

Configurazione di SD-WAN Remote Access (SDRA) con AnyConnect e ISE Server

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Che cos'è una VPN ad accesso remoto?](#)

[Che cos'è SD-WAN Remote Access VPN?](#)

[Tunneling ripartito e tunnel completo](#)

[Prima di SDRA e dopo SDRA](#)

[Cos'è FlexVPN?](#)

[Configurazione prerequisiti](#)

[Configurazione di ISE](#)

[Confronto tra split-tunneling e tunnel nel client AnyConnect](#)

[Configurazione del server CA in Cisco IOS® XE](#)

[Configurazione SD-WAN RA](#)

[Configurazione PKI di crittografia](#)

[Configurazione AAA](#)

[Configurazione FlexVPN](#)

[Esempio di configurazione di SD-WAN RA](#)

[Configurazione client AnyConnect](#)

[Configurazione dell'Editor di profili AnyConnect](#)

[Installare il profilo AnyConnect \(XML\)](#)

[Disabilitazione del download di AnyConnect](#)

[Sblocco dei server non attendibili sul client AnyConnect](#)

[Usa client AnyConnect](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare SD-WAN Remote Access (SDRA) con il client AnyConnect utilizzando una modalità autonoma Cisco IOS® XE come server CA e un server Cisco Identity Services Engine (ISE) per l'autenticazione, l'autorizzazione e l'accounting.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- PKI (Public Key Infrastructure)
- FlexVPN
- server RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C800V versione 17.07.01a
- vManage versione 20.7.1
- CSR1000V versione 17.03.04.a
- ISE versione 2.7.0.256
- AnyConnect Secure Mobility Client versione 4.10.04071

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Che cos'è una VPN ad accesso remoto?

La VPN ad accesso remoto consente all'utente remoto di connettersi in modo sicuro alle reti aziendali, utilizzare applicazioni e dati accessibili solo tramite i dispositivi collegati in ufficio.

Una VPN ad accesso remoto funziona tramite un tunnel virtuale creato tra il dispositivo di un dipendente e la rete aziendale.

Questo tunnel passa attraverso la rete pubblica, ma i dati inviati avanti e indietro attraverso di esso sono protetti da protocolli di crittografia e sicurezza per aiutarlo a mantenerlo privato e sicuro.

I due componenti principali di questo tipo di VPN sono un headend server di accesso alla rete/server di accesso remoto e un software client VPN.

Che cos'è SD-WAN Remote Access VPN?

L'accesso remoto è stato integrato nella soluzione SD-WAN che elimina la necessità di un'infrastruttura Cisco SD-WAN e RA separata e consente una rapida scalabilità dei servizi RA utilizzando Cisco AnyConnect come client software RA.

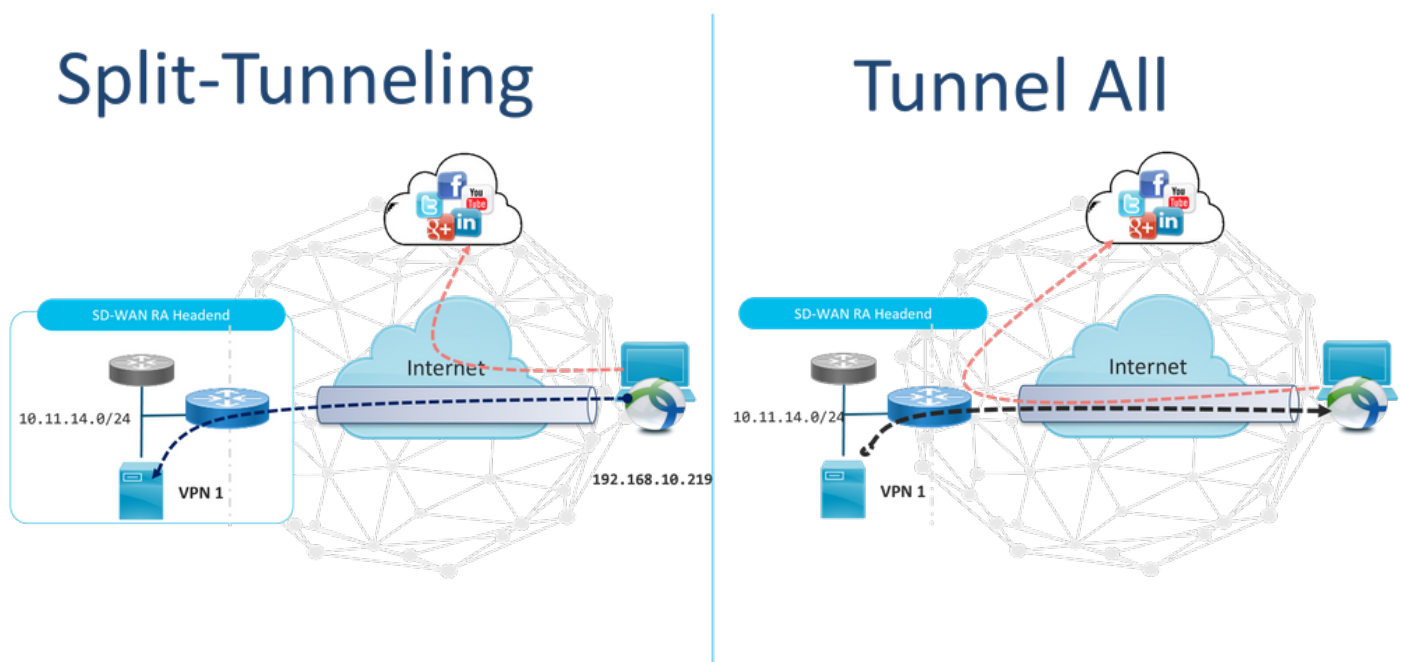
Accesso remoto consente agli utenti remoti di accedere alla rete dell'organizzazione. In questo modo è possibile lavorare da casa.

I vantaggi

- L'accesso remoto consente di accedere alla rete di un'organizzazione da dispositivi/utenti in postazioni remote. HO
- Estende la soluzione Cisco SD-WAN agli utenti RA senza che il dispositivo di ciascun utente RA debba far parte del fabric Cisco SD-WAN.
- Sicurezza dei dati
- Tunneling ripartito o Tunnel tutto
- Scalabilità
- Possibilità di distribuire il carico RSA su numerosi dispositivi Cisco IOS® XE SD-WAN nel fabric Cisco SD-WAN.

Tunneling ripartito e tunnel completo

Il tunneling ripartito è usato negli scenari in cui deve essere tunneling solo del traffico specifico (ad esempio, subnet SD-WAN), come mostrato nell'immagine.

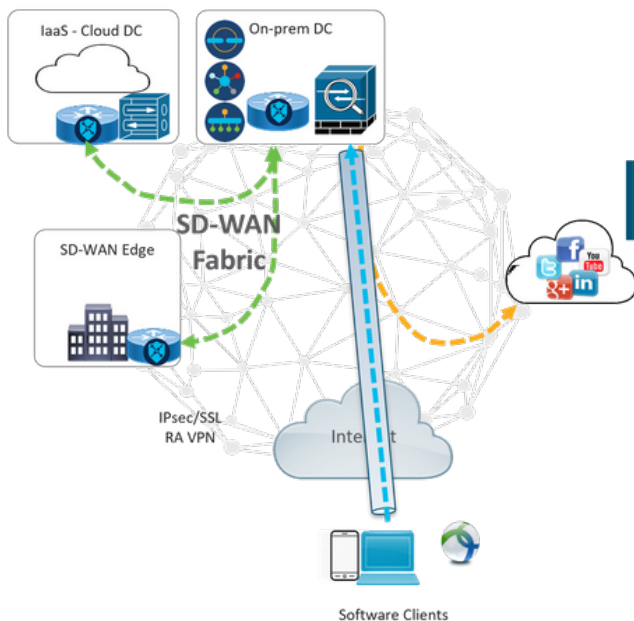


Prima di SDRA e dopo SDRA

La struttura VPN ad accesso remoto tradizionale richiede un'infrastruttura RA separata al di fuori del fabric Cisco SD-WAN per fornire l'accesso remoto degli utenti alla rete come ad esempio appliance non SD-WAN come ASA, Cisco IOS® XE standard o dispositivi di terze parti, e il traffico RA viene spostato verso l'appliance SD-WAN come mostrato nell'immagine.

