

Configurer Anyconnect VPN sur FTD via IKEv2 avec ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[1. Importez le certificat SSL](#)

[2. Configuration du serveur RADIUS](#)

[2.1. Gestion du FTD sur FMC](#)

[2.2. Gestion du FTD sur ISE](#)

[3. Créez un pool d'adresses pour les utilisateurs VPN sur FMC](#)

[4. Télécharger des images AnyConnect](#)

[5. Créer un profil XML](#)

[5.1. Dans l'Éditeur de profil](#)

[5.2.2 Sur FMC](#)

[6. Configuration de l'accès distant](#)

[7. Configuration du profil Anyconnect](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit la configuration de base du VPN d'accès à distance avec authentification IKEv2 et ISE sur FTD géré par le FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN de base, TLS et Internet Key Exchange version 2 (IKEv2)
- Authentification de base, autorisation et comptabilité (AAA) et RADIUS
- Expérience avec Firepower Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

IKEv2 et SSL (Secure Sockets Layer) sont deux protocoles utilisés pour établir des connexions sécurisées, en particulier dans le contexte des réseaux privés virtuels. IKEv2 fournit des méthodes de cryptage et d'authentification puissantes, offrant un haut niveau de sécurité pour les connexions VPN.

Ce document fournit un exemple de configuration pour FTD version 7.2.0 et ultérieure, qui permet un accès VPN à distance afin d'utiliser la sécurité de la couche transport (TLS) et IKEv2. En tant que client, Cisco AnyConnect peut être utilisé, qui est pris en charge sur plusieurs plates-formes.

Configurer

1. Importez le certificat SSL

Les certificats sont essentiels lorsque AnyConnect est configuré.

L'inscription manuelle des certificats comporte des limites :

1. Sur FTD, un certificat d'autorité de certification (CA) est nécessaire avant qu'une demande de signature de certificat (CSR) ne soit générée.
2. Si le CSR est généré en externe, une autre méthode de PKCS12 est utilisée.

Il existe plusieurs méthodes pour obtenir un certificat sur un appareil FTD, mais la méthode la plus sûre et la plus simple consiste à créer un CSR et à le faire signer par une autorité de certification.

Voici comment procéder :

1. **Accédez à** Objects > Object Management > PKI > Cert Enrollment, puis cliquez sur Add Cert Enrollment.
2. Entrez le nom du point de confiance RAVPN-SSL-cert.
3. Sous l'onglet CA Information, choisissez le type d'inscription comme Manual et collez le certificat CA comme illustré dans l'image.

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 - Certificat CA

4. SousCertificate Parameters, entrez le nom de l'objet. Exemple :

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 - Paramètres de certificat

5. Sous l'onglet Key, choisissez le type de clé et indiquez un nom et une taille de bit. Pour RSA, 2 048 bits est le minimum.

6. Cliquez sur 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 - Clé de certificat

7. Accédez à Devices > Certificates > Add > New Certificate.

8. Sélectionnez Device. Sous Cert Enrollment, choisissez le point de confiance créé, puis cliquez sur Add comme illustré dans l'image.

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 - Inscription de certificat au FTD

9. Cliquez sur ID, et une invite pour générer CSR s'affiche, choisissez 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 - Certificat CA inscrit

Warning

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

No

Yes

FMC - Génération de CSR

10. Un CSR est généré et peut être partagé avec l'autorité de certification afin d'obtenir le certificat d'identité.

11. Après avoir reçu le certificat d'identité de l'autorité de certification au format base64, choisissez-le sur le disque en cliquant sur Browse Identity Certificate et Import, comme indiqué dans l'image.

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 - Importer le certificat d'identité

12. Une fois l'importation réussie, le point de confiance RAVPN-SSL-cert est considéré comme :

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

FMC - Inscription de Trustpoint réussie

2. Configuration du serveur RADIUS

2.1. Gestion du FTD sur FMC

1. Accédez à Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. Entrez le nom ISE et ajoutez des serveurs RADIUS en cliquant sur +.

