

透過IKEv2使用ISE配置Anyconnect VPN到FTD

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[1. 導入SSL證書](#)

[2. 配置RADIUS伺服器](#)

[2.1. 在FMC上管理FTD](#)

[2.2. 在ISE上管理FTD](#)

[3. 為FMC上的VPN使用者建立地址池](#)

[4. 上傳AnyConnect映像](#)

[5. 建立XML設定檔](#)

[5.1. 在設定檔編輯器上](#)

[5.2. 在FMC上](#)

[6. 配置遠端訪問](#)

[7. Anyconnect配置檔案配置](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹在FMC管理的FTD上使用IKEv2和ISE驗證的遠端存取VPN的基本組態。

必要條件

需求

思科建議您瞭解以下主題：

- 基本VPN、TLS和Internet金鑰交換版本2 (IKEv2)
- 基本驗證、授權及記帳(AAA)和RADIUS
- 體驗Firepower管理中心(FMC)

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Firepower威脅防禦(FTD) 7.2.0
- Cisco FMC 7.2.0

- AnyConnect 4.10.07073
- 思科ISE 3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IKEv2和安全套接字層(SSL)都是用於建立安全連線的協定，特別是在VPN環境中。IKEv2提供強大的加密和身份驗證方法，為VPN連線提供高級別的安全性。

本檔案提供FTD 7.2.0及更新版本的組態範例，其中允許遠端存取VPN使用傳輸層安全(TLS)和IKEv2。作為客戶端，可以使用Cisco AnyConnect，它受多個平台支援。

設定

1. 導入SSL證書

配置AnyConnect時，證書非常重要。

手動註冊證書有以下限制：

1. 在FTD上，需要憑證授權單位(CA)憑證，才能產生憑證簽署請求(CSR)。
2. 如果從外部生成CSR，則使用PKCS12的其他方法。

在FTD裝置上取得憑證的方法有多種，但安全簡單的方法是建立CSR並由CA簽署。以下是操作方法：

1. 切換作業選項至Objects > Object Management > PKI > Cert Enrollment，然後按一下Add Cert Enrollment。
2. 輸入信任點名稱RAVPN-SSL-cert (可選)。
3. 在CA Information頁籤下，選擇Manual「註冊型別」，然後貼上CA證書，如圖所示。

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  
AGA1UEChMJSWRibIRydXN0MS  
cwJQYDVQQDEx5JZGVu  
VHJ1c3QgQ29tbWVyY2lhbCBSb  
290IENBIDEwHhcNMTkxMjE1MT  
Y1NjE1WhcNMjkx  
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - CA憑證

4. 在Certificate Parameters下，輸入主體名稱。舉例來說：

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 -憑證引數

5. 在Key 頁籤下，選擇金鑰型別，並提供名稱和位大小。對於RSA，最少2048位。

6. 按一下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 -憑證金鑰

7. 定位至Devices > Certificates > Add > New Certificate。

8. 選擇Device。在Cert Enrollment下，選擇建立的信任點，然後按一下Add，如圖所示。

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 - 向FTD註冊憑證

9. 按一下ID，系統將顯示生成CSR的提示，然後選擇Yes。

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is selected. The main content area displays a table of certificates for the device 'ftd'. The table has columns for Name, Domain, Enrollment Type, and Status. The 'RAVPN-SSL-cert' entry is highlighted, and its status is 'Identity certificate import required'.

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

FMC - 已註冊證書CA

Warning

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

No

Yes

FMC -生成CSR

10. 已生成CSR，可以與CA共用該CSR，以便獲取身份證書。

11. 從CA收到base64格式的身份證書後，請按一下Browse Identity Certificate和Import從磁碟中選擇它，如圖所示。

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++p1jIWcdVROn0vtah+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 - 導入身份證書

12. 導入成功後，信任點RAVPN-SSL-cert將被視為：

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

FMC - 信任點註冊成功

2. 配置RADIUS伺服器

2.1. 在FMC上管理FTD

1. 導航至Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group。
2. 輸入名稱ISE，然後按一下+新增「RADIUS伺服器」。

