FDM을 통해 FTD에서 보안 클라이언트에 대한 AAA 및 인증서 인증 구성

목차

소개

이 문서에서는 FDM에서 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 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

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

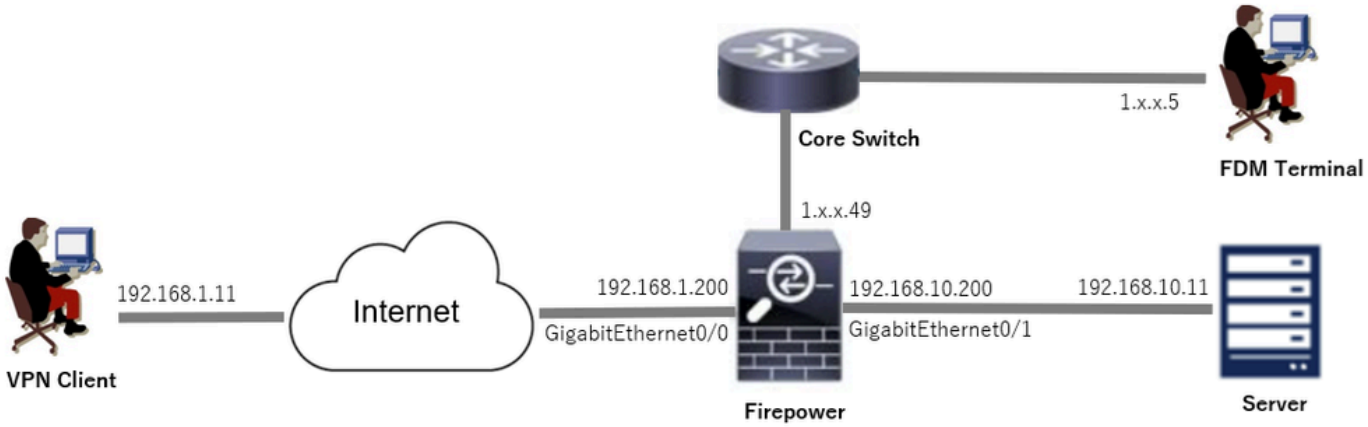
FDM(firepower 장치 관리자)은 Cisco FTD(Firepower Threat Defense) 장치 관리에 사용되는 간소화된 웹 기반 관리 인터페이스입니다. firepower 장치 관리자를 사용하면 네트워크 관리자가 더 복잡한 FMC(Firepower 관리 센터)를 사용하지 않고도 FTD 어플라이언스를 구성하고 관리할 수 있습니다. FDM은 네트워크 인터페이스, 보안 영역, 액세스 제어 정책 및 VPN 설정과 같은 기본 작업은 물론 디바이스 성능 및 보안 이벤트를 모니터링할 수 있는 직관적인 사용자 인터페이스를 제공합니다. 간소화된 관리가 필요한 중소 규모 구축에 적합합니다.
이 문서에서는 미리 채워진 사용자 이름을 FDM에서 관리하는 FTD의 Cisco Secure Client와 통합하는 방법에 대해 설명합니다.
FMC를 사용하여 FTD를 관리하는 경우 FMC를 통해 FTD에서 Configure AAA and Cert Auth for Secure Client on FTD를 참조하십시오.

이는 문서에 사용된 각 인증서의 공통 이름을 가진 인증서 체인입니다.

- 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

FDM의 구성

1단계. FTD 인터페이스 구성

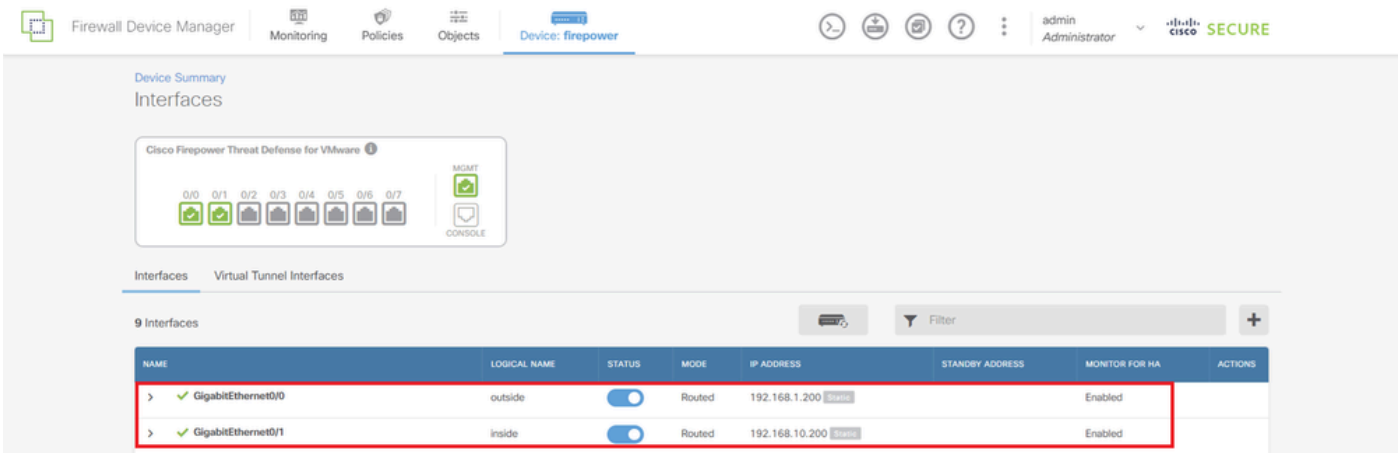
Device(디바이스) > Interfaces(인터페이스) > View All Interfaces(모든 인터페이스 보기)로 이동하고, Interfaces(인터페이스) 탭에서 FTD에 대한 내부 및 외부 인터페이스를 구성합니다.

