보안 클라이언트 VPN 사용자를 위한 고정 IP 주소 할당 구성

목차

소개

이 문서에서는 LDAP 특성 맵을 사용하여 원격 액세스 VPN 사용자에게 고정 IP 주소를 할당하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AD(Active Directory)
- LDAP(Lightweight Directory Access Protocol)
- Cisco Secure Firewall 위협 방어
- Cisco Secure Firewall 관리 센터

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows Server 2022
- FTD 버전 7.4.2
- FMC 버전 7.4.2

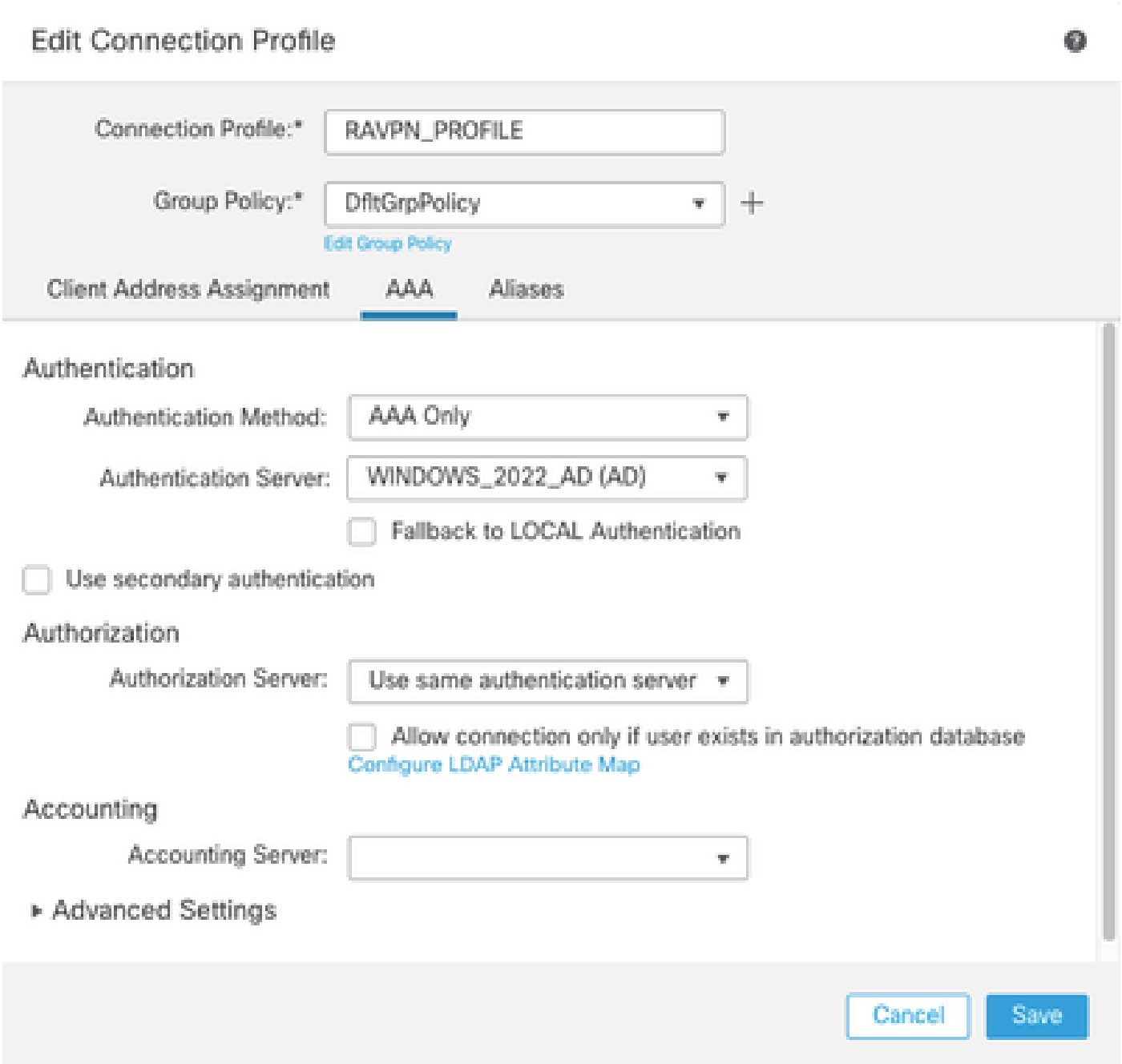
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

참고: IP 주소 할당에 Realm을 사용하고 LDAP 특성 맵을 구성하는 옵션은 firepower 버전 6.7 이상에서 지원됩니다. 계속하기 전에 firepower 버전이 6.7 이상인지 확인하십시오.

