FMC를 통한 FTD 관리 액세스(HTTPS 및 SSH) 컨피그레이션

목차

소개

이 문서에서는 FMC(Firepower Management Center)를 통해 수행할 수 있는 FTD(Firepower Threat Defense)에 대한 관리 액세스(HTTPS 및 SSH) 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
- HTTPS 및 SSH(Secure Shell)를 통한 ASA의 관리 액세스에 대한 사항

사용되는 구성 요소

이 문서의 정보는 아래의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.1 이상에서 실행되는 ASA(Adaptive Security Appliance)(5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)용 ASA Firepower Threat Defense 이미지
- 소프트웨어 버전 6.0.1 이상에서 실행되는 ASA(5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)용 ASA Firepower Threat Defense 이미지
- FMC(Firepower Management Center) 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.

배경 정보

FTD(Firepower Threat Defense)에서는 모든 ASA 관련 컨피그레이션을 GUI에서 수행합니다.

소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서는 **system support diagnostic-cli**를 입력하여 ASA 진단 CLI에 액세스합니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 CLI가 통합되어 있으므로 CLISH에서 전체 ASA 명령을 구성합니다.

```
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

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

firepower> en
Password:
firepower#                                           DIAGNOSTIC CLI
```

외부 네트워크에서 직접 관리 액세스 권한을 얻으려면 HTTPS 또는 SSH를 통한 관리 액세스를 구성해야 합니다. 이 문서에서는 외부에서 SSH 또는 HTTPS를 통해 관리 액세스 권한을 얻는 데 필요한 컨피그레이션에 대해 설명합니다.

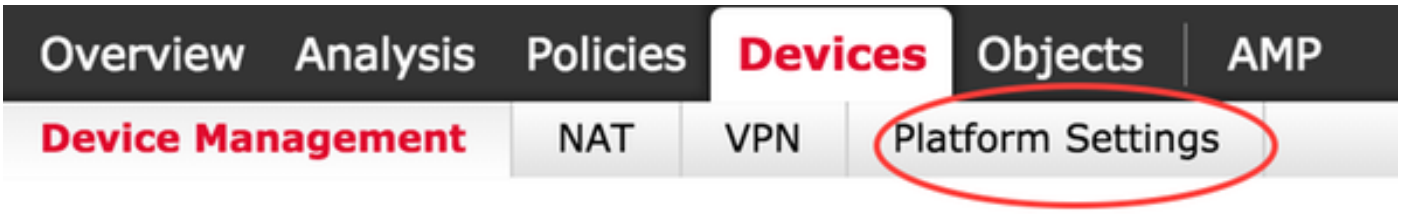
> **참고**: 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서는 로컬 사용자가 CLI에 액세스할 수 없으며 사용자를 인증하기 위한 외부 인증을 구성해야 합니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 로컬 **관리** 사용자가 CLI에 액세스하며, 기타 모든 사용자의 경우에는 외부 인증이 필요합니다.

> **참고**: 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서는 FTD의 **br1**용으로 구성된 IP를 통해 진단 CLI에 직접 액세스할 수 없습니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 관리 액세스용으로 구성된 모든 인터페이스를 통해 통합 CLI에 액세스할 수 있습니다. 단, 해당 인터페이스가 IP 주소를 사용하여 구성되어 있어야 합니다.

