

# Configurer l'accès à distance SD-WAN (SDRA) avec AnyConnect et ISE Server

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Qu'est-ce qu'un VPN d'accès à distance ?](#)

[Qu'est-ce que le VPN d'accès à distance SD-WAN ?](#)

[Fractionner la transmission tunnel et tout le tunnel](#)

[Avant SDRA et après SDRA](#)

[Qu'est-ce que FlexVPN ?](#)

[Configuration requise](#)

[Configuration ISE](#)

[Split-Tunneling vs Tunnel All in AnyConnect Client](#)

[Configuration du serveur AC dans Cisco IOS® XE](#)

[Configuration de la RA SD-WAN](#)

[Configuration de Crypto PKI](#)

[Configuration AAA](#)

[Configuration FlexVPN](#)

[Exemple de configuration de la RA SD-WAN](#)

[Configuration du client AnyConnect](#)

[Configurer AnyConnect Profile Editor](#)

[Installer le profil AnyConnect \(XML\)](#)

[Désactiver le téléchargeur AnyConnect](#)

[Débloquer les serveurs non fiables sur le client AnyConnect](#)

[Utiliser le client AnyConnect](#)

[Vérification](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer SD-WAN Remote Access (SDRA) avec AnyConnect Client à l'aide d'un mode autonome Cisco IOS® XE en tant que serveur d'autorité de certification et d'un serveur Cisco Identity Services Engine (ISE) pour l'authentification, l'autorisation et la comptabilité.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel Cisco (SD-WAN)
- Infrastructure à clé publique (PKI)
- FlexVPN
- serveur RADIUS

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

### Qu'est-ce qu'un VPN d'accès à distance ?

Le VPN d'accès à distance permet à l'utilisateur distant de se connecter en toute sécurité aux réseaux de l'entreprise, d'utiliser des applications et des données accessibles uniquement via les périphériques connectés au bureau.

Un VPN d'accès à distance fonctionne par un tunnel virtuel créé entre le périphérique d'un employé et le réseau de l'entreprise.

Ce tunnel passe par l'internet public mais les données envoyées et envoyées par lui sont protégées par des protocoles de cryptage et de sécurité pour aider à le garder privé et sécurisé.

Les deux principaux composants de ce type de VPN sont un serveur d'accès réseau/tête de réseau d'accès et un logiciel client VPN.

### Qu'est-ce que le VPN d'accès à distance SD-WAN ?

L'accès à distance a été intégré à la solution SD-WAN, ce qui élimine le besoin d'infrastructures Cisco SD-WAN et RA distinctes et permet une évolutivité rapide des services RA grâce à l'utilisation de Cisco AnyConnect en tant que client logiciel RA.

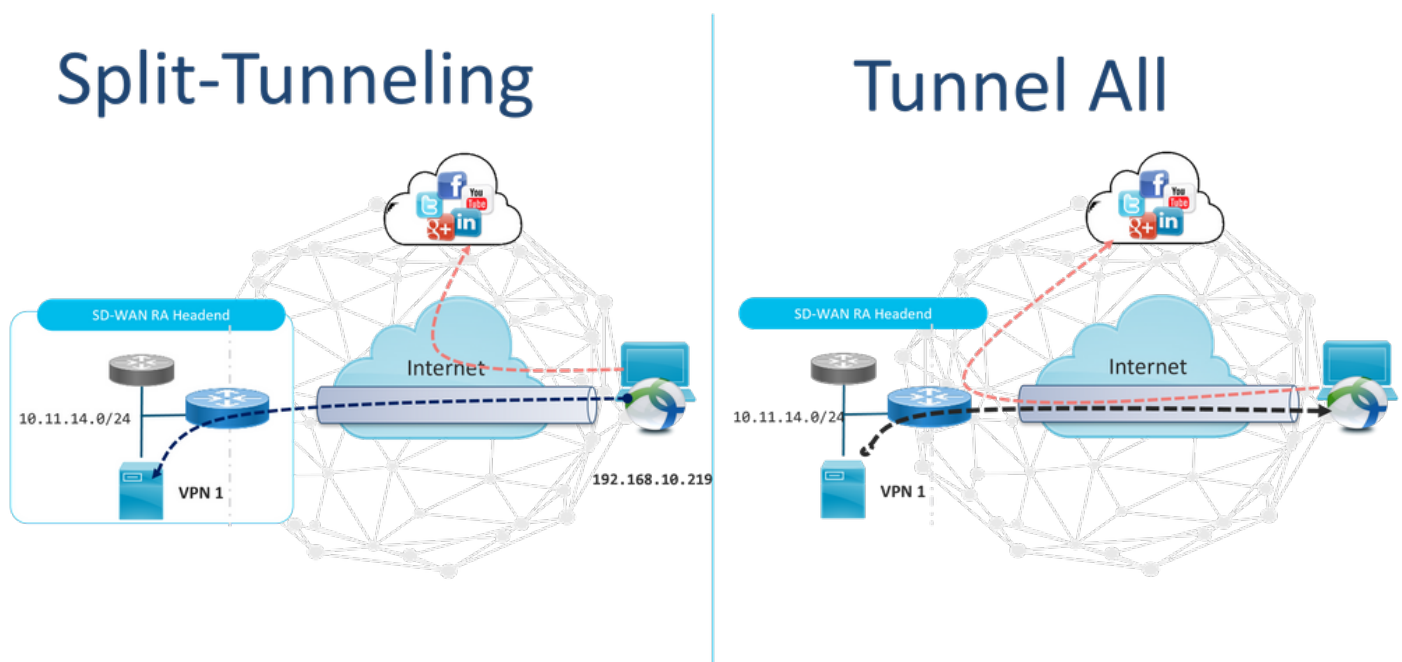
L'accès à distance permet aux utilisateurs distants d'accéder au réseau de l'entreprise. Cela permet le travail à partir de la maison.

### Les avantages

- RA permet d'accéder au réseau d'une organisation à partir d'appareils/d'utilisateurs situés sur des sites distants. (HO)
- Étend la solution Cisco SD-WAN aux utilisateurs RA sans que le périphérique de chaque utilisateur RA doive faire partie du fabric Cisco SD-WAN.
- Sécurité des données
- Fractionner la transmission tunnel ou tout le tunnel
- Évolutivité
- Possibilité de distribuer la charge RA sur de nombreux périphériques SD-WAN Cisco IOS® XE dans le fabric Cisco SD-WAN.

## Fractionner la transmission tunnel et tout le tunnel

La transmission tunnel partagée est utilisée dans des scénarios où seul le trafic spécifique doit être tunnelisé (sous-réseaux SD-WAN par exemple), comme le montre l'image.

