

# Configuración de VPN Anyconnect en FTD mediante IKEv2 con ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[1. Importe el certificado SSL](#)

[2. Configure el servidor RADIUS](#)

[2.1. Gestión del FTD en el CSP](#)

[2.2. Gestión del FTD en ISE](#)

[3. Crear un conjunto de direcciones para usuarios de VPN en FMC](#)

[4. Cargar imágenes de AnyConnect](#)

[5. Crear perfil XML](#)

[5.1. En el Editor de perfiles](#)

[5.2. En el CSP](#)

[6. Configuración del acceso remoto](#)

[7. Configuración del perfil de Anyconnect](#)

[Verificación](#)

[Troubleshoot](#)

---

## Introducción

Este documento describe la configuración básica de VPN de acceso remoto con autenticación IKEv2 e ISE en FTD administrado por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN básica, TLS e Intercambio de claves de Internet versión 2 (IKEv2)
- Autenticación, autorización y contabilidad básicas (AAA) y RADIUS
- Experiencia con Firepower Management Center (FMC)

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Threat Defense (FTD) 7.2.0
- Cisco FMC 7.2.0
- AnyConnect 4.10.07073
- Cisco ISE 3.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

IKEv2 y Secure Sockets Layer (SSL) son protocolos que se utilizan para establecer conexiones seguras, especialmente en el contexto de las VPN. IKEv2 proporciona sólidos métodos de cifrado y autenticación, lo que ofrece un alto nivel de seguridad para las conexiones VPN.

Este documento proporciona un ejemplo de configuración para FTD versión 7.2.0 y posteriores, que permite VPN de acceso remoto para utilizar Transport Layer Security (TLS) e IKEv2. Como cliente, se puede utilizar Cisco AnyConnect, que es compatible con varias plataformas.

## Configurar

### 1. Importe el certificado SSL

Los certificados son esenciales cuando se configura AnyConnect.

La inscripción manual de certificados tiene limitaciones:

1. En FTD, se necesita un certificado de autoridad certificadora (CA) antes de generar una solicitud de firma de certificado (CSR).
2. Si la CSR se genera externamente, se utiliza un método diferente de PKCS12.

Hay varios métodos para obtener un certificado en un dispositivo FTD, pero el más seguro y fácil es crear una CSR y conseguir que esté firmada por una CA. A continuación se explica cómo hacerlo:

1. **Desplácese hasta** Objects > Object Management > PKI > Cert Enrollment y haga clic en Add Cert Enrollment.
2. Introduzca el nombre del punto de confianza RAVPN-SSL-cert.
3. En la CA Information ficha, elija Tipo de inscripción como Manual y pegue el certificado de CA como se muestra en la imagen.

## 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
VHJ1c3QgQ29tbWVyY2lhbCBSb
290IENBIDEwHhcNMTkxMjE1
Y1NjE1WhcNMjE1
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - Certificado de CA

4. En Certificate Parameters, introduzca el nombre del asunto. Por ejemplo:

## 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 - Parámetros de certificado

5. En la Key ficha, seleccione el tipo de clave y proporcione un nombre y un tamaño de bit. Para RSA, 2048 bits es el mínimo.

6. Haga clic en 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 - Clave de certificado

7. Acceda a Devices > Certificates > Add > New Certificate.

8. Seleccione Device. En Cert Enrollment, elija el punto de confianza creado y haga clic Add como se muestra en la imagen.

## 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 - Inscripción de certificados en FTD

9. Haga clic en ID y se mostrará un mensaje para generar CSR. Seleccione 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 inscrito

# Warning

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

No

Yes

*FMC - Generar CSR*

10. Se genera una CSR que se puede compartir con la CA para obtener el certificado de identidad.

11. Después de recibir el certificado de identidad de CA en formato base64, selecciónelo del disco haciendo clic en Browse Identity Certificate y Import como se muestra en la imagen.

# 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 - Importar certificado de identidad

12. Una vez que la importación es exitosa, el punto de confianza RAVPN-SSL-cert se ve como:

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

FMC - Inscripción en Trustpoint correcta

## 2. Configure el servidor RADIUS

### 2.1. Gestión del FTD en el CSP

1. Acceda a Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. Introduzca el nombre ISE y agregue servidores RADIUS haciendo clic en +.



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 - Configuración del servidor Radius

3. Mencione la dirección IP del servidor ISE Radius junto con el secreto compartido (clave), que es el mismo que en el servidor ISE.

4. Seleccione Routing o Specific Interface a través de la cual el FTD se comunica con el servidor ISE.

5. Haga clic Save como se muestra en la imagen.

## 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

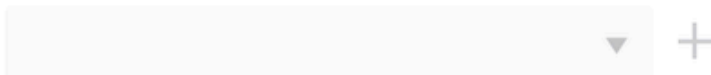
Connect using:

Routing  Specific Interface 

outside



Redirect ACL:



Cancel

Save

6. Una vez guardado, el servidor se agrega bajo el RADIUS Server Group como se muestra en la imagen.

RADIUS Server Group		<a href="#">Add RADIUS Server Group</a>	Filter
RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.			
Name	Value		
ISE	1 Server		

*FMC - Grupo de servidores RADIUS*

## 2.2. Gestión del FTD en ISE

1. Desplácese hasta Network Devices y haga clic en Add.

2. Introduzca el nombre 'Cisco-Radius' del servidor y IP Address del cliente RADIUS que es la interfaz de comunicación FTD.