구성

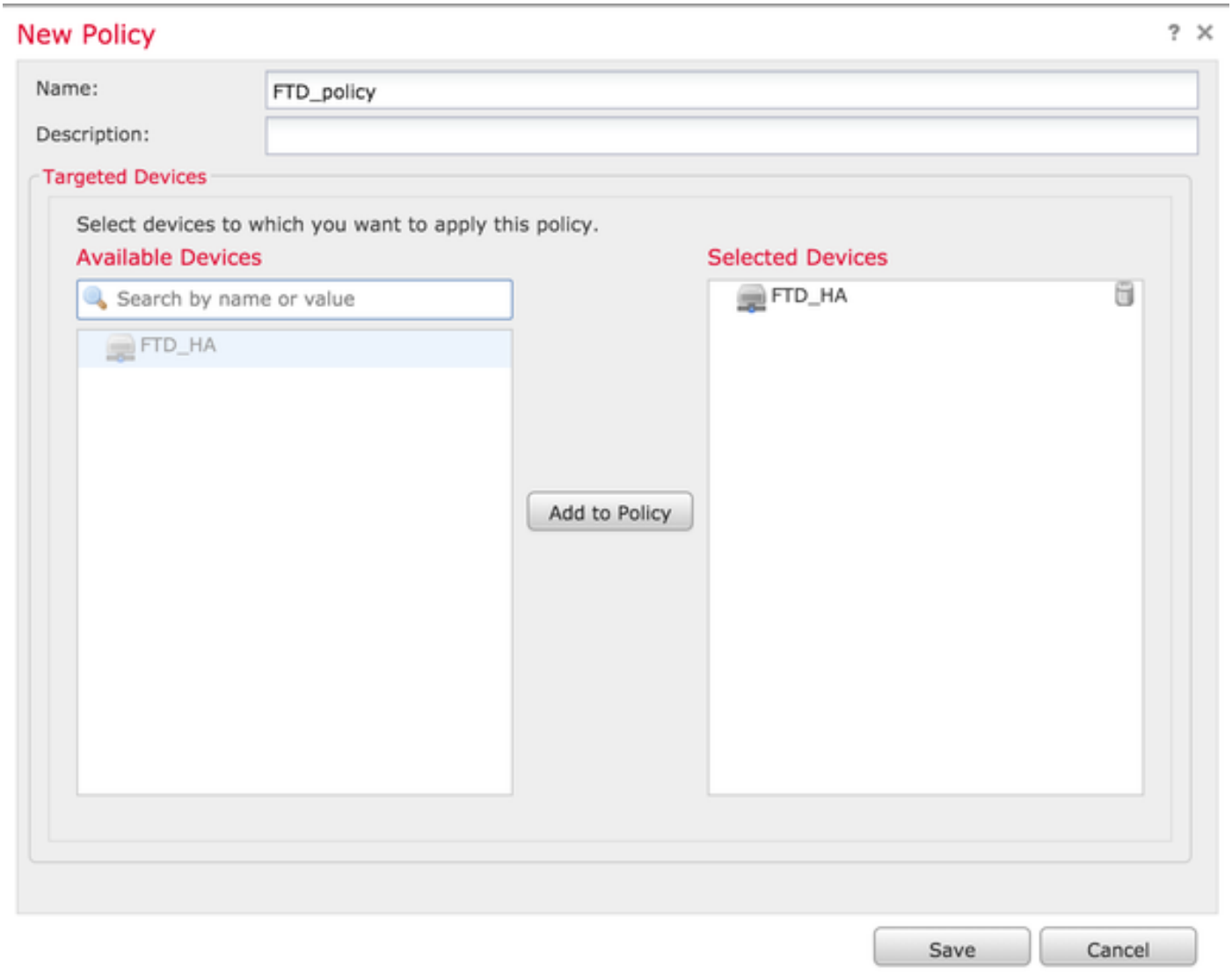
아래 그림에 나와 있는 것처럼 모든 관리 액세스 관련 컨피그레이션을 구성하려면 **Devices(디바이**

스)의 **Platform Settings(플랫폼 설정)** 탭으로 이동합니다.



연필 아이콘을 클릭하여 기존 정책을 수정하거나, 아래 그림에 나와 있는 것처럼 **New Policy(새 정책)** 버튼을 클릭하고 유형으로 **Threat Defense Settings(Threat Defense 설정)**를 선택하여 새 FTD 정책을 생성합니다.

이 정책을 적용할 FTD 어플라이언스를 선택하고 아래 그림에 나와 있는 것처럼 **Save(저장)**를 클릭합니다.



관리 액세스 구성

관리 액세스를 구성하기 위해 수행해야 하는 네 가지 주요 단계는 다음과 같습니다.

