

# ASDM في نم آلا لي م ع ل ا IKEv2/ASA ني و ك ت CERT ة ق د اص م ؛ & AAA م اد خ ت س اب

## ت ا ي و ت ح م ل ا

---

[ة م د ق م ل ا](#)

[ة ي س اس آ ل ا ت اب ل ط ت م ل ا](#)

[ت اب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ت ا ن ي و ك ت ل ا](#)

[ASDM ي ف ني و ك ت ل ا](#)

[VPN ت ا ج ل ا ع م ح ت ف 1 ة و ط خ ل ا](#)

[ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ف ي ر ع ت 2 ة و ط خ ل ا](#)

[VPN ت ا ل و ك و ت و ر ب 3 ة و ط خ ل ا](#)

[ل ي م ع ل ا ر و ص 4 ة و ط خ ل ا](#)

[ة ق د اص م ل ا ب ي ل ا س ا 5 ة و ط خ ل ا](#)

[SAML ني و ك ت 6 ة و ط خ ل ا](#)

[ل ي م ع ل ا ن ا و ن ع ني ي ع ت 7 ة و ط خ ل ا](#)

[ت ا ك ب ش ل ل ا ع ا م س ا ل ي ل ح ت م د ا و خ 8 ة و ط خ ل ا](#)

[NAT ع ا ف ع ا 9 ة و ط خ ل ا](#)

[ع ا ل م ع ل ل ت م ا ر ش ن 10 ة و ط خ ل ا](#)

[ت ا د ا د ع ا ل ا ط ف ح 11 ة و ط خ ل ا](#)

[ه ر ي د ص ت و ن م آ ل ا ل ي م ع ل ا ف ي ر ع ت ف ل م د ي ك ا ت 12 ة و ط خ ل ا](#)

[ن م آ ل ا ل ي م ع ل ا ف ي ر ع ت ف ل م ل ي ص ا ف ت د ي ك ا ت 13 ة و ط خ ل ا](#)

[ASA CLI ي ف ت ا د ا د ع ا ل ا د ي ك ا ت 14 ة و ط خ ل ا](#)

[ر ي ف ش ت ة ي م ز ر ا و خ ة ف ا ض ا 15 ة و ط خ ل ا](#)

[Windows م د ا خ ي ف ني و ك ت ل ا](#)

[ISE ي ف ني و ك ت ل ا](#)

[ز ا ه ج ة ف ا ض ا 1 ة و ط خ ل ا](#)

[Active Directory ة ف ا ض ا 2 ة و ط خ ل ا](#)

[ة ي و ه ل ا ر د ص م ة ل س ل س ة ف ا ض ا 3 ة و ط خ ل ا](#)

[چ ه ن ة و ع و م ج م ة ف ا ض ا 4 ة و ط خ ل ا](#)

[ة ق د اص م ل ا چ ه ن ة ف ا ض ا 5 ة و ط خ ل ا](#)

[ل ي و خ ت ل ا چ ه ن ة ف ا ض ا 6 ة و ط خ ل ا](#)

[ة ح ص ل ل ا ت م ق ق و ح ت ل ا](#)

[Win10 PC1 ي ل ل ا ن م آ ل ا ل ي م ع ل ا ف ي ر ع ت ف ل م خ س ن ا 1 ة و ط خ ل ا](#)

[VPN ل ا ص ت ا ع د ب 2 ة و ط خ ل ا](#)

[ASA ي ل ع Syslog د ي ك ا ت 3 ة و ط خ ل ا](#)

[ASA ي ل ع IPsec ل م ع ة س ل ج د ي ك ا ت 4 ة و ط خ ل ا](#)

[Radius Live ل ج س د ي ك ا ت 5 ة و ط خ ل ا](#)

[ا ه ج ا ل ص ا و ع ا ط خ آ ل ا ف ا ش ك ت س ا](#)

[VPN ل ا ص ت ا ع د ب 1 ة و ط خ ل ا](#)

[CLI ي ف Syslog د ي ك ا ت 2 ة و ط خ ل ا](#)

[ع ج ر م ل ا](#)

---

# ةمدقملا

مادختساب ASA ىلع IKEv2 ربع نمآلا ليمعلا نيوكتل ةمزلالا تاوطخلا دنتسمل اذه فصوي ةداهشلا ةقداصم و AAA مادختساب ASDM.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلال عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت:

- Cisco (ISE) نم ةيوهلا تامدخ كرحم نيوكت
- Cisco نم (ASAv) ةلدعمل ةيرهاطلا نامألا ةزهجأ نيوكت
- Cisco نم (ASDM) ةلدعمل نامألا ةزهجأ ريديم نيوكت
- VPN ةقداصم قفدت

### ةمدختسمل تانوكملا

ةيلال ةيدامل تانوكملا او جماربال تارادصإ ىل دنتسمل اذه يف ةدراولا تامولعمل دنتست:

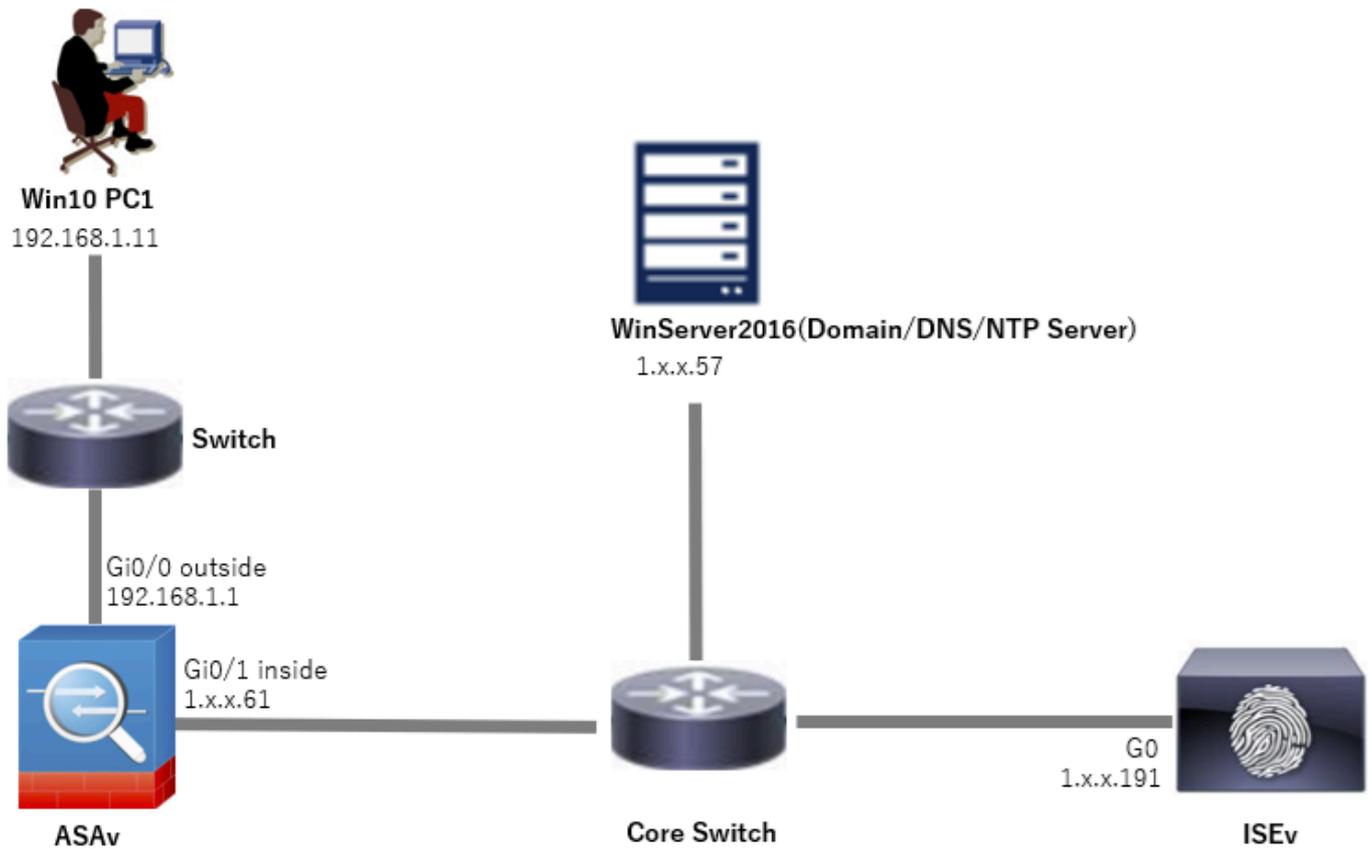
- Identity Services Engine Virtual 3.3 1 حيحصتلا جماربال
- 9.20(2)21 فيكتلل لباقلا يرهاطلا نامألا زاهج
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016 ليغشتلا ماظن
- Windows 10 ليغشتلا ماظن

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسمل اذه يف ةدراولا تامولعمل عاشنإ مت تناك اذإ. (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجألا عيمج تأدب رمأ يال لمحتملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتكتك بيش.

## ةكبشلال يطيختلا مسرلا

دنتسمل اذه لاثمل همادختسا متي يذلا طاطخملا ةروصولا هذه ضرعت.

م تي يذلاو، ad.rem-system.com وه Windows Server 2016 ىلع هن يوكت مت يذلا لاجملا مسلا دنتسمل اذه يف لاثمك همادختسا.