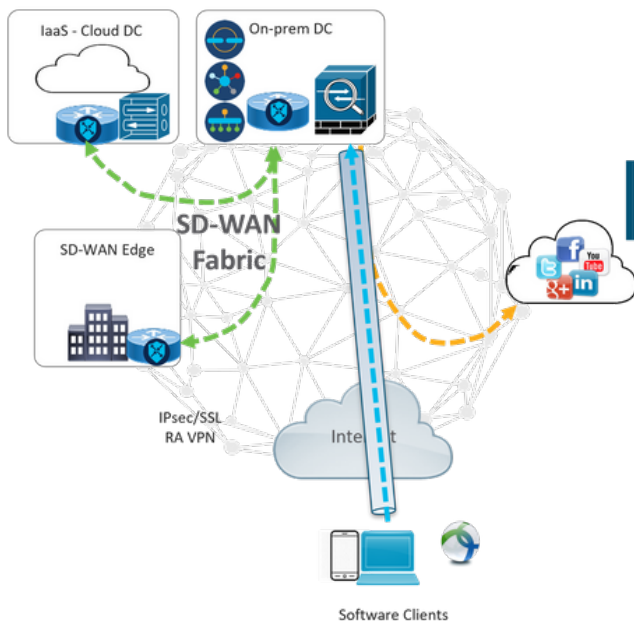


## Avant SDRA et après SDRA

La conception VPN d'accès à distance traditionnelle nécessite une infrastructure d'accès à distance distincte en dehors du fabric Cisco SD-WAN pour fournir un accès à distance aux utilisateurs du réseau, comme les appliances non SD-WAN telles que ASA, Cisco IOS® XE régulier ou des périphériques tiers, et le trafic d'accès à distance est transféré vers l'appliance SD-WAN comme illustré sur l'image.

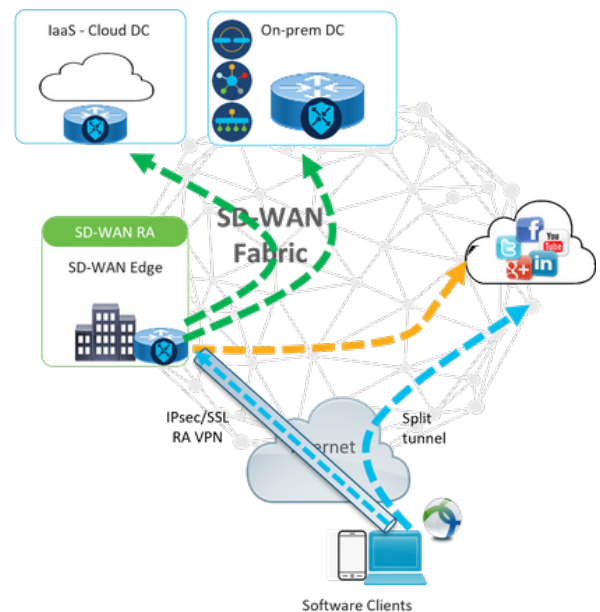
## Before SDRA

Traditional Remote-Access VPN design with SDWAN



## After SDRA

SD-WAN Remote-Access



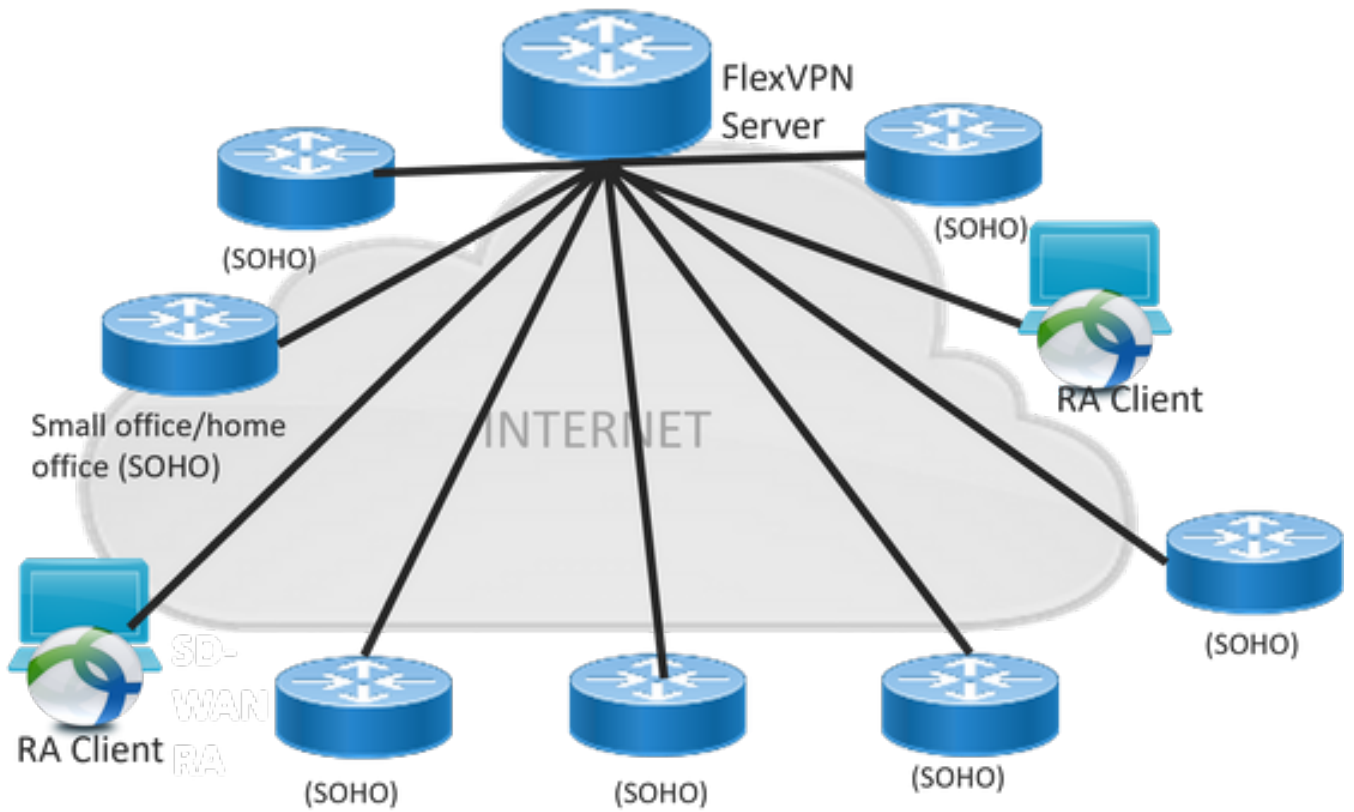
L'accès à distance SD-WAN modifie la façon dont les utilisateurs distants se connectent au réseau. Ils se connectent directement à cEdge qui est utilisé comme tête de réseau d'accès distant. Étend les fonctionnalités et les avantages Cisco SD-WAN aux utilisateurs de RA. Les utilisateurs RA deviennent des utilisateurs LAN de filiale.

Pour chaque client RA, la tête de réseau d'accès SD-WAN attribue une adresse IP à un client RA et ajoute une route d'hôte statique à l'adresse IP attribuée dans le VRF de service dans lequel l'utilisateur RA est placé.

La route statique spécifie le tunnel VPN de la connexion client RA. La tête de réseau d'accès SD-WAN annonce l'IP statique dans le VRF de service du client d'accès distant avec l'utilisation d'OMP à tous les périphériques de périphérie du VPN de service.

