Configurar o Anyconnect VPN para FTD via IKEv2 com ISE

Contents

Introdução

Este documento descreve a configuração básica da VPN de acesso remoto com autenticação IKEv2 e ISE no FTD gerenciado pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN básica, TLS e Internet Key Exchange versão 2 (IKEv2)
- Autenticação, Autorização e Tarifação Básicas (AAA - Basic Authentication, Authorization, and Accounting) e RADIUS
- Experiência com o Firepower Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Defesa contra ameaças do Cisco Firepower (FTD) 7.2.0
- Cisco FMC 7.2.0
- AnyConnect 4.10.07073
- Cisco ISE 3.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

IKEv2 e Secure Sockets Layer (SSL) são protocolos usados para estabelecer conexões seguras, particularmente no contexto de VPNs. O IKEv2 fornece métodos de criptografia e autenticação fortes, oferecendo um alto nível de segurança para conexões VPN.

Este documento fornece um exemplo de configuração para FTD versão 7.2.0 e posterior, que permite VPN de acesso remoto para usar Transport Layer Security (TLS) e IKEv2. Como um cliente, o Cisco AnyConnect pode ser usado, que é suportado em várias plataformas.

Configurar

1. Importar o Certificado SSL

Os certificados são essenciais quando o AnyConnect é configurado.

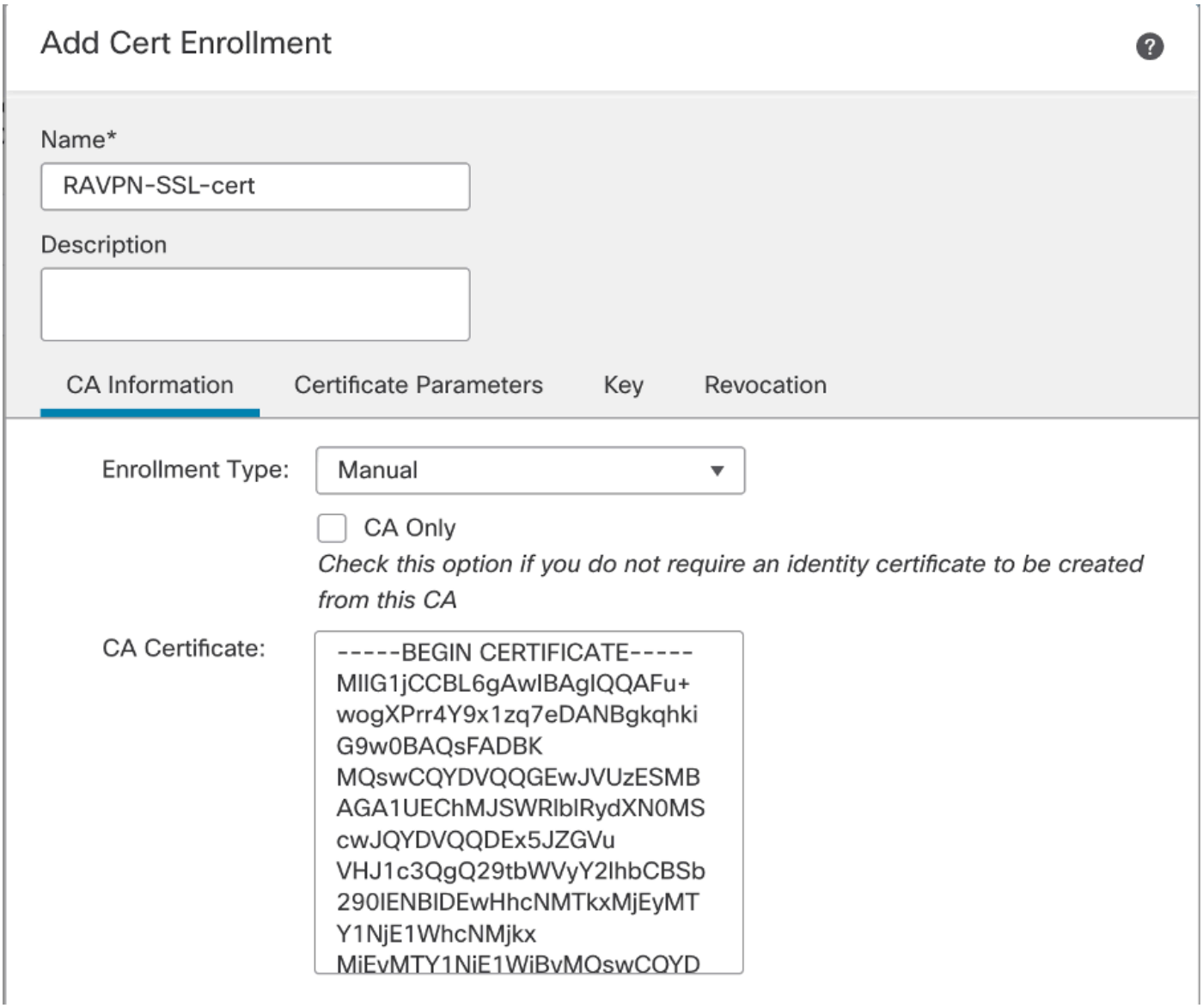
Há limitações para o registro manual de certificados:
1. No FTD, é necessário um certificado de Autoridade de Certificação (CA) antes de gerar uma CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado).
2. Se o CSR for gerado externamente, um método diferente de PKCS12 será usado.

Há vários métodos para obter um certificado no dispositivo FTD, mas o seguro e fácil é criar um CSR e obtê-lo assinado por uma CA. Veja como fazer isso:

1. Navegue até Objects > Object Management > PKI > Cert Enrollment e clique em Add Cert Enrollment.

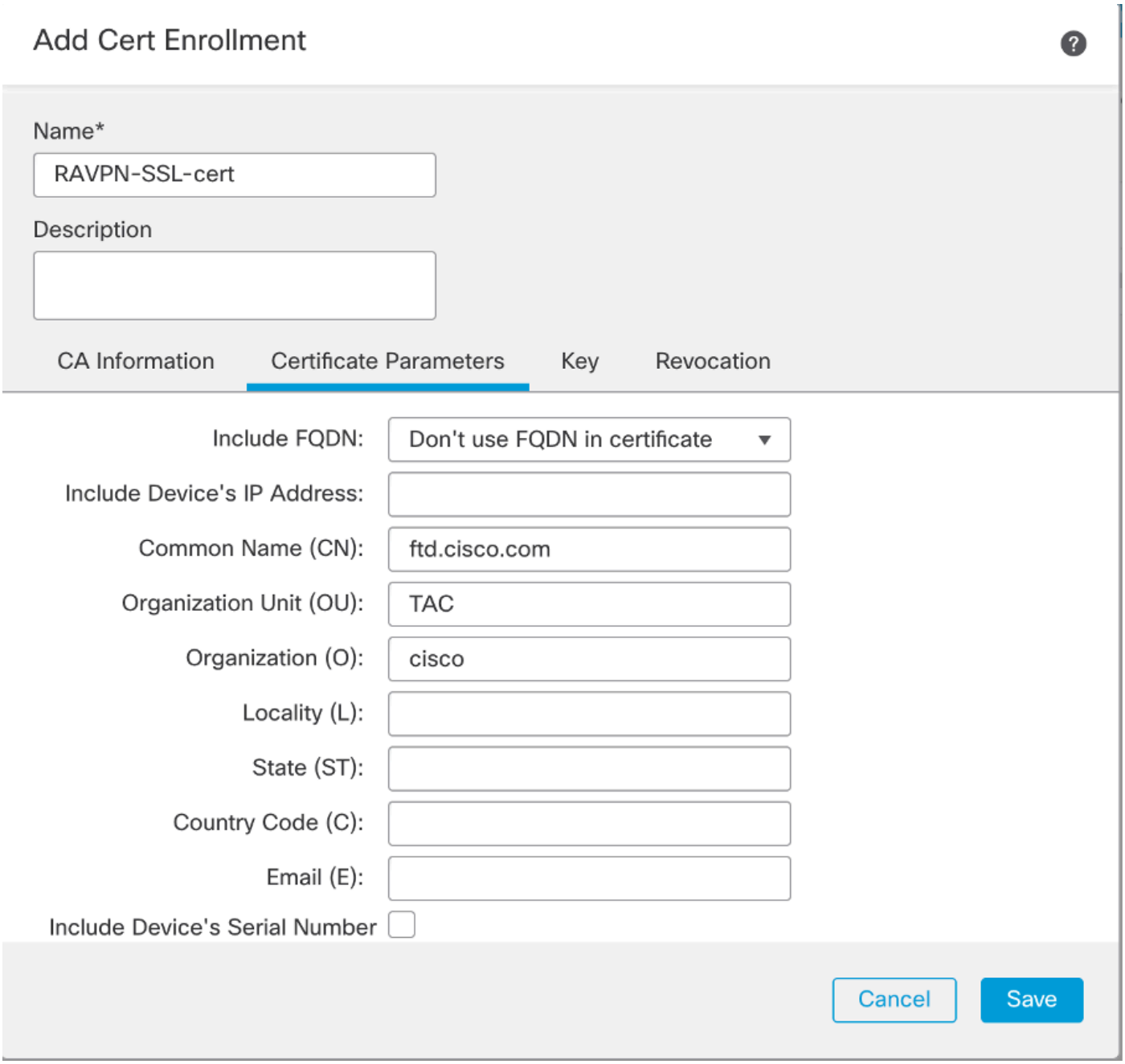
2. Informe o nomeRAVPN-SSL-cert do ponto confiável .

3. Na CA Information guia, escolha Tipo de inscrição como Manual e cole o certificado CA como mostrado na imagem.



Certificado FMC - CA

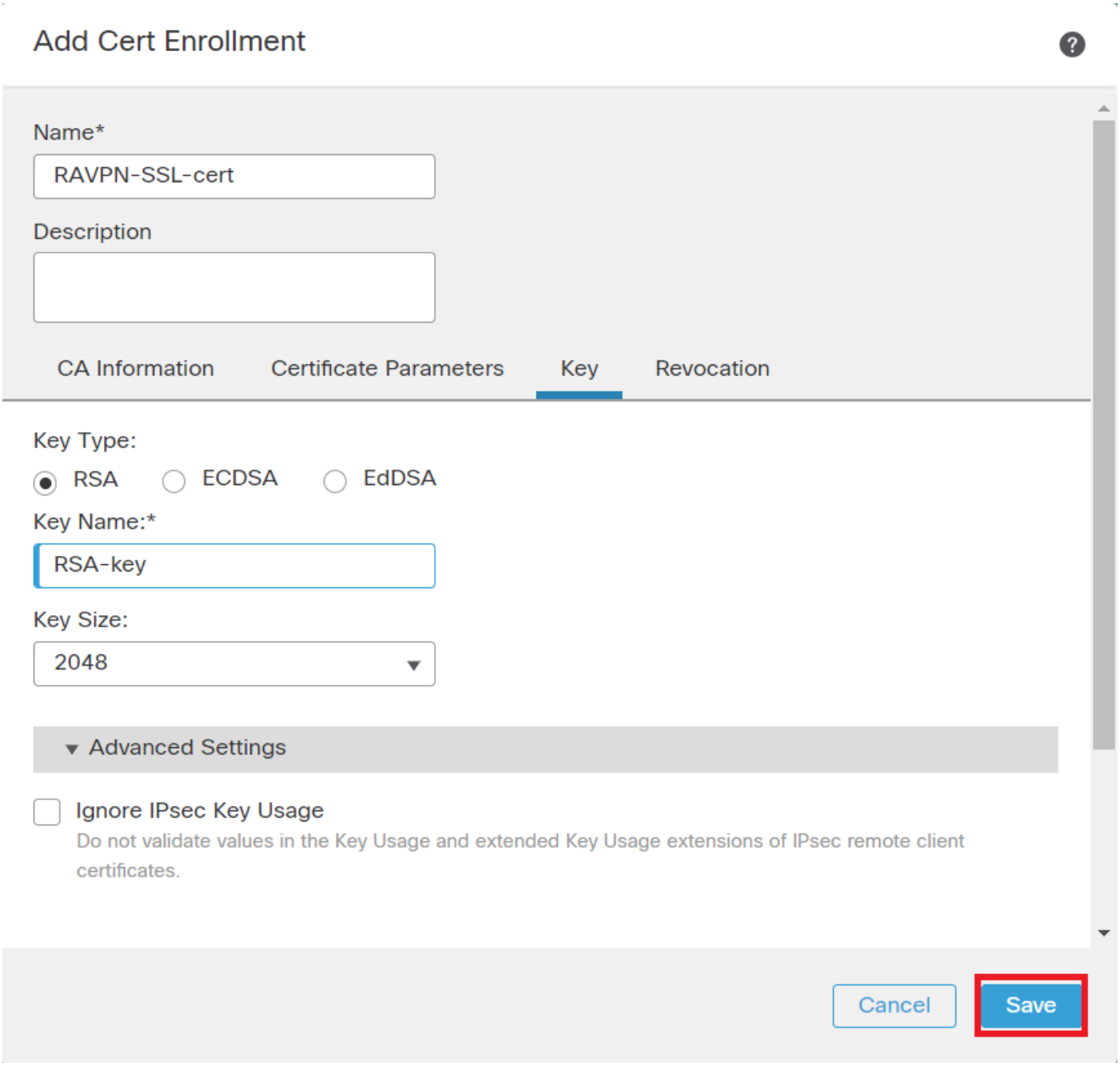
4. Em Certificate Parameters, informe o nome do assunto. Por exemplo:



FMC - Parâmetros do certificado

5. Na Key guia, escolha o tipo de chave e forneça um nome e um tamanho de bit. Para RSA, 2048 bits é o mínimo.

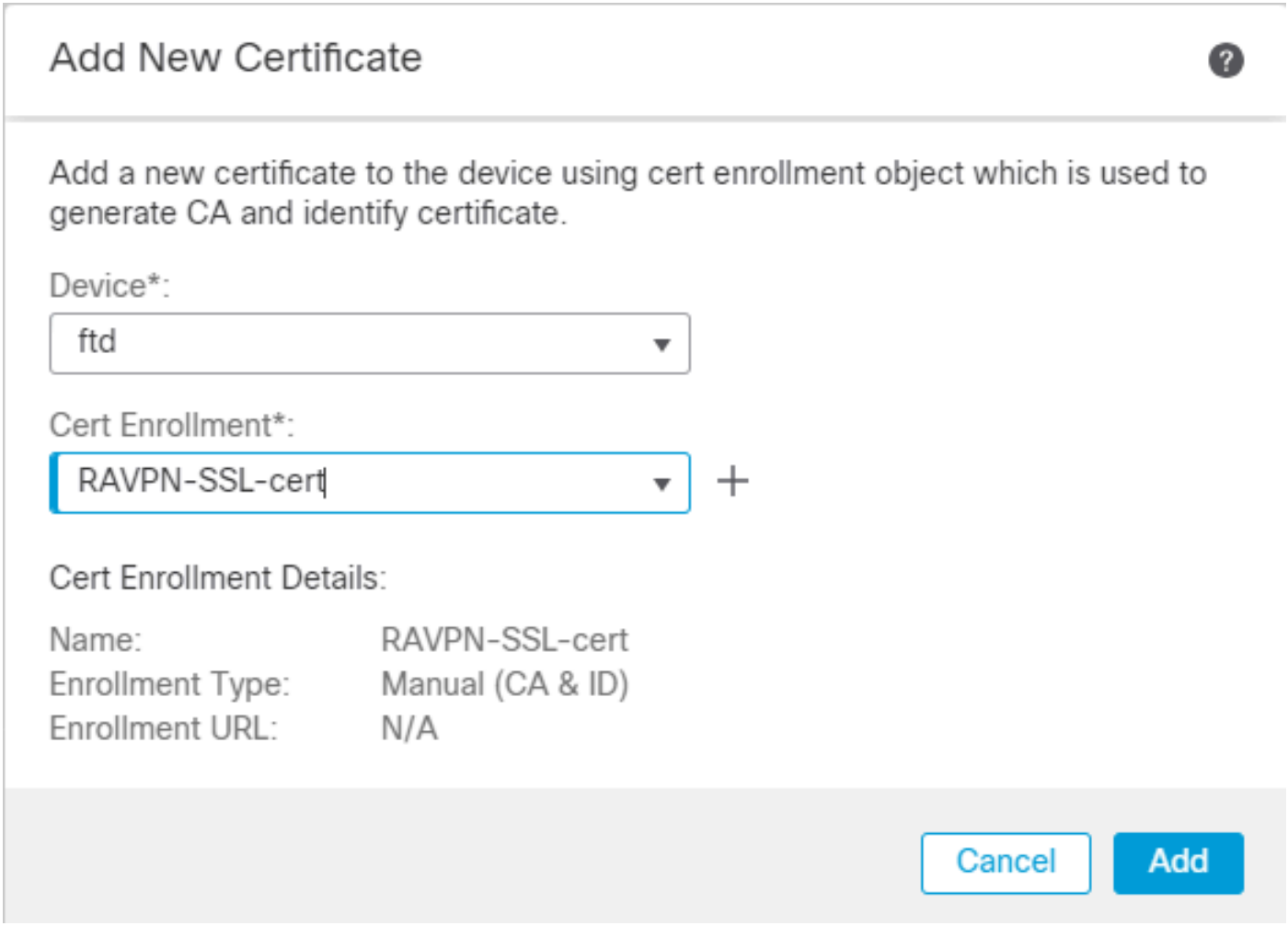
6. Clique em Save.



FMC - Chave de certificado

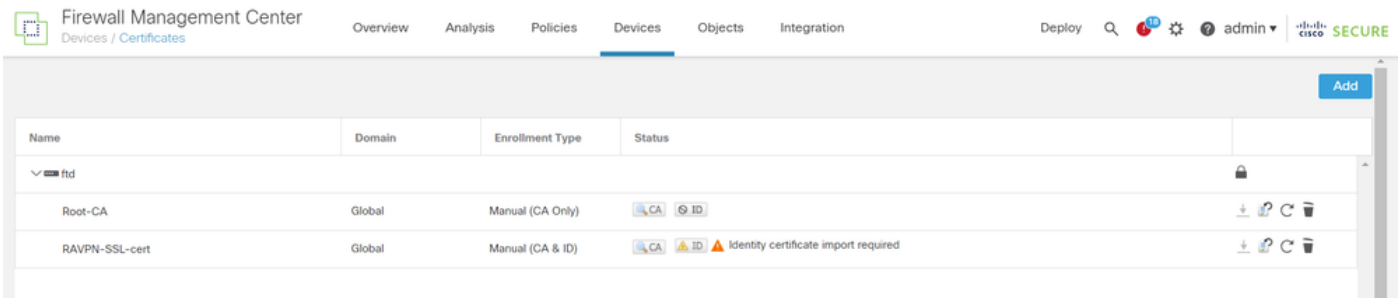
7. Navegue até Devices > Certificates > Add > New Certificate.

8. Escolha Device. Em Cert Enrollment, escolha o ponto de confiança criado e clique Addcomo mostrado na imagem.

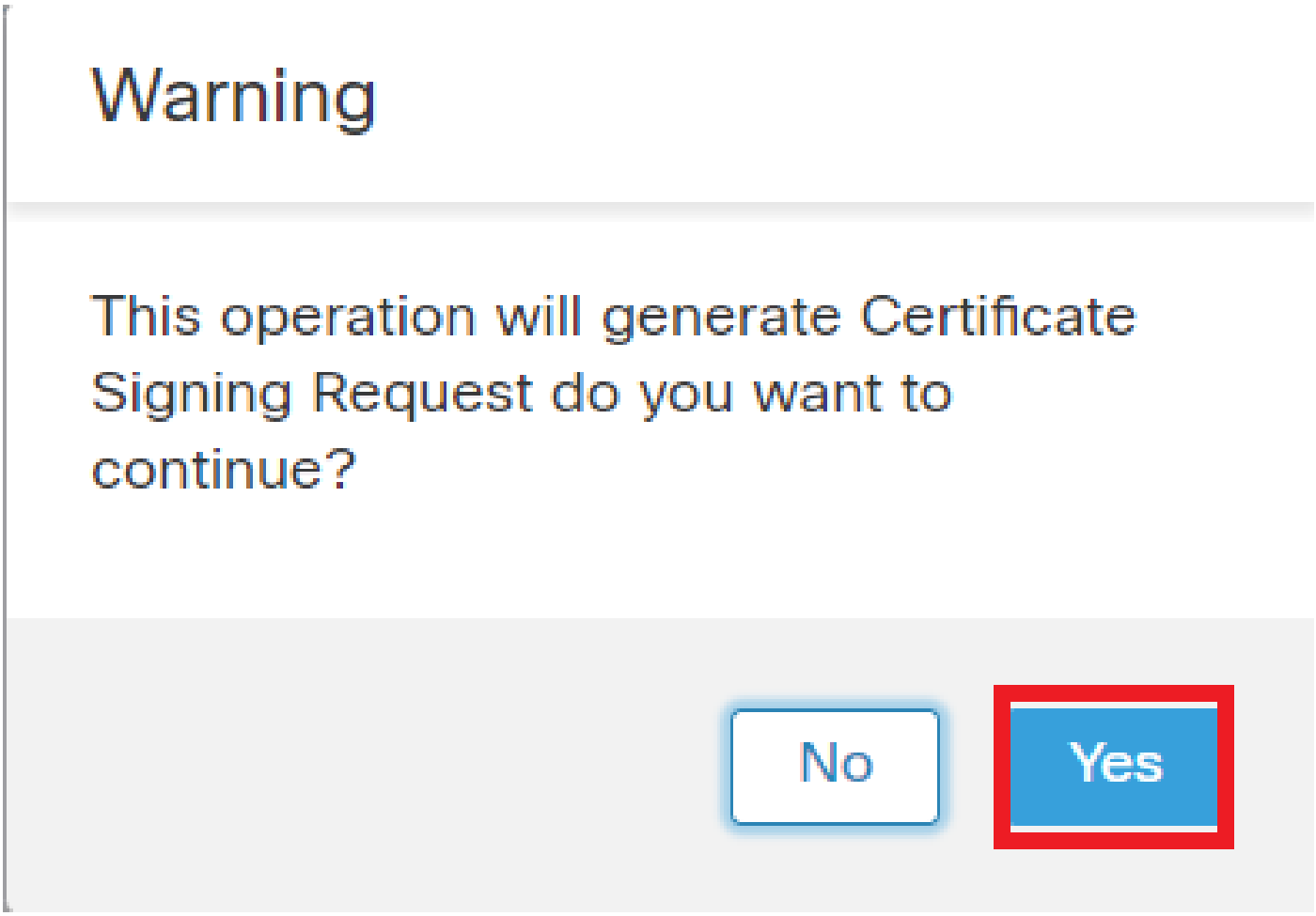


FMC - Inscrição de Certificado no FTD

9. Clique em ID e um prompt para gerar CSR será exibido. Escolha Yes.



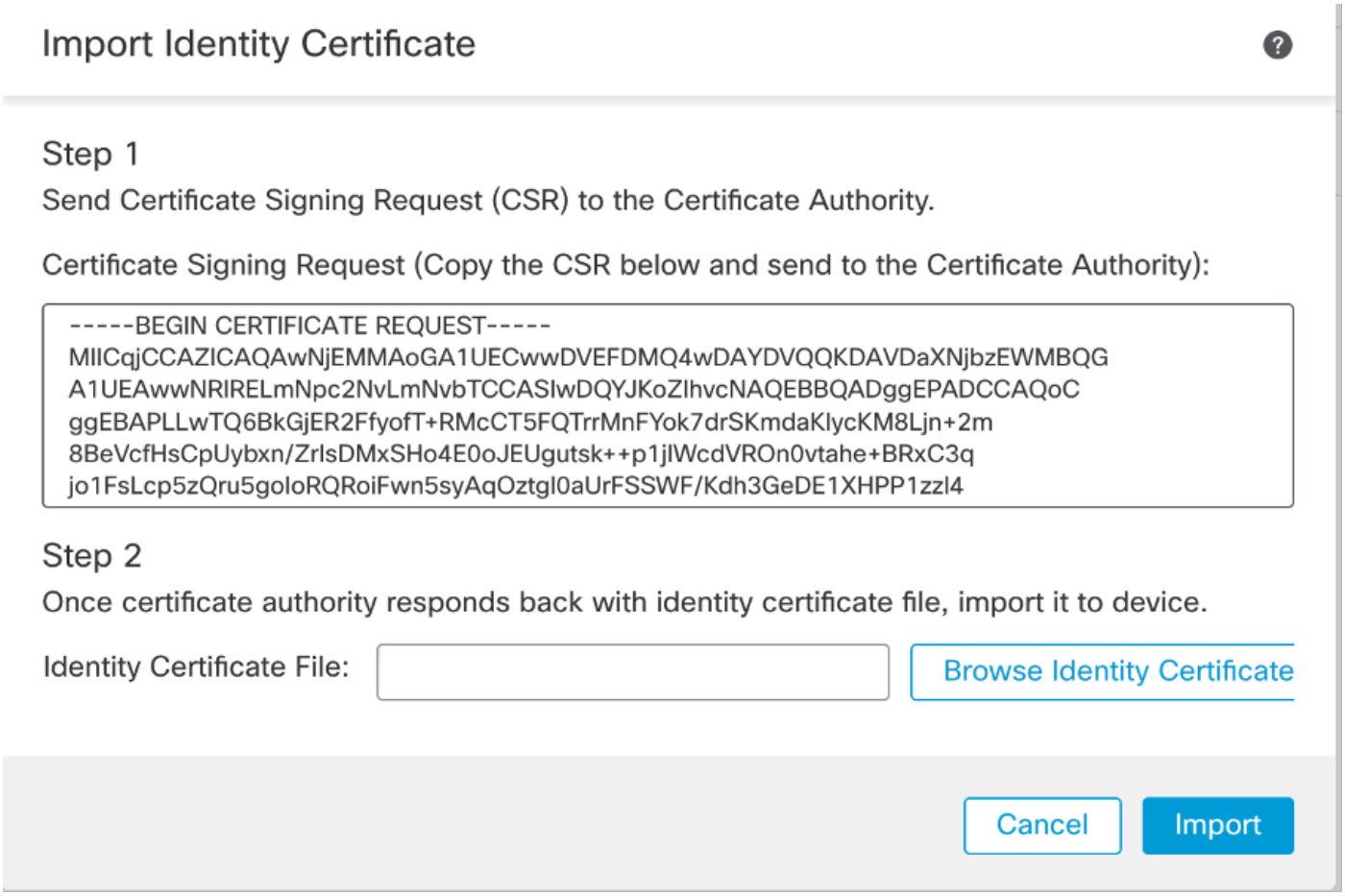
FMC - Certificado CA registrado



FMC - Gerar CSR

10. É gerada uma CSR que pode ser compartilhada com a CA para obter o certificado de identidade.

11. Depois de receber o certificado de identidade da CA no formato base64, escolha-o no disco clicando em Browse Identity Certificate Import e conforme mostrado na imagem.



FMC - Certificado de identidade de importação

12. Quando a importação for bem-sucedida, o ponto de confiança RAVPN-SSL-cert será visto como:

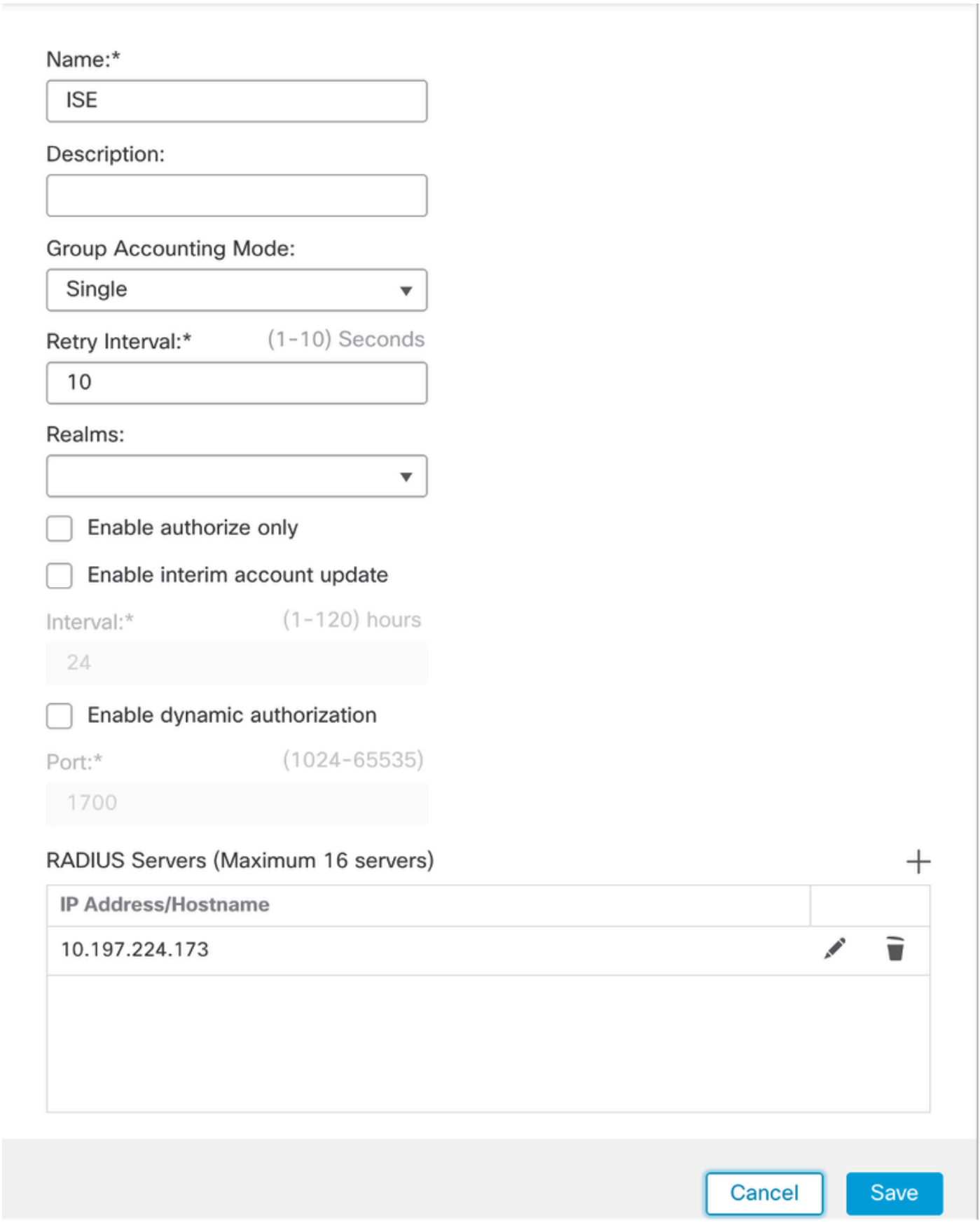
FMC - Registro de Trustpoint Bem-sucedido

2. Configurar o Servidor RADIUS

2.1. Gestão do FTD no CVP

1. Navegue até Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. Insira o nome ISE e adicione Servidores RADIUS clicando em +.

