

FTD에서 Anyconnect VPN 클라이언트 구성:주소 할당을 위한 DHCP 서버

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. DHCP 서버에서 DHCP 범위 구성](#)

[2단계. AnyConnect 구성](#)

[2.1단계. 연결 프로파일 구성](#)

[2.2단계. 그룹 정책 구성](#)

[2.3단계. 주소 할당 정책 구성](#)

[IP 헬퍼 시나리오](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 원격 액세스 VPN 세션에서 타사 DHCP(Dynamic Host Configuration Protocol) 서버에서 할당된 IP 주소를 가져올 수 있도록 버전 6.4의 FTD(Firepower Threat Defense)에 대한 컨피그레이션 예를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD
- FMC(Firepower Management Center).
- DHCP

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMC 6.5
- FTD 6.5
- Windows Server 2016

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 로컬 주소 풀에서 DHCP 주소 할당으로 변경하기 위해 FTD의 필수 컨피그레이션만 포함하여 전체 원격 액세스 컨피그레이션에 대해 설명하지 않습니다.

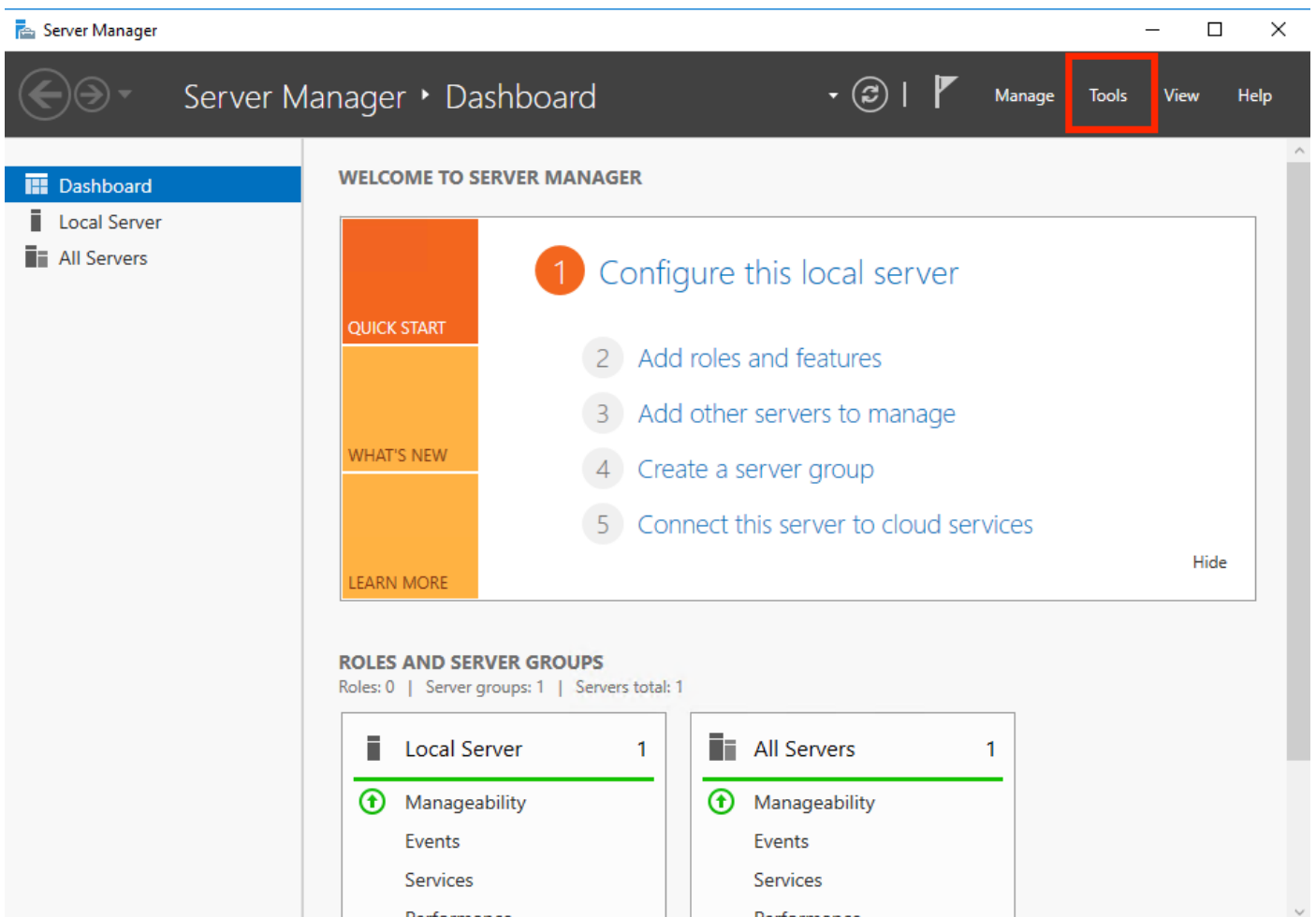
AnyConnect 컨피그레이션 예제 문서를 찾고 있는 경우 "Configure AnyConnect VPN Client on FTD: Healing and NAT Exemption" 문서

