

Configurazione di Anyconnect VPN con FTD tramite IKEv2 con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[1. Importare il certificato SSL](#)

[2. Configurare il server RADIUS](#)

[2.1. Gestione FTD su FMC](#)

[2.2. Gestisci FTD su ISE](#)

[3. Creare un pool di indirizzi per gli utenti VPN su FMC](#)

[4. Carica immagini AnyConnect](#)

[5. Crea profilo XML](#)

[5.1. Nell'Editor di profili](#)

[5.2. Sul CCP](#)

[6. Configurare Accesso remoto](#)

[7. Configurazione Del Profilo Anyconnect](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la configurazione di base della VPN ad accesso remoto con autenticazione IKEv2 e ISE su FTD gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN di base, TLS e Internet Key Exchange versione 2 (IKEv2)
- Autenticazione di base, autorizzazione e accounting (AAA) e RADIUS
- Esperienza con Firepower Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

IKEv2 e SSL (Secure Sockets Layer) sono entrambi protocolli utilizzati per stabilire connessioni protette, in particolare nel contesto delle VPN. IKEv2 fornisce metodi di crittografia e autenticazione efficaci, offrendo un elevato livello di sicurezza per le connessioni VPN.

Questo documento offre un esempio di configurazione per FTD versione 7.2.0 e successive, che permette a VPN ad accesso remoto di usare Transport Layer Security (TLS) e IKEv2. Come client, è possibile usare Cisco AnyConnect, che è supportato su più piattaforme.

Configurazione

1. Importare il certificato SSL

I certificati sono essenziali quando si configura AnyConnect.

Esistono limitazioni per la registrazione manuale dei certificati:

1. Nell'FTD è necessario un certificato dell'Autorità di certificazione (CA) prima che venga generata una richiesta di firma del certificato (CSR).
2. Se la CSR viene generata esternamente, viene utilizzato un metodo diverso di PKCS12.

Esistono diversi metodi per ottenere un certificato su un accessorio FTD, ma quello più semplice e sicuro è creare un CSR e ottenerne la firma da una CA. A tale scopo, eseguire la procedura seguente:

1. **Passare a** Objects > Object Management > PKI > Cert Enrollment e fare clic su Add Cert Enrollment.
2. Inserire il nome del punto di fiducia RAVPN-SSL-cert.
3. Nella CA Information scheda, scegliere Tipo di registrazione come Manual e incollare il certificato CA come mostrato nell'immagine.

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
cwJQYDVQQDEx5JZGVu
VHJ1c3QgQ29tbWVyY2lhbCBSb
290IENBIDEwHhcNMTkxMjE1
Y1NjE1WhcNMjE1
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - Certificato CA

4. In Certificate Parameters, inserire il nome del soggetto. Ad esempio:

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 - Parametri certificato

5. Sotto la Key scheda, scegliere il tipo di chiave e fornire un nome e le dimensioni bit. Per RSA, il valore minimo è 2048 bit.

6. Fare clic su 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 - Chiave certificato

7. Passare a Devices > Certificates > Add > New Certificate.

8. Scegliere Device. In Cert Enrollment, scegliere il trust point creato e fare clic su Add come mostrato nell'immagine.

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 - Registrazione certificato a FTD

9. Fare clic su ID, e viene visualizzato un prompt per generare CSR, scegliere Yes.

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 - Certificato CA registrato

Warning

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

No

Yes

FMC - Genera CSR

- Viene generato un CSR che può essere condiviso con l'autorità di certificazione per ottenere il certificato di identità.
- Dopo aver ricevuto il certificato di identità da CA in formato base64, sceglierlo dal disco facendo clic su Browse Identity Certificate e Import come mostrato nell'immagine.

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-----
MIICqjCCAZICAQAwnJEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQGA1UEAwwNRIRELmNpc2NvLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPLLwTQ6BkGjER2FfyofT+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 - Importa certificato di identità

12. Una volta completata l'importazione, il trust point RAVPN-SSL-cert viene considerato come:

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

FMC - Registrazione Trustpoint riuscita

2. Configurare il server RADIUS

2.1. Gestione FTD su FMC

1. Passare a Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. Inserire il nome ISE e aggiungere i server RADIUS facendo clic su +.

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 - Configurazione server Radius

3. Citare l'indirizzo IP del server ISE Radius insieme al segreto condiviso (chiave) che è lo stesso del server ISE.

4. Scegliere Routing o Specific Interface attraverso il quale l'FTD comunica con il server ISE.

5. Fare clic Save come mostrato nell'immagine.

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

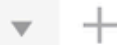
Timeout: (1-300) Seconds

10

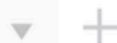
Connect using:

Routing Specific Interface 

outside



Redirect ACL:



