FMC(Firepower Management Center)를 사용하여 FTD에서 DHCP 서버/릴레이 구성

목차

소개

이 문서에서는 FMC를 통해 FTD(Firepower Threat Defense)에서 수행할 수 있는 DHCP 서버 및 DHCP 릴레이 서비스 컨피그레이션을 설명합니다.

사전 요구 사항

요건

다음 항목에 대해 알고 있는 것이 좋습니다.

- Firepower 기술에 대한 사항
- ASA(Adaptive Security Appliance)에 대한 기본적인 사항
- DHCP 서버/DHCP 릴레이에 대한 사항

사용되는 구성 요소

이 문서의 정보는 아래의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA(5506X/5506H-X/5506W-X, ASA 5508-X, ASA

5516-X)용 ASA Firepower Threat Defense 이미지
- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA(5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)용 ASA Firepower Threat Defense 이미지
- FMC 버전 6.0.1 이상

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.

: FTD FMC . FTD FMC FireSIGHT Management Center .

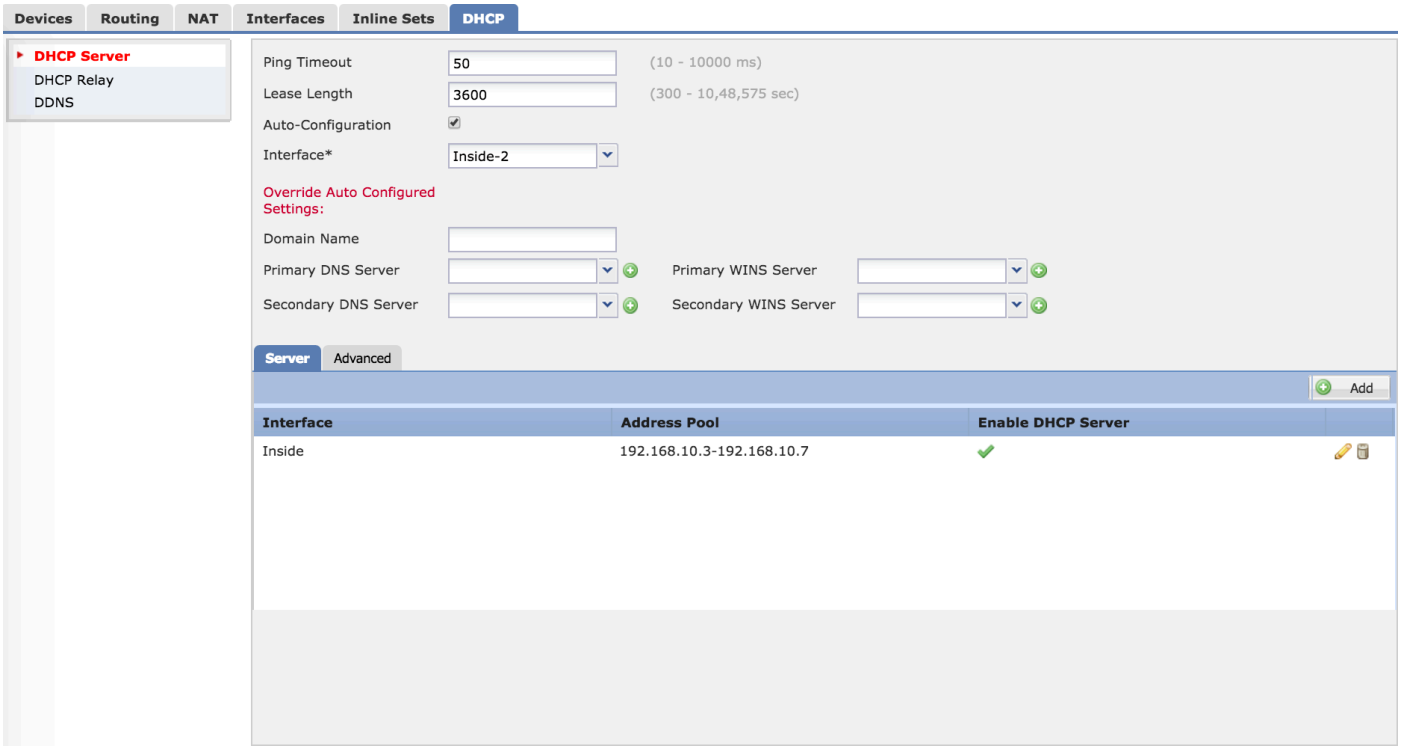
배경 정보

DHCP(Dynamic Host Control Protocol)는 IP 주소, DNS 서버 세부사항 및 기타 파라미터와 같은 네트워크 컨피그레이션 파라미터를 DHCP 클라이언트에 자동으로 제공합니다. FTD 라우팅 인터페이스는 클라이언트에 IP 주소를 제공하기 위한 DHCP 서버 역할을 할 수 있습니다.

FTD는 내부 클라이언트에 DHCP 릴레이 서비스를 제공합니다. 이때 클라이언트는 FTD의 인터페이스 중 하나에 연결되며 외부 DHCP 서버는 다른 인터페이스에 연결됩니다. 릴레이 서비스 작업은 클라이언트에 투명하게 이루어집니다.

DHCP 서버 구성

DHCP 서버를 구성하려면 FMC GUI에 로그인한 다음 **Devices(디바이스) > Device Management(디바이스 관리)**로 이동하여 FTD 어플라이언스의 **edit(수정)** 버튼을 클릭합니다. 그런 다음 **DHCP** 탭으로 이동하여 **DHCP Server(DHCP 서버)** 탭을 클릭합니다.



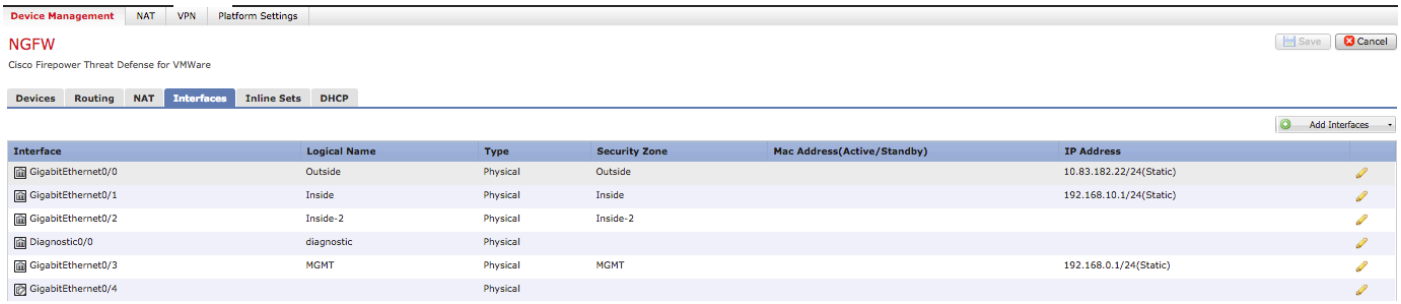
DHCP 서버를 구성하려면 아래의 세 단계를 수행합니다.

1단계. DHCP 서버를 활성화하고 DHCP 풀을 구성합니다.

2단계. 고급 파라미터를 구성합니다.

3단계. DNS/WINS 서버를 구성합니다.

: DHCP IP .



