تكوين الوصول عن بعد إلى SD-WAN (SDRA) باستخدام خادم AnyConnect و ISE

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين SD-WAN للوصول عن بعد (SDRA) مع عميل AnyConnect باستخدام الوضع الذاتي Cisco IOS® XE كخادم CA، وخادم Cisco Identity Services Engine (ISE) للمصادقة والتفويض والمحاسبة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)
- البنية الأساسية للمفاتيح العام (PKI)
- FlexVPN
- خادم RADIUS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

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

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

ما هي شبكة VPN للوصول عن بعد؟

تسمح شبكة VPN للوصول عن بعد للمستخدم البعيد بالاتصال بأمان بشبكات الشركة واستخدام التطبيقات والبيانات التي يمكن الوصول إليها فقط من خلال الأجهزة الموصولة في المكتب.

تعمل شبكة VPN للوصول عن بعد بواسطة نفق ظاهري تم إنشاؤه بين جهاز موظف وشبكة الشركة.

يمر هذا النفق عبر الإنترنت العام ولكن البيانات التي يتم إرسالها ذهابا وإيابا خلاله محمية بواسطة بروتوكولات التشفير والأمان للمساعدة في الحفاظ على خصوصيته وأمنه.

المكونان الرئيسيان في هذا النوع من شبكات VPN هما خادم وصول إلى الشبكة/وحدة الاستقبال والبث الخاصة بـ RA وبرنامج عميل شبكة VPN.

ما هو SD-WAN Remote Access VPN؟

تم دمج الوصول عن بعد في حل SD-WAN الذي يزيل الحاجة إلى بنية أساسية منفصلة من الطرازين Cisco SD-WAN و RA ويتيح إمكانية التوطين السريع لخدمات RA باستخدام Cisco AnyConnect كعميل برنامج RA.

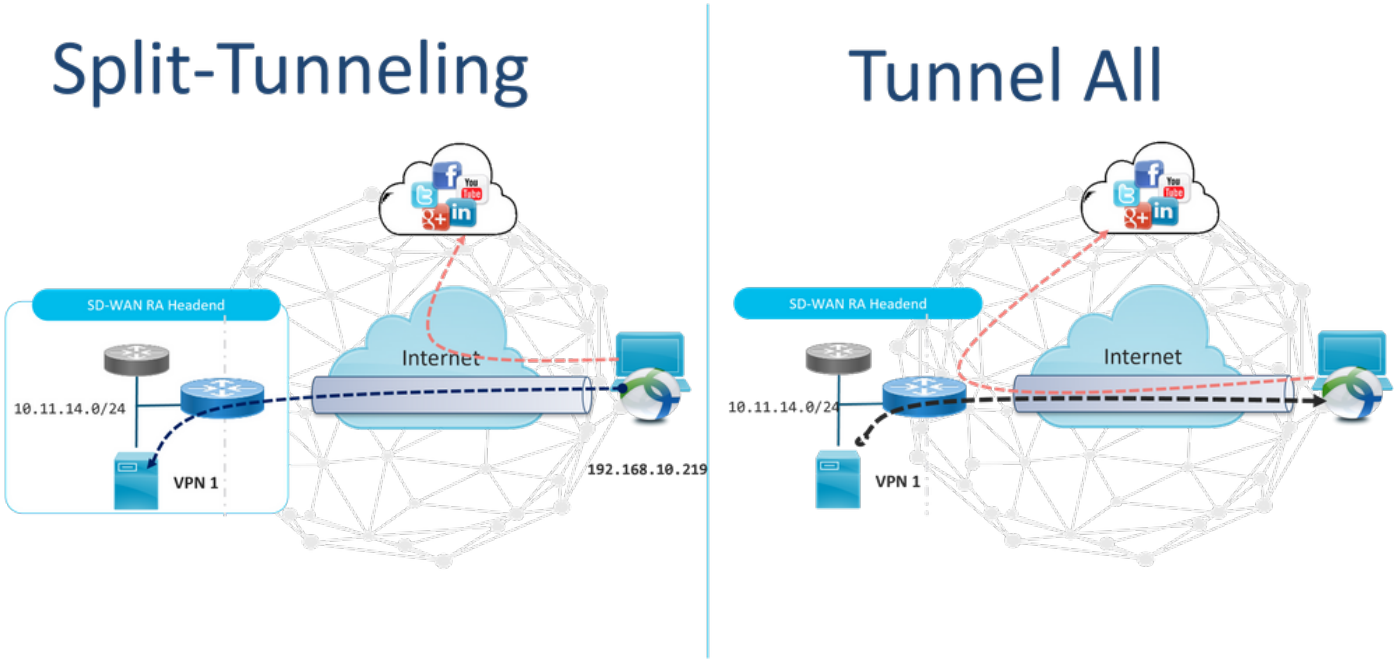
يوفر "الوصول عن بعد" إمكانية وصول المستخدمين عن بعد إلى شبكة المؤسسة. وهذا يمكن العمل من المنزل.

الفوائد

- يوفر RA الوصول إلى شبكة المؤسسة من الأجهزة/المستخدمين في المواقع البعيدة. (منظمة الصحة العالمية)
- قم بتوسيع حل Cisco SD-WAN لمستخدمي RA دون الحاجة إلى أن يكون كل جهاز مستخدم RA جزءا من بنية Cisco SD-WAN.
- أمان البيانات
- انقسام الاتصال النفقي أو نفق الكل
- قابلية التطوير
- القدرة على توزيع حمل RA عبر العديد من أجهزة Cisco IOS® XE SD-WAN في بنية Cisco SD-WAN.