Cancel

Save

6. Una volta salvato, il Server viene aggiunto sotto l'immagine RADIUS Server Group come mostrato nell'immagine.

Name	Value
ISE	1 Server

FMC - Gruppo server RADIUS

2.2. Gestisci FTD su ISE

1. Passare a Network Devices e fare clic su Add.

2. Immettere il nome 'Cisco-Radius' del server e IP Address del client radius che è l'interfaccia di comunicazione FTD.

3. In Radius Authentication Settings, aggiungere il Shared Secret.

4. Fare clic su Save .

The screenshot shows the configuration page for a Network Device named 'Cisco-Radius'. The page is divided into several sections:

- Network Devices List:** Shows the current device 'Cisco-Radius'.
- Basic Information:** Fields for Name (Cisco-Radius), Description, IP Address (10.197.167.5 / 25), Device Profile (Cisco-Radius), Model Name, and Software Version.
- Network Device Group:** Fields for Device Type (All Device Types), IPSEC (No), and Location (All Locations), each with a 'Set To Default' link.
- RADIUS Authentication Settings:** A checked checkbox for 'RADIUS Authentication Settings'.
- RADIUS UDP Settings:** Fields for Protocol (RADIUS), Shared Secret (masked with dots and a 'Show' link), 'Use Second Shared Secret' (unchecked), networkDevices.secondSharedSecret (masked with dots and a 'Show' link), and CoA Port (1700) with a 'Set To Default' link.

ISE - Dispositivi di rete

5. Per creare gli utenti, passare a Network Access > Identities > Network Access Users e fare clic Add su.

6. Creare un nome utente e una password di login come richiesto.

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 - Utenti

7. Per impostare i criteri di base, passare a Policy > Policy Sets > Default > Authentication Policy > Default, scegliere All_User_ID_Stores.

8. Passare a Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, e scegliere PermitAccess come mostrato nell'immagine.

Default

All_User_ID_Stores ⓘ ▾

> Options 4 ⚙

ISE - Criteri di autenticazione

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess × ▾ +

Select from list ▾ + 4 ⚙

ISE - Authorization Policy

3. Creare un pool di indirizzi per gli utenti VPN su FMC

1. Passare a Objects > Object Management > Address Pools > Add IPv4 Pools.
2. Inserire il nome RAVPN-Pool e l'**intervallo di indirizzi**. La maschera è facoltativa.
3. Fare clic su **Salva**.

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 - Pool indirizzi

4. Carica immagini AnyConnect

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

2. Immettere il nome anyconnect-win-4.10.07073-webdeploy e fare clic su Browse per scegliere il file **Anyconnect** dal disco, fare clic su Save come mostrato nell'immagine.

Edit AnyConnect File



Name:*

File Name:*

File Type:*



Description:

FMC - Immagine client Anyconnect

5. Crea profilo XML

5.1. Nell'Editor di profili

1. Scaricare l'Editor di profili da aprirlosoftware.cisco.com.
2. Passa a **Server List > Add...**
3. Inserire il nome visualizzato RAVPN-IKEV2 e il nomeFQDN insieme al **gruppo di utenti** (nome alias).
4. Scegliere il protocollo principale IPsec , facendo clic su **Ok** come mostrato nell'immagine.

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)

Editor profili - Elenco server

5. È stato aggiunto l'elenco dei server. Salva con nome 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

Editor profili - ClientProfile.xml

5.2. Sul CCP

1. Passare a Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Inserire un nome ClientProfile e fare clic su Browse per scegliere ClientProfile.xml il file dal disco.
3. Fare clic su **Save** .

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Profilo VPN Anyconnect

6. Configurare Accesso remoto

1. Passare a Devices > VPN > Remote Accesse fare clic su + per aggiungere un profilo di connessione come mostrato nell'immagine.

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

FMC - Profilo connessione accesso remoto

2. Inserire il nome del profilo di connessione RAVPN-IKEV2 e creare un criterio di gruppo facendo clic su + in **Group Policy** come mostrato nell'immagine.

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 - Criteri di gruppo

3. Inserire il nomeRAVPN-group-policy , scegliere i protocolli VPN SSL and IPsec-IKEv2 come mostrato nell'immagine.

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 - Protocolli VPN

4. In AnyConnect > Profile , scegliere il profilo XML ClientProfile dall'elenco a discesa e fare clic Save come mostrato nell'immagine.

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 - Profilo Anyconnect

5. Aggiungere il pool di indirizzi RAVPN-Pool facendo clic su + 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 - Assegnazione indirizzo client

