FDM에서 관리하는 FTD에서 AAA 인증을 사용하여 IPv6 지원 RAVPN 구성

목차

소개

이 문서에서는 FDM에서 관리되는 FTD에서 AAA 인증을 사용하여 IPv6 지원 원격 액세스 VPN을 구성하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0

- Cisco Secure Client 5.1.6.103

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

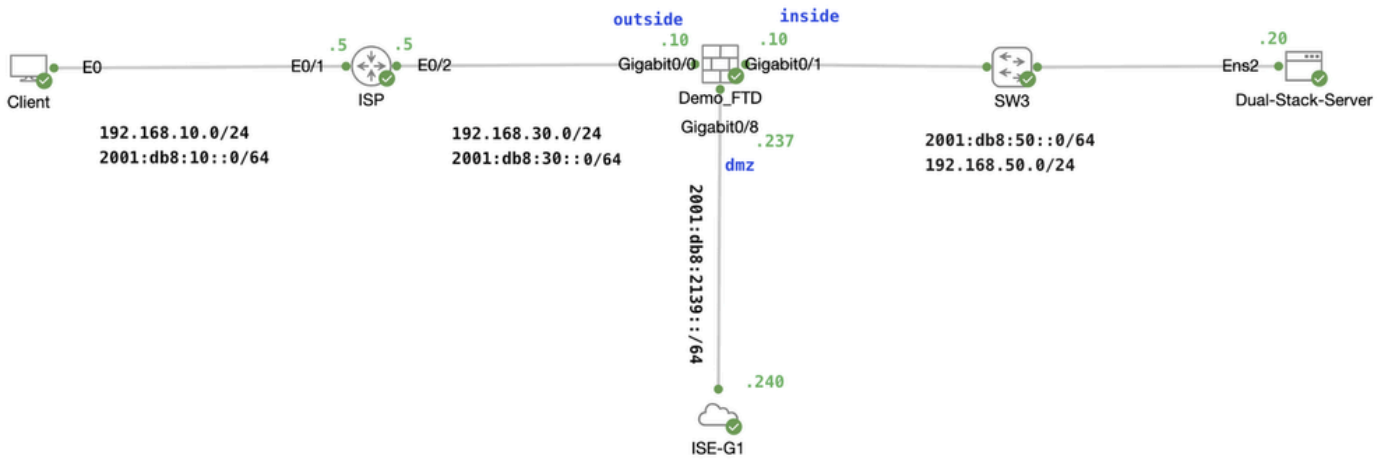
배경 정보

IPv4 주소가 제한되고 거의 소진됨에 따라 IPv4에서 IPv6로 전환되는 IPv6 원격 액세스 VPN(RAVPN)의 중요성이 날로 높아지고 있는 반면, IPv6는 점점 늘어나는 인터넷 연결 장치를 수용하여 사실상 무제한의 주소 공간을 제공합니다. IPv6로 이동하는 네트워크와 서비스의 수가 많을수록 IPv6 기능을 통해 네트워크의 호환성과 액세스 가능성을 유지할 수 있습니다. IPv6 RAVPN은 조직이 안전하고 확장 가능한 원격 연결을 보장하면서 네트워킹의 미래를 준비할 수 있도록 지원합니다.

이 예에서 클라이언트는 서비스 공급자가 제공한 IPv6 주소를 사용하여 VPN 게이트웨이와 통신하지만 Cisco ISE(Identity Service Engine)를 인증 ID 소스로 사용하여 VPN 풀에서 IPv4 및 IPv6 주소를 모두 수신합니다. ISE는 IPv6 주소로만 구성됩니다. 내부 서버는 듀얼 스택 호스트를 나타내는 IPv4 및 IPv6 주소로 구성됩니다. 클라이언트는 필요에 따라 IPv4 또는 IPv6 VPN 주소를 사용하여 내부 리소스에 액세스할 수 있습니다.

구성

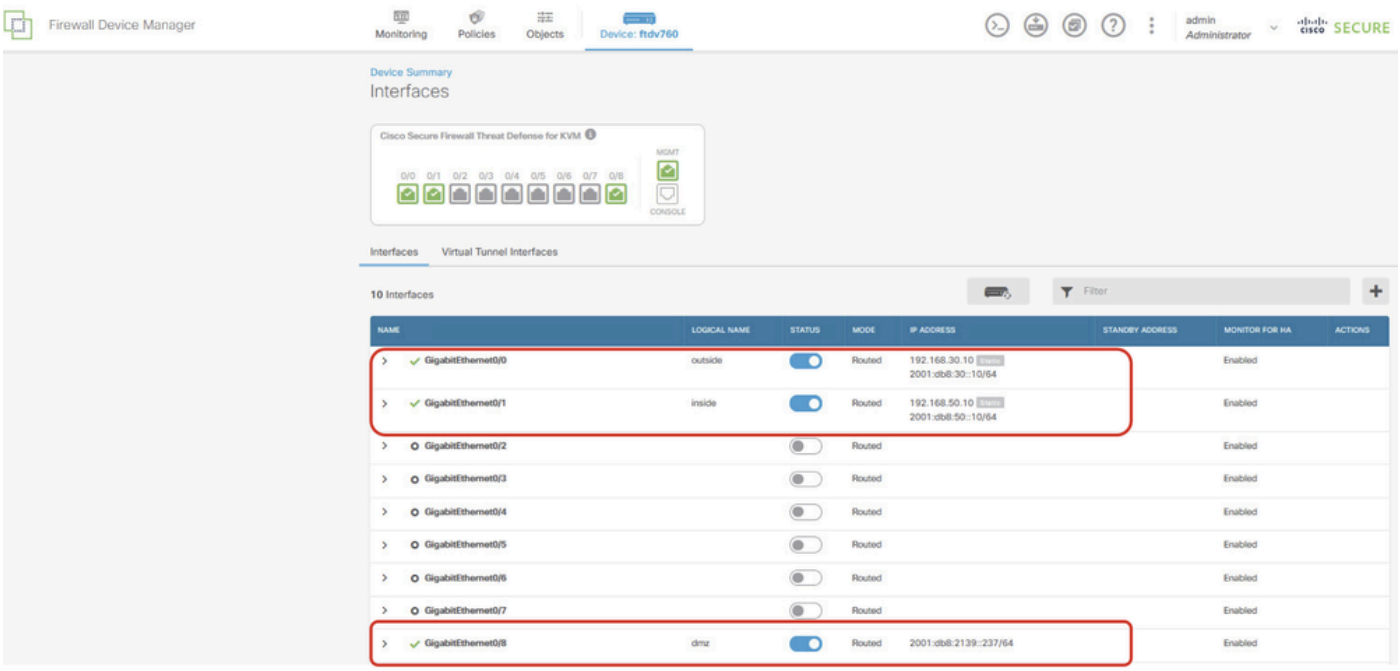
네트워크 다이어그램



토폴로지

FDM의 구성

1단계. 노드 간의 IPv4 및 IPv6 상호 연결의 예비 구성이 올바르게 완료되었는지 확인하는 것이 중요합니다. 클라이언트와 FTD의 게이트웨이는 관련 ISP 주소입니다. 서버의 게이트웨이는 FTD의 IP 내부에 있습니다. ISE는 FTD의 DMZ 영역에 있습니다.

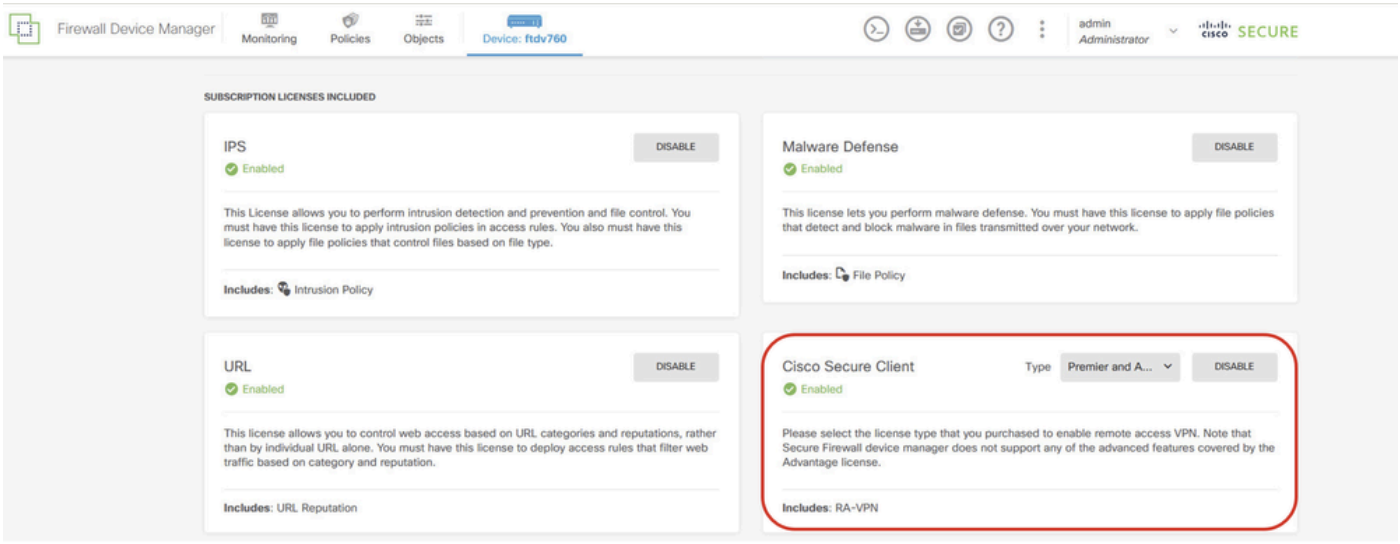


FTD_Interface_IP

FTD_Default_Route

2단계. Cisco Software Download에서 Cisco Secure Client 패키지 이름인 Cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg를 다운로드하고 다운로드한 파일의 md5 체크섬이 Cisco Software Download 페이지와 동일한지 확인하여 다운로드 후 파일이 정상인지 확인합니다.

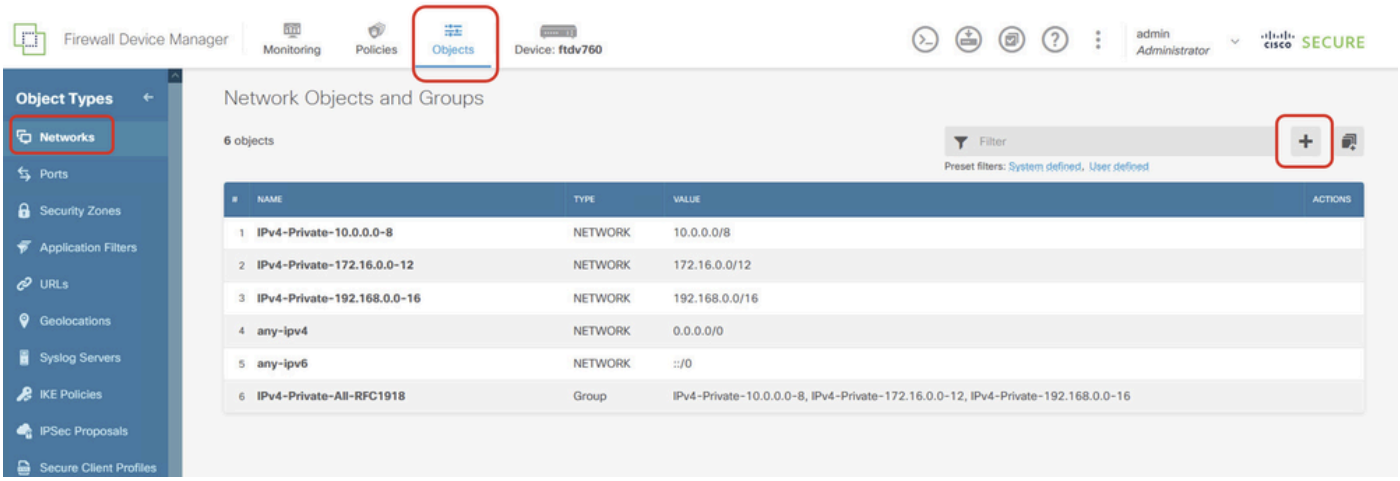
3단계. FTD에서 RAVPN 관련 라이센스가 활성화되었는지 확인합니다.



FDM_라이센스

4단계. VPN 주소 풀을 생성합니다.

4.1단계. 네트워크 객체를 생성하여 IPv6 및 IPv4 주소 풀을 생성합니다. Objects(객체) > Networks(네트워크)로 이동하고+ 버튼을 클릭합니다.

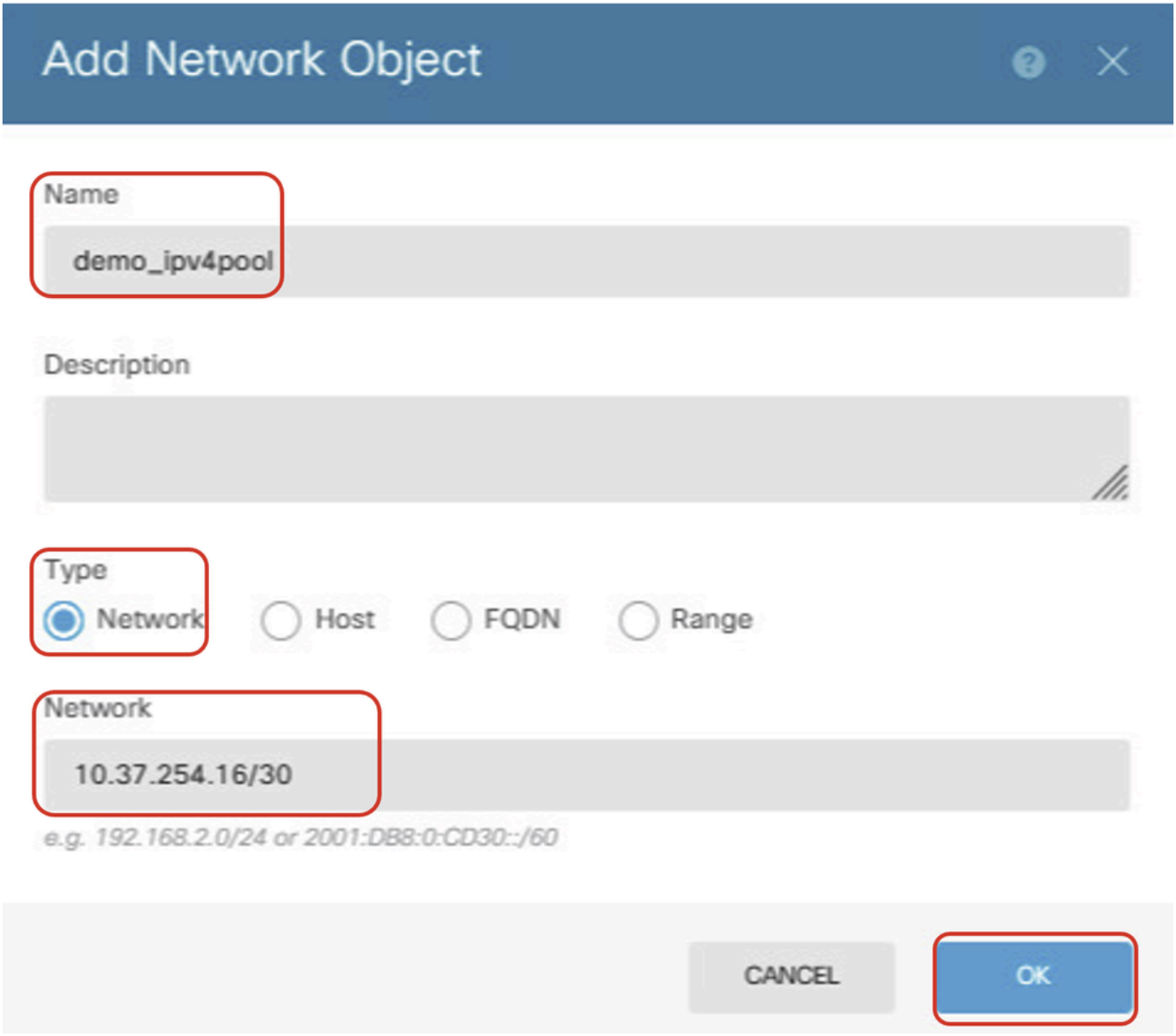


Create_VPN_Address_Pool_1

4.2단계. 각 네트워크 객체의 필요한 정보를 제공합니다. 확인 단추를 클릭합니다.

