Configurer le client sécurisé IKEv2/ASA dans ASDM avec l'authentification de certificat de & AAA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Diagramme du réseau

Configurations

- Configuration dans ASDM
  - Étape 1. Ouvrir les assistants VPN
  - Étape 2. Identification du profil de connexion
  - Étape 3. Protocoles VPN
  - Étape 4. Images client
  - Étape 5. Méthodes d'authentification
  - Étape 6. Configuration SAML
  - Étape 7. Attribution d'adresse client
  - Étape 8. Serveurs de résolution de noms de réseau
  - Étape 9. Exemption NAT
  - Étape 10. Déploiement sécurisé du client
  - Étape 11. Enregistrer les paramètres
  - Étape 12. Confirmer et exporter le profil client sécurisé
  - Étape 13. Confirmer les détails du profil de client sécurisé
  - Étape 14. Confirmer les paramètres dans l'interface CLI ASA
  - Étape 15. Ajouter un algorithme de chiffrement
- Configuration dans Windows Server
- Configuration dans ISE
  - Étape 1. Ajouter un périphérique
  - Étape 2. Ajouter Active Directory
  - Étape 3. Ajouter une séquence source d'identité
  - Étape 4. Ajouter un jeu de stratégies
  - Étape 5. Ajouter une stratégie d'authentification
  - Étape 6. Ajouter une stratégie d'autorisation

Vérifier

- Étape 1. Copier le profil de client sécurisé sur Win10 PC1
- Étape 2. Initiation de la connexion VPN
- Étape 3. Confirmer Syslog sur ASA
- Étape 4. Confirmer la session IPsec sur ASA
- Étape 5. Confirmer le journal Radius en direct

Dépannage

- Étape 1. Initiation de la connexion VPN

Étape 2. Confirmer Syslog dans CLI

Référence

Introduction

Ce document décrit les étapes nécessaires pour configurer le client sécurisé sur IKEv2 sur ASA en utilisant l'ASDM avec AAA et l'authentification de certificat.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine (ISE)
- Configuration de l'appliance virtuel de sécurité adaptatif Cisco(ASAv)
- Configuration de Cisco Adaptive Security Device Manager (ASDM)
- Flux d'authentification VPN

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 1 d'Identity Services Engine Virtual 3.3
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

Le nom de domaine configuré sur Windows Server 2016 est ad.rem-system.com, qui est utilisé comme exemple dans ce document.

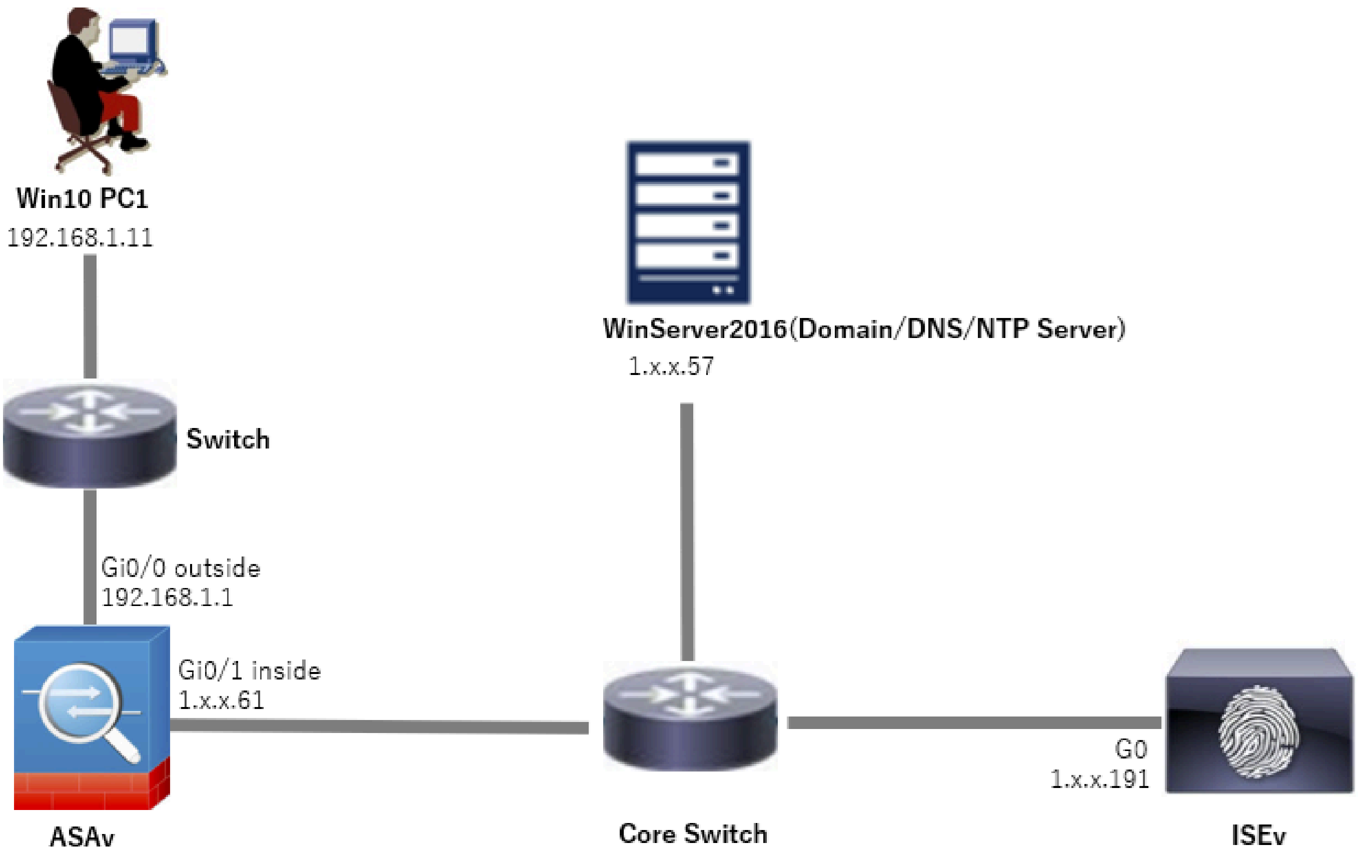


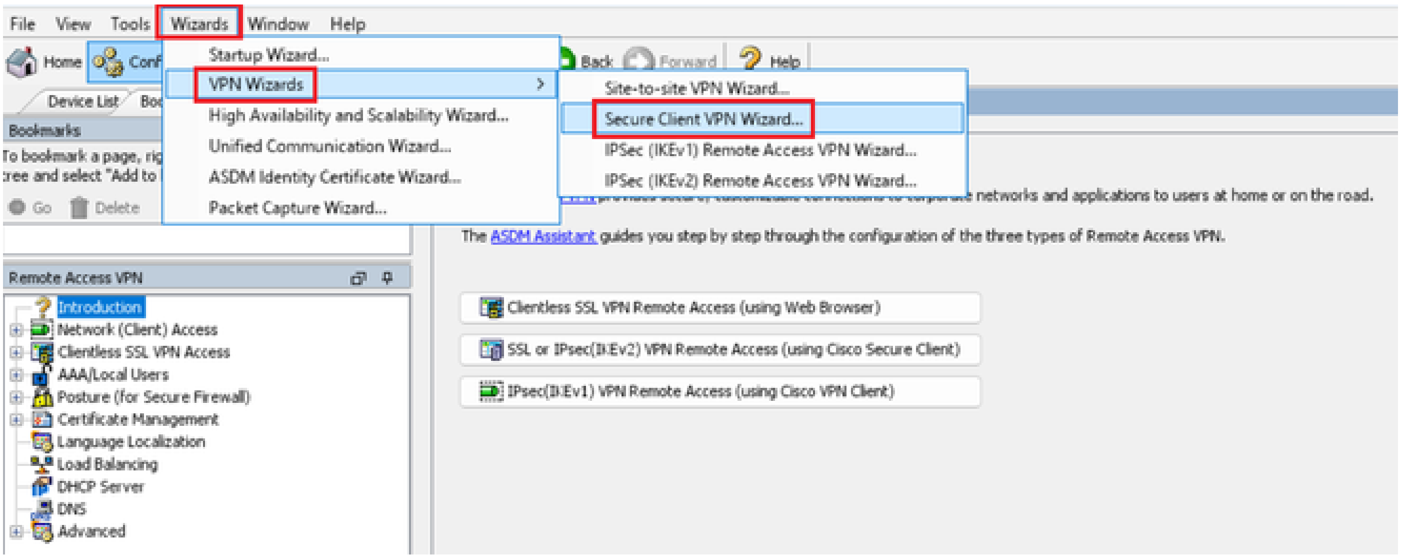
Diagramme du réseau

Configurations

Configuration dans ASDM

Étape 1. Ouvrir les assistants VPN

Accédez à Wizards > VPN Wizards, cliquez sur Secure Client VPN Wizard.


File
View
Tools
Wizards
Window
Help
Home
Conf
Back
Forward
Help
Device List
Bookmarks
Go
Delete
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...
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)

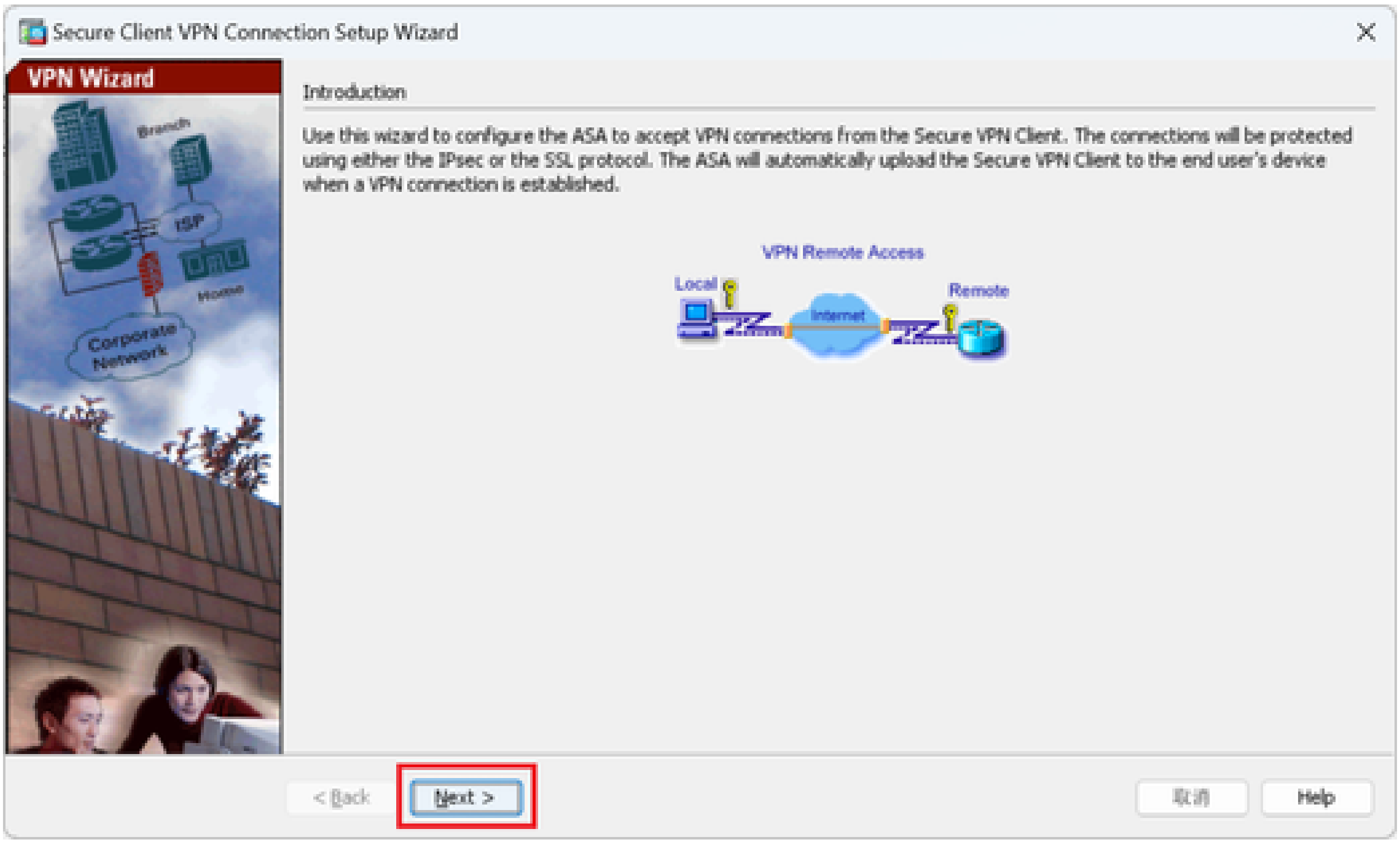
To bookmark a page, rig
tree and select "Add to

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.

Ouvrir les assistants VPN

Cliquez sur Next (Suivant).