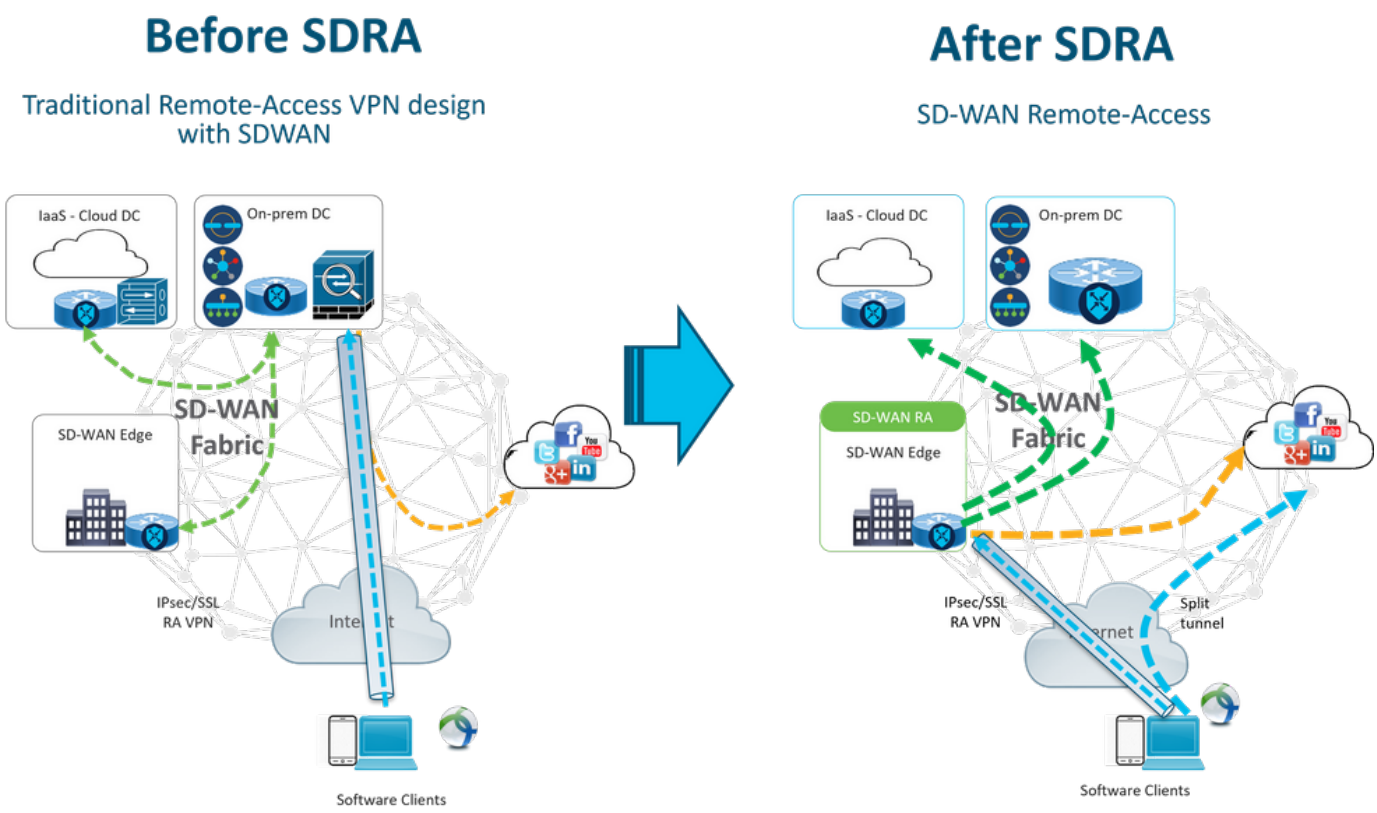
انقسام الاتصال النفقي مقابل النفق الكل

يتم إستخدام الاتصال النفقي المنقسم في السيناريوهات التي يجب فيها إنشاء قنوات لحركة مرور معينة فقط (شبكات SD-WAN الفرعية على سبيل المثال) كما هو موضح في الصورة.



قبل SDRA وبعد SDRA

يتطلب التصميم التقليدي للوصول عن بعد للشبكة الخاصة الظاهرية (VPN) بنية أساسية منفصلة لشبكة RA خارج نطاق بنية SD-WAN من Cisco لتوفير وصول المستخدم عن بعد إلى الشبكة مثل الأجهزة التي ليس لها شبكة SD-WAN مثل ASA أو Cisco IOS® XE العادي أو الأجهزة التابعة لجهة خارجية، ويتم نقل حركة مرور RA إلى جهاز SD-WAN كما هو موضح في الصورة.



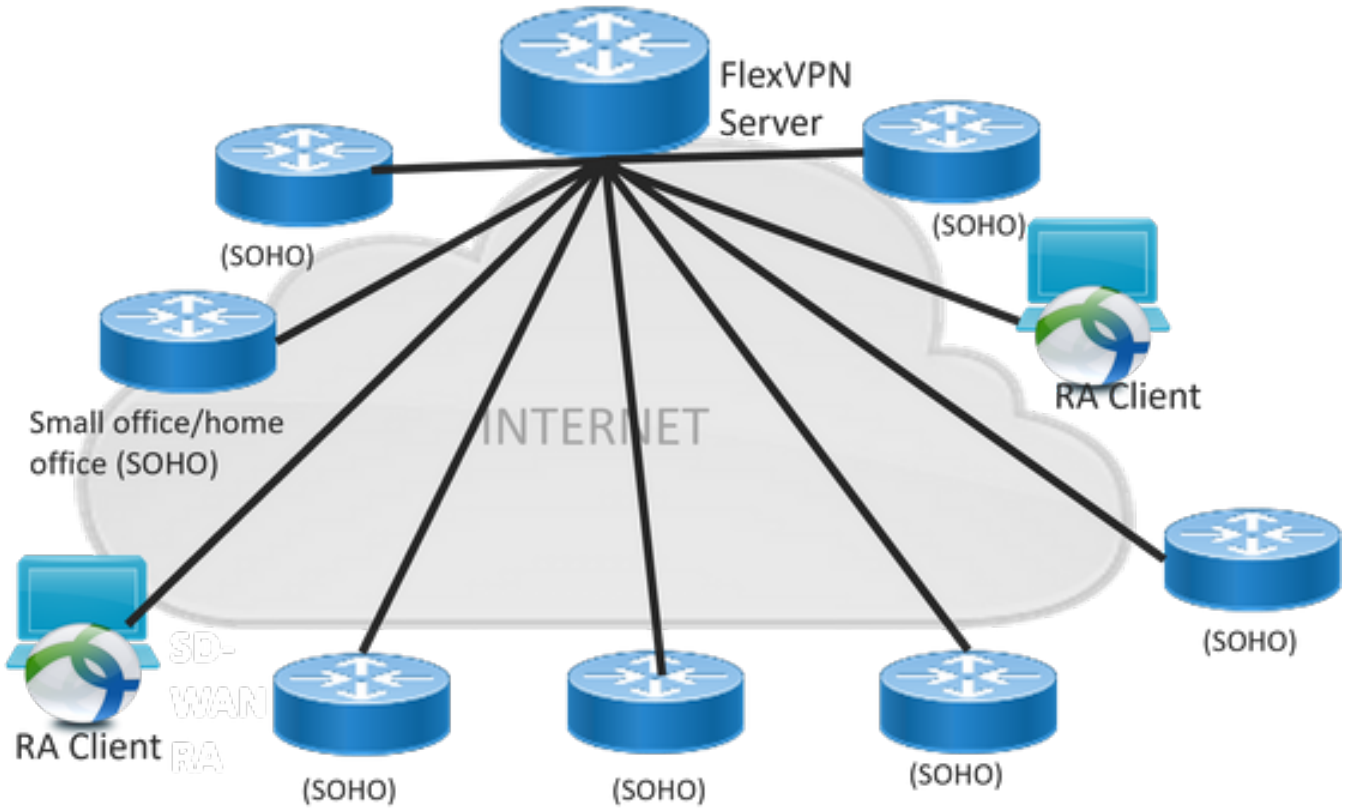
يعمل برنامج SD-WAN للوصول عن بعد على تغيير طريقة اتصال المستخدمين البعيدين بالشبكة. فهي تتصل مباشرة بالخادم طراز cEdge الذي يتم إستخدامه كنقطة الاستقبال والبث طراز RA. توسيع ميزات ومزايا شبكة SD-WAN من Cisco لمستخدمي RA. مستخدمو RA يصبحون مستخدمين فرعيين من جانب شبكة LAN.

بالنسبة لكل عميل RA، تقوم وحدة الاستقبال والبث طراز SD-WAN RA بتعيين عنوان IP إلى عميل RA وإضافة مسار مضيف ثابت إلى عنوان IP المعين في حقل الخدمة VRF الذي يتم فيه وضع مستخدم RA.

يحدد المسار الثابت نفق VPN لاتصال عميل RA. تقوم وحدة الاستقبال والبث SD-WAN RA بالإعلان عن بروتوكول IP الثابت داخل خدمة VRF الخاصة بعميل RA باستخدام OMP إلى جميع الأجهزة الطرفية في شبكة VPN الخاصة بالخدمة.