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 - Configuration du serveur Radius

3. Mentionnez l'adresse IP du serveur ISE Radius avec le secret partagé (clé) qui est le même que sur le serveur ISE.

4. Choisissez soit Routing soit Specific Interface par le biais duquel le FTD communique avec le serveur ISE.

5. Cliquez sur Save comme indiqué dans l'image.

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

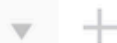
Connect using:

Routing Specific Interface 

outside



Redirect ACL:



Cancel

Save

6. Une fois enregistré, le serveur est ajouté sous le RADIUS Server Group comme indiqué dans l'image.

RADIUS Server Group		Add RADIUS Server Group	Filter
RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.			
Name	Value		
ISE	1 Server		

FMC - Groupe de serveurs RADIUS

2.2. Gestion du FTD sur ISE

1. Accédez à Network Devices et cliquez sur Add.

2. Entrez le nom « Cisco-Radius » du serveur et IP Address du client RADIUS qui est l'interface de communication FTD.

3. Sous Radius Authentication Settings, ajoutez la Shared Secret.

4. Cliquez sur 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'.
- Name**: Set to 'Cisco-Radius'.
- Description**: Empty field.
- IP Address**: Set to '10.197.167.5 / 25'.
- Device Profile**: Set to 'Cisco-Radius'.
- Model Name**: Empty field.
- Software Version**: Empty field.
- 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** (checked):
 - RADIUS UDP Settings**:
 - Protocol**: 'RADIUS'
 - Shared Secret**: Masked with dots (Show)
 - Use Second Shared Secret** (Show)
 - networkDevices.secondSharedSecret**: Empty field (Show)
 - CoA Port**: '1700' (Set To Default)

ISE - Périphériques réseau

5. Pour créer des utilisateurs, accédez à Network Access > Identities > Network Access Users, puis cliquez sur Add.

6. Créez un nom d'utilisateur et un mot de passe de connexion.

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 - Utilisateurs

7. Pour configurer la stratégie de base, accédez à Policy > Policy Sets > Default > Authentication Policy > Default, puis sélectionnez All_User_ID_Stores.

8. Naviguez jusqu'à Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, l'image et choisissez-PermitAccessla.

Default

All_User_ID_Stores

> Options

ISE - Politique d'authentification

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess

Select from list

ISE - Politique d'autorisation

3. Créez un pool d'adresses pour les utilisateurs VPN sur FMC

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

2. Entrez le nom RAVPN-Pool et la **plage d'adresses**, le masque est facultatif.

3. Cliquez sur **Enregistrer**.

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 d'adresses

4. Télécharger des images AnyConnect

1. Accédez à Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Entrez le nom anyconnect-win-4.10.07073-webdeployet cliquez sur Browse afin de choisir le **Anyconnect** fichier à partir du disque, cliquez sur Save comme indiqué dans l'image.

Edit AnyConnect File



Name:*

File Name:*

File Type:*



Description:

FMC - Image client Anyconnect

5. Créer un profil XML

5.1. Dans l'Éditeur de profil

1. Téléchargez l'Éditeur de profil depuis software.cisco.com et ouvrez-le.
2. Accédez à **Server List > Add...**
3. Entrez le nom d'affichage RAVPN-IKEV2 et FQDN ainsi que le **groupe d'utilisateurs** (alias).
4. Choisissez le protocole principal IPsec , comme cliquez sur **Ok** comme indiqué dans l'image.

Server List Entry [X]

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)

Éditeur de profil - Liste des serveurs

5. La liste des serveurs est ajoutée. Enregistrez-le sous ClientProfile.xml .

AnyConnect Profile Editor - VPN [-] [□] [X]

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.

Éditeur de profil - ClientProfile.xml

5.2. Sur FMC

1. Accédez à Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Entrez un nom ClientProfile et cliquez sur Browse afin de choisir le fichier ClientProfile.xml à partir du disque.
3. Cliquez sur **Save** .

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - Profil VPN Anyconnect

6. Configuration de l'accès distant

1. Accédez à Devices > VPN > Remote Access et cliquez sur + afin d'ajouter un profil de connexion comme indiqué dans l'image.

