AnyConnectおよびISEサーバでのSD-WANリモートアクセス(SDRA)の設定

内容

概要

このドキュメントでは、Cisco IOS® XE AutonomousモードをCAサーバとして使用するAnyConnectクライアントと、認証、許可、アカウンティング用のCisco Identity Services Engine(ISE)サーバを使用するSD-WANリモートアクセス(SDRA)の)の)の設定方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-defined Wide Area Network(SD-WAN)
- 公開キー インフラストラクチャ（PKI）
- FlexVPN
- RADIUS サーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.07.01a
- vManageバージョン20.7.1
- CSR1000Vバージョン17.03.04.a
- ISEバージョン2.7.0.256
- AnyConnectセキュアモビリティクライアントバージョン4.10.04071

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

リモートアクセスVPNとは何ですか。

リモートアクセスVPNを使用すると、リモートユーザは会社のネットワークに安全に接続し、アプリケーションを使用して、オフィスに接続されたデバイスからのみアクセスできるデータを使用できます。

リモートアクセスVPNは、従業員のデバイスと会社のネットワークの間に作成された仮想トンネルによって動作します。

このトンネルはパブリックインターネットを通過しますが、送受信されるデータは暗号化およびセキュリティプロトコルによって保護され、プライベートで安全な状態に保たれます。

このタイプのVPNの2つの主要コンポーネントは、ネットワークアクセスサーバ/RAヘッドエンドとVPNクライアントソフトウェアです。

SD-WANリモートアクセスVPNとは何ですか。

リモートアクセスはSD-WANソリューションに統合されており、Cisco SD-WANとRAインフラストラクチャを個別に必要とせず、Cisco AnyConnectをRAソフトウェアクライアントとして使用することで、RAサービスの迅速な拡張性を実現します。

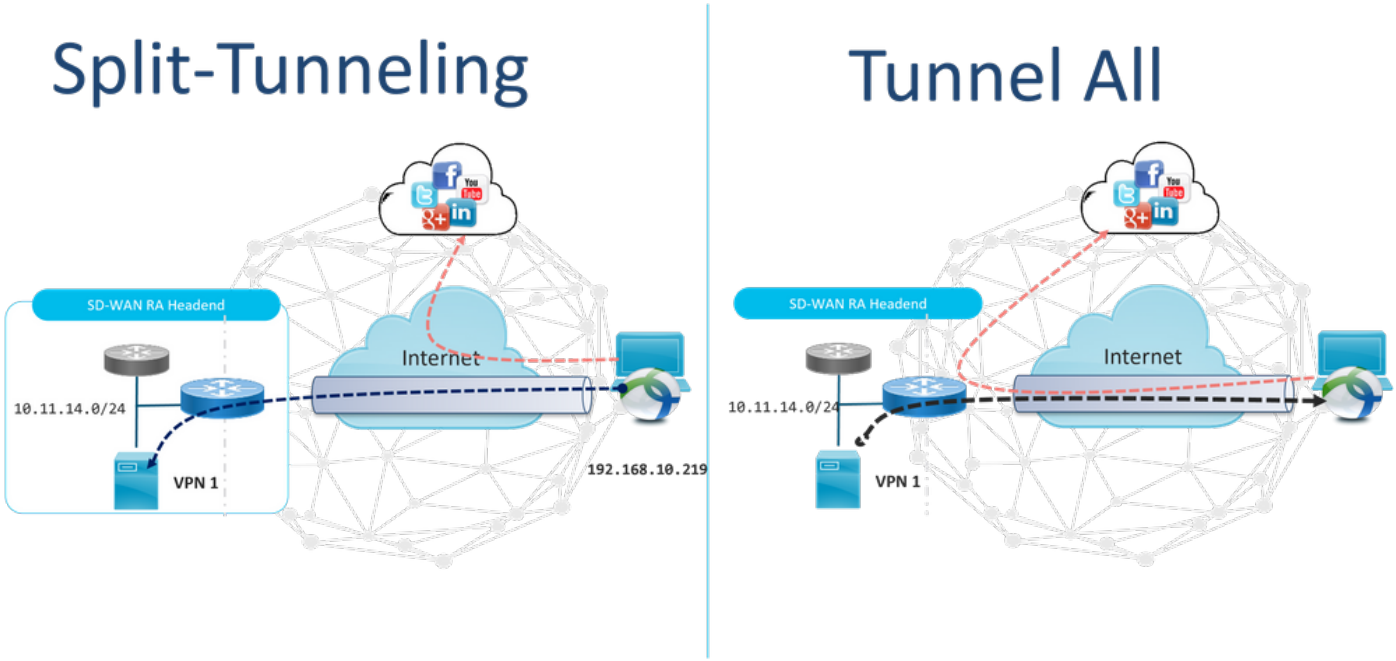
リモートアクセスは、リモートユーザが組織のネットワークにアクセスできるようにします。これにより、自宅からの作業が可能になります。

利点

- RAは、リモートロケーションのデバイス/ユーザから組織のネットワークにアクセスできるようにします。(HO)
- 各RAユーザのデバイスがCisco SD-WANファブリックの一部である必要なく、Cisco SD-WANソリューションをRAユーザに拡張
- データセキュリティ
- スプリットトンネリングまたはTunnel All
- 拡張性
- Cisco SD-WANファブリック内の多数のCisco IOS® XE SD-WANデバイスにRA負荷を分散する機能。

