ASA에서 AnyConnect 관리 VPN 터널 설정

목차

소개

이 문서에서는 VPN 게이트웨이가 Cisco AnyConnect Secure Mobility Client에서 관리 VPN 터널을 통한 연결을 수락할 때 ASA를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASDM(Adaptive Security Device Manager)을 통한 VPN 구성
- 기본 ASA(Adaptive Security Appliance) CLI 컨피그레이션
- X509 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.12(3)9
- Cisco ASDM 소프트웨어 버전 7.12.2
- Windows 10(Cisco AnyConnect Secure Mobility Client 버전 4.8.03036)

참고: AnyConnect VPN 웹 배포 패키지(anyconnect-win*.pkg or anyconnect-macos*.pkg) Cisco Software Download(등록된 고객만 해당) AnyConnect VPN 클라이언트를 원격 사용자 컴퓨터에 다운로드할 ASA의 플래시 메모리에 복사하여 ASA와의 SSL VPN 연결을 설정합니다. 자세한 내

용은 ASA 컨피그레이션 가이드의 AnyConnect 클라이언트 설치 섹션을 참조하십시오.

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

관리 VPN 터널은 최종 사용자가 VPN 연결을 설정하는 경우뿐만 아니라 클라이언트 시스템의 전원이 켜질 때마다 기업 네트워크에 대한 연결을 보장합니다. 사무실 외부 엔드포인트, 특히 사용자가 VPN을 통해 사무실 네트워크에 연결하는 빈도가 낮은 디바이스에 대해 패치 관리를 수행할 수 있습니다. 회사 네트워크 연결이 필요한 엔드포인트 OS 로그인 스크립트도 이 기능을 활용할 수 있습니다.

관리자는 AnyConnect 관리 터널을 사용하여 사용자가 로그인하기 전에 사용자 작업 없이 AnyConnect를 연결할 수 있습니다. AnyConnect 관리 터널은 신뢰할 수 있는 네트워크 탐지와 함께 작동할 수 있으므로 엔드포인트가 오프프레미스 상태이고 사용자가 시작한 VPN에서 연결이 끊어진 경우에만 트리거됩니다. AnyConnect 관리 터널은 엔드 유저에게 투명하며, 사용자가 VPN을 시작하면 자동으로 연결이 끊깁니다.

OS/애플리케이션	최소 버전 요구 사항
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect 버전	4.7.00136
macOS AnyConnect 버전	4.7.01076
Linux	지원되지 않음

관리 터널 작업

AnyConnect VPN 에이전트 서비스는 시스템 부팅 시 자동으로 시작됩니다. 관리 터널 기능이 (관리 VPN 프로필을 통해) 활성화된 것을 탐지하므로 관리 클라이언트 애플리케이션을 시작하여 관리 터널 연결을 시작합니다. 관리 클라이언트 애플리케이션은 관리 VPN 프로필의 호스트 항목을 사용하여 연결을 시작합니다. 그런 다음 VPN 터널이 평소와 같이 설정됩니다. 단, 관리 터널은 사용자에게 투명하게 설정되므로 관리 터널 연결 중에 소프트웨어 업데이트가 수행되지 않습니다.

사용자는 AnyConnect UI를 통해 VPN 터널을 시작하며, 이는 관리 터널 종료를 트리거합니다. 관리 터널이 종료되면 사용자 터널 설정이 평소와 같이 계속됩니다.

사용자가 VPN 터널을 연결 해제하면 관리 터널의 자동 재설정이 트리거됩니다.

제한 사항

- 사용자 상호 작용이 지원되지 않습니다.
- 머신 인증서 저장소(Windows)를 통한 인증서 기반 인증만 지원됩니다.
- 엄격한 서버 인증서 검사가 시행됩니다.
- 개인 프록시는 지원되지 않습니다.
- 공용 프록시가 지원되지 않습니다. ProxyNative 값은 기본 프록시 설정이 브라우저에서 검색되지 않는 플랫폼에서 지원됩니다.

- AnyConnect 사용자 지정 스크립트는 지원되지 않습니다.

참고: 자세한 내용은 관리 VPN 터널 정보를 참조하십시오.

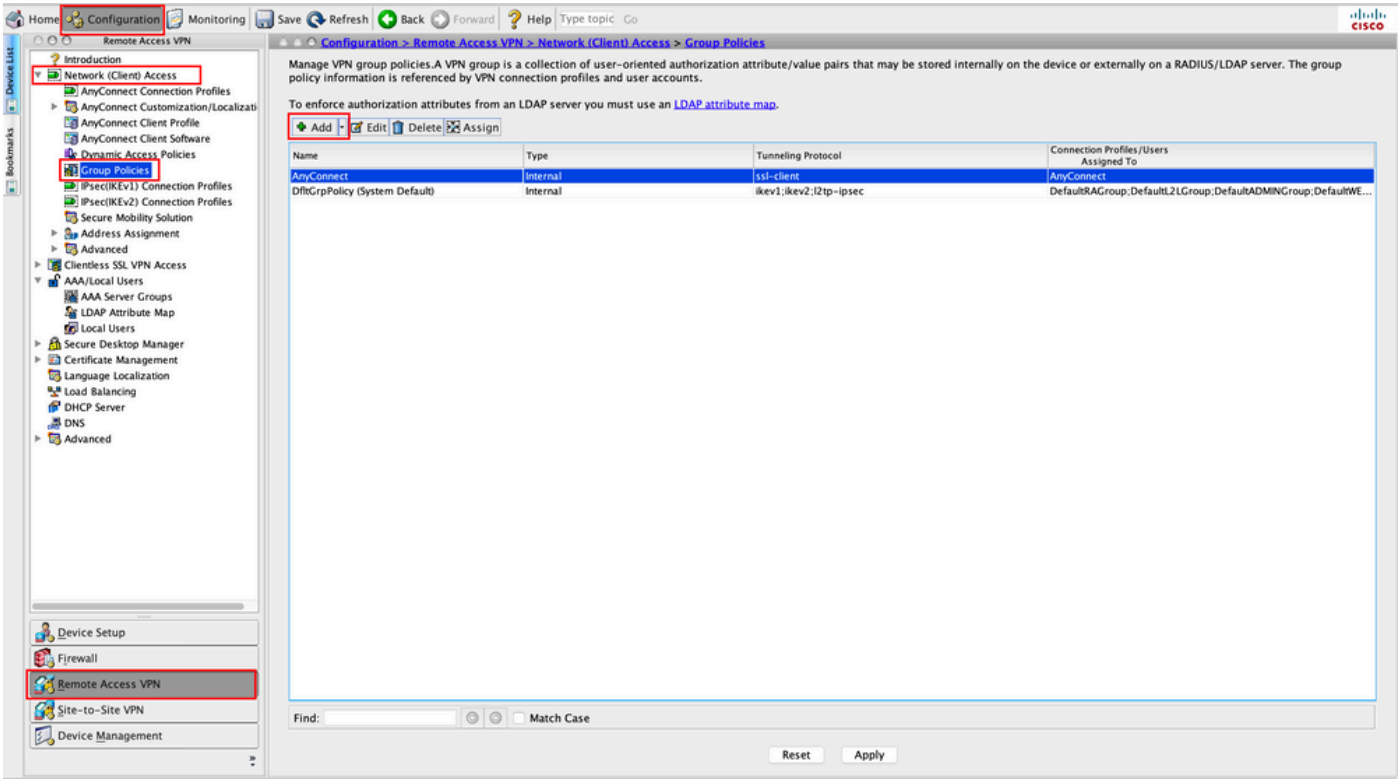
구성

이 섹션에서는 Cisco ASA를 VPN 게이트웨이로 구성하여 AnyConnect 클라이언트에서 관리 VPN 터널을 통해 연결을 수락하는 방법에 대해 설명합니다.

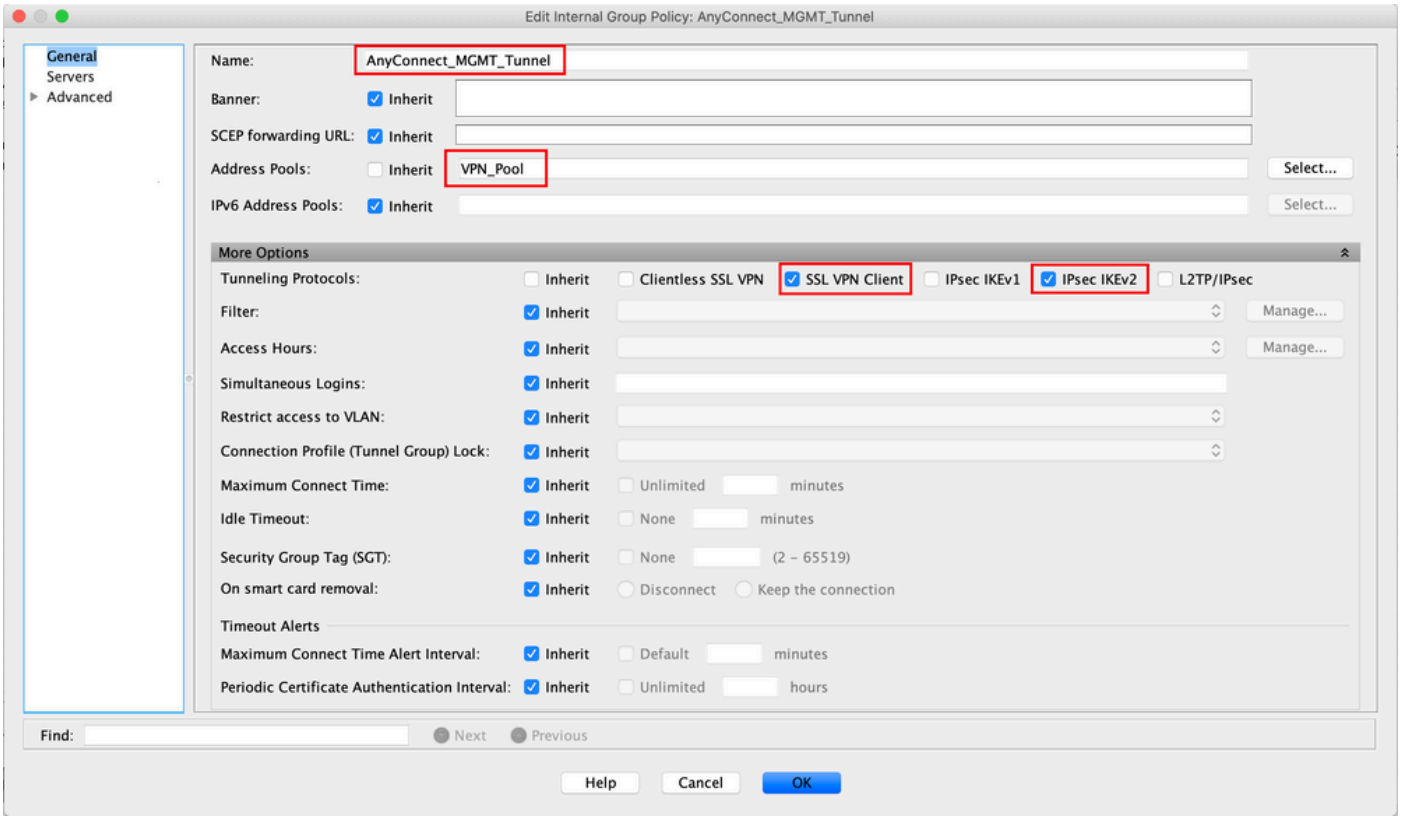
ASDM/CLI를 통한 ASA 컨피그레이션

1단계. AnyConnect 그룹 정책을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > Group Policies. 클릭 Add.

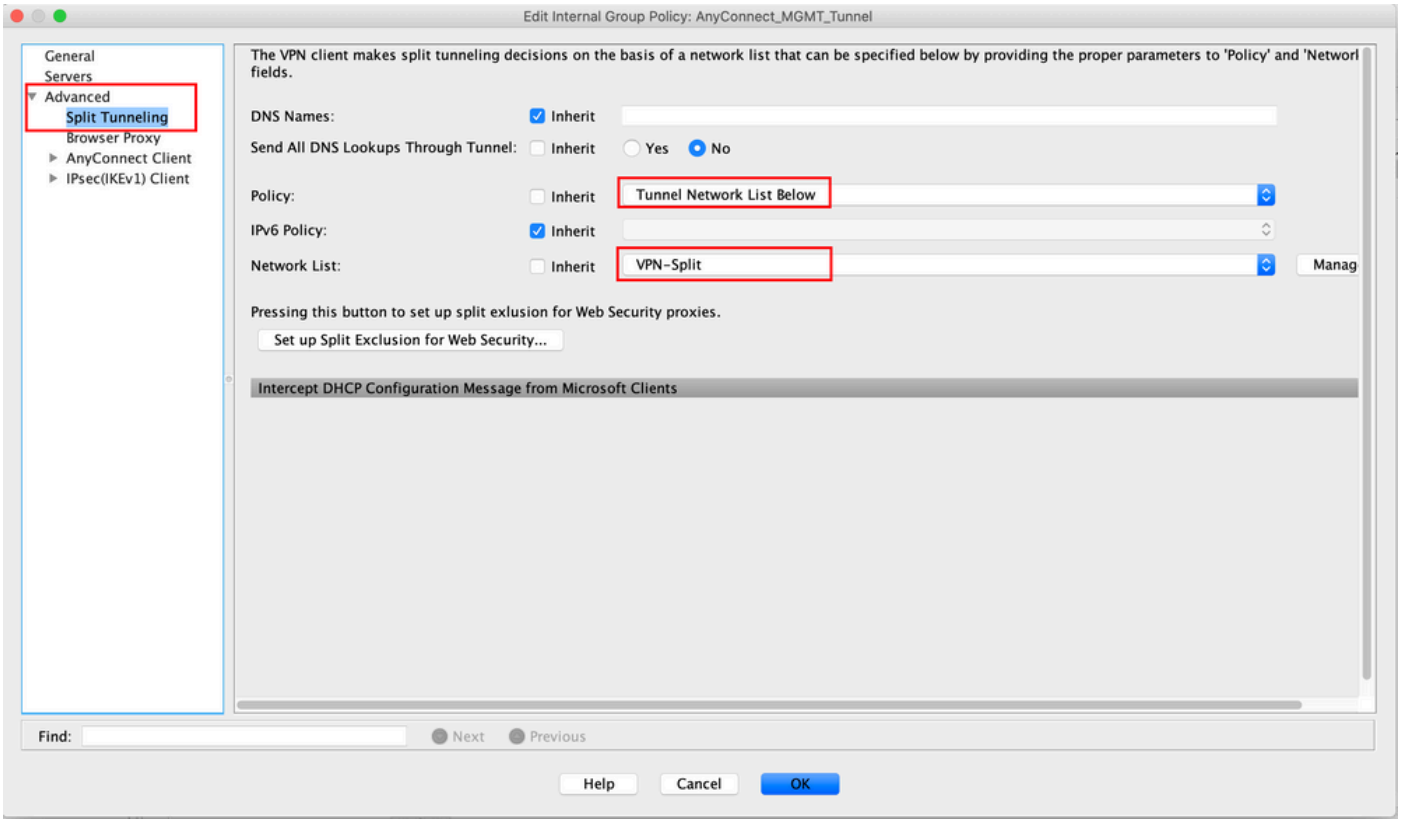
참고: AnyConnect 관리 터널에만 사용되는 새 AnyConnect 그룹 정책을 생성하는 것이 좋습니다.



