

# Toewijzing van RADIUS-kenmerken configureren voor FlexVPN-externe gebruikers

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Routerconfiguratie](#)

[Configuratie van Identity Services Engine \(ISE\)](#)

[Clientconfiguratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Debugs en logbestanden](#)

[Werkscenario](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u FlexVPN kunt configureren met Cisco Identity Services Engine (ISE) om identiteiten te verifiëren en kenmerkende groepstoewijzing uit te voeren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Remote Access Virtual Private Network (RAVPN) met configuratie van IKEV2/IPsec op een Cisco IOS® XE-router via CLI
- Configuratie van Cisco Identity Services Engine (ISE)
- Cisco Secure-client (CSC)
- RADIUS-protocol

### Gebruikte componenten

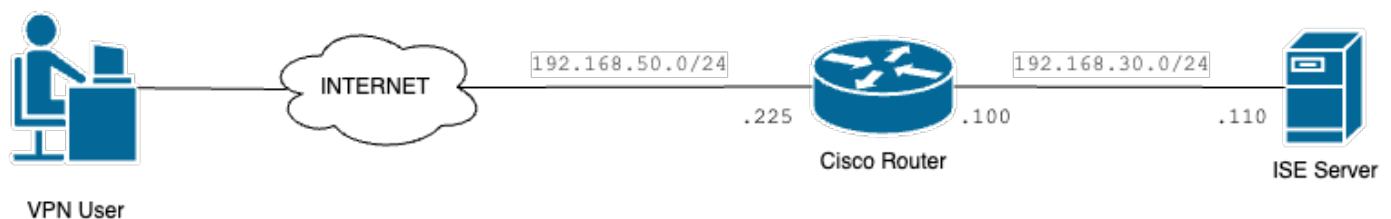
Dit document is gebaseerd op deze software- en hardwareversies:

- Cisco CRS-1000V (VXE) - versie 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1
- Cisco Secure Client (CSC) - versie 5.0.05040
- Windows 11

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.

## Configureren

### Netwerkdigram



Basis netwerkdigram

## Configuraties

### Routerconfiguratie

Stap 1. Een RADIUS-server configureren voor verificatie en lokale autorisatie op het apparaat:

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

De opdracht `aaa authenticatie login <list_name>` verwijst naar de groep verificatie, autorisatie en accounting (AAA) (die de RADIUS-server definieert).

In het lokale opdracht netwerk `<list_name>` staat dat lokaal gedefinieerde gebruikers/groepen moeten worden gebruikt.

Stap 2. Configureer een trustpoint om het routercertificaat op te slaan. Aangezien de lokale verificatie van de router het type RSA is, vereist het apparaat dat de server zichzelf verifieert met behulp van een certificaat:

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsakeypair FlexVPN_KEY
```

Stap 3. Definieer een lokale IP-pool voor elke verschillende gebruikersgroep:

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

Stap 4. Configureer het lokale autorisatiebeleid:

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

Er is geen configuratie vereist in het autorisatiebeleid, aangezien de verificatieserver verantwoordelijk is voor het verzenden van de relevante waarden (DNS, pool, beschermde routes, enzovoort) die zijn gebaseerd op de groep waartoe de gebruiker behoort. Echter, het moet worden geconfigureerd om de gebruikersnaam te definiëren in onze lokale autorisatiedatabank.

Stap 5 (optioneel). Een IKEv2-voorstel en -beleid maken (als deze niet zijn geconfigureerd, worden slimme standaardwaarden gebruikt):

```
crypto ikev2 proposal IKEv2-prop
encryption aes-cbc-256
integrity sha256
group 14
```

```
crypto ikev2 policy IKEv2-pol
proposal IKEv2-prop
```

Stap 6 (optioneel). Configureer de transformatie-set (indien niet geconfigureerd, worden slimme standaardwaarden gebruikt):

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

Stap 7. Configureer een IKEv2-profiel met de juiste lokale en externe identiteiten,

verificatiemethoden (lokaal en extern), trustpoint, AAA en de virtuele sjablooninterface die voor de verbindingen wordt gebruikt:

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

De opdracht `aaa autorisatiegebruiker eap cached` specificeert dat de attributen die tijdens EAP-verificatie worden ontvangen, moeten worden gecached. Deze opdracht is essentieel voor de configuratie omdat zonder deze opdracht de gegevens die door de verificatieserver worden verzonden niet worden gebruikt, wat leidt tot een mislukte verbinding.



Opmerking: de externe key-id moet overeenkomen met de key-id waarde in het XML-bestand. Als de standaard waarde (\*\$AnyConnectClient\$\*) niet wordt aangepast in het XML-bestand, wordt deze gebruikt en moet deze worden geconfigureerd in het IKEv2-profiel.

---

Stap 8. Configureer een IPsec-profiel en wijs de transformatie-set en het IKEv2-profiel toe:

```
crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile
```

Stap 9. Configureer een loopback-interface. De Virtual-Access interfaces lenen het IP-adres uit:

```
interface Loopback100
```

```
ip address 10.0.0.1 255.255.255.255
```

Stap 10. Maak de virtuele sjabloon die gebruikt gaat worden om de verschillende virtuele toegangsinterfaces te maken en koppel het IPSec-profiel dat bij stap 8 gemaakt wordt:

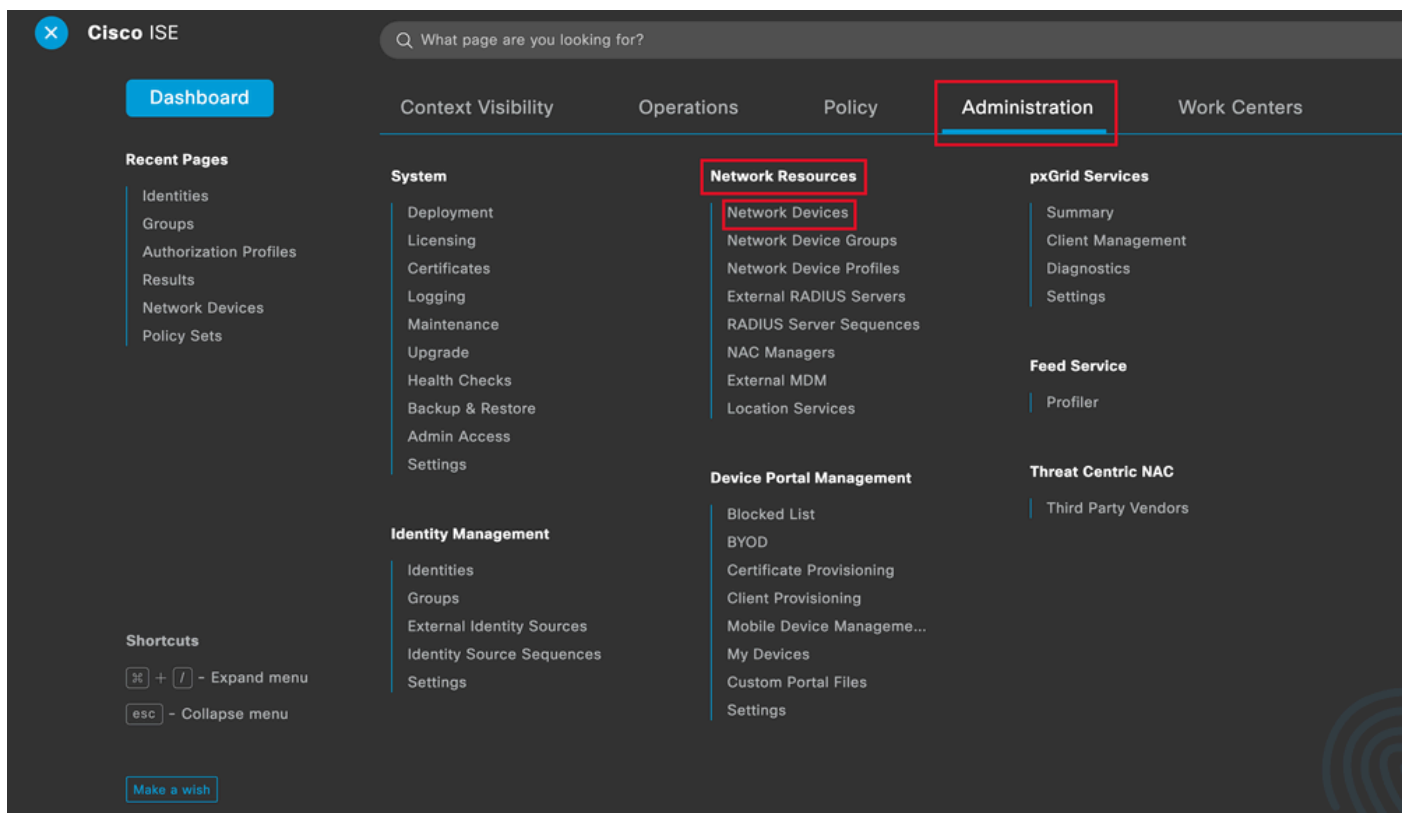
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

Stap 11. Schakel op HTTP-URL gebaseerde certificaat lookup en HTTP-server op de router uit:

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

## Configuratie van Identity Services Engine (ISE)

Stap 1. Log in op de ISE-server en navigeer naar Beheer > Netwerkbronnen > Netwerkkapartaten:



Algemene menu ISE

Stap 2. Klik op Add om de router als AAA-client te configureren:

Network Devices

Selected 0 Total 1

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
CISCO_ROUTER		Cisco	All Locations	All Device Types	

Een nieuw netwerkapparaat toevoegen

Voer in de velden Naam netwerkapparaat en IP-adres in en controleer vervolgens het vakje RADIUS-verificatie-instellingen en voeg het gedeelde geheim toe, deze waarde moet dezelfde zijn als die werd gebruikt toen het RADIUS-serverobject op de router werd gemaakt.

## Network Devices

Name

Description

IP Address

Naam en IP-adres



## ✓ RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

Show

Use Second Shared Secret ⓘ

networkDevices.secondSharedSecret

Show

RADIUS-wachtwoord

Klik op Save (Opslaan).

Stap 3. Ga naar Beheer > Identity Management > Groepen:

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. The left sidebar has 'Recent Pages' (Identities, Groups, Authorization Profiles, Results, Policy Sets) and 'Shortcuts' (Expand menu, Collapse menu). The main content area is divided into several sections: 'System' (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), 'Network Resources' (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), 'Device Portal Management' (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Manageme..., My Devices, Custom Portal Files, Settings), 'pxGrid Services' (Summary, Client Management, Diagnostics, Settings), 'Feed Service' (Profiler), and 'Threat Centric NAC' (Third Party Vendors). In the 'System' section, 'Identity Management' and 'Groups' are highlighted with red boxes.

Algemene menu ISE

Stap 4. Klik op Gebruikersidentiteitsgroepen en klik vervolgens op Toevoegen:



## Identity Groups

EQ



> Endpoint Identity Groups

> **User Identity Groups**

## User Identity Groups

Selected 0 Total 10

Edit **+ Add** Delete Import Export

All Filter

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group

Een nieuwe groep toevoegen

Voer de naam van de groep in en klik op Indienen.

### Identity Group

\* Name

Description

**Submit**

Cancel

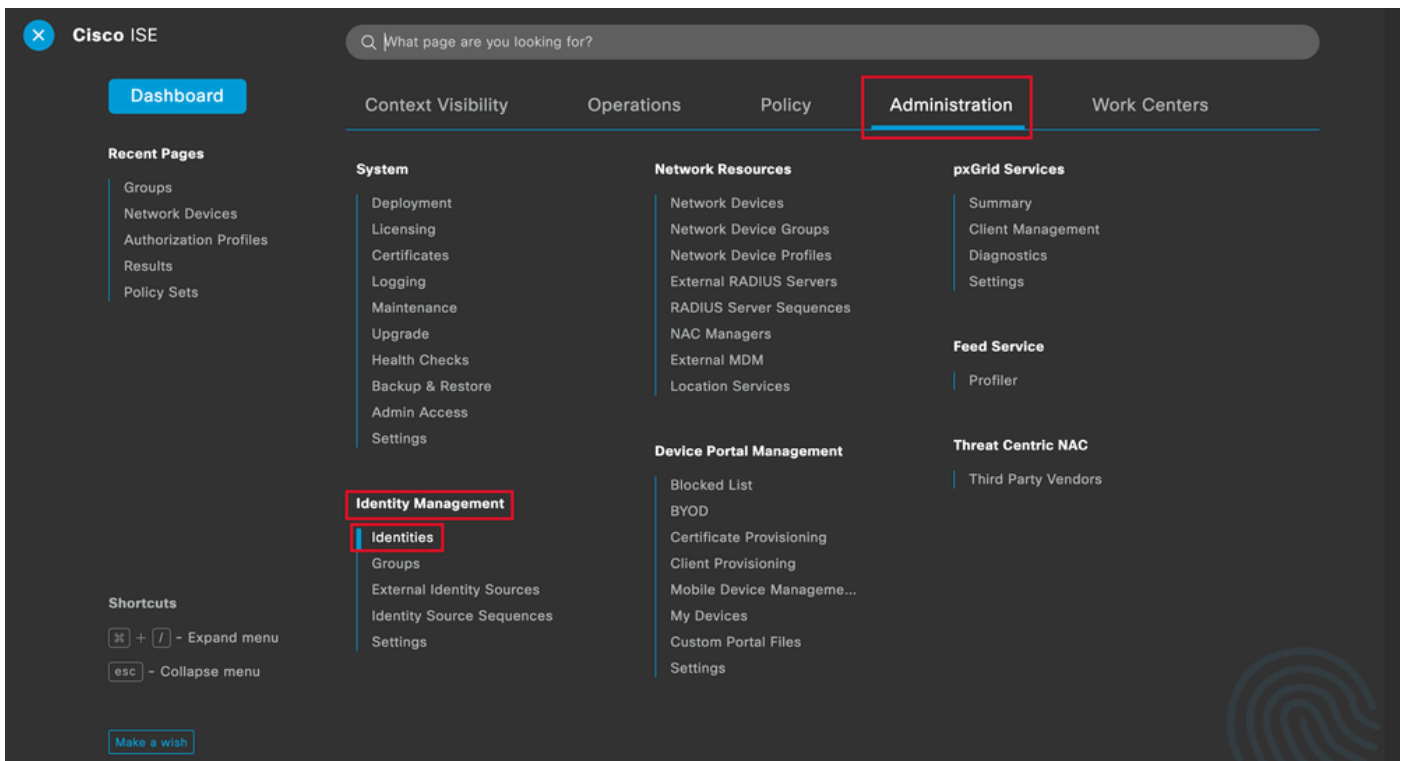
Groepsinformatie



Opmerking: Herhaal stap 3 en 4 om zo veel groepen te maken als nodig is.

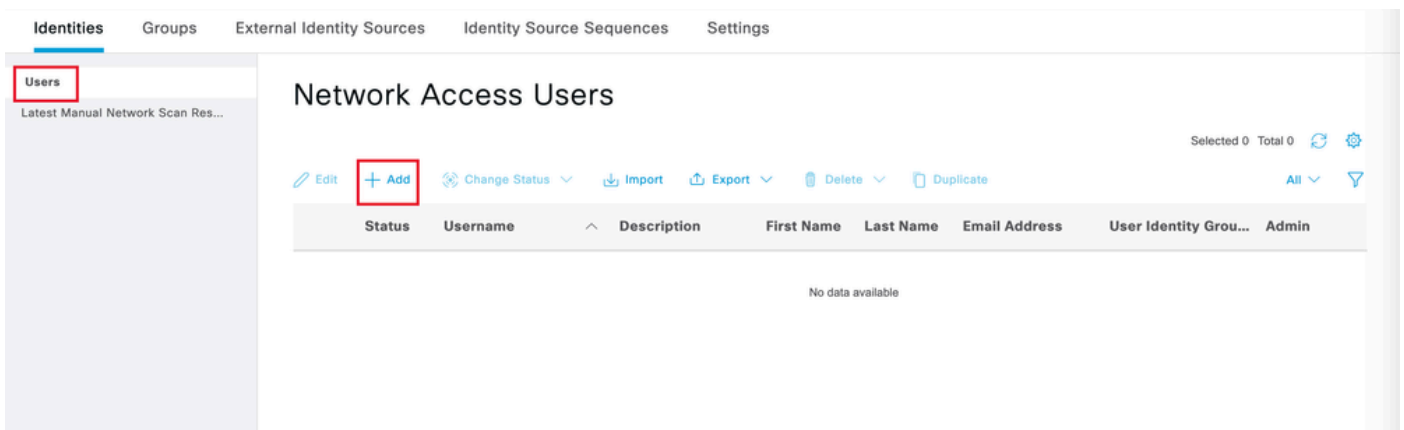
---

Stap 5. Navigeren naar Administratie > Identiteitsbeheer > Identiteiten:



Algemene menu ISE

Stap 6. Klik op Add om een nieuwe gebruiker te maken in de lokale database van de server:



Een gebruiker toevoegen

Voer de gebruikersnaam en het inlogwachtwoord in. Blader vervolgens naar het einde van deze pagina en selecteer de Gebruikersgroep:

Network Access User

\* Username user1

Status  Enabled

Email

Passwords

Password Type: Internal Users

Password

Re-Enter Password

\* Login Password .....

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Gebruikersnaam en wachtwoord

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 20

User Groups

User Groups

EQ

< [icon] [gear]

- ALL\_ACCOUNTS (default)
- Employee
- Group1**
- Group2
- GROUP\_ACCOUNTS (default)

Select an item

De juiste groep toewijzen aan de gebruiker

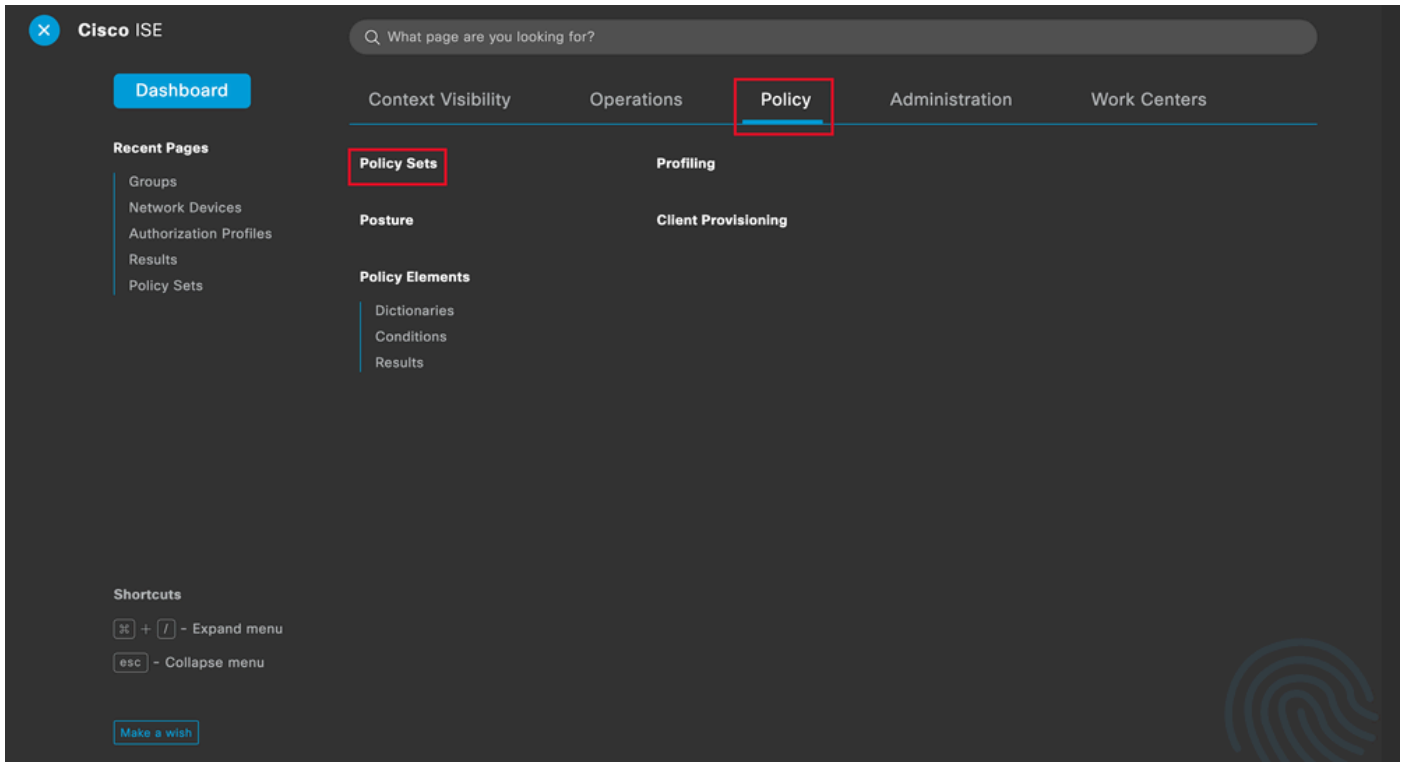
Klik op Save (Opslaan).



Opmerking: Herhaal stap 5 en 6 om de gewenste gebruikers te maken en ze toe te wijzen aan de corresponderende groep.

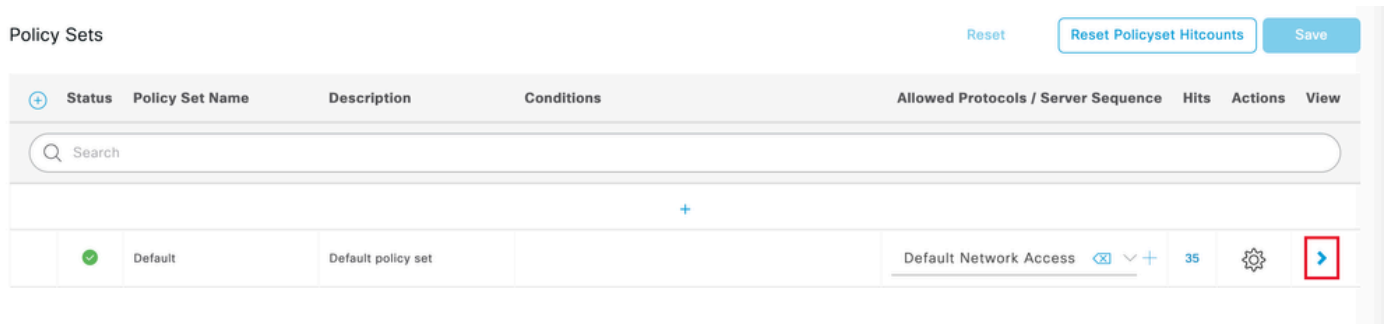
---

Stap 7. Ga naar Policy > Policy Sets:



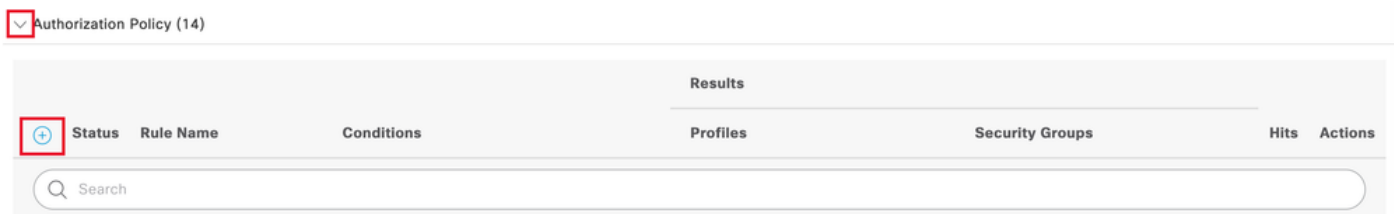
Algemene menu ISE

Selecteer het standaard autorisatiebeleid door op de pijl rechts op het scherm te klikken:



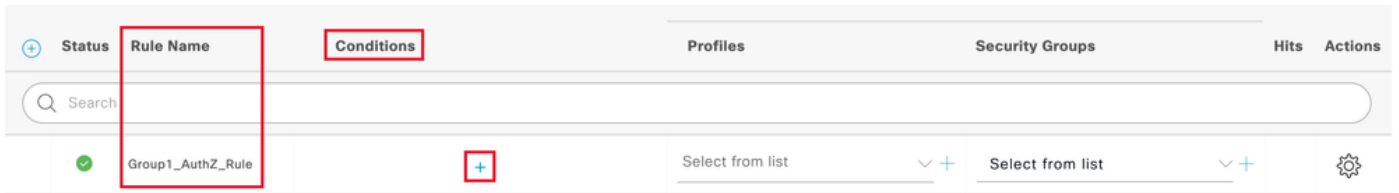
Selecteer het autorisatiebeleid

Stap 8. Klik op het pijltje van het vervolgkeuzemenu naast Autorisatiebeleid om dit uit te vouwen. Klik vervolgens op het pictogram Add (+) om een nieuwe regel toe te voegen:



Een nieuwe autorisatieregel toevoegen

Voer de naam voor de regel in en selecteer het pictogram Add (+) onder de kolom Voorwaarden:



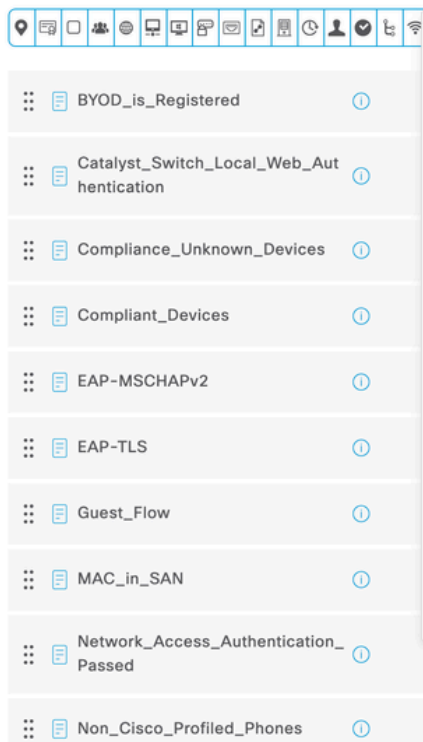
Een voorwaarde toevoegen

Stap 9. Klik in het tekstvak Attributeneditor en klik op het pictogram Identity group. Selecteer het kenmerk Identiteitsgroep - Naam:

## Conditions Studio

### Library

Search by Name



### Editor

Click to add an attribute

#### Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
IdentityGroup	Name		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

Selecteer de voorwaarde

Selecteer Gelijk aan de operator en klik vervolgens op het pijltje van het vervolgkeuzemenu om de beschikbare opties weer te geven en selecteer Gebruikersidentiteitsgroepen:<GROUP\_NAME>.

## Editor

IdentityGroup-Name

Equals

Choose from list or type

Set to 'Is not'

User Identity Groups:GROUP\_ACCOUNTS (default)

User Identity Groups:Group1

User Identity Groups:Group2

User Identity Groups:GuestType\_Contractor (default)

User Identity Groups:GuestType\_Daily (default)

Save

Selecteer de groep

Klik op Save (Opslaan).

Stap 10. Klik in de kolom Profielen op het pictogram Toevoegen (+) en kies Een nieuw autorisatieprofiel maken:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Group1_AuthZ_Rule	IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list	Select from list	10	⚙️
✓	Wireless Black List Default	Wireless_Access AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Create a New Authorization Profile	Select from list	0	⚙️

Het autorisatieprofiel maken

Voer de naam van het profiel in



# Add New Standard Profile

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

### Profielinformatie

Navigeer naar het einde van deze pagina naar Advanced Attribute Settings en klik op het pijltje van het vervolgkeuzemenu. Klik vervolgens op Cisco en selecteer cisco-av-pair--[1]:

Advanced Attributes Settings

Select an item

Cisco

- cisco-abort-cause--[21]
- cisco-account-info--[250]
- cisco-assign-ip-pool--[218]
- cisco-av-pair--[1]**
- cisco-call-filter--[243]
- cisco-call-id--[141]

Attributes Details

Access Type = ACCESS\_ACCEPT

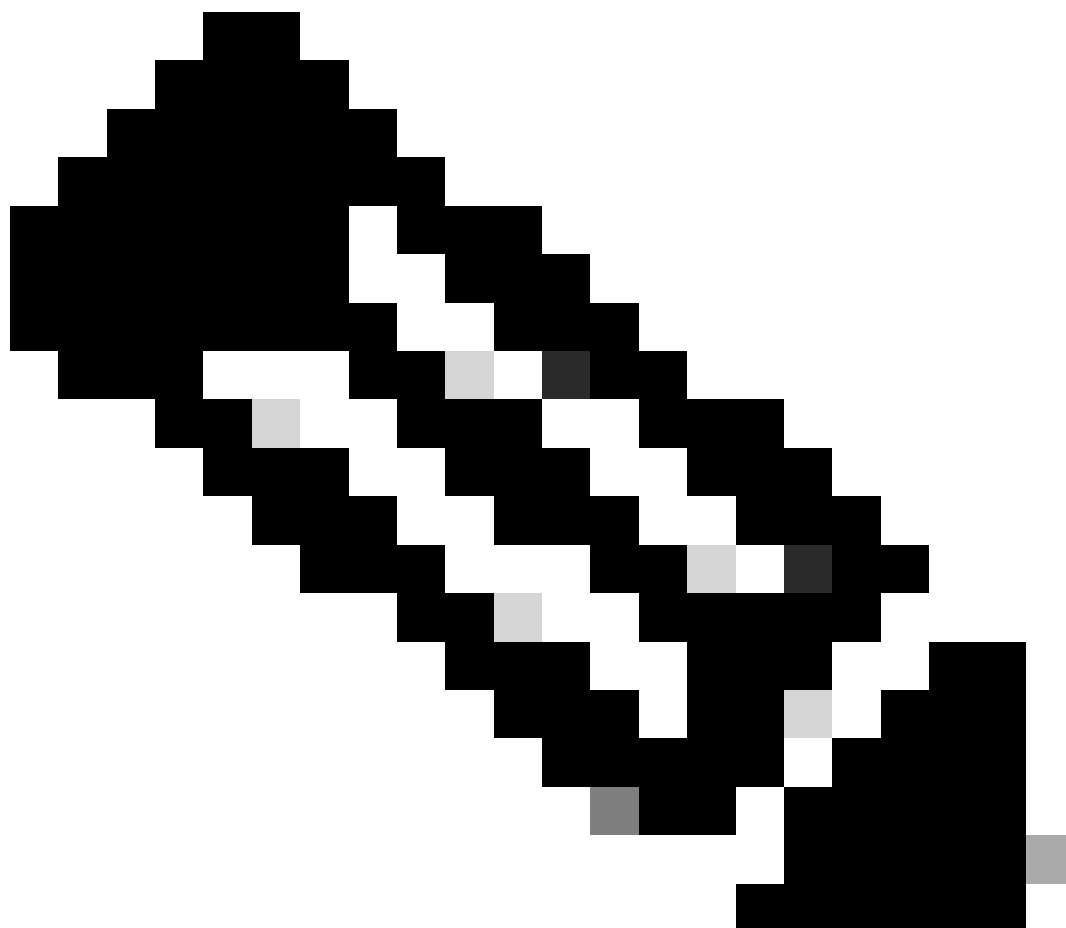
Selecteer het type kenmerk

Voeg het cisco-av-paar attribuut toe dat u wilt configureren en klik op het pictogram Add (+) om een ander attribuut toe te voegen:

### Advanced Attributes Settings

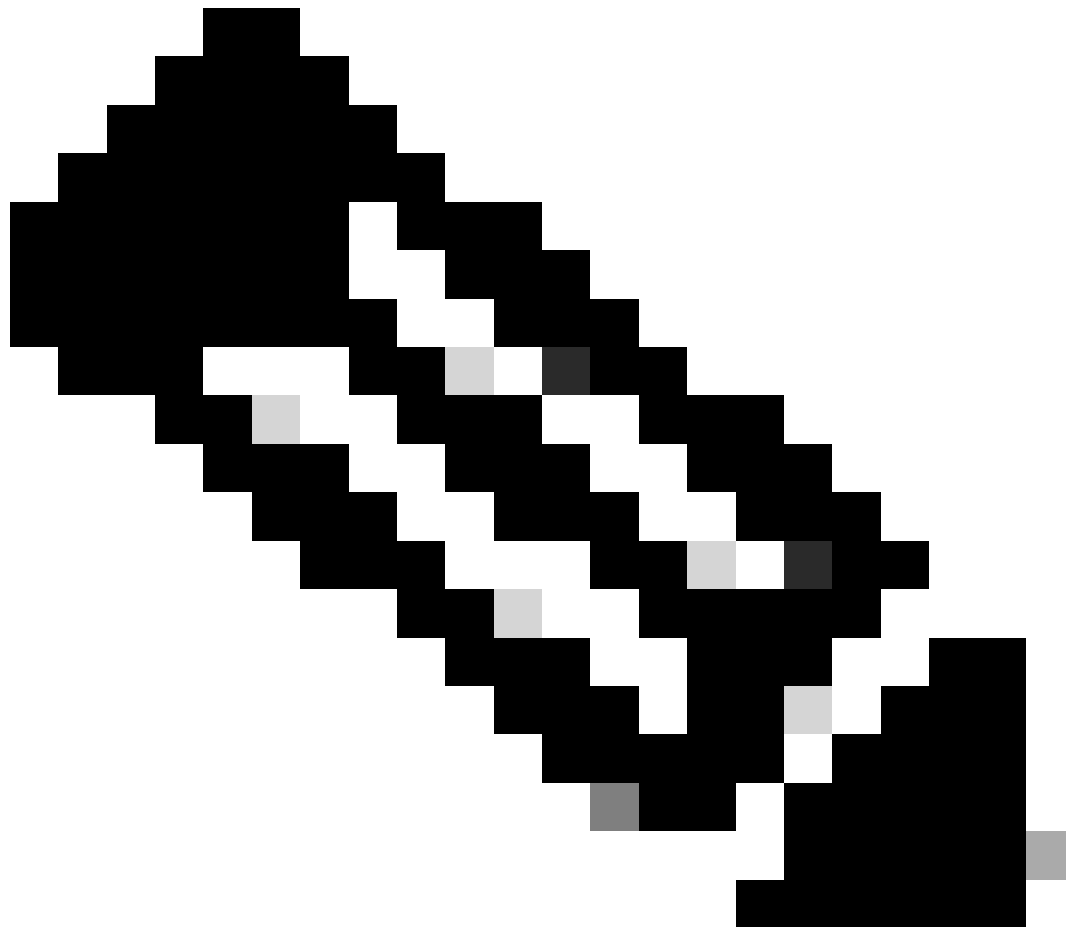
☰ Cisco:cisco-av-pair ▾ = ipsec:dns-servers=10.0.50.10 ▾ - +

Het kenmerk configureren



Opmerking: Raadpleeg voor specificaties van kenmerken (naam, syntaxis, beschrijving, voorbeeld, enz.) de configuratiehandleiding van FlexVPN RADIUS-kenmerken:

[Configuratiehandleiding voor FlexVPN en Internet Key Exchange versie 2, Cisco IOS XE](#)



N.B.: Herhaal de vorige stap om de benodigde kenmerken te maken.

---

Klik op Save (Opslaan).

De volgende attributen werden toegewezen aan elke groep:

- Eigenschappen van groep 1:

Advanced Attributes Settings

⋮	Cisco:cisco-av-pair	▼	=	ipsec:dns-servers=10.0.50.10	▼	—
⋮	Cisco:cisco-av-pair	▼	=	ipsec:route-set=prefix 192.168.100.0/24	▼	—
⋮	Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=group1	▼	— +

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.101  
cisco-av-pair = ipsec:route-set=prefix 192.168.100.0/24  
cisco-av-pair = ipsec:addr-pool=group1

Groep1-kenmerk

- Eigenschappen groep 2:

Advanced Attributes Settings

⋮	Cisco:cisco-av-pair	▼	=	ipsec:dns-servers=10.0.50.20	▼	—
⋮	Cisco:cisco-av-pair	▼	=	ipsec:route-set=prefix 192.168.200.0/24	▼	—
⋮	Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=group2	▼	— +

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.202  
cisco-av-pair = ipsec:route-set=prefix 192.168.200.0/24  
cisco-av-pair = ipsec:addr-pool=group2

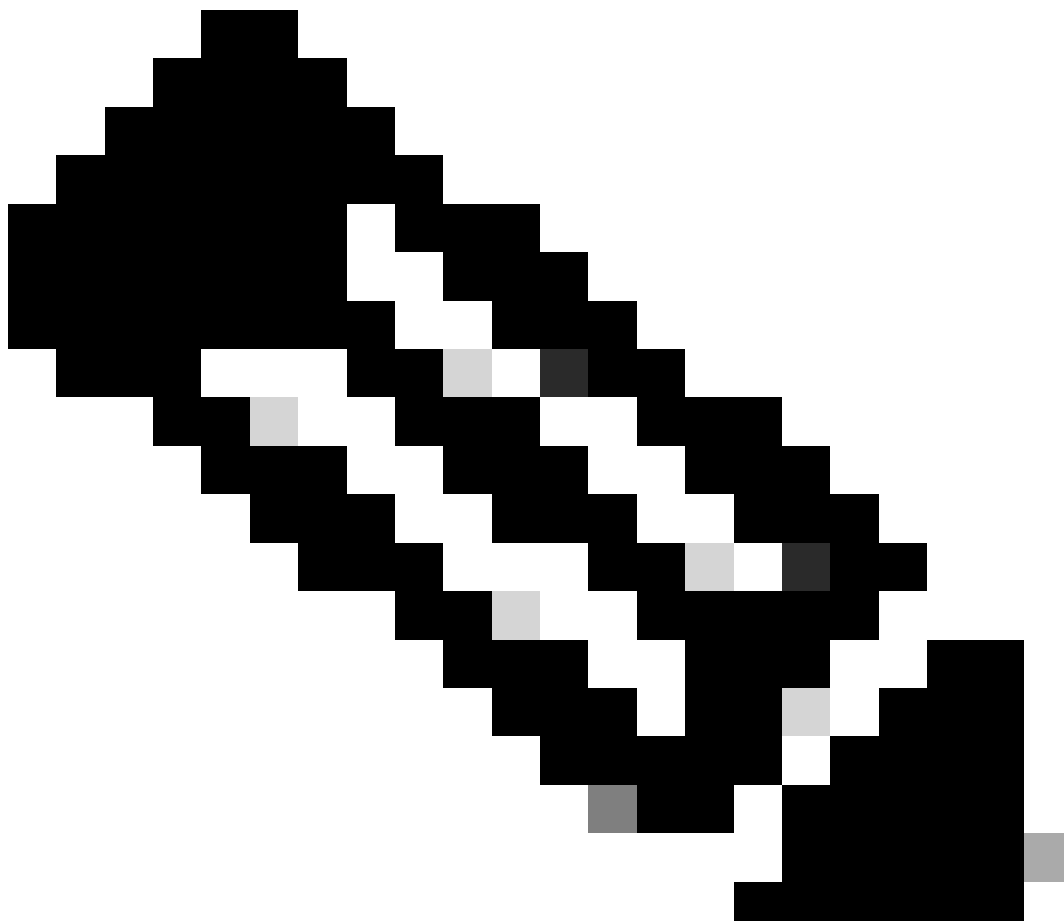
Groep2-kenmerken

Stap 1. Klik op de pijl van het vervolgkeuzemenu en selecteer het autorisatieprofiel dat is gemaakt in stap 10:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Group1_AuthZ_Rule	IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list	Select from list	10	⚙️
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DenyAccess NSP_Onboard Non_Cisco_IP_Phones PermitAccess Profile_group1	Select from list	0	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Non_Cisco_IP_Phones	Select from list	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0	⚙️

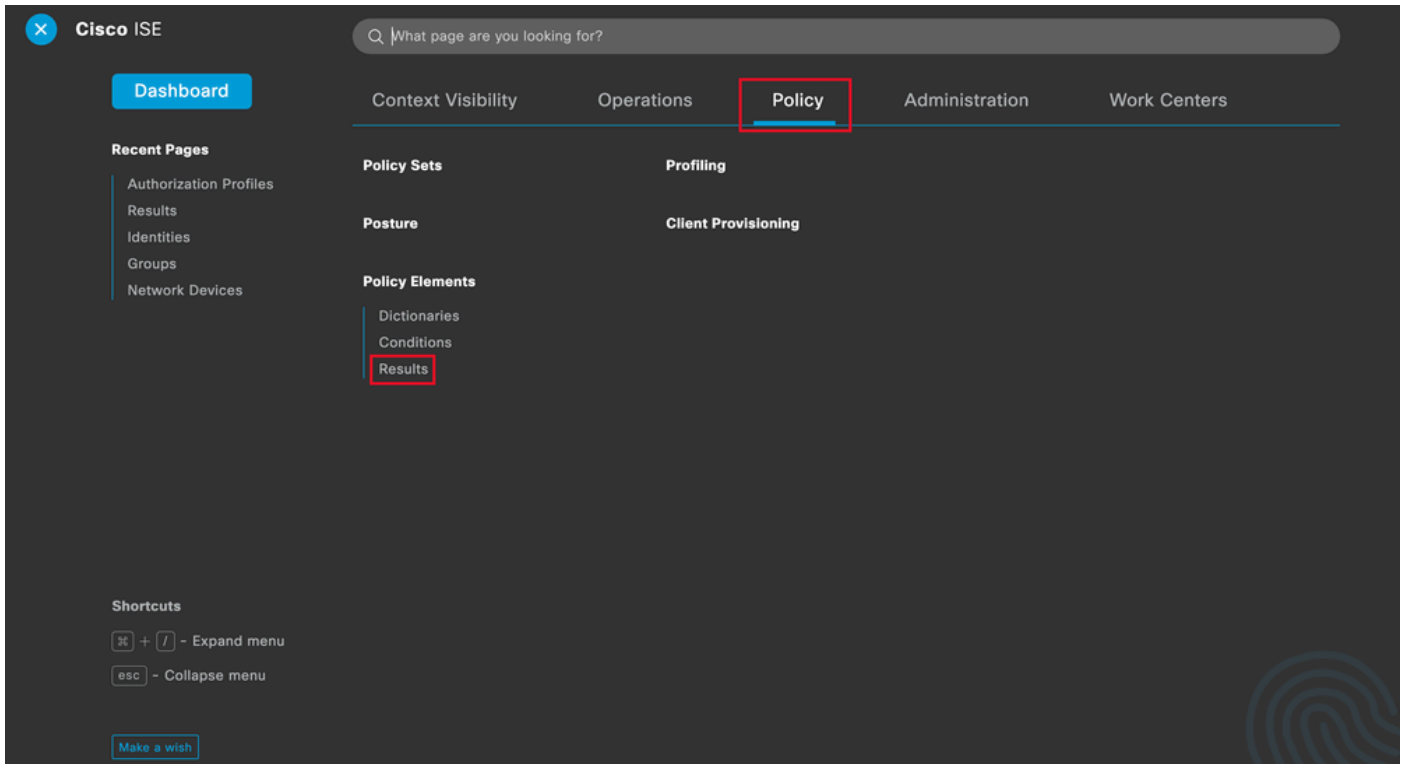
Vergunningsprofiel toewijzen

Klik op Save (Opslaan).



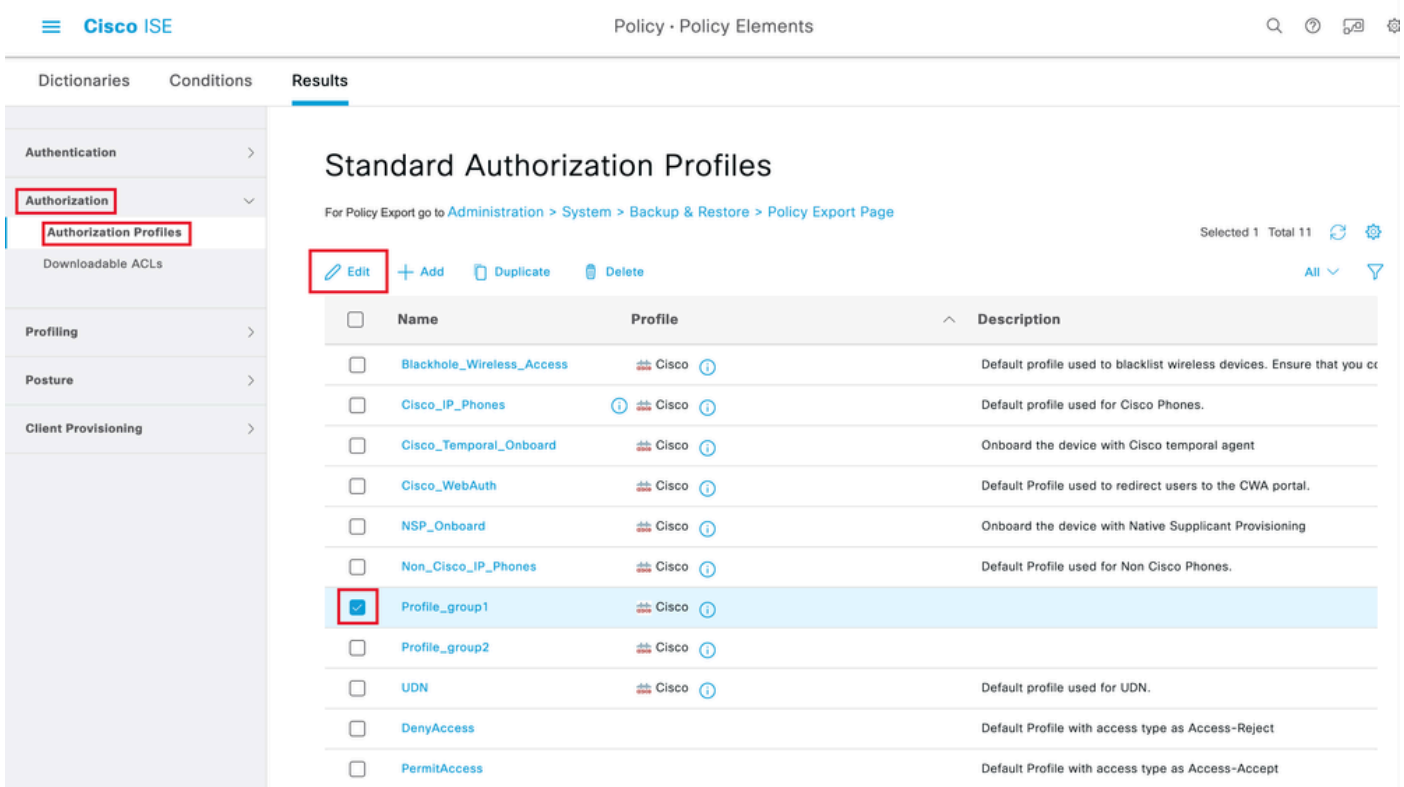
Opmerking: Herhaal stap 8 t/m 11 om voor elke groep de benodigde autorisatieregels te maken.

Stap 12 (facultatief). Als u het autorisatieprofiel wilt bewerken, gaat u naar Policy > Results:



Algemene menu ISE

Ga naar Autorisatie > Autorisatieprofielen. Klik op het aanvinkvakje van het profiel dat u wilt wijzigen en klik vervolgens op Bewerken:



Het autorisatieprofiel bewerken

## Clientconfiguratie

Stap 1. Maak een XML-profiel met de XML-profieleditor. Dit voorbeeld wordt gebruikt voor het maken van dit document:

```
<#root>
```

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinux>All</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">
      true
    </AutoReconnect>
    <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
    <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">
      Disable
    </PPPEExclusion>
    <PPPEExclusionServerIP UserControllable="false"/>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">
      false
    </EnableAutomaticServerSelection>
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    <RetainVpnOnLogoff>false </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>
FlexVPN HUB
      </HostName>
      <HostAddress>
```

192.168.50.225

```
</HostAddress>  
<PrimaryProtocol>
```

**IPsec**

```
<StandardAuthenticationOnly>  
true  
<AuthMethodDuringIKENegotiation>
```

**EAP-MD5**

```
</AuthMethodDuringIKENegotiation>  
<IKEIdentity>
```

**cisco.example**

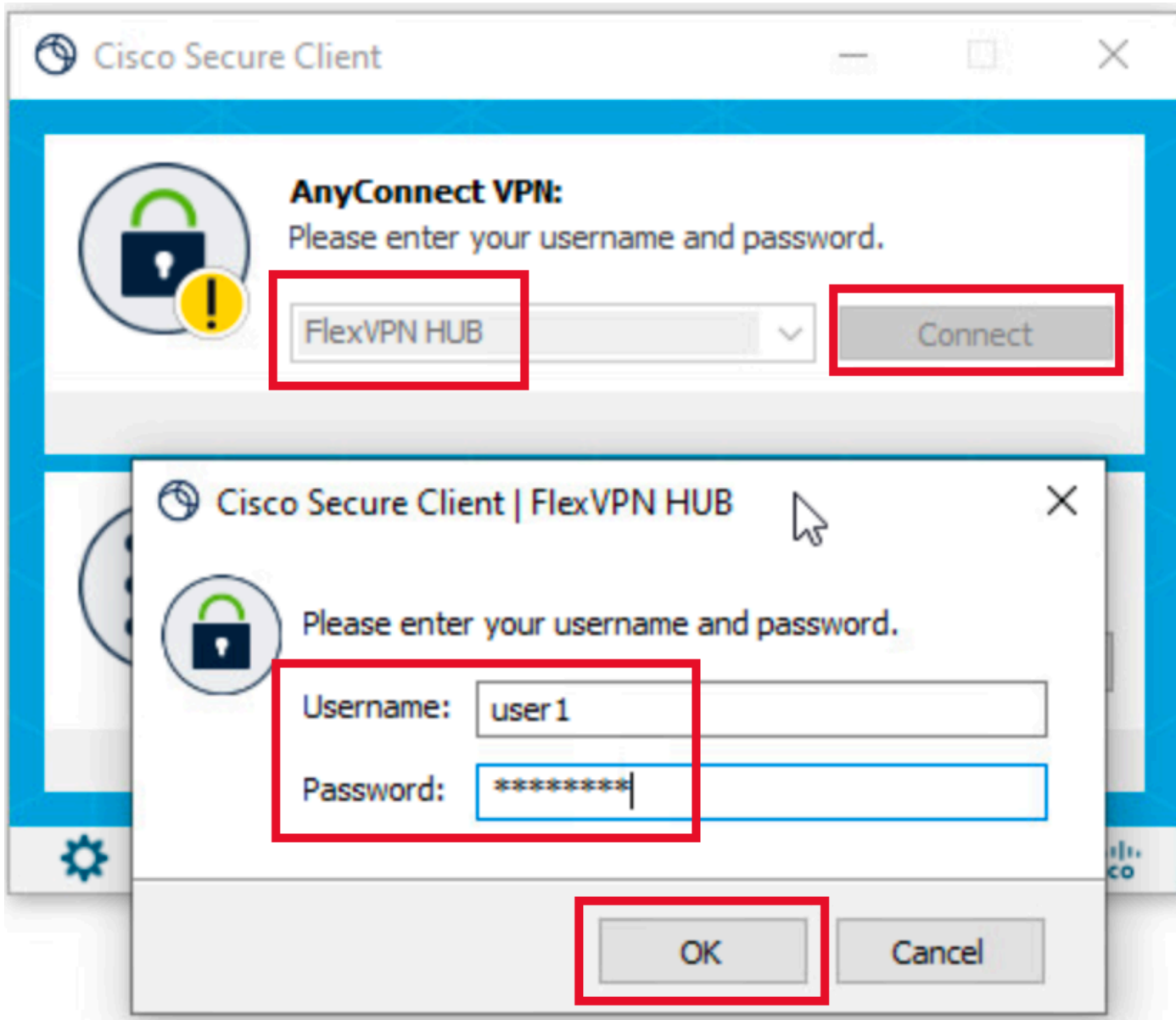
```
</IKEIdentity>  
</StandardAuthenticationOnly>  
</PrimaryProtocol>  
</HostEntry>  
</ServerList>  
</AnyConnectProfile>
```

- **<HostName>** - De alias die wordt gebruikt om te verwijzen naar de host, IP-adres of Full-Qualified Domain Name (FQDN). Dit wordt weergegeven in het vak CSC.
- **<HostAddress>** - IP-adres of FQDN van de FlexVPN-hub.
- **<Primary Protocol>** - Moet worden ingesteld op IPsec om de client te dwingen IKEv2/IPsec te gebruiken in plaats van SSL.
- **<AuthMethodDuringIKENonderhandeling>** - Moet worden ingesteld om EAP-MD5 te gebruiken binnen EAP. Dit is vereist voor verificatie op de ISE-server.
- **<IKEIdentity>** - Deze string wordt door de client verzonden als de payload van de ID\_GROUP type-id. Dit kan worden gebruikt om de client aan te passen aan een specifiek IKEv2-profiel op de hub.