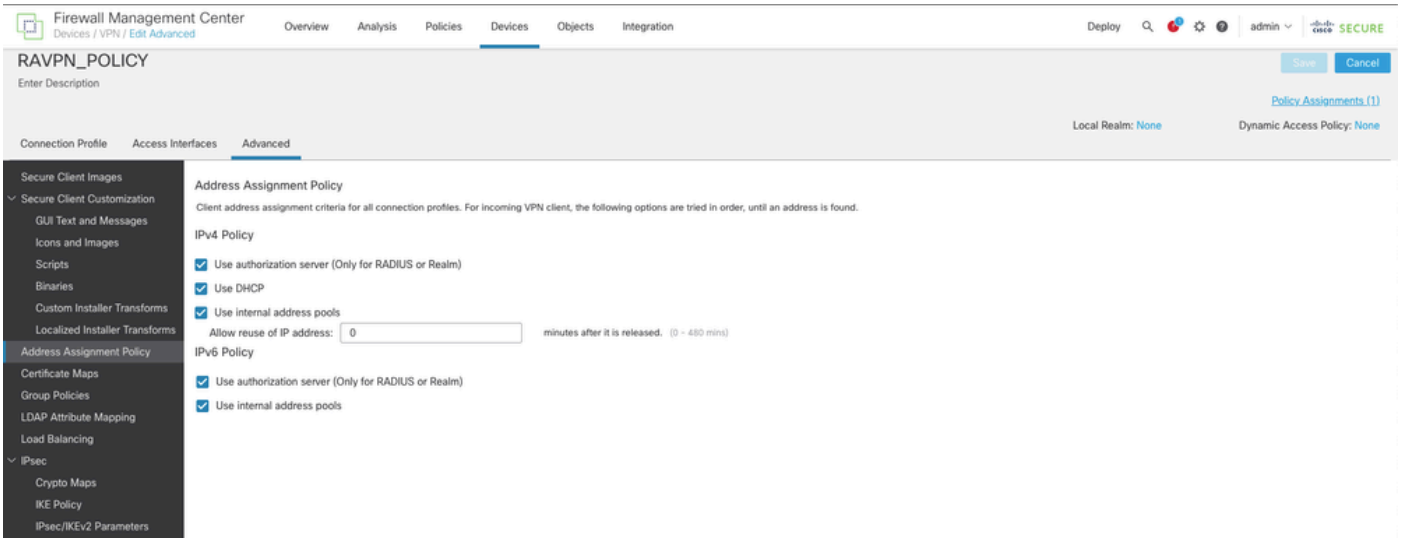
구성

1단계. Devices(디바이스) > Remote Access(원격 액세스)로 이동하고 원하는 Remote Access VPN Policy(원격 액세스 VPN 정책)를 선택합니다. 원하는 연결 프로파일을 선택합니다. AAA 탭 아래에서 인증 서버 및 권한 부여 서버에 대한 영역을 선택합니다.

