

Configuración del acceso remoto SD-WAN (SDRA) con AnyConnect y el servidor ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[¿Qué es una VPN de acceso remoto?](#)

[¿Qué es la VPN de acceso remoto SD-WAN?](#)

[Tunelización dividida vs Túnel todo](#)

[Antes de SDRA y después de SDRA](#)

[¿Qué es FlexVPN?](#)

[Configuración de Prerrequisitos](#)

[Configuración de ISE](#)

[Tunelización dividida vs Túnel todo en AnyConnect Client](#)

[Configuración del servidor de la CA en Cisco IOS® XE](#)

[Configuración de SD-WAN RA](#)

[Configuración de PKI de Crypto](#)

[Configuración AAA](#)

[Configuración de FlexVPN](#)

[Ejemplo de Configuración de SD-WAN RA](#)

[Configuración del cliente AnyConnect](#)

[Configurar el Editor de perfiles de AnyConnect](#)

[Instalación del perfil de AnyConnect \(XML\)](#)

[Desactivar el descargador de AnyConnect](#)

[Desbloquear servidores no fiables en el cliente AnyConnect](#)

[Utilizar cliente AnyConnect](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el acceso remoto SD-WAN (SDRA) con AnyConnect Client utilizando un modo autónomo Cisco IOS® XE como servidor CA y un servidor Cisco Identity Services Engine (ISE) para la autenticación, autorización y contabilidad.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa (SD-WAN) definida por software de Cisco
- Public Key Infrastructure (PKI)
- FlexVPN
- servidor RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8000V versión 17.07.01a
- vManage versión 20.7.1
- CSR1000V versión 17.03.04.a
- ISE versión 2.7.0.256
- AnyConnect Secure Mobility Client versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

¿Qué es una VPN de acceso remoto?

La VPN de acceso remoto permite al usuario remoto conectarse de forma segura a las redes de la empresa, utilizar aplicaciones y datos a los que sólo se puede acceder a través de los dispositivos conectados en la oficina.

Una VPN de acceso remoto funciona mediante un túnel virtual creado entre el dispositivo de un empleado y la red de la empresa.

Este túnel pasa a través de la Internet pública, pero los datos enviados a través de ella están protegidos por protocolos de encriptación y seguridad para mantenerla privada y segura.

Los dos componentes principales de este tipo de VPN son un servidor de acceso a la red/cabecera RA y software de cliente VPN.

¿Qué es la VPN de acceso remoto SD-WAN?

El acceso remoto se ha integrado en la solución SD-WAN que elimina la necesidad de una infraestructura Cisco SD-WAN y RA independiente y permite una rápida escalabilidad de los servicios RA con el uso de Cisco AnyConnect como cliente de software RA.

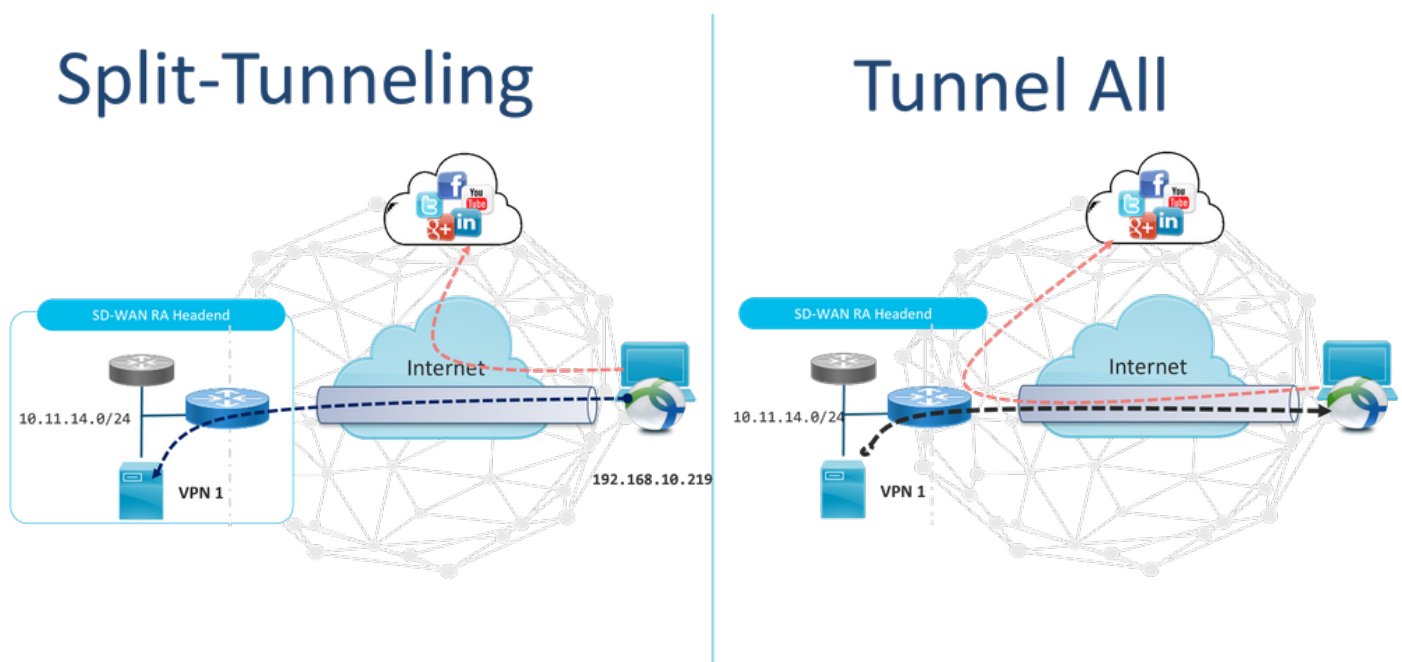
El acceso remoto proporciona a los usuarios remotos acceso a la red de la organización. Esto habilita el trabajo desde el hogar.

Las ventajas

- RA proporciona acceso a la red de una organización desde dispositivos/usuarios en ubicaciones remotas. (HO)
- Amplía la solución Cisco SD-WAN a los usuarios de RA sin el requisito de que cada dispositivo de usuario de RA forme parte del fabric Cisco SD-WAN.
- Seguridad de los datos
- Tunelización dividida o túnel completo
- Escalabilidad
- Capacidad de distribuir la carga RA en numerosos dispositivos SD-WAN Cisco IOS® XE en el fabric de Cisco SD-WAN.

Tunelización dividida vs Túnel todo

La tunelización dividida se utiliza en escenarios donde sólo se debe tunelizar tráfico específico (subredes SD-WAN, por ejemplo), como se muestra en la imagen.

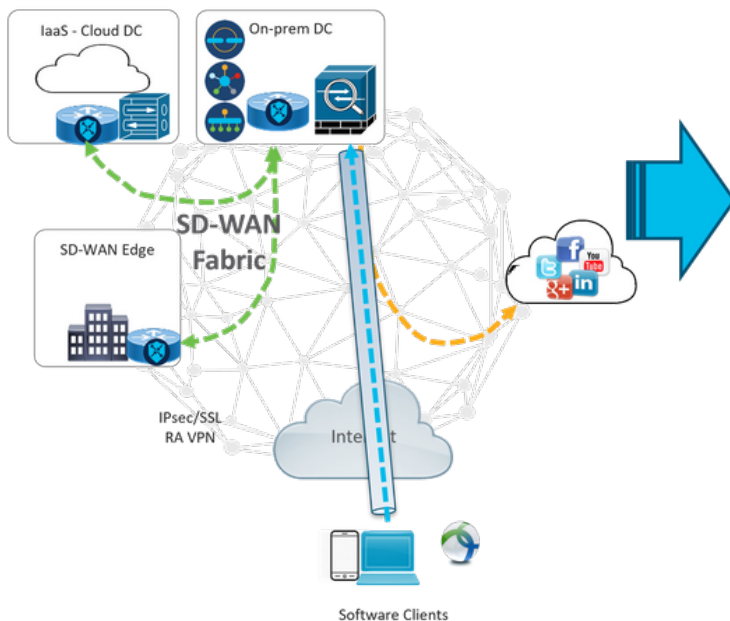


Antes de SDR y después de SDR

El diseño de VPN de acceso remoto tradicional requiere una infraestructura de RA independiente fuera del fabric de Cisco SD-WAN para proporcionar acceso de usuario remoto a la red, como dispositivos que no son SD-WAN, como ASA, Cisco IOS® XE normal o dispositivos de terceros, y el tráfico RA se desplaza hacia el dispositivo SD-WAN, como se muestra en la imagen.

