在具有AAA & ; 证书身份验证的ASDM中配置安全客户端IKEv2/ASA

目录

简介

本文档介绍在ASA上使用带AAA和证书身份验证的ASDM配置IKEv2上的安全客户端所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎(ISE)的配置
- 思科自适应安全虚拟设备(ASAv)的配置
- 思科自适应安全设备管理器(ASDM)的配置
- VPN身份验证流程

使用的组件

本文档中的信息基于以下软件和硬件版本：

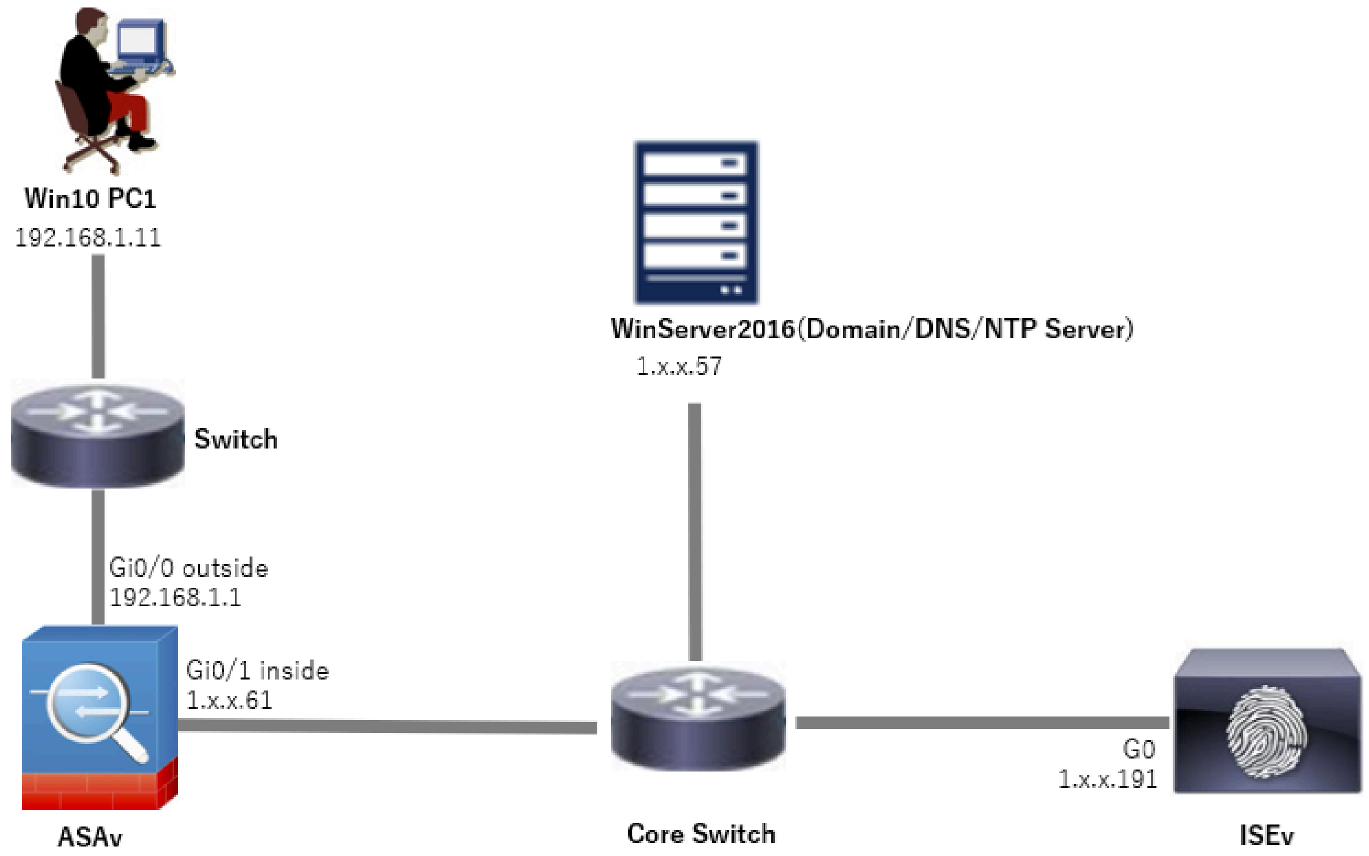
- 身份服务引擎虚拟3.3补丁1
- 自适应安全虚拟设备9.20(2)21
- 自适应安全设备管理器7.20(2)
- 思科安全客户端5.1.3.62
- Windows Server 2016
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图

下图显示本文档示例中使用的拓扑。

在Windows Server 2016上配置的域名是ad.rem-system.com，本文档中将其用作示例。



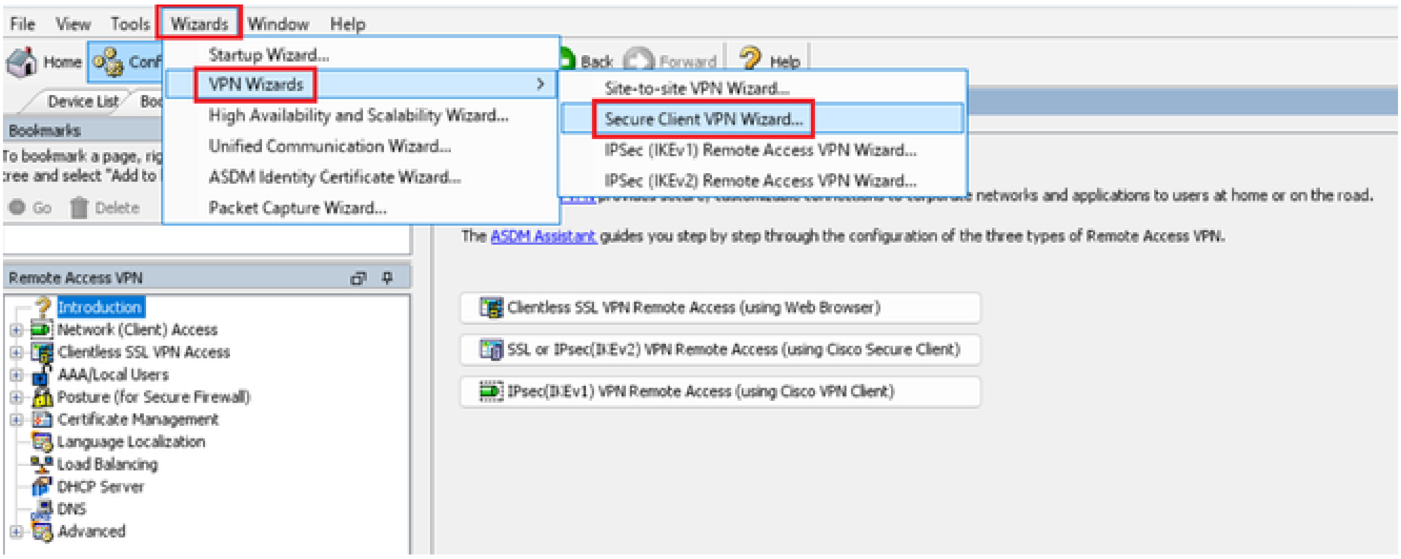
网络图

配置

ASDM中的配置

步骤1:打开VPN向导

导航到Wizards > VPN Wizards，单击Secure Client VPN Wizard。


File
View
Tools
Wizards
Window
Help
Home
Conf
Back
Forward
Help
Device List
Bookmarks
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
ASDM Identity Certificate Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
Secure Client VPN Wizard...
IPSec (IKEv1) Remote Access VPN Wizard...
IPSec (IKEv2) Remote Access VPN Wizard...
Go
Delete
Remote Access VPN
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Posture (for Secure Firewall)
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Clientless SSL VPN Remote Access (using Web Browser)
SSL or IPsec(IKEv2) VPN Remote Access (using Cisco Secure Client)
IPsec(IKEv1) VPN Remote Access (using Cisco VPN Client)

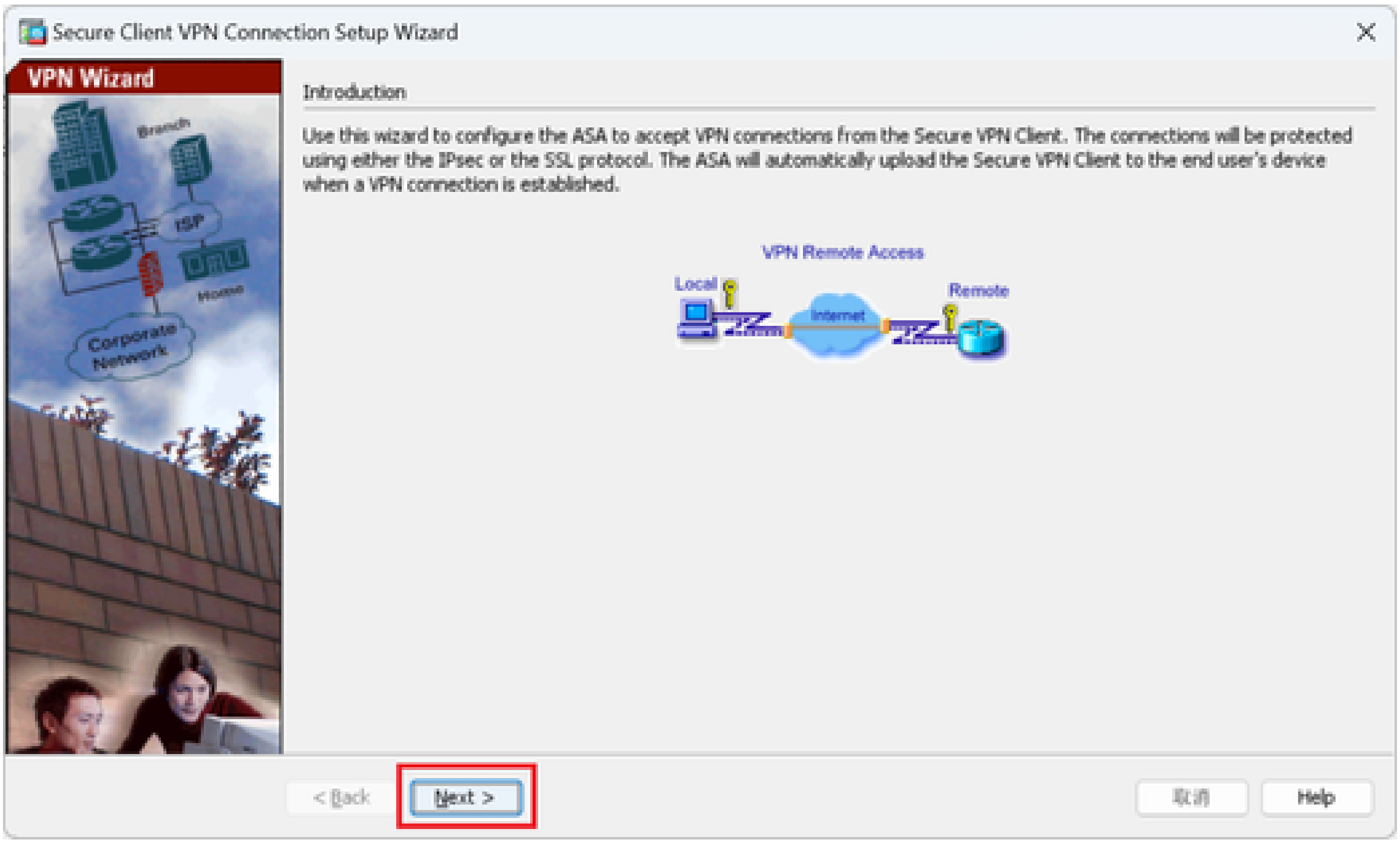
To bookmark a page, rig... tree and select "Add to...

...networks and applications to users at home or on the road.

The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.