GigabitEthernet0/0,

- 이름: outside
- IP 주소: 192.168.1.200/24

GigabitEthernet0/1,

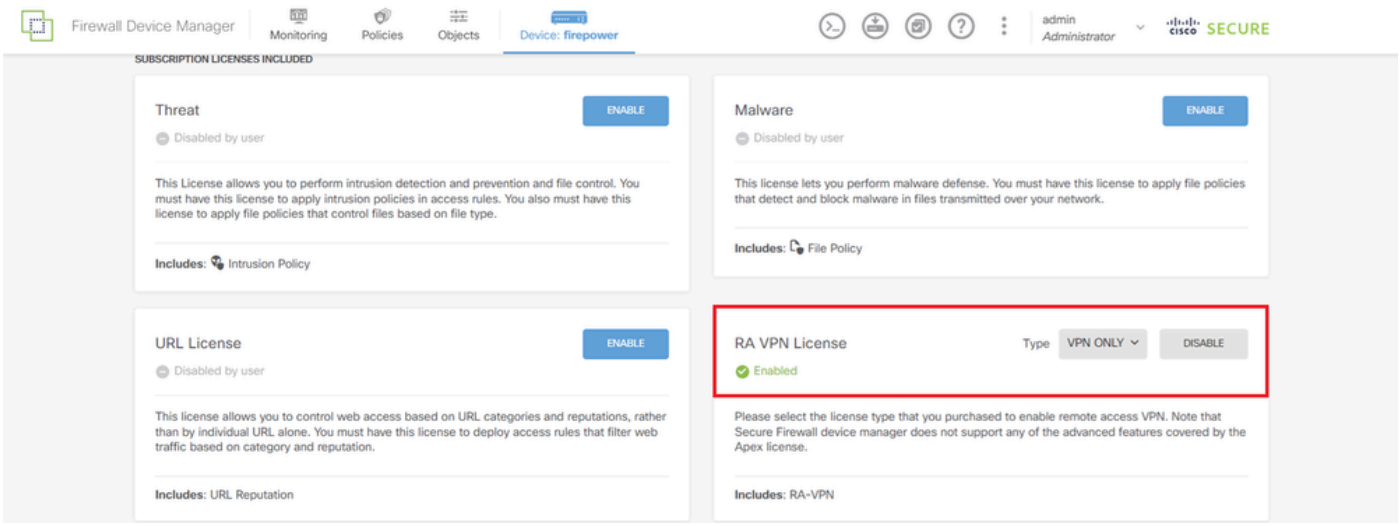
- 이름: inside
- IP 주소: 192.168.10.200/24



FTD 인터페이스

2단계. Cisco Secure Client 라이센스 확인

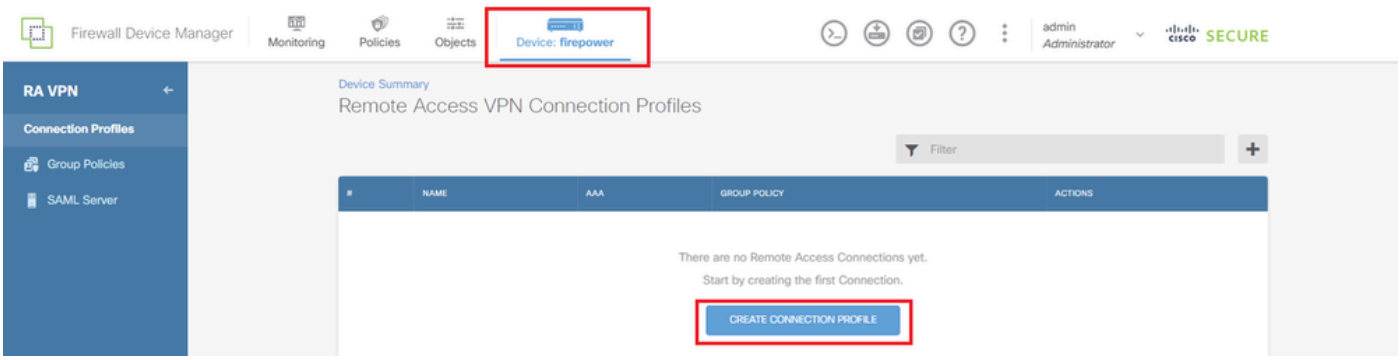
Device(디바이스) > Smart License(스마트 라이센스) > View Configuration(컨피그레이션 보기)으로 이동하여 RA VPN License(RA VPN 라이센스) 항목에서 Cisco Secure Client 라이센스를 확인합니다.



Secure Client 라이센스

3단계. 원격 액세스 VPN 연결 프로파일 추가

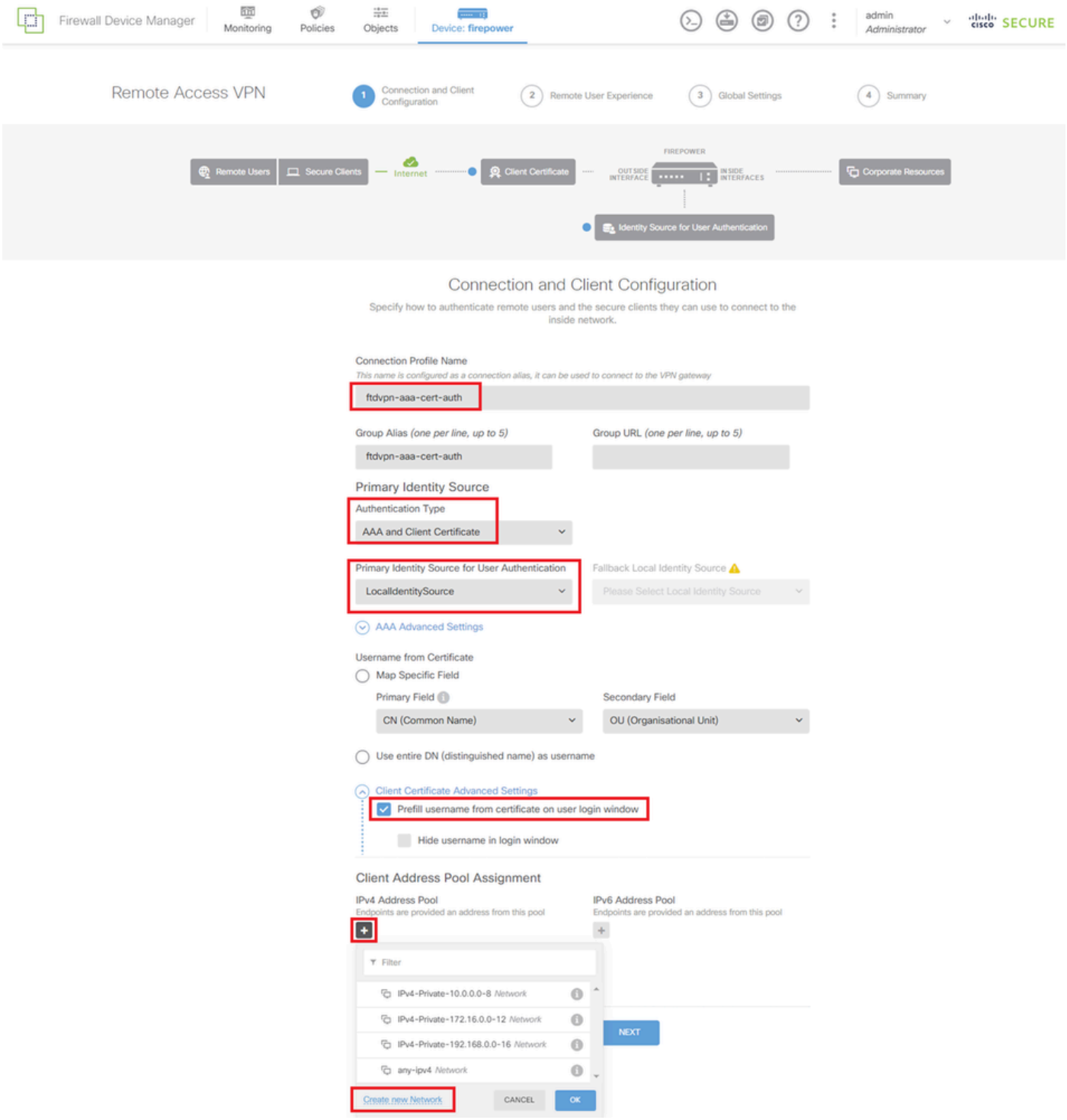
Device(디바이스) > Remote Access VPN(원격 액세스 VPN) > View Configuration(컨피그레이션 보기)으로 이동하고 CREATE CONNECTION PROFILE(연결 프로파일 생성) 버튼을 클릭합니다.



원격 액세스 VPN 연결 프로파일 추가

연결 프로파일에 필요한 정보를 입력하고 IPv4 Address Pool(IPv4 주소 풀) 항목에서 Create new Network(새 네트워크 생성) 버튼을 클릭합니다.

- 연결 프로파일 이름: ftdvpn-aaa-cert-auth
- 인증 유형: AAA 및 클라이언트 인증서
- 사용자 인증을 위한 기본 ID 소스: LocalIdentitySource
- 클라이언트 인증서 고급 설정: 사용자 로그인 창의 인증서에서 사용자 이름 미리 채우기

