

ISE를 사용하여 IKEv2를 통해 FTD에 대한 Anyconnect VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1. SSL 인증서 가져오기](#)

[2. RADIUS 서버 구성](#)

[2.1. FMC에서 FTD 관리](#)

[2.2. ISE에서 FTD 관리](#)

[3. FMC에서 VPN 사용자를 위한 주소 풀 생성](#)

[4. AnyConnect 이미지 업로드](#)

[5. XML 프로필 만들기](#)

[5.1. 프로파일 편집기에서](#)

[5.2. FMC](#)

[6. 원격 액세스 구성](#)

[7. Anyconnect 프로파일 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 FMC에서 관리하는 FTD에서 IKEv2 및 ISE 인증을 사용하는 원격 액세스 VPN의 기본 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 VPN, TLS 및 IKEv2(Internet Key Exchange version 2)
- AAA(Basic Authentication, Authorization, and Accounting) 및 RADIUS
- FMC(Firepower 관리 센터) 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

IKEv2 및 SSL(Secure Sockets Layer)은 모두 보안 연결을 설정하는 데 사용되는 프로토콜이며, 특히 VPN의 컨텍스트에서 사용됩니다. IKEv2는 강력한 암호화 및 인증 방법을 제공하여 VPN 연결에 대해 높은 수준의 보안을 제공합니다.

이 문서에서는 TLS(Transport Layer Security) 및 IKEv2를 사용하기 위해 원격 액세스 VPN을 허용하는 FTD 버전 7.2.0 이상의 컨피그레이션 예를 제공합니다. 클라이언트로서 Cisco AnyConnect를 사용할 수 있으며, 이는 여러 플랫폼에서 지원됩니다.

구성

1. SSL 인증서 가져오기

인증서는 AnyConnect가 구성된 경우 필수적입니다.

수동 인증서 등록에는 제한이 있습니다.

1. FTD에서 CSR(Certificate Signing Request)이 생성되기 전에 CA(Certificate Authority) 인증서가 필요합니다.
2. 외부에서 CSR을 생성하는 경우에는 다른 PKCS12 방법을 사용합니다.

FTD 어플라이언스에서 인증서를 가져오는 몇 가지 방법이 있지만 안전하고 쉬운 방법은 CSR을 생성하고 CA에서 서명을 받는 것입니다. 그 방법은 다음과 같습니다.

1. Objects > Object Management > PKI > Cert Enrollment로 이동하여 Add Cert Enrollment클릭합니다.
2. 신뢰 지점명을 입력합니다RAVPN-SSL-cert.
3. CA Information 탭 아래에서 Enrollment Type(등록 유형)을 Manual 선택하고 이미지에 표시된 대로 CA 인증서를 붙여넣습니다.

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
Y1NjE1WhcNMjkx
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - CA 인증서

4. 아래 Certificate Parameters에 주체 이름을 입력합니다. 예를 들면 다음과 같습니다.

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 - 인증서 매개변수

5. 탭에서 Key 키 유형을 선택하고 이름 및 비트 크기를 제공합니다. RSA의 경우 2048비트가 최소입니다.

6. 을 Save 클릭합니다.

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 - 인증서 키

7. 다음으로 Devices > Certificates > Add > New Certificate 이동합니다.

8. 선택합니다Device. 에서 Cert Enrollment 생성된 신뢰 지점을 선택하고 이미지에 표시된 Add대로 를 클릭합니다.

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 - FTD에 인증서 등록

9. 을 ID 클릭하고 CSR을 생성하라는 프롬프트가 표시되면 을 선택합니다Yes.

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 - 등록된 인증서 CA

Warning

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

No

Yes

FMC - CSR 생성

10. ID 인증서를 가져오기 위해 CA와 공유할 수 있는 CSR이 생성됩니다.

11. base64 형식의 CA에서 ID 인증서를 받은 후 이미지에 표시된 대로 **Import Identity Certificate** 를 클릭하여 Import 디스크에서 선택합니다.

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 - ID 인증서 가져오기

12. 가져오기에 성공하면 신뢰 지점RAVPN-SSL-cert은 다음과 같습니다.

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

FMC - 신뢰 지점 등록 성공

2. RADIUS 서버 구성

2.1. FMC에서 FTD 관리

1. 로 Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group 이동합니다.
2. 이름을 입력하고 ISE 을 눌러 RADIUS 서버를 추가합니다+.

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 서버 컨피그레이션

3. ISE Radius 서버의 IP 주소를 ISE 서버와 동일한 공유 암호(키)와 함께 언급합니다.

4. FTD가 Routing Specific Interface ISE 서버와 통신하는 데 사용할 경로를 선택합니다.

5. 이미지Save 에 표시된 대로 클릭합니다.

