使用AnyConnect和ISE服务器配置SD-WAN远程访问(SDRA)

目录

简介

本文档介绍如何使用Cisco IOS® XE自治模式作为CA服务器和Cisco身份服务引擎(ISE)服务器来配置AnyConnect客户端的SD-WAN远程访问(SDRA)，以进行身份验证、授权和记帐。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义广域网(SD-WAN)
- 公用密钥基础结构 (PKI)
- FlexVPN
- RADIUS 服务器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C8000V版本17.07.01a
- vManage版本20.7.1
- CSR1000V版本17.03.04.a
- ISE版本2.7.0.256
- AnyConnect安全移动客户端版本4.10.04071

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

什么是远程访问VPN?

远程访问VPN允许远程用户安全地连接到公司网络，使用只能通过办公室插入的设备访问的应用和数据。

远程访问VPN通过员工设备与公司网络之间创建的虚拟隧道工作。

此隧道通过公共互联网，但通过它来回发送的数据受加密和安全协议保护，以帮助保持其私有和安全。

此类VPN的两个主要组件是网络接入服务器/RA头端和VPN客户端软件。

什么是SD-WAN远程访问VPN?

远程访问已集成到SD-WAN解决方案中，无需单独的思科SD-WAN和RA基础设施，并通过将Cisco AnyConnect用作RA软件客户端实现RA服务的快速扩展。

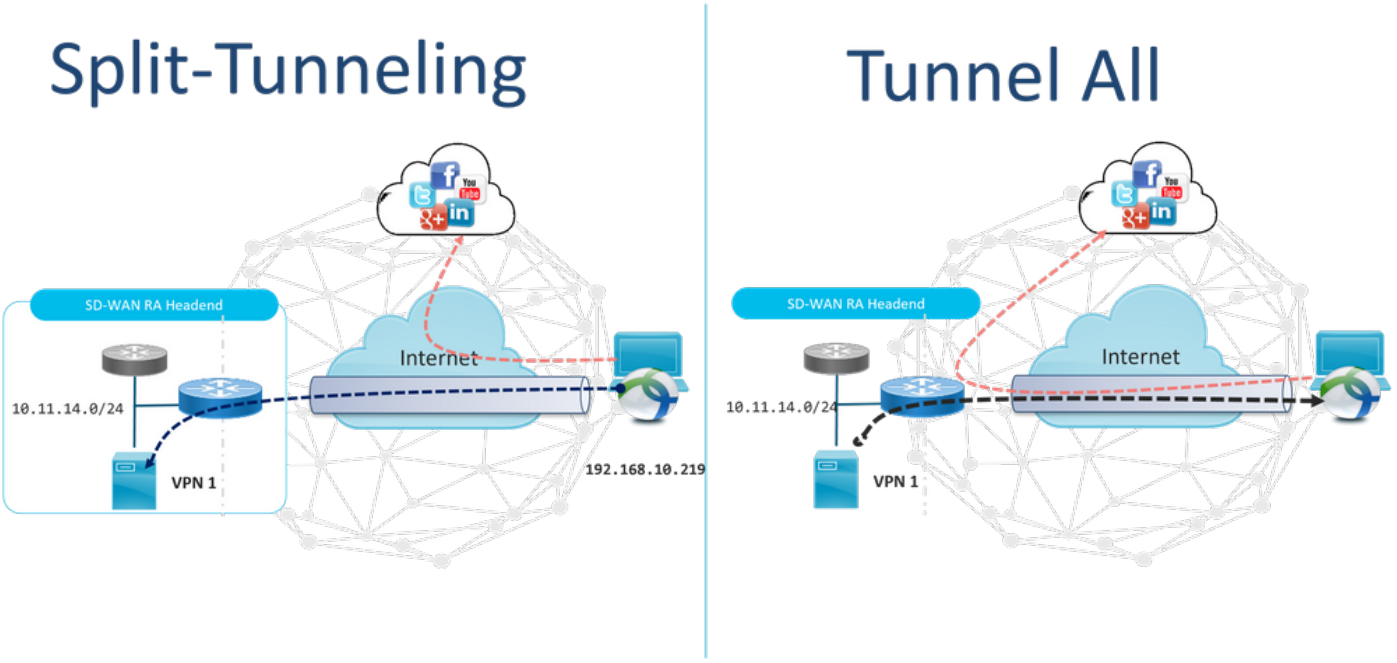
远程访问为远程用户提供对组织网络的访问。这可以从Home（家庭）开始工作。

优势

- RA提供从远程位置的设备/用户访问组织网络的权限。(HO)
- 将思科SD-WAN解决方案扩展到RA用户，而无需每个RA用户的设备加入思科SD-WAN交换矩阵。
- 数据安全
- 分割隧道或全部隧道
- 可扩展性
- 能够在思科SD-WAN交换矩阵中的多个思科IOS® XE SD-WAN设备之间分配RA负载。