1단계. FMC GUI를 통해 FTD 인터페이스에서 IP 구성

FTD가 SSH 또는 HTTPS를 통해 액세스할 수 있는 인터페이스에서 IP를 구성합니다. FTD의 **Interfaces(인터페이스)** 탭으로 이동하여 기존 인터페이스를 수정합니다.

> **참고**: 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서 FTD의 기본 관리 인터페이스는 diagnostic0/0 인터페이스입니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 진단 인터페이스를 제외한 모든 인터페이스가 관리 액세스를 지원합니다.

아래의 여섯 단계를 통해 진단 인터페이스를 구성합니다.

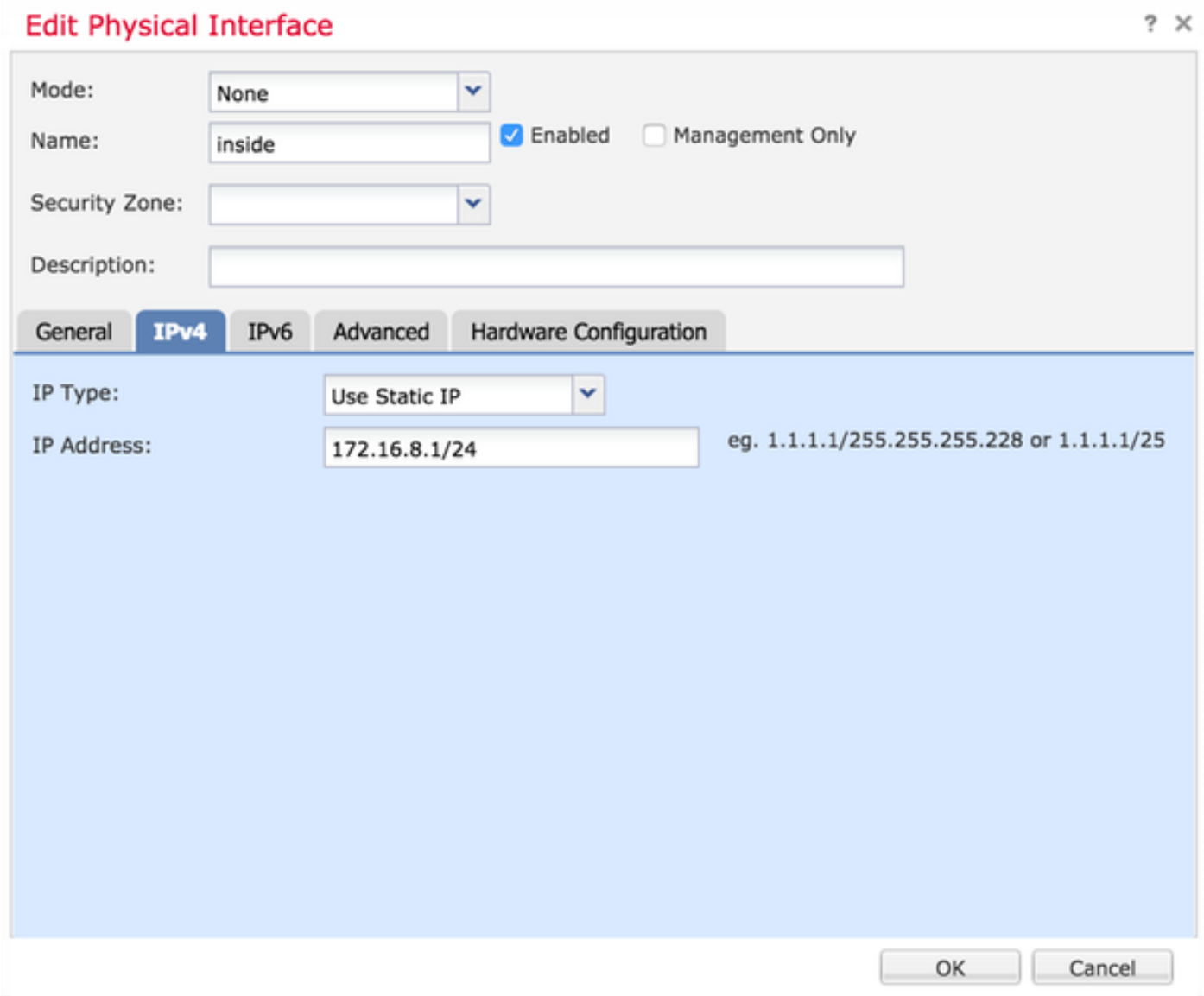
1단계. **Devices(디바이스) > Device Management(디바이스 관리)**로 이동합니다.

