

Configurar o Anyconnect VPN para FTD via IKEv2 com ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[1. Importar o Certificado SSL](#)

[2. Configurar o Servidor RADIUS](#)

[2.1. Gestão do FTD no CVP](#)

[2.2. Gestão do DTF no ISE](#)

[3. Criar um pool de endereços para usuários de VPN no FMC](#)

[4. Carregar imagens do AnyConnect](#)

[5. Criar Perfil XML](#)

[5.1. Sobre o Editor de perfis](#)

[5.2.No CVP](#)

[6. Configurar Acesso Remoto](#)

[7. Configuração do perfil do Anyconnect](#)

[Verificar](#)

[Troubleshooting](#)

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.

Add Cert Enrollment



Name*

RAVPN-SSL-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIG1jCCBL6gAwIBAgIQQAFu+
wogXPrr4Y9x1zq7eDANBgkqhki
G9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMB
AGA1UEChMJSWRlbiRydXN0MS
cwJQYDVQQDEw5JZGVu
VHJ1c3QgQ29tbWV5Y2lhbCBSb
290IENBIDEwHhcNMTkxMjE1
Y1NjE1WhcNMjE1
MiEvMTY1NiE1WiBvMOswCOYD
```

Certificado FMC - CA

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

Add Cert Enrollment



Name*

RAVPN-SSL-cert

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN):

ftd.cisco.com

Organization Unit (OU):

TAC

Organization (O):

cisco

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Cancel

Save

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.

Add Cert Enrollment



Name*
RAVPN-SSL-cert

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
RSA-key

Key Size:
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Cancel **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 Add como mostrado na imagem.

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name: RAVPN-SSL-cert
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

FMC - Inscrição de Certificado no FTD

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

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 cisco SECURE

Name	Domain	Enrollment Type	Status
ftd			
Root-CA	Global	Manual (CA Only)	CA ID
RAVPN-SSL-cert	Global	Manual (CA & ID)	CA ID Identity certificate import required

FMC - Certificado CA registrado

Warning

This operation will generate Certificate Signing Request do you want to continue?

No

Yes

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.

Import Identity Certificate



Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwnJEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQGA1UEAwwNRIRELmNpc2NvLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPLLwTQ6BkGjER2FfyofT+RMcCT5FQTrrMnFYok7drSKmdaKlycKM8Ljn+2m8BeVcfHsCpUybxn/ZrlsDMxSHo4E0oJEUgutsk++p1jIWcdVROn0vtahe+BRxC3qjo1FsLcp5zQru5goloRQRoiFwn5syAqOztgl0aUrFSSWF/Kdh3GeDE1XHPP1zzl4
```

Step 2

Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)

FMC - Certificado de identidade de importação

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

Name	Domain	Enrollment Type	Status
RAVPN-SSL-cert	Global	Manual (CA & ID)	CA ID

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 +.

Name:*

ISE

Description:

Group Accounting Mode:

Single ▼

Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname	
10.197.224.173	 

Cancel

Save

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.

Edit RADIUS Server



IP Address/Hostname:*

10.197.224.173

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

Confirm Key:*

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

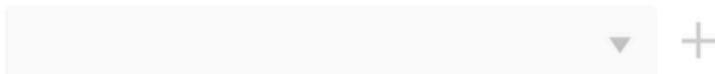
Connect using:

Routing Specific Interface 

outside



Redirect ACL:



Cancel

Save

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

Name	Value
ISE	1 Server

FMC - Grupo de servidores RADIUS

2.2. Gestão do DTF no ISE

1. Navegue até Network Devices e clique em Add.

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

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

4. Clique em Save .

Network Devices List > Cisco-Radius

Network Devices

Name: Cisco-Radius

Description:

IP Address: * IP: 10.197.167.5 / 25

Device Profile: Cisco-Radius

Model Name:

Software Version:

Network Device Group

Device Type: All Device Types [Set To Default](#)

IPSEC: No [Set To Default](#)

Location: All Locations [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: [Show](#)

Use Second Shared Secret [ⓘ](#)

networkDevices.secondSharedSecret: [Show](#)

CoA Port: 1700 [Set To Default](#)

ISE - Dispositivos de rede

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

6. Crie um Nome de Usuário e Senha de Logon conforme necessário.

Overview **Identities** Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports More ▾

Endpoints

Network Access Users

Identity Source Sequences

Network Access Users List > ikev2-user

Network Access User

* Username ikev2-user

Status Enabled ▾

Email

Passwords

Password Type: Internal Users ▾

Password Re-Enter Password

* Login Password Generate Password ⓘ

Enable Password Generate Password ⓘ

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 PermitAccess como mostrado na imagem.