Secure Client VPN Connection Setup Wizard

VPN Wizard

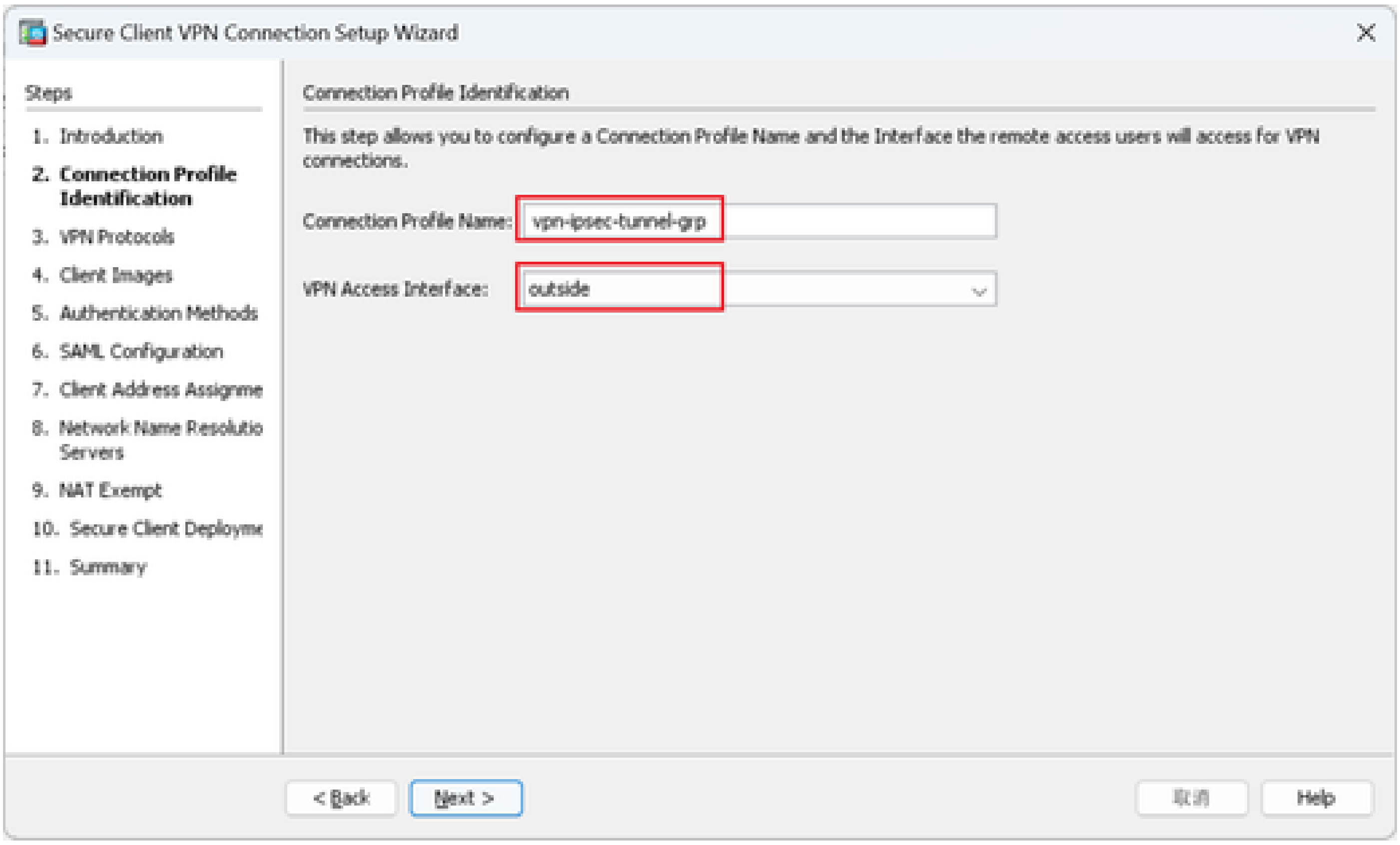
Introduction

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.

Cliquez sur le bouton Suivant

Étape 2. Identification du profil de connexion

Entrez les informations du profil de connexion.
Nom du profil de connexion : vpn-ipsec-tunnel-grp
Interface d'accès VPN : externe


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
< Back
Next >
取消
Help

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.

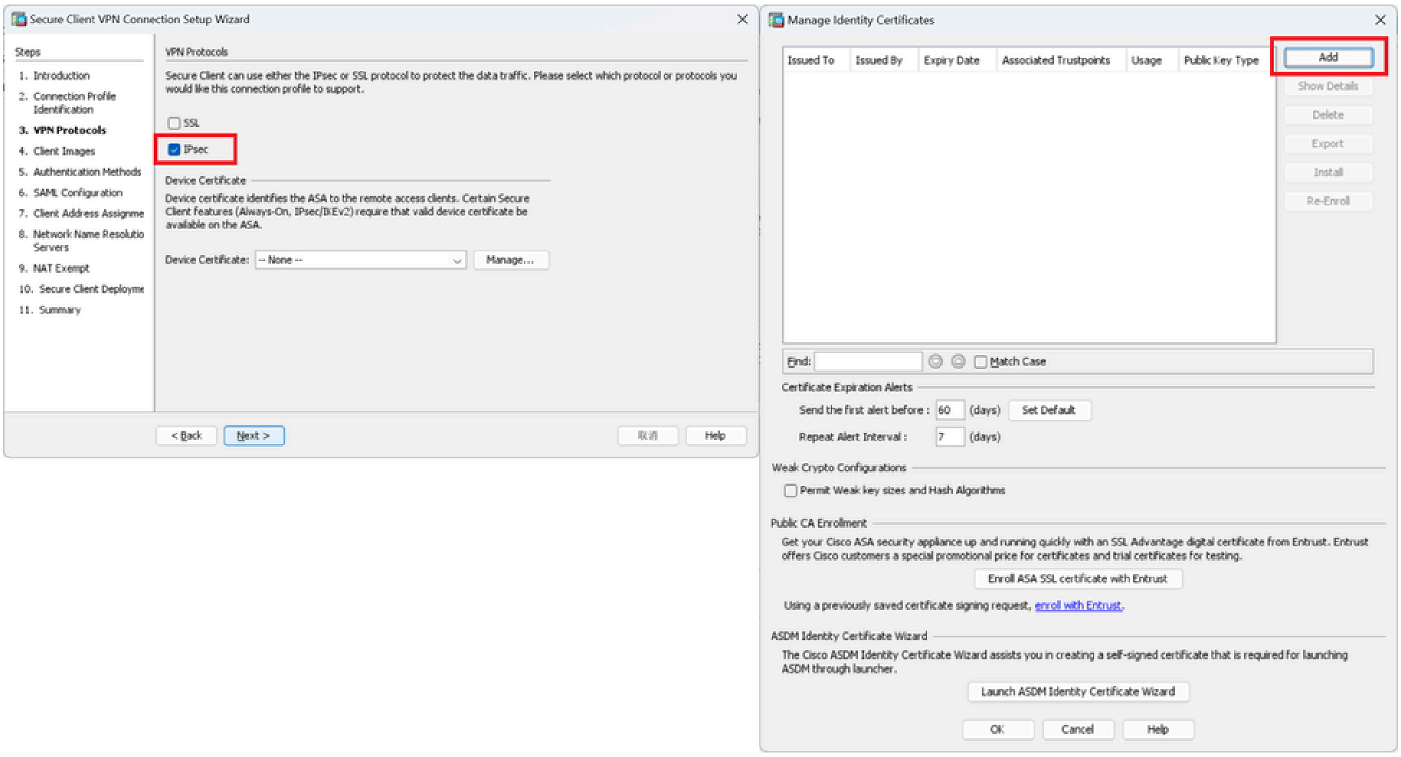
Connection Profile Name: vpn-ipsec-tunnel-grp

VPN Access Interface: outside

Identification du profil de connexion

Étape 3. Protocoles VPN

Sélectionnez IPsec, cliquez sur le bouton Add pour ajouter un nouveau certificat auto-signé.


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
< Back
Next >
取消
Help
Manage Identity Certificates
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 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...

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

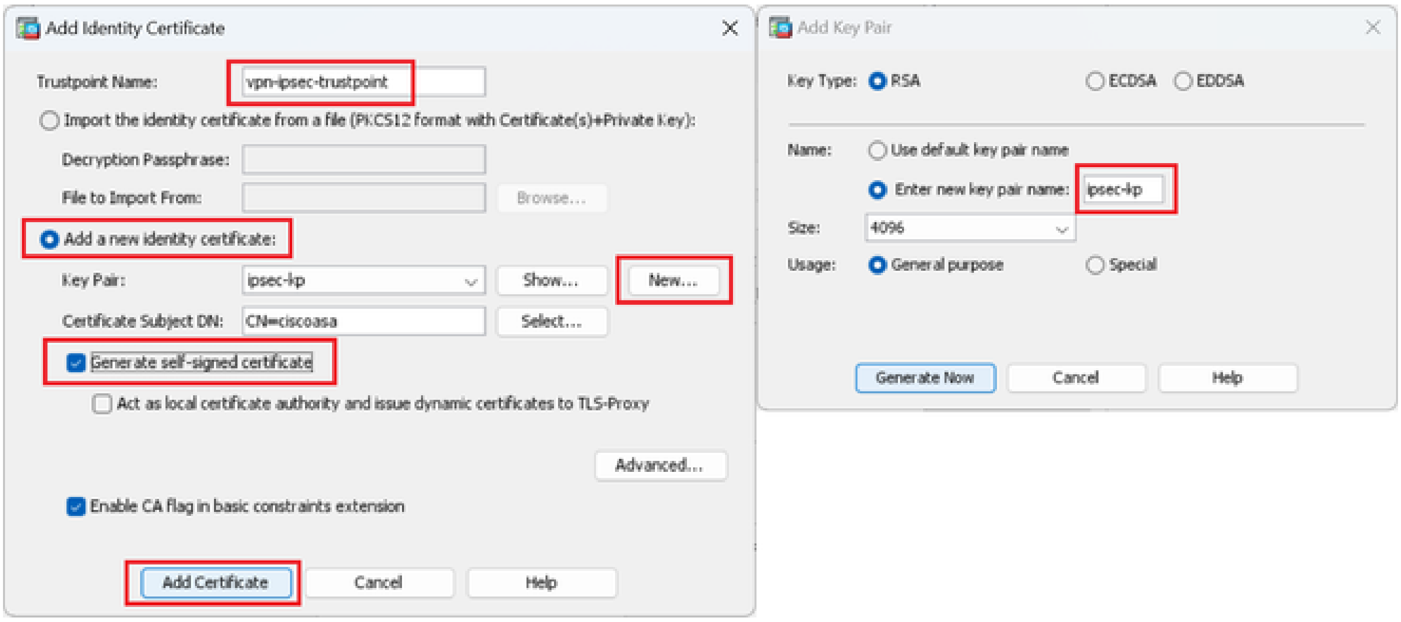
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

Protocoles VPN

Entrez les informations relatives au certificat auto-signé.

Nom du point de confiance : vpn-ipsec-trustpoint

Paire de clés : 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

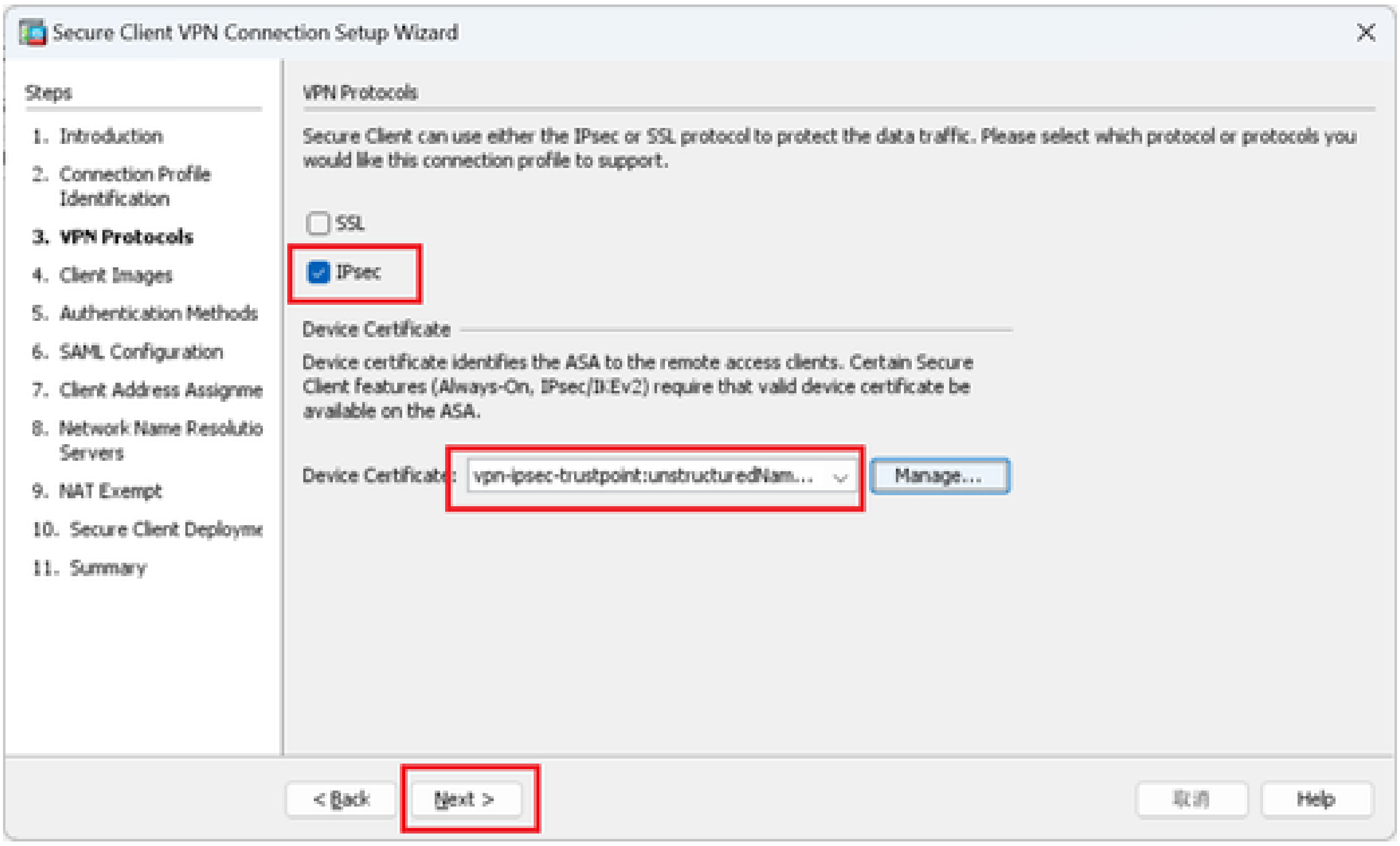
● Enter new key pair name: ipsec-kp

Size: 4096

Usage: ● General purpose ○ Special

Détail du certificat auto-signé

Confirmez les paramètres des protocoles VPN, puis cliquez sur Next.



