

# FDM에서 관리하는 FTD에 원격 액세스 VPN 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[라이센싱](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

#### [구성](#)

[네트워크 다이어그램](#)

[FTD에서 라이선싱 확인](#)

[보호 네트워크 정의](#)

[로컬 사용자 생성](#)

[인증서 추가](#)

[원격 액세스 VPN 구성](#)

[다음을 확인합니다.](#)

#### [문제 해결](#)

[AnyConnect 클라이언트 문제](#)

[초기 연결 문제](#)

[트래픽 관련 문제](#)

---

## 소개

이 문서에서는 버전 6.5.0 이상을 실행하는 온박스 관리자 FDM에서 관리하는 FTD에 RA VPN을 구축하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

FDM(Firepower Device Manager)의 RA VPN(Remote Access Virtual Private Network) 컨피그레이션에 대해 알고 있는 것이 좋습니다.

### 라이센싱

- FTD(Firepower Threat Defense)가 Export Controlled Features(내보내기 제어 기능)가 활성화된 상태로 스마트 라이선싱 포털에 등록되었습니다(RA VPN 구성 탭을 활성화하기 위해).
- 활성화된 모든 AnyConnect 라이선스(APEX, Plus 또는 VPN 전용)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 6.5.0-115를 실행하는 Cisco FTD
- Cisco AnyConnect Secure Mobility Client 버전 4.7.01076

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.

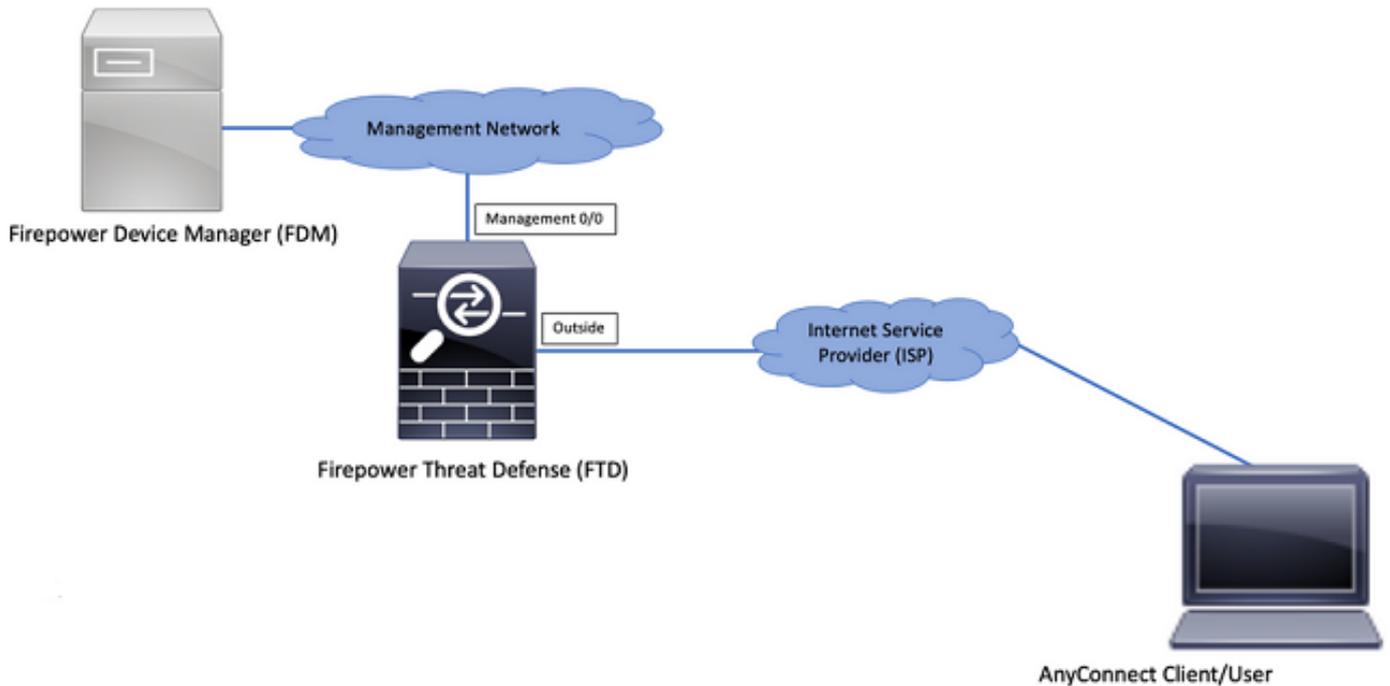
## 배경 정보

FDM을 통한 FTD 구성은 동일한 인터페이스를 통해 관리에 액세스하는 동안 외부 인터페이스를 통해 AnyConnect 클라이언트에 대한 연결을 설정하려고 시도할 때 어려움이 있습니다. 이는 FDM의 알려진 제한 사항입니다. 이 문제에 대한 개선 요청 CSCvm76499가 제출되었습니다.

## 구성

### 네트워크 다이어그램

로컬을 사용하는 AnyConnect 클라이언트 인증



### FTD에서 라이선싱 확인

1단계. 이미지에 표시된 대로 디바이스가 Smart Licensing에 등록되었는지 확인합니다.

