Configurar o acesso remoto SD-WAN (SDRA) com o AnyConnect e o servidor ISE

Contents

Introduction

Este documento descreve como configurar o SDRA (SD-WAN Remote Access) com o AnyConnect Client usando um modo autônomo Cisco IOS® XE como um servidor CA e um servidor Cisco Identity Services Engine (ISE) para a Autenticação, Autorização e Contabilidade.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância (SD-WAN) definida por software da Cisco
- Public Key Infrastructure (PKI)
- FlexVPN
- servidor RADIUS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C8000V versão 17.07.01a
- vManage versão 20.7.1
- CSR1000V versão 17.03.04.a
- ISE versão 2.7.0.256
- AnyConnect Secure Mobility Client versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O que é uma VPN de acesso remoto?

A VPN de acesso remoto permite que o usuário remoto se conecte com segurança às redes da empresa, use aplicativos e dados que só podem ser acessados por meio dos dispositivos conectados no escritório.

Uma VPN de acesso remoto funciona por um túnel virtual criado entre o dispositivo de um funcionário e a rede da empresa.

Esse túnel passa pela internet pública, mas os dados enviados através dela são protegidos por protocolos de criptografia e segurança para ajudar a mantê-la privada e segura.

Os dois componentes principais nesse tipo de VPN são um headend de servidor de acesso à rede/RA e software de cliente VPN.

O que é VPN de acesso remoto SD-WAN?

O acesso remoto foi integrado à solução SD-WAN que elimina a necessidade de infraestruturas separadas Cisco SD-WAN e RA e permite a rápida escalabilidade dos serviços de RA com o uso do Cisco AnyConnect como um cliente de software RA.

O acesso remoto fornece aos usuários remotos acesso à rede da organização. Isso habilita o trabalho em casa.

As vantagens

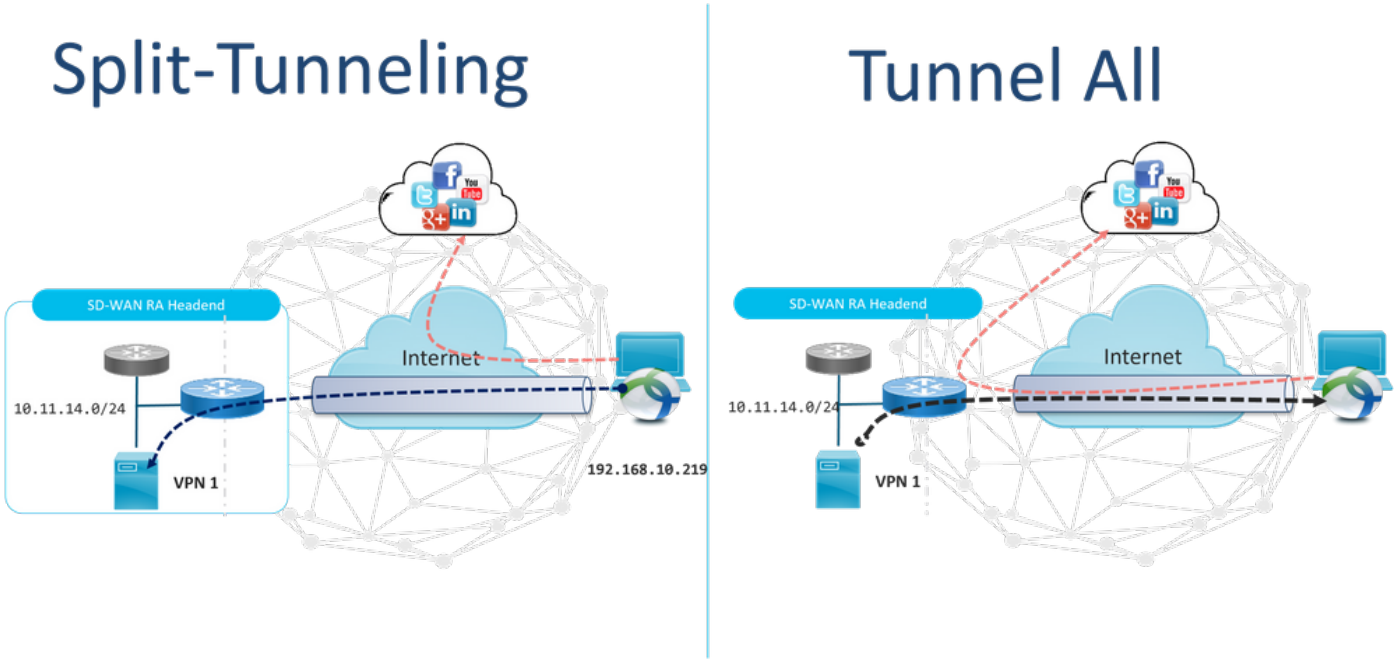
- O RA fornece acesso à rede de uma organização de dispositivos/usuários em locais remotos.

(HO)

- Estende a solução Cisco SD-WAN para usuários RA sem a necessidade do dispositivo de cada usuário RA fazer parte da estrutura Cisco SD-WAN.
- Segurança de dados
- Túnel dividido ou túnel todo
- Escalabilidade
- Capacidade de distribuir a carga do RA através de vários dispositivos Cisco IOS® XE SD-WAN na estrutura do Cisco SD-WAN.

