

& Configureer beveiligde client IKEv2/ASA in ASDM met AAA Cert Auth

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Configuraties](#)

[Configuratie in ASDM](#)

[Stap 1. VPN-wizards openen](#)

[Stap 2. Identificatie van verbindingsprofiel](#)

[Stap 3. VPN-protocollen](#)

[Stap 4. Clientafbeeldingen](#)

[Stap 5. Verificatiemethoden](#)

[Stap 6. SAML-configuratie](#)

[Stap 7. Toewijzing van clientadres](#)

[Stap 8. Netwerknnaamoplossings servers](#)

[Stap 9. NAT-vrijstelling](#)

[Stap 10. Beveiligde clientimplementatie](#)

[Stap 11. Instellingen opslaan](#)

[Stap 12. Beveiligd clientprofiel bevestigen en exporteren](#)

[Stap 13. Bevestig details van beveiligd clientprofiel](#)

[Stap 14. Instellingen in ASA CLI bevestigen](#)

[Stap 15. Cryptografisch algoritme toevoegen](#)

[Configuratie in Windows-server](#)

[Configuratie in ISE](#)

[Stap 1. Apparaat toevoegen](#)

[Stap 2. Actieve map toevoegen](#)

[Stap 3. Identiteitsbroncode toevoegen](#)

[Stap 4. Beleidsset toevoegen](#)

[Stap 5. Verificatiebeleid toevoegen](#)

[Stap 6. Toepassingsbeleid toevoegen](#)

[Verifiëren](#)

[Stap 1. Kopieer een beveiligd clientprofiel naar Win10 PC1](#)

[Stap 2. VPN-verbinding starten](#)

[Stap 3. Syslog op ASA bevestigen](#)

[Stap 4. IPsec-sessie voor ASA bevestigen](#)

[Stap 5. Radius live log bevestigen](#)

[Problemen oplossen](#)

[Stap 1. VPN-verbinding starten](#)

[Stap 2. Syslog in CLI bevestigen](#)

[Referentie](#)

Inleiding

Dit document beschrijft de stappen die nodig zijn om een beveiligde client via IKEv2 op ASA te configureren met behulp van ASDM met AAA en certificaatverificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco Identity Services Engine (ISE)
- Configuratie van Cisco adaptieve security virtuele applicatie (ASAv)
- Configuratie van Cisco Adaptieve Security Device Manager (ASDM)
- VPN-verificatiestroom

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

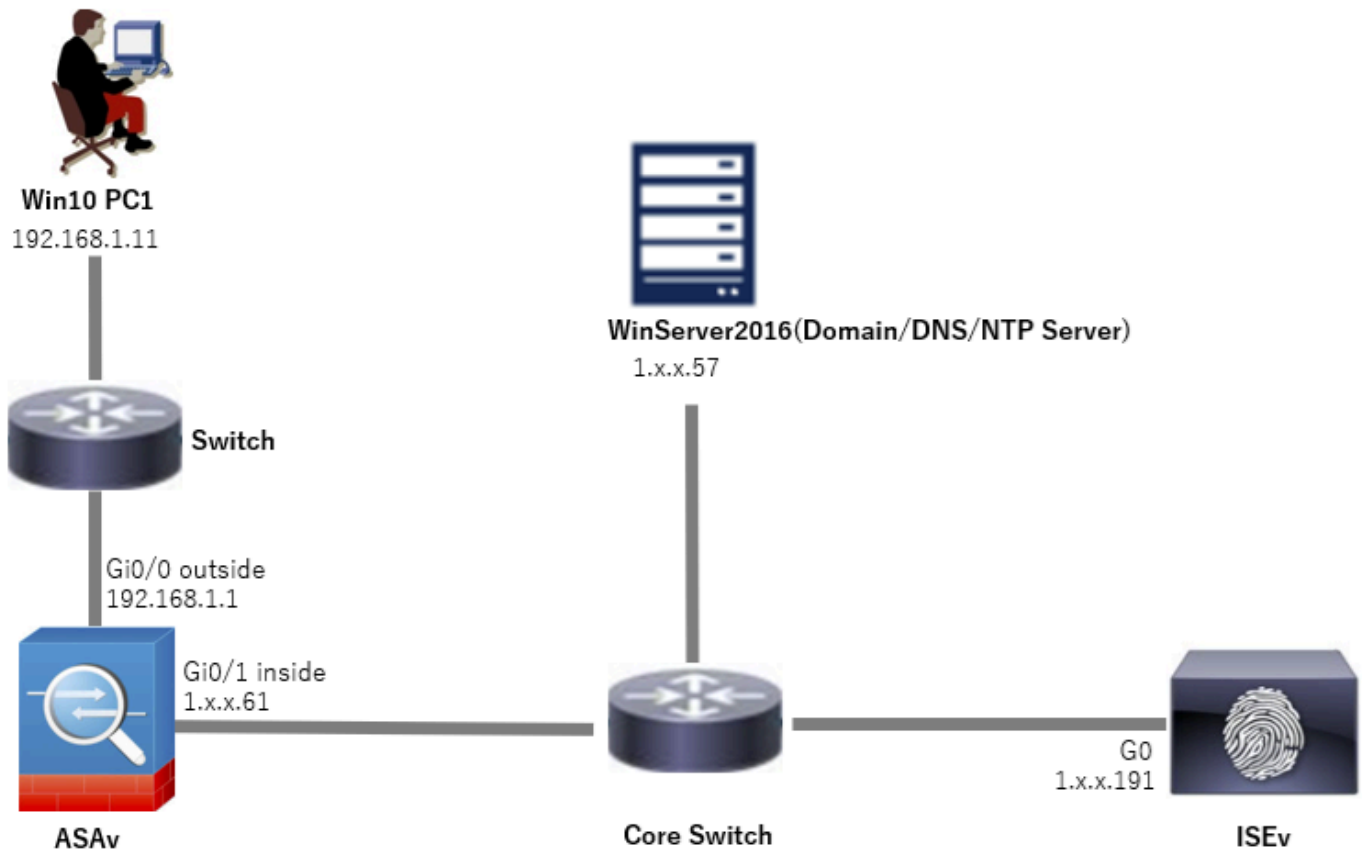
- Identity Services Engine virtuele 3.3-patch 1
- Adaptieve security virtuele applicatie 9.20(2)21
- Adaptieve security apparaatbeheer 7.20(2)
- Cisco Secure-client 5.1.3.62
- Windows Server 2016
- Windows 10

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.

Netwerkdigram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.

De domeinnaam ingesteld op Windows Server 2016 is ad.rem-system.com, die wordt gebruikt als voorbeeld in dit document.



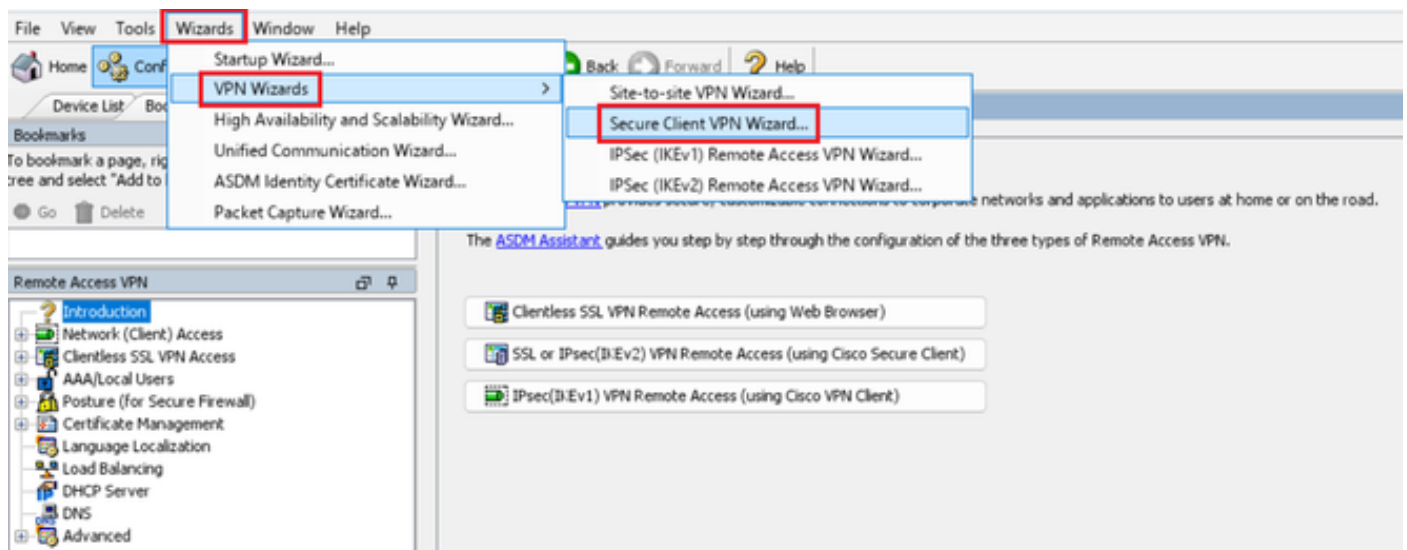
Netwerkdigram

Configuraties

Configuratie in ASDM

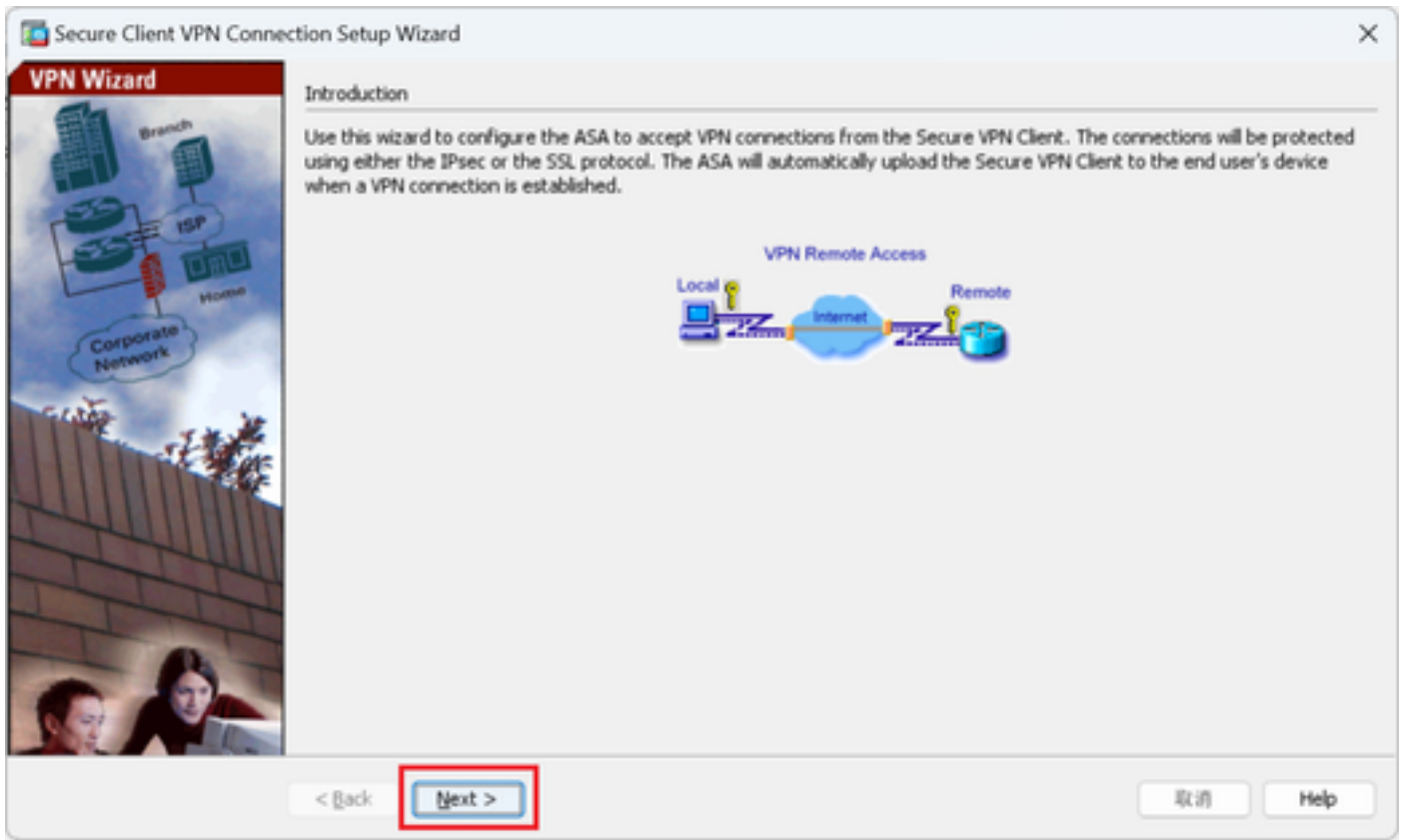
Stap 1. VPN-wizards openen

Navigeer naar Wizards > VPN Wizards, klik op Secure Client VPN Wizard.