3. En Radius Authentication Settings, agregue el Shared Secret.

4. Haga clic en Save .

The screenshot shows the configuration page for a Network Device named 'Cisco-Radius'. The page is divided into several sections:

- Network Devices List:** Shows the current device 'Cisco-Radius'.
- IP Address:** Set to 10.197.167.5 / 25.
- Device Profile:** Set to Cisco-Radius.
- Model Name:** (Empty)
- Software Version:** (Empty)
- 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:** (Checked)
  - RADIUS UDP Settings:**
    - Protocol: RADIUS
    - Shared Secret: (Masked) (Show)
    - Use Second Shared Secret (Info)
    - networkDevices.secondSharedSecret: (Empty) (Show)
    - CoA Port: 1700 (Set To Default)

*ISE - Dispositivos de red*

5. Para crear usuarios, navegue hasta Network Access > Identities > Network Access Users y haga clic Add en.

6. Cree un nombre de usuario y una contraseña de inicio de sesión según sea necesario.

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 - Usuarios

7. Para configurar la política básica, acceda a Policy > Policy Sets > Default > Authentication Policy > Default, seleccione All\_User\_ID\_Stores.

8. Acceda a Policy > Policy Sets > Default > Authorization Policy > Basic\_Authenticated\_Access, y seleccione PermitAccess como se muestra en la imagen.

Default

All\_User\_ID\_Stores ⓘ ▾

> Options 4 ⚙

### ISE - Política de autenticación

Basic\_Authenticated\_Access

Network\_Access\_Authentication\_Passed

PermitAccess × ▾ +

Select from list ▾ + 4 ⚙

### ISE - Política de autorización

3. Crear un conjunto de direcciones para usuarios de VPN en FMC

1. Acceda a Objects > Object Management > Address Pools > Add IPv4 Pools.
2. Introduzca el nombre RAVPN-Pool y el **rango de direcciones**, la máscara es opcional.
3. Haga clic en **Guardar**.

## 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 - Conjunto de direcciones*

#### 4. Cargar imágenes de AnyConnect

1. Acceda a Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Ingrese el nombre anyconnect-win-4.10.07073-webdeploy y haga clic Browse para elegir el archivo **Anyconnect** del disco, haga clic en Save como se muestra en la imagen.

# Edit AnyConnect File



Name:\*

File Name:\*

File Type:\*



Description:

*FMC - Imagen del cliente Anyconnect*

## 5. Crear perfil XML

### 5.1. En el Editor de perfiles

1. Descargue el Editor de perfiles de [software.cisco.com](http://software.cisco.com) y ábralo.
2. Acceda a **Server List > Add...**
3. Introduzca el nombre mostrado RAVPN-IKEV2 y FQDN junto con el **grupo de usuarios** (nombre de alias).
4. Elija el protocolo principal **IPsec**, como haga clic **Ok** como se muestra en la imagen.

**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 perfiles - Lista de servidores

5. Se agrega la lista de servidores. Guárdelo 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 perfiles - ClientProfile.xml

## 5.2. En CSP

1. Acceda a Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Ingrese un nombre ClientProfile y haga clic Browse para elegir el ClientProfile.xml archivo del disco.
3. Haga clic en **Save** .

# Edit AnyConnect File



Name:\*

ClientProfile

File Name:\*

ClientProfile.xml

Browse..

File Type:\*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Perfil VPN de Anyconnect

## 6. Configuración del acceso remoto

1. Navegue hasta Devices > VPN > Remote Accessy haga clic + para agregar un perfil de conexión como se muestra en la imagen.

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

FMC - Perfil de conexión de acceso remoto

2. Introduzca el nombre del perfil de conexión RAVPN-IKEV2 y cree una política de grupo haciendo clic + en **Group Policy** como se muestra en la imagen.



## 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. Ingrese el nombre RAVPN-group-policy , elija los Protocolos VPN SSL and IPsec-IKEv2 como se muestra en la imagen.

## 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. En AnyConnect > Profile , seleccione el perfil XML ClientProfile en el menú desplegable y haga clic Save como se muestra en la imagen.

## 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 de Anyconnect

5. Agregue el pool de direcciones RAVPN-Pool haciendo clic en + 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 - Asignación de dirección de cliente*

6. Acceda a AAA > Authentication Method y seleccione AAA Only.

7. Seleccione 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 - Autenticación AAA

8. Acceda a Aliases e introduzca un nombre de alias RAVPN-IKEV2 , que se utiliza como grupo de usuarios en ClientProfile.xml .