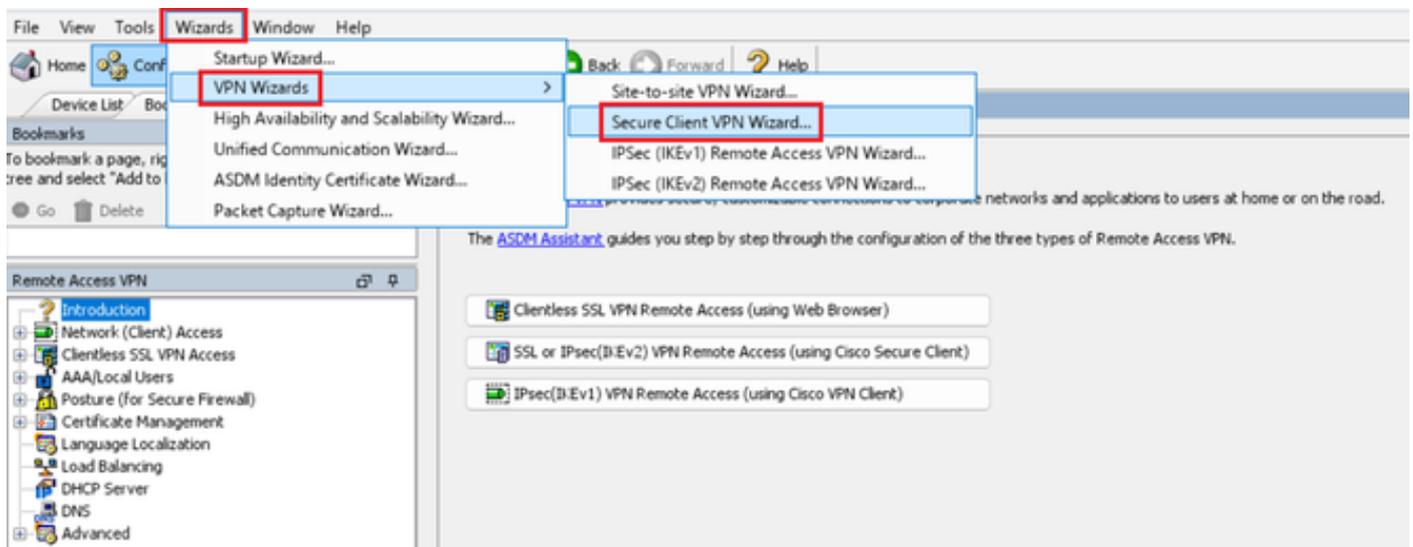
ةكبش ل ل يطيطختل م سر ل

## تانيوكتل

ASDM في نيوكتل

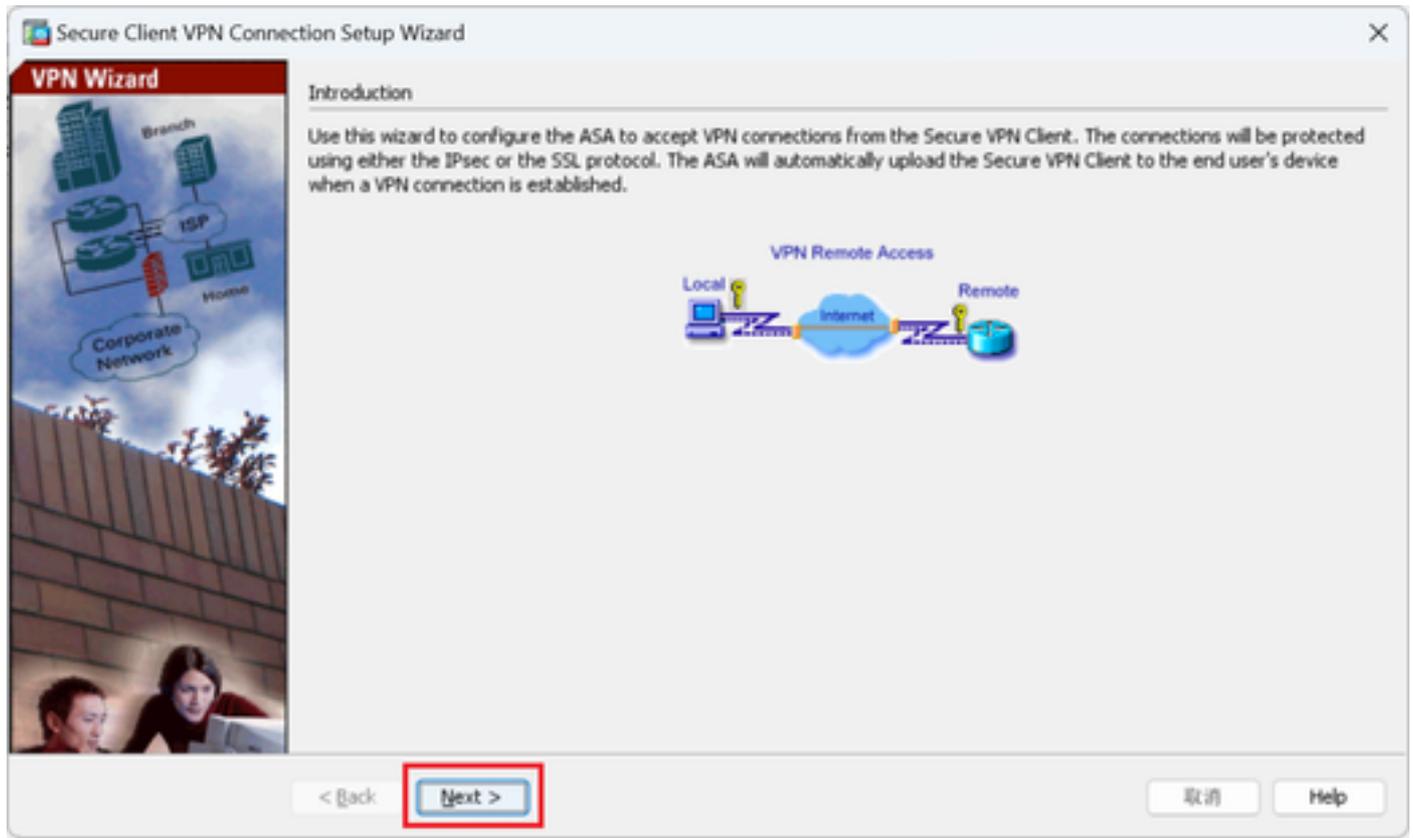
VPN تاجل اع م حتف 1. ةوطخل

نم آلا ليمع ل اب ةصاخ ال VPN ةكبش جلاع م قوف رونا، VPN تاجل اع م > تاجل اع م ال ال لقتنا