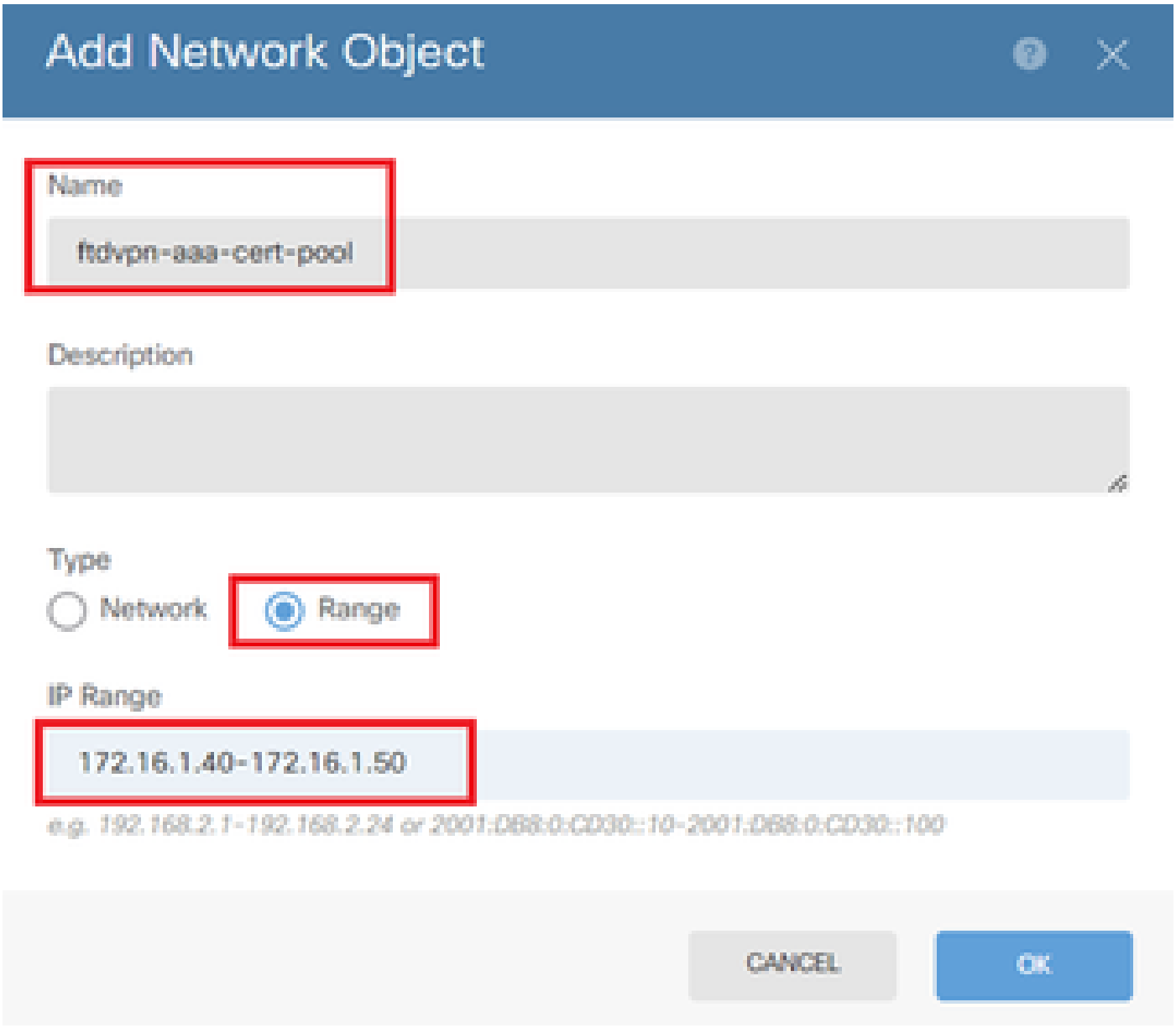


VPN 연결 프로파일 세부사항

4단계. 연결 프로파일에 대한 주소 풀 추가

새 IPv4 주소 풀을 추가하는 데 필요한 정보를 입력합니다. 연결 프로파일에 대해 새로 추가된 IPv4 주소 풀을 선택하고 Next(다음) 버튼을 클릭합니다.

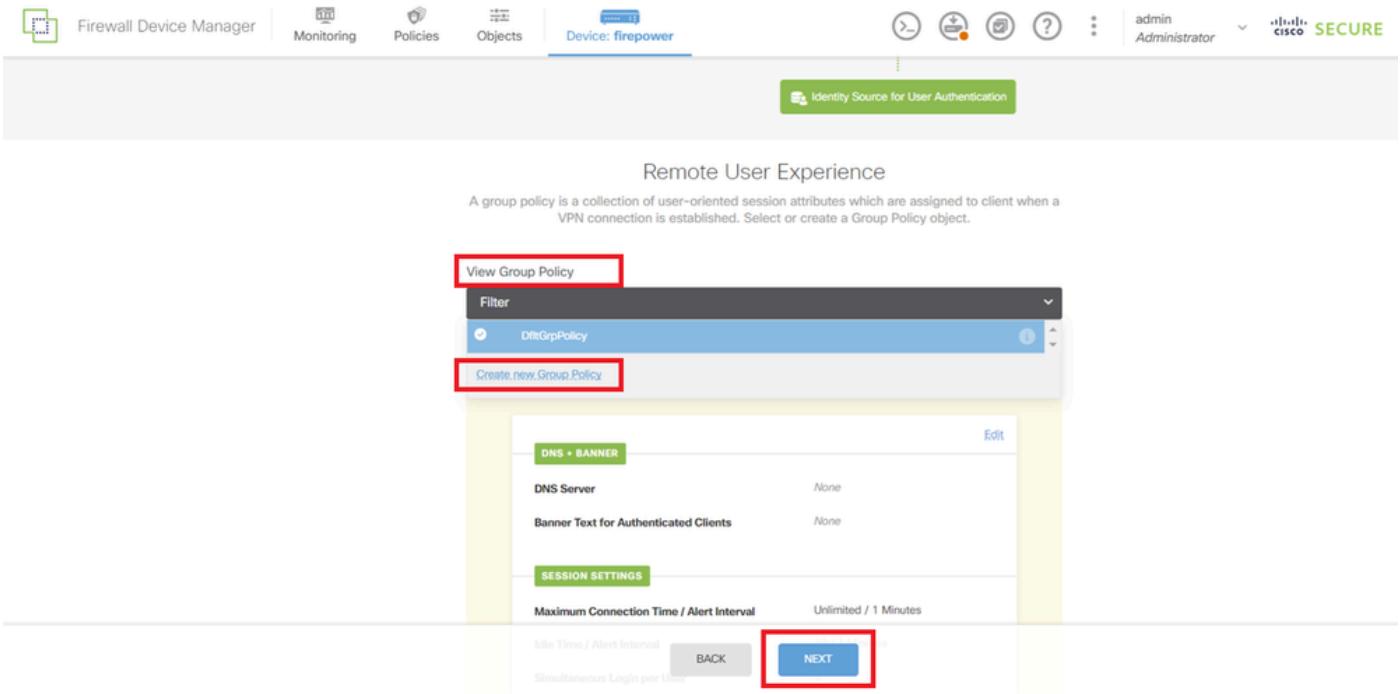
- 이름: ftdvpn-aaa-cert-pool
- 유형: 범위
- IP 범위: 172.16.1.40-172.16.1.50



IPv4 주소 풀 세부 정보

5단계. 연결 프로파일에 대한 그룹 정책 추가

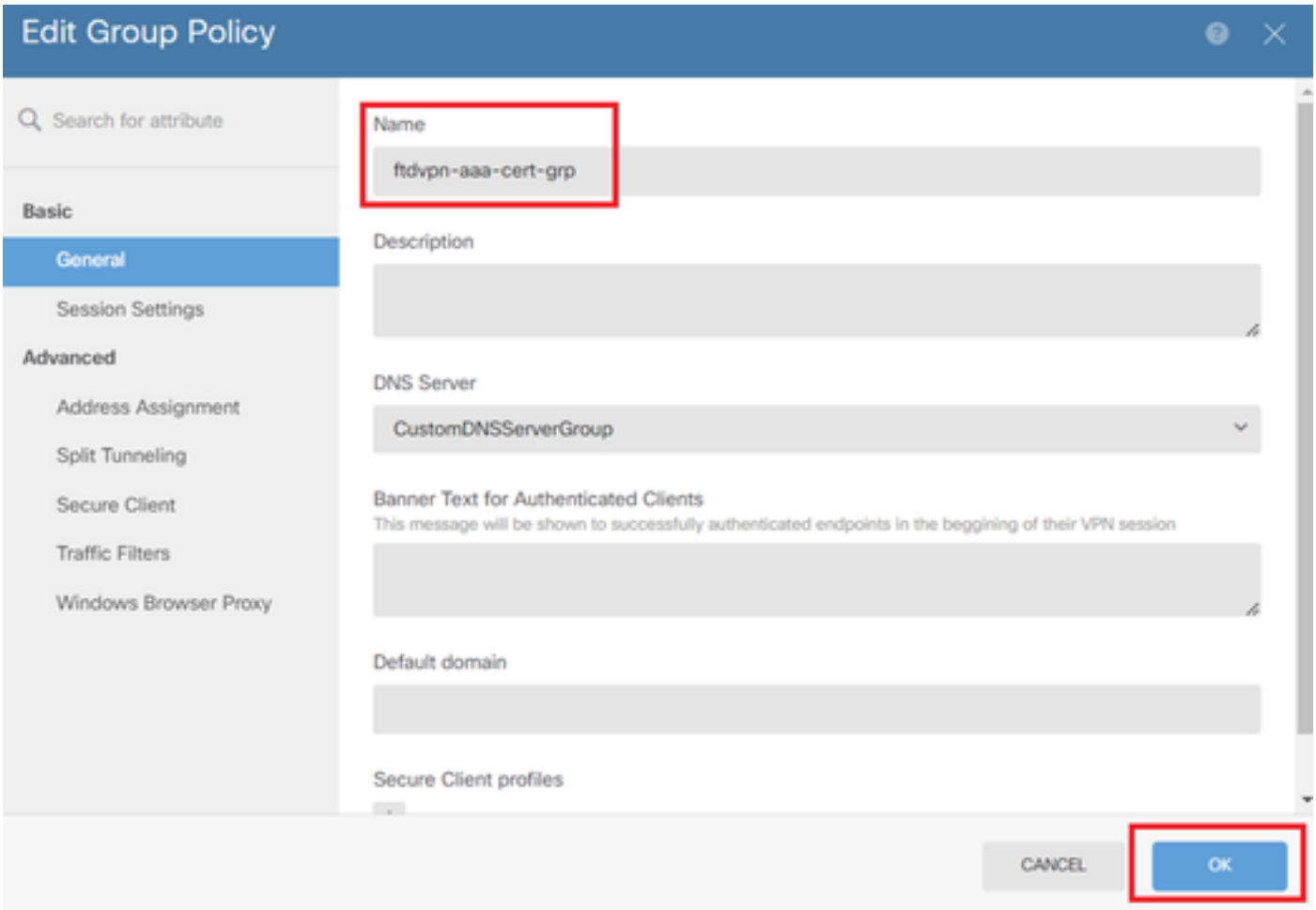
View Group Policy(그룹 정책 보기) 항목에서 Create new Group Policy(새 그룹 정책 생성)를 클릭합니다.