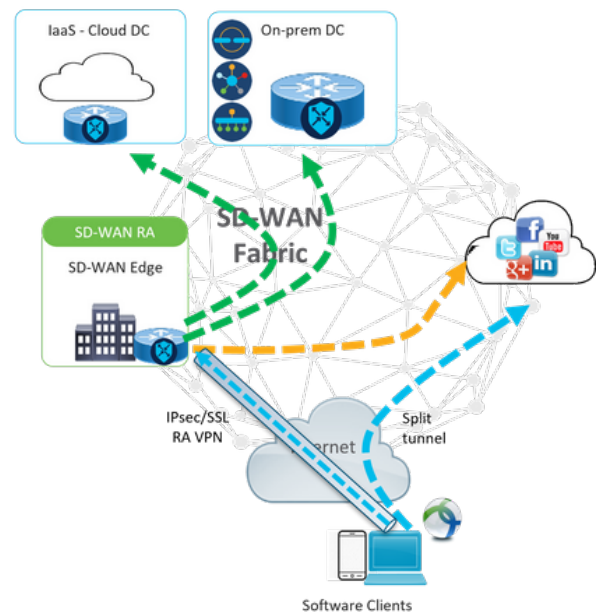
Before SDRA

Traditional Remote-Access VPN design with SDWAN



After SDRA

SD-WAN Remote-Access



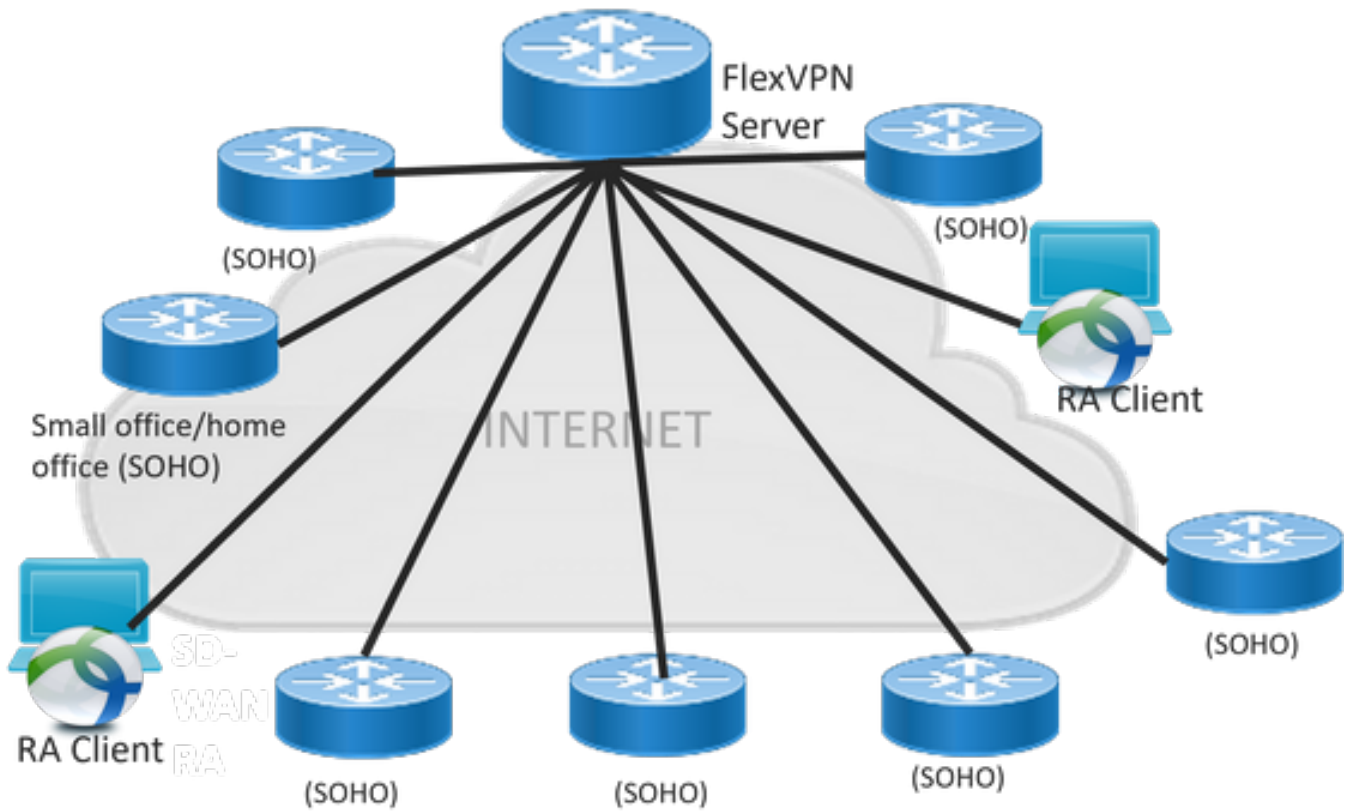
SD-WAN Remote Access cambia il modo in cui gli utenti remoti si connettono alla rete. Si collegano direttamente al cEdge utilizzato come headend RA. Estende le funzionalità e i vantaggi di Cisco SD-WAN agli utenti RSA. Gli utenti RSA diventano utenti di filiali sul lato LAN.

Per ogni client RA, l'headend RA SD-WAN assegna un indirizzo IP a un client RA e aggiunge una route host statica all'indirizzo IP assegnato nel VRF di servizio in cui si trova l'utente RA.

La route statica specifica il tunnel VPN della connessione client di Autorità registrazione integrità. L'headend RA SD-WAN annuncia l'IP statico all'interno del VRF di servizio del client RA con l'utilizzo di OMP su tutti i dispositivi periferici della VPN di servizio.

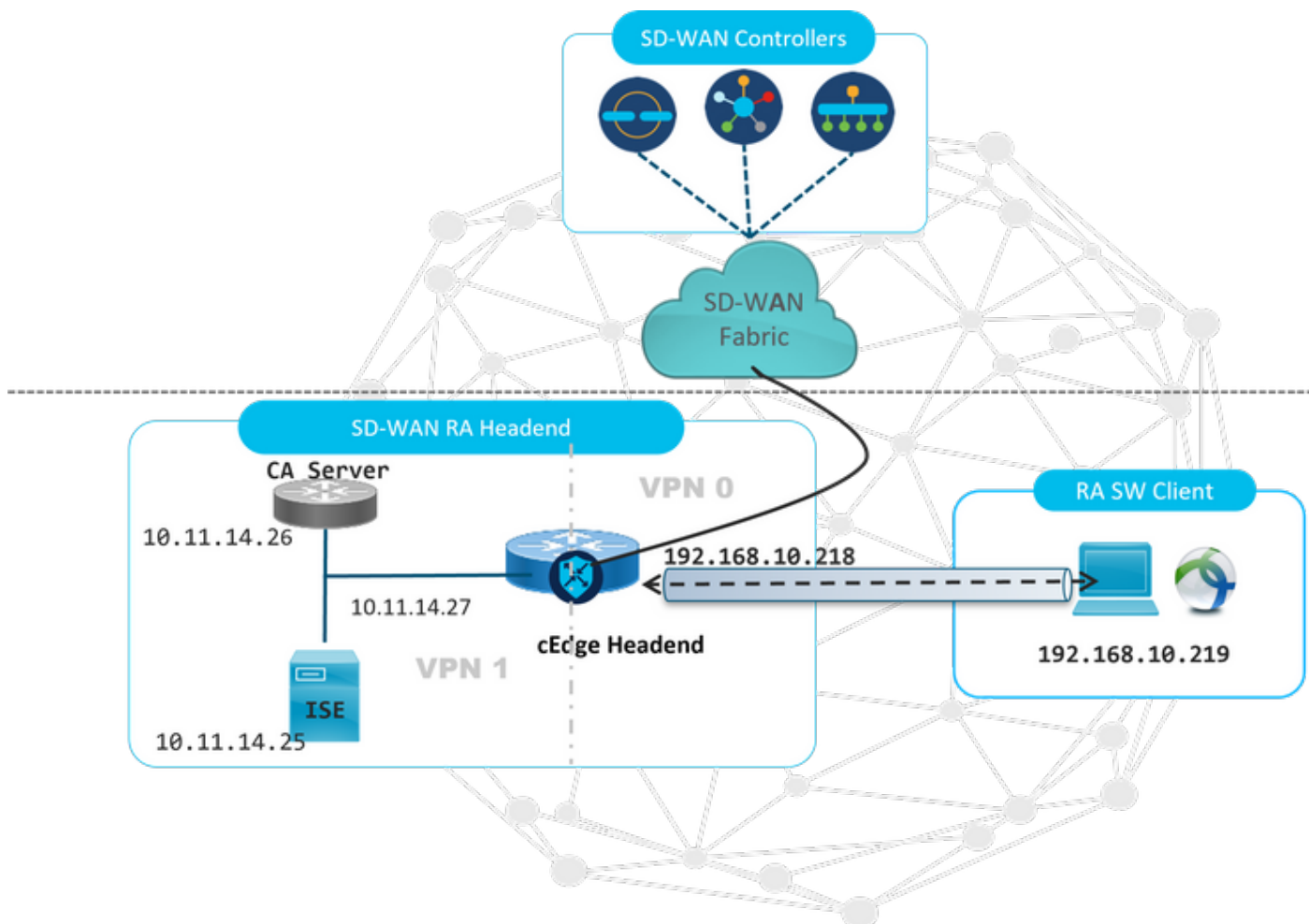
Cos'è FlexVPN?