DHCP 서버 활성화/DHCP 풀 구성

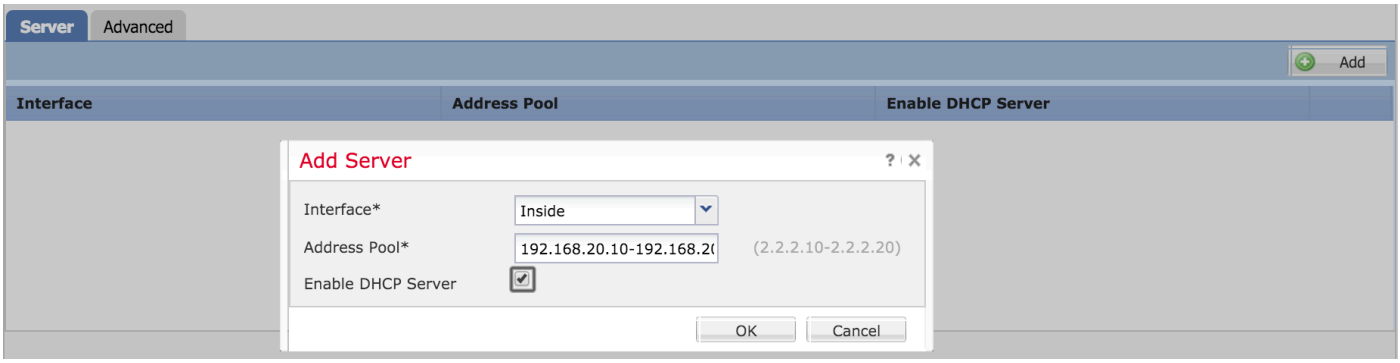
모든 라우팅 인터페이스를 DHCP 서버로 사용할 수 있으며, 이 경우 인터페이스의 IP 주소가 엔드 클라이언트의 게이트웨이로 작동합니다. 따라서 IP 주소 범위만 정의하면 됩니다.

임의의 인터페이스에서 DHCP 서버를 활성화하려면 **Server(서버)** 탭에서 **Add(추가)** 버튼을 클릭합니다.

Interface(인터페이스): DHCP 서버를 활성화할 인터페이스를 드롭다운 목록에서 지정합니다.

Address Pool(주소 풀): IP 주소 범위를 지정합니다.

Enable DHCP Server(DHCP 서버 활성화): 이 인터페이스에서 DHCP 서버를 활성화하려면 체크 박스를 활성화합니다.



OK(확인)를 클릭하여 DHCP 컨피그레이션을 저장합니다.

DNS/WINS 서버 구성

DHCP 서버는 IP 주소 세부사항과 함께 DNS/WINS/도메인 이름 파라미터를 엔드 클라이언트에게 제공합니다. 이러한 파라미터를 통해 이름을 확인할 수 있습니다. 그러므로 이러한 파라미터를 올바르게 구성해야 합니다.

이 파라미터는 두 가지 옵션을 통해 구성할 수 있습니다.

첫째로, FTD의 인터페이스가 DHCP 클라이언트로 구성되어 있으면 **Auto-Configuration(자동 컨피그레이션)** 옵션을 선택할 수 있습니다. 이 방법을 사용하는 경우 DHCP 서버에서 DNS/WINS/도메

인 이름 정보 컨피그레이션을 가져오고 DHCP 클라이언트에 동일한 정보를 제공합니다.

둘째로, 고유한 DNS/WINS/도메인 이름 파라미터를 설정할 수 있습니다. 그러면 해당 파라미터가 엔드 클라이언트에 제공됩니다.

이 파라미터를 구성하려면 **DHCP** 탭으로 이동합니다.

- **Ping Timeout(Ping 시간 초과):** FTD는 주소 충돌을 방지하기 위해 DHCP 클라이언트에 주소를 할당하기 전에 ICMP ping 패킷 2개를 해당 주소로 전송합니다. 이 명령은 해당 패킷의 시간 초과 값을 지정합니다.

- **Lease Length(리스 기간):** 이 리스는 클라이언트가 할당받은 IP 주소를 리스 만료 전까지 사용할 수 있는 시간(초)과 같습니다.
- **Auto Configuration(자동 컨피그레이션):** DNS/WINS/도메인 이름에 대해 자동 컨피그레이션을 구성하려면 이 체크 박스를 활성화합니다
- **Interface(인터페이스):** DHCP 클라이언트 역할을 하는 인터페이스를 지정합니다

Override Auto Configured Setting(자동 구성된 설정 재정의): 고유한 DNS/WINS/도메인 이름을 엔드 클라이언트에 할당하려면 이 옵션을 구성합니다.

