Configuração de VPN site a site no FTD gerenciado pelo FMC

Contents

Introduction

Este documento fornece um exemplo de configuração de VPN site a site no Firepower Threat Defense (FTD) gerenciado pelo FMC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica da VPN
- Experiência com o Firepower Management Center
- Experiência com a linha de comando 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.

Configuração

Comece com a configuração no FTD com FirePower Management Center.

Etapa 1. Defina a topologia VPN.

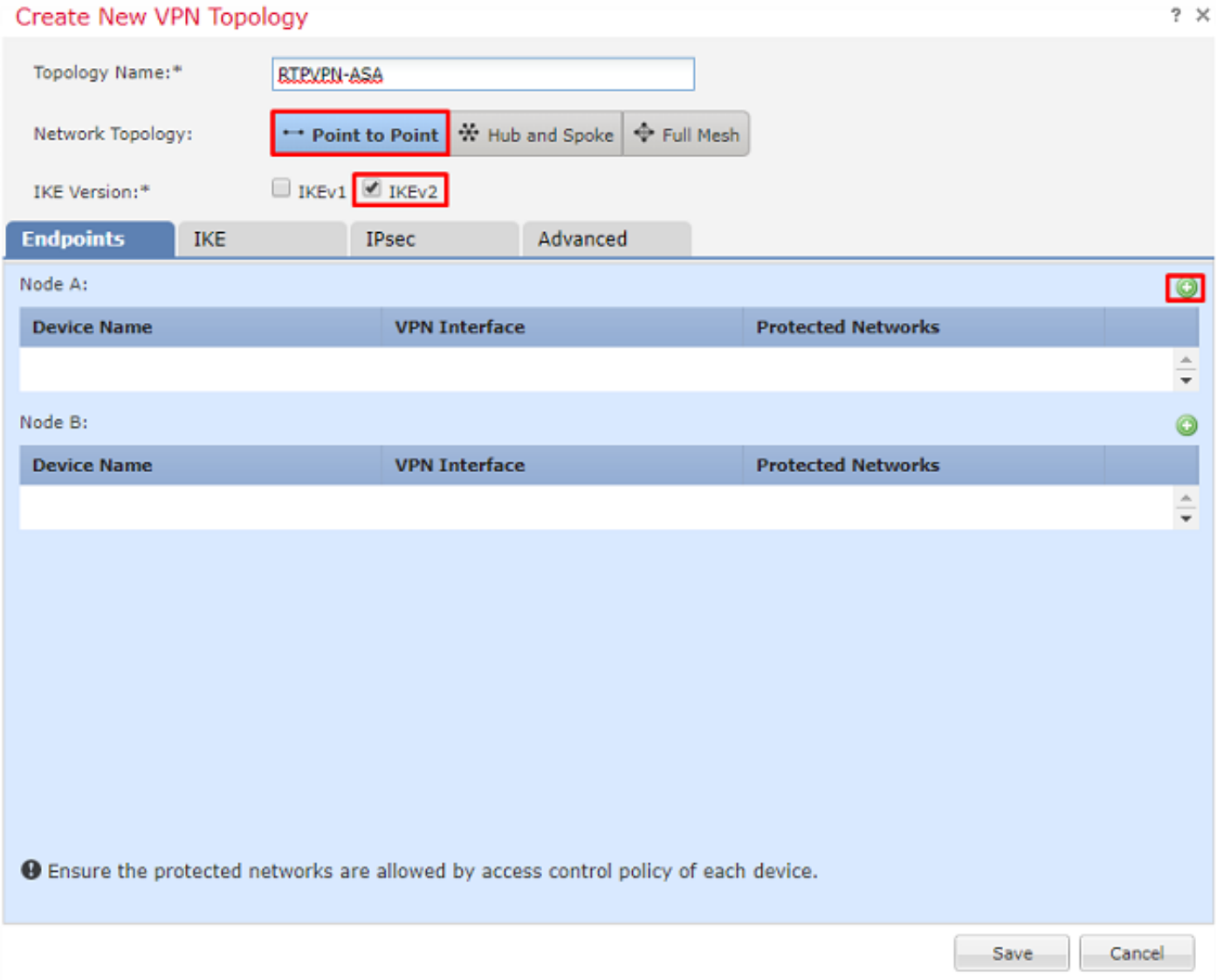
1. Navegue até **Dispositivos > VPN > Site a Site.** Em **Adicionar VPN,** clique em **Firepower Threat Defense Device**, como mostrado nesta imagem.

2. A caixa **Create New VPN Topology (Criar nova topologia de VPN)** é exibida. Forneça à VPN um nome facilmente identificável.

Topologia de rede: Ponto a ponto

Versão IKE: IKEv2

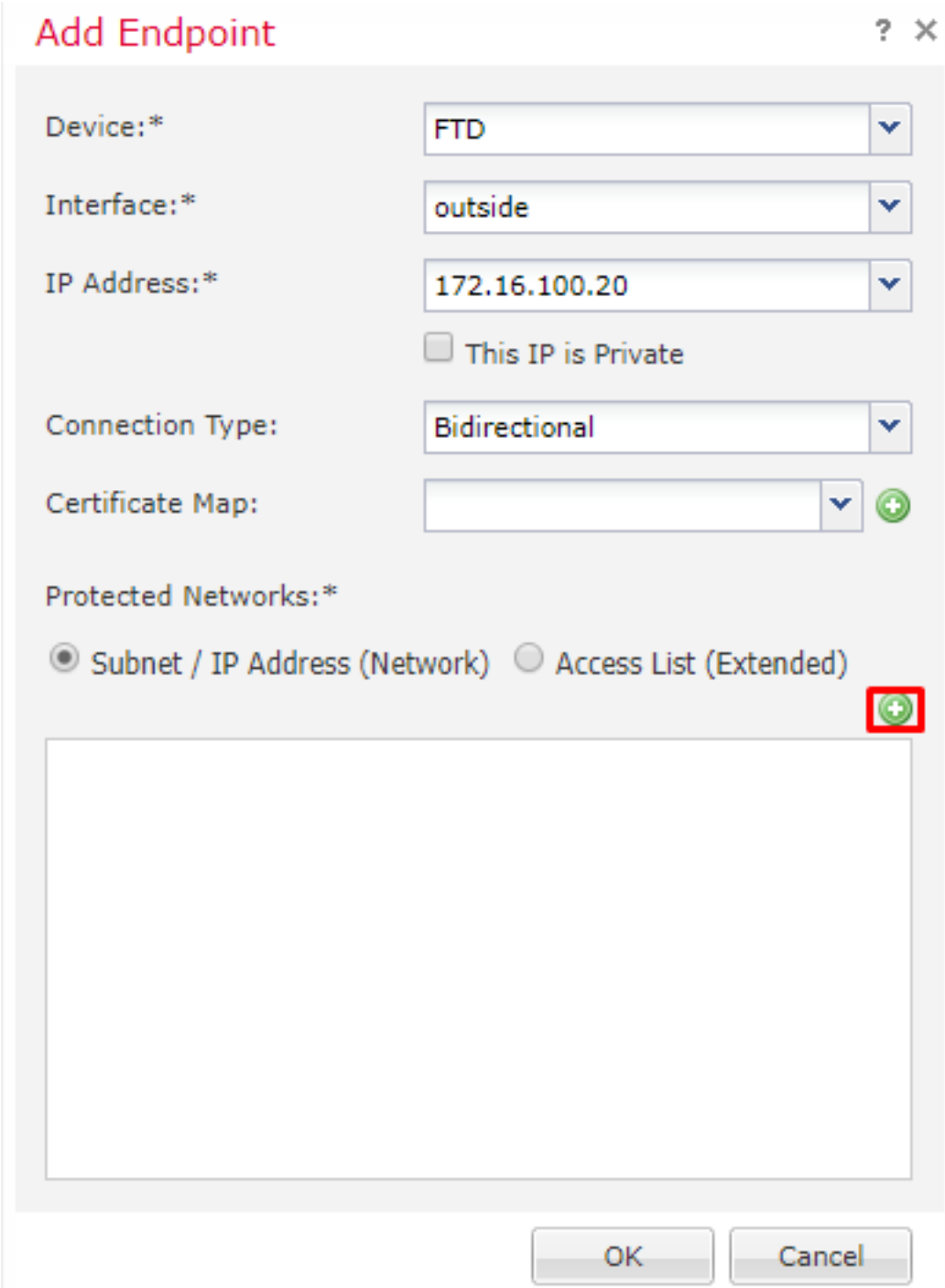
Neste exemplo, quando você seleciona endpoints, o Nó A é o FTD e o Nó B é o ASA. Clique no botão verde mais para adicionar dispositivos à topologia, como mostrado nesta imagem.



3. Adicione o FTD como o primeiro endpoint.

Escolha a interface na qual um mapa de criptografia é colocado. O endereço IP deve ser preenchido automaticamente a partir da configuração do dispositivo.

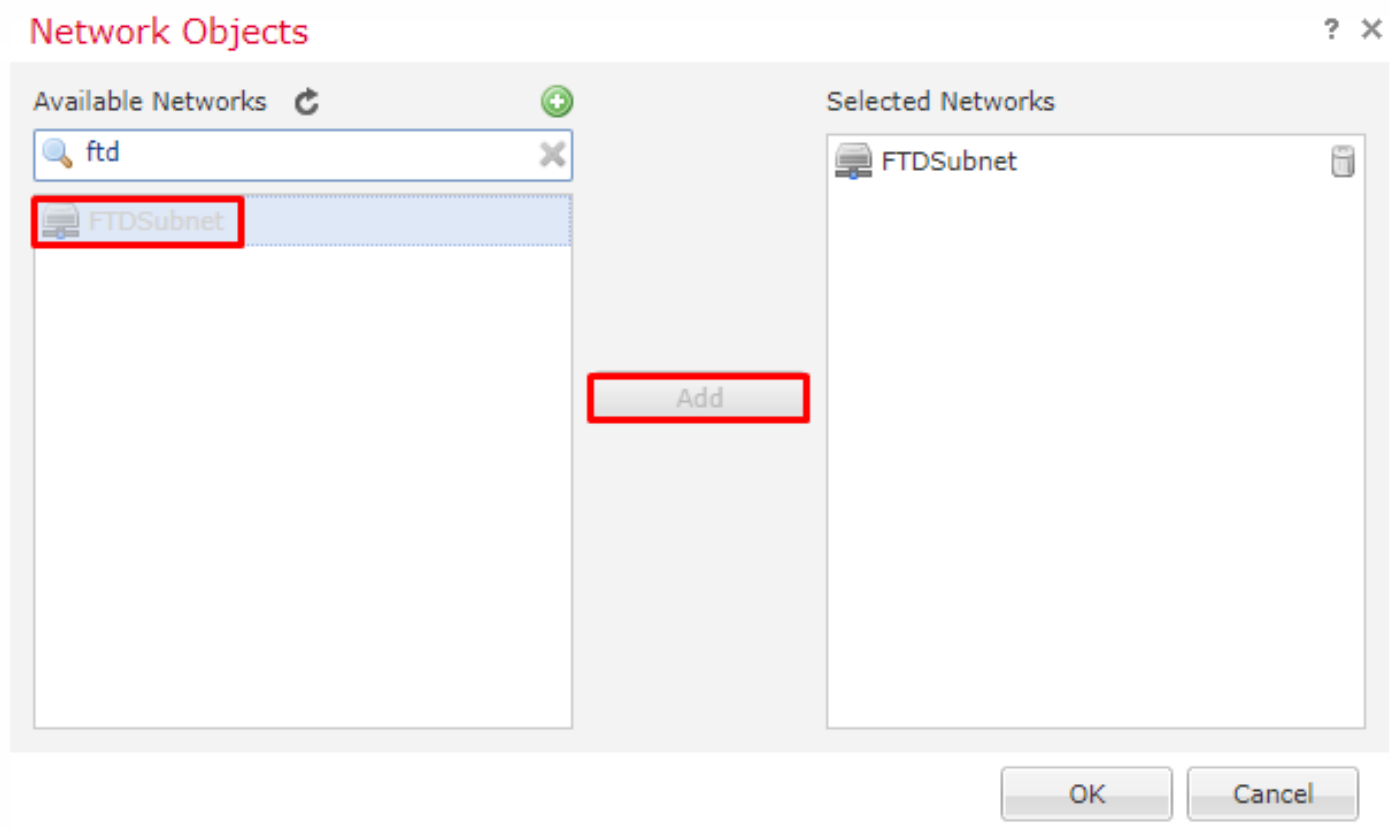
Clique no sinal de mais verde em Redes protegidas, como mostrado nesta imagem, para selecionar quais sub-redes devem ser criptografadas nesta VPN.