구성

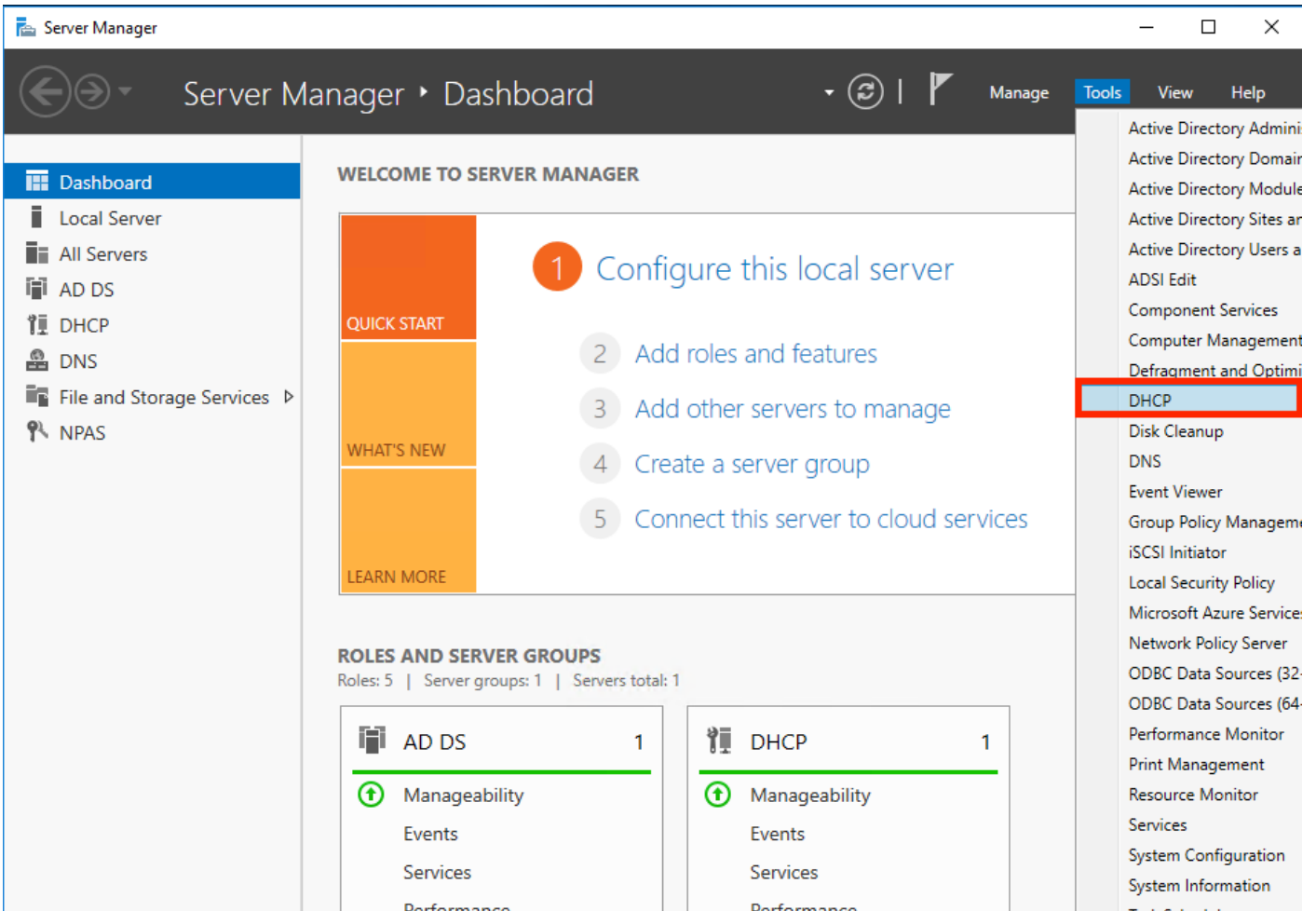
1단계. DHCP 서버에서 DHCP 범위 구성

이 시나리오에서는 DHCP 서버가 FTD의 내부 인터페이스 뒤에 있습니다.