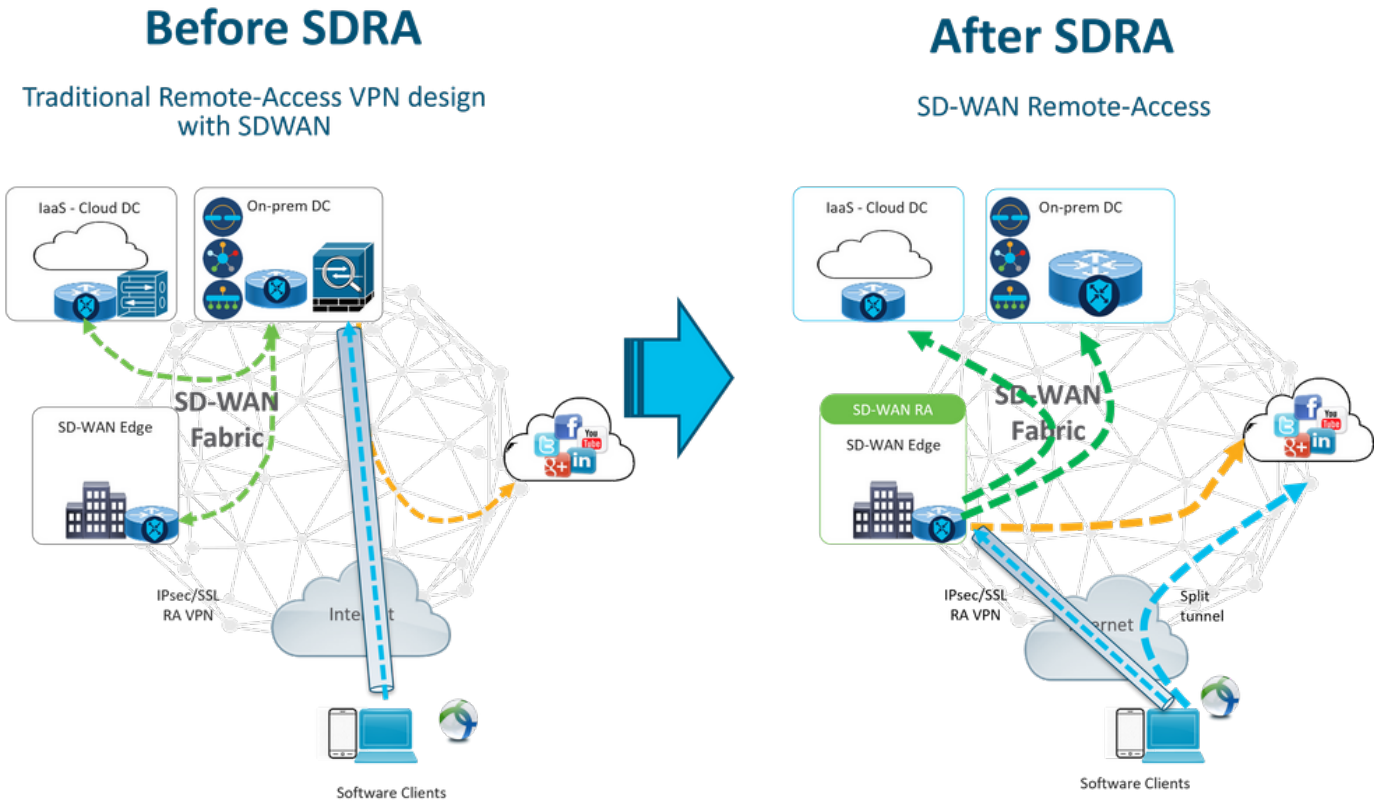
分割隧道与全部隧道

分割隧道用于仅通过隧道传输特定流量（例如SD-WAN子网）的场景，如图所示。



在SDRA之前和SDRA之后

传统远程访问VPN设计要求思科SD-WAN交换矩阵外部的单独RA基础设施，以便远程用户访问网络，如ASA、常规Cisco IOS® XE或第三方设备等，并且RA流量会转移到SD-WAN设备，如图所示。



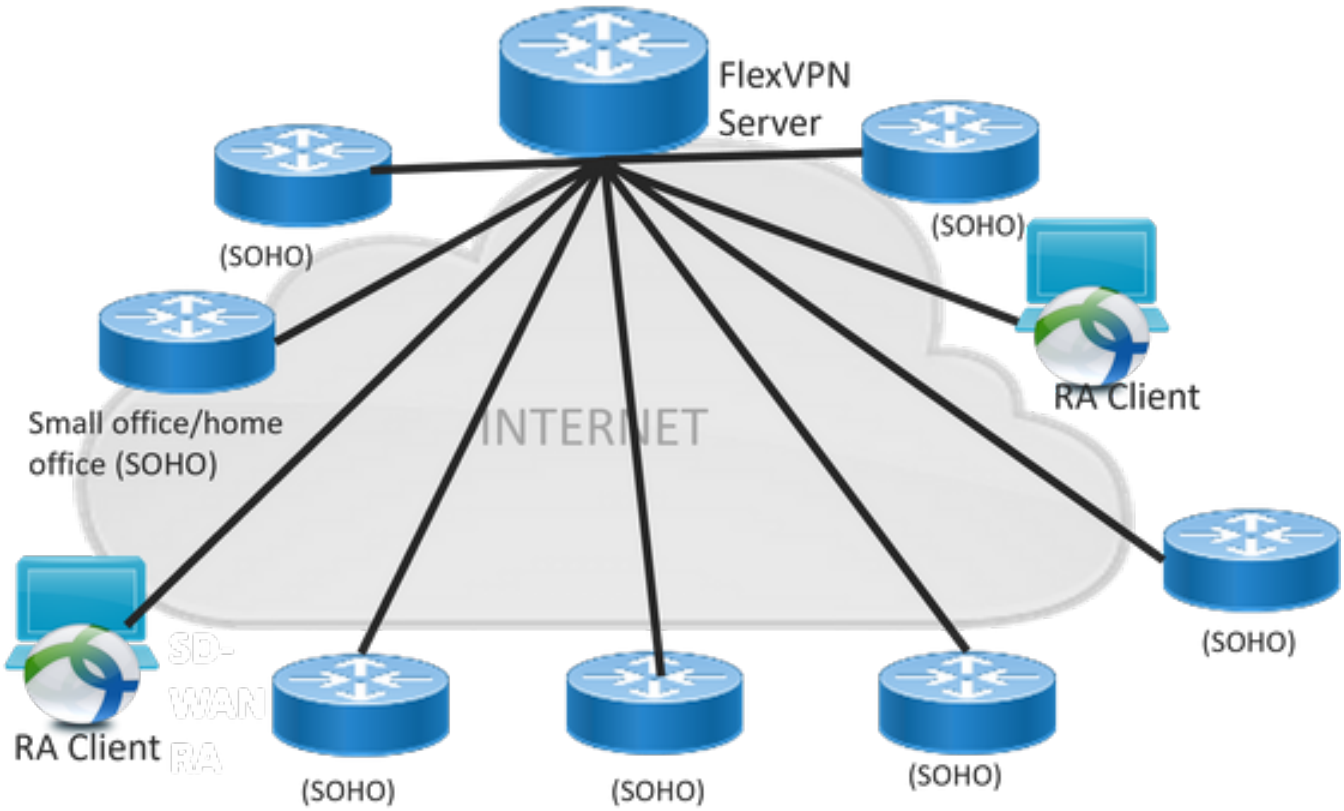
SD-WAN远程访问改变了远程用户连接到网络的方式。它们直接连接到用作RA头端的cEdge。将思科SD-WAN功能和优势扩展到RA用户。RA用户成为分支机构LAN端用户。