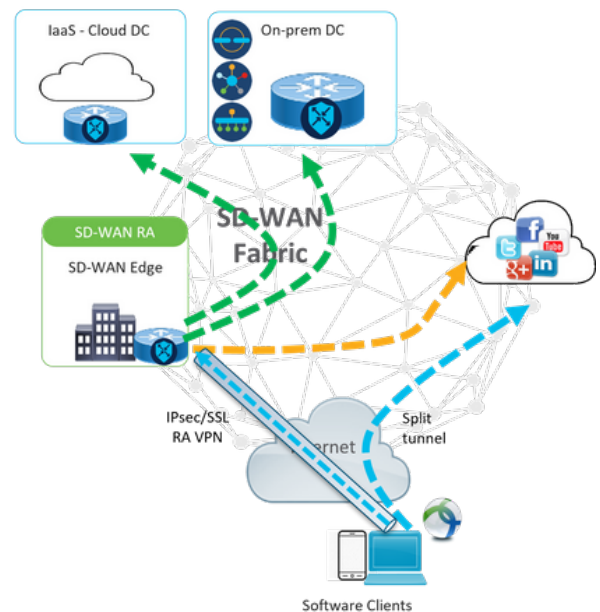
Before SDRA

Traditional Remote-Access VPN design with SDWAN



After SDRA

SD-WAN Remote-Access



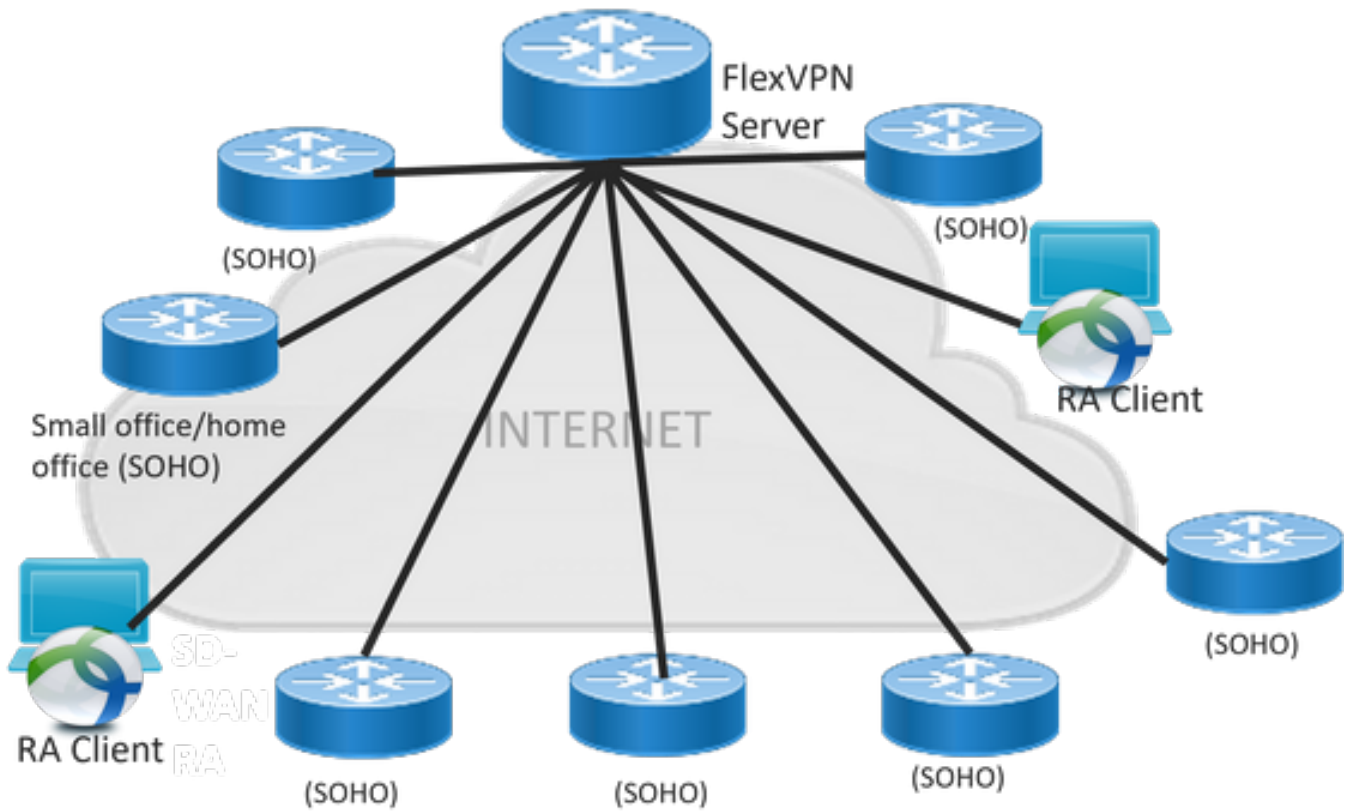
El acceso remoto SD-WAN cambia la forma en que los usuarios remotos se conectan a la red. Se conectan directamente al extremo c que se utiliza como cabecera RA. Amplía las funciones y ventajas de Cisco SD-WAN a los usuarios de RA. Los usuarios RA se convierten en usuarios de la sucursal en el lado de la LAN.

Para cada cliente RA, el centro distribuidor de RA SD-WAN asigna una dirección IP a un cliente RA y agrega una ruta de host estática a la dirección IP asignada en el VRF de servicio en el que se coloca al usuario RA.

La ruta estática especifica el túnel VPN de la conexión del cliente RA. El centro de cabecera SD-WAN RA anuncia la IP estática dentro del VRF de servicio del cliente RA con el uso de OMP a todos los dispositivos periféricos en la VPN de servicio.