2단계. 디바이스 또는 FTD HA 클러스터를 선택합니다.

3단계. **인터페이스** 탭으로 이동합니다.

4단계. 아래 그림에 나와 있는 것처럼 **연필 아이콘**을 클릭하여 인터페이스를 구성/수정해 관리 액세스 권한을 얻습니다.

5단계. **enable(활성화)** 체크 박스를 선택하여 인터페이스를 활성화합니다. **Ipv4** 탭으로 이동하여 IP Type(IP 유형)을 **static or DHCP(고정 또는 DHCP)**로 선택합니다. 그런 후에 인터페이스의 IP 주소를 입력하고 아래 그림에 나와 있는 것처럼 **OK(확인)**를 클릭합니다.



6단계. **Save(저장)**를 클릭한 다음 FTD에 정책을 구축합니다.

> **참고**: 진단 인터페이스를 사용하여 소프트웨어 버전 6.1.0이 설치된 디바이스에서 SSH를 통해 통합 CLI에 액세스할 수는 없습니다.

2단계. 외부 인증 구성

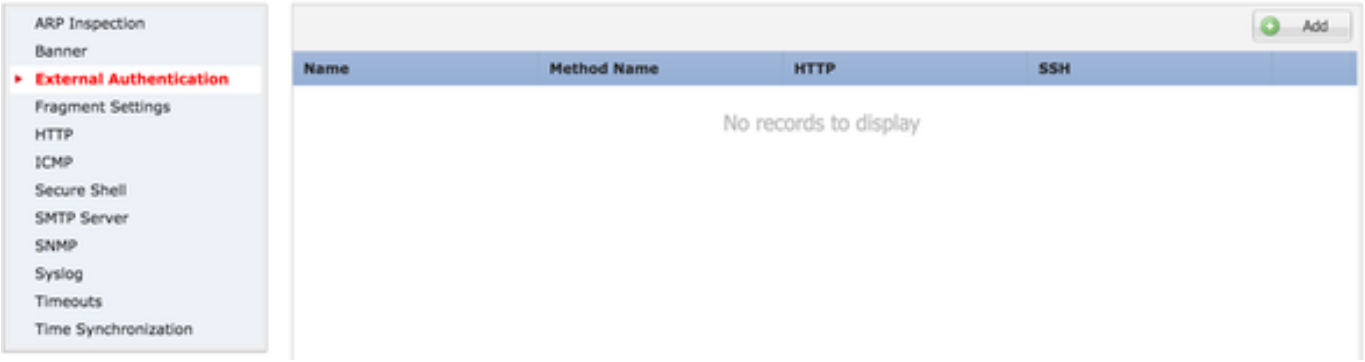
외부 인증을 사용하면 사용자 인증용 Active Directory 또는 RADIUS 서버에 FTD를 쉽게 통합할 수 있습니다. 로컬로 구성된 사용자는 진단 CLI에 직접 액세스할 수 없으므로 이 단계를 수행해야 합니다. LDAP(Lightweight Directory Access Protocol) 또는 RADIUS를 통해 인증된 사용자만 CLI 및 GUI에 액세스할 수 있습니다.

아래의 여섯 단계를 통해 외부 인증을 구성합니다.

1단계. **Devices(디바이스) > Platform Settings(플랫폼 설정)**로 이동합니다.