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

FMC - Profil de connexion d'accès à distance

2. Entrez le nom du profil de connexion RAVPN-IKEV2 et créez une stratégie de groupe + en cliquant sur **Group Policy** comme indiqué dans l'image.

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 - Stratégie de groupe

3. Entrez le nom RAVPN-group-policy , choisissez les protocoles VPN SSL and IPsec-IKEv2 comme indiqué dans l'image.

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 - Protocoles VPN

4. Sous AnyConnect > Profile , choisissez le profil XML ClientProfile dans la liste déroulante, puis cliquez sur Save comme illustré dans l'image.

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 - Profil Anyconnect

5. Ajoutez le pool d'adresses RAVPN-Pool en cliquant sur + 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 - Attribution d'adresses client

6. Accédez à AAA > Authentication Method, puis sélectionnez AAA Only.

7. Choisissez Authentication Server comme ISE (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 : authentication AAA

8. Accédez à Aliases , entrez un nom d'alias RAVPN-IKEV2 , qui est utilisé comme groupe d'utilisateurs dans ClientProfile.xml .

9. Cliquez sur 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

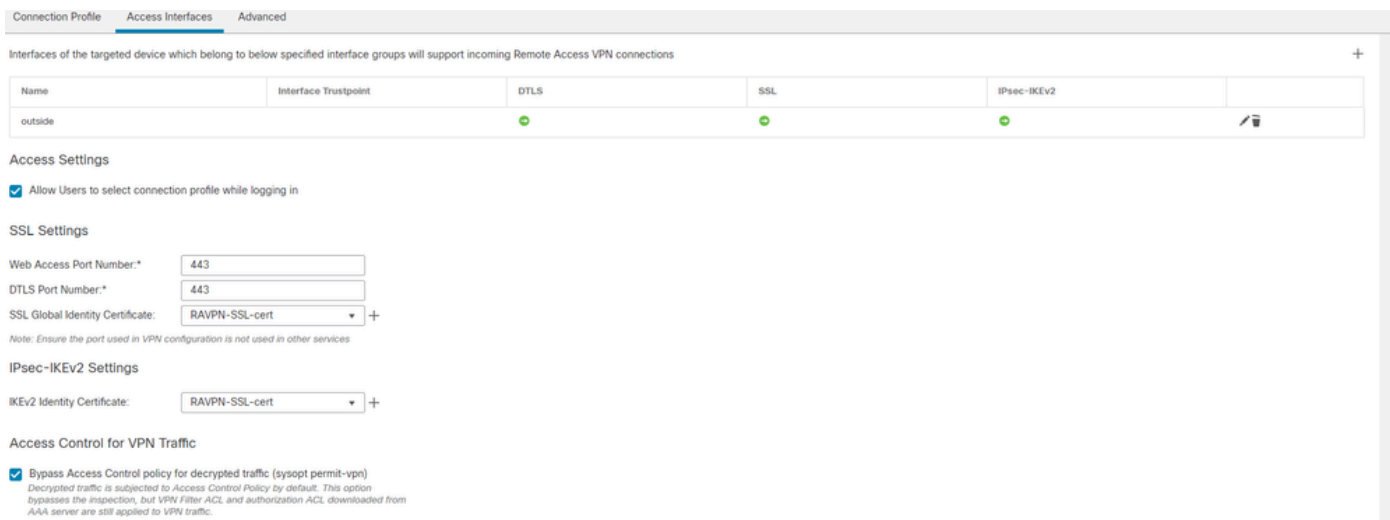
Save

FMC - Alias

10. Accédez à Access Interfaces, puis sélectionnez l'interface sur laquelle RAVPN IKEv2 doit être activé.

11. Choisissez le certificat d'identité pour SSL et IKEv2.

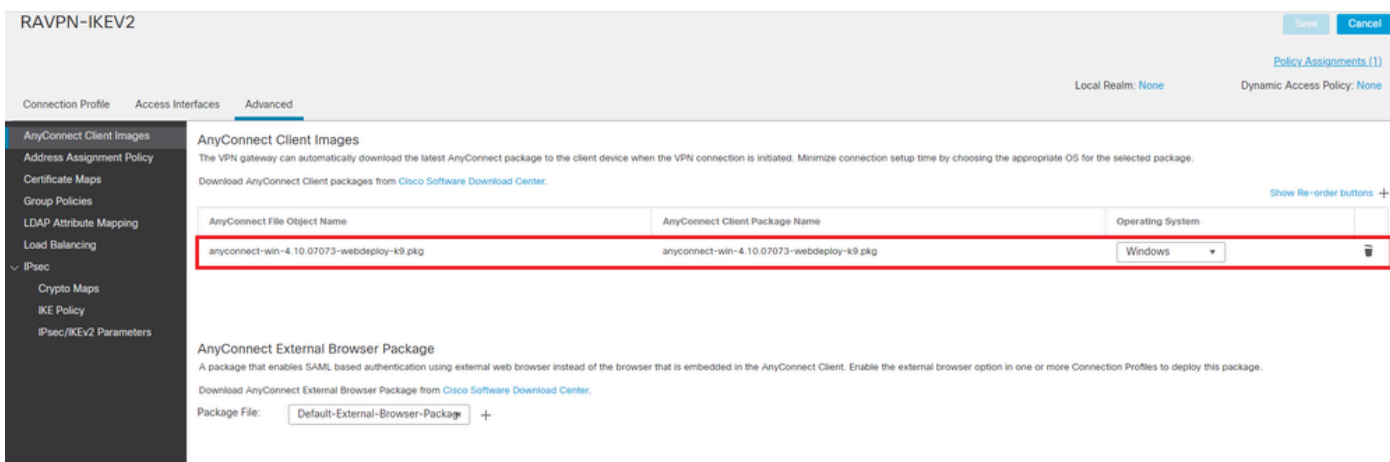
12. Cliquez sur Save.



FMC - Interfaces d'accès

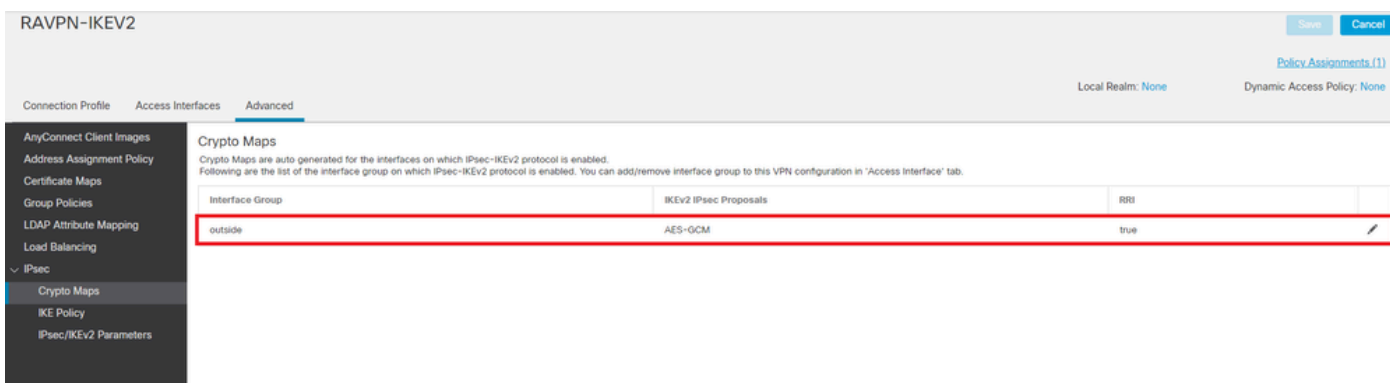
13. Accédez à Advanced .