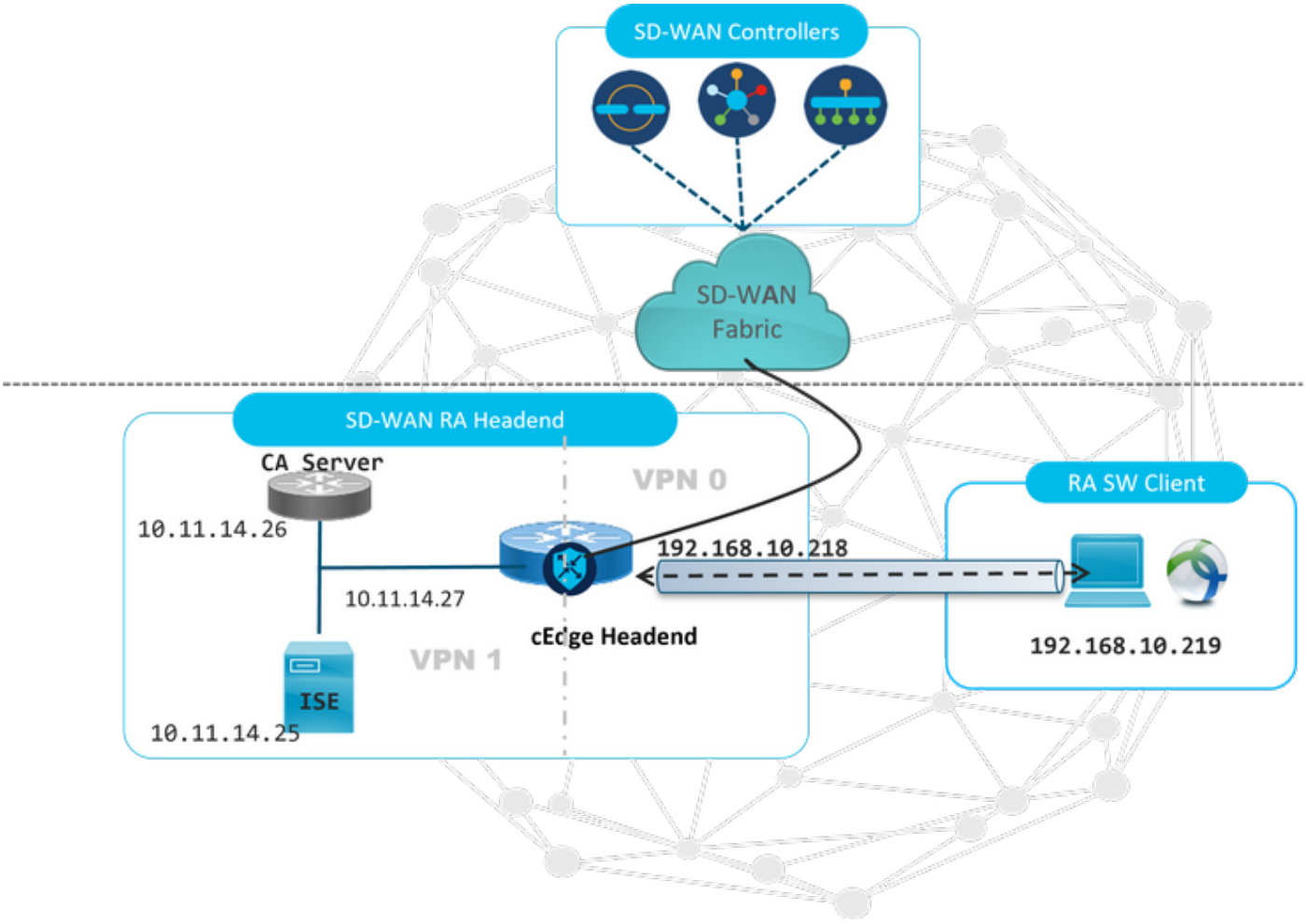
ما هو FlexVPN؟

يستغل SD-WAN RA حل FlexVPN RA من Cisco. FlexVPN هو تطبيق Cisco لميزة معيار IKEv2 نموذج موحد و CLI يجمع بين موقع إلى موقع **والوصول عن بعد** ومخططات محورية ومتحدثة وشبكات جزئية (تحدث مباشرة). توفر شبكة FlexVPN إطار عمل بسيط ولكنه قابل لإضافة وحدات أخرى يستخدم بشكل مكثف نموذج واجهة النفق بينما يظل متوافقا مع عمليات تنفيذ شبكات VPN القديمة.



تكوين المتطلبات الأساسية

لهذا المثال، تم إنشاء إعداد مختبر SD-WAN RA كما هو موضح في الصورة.



تم تكوين مكونات إضافية لسيناريو مختبر SD-WAN RA هذا:

- برنامج Cisco IOS® XE العادي في الوضع الذاتي كخادم CA.
- خادم ISE/RADIUS للمصادقة والتخويل والمحاسبة.
- جهاز كمبيوتر يعمل بنظام التشغيل Windows يتسم بقابلية الوصول إلى الخادم طراز cEdge من خلال واجهة شبكة WAN.
- AnyConnect Client مثبت بالفعل.

ملاحظة: تم وضع خوادم CA و RADIUS في الخدمة VRF 1. يجب أن يكون كل الخادمين قابلين للوصول إليهما من خلال التردد اللاسلكي للخدمة لجميع منافذ SD-WAN RA الرئيسية.

ملاحظة: يتم دعم الوصول عن بعد إلى SD-WAN من Cisco على الإصدار 17.7.1a والأجهزة المحددة ل SDRA. بالنسبة للأجهزة المدعومة، انتقل المرجع إلى: [الأنظمة الأساسية المدعومة لنقطة الاستقبال والبث SD-WAN RA]

تكوين ISE

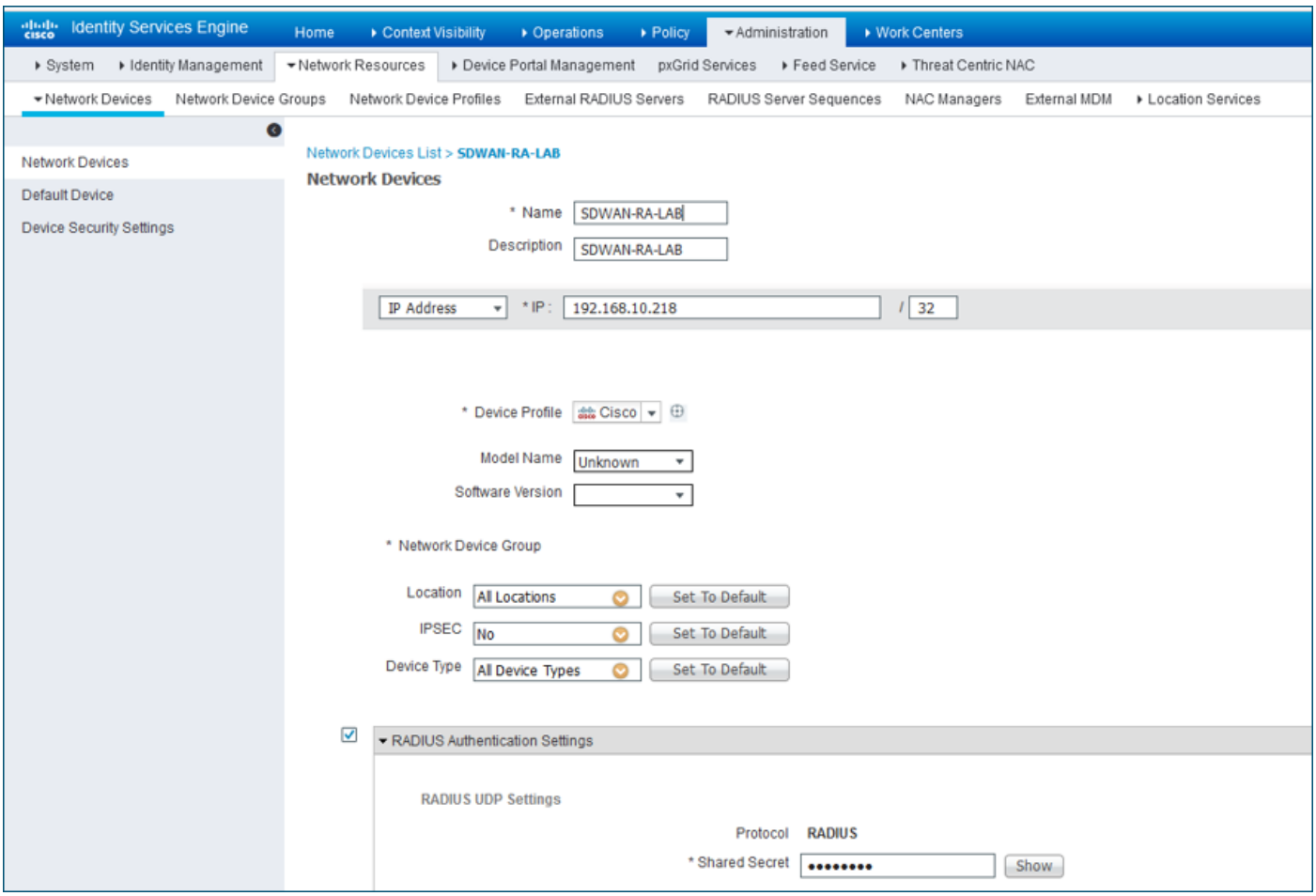
لدعم وحدة الاستقبال والبث SD-WAN RA، تأكد من تكوين المعلمات على خادم RADIUS. هذه المعلمات مطلوبة لاتصالات RA:

- مسوغات مصادقة المستخدم اسم المستخدم وكلمة المرور لاتصالات AnyConnect-EAP
- معلمات النهج (السمات) التي تنطبق على مستخدم أو على مجموعة مستخدمين VRF:

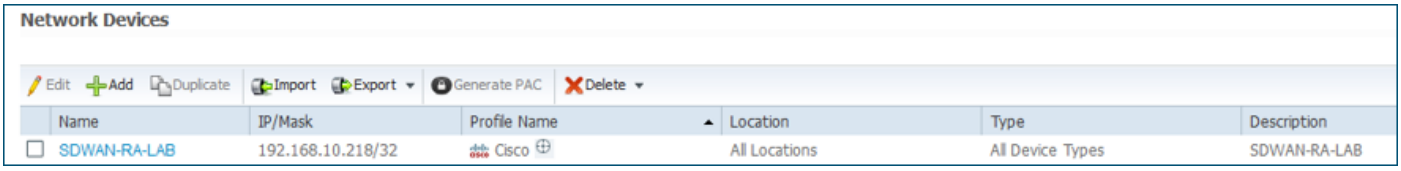
شبكة VPN الخاصة بالخدمة التي تم تعيين مستخدم RA إليها**مسم تجمع IP**: اسم تجمع IP المحدد على وحدة الاستقبال والبث RAI**لشبكات الفرعية للخادم**: وصول الشبكة الفرعية إلى مستخدم RA

الخطوة الأولى لتكوين في ISE هي وحدة الاستقبال والبث طراز RA أو عنوان IP cEdge كجهاز شبكة لتمكين إجراء طلبات RADIUS إلى ISE.

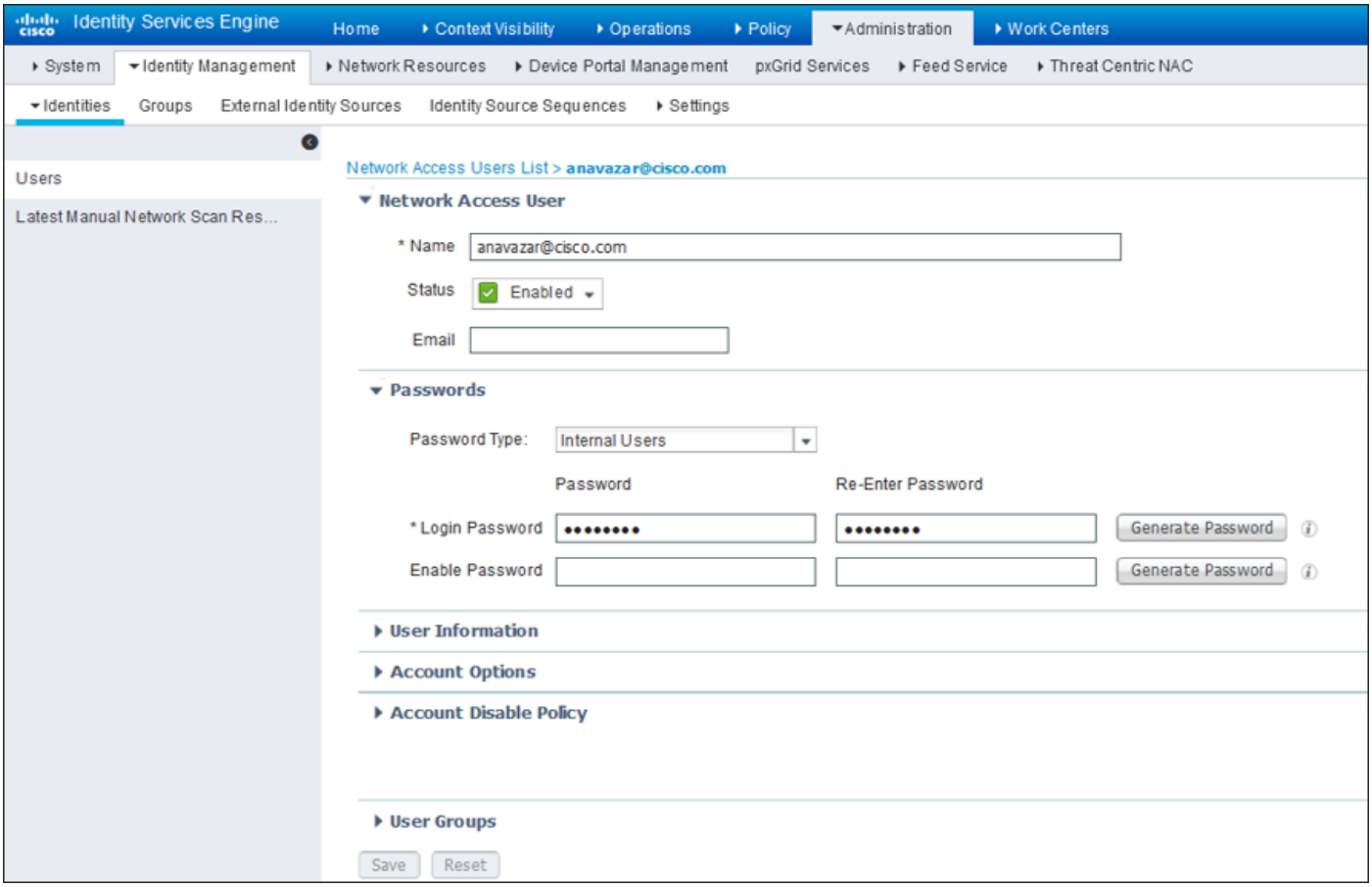
انتقل **إلى الإدارة>أجهزة الشبكة** وأضفت عنوان IP وكلمة المرور RA HEAD HEAD HEAD (cEdge) كما هو موضح في الصورة.



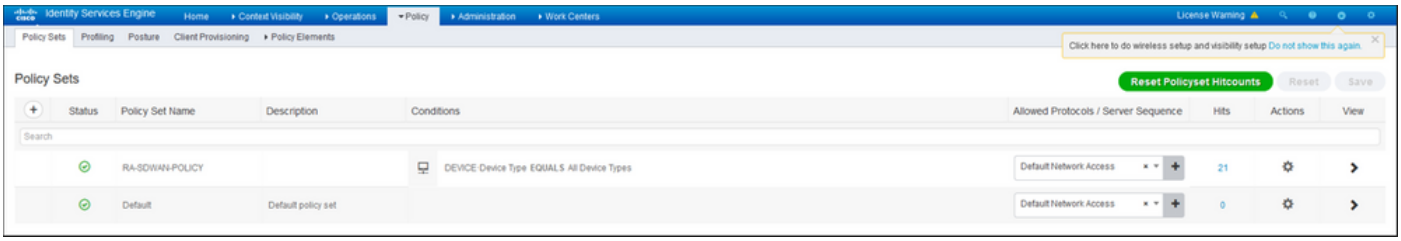
تمت إضافة جهاز الشبكة كما هو موضح في الصورة.



