FMC를 통해 FTD에서 보안 클라이언트에 대한 AAA 및 인증서 인증 구성

목차

소개

이 문서에서는 FMC에서 AAA 및 인증서 인증을 사용하여 관리하는 FTD에서 SSL을 통한 Cisco Secure Client를 구성하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firepower 관리 센터)
- 방화벽 FTD(Threat Defense Virtual)
- 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

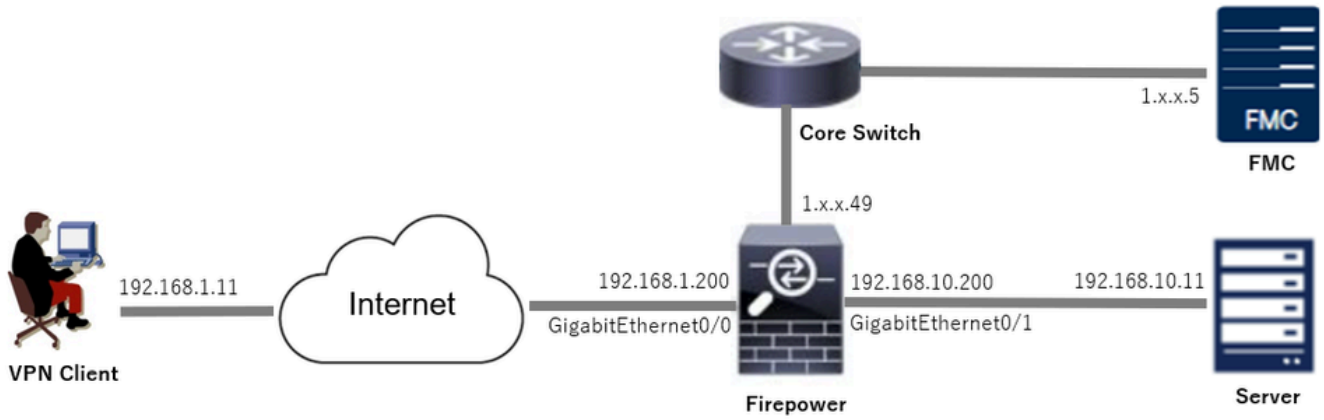
조직에서 더욱 엄격한 보안 조치를 채택함에 따라 2FA(Two-Factor Authentication)와 인증서 기반 인증을 결합하는 것이 보안을 강화하고 무단 액세스를 차단하는 일반적인 관행이 되었습니다. 사용자 경험 및 보안을 크게 개선할 수 있는 기능 중 하나는 Cisco Secure Client에서 사용자 이름을 미리 채우는 기능입니다. 이 기능은 로그인 프로세스를 간소화하고 원격 액세스의 전반적인 효율성을 향상시킵니다.
이 문서에서는 미리 채워진 사용자 이름을 FTD의 Cisco Secure Client와 통합하여 사용자가 빠르고 안전하게 네트워크에 연결하는 방법에 대해 설명합니다.

이러한 인증서는 권한 부여 목적으로 사용되는 공통 이름을 포함합니다.

- CA: ftd-ra-ca-common-name
- 클라이언트 인증서: sslVPNClientCN
- 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

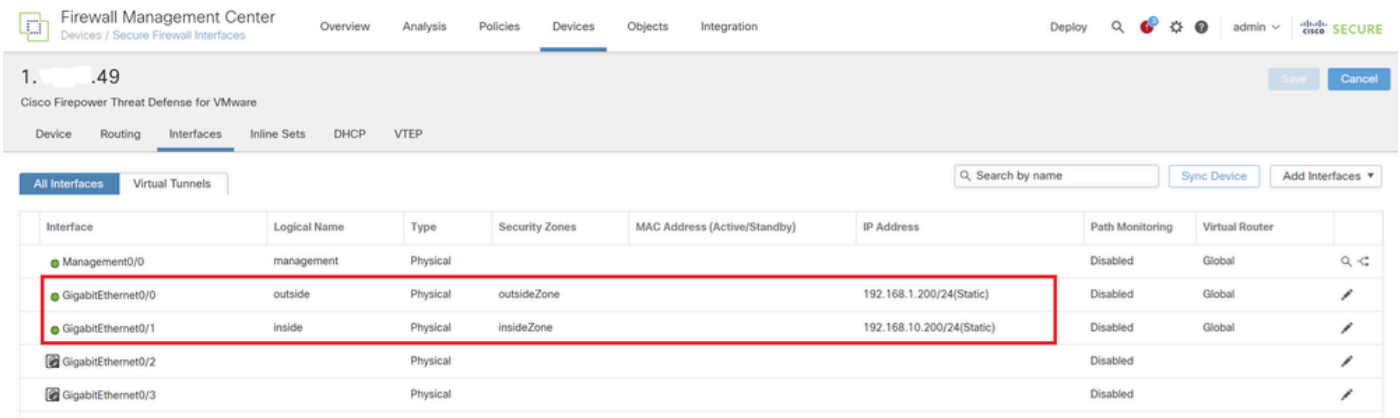
Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 Interfaces(인터페이스) 탭에서 대상 FTD 디바이스, config inside and outside interface for FTD(FTD에 대한 인터페이스 내부 및 외부 인터페이스)를 수정합니다.

GigabitEthernet0/0,

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

GigabitEthernet0/1,

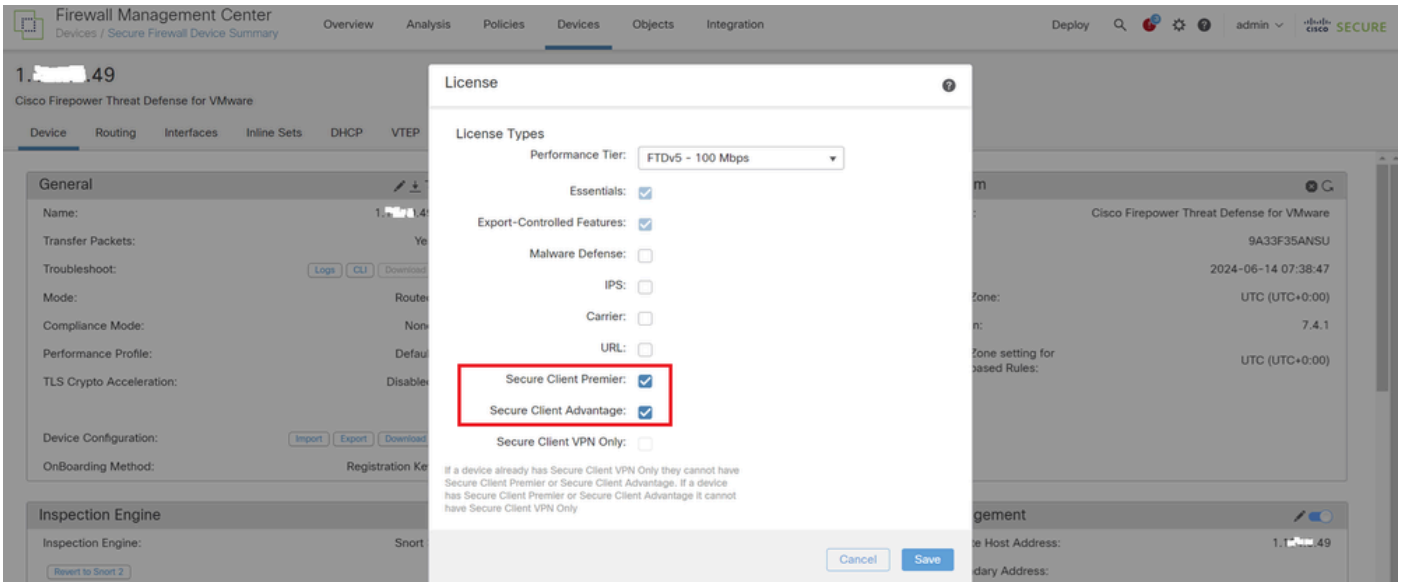
- 이름: inside
- 보안 영역: insideZone
- IP 주소: 192.168.10.200/24



FTD 인터페이스

2단계. Cisco Secure Client 라이센스 확인

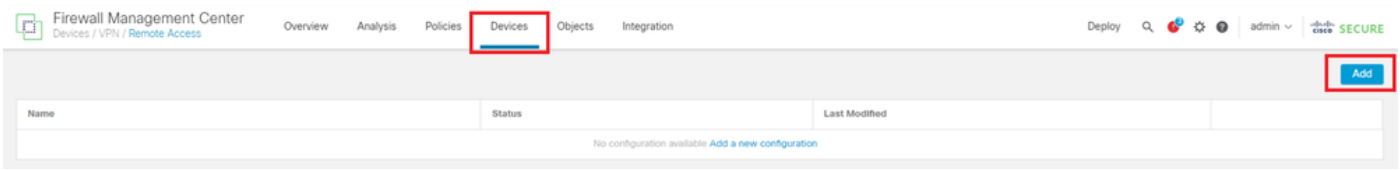
Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 대상 FTD 디바이스를 편집하고 Device(디바이스) 탭에서 Cisco Secure Client 라이센스를 확인합니다.



