Configurar Secure Client IKEv2/ASA no ASDM com AAA & Cert Auth

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Diagrama de Rede

Configurações

- Configuração no ASDM
  - Etapa 1. Assistentes de VPN aberta
  - Etapa 2. Identificação do Perfil de Conexão
  - Etapa 3. Protocolos VPN
  - Etapa 4. Imagens do cliente
  - Etapa 5. Métodos de autenticação
  - Etapa 6. Configuração SAML
  - Passo 7. Designação de Endereço de Cliente
  - Etapa 8. Servidores de Resolução de Nomes de Rede
  - Etapa 9. Isento de NAT
  - Etapa 10. Implantação segura de cliente
  - Etapa 11. Salvar configurações
  - Etapa 12. Confirmar e exportar perfil de cliente seguro
  - Etapa 13. Confirmar detalhes do perfil de cliente seguro
  - Etapa 14. Confirmar configurações no ASA CLI
  - Etapa 15. Adicionar Algoritmo Criptográfico
- Configuração no Windows Server
- Configuração no ISE
  - Etapa 1. Adicionar dispositivo
  - Etapa 2. Adicionar Ative Diretory
  - Etapa 3. Adicionar sequência de origem de identidade
  - Etapa 4. Adicionar conjunto de políticas
  - Etapa 5. Adicionar política de autenticação
  - Etapa 6. Adicionar Política de Autorização

Verificar

- Etapa 1. Copiar Perfil de Cliente Seguro para Win10 PC1
- Etapa 2. Iniciar conexão VPN
- Etapa 3. Confirmar Syslog no ASA
- Etapa 4. Confirmar sessão IPsec no ASA
- Etapa 5. Confirmar registro ao vivo do Radius

Troubleshooting

- Etapa 1. Iniciar conexão VPN
- Etapa 2. Confirmar Syslog na CLI

Referência

Introdução

Este documento descreve as etapas necessárias para configurar o cliente seguro sobre IKEv2 no ASA usando ASDM com AAA e autenticação de certificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine (ISE)
- Configuração do Cisco Adaptive Security Virtual Appliance(ASAv)
- Configuração do Cisco Adaptive Security Device Manager (ASDM)
- Fluxo de autenticação de VPN

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity Services Engine Virtual 3.3 patch 1
- Dispositivo virtual de segurança adaptável 9.20(2)21
- Gerenciador de dispositivos de segurança adaptável 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

O nome de domínio configurado no Windows Server 2016 é ad.rem-system.com, usado como exemplo neste documento.

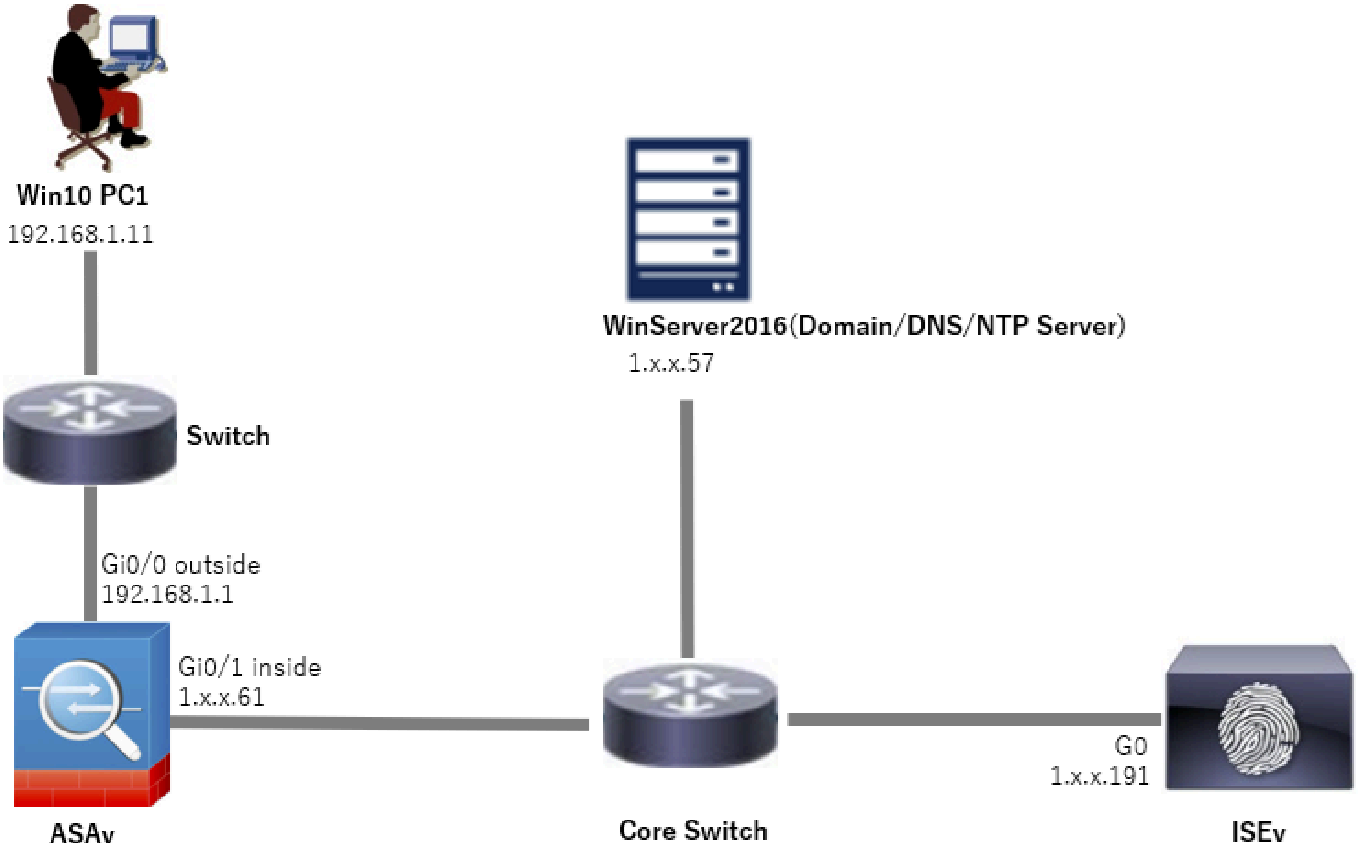


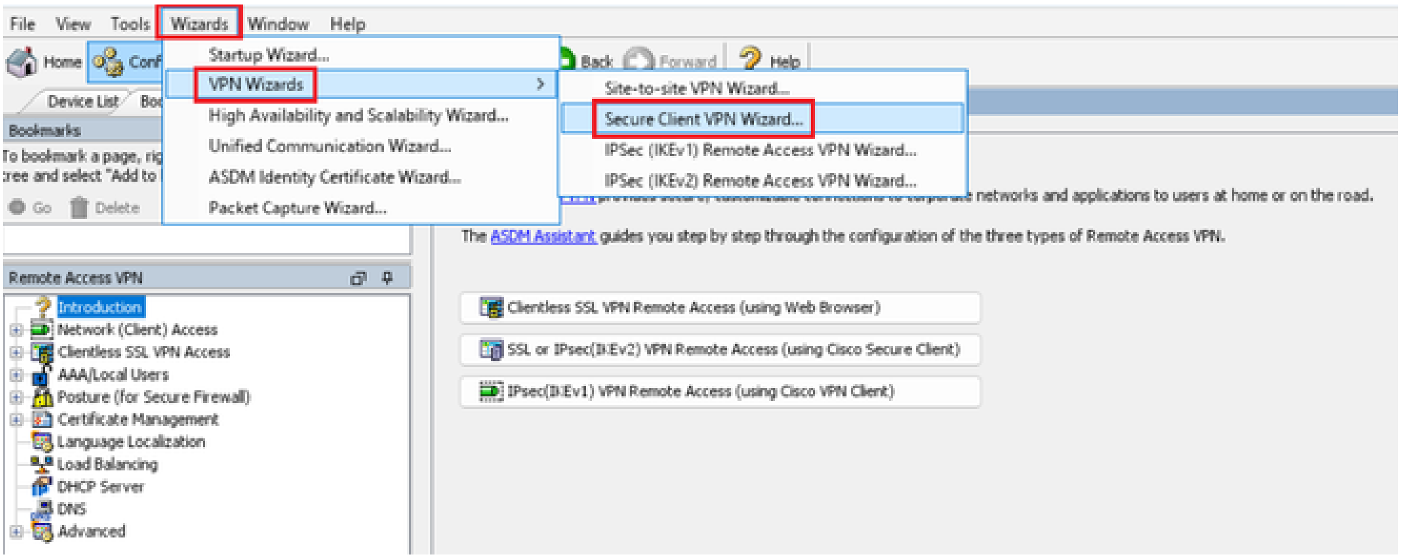
Diagrama de Rede

Configurações

Configuração no ASDM

Etapa 1. Assistentes de VPN aberta

Navegue até Wizards > VPN Wizards, clique em Secure Client VPN Wizard.


File View Tools Wizards Window Help
Home Conf
Back Forward Help
Device List Boo
Bookmarks
To bookmark a page, rig
tree and select "Add to
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

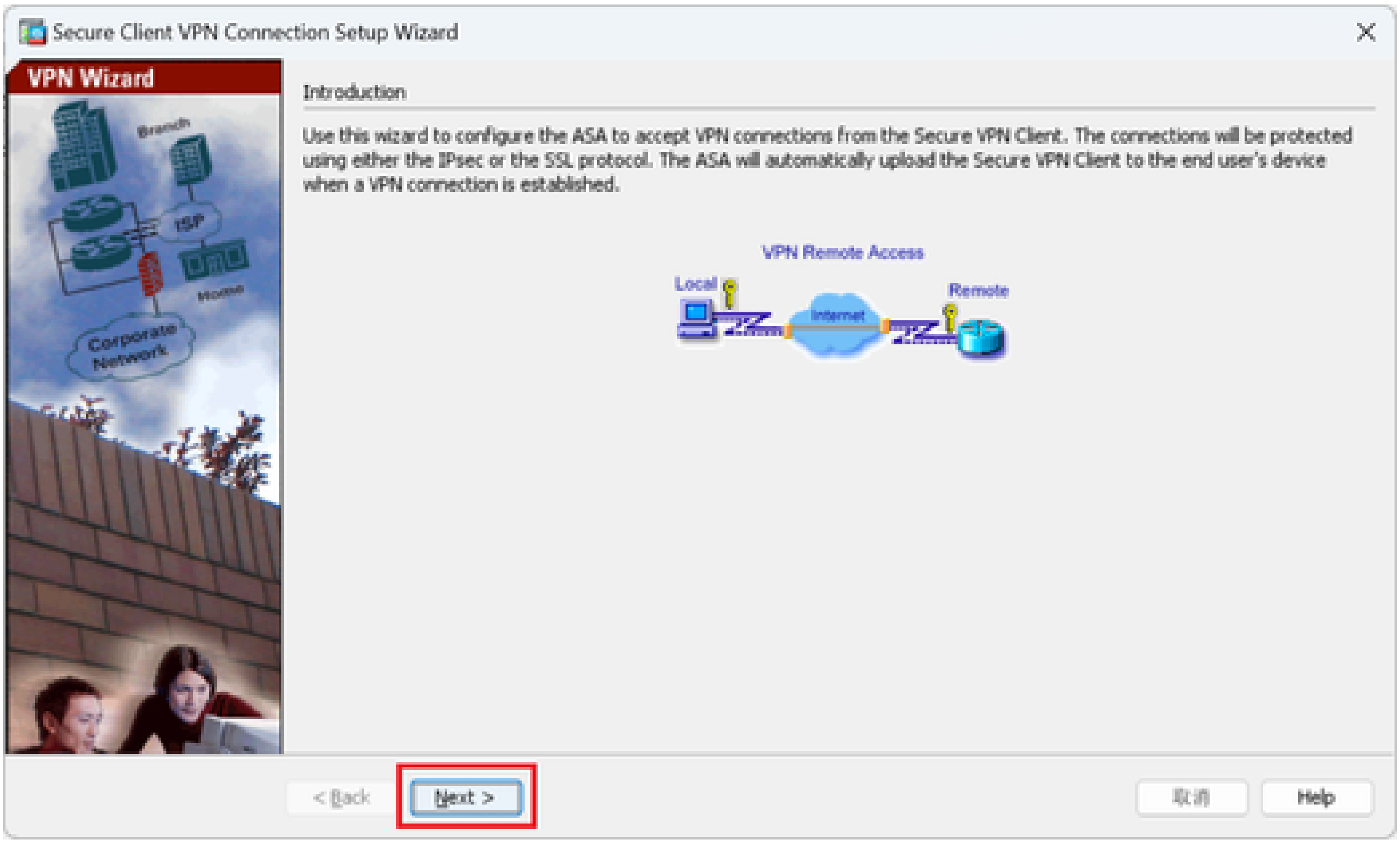
VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

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

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)

Assistentes de VPN aberta

Clique em Next.