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伺服器配置

- 提及ISE Radius伺服器的IP地址以及共用金鑰 (金鑰) , 該金鑰與ISE伺服器上的相同。
- 選擇FTD與ISE伺服器通訊時使用的Routing 或Specific Interface。

5. 按一下Save 如下圖所示。

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. 儲存後，伺服器即增加到RADIUS Server Group 下，如下圖所示。

Name	Value
ISE	1 Server

FMC - RADIUS伺服器組

2.2. 在ISE上管理FTD

1. 定位至Network Devices ，然後按一下Add。
2. 輸入伺服器和FTD通訊介面RADIUS用IP Address戶端的名稱'Cisco-Radius'。
3. 在Radius Authentication Settings 下，增加Shared Secret。
4. 按一下Save。

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 (Info)

networkDevices.secondSharedSecret: (Show)

CoA Port: 1700 (Set To Default)

ISE -網路裝置

5. 若要建立使用者，請切換作業選項至Network Access > Identities > Network Access Users，然後按一下 Add。
6. 視需要建立UsernameandLogin密碼。

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 ⓘ

Enable Password _____ ⓘ

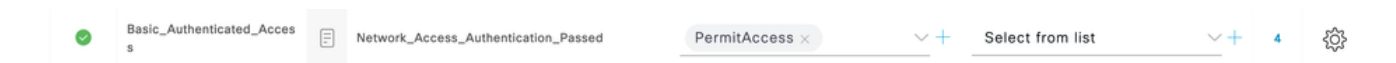
ISE -使用者

7. 要設定基本策略，請定位至Policy > Policy Sets > Default > Authentication Policy > Default，然後選擇All_User_ID_Stores。

8. 切換作業選項至Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access，並選擇PermitAccess，如下圖所示。



ISE -身份驗證策略



ISE -授權策略

3. 為FMC上的VPN使用者建立地址池

1. 定位至Objects > Object Management > Address Pools > Add IPv4 Pools。
2. 輸入名稱RAVPN-Pool與地址範圍，遮罩為選擇性。
3. 按一下儲存。

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 - 地址池

4. 上傳AnyConnect映像

1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
2. 輸入名稱anyconnect-win-4.10.07073-webdeploy，然後按一下Browse 以從磁碟中選擇Anyconnect檔案，然後按一下Save（如圖所示）。

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC - Anyconnect客戶端映像

5. 建立XML設定檔

5.1. 在設定檔編輯器上

1. 從software.cisco.com下載配置檔案編輯器並打開它。
2. 切換作業選項至Server List > Add...
3. 輸入「顯示名稱」RAVPN-IKEV2和FQDN，以及「使用者群組（別名）」。
4. 選擇「主要」通訊協定 IPsec，asclick，如Ok 圖所示。

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)

設定檔編輯器-伺服器清單

5. 新增伺服器清單。另存為ClientProfile.xml。

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

設定檔編輯器- ClientProfile.xml

5.2. 在FMC上

1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
2. 輸入「名稱」ClientProfile，然後按一下Browse 以從磁碟選擇檔案ClientProfile.xml。
3. 按一下Save 。

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Anyconnect VPN配置檔案

6. 配置遠端訪問

1. 導航到Devices > VPN > Remote Access，然後按一下+以增加連線配置檔案，如下圖所示。

RAVPN-IKEV2

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	+

FMC -遠端訪問連線配置檔案

2. 輸入連線配置檔名稱RAVPN-IKEV2，並透過按一下+建立組策略(如Group Policy圖所示)。

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 -組策略

3. 輸入名稱RAVPN-group-policy，然後選擇VPN協定 SSL and IPsec-IKEv2 如圖所示。

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通訊協定

4. 在AnyConnect > Profile下，從下拉選單中選擇XML配置檔案ClientProfile，然後按一下Save（如圖所示）。

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配置檔案

5. 按一下+ as shown in the image增加「地址池」RAVPN-Pool。

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 -客戶端地址分配

6. 切換作業選項至AAA > Authentication Method , 然後選擇AAA Only。

7. 選擇Authentication Server作為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驗證