VPN-wizards openen

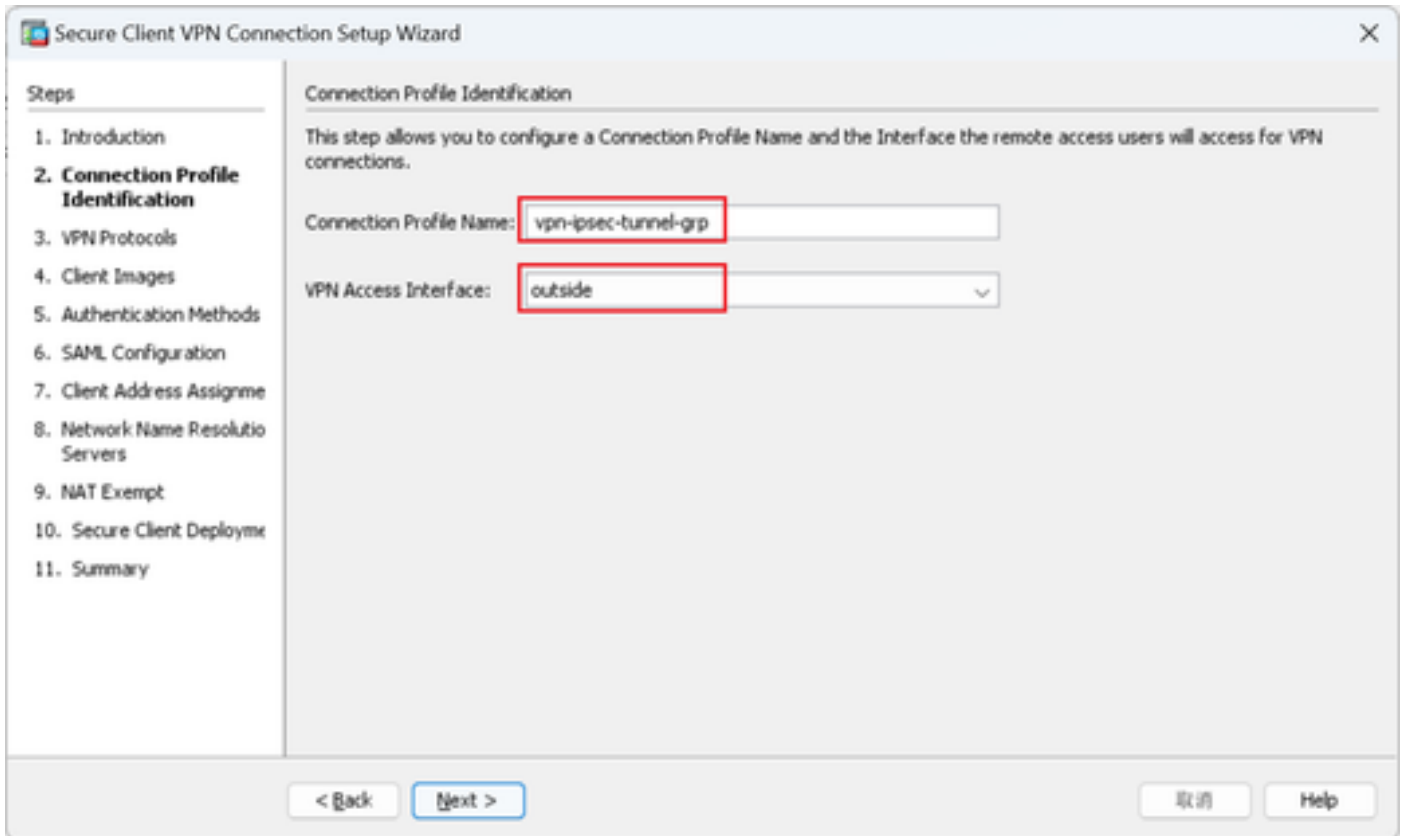
Klik op Next (Volgende).



Klik op Volgende knop

Stap 2. Identificatie van verbindingprofiel

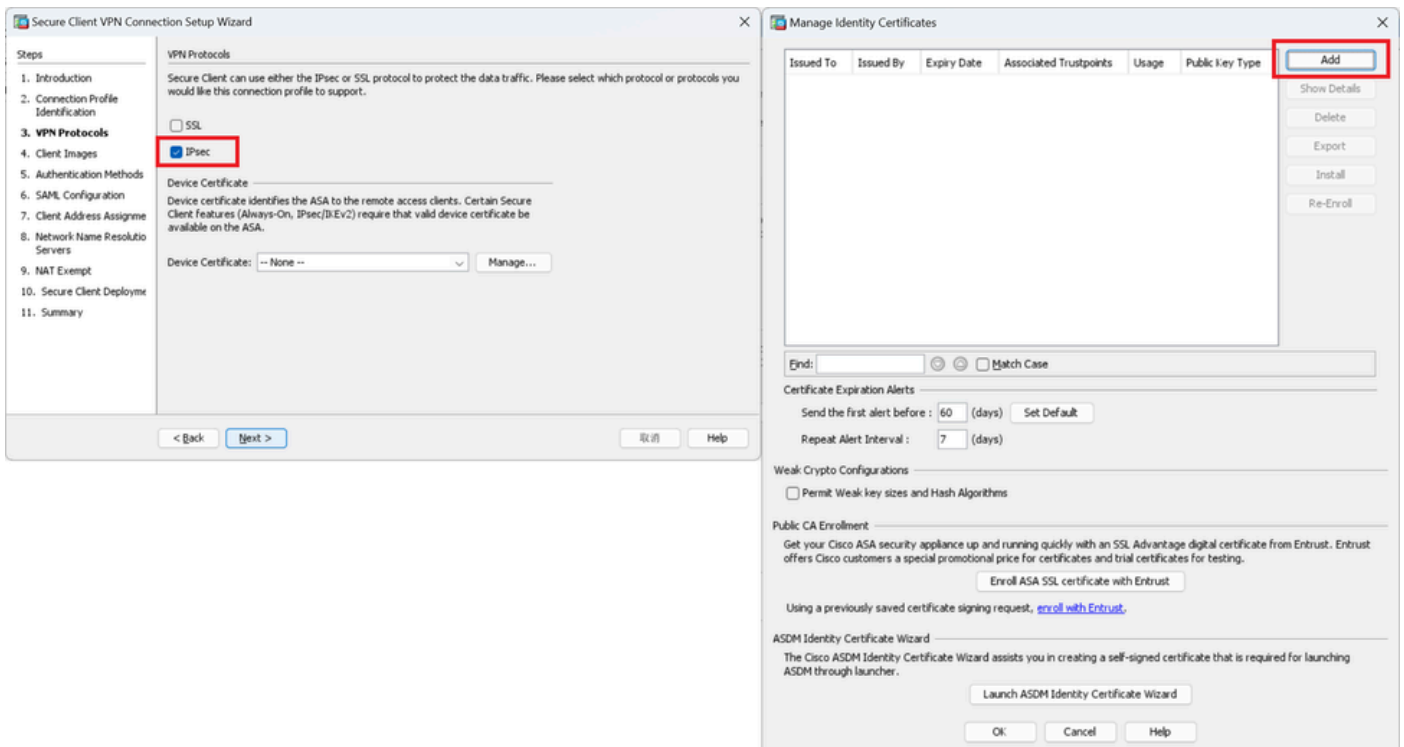
Voer informatie in voor het verbindingprofiel.
Naam verbindingprofiel: vpn-ipsec-tunnel-grp
VPN-toegangsinterface: buiten



Identificatie van verbindingprofiel

Stap 3. VPN-protocollen

Selecteer IPsec en klik op de knop Add om een nieuw zelfondertekend certificaat toe te voegen.

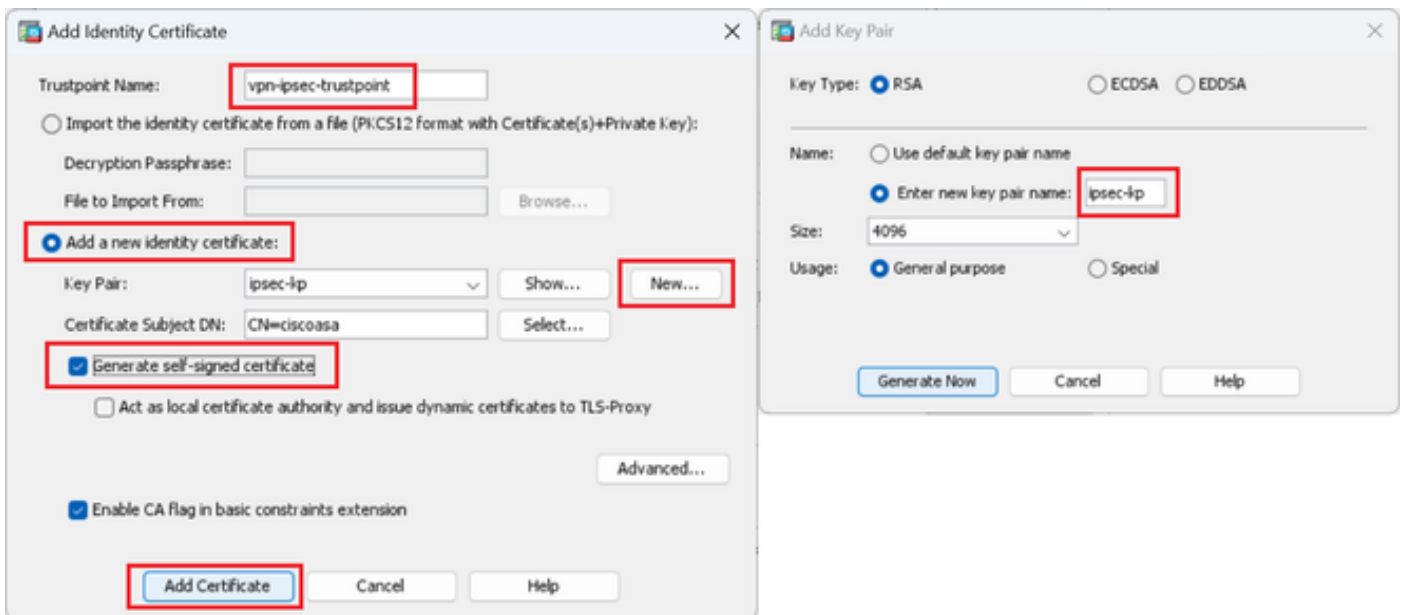


VPN-protocollen

Voer informatie in voor een zelfondertekend certificaat.

