FDM을 통해 FTD에서 보안 클라이언트 인증에 대한 인증서 일치 구성

목차

소개

이 문서에서는 인증에 인증서 일치를 사용하여 FDM을 통해 FTD에서 SSL을 사용하여 Cisco Secure Client를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FDM(Firepower 장치 관리자) 가상
- FTD(Firewall Threat Defense) 가상
- VPN 인증 흐름

사용되는 구성 요소

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8

- Cisco Secure Client 5.1.4.74
- 프로파일 편집기(Windows) 5.1.4.74

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

CertificateMatch는 관리자가 클라이언트가 VPN 서버와의 인증을 위해 클라이언트 인증서를 선택하는 데 사용해야 하는 기준을 구성할 수 있는 기능입니다. 이 컨피그레이션은 프로파일 편집기를 사용하여 관리하거나 수동으로 편집할 수 있는 XML 파일인 클라이언트 프로파일에 지정됩니다. CertificateMatch 기능은 특정 특성의 인증서만 VPN 연결에 사용하도록 하여 VPN 연결의 보안을 강화하는 데 사용할 수 있습니다.

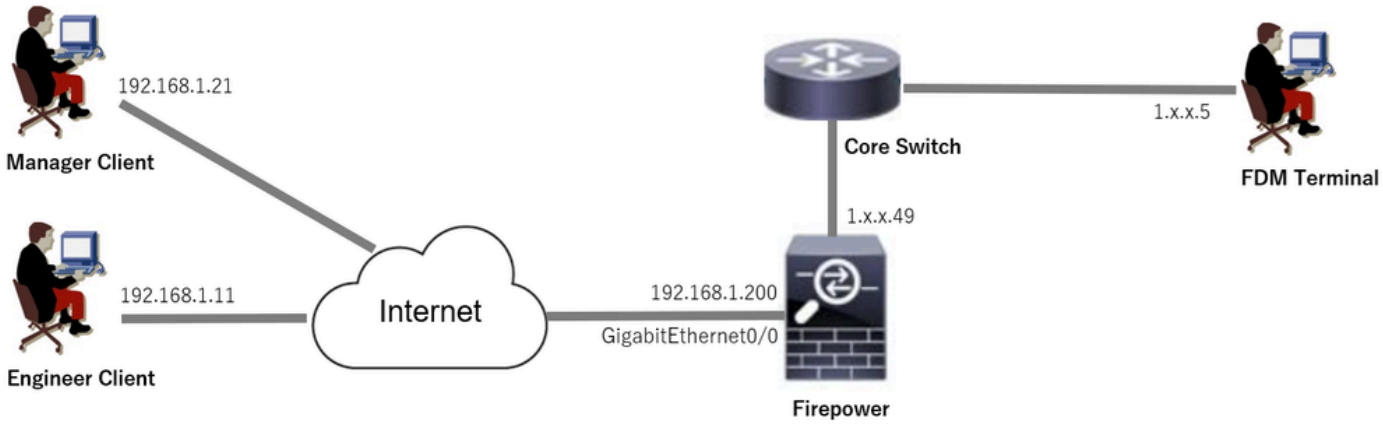
이 문서에서는 SSL 인증서의 일반 이름을 사용하여 Cisco Secure Client를 인증하는 방법에 대해 설명합니다.

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

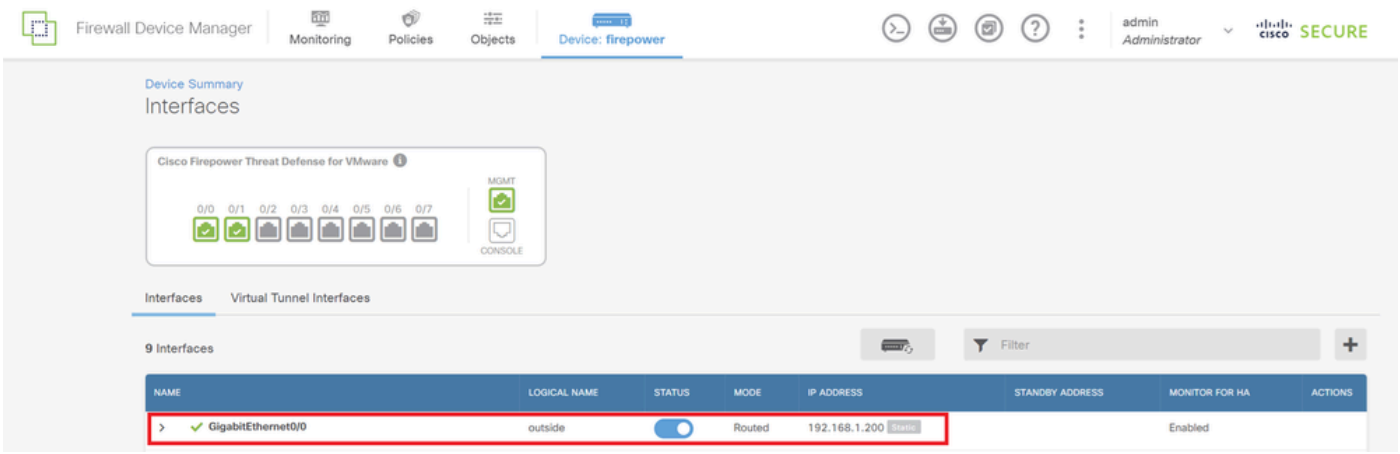
FDM의 구성

1단계. FTD 인터페이스 구성

Device(디바이스) > Interfaces(인터페이스) > View All Interfaces(모든 인터페이스 보기)로 이동하고 Interfaces(인터페이스) 탭에서 FTD에 대한 내부 및 외부 인터페이스를 구성합니다.

GigabitEthernet0/0,

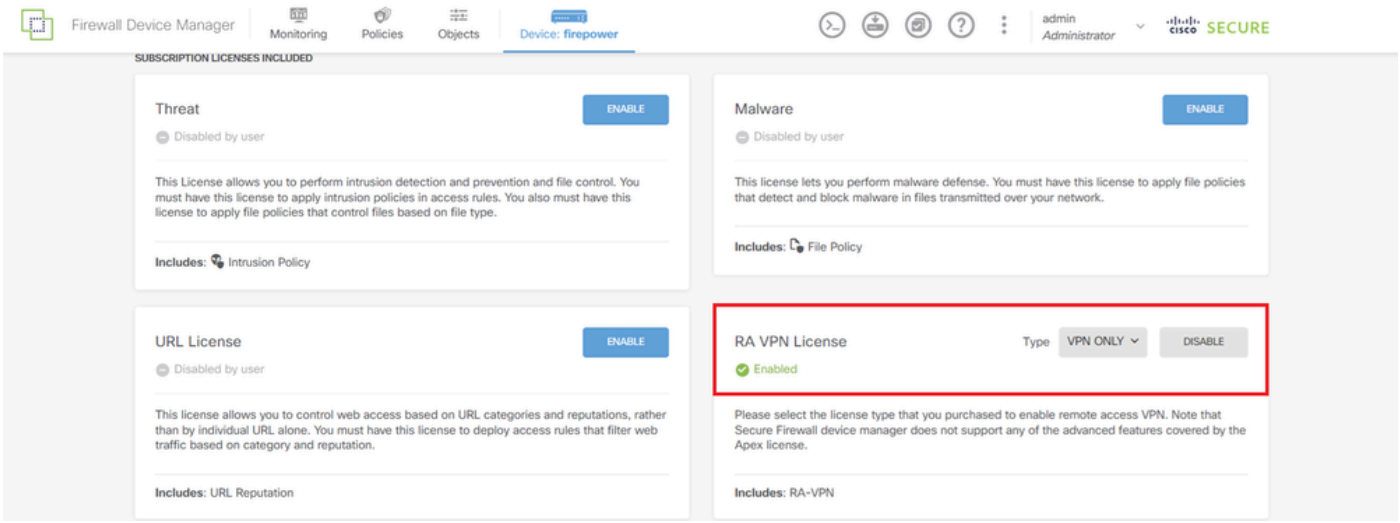
- 이름: outside
- IP 주소: 192.168.1.200/24



FTD 인터페이스

2단계. Cisco Secure Client 라이센스 확인

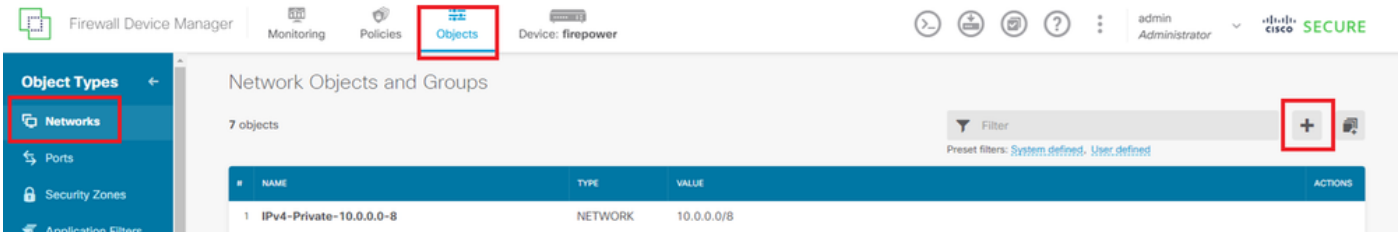
Device(디바이스) > Smart License(스마트 라이센스) > View Configuration(컨피그레이션 보기)으로 이동하여 RA VPN License(RA VPN 라이센스) 항목에서 Cisco Secure Client 라이센스를 확인합니다.



Secure Client 라이센스

3단계. 주소 풀 추가

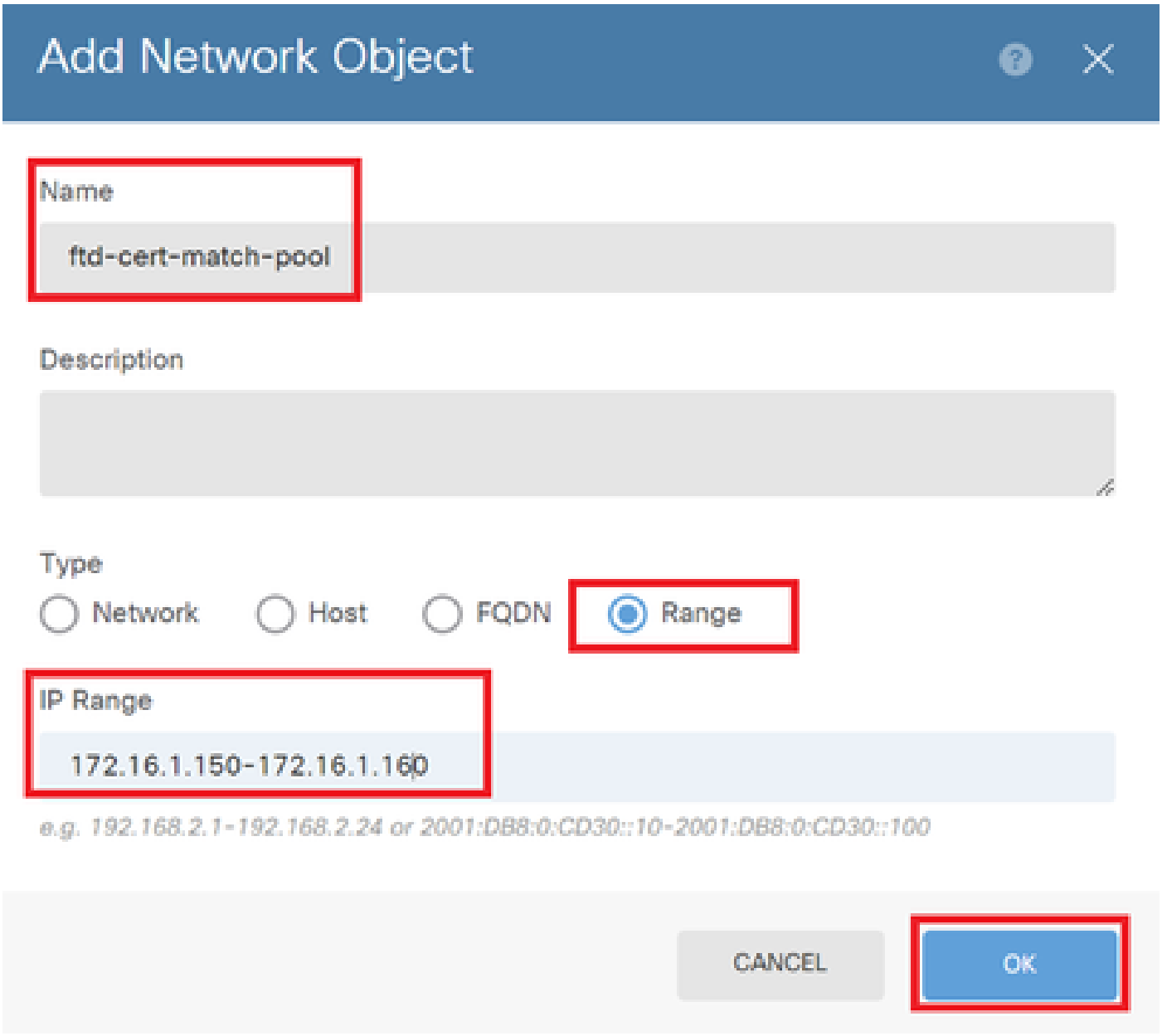
Objects(개체) > Networks(네트워크)로 이동하고 +button을 클릭합니다.