8. 導航到Aliases，輸入別名RAVPN-IKEV2。該別名在ClientProfile.xml中用作使用者組。

9. 按一下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 -別名

10. 導航到Access Interfaces，並選擇必須啟用RAVPN IKEv2的介面。

11. 選擇SSL和IKEv2的身份證書。

12. 按一下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 -存取介面

13. 切換作業選項至Advanced。

14. 按一下+增加Anyconnect客戶端映像。

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客戶端軟體套件

15. 在IPsec下，增加如圖所示Crypto Maps。

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 -加密對映

16. 在IPsec下，按一下+IKE Policy以新增。

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策略

17. 在IPsec 下，增加IPsec/IKEv2 Parameters。

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引數

18. 在Connection Profile下，新建設RAVPN-IKEV2定檔。

19. Save按一下圖所示。

RAVPN-IKEV2 You have unsaved changes Save Cancel

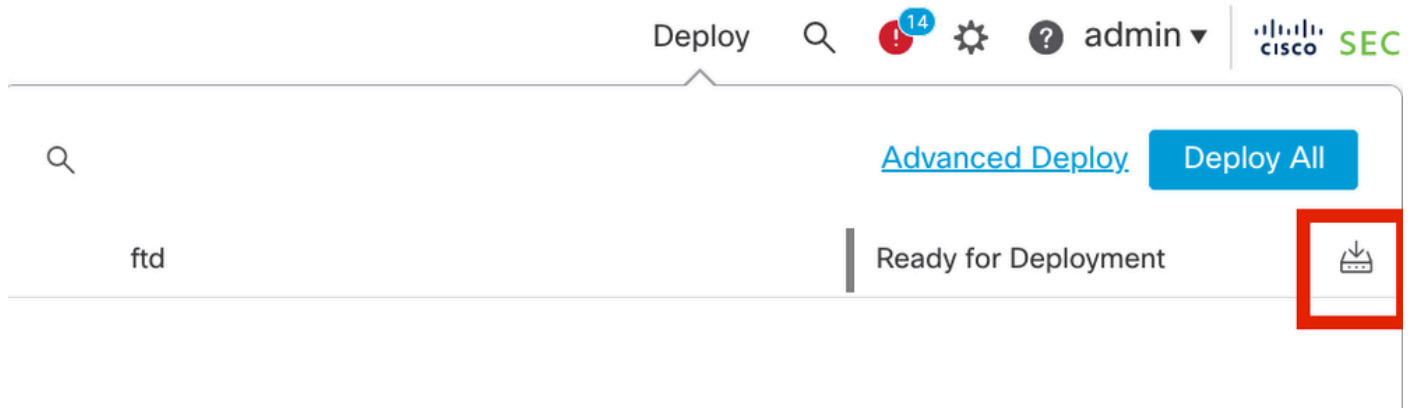
Policy Assignments (1)
Local Realm: None Dynamic Access Policy: None

