

Konfigurieren von AnyConnect VPN für FTD über IKEv2 mit ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[1. SSL-Zertifikat importieren](#)

[2. Konfigurieren des RADIUS-Servers](#)

[2.1. FTD auf FMC verwalten](#)

[2.2. FTD auf der ISE verwalten](#)

[3. Adresspool für VPN-Benutzer auf FMC erstellen](#)

[4. AnyConnect-Bilder hochladen](#)

[5. XML-Profil erstellen](#)

[5.1. Auf dem Profileditor](#)

[5.2. Auf FMC](#)

[6. Konfigurieren des Remotezugriffs](#)

[7. AnyConnect-Profilkonfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die grundlegende Konfiguration des Remote Access-VPN mit IKEv2- und ISE-Authentifizierung auf dem vom FMC verwalteten FTD beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes VPN, TLS und Internet Key Exchange Version 2 (IKEv2)
- AAA (Basic Authentication, Authorization, and Accounting) und RADIUS
- Erfahrung mit FirePOWER Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Firepower Threat Defense (FTD) 7.2.0
- Cisco FMC 7.2.0
- AnyConnect 4,10,07073
- Cisco ISE 3.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

IKEv2 und Secure Sockets Layer (SSL) sind Protokolle, die für den Aufbau sicherer Verbindungen verwendet werden, insbesondere im Kontext von VPNs. IKEv2 bietet leistungsstarke Verschlüsselungs- und Authentifizierungsmethoden, die ein hohes Maß an Sicherheit für VPN-Verbindungen bieten.

Dieses Dokument enthält ein Konfigurationsbeispiel für FTD Version 7.2.0 und höher, das den Remotezugriff-VPN ermöglicht, um Transport Layer Security (TLS) und IKEv2 zu verwenden. Als Client kann Cisco AnyConnect verwendet werden, das auf mehreren Plattformen unterstützt wird.

Konfigurieren

1. SSL-Zertifikat importieren

Zertifikate sind unverzichtbar, wenn AnyConnect konfiguriert ist.

Die manuelle Zertifikatregistrierung unterliegt folgenden Einschränkungen:

1. Für FTD ist ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) erforderlich, bevor eine CSR (Certificate Signing Request) generiert wird.
2. Wenn der CSR extern generiert wird, wird eine andere Methode von PKCS12 verwendet.

Es gibt verschiedene Methoden, um ein Zertifikat auf einer FTD-Appliance zu erhalten, aber die sichere und einfache ist, eine CSR zu erstellen und es von einer Zertifizierungsstelle signieren zu lassen. So gehen Sie vor:

1. Navigieren Sie zu **Objects > Object Management > PKI > Cert Enrollment**, und klicken Sie auf **Add Cert Enrollment**.

2. Geben Sie den Namen des Vertrauenspunkts **RAVPN-SSL-cert** ein.

3. Wählen Sie auf der Registerkarte **CA Information** Option **Anmeldungstyp als**, und fügen Sie das Zertifizierungsstellenzertifikat wie im Bild dargestellt ein **Manual**.