IPv4 풀의 경우 네트워크 또는 범위로 객체 유형을 선택할 수 있습니다. 이 예에서는 데모를 위해 네트워크 객체 유형을 선택합니다.

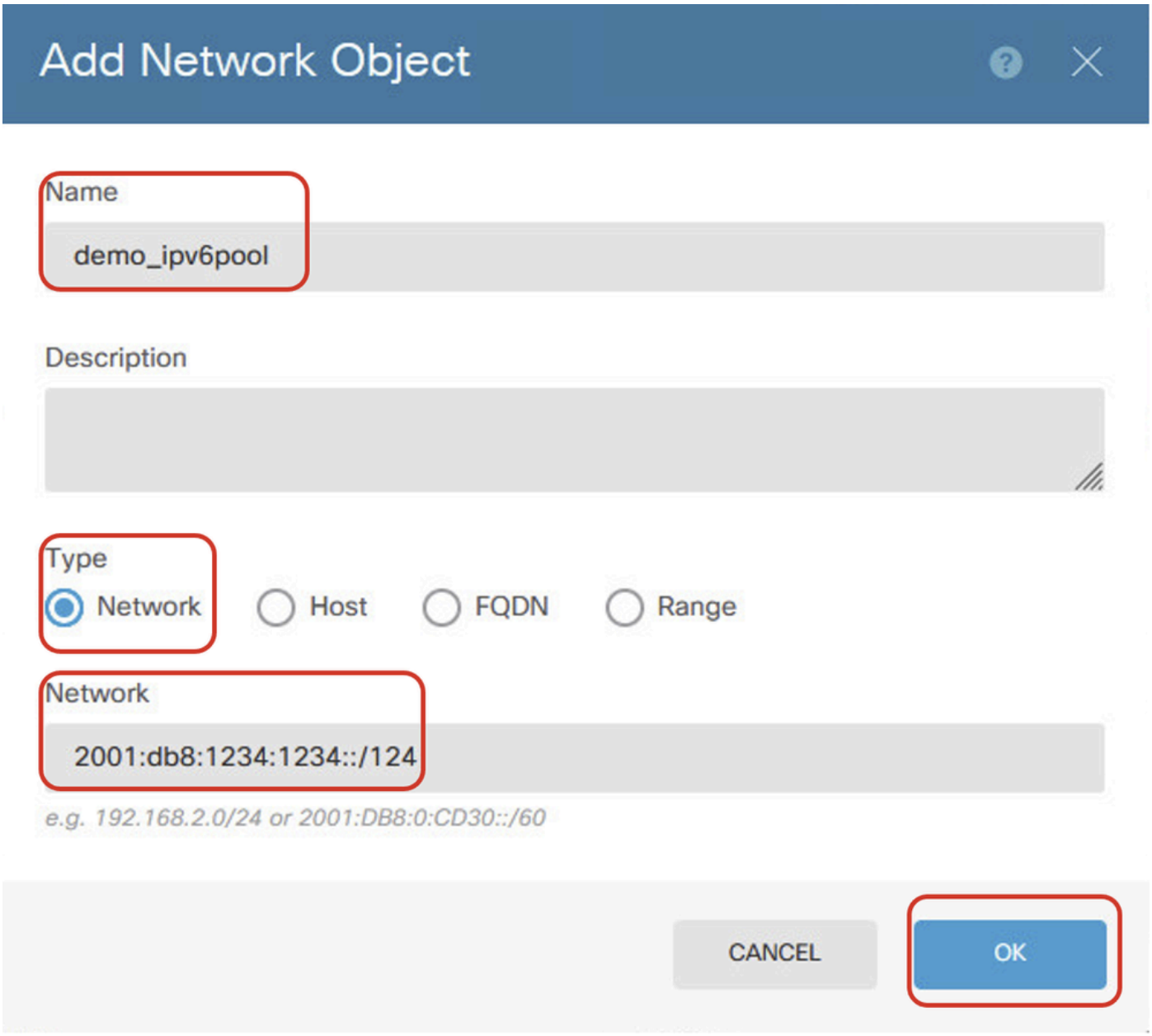
- 이름: demo_ipv4pool
- 유형: 네트워크
- 네트워크: 10.37.254.16/30



Create_VPN_Address_Pool_2_IPv4

IPv6 풀의 경우 개체 유형은 현재 Network에서만 선택할 수 있습니다.

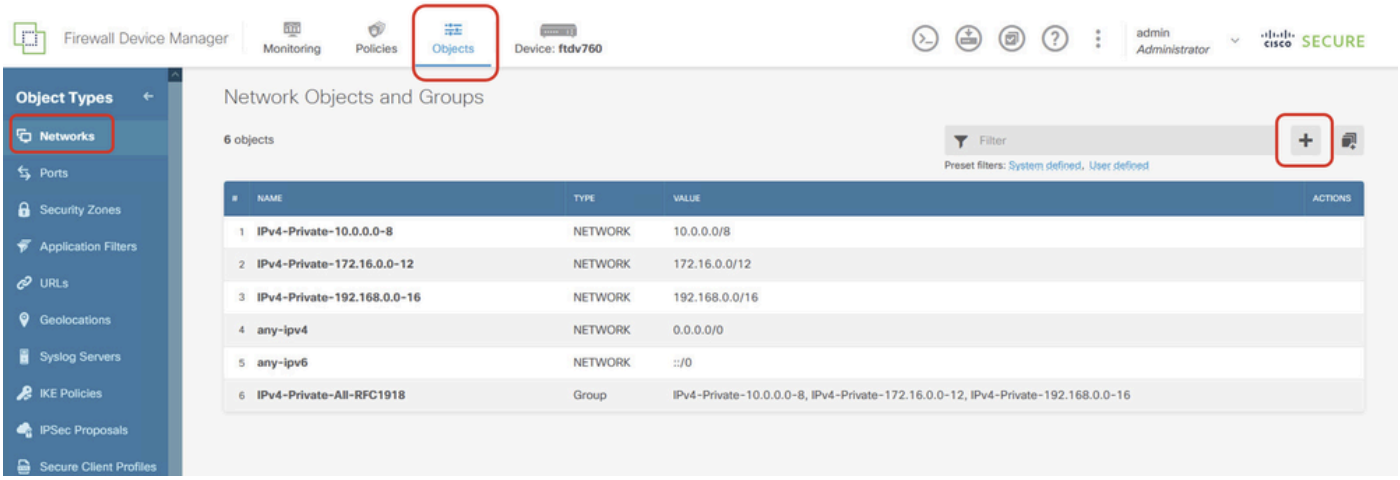
- 이름: demo_ipv6pool
- 유형: 네트워크
- 네트워크: 2001:db8:1234:1234:::/124



Create_VPN_Address_Pool_2_IPv6

5단계. NAT 제외를 위한 내부 네트워크를 생성합니다.

5.1단계. Objects(개체) > Networks(네트워크)로 이동하고 + 버튼을 클릭합니다.

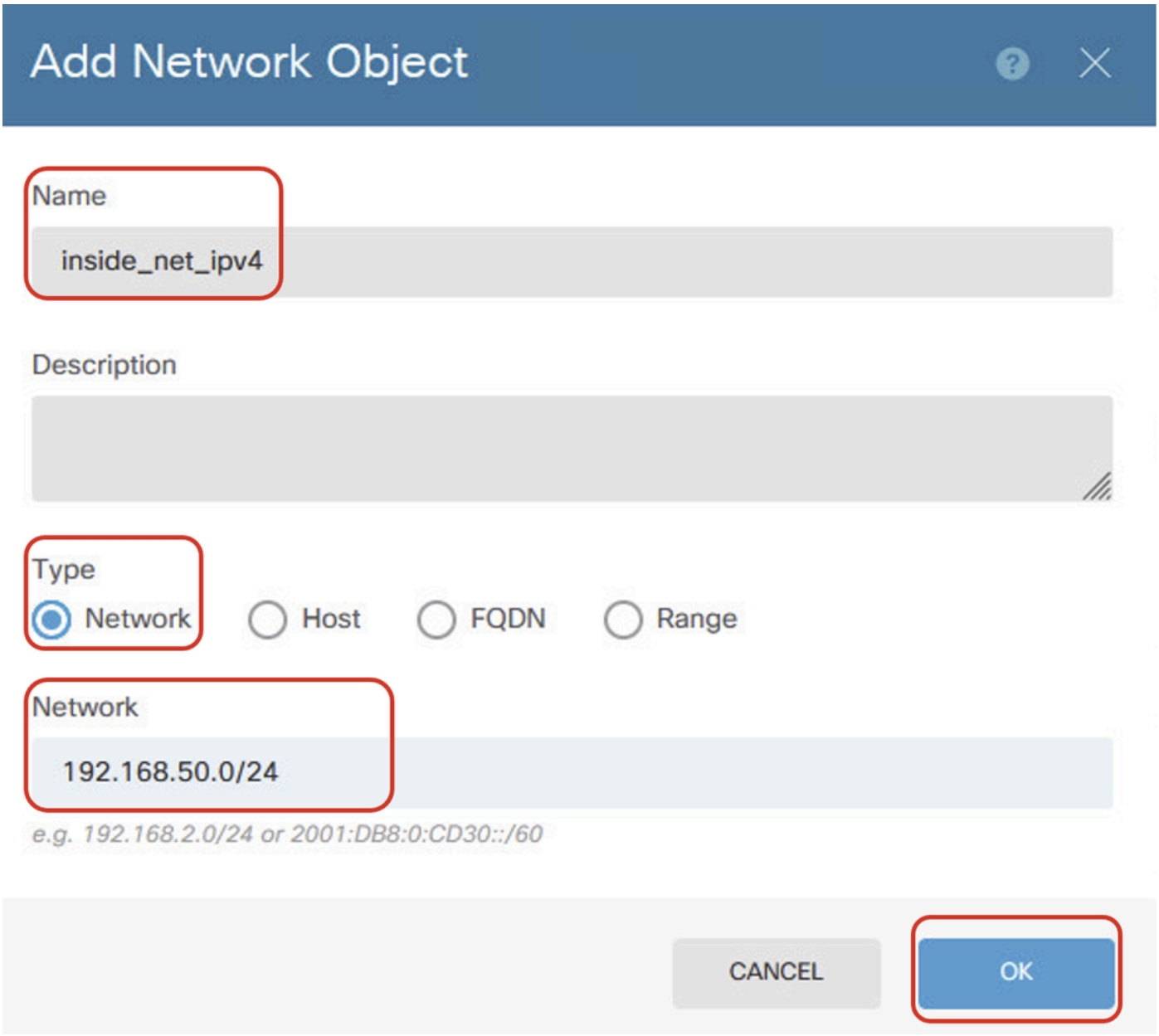


Create_NAT_Exempt_Network_1

5.2단계. 각 네트워크 객체의 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

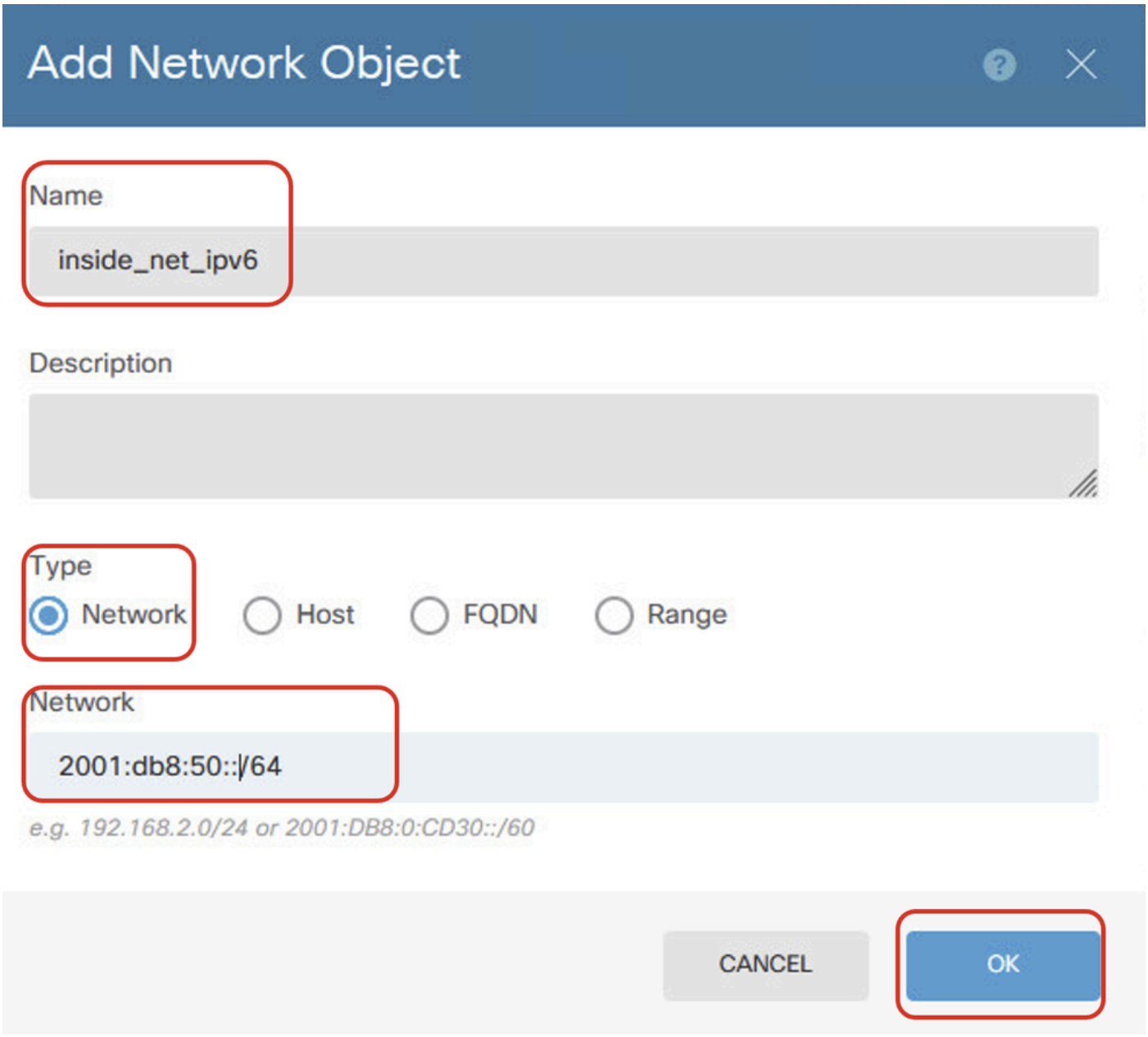
이 예에서는 IPv4 및 IPv6 네트워크가 모두 구성됩니다.

