

# IKEv2 ربيع FTD ىل AnyConnect VPN نيوكت عم ISE

## تايوت حمل

---

[عمدق مل](#)

[ةيساس الابل طت مل](#)

[تابل طت مل](#)

[عمدختس مل تانوك مل](#)

[ةيساس ا تامول عم](#)

[نيوكت مل](#)

[1. SSL ةداهش داري تس](#)

[2. RADIUS مداخ نيوكت](#)

[2.1. FTD ةرادا](#)

[2.2. ISE ىل FTD ةرادا](#)

[3. FMC ىل VPN يم دختس مل نيوان عم مچت عاش نا](#)

[4. AnyConnect روص لي مچت](#)

[5. XML فيرعت فلم عاش نا](#)

[5.1. فيرعت مل فلم برجم يف](#)

[5.2. on FMC](#)

[6. دعب نعل لوصول نيوكت](#)

[7. AnyConnect فيرعت فلم نيوكت](#)

[ةحصل مل نم ققچت مل](#)

[اهج الص او اعطخ ال فاشك تس](#)

---

## عمدق مل

مادختس اب دعب نعل لوصول اب ةصاخ ال VPN ةكبشل يساس ال نيوكت مل دن تس مل اذه فص ي  
FMC ةطس او ب اهتراد ا متت ي ال FTD ىل ISE ةق داص مو IKEv2.

## ةيساس الابل طت مل

### تابل طت مل

ةيلات ال عيضاوم لابل ةفرعم كي دل نوكت نابل Cisco ي صوت:

- تنرتن ال اجات فلم لدابت نم 2 رادصل او، TLS، و، ةيساس ال ةيره اظلا ةصاخ ال تاكبش مل (IKEv2)
- RADIUS و (AAA) ةيساس ال ةبس احم ل او ضي وفت ل او ةق داص مل
- FirePOWER (FMC) ةرادا زكرم ةبرجت

### عمدختس مل تانوك مل



## 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 - قءاهش - CA

4. لاثم لال لبس لى ع. عوضوم لال مسا لخدأ. Certificate Parameters تحت.

## 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

إدخال الشال تامل عم - FMC

5. 2048 ل ىندألا دحلل نوكي، RSA ل ةبسننلاب. تبلا مرجحو مسا ريفوتب مقو، حاتفملا عون رتخأ، بيوتب لةمالة Key تحت.

6. Save رقنا.

## 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

ةداهشلا حاتفم - FMC

7. Devices > Certificates > Add > New Certificate.

8. ةروصللا يف حضوم وه امك Add رقناو، هؤاشنلا مت يذلا TrustPoint رتخأ، Cert Enrollment، تحت Device رتخأ.

## 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

FTD في ةداهش ل ليجست - FMC

9. Yes. رتخأ CSR، ةاشناب ةبل اطم ضرع م تي و ID رونا.

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

ةلجسم CA ةداهش - FMC

# Warning

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

No

Yes

CSR ءاشن | FMC

10. ةيوهلا ةءاهش ىلع لوصحلل CA عم هتكاراشم نكمي يذلا CSR ءاشن امتي.

11. حضوم وه امك Browse Identity Certificate Import رقرنلاب صرقلا نم اهترخ|، base64 قيسننتب CA نم ةيوهلا ةءاهش يقلت دعب. ةروصلا يف.

# 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](#)

ةي وهلا ةداهش داري تس | FMC

12. اهنأ ىلع ةقثلال RAVPN-SSL-cert ةطقن ىل رظن ي، داري تس ال حاجن درجم ب:

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

FMC - TrustPoint لي جس تس حاجن -

## 2. رADIUS مداخ ني وك ت

### 2.1. FMC ىل ع FTD ةراد |

1. ىل لقتنا . Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. + قوف رقن لابل RADIUS مداوخ فضأو ISE م سال ال لخدأ .



