AAA &；証明書認証を使用したASDMでのセキュアクライアントIKEv2/ASAの設定

内容

はじめに

このドキュメントでは、ASDMとAAAおよび証明書認証を使用して、ASA上でIKEv2を介したセキュアクライアントを設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine(ISE)の設定
- Cisco適応型セキュリティ仮想アプライアンス(ASAv)の設定
- Cisco Adaptive Security Device Manager(ASDM)の設定
- VPN認証のフロー

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

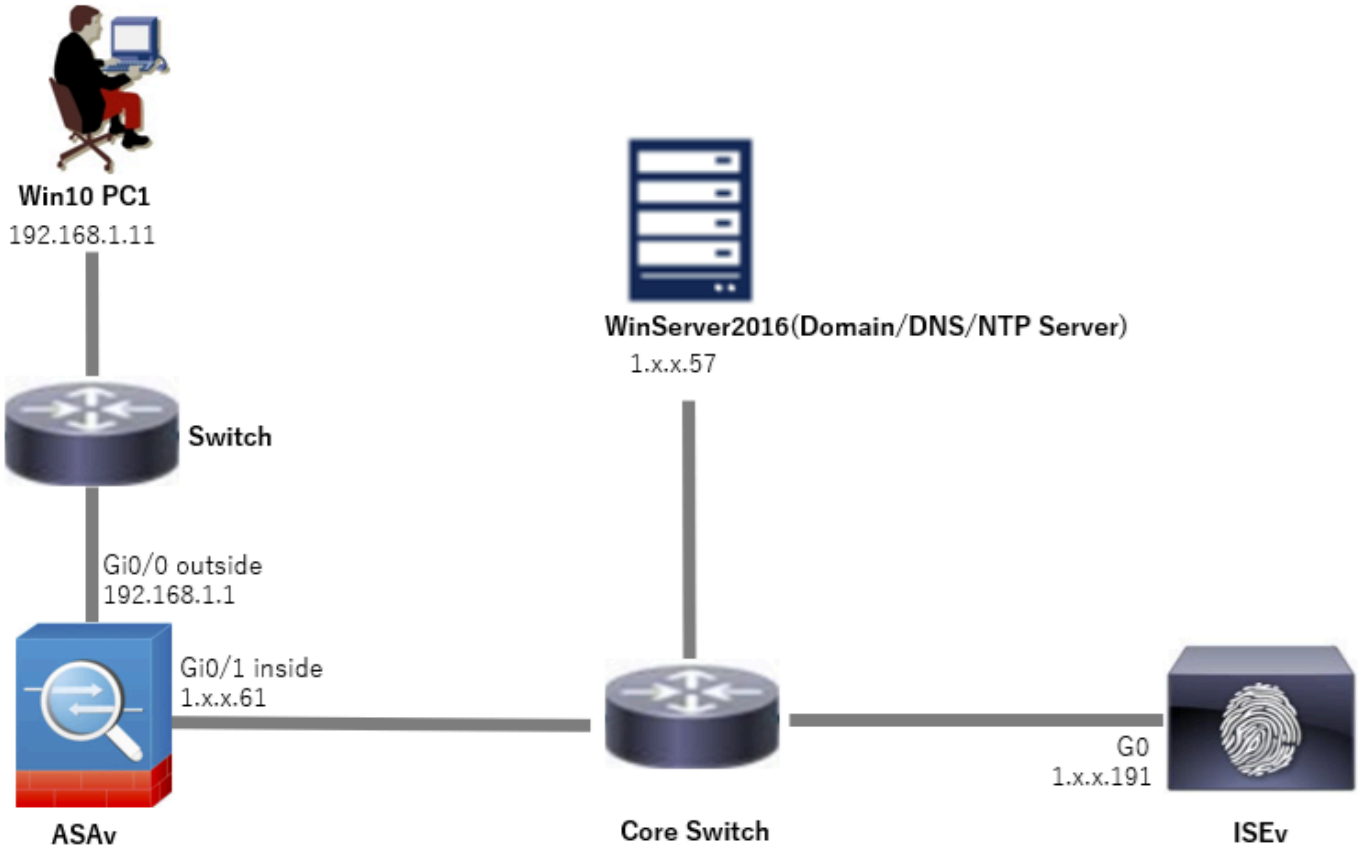
- Identity Services Engine仮想3.3パッチ1
- 適応型セキュリティ仮想アプライアンス9.20(2)21
- Adaptive Security Device Manager(ASDM)7.20
- Cisco Secureクライアント5.1.3.62
- Windows Server 2016
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。