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

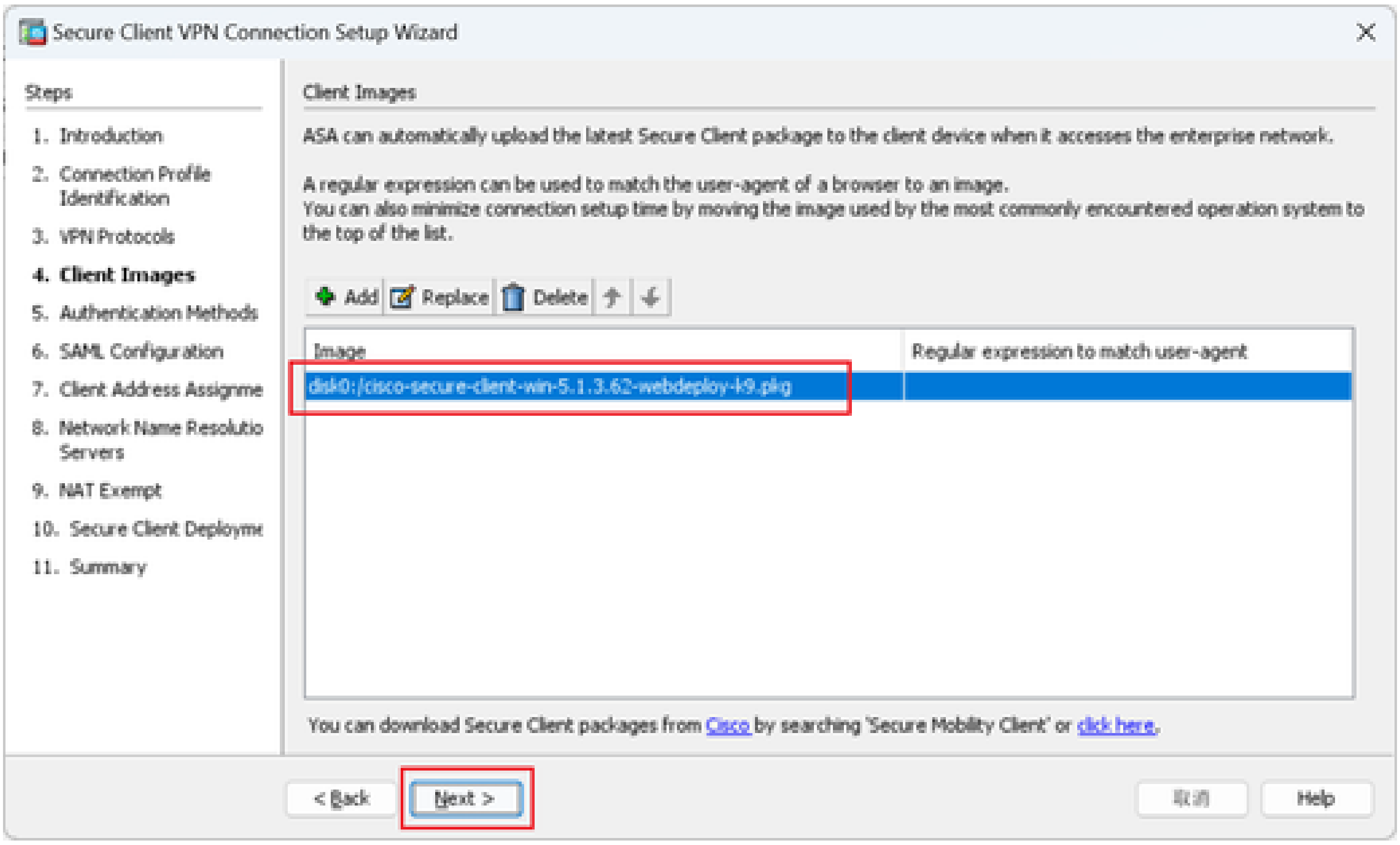
Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

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

Confirmer les paramètres du protocole VPN

Étape 4. Images client

Cliquez sur Add button pour ajouter une image de client sécurisé, cliquez sur Next button.



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.

Images client

Étape 5. Méthodes d'authentification

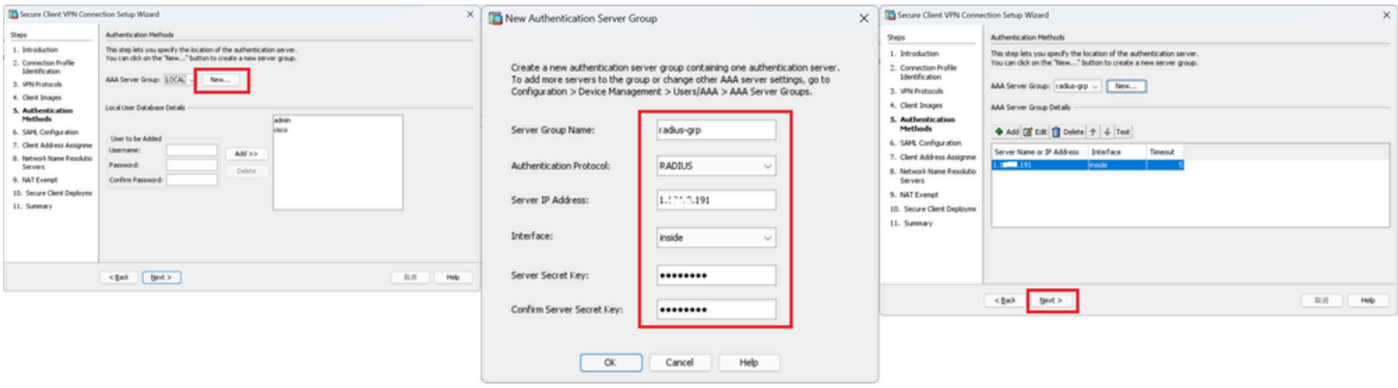
Cliquez sur New button pour ajouter un nouveau serveur aaa, cliquez sur Next button.

Nom du groupe de serveurs : radius-grp

Protocole d'authentification : RADIUS

Adresse IP du serveur : 1.x.x.191

Interface : interne



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: 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

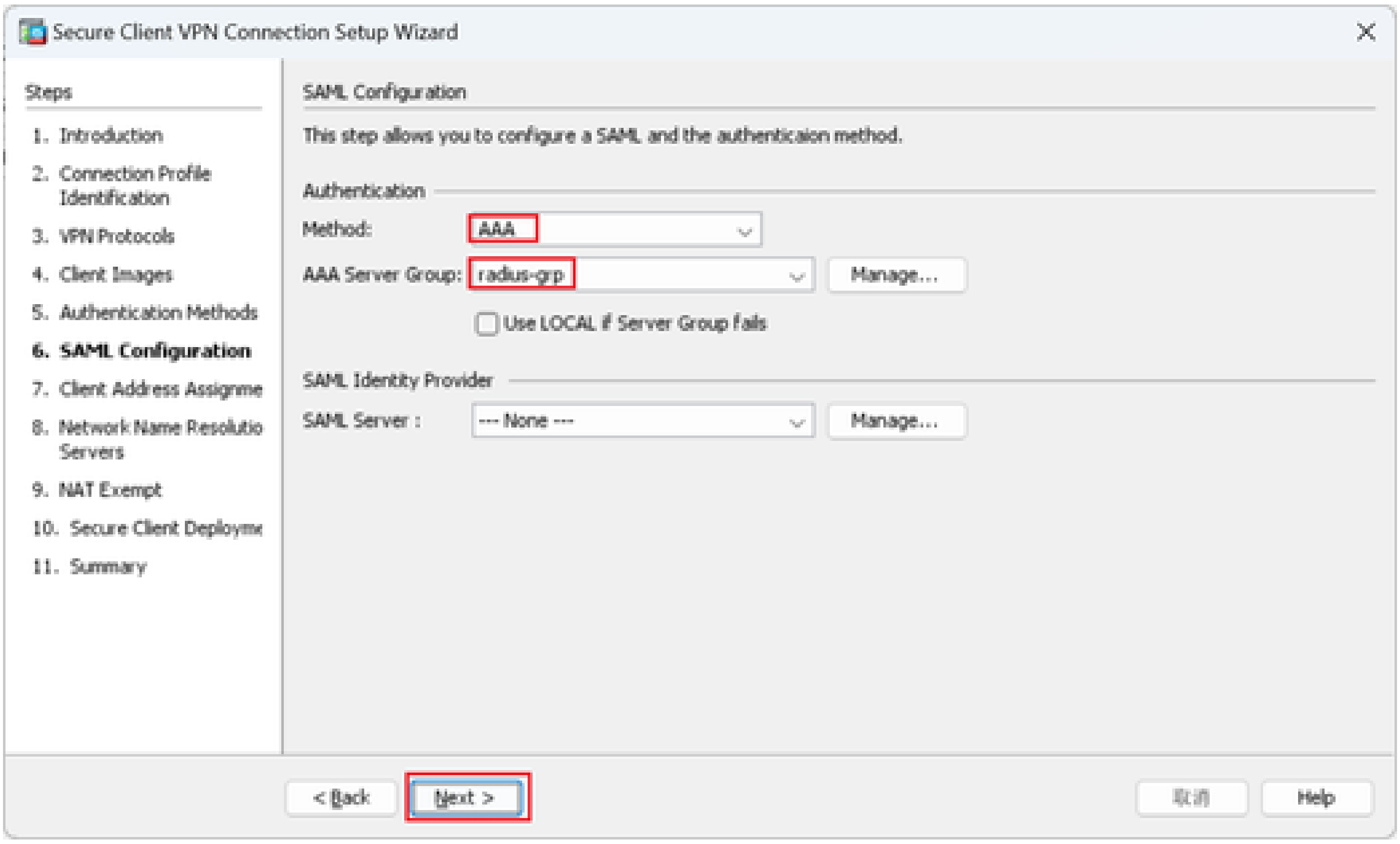
AAA Server Group Details

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

Méthodes d'authentification

Étape 6. Configuration SAML

Cliquez sur le bouton Suivant.



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
Manage...
Manage...
< Back
Next >
取消
Help

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 ---

Configuration SAML

Étape 7. Attribution d'adresse client

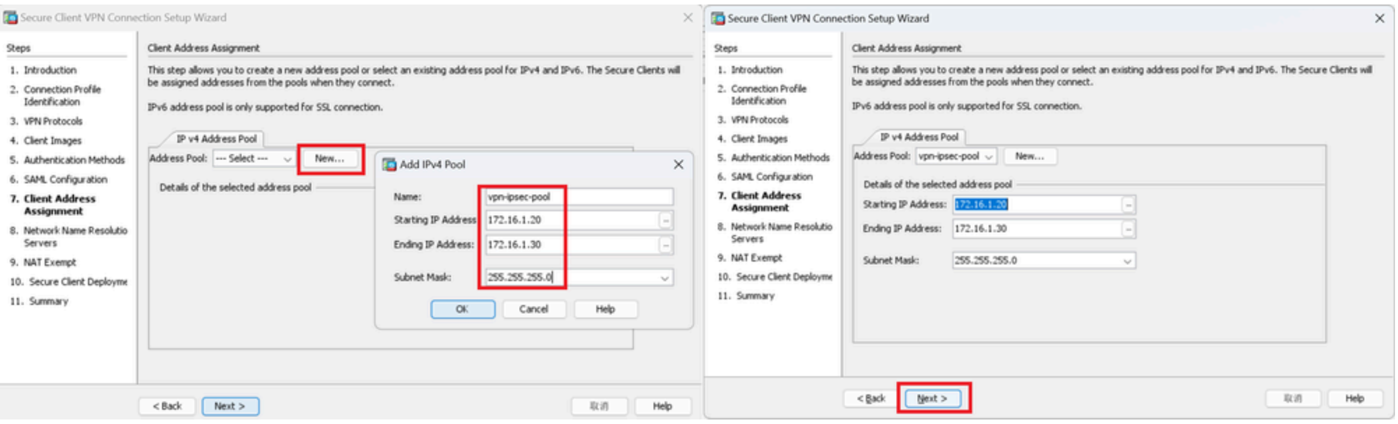
Cliquez sur New button pour ajouter un nouveau pool IPv4, cliquez sur Next button.