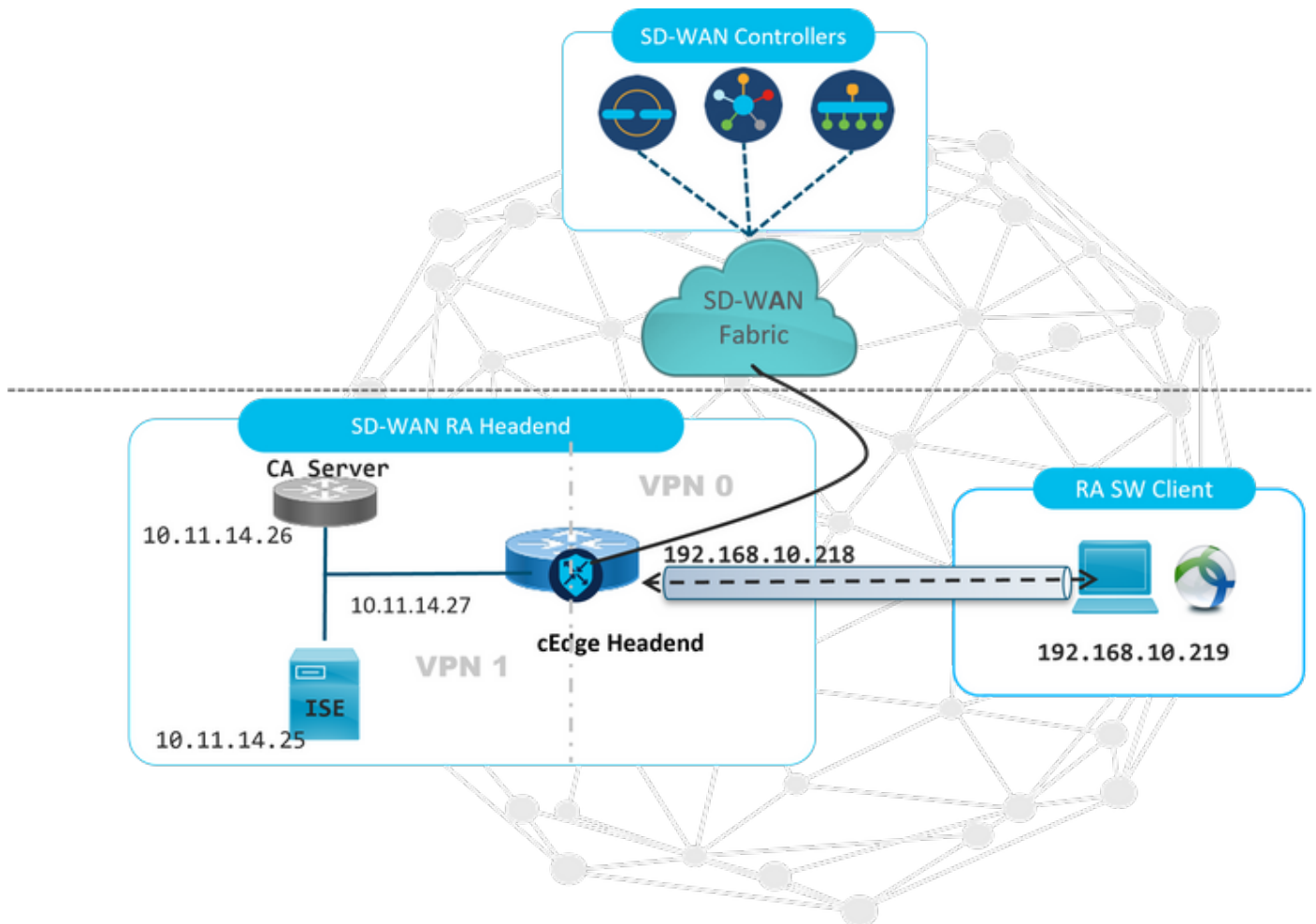
¿Qué es FlexVPN?

SD-WAN RA aprovecha la solución Cisco FlexVPN RA. FlexVPN es la implementación de Cisco de la función estándar IKEv2, un paradigma unificado y CLI que combina sitio a sitio, **acceso remoto**, topologías radiales y radiales, y mallas parciales (spoke to spoke direct). FlexVPN ofrece un marco sencillo pero modular que utiliza ampliamente el paradigma de la interfaz de túnel mientras sigue siendo compatible con las implementaciones de VPN heredadas.



Configuración de Prerrequisitos

Para este ejemplo, se ha creado una configuración de laboratorio de RA de SD-WAN como se muestra en la imagen.



Se han configurado componentes adicionales para este escenario de laboratorio de SD-WAN:

- Un Cisco IOS® XE regular en modo autónomo como servidor CA.
- Servidor ISE/Radius para Autenticación, Autorización y Contabilización.
- PC con Windows que puede acceder al extremo c a través de la interfaz WAN.
- AnyConnect Client ya está instalado.

Nota: Los servidores CA y RADIUS se han colocado en el servicio VRF 1. Ambos servidores deben ser accesibles a través del VRF de servicio para todos los cabeceros de RA SD-WAN.

Nota: El acceso remoto SD-WAN de Cisco es compatible con la versión 17.7.1a y con dispositivos específicos para SDRA. Para obtener información sobre los dispositivos compatibles, vaya a: [Plataformas compatibles con la cabecera SD-WAN RA](#)

Configuración de ISE

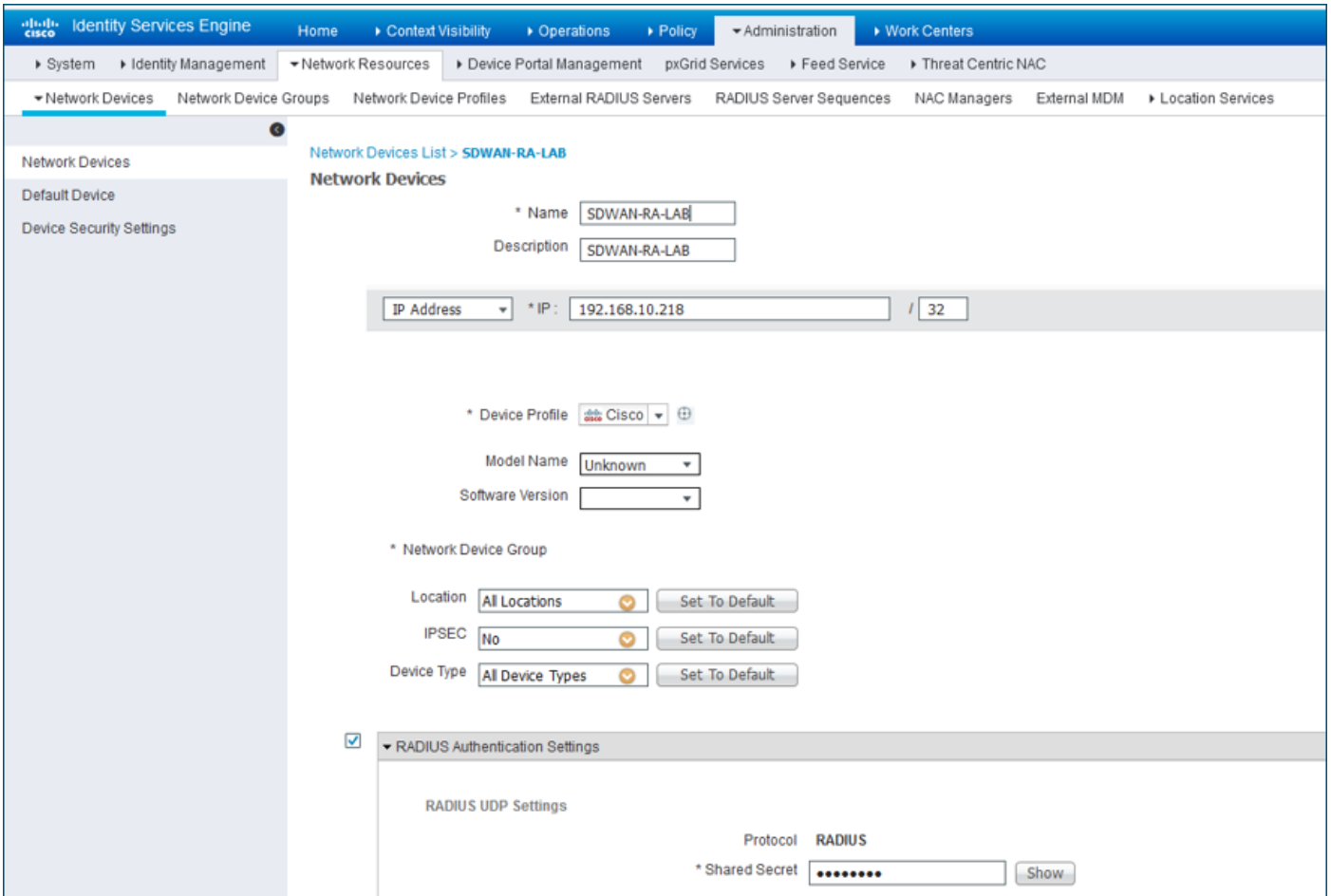
Para admitir el encabezado de RA SD-WAN, asegúrese de que los parámetros estén configurados en el servidor RADIUS. Estos parámetros son obligatorios para las conexiones RA:

- Credenciales de autenticación de usuario Nombre de usuario y contraseña para las conexiones AnyConnect-EAP
- Parámetros de política (atributos) que se aplican a un usuario o a un grupo de usuarios **VRF**:

VPN de servicio a la que está asignado el usuario **RANombre del conjunto IP**: Nombre del conjunto IP definido en la cabecera **RASubredes de servidor**: Acceso a subred para proporcionar al usuario de RA

El primer paso para configurar en el ISE es la cabecera RA o la dirección IP del extremo c como dispositivo de red para poder realizar solicitudes Radius al ISE.