14. Ajoutez les images Anyconnect Client en cliquant sur +.



FMC - Package client Anyconnect

15. SousIPsec, ajoutez lesCrypto Maps comme indiqué dans l'image.



FMC - Crypto-cartes

16. Sous IPsec , ajoutez le IKE Policy en cliquant sur +.

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 - Politique IKE

17. Sous IPsec , ajoutez la 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 - Paramètres IPsec/IKEv2

18. Sous Connection Profile, un nouveau profil RAVPN-IKEV2 est créé.

19. SaveCliquier comme indiqué sur l'image.

RAVPN-IKEV2 You have unsaved changes Save Cancel

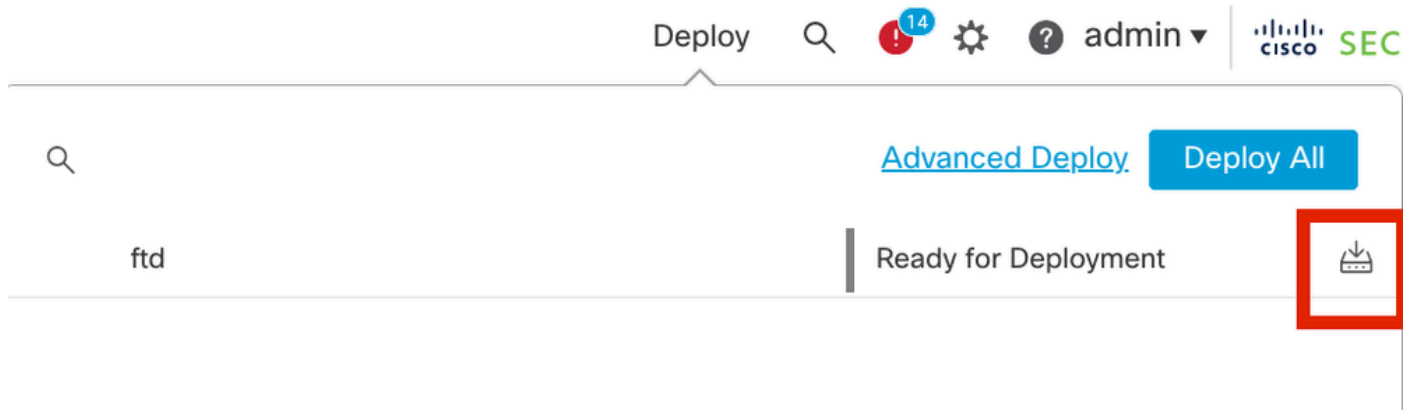
Policy Assignments (1)
Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

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

FMC - Profil de connexion RAVPN-IKEV2

20. Déployez la configuration.



FMC - Déploiement FTD

7. Configuration du profil Anyconnect

Profil sur PC, enregistré sous C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .

<#root>

```
<?xml version="1.0" encoding="UTF-8"?> <AnyConnectProfile xmlns="http://schemas[dot]xmlsoap[dot]org/encoding/" xmlns:xsi="http://www[dot]w3[dot]org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ http://www.w3.org/2001/XMLSchema-instance" >  
  <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGroup>  
  </HostEntry> </ServerList> </AnyConnectProfile>
```



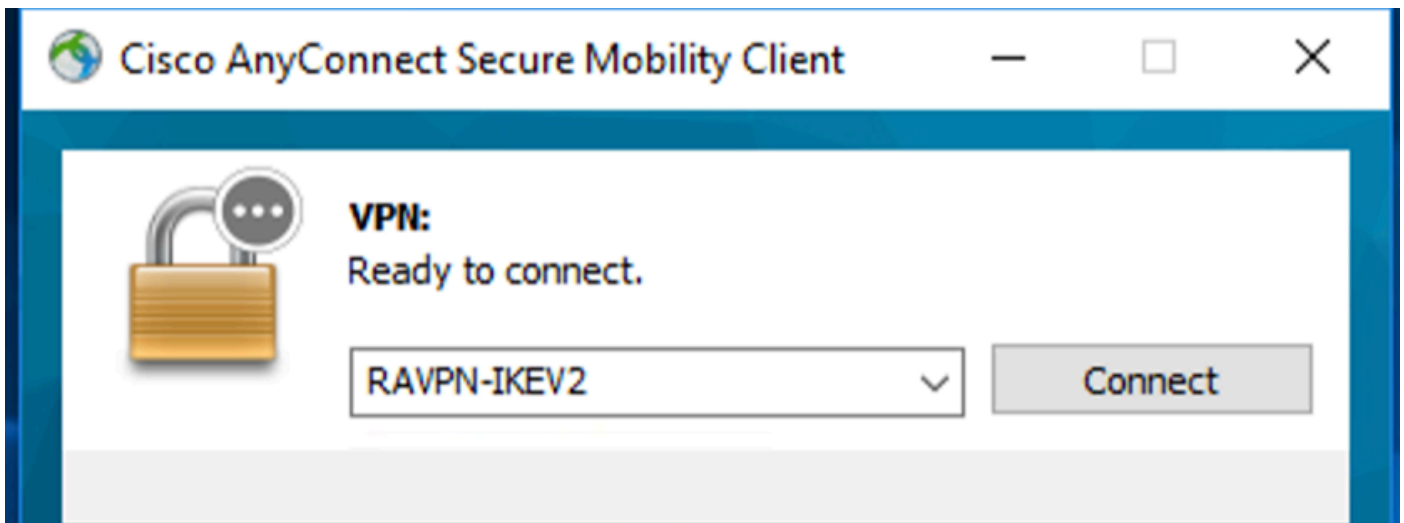
Remarque : il est recommandé de désactiver le client SSL en tant que protocole de tunnellation sous la stratégie de groupe une fois que le profil client est téléchargé sur le PC de tous les utilisateurs. Cela garantit que les utilisateurs peuvent se connecter exclusivement à l'aide du protocole de tunnellation IKEv2/IPsec.

