

ISEでのIKEv2によるFTDへのAnyConnect VPNの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[1. SSL証明書のインポート](#)

[2. RADIUSサーバの設定](#)

[2.1. FMCでのFTDの管理](#)

[2.2. ISEでのFTDの管理](#)

[3. FMC上のVPNユーザ用のアドレスプールの作成](#)

[4. AnyConnectイメージのアップロード](#)

[5. XMLプロファイルの作成](#)

[5.1. プロファイルエディタ](#)

[5.2. FMC上](#)

[6. リモートアクセスの設定](#)

[7. Anyconnectプロファイルの設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、FMCによって管理されるFTDでのIKEv2およびISE認証を使用したリモートアクセスVPN(RVPN)の基本設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なVPN、TLS、およびインターネットキーエクスチェンジバージョン2(IKEv2)
- 基本認証、許可、アカウンティング(AAA)およびRADIUS
- Firepower Management Center(FMC)の使用経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IKEv2とSecure Sockets Layer(SSL)はどちらも、特にVPNのコンテキストでセキュアな接続を確立するために使用されるプロトコルです。IKEv2は、強力な暗号化方式と認証方式を提供し、VPN接続に高レベルのセキュリティを提供します。

このドキュメントでは、Transport Layer Security(TLS)とIKEv2を使用するためにリモートアクセスVPNを可能にするFTDバージョン7.2.0以降の設定例を示します。Cisco AnyConnectはクライアントとして使用でき、複数のプラットフォームでサポートされています。

設定

1. SSL証明書のインポート

証明書は、AnyConnectが設定されている場合に不可欠です。

証明書の手動登録には制限があります。

1. FTDでは、証明書署名要求(CSR)を生成する前に認証局(CA)証明書が必要です。
2. CSRが外部で生成される場合、PKCS12の別の方法が使用されます。

FTDアプライアンスで証明書を取得する方法はいくつかありますが、安全で簡単な方法は、CSRを作成し、CAによって署名してもらうことです。その方法を次に示します。

1. Objects > Object Management > PKI > Cert Enrollmentに移動し、Add Cert Enrollmentをクリックします。
2. トラストポイント名RAVPN-SSL-certを入力します。
3. CA Informationタブで、登録タイプとしてManualを選択し、図に示すようにCA証明書を貼り付けます。

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証明書

4. 「Certificate Parameters」で、サブジェクト名を入力します。例：

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 (証明書パラメータ)

5. Key タブで、キー・タイプを選択し、名前とビット・サイズを指定します。RSAでは、2048ビットが最小です。

6. Saveをクリックします。

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 (証明書キー)

7. Devices > Certificates > Add > New Certificateに移動します。

8. Deviceを選択します。Cert Enrollmentで、作成したトラストポイントを選択し、図に示すようAddをクリックします。

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:FTDへの証明書の登録

9. 「ID」をクリックし、CSRを生成するためのプロンプトが表示されたら、「Yes」を選択します。

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:Certificate CA Enrolled (証明書CA登録済み)

Warning

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

No

Yes

FMC:CSRの生成

10. CSRが生成されます。CSRは、ID証明書を取得するためにCAと共有できます。

11. Base64形式のCAからID証明書を受信したら、図のようにBrowse Identity CertificateおよびImportをクリックしてディスクから選択します。

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:ID証明書のインポート

12. インポートが成功すると、トラストポイントは次のように表示されRAVPN-SSL-certです。

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

FMC:Trustpoint Enrollment Successful (トラストポイント登録成功)

2. RADIUSサーバの設定

2.1. FMCでのFTDの管理

1. Objects > Object Management > RADIUS Server Group > Add RADIUS Server Groupに移動します。

2. 名前を入力しISE、「+」をクリックしてRADIUSサーバーを追加します。

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サーバの設定

3. ISE RadiusサーバのIPアドレスを、ISEサーバと同じ共有秘密 (キー) とともに指定します。

4. FTDがISEサーバと通信するために使用するRouting またはSpecific Interfaceのいずれかを選択します。

5.図に示すよSave うにクリックします。

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

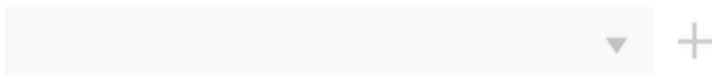
Connect using:

Routing Specific Interface 

outside



Redirect ACL:



Cancel

Save

6. 保存されたサーバは、図に示すようにRADIUS Server Group の下に追加されます。

Name	Value
ISE	1 Server

FMG:RADIUS Server Group (RADIUSサーバグループ)

2.2. ISEでのFTDの管理

1. Network Devices に移動し、Addをクリックします。

2. サーバの「Cisco-Radius」名と、FTD通信インターフェイスであるRADIUSクライアントIP Addressの「Cisco-Radius」名を入力します。

3. Radius Authentication Settingsで、Shared Secretを追加します。

4. 「Save」をクリックします。

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 [Show](#)

CoA Port [Set To Default](#)

ISE:Network Devices (ネットワークデバイス)

5. ユーザを作成するには、Network Access > Identities > Network Access Usersに移動して、をクリックし Addます。

6. 必要に応じて、UsernameandLoginパスワードを作成します。

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 – ユーザ

7. 基本ポリシーを設定するために、Policy > Policy Sets > Default > Authentication Policy > Defaultに移動し、All_User_ID_Storesを選択します。

8. 図に示すように、Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, に移動しPermitAccessで選択します。

Default

All_User_ID_Stores

> Options

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess x

Select from list

ISE:Authentication Policy (認証ポリシー)

ISE:Authorization Policy (認可ポリシー)

3. FMC上のVPNユーザ用のアドレスプールの作成

1. Objects > Object Management > Address Pools > Add IPv4 Poolsに移動します。
2. 名前RAVPN-Poolとアドレス範囲を入力します。マスクはオプションです。
3. Saveをクリックします。

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 (アドレスプール)

4. AnyConnectイメージのアップロード

1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileに移動します。

2. 名前を入力しanyconnect-win-4.10.07073-webdeployをクリックして、ディスクBrowse からAnyconnectファイルを選択し、図に示すようにクリックSave します。

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC: Anyconnectクライアントイメージ

5. XMLプロファイルの作成

5.1. プロファイルエディタ

1. プロファイルエディタをsoftware.cisco.comからダウンロードして開きます。
2. **Server List > Add...**に移動します。
3. 表示名RAVPN-IKEV2FQDN および**ユーザー・グループ** (別名) を入力します。
4. 図に示すように、プライマリ・プロトコル IPsec , asclick**Ok** を選択します。

Server List Entry

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)

プロファイルエディタ – サーバリスト

5. サーバリストが追加されます。ClientProfile.xmlとして保存します。

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

プロファイルエディタ – ClientProfile.xml

5.2. FMC上

1. Objects > Object Management > VPN > AnyConnect File > Add AnyConnect Fileに移動します。
2. 名前を入力ClientProfileし、をクリックBrowseして、ディスクからファイルを選択ClientProfile.xmlします。
3. 「Save」をクリックします。

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC:Anyconnect VPNプロファイル

6. リモートアクセスの設定

1. 図に示すように、接続プロファイルを追加するために、Devices > VPN > Remote Accessに移動し、+をクリックします。

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

FMC:Remote Access Connection Profile (リモートアクセス接続プロファイル)

2. 接続プロファイル名を入力RAVPN-IKEV2し、図に示すように+Group Policyをクリックしてグループポリシーを作成します。

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 (グループポリシー)

3. 名前を入力しRAVPN-group-policy、図に示すようにVPNプロトコル SSL and IPsec-IKEv2 を選択します。

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プロトコル

4.AnyConnect > Profileの下で、ドロップダウンからXMLプロファイルClientProfileを選択し、図に示すよSaveうにクリックします。

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プロファイル

5. 「+ as shown in the image」をクリックしてアドレス・プールRAVPN-Poolを追加します。

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 (クライアントアドレス割り当て)