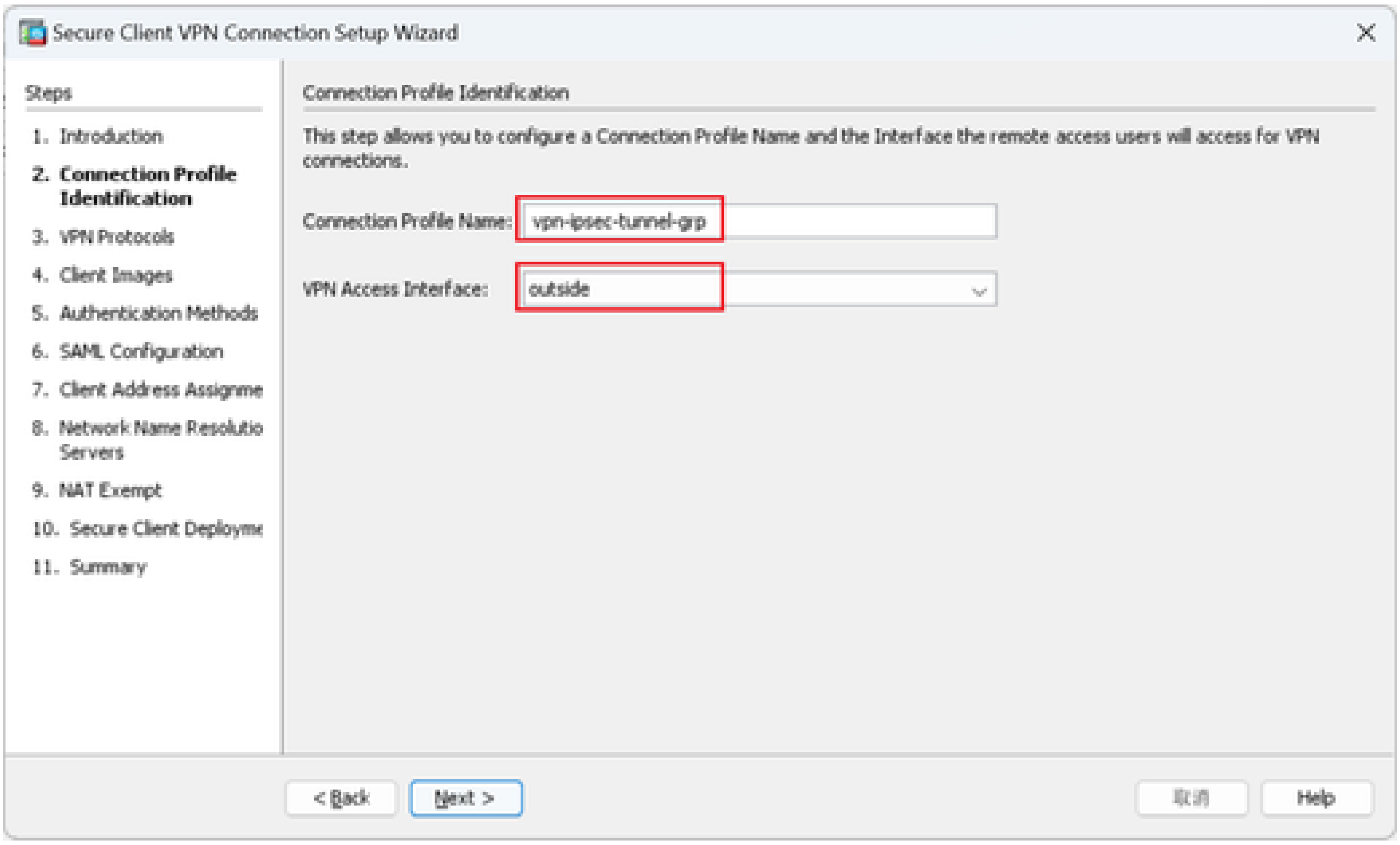


Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device when a VPN connection is established.

Clique no botão Avançar

Etapa 2. Identificação do Perfil de Conexão

Informações de entrada para o perfil de conexão.
Nome do perfil de conexão : vpn-ipsec-tunnel-grp
Interface de acesso VPN : exterior



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

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.

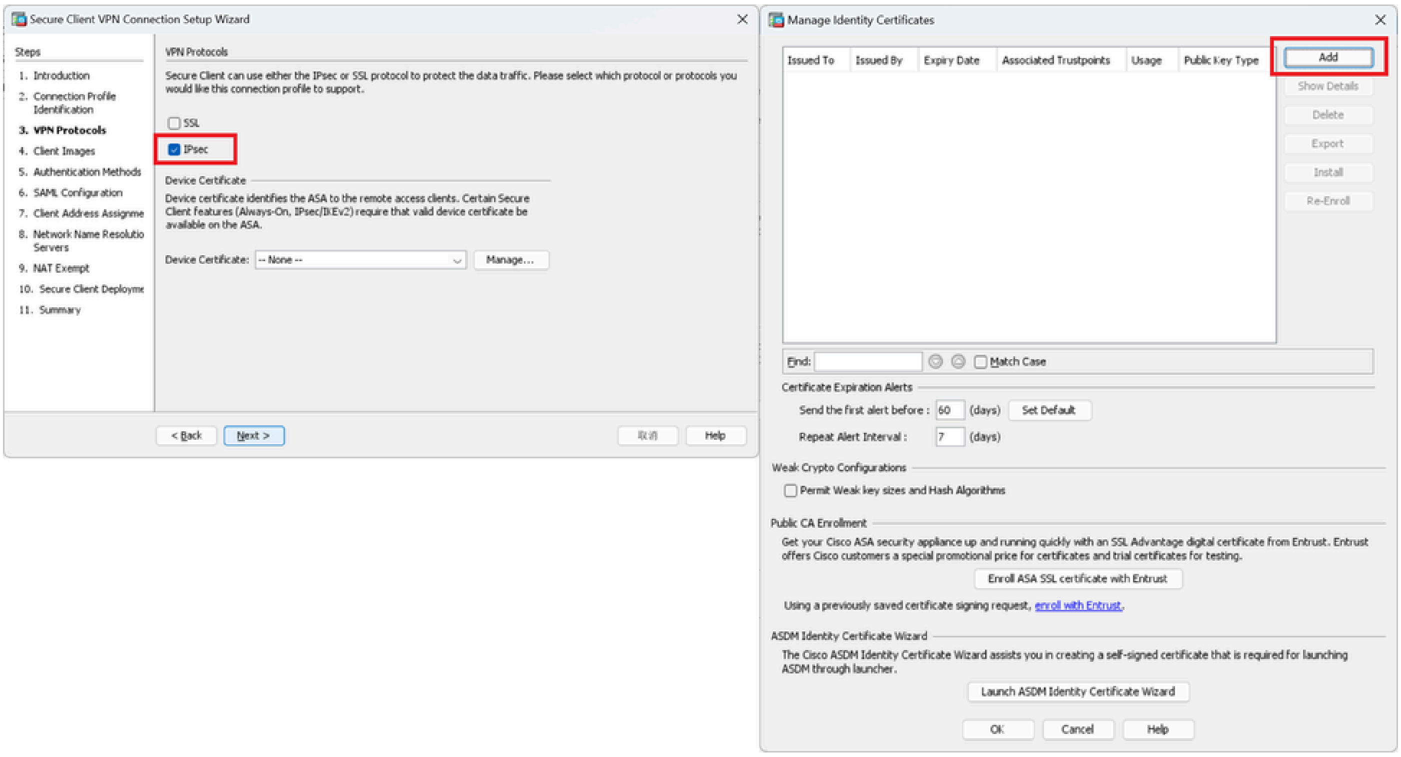
Connection Profile Name: vpn-ipsec-tunnel-grp

VPN Access Interface: outside

Identificação do Perfil de Conexão

Etapa 3. Protocolos VPN

Selecione IPsec, clique no botão Add para adicionar um novo certificado autoassinado.



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: -- 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

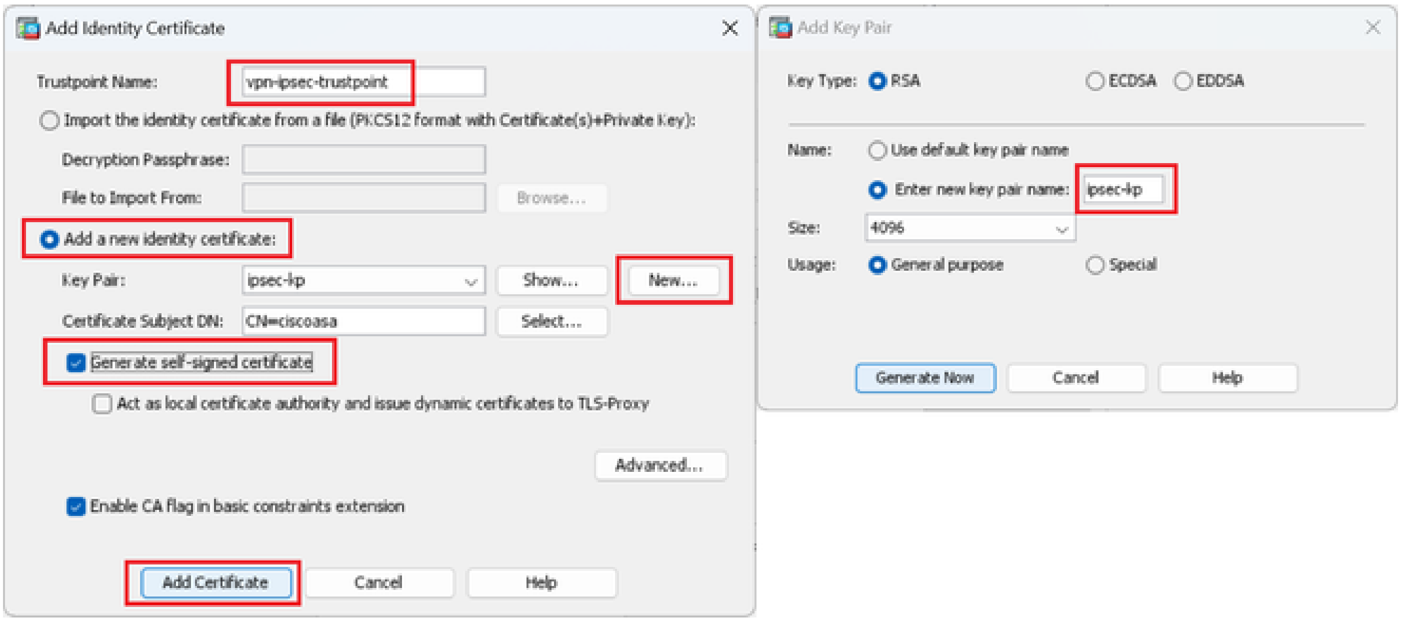
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

Protocolos VPN

Informações de entrada para certificado autoassinado.

Nome do ponto de confiança : vpn-ipsec-trustpoint

Par de chaves : 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: Browse...

● Add a new identity certificate:

Key Pair: ipsec-kp Show... New...

Certificate Subject DN: CN=ciscoasa Select...

☑ Generate self-signed certificate

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

Advanced...