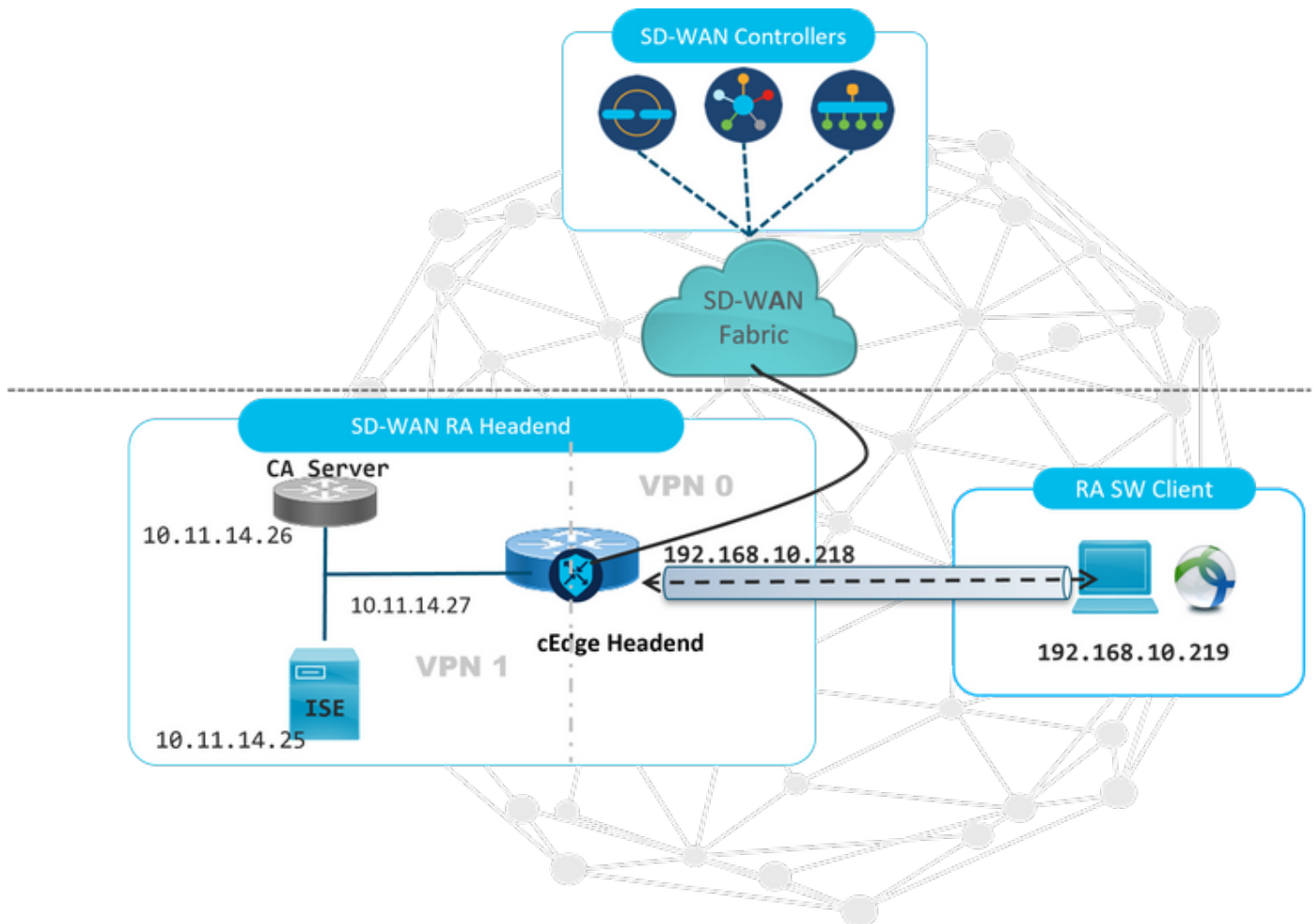
## Qu'est-ce que FlexVPN ?

SD-WAN RA Exploite la solution Cisco FlexVPN RA. FlexVPN est la mise en oeuvre de la norme IKEv2 par Cisco. Elle repose sur un paradigme unifié et une interface de ligne de commande qui associe site à site, **accès à distance**, topologies en étoile et en étoile et maillages partiels (satellite direct). FlexVPN offre un cadre simple mais modulaire qui utilise largement le paradigme d'interface de tunnel tout en restant compatible avec les implémentations VPN existantes.



## Configuration requise

Pour cet exemple, une configuration de TP d'évaluation SD-WAN a été créée, comme l'illustre l'image.



D'autres composants ont été configurés pour ce scénario de travaux pratiques d'évaluation de la faisabilité du SD-WAN :

- Cisco IOS® XE standard en mode autonome en tant que serveur AC.
- Serveur ISE/Radius pour l'authentification, l'autorisation et la comptabilité.
- Un PC Windows avec une accessibilité à cEdge via l'interface WAN.
- AnyConnect Client est déjà installé.

**Note:** Les serveurs CA et RADIUS ont été placés dans le service VRF 1. Les deux serveurs doivent être accessibles via le VRF de service pour toutes les têtes de réseau d'accès SD-WAN.

**Note:** L'accès à distance Cisco SD-WAN est pris en charge sur la version 17.7.1a et sur des périphériques spécifiques pour SDR. Pour les périphériques pris en charge, reportez-vous à : [Plates-formes prises en charge pour la tête de réseau d'accès à distance SD-WAN](#)

## Configuration ISE

Pour prendre en charge la tête de réseau d'accès à distance SD-WAN, assurez-vous que les paramètres sont configurés sur le serveur RADIUS. Ces paramètres sont requis pour les connexions RA :

- Informations d'authentification utilisateur Nom d'utilisateur et mot de passe pour les connexions AnyConnect-EAP

- Paramètres de stratégie (attributs) qui s'appliquent à un utilisateur ou à un groupe d'utilisateurs **VRF** : VPN de service auquel l'utilisateur RA est affecté **Nom du pool d'adresses IP** : Nom du pool d'adresses IP défini sur la tête de réseau d'accès distant **Sous-réseaux du serveur** : Accès au sous-réseau pour fournir à l'utilisateur RA

La première étape à configurer dans l'ISE est la tête de réseau ou l'adresse IP cEdge de RA en tant que périphérique réseau pour pouvoir envoyer des requêtes Radius à l'ISE.

Accédez à **Administration > Périphériques réseau** et ajoutez l'adresse IP et le mot de passe en tête d'annonce de routeur (cEdge), comme indiqué dans l'image.

The screenshot shows the 'Network Devices' configuration page in the ISE Administration console. The breadcrumb trail is: Administration > Network Resources > Network Devices. The page title is 'Network Devices List > SDWAN-RA-LAB'. The configuration fields are as follows:

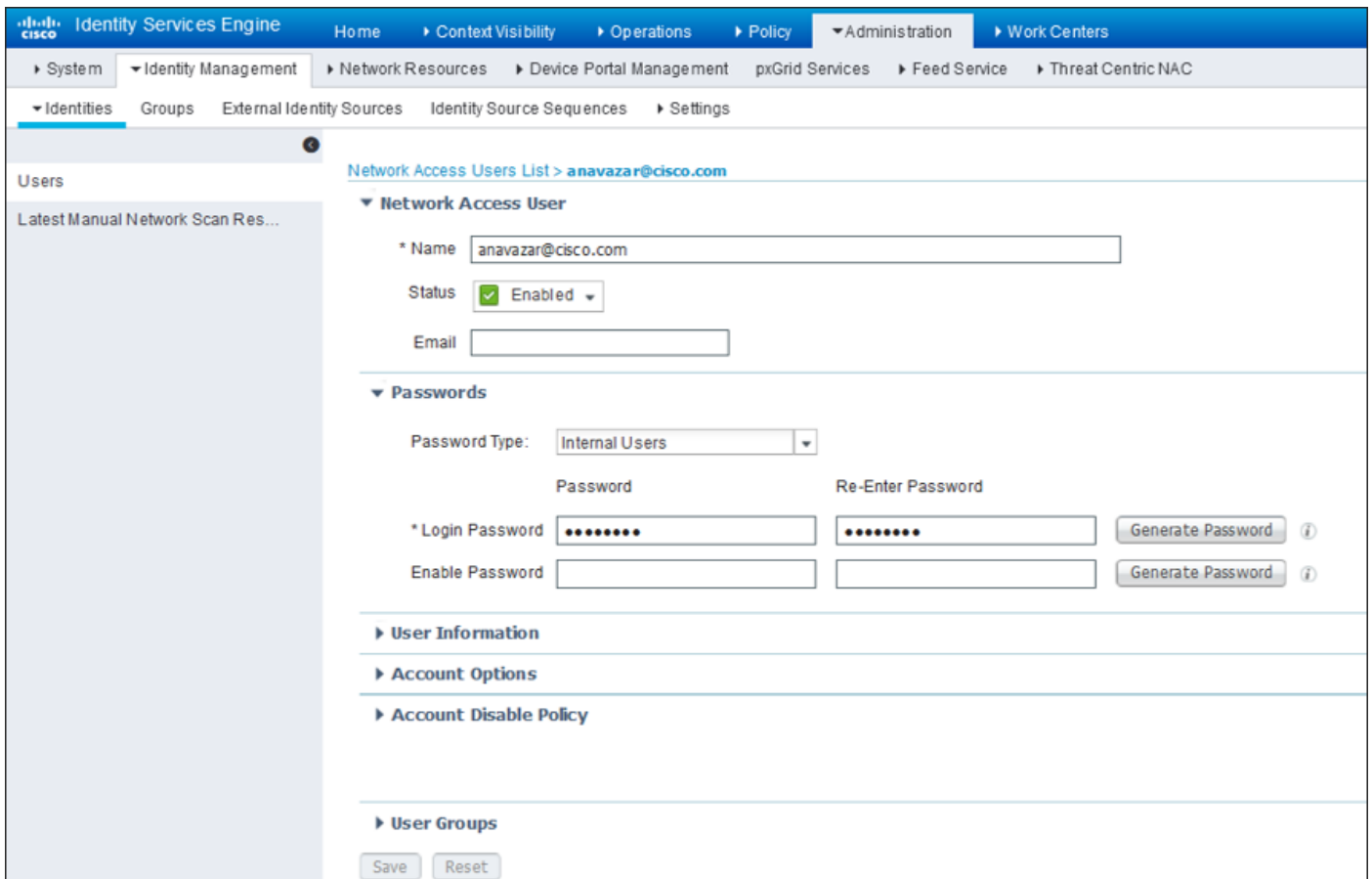
- Name:** SDWAN-RA-LAB
- Description:** SDWAN-RA-LAB
- IP Address:** 192.168.10.218 / 32
- Device Profile:** Cisco
- Model Name:** Unknown
- Software Version:** (empty)
- Network Device Group:**
  - Location:** All Locations (Set To Default)
  - IPSEC:** No (Set To Default)
  - Device Type:** All Device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

Périphérique réseau ajouté comme illustré dans l'image.

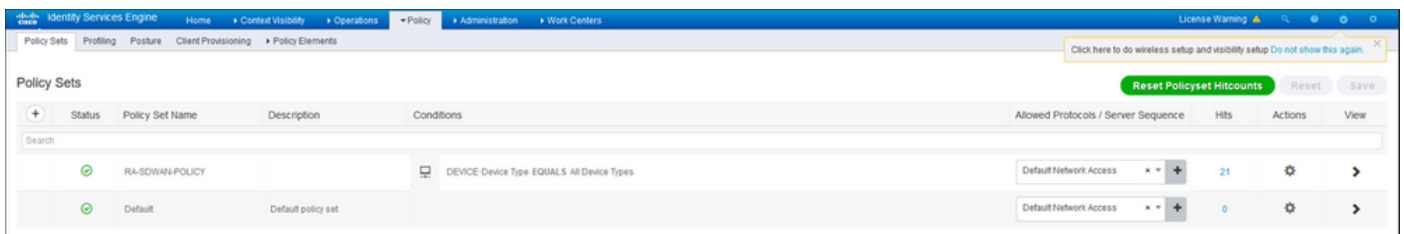
The screenshot shows the 'Network Devices' list table in the ISE Administration console. The table has the following columns and data:

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

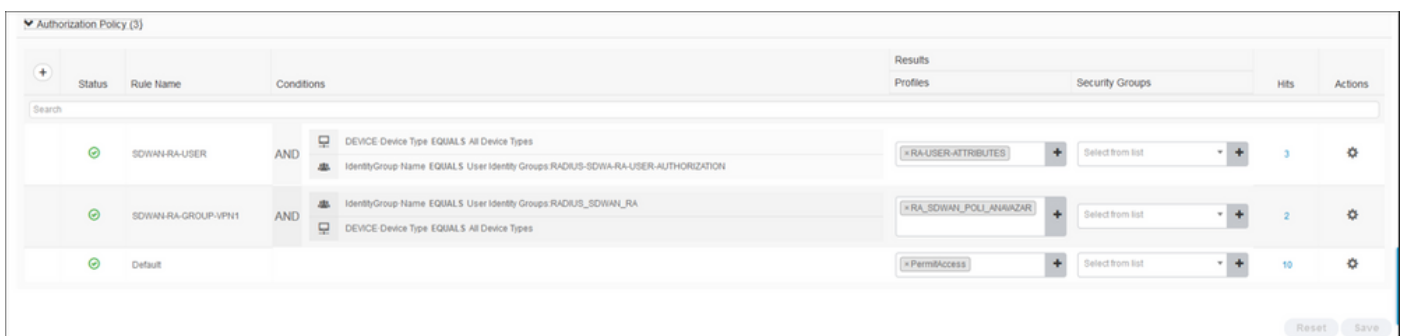
Dans le serveur RADIUS, il est nécessaire de configurer les noms d'utilisateur et le mot de passe pour l'authentification AnyConnect, comme indiqué dans l'image. Accédez à **Administration > Identities**.



Un jeu de stratégies doit être créé avec la condition de correspondance à atteindre, comme le montre l'image. Dans ce cas, la condition **Tous les types de périphériques** est utilisée, ce qui signifie que tous les utilisateurs accèdent à cette stratégie.



Ensuite, la stratégie d'autorisation a été créée par condition. Condition **Tous les types de périphériques** et les groupes d'identités correspondants.