2단계. 제공: Name 그룹 정책. 할당/생성 Address Pool. 선택 Tunneling Protocols 다음으로 SSL VPN Client 및/또는 IPsec IKEv2에 나와 있는 것처럼.



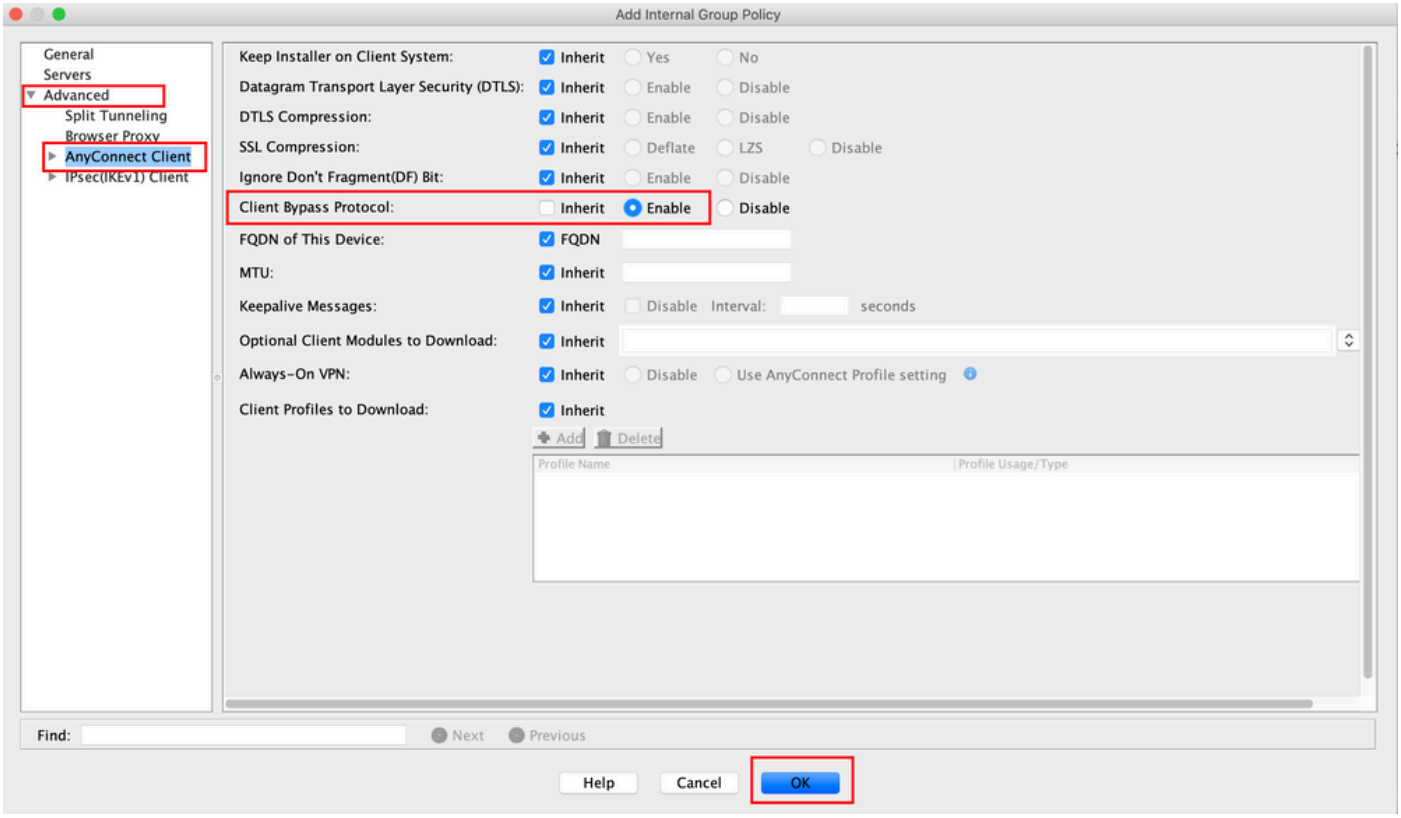
3단계. 탐색 Advanced > Split Tunneling. 구성 Policy 다음으로 Tunnel Network List Below Firepower Threat Defense Network List에 나와 있는 것처럼.



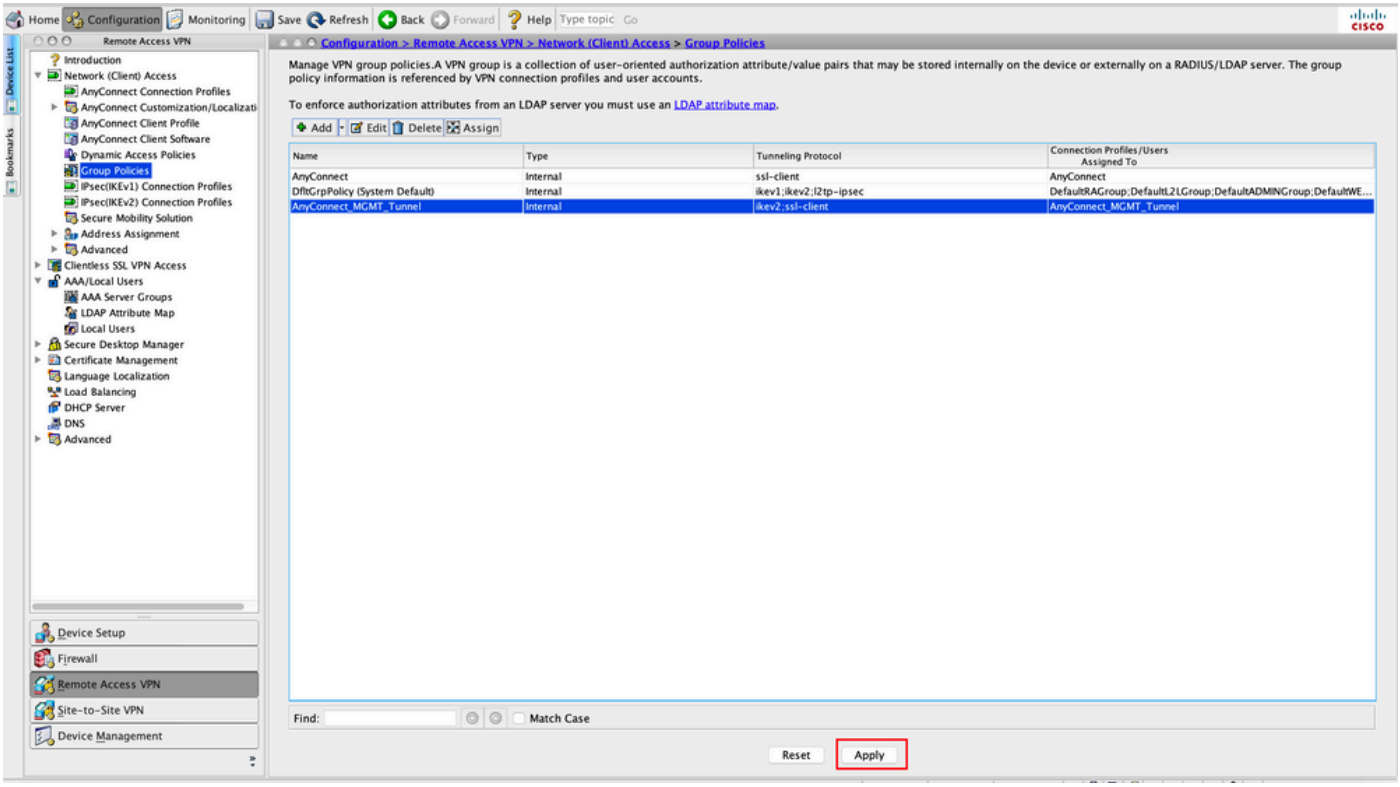
참고: 두 IP 프로토콜(IPv4 및 IPv6) 모두에 대해 클라이언트 주소가 푸시되지 않으면 **Client Bypass Protocol** 설정은 다음과 같아야 합니다 enabled 해당 트래픽이 관리 터널에 의해 중단되지 않도록 합니다. 구성하려면 4단계를 참조하십시오.

4단계. 탐색 Advanced > AnyConnect Client. 설정 Client Bypass Protocol 수신 Enable. 클릭 OK 을 눌러 이미지

에 표시된 대로 저장합니다.



5단계. 이 그림과 같이 Apply ASA에 컨피그레이션을 푸시합니다.



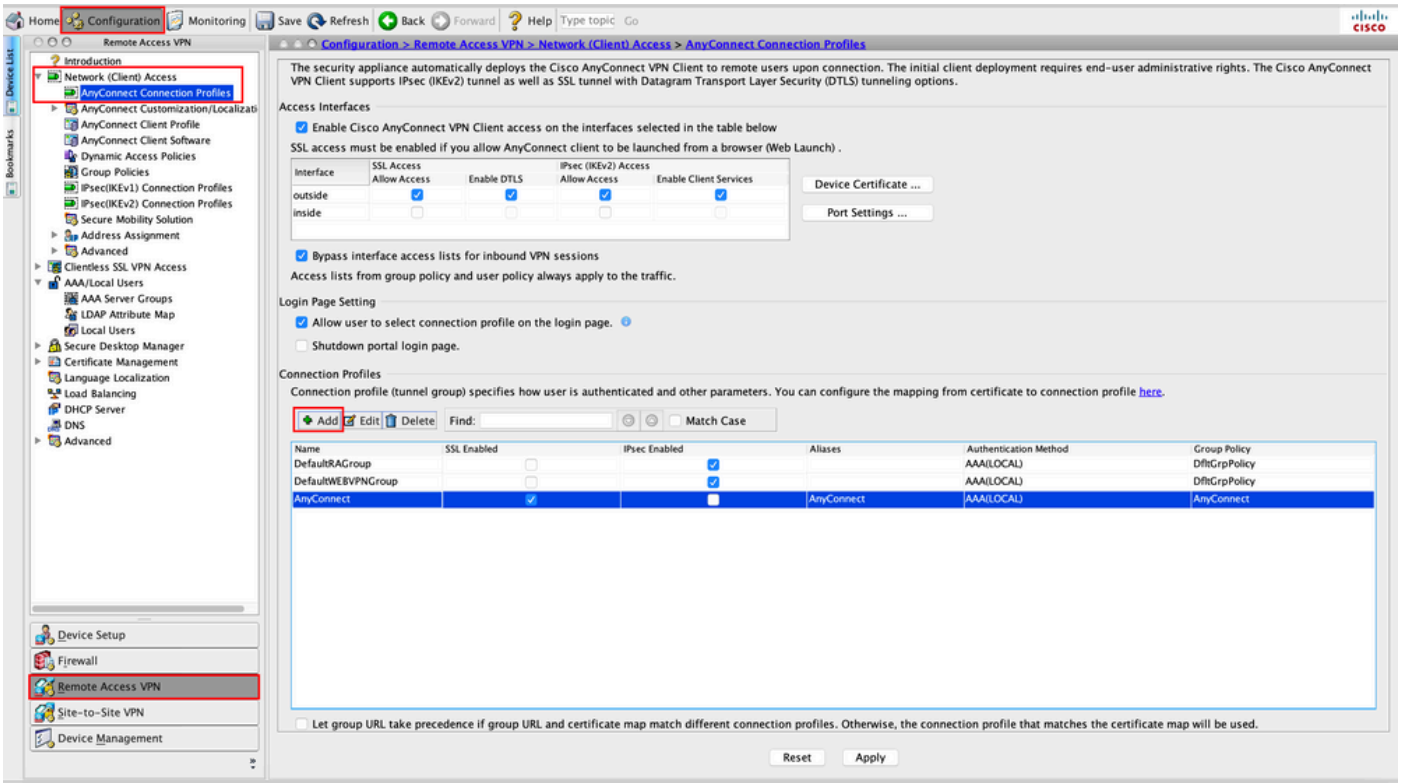
그룹 정책에 대한 CLI 구성:

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
```

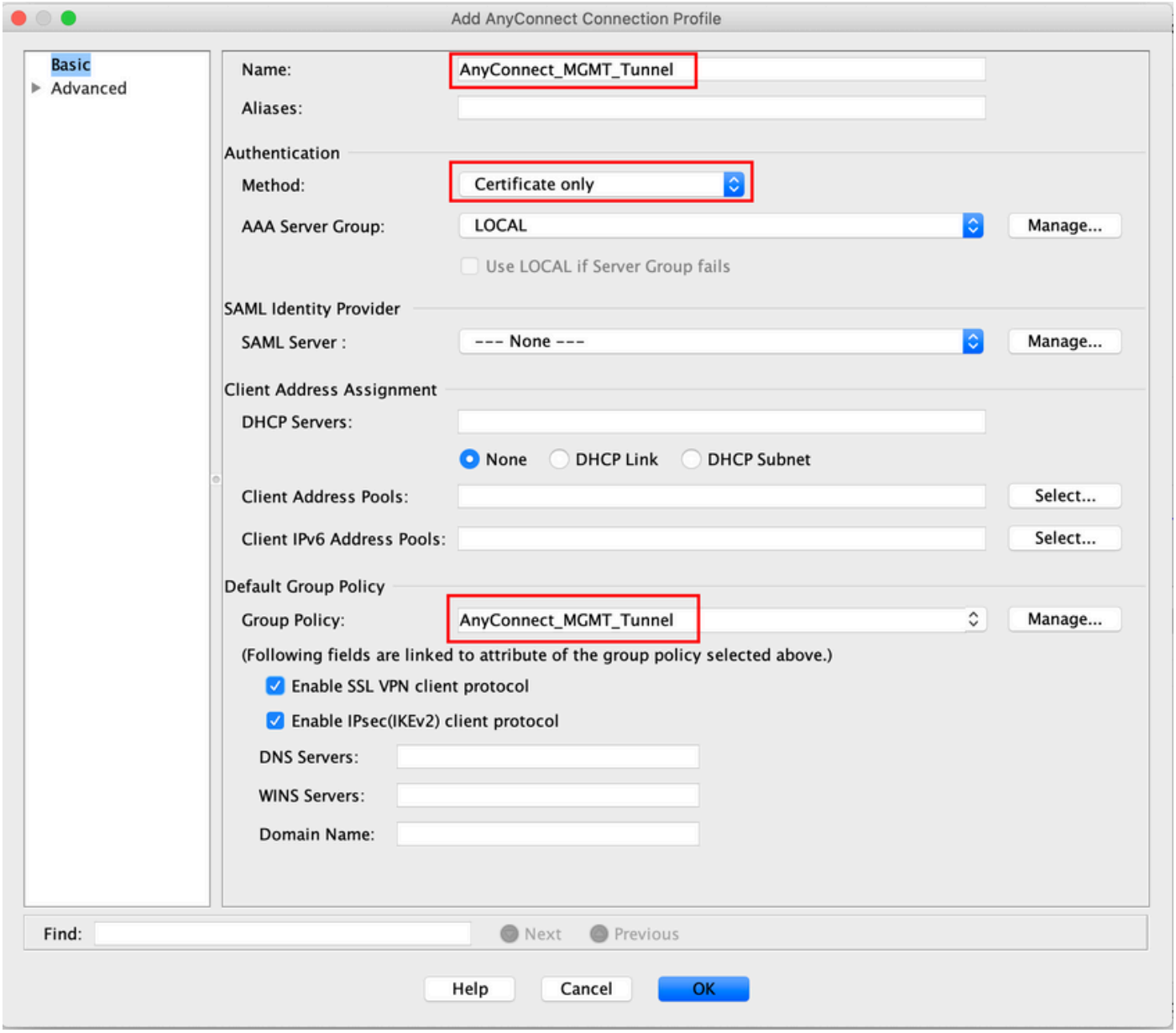
```
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

6단계. AnyConnect 연결 프로파일을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 클릭 Add.