9. Haga clic en 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

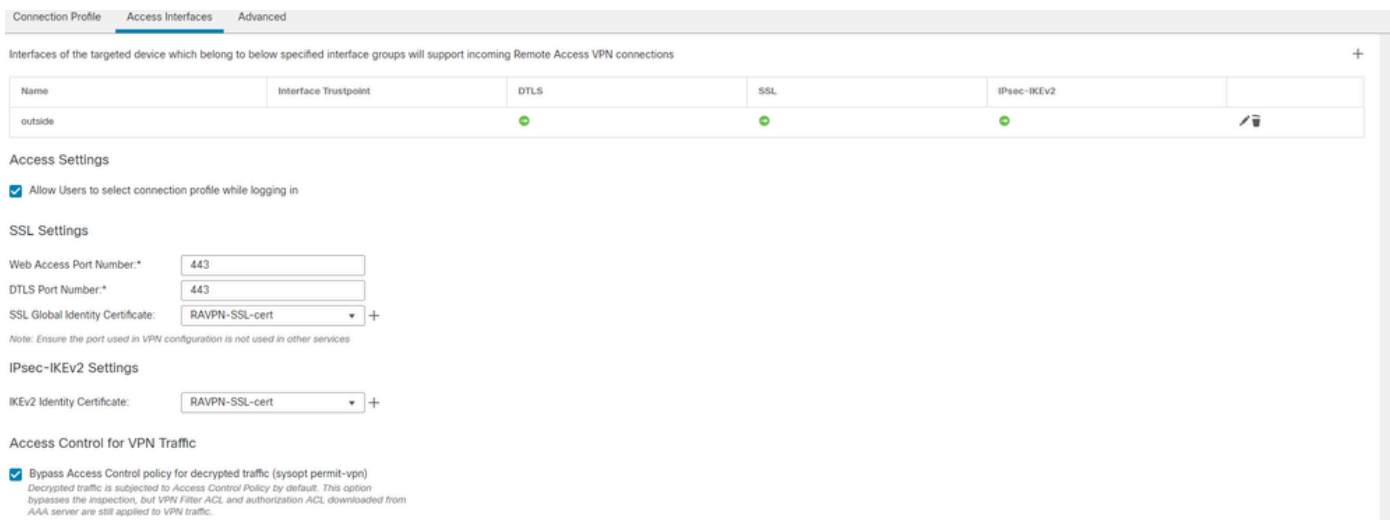
Save

FMC - Alias

10. Desplácese hasta Access Interfaces y seleccione la interfaz en la que debe activarse RAVPN IKEv2.

11. Seleccione el certificado de identidad tanto para SSL como para IKEv2.

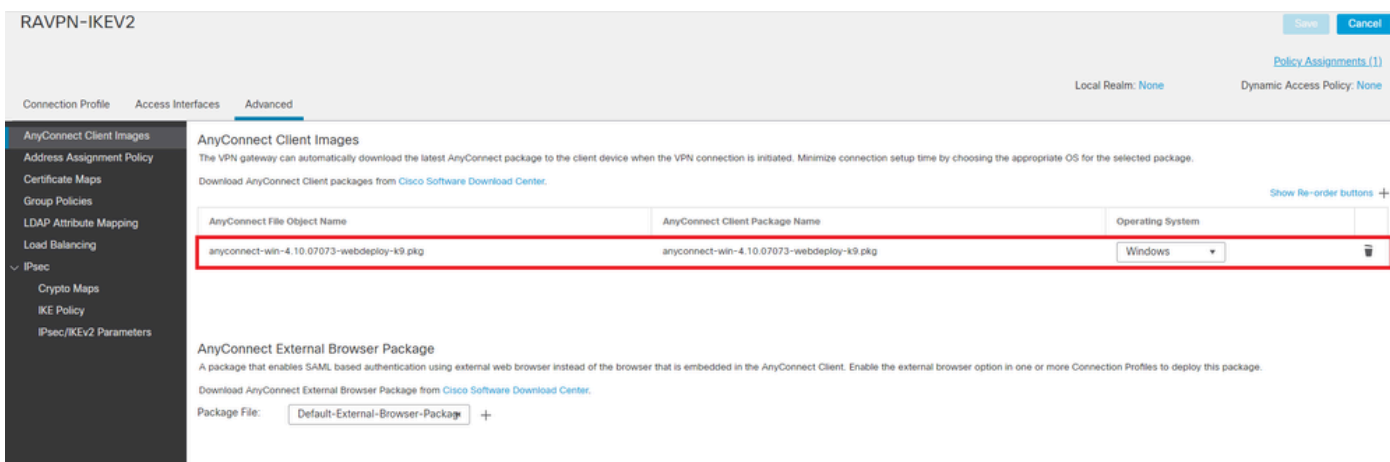
12. Haga clic en Save.



FMC - Interfaces de acceso

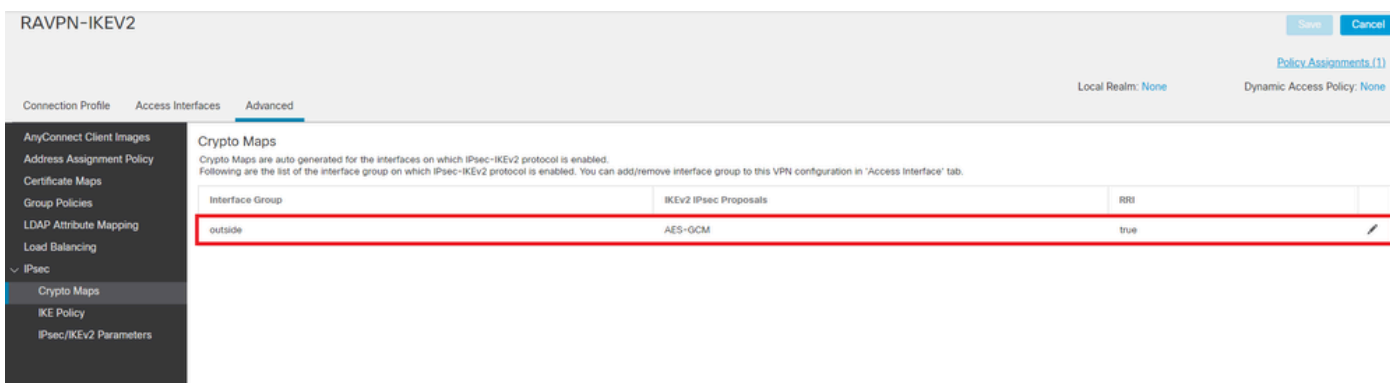
13. Acceda a Advanced .