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

RADIUS مداخل نيوكوت - FMC

3. ISE مداخل يلع دوجومال هسفن وهو (حاتفملا) كرتشملا رسلا عم ISE Radius مداخل صاخلا IP ناووع ركذا.

4. ISE مداخل (FTD) ةرسلا قئاف لاسرالا جم انرب هلاخ نم لصتي يذلل Specific Interfacel و Routing ام ارتخأ.

## 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

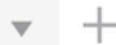
Timeout: (1-300) Seconds

10

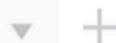
Connect using:

Routing  Specific Interface

outside



Redirect ACL:



Cancel

Save

6. ةروصولا يف حضورم وه امك RADIUS Server Group نمض مداخل ةفاض ا متت ،اهظفح درجم ب .

Name	Value
ISE	1 Server

RADIUS مداول ةومجم - FMC

## 2.2. ISE لىل FTD ةرادا

1. Add لىل رقناو ، Network Devices لىل لقتنا .

2. FTD لاصتا ةهجاو وه يذل RADIUS IP Address لىل مءوم مداخل ل "Cisco-RADIUS" مسا لءدا .

3. Radius Authentication Settings، ءضأ Shared Secret تحت .

4. Save . رقنا .

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | Location Services

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 [Show](#)

networkDevices.secondSharedSecret: ..... [Show](#)

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

ةكبشلال ةزهجا - ISE

5. Add قوف رقناو ، Network Access > Identities > Network Access Users لىل لقتنا ، نىمءختسم ءاشنال .

6. ءءال بسح UserNameAndLogin رورم ةملك ءاشنال ب مق .

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 ⓘ

نومدخستسمل - ISE

7. رتخاو، Policy > Policy Sets > Default > Authentication Policy > Default، ةسايسال ةسايسال دادع| لجأ نم 7. All\_User\_ID\_Stores.

8. يف حضورم وه امك PermitAccess رتخاو، Policy > Policy Sets > Default > Authorization Policy > Basic\_Authenticated\_Access، ةروصلال ةروصلال.

Default

All\_User\_ID\_Stores ⓘ ▾

> Options 4 ⚙️

Basic\_Authenticated\_Access Network\_Access\_Authentication\_Passed PermitAccess x ▾ + Select from list ▾ + 4 ⚙️

ةقداصلال ةسايس - ISE

ليوختال ةسايس - ISE

3. FMC لى VPN يمدخستسمل نيوانع عمجت عاشن|.

1. Objects > Object Management > Address Pools > Add IPv4 Pools.

2. يرايخ| عانقلالو، ناونعلال قاطنو RAVPN-Pool مسالال لخدأ.

3. ظفح قوف رقنا.

## 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

نيوانعلا عمحت - FMC

#### 4. روص لي محت AnyConnect

1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.

2. Save رقمنا، صرقلا نم **AnyConnect** فلم راي تخال Browse قوف رقمناو anyconnect-win-4.10.07073-webdeploy م سال لخدأ. روصلا يف حضوم.

# Edit AnyConnect File



Name:\*

File Name:\*

[Browse..](#)

File Type:\*

AnyConnect Client Image ▼

Description:

[Cancel](#)

[Save](#)

FMC - AnyConnect ليمع ةروص -

5. XML فيرعت فلم ءاشن |

5.1 فيرعتل فلم ررحم في

1. هتفو software.cisco.com نم فيرعتل فلم ررحم ليزنتب مق .

2. **Server List > Add..** لى لقتنا .

3. (راعستسملال مسالال مسالال) نيمدختسملال ةوعومجم عم RAVPN-IKEV2 FQDN ررعال مسالال لخدأ .

4. ةروصلال في حضورم وه امك **Ok** , IPsec يساسألال لوكوتوربلال رتخأ .

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) RAVPN-IKEV2

FQDN or IP Address User Group

ftd.cisco.com / RAVPN-IKEV2

Group URL

ftd.cisco.com/RAVPN-IKEV2

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

مداوخل اعمىاق - فيرعتال فلم ررحم

5. مداوخل اعمىاق ةفاضل متت . ClientProfile.xml مساب ظفح .

AnyConnect Profile Editor - VPN

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.

Add... Delete

Edit... Details

مداوخل اعمىاق - ClientProfile.xml فيرعتال فلم ررحم

## 5.2. فمىل فMC

1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. صرقلال نم فلم ClientProfile.xml رايتخال Browse قوف ررقلال او ClientProfile.xml امسا لخدأ .
3. ررقلال Save .