- 이름: inside_net_ipv4
- 유형: 네트워크
- 네트워크: 192.168.50.0/24



Create_NAT_Exempt_Network_2_IPv4

- 이름: inside_net_ipv6
- 유형: 네트워크
- 네트워크: 2001:db8:50::/64

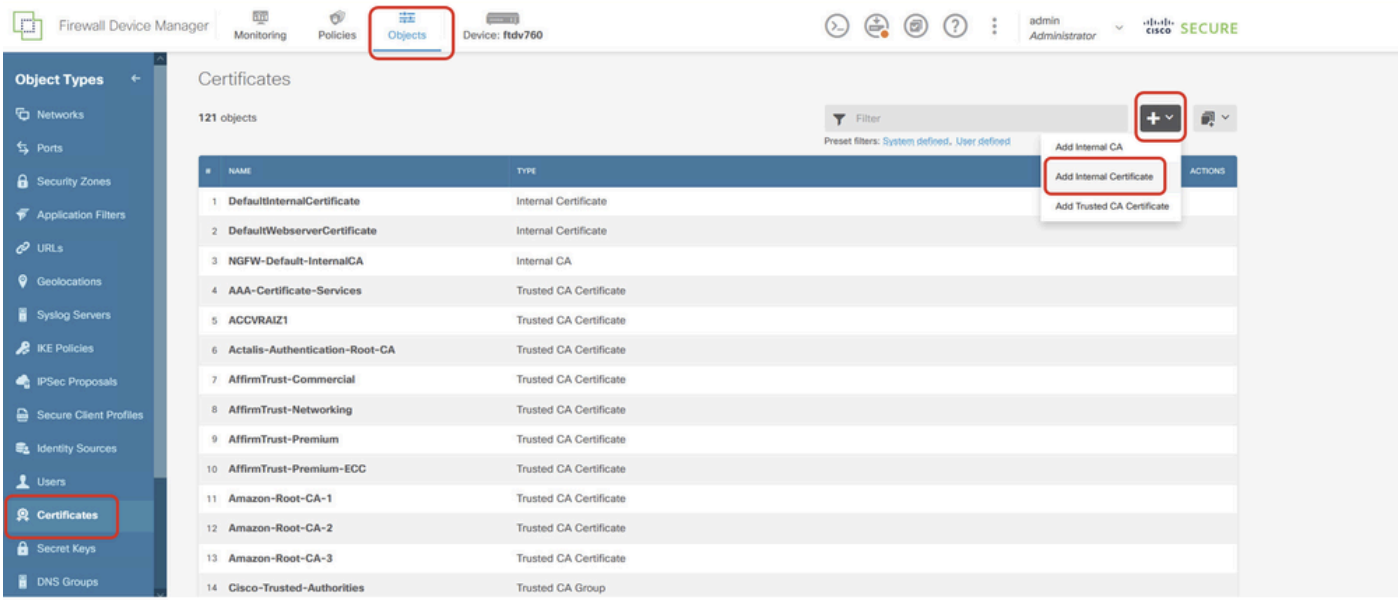


Create_NAT_Exempt_Network_2_IPv6

6단계. RAVPN에 사용되는 인증서를 생성합니다. 두 가지 옵션이 있습니다. 서드파티 CA(Certificate Authority)에서 서명한 인증서를 업로드하거나 새 자체 서명 인증서를 생성할 수 있습니다.

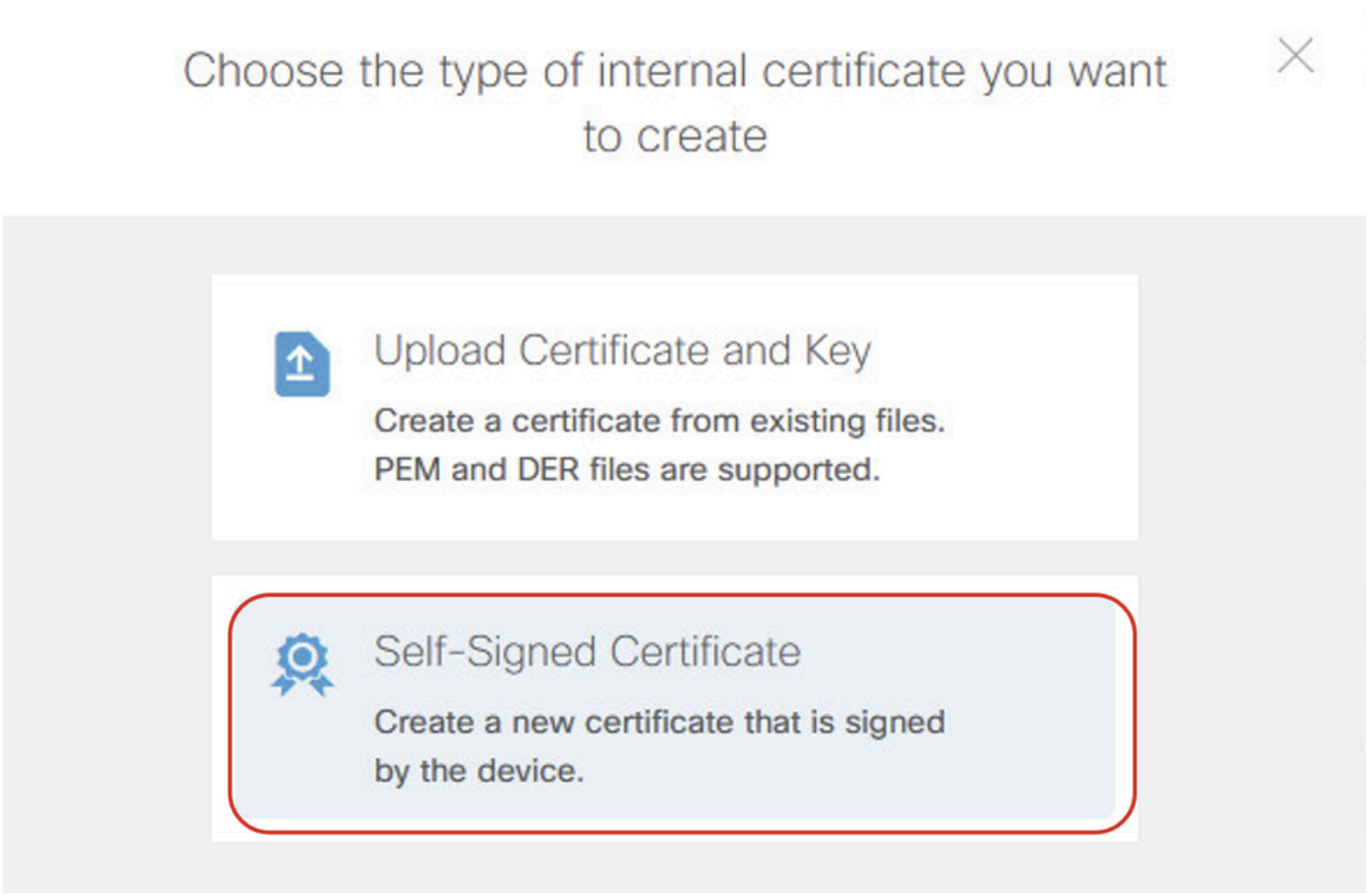
이 예에서는 새로운 자체 서명 인증서가 데모용으로 사용자 지정된 인증서 콘텐츠와 함께 사용됩니다.

6.1단계. Objects(개체) > Certificates(인증서)로 이동합니다. +버튼을 클릭하고 Add Internal Certificate(내부 인증서 추가)를 선택합니다.



Create_Certificate_1

6.2단계. Self-Signed Certificate를 클릭합니다.



6.3단계. 일반 탭을 클릭하고 필요한 정보를 제공합니다.

이름: 제거

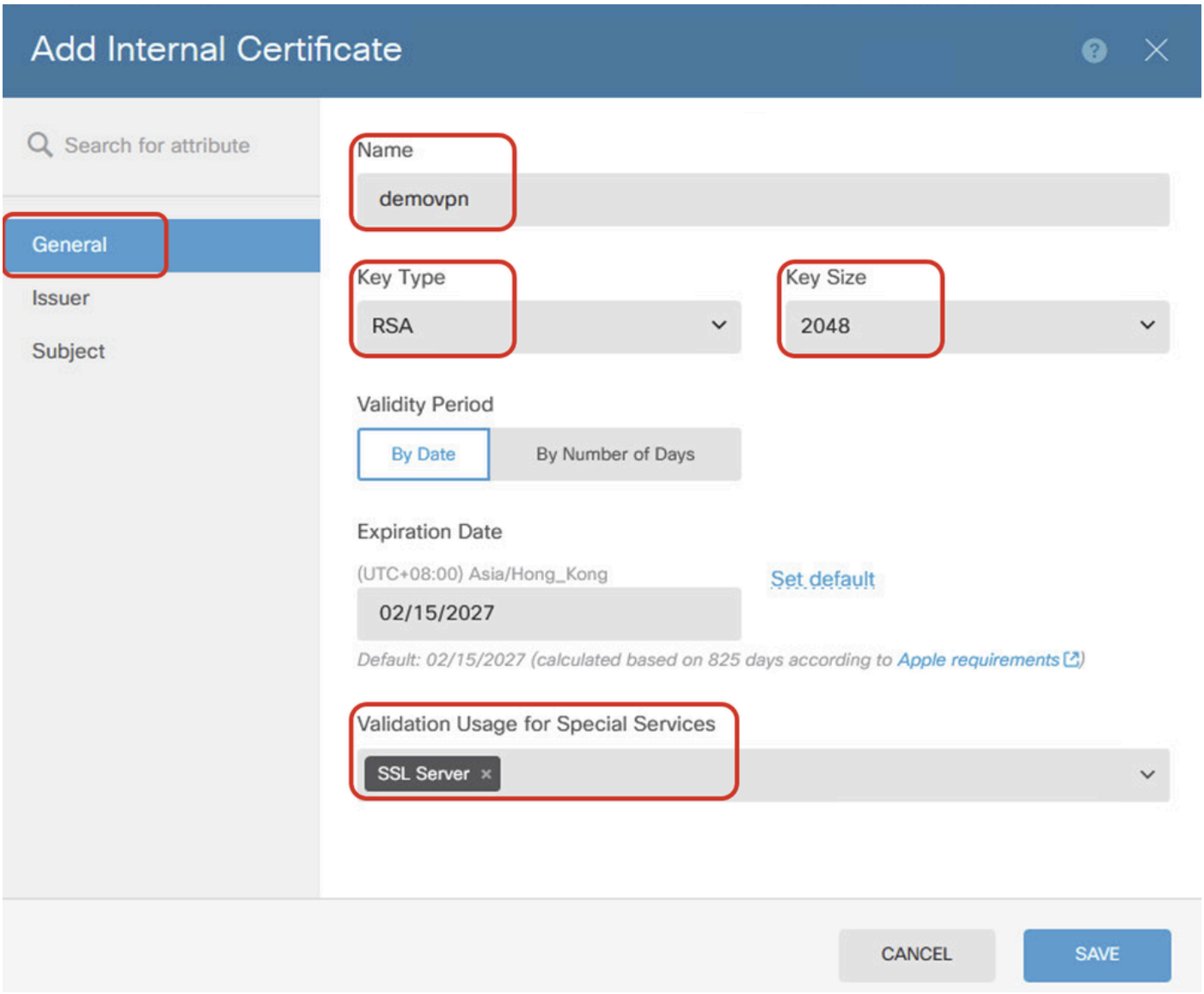
키 유형: RSA

키 크기: 2048

유효 기간: 기본값

만료 날짜: 기본값

특별 서비스에 대한 검증 사용: SSL 서버

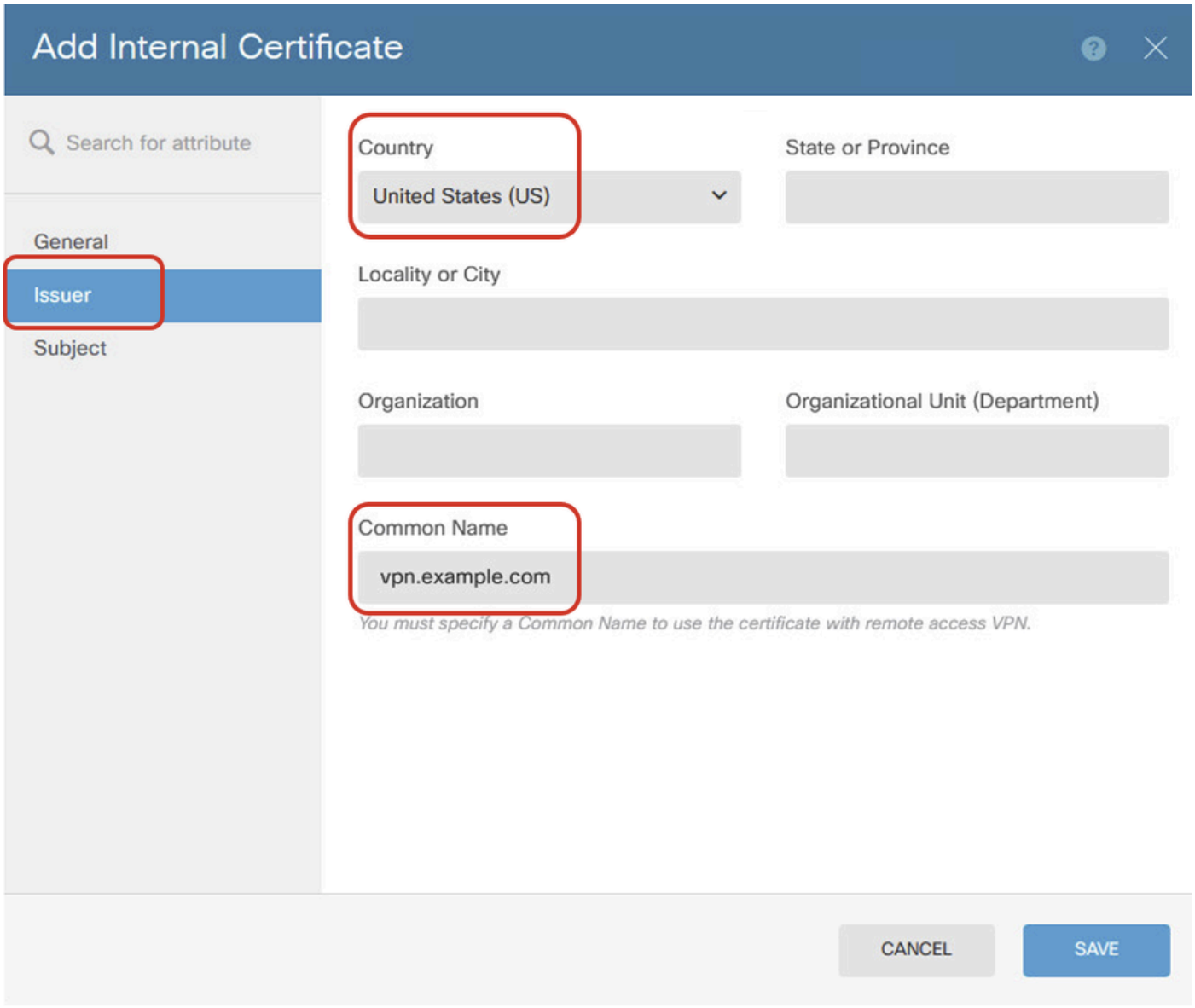


Create_Certificate_3

6.4단계. Issuer(발급자) 탭을 클릭하고 필요한 정보를 제공합니다.

