使用AnyConnect和ISE伺服器配置SD-WAN遠端訪問(SDRA)

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[什麼是遠端訪問VPN?](#)
[什麼是SD-WAN遠端訪問VPN?](#)
[分割通道與所有通道](#)
[SDRA之前和SDRA之後](#)
[什麼是FlexVPN?](#)
[必要條件配置](#)
[ISE 組態](#)
[AnyConnect客戶端中的分割隧道與全部隧道](#)
[Cisco IOS® XE中的CA伺服器配置](#)
[SD-WAN RA配置](#)
[加密PKI配置](#)
[AAA組態](#)
[FlexVPN配置](#)
[SD-WAN RA配置示例](#)
[AnyConnect客戶端配置](#)
[配置AnyConnect配置檔案編輯器](#)
[安裝AnyConnect配置檔案(XML)](#)
[禁用AnyConnect下載程式](#)
[在AnyConnect客戶端上取消阻止不受信任的伺服器](#)
[使用AnyConnect客戶端](#)
[驗證](#)
[相關資訊](#)

簡介

本文檔介紹如何使用Cisco IOS® XE自主模式作為CA伺服器使用AnyConnect客戶端配置SD-WAN遠端訪問(SDRA)，並使用Cisco Identity Services Engine(ISE)伺服器進行身份驗證、授權和記帳。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- 公開金鑰基礎架構 (PKI)
- FlexVPN
- RADIUS伺服器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C8000V版本17.07.01a
- vManage版本20.7.1
- CSR1000V版本17.03.04.a
- ISE版本2.7.0.256
- AnyConnect安全行動化使用者端版本4.10.04071

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

什麼是遠端訪問VPN?

遠端訪問VPN允許遠端使用者安全地連線到公司網路、使用只能通過辦公室中外掛的裝置訪問的應用程式和資料。

遠端訪問VPN通過員工裝置和公司網路之間建立的虛擬隧道工作。

此隧道通過公共Internet，但通過它來回傳送的資料受加密和安全協定的保護，以幫助保持其私密性和安全性。

此類VPN中的兩個主要元件是網路接入伺服器/RA頭端和VPN客戶端軟體。

什麼是SD-WAN遠端訪問VPN?

遠端訪問已整合到SD-WAN解決方案中，不再需要單獨的Cisco SD-WAN和RA基礎設施，並且使用Cisco AnyConnect作為RA軟體客戶端實現RA服務的快速可擴充性。

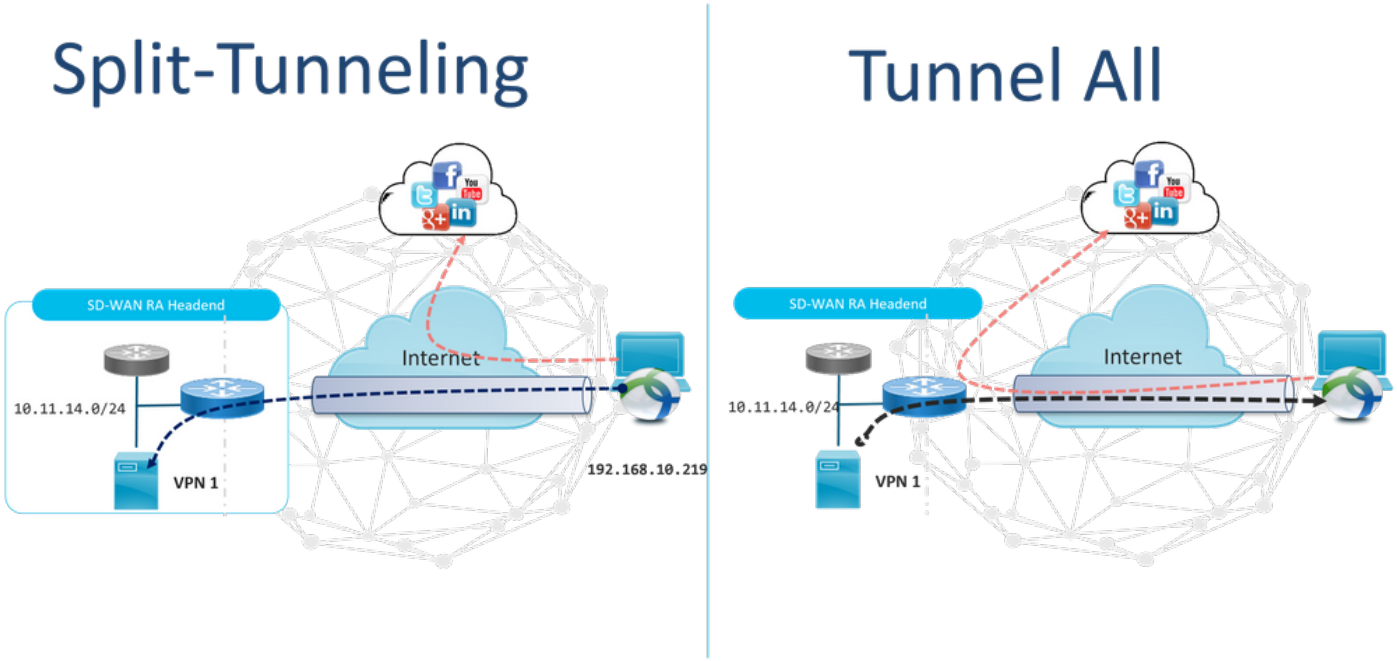
遠端訪問為遠端使用者提供對組織網路的訪問。這將啟用在家中的工作。

優勢

- RA提供從遠端位置的裝置/使用者訪問組織網路的許可權。(HO)
- 將Cisco SD-WAN解決方案擴展到RA使用者，無需每個RA使用者的裝置成為Cisco SD-WAN交換矩陣的一部分。
- 資料安全
- 分割通道或全部通道
- 可擴充性
- 能夠在Cisco SD-WAN交換矩陣中的多個Cisco IOS® XE SD-WAN裝置之間分配RA負載。

