تكوين IKEv2/ASA العميل الآمن في ASDM باستخدام AAA &؛ مصادقة CERT

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لتكوين العميل الآمن عبر IKEv2 على ASA باستخدام AAA ومصادقة الشهادة باستخدام ASDM.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين محرك خدمات الهوية من Cisco (ISE)
- تكوين أجهزة الأمان الظاهرية المعدلة (ASAv) من Cisco
- تكوين مدير أجهزة الأمان المعدلة (ASDM) من Cisco
- تدفق مصادقة VPN

المكونات المستخدمة

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

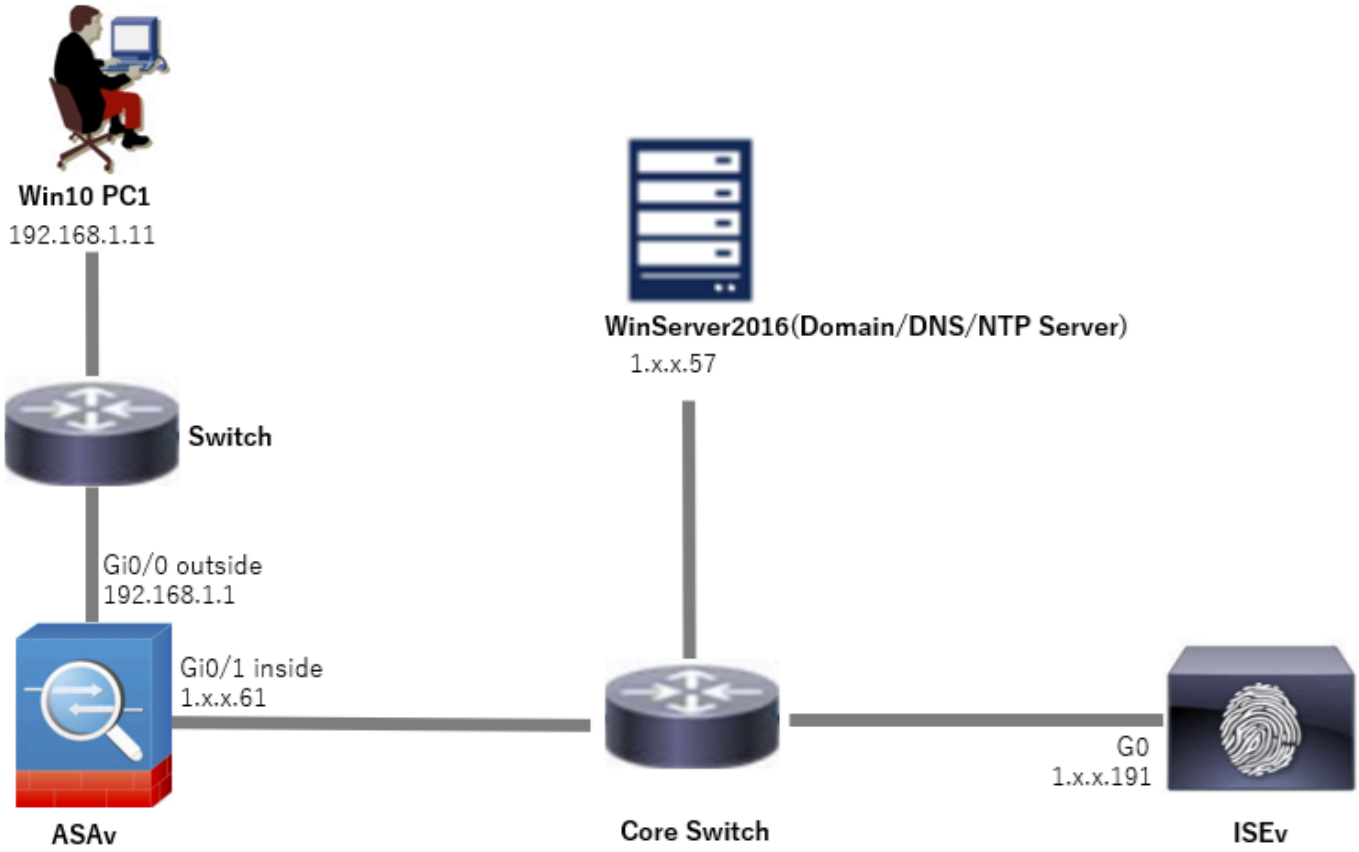
- برنامج التصحيح Identity Services Engine Virtual 3.3 1
- جهاز الأمان الظاهري القابل للتكيف 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- نظام التشغيل Windows Server 2016
- نظام التشغيل Windows 10

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

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.

اسم المجال الذي تم تكوينه على Windows Server 2016 هو ad.rem-system.com، والذي يتم إستخدامه كمثال في هذا المستند.



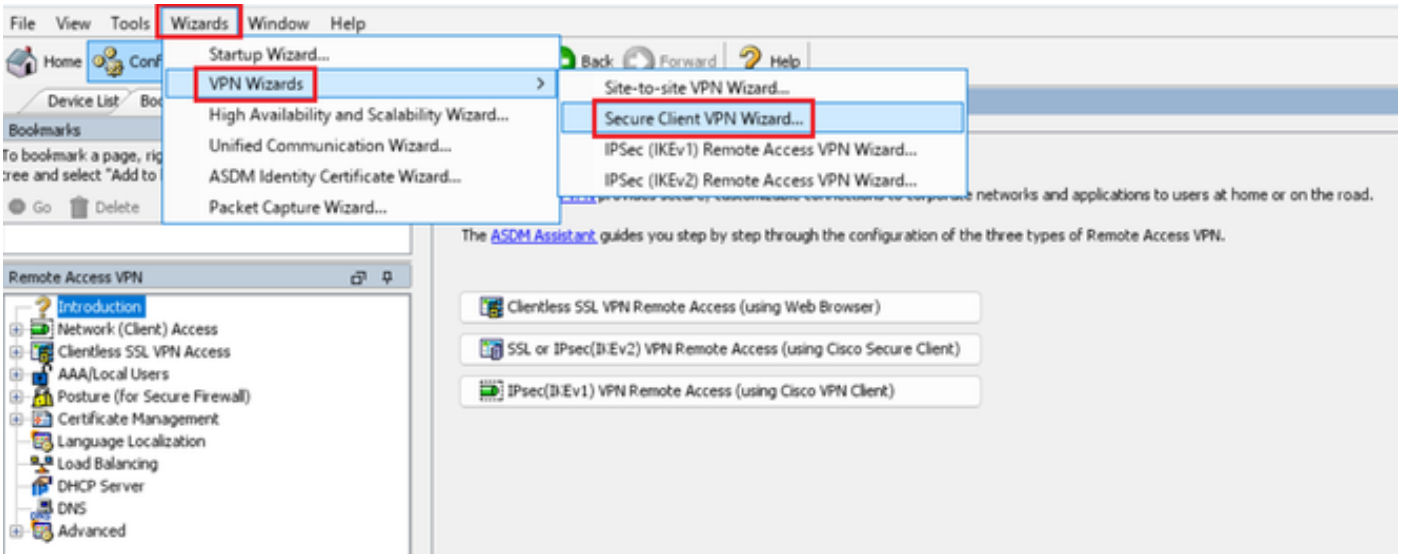
الرسم التخطيطي للشبكة

التكوينات

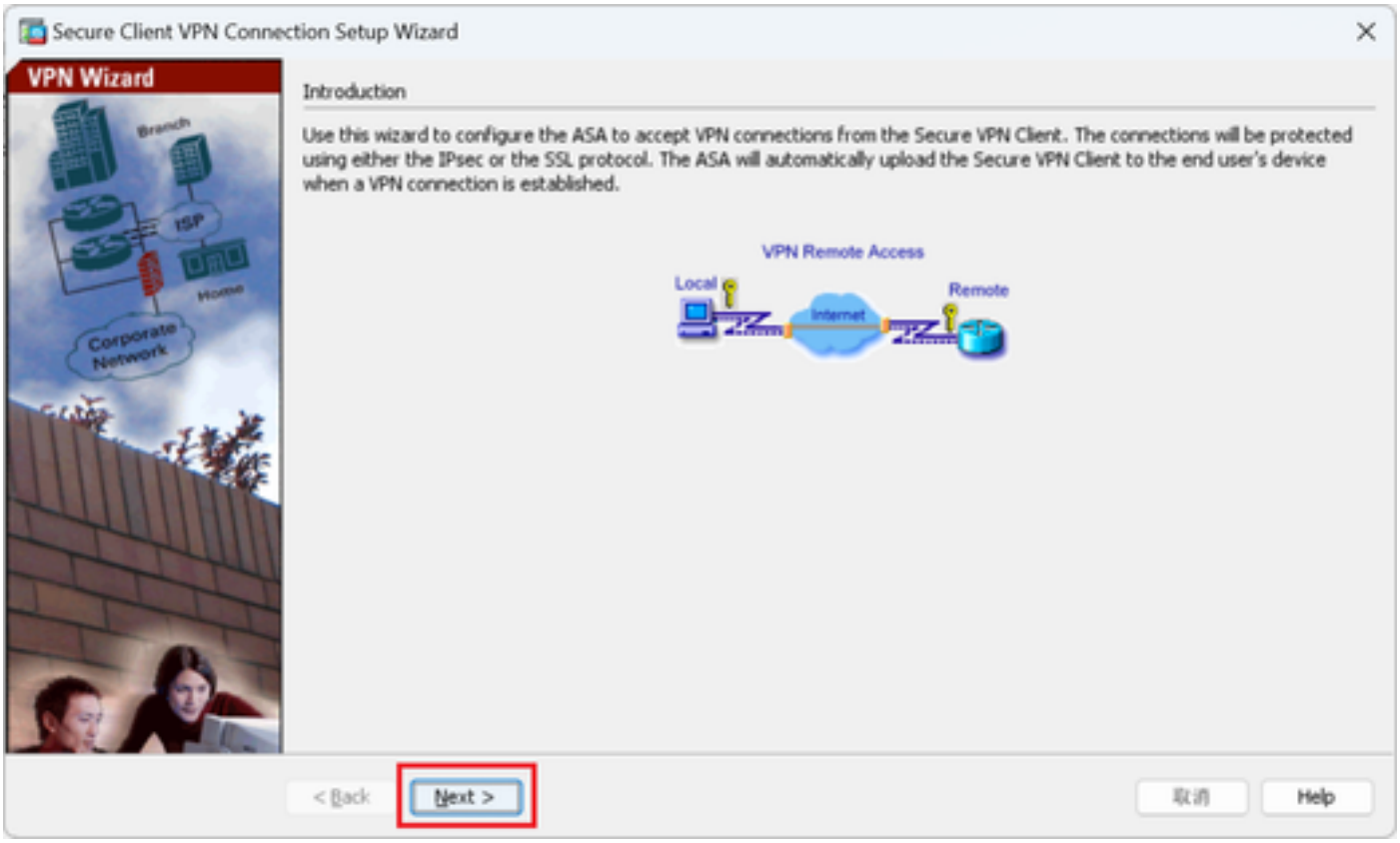
التكوين في ASDM

الخطوة 1. فتح معالجات VPN

انتقل إلى المعالجات > معالجات VPN، انقر فوق معالج شبكة VPN الخاصة بالعميل الآمن.



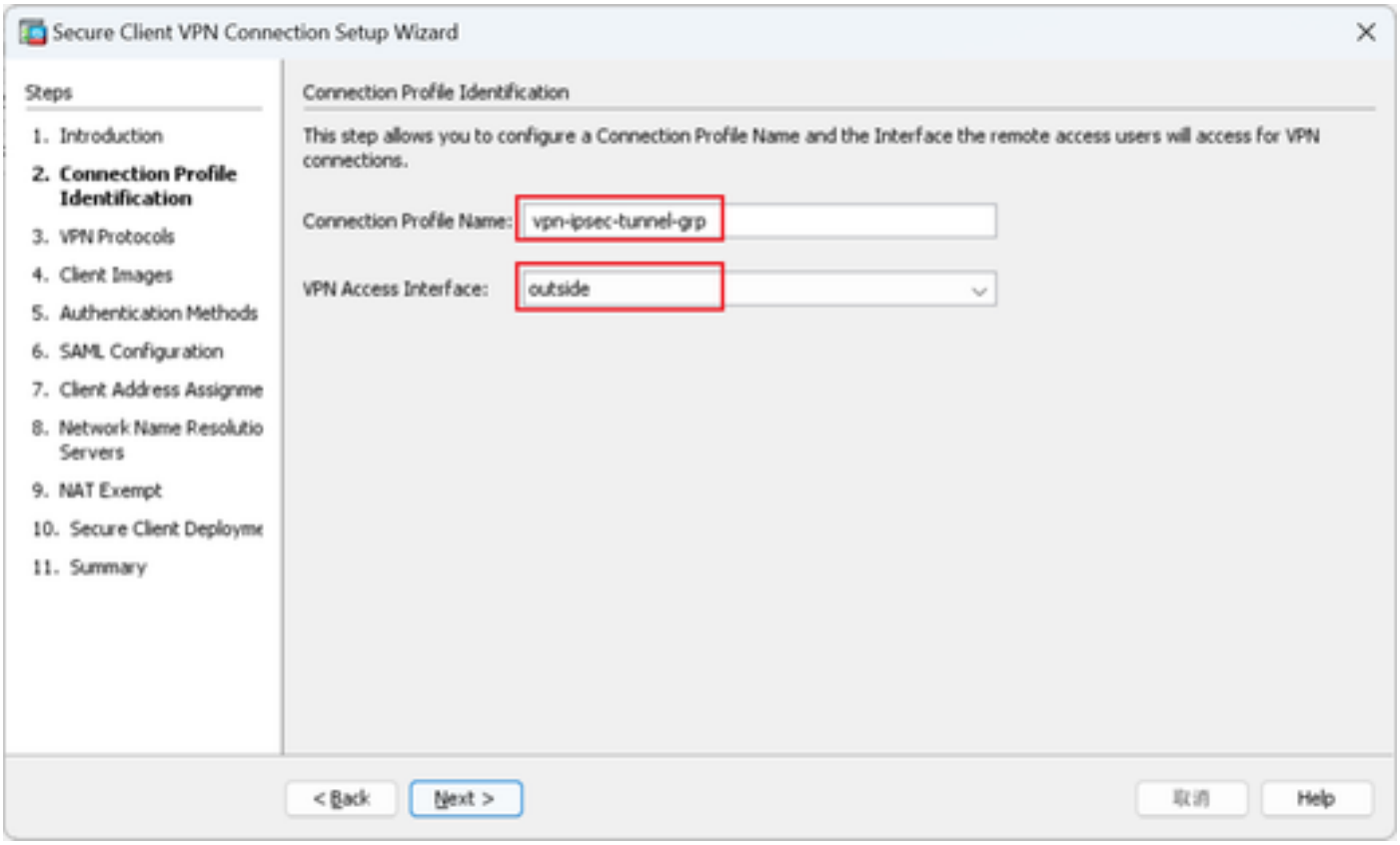
انقر فوق Next (التالي).



