Konfigurieren von SD-WAN Remote Access (SDRA) mit AnyConnect und ISE-Server

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der SD-WAN Remote Access (SDRA) mit dem AnyConnect Client mithilfe eines unabhängigen Cisco IOS® XE-Modus als CA-Server und eines Cisco Identity Services Engine (ISE)-Servers für Authentifizierung, Autorisierung und Abrechnung konfiguriert wird.

Voraussetzungen

Anforderungen

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

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Public Key Infrastructure (PKI)
- FlexVPN
- RADIUS-Server

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V, Version 17.07.01a
- vManage Version 20.7.1
- CSR1000V, Version 17.03.04.a
- ISE Version 2.7.0.256
- AnyConnect Secure Mobility Client Version 4.10.04071

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

Hintergrundinformationen

Was ist ein Remote Access VPN?

Mit dem Remote Access VPN kann der Remote-Benutzer eine sichere Verbindung zu den Unternehmensnetzwerken herstellen, Anwendungen und Daten verwenden, auf die nur über die im Büro angeschlossenen Geräte zugegriffen werden kann.

Ein Remote-Access-VPN wird über einen virtuellen Tunnel zwischen dem Gerät eines Mitarbeiters und dem Netzwerk des Unternehmens erstellt.

Dieser Tunnel durchläuft das öffentliche Internet, aber die Daten, die durch das Internet gesendet werden, werden durch Verschlüsselungs- und Sicherheitsprotokolle geschützt, um ihn privat und sicher zu halten.

Die beiden Hauptkomponenten dieses VPN-Typs sind ein Netzwerkzugriffsserver/RA-Headend und eine VPN-Clientsoftware.

Was ist SD-WAN Remote Access VPN?

Der Remote-Zugriff wurde in die SD-WAN-Lösung integriert, sodass keine separate Cisco SD-WAN- und RA-Infrastruktur erforderlich ist. Durch den Einsatz von Cisco AnyConnect als RA-Software-Client können RA-Services schnell skalierbar werden.

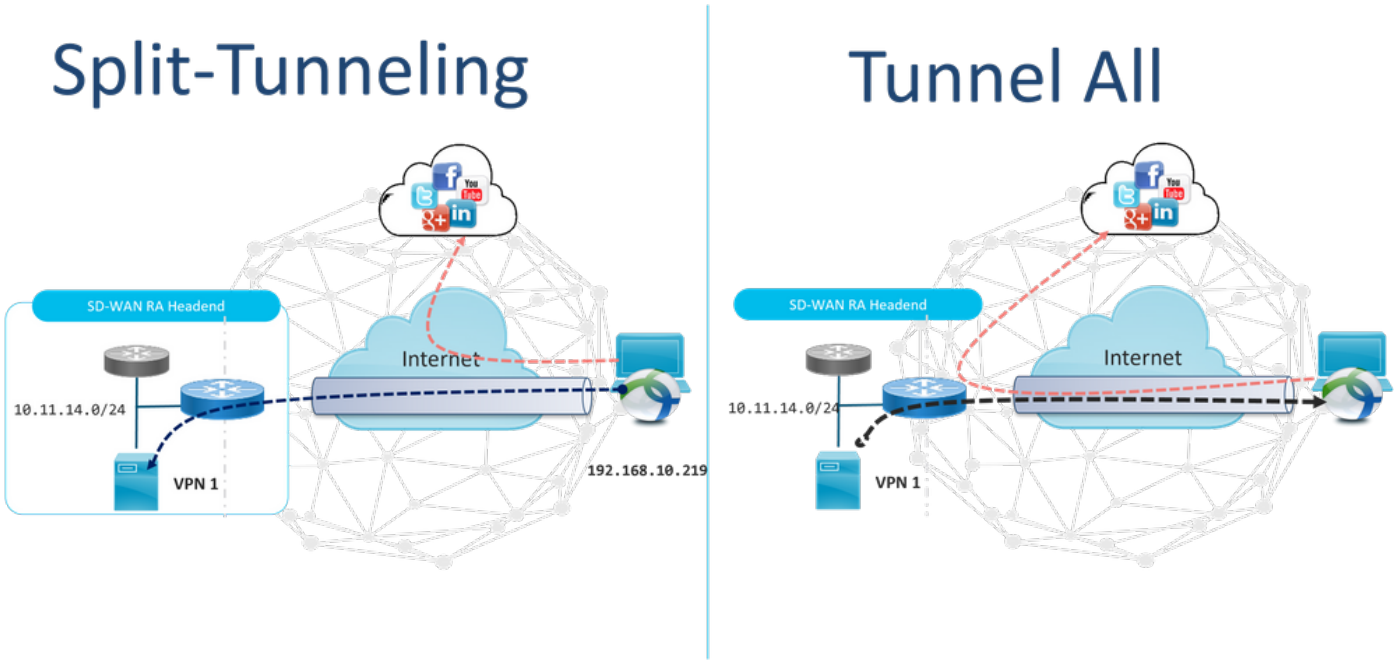
Remote-Zugriff ermöglicht Remote-Benutzern den Zugriff auf das Netzwerk des Unternehmens. Dies ermöglicht die Arbeit von zu Hause aus.

Die Vorteile

- RA ermöglicht den Zugriff auf das Netzwerk eines Unternehmens von Geräten/Benutzern an Remote-Standorten aus. (HO)
- Erweitert die Cisco SD-WAN-Lösung auf Benutzer mit Remote-Zugriff, ohne dass jedes Gerät eines RA-Benutzers Teil der Cisco SD-WAN-Fabric sein muss.
- Datensicherheit
- Split-Tunneling oder Tunnel All
- Skalierbarkeit
- Möglichkeit zur Verteilung der RA-Last auf zahlreiche Cisco IOS® XE SD-WAN-Geräte in der Cisco SD-WAN-Fabric