6. Passare a AAA > Authentication Method e scegliere AAA Only.

7. Scegliere Authentication Server come 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 - Autenticazione AAA

8. Passare a Aliases , inserire un nome alias RAVPN-IKEV2 utilizzato come gruppo di utenti in ClientProfile.xml .

9. Fare clic su 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

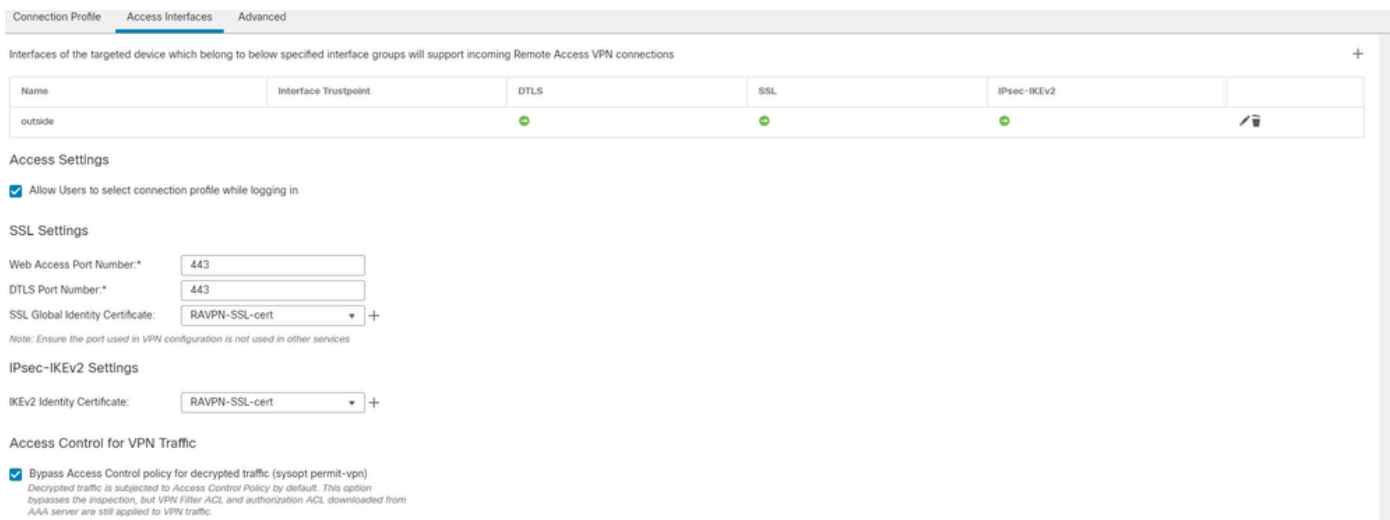
Save

FMC - Alias

10. Passare a Access Interfaces e scegliere l'interfaccia in cui RAVPN IKEv2 deve essere abilitato.

11. Scegliere il certificato di identità per SSL e IKEv2.

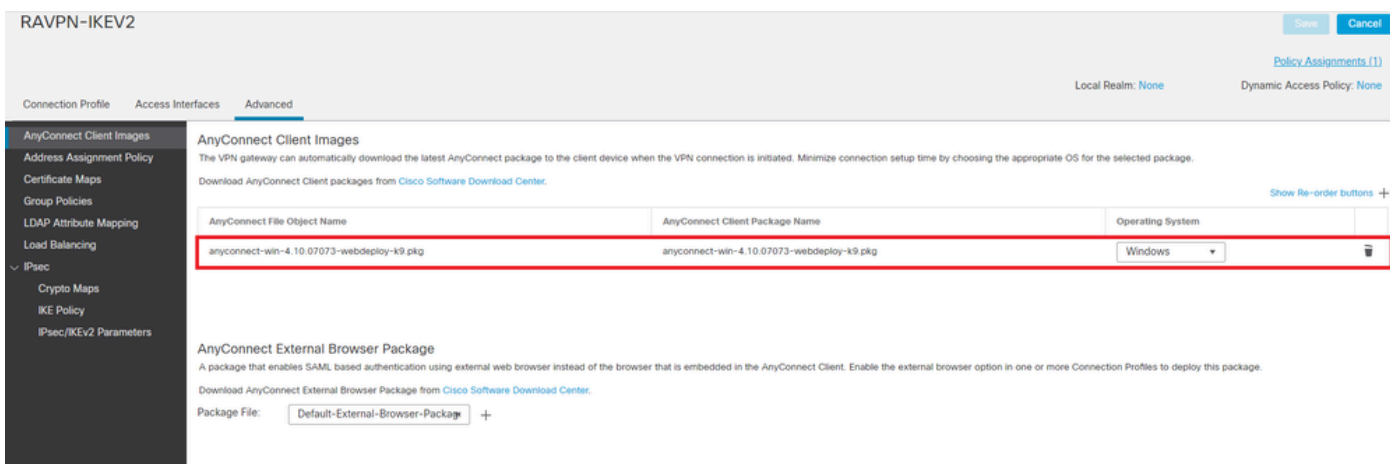
12. Fare clic su Save.