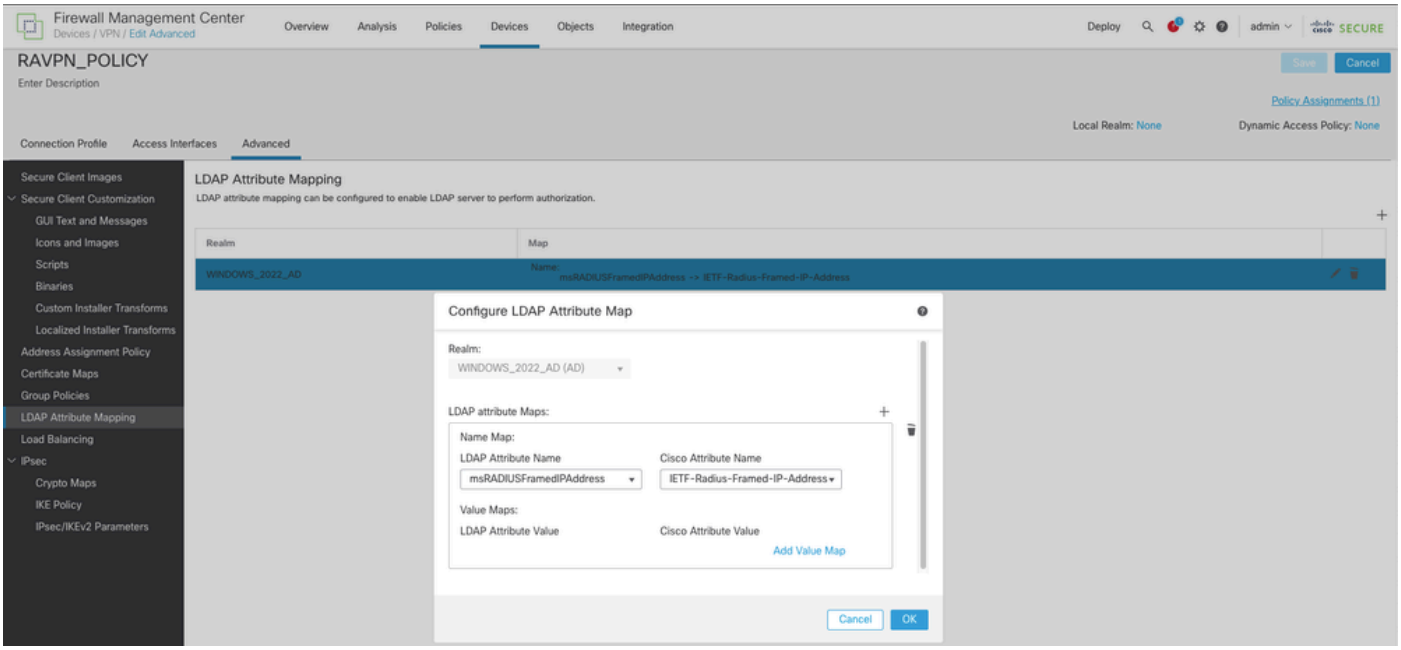


2단계. Devices(디바이스) > Remote Access(원격 액세스)로 이동하고 원하는 Remote Access

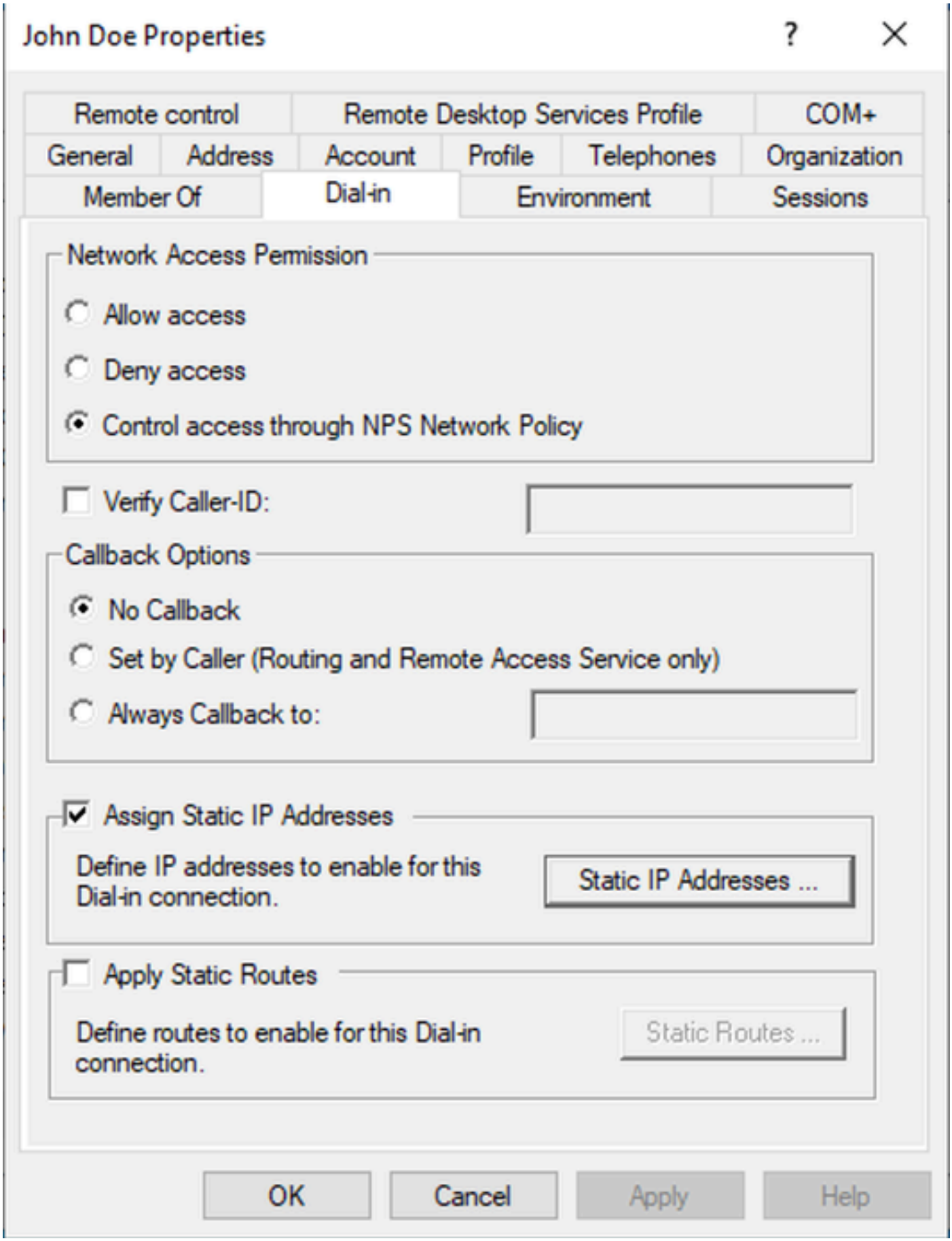
VPN(원격 액세스 VPN) 정책을 선택합니다. Advanced(고급) > Address Assignment Policy(주소 할당 정책)로 이동하여 Use authorization server(권한 부여 서버 사용)(RADIUS 또는 영역에만 해당) 옵션이 활성화되어 있는지 확인합니다.