Firepower Device Manager

Monitoring Policies Objects **Device: firepower**

Model: Cisco Firepower Threat Defense for VMWa... Software: 6.5.0-115 VDB: 309.0 Rule Update: 2019-08-12-001-vrt High Availability: Not Configured

<b>Interfaces</b> Connected Enabled 3 of 4 <a href="#">View All Interfaces</a>	<b>Routing</b> There are no routes yet <a href="#">Create the first static route</a>	<b>Updates</b> Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds <a href="#">View Configuration</a>	<b>System Settings</b> <a href="#">Management Access</a> <a href="#">Logging Settings</a> <a href="#">DHCP Server</a> <a href="#">DNS Server</a> <a href="#">Management interface</a> <a href="#">Hostname</a> <a href="#">NTP</a> <a href="#">Cloud Services</a> <a href="#">Reboot/Shutdown</a> <b>Traffic Settings</b> <a href="#">URL Filtering Preferences</a>
<b>Smart License</b> Registered <a href="#">View Configuration</a>	<b>Backup and Restore</b> <a href="#">View Configuration</a>	<b>Troubleshoot</b> No files created yet REQUEST FILE TO BE CREATED	
<b>Site-to-Site VPN</b> There are no connections yet <a href="#">View Configuration</a>	<b>Remote Access VPN</b> Requires RA VPN license No connections   1 Group Policy <a href="#">View Configuration</a>	<b>Advanced Configuration</b> Includes: FlexConfig, Smart CLI <a href="#">View Configuration</a>	<b>Device Administration</b> Audit Events, Deployment History, Download Configuration <a href="#">View Configuration</a>

2단계. 이미지에 표시된 대로 디바이스에서 AnyConnect 라이선스가 활성화되어 있는지 확인합니다.

Device Summary  
Smart License

CONNECTED SUFFICIENT LICENSE  
Last sync: 04 Apr 2020 02:10 PM  
Next sync: 04 Apr 2020 02:20 PM  
Go to Cloud Services

SUBSCRIPTION LICENSES INCLUDED

**Threat** ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

**Malware** ENABLE

Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

**URL License** ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

**RA VPN License** Type: APEX AND PLUS DISABLE

Enabled

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

**Base License** ENABLED ALWAYS

Enabled

3단계. 이미지에 표시된 대로 토큰에서 Export-controlled Features가 활성화되어 있는지 확인합니다.

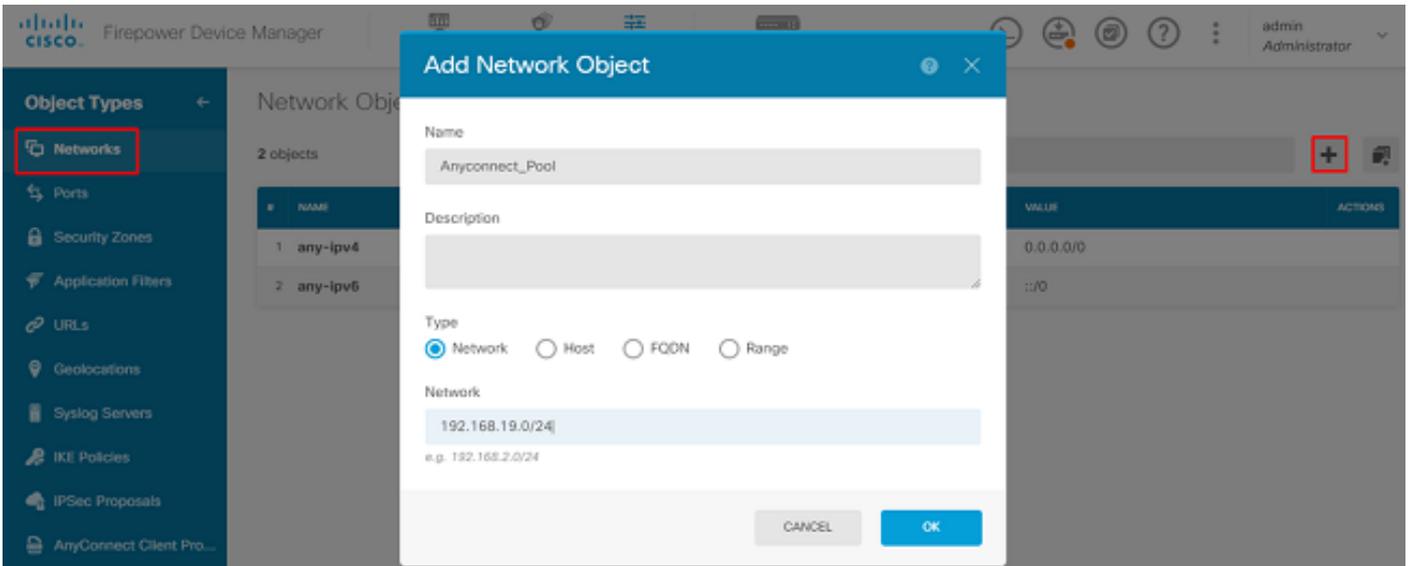
Device Summary  
Smart License

CONNECTED SUFFICIENT LICENSE  
Last sync: 04 Apr 2020 02:10 PM  
Next sync: 04 Apr 2020 02:20 PM