Secure Client 라이센스

3단계. 정책 할당 추가

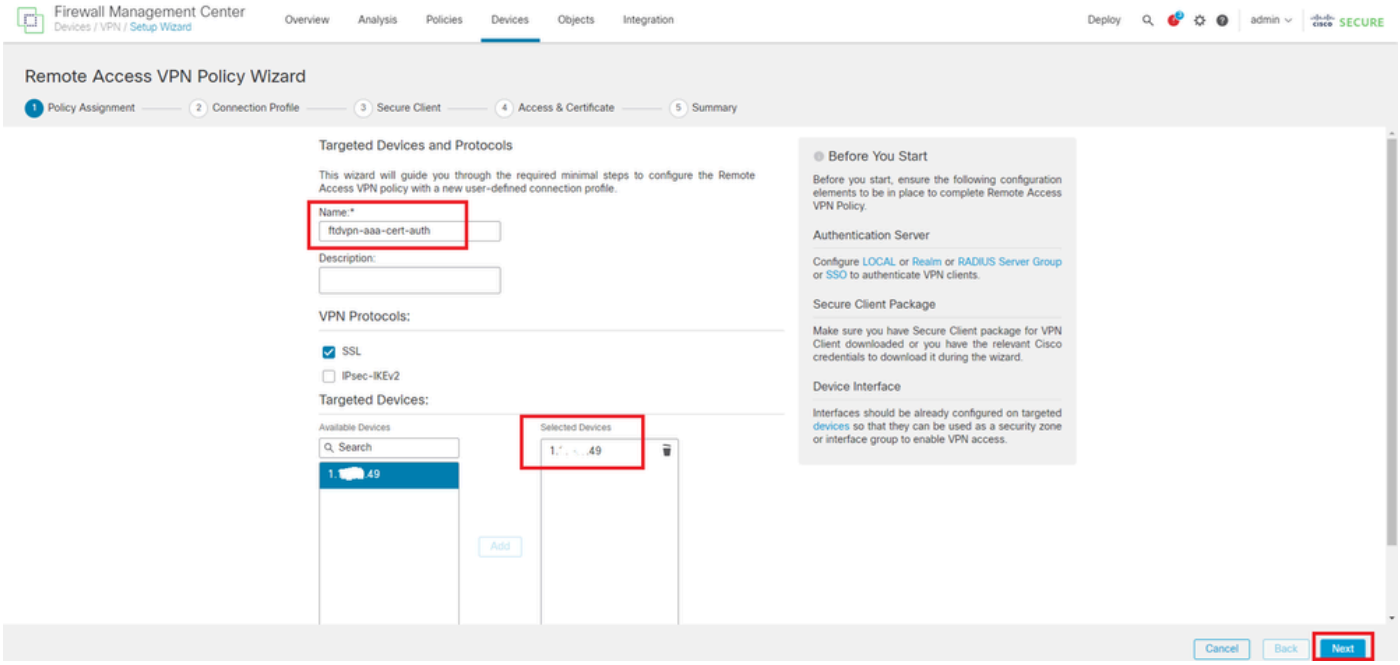
Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하고 Add(추가) 버튼을 클릭합니다.



원격 액세스 VPN 추가

필요한 정보를 입력하고 Next(다음) 버튼을 클릭합니다.

- 이름: ftdvpn-aaa-cert-auth
- VPN 프로토콜: SSL
- 대상 장치: 1.x.x.49

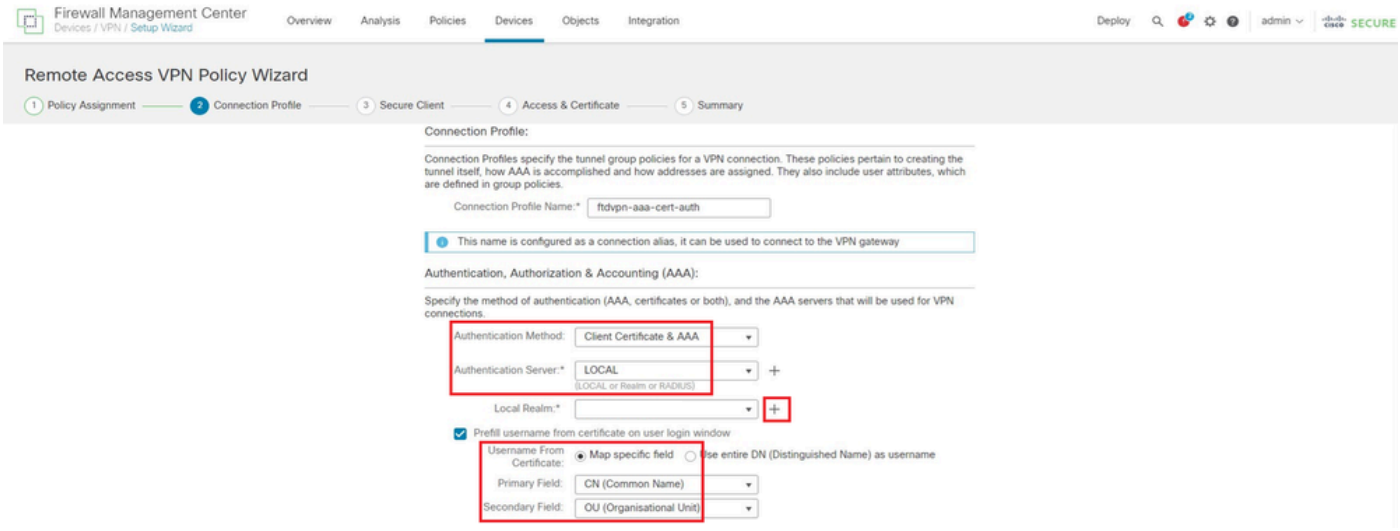


정책 할당

4단계. 연결 프로파일에 대한 컨피그레이션 세부사항

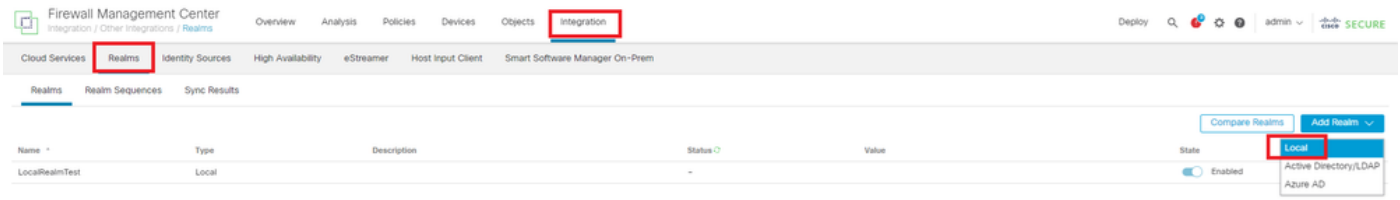
연결 프로파일에 필요한 정보를 입력하고 로컬 영역 항목 옆에 있는 + 버튼을 클릭합니다.

- 인증 방법 : 클라이언트 인증서 및 AAA
- 인증 서버: LOCAL
- Username From Certificate(인증서의 사용자 이름): Map specific(맵) 필드
- 기본 필드: CN(공통 이름)
- 보조 필드: OU(조직 단위)



연결 프로파일 세부사항

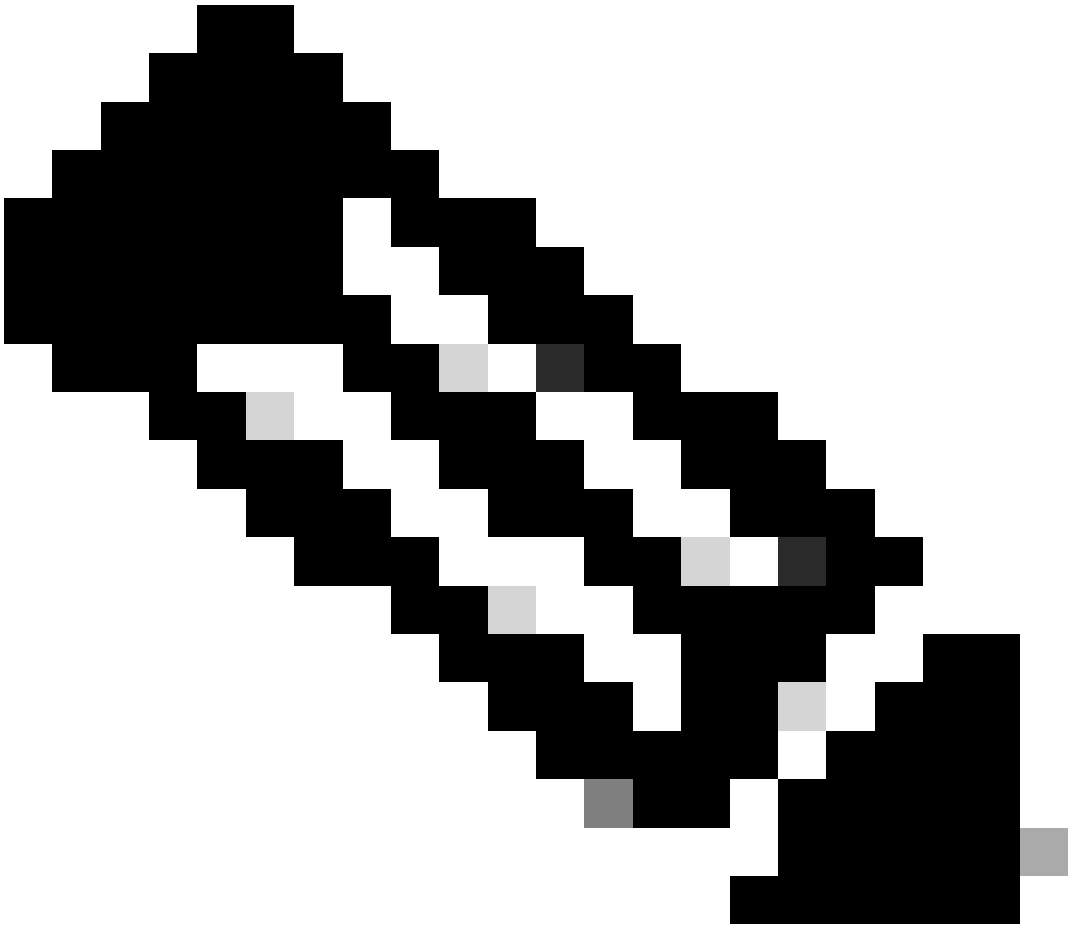
Add Realm(영역 추가) 드롭다운 목록에서 Local(로컬)을 클릭하여 새 로컬 영역을 추가합니다.