☑ Enable CA flag in basic constraints extension

Add Certificate Cancel Help

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

● Enter new key pair name: ipsec-kp

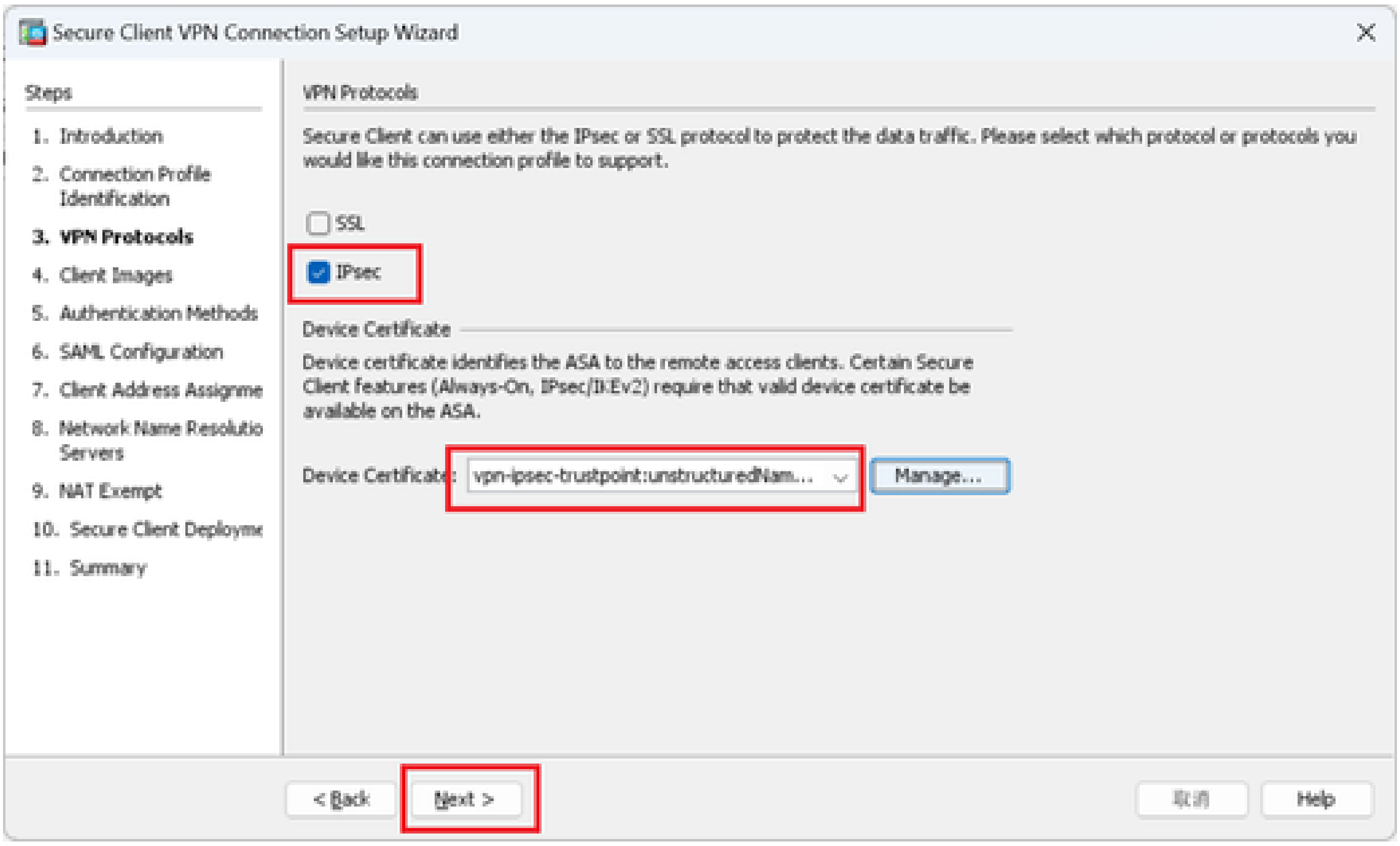
Size: 4096

Usage: ● General purpose ○ Special

Generate Now Cancel Help

Detalhes do certificado autoassinado

Confirme as configurações dos protocolos VPN e clique no botão 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.

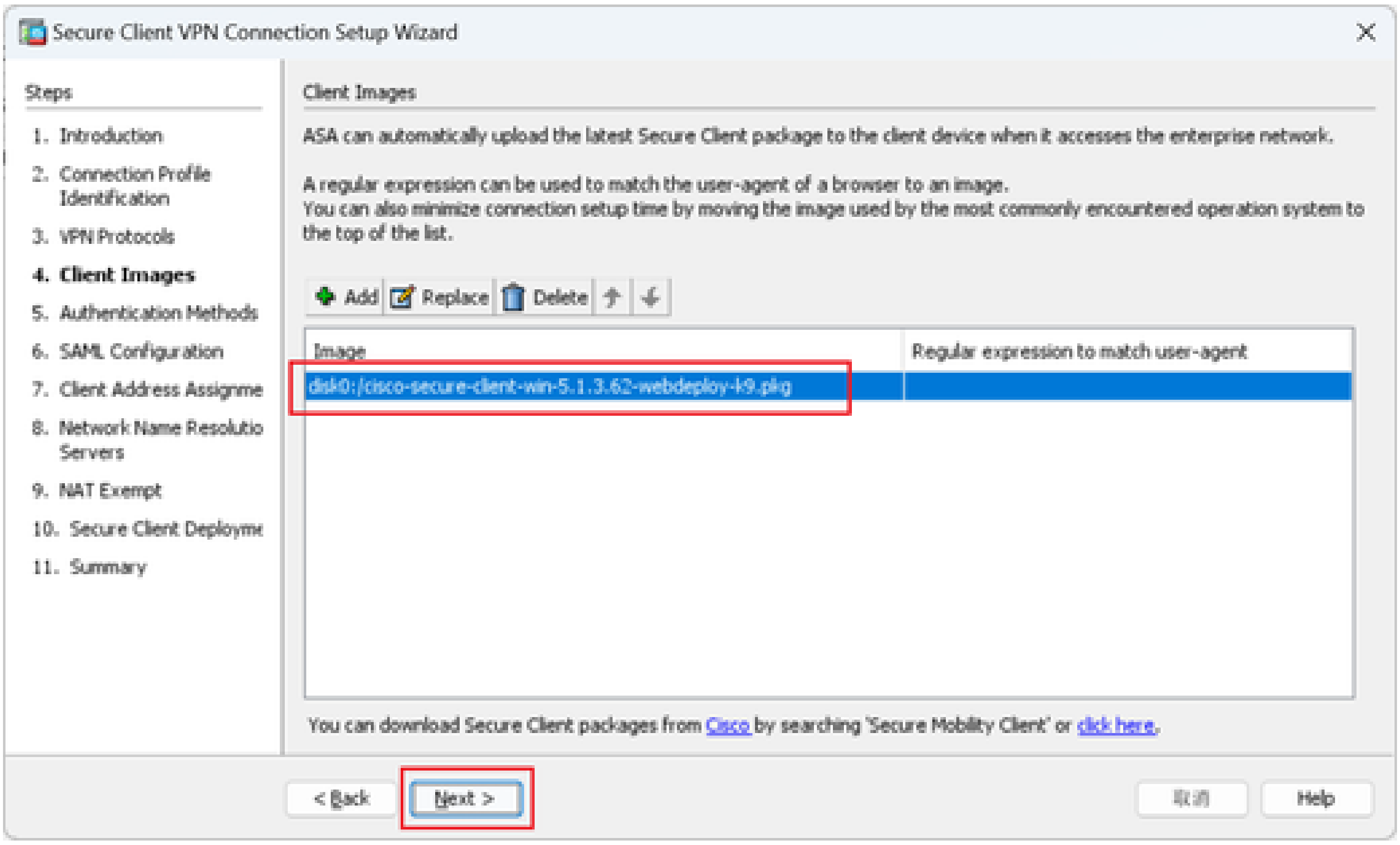
Device Certificate: vpn-ipsec-trustpoint:unstructuredNam... Manage...

< Back Next > 取消 Help

Confirmar configurações do protocolo VPN

Etapa 4. Imagens do cliente

Clique no botão Add para adicionar uma imagem de cliente segura e clique no botão 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

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.

Imagens do cliente

Etapa 5. Métodos de autenticação

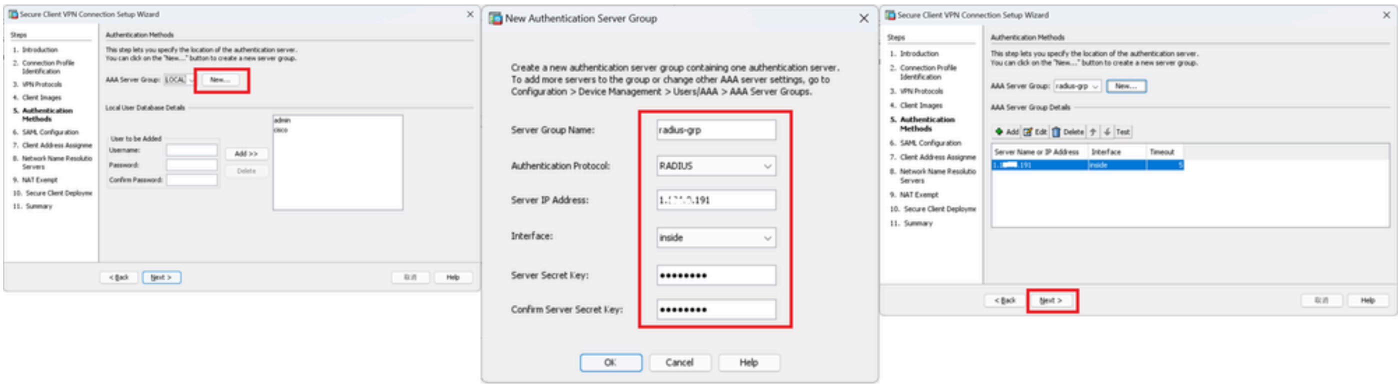
Clique no botão New para adicionar um novo servidor aaa, clique no botão Next.

Nome do grupo de servidores : radius-grp

Protocolo de autenticação : RADIUS

Endereço IP do servidor : 1.x.x.191

Interface : interna



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

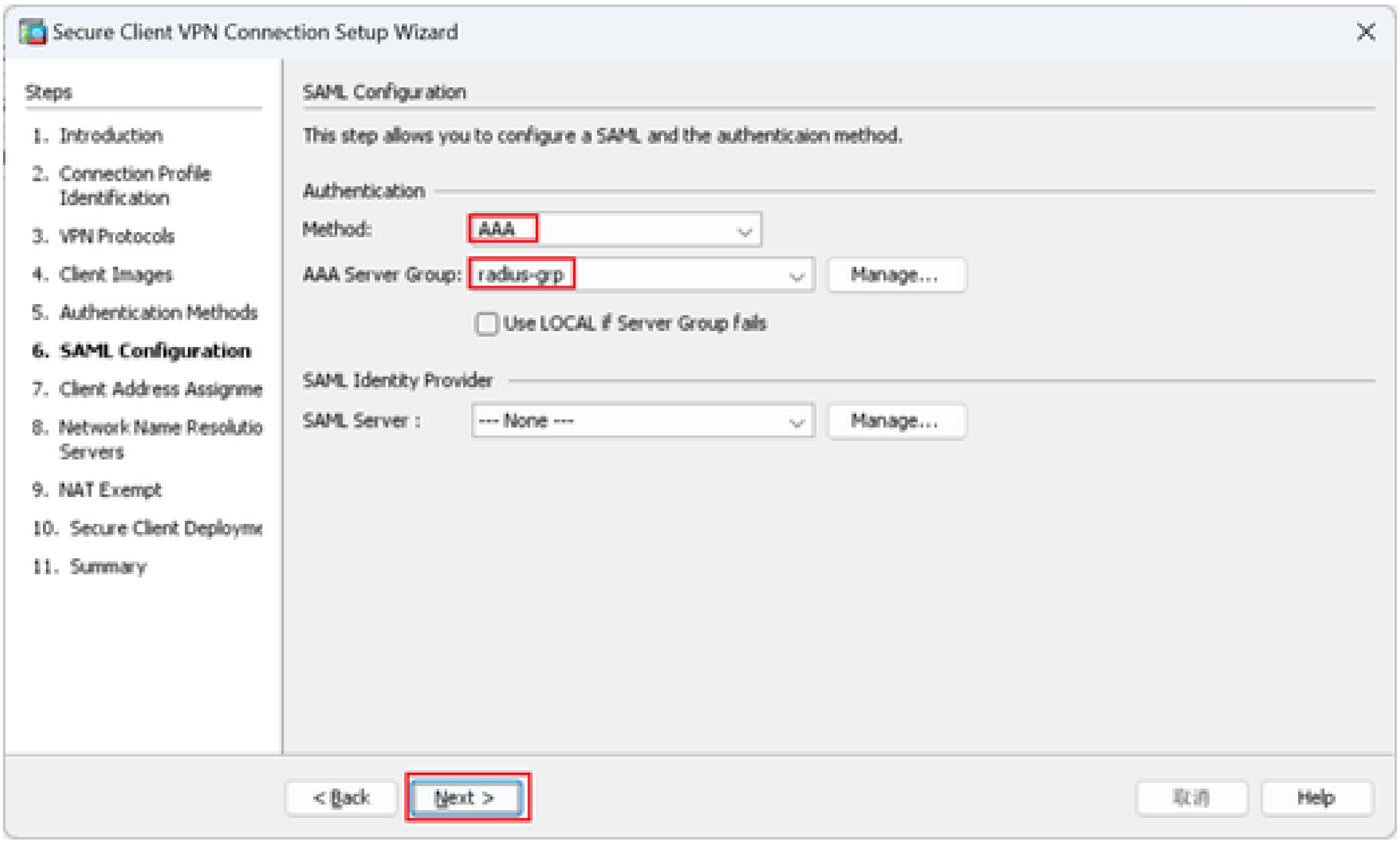
AAA Server Group Details

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

Métodos de autenticação

Etapa 6. Configuração SAML

Clique no botão Avançar.