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

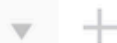
Connect using:

Routing Specific Interface 

outside



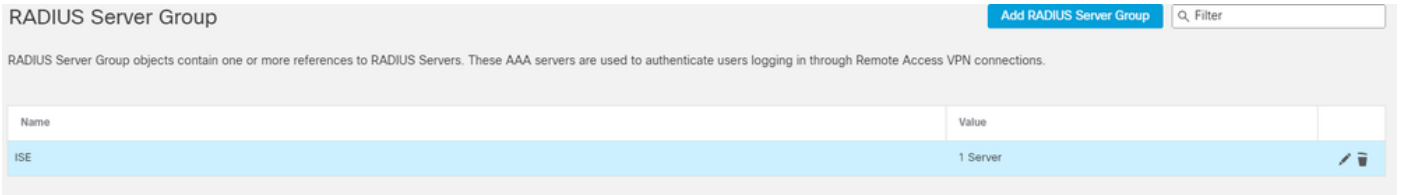
Redirect ACL:



Cancel

Save

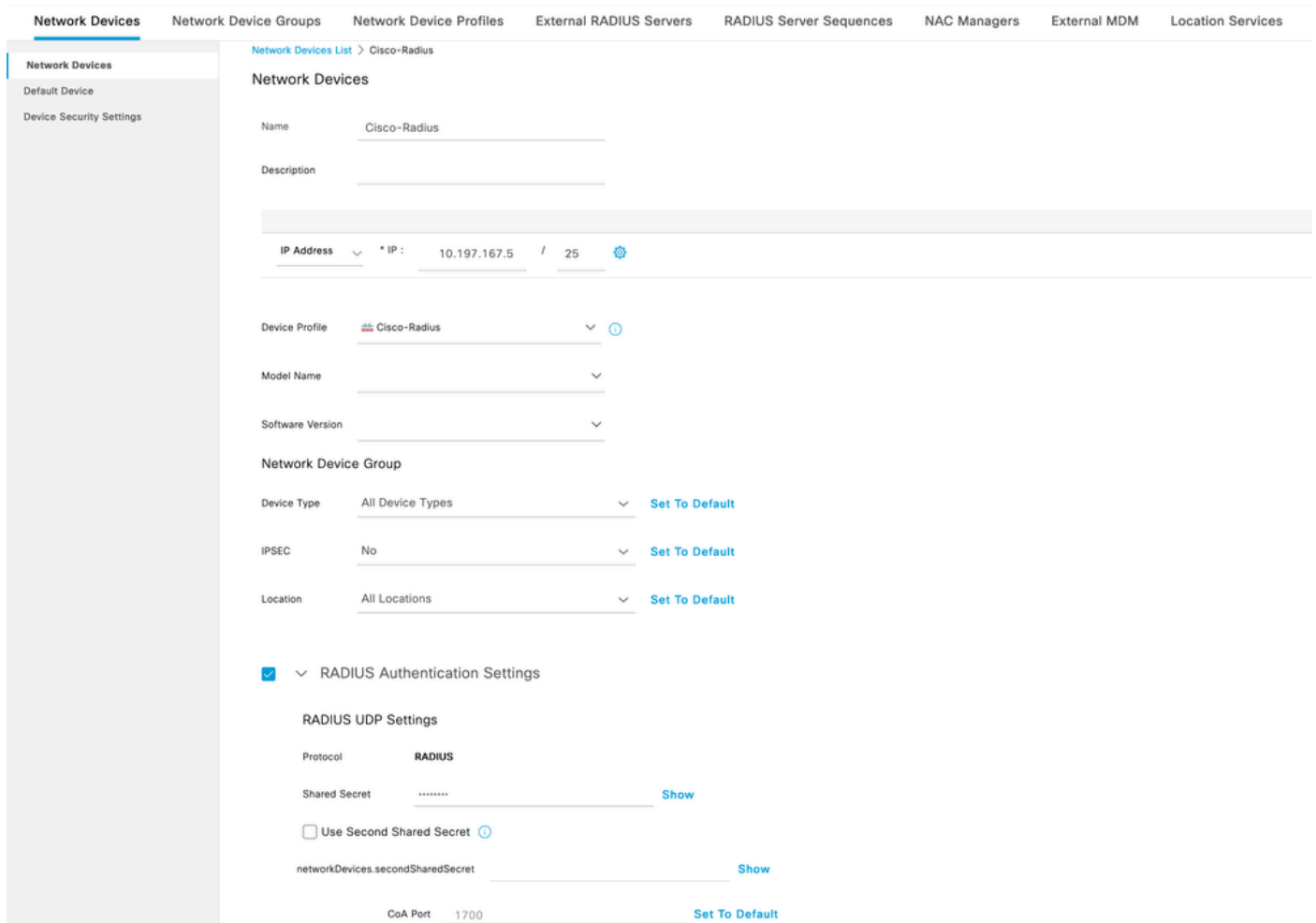
6. 저장하면 이미지가 표시된 RADIUS Server Group 것처럼 서버가 아래에 추가됩니다.