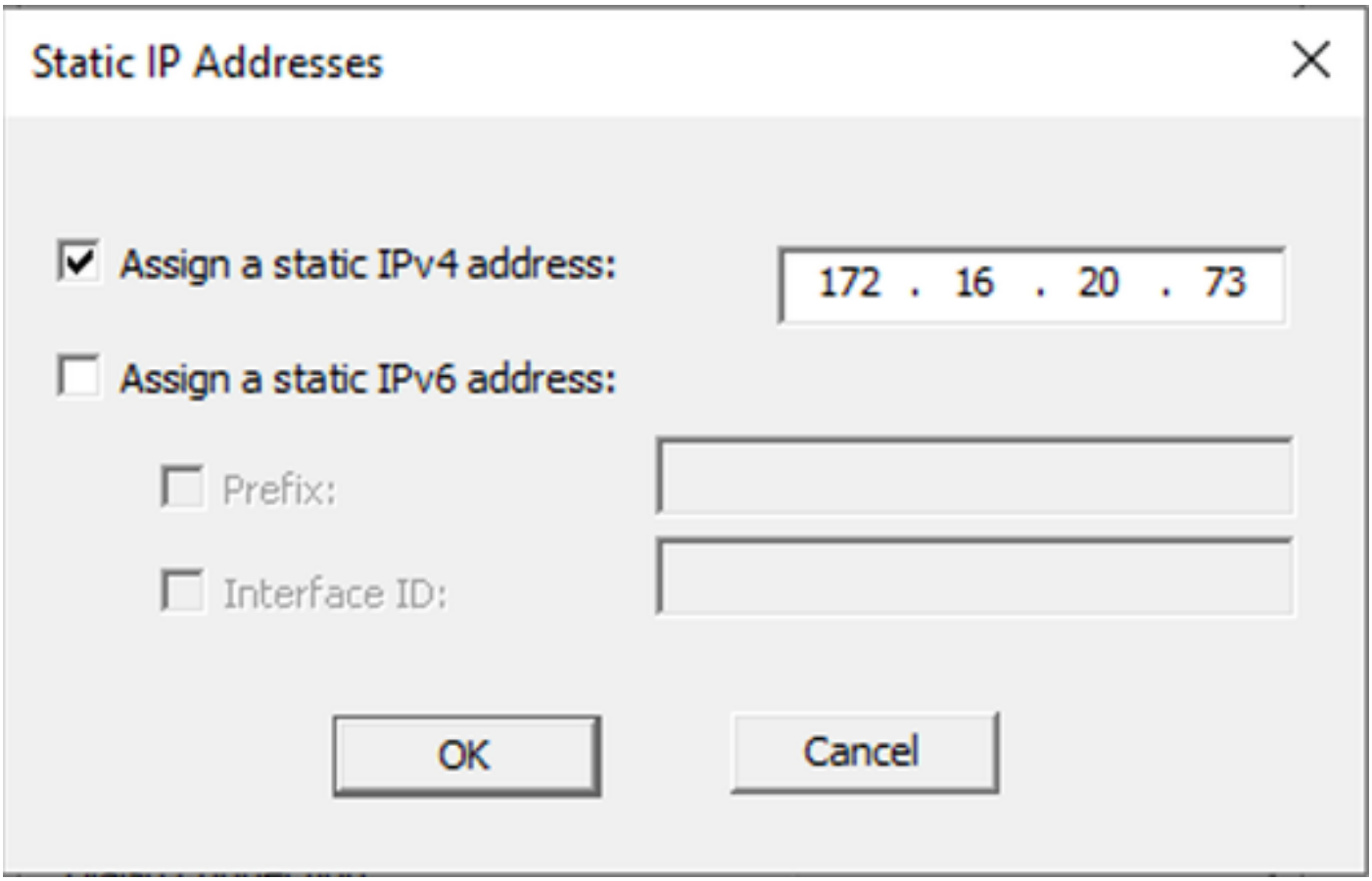
3단계. Advanced(고급) > LDAP Attribute Mapping(LDAP 특성 매핑)으로 이동하고 LDAP Attribute Name(LDAP 특성 이름)이 msRADIUSFramedIPAddress로, Cisco Attribute Name(Cisco 특성 이름)이 IETF-Radius-Framed-IP-Address로 설정된 Name Map(이름 맵)을 추가합니다.