打开VPN向导

单击 Next。


Secure Client VPN Connection Setup Wizard

VPN Wizard

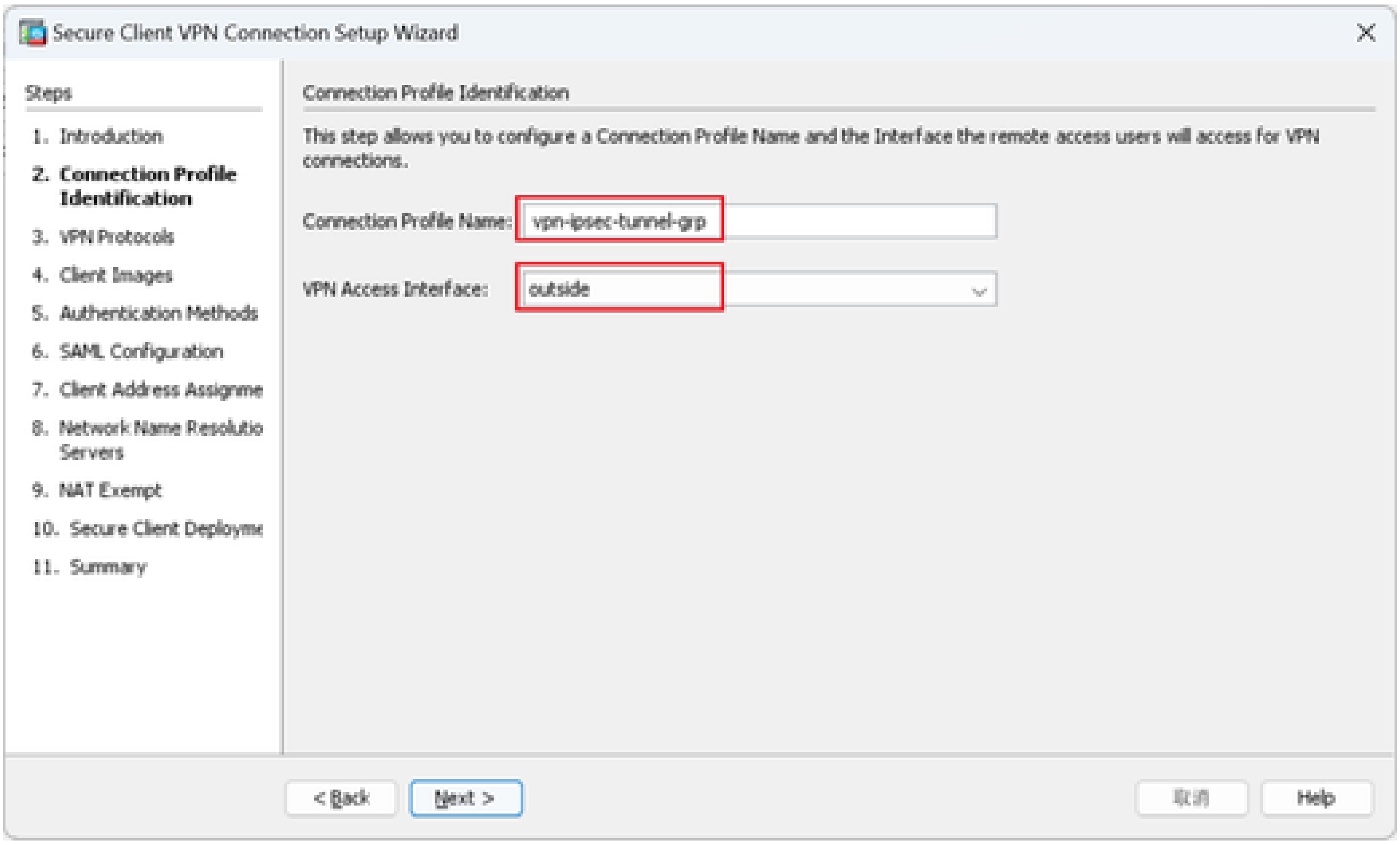
Introduction

Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device when a VPN connection is established.

单击“下一步”按钮

第二步：连接配置文件标识

输入连接配置文件的信息。
连接配置文件名称：vpn-ipsec-tunnel-grp
VPN访问接口：outside



Secure Client VPN Connection Setup Wizard

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: vpn-ipsec-tunnel-grp

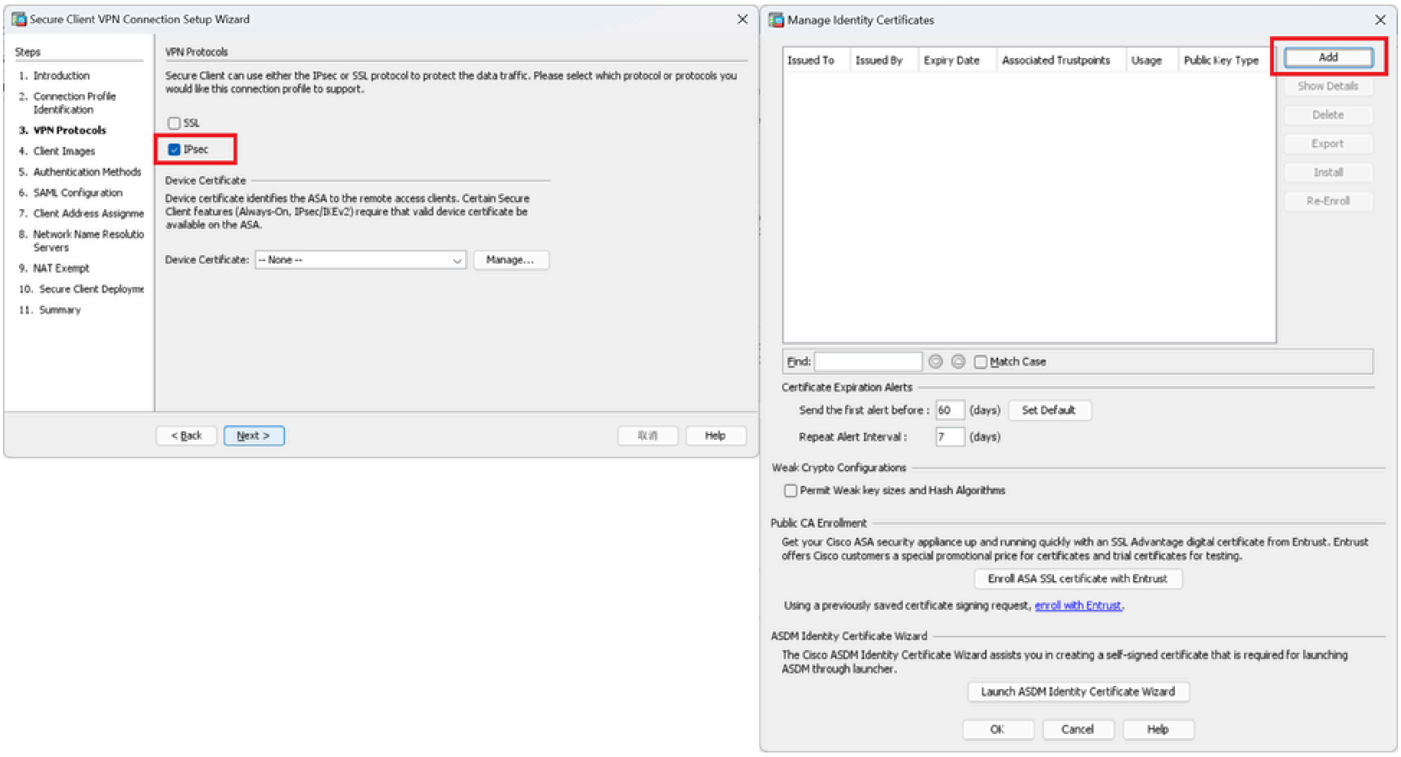
VPN Access Interface: outside

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
< Back
Next >
取消
Help

连接配置文件标识

第三步：VPN协议

选择IPsec，单击Add按钮以添加新的自签名证书。



Secure Client VPN Connection Setup Wizard

VPN Protocols

Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☐ SSL

☑ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: -- None --

Manage Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Find: ☐ Match Case

Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

Weak Crypto Configurations

☐ Permit Weak key sizes and Hash Algorithms

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

ASDM Identity Certificate Wizard

The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

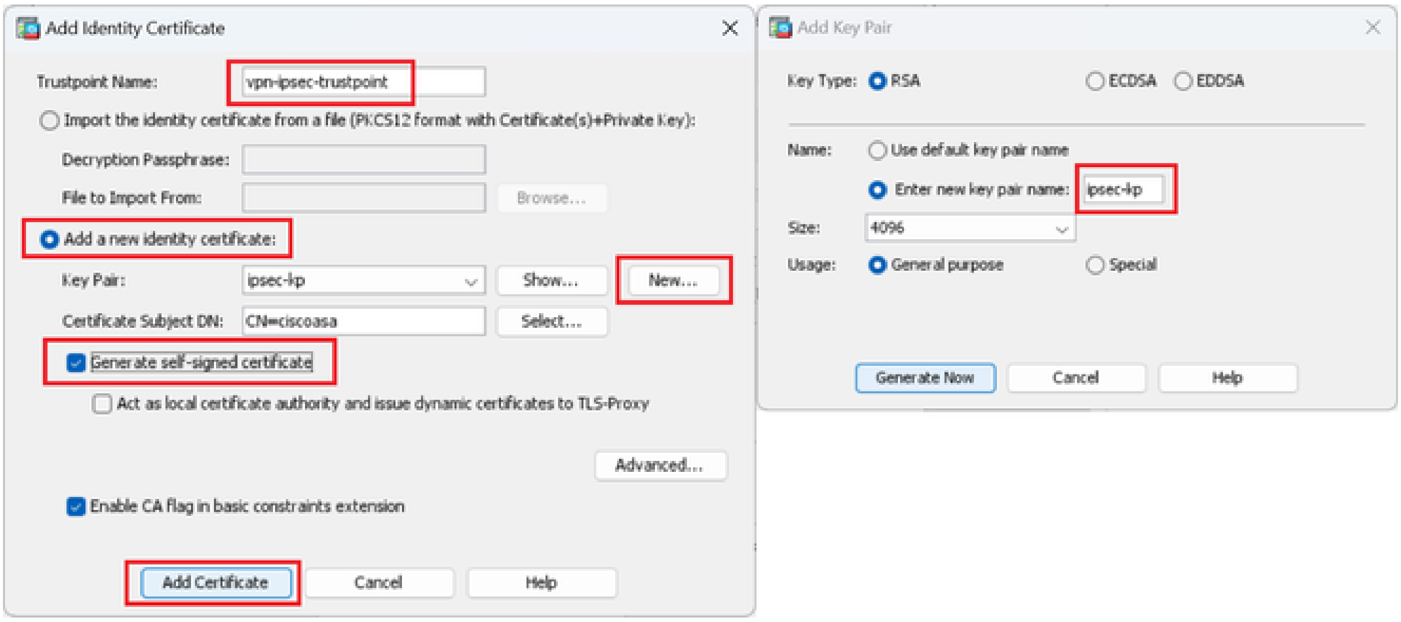
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
Manage...
< Back
Next >
取消
Help
Add
Show Details
Delete
Export
Install
Re-Enroll
Set Default
Enroll ASA SSL certificate with Entrust
Launch ASDM Identity Certificate Wizard
OK
Cancel
Help

VPN协议

输入自签名证书的信息。

信任点名称：vpn-ipsec-trustpoint

密钥对：ipsec-kp



Add Identity Certificate

Trustpoint Name: vpn-ipsec-trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: ipsec-kp

Certificate Subject DN: CN=ciscoasa

☑ Generate self-signed certificate

☐ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

☑ Enable CA flag in basic constraints extension

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

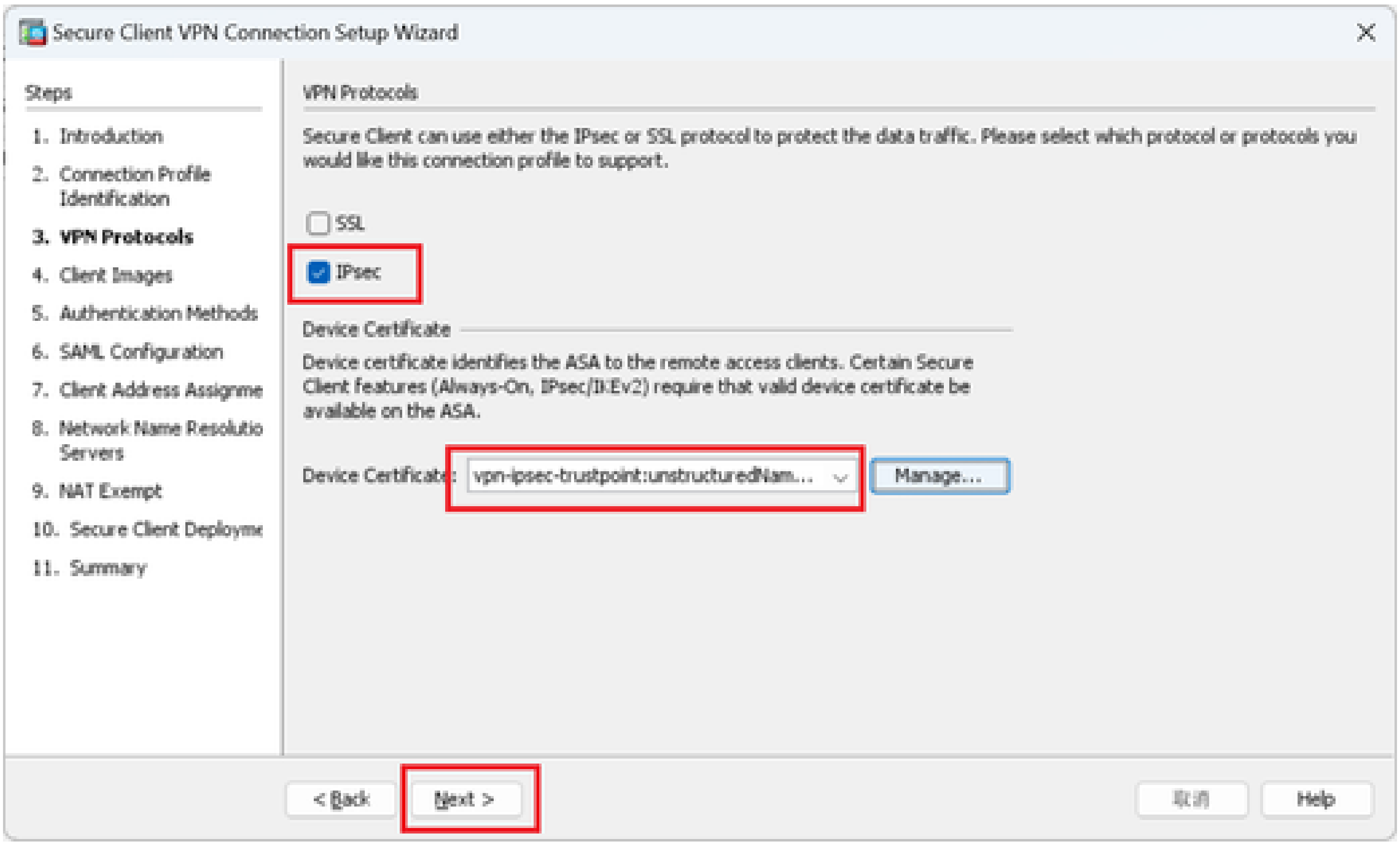
● Enter new key pair name: ipsec-kp

Size: 4096

Usage: ● General purpose ○ Special

自签名证书的详细信息

确认VPN协议的设置，单击Next按钮。



Secure Client VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. **VPN Protocols**
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