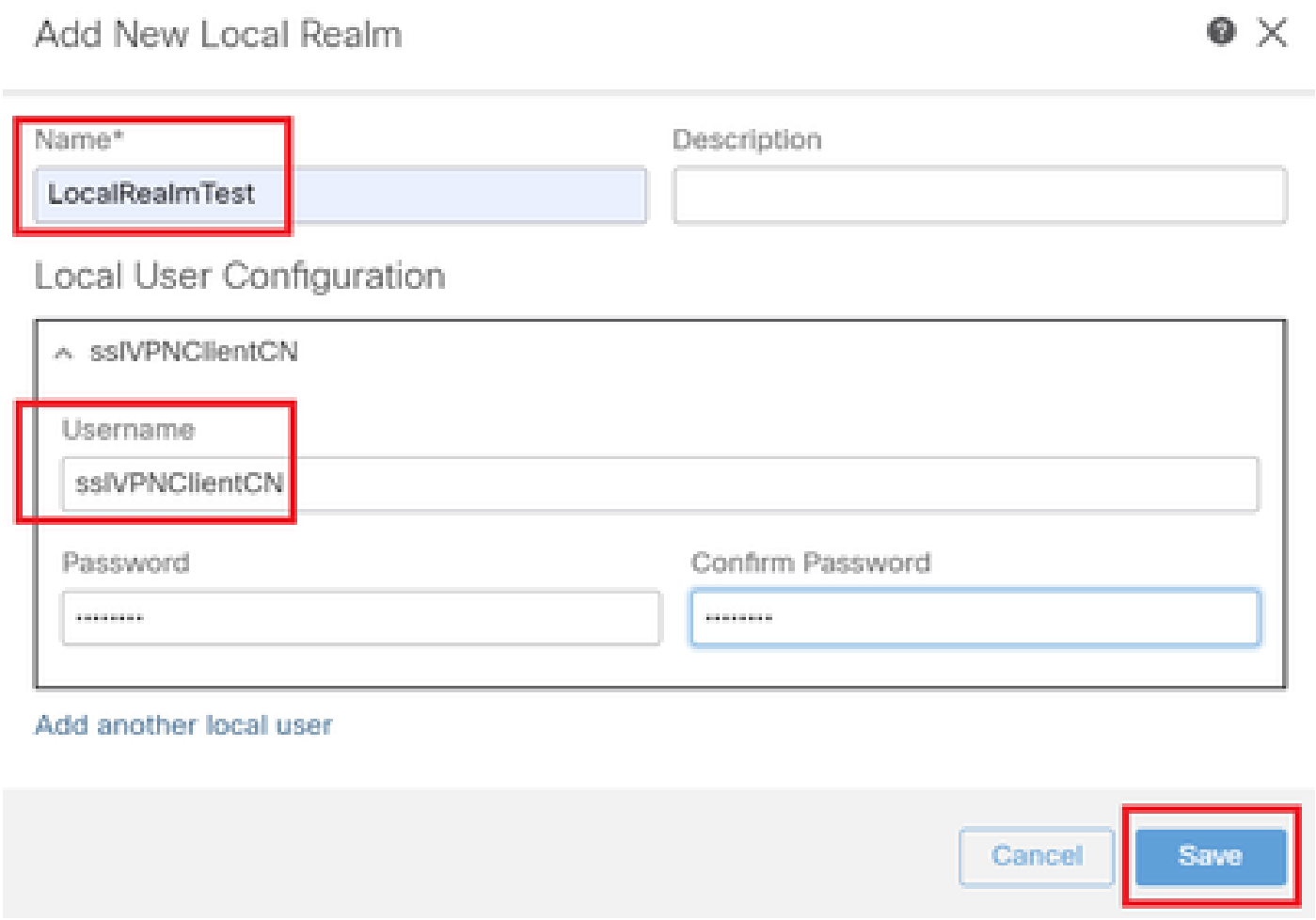
로컬 영역 추가

로컬 영역에 필요한 정보를 입력하고 Save(저장) 버튼을 클릭합니다.

- 이름: LocalRealmTest
- 사용자 이름: sslVPNClientCN



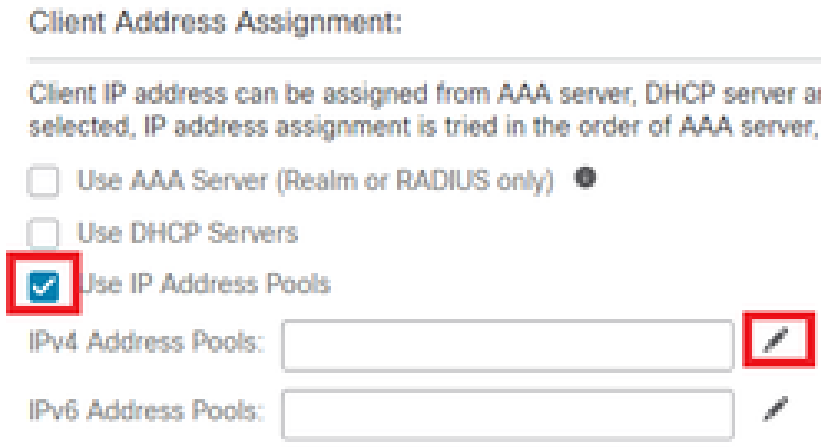
참고: 사용자 이름은 클라이언트 인증서 내의 공통 이름과 같습니다



로컬 영역 세부 정보

5단계. 연결 프로파일에 대한 주소 풀 추가

IPv4 Address Pools(IPv4 주소 풀) 항목 옆에 있는 edit(수정) 버튼을 클릭합니다.