FMC - Interfacce di accesso

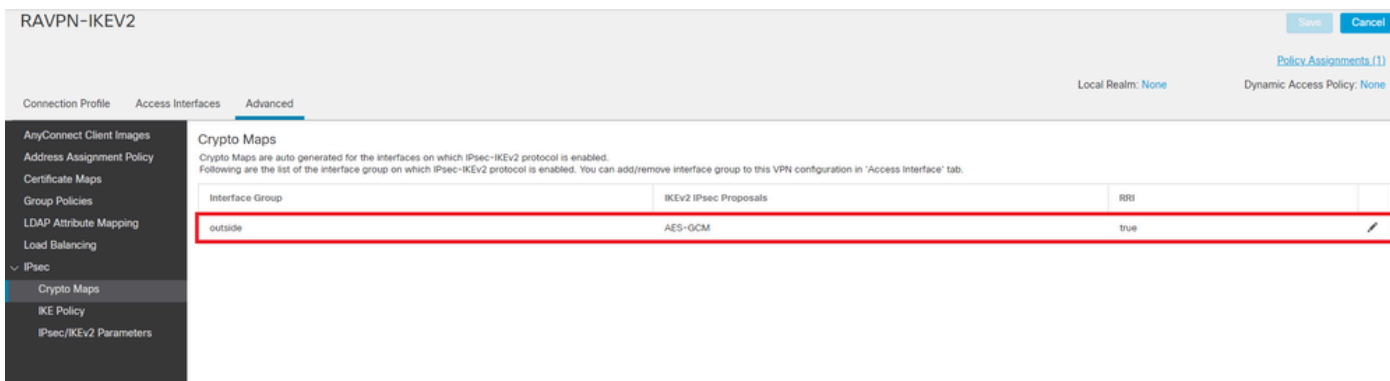
13. Passare a Advanced .