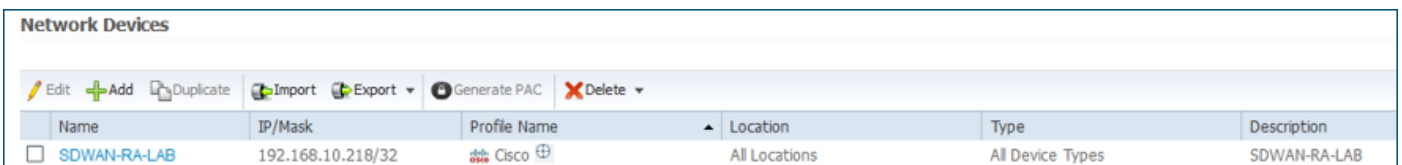
Vaya a **Administration > Network Devices** y agregue la dirección IP y la contraseña con encabezado RA (cEdge), como se muestra en la imagen.



The screenshot shows the configuration page for a Network Device in the Cisco Identity Services Engine (ISE) interface. The page is titled "Network Devices List > SDWAN-RA-LAB". The configuration fields are as follows:

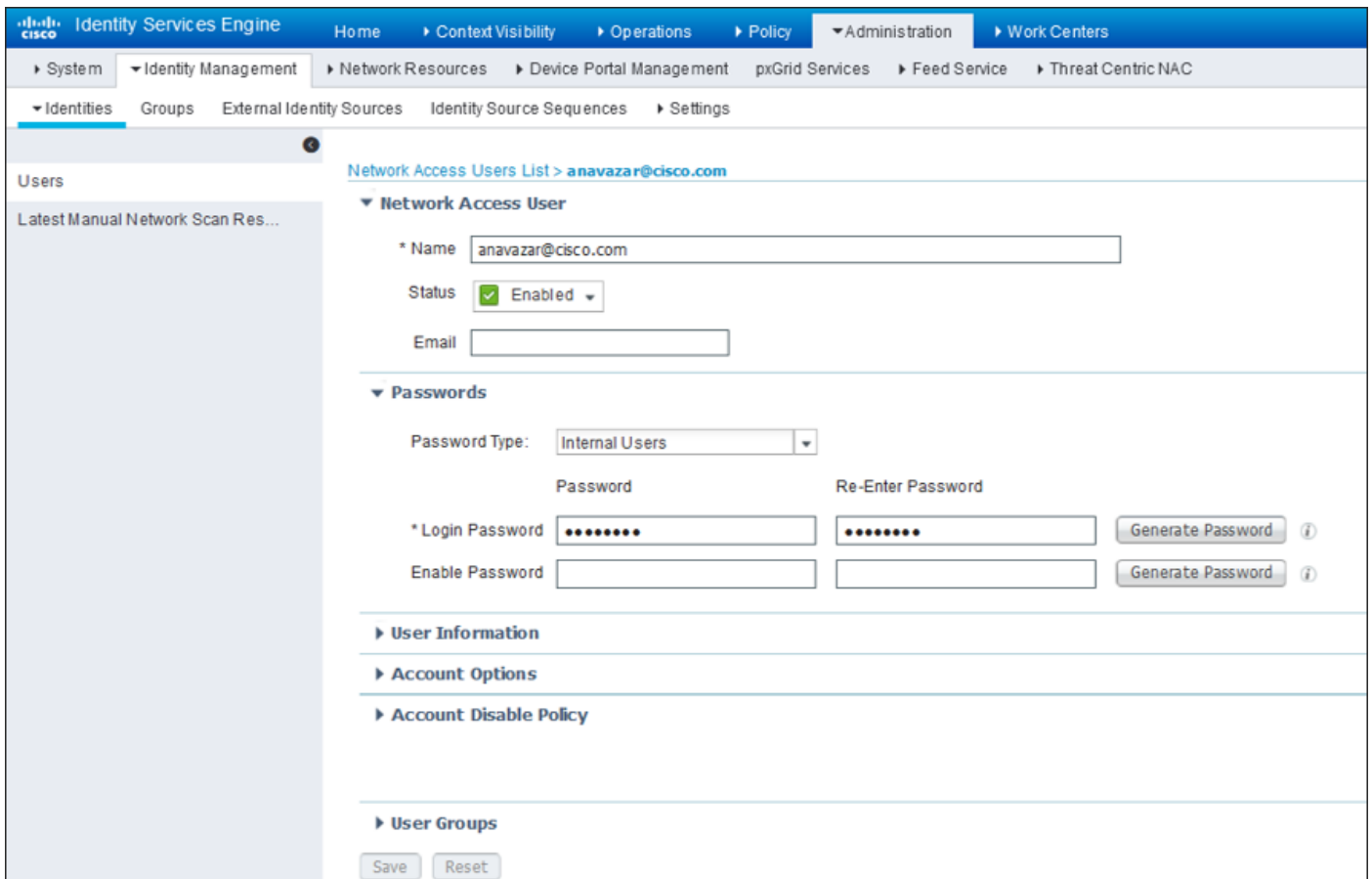
- Name: SDWAN-RA-LAB
- Description: SDWAN-RA-LAB
- IP Address: 192.168.10.218 / 32
- Device Profile: Cisco
- Model Name: Unknown
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations
- IPSEC: No
- Device Type: All Device Types
- RADIUS Authentication Settings: RADIUS Authentication Settings
 - RADIUS UDP Settings
 - Protocol: RADIUS
 - * Shared Secret: (masked)

Dispositivo de red agregado como se muestra en la imagen.

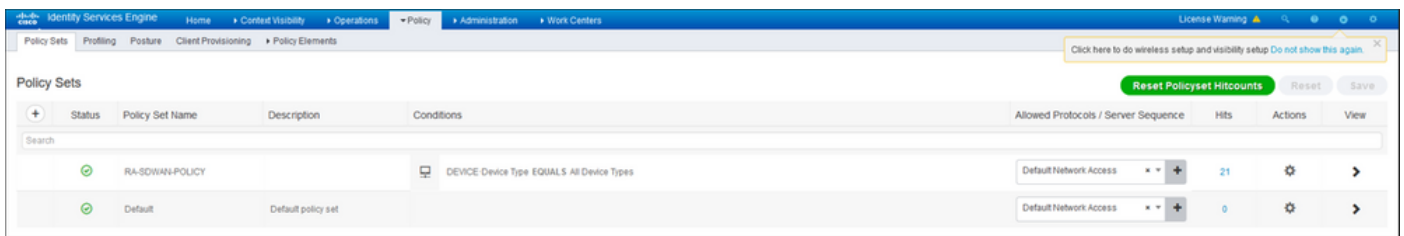


Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> SDWAN-RA-LAB	192.168.10.218/32	Cisco	All Locations	All Device Types	SDWAN-RA-LAB

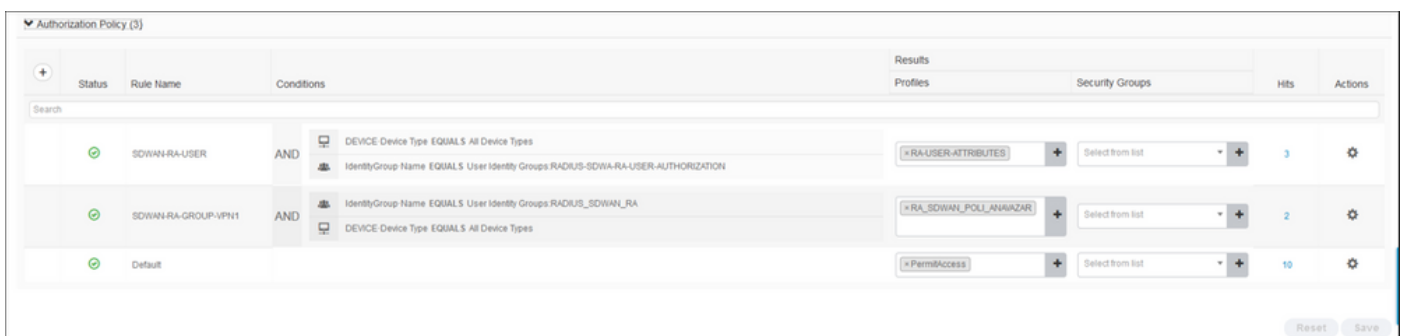
En el servidor RADIUS se necesita configurar los nombres de usuario y la contraseña para la autenticación de AnyConnect como se muestra en la imagen. Vaya a **Administración > Identidades**.



