

AnyConnect VPN met FTD configureren via IKEv2 met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[1. Voer het SSL-certificaat in](#)

[2. RADIUS-server configureren](#)

[2.1. FTD op het VCC beheren](#)

[2.2. FTD beheren op ISE](#)

[3. Maak een adresgroep voor VPN-gebruikers op FMC](#)

[4. AnyConnect-afbeeldingen uploaden](#)

[5. XML-profiel maken](#)

[5.1. Over de profieeditor](#)

[5.2.VCC](#)

[6. Externe toegang configureren](#)

[7. Profielconfiguratie voor AnyConnect](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de basisconfiguratie van Remote Access VPN met IKEv2- en ISE-verificatie op FTD die wordt beheerd door het FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis VPN, TLS en Internet Key Exchange versie 2 (IKEv2)
- Basisverificatie, autorisatie en accounting (AAA) en RADIUS
- Ervaring met Firepower Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Firepower Threat Defence (FTD) 7.2.0
- Cisco VCC 7.2.0
- AnyConnect 4.10.07073
- Cisco ISE-lijnkaart 3.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

IKEv2 en Secure Sockets Layer (SSL) zijn beide protocollen die worden gebruikt voor het opzetten van beveiligde verbindingen, met name in de context van VPN's. IKEv2 biedt sterke encryptie- en verificatiemethoden die een hoog beveiligingsniveau voor VPN-verbindingen bieden.

Dit document biedt een configuratievoorbeeld voor FTD versie 7.2.0 en hoger, die externe toegang tot VPN biedt om Transport Layer Security (TLS) en IKEv2 te gebruiken. Als client kan Cisco AnyConnect worden gebruikt, wat op meerdere platforms wordt ondersteund.

Configureren

1. Voer het SSL-certificaat in

Certificaten zijn essentieel wanneer AnyConnect is geconfigureerd.

Er zijn beperkingen aan handmatige certificaatinschrijving:

1. Op de FTD is een certificaat van de certificeringsinstantie (CA) vereist voordat een verzoek tot ondertekening van het certificaat (CSR) wordt gegenereerd.
2. Indien de MVO extern wordt gegenereerd, wordt een andere methode van PKCS12 gebruikt.

Er zijn verschillende methoden om een certificaat op FTD-apparaat te verkrijgen, maar de veilige en gemakkelijke manier is om een CSR te maken en het ondertekend te krijgen door een CA. Dit is de manier om dat te doen:

1. **Navigeer naar** Objects > Object Management > PKI > Cert Enrollment en klik op Add Cert Enrollment.
2. Voer de naam van het trustpoint in RAVPN-SSL-cert.
3. Kies onder het CA Information tabblad Inschrijftype als Manual en plak het CA-certificaat zoals in de afbeelding.