## 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

فمجة ومجملة ةسايس - FMC

3. ةروصل اليف حضوم وه امك VPN SSL and IPsec-IKEv2 تالوك وتورب رتخأ، RAVPN-group-policy م س الال لخدأ.

## 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

VPN تالوكوتورپ - FMC

4. في حضوره وه امك Save رقناو، ةلدس نم لة مئاق ل نم XML ClientProfile صي صخت فلم رتخأ ، AnyConnect > Profile تحت 4. ةروصل لة.

## 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 فيرمت فلم -

5. + قوف رقن لابل RAVPN-Pool نيو انعال عمجت فضا.

## Edit Connection Profile

Connection Profile:\* RAVPN-IKEV2

Group Policy:\* RAVPN-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

لېم عمل ناوونع نېږدېت - FMC

6. AAA Only رتځاو، AAA > Authentication Method څېړل لقت نا.

7. Authentication Server ISE (RADIUS) رتځا.

## 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 - AAA إعدادات

8. ClientProfile.xml في نيم دختسم ةومجكم هم ادختس امتي يذلاو، راعتسم RAVPN-IKEV2 م سا لخدأو، Aliases ل لقتنا .

9. Save رقتنا .

## 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

قراعتسم عامسأ - FMC

10. اءب RAVPN IKEv2 نءكمت بءء ءءءا ءهءاولا رءءاو، Access Interfaces ءءل لءقءنا.

11. IKEv2 و SSL نم لءل ءءءهءل ءءاهش رءءأ.

12. رءنا 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.

لوصول تاهج او - FMC

Advanced لى لقتنا .

+ قوف رقب لاب AnyConnect Client روص فضا .

RAVPN-IKEV2 Save Cancel

Policy Assignments (1)  
Local Realm: None Dynamic Access Policy: None

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.

Show Re-order buttons +

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:  +

AnyConnect Client ةم زح - FMC

ةروصل لى ف حصوصم وه امك Crypto Maps فضا ، IPsec تحت .

RAVPN-IKEV2 Save Cancel

Policy Assignments (1)  
Local Realm: None Dynamic Access Policy: None

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

رى فشت لى طئارخ - FMC

+ رقب IKE Policy فضا ، IPsec تحت .

RAVPN-IKEV2 Save Cancel

Policy Assignments (1)  
Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

**AnyConnect Client Images**  
Address Assignment Policy  
Certificate Maps  
Group Policies  
LDAP Attribute Mapping  
Load Balancing  
IPsec  
Crypto Maps  
**IKE Policy**  
IPsec/IKEv2 Parameters

**IKE Policy**  
This list specifies all of the IKEv2 policy objects applicable for this VPN policy when AnyConnect endpoints connect via IPsec-IKEv2 protocol.

Name	Integrity	Encryption	PRF Hash	DH Group
AES-SHA-SHA-LATEST	SHA, SHA256, SHA384, SHA512	AES, AES-192, AES-256	SHA, SHA256, SHA384, SHA512	14, 15, 16, 19, 20, 21

FMC - IKE ةساي س -

17. IPsec ةفضأ ، IPsec/IKEv2 Parameters تحت .

Connection Profile Access Interfaces **Advanced**

**AnyConnect Client Images**  
Address Assignment Policy  
Certificate Maps  
Group Policies  
LDAP Attribute Mapping  
Load Balancing  
IPsec  
Crypto Maps  
IKE Policy  
**IPsec/IKEv2 Parameters**

**IKEv2 Session Settings**

Identity Sent to Peers: Auto

Enable Notification on Tunnel Disconnect  
 Do not allow device reboot until all sessions are terminated

**IKEv2 Security Association (SA) Settings**

Cookie Challenge: Custom

Threshold to Challenge Incoming Cookies: 50 %

Number of SAs Allowed in Negotiation: 100 %

Maximum number of SAs Allowed: Device maximum

**IPsec Settings**

Enable Fragmentation Before Encryption  
 Path Maximum Transmission Unit Aging

Value Reset Interval: Minutes (Range 10 - 30)

**NAT Transparency Settings**

Enable IPsec over NAT-T

Note: NAT-Traversal will use port 4500. Ensure that this port number is not used in other services, e.g. NAT Policy.