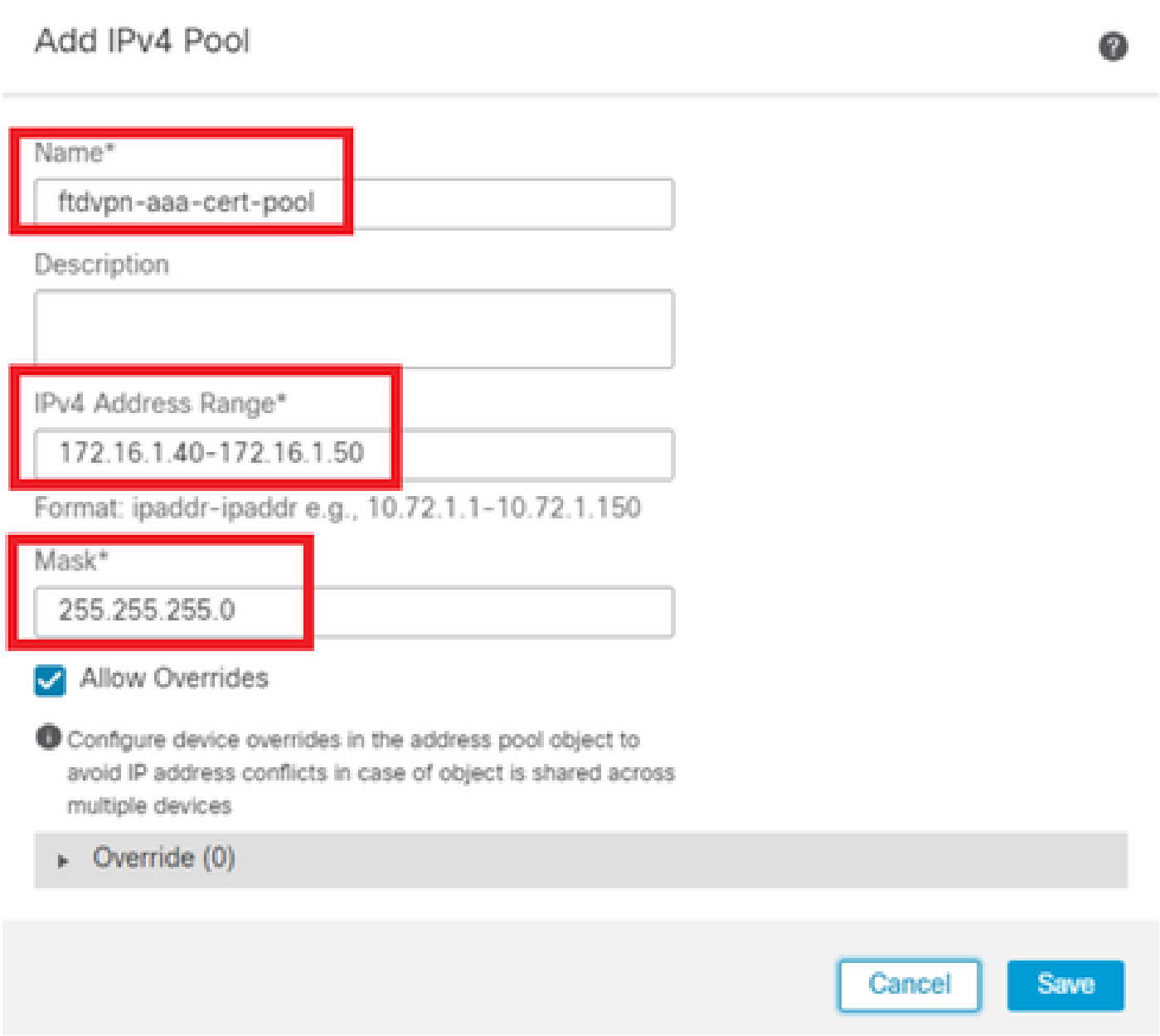


IPv4 주소 풀 추가

새 IPv4 주소 풀을 추가하는 데 필요한 정보를 입력합니다. 연결 프로파일에 대한 새 IPv4 주소 풀을 선택합니다.

- 이름: ftdvpn-aaa-cert-pool
- IPv4 주소 범위: 172.16.1.40-172.16.1.50

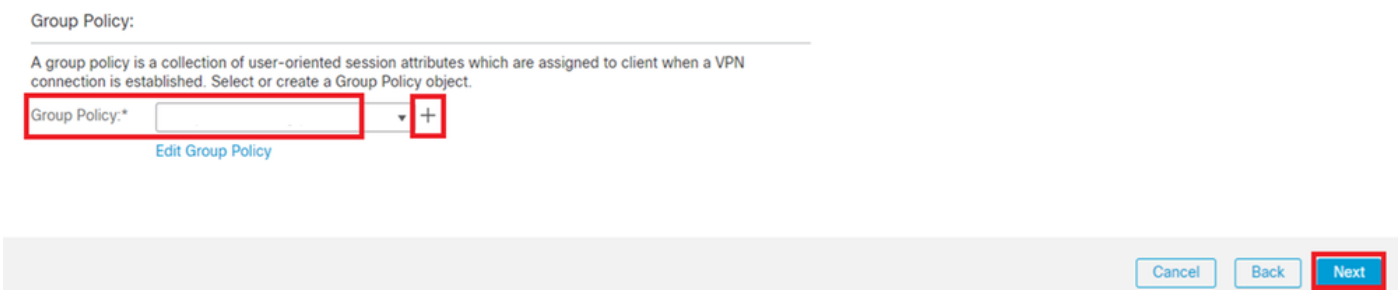
- 마스크 : 255.255.255.0



IPv4 주소 풀 세부 정보

6단계. 연결 프로파일에 대한 그룹 정책 추가

그룹 정책 항목 옆에 있는 + 단추를 클릭합니다.

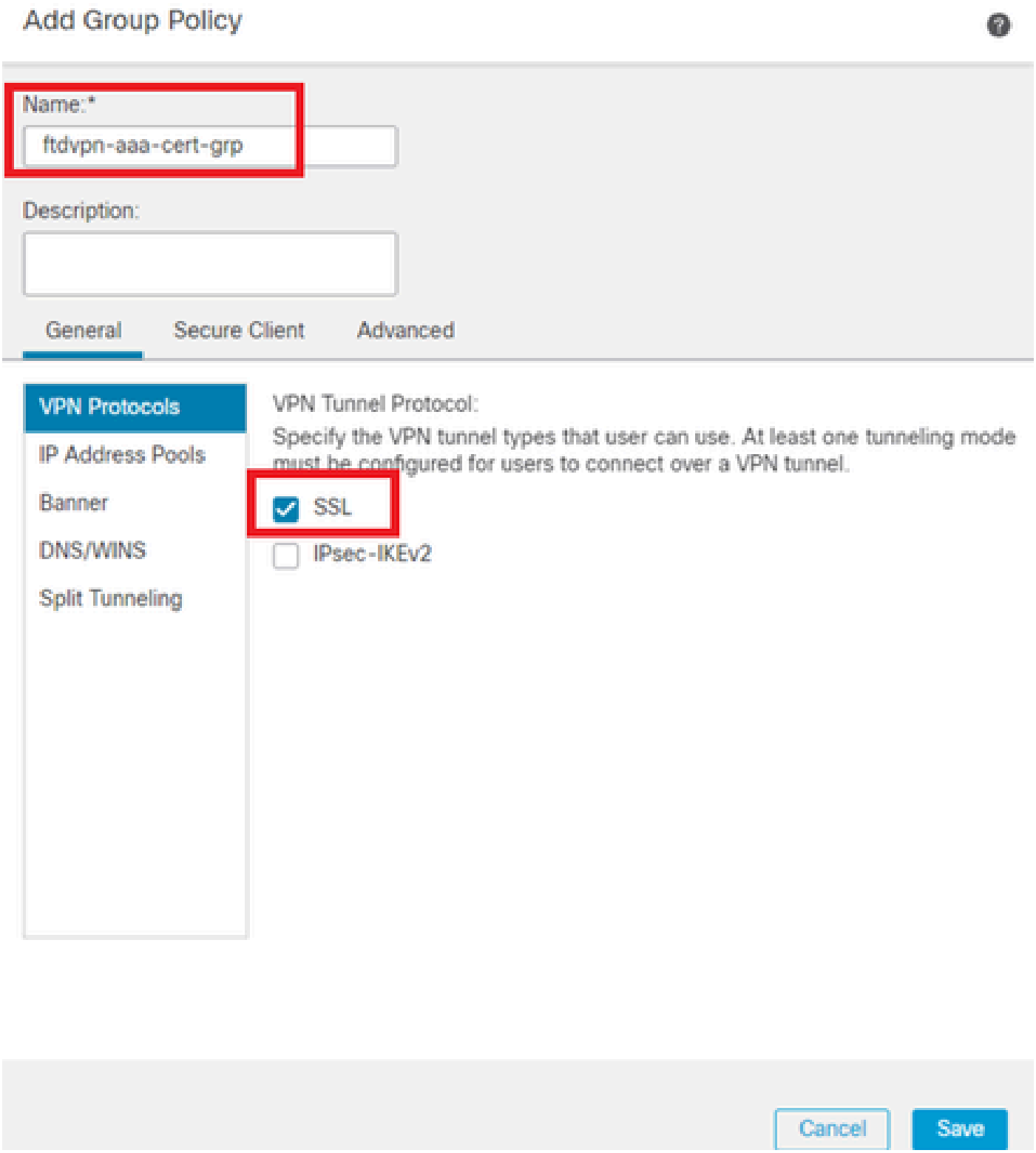


그룹 정책 추가

새 그룹 정책을 추가하는 데 필요한 정보를 입력합니다. 연결 프로파일에 대한 새 그룹 정책을 선택

합니다.

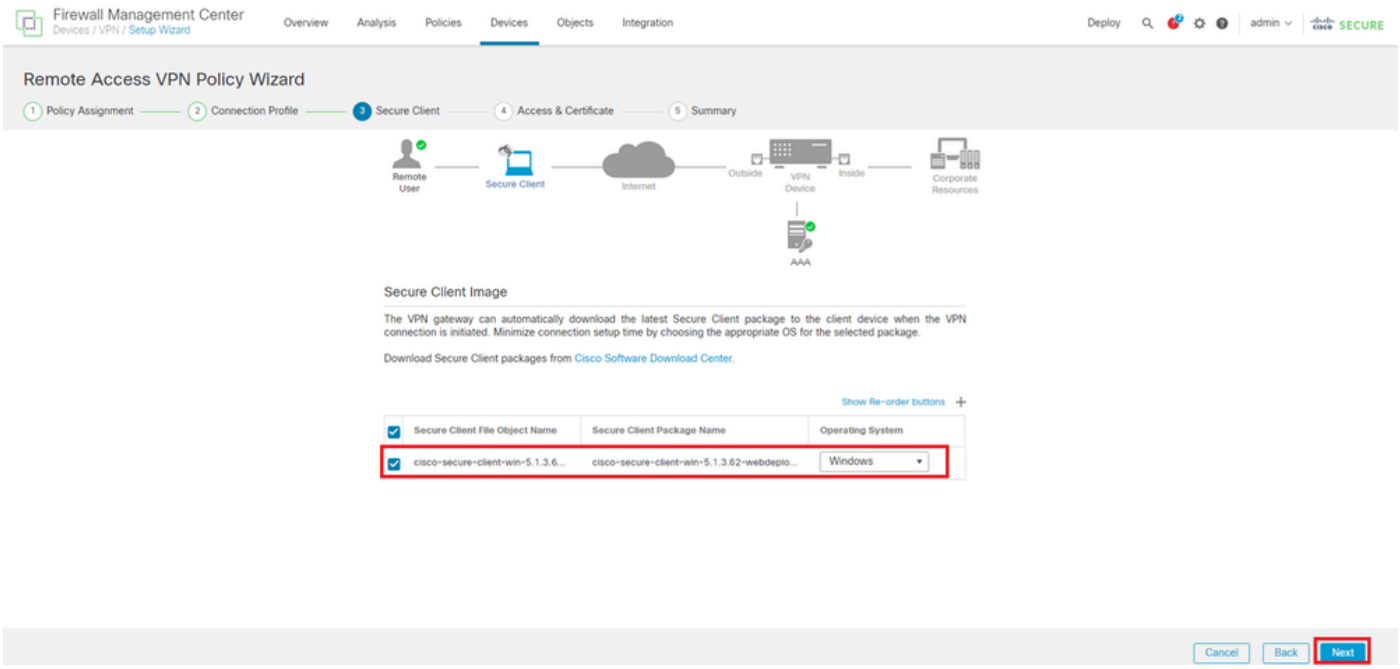
- 이름: ftdvpn-aaa-cert-grp
- VPN 프로토콜: SSL



그룹 정책 세부 정보

7단계. 연결 프로파일에 대한 보안 클라이언트 이미지 구성

보안 클라이언트 이미지 파일을 선택하고 Next(다음) 버튼을 클릭합니다.