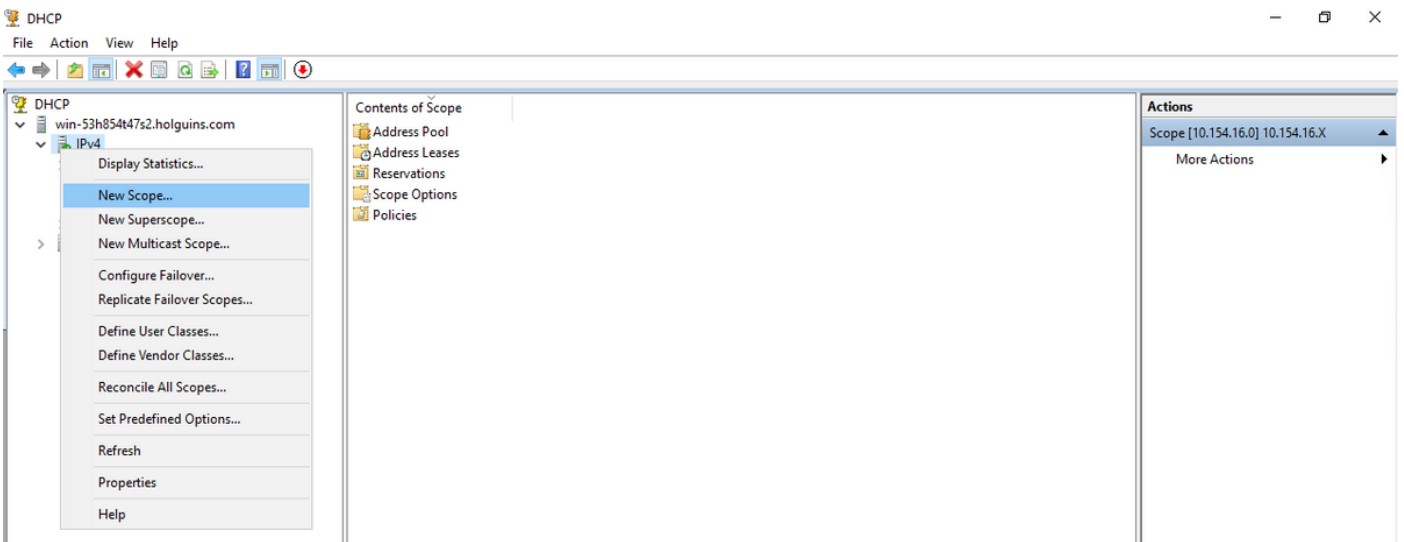
1. Windows 서버에서 서버 관리자를 열고 이미지에 표시된 대로 도구를 선택합니다.



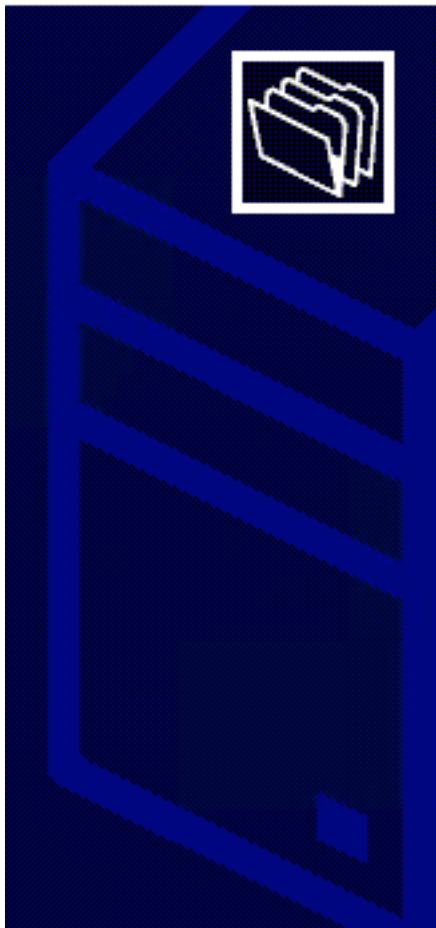
2. DHCP를 선택합니다.