국가: 미국(미국)

공용 이름: vpn.example.com

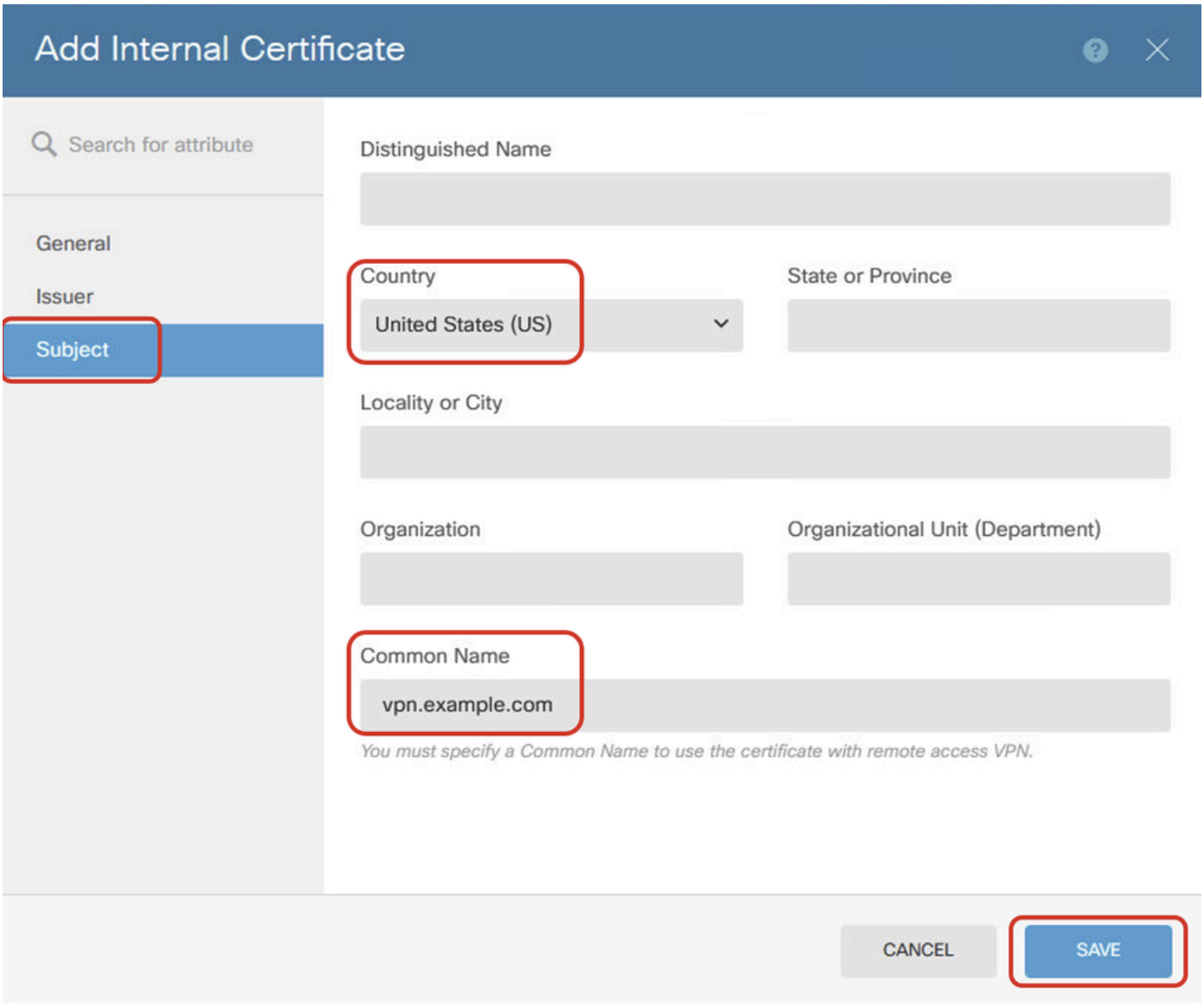


Create_Certificate_4

6.5단계. Subject(제목) 탭을 클릭하고 필요한 정보를 제공한 다음 SAVE(저장)를 클릭합니다.

국가: 미국(미국)

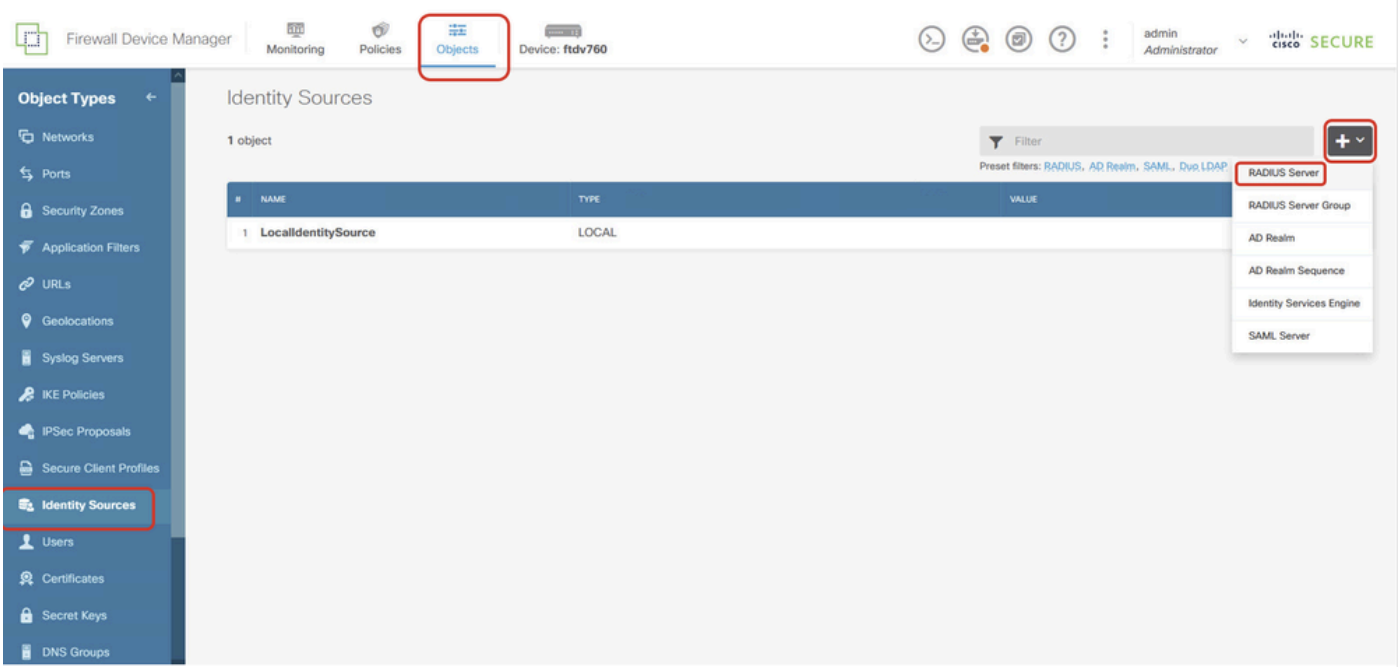
공용 이름: vpn.example.com



Create_Certificate_5

7단계. RADIUS 서버 ID 소스를 생성합니다.

7.1단계. Objects(개체) > Identity Sources(ID 소스)로 이동하고, +button을 클릭한 다음 RADIUS Server(RADIUS 서버)를 선택합니다.



Create_Radius_Source_1

7.2단계. RADIUS 서버의 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

이름: 데모_ise

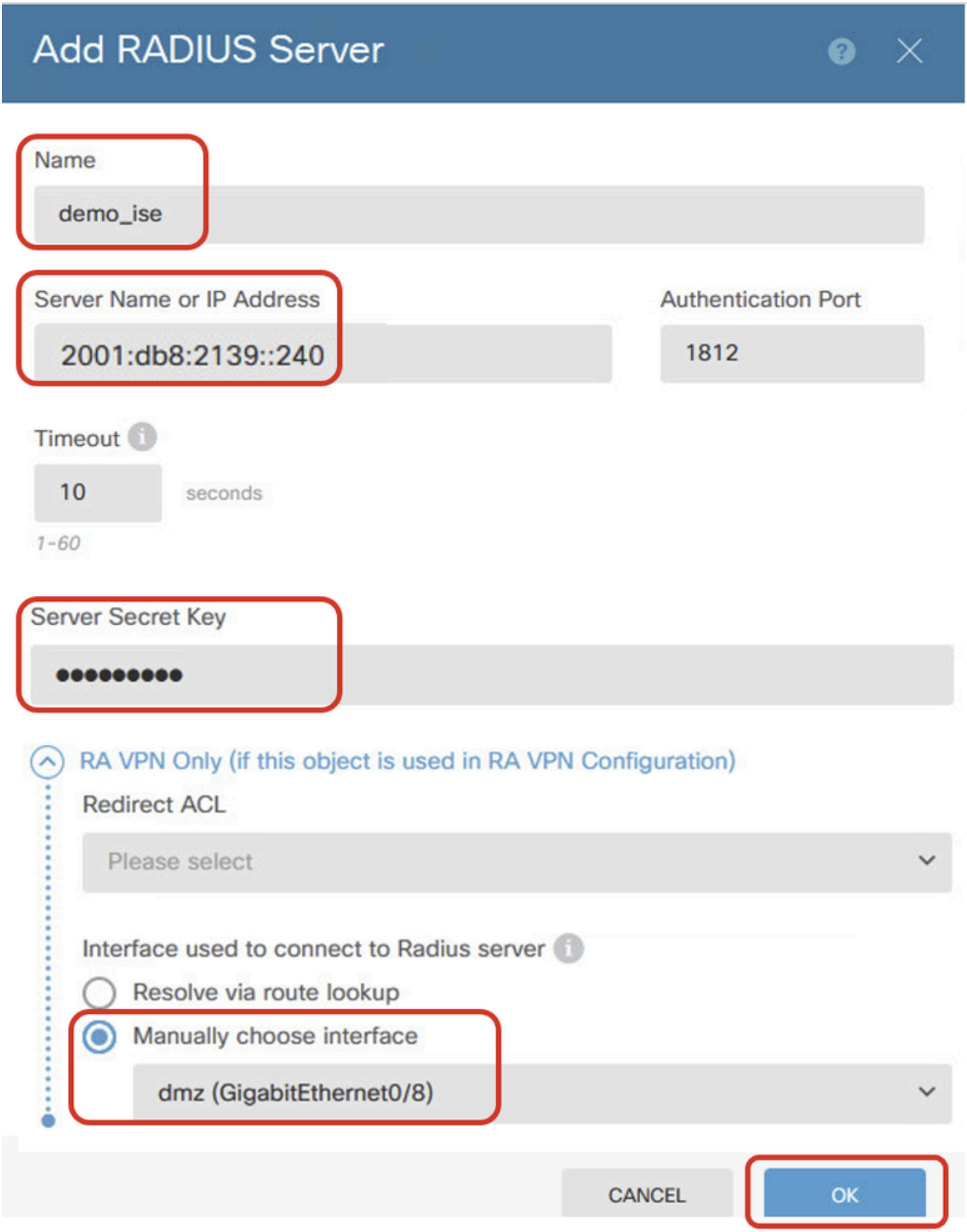
서버 이름 또는 IP 주소: 2001:db8:2139::240

인증 포트: 1812(기본값)

시간 초과: 10(기본값)

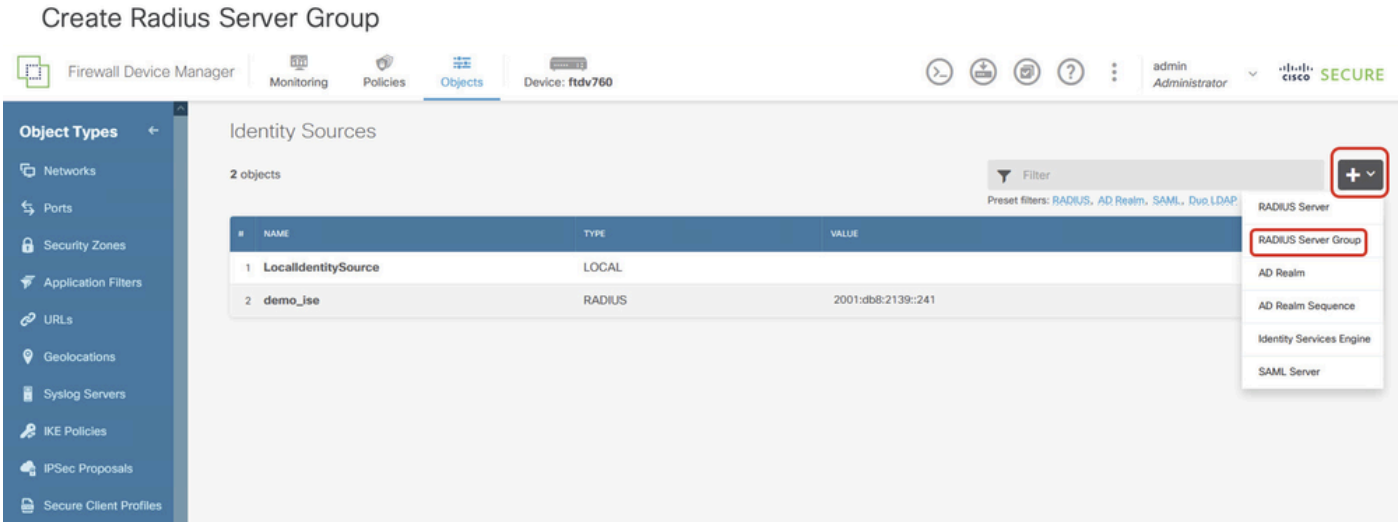
서버 암호 키: 시스코

Radius 서버에 연결하는 데 사용되는 인터페이스: 인터페이스를 수동으로 선택합니다. 이 예에서는 dmz(GigabitEthernet0/8)를 선택합니다.



Create_Radius_Source_2

7.3단계. Objects(객체) > Identity Sources(ID 소스)로 이동합니다. +버튼을 클릭하고 RADIUS 서버 그룹을 선택합니다.



Create_Radius_Source_3

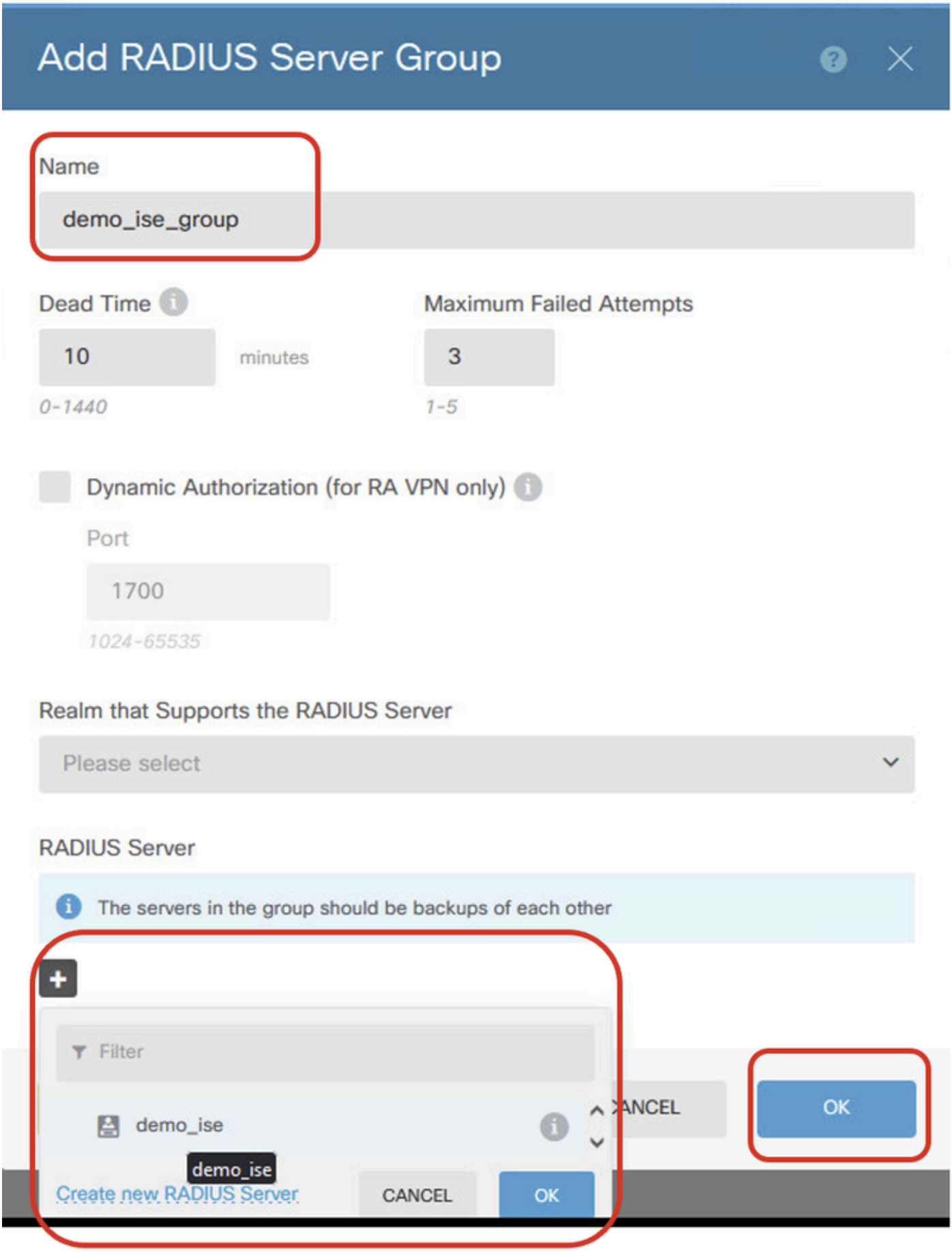
7.4단계. RADIUS 서버 그룹에 필요한 정보를 제공합니다. OK(확인) 버튼을 클릭합니다.