14. Agregue las imágenes del cliente Anyconnect haciendo clic en +.



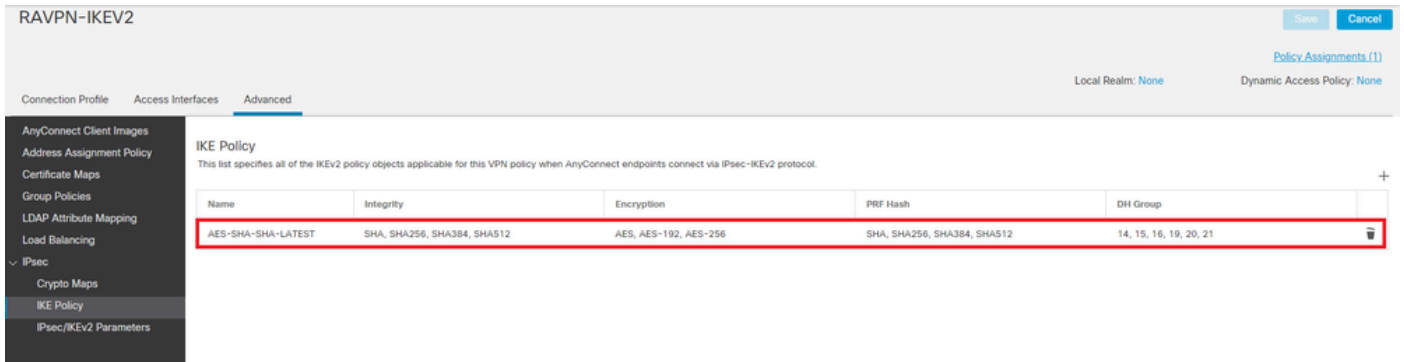
FMC - Paquete de cliente Anyconnect

15. DebajoIPsec, agregue losCrypto Maps como se muestra en la imagen.



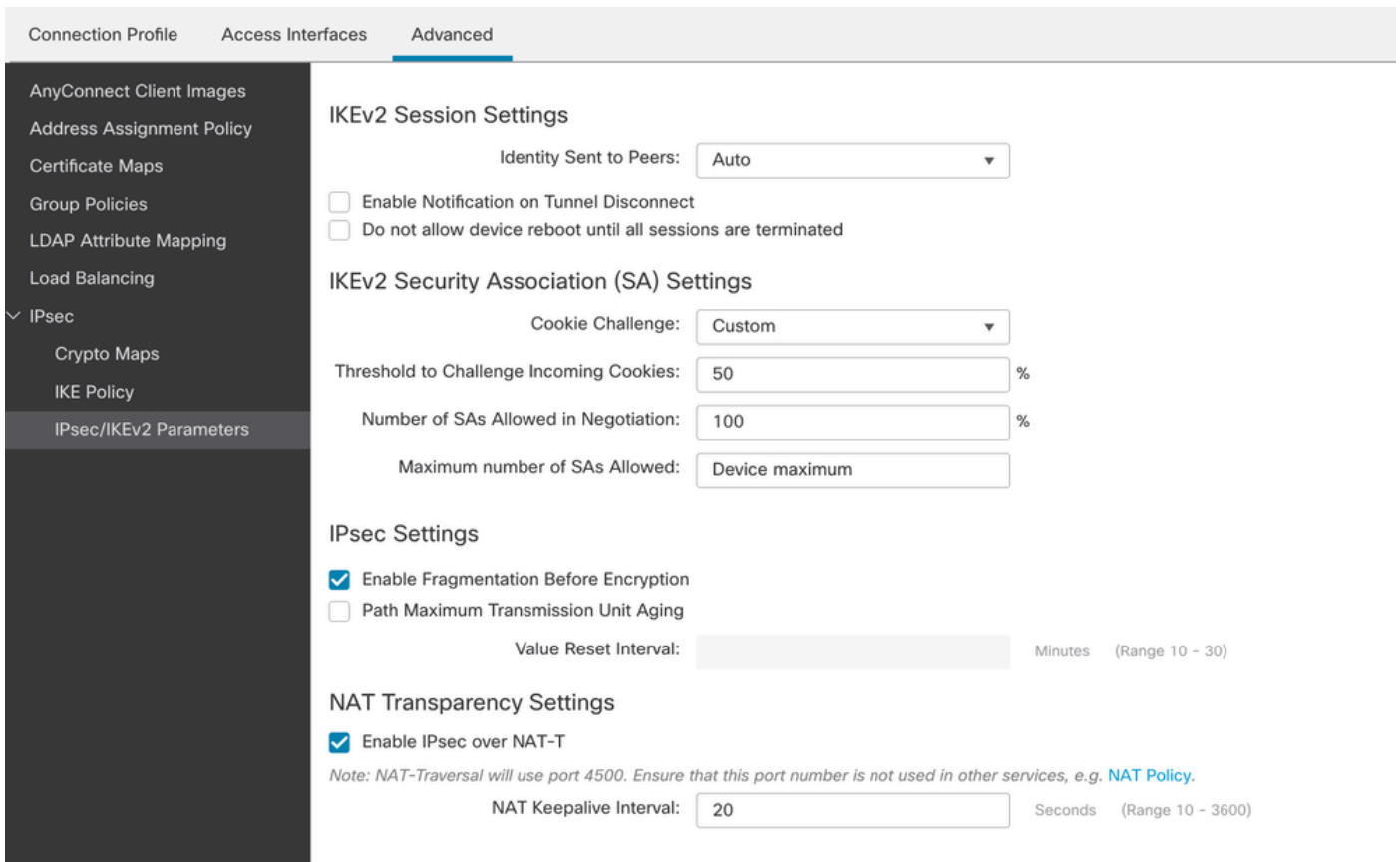
FMC: mapas criptográficos

16. En IPsec , agregue el IKE Policy haciendo clic en +.