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
```

VCC - CA-certificaat

4. Voer onder Certificate Parameters de onderwerpnaam in. Voorbeeld:

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

VCC - certificaatparameters

5. Kies onder het Key tabblad het sleuteltype en geef een naam en bitgrootte op. Voor RSA zijn 2048 bits het minimum.

6. Klik op 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

VCC - certificaatsleutel

7. Navigeer naar Devices > Certificates > Add > New Certificate.

8. Kies Device. Kies onder Cert Enrollment, het gemaakte trustpoint en klik Add zoals in de afbeelding.

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 - Inschrijving certificaat bij FTD

9. Klik op ID, en er wordt een melding getoond om MVO te genereren, kies 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, showing its enrollment type as 'Manual (CA & ID)' and a status message: 'Identity certificate import required'. The interface also includes a search bar, a user profile 'admin', and a 'SECURE' indicator.

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

VCC - Certificaat CA ingeschreven

Warning

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

No

Yes

VCC - CSR genereren

10. Er wordt een MVO gegenereerd die met de bevoegde instantie kan worden gedeeld om het identiteitsbewijs te verkrijgen.

11. Nadat u het identiteitsbewijs van CA in het base64-formaat hebt ontvangen, kiest u dit op de schijf door op Browse Identity Certificate en Import zoals in het beeld te klikken.

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](#)

VCC - Identificatiecertificaat voor invoer

12. Zodra de invoer succesvol is, wordt het trustpointRAVPN-SSL-cert als volgt beschouwd:

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

FMC - Trustpoint inschrijving geslaagd

2. RADIUS-server configureren

2.1. FTD op het VCC beheren

1. Navigeer naar Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.
2. Voer de naam in ISE en voeg RADIUS-servers toe door op + te klikken.

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 - Configuratie van RADIUS-server

3. Vermeld het IP-adres van de ISE Radius-server en het gedeelde geheim (sleutel), dat hetzelfde is als op de ISE-server.

