

# Configure Anyconnect VPN to FTD via IKEv2 with ISE

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[1. Import the SSL Certificate](#)

[2. Configure RADIUS Server](#)

[2.1. Manage FTD on FMC](#)

[2.2. Manage FTD On ISE](#)

[3. Create an Address Pool for VPN Users on FMC](#)

[4. Upload AnyConnect Images](#)

[5. Create XML Profile](#)

[5.1. On Profile Editor](#)

[5.2. On FMC](#)

[6. Configure Remote Access](#)

[7. Anyconnect Profile Configuration](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes the basic configuration of Remote Access VPN with IKEv2 and ISE authentication on FTD managed by the FMC.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic VPN, TLS, and Internet Key Exchange version 2 (IKEv2)
- Basic Authentication, Authorization, and Accounting (AAA) and RADIUS
- Experience with Firepower Management Center (FMC)

### Components Used

The information in this document is based on these software versions:

- Cisco Firepower Threat Defense (FTD) 7.2.0

- Cisco FMC 7.2.0
- AnyConnect 4.10.07073
- Cisco ISE 3.1

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. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

IKEv2 and Secure Sockets Layer (SSL) are both protocols used for establishing secure connections, particularly in the context of VPNs. IKEv2 provides strong encryption and authentication methods, offering a high level of security for VPN connections.

This document provides a configuration example for FTD version 7.2.0 and later, which allows remote access VPN in order to use Transport Layer Security (TLS) and IKEv2. As a client, Cisco AnyConnect can be used, which is supported on multiple platforms.

## Configure

### 1. Import the SSL Certificate

Certificates are essential when AnyConnect is configured.

There are limitations to manual certificate enrollment:

1. On FTD, a Certificate Authority (CA) certificate is needed before a Certificate Signing Request (CSR) is generated.
2. If the CSR is generated externally, a different method of PKCS12 is used.

There are several methods to obtain a certificate on FTD appliance, but the safe and easy one is to create a CSR and get it signed by a CA. Here is how to do that:

1. Navigate to `Objects > Object Management > PKI > Cert Enrollment`, and click `Add Cert Enrollment`.
2. Enter the trustpoint name `RAVPN-SSL-cert`.
3. Under the `CA Information` tab, choose `Enrollment Type` as `Manual` and paste the CA certificate as shown in the image.

## 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 - CA Certificate

4. Under Certificate Parameters, enter the subject name. For example:

## 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 - Certificate Parameters

5. Under the **Key** tab, choose the key type, and provide a name, and bit size. For RSA, 2048 bits is the minimum.

6. Click **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 - Certificate Key

7. Navigate to `Devices > Certificates > Add > New Certificate`.

8. Choose `Device`. Under `Cert Enrollment`, choose the trustpoint created, and click `Add` as shown in the image.

## 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 - Certificate Enrollment to FTD

9. Click ID, and a prompt to generate CSR is shown, choose Yes.

Firewall Management Center  
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🔒 ⚙️ 👤 admin 🔒 CISCO SECURE

Add

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 - Certificate CA Enrolled

# Warning

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

No

Yes

*FMC - Generate CSR*

10. A CSR is generated which can be shared with the CA in order to get the identity certificate.

11. After receiving the identity certificate from CA in base64 format, choose it from the disk by clicking **Browse Identity Certificate** and **Import** as shown in the image.

# 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-----
MIICqjCCAZICAQAwnNjEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQGA1UEAwwNRIRELmNpc2NvLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPLLwTQ6BkGjER2FfyofT+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 - Import Identity Certificate

12. Once the import is successful, the trustpoint RAVPN-SSL-cert is seen as:

Name	Domain	Enrollment Type	Status
RAVPN-SSL-cert	Global	Manual (CA & ID)	<a href="#">CA</a> <a href="#">ID</a>

FMC - Trustpoint Enrollment Successful

## 2. Configure RADIUS Server

### 2.1. Manage FTD on FMC

1. Navigate to **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group** .
2. Enter the name **ISE** and add RADIUS Servers by clicking **+**.



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 - Radius Server Configuration

3. Mention the IP address of the ISE Radius server along with the shared secret (Key) which is the same as on the ISE server.

4. Choose either Routing OR Specific Interface through which the FTD communicates with the ISE server.

5. Click Save as shown in the image.

## Edit RADIUS Server ?

IP Address/Hostname:\*

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\* (1-65535)

Key:\*

Confirm Key:\*

Accounting Port: (1-65535)

Timeout: (1-300) Seconds

Connect using:

Routing  Specific Interface i

▼ +

Redirect ACL:  
 ▼ +

6. Once saved, the Server is added under the RADIUS Server Group as shown in the image.

Name	Value
ISE	1 Server

*FMC - RADIUS Server Group*

## 2.2. Manage FTD On ISE

1. Navigate to **Network Devices** , and click **Add**.
2. Enter the Name 'Cisco-Radius' of the server and IP Address of the radius client which is the FTD communicating interface.
3. Under **Radius Authentication Settings**, add the **Shared Secret**.
4. Click **Save** .