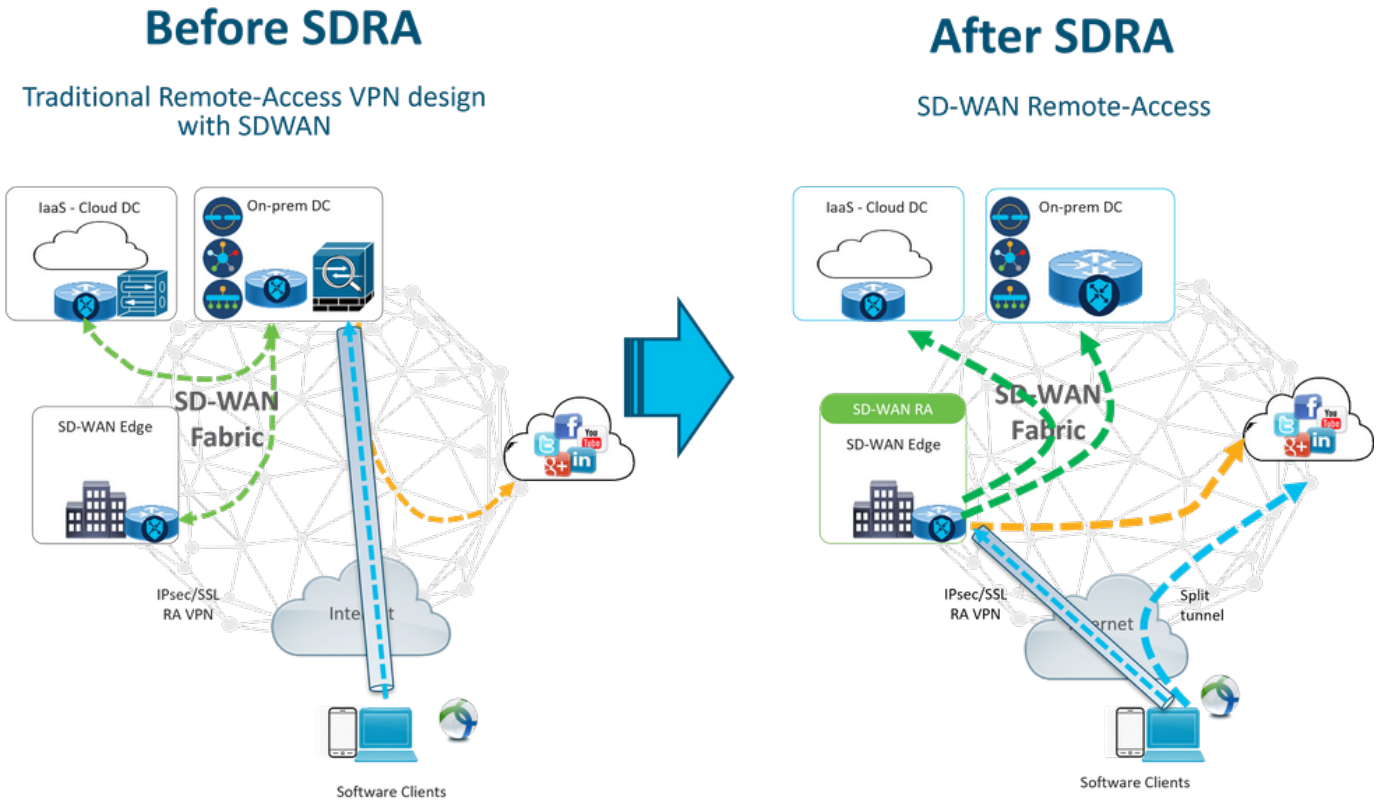
分割通道與所有通道

如圖所示，分割隧道用於只有特定流量必須進行隧道化的場景（例如SD-WAN子網）。



SDRA之前和SDRA之後

傳統的遠端訪問VPN設計要求在Cisco SD-WAN交換矩陣之外使用單獨的RA基礎設施，以便向遠端使用者提供對網路的訪問，如非SD-WAN裝置(如ASA、常規Cisco IOS® XE或第三方裝置)，並且RA流量會向前移動到SD-WAN裝置，如圖所示。



SD-WAN遠端訪問改變了遠端使用者連線到網路的方式。它們直接連線到用作RA頭端的cEdge。將

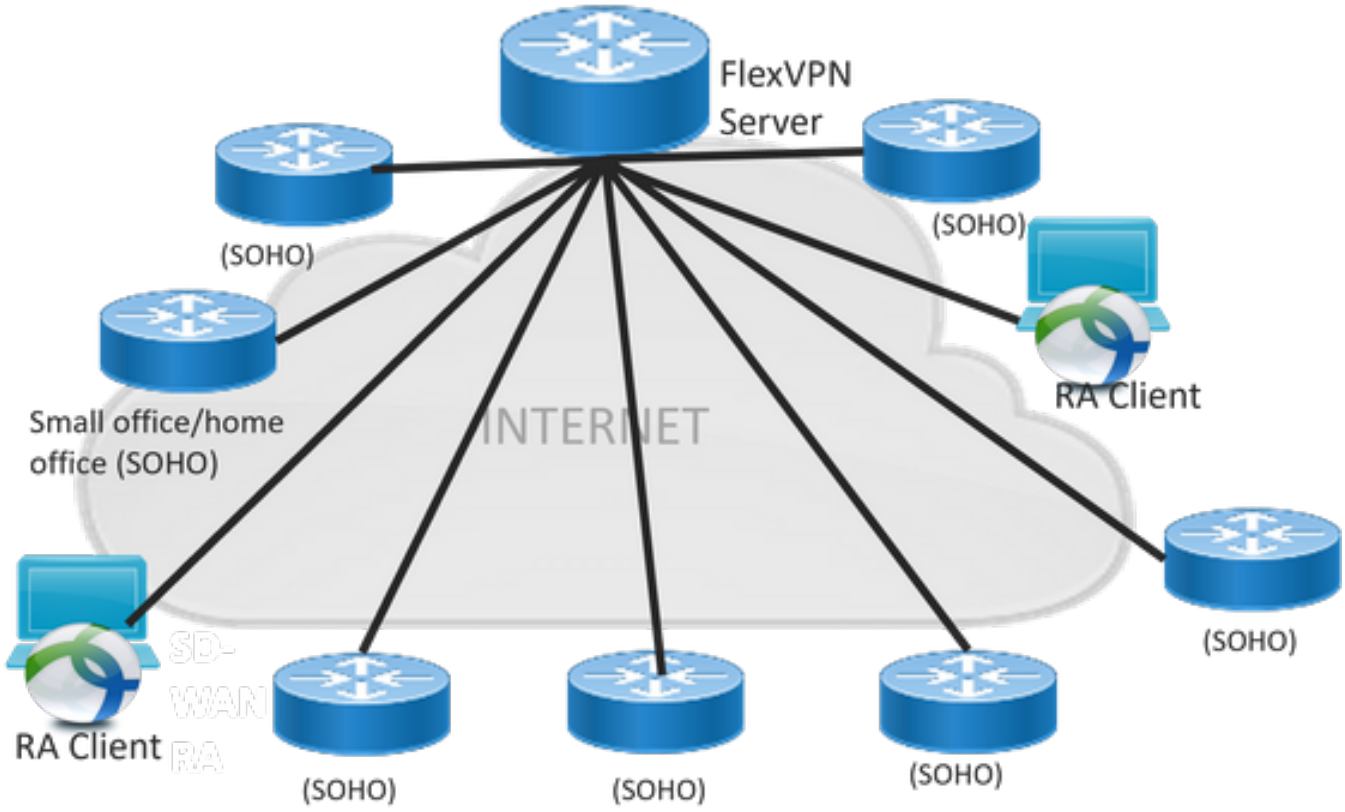
Cisco SD-WAN功能和優勢擴展到RA使用者。RA使用者成為分支機構LAN端使用者。