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
Y1NjE1WhcNMjkx
MiEvMTY1NiE1WiBvMOswCOYD
```

FMC - CA-Zertifikat

4. Geben Sie unter Certificate Parameters den Betreffnamen ein. Beispiele:

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 - Zertifikatsparameter

5. Unter dem Key Tab, wählen Sie den Schlüsseltyp, und geben Sie einen Namen und Bitgröße. Für RSA sind mindestens 2048 Bit erforderlich.

6. Klicken Sie auf 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 - Zertifikatschlüssel

7. Navigieren Sie zu Devices > Certificates > Add > New Certificate.

8. Wählen Sie Device. Wählen Sie unter Cert Enrollment den erstellten Vertrauenspunkt aus, und klicken Sie Addwie im Bild dargestellt auf.

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 - Registrierung von Zertifikaten für FTD

9. Klicken Sie ID, und eine Aufforderung zur CSR-Generierung wird angezeigt, wählen Sie Yes.

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒

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 - Zertifizierungsstelle angemeldet

Warning

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

No

Yes

FMC - CSR generieren

10. Es wird ein CSR generiert, der für die CA freigegeben werden kann, um das Identitätszertifikat zu erhalten.

11. Nachdem Sie das Identitätszertifikat von CA im Base64-Format erhalten haben, wählen Sie es von der Festplatte aus, indem Sie auf Browse Identity Certificate und klicken, wie im Bild dargestellt Import.

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-----
MIICqjCCAZICAQAwwNjEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQGA1UEAwwNRIRELmNpc2NvLmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPLLwTQ6BkGjER2FfyofT+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 - Identitätszertifikat importieren

12. Sobald der Import erfolgreich ist, wird der VertrauenspunktRAVPN-SSL-cert wie folgt betrachtet:

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

FMC - Trustpoint-Registrierung erfolgreich

2. Konfigurieren des RADIUS-Servers

2.1. FTD auf FMC verwalten

1. Navigieren Sie zu Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group .

2. Geben Sie den Namen ein, und fügen SieISE RADIUS-Server hinzu, indem Sie auf klicken +.

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-Serverkonfiguration

3. Geben Sie die IP-Adresse des ISE Radius-Servers zusammen mit dem gemeinsamen geheimen Schlüssel an, der mit dem Schlüssel auf dem ISE-Server übereinstimmt.

4. Wählen Sie entweder Routing oder Specific Interface aus, über die die FTD mit dem ISE-Server kommuniziert.

5. Klicken Sie Save wie im Bild dargestellt.

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

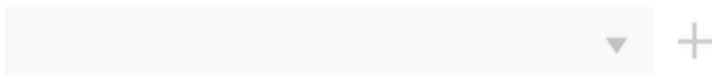
Connect using:

Routing Specific Interface 

outside



Redirect ACL:



Cancel

Save

6. Nach dem Speichern wird der Server RADIUS Server Group wie im Bild dargestellt unter der hinzugefügt.

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 = RADIUS Server Group

2.2. FTD auf der ISE verwalten

1. Navigieren Sie zu Network Devices , und klicken Sie auf Add.

2. Geben Sie den Namen "Cisco-Radius" des Servers und IP Address des Radius-Clients ein, der die FTD-Kommunikationsschnittstelle darstellt.

3. Unter Radius Authentication Settings, fügen Sie die Shared Secret.

4. Klicken Sie auf 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 Address field set to 10.197.167.5 / 25.
- Device Profile**: Set to Cisco-Radius.
- Model Name**: Empty field.