4. Kies Routing of Specific Interface door welke het FTD communiceert met de ISE-server.

5. Klik Save zoals in de afbeelding.

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

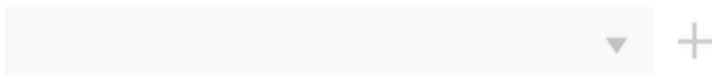
Connect using:

Routing Specific Interface 

outside





Redirect ACL:



Cancel

Save

6. Zodra de server is opgeslagen, wordt deze toegevoegd onder de afbeelding RADIUS Server Group zoals in de afbeelding wordt weergegeven.

RADIUS Server Group		Add RADIUS Server Group	<input type="text" value="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 - RADIUS-servergroep

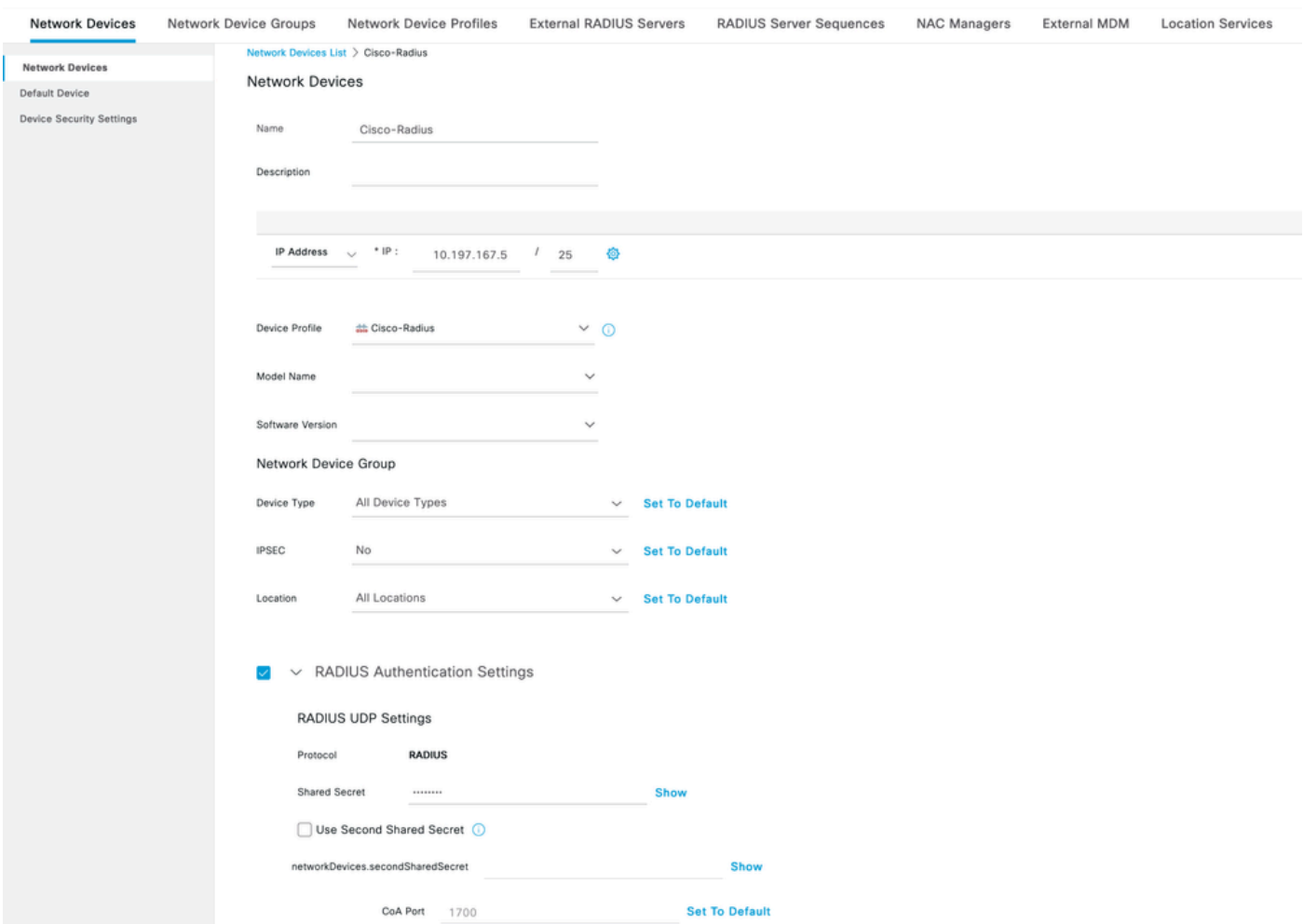
2.2. FTD beheren op ISE

1. Navigeer naar Network Devices en klik op Add.

2. Voer de naam 'Cisco-Radius' in van de server en IP Address van de radiusclient die de FTD-communicatie-interface is.

3. Voeg onder Radius Authentication Settings de Shared Secret code toe.

4. Klik op 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'.
- Network Devices:** Fields for Name (Cisco-Radius) and Description.
- IP Address:** * IP: 10.197.167.5 / 25.
- Device Profile:** Cisco-Radius.
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** Device Type: All Device Types, IPSEC: No, Location: All Locations. Each has a 'Set To Default' link.
- RADIUS Authentication Settings:** Checked. Includes RADIUS UDP Settings with Protocol: RADIUS, Shared Secret (masked), and Use Second Shared Secret (unchecked).
- CoA Port:** 1700.

ISE - netwerkapparaten

5. Ga naar Network Access > Identities > Network Access Users om gebruikers te maken en klik Add op.

6. Maak indien nodig een gebruikersnaam en inlogwachtwoord aan.

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 - gebruikers

7. Om basisbeleid in te stellen, navigeer naar Policy > Policy Sets > Default > Authentication Policy > Default, kies All_User_ID_Stores.

8. Navigeer naar Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, en kies PermitAccesszoals in de afbeelding.

Default

All_User_ID_Stores

> Options

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess

Select from list

ISE - verificatiebeleid

ISE - autorisatiebeleid

3. Maak een adresgroep voor VPN-gebruikers op FMC

