AAA & 인증서 인증을 사용하여 ASDM에서 보안 클라이언트 IKEv2/ASA 구성

목차

소개

이 문서에서는 ASDM과 AAA 및 인증서 인증을 사용하여 ASA에서 IKEv2를 통한 보안 클라이언트를 구성하는 데 필요한 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE(Identity Services Engine) 구성
- Cisco ASAv(Adaptive Security Virtual Appliance) 컨피그레이션
- Cisco ASDM(Adaptive Security Device Manager) 구성
- VPN 인증 흐름

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

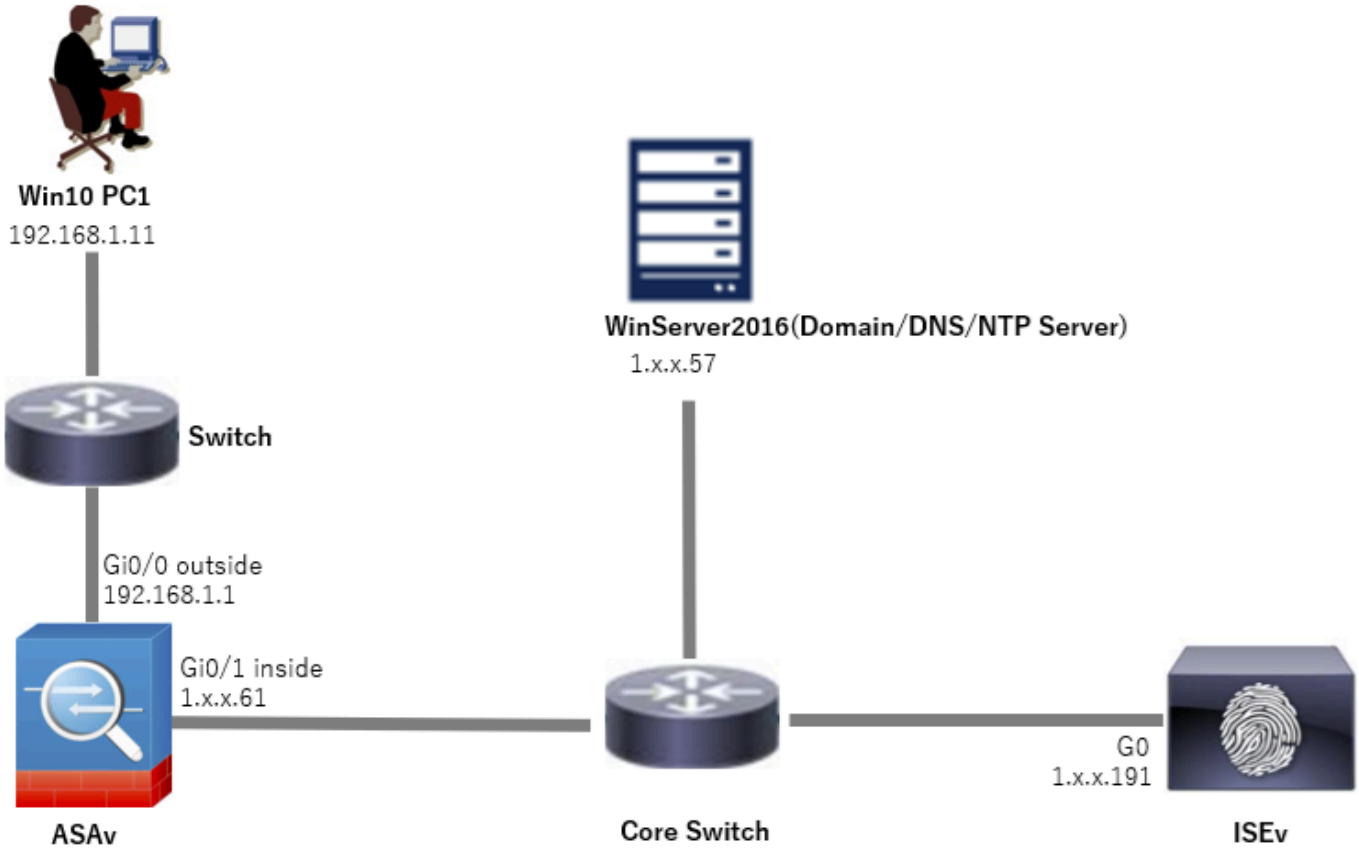
- Identity Services Engine Virtual 3.3 패치 1
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.

Windows Server 2016에 구성된 도메인 이름은 ad.rem-system.com이며 이 문서의 예제로 사용됩니다.



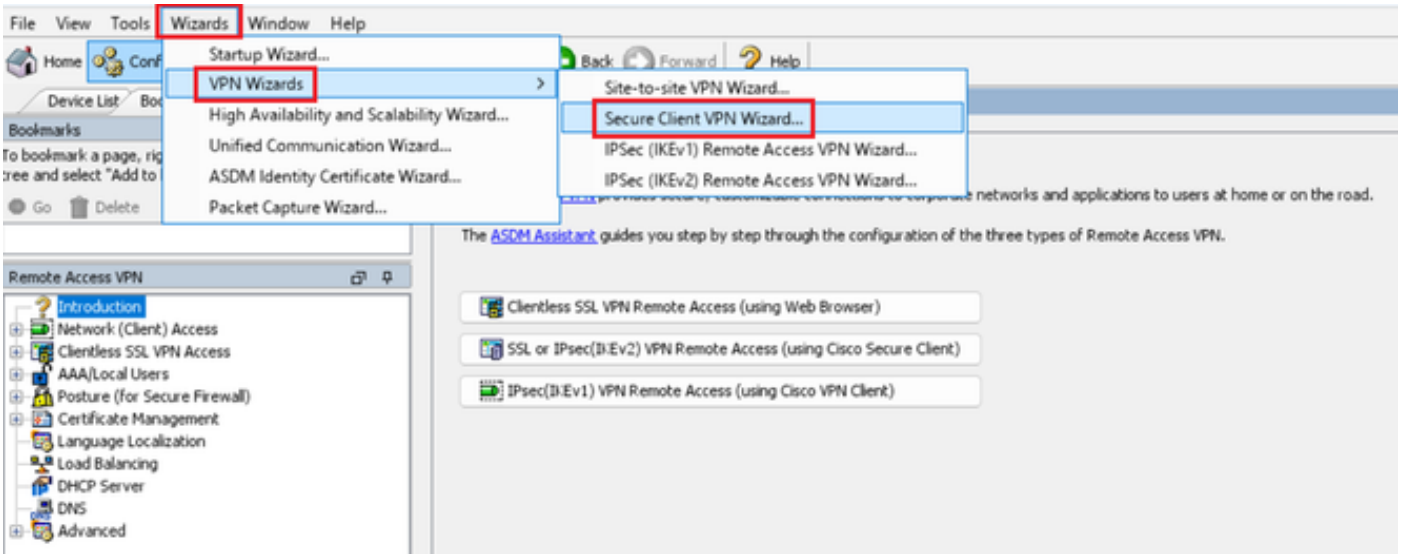
네트워크 다이어그램

설정

ASDM의 컨피그레이션

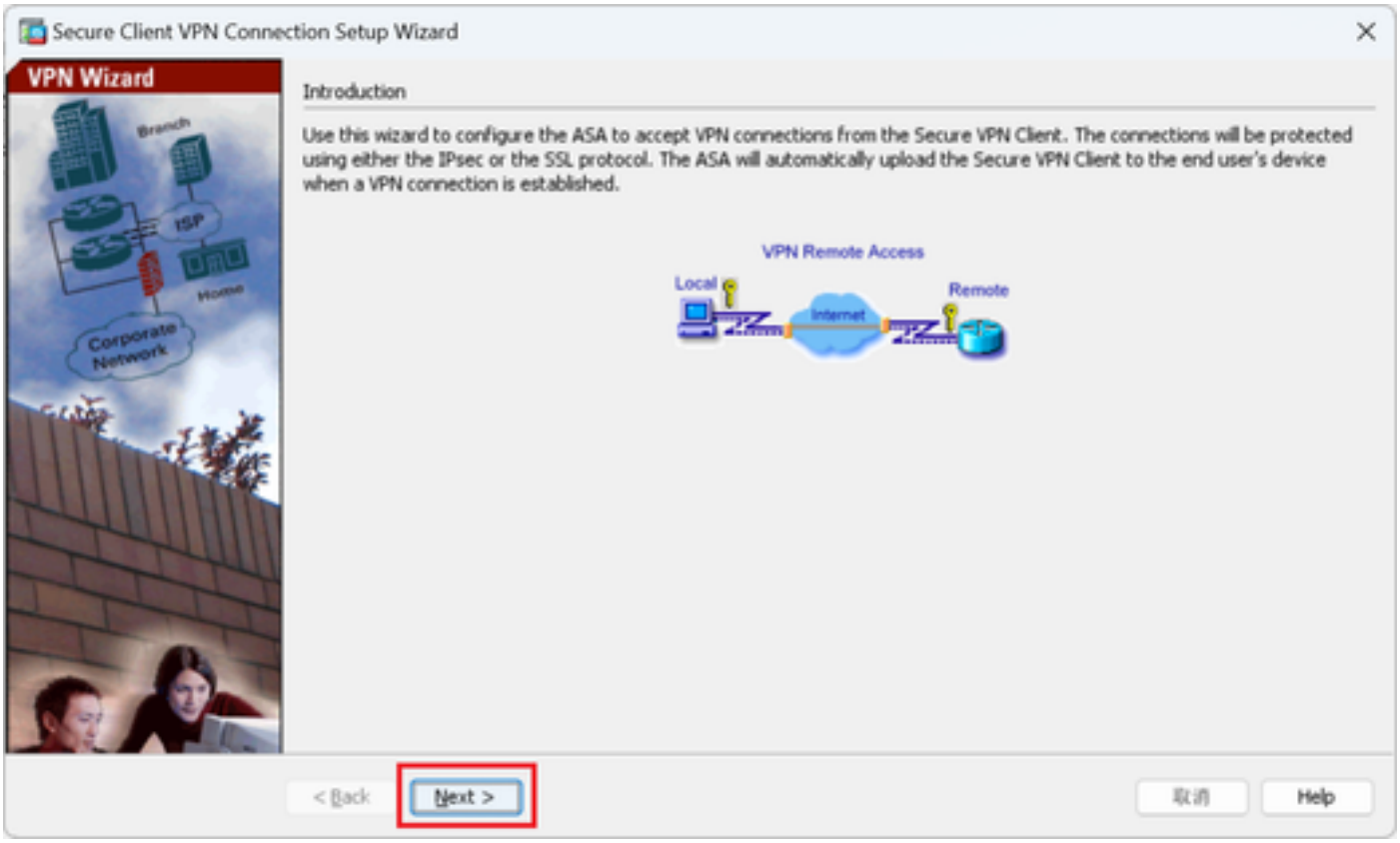
1단계. VPN 마법사 열기

Wizards(마법사) > VPN Wizards(VPN 마법사)로 이동하고 Secure Client VPN Wizard(보안 클라이언트 VPN 마법사)를 클릭합니다.