- Software Version**: Empty field.
- 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**:
 - RADIUS UDP Settings**: Protocol set to RADIUS.
 - Shared Secret**: A field with a "Show" link.
 - Use Second Shared Secret (with a help icon).
 - networkDevices.secondSharedSecret**: A field with a "Show" link.
 - CoA Port**: Set to 1700, with a "Set To Default" link.

ISE - Netzwerkgeräte

5. Um Benutzer zu erstellen, navigieren Sie zu Network Access > Identities > Network Access Users, und klicken Sie auf Add.

6. Erstellen Sie nach Bedarf einen Benutzernamen und einAnmeldekennwort.

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 - Benutzer

7. Um eine grundlegende Richtlinie einzurichten, navigieren Sie zu Policy > Policy Sets > Default > Authentication Policy > Default, und wählen Sie All_User_ID_Stores.

8. Navigieren Sie zu Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, und wählen Sie PermitAccess wie im Bild dargestellt aus.

Default

All_User_ID_Stores ▾

> Options 4

ISE - Authentifizierungsrichtlinie

Basic_Authenticated_Access

Network_Access_Authentication_Passed

PermitAccess + ▾

Select from list + ▾ 4

ISE - Autorisierungsrichtlinie

3. Adresspool für VPN-Benutzer auf FMC erstellen

1. Navigieren Sie zu Objects > Object Management > Address Pools > Add IPv4 Pools.
2. Geben Sie den Namen RAVPN-Pool und den **Adressbereich ein**. Die Maske ist optional.
3. Klicken Sie auf **Speichern**.

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 - Adresspool

4. AnyConnect-Bilder hochladen

1. Navigieren Sie zu Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Geben Sie den Namen ein anyconnect-win-4.10.07073-webdeploy und klicken Sie Browse auf, um die **AnyConnect**-Datei von der Festplatte wählen, klicken Sie auf Save wie im Bild gezeigt.

Edit AnyConnect File



Name:*

File Name:*

File Type:*



Description:

FMC - AnyConnect Client-Image

5. XML-Profil erstellen

5.1. Auf dem Profileditor

1. Laden Sie den Profil-Editor von [herunter software.cisco.com](https://software.cisco.com), und öffnen Sie ihn.
2. Navigieren Sie zu **Server List** > **Add...**
3. Geben Sie den Anzeigenamen RAVPN-IKEV2 und FQDN zusammen mit der **Benutzergruppe** (Aliasname) ein.
4. Wählen Sie das primäre Protokoll **IPsec**, asclick **Ok** wie im Bild gezeigt.

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)

Profil-Editor - Serverliste

5. Serverliste wurde hinzugefügt. Speichern Sie es unter 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

Profil-Editor - ClientProfile.xml

5.2. Auf FMC

1. Navigieren Sie zu Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
2. Geben Sie einen Namen ein ClientProfile, und klicken Sie Browse auf, um die Datei von der Festplatte auszuwählen ClientProfile.xml.
3. Klicken Sie auf **Save** .

Edit AnyConnect File



Name:*

File Name:*

File Type:*

Description:

FMC - AnyConnect VPN-Profil

6. Konfigurieren des Remotezugriffs

1. Navigieren Sie zu Devices > VPN > Remote Access und klicken Sie + auf, um ein Verbindungsprofil hinzuzufügen, wie im Bild gezeigt.

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	DFGripPolicy	

FMC - Remote Access Connection-Profil

2. Geben Sie den Namen des Verbindungsprofils ein RAVPN-IKEV2, und erstellen Sie eine Gruppenrichtlinie, indem Sie +wie **Group Policy** im Bild dargestellt auf klicken.

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 - Gruppenrichtlinie