VPN Protocols

Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☐ SSL

☑ IPsec

Device Certificate

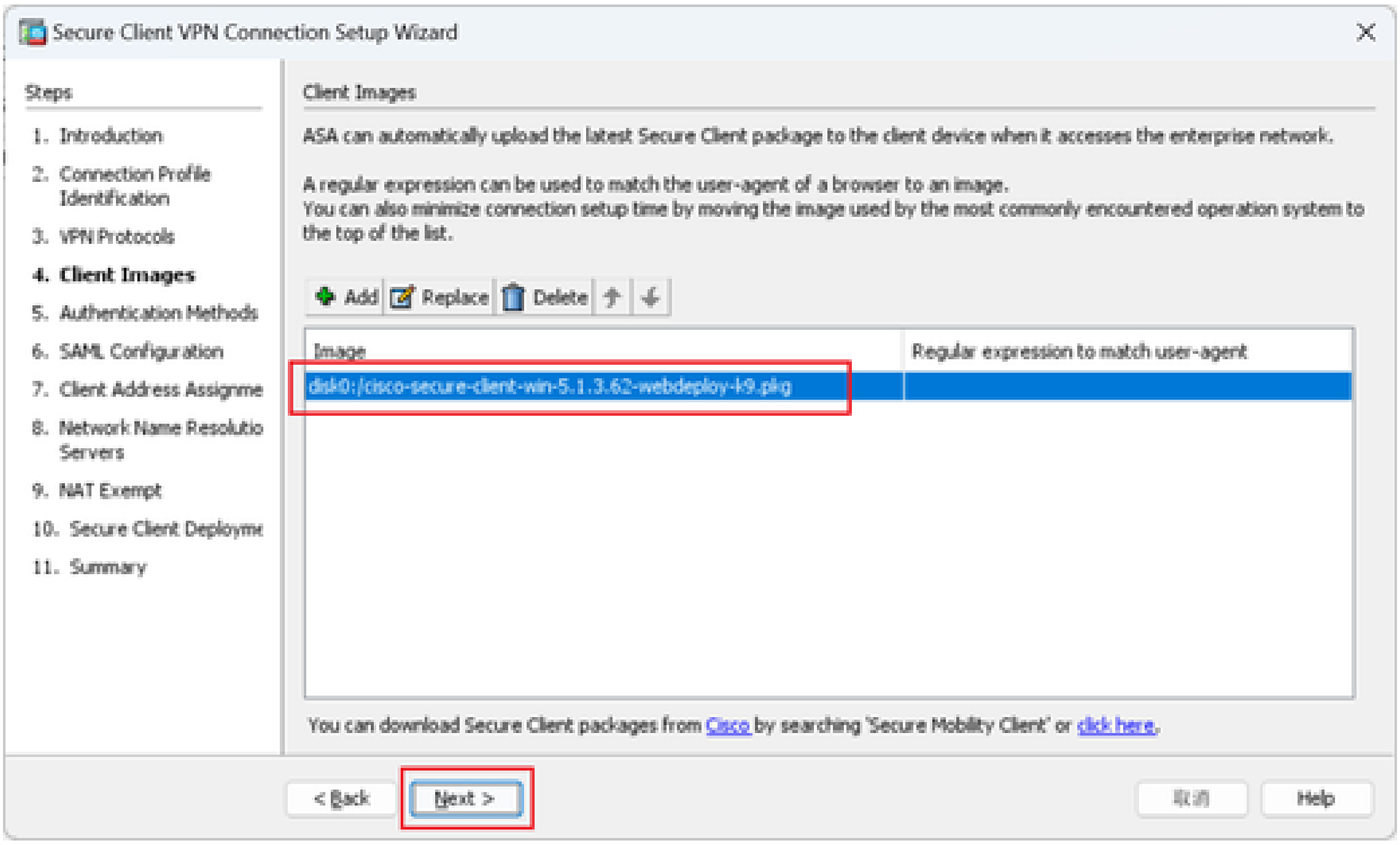
Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: vpn-ipsec-trustpoint:unstructuredNam...

确认VPN协议的设置

第四步：客户端映像

单击Add按钮添加安全客户端映像，然后单击Next按钮。



Secure Client VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. **Client Images**
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

Client Images

ASA can automatically upload the latest Secure Client package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg	

You can download Secure Client packages from Cisco by searching 'Secure Mobility Client' or click here.

客户端映像

第五步：身份验证方法

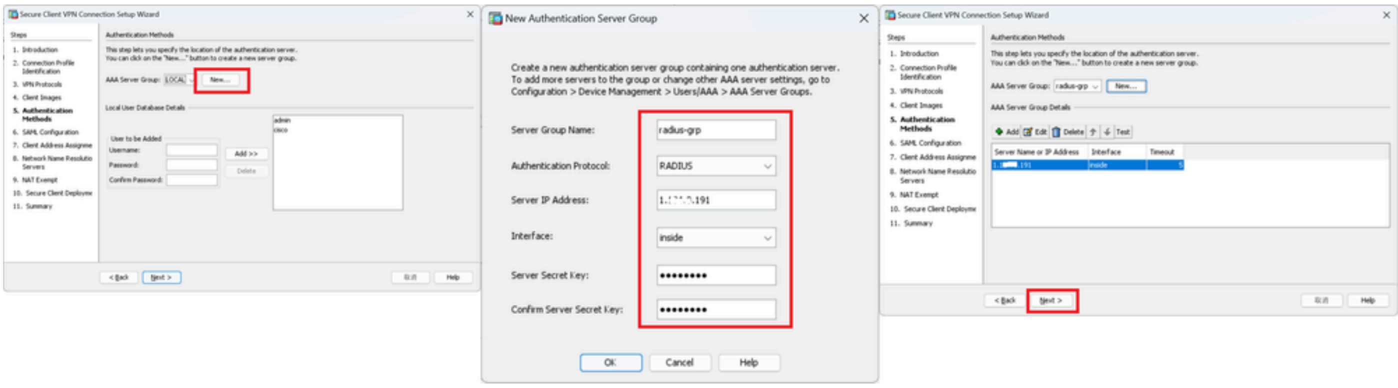
单击New按钮添加新的AAA服务器，单击Next按钮。

服务器组名称：radius-grp

身份验证协议：RADIUS

服务器IP地址：1.x.x.191

接口：内部



Secure Client VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. **Authentication Methods**
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: LOCAL

Local User Database Details

User to be Added

Username:

Password:

Confirm Password:

admin
cisco

New Authentication Server Group

Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: radius-grp

Authentication Protocol: RADIUS

Server IP Address: 1.[redacted].191

Interface: inside

Server Secret Key: ●●●●●●●●●

Confirm Server Secret Key: ●●●●●●●●●

Secure Client VPN Connection Setup Wizard

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: radius-grp

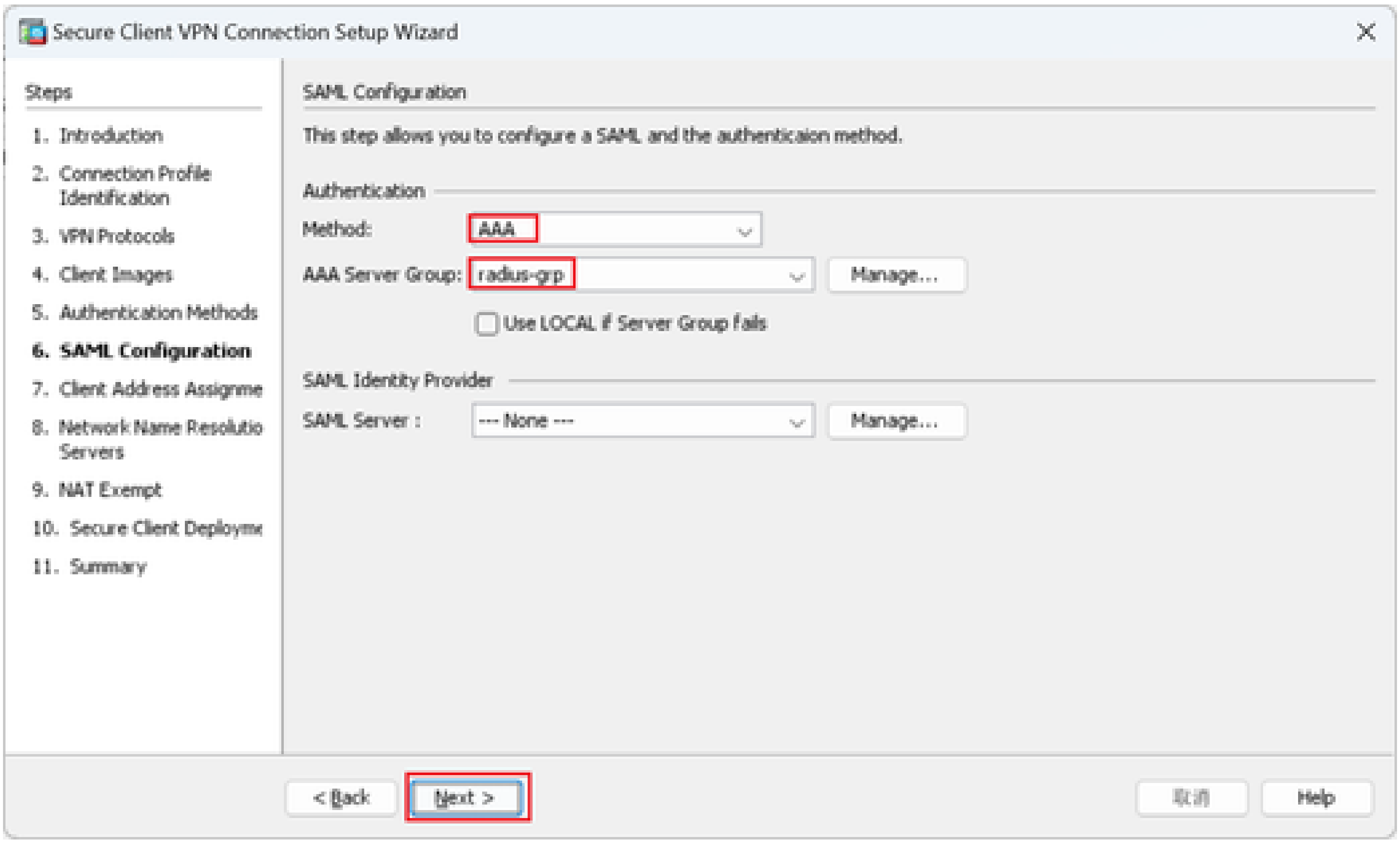
AAA Server Group Details

Server Name or IP Address	Interface	Timeout
1.[redacted].191	inside	5

身份验证方法

第六步：SAML配置

单击Next按钮。



Secure Client VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. **SAML Configuration**
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

SAML Configuration

This step allows you to configure a SAML and the authenticaion method.

Authentication

Method: AAA

AAA Server Group: radius-grp

□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

SAML配置

步骤 7.客户端地址分配

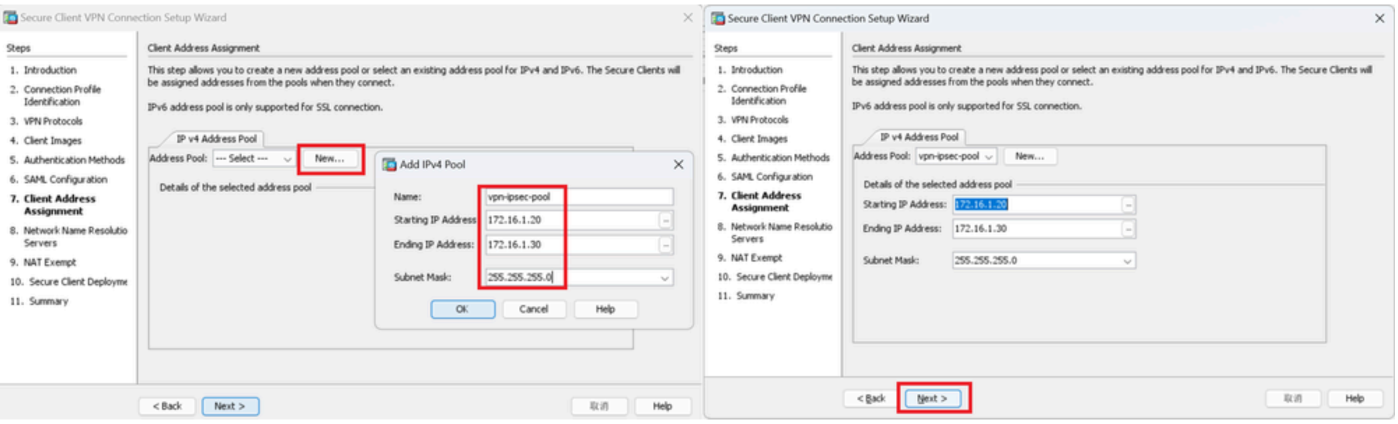
单击New按钮以添加新的IPv4池，然后单击Next按钮。

名称：vpn-ipsec-pool

起始IP地址：172.16.1.20

结束IP地址：172.16.1.30

子网掩码：255.255.255.0



Secure Client VPN Connection Setup Wizard

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignment
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

