

SD-WAN Remote Access (SDRA) configureren met AnyConnect en ISE-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Wat is een VPN voor externe toegang?](#)

[Wat is SD-WAN Remote Access VPN?](#)

[Split-tunneling vs Tunnel allemaal](#)

[Voor SDRA en na SDRA](#)

[Wat is FlexVPN?](#)

[Configuratie van voorwaarden](#)

[ISE-configuratie](#)

[Split-tunneling vs Tunnel allemaal in AnyConnect-client](#)

[CA-serverconfiguratie in Cisco IOS® XE](#)

[SD-WAN RA configuratie](#)

[Configuratie van Cryptie PKI](#)

[AAA-configuratie](#)

[FlexVPN-configuratie](#)

[SD-WAN RA configuratievoorbeeld](#)

[AnyConnect-clientconfiguratie](#)

[AnyConnect Profile Editor configureren](#)

[Installeer het AnyConnect Profile \(XML\)](#)

[De AnyConnect-downloader uitschakelen](#)

[Onvertrouwde servers verwijderen op AnyConnect-client](#)

[AnyConnect-client gebruiken](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u SD-WAN Remote Access (SDRA) kunt configureren met AnyConnect-client met een Cisco IOS® XE Autonomous Mode als een CA server en een Cisco Identity Services Engine (ISE) server voor verificatie, autorisatie en accounting.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- PKI-infrastructuur
- FlexVPN
- RADIUS-server

Gebruikte componenten

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

- C800V versie 17.07.01a
- vManager versie 20.7.1
- CSR 1000V-versie 17.03.04.a
- ISE versie 2.7.0.256
- AnyConnect Secure Mobility Client versie 4.10.04071

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Wat is een VPN voor externe toegang?

Op Remote Access VPN kan de externe gebruiker op een veilige manier verbinding maken met de bedrijfsnetwerken, toepassingen en gegevens gebruiken die alleen toegankelijk zijn via de apparaten die op het kantoor in de stekker zijn aangesloten.

Een VPN op afstand werkt door een virtuele tunnel die tussen het apparaat van een werknemer en het netwerk van het bedrijf is gemaakt.

Deze tunnel gaat door het openbare internet, maar de data die heen en weer gestuurd worden, worden beschermd door encryptie en veiligheidsprotocollen om het privé en veilig te houden.

De twee belangrijkste componenten in dit type VPN zijn een server voor netwerktoegang/RA head-end en VPN clientsoftware.

Wat is SD-WAN Remote Access VPN?

De externe toegang is geïntegreerd in de SD-WAN oplossing die de noodzaak van afzonderlijke Cisco SD-WAN en RA-infrastructuur overbodig maakt en snelle schaalbaarheid van RA-services mogelijk maakt met het gebruik van Cisco AnyConnect als RA-softwareclient.

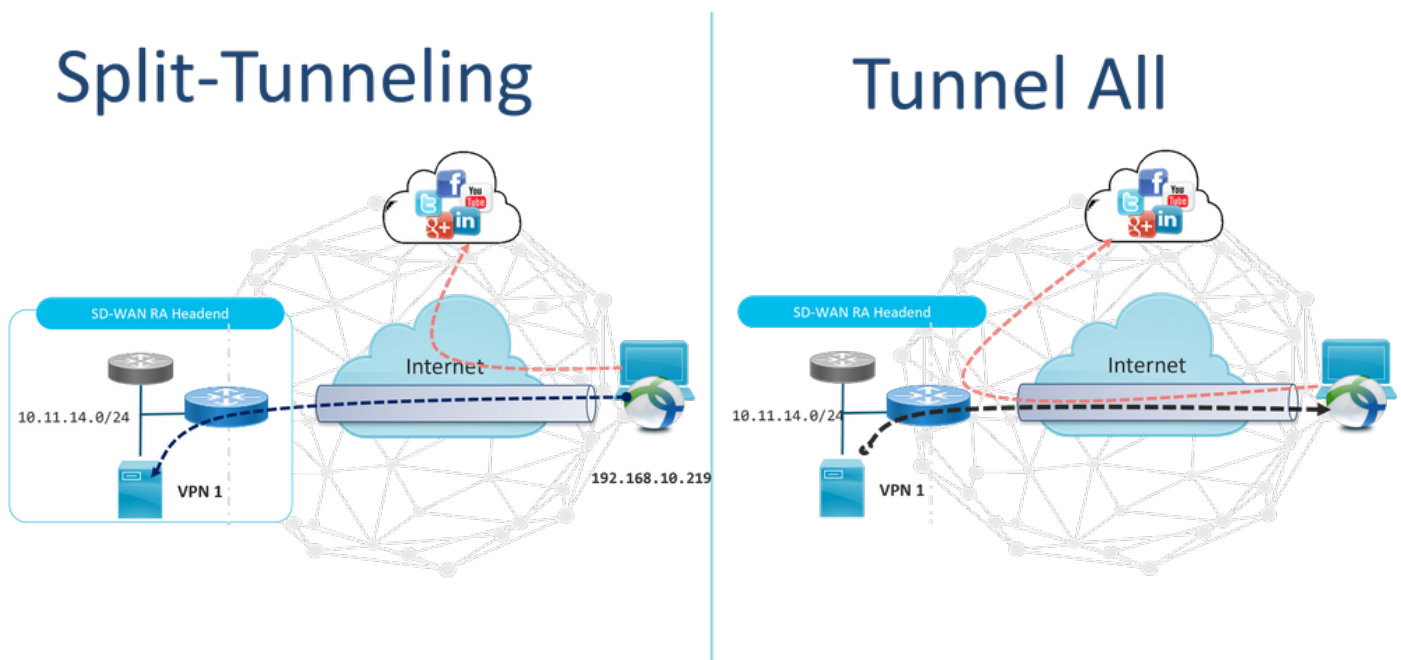
Externe toegang biedt externe gebruikers toegang tot het netwerk van de organisatie. Hierdoor kan het werk van thuis worden uitgevoerd.

De voordelen

- RA biedt toegang tot het netwerk van een organisatie vanaf apparaten/gebruikers op afgelegen locaties. (HO)
- Hiermee wordt de Cisco SD-WAN oplossing uitgebreid naar gebruikers die niet beschikken over het apparaat van elke RA-gebruiker om deel uit te maken van het Cisco SD-WAN weefsel.
- Gegevensbeveiliging
- Split-tunneling of Tunnel allemaal
- schaalbaarheid
- Vermogen om de RA lading over talrijke Cisco IOS® XE SD-WAN apparaten in de Cisco SD-WAN stof te verdelen.

Split-tunneling vs Tunnel allemaal

Split-tunneling wordt gebruikt in scenario's waar alleen specifiek verkeer moet worden getunneld (SD-WAN bijvoorbeeld) zoals in de afbeelding.

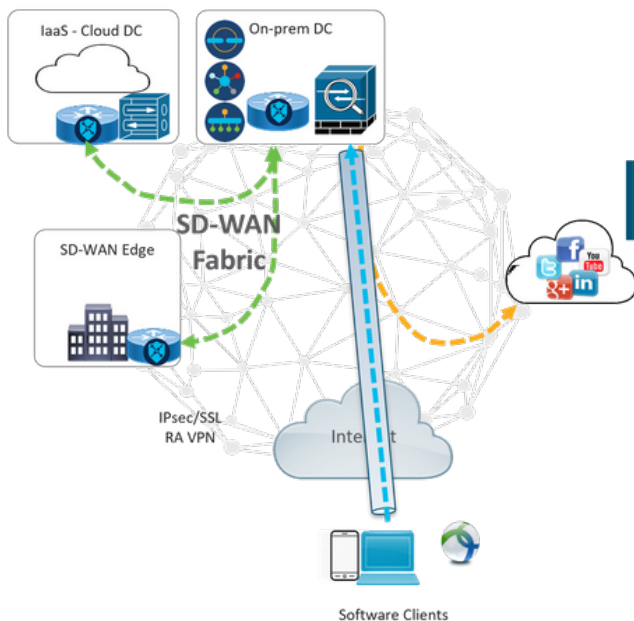


Voor SDRA en na SDRA

Het traditionele ontwerp van VPN-toegang op afstand vereist afzonderlijke RA-infrastructuur buiten de Cisco SD-WAN fabric om toegang van externe gebruikers tot het netwerk te bieden zoals niet SD-WAN-apparaten zoals ASA, Reguliere Cisco IOS® XE of apparaten van derden, en RA-verkeer wordt naar SD-WAN verplaatst zoals in de afbeelding wordt weergegeven.