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 ---

Configuração SAML

Passo 7. Designação de Endereço de Cliente

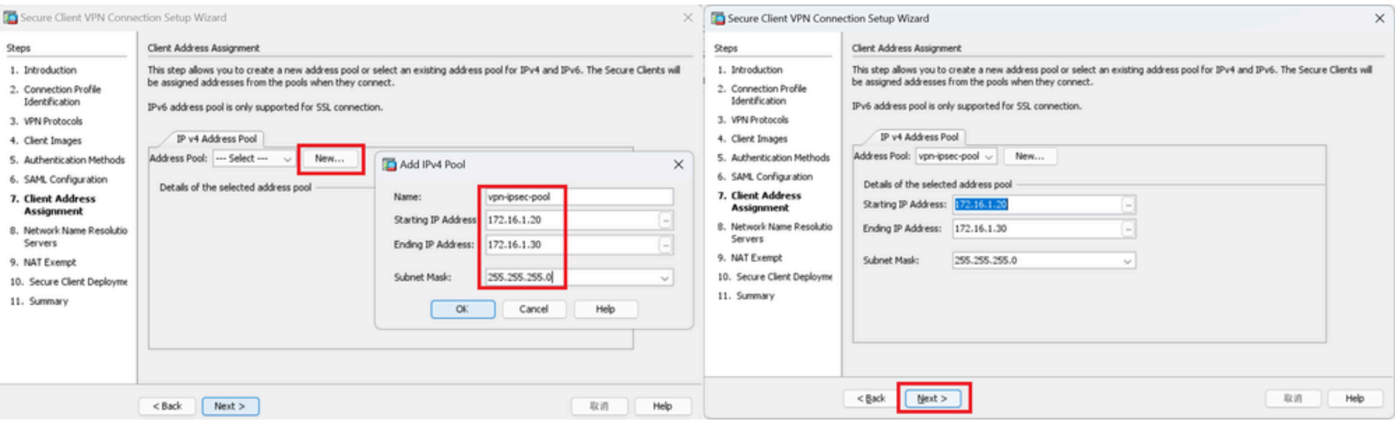
Clique no botão New para adicionar um novo pool IPv4 e clique no botão Next.

Nome : vpn-ipsec-pool

Endereço IP inicial: 172.16.1.20

Endereço IP final: 172.16.1.30

Máscara de sub-rede : 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

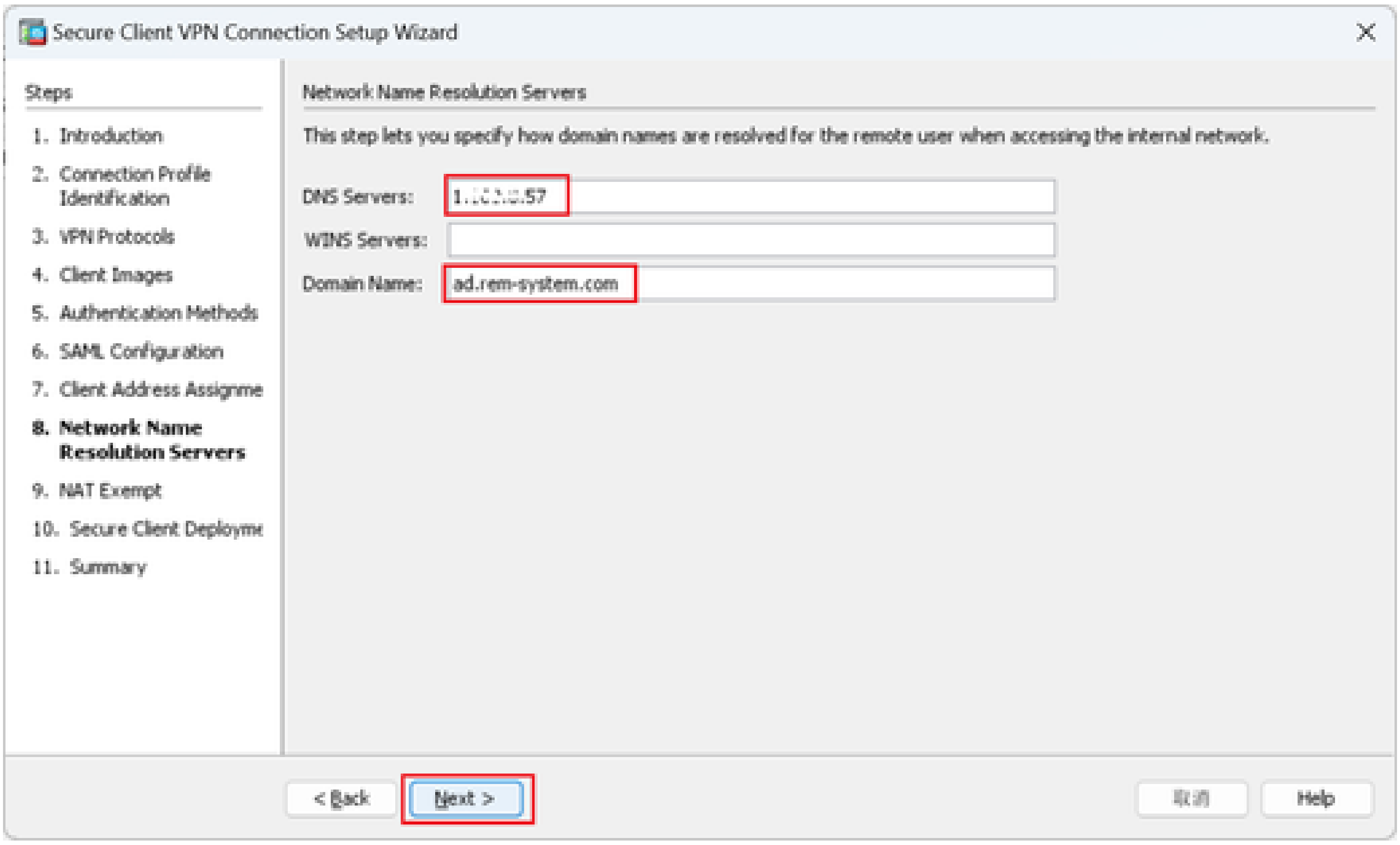
Atribuição de endereço de cliente

Etapa 8. Servidores de Resolução de Nomes de Rede

Insira informações para DNS e domínio, clique no botão Avançar.

Servidores DNS : 1.x.x.57

Nome do domínio: 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

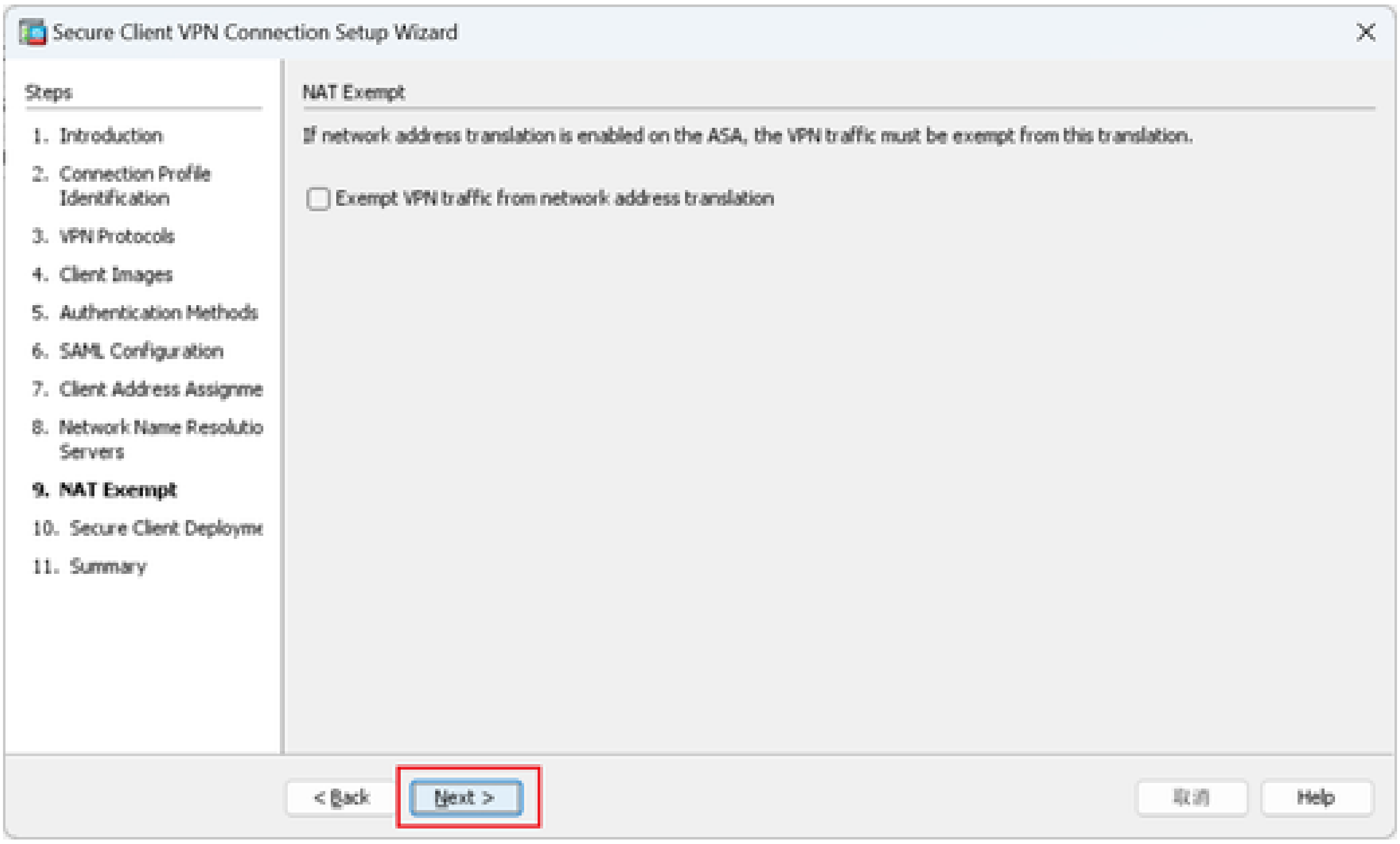
WINS Servers:

Domain Name: ad.rem-system.com

Servidores de Resolução de Nomes de Rede

Etapa 9. Isento de NAT

Clique no botão Avançar.



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.

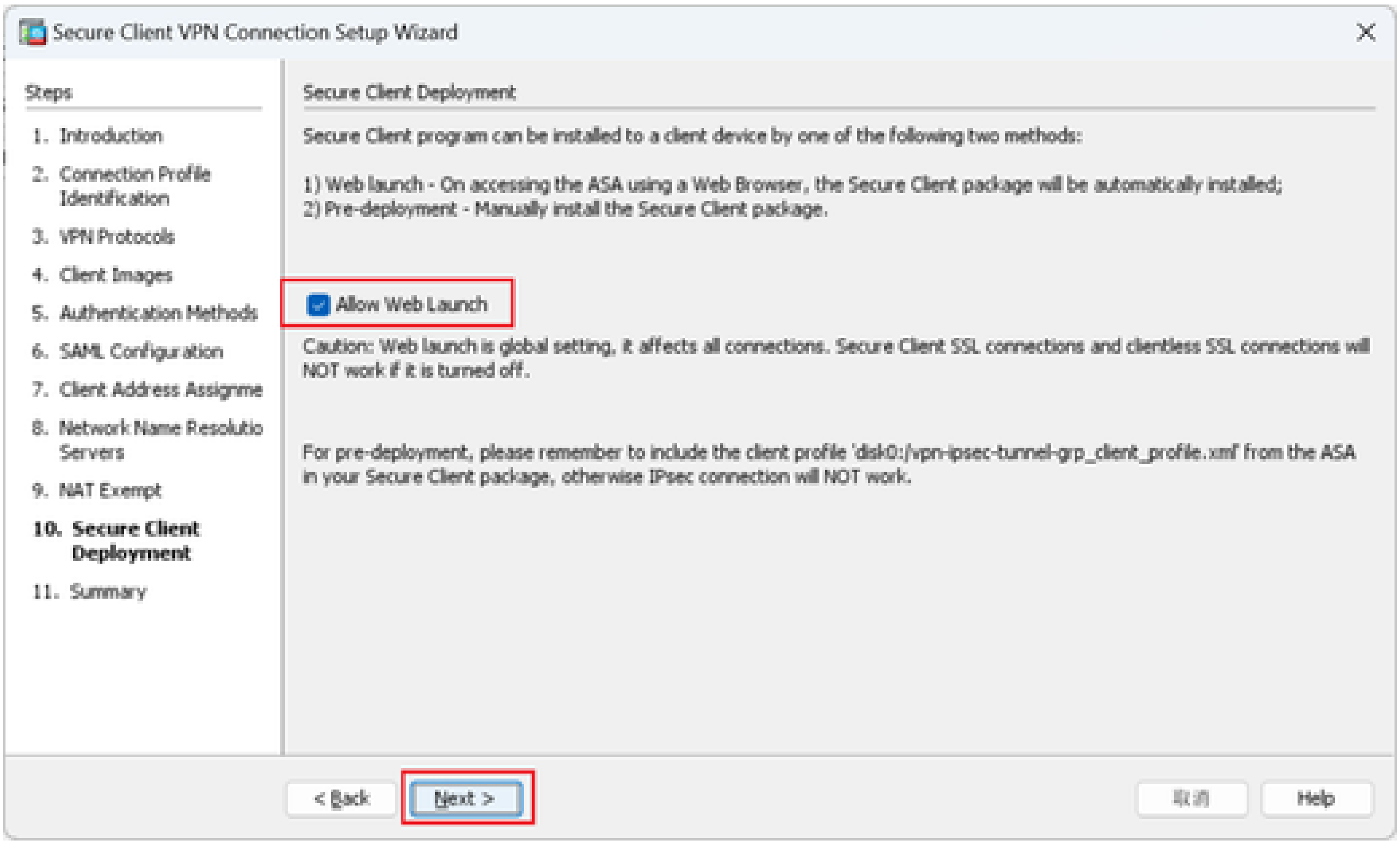
□ Exempt VPN traffic from network address translation

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

Isento de NAT

Etapa 10. Implantação segura de cliente

Selecione Allow Web Launch, clique no botão Next.