IP v4 Address Pool

Address Pool: --- Select ---

Details of the selected address pool

Add IPv4 Pool

Name: vpn-ipsec-pool

Starting IP Address: 172.16.1.20

Ending IP Address: 172.16.1.30

Subnet Mask: 255.255.255.0

Secure Client VPN Connection Setup Wizard

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

IP v4 Address Pool

Address Pool: vpn-ipsec-pool

Details of the selected address pool

Starting IP Address: 172.16.1.20

Ending IP Address: 172.16.1.30

Subnet Mask: 255.255.255.0

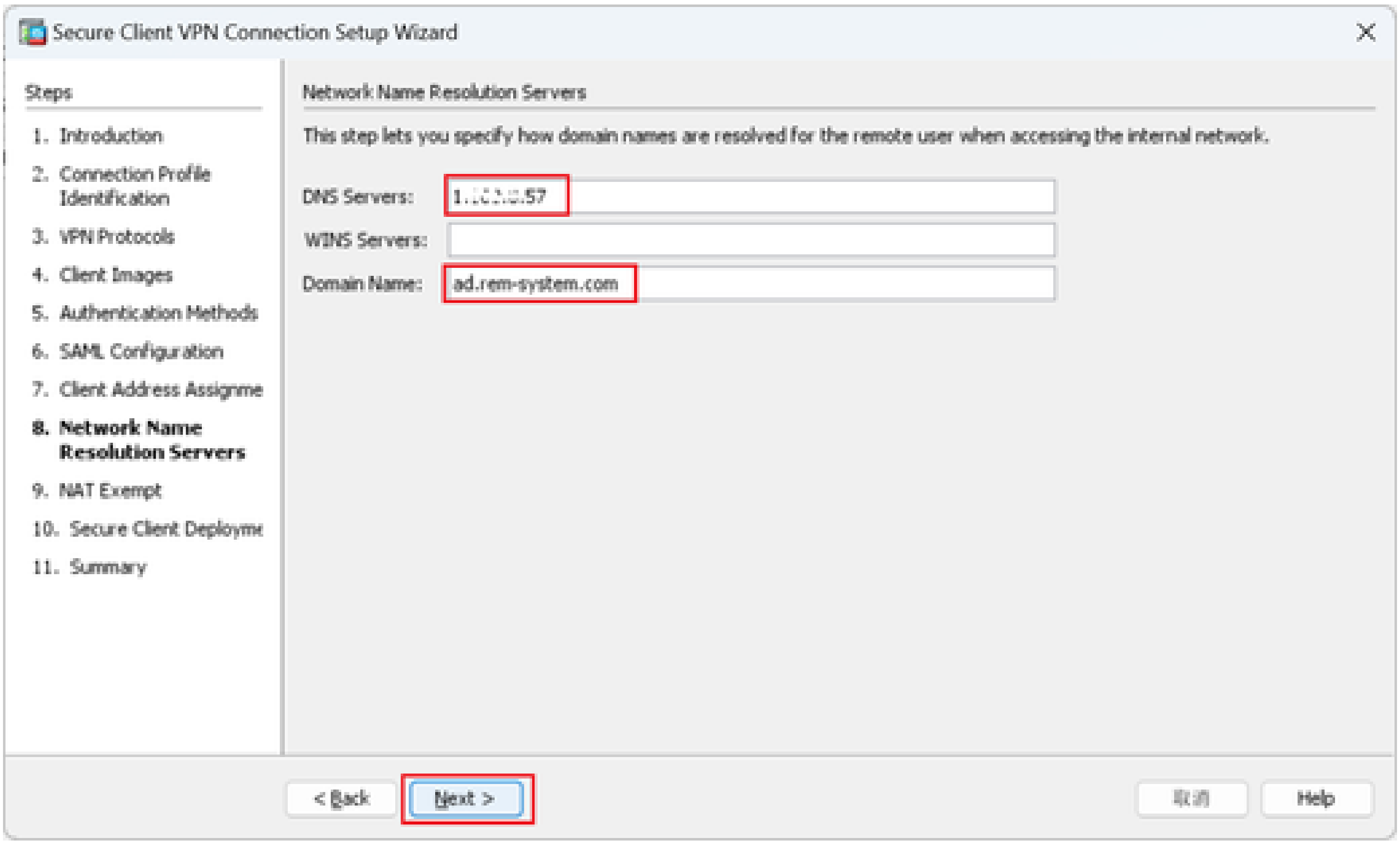
客户端地址分配

步骤 8网络名称解析服务器

输入DNS和域的信息，单击Next按钮。

DNS服务器：1.x.x.57

域名：ad.rem-system.com



Secure Client VPN Connection Setup Wizard

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolution Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 1.[redacted].57

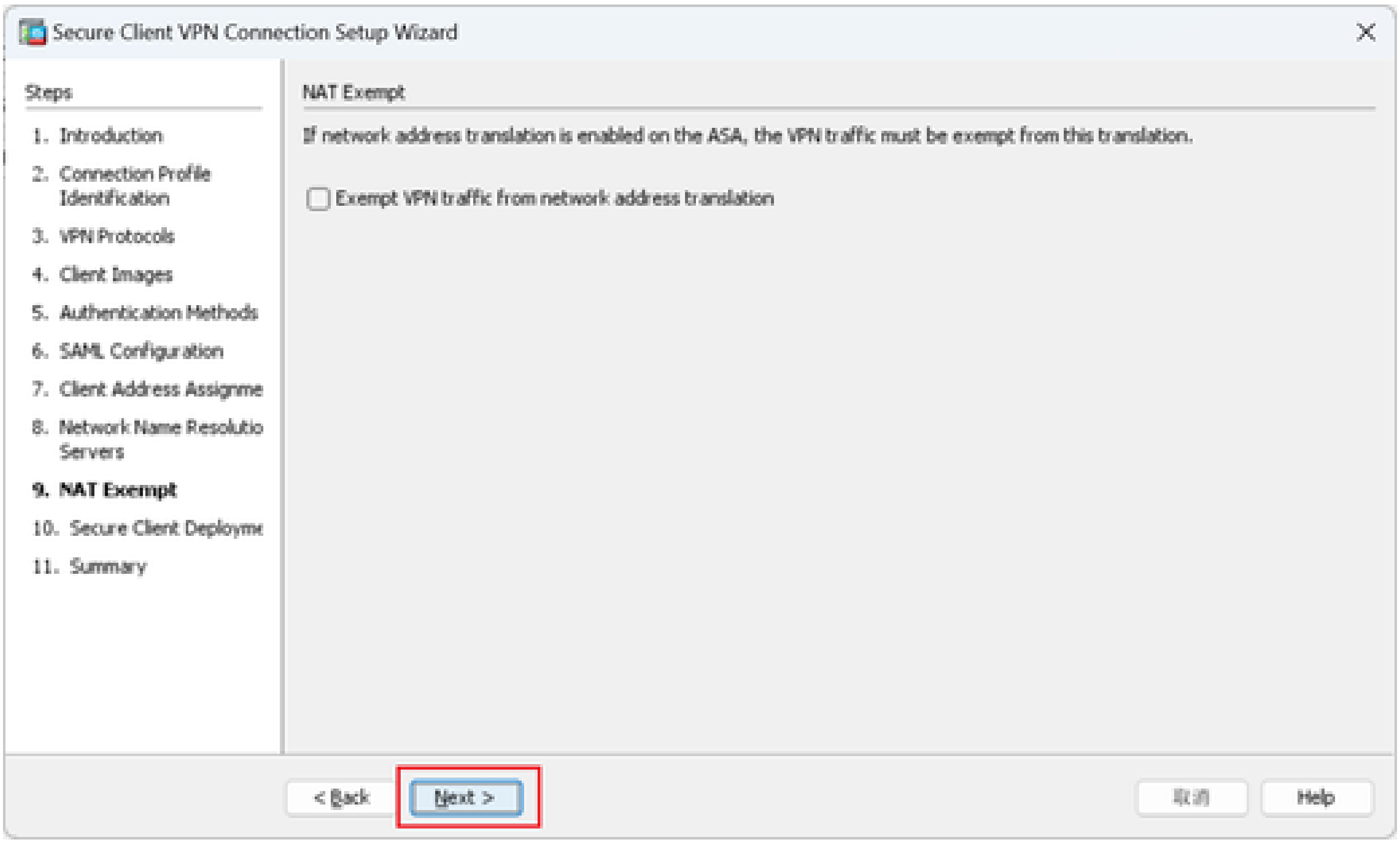
WINS Servers:

Domain Name: ad.rem-system.com

网络名称解析服务器

步骤 9NAT免除

单击Next按钮。


Secure Client VPN Connection Setup Wizard

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

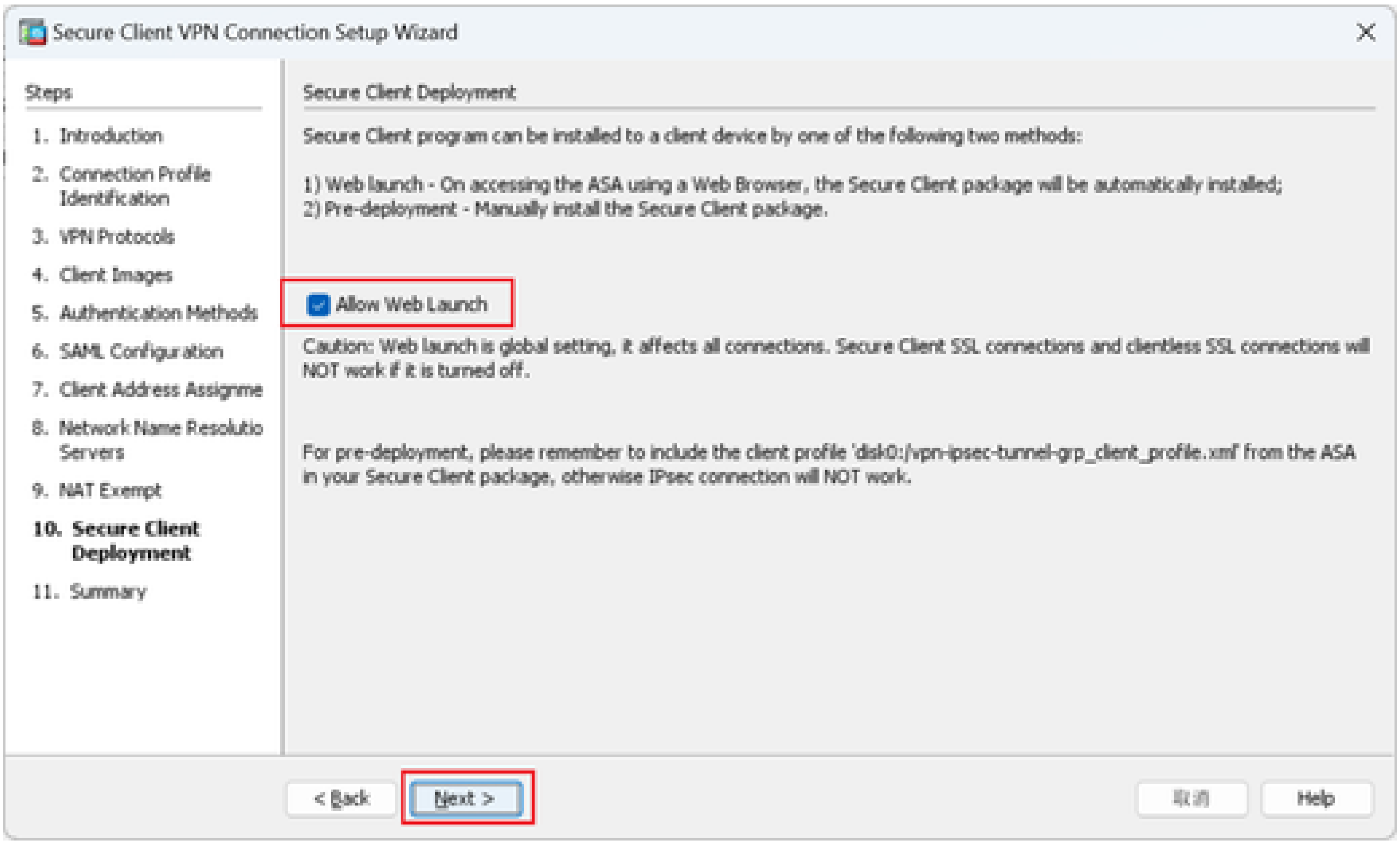
□ Exempt VPN traffic from network address translation

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployme
11. Summary
< Back
Next >
取消
Help

NAT免除

步骤 10安全客户端部署

选择允许Web启动，然后单击“下一步”按钮。


Secure Client VPN Connection Setup Wizard

Secure Client Deployment

Secure Client program can be installed to a client device by one of the following two methods:

1) Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed;
2) Pre-deployment - Manually install the Secure Client package.