VPN 마법사 열기

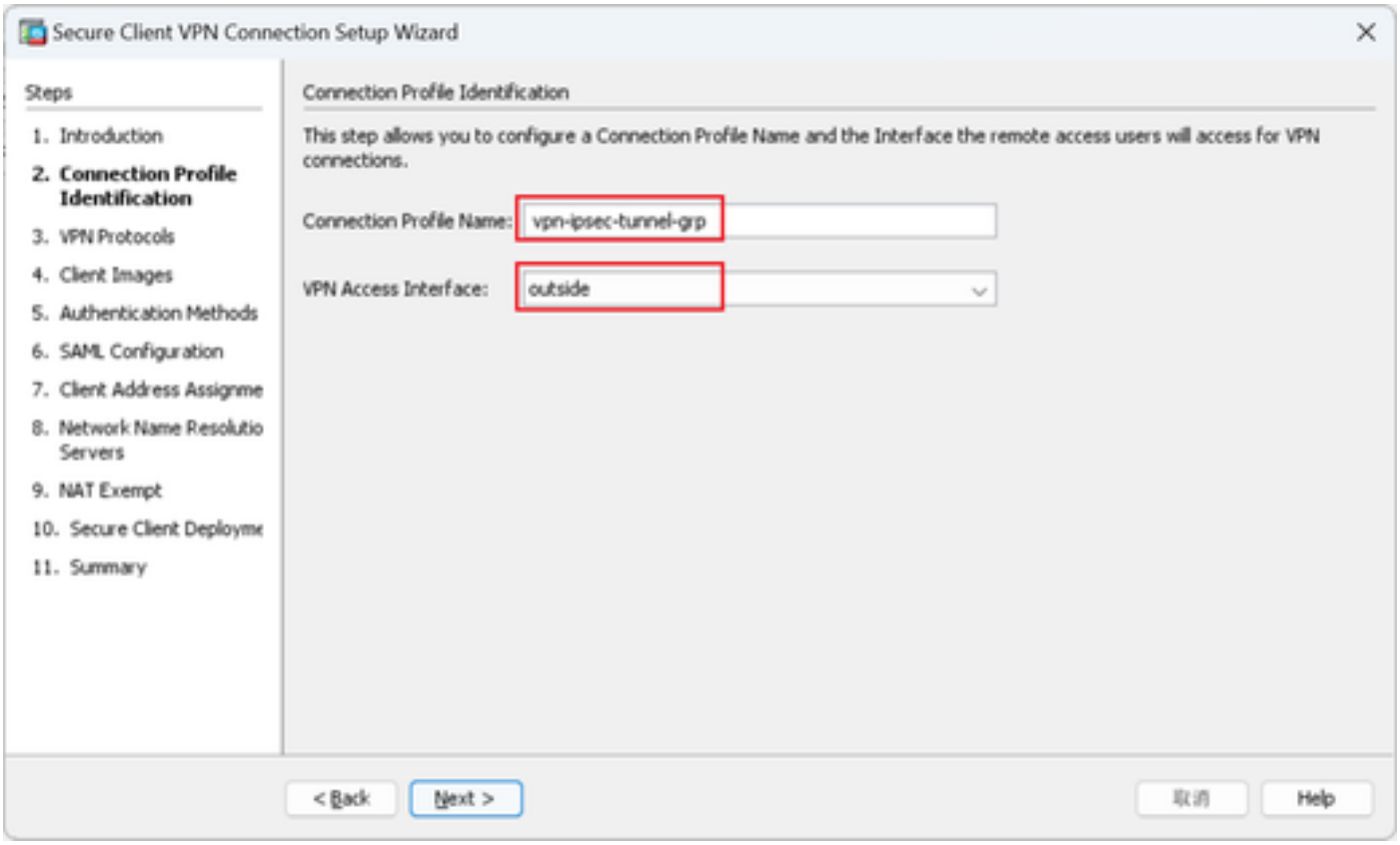
Next(다음)를 클릭합니다.



Next(다음) 버튼 클릭

2단계. 연결 프로파일 식별

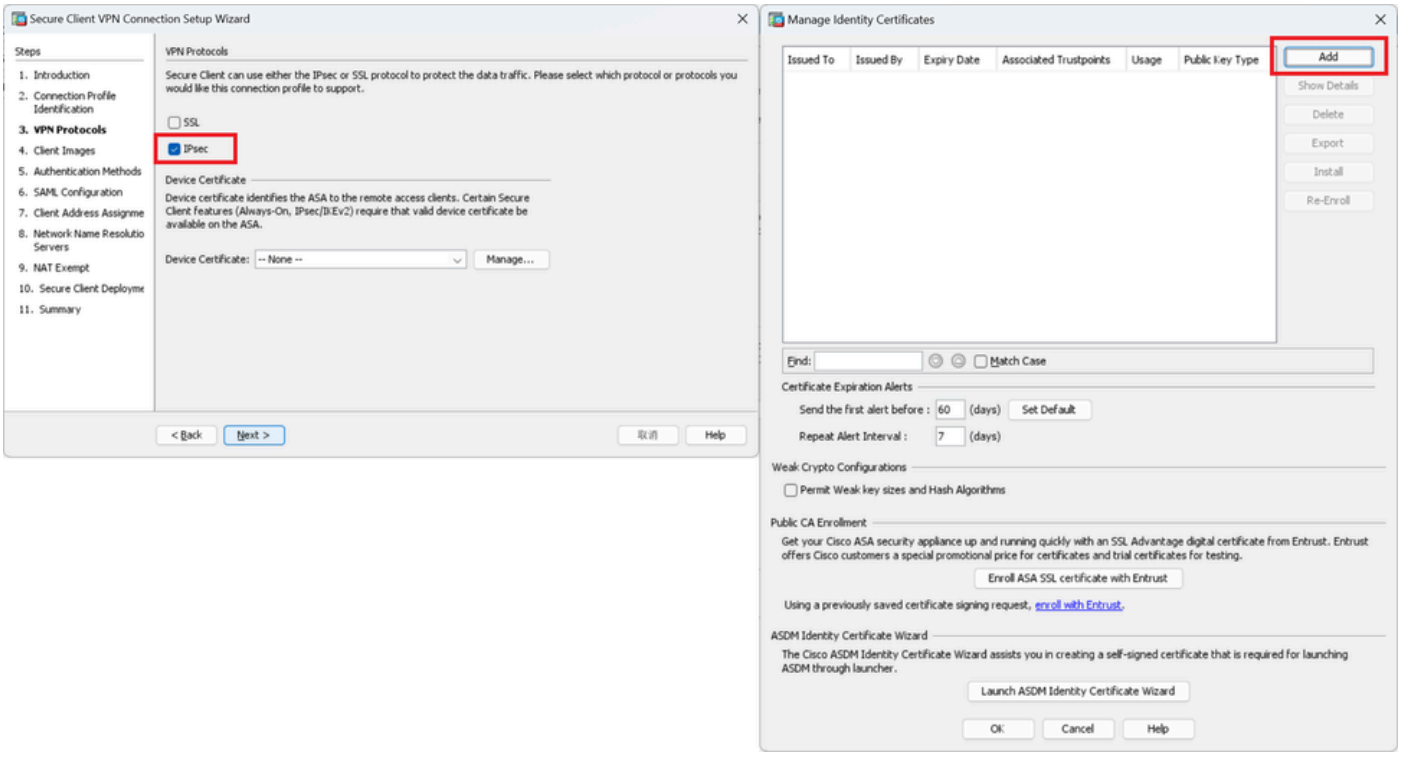
연결 프로파일에 대한 정보를 입력합니다.
연결 프로파일 이름: vpn-ipsec-tunnel-grp
VPN 액세스 인터페이스: 외부



연결 프로파일 식별

3단계. VPN 프로토콜

IPsec을 선택하고 Add(추가) 버튼을 클릭하여 새 자체 서명 인증서를 추가합니다.

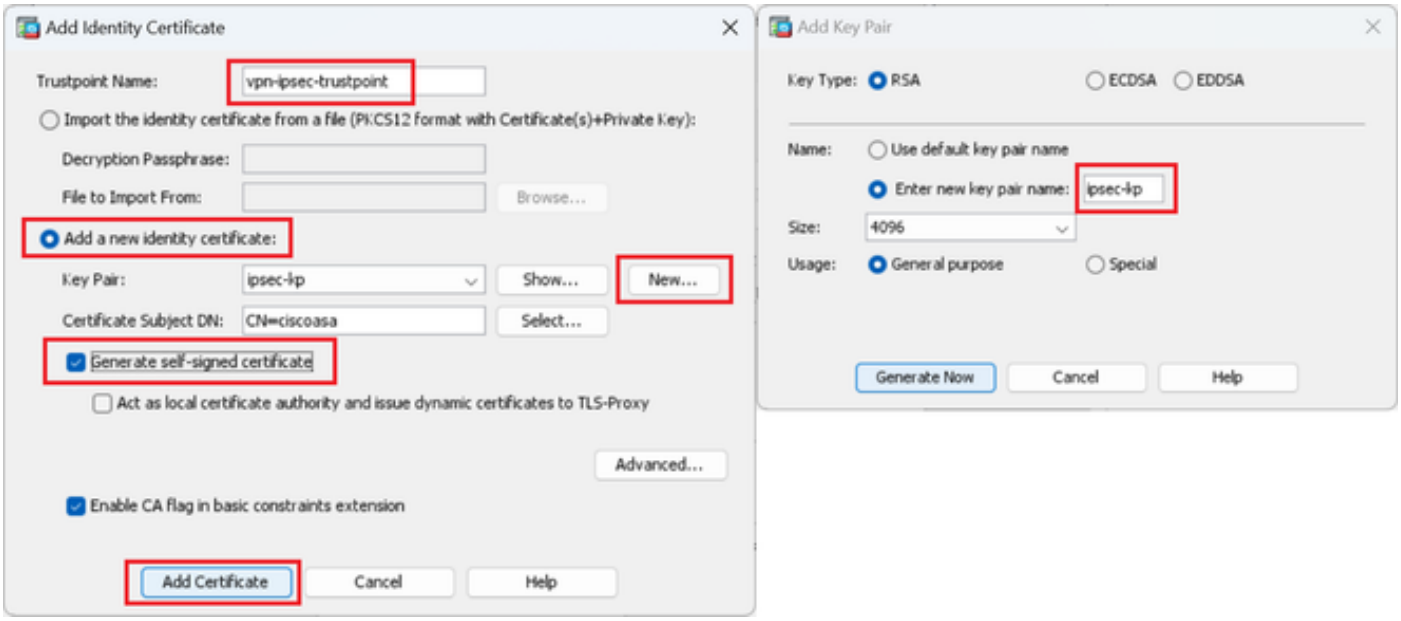


VPN 프로토콜

자체 서명 인증서에 대한 정보를 입력합니다.