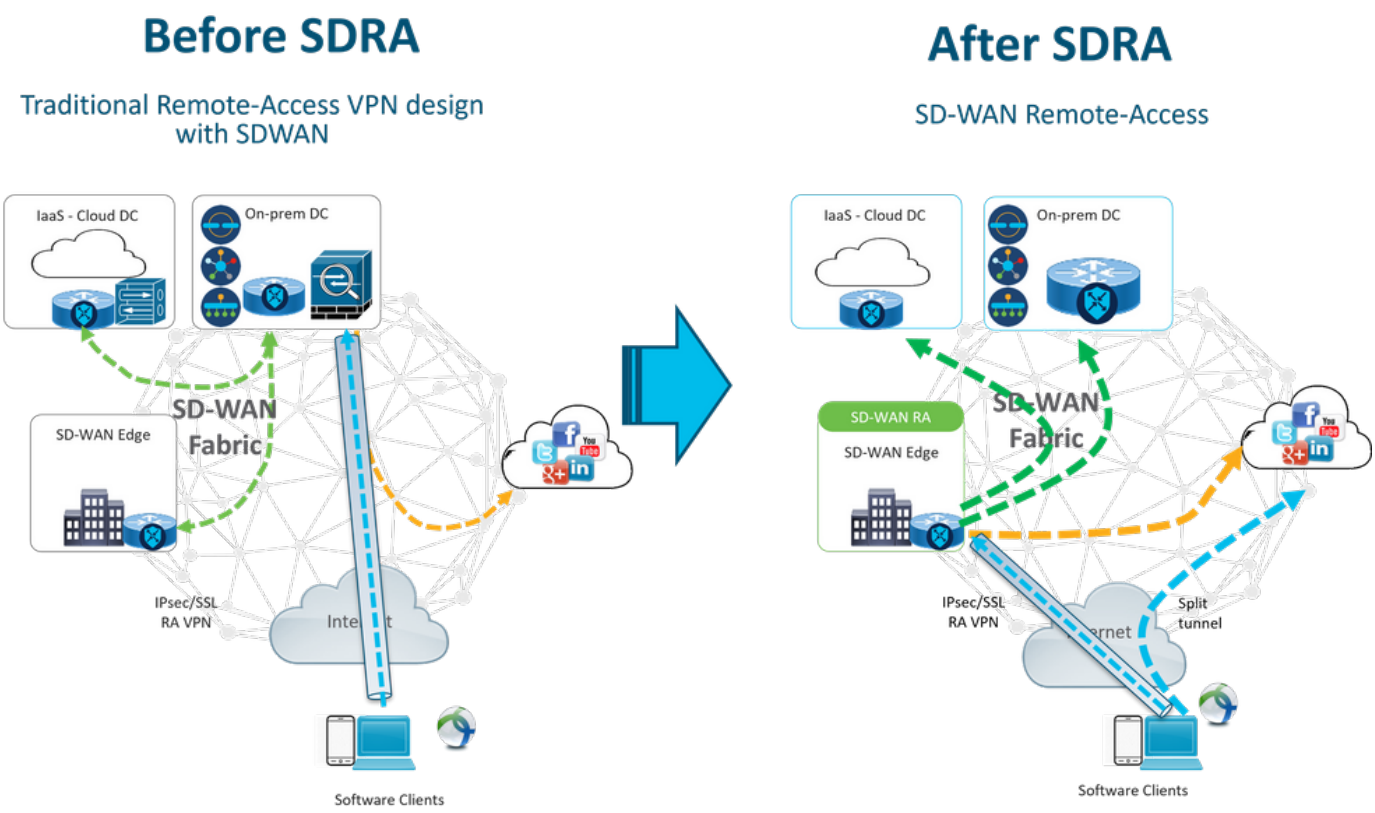
スプリットトンネリングとTunnel All

図に示すように、スプリットトンネリングは、特定のトラフィックだけをトンネリングする必要があるシナリオ（SD-WANサブネットなど）で使用されます。



SDRAの前とSDRAの後

従来のリモートアクセスVPN設計では、ASA、通常のCisco IOS® XE、またはサードパーティ製デバイスなどの非SD-WANアプライアンスのようなネットワークへのリモートアクセスを提供するために、Cisco SD-WANファブリックの外部に個別のRAインフラストラクチャが必要です。



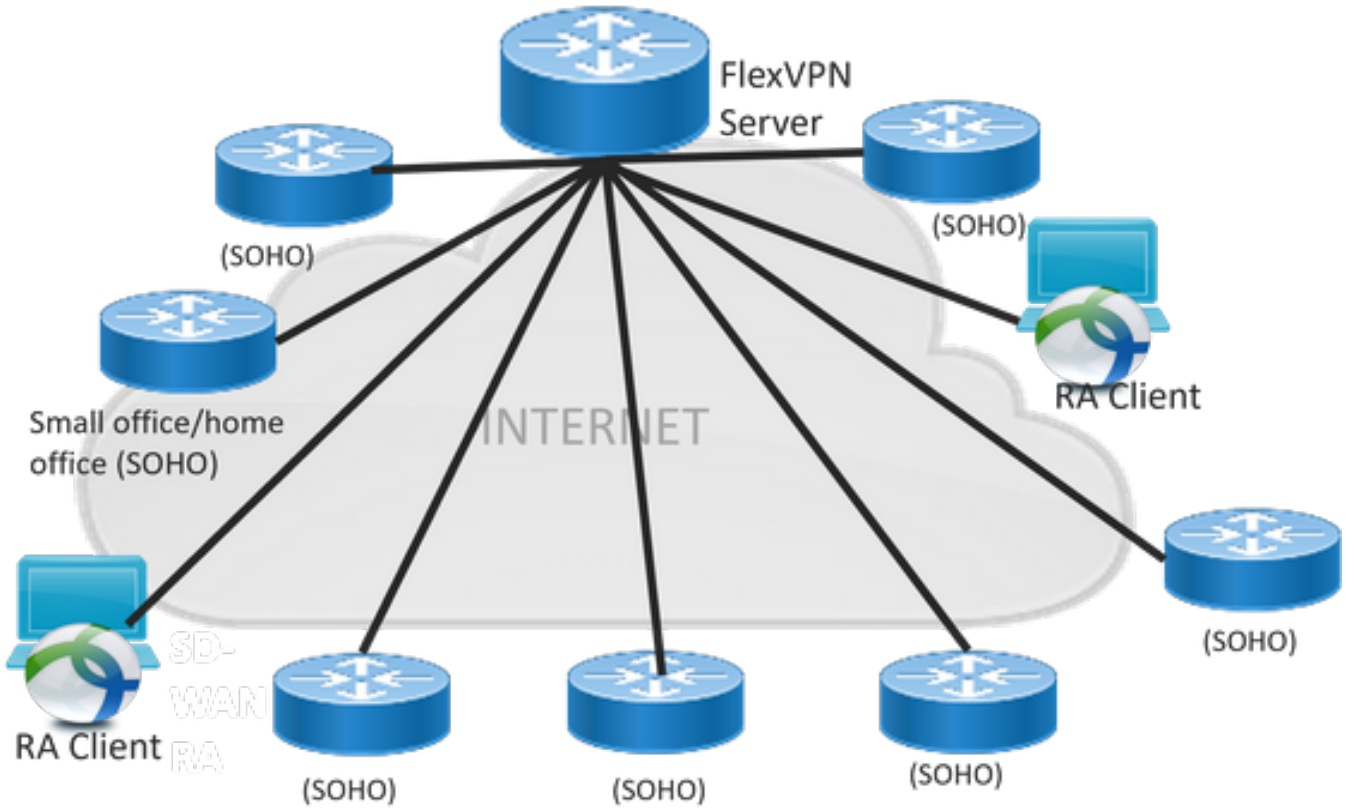
SD-WANリモートアクセスは、リモートユーザがネットワークに接続する方法を変更します。これらはRAヘッドエンドとして使用されるcEdgeに直接接続されます。Cisco SD-WANの機能と利点をRAユーザに拡張RAユーザはブランチLAN側のユーザになります。

各RAクライアントに対して、SD-WAN RAヘッドエンドはRAクライアントにIPアドレスを割り当て、RAユーザが配置されるサービスVRF内の割り当てられたIPアドレスにスタティックホストルートを追加します。

スタティックルートは、RAクライアント接続のVPNトンネルを指定します。SD-WAN RAヘッドエンドは、OMPを使用してRAクライアントのサービスVRF内のスタティックIPをサービスVPN内のすべてのエッジデバイスにアドバタイズします。