對於每個RA客戶端，SD-WAN RA頭端為RA客戶端分配IP地址，並將靜態主機路由新增到放置RA使用者的服務VRF中分配的IP地址。

靜態路由指定RA客戶端連線的VPN隧道。SD-WAN RA前端使用OMP將RA客戶端的服務VRF中的靜態IP通告給服務VPN中的所有邊緣裝置。

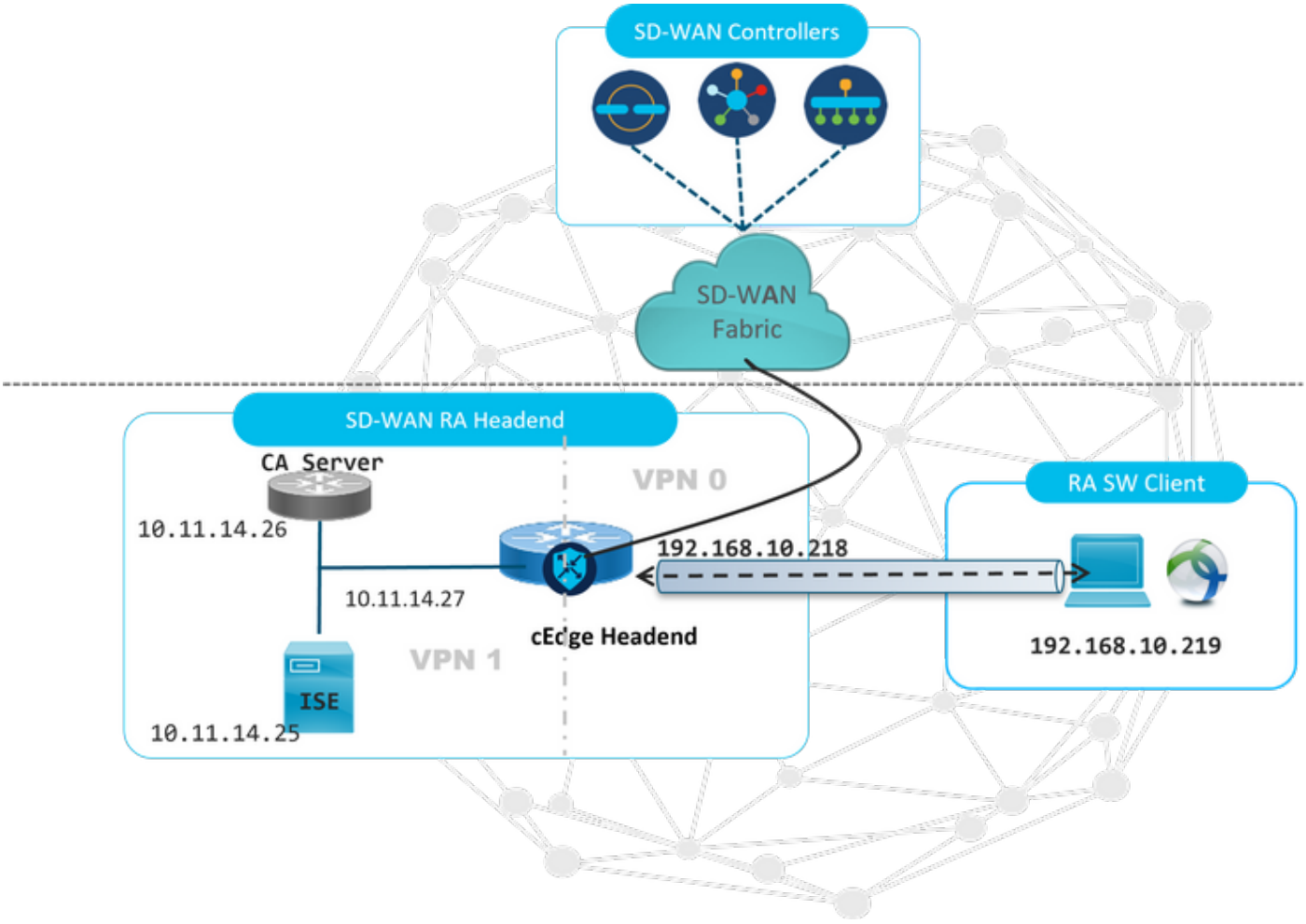
什麼是FlexVPN?

SD-WAN RA利用Cisco FlexVPN RA解決方案。FlexVPN是思科實施的IKEv2標準，其功能是一個統一的範例和CLI，將站點到站點、遠端訪**問、中心輻射型拓撲和部分網格（直接輻射型到輻射型）結合起**來。 FlexVPN提供簡單但模組化的框架，廣泛使用隧道介面模式，同時保持與傳統VPN實施相容。



必要條件配置

在本例中，已建立SD-WAN RA實驗設定，如下圖所示。



為此SD-WAN RA實驗場景配置了其他元件：

- 在自治模式下作為CA伺服器的常規Cisco IOS® XE。
- 用於身份驗證、授權和計費的ISE/Radius伺服器。
- 可通過WAN介面訪問cEdge的Windows PC。
- 已安裝AnyConnect客戶端。

附註：CA和RADIUS伺服器已置於服務VRF 1中。 兩台伺服器都必須通過所有SD-WAN RA前端的服務VRF訪問。

附註：17.7.1a版本和SDRA的特定裝置支援Cisco SD-WAN遠端訪問。有關支援的裝置參考，請導航至：SD-WAN RA頭端支援的平台

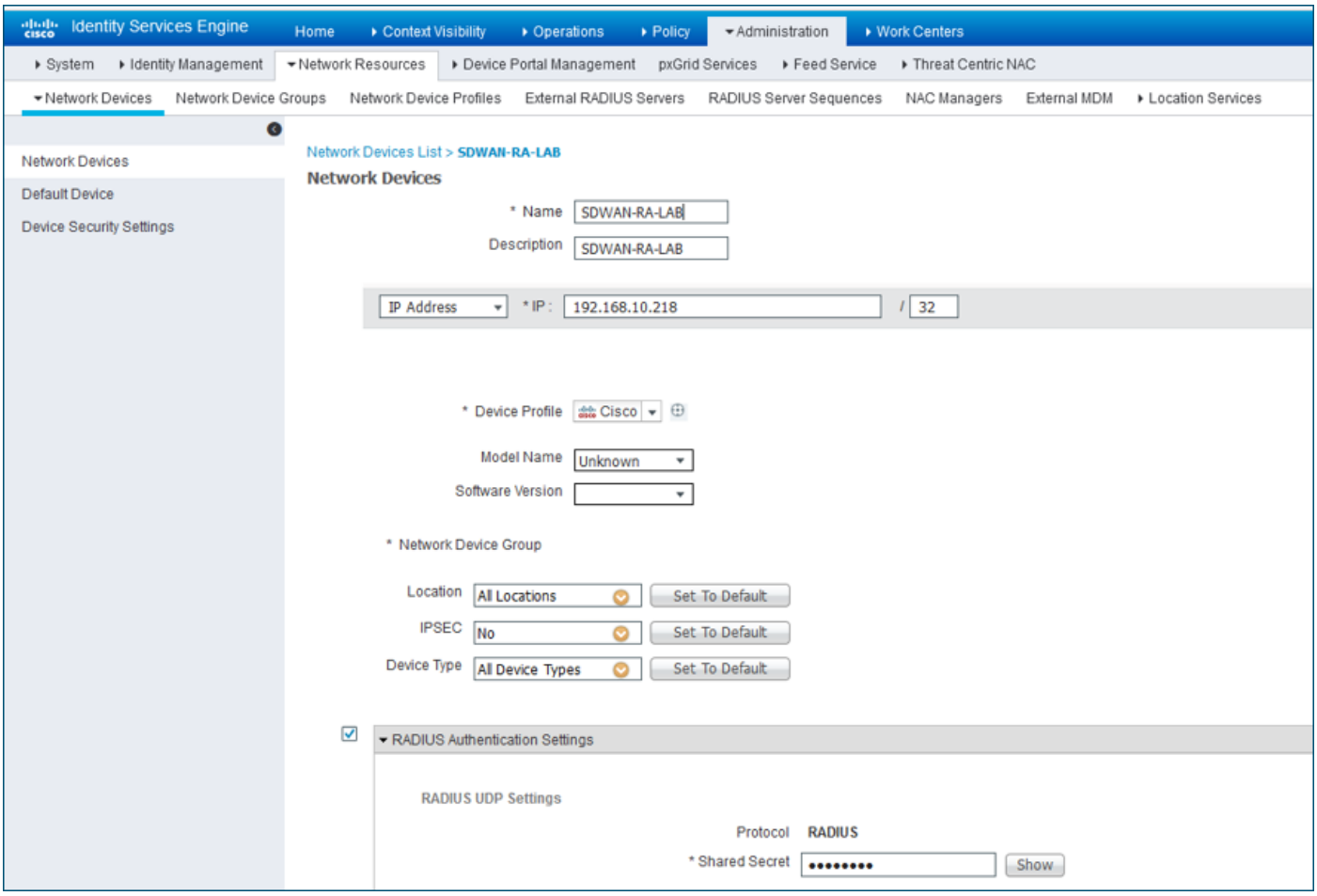
ISE 組態

要支援SD-WAN RA頭端，請確保在RADIUS伺服器上配置引數。RA連線需要以下引數：

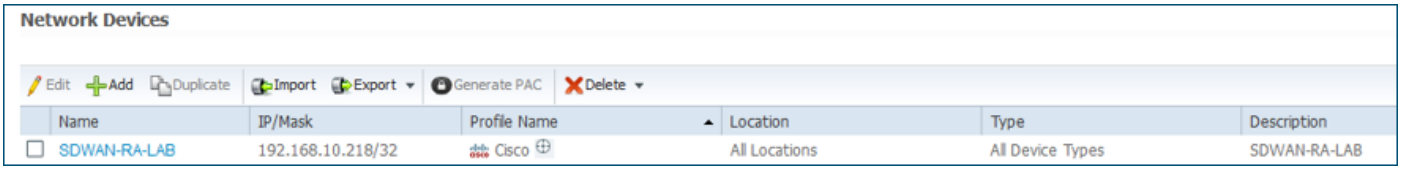
- 使用者身份驗證憑據 AnyConnect-EAP連線的使用者名稱和密碼
- 應用於使用者或使用者組的策略引數（屬性） **VRF**:RA使用者分配到的服務VPN**IP池名稱**:在RA頭端上定義的IP池的名稱**伺服器子**網：為RA使用者提供子網訪問