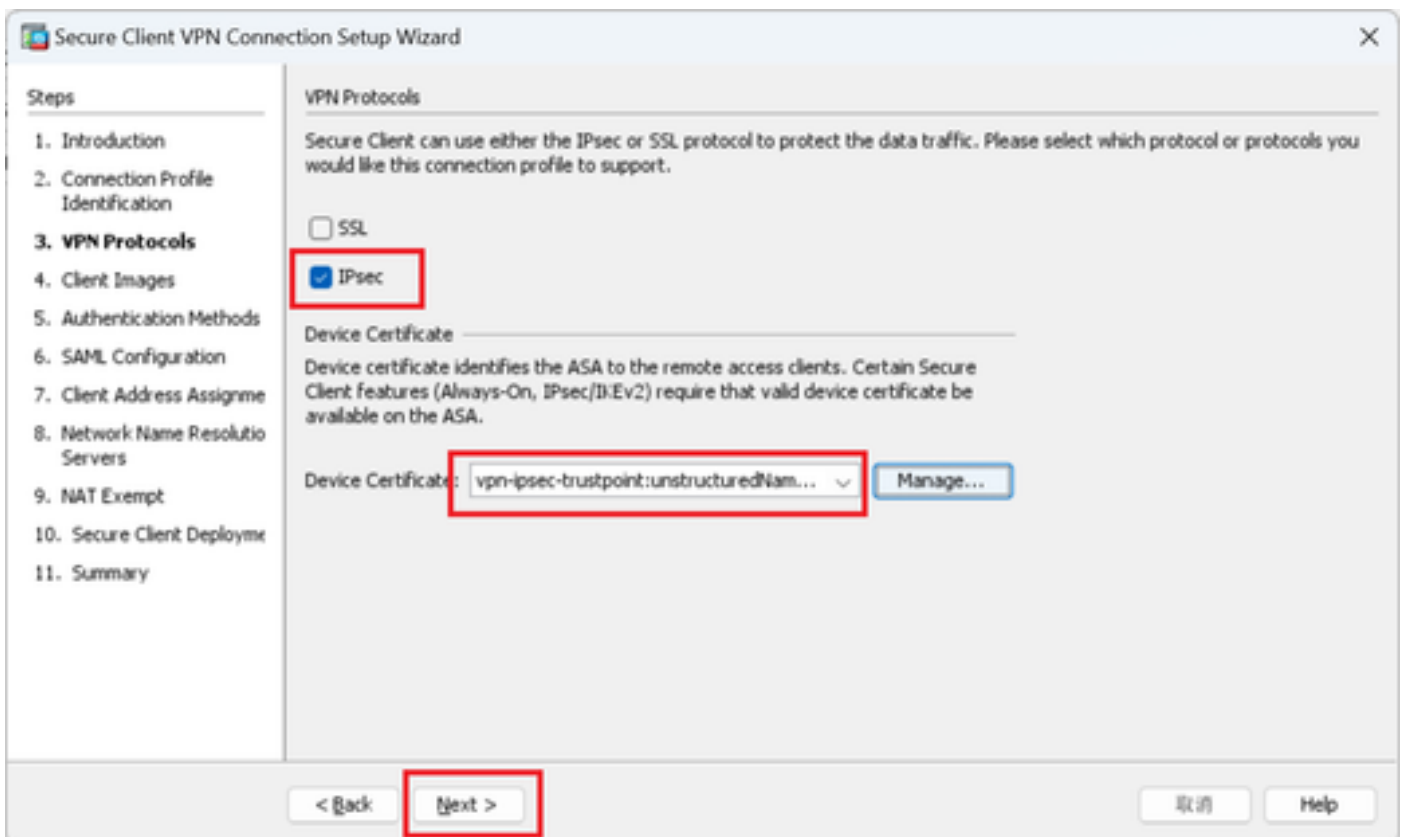
Trustpoint Naam: vpn-ipsec-trustpoint

Toetsenpaar: ipsec-kp



Details van het zelfondertekende certificaat

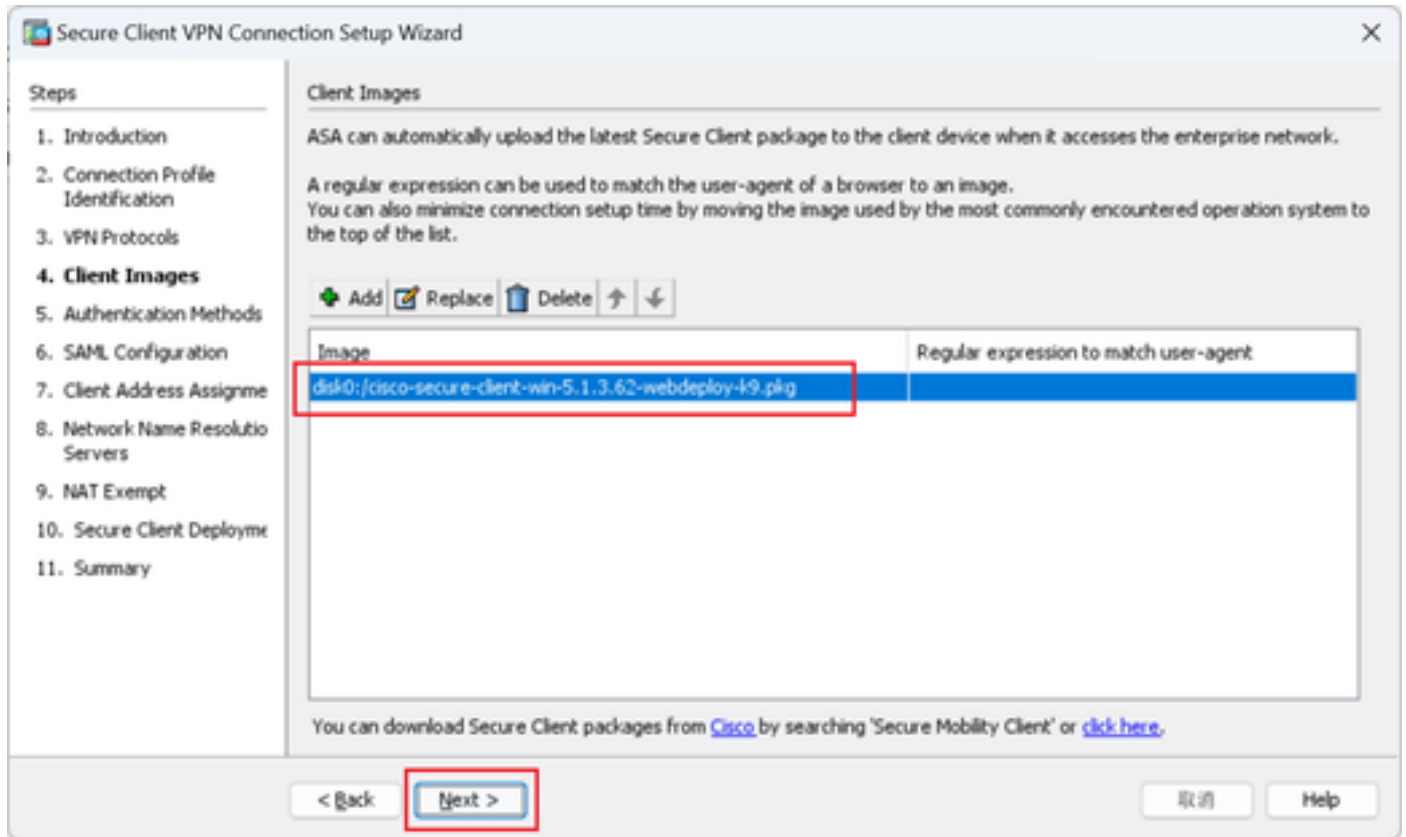
Bevestig de instellingen van VPN-protocollen en klik op Volgende.



Instellingen VPN-protocol bevestigen

Stap 4. Clientafbeeldingen

Klik op de knop Add om een beveiligd cliëntbeeld toe te voegen en klik op Next.



Clientafbeeldingen

Stap 5. Verificatiemethoden

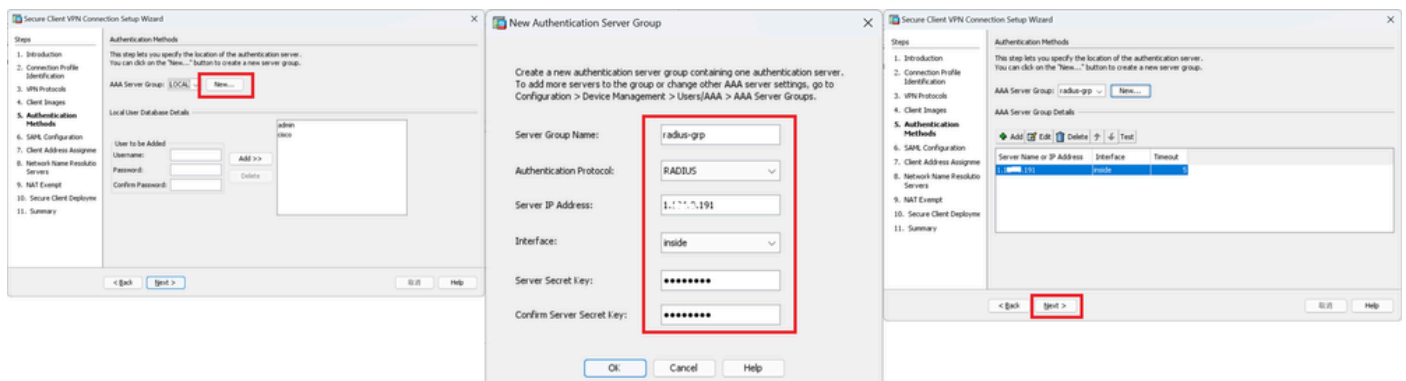
Klik op de knop Nieuw om een nieuwe server toe te voegen en klik op Volgende.

Naam servergroep : radius-grp

Verificatieprotocol: RADIUS

IP-adres server: 1.x.x.191

Interface: binnen



Stap 6. SAML-configuratie

Klik op de knop Volgende.

The screenshot shows the 'Secure Client VPN Connection Setup Wizard' window. The 'Steps' list on the left includes: 1. Introduction, 2. Connection Profile Identification, 3. VPN Protocols, 4. Client Images, 5. Authentication Methods, 6. SAML Configuration (highlighted), 7. Client Address Assignme, 8. Network Name Resolutio Servers, 9. NAT Exempt, 10. Secure Client Deployme, and 11. Summary. The main area is titled 'SAML Configuration' and contains the following fields: 'Authentication Method' set to 'AAA', 'AAA Server Group' set to 'radius-grp', and 'SAML Identity Provider SAML Server' set to '--- None ---'. There are 'Manage...' buttons next to the 'AAA Server Group' and 'SAML Server' fields. A checkbox for 'Use LOCAL if Server Group fails' is unchecked. At the bottom, there are '< Back', 'Next >', '取消', and 'Help' buttons. The 'Next >' button is highlighted with a red box.

SAML-configuratie

Stap 7. Toewijzing van clientadres

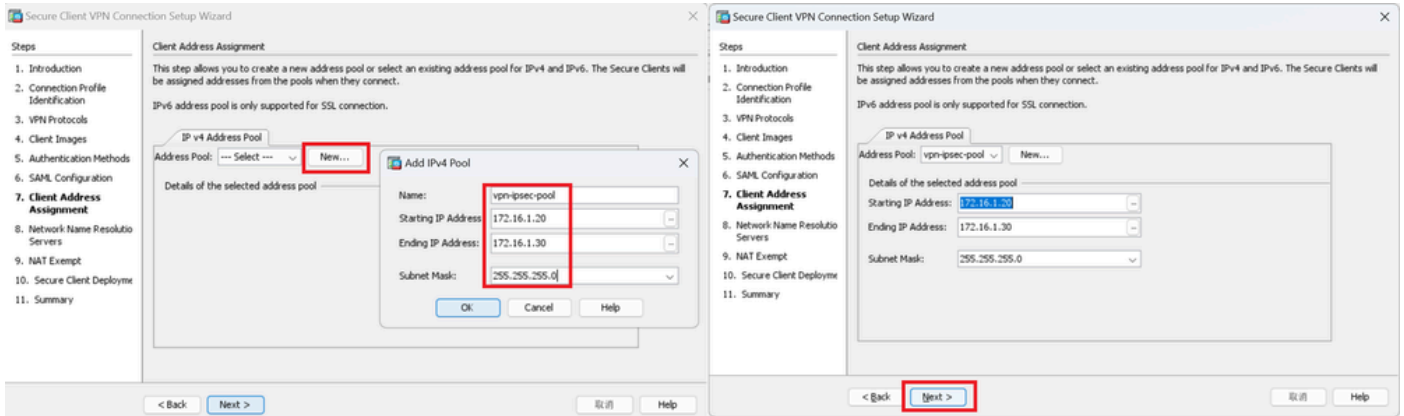
Klik op Nieuwe knop om een nieuwe IPv4-pool toe te voegen en klik op Volgende knop.