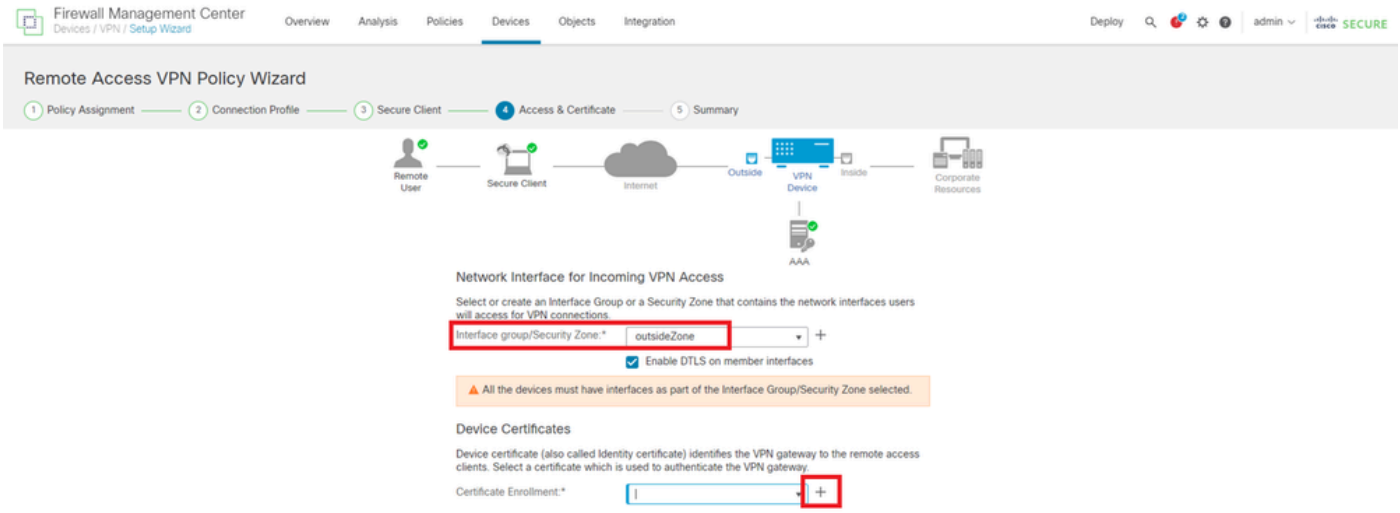


Secure Client Image(보안 클라이언트 이미지) 선택

8단계. 연결 프로파일용 컨피그레이션 액세스 및 인증서

VPN 연결을 위한 보안 영역을 선택하고 인증서 등록 항목 옆에 있는 + 버튼을 클릭합니다.