3. Geben Sie den Namen RAVPN-group-policy ein, wählen Sie die VPN-Protokolle **SSL and IPsec-IKEv2** wie im Bild dargestellt.

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-Protokolle

4. Wählen Sie unter AnyConnect > Profile ClientProfile das XML-Profil aus dem Dropdown-Menü aus, und klicken Sie auf, Savewie im Bild dargestellt.

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-Profil

5. Fügen Sie den Adresspool RAVPN-Pool hinzu, indem Sie auf + as shown in the image klicken.

Edit Connection Profile

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
RAVPN-Pool	10.1.1.0-10.1.1.255	 

DHCP Servers: +

Name	DHCP Server IP Address	

Cancel

Save

FMC = Client Address Assignment

6. Navigieren Sie zu AAA > Authentication Method, und wählen Sie AAA Only.

7. Wählen Sie 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-Authentifizierung

8. Navigieren Sie zu, Aliases geben Sie einen Aliasnamen ein RAVPN-IKEV2, der in als Benutzergruppe verwendet wird ClientProfile.xml.

9. Klicken Sie auf 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 - Aliase

10. Navigieren Sie zu Access Interfaces, und wählen Sie die Schnittstelle aus, auf der RAVPN IKEv2 aktiviert werden muss.

11. Wählen Sie das Identitätszertifikat für SSL und IKEv2 aus.

12. Klicken Sie auf 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 = Access Interfaces

13. Navigieren Sie zu Advanced .

14. Fügen Sie die Bilder des AnyConnect-Clients hinzu, indem Sie auf klicken +.

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 Client-Paket

15. UnterIPsec, fügen Sie dieCrypto Maps wie im Bild gezeigt.

RAVPN-IKEV2 Save Cancel

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

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images

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 - Crypto Maps

16. Unter IPsec , fügen Sie die IKE Policy durch Klicken +.

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-Richtlinie

17. Fügen Sie unter IPsec das IPsec/IKEv2 Parameters hinzu.

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images
 Address Assignment Policy
 Certificate Maps
 Group Policies
 LDAP Attribute Mapping
 Load Balancing
 IPsec
 Crypto Maps
 IKE Policy
 IPsec/IKEv2 Parameters

IKEv2 Session Settings

Identity Sent to Peers:

Enable Notification on Tunnel Disconnect
 Do not allow device reboot until all sessions are terminated

IKEv2 Security Association (SA) Settings

Cookie Challenge:

Threshold to Challenge Incoming Cookies: %

Number of SAs Allowed in Negotiation: %

Maximum number of SAs Allowed:

IPsec Settings

Enable Fragmentation Before Encryption
 Path Maximum Transmission Unit Aging

Value Reset Interval: Minutes (Range 10 - 30)

NAT Transparency Settings

Enable IPsec over NAT-T

Note: NAT-Traversal will use port 4500. Ensure that this port number is not used in other services, e.g. NAT Policy.

NAT Keepalive Interval: Seconds (Range 10 - 3600)

FMC - IPsec/IKEv2-Parameter

18. Unter Connection Profile wird neues ProfilRAVPN-IKEV2 erstellt.

19. SaveKlicken Sie auf das Bild.

RAVPN-IKEV2 You have unsaved changes Save Cancel

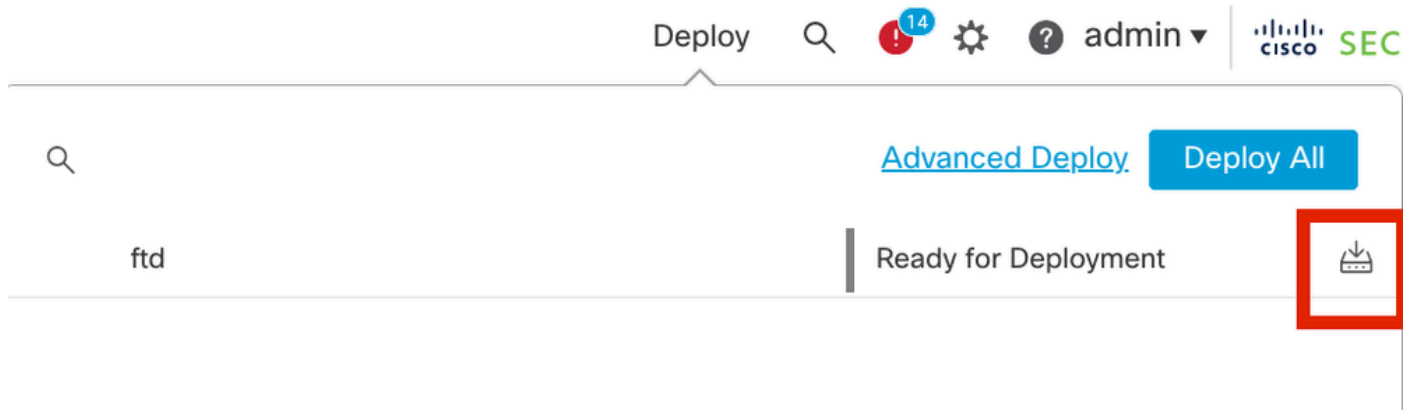
Policy Assignments (1)
Local Realm: None Dynamic Access Policy: None

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 - Verbindungsprofil RAVPN-IKEV2

20. Bereitstellen der Konfiguration.



FMC - FTD-Bereitstellung

7. AnyConnect-Profilkonfiguration

Profil auf dem PC, gespeichert unter 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>
```