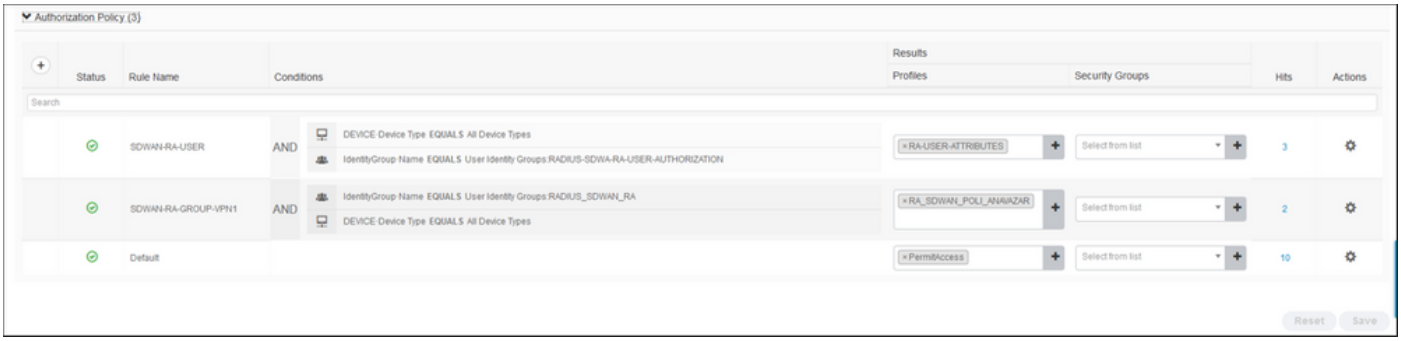
يلزم خادم RADIUS لتكوين أسماء المستخدمين وكلمة المرور لمصادقة AnyConnect كما هو موضح في الصورة. انتقل إلى **إدارة > هوياتي**.



يجب إنشاء "مجموعة نمج" باستخدام حالة مطابقة ليتم الوصول إليها كما هو موضح في الصورة. في هذه الحالة، يتم إستخدام شرط **جميع أنواع الأجهزة**، مما يعني أن جميع المستخدمين يضربون هذا النمج.



بعد ذلك، تم إنشاء "نمج التخويل" واحد لكل شرط. الشرط **كافة أنواع الأجهزة** ومجموعات الهوية للمطابقة.

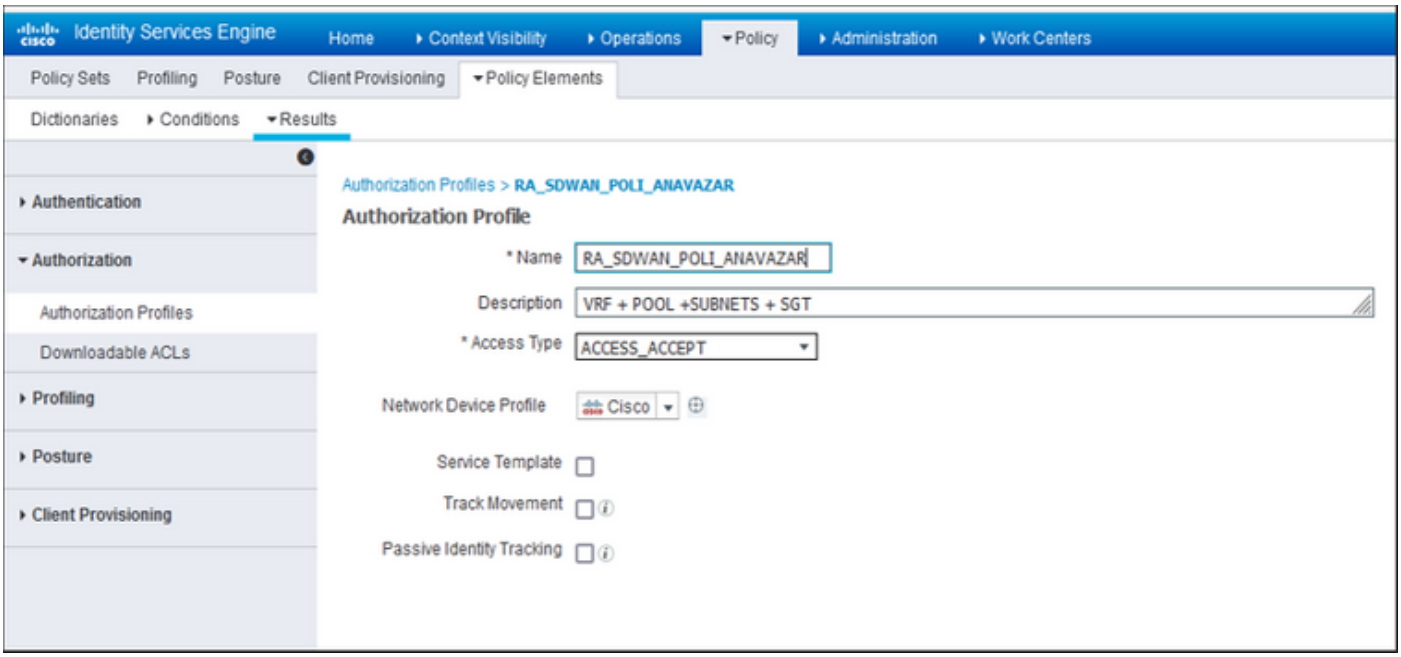


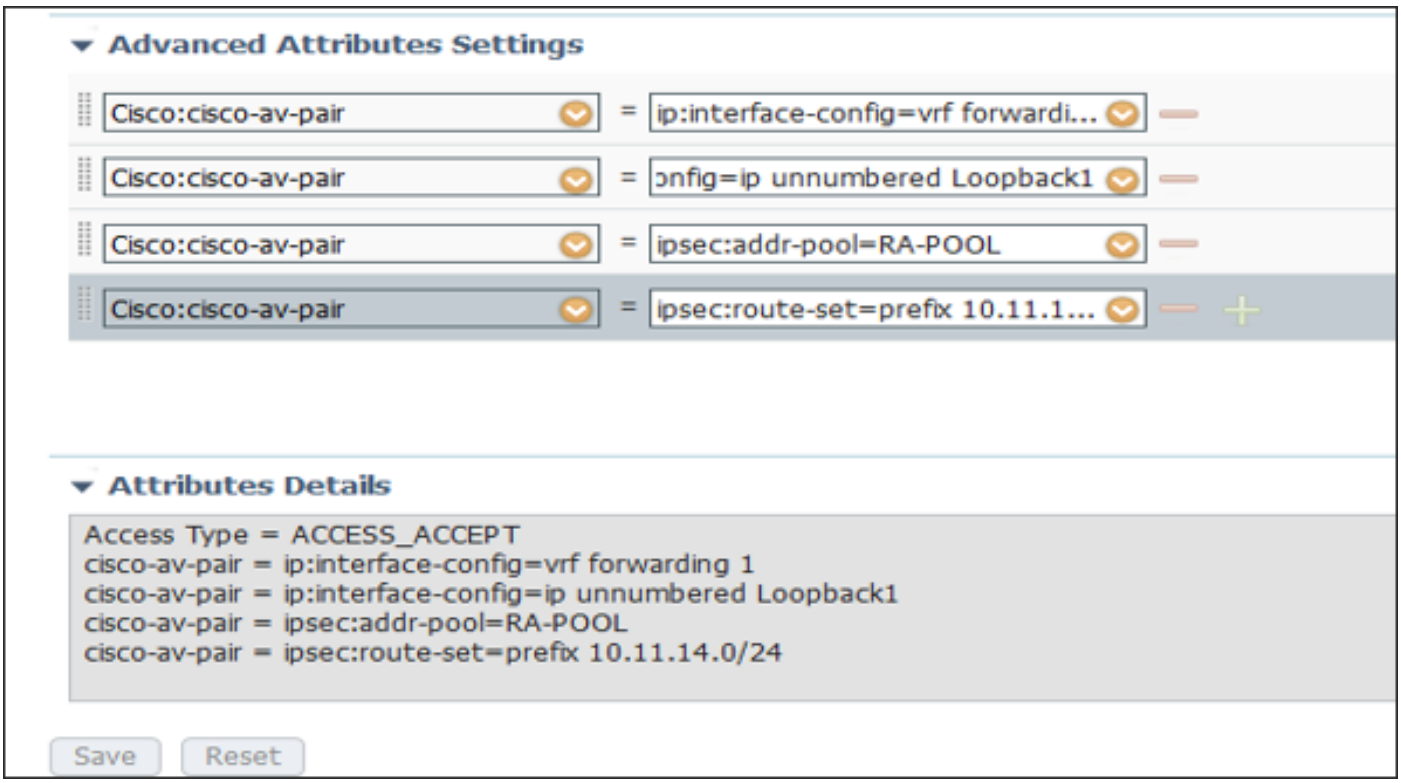
في ملف تعريف **التخويل**، نحتاج إلى تكوين **نوع الوصول** على أنه access_ACCEPT ضمن **إعدادات السمات المتقدمة**، حدد مورد Cisco وسمة **زوج Cisco وCisco-AV.**