SD-WAN RA Sfrutta la soluzione Cisco FlexVPN RA. FlexVPN è l'implementazione Cisco dello standard IKEv2, un paradigma unificato e una CLI che combina sito a sito, **accesso remoto**, topologie hub e spoke e trame parziali (spoke diretto). FlexVPN offre un framework semplice ma modulare che utilizza ampiamente il paradigma dell'interfaccia tunnel pur rimanendo compatibile con le implementazioni VPN legacy.



Configurazione prerequisiti

Per questo esempio, è stata creata un'impostazione del laboratorio RA SD-WAN, come mostrato nell'immagine.



Sono stati configurati componenti aggiuntivi per questo scenario di laboratorio RA SD-WAN:

- Cisco IOS® XE standard in modalità autonoma come server CA.
- Un server ISE/RADIUS per autenticazione, autorizzazione e accounting.
- Un PC Windows raggiungibile da cEdge tramite l'interfaccia WAN.
- AnyConnect Client già installato.

Nota: I server CA e RADIUS sono stati inseriti nel servizio VRF 1. Entrambi i server devono essere raggiungibili tramite il VRF di servizio per tutti gli headend RA SD-WAN.

Nota: L'accesso remoto SD-WAN Cisco è supportato nella versione 17.7.1a e da dispositivi specifici per SDRA. Per i dispositivi supportati, vedere: [Piattaforme supportate per l'headend SD-WAN RA](#)

Configurazione di ISE

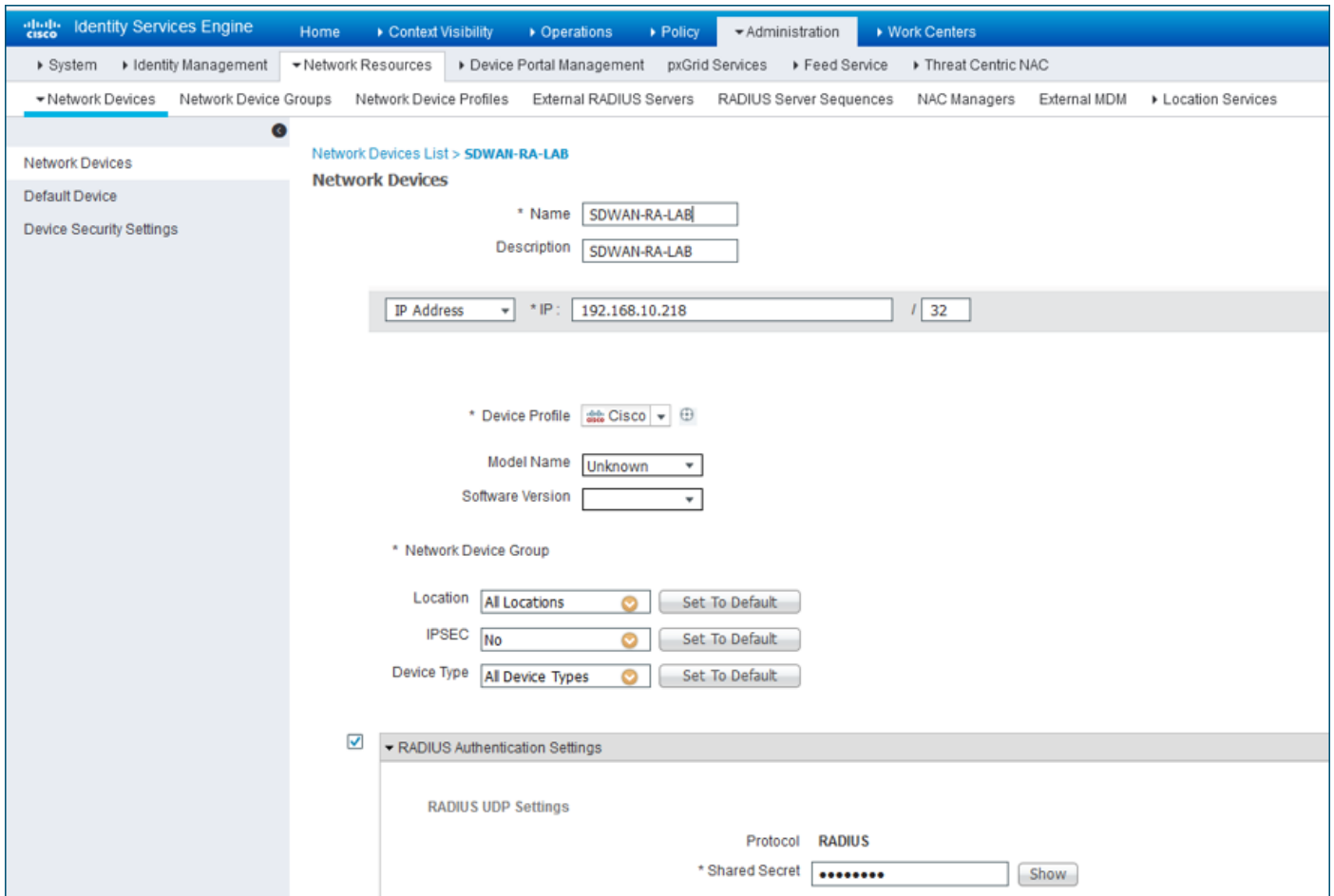
Per supportare l'headend RA SD-WAN, verificare che i parametri siano configurati sul server RADIUS. Questi parametri sono obbligatori per le connessioni RA:

- Credenziali di autenticazione utente Nome utente e password per le connessioni AnyConnect-EAP
- Parametri (attributi) dei criteri applicati a un utente o a un gruppo di utenti VRF: VPN del servizio assegnata all'utente RANome pool IP: Nome del pool IP definito nell'headend

RASubnet server: Accesso alla subnet da fornire all'utente RA

Il primo passaggio da configurare nell'ISE è l'headend RA o l'indirizzo IP cEdge come dispositivo di rete per poter effettuare richieste Radius all'ISE.