对于每个RA客户端，SD-WAN RA头端向RA客户端分配IP地址，并在RA用户所在的服务VRF中向分配的IP地址添加静态主机路由。

静态路由指定RA客户端连接的VPN隧道。SD-WAN RA头端使用OMP向服务VPN中的所有边缘设备通告RA客户端服务VRF中的静态IP。

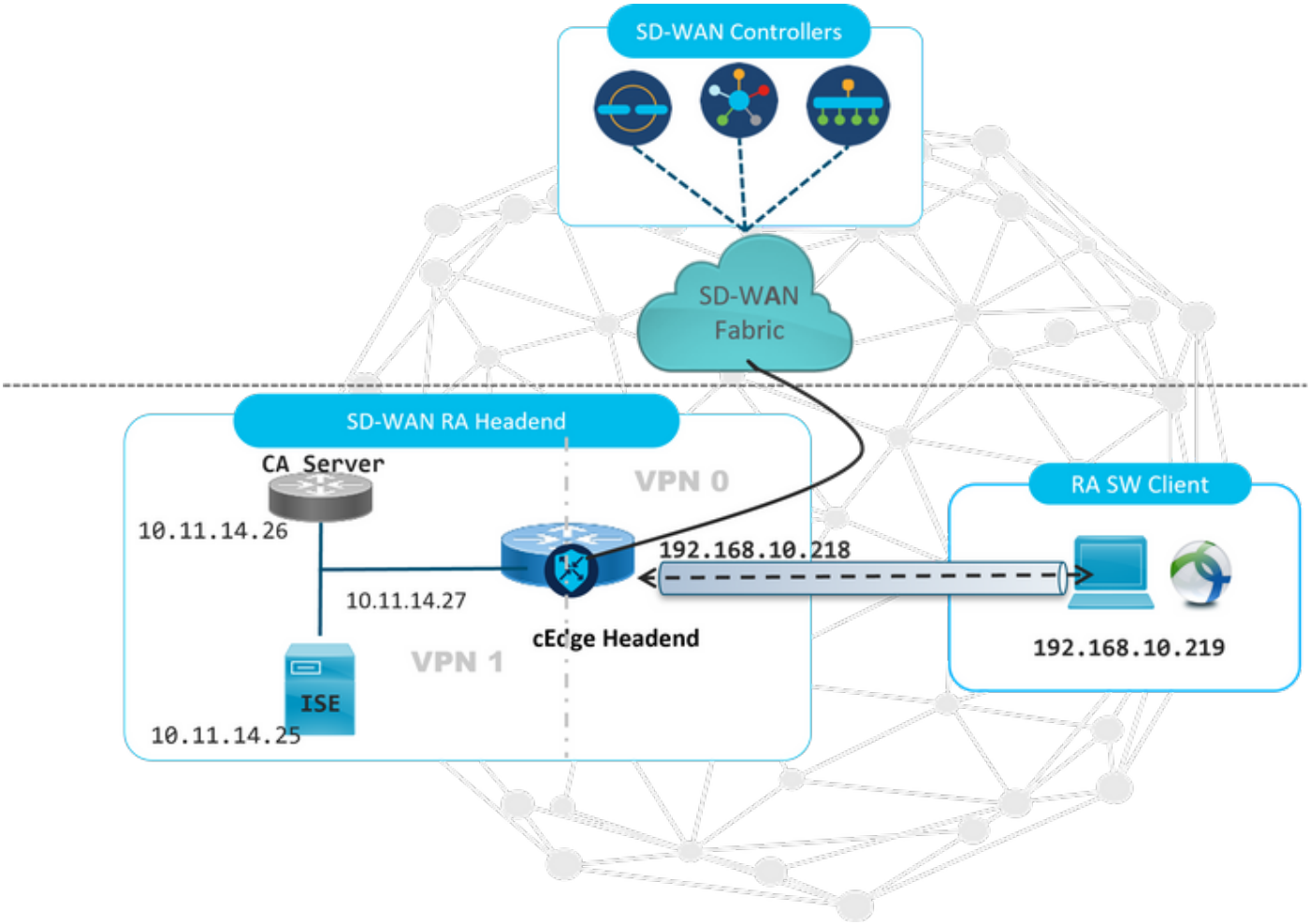
什么是FlexVPN?

SD-WAN RA利用Cisco FlexVPN RA解决方案。FlexVPN是思科对IKEv2标准的实施，它采用统一的范式和CLI，将站点到站点、远程访问、中心和分支拓扑以及部分网格（分支到分支直接）结**合在**一起。 FlexVPN提供简单但模块化的框架，该框架广泛使用隧道接口范式，同时保持与传统VPN实施兼容。



先决条件配置

在本示例中，已创建SD-WAN RA实验室设置，如图所示。



此SD-WAN RA实验场景已配置了其他组件：

- 作为CA服务器在自治模式下的常规Cisco IOS® XE。
- 用于身份验证、授权和记帐的ISE/Radius服务器。
- Windows PC可通过WAN接口访问cEdge。
- 已安装AnyConnect客户端。