من الضروري تكوين بعض معلمات النمج للمستخدمين:

- VRF، خدمة VRF التي ينتمي إليها المستخدم.
- اسم تجمع IP، يتم تعيين عنوان IP لكل اتصال مستخدم، ينتمي إلى تجمع IP الذي تم تكوينه في cEdges.
- الشبكات الفرعية التي يمكن للمستخدم الوصول إليها

تحذير: يجب أن يأتي الأمر **ip vrf forwarding** قبل الأمر **ip unnumber**. إذا تم نسخ واجهة الوصول الظاهرية من القالب الظاهري، وتم تطبيق الأمر **ip vrf forwarding** بعد ذلك، فسيتم إزالة أي تكوين IP من واجهة الوصول الظاهري.





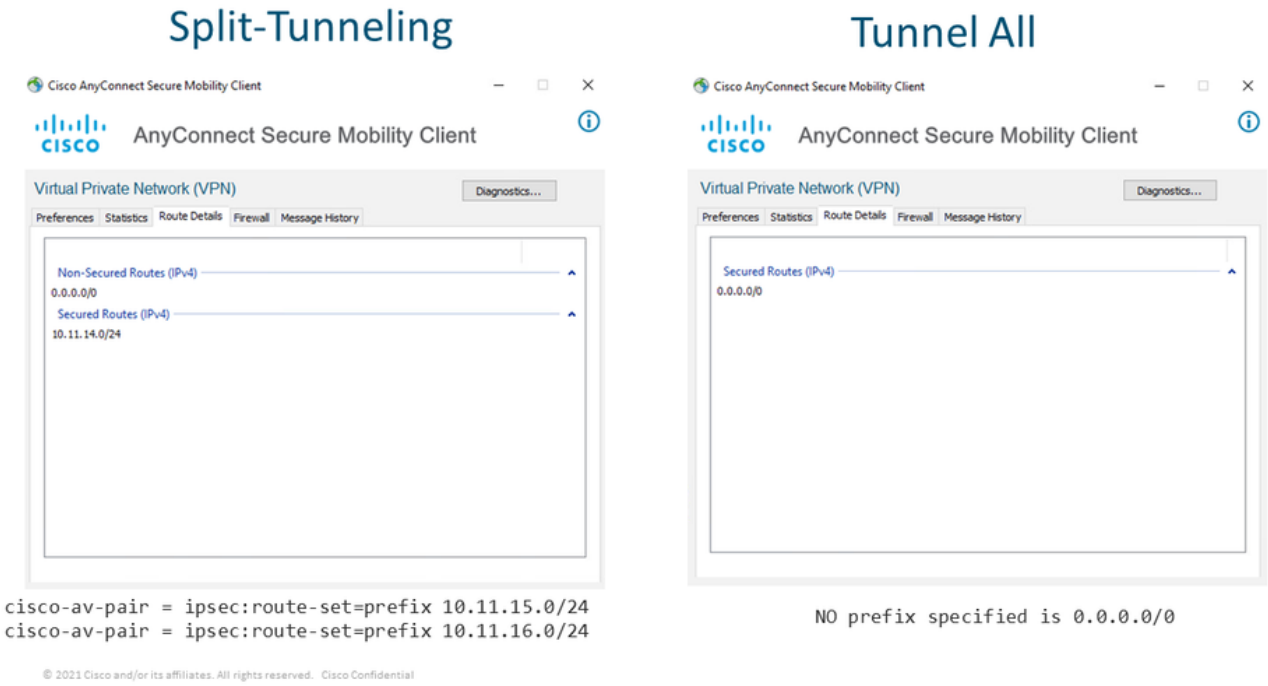
سمات المستخدم:

```
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 مقابل Tunnel all في AnyConnect Client

يتم تثبيت سمة **ipsEc:route-set=prefix** التي تم تلقيها في عميل AnyConnect كما هو موضح في الصورة.




```
cisco-av-pair = ipsec:route-set=prefix 10.11.15.0/24
cisco-av-pair = ipsec:route-set=prefix 10.11.16.0/24
```

```
NO prefix specified is 0.0.0.0/0
```


تكوين خادم CA في Cisco IOS® XE

يوفر خادم CA الشهادات لأجهزة Cisco IOS® XE SD-WAN ويمكن وحدة الاستقبال والبث RA من مصادقة نفسها على عملاء RA.

لا يمكن أن يكون CEDGE خادم CA لأن أوامر خادم PKI المشفرة هذه غير مدعومة في CISCO IOS® XE SD-WAN.

- إنشاء زوج مفاتيح RSA
- إنشاء PKI TrustPoint لخادم CA قم بتكوين زوج المفاتيح باستخدام KEY-CA الذي تم إنشاؤه مسبقا.

  ملاحظة: يجب أن يستخدم خادم PKI و PKI TrustPoint نفس الاسم.

- إنشاء خادم CA تكوين اسم المصدر لخادم CAقم بتنشيط خادم CA باستخدام "عدم إيقاف التشغيل"

```
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
!
```

تحقق ما إذا تم تمكين خادم CA.

```
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
```

تحقق ما إذا كانت شهادة خادم CA مثبتة.

```
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
```

يتم إستخدام **بصمة الإصبع SHA 1** من شهادة CA على **Crypto PKI TrustPoint** في موجه cEdge (وحدة الاستقبال والبث RA) مع تكوين الوصول عن بعد.

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

تكوين SD-WAN RA

> **ملاحظة**: الا يغطي هذا المستند عملية ضم شبكة SD-WAN لوحدات التحكم و cEdge. ومن المفترض أن بنية شبكة SD-WAN تعمل بكفاءة تامة وكاملة.

تكوين PKI للتشفير

- إنشاء نقطة ثقة PKI.
- قم بتكوين عنوان URL لخادم CA.
- انسخ بصمة الإصبع SHA 1 من شهادة خادم CA.
- قم بتكوين اسم الموضوع واسم بديل للشهادة الهوية الجديدة.
- قم بتكوين rsakeypar باستخدام KEY-ID الذي تم إنشاؤه مسبقا.