Windows Server 2016で設定されるドメイン名は、このドキュメントの例で使用するad.rem-system.comです。



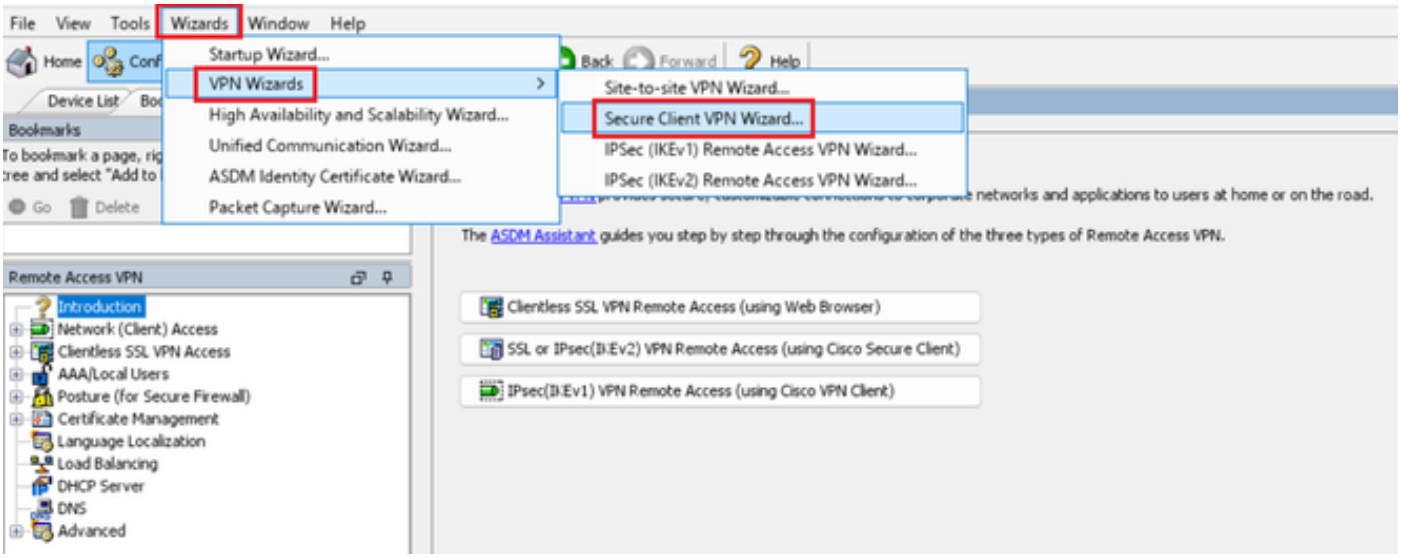
ネットワーク図

コンフィギュレーション

ASDMでの設定

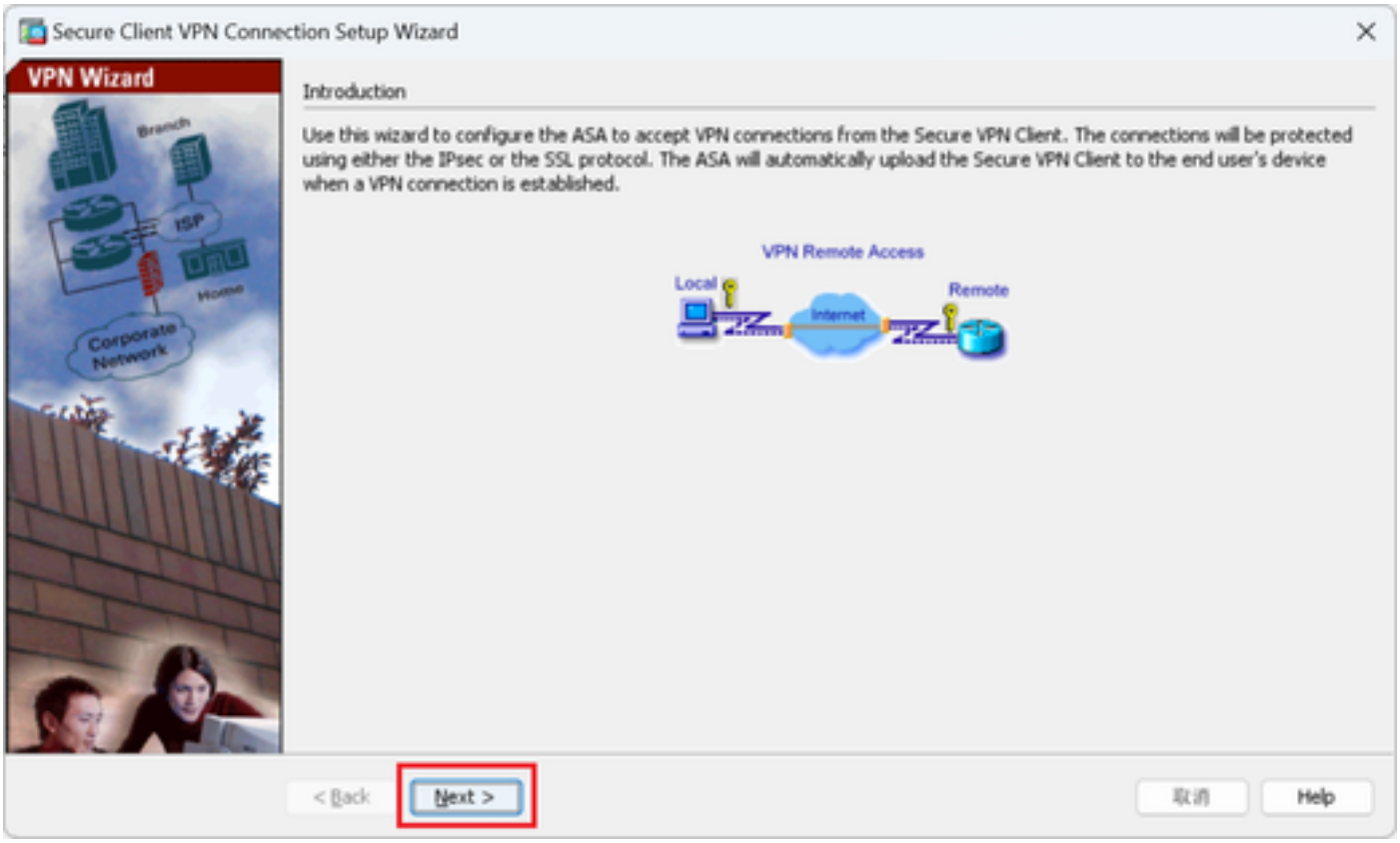
ステップ 1：VPNウィザードを開く

Wizards > VPN Wizardsの順に移動し、Secure Client VPN Wizardをクリックします。



VPNウィザードを開く

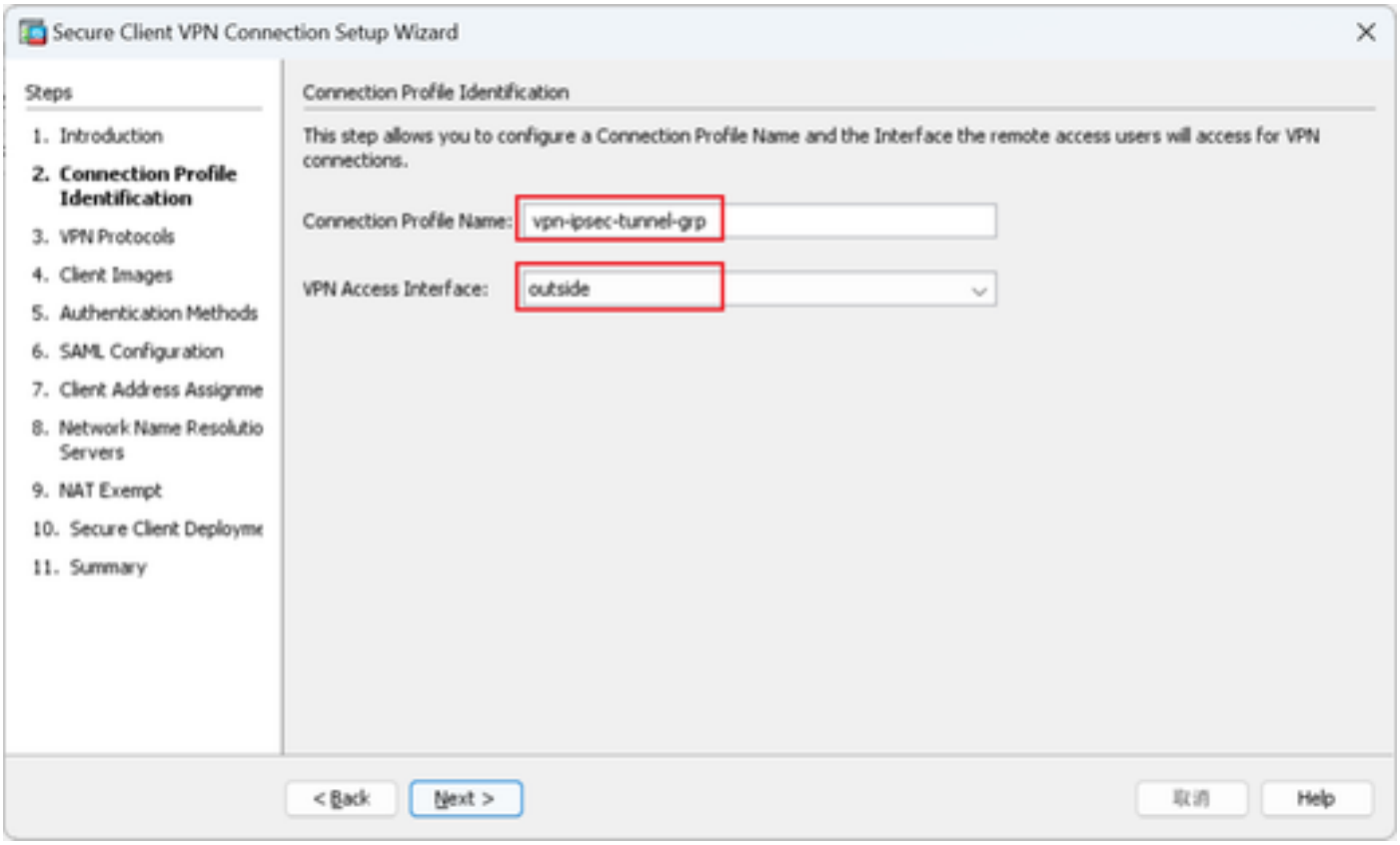
[Next] をクリックします。



[次へ]ボタンをクリックします

ステップ 2：接続プロファイルID

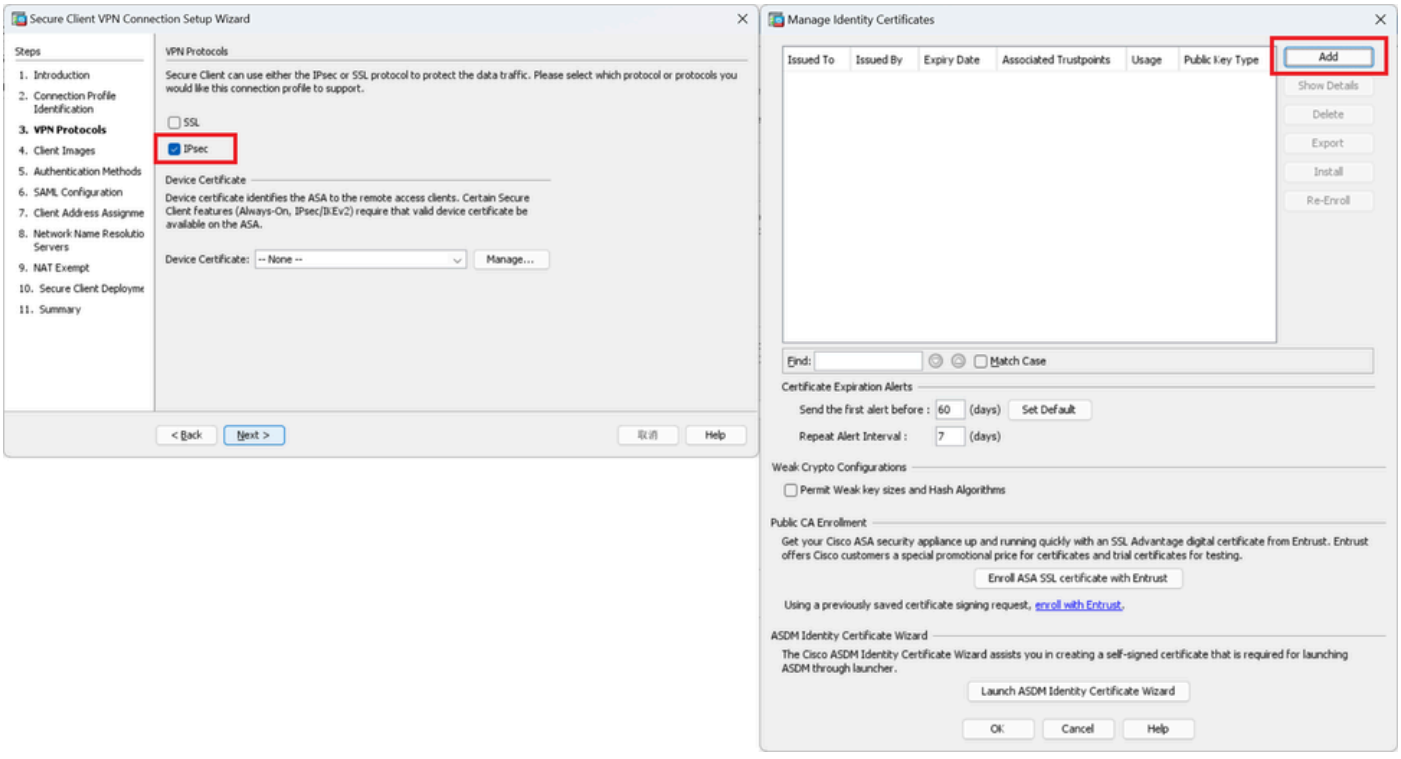
接続プロファイルの情報を入力します。
接続プロファイル名:vpn-ipsec-tunnel-grp
VPNアクセスインターフェイス: outside



