FMC를 통해 FTD에서 보안 클라이언트 인증을 위한 인증서 매핑 구성

목차

소개

이 문서에서는 인증을 위해 인증서 매핑을 사용하여 FMC를 통해 FTD에서 SSL을 사용하여 Cisco Secure Client를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firepower 관리 센터)
- FTD(Firewall Threat Defense) 가상
- VPN 인증 흐름

사용되는 구성 요소

- firepower Cisco Domain Management Center for VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

인증서 매핑은 클라이언트 인증서가 로컬 사용자 계정에 매핑되거나 인증서 내의 특성이 권한 부여를 위해 사용되는 VPN 연결에 사용되는 방법입니다. 디지털 인증서가 사용자 또는 장치를 식별하는 수단으로 사용되는 프로세스입니다. 인증서 매핑을 사용하여 자격 증명을 입력할 필요 없이 SSL 프로토콜을 사용하여 사용자를 인증합니다.

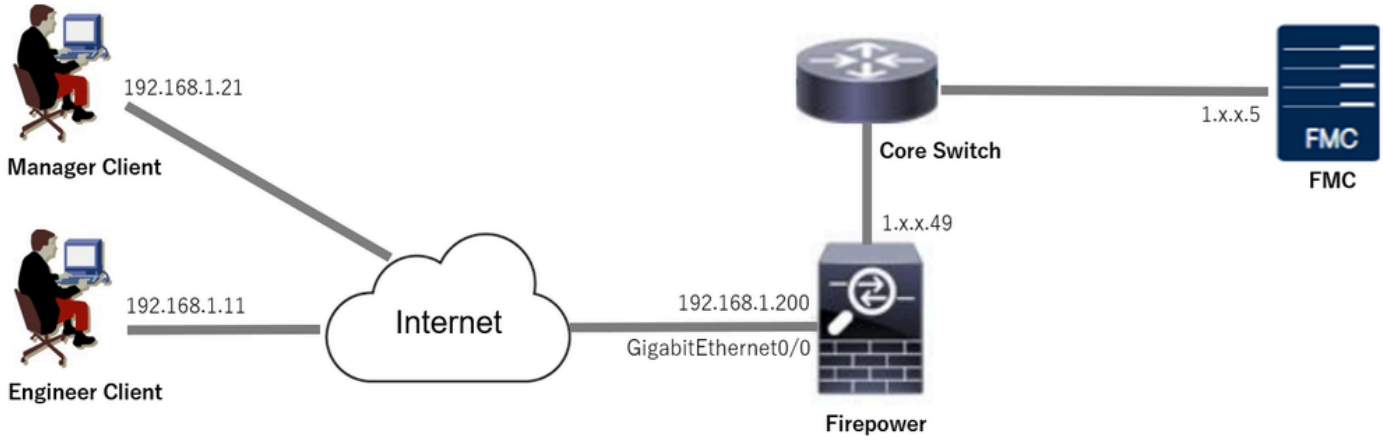
이 문서에서는 SSL 인증서의 일반 이름을 사용하여 Cisco Secure Client를 인증하는 방법에 대해 설명합니다.

이러한 인증서는 권한 부여 목적으로 사용되는 공통 이름을 포함합니다.

- CA: ftd-ra-ca-common-name
- Engineer VPN Client Certificate(엔지니어 VPN 클라이언트 인증서): vpnEngineerClientCN
- 관리자 VPN 클라이언트 인증서: vpnManagerClientCN
- 서버 인증서: 192.168.1.200

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.



네트워크 다이어그램

설정

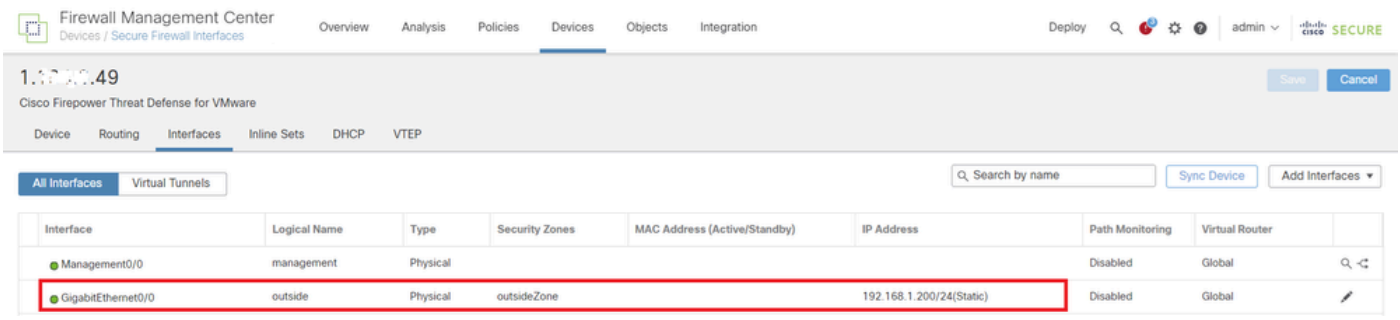
FMC의 컨피그레이션

1단계. FTD 인터페이스 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하고, 대상 FTD 디바이스를 편집하며, FTD inInterface(인터페이스)에 대한 외부 인터페이스를 구성합니다.

GigabitEthernet0/0,

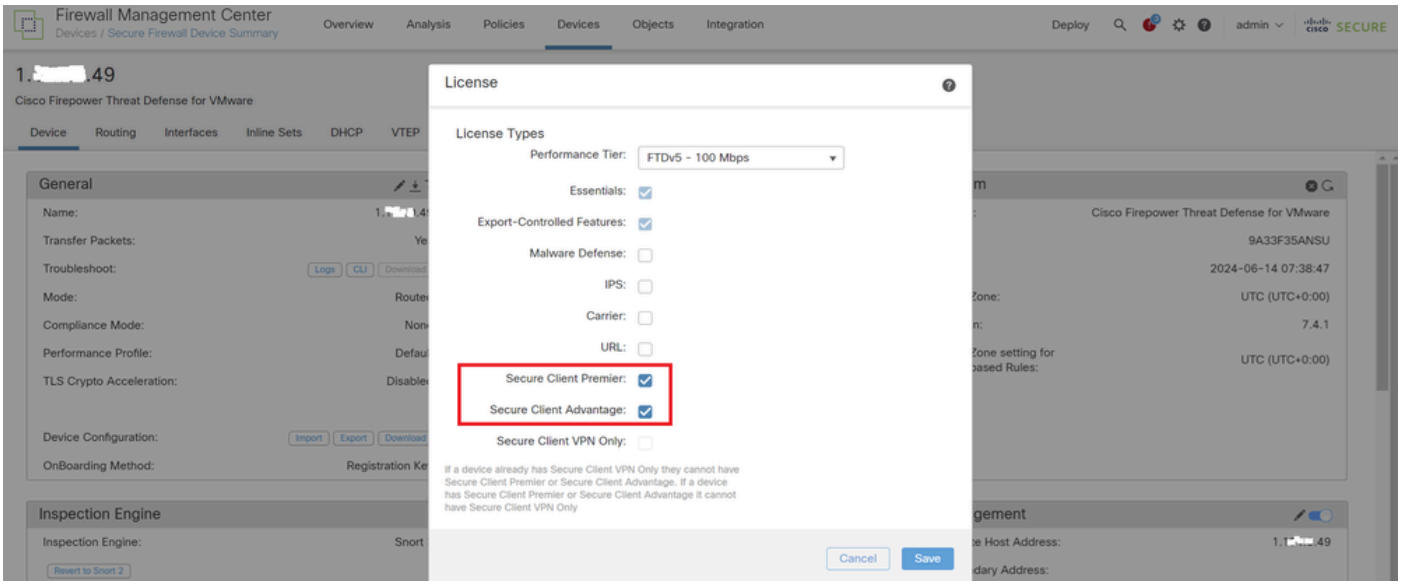
- 이름: outside
- 보안 영역: outsideZone
- IP 주소: 192.168.1.200/24



FTD 인터페이스

2단계. Cisco Secure Client 라이센스 확인

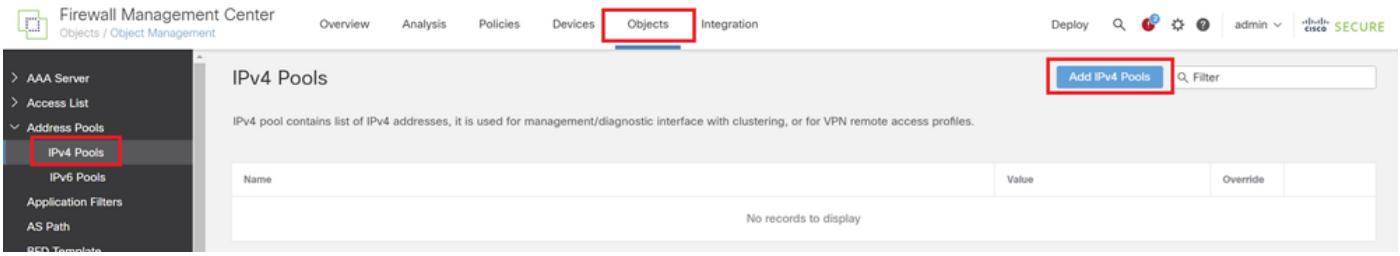
Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 대상 FTD 디바이스를 편집하고 Devices(디바이스) 탭에서 Cisco Secure Client 라이센스를 확인합니다.



Secure Client 라이센스

3단계. IPv4 주소 풀 추가

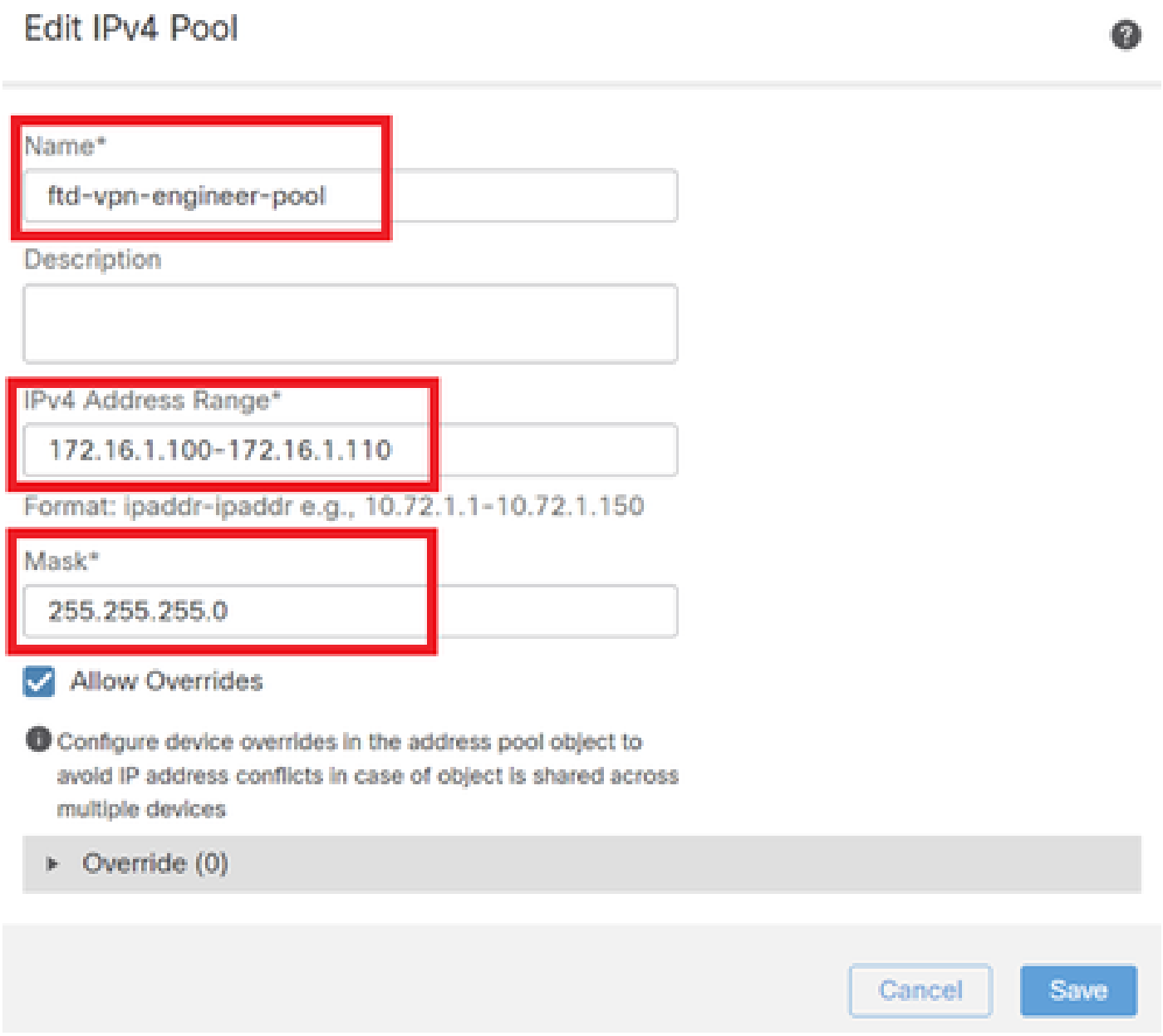
Object(개체) > Object Management(개체 관리) > Address Pools(주소 풀) > IPv4 Pools(IPv4 풀)로 이동하고 Add IPv4 Pools(IPv4 풀 추가) 버튼을 클릭합니다.



IPv4 주소 풀 추가

엔지니어 VPN 클라이언트에 대한 IPv4 주소 풀을 생성하는 데 필요한 정보를 입력합니다.