## Verifiëren

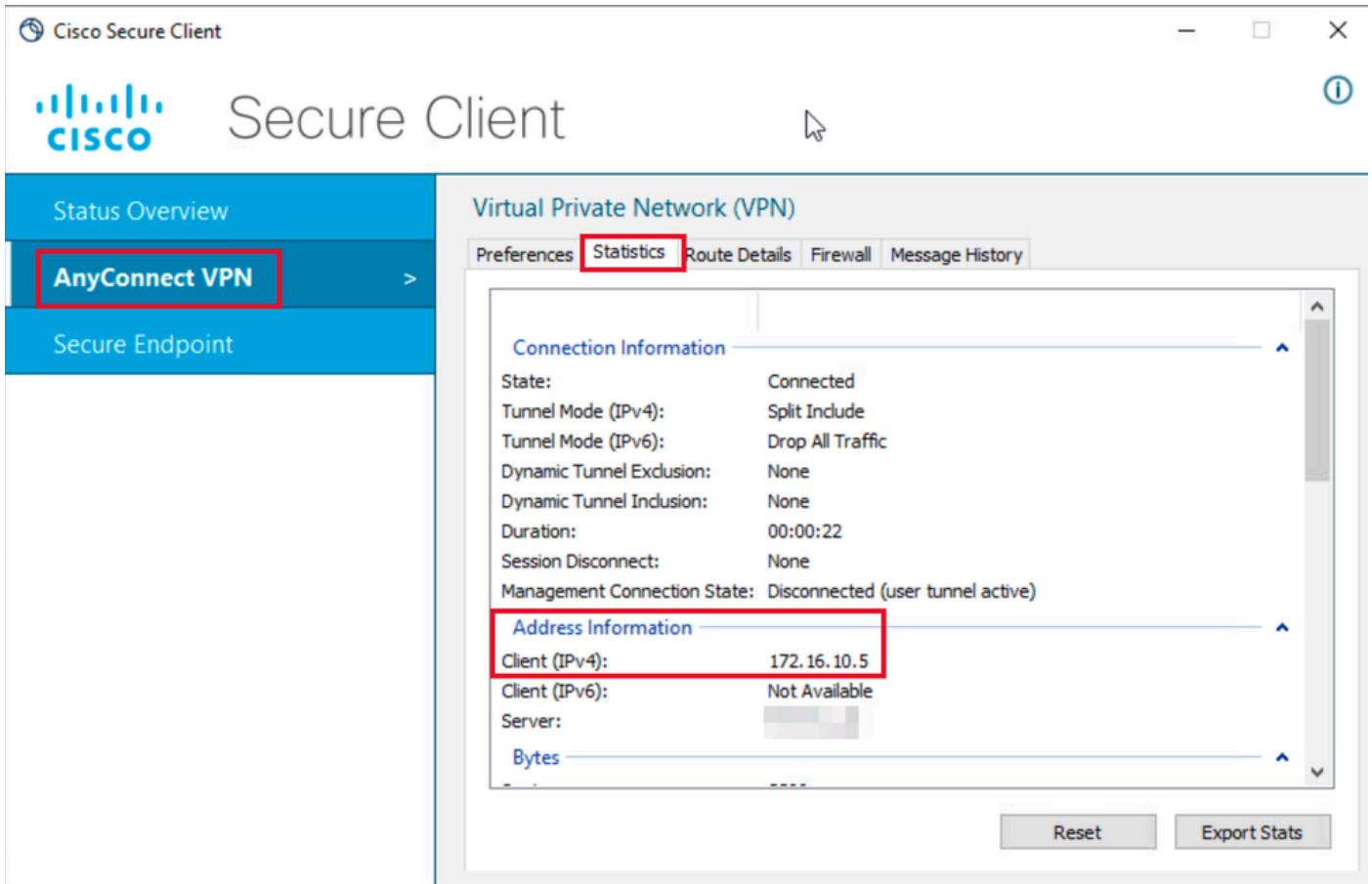
Stap 1. Navigeer naar de clientmachine waar CSC is geïnstalleerd. Maak verbinding met de FlexVPN-hub en voer de user1-referenties in:





Gebruikersreferenties1

Stap 2. Wanneer de verbinding tot stand is gebracht, klikt u op het tandwiel pictogram (linker benedenhoek) en navigeert u naar AnyConnectVPN > Statistics. Bevestig in het gedeelte Adres Information dat het toegewezen IP-adres behoort tot de pool die voor groep1 is geconfigureerd:



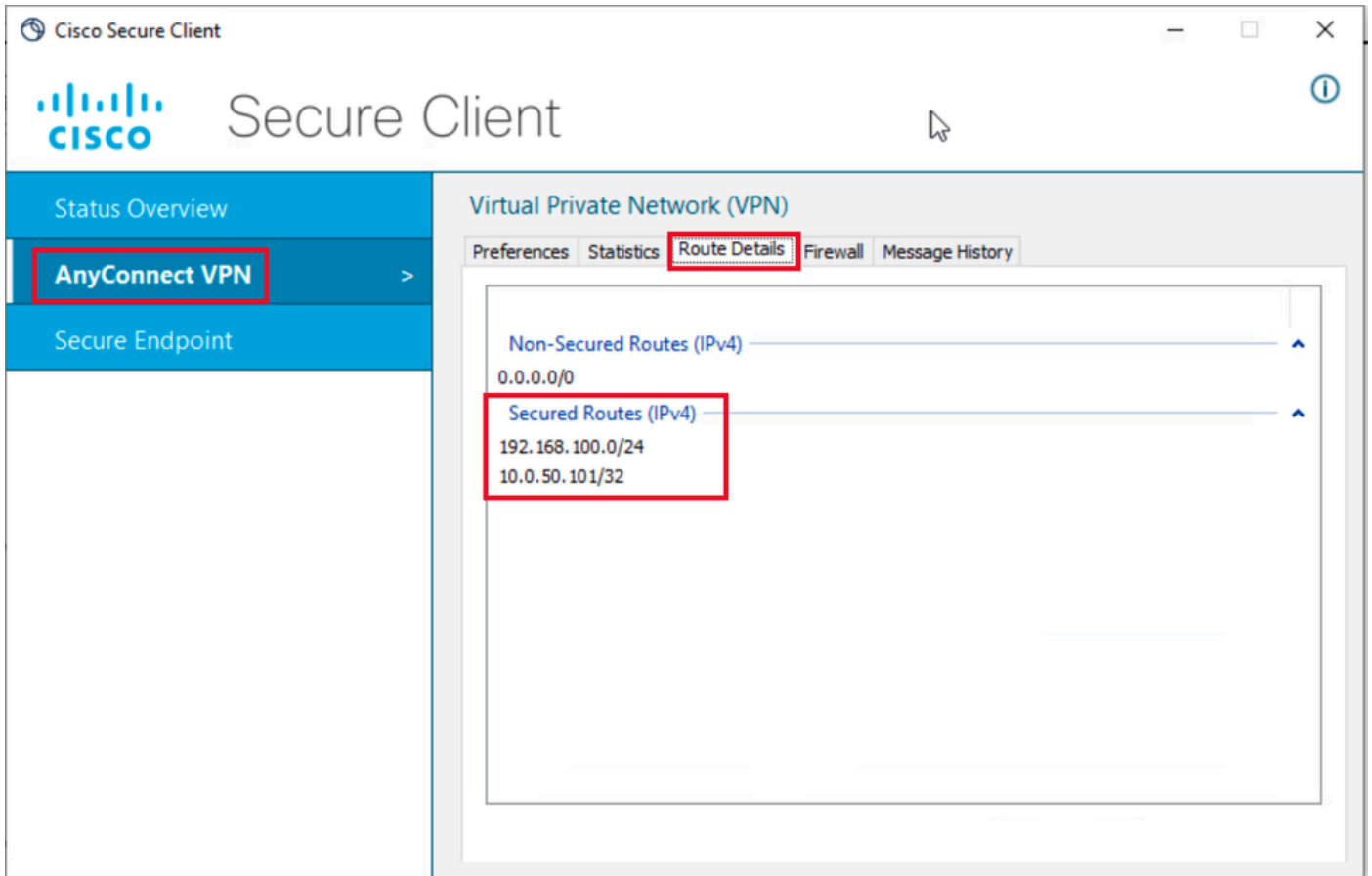
The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane includes 'Status Overview', 'AnyConnect VPN' (highlighted with a red box), and 'Secure Endpoint'. The main window is titled 'Virtual Private Network (VPN)' and has tabs for 'Preferences', 'Statistics' (highlighted with a red box), 'Route Details', 'Firewall', and 'Message History'. The 'Statistics' tab is active, showing 'Connection Information' and 'Address Information' sections. The 'Address Information' section is also highlighted with a red box and contains the following data:

Address Information	
Client (IPv4):	172.16.10.5
Client (IPv6):	Not Available
Server:	[Redacted]

At the bottom of the statistics window, there are 'Reset' and 'Export Stats' buttons.