> **참고:** AnyConnect 관리 터널에만 사용되는 새 AnyConnect 연결 프로파일을 생성하는 것이 좋습니다.



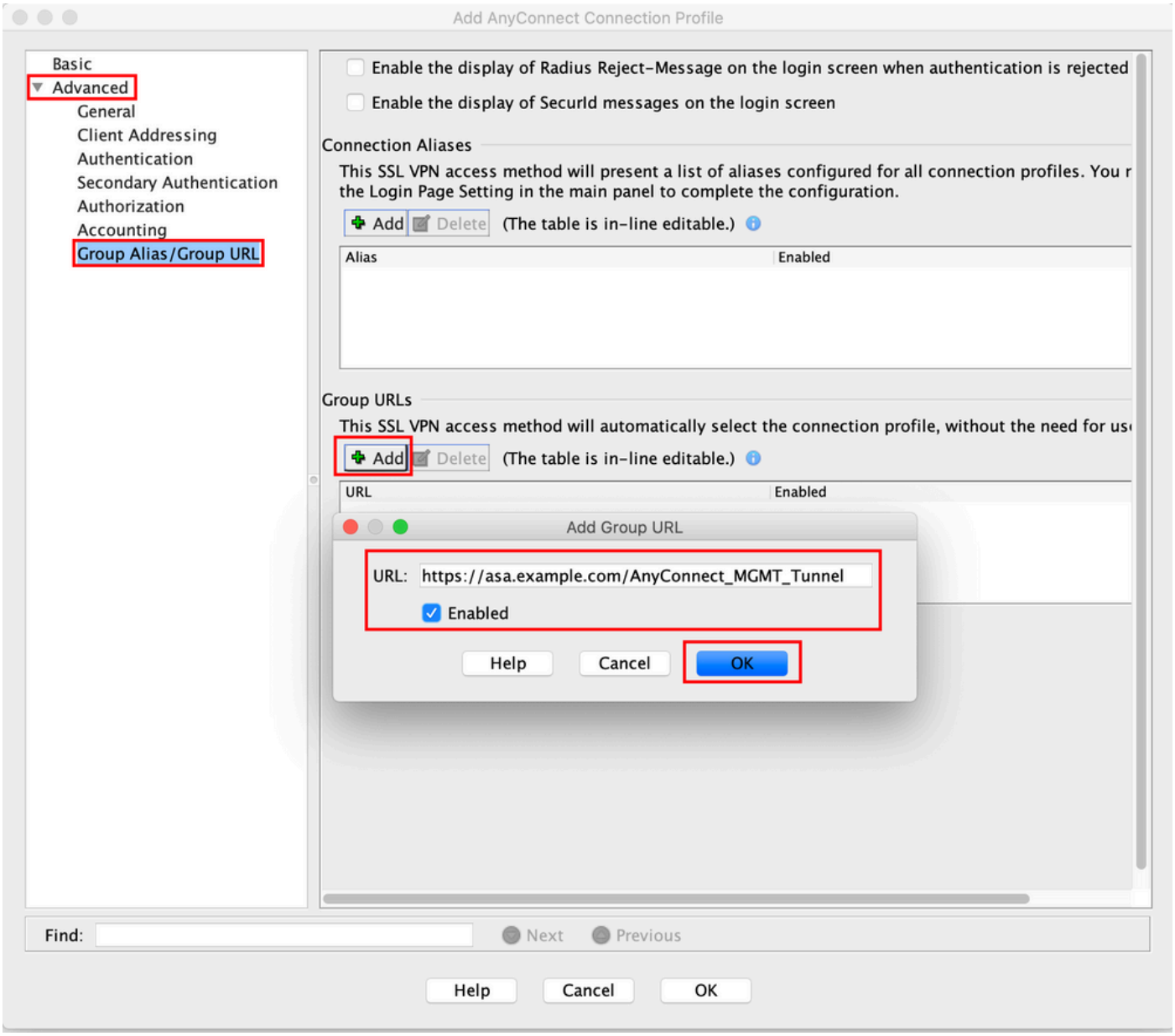
7단계. 제공: Name Connection Profile에 대해 Authentication Method 다음으로 Certificate only. 다음을 선택합니다. Group Policy 1단계에서 생성한 것입니다.



참고: 로컬 CA의 루트 인증서가 ASA에 있어야 합니다. 탐색 Configuration > Remote Access VPN > Certificate Management > CA Certificates 인증서를 추가/봅니다.

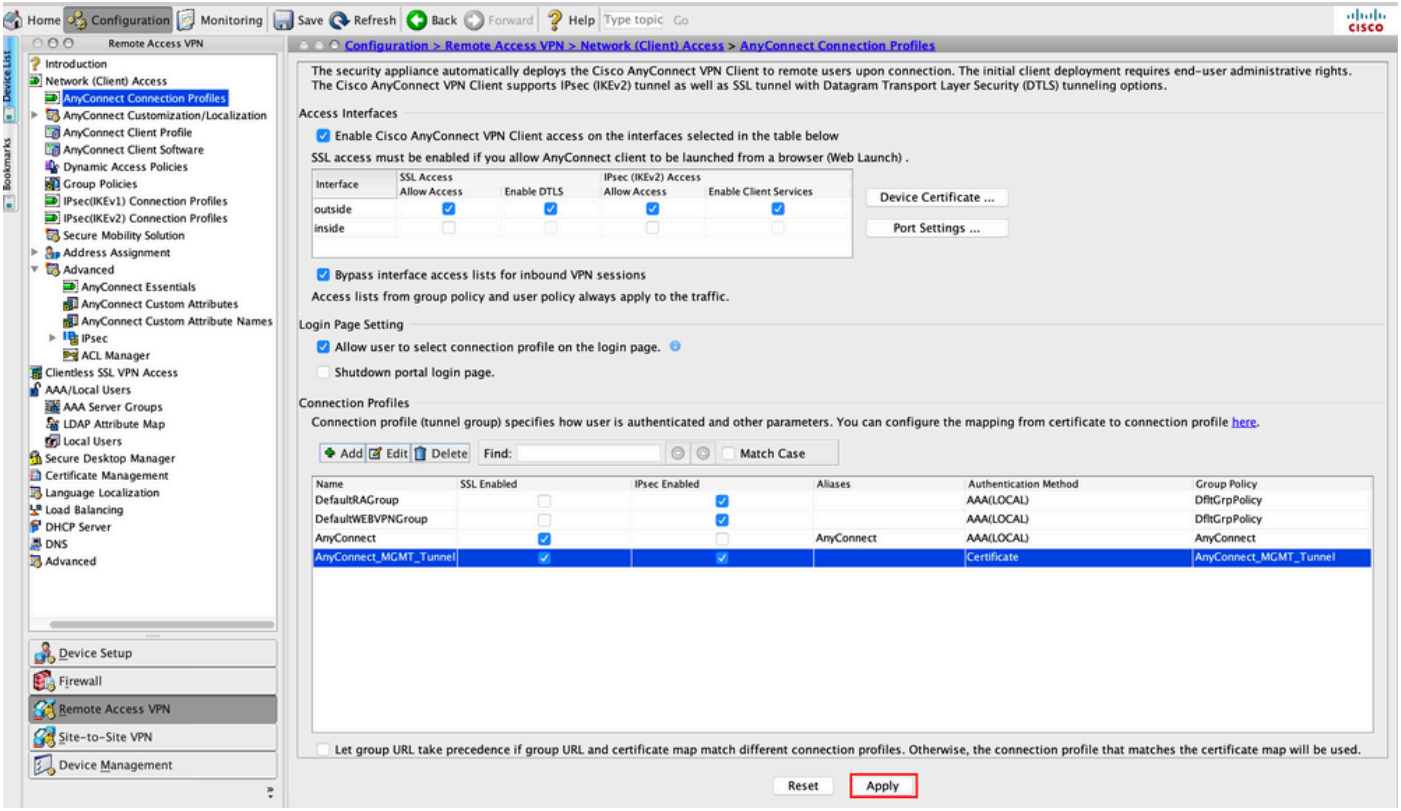
참고: 동일한 로컬 CA에서 발급한 ID 인증서가 머신 인증서 저장소(Windows용) 및/또는 시스템 키 체인(macOS용)에 있는지 확인하십시오.

8단계. 탐색 Advanced > Group Alias/Group URL. 클릭 Add 의 밑에 Group URLs 및 URL. 확인 Enabled 이(가) 선택되어 있습니다. 클릭 OK 을 눌러 이미지에 표시된 대로 저장합니다.



IKEv2를 사용하는 경우 IPsec (IKEv2) Access AnyConnect에 사용되는 인터페이스에서 활성화됩니다.

9단계. 클릭 Apply ASA에 컨피그레이션을 푸시합니다.