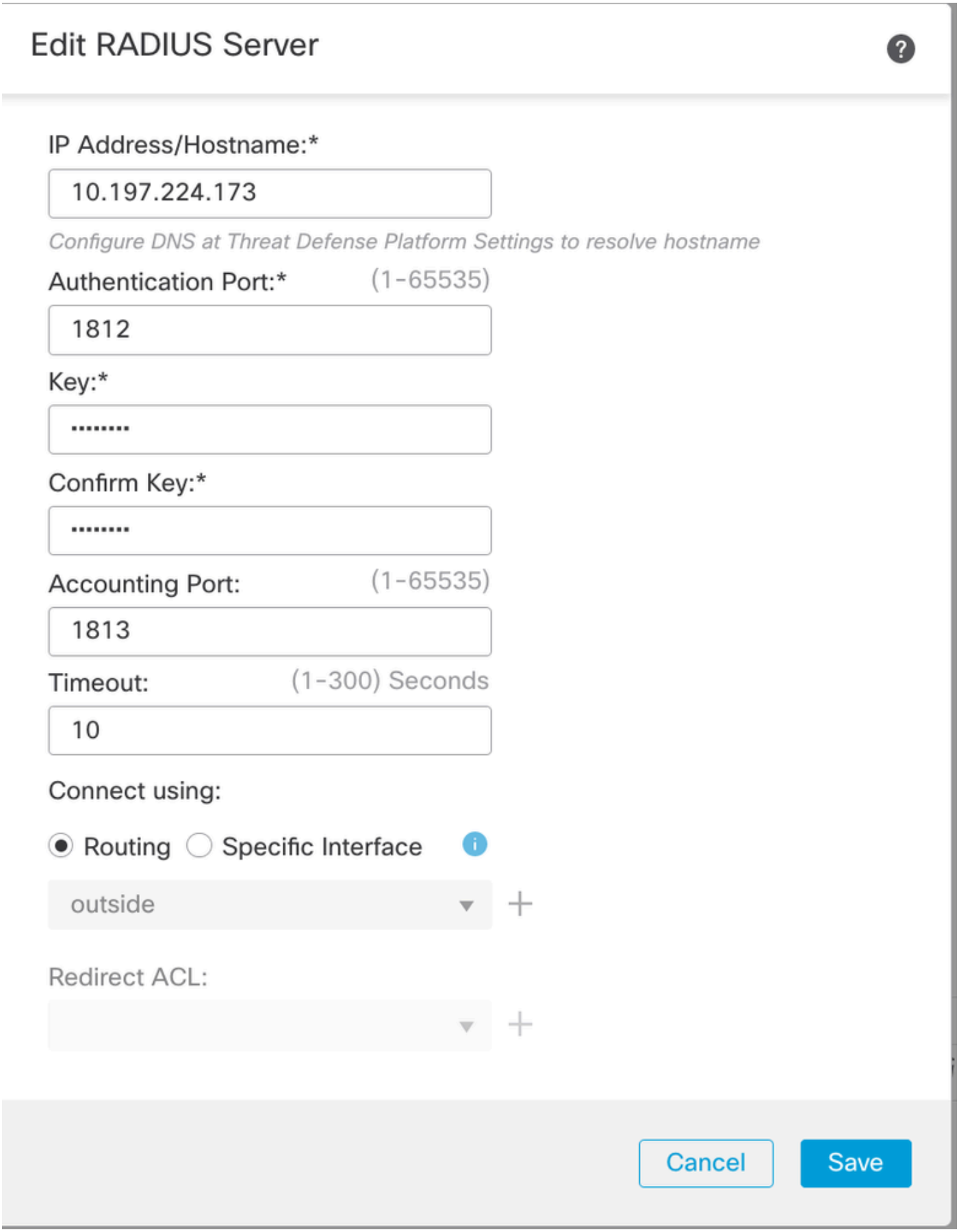


FMC - Configuração do servidor Radius

3. Mencione o endereço IP do servidor ISE Radius junto com o segredo compartilhado (chave) que é o mesmo do servidor ISE.

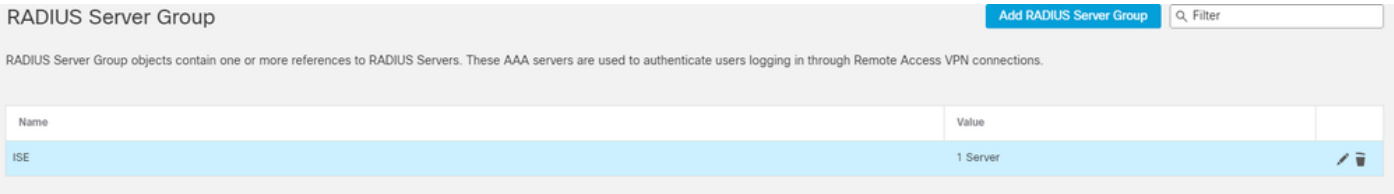
4. Escolha Routing ou Specific Interface através do qual o FTD se comunica com o servidor ISE.

5. Clique Save conforme mostrado na imagem.



FMC - Servidor ISE

6. Uma vez salvo, o Servidor é adicionado sob o RADIUS Server Group como mostrado na imagem.



FMC - Grupo de servidores RADIUS

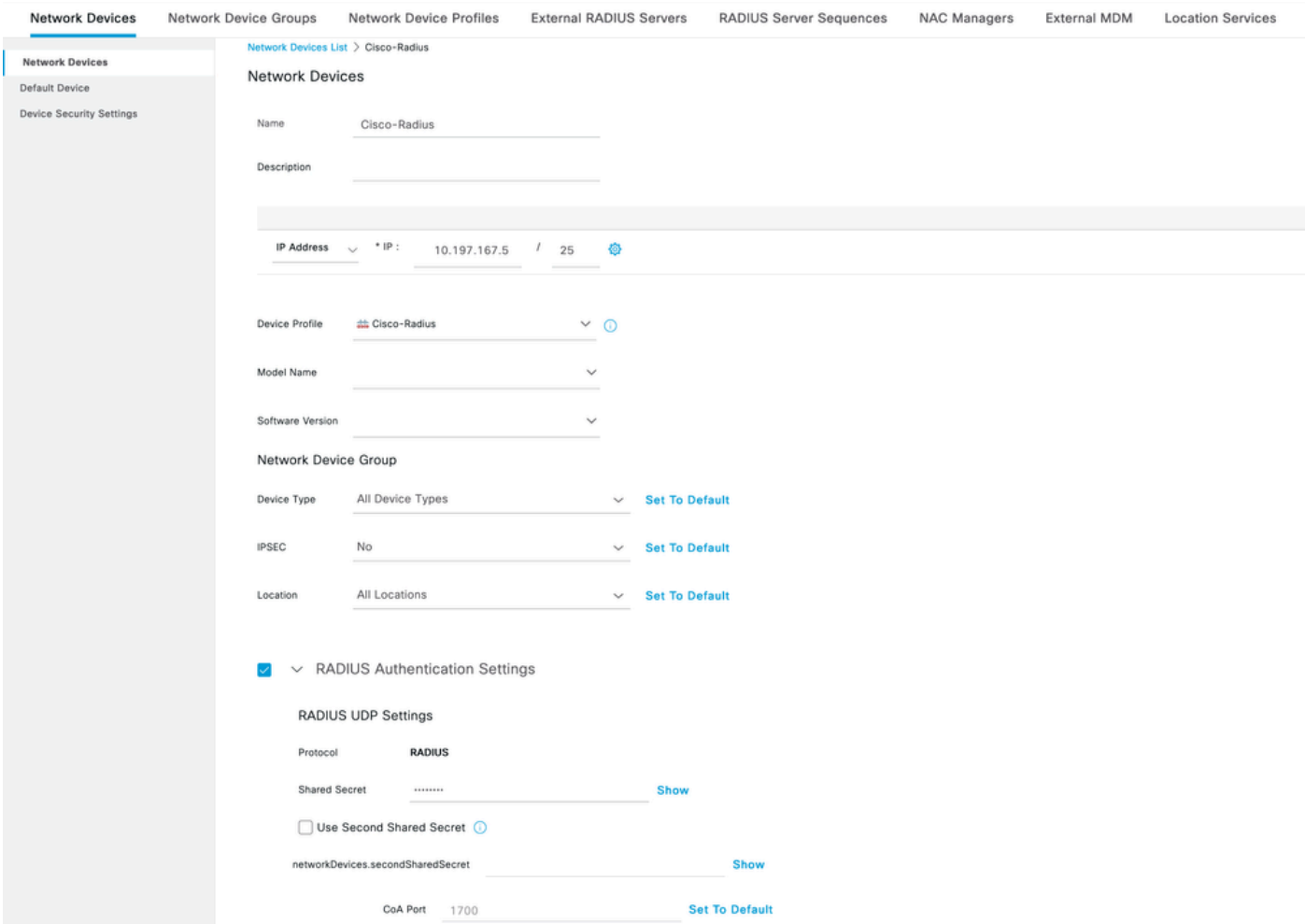
2.2. Gestão do DTF no ISE

1. Navegue até Network Devices e clique emAdd.

2. Insira o Nome 'Cisco-Radius' do servidor e IP Addressdo cliente radius que é a interface de comunicação do FTD.

3. Em Radius Authentication Settings, adicione o Shared Secret.

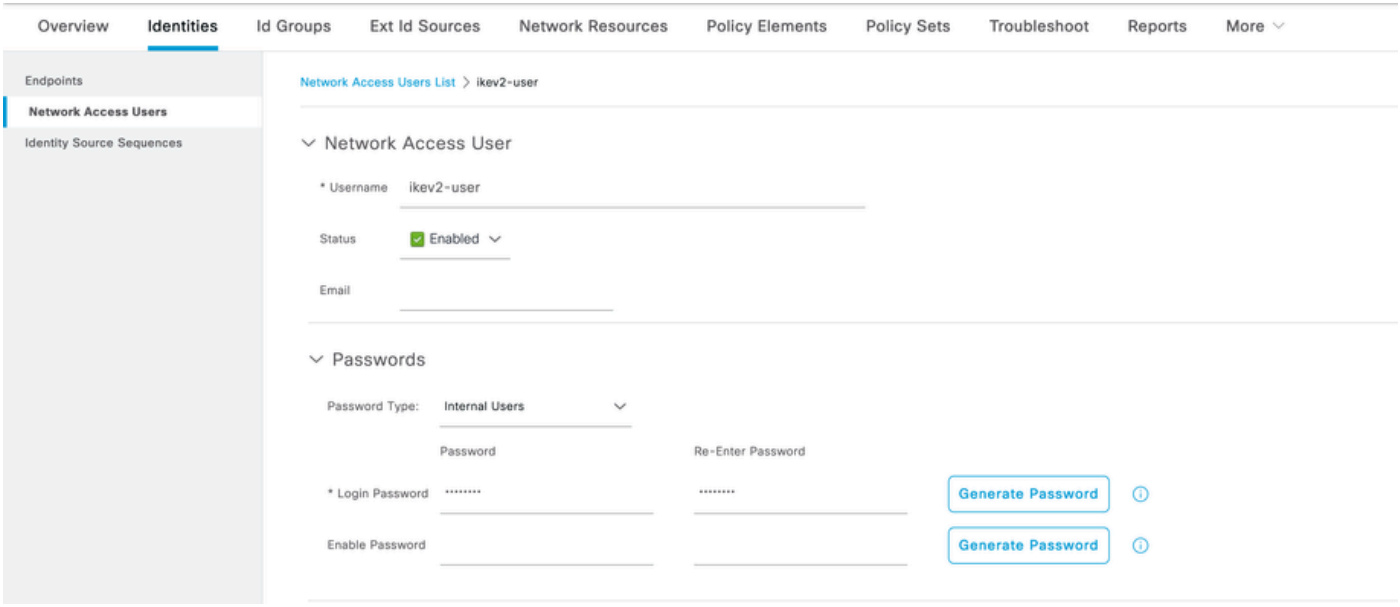
4. Clique em Save .



ISE - Dispositivos de rede

5. Para criar usuários, navegue até Network Access > Identities > Network Access Users e clique em Add.

6. Crie um NomedeUsuário eSenha de Logon conforme necessário.



ISE - Usuários

7. Para configurar a política básica, navegue até Policy > Policy Sets > Default > Authentication Policy > Default, escolha All_User_ID_Stores.