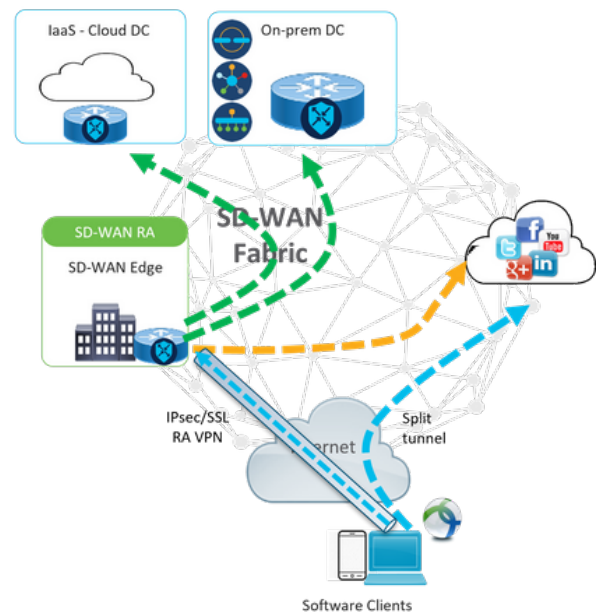
Before SDRA

Traditional Remote-Access VPN design with SDWAN



After SDRA

SD-WAN Remote-Access



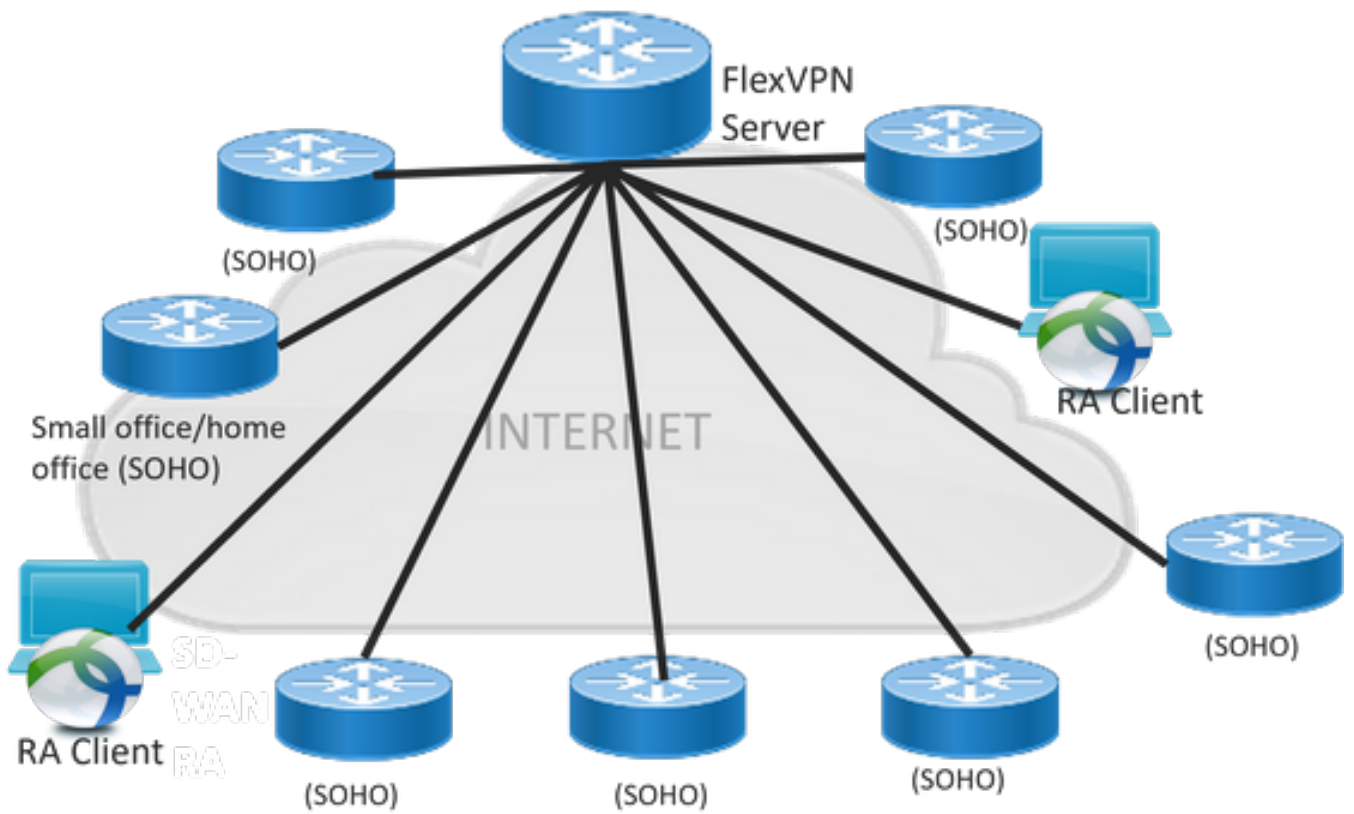
De SD-WAN Remote Access verandert de manier waarop gebruikers op afstand met het netwerk verbinden. Ze verbinden rechtstreeks aan de cEdge die als RA-head-end wordt gebruikt. Uitbreidt Cisco SD-WAN functies en voordelen voor RA gebruikers. RA-gebruikers worden tak LAN-zijgebruikers.

Voor elke RA-client kent de SD-WAN RA head-end een IP-adres toe aan een RA-client en voegt een statische host-route toe aan het toegewezen IP-adres in het VRF waarin de RA-gebruiker wordt geplaatst.

De statische route specificeert de VPN-tunnel van de RA client-verbinding. De SD-WAN RA head-end adverteert de statische IP binnen de service VRF van de RA client met het gebruik van OMP aan alle randapparaten in de service VPN.

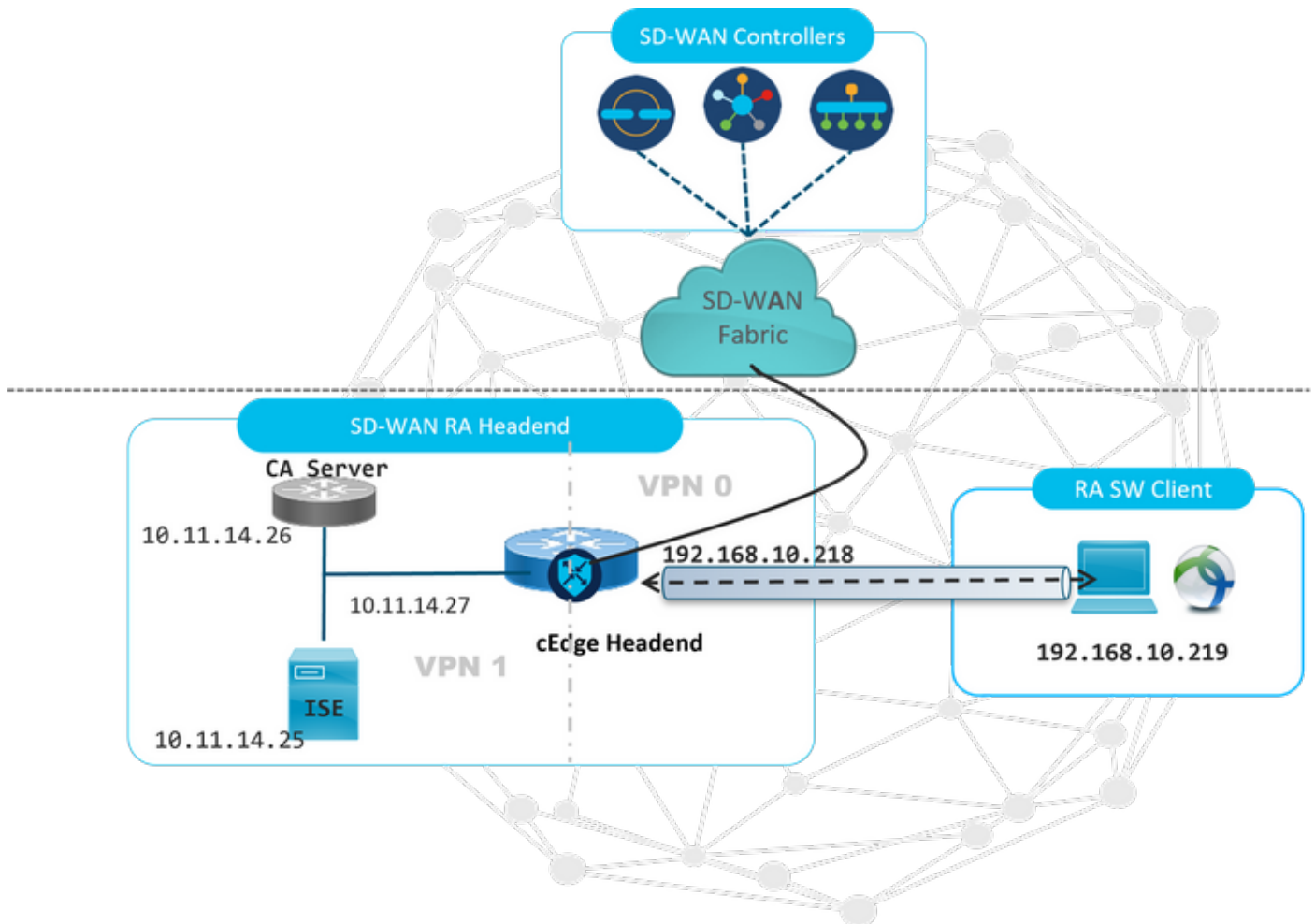
Wat is FlexVPN?