**Network Devices**

Network Devices List > Cisco-Radius

**Network Devices**

Name

Description

IP Address  /

Device Profile

Model Name

Software Version

**Network Device Group**

Device Type  [Set To Default](#)

IPSEC  [Set To Default](#)

Location  [Set To Default](#)

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol

Shared Secret  [Show](#)

Use Second Shared Secret [Show](#)

networkDevices.secondSharedSecret

CoA Port  [Set To Default](#)

*ISE - Network Devices*

5. In order to create users, navigate to **Network Access > Identities > Network Access Users**, and click **Add**.
6. Create a Username and Login Password as required.

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 - Users

7. In order to setup basic policy, navigate to Policy > Policy Sets > Default > Authentication Policy > Default, choose All\_User\_ID\_Stores.

8. Navigate to Policy > Policy Sets > Default > Authorization Policy > Basic\_Authenticated\_Access, and choose PermitAccessas shown in the image.

Default

All\_User\_ID\_Stores

> Options

Basic\_Authenticated\_Access

Network\_Access\_Authentication\_Passed

PermitAccess

Select from list

ISE - Authentication Policy

ISE - Authorization Policy

### 3. Create an Address Pool for VPN Users on FMC

1. Navigate to Objects > Object Management > Address Pools > Add IPv4 Pools.
2. Enter the name RAVPN-Pool and **Address Range**, mask is optional.
3. Click **Save**.

## 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 - Address Pool

### 4. Upload AnyConnect Images

1. Navigate to Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Enter the name anyconnect-win-4.10.07073-webdeploy and click Browse in order to choose the **Anyconnect** file from the disk, click Save as shown in the image.

# Edit AnyConnect File



Name:\*

File Name:\*

File Type:\*

Description:

*FMC - Anyconnect Client Image*

## 5. Create XML Profile

### 5.1. On Profile Editor

1. Download the Profile Editor from [software.cisco.com](http://software.cisco.com) and open it.
2. Navigate to **Server List > Add...**
3. Enter the Display Name `RAVPN-IKEV2` and FQDN along with the **User Group** (alias name).
4. Choose the Primary protocol as `IPsec`, click **Ok** as shown in the image.

**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)

Profile Editor - Server List

5. Server List is added. Save it as 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.

Profile Editor - ClientProfile.xml

## 5.2. On FMC

1. Navigate to Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Enter a Name ClientProfile and click Browse in order to choose ClientProfile.xml file from disk.
3. Click Save .

# Edit AnyConnect File



Name:\*

File Name:\*

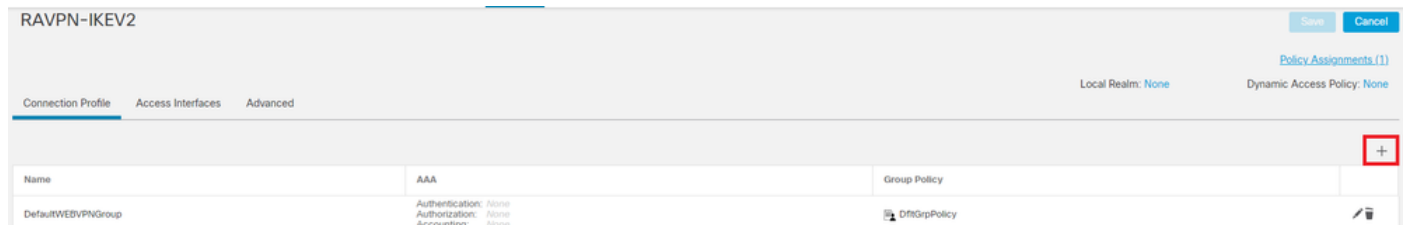
File Type:\*

Description:

FMC - Anyconnect VPN Profile

## 6. Configure Remote Access

1. Navigate to Devices > VPN > Remote Access and click + in order to add a Connection Profile as shown in the image.



FMC - Remote Access Connection Profile

2. Enter the connection profile name RAVPN-IKEV2 and create a group policy by clicking + in Group Policy as shown in the image.



## 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 - Group Policy

3. Enter the name `RAVPN-group-policy`, choose the VPN Protocols `SSL` and `IPsec-IKEv2` as shown in the image.

## 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 - VPN Protocols

4. Under AnyConnect > Profile , choose the XML profile ClientProfile from the dropdown, and click Save as shown in the image.

## 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 - Anyconnect Profile

5. Add the Address Pool RAVPN-Pool by clicking + 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 - Client Address Assignment

6. Navigate to AAA > Authentication Method, and choose AAA Only.
7. Choose Authentication Server as ISE (RADIUS).

## Edit Connection Profile



Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment   **AAA**   Aliases

### Authentication

Authentication Method:

Authentication Server:

Fallback to LOCAL Authentication

Use secondary authentication

### Authorization

Authorization Server:

Allow connection only if user exists in authorization database

### Accounting

Accounting Server:

▶ Advanced Settings

Cancel

Save

FMC - AAA Authentication

8. Navigate to `Aliases` , enter an Alias Name `RAVPN-IKEV2` , which is used as a user group in `ClientProfile.xml` .
9. Click `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 - Aliases

10. Navigate to *Access Interfaces*, and choose the interface where RAVPN IKEv2 must be enabled.
11. Choose the identity certificate for both SSL and IKEv2.
12. Click *Save*.