Nom : vpn-ipsec-pool

Adresse IP de début : 172.16.1.20

Adresse IP de fin : 172.16.1.30

Masque de sous-réseau : 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
IP v4 Address Pool
New...
Add IPv4 Pool
OK
Cancel
Help
< Back
Next >
取消
Help

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.

Address Pool: --- Select ---

Details of the selected address 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

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

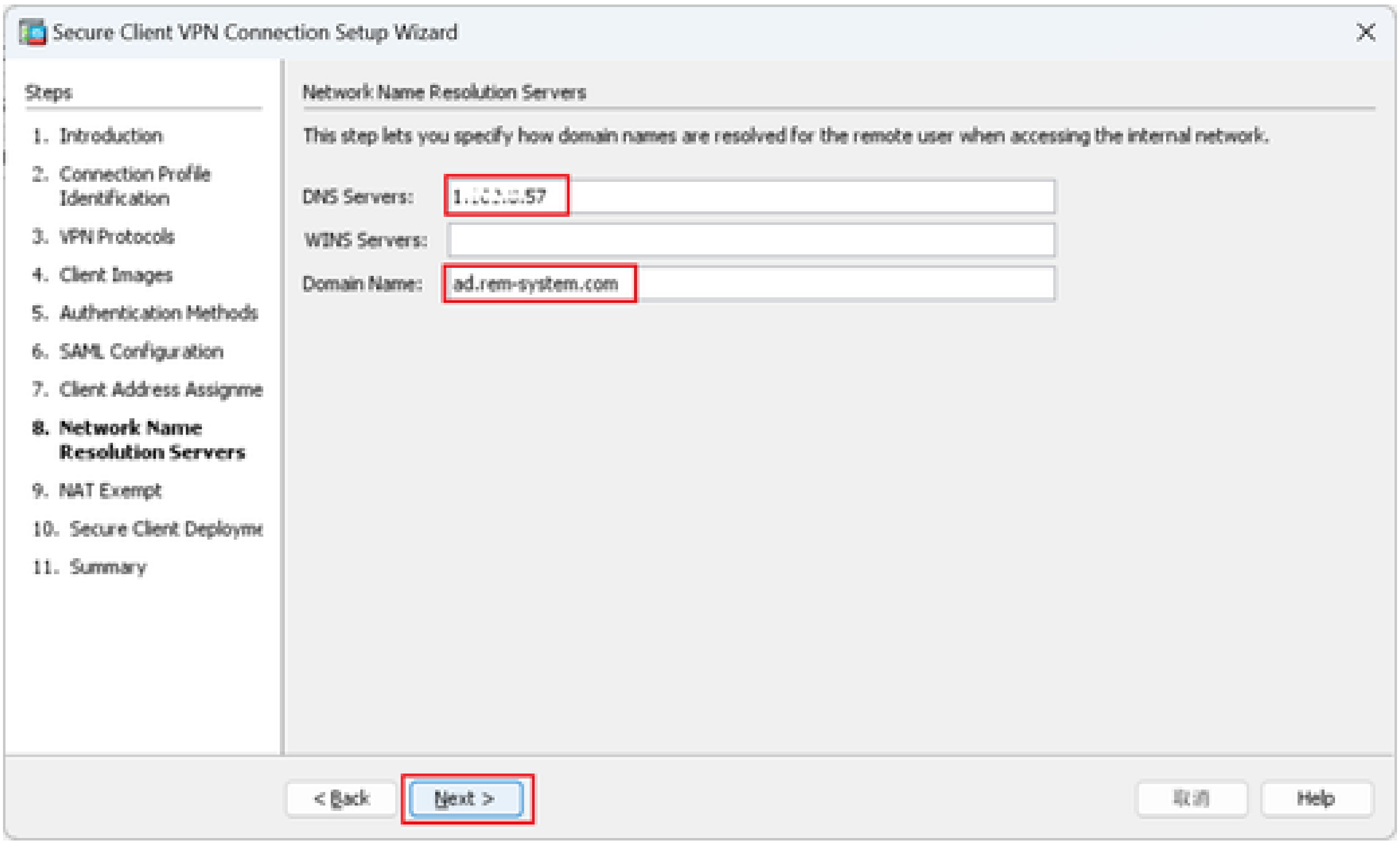
Attribution d'adresses client

Étape 8. Serveurs de résolution de noms de réseau

Saisissez les informations relatives au DNS et au domaine, puis cliquez sur Next.

Serveurs DNS : 1.x.x.57

Nom de domaine : 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
< Back
Next >
取消
Help

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

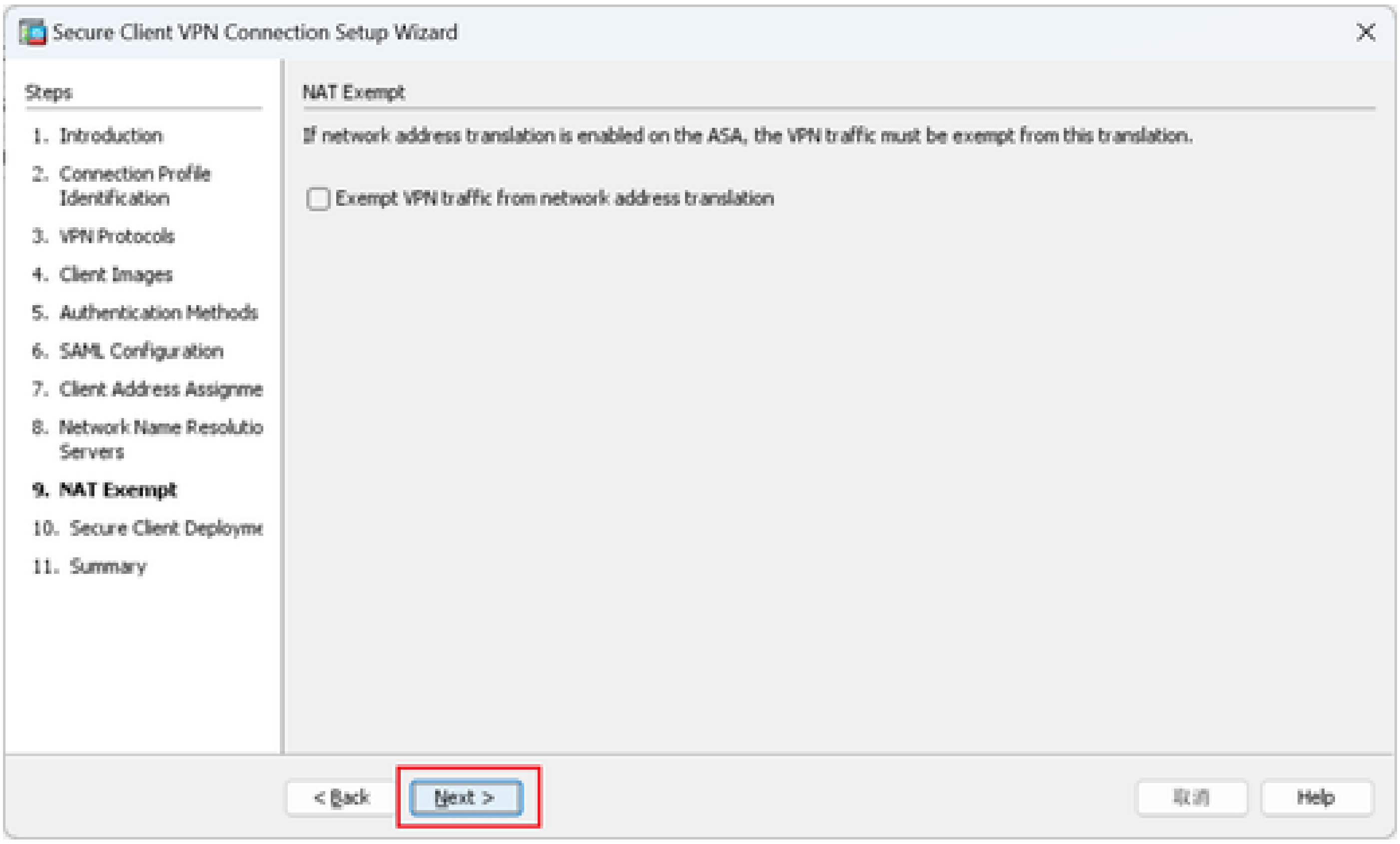
WINS Servers:

Domain Name: ad.rem-system.com

Serveurs de résolution de noms de réseau

Étape 9. Exemption NAT

Cliquez sur le bouton Suivant.


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

NAT Exempt

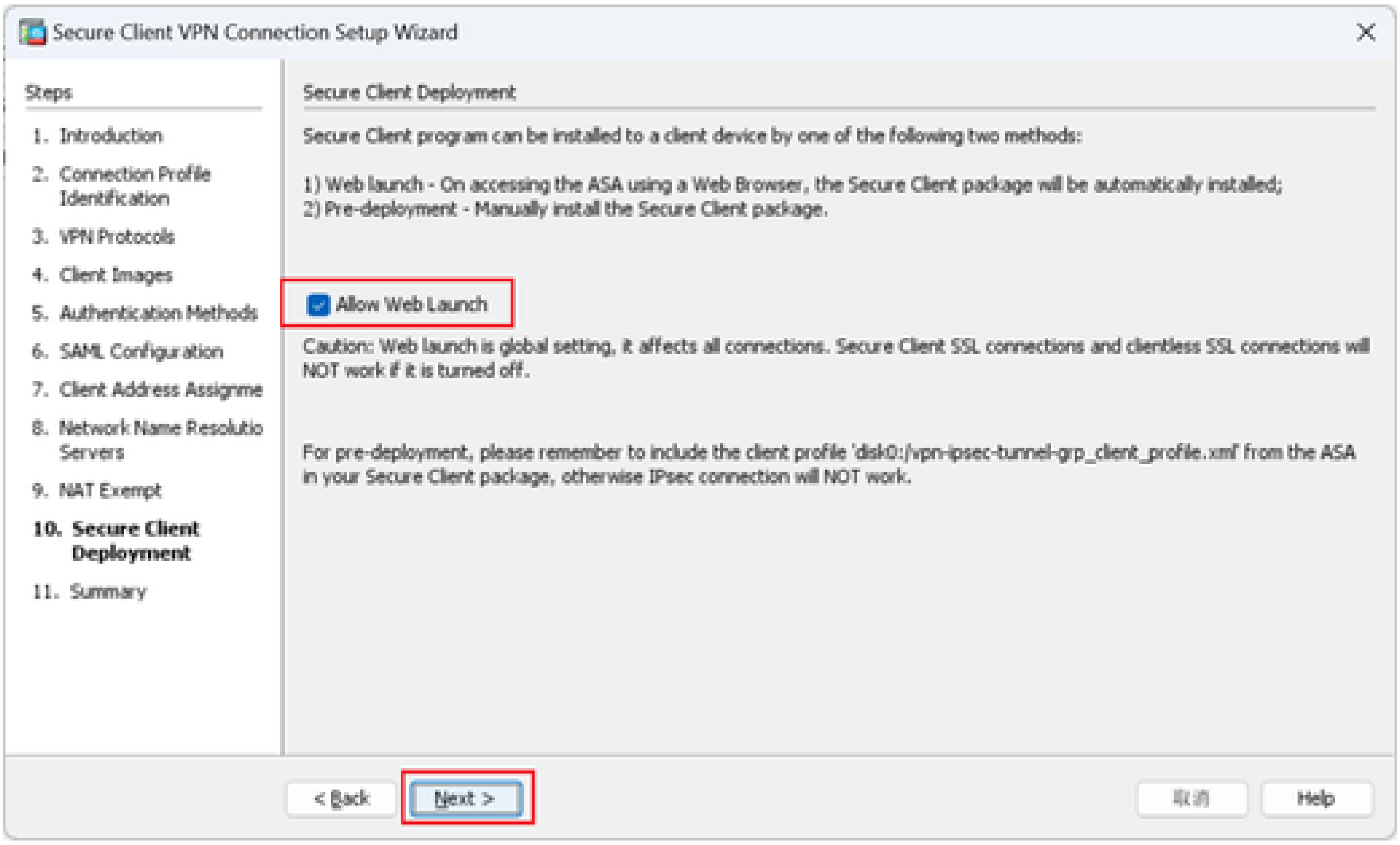
If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

□ Exempt VPN traffic from network address translation

Exemption NAT

Étape 10. Déploiement sécurisé du client

Sélectionnez Allow Web Launch, puis cliquez sur le bouton Next.


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 Deployment**
11. Summary

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.