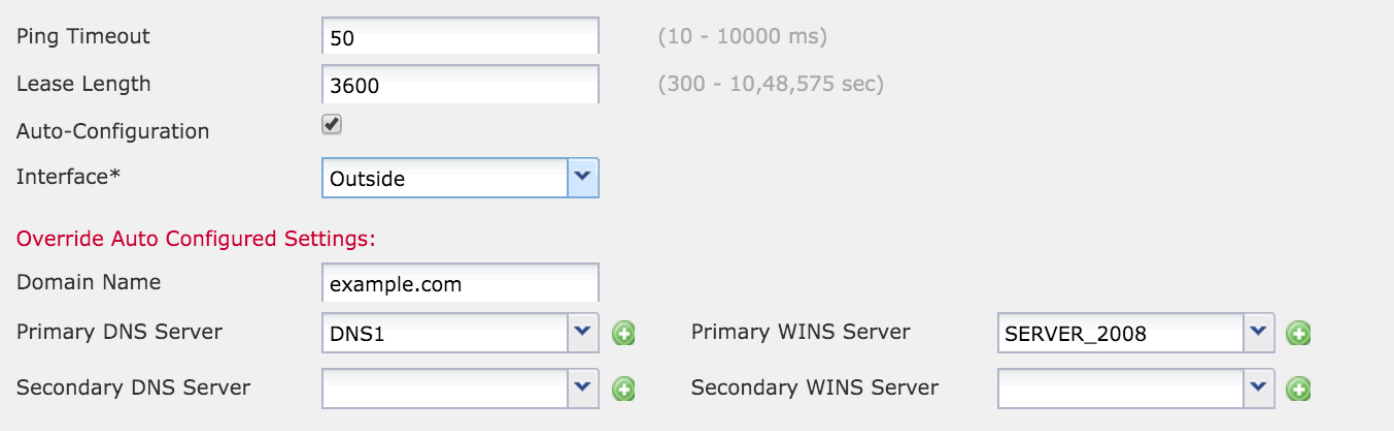
Domain Name(도메인 이름): 도메인 이름을 지정합니다.

Primary DNS Server(기본 DNS 서버): 기본 DNS 서버를 지정합니다. 드롭다운 목록에서 네트워크 개체를 선택할 수도 있고, **더하기(+)** 아이콘을 클릭하여 기본 DNS 서버용 네트워크 개체를 생성할 수도 있습니다.

Secondary DNS Server(보조 DNS 서버): 보조 DNS 서버를 지정합니다. 드롭다운 목록에서 네트워크 개체를 선택할 수도 있고, **더하기(+)** 아이콘을 클릭하여 보조 DNS 서버용 네트워크 개체를 생성할 수도 있습니다.

Primary WINS Server(기본 WINS 서버): 보조 DNS 서버를 지정합니다. 드롭다운 목록에서 네트워크 개체를 선택할 수도 있고, **더하기(+)** 아이콘을 클릭하여 보조 DNS 서버용 네트워크 개체를 생성할 수도 있습니다.

Secondary WINS Server(보조 WINS 서버): 보조 DNS 서버를 지정합니다. 드롭다운 목록에서 네트워크 개체를 선택할 수도 있고, **더하기(+)** 아이콘을 클릭하여 보조 DNS 서버용 네트워크 개체를 생성할 수도 있습니다.