Default

All_User_ID_Stores ⓘ ▾

> Options 4 ⚙

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess × ▾ +

Select from list ▾ + 4 ⚙

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**.

Edit IPv4 Pool



Name*

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

Save

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.

Edit AnyConnect File



Name:*

File Name:*

File Type:*



Description:

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.

Server List Entry [X]

Server | Load Balancing Servers | SCEP | Mobile | Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address / User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Editor de perfis - Lista de servidores

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

AnyConnect Profile Editor - VPN [-] [□] [X]

File Help

- VPN
- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: C:\Users\Amrutha\Documents\ClientProfile.xml

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
RAVPN-IKEV2	ftd.cisco.com	RAVPN-IKEV2	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

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** .

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Perfil de VPN do Anyconnect

6. Configurar Acesso Remoto

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

RAVPN-IKEV2

Save Cancel

Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DFGripPolicy	

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.

Add Connection Profile



Connection Profile:*

Group Policy:* 

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools: 

Name	IP Address Range	

DHCP Servers: 

Name	DHCP Server IP Address	

Cancel

Save

FMC - Política de grupo

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

Edit Group Policy



Name:*

RAVPN-group-policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

FMC - Protocolos VPN

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

Edit Group Policy



Name:*

RAVPN-group-policy

Description:

General

AnyConnect

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

AnyConnect profiles contains settings for the VPN client functionality and optional features. Firewall Threat Defense deploys the profiles during AnyConnect client connection.

Client Profile:

ClientProfile



Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from [Cisco Software Download Center](#).

Cancel

Save

FMC - Perfil do Anyconnect

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

Edit Connection Profile

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
RAVPN-Pool	10.1.1.0-10.1.1.255	

DHCP Servers: +

Name	DHCP Server IP Address	

Cancel

Save

FMC - Atribuição de endereço de cliente

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

7. Escolha Authentication Server como ISE (RADIUS).

Edit Connection Profile



Connection Profile:* RAVPN-IKEV2

Group Policy:* RAVPN-group-policy +

[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE (RADIUS)

Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server: Use same authentication server

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

▶ Advanced Settings

Cancel

Save

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.

Edit Connection Profile



Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.



Name	Status	
RAVPN-IKEV2	Enabled	

URL Alias:

Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.