在ISE中配置的第一步是將RA頭端或cEdge IP地址配置為能夠向ISE發出RADIUS請求的網路裝置。

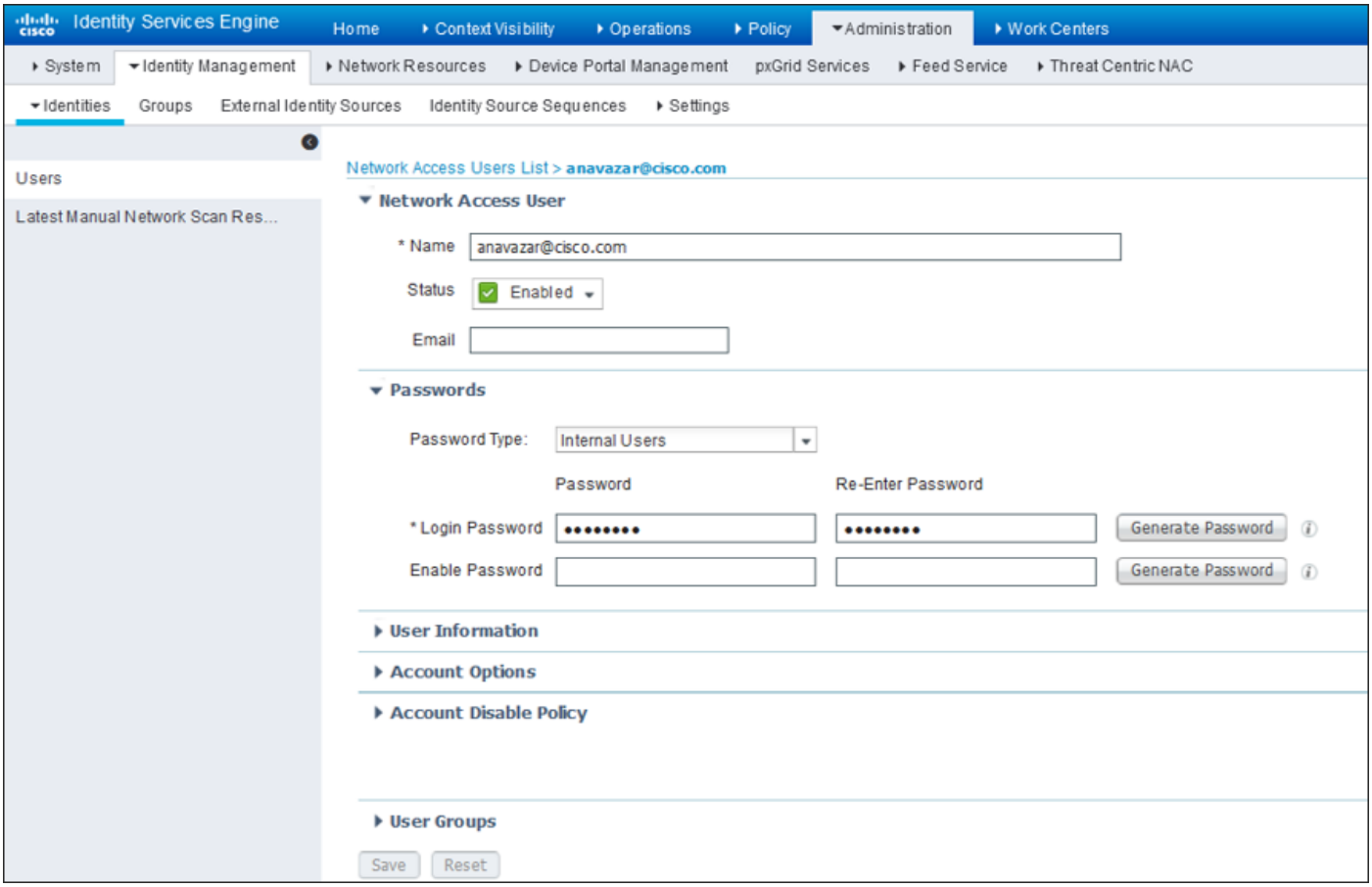
導覽至**Administration > Network Devices**，然後新增RA標頭(cEdge)IP位址和密碼，如下圖所示。



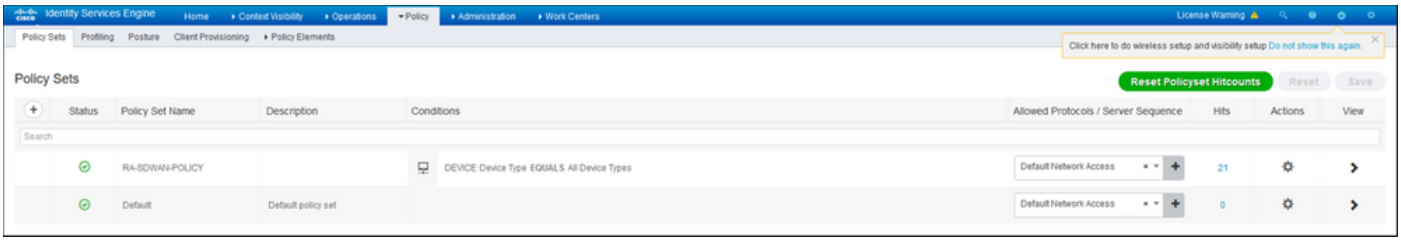
如圖所示新增的網路裝置。



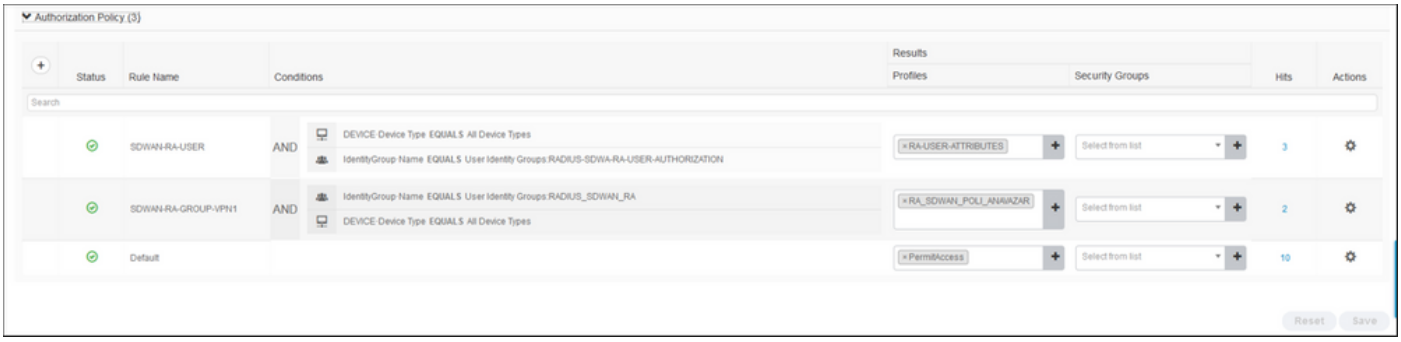
在RADIUS伺服器中，需要配置AnyConnect身份驗證的使用者名稱和密碼，如下圖所示。導覽至**Administration > Identities**。



