Configure SD-WAN Remote Access (SDRA) with AnyConnect and ISE Server

Contents

Introduction

This document describes how to configure SD-WAN Remote Access (SDRA) with AnyConnect Client using a Cisco IOS® XE Autonomous mode as a CA server, and a Cisco Identity Services Engine (ISE) server for the Authentication, Authorization, and Accounting.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- C8000V version17.07.01a
- 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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

What is a Remote Access VPN?

Remote Access VPN allows the remote user to securely connect to the company networks, use applications, and data that is only accessible through the devices plugged in at the office.

A remote-access VPN works by a virtual tunnel created between an employee’s device and the company’s network.

This tunnel goes through the public internet but the data sent back and forth through it is protected by encryption and security protocols to help keep it private and secure.

The two main components in this type of VPN are a network access server/RA headend and VPN client software.

What is SD-WAN Remote Access VPN?

The Remote Access has been integrated into the SD-WAN solution that eliminates the need for separate Cisco SD-WAN and RA infrastructure and enables rapid scalability of RA services with the use of the Cisco AnyConnect as an RA software Client.

Remote Access provides remote users access to the organization's network. This enables the work from Home.

The Advantages

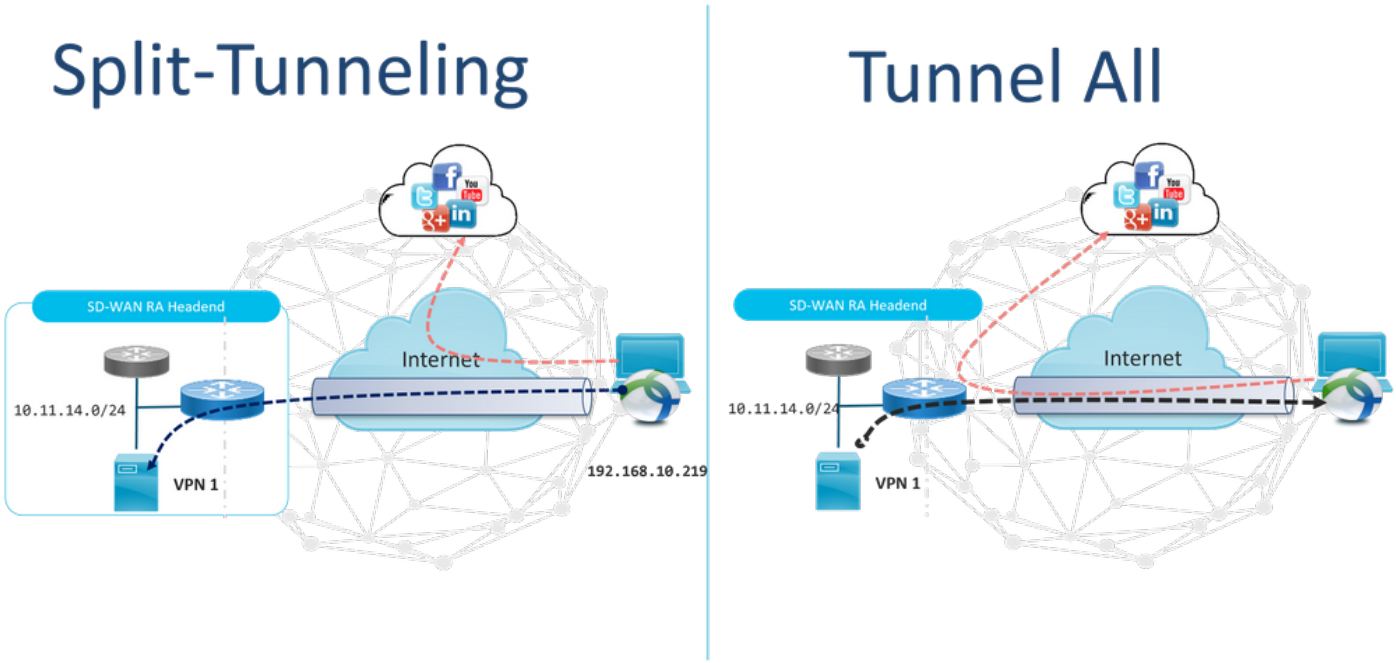
- RA provides access to an organization's network from devices/users at remote locations. (HO)
- Extends the Cisco SD-WAN solution to RA users without the requirement of each RA user's

device to be part of the Cisco SD-WAN fabric.

- Data Security
- Split-Tunneling or Tunnel All
- Scalability
- Ability to distribute the RA load across numerous Cisco IOS® XE SD-WAN devices in the Cisco SD-WAN fabric.