URL	Status	
-----	--------	--

Cancel

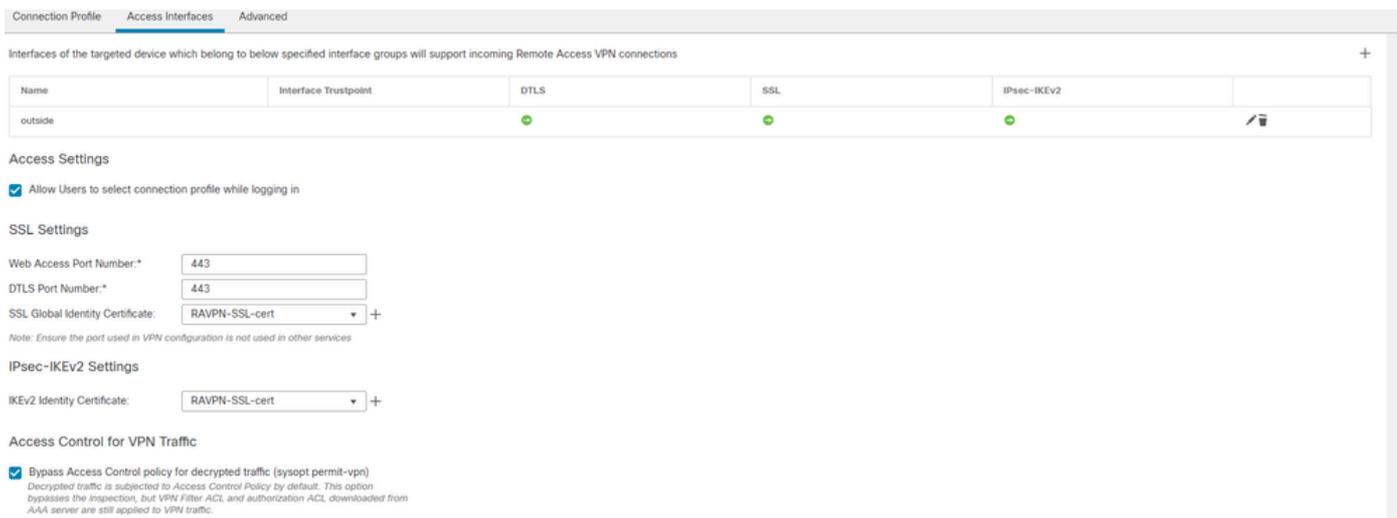
Save

FMC - Alcinhas

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.

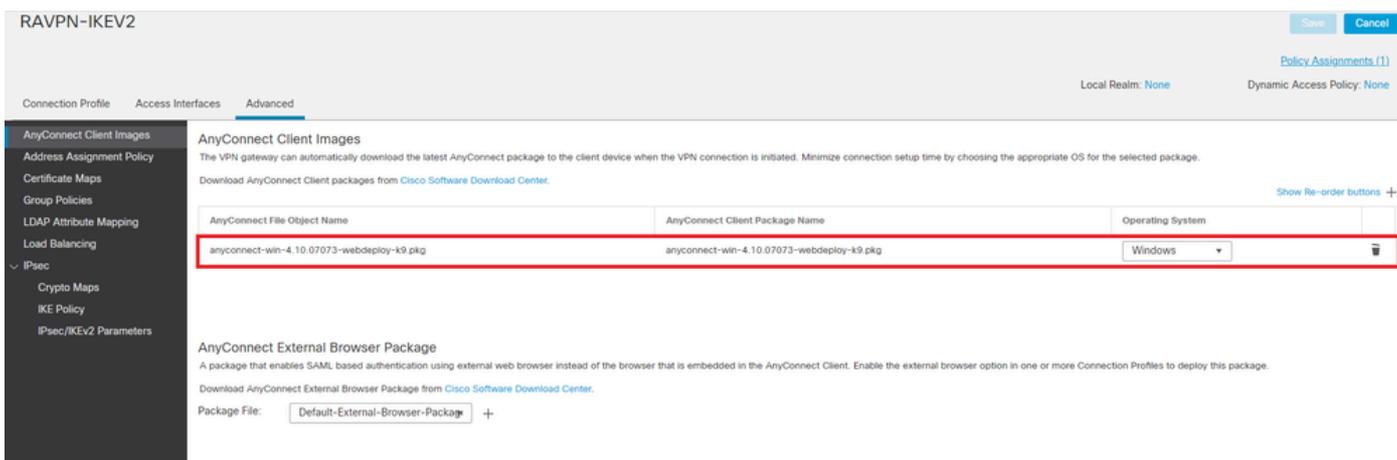
12. Clique em Save.



FMC - Interfaces de acesso

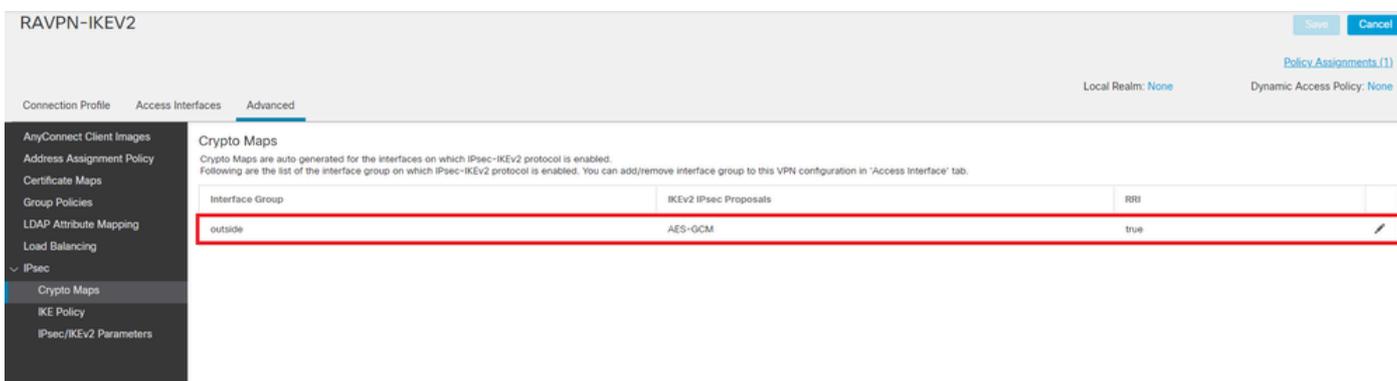
13. Navegue até Advanced .