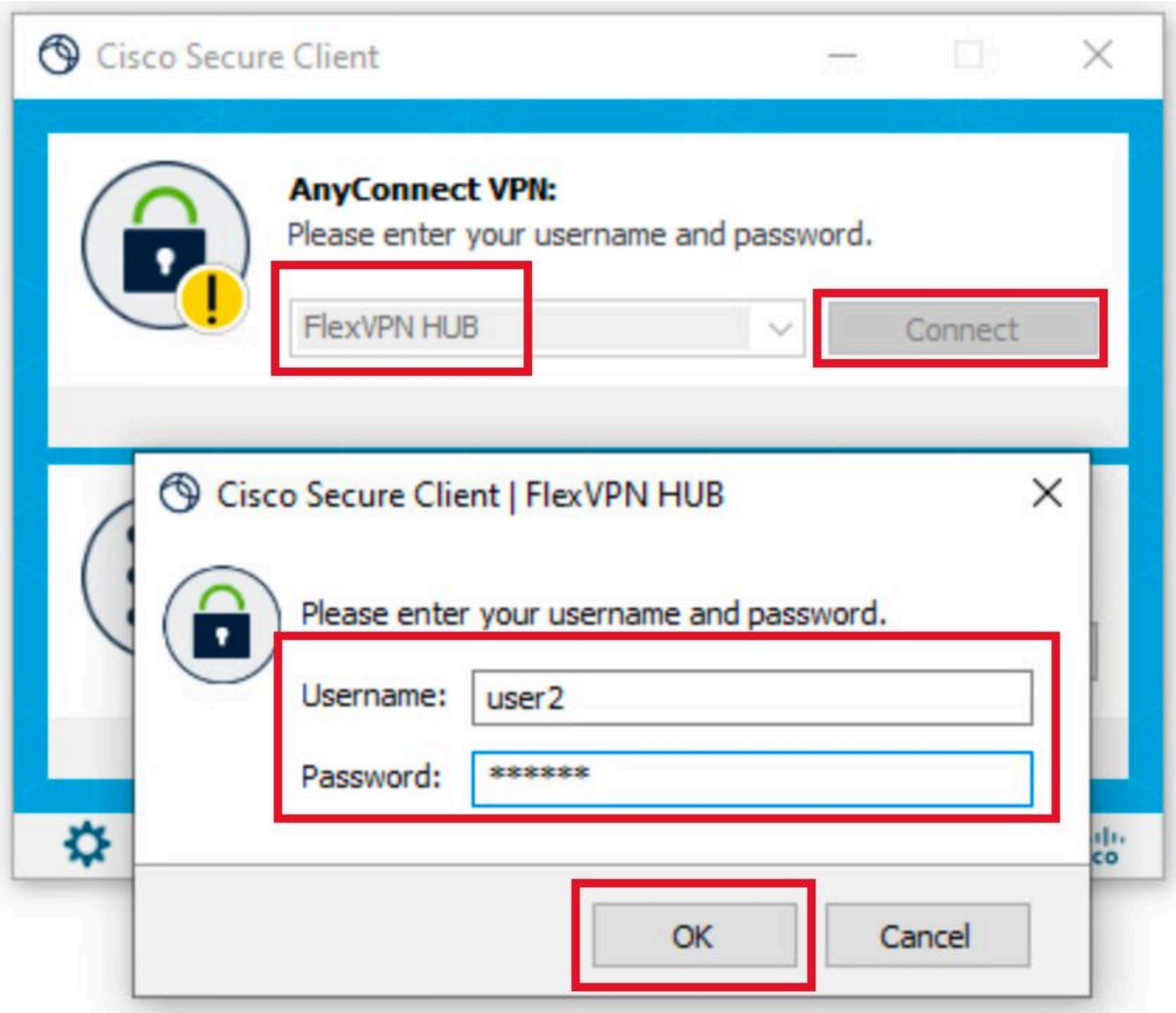
Statistieken gebruiker1

Navigeer naar AnyConnectVPN > Routegegevens en bevestig dat de weergegeven informatie overeenkomt met de beveiligde routes en DNS die zijn geconfigureerd voor groep1:



Gebruiker1-routegegevens

Stap 3. Herhaal stap 1 en 2 met user2-referenties om te controleren of de informatie overeenkomt met de waarden die zijn geconfigureerd in het ISE-autorisatiebeleid voor deze groep:



Gebruikersreferenties2

Cisco Secure Client

# Secure Client

Status Overview

**AnyConnect VPN**

Secure Endpoint

## Virtual Private Network (VPN)

Preferences **Statistics** Route Details Firewall Message History

**Connection Information**

State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:12
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

**Address Information**

Client (IPv4):	172.16.20.5
Client (IPv6):	Not Available
Server:	

Bytes

Reset Export Stats

Gebruiker2 Statistieken

Cisco Secure Client

# Secure Client

Status Overview

**AnyConnect VPN**

Secure Endpoint

## Virtual Private Network (VPN)

Preferences Statistics **Route Details** Firewall Message History

**Non-Secured Routes (IPv4)**

0.0.0.0/0

**Secured Routes (IPv4)**

192.168.200.0/24
10.0.50.202/32

Gebruiker2-routegegevens

# Problemen oplossen

## Debugs en logbestanden

Op Cisco router:

1. Gebruik de debug van IKEv2 en IPSec om de onderhandeling tussen de head-end en de client te verifiëren:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. Gebruik AAA-debuggs om de toewijzing van lokale en/of externe kenmerken te verifiëren:

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

ISE:

- Live RADIUS-logbestanden

## Werkscenario

De volgende uitgangen zijn voorbeelden van de succesvolle verbindingen:

- Gebruiker1 debug-uitvoer:

<#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
```

```
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
```

```
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
```

```
Jan 30 02:57:21.088: idb is NULL
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
```

Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.089: RADIUS(000000FF): sending  
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.089: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34  
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12  
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]  
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18  
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II\*?0"  
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.094: RADIUS:

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5  
Jan 30 02:57:21.094: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8  
RADIUS: 01 52 00 06 0D 20 [ R ]  
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18  
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@0XH6]  
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85  
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes  
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.097: idb is NULL

Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.097: RADIUS(000000FF): sending  
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.097: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC

Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.098: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8  
RADIUS: 02 52 00 06 03 04 [ R]  
Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18  
RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g\$D&d]  
Jan 30 02:57:21.098: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.101: RADIUS:

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1

Jan 30 02:57:21.101: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32  
RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai  
Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18  
RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!]  
Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86  
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes  
Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):



Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.104: idb is NULL  
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.104: RADIUS(000000FF): sending  
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.104: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46  
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24  
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]  
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18  
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>Tv]  
Jan 30 02:57:21.104: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.170: RADIUS:

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6  
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.170: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]

```
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams()]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31
```

```
"ipsec:dns-servers=10.0.50.101"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41
```

```
"ipsec:route-set=prefix 192.168.100.0/24"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24
```

```
"ipsec:addr-pool=group1"
```

```
Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):
```

```
Pick method list 'FlexVPN-Authorization-List'
```

```
Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:
```

```
Line protocol on Interface Virtual-Access1, changed state to up
```

- Gebruiker2 debug uitvoer:

```
<#root>
```

```
Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64  
Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26  
Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36  
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phrase1-id=cisco.example"

Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64  
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"  
Jan 30 03:28:58.104: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21  
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12  
RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]  
Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18  
RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]  
Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet  
Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout  
Jan 30 03:28:58.109: RADIUS:

Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43  
Jan 30 03:28:58.109: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]  
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]  
Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8  
RADIUS: 01 35 00 06 0D 20 [ 5 ]  
Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18  
RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]  
Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88  
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes  
Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC  
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0  
Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 03:28:58.113: idb is NULL  
Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::  
Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct\_session\_id: 4249  
Jan 30 03:28:58.113: RADIUS(00000103): sending  
Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded  
Jan 30 03:28:58.113: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C

Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30

"isakmp-phrase1-id=cisco.example"

Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"

Jan 30 03:28:58.113: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"

Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8

RADIUS: 02 35 00 06 03 04 [ 5]

Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18

RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]

Jan 30 03:28:58.113: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100

Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet

Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout

Jan 30 03:28:58.116: RADIUS:

Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02

Jan 30 03:28:58.116: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32

RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM]

Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18

RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]

Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89

RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes

Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-

Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0

Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]

Jan 30 03:28:58.118: idb is NULL  
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: ::  
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct\_session\_id: 4249  
Jan 30 03:28:58.118: RADIUS(00000103): sending  
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded  
Jan 30 03:28:58.119: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332

RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE  
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"  
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24  
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]  
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18  
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]  
Jan 30 03:28:58.119: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]  
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]  
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet  
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout  
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233  
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD  
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.186: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]  
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]  
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]  
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]  
RADIUS: 33 30 [ 30]  
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6  
RADIUS: 03 36 00 04 [ 6]  
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18  
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]  
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37  
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.202"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.200.0/24"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group2"

Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90

RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes

Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f

Jan 30 03:28:58.190: AAA/AUTHOR (0x104):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to

Jan 30 03:28:58.209: %SYS-5-CONFIG\_P: Configured programmatically by process Crypto INT from console as

Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access2, changed state to up

## Gerelateerde informatie

- [Cisco Technical Support en downloads](#)

## 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.