Connection Profile Access Interfaces Advanced

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside		+	+	+

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:\*

DTLS Port Number:\*

SSL Global Identity Certificate:  +

Note: Ensure the port used in VPN configuration is not used in other services

IPsec-IKEv2 Settings

IKEv2 Identity Certificate:  +

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

### FMC - Access Interfaces

13. Navigate to Advanced .

14. Add the Anyconnect Client images by clicking +.

RAVPN-IKEV2

Connection Profile Access Interfaces Advanced

AnyConnect Client Images

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.  
Download AnyConnect Client packages from Cisco Software Download Center.

AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
anyconnect-win-4.10.07073-webdeploy-k9.pkg	anyconnect-win-4.10.07073-webdeploy-k9.pkg	Windows

AnyConnect External Browser Package

A package that enables SAML based authentication using external web browser instead of the browser that is embedded in the AnyConnect Client. Enable the external browser option in one or more Connection Profiles to deploy this package.  
Download AnyConnect External Browser Package from Cisco Software Download Center.

Package File:  +

### FMC - Anyconnect Client Package

15. Under IPsec, add the Crypto Maps as shown in the image.

RAVPN-IKEV2

Connection Profile Access Interfaces Advanced

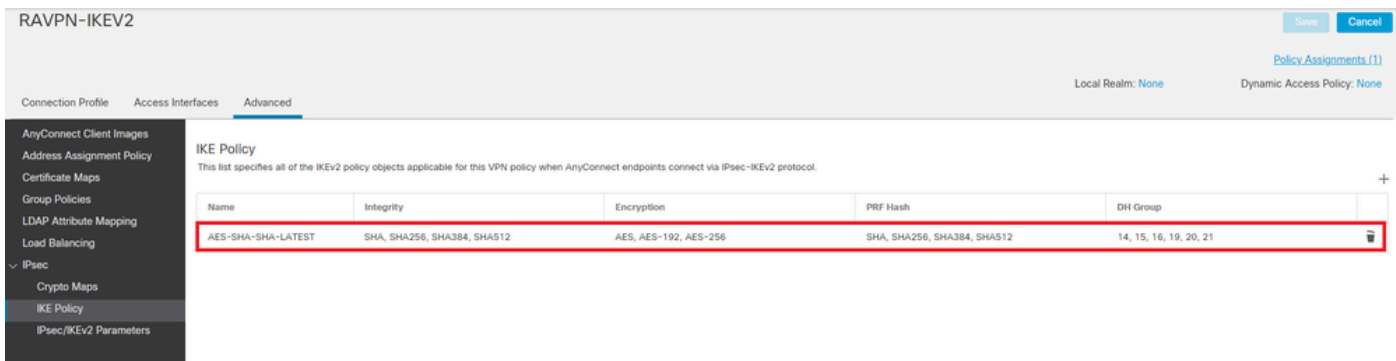
Crypto Maps

Crypto Maps are auto generated for the interfaces on which IPsec-IKEv2 protocol is enabled.  
Following are the list of the interface group on which IPsec-IKEv2 protocol is enabled. You can add/remove interface group to this VPN configuration in 'Access Interface' tab.