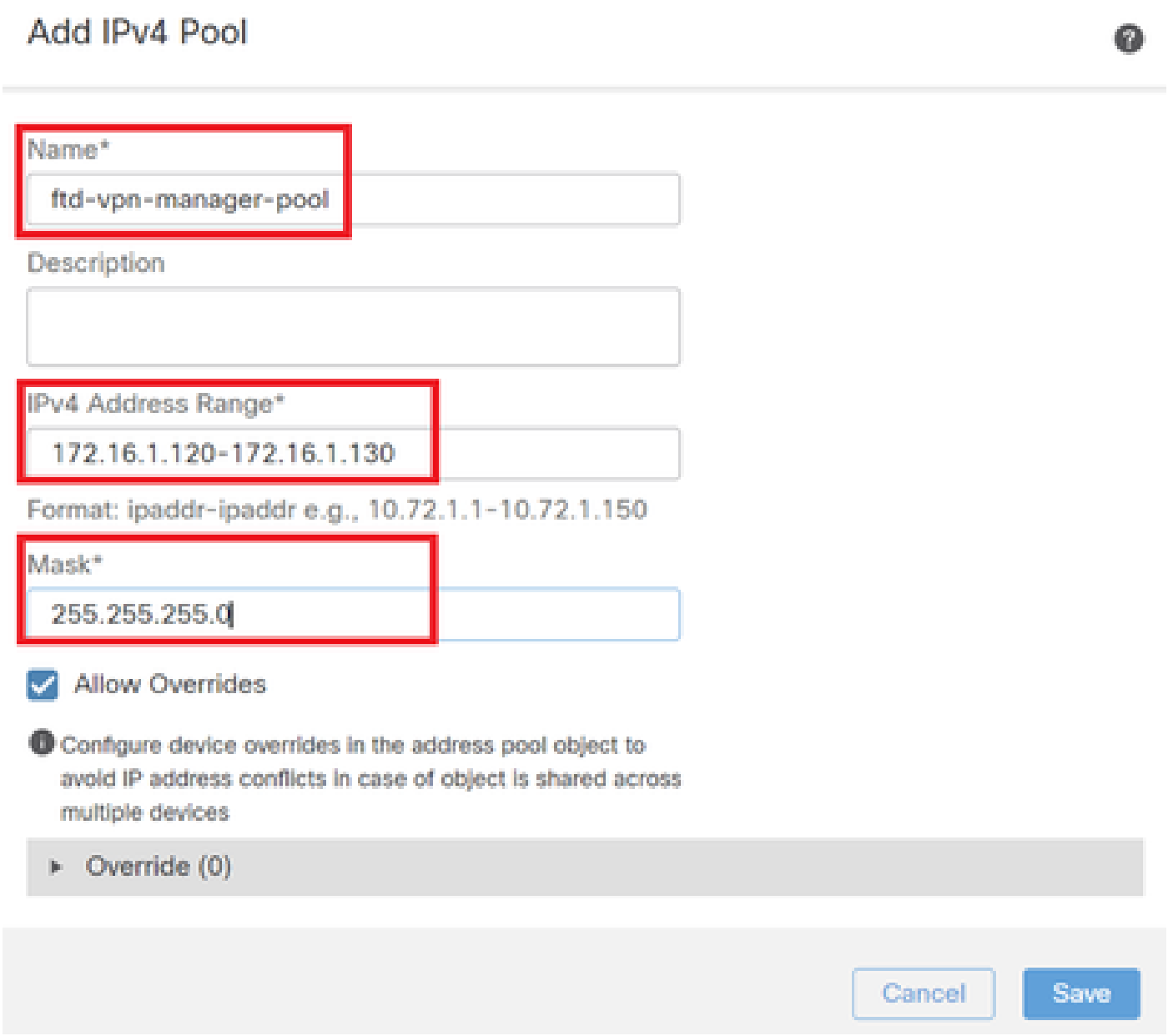
- 이름: ftd-vpn-engineer-pool
- IPv4 주소 범위: 172.16.1.100-172.16.1.110
- 마스크: 255.255.255.0



엔지니어 VPN 클라이언트의 IPv4 주소 풀

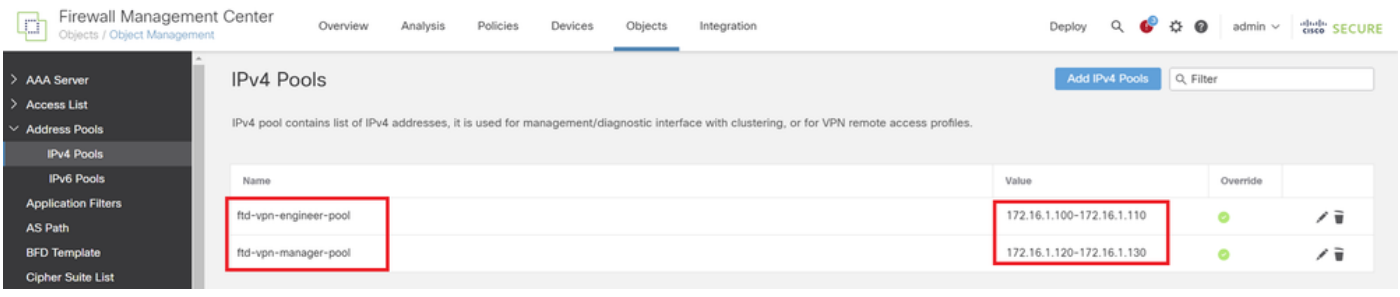
관리자 VPN 클라이언트에 대한 IPv4 주소 풀을 생성하는 데 필요한 정보를 입력합니다.

- 이름: ftd-vpn-manager-pool
- IPv4 주소 범위: 172.16.1.120-172.16.1.130
- 마스크: 255.255.255.0



Manager VPN 클라이언트용 IPv4 주소 풀

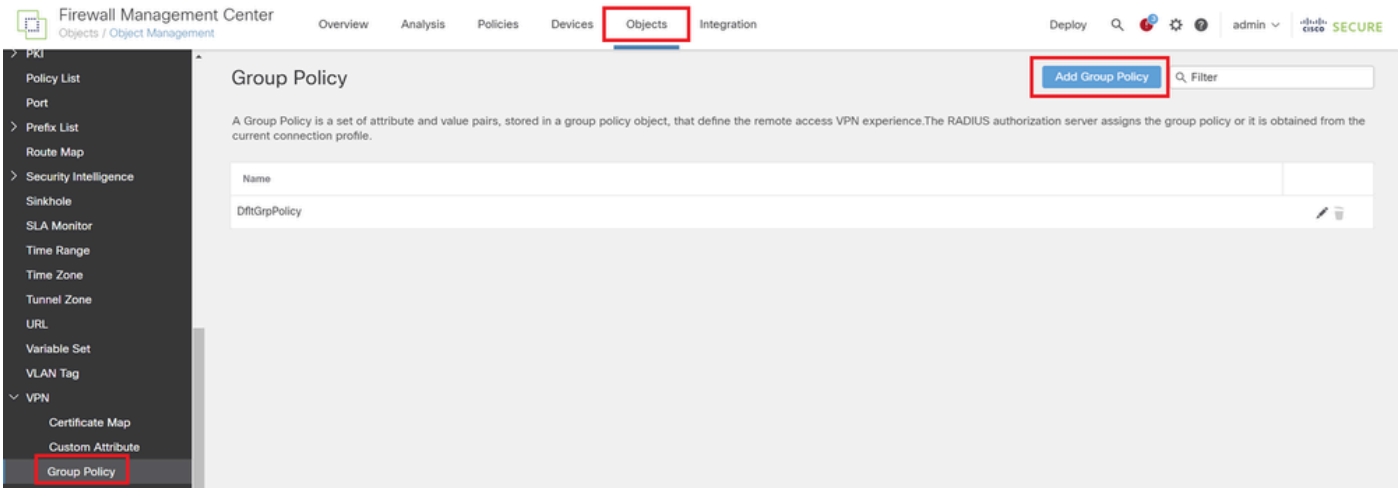
새 IPv4 주소 풀을 확인합니다.



새 IPv4 주소 풀

4단계. 그룹 정책 추가

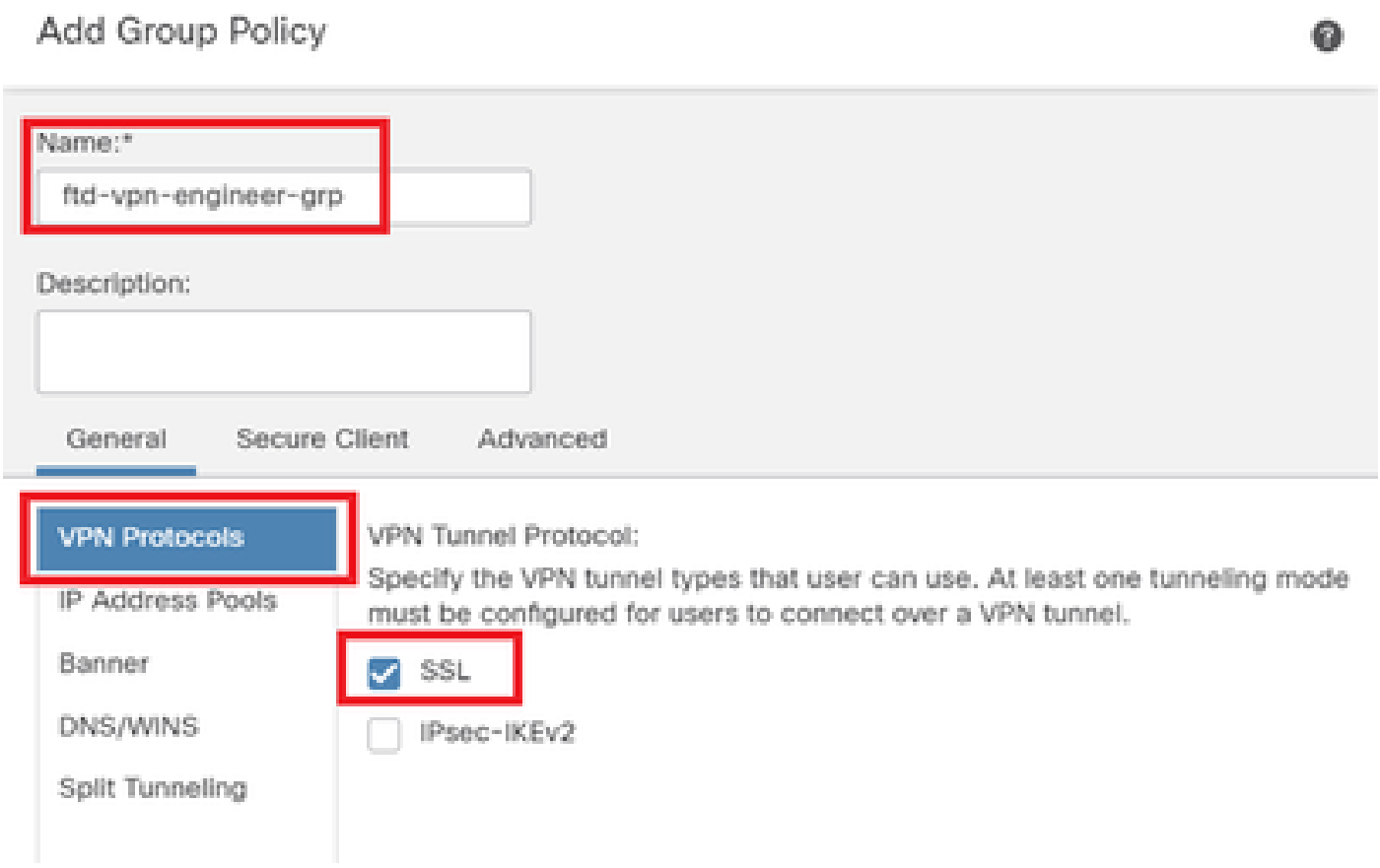
Object(개체) > Object Management(개체 관리) > VPN > Group Policy(그룹 정책)로 이동하고 Add Group Policy(그룹 정책 추가) 버튼을 클릭합니다.



그룹 정책 추가

엔지니어 VPN 클라이언트에 대한 그룹 정책을 생성하는 데 필요한 정보를 입력합니다.

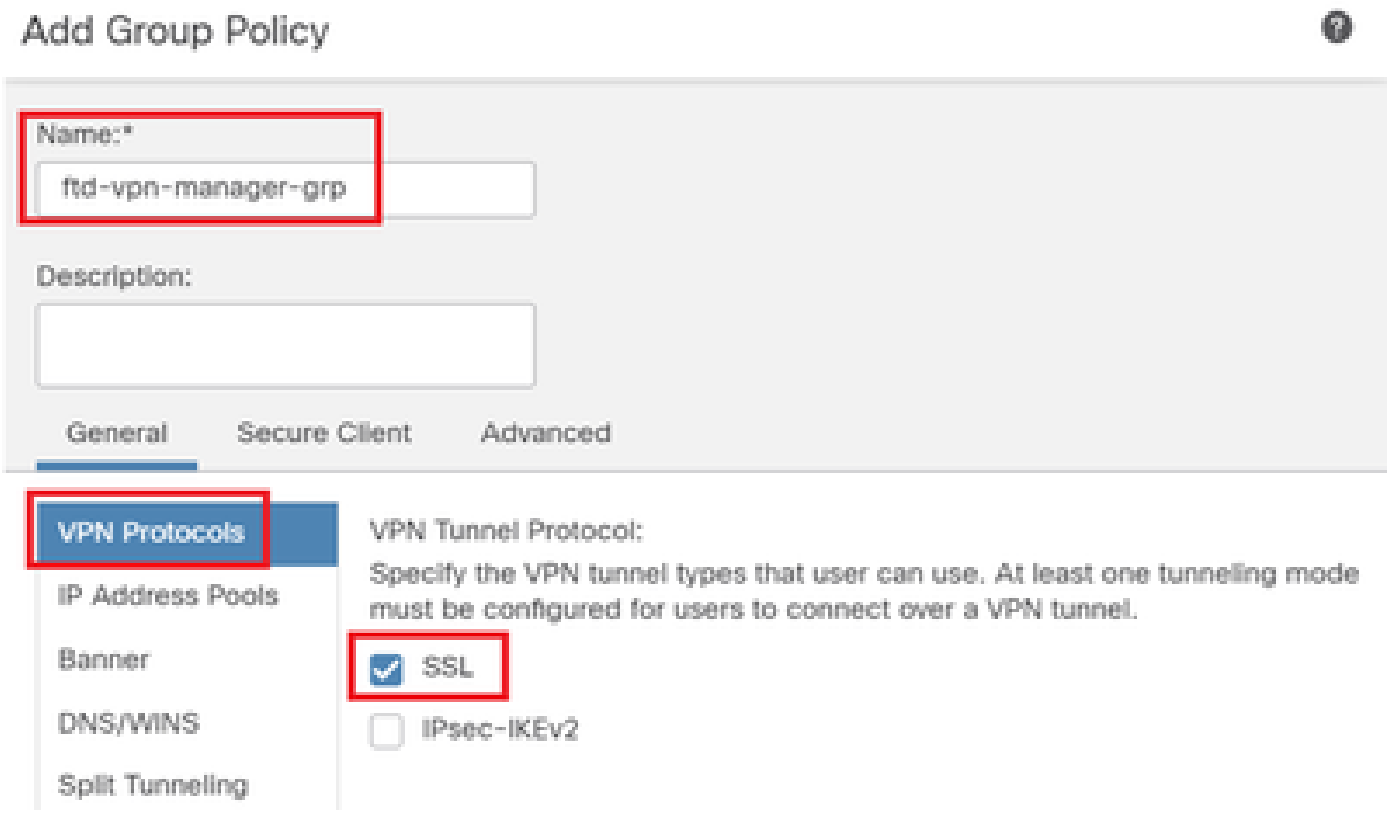
- 이름: ftd-vpn-engineer-grp
- VPN 프로토콜: SSL



엔지니어 VPN 클라이언트에 대한 그룹 정책

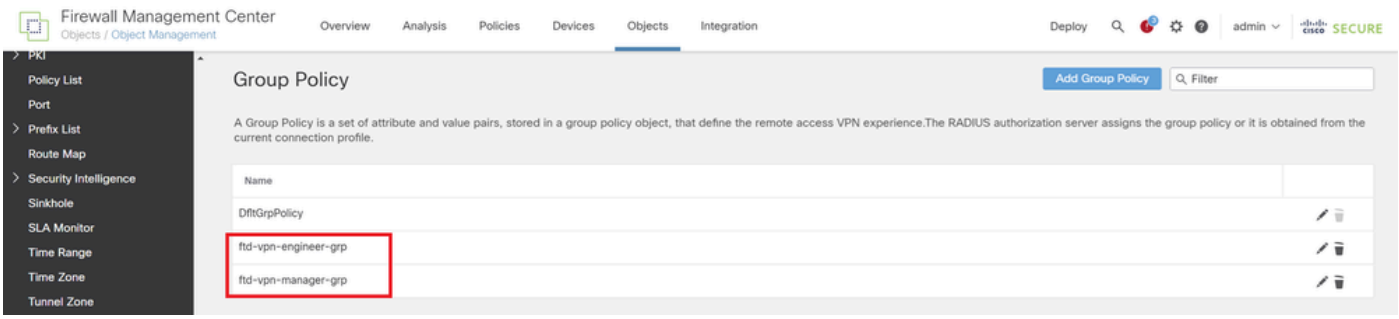
관리자 VPN 클라이언트에 대한 그룹 정책을 만드는 데 필요한 정보를 입력합니다.