3. IPv4를 선택하고 마우스 오른쪽 버튼으로 클릭한 다음 이미지에 표시된 새 범위를 선택합니다.



4. 이미지에 표시된 마법사를 따릅니다.



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back

Next >

Cancel

5. 이미지에 표시된 대로 범위에 이름을 지정합니다.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

6. 이미지에 표시된 대로 주소 범위를 구성합니다.

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

7.(선택 사항) 이미지에 표시된 대로 제외를 구성합니다.

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

8. 이미지에 표시된 대로 리스 기간을 구성합니다.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

Next >

Cancel

9.(선택 사항) DHCP 범위 옵션을 구성합니다.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

10:이 이미지에 표시된 대로 완료를 선택합니다.

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

Before clients can receive addresses you need to do the following:

1. Add any scope specific options (optional).
2. Activate the scope.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

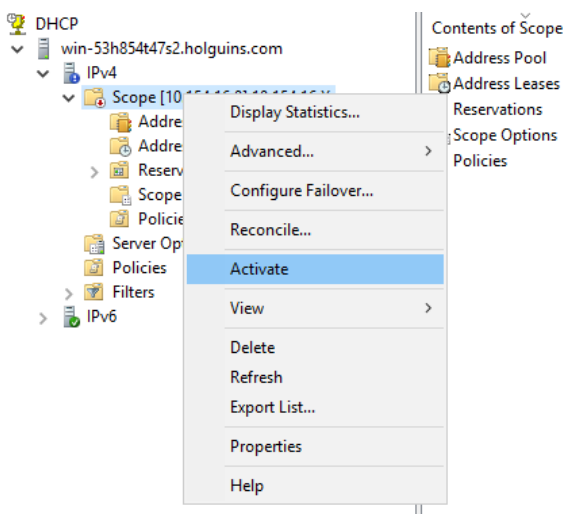
To close this wizard, click Finish.

< Back

Finish

Cancel


11:방금 생성한 범위를 마우스 오른쪽 버튼으로 클릭하고 이미지에 표시된 대로 **Activate**를 선택합니다.