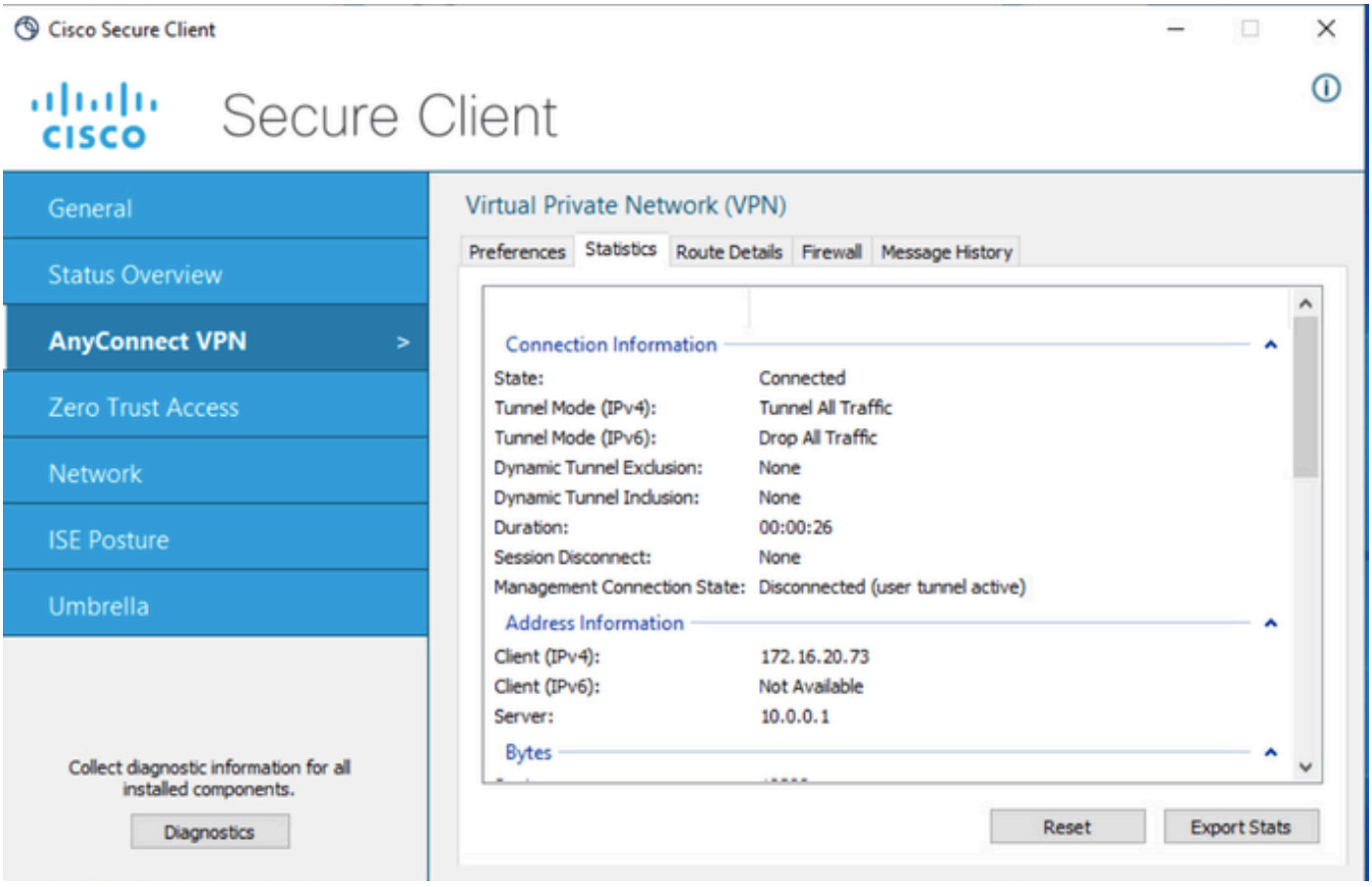
4단계. Windows AD 서버에서 서버 관리자를 열고 도구 > Active Directory 사용자 및 컴퓨터로 이동합니다. 사용자를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) > Dial-in(다이얼인)을 선택하고 Assign Static IP Addresses(고정 IP 주소 할당)라는 확인란을 선택합니다.



5단계. Static IP Addresses(고정 IP 주소)를 선택하고 고정 IP 주소를 사용자에게 할당합니다.



6단계. VPN 게이트웨이에 연결하고 Cisco Secure Client를 사용하여 로그인합니다. 사용자에게 사용자가 구성한 고정 IP 주소가 할당됩니다.



다음을 확인합니다.

debug ldap 255를 활성화하고 msRADIUSFramedIPAddress LDAP 특성이 검색되는지 확인합니다
.

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = ......fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = ............Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

```
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dSCorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

문제 해결

디버그 명령:

디버그 webvpn 255

ldap 디버그

원하는 RA VPN 사용자에게 할당된 고정 IP 주소를 검증하는 명령:

show vpn-sessiondb anyconnect 필터 이름 <username>

<#root>

```
firepower#
```

show vpn-sessiondb anyconnect filter name jdoe

```
Session Type: AnyConnect

Username : jdoe Index : 7
Assigned IP : 172.16.20.73 Public IP : 10.0.0.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14664 Bytes Rx : 26949
Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE
Login Time : 11:45:48 UTC Sun Sep 29 2024
Duration : 0h:38m:59s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000700066f93dec
Security Grp : none Tunnel Zone : 0
```

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.