FMC - Política IKE

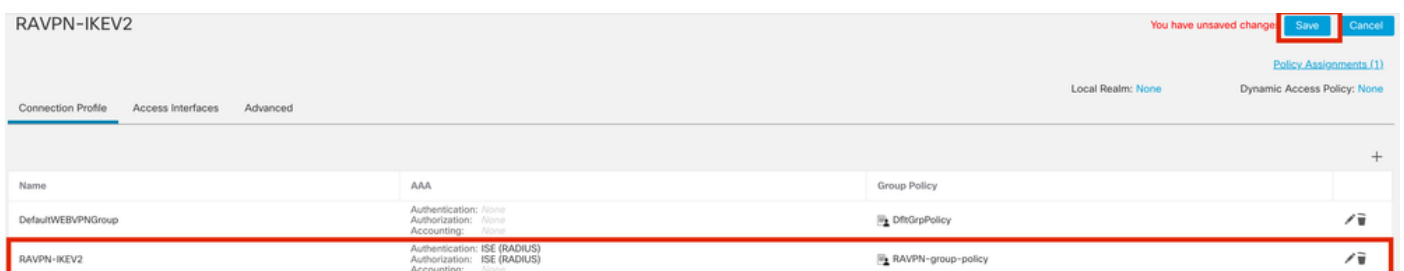
17. En IPsec , añade el IPsec/IKEv2 Parameters .



FMC - Parámetros IPsec/IKEv2

18. En Connection Profile, se crea un nuevo perfilRAVPN-IKEV2.

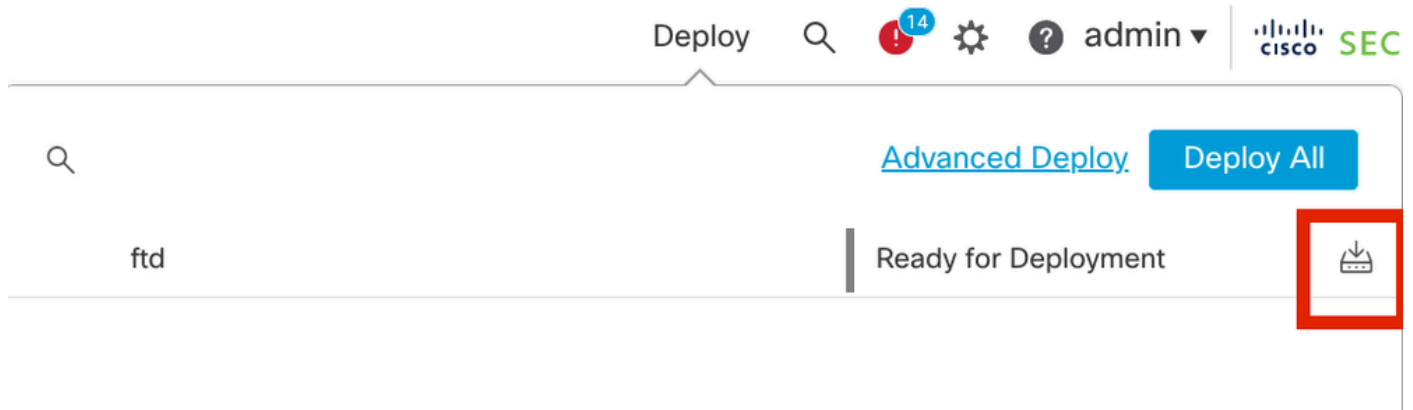
19. Haga Save clic como se muestra en la imagen.