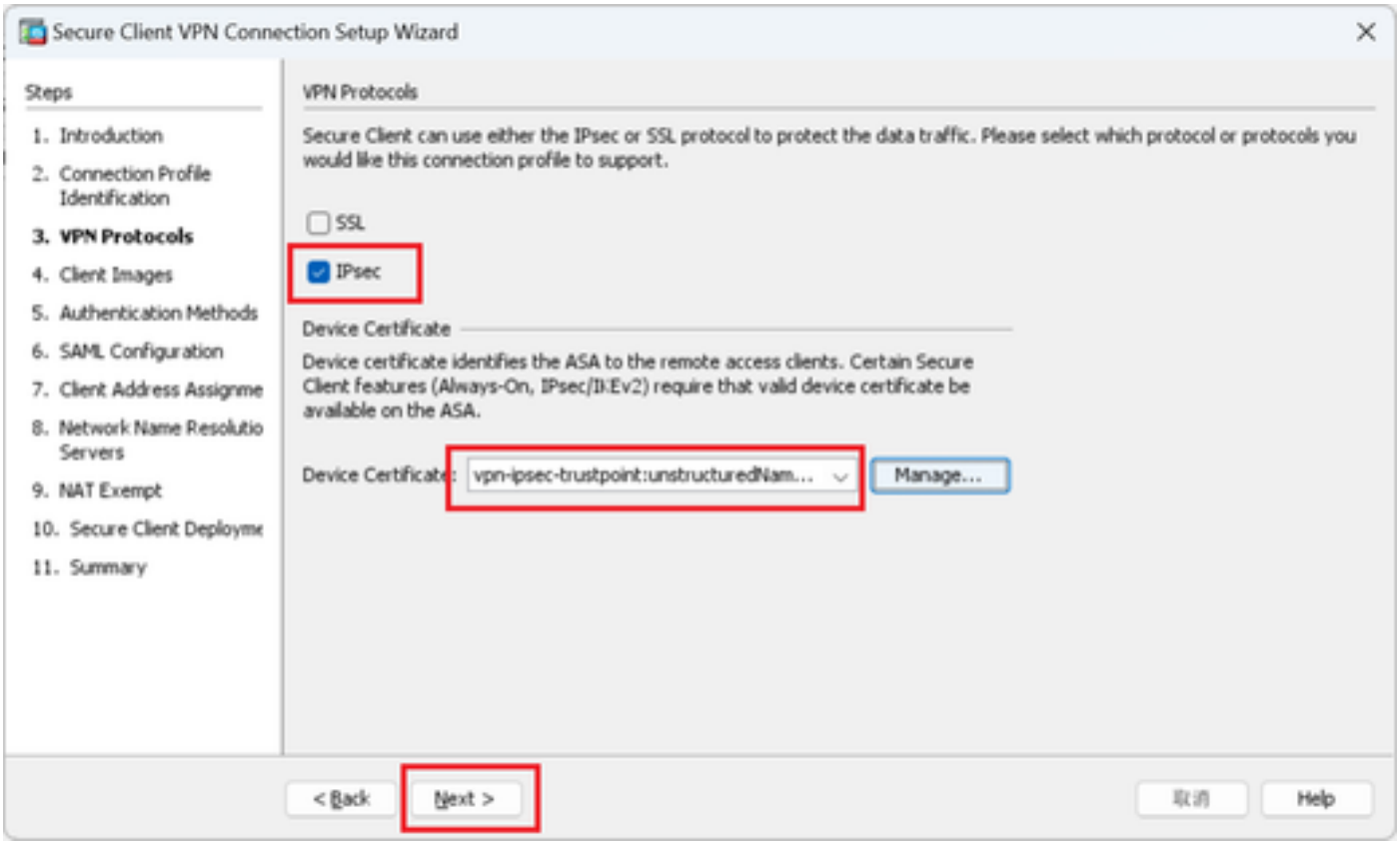
신뢰 지점 이름: vpn-ipsec-trustpoint

키 쌍: ipsec-kp



자체 서명 인증서의 세부 정보

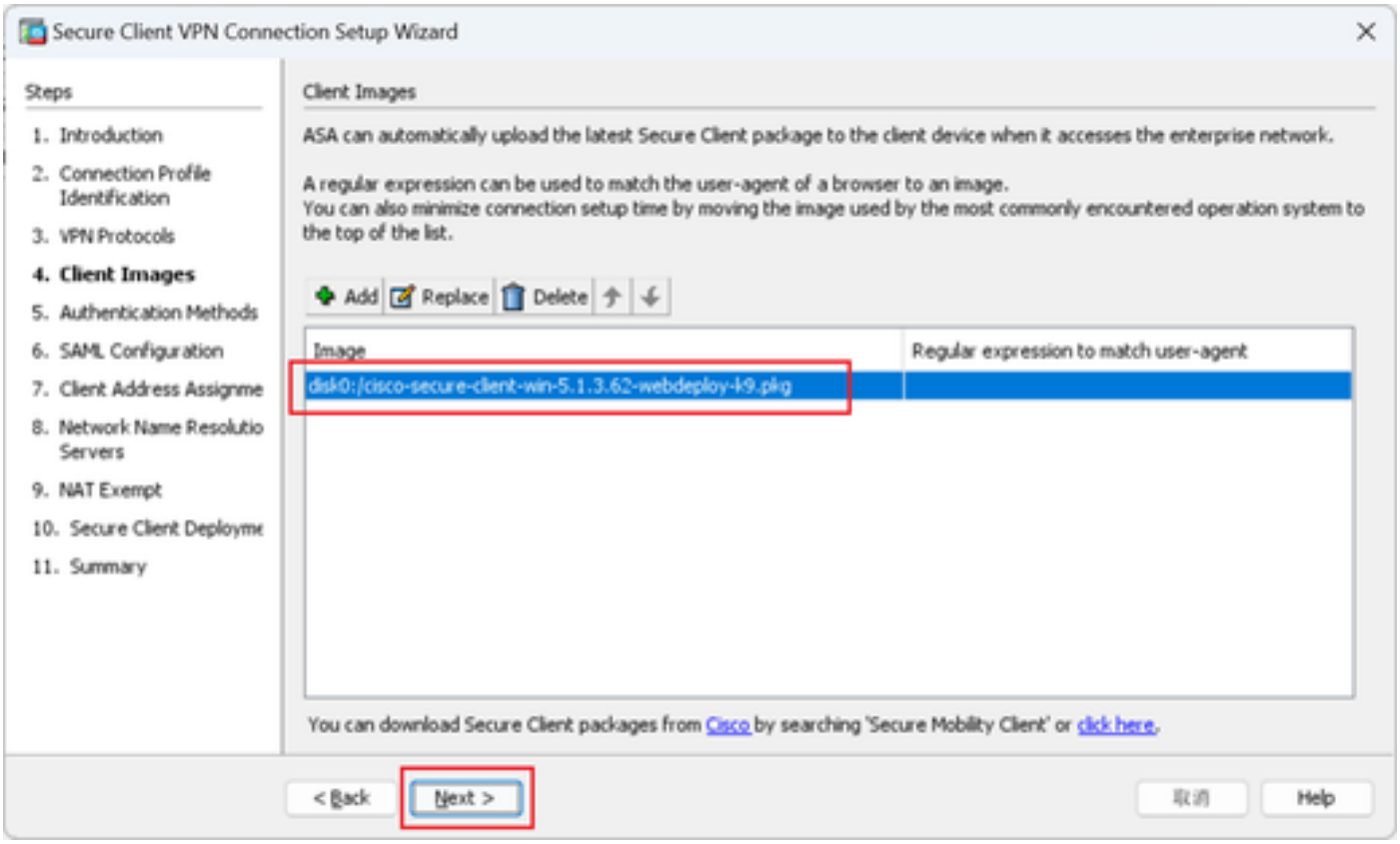
VPN 프로토콜의 설정을 확인하고 Next(다음) 버튼을 클릭합니다.



VPN 프로토콜 설정 확인

4단계. 클라이언트 이미지

보안 클라이언트 이미지를 추가하려면 Add(추가) 버튼을 클릭하고 Next(다음) 버튼을 클릭합니다.



클라이언트 이미지

5단계. 인증 방법

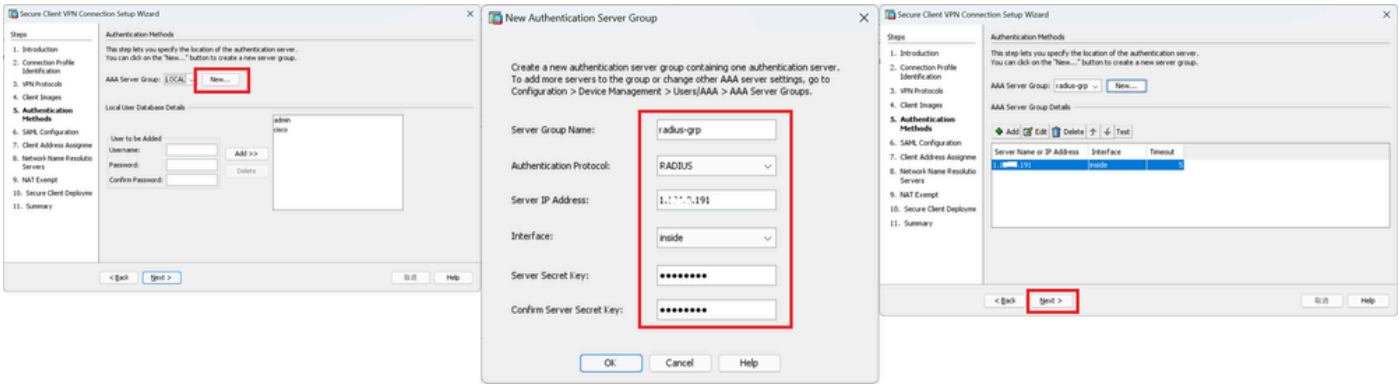
새 aaa 서버를 추가하려면 New 버튼을 클릭하고 Next 버튼을 클릭합니다.

서버 그룹 이름 : radius-grp

인증 프로토콜 : RADIUS

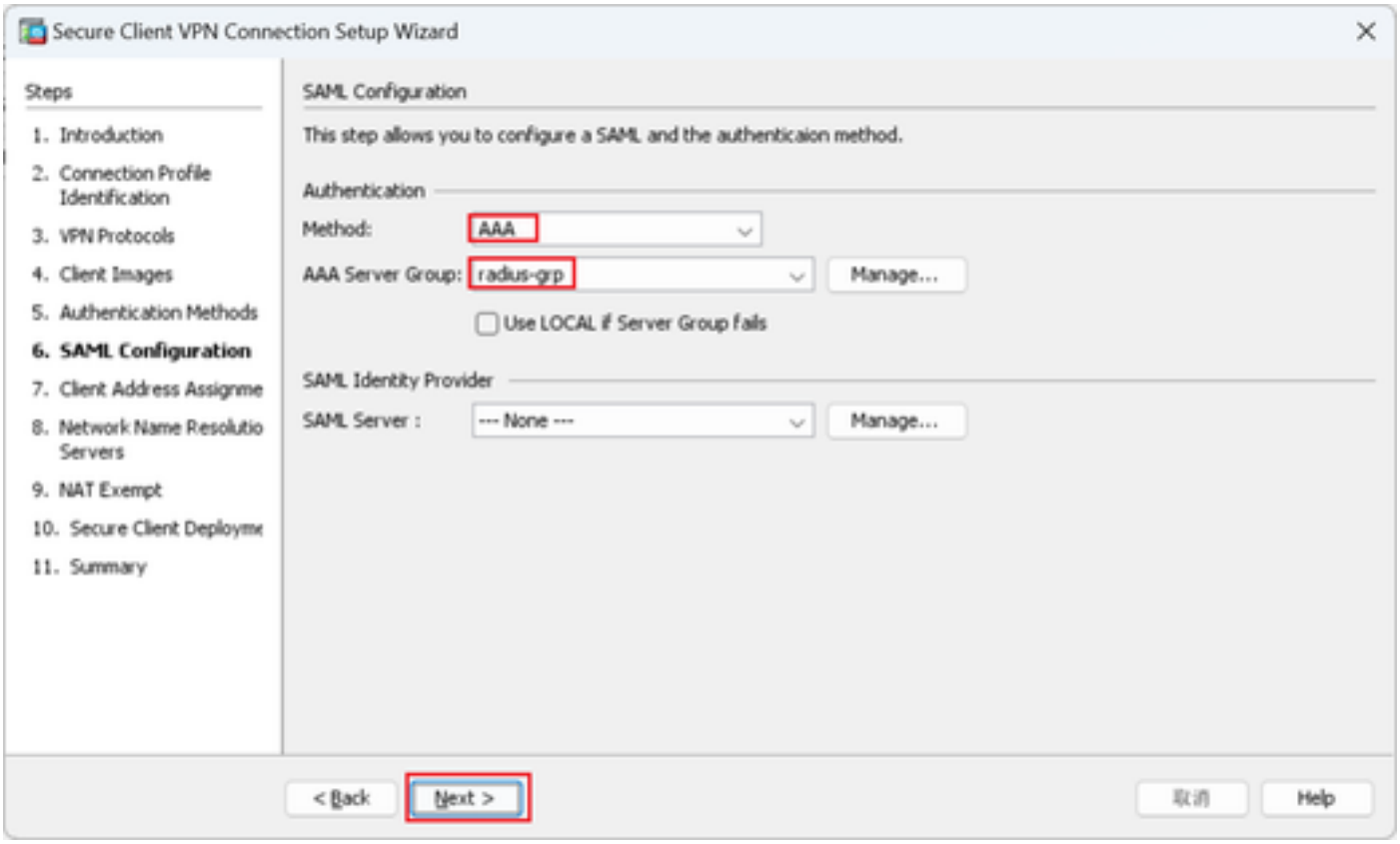
서버 IP 주소: 1.x.x.191

인터페이스 : 내부



6단계. SAML 컨피그레이션

Next(다음) 버튼을 클릭합니다.



SAML 컨피그레이션

7단계. 클라이언트 주소 할당

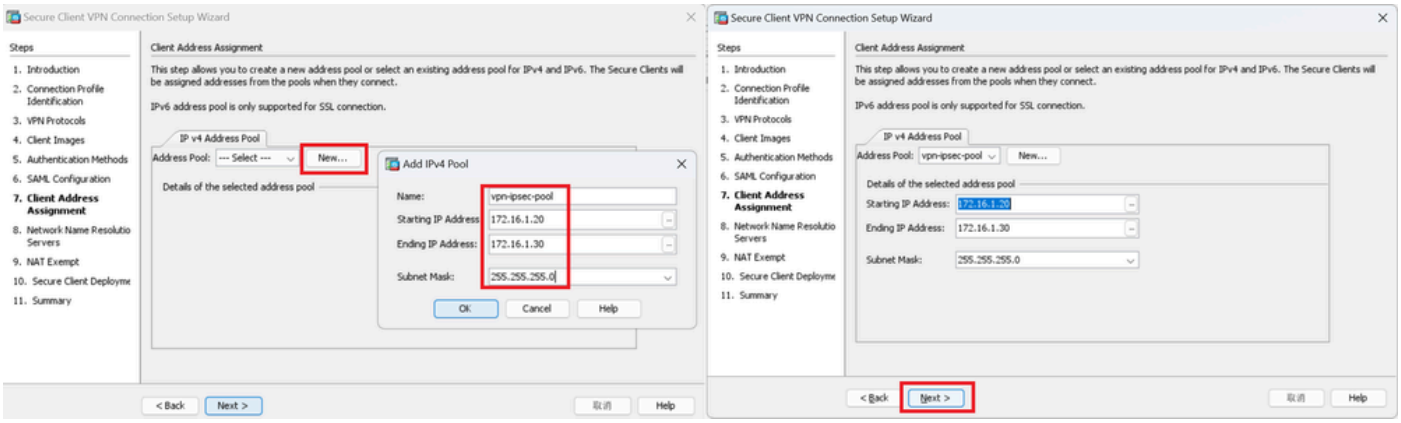
새 IPv4 풀을 추가하려면 New 버튼을 클릭하고 Next 버튼을 클릭합니다.