주소 풀 추가

새 IPv4 주소 풀을 추가하는 데 필요한 정보를 입력합니다. 확인 단추를 누릅니다.

- 이름: ftd-cert-match-pool
- 유형: 범위
- IP 범위: 172.16.1.150-172.16.1.160

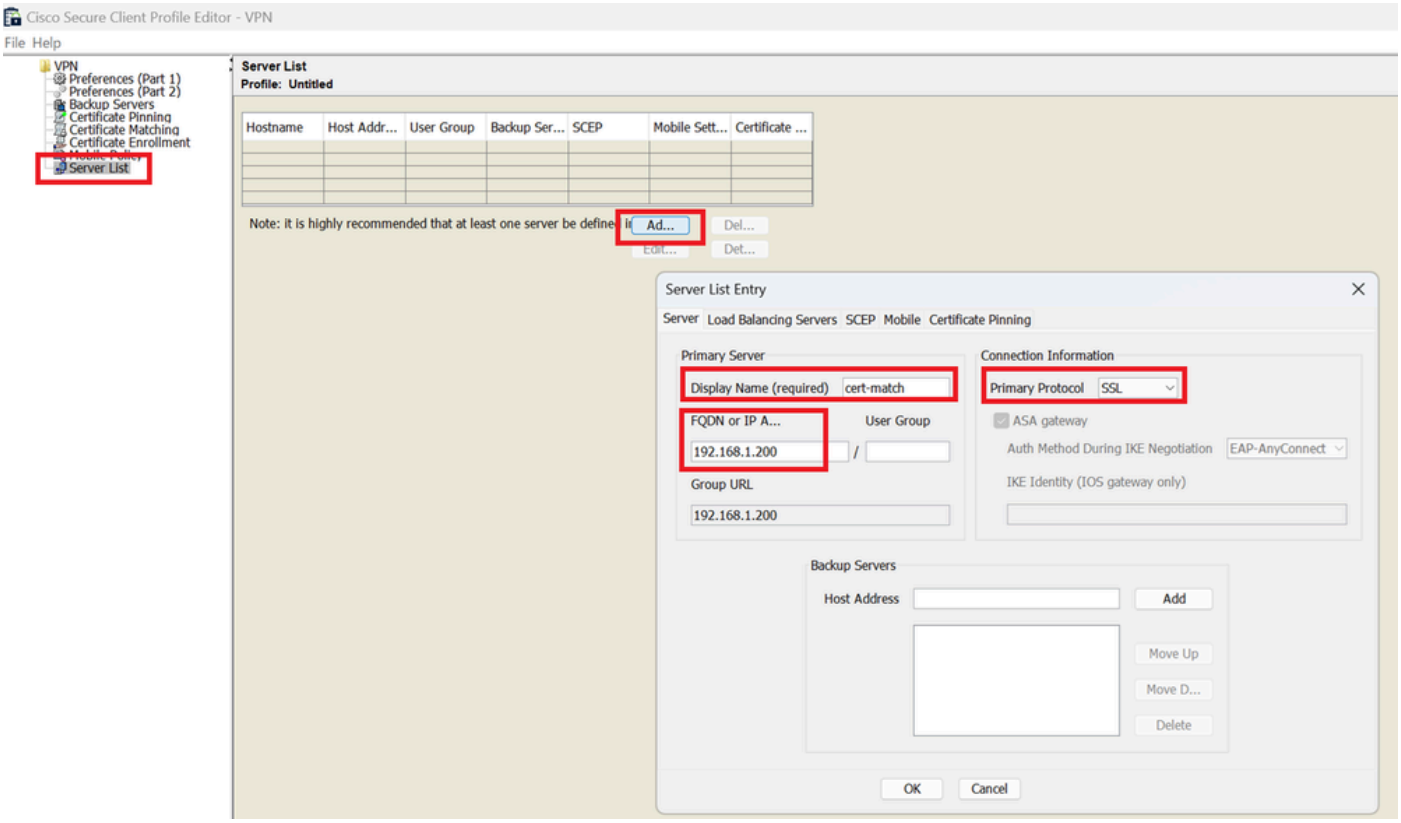


IPv4 주소 풀 세부 정보

4단계. 보안 클라이언트 프로파일 생성

Cisco Software 사이트에서 Secure Client Profile Editor를 다운로드하여 설치합니다. Server List(서버 목록)로 이동하고 Add(추가) 버튼을 클릭합니다. 서버 목록 항목을 추가하는 데 필요한 정보를 입력하고 OK(확인) 버튼을 클릭합니다.

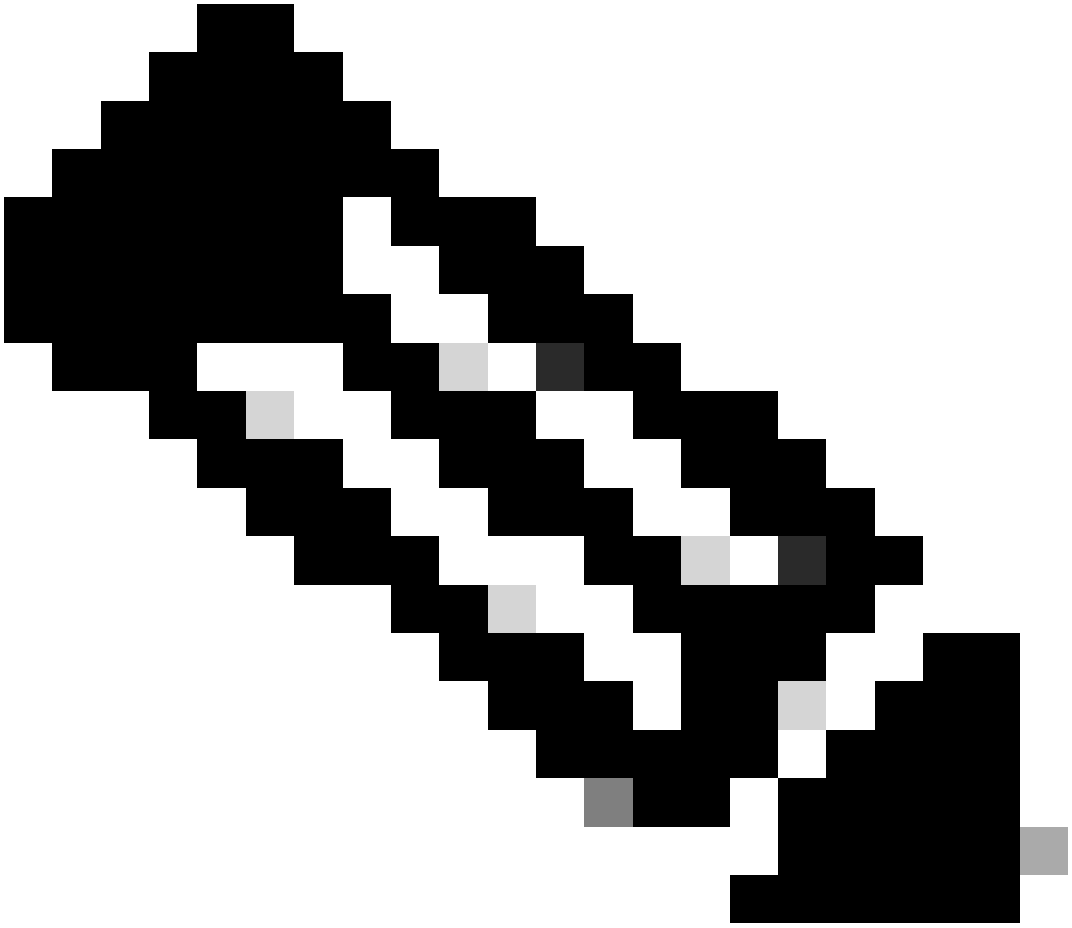
- 표시 이름: cert-match
- FQDN 또는 IP 주소: 192.168.1.200
- 기본 프로토콜: SSL



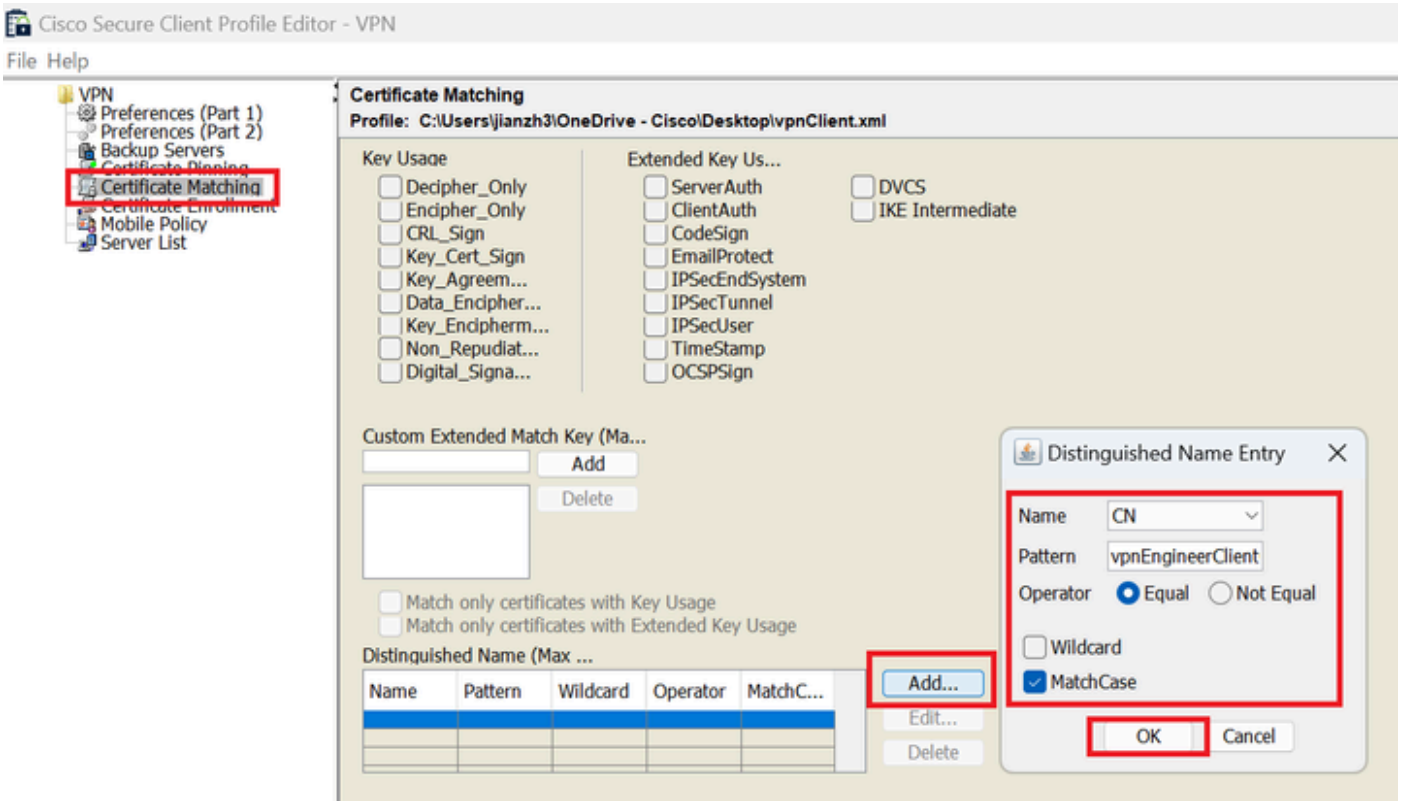
서버 목록 항목

Certificate Matching(인증서 일치)으로 이동하고 Add(추가) 버튼을 클릭합니다. Distinguished Name Entry를 추가하는 데 필요한 정보를 입력하고 OK(확인) 버튼을 클릭합니다.