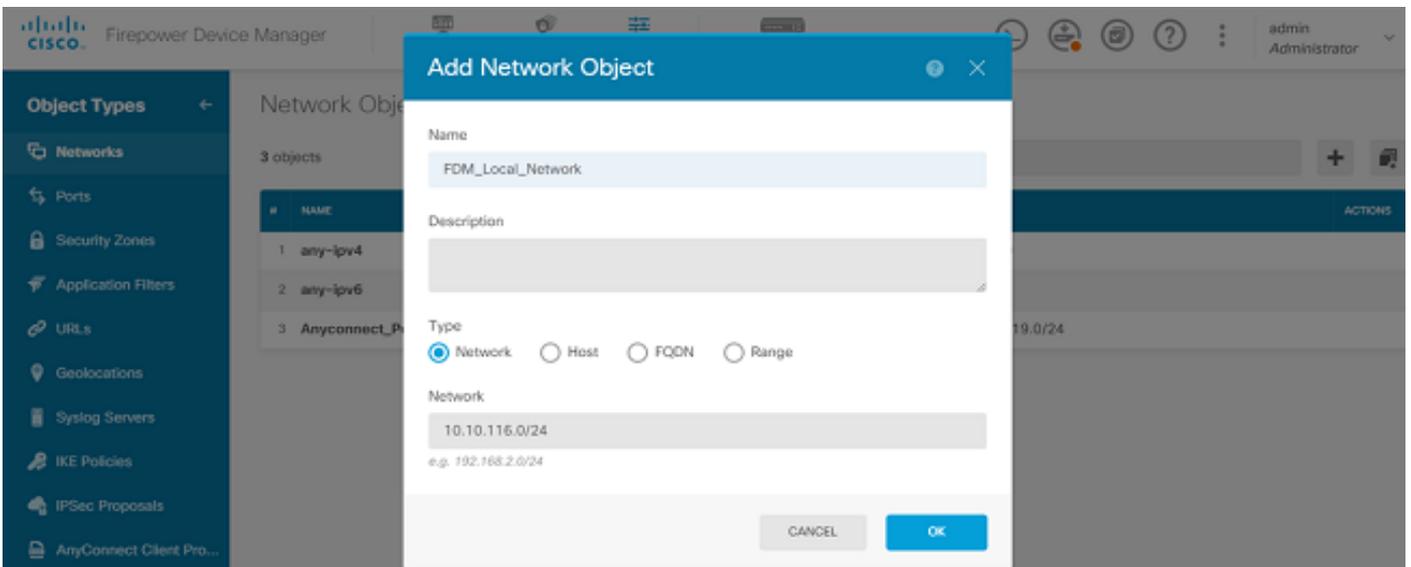
Assigned Virtual Account: SEC TAC  
Export-controlled features: Enabled  
Go to [Cisco Smart Software Manager](#).

## 보호 네트워크 정의

탐색 Objects > Networks > Add new Network. FDM GUI에서 VPN 풀 및 LAN 네트워크를 구성합니다. 이미지에 표시된 대로 AnyConnect 사용자에게 대한 로컬 주소 할당에 사용할 VPN 풀을 생성합니다.