NAT Keepalive Interval: 20 Seconds (Range 10 - 3600)

FMC - IPsec/IKEv2 تامل عم -

18. Connection Profile تحت ، RAVPN-IKEV2 تقلخ ، ةديج في صوت .

19. ةروصلا في ةحضوملا ةس نل Save .

RAVPN-IKEV2 You have unsaved changes Save Cancel

Policy Assignments (1)  
Local Realm: None Dynamic Access Policy: None

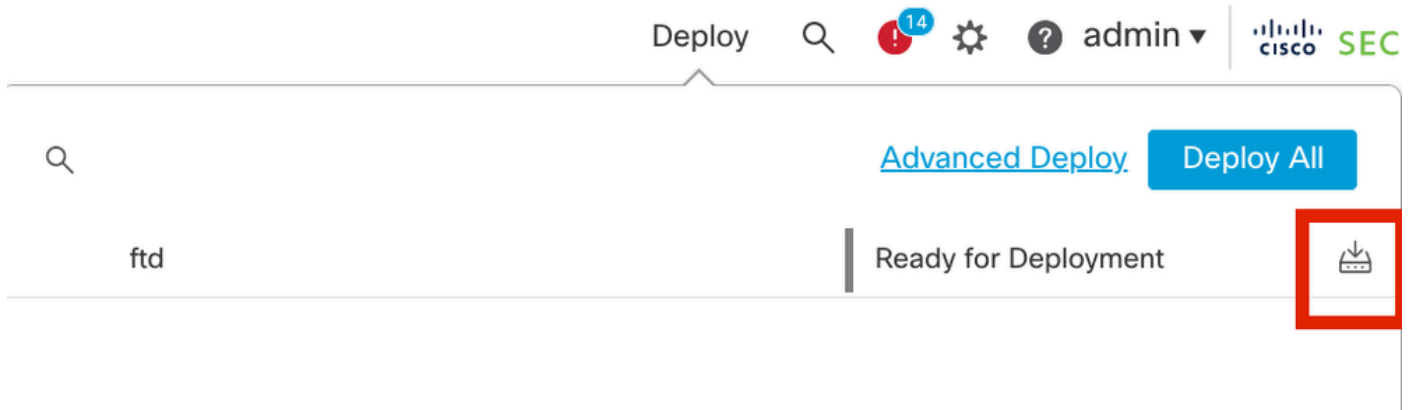
Connection Profile Access Interfaces **Advanced**

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
RAVPN-IKEV2	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: None	RAVPN-group-policy

FMC - RAPN-IKEV2 لاصتال اعجم -



20. نيوكتال رشن ب م ق .