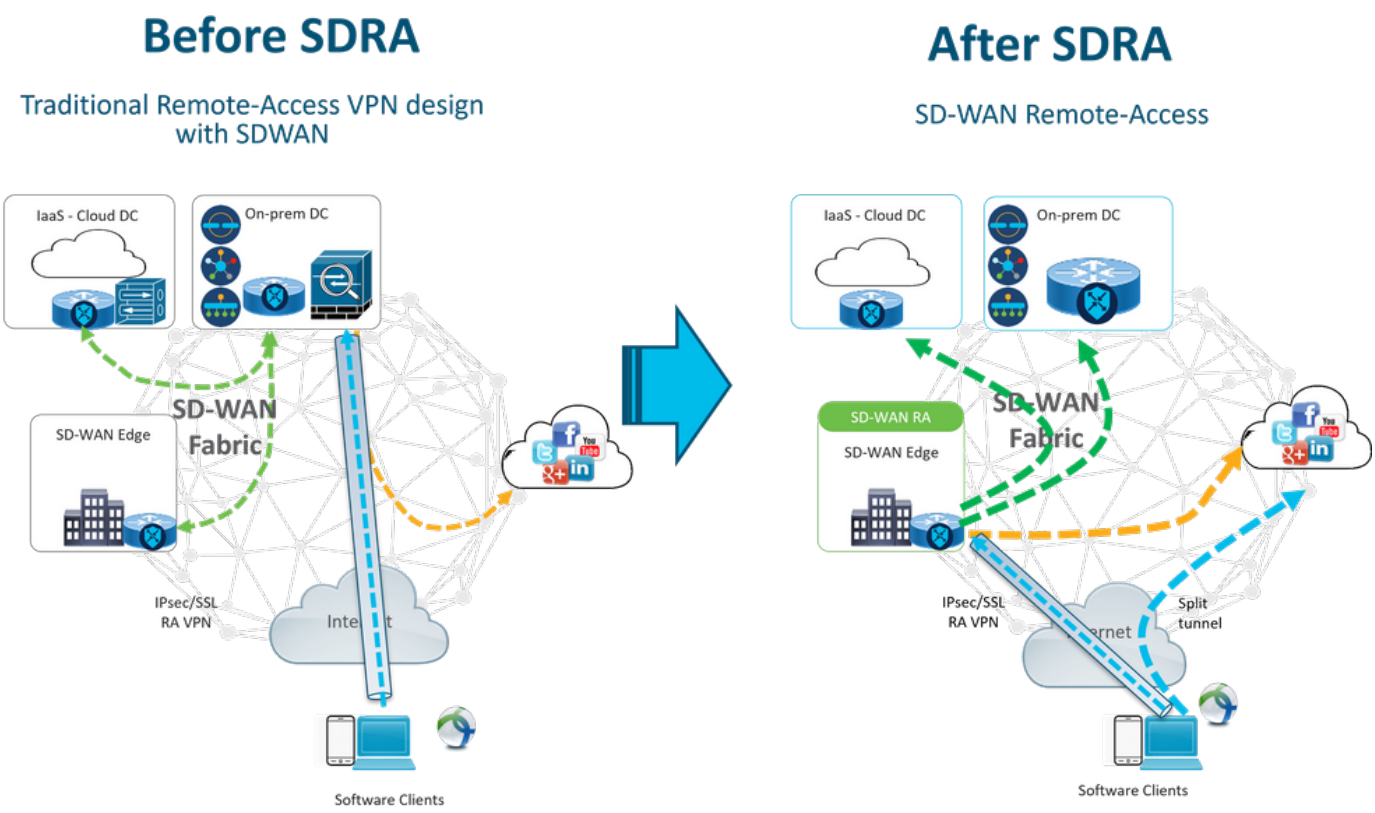
Dividir túnel versus túnel tudo

O tunelamento dividido é usado em cenários em que somente o tráfego específico deve ser encapsulado (sub-redes SD-WAN, por exemplo), como mostrado na imagem.



Antes da SDRA e após a SDRA

O design de VPN de acesso remoto tradicional requer uma infraestrutura de RA separada fora da estrutura do Cisco SD-WAN para fornecer acesso de usuário remoto à rede, como dispositivos que não são SD-WAN, como ASA, Cisco IOS® XE Regular ou dispositivos de terceiros, e o tráfego de RA é encaminhado para o dispositivo SD-WAN, como mostrado na imagem.



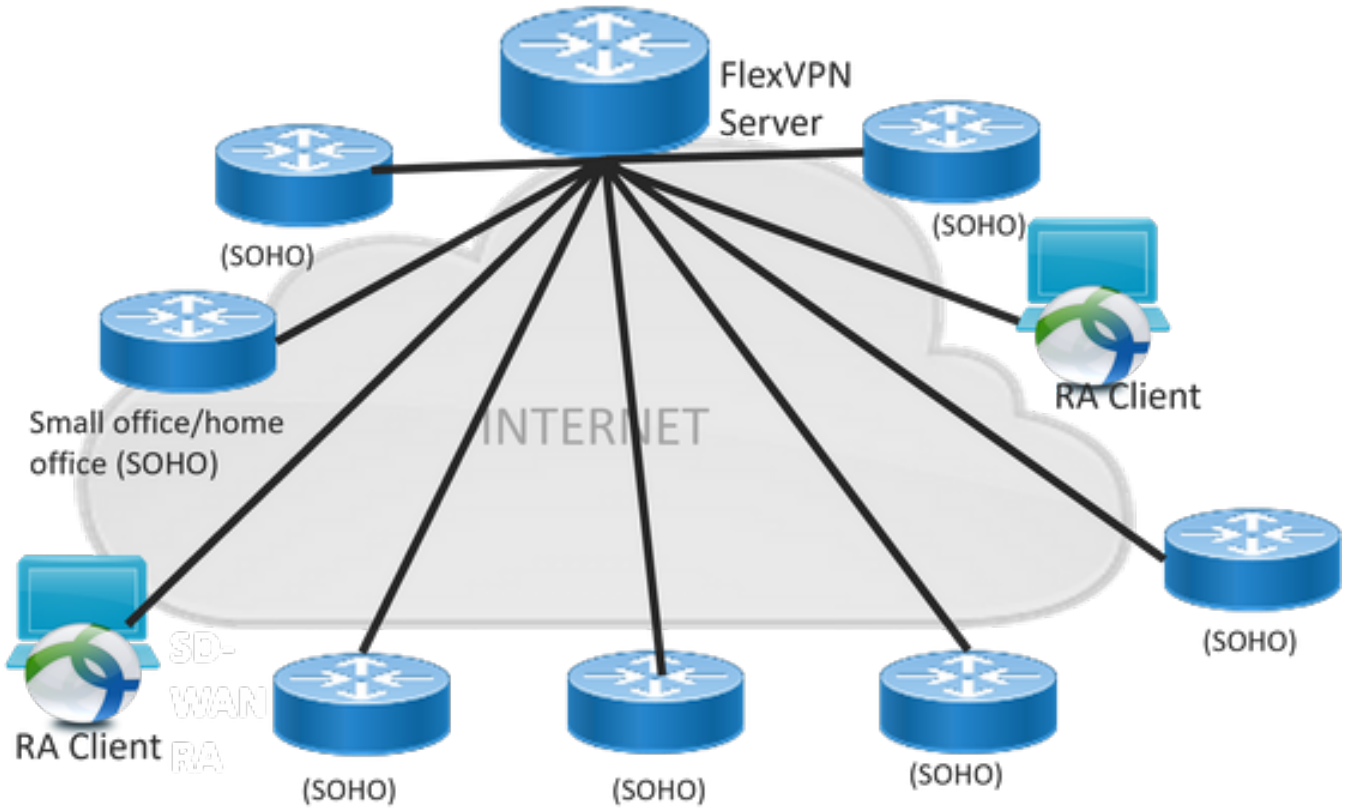
O SD-WAN Remote Access altera a forma como os usuários remotos se conectam à rede. Eles se conectam diretamente ao cEdge usado como headend de RA. Estende os recursos e benefícios do Cisco SD-WAN para usuários do RA. Os usuários de RA se tornam usuários da LAN da filial.

Para cada cliente RA, o headend SD-WAN RA atribui um endereço IP a um cliente RA e adiciona uma rota de host estática ao endereço IP atribuído no VRF de serviço no qual o usuário RA é colocado.

A rota estática especifica o túnel VPN da conexão do cliente RA. O headend SD-WAN RA anuncia o IP estático dentro do VRF de serviço do cliente RA com o uso do OMP para todos os dispositivos de borda na VPN de serviço.

