sAclDestNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclDestNwgV4|c9911223-779d-11ea-9c1b-
5ddd47126971 no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc
outside any rule-id 268435457 event-log both
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971
|s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 destination static
|s2sAclDestNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclDestNwgV4|c9911223-779d-11ea-9c1b-
5ddd47126971 no-proxy-arp route-lookup
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
```

```
output-status: up
output-line-status: up
Action: allow
```

Para monitorar o status do túnel, navegue até a CLI do FTD ou do ASA.

Na CLI do FTD, verifique a fase-1 e a fase-2 com o comando **show crypto ikev2 sa**.

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local
Remote                                          Status         Role
  3821043 172.16.100.10/500
192.168.200.10/500                                 READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Problemas iniciais de conectividade

Quando você constrói uma VPN, há dois lados negociando o túnel. Portanto, é melhor obter os dois lados da conversação quando você soluciona qualquer tipo de falha de túnel. Um guia detalhado sobre como depurar túneis IKEv2 pode ser encontrado aqui: Como depurar VPNs IKEv2

A causa mais comum de falhas de túnel é um problema de conectividade. A melhor maneira de determinar isso é fazer capturas de pacotes no dispositivo.

Use este comando para capturar capturas de pacote no dispositivo:

```
Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10
```

Depois que a captura estiver estabelecida, tente enviar tráfego pela VPN e verifique o tráfego bidirecional na captura de pacotes.

Revise a captura de pacotes com o comando **show cap capout**.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
```

```
3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

Problemas específicos de tráfego

Os problemas comuns de tráfego que os usuários enfrentam são:

- Problemas de roteamento por trás do FTD - a rede interna não pode rotear pacotes de volta aos endereços IP e clientes VPN atribuídos.
- As listas de controle de acesso bloqueiam o tráfego.
- A Conversão de Endereço de Rede (NAT - Network Address Translation) não está sendo ignorada para tráfego VPN.

Para obter mais informações sobre VPNs de site a site no FTD gerenciado pelo FDM, você pode encontrar o guia de configuração completo aqui: FTD gerenciado pelo guia de configuração do FDM.