이름: vpn-ipsec-pool

시작 IP 주소: 172.16.1.20

종료 IP 주소: 172.16.1.30

서브넷 마스크: 255.255.255.0



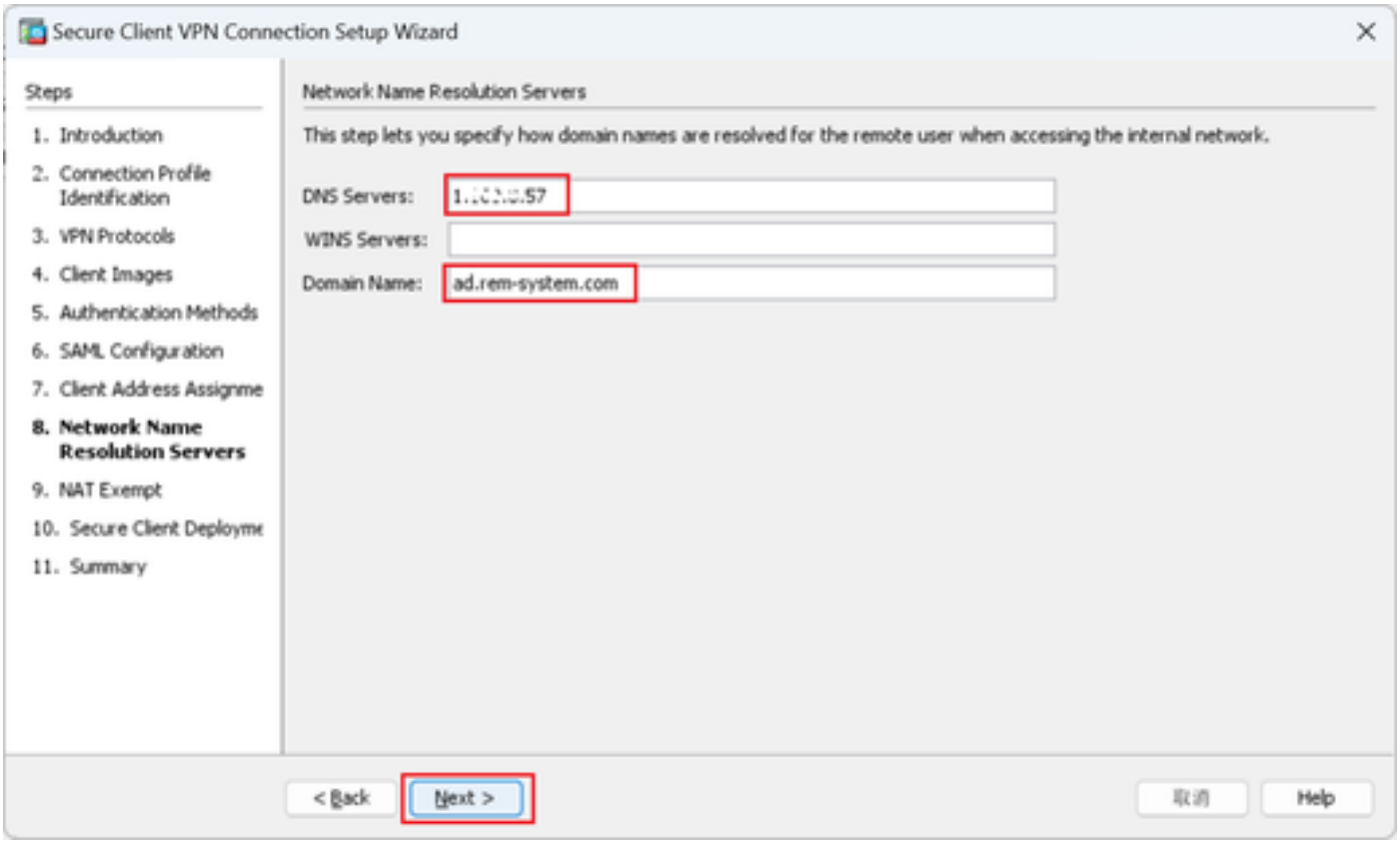
클라이언트 주소 할당

8단계. 네트워크 이름 확인 서버

DNS 및 도메인에 대한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

DNS 서버: 1.x.x.57

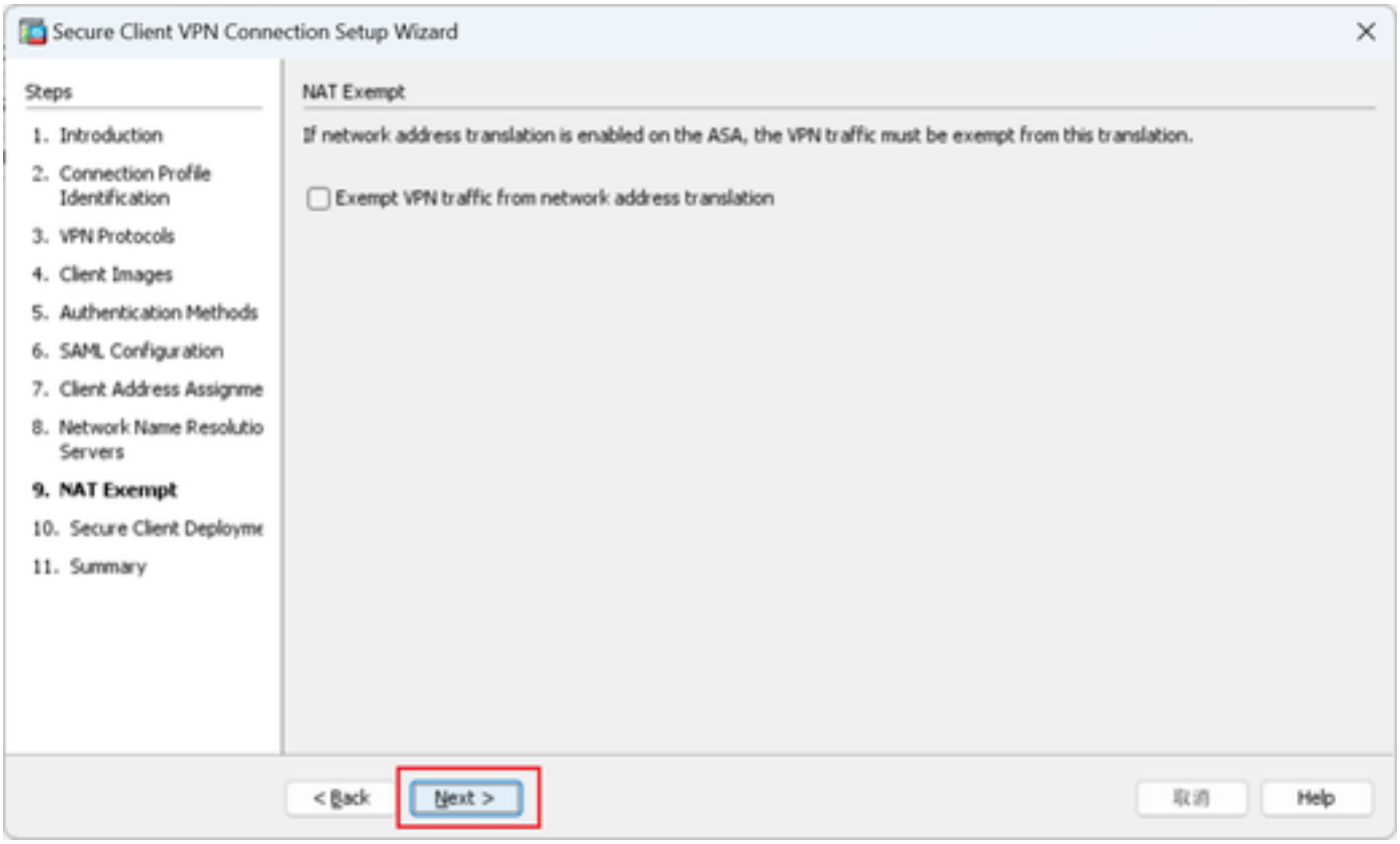
도메인 이름: ad.rem-system.com



네트워크 이름 확인 서버

9단계. NAT 제외

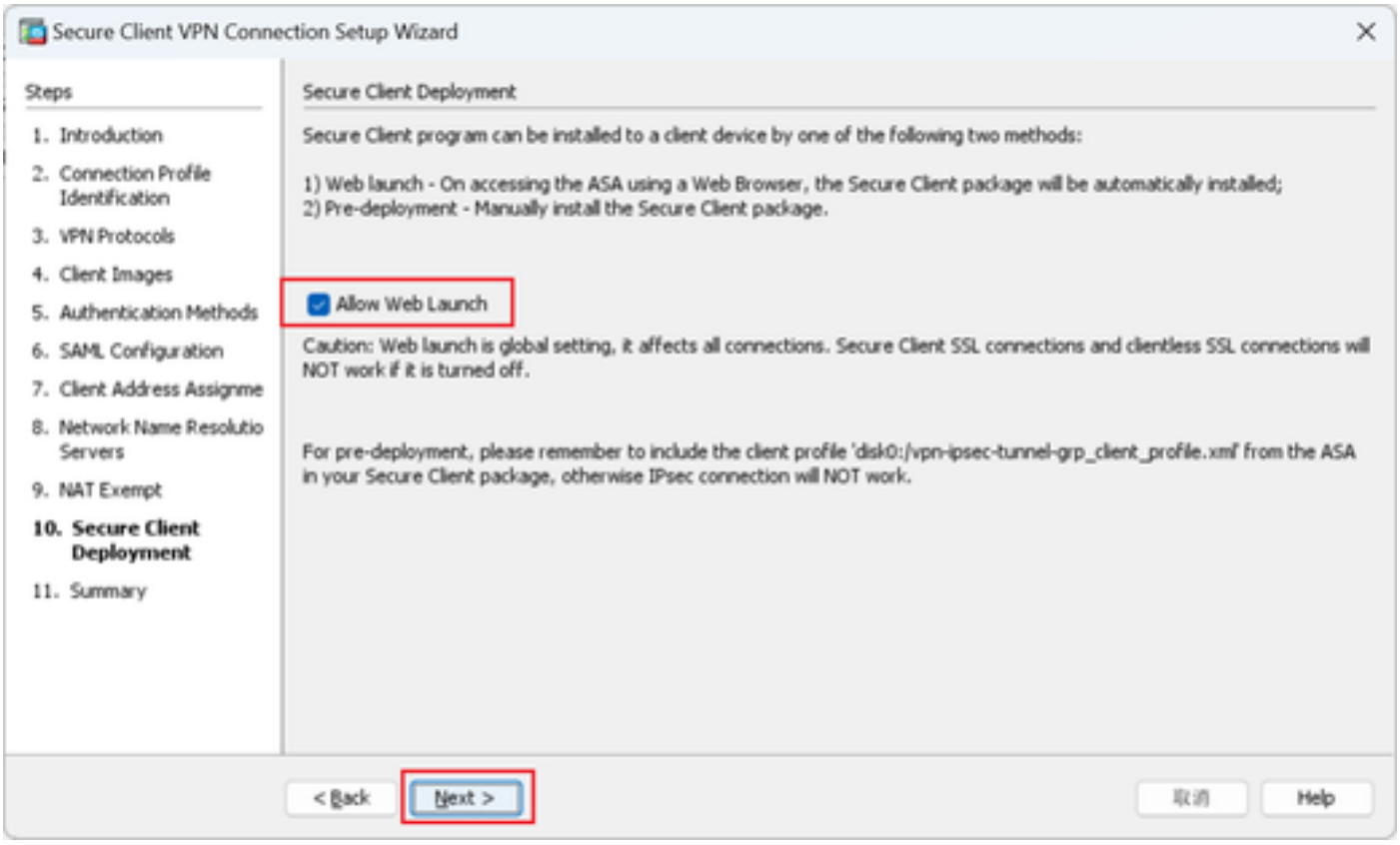
Next(다음) 버튼을 클릭합니다.