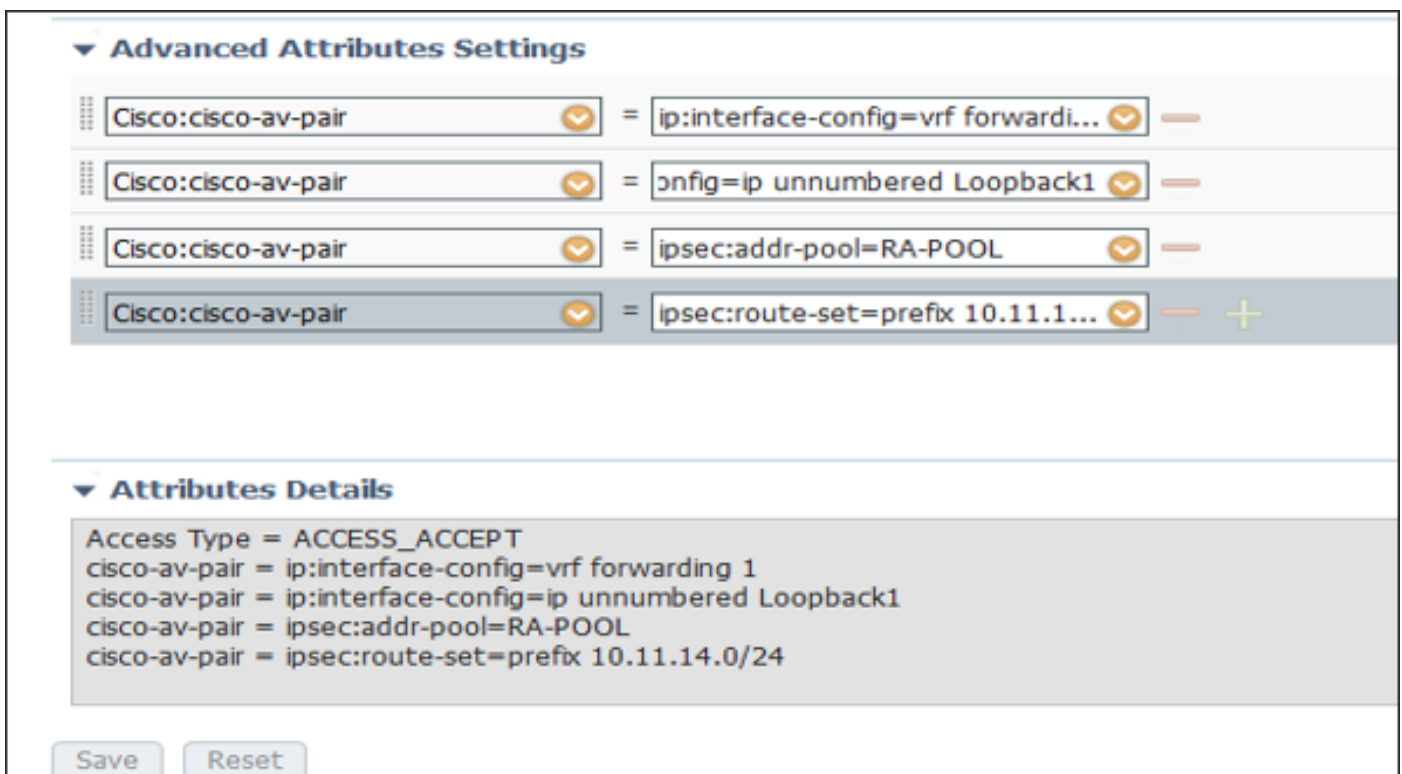
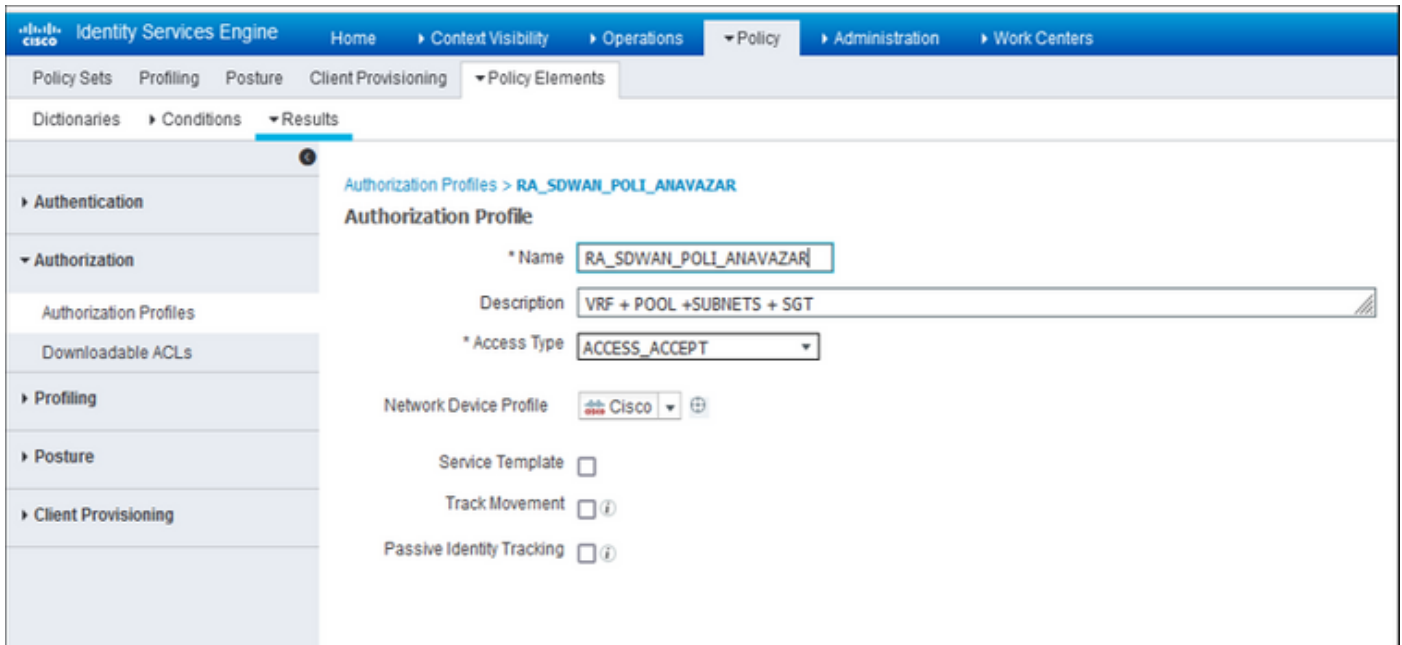
Dans le **profil d'autorisation**, nous devons configurer le **type d'accès** en tant que **Access\_ACCEPT** sous les **paramètres des attributs avancés**, sélectionner le fournisseur Cisco et l'attribut paire **AV-Cisco**.

Il est nécessaire de configurer certains paramètres de stratégie pour les utilisateurs :



- VRF, le VRF de service auquel l'utilisateur appartient.
- Nom du pool d'adresses IP, chaque connexion utilisateur se voit attribuer une adresse IP, qui appartient au pool d'adresses IP configuré dans les arêtes.
- Les sous-réseaux auxquels l'utilisateur peut accéder

**Avertissement :** la commande **IP vrf forwarding** doit précéder la commande **IP unnumbered**. Si l'interface d'accès virtuel est clonée à partir du modèle virtuel et que la commande **IP vrf forwarding** est appliquée, toute configuration IP est supprimée de l'interface d'accès virtuel.