그룹 정책 추가

새 그룹 정책을 추가하는 데 필요한 정보를 입력하고 OK(확인) 버튼을 클릭합니다. 연결 프로파일에 대해 새로 추가된 그룹 정책을 선택합니다.

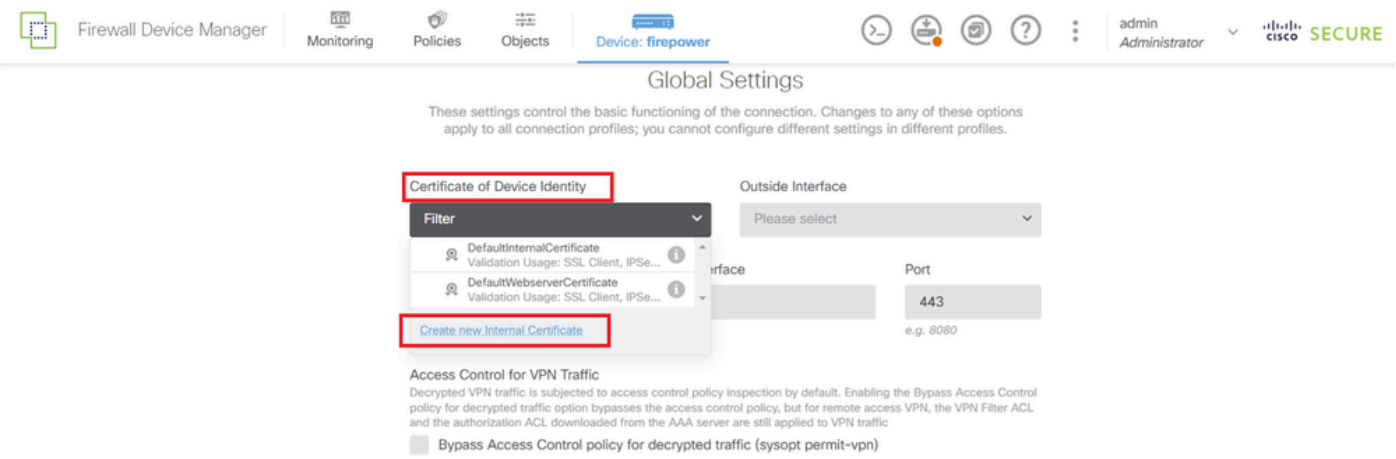
- 이름: ftdvpn-aaa-cert-grp



그룹 정책 세부 정보

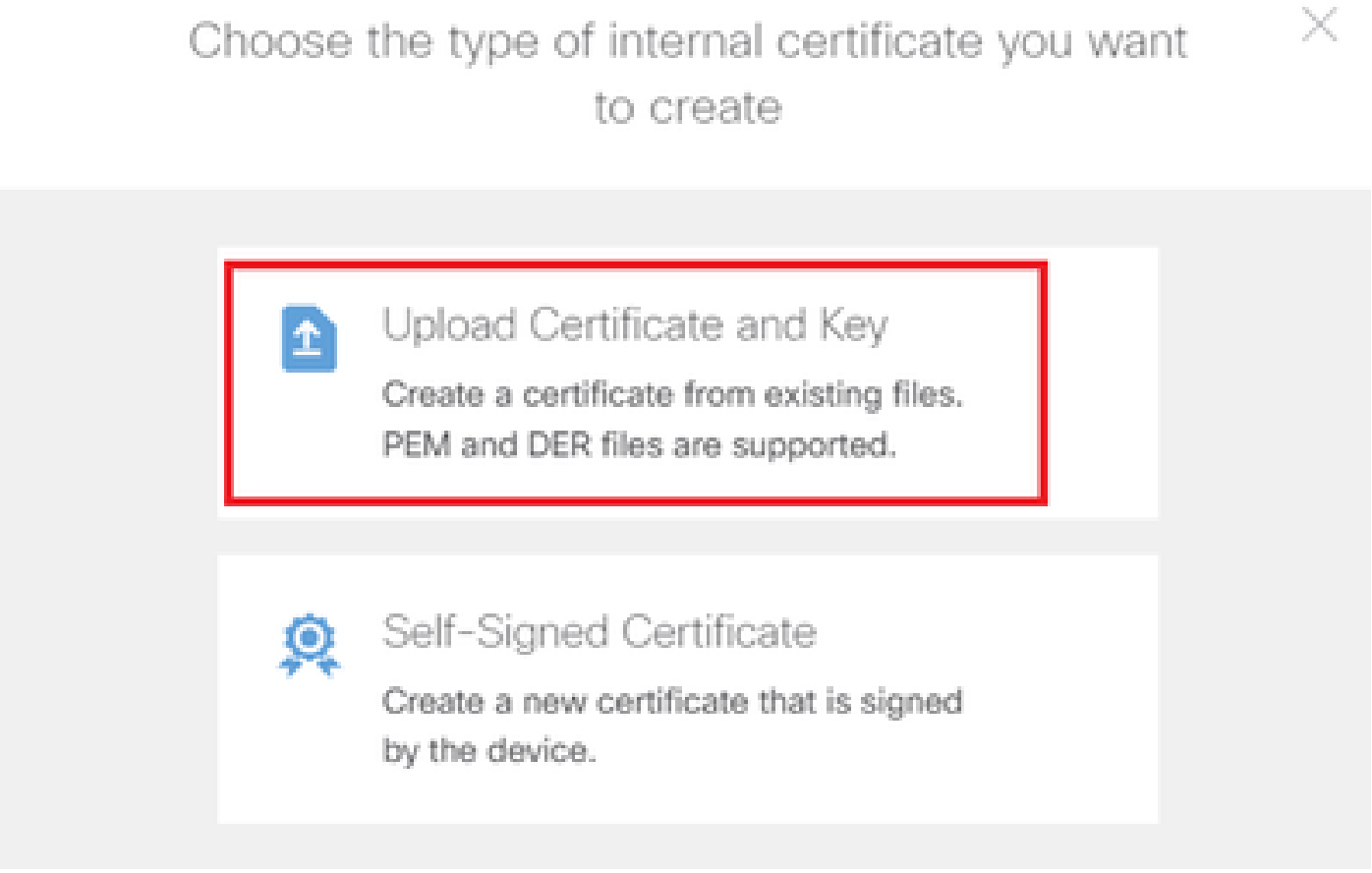
6단계. 연결 프로파일에 대한 장치 ID 및 외부 인터페이스의 인증서 구성

Certificate of Device Identity(디바이스 ID의 인증서) 항목에서 Create new Internal certificate(새 내부 인증서 생성)를 클릭합니다.