2단계. 연필 아이콘을 클릭하여 기존 정책을 수정하거나, **New Policy(새 정책)** 버튼을 클릭하고 유형으로 **Threat Defense Settings(Threat Defense 설정)**를 선택하여 새 FTD 정책을 생성합니다.

3단계. 그림에 나와 있는 것처럼 **External Authentication(외부 인증)** 탭으로 이동합니다.



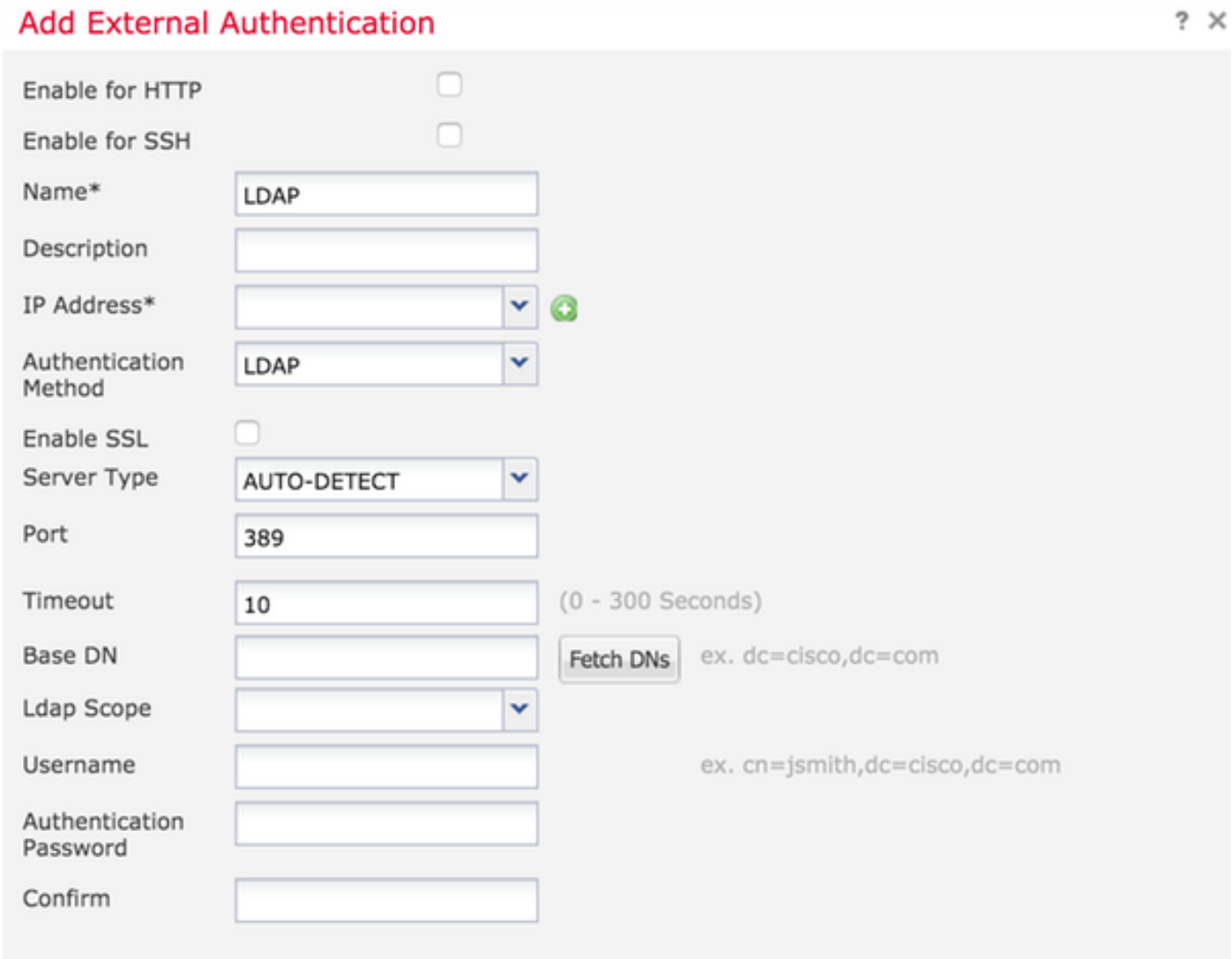
4단계. **Add(추가)**를 클릭하면 그림에 나와 있는 것처럼 대화 상자가 나타납니다.