```
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
```

اطلب مصادقة شهادة المرجع المصدق:

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

يولد CSR، ويرسل إلى خادم CA ويستلم شهادة الهوية الجديدة:

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

تحقق من شهادة CA وشهادة 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
```

تكوين 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
```

تكوين FlexVPN

تكوين تجمع IP

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

تكوين مقترحات IKEv2 (التشفير والمعلمات) والنهج:

```
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
```

تكوين مدير اسم ملف تعريف IKEv2:

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

ملاحظة: يستخدم **name-mangler** الاسم من البادئة في هوية EAP (اسم المستخدم) التي تحدد في هوية EAP التي تفصل البادئة واللاحقة.

تكوين شفرات IPsec:

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

تكوين ملف تعريف IKEv2 للتشفير:

```
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
```

تكوين ملف تعريف IPsec للتشفير:

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

تكوين واجهة القالب الظاهري:

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

تكوين القالب الظاهري في ملف تعريف IKEv2 للتشفير:

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

مثال تكوين SD-WAN RA

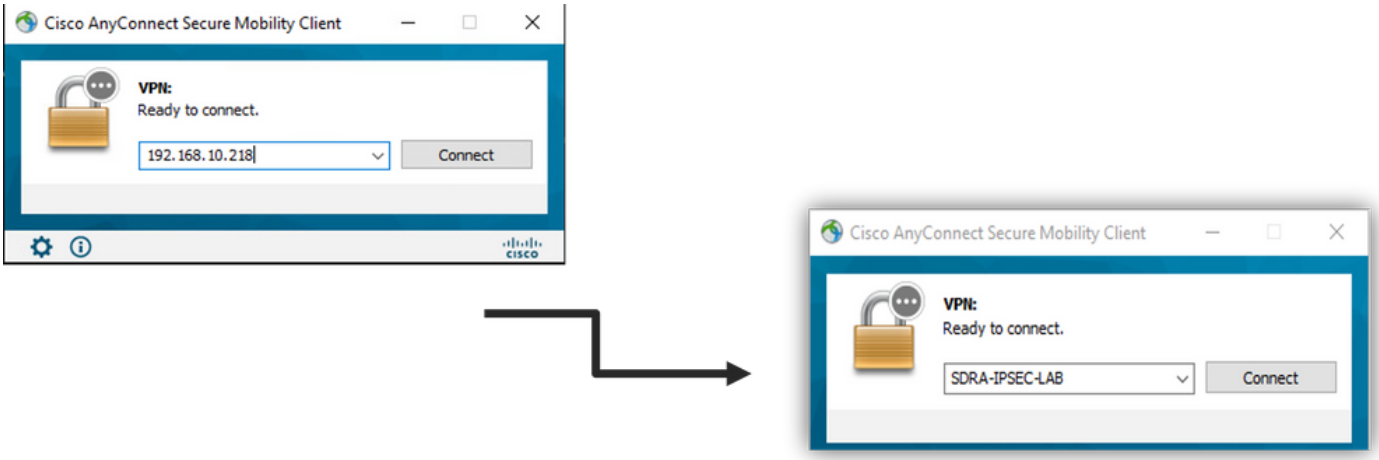
```
aaa new-model
!
aaa group server radius ISE-RA-Group
server-private 10.11.14.225 key Cisc0123
!
aaa authentication login ISE-RA-Authentication group ISE-RA-Group
aaa authorization network ISE-RA-Authorization group ISE-RA-Group
aaa accounting network ISE-RA-Accounting start-stop group ISE-RA-Group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

تكوين عميل AnyConnect

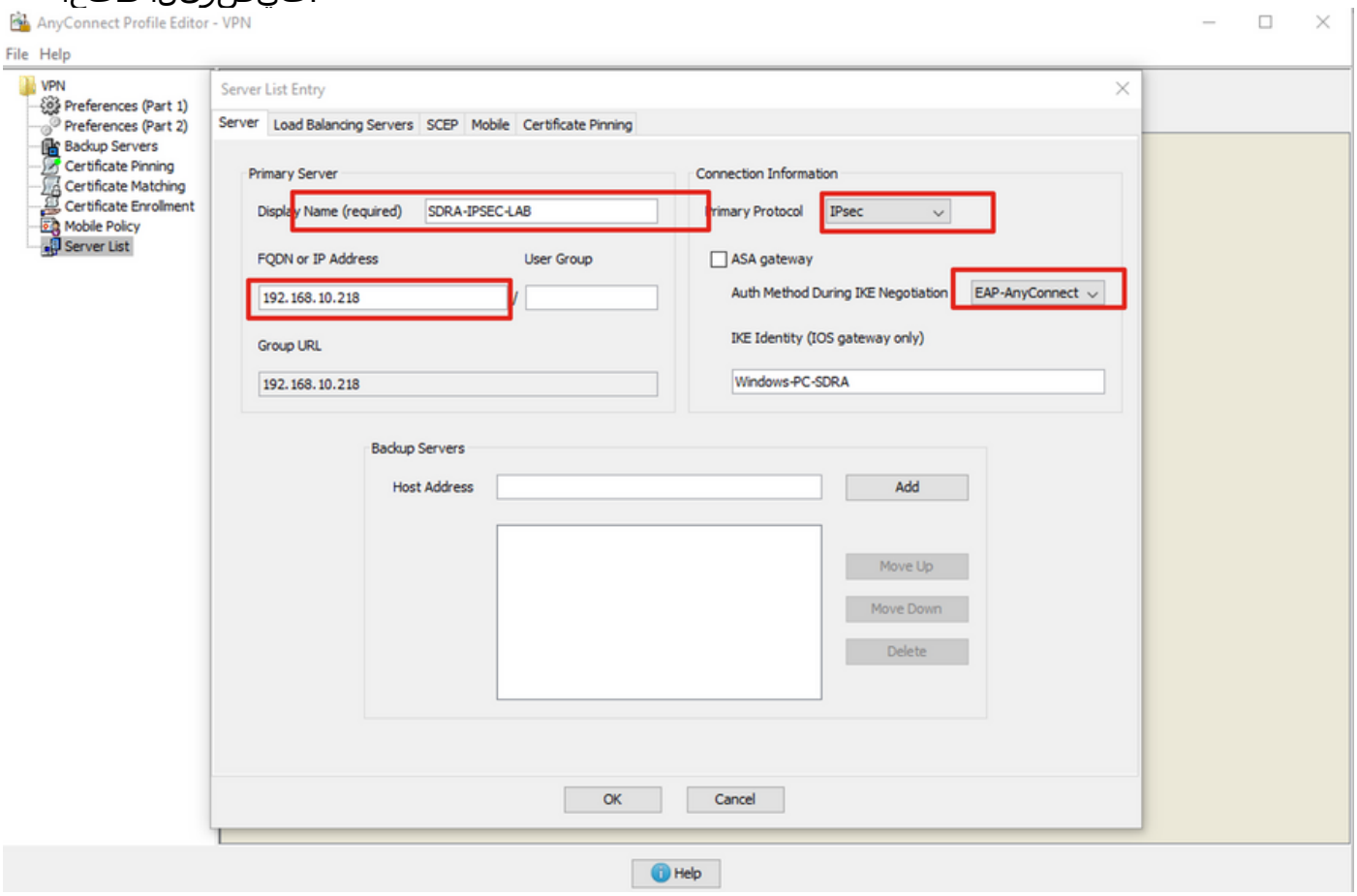
يستخدم عميل AnyConnect SSL كبروتوكول افتراضي لإنشاء النفق، وهو اذا البروتوكول غير مدعوم ل SD-WAN RA (خريطة الطريق). يستخدم RA FlexVPN، وبالتالي فإن IPSec وه تعريف ملف تعريف خالل من ذلك بذلك القيام تمت و ذلك تغيير لتمي إلزامي وهو المستخدم البروتوكول XML.

يمكن للمستخدم إدخال FQDN لعبارة VPN ودي في شريط العناوين الخاص بعميل AnyConnect. ينتج عن ذلك اتصال SSL بالبوابة.



تكوين محرر ملف تعريف AnyConnect

- انتقل إلى **قائمة الخوادم** وانقر فوق **إضافة**.
- حدد **IPsec** كبروتوكول أساسي.
- قم بإلغاء تحديد خيار **عبارة ASA**.
- حدد **EAP-AnyConnect** على أنه "طريقة المصادقة أثناء تفاوض IKE".
- **Display/Name (مطلوب) هو الاسم المستخدم لحفظ هذا الاتصال ضمن عميل AnyConnect.**
- **يجب تصنيف FQDN أو IP مع عنوان IP الخاص ب cEdge (الداخلي).**
- احفظ التوصيف.