- 이름: CN
- 패턴: vpnEngineerClientCN
- 연산자: 같음



참고: 이 문서에서 MatchCase 옵션을 선택합니다.



고유 이름 항목

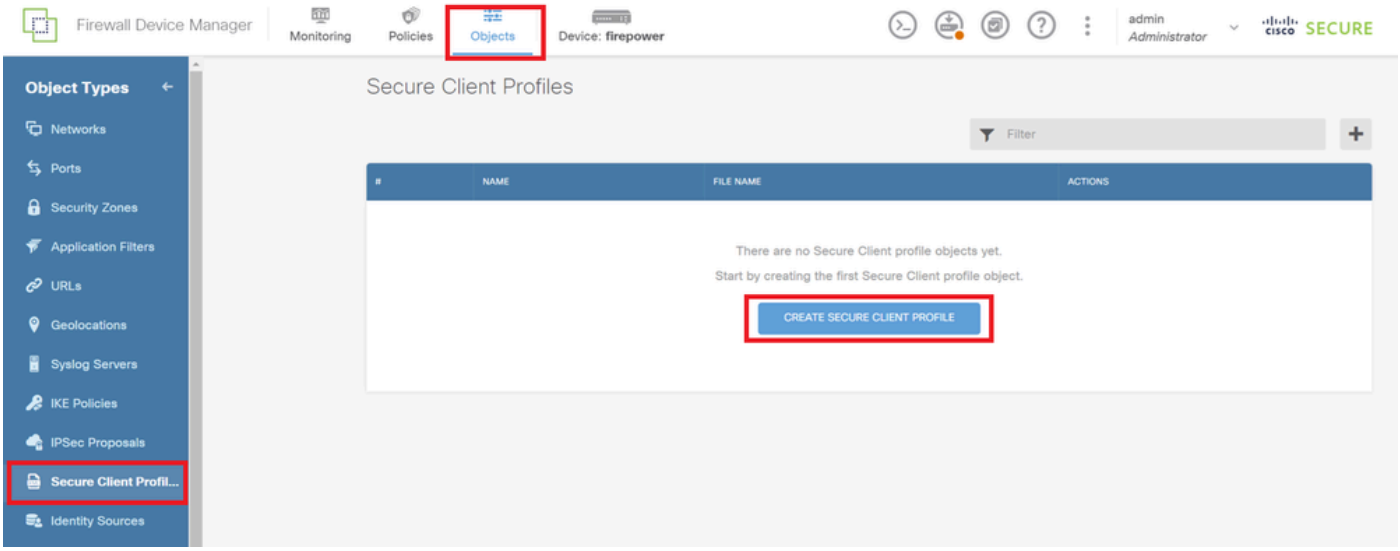
보안 클라이언트 프로파일을 로컬 컴퓨터에 저장하고 프로파일 세부사항을 확인합니다.

```
▼<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  ▼<DistinguishedName>
    ▼<DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
▼<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
▼<ServerList>
  ▼<HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

보안 클라이언트 프로파일

5단계. FDM에 보안 클라이언트 프로파일 업로드

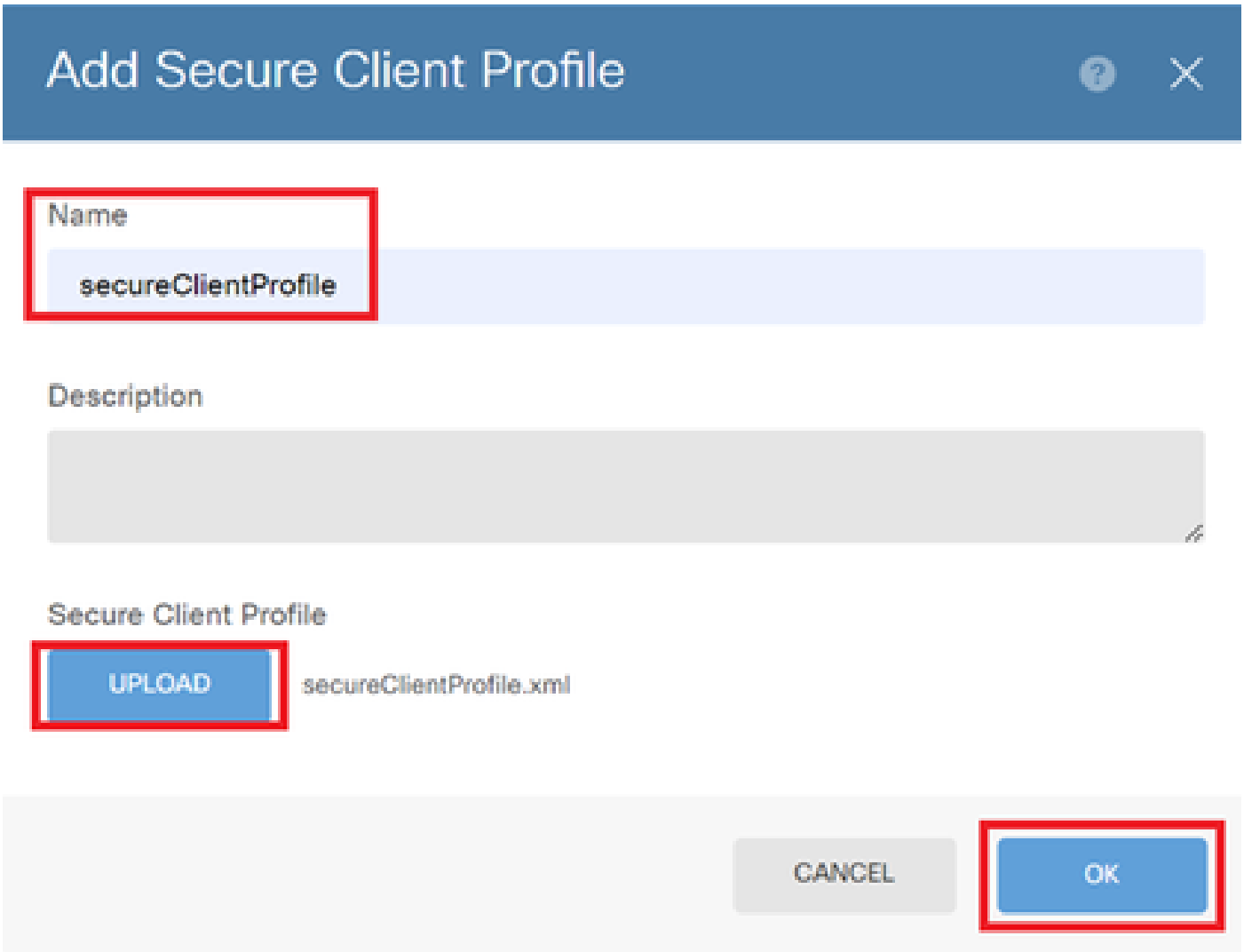
Objects(개체) > Secure Client Profile(보안 클라이언트 프로파일)로 이동하고 CREATE SECURE CLIENT PROFILE(보안 클라이언트 프로파일 생성) 버튼을 클릭합니다.



보안 클라이언트 프로파일 생성

보안 클라이언트 프로파일을 추가하는 데 필요한 정보를 입력하고 OK(확인) 버튼을 클릭합니다.

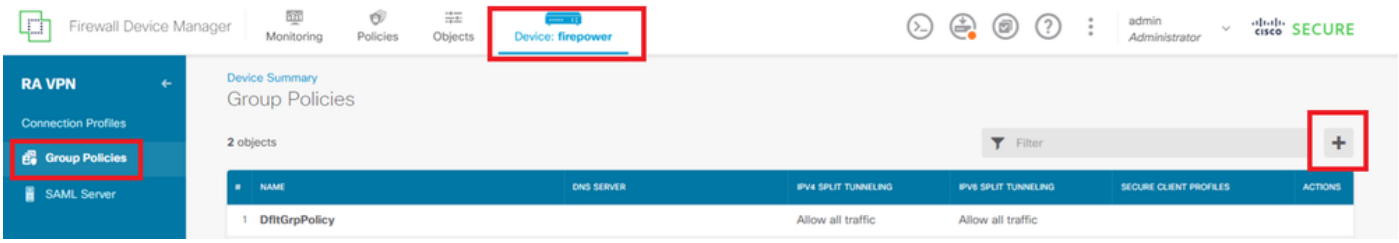
- 이름: secureClientProfile
- 보안 클라이언트 프로파일: secureClientProfile.xml(로컬 컴퓨터에서 업로드)



보안 클라이언트 프로파일 추가

6단계. 그룹 정책 추가

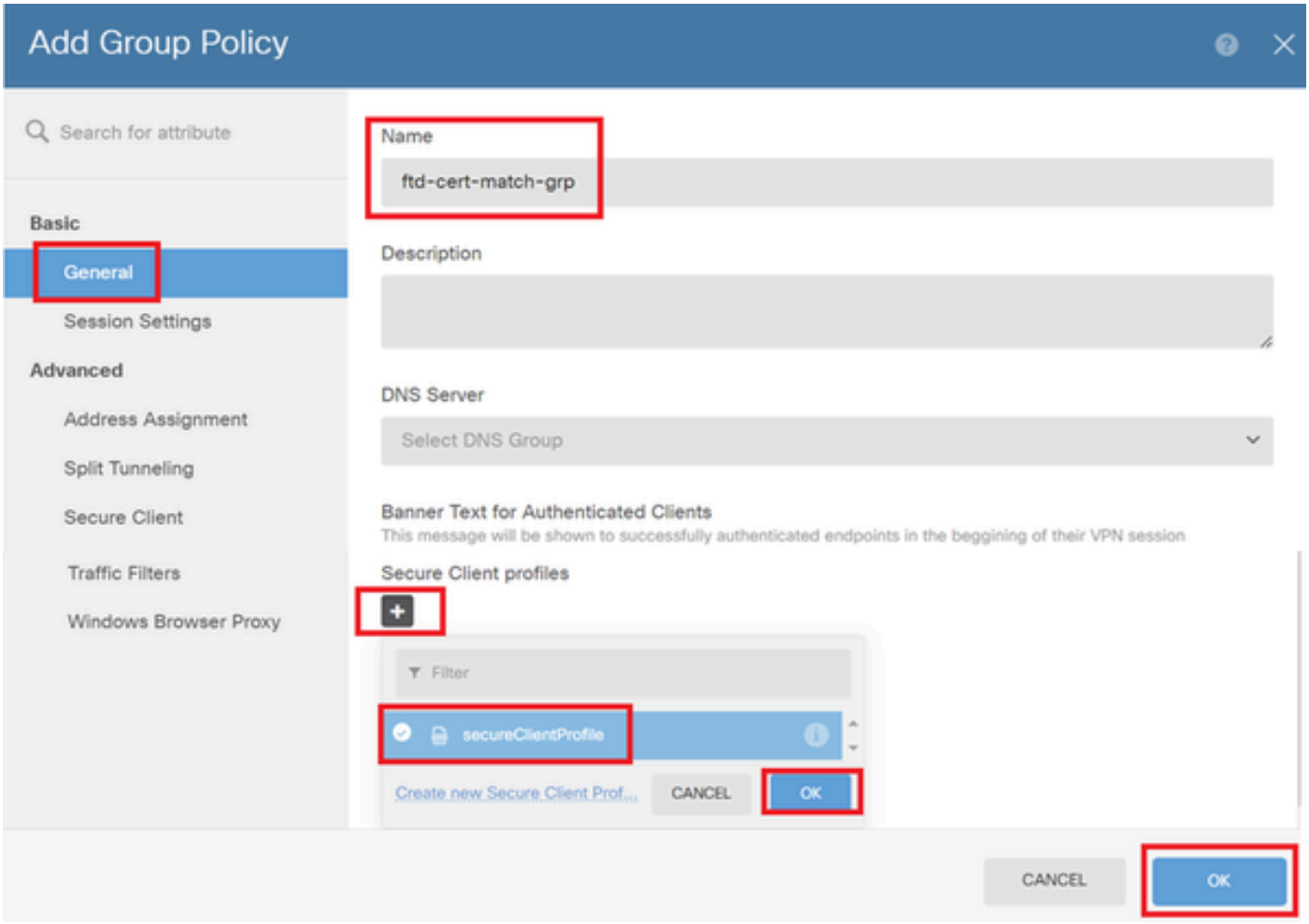
Device(디바이스) > Remote Access VPN(원격 액세스 VPN) > View Configuration(컨피그레이션 보기) > Group Policies(그룹 정책)로 이동하고 + 버튼을 클릭합니다.