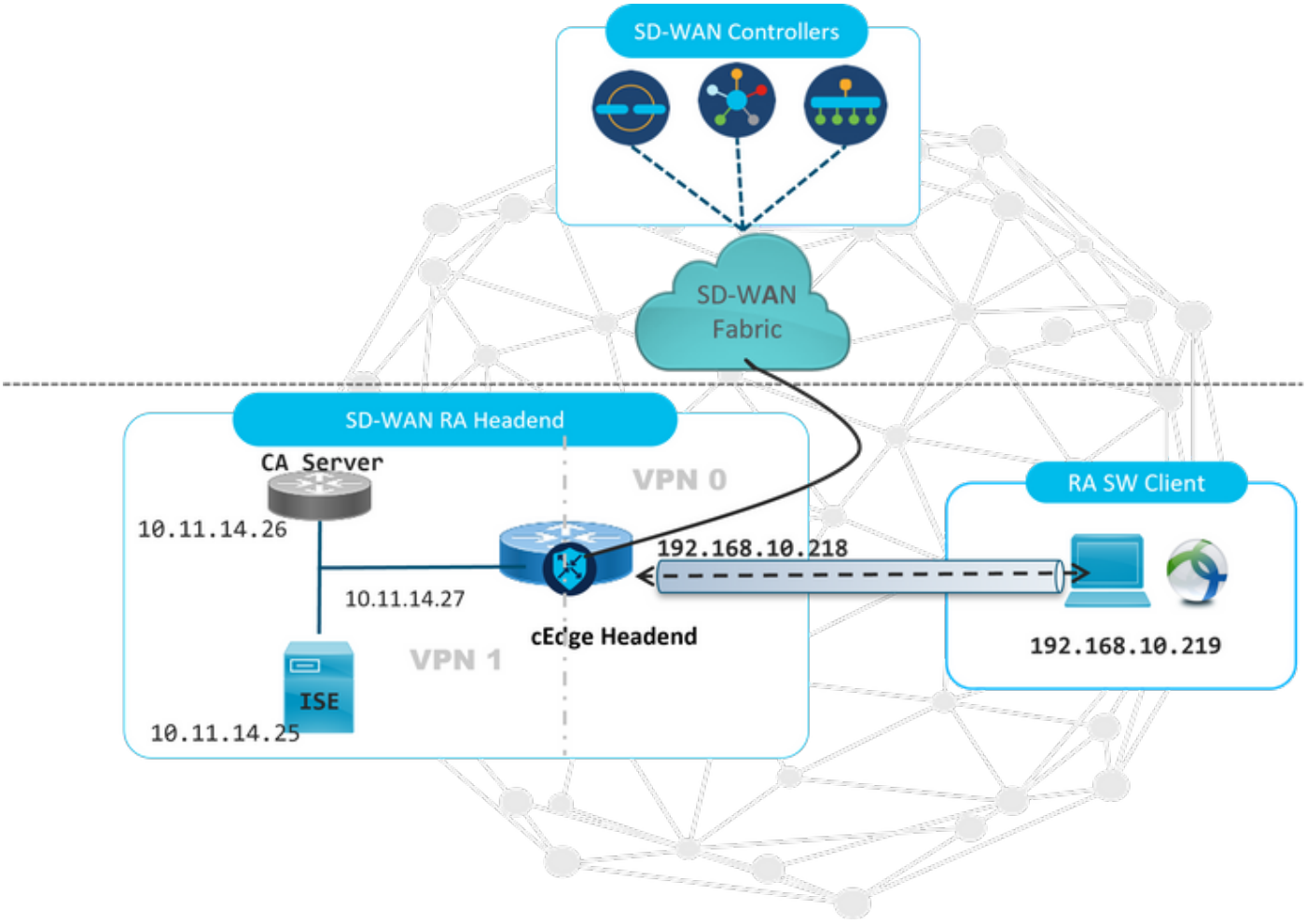
FlexVPNとは何ですか。

SD-WAN RAはCisco FlexVPN RAソリューションを活用します。FlexVPNは、シスコのIKEv2標準の実装で、サイト間、リモート**アクセス、ハブとスポークのトポロジ、および部分メッシュ（スポークからスポークへの直接）を結合する統合パラダイムおよびCLIを備えています。**
FlexVPNは、従来のVPN実装との互換性を維持しながら、トンネルインターフェイスのパラダイムを幅広く使用する、シンプルでモジュラ型のフレームワークを提供します。



前提条件の設定

この例では、図に示すように、SD-WAN RAラボのセットアップが作成されています。



このSD-WAN RAラボシナリオには、追加のコンポーネントが設定されています。

- Autonomousモードの通常のCisco IOS® XEをCAサーバとして使用。
- 認証、許可、アカウンティング用のISE/RADIUSサーバ。
- WANインターフェイス経由でcEdgeに到達できるWindows PC。
- AnyConnect Clientはすでにインストールされています。

注：CAサーバとRADIUSサーバは、サービスVRF 1に配置されています。 すべてのSD-WAN RAヘッドエンドのサービスVRFを介して両方のサーバに到達できる必要があります。

注：Cisco SD-WANリモートアクセスは、SDRAの17.7.1aバージョンと特定のデバイスでサポートされています。サポートされるデバイスの参照先：SD-WAN RAヘッドエンドでサポートされるプラットフォーム

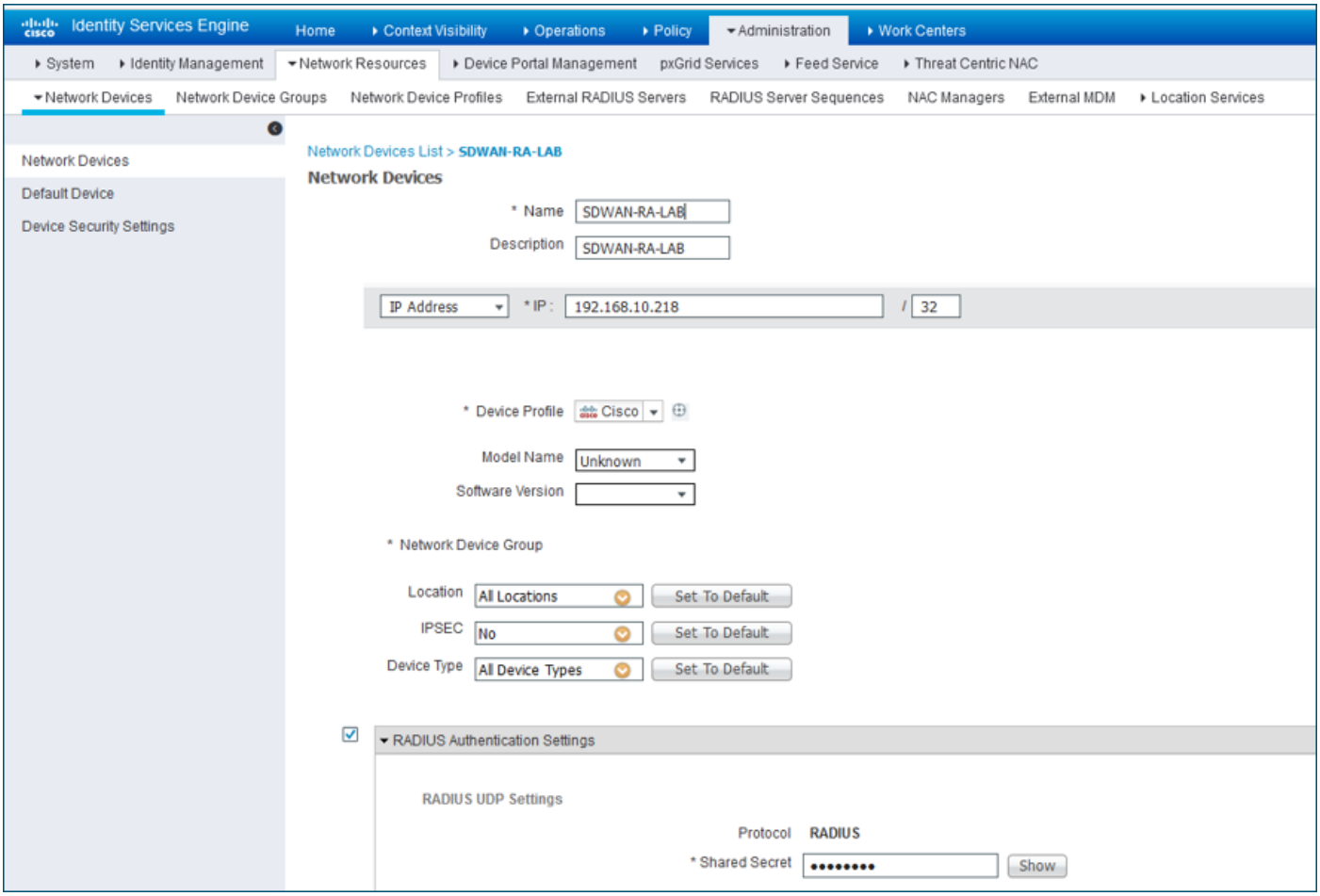
ISE の設定

SD-WAN RAヘッドエンドをサポートするには、RADIUSサーバでパラメータが設定されていることを確認します。RA接続には次のパラメータが必要です。

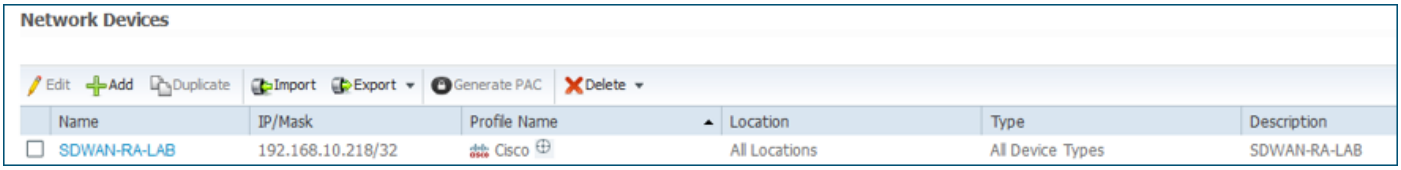
- ユーザ認証資格情報 AnyConnect-EAP接続用のユーザ名とパスワード
- ユーザまたはユーザグループに適用されるポリシーパラメータ（属性）**VRF:**RAユーザが割り当てられているサービスVPN**IPプール名**:RAヘッドエンドで定義されているIPプールの名前 **サーバサブネット**:RAユーザに提供するためのサブネットアクセス