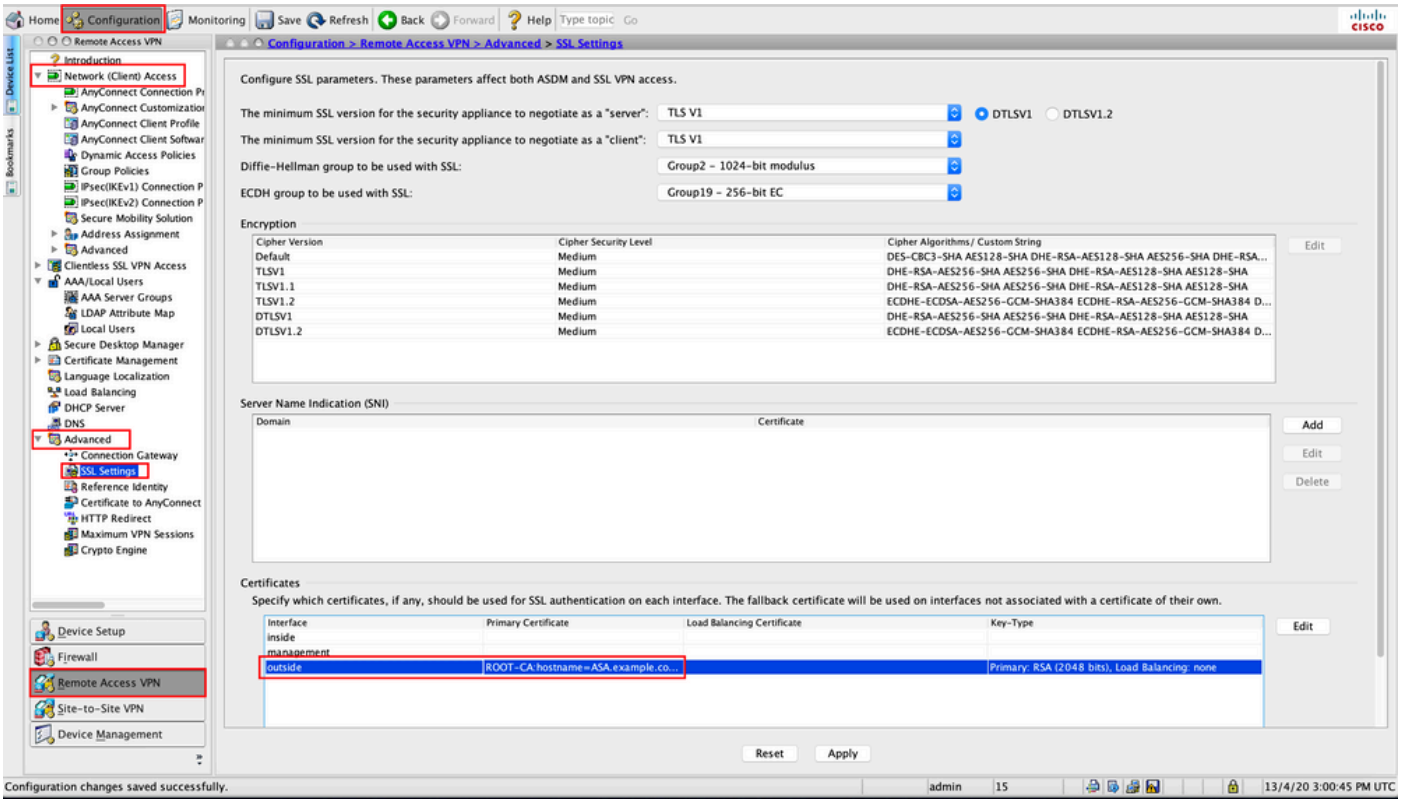


연결 프로파일(터널 그룹)에 대한 CLI 컨피그레이션:

```
tunnel-group AnyConnect_MGMT_Tunnel type remote-access
tunnel-group AnyConnect_MGMT_Tunnel general-attributes
 default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
 authentication certificate
 group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

10단계. 신뢰할 수 있는 인증서가 ASA에 설치되어 있고 AnyConnect 연결에 사용되는 인터페이스에 바인딩되어 있는지 확인합니다. 탐색 Configuration > Remote Access VPN > Advanced > SSL Settings 을 클릭하면 이 설정을 추가/볼 수 있습니다.

참고: ASA에 ID 인증서 설치를 참조하십시오.

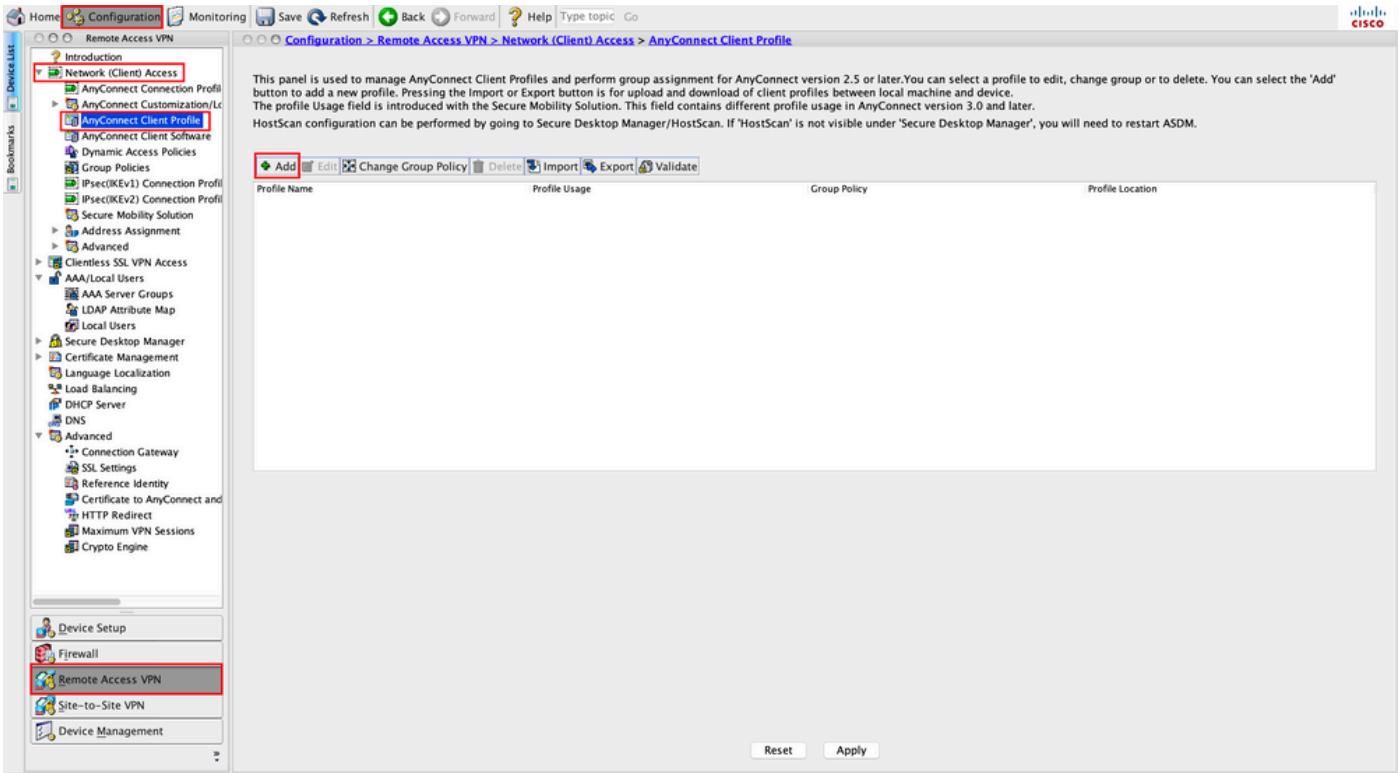


SSL 신뢰 지점에 대한 CLI 구성:

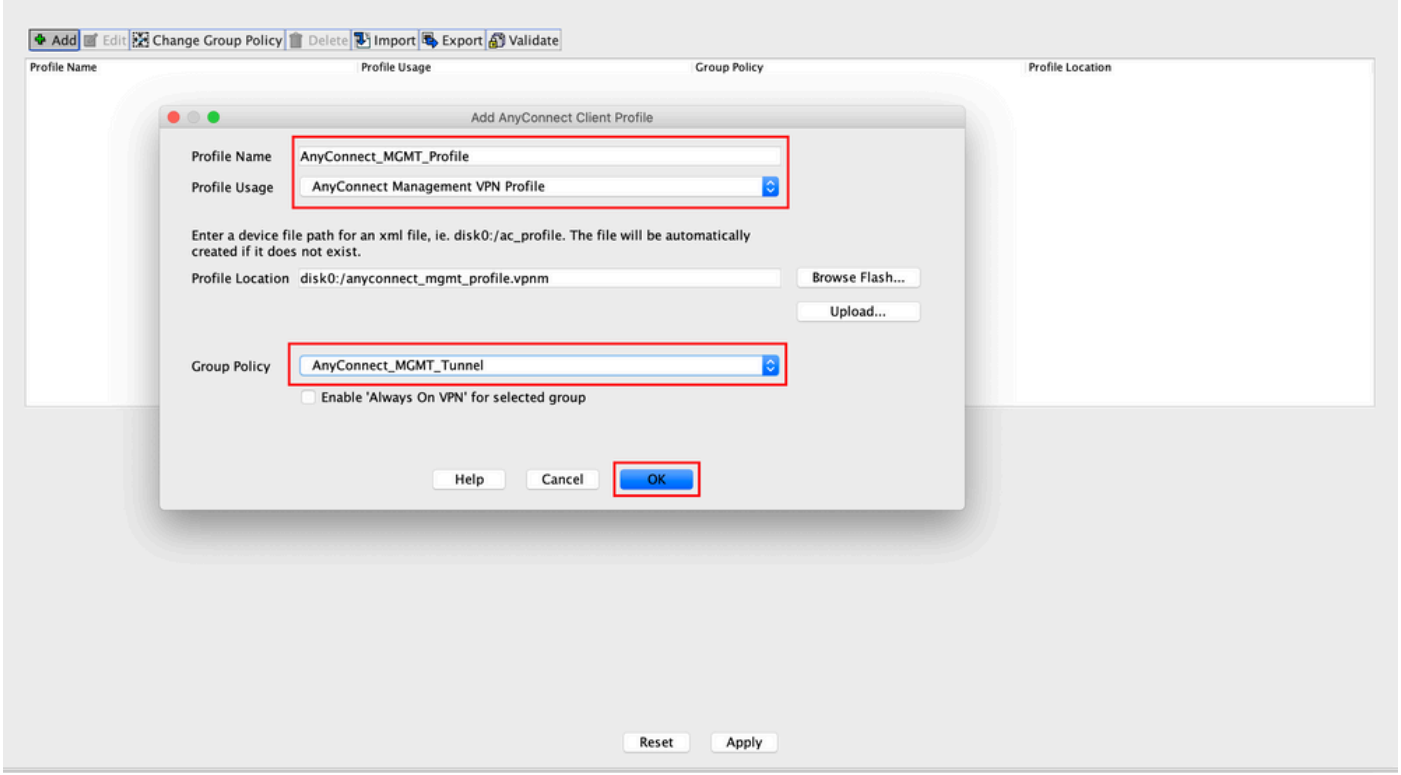
```
ssl trust-point ROOT-CA outside
```

AnyConnect 관리 VPN 프로파일 생성

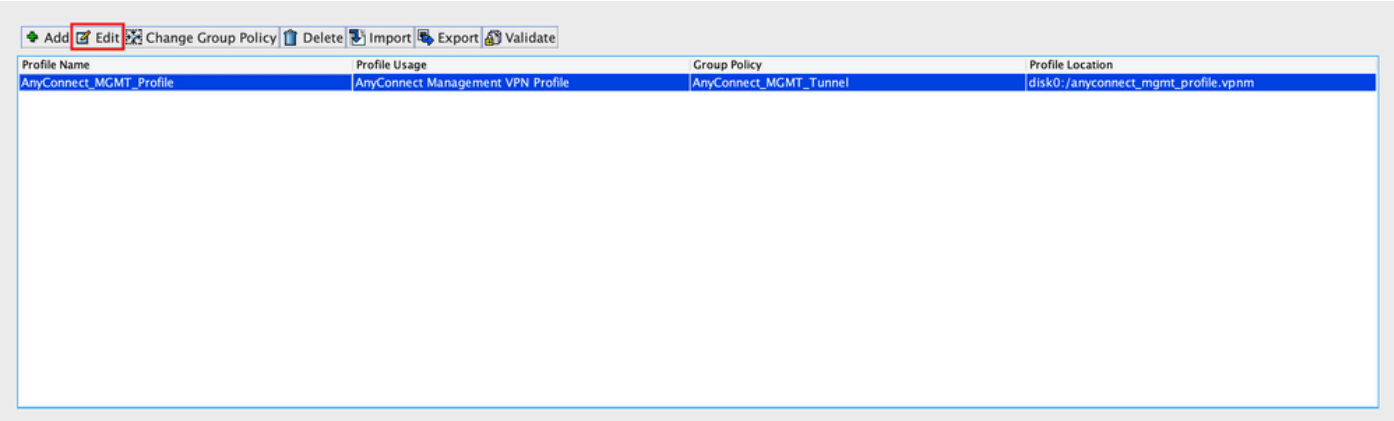
1단계. AnyConnect 클라이언트 프로파일을 생성합니다. 탐색 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. 클릭 Add에 나와 있는 것처럼.



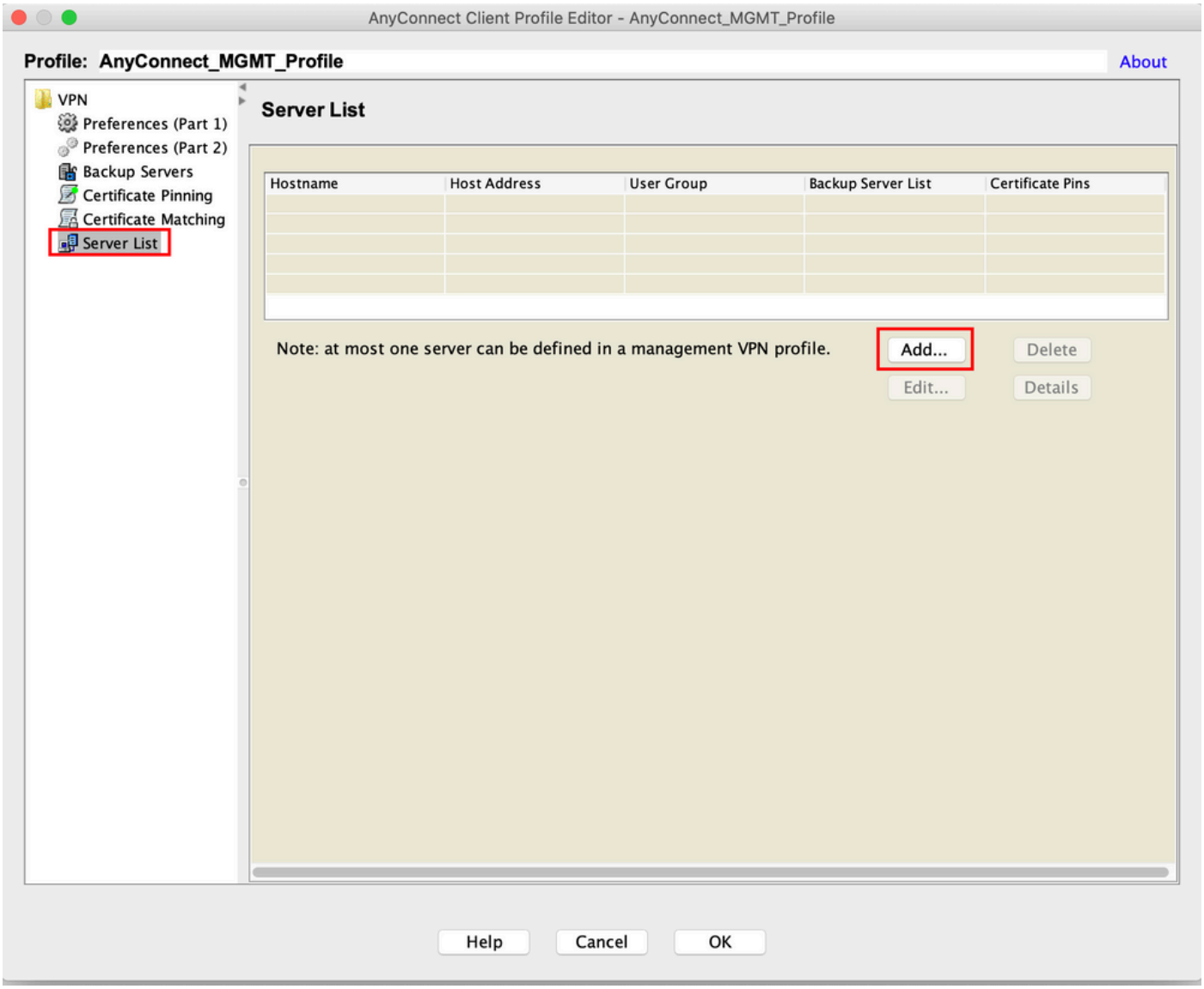
2단계. 제공: Profile Name. 다음을 선택합니다. Profile Usage 다음으로 AnyConnect Management VPN profile. 다음을 선택합니다. Group Policy 1단계에서 생성됩니다. 클릭 OK 에 나와 있는 것처럼.



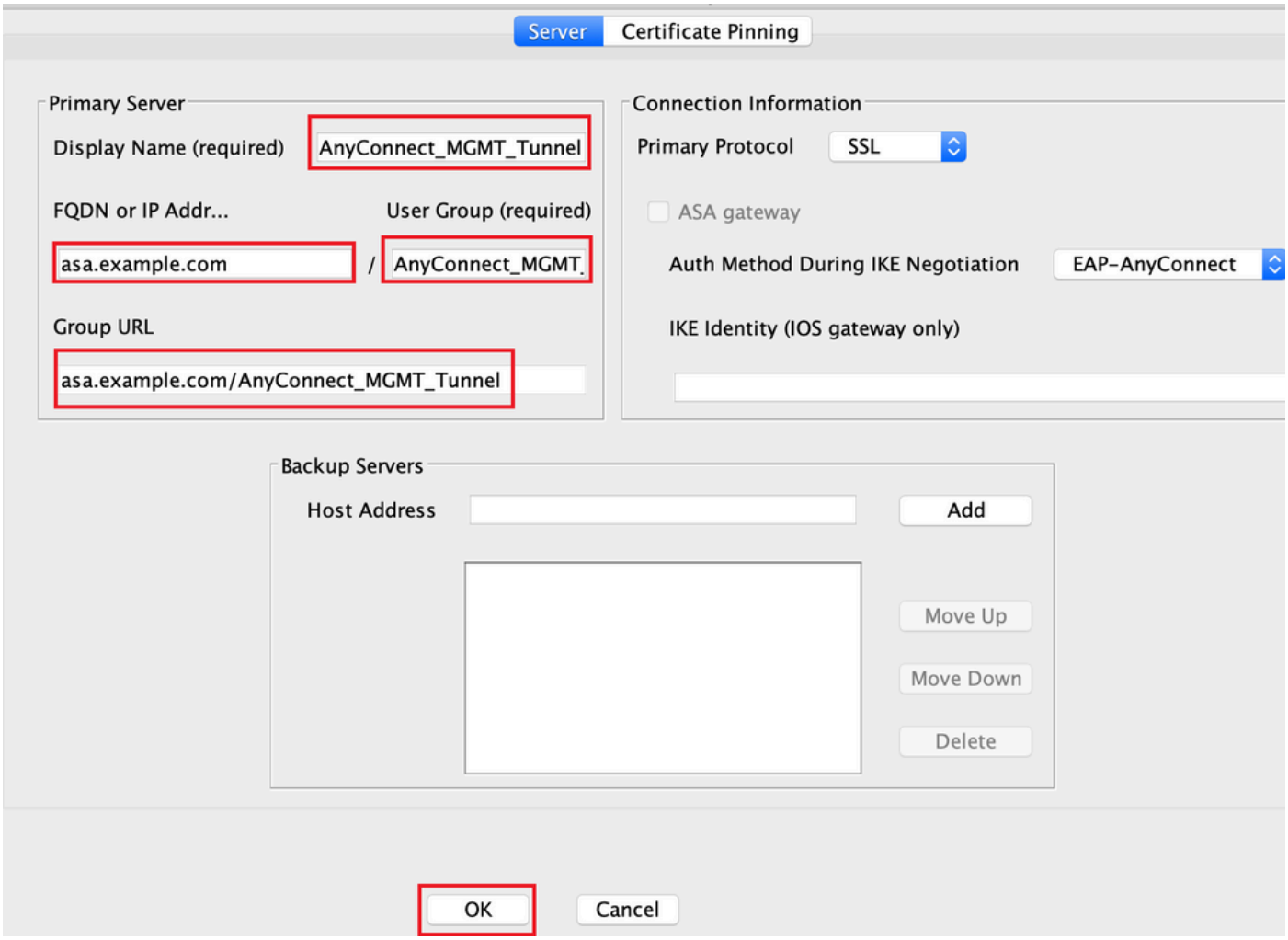
3단계. 생성된 프로필을 선택하고 Edit에 나와 있는 것처럼.



4단계. 탐색 Server List. 클릭 Add 새 서버 목록 항목을 추가합니다(이미지 참조).



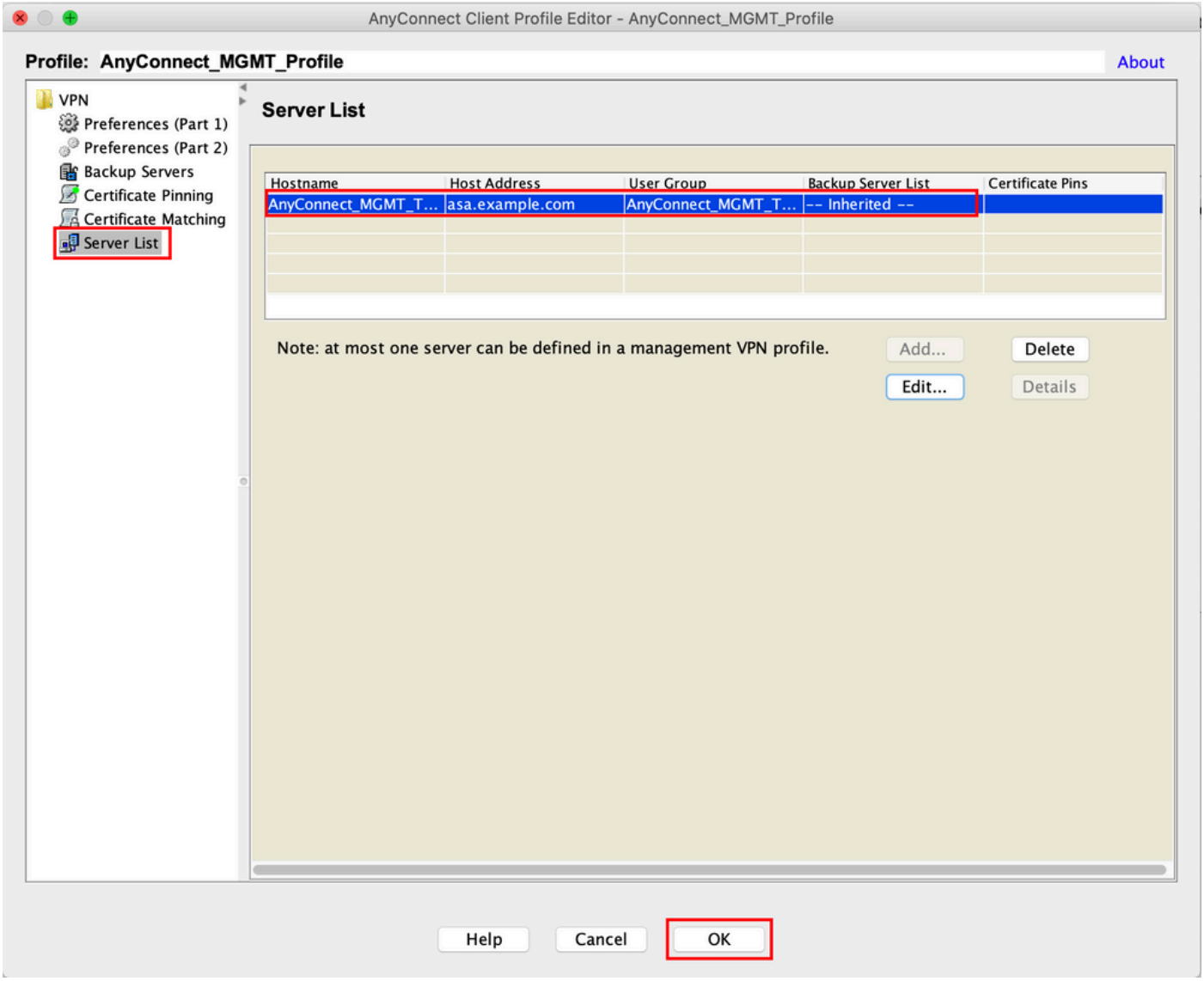
5단계. 제공: Display Name. 추가 FQDN/IP address ASA를 구성합니다 제공: User Group 를 터널 그룹 이름으로 사용합니다. Group URL 자동으로 채워집니다 FQDN 및 User Group. 클릭 OK.



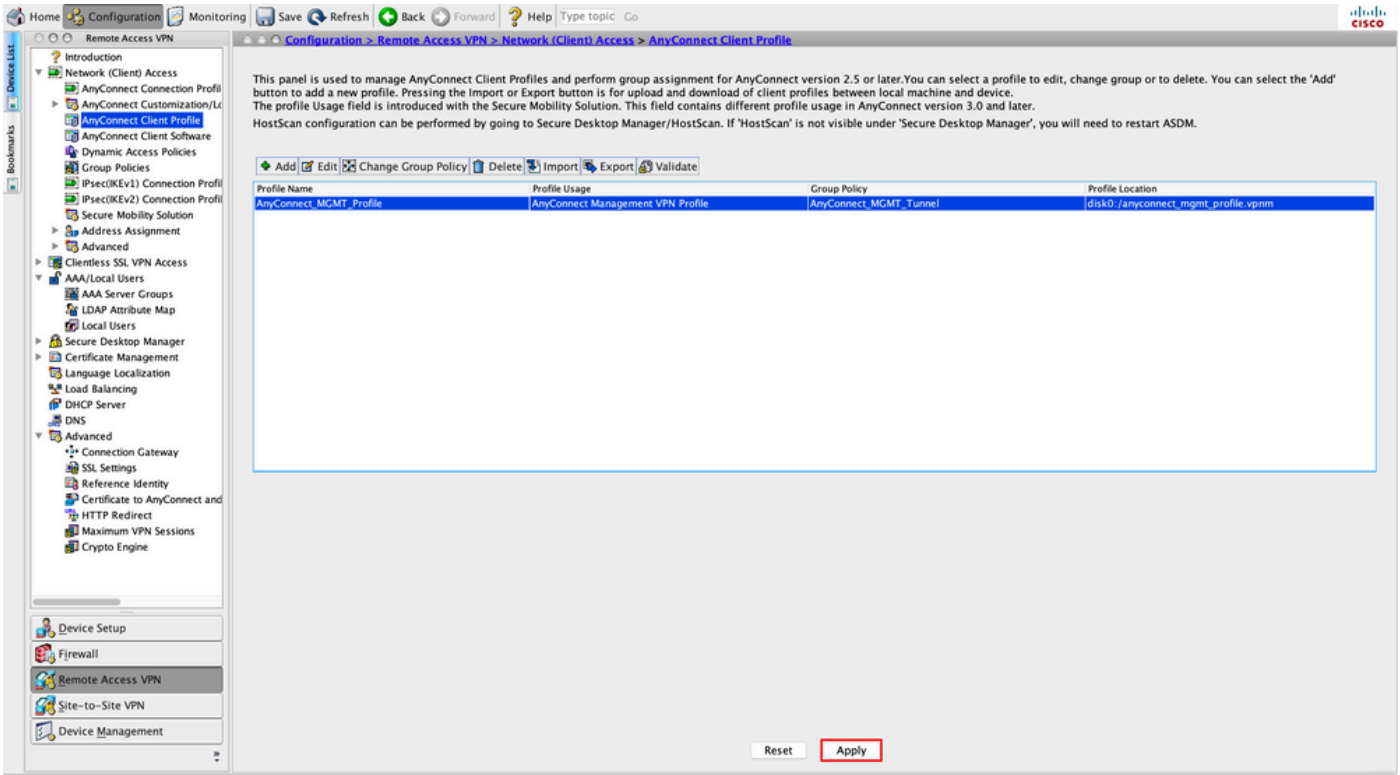
참고: FQDN/IP 주소 + 사용자 그룹은 8단계에서 AnyConnect 연결 프로파일 컨피그레이션 중에 언급된 그룹 URL과 동일해야 합니다.

참고: IKEv2를 프로토콜로 사용하는 AnyConnect를 사용하여 ASA에 대한 관리 VPN을 설정할 수도 있습니다. 확인 Primary Protocol 다음으로 설정됨 IPsec 5단계.

6단계. 그림에 표시된 대로 OK 저장하십시오.



7단계. 클릭 Apply t을 눌러 그림과 같이 ASA에 컨피그레이션을 푸시합니다.



AnyConnect 관리 VPN 프로파일 추가 후 CLI 구성