> **注意**：CA和RADIUS服务器已放置在服务VRF 1中。 所有SD-WAN RA头端都必须通过服务VRF访问两台服务器。

> **注意**：17.7.1a版本和SDRA的特定设备支持思科SD-WAN远程访问。对于支持的设备，请导航至：支持的SD-WAN RA头端平台

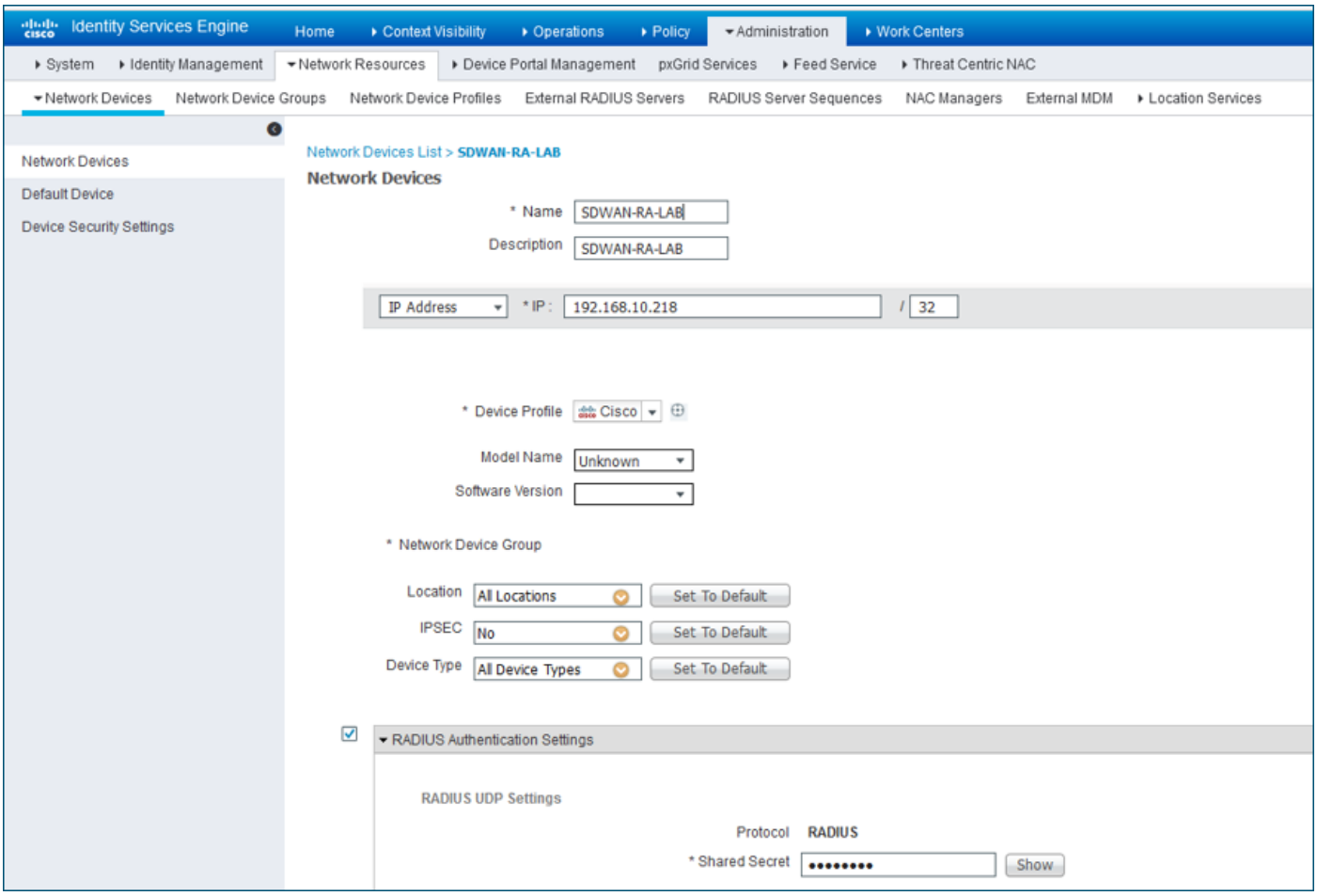
ISE配置

要支持SD-WAN RA头端，请确保在RADIUS服务器上配置参数。RA连接需要以下参数：

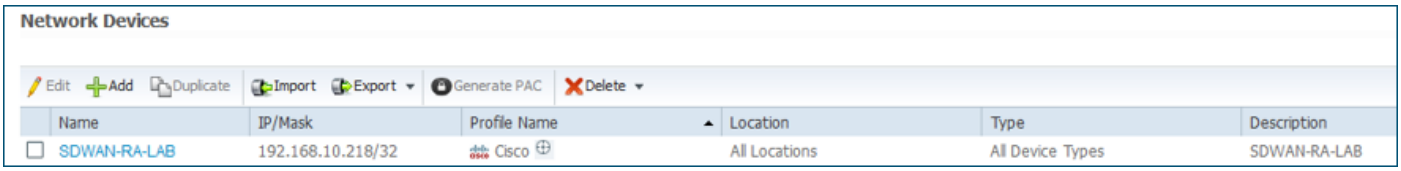
- 用户身份验证凭证 AnyConnect-EAP连接的用户名和密码
- 应用于用户或用户组的策略参数（属性） **VRF**:RA用户分配到的服务VPN**IP池名称**:RA头端上定义的IP池的名称**服务器子网**:为RA用户提供子网访问

在ISE中配置的第一步是RA头端或cEdge IP地址作为网络设备，以便能够向ISE发出Radius请求。

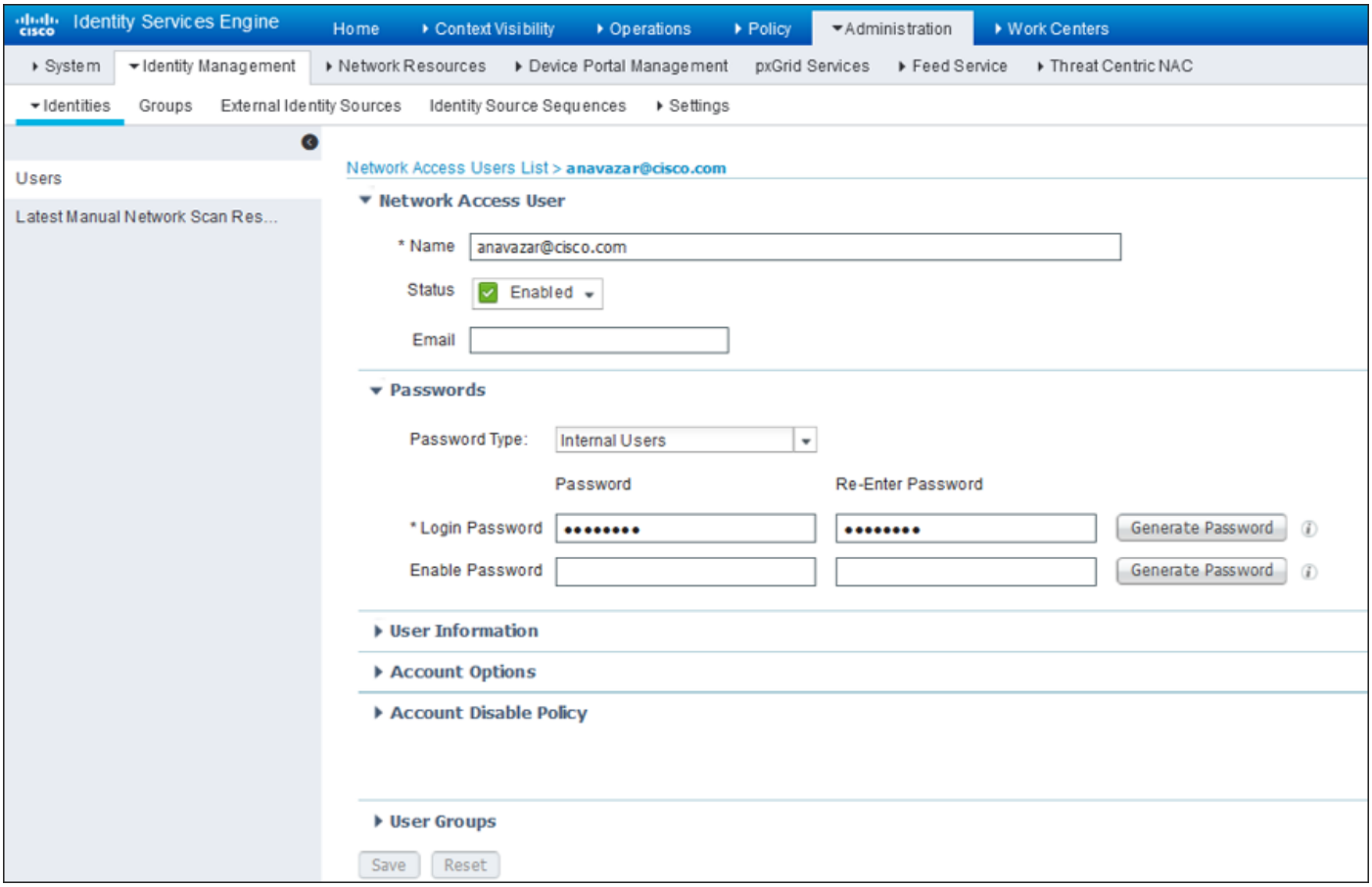
导航至**Administration > Network Devices**，并添加RA Headend(cEdge)IP地址和密码，如图所示。