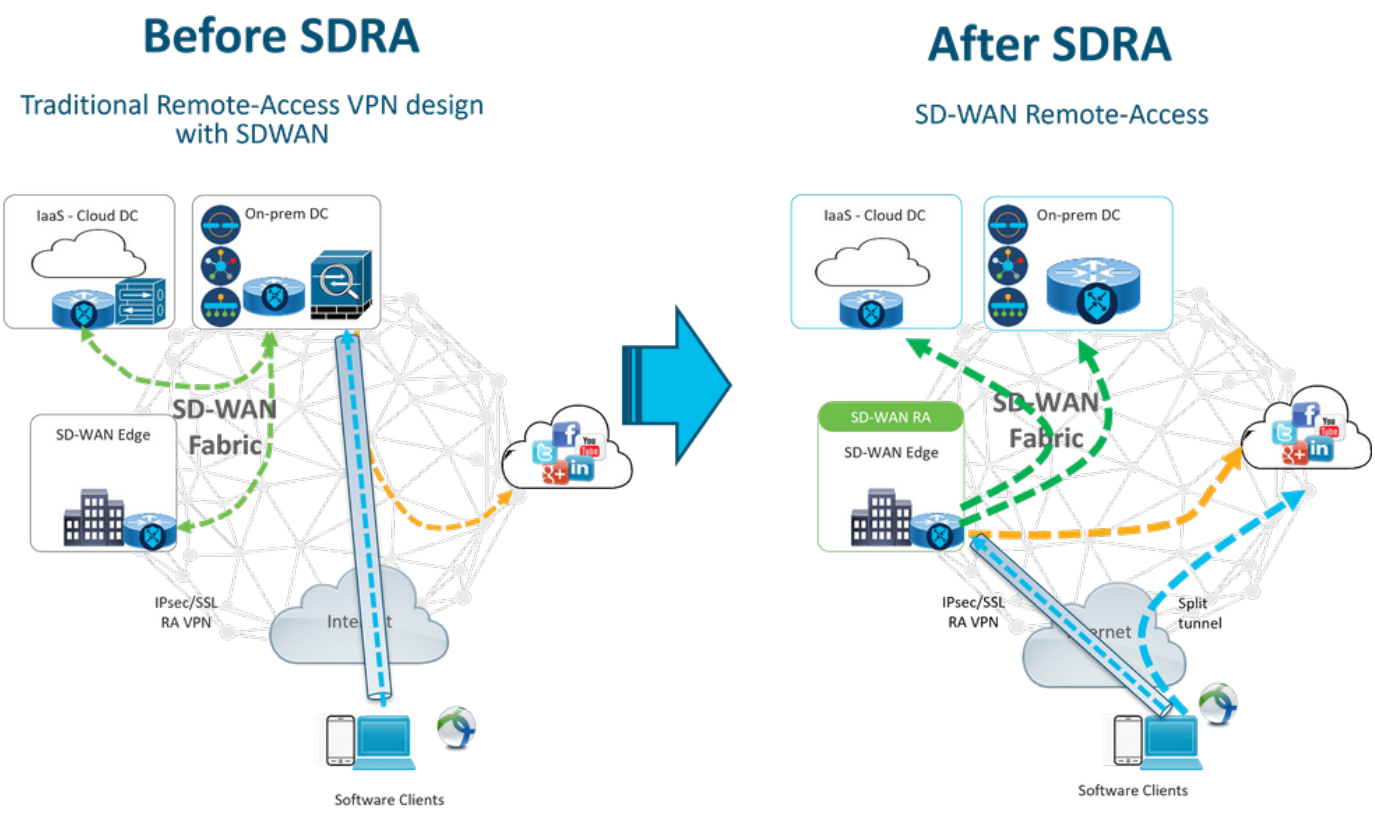
Split Tunneling und Tunnel All

Split-Tunneling wird in Szenarien verwendet, in denen nur bestimmter Datenverkehr getunnelt werden muss (z. B. SD-WAN-Subnetze), wie im Bild gezeigt.



Vor SDRA und nach SDRA

Das herkömmliche VPN-Design für Remote-Zugriff erfordert eine separate RA-Infrastruktur außerhalb der Cisco SD-WAN-Fabric, um Remote-Benutzerzugriff auf das Netzwerk wie Nicht-SD-WAN-Appliances wie ASA, Cisco IOS® XE oder Drittanbietergeräte zu ermöglichen. Der RA-Datenverkehr wird, wie im Bild gezeigt, an die SD-WAN-Appliance weitergeleitet.



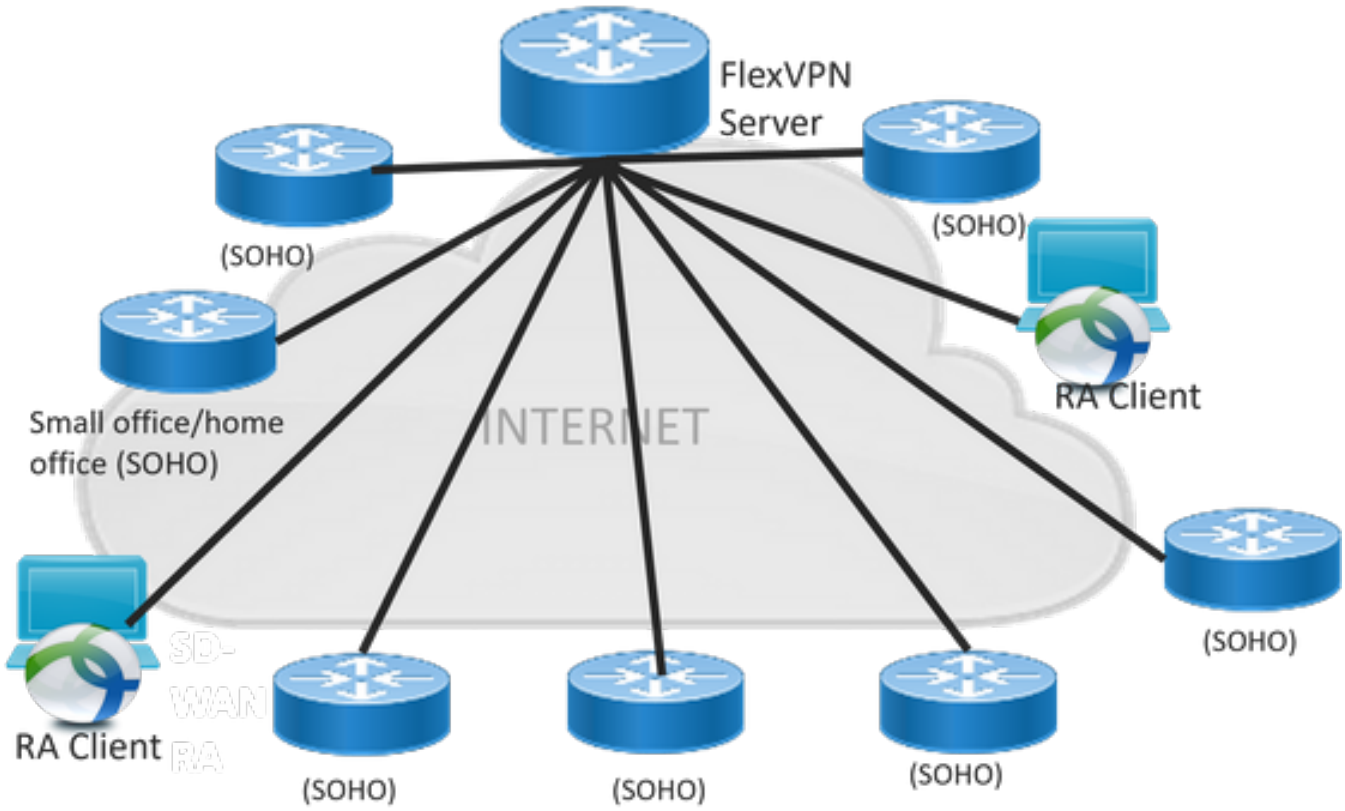
Der SD-WAN-Remote-Zugriff ändert die Art und Weise, wie Remote-Benutzer eine Verbindung zum Netzwerk herstellen. Sie sind direkt mit dem cEdge verbunden, der als RA-Headend verwendet wird. Erweitert die Cisco SD-WAN-Funktionen und Vorteile auf Benutzer mit RA-Zertifizierung. RA-Benutzer werden zu LAN-Benutzern in Zweigstellen.

Für jeden RA-Client weist das SD-WAN RA-Headend einem RA-Client eine IP-Adresse zu und fügt der zugewiesenen IP-Adresse in der Service-VRF-Instanz, in der der RA-Benutzer untergebracht ist, eine statische Host-Route hinzu.

Die statische Route gibt den VPN-Tunnel der RA-Client-Verbindung an. Das SD-WAN-RA-Headend kündigt allen Edge-Geräten im Service-VPN die statische IP innerhalb der Service-VRF-Instanz des RA-Clients mithilfe von OMP an.