```
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

AnyConnect 클라이언트 머신의 AnyConnect 관리 VPN 프로파일:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>




        <ShowPreConnectMessage>false</ShowPreConnectMessage>




        <ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

참고: 사용자 AnyConnect VPN 프로파일에서 TND(Trusted Network Detection)를 사용하는 경우 일관된 사용자 환경을 위해 관리 VPN 프로파일에서 동일한 설정을 확인하는 것이 좋습니다. 관리 VPN 터널은 사용자 VPN 터널 프로파일에 적용된 TND 설정에 따라 트리거됩니다. 또한 관리 VPN 프로파일의 TND 연결 작업(관리 VPN 터널이 활성 상태일 때만 시행됨)은 관리 VPN 터널이 최종 사용자에게 투명하게 유지되도록 항상 사용자 VPN 터널에 적용됩니다.

참고: 모든 최종 사용자 PC에서 Management VPN 프로필에 TND 설정이 활성화되어 있고 사용자 VPN 프로필이 누락된 경우, 누락된 사용자 VPN 프로필 대신 TND에 대한 기본 환경 설정(AC 클라이언트 애플리케이션의 기본 환경 설정에서 비활성화됨)을 고려합니다. 이러한 불일치는 예기치 않은/정의되지 않은 동작으로 이어질 수 있습니다.
기본적으로 TND 설정은 기본 환경 설정에서 비활성화되어 있습니다.
AnyConnect 클라이언트 애플리케이션에서 기본 환경 설정 하드코딩된 설정을 극복하려면 최종 사용자 PC에 두 개의 VPN 프로파일, 즉 사용자 VPN 프로파일과 AC 관리 VPN 프로파일이 있어야 하며 두 프로파일 모두 동일한 TND 설정이 있어야 합니다.
관리 VPN 터널 연결 및 연결 해제의 논리는 AC 에이전트가 관리 VPN 터널을 설정하기 위해 사용자 VPN 프로필 TND 설정을 사용하고 관리 VPN 터널의 연결을 해제하려면 관리 VPN 프로필 TND 설정을 확인하는 것입니다.

AnyConnect 관리 VPN 프로파일의 구축 방법

- VPN 게이트웨이에서 AnyConnect 관리 VPN 프로파일을 다운로드하기 위해 ASA 연결 프로파일을 사용하여 성공한 사용자 VPN 연결이 완료되었습니다.

  참고: 관리 VPN 터널에 사용된 프로토콜이 IKEv2인 경우 SSL을 통해 첫 번째 연결을 설정해야 합니다(ASA에서 AnyConnect 관리 VPN 프로파일을 다운로드하려면).

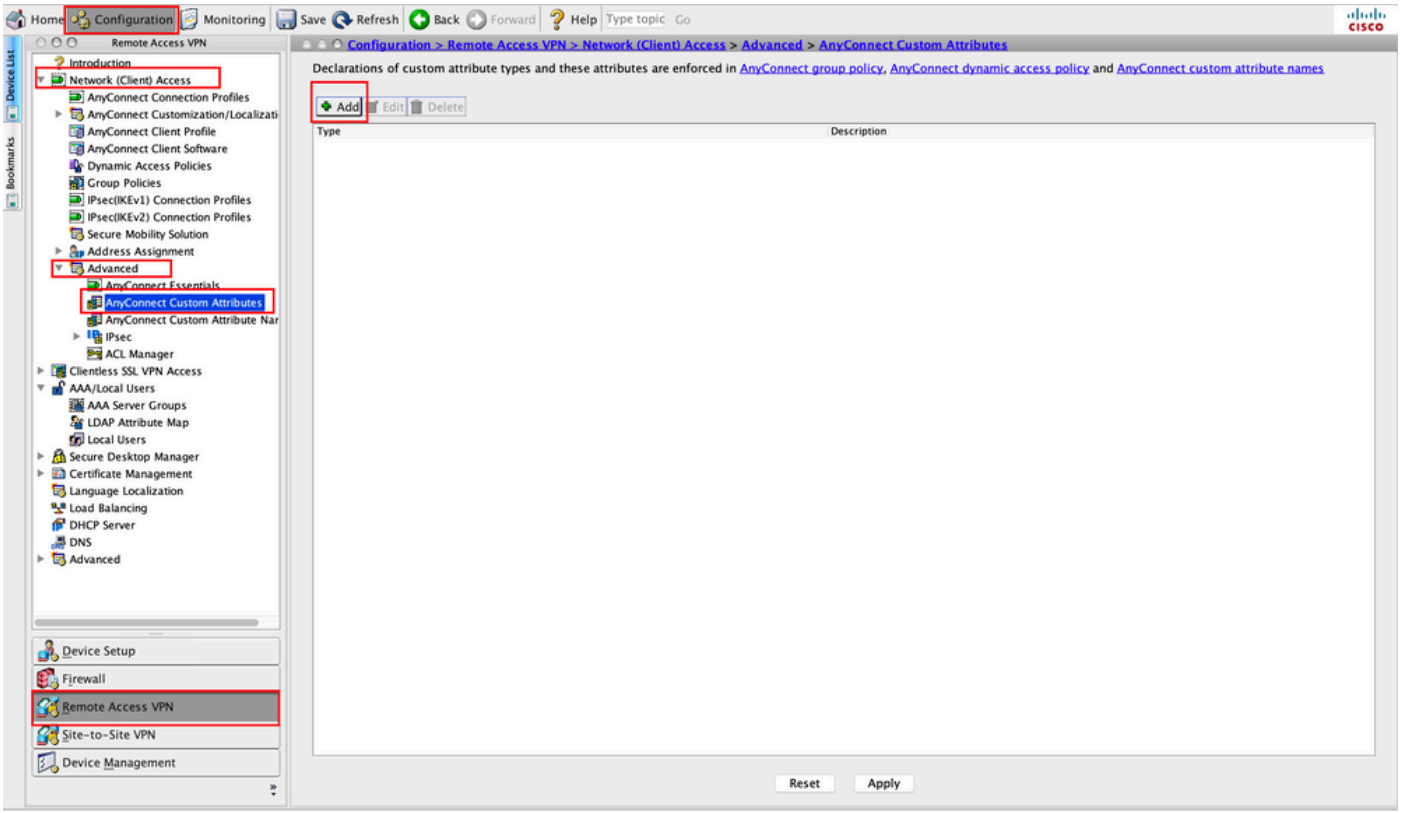
- AnyConnect 관리 VPN 프로필은 GPO 푸시를 통해 또는 수동 설치를 통해 클라이언트 머신에 수동으로 업로드할 수 있습니다(프로필의 이름이 VpnMgmtTunProfile.xml).