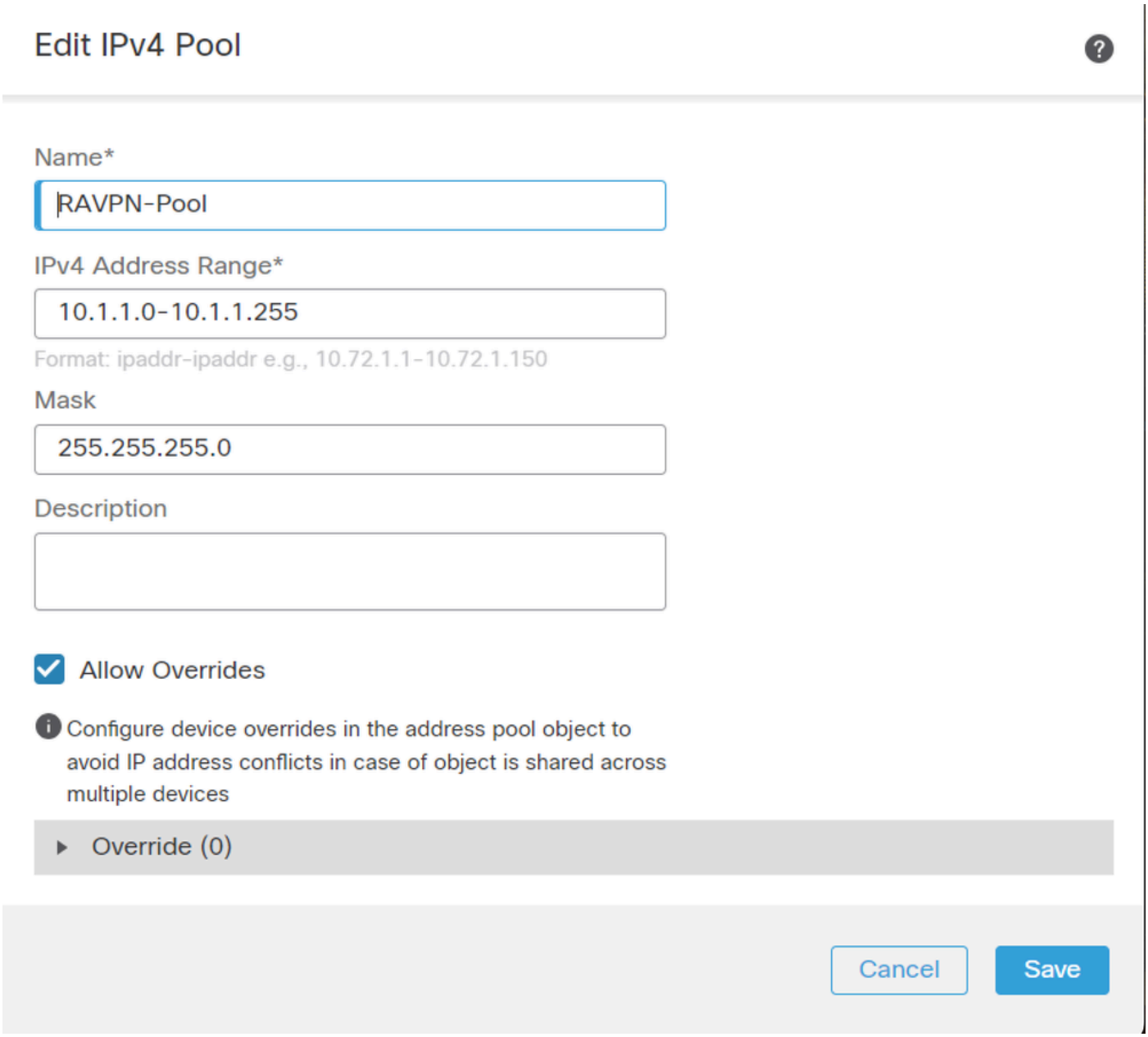
8. Navegue até Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, e escolha PermitAccesscomo mostrado na imagem.

ISE - Política de autenticação

ISE - Política de autorização

3. Criar um pool de endereços para usuários de VPN no FMC

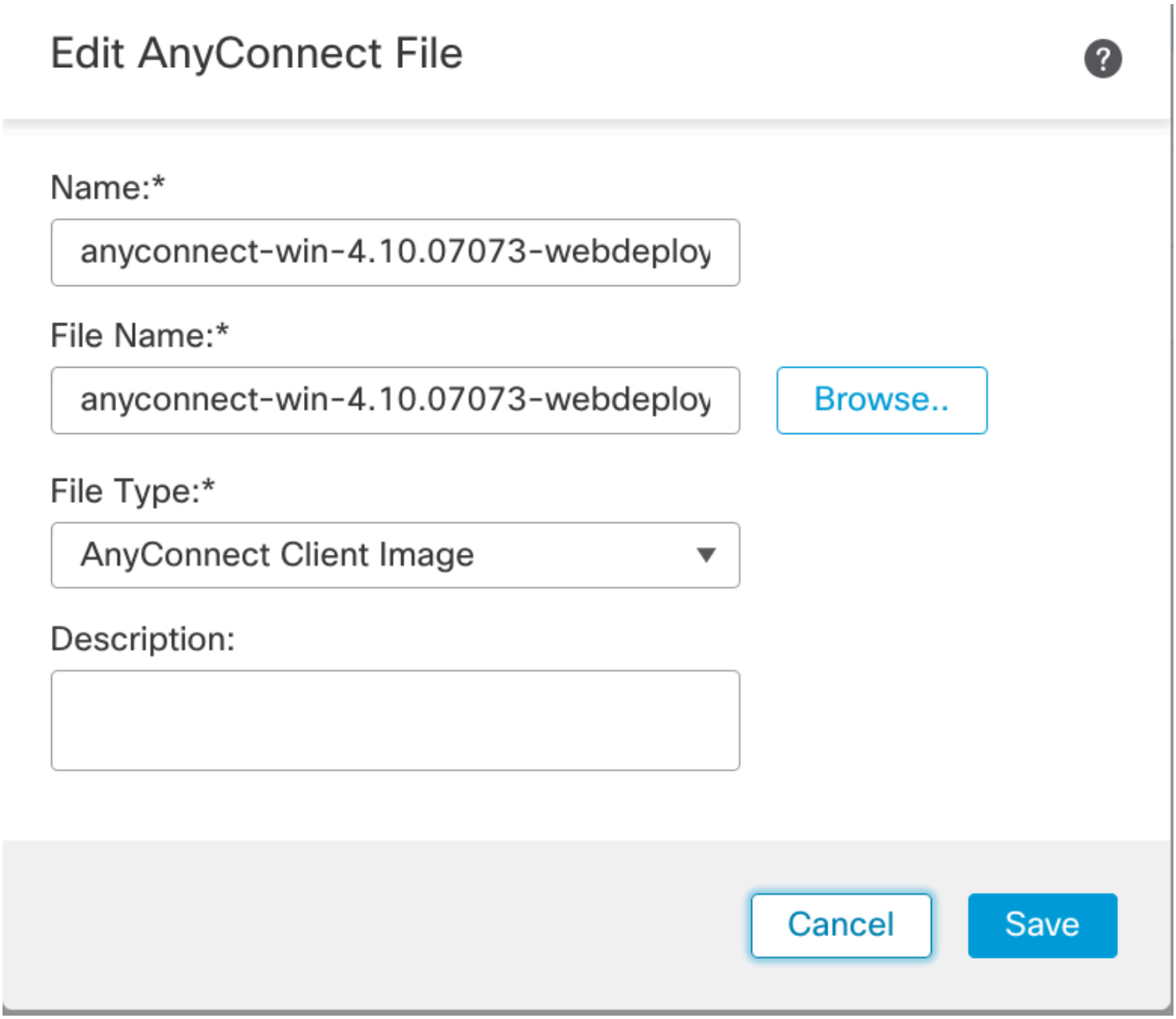
1. Navegue até Objects > Object Management > Address Pools > Add IPv4 Pools.
2. Informe o nome RAVPN-Pool e **a Faixa de Endereços**, a máscara é opcional.
3. Clique em **Salvar**.



FMC - Pool de endereços

4. Carregar imagens do AnyConnect

1. Navegue até Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Insira o nome anyconnect-win-4.10.07073-webdeploy e clique Browse para escolher o arquivo **Anyconnect** do disco, clique em Save como mostrado na imagem.



FMC - Imagem do Anyconnect Client

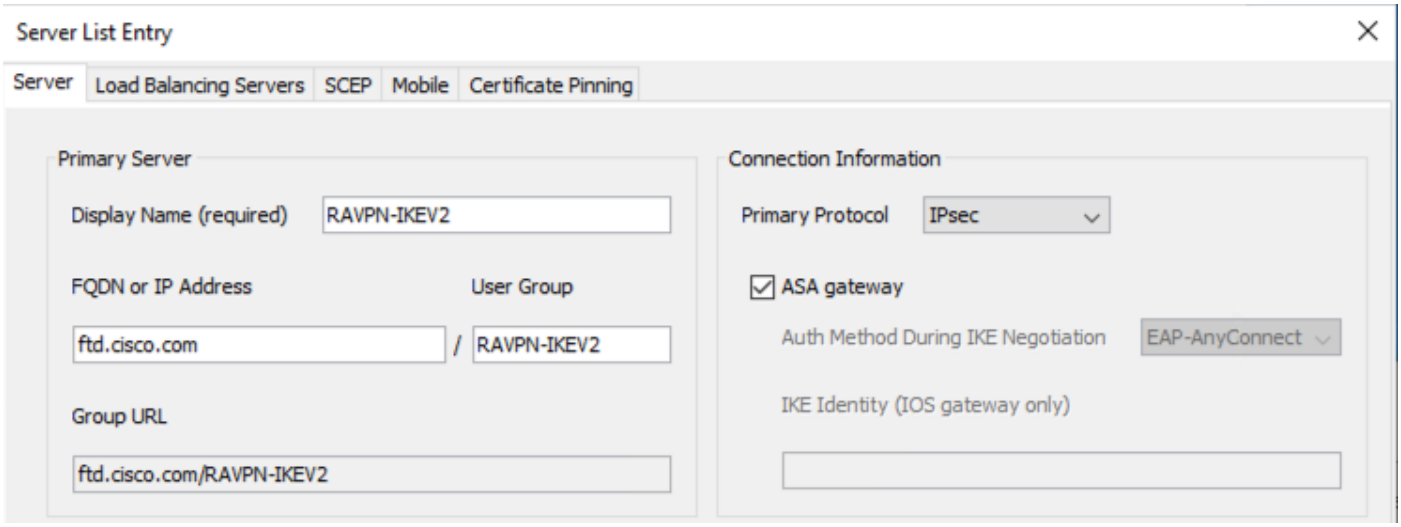
5. Criar Perfil XML

5.1. Sobre o Editor de perfis

1. Faça o download do Editor de perfis no software.cisco.com e abra-o.
2. Navegue até **Server List** > **Add**...

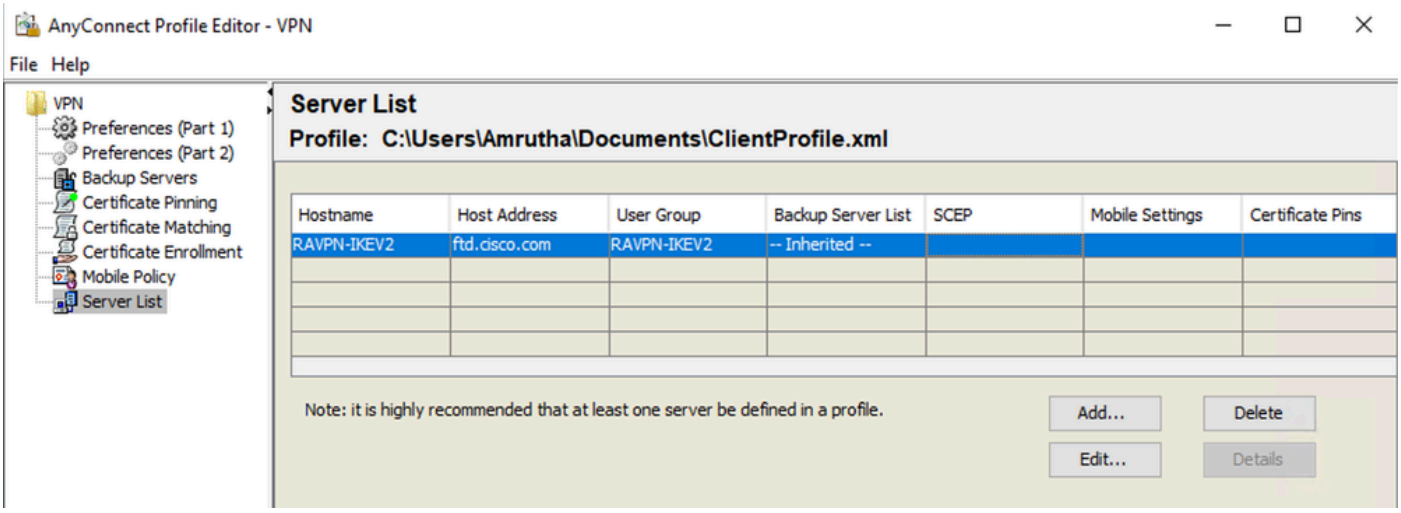
3. Informe o Nome para Exibição RAVPN-IKEV2 e FQDN juntamente com o **Grupo de Usuários** (nome do alias).

4. Escolha o protocolo primário IPsec , asclique **Ok** conforme mostrado na imagem.



Editor de perfis - Lista de servidores

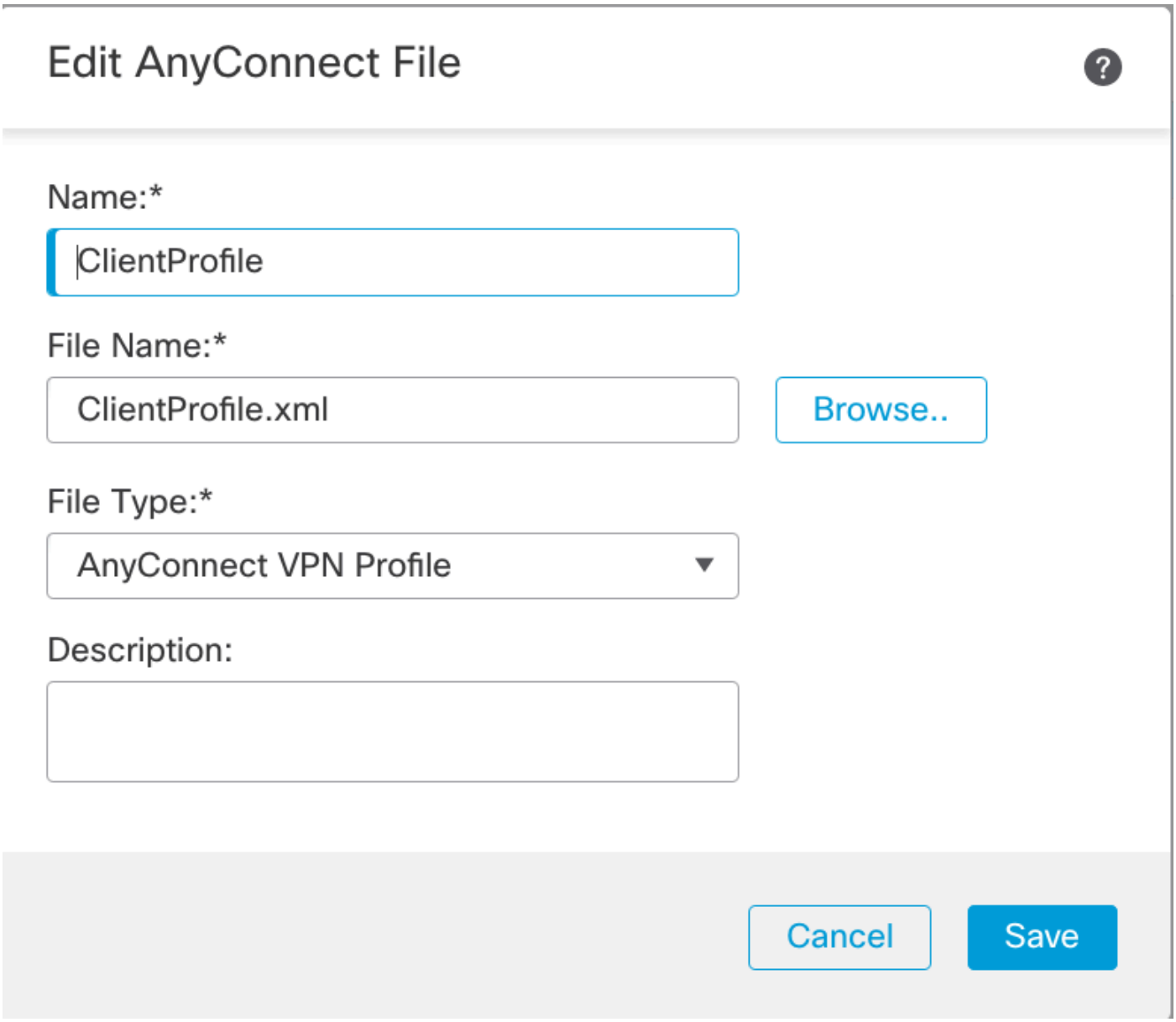
5. A Lista de Servidores é adicionada. Salve-o como ClientProfile.xml .