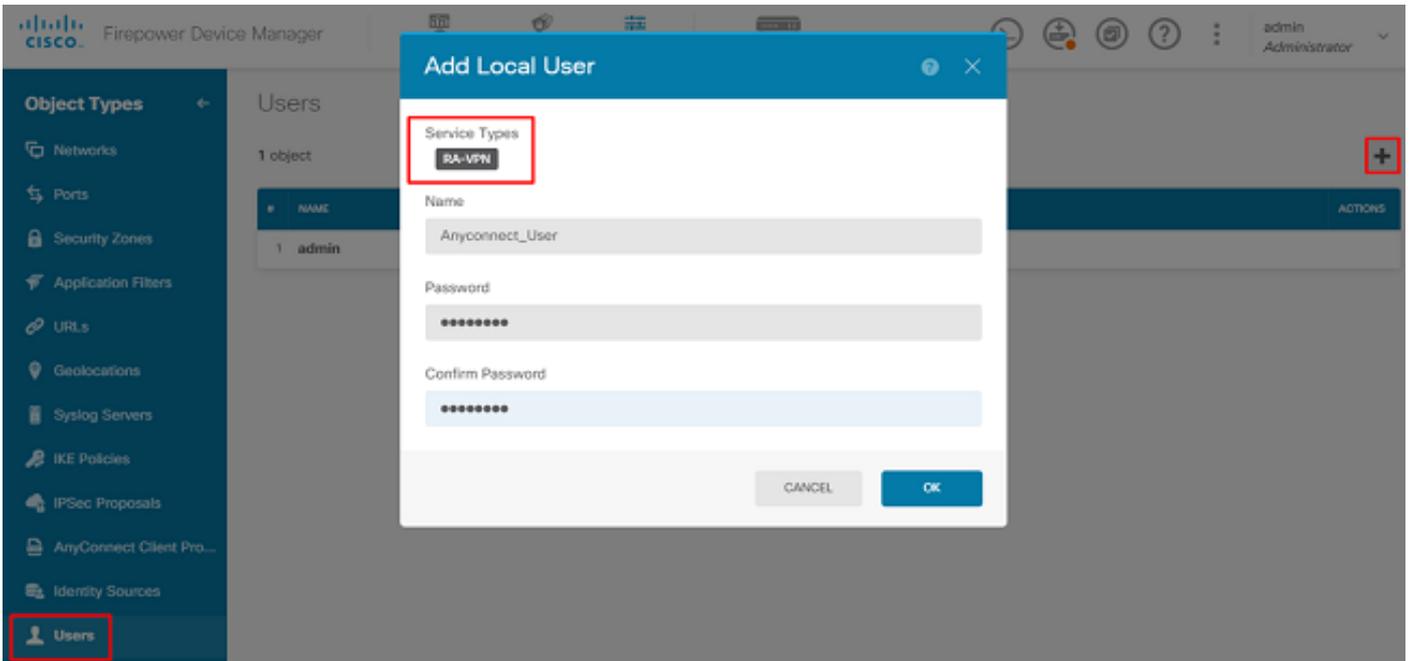


이미지에 표시된 대로 FDM 디바이스 뒤에 로컬 네트워크에 대한 객체를 생성합니다.



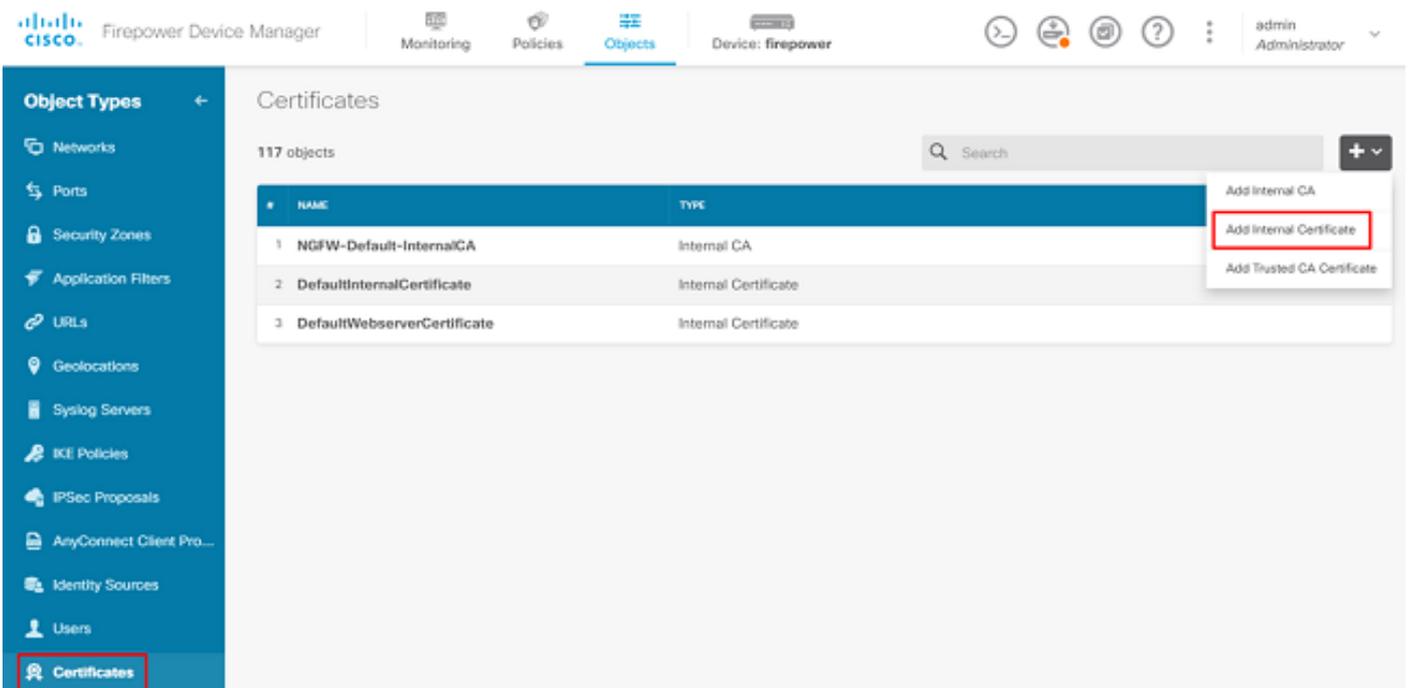
## 로컬 사용자 생성

탐색 Objects > Users > Add User. Anyconnect를 통해 FTD에 연결하는 VPN 로컬 사용자를 추가합니다. 이 이미지에 표시된 대로 로컬 사용자를 생성합니다.



## 인증서 추가

탐색 Objects > Certificates > Add Internal Certificate. 이미지에 표시된 대로 인증서를 구성합니다.