Naam : vpn-ipsec-pool

IP-startadres: 172.16.1.20

EindIP-adres: 172.16.1.30

Subnetmasker: 255.255.255.0



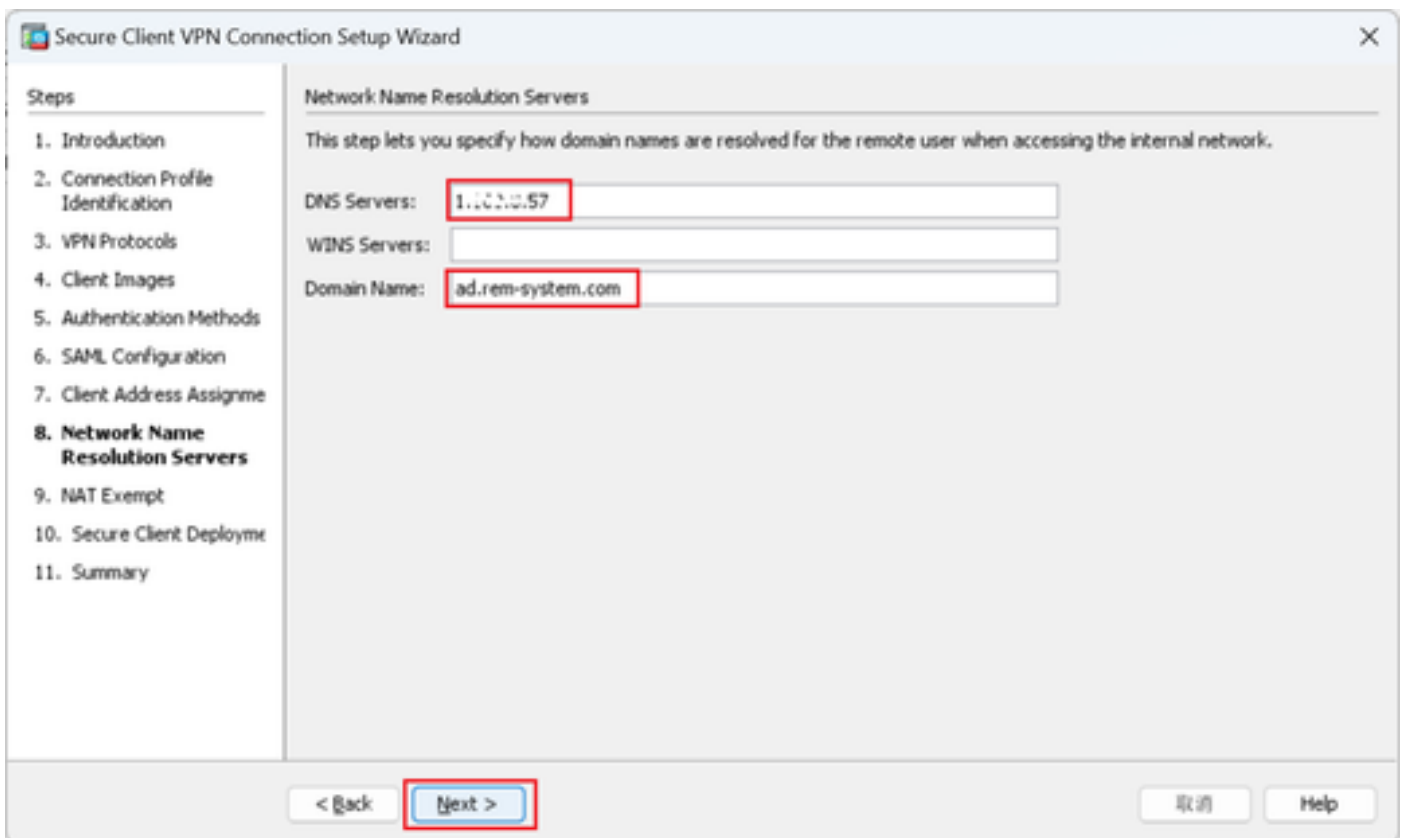
Clientadrestoewijzing

Stap 8. Netwerknnaamoplossingservers

Invoerinformatie voor DNS en domein, klik op Volgende knop.

DNS-servers : 1.x.x.57

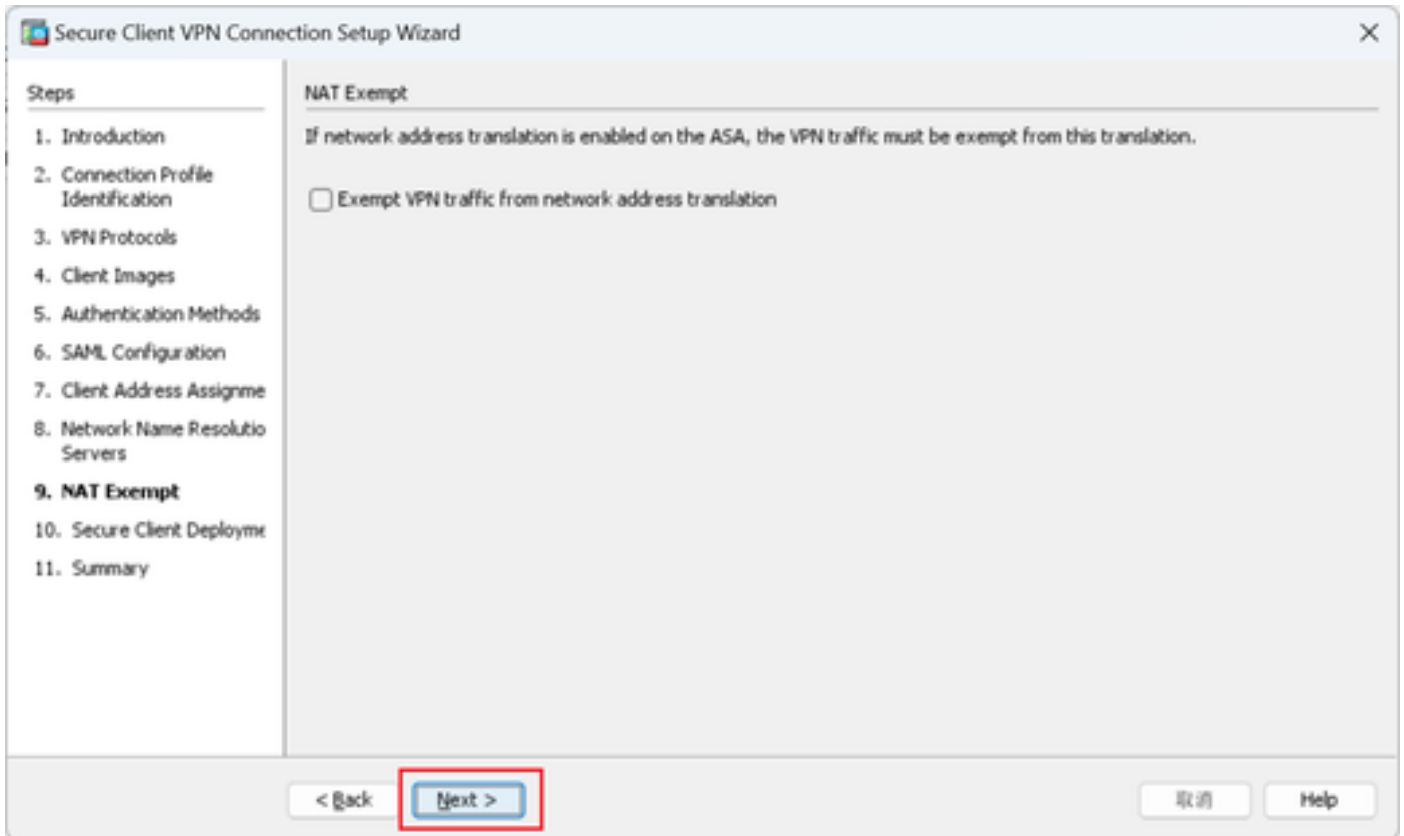
Domeinnaam: ad.rem-system.com



Netwerknnaamoplossingservers

Stap 9. NAT-vrijstelling

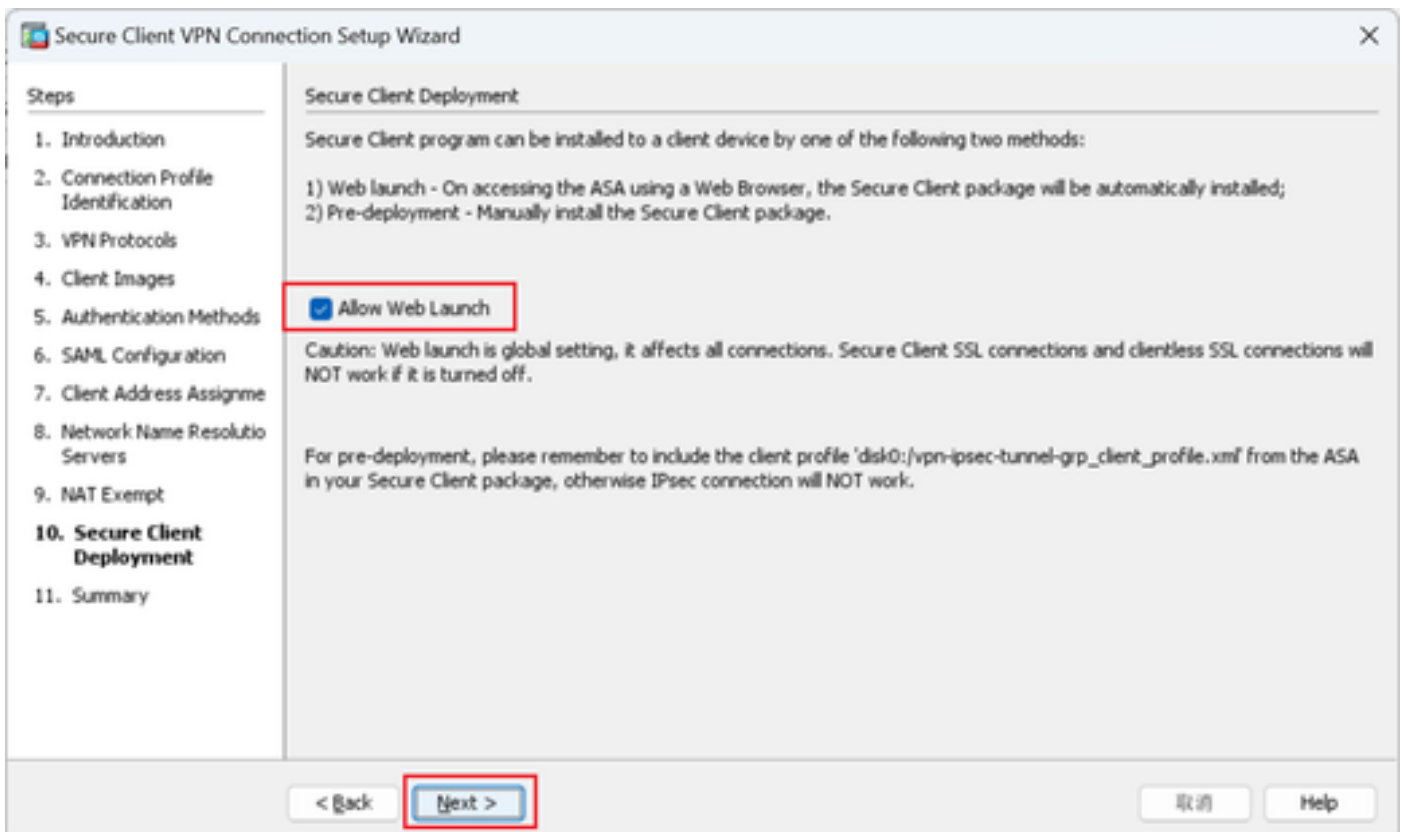
Klik op de knop Volgende.