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 -

20. 部署配置。



FMC - FTD部署

7. Anyconnect配置檔案配置

PC上的配置檔案，儲存在 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>
```

注意：建議在將客戶端配置檔案下載到所有使用者的PC後，在組策略下停用SSL客戶端作為隧道協定。這可以確保使用者只能使用IKEv2/IPsec隧道協定進行連線。

驗證

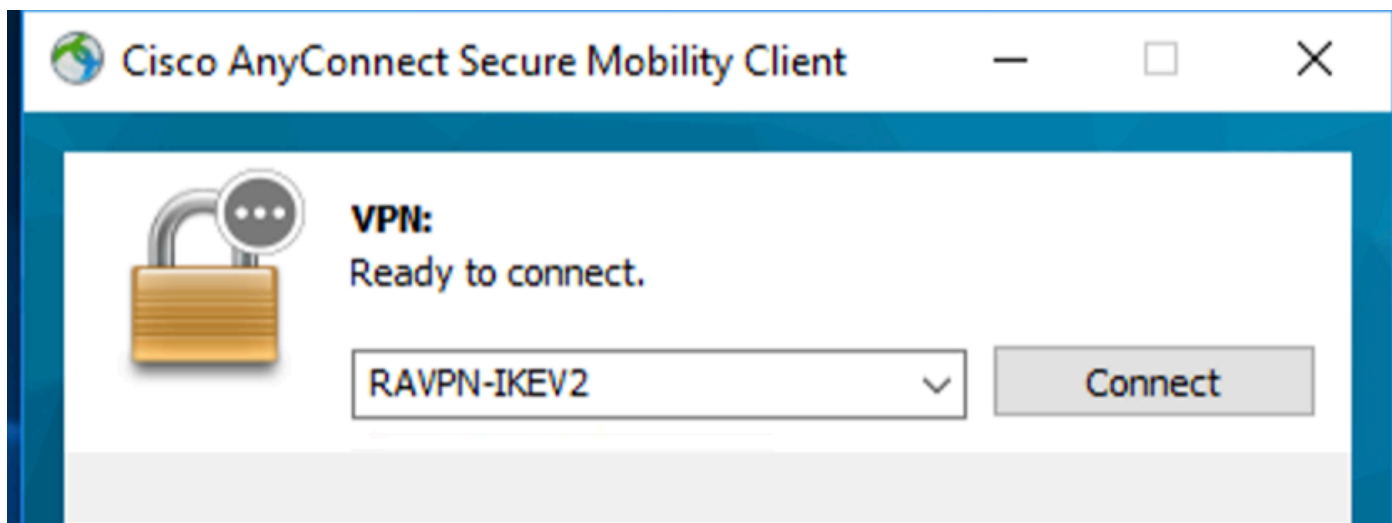
您可以使用此部分來確認您的配置是否正常工作。

1. 對於第一個連線，使用FQDN/IP透過Anyconnect從使用者PC建立SSL連線。

ClientProfile.xml 2. 如果已停用SSL協定，並且無法執行上一步驟，請確保PC上客戶端配置檔案位於C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile路徑下（例如，TFTP伺服器或TFTP伺服器）。