이미지에 표시된 대로 인증서와 개인 키를 모두 업로드합니다.



Choose the type of internal certificate you want to create



### Upload Certificate and Key

Create a certificate from existing files.  
PEM and DER files are supported.



### Self-Signed Certificate

Create a new certificate that is signed  
by the device.

그림과 같이 각 파일의 복사 및 붙여넣기 또는 업로드 버튼을 사용하여 인증서와 키를 업로드할 수 있습니다.

## Add Internal Certificate



Name

Anyconnect\_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjCgYEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jviv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGqqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

## 원격 액세스 VPN 구성

탐색 Remote Access VPN > Create Connection Profile. 이미지에 표시된 대로 FDM에서 RA VPN 마법사를 탐색합니다.

Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model Cisco Firepower Threat Defense for VMWa... Software 6.5.0-115 VDB 309.0 Rule Update 2019-08-12-001-vrt High Availability Not Configured CONFIGURE

Interfaces  
Connected  
Enabled 3 of 4  
View All Interfaces

Smart License  
Registered  
View Configuration

Site-to-Site VPN  
There are no connections yet  
View Configuration

Remote Access VPN  
Configured  
No connections | 1 Group Policy  
View Configuration

Routing  
There are no routes yet  
Create the first static route

Updates  
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds  
View Configuration

Troubleshoot  
No files created yet  
REQUEST FILE TO BE CREATED

Advanced Configuration  
Includes: FlexConfig, Smart CLI  
View Configuration

System Settings  
Management Access  
Logging Settings  
DHCP Server  
DNS Server  
Management Interface  
Hostname  
NTP  
Cloud Services  
Reboot/Shutdown  
Traffic Settings  
URL Filtering Preferences

Device Administration  
Audit Events, Deployment History, Download Configuration  
View Configuration

Firepower Device Manager

Monitoring Policies Objects Device: firepower

RA VPN

Connection Profiles

Group Policies

Device Summary  
Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

연결 프로파일을 생성하고 이미지에 표시된 대로 컨피그레이션을 시작합니다.

# Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

## Connection Profile Name

*This name is configured as a connection alias, it can be used to connect to the VPN gateway*

Anyconnect

## Group Alias

Anyconnect

[Add Group Alias](#)

## Group URL

[Add Group URL](#)

이미지에 표시된 인증 방법을 선택합니다. 이 설명서에서는 로컬 인증을 사용합니다.

## Primary Identity Source

Authentication Type

AAA Only  Client Certificate Only  AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource ▼

Fallback Local Identity Source ⚠

Please Select Local Identity Source ▼

Strip Identity Source server from username

Strip Group from Username

---

## Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source ▼

⌵ Advanced

---

Authorization Server

Please select ▼

Accounting Server

Please select ▼

다음을 선택합니다. Anyconnect\_Pool 그림과 같은 개체:

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect\_Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

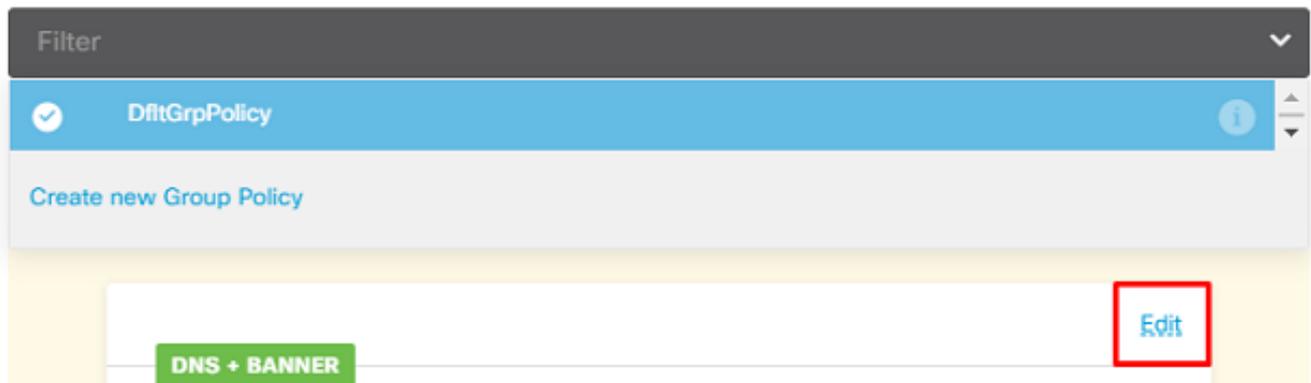
NEXT

기본 그룹 정책의 요약이 다음 페이지에 표시됩니다. 드롭다운을 누르고 다음 옵션을 선택하면 새 그룹 정책을 생성할 수 있습니다. *Create a new Group Policy.* 이 설명서에서는 기본 그룹 정책이 사용됩니다. 이미지에 표시된 대로 정책의 맨 위에 있는 수정 옵션을 선택합니다.

## Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

### View Group Policy



그룹 정책에서 분할 터널링을 추가하여 Anyconnect에 연결된 사용자가 Anyconnect 클라이언트를 통해 내부 FTD 네트워크로 향하는 트래픽만 전송하고 다른 모든 트래픽은 이미지에 표시된 대로 사용자의 ISP 연결에서 나가도록 합니다.