그룹 정책 추가

그룹 정책을 추가하는 데 필요한 정보를 입력하고 OK(확인) 버튼을 클릭합니다.

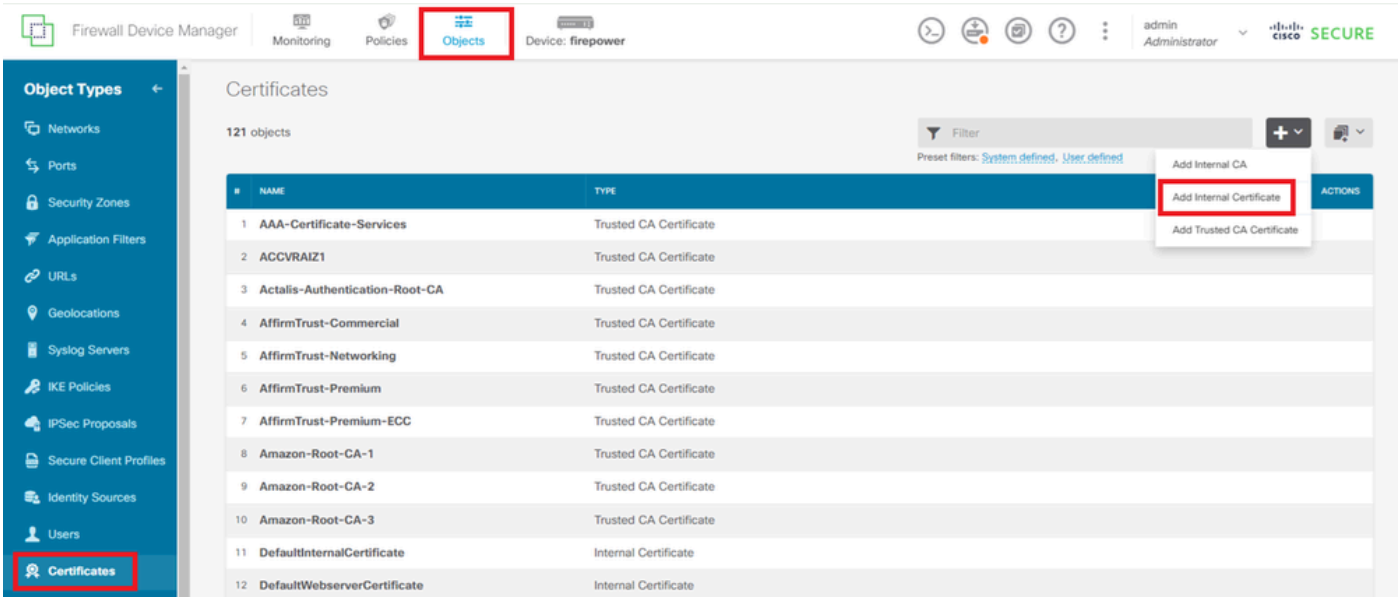
- 이름: ftd-cert-match-grp
- 보안 클라이언트 프로파일: secureClientProfile



그룹 정책 세부 정보

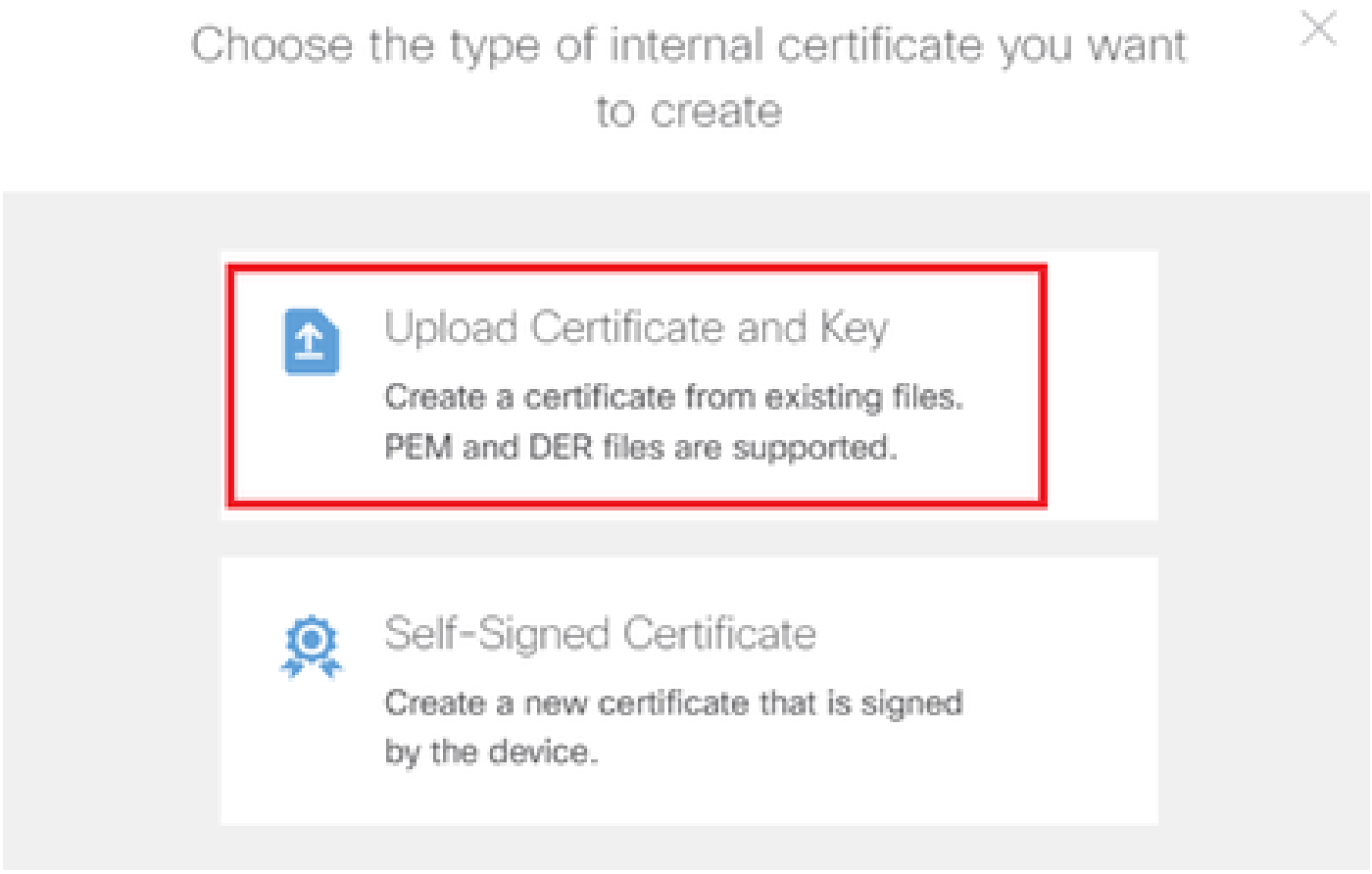
7단계. FTD 인증서 추가

Objects(개체) > Certificates(인증서)로 이동하고 Add Internal Certificate from +item(항목에서 내부 인증서 추가)을 클릭합니다.



내부 인증서 추가

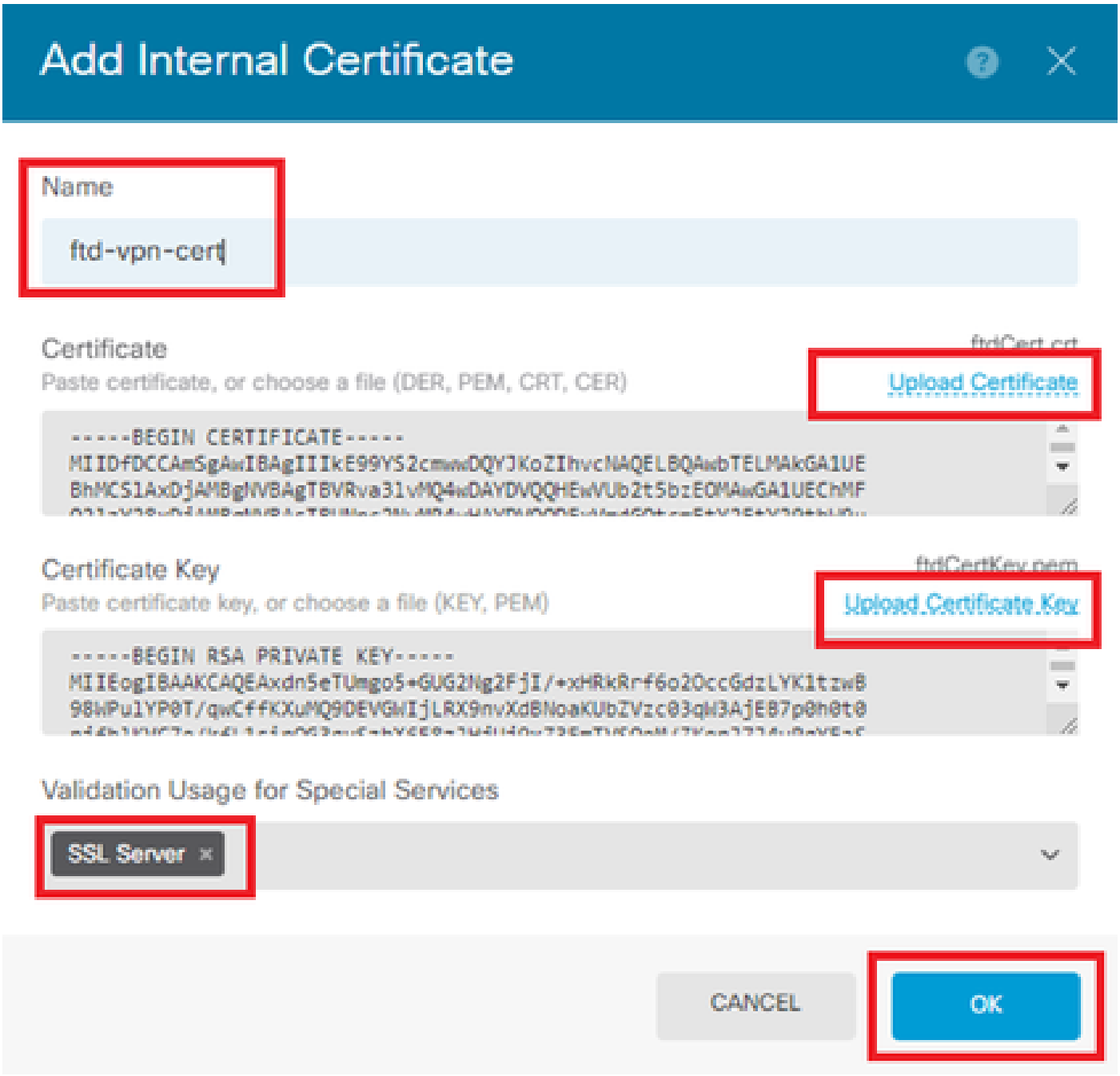
Upload Certificate and Key(인증서 및 키 업로드)를 클릭합니다.



인증서 및 키 업로드

FTD 인증서에 필요한 정보를 입력하고 로컬 컴퓨터에서 인증서와 인증서 키를 가져온 다음 OK(확인) 버튼을 클릭합니다.

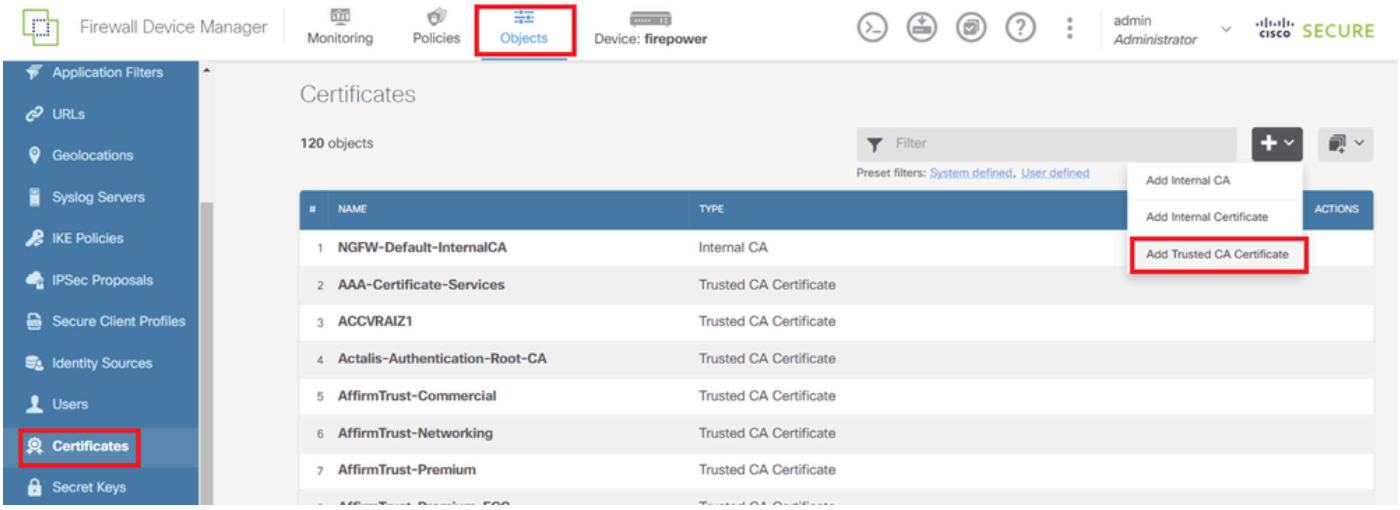
- 이름: ftd-vpn-cert
- 특수 서비스의 유효성 검사 사용: SSL 서버



내부 인증서 세부 정보

8단계. FTD에 CA 추가

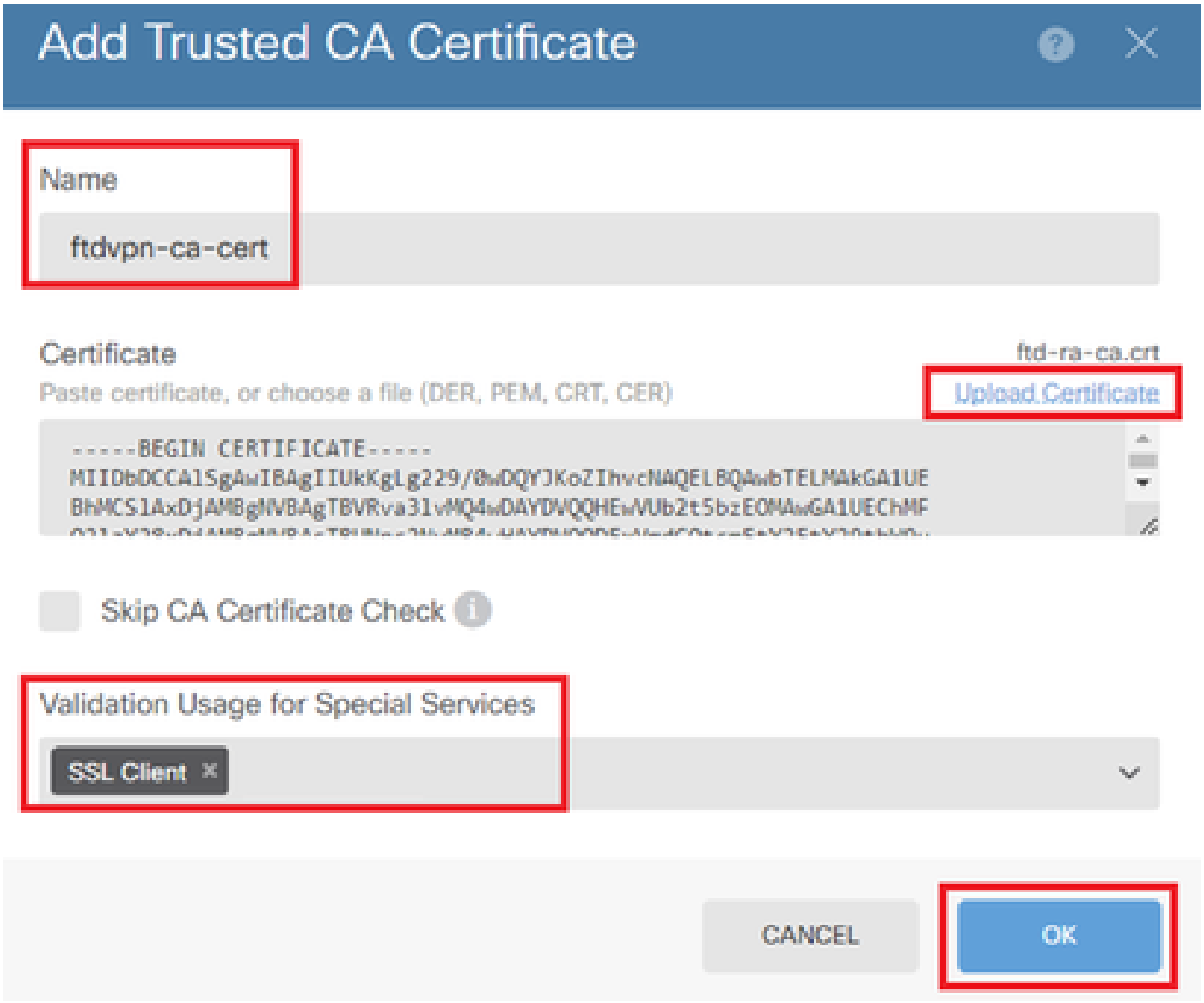
Objects(개체) > Certificates(인증서)로 이동하여 Add Trusted CA Certificate from +item(항목에서 신뢰할 수 있는 CA 인증서 추가)을 클릭합니다.



신뢰할 수 있는 CA 인증서 추가

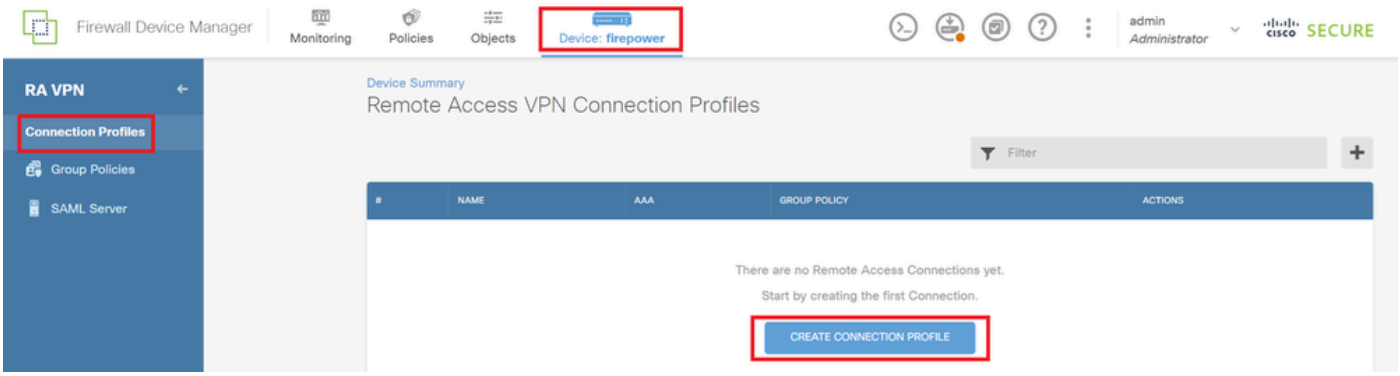
CA에 필요한 정보를 입력하고 로컬 컴퓨터에서 인증서를 가져옵니다.

- 이름: ftdvpn-ca-cert
- 특별 서비스에 대한 유효성 검사 사용: SSL 클라이언트



9단계. 원격 액세스 VPN 연결 프로파일 추가