VPN تاجل اع م حتف

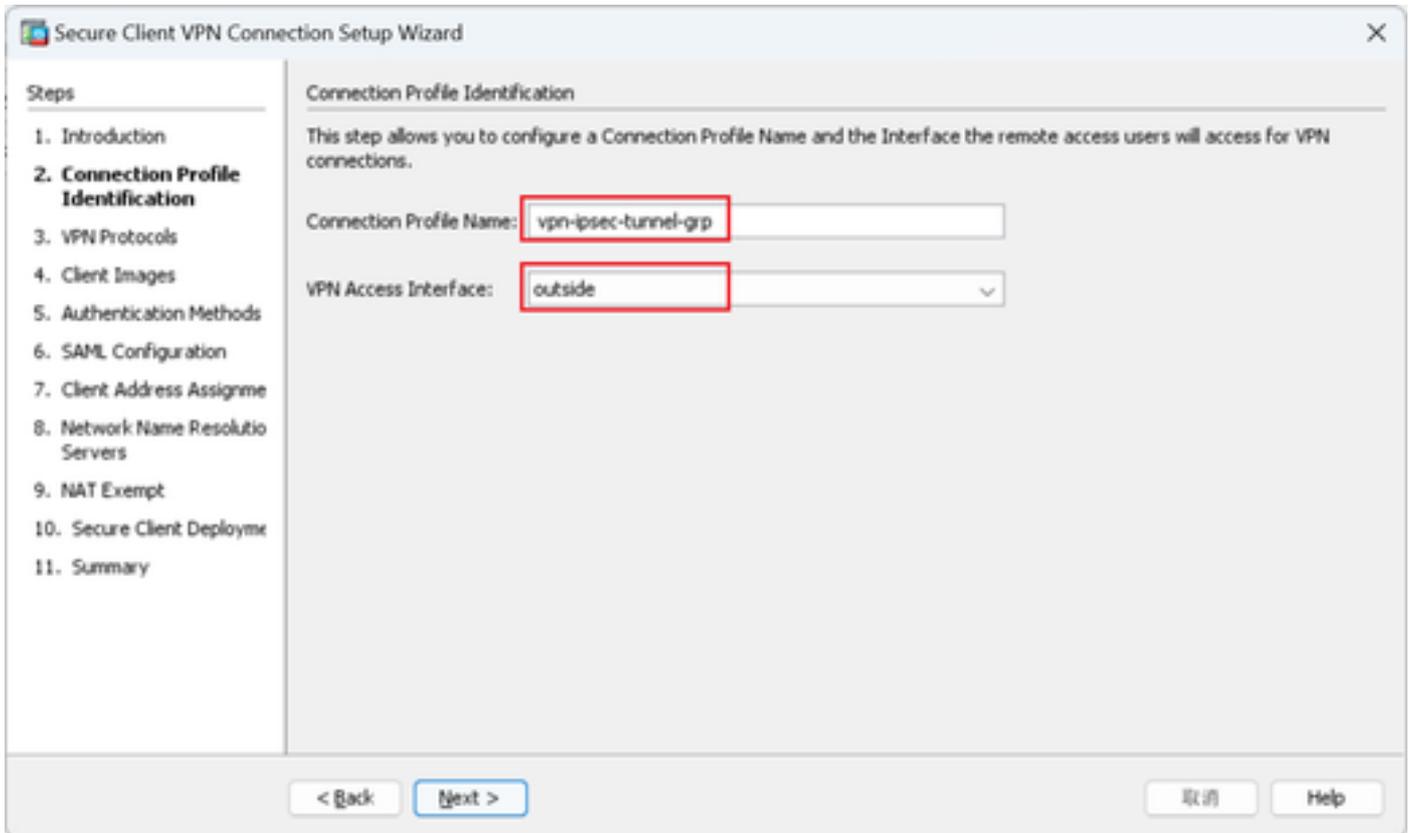
(ي لاتل) Next قوف ر قنا



ي لاتل رزلا قوف ر قنا

لاصتال فيرعت فلم فيرعت 2. ةوطخال

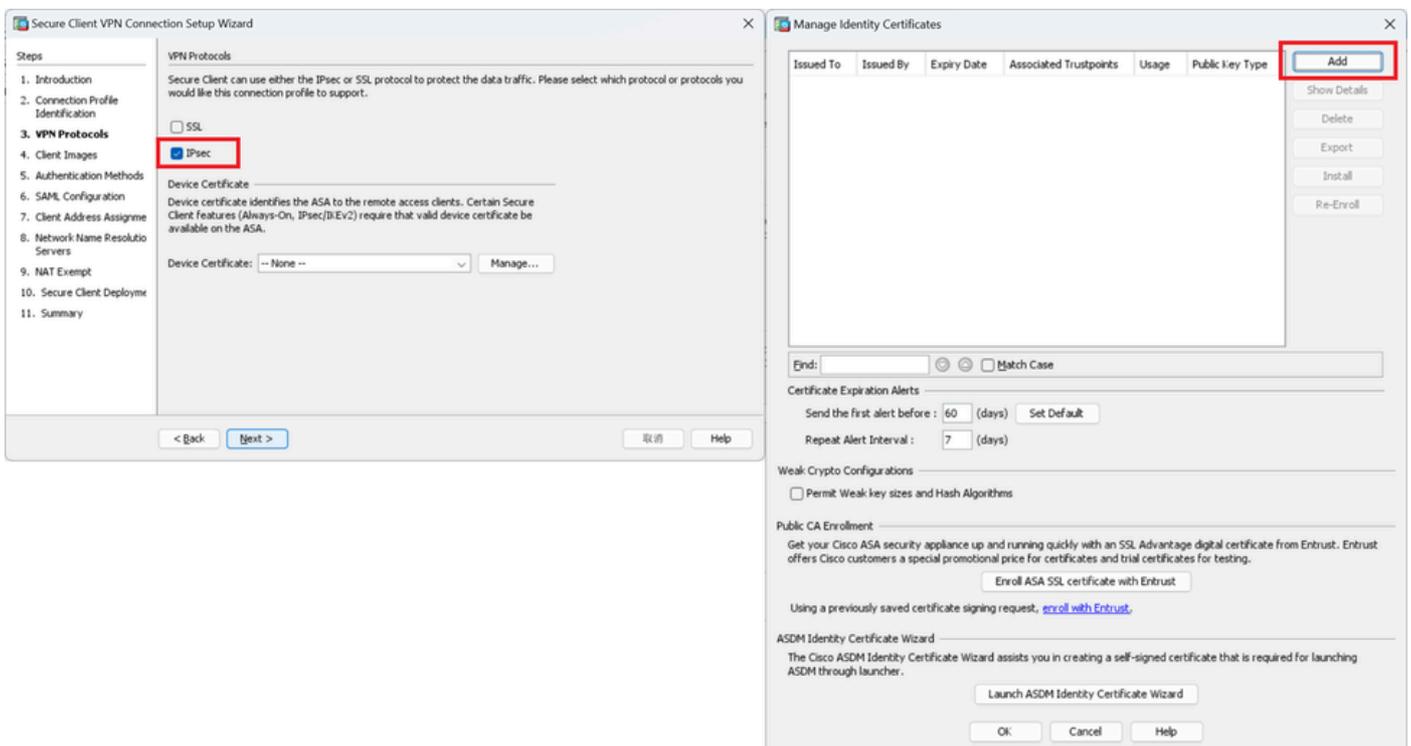
لاصتال فيرعت فلم ل لاخال تامولعم  
لاصتال فيرعت فلم مسا : vpn-ips-tunnel-grp  
جراخ : VPN ل لوصول ةهواو



لاصتالال فيرعت فلم فيرعت

### VPN تالوكوتورب 3. ةوطخال

ةديج ايتاذ ةعقوم ةداهش ةفاضال ةفاضال رز قوف رقنا، IPsec دح.