Vérifier

Vous pouvez utiliser cette section afin de confirmer que votre configuration fonctionne correctement.

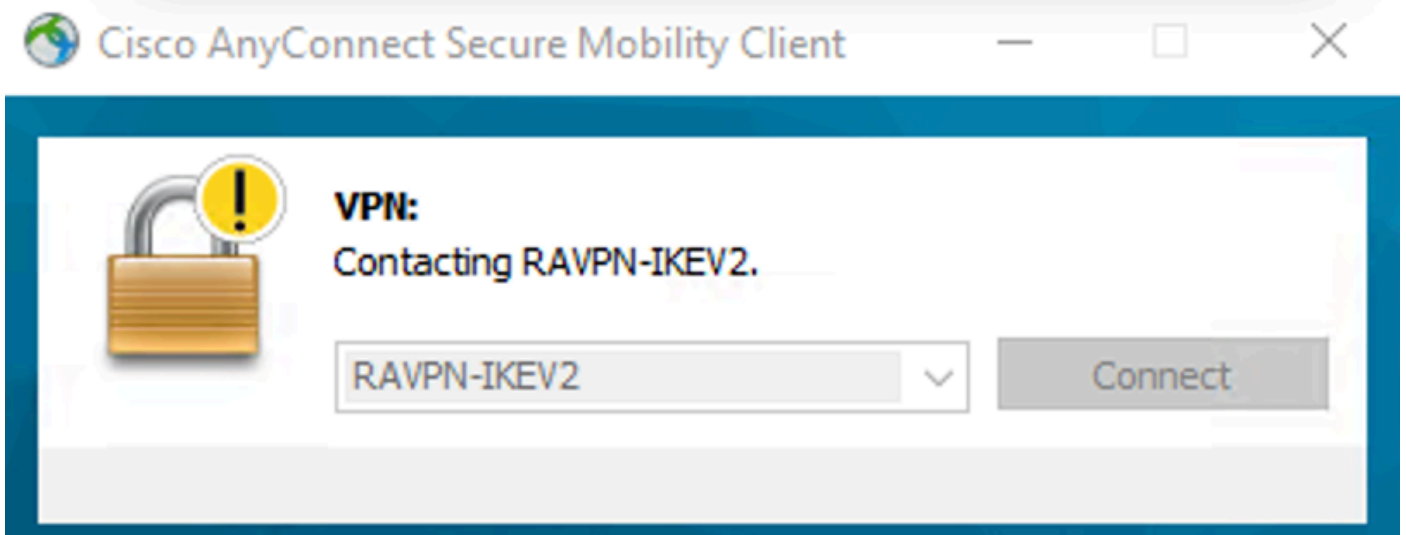
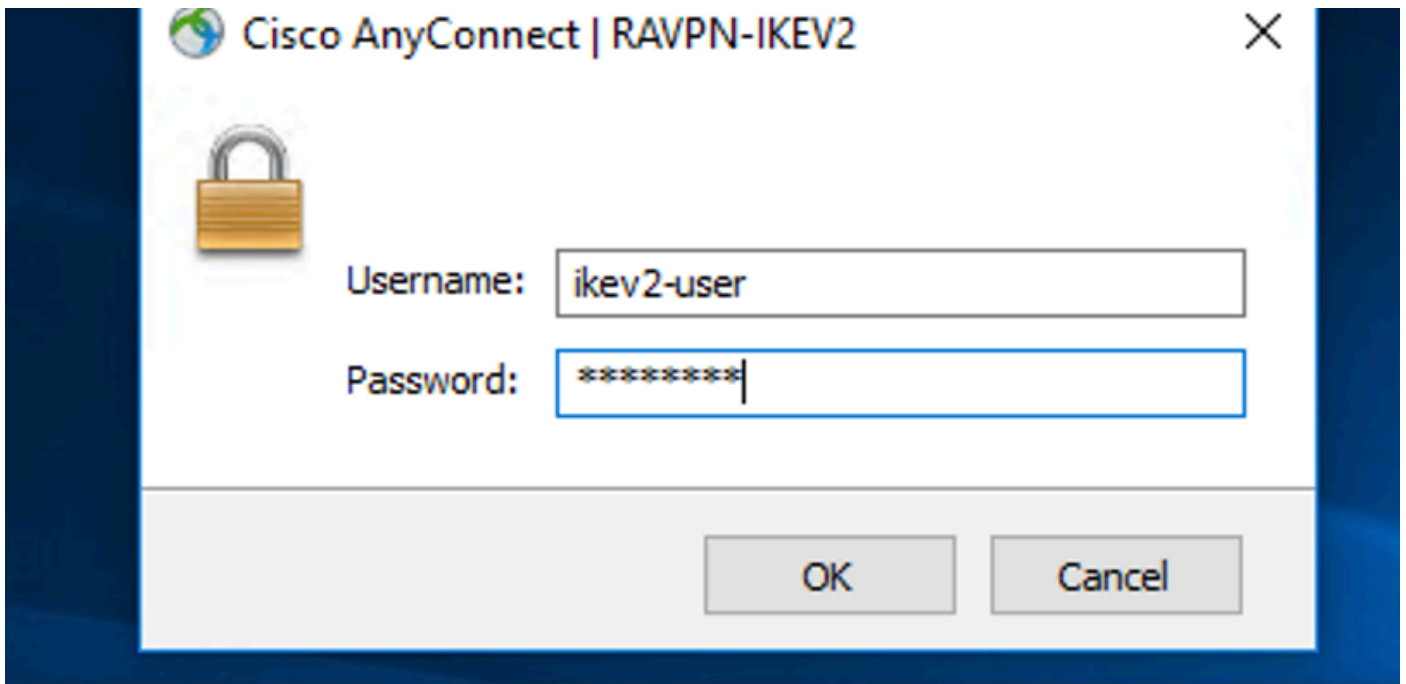
1. Pour la première connexion, utilisez le FQDN/IP afin d'établir une connexion SSL à partir du PC de l'utilisateur via Anyconnect.
2. Si le protocole SSL est désactivé et que l'étape précédente ne peut pas être effectuée, assurez-vous que le profil client ClientProfile.xml est présent sur le PC sous le chemin C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile .
3. Entrez le nom d'utilisateur et le mot de passe pour l'authentification une fois invité.

4. Une fois l'authentification réussie, le profil client est téléchargé sur le PC de l'utilisateur.
5. Déconnectez-vous d'Anyconnect.
6. Une fois le profil téléchargé, utilisez la liste déroulante afin de choisir le nom d'hôte mentionné dans le profil client **RAVPN-IKEV2** afin de se connecter à Anyconnect à l'aide d'IKEv2/IPsec.
7. Cliquez sur Connect.