1. Navigeer naar Objects > Object Management > Address Pools > Add IPv4 Pools.

2. Voer de naam RAVPN-Pool en het **adresbereik in**; het masker is optioneel.

3. Klik op **Opslaan**.

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

VCC - adresgroep

4. AnyConnect-afbeeldingen uploaden

1. Navigeer naar Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.

2. Voer de naam in anyconnect-win-4.10.07073-webdeploy en klik op Browse om het **AnyConnect**-bestand op de schijf te kiezen. Klik Save zoals in het beeld.

Edit AnyConnect File



Name:*

File Name:*

File Type:*



Description:

FMC - AnyConnect-clientafbeelding

5. XML-profiel maken

5.1. Over de profieeditor

1. Download de Profile Editor van software.cisco.com en open het.
2. Navigeren naar **Server List > Add...**
3. Voer de Display Name RAVPN-IKEV2 en FQDN tezamen met de **User Group** (alias naam) in.
4. Kies het Primaire protocol IPsec , als klik **Ok** zoals in de afbeelding.

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)

Profiel editor - Serverlijst

5. De serverlijst wordt toegevoegd. Sla dit op als 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.

Profiel editor - ClientProfile.xml

5.2. VCC

1. Navigeer naar Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Voer een naam in ClientProfile en klik op Browse om bestand van schijf te kiezen ClientProfile.xml.
3. Klik **Save** op.

Edit AnyConnect File



Name:*

ClientProfile

File Name:*

ClientProfile.xml

Browse..

File Type:*

AnyConnect VPN Profile

Description:

Cancel

Save

FMC - AnyConnect VPN-profiel

6. Externe toegang configureren

1. Navigeer naar Devices > VPN > Remote Accessen klik op + om een verbindingsprofiel toe te voegen zoals in de afbeelding.

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

FMC - profiel voor externe toegangsverbinding

2. Voer de naam van het verbindingsprofiel in RAVPN-IKEV2 en voer een groepsbeleid in door +op te klikken **Group Policy** zoals in de afbeelding.

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 - Groepsbeleid

3. Voer de naam in RAVPN-group-policy en kies de VPN-protocollen **SSL and IPsec-IKEv2** zoals in de afbeelding.

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-protocollen