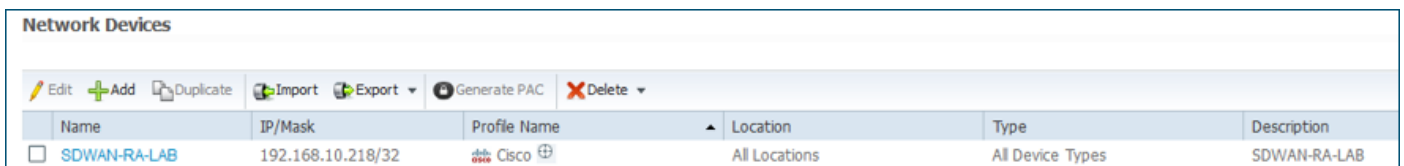
Passare a **Amministrazione > Dispositivi di rete** e aggiungere l'indirizzo IP e la password dell'intestazione RA (cEdge) come mostrato nell'immagine.



The screenshot shows the configuration page for a Network Device in the Cisco Identity Services Engine (ISE) interface. The page is titled "Network Devices" and includes a sidebar with "Default Device" and "Device Security Settings". The main content area is titled "Network Devices List > SDWAN-RA-LAB" and "Network Devices". 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: All Locations, No IPSEC, All Device Types
- RADIUS Authentication Settings: Protocol: RADIUS, Shared Secret: (masked)

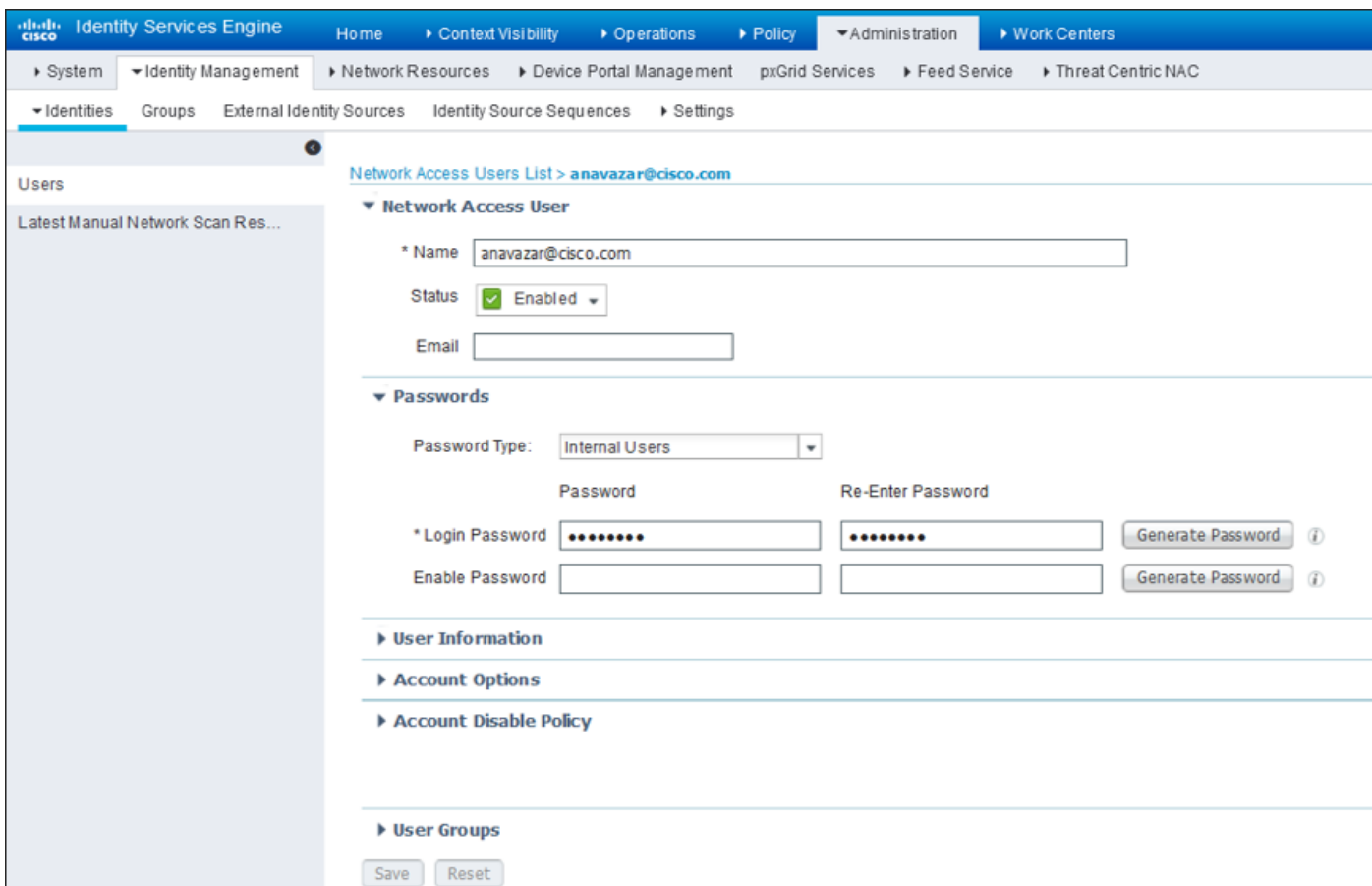
Dispositivo di rete aggiunto come mostrato nell'immagine.



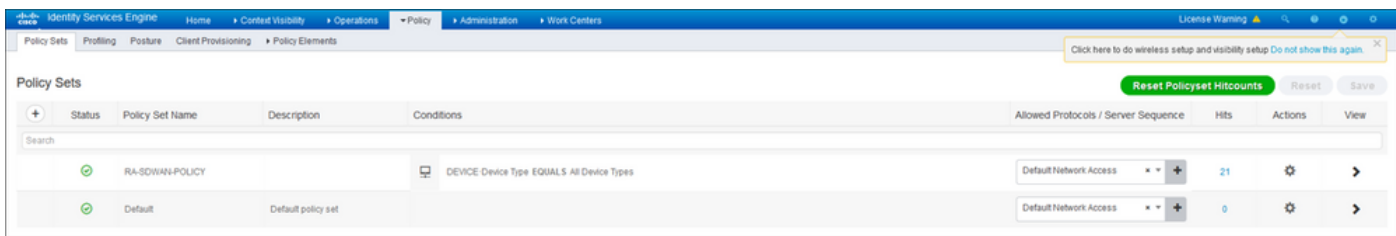
The screenshot shows the "Network Devices" list in the Cisco Identity Services Engine (ISE) interface. The table below displays the configuration for the device "SDWAN-RA-LAB".

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

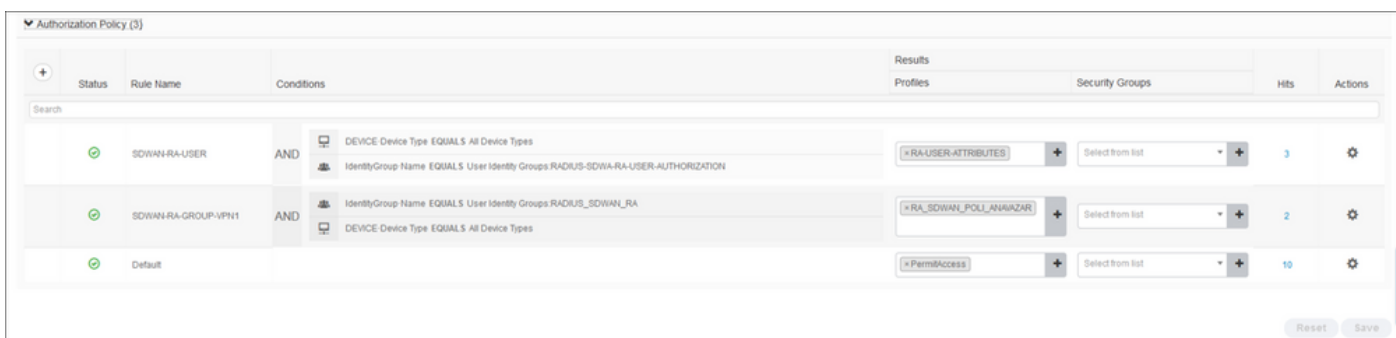
Sul server RADIUS, è necessario configurare i nomi utente e la password per l'autenticazione AnyConnect, come mostrato nell'immagine. Passare a **Amministrazione > Identità**.