NAT 제외

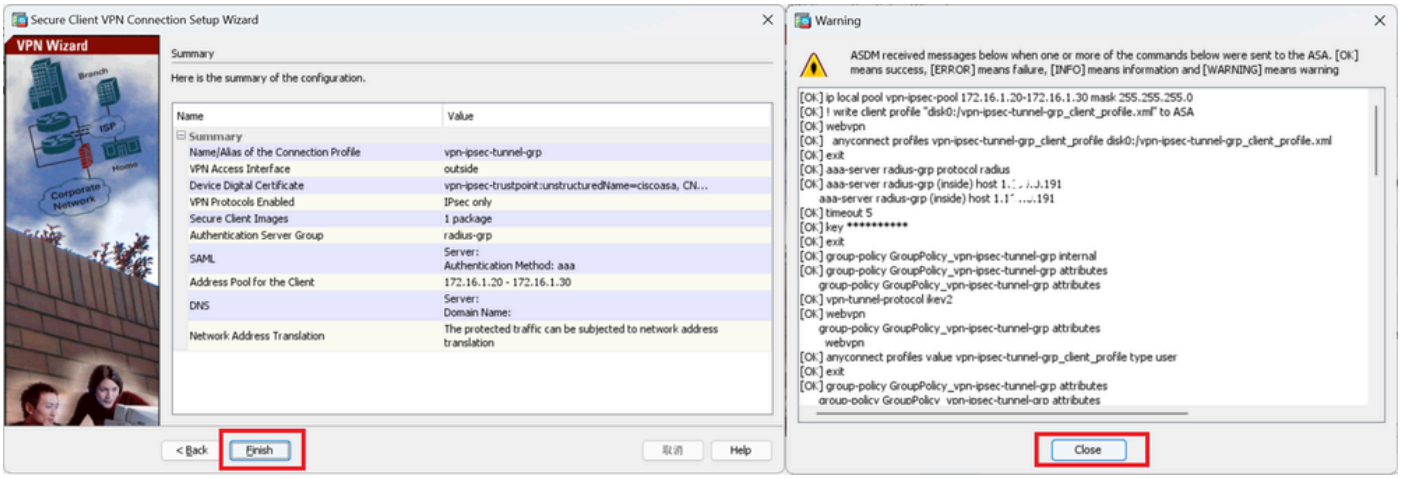
10단계. 보안 클라이언트 구축

Allow Web Launch(웹 실행 허용)를 선택하고 Next(다음) 단추를 클릭합니다.



11단계. 설정 저장

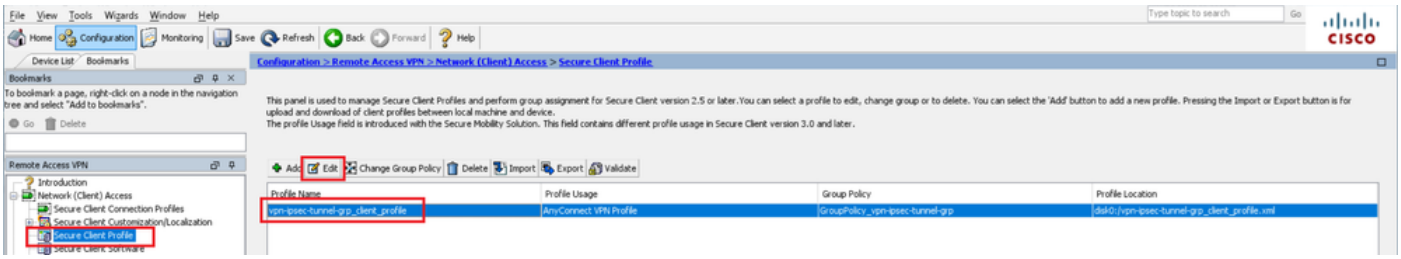
Finish(마침) 버튼을 클릭하고 설정을 저장합니다.



설정 저장

12단계. 보안 클라이언트 프로파일 확인 및 내보내기

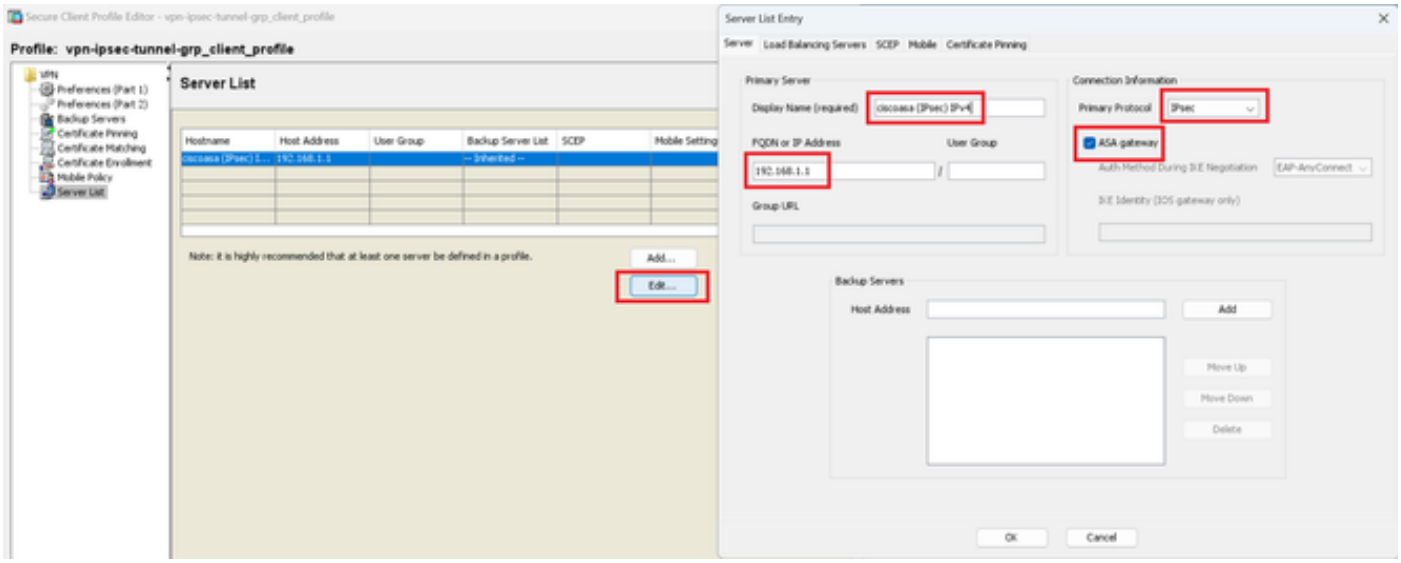
Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Client Profile(보안 클라이언트 프로파일)로 이동하고 Edit(편집) 버튼을 클릭합니다.



보안 클라이언트 프로파일 편집

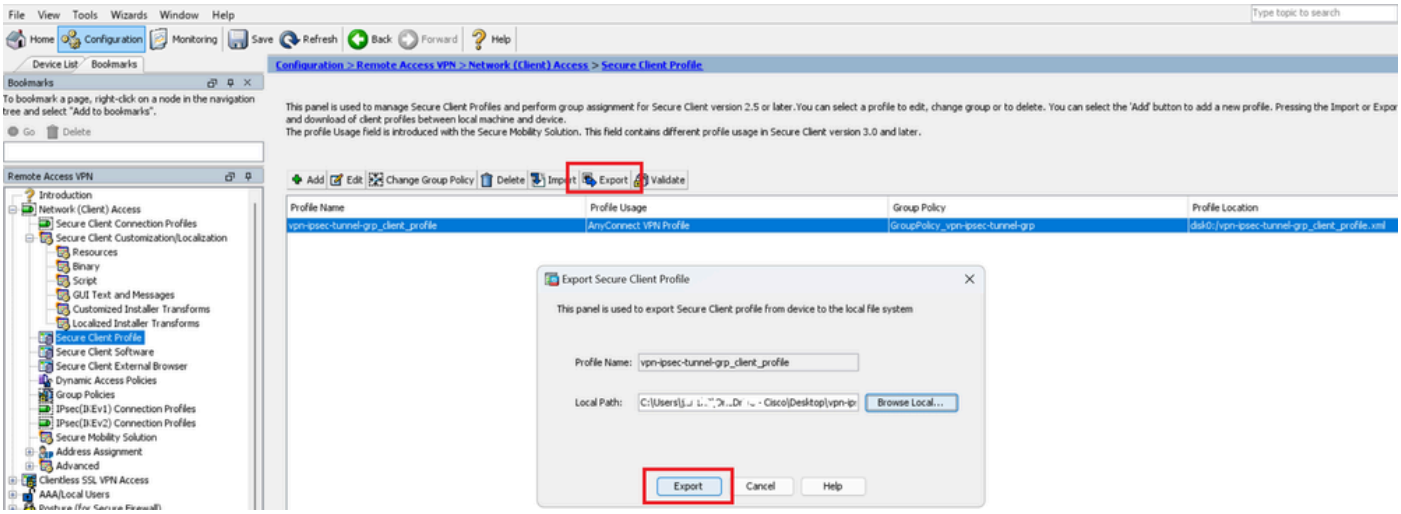
프로필의 세부사항을 확인합니다.

- 표시 이름(필수) : ciscoasa (IPsec) IPv4
- FQDN 또는 IP 주소: 192.168.1.1
- 기본 프로토콜: IPsec



보안 클라이언트 프로파일 확인

프로필을 로컬 PC로 내보내려면 Export(내보내기) 버튼을 클릭합니다.



보안 클라이언트 프로파일 내보내기

13단계. 보안 클라이언트 프로파일 세부 정보 확인

Secure Client Profile by browser(브라우저별 보안 클라이언트 프로파일)를 열고 호스트의 기본 프로토콜이 IPsec인지 확인합니다.

```
<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>
```

14단계. ASA CLI에서 설정 확인

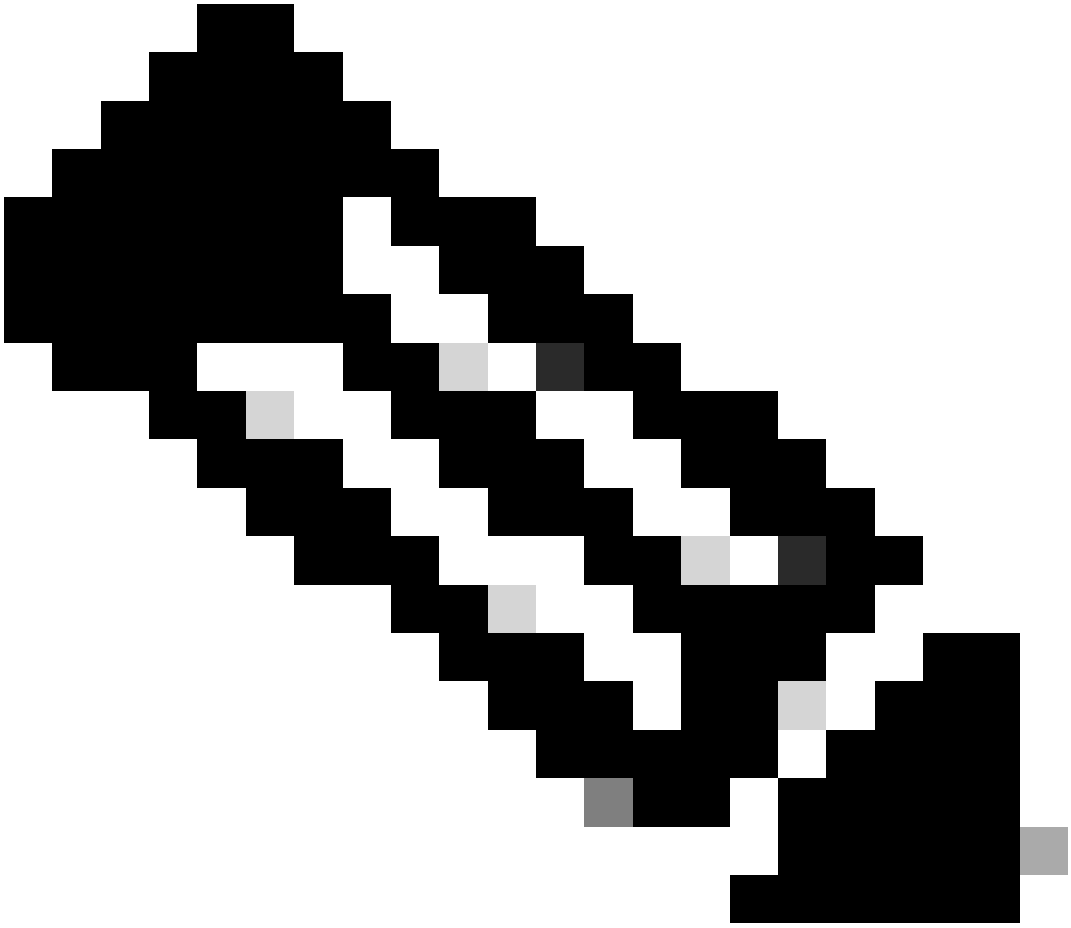
ASA CLI에서 ASDM에 의해 생성된 IPsec 설정을 확인합니다.

```
// 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
```

15단계. 암호화 알고리즘 추가

ASA CLI에서 IKEv2 정책에 그룹 19를 추가합니다.