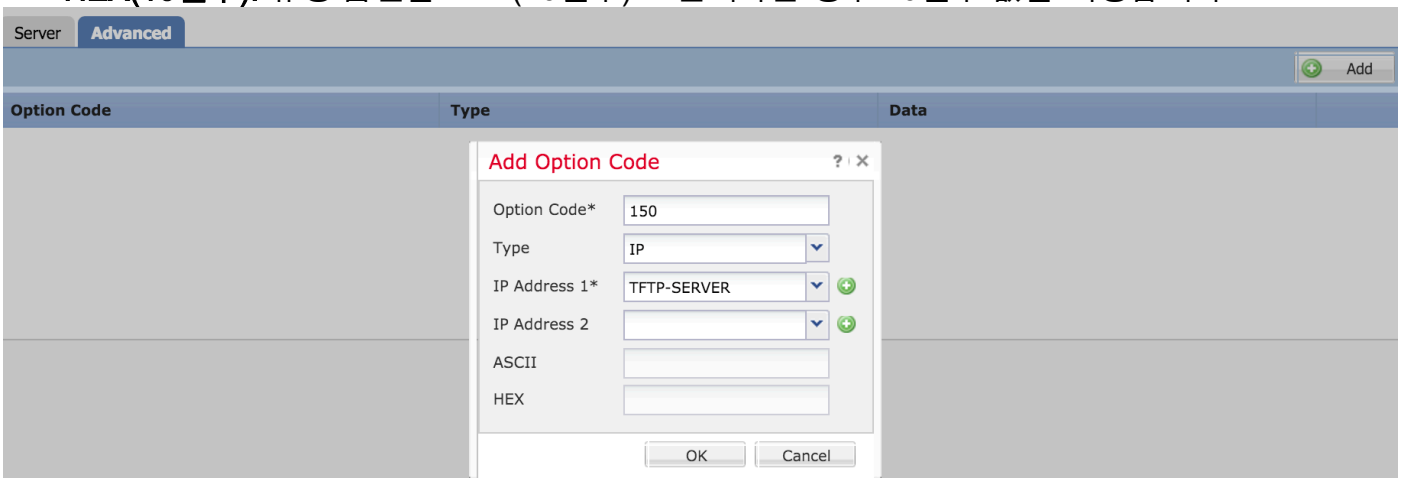


고급 파라미터 구성

FTD 인터페이스의 DHCP에는 DHCP 코드 및 옵션을 포함하는 기능이 있습니다. 예를 들어 Cisco IP Phone은 TFTP 서버에서 펌웨어를 다운로드할 수 있도록 옵션(150/66)이 포함된 요청을 DHTP 서버에 보내 TFTP 서버의 IP 주소를 가져올 수 있습니다.

이 파라미터를 구성하려면 **DHCP > Advanced(고급)** 옵션으로 이동하여 **Add(추가)**를 클릭합니다.

- **Option Code(옵션 코드):** RFC 2132, RFC 2562, RFC 5510에 나와 있는 대로 옵션 코드를 지정합니다.
- **Type(유형):** 드롭다운에서 유형을 지정합니다.
- **IP Address 1(IP 주소 1):** 유형 옵션을 IP로 선택하는 경우 첫 번째 TFTP 서버의 IP 주소를 지정합니다.
- **IP Address 2(IP 주소 2):** 유형 옵션을 IP로 선택하는 경우 첫 번째 TFTP 서버의 IP 주소를 지정합니다.
- **ASCII:** 유형 옵션을 ASCII로 선택하는 경우 ASCII 값을 지정합니다.
- **HEX(16진수):** 유형 옵션을 HEX(16진수)로 선택하는 경우 16진수 값을 지정합니다.



OK(확인)를 클릭하여 컨피그레이션을 저장합니다.

Save(저장) 버튼을 클릭하여 플랫폼 설정을 저장합니다. 그런 다음 **Deploy(구축)** 옵션으로 이동하여 변경 사항을 적용할 FTD 어플라이언스를 선택하고 **Deploy(구축)** 버튼을 클릭하여 플랫폼 설정 구축을 시작합니다.

Save(저장) 버튼을 클릭하여 플랫폼 설정을 저장합니다. 그런 다음 **Deploy(구축)** 옵션으로 이동하여 변경 사항을 적용할 FTD 어플라이언스를 선택하고 **Deploy(구축)** 버튼을 클릭하여 플랫폼 설정 구축을 시작합니다.

DHCP 릴레이 구성

FTD 인터페이스는 클라이언트와 외부 DHCP 서버 간의 DHCP 릴레이 에이전트로 작동합니다. 인터페이스는 클라이언트 요청을 수신 대기하며 DHCP 서버가 클라이언트에 대해 주소를 할당하는 데 필요한 클라이언트의 링크 정보와 같은 중요 컨피그레이션 데이터를 추가합니다. DHCP 서버가 응답하면 인터페이스는 회신 패킷을 DHCP 클라이언트에 다시 전달합니다.