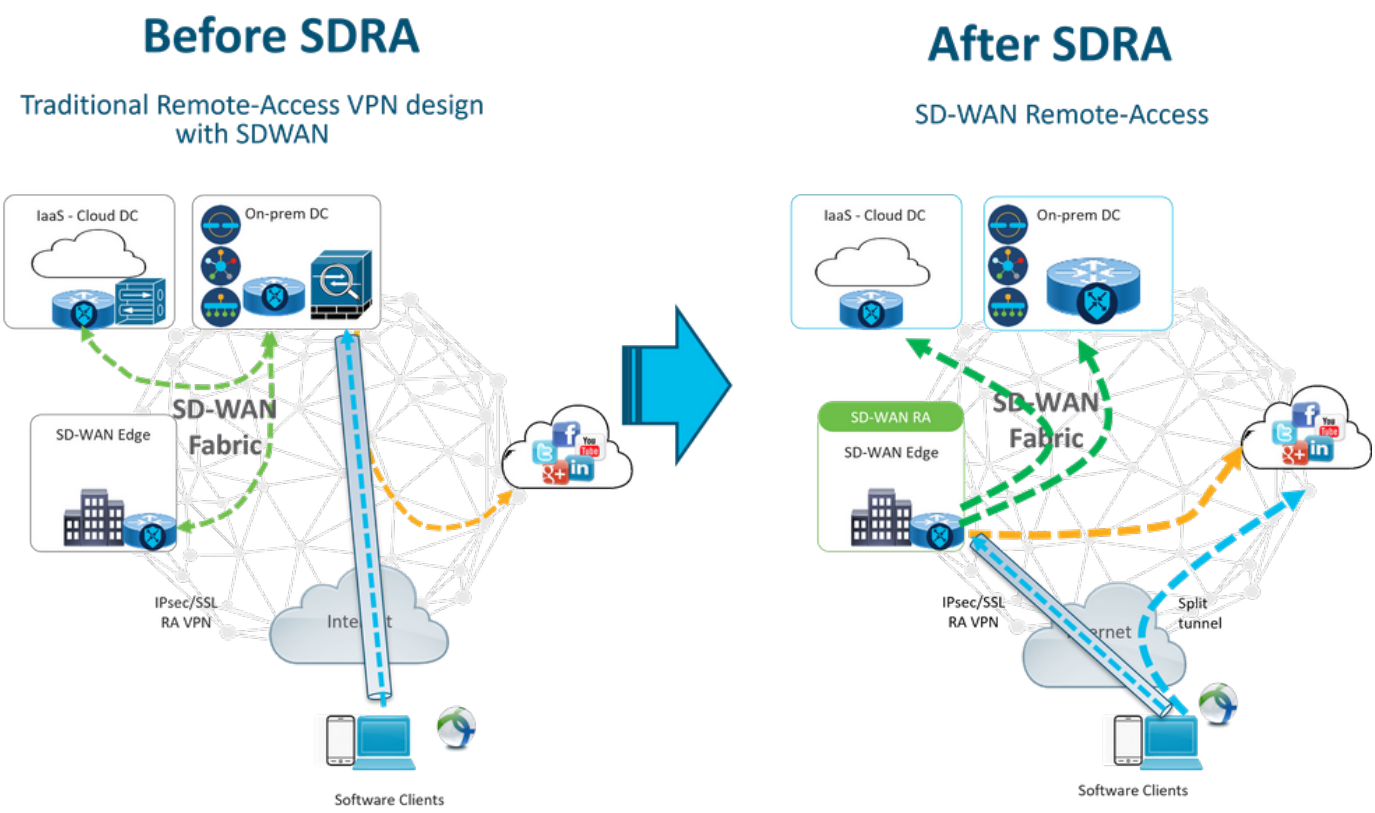
Split Tunneling vs Tunnel All

Split tunneling is used in scenarios where only specific traffic must be tunneled (SD-WAN subnets for example) as shown in the image.



Before SDRA and After SDRA

The traditional remote access VPN design requires separate RA infrastructure outside of the Cisco SD-WAN fabric to provide remote user access to the network like non SD-WAN appliances such as ASA, Regular Cisco IOS® XE, or third-party devices, and RA traffic is moved forward to SD-WAN appliance as shown in the image.



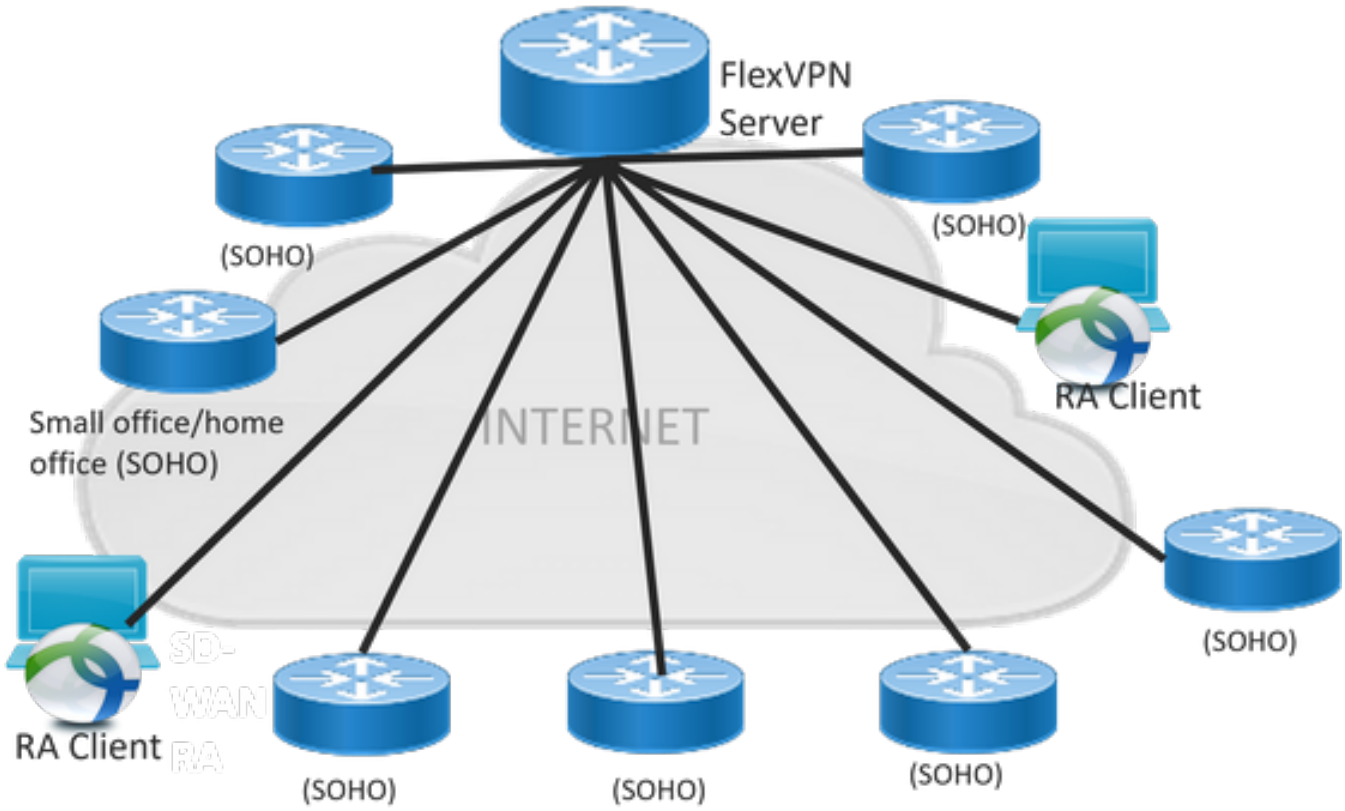
The SD-WAN Remote Access changes the way remote users connect to the network. They connect directly to the cEdge that is used as RA headend. Extends Cisco SD-WAN features and benefits to RA users. RA users become branch LAN-side users.

For each RA client, the SD-WAN RA headend assigns an IP address to an RA client and adds a static host route to the assigned IP address in the service VRF in which the RA user is placed.

The static route specifies the VPN tunnel of the RA client connection. The SD-WAN RA headend advertises the static IP within the service VRF of the RA client with the use of OMP to all edge devices in the service VPN.