انقر فوق الزر التالي

الخطوة 2. تعريف ملف تعريف الاتصال

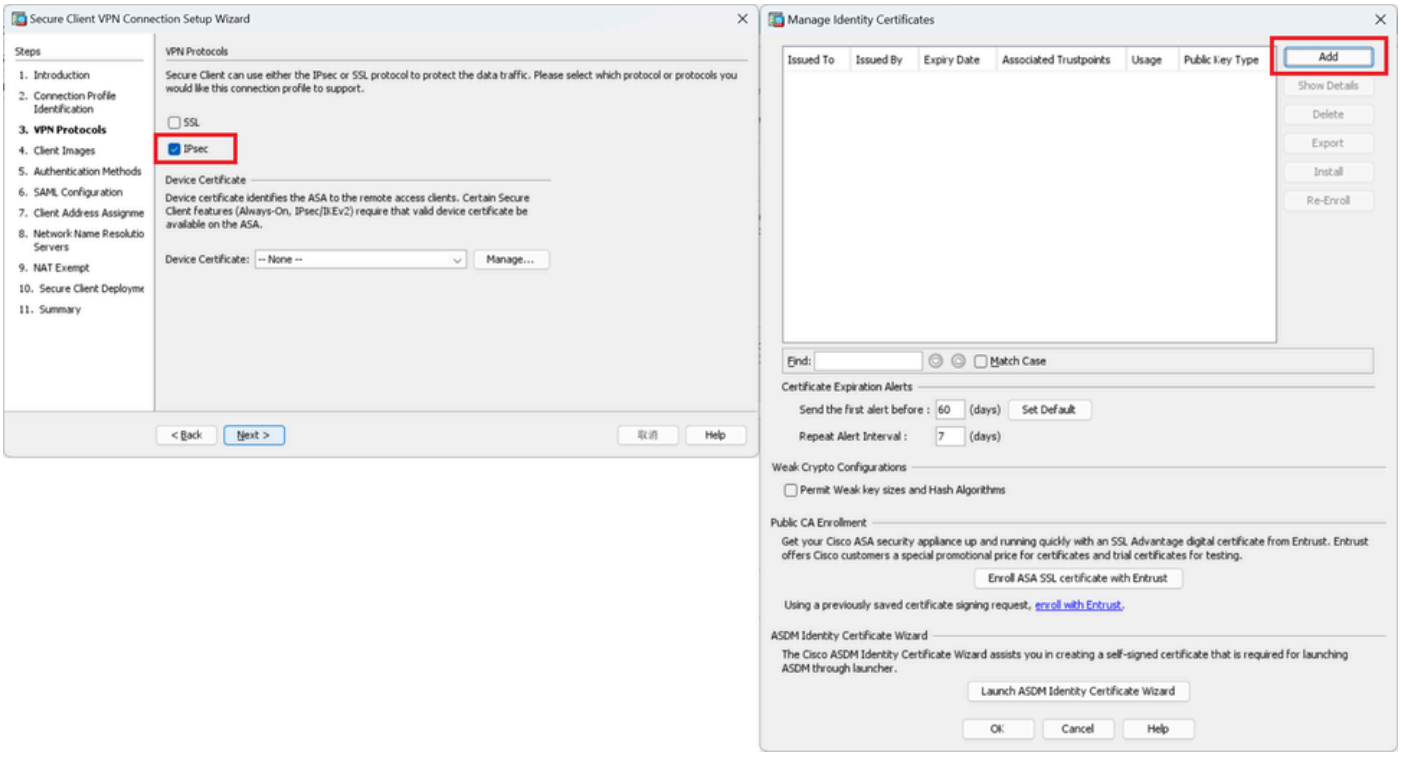
معلومات الإدخال لملف تعريف الاتصال.
اسم ملف تعريف الاتصال: vpn-ips-tunnel-grp
واجهة الوصول إلى VPN : خارج



تعريف ملف تعريف الاتصال

الخطوة 3. بروتوكولات VPN

حدد IPsec، انقر فوق زر إضافة لإضافة شهادة موقعة ذاتيا جديدة.

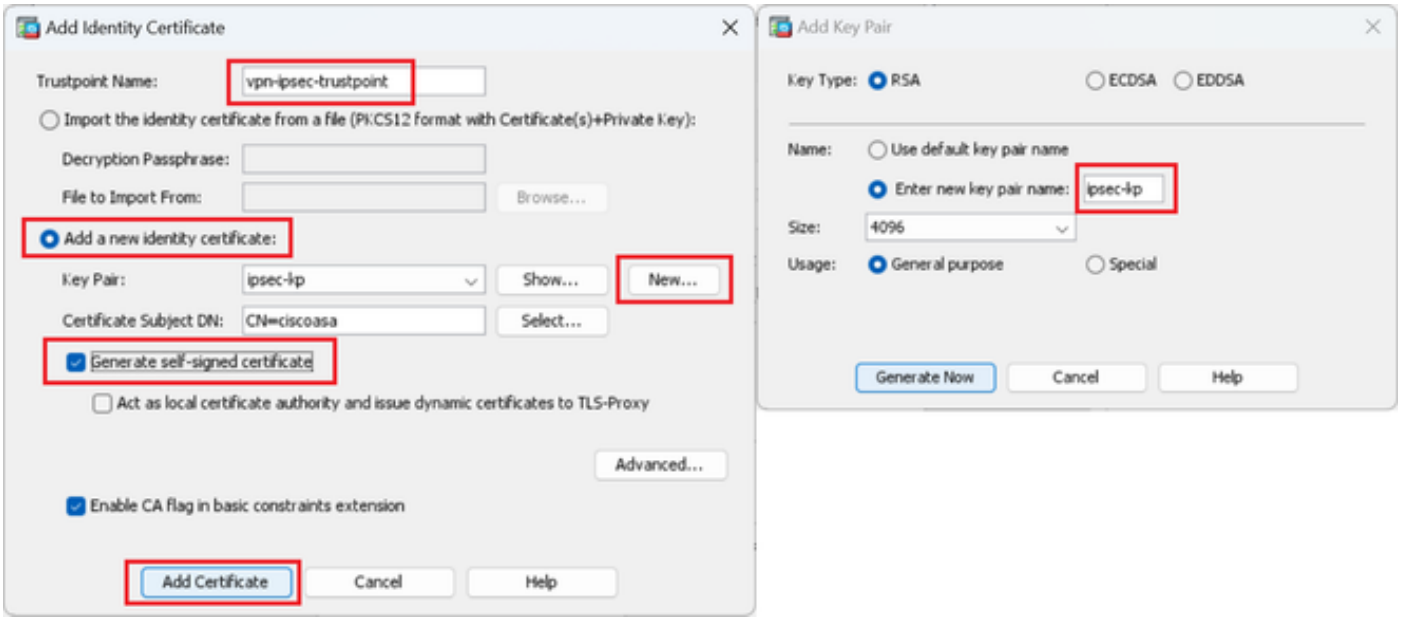


بروتوكولات VPN

إدخال معلومات للشهادة الموقعة ذاتيا.