ISEで設定する最初のステップは、ISEに対してRADIUS要求を実行できるネットワークデバイスとしてのRAヘッドエンドまたはcEdge IPアドレスです。

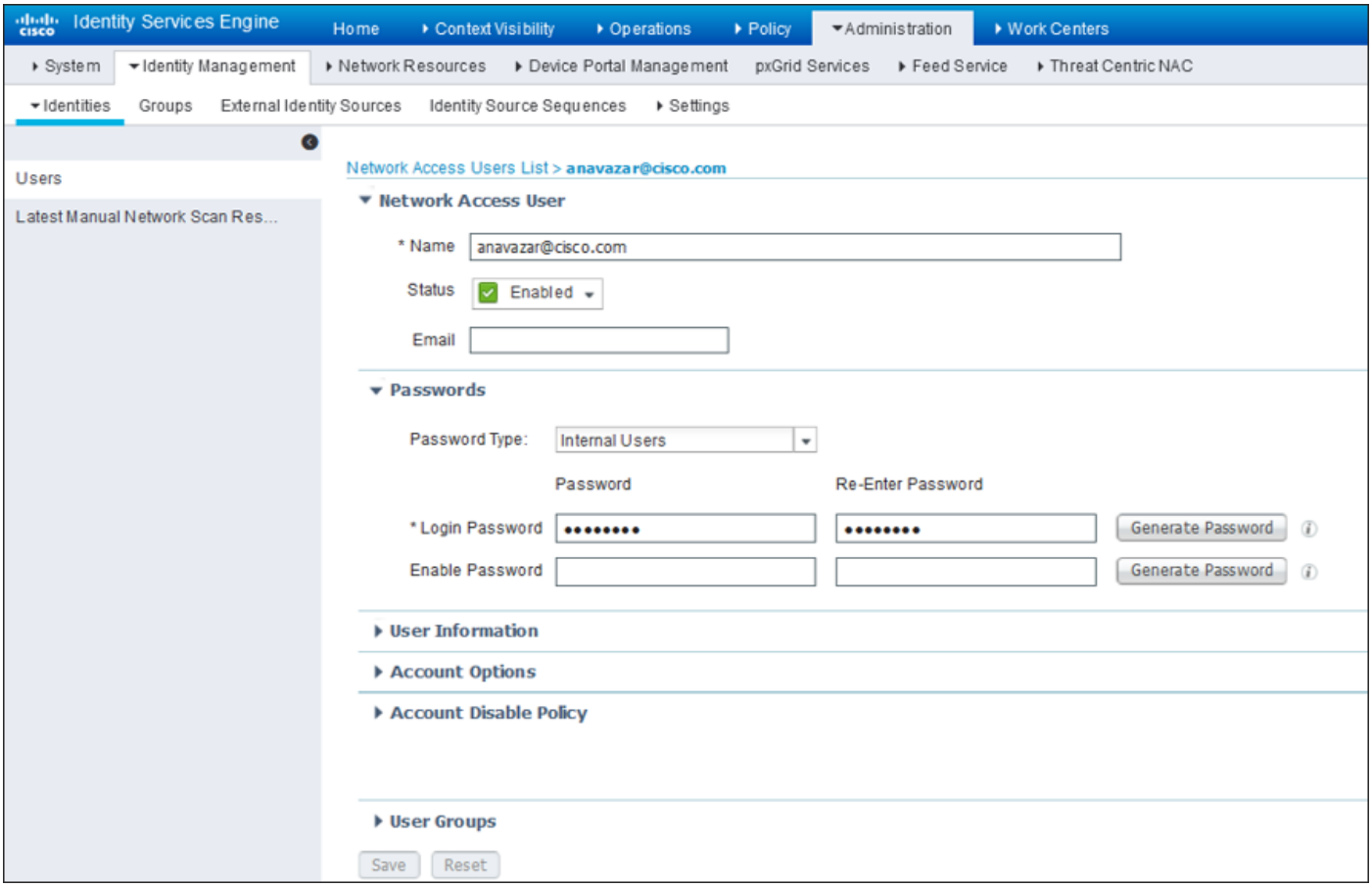
[Administration] > [Network Devices]に移動し、図に示すように、RAヘッド(cEdge)のIPアドレスとパスワードを追加します。



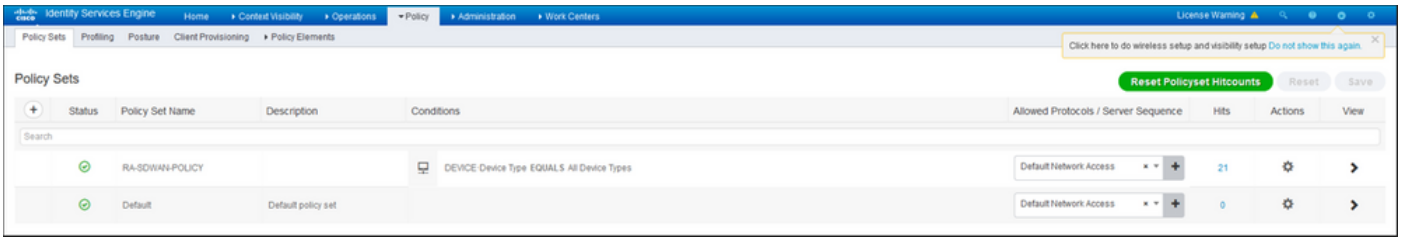
図に示すように、ネットワークデバイスが追加されました。



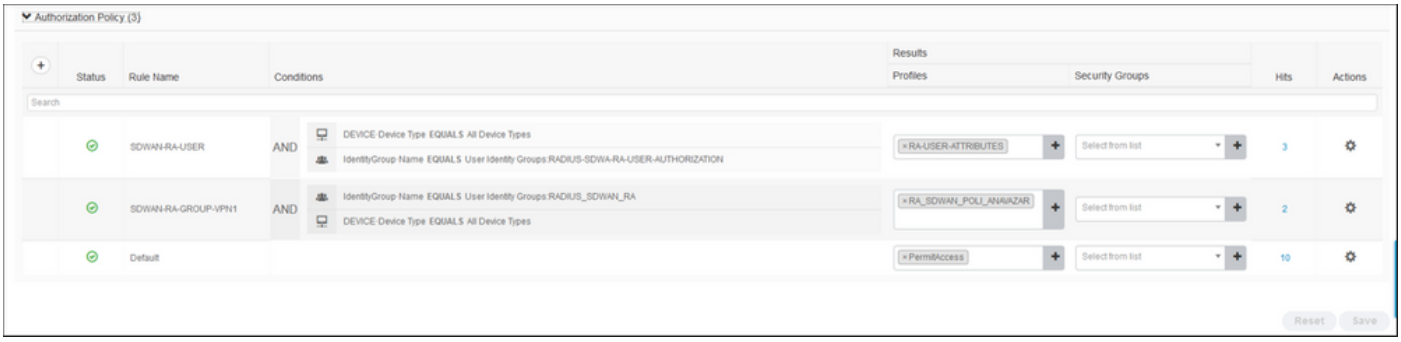
RADIUSサーバでは、図に示すように、AnyConnect認証のユーザ名とパスワードを設定する必要があります。[Administration] > [Identities]に移動します。



図に示すように、一致する条件を含むポリシーセットを作成する必要があります。この場合、すべてのデバイスタイプの条件**が使用され**ます。これは、すべてのユーザがこのポリシーにヒットすることを意味します。



次に、認可ポリシーが条件ごとに1つ作成されます。条件**All Device types**とIdentity groups to match.