NAT-vrijstelling

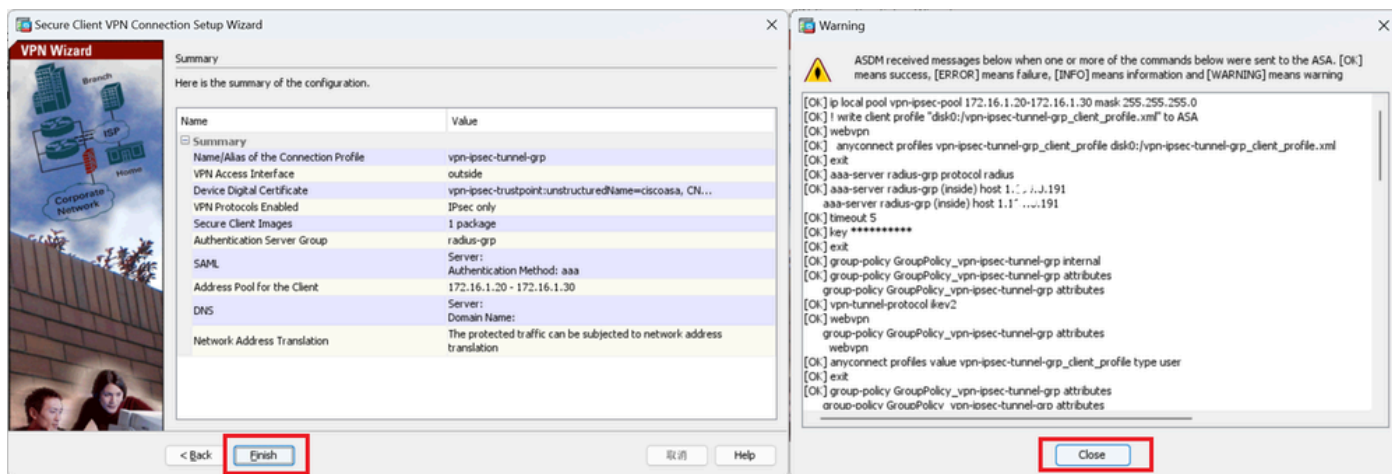
Stap 10. Beveiligde clientimplementatie

Selecteer Toestaan dat het web wordt gestart en klik op Volgende.



Stap 11. Instellingen opslaan

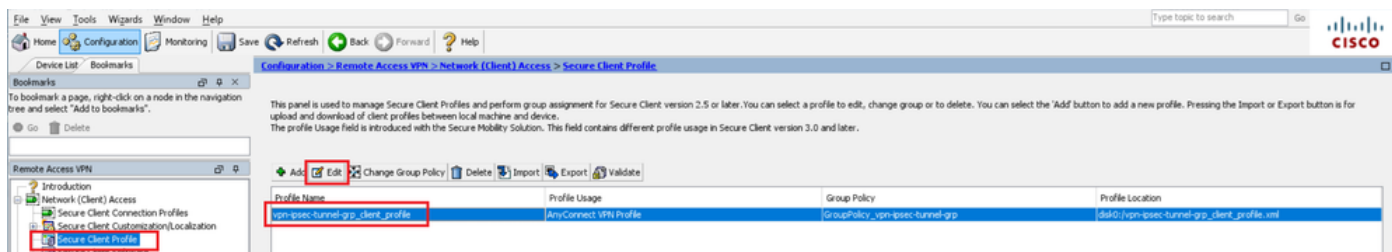
Klik op Finish (Voltoeien) en sla de instellingen op.



Instellingen opslaan

Stap 12. Beveiligd clientprofiel bevestigen en exporteren

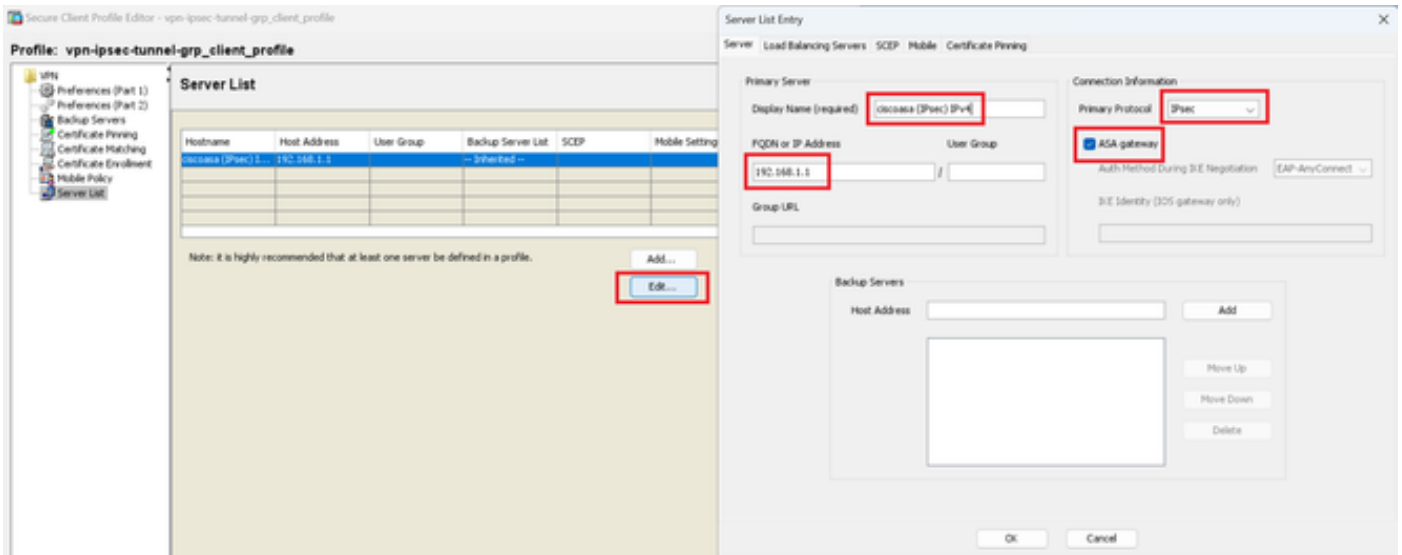
Navigeer naar Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, klik op Edit knop.



Beveiligd clientprofiel bewerken

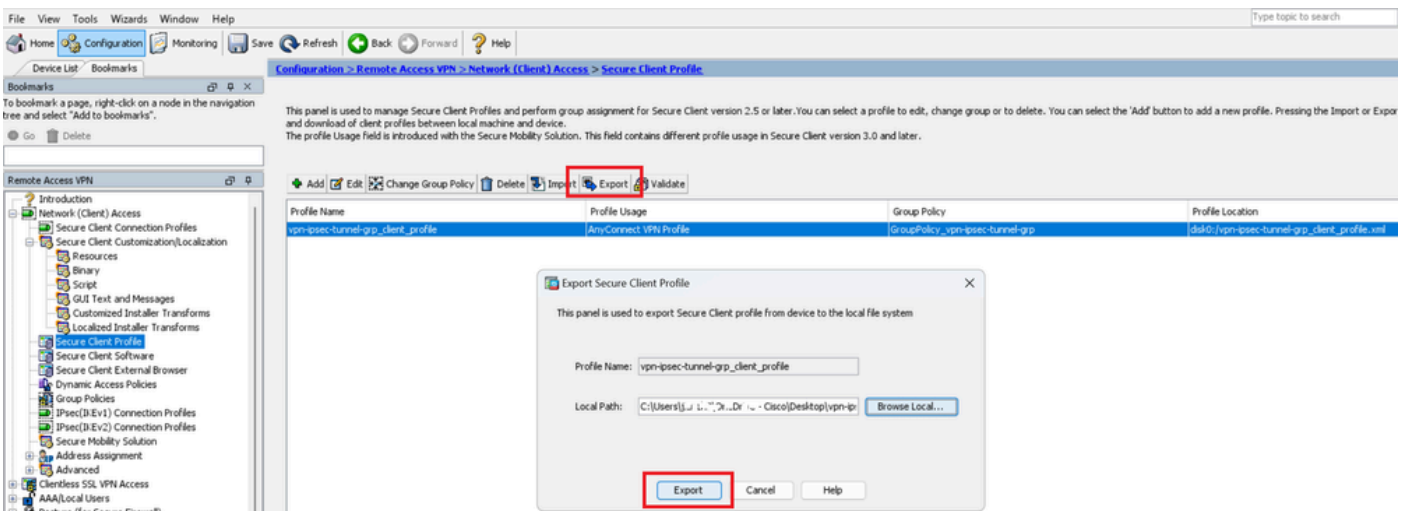
Bevestig de details van het profiel.

- Display naam (verplicht): ciscoasa (IPsec) IPv4
- FQDN- of IP-adres: 192.168.1.1
- Primair protocol: IPsec



Beveiligd clientprofiel bevestigen

Klik op de knop Exporteren om het profiel naar een lokale pc te exporteren.



Beveiligd clientprofiel exporteren

Stap 13. Bevestig details van beveiligd clientprofiel

Open een beveiligd clientprofiel via de browser en bevestig dat het primaire protocol voor de host IPsec is.

```

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
  <ServerList>
    <HostEntry>
      <HostName>ciscoasa (IPsec) IPv4</HostName>
      <HostAddress>192.168.1.1</HostAddress>
      <PrimaryProtocol>IPsec</PrimaryProtocol>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>