## Corporate Resources (Split Tunneling)

### IPv4 Split Tunneling

Allow specified traffic over tunnel



### IPv6 Split Tunneling

Allow all traffic over tunnel



### IPv4 Split Tunneling Networks



FDM\_Local\_Network

다음 페이지에서 `Anyconnect_Certificate certificate`(인증서) 섹션에 추가되었습니다. 다음으로, FTD가 AnyConnect 연결을 수신 대기하는 인터페이스를 선택합니다. 암호 해독된 트래픽에 대한 Bypass Access Control(액세스 제어 우회) 정책을 선택합니다(`sysopt permit-vpn`). 이 명령은 다음 경우에 사용할 수 있는 선택적 명령입니다. `sysopt permit-vpn` 이(가) 선택되지 않았습니다. 이미지에 표시된 대로 Anyconnect 클라이언트의 트래픽이 내부 네트워크에 액세스하도록 허용하는 액세스 제어 정책을 생성해야 합니다.

## Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

### Certificate of Device Identity

Anyconnect\_Certificate



### Outside Interface

outside (GigabitEthernet0/0)



### Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

### Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic



Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

아래에서 수동으로 NAT 제외를 구성할 수 있습니다. `Policies > NAT` 자동으로도 구성할 수도 있습니다. 이미지에 표시된 대로 Anyconnect 클라이언트가 액세스하기 위해 필요로 하는 내부 인터페이스 및 네트워크를 선택합니다.

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM\_Local\_Network

이미지에 표시된 대로 사용자가 연결할 수 있는 각 운영 체제(Windows/Mac/Linux)에 대한 Anyconnect 패키지를 선택합니다.

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com). You must have the necessary AnyConnect software license.

### Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

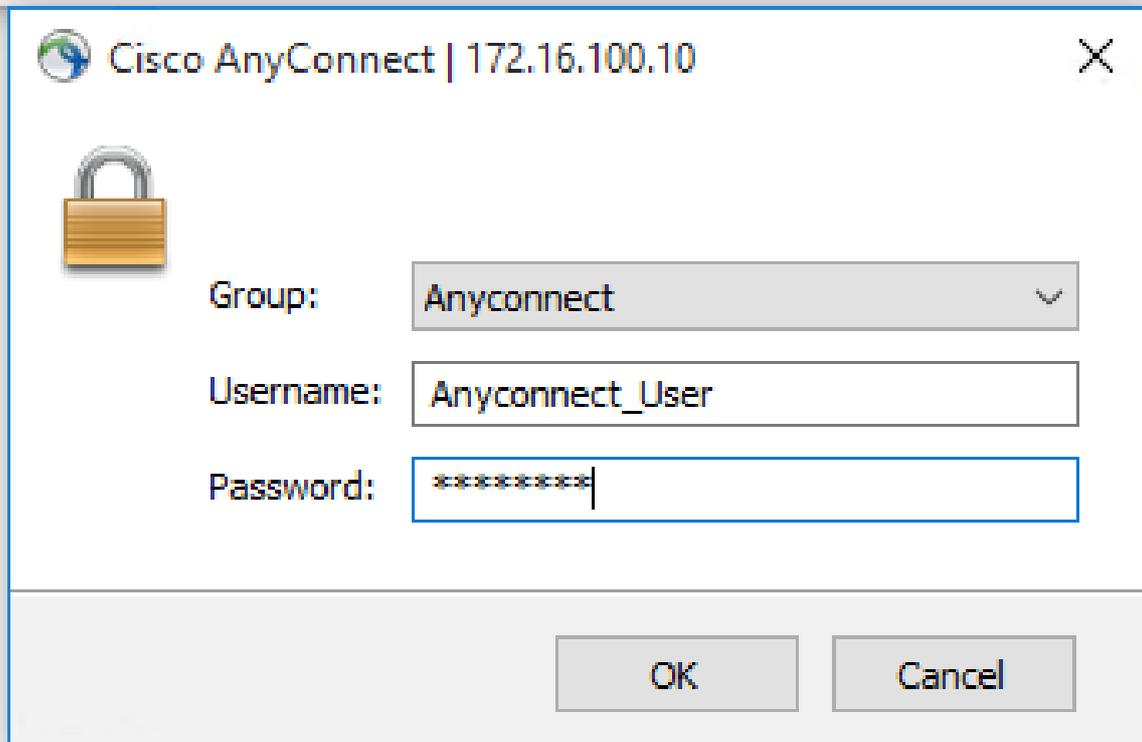
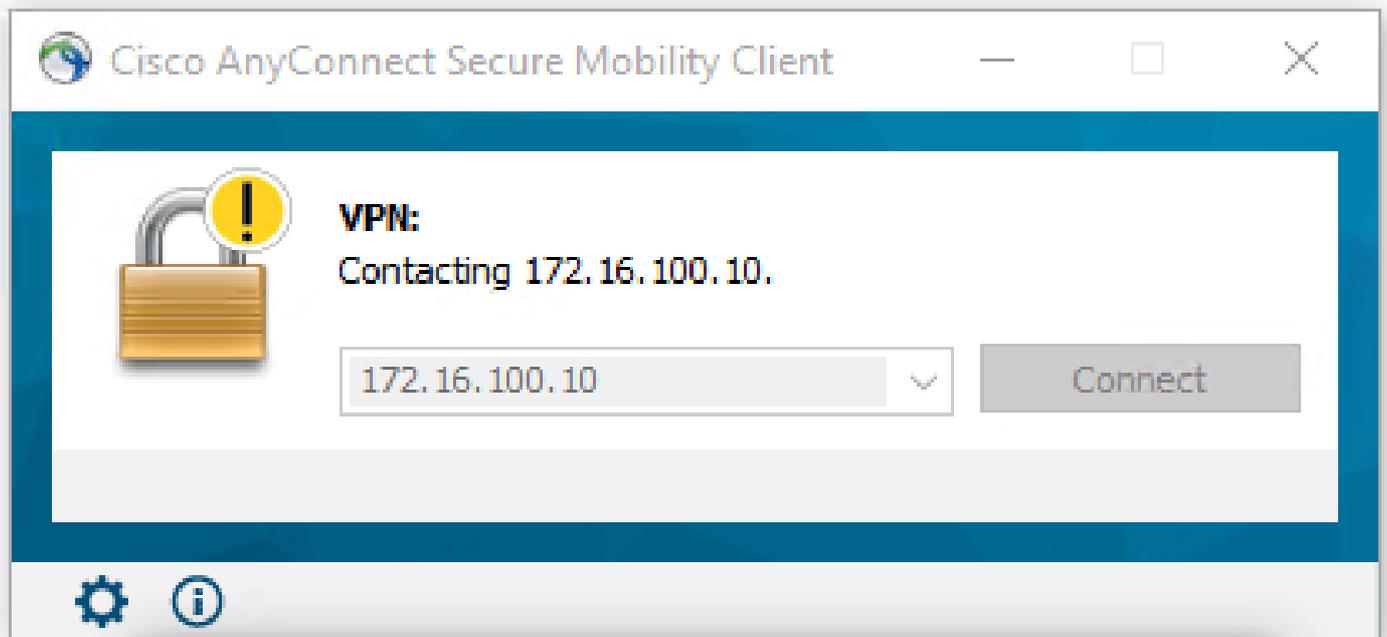
NEXT