SD-WAN RA maakt gebruik van de Cisco FlexVPN RA-oplossing. FlexVPN is de implementatie van Cisco van de IKEv2 standaard optie een verenigd paradigma en CLI die site combineert met site, **externe toegang**, hub en gedeelde topologieën en partiële netwerken (gesproken met Direct). FlexVPN biedt een eenvoudig maar modulair kader dat uitgebreid het paradigma van de tunnelinterface gebruikt terwijl het compatibel blijft met oudere VPN-implementaties.



Configuratie van voorwaarden

Dit voorbeeld: er is een SD-WAN RA lab instellingen gemaakt zoals in de afbeelding.



Er zijn extra onderdelen ingesteld voor dit SD-WAN RA-labscenario:

- Een reguliere Cisco IOS® XE in Autonomous Mode als een CA server.
- Een ISE/RADIUS-server voor verificatie, autorisatie en accounting.
- Een Windows PC met bereikbaarheid aan de cEdge door de WAN-interface.
- AnyConnect-client al geïnstalleerd.

Opmerking: De CA- en RADIUS-servers zijn in de dienst VRF 1 geplaatst. Beide servers moeten bereikbaar zijn via de service VRF voor alle SD-WAN RA head-ends.

Opmerking: De Cisco SD-WAN Remote Access wordt ondersteund op de versie 17.7.1a en specifieke apparaten voor SDRA. Raadpleeg voor ondersteunde apparaten: [Ondersteunde platforms voor de SD-WAN RA head-end](#)

ISE-configuratie

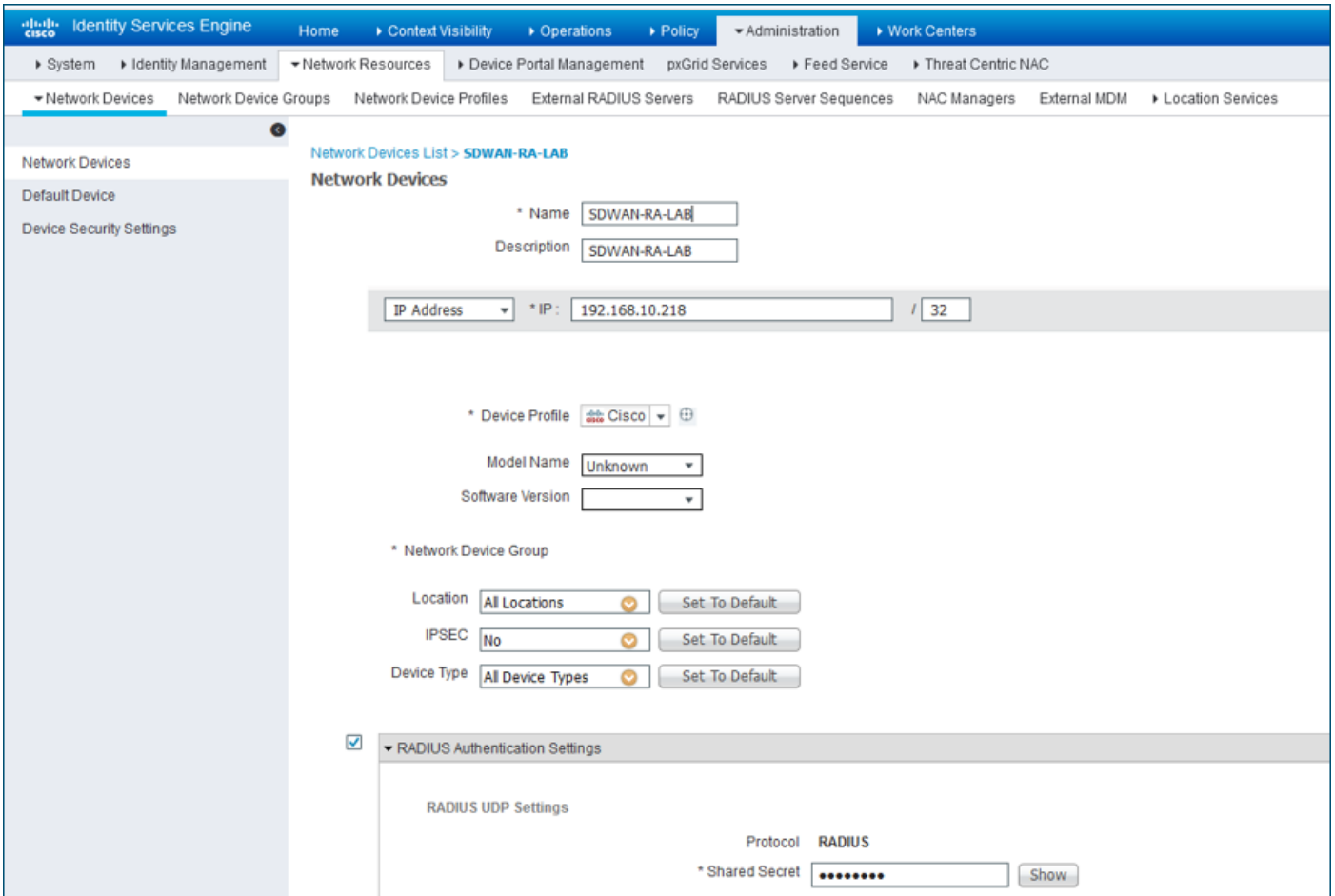
Om het SD-WAN RA head-end te ondersteunen, moet u ervoor zorgen dat de parameters op de RADIUS-server worden geconfigureerd. Deze parameters zijn vereist voor RA-verbindingen:

- Verificatiegegevens gebruiker Gebruikersnaam en wachtwoord voor AnyConnect-EAP-verbindingen
- Beleidsparameters (eigenschappen) die van toepassing zijn op een gebruiker of een gebruikersgroep **VRF:** Service VPN die de RA-gebruiker heeft toegewezen aan **IP-poolnaam:**

Naam van de IP-pool die op het hoofd van de RA is gedefinieerd **Serversubnetten**:
Subnettoegang voor de RA-gebruiker

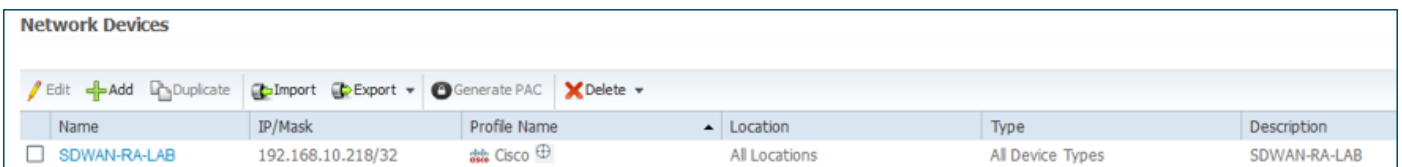
De eerste stap om in ISE te configureren is het RA head-end of cEdge IP-adres als een netwerkapparaat dat Radius-verzoeken aan ISE kan indienen.

Blader naar > **Netwerkapparaten** en voeg het RA head-end (cEdge) IP-adres en wachtwoord toe zoals in de afbeelding.