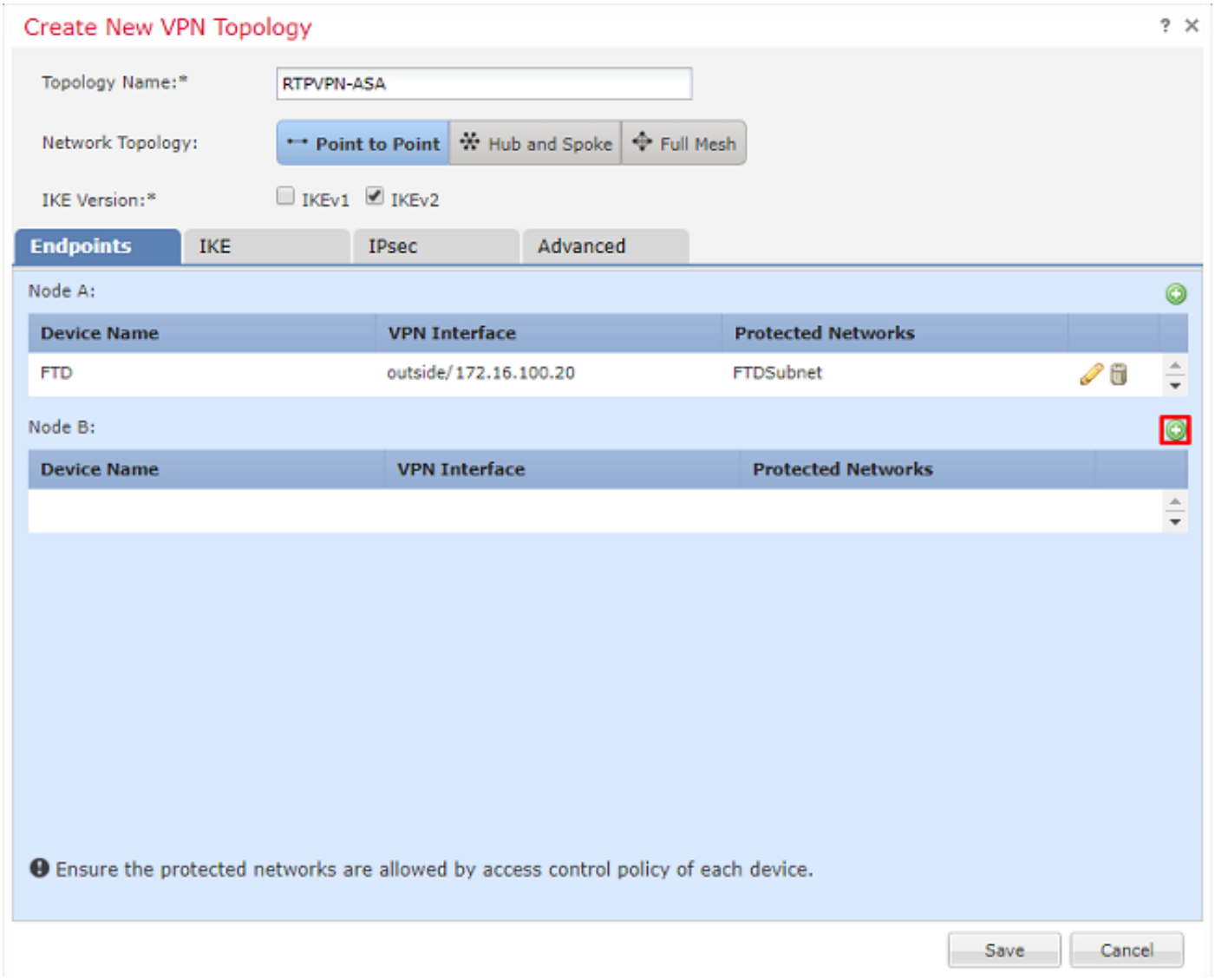
4. Clique em verde mais e um objeto de rede é criado aqui.

5. Adicione todas as sub-redes locais ao FTD que precisam ser criptografadas. Clique em **Adicionar** para movê-los para Redes selecionadas. Agora clique em **OK**, como mostrado nesta imagem.

FTDSubnet = 10.10.113.0/24

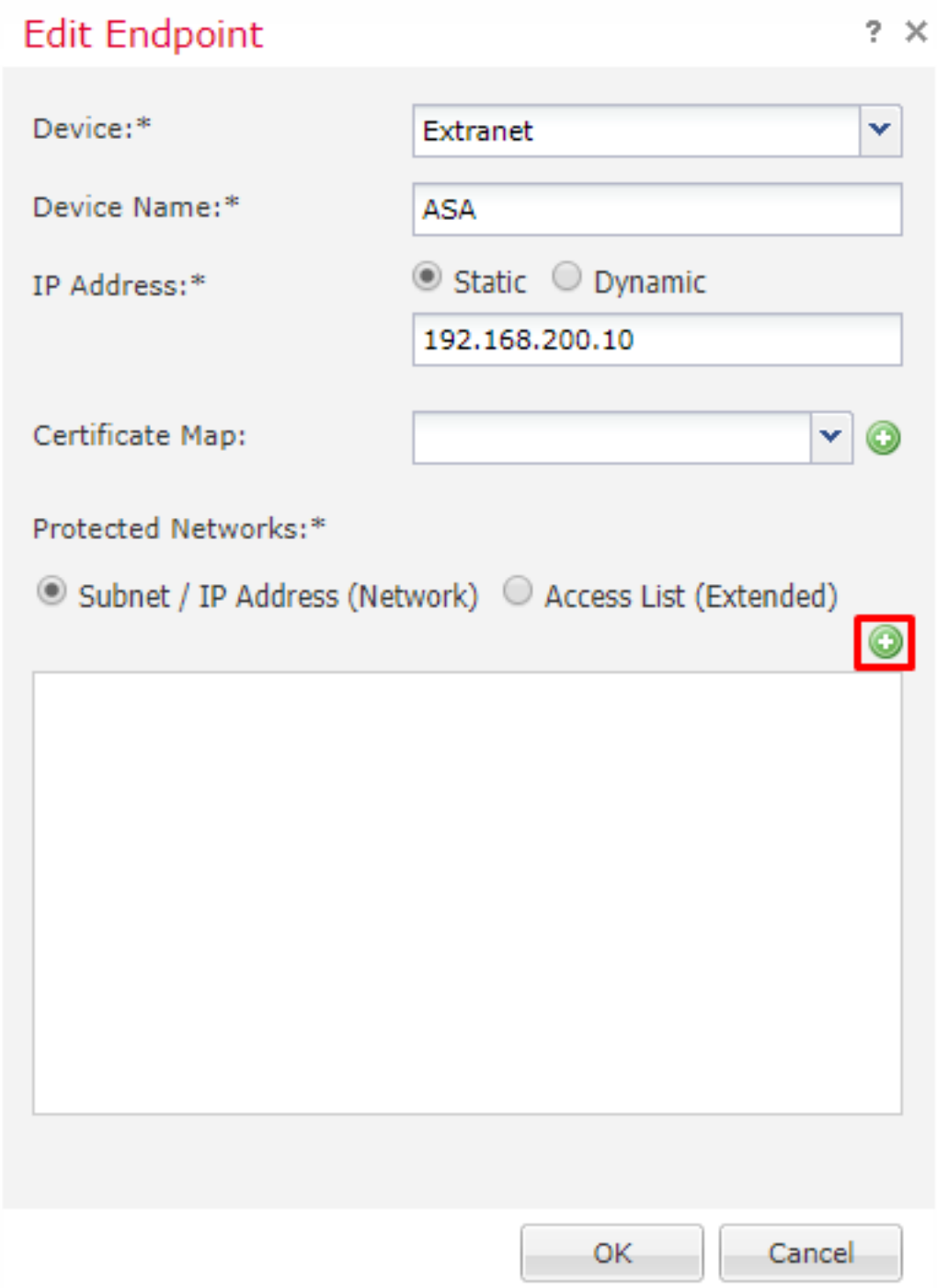


Nó A: O endpoint (FTD) está concluído. Clique no sinal de mais verde para o Nó B, como mostrado na imagem.