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

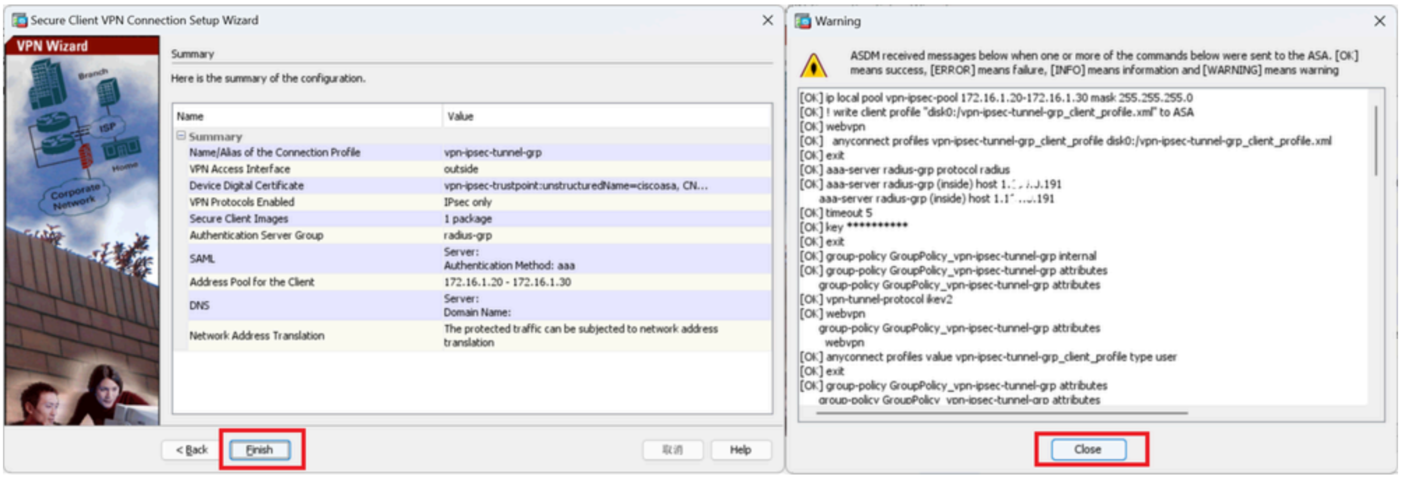
Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will NOT work if it is turned off.

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

Etapa 11. Salvar configurações

Clique no botão Finish e salve as configurações.



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

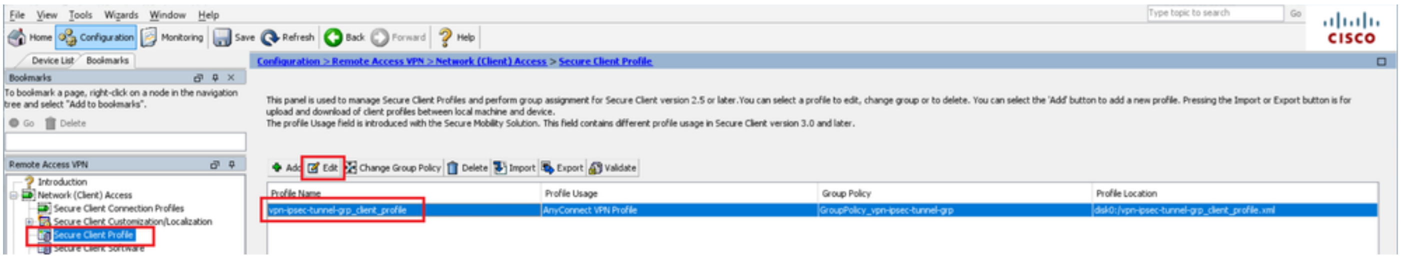
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[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
```

Salvar configurações

Etapa 12. Confirmar e exportar perfil de cliente seguro

Navegue para Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, clique no botão Edit.



File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Type topic to search
Go
cisco
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

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

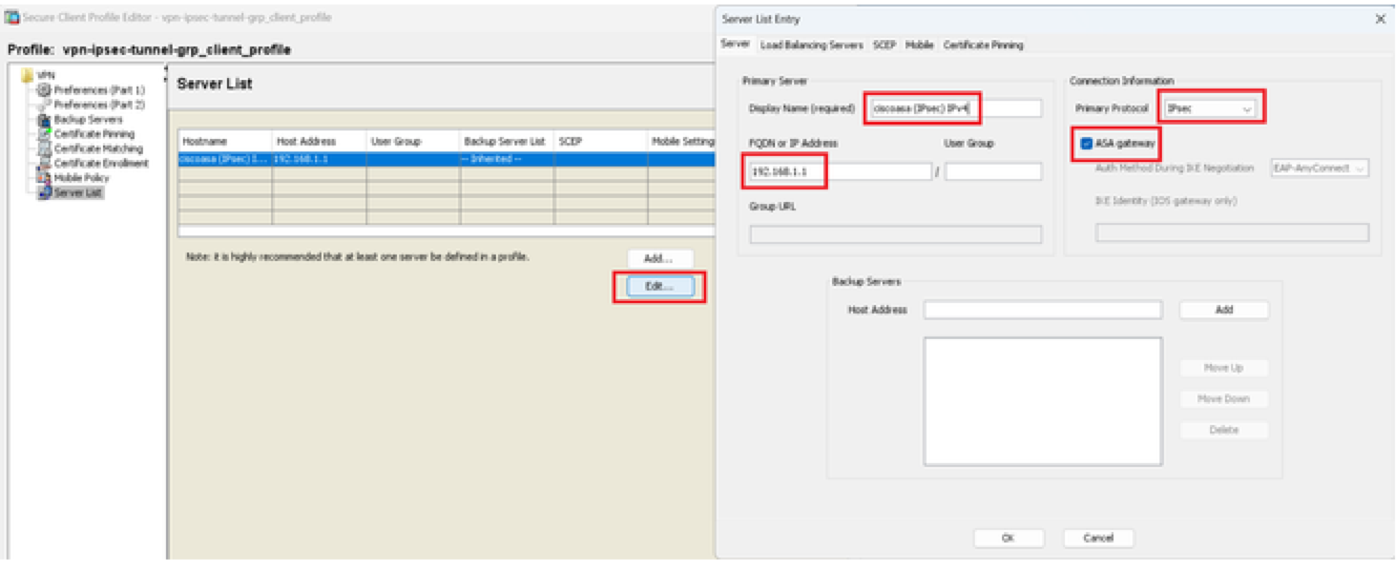
This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of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

Editar perfil de cliente seguro

Confirme os detalhes do perfil.

- Nome para Exibição (obrigatório): ciscoasa (IPsec) IPv4
- FQDN ou endereço IP : 192.168.1.1
- Protocolo primário: 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.

Server List Entry

Primary Server

Display Name (required): ciscoasa (IPsec) IPv4

FQDN or IP Address: 192.168.1.1

Connection Information

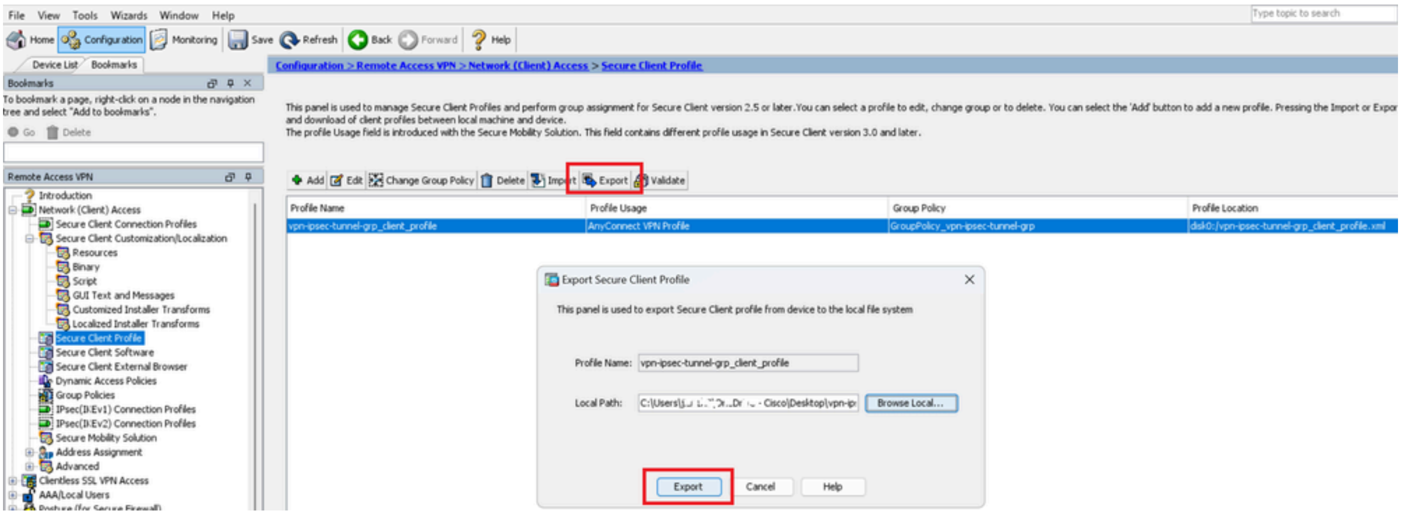
Primary Protocol: IPsec

☑ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

Confirmar perfil de cliente seguro

Clique no botão Export para exportar o perfil para o PC local.



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

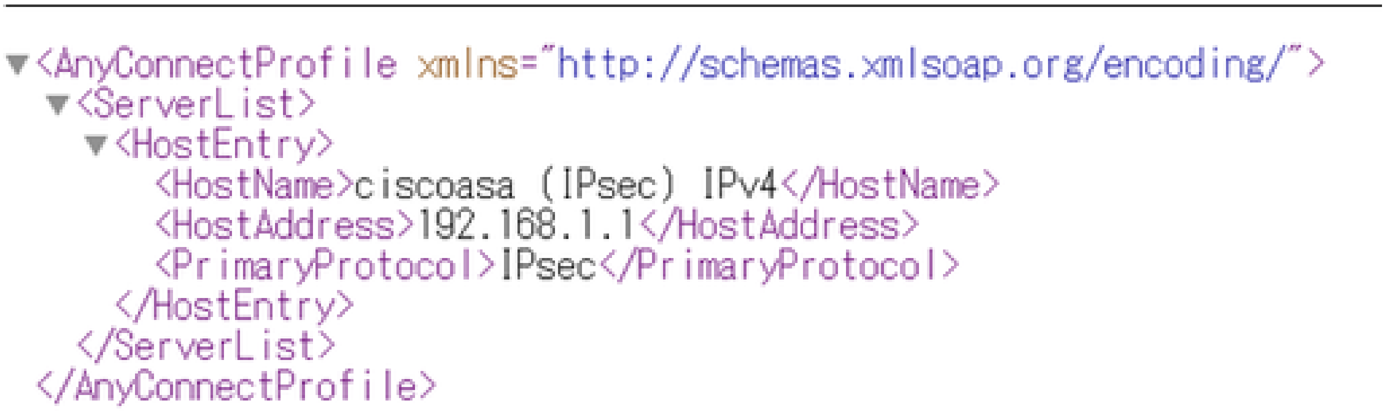
Profile Name: vpn-ipsec-tunnel-grp_client_profile

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

Exportar perfil de cliente seguro

Etapa 13. Confirmar detalhes do perfil de cliente seguro

Abra o Secure Client Profile pelo navegador e confirme se o protocolo principal para o host é o 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>
```