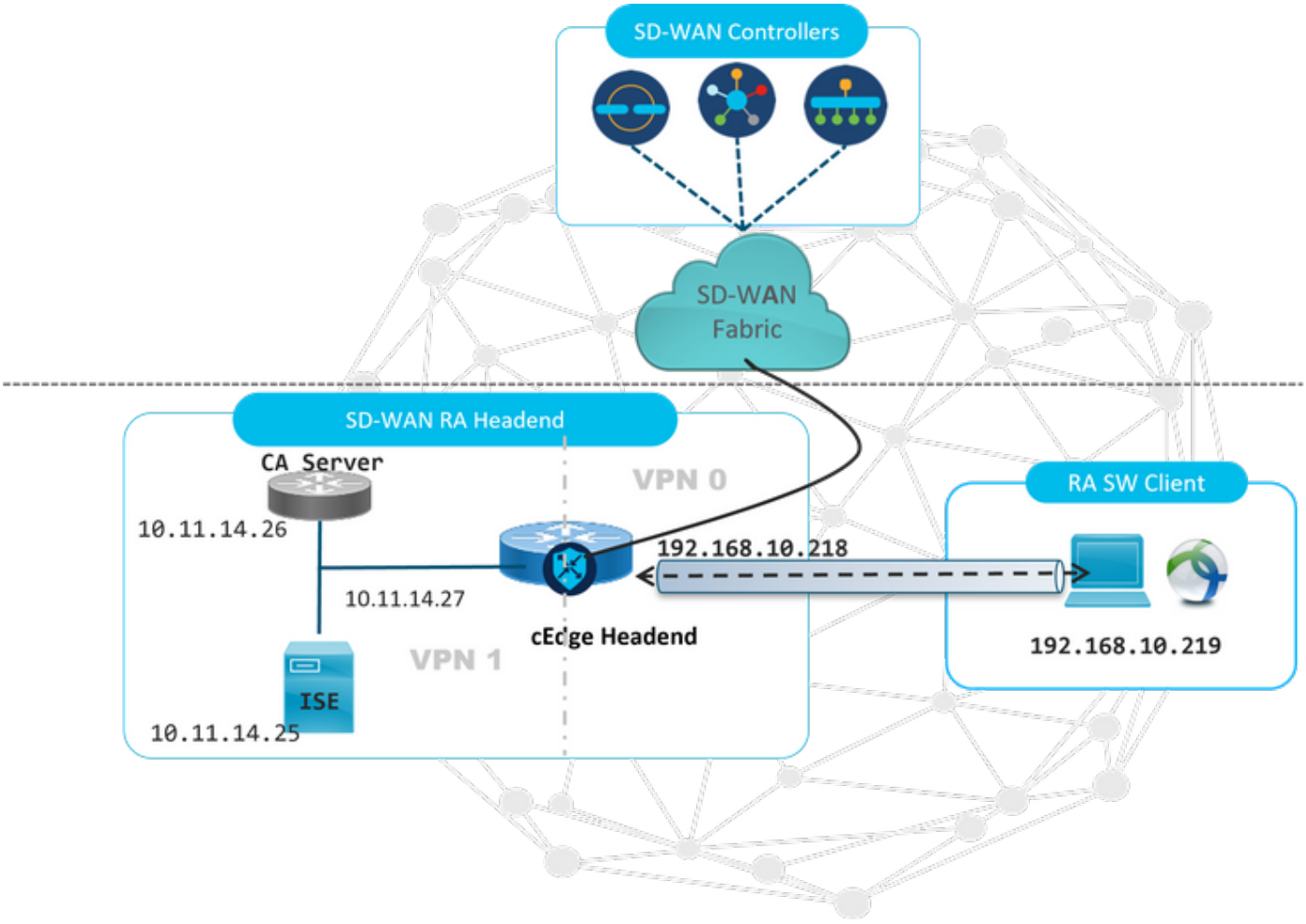
What is FlexVPN?

SD-WAN RA Leverages the Cisco FlexVPN RA solution. FlexVPN is Cisco's implementation of the IKEv2 standard feature a unified paradigm and CLI that combines site to site, **remote access**, hub and spoke topologies, and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while it remains compatible with legacy VPN implementations.



Prerequisites Configuration

For this example, an SD-WAN RA lab setup has been created as shown in the image.



Additional components have been configured for this SD-WAN RA lab scenario:

- A Regular Cisco IOS® XE in Autonomous mode as a CA server.
- An ISE/Radius server for Authentication, Authorization, and Accounting.
- A Windows PC with reachability to the cEdge through the WAN interface.
- AnyConnect Client already installed.

> **Note**: The CA and RADIUS servers have been placed in the service VRF 1. Both servers must be reachable through the service VRF for all the SD-WAN RA headends.

> **Note**: The Cisco SD-WAN Remote Access is supported on the 17.7.1a version and specific devices for SDRA. For supported devices reference navigate to: Supported platforms for the SD-WAN RA headend

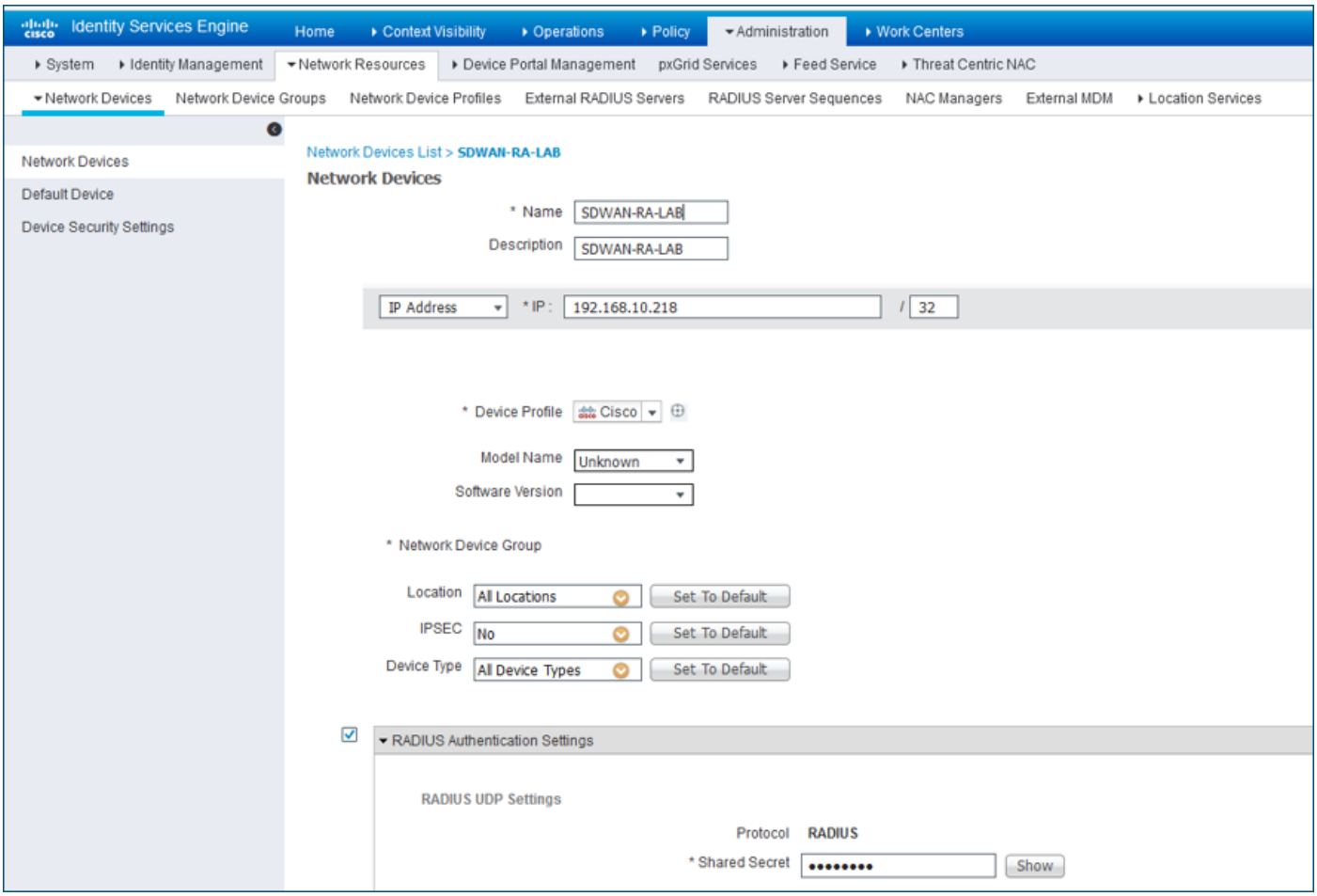
ISE Configuration

To support the SD-WAN RA headend, ensure that the parameters are configured on the RADIUS server. These parameters are required for RA connections:

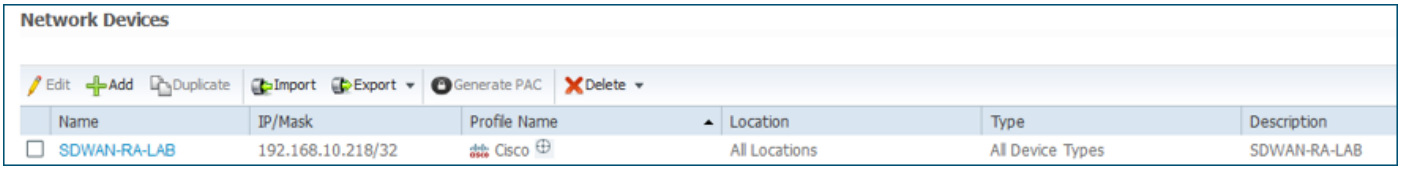
- User authentication credentials Username and password for AnyConnect-EAP connections
- Policy parameters (attributes) that apply to a user or to a user group **VRF**: Service VPN that the RA user is assigned to**IP pool name**: Name of the IP pool defined on the RA headend**Server subnets**: Subnet access to provide to the RA user

The first step to configure in the ISE is the RA headend or cEdge IP address as a Network device to be able to make Radius requests to the ISE.

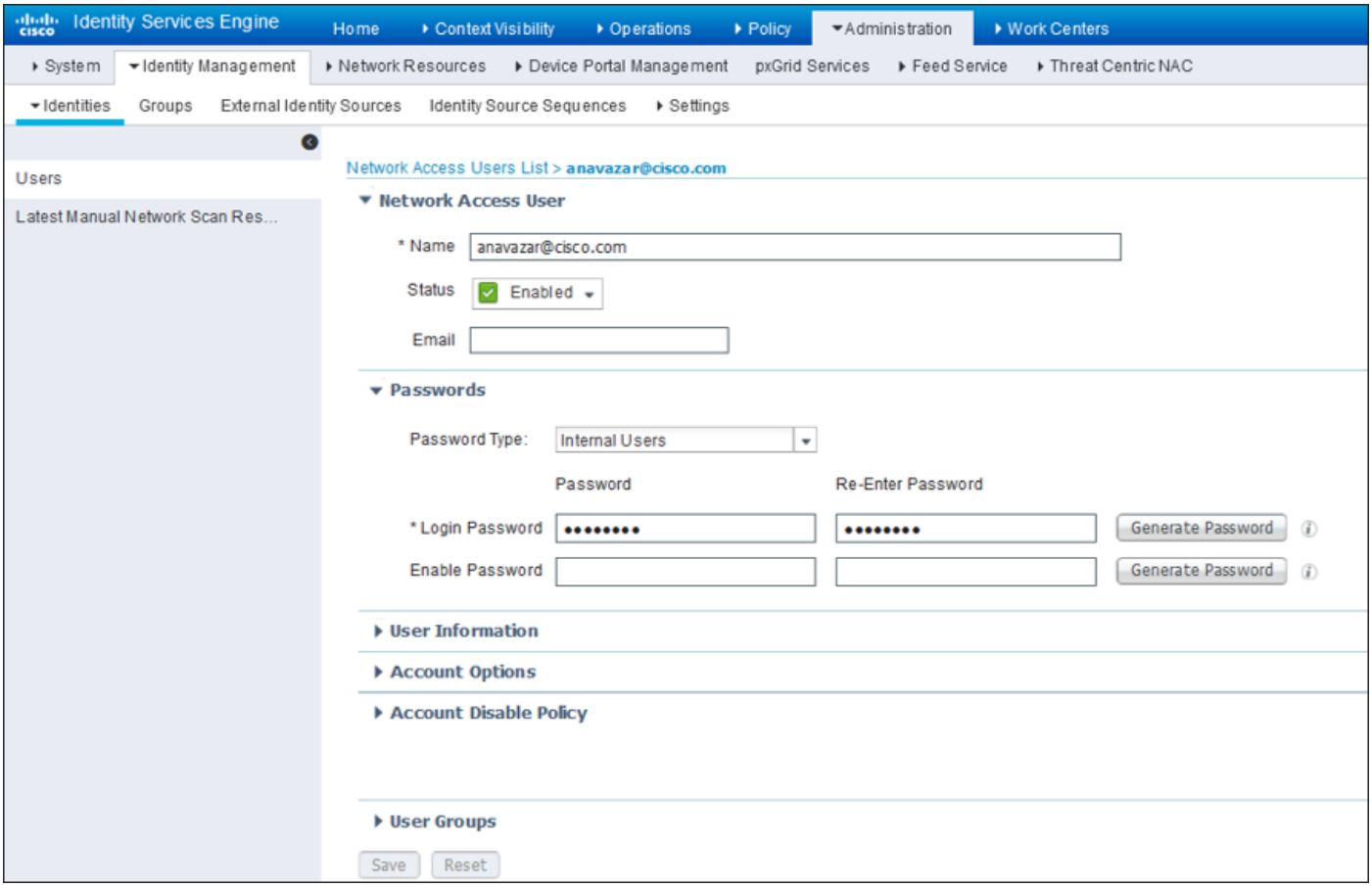
Navigate **to Administration** > **Network Devices** and add the RA Headed (cEdge) IP address and Password as shown in the image.



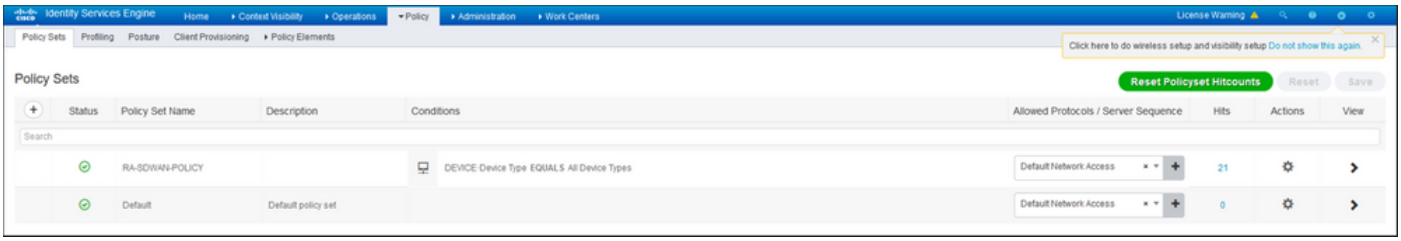
Network device added as shown in the image.