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



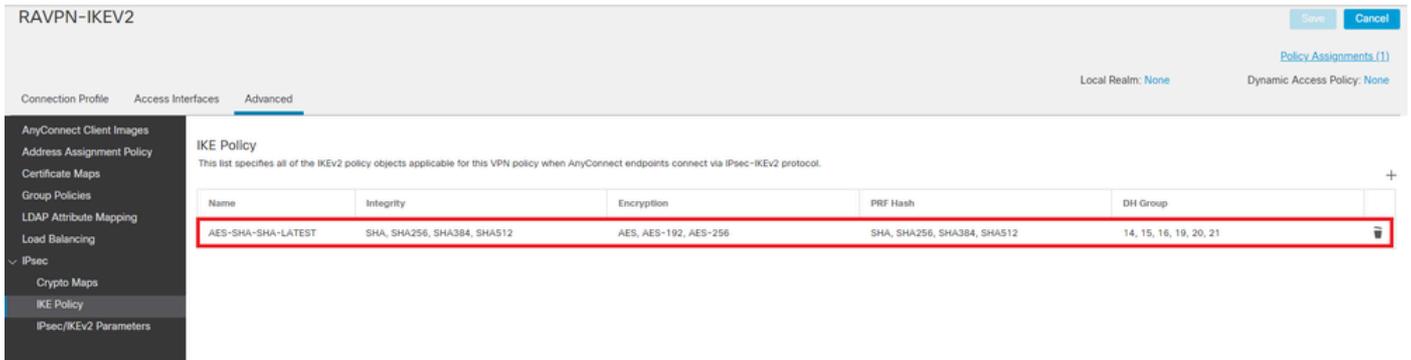
FMC - Pacote do cliente Anyconnect

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



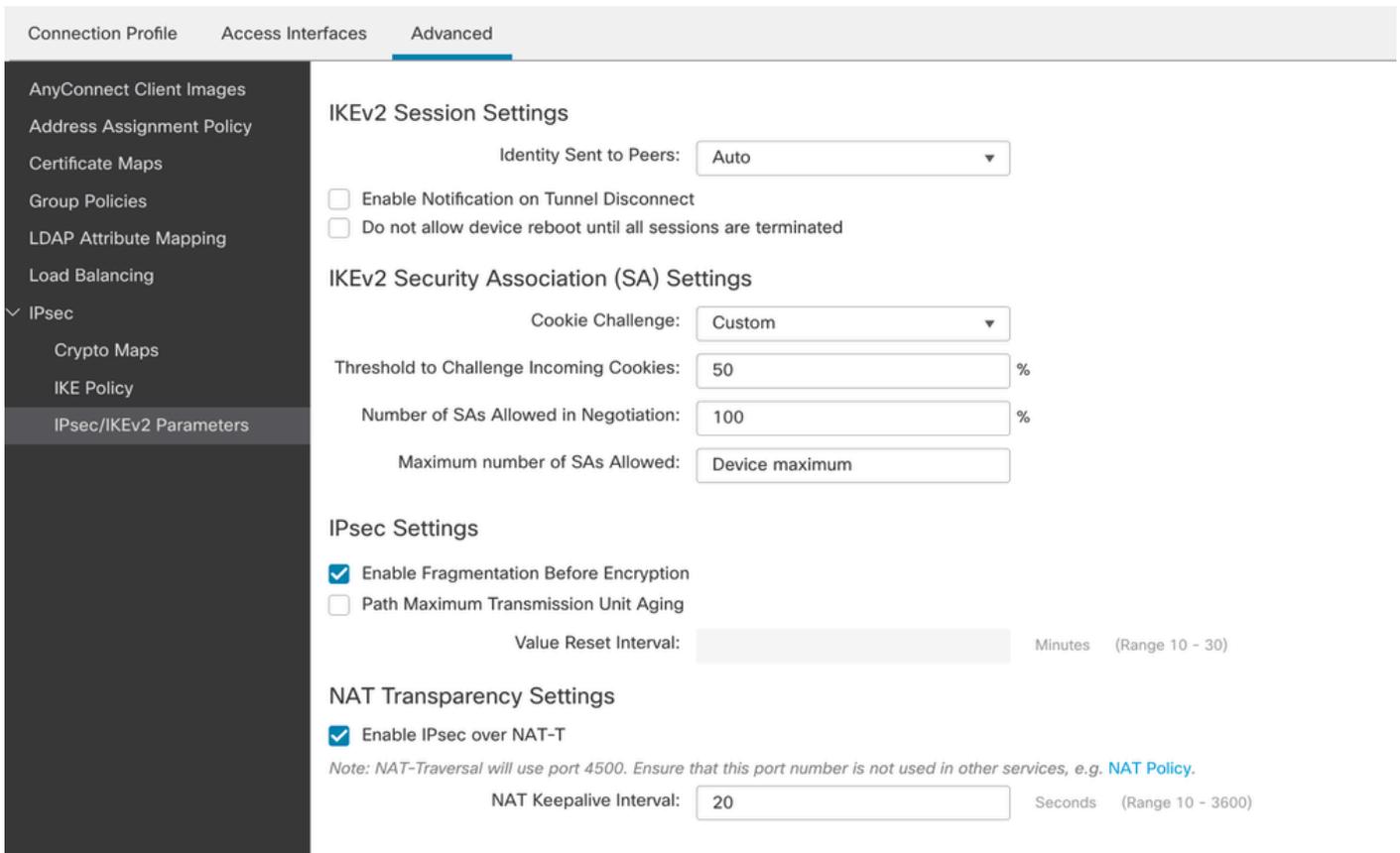
FMC - Mapas de criptografia