FMC - RADIUS 서버 그룹

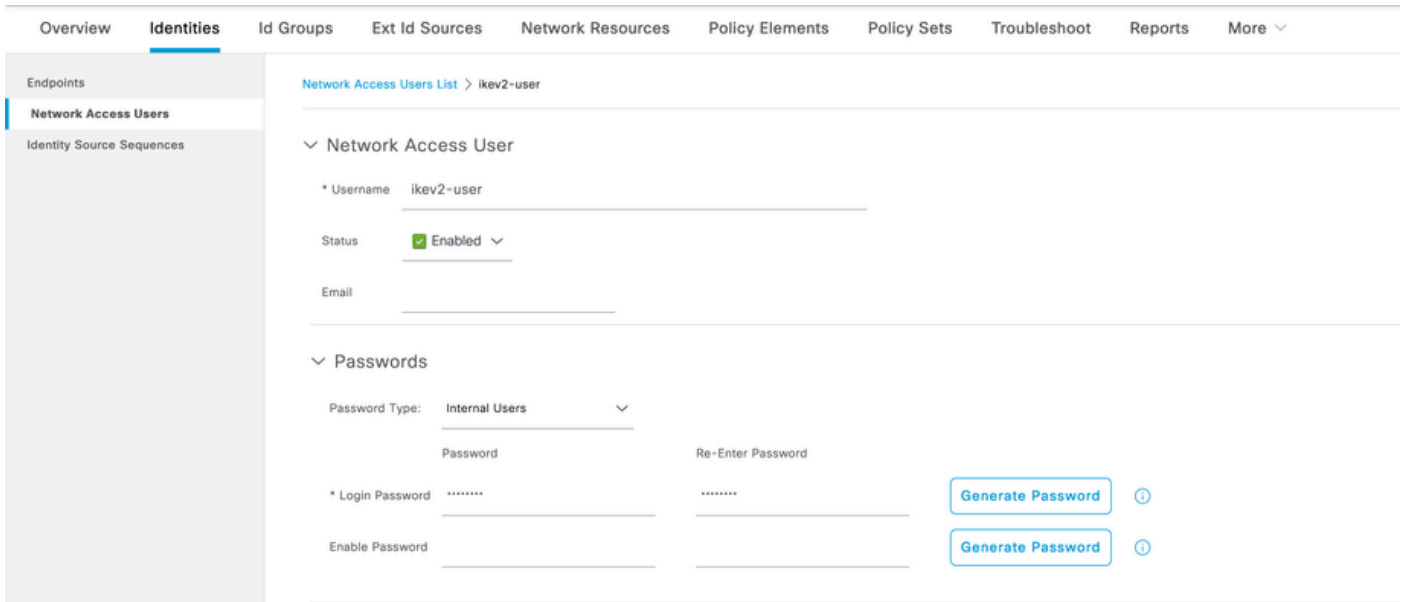
2.2. ISE에서 FTD 관리

1. Network Devices 로 이동하여 을 클릭합니다Add.
2. 서버 및 FTD 통신 인터페이스인 radius 클라이언트IP Address의 이름 'Cisco-Radius'를 입력합니다.
3. 아래Radius Authentication Settings에 를 추가합니다Shared Secret.
4. 을 클릭합니다Save.



ISE - 네트워크 디바이스

5. 사용자를 생성하려면 로 이동하여 Network Access > Identities > Network Access Users 을 클릭합니다 Add.
6. 필요에 따라 사용자 이름 및 로그인 비밀번호를 생성합니다.



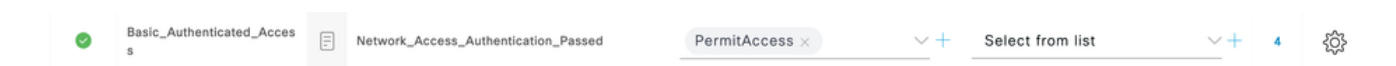
ISE - 사용자

7. 기본 정책을 설정하려면 로 이동하여 Policy > Policy Sets > Default > Authentication Policy > Default 선택합니다 All_User_ID_Stores.

8. 이미지에 표시된 대로 Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, 이동하여 PermitAccess 선택합니다.



ISE - 인증 정책



ISE - 권한 부여 정책

3. FMC에서 VPN 사용자를 위한 주소 풀 생성

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

2. 이름 및 주소 RAVPN-Pool 범위를 입력합니다. 마스크는 선택사항입니다.

3. 저장을 클릭합니다.

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 - 주소 풀

4. AnyConnect 이미지 업로드

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

2. 이름을 anyconnect-win-4.10.07073-webdeploy 입력하고 Browse 을 클릭하여 디스크에서 **Anyconnect** 파일을 선택하고 Save 그림과 같이 클릭합니다.