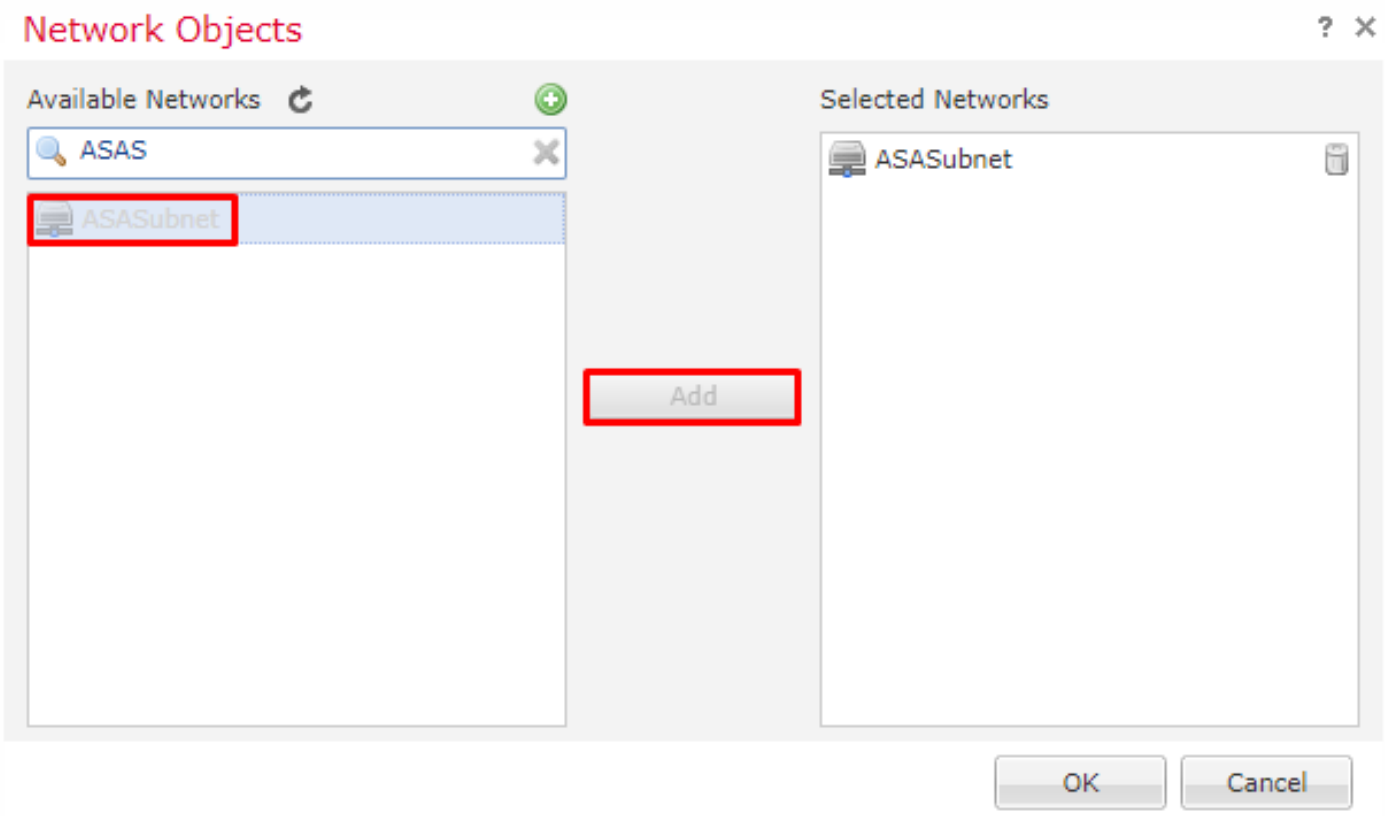
O nó B é um ASA. Os dispositivos que não são gerenciados pelo FMC são considerados extranet.

6. Adicione um nome de dispositivo e um endereço IP. Clique no sinal de mais verde para adicionar redes protegidas, como mostrado na imagem.



7. Como mostrado nesta imagem, selecione as **sub-redes ASA** que precisam ser criptografadas e adicione-as às redes selecionadas.

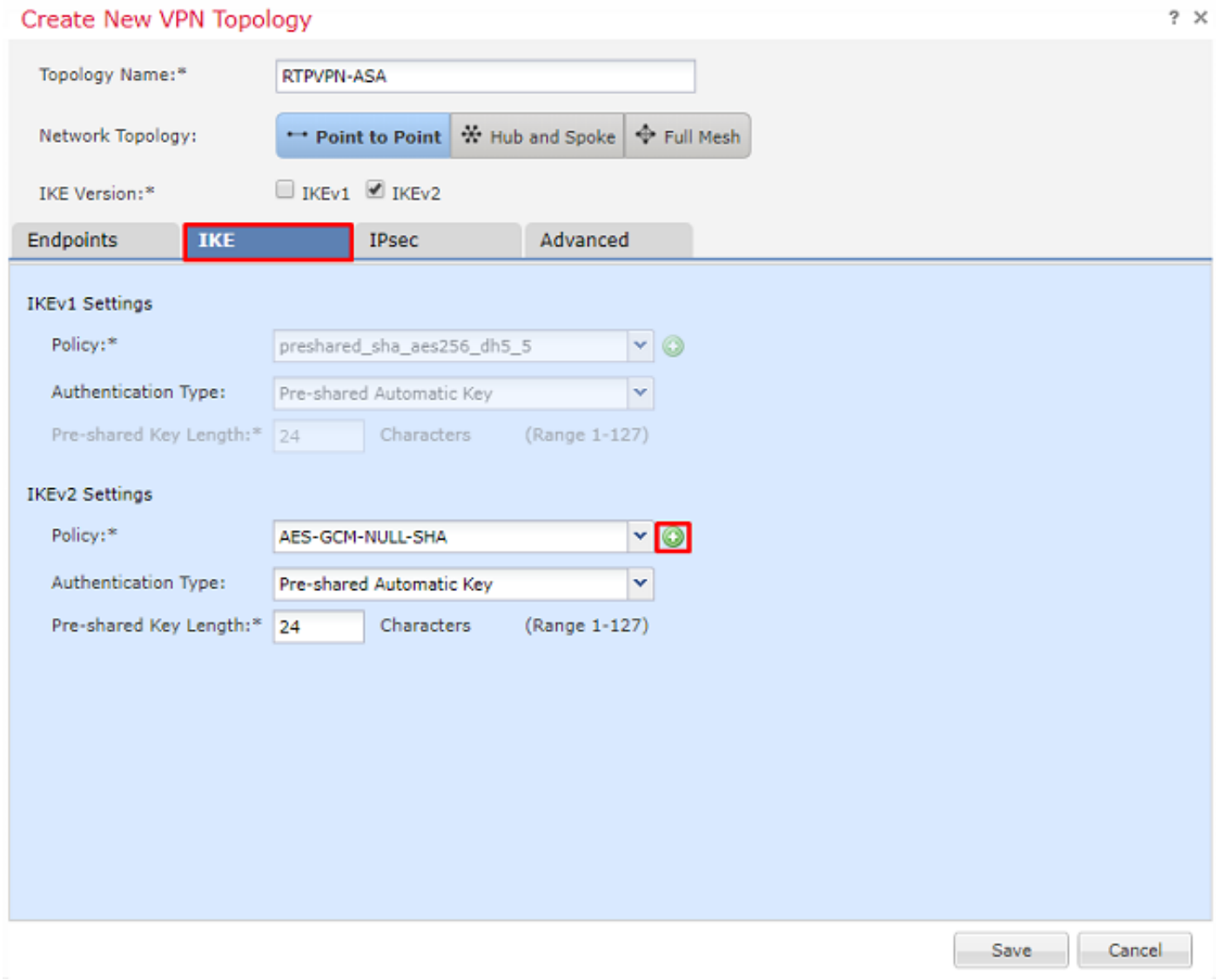
ASASubnet = 10.10.110.0/24



Etapa 2. Configurar parâmetros IKE.

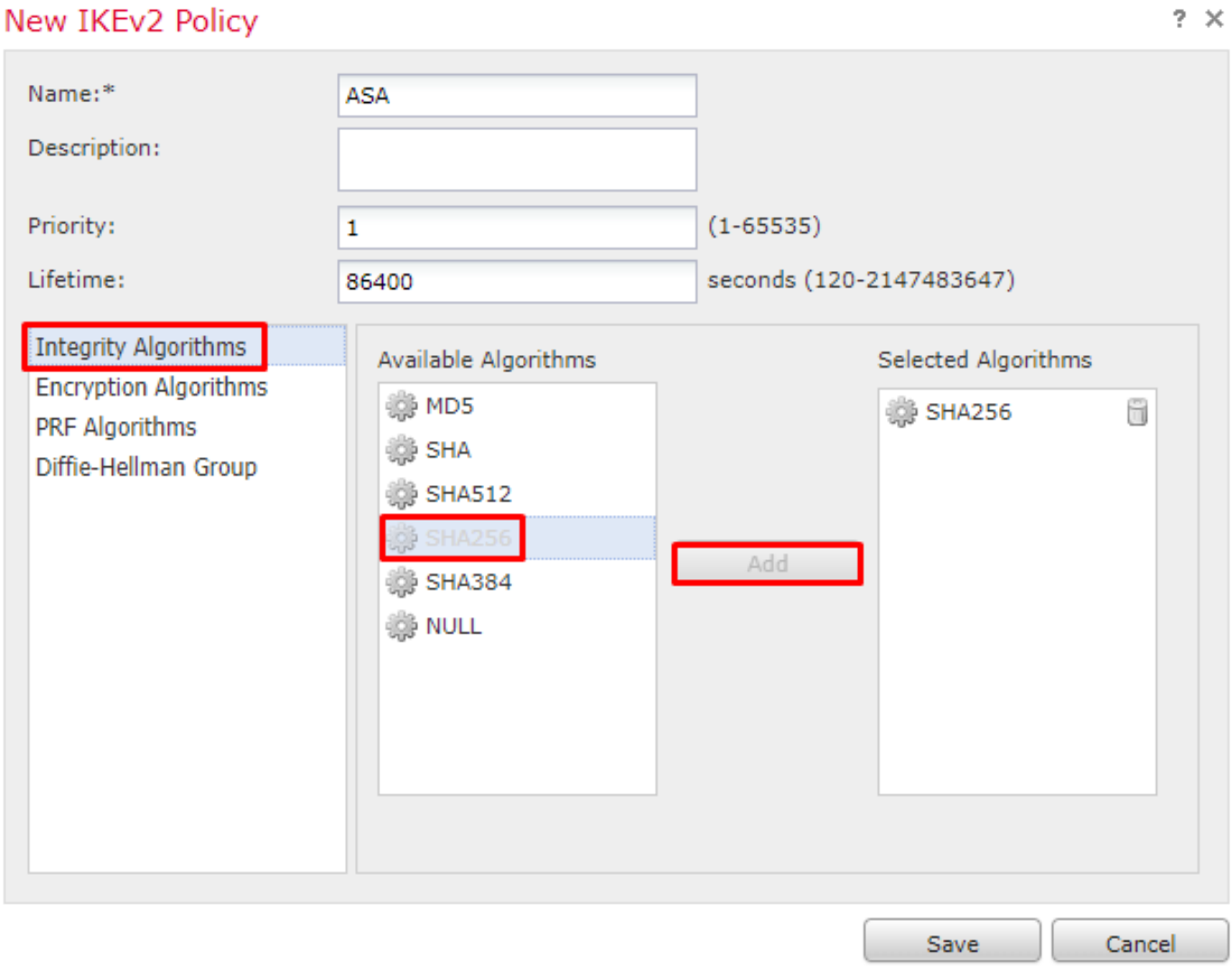
Agora, ambos os endpoints estão instalados para passar pela configuração IKE/IPSEC.