FTD لوكوتورب رشن - FMC

7. فيري ت فلم نيوكت AnyConnect

نمض ظروفحم ،رتوي بمكل ال ع دوجوم ال فيري ت ال فلم 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://www.w3.org/2001/XMLSchema-instance">
  <HostEntry>
    <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>
  </HostEntry>
</ServerList> </AnyConnectProfile>
```



C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile . راسملا نمضي صخشلا رتوي بمكلا ىلع

3. اهبلط درجمب ةقداصم لل رورملا ةملاك و مدختسملا مسا لخدأ .

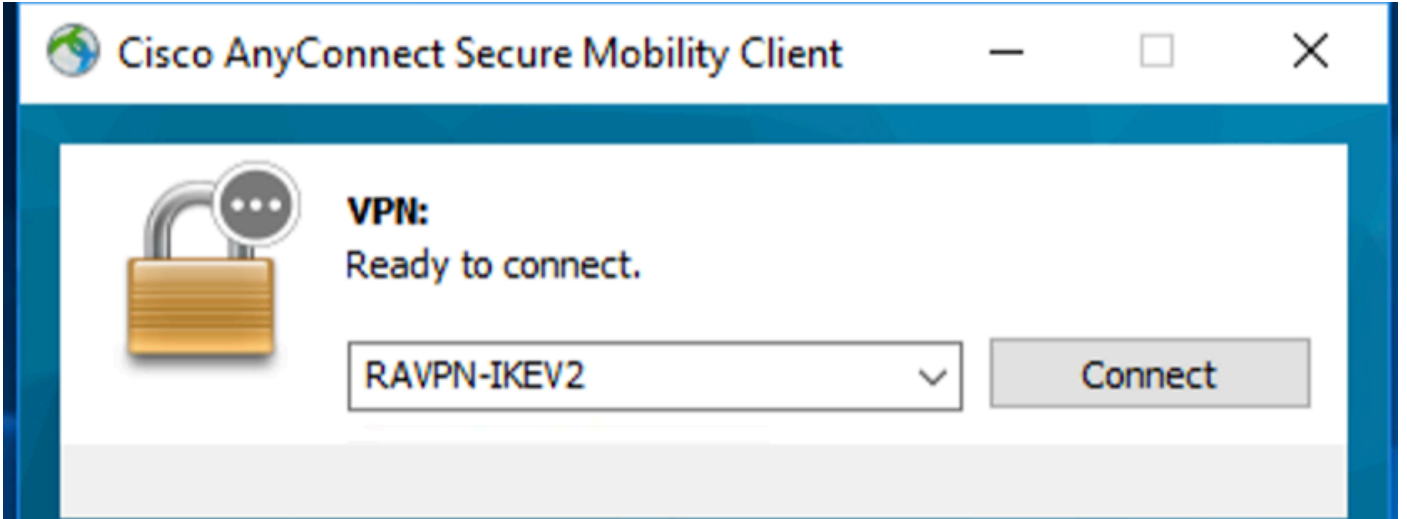