FMC - Perfil de conexión RAVPN-IKEV2



20. Implemente la configuración.



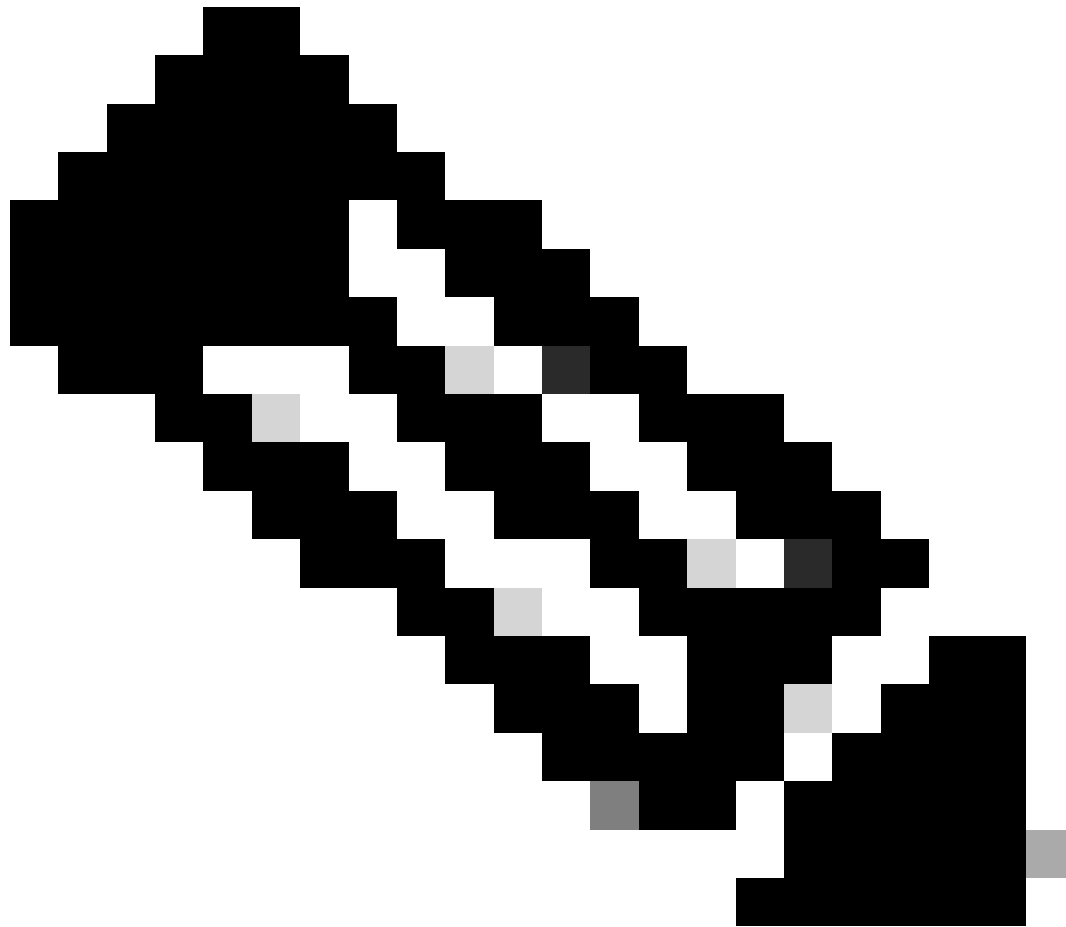
*FMC - Implementación de FTD*

7. Configuración del perfil de Anyconnect

Perfil en el PC, guardado en 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">
  <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>
</HostEntry> </ServerList> </AnyConnectProfile>
```



**Nota:** Se recomienda inhabilitar el cliente SSL como protocolo de tunelización bajo la política de grupo una vez que el perfil del cliente se descarga en la PC de todos los usuarios. Esto garantiza que los usuarios puedan conectarse exclusivamente mediante el protocolo de tunelación IKEv2/IPsec.

---

## Verificación

Puede utilizar esta sección para confirmar que su configuración funciona correctamente.