È necessario creare un set di criteri con la condizione di corrispondenza da raggiungere, come mostrato nell'immagine. In questo caso viene utilizzata la condizione **Tutti i tipi di dispositivo**, che indica che tutti gli utenti hanno eseguito questa impostazione.



I criteri di autorizzazione sono stati quindi creati uno per ogni condizione. La condizione **Tutti i tipi di dispositivo** e i gruppi di identità corrispondenti.

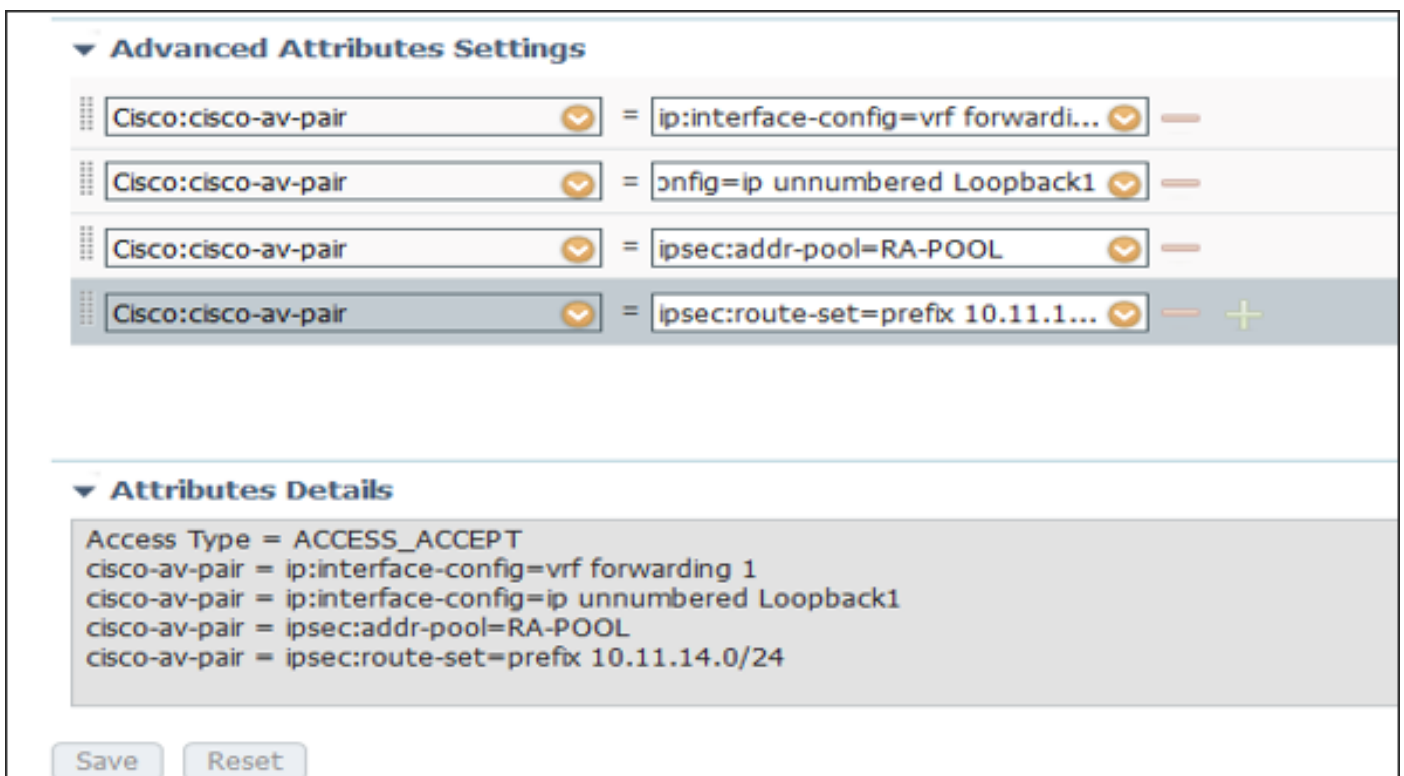
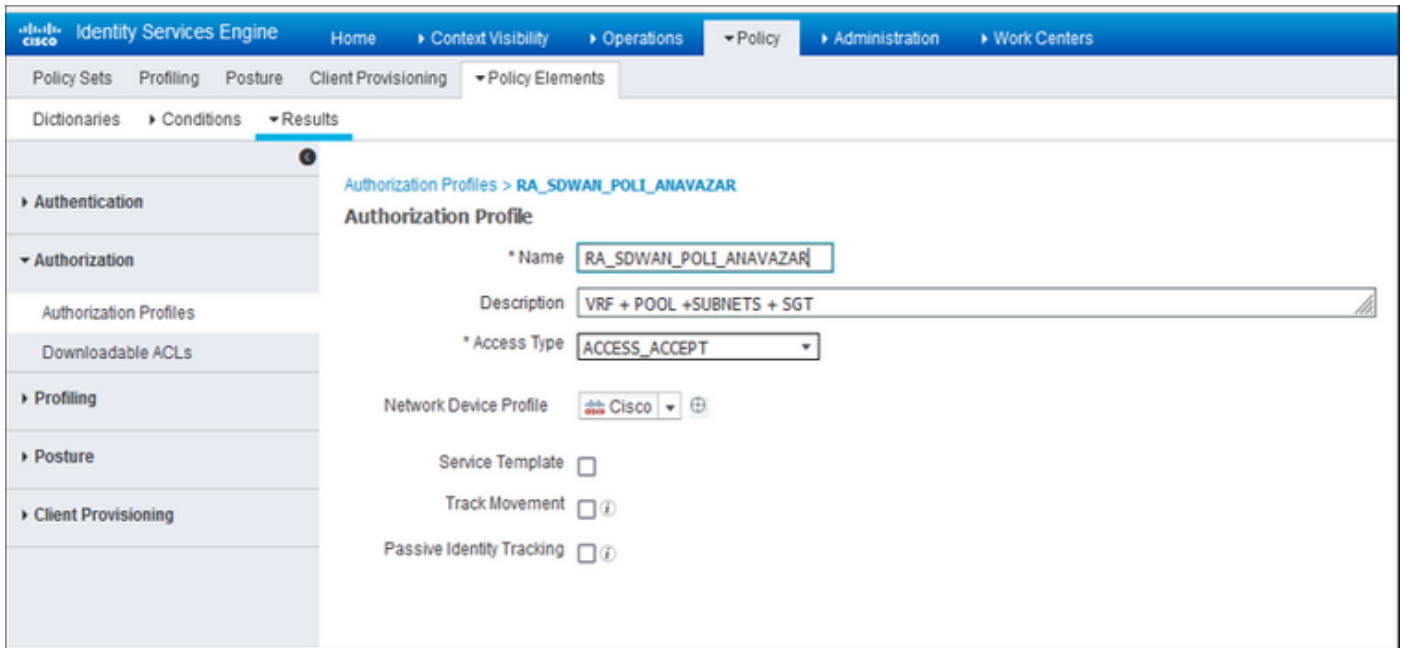


Nel **profilo di autorizzazione**, è necessario configurare il **tipo di accesso** come **Access_ACCEPT** in **Impostazioni avanzate attributi**, selezionare il fornitore Cisco e l'**attributo Cisco-AV-pair**.

È necessario configurare alcuni parametri dei criteri per gli utenti:

- VRF, il VRF del servizio a cui appartiene l'utente.
- Al nome del pool IP, a ogni connessione utente viene assegnato un indirizzo IP, che appartiene al pool IP configurato nei bordi.
- le subnet a cui l'utente può accedere

Attenzione: Il comando **IP vrf forwarding** deve precedere il comando **IP senza numero**. Se l'interfaccia di accesso virtuale viene clonata dal modello virtuale e viene quindi applicato il comando **IP vrf forwarding**, qualsiasi configurazione IP viene rimossa dall'interfaccia di accesso virtuale.