接続プロファイルID

ステップ 3：VPN プロトコル

IPsecを選択し、Addボタンをクリックして、新しい自己署名証明書を追加します。

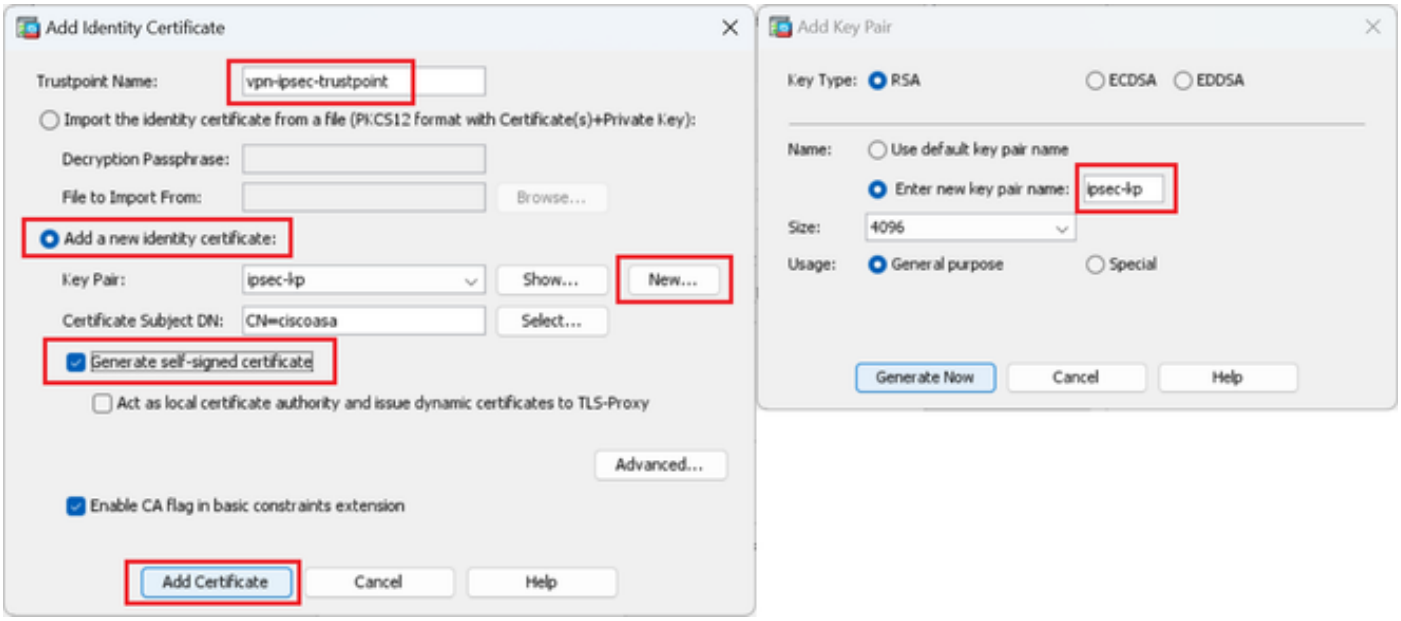


VPN プロトコル

自己署名証明書の情報を入力します。

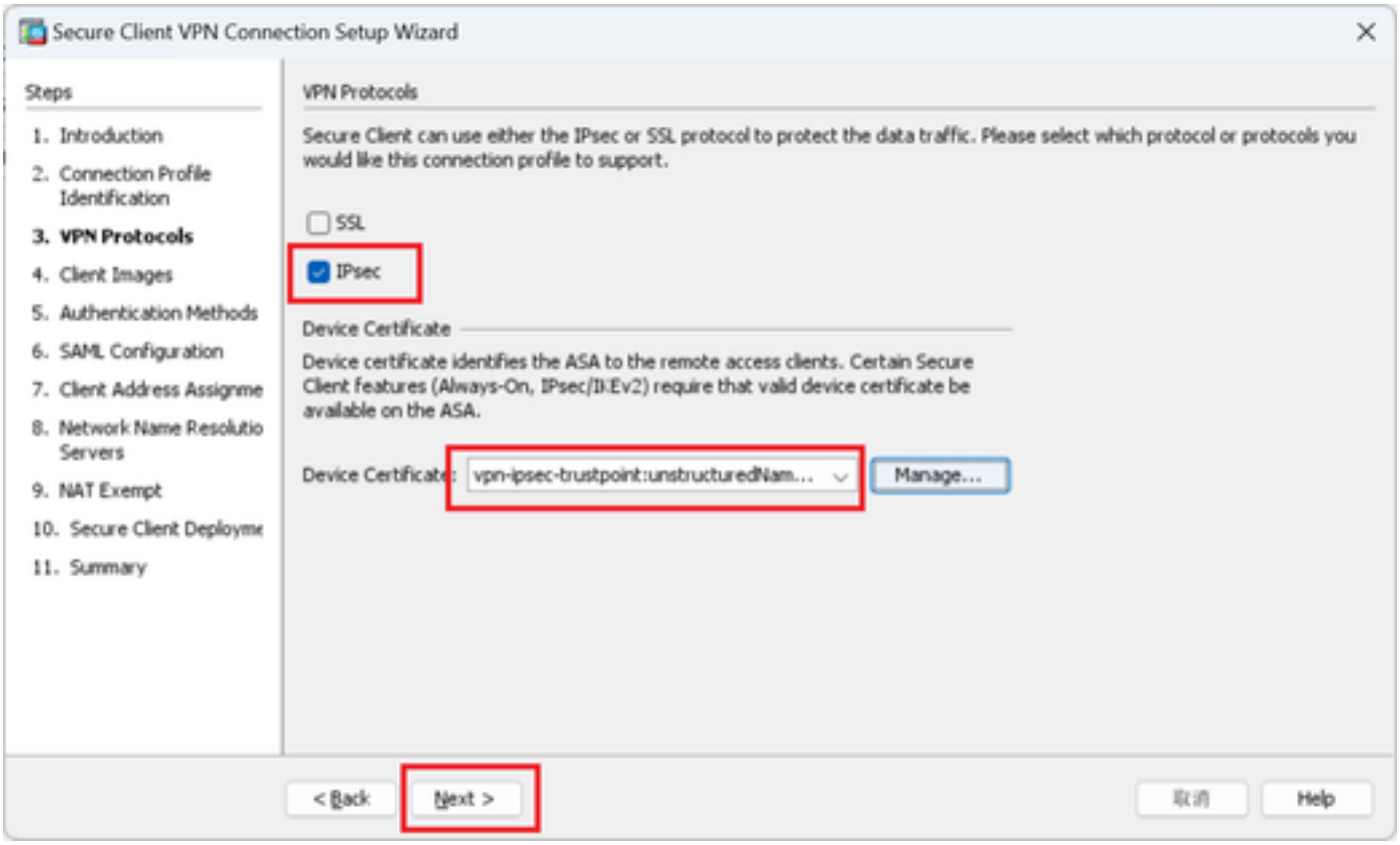
トラストポイント名:vpn-ipsec-trustpoint

キーペア:ipsec-kp



自己署名証明書の詳細

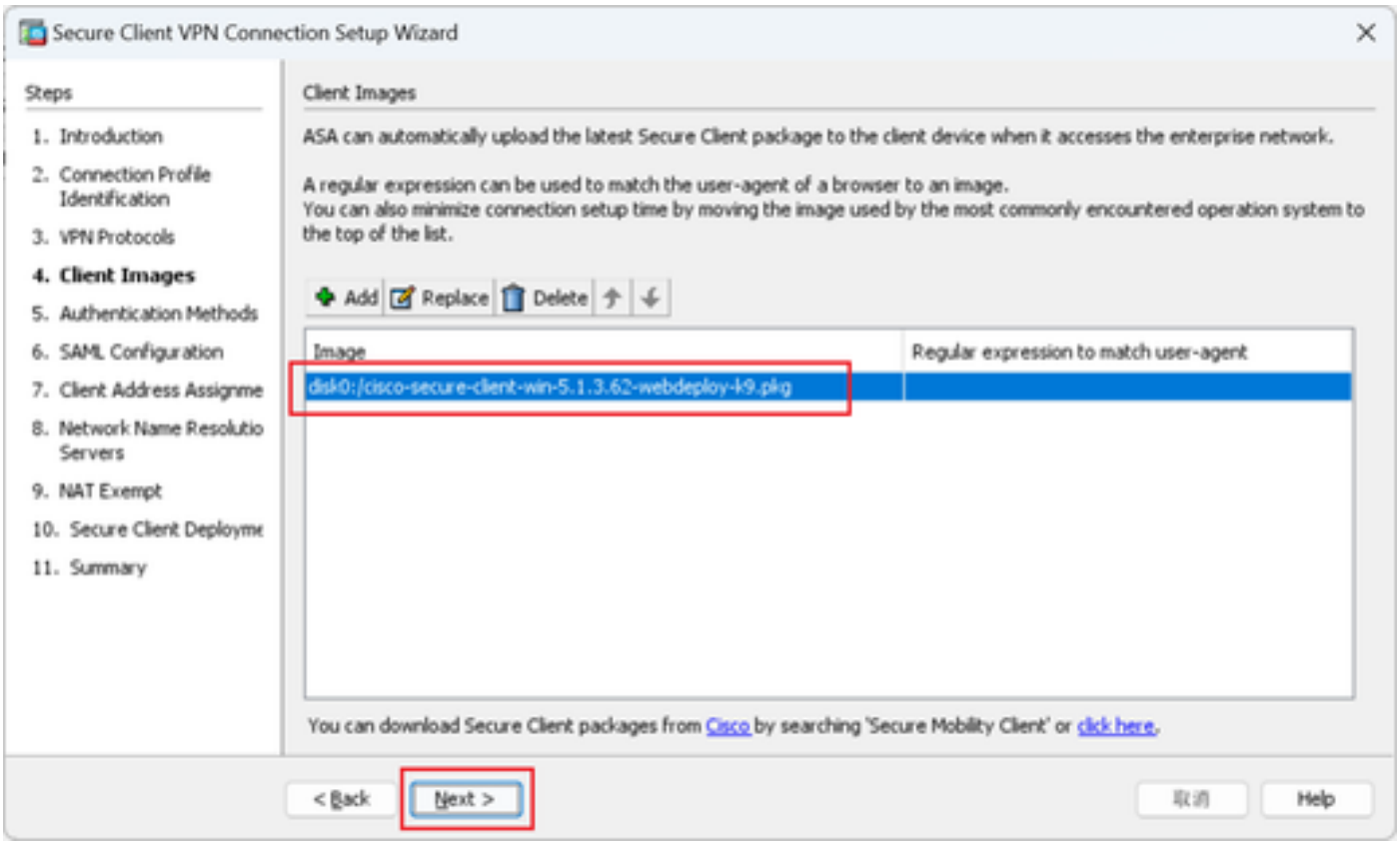
VPNプロトコルの設定を確認し、Nextボタンをクリックします。



VPNプロトコルの設定の確認

ステップ 4：クライアントイメージ

Addボタンをクリックしてセキュアなクライアントイメージを追加し、Nextボタンをクリックします。



クライアントイメージ

ステップ 5：認証方式

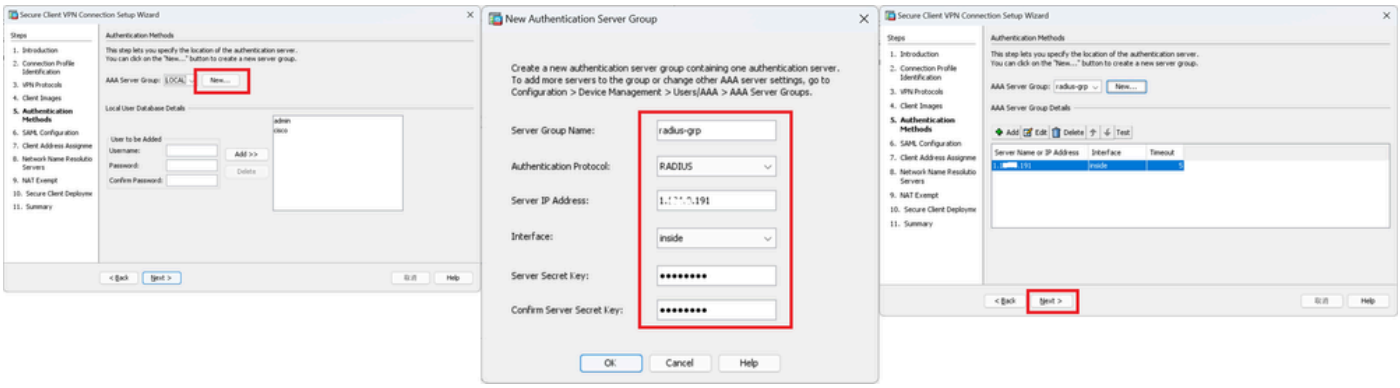
Newボタンをクリックして新しいaaaサーバを追加し、Nextボタンをクリックします。

サーバグループ名:radius-grp

認証プロトコル:RADIUS

サーバIPアドレス:1.x.x.191

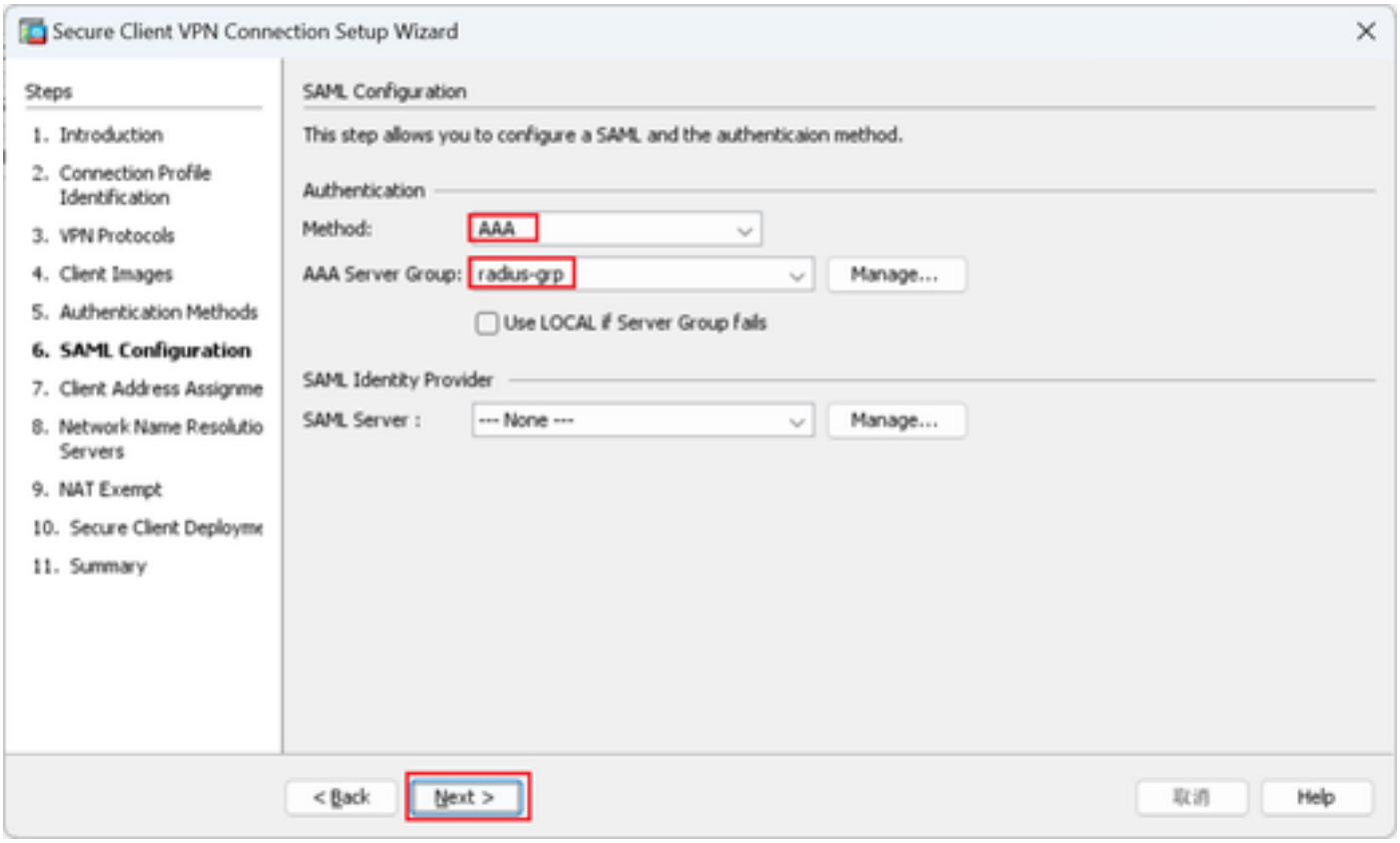
インターフェイス：内部



認証方式

手順 6：SAML設定

Nextボタンをクリックします。



SAML設定

手順 7：クライアントアドレス割り当て

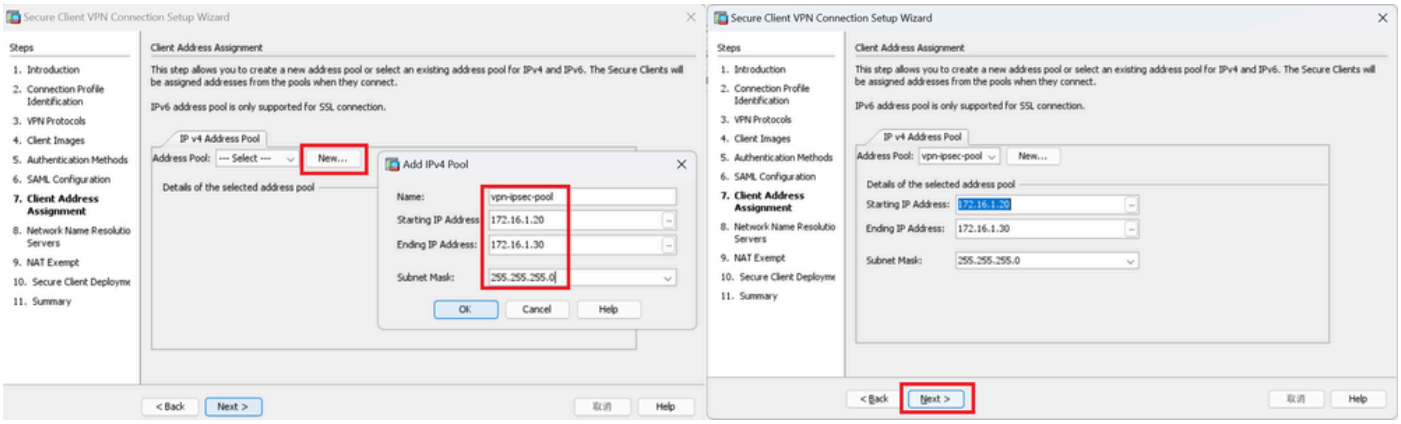
Newボタンをクリックして新しいIPv4プールを追加し、Nextボタンをクリックします。