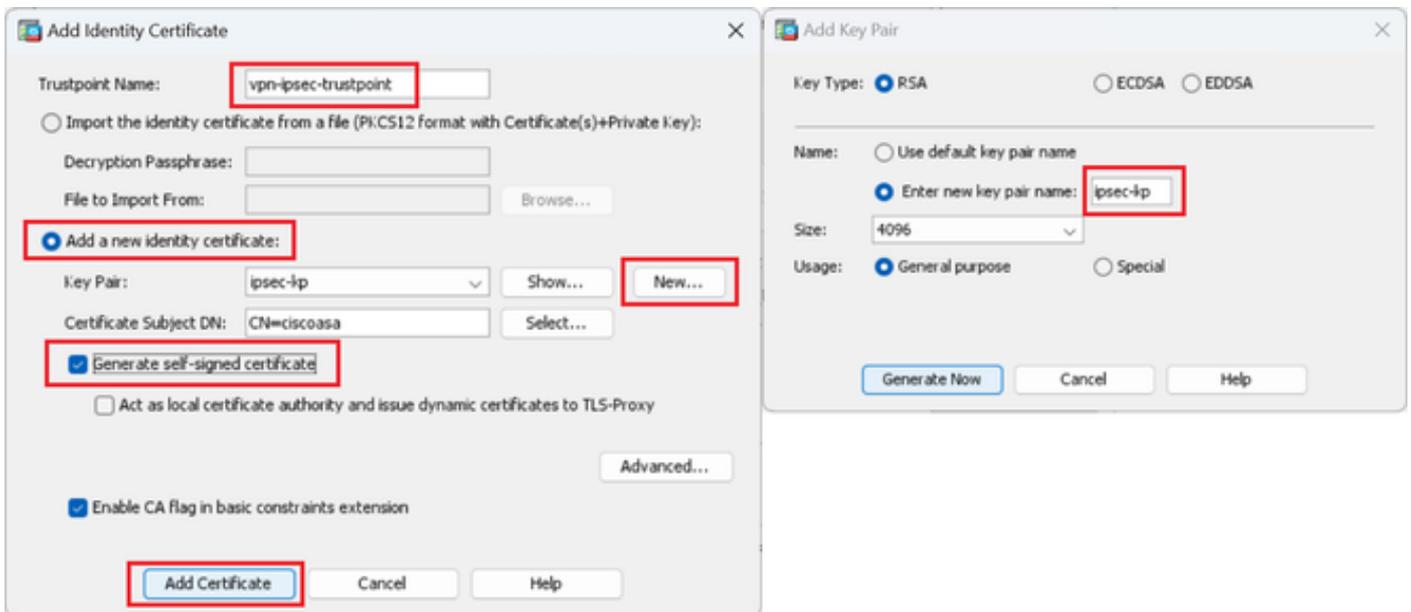


VPN تالوكوتورب

ايتاذة عقوملا ةداهشلل تامولعم لاخذإ

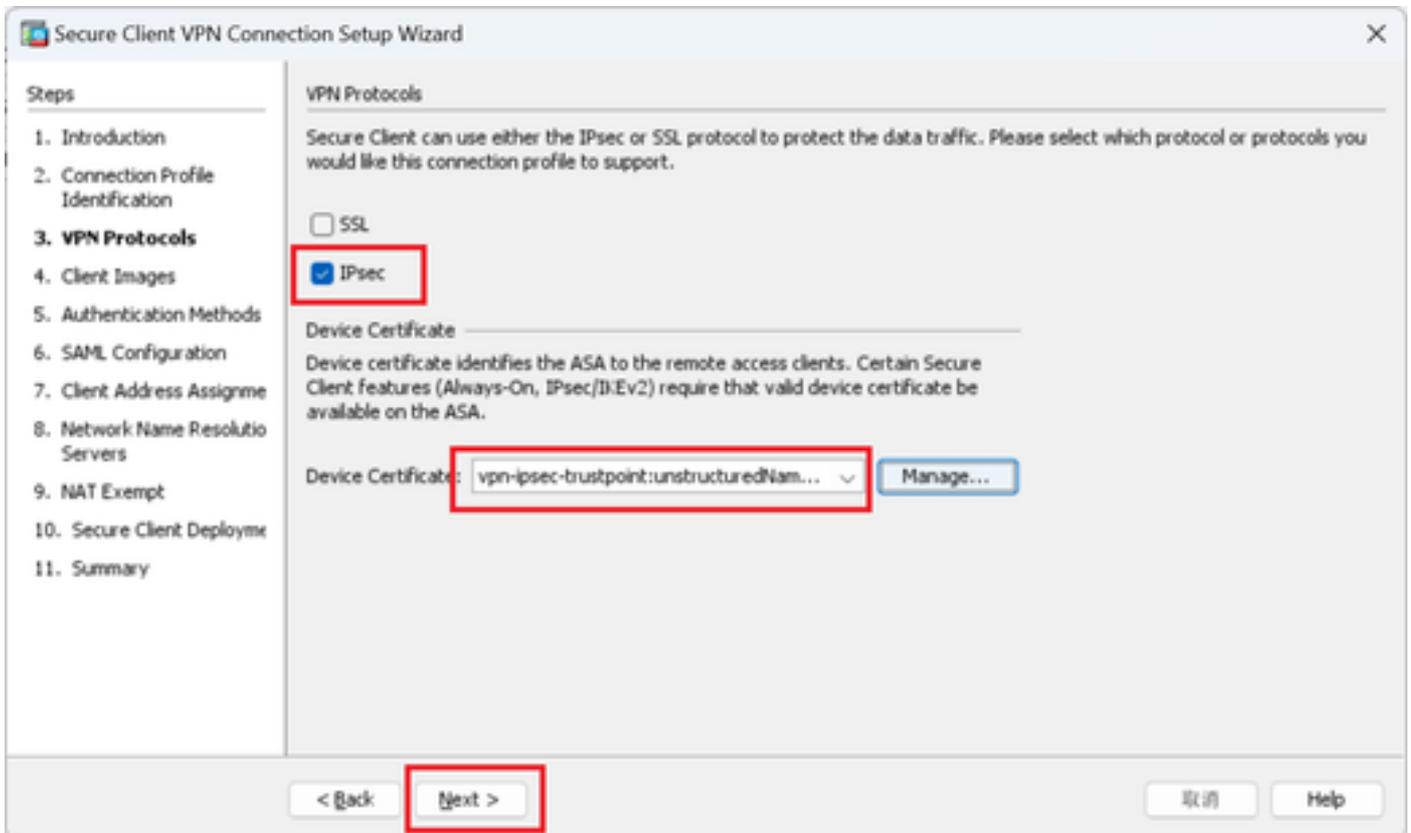
مس TrustPoint: vpn-ipsEc-TrustPoint

جوز : IPsec-KP حيتافملا



ايتاذة عقوملا ةداهشلل ليصافات

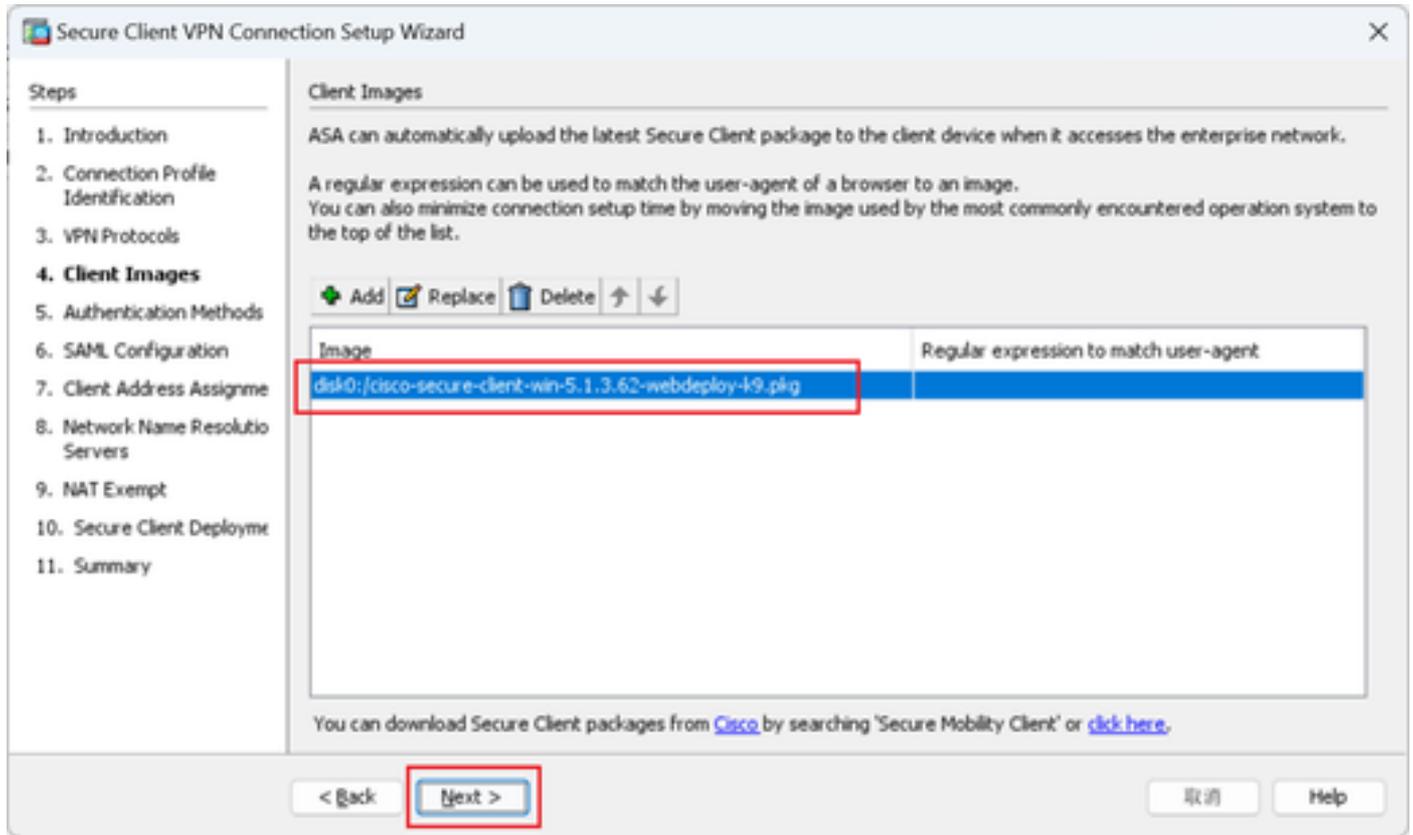
رز كلذ دعب تقطوط VPN، تالوكوتورب دادعإ ةيلمعل تذكأ



VPN لوكوتورب تادادعإ ديكأت

## لي م عمل روص 4. ة و ط خ ل

ي ل ل ر ز ل ق و ف ر ق ن ا ، ة ن م آ ل ي م ع ة ر و ص ة ف ا ض ا ل ر ز ة ف ا ض ا ق و ف ر ق ن ا



لي م عمل روص

## ة ق د ا ص م ل ب ي ل ل ا س ا 5. ة و ط خ ل

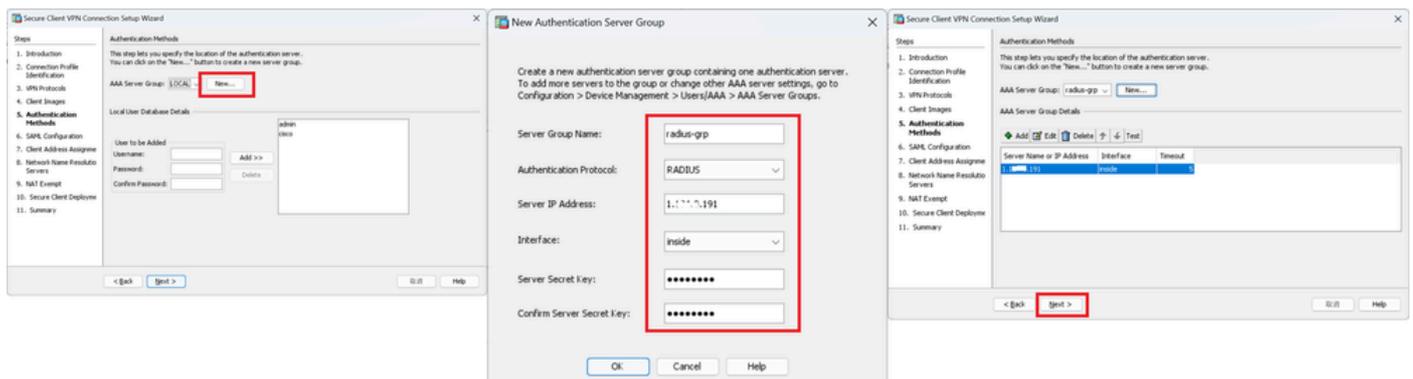
ي ل ل ر ز ل ق و ف ر ق ن ا ، د ي د ج A A A م د ا خ ة ف ا ض ا ل د ي د ج ر ز ق و ف ر ق ن ا

م د ا و خ ل ة و م ج م م س ا : R A D I U S - G R P

ة ق د ا ص م ل ل و ك و ت و ر ب : R A D I U S

م د ا و خ ل ل I P ن ا و ن ع : 1 . x . x . 1 9 1

ل خ ا د ل ا : ة ه ج ا و ل ا



ةقد اصم ال بيل اسأ

## 6. ةوطخ ال SAML نيوك ت

رز كل ذ دع ب تق طقط

The screenshot shows the 'Secure Client VPN Connection Setup Wizard' window. The 'Steps' list on the left includes: 1. Introduction, 2. Connection Profile Identification, 3. VPN Protocols, 4. Client Images, 5. Authentication Methods, 6. SAML Configuration (highlighted), 7. Client Address Assignme, 8. Network Name Resolutio Servers, 9. NAT Exempt, 10. Secure Client Deployme, and 11. Summary. The main area is titled 'SAML Configuration' and contains the following fields: 'Authentication Method' set to 'AAA', 'AAA Server Group' set to 'radius-grp', and 'SAML Identity Provider SAML Server' set to '--- None ---'. There are 'Manage...' buttons next to the 'AAA Server Group' and 'SAML Server' fields. A checkbox for 'Use LOCAL # Server Group fails' is unchecked. At the bottom, there are '< Back', 'Next >', '取消', and 'Help' buttons. The 'Next >' button is highlighted with a red box.

SAML نيوك ت

## ل بمل ال ناوع ني عت 7. ةوطخ ال

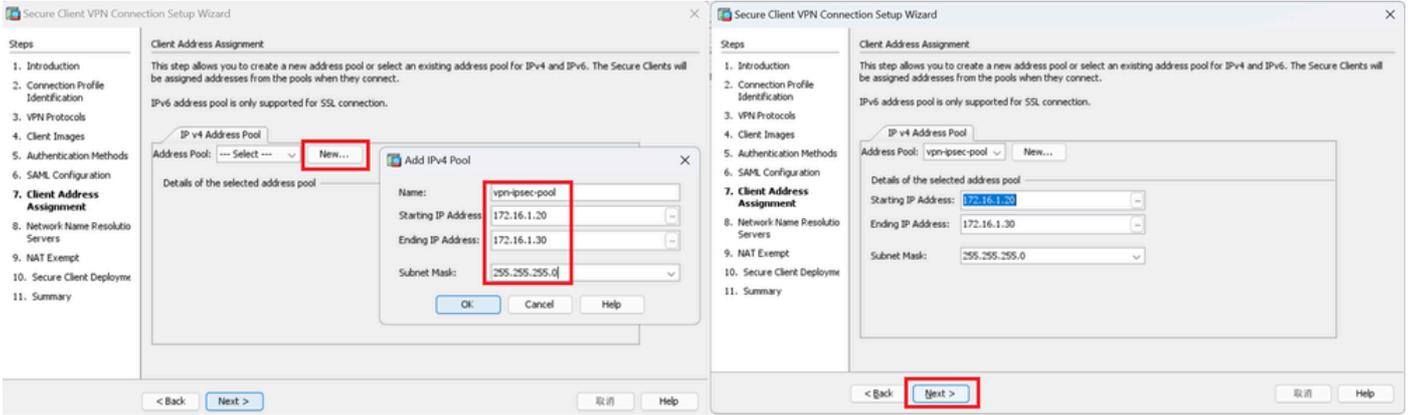
يل ال رزل ا قوف رقا ، ديدج IPv4 عمج ة فاضال ديدج رز قوف رقا