14. Aggiungere le immagini del client Anyconnect facendo clic su +.



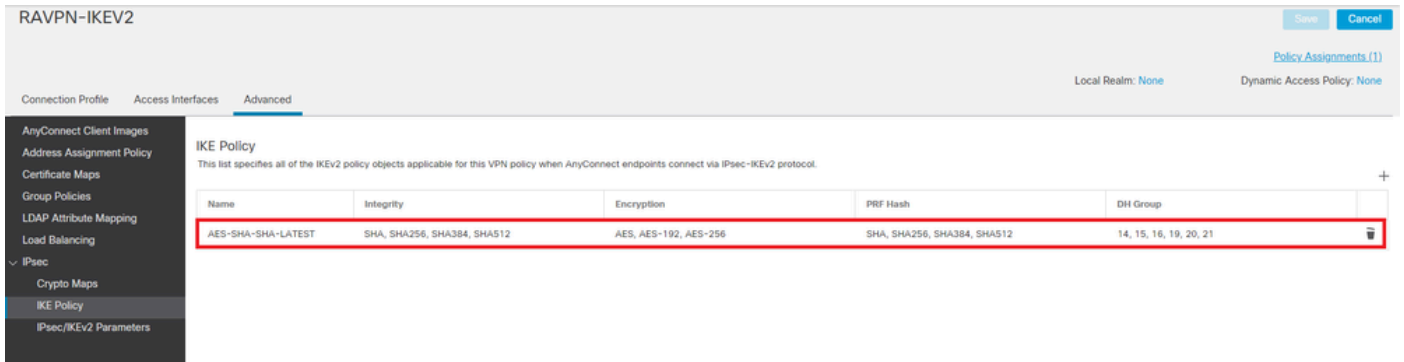
FMC - Pacchetto client Anyconnect

15. SottoIPsec, aggiungereCrypto Maps come mostrato nell'immagine.



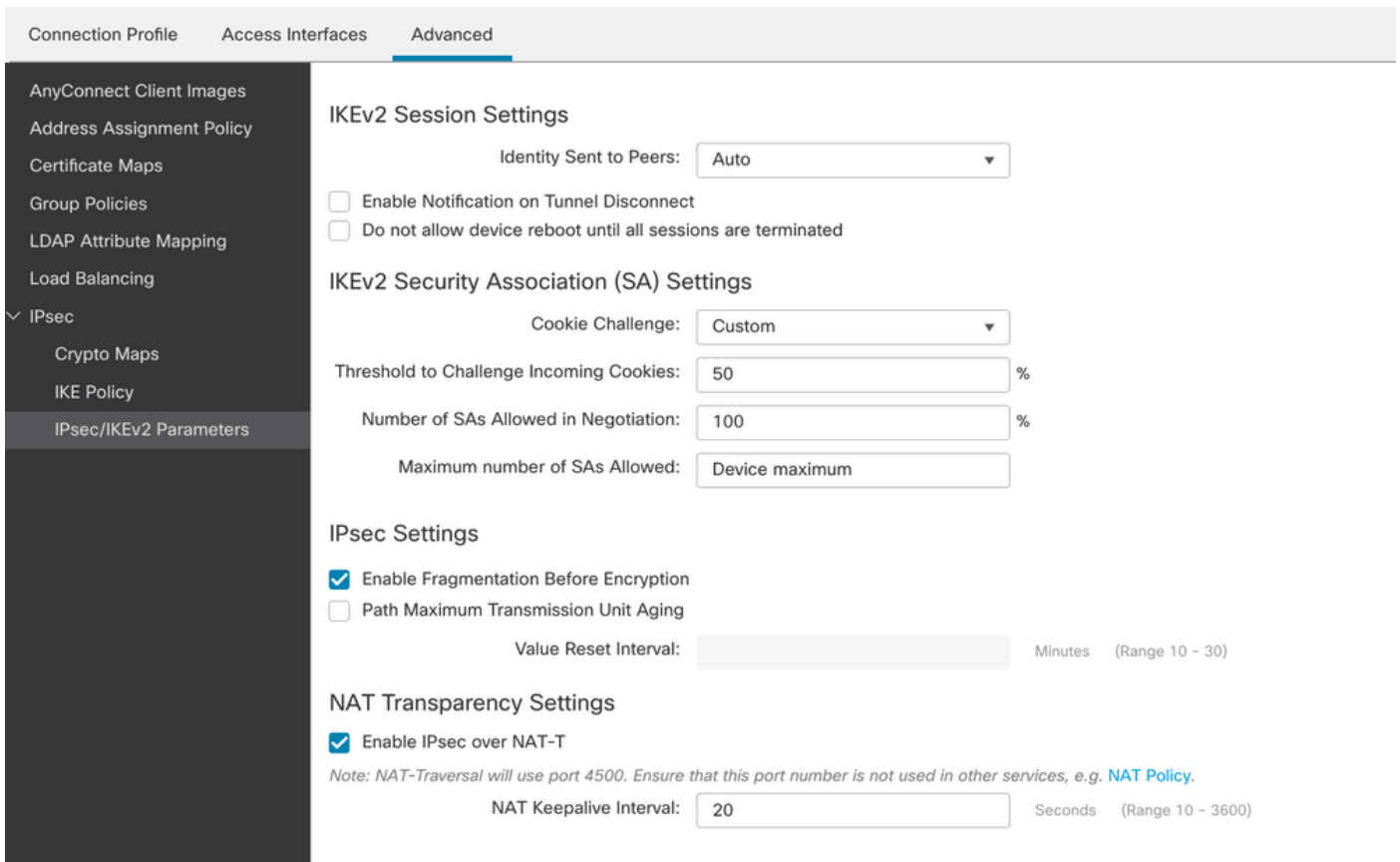
FMC - Mappe crittografiche