마지막 페이지는 전체 구성에 대한 요약を提供합니다. 올바른 매개변수가 설정되었는지 확인하고 Finish(마침) 버튼을 누르고 새 컨피그레이션을 구축합니다.

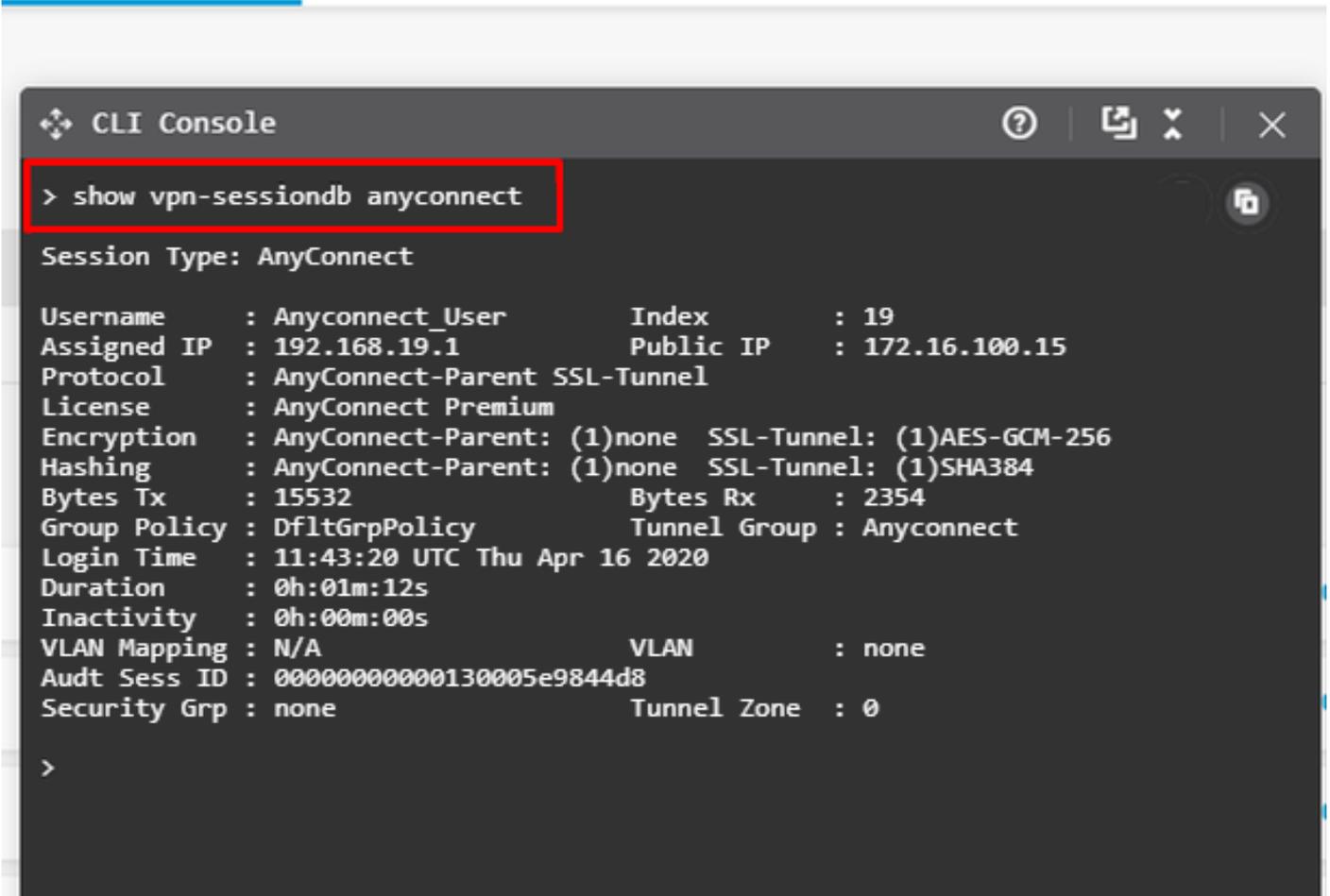
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