이름: demo_ise_group

Dead Time(데드 시간): 10(기본값)

최대 실패 시도 수: 3(기본값)

RADIUS 서버: +버튼을 클릭하고 6.2단계에서 생성한 이름을 선택합니다. 이 예에서는 demo_ise입니다.



Create_Radius_Source_4

8단계. RAVPN에 사용되는 그룹 정책을 생성합니다. 이 예에서는 데모용으로 사용자 지정 배너 및 시간 초과 설정이 구성됩니다. 실제 요구 사항에 따라 수정할 수 있습니다.

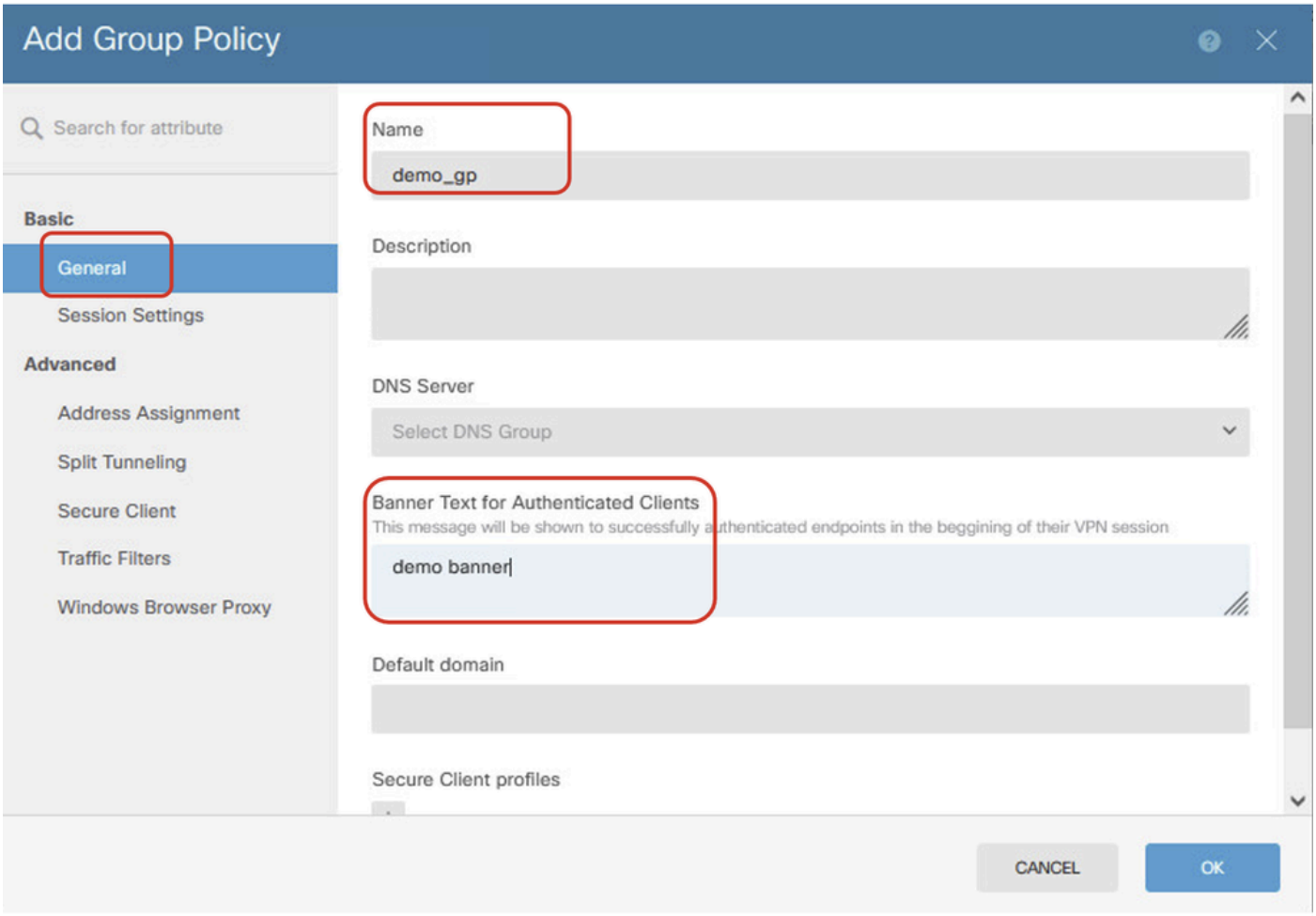
8.1단계. Remote Access VPN(원격 액세스 VPN) > View Configuration(컨피그레이션 보기)으로 이동합니다. 왼쪽 사이드바에서 Group Policies(그룹 정책)를 클릭한 다음 + 버튼을 클릭합니다.

Create_Group_Policy_1

8.2단계. General(일반)을 클릭하고 필요한 정보를 제공합니다.

이름: 데모_그룹

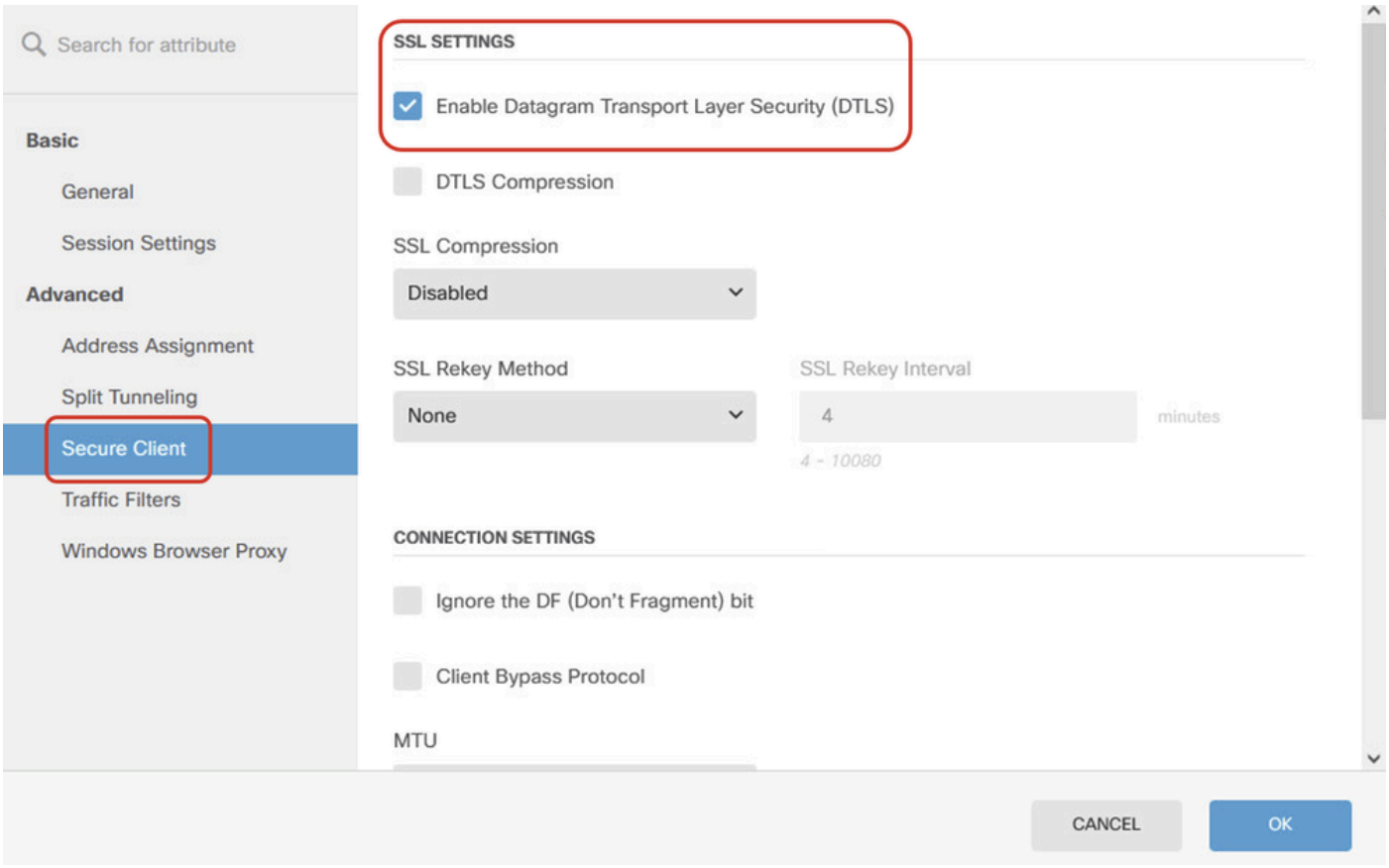
인증된 클라이언트에 대한 배너 텍스트: 데모 배너



Create_Group_Policy_2

8.3단계. Secure Client(클라이언트 보안)를 클릭하고 필요한 정보를 제공합니다.

Enable Datagram Transport Layer Security (DTLS)(DTLS(데이터그램 전송 계층 보안) 활성화)를 선택합니다.

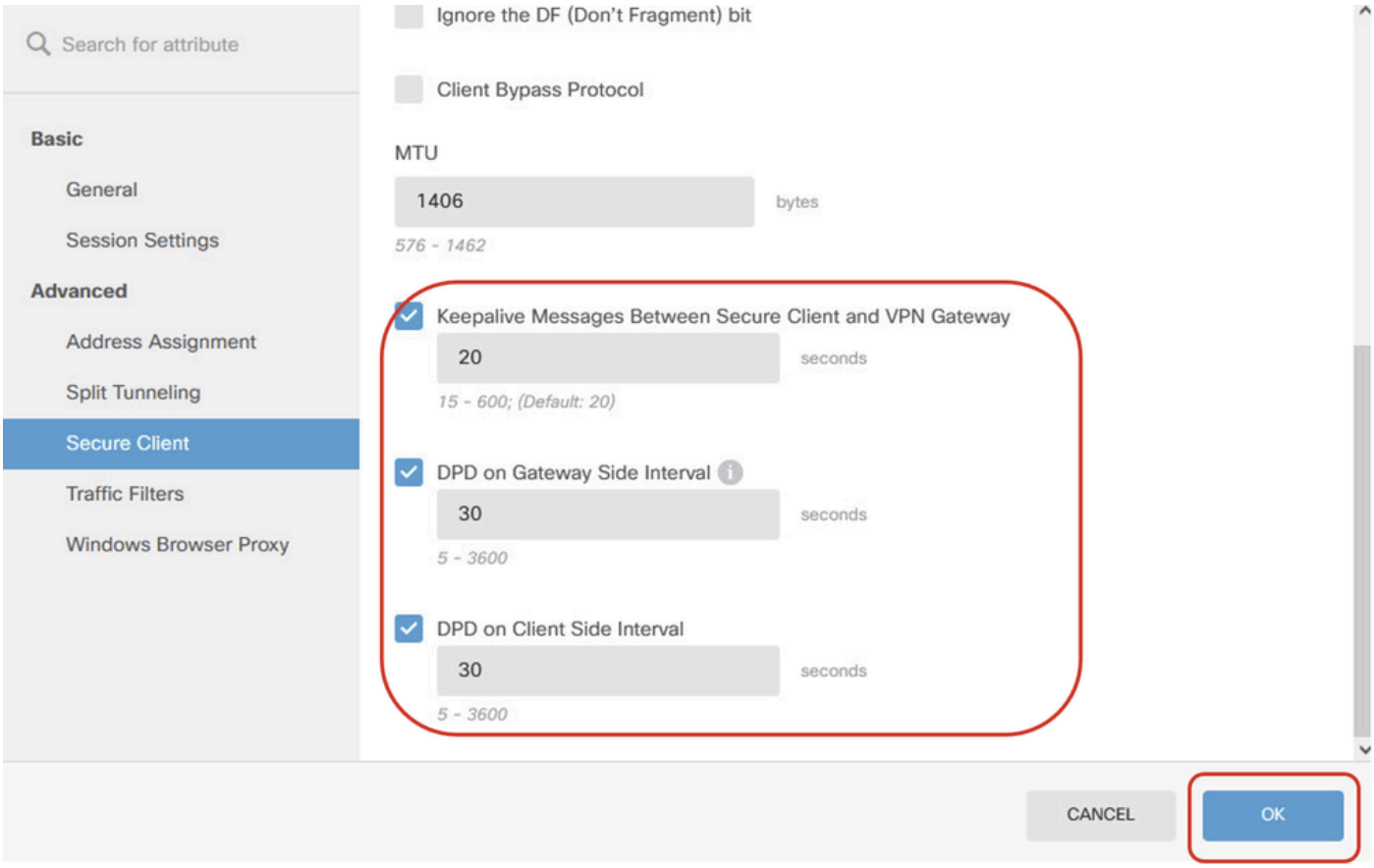


Create_Group_Policy_3

Keepalive Messages Between Secure Client and VPN Gateway(기본값)를 선택합니다.

Gateway Side Interval(게이트웨이 측 간격)에서 DPD를 선택합니다(기본값).

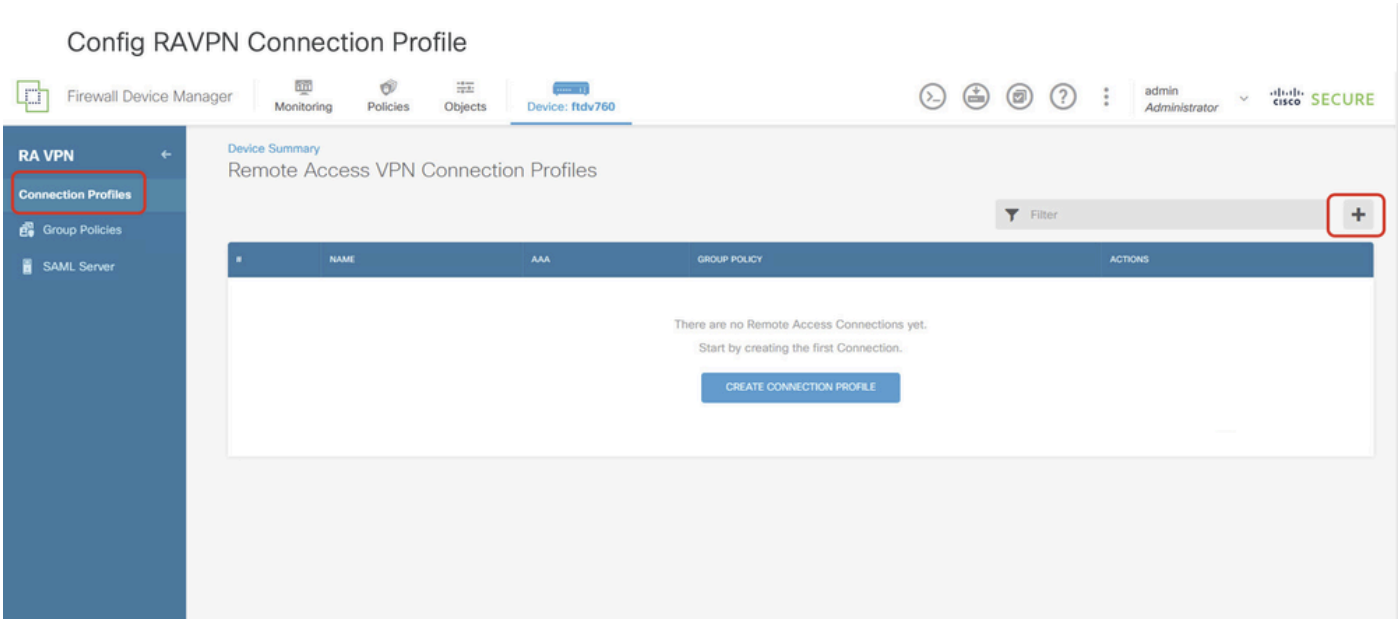
Client Side Interval(클라이언트 측 간격)에서 DPD를 선택합니다(기본값).



Create_Group_Policy_3_계속

9단계. RAVPN 연결 프로파일을 생성합니다.