4. مدختسملا رتوي بمك زايج ىلع ليمعلا فيرعت فلم ليزنت متي ، ةحجانلا ةقداصملا دعب .

5. AnyConnect ب لاصتالا عطق .

6. ليمعلا فيرعت فلم ي ف روكذملا فيضملا مسا رايتخال ةلدسنملا ةمئاقلا مدختسأ ، فيرعتلا فلم ليزنت درجمب .

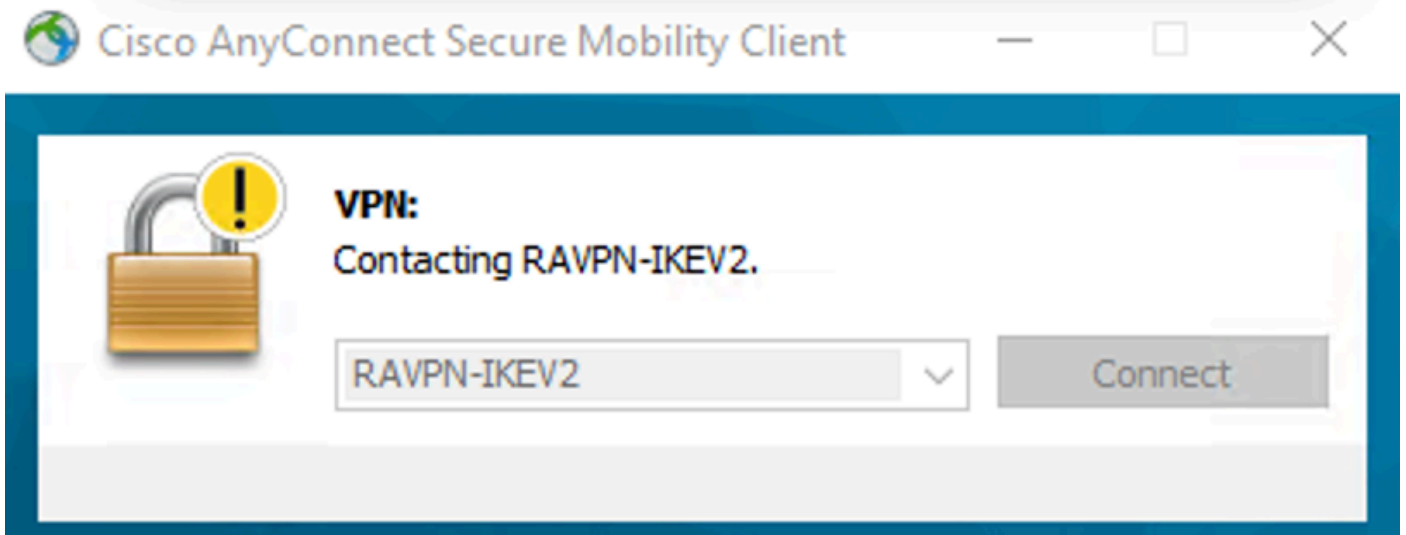
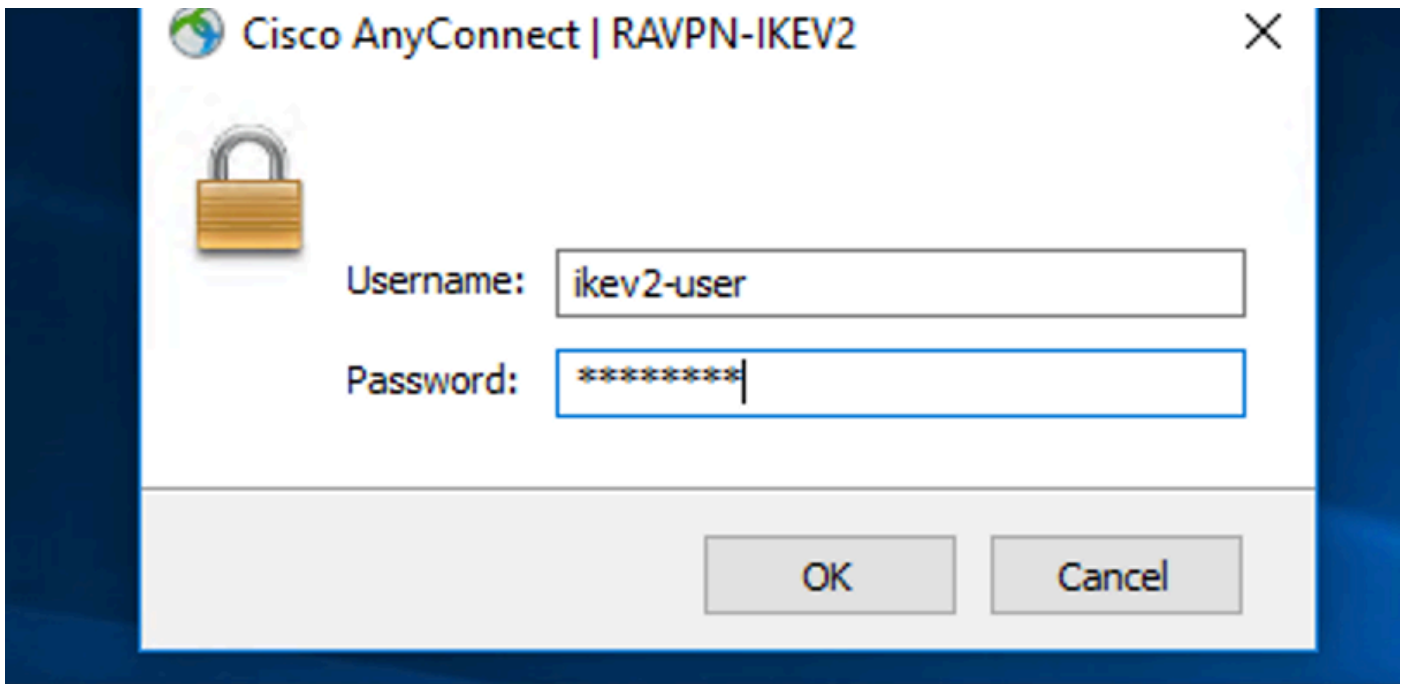
RAVPN-IKEV2 ب لاصتالا IKEv2/IPsec مادختساب AnyConnect ب لاصتالا .

7. Connect رقنا .



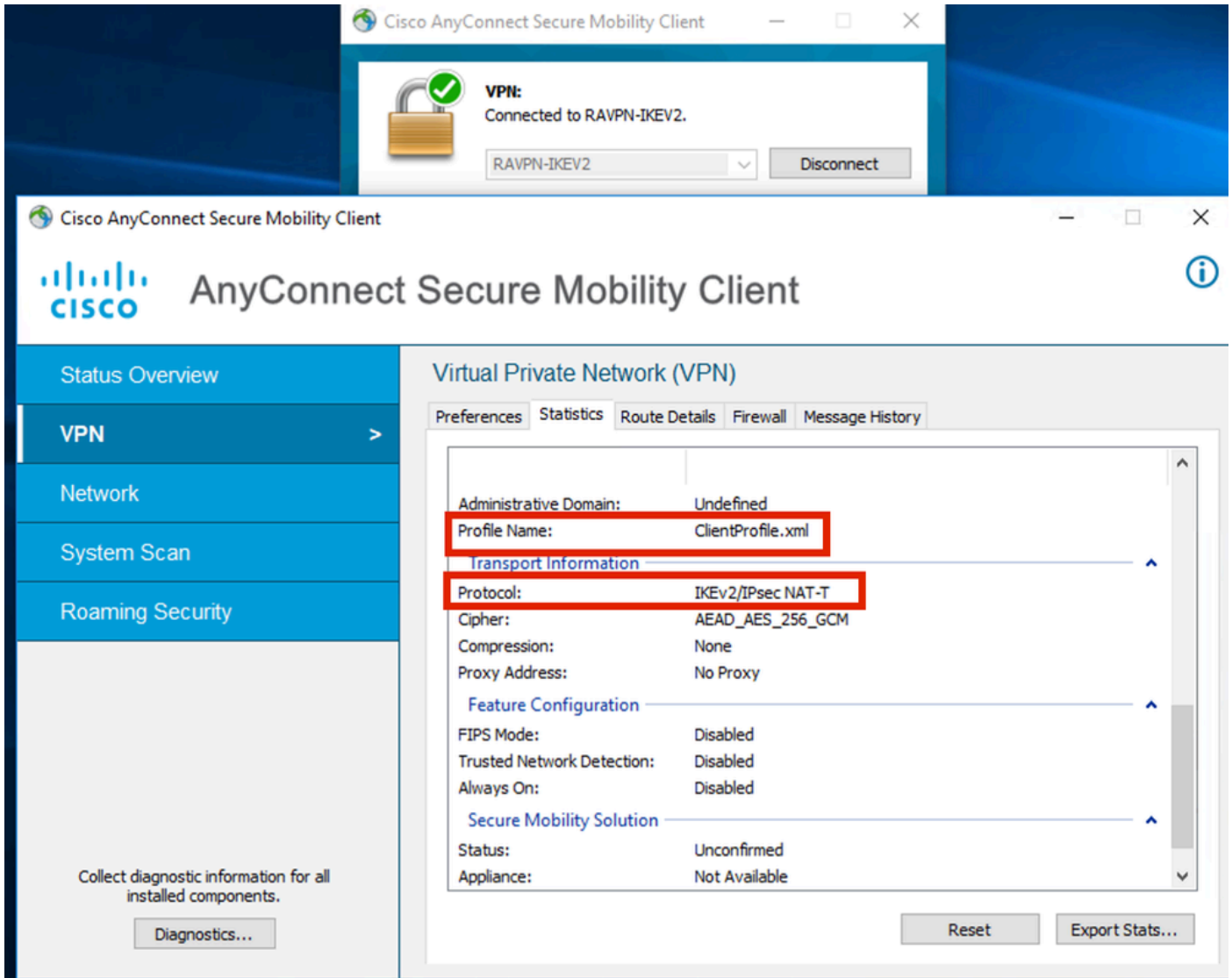
AnyConnect ةلدسنملا ةمئاقلا

8. ISE مداخ ىلع اهؤاشنإ متي تالا ةقداصم لل رورملا ةملاك و مدختسملا مسا لخدأ .



AnyConnect لاصتا

9. لاصتالال درج مې مځتسمال (IKEv2/IPsec) لوكوتوربال او فيرعتالال فلم نم ققحتالال.



لصت م AnyConnect

FTD: يف رم او ال رطس ةهجاو تاج رخم

<#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

ISE تالچس:

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	

قرش ابم ل تالچس ل - ISE

اه حال ص او عا ط خ ا ل فاش ك ت س ا

اه حال ص او ني و ك ت ل ا عا ط خ ا فاش ك ت س ا ل ا ه ا م ا د خ ت س ا ل ك ن ك م ي ت ا م و ل ع م م س ق ل ا ا ذ ه ر ف و ي

debug radius all

debug crypto ikev2 platform 255

debug crypto ikev2 protocol 255

debug crypto ipsec 255