需要建立一個策略集，使其滿足匹配條件，如下圖所示。在這種情況下，會使用**All Device types**條件，這意味著所有使用者都命中此策略。



然後，每個條件都建立了一個授權策略。條件**All Device types**和要匹配的身份組。



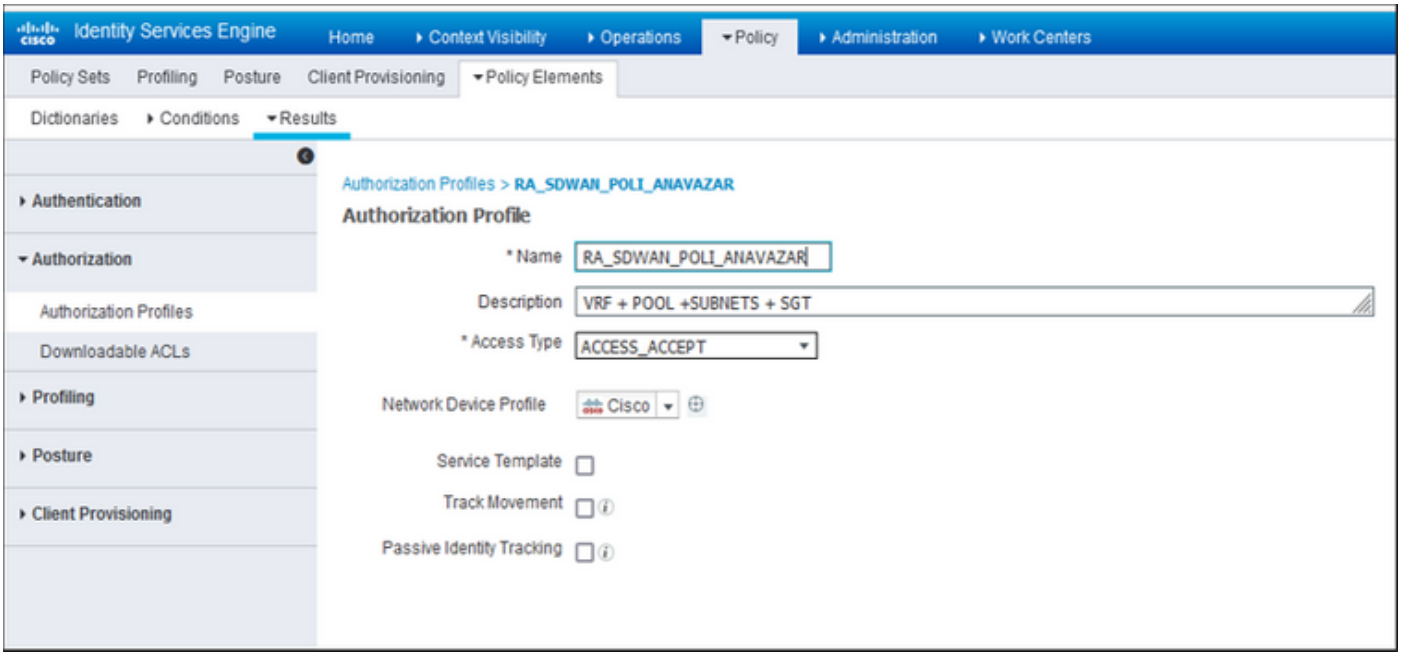
在**Authorization Profile**中，我們需要在**Advanced Attributes Settings**下將**Access Type**配置為**Access_ACCEPT**，選擇Cisco vendor and**Cisco-AV-pair屬性。**

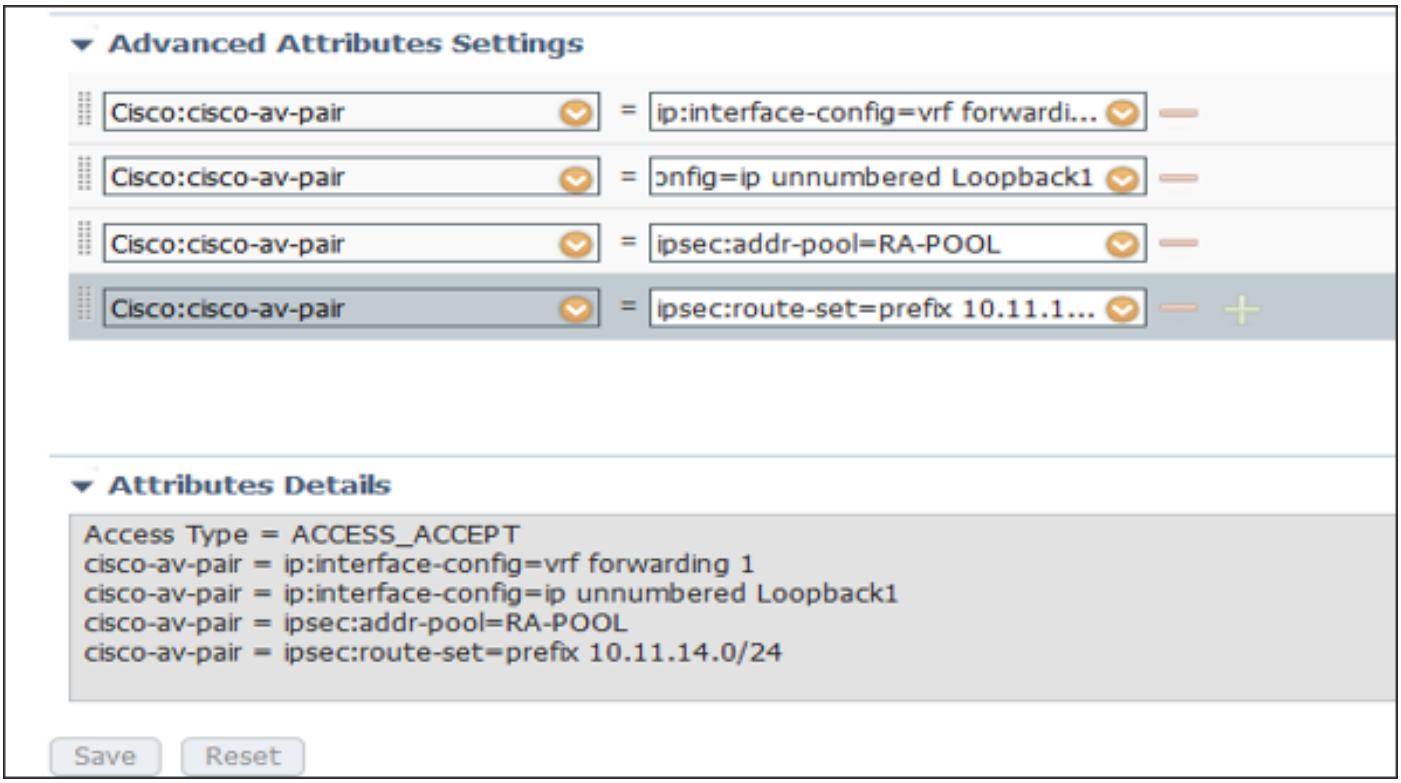
需要為使用者配置一些策略引數：

- VRF，使用者所屬的服務VRF。
- IP池名稱，每個使用者連線都分配了一個IP地址，該地址屬於在cEdge中配置的IP池。

- 使用者可以訪問的子網

注意： IP vrf forwarding命令必須位於IP unnumbered命令之前。如果虛擬訪問介面從虛擬模板克隆，然後應用IP vrf forwarding命令，則將從虛擬訪問介面刪除任何IP配置。