4. Kies onder AnyConnect > Profile , het XML-profiel ClientProfile uit de vervolgkeuzelijst en klik op Save zoals in de afbeelding.

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-profiel

5. Voeg de adrespool toe RAVPN-Pool door op + as shown in the imagete klikken.

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 - Toewijzing van clientadres

6. Navigeer naar AAA > Authentication Method en kies AAA Only.

7. Kies Authentication Server als 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 - AAA-verificatie

8. Navigeer naar Aliases , voer een aliasnaam in RAVPN-IKEV2 , die wordt gebruikt als gebruikersgroep in ClientProfile.xml.

9. Klik op 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 - Aliassen

10. Navigeer naar Access Interfaces en kies de interface waar RAVPN IKEv2 ingeschakeld moet worden.

11. Kies het identiteitscertificaat voor zowel SSL als IKEv2.

12. Klik op 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 - toegangsinterfaces

13. Navigeer naar Advanced .

14. Voeg de AnyConnect-clientafbeeldingen toe door op + te klikken.

RAVPN-IKEV2 Save Cancel

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

Connection Profile Access Interfaces Advanced

AnyConnect Client Images

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-clientpakket

15. Voeg onderIPsec de afbeelding toeCrypto Maps zoals in de afbeelding.

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 - cryptokaarten

16. Voeg onder IPsec de afbeelding toe IKE Policy door te klikken +.

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-beleid

17. Onder IPsec , voeg de 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-parameters

18. Onder Connection Profile wordt een nieuw profiel RAVPN-IKEV2 gemaakt.

19. SaveClickas op de afbeelding.

RAVPN-IKEV2 You have unsaved changes Save Cancel

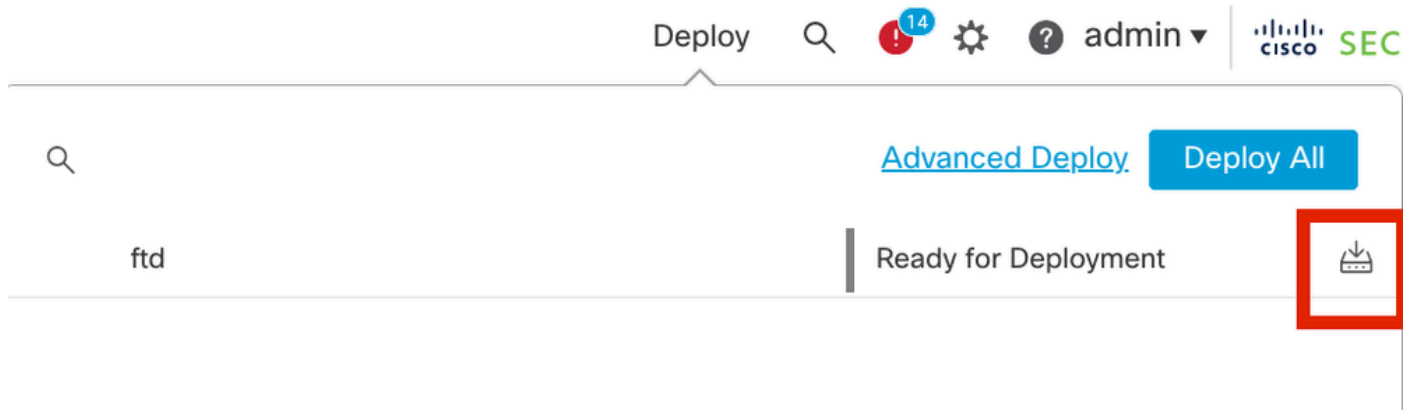
Policy Assignments (1)
Local Realm: None Dynamic Access Policy: None

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 - Verbindingsprofiel RAVPN-IKEV2

20. Stel de configuratie in.



FMC - FTD-implementatie

7. Profielconfiguratie voor AnyConnect

Profiel op pc, opgeslagen onder 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>
```