Interface Group	IKEv2 IPsec Proposals	RRR
outside	AES-GCM	true

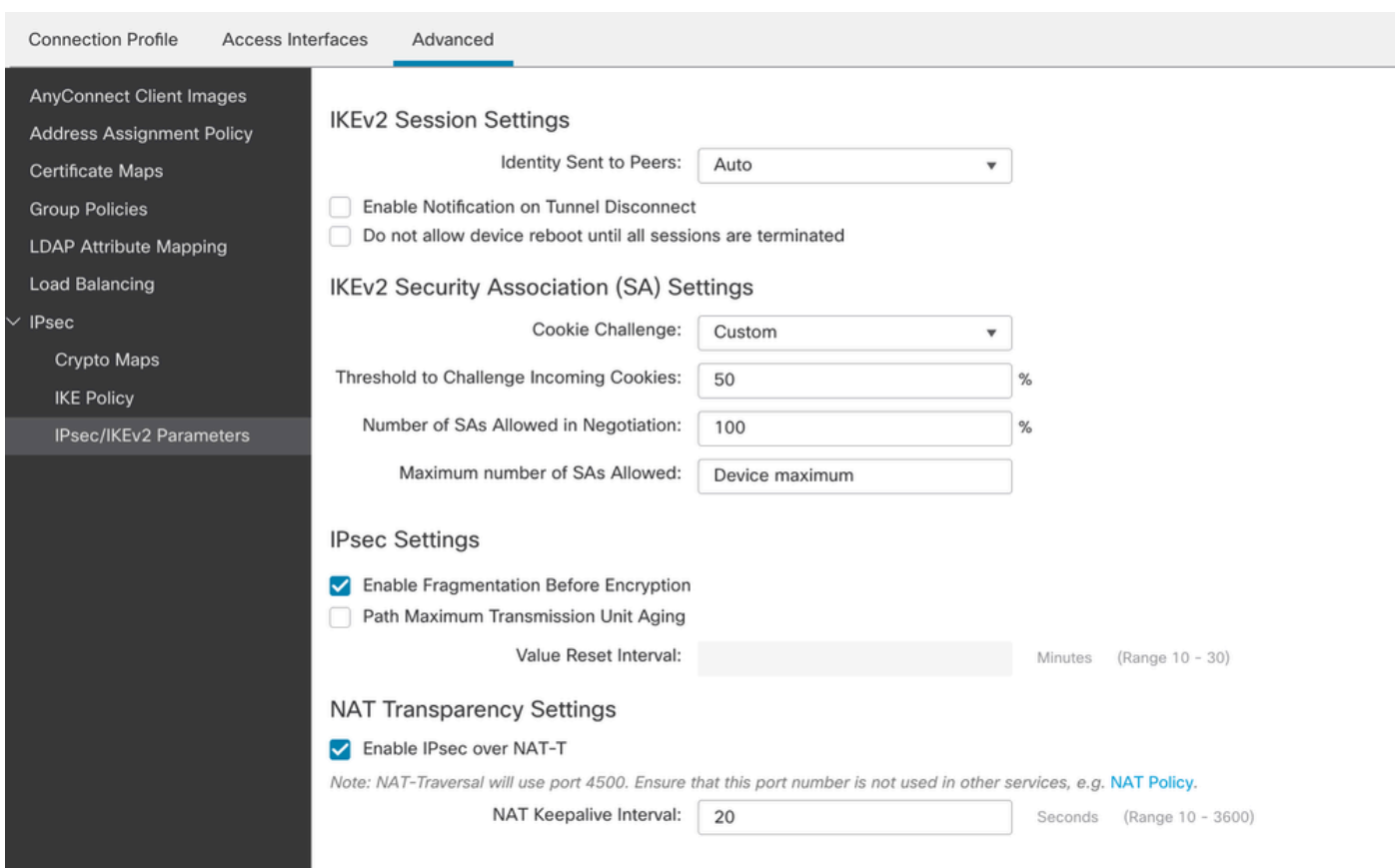
### FMC - Crypto Maps

16. Under IPsec, add the IKE Policy by clicking +.



FMC - IKE Policy

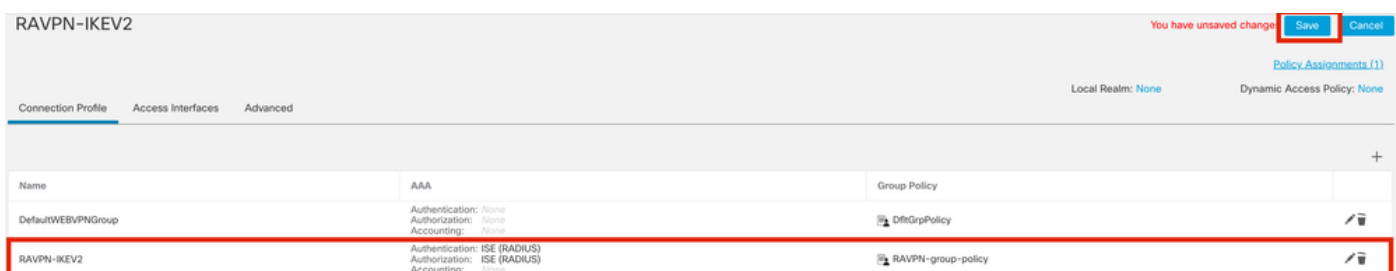
17. Under IPsec , add the IPsec/IKEv2 Parameters .