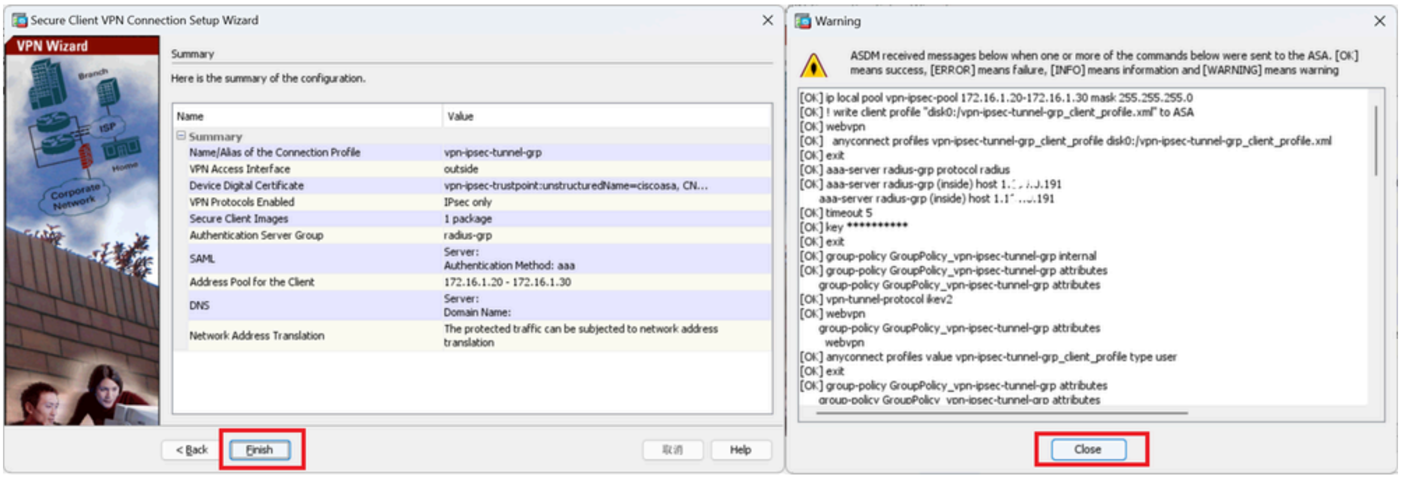
☑ Allow Web Launch

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.

Étape 11. Enregistrer les paramètres

Cliquez sur le bouton Finish et enregistrez les paramètres.



Secure Client VPN Connection Setup Wizard

VPN 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

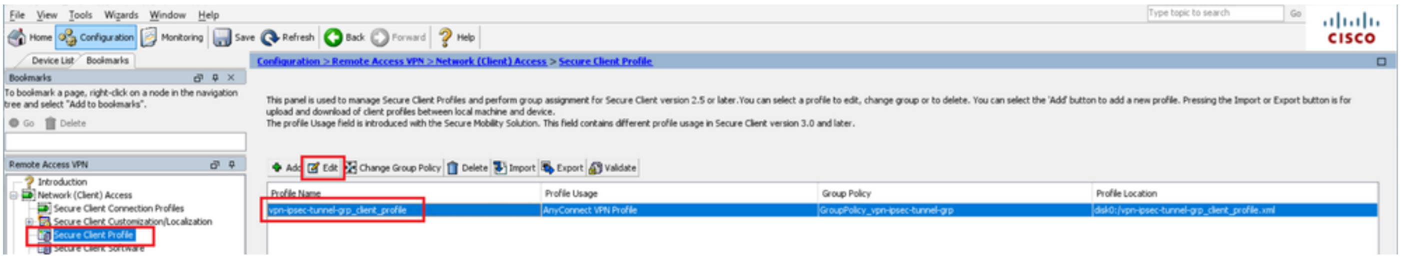
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[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
```

Enregistrer les paramètres

Étape 12. Confirmer et exporter le profil client sécurisé

Accédez à Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, cliquez sur Edit button.



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

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

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.

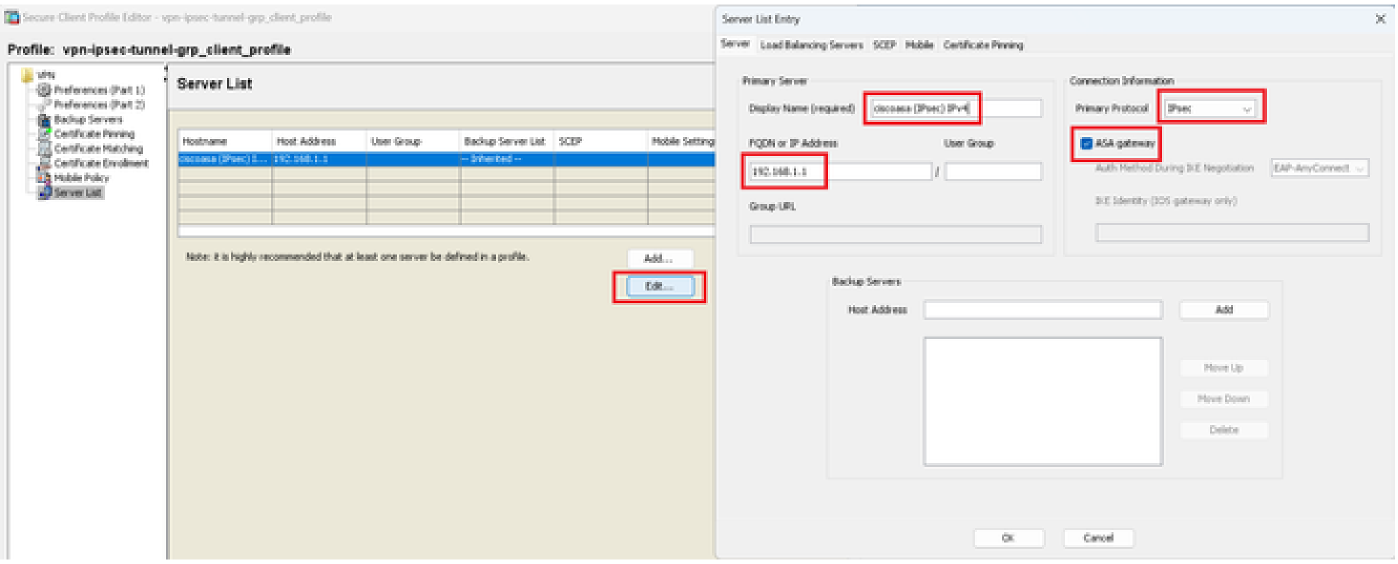
Profile Name	Profile Usage	Group Policy	Profile Location
vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml

File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Type topic to search Go
Device List Bookmarks
Bookmarks
Go Delete
Remote Access VPN
Introduction
Network (Client) Access
Secure Client Connection Profiles
Secure Client Customization/Localization
Secure Client Profile
Secure Client Software
Add Edit Change Group Policy Delete Import Export Validate

Modifier le profil client sécurisé

Confirmez le détail du profil.

- Nom d'affichage (obligatoire) : ciscoasa (IPsec) IPv4
- Nom de domaine complet ou adresse IP : 192.168.1.1
- Protocole principal : IPsec



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.

Primary Server

Display Name (required): ciscoasa (IPsec) IPv4

FQDN or IP Address: 192.168.1.1 / User Group:

Group URL:

Connection Information

Primary Protocol: IPsec

☑ ASA gateway

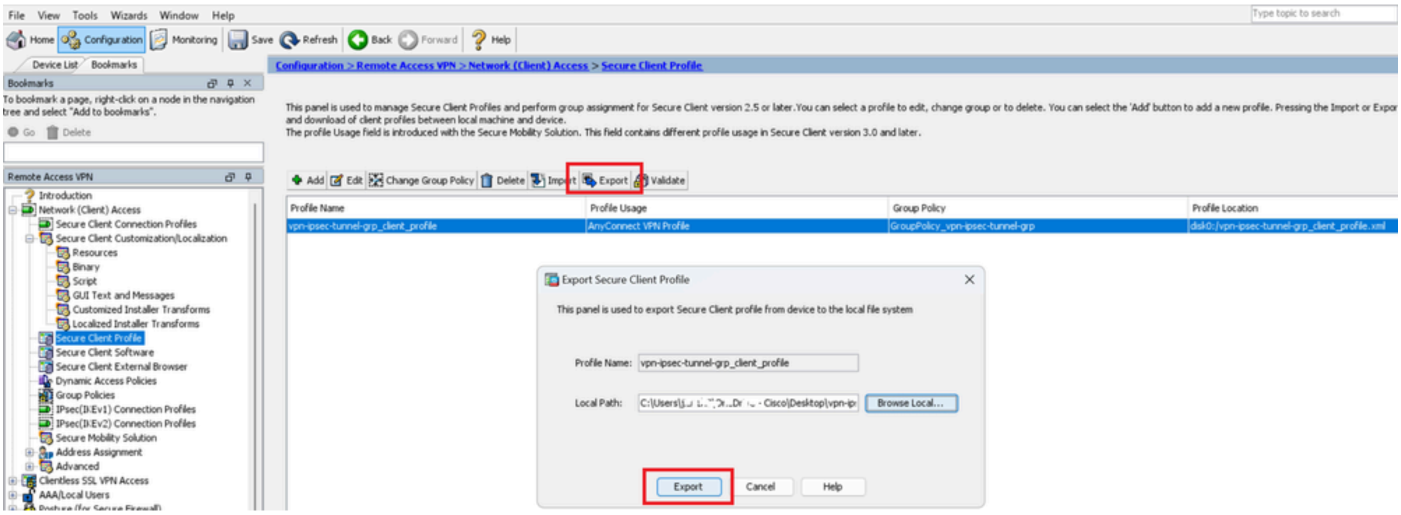
Auth Method During IKE Negotiation: EAP-AnyConnect

IKE Identity (IOS gateway only)

Host Address:

Confirmer le profil client sécurisé

Cliquez sur le bouton Export pour exporter le profil vers le PC local.



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 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

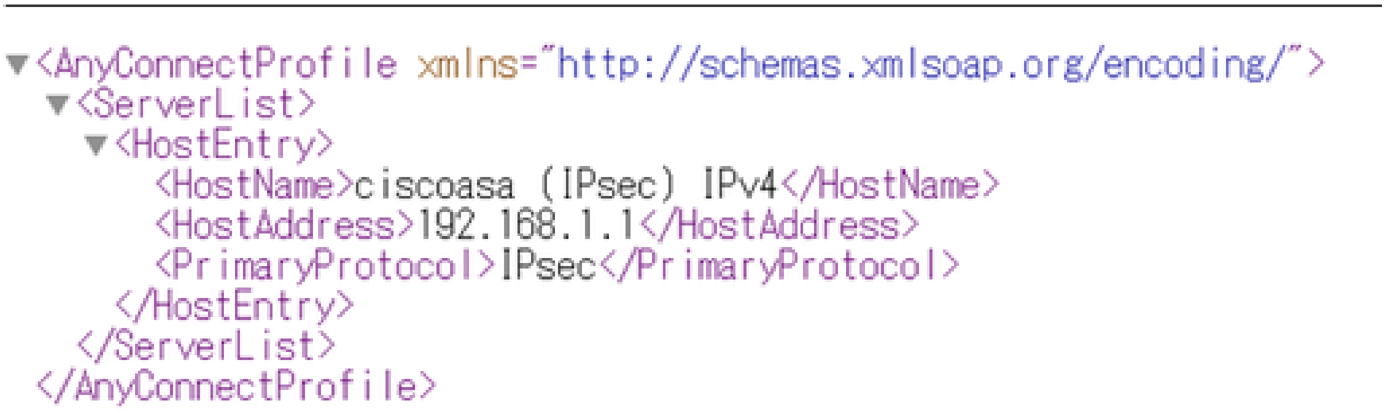
Profile Name: vpn-ipsec-tunnel-grp_client_profile

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

Exporter le profil client sécurisé

Étape 13. Confirmer les détails du profil de client sécurisé

Ouvrez Secure Client Profile par navigateur, confirmez que le protocole principal pour l'hôte est 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>
```