  프로필을 추가해야 하는 폴더의 위치:
  창: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  맥OS: /opt/cisco/anyconnect/profile/mgmttun/

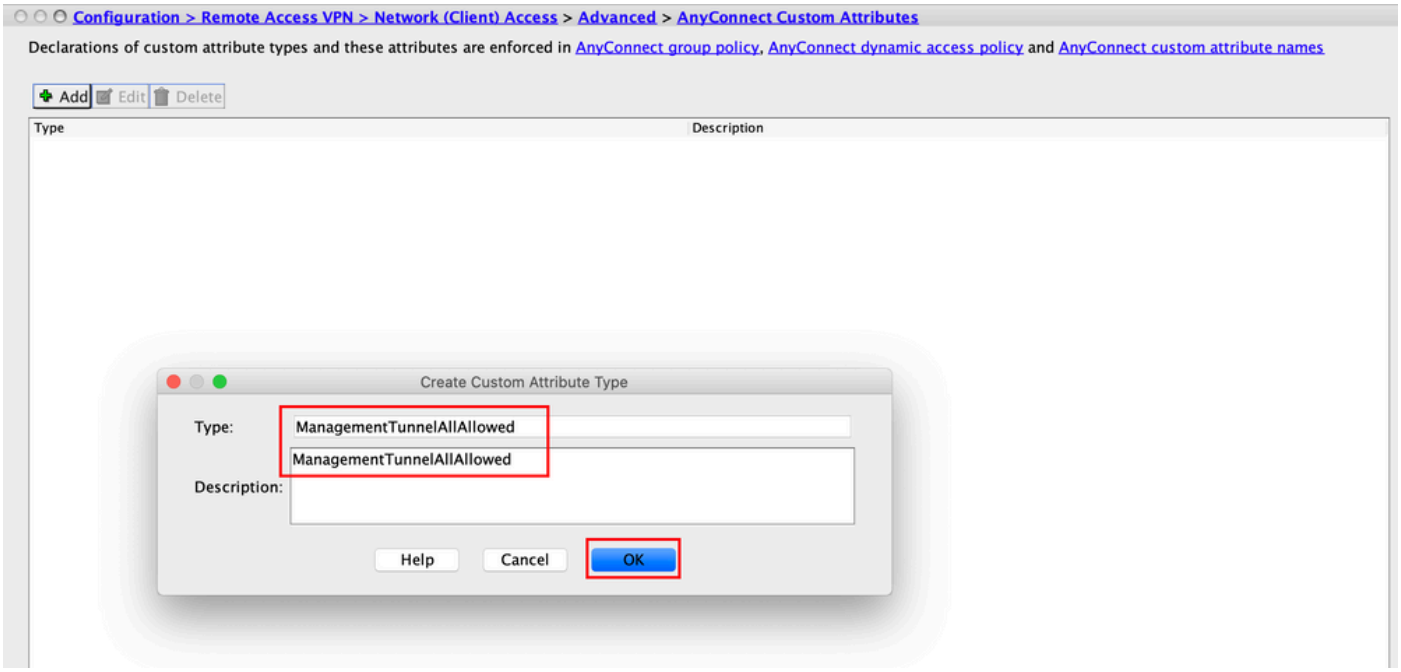
(선택 사항) Tunnel-All 컨피그레이션을 지원하도록 사용자 지정 특성을 구성합니다

사용자가 시작한 네트워크 통신에 영향을 주지 않으려면 관리 VPN 터널에는 기본적으로 터널링 컨피그레이션이 포함된 분할이 필요합니다. 관리 터널 연결에서 사용하는 그룹 정책에서 사용자 지정 특성을 구성할 때 이를 무시할 수 있습니다.

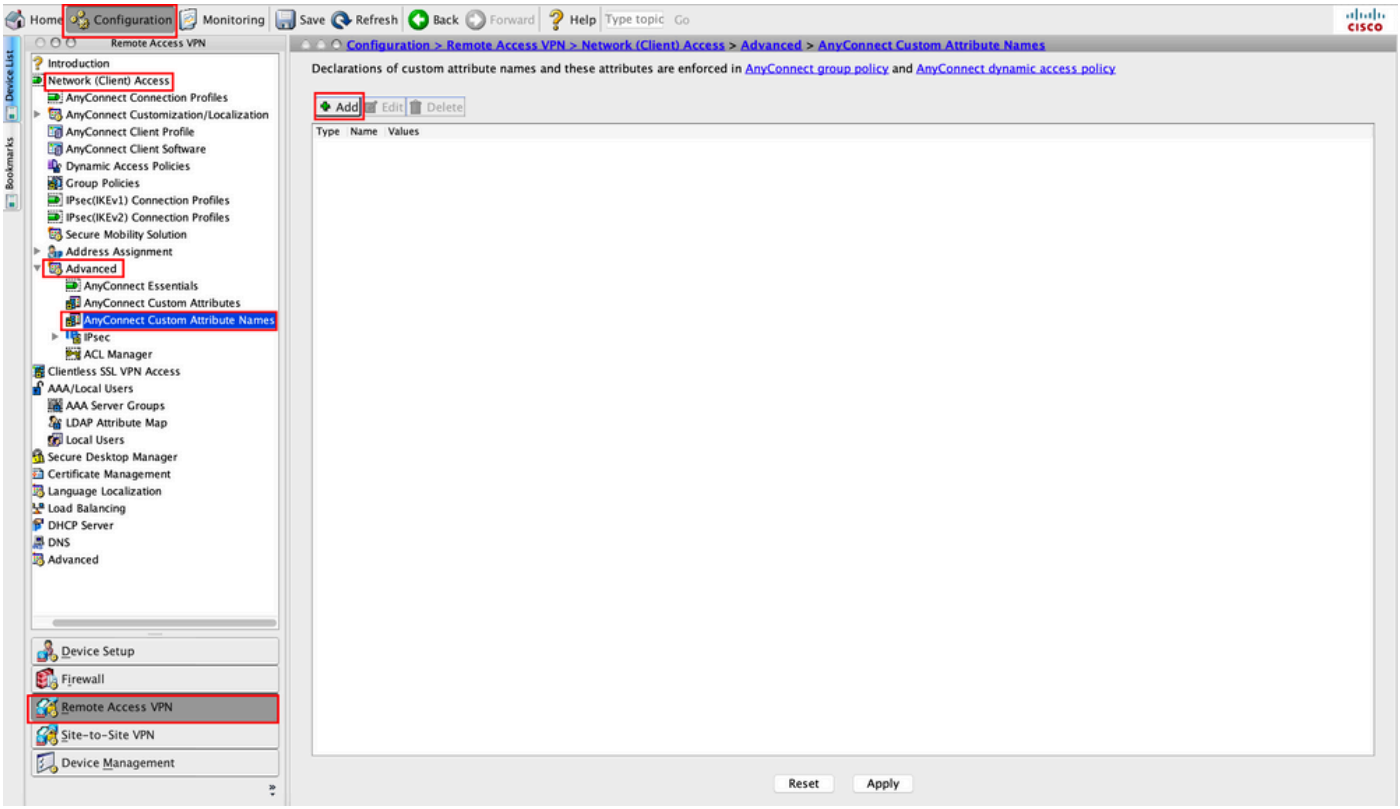
1단계. 탐색Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 클릭 Add에 나와 있는 것처럼.



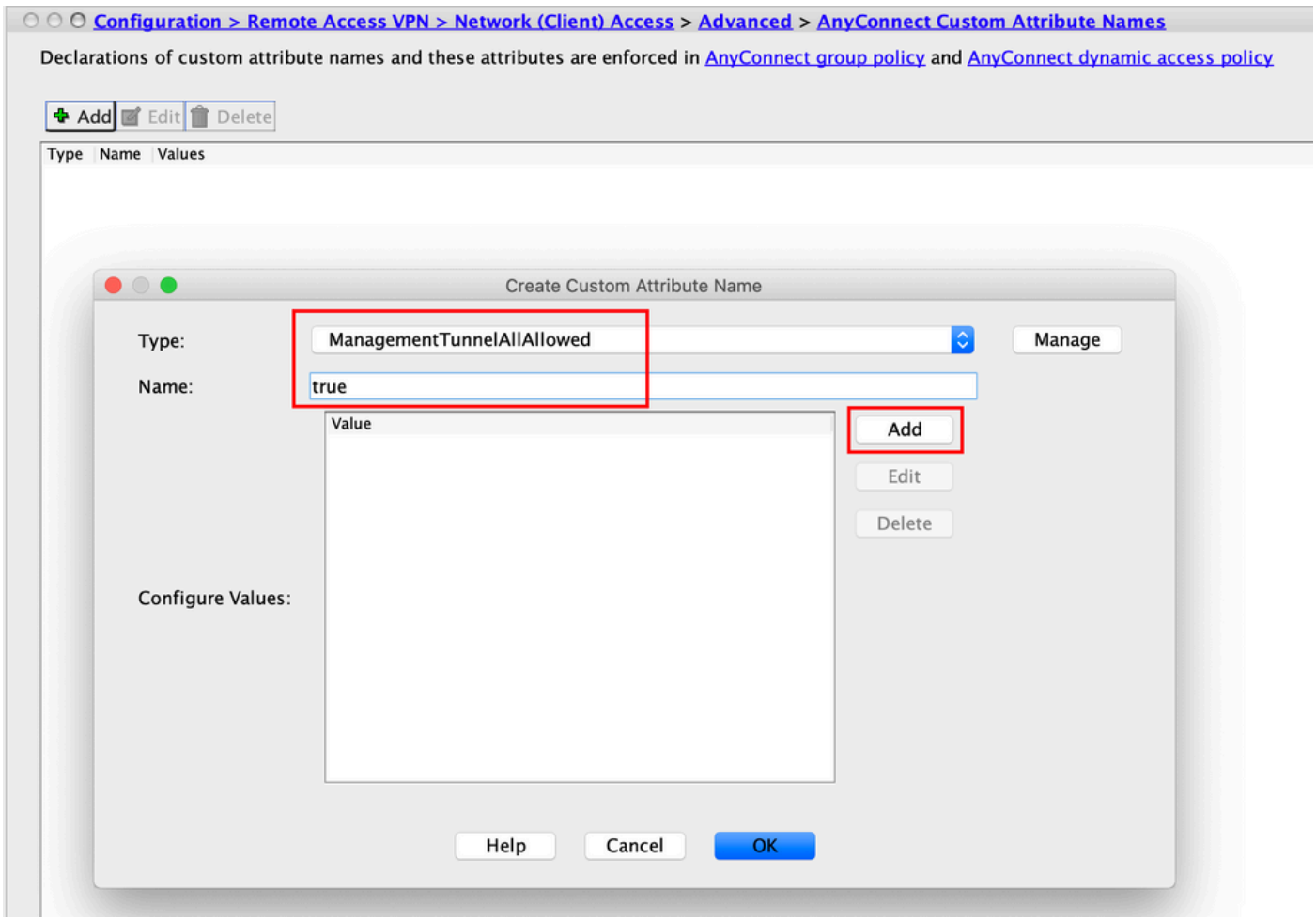
2단계. 사용자 지정 특성 유형 설정 ManagementTunnelAllAllowed Cisco의 Description. 클릭 OK에 나와 있는 것처럼.



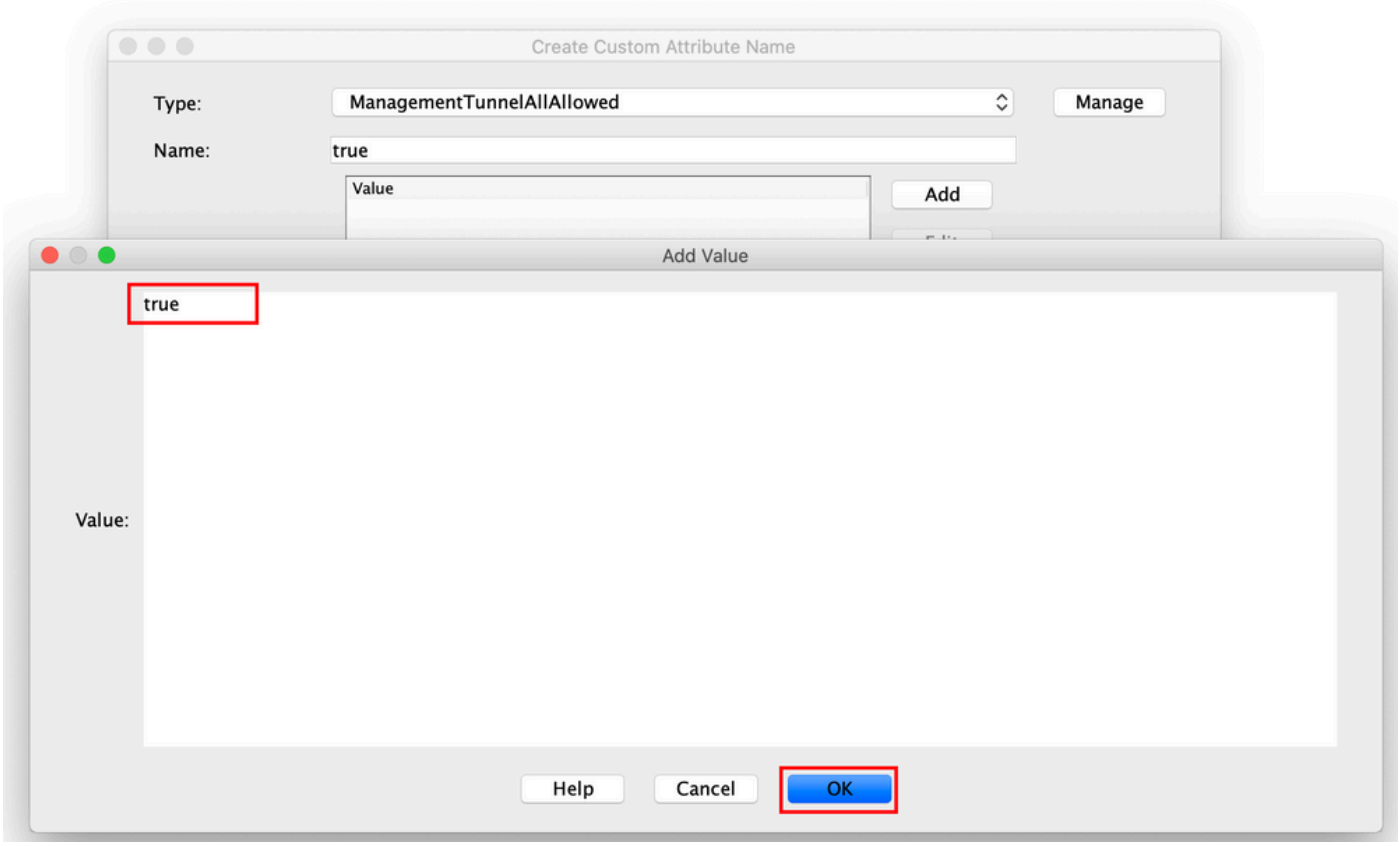
3단계. 탐색 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** 클릭 Add에 나와 있는 것처럼.