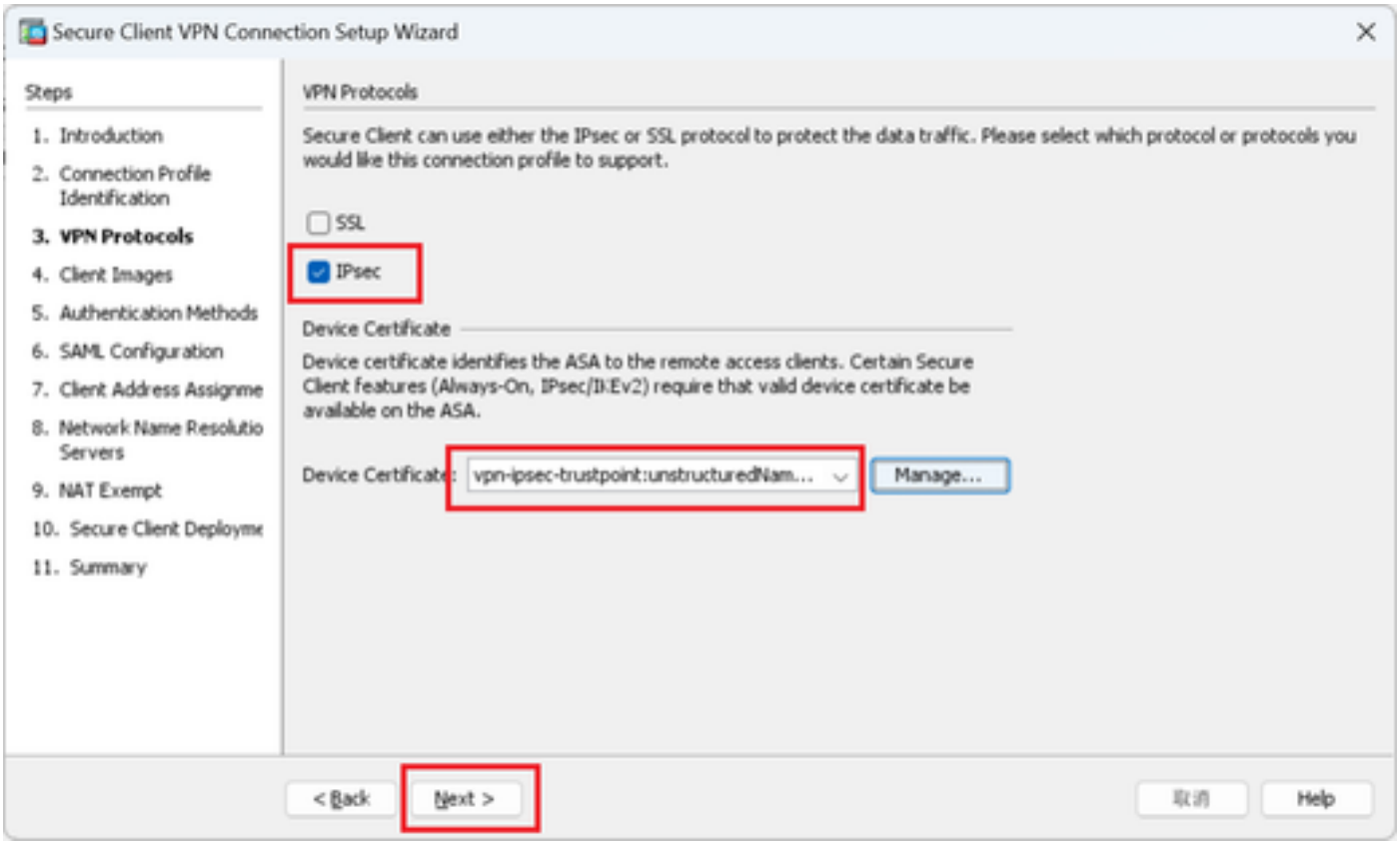
اسم TrustPoint: vpn-ipsEc-TrustPoint

زوج المفاتيح : IPSec-KP



تفاصيل الشهادة الموقعة ذاتيا

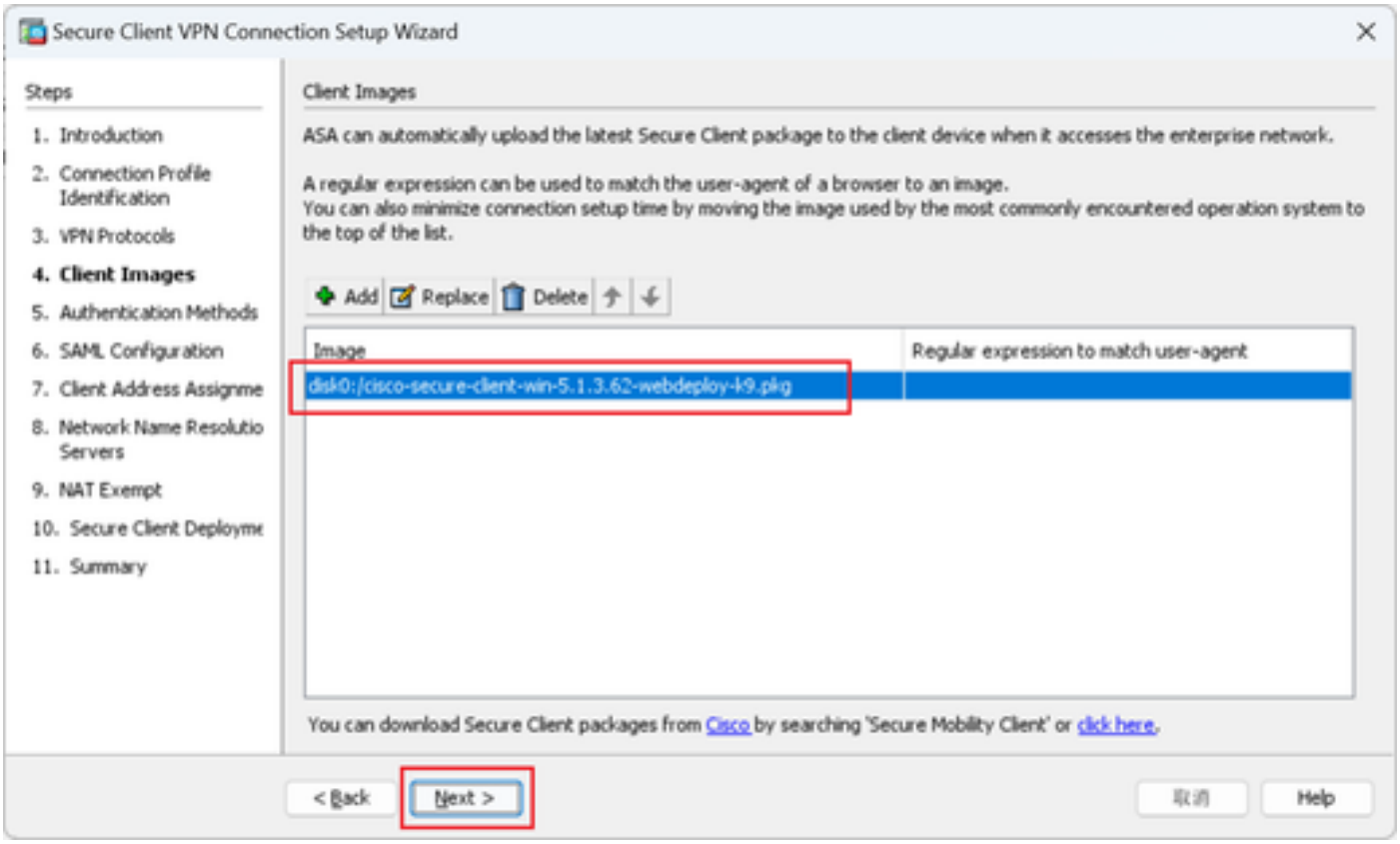
أكدت العملية إعداد بروتوكولات VPN، طقطقت بعد ذلك زر.



تأكيد إعدادات بروتوكول VPN

الخطوة 4. صور العميل

انقر فوق إضافة زر لإضافة صورة عميل آمنة، انقر فوق الزر التالي.



صور العميل

الخطوة 5. أساليب المصادقة

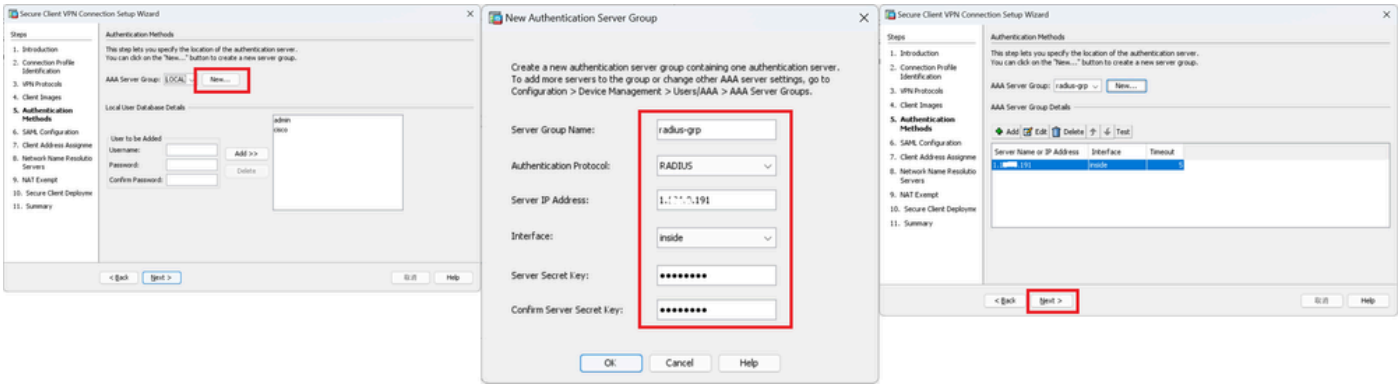
انقر فوق زر جديد لإضافة خادم AAA جديد، انقر فوق الزر التالي.

اسم مجموعة الخوادم : RADIUS-GRP

بروتوكول المصادقة: RADIUS

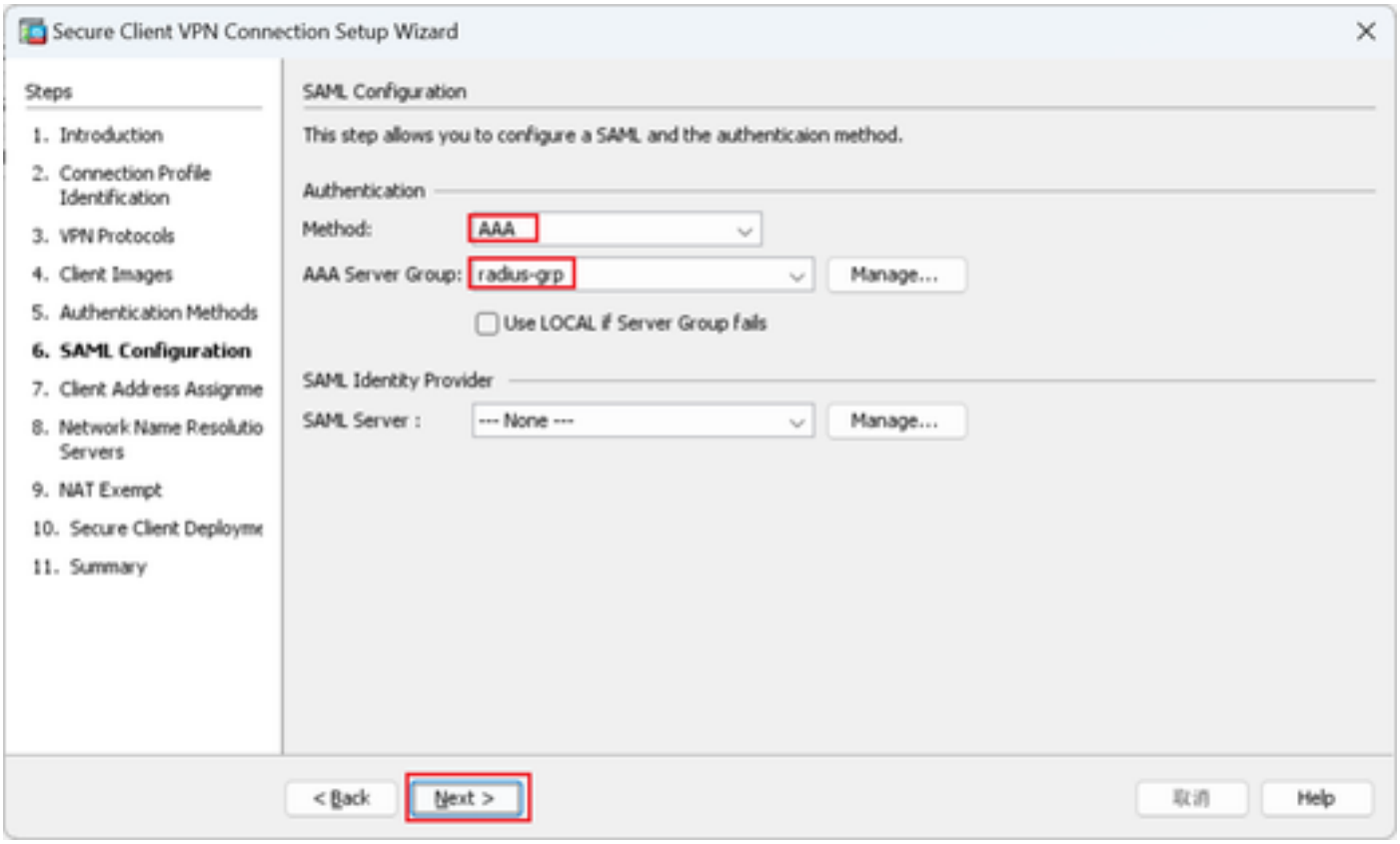
عنوان IP للخادم: 1.x.x.191

الواجهة : الداخل



الخطوة 6. تكوين SAML

طقطقت بعد ذلك زر.



تكوين SAML

الخطوة 7. تعيين عنوان العميل

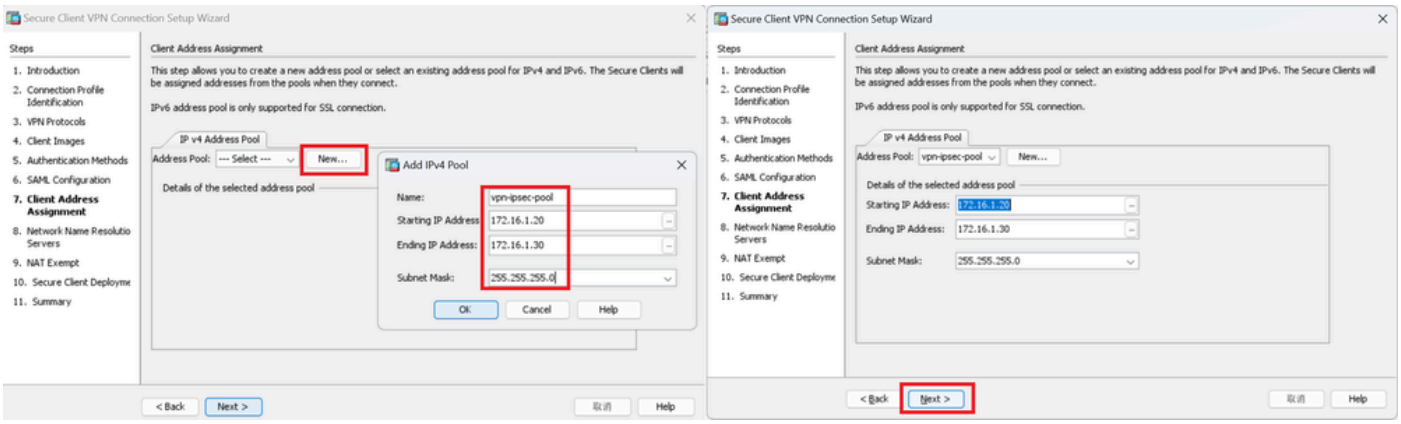
انقر فوق زر جديد لإضافة تجمع IPv4 جديد، انقر فوق الزر التالي.