名前:vpn-ipsec-pool

開始IPアドレス:172.16.1.20

終了IPアドレス:172.16.1.30

サブネットマスク:255.255.255.0



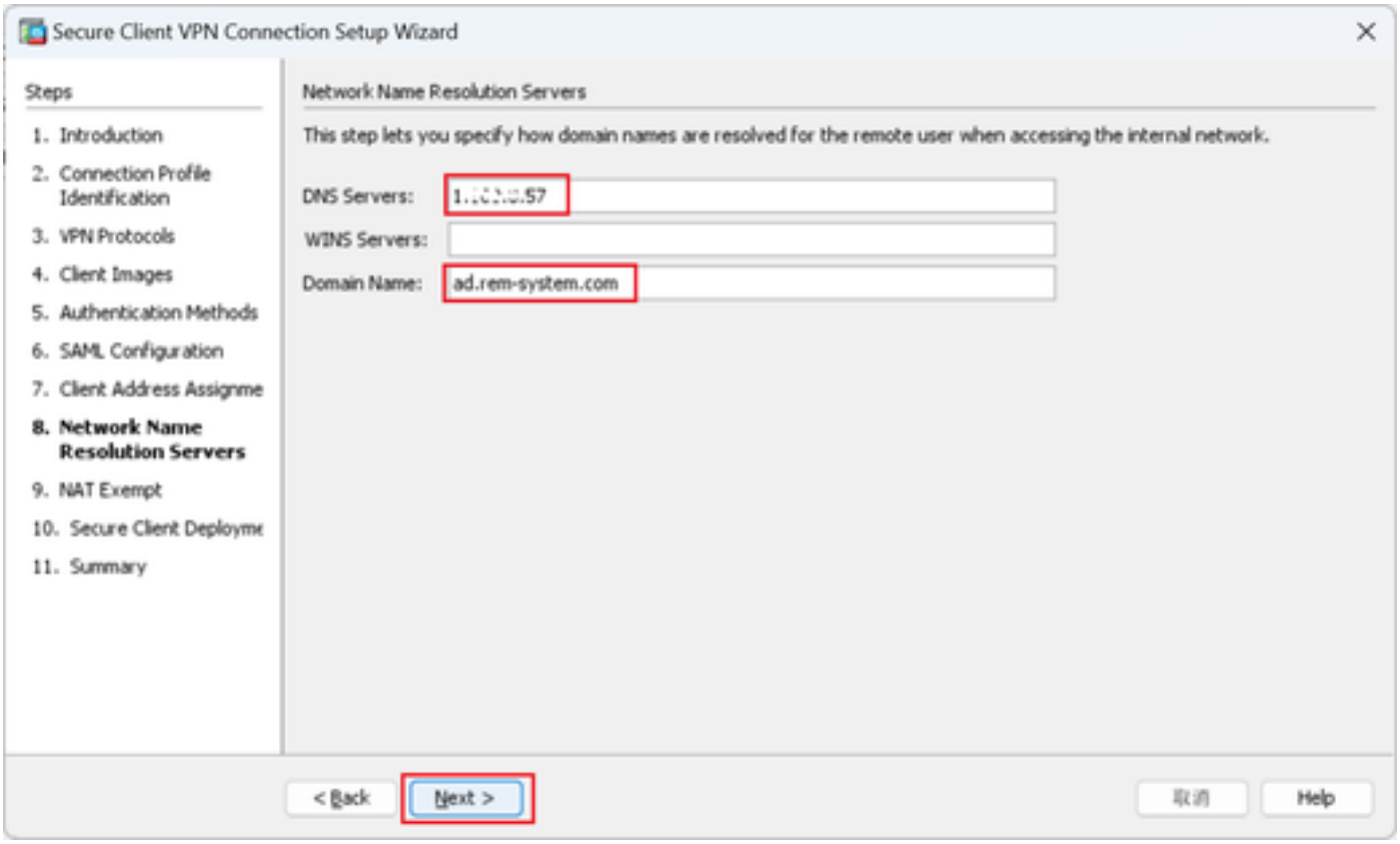
クライアントアドレスの割り当て

ステップ 8：ネットワーク名前解決サーバ

DNSとドメインの情報を入力し、Nextボタンをクリックします。

DNSサーバ:1.x.x.57

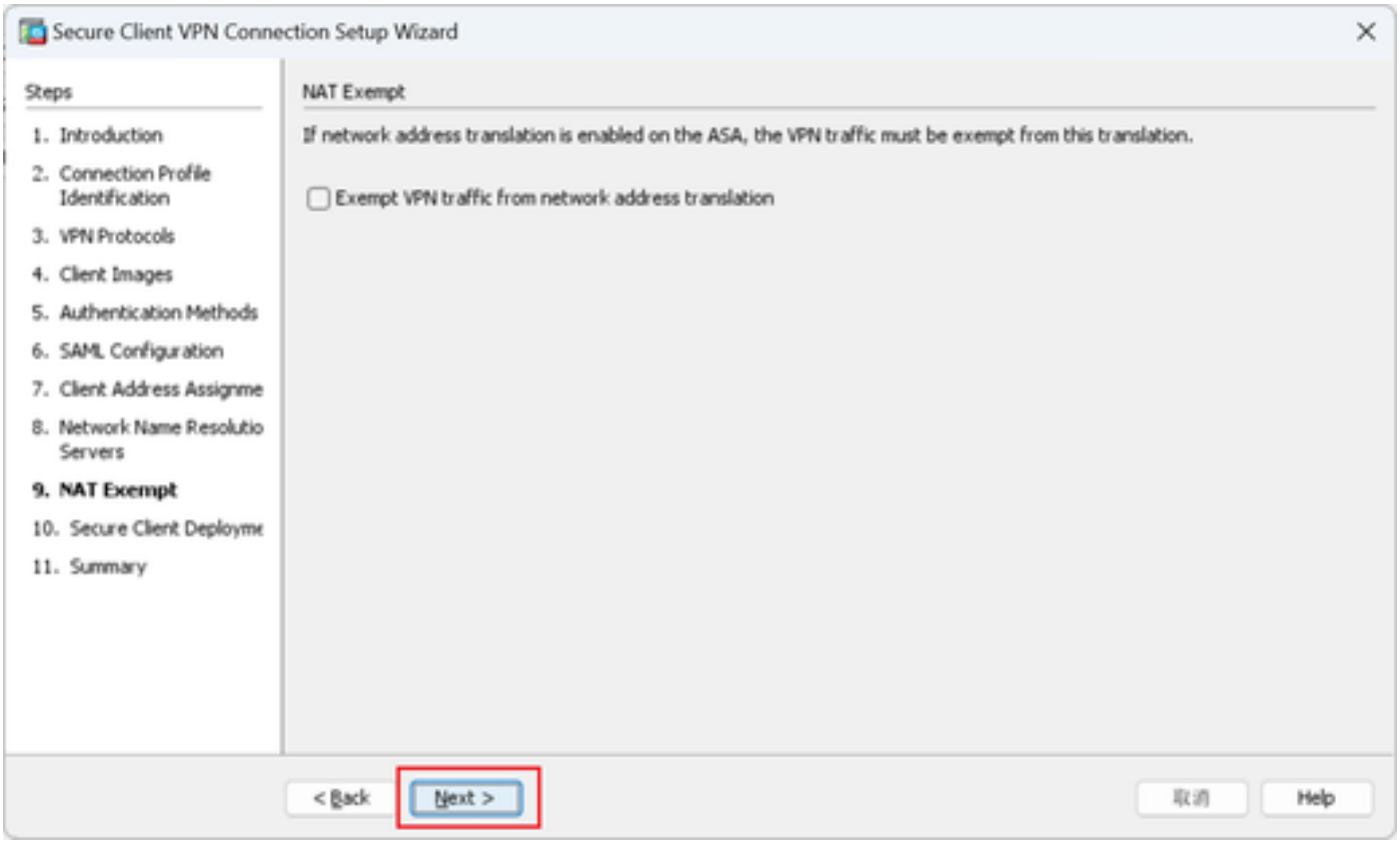
ドメイン名:ad.rem-system.com



ネットワーク名前解決サーバ

ステップ 9：NAT免除

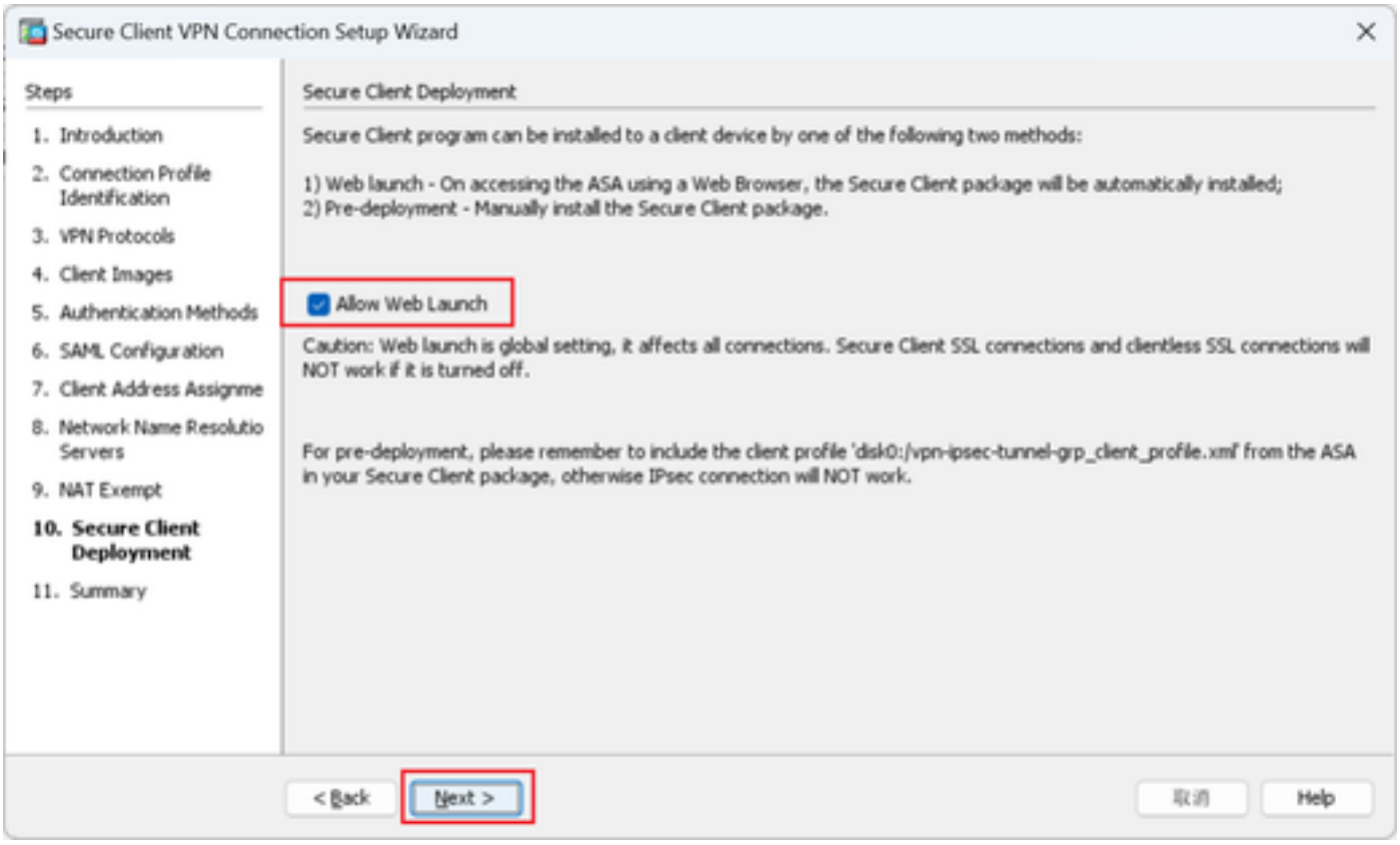
Nextボタンをクリックします。



NAT免除

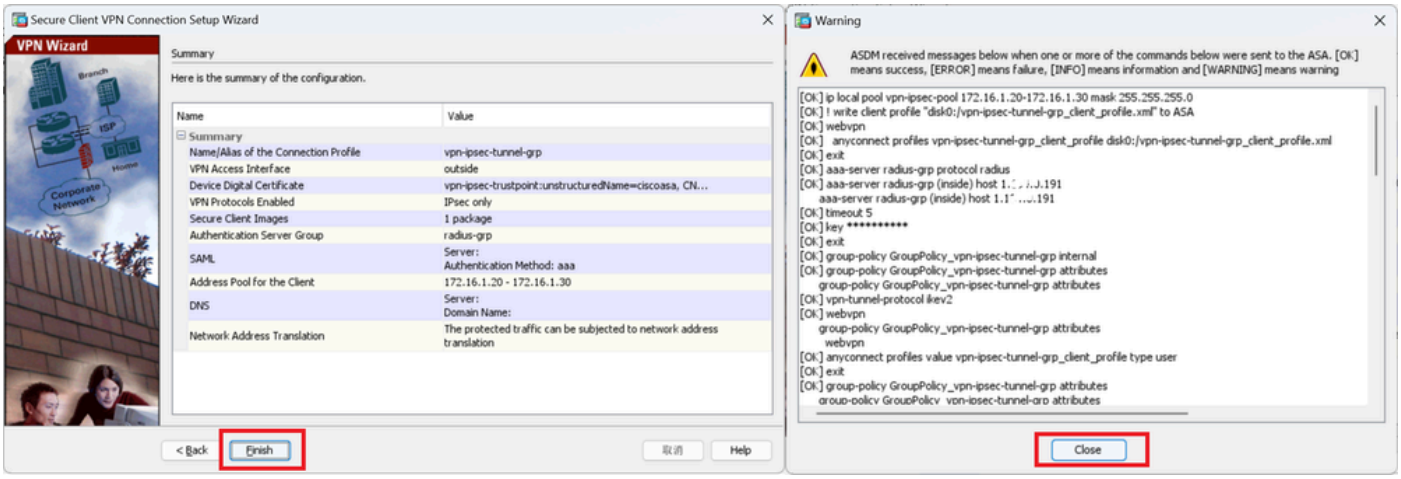
ステップ 10：セキュアなクライアント展開

Allow Web Launchを選択し、Nextボタンをクリックします。



ステップ 11設定の保存

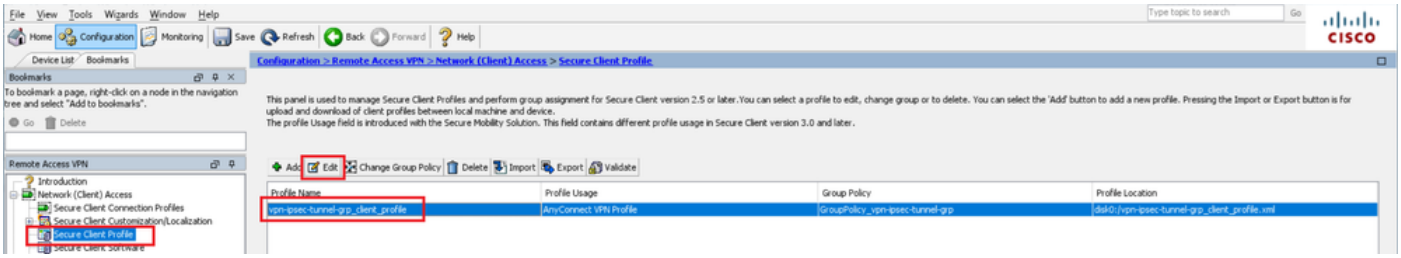
Finishボタンをクリックして、設定を保存します。



設定の保存

ステップ 12セキュアクライアントプロファイルの確認とエクスポート

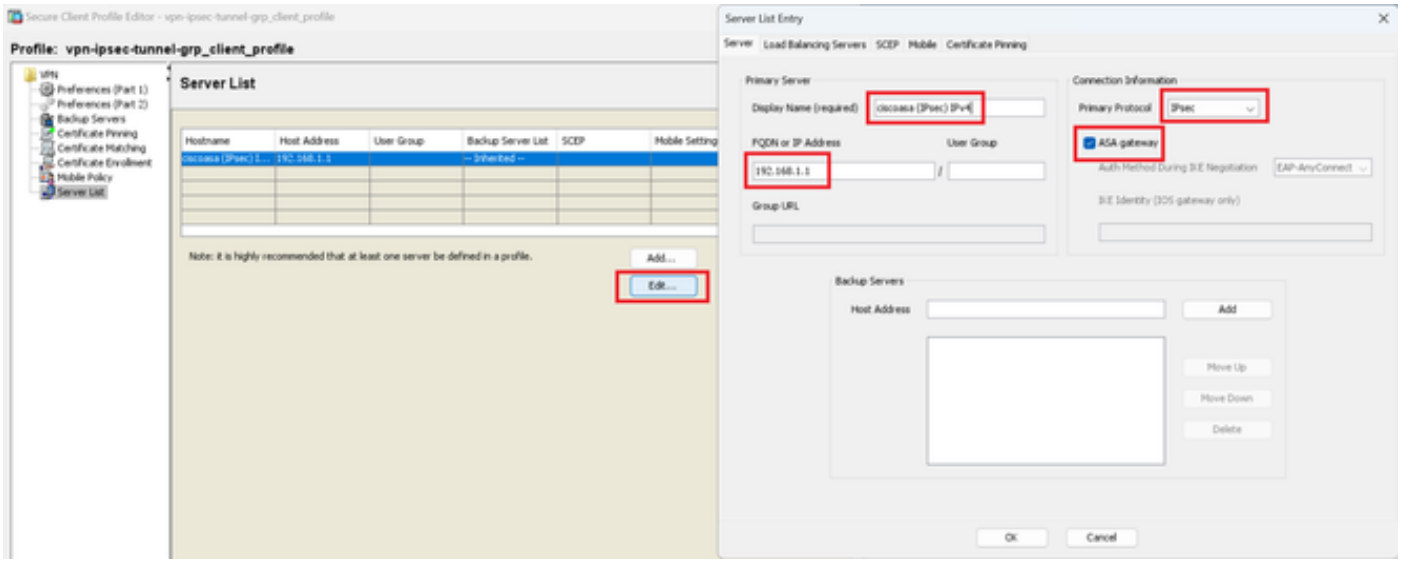
Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profileの順に移動し、Editボタンをクリックします。



セキュアクライアントプロファイルの編集

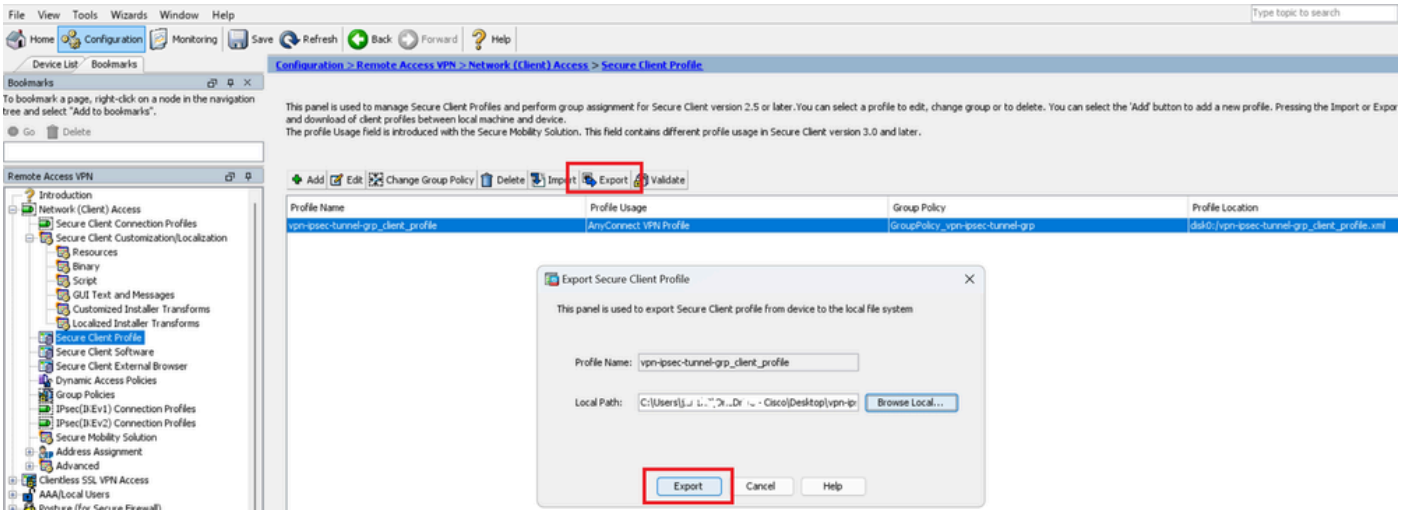
プロファイルの詳細を確認します。

- 表示名（必須）:ciscoasa(IPsec)IPv4
- FQDNまたはIPアドレス:192.168.1.1
- プライマリプロトコル:IPsec



セキュアクライアントプロファイルの確認

Exportボタンをクリックして、プロファイルをローカルPCにエクスポートします。



セキュアクライアントプロファイルのエクスポート

ステップ 13セキュアクライアントプロファイルの詳細の確認

ブラウザでセキュアクライアントプロファイルを開き、ホストのプライマリプロトコルがIPsecであることを確認します。

```
▼<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>
```

ステップ 14：ASA CLIでの設定の確認

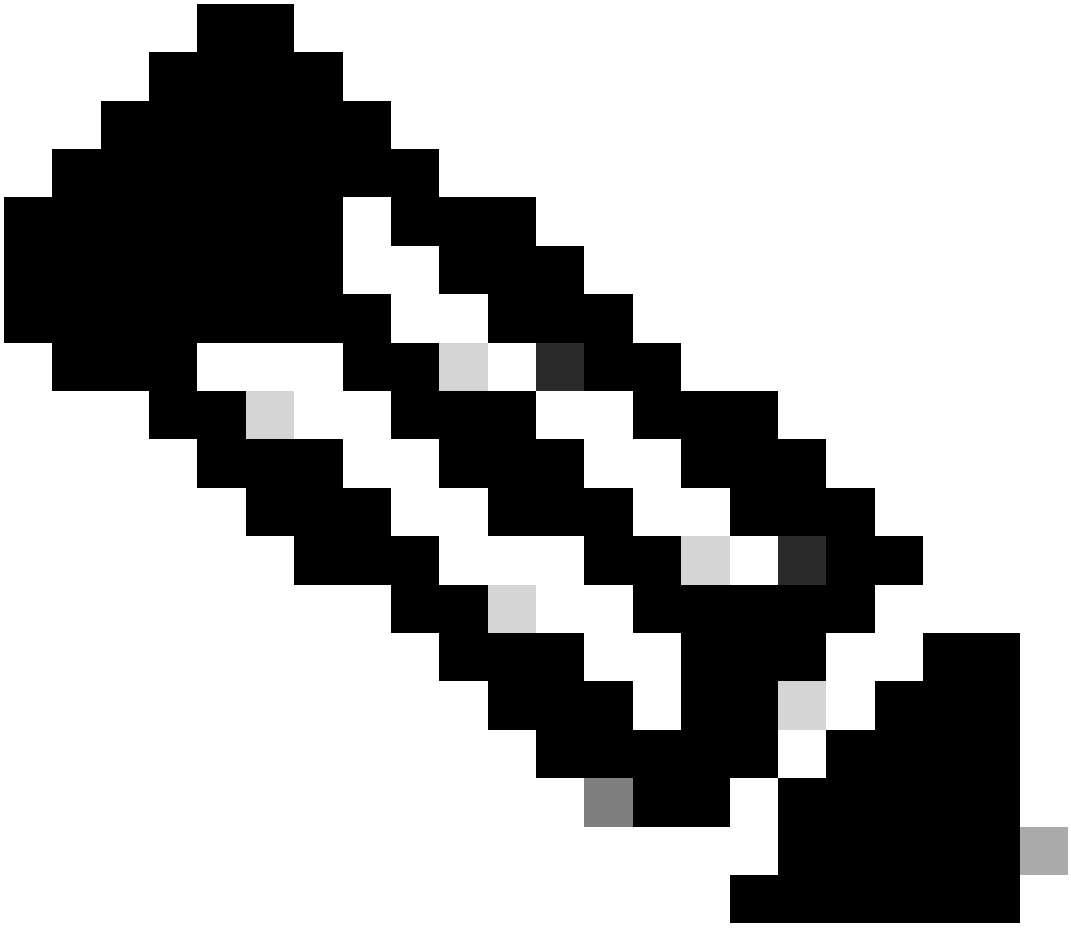
ASA CLIでASDMによって作成されたIPsec設定を確認します。

```
// 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
```