Détail du profil de client sécurisé

Étape 14. Confirmer les paramètres dans l'interface CLI ASA

Confirmez les paramètres IPsec créés par ASDM dans l'interface de ligne de commande 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
```

Étape 15. Ajouter un algorithme de chiffrement

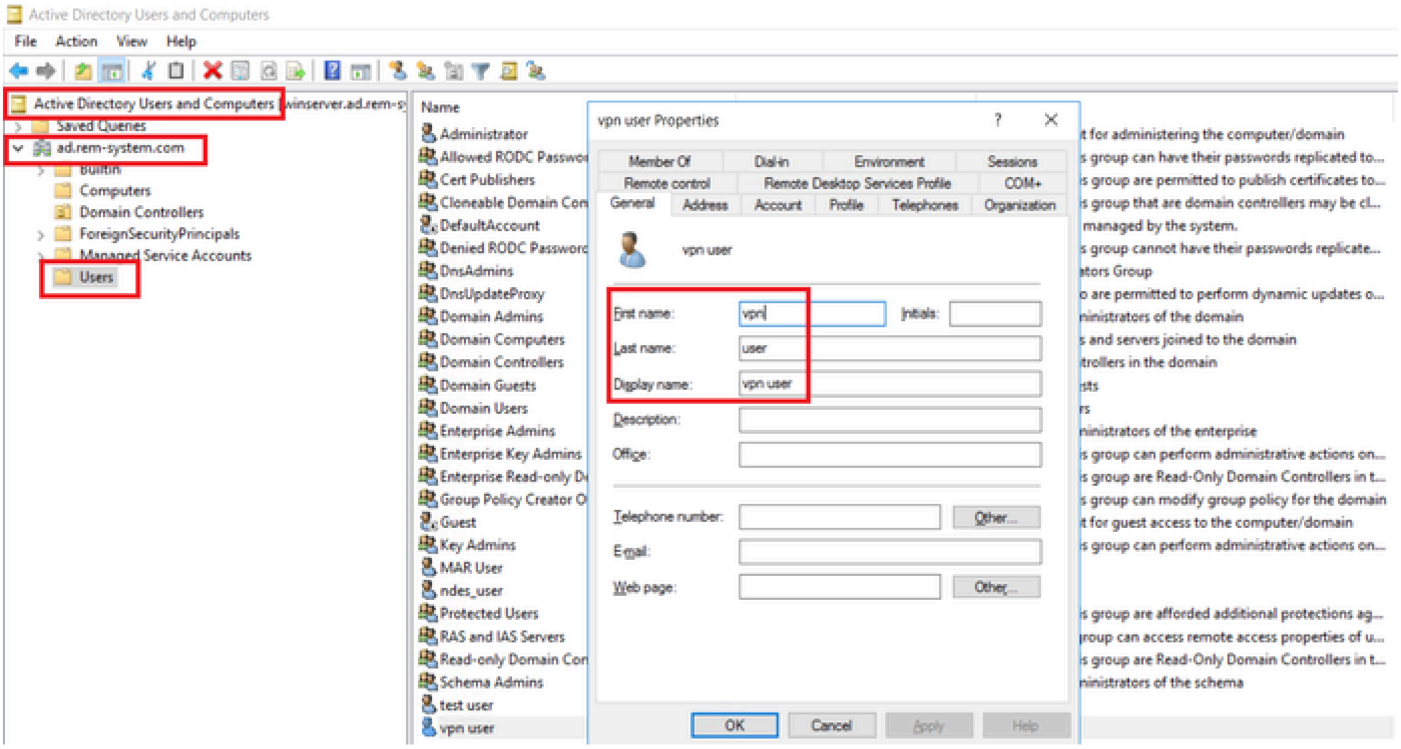
Dans l'interface CLI ASA, ajoutez le groupe 19 à la stratégie IKEv2.

Remarque : pour les connexions IKEv2/IPsec, Cisco Secure Client ne prend plus en charge les groupes Diffie-Hellman (DH) 2, 5, 14 et 24 à partir de la version 4.9.00086. Cette modification peut entraîner des échecs de connexion en raison de discordances d'algorithmes de chiffrement.

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

Configuration dans Windows Server

Vous devez ajouter un utilisateur de domaine pour la connexion VPN. Accédez à Utilisateurs et ordinateurs Active Directory, puis cliquez surUtilisateurs. Ajoutez vpnuser en tant qu'utilisateur de domaine.



Active Directory Users and Computers

File Action View Help

- 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

t for administering the computer/domain
s group can have their passwords replicated to...
s group are permitted to publish certificates to...
s group that are domain controllers may be cl...
managed by the system.
s group cannot have their passwords replicate...
ators Group
o are permitted to perform dynamic updates o...
ninistrators of the domain
s and servers joined to the domain
trollers in the domain
sts
rs
ninistrators of the enterprise
s group can perform administrative actions on...
s group are Read-Only Domain Controllers in t...
s group can modify group policy for the domain
t for guest access to the computer/domain
s group can perform administrative actions on...
s group are afforded additional protections ag...
roup can access remote access properties of u...
s group are Read-Only Domain Controllers in t...
ninistrators of the schema

vpn user Properties

Member Of | Dial-in | Environment | Sessions
Remote control | Remote Desktop Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization

vpn user

First name: vpn

Initials:

Last name: user

Display name: vpn user

Description:

Office:

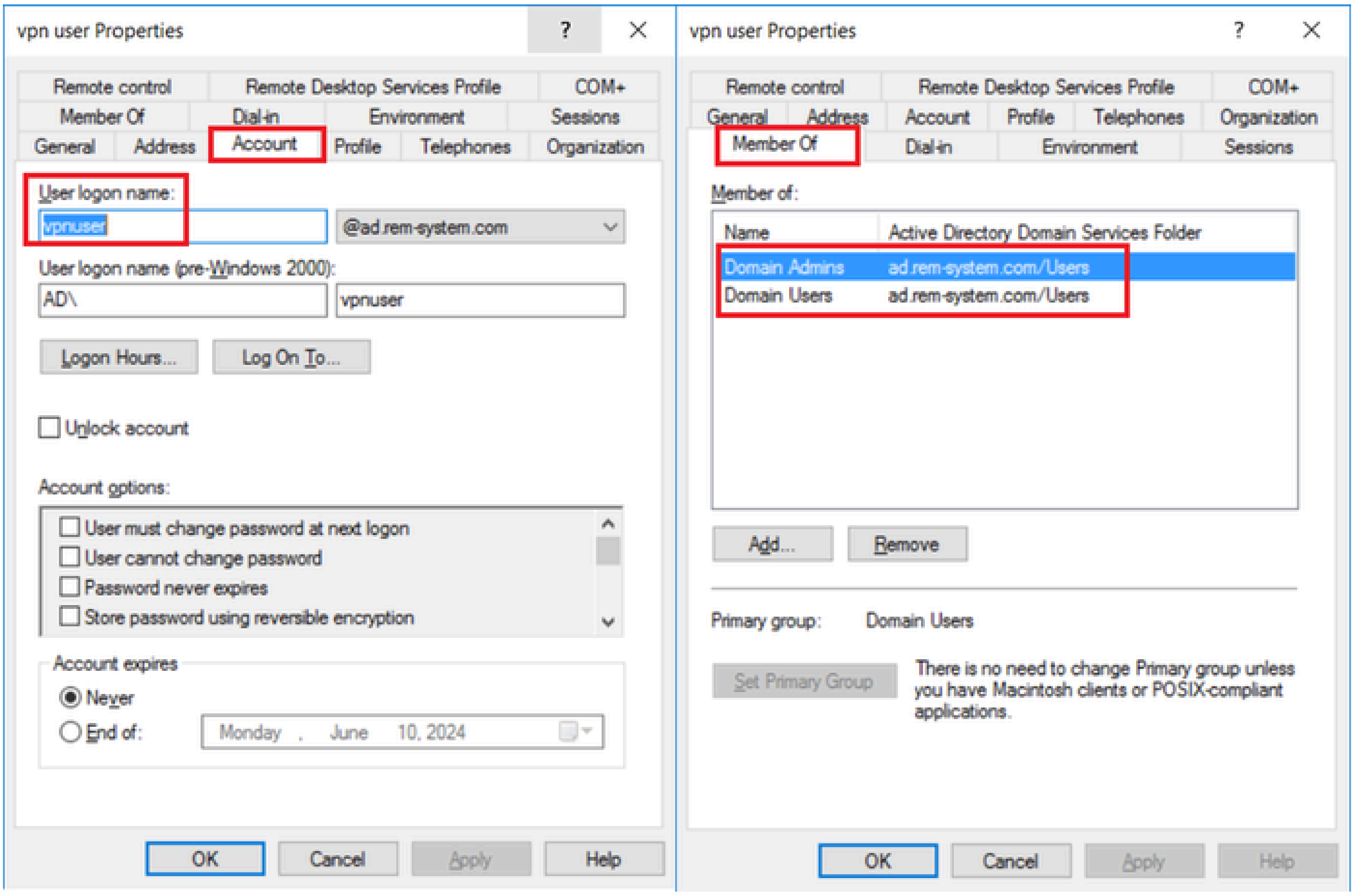
Telephone number: Other...

E-mail:

Web page: Other...

Ajouter un utilisateur de domaine

Ajoutez l'utilisateur du domaine aux membres Admins du domaine et Utilisateurs du domaine.



vpn user Properties

Remote control | Remote Desktop Services Profile | COM+
Member Of | Dial-in | Environment | Sessions
General | Address | Account | Profile | Telephones | Organization

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

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

Logon Hours...
Log On To...

□ 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

Remote control | Remote Desktop Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization
Member Of | Dial-in | Environment | Sessions

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

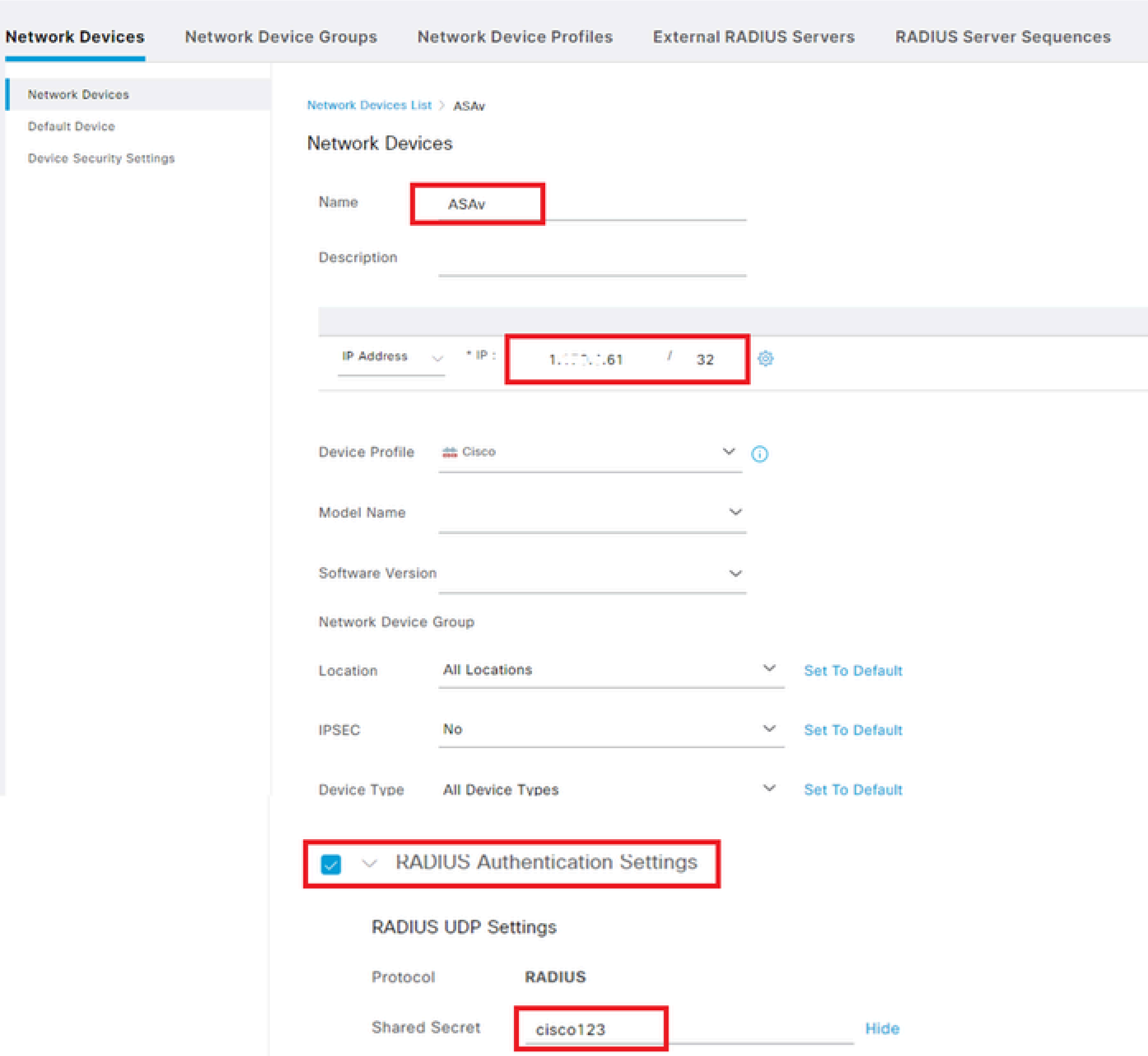
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Administrateurs de domaine et utilisateurs de domaine

Configuration dans ISE

Étape 1. Ajouter un périphérique

Accédez à Administration > Network Devices, cliquez sur Addbutton pour ajouter un périphérique ASAv.



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 — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

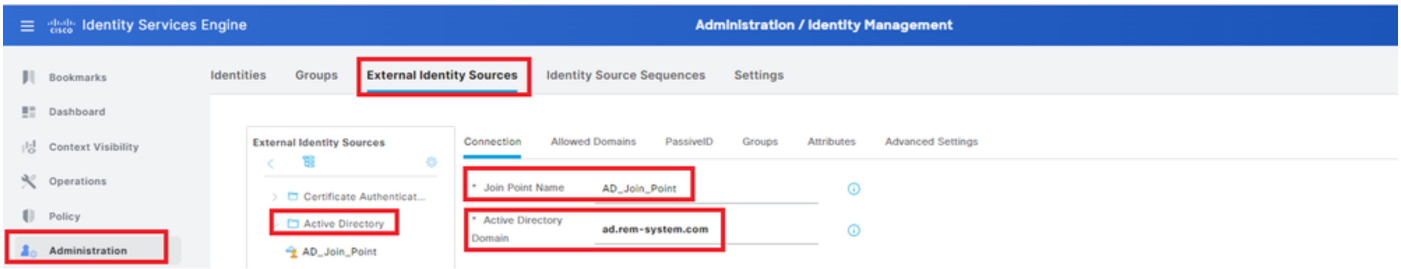
Shared Secret: cisco123 — Hide

Ajouter un périphérique

Étape 2. Ajouter Active Directory

Accédez à Administration > Sources d'identité externes > Active Directory, cliquez sur l'onglet Connexion, ajoutez Active Directory à ISE.

- Nom du point de jointure : AD_Join_Point
- Domaine Active Directory : ad.rem-system.com

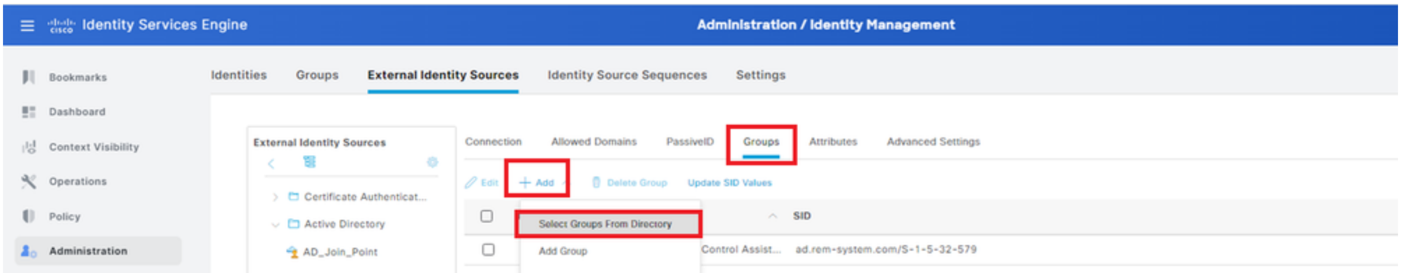


* Join Point Name: AD_Join_Point

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