Se debe crear un conjunto de políticas con la condición de coincidencia para que se produzca como se muestra en la imagen. En este caso, se utiliza la condición **Todos los tipos de dispositivo**, lo que significa que todos los usuarios acceden a esta política.



A continuación, se ha creado una política de autorización por condición. La condición **Todos los tipos de dispositivo** y los grupos de identidad que deben coincidir.

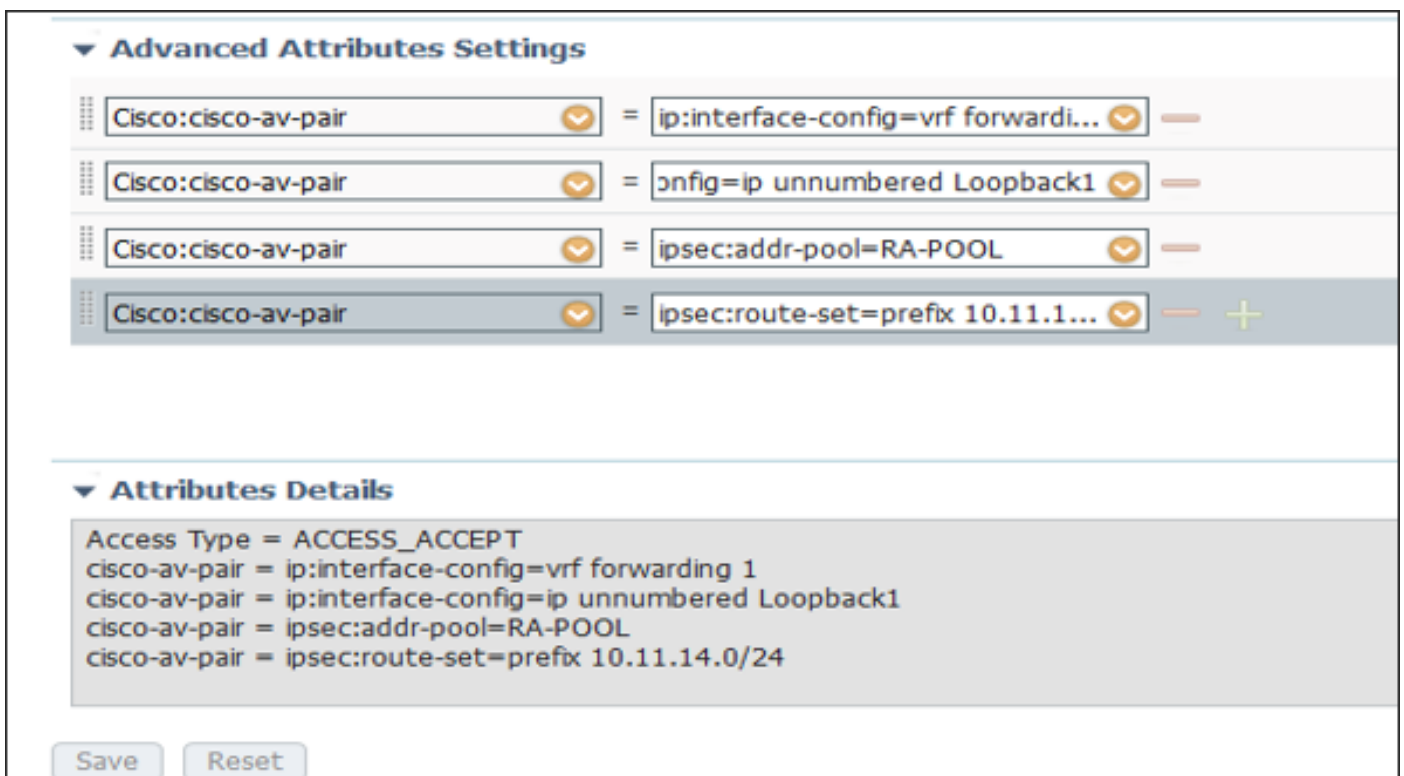
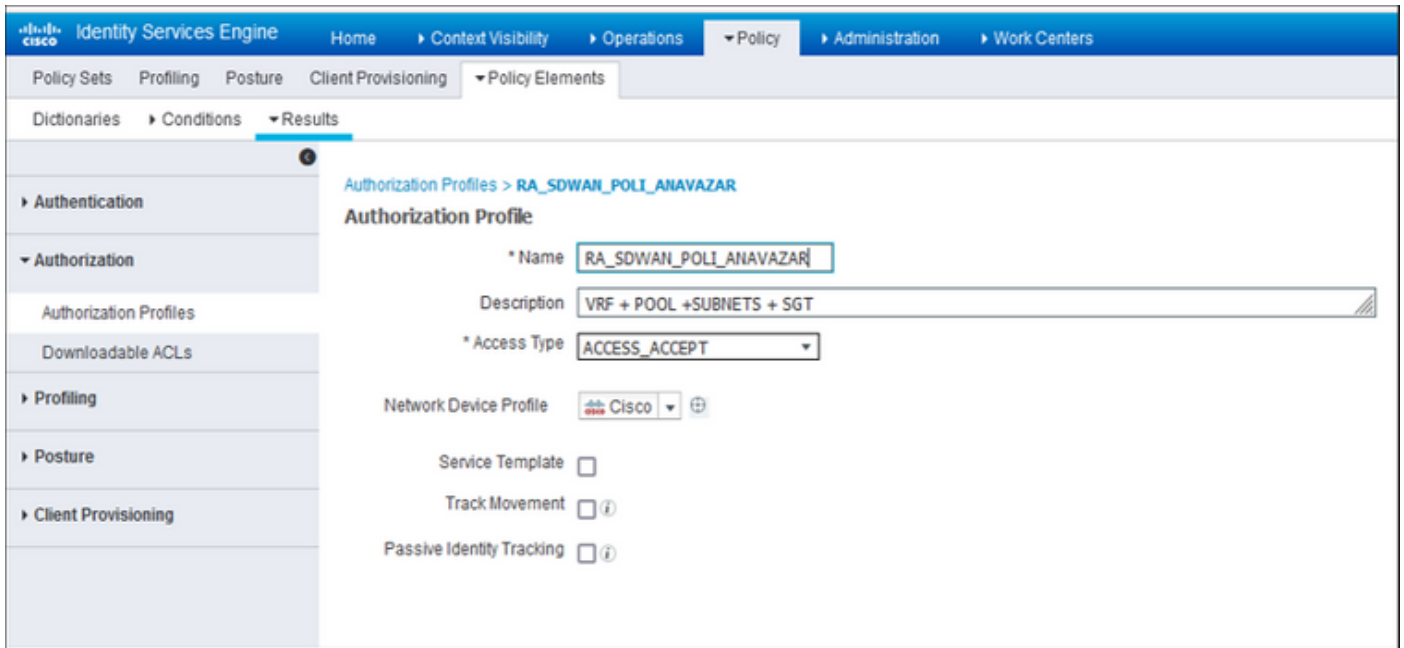


En el **perfil de autorización**, necesitamos configurar el **tipo de acceso** como **Access_ACCEPT** en la **configuración de atributos avanzados**, seleccionar el proveedor de Cisco y el atributo de par Cisco-AV.

Es necesario configurar algunos parámetros de política para los usuarios:

- VRF, el VRF de servicio al que pertenece el usuario.
- El nombre del conjunto IP, cada conexión de usuario, tiene asignada una dirección IP que pertenece al conjunto IP configurado en los Bordes.
- las subredes a las que el usuario puede acceder

Precaución: El comando **IP vrf forwarding** debe aparecer antes del comando **IP unnumbered**. Si la interfaz de acceso virtual se clona de la plantilla virtual y se aplica el comando **IP vrf forwarding**, cualquier configuración IP se elimina de la interfaz de acceso virtual.