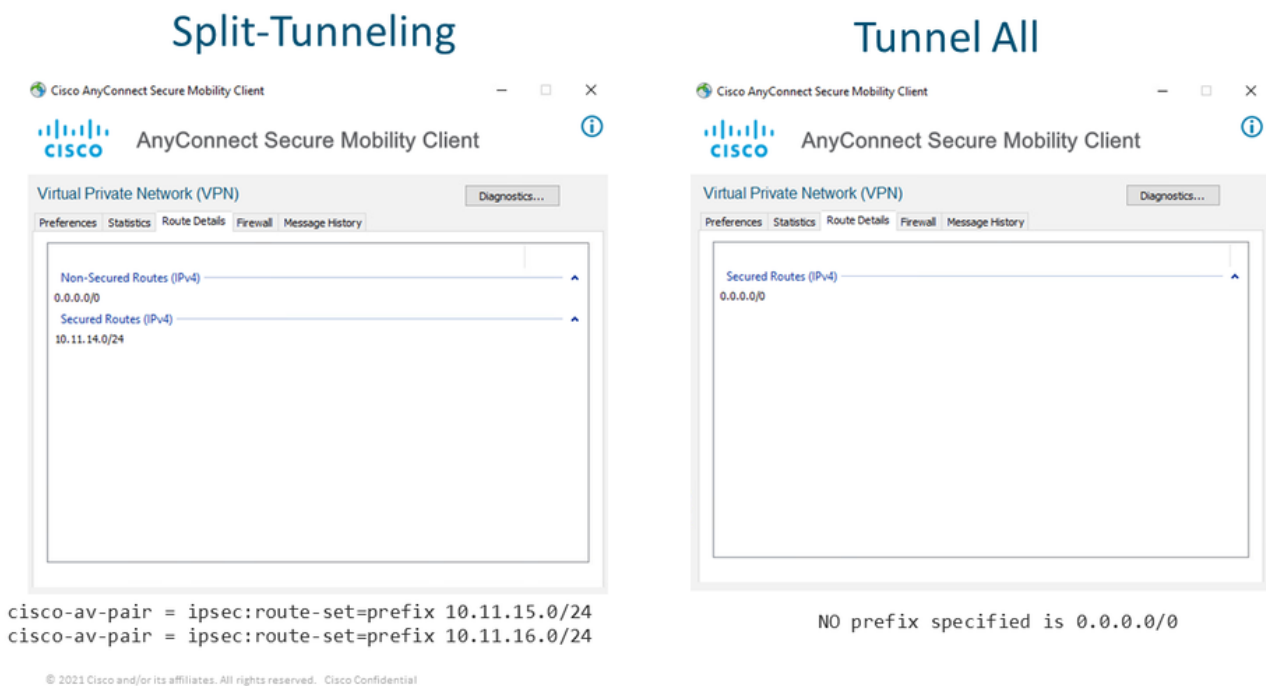
Attributi utente:

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
```

Confronto tra split-tunneling e tunnel nel client AnyConnect

`ipsec:route-set=prefix` ricevuto nel client AnyConnect viene installato come mostrato nell'immagine.



Configurazione del server CA in Cisco IOS® XE

Il server CA fornisce i certificati ai dispositivi Cisco IOS® XE SD-WAN e consente all'headend RA di autenticarsi ai client RA.

CEDGE non può essere un server CA perché questi comandi del server crypto PKI non sono supportati in Cisco IOS® XE SD-WAN.

- Generare una coppia di chiavi RSA
- Creare il trust point PKI per il server CA Configurare la coppia di chiavi con la chiave generata in precedenza da KEY-CA.

Nota: Il server PKI e il trust point PKI devono utilizzare lo stesso nome.

- Creare il server CA Configurare il nome dell'autorità emittente per il server CA Attivare il server CA utilizzando "No shutdown" (Nessun arresto)

```
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
!
```

Verificare se il server CA è abilitato.

```
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
```

Verificare che il certificato del server CA sia installato.

```
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
```

L'impronta digitale SHA 1 dal certificato CA viene utilizzata sul trust point PKI crittografico nel router cEdge (headend RA) con la configurazione di accesso remoto.

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

Configurazione SD-WAN RA

Nota: Questo documento non descrive il processo di onboarding SD-WAN per Controller e cEdge. Si presume che il fabric SD-WAN sia attivo e completamente funzionante.

Configurazione PKI di crittografia

- Creare un trust point PKI.
- Configurare l'URL per il server CA.
- Copiare l'impronta digitale sha 1 dal certificato del server CA.
- Configurare il Nome soggetto e il Nome alternativo per il nuovo certificato di identità.
- Configurare il parametro rsakeypair con l'ID della chiave generato in precedenza.

```
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
```

Chiedere il certificato CA da autenticare:

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

Genera il CSR, lo invia al server CA e riceve il nuovo certificato di identità:

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

Verificare il certificato CA e il certificato 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
```

Configurazione 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
```

Configurazione FlexVPN

Configura pool IP

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

Configurare una proposta IKEv2 (cifrature e parametri) e un criterio:

```
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
```

Configurare un gestore dei nomi dei profili IKEv2:

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

Nota: Il gestore del nome deriva il nome dal prefisso dell'identità EAP (nome utente) che delimita l'identità EAP che separa il prefisso dal suffisso.

Configurare le cifrature IPsec:

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

Configurare il profilo 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
```

Configurare il profilo IPSEC di crittografia:

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

Configura interfaccia modello virtuale:

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

Configurare il modello virtuale nel profilo Crypto IKEv2:

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

Esempio di configurazione di 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
```