Detalhes do perfil de cliente seguro

Etapa 14. Confirmar configurações no ASA CLI

Confirme as configurações de IPsec criadas pelo ASDM na CLI do 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
```

Etapa 15. Adicionar Algoritmo Criptográfico

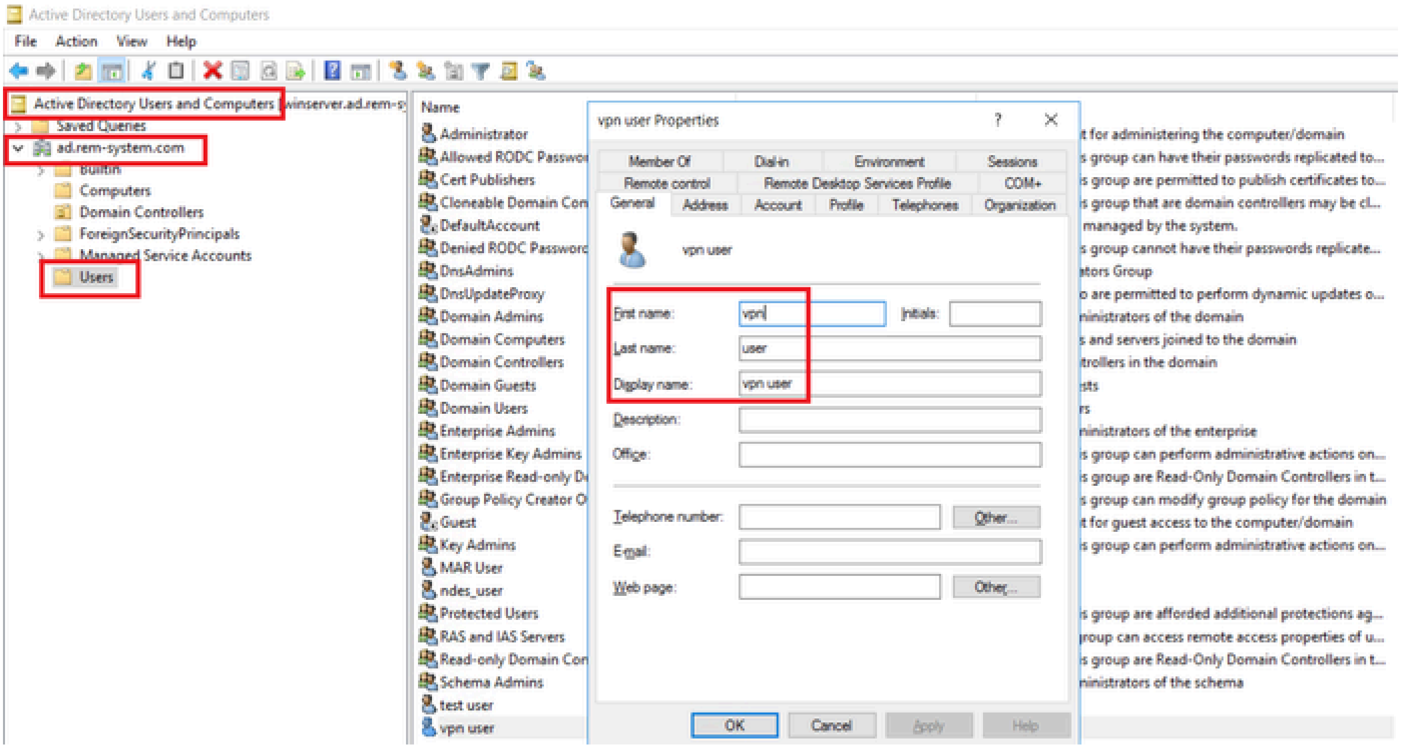
No CLI do ASA, adicione o grupo 19 à Política IKEv2.

Observação: para conexões IKEv2/IPsec, o Cisco Secure Client não oferece mais suporte a grupos Diffie-Hellman (DH) 2, 5, 14 e 24 a partir da versão 4.9.00086. Essa alteração pode resultar em falhas de conexão devido a incompatibilidades de algoritmo criptográfico.

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

Configuração no Windows Server

Você precisa adicionar um usuário de domínio para a conexão VPN. Navegue atéUsuários e computadores do Ative Diretory, clique emUsuários. Adicione vpnuser como usuário do domínio.



Active Directory Users and Computers

ad.rem-system.com

Users

vpn user Properties

General

vpn user

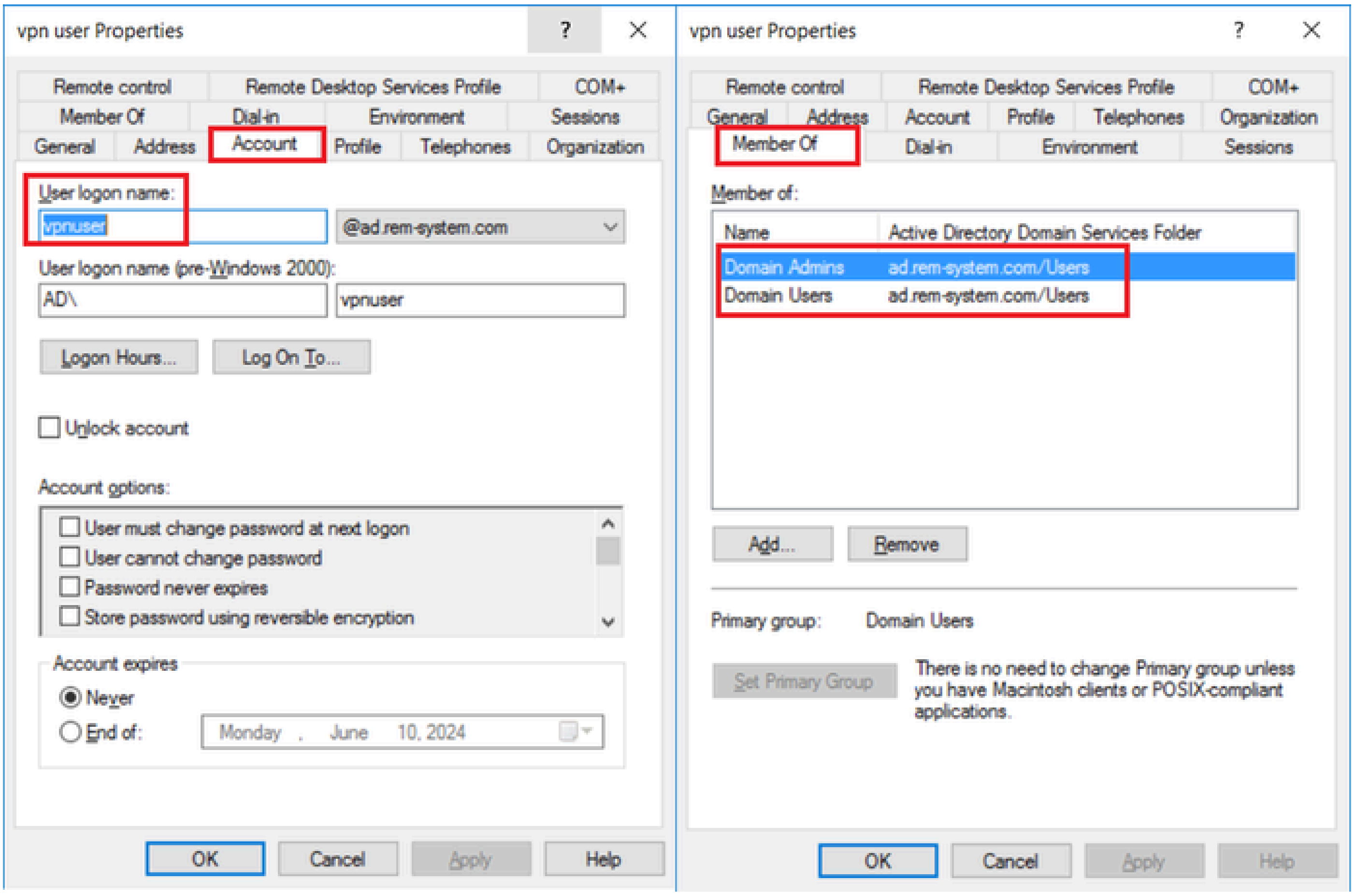
First name: vpn

Last name: user

Display name: vpn user

Adicionar usuário de domínio

Adicione o usuário de domínio ao membro de Admins. do Domínio e Usuários do Domínio.



vpn user Properties

Account

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

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

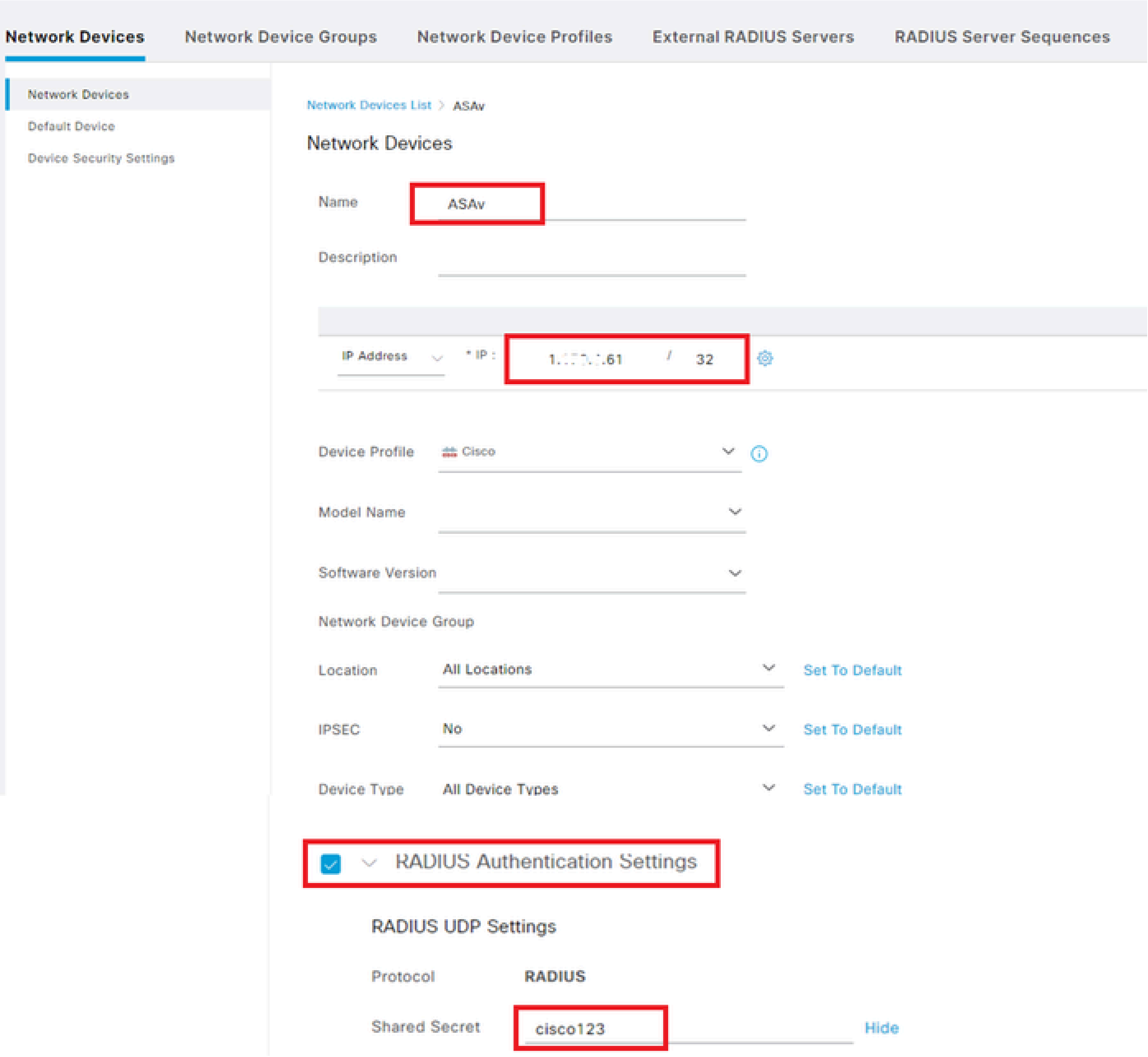
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Admins. e Usuários do Domínio

Configuração no ISE

Etapa 1. Adicionar dispositivo

Navegue para Administração > Dispositivos de rede, clique no botão Adicionar para adicionar o dispositivo 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

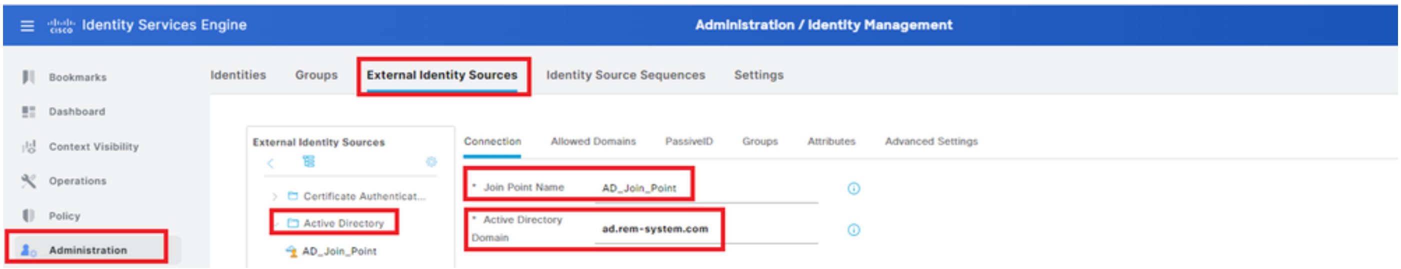
Shared Secret: cisco123 — Hide

Adicionar dispositivo

Etapa 2. Adicionar Ative Diretory

Navegue até Administração > Fontes de identidade externas > Ative Diretory, clique na guiaConexão e adicione o Ative Diretory ao ISE.

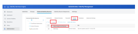
- Nome do ponto de junção: AD_Join_Point
- Domínio do Ative Diretory: ad.rem-system.com



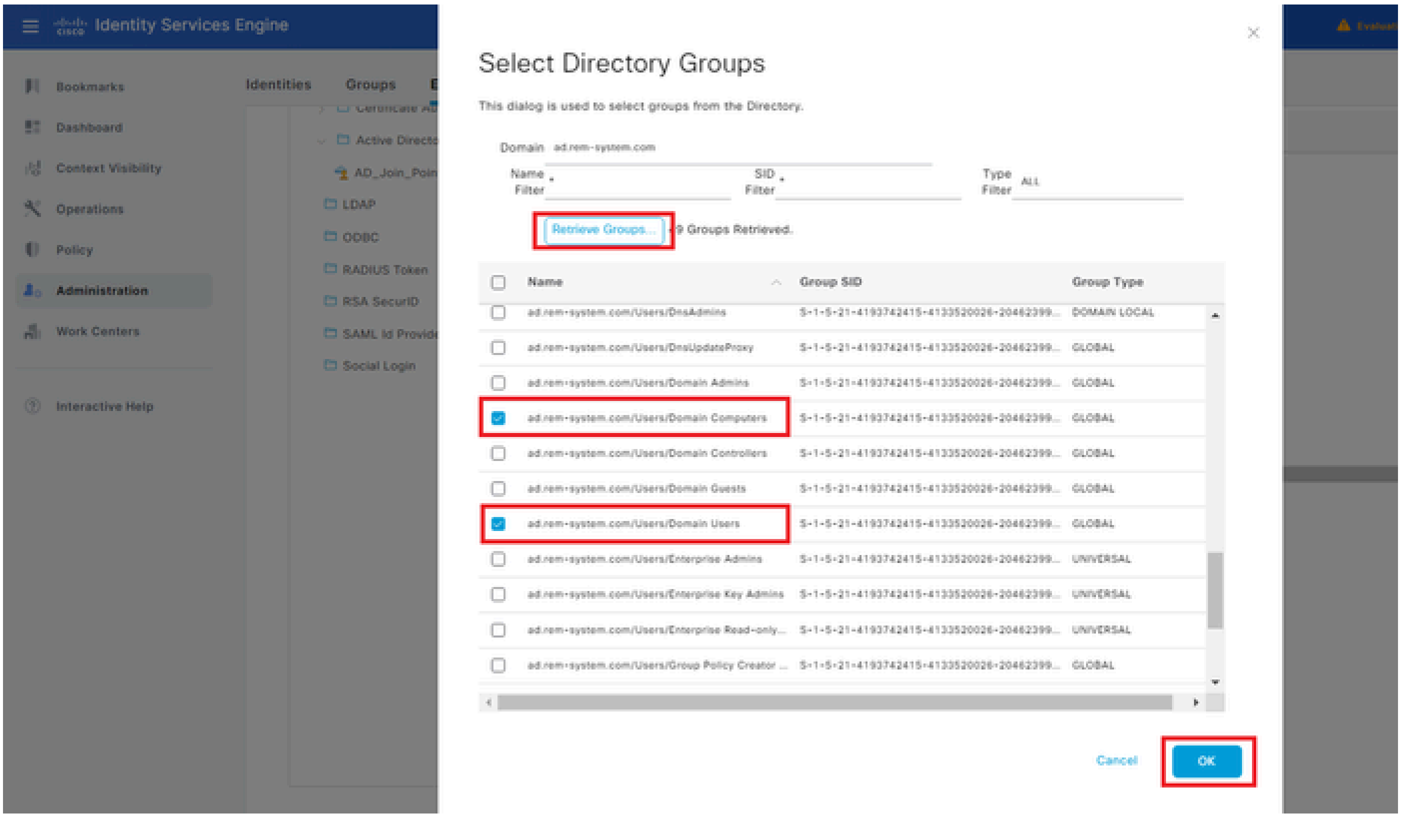
* Join Point Name: AD_Join_Point

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

Adicionar Ative Diretory

Navegue até a guia Grupos e selecione Selecionar grupos do diretório na lista suspensa.  Selecione grupos do diretório

Clique em Recuperar grupos na lista suspensa. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Usuários e clique em 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.

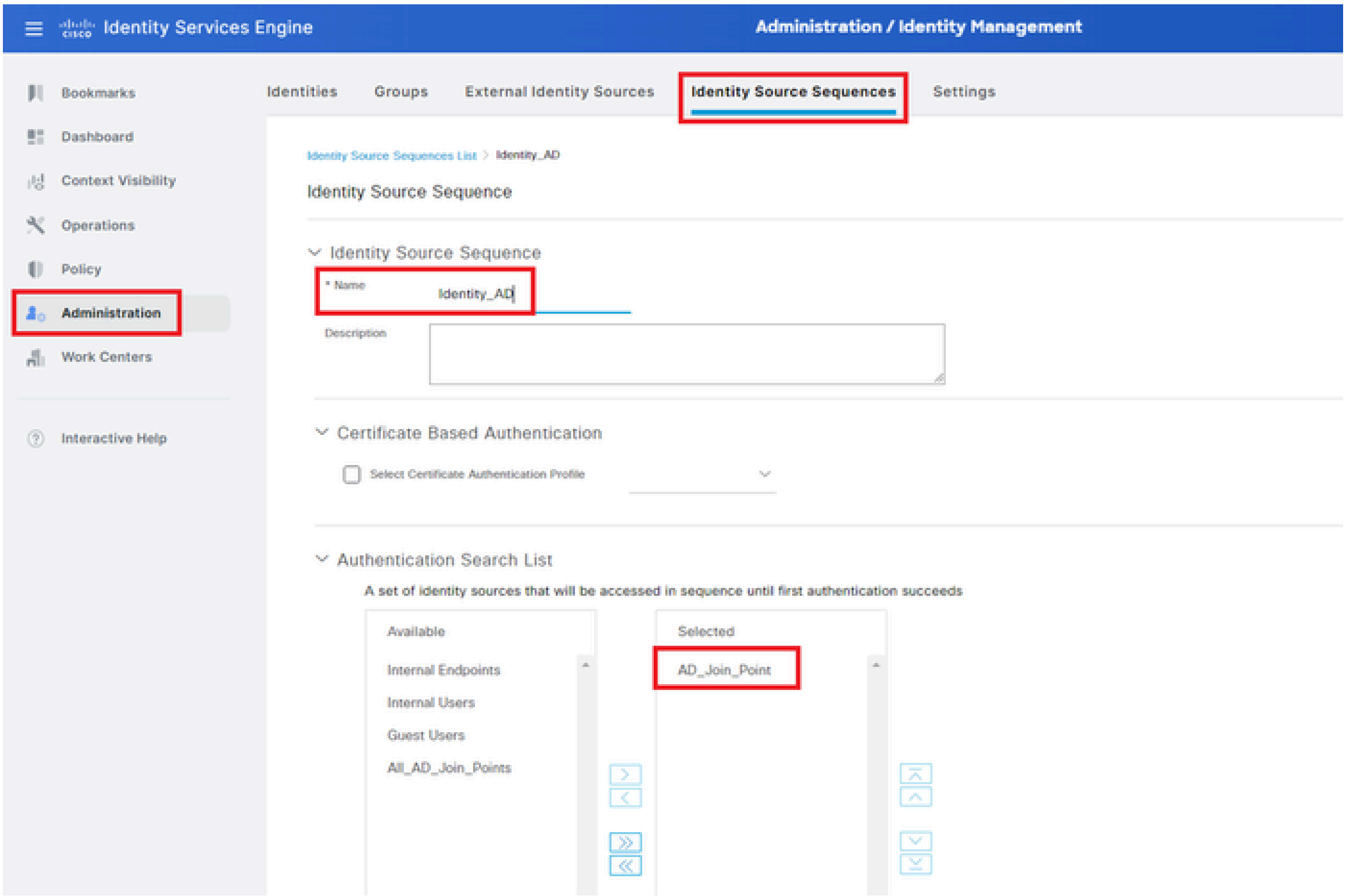
□	Name	Group SID	Group Type
□	ad.rem-system.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
□	ad.rem-system.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
□	ad.rem-system.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL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