ステップ 15：暗号化アルゴリズムの追加

ASA CLIで、グループ19をIKEv2ポリシーに追加します。

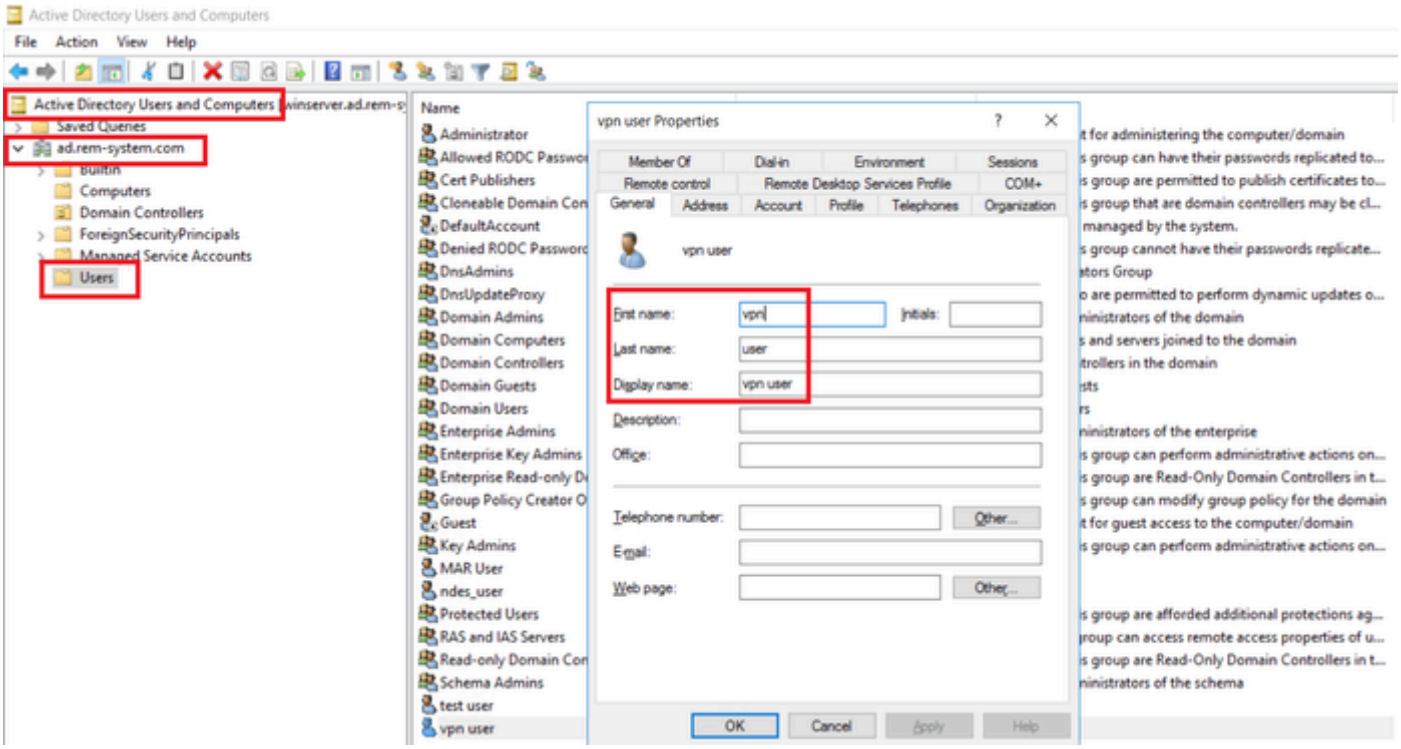


注:IKEv2/IPsec接続に関して、Cisco Secure ClientではバージョンIKEv2/IPsec接続に関して、Cisco Secure Clientではバージョン4.9.00086以降、Diffie-Hellman(DH)グループ2、5、14、および24をサポートしていません。この変更により、暗号化アルゴリズムの不一致が原因で接続エラーが発生する可能性があります。

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

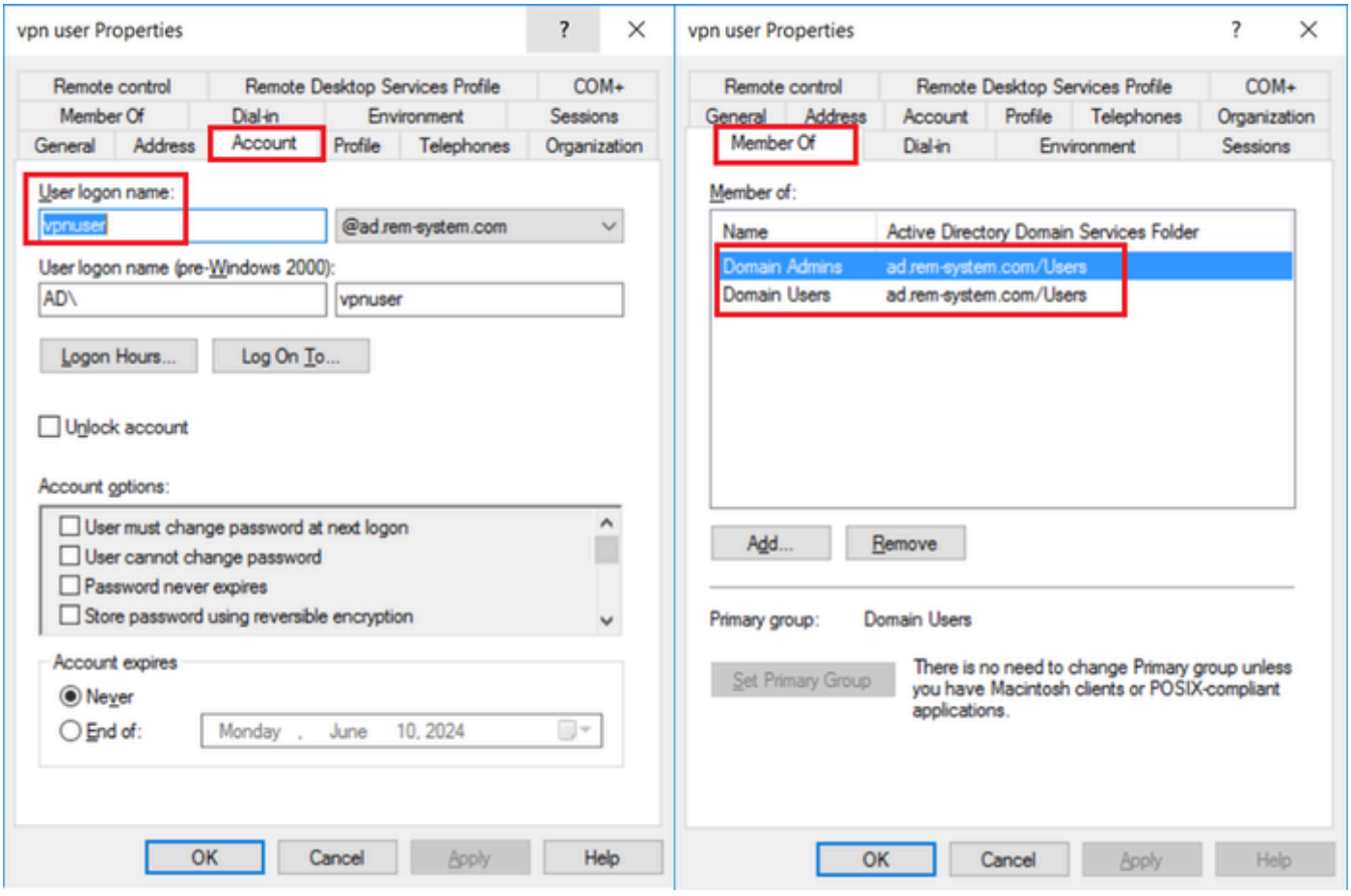
Windows Serverでの設定

VPN接続用のドメインユーザを追加する必要があります。 Active Directory Users and Computersに移動し、Usersをクリックします。ドメインユーザとしてvpnuserを追加します。



ドメインユーザの追加

Domain AdminsとDomain Usersのメンバにドメインユーザを追加します。

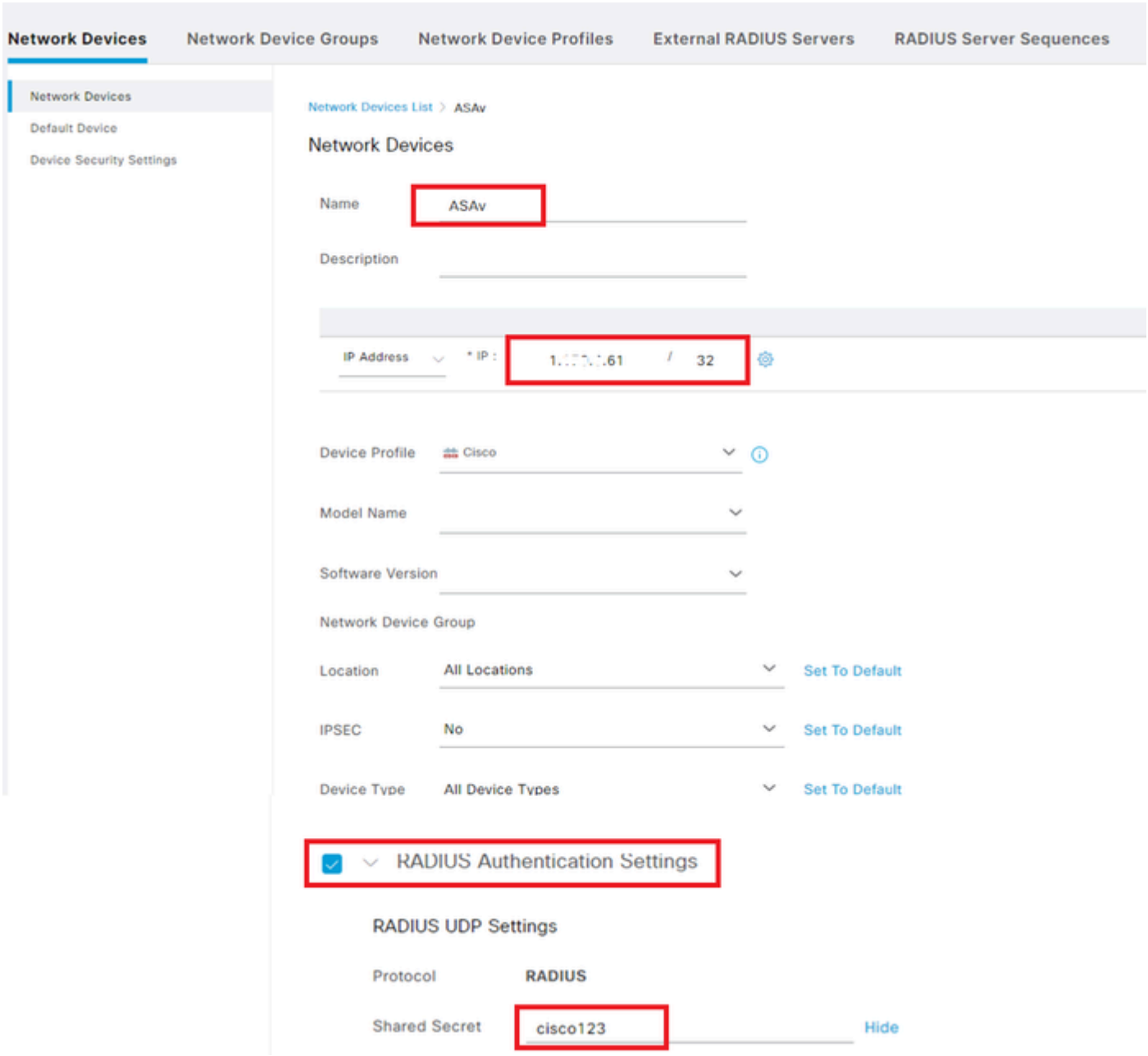


ドメイン管理者とドメインユーザー

ISEでの設定

ステップ 1：デバイスの追加

Administration > Network Devicesの順に移動し、Addbuttonをクリックしてデバイスを追加します。

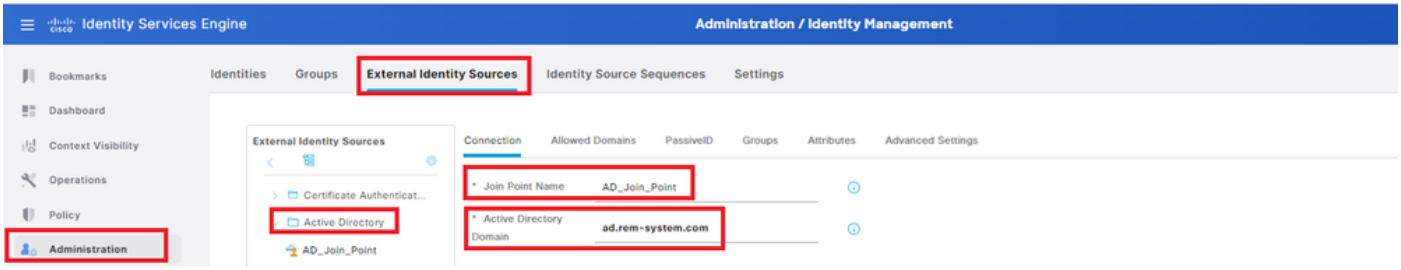


デバイスの追加

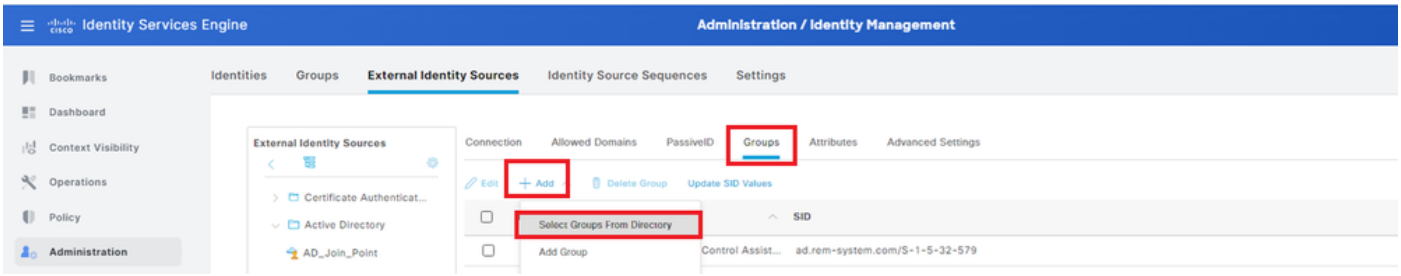
ステップ 2：Active Directoryの追加

Administration > External Identity Sources > Active Directoryの順に移動し、Connectiontabをクリックし、Active DirectoryをISEに追加します。