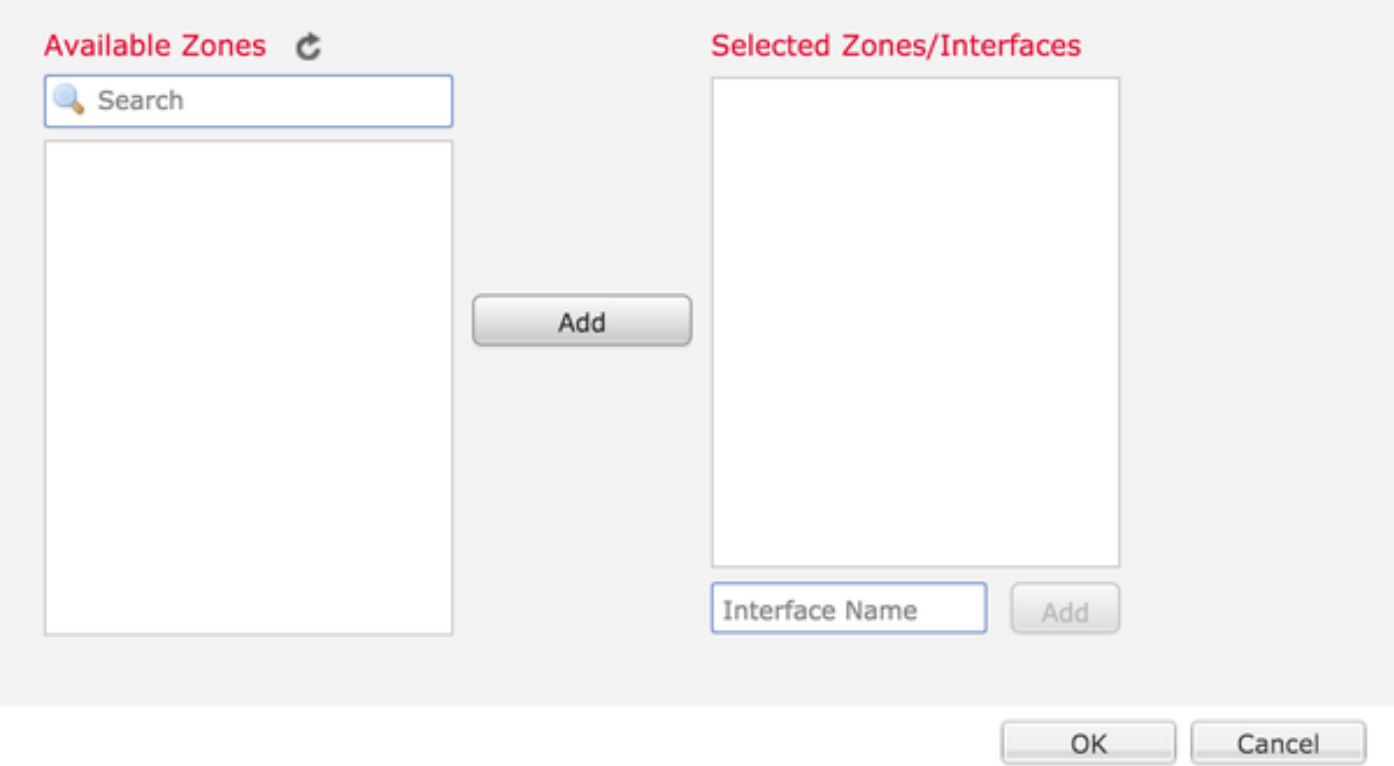
- **Enable for HTTP(HTTP용으로 활성화)** - HTTPS를 통해 FTD 액세스 권한을 제공하려면 이 옵션을 활성화합니다.
- **Enable for SSH(SSH용으로 활성화)** - SSH를 통해 FTD 액세스 권한을 제공하려면 이 옵션을 활성화합니다.
- **Name(이름)** - LDAP 연결의 이름을 입력합니다.
- **Description(설명)** - 외부 인증 개체에 대한 설명(선택 사항)을 입력합니다.
- **IP address(IP 주소)** - 외부 인증 서버의 IP가 저장되는 네트워크 개체를 입력합니다. 네트워크 개체가 구성되어 있지 않으면 **(+)** 아이콘을 클릭하여 새 개체를 생성합니다.
- **Authentication Method(인증 방법)** - 인증용으로 RADIUS 또는 LDAP 프로토콜을 선택합니다.
- **Enable SSL(SSL 활성화)** - 인증 트래픽을 암호화하려면 이 옵션을 활성화합니다.
- **Server Type(서버 유형)** - 서버 유형을 선택합니다. 알려진 서버 유형으로는 MS Active Directory, Sun, OpenLDAP, Novell 등이 있습니다. 이 옵션은 기본적으로 서버 유형을 자동 감지하도록 설정됩니다.
- **Port(포트)** - 인증이 수행되는 포트를 입력합니다.
- **Timeout(시간 초과)** - 인증 요청의 시간 초과 값을 입력합니다.
- **Base DN(기본 DN)** - 사용자가 있어야 하는 범위를 제공하는 기본 DN을 입력합니다.
- **LDAP Scope(LDAP 범위)** - 확인할 LDAP 범위를 선택합니다. 같은 레벨 내를 확인하거나 하위 트리 내를 확인하도록 범위를 지정할 수 있습니다.
- **Username(사용자 이름)** - LDAP 디렉터리에 바인딩할 사용자 이름을 입력합니다.