Adicionar computadores e usuários de domínio

Etapa 3. Adicionar sequência de origem de identidade

Navegue até Administração > Sequências de origem de identidade, adicione uma Sequência de origem de identidade.

- Nome: Identity_AD
- Lista de pesquisa de autenticação: 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

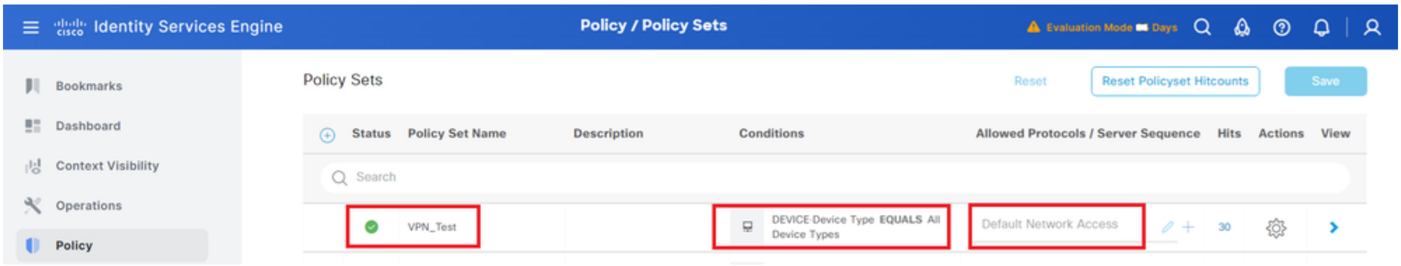
Available	Selected
Internal Endpoints	AD_Join_Point
Internal Users	
Guest Users	
All_AD_Join_Points	

Adicionar Sequências de Origem de Identidade

Etapa 4. Adicionar conjunto de políticas

Navegue para Política > Conjuntos de políticas, clique em + para adicionar um conjunto de políticas.

- Nome do conjunto de políticas: VPN_Test
- Condições : Tipo de dispositivo de dispositivo IGUAL a todos os tipos de dispositivo
- Protocolos Permitidos/Sequência de Servidores: Acesso Padrão à Rede



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		>

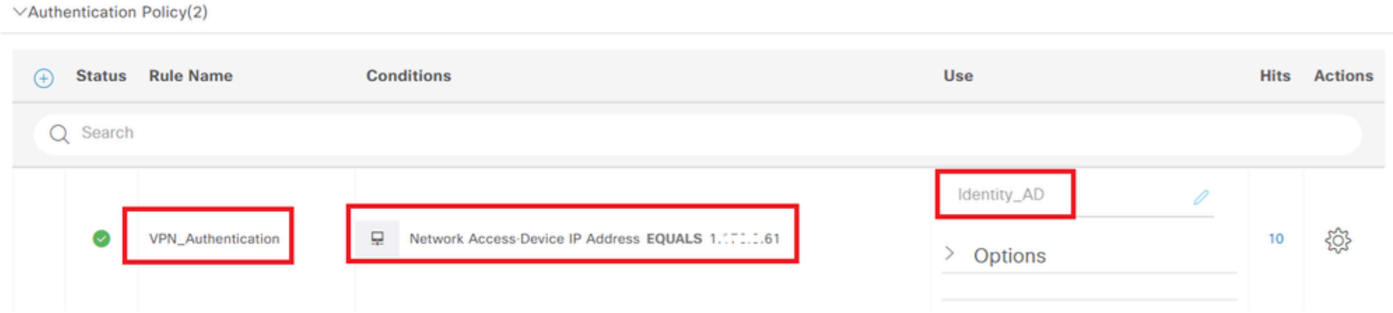
Adicionar conjunto de políticas

Etapa 5. Adicionar política de autenticação

Navegue para Policy Sets, clique em VPN_Test para adicionar uma política de autenticação.

- Nome da regra : VPN_Authentication
- Condições : endereço IP do dispositivo de acesso à rede IGUAL a 1.x.x.61

- Uso: Identity_AD



Authentication Policy(2)

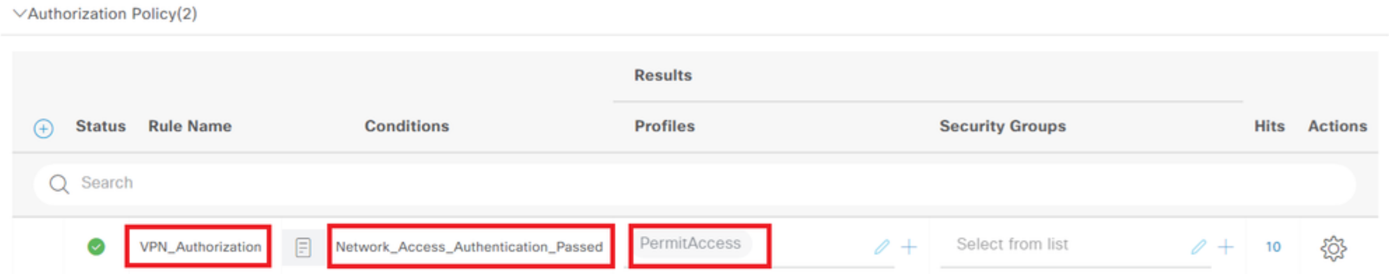
Status	Rule Name	Conditions	Use	Hits	Actions
✓	VPN_Authentication	Network Access·Device IP Address EQUALS 1.[redacted].61	Identity_AD Options	10	⚙

Adicionar política de autenticação

Etapa 6. Adicionar Política de Autorização

Navegue até Policy Sets, clique em VPN_Test para adicionar uma política de autorização.

- Nome da regra : VPN_Authorization
- Condições : Network_Access_Authentication_Passed
- Resultados: PermitAccess



Authorization Policy(2)

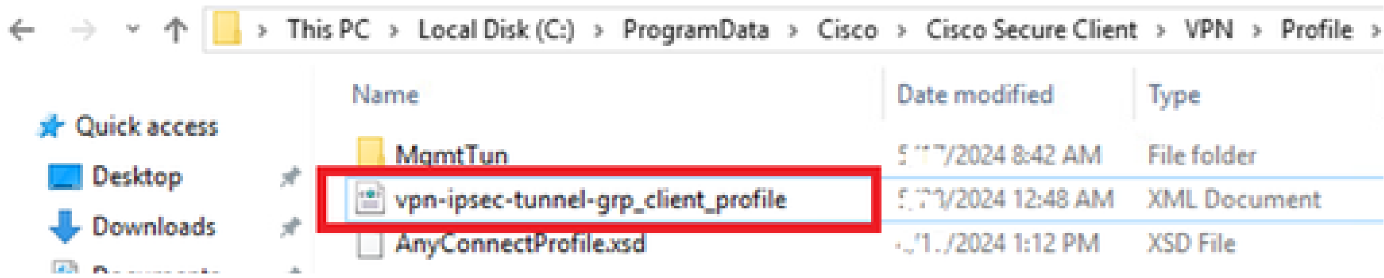
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	⚙

Adicionar política de Autorização

Verificar

Etapa 1. Copiar Perfil de Cliente Seguro para Win10 PC1

Copie o perfil de cliente seguro para o diretório C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



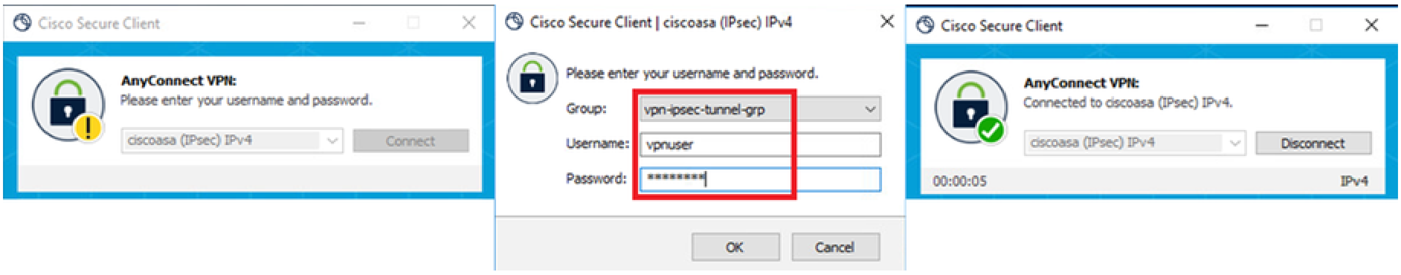
This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > VPN > Profile >

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

Copiar perfil para PC

Etapa 2. Iniciar conexão VPN

No endpoint, execute o Cisco Secure Client, insira o nome de usuário e a senha e, em seguida, confirme se o Cisco Secure Client se conecta com êxito.



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

Conexão bem-sucedida

Etapa 3. Confirmar Syslog no ASA

No syslog, confirme se a conexão IKEv2 foi bem-sucedida.

<#root>

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

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 I
```