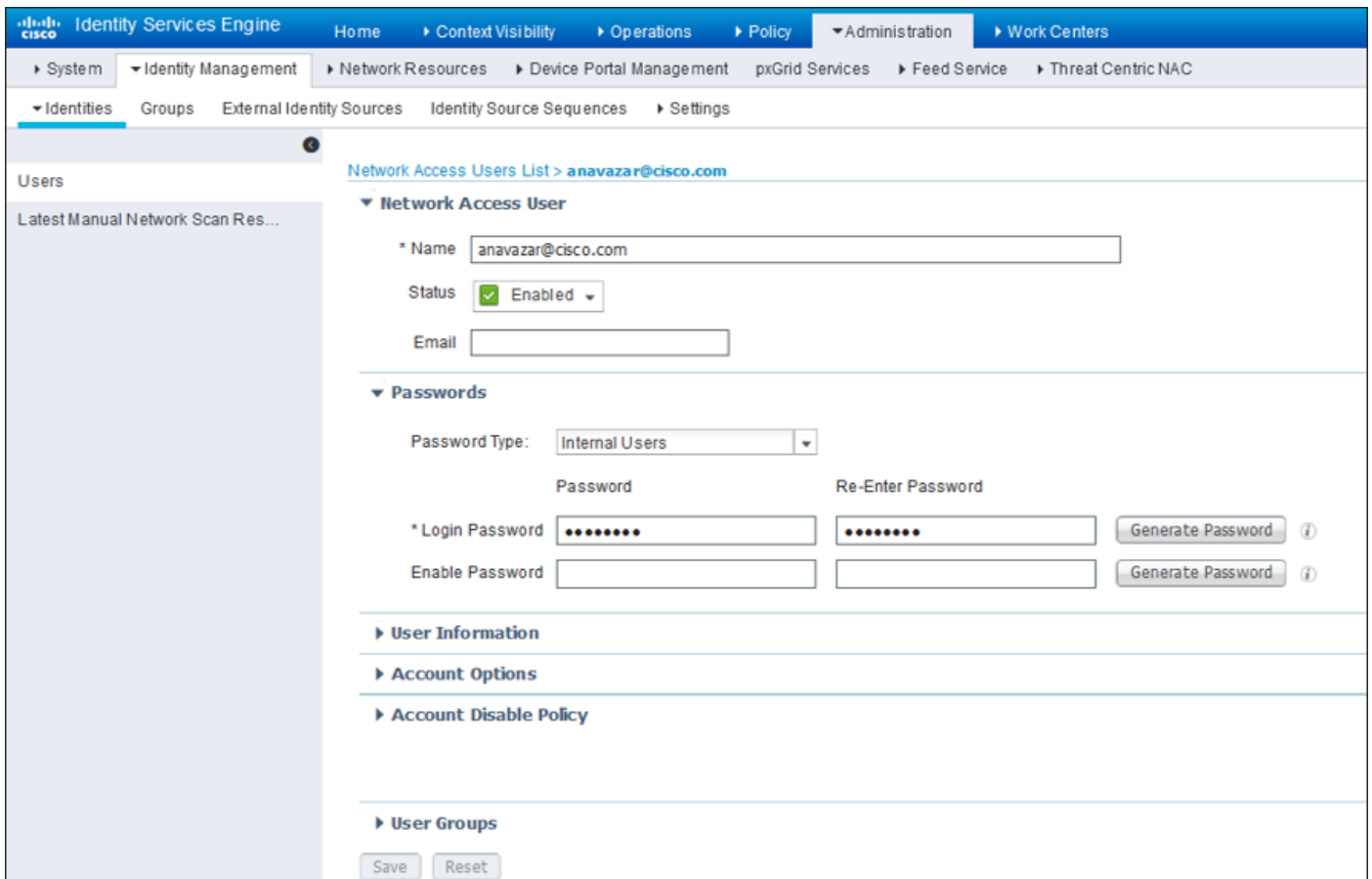
The screenshot shows the configuration page for a Network Device in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices List > SDWAN-RA-LAB' and 'Network Devices'. The configuration fields are: Name: SDWAN-RA-LAB, Description: SDWAN-RA-LAB, IP Address: 192.168.10.218 / 32, Device Profile: Cisco, Model Name: Unknown, Software Version: (empty), Network Device Group: Location: All Locations, IPSEC: No, Device Type: All Device Types. The 'RADIUS Authentication Settings' section is checked and shows 'RADIUS UDP Settings' with Protocol: RADIUS and a Shared Secret field.

Netwerkapparaat toegevoegd zoals in de afbeelding.

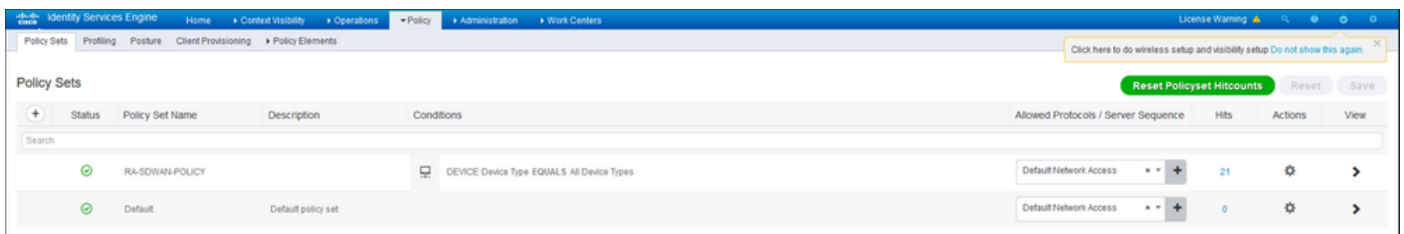


Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> SDWAN-RA-LAB	192.168.10.218/32	Cisco	All Locations	All Device Types	SDWAN-RA-LAB

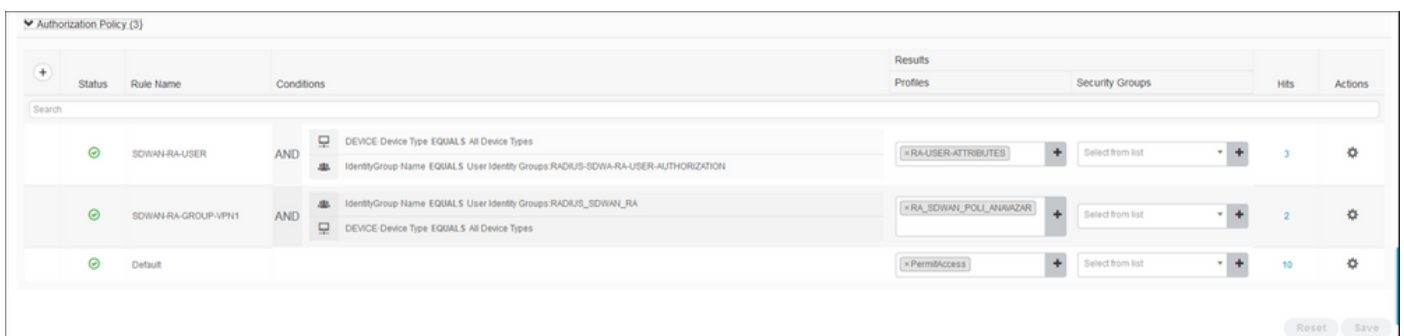
In de RADIUS-server moet u de gebruikersnamen en het wachtwoord voor de AnyConnect-verificatie configureren zoals in de afbeelding. Navigeer naar **Administratie > Identificaties**.



Er moet een beleidsset worden gemaakt met de matchconditie die moet worden gebruikt, zoals in de afbeelding. In dit geval wordt de voorwaarde **Alle apparaten** gebruikt, wat betekent dat alle gebruikers op dit beleid klikken.



Vervolgens is het machtigingsbeleid per voorwaarde in het leven geroepen. De voorwaarde **Alle apparaten** en de identiteitsgroepen die moeten worden aangepast.



In het **autorisatieprofiel** moeten we het **toegangstype** als **Access_ACCEPT** configureren onder de **geavanceerde kenmerken-instellingen**, de **Cisco-verkoper** en **Cisco-AV-paar-eigenschap** selecteren.

Het is nodig om bepaalde beleidsparameters voor de gebruikers te configureren:

- VRF, de service VRF waartoe de gebruiker behoort.
- De IP pool naam, elke gebruikersverbinding wordt een IP adres toegewezen, dat tot de IP pool in de cEdge gevormd behoort.
- het subnetwerk waartoe de gebruiker toegang heeft

Voorzichtig: De opdracht **IP-doorsturen** moet vóór de **IP**-opdracht zonder **nummer** komen. Als de virtuele toegangsinterface van de virtuele sjabloon is gekloond en de opdracht **IP-doorsturen** dan wordt toegepast, wordt elke IP-configuratie verwijderd van de virtuele toegangsinterface.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled 'Authorization Profiles > RA_SDWAN_POLI_ANAVAZAR' and shows the configuration for an Authorization Profile. The fields are as follows:

- * Name: RA_SDWAN_POLI_ANAVAZAR
- Description: VRF + POOL + SUBNETS + SGT
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

The screenshot shows the 'Advanced Attributes Settings' and 'Attributes Details' for the RA_SDWAN_POLI_ANAVAZAR profile. The 'Advanced Attributes Settings' section contains four rows of attribute mappings:

- Cisco:cisco-av-pair = ip:interface-config=vrf forwardi...
- Cisco:cisco-av-pair = onfig=ip unnumbered Loopback1
- Cisco:cisco-av-pair = ipsec:addr-pool=RA-POOL
- Cisco:cisco-av-pair = ipsec:route-set=prefix 10.11.1...