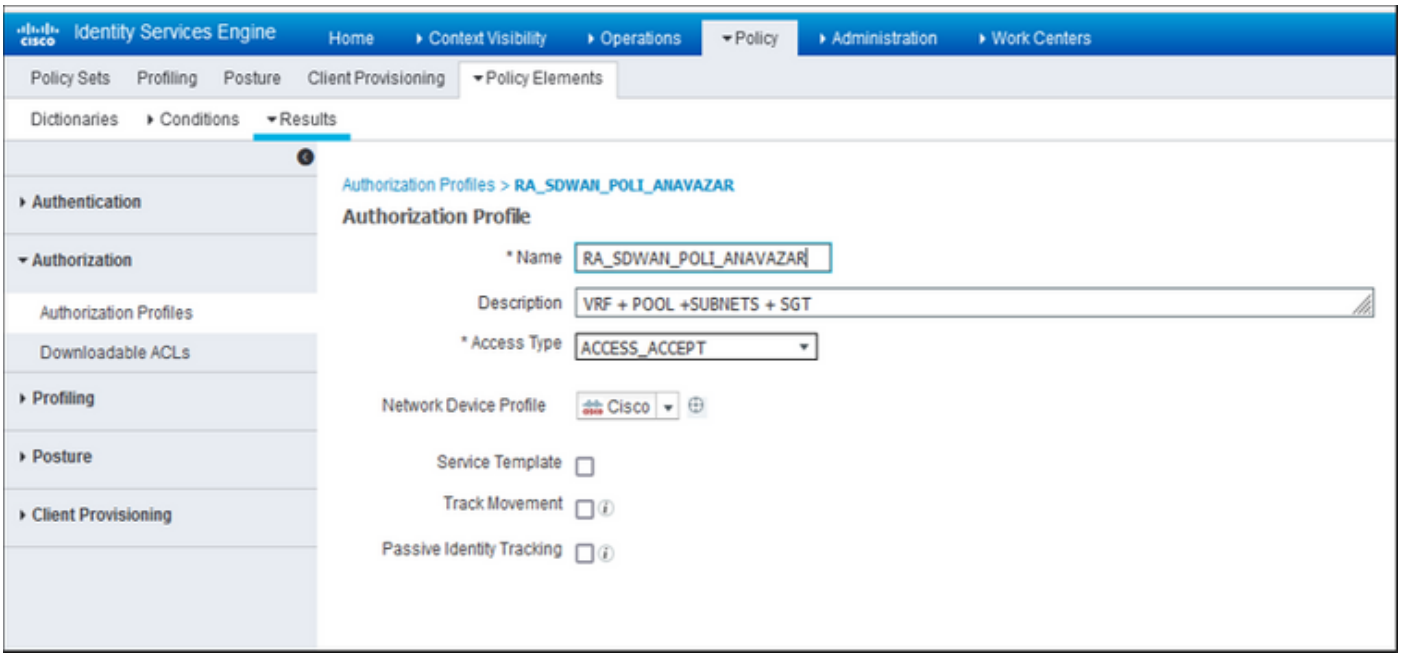


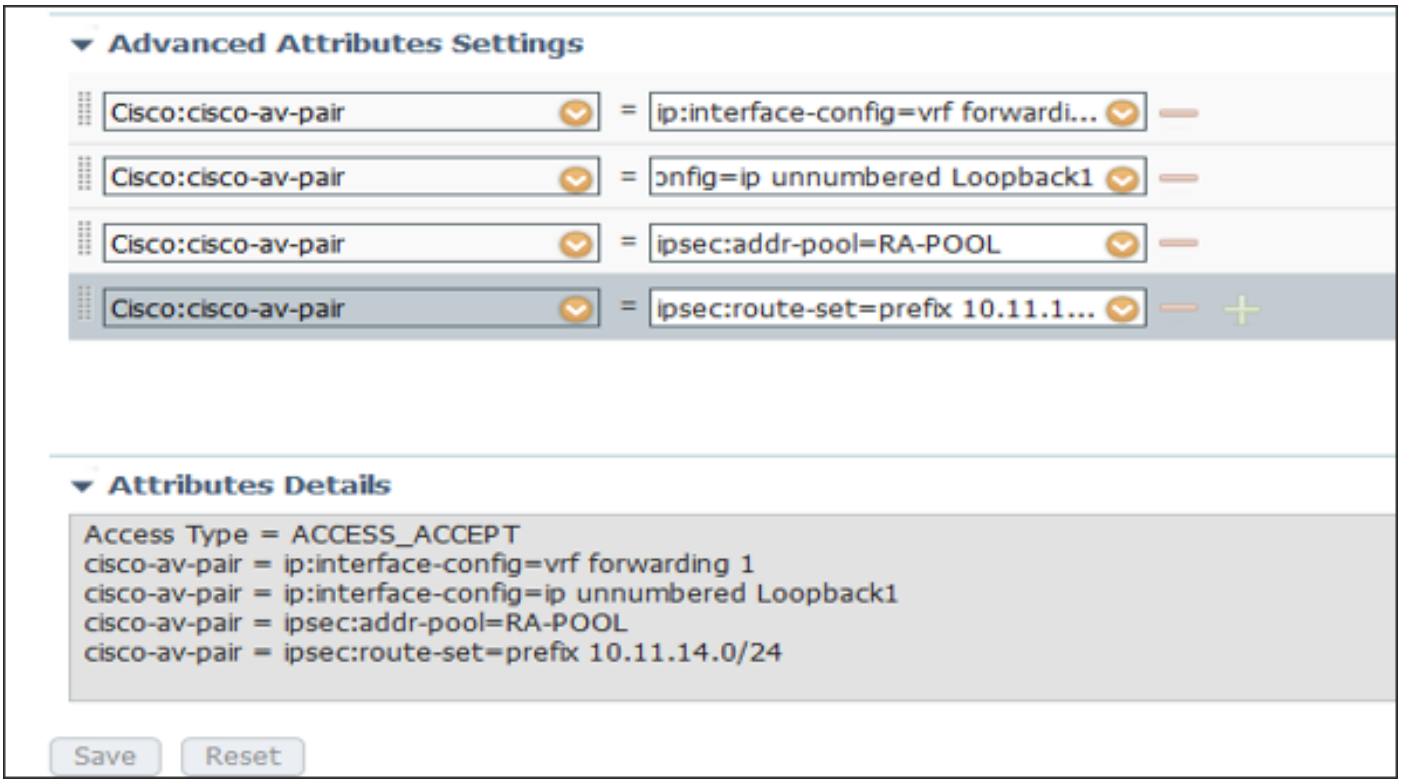
[Authorization Profile] で、[Advanced Attributes Settings] の[Access Type] を[Access_ACCEPT] に設定し、[Cisco vendor]属性と[Cisco-AV-pair]属性を選択する必要があります。

ユーザのポリシーパラメータを設定する必要があります。

- ユーザが属するサービスVRF。
- 各ユーザ接続のIPプール名にはIPアドレスが割り当てられます。このIPアドレスは、cEdgeで設定されたIPプールに属しています。
- ユーザがアクセスできるサブネット