Atributos de usuario:

Access Type = ACCESS_ACCEPT

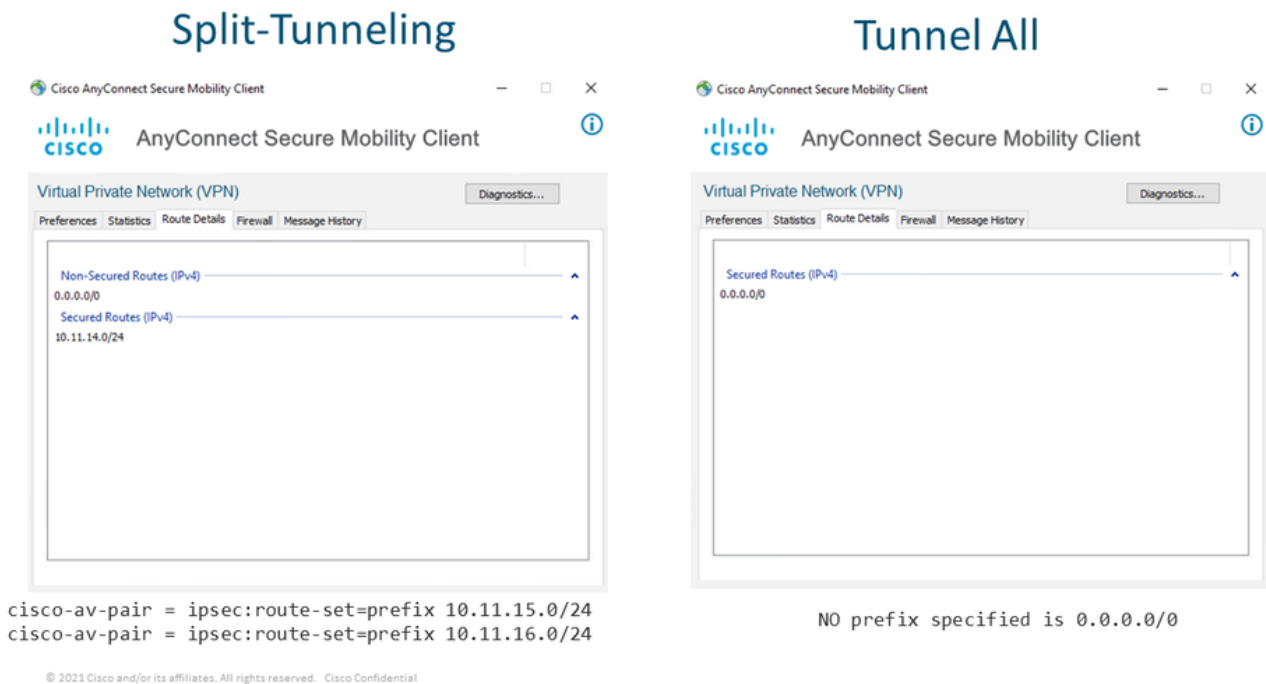
```

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

```

Tunelización dividida vs Túnel todo en AnyConnect Client

`ipsec:route-set=el` atributo `prefix` recibido en AnyConnect Client se instala como se muestra en la imagen.



Configuración del servidor de la CA en Cisco IOS® XE

El servidor de la CA suministra certificados a los dispositivos SD-WAN del IOS® XE de Cisco y permite que la cabecera RA se autentique a los clientes RA.

El CEDGE no puede ser un servidor de la CA, ya que estos comandos de servidor de PKI crypto no se soportan en la SD-WAN de Cisco IOS® XE.

- Generar un par de llaves RSA
- Cree el punto de confianza PKI para el servidor CA Configure el par de tramas con el KEY-CA generado anteriormente.

Nota: El servidor PKI y el punto de confianza PKI deben utilizar el mismo nombre.

- Crear el servidor CA Configure el nombre del emisor para el servidor de la CAActive el servidor de la CA mediante "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  
!
```

Verifique si el servidor de la CA está habilitado.

```
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
```

Verifique si el certificado del servidor de la CA está instalado.

```
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
```

La huella digital SHA 1 del certificado CA se utiliza en el trustpoint crypto pki en el router cEdge (cabecera RA) con la configuración de acceso remoto.

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

Configuración de SD-WAN RA

Nota: Este documento no cubre el proceso de incorporación de SD-WAN para controladores y cEdge. Se supone que el fabric de SD-WAN está activo y completamente funcional.

Configuración de PKI de Crypto

- Cree un punto de confianza PKI.
- Configure la URL para el servidor de la CA.
- Copie la huella digital sha 1 del certificado del servidor de la CA.
- Configure el nombre del asunto y el nombre alternativo para el nuevo certificado de identidad.
- Configure el teclado con el ID de CLAVE generado anteriormente.

```
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
```

Solicite el certificado de CA para la autenticación:

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

Genera el CSR, envía al servidor de la CA y recibe el nuevo certificado de identidad:

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

Verifique el certificado CA y el certificado cEdge:

```
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

Configuración AAA

```
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
```

Configuración de FlexVPN

Configurar conjunto IP

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

Configuración de propuestas IKEv2 (Cifrados y parámetros) y política:

```
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 un identificador de nombre de perfil IKEv2:

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

Nota: El **administrador de nombres** deriva el nombre del prefijo en la identidad EAP (nombre de usuario) que se delimita en la identidad EAP que separa el prefijo y el sufijo.

Configuración de cifrados IPsec:

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

Configuración del perfil Crypto IKEv2:

```
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
```

Configuración del perfil IPSEC de Crypto:

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

Configuración de la Interfaz de Plantilla Virtual:

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

Configure la plantilla virtual en el perfil Crypto IKEv2:

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

Ejemplo de Configuración de SD-WAN RA