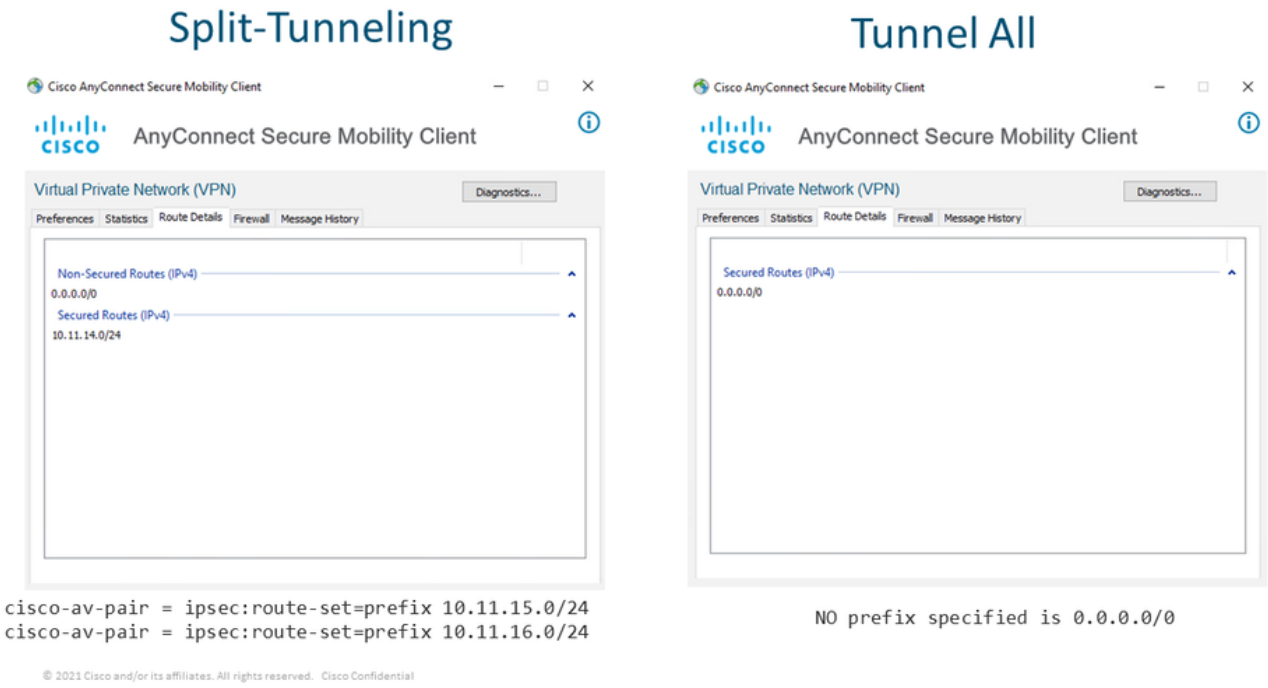


使用者屬性：

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

AnyConnect客戶端中的分割隧道與全部隧道

如圖所示，安裝AnyConnect客戶端中接收的ipsec:route-set=prefix屬性。



Cisco IOS® XE中的CA伺服器配置

CA伺服器向Cisco IOS® XE SD-WAN裝置提供證書，並使RA頭端能夠向RA客戶端驗證其自身。

CEDGE不能是CA伺服器，因為Cisco IOS® XE SD-WAN中不支援這些加密PKI伺服器命令。

- 生成RSA金鑰對
- 為CA伺服器建立PKI信任點 使用之前生成的KEY-CA配置rsakeypair。

  附註：PKI伺服器和PKI信任點必須使用相同的名稱。

- 建立CA伺服器 配置CA伺服器的頒發者名稱使用「No shutdown」啟用CA伺服器

```
crypto key generate rsa modulus 2048 label KEY-CA
!
crypto pki trustpoint CA
 revocation-check none
 rsakeypair KEY-CA
 auto-enroll
!
crypto pki server CA
 no database archive
 issuer-name CN=CSR1Kv_SDWAN_RA
 grant auto
 hash sha1
 lifetime certificate 3600
```

```
 lifetime ca-certificate 3650
 auto-rollover
no shutdown
!
```

驗證CA伺服器是否已啟用。

```
CA-Server-CSRv#show crypto pki server CA
Certificate Server CA:
    Status: enabled
    State: enabled
   Server's configuration is locked  (enter "shut" to unlock it)
   Issuer name: CN=CSR1Kv_SDWAN_RA
   CA cert fingerprint: 10DA27AD EF54A3F8 12925750 CE2E27EB
   Granting mode is: auto
   Last certificate issued serial number (hex): 3
   CA certificate expiration timer: 23:15:33 UTC Jan 17 2032
   CRL NextUpdate timer: 05:12:12 UTC Jan 22 2022
   Current primary storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
   Auto-Rollover configured, overlap period 30 days
   Autorollover timer: 23:15:37 UTC Dec 18 2031
```

驗證是否安裝了CA伺服器證書。

```
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
```

來自CA證書的**指紋SHA 1**用於具有遠端訪問配置的cEdge路由器（RA前端）中的**加密pki信任點**。

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

SD-WAN RA配置

> **附註**：本文檔不介紹控制器和cEdge的SD-WAN自註冊過程。假設SD-WAN交換矩陣已啟動且功能完整。

加密PKI配置

- 建立PKI信任點。
- 配置CA伺服器的URL。
- 從CA伺服器證書複製指紋sha 1。
- 配置新身份證書的使用者名稱和備用名稱。
- 使用之前生成的KEY-ID配置rsakeypar。

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

要求CA憑證進行驗證：

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

產生CSR，傳送到CA伺服器並收到新的身分識別憑證：

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

驗證CA憑證和cEdge憑證：

```
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組態

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

FlexVPN配置

配置IP池

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

配置IKEv2提議（密碼和引數）和策略：

```
crypto ikev2 proposal IKEV2-RA-PROP
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256

crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
```

配置IKEv2配置檔名稱管理器：

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

> **附註**：name-manager從EAP身份（使用者名稱）中的字首派生名稱，EAP身份中分隔字首和字尾。

配置IPsec密碼：

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

配置加密IKEv2配置檔案：

```
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 match identity remote any
 identity local address 192.168.10.218
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint RA-TRUSTPOINT
 aaa authentication anyconnect-eap ISE-RA-Authentication
 aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
 aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
 aaa accounting anyconnect-eap ISE-RA-Accounting
```

配置加密IPSEC配置檔案：

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

配置虛擬模板介面：

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

在加密IKEv2配置檔案中配置虛擬模板：

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

SD-WAN RA配置示例

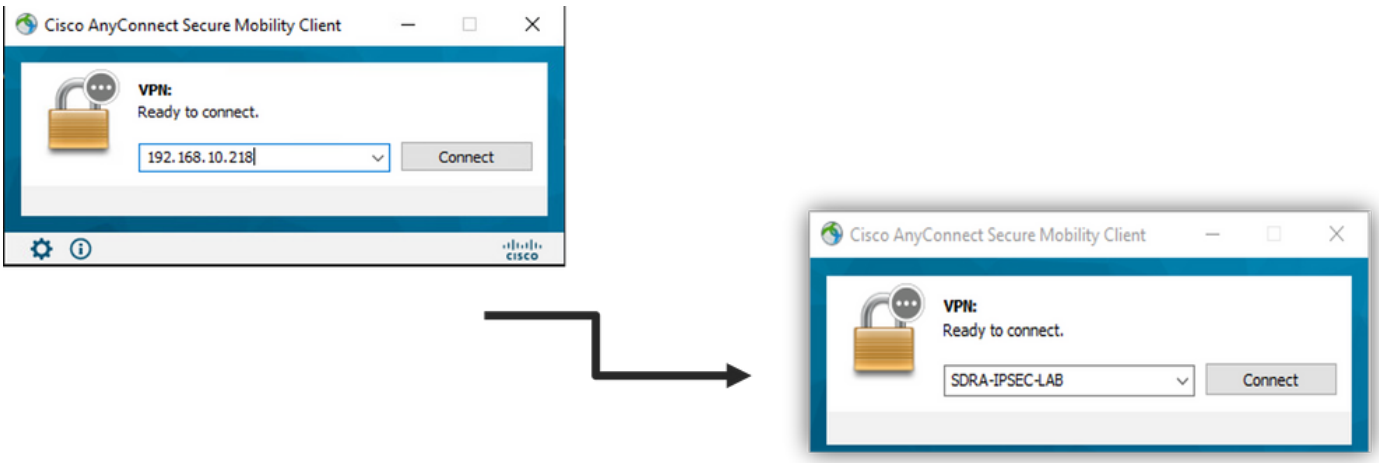
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group
!
crypto pki trustpoint RA-TRUSTPOINT
 subject-name CN=cEdge-SDWAN-1.crv
 enrollment url http://10.11.14.226:80
 fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
 subject-name CN=cEdge-SDWAN-1.crv
 vrf 1
 rsakeypair KEY-NEW
 revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap suffix delimiter @
!
crypto ikev2 proposal IKEV2-RA-PROP
```

```
 encryption aes-cbc-256
 integrity sha256
 group 19
 prf sha256
!
crypto ikev2 policy IKEV2-RA-POLICY
 proposal IKEV2-RA-PROP
!
crypto ipsec transform-set IKEV2-RA-TRANSFORM-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 match identity remote any
 identity local address 192.168.10.218
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint RA-TRUSTPOINT
 aaa authentication anyconnect-eap ISE-RA-Authentication
 aaa authorization group anyconnect-eap list ISE-RA-Authorization name-mangler IKEV2-RA-MANGLER
password Cisc0123456
 aaa authorization user anyconnect-eap list ISE-RA-Authorization USER-SDWAN password Us3r123456
 aaa accounting anyconnect-eap ISE-RA-Accounting
!
crypto ipsec profile IKEV2-RA-PROFILE
 set transform-set IKEV2-RA-TRANSFORM-SET
 set ikev2-profile RA-SDWAN-IKEV2-PROFILE
!
interface Virtual-Template101 type tunnel
 vrf forwarding 1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IKEV2-RA-PROFILE
!
crypto ikev2 profile RA-SDWAN-IKEV2-PROFILE
 virtual-template 101
```