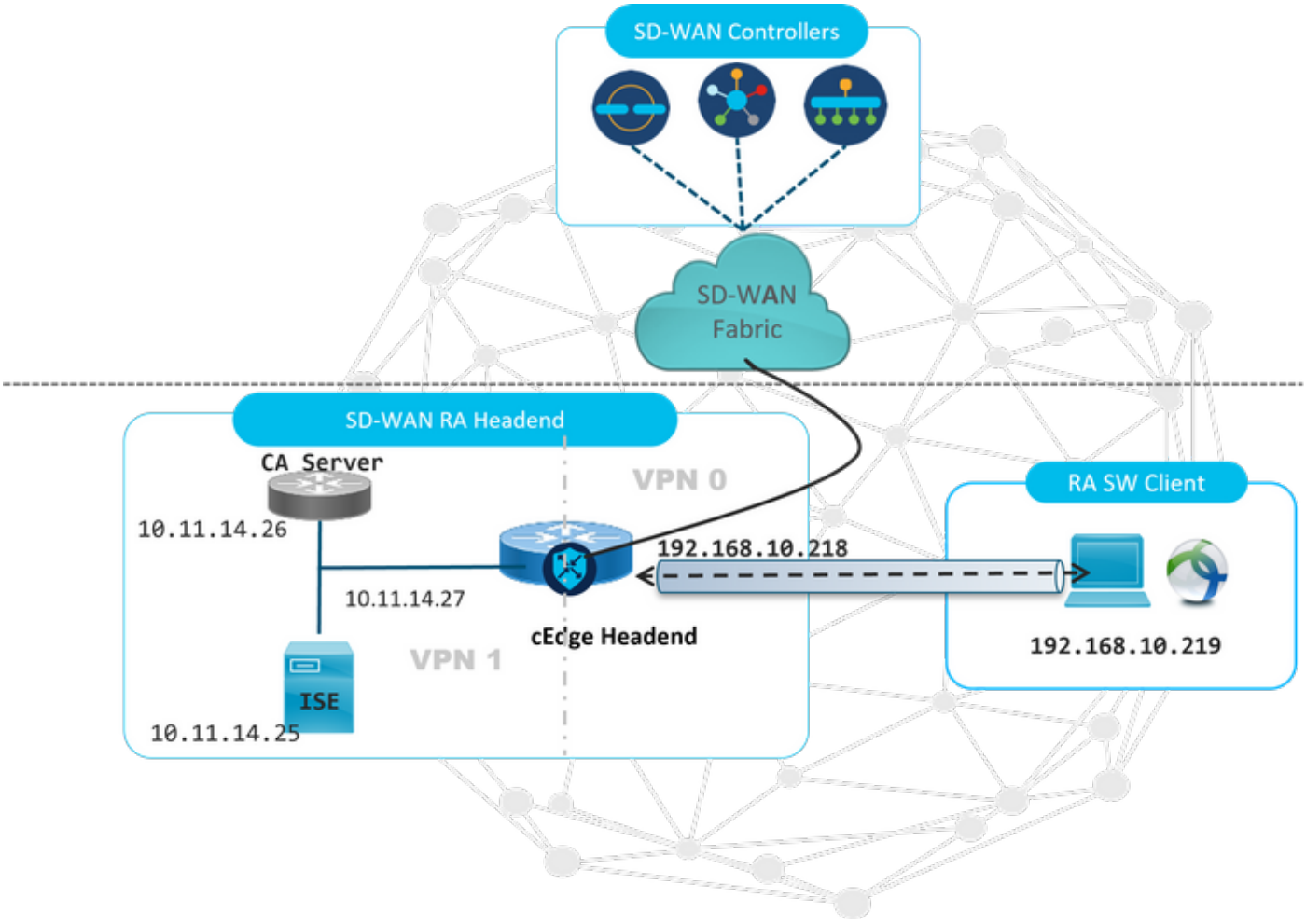
Was ist FlexVPN?

SD-WAN RA nutzt die Cisco FlexVPN RA-Lösung. FlexVPN ist die Implementierung der IKEv2-Standardfunktion durch Cisco, einem einheitlichen Paradigma und einer einheitlichen CLI, die Standort-zu-Standort-, **Remote-Zugriff**-, Hub-and-Spoke-Topologien und partielle Mesh-Verbindungen (Spoke to Spoke direkt) vereint. FlexVPN bietet ein einfaches, aber modulares Framework, das das Tunnelschnittstellen-Paradigma umfassend nutzt, während es mit älteren VPN-Implementierungen kompatibel bleibt.



Erforderliche Konfiguration

In diesem Beispiel wurde ein SD-WAN RA Lab-Setup erstellt, wie im Bild gezeigt.



Für dieses SD-WAN-RA-Lab-Szenario wurden weitere Komponenten konfiguriert:

- Ein reguläres Cisco IOS® XE im Autonomous-Modus als CA-Server.
- Ein ISE/Radius-Server für Authentifizierung, Autorisierung und Abrechnung.
- Ein Windows-PC, der über die WAN-Schnittstelle für den cEdge erreichbar ist.
- AnyConnect Client ist bereits installiert.

Anmerkung: Die CA- und RADIUS-Server wurden in Service-VRF 1 platziert. Beide Server müssen über das Service-VRF für alle SD-WAN RA-Headends erreichbar sein.

Anmerkung: Der Cisco SD-WAN Remote Access wird von der Version 17.7.1a und bestimmten Geräten für SDRA unterstützt. Navigieren Sie für unterstützte Geräte zu: Unterstützte Plattformen für das SD-WAN RA-Headend

ISE-Konfiguration

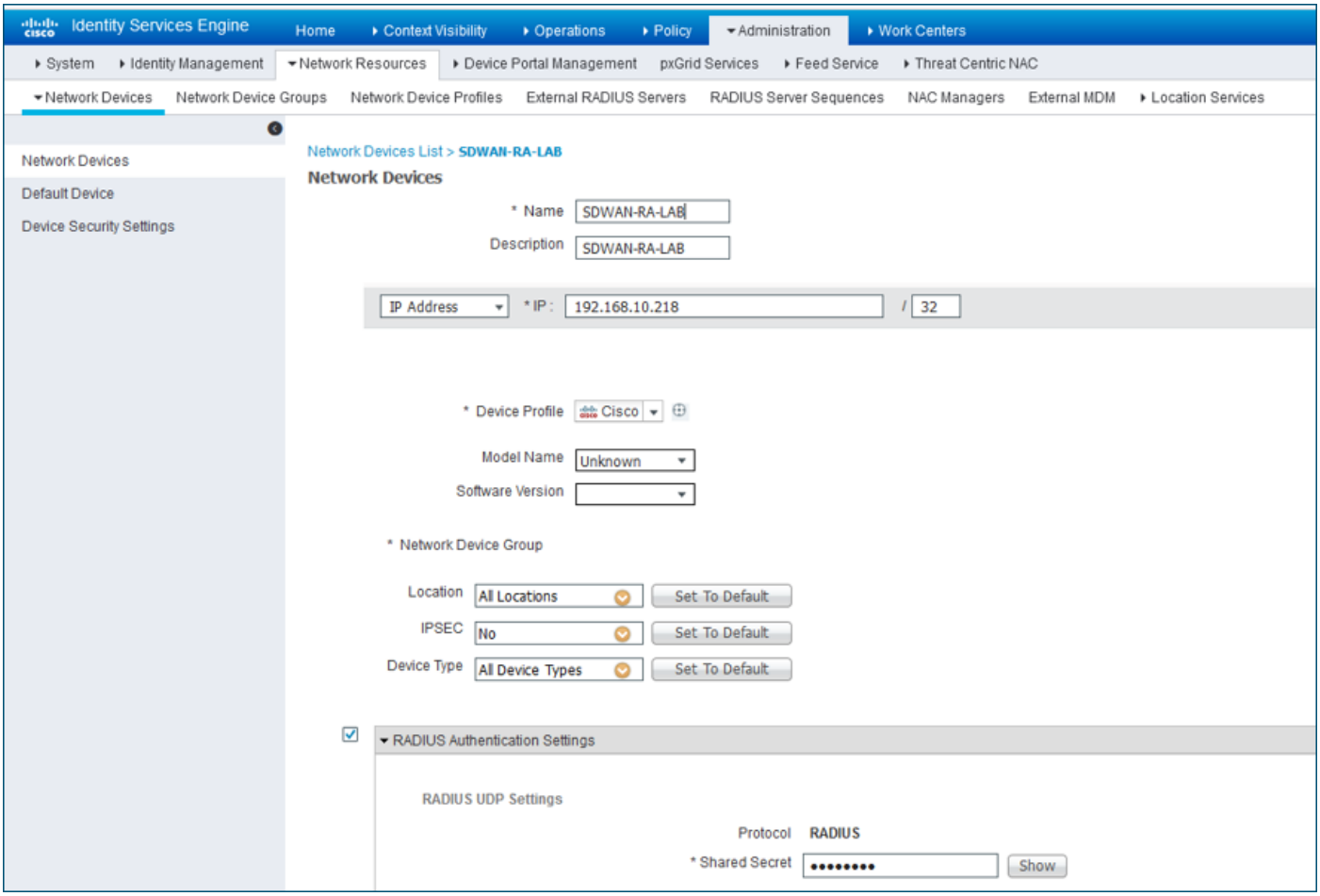
Um das SD-WAN RA-Headend zu unterstützen, stellen Sie sicher, dass die Parameter auf dem RADIUS-Server konfiguriert sind. Diese Parameter sind für RA-Verbindungen erforderlich:

- Anmeldeinformationen für die Benutzerauthentifizierung Benutzername und Kennwort für AnyConnect-EAP-Verbindungen
- Richtlinienparameter (Attribute), die für einen Benutzer oder eine Benutzergruppe gelten **VRF**: Service-VPN, dem der RA-Benutzer zugewiesen ist**Name des IP-Pools**: Name des auf dem

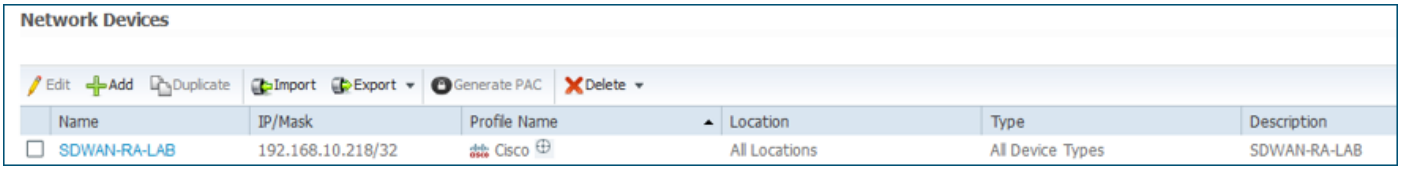
RA-Headend definierten IP-Pools**Server-Subnetze**: Subnetzzugriff für RA-Benutzer

Der erste Schritt, der in der ISE konfiguriert werden muss, ist das RA-Headend oder die cEdge-IP-Adresse als Netzwerkgerät, das Radius-Anfragen an die ISE senden kann.

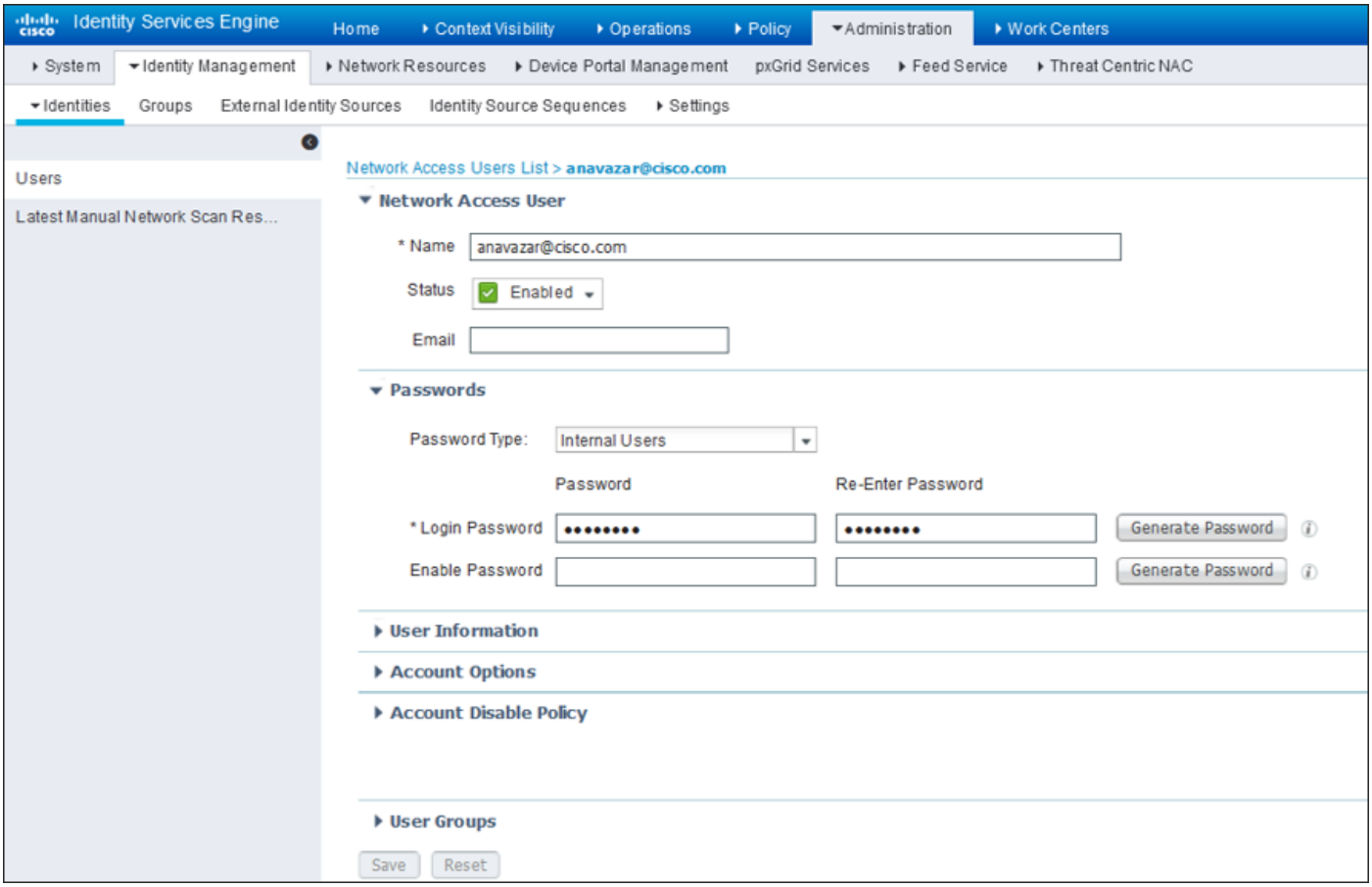
Navigieren Sie **zu Administration > Network Devices (Netzwerkgeräte),** und fügen Sie die IP-Adresse und das Kennwort für den RA Headed (cEdge) hinzu, wie im Bild gezeigt.



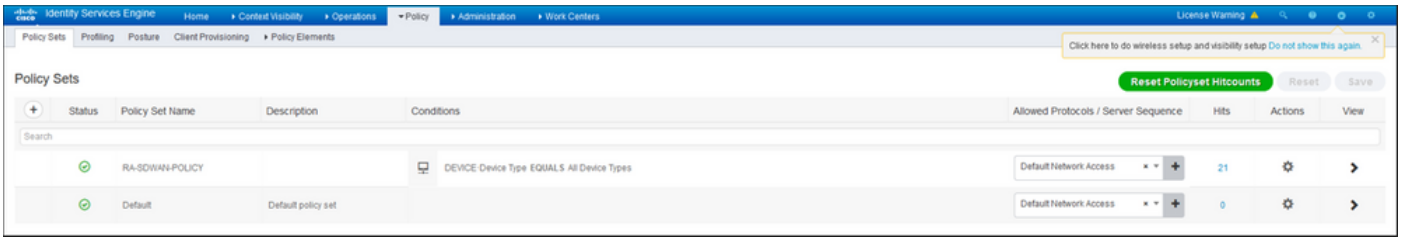
Netzwerkgerät hinzugefügt, wie im Bild gezeigt.