注意： ip vrf forwarding コマンドは ip unnumbered コマンドよりも前に位置している必要があります。仮想アクセス インターフェイスが仮想テンプレートから複製され、その後 ip vrf forwarding コマンドが適用されると、仮想アクセス インターフェイスからすべての IP 設定が削除されます。





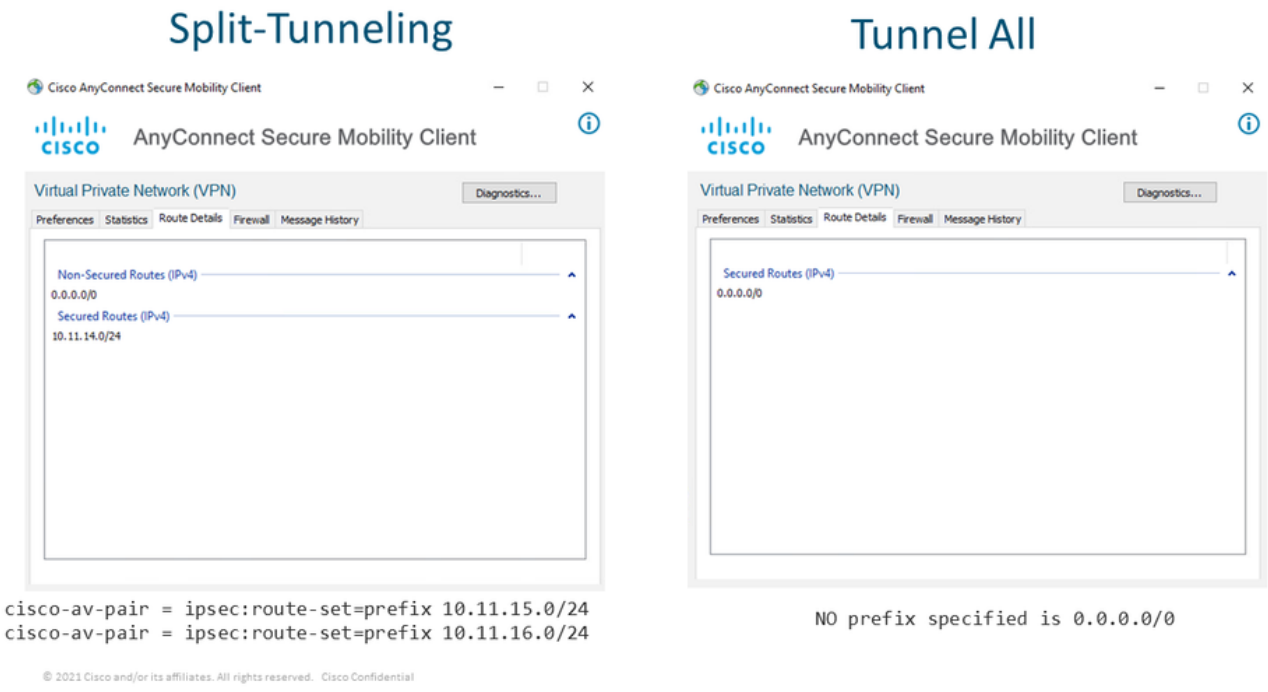
ユーザ属性：

```
Access Type = ACCESS_ACCEPT
```

```
cisco-av-pair = ip:interface-config=vrf forwarding 1
cisco-av-pair = ip:interface-config=ip unnumbered Loopback1
cisco-av-pair = ipsec:addr-pool=RA-POOL
cisco-av-pair = ipsec:route-set=prefix 10.11.15.0/24
cisco-av-pair = ipsec:route-set=prefix 10.11.16.0/24
```

AnyConnectクライアントでのスプリットトンネリングとTunnel All

AnyConnectクライアントで受信したipsec:route-set=prefix属性は、図に示すようにインストールされます。



Cisco IOS® XEにおけるCAサーバの設定

CAサーバは、Cisco IOS® XE SD-WANデバイスに証明書をプロビジョニングし、RAヘッドエンドがRAクライアントに対して自身を認証できるようにします。

Cisco IOS® XE SD-WANでは次のcrypto PKI serverコマンドがサポートされていないため、CEDGEをCAサーバにすることはできません。

- RSA キーペアを生成する
- CAサーバのPKIトラストポイントを作成します 以前に生成したKEY-CAを使用してrsakeypairを設定します。

  注：PKIサーバとPKIトラストポイントは同じ名前を使用する必要があります。

- CAサーバの作成 CAサーバのissuer-nameの設定「No shutdown」を使用してCAサーバをアクティブにします

```
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
!
```

CAサーバが有効になっているかどうかを確認します。

```
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
```

CAサーバ証明書がインストールされているかどうかを確認します。

```
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
```

CA証明書**のフィンガープリントSHA 1**は、リモートアクセス構成のcEdgeルータ（RAヘッドエンド）のcrypto pki trustpointで使用されます。

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

SD-WAN RAの設定

> **注**：このドキュメントでは、コントローラおよびcEdgeのSD-WANオンボーディングプロセスについては説明しません。SD-WANファブリックが稼働しており、完全に機能していることを前提としています。

Crypto PKIの設定

- PKIトラストポイントを作成します。
- CAサーバのURLを設定します。
- CAサーバ証明書からフィンガープリントsha 1をコピーします。
- 新しいID証明書の[Subject Name]と[Alt Name]を設定します。
- 以前に生成したKEY-IDを使用してrsakeypairを設定します。

```
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
```

認証するCA証明書を要求します。

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

CSRを生成し、CAサーバに送信し、新しいアイデンティティ証明書を受信します。

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

CA証明書とcEdge証明書を確認します。

```
cEdge-207#show crypto pki certificates RA-TRUSTPOINT
Certificate
 Status: Available
```

```
 Certificate Serial Number (hex): 04
 Certificate Usage: General Purpose
 Issuer:
   cn=CSR1Kv_SDWAN_RA
 Subject:
   Name: cEdge-207
   hostname=cEdge-207
   cn=cEdge-SDWAN-1.crv
 Validity Date:
   start date: 03:25:40 UTC Jan 24 2022
   end   date: 03:25:40 UTC Dec 3 2031
 Associated Trustpoints: RA-TRUSTPOINT
 Storage: nvram:CSR1Kv_SDWAN#4.cer
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CSR1Kv_SDWAN_RA
 Subject:
   cn=CSR1Kv_SDWAN_RA
 Validity Date:
   start date: 23:15:33 UTC Jan 19 2022
   end   date: 23:15:33 UTC Jan 17 2032
 Associated Trustpoints: RA-TRUSTPOINT
Storage: nvram:CSR1Kv_SDWAN#1CA.cer
```

AAA 設定

```
aaa new-model
!
aaa group server radius ISE-RA-Group
 server-private 10.11.14.225 key Cisc0123
 ip radius source-interface GigabitEthernet2
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
```

FlexVPN の設定

IPプールの設定

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

IKEv2プロポーザル（暗号とパラメータ）とポリシーを設定します。

```
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
```

IKEv2プロファイル名マネージャを設定します。

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

注：name-manglerは、プレフィックスとサフィックスを区切るEAPアイデンティティ（ユーザ名）で区切られたEAPアイデンティティのプレフィクスから名前を取得します。

IPsec暗号を設定します。

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

Crypto IKEv2プロファイルを設定します。

```
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
```