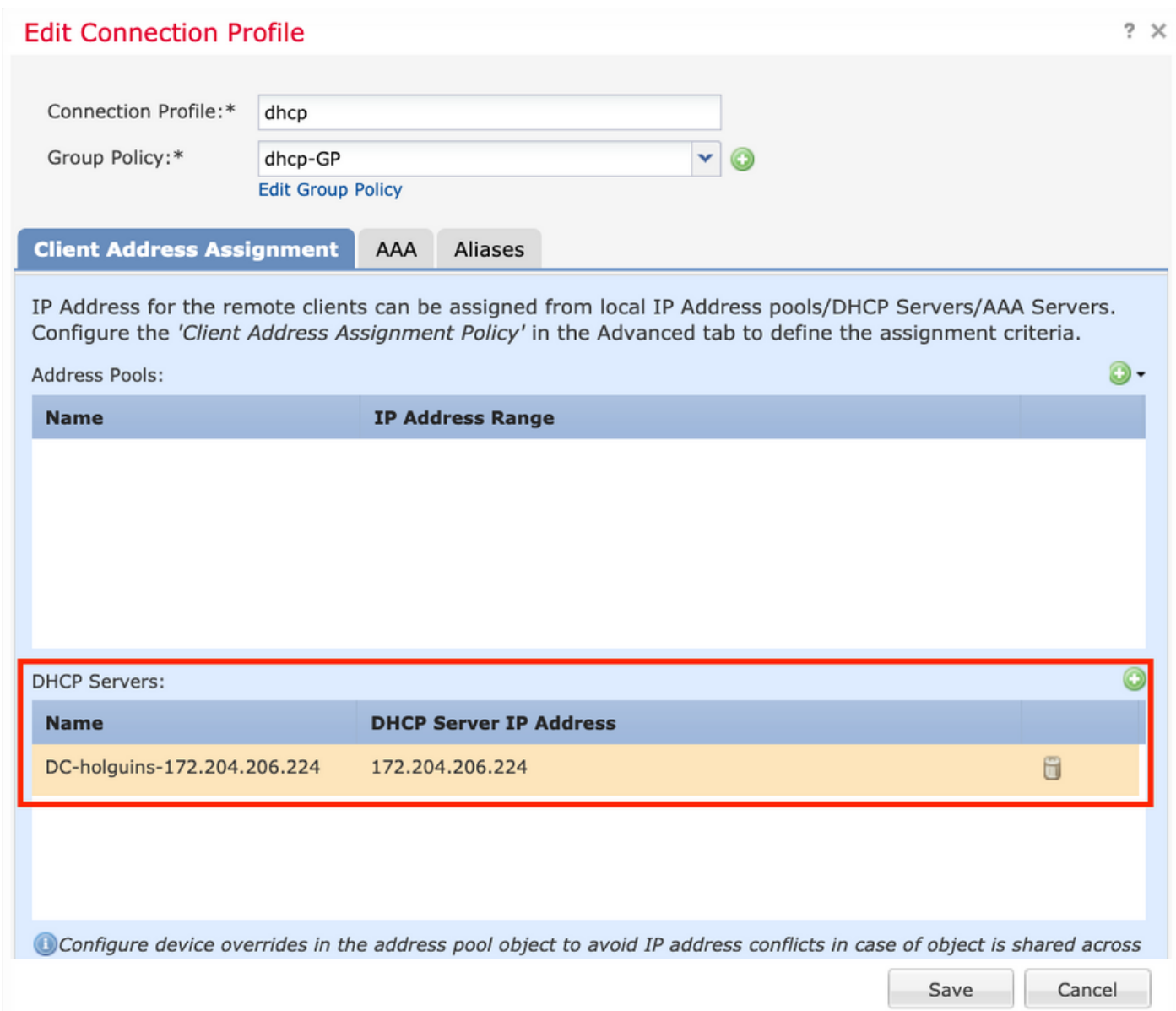
2단계. AnyConnect 구성

DHCP 범위가 구성 및 활성화되면 FMC에서 다음 절차가 수행됩니다.

2.1단계. 연결 프로파일 구성


1. DHCP Servers(DHCP 서버) 섹션에서  DHCP 서버의 IP 주소를 사용하여 개체를 만들고 기호를 클릭합니다.

2. 이미지에 표시된 대로 IP 주소를 요청하려면 객체를 DHCP 서버로 선택합니다.




Edit Connection Profile ? x

Connection Profile:* dhcp


Group Policy:* dhcp-GP  [Edit Group Policy](#)


Client Address Assignment AAA Aliases


IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools: 

Name	IP Address Range
------	------------------

DHCP Servers: 

Name	DHCP Server IP Address
DC-holguins-172.204.206.224	172.204.206.224 

 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across

Save Cancel

2.2단계. 그룹 정책 구성

1. Group Policy(그룹 정책) 메뉴 내에서 **General(일반) > DNS/WINS(DNS/WINS)**로 이동하고 이미지에 표시된 대로 **DHCP Network Scope(DHCP 네트워크 범위)** 섹션이 있습니다.