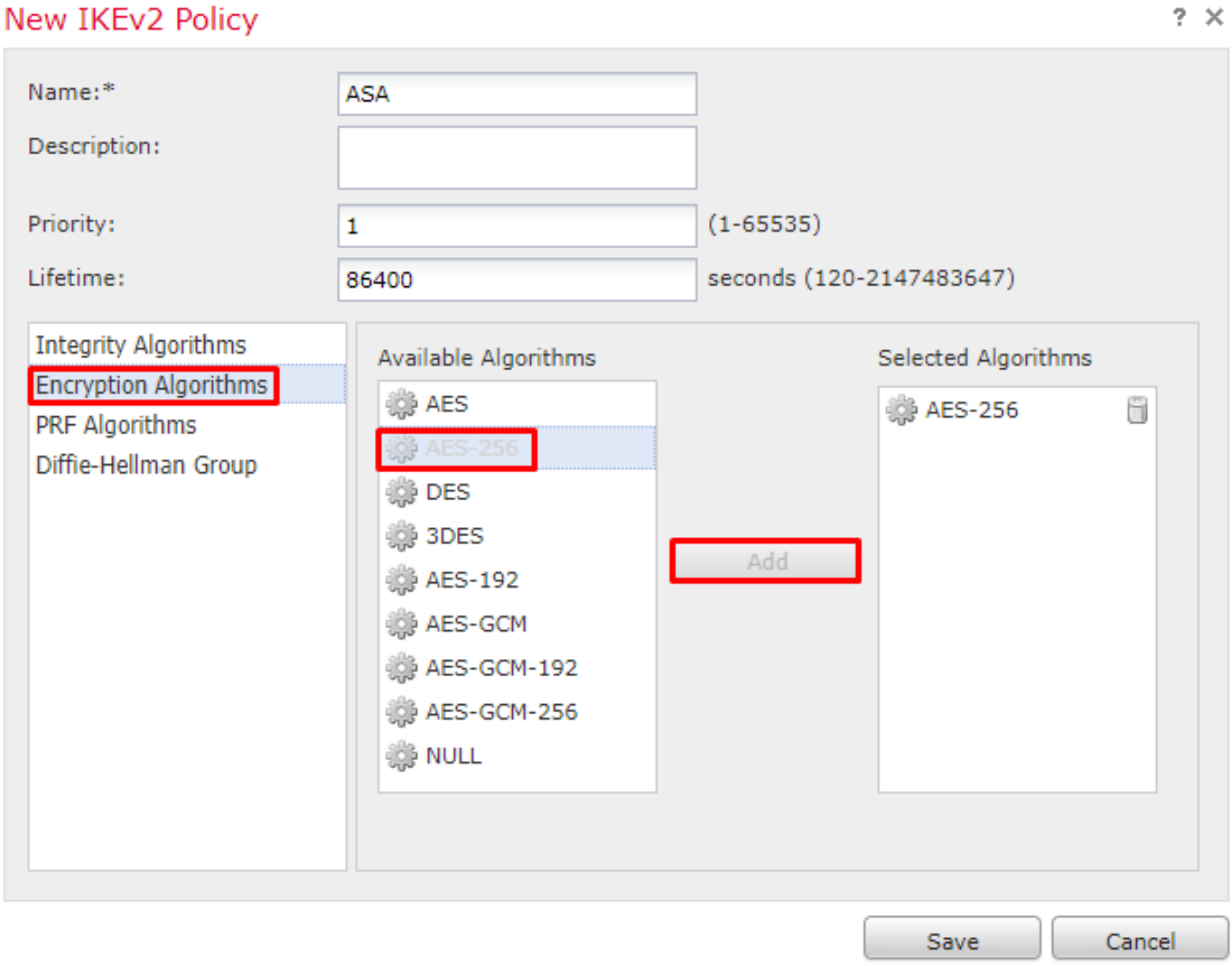
1. Na guia **IKE**, especifique os parâmetros usados para a troca inicial de IKEv2. Clique no sinal de mais verde para criar uma nova política IKE, como mostrado na imagem.

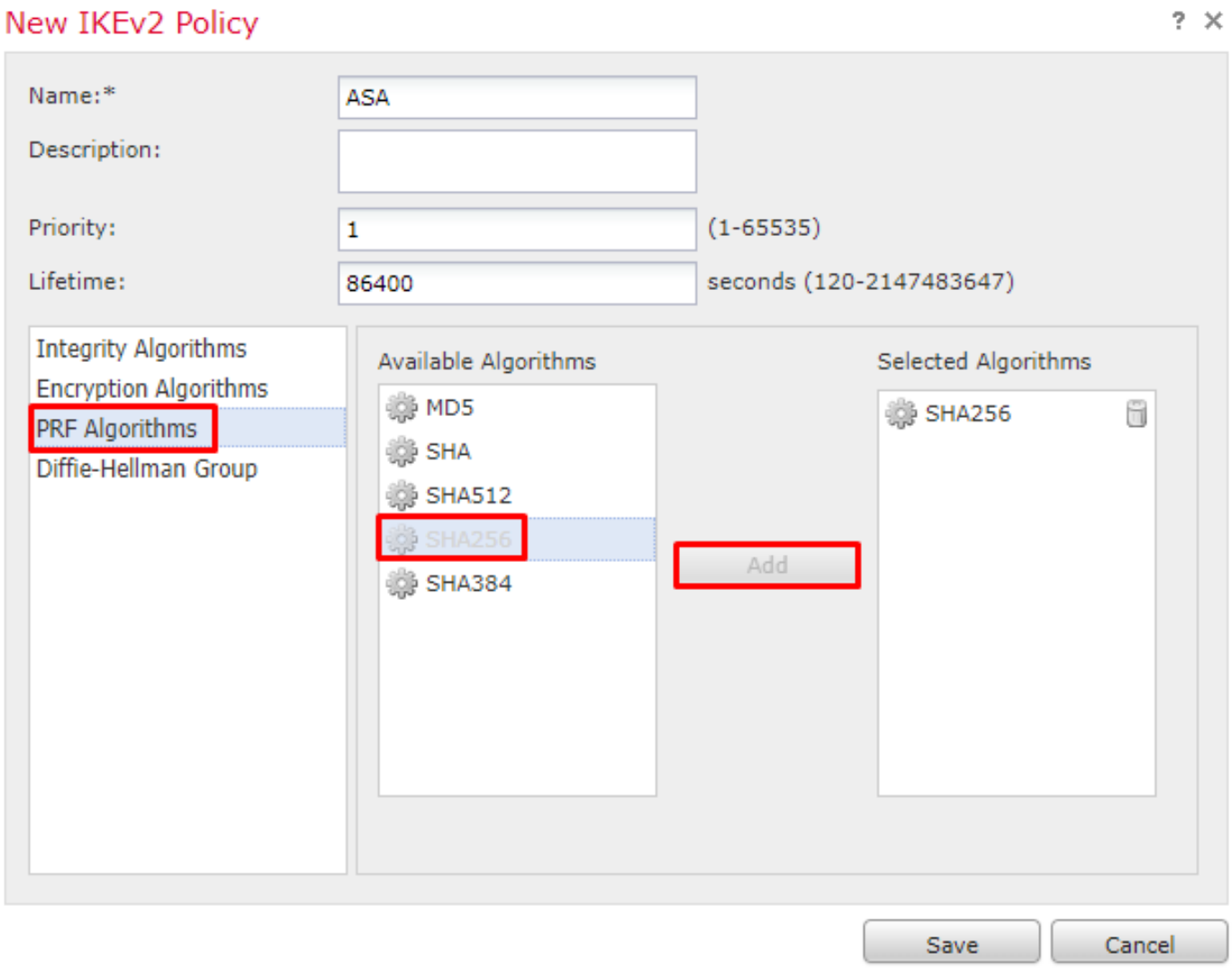


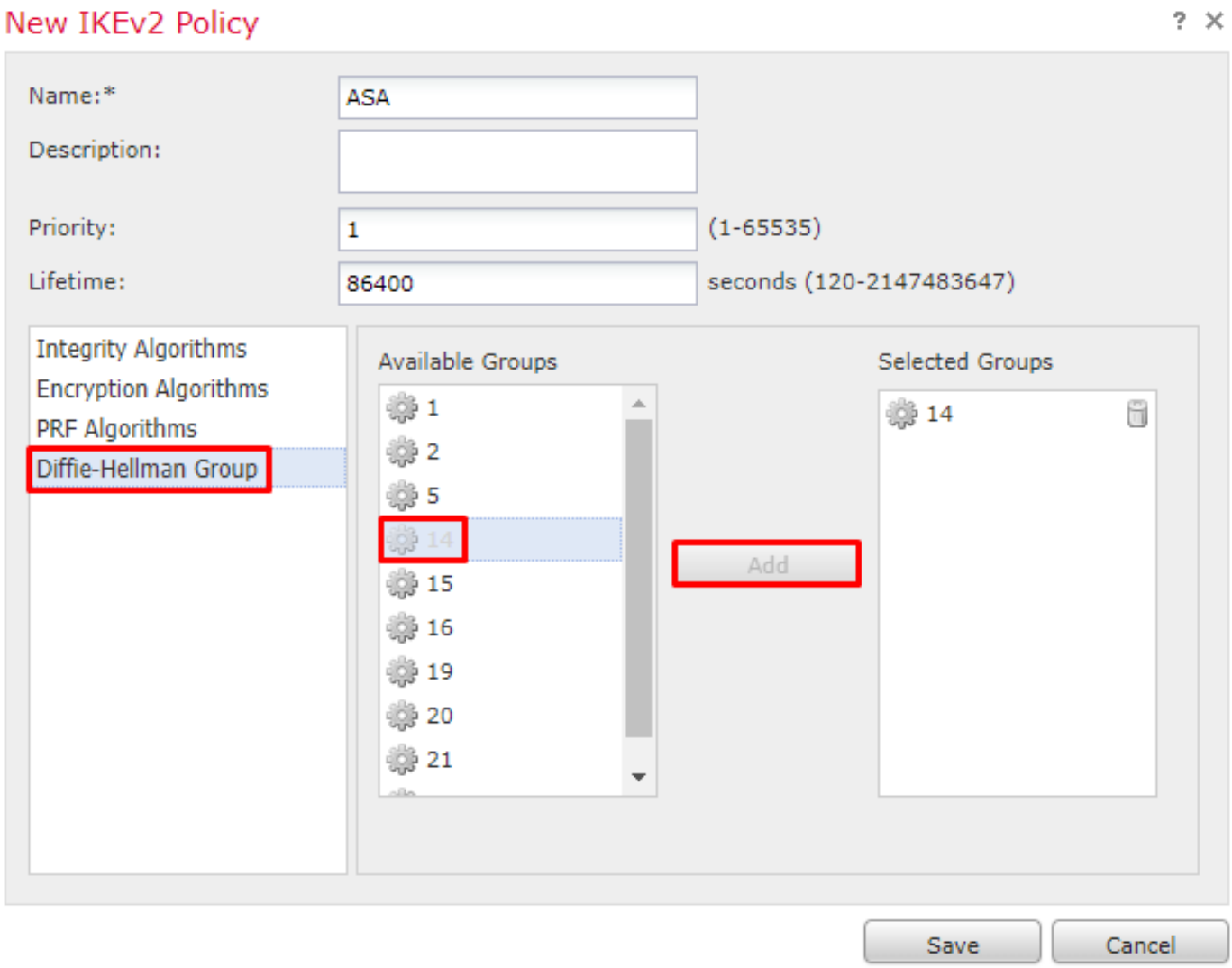
2. Na nova política IKE, especifique um número de prioridade, bem como a duração da fase 1 da conexão. Este documento usa estes parâmetros para a troca inicial: Integrity (SHA256), Encryption (AES-256), PRF (SHA256) e Diffie-Hellman Group (Grupo 14)

> **Note**: Todas as políticas de IKE no dispositivo são enviadas ao peer remoto, independentemente do que está na seção de política selecionada. A primeira política IKE correspondente pelo peer remoto será selecionada para a conexão VPN. Escolha qual política é enviada primeiro usando o campo de prioridade. A prioridade 1 será enviada primeiro.