```

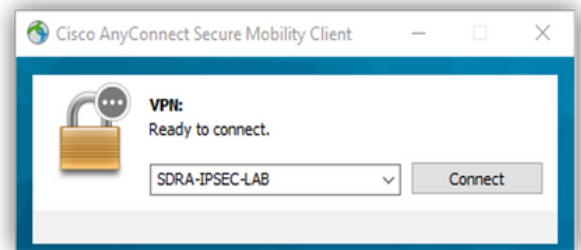
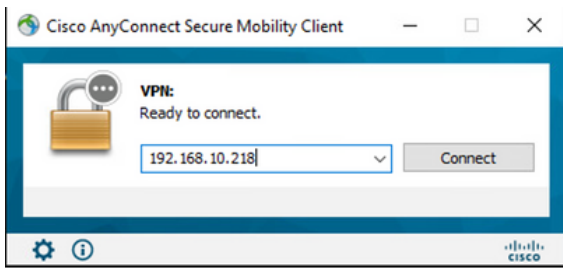
subject-name CN=cEdge-SDWAN-1.crv
enrollment url http://10.11.14.226:80
fingerprint 44E256C34FA45C5DF03986309D88B75E5026CE4A
subject-name CN=cEdge-SDWAN-1.crv
vrf 1
rsakeypair KEY-NEW
revocation-check none
!
ip local pool RA-POOL 10.20.14.1 10.20.14.100
!
crypto ikev2 name-mangler IKEV2-RA-MANGLER
 eap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

```

Configurazione client AnyConnect

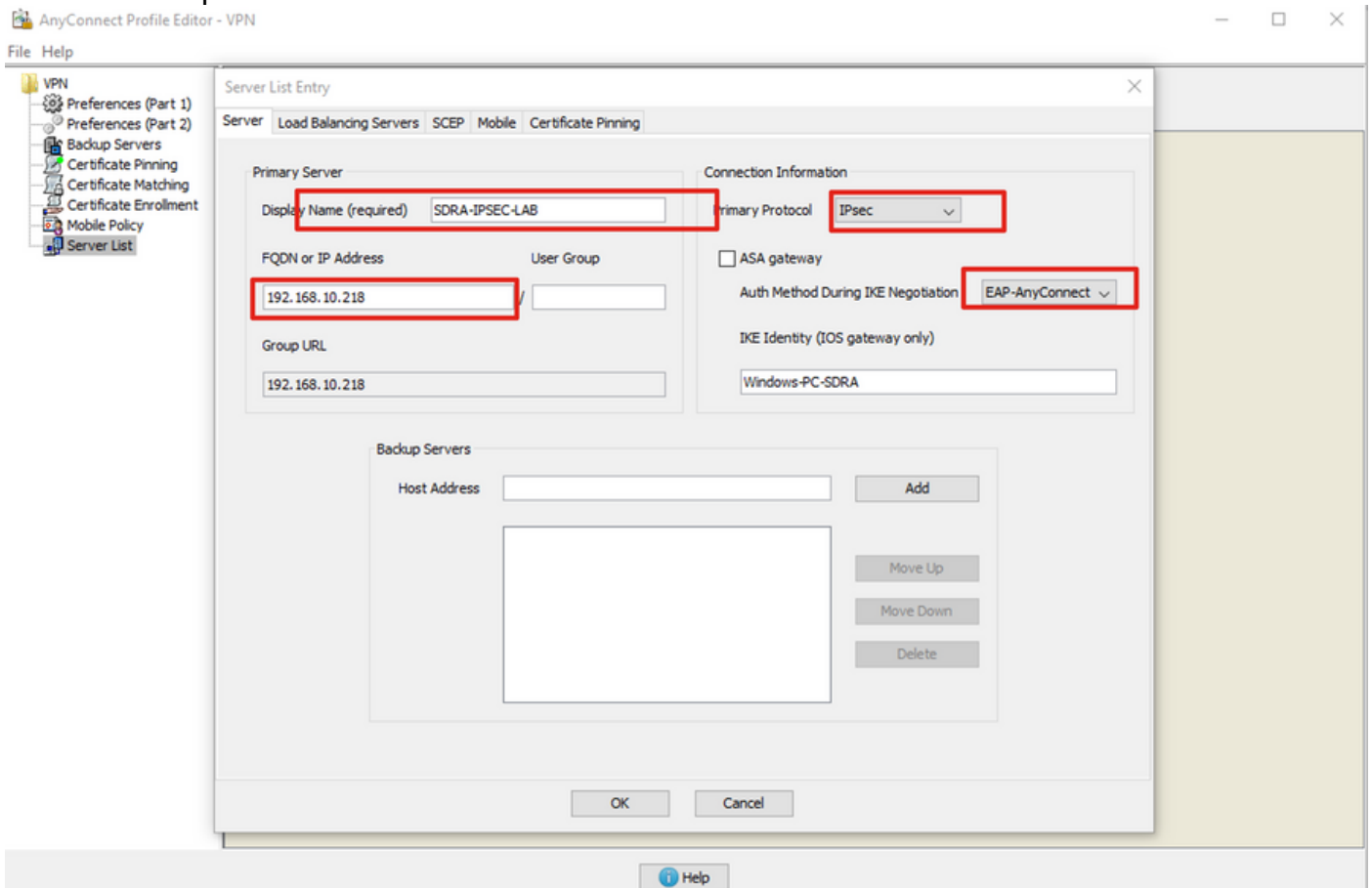
Il client AnyConnect utilizza SSL come protocollo predefinito per la definizione del tunnel e questo protocollo non è supportato per SD-WAN RA (Road map). RSA utilizza FlexVPN, pertanto IPSEC è il protocollo utilizzato ed è obbligatorio modificarlo e ciò avviene tramite il profilo XML.

L'utente può immettere manualmente il nome di dominio completo del gateway VPN nella barra degli indirizzi del client AnyConnect. Il risultato è la connessione SSL al gateway.



Configurazione dell'Editor di profili AnyConnect

- Passare a **Elenco server** e fare clic su **Aggiungi**.
- Selezionare **IPsec** come "Protocollo primario".
- Deselezionare l'opzione **ASA gateway**.
- Selezionare **EAP-AnyConnect** come "Metodo di autenticazione durante la negoziazione IKE".
- **Display/Name (obbligatorio)** è il nome usato per salvare la connessione sul client AnyConnect.
- **L'FQDN o l'indirizzo IP** deve essere archiviato con l'indirizzo IP del perimetro (pubblico).
- Salvare il profilo.



Installare il profilo AnyConnect (XML)

Il profilo XML può essere inserito manualmente nella directory:

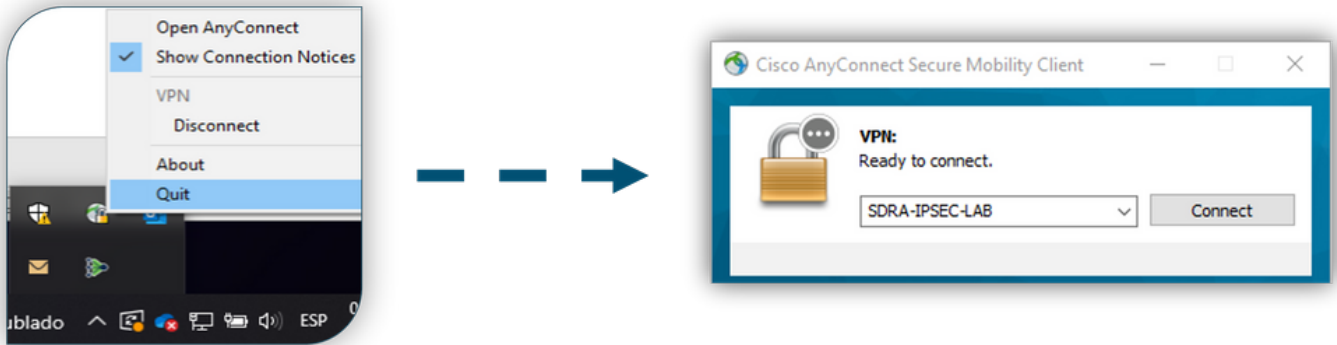
For Windows:

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

For MAC OS:

```
/opt/cisco/anyconnect/profile
```

Affinché il profilo sia visibile nella GUI, è necessario riavviare il client AnyConnect. Per riavviare il processo, fare clic con il pulsante destro del mouse sull'icona AnyConnect nell'area di notifica di Windows e selezionare l'opzione **Quit (Esci)**:



Disabilitazione del download di AnyConnect

Il client AnyConnect tenta di eseguire il download del profilo XML dopo aver eseguito l'accesso per impostazione predefinita.

Se il profilo non è disponibile, la connessione non riesce. Per risolvere questo problema, è possibile disabilitare la funzionalità di download dei profili AnyConnect sul client stesso.

Per Windows:

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

Per MAC OS:

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

L'opzione "BypassDownloader" è impostata su "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>
```