- 이름: ftd-vpn-manager-grp
- VPN 프로토콜: SSL



관리자 VPN 클라이언트에 대한 그룹 정책

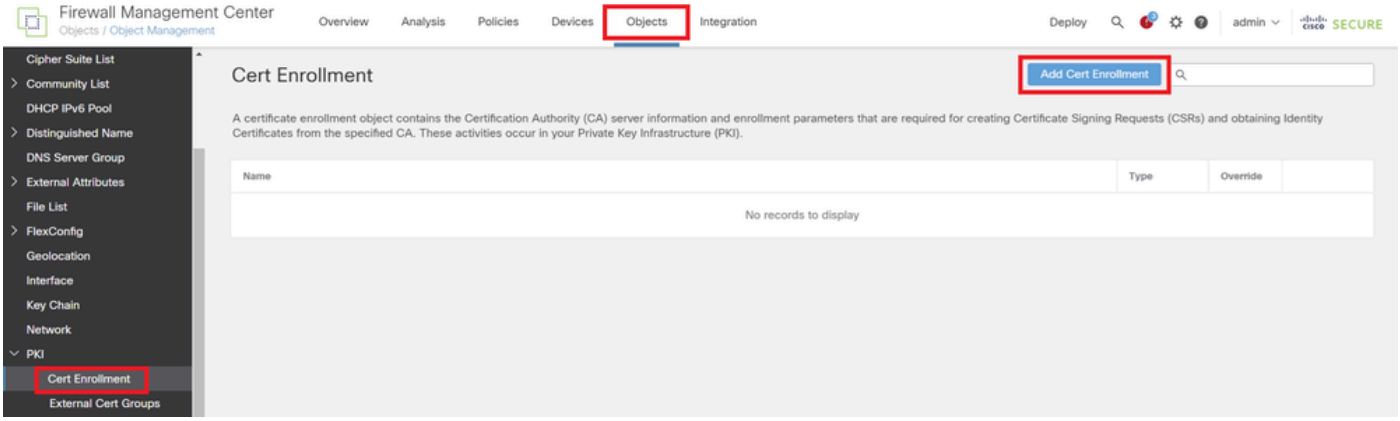
새 그룹 정책을 확인합니다.



새 그룹 정책

5단계. FTD 인증서 추가

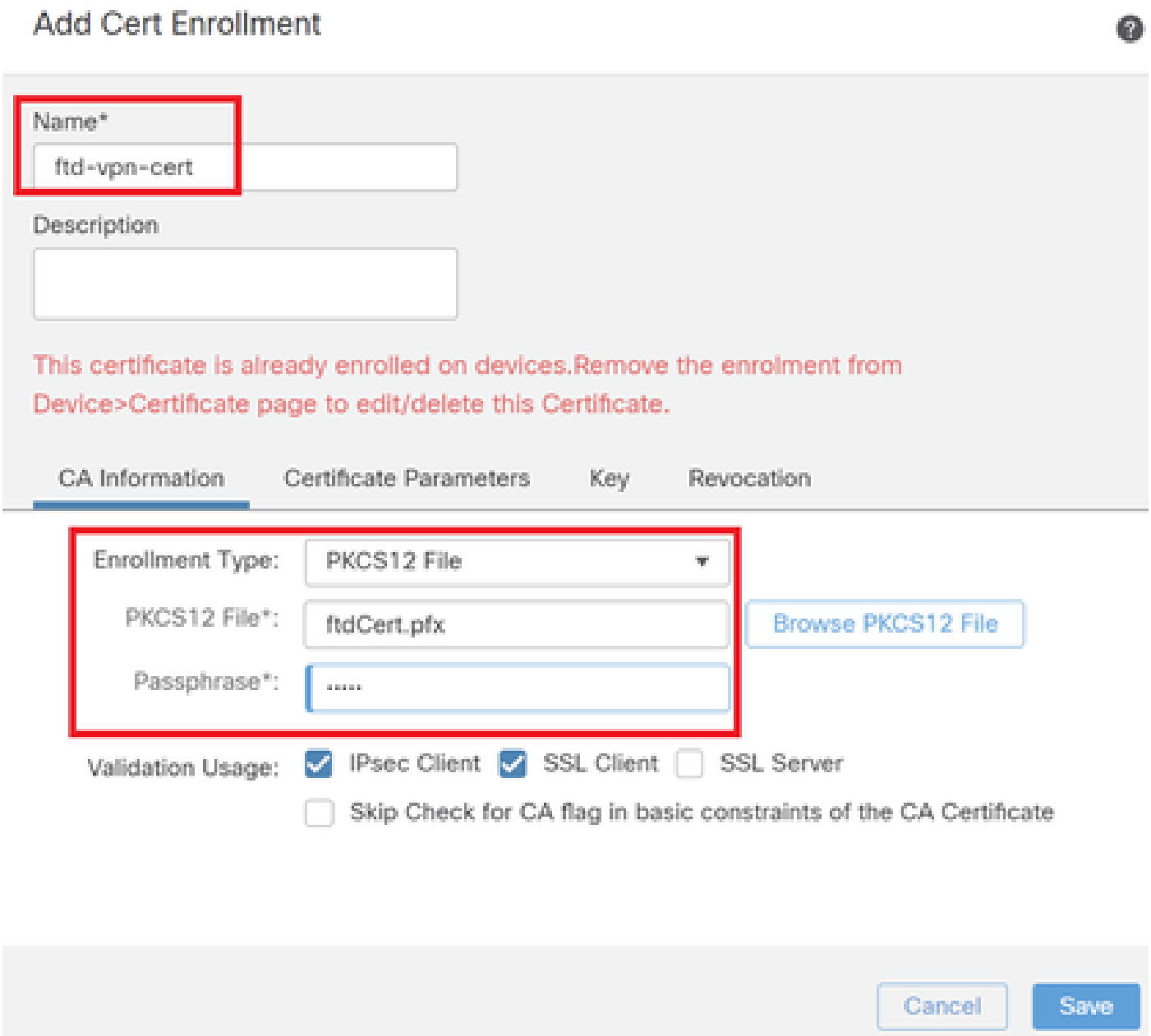
Object(개체) > Object Management(개체 관리) > PKI > Cert Enrollment(인증서 등록)로 이동하고 Add Cert Enrollment(인증서 등록 추가) 버튼을 클릭합니다.



인증서 등록 추가

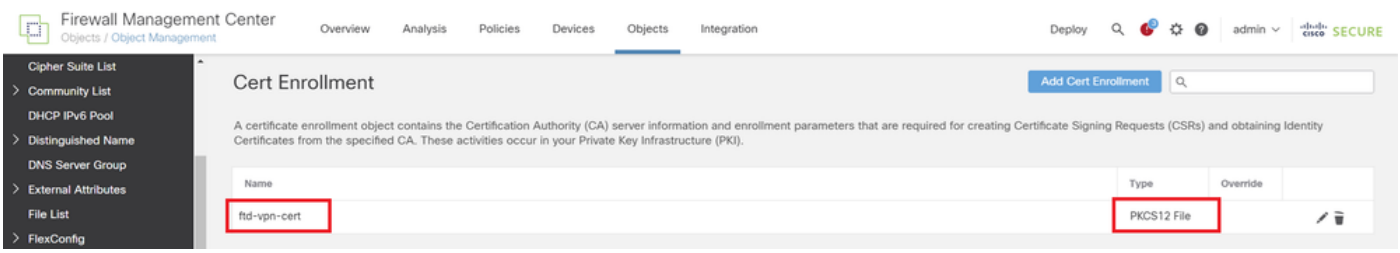
FTD 인증서에 필요한 정보를 입력하고 로컬 컴퓨터에서 PKCS12 파일을 가져옵니다.

- 이름: ftd-vpn-cert
- 등록 유형: PKCS12 파일



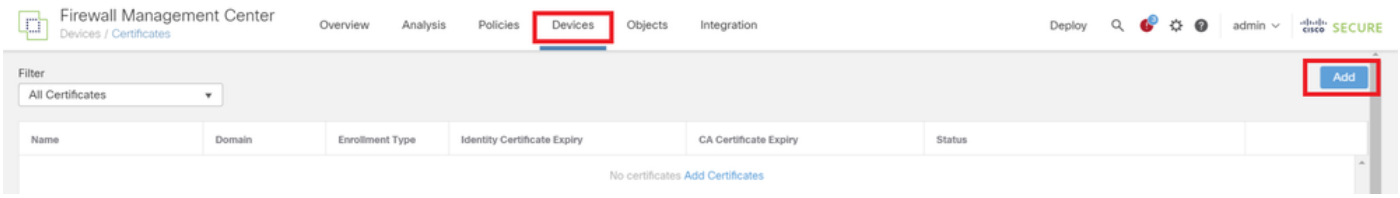
인증서 등록 세부 정보

새 인증서 등록을 확인합니다.



새 인증서 등록

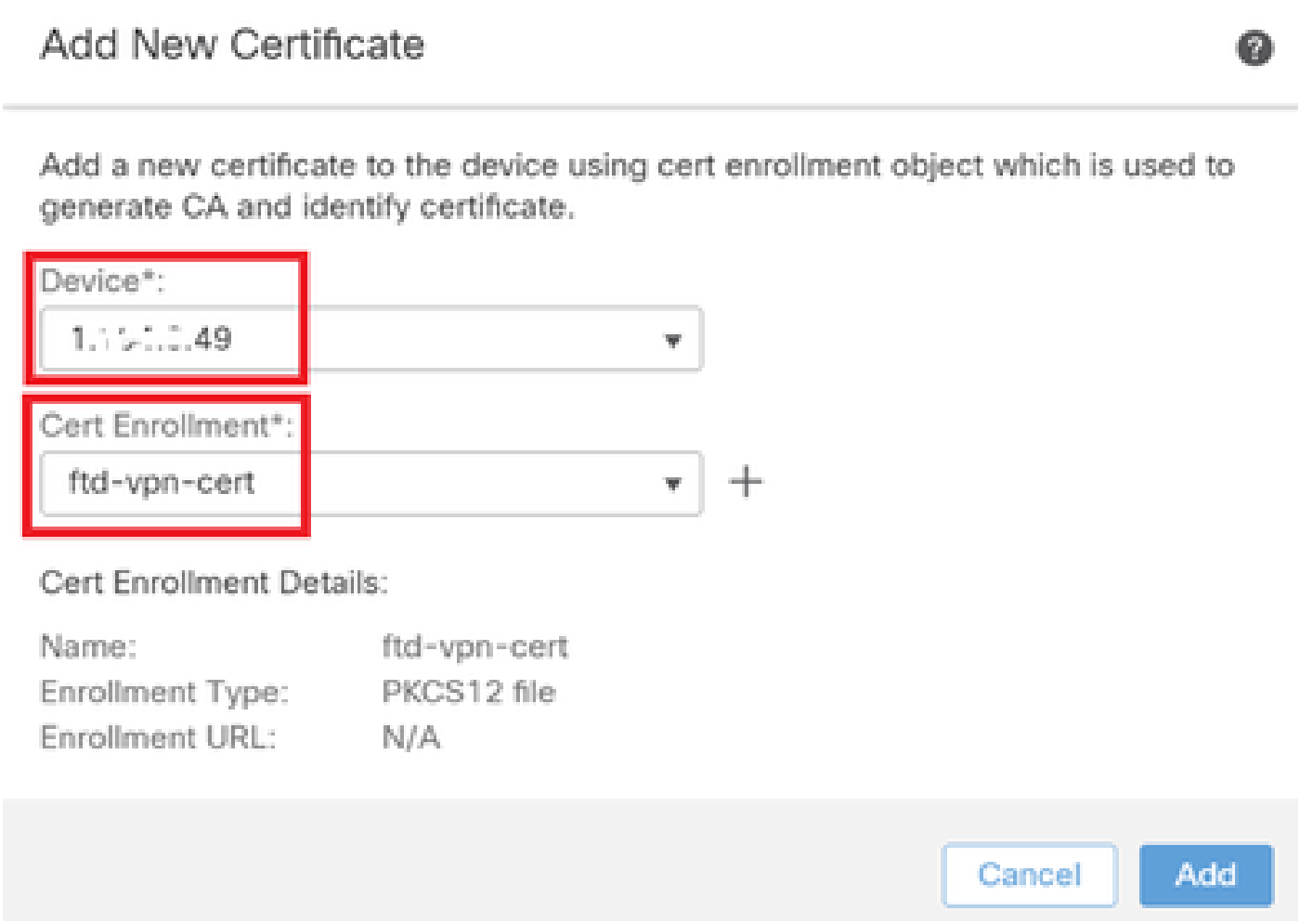
Devices(디바이스) > Certificates(인증서)로 이동하고 Add(추가) 버튼을 클릭합니다.



FTD 인증서 추가

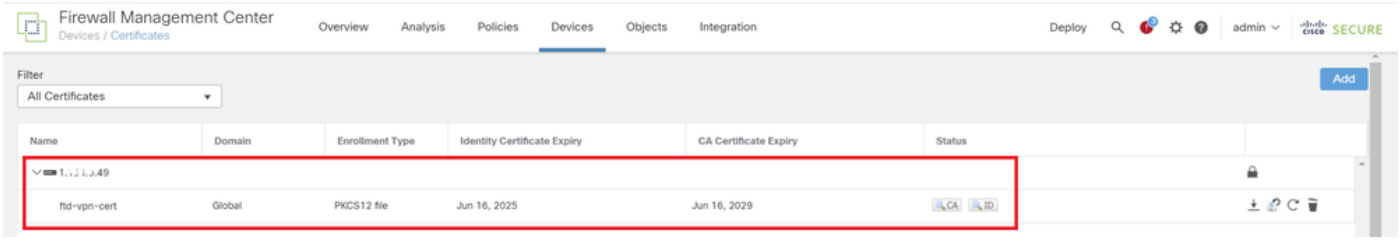
새 인증서 등록을 FTD에 바인딩하는 데 필요한 정보를 입력합니다.