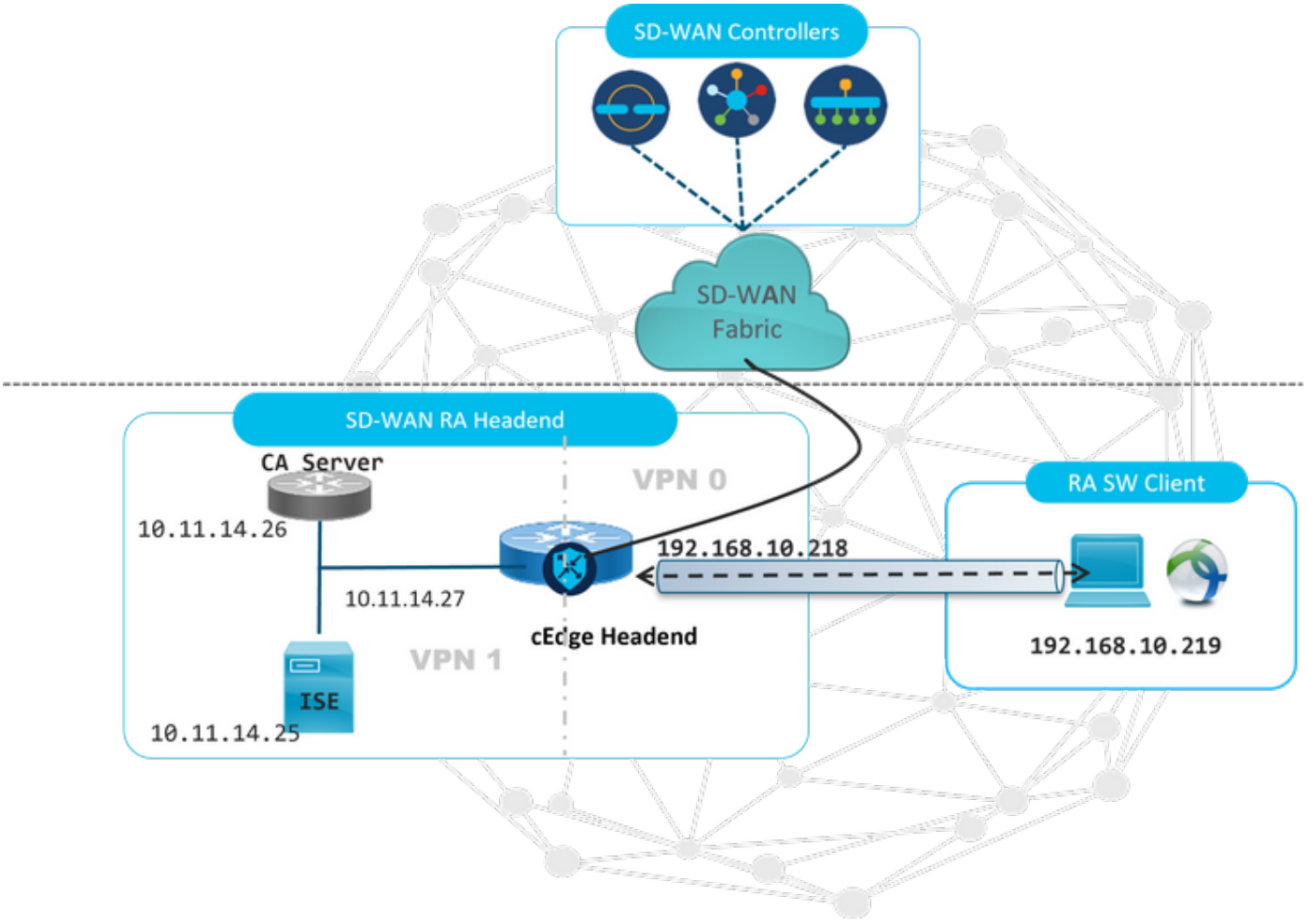
O que é FlexVPN?

O SD-WAN RA aproveita a solução Cisco FlexVPN RA. FlexVPN é a implementação da Cisco do recurso padrão IKEv2, um paradigma unificado e CLI que combina site a site, **acesso remoto**, topologias hub e spoke e malhas parciais (spoke to spoke direct). O FlexVPN oferece uma estrutura simples, mas modular, que usa extensivamente o paradigma da interface do túnel enquanto permanece compatível com implementações de VPN legadas.



Configuração de pré-requisitos

Para este exemplo, uma configuração de laboratório SD-WAN RA foi criada conforme mostrado na imagem.



Componentes adicionais foram configurados para este cenário de laboratório de RA SD-WAN:

- Um Cisco IOS® XE regular no modo autônomo como um servidor CA.
- Um servidor ISE/Radius para autenticação, autorização e contabilidade.
- Um PC Windows com acesso ao cEdge através da interface WAN.
- O AnyConnect Client já está instalado.

Note: Os servidores CA e RADIUS foram colocados no serviço VRF 1. Ambos os servidores devem estar acessíveis através do VRF de serviço para todos os headends de RA SD-WAN.

Note: O Cisco SD-WAN Remote Access é suportado na versão 17.7.1a e em dispositivos específicos para SDRA. Para dispositivos suportados, consulte: Plataformas suportadas para o headend SD-WAN RA

Configuração do ISE

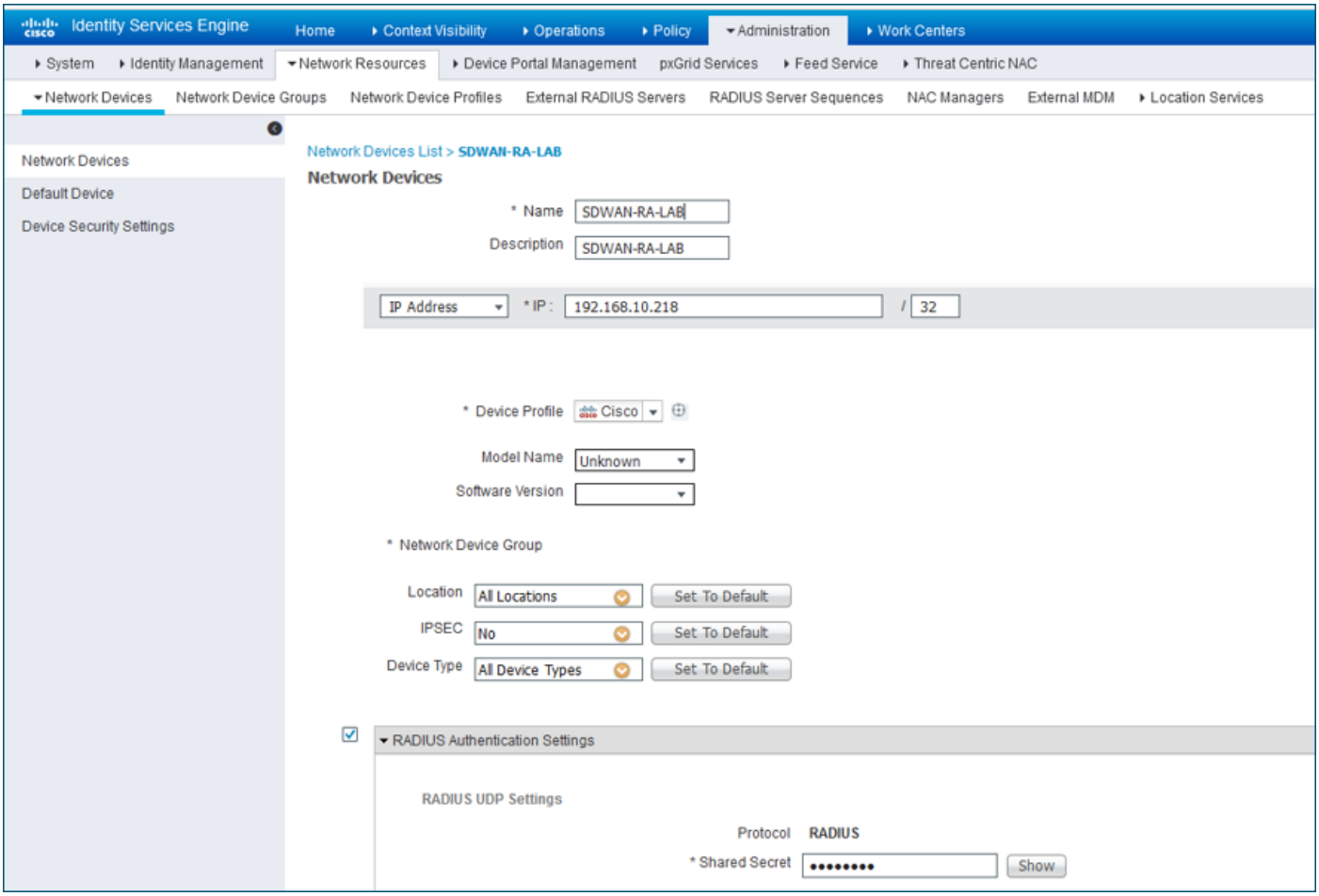
Para suportar o headend de RA SD-WAN, assegure-se de que os parâmetros estejam configurados no servidor RADIUS. Estes parâmetros são necessários para conexões de RA:

- Credenciais de autenticação de usuário Nome de usuário e senha para conexões AnyConnect-EAP
- Parâmetros de política (atributos) que se aplicam a um usuário ou a um grupo de usuários

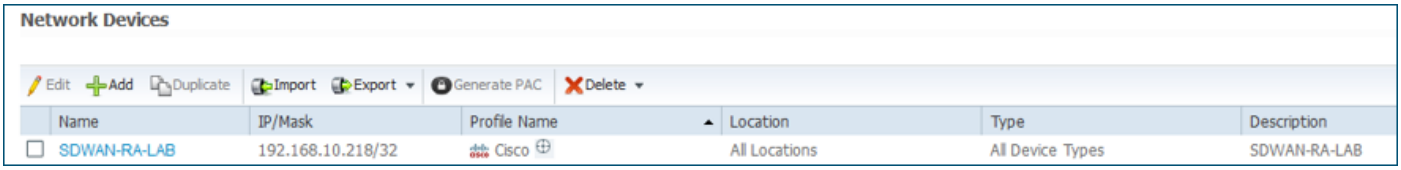
VRF: VPN de serviço ao qual o usuário RA está atribuído**Nome do pool IP**: Nome do pool IP definido no headend do RA**Sub-redes do servidor**: Acesso à sub-rede para fornecer ao usuário do RA

A primeira etapa a ser configurada no ISE é o headend do RA ou o endereço IP do cEdge como um dispositivo de rede para poder fazer solicitações Radius ao ISE.

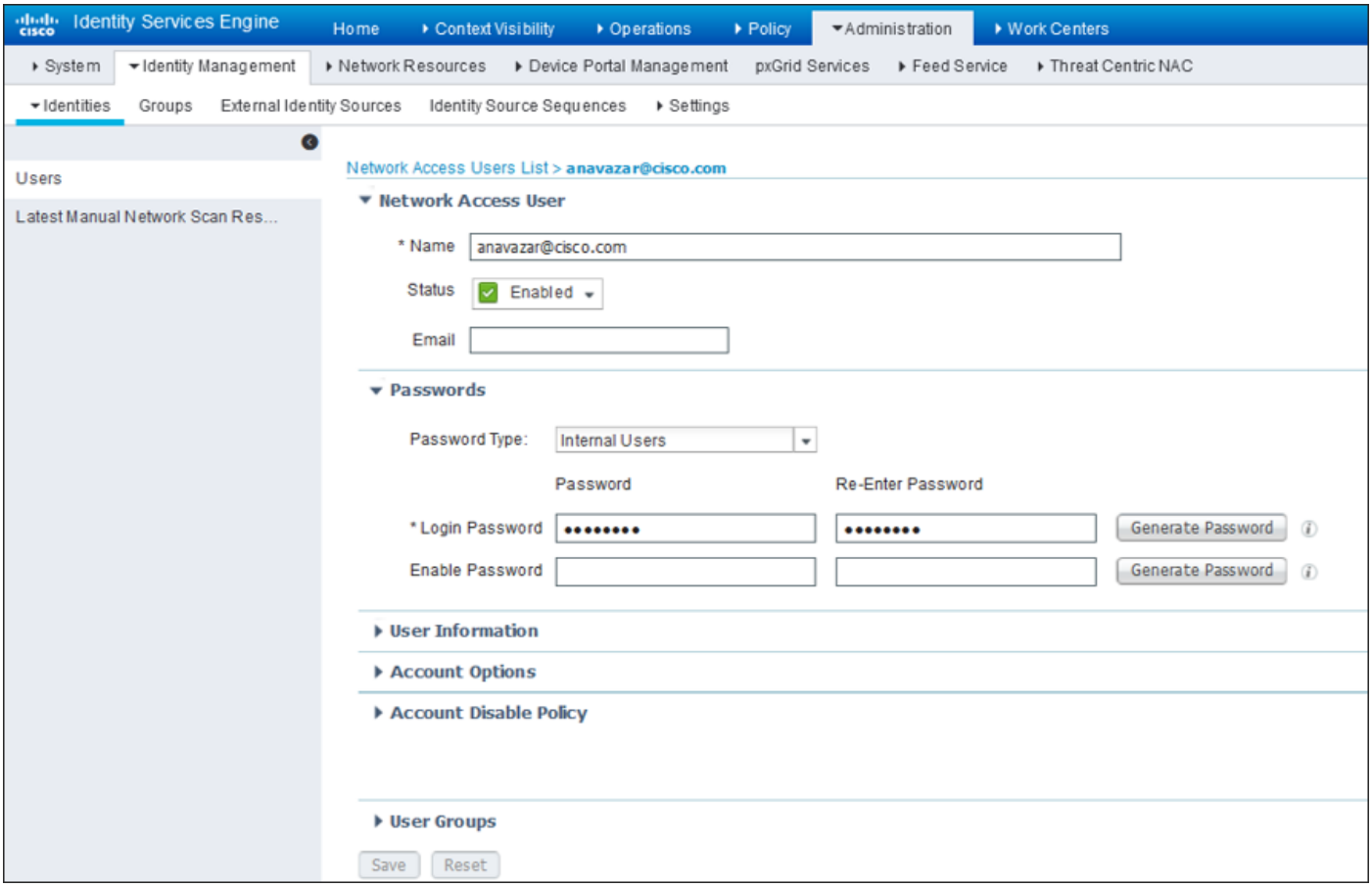
Navegue **para Administração > Dispositivos de rede** e adicione o endereço IP e a senha do cabeçalho RA (cEdge) como mostrado na imagem.



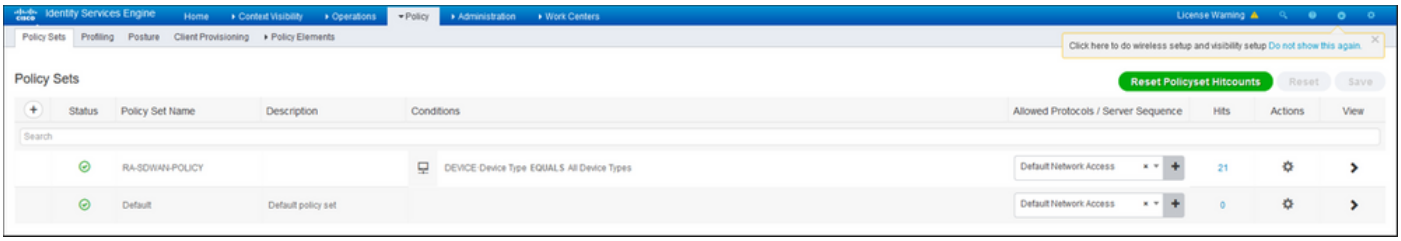
Dispositivo de rede adicionado conforme mostrado na imagem.