```

Stap 14. Instellingen in ASA CLI bevestigen

Bevestig de IPsec-instellingen die door ASDM in de ASA CLI zijn gemaakt.

```
// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0

// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5

// Define the transform sets that IKEv2 can use
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1

// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map outside_map interface outside

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
cr1 configure

// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b
.....
ac76f984 efd41d13 073d0be6 f923a9c6 7b
quit

// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10
```

```

encryption aes-192
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 40
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400

// Enabling client-services on the outside interface
crypto ikev2 enable outside client-services port 443

// Specifies the certificate the ASA uses for IKEv2
crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint

// Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
enable
anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1
anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
anyconnect enable
tunnel-group-list enable

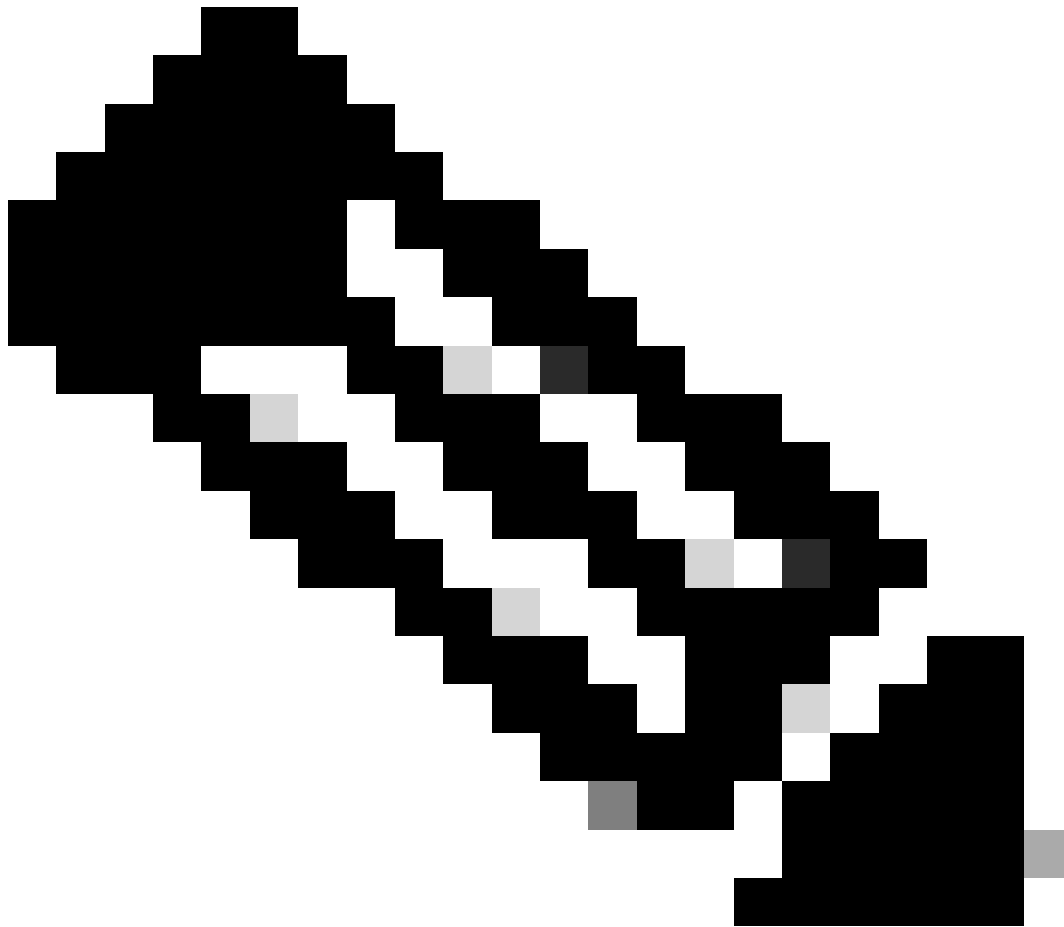
// Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile
group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
wins-server none
dns-server value 1.x.x.57
vpn-tunnel-protocol ikev2
default-domain value ad.rem-system.com
webvpn
anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user

// Ties the pool of addresses to the vpn connection
tunnel-group vpn-ipsec-tunnel-grp type remote-access
tunnel-group vpn-ipsec-tunnel-grp general-attributes
address-pool vpn-ipsec-pool
authentication-server-group radius-grp
default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp
tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes
group-alias vpn-ipsec-tunnel-grp enable

```

Stap 15. Cryptografisch algoritme toevoegen

In ASA CLI voegt u groep 19 toe aan het IKEv2-beleid.