Editor de perfis - ClientProfile.xml

5.2. **No CVP**

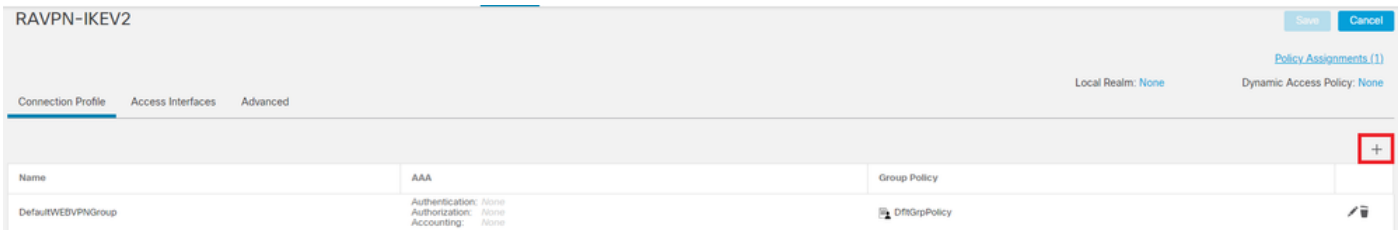
1. Navegue até Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Insira um Nome ClientProfile e clique Browse para escolher ClientProfile.xml arquivo do disco.
3. Clique em **Save** .



FMC - Perfil de VPN do Anyconnect

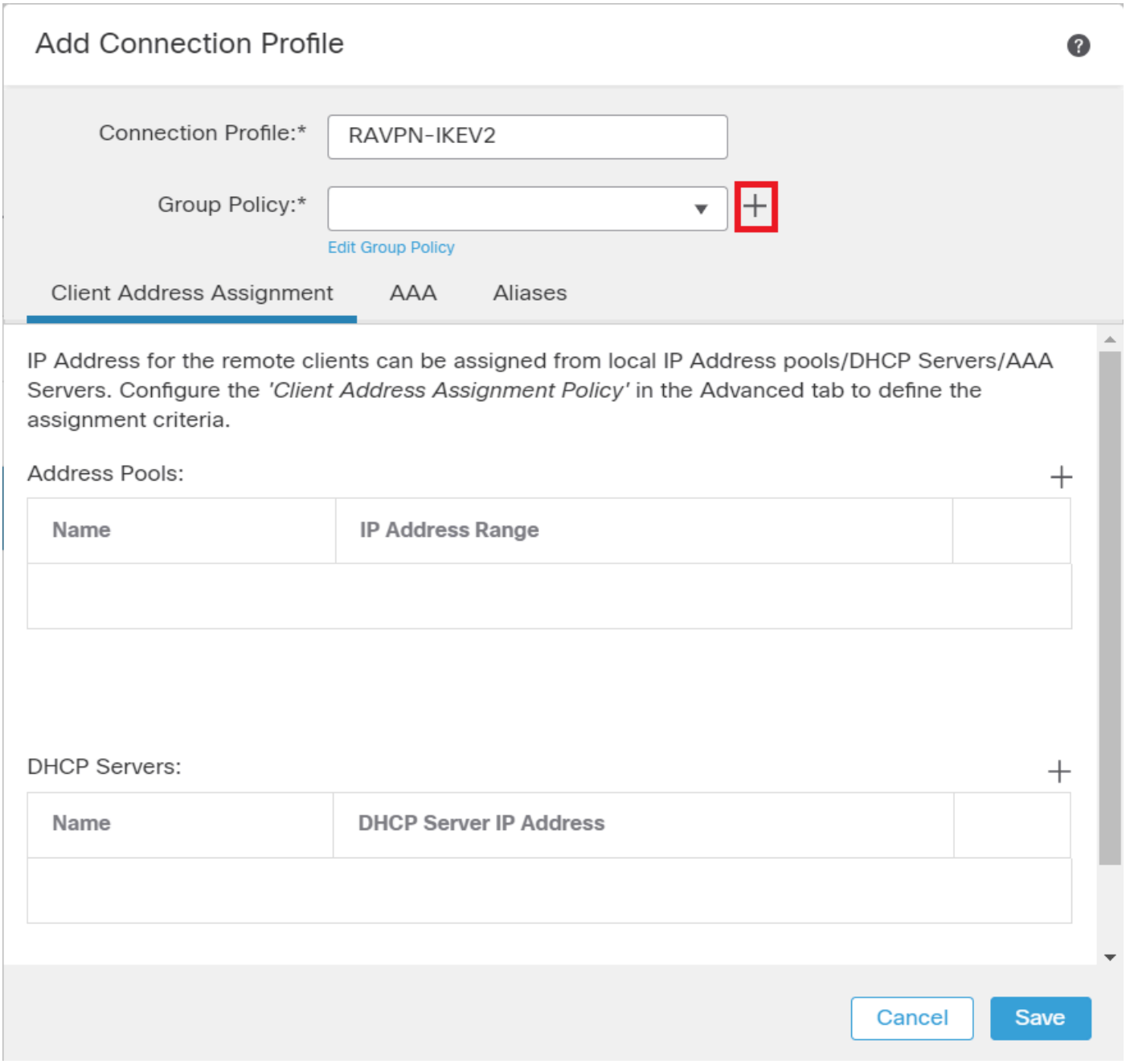
6. Configurar Acesso Remoto

1. Navegue até Devices > VPN > Remote Accesse clique em + para adicionar um Perfil de Conexão conforme mostrado na imagem.



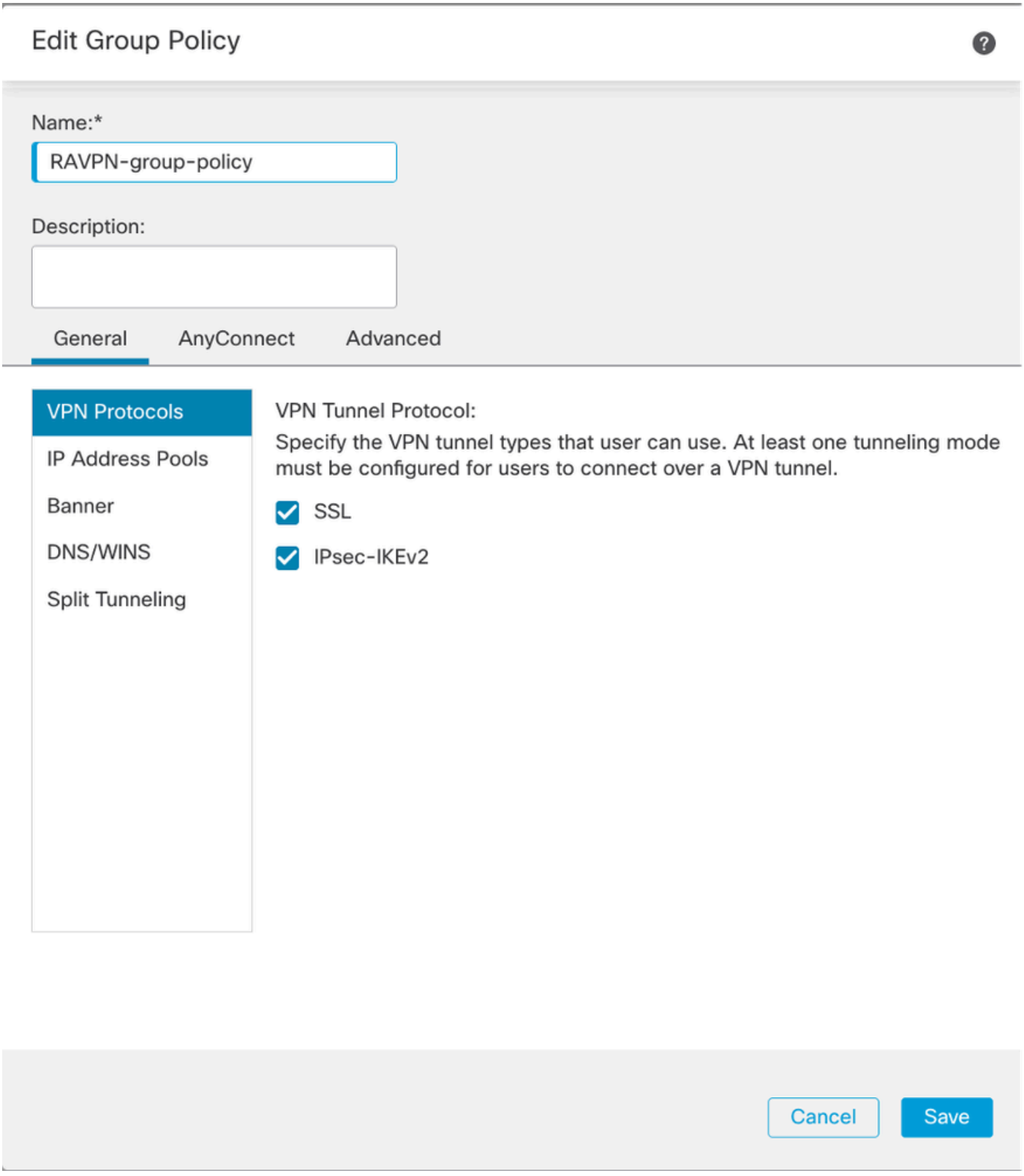
FMC - Remote Access Connection Profile (Perfil de conexão de acesso remoto)

2. Digite o nome do perfil de conexão RAVPN-IKEV2 e crie uma política de grupo clicando +em **Group Policy**como mostrado na imagem.