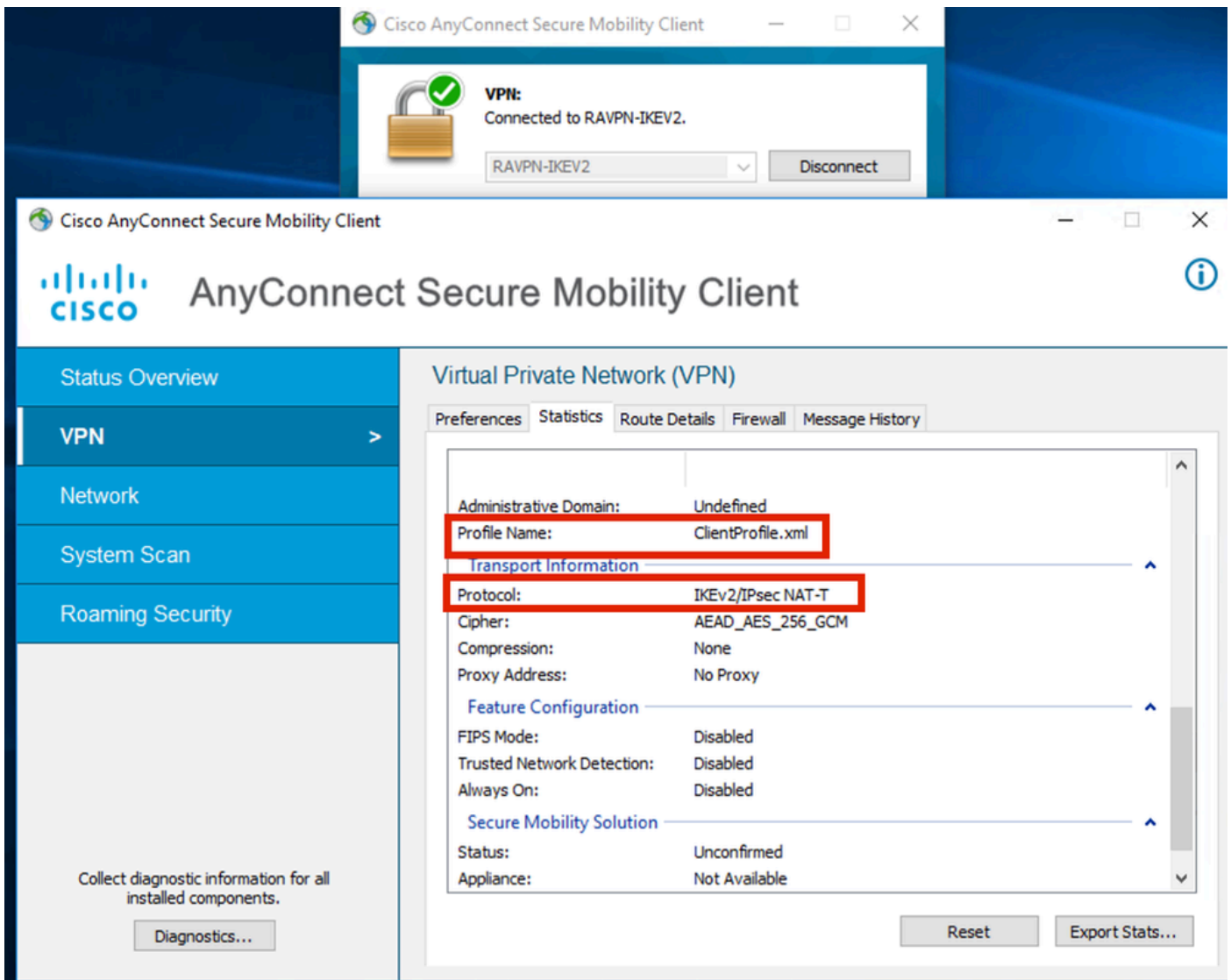
Liste déroulante Anyconnect

8. Entrez le nom d'utilisateur et le mot de passe d'authentification créés sur le serveur ISE.



Connexion Anyconnect

9. Vérifiez le profil et le protocole (IKEv2/IPsec) utilisés une fois connectés.



Anyconnect Connected

Sorties 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

Journaux 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 - Journaux en direct

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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


À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.