- 장치: 1.x.x.49
- 인증서 등록: ftd-vpn-cert



FTD에 인증서 바인딩

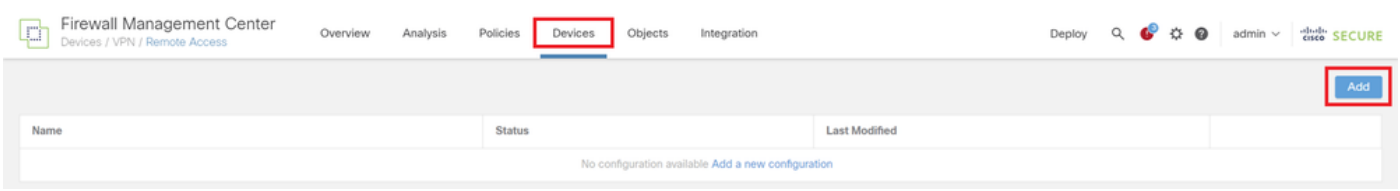
인증서 바인딩의 상태를 확인합니다.



인증서 바인딩 상태

6단계. 엔지니어 연결 프로파일에 대한 정책 할당 추가

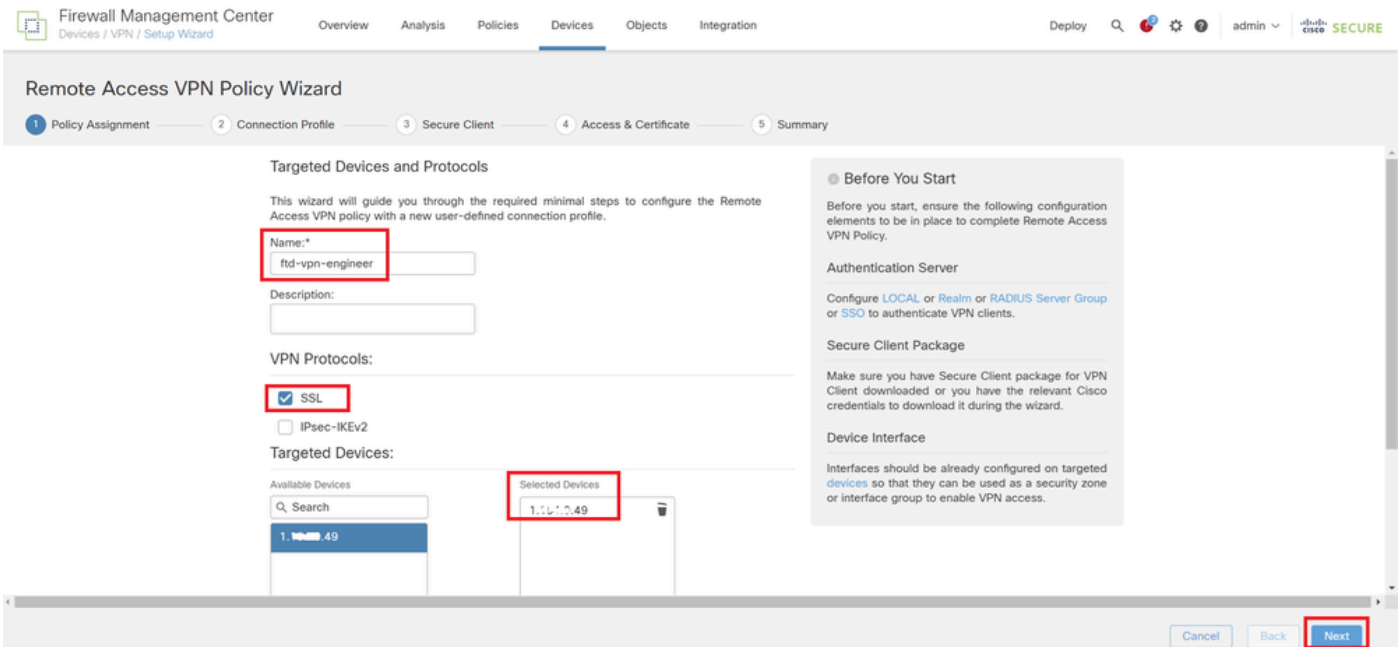
Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하고 Addbutton(추가 버튼)을 클릭합니다.



원격 액세스 VPN 추가

필요한 정보를 입력하고 Nextbutton을 클릭합니다.

- 이름: ftd-vpn-engineer
- VPN 프로토콜: SSL
- 대상 장치: 1.x.x.49



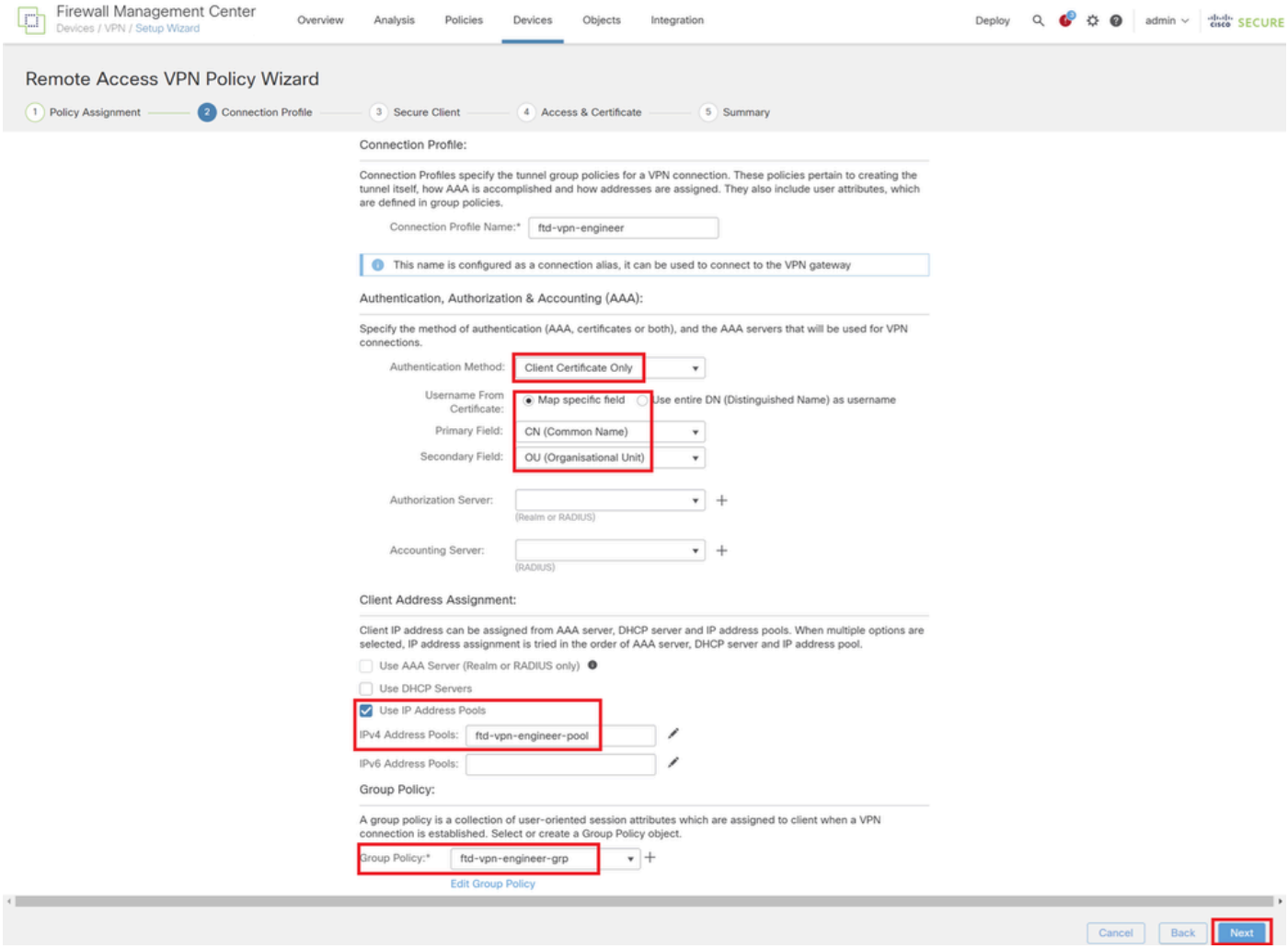
정책 할당

7단계. 엔지니어 연결 프로파일에 대한 세부사항 구성

필요한 정보를 입력하고 Nextbutton을 클릭합니다.

- 인증 방법: 클라이언트 인증서 전용
- Username From Certificate(인증서의 사용자 이름): Map specific(맵) 필드
- 기본 필드: CN(Common Name)
- 보조 필드: OU(조직 단위)

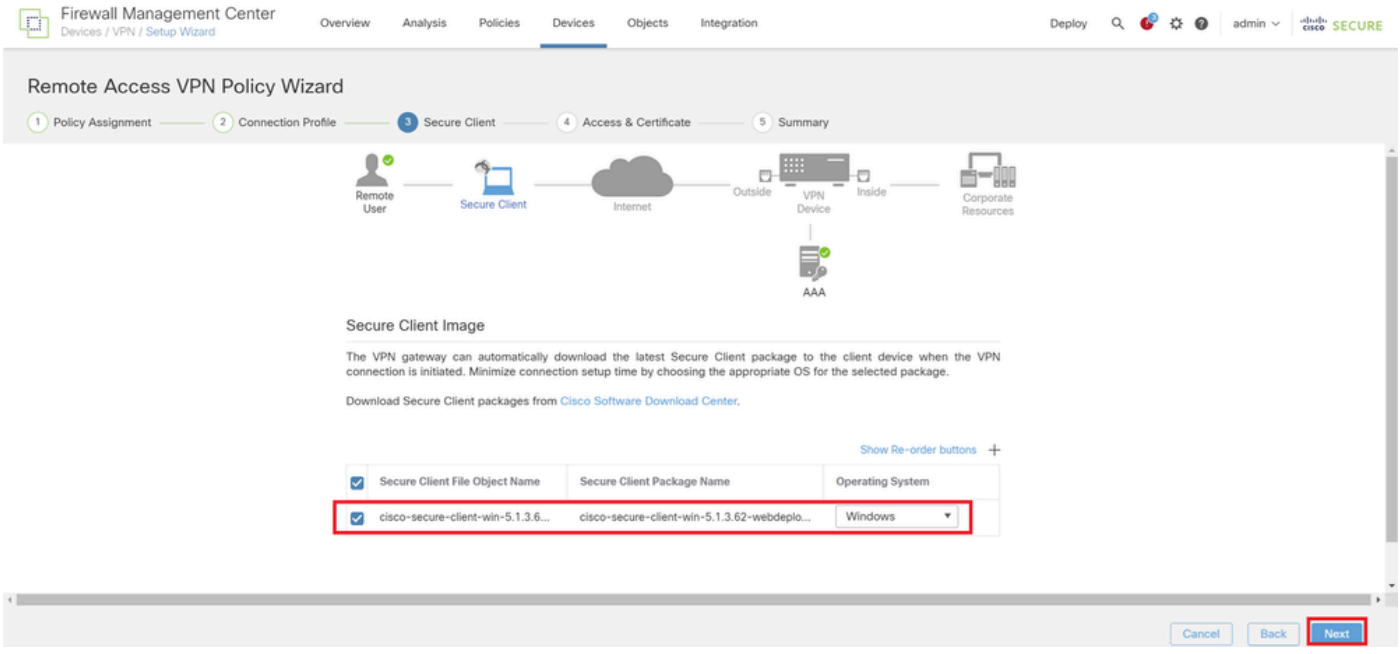
- IPv4 주소 풀: ftd-vpn-engineer-pool
- 그룹 정책: ftd-vpn-engineer-grp



연결 프로파일 세부사항

8단계. 엔지니어 연결 프로파일에 대한 보안 클라이언트 이미지 구성

보안 클라이언트 이미지 파일을 선택하고 다음 버튼을 클릭합니다.

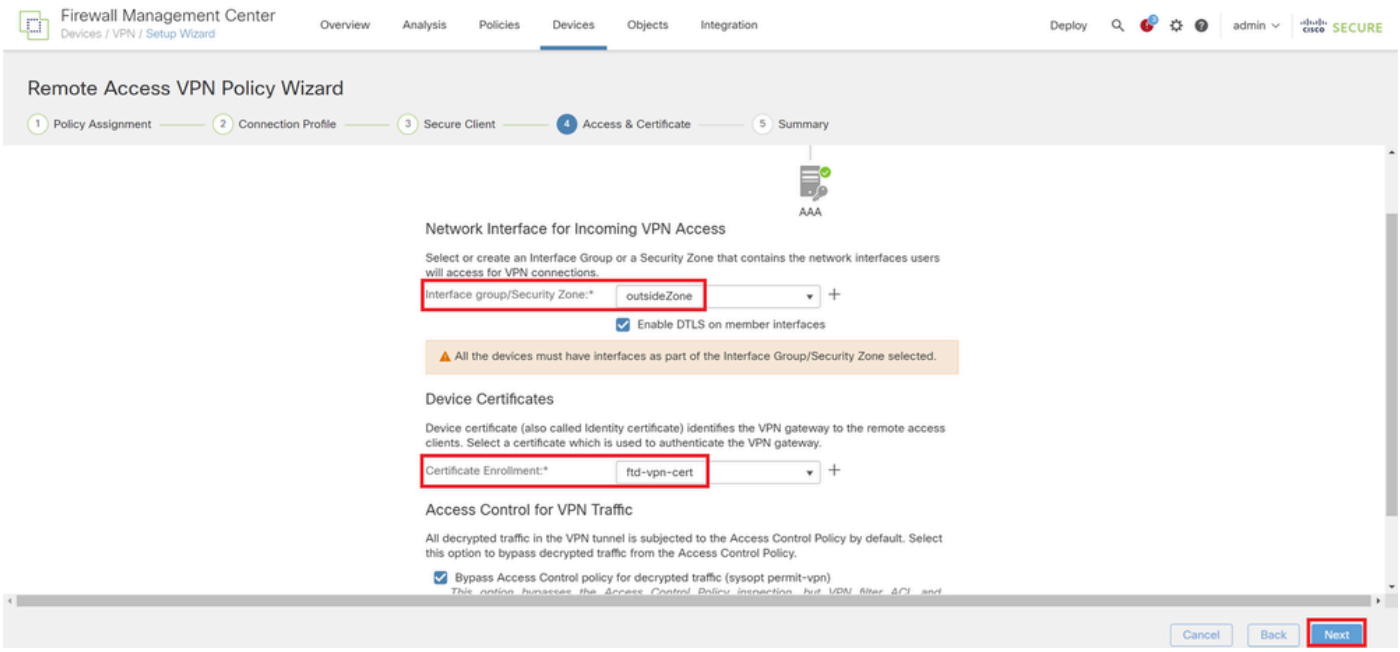


Secure Client 선택

9단계. 엔지니어 연결 프로파일에 대한 액세스 및 인증서 구성

인터페이스 그룹/보안 영역 및 인증서 등록 항목의 값을 선택하고 Next(다음) 버튼을 클릭합니다.