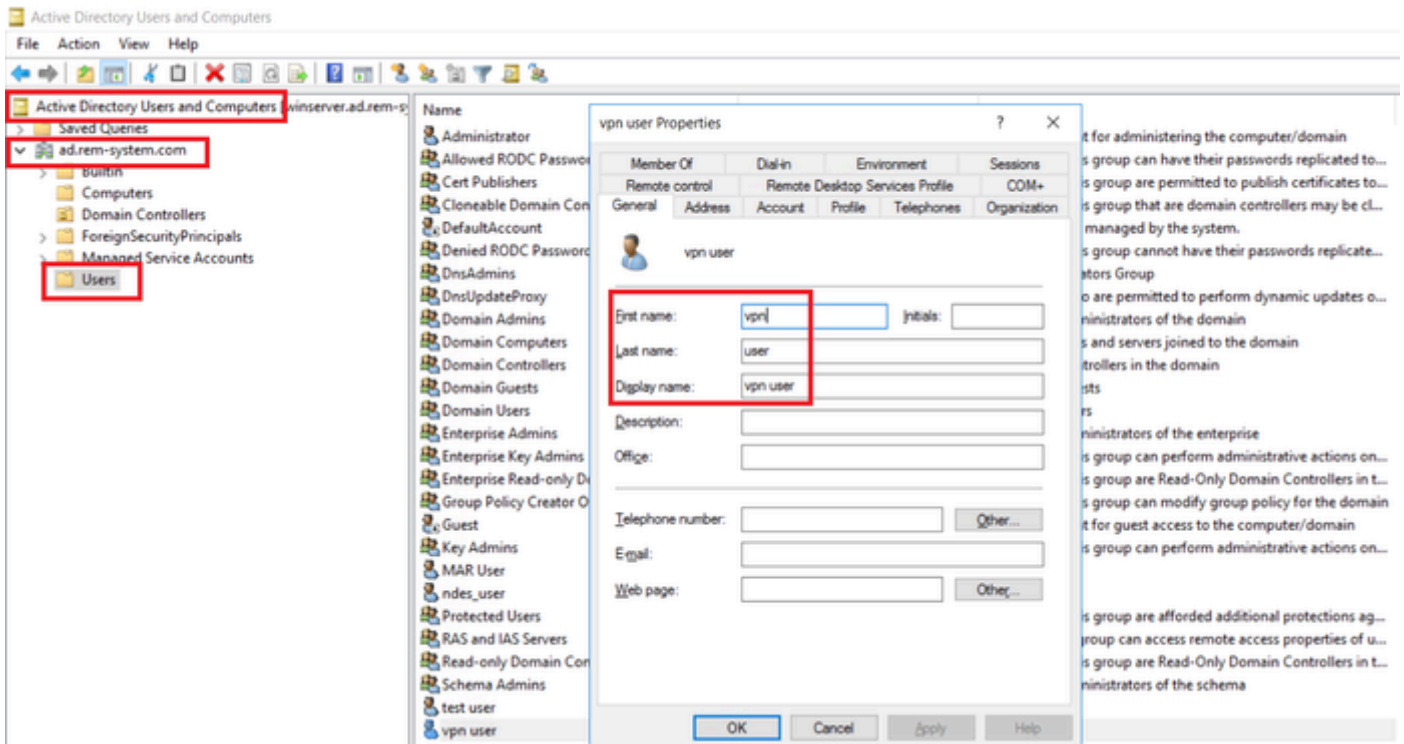


Opmerking: voor IKEv2/IPsec-verbindingen ondersteunt Cisco Secure Client vanaf versie 4.9.00086 niet langer Diffie-Hellman (DH) groepen 2, 5, 14 en 24. Deze verandering kan in verbindingsmislukkingen resulteren toe te schrijven aan cryptografische algoritmemismatches.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#
```

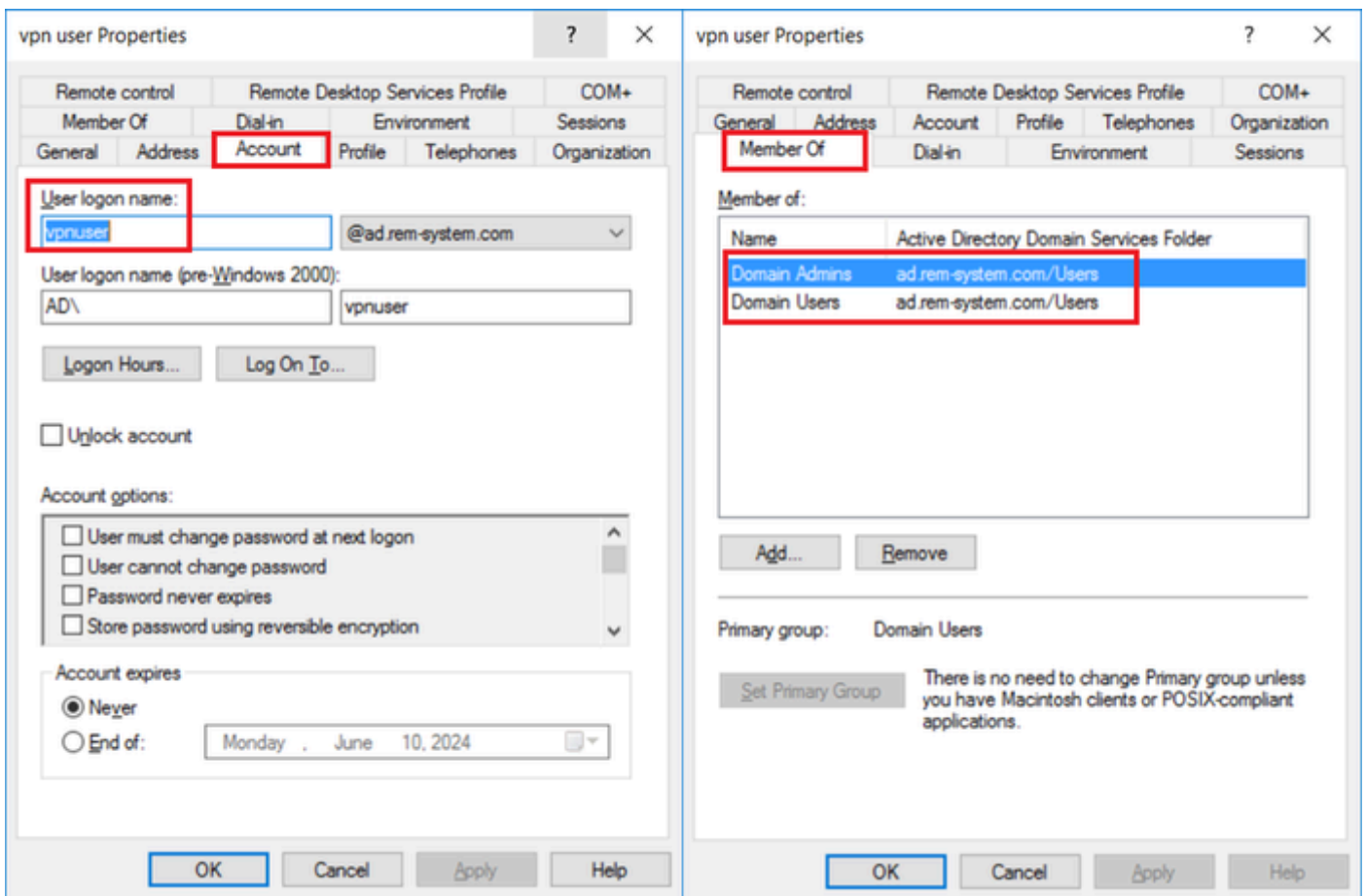
Configuratie in Windows-server

U moet een domeingebruiker toevoegen voor een VPN-verbinding. Navigeer naar Active Directory-gebruikers en -computers, klik op Gebruikers. Voeg vpnuser toe als domeingebruiker.



Domeingebruiker toevoegen

Voeg de domeingebruiker toe aan het lid van Domeinbeheerders en Domeingebruikers.

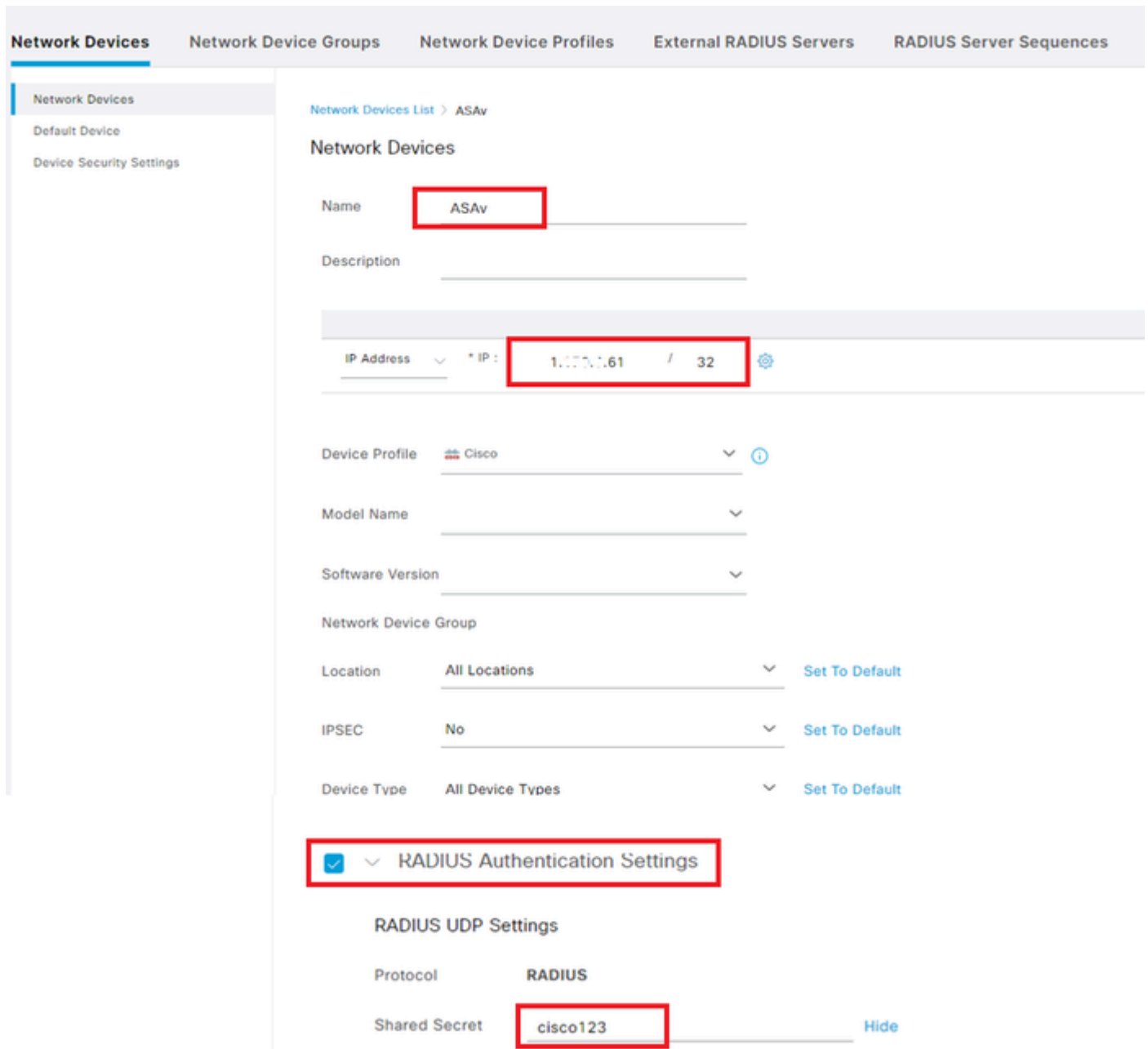


Domain Admins en domeingebruikers

Configuratie in ISE

Stap 1. Apparaat toevoegen

Navigeer naar Beheer > Netwerkkapparaten, klik op de knop Toevoegen om ASAv-apparaat toe te voegen.



The screenshot displays the ISE configuration interface for a Network Device. The main navigation tabs are Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, and RADIUS Server Sequences. The left sidebar shows the current configuration path: Network Devices > Default Device > Device Security Settings.

The configuration form for the ASAv device includes the following fields:

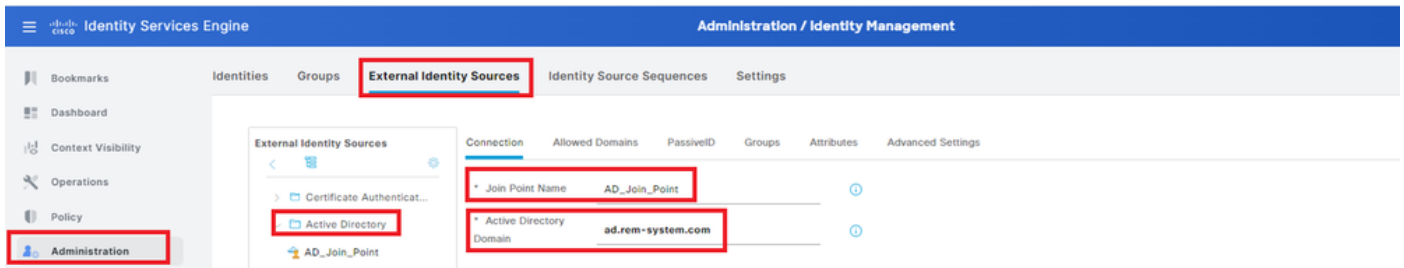
- Name: ASAv
- Description: (empty)
- IP Address: 1.1.1.1 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings
- RADIUS UDP Settings
 - Protocol: RADIUS
 - Shared Secret: cisco123 (Hide)

Apparaat toevoegen

Stap 2. Actieve map toevoegen

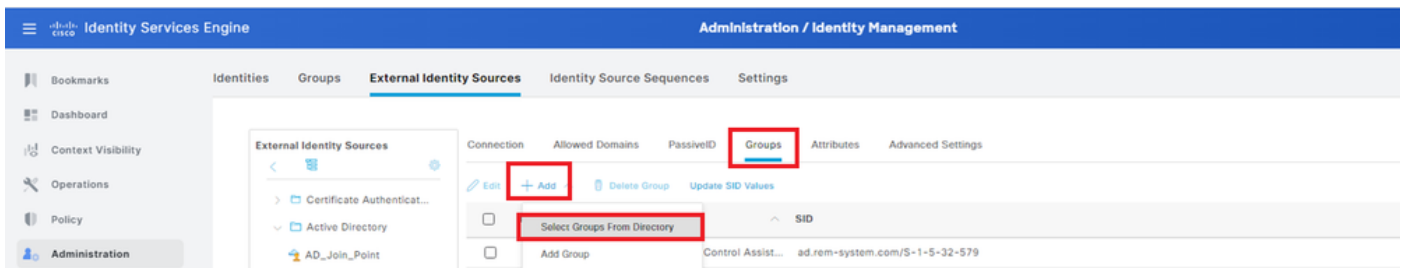
Navigeer naar Beheer > Externe Identiteitsbronnen > Active Directory, klik op Connectiontab, voeg Active Directory toe aan ISE.

- Lid worden: AD_Join_Point
- Active Directory-domein: ad.rem-system.com



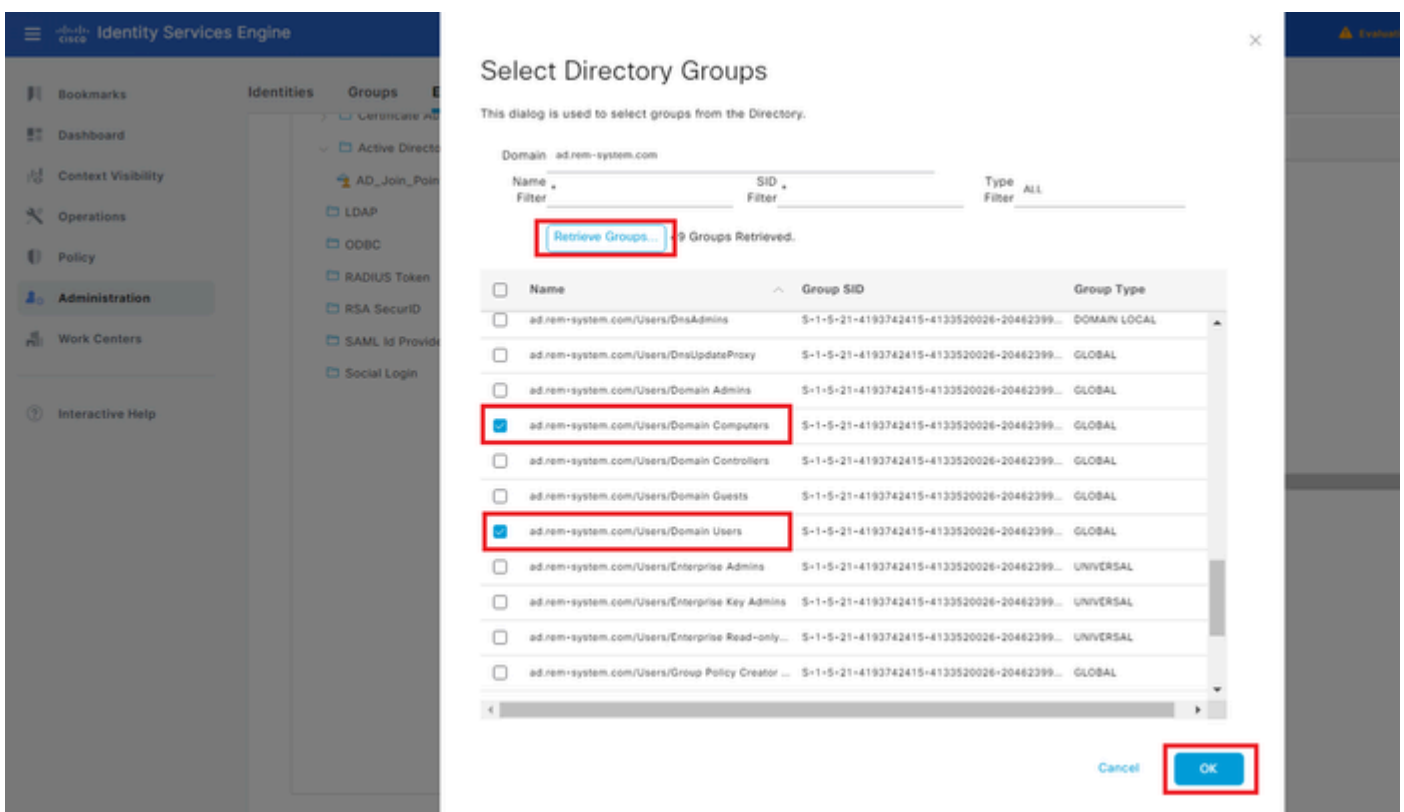
Actieve map toevoegen

Navigeer naar het tabblad Groepen, selecteer Groepen uit directoraat uit vervolgkeuzelijst.



Selecteer Groepen uit map

Klik op Groepen ophalen in de vervolgkeuzelijst. Checkad.rem-system.com/Users/Domain Computers and ad.rem-system.com/Users/Domain Gebruikers en klik op OK.



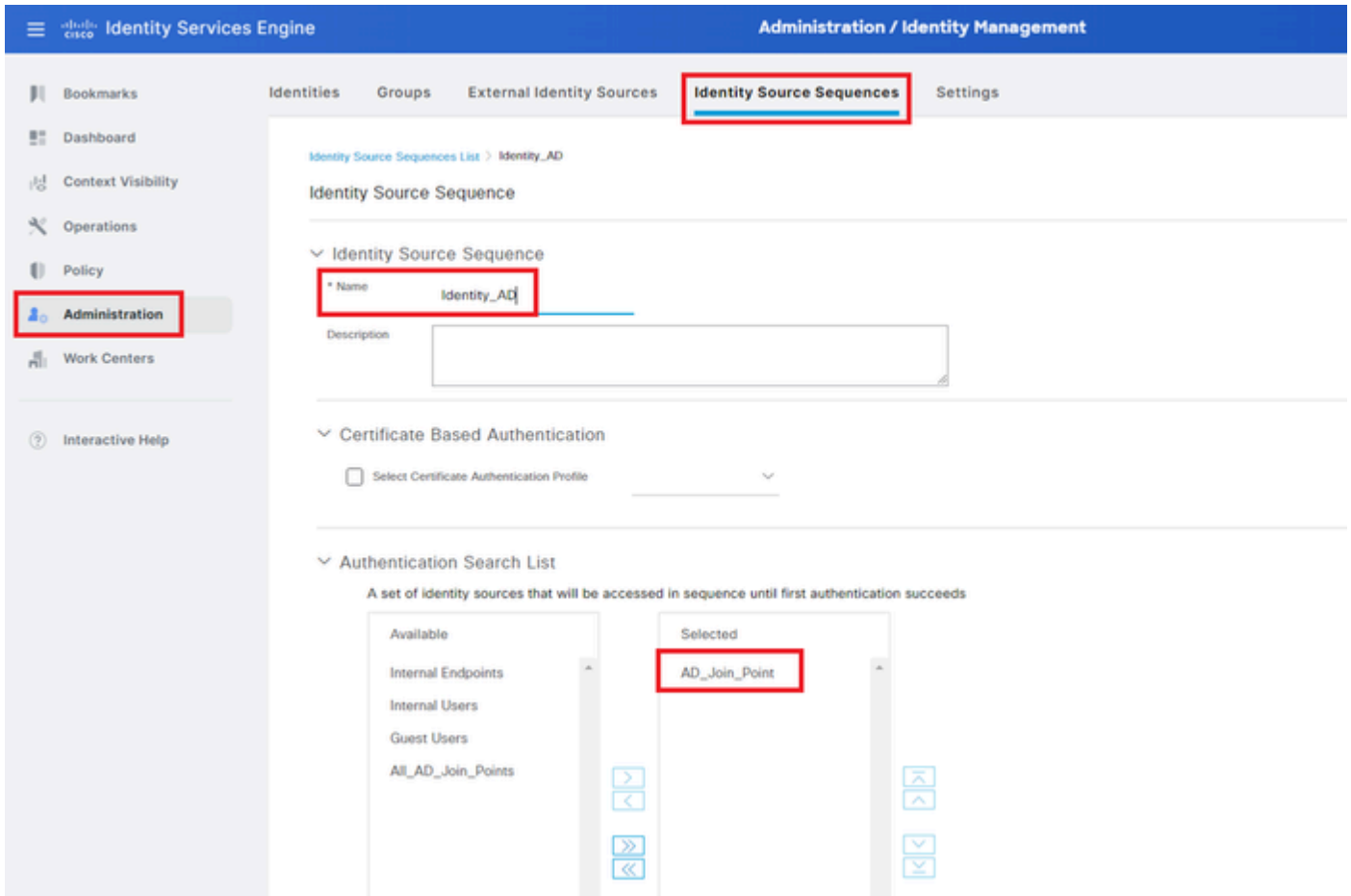
Domeincomputers en -gebruikers toevoegen

Stap 3. Identiteitsbroncode toevoegen

Navigeer naar Beheer > Identity Source Sequences, voeg een Identity Source Sequence toe.

- Naam: Identity_AD

- Verificatie Zoeklijst: AD_Join_Point

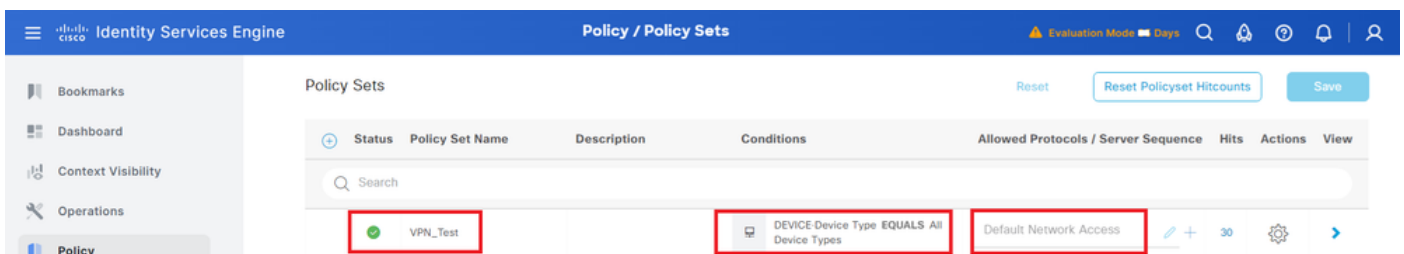


Identity Source Sequences toevoegen

Stap 4. Beleidsset toevoegen

Navigeer naar Policy > Policy Sets, klik op + om een policy set toe te voegen.

- Naam reeks beleid: VPN_Test
- Voorwaarden: Apparaattype komt overeen met alle apparaattypen
- Toegestane protocollen/serverreeks: standaard netwerktoegang



Beleidsset toevoegen

Stap 5. Verificatiebeleid toevoegen

Navigeer naar Beleidssets, klik op VPN_Test om een verificatiebeleid toe te voegen.

- Regelnaam: VPN_Verificatie

- Voorwaarden: IP-adres voor netwerktoegangsapparaat is gelijk aan 1.x.x.61
- Gebruik: Identity_AD

Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
+	VPN_Authentication	Network Access-Device IP Address EQUALS 1.1.1.1.61	Identity_AD > Options	10	

Verificatiebeleid toevoegen

Stap 6. Toepassingsbeleid toevoegen

Navigeer naar Beleidssets, klik op VPN_Test om een autorisatiebeleid toe te voegen.

- Regel Naam: VPN_Authorisation
- Voorwaarden: Network_Access_Authentication_Passed
- Resultaten: PermitAccess

Authorization Policy(2)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	

Toepassingsbeleid toevoegen

Verifiëren

Stap 1. Kopieer een beveiligd clientprofiel naar Win10 PC1

Kopieer het beveiligde clientprofiel naar de map C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.

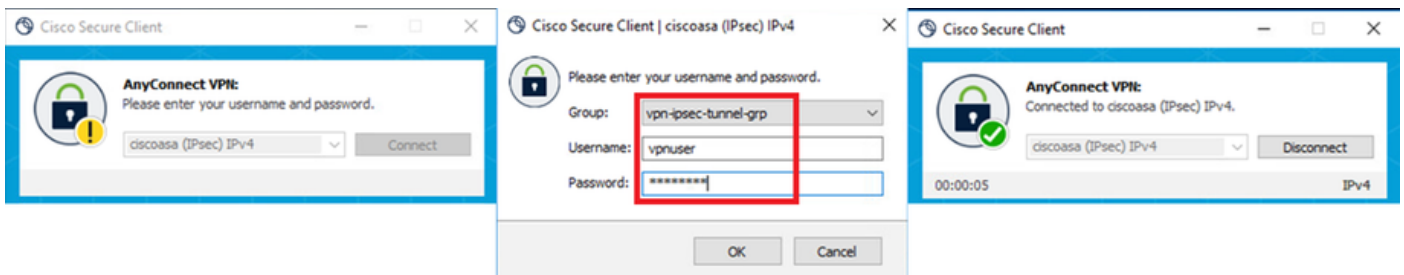
This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > VPN > Profile

Name	Date modified	Type
MgmtTun	5/17/2024 8:42 AM	File folder
vpn-ipsec-tunnel-grp_client_profile	5/17/2024 12:48 AM	XML Document
AnyConnectProfile.xsd	5/17/2024 1:12 PM	XSD File

Profiel naar PC kopiëren

Stap 2. VPN-verbinding starten

Voer in het eindpunt Cisco Secure Client uit en voer de gebruikersnaam en het wachtwoord in en controleer vervolgens of de verbindingen met Cisco Secure Client zijn geslaagd.



Verbinding geslaagd

Stap 3. Syslog op ASA bevestigen

In syslog, bevestig dat de verbinding IKEv2 slaagde.