- 結合ポイント名: AD_Join_Point
- Active Directoryドメイン:ad.rem-system.com



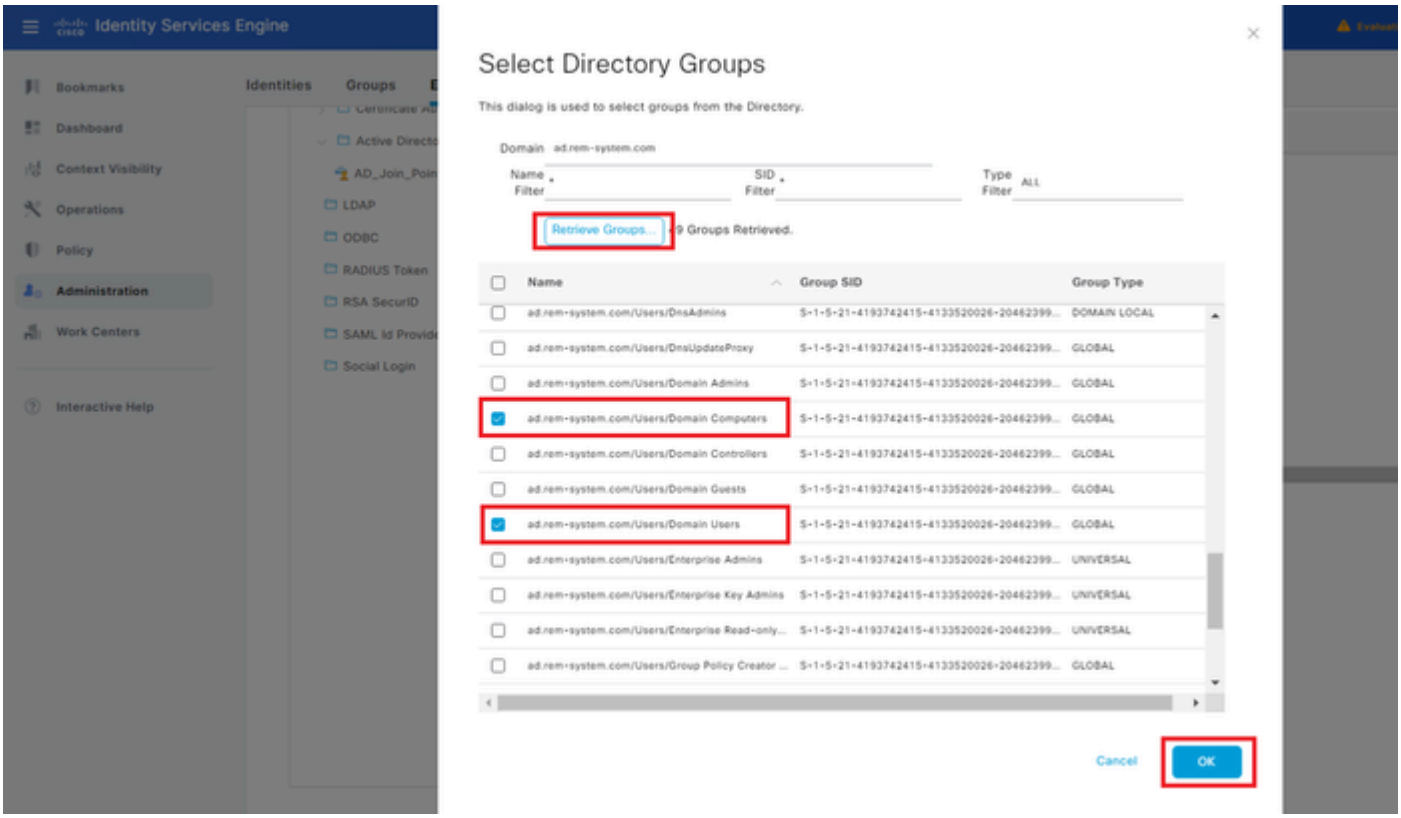
Active Directoryの追加



Groupsタブに移動し、Select Groups From Directoryドロップダウンリストからグループを選択します。

Select Groups from Directory

[グループの取り出し]ドロップダウンリストをクリックします。Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain ユーザを選択し、[OK] をクリックします。

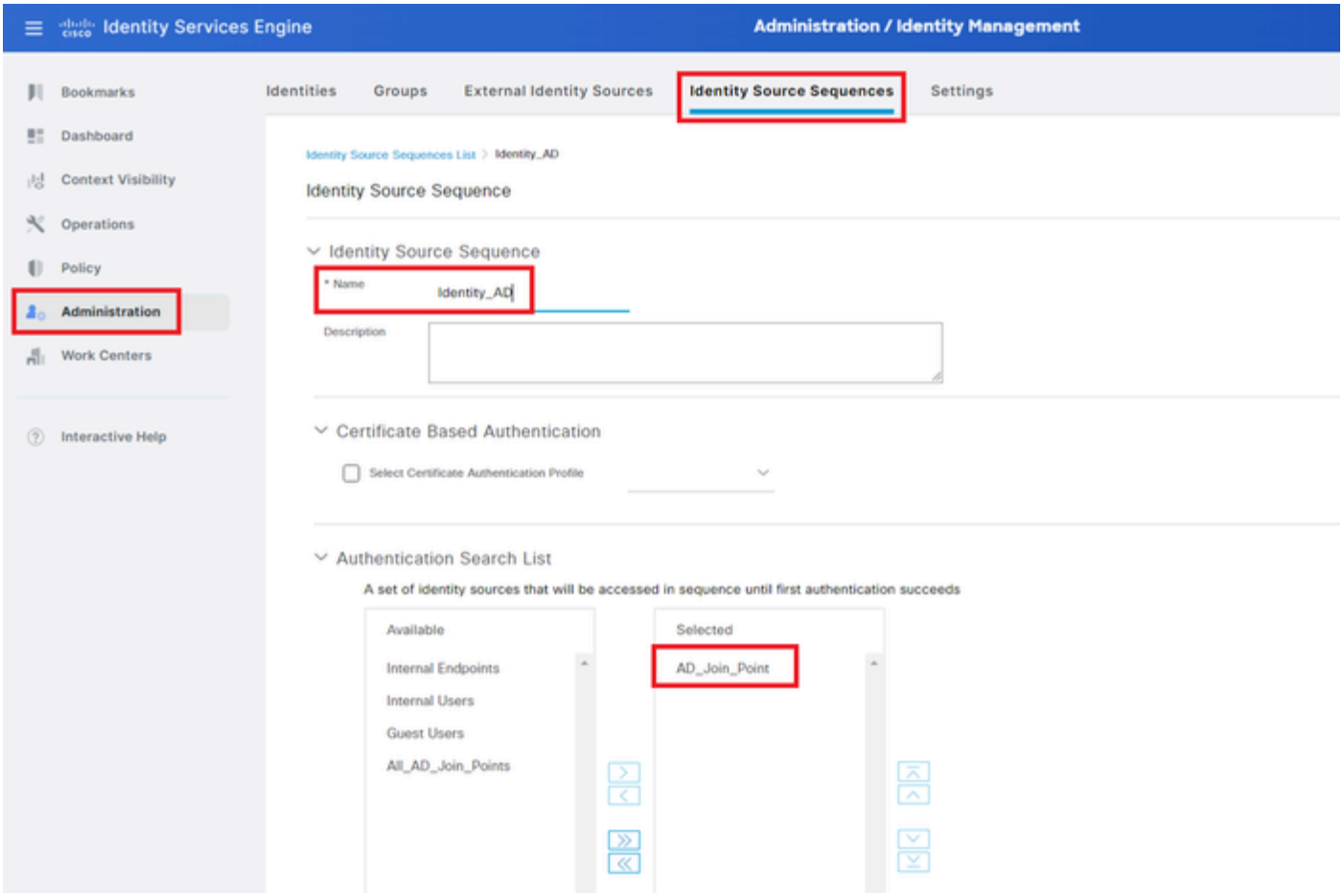


ドメインコンピューターとユーザーの追加

ステップ 3：アイデンティティソースシーケンスの追加

Administration > Identity Source Sequencesの順に移動し、Identity Source Sequenceを追加します。

- 名前: Identity_AD
- 認証検索リスト:AD_Join_Point

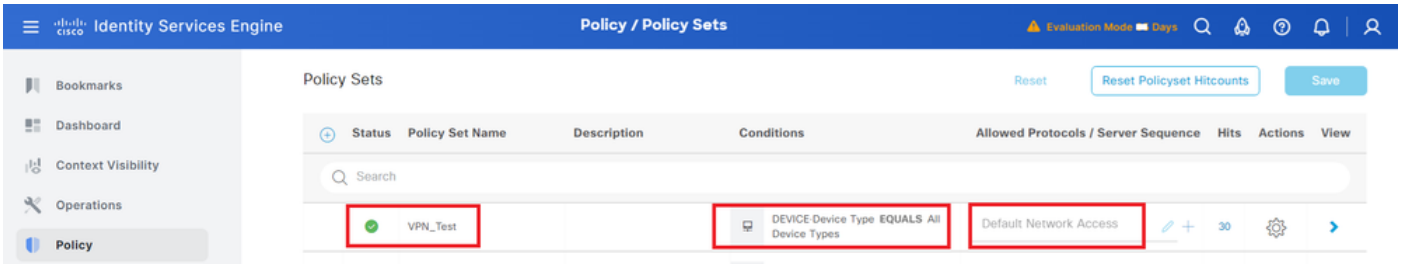


アイデンティティソースシーケンスの追加

ステップ 4：ポリシーセットの追加

Policy > Policy Setsの順に移動し、+ をクリックしてポリシーセットを追加します。

- ポリシーセット名:VPN_Test
- 条件:DEVICE Device Type はすべてのデバイスタイプと同じ
- 許可されるプロトコル/サーバシーケンス：デフォルトのネットワークアクセス

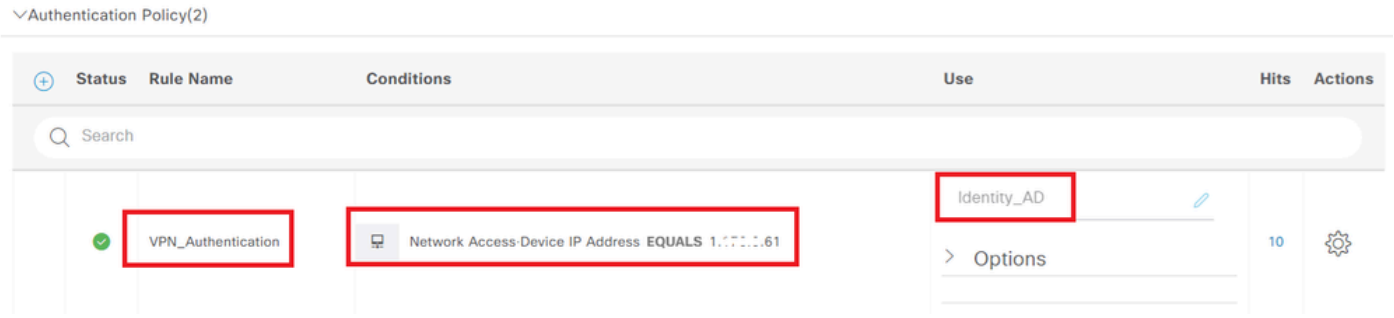


ポリシーセットの追加

ステップ 5：認証ポリシーの追加

Policy Setsに移動し、VPN_Testをクリックして認証ポリシーを追加します。

- ルール名:VPN_Authentication
- 条件：ネットワークアクセスデバイスのIPアドレスが1.x.x.61と等しい
- 使用：Identity_AD