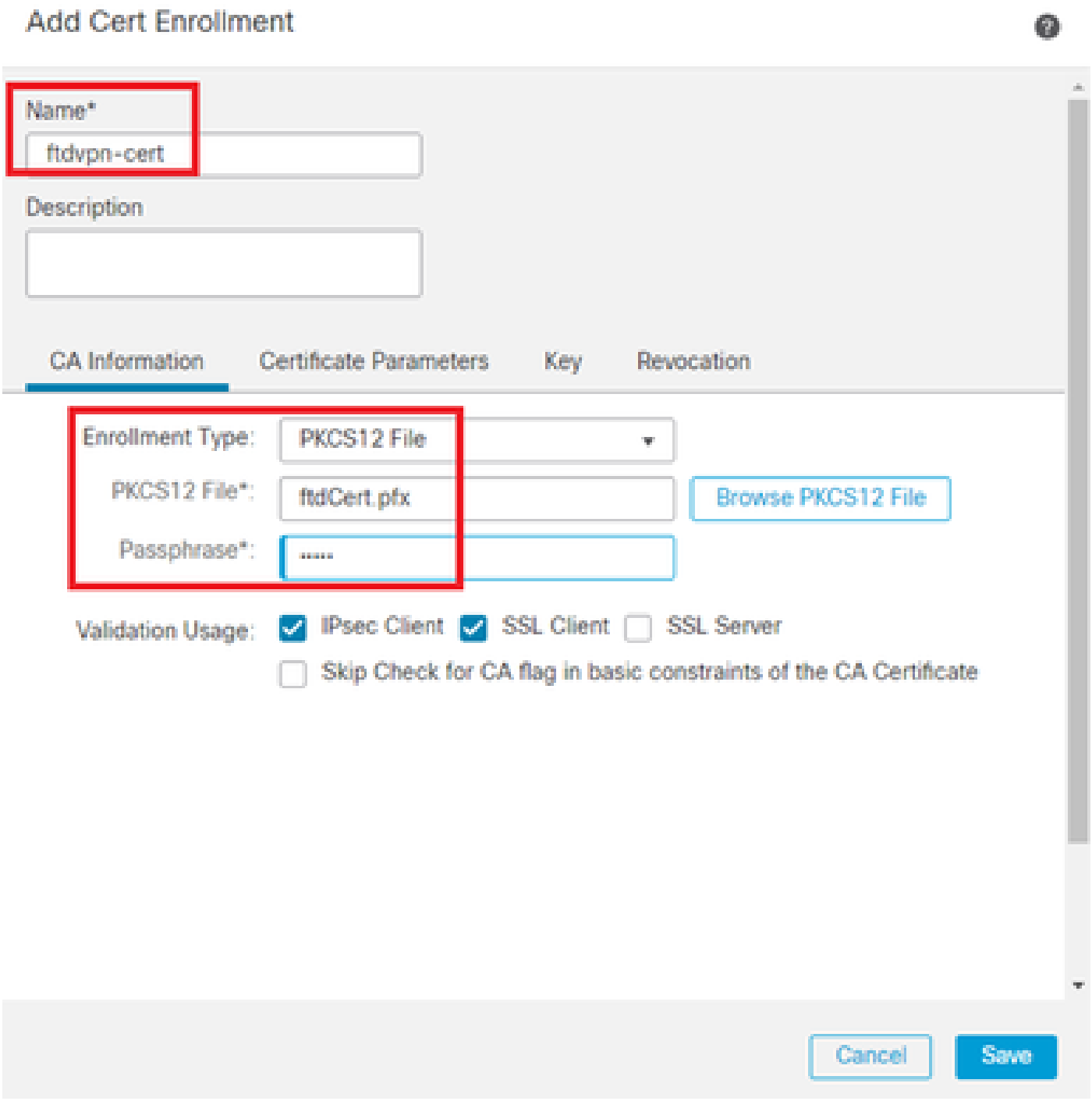
- 인터페이스 그룹/보안 영역: outsideZone



보안 영역 선택

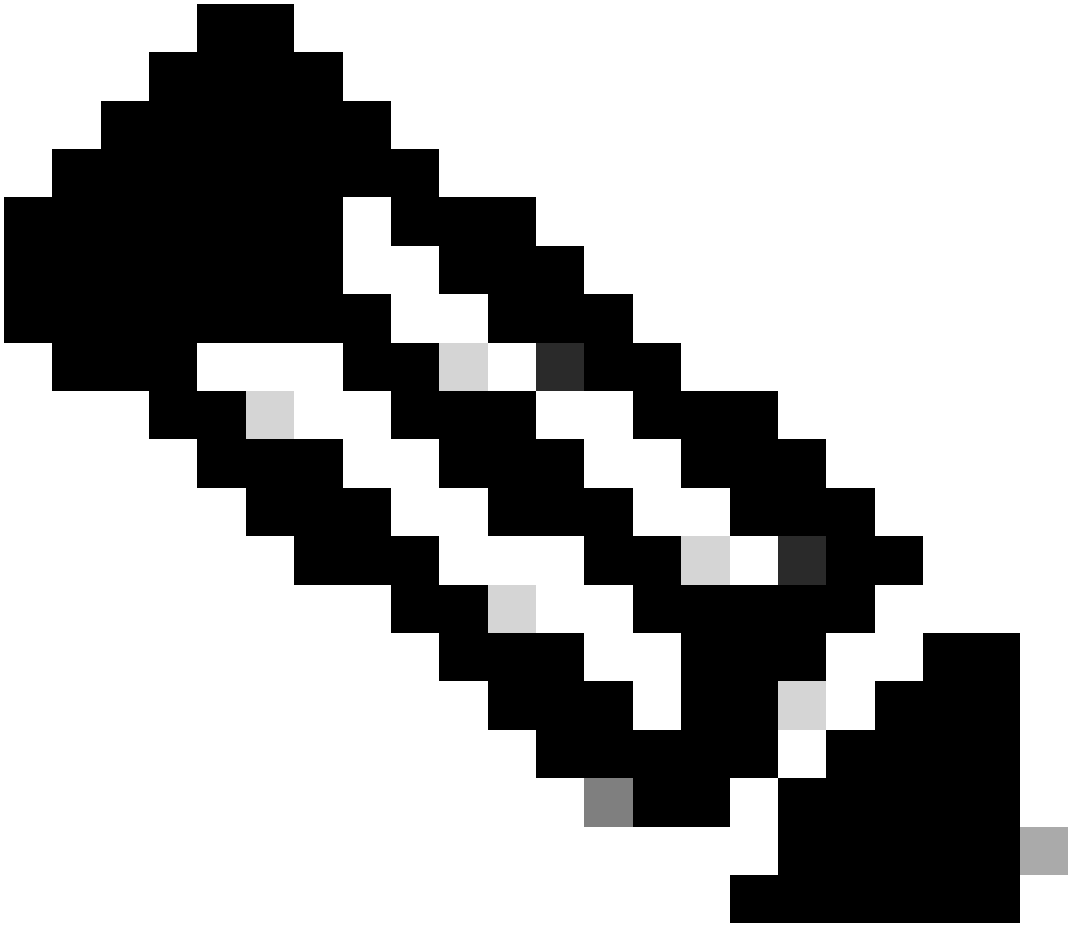
FTD 인증서에 필요한 정보를 입력하고 로컬 컴퓨터에서 PKCS12 파일을 가져옵니다.

- 이름: ftdvpn-cert
- 등록 유형: PKCS12 파일

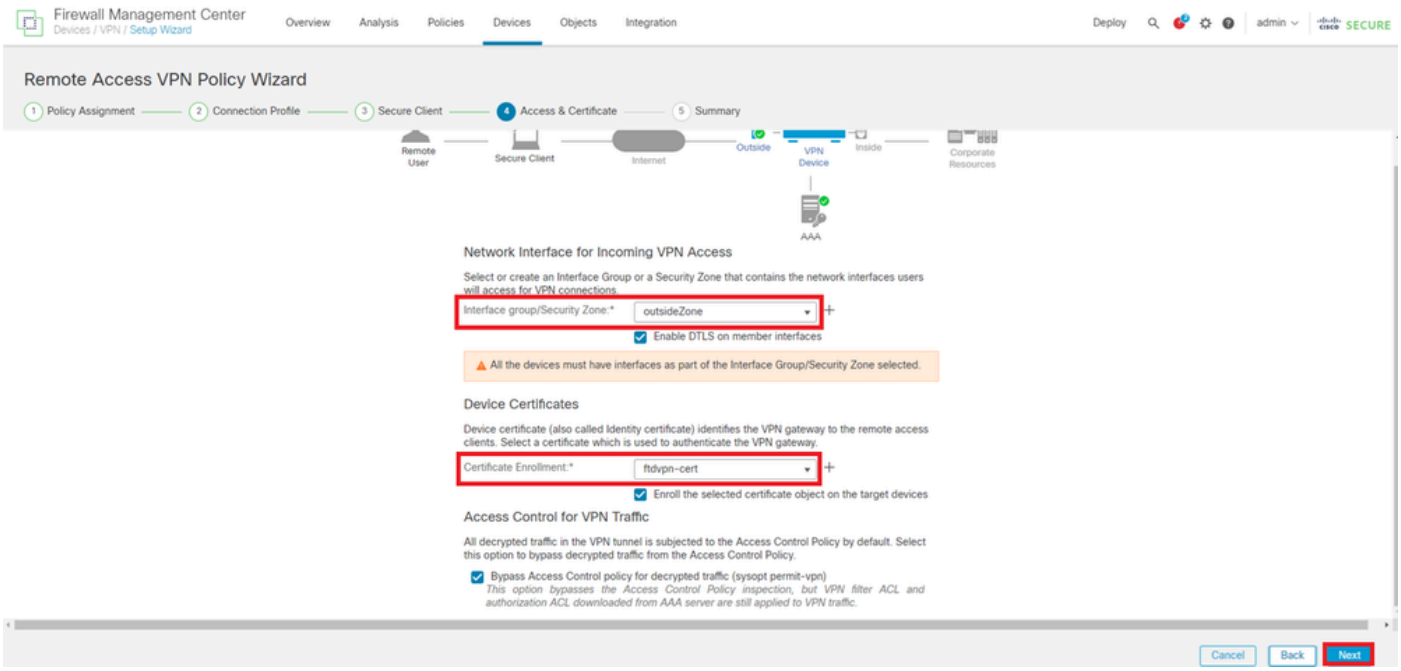


FTD 인증서 추가

Access & Certificate(액세스 및 인증서) 마법사에서 입력한 정보를 확인하고 Next(다음) 버튼을 클릭합니다.



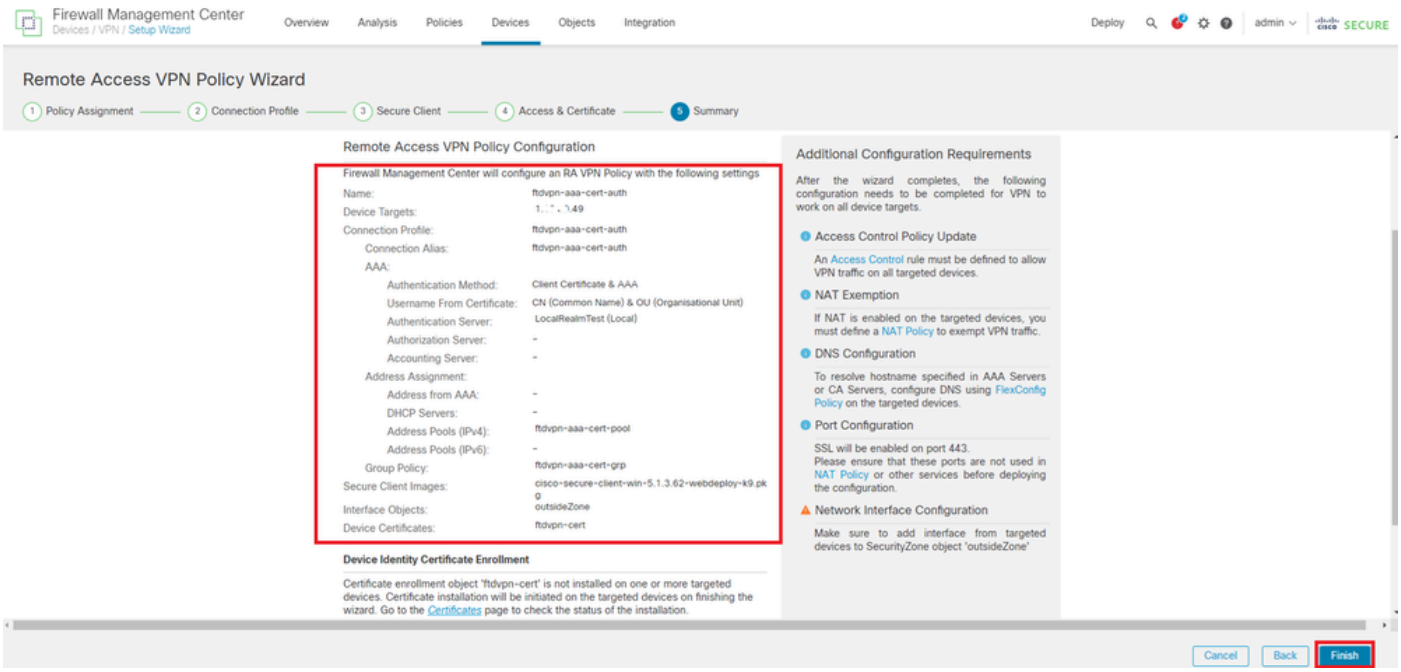
참고: 암호 해독된 VPN 트래픽이 액세스 제어 정책 검사를 받지 않도록 암호 해독된 트래픽에 대해 Bypass Access Control 정책을 활성화합니다(sysopt permit-vpn).