내부 인증서 추가

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

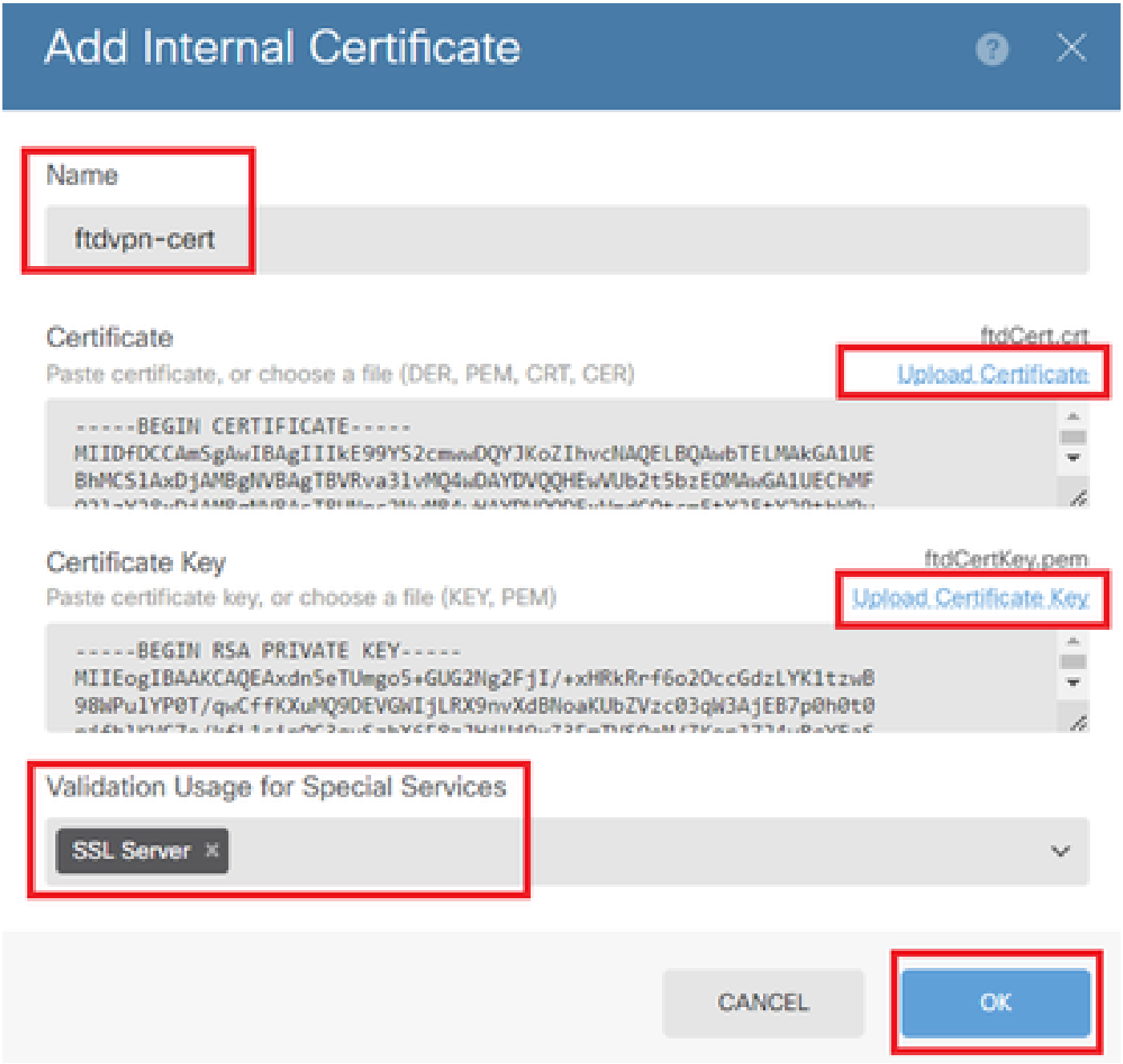


인증서 및 키 업로드

FTD 인증서에 필요한 정보를 입력하고 로컬 컴퓨터에서 인증서와 인증서 키를 가져온 다음 OK(확

인) 버튼을 클릭합니다.

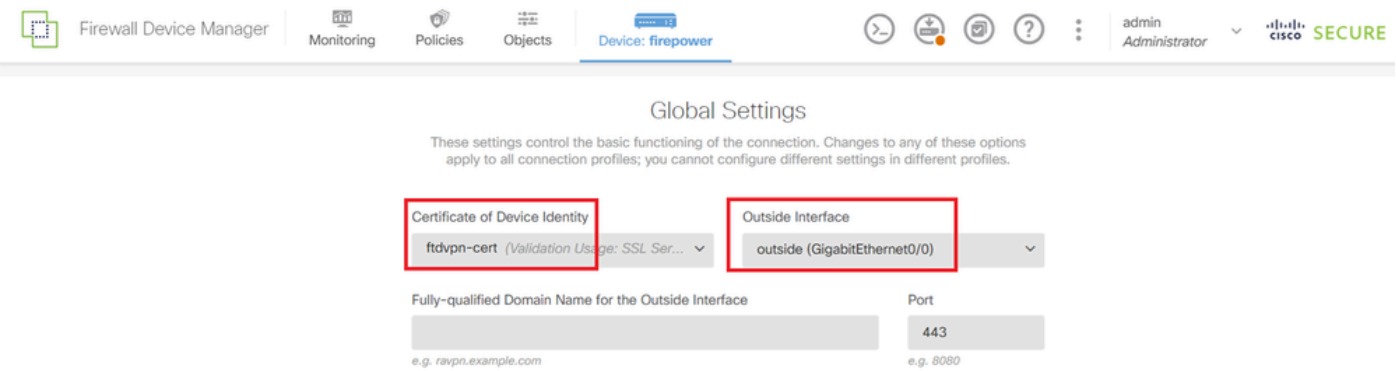
- 이름: ftdvpn-cert
- 특수 서비스의 유효성 검사 사용: SSL 서버



내부 인증서 세부 정보

Certificate of Device Identity and Outside Interface for VPN connection을 선택합니다.

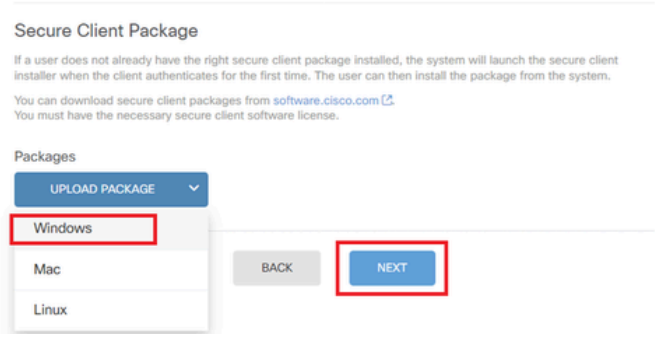
- 디바이스 ID 인증서: ftdvpn-cert
- 외부 인터페이스: 외부(GigabitEthernet0/0)