6. AAA > Authentication Methodに移動し、AAA Onlyを選択します。

7. Authentication ServerISE (RADIUS) として選択します。

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認証

8. Aliases に移動し、エイリアス名を入力します。RAVPN-IKEV2は、ClientProfile.xmlでユーザグループとして使用されます。

9. Saveをクリックします。

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 : エイリアス

10. Access Interfacesに移動し、RAVPN IKEv2を有効にする必要があるインターフェイスを選択します。
11. SSLとIKEv2の両方のID証明書を選択します。
12. Saveをクリックします。

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 : アクセスインターフェイス

13. Advanced に移動します。

14. +をクリックして、Anyconnectクライアントイメージを追加します。

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: +

FMC: Anyconnectクライアントパッケージ

15. の下にIPsec、図に示すようにCrypto Maps、を追加します。

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

FMC : 暗号マップ

16. 「IPsec」で、「+」をクリックしIKE Policy を追加します。

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ポリシー

17. IPsec で、IPsec/IKEv2 Parametersを追加します。

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パラメータ

18. Connection Profileの下に、新しいプロファイルRAVPN-IKEV2が作成されます。

19.図に示すようにクSaveリックします。

RAVPN-IKEV2 You have unsaved changes Save Cancel

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

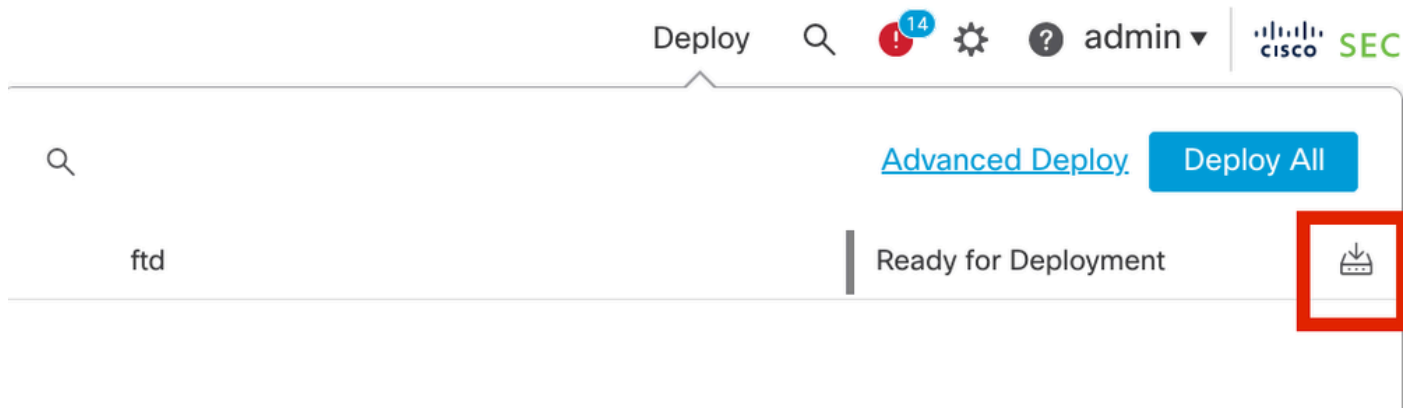
Connection Profile Access Interfaces **Advanced**