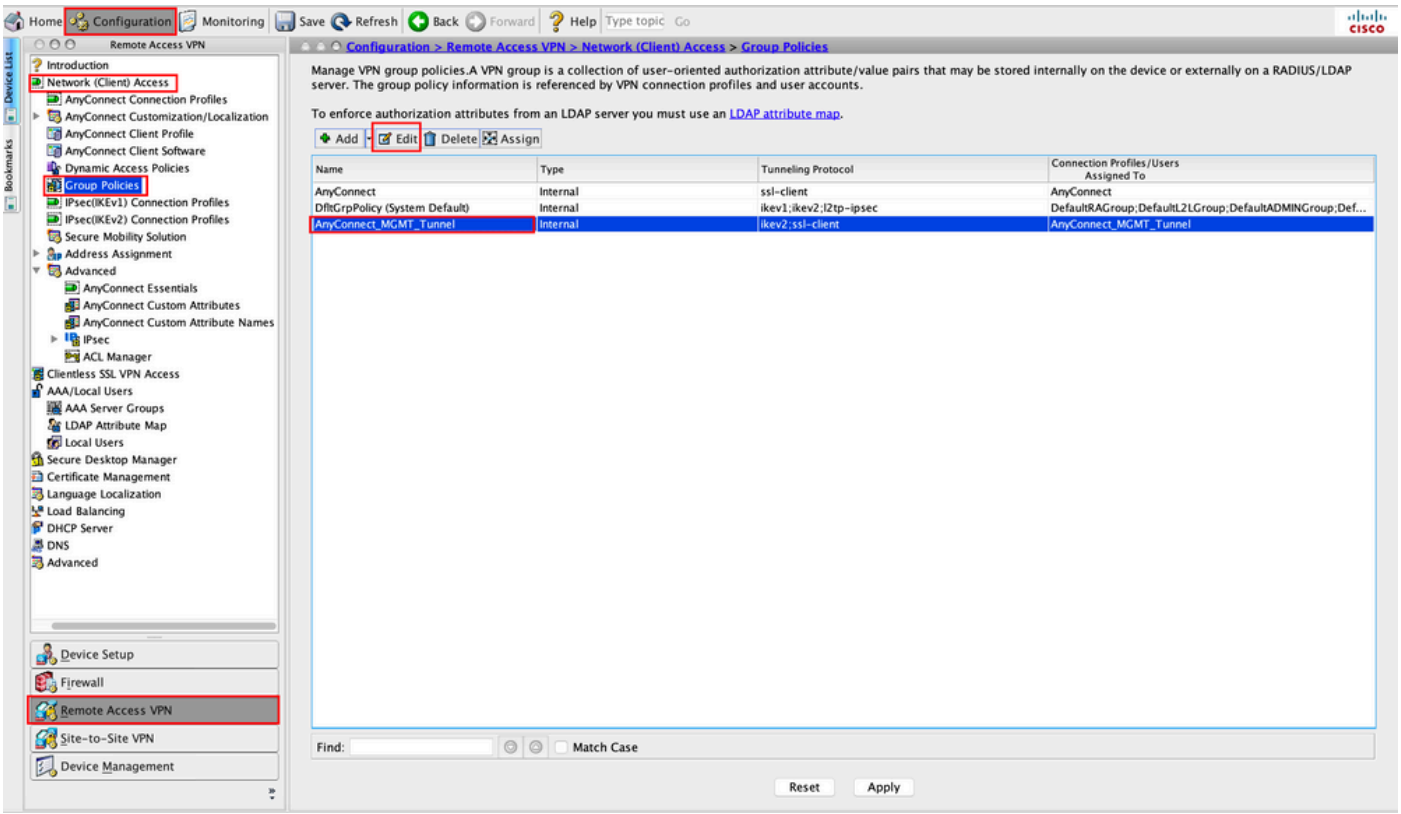
4단계. Type(유형)을 ManagementTunnelAllAllowed . Name(이름)을 true. 클릭 Add- 이미지에 표시된 대로 사용자 지정 특성 값을 제공합니다.



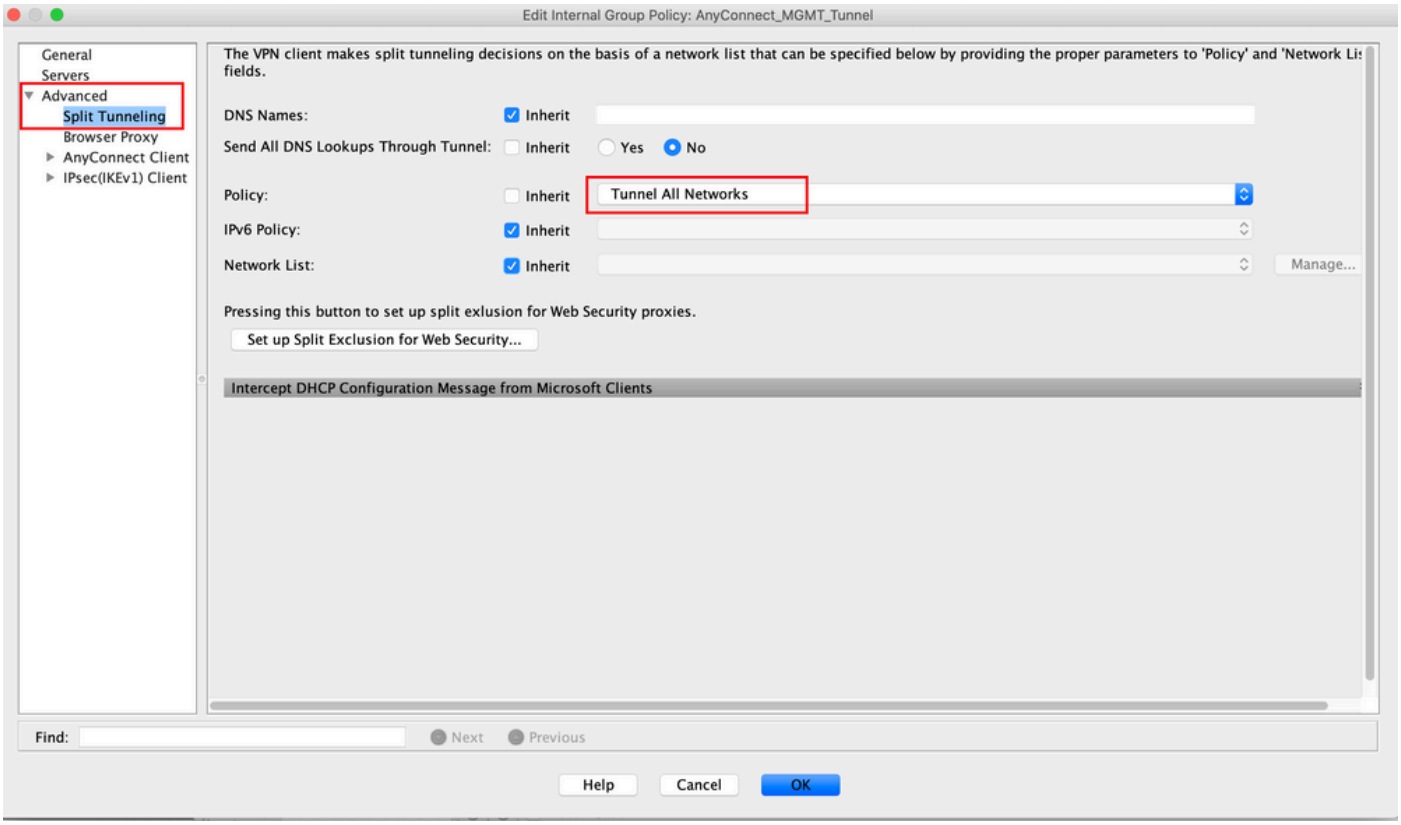
5단계. 값 설정 true. 클릭 OK에 나와 있는 것처럼.



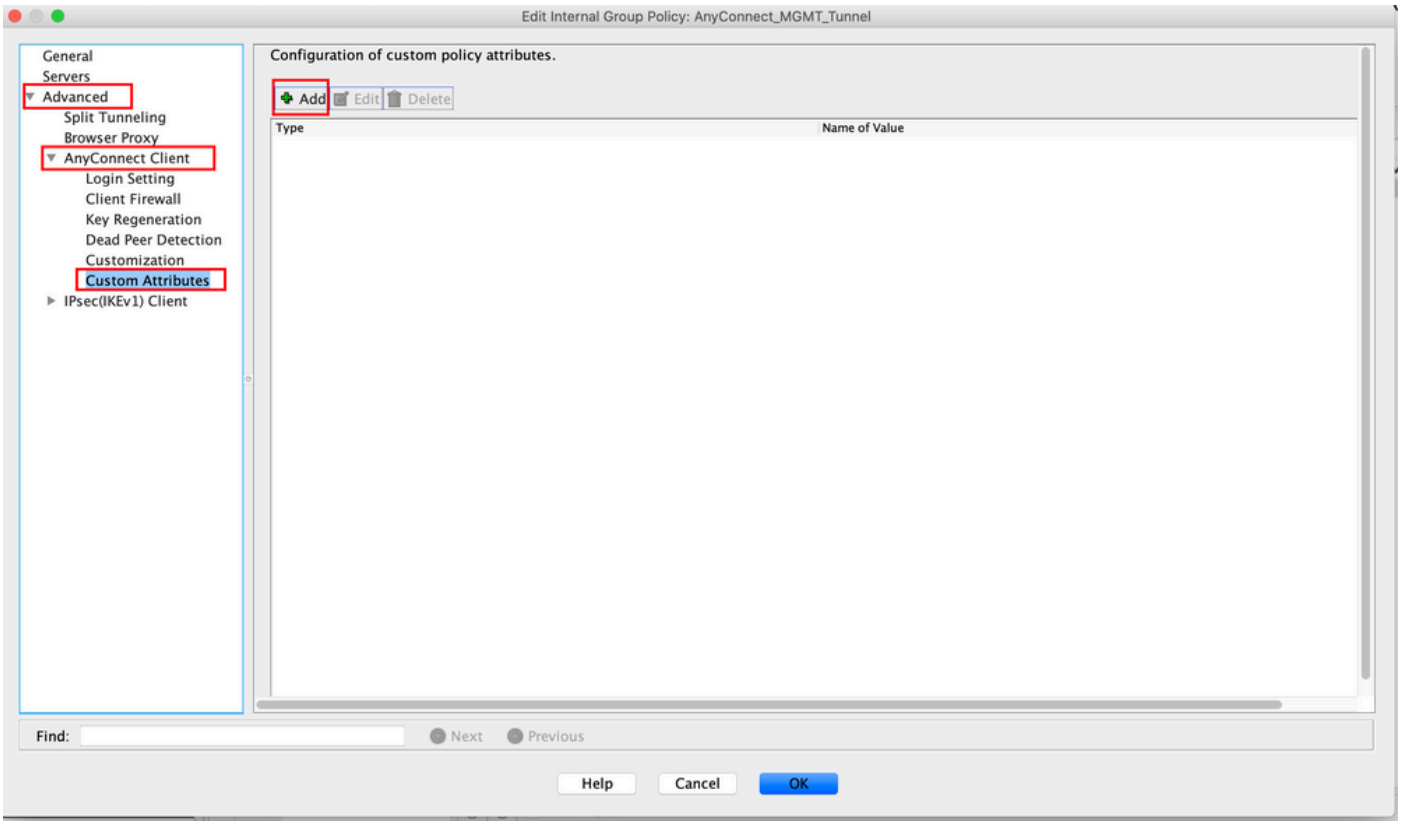
6단계. 탐색 Configuration > Remote Access VPN > Network (Client) Access > Group Policies. 그룹 정책을 선택합니다. 클릭 Edit 에 나와 있는 것처럼.



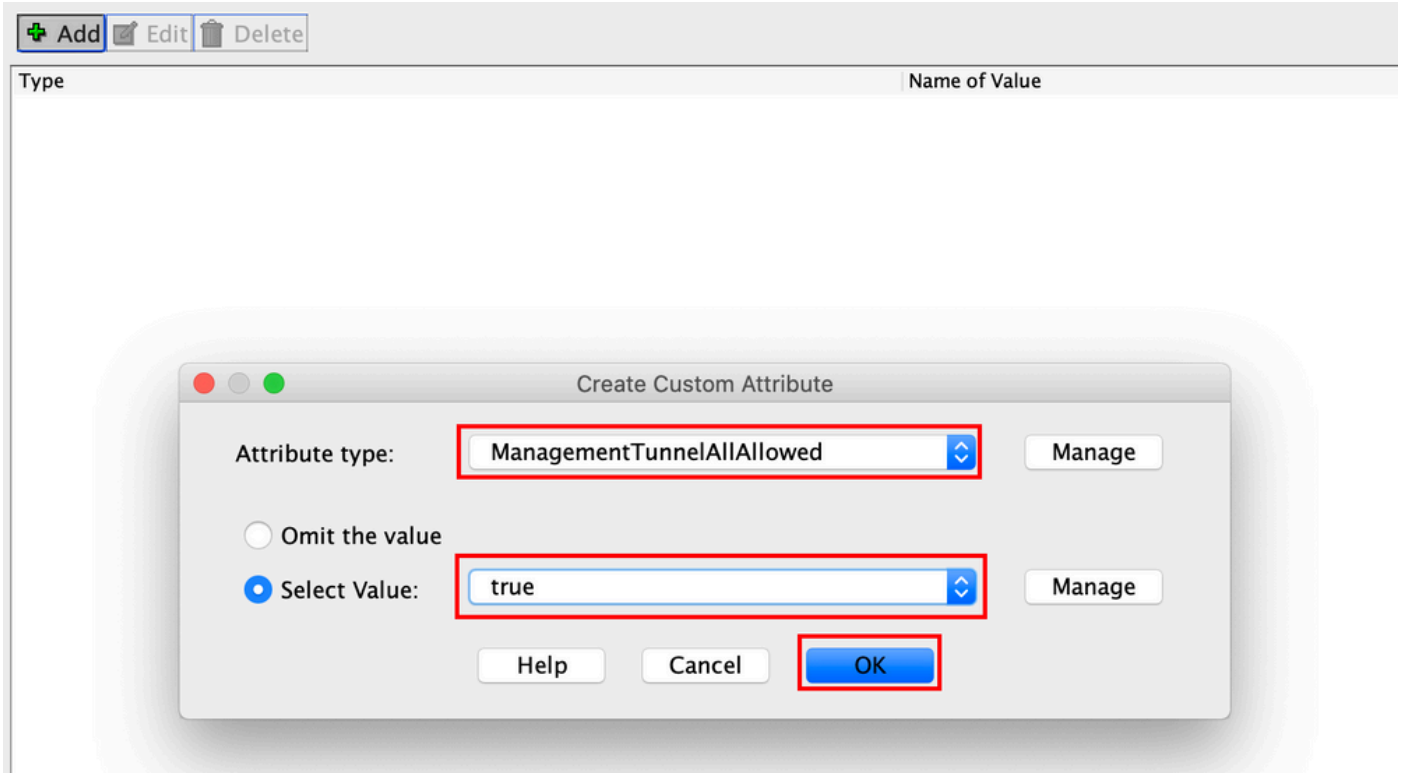
7단계. 이 이미지에 표시된 대로 Advanced > Split Tunneling. 정책 구성 Tunnel All Networks.