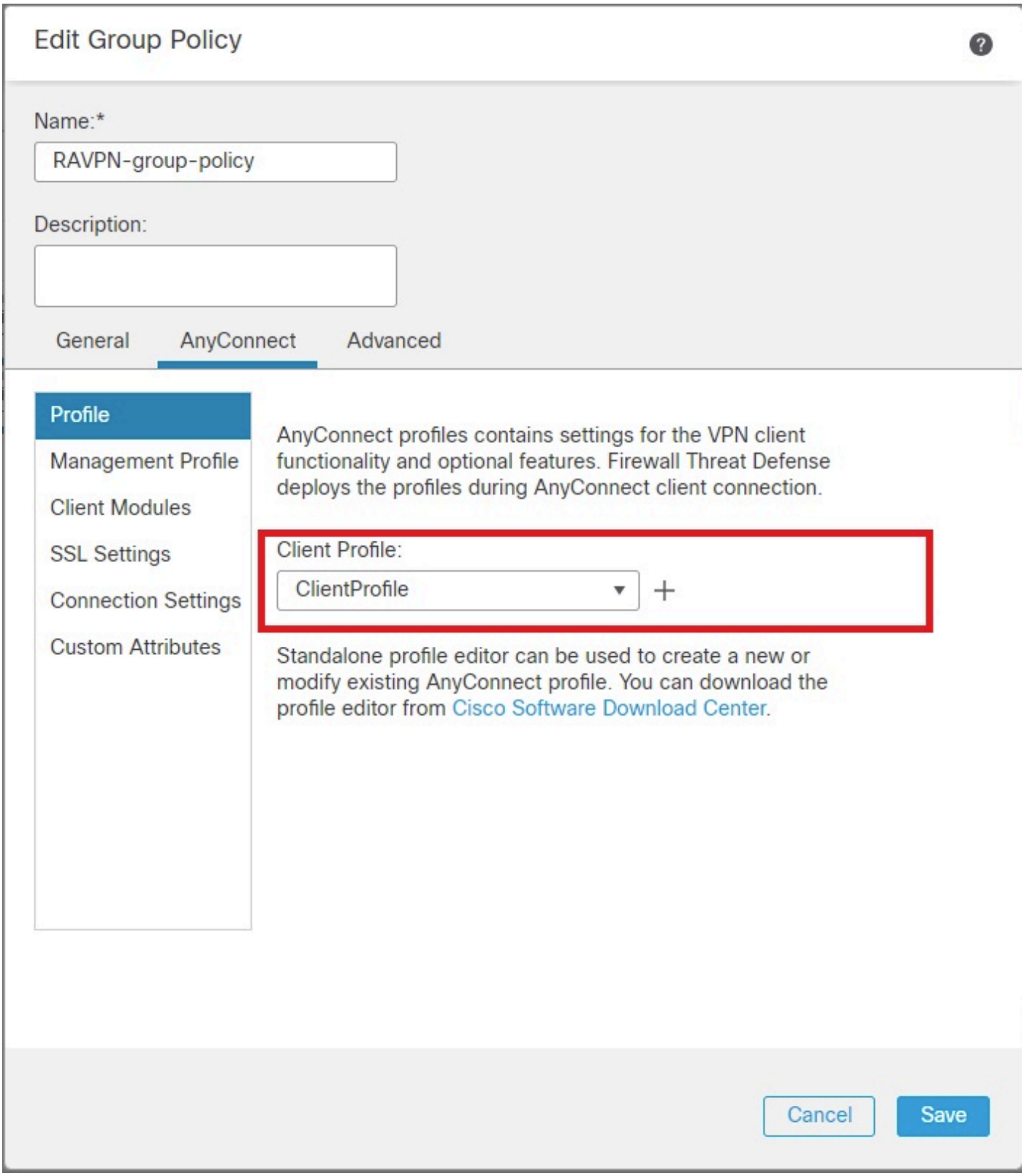
FMC - Política de grupo

3. Insira o nome RAVPN-group-policy e escolha os protocolos VPN **SSL and IPsec-IKEv2** como mostrado na imagem.



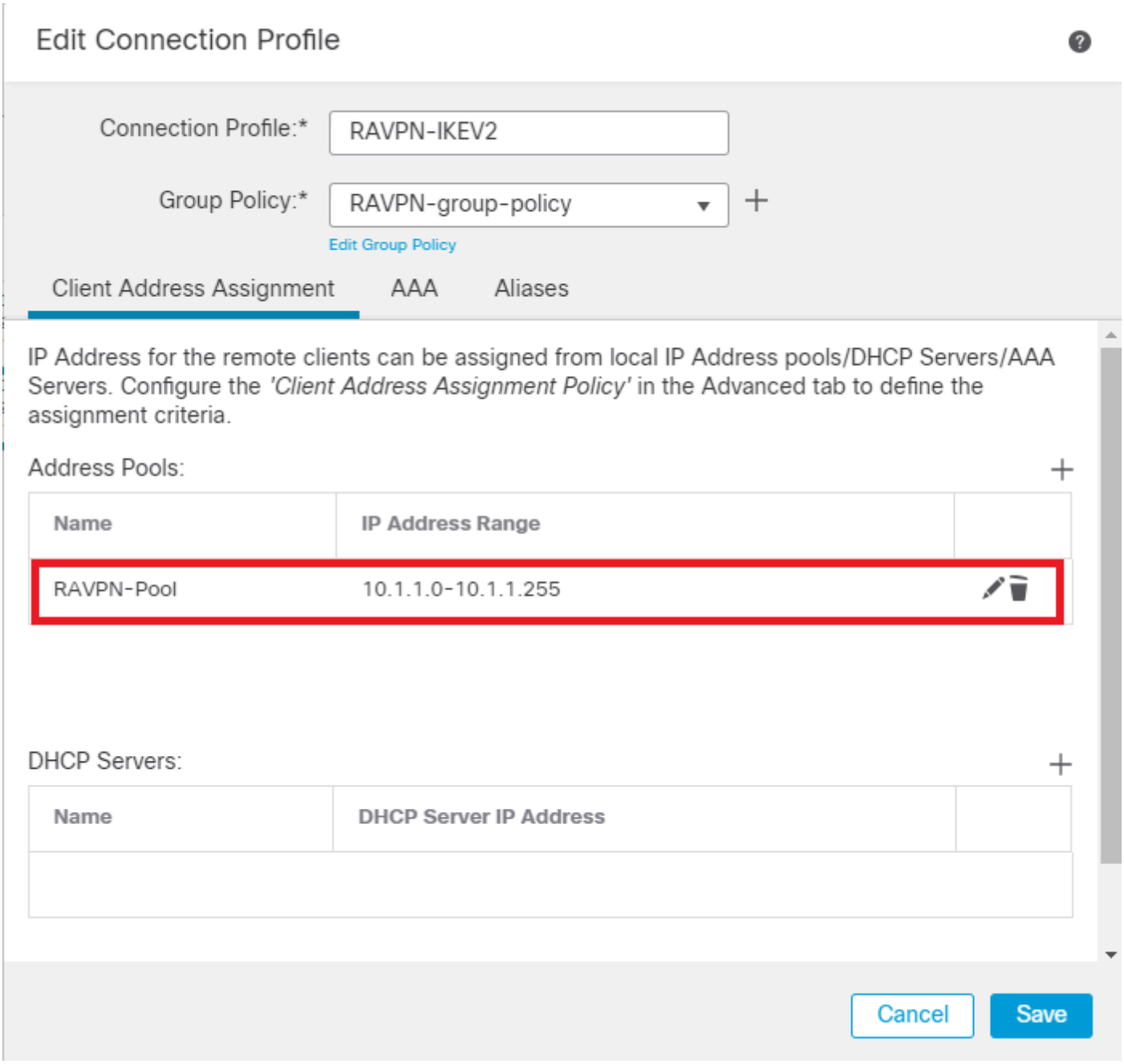
FMC - Protocolos VPN

4. Em AnyConnect > Profile , escolha o perfil XML ClientProfile no menu suspenso e clique em Saveconforme mostrado na imagem.



FMC - Perfil do Anyconnect

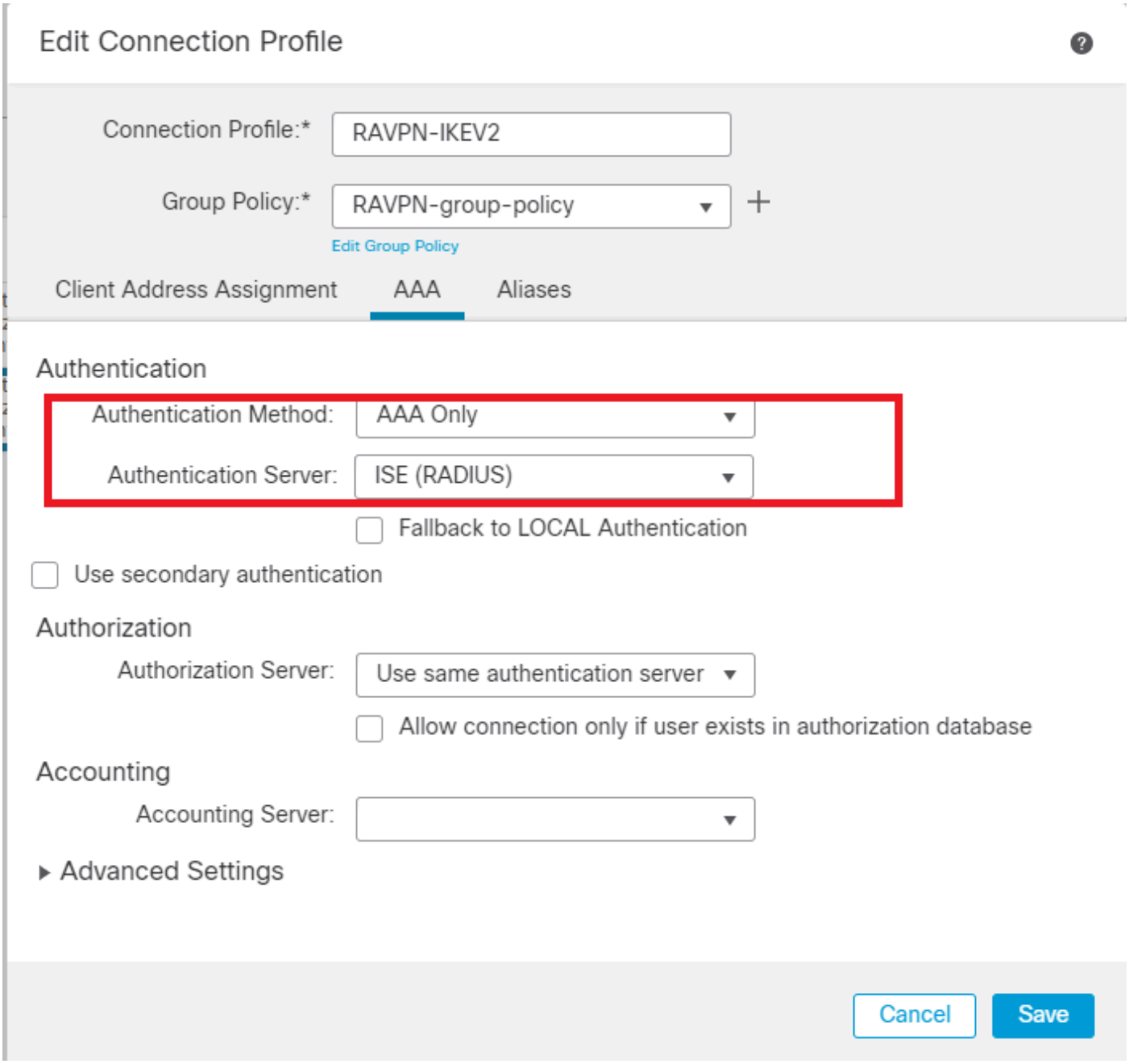
5. Adicione o Pool RAVPN-Pool de Endereços clicando em + as shown in the image.



FMC - Atribuição de endereço de cliente

6. Navegue até AAA > Authentication Method e escolha AAA Only.

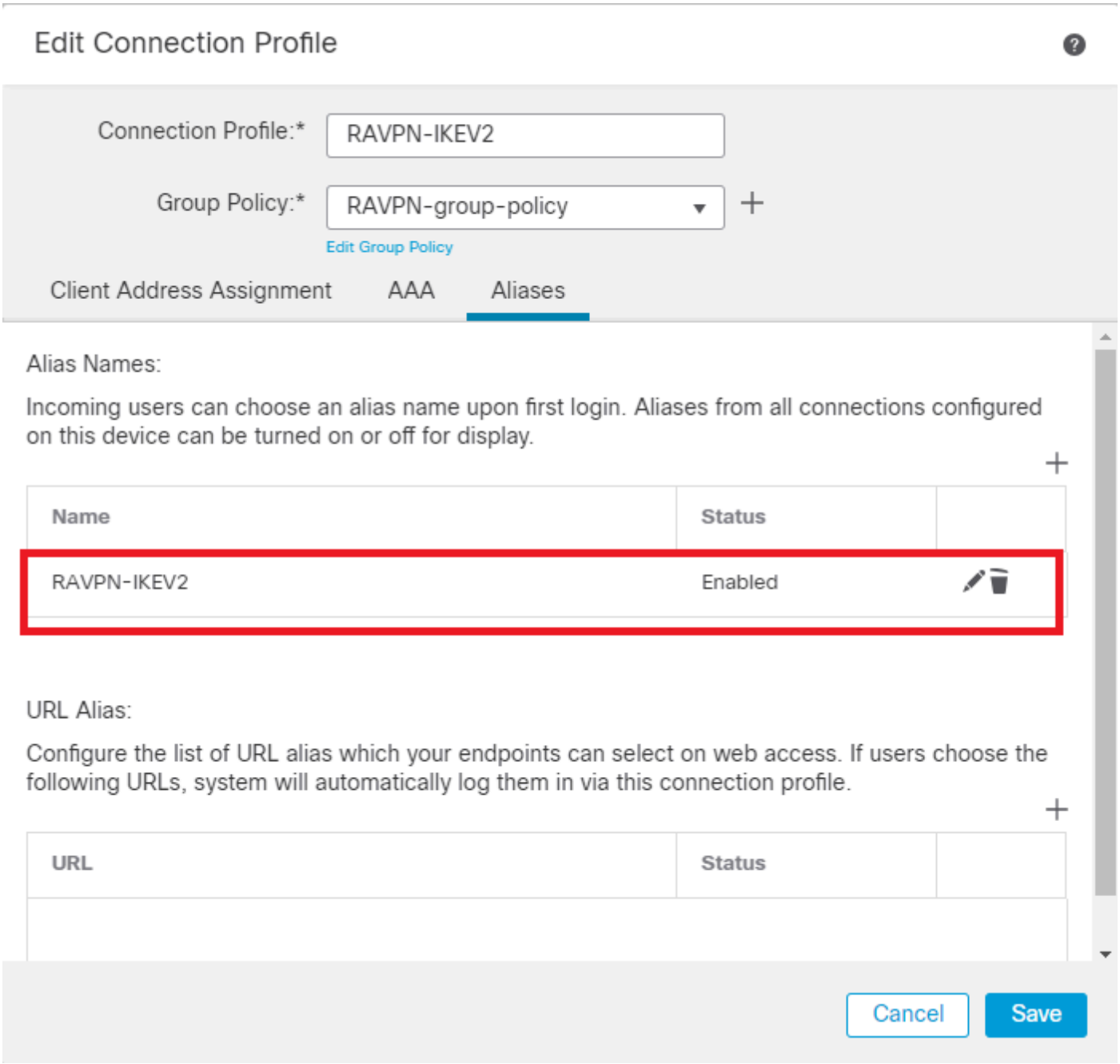
7. Escolha Authentication Server como ISE (RADIUS).



FMC - Autenticação AAA

8. Navegue até Aliases , insira um Nome de Alias RAVPN-IKEV2 , que é usado como um grupo de usuários no ClientProfile.xml .

9. Clique em Save.

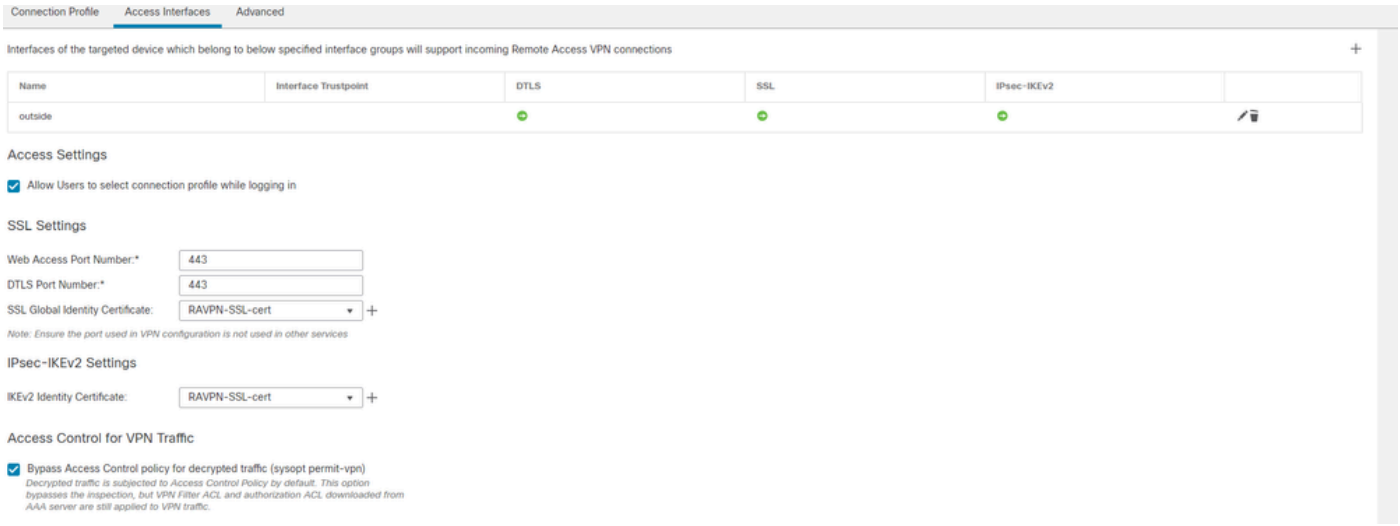


FMC - Alcunhas

10. Navegue até Access Interfaces e escolha a interface onde RAVPN IKEv2 deve ser habilitado.

11. Escolha o certificado de identidade para SSL e IKEv2.

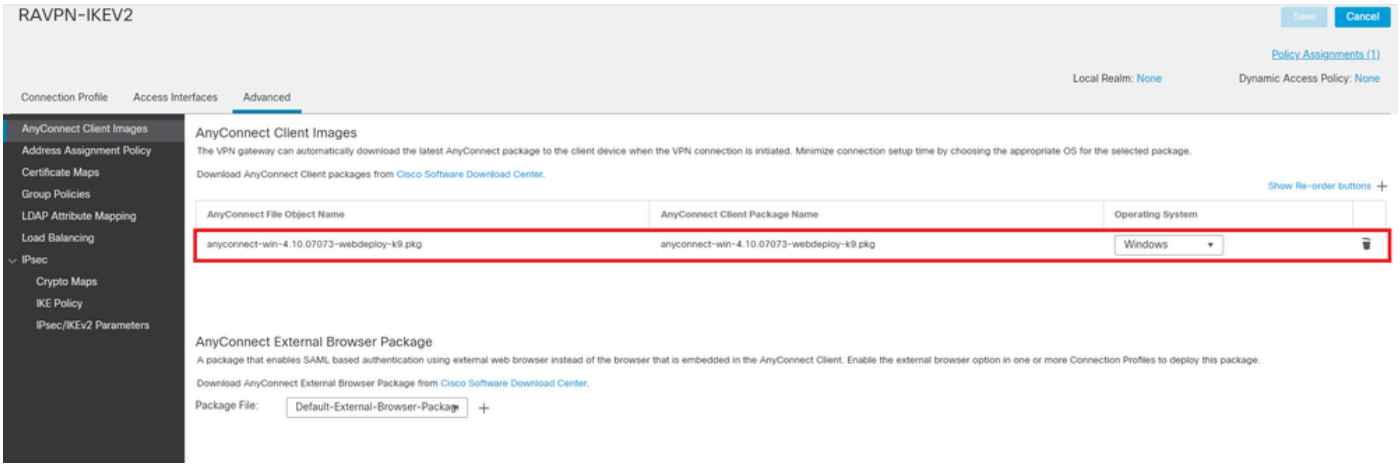
12. Clique em Save.