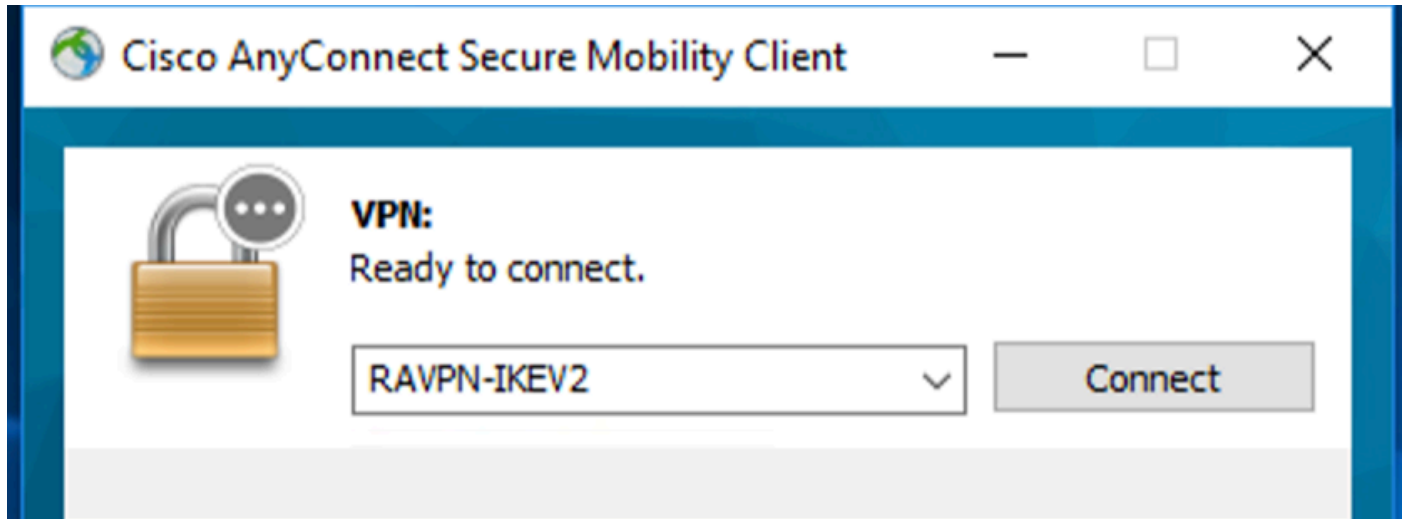
Hinweis: Es wird empfohlen, den SSL-Client als Tunneling-Protokoll in der Gruppenrichtlinie zu deaktivieren, sobald das Client-Profil auf den PC aller Benutzer heruntergeladen wurde. Dadurch wird sichergestellt, dass Benutzer ausschließlich über das IKEv2/IPsec-Tunneling-Protokoll eine Verbindung herstellen können.