Attributs utilisateur :

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=vrf forwarding 1
  
```

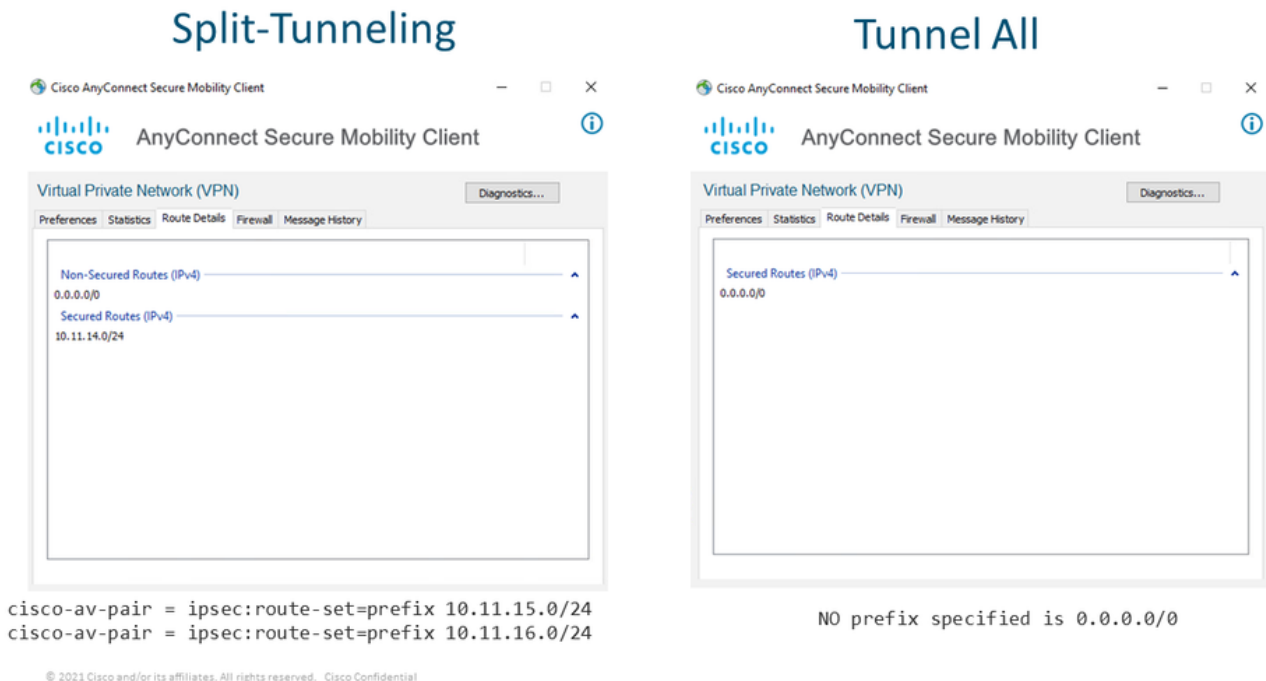
```

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** attribut reçu dans AnyConnect Client est installé comme indiqué dans l'image.



## Configuration du serveur AC dans Cisco IOS® XE

Le serveur AC fournit des certificats aux périphériques SD-WAN Cisco IOS® XE et permet à la tête de réseau d'accès distant de s'authentifier auprès des clients RA.

Le CEDGE ne peut pas être un serveur AC, car ces commandes de serveur de cryptage PKI ne sont pas prises en charge dans le SD-WAN Cisco IOS® XE.

- Générer une paire de clés RSA
- Créer le point de confiance PKI pour le serveur AC Configurez la paire de rôties avec la clé KEY-CA générée précédemment.

**Note:** Le serveur PKI et le point de confiance PKI doivent utiliser le même nom.

- Créer le serveur AC Configurer le nom de l'émetteur pour votre serveur ACActiver le serveur AC à l'aide de " 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  
!
```

Vérifiez si le serveur AC est activé.

```
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
```

Vérifiez si le certificat du serveur AC est installé.

```
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
```

Le **Fingerprint SHA 1** du certificat CA est utilisé sur le **point de confiance crypto pki** dans le routeur cEdge (tête de réseau RA) avec la configuration d'accès à distance.

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

## Configuration de la RA SD-WAN

**Note:** Ce document ne couvre pas le processus d'intégration SD-WAN pour les contrôleurs et cEdge. Il est supposé que la structure SD-WAN est opérationnelle et entièrement fonctionnelle.

### Configuration de Crypto PKI

- Créez un point de confiance PKI.
- Configurez l'URL du serveur AC.
- Copiez l'empreinte digitale sha 1 à partir du certificat du serveur AC.
- Configurez le nom du sujet et le nom Alt pour le nouveau certificat d'identité.
- Configurez rsakeypair avec l'ID de clé précédemment généré.

```
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
```

Demandez le certificat de l'autorité de certification pour l'authentification :

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

Génère le CSR, envoie au serveur AC et reçoit le nouveau certificat d'identité :

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

Vérifiez le certificat CA et le certificat 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

## Configuration 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
```

## Configuration FlexVPN

### Configurer le pool IP

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

### Configurer des propositions IKEv2 (Chiffres et paramètres) et une politique :

```
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
```

### Configurez un gestionnaire de noms de profil IKEv2 :

```
crypto ikev2 name-mangler IKEV2-RA-MANGLER
```

```
eap suffix delimiter @
```

**Note:** Le **gestionnaire de noms** dérive le nom du préfixe dans l'identité EAP (nom d'utilisateur) délimitant dans l'identité EAP qui sépare le préfixe et le suffixe.

Configurer les chiffrement IPsec :

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

Configurer le profil 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
```

Configurer le profil IPSEC de chiffrement :

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

Configurer l'interface de modèle virtuel :

```
!
interface Virtual-Templat101 type tunnel
vrf forwarding 1
tunnel mode ipsec ipv4
tunnel protection ipsec profile IKEV2-RA-PROFILE
```

Configurer le modèle virtuel dans le profil Crypto IKEv2 :

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

## Exemple de configuration de la RA SD-WAN