```
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
```

```

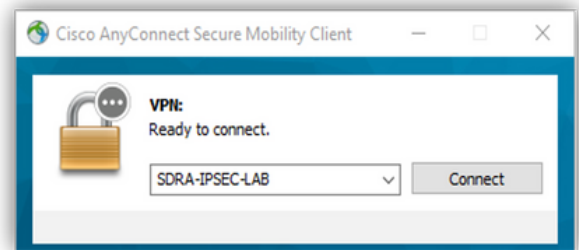
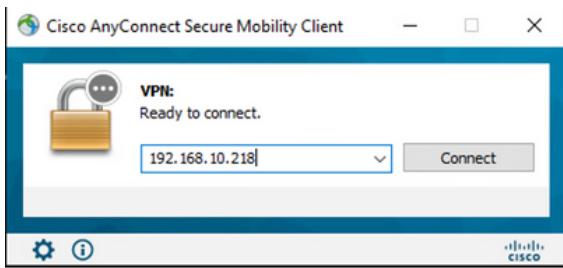
subject-name CN=cEdge-SDWAN-1.crv
enrollment url http://10.11.14.226:80
fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
subject-name CN=cEdge-SDWAN-1.crv
vrf 1
rsakeypair KEY-NEW
revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap 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

```

Configuración del cliente AnyConnect

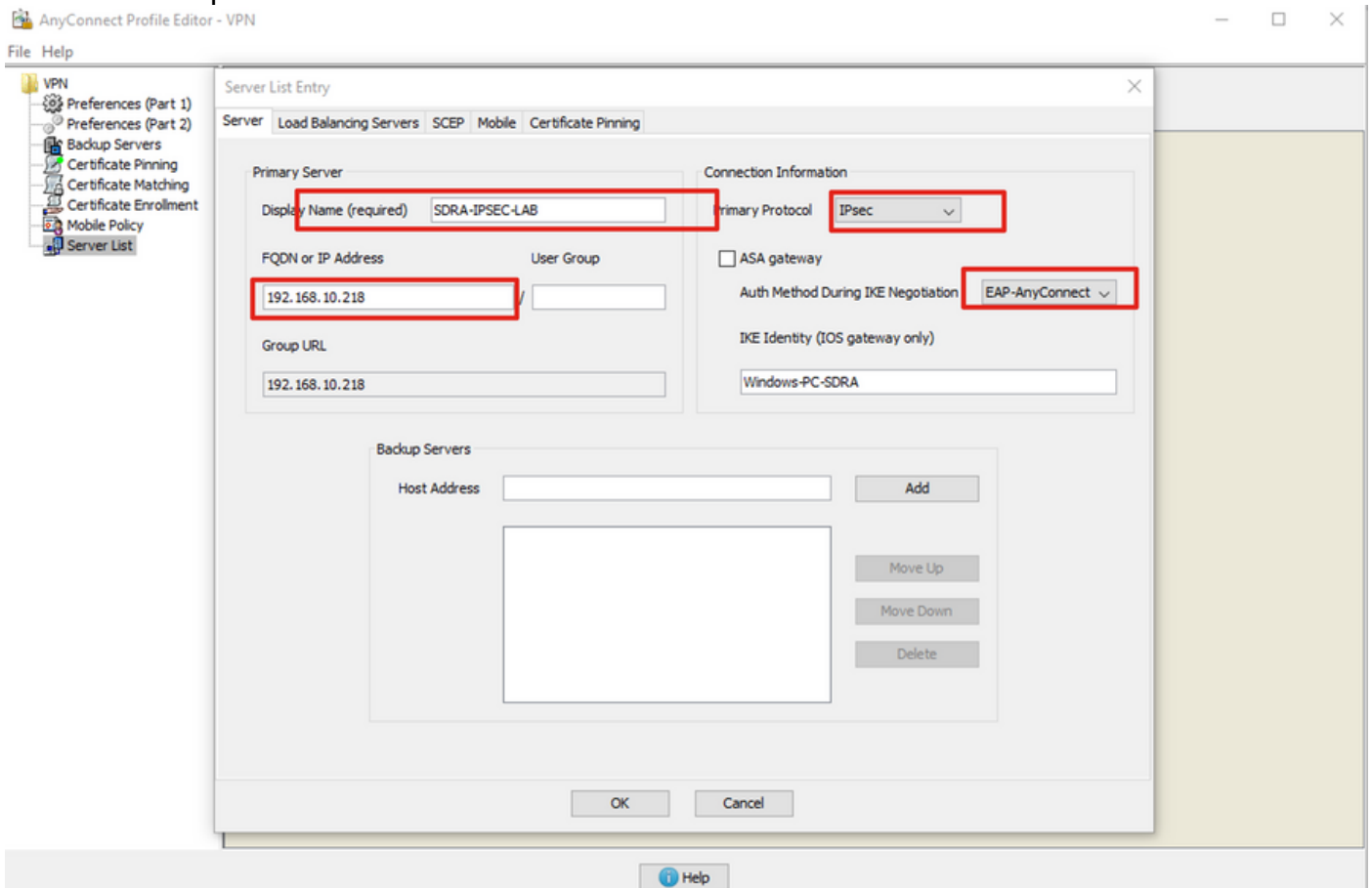
AnyConnect Client utiliza SSL como protocolo predeterminado para el establecimiento del túnel y este protocolo no es compatible con SD-WAN RA (hoja de ruta). RA utiliza FlexVPN, por lo que IPSEC es el protocolo utilizado y es obligatorio cambiarlo y esto se hace a través del perfil XML.

El usuario puede introducir manualmente el FQDN del gateway VPN en la barra de direcciones del cliente AnyConnect. Esto da como resultado la conexión SSL al gateway.



Configurar el Editor de perfiles de AnyConnect

- Navegue hasta **Lista de servidores** y haga clic en **Agregar**.
- Seleccione **IPsec** como "Protocolo principal".
- Desmarque la opción **ASA gateway**.
- Seleccione **EAP-AnyConnect** como "Método de autenticación durante la negociación IKE".
- **Display/Name (Required)** es el nombre utilizado para guardar esta conexión en el cliente AnyConnect.
- El **FQDN** o la dirección IP se deben archivar con la dirección IP cEdge (pública).
- Guarde el perfil.



Instalación del perfil de AnyConnect (XML)

El perfil XML se puede colocar manualmente en el directorio:

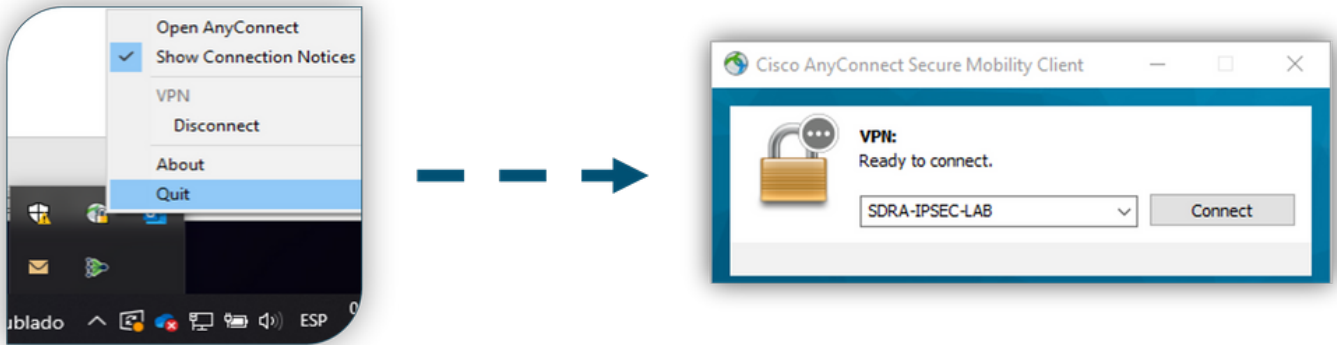
For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/profile

El cliente AnyConnect debe reiniciarse para que el perfil sea visible en la GUI. El proceso se puede reiniciar haciendo clic con el botón derecho del ratón en el icono de AnyConnect en la bandeja de Windows y seleccionando la opción **Salir**:



Desactivar el descargador de AnyConnect

El cliente AnyConnect intenta descargar el perfil XML después de iniciar sesión correctamente de forma predeterminada.

Si el perfil no está disponible, la conexión falla. Como solución alternativa, es posible inhabilitar la capacidad de descarga del perfil de AnyConnect en el propio cliente.

Para Windows:

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

Para MAC OS:

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

La opción "BypassDownloader" se establece en "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>
```