暗号化IPSECプロファイルを設定します。

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

バーチャルテンプレートインターフェイスの設定：

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

暗号化IKEv2プロファイルの仮想テンプレートの設定：

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

SD-WAN RAの設定例

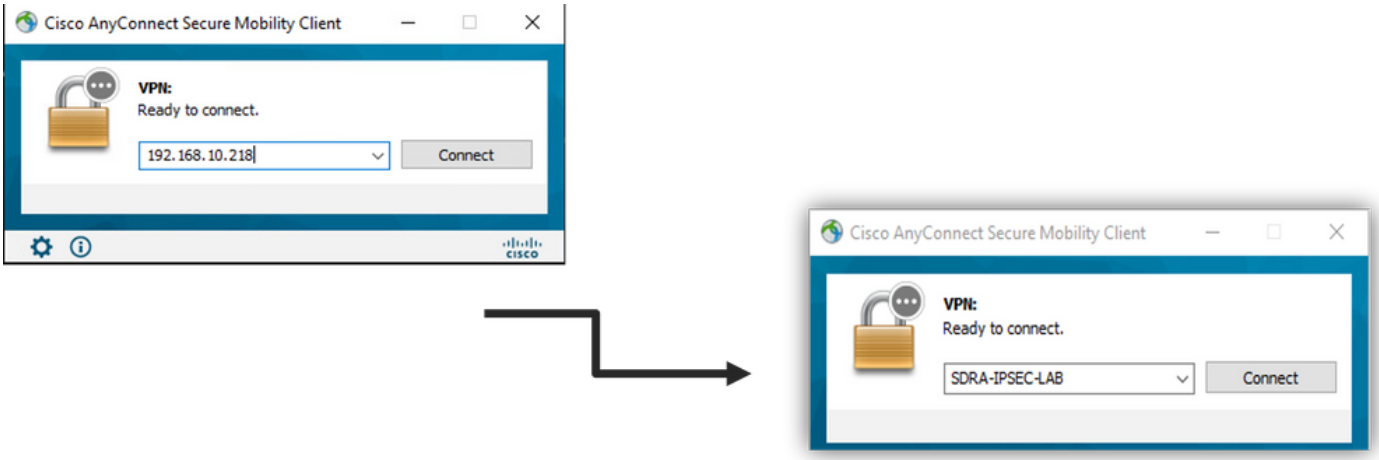
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
```

```
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
!
crypto pki trustpoint RA-TRUSTPOINT
 subject-name CN=cEdge-SDWAN-1.crv
 enrollment url http://10.11.14.226:80
 fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
 subject-name CN=cEdge-SDWAN-1.crv
 vrf 1
 rsakeypair KEY-NEW
 revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap suffix delimiter @
!
crypto ikev2 proposal IKEV2-RA-PROP
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256
!
crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
!
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 match identity remote any
 identity local address 192.168.10.218
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint RA-TRUSTPOINT
 aaa authentication anyconnect-eap ISE-RA-Authentication
 aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
 aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
 aaa accounting anyconnect-eap ISE-RA-Accounting
!
crypto ipsec profile IKEV2-RA-PROFILE
 set transform-set IKEV2-RA-TRANSFORM-SET
 set ikev2-profile RA-SDWAN-IKEV2-PROFILE
!
interface Virtual-Template101 type tunnel
 vrf forwarding 1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IKEV2-RA-PROFILE
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 virtual-template 101
```

AnyConnectクライアントの設定

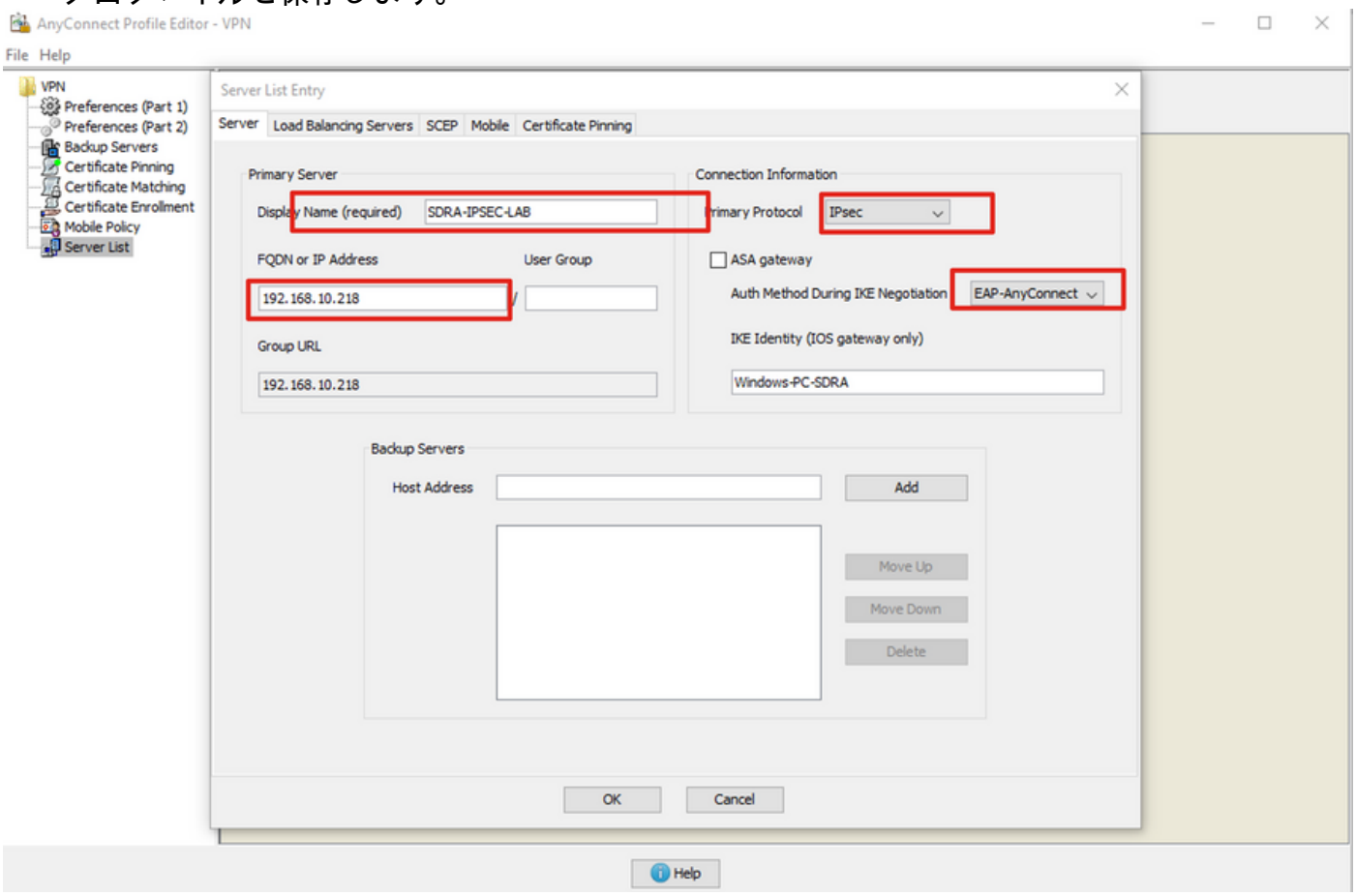
AnyConnectクライアントは、トンネル確立のデフォルトプロトコルとしてSSLを使用し、このプロトコルはSD-WAN RA（ロードマップ）ではサポートされません。RAはFlexVPNを使用するため、IPSECが使用されるプロトコルであり、変更が必須であり、これはXMLプロファイルを使用して行われます。

ユーザは、AnyConnectクライアントのアドレスバーに、VPNゲートウェイのFQDNを手動で入力できます。これにより、ゲートウェイへのSSL接続が確立されます。



AnyConnectプロファイルエディタの設定

- [Server List]に移動し、**[Add]をクリックします。**
- [IPsec]**を[**Primary Protocol]として選択します。
- ASAゲートウェイのオプ**ションをオフ**にします。
- [Auth Method During IKE Negotiation]で[EAP-AnyConnect]を選択します。
- [Display/**Name (Required)] は、AnyConnectクライアントでこの接続を保存するために使用する名前です。**
- **FQDNまたはIPアドレスは、**cEdge（パブリック）IPアドレスで入力する必要があります。
- プロファイルを保存します。



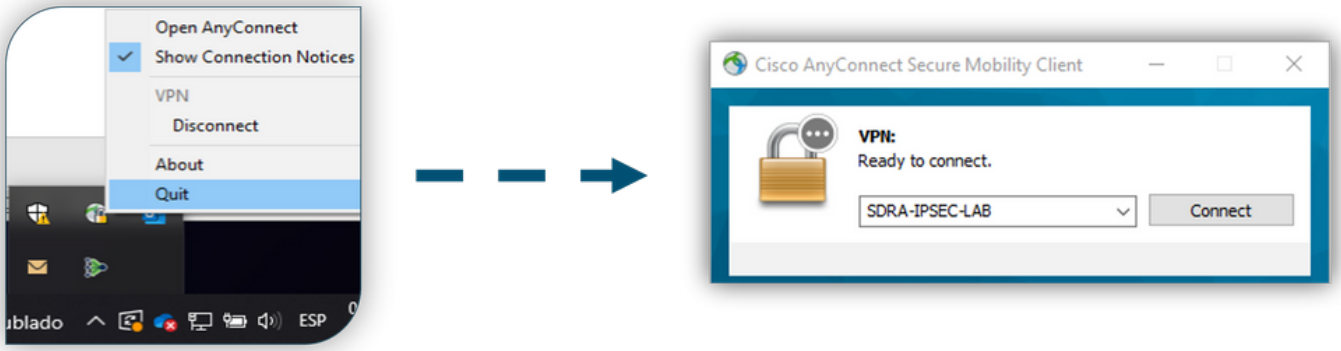
AnyConnectプロファイル(XML)のインストール

XMLプロファイルは、手動でディレクトリに配置できます。

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

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

プロファイルがGUIに表示されるようにするには、AnyConnectクライアントを再起動する必要があります。Windowsトレイの[AnyConnect]アイコンを右クリックし、[Quit]オプションを選択することで、プロセスを再起動できます。



AnyConnectダウンローダの無効化

AnyConnectクライアントは、デフォルトで正常にログインした後、XMLプロファイルのダウンロードを試行します。

プロファイルが使用できない場合、接続は失敗します。回避策として、クライアント自体でAnyConnectプロファイルのダウンロード機能を無効にできます。

Windows の場合：

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

MAC OSの場合：

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

「BypassDownloader」オプションは「true」に設定されています。