الاسم: VPN-IPSec-pool

عنوان IP الأولي: 172.16.1.20

نهاية عنوان IP: 172.16.1.30

قناع الشبكة الفرعية: 255.255.255.0



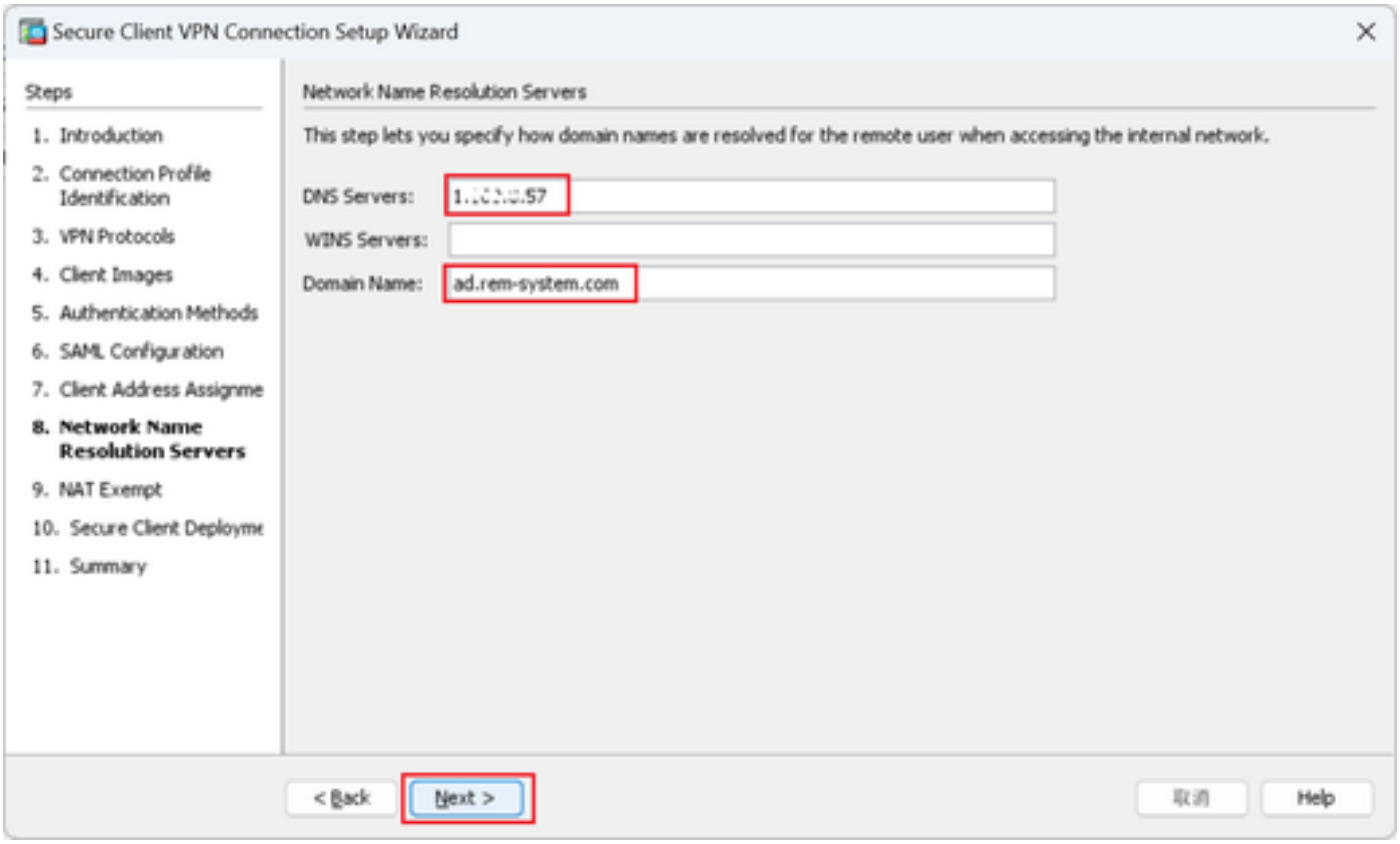
تعيين عنوان العميل

الخطوة 8. خوادم تحليل أسماء الشبكات

إدخال معلومات ل DNS والمجال، انقر فوق الزر التالي.

خوادم DNS: 1.x.x.57

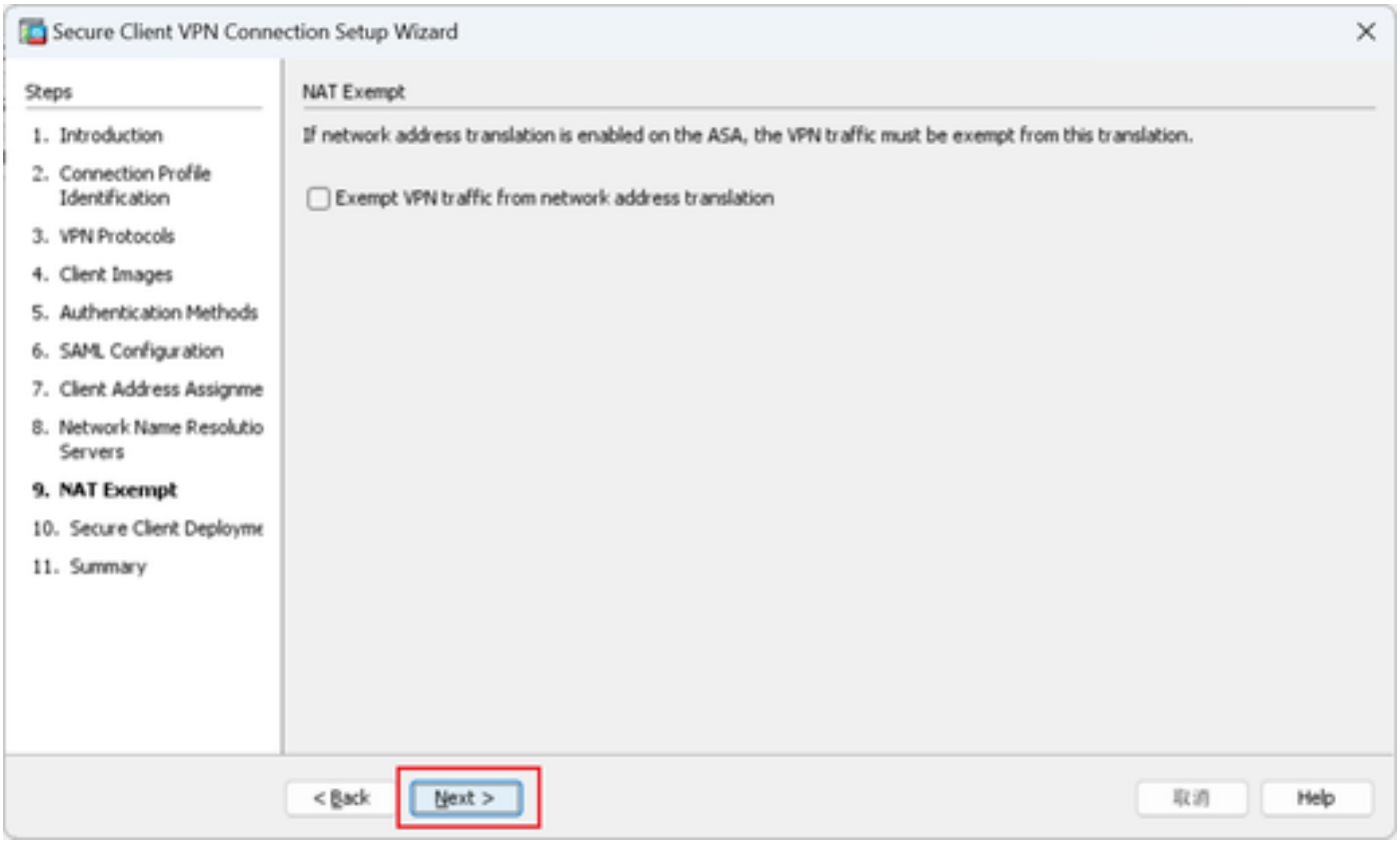
اسم المجال: ad.rem-system.com



خوادم تحليل أسماء الشبكات

الخطوة 9. إعفاء NAT

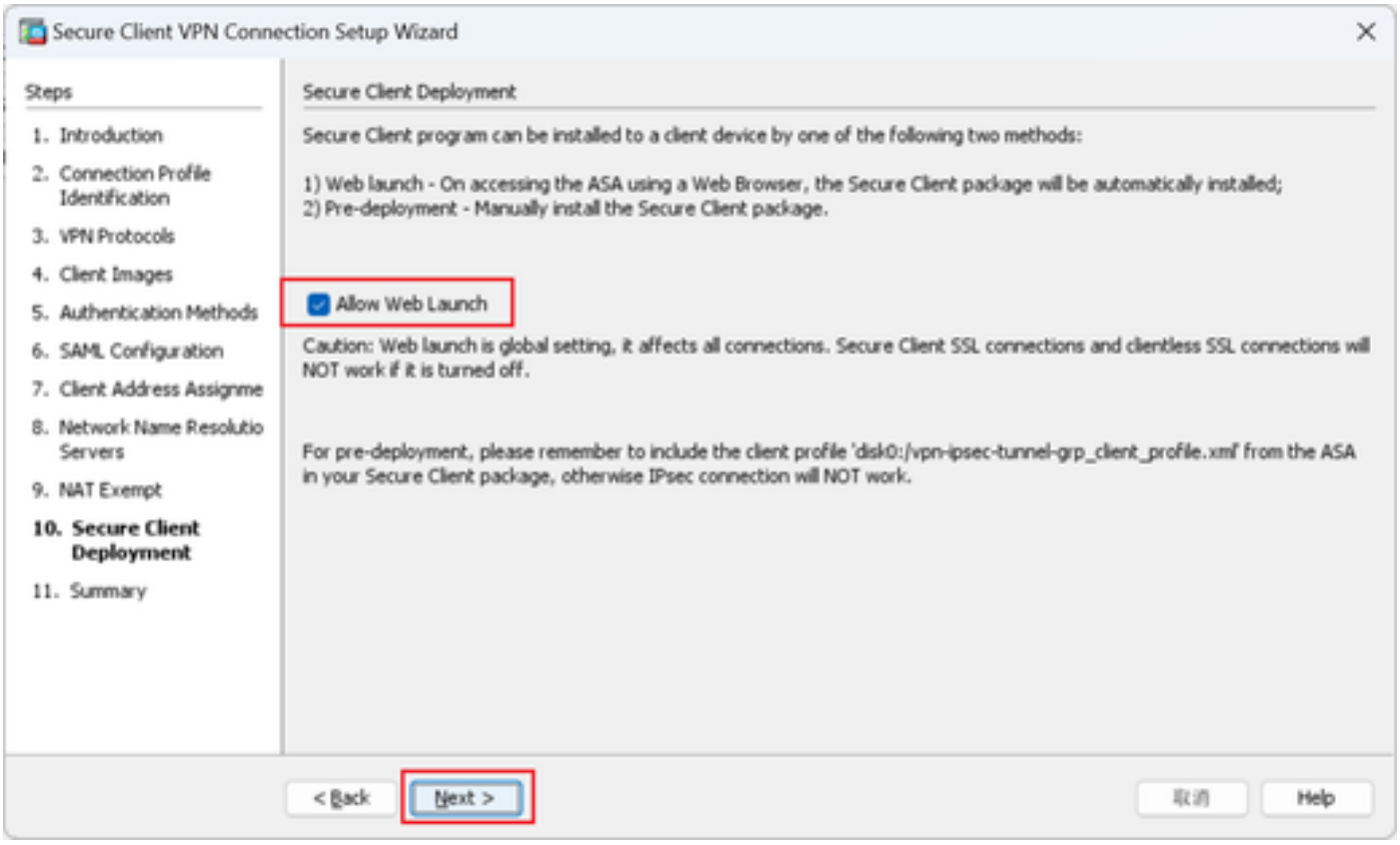
طقطقت بعد ذلك زر.



إعفاء NAT

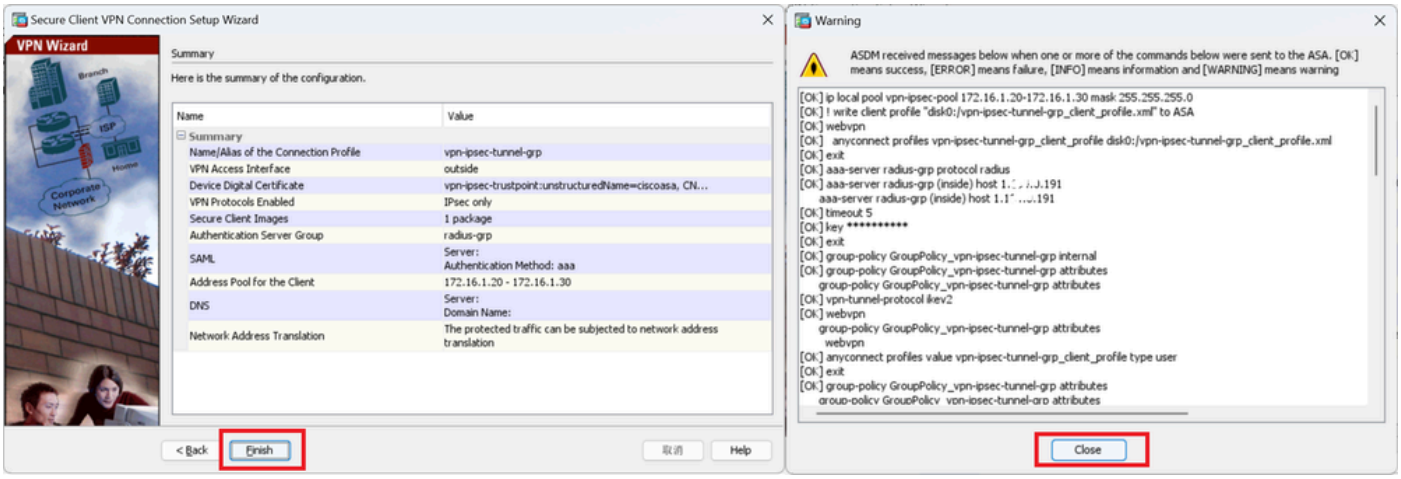
الخطوة 10. نشر آمن للعملاء

حدد السماح بتشغيل الويب، انقر فوق الزر التالي.