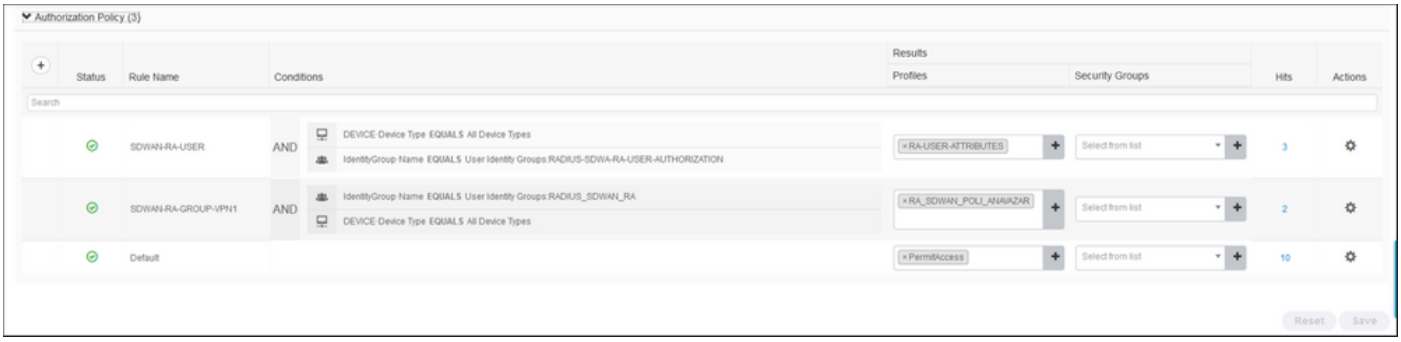
No servidor RADIUS, é necessário configurar os nomes de usuário e a senha para a autenticação do AnyConnect, como mostrado na imagem. Navegue até **Administração > Identidades**.



Énecessário criar um conjunto de políticas com a condição de correspondência a ser atingida, conforme mostrado na imagem. Nesse caso, a condição **Todos os tipos de dispositivos** é usada, o que significa que todos os usuários acessam essa política.



Em seguida, a Política de autorização foi criada uma por condição. A condição **Todos os tipos de dispositivos** e os grupos de identidades a corresponderem.