☑ Allow Web Launch

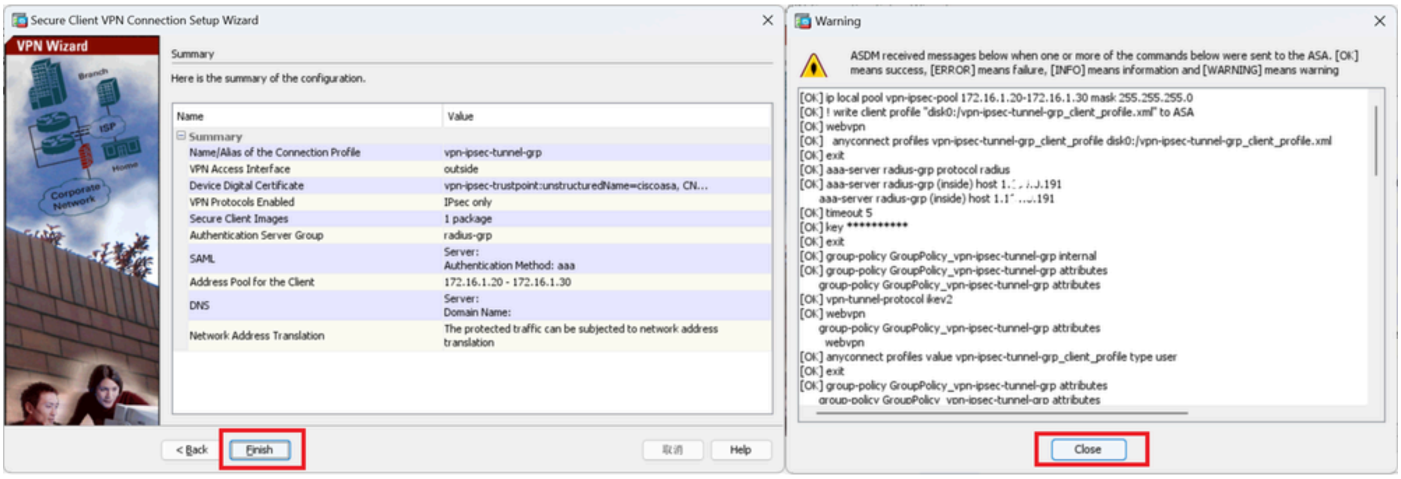
Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will NOT work if it is turned off.

For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA in your Secure Client package, otherwise IPsec connection will NOT work.

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignme
8. Network Name Resolutio Servers
9. NAT Exempt
10. Secure Client Deployment
11. Summary
< Back
Next >
取消
Help

步骤 11保存设置

单击Finish按钮并保存设置。



Secure Client VPN Connection Setup Wizard

Summary

Here is the summary of the configuration.

Name	Value
⊟ Summary	
Name/Alias of the Connection Profile	vpn-ipsec-tunnel-grp
VPN Access Interface	outside
Device Digital Certificate	vpn-ipsec-trustpoint:unstructuredName=ciscoasa, CN...
VPN Protocols Enabled	IPsec only
Secure Client Images	1 package
Authentication Server Group	radius-grp
SAML	Server: Authentication Method: aaa
Address Pool for the Client	172.16.1.20 - 172.16.1.30
DNS	Server: Domain Name:
Network Address Translation	The protected traffic can be subjected to network address translation

Warning

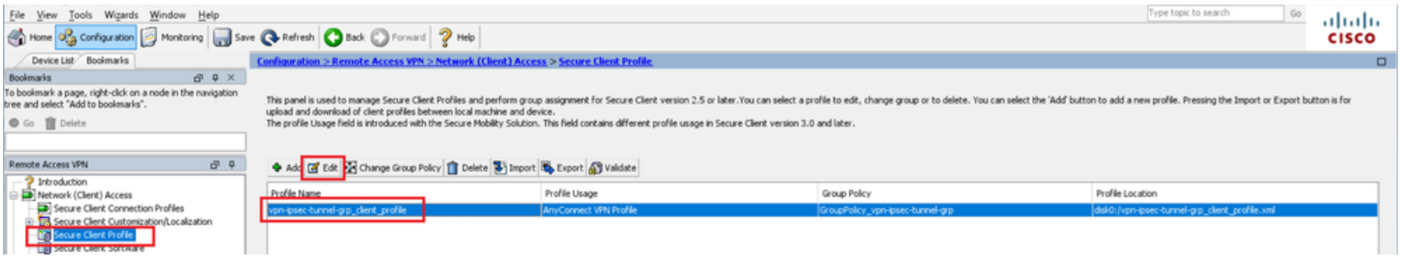
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[OK] ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0
[OK] ! write client profile "disk0:/vpn-ipsec-tunnel-grp_client_profile.xml" to ASA
[OK] webvpn
[OK]   anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
[OK] exit
[OK] aaa-server radius-grp protocol radius
[OK] aaa-server radius-grp (inside) host 1.[redacted].191
   aaa-server radius-grp (inside) host 1.1[redacted].191
[OK] timeout 5
[OK] key **********
[OK] exit
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
   group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
[OK] vpn-tunnel-protocol ikev2
[OK] webvpn
   group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
    webvpn
[OK] anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user
[OK] exit
[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
   group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes
```

保存设置

步骤 12确认并导出安全客户端配置文件

导航到Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile，单击Edit按钮。



Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

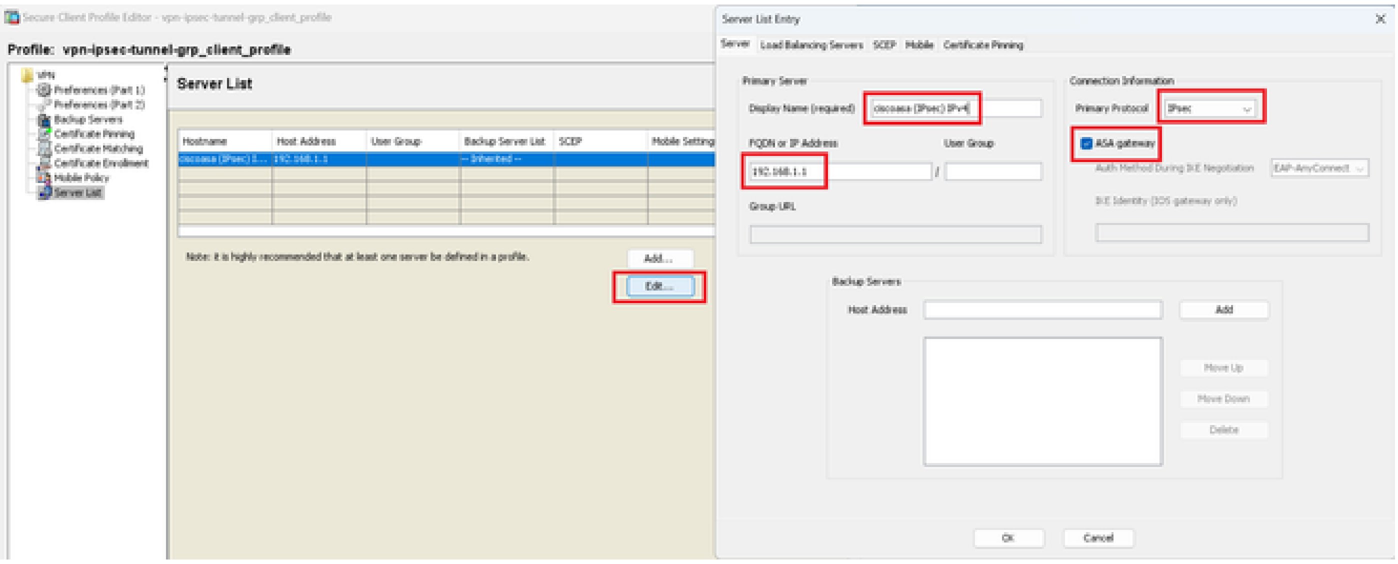
This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Client version 3.0 and later.

Profile Name	Profile Usage	Group Policy	Profile Location
vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml

编辑安全客户端配置文件

确认配置文件的详细信息。

- 显示名称（必填）：ciscoasa (IPsec) IPv4
- FQDN或IP地址：192.168.1.1
- 主协议：IPsec



Secure Client Profile Editor - vpn-ipsec-tunnel-grp_client_profile

Profile: vpn-ipsec-tunnel-grp_client_profile

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Setting
ciscoasa (IPsec) I...	192.168.1.1		-- Inherited --		

Note: it is highly recommended that at least one server be defined in a profile.

Server List Entry

Primary Server — Display Name (required): ciscoasa (IPsec) IPv4

FQDN or IP Address: 192.168.1.1

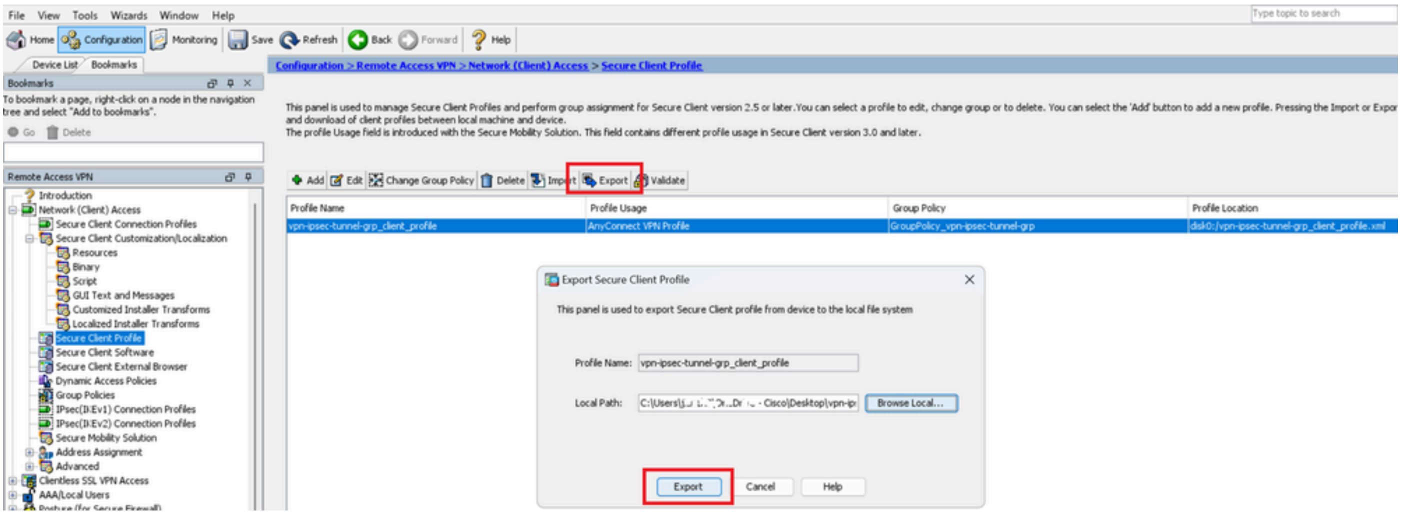
Connection Information — Primary Protocol: IPsec

☑ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

确认安全客户端配置文件

单击Export按钮将配置文件导出到本地PC。



Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Expor and download of client profiles between local machine and device.

The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Client version 3.0 and later.

Profile Name	Profile Usage	Group Policy	Profile Location
vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml

Export Secure Client Profile

This panel is used to export Secure Client profile from device to the local file system

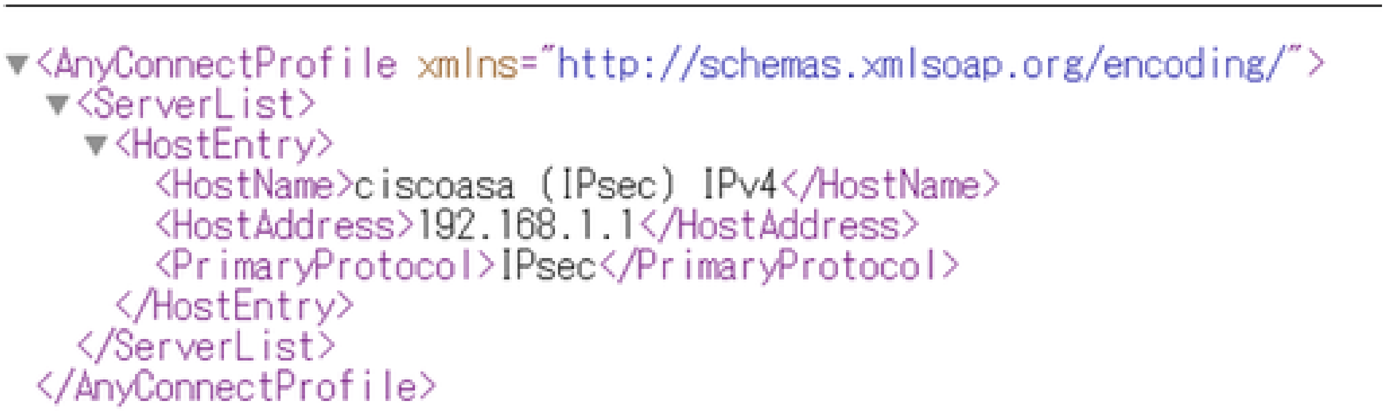
Profile Name: vpn-ipsec-tunnel-grp_client_profile

Local Path: C:\Users\[illegible] - Cisco\Desktop\vpn-ip

导出安全客户端配置文件

步骤 13确认安全客户端配置文件的详细信息

通过浏览器打开“安全客户端配置文件”，确认主机的主要协议为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>
```

步骤 14确认ASA CLI中的设置

确认ASDM在ASA CLI中创建的IPsec设置。

```
// 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
```