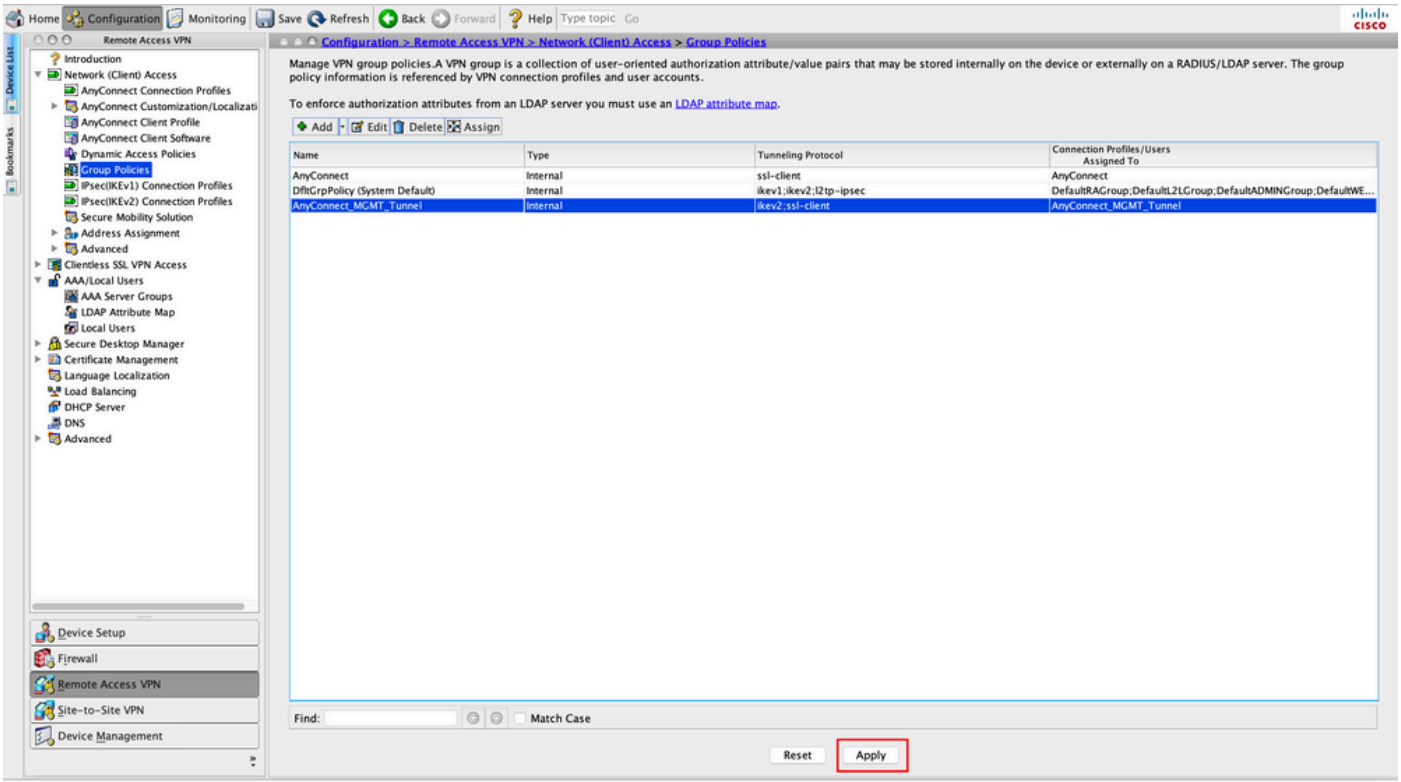
8단계. 탐색 Advanced > Anyconnect Client > Custom Attributes. 클릭 Add에 나와 있는 것처럼.



9단계. 특성 유형을 다음과 같이 선택합니다. ManagementTunnelAllAllowed Value as(값)를 true. 클릭 OK에 나와 있는 것처럼.



10단계. 클릭 Apply 를 클릭하면 그림과 같이 ASA에 컨피그레이션을 푸시합니다.



다음 이후의 CLI 컨피그레이션 ManagementTunnelAllAllowed 사용자 지정 특성이 추가되었습니다.

```
webvpn
 enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
 hsts
  enable
  max-age 31536000
```

```
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
anyconnect-custom-data ManagementTunnelAllAllowed true true
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelall
 client-bypass-protocol enable
 address-pools value VPN_Pool
 anyconnect-custom ManagementTunnelAllAllowed value true
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

다음을 확인합니다.

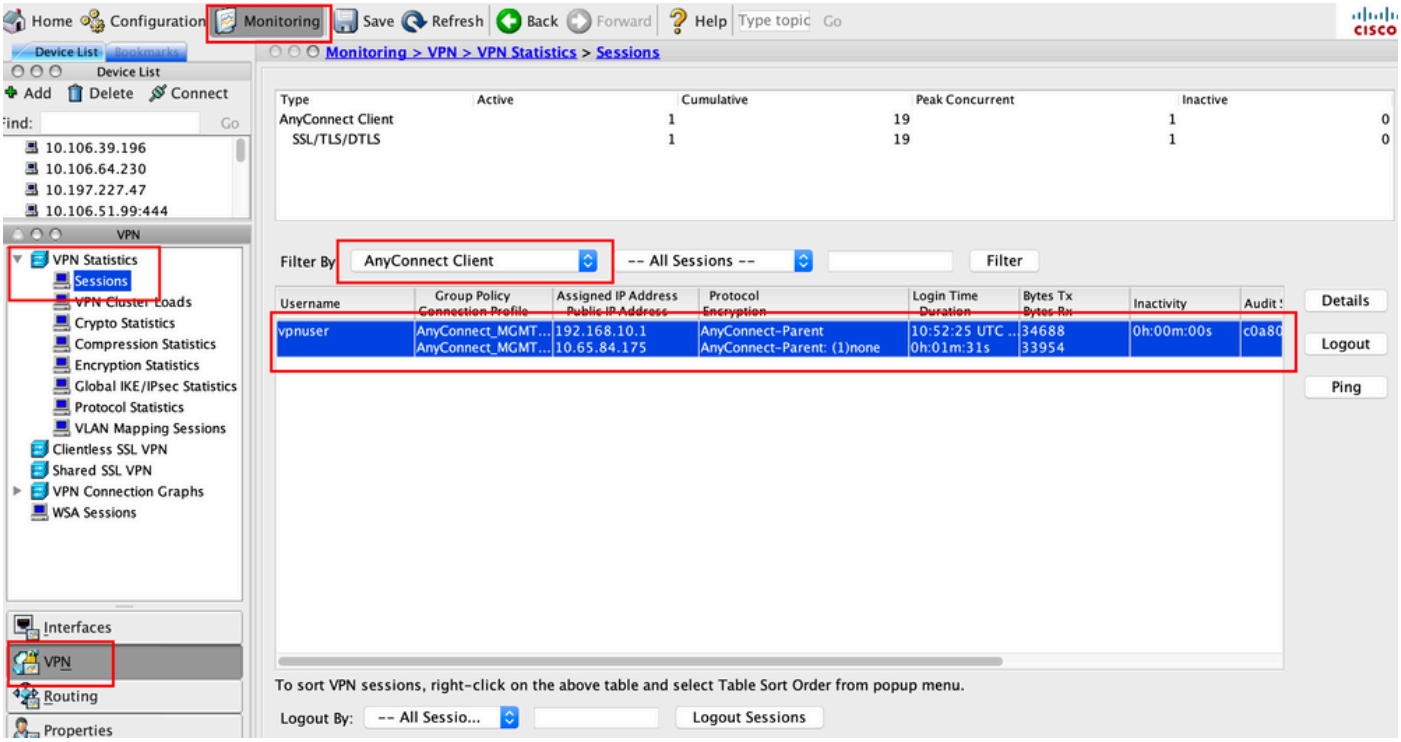
ASA CLI에서 관리 VPN 터널 연결을 show vpn-sessiondb detail anyconnect 명령을 실행합니다.

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 10
Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-
256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time   : 01:23:55 UTC Tue Apr 14 2020
Duration     : 0h:11m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none

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

--- Output Omitted ---
DTLS-Tunnel:
  Tunnel ID    : 10.3
  Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 57053
```

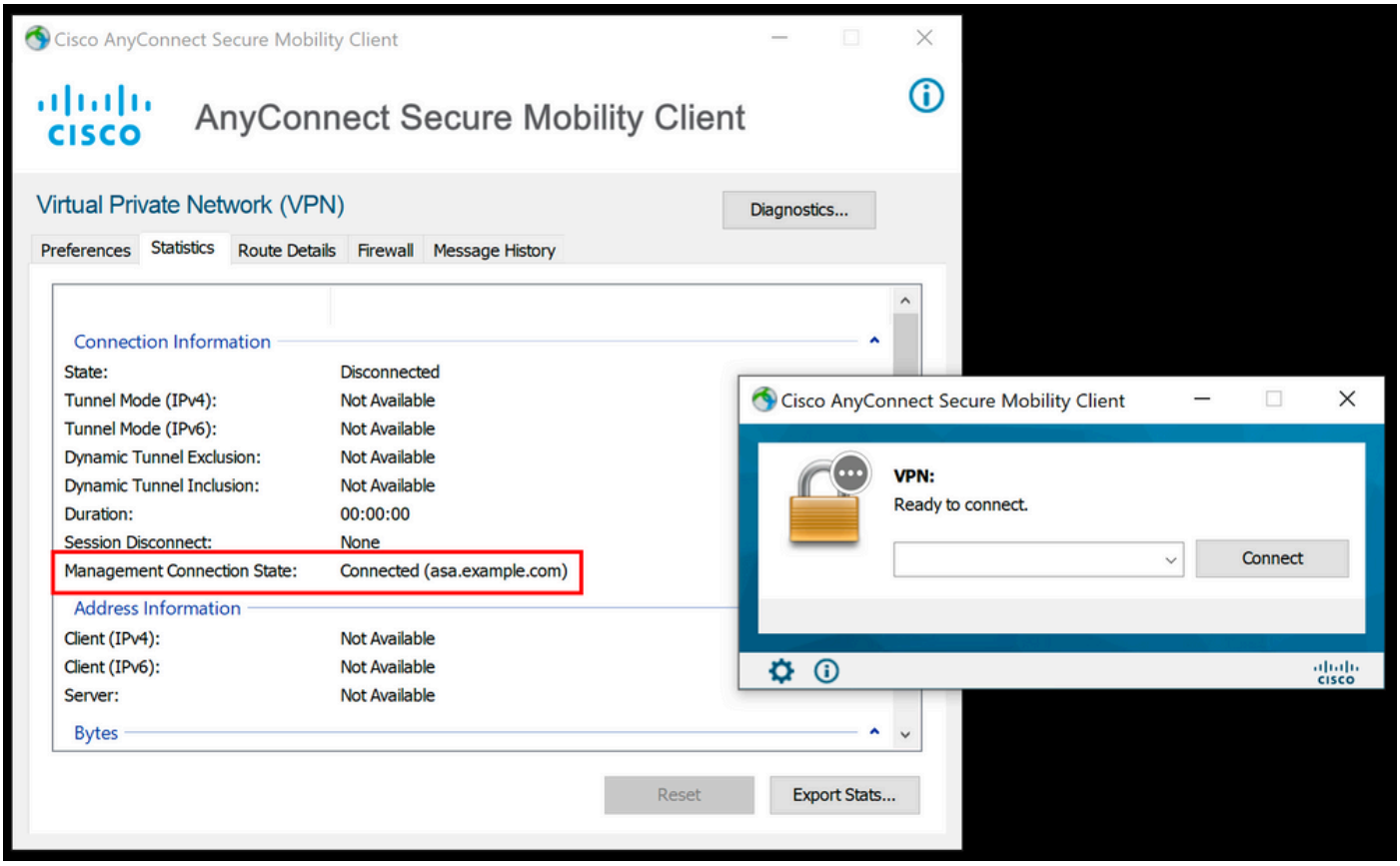
```
UDP Dst Port : 443                    Auth Mode     : Certificate
Idle Time Out: 30 Minutes             Idle TO Left  : 18 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx     : 17238                  Bytes Rx      : 1988
Pkts Tx      : 12                     Pkts Rx       : 13
Pkts Tx Drop : 0                      Pkts Rx Drop  : 0
```

ASDM에서 관리 VPN 터널 연결을 확인합니다.

Monitoring(**모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션)로 이동합니다**. 클라이언트 세션**을** 보려면 AnyConnect 클라이언트로 필터링합니다.



클라이언트 컴퓨터에서 관리 VPN 터널 연결 확인:



문제 해결

새 UI Statistics 라인(Management Connection State(관리 연결 상태))을 사용하여 관리 터널 연결 문제를 해결할 수 있습니다. 일반적으로 나타나는 오류 상태입니다.

연결 끊김(사용 안 함):

- 기능이 비활성화되어 있습니다.
- 사용자 터널 연결(사용자 터널 그룹 정책에 관리 VPN 프로파일을 추가해야 함)을 통해 관리 VPN 프로파일이 클라이언트에 배포되었거나 프로파일 수동 업로드를 통해 대역 외 상태인지 확인합니다.
- 관리 VPN 프로필이 터널 그룹을 포함하는 단일 호스트 항목으로 구성되어 있는지 확인합니다.

연결 끊김(신뢰할 수 있는 네트워크):

- TND가 트러스트된 네트워크를 탐지하여 관리 터널이 설정되지 않았습니다.

연결 끊김(사용자 터널 활성):

- 사용자 VPN 터널이 현재 활성 상태입니다.

연결 끊김(프로세스 시작 실패):

- 관리 터널 연결을 시도하는 동안 프로세스 시작 오류가 발생했습니다.

연결 끊김(연결 실패):

- 관리 터널을 설정하는 동안 연결 오류가 발생했습니다.
- 인증서 인증이 터널 그룹에 구성되어 있고 그룹 정책에 배너가 없으며 서버 인증서를 신뢰할 수 있어야 합니다.

연결 끊김(잘못된 VPN 구성):

- VPN 서버에서 잘못된 스플릿 터널링 구성을 받았습니다.
- 관리 터널 그룹 정책에서 스플릿 터널링 컨피그레이션을 확인합니다.

연결 끊김(소프트웨어 업데이트 보류 중):

- AnyConnect 소프트웨어 업데이트가 현재 보류 중입니다.

연결 끊김:

- 관리 터널이 설치되려고 하거나 다른 이유로 설치할 수 없습니다.

추가 트러블슈팅을 위해 DART를 수집합니다.

관련 정보

- 관리 VPN 터널 구성
- 관리 VPN 터널 문제 해결
- 기술 지원 및 문서 – Cisco Systems

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.