Opmerking: aanbevolen wordt om de SSL-client uit te schakelen als een tunnelprotocol onder het groepsbeleid zodra het clientprofiel is gedownload naar de pc van alle gebruikers. Dit waarborgt dat gebruikers uitsluitend verbinding kunnen maken met behulp van het IKEv2/IPsec-tunnelprotocol.

Verifiëren

U kunt deze sectie gebruiken om te bevestigen dat uw configuratie correct werkt.

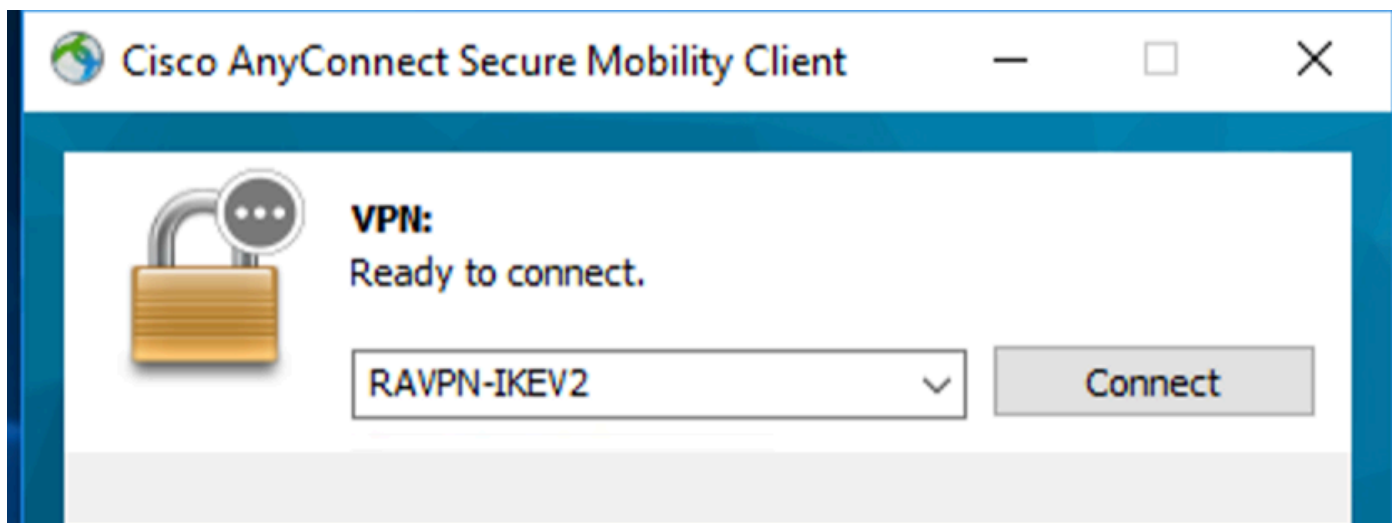
1. Gebruik voor de eerste verbinding de FQDN/IP om via AnyConnect een SSL-verbinding vanaf de pc van de gebruiker tot stand te brengen.
2. Als het SSL-protocol is uitgeschakeld en de vorige stap niet kan worden uitgevoerd, moet u ervoor zorgen dat het clientprofiel ClientProfile.xml op de pc onder het pad C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile aanwezig is.
3. Voer de gebruikersnaam en het wachtwoord voor verificatie in zodra dit wordt gevraagd.