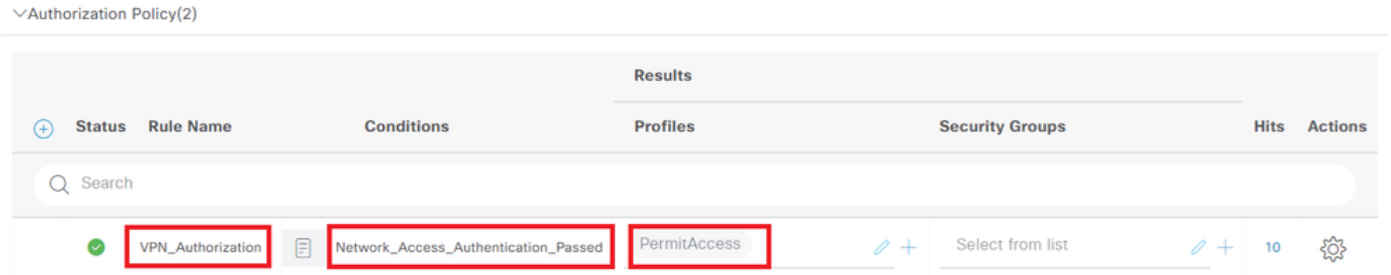


認証ポリシーの追加

手順 6：許可ポリシーの追加

Policy Setsに移動し、VPN_Testをクリックして認可ポリシーを追加します。

- ルール名:VPN_Authorization
- 条件:Network_Access_Authentication_Passed
- 結果:PermitAccess

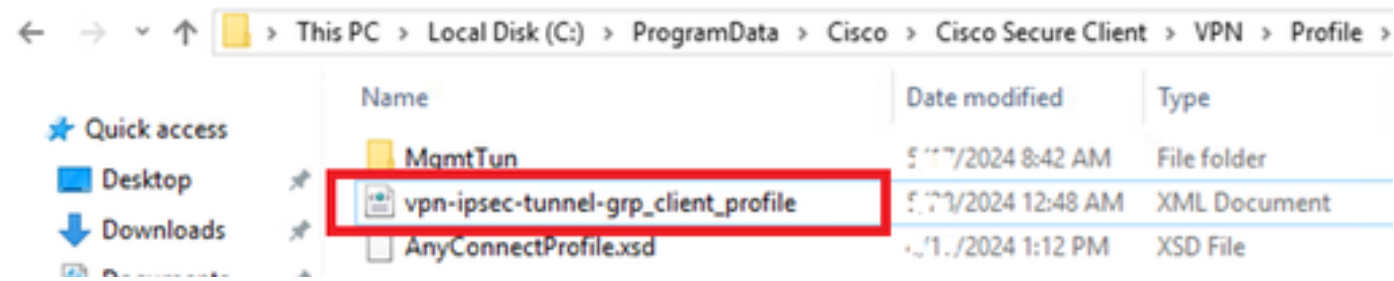


許可ポリシーの追加

確認

ステップ 1：セキュアクライアントプロファイルのWin10 PC1へのコピー

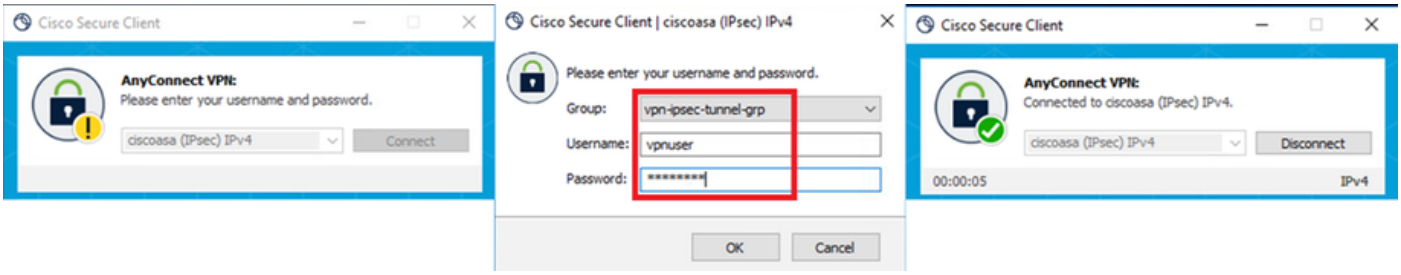
セキュアクライアントプロファイルをC:\ProgramData\Cisco\Cisco Secure Client\VPN\Profileディレクトリにコピーします。



プロファイルをPCにコピー

ステップ 2：VPN接続の開始

エンドポイントで、Cisco Secure Clientを実行し、ユーザ名とパスワードを入力して、Cisco Secure Clientが正常に接続されていることを確認します。



Connection succeeded

ステップ 3：ASAでのSyslogの確認

syslogで、IKEv2接続が成功したことを確認します。

<#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
```

ステップ 4：ASAでのIPsecセッションの確認

show vpn-sessiondb detail anyconnectコマンドを実行して、ASAでのIKEv2/IPsecセッションを確認します。

<#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

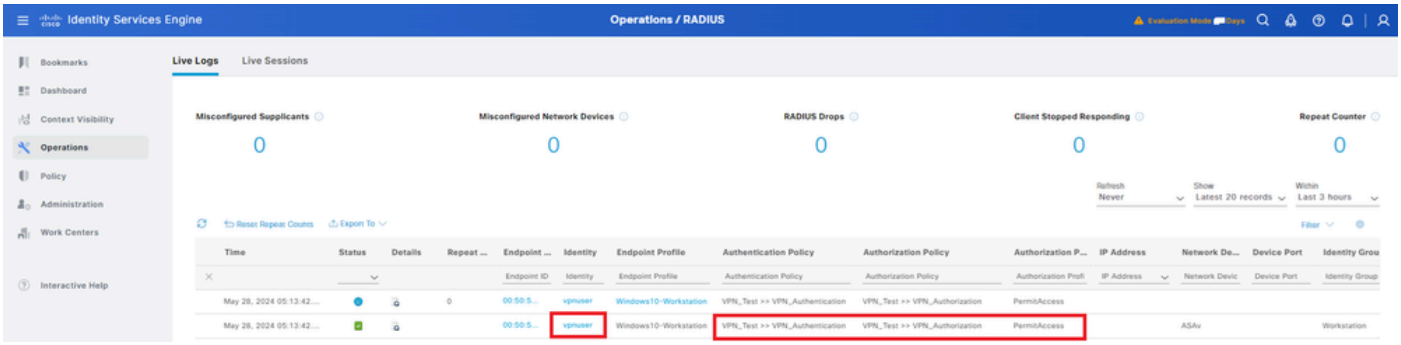
IPsecOverNatT Tunnels: 1

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
```

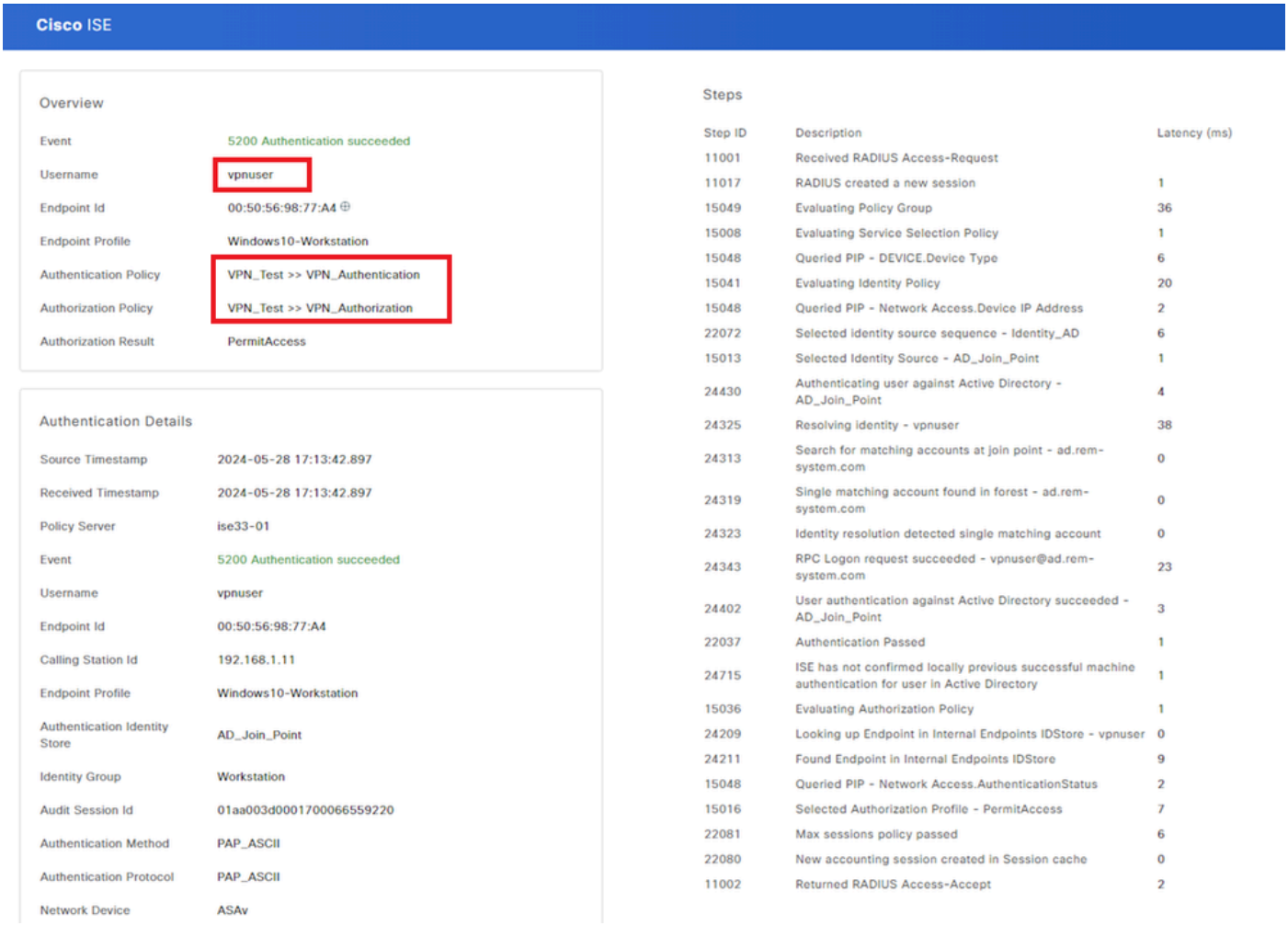
ステップ 5：Radiusライブログの確認

ISE GUIで**Operations** > **RADIUS** > **Live**の順に移動し、vpn認証のライブログを確認します。



*Radius*ライブログ

[ステータス]をクリックして、ライブログの詳細を確認します。



ライブログの詳細

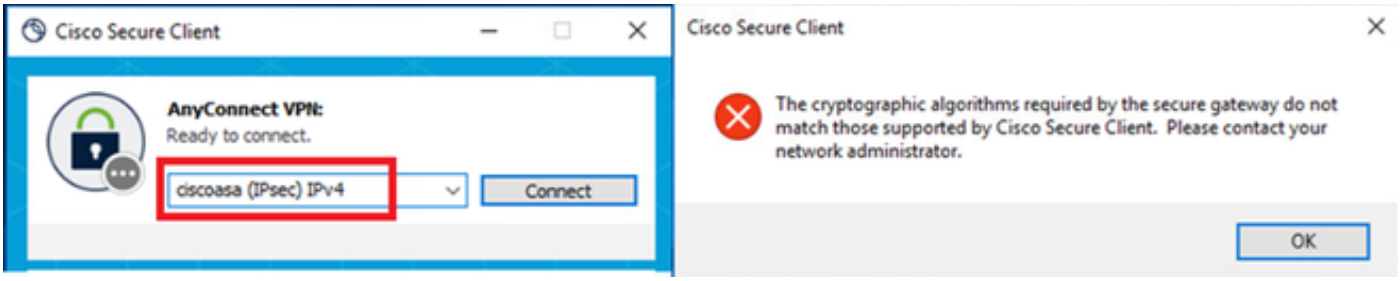
トラブルシュート

暗号化アルゴリズムのミスマッチにより、接続障害が発生する可能性があります。これは、アルゴリズムの不一致の問題が発生する場合の例です。ASDMでセクション「設定」のステップ15を実行すると、この問題を解決できます。

ステップ 1：VPN接続の開始

エンドポイントでCisco Secure Clientを実行し、暗号化アルゴリズムの不一致が原因で接続が失敗したことを確認します。

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



接続に失敗しました。

ステップ 2：CLIでのSyslogの確認

syslogで、IKEv2ネゴシエーションが失敗したことを確認します。

<#root>

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

Failed to find a matching policy

参考

AAA 認証と証明書認証を使用した、IKEv2 による ASA への AnyConnect

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。