```
<?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>
```

AnyConnectクライアントの信頼できないサーバのブロックを解除する

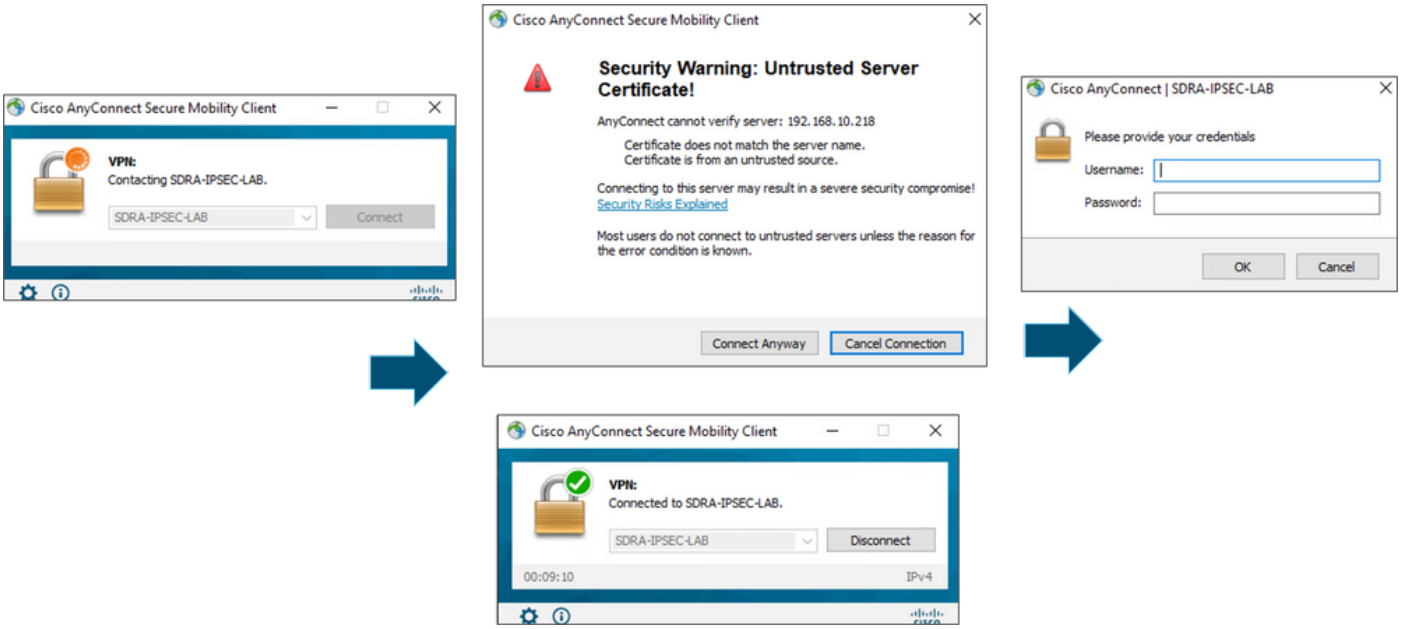
[Settings] > [Preferences]に移動し、すべてのボックスのオプションをオフにします。

最も重要な点は、このシナリオの「**信頼できないサーバへの接続をブロック**」です。

> **注**：RAヘッドエンド/cEdge認証に使用される証明書は、Cisco IOS® XEのCAサーバによって以前に作成され、署名されたものです。このCAサーバは、GoDaddy、Symantec、Ciscoなどのパブリックエンティティではないため、PCクライアントは、証明書を信頼できないサーバとして解釈します。これは、会社が信頼する公開証明書またはCAサーバを使用して修正されます。

AnyConnectクライアントの使用

すべてのSDRA設定が完了すると、接続が成功するためのフローが図に示されます。



確認

仮想テンプレートインターフェイスは、暗号化チャネルを開始し、サーバ(cEdge)とクライアント（ AnyConnectユーザ ）間でIKEv2およびIPsecセキュリティアソシエーション(SA)を確立するための仮想アクセスインターフェイスを作成するために使用されます。

> **注：仮想テンプレートインターフェイスは常にup/downです。Status is** up **and** Protocol is **down**.

```
cEdge-207#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES unset  up                    up
GigabitEthernet2       192.168.10.218  YES other  up                    up
GigabitEthernet3       10.11.14.227    YES other  up                    up
Sdwan-system-intf      10.1.1.18        YES unset  up                     up
Loopback1              192.168.50.1    YES other  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
NVI0                   unassigned      YES unset  up                    up
Tunnel2                192.168.10.218  YES TFTP   up                    up
Virtual-Access1        192.168.50.1    YES unset  up                    up
Virtual-Template101    unassigned      YES unset  up                    down
```

show derived-config interface virtual-access <number>を使用して、クライアントに関連付けられたバーチャルアクセスインターフェイスに適用された実際の設定を確認します。

```
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
```

AnyConnectクライアントのIPsecセキュリティアソシエーション(SA)を**show crypto ipsec sa peer <AnyConnect Public IP >で確認します。**

```
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….
```

セッション、ユーザ名、割り当てられたIPのIKEv2 SAパラメータを確認します。

> **注：**割り当てられたIPアドレスは、AnyConnectクライアント側のIPアドレスと一致している必要があります。

```
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
```

関連情報

- Cisco SD-WANリモートアクセス
- FlexVPNサーバの設定
- AnyConnectのダウンロード
- テクニカル サポートとドキュメント – Cisco Systems