AnyConnect客戶端配置

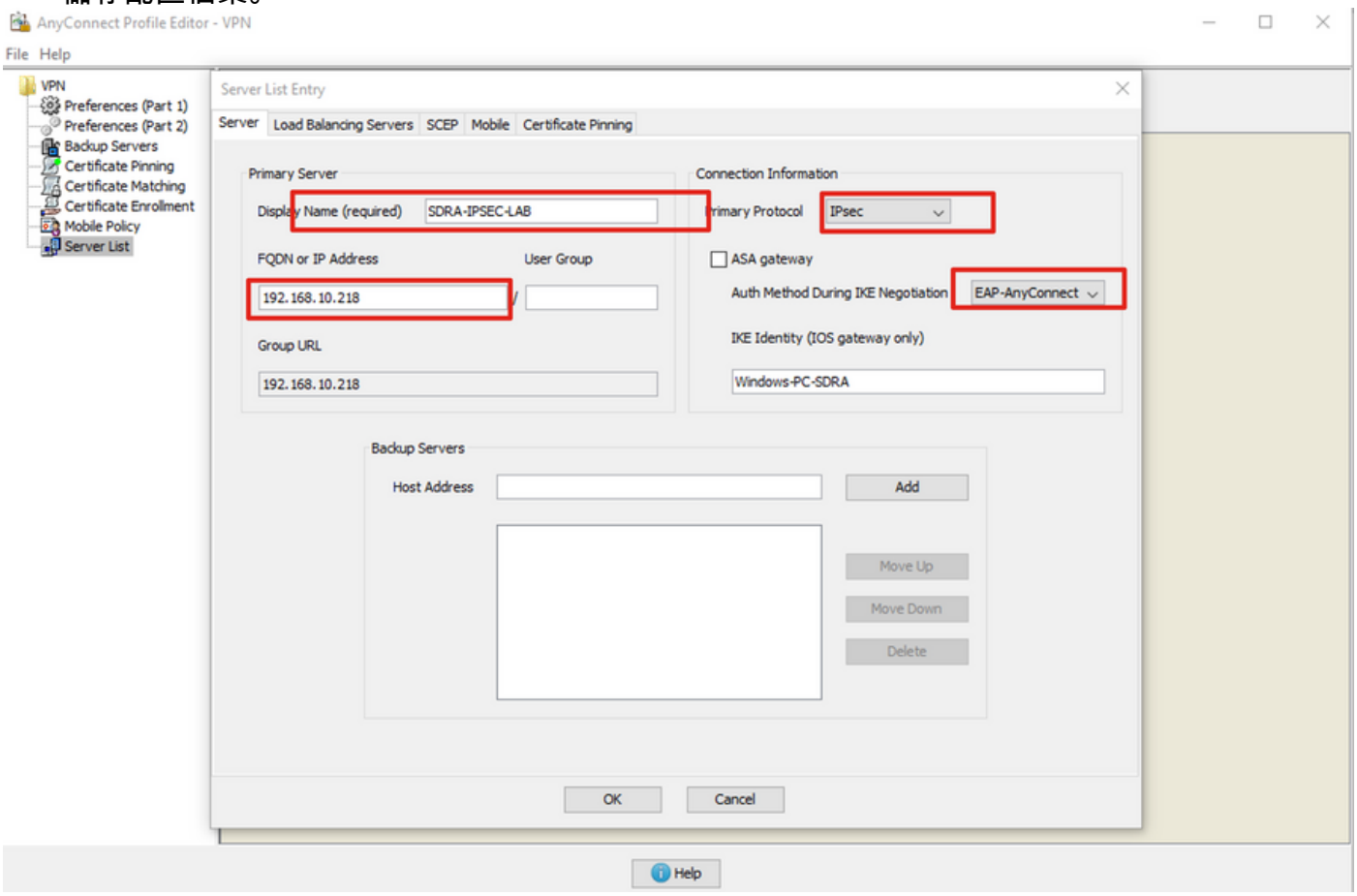
AnyConnect客戶端使用SSL作為隧道建立的預設協定，SD-WAN RA（路線圖）不支援此協定。RA使用FlexVPN，因此IPSEC是使用的協定，必須對其進行更改，並且此操作是通過XML配置檔案完成的。

使用者可以手動在AnyConnect客戶端的位址列中輸入VPN網關的FQDN。這會導致到網關的SSL連線。



配置AnyConnect配置檔案編輯器

- 導覽至**Server List**，然後按一下**Add**。
- 選擇**IPsec**作為「主協定」。
- 取消選中**ASA網關**選項。
- 選擇**EAP-AnyConnect**作為「IKE協商期間的身份驗證方法」。
- **Display/Name（必需）**是用於在AnyConnect客戶端下儲存此連線的名稱。
- FQDN **或IP Address 必須用**Edge（公共）IP地址進行歸檔。
- 儲存配置檔案。



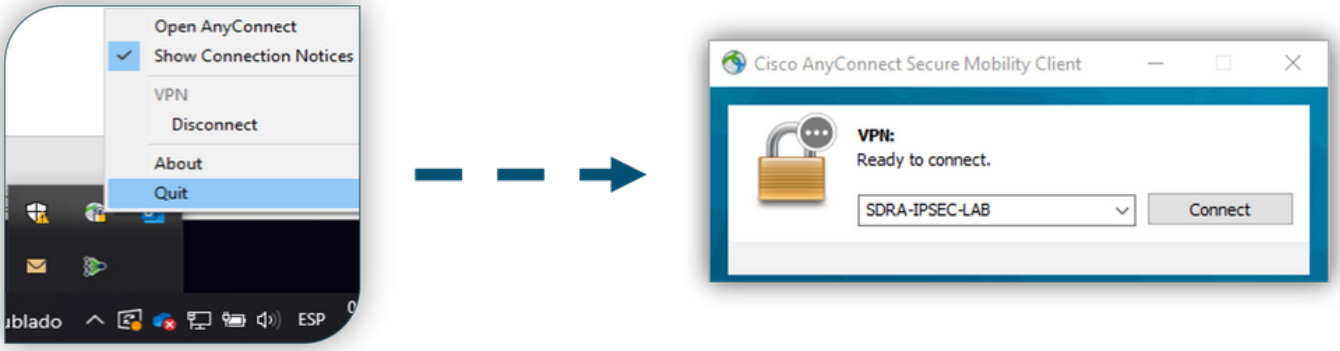
安裝AnyConnect配置檔案(XML)