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC - Anyconnect 클라이언트 이미지

5. XML 프로필 만들기

5.1. 프로파일 편집기에서

1. 프로파일 편집기를 software.cisco.com에서 다운로드하여 엽니다.
2. 다음으로 **Server List > Add** 이동합니다.
3. 표시 이름 RAVPN-IKEV2과 FQDN 사용자 그룹(별칭 이름)을 입력합니다.
4. 이미지에 표시된 IPsec, 것처럼 클릭할 때 기본 프로토콜 **Ok** 을 선택합니다.

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)

프로파일 편집기 - 서버 목록

5. 서버 목록이 추가됩니다. 다른 이름으로 ClientProfile.xml 저장합니다.

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

프로파일 편집기 - ClientProfile.xml

5.2. FMC

- 로 Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File 이동합니다.
- 이름을 ClientProfile 입력하고 Browse 을 클릭하여 디스크에서 파일을 ClientProfile.xml 선택합니다.
- Save 클릭합니다.

Edit AnyConnect File



Name:*

File Name:*

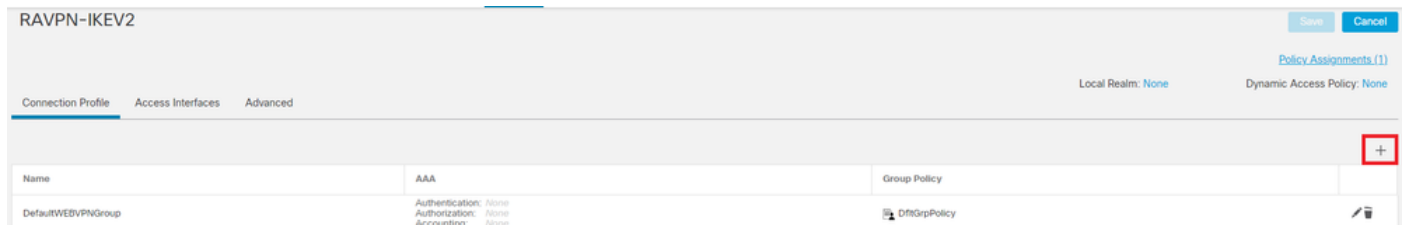
File Type:*

Description:

FMC - Anyconnect VPN 프로파일

6. 원격 액세스 구성

1. 이미지에 표시된 대로 Devices > VPN > Remote Access 연결 프로파일을 추가하려면 로 이동하여 클릭하십시오+.



FMC - 원격 액세스 연결 프로파일

2. 연결 프로파일 이름을 RAVPN-IKEV2 입력하고 이미지에 표시된 대로 +로그인을 **Group Policy**클릭하여 그룹 정책을 생성합니다.

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 - 그룹 정책

3. 이름을 RAVPN-group-policy 입력하고 이미지에 표시된 **SSL and IPsec-IKEv2** 대로 VPN 프로토콜을 선택합니다.

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 프로토콜

4. 아래의 AnyConnect > Profile 드롭다운에서 XML 프로파일ClientProfile을 선택하고 이미지Save에 표시된 대로 클릭합니다.

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 프로파일

5. 클릭하여 주소 풀RAVPN-Pool을 추가합니다+ 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 - 클라이언트 주소 할당

6. 탐색AAA > Authentication Method 후 선택합니다AAA Only.

7. 다음으로Authentication Server 선택합니다ISE (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 - AAA 인증

8. Aliases 에서 사용자 그룹으로 사용되RAVPN-IKEV2는 별칭 이름을 입력합니다ClientProfile.xml.

9. 을 Save 클릭합니다.

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 - 별칭

10. RAVPN IKEvAccess Interfaces2를 활성화해야 하는 인터페이스로 이동하여 선택합니다.

11. SSL 및 IKEv2 모두에 대한 ID 인증서를 선택합니다.

12. 을 Save 클릭합니다.

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 - 액세스 인터페이스

13. 다음으로 Advanced 이동합니다.

14. 를 클릭하여 Anyconnect 클라이언트 이미지를 추가합니다+.

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 클라이언트 패키지

15. 아래에 IPsec 이미지에 Crypto Maps 표시된 대로 를 추가합니다.

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 - 암호화 맵

16. 아래에서 IPsec 를 클릭하여 IKE Policy 를 추가합니다+.

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 정책

17. 아래IPsec 에 를 IPsec/IKEv2 Parameters 추가합니다.

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:

Enable Notification on Tunnel Disconnect

Do not allow device reboot until all sessions are terminated

IKEv2 Security Association (SA) Settings

Cookie Challenge:

Threshold to Challenge Incoming Cookies: %

Number of SAs Allowed in Negotiation: %

Maximum number of SAs Allowed:

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: Seconds (Range 10 - 3600)

FMC - IPsec/IKEv2 매개변수

18. 아래Connection Profile에 새 프로파일RAVPN-IKEV2이 생성됩니다.