```
<#root>
```

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser  
New Connection Established
```

```
May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

Stap 4. IPsec-sessie voor ASA bevestigen

voer de opdracht uit `show vpn-sessiondb detail anyconnect` om de IKEv2/IPsec-sessie op ASA te bevestigen.

```
<#root>
```

```
ciscoasa#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : vpnuser Index : 23  
Assigned IP : 172.16.1.20 Public IP : 192.168.1.11  
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent  
License : AnyConnect Premium  
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none  
Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none  
Bytes Tx : 840 Bytes Rx : 52408  
Pkts Tx : 21 Pkts Rx : 307  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp  
Tunnel Group : vpn-ipsec-tunnel-grp  
Login Time : 08:13:20 UTC Tue May 28 2024  
Duration : 0h:10m:10s  
Inactivity : 0h:00m:00s
```

VLAN Mapping : N/A VLAN : none
Audt Sess ID : 01aa003d0001700066559220
Security Grp : none

IKEv2 Tunnels: 1

IPsecOverNatT Tunnels: 1

AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 23.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : 5.1.3.62

IKEv2:
Tunnel ID : 23.2
UDP Src Port : 50982 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds
PRF : SHA256 D/H Group : 19
Filter Name :
Client OS : Windows Client Type : AnyConnect

IPsecOverNatT:
Tunnel ID : 23.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.1.20/255.255.255.255/0/0
Encryption : AES256 Hashing : SHA256
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307

Stap 5. Radius live log bevestigen

Navigeer naar **Operations > RADIUS > Live** Logs in ISE GUI en bevestig het live log voor VPN-verificatie.

Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...	Device Port	Identity Group
May 28, 2024 05:13:42...	●		0	00:50:56:98:77:A4	vpuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess				
May 28, 2024 05:13:42...	●		0	00:50:56:98:77:A4	vpuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation

RADIUS live log

Klik op Status om de details van het bewegend logbestand te bevestigen.

Overview

Event	5200 Authentication succeeded
Username	vpuser
Endpoint Id	00:50:56:98:77:A4
Endpoint Profile	Windows10-Workstation
Authentication Policy	VPN_Test >> VPN_Authentication
Authorization Policy	VPN_Test >> VPN_Authorization
Authorization Result	PermitAccess

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	1
15049	Evaluating Policy Group	36
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	6
15041	Evaluating Identity Policy	20
15048	Queried PIP - Network Access.Device IP Address	2
22072	Selected identity source sequence - Identity_AD	6
15013	Selected Identity Source - AD_Join_Point	1
24430	Authenticating user against Active Directory - AD_Join_Point	4
24325	Resolving identity - vpuser	38
24313	Search for matching accounts at join point - ad.rem-system.com	0
24319	Single matching account found in forest - ad.rem-system.com	0
24323	Identity resolution detected single matching account	0
24343	RPC Logon request succeeded - vpuser@ad.rem-system.com	23
24402	User authentication against Active Directory succeeded - AD_Join_Point	3
22037	Authentication Passed	1
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
15036	Evaluating Authorization Policy	1
24209	Looking up Endpoint in Internal Endpoints IDStore - vpuser	0
24211	Found Endpoint in Internal Endpoints IDStore	9
15048	Queried PIP - Network Access.AuthenticationStatus	2
15016	Selected Authorization Profile - PermitAccess	7
22081	Max sessions policy passed	6
22080	New accounting session created in Session cache	0
11002	Returned RADIUS Access-Accept	2

Detail van bewegend logboek

Problemen oplossen

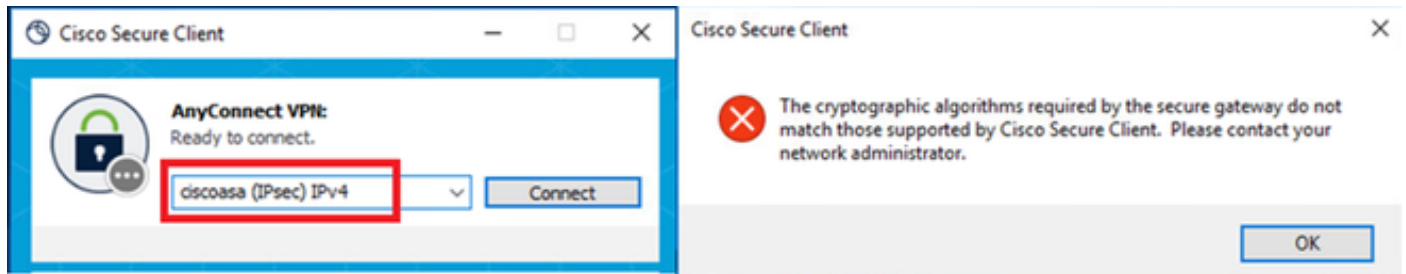
De cryptografische algoritmen mismatch kan resulteren in verbindingfouten. Dit is een voorbeeld van een probleem waarbij algoritmen niet overeenkomen. Het uitvoeren van Stap 15 van de sectie Configuration in ASDM kan het probleem oplossen.

Stap 1. VPN-verbinding starten

Voer op het eindpunt de Cisco Secure Client uit en bevestig dat de verbinding is mislukt vanwege een verkeerde match van cryptografische

algoritmen.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect. Please contact your network administrator.



Verbinding is mislukt

Stap 2. Syslog in CLI bevestigen

Bevestig in syslog dat de IKEv2-onderhandeling is mislukt.

<#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ

May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ER

Failed to find a matching policy

Referentie

[AnyConnect over IKEv2 naar ASA met AAA- en certificaatverificatie](#)

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.