The 'Attributes Details' section shows the following configuration:

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=vrf forwarding 1
cisco-av-pair = ip:interface-config=ip unnumbered Loopback1
cisco-av-pair = ipsec:addr-pool=RA-POOL
cisco-av-pair = ipsec:route-set=prefix 10.11.14.0/24

```

At the bottom of the section, there are 'Save' and 'Reset' buttons.

Kenmerken gebruiker:

Access Type = ACCESS_ACCEPT

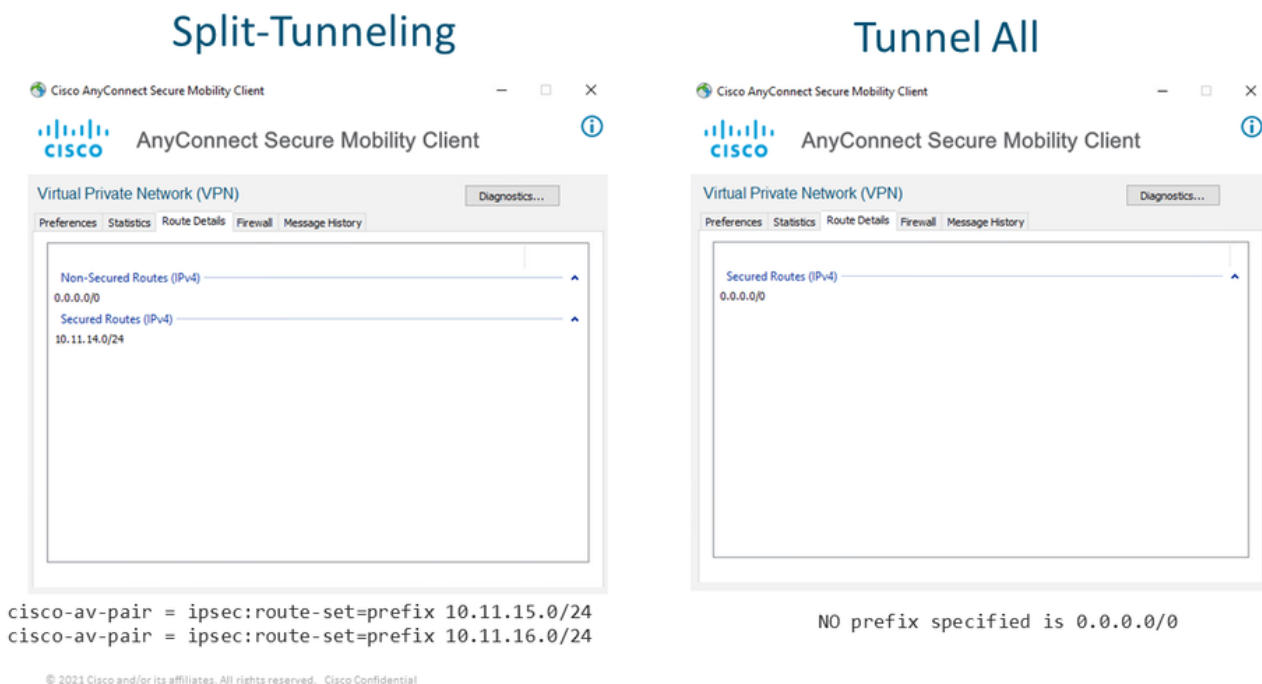
```

cisco-av-pair = ip:interface-config=vrf forwarding 1
cisco-av-pair = ip:interface-config=ip unnumbered Loopback1
cisco-av-pair = ipsec:addr-pool=RA-POOL
cisco-av-pair = ipsec:route-set=prefix 10.11.15.0/24
cisco-av-pair = ipsec:route-set=prefix 10.11.16.0/24

```

Split-tunneling vs Tunnel allemaal in AnyConnect-client

`ipsec:route-set=prefix` dat wordt ontvangen in de AnyConnect-client is geïnstalleerd zoals in de afbeelding.



CA-serverconfiguratie in Cisco IOS® XE

De CA server provisioningcertificaten aan de Cisco IOS® XE SD-WAN apparaten en stelt de RA head-end in staat om zichzelf te authentifieren aan RA klanten.

CEDGE kan geen CA server zijn aangezien deze crypto PKI serveropdrachten niet worden ondersteund in Cisco IOS® XE SD-WAN.

- Een RSA-toetsenpaar genereren
- Maak het PKI-beheerpunt voor de CA-server Configureer het raypaar met de eerder gegenereerde SLEUTEL-CA.

Opmerking: De PKI server en PKI trustpoint moeten dezelfde naam gebruiken.

- Een CA-server maken Emulation Name voor uw CA-server instellenActiveert de CA-server met "No shutdown"

```
crypto key generate rsa modulus 2048 label KEY-CA
!
crypto pki trustpoint CA
  revocation-check none
  rsakeypair KEY-CA
  auto-enroll
!
crypto pki server CA
  no database archive
  issuer-name CN=CSR1Kv_SDWAN_RA
  grant auto
  hash sha1
  lifetime certificate 3600
  lifetime ca-certificate 3650
  auto-rollover
no shutdown
!
```

Controleer of de CA server is ingeschakeld.

```
CA-Server-CSRv#show crypto pki server CA
Certificate Server CA:
  Status: enabled
  State: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: CN=CSR1Kv_SDWAN_RA
  CA cert fingerprint: 10DA27AD EF54A3F8 12925750 CE2E27EB
  Granting mode is: auto
  Last certificate issued serial number (hex): 3
  CA certificate expiration timer: 23:15:33 UTC Jan 17 2032
  CRL NextUpdate timer: 05:12:12 UTC Jan 22 2022
  Current primary storage dir: nvram:
  Database Level: Minimum - no cert data written to storage
  Auto-Rollover configured, overlap period 30 days
  Autorollover timer: 23:15:37 UTC Dec 18 2031
```

Controleer of het CA-servercertificaat is geïnstalleerd.

```
CA-Server-CSRv#show crypto pki certificates verbose CA
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
  cn=CSR1Kv_SDWAN_RA
  Subject:
  cn=CSR1Kv_SDWAN_RA
  Validity Date:
  start date: 23:15:33 UTC Jan 19 2022
  end date: 23:15:33 UTC Jan 17 2032
  Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 10DA27AD EF54A3F8 12925750 CE2E27EB
  Fingerprint SHA1: 44E256C3 4FA45C5D F0398630 9D88B75E 5026CE4A
  X509v3 extensions:
  X509v3 Key Usage: 86000000
  Digital Signature
  Key Cert Sign
  CRL Signature
```

```
X509v3 Subject Key ID: 92F7CD72 355AA85F 672867D4 EC0C10C5 0B177C38
X509v3 Basic Constraints:
CA: TRUE
X509v3 Authority Key ID: 92F7CD72 355AA85F 672867D4 EC0C10C5 0B177C38
Authority Info Access:
Cert install time: 23:44:35 UTC Mar 13 2022
Associated Trustpoints: -RA-trustpoint CA
Storage: nvram:CSR1Kv_SDWAN#1CA.cer
```

De **Fingerprint SHA 1** van het CA-certificaat wordt gebruikt op het **crypto-ki-trustpunt** in de cEdge-router (RA head-end) met de configuratie van de toegang op afstand.

```
Fingerprint SHA1: 44E256C3 4FA45C5D F0398630 9D88B75E 5026CE4A
```

SD-WAN RA configuratie

Opmerking: Dit document is niet van toepassing op het SD-WAN onboarding proces voor controllers en cEdge. Er wordt aangenomen dat het SD-WAN weefsel omhoog en volledig functioneert.

Configuratie van Cryptie PKI

- Maak PKI-vertrouwen.
- Configureer de URL voor de CA-server.
- Kopieer de vingerafdruk sha 1 van het CA server certificaat.
- Configureer de naam van het onderwerp en de ALT-naam voor het nieuwe identiteitsbewijs.
- Configureer de parameter met de eerder gegenereerde SLEUTEL-ID.

```
crypto pki trustpoint RA-TRUSTPOINT
subject-name CN=cEdge-SDWAN-1.crv
enrollment url http://10.11.14.226:80
fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
subject-name CN=cEdge-SDWAN-1.crv
vrf 1
rsa-keypair KEY-NEW
revocation-check none
```

Vraag om een CA-certificaat voor authenticatie:

```
crypto pki authenticate RA-TRUSTPOINT
```

hiermee wordt de CSR gegenereerd, naar de CA-server verzonden en het nieuwe identiteitsbewijs ontvangen:

```
Crypto pki enroll RA-TRUSTPOINT
```

Controleer het CA-certificaat en het cEdge-certificaat:

```
cEdge-207#show crypto pki certificates RA-TRUSTPOINT
Certificate
```

Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
 cn=CSR1Kv_SDWAN_RA
Subject:
 Name: cEdge-207
 hostname=cEdge-207
 cn=cEdge-SDWAN-1.crv
Validity Date:
 start date: 03:25:40 UTC Jan 24 2022
 end date: 03:25:40 UTC Dec 3 2031
Associated Trustpoints: **RA-TRUSTPOINT**
Storage: nvram:CSR1Kv_SDWAN#4.cer

CA Certificate

Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
 cn=CSR1Kv_SDWAN_RA
Subject:
 cn=CSR1Kv_SDWAN_RA
Validity Date:
 start date: 23:15:33 UTC Jan 19 2022
 end date: 23:15:33 UTC Jan 17 2032
Associated Trustpoints: **RA-TRUSTPOINT**
Storage: nvram:CSR1Kv_SDWAN#1CA.cer

AAA-configuratie