19. Save이미지에 표시된 대로 클릭합니다.

RAVPN-IKEV2 You have unsaved changes Save Cancel

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

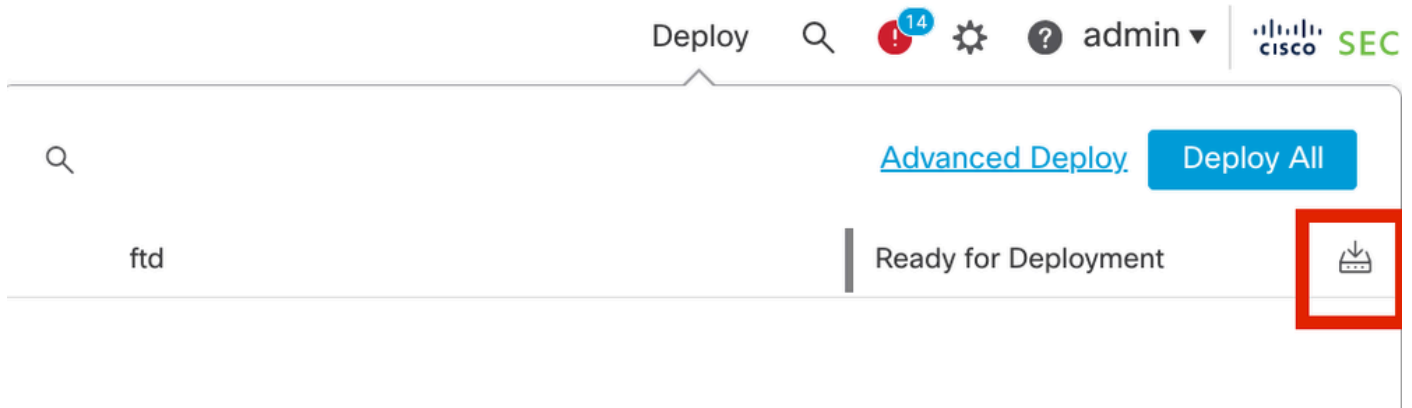
Connection Profile Access Interfaces **Advanced**

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 -

연결 프로파일 RAVPN-IKEV2

20. 구성을 배포합니다.