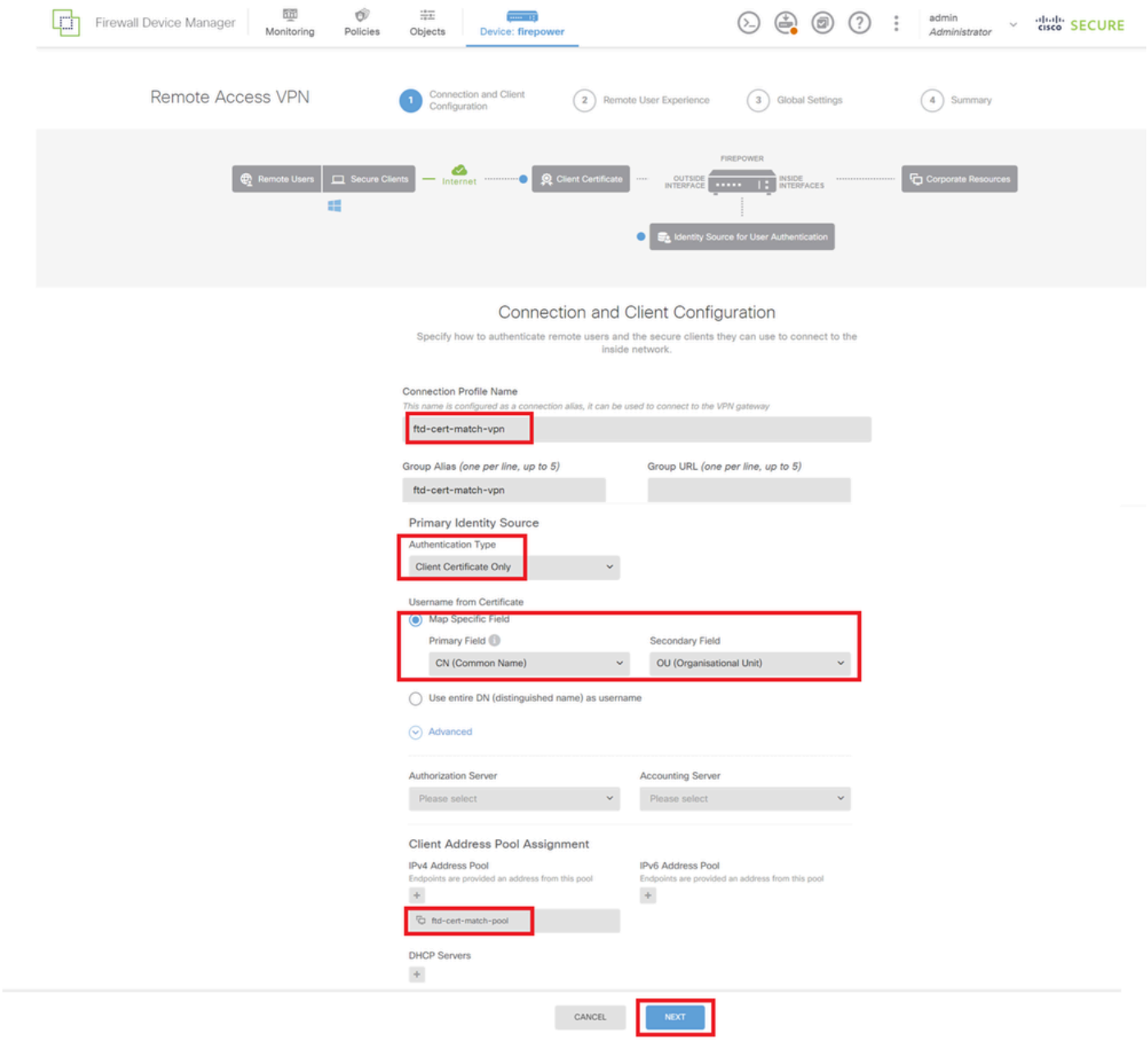
Device(디바이스) > Remote Access VPN(원격 액세스 VPN) > View Configuration(컨피그레이션 보기) > Connection Profiles(연결 프로파일)로 이동하고 CREATE CONNECTION PROFILE(연결 프로파일 생성) 버튼을 클릭합니다.



원격 액세스 VPN 연결 프로파일 추가

연결 프로파일에 필요한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

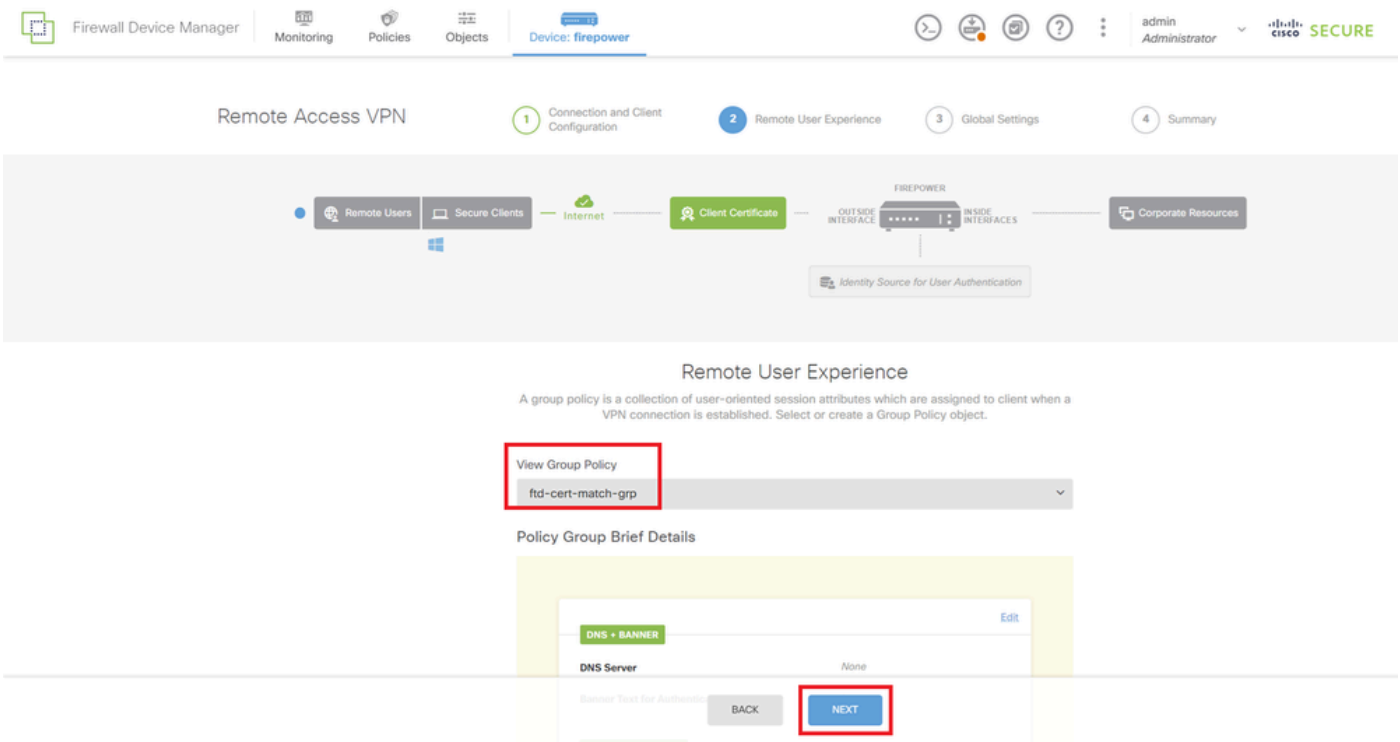
- 연결 프로파일 이름: ftd-cert-match-vpn
- 인증 유형: 클라이언트 인증서 전용
- Username From Certificate(인증서의 사용자 이름): Map specific(맵) 필드
- 기본 필드: CN(Common Name)
- 보조 필드: OU(조직 단위)
- IPv4 주소 풀: ftd-cert-match-pool



VPN 연결 프로파일 세부사항

그룹 정책에 필요한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

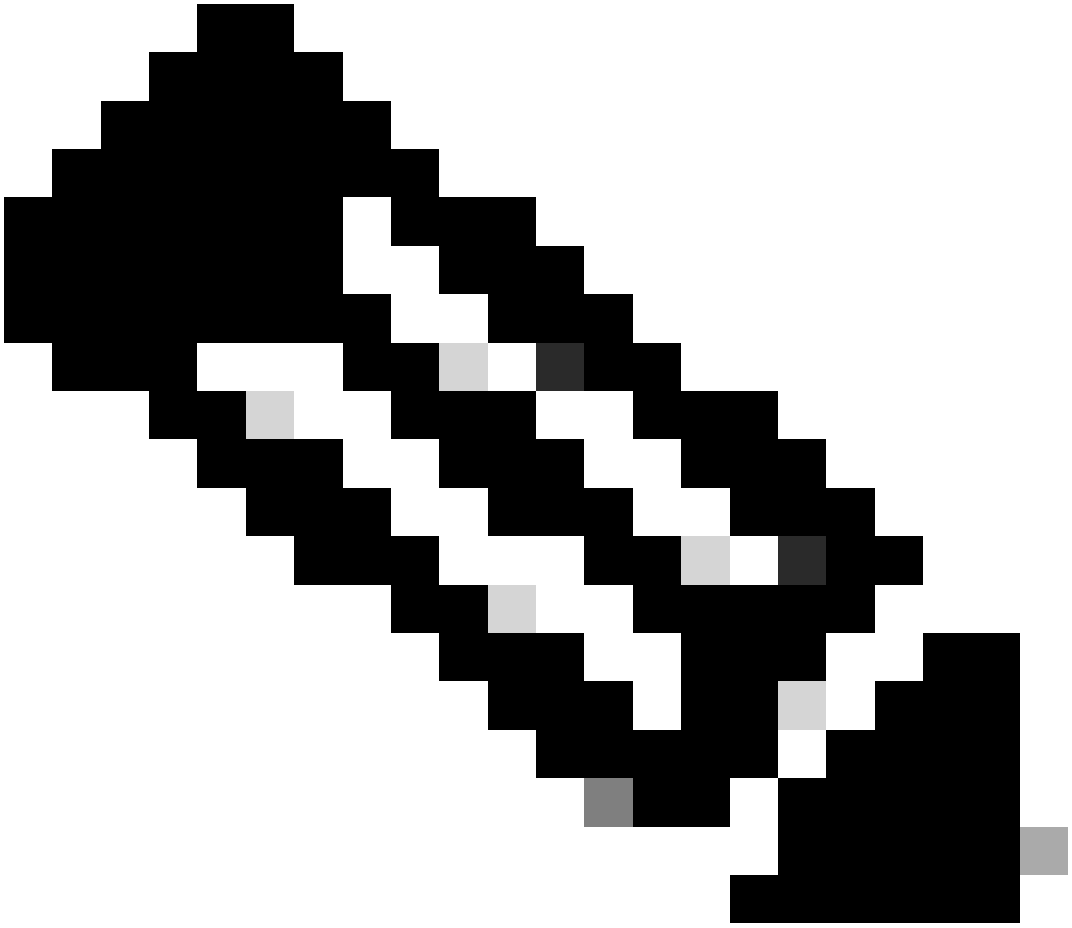
- 그룹 정책 보기: ftd-cert-match-grp



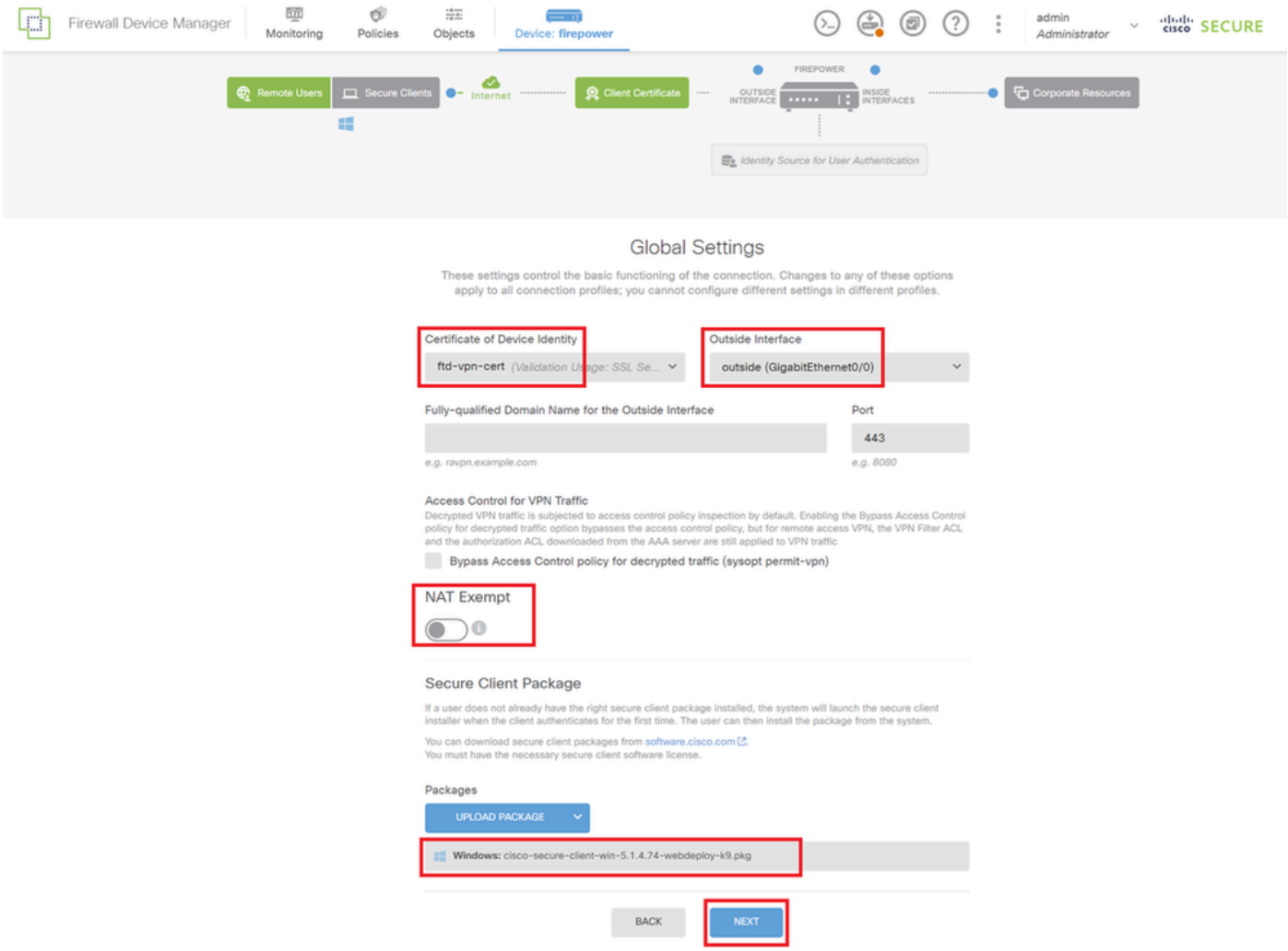
그룹 정책 선택

Certificate of Device Identity(디바이스 ID 인증서), Outside Interface(외부 인터페이스), Secure Client Package for VPN Connection(VPN 연결용 보안 클라이언트 패키지)을 선택합니다.

- Certificate of Device Identity(디바이스 ID 인증서): ftd-vpn-cert
- 외부 인터페이스: 외부(GigabitEthernet0/0)
- 보안 클라이언트 패키지: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