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
NULL
Add
Selected Algorithms
SHA256
Save
Cancel

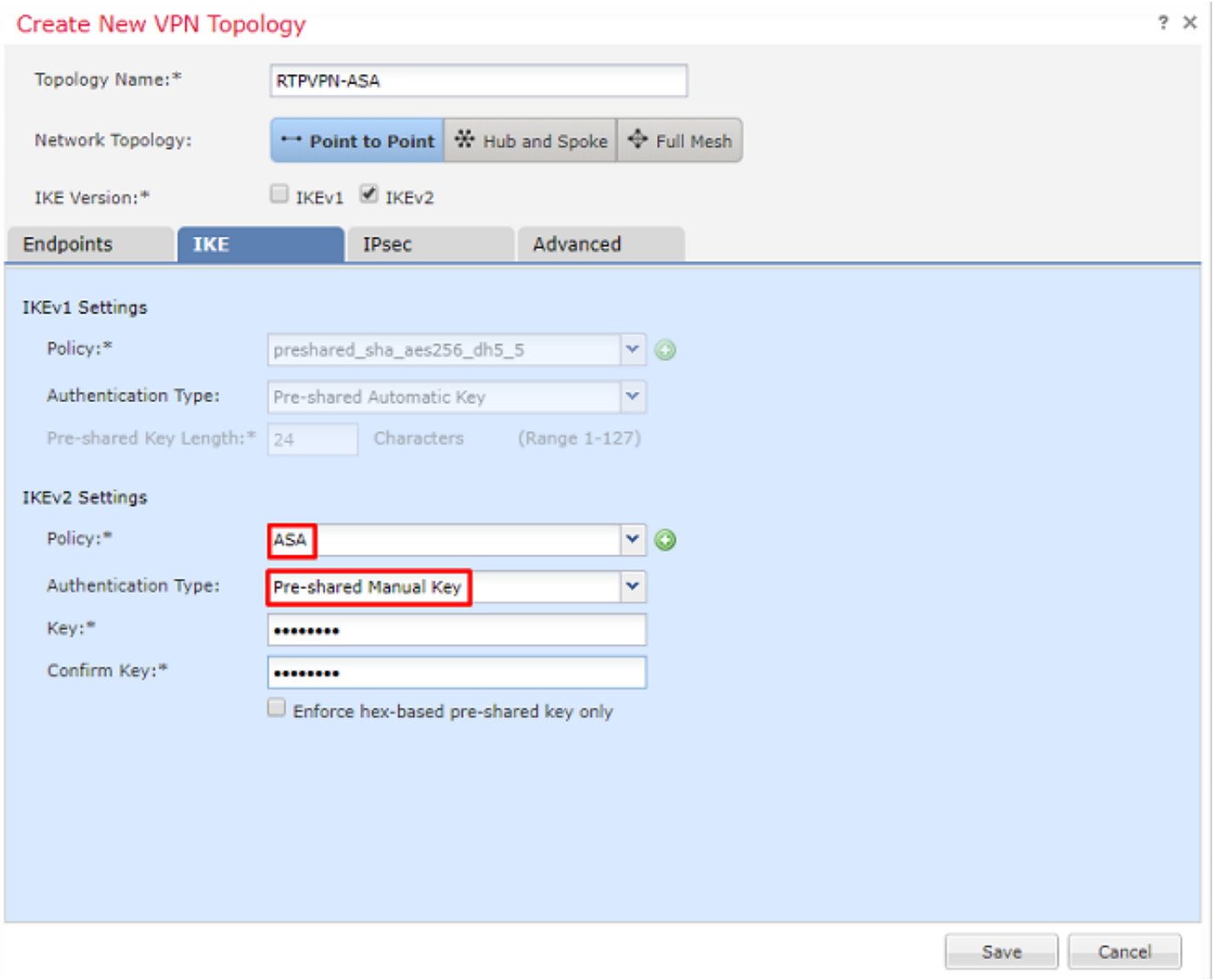

New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
Add
Selected Algorithms
SHA256
Save
Cancel



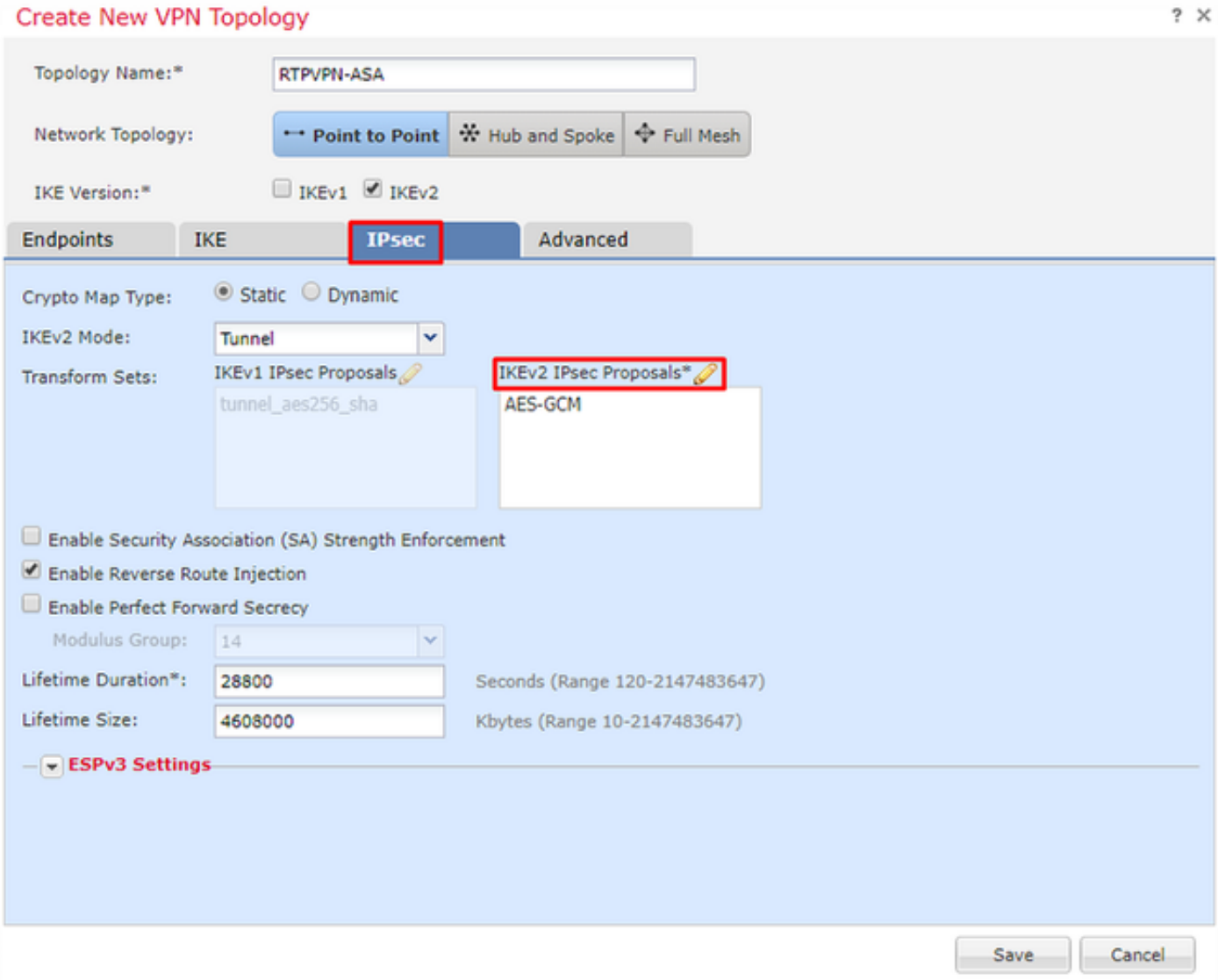
3. Depois que os parâmetros forem adicionados, selecione essa política e escolha o **Tipo de autenticação**.

4. Escolha o manual **da chave pré-compartilhada**. Para este documento, o PSK cisco123 é usado.



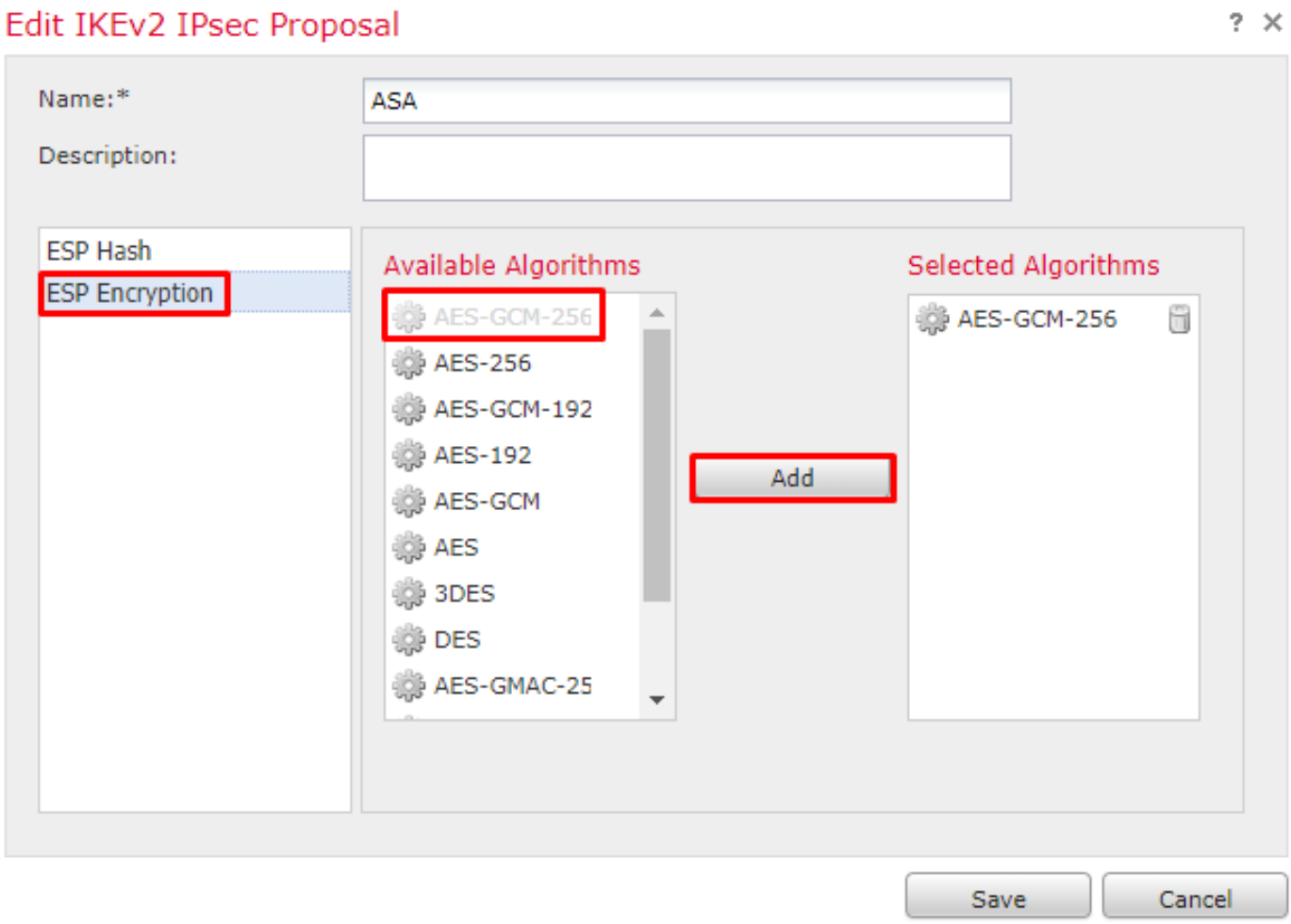
Etapa 3. Configurar parâmetros IPsec.