16. In IPsec , aggiungere il IKE Policy facendo clic su +.



FMC - Criterio IKE

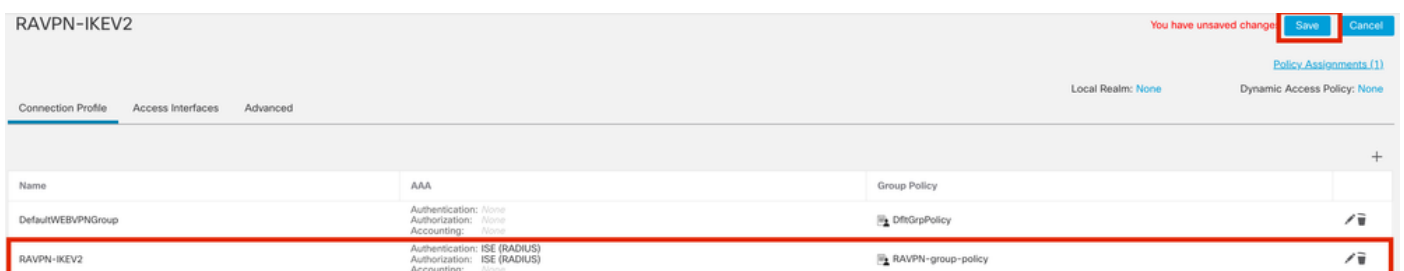
17. In IPsec , aggiungere il simbolo IPsec/IKEv2 Parameters .



FMC - Parametri IPsec/IKEv2

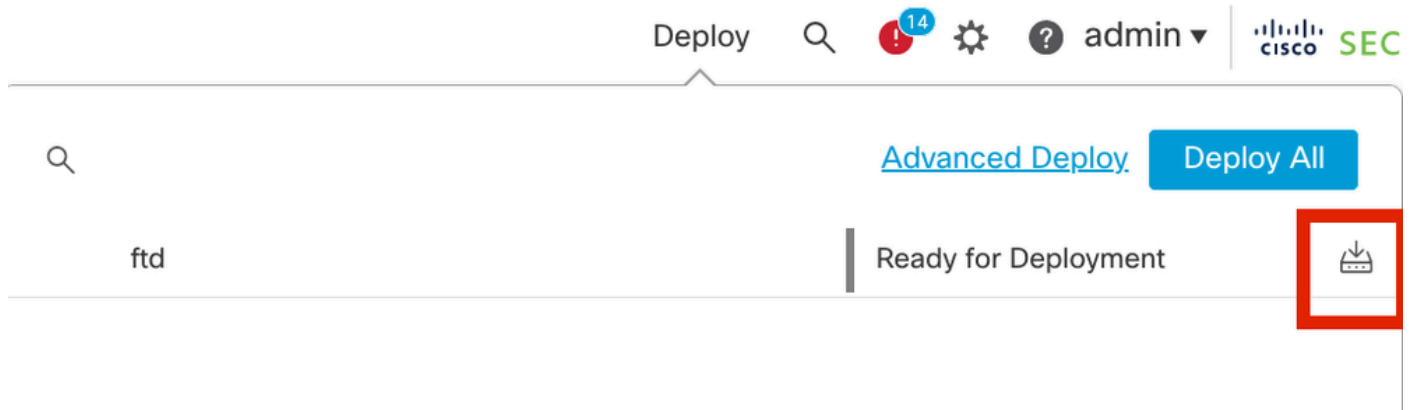
18. In Connection Profile, viene creato un nuovo profilo RAVPN-IKEV2.