步骤 15添加加密算法

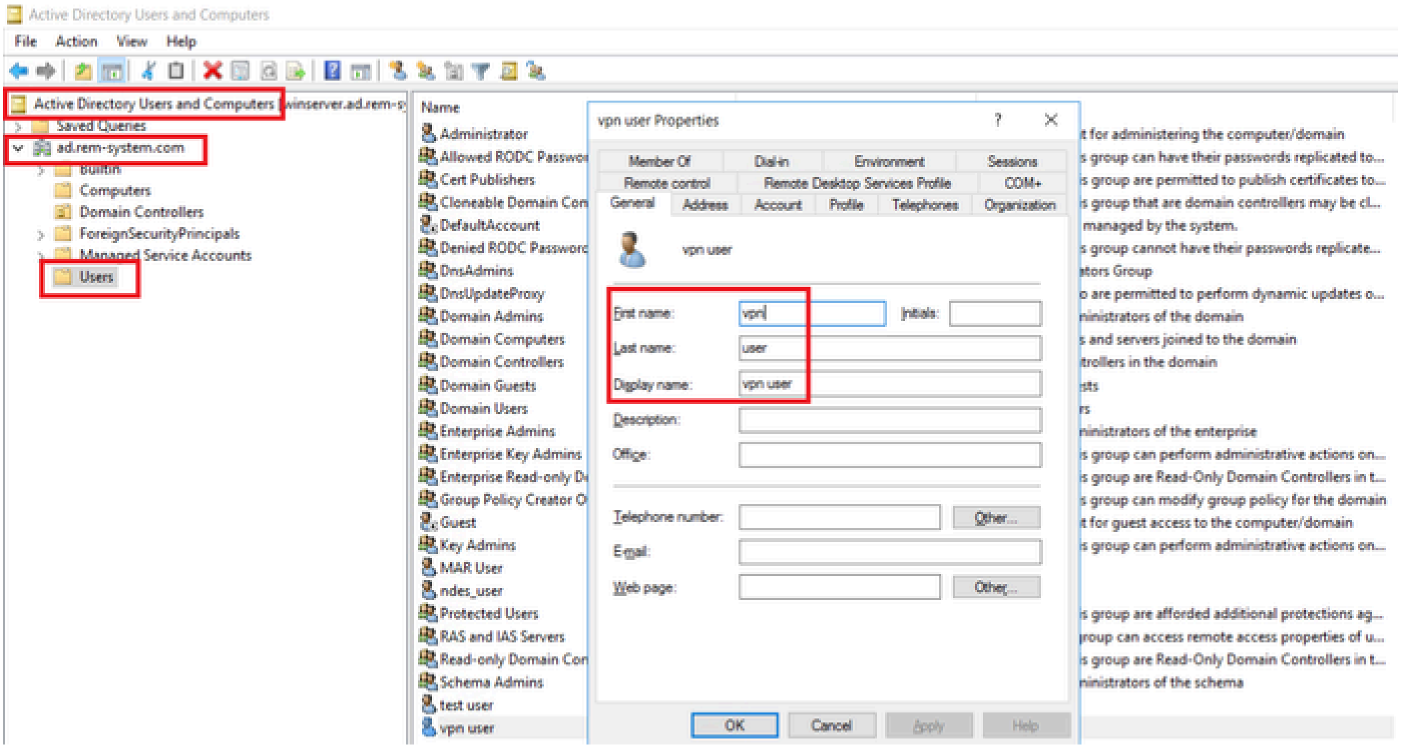
在ASA CLI中，将组19添加到IKEv2 Policy。

注意：对于IKEv2/IPsec连接，自版本4.9.00086起，思科安全客户端不再支持Diffie-Hellman (DH)组2、5、14和24。此更改可能会导致由于加密算法不匹配而导致连接失败。

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

Windows Server中的配置

您需要为VPN连接添加域用户。 导航到Active Directory用户和计算机，然后单击用户。将vpnuser添加为域用户。



Active Directory Users and Computers

- Active Directory Users and Computers [winserver.ad.rem-s
  - Saved Queries
  - ad.rem-system.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users

Name

- Administrator
- Allowed RODC Passwo
- Cert Publishers
- Cloneable Domain Con
- DefaultAccount
- Denied RODC Passwor
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Key Admins
- Enterprise Read-only D
- Group Policy Creator O
- Guest
- Key Admins
- MAR User
- ndes_user
- Protected Users
- RAS and IAS Servers
- Read-only Domain Con
- Schema Admins
- test user
- vpn user

vpn user Properties

vpn user

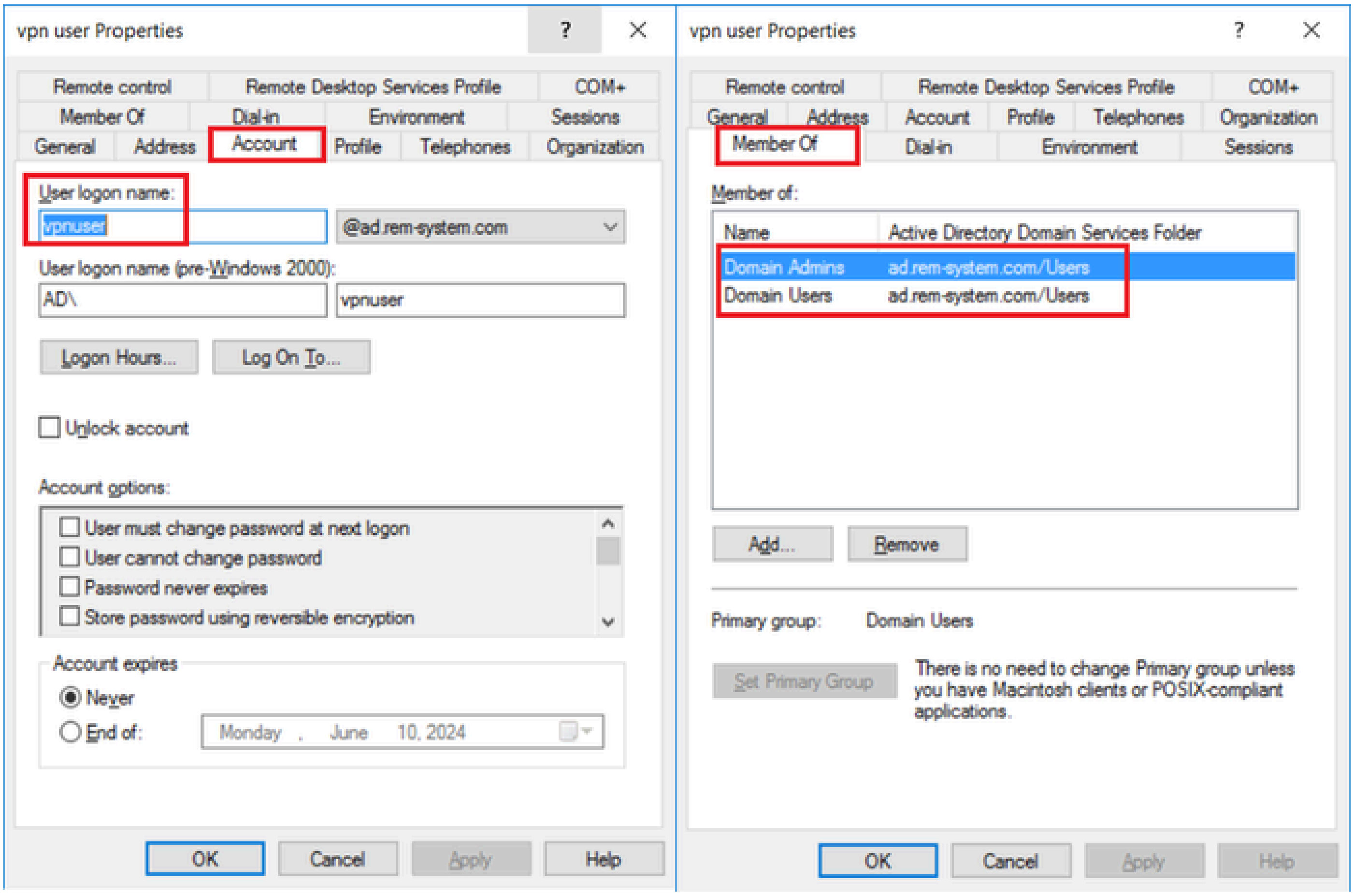
First name: vpn

Last name: user

Display name: vpn user

添加域用户

将域用户添加到域管理员和域用户的成员。



vpn user Properties

User logon name: vpnuser @ad.rem-system.com

User logon name (pre-Windows 2000): AD\ vpnuser

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Monday , June 10, 2024

vpn user Properties

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-system.com/Users
Domain Users	ad.rem-system.com/Users

Primary group: Domain Users

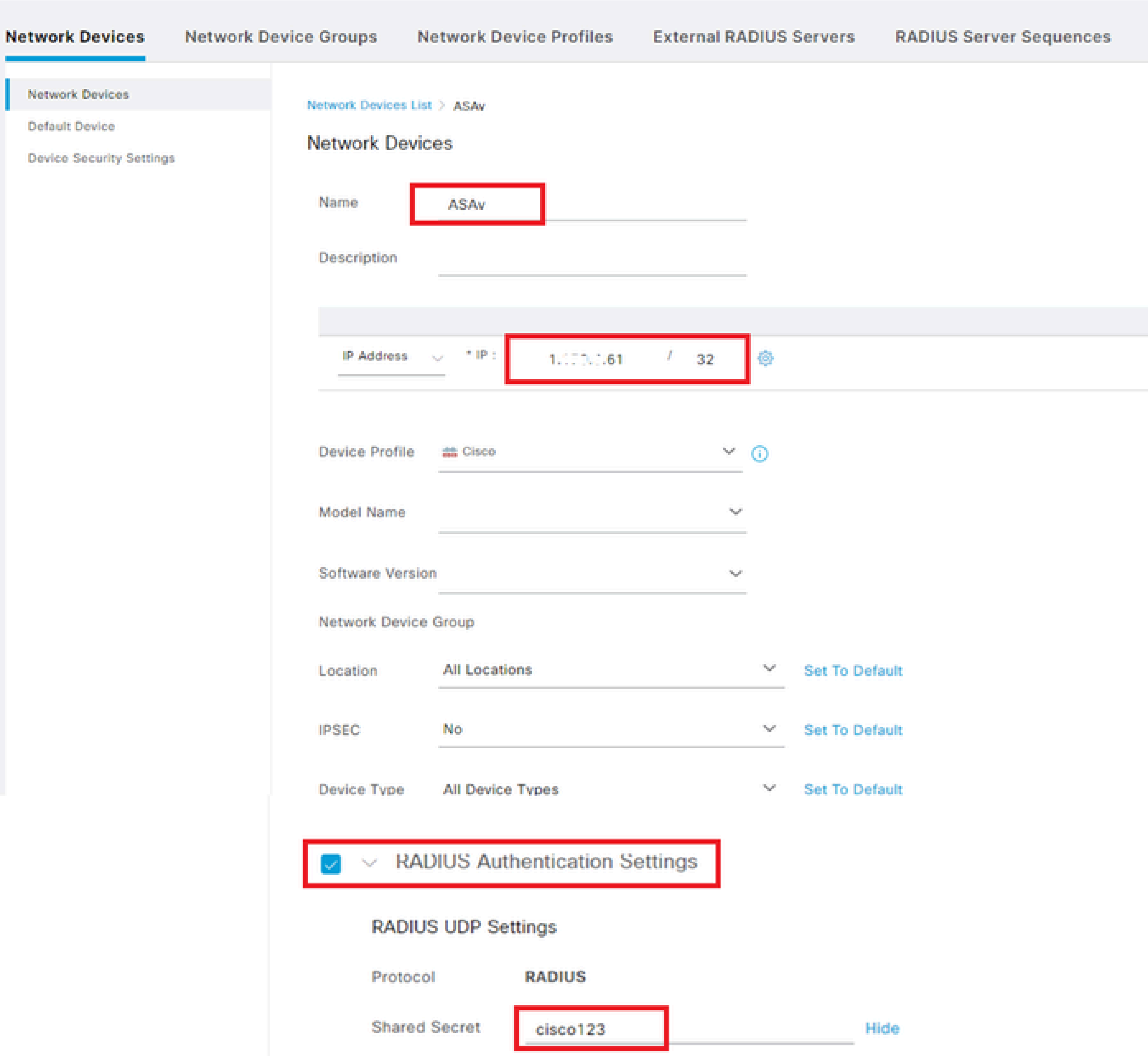
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

域管理员和域用户

ISE中的配置

步骤1:添加设备

导航到管理>网络设备，点击添加按钮以添加ASAv设备。



Network Devices

Name: ASAv

Description:

IP Address * IP : 1.[redacted].61 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