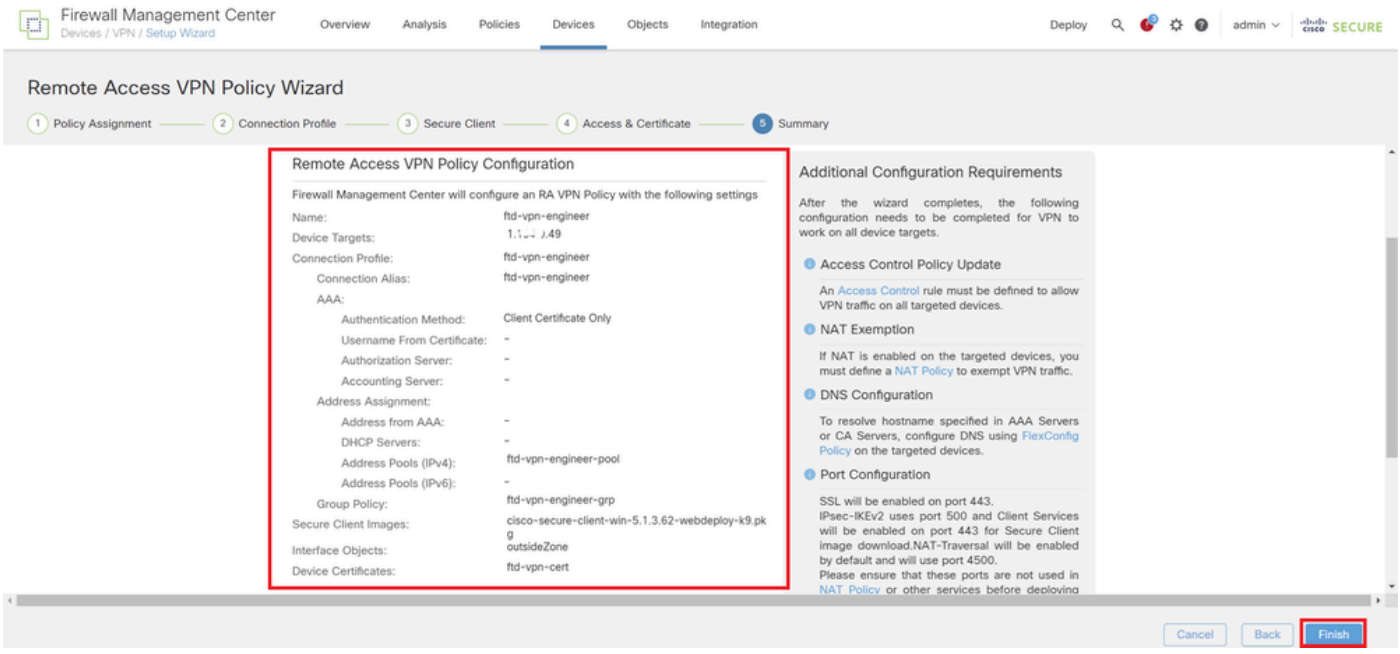
- 인터페이스 그룹/보안 영역: outsideZone
- 인증서 등록: ftd-vpn-cert



액세스 및 인증서 세부사항

10단계. 엔지니어 연결 프로파일 요약 확인

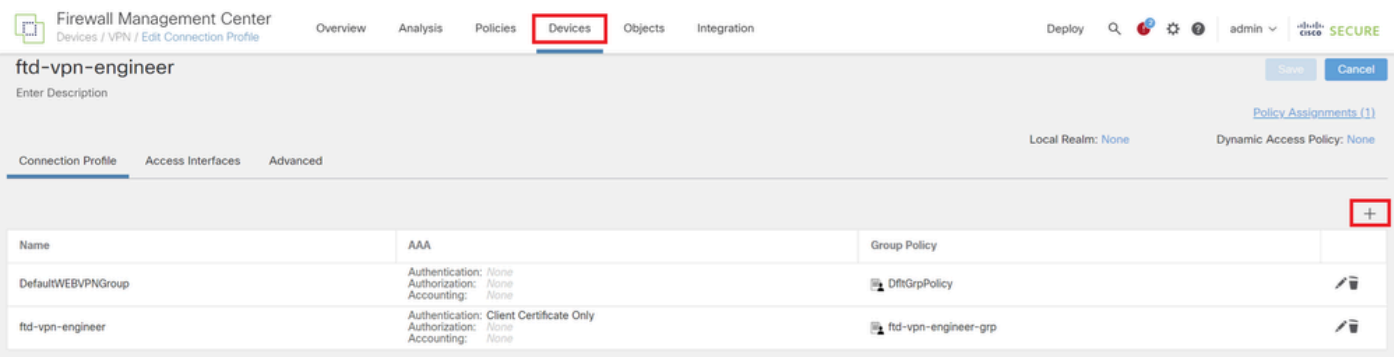
원격 액세스 VPN 정책에 대해 입력한 정보를 확인하고 Finish(마침) 버튼을 클릭합니다.



원격 액세스 VPN 정책 세부 정보

11단계. Manager VPN 클라이언트에 대한 연결 프로파일 추가

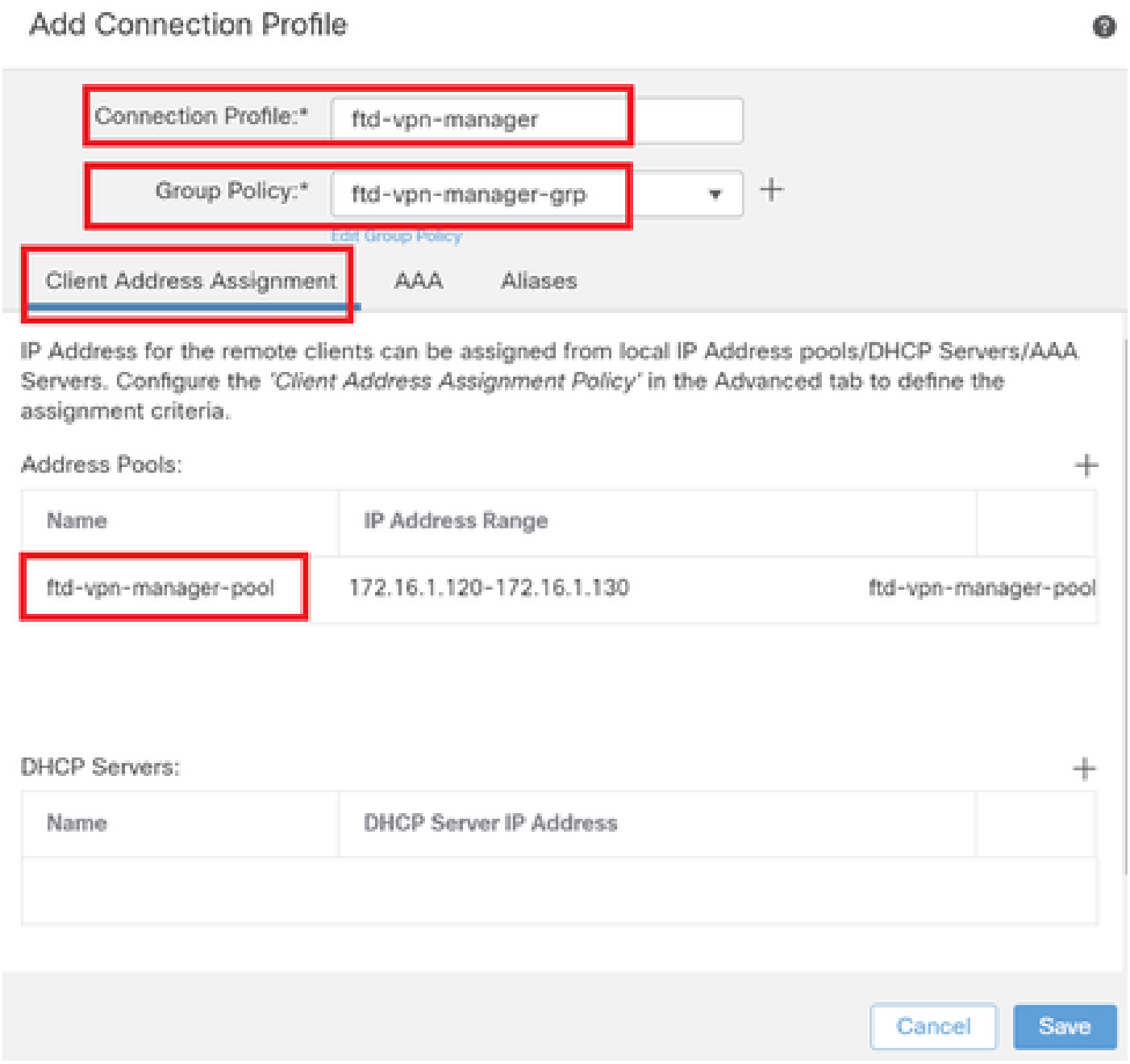
Devices(디바이스) > VPN > Remote Access(원격 액세스) > Connection Profile(연결 프로파일)로 이동하고 + 버튼을 클릭합니다.



Manager VPN 클라이언트에 대한 연결 프로파일 추가

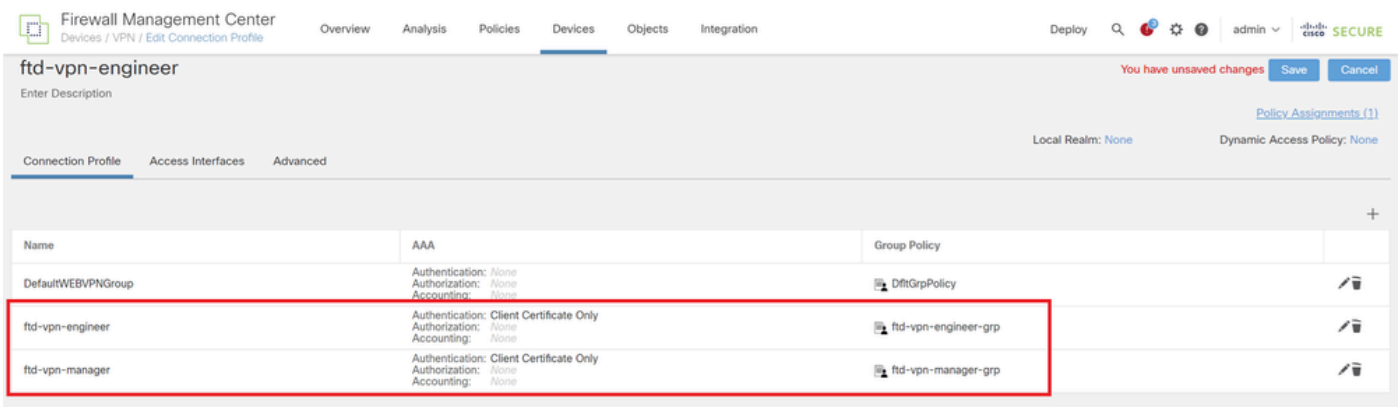
연결 프로파일에 필요한 정보를 입력하고 Save(저장) 버튼을 클릭합니다.

- 이름: ftd-vpn-manager
- 그룹 정책: ftd-vpn-manager-grp
- IPv4 주소 풀: ftd-vpn-manager-pool



Manager VPN Client에 대한 연결 프로파일 세부사항

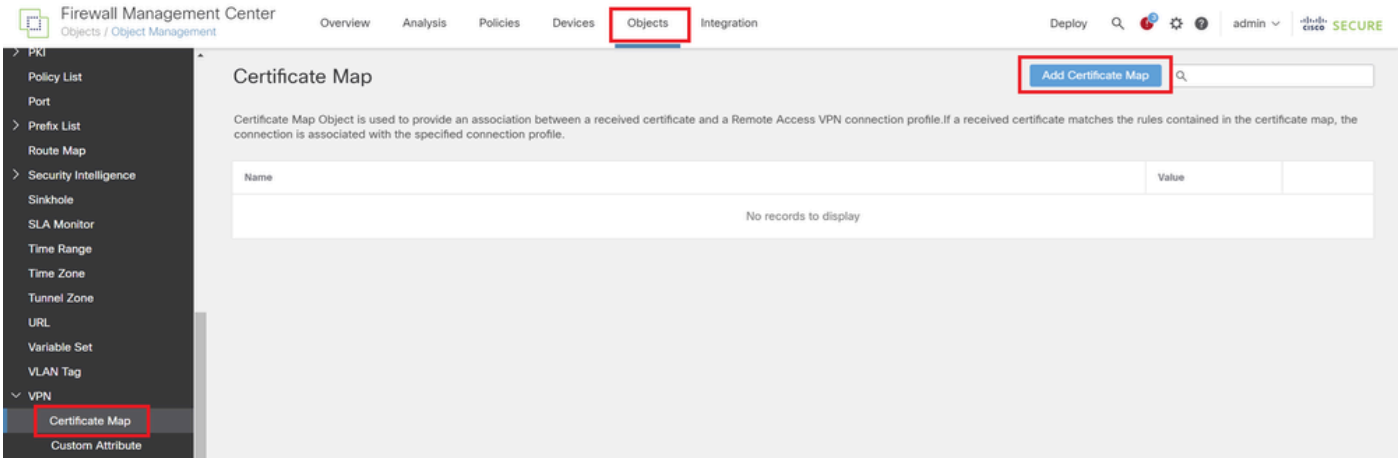
새로 추가된 연결 프로파일을 확인합니다.