액세스 및 인증서의 설정 확인

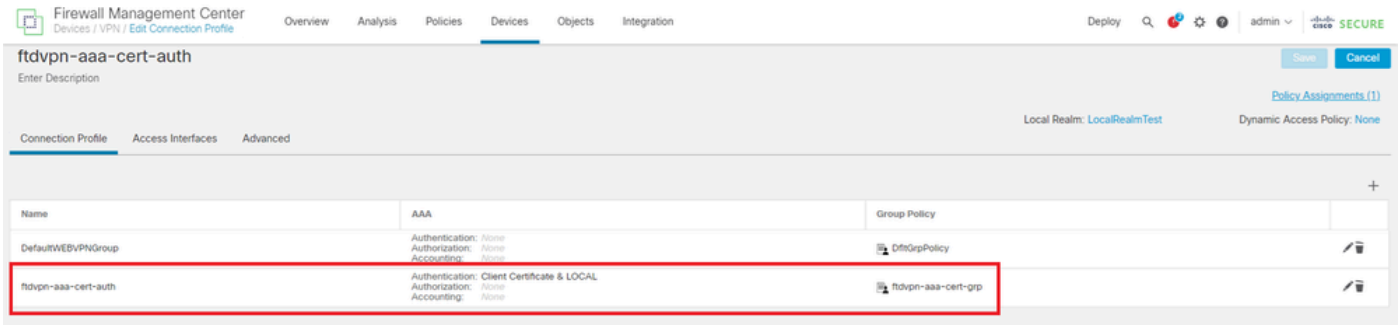
9단계. 연결 프로파일에 대한 요약 확인

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



VPN 연결 설정 확인

원격 액세스 VPN 정책의 요약을 확인하고 FTD에 설정을 구축합니다.



원격 액세스 VPN 정책 요약

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
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0