9.1단계. Remote Access VPN(원격 액세스 VPN) > View Configuration(컨피그레이션 보기)으로 이동합니다. 왼쪽 사이드바에서 Connection Profile(연결 프로파일)을 클릭한 다음 + 버튼을 클릭하여 마법사를 시작합니다.



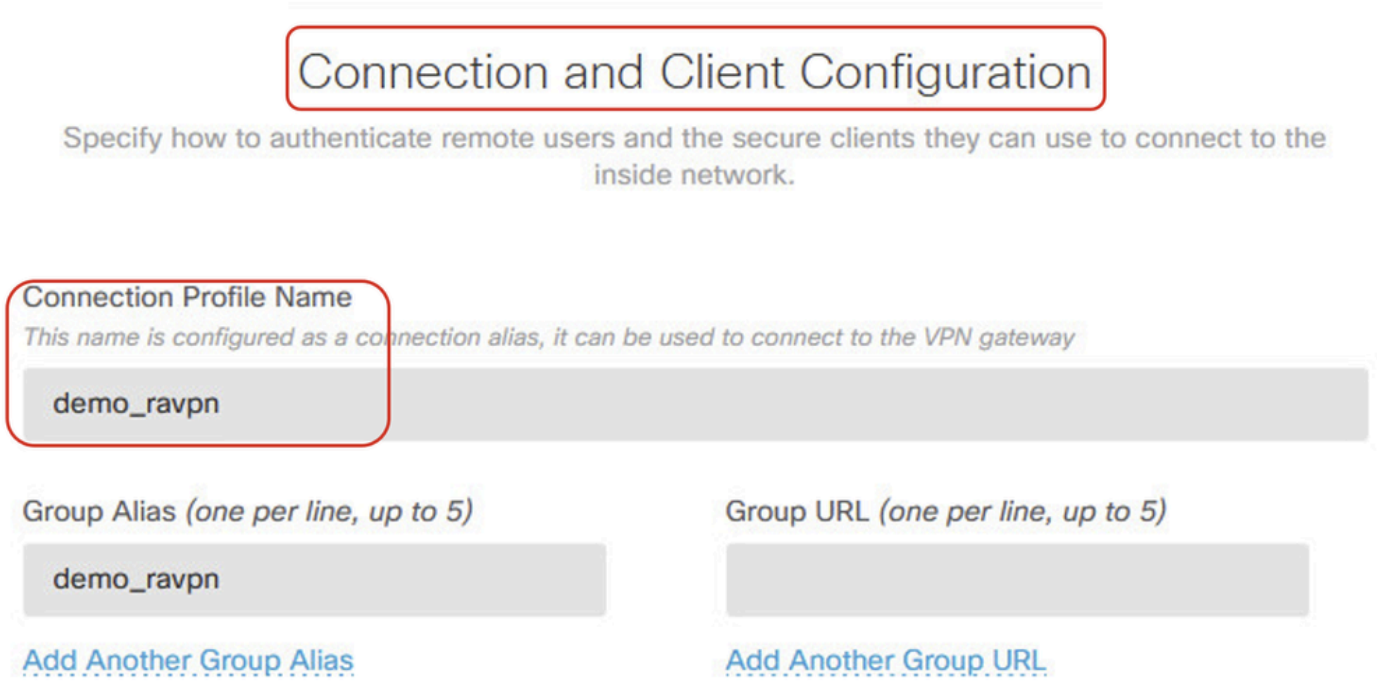
Create_RAVPN_Wizard_1

9.2단계. Connection and Client Configuration(연결 및 클라이언트 컨피그레이션) 섹션에서 필요한

정보를 제공하고 NEXT(다음) 버튼을 클릭합니다.

연결 프로파일 이름: demo_ravpn

그룹 별칭: demo_ravpn



Create_RAVPN_Wizard_2_Conn_Name

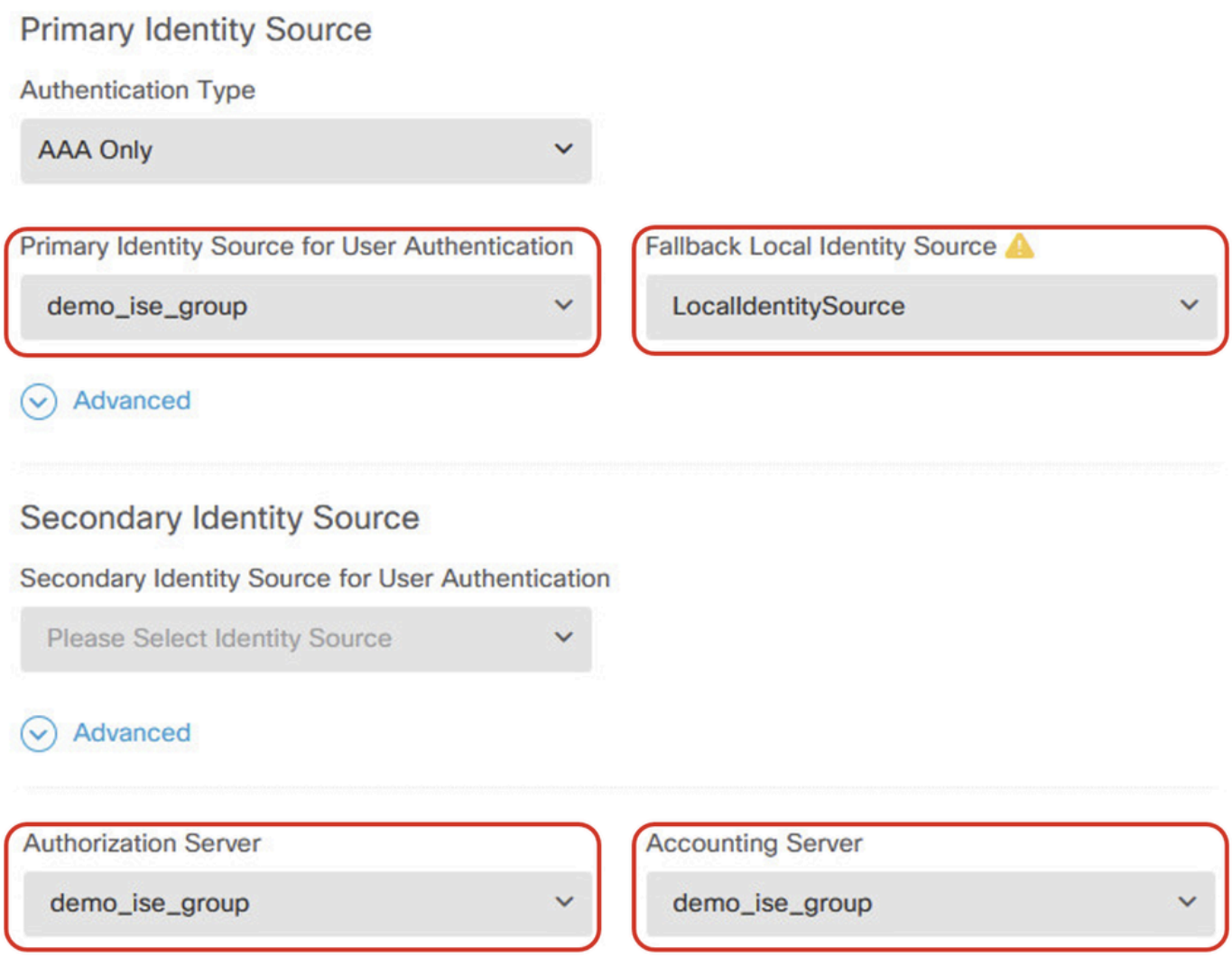
기본 ID 소스 > 인증 유형: AAA만

Primary Identity Source(기본 ID 소스) > Primary Identity Source(기본 ID 소스): demo_ise_group(7.4단계에서 구성된 이름)

대체 로컬 ID 원본: 로컬 ID 소스

권한 부여 서버: demo_ise_group(7.4단계에서 구성된 이름)

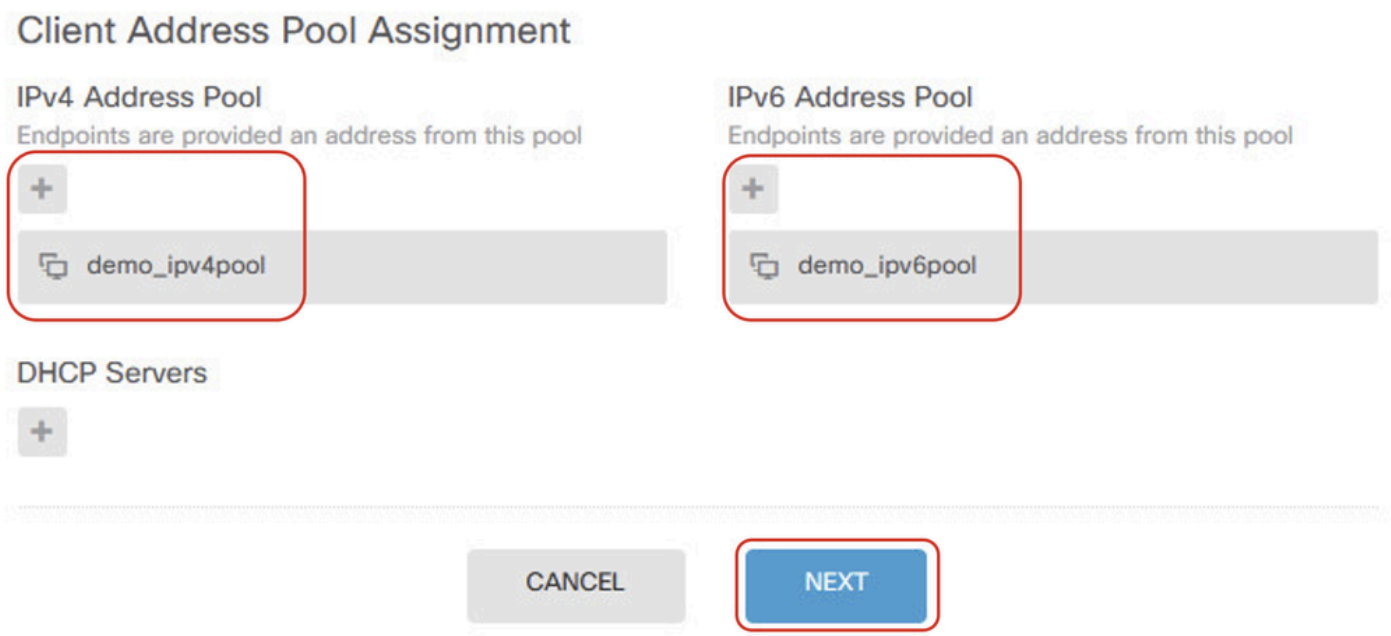
어카운팅 서버: demo_ise_group(7.4단계에서 구성된 이름)



Create_RAVPN_Wizard_2_Identity_Source

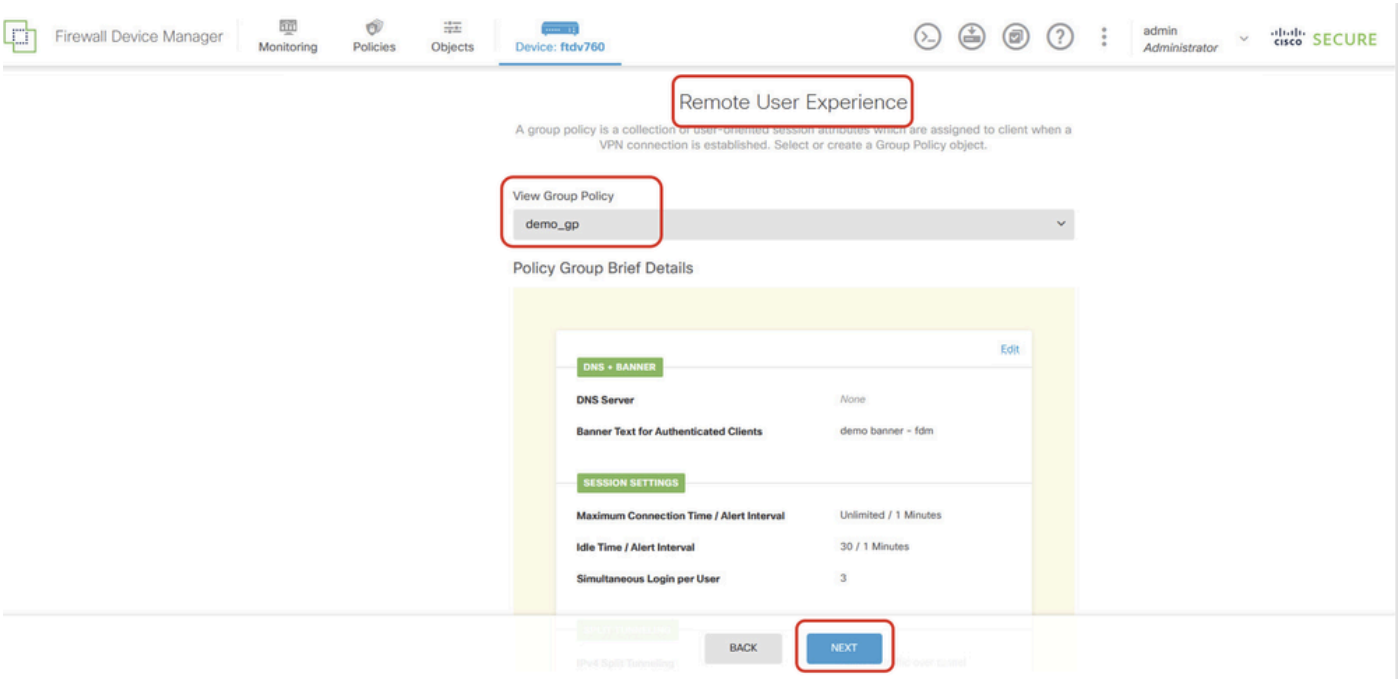
IPv4 주소 풀: demo_ipv4pool(4.2단계에서 구성된 이름)

IPv6 주소 풀: demo_ipv6pool(4.2단계에서 구성된 이름)



Create_RAVPN_Wizard_2_Address_Pool

9.3단계. 8.2단계에서 구성한 그룹 정책을 Remote User Experience(원격 사용자 환경) 섹션에서 선택하고 NEXT(다음) 버튼을 클릭합니다.

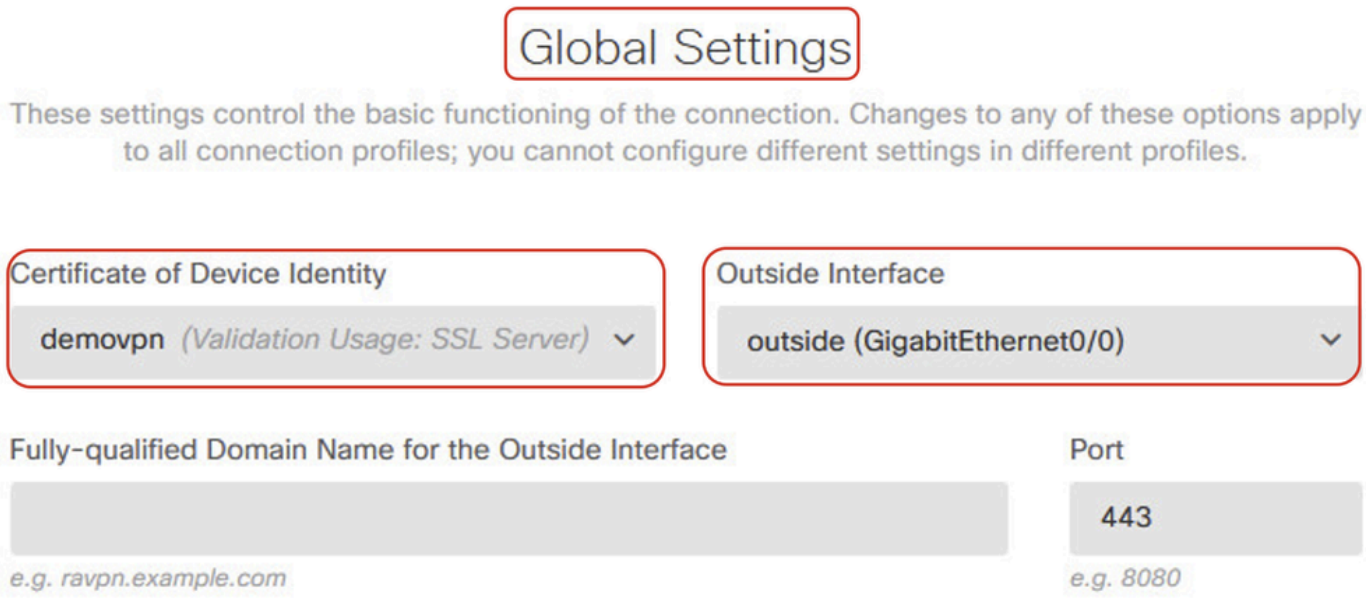


Create_RAVPN_Wizard_3

9.4단계. Global Setting(전역 설정) 섹션에 필요한 정보를 입력하고 NEXT(다음) 버튼을 클릭합니다
.