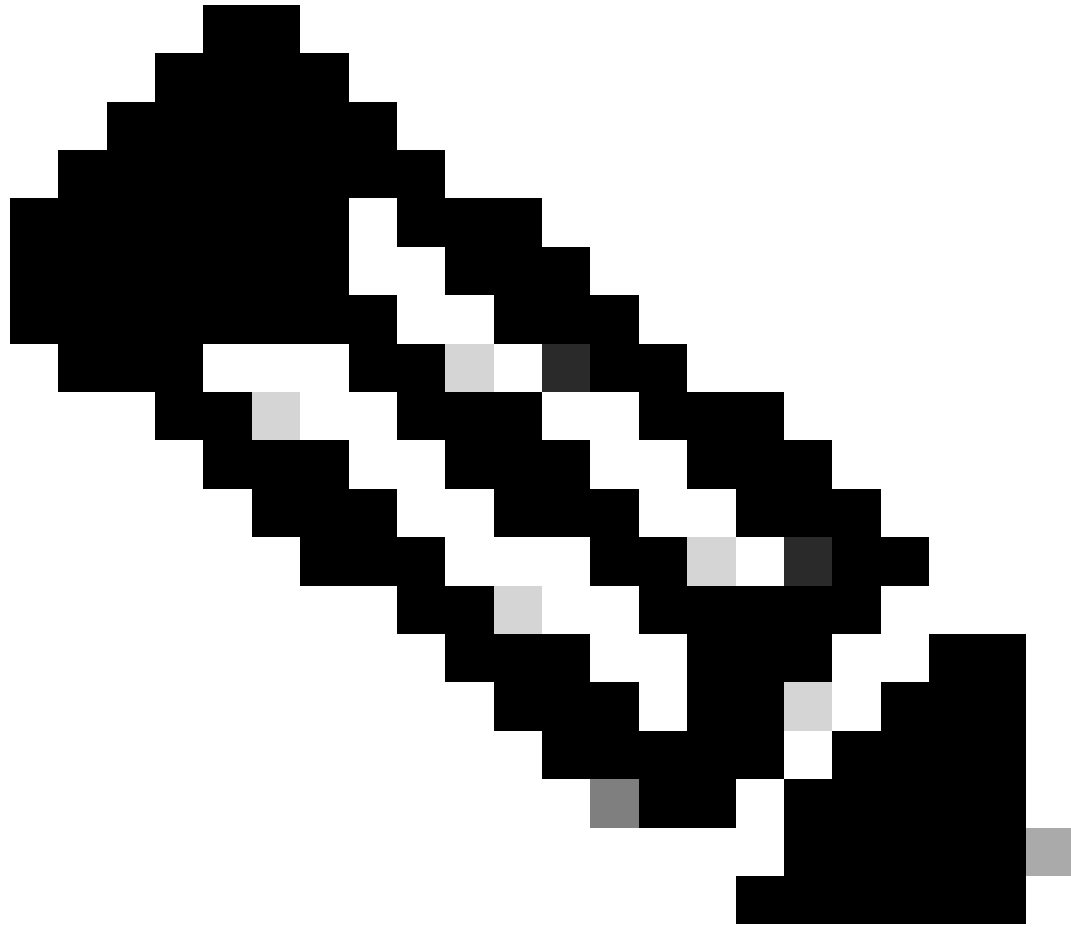
FMC - FTD 구축

7. Anyconnect 프로파일 컨피그레이션

PC의 프로파일, 아래에 저장 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">
  <HostEntry>
    <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>
  </HostEntry> </ServerList> </AnyConnectProfile>
```



참고: 모든 사용자의 PC에 클라이언트 프로파일을 다운로드한 후에는 그룹 정책에서 SSL 클라이언트를 터널링 프로토콜로 비활성화하는 것이 좋습니다. 이렇게 하면 사용자가 IKEv2/IPsec 터널링 프로토콜을 사용하여 독점적으로 연결할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인할 수 있습니다.

1. 첫 번째 연결의 경우 FQDN/IP를 사용하여 Anyconnect를 통해 사용자의 PC에서 SSL 연결을 설정합니다.