전역 설정 세부 정보

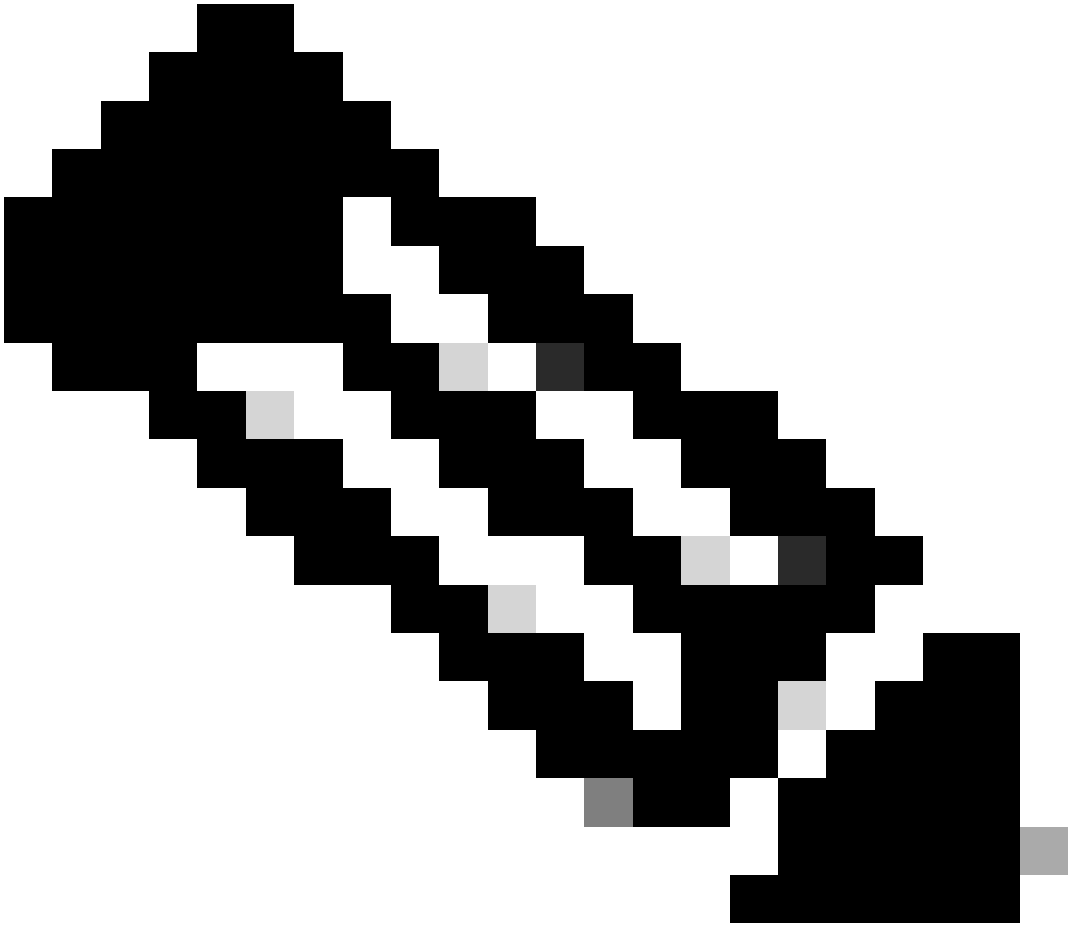
7단계. 연결 프로파일에 대한 보안 클라이언트 이미지 구성

패키지 항목에서 Windows 선택

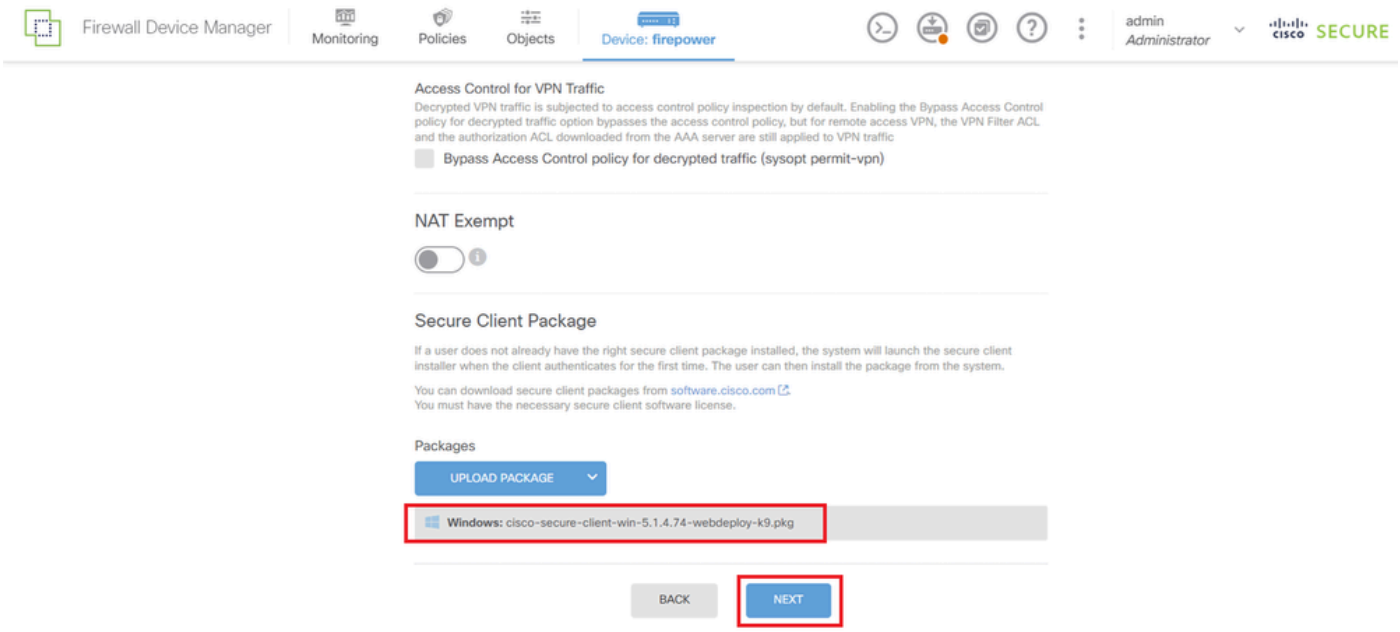


보안 클라이언트 이미지 패키지 업로드

로컬 컴퓨터에서 보안 클라이언트 이미지 파일을 업로드하고 다음 버튼을 클릭합니다.



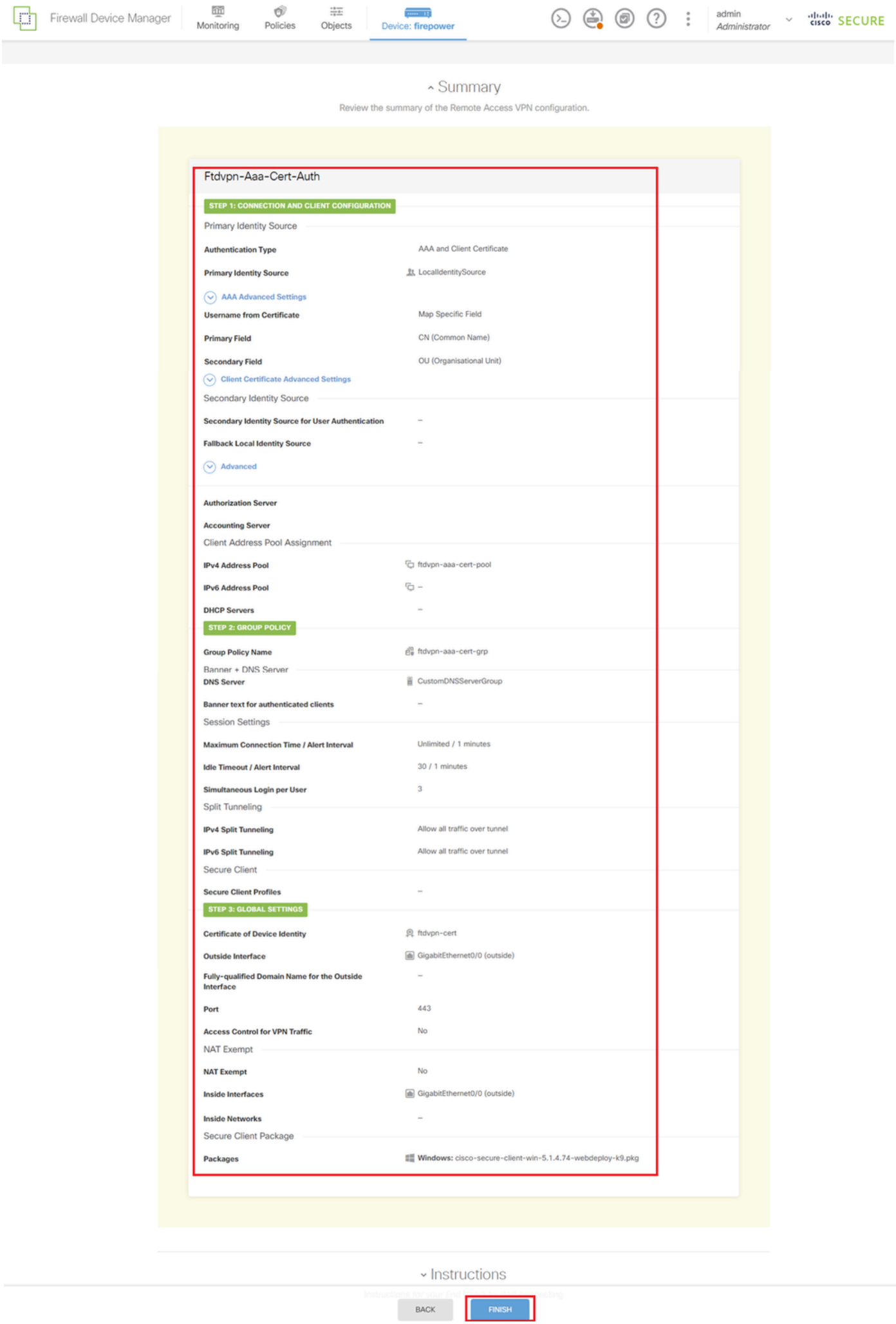
참고: 이 문서에서는 NAT 제외 기능을 사용할 수 없습니다. 기본적으로 암호 해독된 트래픽에 대한 Bypass Access Control policy(sysopt permit-vpn) 옵션은 비활성화되어 있습니다. 즉, 암호 해독된 VPN 트래픽은 액세스 제어 정책 검사를 거치게 됩니다.