추가된 연결 프로파일 확인

12단계. 인증서 맵 추가

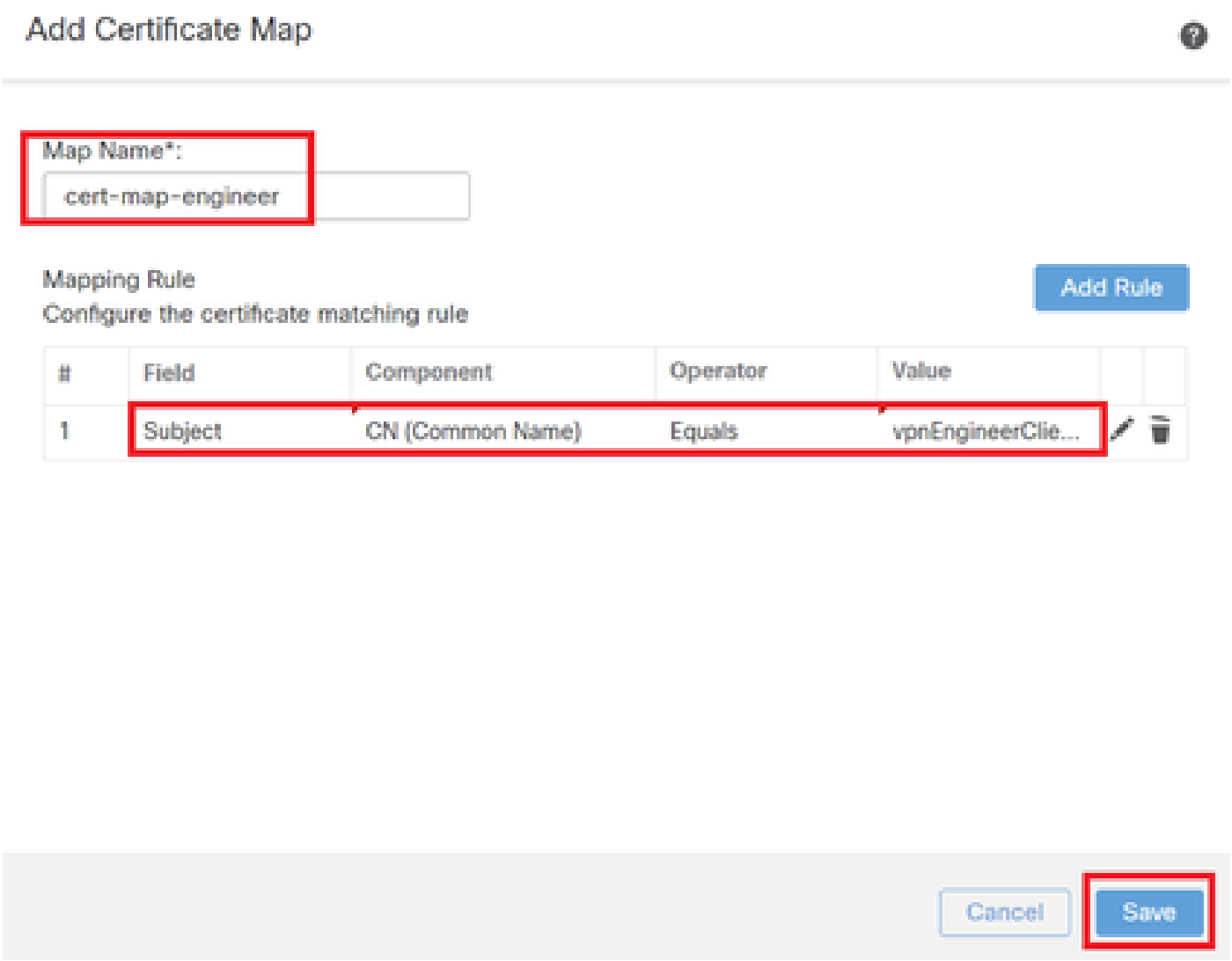
Objects(개체) > Object Management(개체 관리) > VPN > Certificate Map(인증서 맵)으로 이동하고 Add(추가)Certificate Map(인증서 맵) 버튼을 클릭합니다.



인증서 맵 추가

엔지니어 VPN 클라이언트의 인증서 맵에 필요한 정보를 입력하고 Save(저장) 버튼을 클릭합니다.

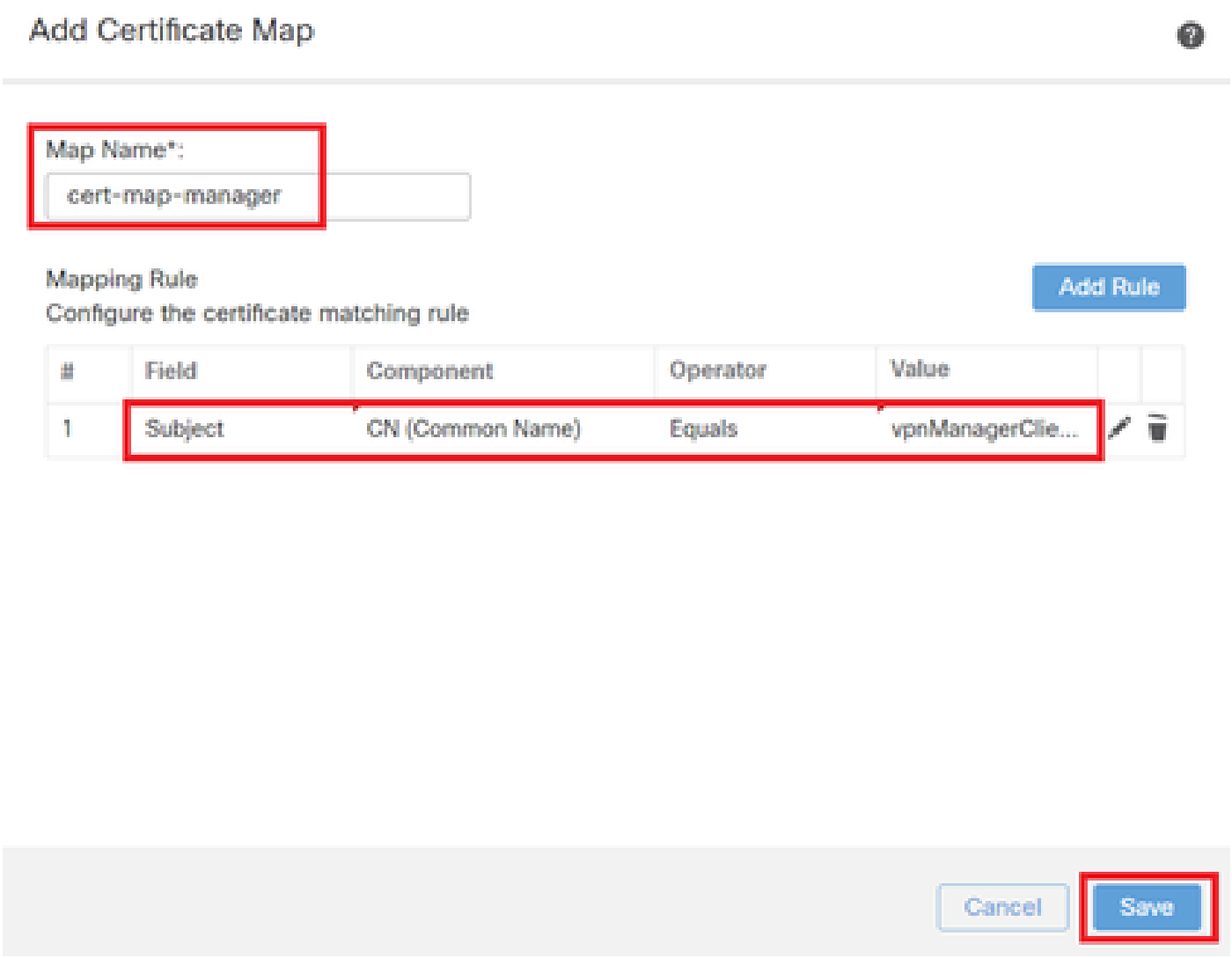
- 맵 이름: cert-map-engineer
- 매핑 규칙: CN(Common Name) Equals vpnEngineerClientCN



엔지니어 클라이언트의 인증서 맵

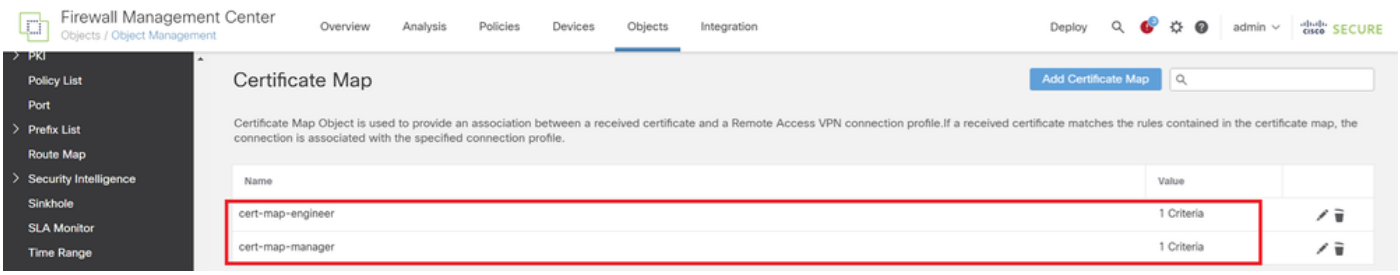
관리자 VPN 클라이언트의 인증서 맵에 필요한 정보를 입력하고 Save(저장) 버튼을 클릭합니다.

- 맵 이름: cert-map-manager
- 매핑 규칙: CN(Common Name) Equals vpnManagerClientCN



관리자 클라이언트의 인증서 맵

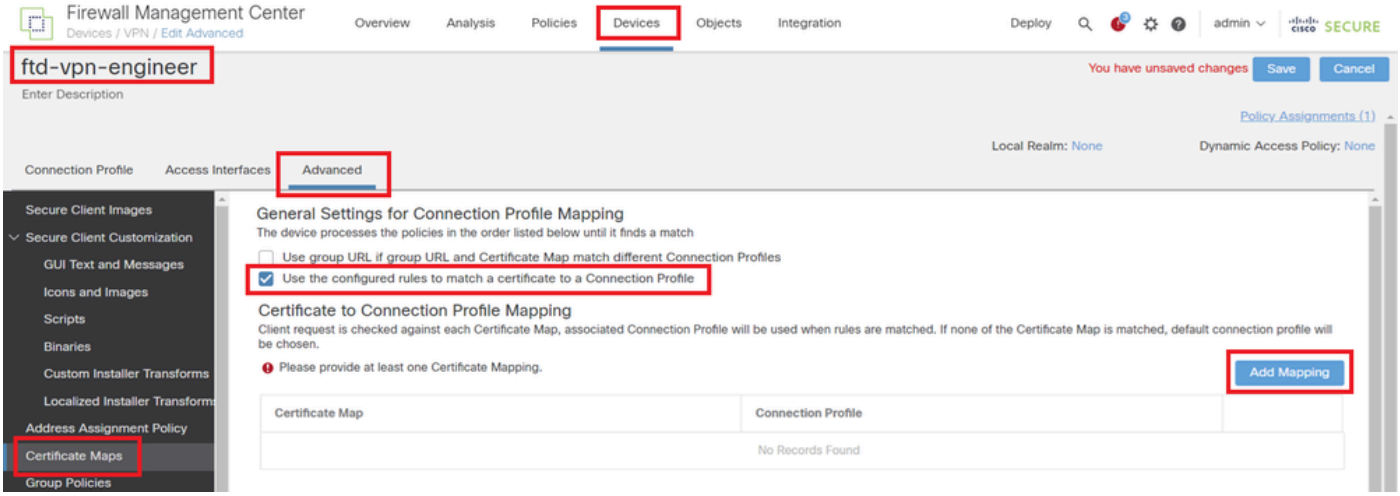
새로 추가된 인증서 맵을 확인합니다.



새 인증서 맵

13단계. 연결 프로파일에 인증서 맵 바인딩

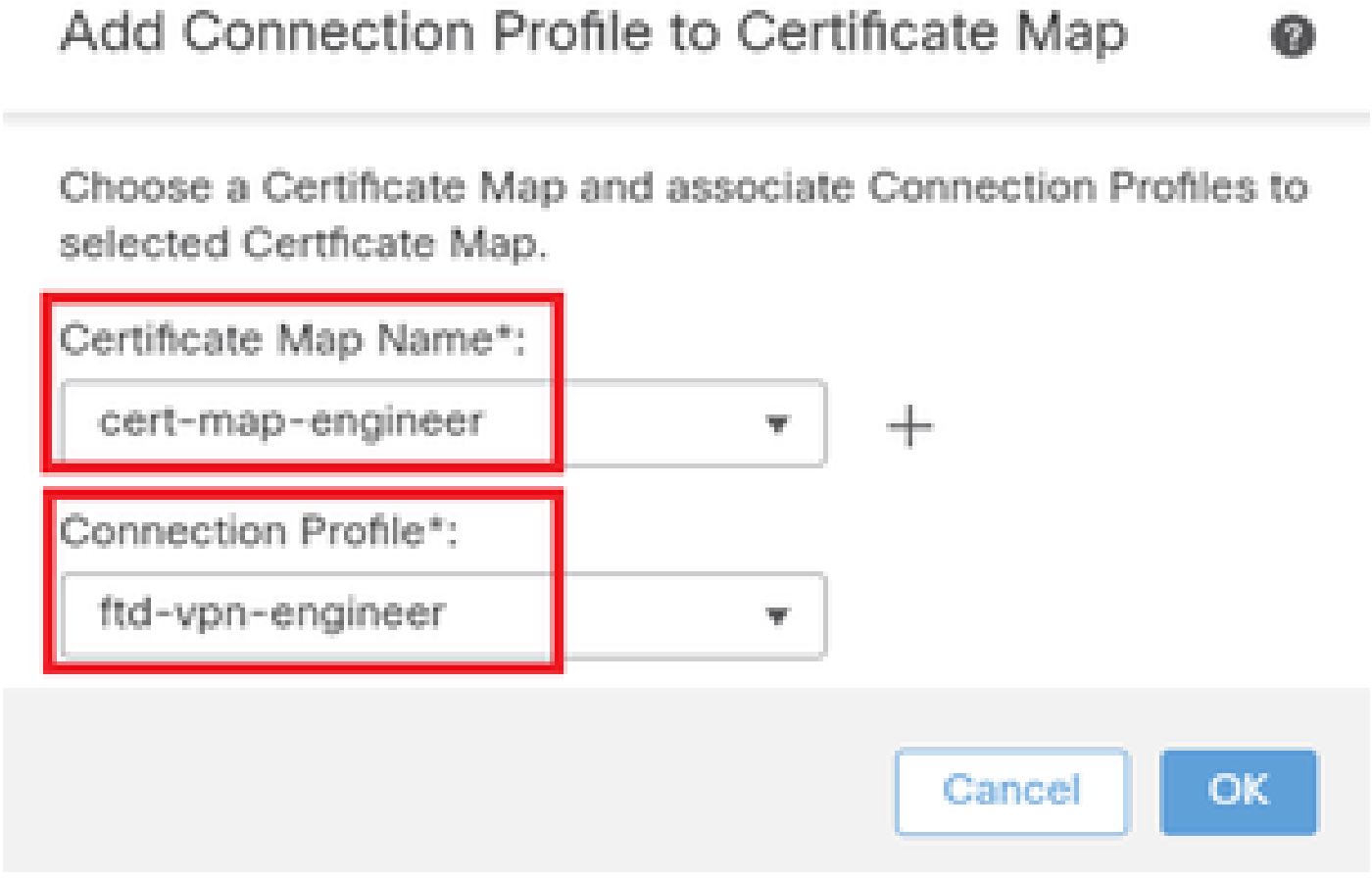
Devices(디바이스) > VPN > Remote Access(원격 액세스), edit ftd-vpn-engineer(ftd-vpn-engineer 수정)로 이동합니다. 그런 다음 Advanced(고급) > Certificate Maps(인증서 맵)로 이동하고 Add Mapping(매핑 추가) 버튼을 클릭합니다.