// Defines a local user
username sslVPNClientCN password ***** encrypted

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

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

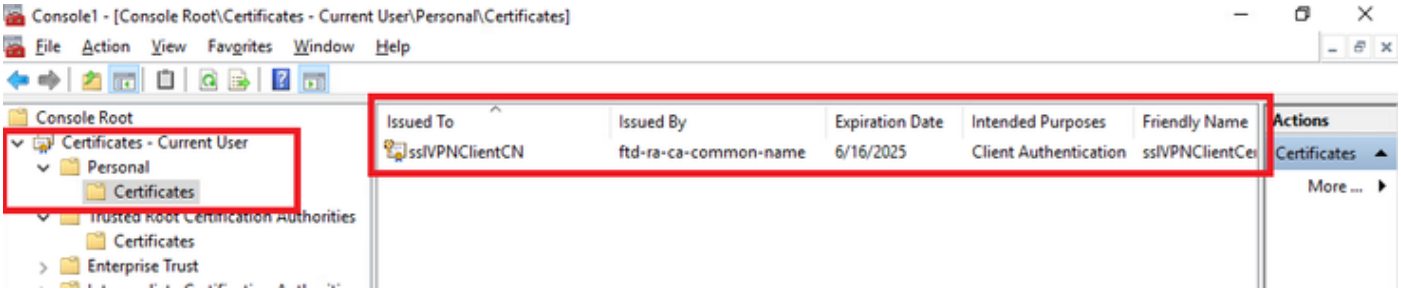
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-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 aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

```
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

VPN 클라이언트에서 확인

1단계. 클라이언트 인증서 확인

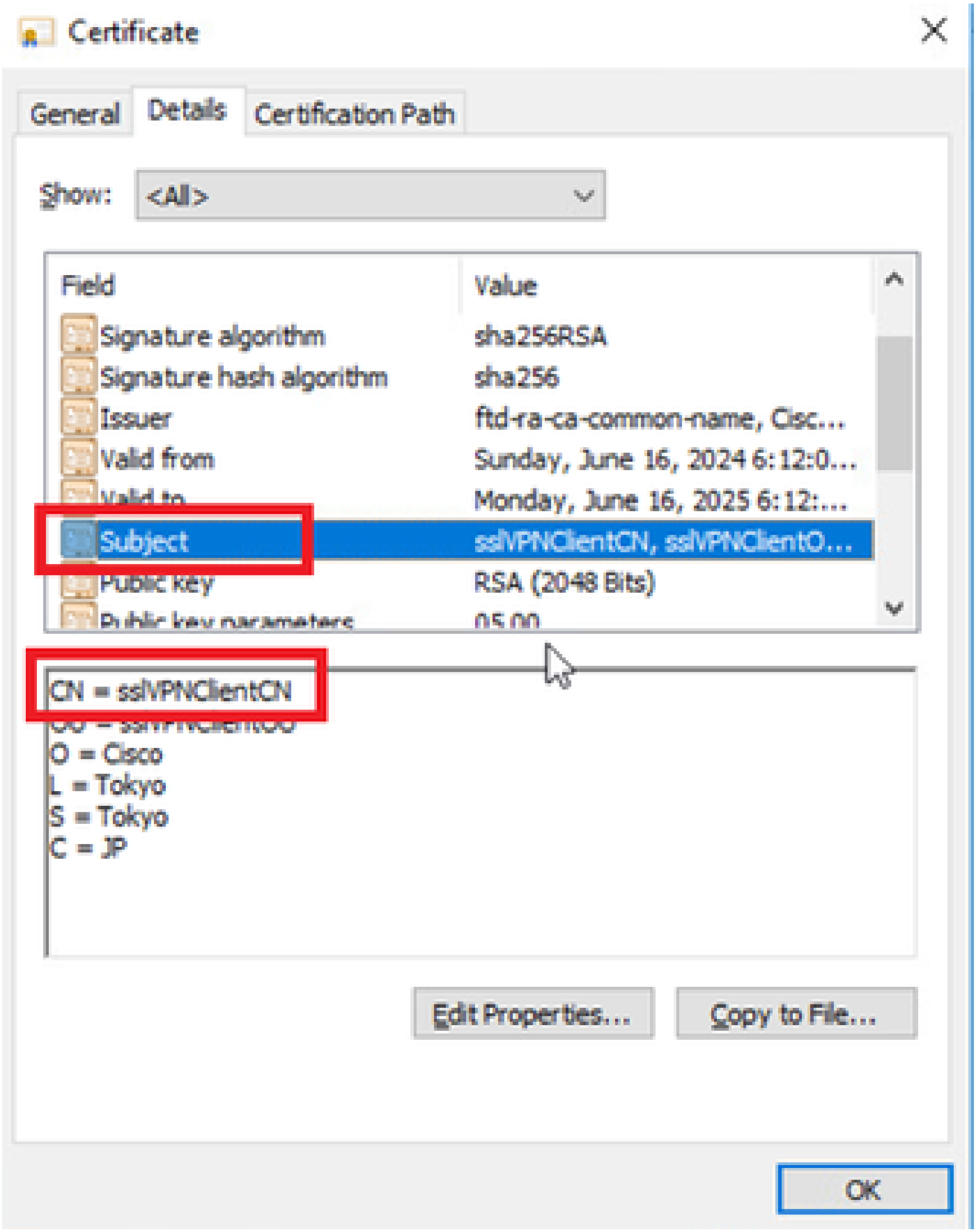
Certificates - Current User > Personal > Certificates로 이동하여 인증에 사용되는 클라이언트 인증서를 확인합니다.



클라이언트 인증서 확인

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

- 제목: CN = sslVPNClientCN



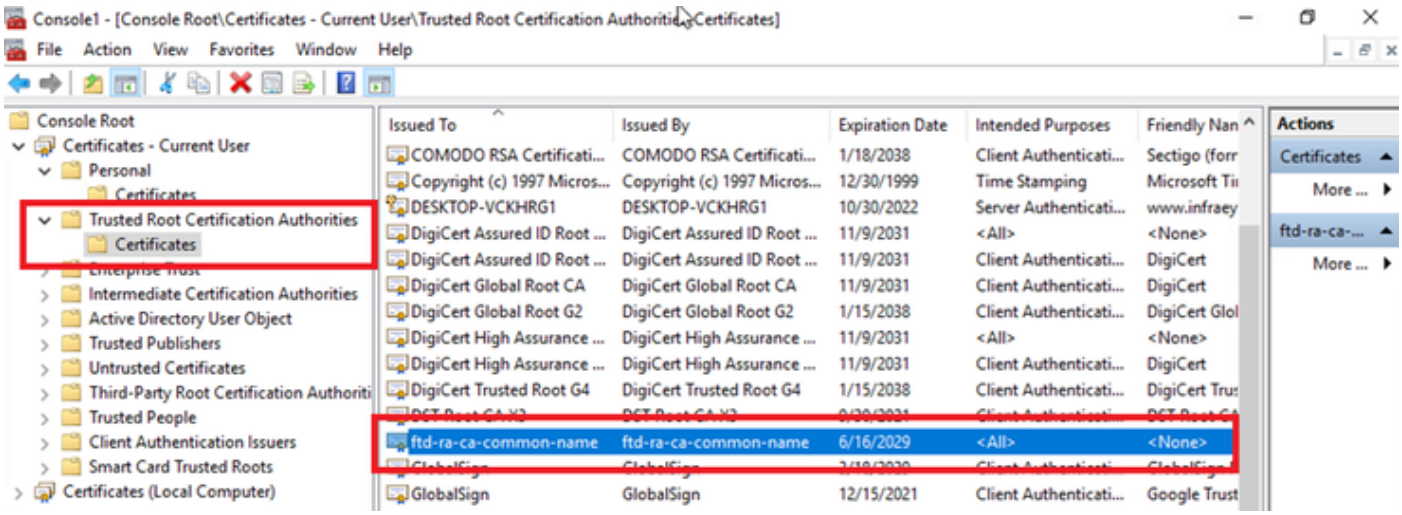
클라이언트 인증서 세부사항

2단계. CA 확인

Certificates - Current User(인증서 - 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

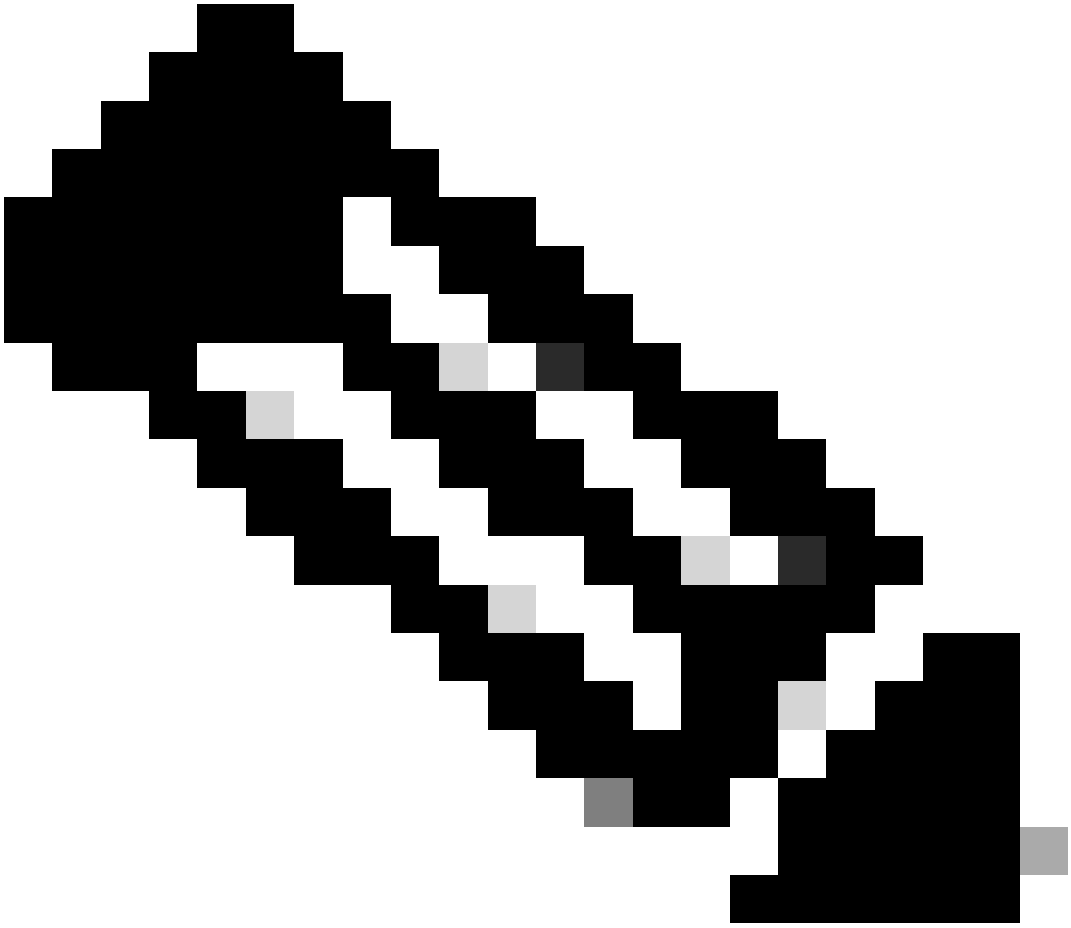


CA 확인

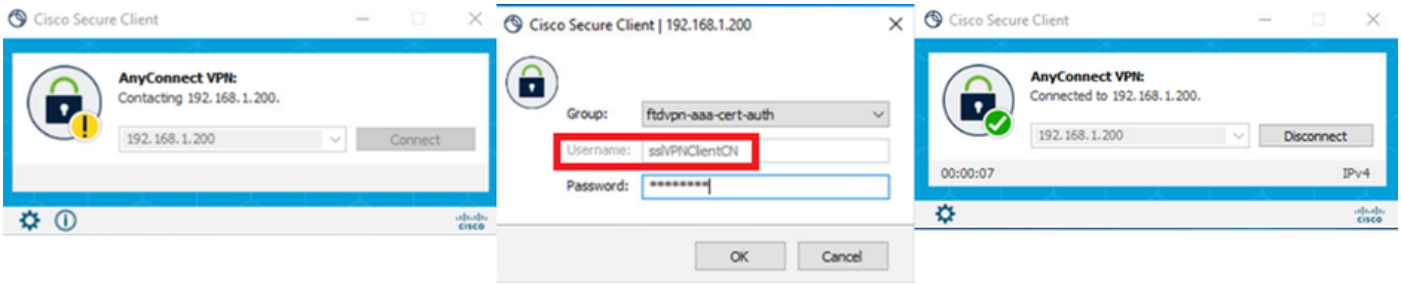
다음을 확인합니다.

1단계. VPN 연결 시작

엔드포인트에서 Cisco Secure Client 연결을 시작합니다. 사용자 이름은 클라이언트 인증서에서 추출됩니다. VPN 인증을 위해 비밀번호를 입력해야 합니다.



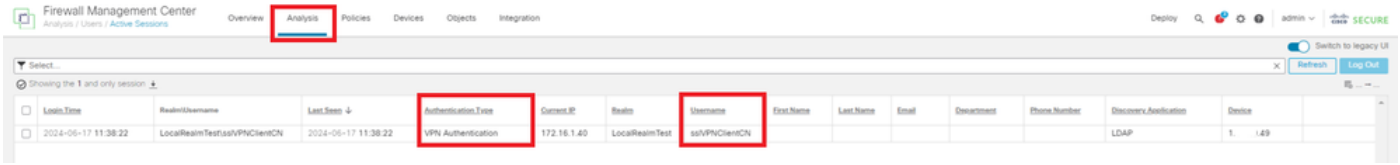
참고: 사용자 이름은 이 문서에 있는 클라이언트 인증서의 CN(Common Name) 필드에서 추출됩니다.



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 VPN 세션을 확인합니다.

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 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 : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 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 : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

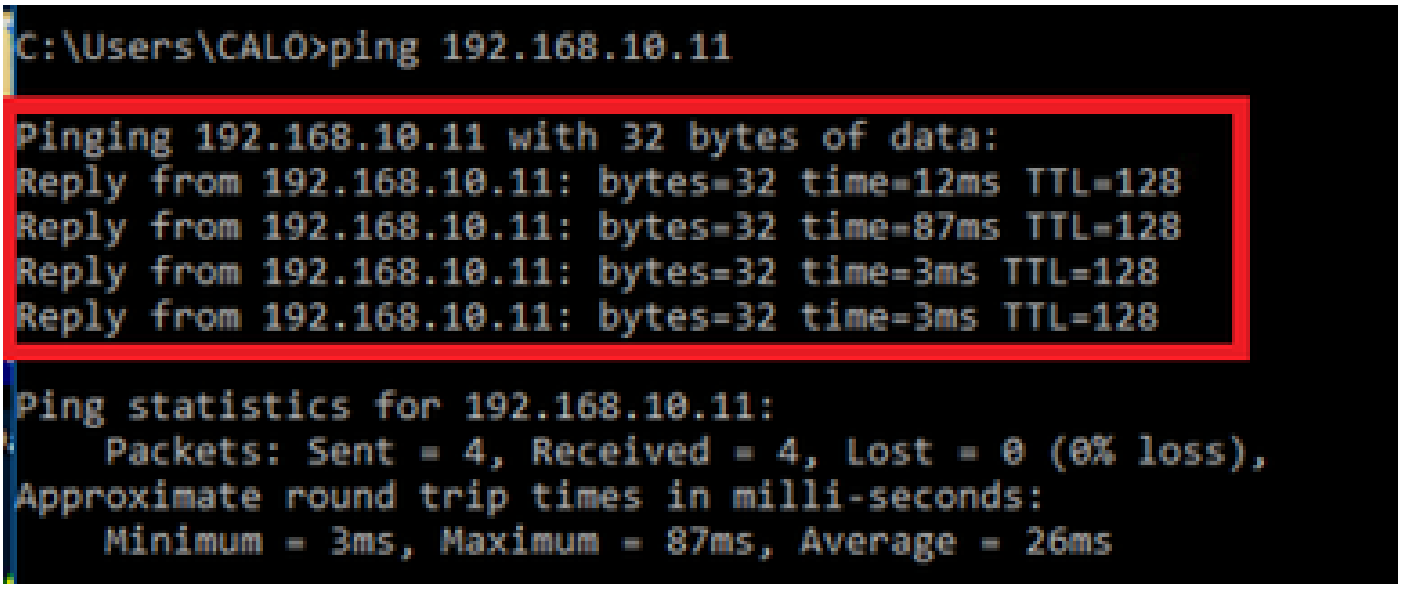
SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
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 : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

4단계. 서버와의 통신 확인

VPN 클라이언트에서 서버로 ping을 시작하고 VPN 클라이언트와 서버 간의 통신이 성공했는지 확인합니다.



Ping 성공

FTD(capture in interface inside real-timeLina) CLI에서 명령을 실행하여 패킷 캡처를 확인합니다.

ftd702#

```
capture in interface inside real-time


Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

문제 해결

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

Lina 엔진의 디버그 로그 예입니다.

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

이러한 디버그는 컨피그레이션 문제를 해결하기 위해 사용할 수 있는 정보를 제공하는 FTD의 진단 CLI에서 실행할 수 있습니다.

- debug crypto ca 14
- webvpn anyconnect 255 디버그
- 디버그 crypto ike-common 255

참조

FTD에서 AnyConnect 원격 액세스 VPN 구성

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.