可以將XML配置檔案手動放入目錄：

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

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

AnyConnect客戶端需要重新啟動，才能在GUI中看到配置檔案。通過按一下右鍵Windows工作列中的AnyConnect圖示並選擇**Quit**選項，可以重新啟動該進程：



禁用AnyConnect下載程式

預設情況下，成功登入後，AnyConnect客戶端會嘗試下載XML配置檔案。

如果配置檔案不可用，連線將失敗。作為解決方法，可以在客戶端本身上禁用AnyConnect配置檔案下載功能。

對於Windows:

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

對於MAC OS:

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

「BypassDownloader」選項設定為「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>
```

在AnyConnect客戶端上取消阻止不受信任的伺服器

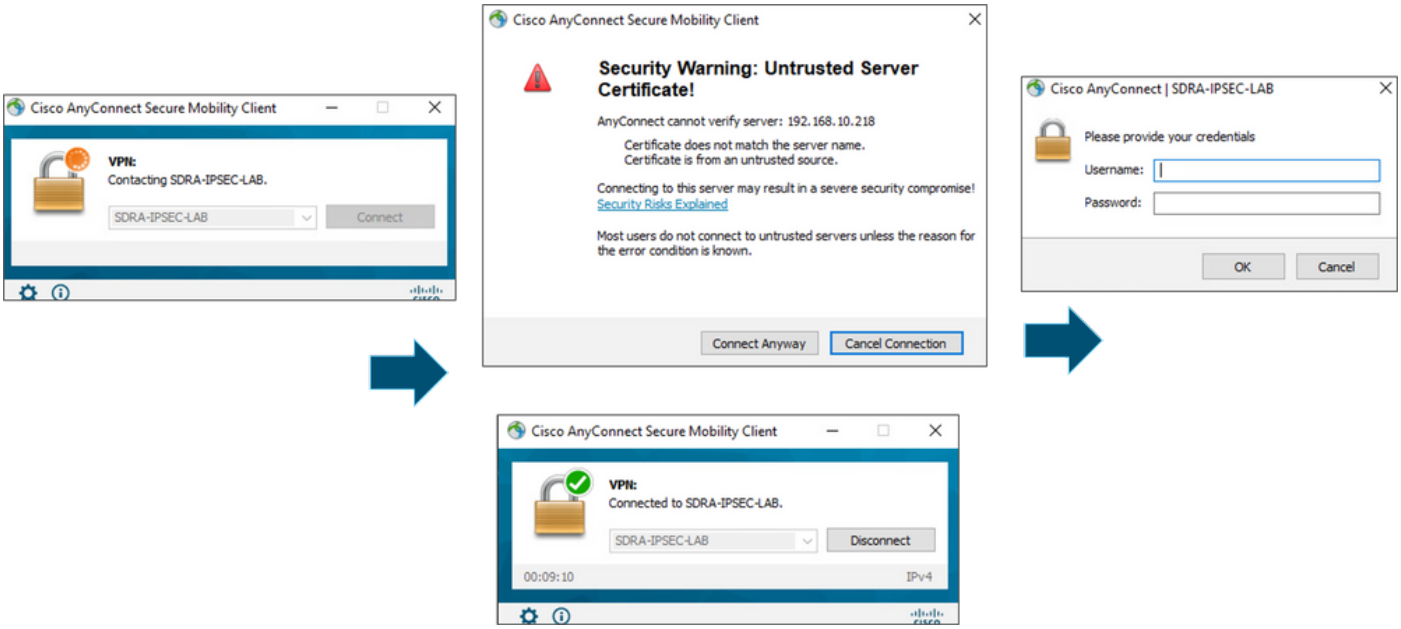
導覽至**Settings > Preferences**，然後取消選中所有框選項。

最重要的是此場景的「**阻止到不受信任**伺服器的連線」。

> **附註**：用於RA頭端/cEdge身份驗證的證書是先前由Cisco IOS® XE中的CA伺服器建立和簽名的證書。因為此CA伺服器不是GoDaddy、Symantec、Cisco等公共實體。PC客戶端將證書解釋為不受信任的伺服器。這可通過使用公司信任的公用證書或CA伺服器來修復。

使用AnyConnect客戶端

在放置所有SDRA配置後，成功連線的流程將顯示為影象。



驗證

虛擬模板介面用於建立虛擬訪問介面以啟動加密通道並在伺服器(cEdge)和客戶端（AnyConnect使用者）之間建立IKEv2和IPsec安全關聯(SA)。

附註：虛擬模板介面始終為up/down。狀態為up,Protocol 為down。

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

使用**show derived-config interface virtual-access <number>**，檢查為與客戶端關聯的Virtual-Access介面應用的實際配置。

```
cEdge-207#show derived-config interface virtual-access 1
Building configuration...
Derived configuration : 252 bytes
!
interface Virtual-Access1
 vrf forwarding 1
 ip unnumbered Loopback1
 tunnel source 192.168.10.218
 tunnel mode ipsec ipv4
 tunnel destination 192.168.10.219
 tunnel protection ipsec profile IKEV2-RA-PROFILE
```

```
 no tunnel protection ipsec initiate
end
```

使用**show crypto ipsec sa peer <AnyConnect Public IP >**檢查AnyConnect客戶端的IPsec安全關聯(SA)。

```
cEdge-207#show crypto ipsec sa peer 192.168.10.219
interface: Virtual-Access2
   Crypto map tag: Virtual-Access2-head-0, local addr 192.168.10.218
  protected vrf: 1
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.20.14.13/255.255.255.255/0/0)
  current_peer 192.168.10.219 port 50787
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
    outbound pcp sas:
… Output Omitted….
```

檢查會話的IKEv2 SA引數、使用者名稱和分配的IP。

附註：分配的IP地址必須與AnyConnect客戶端的IP地址匹配。

```
cEdge-207#sh crypto ikev2 session detail
 IPv4 Crypto IKEv2 Session
Session-id:21, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.10.218/4500   192.168.10.219/62654  none/1               READY
     Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth
verify: AnyConnect-EAP
     Life/Active Time: 86400/532 sec
     CE id: 1090, Session-id: 21
     Local spi: DDB03CE8B791DCF7       Remote spi: 60052513A60C622B
     Status Description: Negotiation done
     Local id: 192.168.10.218
     Remote id: *$AnyConnectClient$*
     Remote EAP id: anavazar@cisco.com
     Local req msg id:  0              Remote req msg id:  23
     Local next msg id: 0              Remote next msg id: 23
     Local req queued:  0              Remote req queued:  23
     Local window:      5              Remote window:      1
     DPD configured for 45 seconds, retry 2
     Fragmentation not  configured.
     Dynamic Route Update: disabled
     Extended Authentication not configured.
     NAT-T is detected  outside
     Cisco Trust Security SGT is disabl
      Assigned host addr: 10.20.14.19
     Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.20.14.19/0 - 10.20.14.19/65535
         ESP spi in/out: 0x43FD5AD3/0xC8349D4F
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
         Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
         ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
 IPv6 Crypto IKEv2 Session
```

```
cEdge-207#show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN
Interface: Virtual-Access1
Profile: RA-SDWAN-IKEV2-PROFILE
Uptime: 00:17:07
Session status: UP-ACTIVE
Peer: 192.168.10.219 port 62654 fvrf: (none) ivrf: 1
     Phase1_id: *$AnyConnectClient$*
     Desc: (none)
 Session ID: 94
 IKEv2 SA: local 192.168.10.218/4500 remote 192.168.10.219/62654 Active
         Capabilities:DN connid:1 lifetime:23:42:53
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.14.19
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 89 drop 0 life (KB/Sec) 4607976/2573
       Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/2573
```

相關資訊

- Cisco SD-WAN遠端存取
- 配置FlexVPN伺服器
- 下載AnyConnect
- 技術支援與文件 - Cisco Systems