VPN-IPSec-pool : م سال ال

172.16.1.20 : ي ل و ال IP ناوع

172.16.1.30 IP : ناوع ة ياهن

255.255.255.0 : ة ي عرف ال ةك بشل ال عانق



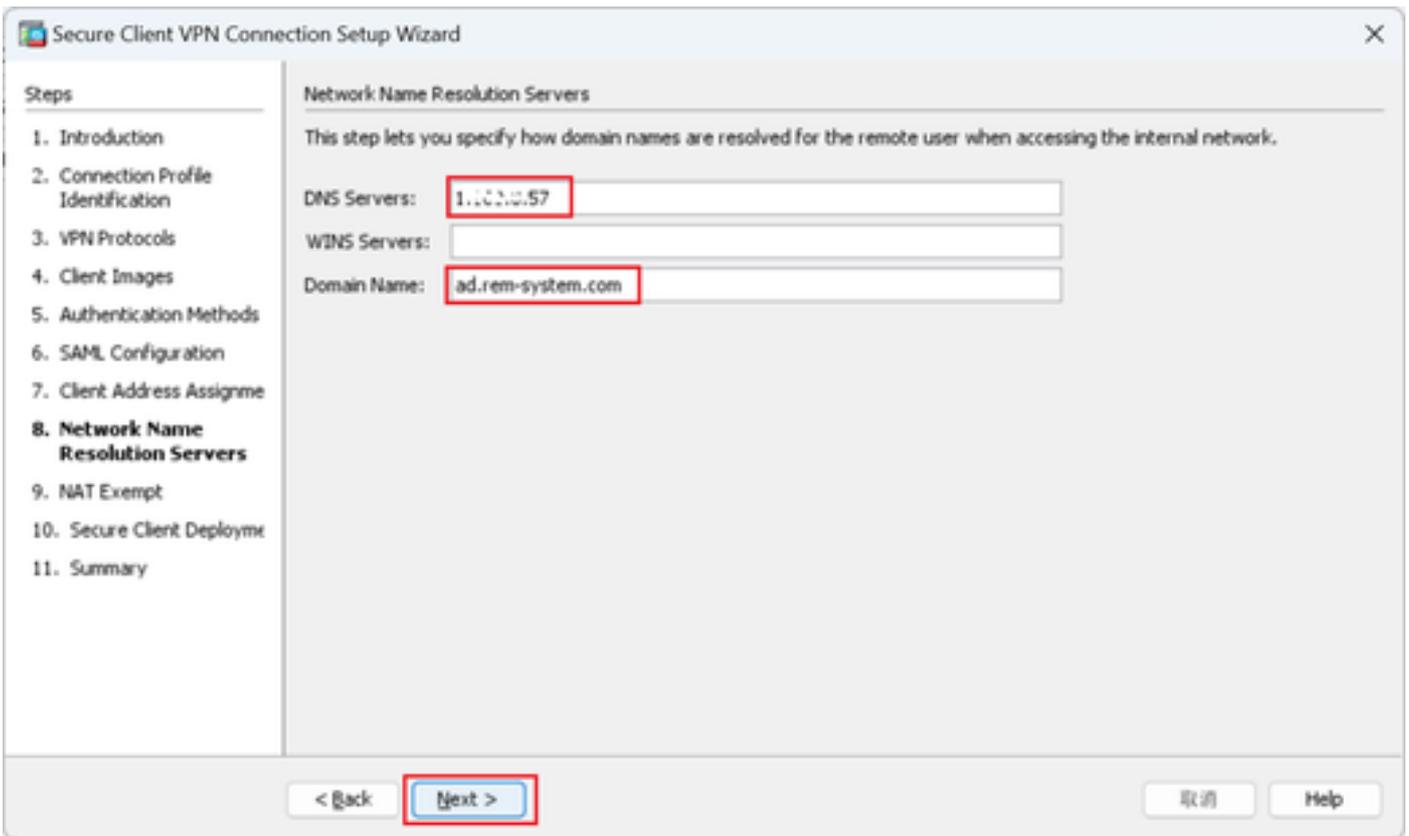
ليعمل ناونع نيعت

تاكبشال عامس ليلحت مداوخ. 8 ةوطخل

يللال رزل قوف رونا، لاجمل او DNS ل تامولعم لاخدا

DNS: 1.x.x.57 مداوخ

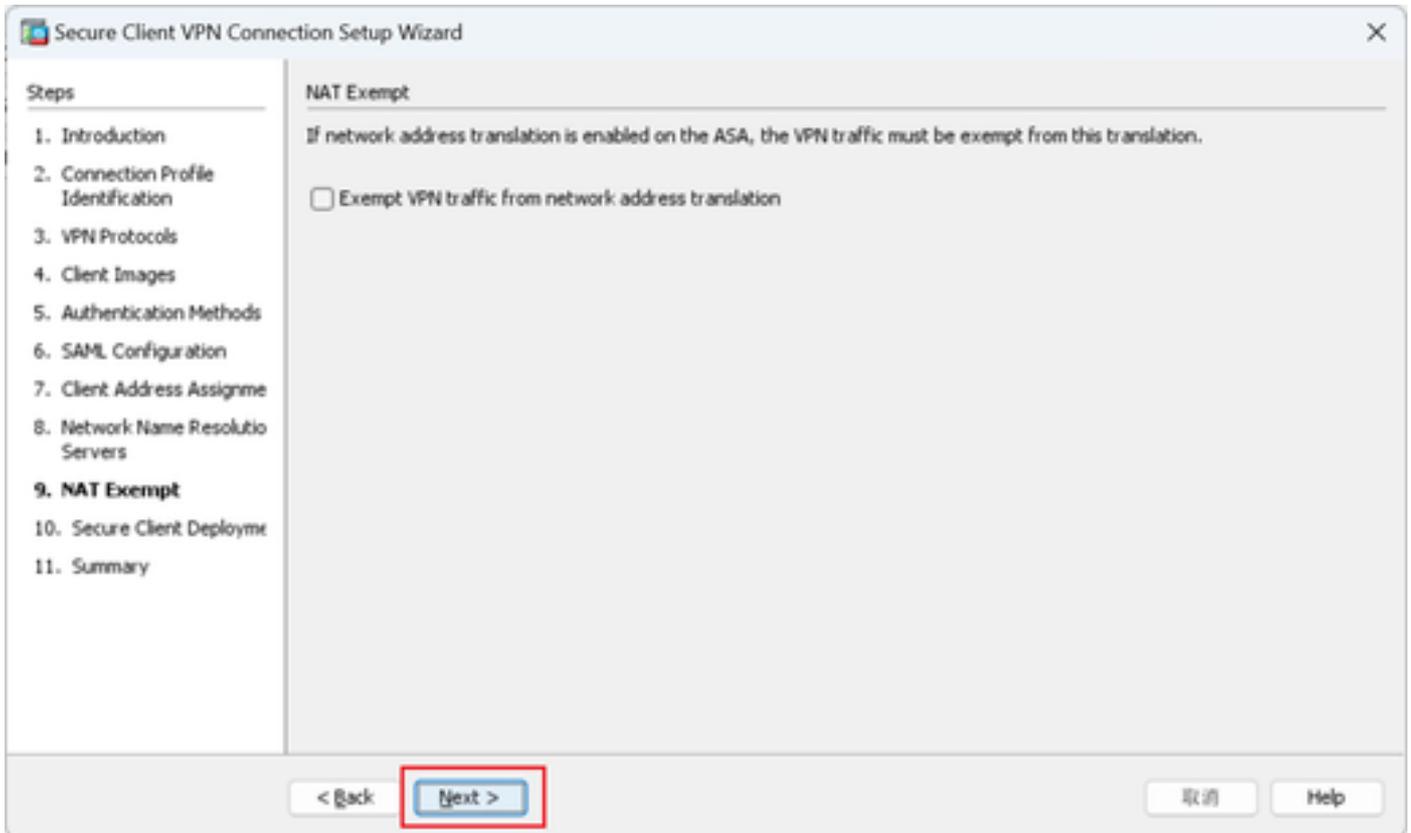
لاجمل مس: ad.rem-system.com



تاكبشال عامس ليلحت مداوخ

NAT افع | 9 ةوطخل

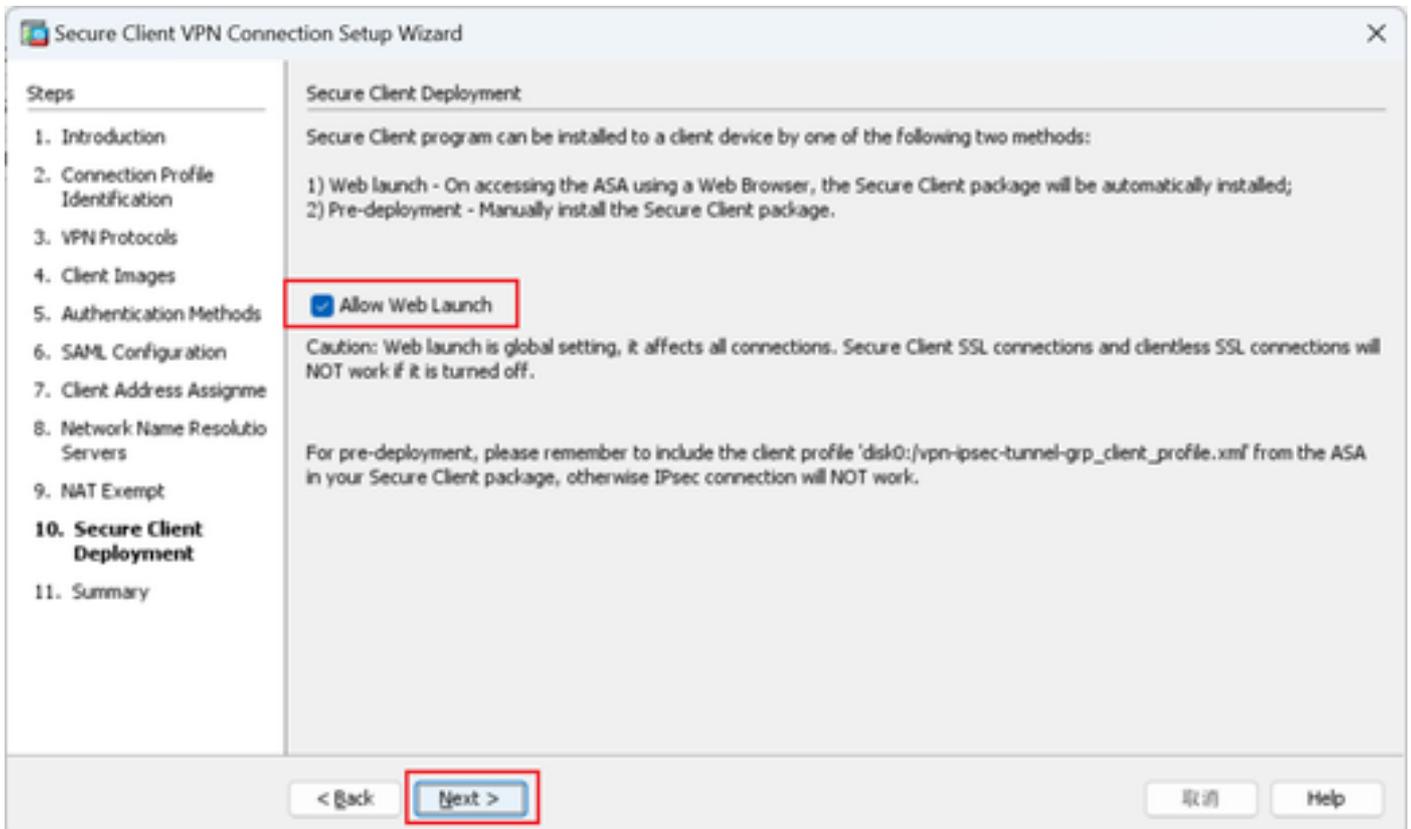
رزل لذب تقوط



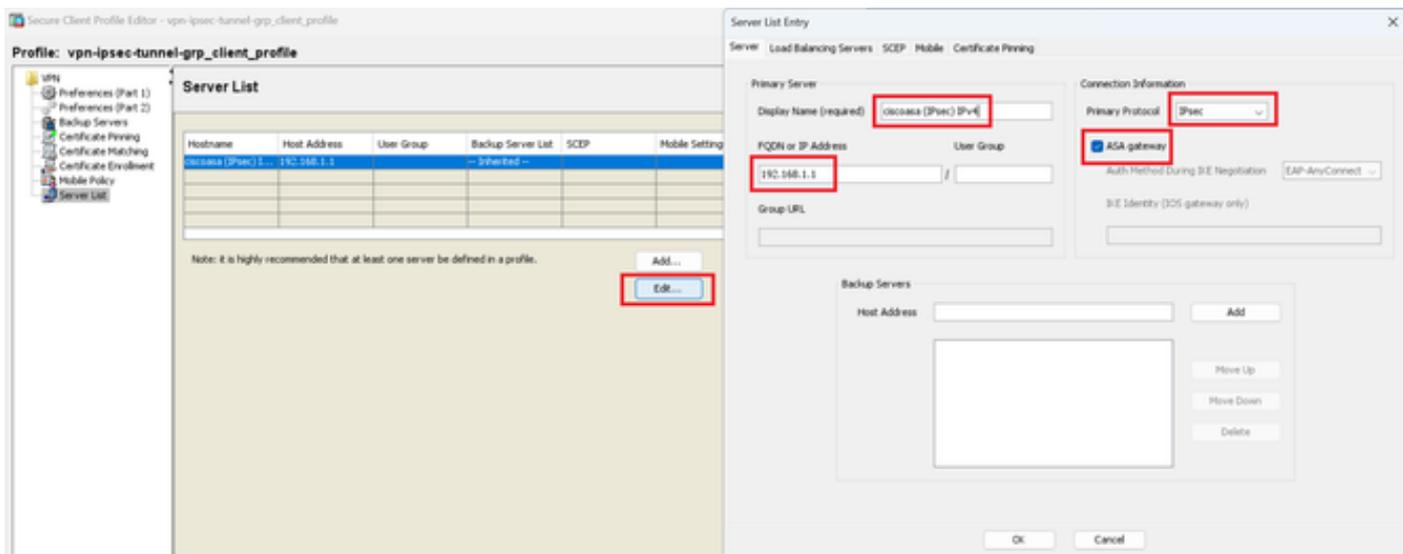
NAT اءافع

ءالء ل ل نم آ رشن 10 ة و طء ل

ء ل ل ر ز ل ق و ف ر ق ن ا ، ب ء و ل ل ء ء ش ت ب ء ا م س ل ل ء ء

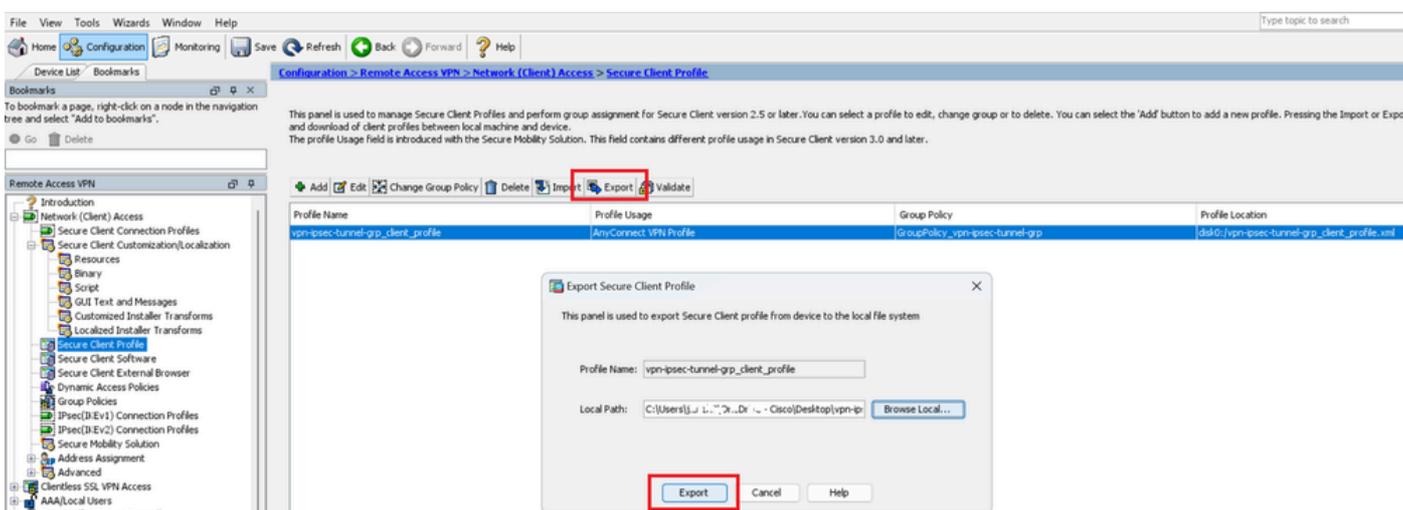






نم آلا ليعرعت فلم ديكتأت

يلحمل رت وويبمكلا لى لى فيصوتلا ريصت ل ريصت رز لى ع رونا



نم آلا ليعرعت فلم ريصت

نم آلا ليعرعت فلم لى صافات ديكتأت 13 ةوطخل

يساس آلا لوكوتوربال نا نم دكأتو، ضرعت سمل ةطساوب "نم آلا ليعرعت فلم" حتفا و 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>

```

نمآل ليمعلا فيرعت فلم ليرصافت

## ASA CLI في تاداعإل ديكتأت 14. ةوطخل

ASA ل (CLI) رمأوال رطس ةهجاو في ASDM ةطساوب اهؤاشنإ مت يتل IPsec تاداعإ ديكتأت

```
// 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_CRYPTOMAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map outside_map interface outside

// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
cr1 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