4. Na succesvolle verificatie wordt het clientprofiel gedownload op de pc van de gebruiker.

5. Verbinding met AnyConnect verbreken.

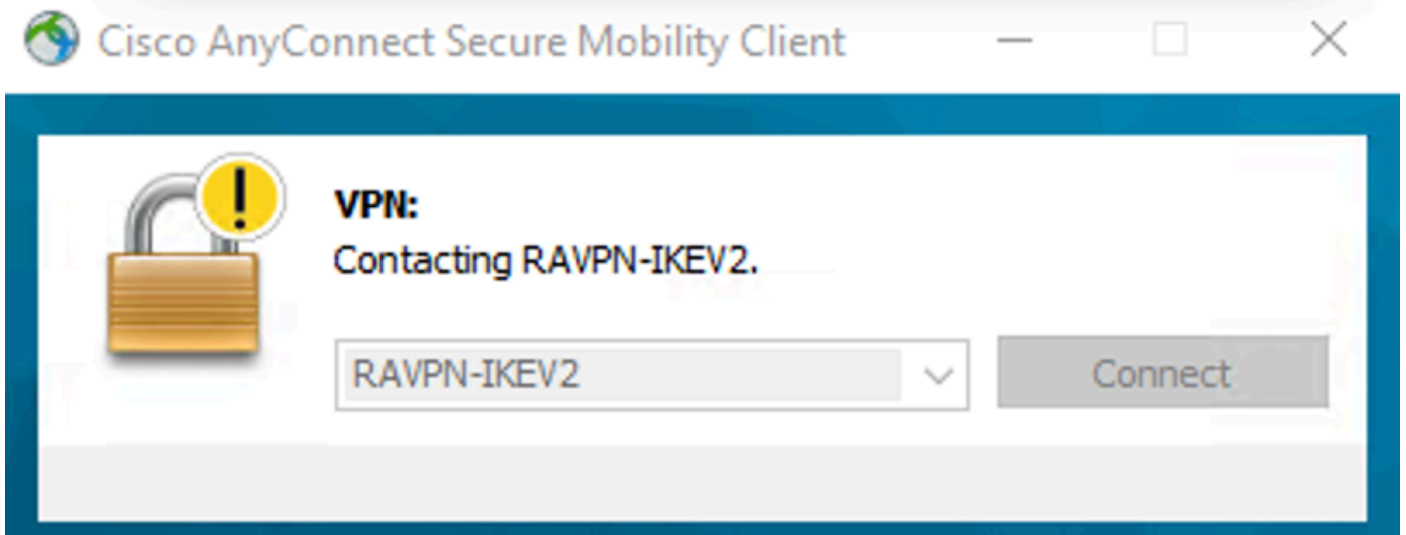
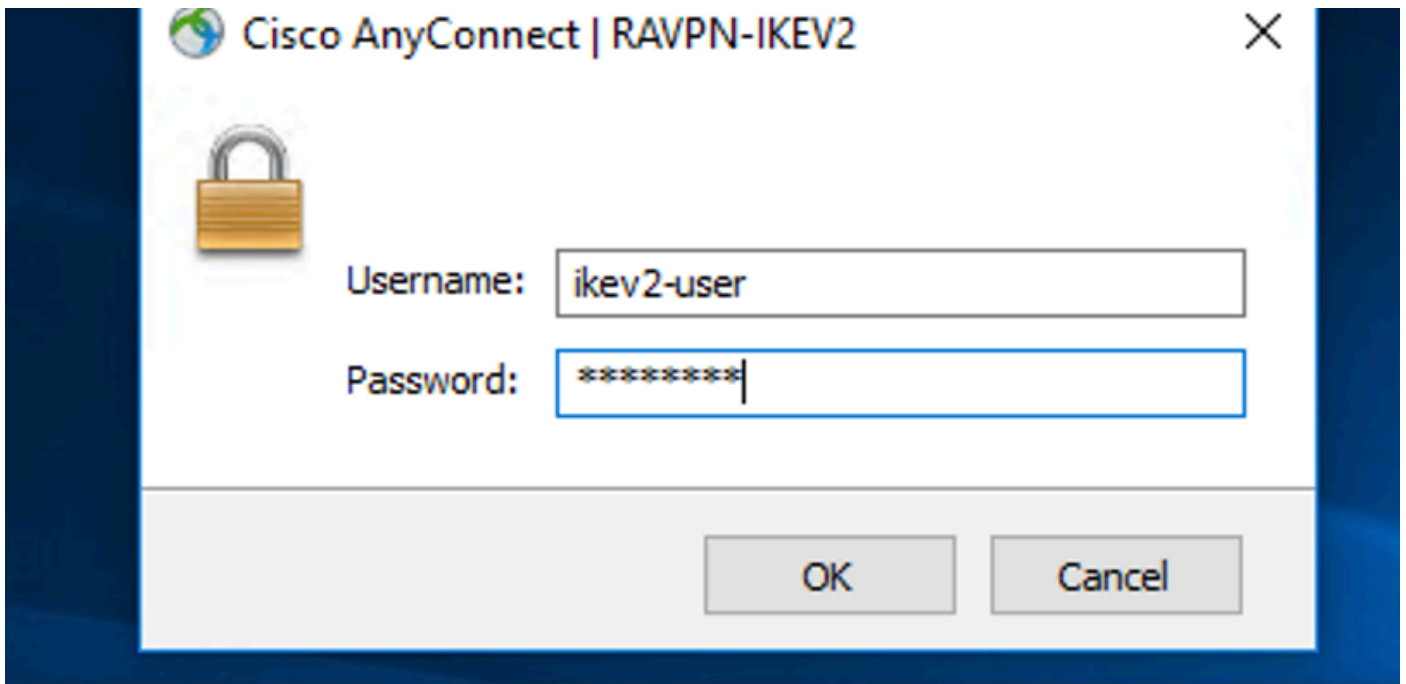
RAVPN-IKEV2 6. Zodra het profiel is gedownload, gebruikt u de vervolgkeuzelijst om de hostnaam te kiezen die in het clientprofiel wordt vermeld, zodat u verbinding kunt maken met AnyConnect via IKEv2/IPsec.