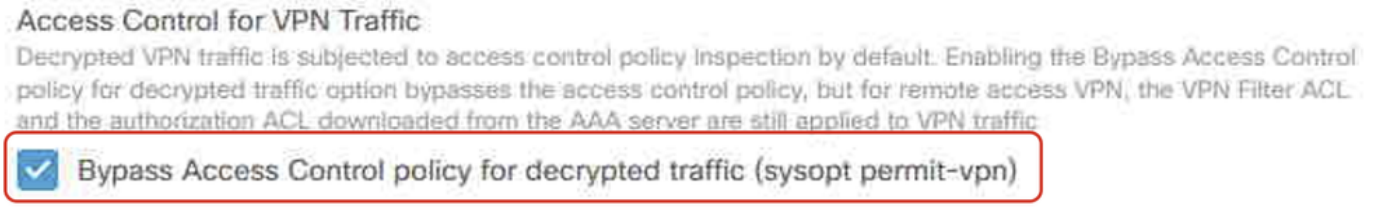
디바이스 ID 인증서: demovpn(6.3단계에서 구성된 이름)

외부 인터페이스: 외부



Create_RAVPN_Wizard_4

VPN 트래픽에 대한 액세스 제어: 암호 해독된 트래픽에 대한 Bypass Access Control policy(액세스 제어 정책 우회)를 선택합니다(sysopt permit-vpn).

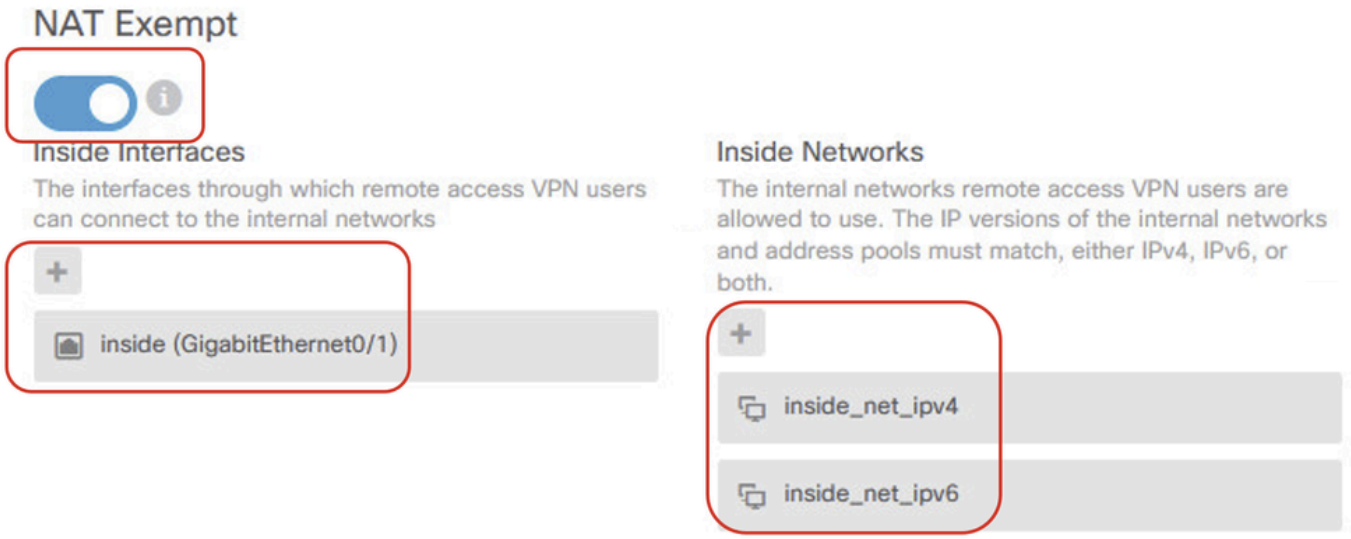


Create_RAVPN_Wizard_4_VPN_ACP

NAT 제외: Enabled(활성화됨) 위치에 있는 슬라이더를 클릭합니다

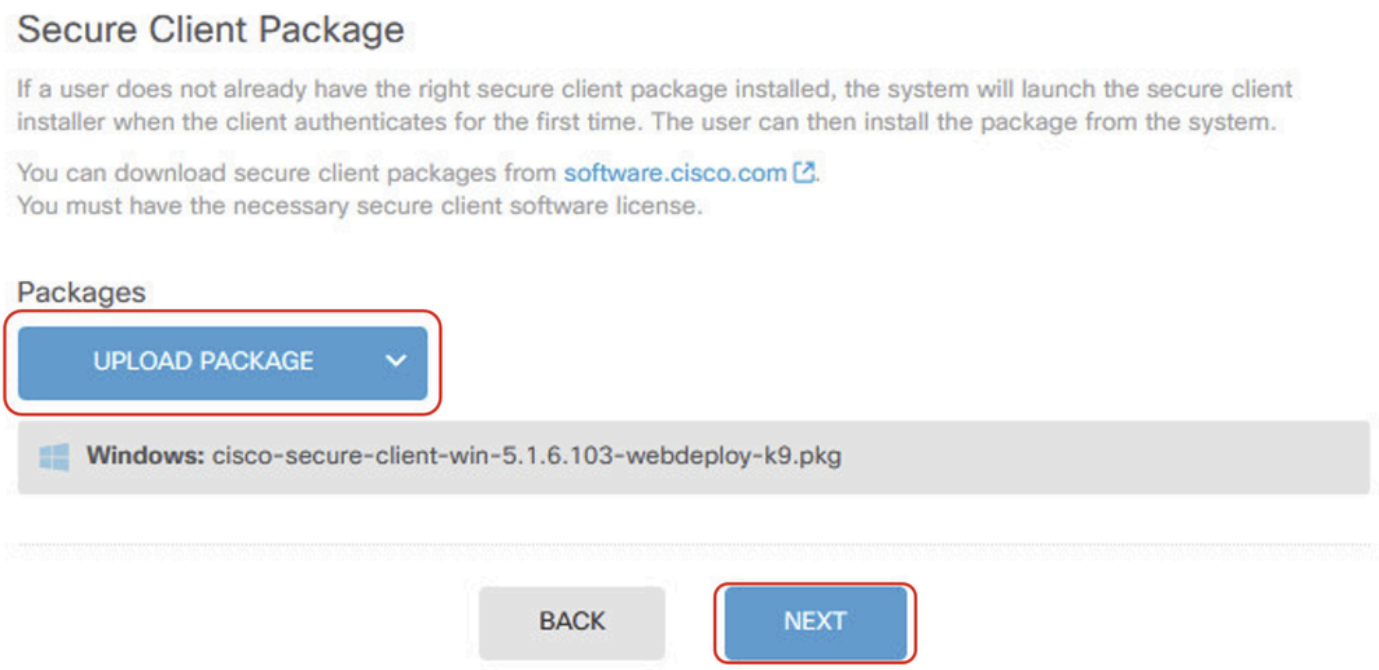
내부 인터페이스: 안쪽에

내부 네트워크: inside_net_ipv4, inside_net_ipv6(5.2단계에서 구성한 이름)



Create_RAVPN_Wizard_4_VPN_NATExempt

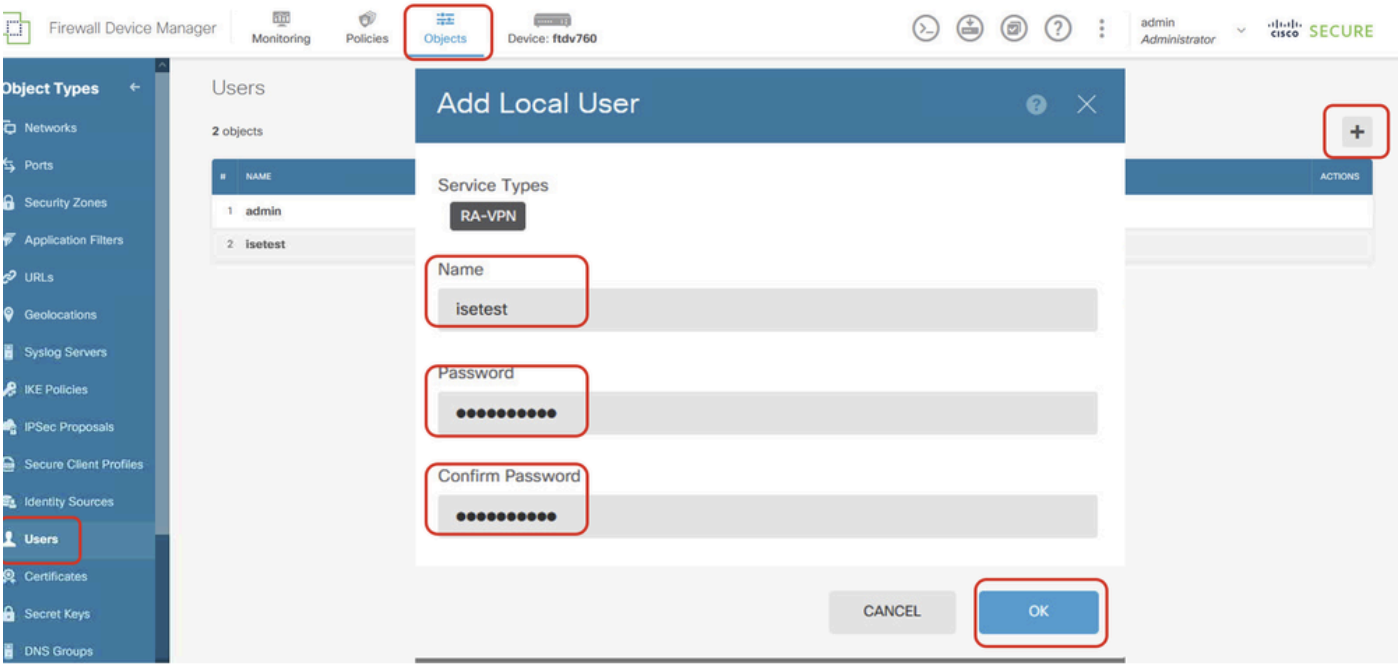
보안 클라이언트 패키지: UPLOAD PACKAGE(패키지 업로드)를 클릭하고 패키지를 적절히 업로드합니다. 이 예에서는 Windows 패키지가 업로드됩니다.



Create_RAVPN_Wizard_4_Image

9.5단계. 요약을 검토합니다. 수정해야 할 사항이 있으면 BACK(뒤로) 버튼을 클릭합니다. 모든 것이 정상인 경우 FINISH(마침) 버튼을 클릭합니다.

10단계. 9.2단계에서 LocalIdentitySourcein과 함께 Fallback Local Identity Source(로컬 ID 소스 대체)를 선택한 경우 로컬 사용자를 생성합니다. 로컬 사용자의 비밀번호는 ISE에 구성된 비밀번호와 동일해야 합니다.



Create_Local_User

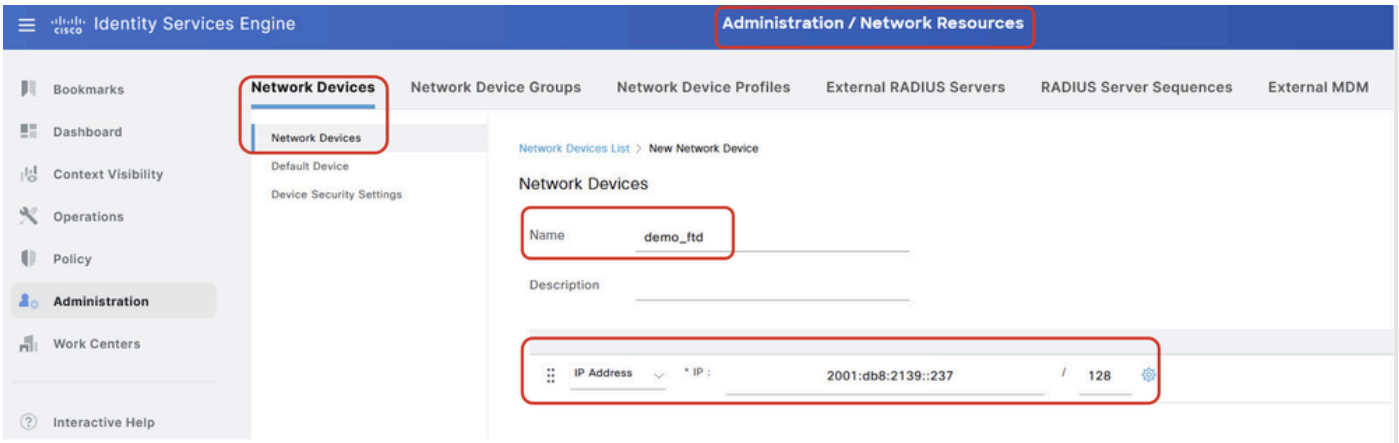
11단계. 구성 변경 사항을 배포합니다.

배포_변경

ISE의 컨피그레이션

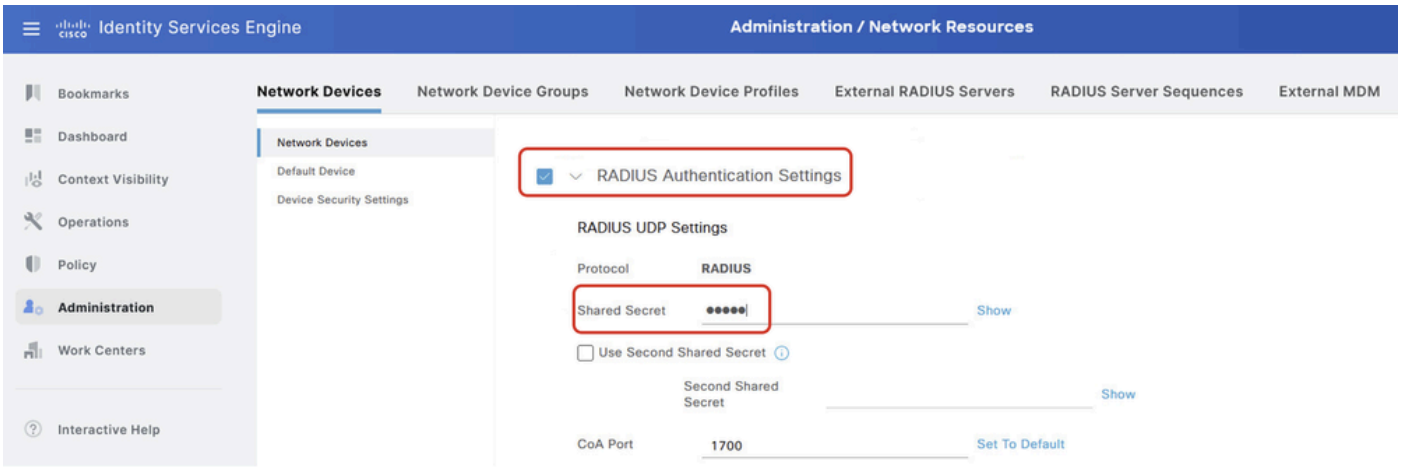
12단계. 네트워크 디바이스를 생성합니다.

12.1단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고, Add(추가)를 클릭하고, Name(이름), IP Address(IP 주소)를 입력한 후 페이지를 아래로 스크롤합니다.