// Specifies 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 addresses 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

```

ري فشت ةي مزراوخ ةفاضلا 15 ةوطخل

IKEv2 جهن ىلإ 19 ةومجمل فضا، ASA رماو ا رطس ةهجاو يف

---

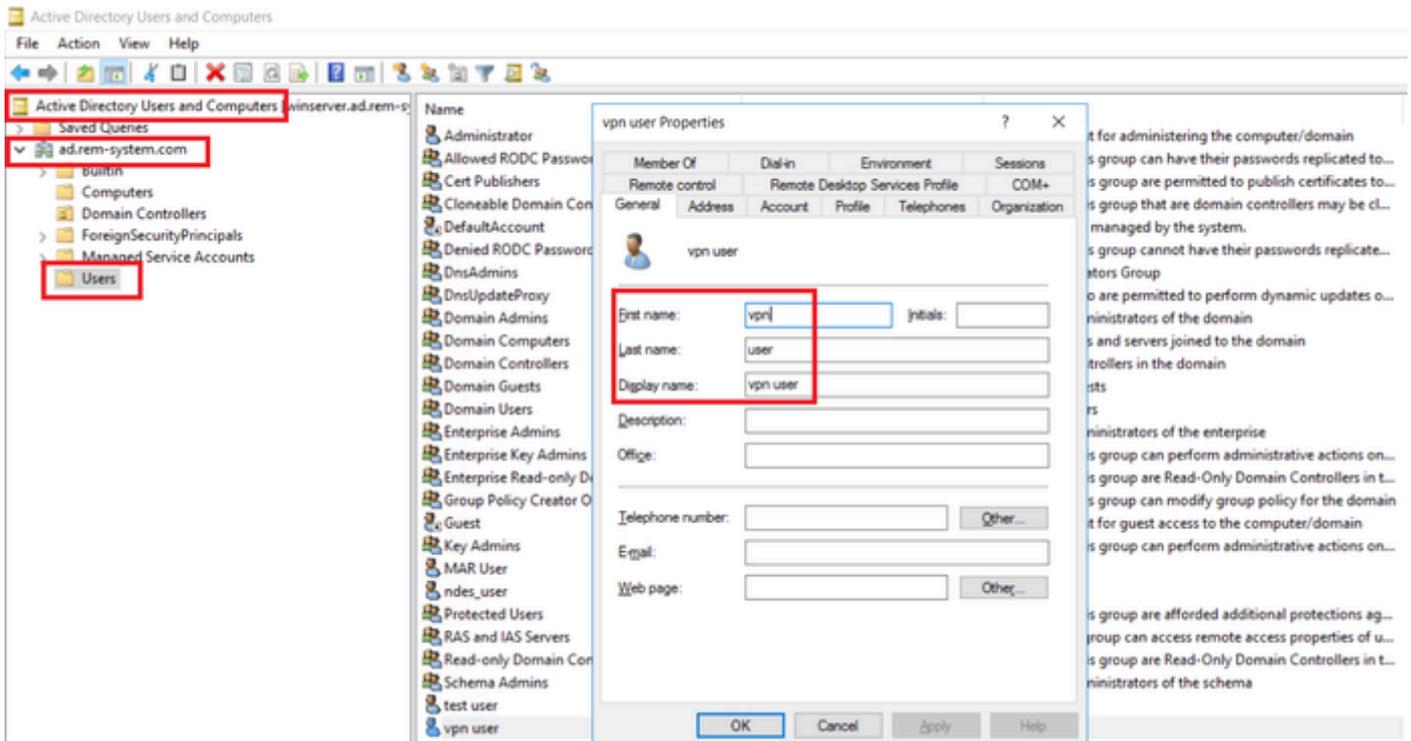
تاعومجم معدت Cisco Secure Client دع مل IKEv2/IPsec، تالاصتال ةبسنلاب :ةظحال م ربيغتلا اذه يدوي دق. 4.9.00086 رادصلل اق فو 24 و 14 و 5 و 2 ماقراً Diffie-Hellman (DH) ريفشلتال ةيمزراوخ قباطت مدع ببسب لاصتالا يف لشف تالاح ثودح ىلإ.

---

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

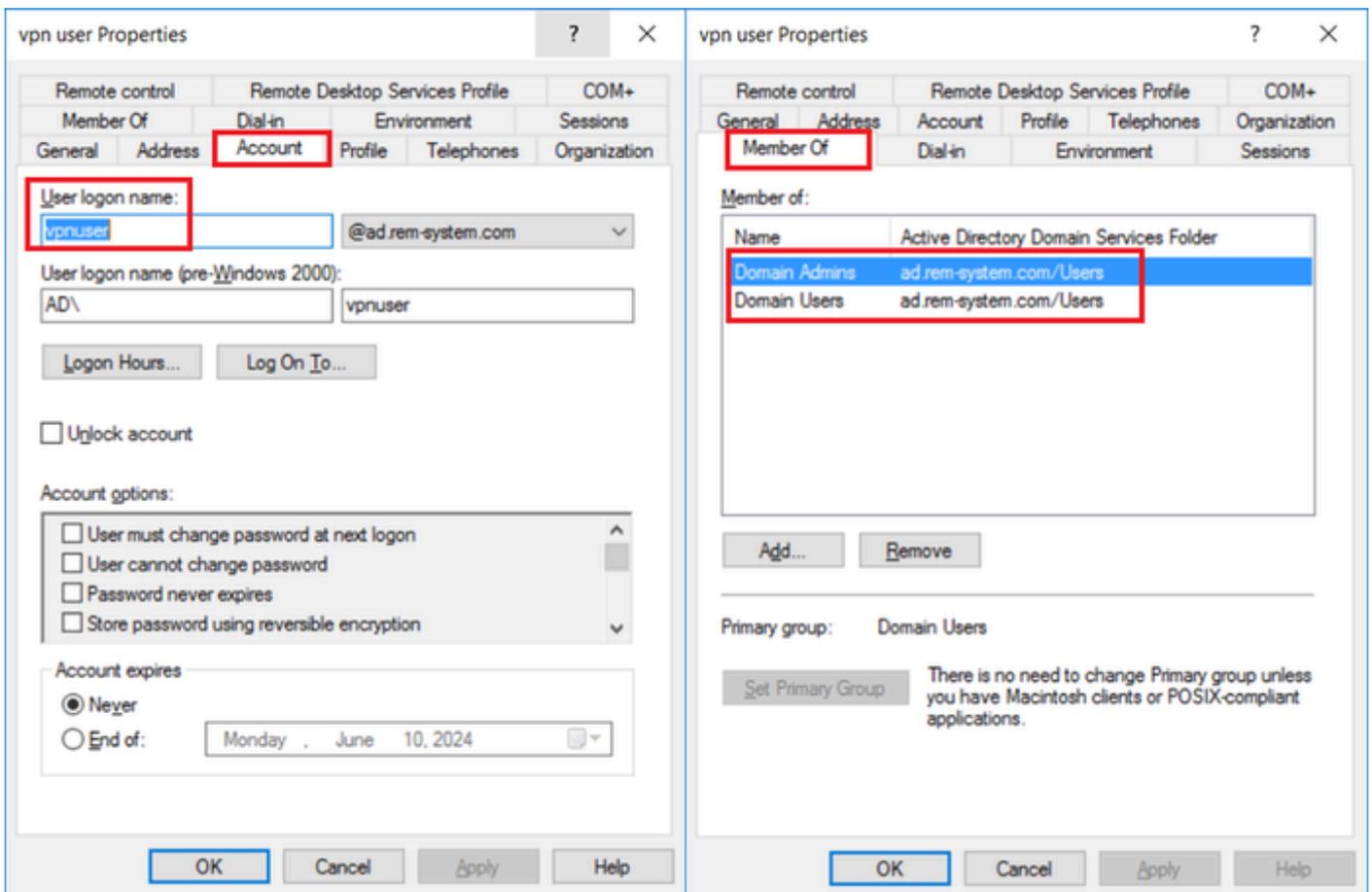
## Windows مداخل في نيوكتلا

VPN لاصتال لمعتسم لاجم فيضي نأجاتحت تنأ Active Directory Users and Computers ىلإ لقتنا. لاجم مدختسمك vpnUser ةفاضلإ Users قوف رونا، Computers.



لاجم مدختم ةفاض

لاجم لايم مدختم و لاجم لايل وؤسم وضع يلا لاجم لا مدختم ةفاض



لاجم لاوم مدختم و لاجم لا وؤسم

## ISE في نيوكتل

زاهج ةفاضل 1. ةوطخل

ASAv. زاهج ةفاضل AddButton قوف رونا، ةكبشلا ةزهجأ > Administration لىل لقتن

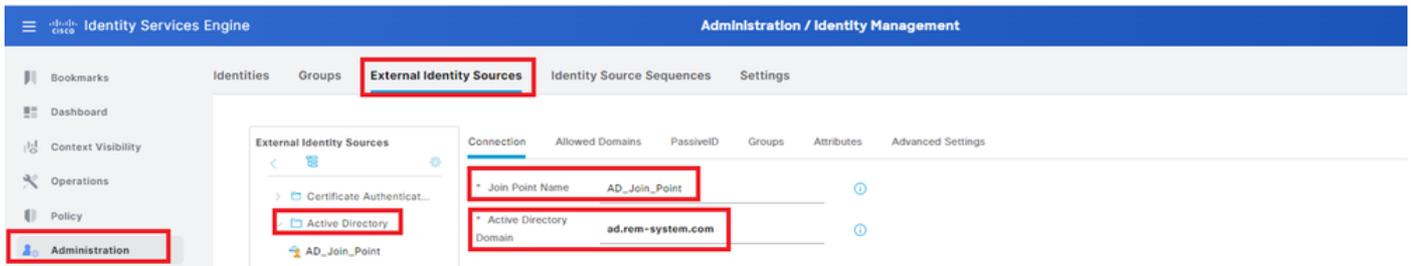
The screenshot displays the configuration page for a Network Device in ISE. The device name is ASAv. The IP address is 1.1.1.1/32. The device profile is Cisco. The RADIUS Authentication Settings are enabled, and the RADIUS UDP Settings are configured with Protocol set to RADIUS and Shared Secret set to cisco123.

زاهج ةفاضل

Active Directory ةفاضل 2. ةوطخل

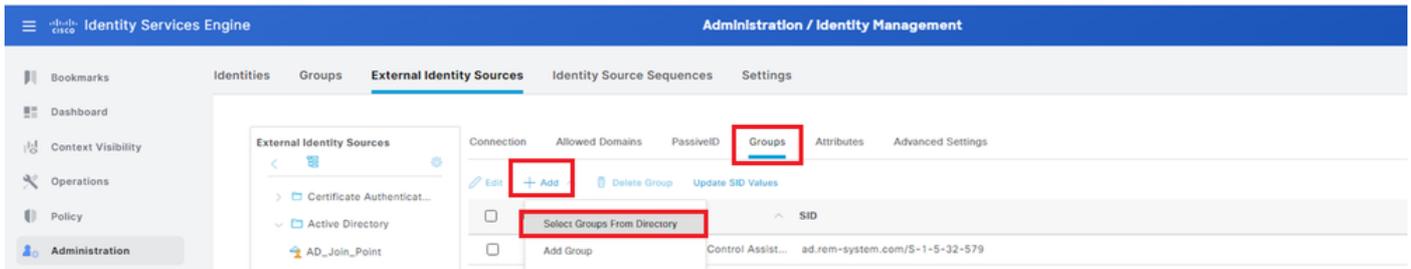
ConnectTab. قوف رونا، Active Directory > ةيجراخل ةيوهلا رداصم > Administration لىل لقتن  
ISE. لىل Active Directory ةفاضل مقو

- طبرلا ةطقن مسا: AD\_JOIN\_POINT
- Active Directory لاجم: ad.rem-system.com



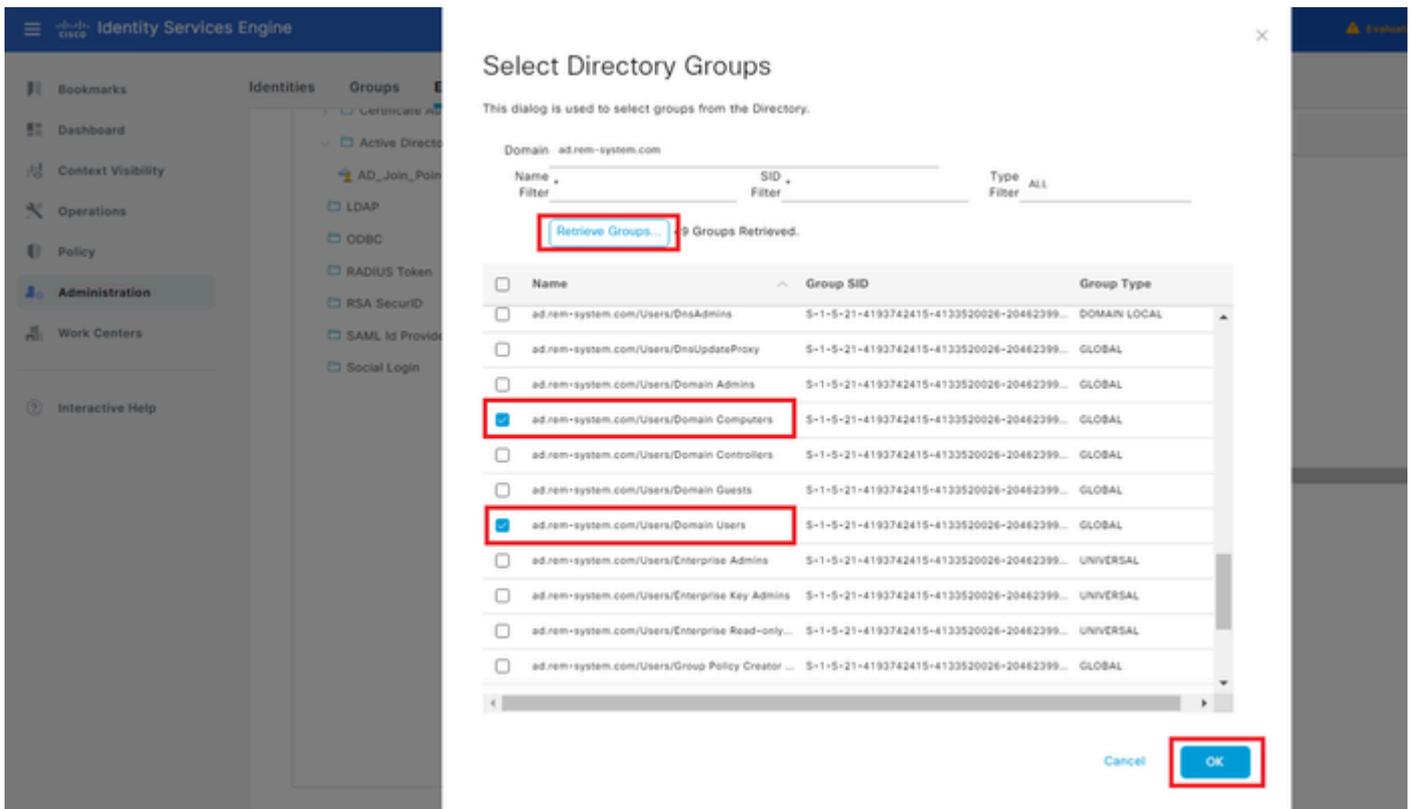
إضافة Active Directory

عملية ازالة Directory من دس نمل ازالة من تاعومجم دح، تاعومجم بيوبت الة عمال ع الى لقتنا الة دس نمل.