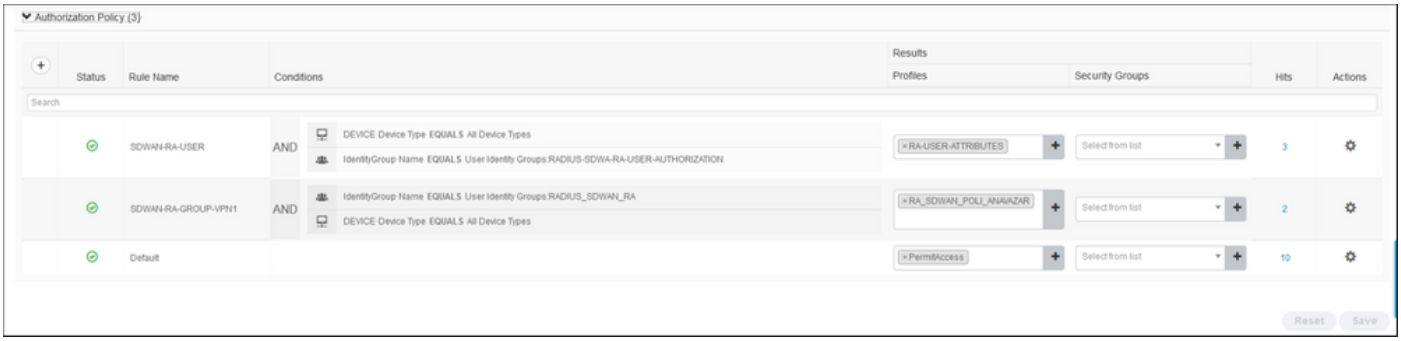
In the RADIUS Server is needed to configure the usernames and password for the AnyConnect authentication as shown in the image. Navigate to **Administration** > **Identities**.



A policy Set needs to be created with the match condition to hit as shown in the image. In this case, the **All Device types** condition is used, which means all the users hit this Policy.



Then, the Authorization Policy has been created one per condition. The condition **All Device types** and the Identity groups to match.



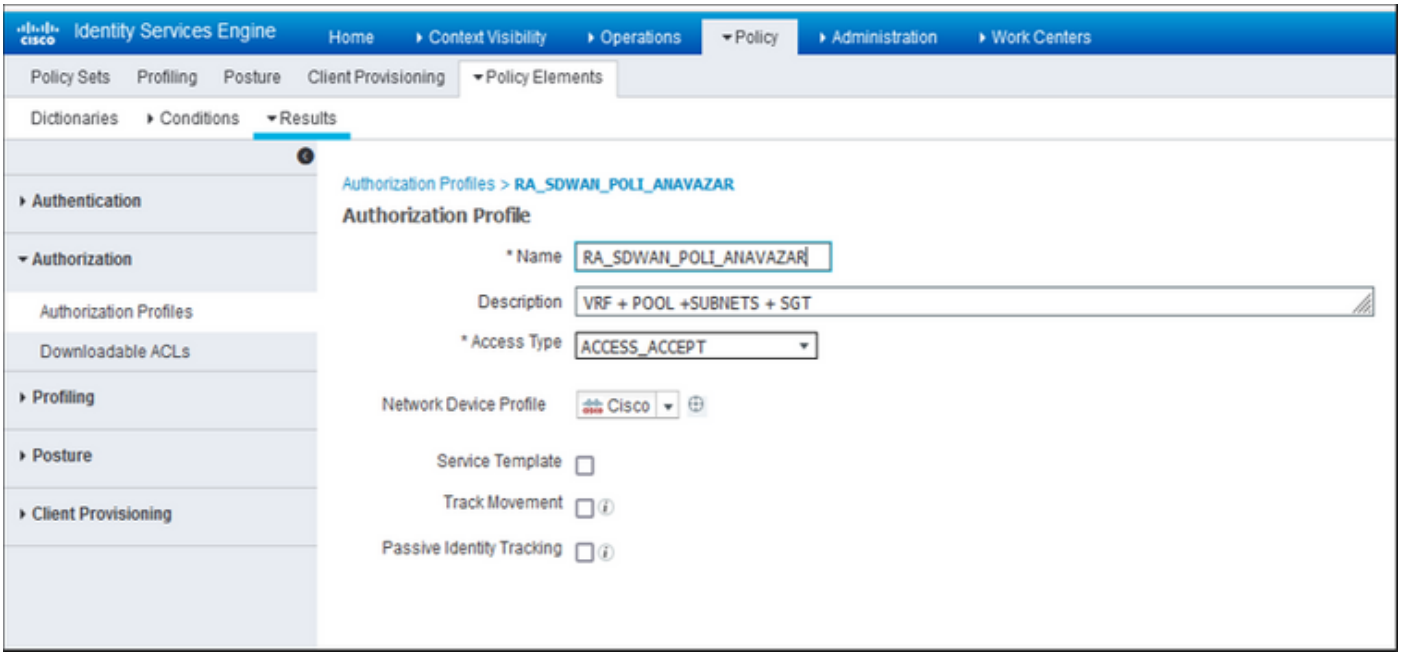
In the **Authorization Profile**, we need to configure the **Access Type** as **Access_ACCEPT** under the **Advanced Attributes Settings**, select the Cisco vendor and **Cisco-AV-pair attribute.**