1. Em **IPsec,** clique no lápis para editar o conjunto de transformações e criar uma nova proposta de IPsec, como mostrado nesta imagem.

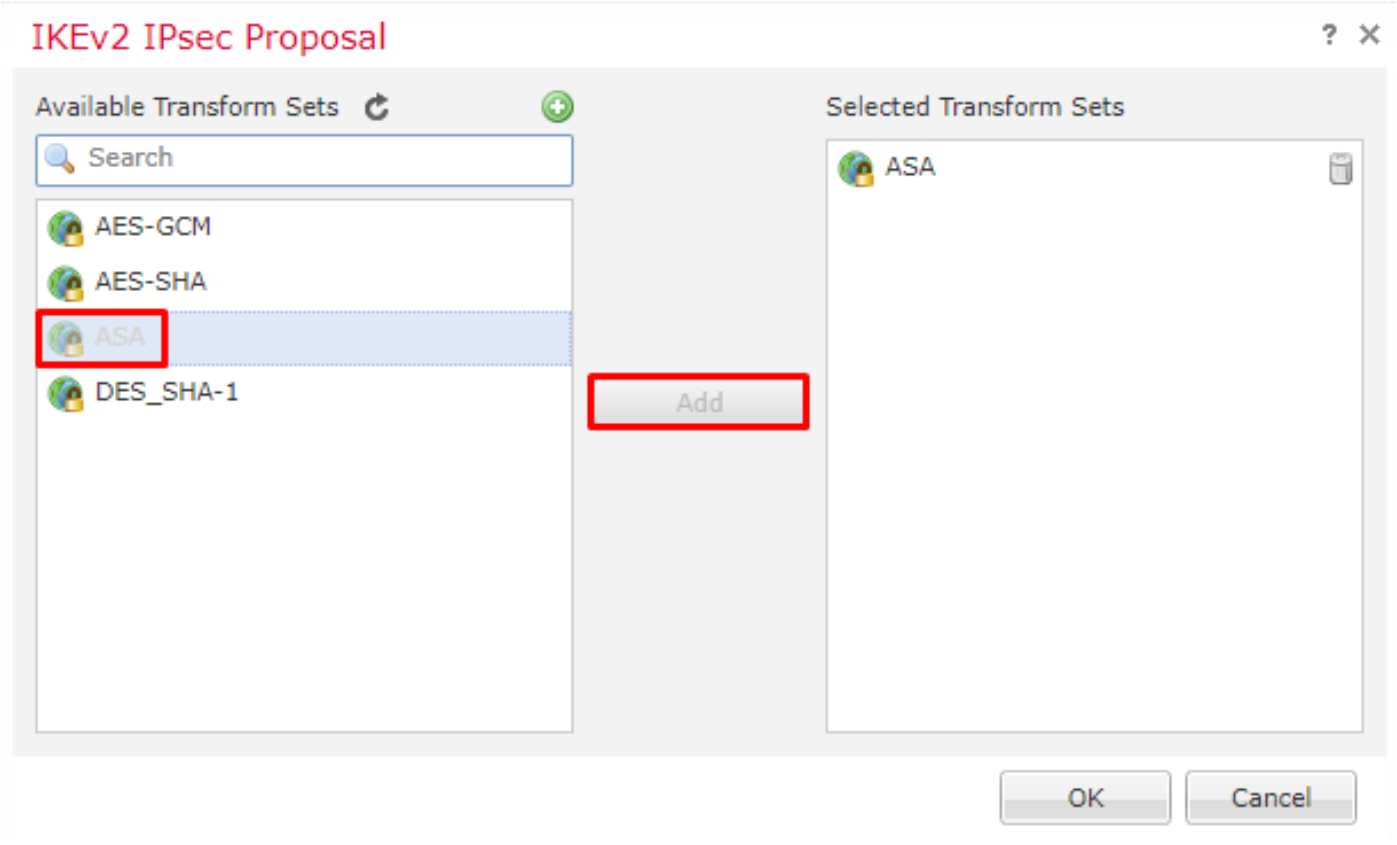


2. Para criar uma nova Proposta IPsec IKEv2, clique no sinal verde e insira os parâmetros da fase 2.

Selecione **ESP Encryption > AES-GCM-256**. Quando o algoritmo GCM é usado para criptografia, não é necessário um algoritmo Hash. Com o GCM, a função de hash é incorporada.

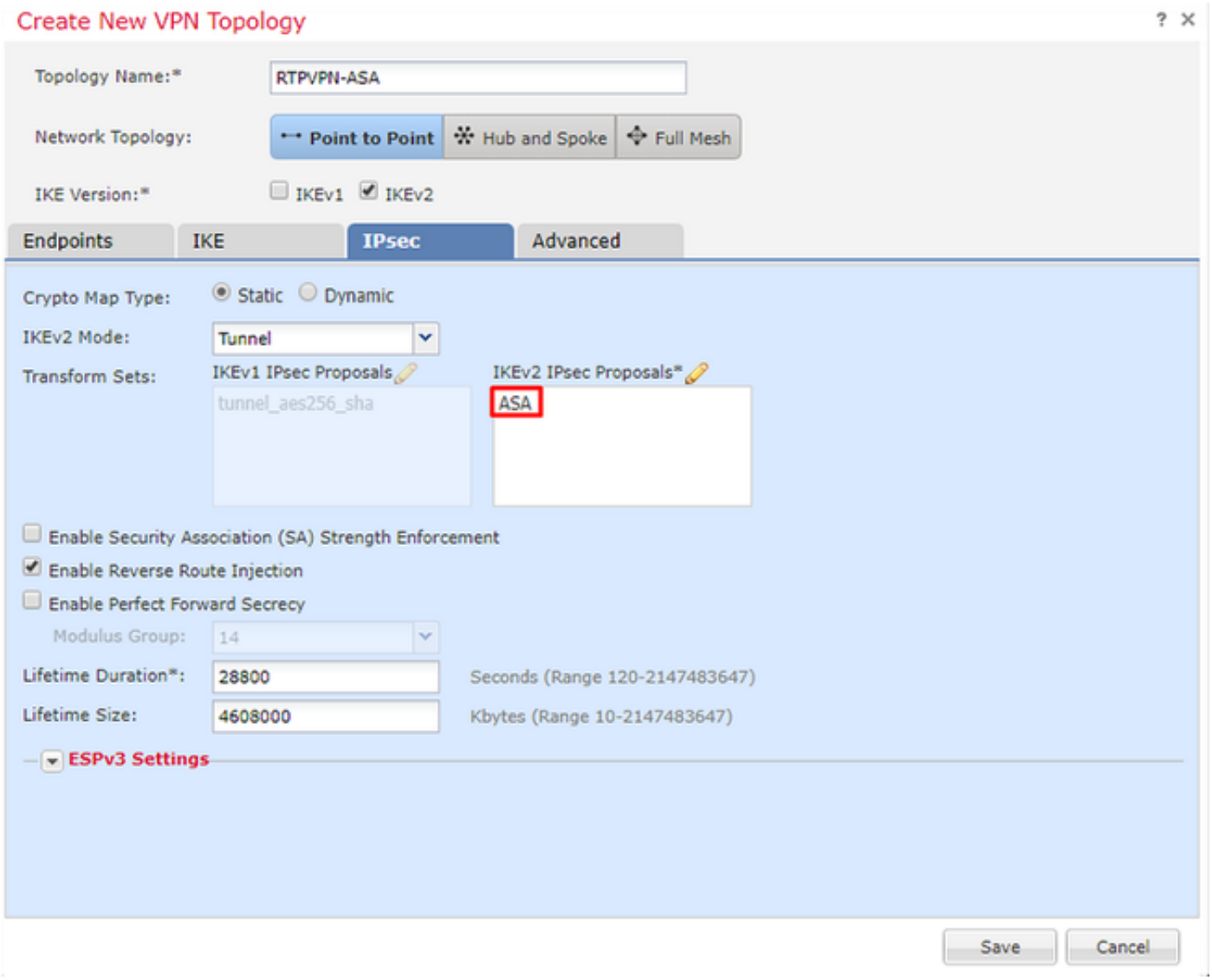


3. Depois que a nova proposta de IPsec for criada, adicione-a aos conjuntos de transformação selecionados.



A proposta de IPSec recentemente selecionada agora está listada nas propostas de IPSec IKEv2.

Se necessário, o tempo de vida da fase 2 e o PFS podem ser editados aqui. Para este exemplo, o tempo de vida será definido como padrão e o PFS desabilitado.

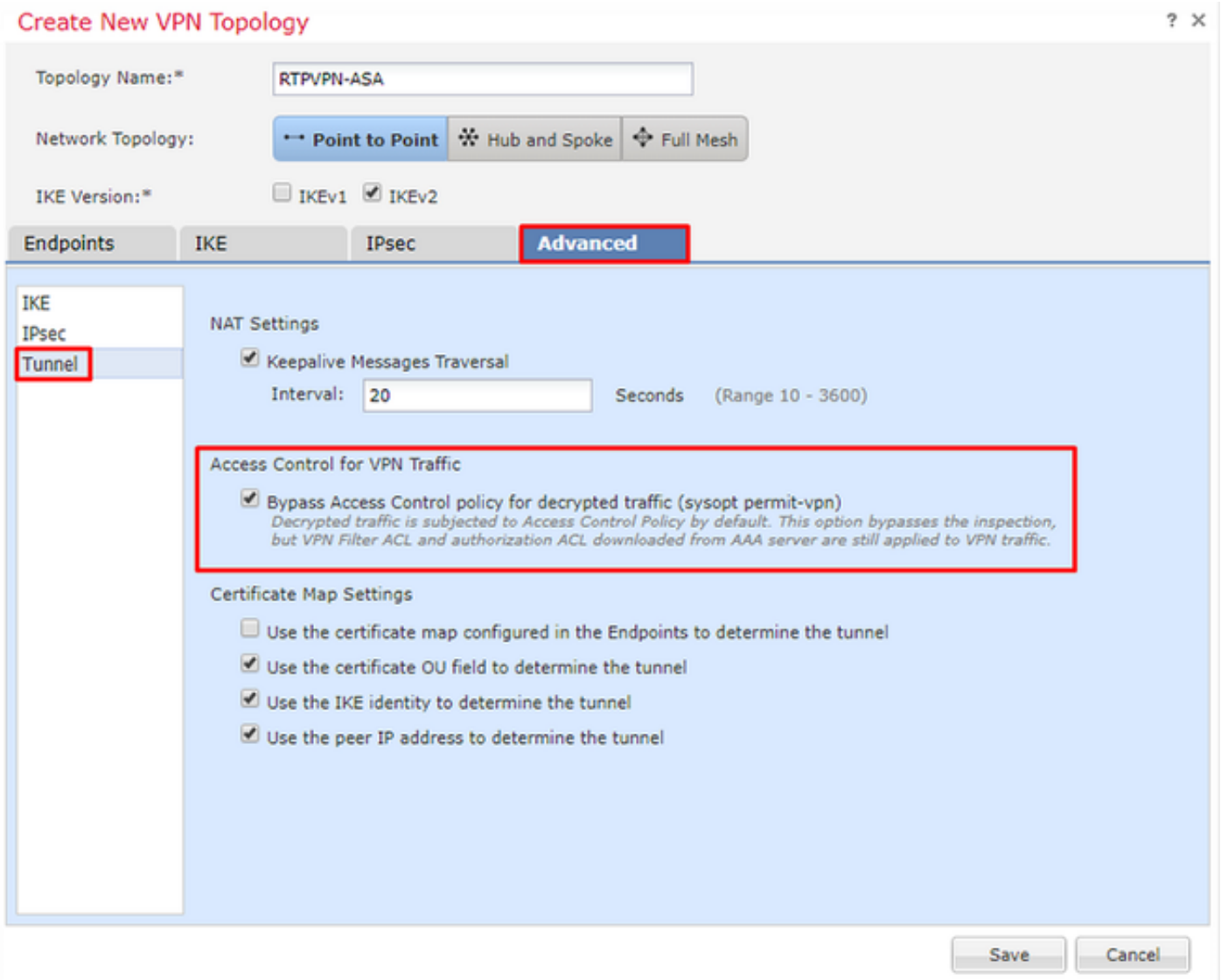


Opcional - Você deve concluir a opção Ignorar Controle de Acesso ou Criar uma Política de Controle de Acesso.