FMC - Interfaces de acesso

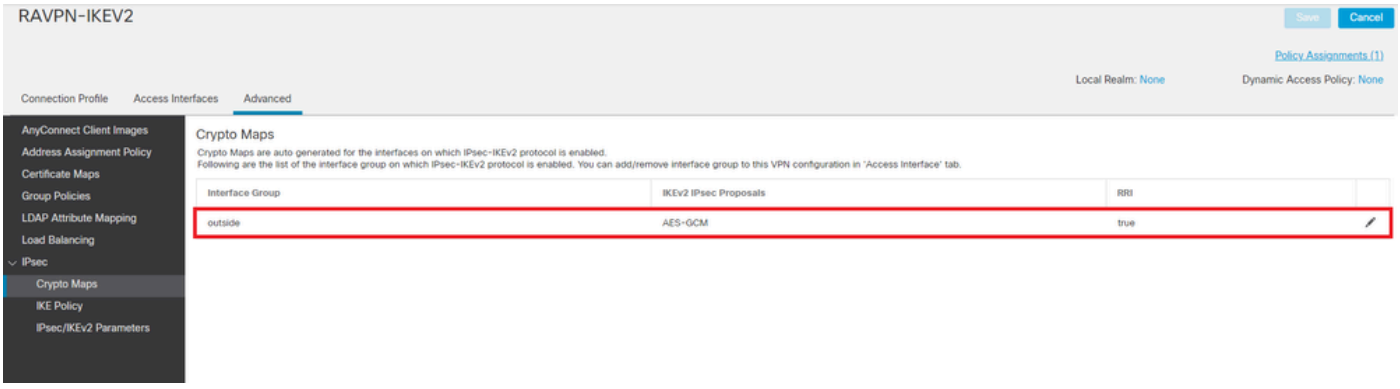
13. Navegue até Advanced .

14. Adicione as imagens do Anyconnect Client clicando em +.



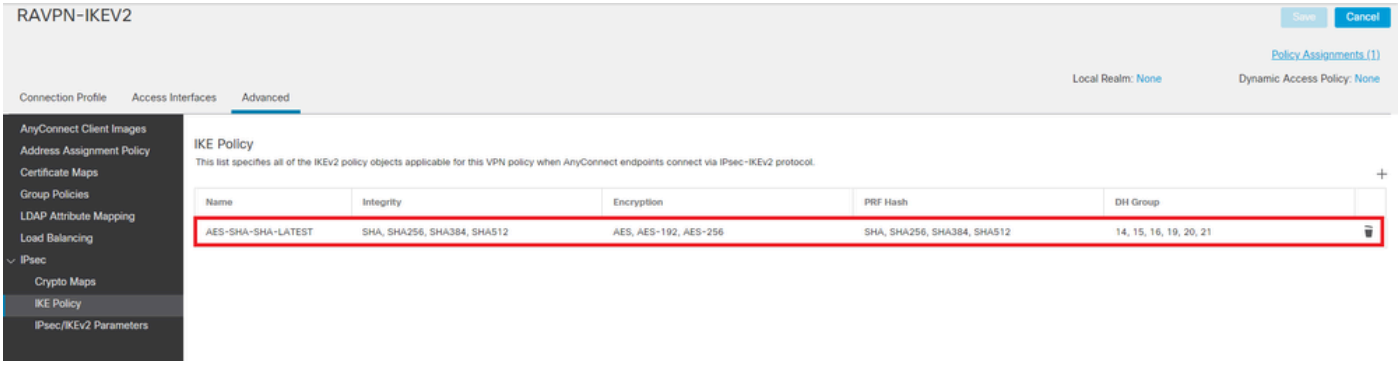
FMC - Pacote do cliente Anyconnect

15. EmIPsec, adicione oCrypto Maps como mostrado na imagem.



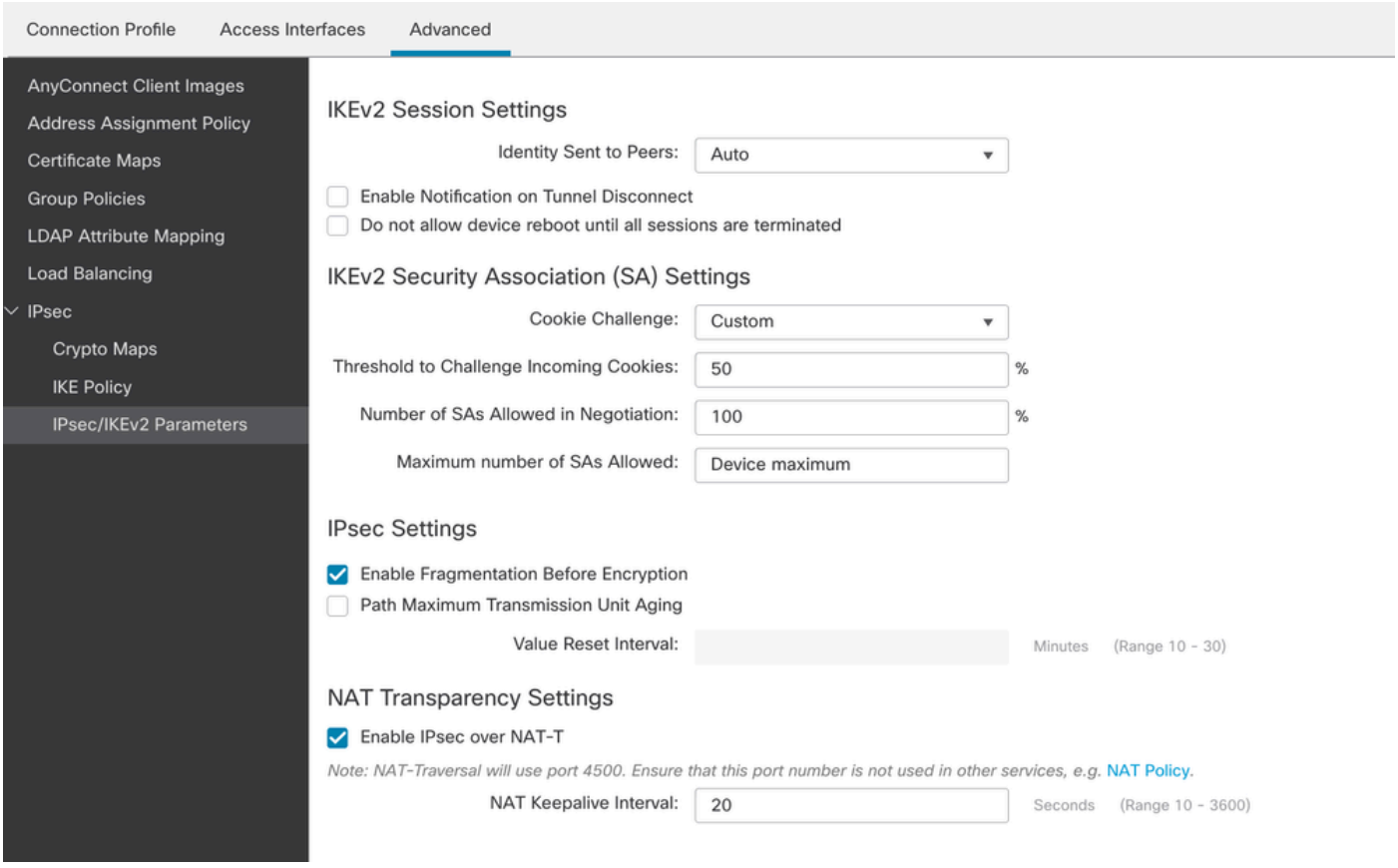
FMC - Mapas de criptografia

16. Em IPsec , adicione o IKE Policy clicando em +.



FMC - Política IKE

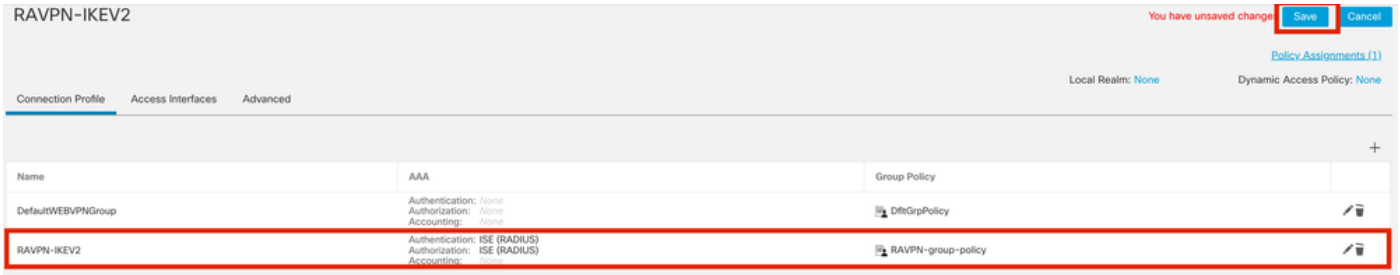
17. Em IPsec , adicione o IPsec/IKEv2 Parameters .



FMC - Parâmetros IPsec/IKEv2

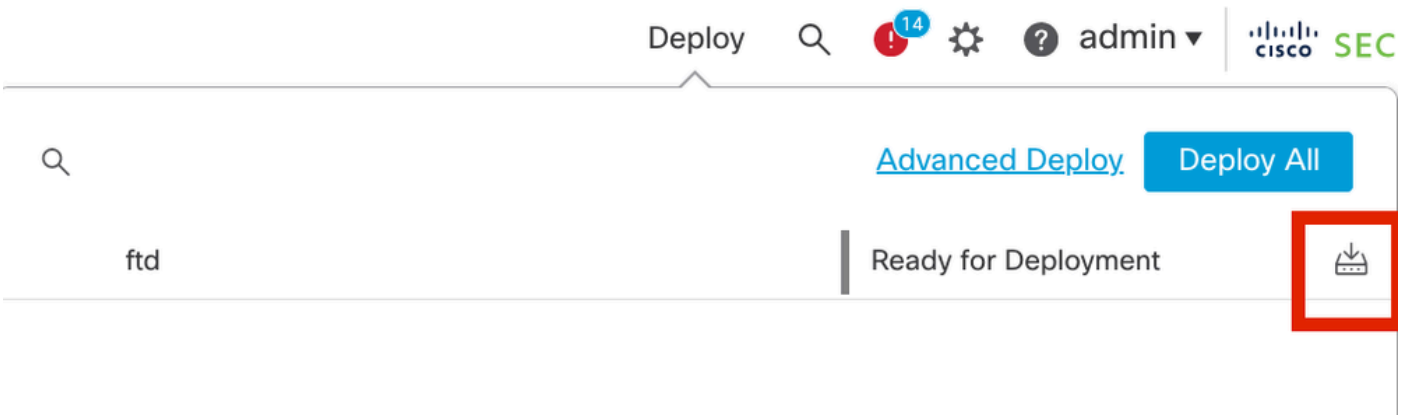
18. Em Connection Profile, é criado um novo perfilRAVPN-IKEV2.

19. SaveClickas mostrado na imagem.



FMC - Perfil de conexão RAVPN-IKEV2

20. Implante a configuração.



FMC - Implantação do FTD

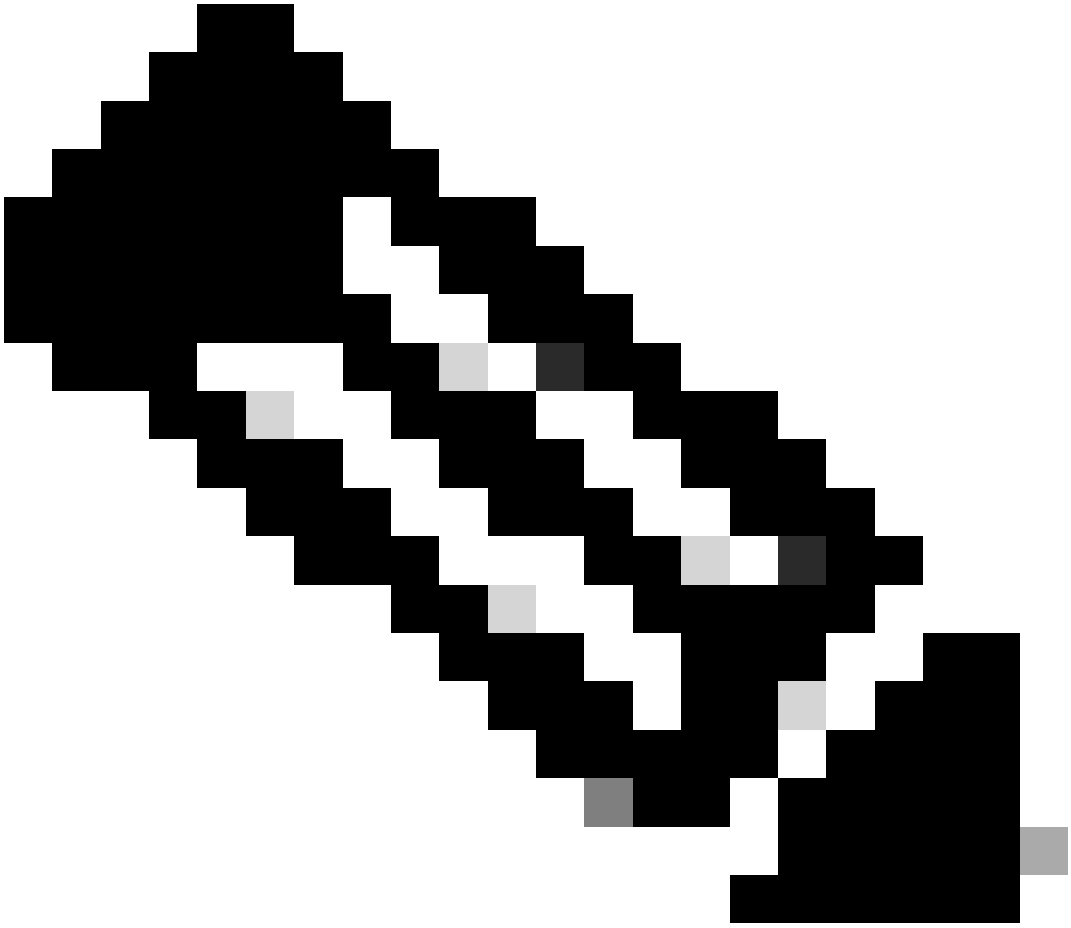
7. Configuração do perfil do Anyconnect

Perfil no PC, salvo em C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .

<#root>

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectProfile xmlns="http://schemas[dot]xmlsoap<dot>org/encoding/" xmlns:xsi="http://www[dot]w3

```
<HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserG
</HostEntry> </ServerList> </AnyConnectProfile>
```



Observação: é recomendável desativar o cliente SSL como protocolo de tunelamento na política de grupo quando o perfil do cliente for baixado para o PC de todos os usuários. Isso garante que os usuários possam se conectar exclusivamente usando o protocolo de tunelamento IKEv2/IPsec.

Verificar

Você pode usar esta seção para confirmar se sua configuração funciona corretamente.