2. SSL 프로토콜이 비활성화되어 있고 이전 단계를 수행할 수 없는 경우, 클라이언트 프로파일이 ClientProfile.xml PC의 경로 아래에 있는지 C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile 확인합니다.
- 3.

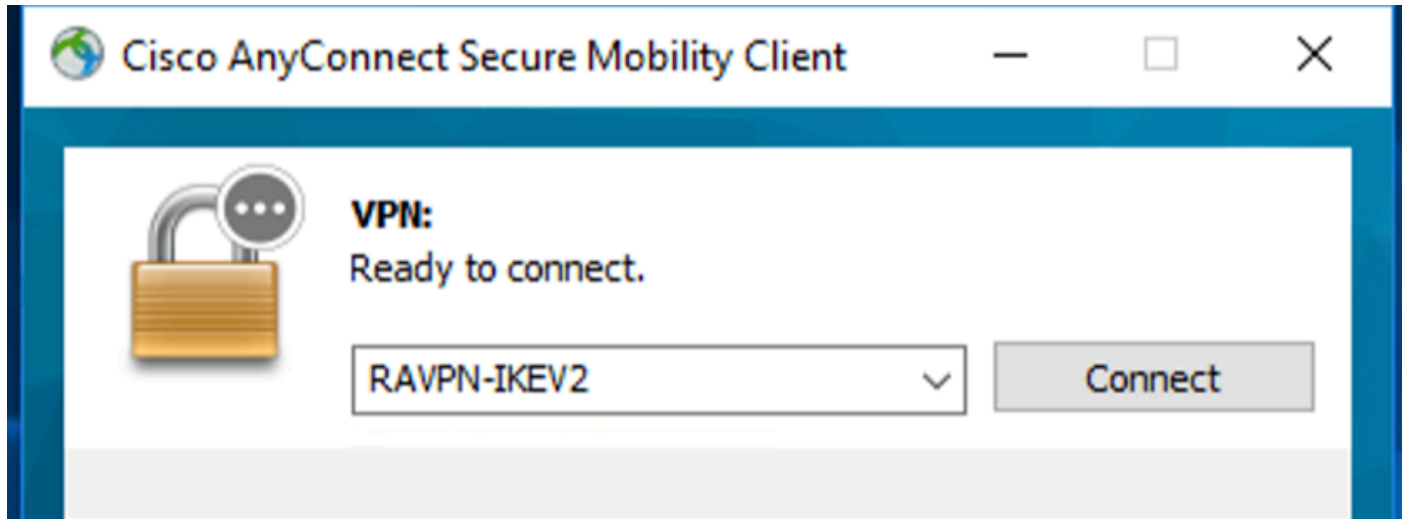
프롬프트가 표시되면 인증을 위한 사용자 이름 및 비밀번호를 입력합니다.

4. 인증에 성공하면 사용자의 PC에 클라이언트 프로파일이 다운로드됩니다.

5. Anyconnect에서 연결을 끊습니다.

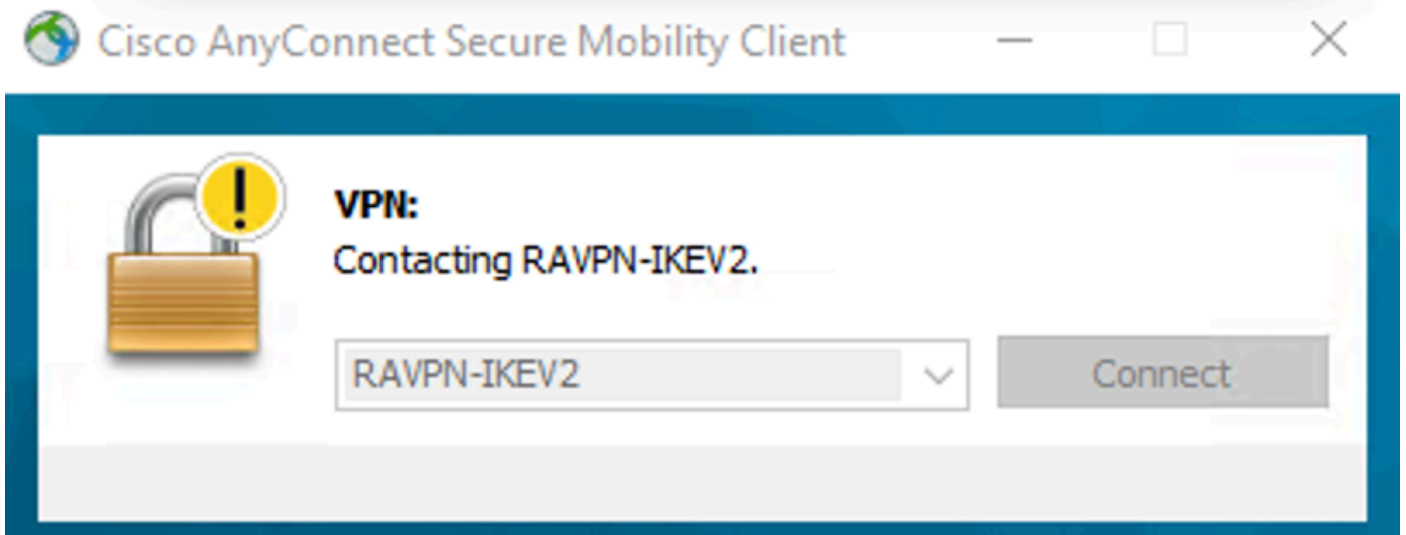
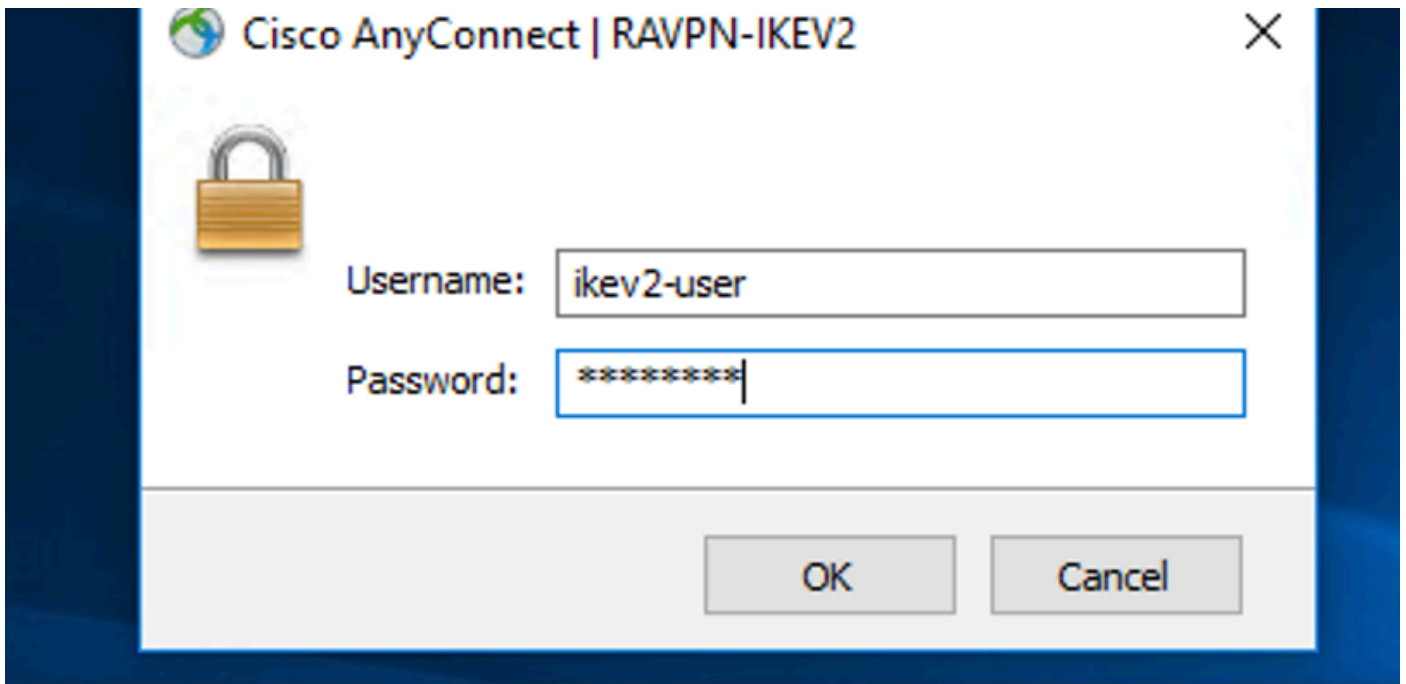
6. 프로파일이 다운로드되면 IKEv2/IPsec을 사용하여 Anyconnect에 연결하기 **RAVPN-IKEV2** 위해 클라이언트 프로파일에 언급된 호스트 이름을 선택하려면 드롭다운을 사용합니다.

7. 을 Connect 클릭합니다.