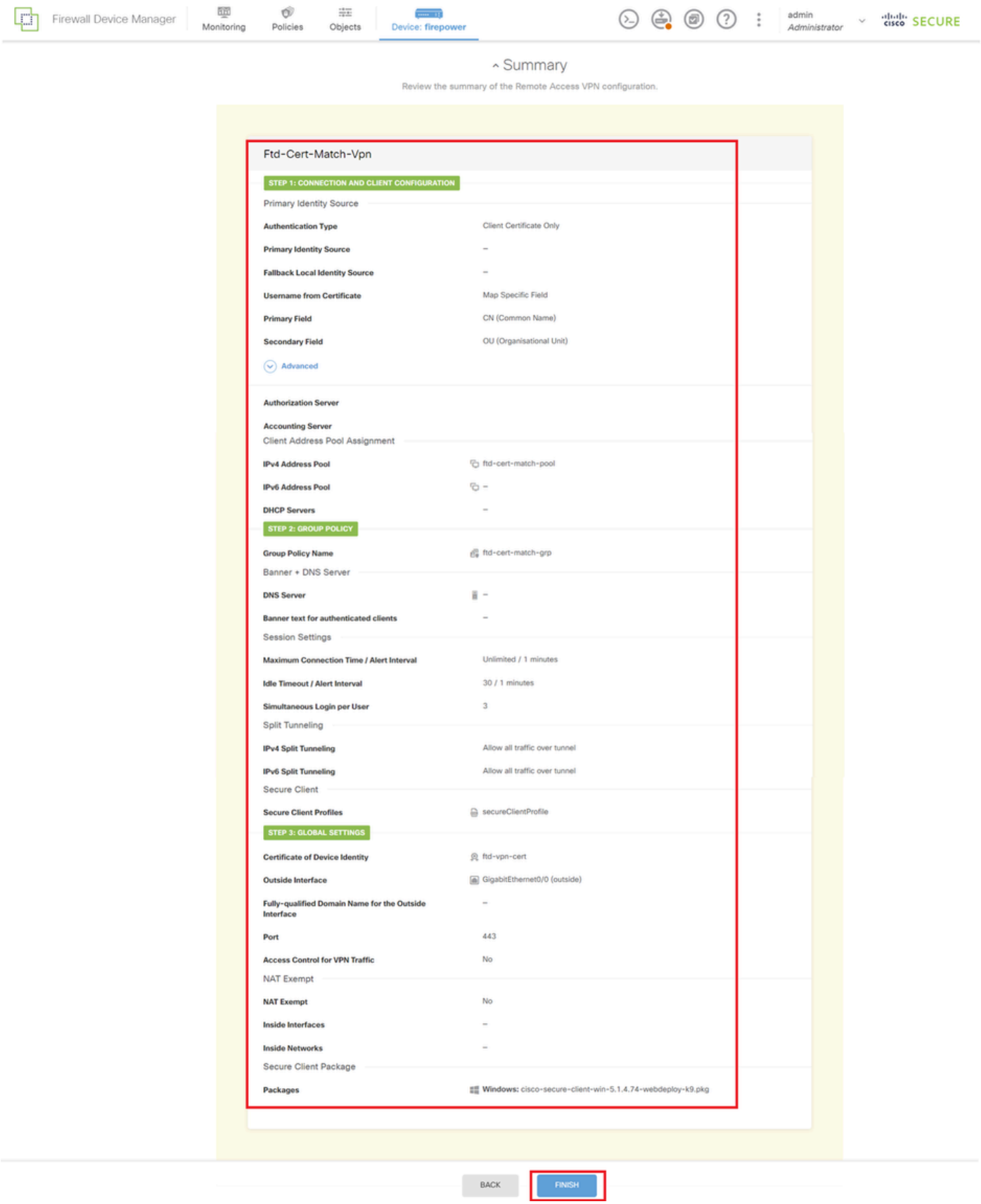
참고: 이 문서에서 NAT 제외 기능을 비활성화했습니다.



전역 설정 세부 정보

10단계. 연결 프로파일에 대한 요약 확인

VPN 연결을 위해 입력한 정보를 확인하고 FINISH(마침) 버튼을 클릭합니다.



연결 프로파일에 대한 요약 확인

FTD CLI에서 확인

FDM에서 구축한 후 FTD CLI에서 VPN 연결 설정을 확인합니다.

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

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

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// 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:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

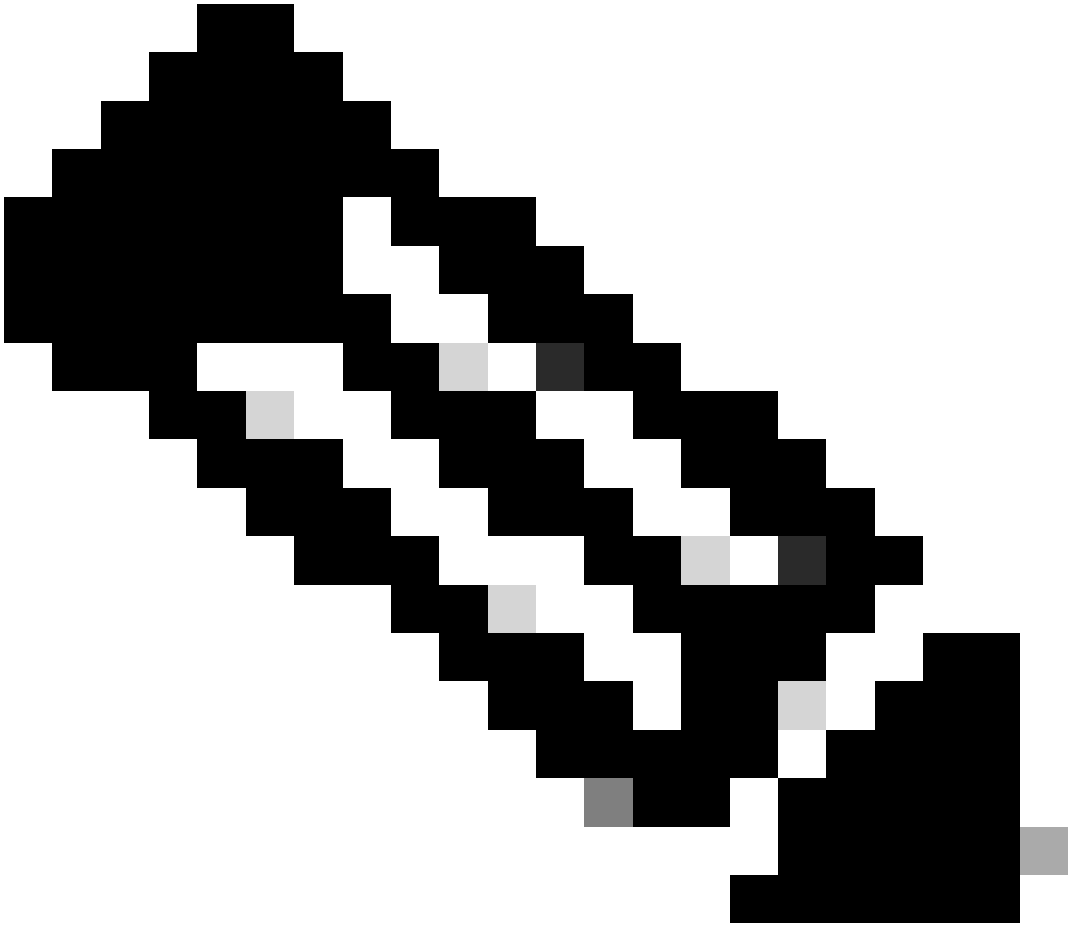
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

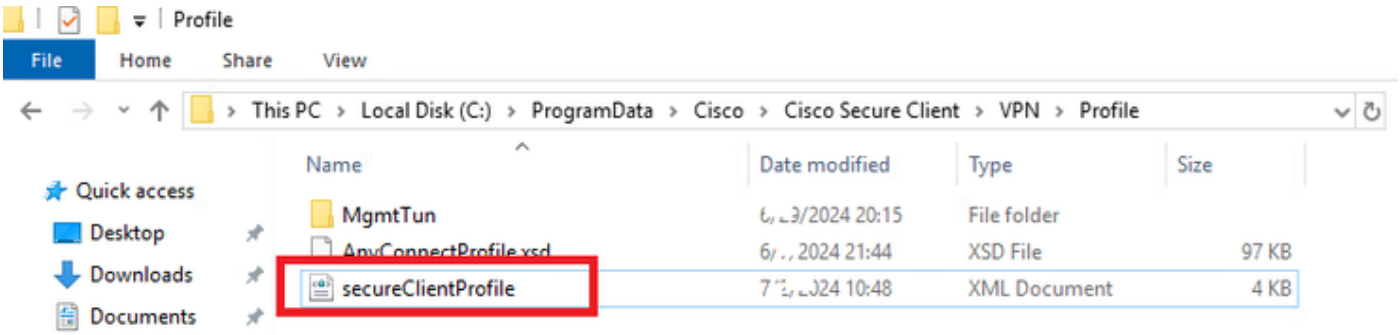
VPN 클라이언트에서 확인

1단계. VPN 클라이언트에 보안 클라이언트 프로파일 복사

VPN 클라이언트 및 관리자 VPN 클라이언트를 엔지니어링하기 위해 보안 클라이언트 프로파일을 복사합니다.



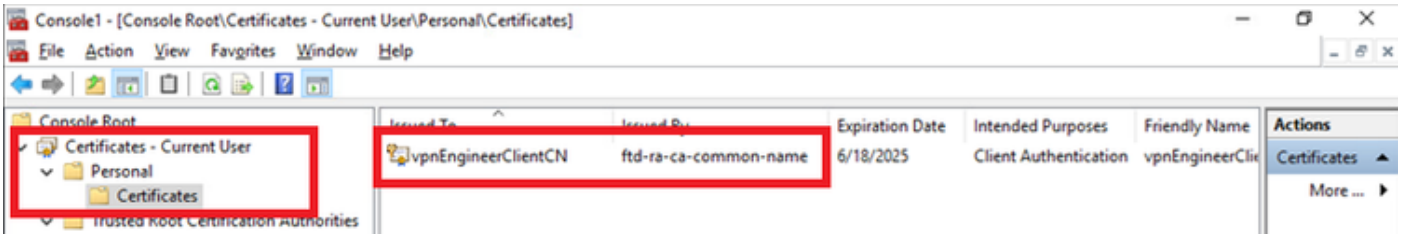
참고: Windows 컴퓨터의 보안 클라이언트 프로파일 디렉터리:
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



VPN 클라이언트에 보안 클라이언트 프로파일 복사

2단계. 클라이언트 인증서 확인

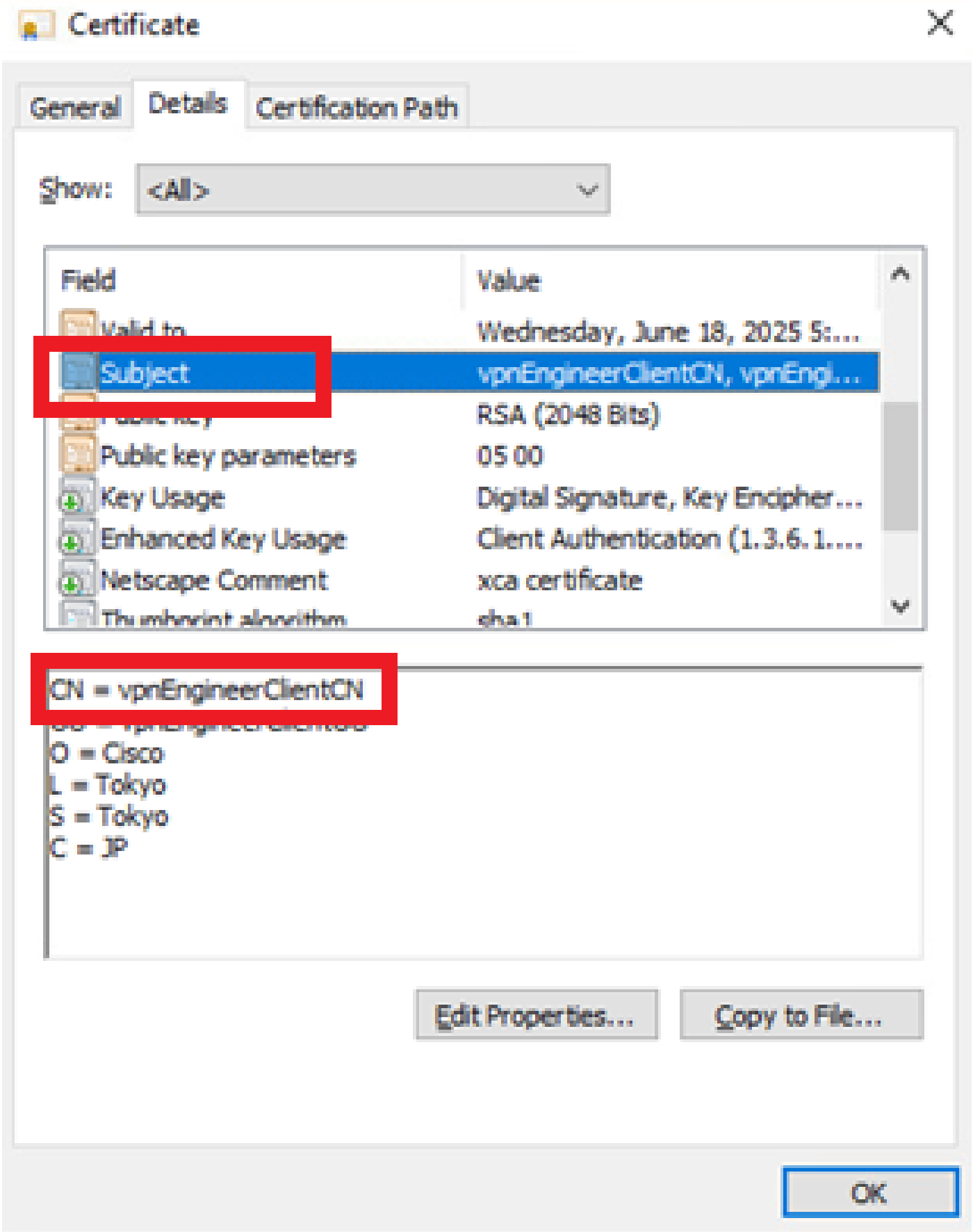