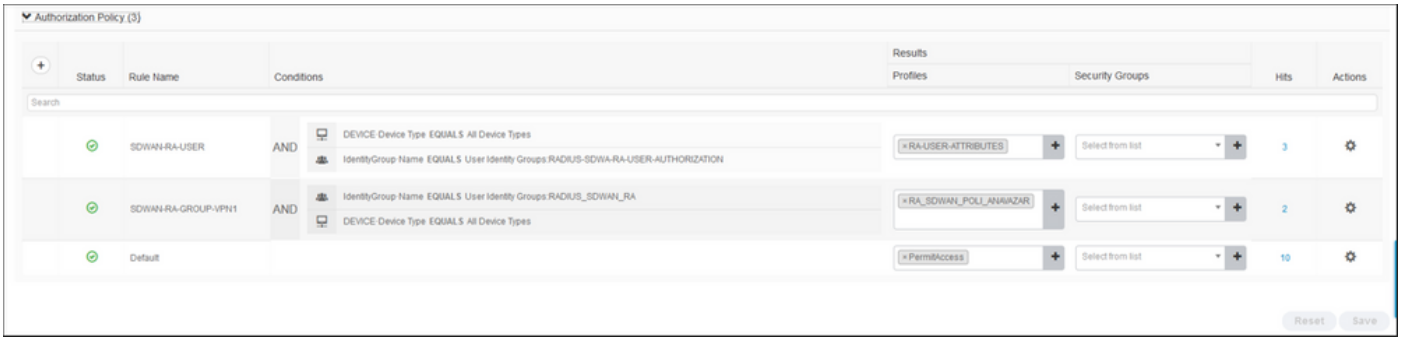
Im RADIUS-Server müssen die Benutzernamen und das Kennwort für die AnyConnect-Authentifizierung wie im Bild gezeigt konfiguriert werden. Navigieren Sie zu **Administration > Identities**.



Es muss ein Richtliniensatz mit der Übereinstimmungsbedingung erstellt werden, um wie im Bild gezeigt zu drücken. In diesem Fall wird die Bedingung **Alle Gerätetypen** verwendet, d. h. alle Benutzer treffen diese Richtlinie.



Anschließend wurde eine Autorisierungsrichtlinie pro Bedingung erstellt. Die Bedingung **Alle Gerätetypen** und die zuzuordnenden Identitätsgruppen.

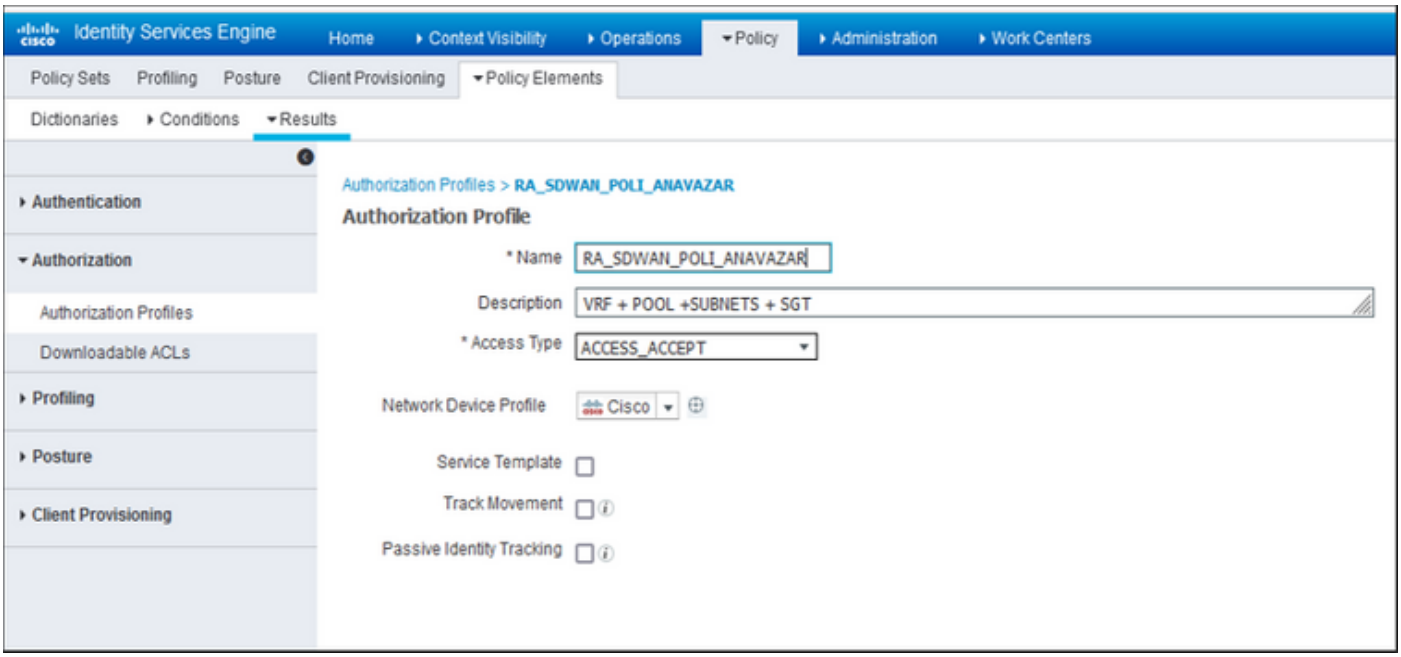


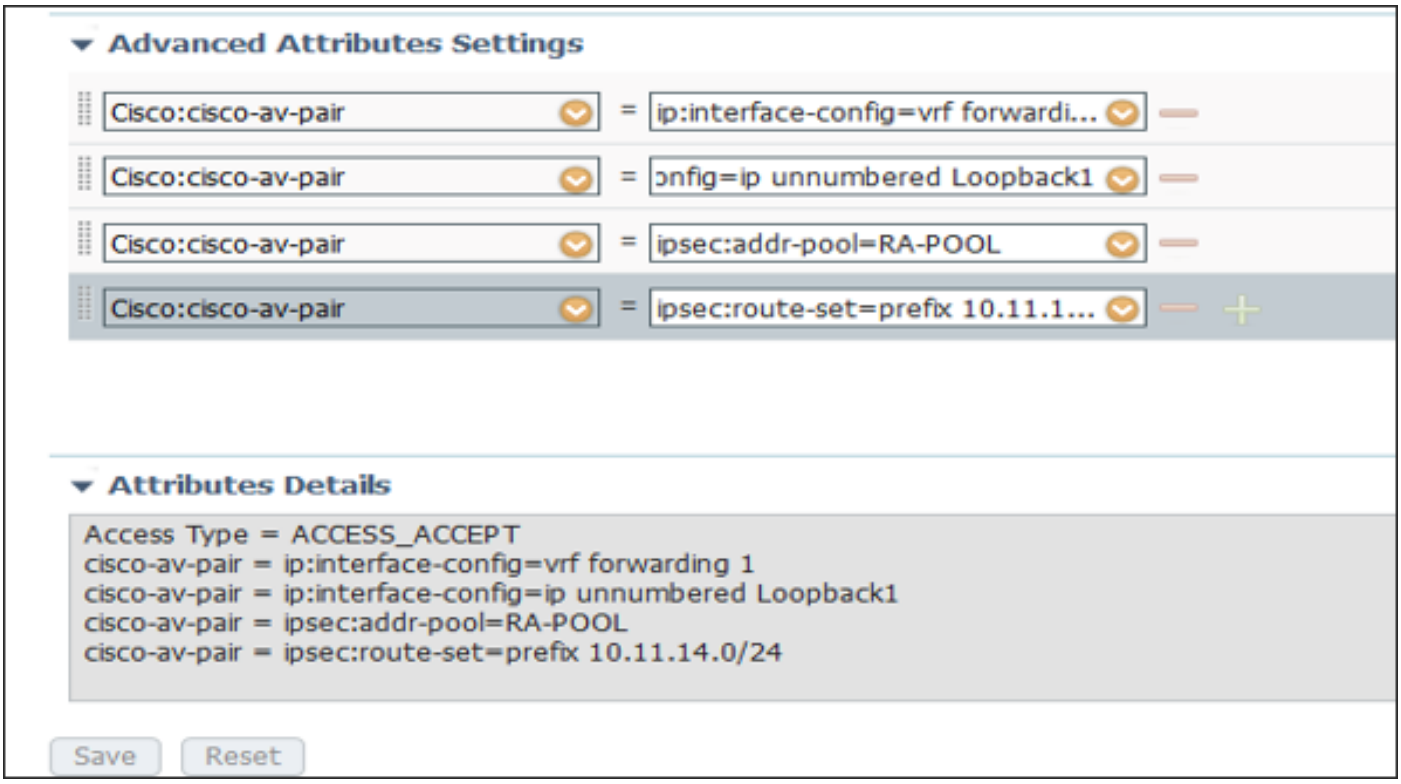
Im **Autorisierungsprofil** müssen wir den **Zugriffstyp** als **Access_ACCEPT** unter **Erweiterte Attributeinstellungen** konfigurieren, indem wir das Attribut "Cisco Vendor" und **Cisco-AV-pair** auswählen.