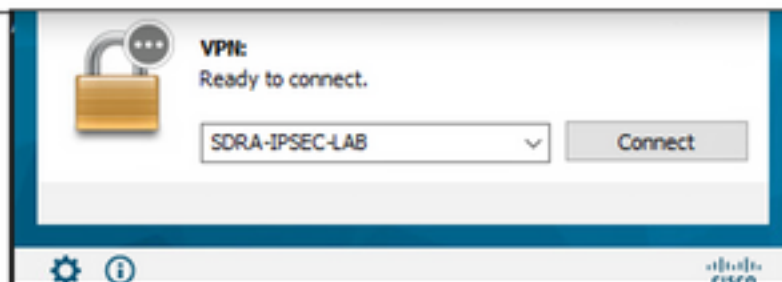
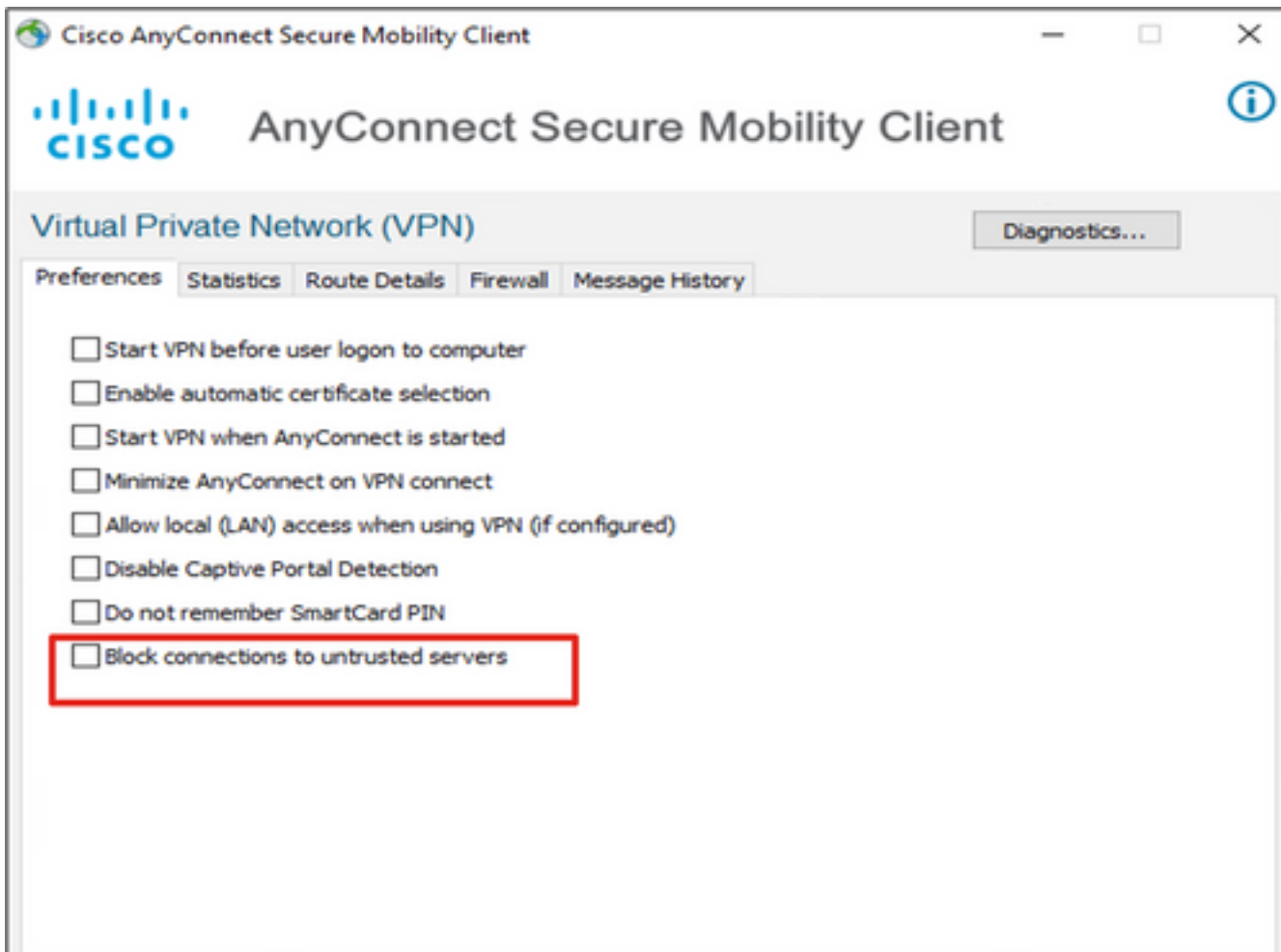
```
<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
<RestrictWebLaunch>>false</RestrictWebLaunch>
<StrictCertificateTrust>>false</StrictCertificateTrust>
<UpdatePolicy>
<AllowComplianceModuleUpdatesFromAnyServer>>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>>true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

Desbloquear servidores no fiables en el cliente AnyConnect

Navegue hasta **Settings > Preferences** y desmarque todas las opciones de la casilla.

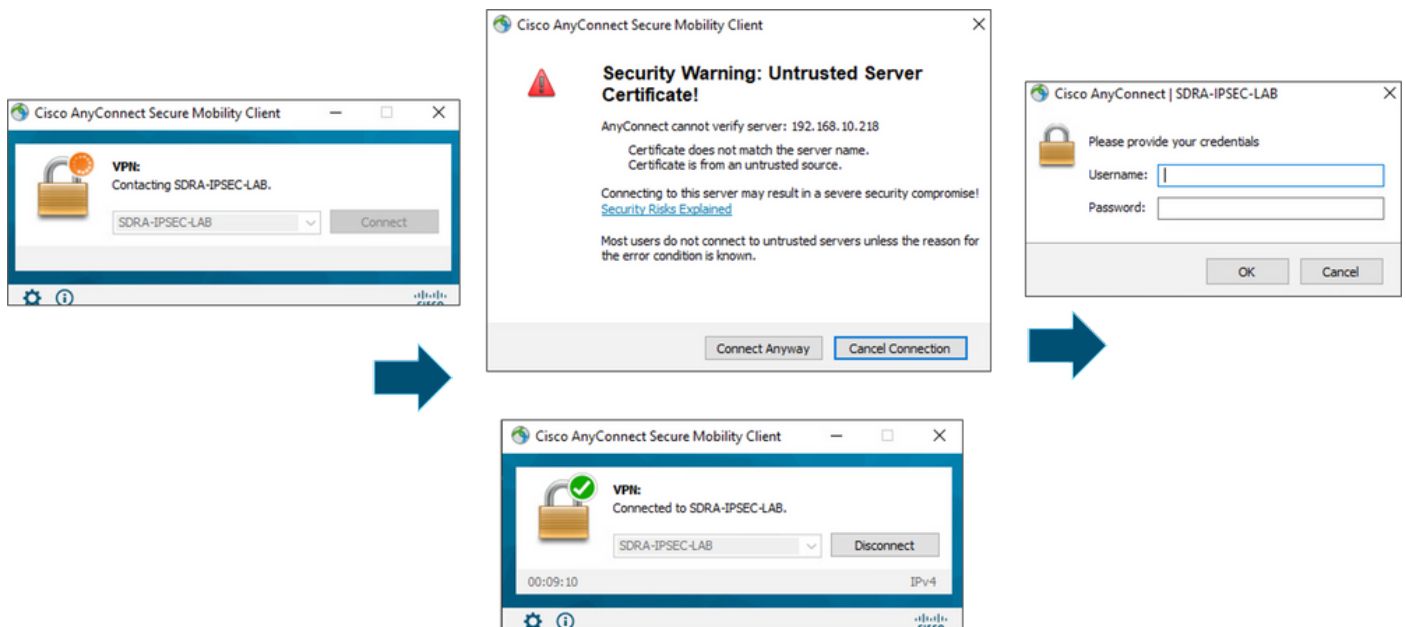
Lo más importante es el **"Block Connections to untrustservers"** (Bloquear conexiones a servidores no confiables) para este escenario.

Nota: El certificado utilizado para la autenticación de cabecera/extremo de extremo de la red RA es el creado y firmado previamente por el servidor de la CA en Cisco IOS® XE. Como este servidor de la CA no es una entidad pública como GoDaddy, Symantec, Cisco, etc. El cliente PC interpreta el certificado como un servidor no confiable. Se corrige mediante un certificado público o un servidor de la CA en el que confía su empresa.



Utilizar cliente AnyConnect

Una vez realizada toda la configuración de SDRA, el flujo para una conexión exitosa se muestra como la imagen.



Verificación

La interfaz de plantilla virtual se utiliza para crear la interfaz de acceso virtual para iniciar un canal criptográfico y establecer asociaciones de seguridad (SA) IKEv2 e IPsec entre el servidor (cEdge) y el cliente (usuario de AnyConnect).

Nota: La interfaz de plantilla virtual siempre está activa/inactiva. El estado está activo y el protocolo está inactivo.

```
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
```

Verifique la configuración real aplicada para la interfaz de Virtual-Access asociada con el cliente con **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
```

Verifique las asociaciones de seguridad IPsec (SAs) para el cliente AnyConnect con el comando **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...
```

Verifique los parámetros SA IKEv2 para la sesión, el nombre de usuario y la IP asignada.

Nota: La dirección IP asignada debe coincidir con la dirección IP del lado de 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
```

Información Relacionada

- [Acceso remoto SD-WAN de Cisco](#)
- [Configuración del servidor FlexVPN](#)
- [Descargar AnyConnect](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)