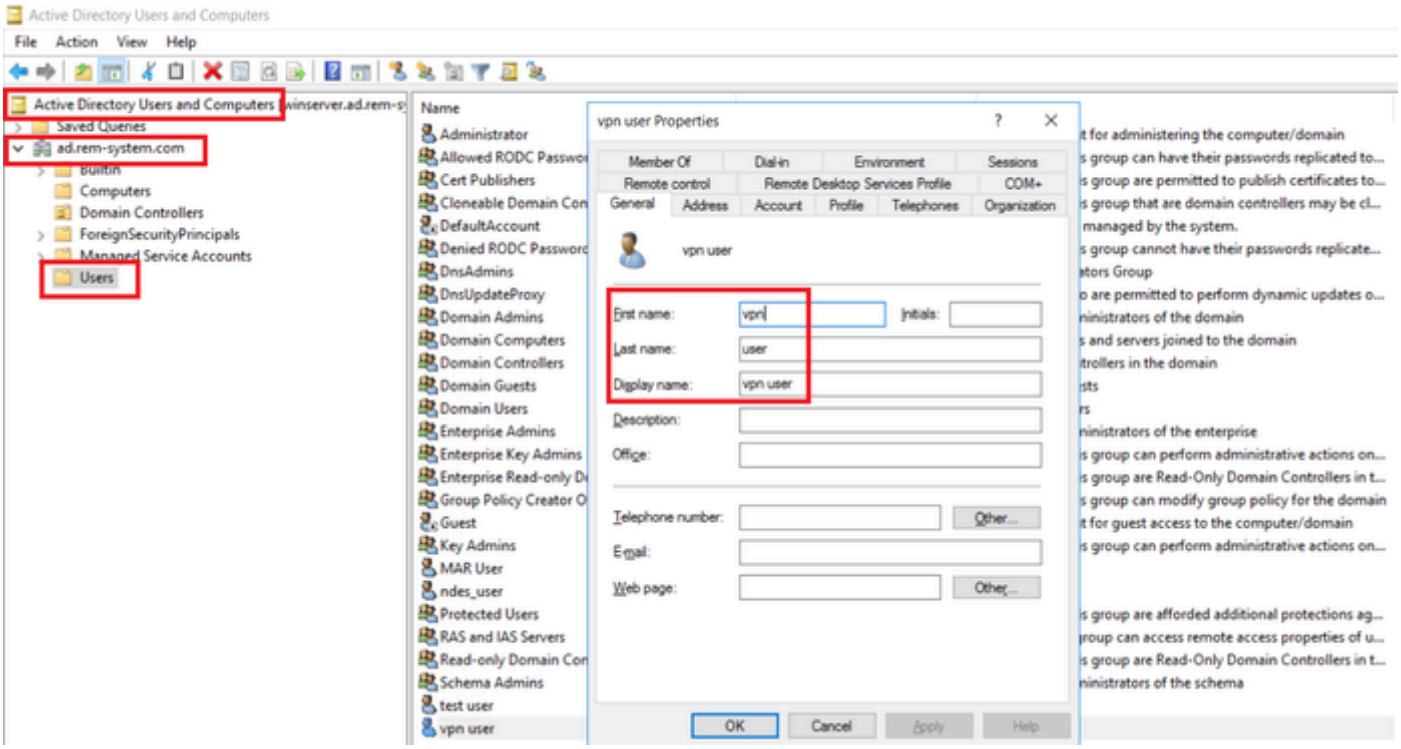


참고: IKEv2/IPsec 연결의 경우 Cisco Secure Client는 버전 4.9.00086부터 DH(Diffie-Hellman) 그룹 2, 5, 14, 24를 더 이상 지원하지 않습니다. 이러한 변경으로 인해 암호화 알고리즘 불일치로 인해 연결 실패가 발생할 수 있습니다.

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

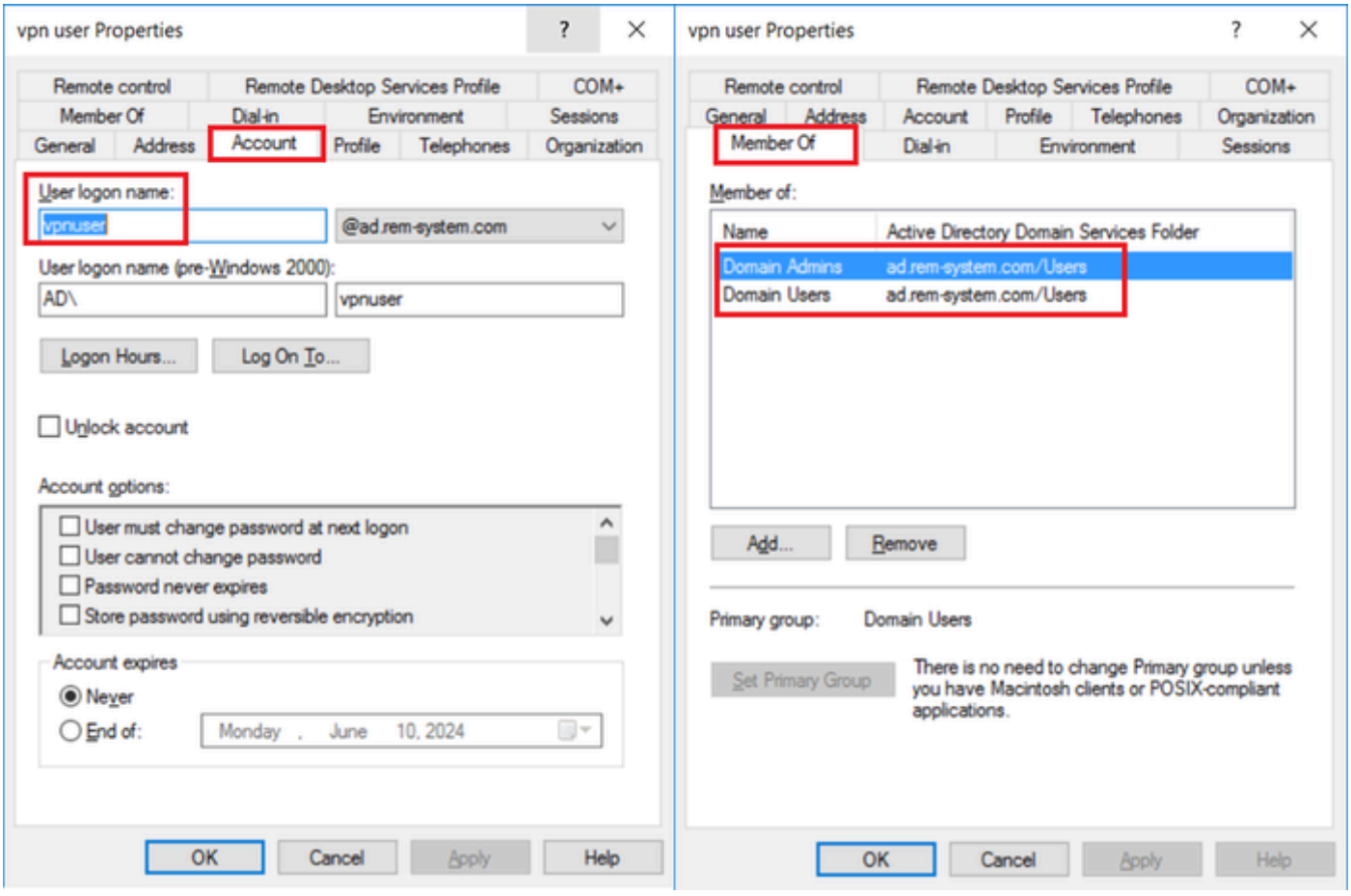
Windows Server의 구성

VPN 연결을 위해 도메인 사용자를 추가해야 합니다. Active Directory 사용자 및 컴퓨터로 이동한 다음 사용자를 클릭합니다. vpnuser를 도메인 사용자로 추가합니다.



도메인 사용자 추가

Domain Admins 및 Domain Users의 구성원에 도메인 사용자를 추가합니다.

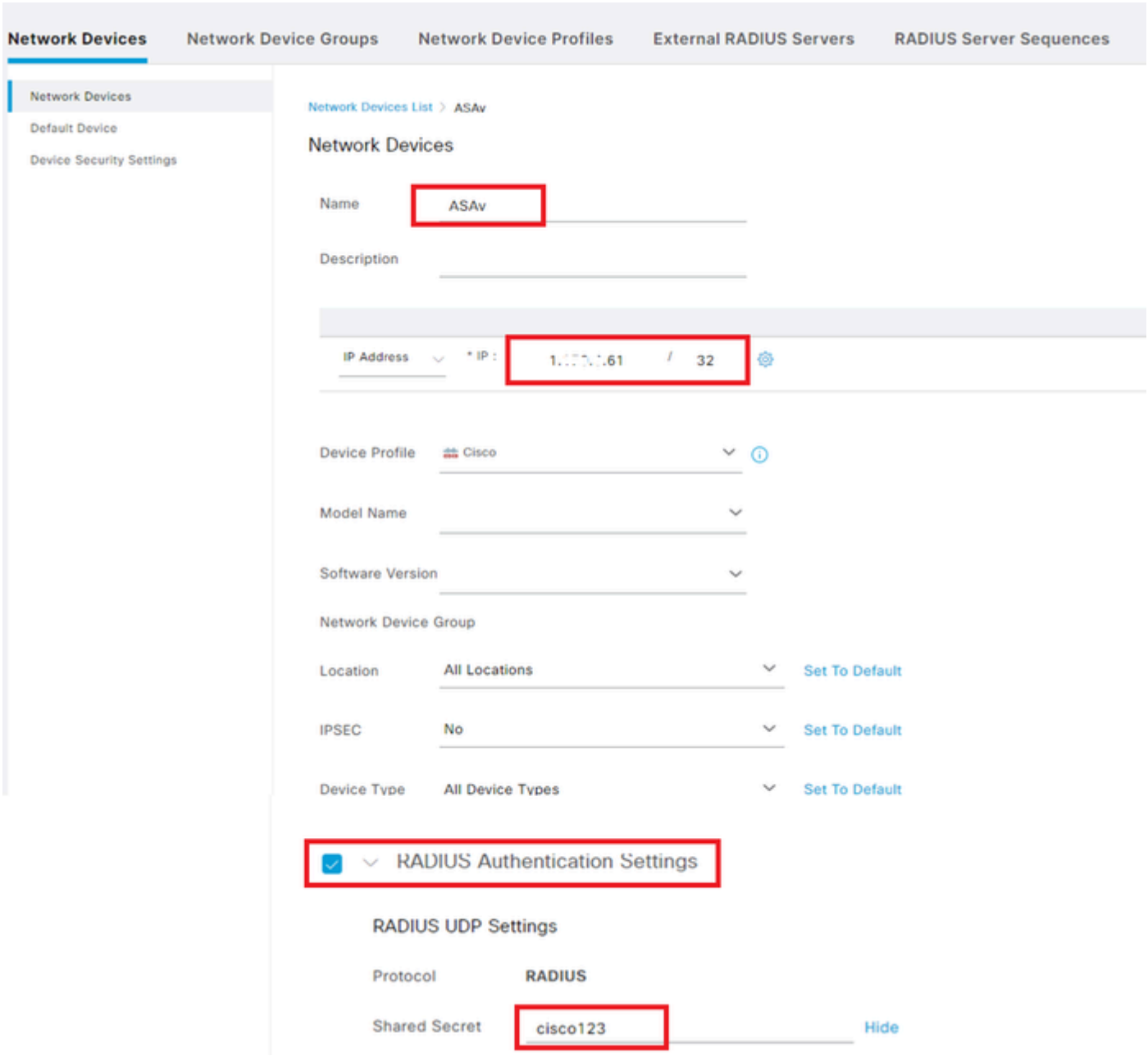


도메인 관리자 및 도메인 사용자

ISE의 컨피그레이션

1단계. 장치 추가

Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)button을 클릭하여 ASAv 디바이스를 추가합니다.

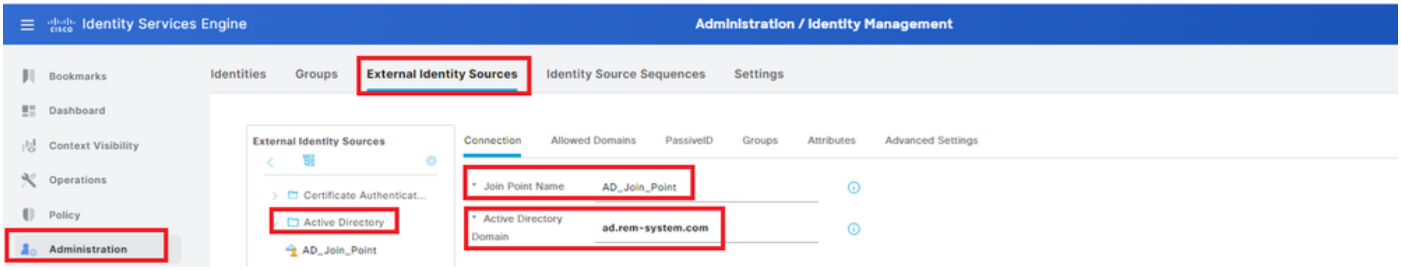


장치 추가

2단계. Active Directory 추가

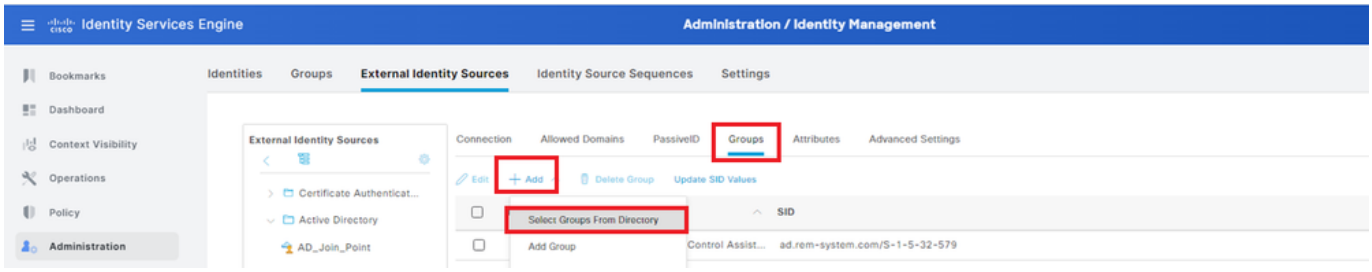
Administration(관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동하고 Connectiontab(연결 탭)을 클릭한 다음 Active Directory를 ISE에 추가합니다.