```
aaa new-model
!
aaa group server radius ISE-RA-Group
 server-private 10.11.14.225 key Cisc0123
 ip radius source-interface GigabitEthernet2
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
```

FlexVPN-configuratie

IP-telefoon configureren

```
ip local pool RA-POOL 10.20.14.1 10.20.14.100
```

Configureer een IKEv2-voorstel (CIFERS en parameters) en beleid:

```
crypto ikev2 proposal IKEV2-RA-PROP
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256
```

```
crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
```

Het configureren van een IKEv2 profielnaam:

```
crypto ikev2 name-mangler IKEV2-RA-MANGLER
eap suffix delimiter @
```

Opmerking: De naam-beheerder leidt de naam af van het voorvoegsel in de EAP-identiteit (gebruikersnaam) die wordt gedefinieerd in de EAP-identiteit die het voorvoegsel en het achtervoegsel scheidt.

IPsec-telefoons configureren:

```
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
mode tunnel
```

Configuratie van Crypto IKEv2 profiel:

```
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
match identity remote any
identity local address 192.168.10.218
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint RA-TRUSTPOINT
aaa authentication anyconnect-eap ISE-RA-Authentication
aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
aaa accounting anyconnect-eap ISE-RA-Accounting
```

Configuratie van Crypto IPSEC profiel:

```
crypto ipsec profile IKEV2-RA-PROFILE
set transform-set IKEV2-RA-TRANSFORM-SET
set ikev2-profile RA-SDWAN-IKEV2-PROFILE
```

Sjablooninterface configureren

```
!
interface Virtual-Template101 type tunnel
vrf forwarding 1
tunnel mode ipsec ipv4
tunnel protection ipsec profile IKEV2-RA-PROFILE
```

Configuratie van virtuele sjabloon in het profiel Crypto IKEv2:

```
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
virtual-template 101
```

SD-WAN RA configuratievoorbeeld

```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
```

```

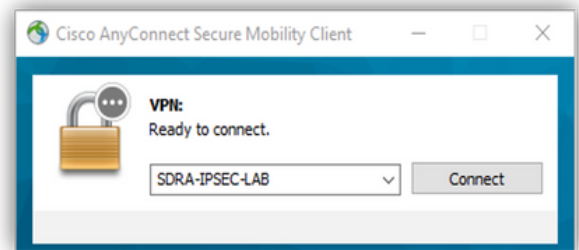
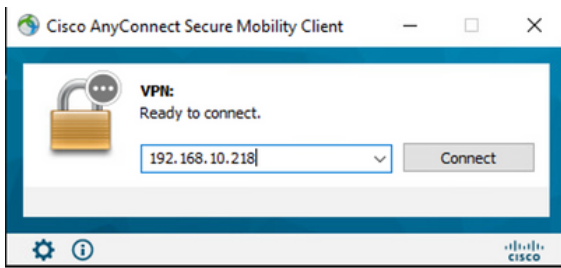
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
!
crypto pki trustpoint RA-TRUSTPOINT
  subject-name CN=cEdge-SDWAN-1.crv
  enrollment url http://10.11.14.226:80
  fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
  subject-name CN=cEdge-SDWAN-1.crv
  vrf 1
  rsakeypair KEY-NEW
  revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
  eap suffix delimiter @
!
crypto ikev2 proposal IKEV2-RA-PROP
  encryption aes-cbc-256
  integrity sha256
  group 19
  prf sha256
!
crypto ikev2 policy IKEV2-RA-POLICY
  proposal IKEV2-RA-PROP
!
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
  match identity remote any
  identity local address 192.168.10.218
  authentication local rsa-sig
  authentication remote anyconnect-eap aggregate
  pki trustpoint RA-TRUSTPOINT
  aaa authentication anyconnect-eap ISE-RA-Authentication
  aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
  aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
  aaa accounting anyconnect-eap ISE-RA-Accounting
!
crypto ipsec profile IKEV2-RA-PROFILE
  set transform-set IKEV2-RA-TRANSFORM-SET
  set ikev2-profile RA-SDWAN-IKEV2-PROFILE
!
interface Virtual-Template101 type tunnel
  vrf forwarding 1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile IKEV2-RA-PROFILE
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
  virtual-template 101

```

AnyConnect-clientconfiguratie

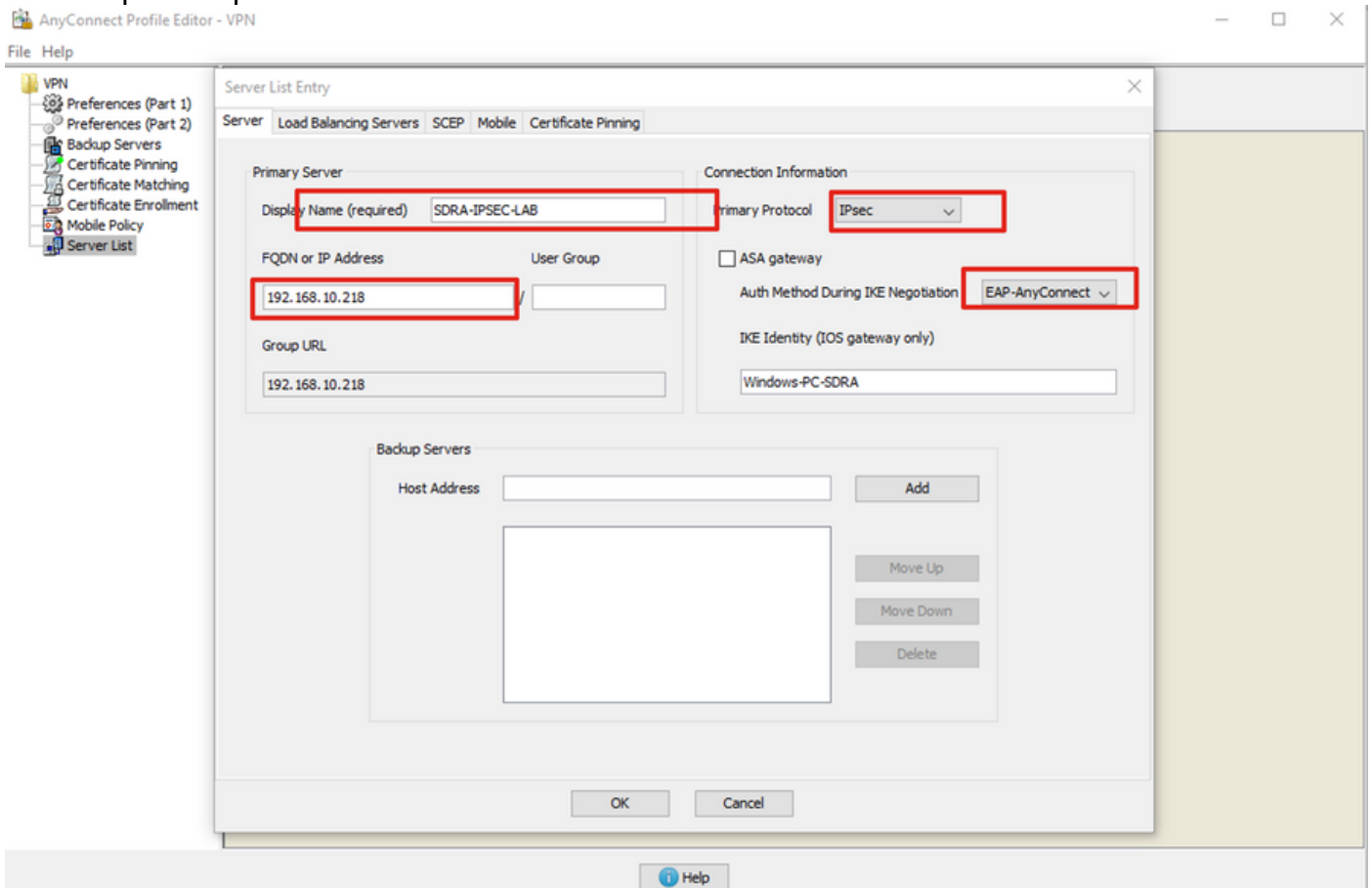
De AnyConnect-client gebruikt SSL als het standaardprotocol voor tunnelvestiging, en dit protocol wordt niet ondersteund voor SD-WAN RA (Routekaart). RA gebruikt FlexVPN, daarom is IPSEC het gebruikte protocol en is het verplicht om het te veranderen en dit gebeurt via het XML-profiel.

De gebruiker kan de FQDN van de gateway van VPN in de adresbalk van de AnyConnect-client invoeren. Dit resulteert in de SSL verbinding naar de gateway.



AnyConnect Profile Editor configureren

- Navigeer naar **serverlijst** en klik op **Toevoegen**.
- Selecteer **IPsec** als "Primair Protocol".
- Schakel de optie **ASA-gateway** uit.
- Selecteer **EAP-AnyConnect** als de "Auth Methode Tijdens de IKE-onderhandeling".
- **Display/Name (Requirements)** is de naam die wordt gebruikt om deze verbinding op te slaan onder de AnyConnect-client.
- **FQDN - of IP-adres** moet bij het cEdge (openbare) IP-adres worden ingevuld.
- Het profiel opslaan.



Installeer het AnyConnect Profile (XML)

Het XML-profiel kan handmatig in de directory worden geplaatst:

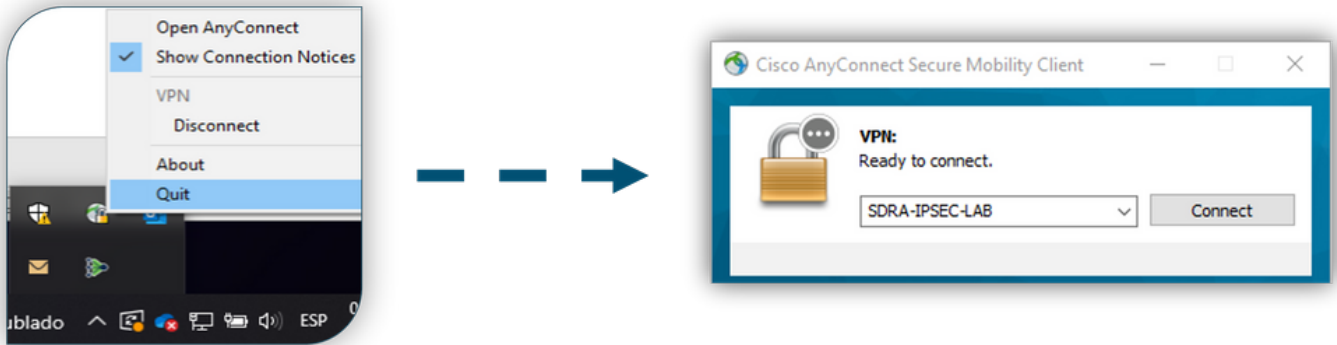
For Windows:

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
```