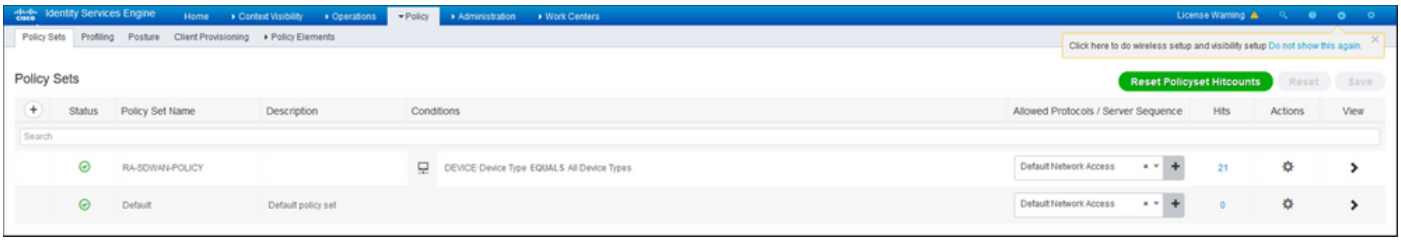
如图所示添加的网络设备。



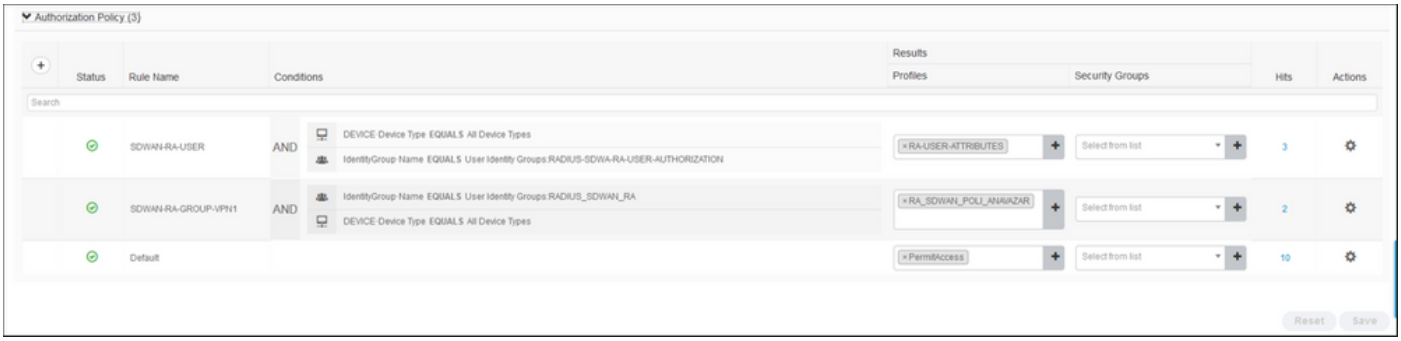
在RADIUS服务器中，需要配置AnyConnect身份验证的用户名和密码，如图所示。导航至**管理>身份**。



需要创建具有匹配条件的策略集，如图所示。在这种情况下，将使用**“所有设备类**型”条件，这意味着所有用户都符合此策略。



然后，已为每个条件创建一个授权策略。要匹配**的所有设**备类型和身份组条件。



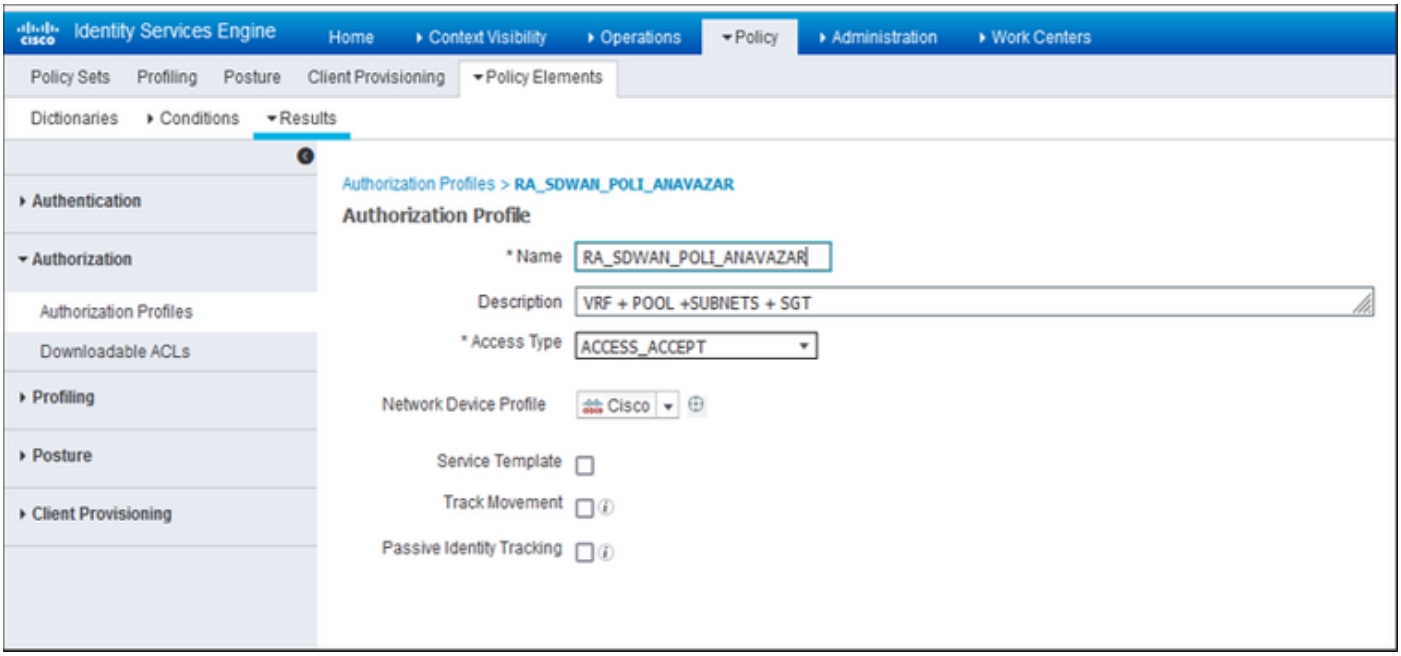
在**授权配置文件**中，我们需要在**高级属性设置**下将**访问类型**配置为Access_ACCEPT，选择Cisco供应商和**Cisco-AV-pair属性。**