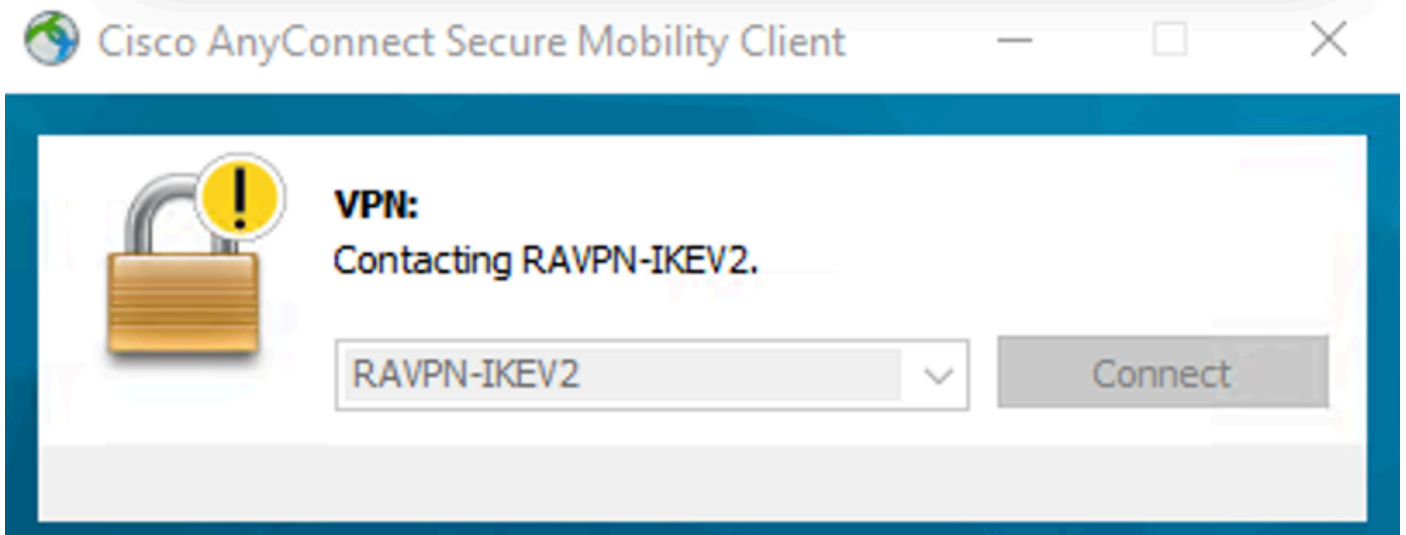
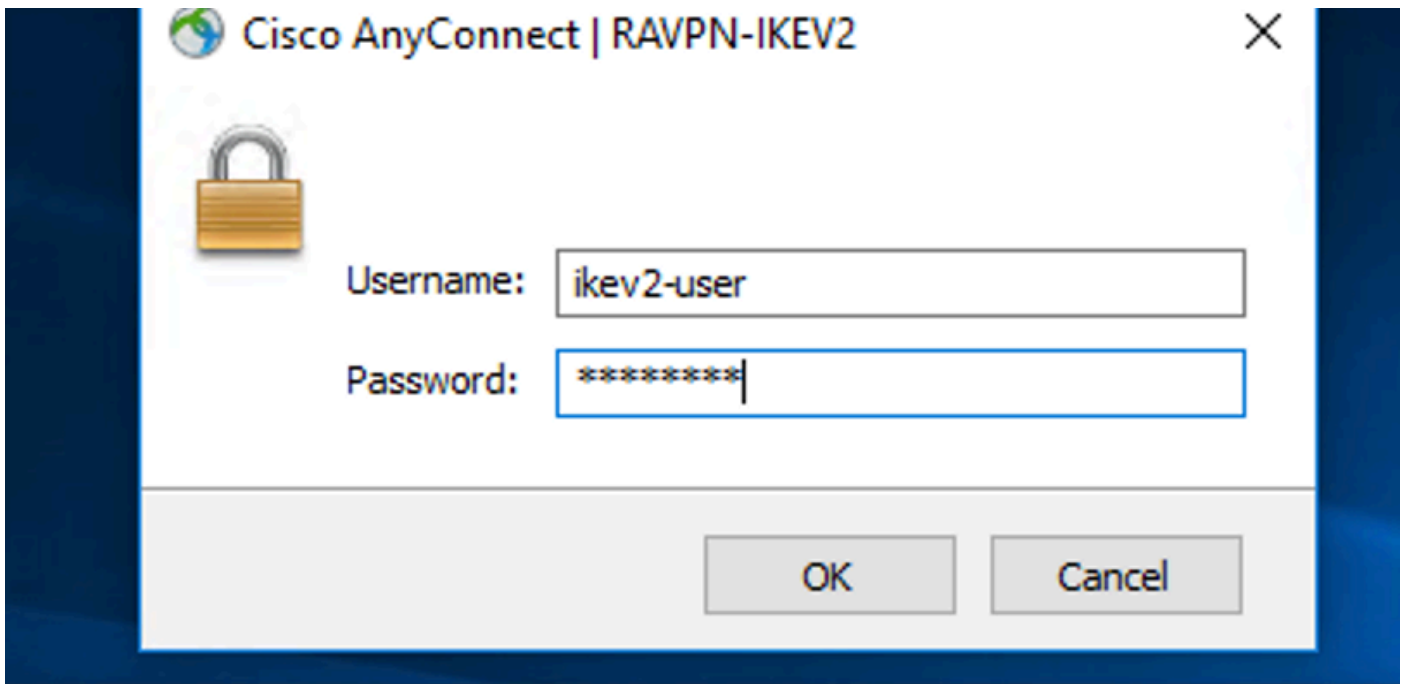
3. 在出現提示後，輸入用於身份驗證的使用者名稱和密碼。

- 身份驗證成功後，客戶端配置檔案會下載到使用者的PC上。
- 斷開與Anyconnect的連線。
- 下載配置檔案後，請使用下拉選單選擇客戶端配置檔案中提及的主機名，**RAVPN-IKEV2** 以便使用IKEv2/IPsec連線到Anyconnect。
- 按一下Connect。



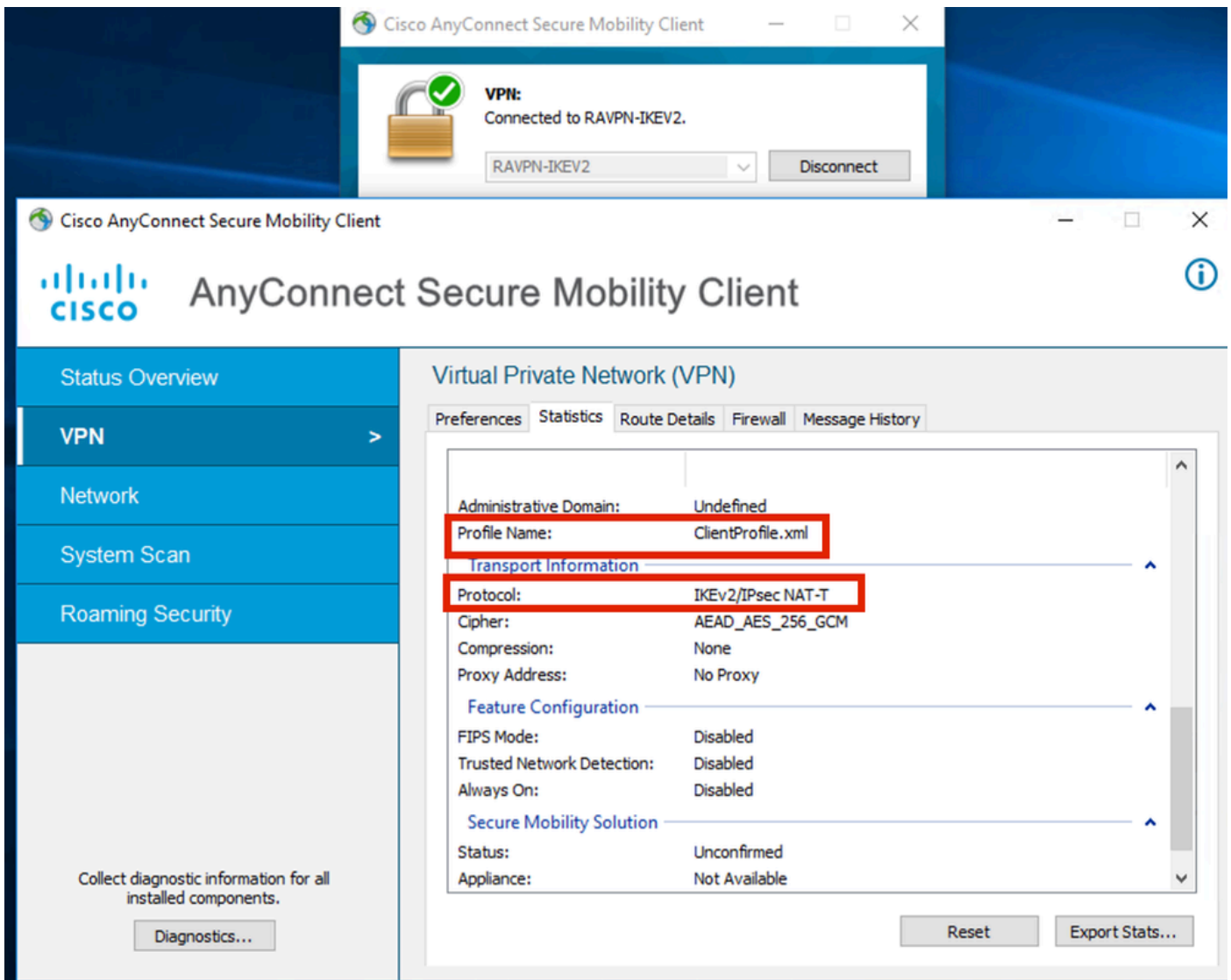
Anyconnect 下拉選單

- 輸入在ISE伺服器上建立的身份驗證的使用者名稱和密碼。



Anyconnect連線

9. 驗證連線後使用的配置檔案和協定(IKEv2/IPsec)。



Anyconnect已連線

FTD CLI輸出：

```
<#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                                       fvrf/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日誌：

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 -即時日誌

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

```
debug radius all
```

```
debug crypto ikev2 platform 255
```

```
debug crypto ikev2 protocol 255
```

```
debug crypto ipsec 255
```


關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。