19. Fare Save clic come mostrato nell'immagine.



FMC - Profilo di connessione RAVPN-IKEV2

20. Distribuire la configurazione



FMC - Distribuzione FTD

7. Configurazione Del Profilo Anyconnect

Profilo sul PC, salvato in 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>
```



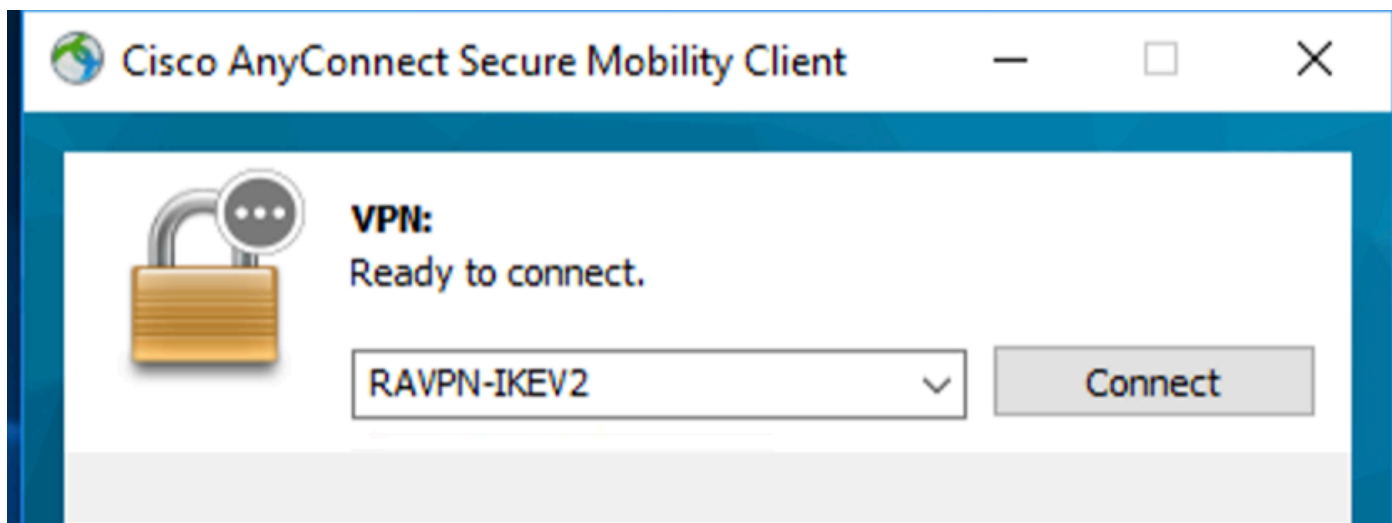
Nota: si consiglia di disabilitare il client SSL come protocollo di tunneling in Criteri di gruppo dopo aver scaricato il profilo client nel PC di tutti gli utenti. In questo modo, gli utenti possono connettersi esclusivamente tramite il protocollo di tunneling IKEv2/IPsec.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

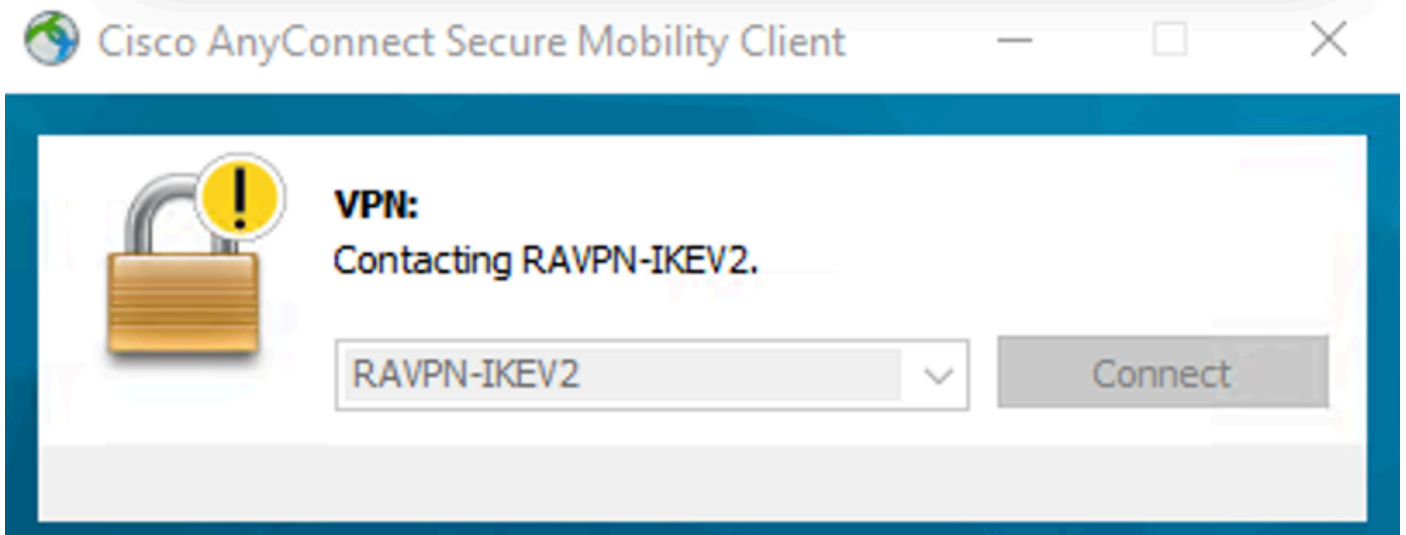
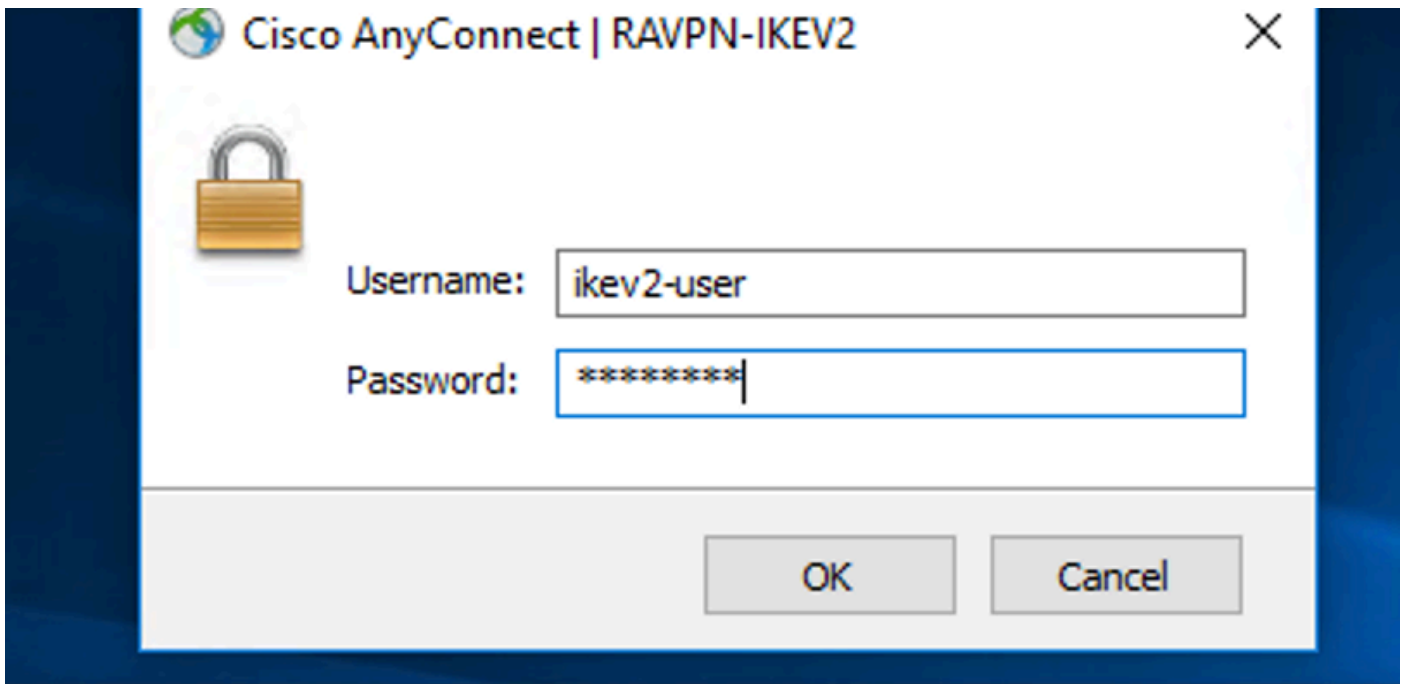
1. Per la prima connessione, usare il nome FQDN/IP per stabilire una connessione SSL dal PC dell'utente tramite Anyconnect. ClientProfile.xml
2. Se il protocollo SSL è disabilitato e non è possibile eseguire il passaggio precedente, verificare che il profilo client sia presente sul PC nel percorso C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .
3. Inserire il nome utente e la password per l'autenticazione quando richiesto.