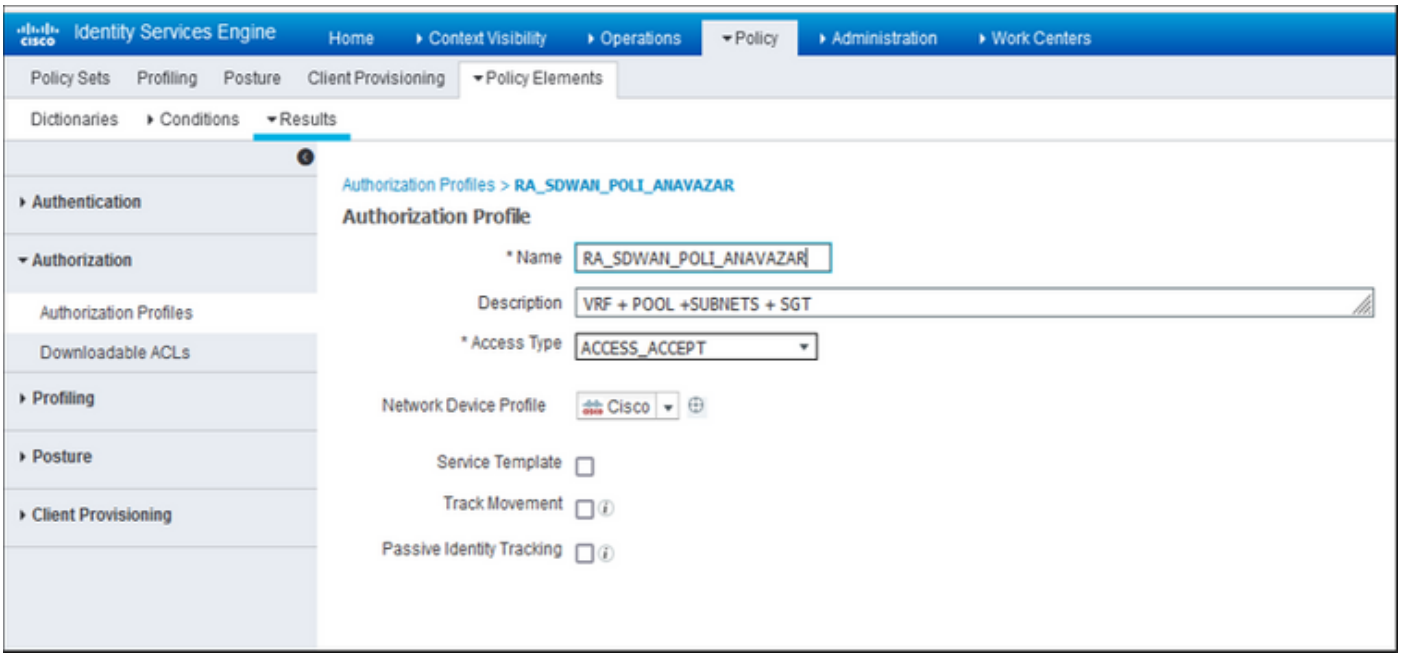


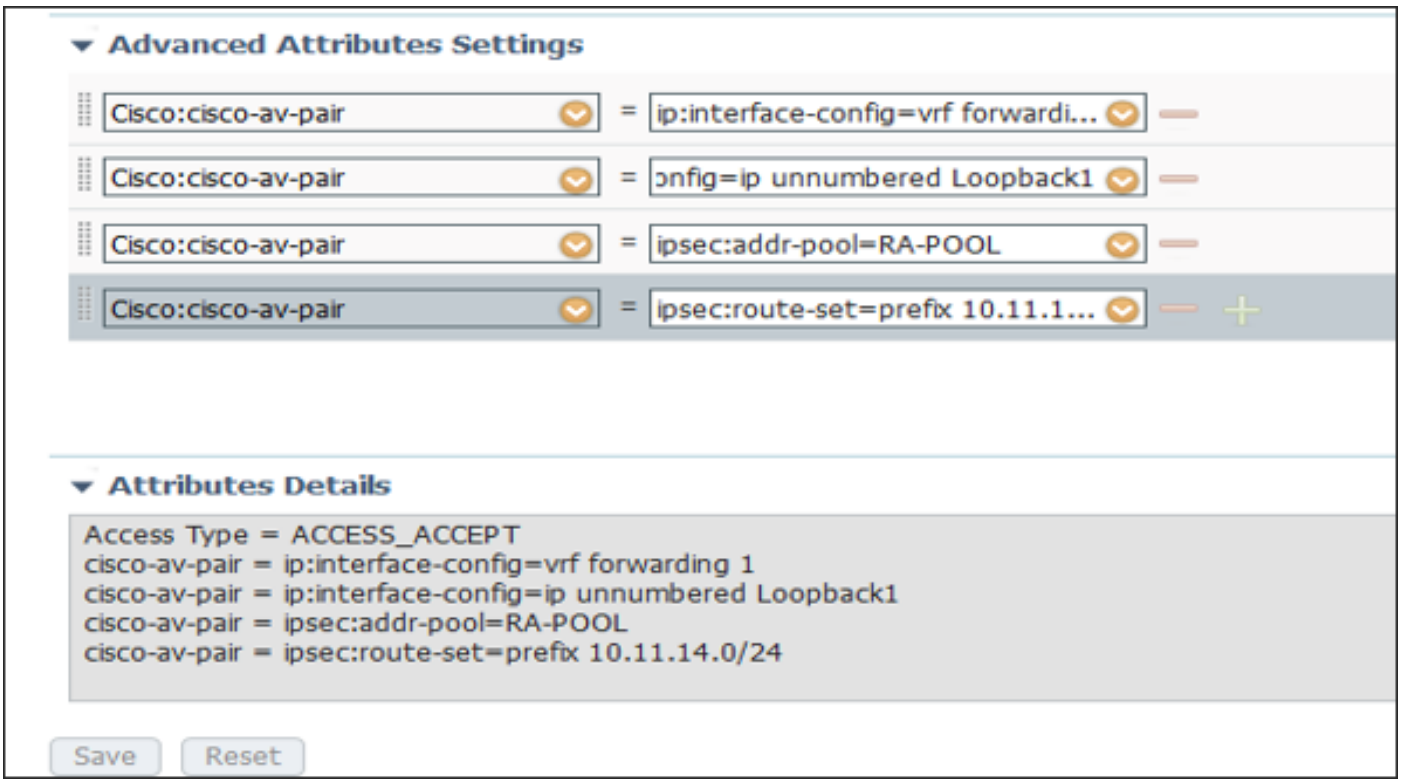
No **Perfil de autorização**, precisamos configurar o **Tipo de acesso** como **Access_ACCEPT** nas **Configurações avançadas de atributos**, selecionar o fornecedor da Cisco e o atributo de par **AV da Cisco.**

Énecessário configurar alguns parâmetros de política para os usuários:

- VRF, o VRF de serviço ao qual o usuário pertence.
- O nome do pool de IP, cada conexão de usuário, recebe um endereço IP que pertence ao pool de IPs configurado nas Bordas.
- as sub-redes que o usuário pode acessar

Cuidado: o comando **IP vrf forwarding** deve aparecer antes do comando **IP unnumbered**. Se a interface de acesso virtual for clonada do modelo virtual e o comando **IP vrf forwarding** for aplicado, qualquer configuração IP será removida da interface de acesso virtual.





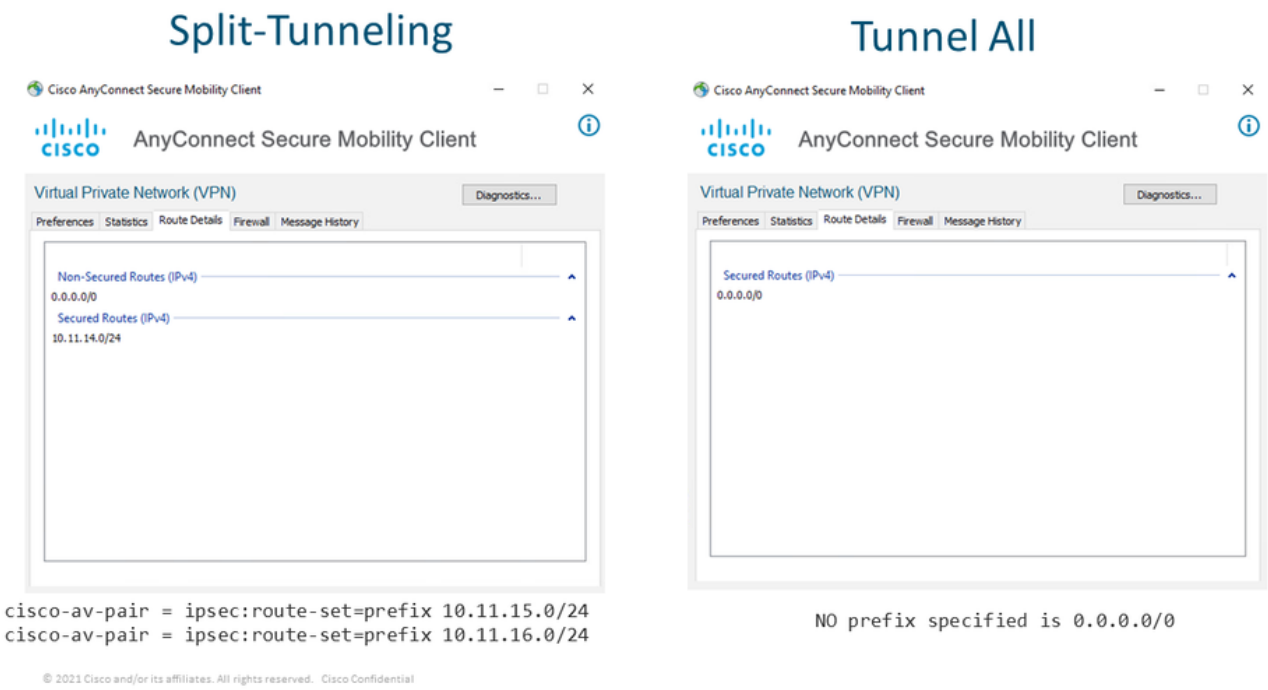
Atributos do usuário:

```
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 versus Tunnel All no AnyConnect Client

ipsec:route-set=prefix attribute recebido no AnyConnect Client é instalado conforme mostrado na imagem.



Configuração do servidor de CA no Cisco IOS® XE

O servidor CA provisiona certificados para os dispositivos Cisco IOS® XE SD-WAN e permite que o headend RA autentique-se aos clientes RA.

O CEDGE não pode ser um servidor CA, pois esses comandos crypto PKI server não são suportados no Cisco IOS® XE SD-WAN.

- Gerar um par de chaves RSA
- Crie o ponto de confiança PKI para o servidor CA Configure o par de chaves com o KEY-CA anteriormente gerado.

  Note: O servidor PKI e o ponto de confiança PKI devem usar o mesmo nome.

- Crie o servidor CA Configurar o nome do emissor para o servidor CAAtive o servidor CA usando "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 se o servidor CA está ativado.