- 조인 지점 이름: AD_Join_Point
- Active Directory 도메인: ad.rem-system.com



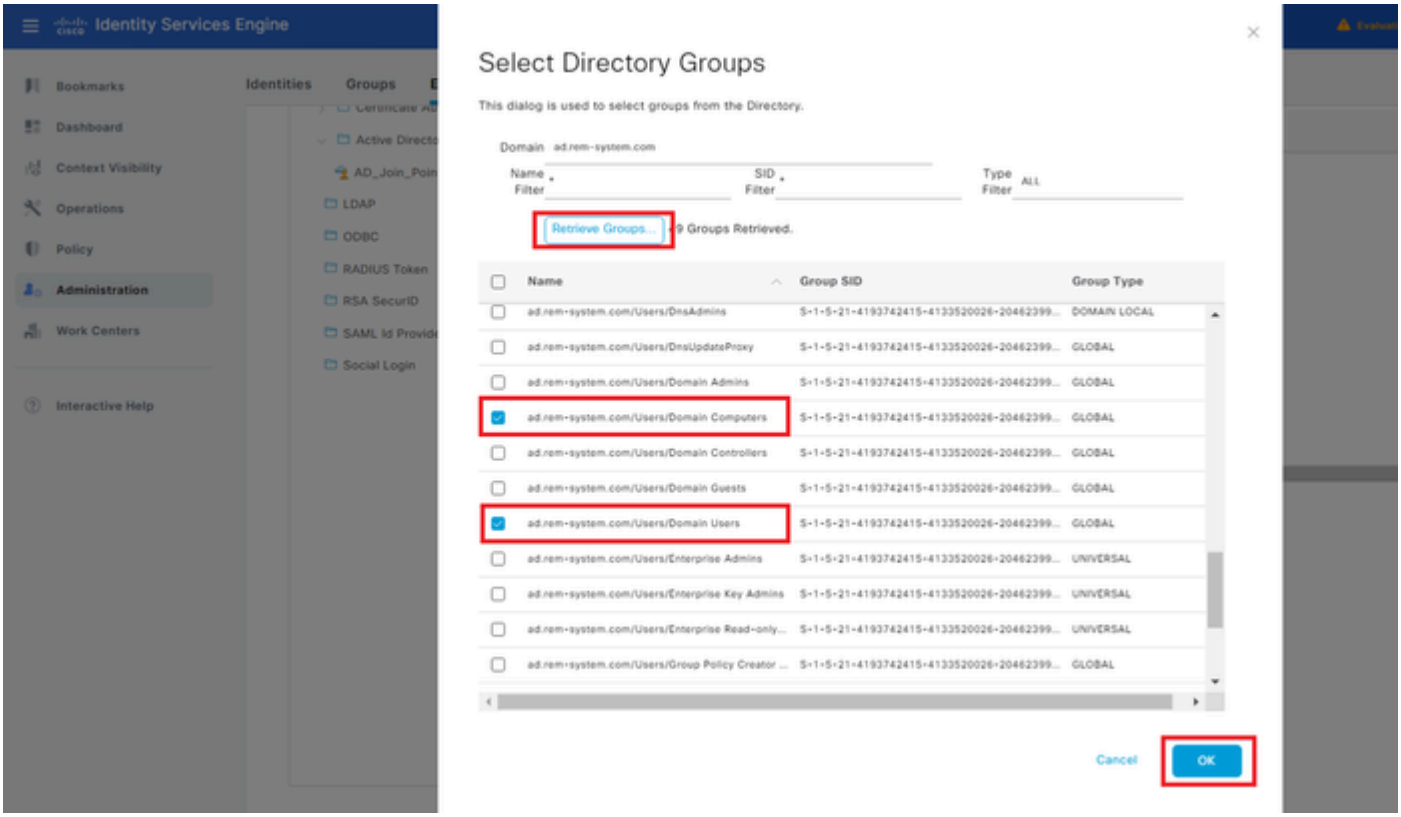
Active Directory 추가

그룹 탭으로 이동하여 디렉터리에서 그룹 선택 드롭다운 목록을 선택합니다.디렉터리에서 그룹



을
선택합니다

그룹 검색(Retrieve Groups)시작(From) 드롭다운 목록을 누릅니다. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain 사용자를 클릭한 다음 OK를 클릭합니다.



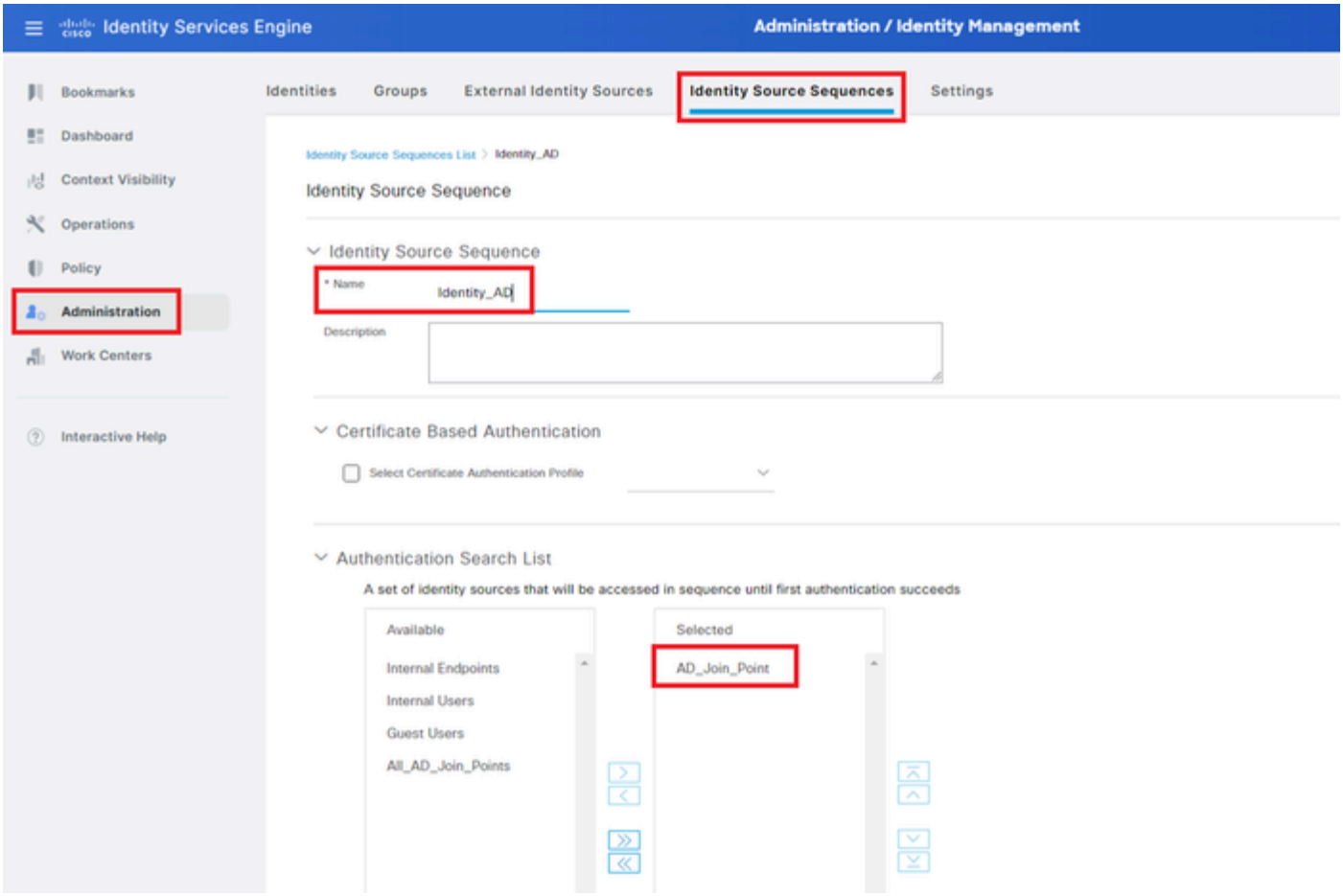
도메인 컴퓨터 및 사용자 추가

3단계. ID 소스 시퀀스 추가

Administration(관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동하여 ID 소스 시퀀스를

추가합니다.

- 이름: Identity_AD
- 인증 검색 목록: AD_Join_Point

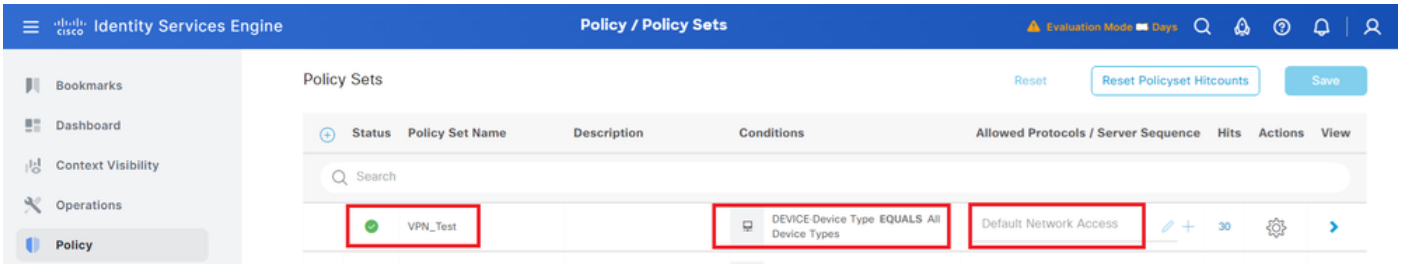


ID 소스 시퀀스 추가

4단계. 정책 집합 추가

Policy(정책) > Policy Sets(정책 세트)로 이동하고 +를 클릭하여 정책 세트를 추가합니다.

- 정책 집합 이름: VPN_Test
- 조건: 장치 장치 유형이 모든 장치 유형과 같음
- 허용되는 프로토콜/서버 시퀀스: 기본 네트워크 액세스

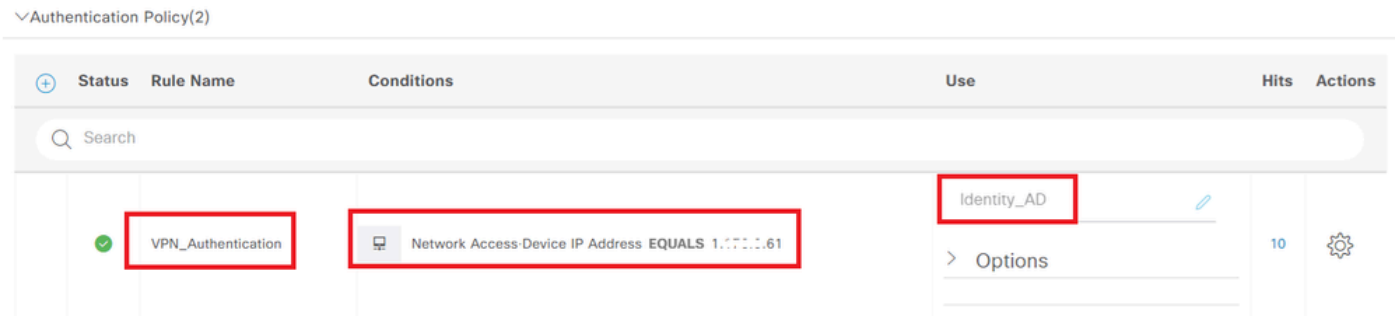


정책 집합 추가

5단계. 인증 정책 추가

Policy Sets(정책 집합)로 이동하고 VPN_Test를 클릭하여 인증 정책을 추가합니다.