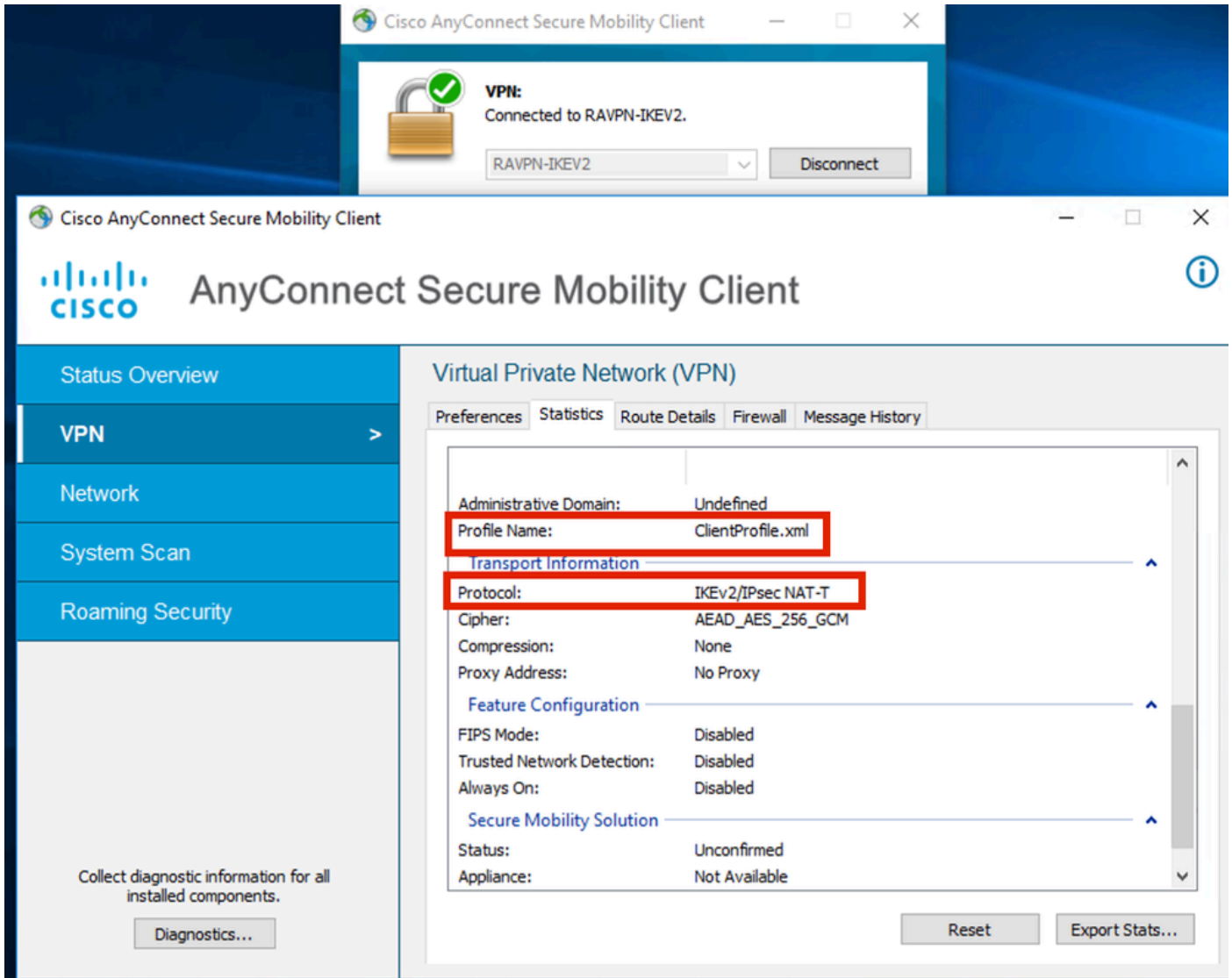
Anyconnect 드롭다운

8. ISE 서버에서 생성한 인증의 사용자 이름과 비밀번호를 입력합니다.



Anyconnect 연결

9. 연결된 후에 사용된 프로파일 및 프로토콜(IKEv2/IPsec)을 확인합니다.



Anyconnect 연결됨

FTD CLI 출력:

```
<#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 로그:

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	00:50:56:8D: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	

ISE - 라이브 로그

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

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


이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.