보안 클라이언트 이미지 패키지 선택

8단계. 연결 프로파일에 대한 요약 확인

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



연결 프로파일에 대한 설정 확인

```
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
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
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

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

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

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
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 enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
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 none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// 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

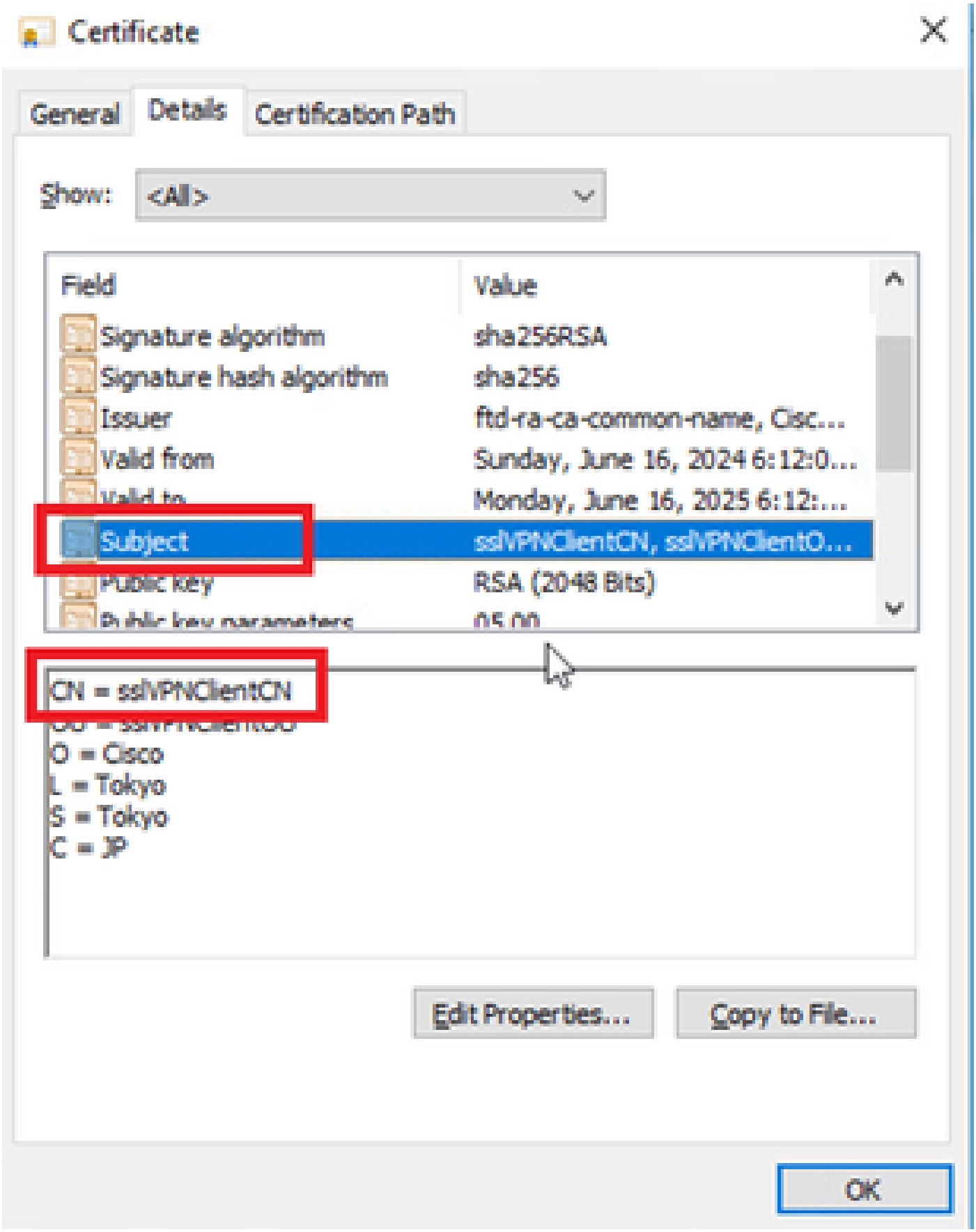
1단계. 클라이언트 인증서 확인

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

클라이언트 인증서 확인

클라이언트 인증서를 더블 클릭하고 Details로 이동하여 Subject의 세부사항을 확인합니다.

- 제목: CN = sslVPNClientCN



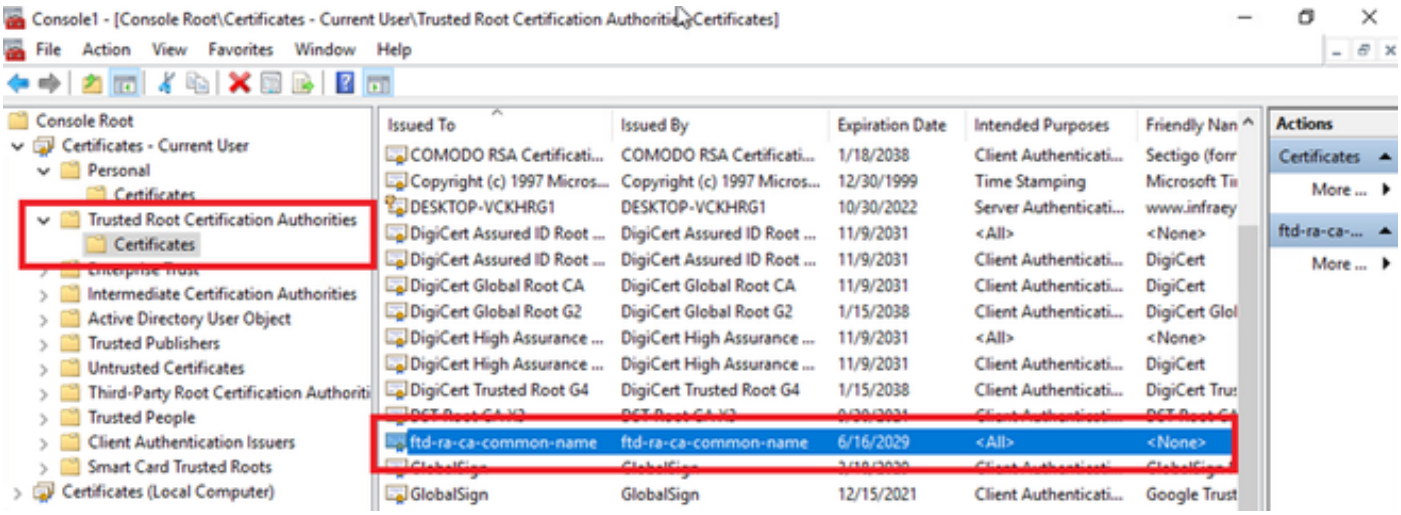
클라이언트 인증서 세부사항

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

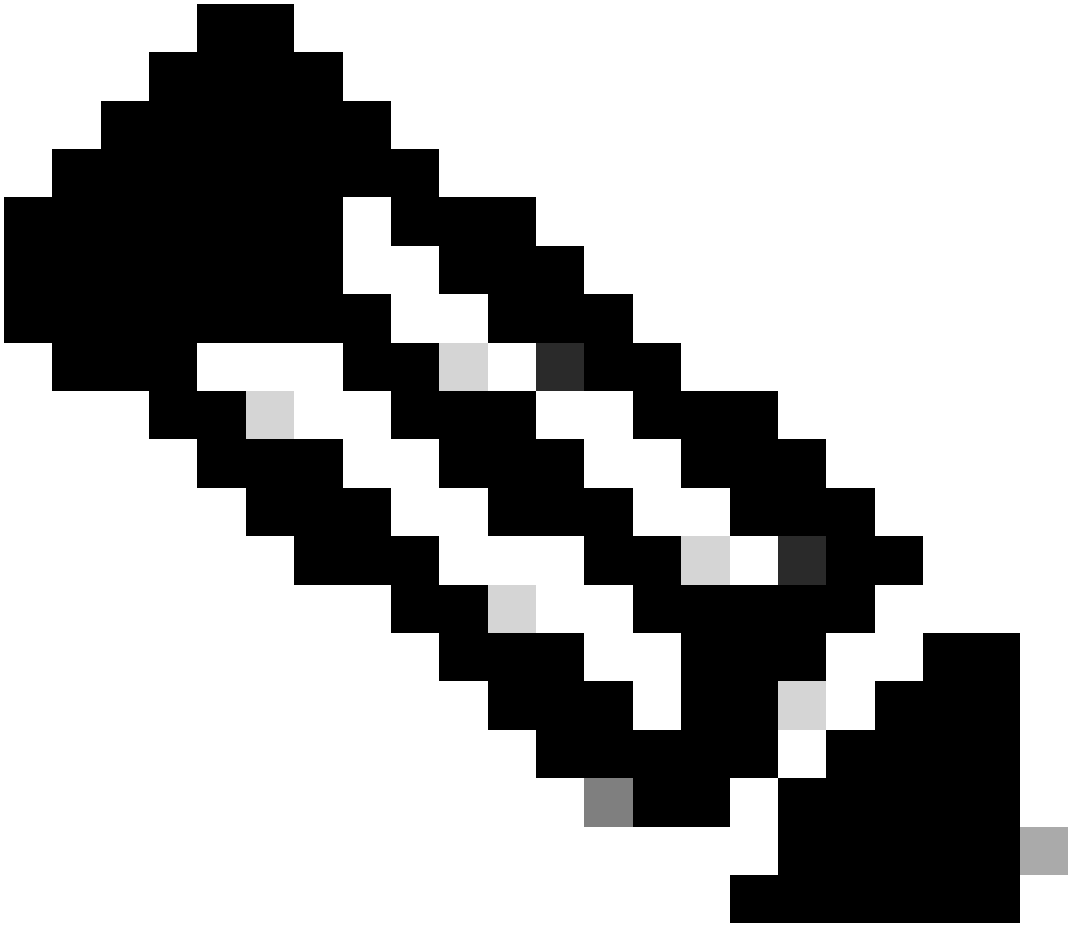


CA 확인

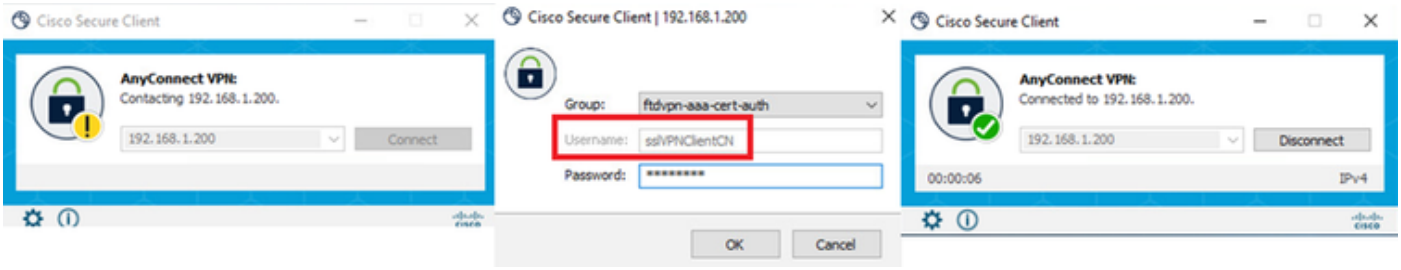
다음을 확인합니다.