For MAC OS:

```
/opt/cisco/anyconnect/profile
```

De AnyConnect-client moet opnieuw worden gestart zodat het profiel in de GUI zichtbaar wordt. Het proces kan opnieuw worden opgestart door met de rechtermuisknop op het AnyConnect-pictogram in het Windows-vak te klikken en de optie **Quit** te selecteren:



De AnyConnect-downloader uitschakelen

De AnyConnect-client probeert de download van het XML-profiel uit te voeren na een succesvol inloggen standaard.

Als het profiel niet beschikbaar is, wordt de verbinding verbroken. Als tijdelijke oplossing is het mogelijk de AnyConnect-downloadmogelijkheid voor het profiel op de client zelf uit te schakelen.

Voor Windows:

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml
```

Voor MAC OS:

```
/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml
```

De optie "BypassDownloader" is ingesteld op "True":

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="4.9.04043">
<BypassDownloader>true</BypassDownloader>
<EnableCRLCheck>>false</EnableCRLCheck>
<ExcludeFirefoxNSSCertStore>>false</ExcludeFirefoxNSSCertStore>
<ExcludeMacNativeCertStore>>false</ExcludeMacNativeCertStore>
<ExcludePemFileCertStore>>false</ExcludePemFileCertStore>
<ExcludeWinNativeCertStore>>false</ExcludeWinNativeCertStore>
<FipsMode>>false</FipsMode>
<RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
<RestrictServerCertStore>>false</RestrictServerCertStore>
```

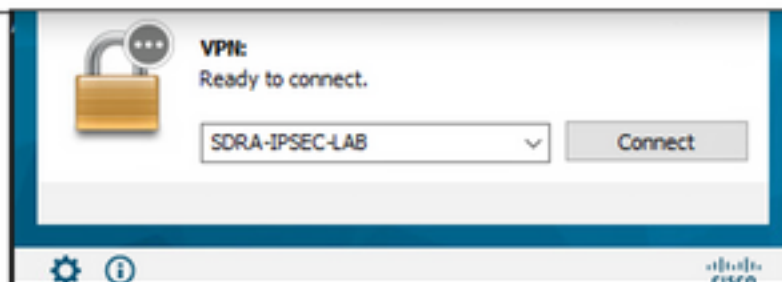
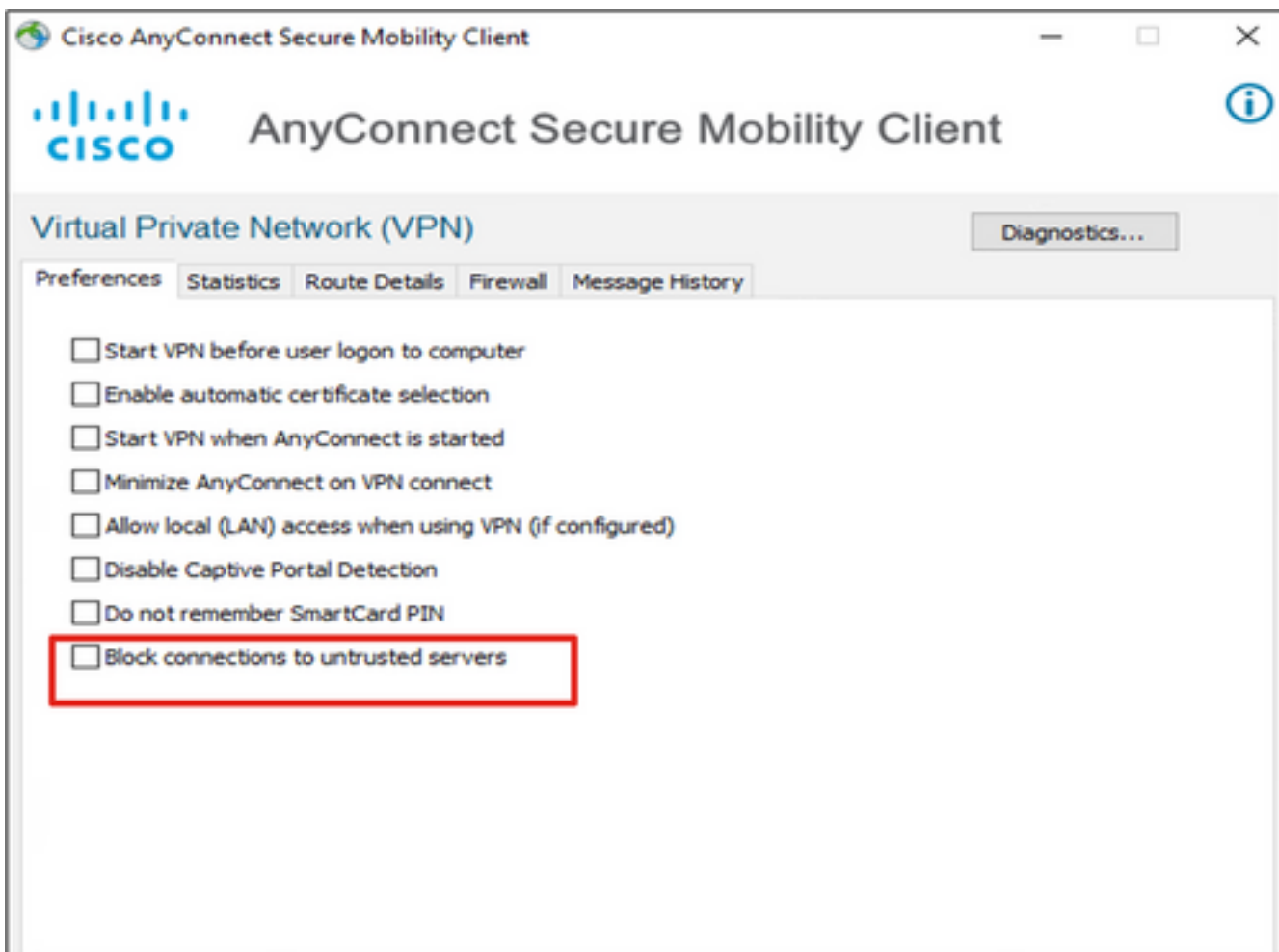
```
<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>  
<RestrictWebLaunch>>false</RestrictWebLaunch>  
<StrictCertificateTrust>>false</StrictCertificateTrust>  
<UpdatePolicy>  
<AllowComplianceModuleUpdatesFromAnyServer>>true</AllowComplianceModuleUpdatesFromAnyServer>  
<AllowISEProfileUpdatesFromAnyServer>>true</AllowISEProfileUpdatesFromAnyServer>  
<AllowManagementVPNProfileUpdatesFromAnyServer>>true</AllowManagementVPNProfileUpdatesFromAnyServer>  
<AllowServiceProfileUpdatesFromAnyServer>>true</AllowServiceProfileUpdatesFromAnyServer>  
<AllowSoftwareUpdatesFromAnyServer>>true</AllowSoftwareUpdatesFromAnyServer>  
<AllowVPNProfileUpdatesFromAnyServer>>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>  
</AnyConnectLocalPolicy>
```

Onvertrouwde servers verwijderen op AnyConnect-client

Navigeer naar **Instellingen > Voorkeuren** en controleer alle opties van het vakje los.