Es müssen einige Richtlinienparameter für die Benutzer konfiguriert werden:

- VRF, das Service-VRF, zu dem der Benutzer gehört.
- Der Name des IP-Pools, jeder Benutzerverbindung wird eine IP-Adresse zugewiesen, die zum in den Edges konfigurierten IP-Pool gehört.
- die Subnetze, auf die der Benutzer zugreifen kann

Vorsicht: Der Befehl **IP-VRF-Weiterleitung** muss vor dem Befehl **IP unnumbered (nicht nummerierte IP-Adressen)** stehen. Wenn die virtuelle Zugriffsschnittstelle aus der virtuellen Vorlage geklont und der Befehl **IP VRF-Forwarding** angewendet wird, wird jede IP-Konfiguration aus der virtuellen Zugriffsschnittstelle entfernt.





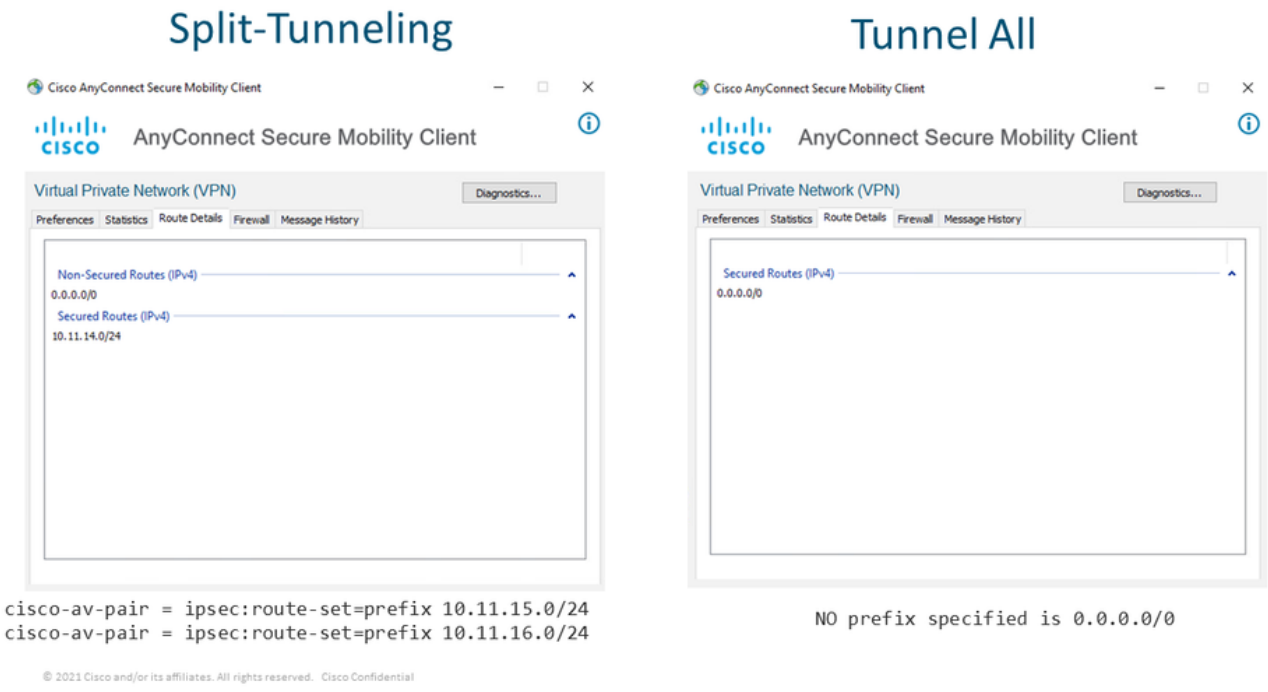
Benutzerattribute:

```
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 und Tunnel im AnyConnect-Client

ipsec:route-set=prefix-Attribut, das im AnyConnect-Client empfangen wird, wird wie im Bild gezeigt installiert.



CA-Serverkonfiguration in Cisco IOS® XE

Der CA-Server stellt Zertifikate für die Cisco IOS® XE SD-WAN-Geräte bereit und ermöglicht dem RA-Headend die Authentifizierung gegenüber RA-Clients.

Der CEDGE kann kein CA-Server sein, da diese Crypto PKI-Serverbefehle im Cisco IOS® XE SD-WAN nicht unterstützt werden.

- Generieren eines RSA-Keypair
- Erstellen Sie den PKI-Trustpoint für den CA-Server. Konfigurieren Sie die rsakeypair mit der zuvor generierten KEY-CA.

  Anmerkung: Der PKI-Server und der PKI-Trustpoint müssen denselben Namen verwenden.

- Erstellen des CA-Servers Konfigurieren Sie den Namen des Ausstellers für Ihren CA-Server.Aktivieren Sie den CA-Server mithilfe von "No Shutdown" (Kein Herunterfahren).

```
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
!
```

Überprüfen Sie, ob der CA-Server aktiviert ist.

```
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
```

Überprüfen Sie, ob das Zertifikat des CA-Servers installiert ist.

```
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-truspoint CA
Storage: nvram:CSR1Kv_SDWAN#1CA.cer
```

Der **Fingerabdruck SHA 1** aus dem CA-Zertifikat wird auf dem **crypto pki trustpoint** im cEdge-Router (RA-Headend) mit der Remote-Zugriffskonfiguration verwendet.

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

SD-WAN-RA-Konfiguration

> **Anmerkung:** Dieses Dokument behandelt nicht den SD-WAN-Integrationsprozess für Controller und cEdge. Es wird davon ausgegangen, dass die SD-WAN-Fabric betriebsbereit und voll funktionsfähig ist.

Crypto PKI-Konfiguration

- Erstellen Sie einen PKI-Trustpoint.
- Konfigurieren Sie die URL für den CA-Server.
- Kopieren Sie den Fingerabdruck sha 1 aus dem Zertifikat des CA-Servers.
- Konfigurieren Sie den Betreffnamen und den Alt-Namen für das neue Identitätszertifikat.
- Konfigurieren Sie die rsakeypar mit der zuvor generierten KEY-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
 rsakeypair KEY-NEW
 revocation-check none
```

Bitten Sie um Authentifizierung des Zertifizierungsstellenzertifikats:

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

Generiert den CSR, sendet an den CA-Server und erhält das neue Identitätszertifikat:

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

Überprüfen Sie das Zertifizierungsstellenzertifikat und das cEdge-Zertifikat:

```
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-Konfiguration

```
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-Konfiguration

Konfigurieren des IP-Pools

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

Konfigurieren Sie IKEv2-Vorschläge (Chiffren und Parameter) und Richtlinien:

```
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
```

Konfigurieren eines IKEv2-Profilnamens-Managers:

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

> **Anmerkung:** Der **Name-Manager** leitet den Namen vom Präfix in der EAP-Identität (Benutzername) ab, die in der EAP-Identität getrennt ist, die das Präfix und das Suffix trennt.