7. Klik op Connect.



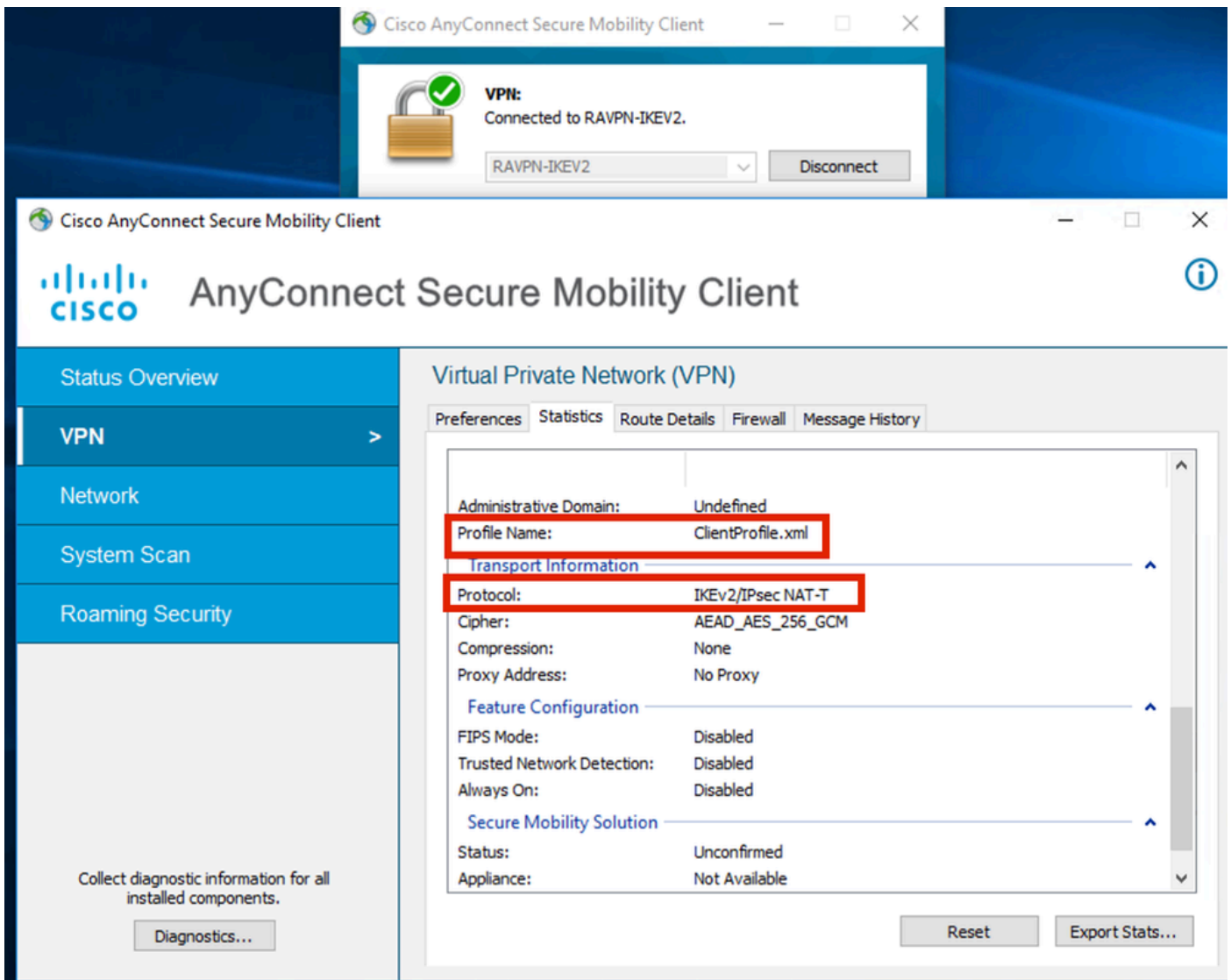
AnyConnect-vervolgkeuzelijst

8. Voer de gebruikersnaam en het wachtwoord in voor verificatie die op de ISE-server is gemaakt.



AnyConnect

9. Controleer het gebruikte profiel en het gebruikte protocol (IKEv2/IPsec) zodra er verbinding mee is gemaakt.



AnyConnect verbonden

FTD CLI-uitgangen:

```
<#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-logbestanden:

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 logs

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

debug radius all

debug crypto ikev2 platform 255

debug crypto ikev2 protocol 255

debug crypto ipsec 255

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.