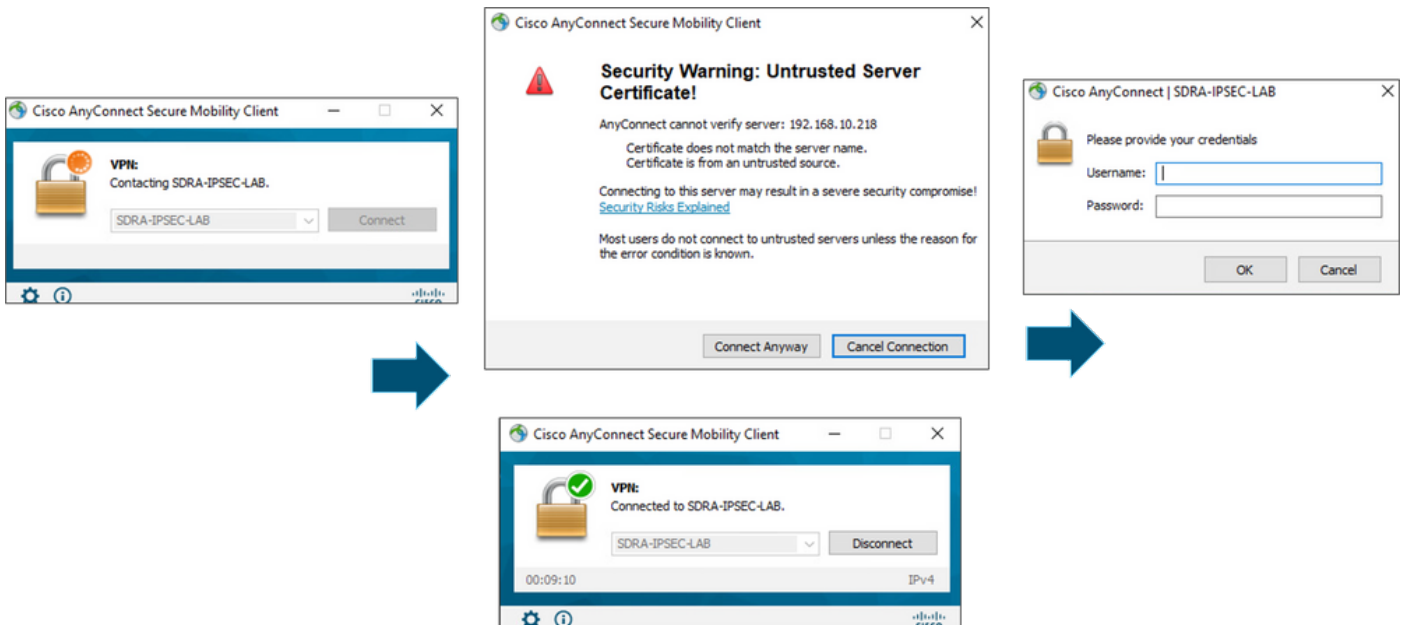
Het belangrijkste is de "**Block Connections to onvertrouwde servers**" voor dit scenario.

Opmerking: Het certificaat dat wordt gebruikt voor RA head-end/cEdge-verificatie is het certificaat dat eerder is gemaakt en ondertekend door de CA-server in Cisco IOS® XE. Aangezien deze CA server geen openbare entiteit is zoals GoDaddy, Symantec, Cisco etc. De PC Client interpreteert het certificaat als een onvertrouwde server. Dit is gemaakt met behulp van een openbare certificering of een CA-server waarop uw bedrijf vertrouwen heeft.



AnyConnect-client gebruiken

Zodra alle SDRA-configuratie is geplaatst, wordt de stroom voor een succesvolle verbinding als afbeelding weergegeven.



Verifiëren

De virtuele sjabloon-interface wordt gebruikt om de virtuele toegangsinterface te maken om een cryptokanaal te starten en om IKEv2- en IPsec-beveiligingsassociaties (SAs) tussen de server (cEdge) en de client (AnyConnect-gebruiker) op te zetten.

Opmerking: De virtuele-sjabloon-interface is altijd omhoog/omlaag. De status is omhoog en het protocol is omlaag.

```
cEdge-207#show ip int brief
Interface                IP-Address      OK? Method Status Protocol
GigabitEthernet1        unassigned      YES unset  up      up
GigabitEthernet2        192.168.10.218 YES other   up      up
GigabitEthernet3        10.11.14.227   YES other   up      up
Sdwan-system-intf       10.1.1.18      YES unset   up      up
Loopback1                192.168.50.1   YES other   up      up
Loopback65528           192.168.1.1    YES other   up      up
NVI0                    unassigned      YES unset   up      up
Tunnel2                 192.168.10.218 YES TFTP    up      up
Virtual-Access1        192.168.50.1   YES unset   up      up
Virtual-Template101    unassigned     YES unset   up      down
```

Controleer de eigenlijke configuratie die is toegepast voor de interface Virtual-Access die aan de client is gekoppeld met **toonaangevend virtueel-configuratie interface <number>**.

```
cEdge-207#show derived-config interface virtual-access 1
Building configuration...
Derived configuration : 252 bytes
!
interface Virtual-Access1
 vrf forwarding 1
 ip unnumbered Loopback1
 tunnel source 192.168.10.218
 tunnel mode ipsec ipv4
```

```
tunnel destination 192.168.10.219
tunnel protection ipsec profile IKEV2-RA-PROFILE
no tunnel protection ipsec initiate
end
```

Controleer de IPsec security associaties (SAs) voor AnyConnect client met de **show crypto ipsec als peer <AnyConnect Public IP >**.

```
cEdge-207#show crypto ipsec sa peer 192.168.10.219
interface: Virtual-Access2
  Crypto map tag: Virtual-Access2-head-0, local addr 192.168.10.218
  protected vrf: 1
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.20.14.13/255.255.255.255/0/0)
  current_peer 192.168.10.219 port 50787
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
      outbound pcp sas:
... Output Omitted...
```

Controleer IKEv2 SA parameters voor de sessie, de gebruikersnaam en de toegewezen IP.

Opmerking: Het toegewezen IP-adres moet overeenkomen met het IP-adres aan de zijde AnyConnect Client.

```
cEdge-207#sh crypto ikev2 session detail
IPv4 Crypto IKEv2 Session
Session-id:21, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status
1 192.168.10.218/4500 192.168.10.219/62654 none/1 READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth
verify: AnyConnect-EAP
Life/Active Time: 86400/532 sec
CE id: 1090, Session-id: 21
Local spi: DDB03CE8B791DCF7 Remote spi: 60052513A60C622B
Status Description: Negotiation done
Local id: 192.168.10.218
Remote id: *$AnyConnectClient$*
Remote EAP id: anavazar@cisco.com
Local req msg id: 0 Remote req msg id: 23
Local next msg id: 0 Remote next msg id: 23
Local req queued: 0 Remote req queued: 23
Local window: 5 Remote window: 1
DPD configured for 45 seconds, retry 2
Fragmentation not configured.
Dynamic Route Update: disabled
Extended Authentication not configured.
NAT-T is detected outside
Cisco Trust Security SGT is disabl
Assigned host addr: 10.20.14.19
Initiator of SA : No
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.20.14.19/0 - 10.20.14.19/65535
ESP spi in/out: 0x43FD5AD3/0xC8349D4F
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
```

```
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
IPv6 Crypto IKEv2 Session
```

```
cEdge-207#show crypto session detail
```

```
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN
```

Interface: Virtual-Access1

```
Profile: RA-SDWAN-IKEV2-PROFILE
```

```
Uptime: 00:17:07
```

```
Session status: UP-ACTIVE
```

```
Peer: 192.168.10.219 port 62654 fvrf: (none) ivrf: 1
```

```
Phase1_id: *$AnyConnectClient$*
```

```
Desc: (none)
```

```
Session ID: 94
```

```
IKEv2 SA: local 192.168.10.218/4500 remote 192.168.10.219/62654 Active
```

```
Capabilities:DN connid:1 lifetime:23:42:53
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.14.19
```

```
Active SAs: 2, origin: crypto map
```

```
Inbound: #pkts dec'ed 89 drop 0 life (KB/Sec) 4607976/2573
```

```
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/2573
```

Gerelateerde informatie

- [Cisco SD-WAN externe toegang](#)
- [De FlexVPN-server configureren](#)
- [Download AnyConnect](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)