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

: 接続プロファイルRAVPN-IKEV2

20. 設定を展開します。



FMC:FTDの導入

7. Anyconnectプロファイルの設定

PC上のプロファイル (以下に保存) 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>
```



注：クライアントプロファイルがすべてのユーザのPCにダウンロードされたら、グループポリシーでトンネリングプロトコルとしてSSLクライアントをディセーブルにすることを推奨します。これにより、ユーザはIKEv2/IPsecトンネリングプロトコルを使用して排他的に接続できます。

確認

このセクションを使用して、設定が正しく動作していることを確認できます。

1. 最初の接続では、FQDN/IPを使用して、ユーザのPCからAnyConnect経由でSSL接続を確立します。
2. SSLプロトコルが無効で、前の手順を実行できない場合、クライアントプロファイルClientProfile.xmlがパスの下のPC上に存在することを確認します(PCがSSLプロトコルを使用していない場合は、SSLプロトコルを使用しますC:\ProgramData\Cisco\Cisco

Anyconnect Secure Mobility Client(Profile)。

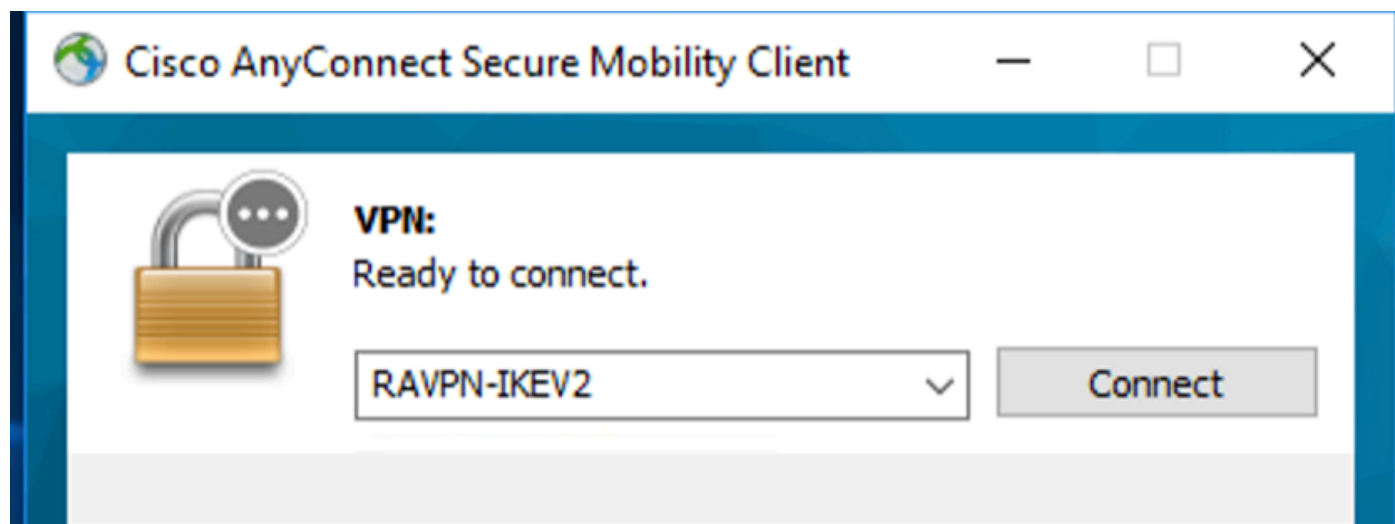
3. プロンプトが表示されたら、認証用のユーザ名とパスワードを入力します。

4. 認証に成功すると、クライアントプロファイルがユーザのPCにダウンロードされます。

5. Anyconnectを切断します。

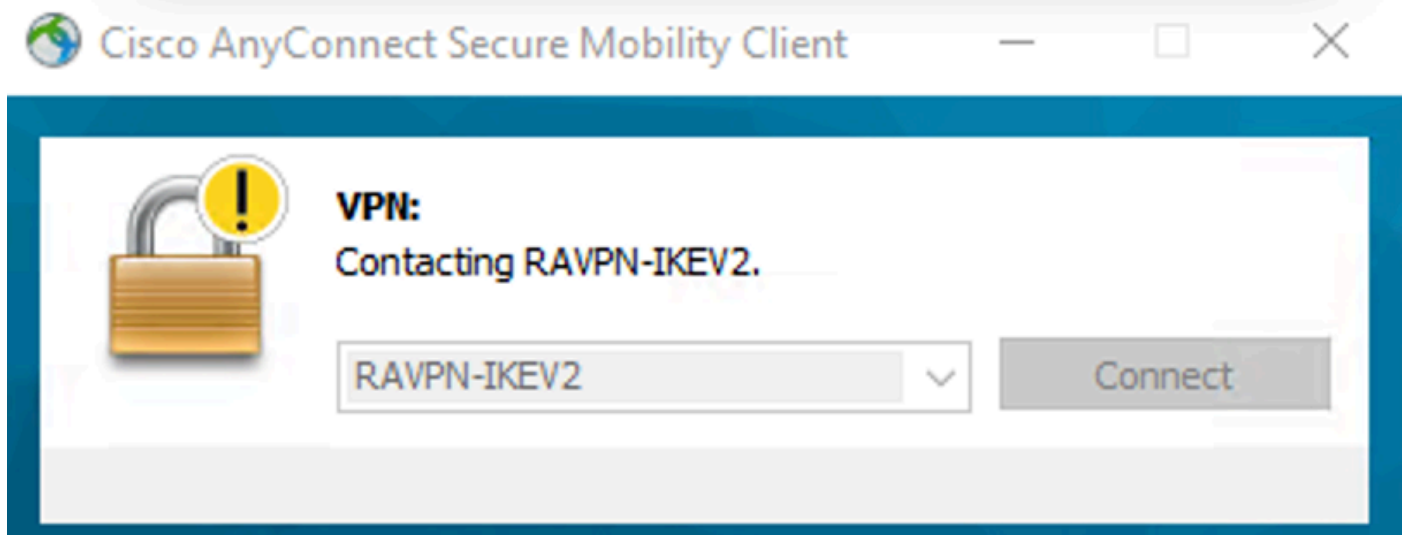
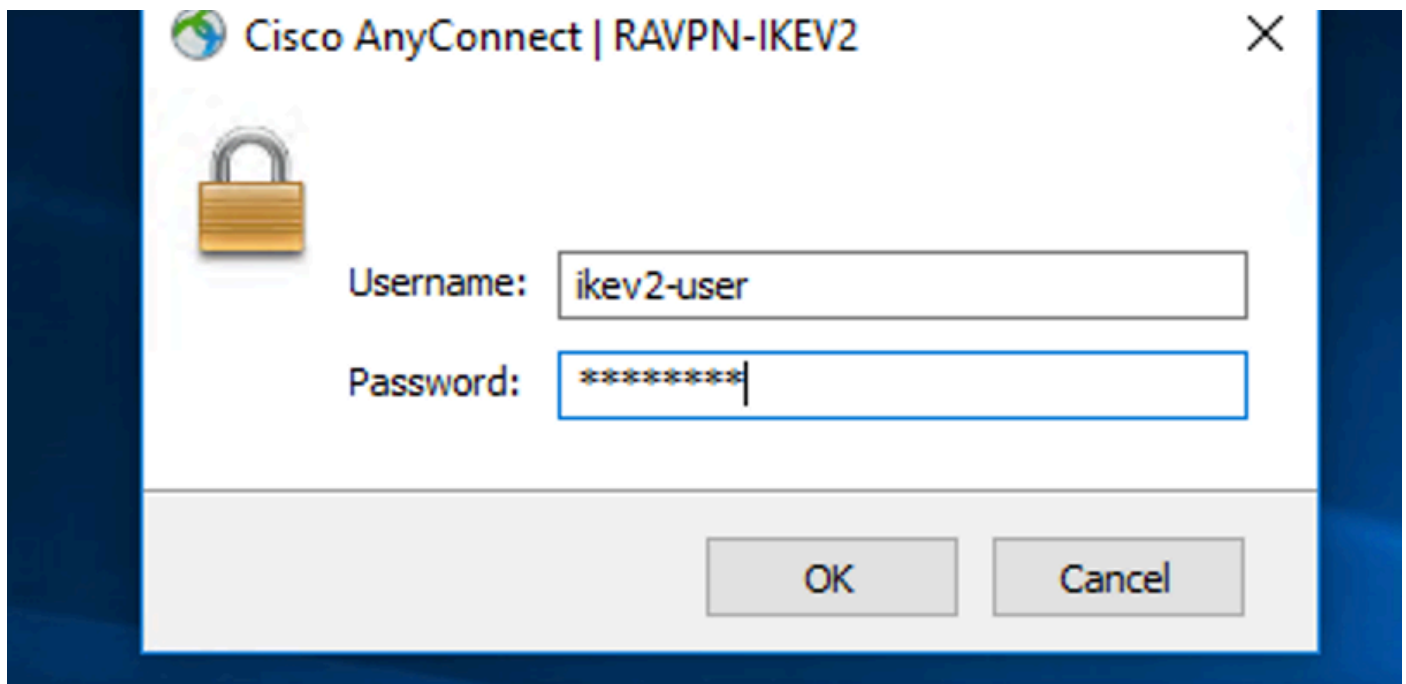
6. プロファイルをダウンロードしたら、IKEv2/IPsecを使用してAnyconnectに接続するために、クライアントプロファイル**RAVPN-IKEV2** に示されているホスト名をドロップダウンから選択します。