```
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
```

```

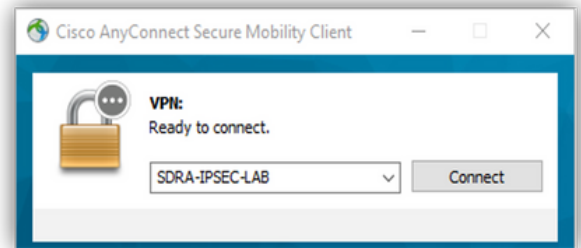
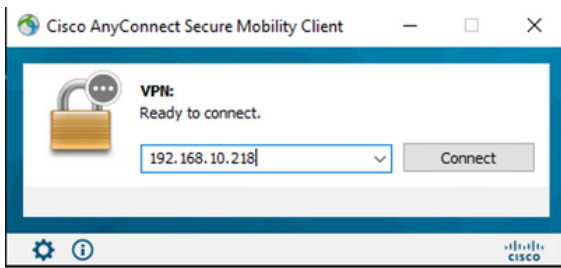
!
crypto pki trustpoint RA-TRUSTPOINT
  subject-name CN=cEdge-SDWAN-1.crv
  enrollment url http://10.11.14.226:80
  fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
  subject-name CN=cEdge-SDWAN-1.crv
  vrf 1
  rsakeypair KEY-NEW
  revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100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

```

## Configuration du client AnyConnect

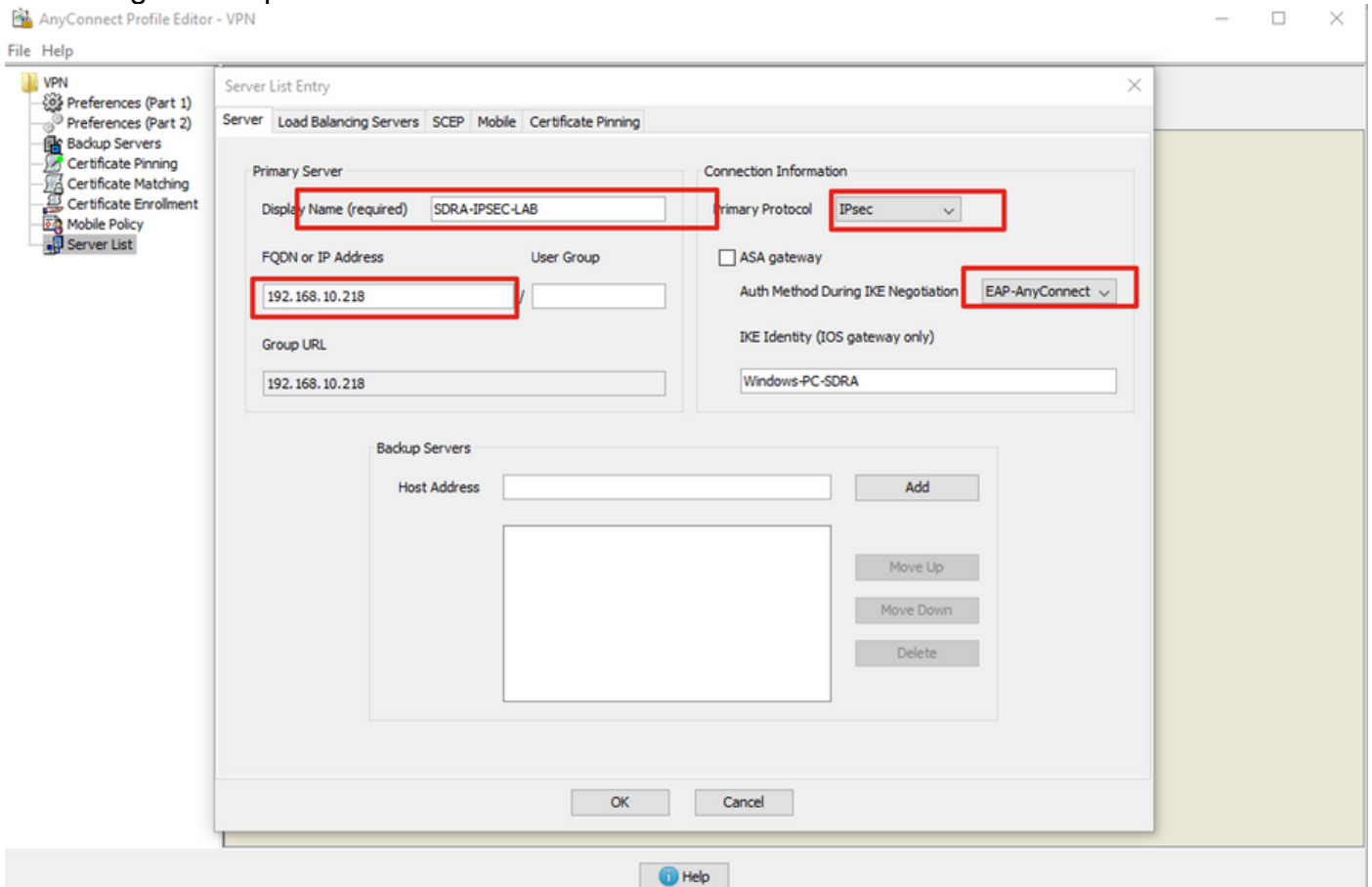
Le client AnyConnect utilise SSL comme protocole par défaut pour l'établissement du tunnel, et ce protocole n'est pas pris en charge pour SD-WAN RA (Road map). RA utilise FlexVPN, par conséquent IPSEC est le protocole utilisé et il est obligatoire de le modifier, et ceci via le profil XML.

L'utilisateur peut entrer manuellement le nom de domaine complet de la passerelle VPN dans la barre d'adresse du client AnyConnect. Cela entraîne la connexion SSL à la passerelle.



## Configurer AnyConnect Profile Editor

- Accédez à **Liste des serveurs** et cliquez sur **Ajouter**.
- Sélectionnez **IPsec** comme « Protocole principal ».
- Désactivez l'option **passerelle ASA**.
- Sélectionnez **EAP-AnyConnect** comme méthode d'authentification “ pendant la ” de négociation IKE.
- **Display/Name (Obligatoire)** est le nom utilisé pour enregistrer cette connexion sous le client AnyConnect.
- **Le nom de domaine complet ou l'adresse IP** doivent être classés avec l'adresse IP (publique) cEdge.
- Enregistrez le profil.



## Installer le profil AnyConnect (XML)



Le profil XML peut être placé manuellement dans le répertoire :

For Windows :

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

For MAC OS :

/opt/cisco/anyconnect/profile

Le client AnyConnect doit être redémarré pour que le profil soit visible dans l'interface utilisateur graphique. Vous pouvez redémarrer le processus en cliquant avec le bouton droit sur l'icône AnyConnect dans la barre d'état système de Windows et en sélectionnant l'option **Quitter** :



## Désactiver le téléchargeur AnyConnect

Le client AnyConnect tente d'effectuer le téléchargement du profil XML après une connexion réussie par défaut.

Si le profil n'est pas disponible, la connexion échoue. Pour contourner ce problème, il est possible de désactiver la fonctionnalité de téléchargement de profil AnyConnect sur le client lui-même.

Pour Windows :

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

Pour MAC OS :

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

L'option « BypassDownloader » est définie sur « 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>
```