인증서 맵 바인딩

엔지니어 VPN 클라이언트의 연결 프로파일에 인증서 맵 바인딩

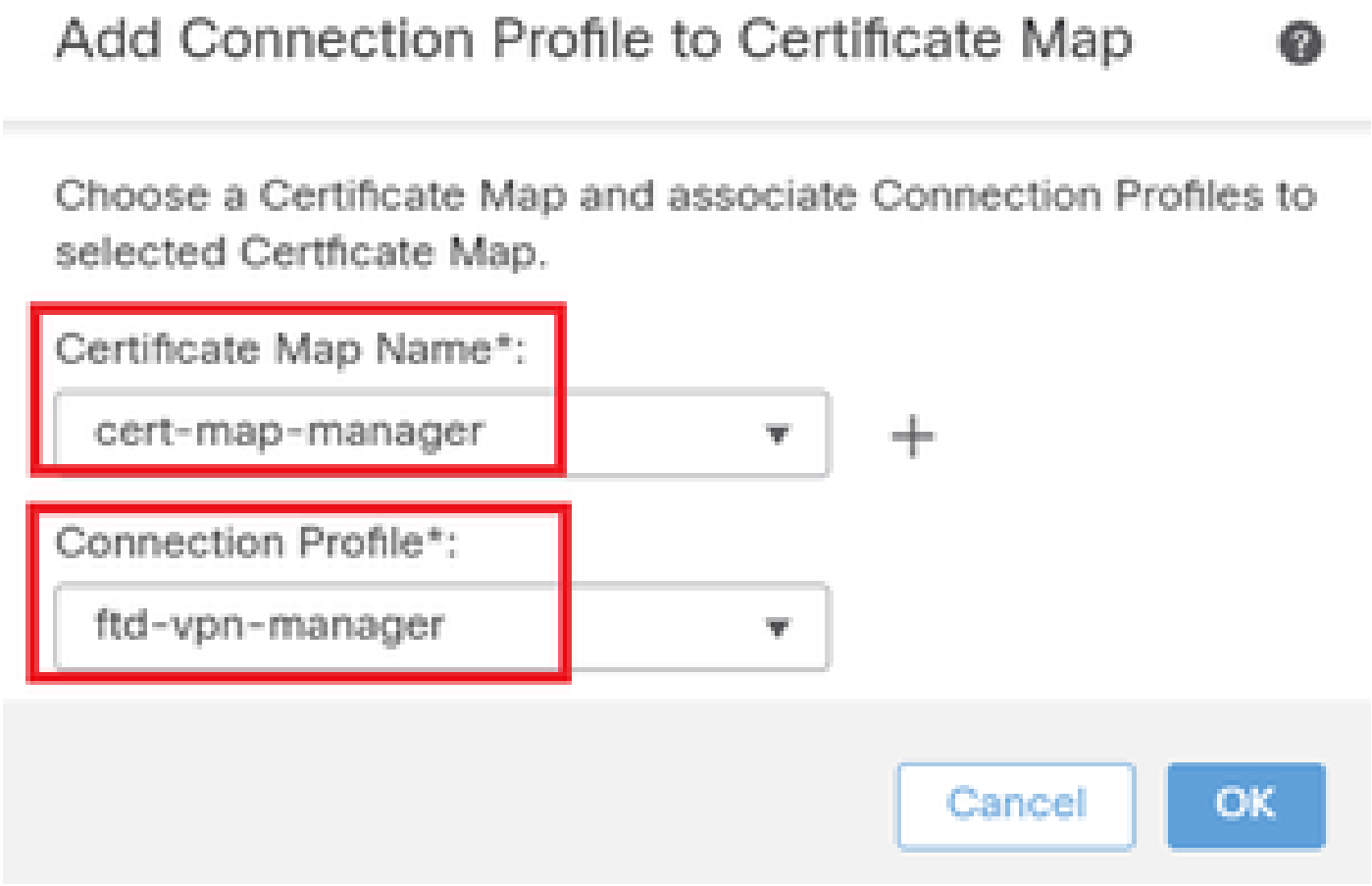
- 인증서 맵 이름: cert-map-engineer
- 연결 Profile: ftd-vpn-engineer



Engineer VPN 클라이언트에 대한 인증서 맵 바인딩

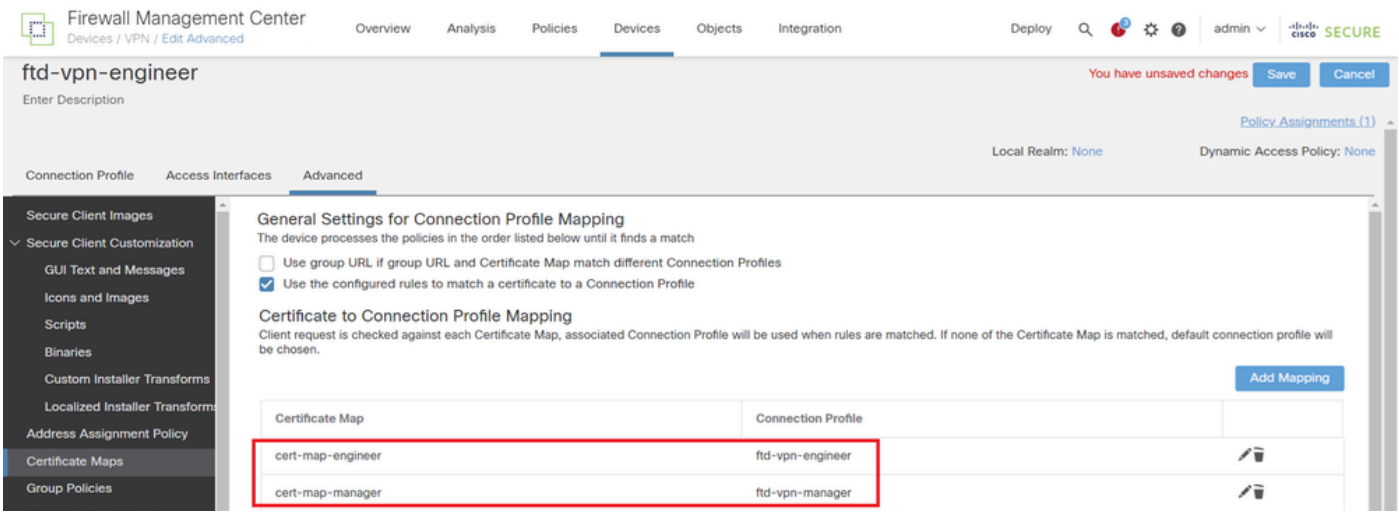
관리자 VPN 클라이언트에 대한 연결 프로파일에 인증서 맵을 바인딩합니다.

- 인증서 맵 이름: cert-map-manager
- 연결 프로파일: ftd-vpn-manager



Manager VPN 클라이언트에 대한 인증서 맵 바인딩

인증서 바인딩의 설정을 확인합니다.



인증서 바인딩 확인

FTD CLI에서 확인

FMC에서 구축한 후 FTD CLI에서 VPN 연결 설정을 확인합니다.

```
// Defines IP of interface
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
keypair ftd-vpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftd-vpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-grp attributes
banner none
wins-server none
dns-server none
```