```
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 se o certificado do servidor 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
```

O **Fingerprint SHA 1** do certificado CA é usado no **ponto confiável de pki de criptografia** no roteador cEdge (headend RA) com a configuração de acesso remoto.

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

Configuração do RA SD-WAN

> **Note**: Este documento não cobre o processo de integração SD-WAN para Controladores e cEdge. Supõe-se que a estrutura SD-WAN está ativa e totalmente funcional.

Configuração de PKI de criptografia

- Criar ponto de confiança PKI.
- Configure o URL para o servidor CA.
- Copie a impressão digital sha 1 do certificado do servidor CA.
- Configure o nome do assunto e o nome Alt do novo certificado de identidade.
- Configure o rsakeypar com a ID-chave gerada 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
 rsakeypair KEY-NEW
 revocation-check none
```

Solicite o certificado CA para autenticar:

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

Gera o CSR, envia para o servidor CA e recebe o novo certificado de identidade:

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

Verifique o certificado CA e o 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
```

Configuração 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
```

Configuração FlexVPN

Configurar Pool IP

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

Configurar propostas de IKEv2 (cifras e parâmetros) e 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
```

Configurar um gerenciador de nomes de perfis IKEv2:

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

Note: O **gerenciador de nomes** deriva o nome do prefixo na identidade EAP (nome de usuário) que delimita na identidade EAP que separa o prefixo e o sufixo.

Configurar cifras IPsec:

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

Configurar o 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
```

Configurar o perfil Crypto IPSEC:

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

Configurar Virtual Template Interface:

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

Configure o modelo virtual no perfil Crypto IKEv2:

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

Exemplo de configuração de SD-WAN RA

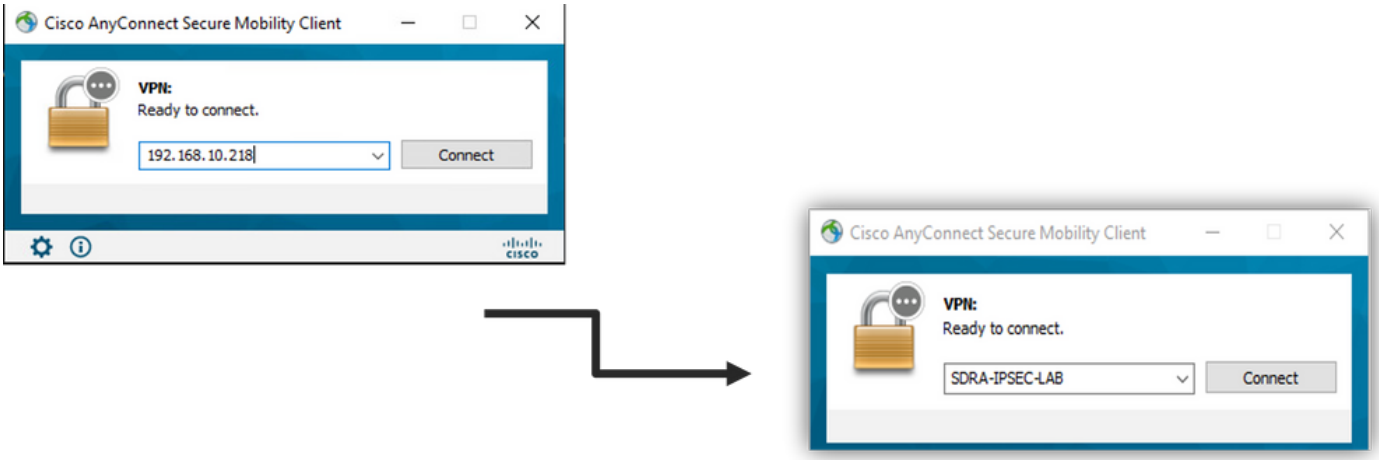
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group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

Configuração do AnyConnect Client

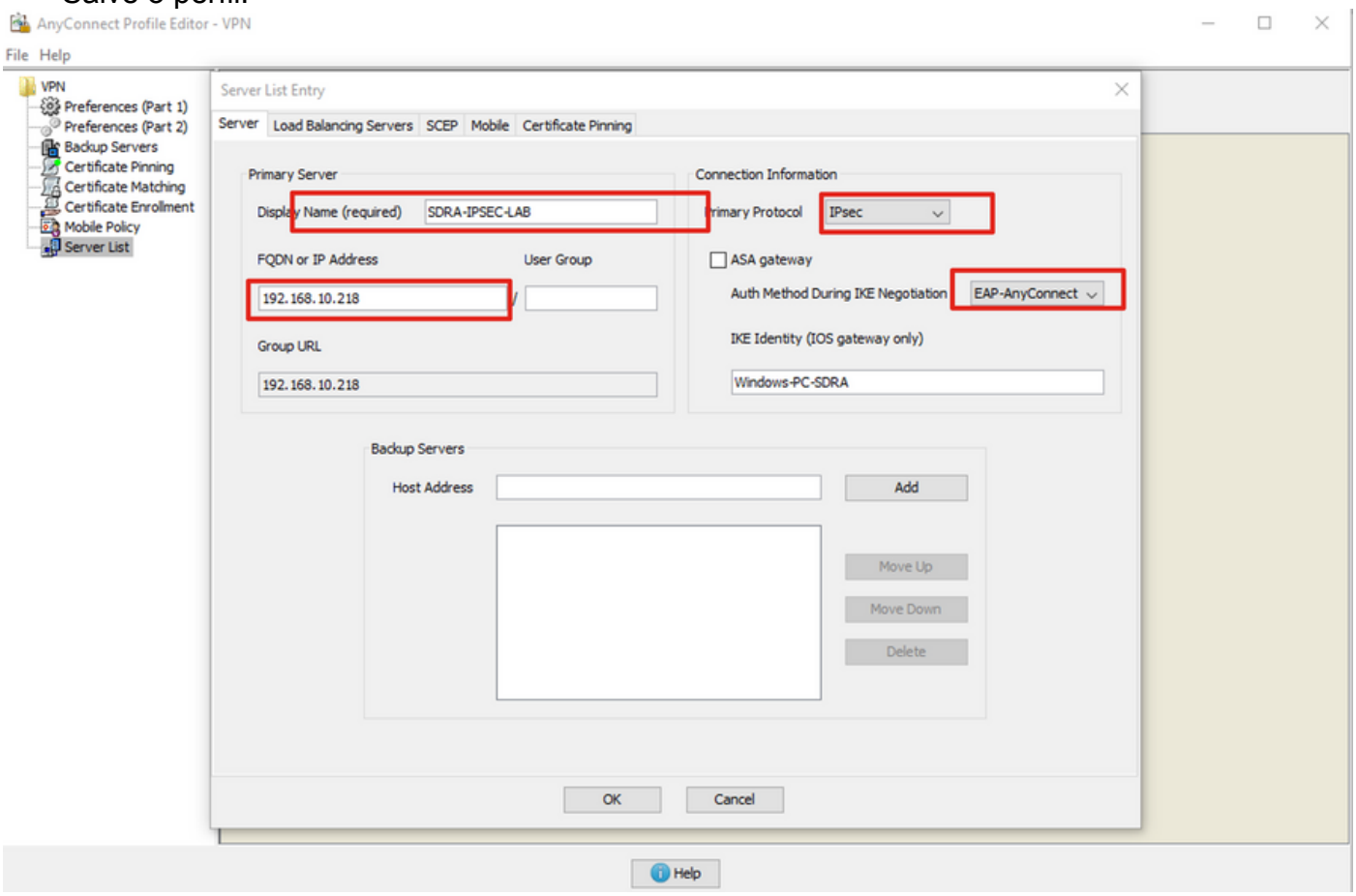
O AnyConnect Client usa SSL como o protocolo padrão para estabelecimento de túnel, e esse protocolo não é suportado para SD-WAN RA (Roteiro). O RA usa FlexVPN, portanto, IPSEC é o protocolo usado e é obrigatório alterá-lo, e isso é feito através do perfil XML.

O usuário pode inserir manualmente o FQDN do gateway VPN na barra de endereços do cliente AnyConnect. Isso resulta na conexão SSL com o gateway.