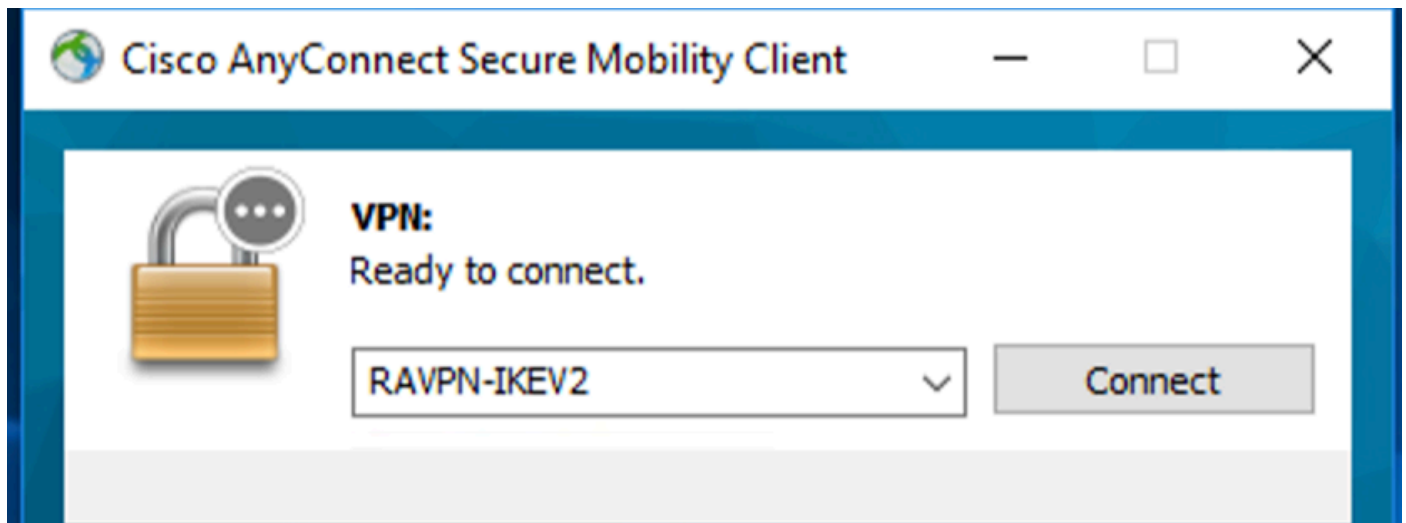
1. Para la primera conexión, utilice el FQDN/IP para establecer una conexión SSL desde el PC del usuario a través de Anyconnect.
2. Si el protocolo SSL está inhabilitado y no se puede realizar el paso anterior, asegúrese de que el perfil de cliente ClientProfile.xml esté presente en la PC bajo la trayectoria C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .
3. Introduzca el nombre de usuario y la contraseña para la autenticación una vez que se le solicite.

4. Después de la autenticación exitosa, el perfil del cliente se descarga en el PC del usuario.

5. Desconectar de Anyconnect.

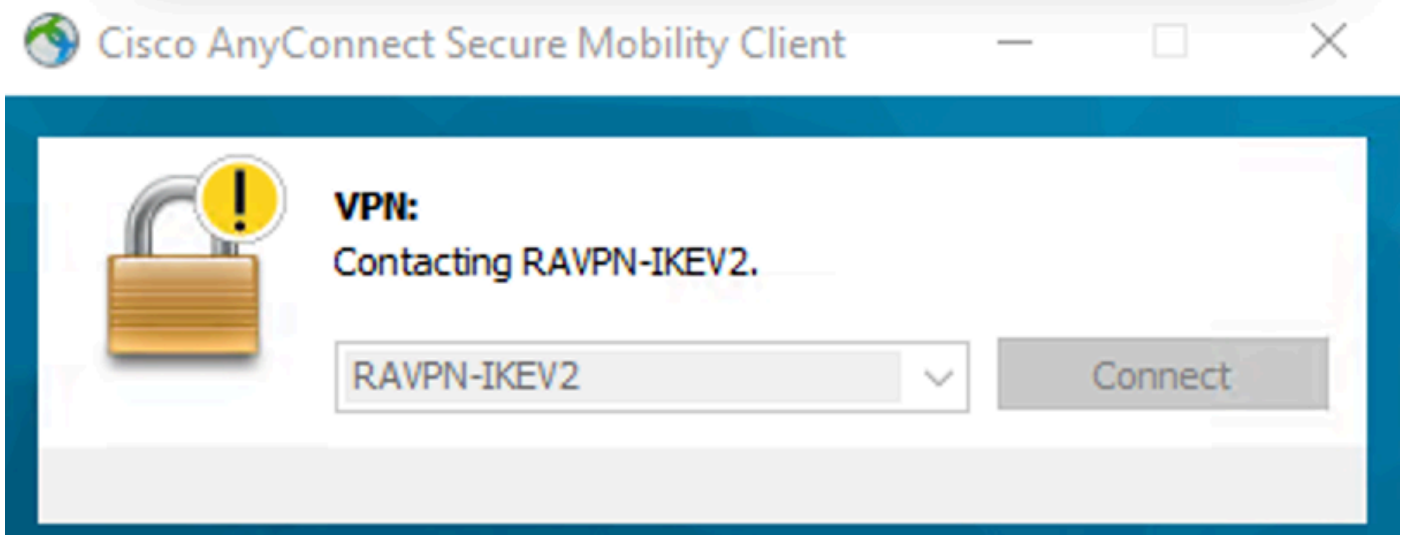
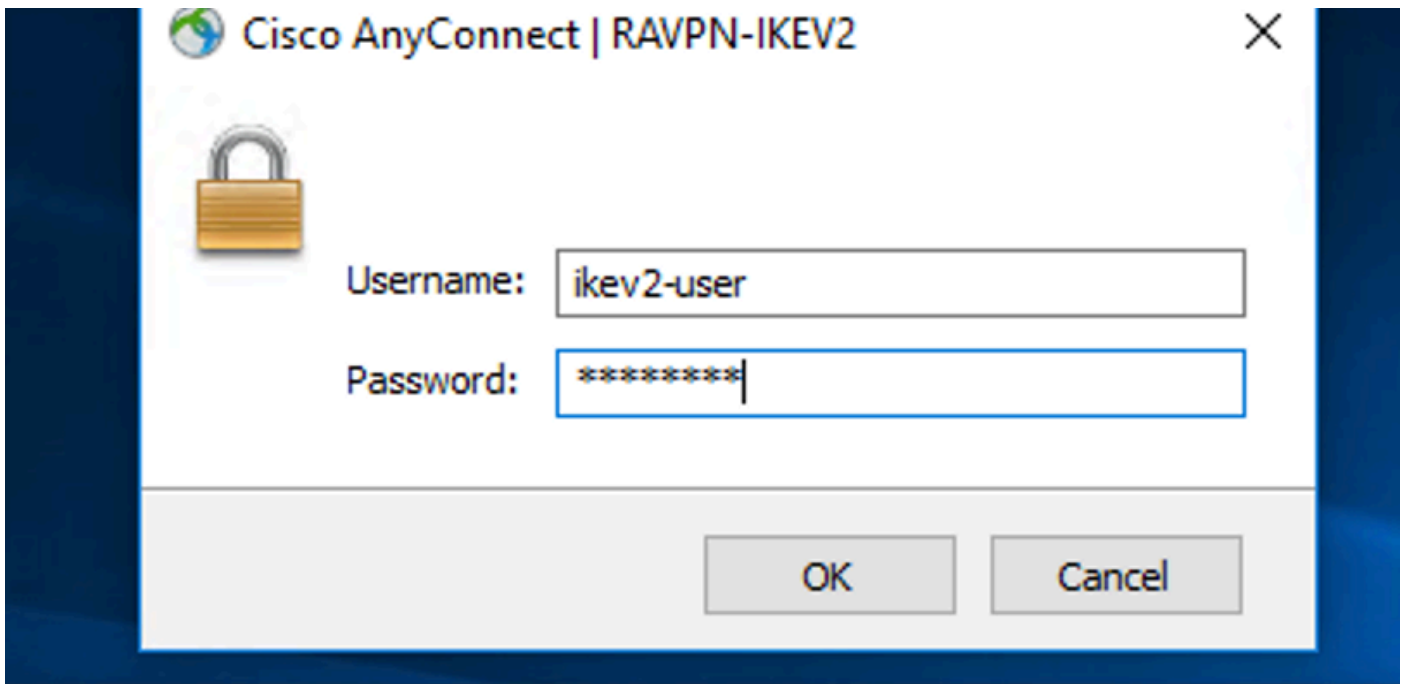
**RAVPN-IKEV2** 6. Una vez que se descarga el perfil, utilice el menú desplegable para elegir el nombre de host mencionado en el perfil del cliente para conectarse a Anyconnect mediante IKEv2/IPsec.

7. Haga clic en Connect.