لي ل دلا من تاعومجم دح

الة دس نمل ازالة من تاعومجم الة دادرست الى قوف رونا Checkad.rem-system.com/Users/Domain Computers and ad.rem-system.com/Users/Domain User And click OK.



نم دختس مل او لاجم الة رتوي بمك زهجا ة فاضا

ة يوه الة رصم الة لس لس ة فاضا 3. ة وطلخا

ة يوه رصم لس لس ة فاضا ب مقو، ة يوه الة رصم الة لس لس ت > ة راد الى لقتنا

- مسال: Identity\_AD
- قءاصم ال نع ءءب ال ءمءاق: AD\_JOIN\_POINT

The screenshot shows the Cisco Identity Services Engine Administration / Identity Management interface. The 'Identity Source Sequences' tab is selected. The 'Identity Source Sequence' section is expanded, showing the 'Name' field set to 'Identity\_AD'. Below this, the 'Authentication Search List' section is expanded, showing a list of available identity sources and a 'Selected' list containing 'AD\_Join\_Point'.

ءوء ال رءصم ءال سلسء ءءاضا

ءهن ءءومءم ءءاضا 4. ءوءءال

ءهن ءءومءم ءءاضا + قوف رءنا، ءهن ءءومءم > ءهن ال لءءنا

- ءهن ال ءءومءم مسا: VPN\_TEST
- ءهءال ءاون ءءمء ءواسء زاهءال ءون: ءورءش ال
- ءءبءش ال ال ءءارءءال لوءول: مءءال ل سلسءء / اءء ءومءم ال ءالوءءورءب ال

The screenshot shows the Cisco Identity Services Engine Policy / Policy Sets interface. The 'Policy Sets' table is displayed, showing a row for 'VPN\_Test' with a status of 'Success' and a description of 'Default Network Access'.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Success	VPN_Test	Default Network Access	DEVICE Device Type EQUALS All Device Types		30		

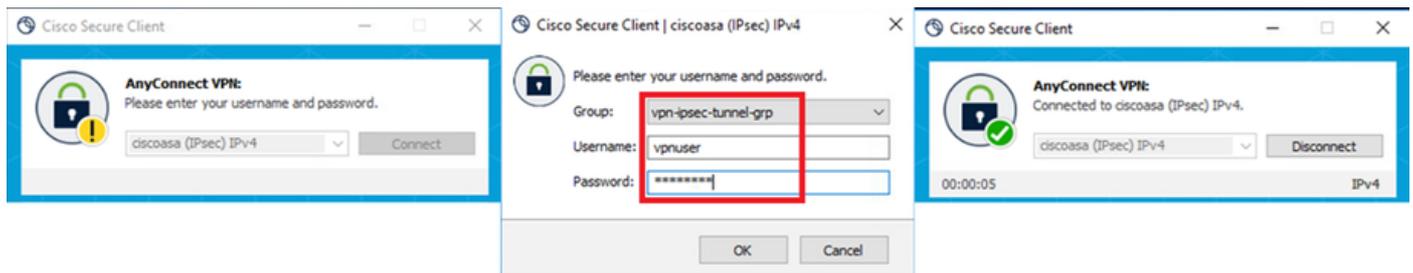
ءهن ءءومءم ءءاضا

ءءءاصم ال ءهن ءءاضا 5. ءوءءال

ءءءاصم ءهن ءءاضا VPN\_TEST قوف رءنا، ءهن ال ءءومءم ال لءءنا



م ت، رورملا ةم لك و مدخت س م ل ا م سا لخدأو Cisco Secure Client لي غشت ب مق، ةي اهنلا ةطقن ل ع  
حاجن ب Cisco Secure Client لاصتا دي كأت ب مق.



لاصتالاجن

### ASA ل ع Syslog دي كأت 3. ةوطخل

IKEv2 لاصتا حاجن نم دكأت، syslog، يف