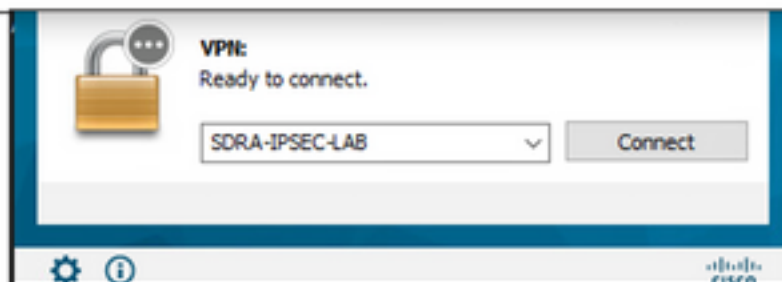
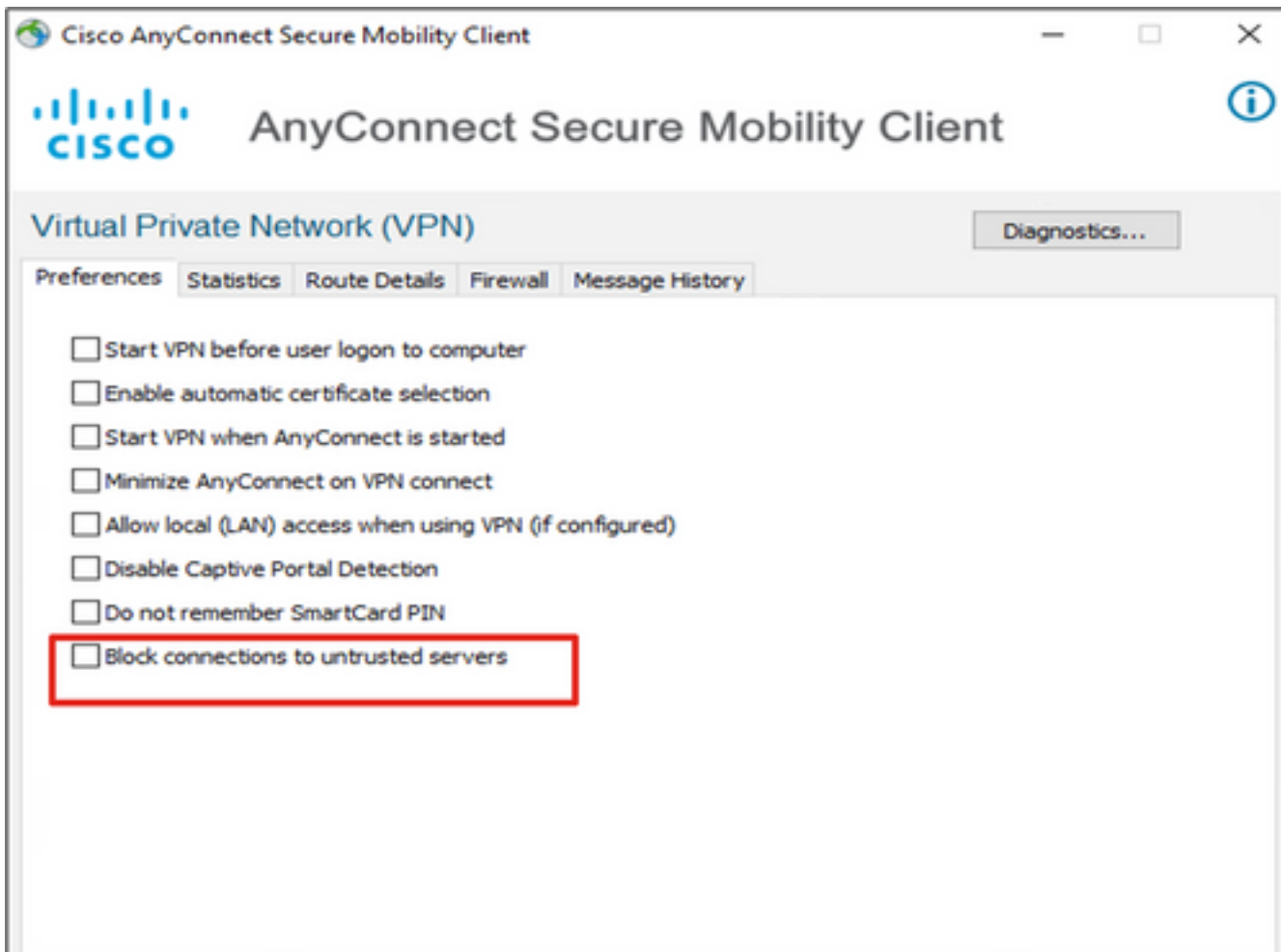
```
<FipsMode>>false</FipsMode>
<RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
<RestrictServerCertStore>>false</RestrictServerCertStore>
<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
<RestrictWebLaunch>>false</RestrictWebLaunch>
<StrictCertificateTrust>>false</StrictCertificateTrust>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

## Débloquer les serveurs non fiables sur le client AnyConnect

Accédez à **Paramètres > Préférences** et décochez toutes les options de la case.

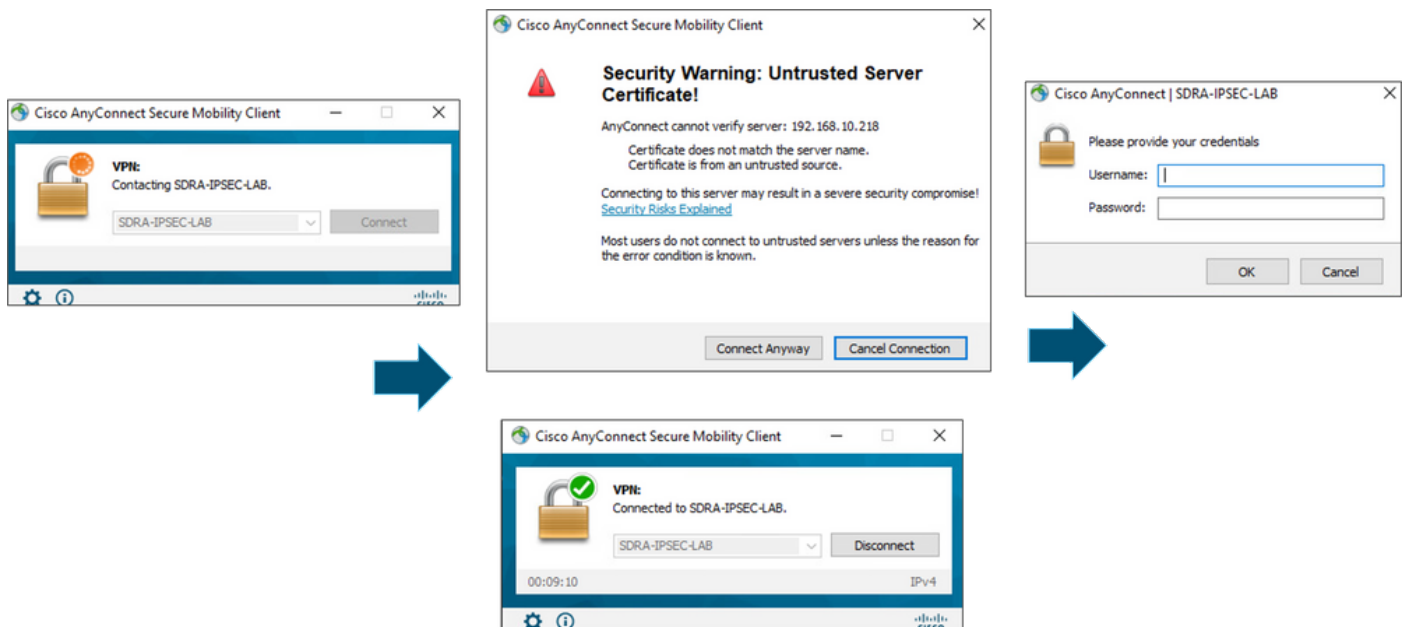
Le plus important est le blocage “ **des connexions aux serveurs non approuvés** ” pour ce scénario.

**Note:** Le certificat utilisé pour l'authentification tête de réseau/cEdge est celui précédemment créé et signé par le serveur AC dans Cisco IOS® XE. Comme ce serveur AC n'est pas une entité publique comme GoDaddy, Symantec, Cisco, etc. Le client PC interprète le certificat comme un serveur non approuvé. Ceci est corrigé à l'aide d'un certificat public ou d'un serveur d'autorité de certification auquel votre société fait confiance.



## Utiliser le client AnyConnect

Une fois que la configuration SDRA est placée, le flux pour une connexion réussie est affiché comme image.



## Vérification

L'interface de modèle virtuel est utilisée pour créer l'interface d'accès virtuel pour démarrer un canal de chiffrement et établir des associations de sécurité (SA) IKEv2 et IPsec entre le serveur (cEdge) et le client (utilisateur AnyConnect).

**Note:** L'interface de modèle virtuel est toujours up/down. L'état est activé et le protocole est désactivé.

```
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
```

Vérifiez la configuration réelle appliquée à l'interface d'accès virtuel associée au client avec **show external-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
```

Vérifiez les associations de sécurité IPsec (SA) pour le client AnyConnect avec la commande **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...
```

Vérifiez les paramètres de SA IKEv2 pour la session, le nom d'utilisateur et l'adresse IP attribuée.

**Note:** L'adresse IP attribuée doit correspondre à l'adresse IP du côté client AnyConnect.

```
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
```

## Informations connexes

- [Accès à distance Cisco SD-WAN](#)
- [Configuration du serveur FlexVPN](#)
- [Télécharger AnyConnect](#)
- [Support et documentation techniques - Cisco Systems](#)