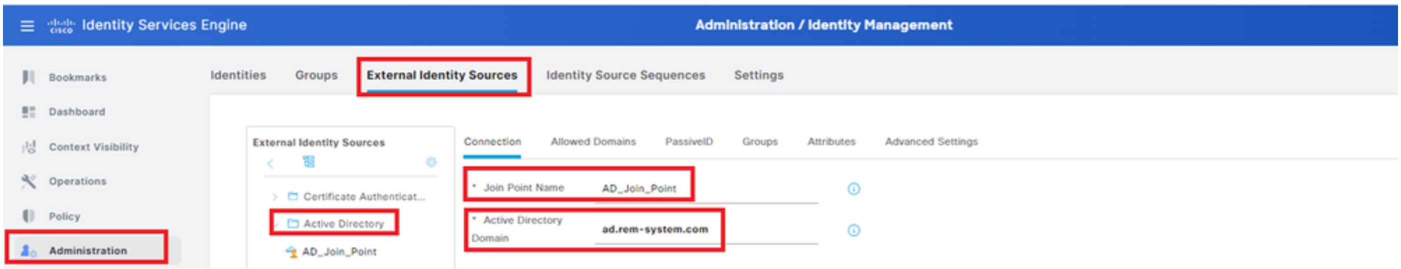
Shared Secret: cisco123

添加设备

第二步：添加Active Directory

导航到管理>外部身份源> Active Directory，点击连接选项卡，将Active Directory添加到ISE。

- 加入点名称：AD_Join_Point
- Active Directory域：ad.rem-system.com

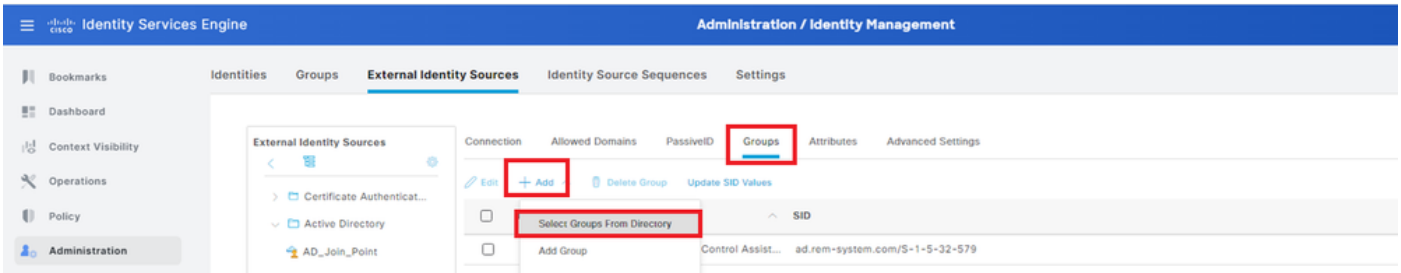


* Join Point Name: AD_Join_Point

* Active Directory Domain: ad.rem-system.com

添加Active Directory

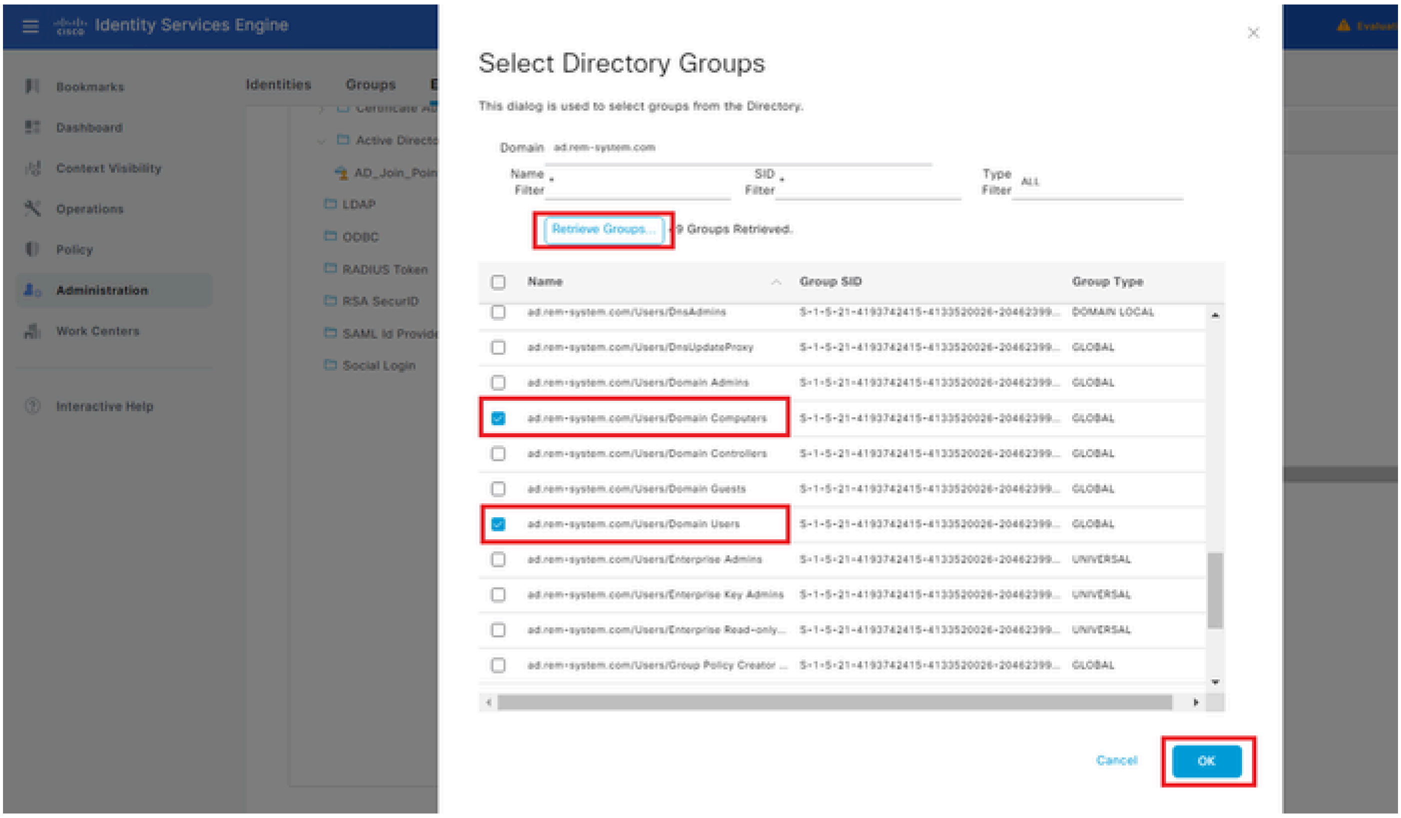
导航到组选项卡，选择从目录选择组从下拉列表。



	SID
Control Assist...	ad.rem-system.com/S-1-5-32-579

从目录选择组

单击Retrieve Groupsfrom下拉列表。Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain 用户并单击OK。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: ad.rem-system.com

Name Filter: *

SID Filter: *

Type Filter: ALL

9 Groups Retrieved.

	Name	Group SID	Group Type
☐	ad.rem-system.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-system.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-system.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-system.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-system.com/Users/Enterprise Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Enterprise Key Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Enterprise Read-only...	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-system.com/Users/Group Policy Creator ...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

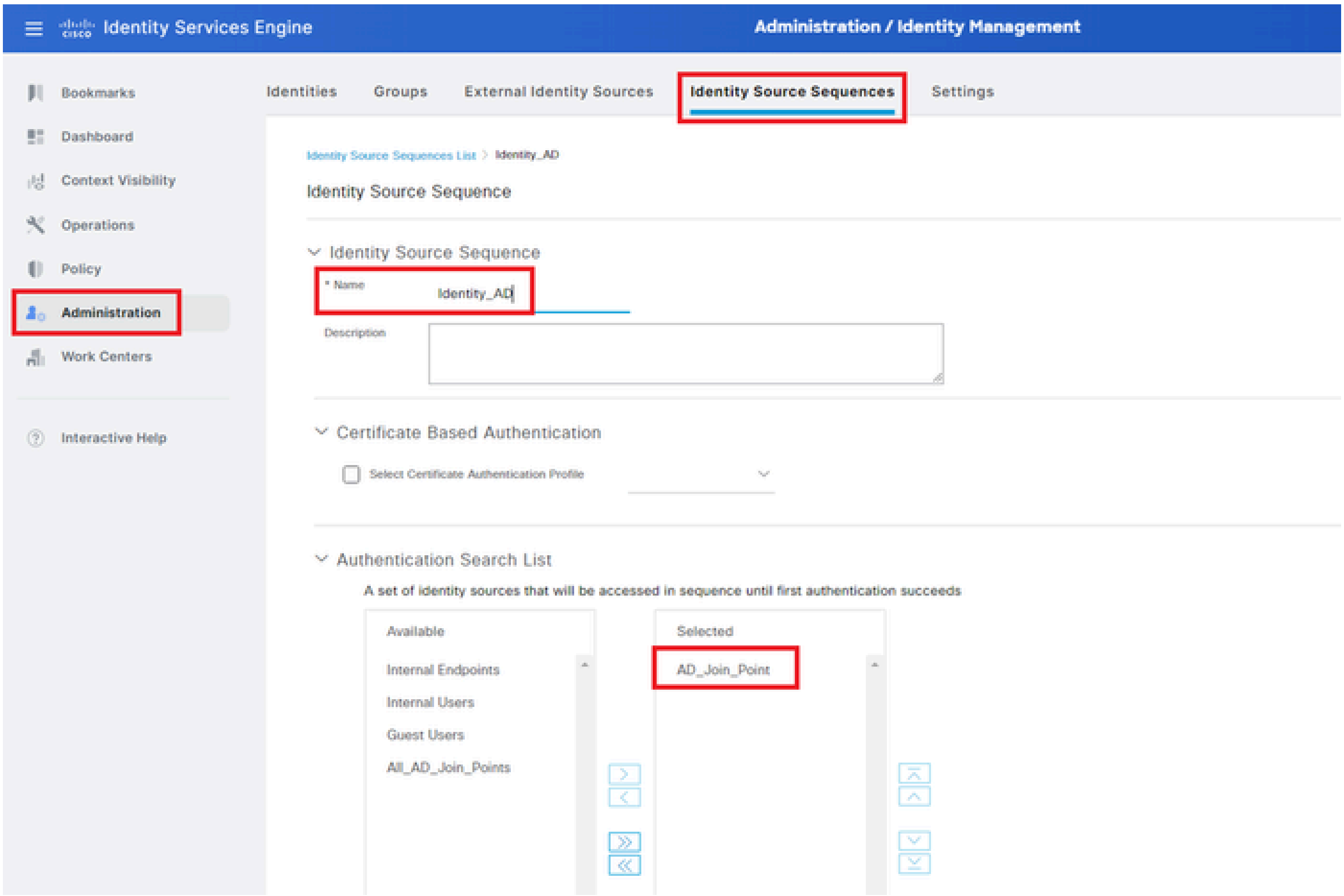
添加域计算机和用户

第三步：添加身份源隔离

导航到管理>身份源序列，添加身份源序列。

- 名称：Identity_AD

- 身份验证搜索列表：AD_Join_Point



Identity Source Sequences List > Identity_AD

Identity Source Sequence

Identity Source Sequence

* Name Identity_AD

Description

Certificate Based Authentication

□ Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

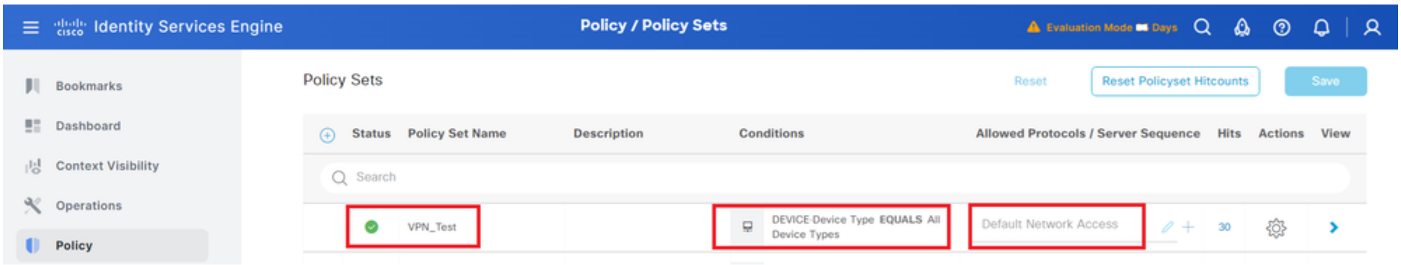
Available	Selected
Internal Endpoints	AD_Join_Point
Internal Users	
Guest Users	
All_AD_Join_Points	

添加身份源序列

第四步：添加策略集

导航到策略>策略集，点击+ 添加策略集。

- 策略集名称：VPN_Test
- 条件：设备设备类型等于所有设备类型
- 允许的协议/服务器序列：默认网络访问



Policy Sets

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

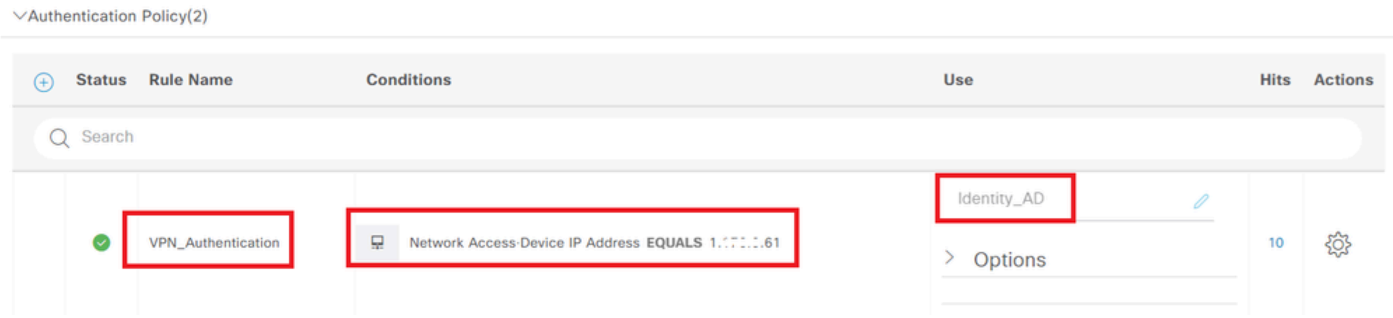
添加策略集

第五步：添加身份验证策略

导航到策略集，点击VPN_Test添加身份验证策略。

- 规则名称：VPN_Authentication

- 条件：网络接入设备IP地址等于1.x.x.61
- 使用：Identity_AD



Authentication Policy(2)