Etapa 4. Ignorar Controle de Acesso.

Opcionalmente, **sysopt permit-vpn** pode ser ativado em **Advanced > Tunnel**.

Isso remove a possibilidade de usar a Política de controle de acesso para inspecionar o tráfego proveniente dos usuários. Os filtros de VPN ou ACLs que podem ser baixadas ainda podem ser usados para filtrar o tráfego do usuário. Este é um comando global e se aplicará a todas as VPNs se essa caixa de seleção estiver habilitada.

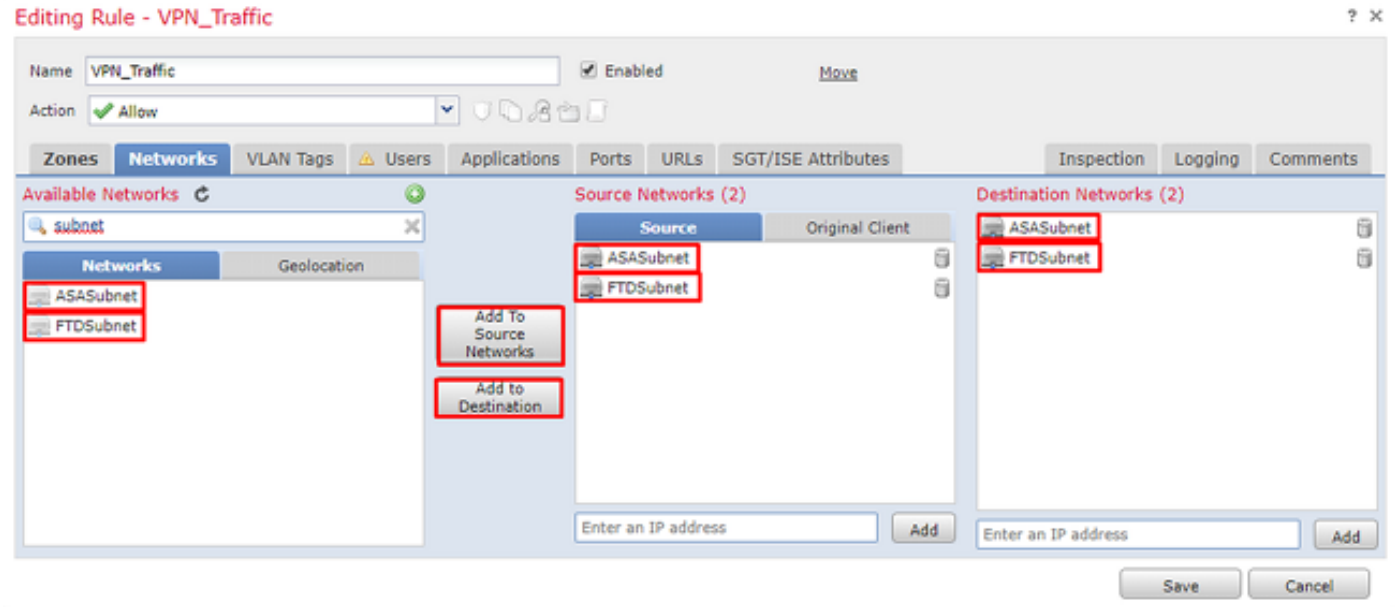


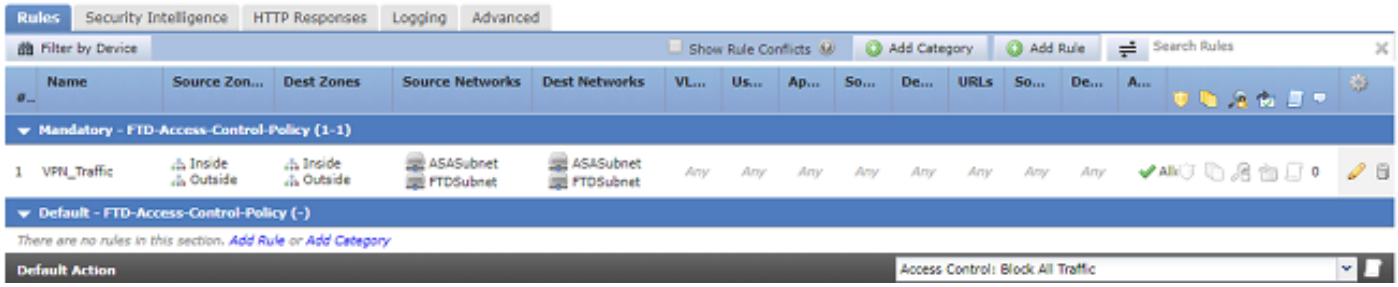
Se **sysopt permit-vpn** não estiver habilitada, uma política de controle de acesso deve ser criada para permitir o tráfego VPN através do dispositivo FTD. Se **sysopt permit-vpn** estiver habilitado, ignore a criação de uma política de controle de acesso.

Etapa 5. Crie uma política de controle de acesso.

Em Access Control Policies, navegue para **Policies > Access Control > Access Control** e selecione a Política que visa o dispositivo FTD. Para adicionar uma regra, clique em **Adicionar regra**, como mostrado na imagem aqui.

O tráfego deve ser permitido da rede interna para a rede externa e da rede externa para a rede interna. Crie uma regra para fazer ambas ou crie duas regras para mantê-las separadas. Neste exemplo, uma regra é criada para fazer ambos.

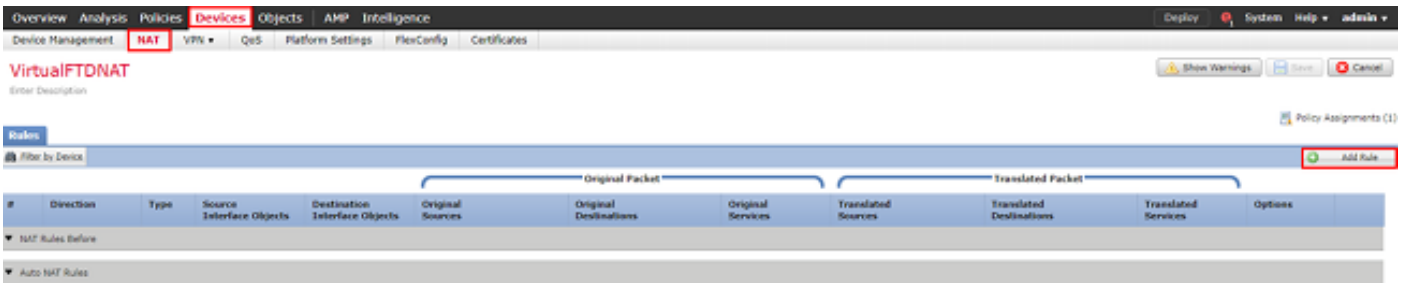




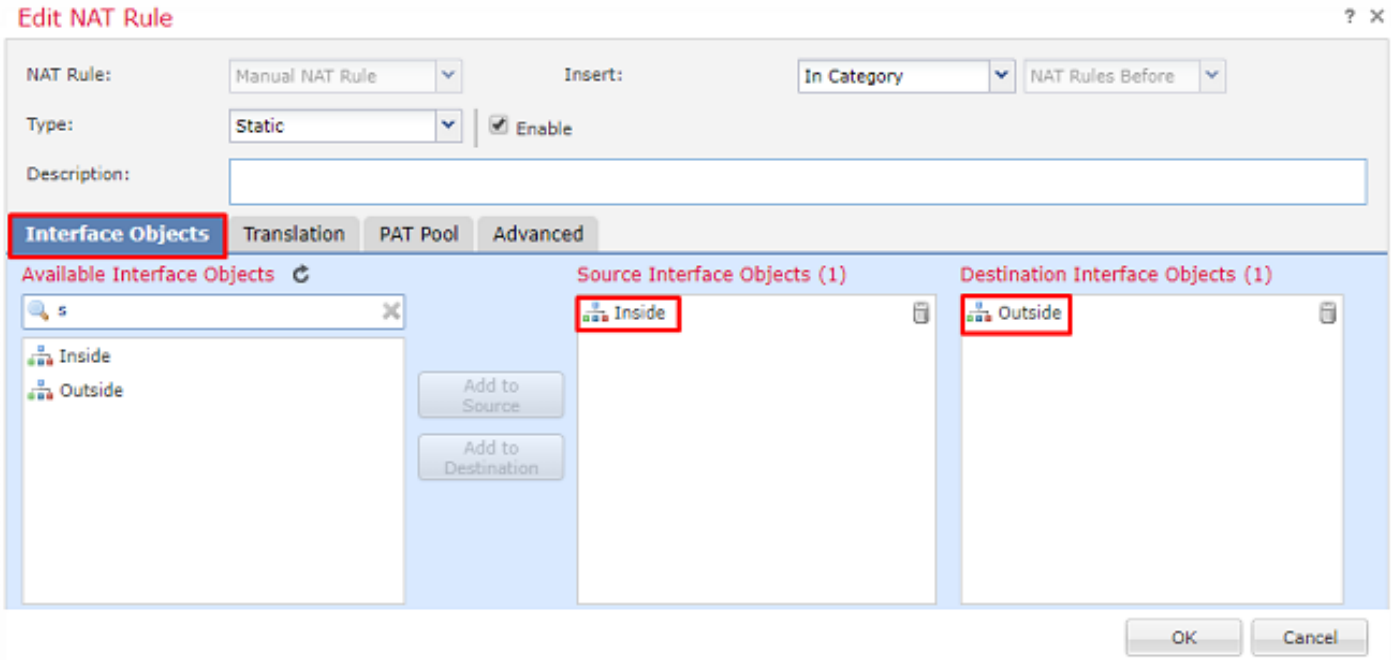
Etapa 6. Configure a isenção de NAT.

Configure uma declaração de isenção de NAT para o tráfego VPN. A isenção de NAT deve estar em vigor para impedir que o tráfego VPN atinja outra instrução NAT e converta incorretamente o tráfego VPN.