Etapa 4. Confirmar sessão IPsec no ASA

execute show vpn-sessiondb detail anyconnect o comando para confirmar a sessão IKEv2/IPsec no ASA.

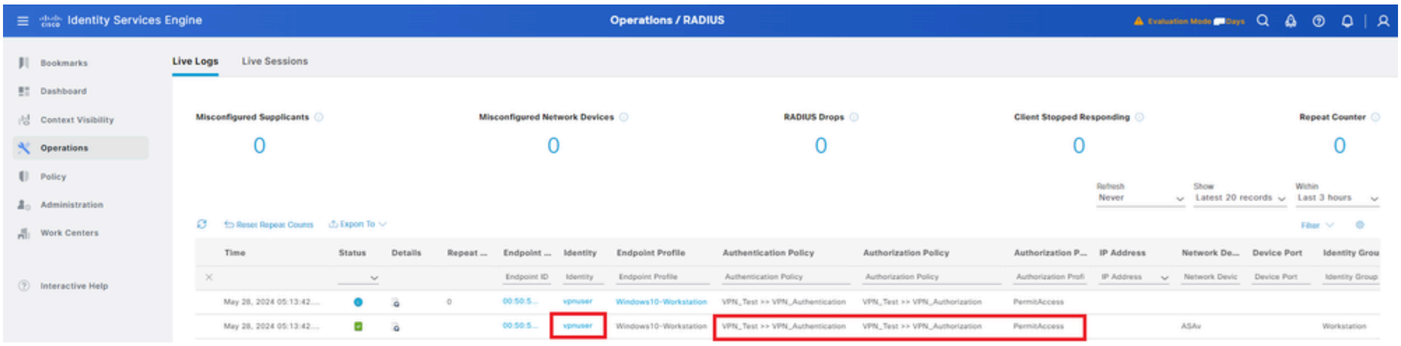
<#root>

```
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
```

Etapa 5. Confirmar registro ao vivo do Radius

Navegue até **Operations** > **RADIUS** > **Live** Logons na GUI do ISE, confirme o registro ao vivo para autenticação da vpn.



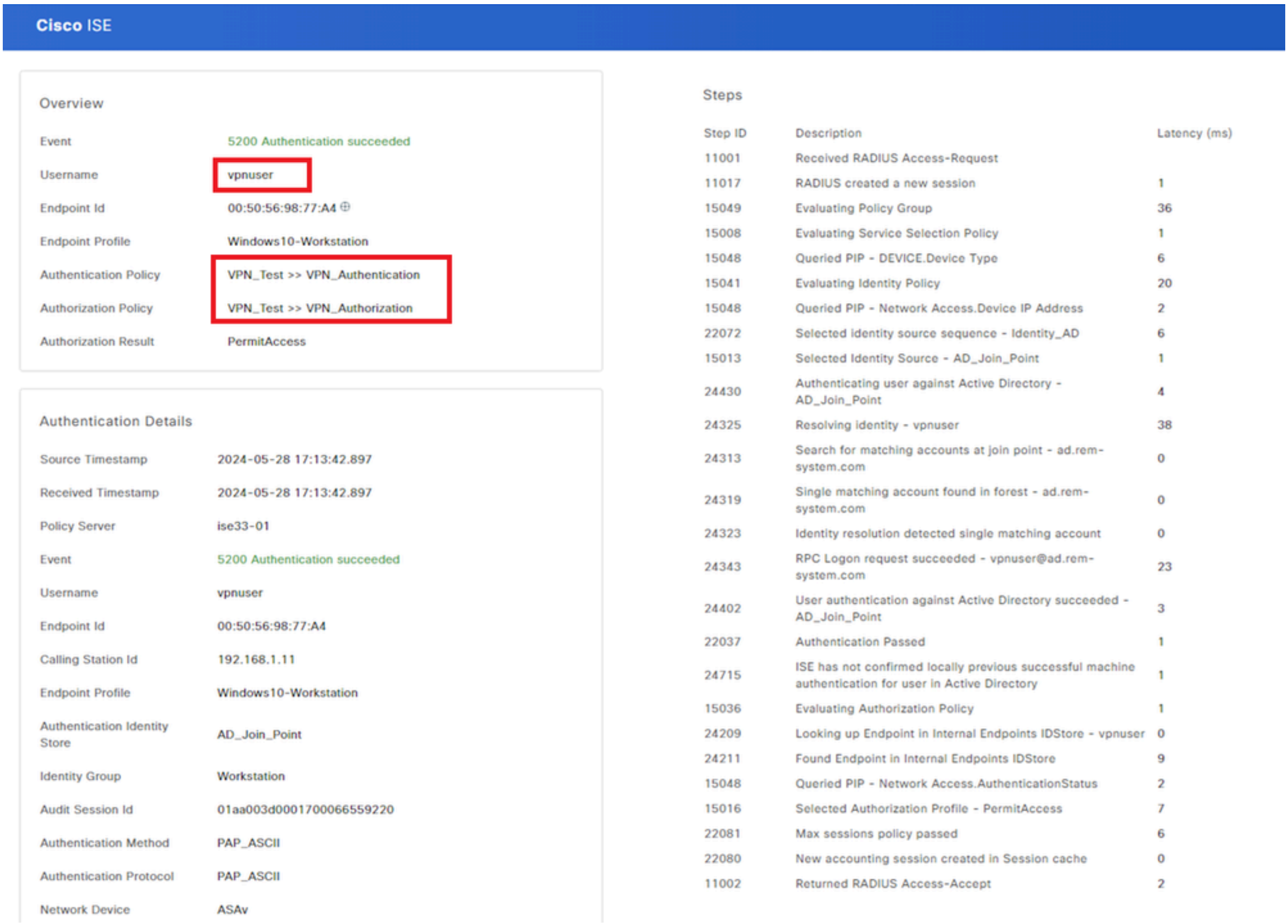
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

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

Log ao vivo do Radius

Clique em Status para confirmar os detalhes do log ao vivo.



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

Detalhe do Log ao Vivo

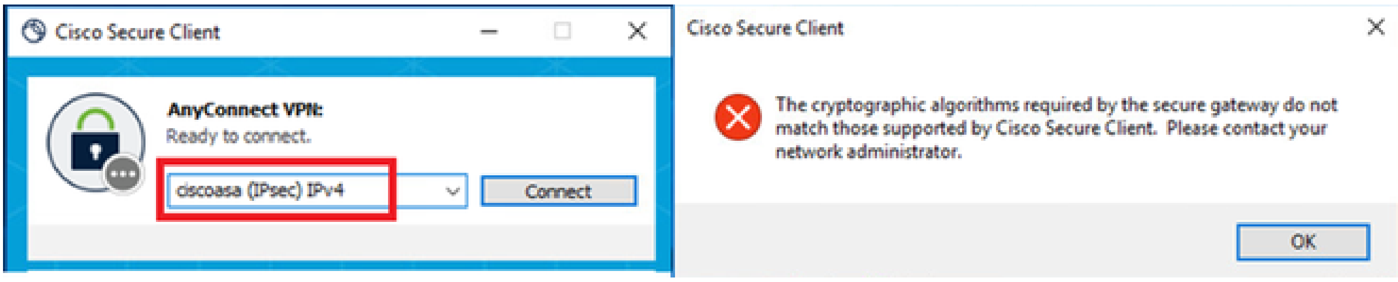
Troubleshooting

A incompatibilidade de algoritmos criptográficos pode resultar em falhas de conexão. Este é um exemplo de quando ocorre um problema de incompatibilidade de algoritmos. A execução da Etapa 15 da seção Configuração no ASDM pode resolver o problema.

Etapa 1. Iniciar conexão VPN

No endpoint, execute o Cisco Secure Client e confirme se a conexão falhou devido a uma incompatibilidade de algoritmos criptográficos.

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.

Falha na conexão

Etapa 2. Confirmar Syslog na CLI

No syslog, confirme se a negociação de IKEv2 falhou.

```
<#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
```

Referência

[AnyConnect via IKEv2 para ASA com AAA e autenticação de certificado]