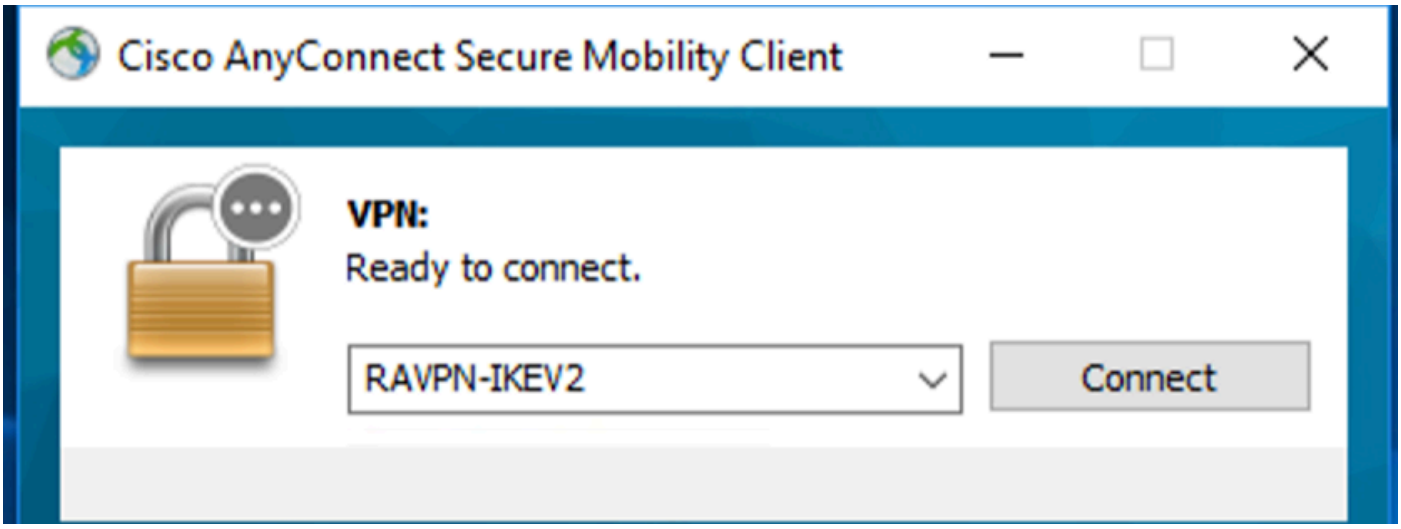
1. Para a primeira conexão, use o FQDN/IP para estabelecer uma conexão SSL do PC do usuário através do Anyconnect.
2. Se o protocolo SSL estiver desativado e a etapa anterior não puder ser executada, certifique-se de que o perfil do cliente ClientProfile.xml esteja presente no PC no caminho C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .
3. Informe o nome de usuário e a senha para a autenticação quando solicitado.

4. Após a autenticação bem-sucedida, o perfil do cliente é baixado no PC do usuário.

5. Desconecte do Anyconnect.

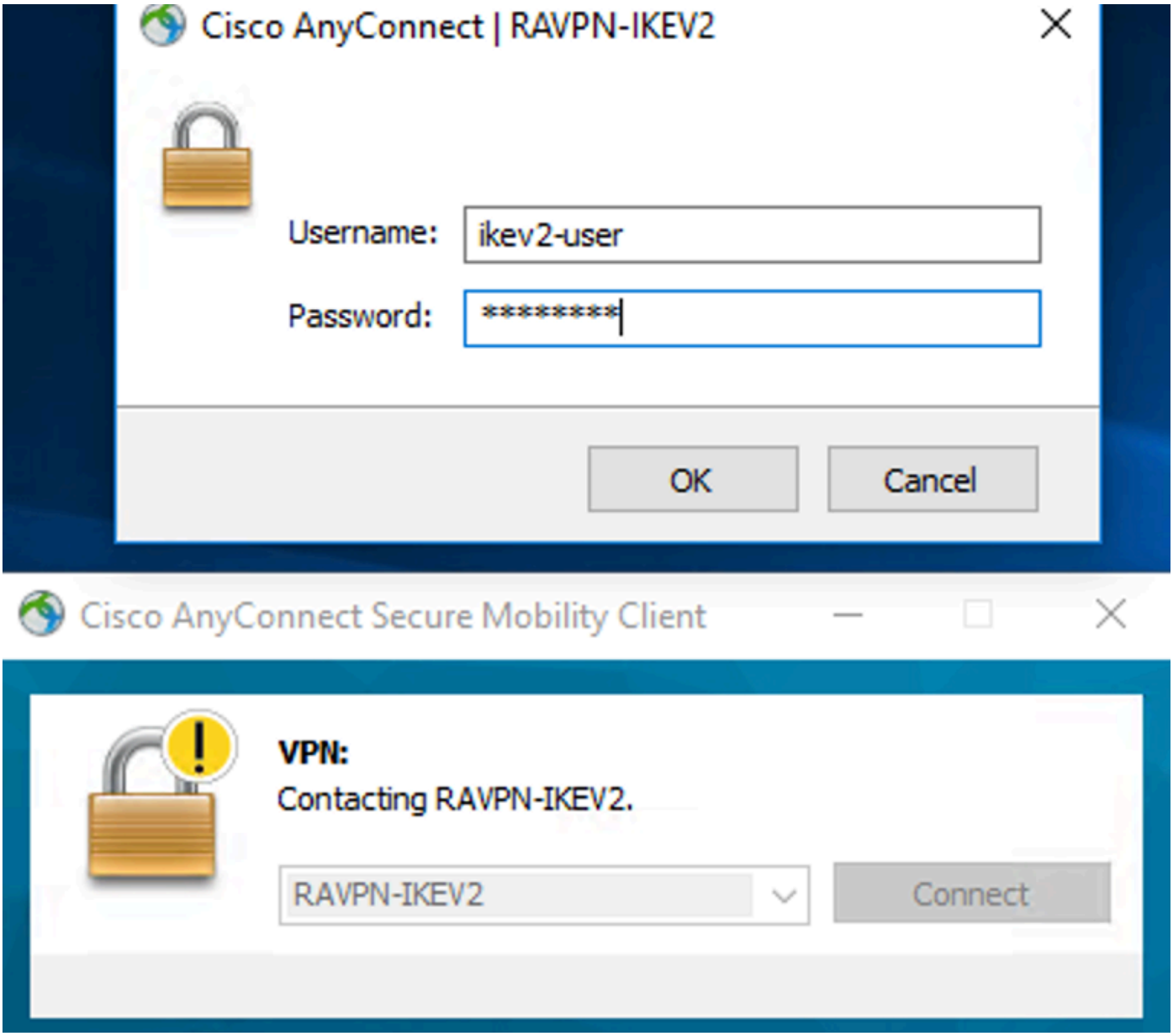
6. Depois que o Perfil for baixado, use a lista suspensa para escolher o nome de host mencionado no perfil do cliente **RAVPN-IKEV2** para se conectar ao Anyconnect usando IKEv2/IPsec.

7. Clique em Connect.



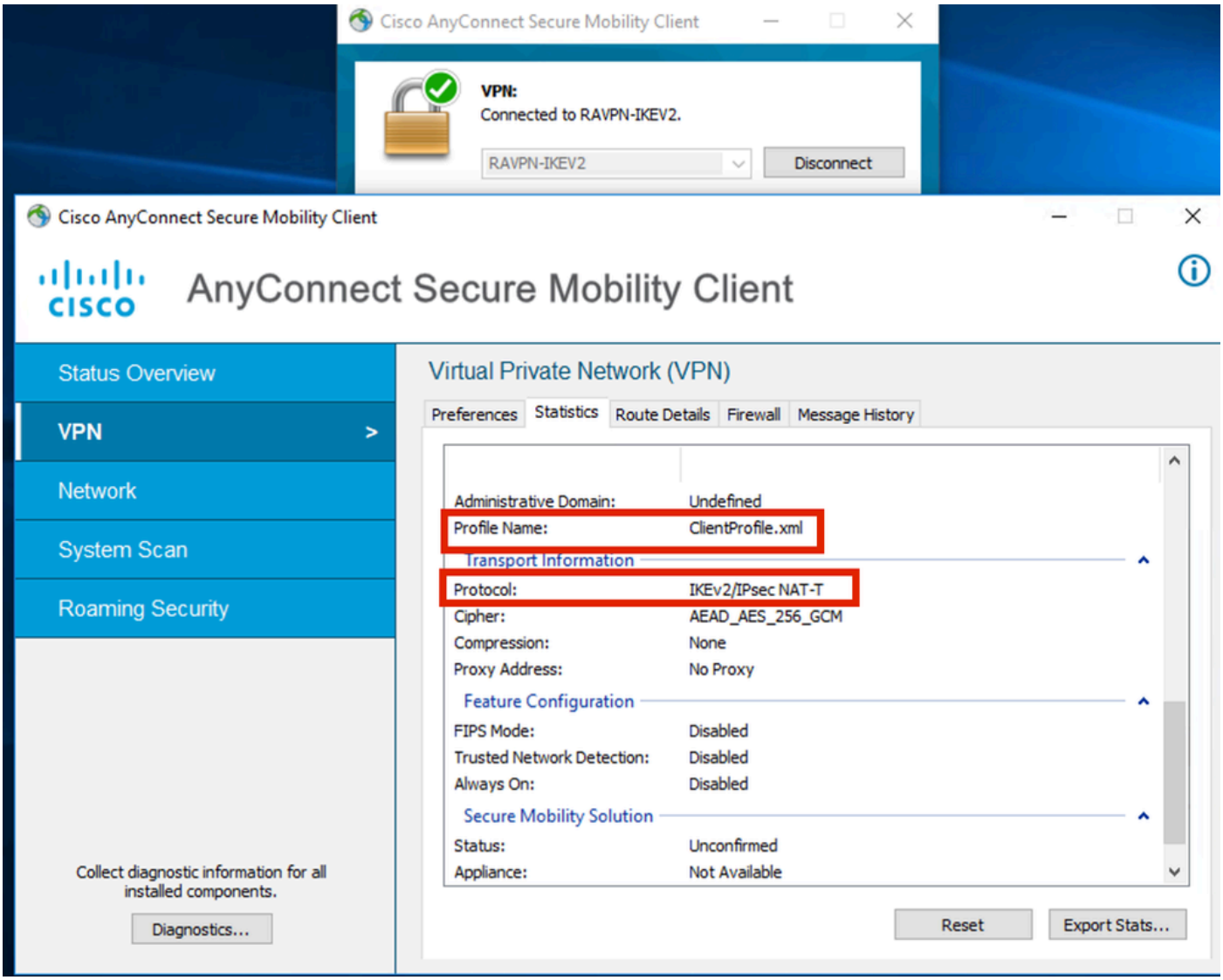
Menu suspenso do Anyconnect

8. Insira o nome de usuário e a senha para a autenticação criada no servidor ISE.



Conexão do Anyconnect

9. Verifique se o Perfil e o Protocolo (IKEv2/IPsec) usados foram conectados.



Anyconnect conectado

Saídas CLI de FTD:

<#root>

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect

Username : ikev2-user Index : 9
Assigned IP : 10.1.1.1 Public IP : 10.106.55.22
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES-GCM-256 AnyConnect-Parent: (1)none

```
Hashing      : IKEv2: (1)SHA512 IPsecOverNatT: (1)none AnyConnect-Parent: (1)none
Bytes Tx     : 450                          Bytes Rx     : 656
Pkts Tx      : 6                            Pkts Rx      : 8
Pkts Tx Drop : 0                            Pkts Rx Drop : 0
Group Policy : RAVPN-group-policy           Tunnel Group : RAVPN-IKEV2
Login Time   : 07:14:08 UTC Thu Jan 4 2024
Duration     : 0h:00m:08s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                           VLAN         : none
Audt Sess ID : 0ac5e205000090006596618c
Security Grp : none                          Tunnel Zone  : 0

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID    : 9.1
Public IP    : 10.106.55.22
Encryption.  : none.                         Hashing     : none

Auth Mode    : userPassword
Idle Time out: 30 Minutes                    Idle TO Left : 29 Minutes
Client OS    : win
Client OS Ver: 10.0.15063
Client Type  : AnyConnect
Client Ver   : 4.10.07073

IKEv2:
Tunnel ID : 9.2
UDP Src Port : 65220                          UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption   : AES256                          Hashing      : SHA512
Rekey Int (T): 86400 Seconds                   Rekey Left(T): 86391 Seconds
PRF : SHA512                                   D/H Group    : 19
Filter Name  :
Client OS    : Windows Client                  Type         : AnyConnect

IPsecOverNatT:
Tunnel ID    : 9.3
Local Addr   : 0.0.0.0/0.0.0.0/0/0
Remote Addr  : 10.1.1.1/255.255.255.255/0/0
Encryption   : AES-GCM-256                     Hashing       : none
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds                   Rekey Left(T) : 28791 Seconds
Idle Time Out: 30 Minutes                      Idle TO Left  : 29 Minutes
Bytes Tx     : 450 Bytes                       Rx            : 656
Pkts Tx      : 6                               Pkts Rx       : 8
```

```
firepower# show crypto ikev2 sa
```

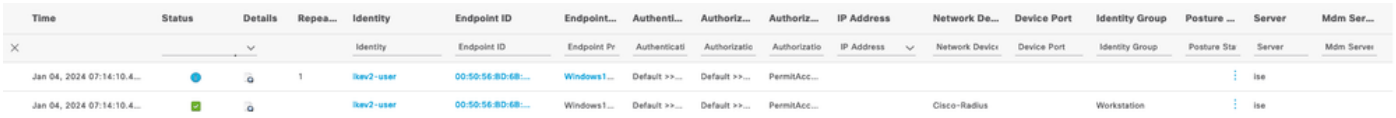
```
IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                          Remote                                          fvrf/ivrf
16530741  10.197.167.5/4500              10.106.55.22/65220
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/17 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.1.1.1/0 - 10.1.1.1/65535
ESP spi in/out: 0x6f7efd61/0xded2cbc8
```

```
firepower# show crypto ipsec sa
```

```
interface: Outside
    Crypto map tag: CSM_Outside_map_dynamic, seq num: 30000, local addr: 10.197.167.5

      Protected vrf:
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
      current_peer: 10.106.55.22, username: ikev2-user
      dynamic allocated peer ip: 10.1.1.1
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
      #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 10.197.167.5/4500, remote crypto endpt.: 10.106.55.22/65220
      path mtu 1468, ipsec overhead 62(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: DED2CBC8
      current inbound spi : 6F7EFD61

  inbound esp sas:
     spi: 0x6F7EFD61 (1870593377)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
     slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
     sa timing: remaining key lifetime (sec): 28723
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
```

```
    0x00000000 0x000001FF

  outbound esp sas:
    spi: 0xDED2CBC8 (3738356680)
    SA State: active
    transform: esp-aes-gcm-256 esp-null-hmac no compression
    in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
    slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
    sa timing: remaining key lifetime (sec): 28723
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
    0x00000000 0x00000001
```

Logs ISE:



ISE - Registros ao vivo

Troubleshooting

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

```
debug radius all
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

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.