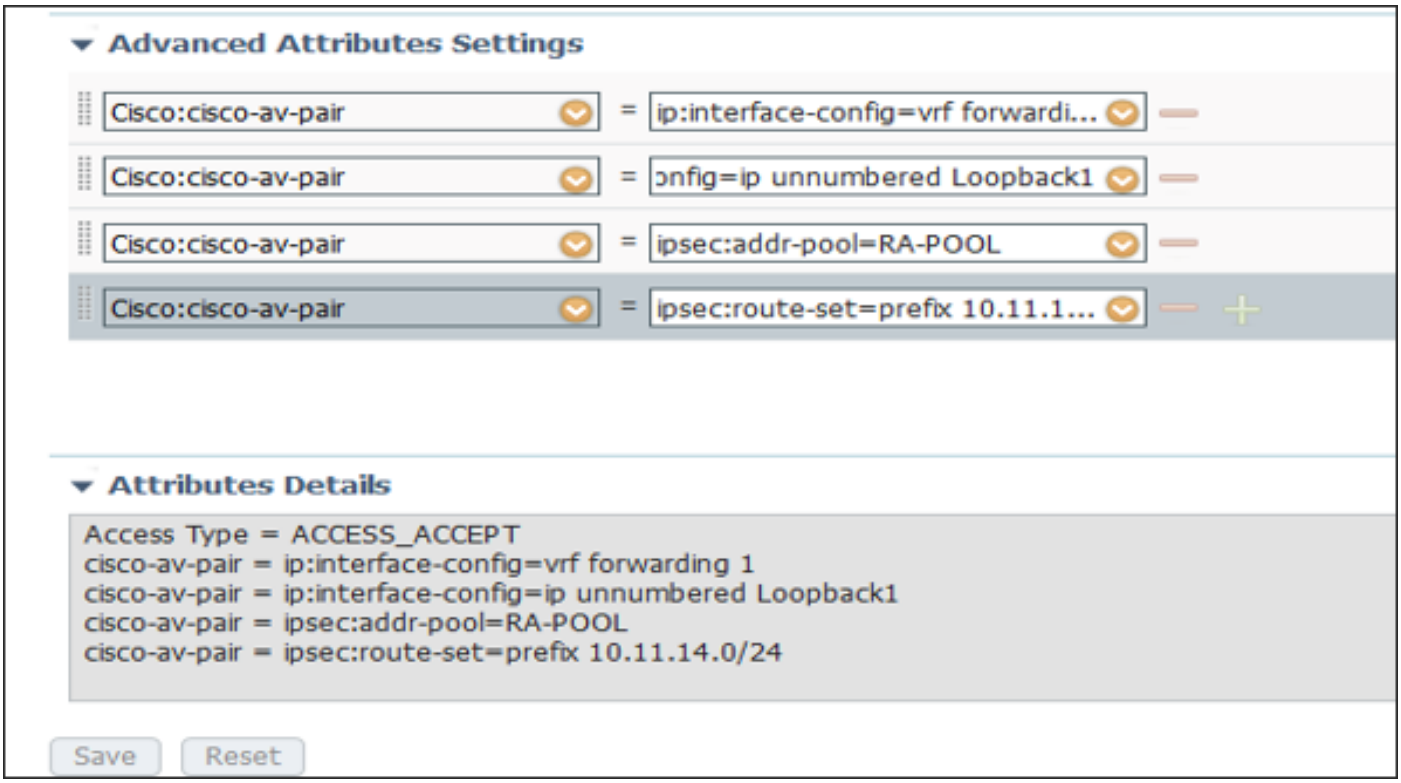
必须为用户配置一些策略参数：

- VRF，用户所属的服务VRF。
- IP池名称，每个用户连接都分配了属于cEdge中配置的IP池的IP地址。

- 用户可以访问的子网

警告： IP vrf forwarding**命令必**须位于IP unnumbered命**令之**前。如果从虚拟模板克隆虚拟访问接口，然后应用**IP vrf forwarding**命令，则会从虚拟访问接口删除任何IP配置。



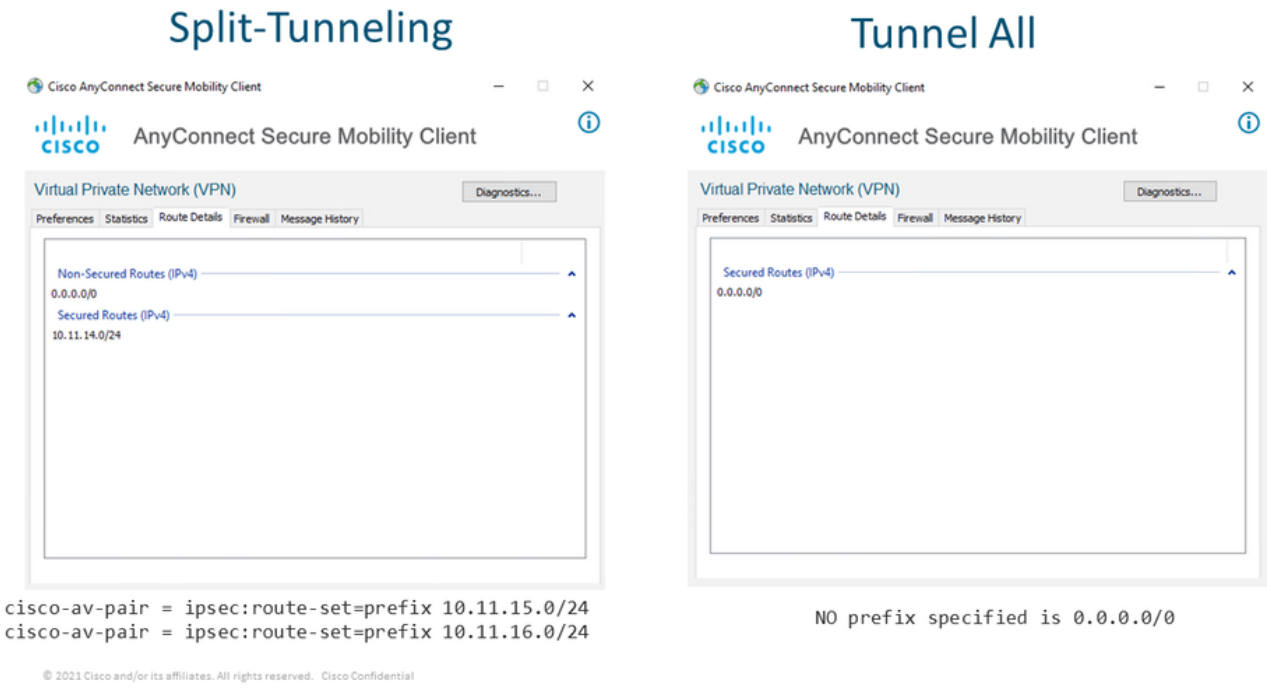


用户属性：

```
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
```

AnyConnect客户端中的分割隧道与全部隧道

在AnyConnect客户端中收到的ipsec:route-set=prefix属性如图所示安装。



Cisco IOS® XE中的CA服务器配置

CA服务器将证书调配到Cisco IOS® XE SD-WAN设备，并使RA头端能够向RA客户端验证自身。

CEDGE不能是CA服务器，因为Cisco IOS® XE SD-WAN不支持这些crypto PKI服务器命令。

- 生成RSA密钥对
- 为CA服务器创建PKI信任点 使用之前生成的KEY-CA配置rsakeypair。

  注意：PKI服务器和PKI信任点必须使用相同的名称。

- 创建CA服务器 为CA服务器配置颁发者名称使用“No shutdown”激活CA服务器

```
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
!
```