Überprüfung

In diesem Abschnitt können Sie überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

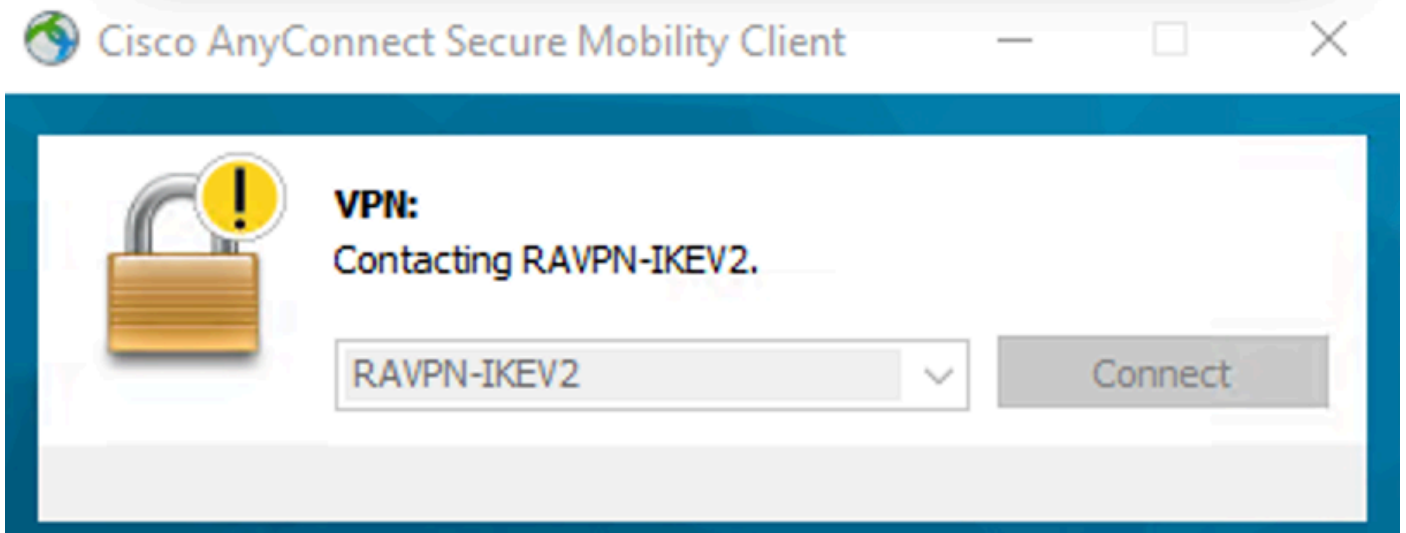
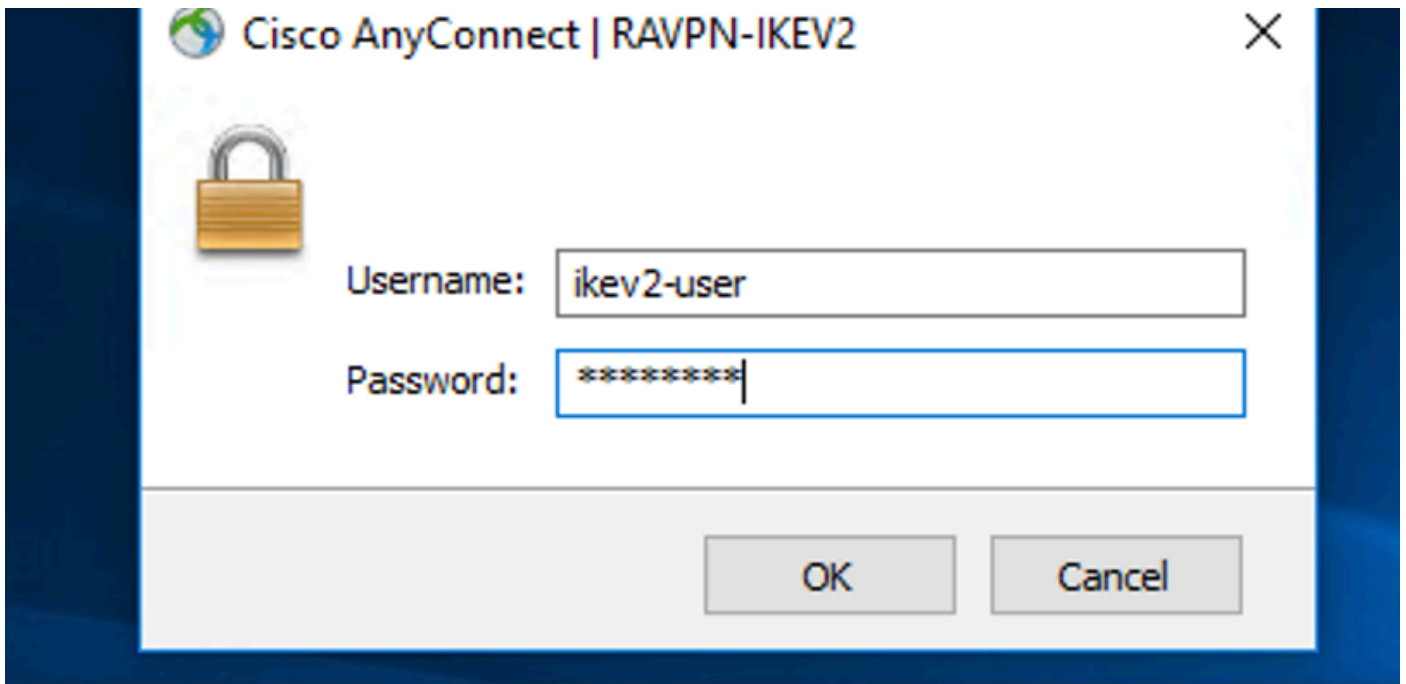
1. Verwenden Sie für die erste Verbindung den FQDN/IP, um eine SSL-Verbindung vom PC des Benutzers über AnyConnect herzustellen.
2. Wenn das SSL-Protokoll deaktiviert ist und der vorherige Schritt nicht ausgeführt werden kann, stellen Sie sicher, dass das ClientprofilClientProfile.xml auf dem PC unter dem Pfad C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile vorhanden ist.

3. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung ein, sobald Sie dazu aufgefordert werden.
4. Nach erfolgreicher Authentifizierung wird das Client-Profil auf den PC des Benutzers heruntergeladen.
5. Trennen Sie die Verbindung zu AnyConnect.
6. Nachdem das Profil heruntergeladen wurde, wählen Sie den im Clientprofil erwähnten Hostnamen über das Dropdown-Menü aus, **RAVPN-IKEV2** um eine Verbindung mit AnyConnect über IKEv2/IPsec herzustellen.
7. Klicken Sie auf Connect.