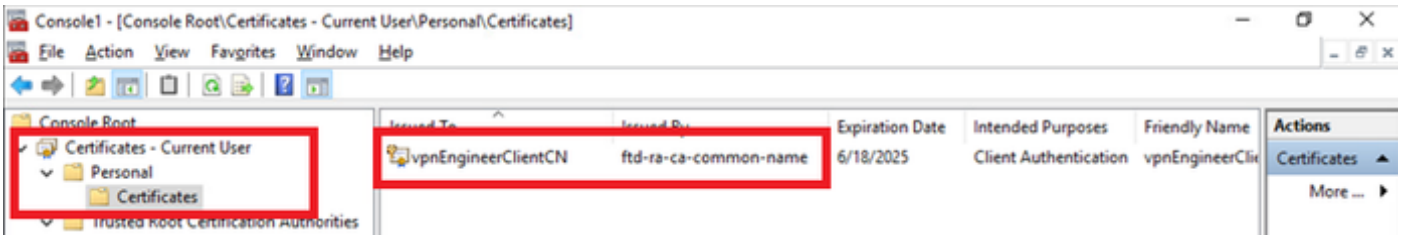
```
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
```

```
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the tunnel-group to use the certificate authentication for engineer VPN clients
tunnel-group ftd-vpn-engineer type remote-access
tunnel-group ftd-vpn-engineer general-attributes
address-pool ftd-vpn-engineer-pool
default-group-policy ftd-vpn-engineer-grp
tunnel-group ftd-vpn-engineer webvpn-attributes
authentication certificate
group-alias ftd-vpn-engineer enable

// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

VPN 클라이언트에서 확인

1단계. 클라이언트 인증서 확인

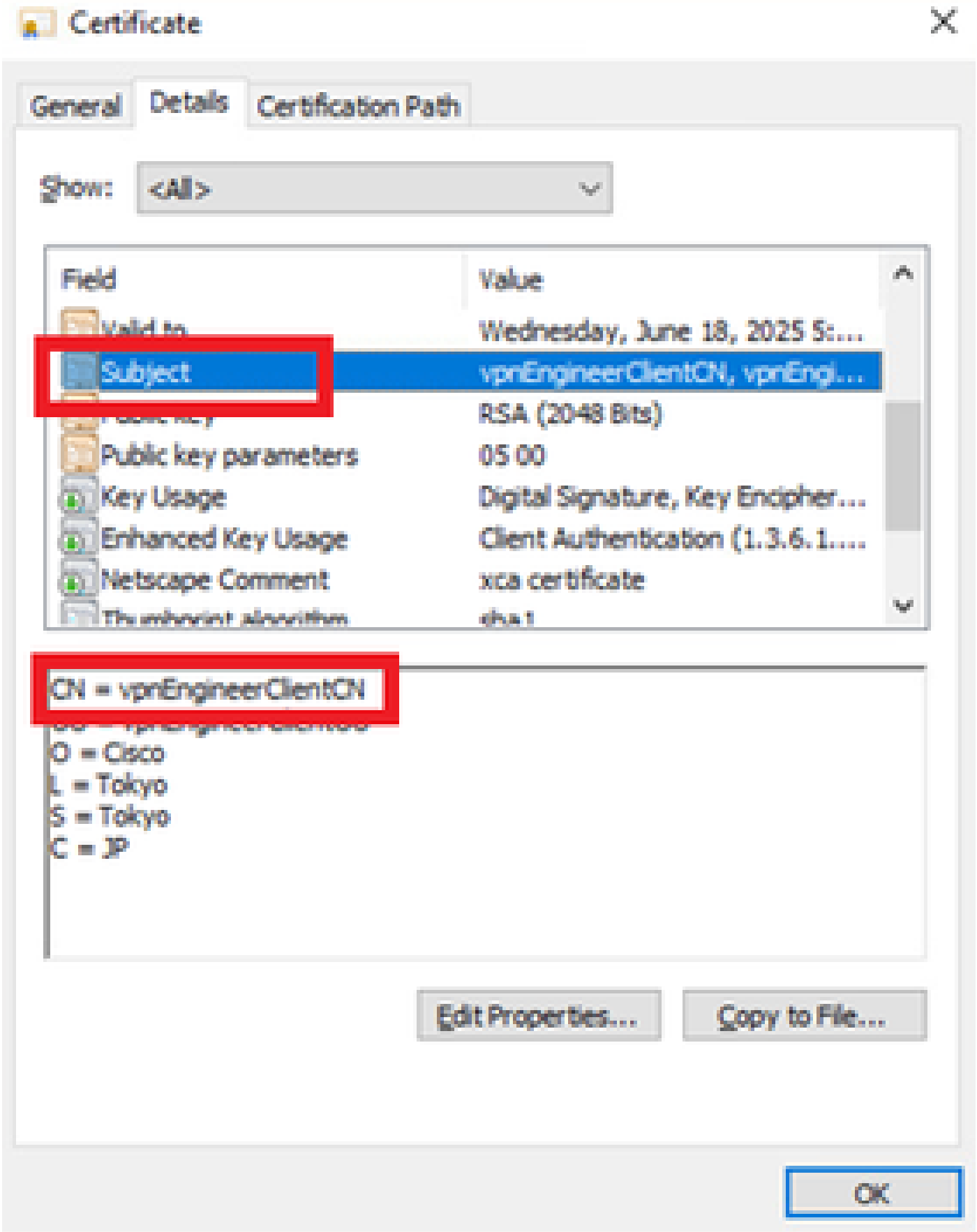
Engineer VPN 클라이언트에서 Certificates - Current User > Personal > Certificates로 이동하여 인증에 사용된 클라이언트 인증서를 확인합니다.



엔지니어 VPN 클라이언트의 인증서 확인

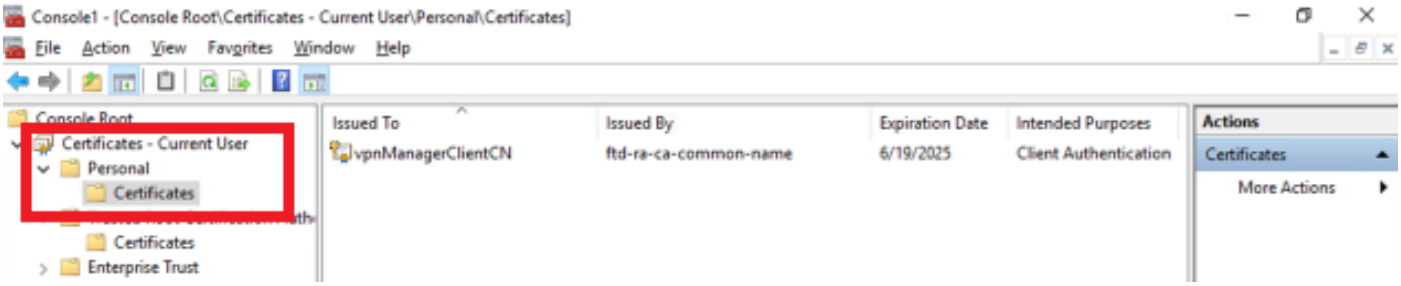
클라이언트 인증서를 두 번 클릭하고 Details(세부사항)로 이동하여 Subject(주체)의 세부사항을 확인합니다.

- 제목: CN = vpnEngineerClientCN



엔지니어 클라이언트 인증서 세부사항

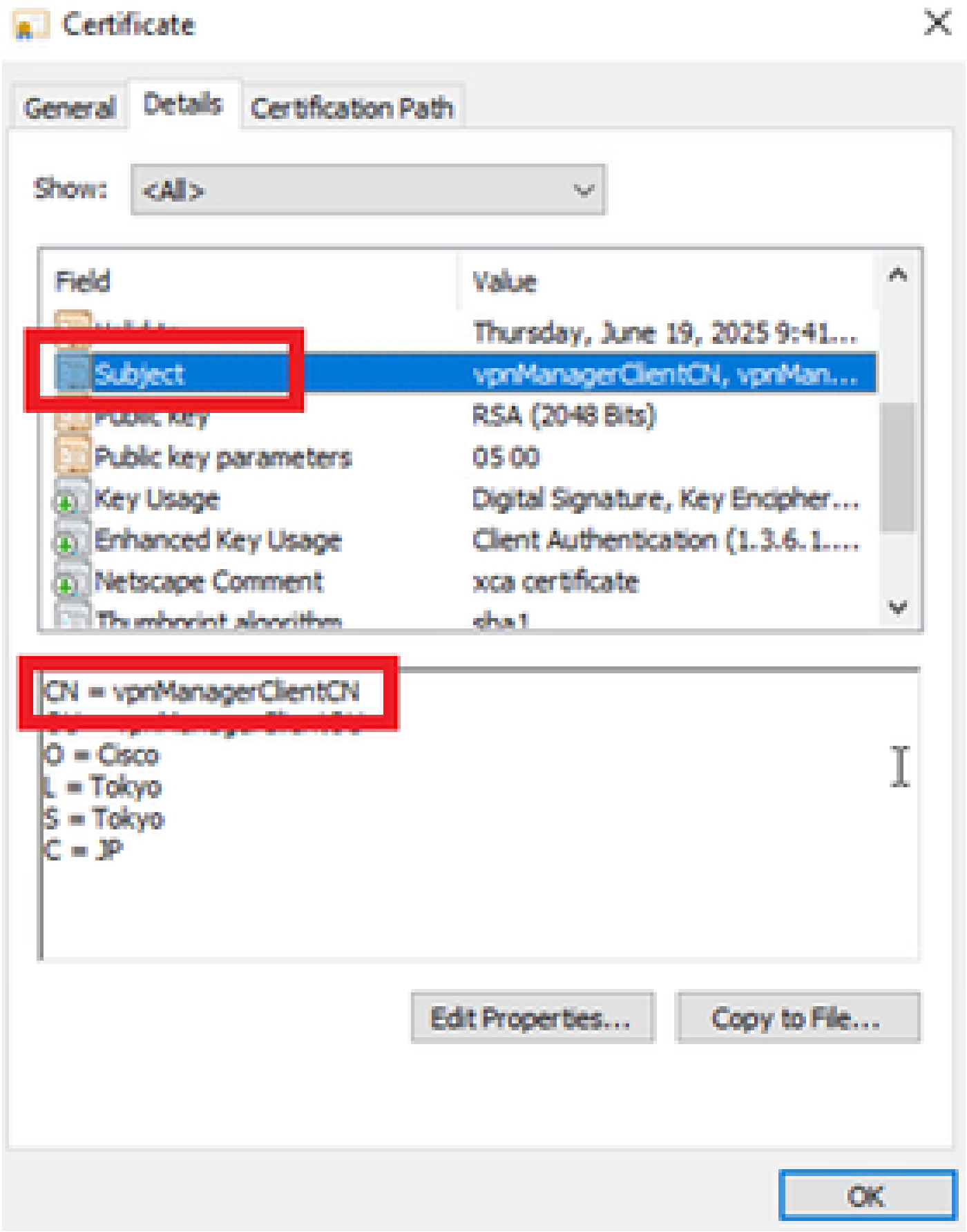
관리자 VPN 클라이언트에서 Certificates - Current User > Personal > Certificates로 이동하여 인증에 사용되는 클라이언트 인증서를 확인합니다.



관리자 VPN 클라이언트에 대한 인증서 확인

클라이언트 인증서를 두 번 클릭하고 Details(세부사항)로 이동하여 Subject(주체)의 세부사항을 확인합니다.

- 제목: CN = vpnManagerClientCN

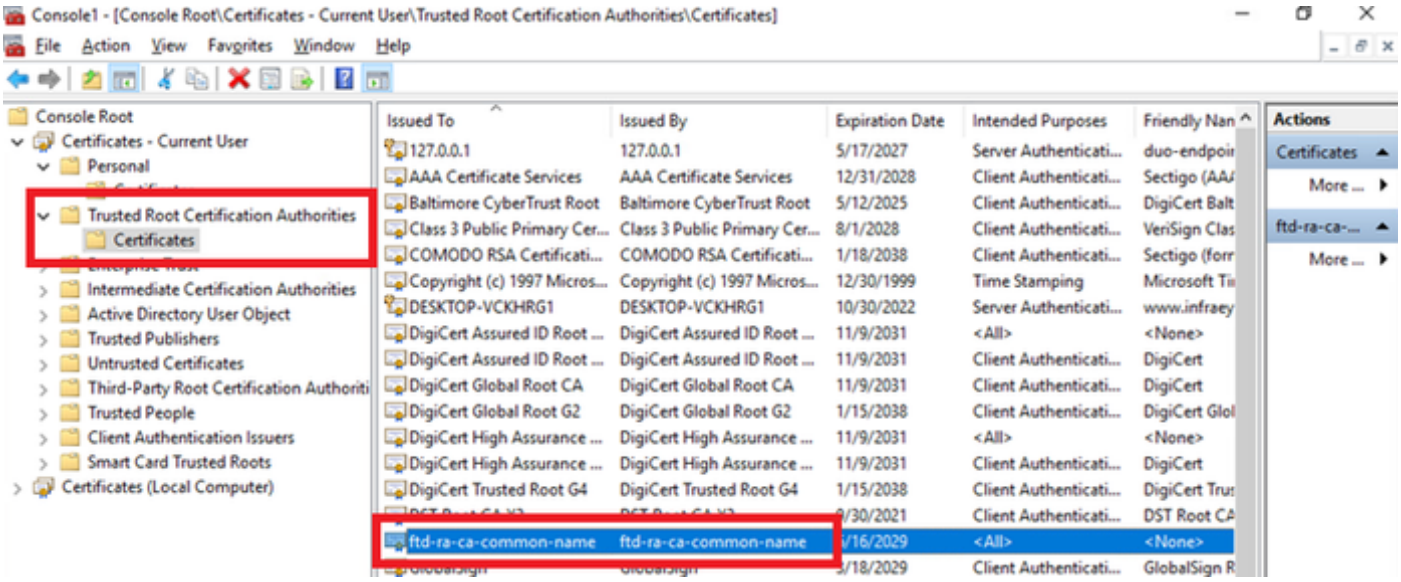


관리자 클라이언트 인증서 세부 정보

2단계. CA 확인

Engineer VPN 클라이언트와 manager VPN 클라이언트에서 Certificates - Current User(인증서 - 현재 사용자) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(인증서)로 이동하여 인증에 사용되는 CA를 확인합니다.

- 발급자: ftd-ra-ca-common-name

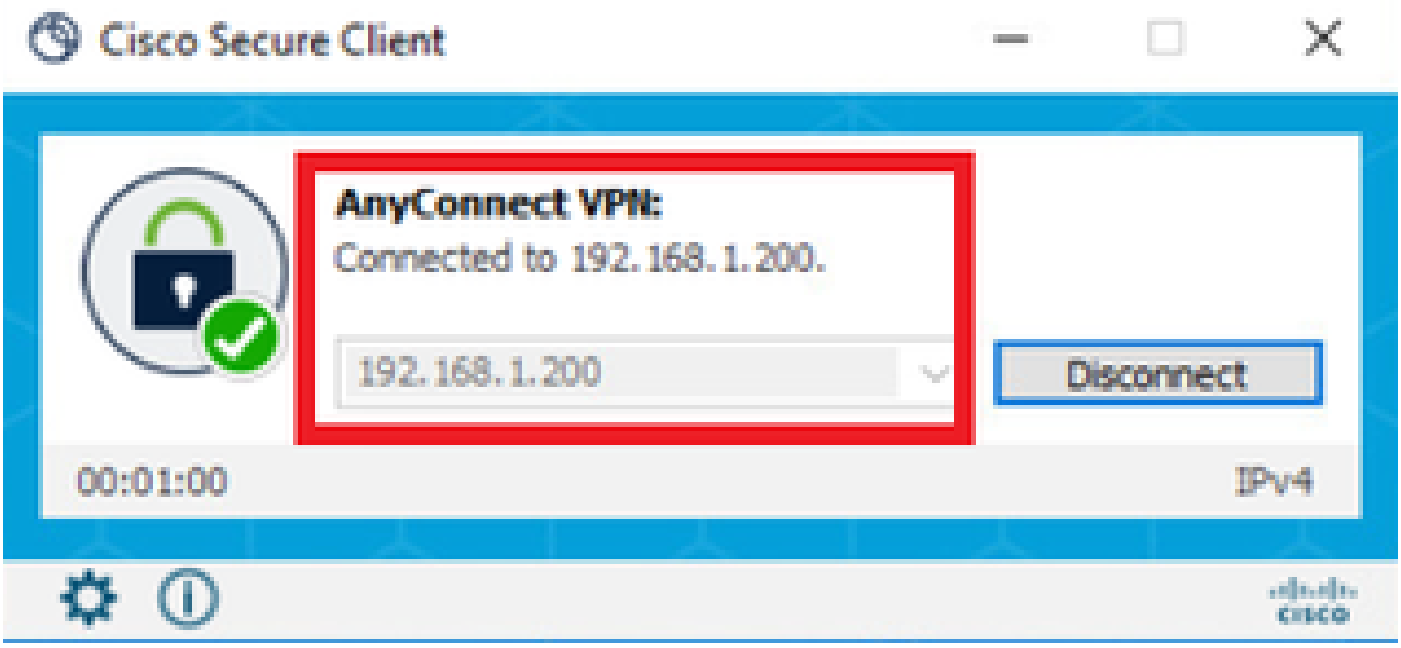


CA 확인

다음을 확인합니다.

1단계. VPN 연결 시작

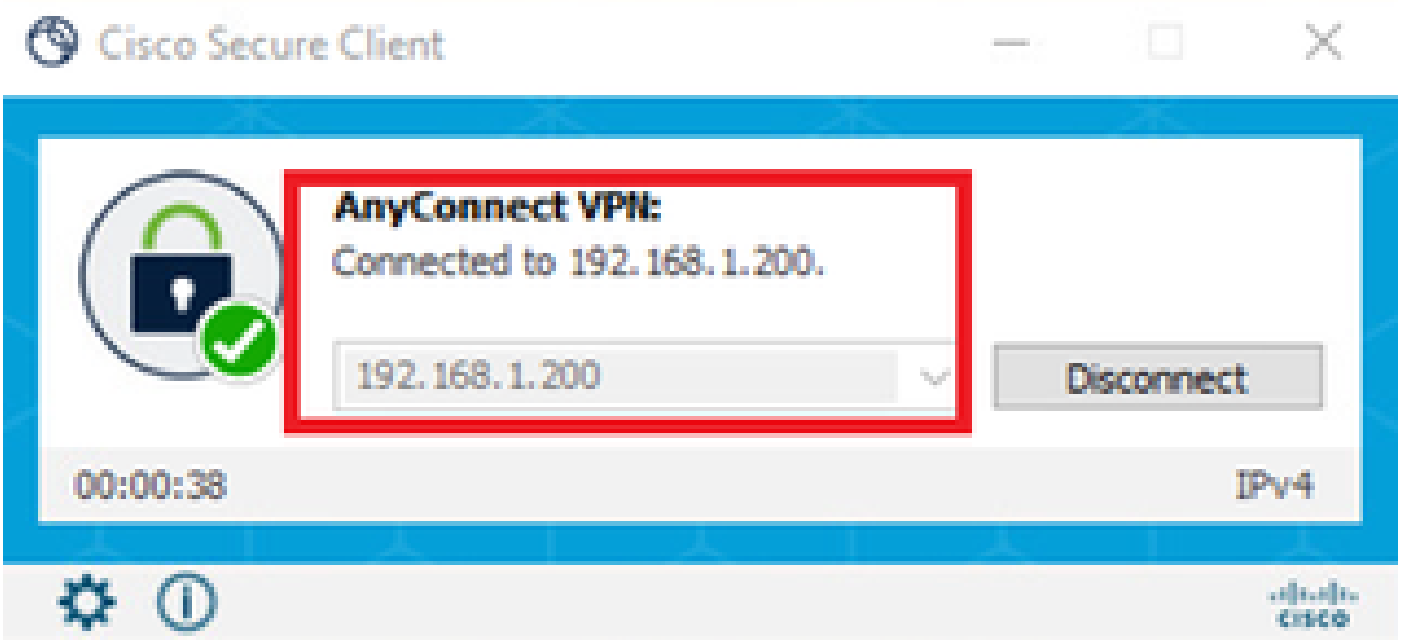
엔지니어 VPN 클라이언트에서 Cisco Secure Client 연결을 시작합니다. 사용자 이름과 비밀번호를 입력할 필요가 없습니다. VPN이 성공적으로 연결되었습니다.



엔지니어 클라이언트에서 VPN 연결 시작

관리자 VPN 클라이언트에서 Cisco Secure Client 연결을 시작합니다. 사용자 이름과 비밀번호를

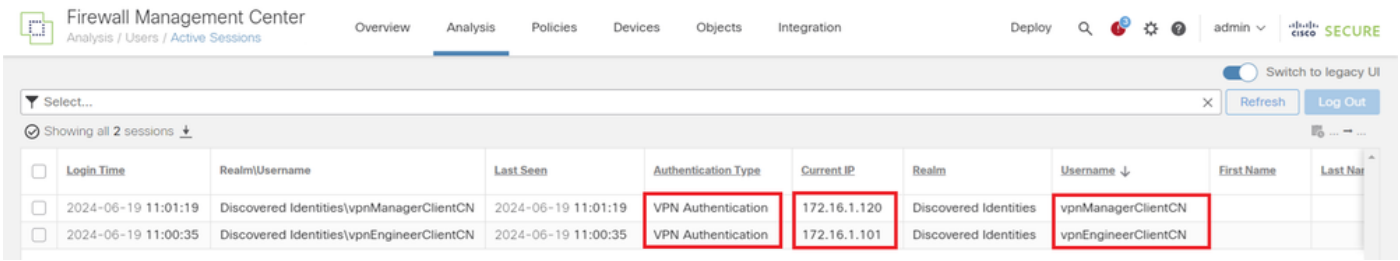
입력할 필요가 없습니다. VPN이 성공적으로 연결되었습니다.



관리자 클라이언트에서 VPN 연결 시작

2단계. FMC에서 활성 세션 확인

Analysis(분석) > Users(사용자) > Active Sessions(활성 세션)로 이동하여 활성 세션에서 VPN 인증을 확인합니다.



활성 세션 확인

3단계. FTD CLI에서 VPN 세션 확인

FTDshow vpn-sessiondb detail anyconnect(Lina) CLI에서 명령을 실행하여 엔지니어와 관리자의 VPN 세션을 확인합니다.

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
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 : 14782 Bytes Rx : 12714
```

Pkts Tx : 2 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
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 : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

문제 해결

Lina 엔진의 디버그 syslog 및 Windows PC의 DART 파일에서 VPN 인증에 대한 정보를 찾을 수 있습니다.

다음은 엔지니어 클라이언트에서 VPN에 연결하는 동안 Lina 엔진에 있는 디버그 로그의 예입니다.

<#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jun 19 2024 02:00:35: %FTD-6-717022:

Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEnginee
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50

관리자 클라이언트에서 VPN에 연결하는 동안 Lina 엔진에 있는 디버그 로그의 예입니다.

<#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vp
Jun 19 2024 02:01:19: %FTD-6-717022:

Certificate was successfully validated

. serial number: 1AD1B5EAE28C6D3C, subject name:

CN=vpnManagerClientCN

,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-manager

, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerC
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65

관련 정보

모바일 액세스를 위한 Anyconnect 인증서 기반 인증 구성

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.