FMC - IPsec/IKEv2 Parameters

18. Under Connection Profile, new profile RAVPN-IKEV2 is created.

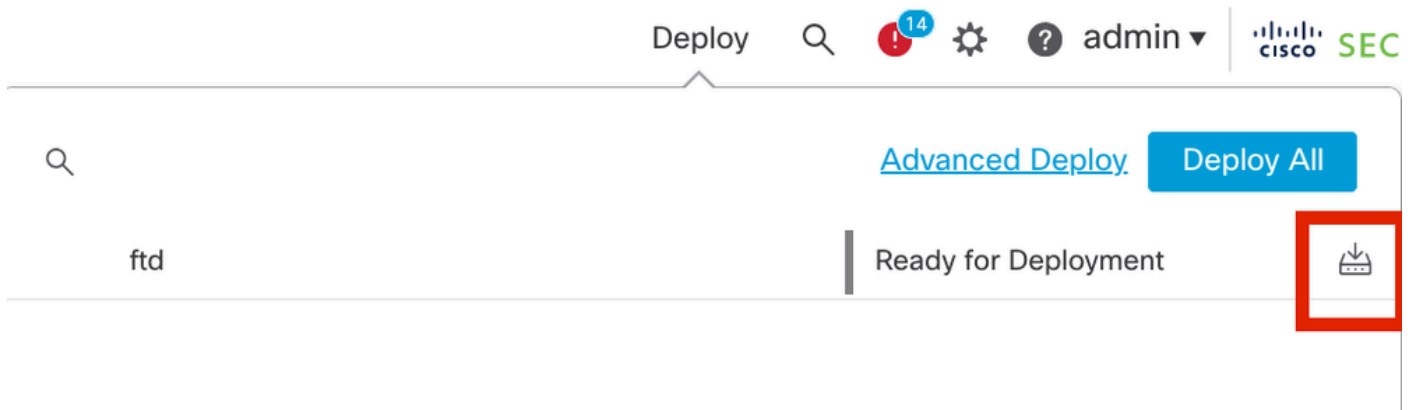
19. Click Save as shown in the image.



FMC - Connection Profile RAVPN-IKEV2



## 20. Deploy the configuration.



FMC - FTD Deployment

## 7. Anyconnect Profile Configuration

Profile on PC, saved under 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">
```

```
  <ClientInitialization>
```

```
    <UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
```

```
    <AutomaticCertSelection UserControllable="true">>false
```

```
  </AutomaticCertSelection>
```

```
  <ShowPreConnectMessage>>false</ShowPreConnectMessage>
```

```
  <CertificateStore>All</CertificateStore>
```

```
  <CertificateStoreOverride>>false</CertificateStoreOverride>
```

```
  <ProxySettings>Native</ProxySettings>
```

```
  <AllowLocalProxyConnections>>true</AllowLocalProxyConnections>
```

```
  <AuthenticationTimeout>12</AuthenticationTimeout>
```

```
  <AutoConnectOnStart UserControllable="true">>false</AutoConnectOnStart>
```

```
  <MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
```

```
  <LocalLanAccess UserControllable="true">>false</LocalLanAccess>
```

```
  <ClearSmartcardPin UserControllable="true">>true</ClearSmartcardPin>
```

```
  <AutoReconnect UserControllable="false">>true
```

```
    <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
```

```
    </AutoReconnectBehavior>
```

```
  </AutoReconnect>
```

```
  <AutoUpdate UserControllable="false">>true</AutoUpdate>
```

```
  <RSASecurIDIntegration UserControllable="true">Automatic
```

```
  </RSASecurIDIntegration>
```

```
  <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
```

```
  <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
```

```
  <AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
```

```
  <PPPExclusion UserControllable="false">Disable
```

```
    <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
```

```
  </PPPExclusion>
```

```
  <EnableScripting UserControllable="false">>false</EnableScripting>
```

```
  <EnableAutomaticServerSelection UserControllable="false">>false
```

```
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
```

```
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
```

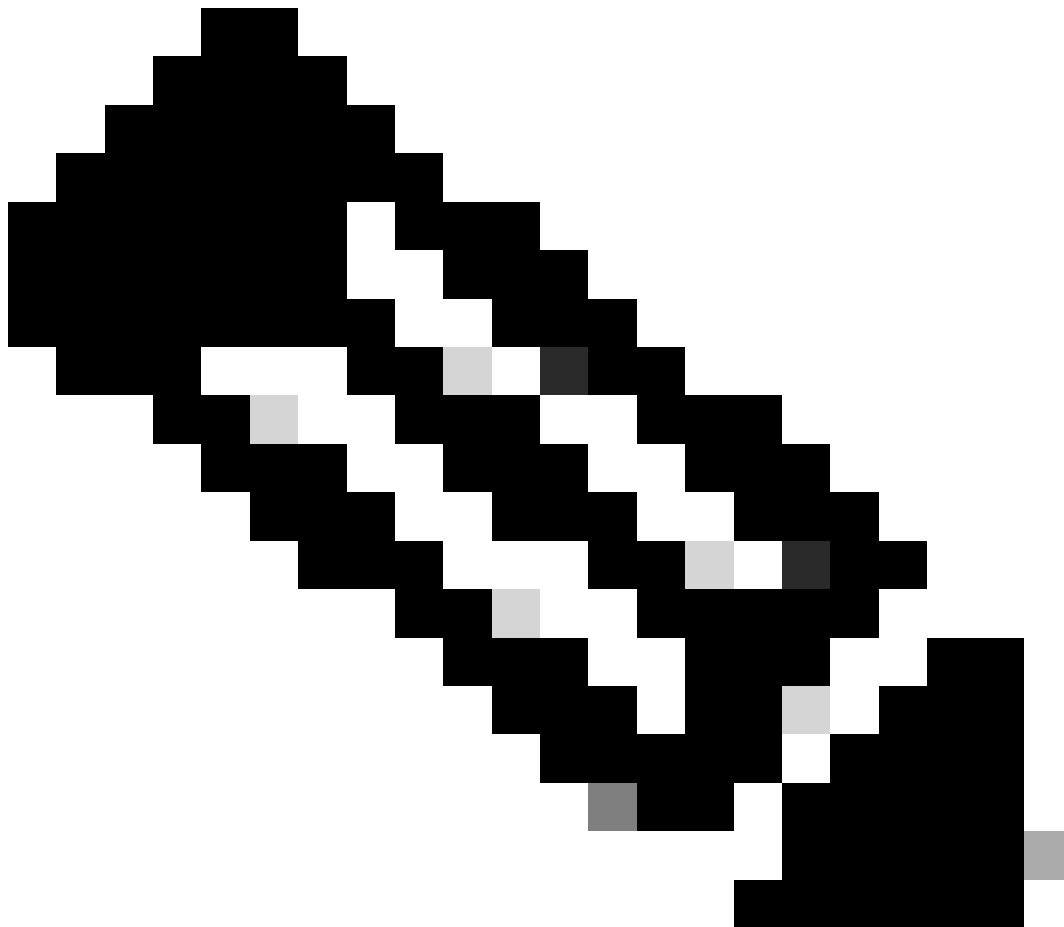
```
  </EnableAutomaticServerSelection>
```