DHCP 릴레이 컨피그레이션에서는 기본적으로 아래의 두 컨피그레이션 단계를 수행합니다.

1단계. DHCP 릴레이 에이전트를 구성합니다.

2단계. 외부 DHCP 서버를 구성합니다.

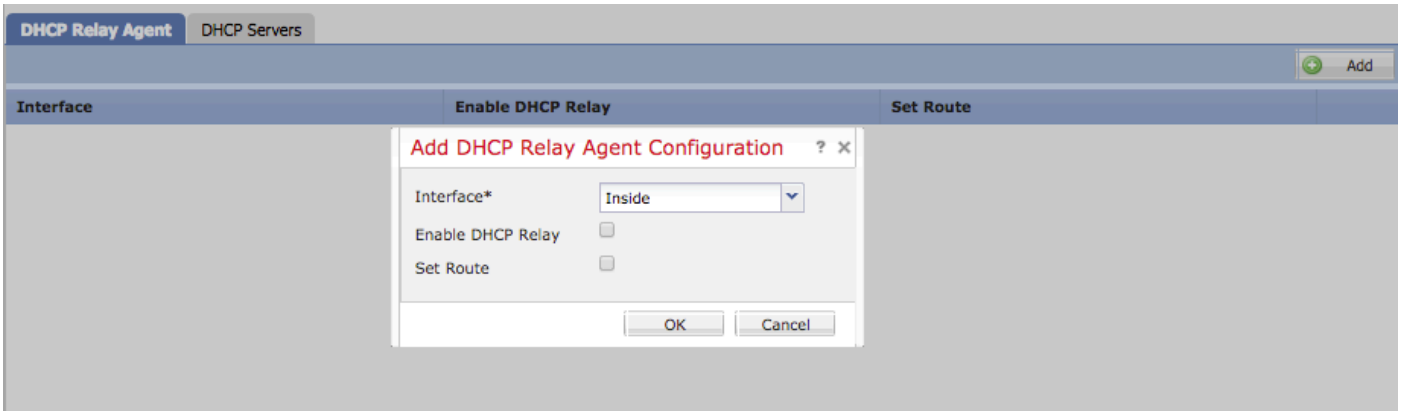
DHCP 릴레이 에이전트 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 FTD 어플라이언스의 **edit(수정)** 버튼을 클릭합니다. **DHCP > DHCP Relay(DHCP 릴레이)** 옵션으로 이동합니다. **Add(추가)** 버튼을 클릭합니다.

Interface(인터페이스): 인터페이스가 클라이언트 요청을 수신 대기하는 인터페이스를 드롭다운 목록에서 지정합니다. DHCP 클라이언트는 IP 주소 요청 시 이 인터페이스에 직접 연결해야 합니다.

Enable DHCP Relay(DHCP 릴레이 활성화): DHCP 릴레이 서비스를 활성화하려면 체크 박스를 활성화합니다.

Set Route(경로 설정): 인터페이스 IP 주소를 기본 게이트웨이로 설정하려면 체크 박스를 활성화합니다.



OK(확인) 버튼을 클릭하여 DHCP 릴레이 에이전트 컨피그레이션을 저장합니다.