الخطوة 11. حفظ الإعدادات

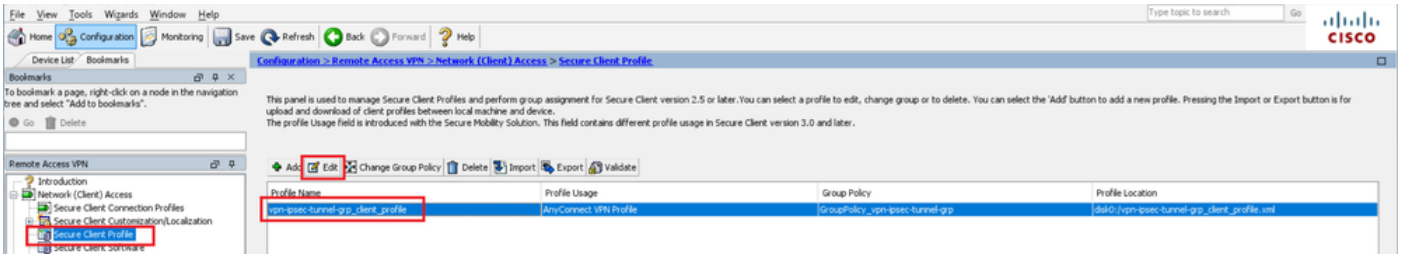
طقطقت إنجاز زر وحفظ العملية إعداد.



حفظ الإعدادات

الخطوة 12. تأكيد ملف تعريف العميل الآمن وتصديره

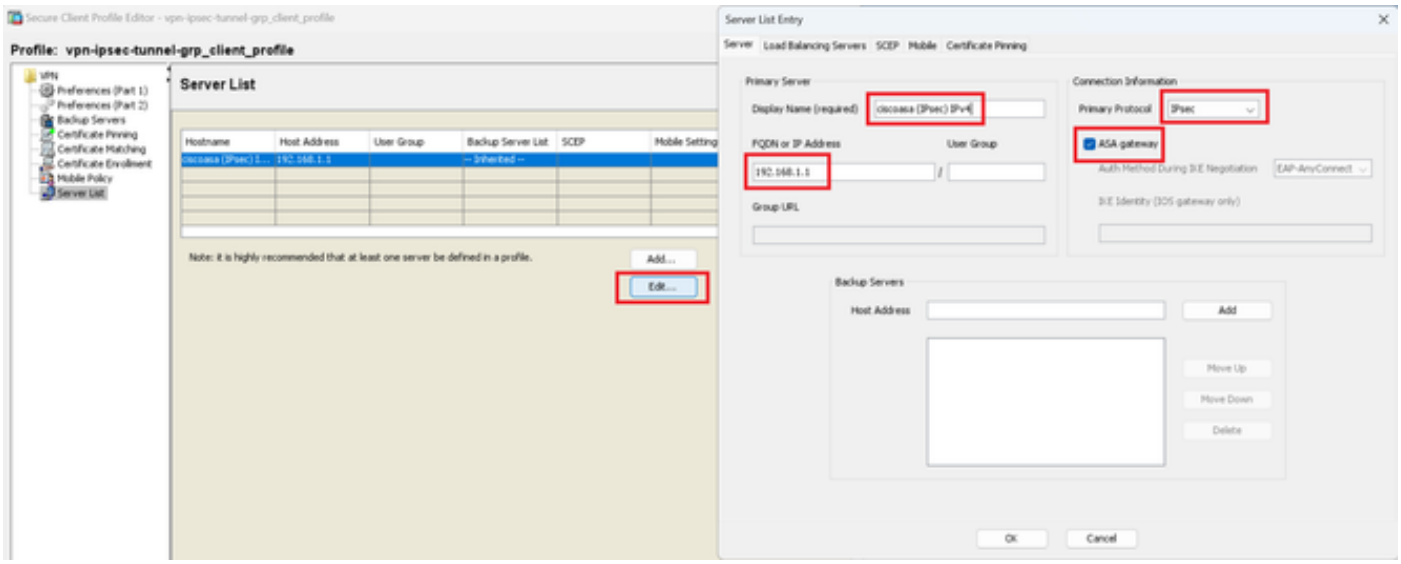
انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > Network (Client) Access (الوصول إلى الشبكة) > Secure Client Profile، انقر فوق زر تحرير .



تحرير ملف تعريف عميل آمن

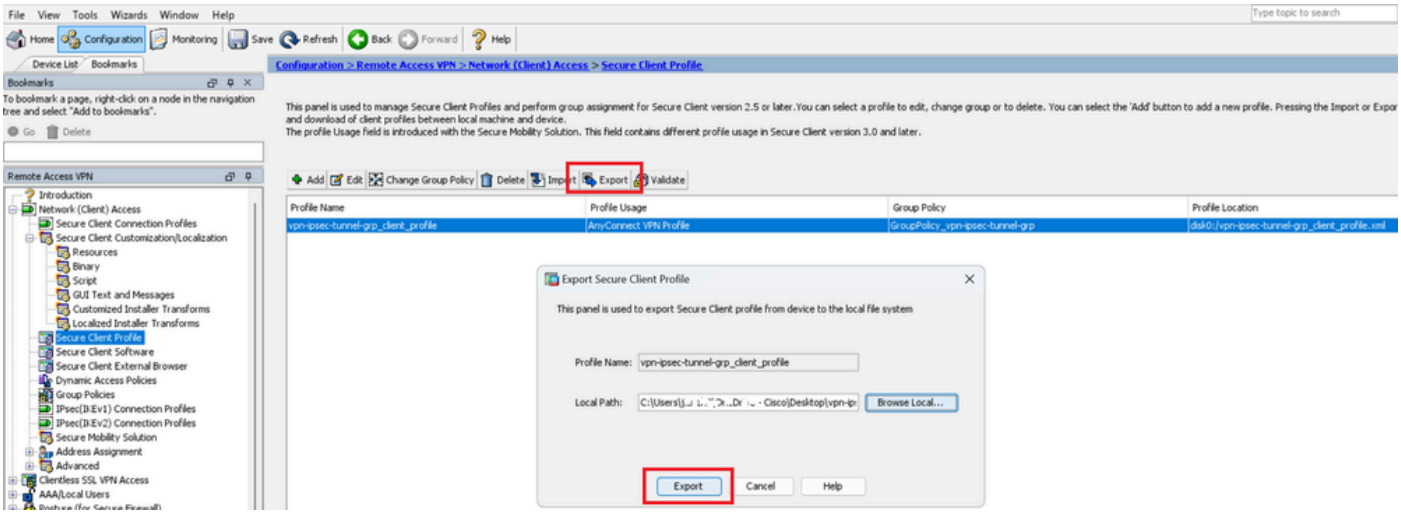
تأكيد تفاصيل ملف التعريف.

- اسم العرض (مطلوب) : CiscoASA (IPsec) IPv4
- FQDN أو عنوان IP: 192.168.1.1
- البروتوكول الأساسي: IPsec



تأكيد ملف تعريف العميل الآمن

انقر على زر تصدير لتصدير التوصيف إلى الكمبيوتر المحلي.



تصدير ملف تعريف العميل الآمن

الخطوة 13. تأكيد تفاصيل ملف تعريف العميل الآمن

افتح "ملف تعريف العميل الآمن" بواسطة المستعرض، وتأكد من أن البروتوكول الأساسي للمضيف هو IPsec.

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
  <ServerList>
    <HostEntry>
      <HostName>ciscoasa (IPsec) IPv4</HostName>
      <HostAddress>192.168.1.1</HostAddress>
      <PrimaryProtocol>IPsec</PrimaryProtocol>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

الخطوة 14. تأكيد الإعدادات في ASA CLI

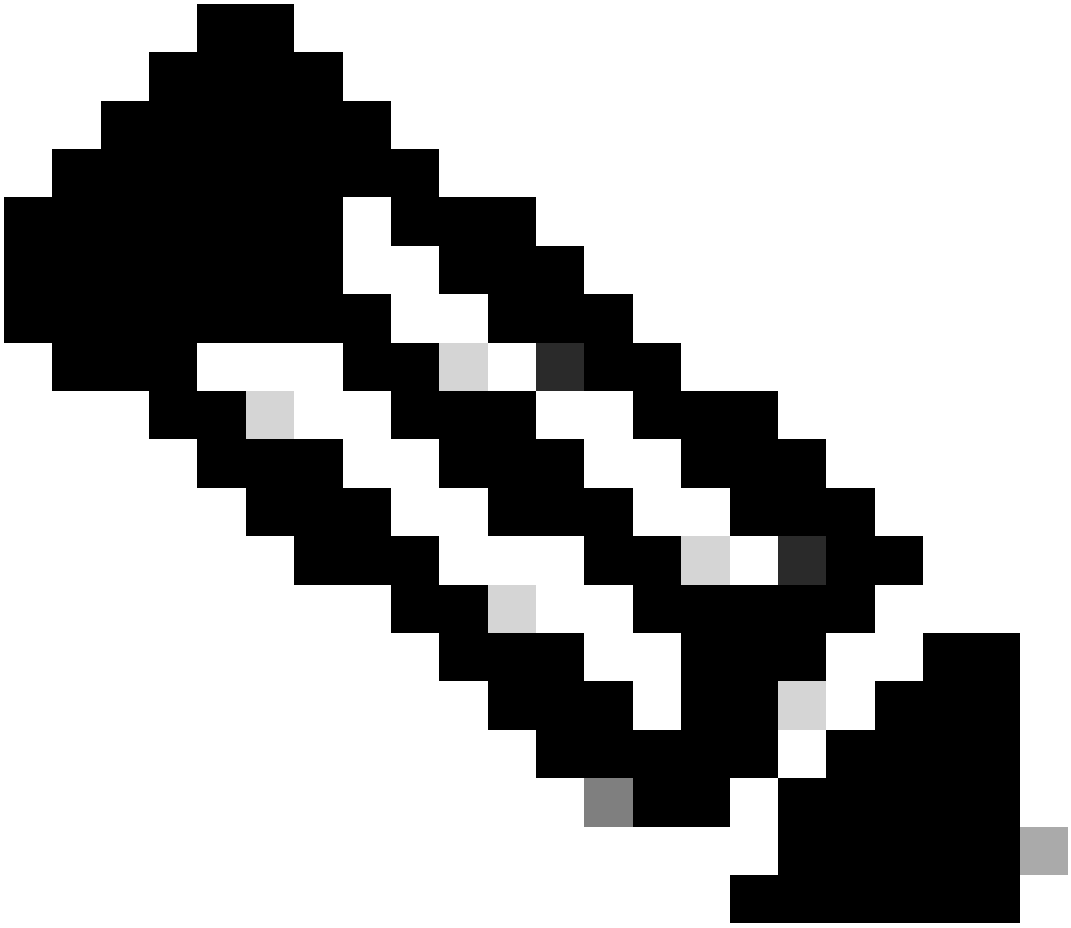
تأكيد إعدادات IPsec التي تم إنشاؤها بواسطة ASDM في واجهة سطر الأوامر (CLI) لـ ASA.

```
// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0

// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5

// Define the transform sets that IKEv2 can use
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1

// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
crl configure

// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b
......
ac76f984 efd41d13 073d0be6 f923a9c6 7b
quit

// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10
```

```
encryption aes-192
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 40
encryption aes
integrity sha256
group 5
prf sha256
lifetime seconds 86400

// Enabling client-services on the outside interface
crypto ikev2 enable outside client-services port 443

// Specifiies the certificate the ASA uses for IKEv2
crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint

// Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
enable
anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1
anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
anyconnect enable
tunnel-group-list enable

// Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile
group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
wins-server none
dns-server value 1.x.x.57
vpn-tunnel-protocol ikev2
default-domain value ad.rem-system.com
webvpn
anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user

// Ties the pool of addressess to the vpn connection
tunnel-group vpn-ipsec-tunnel-grp type remote-access
tunnel-group vpn-ipsec-tunnel-grp general-attributes
address-pool vpn-ipsec-pool
authentication-server-group radius-grp
default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp
tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes
group-alias vpn-ipsec-tunnel-grp enable
```

الخطوة 15. إضافة خوارزمية تشفير

في واجهة سطر أوامر ASA، أضف المجموعة 19 إلى نهج IKEv2.