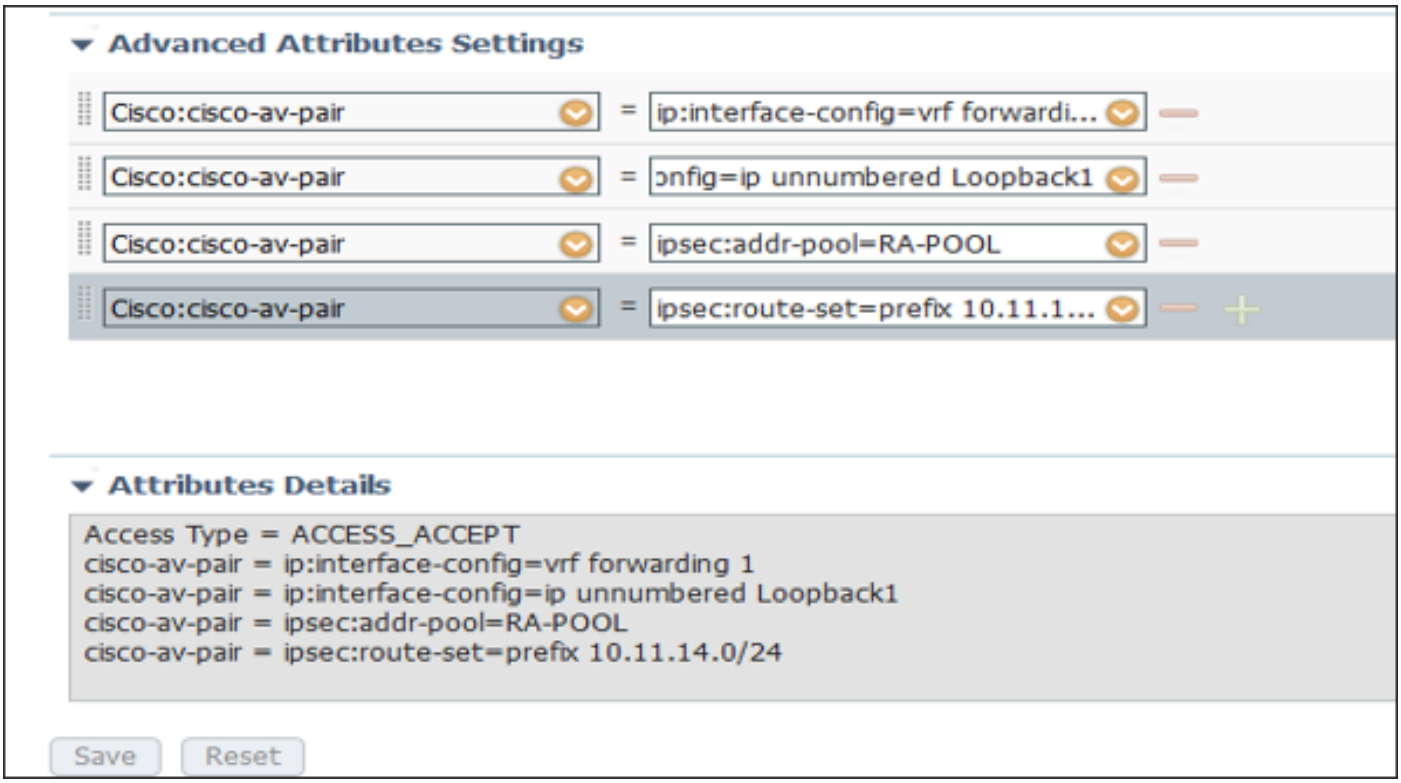
It Is necessary to configure some policy parameters for the users:

- VRF, the Service VRF to which the user belongs.

- The IP pool name, each user connection is assigned an IP address, that belongs to the IP pool configured in the cEdges.
- the subnets that the user can access

Caution: The **IP vrf forwarding** command must come before the **IP unnumbered** command. If the virtual access interface is cloned from the virtual template, and the **IP vrf forwarding** command is then applied, any IP configuration is removed from the virtual access interface.





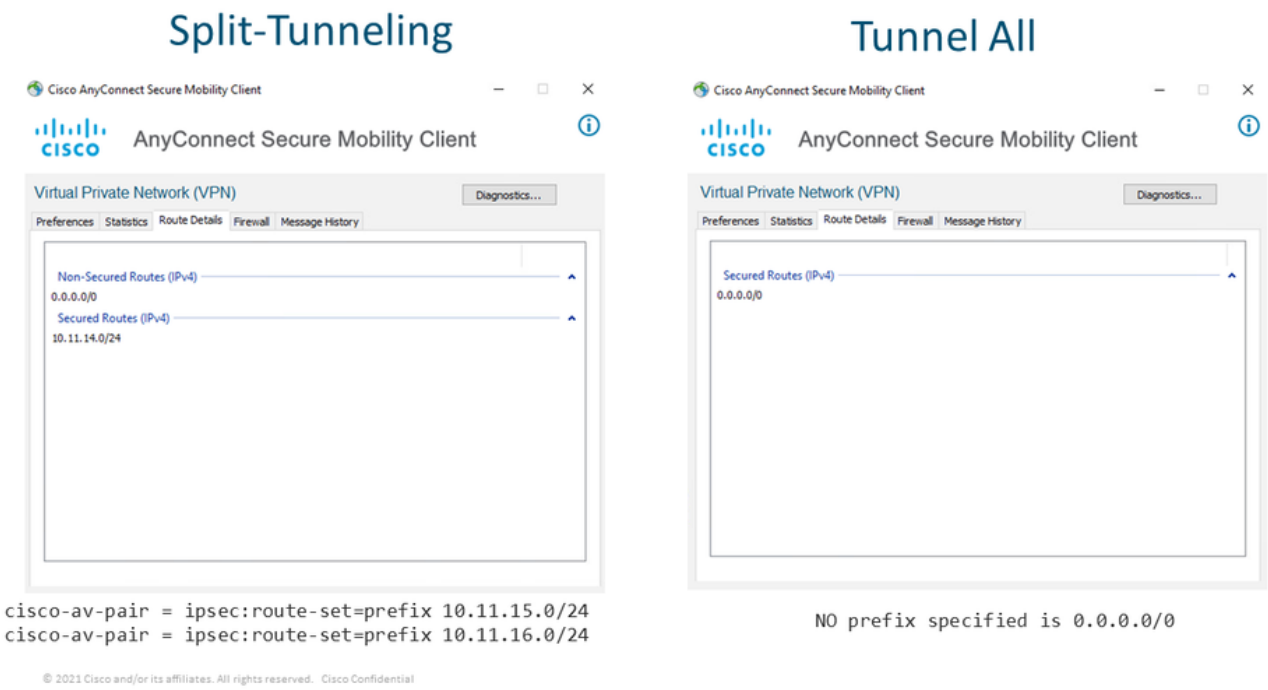
User attributes:

```
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 All in AnyConnect Client

ipsec:route-set=prefix attribute received in the AnyConnect Client is installed as shown in the image.



CA Server Configuration in Cisco IOS® XE

The CA server provisions certificates to the Cisco IOS® XE SD-WAN devices and enables the RA headend to authenticate itself to RA clients.

The CEDGE cannot be a CA server as these crypto PKI server commands are not supported in the Cisco IOS® XE SD-WAN.

- Generate an RSA Keypair
- Create the PKI trustpoint for the CA server Configure the rsakeypair with the previously KEY-CA generated.

  Note: The PKI server and PKI trustpoint must use the same name.

- Create the CA server Configure issuer-name for your CA serverActivate the CA server using “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
!
```

Verify if the CA server is enabled.

```
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
```

Verify if the CA server certificate is installed.

```
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
```

The **Fingerprint SHA 1** from the CA certificate is used on the **crypto pki trustpoint** in the cEdge router (RA headend) with the remote access configuration.

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

SD-WAN RA Configuration

> **Note**: This document does not cover the SD-WAN onboarding process for Controllers and cEdge. It is assumed the SD-WAN fabric is up and fully functional.

Crypto PKI Configuration

- Create PKI trustpoint.
- Configure the URL for the CA server.
- Copy the fingerprint sha 1 from the CA server certificate.
- Configure the Subject Name and Alt Name for the new Identity certificate.
- Configure the rsakeypar with the previously KEY-ID generated.

```
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
```

Ask for the CA certificate to authenticate:

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

Generates the CSR, sends to the CA server and it receives the new Identity certificate:

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

Verify the CA certificate and the cEdge certificate:

```
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 Configuration

```
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 Configuration

Configure IP Pool

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

Configure an IKEv2 Proposals (Ciphers and parameters) and Policy:

```
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
```

Configure an IKEv2 Profile name-mangler:

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

Note: The **name-mangler** derives the name from the prefix in the EAP identity (username) delimitating in the EAP identity that separates the prefix and the suffix.