Ajouter Active Directory

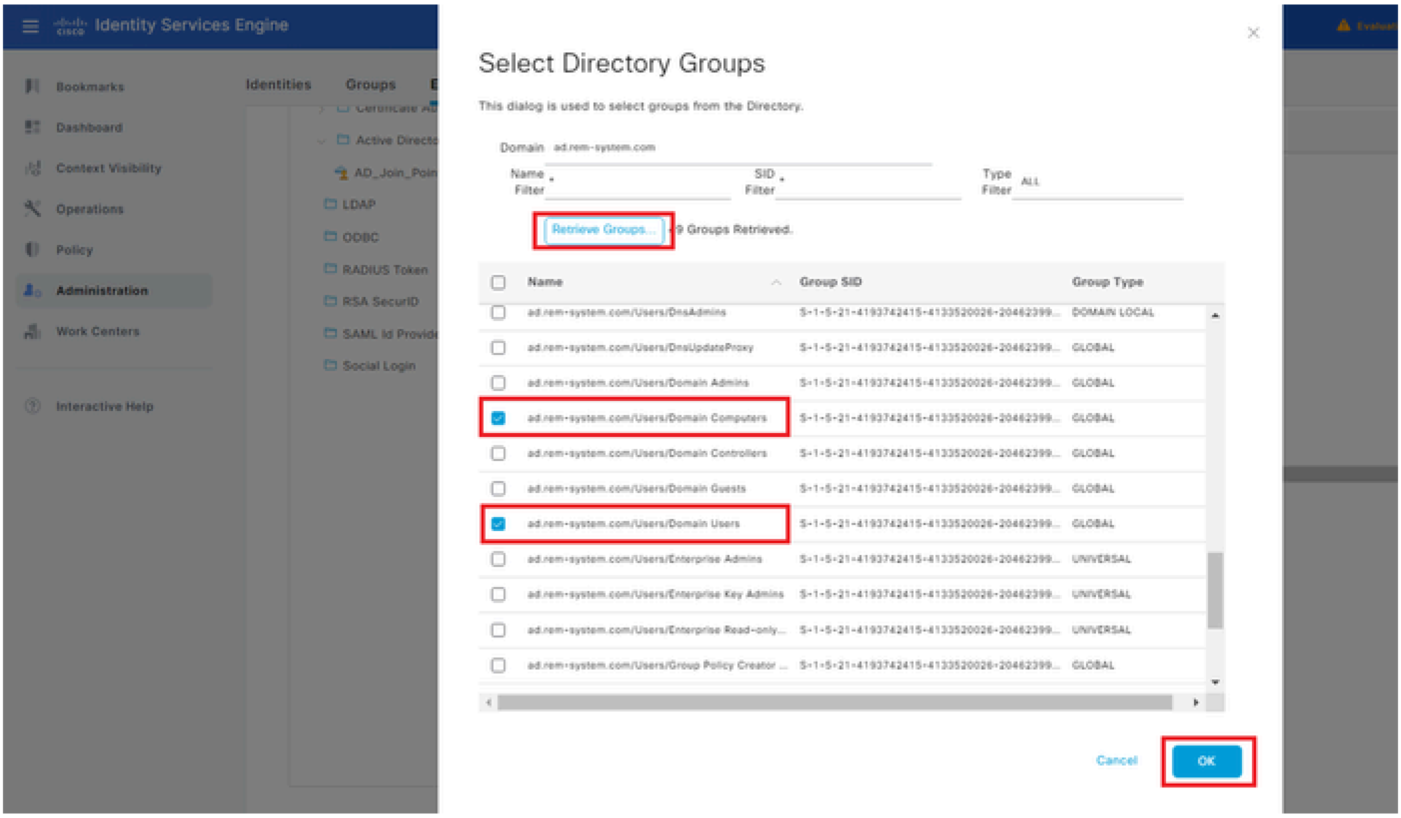
Accédez à l'onglet Groupes, sélectionnezSélectionner les groupes du répertoire dans la liste déroulante.



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

Sélectionner les groupes du répertoire

Cliquez sur la liste déroulante Récupérer des groupes. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Utilisateurs et cliquez sur 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

49 Groups Retrieved.

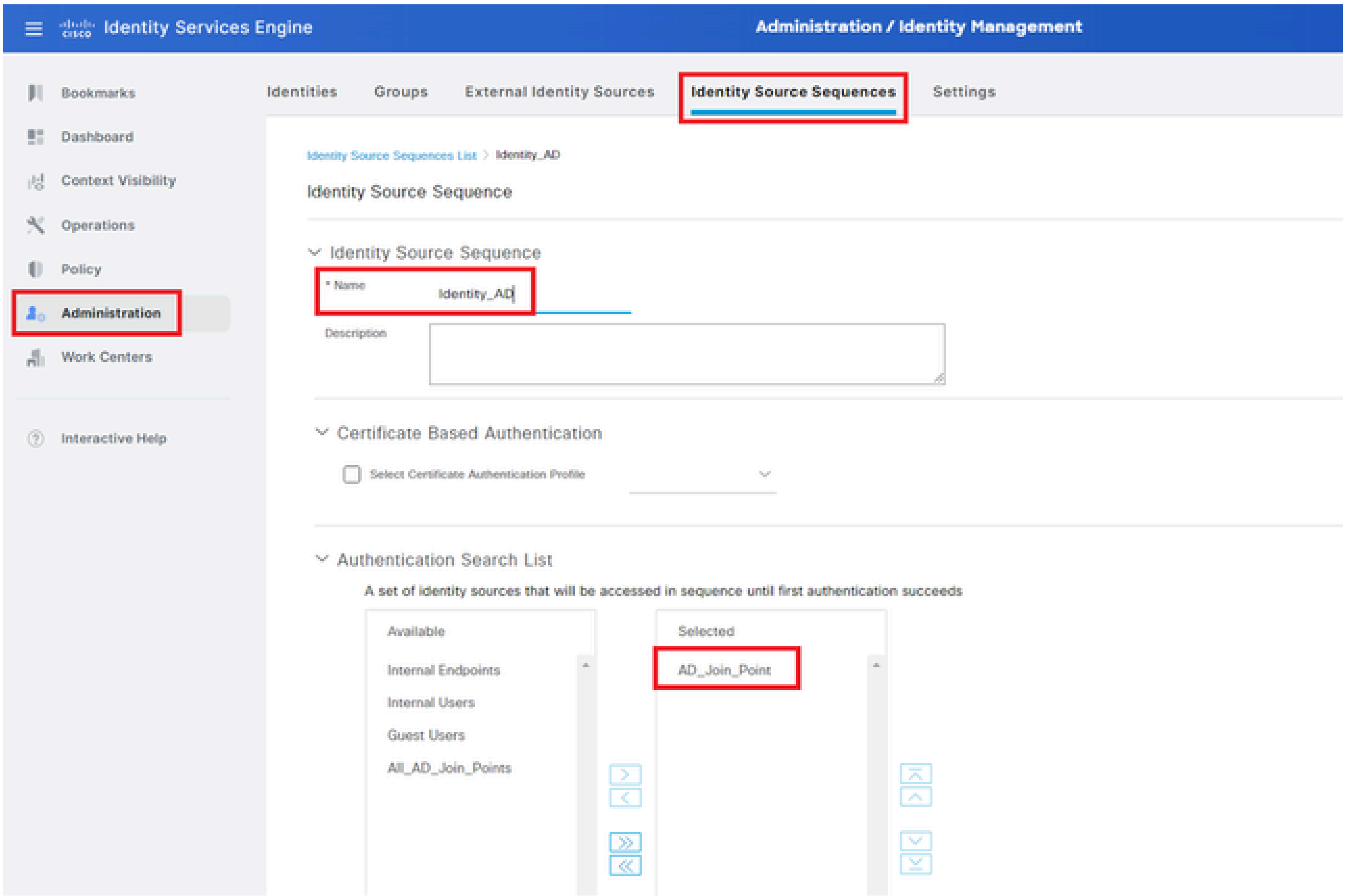
	Name	Group SID	Group Type
□	ad.rem-system.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-system.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-system.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	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

Ajouter des ordinateurs et des utilisateurs de domaine

Étape 3. Ajouter une séquence source d'identité

Accédez à Administration > Identity Source Sequences, ajoutez une Identity Source Sequence.

- Nom : Identity_AD
- Liste de recherche d'authentification : AD_Join_Point



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

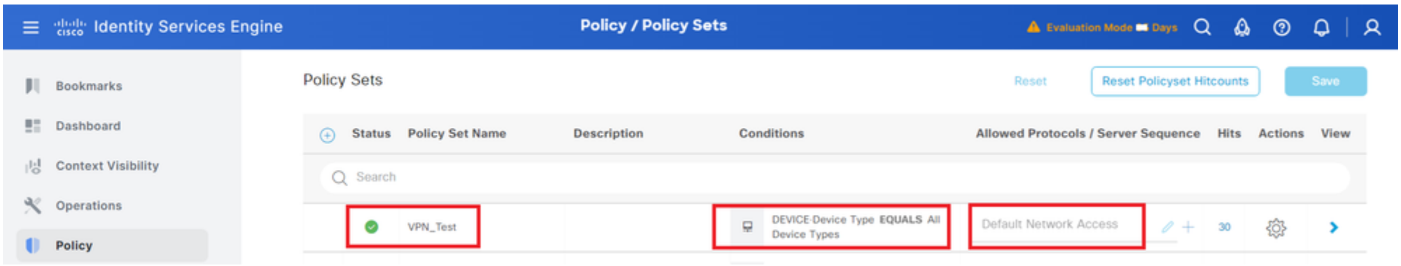
Available	Selected
Internal Endpoints Internal Users Guest Users All_AD_Join_Points	AD_Join_Point

Ajouter des séquences source d'identité

Étape 4. Ajouter un jeu de stratégies

Accédez à Policy > Policy Sets, cliquez sur + pour ajouter un jeu de stratégies.

- Nom du jeu de stratégies : VPN_Test
- Conditions : PÉRIPHÉRIQUE Type de périphérique ÉGAL à tous les types de périphériques
- Protocoles autorisés / Séquence de serveurs : accès réseau par défaut



Policy Sets

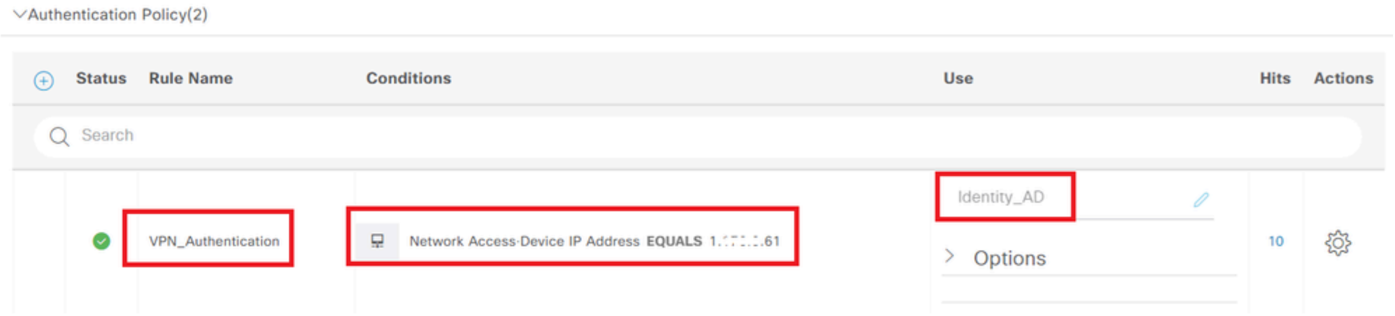
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	VPN_Test		DEVICE·Device Type EQUALS All Device Types	Default Network Access	30		>

Ajouter un jeu de stratégies

Étape 5. Ajouter une stratégie d'authentification

Accédez à Policy Sets, cliquez sur VPN_Test pour ajouter une stratégie d'authentification.

- Nom de la règle : VPN_Authentication
- Conditions : Adresse IP du périphérique d'accès réseau ÉGALE 1.x.x.61
- Utiliser : Identity_AD



Authentication Policy(2)

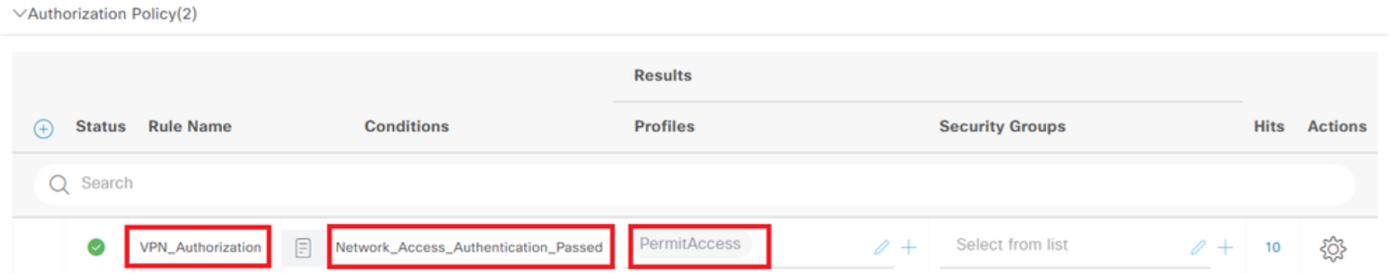
Status	Rule Name	Conditions	Use	Hits	Actions
✓	VPN_Authentication	Network Access·Device IP Address EQUALS 1.[redacted].61	Identity_AD Options	10	⚙

Ajouter une stratégie d'authentification

Étape 6. Ajouter une stratégie d'autorisation

Accédez à Policy Sets, cliquez sur VPN_Test pour ajouter une stratégie d'autorisation.

- Nom de la règle : VPN_Authorization
- Conditions : Network_Access_Authentication_Passed
- Résultats : PermitAccess



Authorization Policy(2)

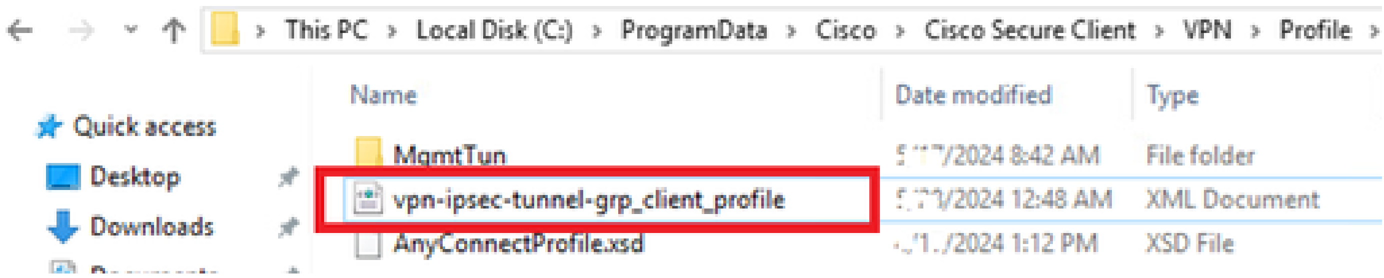
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	⚙

Ajouter une stratégie d'autorisation

Vérifier

Étape 1. Copier le profil de client sécurisé sur Win10 PC1

Copiez le profil de client sécurisé dans le répertoire C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



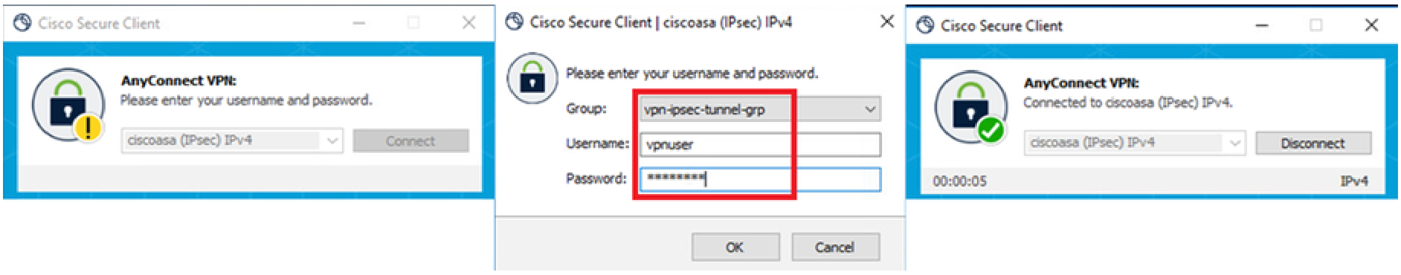
This PC › Local Disk (C:) › ProgramData › Cisco › Cisco Secure Client › VPN › Profile ›

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

Copier le profil sur le PC

Étape 2. Initiation de la connexion VPN

Sur le terminal, exécutez Cisco Secure Client et saisissez le nom d'utilisateur et le mot de passe, puis vérifiez que Cisco Secure Client se connecte correctement.



Cisco Secure Client

AnyConnect VPN:
Please enter your username and password.

ciscoasa (IPsec) IPv4

Cisco Secure Client | ciscoasa (IPsec) IPv4

Please enter your username and password.

Group: vpn-ipsec-tunnel-grp

Username: vpnuser

Password: ********

Cisco Secure Client

AnyConnect VPN:
Connected to ciscoasa (IPsec) IPv4.

ciscoasa (IPsec) IPv4

00:00:05 IPv4

Connexion réussie

Étape 3. Confirmer Syslog sur ASA

Dans le journal système, vérifiez que la connexion IKEv2 a réussi.

<#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
```