```
  <RetainVpnOnLogoff>>false
```

```
</RetainVpnOnLogoff>
```

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

---



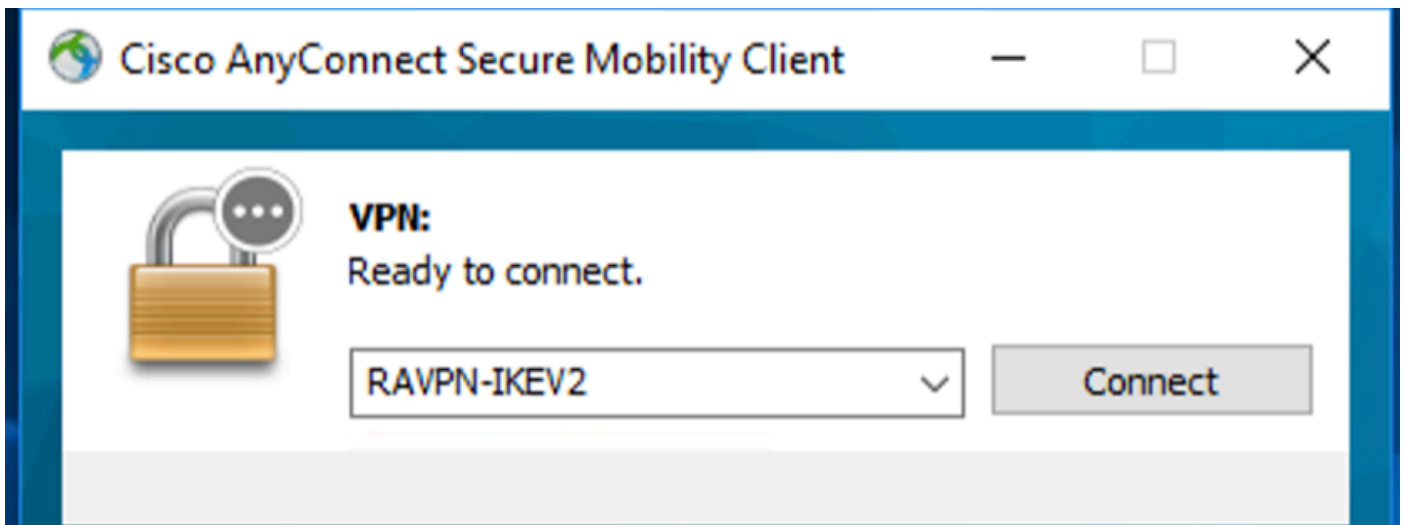
**Note:** It is recommended to disable the SSL client as tunneling protocol under the group policy once the client profile is downloaded to the PC of all the users. This ensures that users can connect exclusively using the IKEv2/IPsec tunneling protocol.

---

## Verify

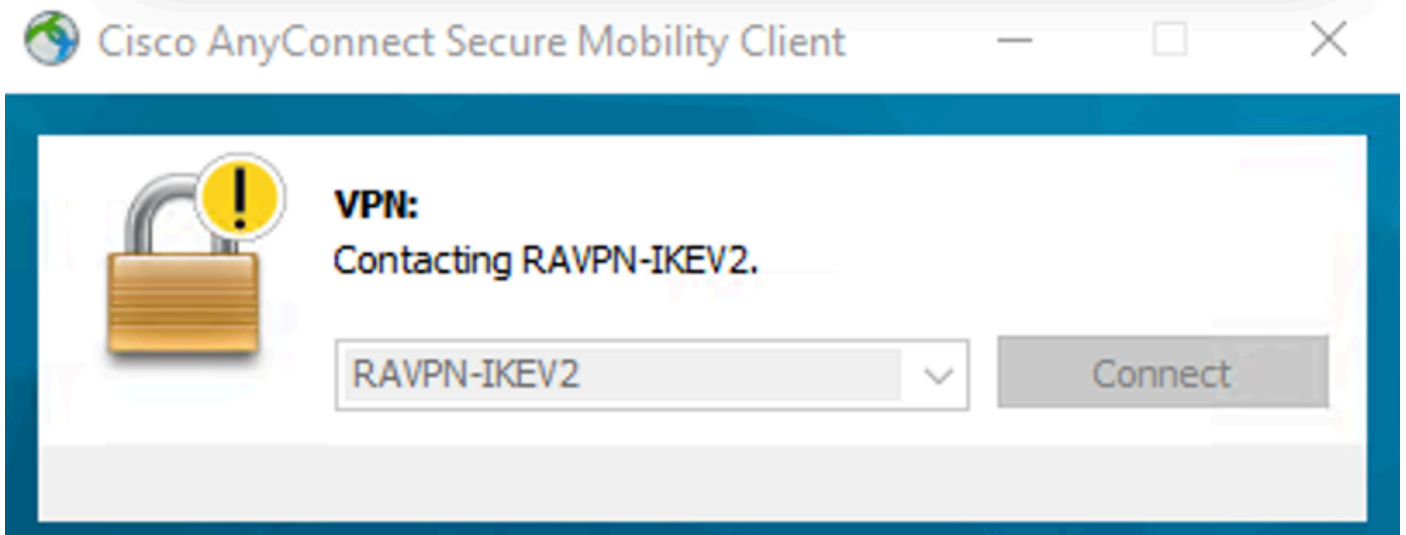
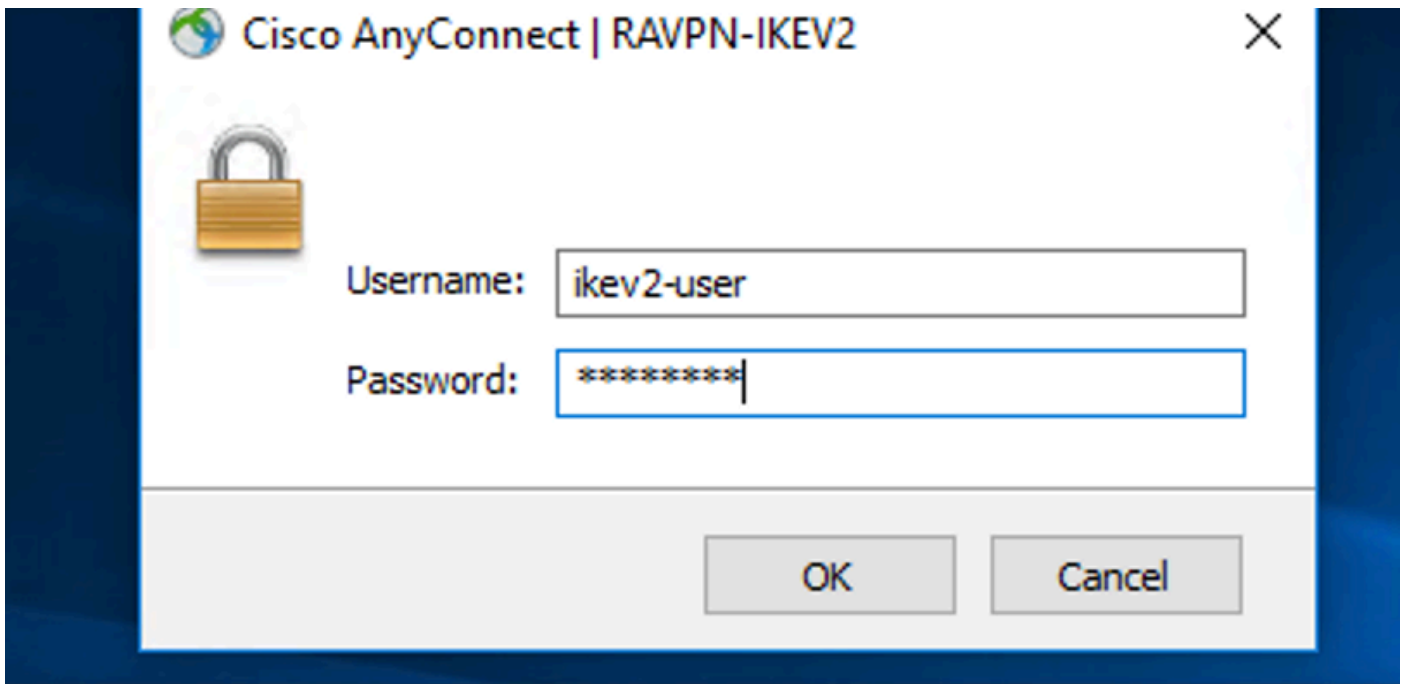
You can use this section in order to confirm that your configuration works properly.

1. For the first connection, use the FQDN/IP in order to establish an SSL connection from the PC of the user through Anyconnect.