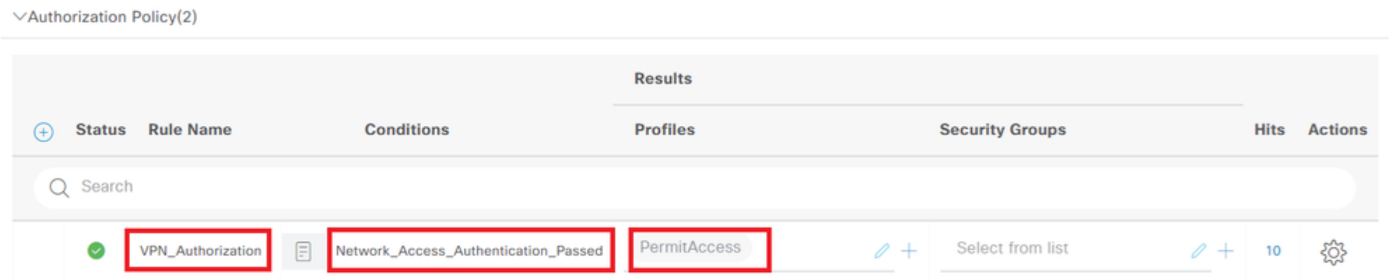
Status	Rule Name	Conditions	Use	Hits	Actions
✓	VPN_Authentication	Network Access·Device IP Address EQUALS 1.[redacted].61	Identity_AD Options	10	⚙

添加身份验证策略

第六步：添加授权策略

导航到策略集，点击VPN_Test添加授权策略。

- 规则名称：VPN_Authorization
- 条件：Network_Access_Authentication_Passed
- 结果：PermitAccess



Authorization Policy(2)

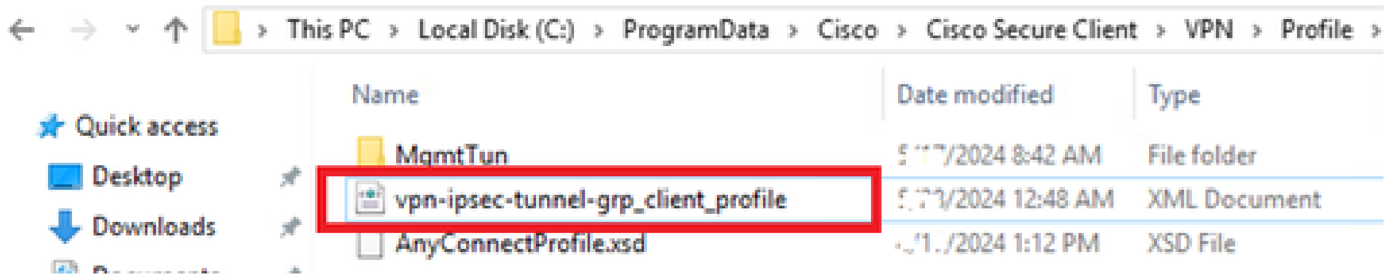
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	⚙

添加授权策略

验证

步骤1:将安全客户端配置文件复制到Win10 PC1

将安全客户端配置文件复制到C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile目录。



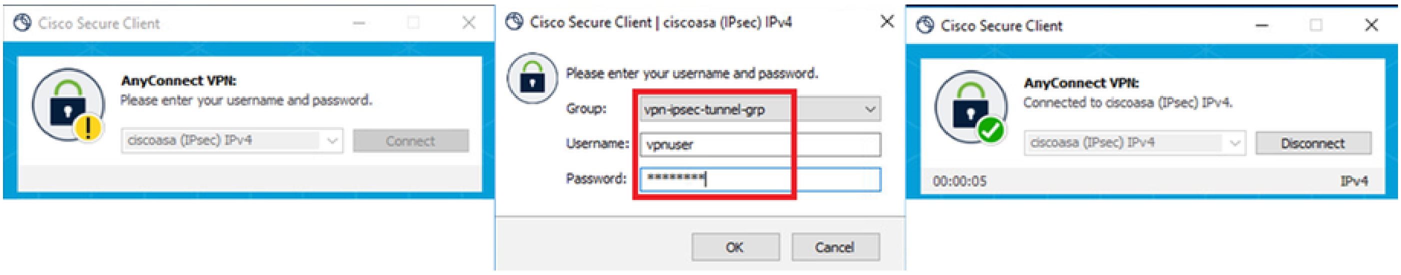
This PC › Local Disk (C:) › ProgramData › Cisco › Cisco Secure Client › VPN › Profile ›

Name	Date modified	Type
MgmtTun	[redacted]/2024 8:42 AM	File folder
vpn-ipsec-tunnel-grp_client_profile	[redacted]/2024 12:48 AM	XML Document
AnyConnectProfile.xsd	[redacted]/2024 1:12 PM	XSD File

将配置文件复制到PC

第二步：启动VPN连接

在终端上，运行Cisco Secure Client并输入用户名和密码，然后确认Cisco Secure Client连接成功。



AnyConnect VPN:
Please enter your username and password.
ciscoasa (IPsec) IPv4

Please enter your username and password.
Group: vpn-ipsec-tunnel-grp
Username: vpnuser
Password: ********

AnyConnect VPN:
Connected to ciscoasa (IPsec) IPv4.
ciscoasa (IPsec) IPv4

连接成功

第三步：确认ASA上的系统日志

在系统日志中，确认IKEv2连接成功。

<#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
```

第四步：确认ASA上的IPsec会话

运行show vpn-sessiondb detail anyconnect命令以确认ASA上的IKEv2/IPsec会话。

<#root>

ciscoasa#

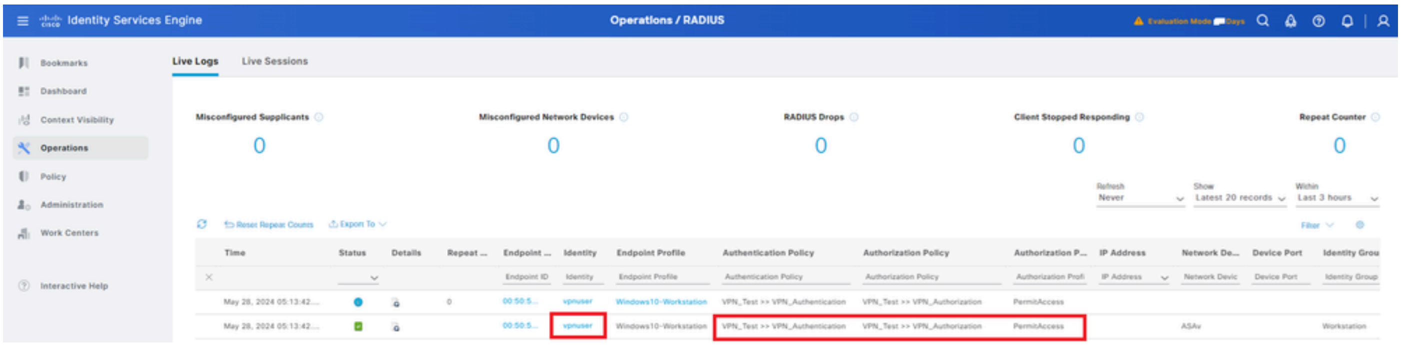
show vpn-sessiondb detail anyconnect

```
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
```

第五步：确认Radius实时日志

导航到操作> RADIUS >实时日志 ISE GUI中，确认vpn身份验证的实时日志。



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh: Never

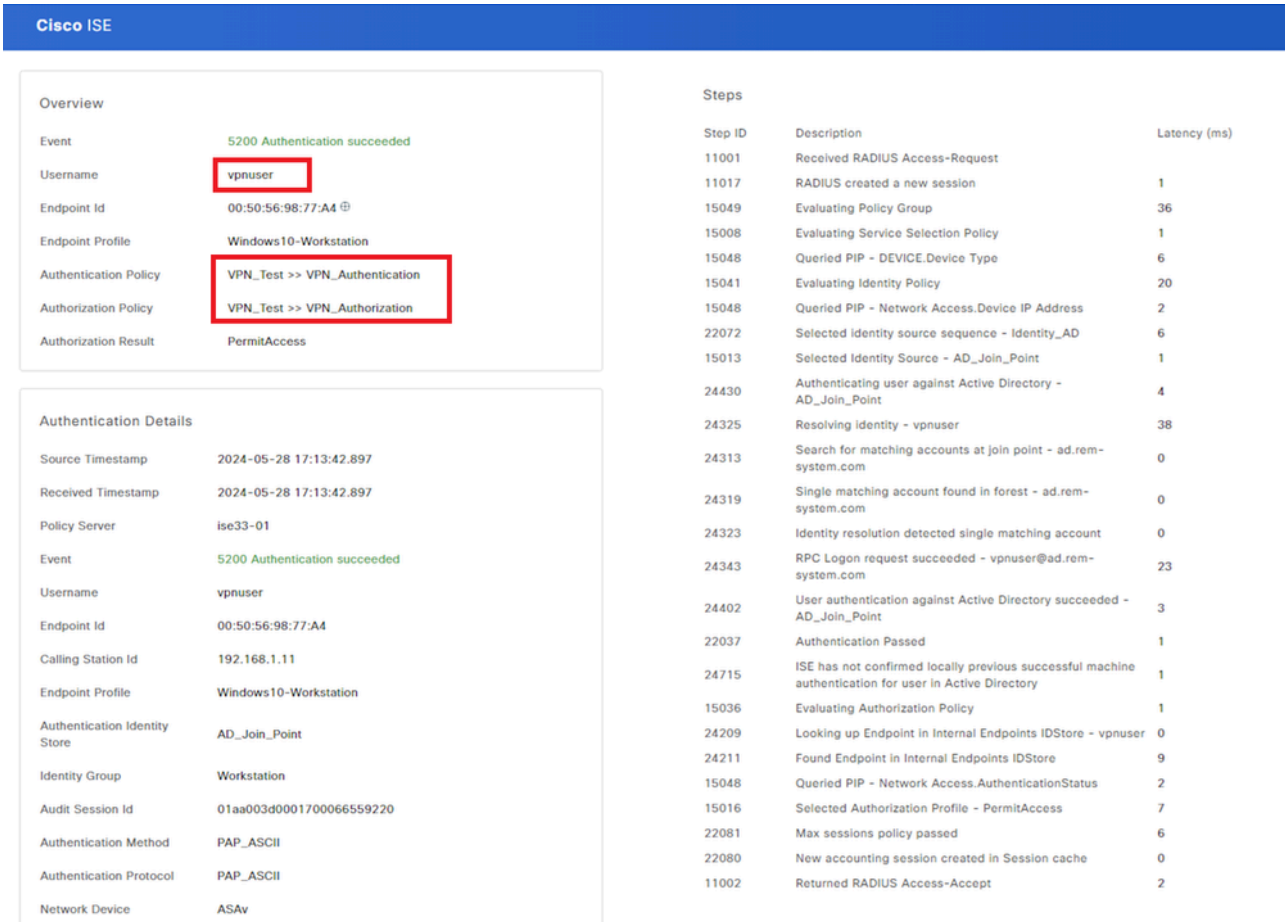
Show: Latest 20 records

Within: Last 3 hours

Time	Status	Details	Repeat ...	Endpoint ...	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...	Device Port	Identity Grou
				Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	Network Devic	Device Port	Identity Group
May 28, 2024 05:13:42....	●		0	00:50:5...	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess				
May 28, 2024 05:13:42....	☑			00:50:5...	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation

*Radius*实时日志

点击Status以确认实时日志的详细信息。



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

实时日志的详细信息

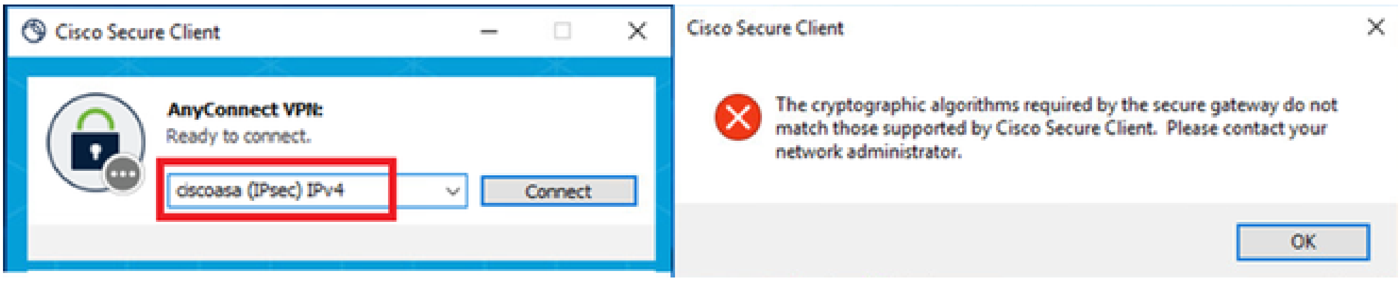
故障排除

加密算法不匹配可能导致连接故障。这是出现算法不匹配问题的示例。在ASDM中执行Configuration部分的第15步可以解决此问题。

步骤1:启动VPN连接

在终端上，运行Cisco Secure Client并确认由于加密算法不匹配导致连接失败。

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



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

ciscoasa (IPsec) IPv4

Cisco Secure Client

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

连接失败

第二步：在CLI中确认系统日志

在系统日志中，确认IKEv2协商失败。

<#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
```

参考

[通过IKEv2的AnyConnect连接到ASA，进行AAA和证书身份验证]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。