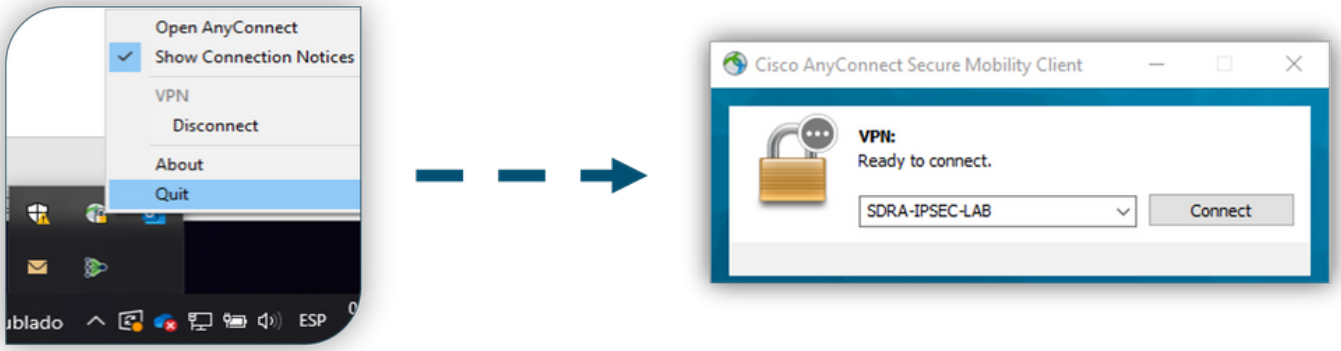
تثبيت ملف تعريف AnyConnect (XML)

يمكن وضع ملف تعريف XML يدويا في الدليل:

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

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

يلزم إعادة تشغيل عميل AnyConnect حتى يصبح ملف التعريف مرئيا في واجهة المستخدم الرسومية (GUI). يمكن إعادة تشغيل العملية بالنقر بزر الماوس الأيمن على رمز AnyConnect في درج Windows وتحديد خيار **إنهاء** التشغيل:



تعطيل أداة تنزيل AnyConnect

يحاول عميل AnyConnect إجراء تنزيل ملف تعريف XML بعد نجاح تسجيل الدخول بشكل افتراضي.

إذا لم يكن التوصيف متاحا ففشل التوصيل. كحل بديل، من الممكن تعطيل قدرة تنزيل ملف تعريف AnyConnect على العميل نفسه.

بالنسبة لنظام التشغيل Windows:

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

لنظام التشغيل Mac OS:

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

تم تعيين الخيار "BypassDownloader" على "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>
```

إلغاء حظر الخوادم غير الموثوق بها على عميل AnyConnect

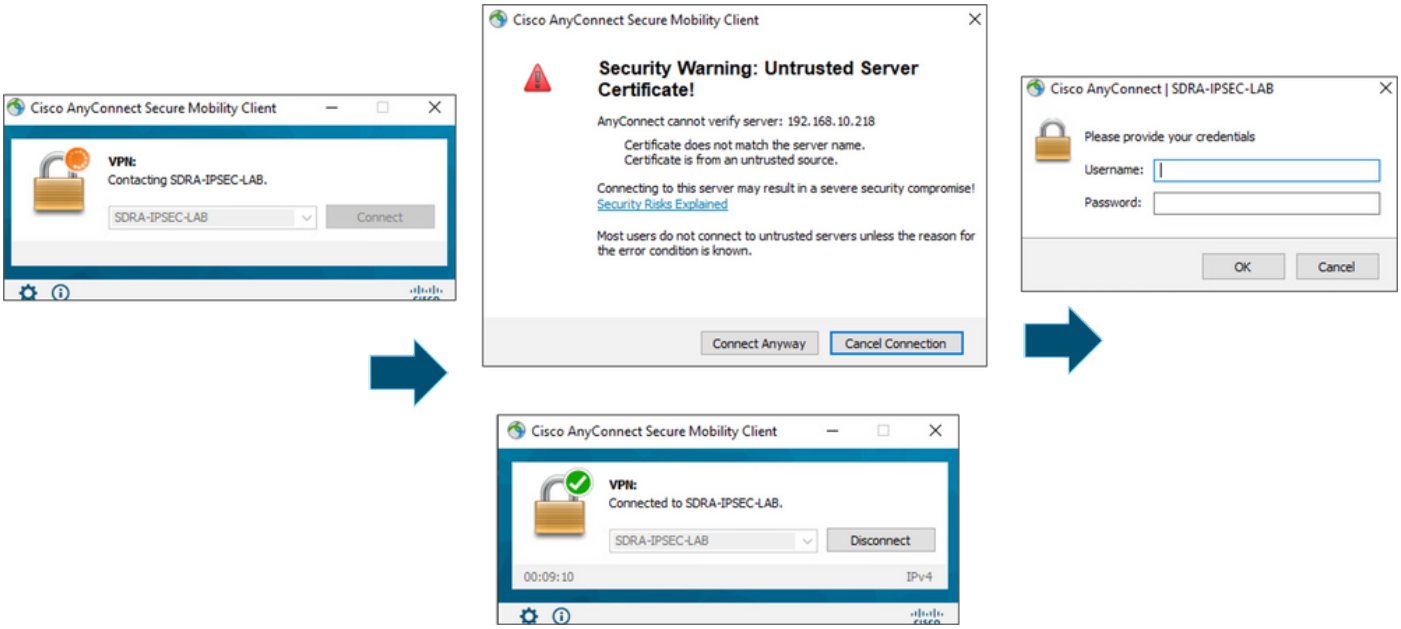
انتقل إلى **الإعدادات** > **التفضيلات** وألغي تحديد كل خيارات المربع.

والأهم من ذلك هو **حظر الاتصالات بالخوادم غير الموثوقة** "لهذا السيناريو.

> **ملاحظة:** الشهادة المستخدمة لمصادقة وحدة الاستقبال والبث RA/cEdge هي الشهادة التي تم إنشاؤها والتوقيع عليها مسبقا من قبل خادم CA في Cisco IOS® XE. بما أن خادم CA هذا ليس كيانا عاما مثل GoDaddy و Symantec و Cisco وما إلى ذلك. يفسر "العميل الكمبيوتر" الشهادة كخادم غير موثوق به. يتم إصلاح هذا الإجراء باستخدام شهادة عامة أو خادم CA موثوق به من قبل شركتك.

إستخدام عميل AnyConnect

بمجرد وضع تكوين SDRA بالكامل، يتم عرض التدفق لاتصال ناجح كصورة.



التحقق من الصحة

يتم إستخدام واجهة القالب الظاهري لإنشاء واجهة الوصول الظاهرية لبدء قناة تشفير وإنشاء اقترانات أمان IKEv2 و IPsec (SAs) بين الخادم (cEdge) والعميل (مستخدم AnyConnect).

> **ملاحظة**: واجهة القالب الظاهري دائما **لأعلى/لأسفل**. **الحالة** قيد **التشغيل** والبروتوكول **معطل**.

```
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
```

تحقق من التكوين الفعلي المطبق على واجهة الوصول الظاهري المرتبطة بالعميل باستخدام **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
```

تحقق من اقترانات أمان IPsec (SAs) لعميل AnyConnect باستخدام نظير **show crypto ipSec <AnyConnect Pubic IP >**.

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

تحقق من معلمات IKEv2 SA لجلسة العمل، واسم المستخدم، و IP المعين.

ملاحظة: يجب أن يتطابق عنوان IP المعين مع عنوان IP الموجود على جانب عميل 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
```

معلومات ذات صلة

- الوصول عن بعد إلى SD-WAN من Cisco
- تكوين خادم FlexVPN
- تنزيل AnyConnect
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).