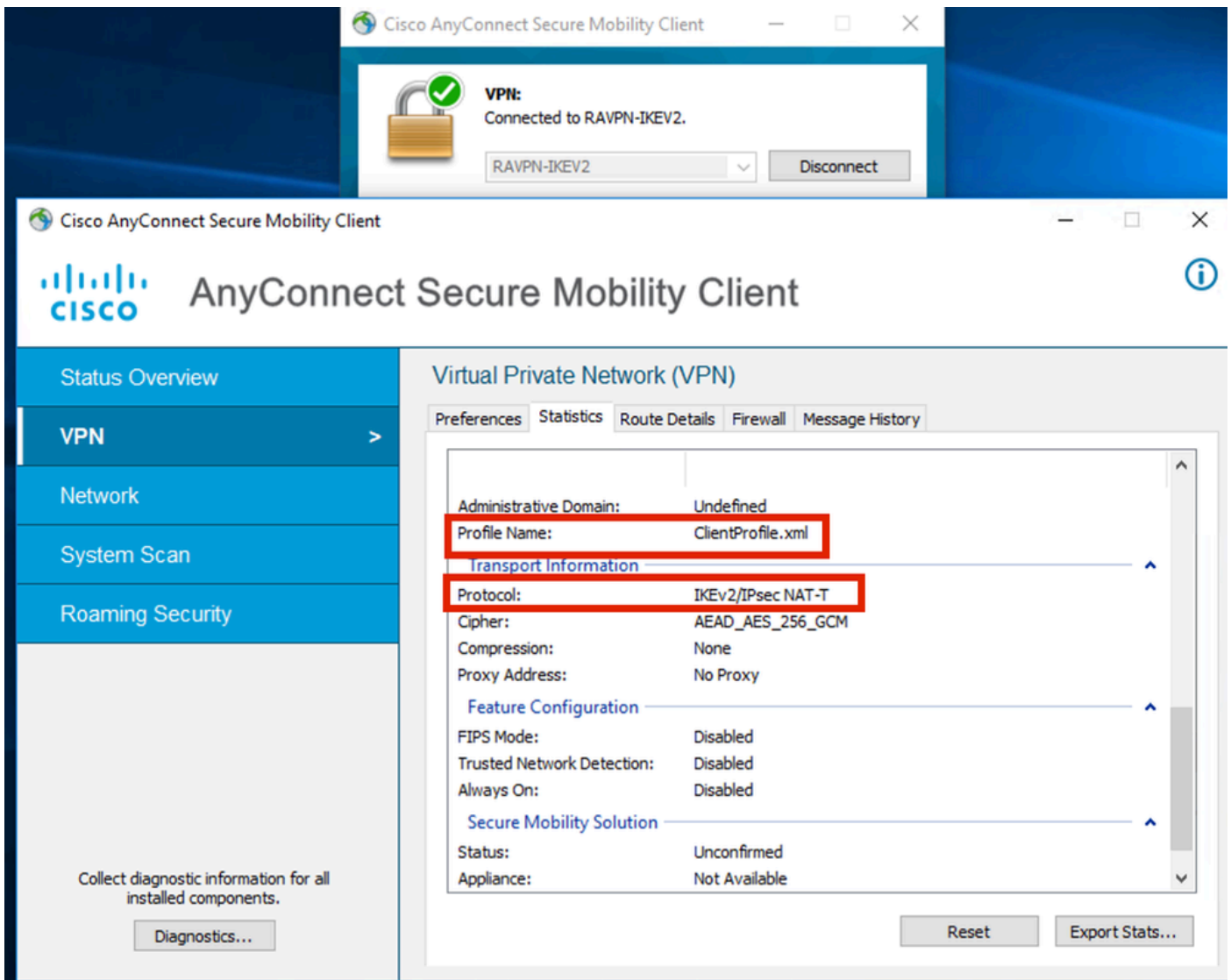
AnyConnect-Dropdown

8. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung ein, die auf dem ISE-Server erstellt wurde.



AnyConnect-Verbindung

9. Überprüfen Sie das Profil und Protokoll (IKEv2/IPsec), das nach dem Herstellen der Verbindung verwendet wird.



AnyConnect verbunden

FTD CLI-Ausgänge:

```
<#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-Protokolle:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Pr	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-Protokolle

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

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


Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.