- **Authentication password(인증 비밀번호)** - 이 사용자의 비밀번호를 입력합니다.
- **Confirm(확인)** - 비밀번호를 다시 입력합니다.
- **Available Interfaces(사용 가능한 인터페이스)** - FTD에서 사용 가능한 인터페이스 목록이 표시됩니다.
- **Selected zones and interfaces(선택한 영역 및 인터페이스)** - 여기에는 인증 서버에 액세스하는 데 사용되는 인터페이스의 목록이 표시됩니다.

RADIUS 인증의 경우에는 서버 유형 기본 DN 또는 LDAP 범위가 없습니다. 포트는 RADIUS 포트 1645입니다.

Secret(비밀) - RADIUS용 비밀 키를 입력합니다.





5단계. 컨피그레이션을 완료한 후 **OK(확인)**를 클릭합니다.

6단계. 정책을 저장하고 Firepower Threat Defense 디바이스에 구축합니다.

> **참고**: 외부 인증을 사용하여 소프트웨어 버전 6.1.0이 설치된 디바이스에서 SSH를 통해 통합 CLI에 액세스할 수는 없습니다.

3단계. SSH 액세스 구성

SSH를 사용하면 통합 CLI에 직접 액세스할 수 있습니다. CLI에 직접 액세스하여 디버그 명령을 실행하려면 이 옵션을 사용합니다. 이 섹션에서는 FTD CLI에 액세스하기 위해 SSH를 구성하는 방법을 설명합니다.

> **참고**: 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서는 Platform Settings(플랫폼 설정)의 SSH 컨피그레이션을 통해 CLISH가 아닌 진단 CLI에 직접 액세스할 수 있습니다. CLISH에 액세스하려면 **br1**에 구성된 IP 주소에 연결해야 합니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 모든 인터페이스에서 SSH를 통해 액세스하는 경우 통합 CLI로 이동하게 됩니다.

아래의 여섯 단계를 통해 ASA에서 SSH를 구성합니다.

6.0.1 디바이스의 경우에만:

소프트웨어 버전이 6.0.1 이상, 6.1.0 미만인 FTD 디바이스에서는 아래 단계를 수행합니다. 6.1.0 디바이스에서는 이러한 파라미터가 OS에서 상속됩니다.