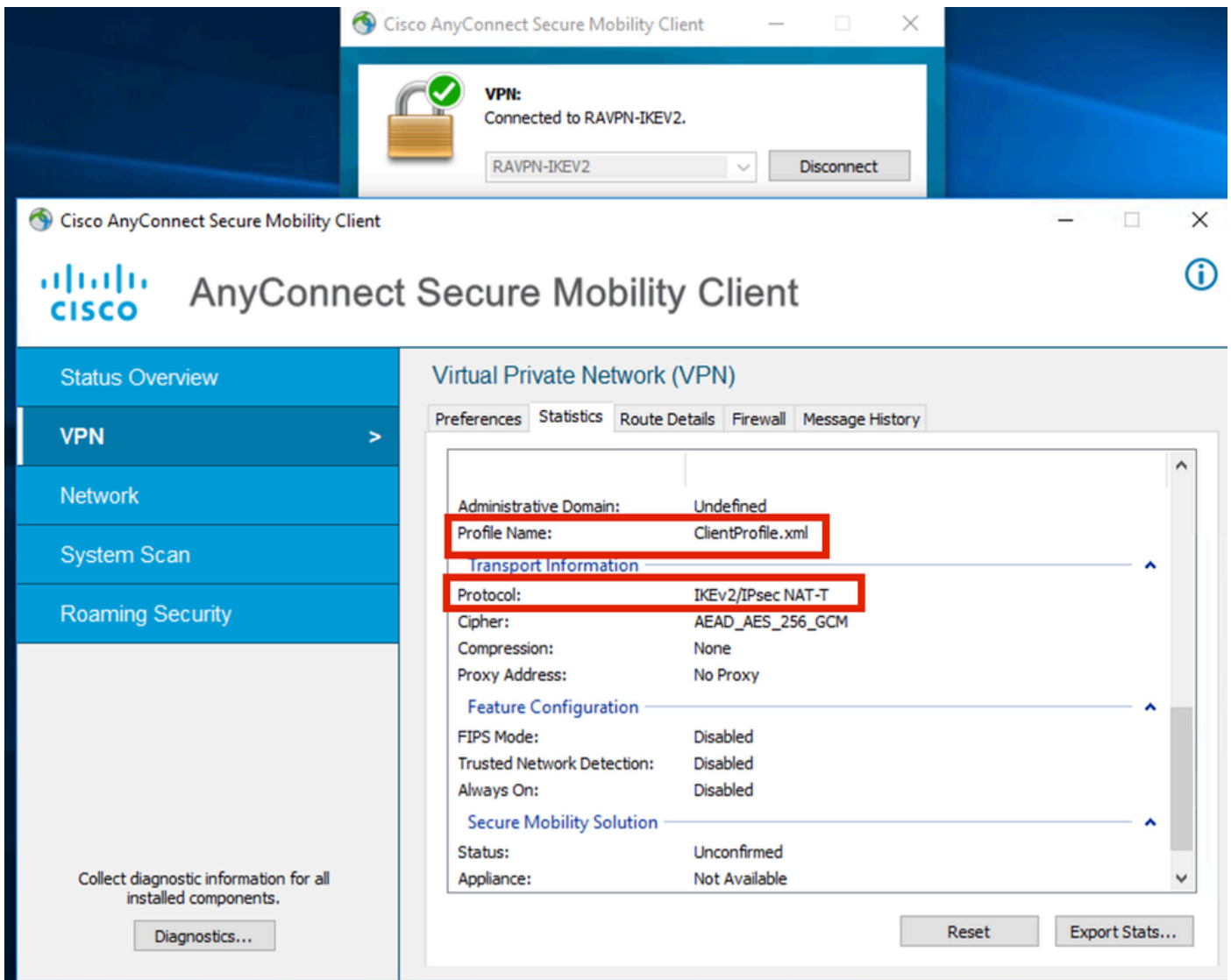
*Menú desplegable Anyconnect*

8. Introduzca el nombre de usuario y la contraseña para la autenticación creada en el servidor ISE.



*Conexión Anyconnect*

9. Compruebe el perfil y el protocolo (IKEv2/IPsec) que se utilizan una vez conectados.



Anyconnect conectado

Salidas 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

Registros de 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 - Live Logs

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

```
debug radius all
```

```
debug crypto ikev2 platform 255
```

```
debug crypto ikev2 protocol 255
```

```
debug crypto ipsec 255
```



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).