컨피그레이션이 구축되면 연결을 시도합니다. FTD의 외부 IP로 확인되는 FQDN이 있는 경우 Anyconnect 연결 상자에 입력합니다. 이 예에서는 FTD의 외부 IP 주소가 사용됩니다. 이미지에 표시된 대로 FDM의 [객체] 섹션에서 생성된 사용자 이름/비밀번호를 사용합니다.



FDM 6.5.0부터는 FDM GUI를 통해 Anyconnect 사용자를 모니터링할 방법이 없습니다. 유일한 옵션은 CLI를 통해 Anyconnect 사용자를 모니터링하는 것입니다. FDM GUI의 CLI 콘솔을 사용하여 사용자가 연결되었는지 확인할 수도 있습니다. 이 명령을 사용하여 `Show vpn-sessiondb anyconnect.`



동일한 명령을 CLI에서 직접 실행할 수 있습니다.

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1        Public IP  : 172.16.100.15
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      : 38830              Bytes Rx   : 172
Group Policy  : DfltGrpPolicy      Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                Tunnel Zone : 0
```

## 문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다.

사용자가 SSL을 사용하여 FTD에 연결할 수 없는 경우 SSL 협상 문제를 격리하려면 다음 단계를 수행합니다.

1. FTD 외부의 IP 주소가 사용자의 컴퓨터를 통해 ping될 수 있는지 확인합니다.
2. TCP 3-way 핸드셰이크의 성공 여부를 확인하려면 외부 스니퍼를 사용합니다.

## AnyConnect 클라이언트 문제

이 섹션에서는 가장 일반적인 두 가지 AnyConnect VPN 클라이언트 문제를 해결하기 위한 지침을 제공합니다. AnyConnect 클라이언트에 대한 트러블슈팅 가이드는 AnyConnect [VPN 클라이언트 트러블슈팅 가이드에서 확인할 수 있습니다](#).

### 초기 연결 문제

사용자에게 초기 연결 문제가 있는 경우 디버그를 활성화합니다 `webvpn` FTD에서 AnyConnect를 실행하고 디버그 메시지를 분석합니다. 디버그는 FTD의 CLI에서 실행해야 합니다. 다음 명령을 사용하여 `debug webvpn anyconnect 255`.

AnyConnect에서 로그를 가져오기 위해 클라이언트 시스템에서 DART 번들을 수집합니다. DART 번들을 수집하는 방법에 대한 지침은 DART 번들 수집을 [참조하십시오](#).

### 트래픽 관련 문제

연결에 성공했지만 트래픽이 SSL VPN 터널을 통해 실패할 경우 클라이언트의 트래픽 통계를 확인하여 트래픽이 클라이언트에서 수신 및 전송되는지 확인합니다. 자세한 클라이언트 통계는 모든 버전의 AnyConnect에서 사용할 수 있습니다. 클라이언트에서 트래픽이 전송 및 수신되고 있음을 표시하는 경우 FTD에서 수신 및 전송된 트래픽을 확인합니다. FTD에서 필터를 적용하면 필터 이름이 표시되고 ACL 항목을 확인하여 트래픽이 삭제되고 있는지 확인할 수 있습니다. 사용자가 겪는 일반적인 트래픽 문제:

- FTD 뒤에 라우팅 문제 - 내부 네트워크에서 할당된 IP 주소 및 VPN 클라이언트로 패킷을 다시 라우팅할 수 없습니다.
- 액세스 제어 목록 차단 트래픽
- VPN 트래픽에 대해 네트워크 주소 변환이 우회되지 않음

FDM에서 관리하는 FTD의 원격 액세스 VPN에 대한 자세한 내용은 FDM에서 관리하는 [Remote Access FTD](#)의 전체 구성 [설명서를 참조하십시오](#).

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.