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. FTD CLI에서 VPN 세션 확인

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

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 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 : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

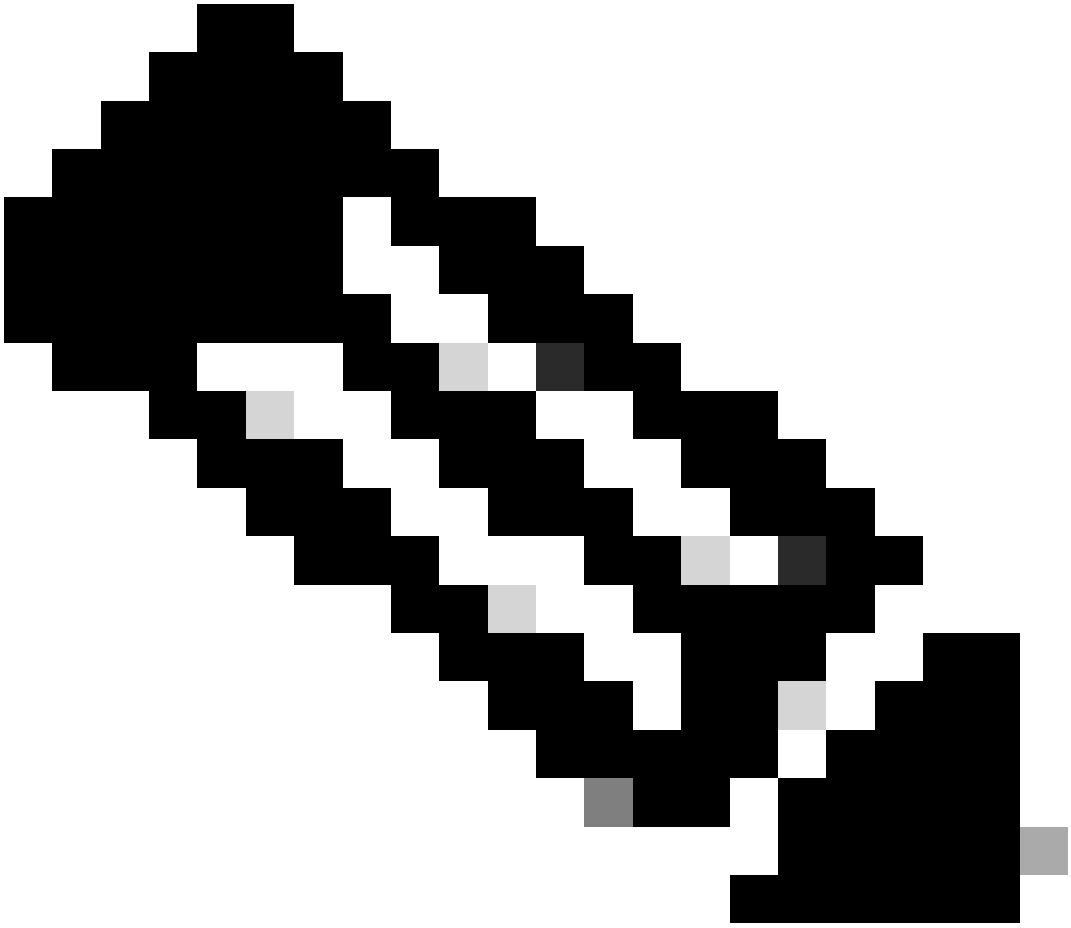
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 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 : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

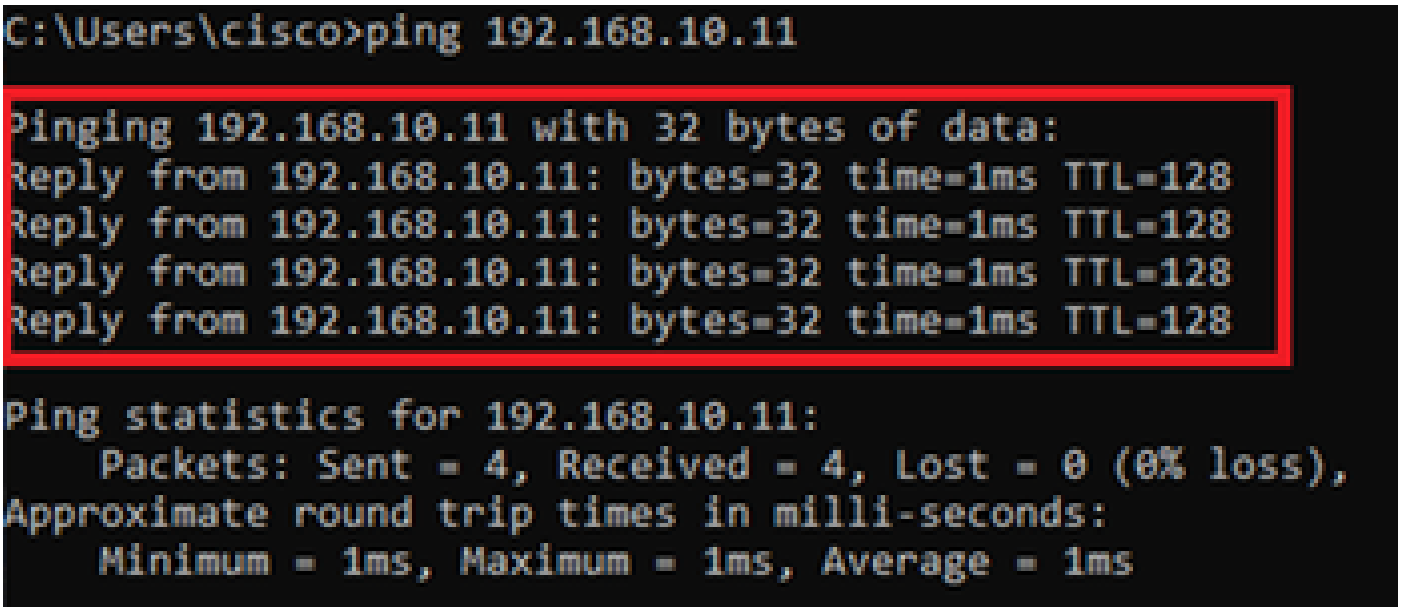
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0

3단계. 서버와의 통신 확인

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



참고: 7단계에서 암호 해독된 트래픽에 대한 Bypass Access Control Policy(sysopt permit-vpn) 옵션이 비활성화되므로 IPv4 주소 풀의 서버 액세스를 허용하는 액세스 제어 규칙을 만들어야 합니다.



Ping 성공

capture in interface inside real-timeFTD(Lina) CLI에서 Runcommand를 실행하여 패킷 캡처를 확인합니다.

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply

문제 해결

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

Lina 엔진의 디버그 로그 예입니다.

// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %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

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.