Konfigurieren von IPsec-Chiffren:

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

Konfigurieren des Krypto-IKEv2-Profils:

```
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
```

Konfigurieren Sie das Crypto IPSEC-Profil:

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

Konfigurieren der Virtual Template-Schnittstelle:

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

Konfigurieren einer virtuellen Vorlage im Krypto-IKEv2-Profil:

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

Beispiel für eine SD-WAN-RA-Konfiguration

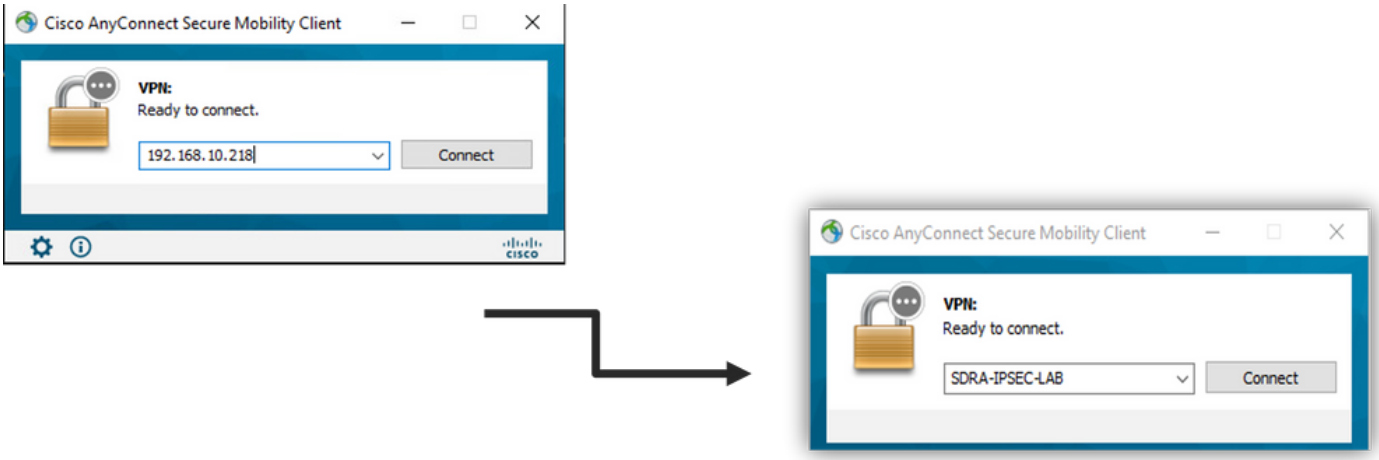
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
```

```
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 Client-Konfiguration

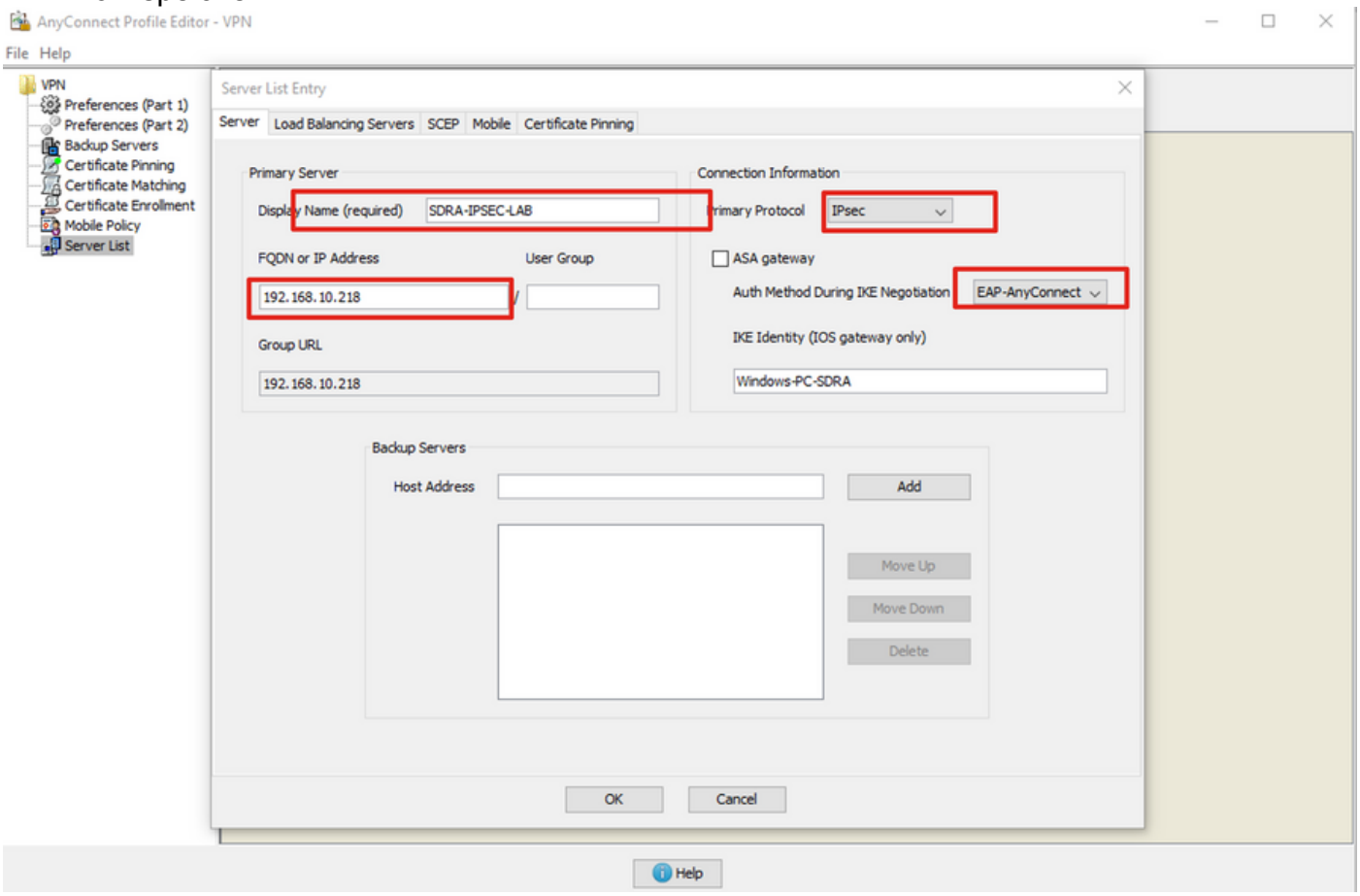
Der AnyConnect-Client verwendet SSL als Standardprotokoll für die Tunneleinrichtung. Dieses Protokoll wird für SD-WAN RA (Road Map) nicht unterstützt. RA verwendet FlexVPN. Daher ist IPSEC das verwendete Protokoll und es ist obligatorisch, es zu ändern. Dies erfolgt über das XML-Profil.

Der Benutzer kann den FQDN des VPN-Gateways manuell in die Adressleiste des AnyConnect-Clients eingeben. Dies führt zur SSL-Verbindung mit dem Gateway.