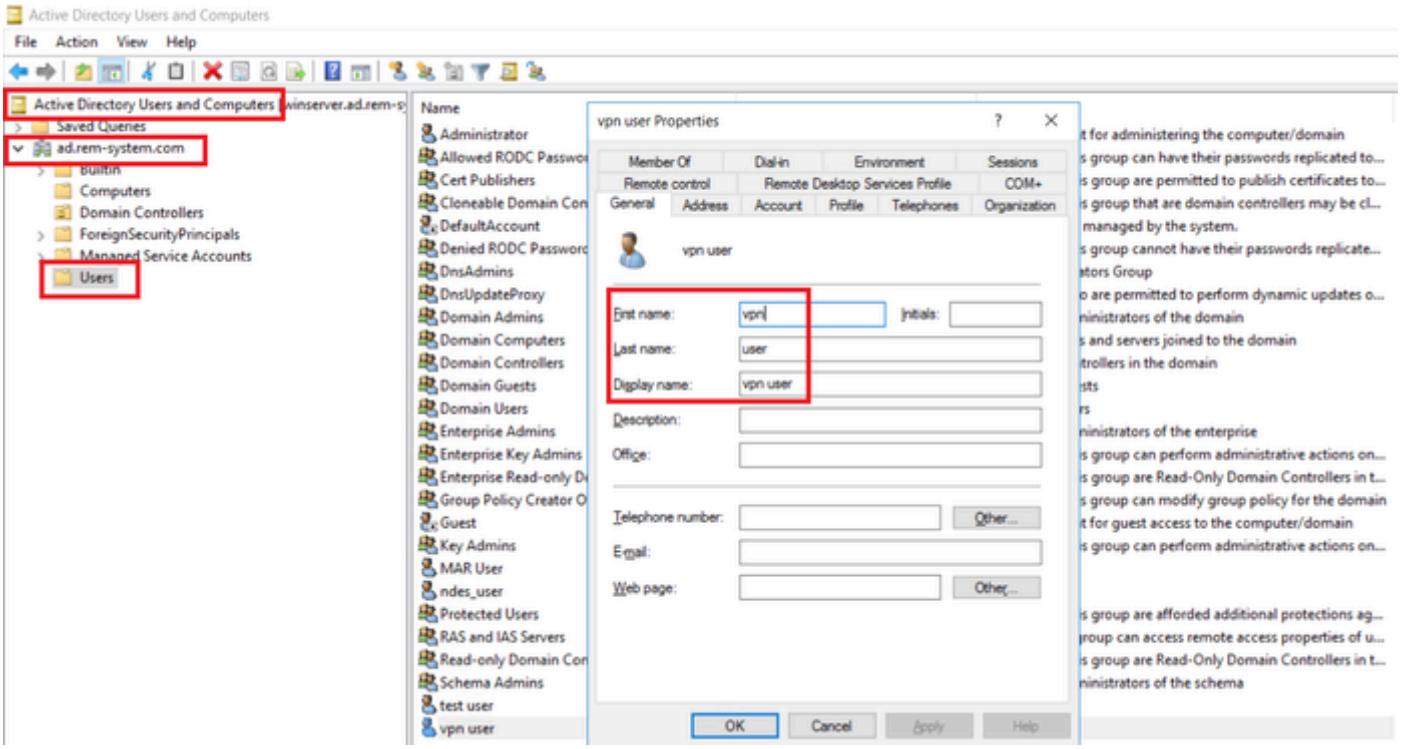


ملاحظة: بالنسبة لاتصالات IKEv2/IPsec، لم تعد Cisco Secure Client تدعم مجموعات Diffie-Hellman (DH) أرقام 2 و 5 و 14 و 24 وفقا للإصدار 4.9.00086. قد يؤدي هذا التغيير إلى حدوث حالات فشل في الاتصال بسبب عدم تطابق خوارزمية التشفير.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#
```

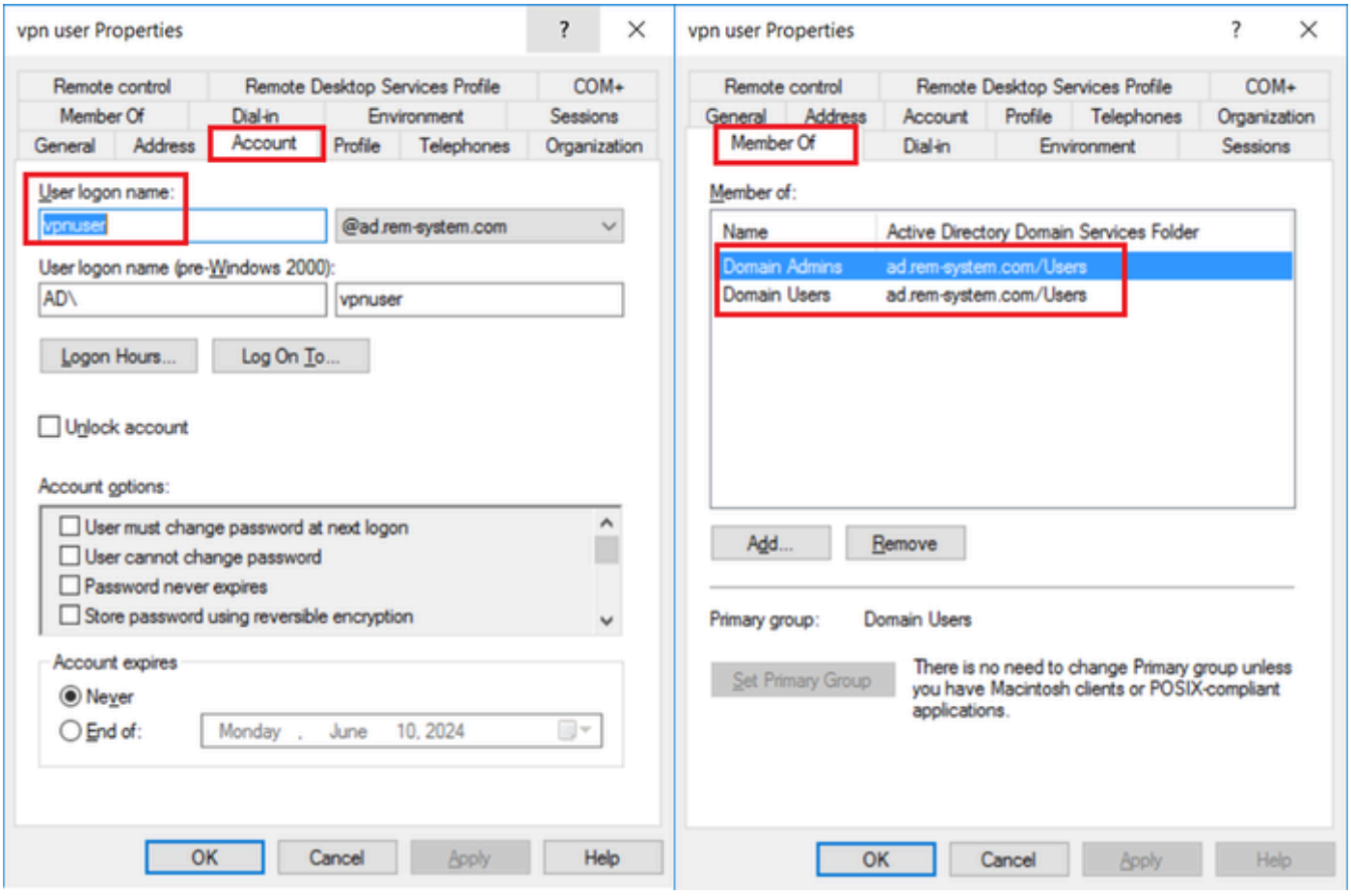
التكوين في خادم Windows

أنت تحتاج أن يضيف مجال مستعمل لاتصال VPN. انتقل إلى Active Directory Users and Computers، انقر فوق Users. إضافة vpnUser كمستخدم مجال.



إضافة مستخدم مجال

إضافة مستخدم المجال إلى عضو مسؤولي المجال ومستخدمي المجال.

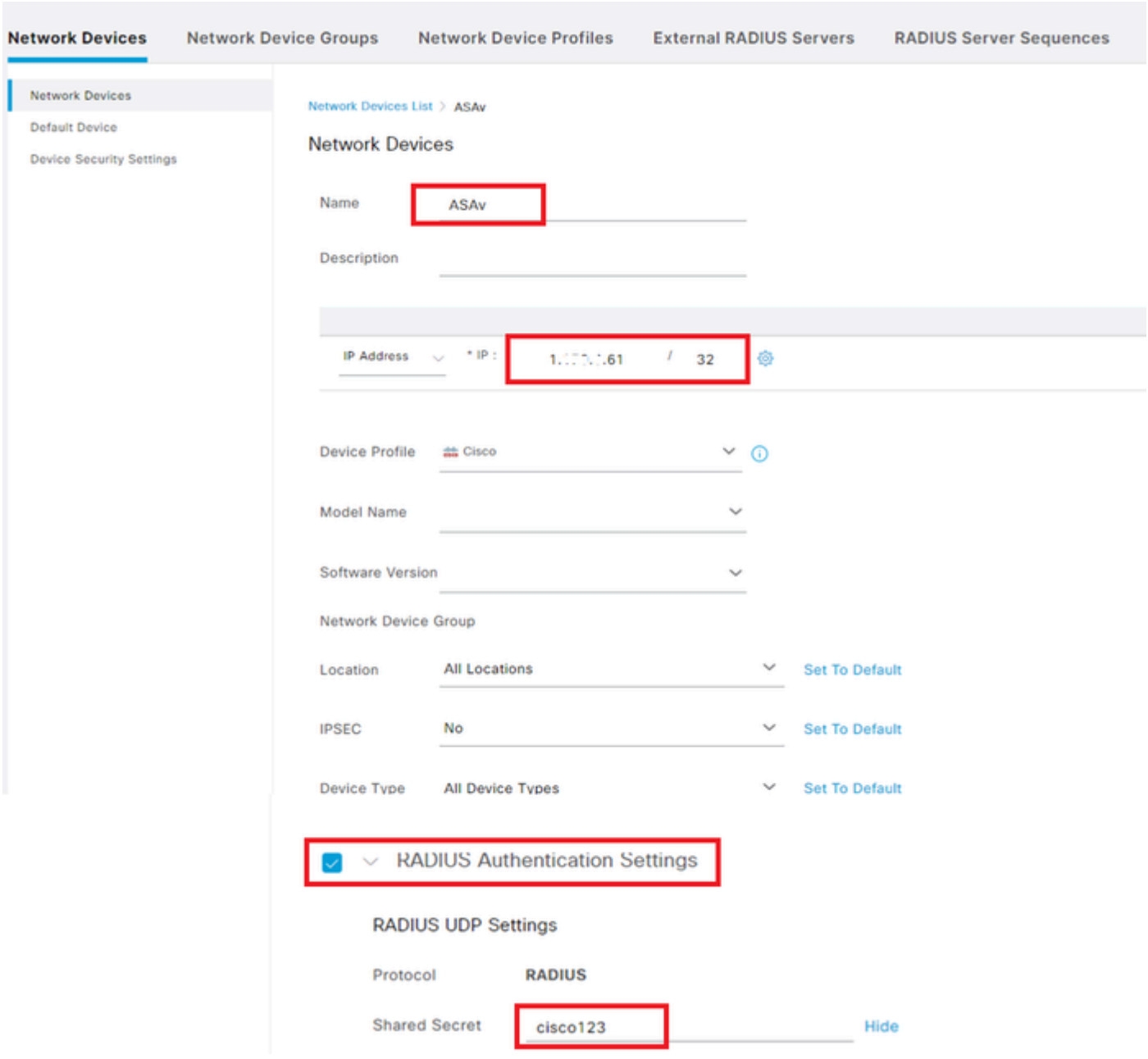


مسؤول المجال ومستخدم المجال

التكوين في ISE

الخطوة 1. إضافة جهاز

انتقل إلى Administration > أجهزة الشبكة، انقر فوق AddButton لإضافة جهاز ASAv.

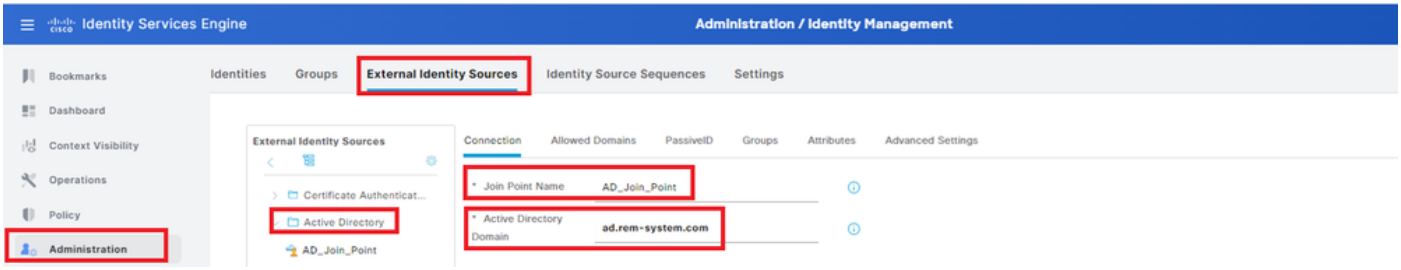


إضافة جهاز

الخطوة 2. إضافة Active Directory

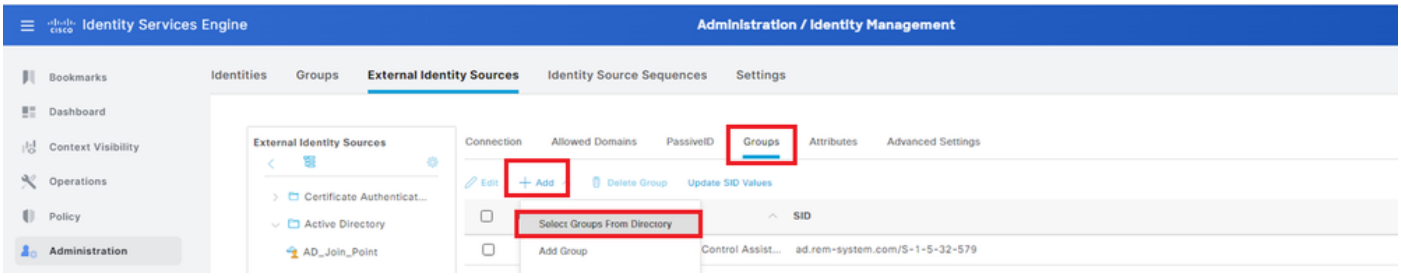
انتقل إلى Administration > مصادر الهوية الخارجية > Active Directory، انقر فوق ConnectTab، وقم بإضافة Active Directory إلى ISE.

- اسم نقطة الربط: AD_JOIN_POINT
- مجال Active Directory: ad.rem-system.com



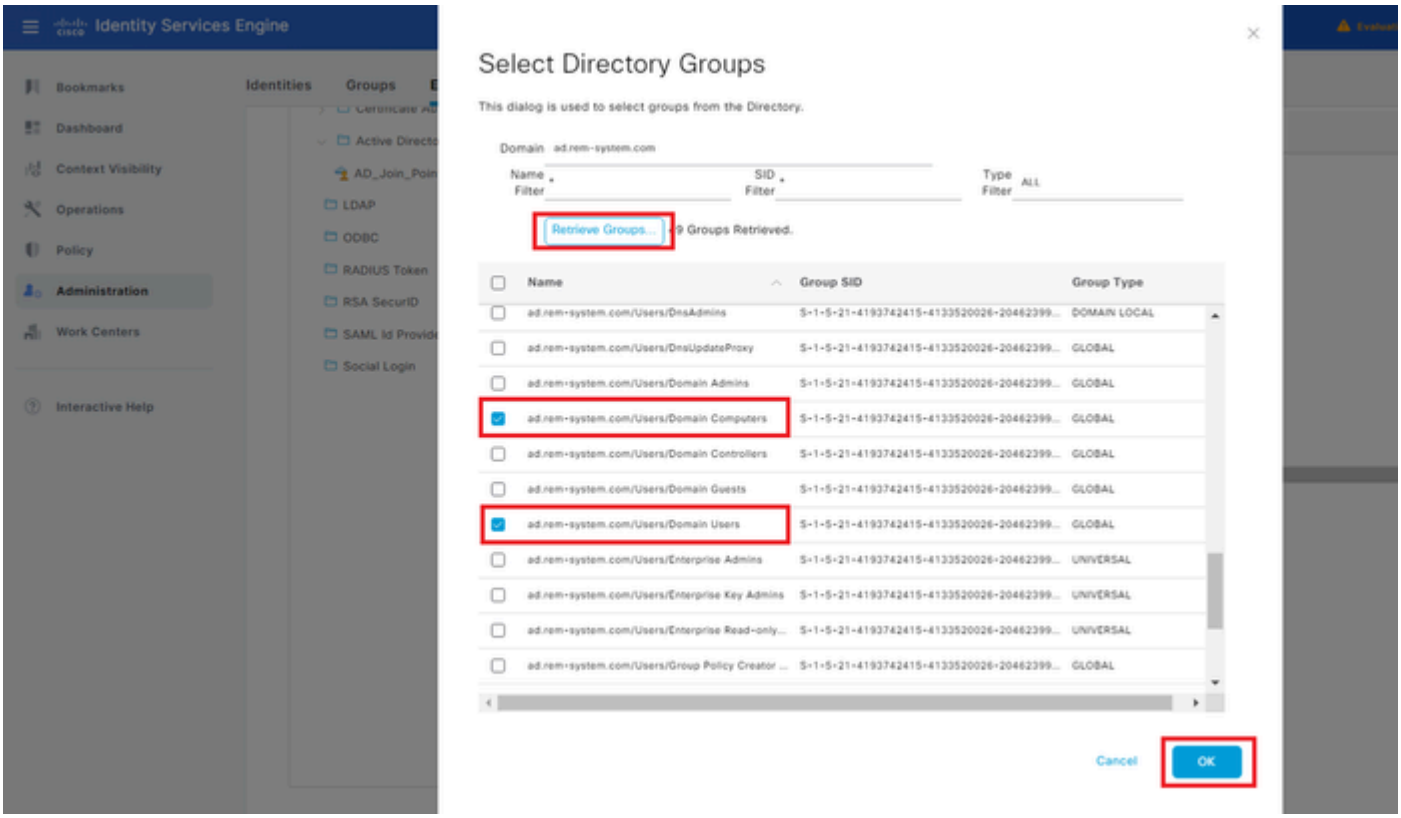
إضافة Active Directory

انتقل إلى علامة التبويب مجموعات، حدد مجموعات من القائمة المنسدلة Directoryمن القائمة المنسدلة.



حدد مجموعات من الدليل

انقر فوق إستردادالمجموعات من القائمة المنسدلة. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain UserAnd clickOK.

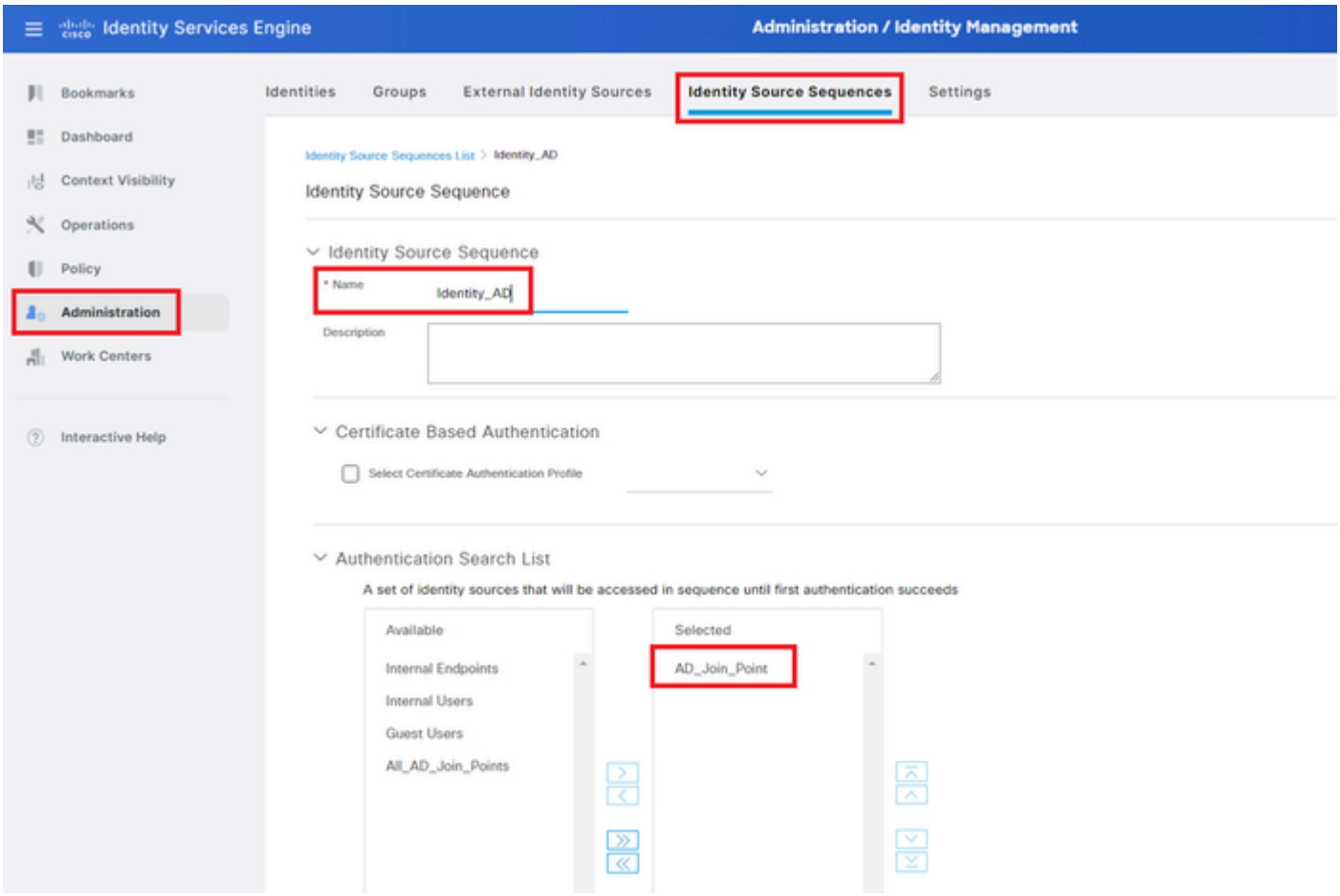


إضافة أجهزة كمبيوتر المجال والمستخدمين

الخطوة 3. إضافة سلسلة مصدر الهوية