7. Connectをクリックします。



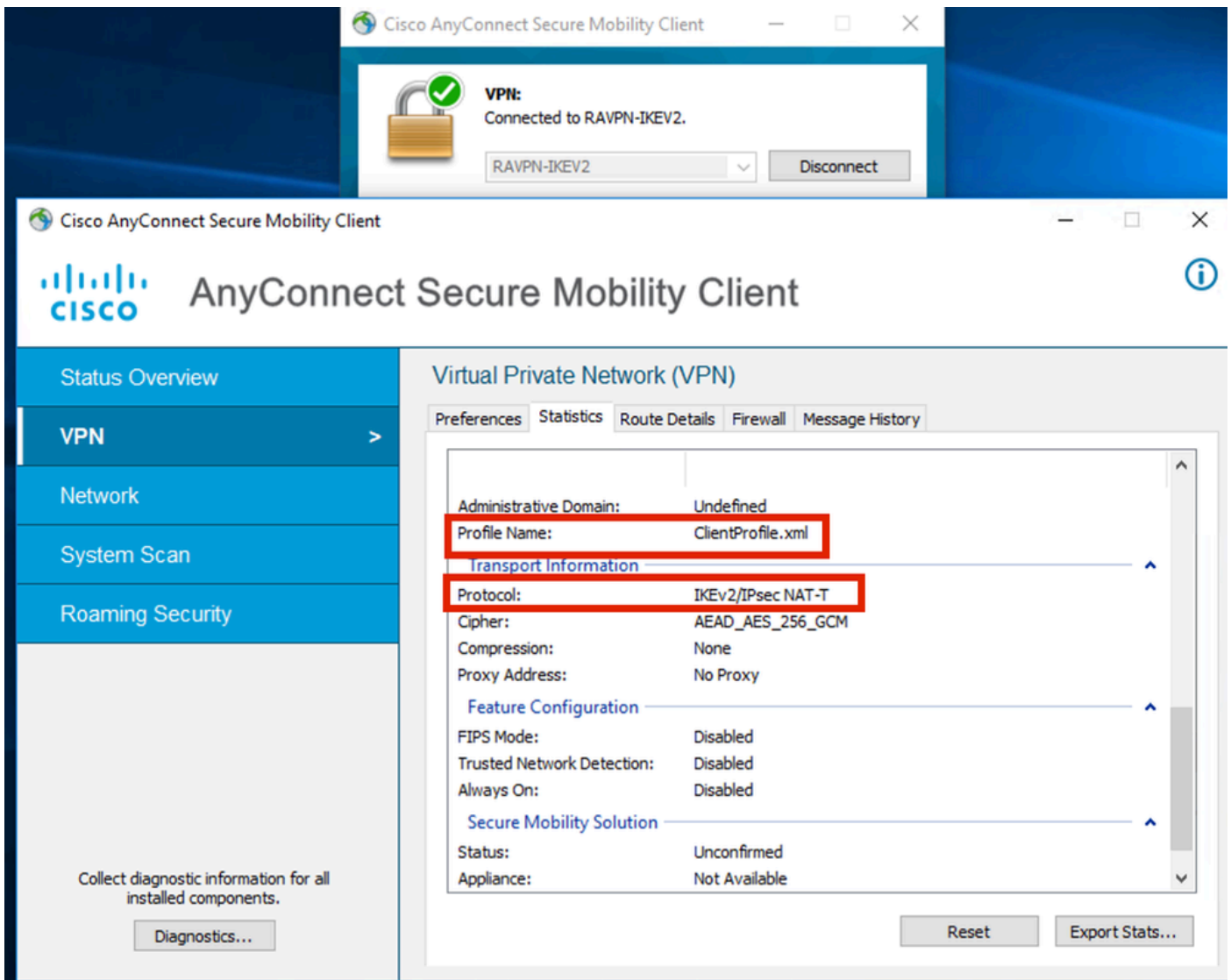
Anyconnectドロップダウン

8. ISEサーバ上で作成された認証用のユーザ名とパスワードを入力します。



Anyconnect接続

9. 接続後に使用するプロファイルとプロトコル(IKEv2/IPsec)を確認します。



Anyconnect接続

FTD CLI出力 :

<#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ログ :

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 : ライブログ

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

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


翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。