Configurar o Editor de perfis do AnyConnect

- Navegue até **Server List** e clique em **Add**.
- Selecione **IPsec** como "Protocolo primário".
- Desmarque a opção de **gateway ASA**.
- Selecione **EAP-AnyConnect** como o "Método de autenticação durante a negociação de IKE".
- **Display/Name (Obrigatório)** é o nome usado para salvar essa conexão no cliente AnyConnect.
- **FQDN ou endereço IP devem** ser arquivados no endereço IP cEdge (público).
- Salve o perfil.



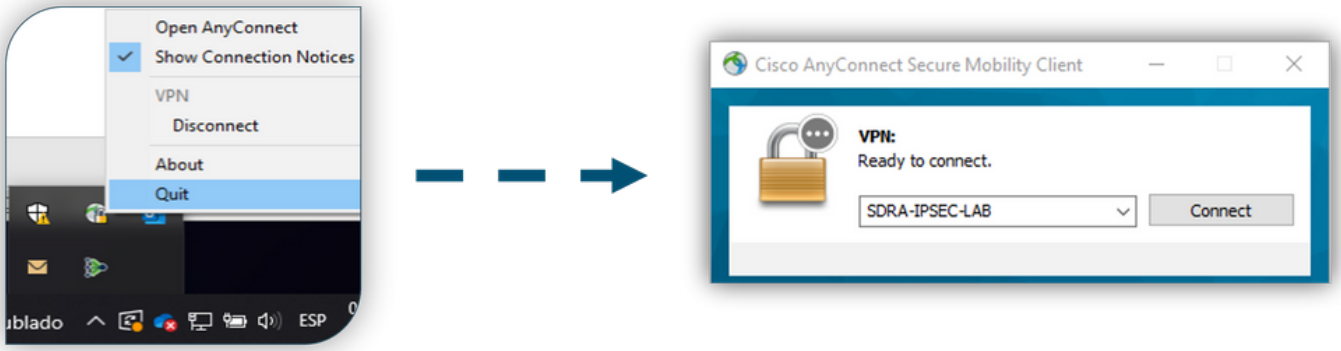
Instalar o perfil do AnyConnect (XML)

O perfil XML pode ser colocado manualmente no diretório:

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

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

O cliente AnyConnect precisa ser reiniciado para que o perfil fique visível na GUI. O processo pode ser reiniciado clicando com o botão direito do mouse no ícone do AnyConnect na bandeja do Windows e selecionando a opção **Sair**:



Desative o downloader do AnyConnect

Por padrão, o cliente AnyConnect tenta fazer o download do perfil XML após o login bem-sucedido.

Se o perfil não estiver disponível, a conexão falhará. Como solução alternativa, é possível desativar o recurso de download de perfil do AnyConnect no próprio cliente.

Para Windows:

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

Para MAC OS:

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

A opção "BypassDownloader" está definida como "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>
```

Desbloquear servidores não confiáveis no AnyConnect Client

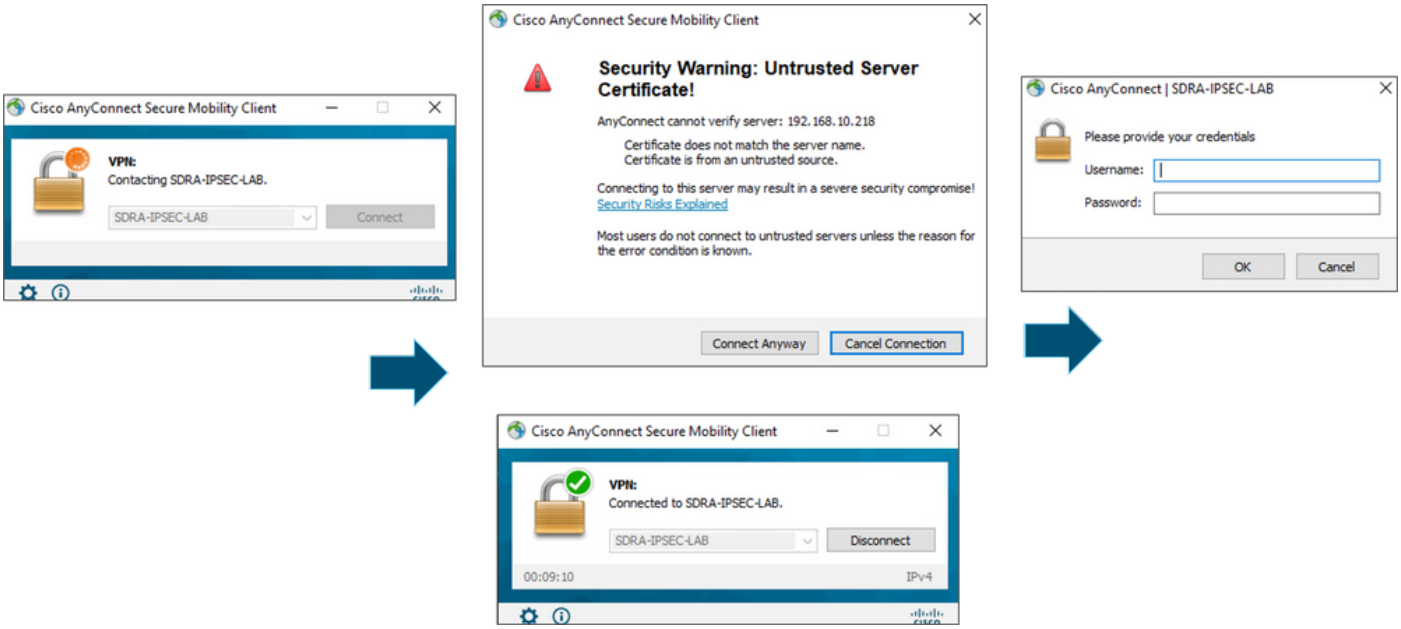
Navegue até **Configurações > Preferências** e desmarque todas as opções da caixa.

O mais importante é o "**Bloquear Conexões a servidores não confiáveis**" para este cenário.

> **Note:** O certificado usado para autenticação de headend de RA/cEdge é o certificado criado e assinado anteriormente pelo servidor de CA no Cisco IOS® XE. Como este servidor CA não é uma entidade pública como GoDaddy, Symantec, Cisco, etc. O PC Client interpreta o certificado como um servidor não confiável. Isso é corrigido usando um certificado público ou um servidor CA confiável pela sua empresa.

Usar o AnyConnect Client

Quando toda a configuração de SDRA é colocada, o fluxo para uma conexão bem-sucedida é mostrado como a imagem.



Verificar

A interface de modelo virtual é usada para criar a interface de acesso virtual para iniciar um canal de criptografia e estabelecer associações de segurança (SAs) IKEv2 e IPsec entre o servidor (cEdge) e o cliente (usuário do AnyConnect).

> **Note**: A interface de modelo virtual está sempre **ativa/inativa**. **O status** está **ativo** e **o protocolo** está **inativo**.

```
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 a configuração real aplicada para a interface Virtual-Access associada ao cliente com **show derivado-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 as associações de segurança (SAs) IPsec para o cliente AnyConnect com o **comando 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….
```

Verifique os parâmetros SA do IKEv2 para a sessão, o nome de usuário e o IP atribuído.

> **Note**: O endereço IP atribuído deve corresponder ao endereço IP no lado do 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
```

Informações Relacionadas

- Acesso remoto Cisco SD-WAN
- Configurar o servidor FlexVPN
- Baixe o AnyConnect
- Suporte Técnico e Documentação - Cisco Systems