验证CA服务器是否已启用。

```
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
```

验证是否安装了CA服务器证书。

```
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
```

来自**CA证书的**指纹SHA 1在cEdge路由器（RA头端）**的加密**pki信任点上使用远程访问配置。

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

SD-WAN RA配置

> **注意：**本文档不介绍控制器和CEdge的SD-WAN自注册过程。假设SD-WAN交换矩阵已启用且完全正常工作。

加密PKI配置

- 创建PKI信任点。
- 配置CA服务器的URL。
- 从CA服务器证书复制指纹sha 1。
- 配置新身份证书的使用者名称和备用名称。
- 使用之前生成的KEY-ID配置rsakeypar。

```
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
```

请求CA证书进行身份验证：

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

生成CSR，发送到CA服务器，并接收新的身份证书：

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

验证CA证书和cEdge证书：

```
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配置

```
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配置

配置IP池

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

配置IKEv2提议（密码和参数）和策略：

```
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
```

配置IKEv2配置文件名称 — mangler:

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

> **注意：name-mangler**从EAP身份（用户名）中限定的前缀（EAP身份中分隔前缀和后缀）派生名称。

配置IPsec密码：

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

配置加密IKEv2配置文件：

```
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
```

配置加密IPSEC配置文件：

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

配置虚拟模板接口：

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

在加密IKEv2配置文件中配置虚拟模板：

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

SD-WAN RA配置示例

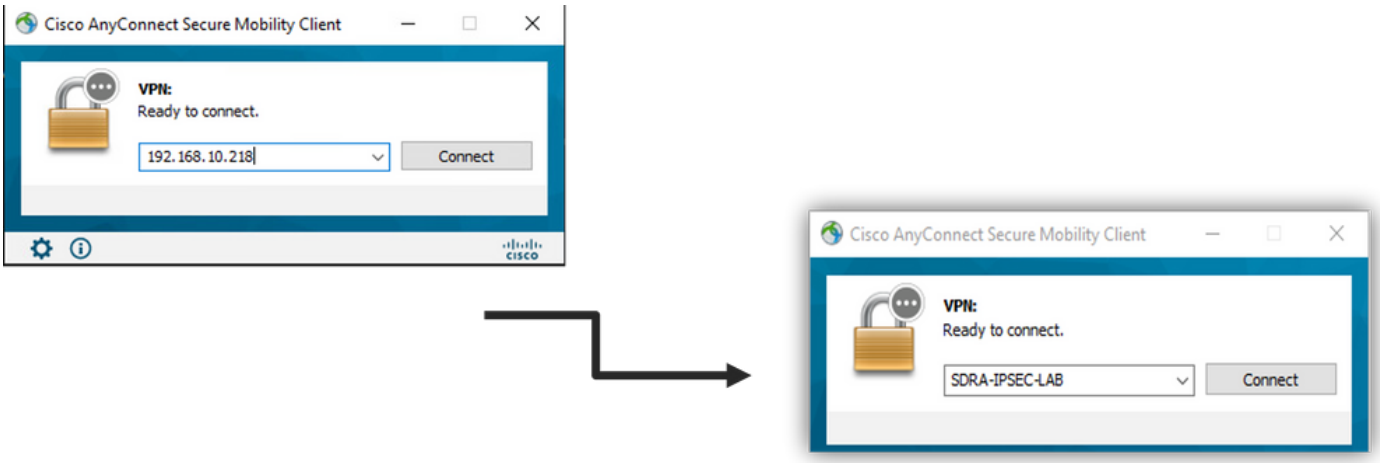
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group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

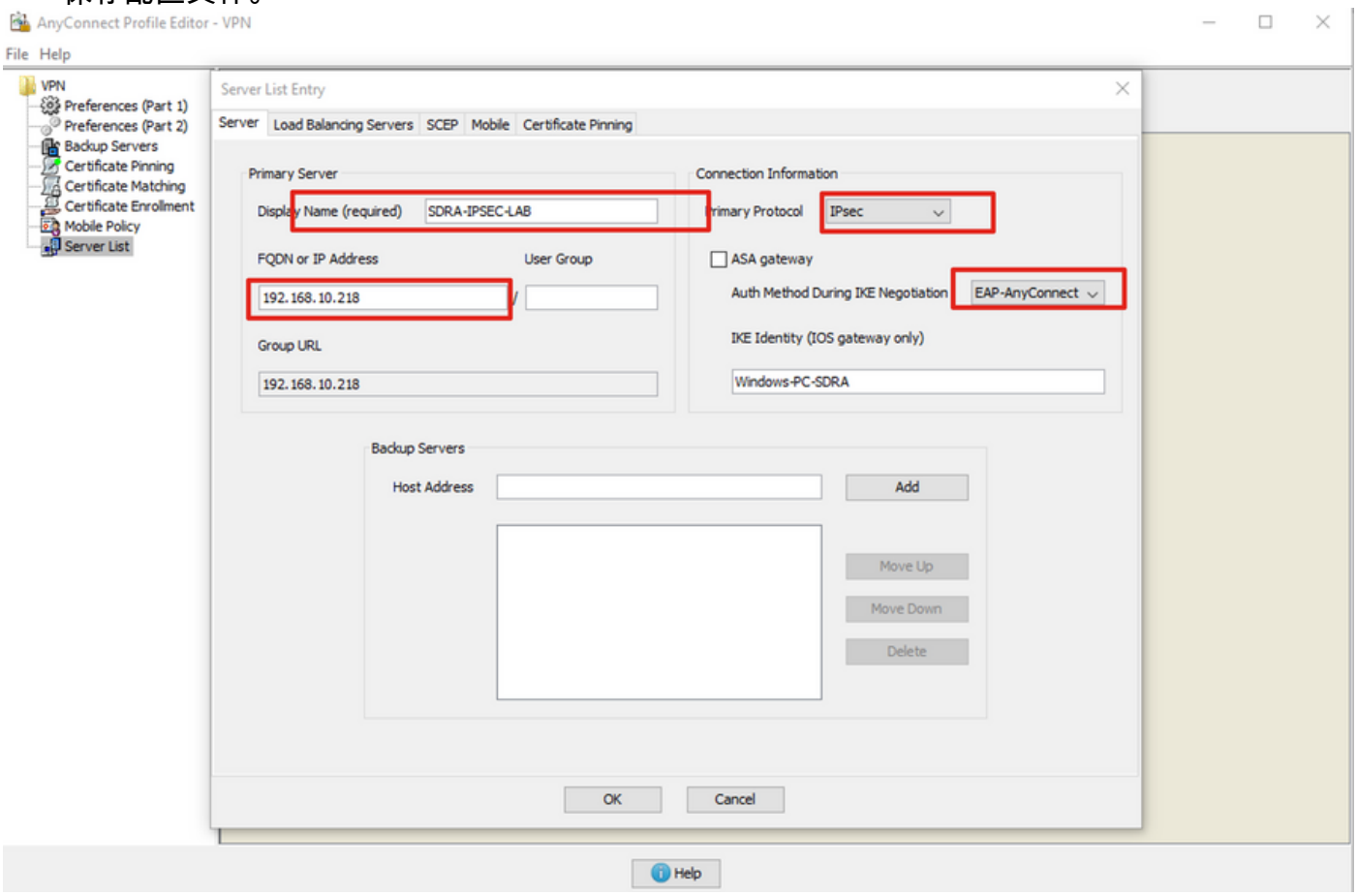
AnyConnect客户端使用SSL作为隧道建立的默认协议，SD-WAN RA（路线图）不支持此协议。RA使用FlexVPN，因此IPSEC是使用的协议，必须更改它，这是通过XML配置文件完成的。