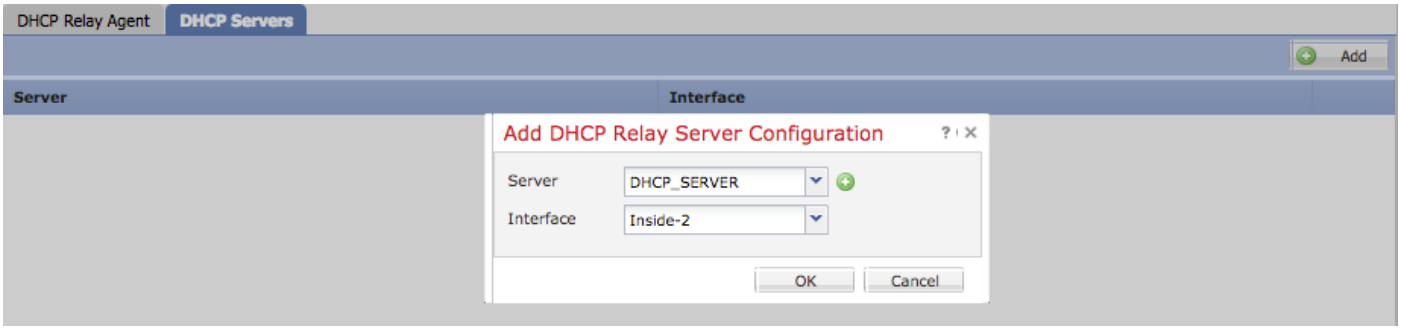
외부 DHCP 서버 구성

클라이언트 요청이 전달되는 외부 DHCP 서버의 IP 주소를 지정해야 합니다.

DHCP 서버를 지정하려면 **DHCP Server(DHCP 서버)**로 이동하여 **Add(추가)**를 클릭합니다.

Server(서버): DHCP 서버의 IP 주소를 지정합니다. 드롭다운 목록에서 네트워크 개체를 선택할 수도 있고, **더하기(+)** 아이콘을 클릭하여 DHCP 서버용 네트워크 개체를 생성할 수도 있습니다.

Interface(인터페이스): DHCP 서버가 연결되는 인터페이스를 지정합니다



OK(확인)를 클릭하여 컨피그레이션을 저장합니다.

Save(저장) 버튼을 클릭하여 플랫폼 설정을 저장합니다. 그런 다음 **Deploy(구축)** 옵션으로 이동하여 변경 사항을 적용할 FTD 어플라이언스를 선택하고 **Deploy(구축)** 버튼을 클릭하여 플랫폼 설정 구축을 시작합니다.

모니터링 및 트러블슈팅

- DHCP 서버/릴레이를 구성하기 전에 FTD가 FMC에 등록되어 있는지 확인합니다
- DHCP 릴레이 컨피그레이션에서 DHCP 서버에 대한 연결을 확인합니다.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# ping <DHCP_SERVER_IP>
```

- FTD CLI에서 DHCP 관련 컨피그레이션을 확인합니다. FTP CLI에 로그인하여 관리 인터페이스에 액세스한 다음 명령을 실행할 수 있습니다.

```
firepower# show running-config dhcpd
dhcpd auto_config Inside-2
!
dhcpd address 192.168.10.3-192.168.10.7 Inside
!
```

- 정책 구축이 정상적으로 적용되었는지 확인합니다.
- 자동 컨피그레이션 또는 수동 컨피그레이션을 통해 올바른 DNS/WINS 서버 항목을 구성했는지 확인합니다.
- IP 주소 풀은 인터페이스 IP 주소와 동일한 서브넷에 있어야 합니다.
- 인터페이스에서 IP 주소 및 논리적 이름이 구성되어 있는지 확인합니다.
- 클라이언트가 IP 주소를 가져오지 않는 문제를 트러블슈팅하기 위해 FTP 라우팅 인터페이스에서 패킷 캡처를 가져올 수 있습니다. 패킷 캡처에서 DHCP 서버의 DORA 프로세스를 확인할 수 있습니다. CLI 및 ASDM을 사용한 ASA 패킷 캡처 컨피그레이션 예의 설명에 따라 패킷 캡처를 가져올 수 있습니다.
- 커맨드 라인에서 DHCP 통계를 확인합니다.

```
firepower# show dhcpd statistics
```

- CLI에서 DHCP 바인딩 정보를 확인합니다.

```
firepower# show dhcpd binding
```

- **Device(디바이스) > Platform Setting(플랫폼 설정) > FTD Policy(FTD 정책) > System logging(시스템 로깅)**에서 적절한 로깅을 활성화하고 FTD에 플랫폼 설정을 구축합니다. FTD CLI에 로그인한 다음 아래 명령을 실행하여 Syslog 메시지를 확인합니다.

```
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower# show logging
```