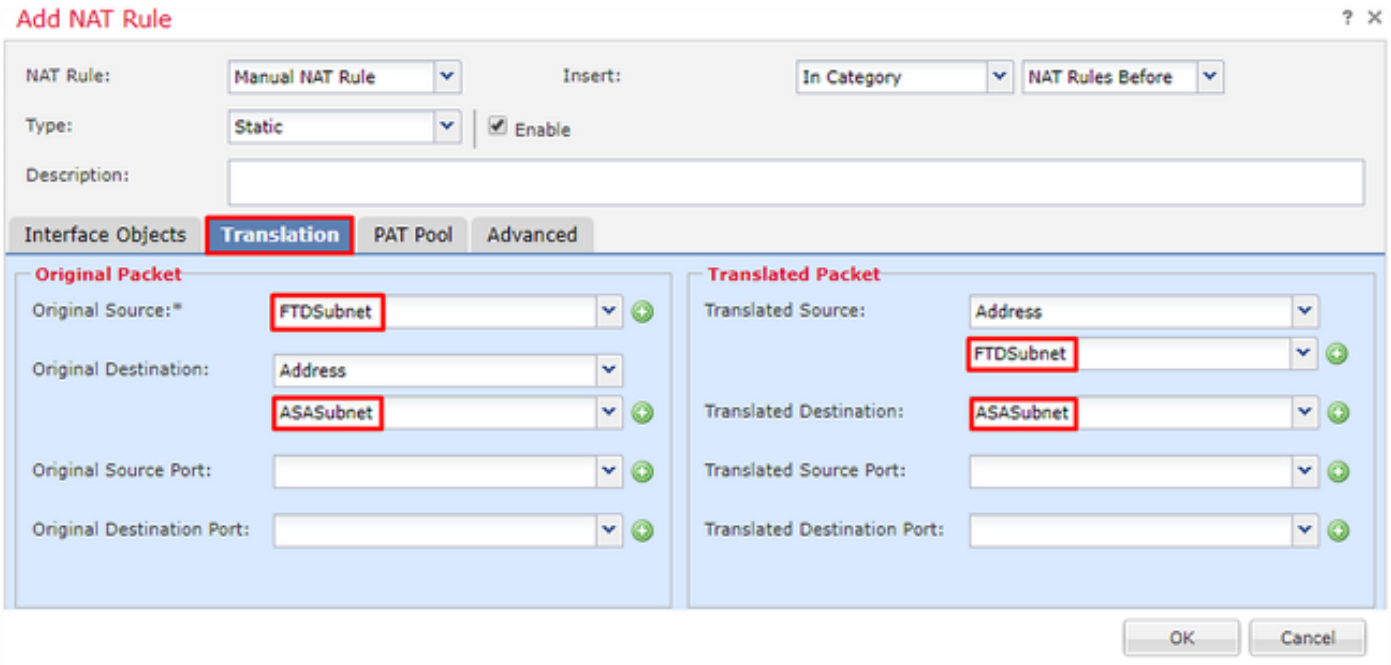
1. Navegue até **Dispositivos > NAT**, selecione a política de NAT que visa o FTD. Crie uma nova regra quando clicar no botão **Adicionar regra**.



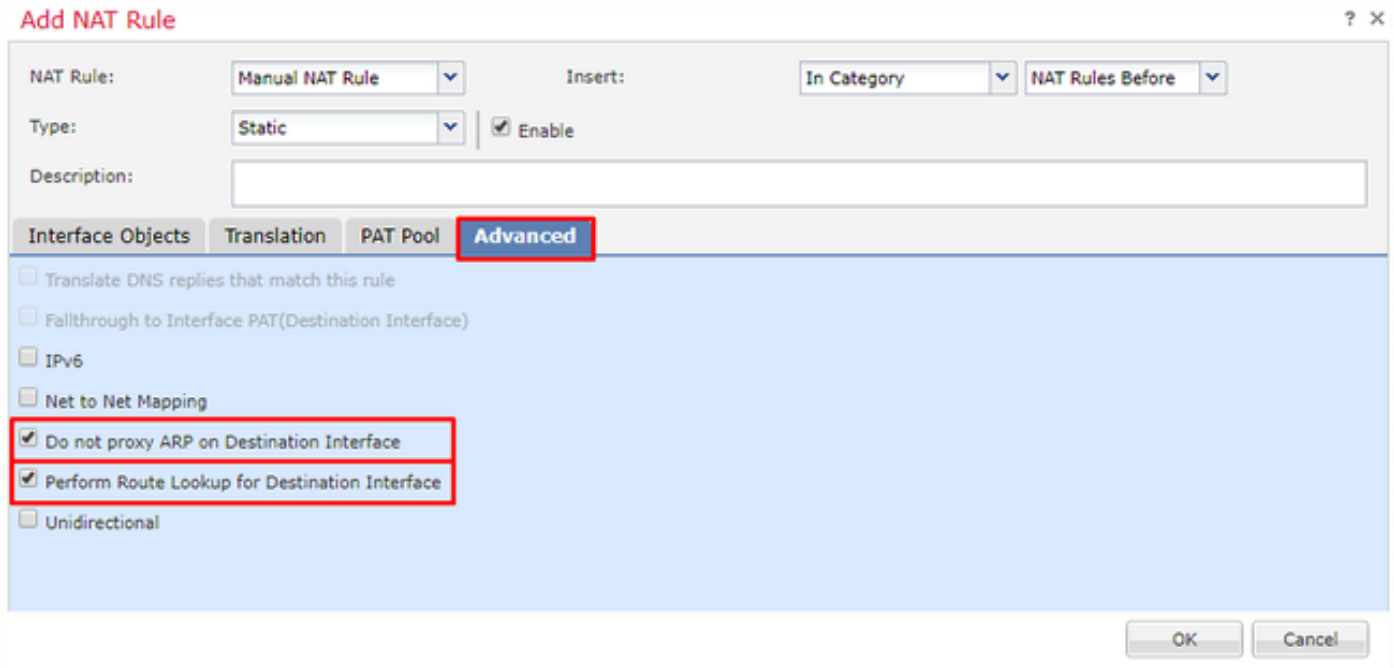
2. Crie uma nova regra NAT manual estática. Consulte as interfaces interna e externa.



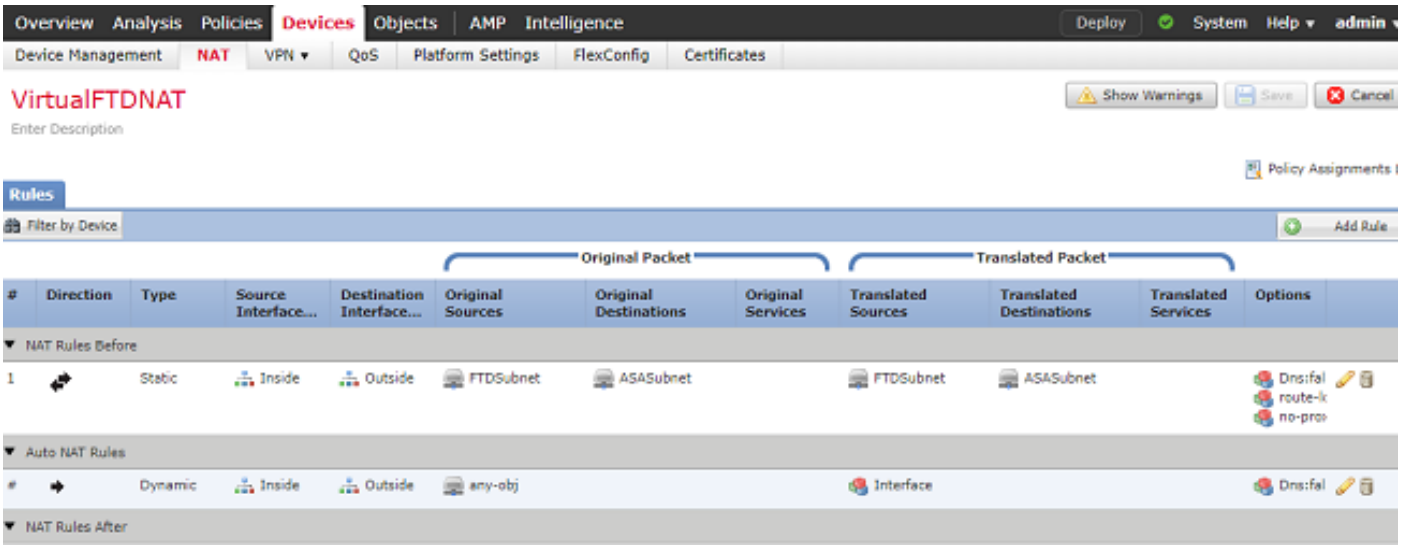
3. Na guia **Tradução** e selecione as sub-redes de origem e de destino. Como esta é uma regra de isenção de NAT, torne a origem/destino original e a origem/destino traduzidos iguais, como mostrado nesta imagem:



4. Por fim, vá para a guia **Avançado** e ative no-proxy-arp e route-lookup.



5. Salve essa regra e examine os resultados finais na lista NAT.



6. Quando a configuração for concluída, salve e implante a configuração no FTD.

Passo 7. Configure o 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 FTD_GP internal
Group-policy FTD_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 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. Crie uma lista de acesso que defina o tráfego a ser criptografado: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSubnet
Subnet 10.10.113.0 255.255.255.0
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 referindo-se aos algoritmos especificados no FTD:

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

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

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 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 FTDSubnet FTDSubnet
no-proxy-arp route-lookup
```

Verificar

> **Note**: No momento, não há como revisar o status do túnel VPN do FMC. Há uma solicitação de aprimoramento para esse recurso CSCvh77603.

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. Ao usar o comando packet-tracer para ativar o túnel VPN, ele deve ser executado duas vezes para verificar se o túnel está ativado. A primeira vez que o comando é emitido, o túnel VPN está inoperante, de modo que o comando packet-tracer falhará com o DROP de criptografia 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 10.10.113.10 8 0 10.10.110.10

Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.113.10 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 FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
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 CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483
ifc outside object-group FMC_INLINE_dst_rule_268436483 rule-id 268436483
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy -
Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
no-proxy-arp route-lookup
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0
```

```
Phase: 10
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 este comando:

Show crypto ikev2 sa

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local
Remote                                                Status         Role
 9528731 172.16.100.20/500
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: 86400/118 sec
Child sa: local selector  10.10.113.0/0 - 10.10.113.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x66be357d/0xb74c8753
```

Solucionar problemas e depurar

Problemas iniciais de conectividade

Ao criar 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 172.16.100.20 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 este comando:

show cap capout

```
firepower# show cap capout

4 packets captured

  1: 11:51:12.059628       172.16.100.20.500 > 192.168.200.10.500:  udp 690
  2: 11:51:12.065243       192.168.200.10.500 > 172.16.100.20.500:  udp 619
  3: 11:51:12.066692       172.16.100.20.500 > 192.168.200.10.500:  udp 288
  4: 11:51:12.069835       192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

Problemas específicos de tráfego

Os problemas comuns de tráfego que você enfrenta 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 Tradução de Endereço de Rede não está sendo ignorada para tráfego VPN.

Para obter mais informações sobre VPNs no FTD gerenciado pelo FMC, você pode encontrar o guia de configuração completo aqui: Guia de configuração do FTD gerenciado pelo FMC