انتقل إلى إدارة > تسلسلات مصدر الهوية، وقم بإضافة تسلسل مصدر هوية.

- الاسم: Identity_AD
- قائمة البحث عن المصادقة: AD_JOIN_POINT

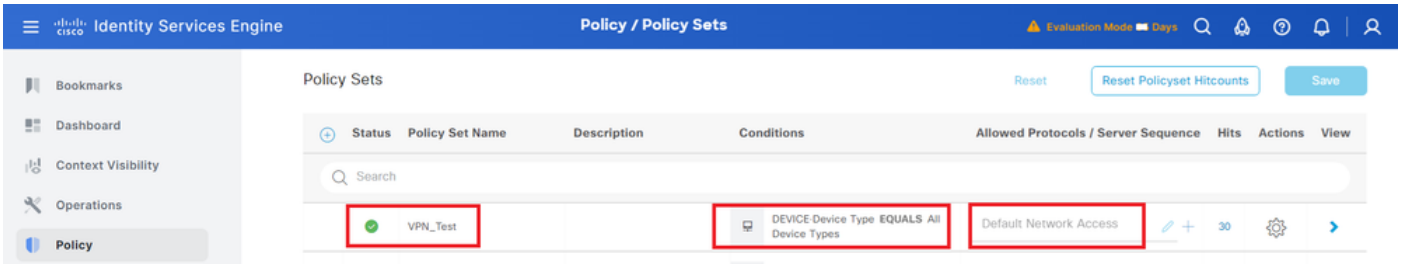


إضافة تسلسلات مصدر الهوية

الخطوة 4. إضافة مجموعة نهج

انتقل إلى نهج > مجموعات نهج، انقر فوق + لإضافة مجموعة نهج.

- اسم مجموعة النهج: VPN_TEST
- الشروط: نوع الجهاز يساوي جميع أنواع الأجهزة
- البروتوكولات المسموح بها / تسلسل الخادم: الوصول الافتراضي إلى الشبكة

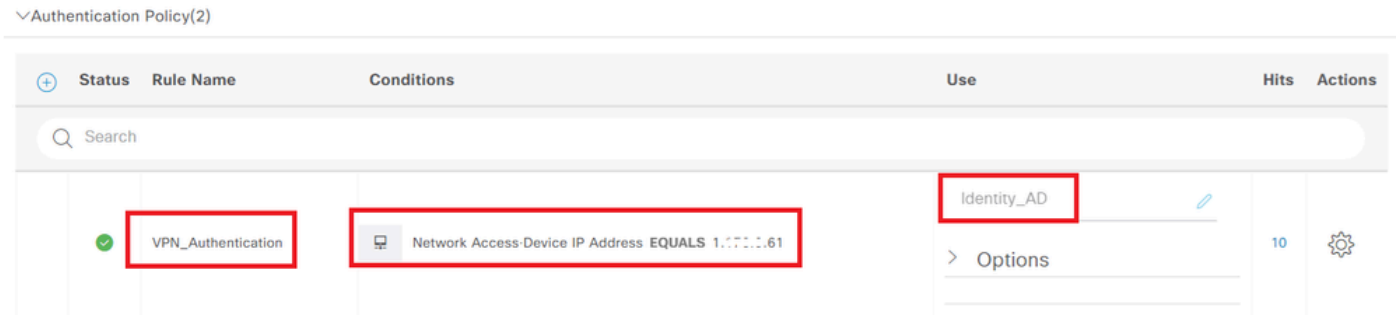


إضافة مجموعة نهج

الخطوة 5. إضافة نهج المصادقة

انتقل إلى مجموعات النهج، انقر فوق VPN_TEST لإضافة نهج مصادقة.

- اسم القاعدة: VPN_AUTHENTICATION
- الشروط: عنوان IP لجهاز الوصول إلى الشبكة يساوي 1.x.x.61
- الاستخدام: Identity_AD

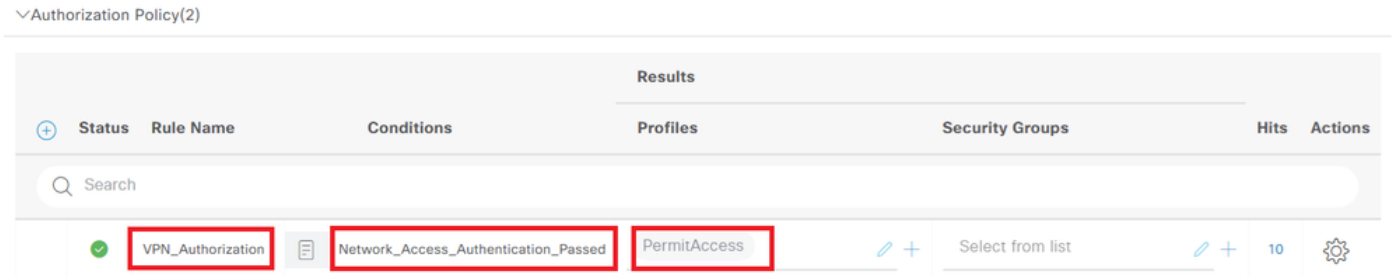


إضافة نهج المصادقة

الخطوة 6. إضافة نهج التخويل

انتقل إلى مجموعات النهج، وانقر فوق VPN_TEST لإضافة نهج تخويل.

- اسم القاعدة: VPN_AUTHORIZATION
- الشروط: Network_ACCESS_AUTHENTICATION_PASS
- النتائج: PermitAccess

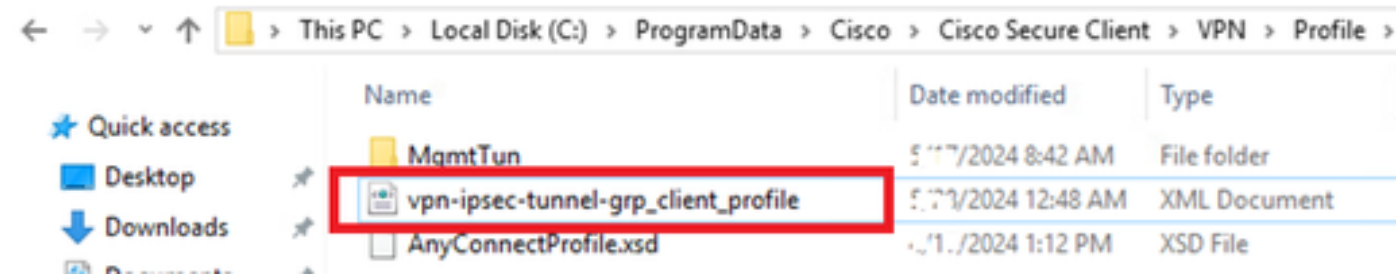


إضافة نهج التخويل

التحقق من الصحة

الخطوة 1. انسخ ملف تعريف العميل الآمن إلى Win10 PC1

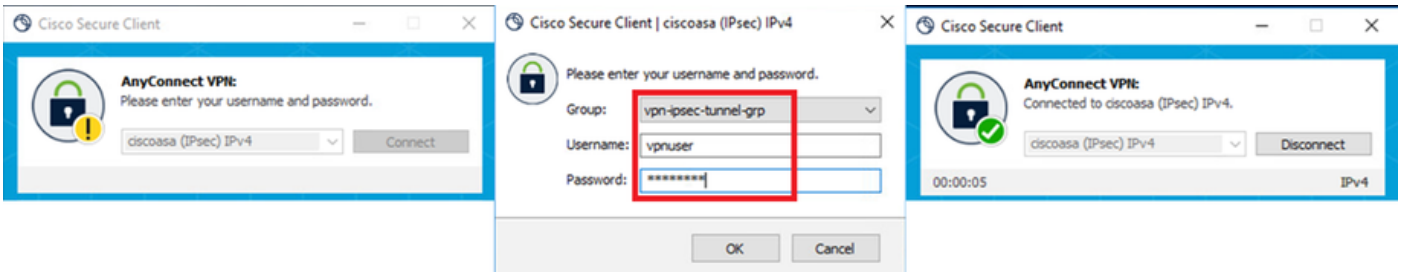
انسخ ملف تعريف العميل الآمن إلى دليل C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



نسخ ملف التعريف إلى الكمبيوتر

الخطوة 2. بدء اتصال VPN

على نقطة النهاية، قم بتشغيل Cisco Secure Client وأدخل اسم المستخدم وكلمة المرور، ثم قم بتأكيد اتصال Cisco Secure Client بنجاح.



نجح الاتصال

الخطوة 3. تأكيد Syslog على ASA

في syslog، تأكد من نجاح اتصال IKEv2.

<#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

New Connection Established