Edit Group Policy

? X

Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

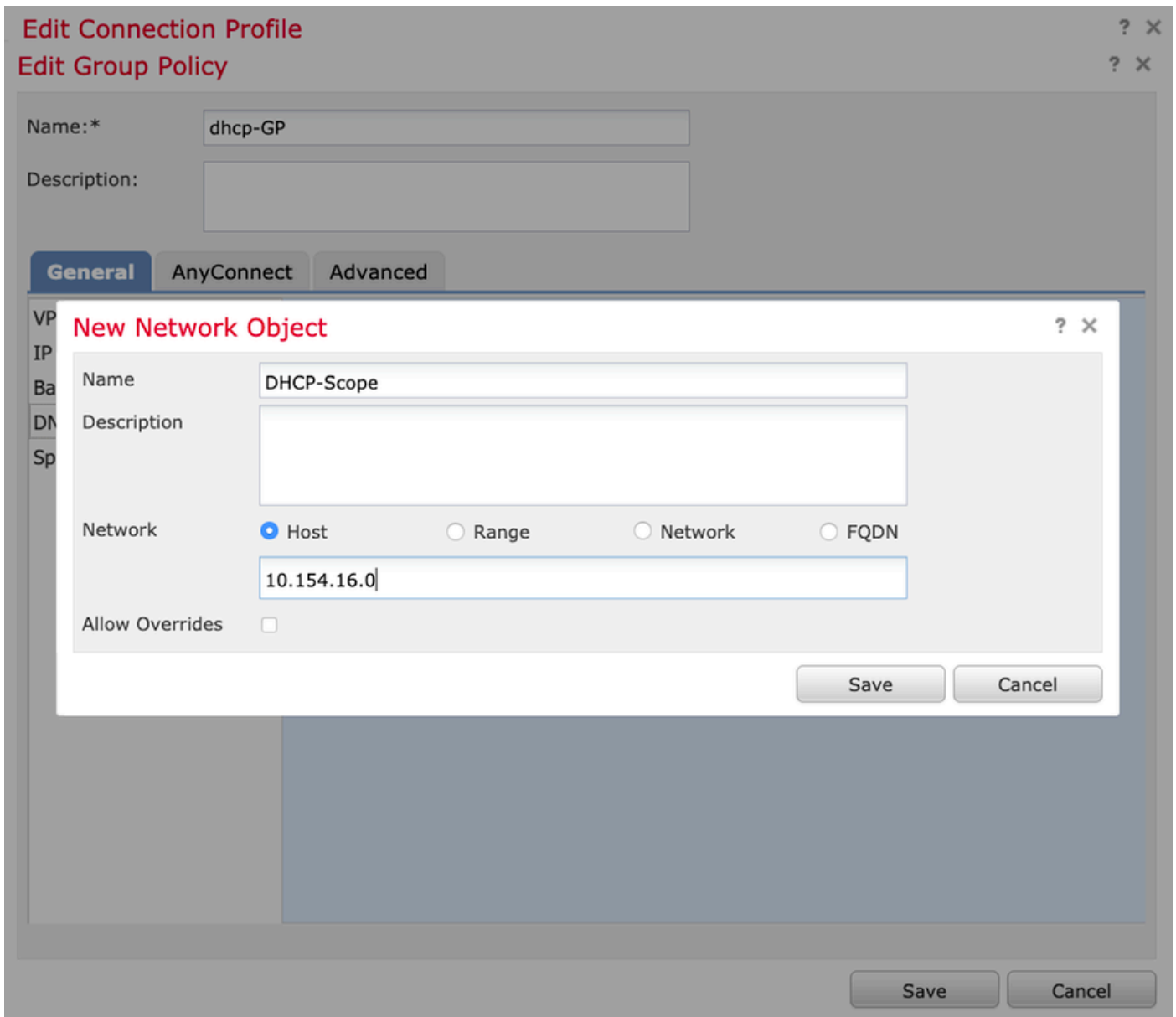
Secondary WINS Server:

DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

2. 새 개체를 만듭니다. 이 개체는 DHCP 서버와 동일한 네트워크 범위를 가져야 합니다.

참고: .



3. DHCP 범위 객체를 선택하고 이미지에 표시된 대로 저장을 선택합니다.

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

Primary DNS Server: +

Secondary DNS Server: +

Primary WINS Server: +

Secondary WINS Server: +

DHCP Network Scope: DHCP-SCOPE +

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Save Cancel

2.3단계. 주소 할당 정책 구성

1. **Advanced(고급) > Address Assignment Policy(주소 할당 정책)**로 이동하고 이미지에 표시된 대로 Use DHCP(DHCP 사용) 옵션이 전환되었는지 확인합니다.

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Anyconnect-FTD

Policy Assignments (1)

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies
IPsec
Crypto Maps
IKE Policy
IPsec/IKEv2 Parameters

Address Assignment Policy
Client address assignment criteria for all connection profiles. For incoming VPN client, the following options are tried in order, until an address is found.