2. If the SSL protocol is disabled and the previous step cannot be performed, ensure that the client profile `ClientProfile.xml` is present on the PC under the path `C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile`.
3. Enter the username and password for authentication once prompted.
4. After successful authentication, the client profile is downloaded on the PC of the user.
5. Disconnect from Anyconnect.
6. Once the Profile is downloaded, use the drop-down in order to choose the hostname mentioned in the client profile `RAVPN-IKEV2` in order to connect to Anyconnect using IKEv2/IPsec.
7. Click `Connect`.



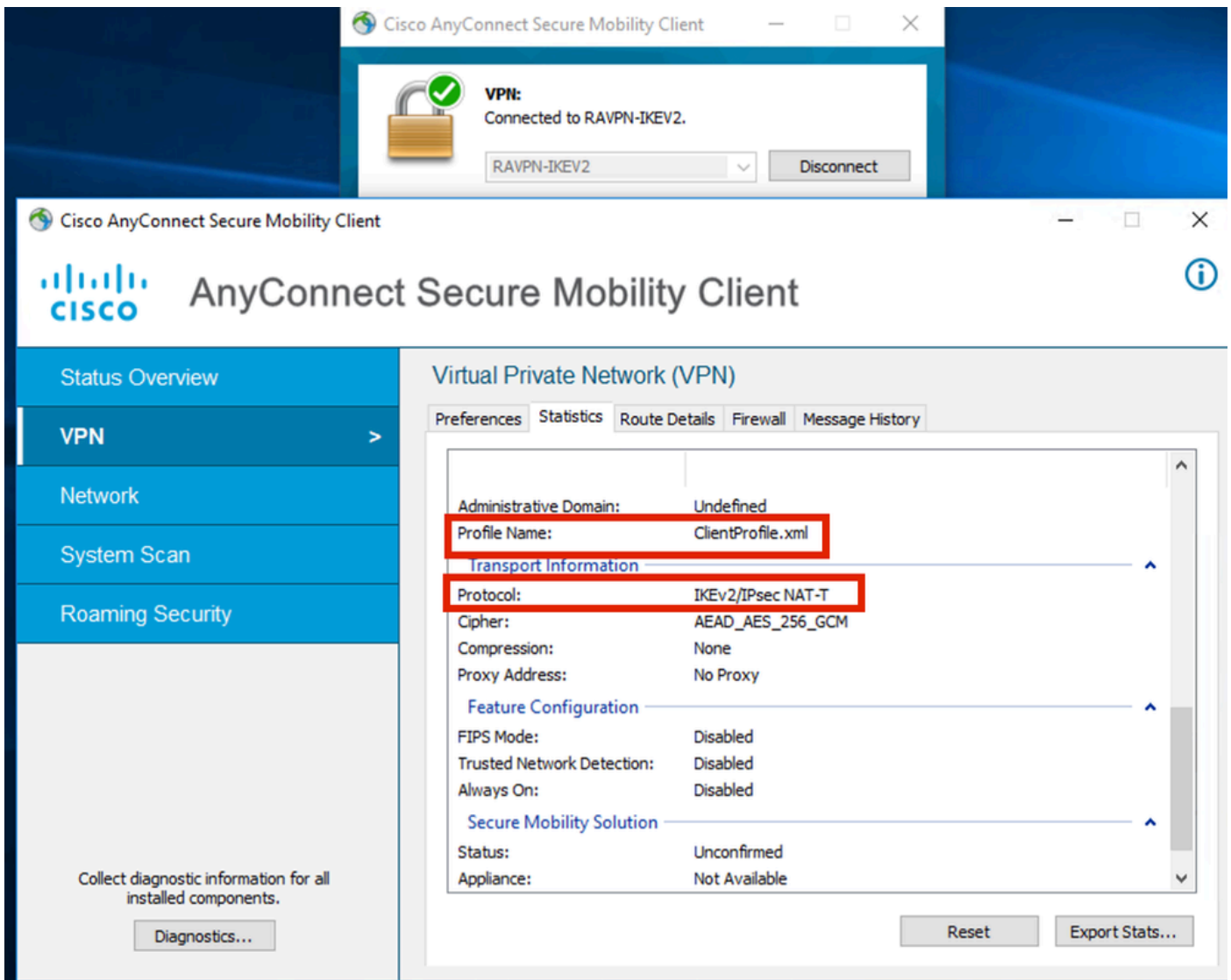
*Anyconnect dropdown*

8. Enter the username and password for authentication that was created on the ISE server.



*Anyconnect Connection*

9. Verify the Profile and Protocol (IKEv2/IPsec) used once connected.



Anyconnect Connected

## FTD CLI Outputs:

<#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: 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

### ISE Logs:

Time	Status	Details	Repe...	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	00:50:56:8D:6B:...	Windows1...	Default >>...	Default >>...	PermitAcc...							ise
Jan 04, 2024 07:14:10.4...				ikev2-user	00:50:56:8D:6B:...	Windows1...	Default >>...	Default >>...	PermitAcc...		Cisco-Radius		Workstation			ise

## **Troubleshoot**

This section provides information you can use in order to troubleshoot your configuration.

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