Konfigurieren des AnyConnect-Profil-Editors

- Navigieren Sie zur **Serverliste,** und klicken Sie auf **Hinzufügen**.
- Wählen Sie **IPsec** als "Primary Protocol" (Primärprotokoll) aus.
- Deaktivieren Sie die Option **ASA-Gateway**.
- Wählen Sie **EAP-AnyConnect** als "Authentifizierungsmethode während der IKE-Aushandlung" aus.
- **Anzeige/Name (erforderlich)** ist der Name, der zum Speichern dieser Verbindung unter dem AnyConnect-Client verwendet wird.
- **FQDN oder IP-Adresse** muss mit der cEdge (Public)-IP-Adresse eingereicht werden.
- Profil speichern



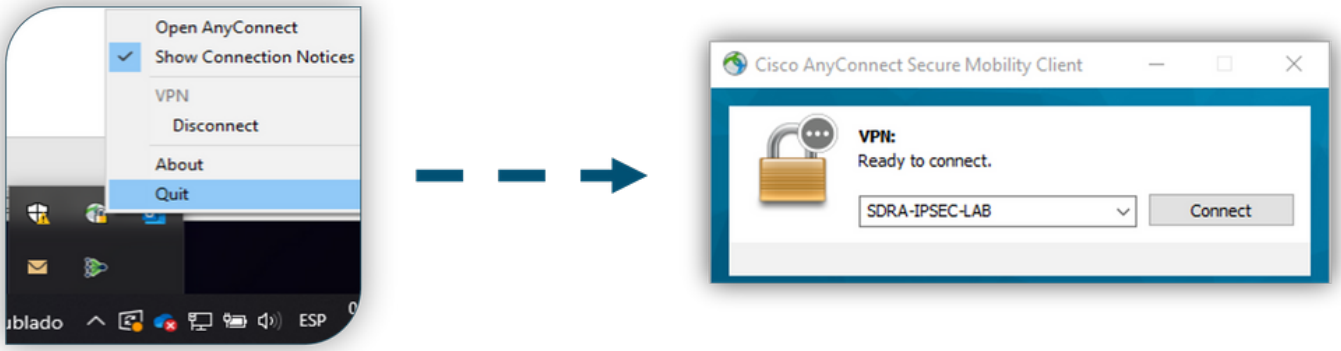
Installieren des AnyConnect-Profils (XML)

Das XML-Profil kann manuell in das Verzeichnis eingefügt werden:

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

For MAC OS:
/opt/cisco/anyconnect/profile
```

Der AnyConnect-Client muss neu gestartet werden, damit das Profil in der GUI angezeigt wird. Sie können den Vorgang neu starten, indem Sie mit der rechten Maustaste in der Windows-Taskleiste auf das AnyConnect-Symbol klicken und die **Quit-**Option auswählen:



Deaktivieren Sie den AnyConnect-Downloader.

Der AnyConnect-Client versucht, das XML-Profil nach erfolgreicher Anmeldung standardmäßig herunterzuladen.

Wenn das Profil nicht verfügbar ist, schlägt die Verbindung fehl. Als Problemumgehung ist es möglich, die Download-Funktion für das AnyConnect-Profil auf dem Client selbst zu deaktivieren.

Für Windows:

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

Für MAC OS:

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

Die Option "BypassDownloader" ist auf "true" eingestellt:

```
<?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</AllowManagementVPNProfileUpdatesFromAnyServ
er>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

Blockierung nicht vertrauenswürdiger Server auf dem AnyConnect-Client aufheben

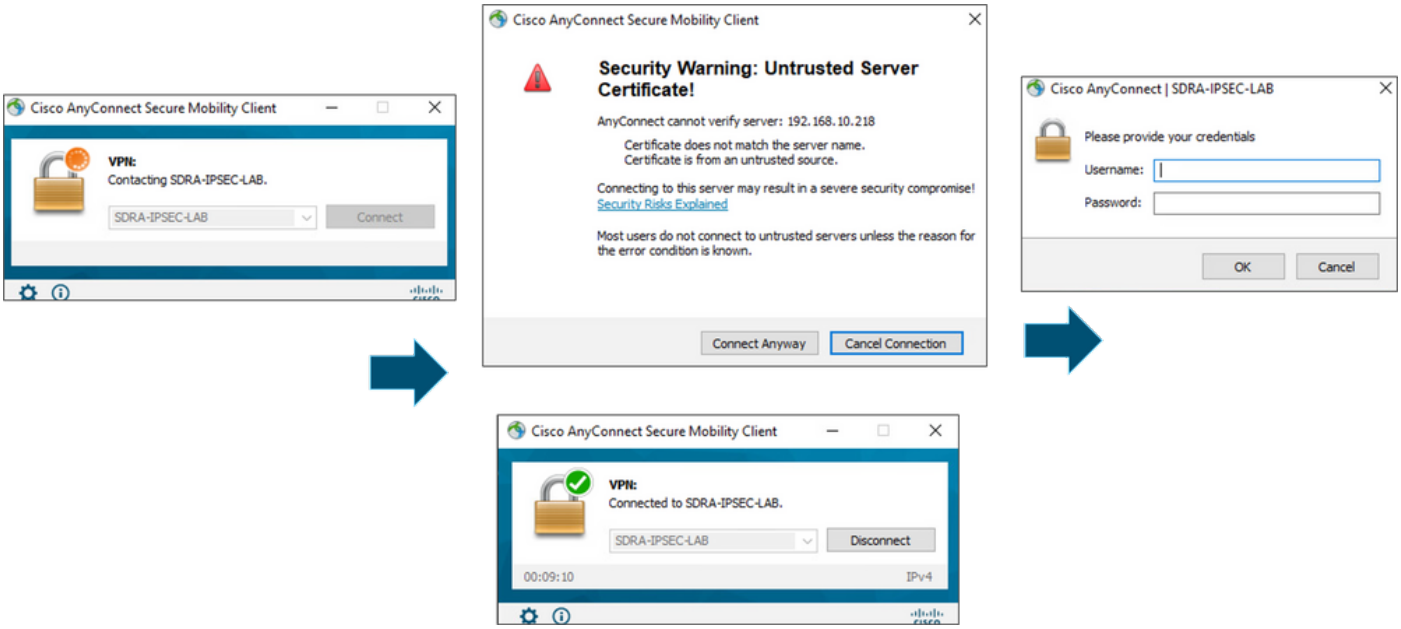
Navigieren Sie zu **Einstellungen > Voreinstellungen**, und deaktivieren Sie alle Kontrollkästchen.

Das wichtigste ist für dieses Szenario die **Blockierung von Verbindungen mit nicht vertrauenswürdigen Servern**.

> **Anmerkung:** Das für die RA-Headend-/cEdge-Authentifizierung verwendete Zertifikat ist das Zertifikat, das zuvor vom CA-Server in Cisco IOS® XE erstellt und signiert wurde. Da dieser CA-Server keine öffentliche Einrichtung ist, wie GoDaddy, Symantec, Cisco usw. Der PC-Client interpretiert das Zertifikat als nicht vertrauenswürdigen Server. Dies wird mithilfe eines öffentlichen Zertifikats oder eines CA-Servers behoben, dem Ihr Unternehmen vertraut.

AnyConnect-Client verwenden

Sobald alle SDRA-Konfigurationen vorgenommen wurden, wird der Fluss für eine erfolgreiche Verbindung als Bild angezeigt.



Überprüfung

Die virtuelle Vorlagenschnittstelle wird zum Erstellen der virtuellen Zugriffsschnittstelle verwendet, um einen Kryptokanal zu starten und IKEv2- und IPsec-Sicherheitszuordnungen (SAs) zwischen dem Server (cEdge) und dem Client (AnyConnect-Benutzer) einzurichten.

> **Anmerkung:** Die Virtual-Template-Schnittstelle ist immer **aktiv/inaktiv**. **Der Status** ist **aktiv** und das **Protokoll** ist **inaktiv**.

```
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
```

Überprüfen Sie die tatsächliche Konfiguration für die Virtual-Access-Schnittstelle, die dem Client mit **show derived-config interface virtual-access <number>** zugeordnet ist.

```
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
```

Prüfen Sie die IPsec-Sicherheitszuordnungen (SAs) für den AnyConnect-Client mit der **show crypto ipsec sa 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….
```

Überprüfen Sie die IKEv2 SA-Parameter für die Sitzung, den Benutzernamen und die zugewiesene IP.

> **Anmerkung:** Die zugewiesene IP-Adresse muss mit der IP-Adresse auf der Seite des AnyConnect-Clients übereinstimmen.

```
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
```

Zugehörige Informationen

- Cisco SD-WAN-Remote-Zugriff
- Konfigurieren des FlexVPN-Servers
- AnyConnect herunterladen
- Technischer Support und Dokumentation für Cisco Systeme