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



FMC - Política IKE

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



FMC - Parâmetros IPsec/IKEv2

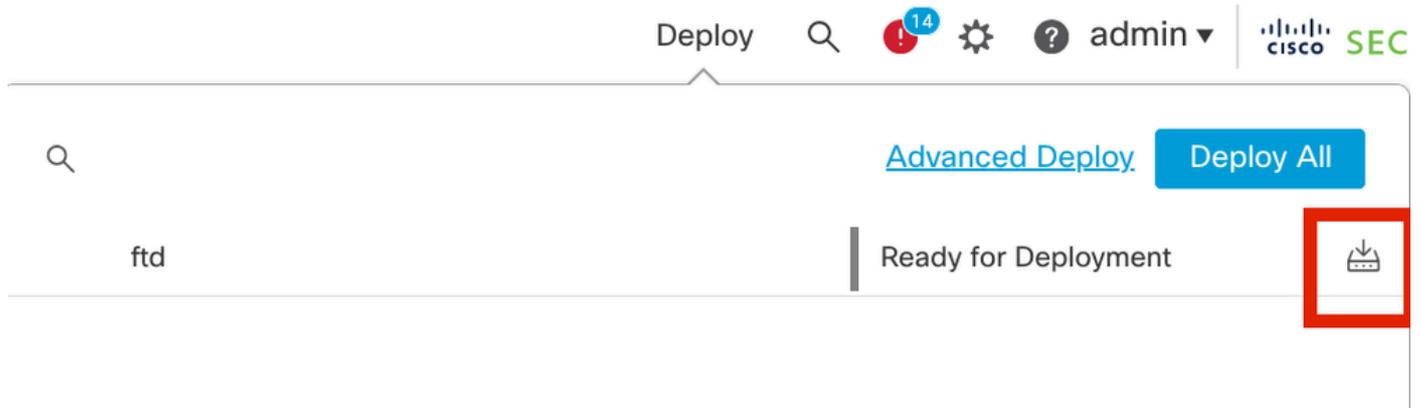
18. Em Connection Profile, é criado um novo perfilRAVPN-IKEV2.