4. Dopo l'autenticazione, il profilo client viene scaricato sul PC dell'utente.
5. Disconnettersi da Anyconnect.
6. Una volta scaricato il profilo, usare l'elenco a discesa per scegliere il nome host indicato nel profilo del client **RAVPN-IKEV2** per connettersi a Anyconnect con IKEv2/IPsec.
7. Fare clic su Connect.



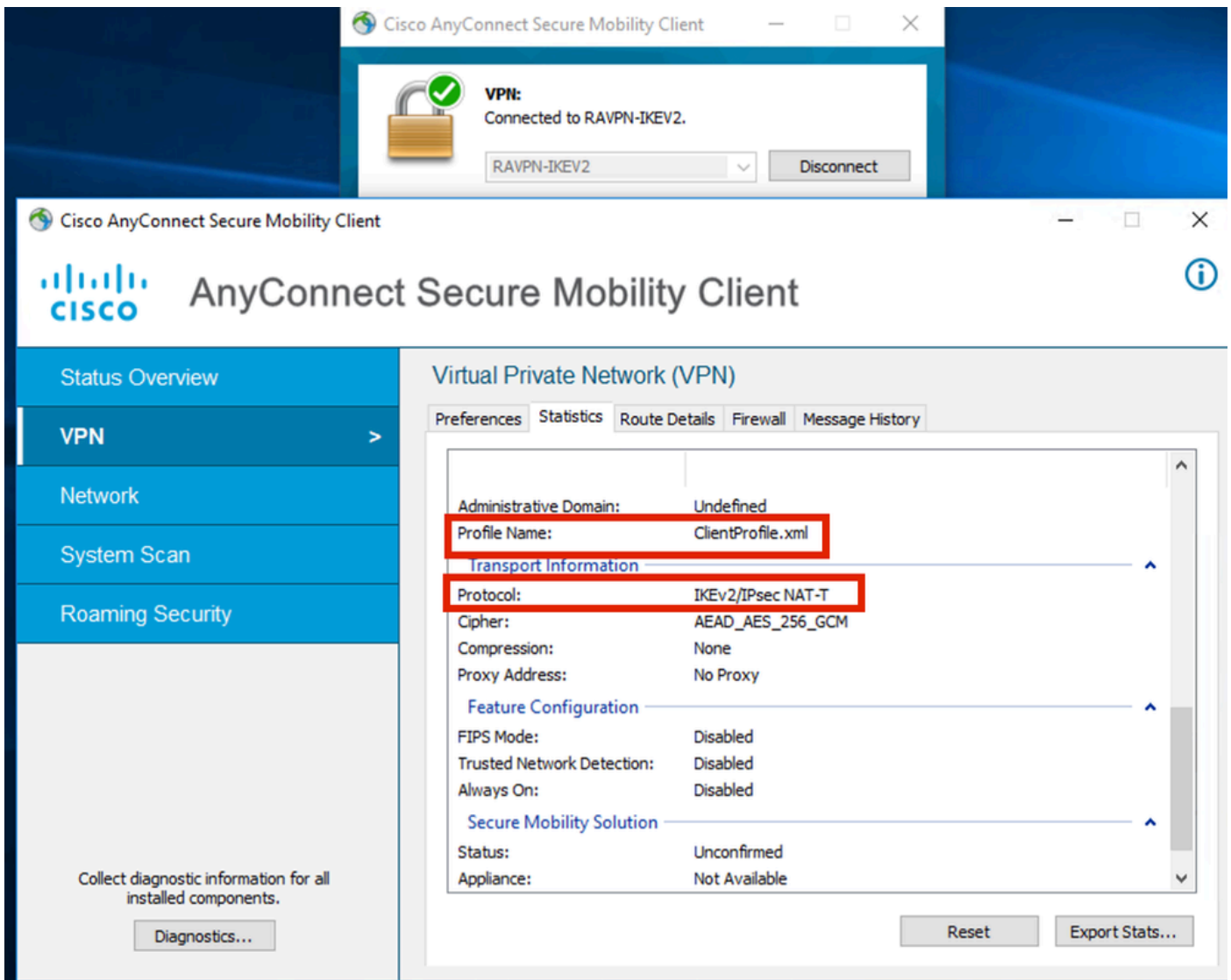
Elenco a discesa Anyconnect

8. Immettere il nome utente e la password per l'autenticazione creata sul server ISE.



Anyconnect Connection

9. Verificare il profilo e il protocollo (IKEv2/IPsec) utilizzati dopo la connessione.



Anyconnect Connected

Output CLI FTD:

```
<#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

Log ISE:

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:BD:6B:...	Windows1...	Default >>...	Default >>...	PermitAcc...							ise
Jan 04, 2024 07:14:10.4...				ikev2-user	00:50:56:BD:6B:...	Windows1...	Default >>...	Default >>...	PermitAcc...		Cisco-Radius		Workstation			ise

ISE - Live Log

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

debug radius all

debug crypto ikev2 platform 255

debug crypto ikev2 protocol 255

debug crypto ipsec 255

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).