Engineer VPN 클라이언트에서 Certificates(인증서) - Current User(현재 사용자) > Personal(개인) > Certificates(인증서)로 이동하여 인증에 사용된 클라이언트 인증서를 확인합니다.



엔지니어 VPN 클라이언트의 인증서 확인

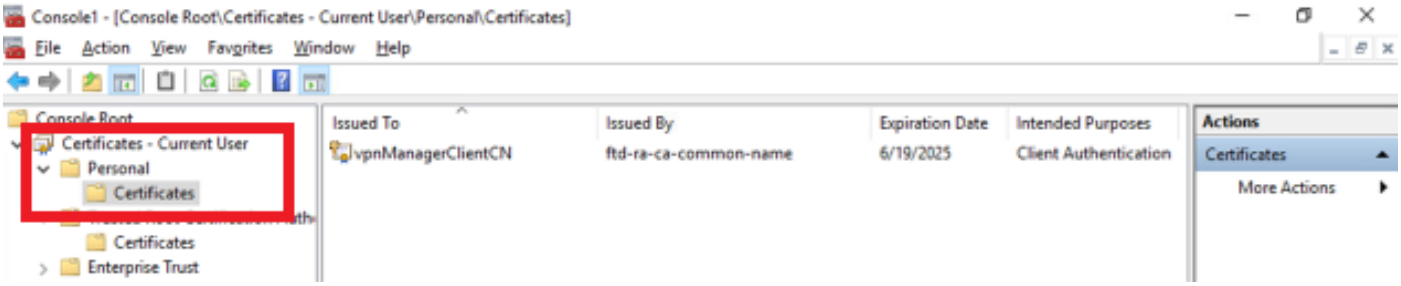
클라이언트 인증서를 두 번 클릭하고 Details(세부사항)로 이동하여 Subject(주체)의 세부사항을 확인합니다.

- 제목: CN = vpnEngineerClientCN



엔지니어 클라이언트 인증서 세부사항

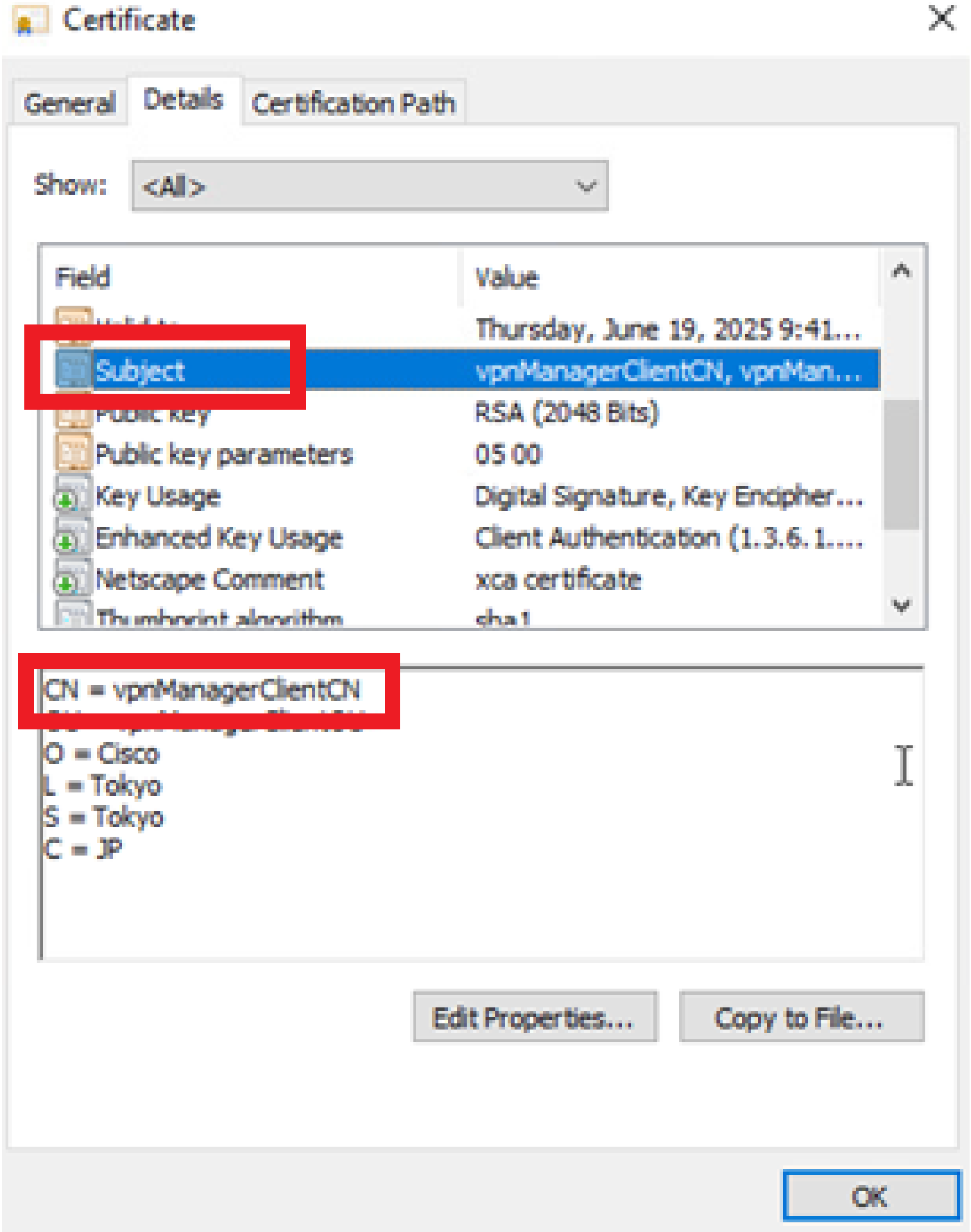
관리자 VPN 클라이언트에서 Certificates - Current User > Personal > Certificates로 이동하여 인증에 사용된 클라이언트 인증서를 확인합니다.



관리자 VPN 클라이언트에 대한 인증서 확인

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

- 제목: CN = vpnManagerClientCN

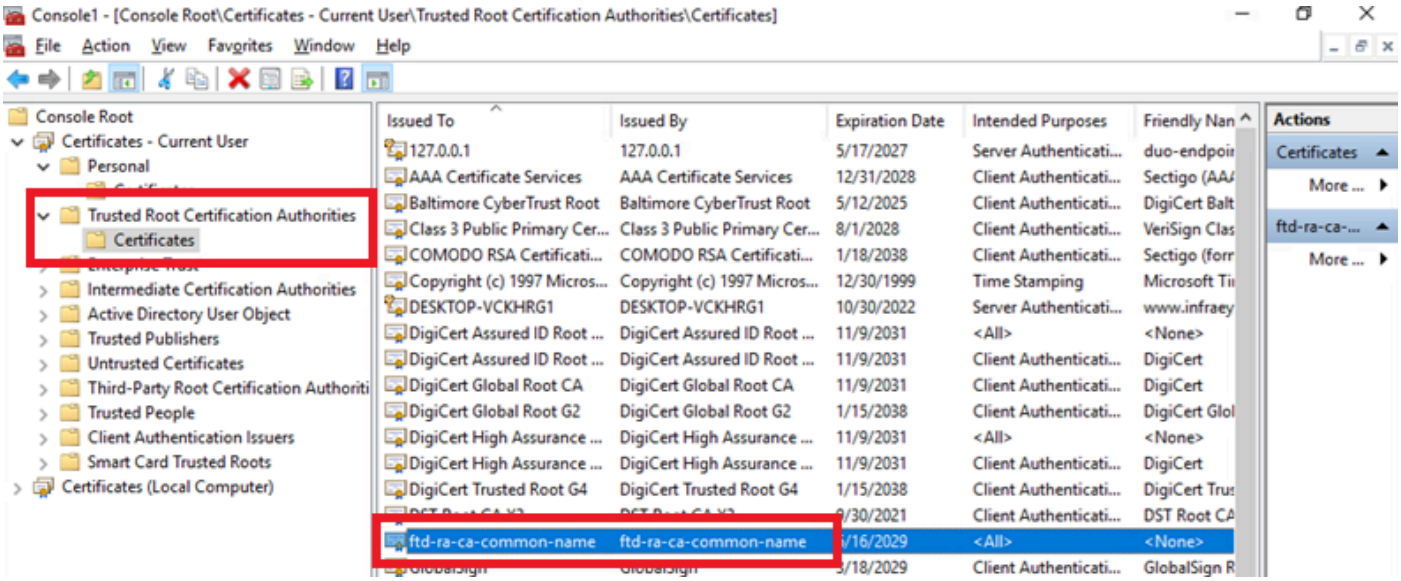


관리자 클라이언트 인증서 세부 정보

3단계. CA 확인

Engineer VPN client(엔지니어 VPN 클라이언트) 및 manager VPN client(관리자 VPN 클라이언트)에서 Certificates(인증서) - Current User(현재 사용자) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(인증서)로 이동하여 인증에 사용된 CA를 확인합니다.

- 발급자: ftd-ra-ca-common-name



CA 확인

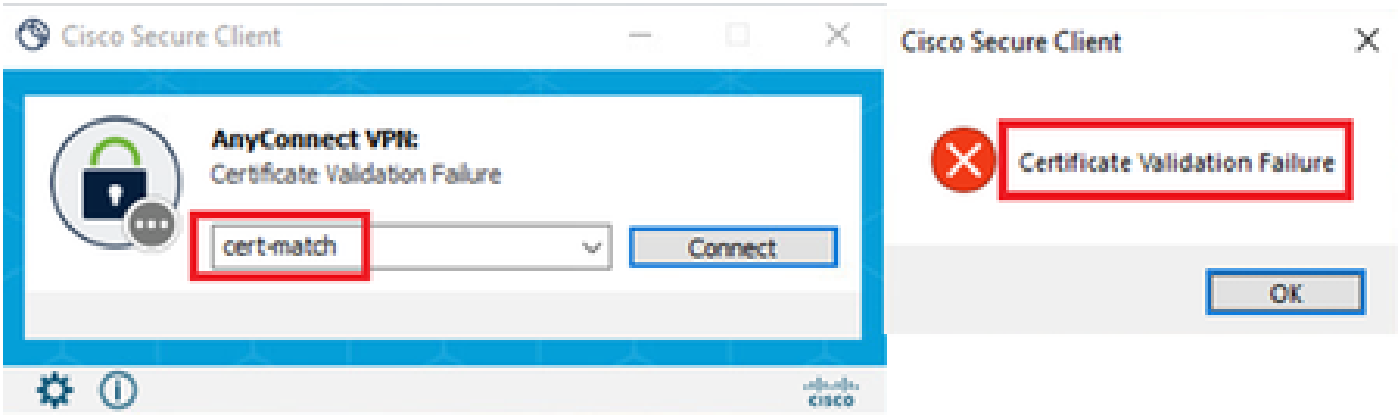
다음을 확인합니다.

1단계. VPN 연결 시작

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

엔지니어 VPN 클라이언트에 대한 VPN 연결 성공

관리자 VPN 클라이언트에서 Cisco Secure Client 연결을 시작합니다. 인증서 유효성 검사 실패로 인해 연결된 VPN이 실패했습니다.



관리자 VPN 클라이언트에 대한 VPN 연결 실패

2단계. FTD CLI에서 VPN 세션 확인

FTD(Lina) CLI에서 명령을 실행하여 엔지니어의 VPN 세션을 확인합니다show vpn-sessiondb detail anyconnect.

```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000000200006683932b
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
```

Bytes Tx : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 32.2
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 50177
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 12919
Pkts Tx : 1 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0

문제 해결

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

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

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClie
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

관련 정보

[firepower 2100에 대한 FDM On-Box Management Service 구성]
[FDM에서 관리하는 FTD에 원격 액세스 VPN 구성]
[firepower 장치 관리자에서 Syslog 구성 및 확인]

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.