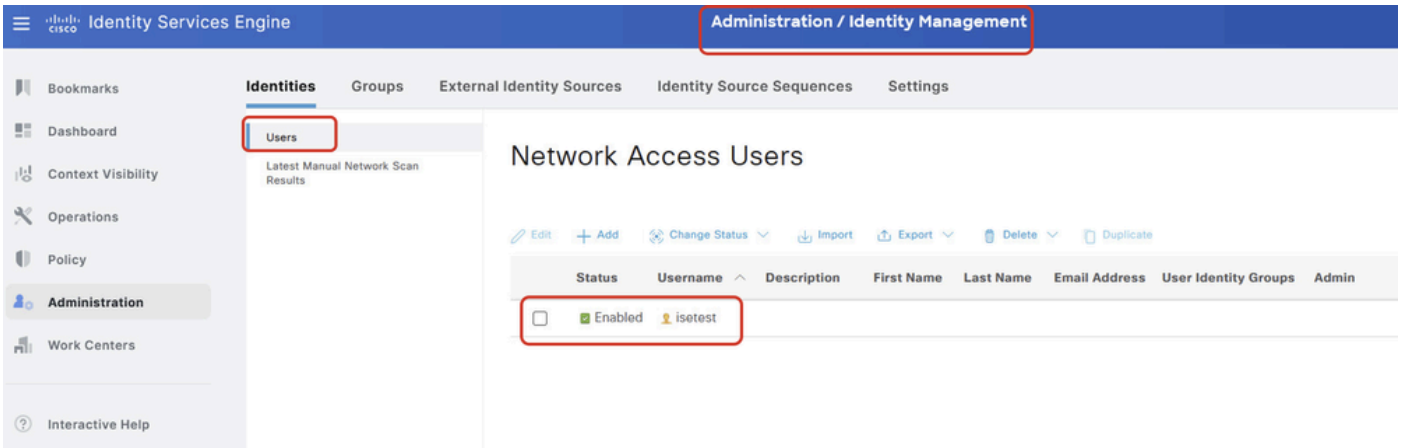
Create_Network_Devices

12.2단계. RADIUS Authentication Settings(RADIUS 인증 설정)의 확인란을 선택합니다. 공유 암호를 입력하고 Submit(제출)을 클릭합니다.



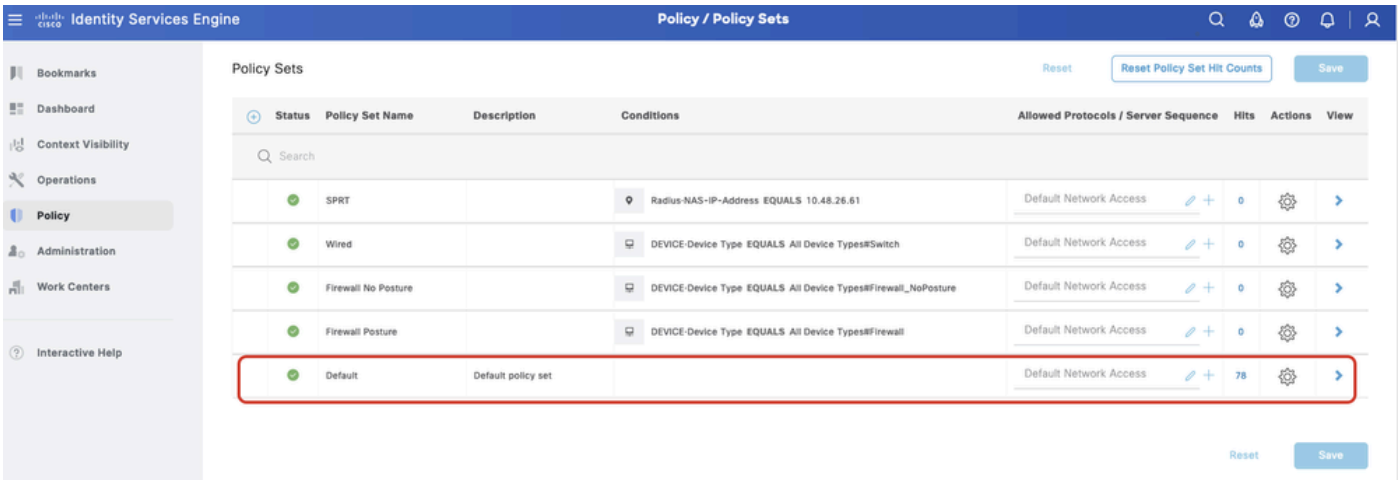
Create_Network_Devices_계속

13단계. 네트워크 액세스 사용자를 생성합니다. Administration(관리) > Identity Management(ID 관리) > Identities(ID)로 이동합니다. 새 사용자를 생성하려면 Add(추가)를 클릭합니다. 비밀번호는 10단계에서 생성된 FDM 로컬 사용자와 동일합니다. 이는 대체가 제대로 작동하도록 하기 위한 것입니다.



사용자 만들기(_U)

14단계(선택 사항) 사용자 지정 인증 규칙 및 권한 부여 규칙을 사용하여 새 정책 집합을 생성합니다. 이 예에서는 기본 정책 집합이 데모용으로 사용됩니다.

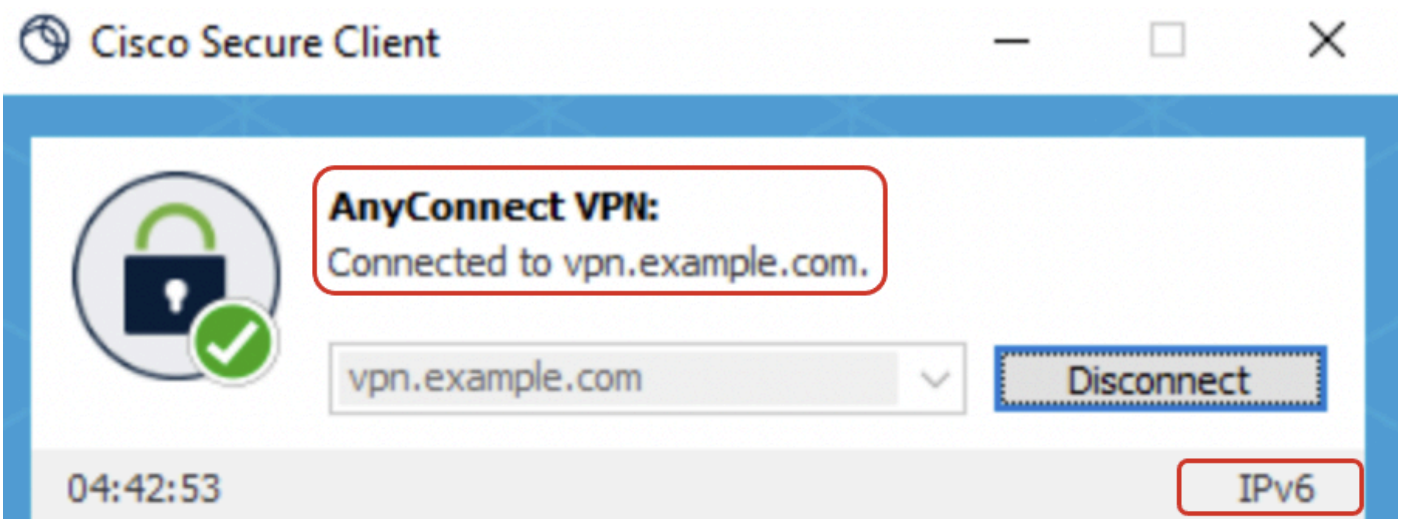


ISE_Default_Policy_Set

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

15단계. 클라이언트에서 IPv6 주소를 통해 VPN 게이트웨이를 연결합니다. VPN 연결에 성공했습니다.



Verify_Connection_Succeeded

16단계. SSH 또는 콘솔을 통해 FTD의 CLI로 이동합니다. show vpn-sessiondb detail anyconnect 명령을 FTD(Lina) CLI에서 실행하여 VPN 세션 세부사항을 확인합니다.

```
<#root>

ftdv760# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

Username : isetest

Index : 2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

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 : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 2.1

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
```

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : 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 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10
```

17단계. 클라이언트에 대한 Ping 테스트입니다. 이 예에서 클라이언트는 서버의 IPv4 및 IPv6 주소를 모두 성공적으로 Ping합니다.

Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 2001:db8:50::20

Pinging 2001:db8:50::20 with 32 bytes of data:
Request timed out.
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=3ms

Ping statistics for 2001:db8:50::20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Select Command Prompt

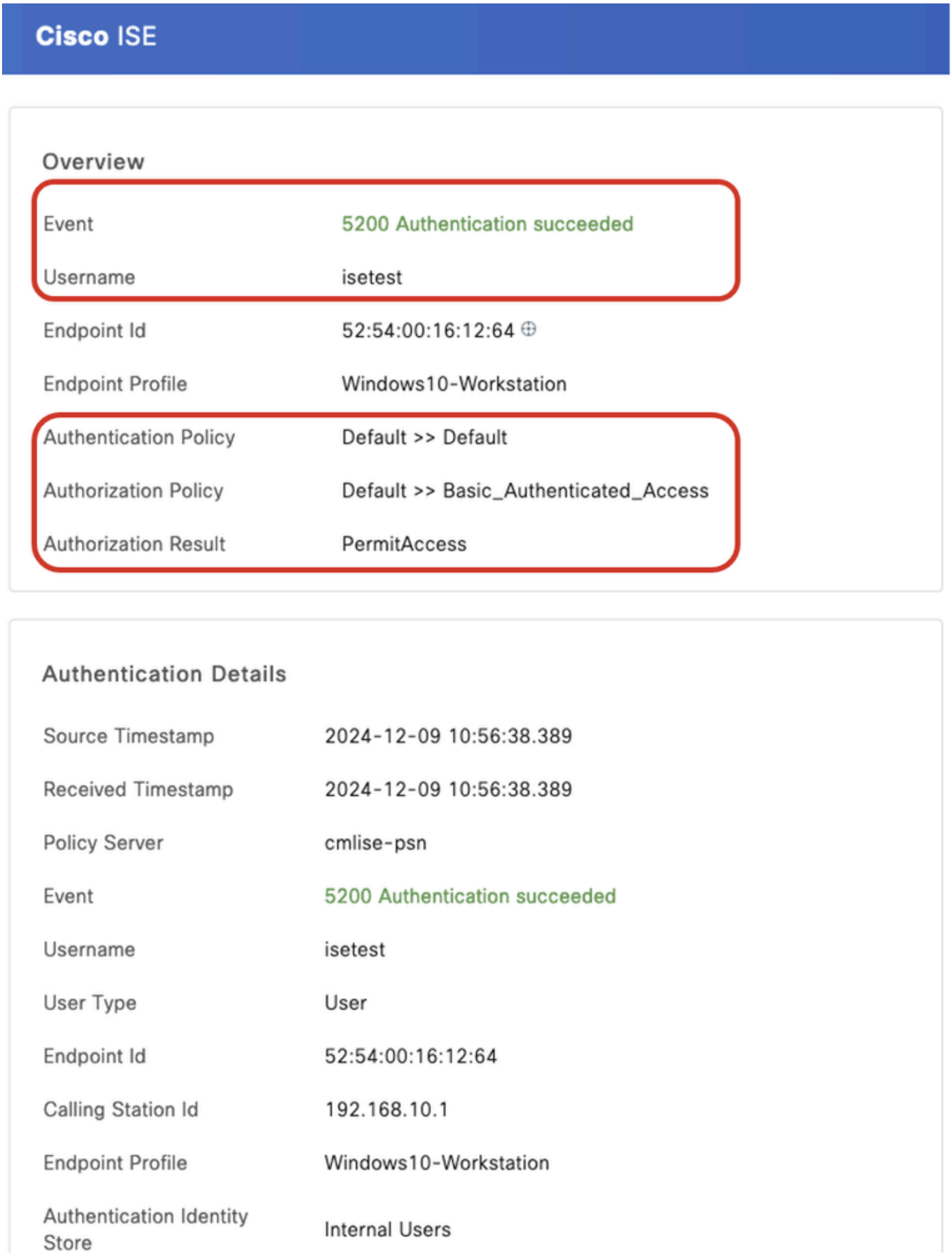
```
C:\Users\admin>
C:\Users\admin>ping 192.168.50.20

Pinging 192.168.50.20 with 32 bytes of data:
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.50.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Verify_Cisco_Secure_Client_Ping

18단계. ISE radius 라이브 로그에 성공적인 인증이 표시됩니다.



ISE_Authentication_Success_Log

19단계. 테스트 FTD 인증은 FTD가 ISE에 연결할 수 없을 때 LOCAL로 이동합니다.

19.1단계. FTD 인증이 ISE로 이동하면 FTD (Lina) CLI에서 show aaa-server 명령을 실행하여 통계를 확인합니다.

이 예에서는 LOCAL에 대한 카운터가 없으며 인증은 RADIUS 서버로 전달됩니다.

<#root>

```
ftdv760# show aaa-server

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius


Server Address:  2001:db8:2139::240


Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           1  <== Increased


Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

19.2단계. ISE 인터페이스를 종료하여 FTD가 ISE에서 응답을 수신할 수 없음을 시뮬레이션합니다.

<#root>

```
ftdv760# ping 2001:db8:2139::240


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:
???
Success rate is 0 percent (0/3)
```

19.3단계. 클라이언트가 VPN 연결을 시작하고 10단계에서 생성한 동일한 사용자 이름 비밀번호를 입력하면 VPN 연결은 계속 성공합니다.

통계를 확인하기 위해 FTD(Lina) CLI에서 명령 show aaa-server를 다시 실행하면 LOCAL에 대한 인증, 권한 부여 및 수락 카운터가 증가했습니다. RADIUS 서버에 대한 허용 카운터가 증가하지 않았습니다.

<#root>

```
ftdv760# show aaa-server
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 0ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           0
Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius

Server Address:  2001:db8:2139::240
Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms
Number of authentication requests       2
```

```
Number of authorization requests        1
Number of accounting requests           6
Number of retransmissions               0

Number of accepts                       2  <== Not increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      6
Number of unrecognized responses        0
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

VPN 섹션의 문제를 해결하려면 FTD Lina에서 이러한 명령을 실행할 수 있습니다.

```
debug webvpn 255
debug webvpn anyconnect 255
```

VPN 문제 해결을 위해 클라이언트에서 DART 파일을 수집하여 보안 클라이언트에 문제가 있는지 확인할 수 있습니다. 자세한 내용은 관련 CCO 문서 Collect [DART Bundle for Secure Client를 참조하십시오](#).

Radius 섹션의 문제를 해결하려면 FTD Lina에서 이러한 명령을 실행할 수 있습니다.

```
ftdv760# debug radius ?

all      All debug options
decode   Decode debug option
dynamic-authorization CoA listener debug option
session  Session debug option
user     User debug option
<cr>
```

```
ftdv760# debug aaa ?

accounting
authentication
authorization
common
condition
internal
shim
url-redirect
```

<cr>

VPN 연결이 성공적으로 완료된 후 트래픽 관련 문제를 해결하려면 이러한 내용을 검토할 수 있습니다.

1. FTD Lina의 트래픽을 캡처하여 Lina가 트래픽을 삭제하는지 확인합니다(이 CCO 문서 참조). Firepower Threat Defense 캡처 및 패킷 추적기 사용 - Cisco.
2. 암호 해독된 트래픽에 대한 Bypass Access Control(액세스 제어 우회) 정책이 비활성화된 경우 관련 VPN 트래픽이 통과하도록 허용되는지 확인하려면 액세스 제어 정책을 검토합니다.
3. VPN 트래픽이 NAT에서 제외되는지 확인하려면 NAT 제외를 검토합니다.

관련 정보

- RAVPN의 FDM 컨피그레이션 가이드 - Cisco
- Secure Client용 DART 번들 수집 - Cisco
- firepower Threat Defense 캡처 및 패킷 추적기 사용 - Cisco
- Cisco Secure Client 문제 해결 - Cisco
- Cisco 기술 지원 및 다운로드

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.