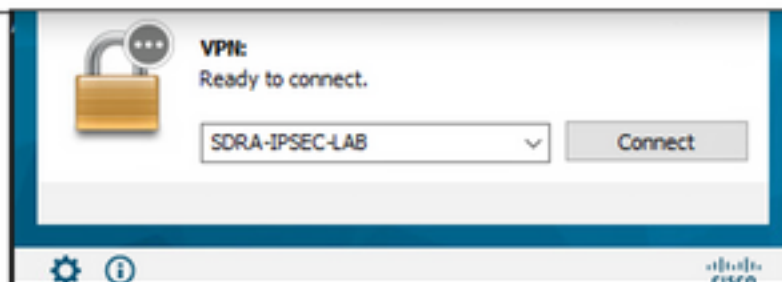
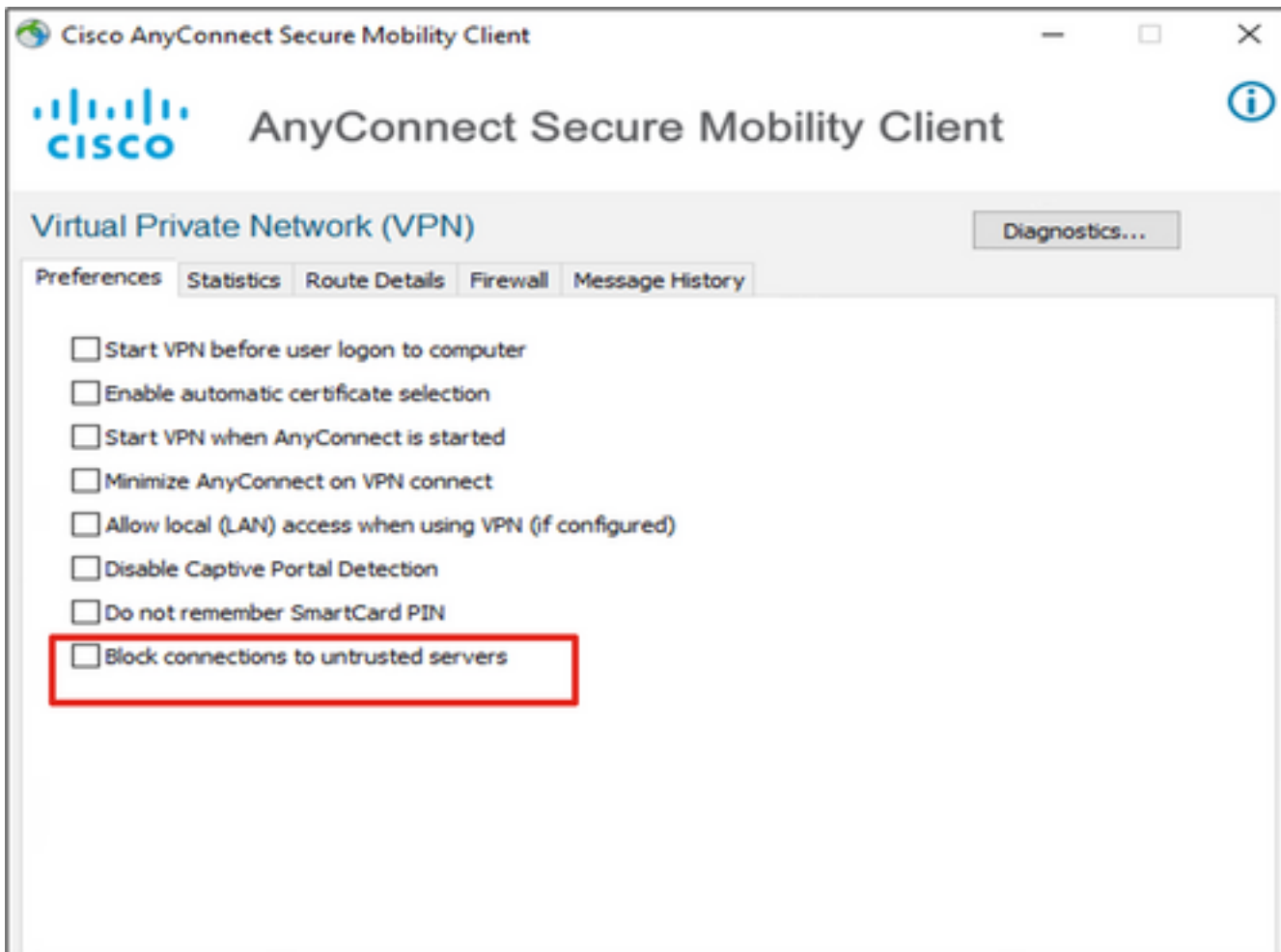
```
<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
<RestrictWebLaunch>>false</RestrictWebLaunch>
<StrictCertificateTrust>>false</StrictCertificateTrust>
<UpdatePolicy>
<AllowComplianceModuleUpdatesFromAnyServer>>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>>true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

Sblocco dei server non attendibili sul client AnyConnect

Passare a **Impostazioni > Preferenze** e deselezionare tutte le opzioni della casella.

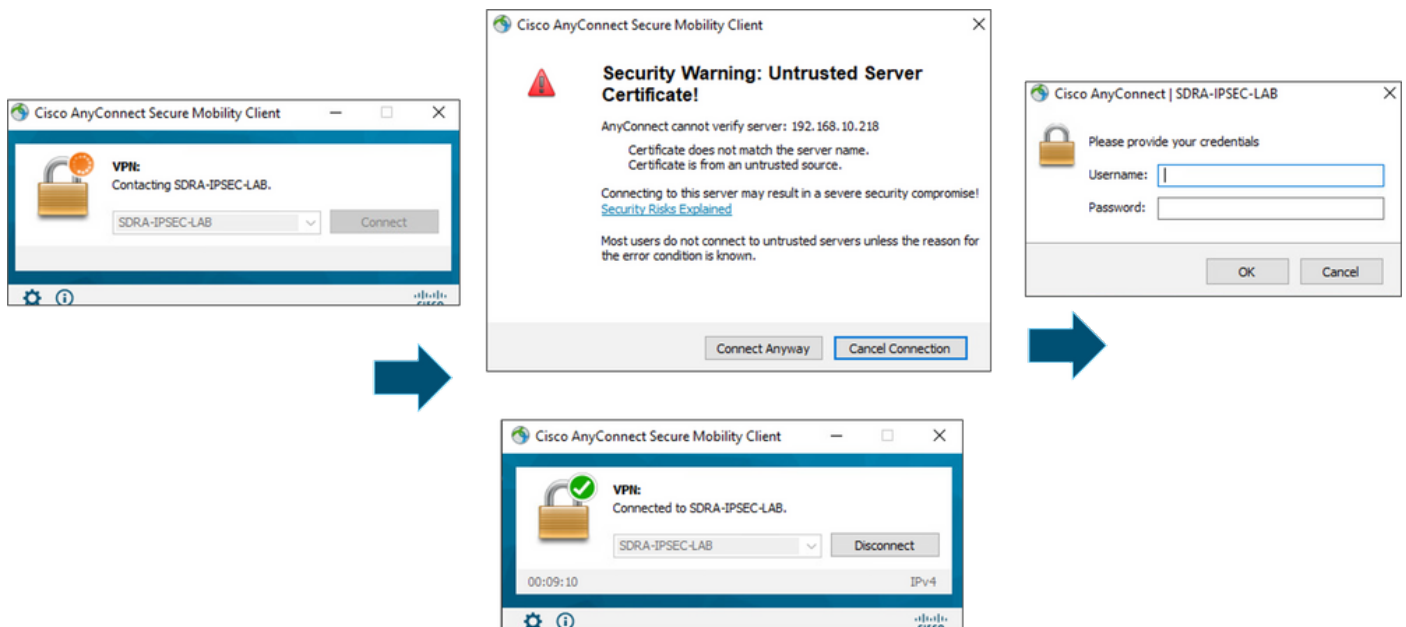
Il più importante è il **"Blocca connessioni a server non attendibili"** per questo scenario.

Nota: Il certificato utilizzato per l'autenticazione dell'headend/cEdge RA è quello creato e firmato in precedenza dal server CA in Cisco IOS® XE. Poiché questo server CA non è un'entità pubblica come GoDaddy, Symantec, Cisco e così via. Il client del PC interpreta il certificato come un server non attendibile. Questo problema viene risolto utilizzando un certificato pubblico o un server CA considerato attendibile dalla società.



Usa client AnyConnect

Una volta posizionata tutta la configurazione SDRA, il flusso per una connessione riuscita viene mostrato come immagine.



Verifica

L'interfaccia del modello virtuale viene utilizzata per creare l'interfaccia di accesso virtuale per avviare un canale crittografico e stabilire le associazioni di sicurezza (SA) IKEv2 e IPsec tra il server (cEdge) e il client (utente AnyConnect).

Nota: L'interfaccia del modello virtuale è sempre **attiva/inattiva**. Lo stato è **attivo** e il protocollo è **inattivo**.

```
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
```

Controllare la configurazione effettiva applicata per l'interfaccia Virtual-Access associata al client con il comando **show derived-config interface virtual-access<number>**.

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

```
tunnel destination 192.168.10.219
tunnel protection ipsec profile IKEV2-RA-PROFILE
no tunnel protection ipsec initiate
end
```

Verificare le associazioni di sicurezza IPsec (SA) del client AnyConnect con il comando **show crypto ipsec sa peer <AnyConnect Public IP >**.

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

Controllare i parametri SA IKEv2 per la sessione, il nome utente e l'indirizzo IP assegnato.

Nota: L'indirizzo IP assegnato deve corrispondere all'indirizzo IP sul lato client di 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
```

Informazioni correlate

- [Accesso remoto Cisco SD-WAN](#)
- [Configurazione del server FlexVPN](#)
- [Scarica AnyConnect](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)