- 규칙 이름: VPN_Authentication
- 조건: 네트워크 액세스 디바이스 IP 주소가 1.x.x.61과 같음
- 사용: Identity_AD

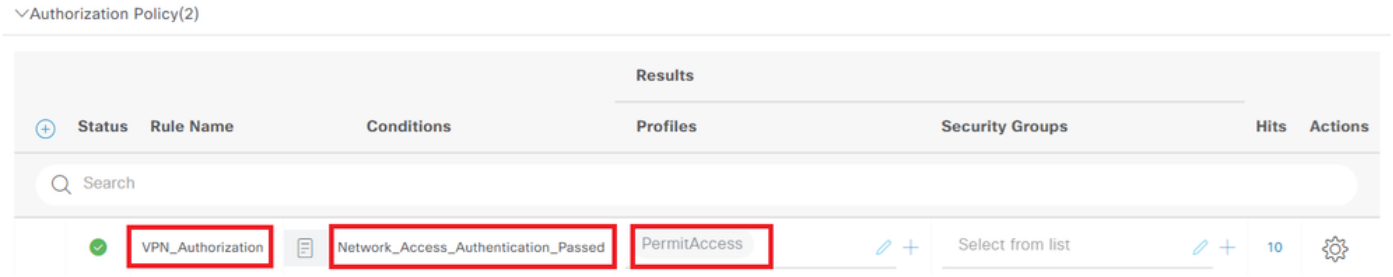


인증 정책 추가

6단계. 권한 부여 정책 추가

Policy Sets(정책 집합)로 이동하고 VPN_Test를 클릭하여 권한 부여 정책을 추가합니다.

- 규칙 이름: VPN_Authorization
- 조건: Network_Access_Authentication_Passed
- 결과: PermitAccess

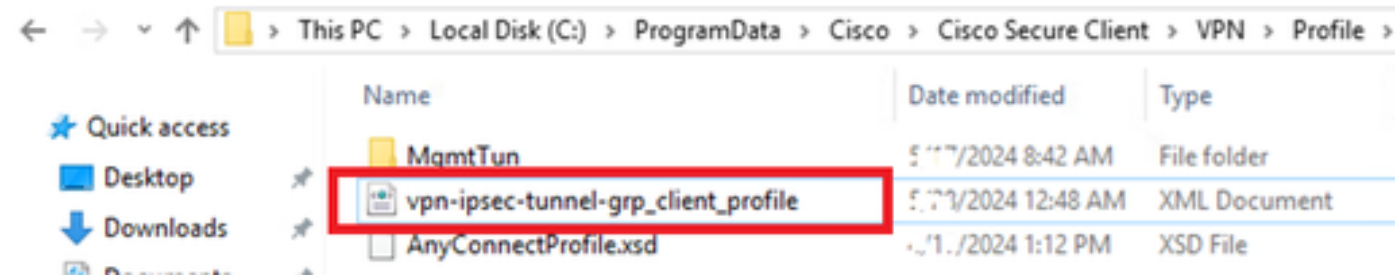


권한 부여 정책 추가

다음을 확인합니다.

1단계. Win10 PC1에 보안 클라이언트 프로필 복사

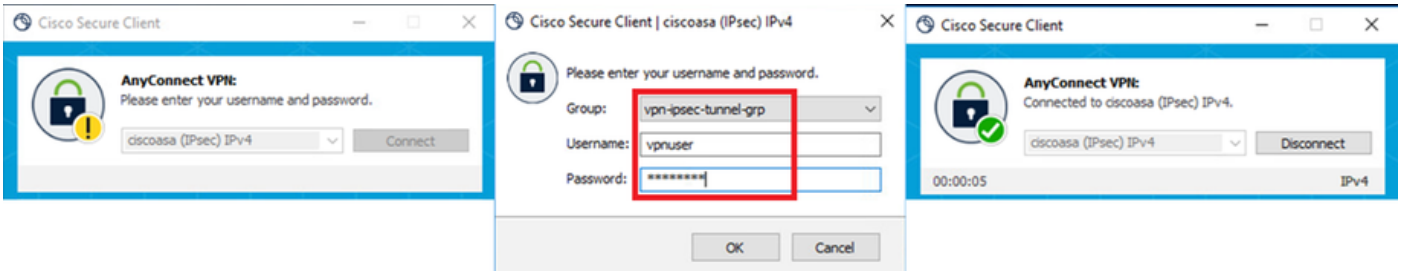
보안 클라이언트 프로파일을 C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile 디렉토리에 복사합니다.



PC에 프로필 복사

2단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client를 실행하고 사용자 이름과 비밀번호를 입력한 다음 Cisco Secure Client가 성공적으로 연결되었는지 확인합니다.



연결 성공

3단계. ASA의 Syslog 확인

syslog에서 IKEv2 연결이 성공했는지 확인합니다.

<#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
```

4단계. ASA에서 IPsec 세션 확인

run show vpn-sessiondb detail anyconnect 명령을 사용하여 ASA의 IKEv2/IPsec 세션을 확인합니다.

<#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

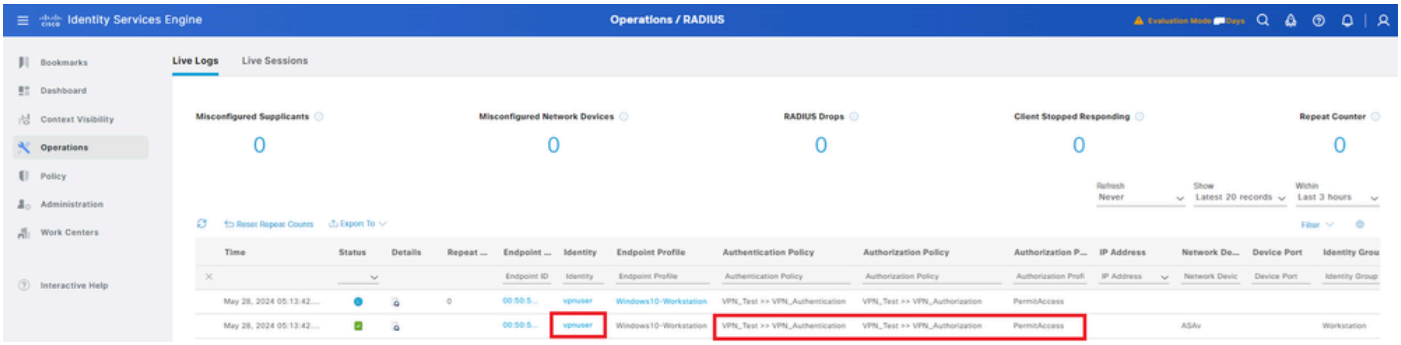
IPsecOverNatT Tunnels: 1

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
```

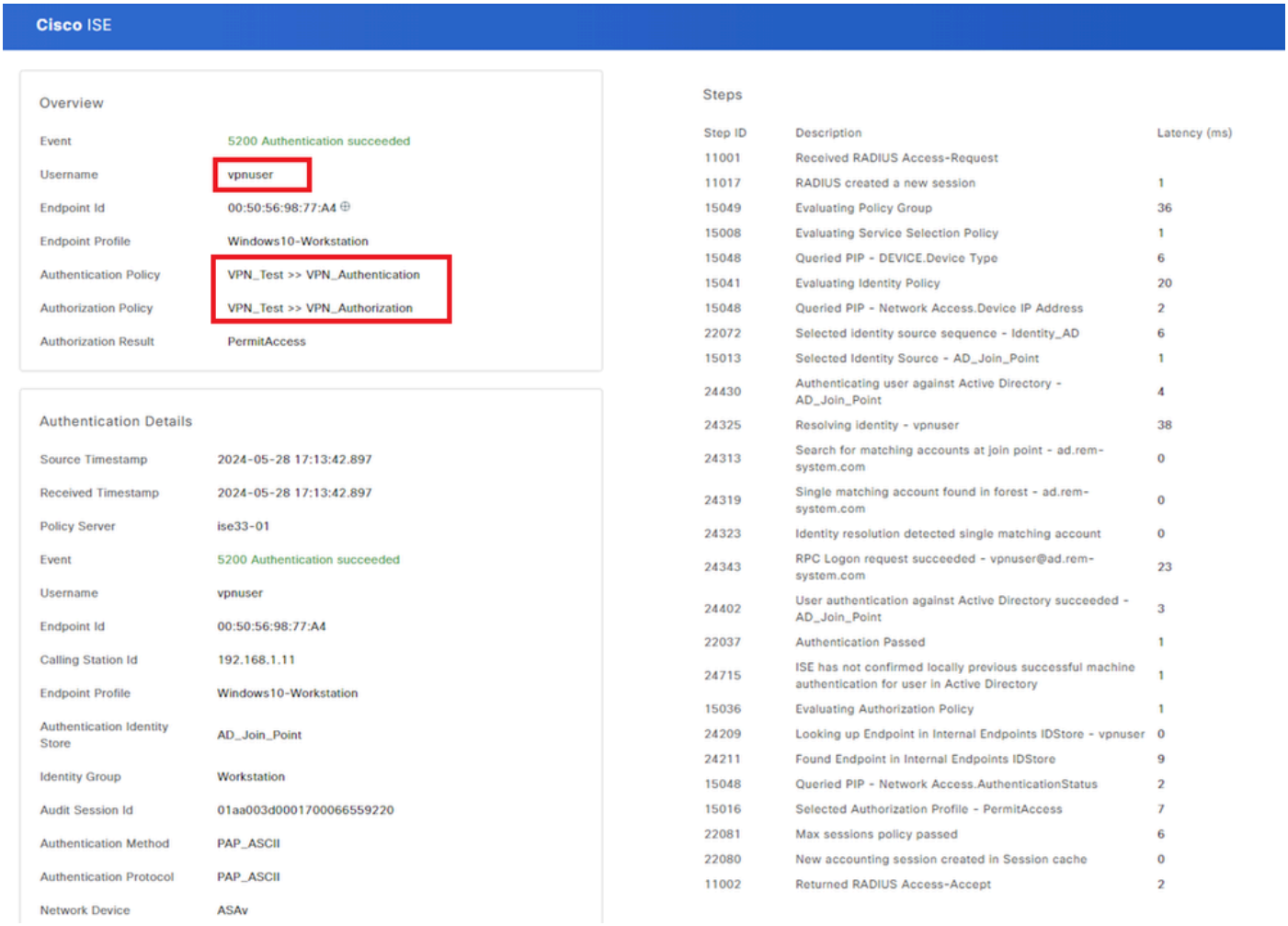
5단계. Radius 라이브 로그 확인

ISE GUI에서 **Operations(운영) > RADIUS** > **Live** Log(라이브 로그)로 이동하여 vpn 인증을 위한 라이브 로그를 확인합니다.



Radius 라이브 로그

Status(상태)를 클릭하여 라이브 로그의 세부사항을 확인합니다.



라이브 로그 세부 정보

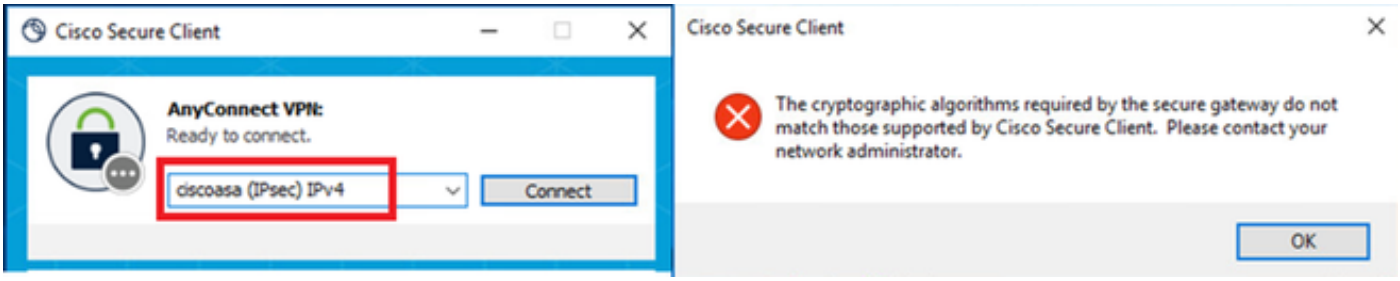
문제 해결

암호화 알고리즘이 일치하지 않으면 연결 오류가 발생할 수 있습니다. 알고리즘 불일치 문제가 발생하는 경우의 예입니다. ASDM에서 섹션 구성의 15단계를 실행하면 문제가 해결될 수 있습니다.

1단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client를 실행하고 암호화 알고리즘 불일치로 인해 연결이 실패했음을 확인합니다.

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



연결 실패

2단계. CLI에서 Syslog 확인

syslog에서 IKEv2 협상이 실패했음을 확인합니다.

<#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

참조

AAA 및 인증서 인증을 사용하여 ASA에 AnyConnect Over IKEv2

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.