```
May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

الخطوة 4. تأكيد جلسة عمل IPsec على ASA

قم بتشغيل show vpn-sessiondb detail anyconnect الأمر لتأكيد جلسة عمل IKEv2/IPsec على ASA.

<#root>

ciscoasa#

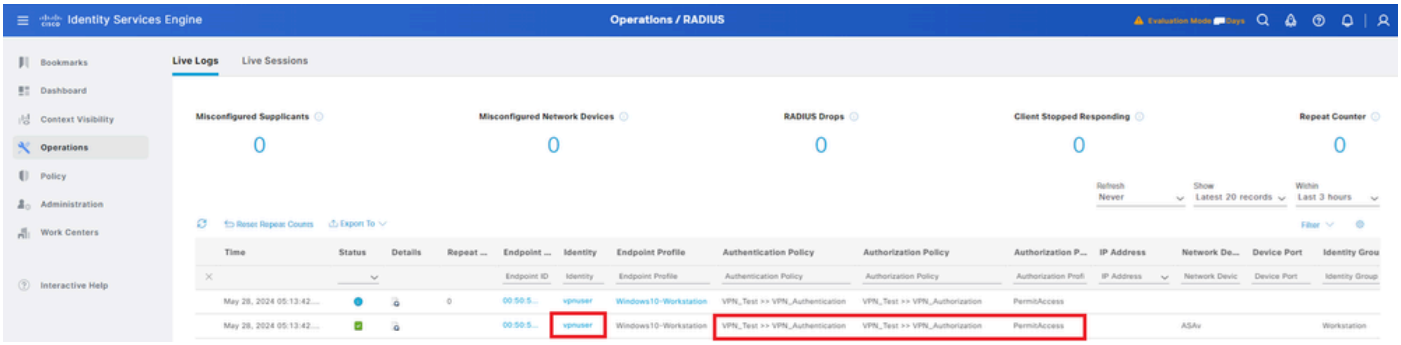
show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed

Username : vpnuser Index : 23
Assigned IP : 172.16.1.20 Public IP : 192.168.1.11
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp
Tunnel Group : vpn-ipsec-tunnel-grp
Login Time : 08:13:20 UTC Tue May 28 2024
Duration : 0h:10m:10s
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 01aa003d0001700066559220
Security Grp : none

IKEv2 Tunnels: 1

IPsecOverNatT Tunnels: 1

AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 23.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : 5.1.3.62

IKEv2:
Tunnel ID : 23.2
UDP Src Port : 50982 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds
PRF : SHA256 D/H Group : 19
Filter Name :
Client OS : Windows Client Type : AnyConnect

IPsecOverNatT:
Tunnel ID : 23.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.1.20/255.255.255.255/0/0
Encryption : AES256 Hashing : SHA256
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
```

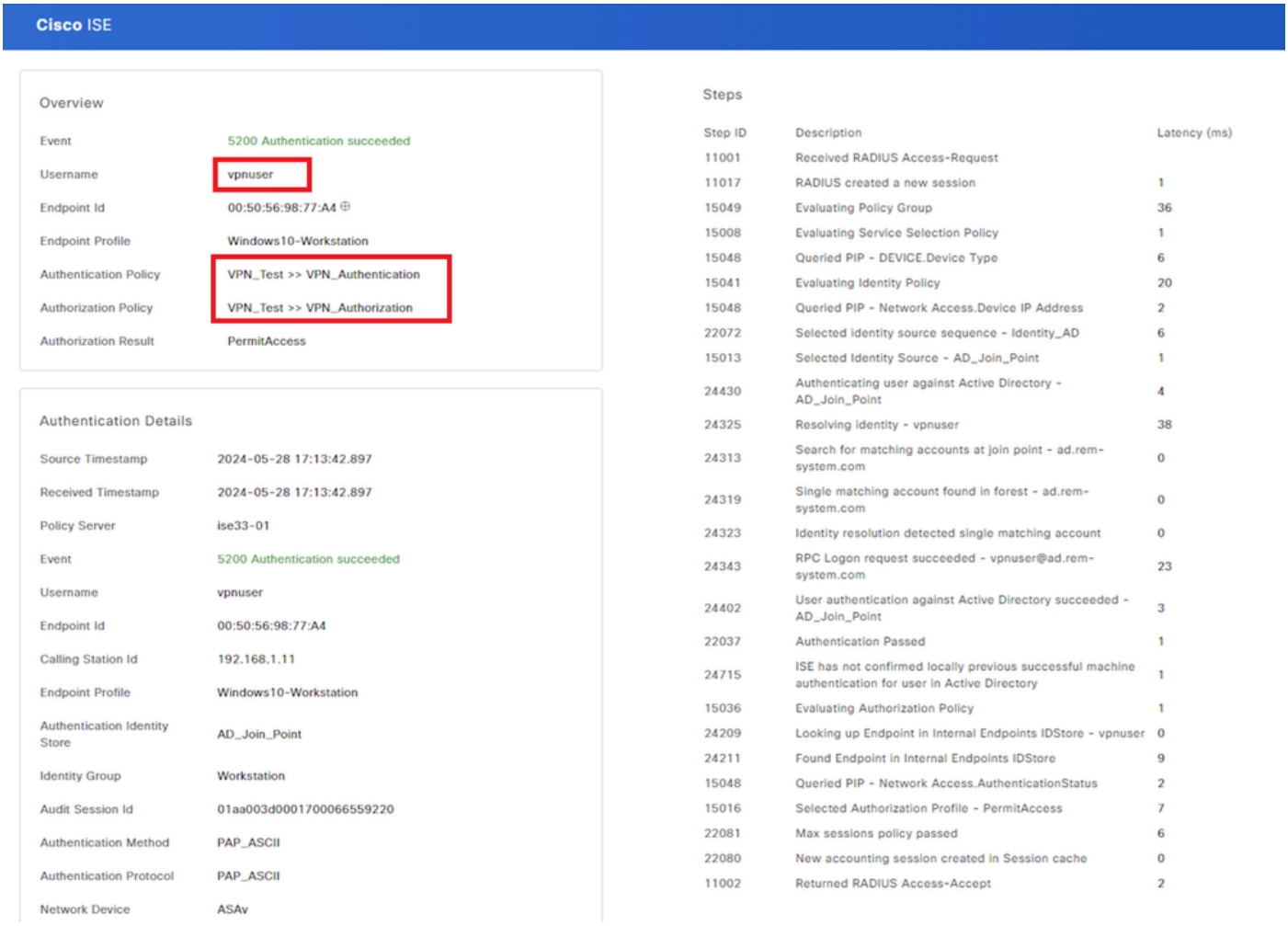
الخطوة 5. تأكد من سجل Radius Live

انتقل إلى العمليات **> RADIUS** > واجهة المستخدم الرسومية (GUI) المباشرة LogISE، أكد سجل التشغيل لمصادقة VPN.



سجل *Radius Live*

انقر فوق "حالة" لتأكيد تفاصيل سجل التشغيل المباشر.



تفاصيل السجل المباشر

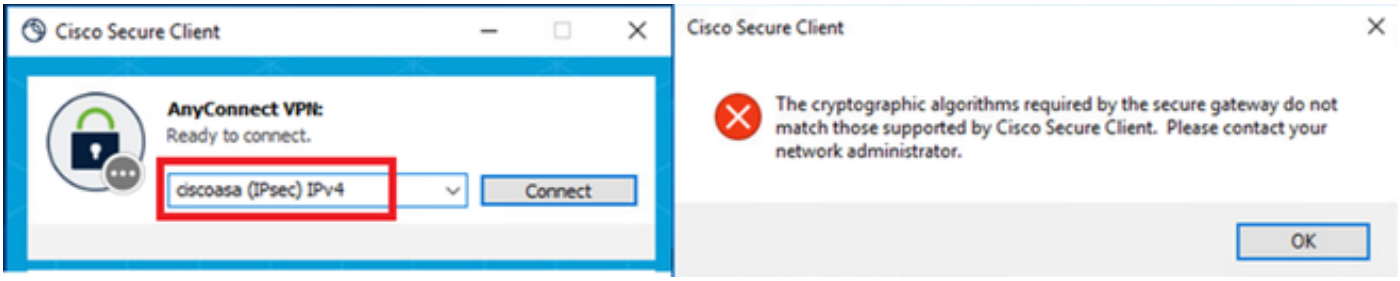
استكشاف الأخطاء وإصلاحها

قد يؤدي عدم تطابق خوارزميات التشفير إلى حدوث حالات فشل في الاتصال. هذا مثال على متى تحدث مشكلة عدم تطابق الخوارزميات. تنفيذ الخطوة 15 من تكوين القسم في ASDM يمكن أن يحل المشكلة.

الخطوة 1. بدء اتصال VPN

على نقطة النهاية، قم بتشغيل Cisco Secure Client وتأكد من فشل الاتصال بسبب عدم تطابق خوارزميات التشفير.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.



فشل الاتصال

الخطوة 2. تأكيد Syslog في CLI

في syslog، تأكد من فشل مفاوضات IKEv2.

<#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ
May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERR

Failed to find a matching policy

المرجع

[AnyConnect عبر IKEv2 إلى ASA باستخدام AAA وشهادة المصادقة](#)

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).