IPv4 Policy

- Use authorization server (RADIUS Only)
- Use DHCP ←
- Use internal address pools

Reuse an IP address: minutes until session released. (0 - 480 mins)

IPv6 Policy

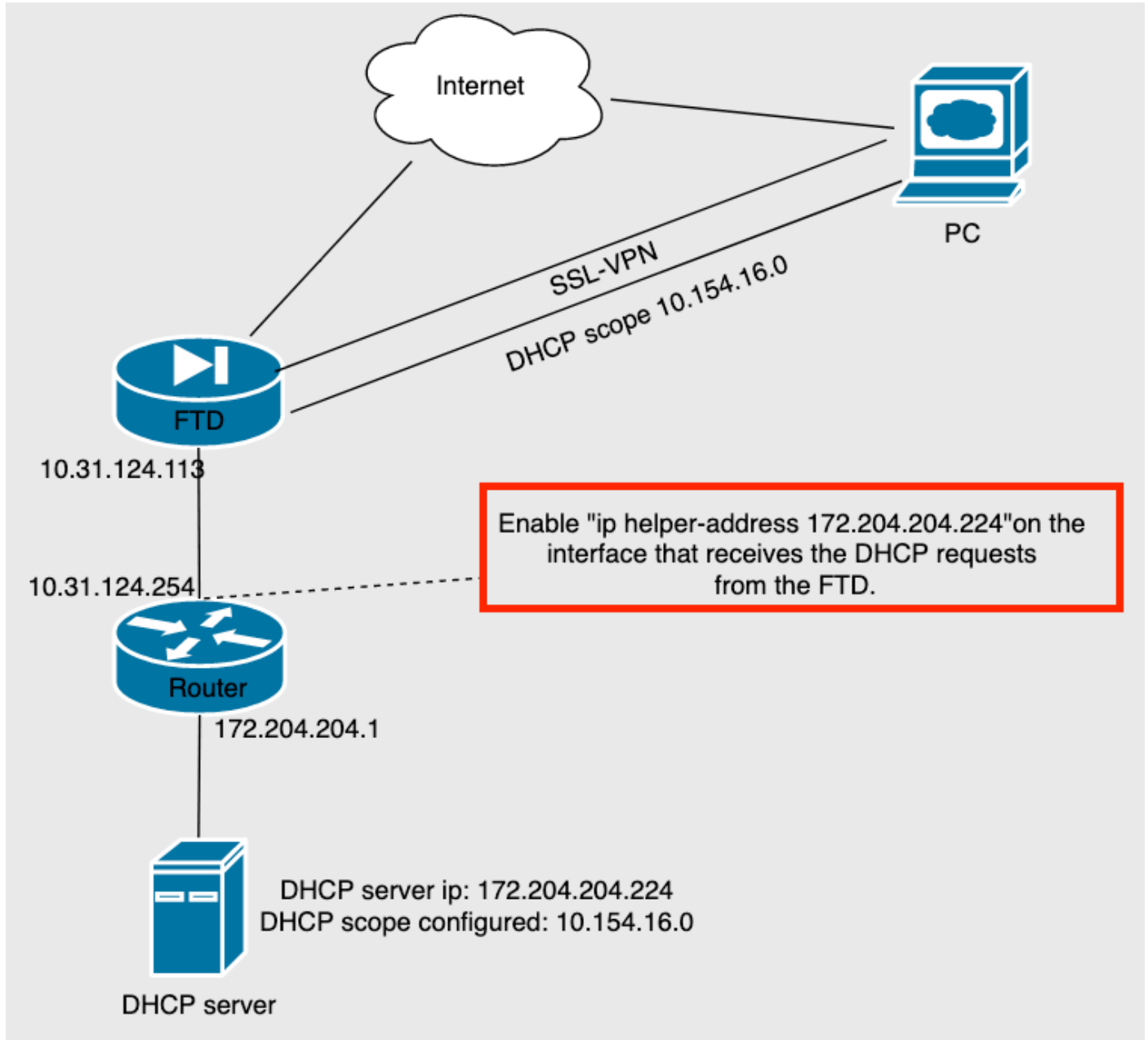
- Use authorization server (RADIUS Only)
- Use internal address pools

2. 변경 사항을 저장하고 구성을 배포합니다.