Étape 4. Confirmer la session IPsec sur ASA

exécutez la commande runshow vpn-sessiondb detail anyconnect pour confirmer la session IKEv2/IPsec sur ASA.

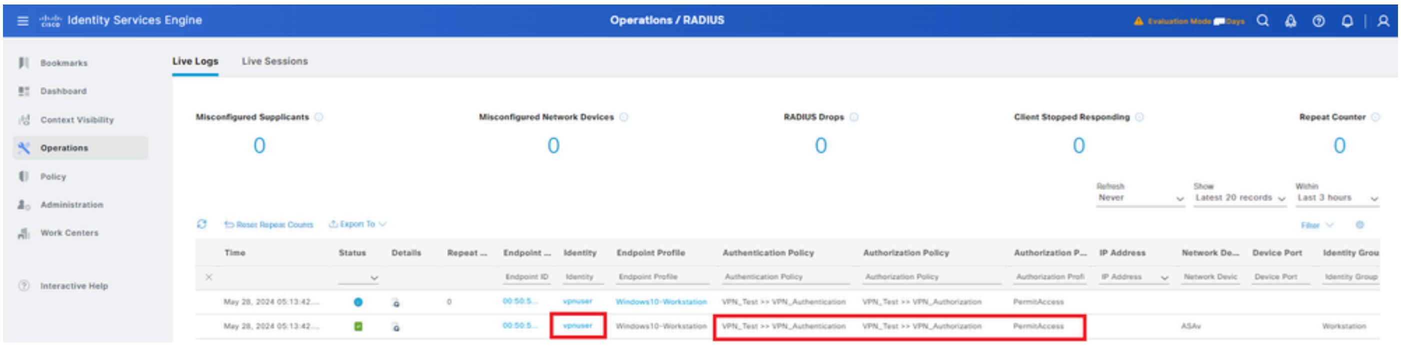
<#root>

```
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
```

Étape 5. Confirmer le journal Radius en direct

Accédez à **Operations** > **RADIUS** > **Live Login** ISE GUI, confirmez le journal en direct pour l'authentification vpn.



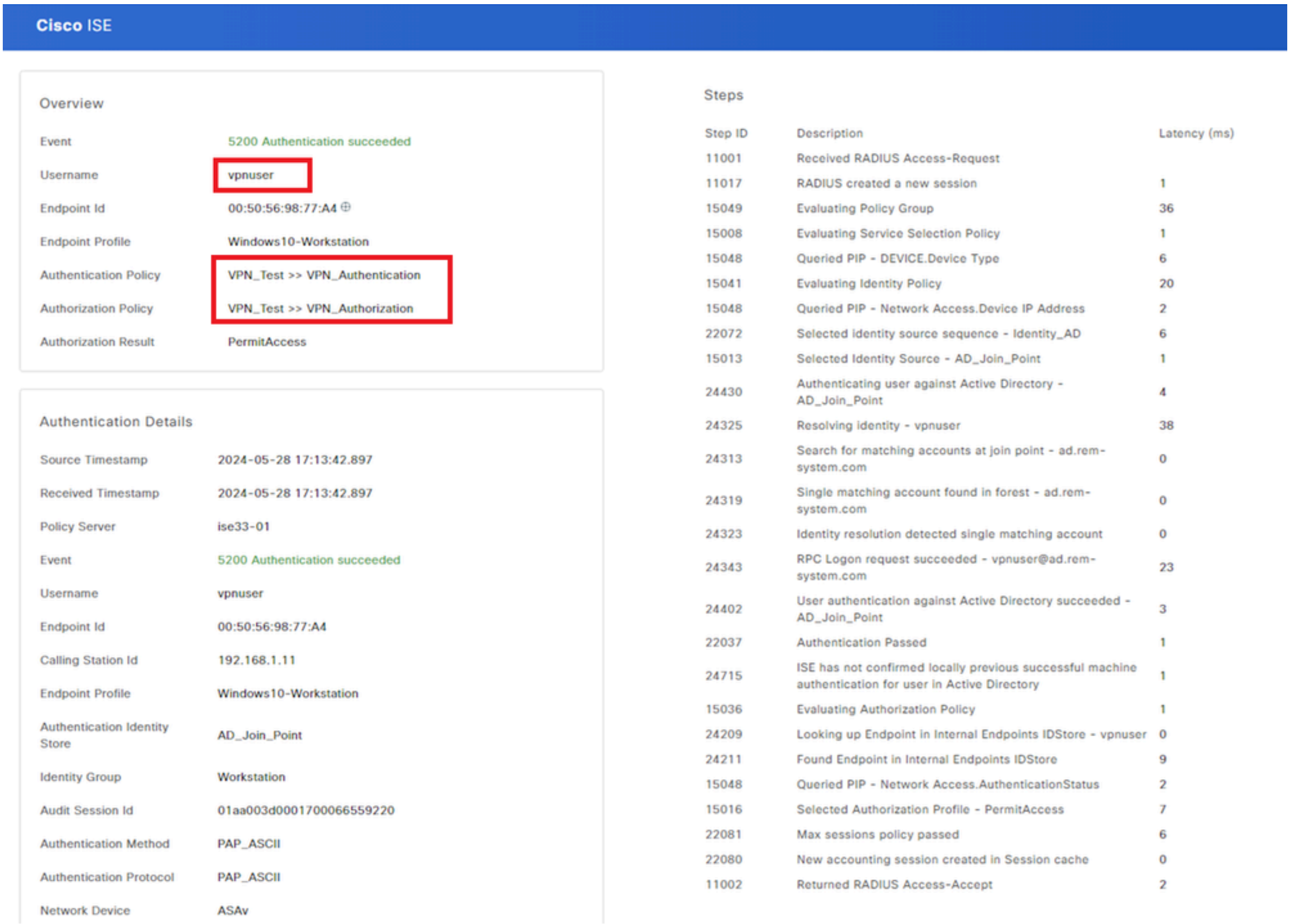
Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0 | Repeat Counter 0

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

Journal Radius Live

Cliquez sur Status pour confirmer les détails du journal en direct.



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

Détail du journal en direct

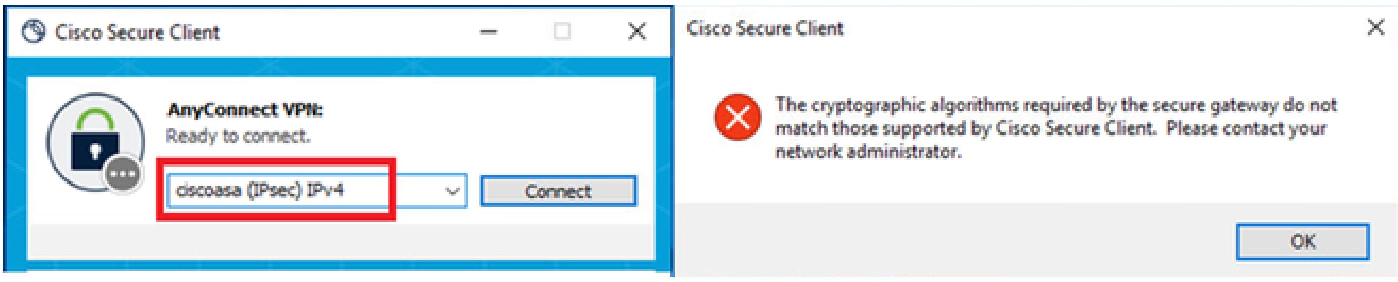
Dépannage

La non-concordance des algorithmes de chiffrement peut entraîner des échecs de connexion. Voici un exemple de problème de non-concordance d'algorithmes. L'exécution de l'étape 15 de la section Configuration dans ASDM peut résoudre le problème.

Étape 1. Initiation de la connexion VPN

Sur le terminal, exécutez le client sécurisé Cisco et vérifiez que la connexion a échoué en raison d'une non-concordance des algorithmes de chiffrement.

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



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

Échec de connexion

Étape 2. Confirmer Syslog dans CLI

Dans le journal système, vérifiez que la négociation IKEv2 a échoué.

<#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 ERI

Failed to find a matching policy
```

Référence

[AnyConnect sur IKEv2 vers ASA avec AAA et authentification par certificat]

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.