用户可以在AnyConnect客户端的地址栏中手动输入VPN网关的FQDN。这会导致与网关的SSL连接。



配置AnyConnect配置文件编辑器

- 导航至“服**务器列表**”，然后单**击“添加**”。
- 选择**IPsec**作为“Primary Protocol”。
- 取消选中**ASA网关**选项。
- 选**择EAP-AnyConnect**作为“IKE协商期间的身份验证方法”。
- Display/**Name（必需）是用于在AnyConnect客户端下保存此连接的名称。**
- **FQDN或IP地址必**须与cEdge（公有）IP地址一起归档。
- 保存配置文件。



安装AnyConnect配置文件(XML)

XML配置文件可手动放入目录：

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

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

需要重新启动AnyConnect客户端，以使配置文件在GUI中可见。通过右键单击Windows托盘中的AnyConnect图标并选择“退出”选项，可以重**新启**动进程：

禁用AnyConnect下载程序

默认情况下，AnyConnect客户端在成功登录后尝试执行XML配置文件的下载。

如果配置文件不可用，则连接失败。解决方法是，可以禁用客户端本身上的AnyConnect配置文件下载功能。

Windows：

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

对于MAC OS:

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

“BypassDownloader”选项设置为“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>
```

取消阻止AnyConnect客户端上的不受信任服务器

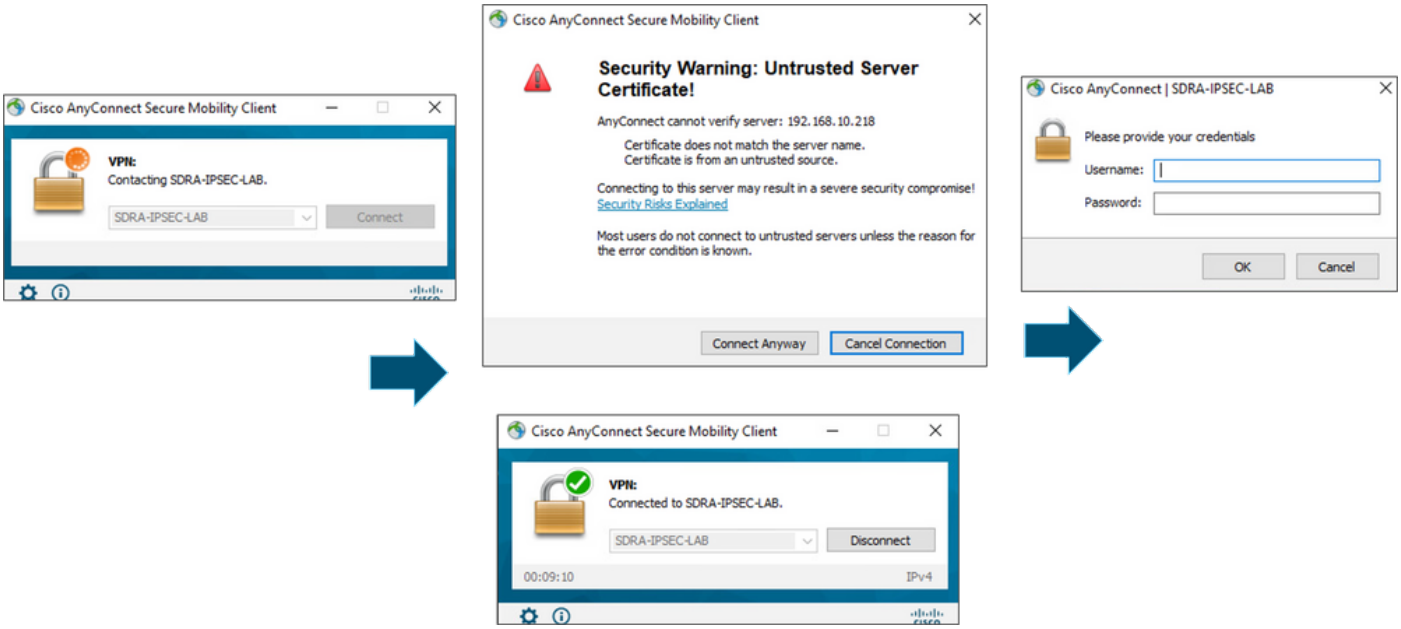
导航至**设置> 首选项**，并取消选中所有框选项。

对于此方案，最重要的是“**阻止到不受信任的服**务器的连接”。

> **注意：**用于RA头端/cEdge身份验证的证书是之前由Cisco IOS® XE中的CA服务器创建和签名的证书。因为此CA服务器不是GoDaddy、Symantec、Cisco等公共实体。PC客户端将证书解释为不受信任的服务器。这是使用您的公司信任的公共证书或CA服务器修复的。

使用AnyConnect客户端

一旦所有SDRA配置都被放置，成功连接的流将显示为图像。



验证

虚拟模板接口用于创建虚拟访问接口以启动加密通道并在服务器(cEdge)和客户端（AnyConnect用户）之间建立IKEv2和IPsec安全关联(SA)。

> **注意**：虚拟模板接口始终**打开/关闭**。**状态**为**up**，协**议**为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
```

使用show derived-config interface virtual-access <number>检查应用于与客户端**关联的虚拟访问接口的实际配置**。

```
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
```

使用show crypto ipsec sa peer <AnyConnect Public IP >检查AnyConnect客户端的IPsec安全关联(SA)。

```
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….
```

检查会话、用户名和分配的IP的IKEv2 SA参数。

注意：分配的IP地址必须与AnyConnect客户端上的IP地址匹配。

```
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
```

相关信息

- 思科SD-WAN远程访问
- 配置FlexVPN服务器
- 下载AnyConnect
- 技术支持和文档 - Cisco Systems