```
<#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
```

### ASA ل ع IPsec لمع ةسلج دي كأت 4. ةوطخل

ASA ل ع IKEv2/IPsec لمع ةسلج دي كأت لرمأل show vpn-sessiondb detail anyconnect لي غشت ب مق.

```
<#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  
Auds 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

Radius Live لجس ديكأت 5 ةوطخلال

VPN ةقداصم ل ليغشت لالجس دكأ، LogISE ةرشابم ل (GUI) ةيموسر لمدختسم ل ةهجاو > RADIUS > تاي لمعلا ل ل لقتنا

Time	Status	Details	Repeat	Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...	Device Port	Identity Group
May 28, 2024 05:13:42...	<span style="color: green;">●</span>		0	00:50:56:98:77:A4	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess				
May 28, 2024 05:13:42...	<span style="color: green;">●</span>		0	00:50:56:98:77:A4	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation

## رصد Radius Live

رصد المجلد لعمليات الجس لخصائصه "الاح" قوف رقمنا.

Cisco ISE

**Overview**

Event: 5200 Authentication succeeded

Username: vpnuser

Endpoint Id: 00:50:56:98:77:A4

Endpoint Profile: Windows10-Workstation

Authentication Policy: VPN\_Test >> VPN\_Authentication

Authorization Policy: VPN\_Test >> VPN\_Authorization

Authorization Result: PermitAccess

**Authentication Details**

Source Timestamp: 2024-05-28 17:13:42.897

Received Timestamp: 2024-05-28 17:13:42.897

Policy Server: ise33-01

Event: 5200 Authentication succeeded

Username: vpnuser

Endpoint Id: 00:50:56:98:77:A4

Calling Station Id: 192.168.1.11

Endpoint Profile: Windows10-Workstation

Authentication Identity Store: AD\_Join\_Point

Identity Group: Workstation

Audit Session Id: 01aa003d0001700066559220

Authentication Method: PAP\_ASCII

Authentication Protocol: PAP\_ASCII

Network Device: ASAv

**Steps**

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	1
15049	Evaluating Policy Group	36
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	6
15041	Evaluating Identity Policy	20
15048	Queried PIP - Network Access.Device IP Address	2
22072	Selected identity source sequence - Identity_AD	6
15013	Selected Identity Source - AD_Join_Point	1
24430	Authenticating user against Active Directory - AD_Join_Point	4
24325	Resolving identity - vpnuser	38
24313	Search for matching accounts at join point - ad.rem-system.com	0
24319	Single matching account found in forest - ad.rem-system.com	0
24323	Identity resolution detected single matching account	0
24343	RPC Logon request succeeded - vpnuser@ad.rem-system.com	23
24402	User authentication against Active Directory succeeded - AD_Join_Point	3
22037	Authentication Passed	1
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
15036	Evaluating Authorization Policy	1
24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
24211	Found Endpoint in Internal Endpoints IDStore	9
15048	Queried PIP - Network Access.AuthenticationStatus	2
15016	Selected Authorization Profile - PermitAccess	7
22081	Max sessions policy passed	6
22080	New accounting session created in Session cache	0
11002	Returned RADIUS Access-Accept	2

رصد المجلد لعمليات الجس لخصائصه

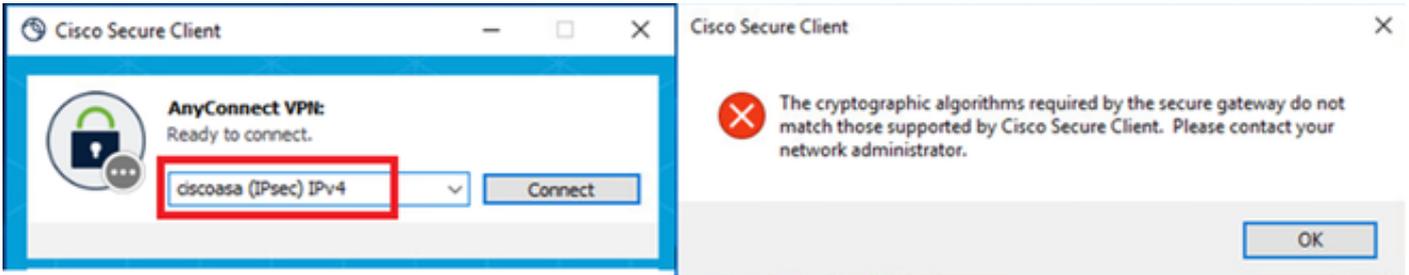
## احال الصاوا عا طخال فاشكتسا

قباط مدع لكشم ثدحت ىتم لىع لاثم اذه .لاصتالا يف لشف تالاح ثودح لى ريفشتتالا تايمزراوخ قباط مدع يدوي دق .لكشم لىح نأ نك م ASDM يف مسقلا نيوكت نم 15 ةوطخال ذيفنت .تايمزراوخ لى

VPN لاصتلا ادب .1 ةوطخال

ريفشتتالا تايمزراوخ قباط مدع ب سب لاصتالا لشف نم دكأتو Cisco Secure Client لىغشبت مق .ةياهنلا ةطقن لىع

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



لاصتالالاشف

لاصتالالاشف 2. ةوطخلال

يف syslog، نم دكأت، تاضوافم لشف يف 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 request

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 ERI

**Failed to find a matching policy**

عجرملا

[قدهاشلا، ةق، داصمو AAA مادختساب ASA لال IKEv2 ربع AnyConnect](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزىلچنل دن تسمل