IP 헬퍼 시나리오

DHCP 서버가 LAN(Local Area Network)의 다른 라우터 뒤에 있는 경우 요청을 DHCP 서버로 전달하려면 "IP 헬퍼"가 필요합니다.

이미지에 표시된 것처럼 토폴로지는 네트워크의 시나리오와 필요한 변경 사항을 보여줍니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

이 섹션에서는 FTD와 DHCP 서버 간에 교환되는 DHCP 패킷에 대해 설명합니다.

- 검색: FTD의 내부 인터페이스에서 DHCP 서버로 전송되는 유니캐스트 패킷입니다. 페이로드에서 릴레이 에이전트 IP 주소는 이미지에 표시된 대로 DHCP 서버의 범위를 지정합니다.

```
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0765c988
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.154.16.0
  Client MAC address: Vmware_96:d1:70 (00:50:56:96:d1:70)
  Client hardware address padding: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

- 제안:이 패킷은 DHCP 서버의 응답이며, FTD에서 DHCP 서버 소스 및 DHCP 범위의 대상과 함께 제공됩니다.
- 요청:FTD의 내부 인터페이스에서 DHCP 서버로 전송되는 유니캐스트 패킷입니다.
- ACK:이 패킷은 DHCP 서버의 응답이며, FTD에서 DHCP 서버 소스 및 DHCP 범위의 대상과 함께 제공됩니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1단계. DHCP 서버에서 wireshark를 다운로드하고 활성화합니다.

2단계. 이미지에 표시된 대로 DHCP를 캡처 필터로 적용합니다.

No.	Time	Source	Destination	Protocol	Length	Info
						Number

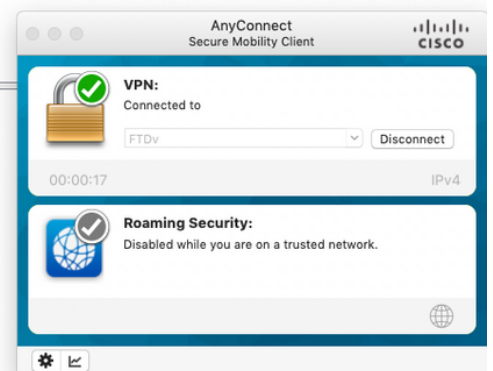


3단계. AnyConnect에 로그인하면 DHCP 협상이 이미지에 표시된 것처럼 표시됩니다.

No.	Time	Source	Destination	Protocol	Length	Info
4125	211.109079	10.31.124.113	172.204.204.224	DHCP	590	DHCP Discover - Transaction ID 0x765c988
4126	211.109321	172.204.204.224	10.154.16.0	DHCP	342	DHCP Offer - Transaction ID 0x765c988
4127	211.111245	10.31.124.113	172.204.204.224	DHCP	590	DHCP Request - Transaction ID 0x765c988
4128	211.111514	172.204.204.224	10.154.16.0	DHCP	342	DHCP ACK - Transaction ID 0x765c988

```
> Frame 4125: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{B27A96D9-4596-4DC3-A4C6-58020274134D}, id 0
> Ethernet II, Src: Cisco_d1:2d:30 (28:6f:7f:d1:2d:30), Dst: Vmware_96:23:b6 (00:50:56:96:23:b6)
> Internet Protocol Version 4, Src: 10.31.124.113, Dst: 172.204.204.224
> User Datagram Protocol, Src Port: 67, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000  00 50 56 96 23 b6 28 6f 7f d1 2d 30 08 00 45 00  .PV.#-(o---0--E
0010  02 40 1f 99 00 00 00 11 18 d7 0a 1f 7c 71 ac cc  @.....|q--
0020  cc e0 00 43 00 43 02 2c cb e4 01 01 06 00 07 65  .C.C.,.....e
0030  c9 88 00 00 00 00 00 00 00 00 00 00 00 00 00  .P.V.-p...
0040  00 00 0a 9a 10 00 00 50 56 96 d1 70 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```



관련 정보

- 이 비디오에서는 원격 액세스 VPN 세션에서 타사 DHCP 서버에서 할당한 IP 주소를 가져올 수 있도록 하는 FTD의 컨피그레이션 예를 제공합니다.
- [기술 지원 및 문서 - Cisco Systems](#)