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[dot]org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ http://schemas.xmlsoap.org/encoding/2001/XMLSchema.xsd">
  <HostEntry>
    <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>
  </HostEntry> </ServerList> </AnyConnectProfile>
```

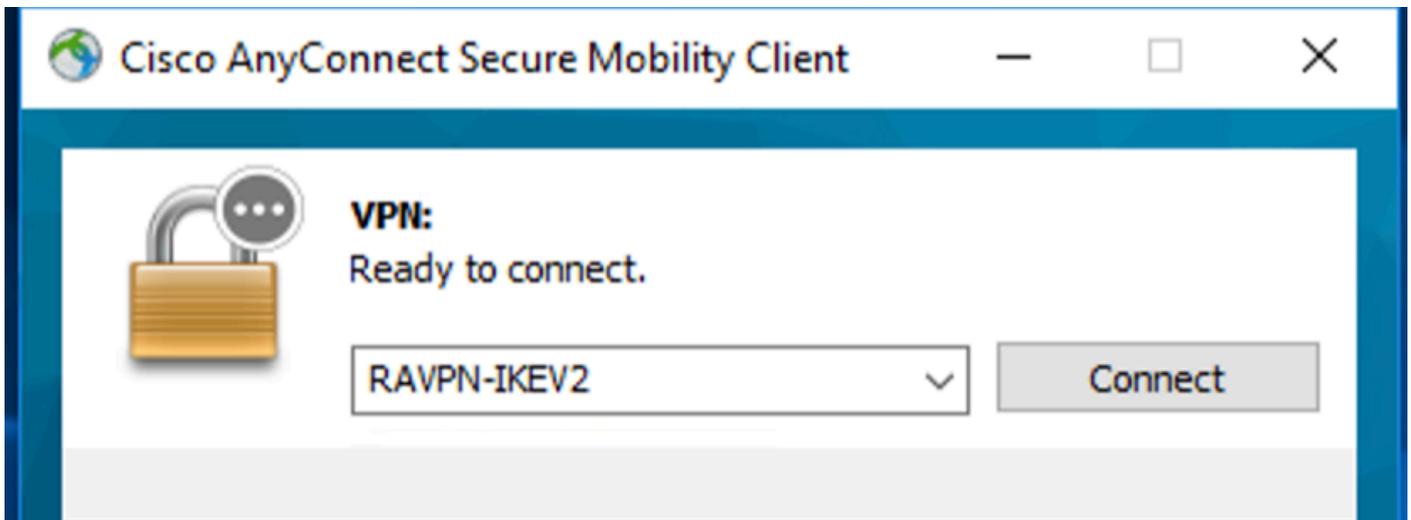
Observação: é recomendável desativar o cliente SSL como protocolo de tunelamento na política de grupo quando o perfil do cliente for baixado para o PC de todos os usuários. Isso garante que os usuários possam se conectar exclusivamente usando o protocolo de tunelamento IKEv2/IPsec.