Configure IPsec ciphers:

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

Configure Crypto IKEv2 profile:

```
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
```

Configure Crypto IPSEC profile:

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

Configure Virtual Template Interface:

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

Configure Virtual Template in the Crypto IKEv2 Profile:

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

SD-WAN RA Configuration Example

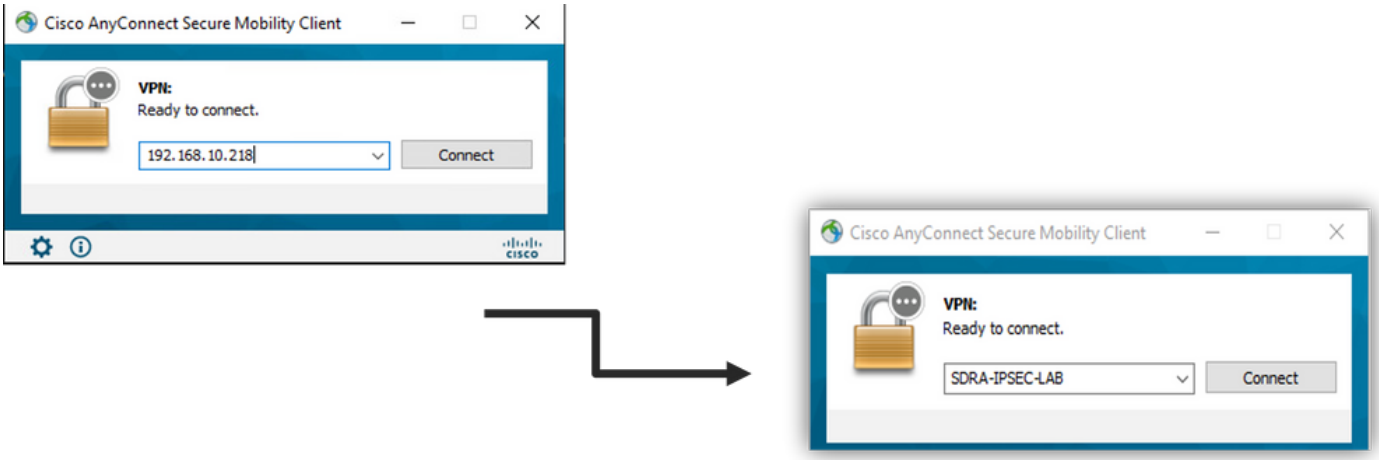
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group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

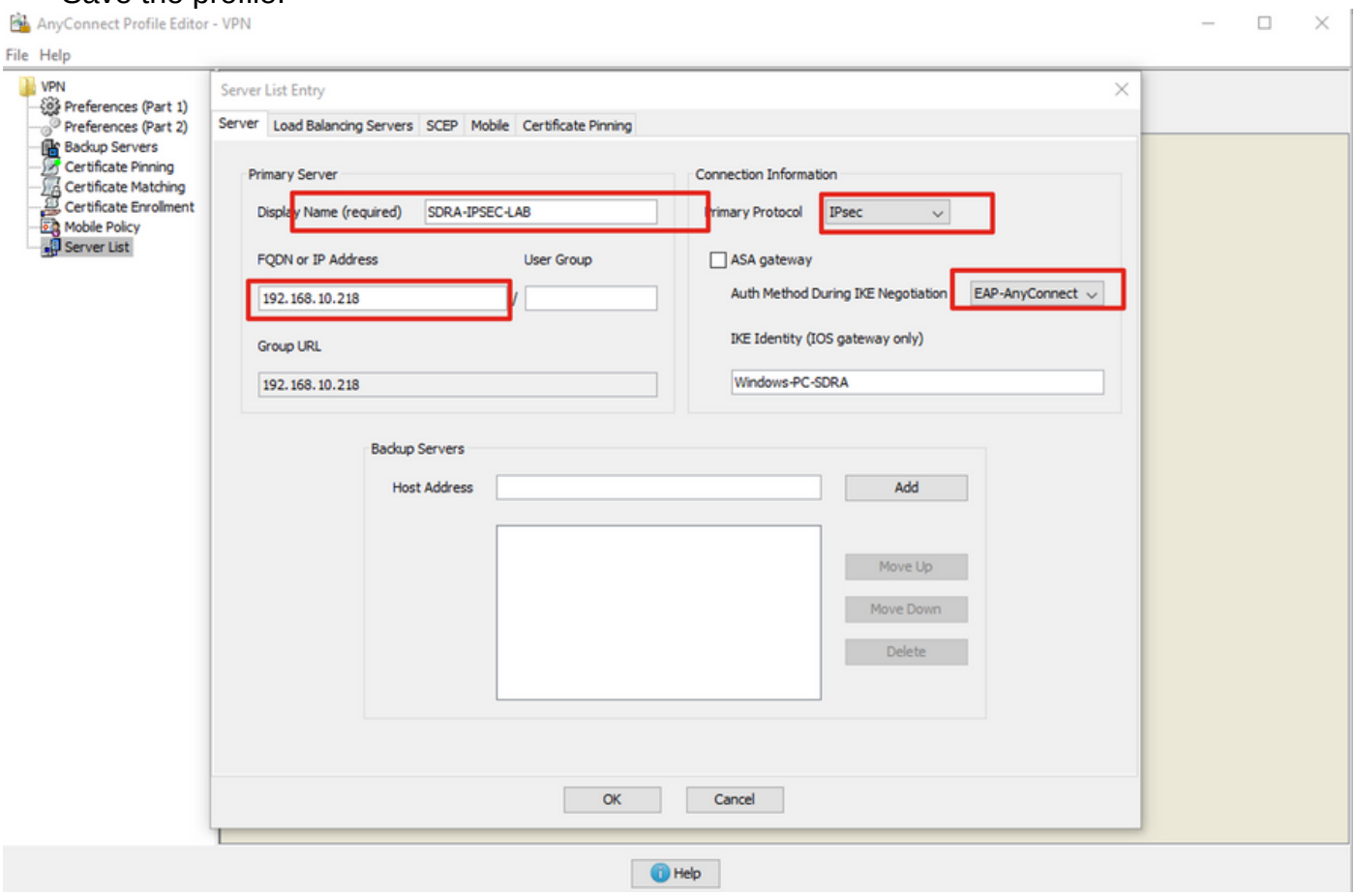
The AnyConnect Client uses SSL as the default protocol for tunnel establishment, and this protocol is not supported for SD-WAN RA (Road map). RA uses FlexVPN, therefore IPSEC is the protocol used and it is mandatory to change it and this is done through the XML profile.

The user can manually enter the FQDN of the VPN gateway in the address bar of the AnyConnect client. This results in the SSL connection to the gateway.



Configure AnyConnect Profile Editor

- Navigate to **Server List** and click **Add**.
- Select **IPsec** as "Primary Protocol".
- Uncheck the **ASA gateway** option.
- Select **EAP-AnyConnect** as the “Auth Method During IKE Negotiation”.
- **Display/Name (Required)** is the name used to save this connection under the AnyConnect client.
- **FQDN or IP Address must** be filed with the cEdge (Public) IP Address.
- Save the profile.



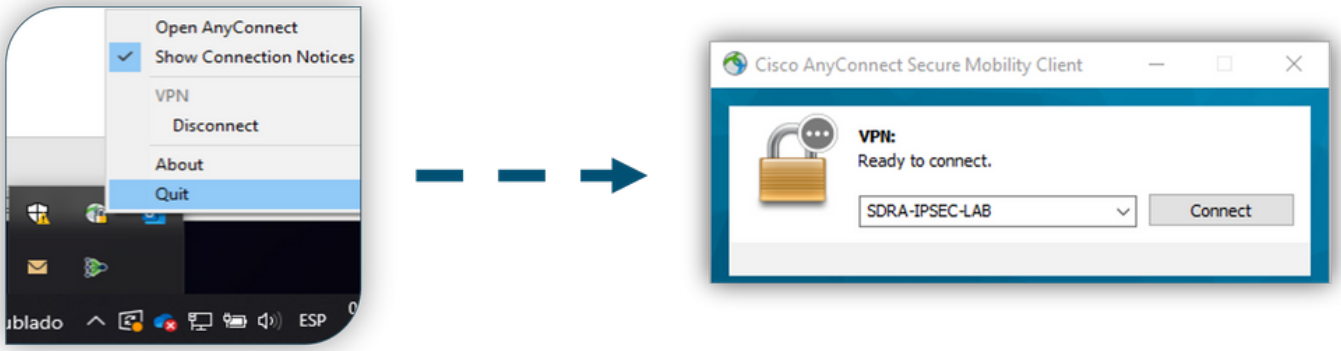
Install the AnyConnect Profile (XML)

The XML profile can be manually put into the directory:

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

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

The AnyConnect client needs to be restarted in order for the profile to become visible in the GUI. The process can be restarted by right-clicking the AnyConnect icon in the Windows tray and selecting the **Quit** option:



Disable the AnyConnect Downloader

The AnyConnect client tries to perform the download of the XML profile after successful log in by default.

If the profile is not available, the connection fails. As a workaround, it is possible to disable the AnyConnect profile download capability on the client itself.

For Windows:

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

For MAC OS:

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

The "BypassDownloader" option is set to "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</AllowManagementVPNProfileUpdatesFromAnyServ
er>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

Unblock Untrusted Servers on AnyConnect Client

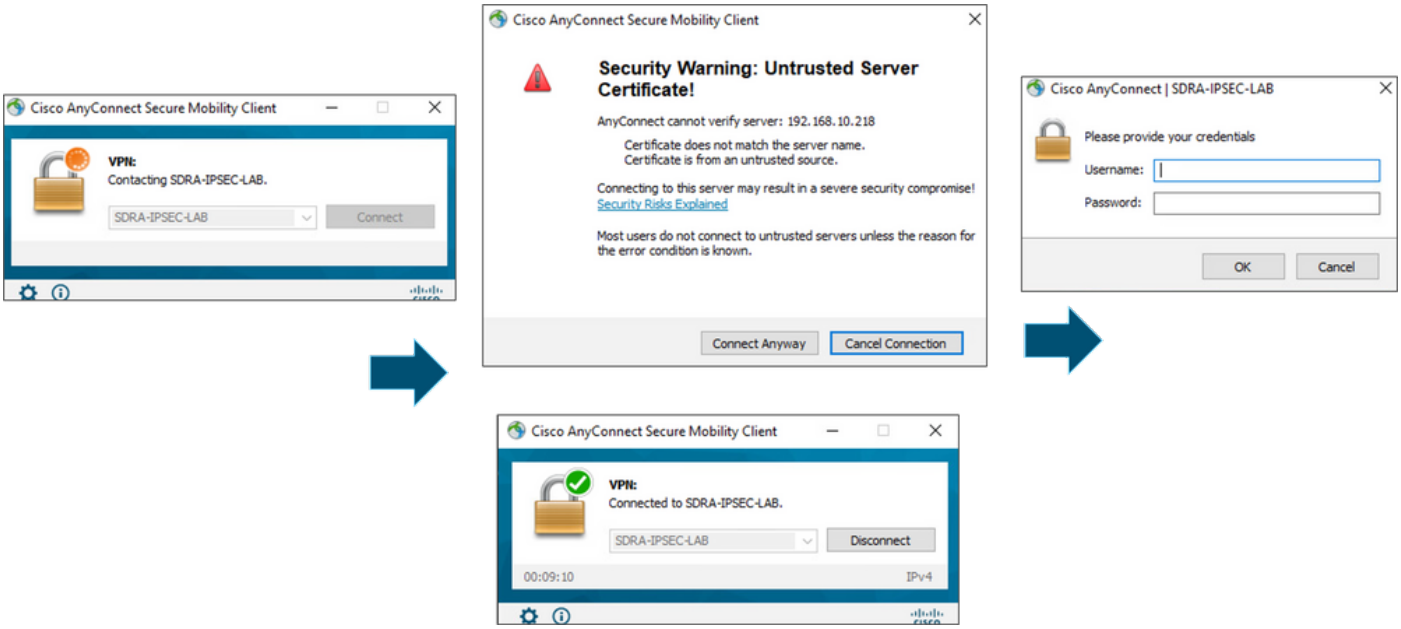
Navigate to **Settings** > **Preferences** and uncheck all the box options.

The most important is the “**Block Connections to untrusted servers**“ for this scenario.

> **Note:** The Certificate used for RA headend/cEdge authentication is the one previously created and signed by the CA server in Cisco IOS® XE. As this CA server is not a Public entity like GoDaddy, Symantec, Cisco, and so on. The PC Client interprets the certificate as an untrusted server. This is fixed using a Public Certificate or CA server your company trusts.

Use AnyConnect Client

Once all the SDRA configuration is placed the flow for a successful connection is shown as the image.



Verify

The virtual template interface is used to create the virtual access interface to start a crypto channel and establish IKEv2 and IPsec security associations (SAs) between the server (cEdge) and the client (AnyConnect user).

> **Note**: The virtual-template interface is always **up/down**. **Status** is **up** and **Protocol** is **down**.

```
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
```

Check the actual configuration applied for the Virtual-Acces interface associated with the client with **show derived-config interface virtual-access <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
```

Check the IPsec security associations (SAs) for AnyConnect client with the **show crypto ipsec sa peer <AnyConnect Pubic 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….
```

Check IKEv2 SA parameters for the session, the username, and the assigned IP.

Note: The assigned IP address must match the IP address on the AnyConnect Client side.

```
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
```

Related Information

- Cisco SD-WAN Remote Access
- Configure the FlexVPN Server
- Download AnyConnect
- Technical Support & Documentation - Cisco Systems