Verificar

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

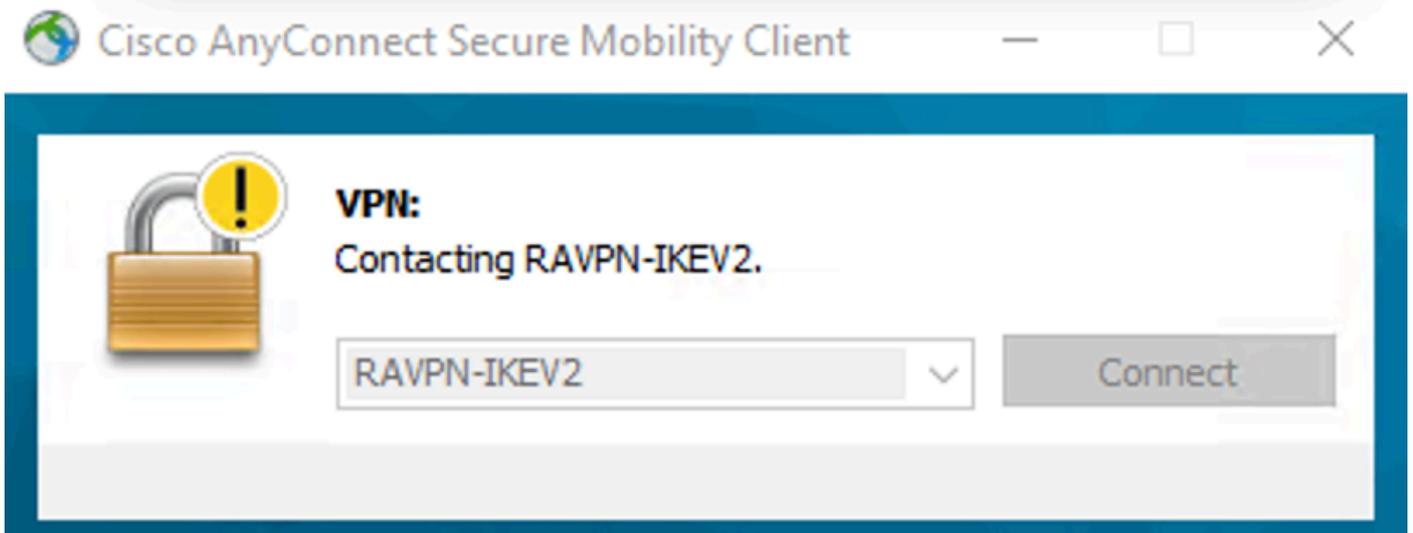
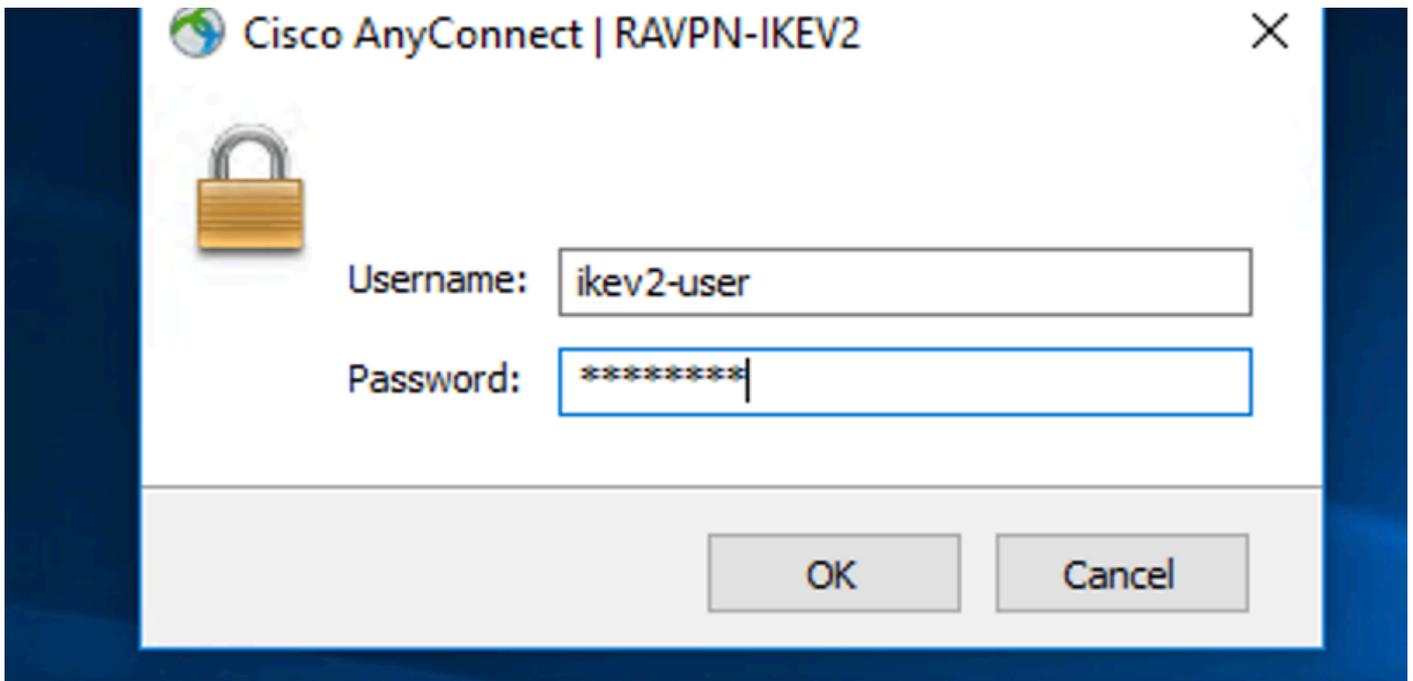
1. Para a primeira conexão, use o FQDN/IP para estabelecer uma conexão SSL do PC do usuário através do Anyconnect.
2. Se o protocolo SSL estiver desativado e a etapa anterior não puder ser executada, certifique-se de que o perfil do cliente ClientProfile.xml esteja presente no PC no caminho C:\ProgramData\Cisco\Cisco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



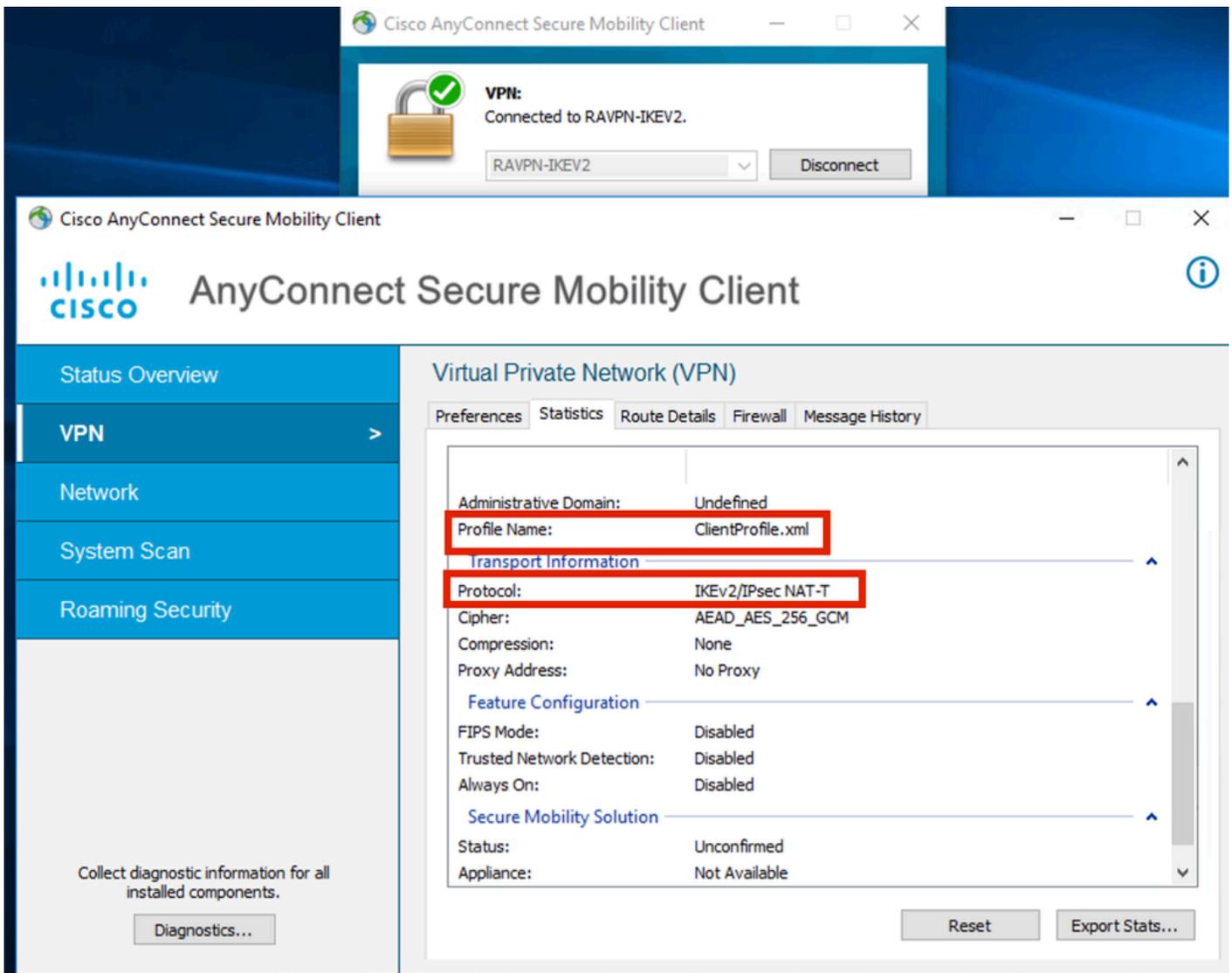
Menu suspenso do Anyconnect

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 fvr/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: 0xDEDED2CBC8 (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:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Ser...
Jan 04, 2024 07:14:10.4...			1	ikev2-user	00-50-56-BD-6B...	Windows1...	Default >>...	Default >>...	PermitAcc...							ise
Jan 04, 2024 07:14:10.4...				ikev2-user	00-50-56-BD-6B...	Windows1...	Default >>...	Default >>...	PermitAcc...		Cisco-Radius		Workstation			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.