1단계. **Devices(디바이스) > Platform Settings(플랫폼 설정)**로 이동합니다.

2단계. 연필 아이콘을 클릭하여 기존 정책을 수정하거나, **New Policy(새 정책)** 버튼을 클릭하고 유형으로 **Threat Defense Settings(Threat Defense 설정)**를 선택하여 새 Firepower Threat Defense 정책을 생성합니다.

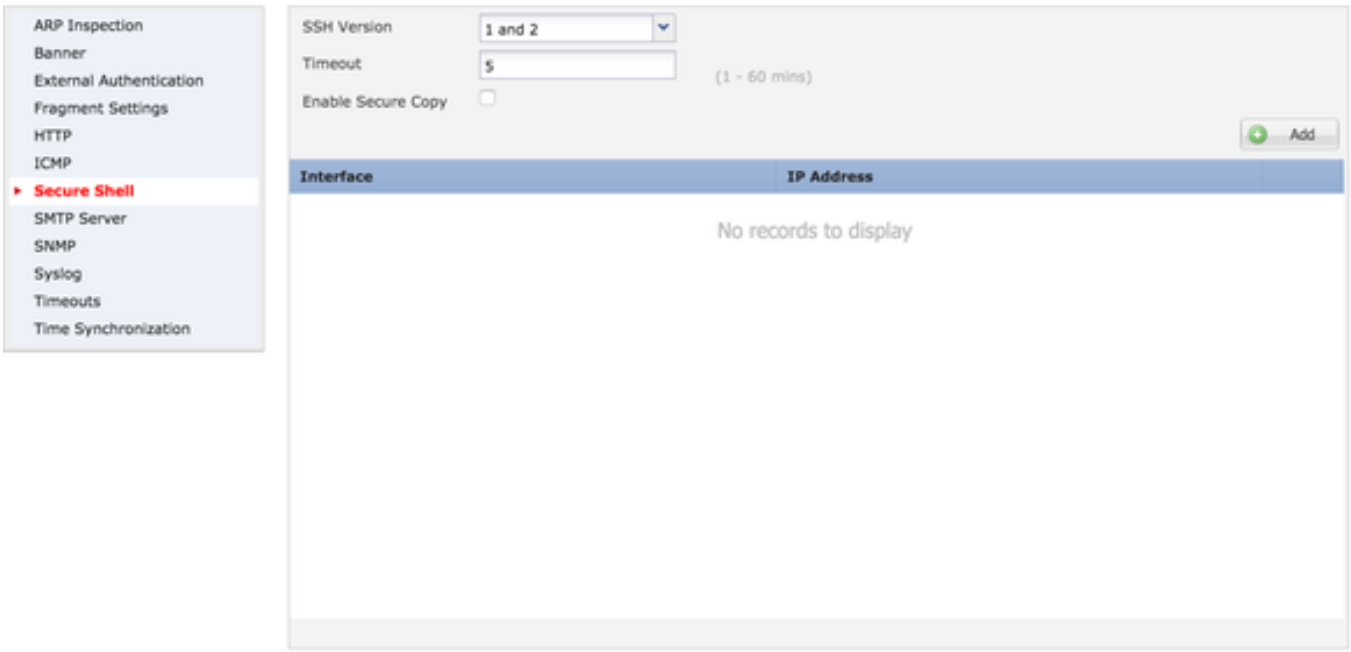
3단계. **Secure Shell** 섹션으로 이동합니다. 그림에 나와 있는 것과 같은 페이지가 표시됩니다.

SSH version(SSH 버전): ASA에서 활성화할 SSH 버전을 선택합니다. 다음과 같은 세 가지 옵션이 있습니다.

- **1:** SSH 버전 1만 활성화합니다.
- **2:** SSH 버전 2만 활성화합니다.
- **1 and 2(1 및 2):** SSH 버전 1과 2를 모두 활성화합니다.

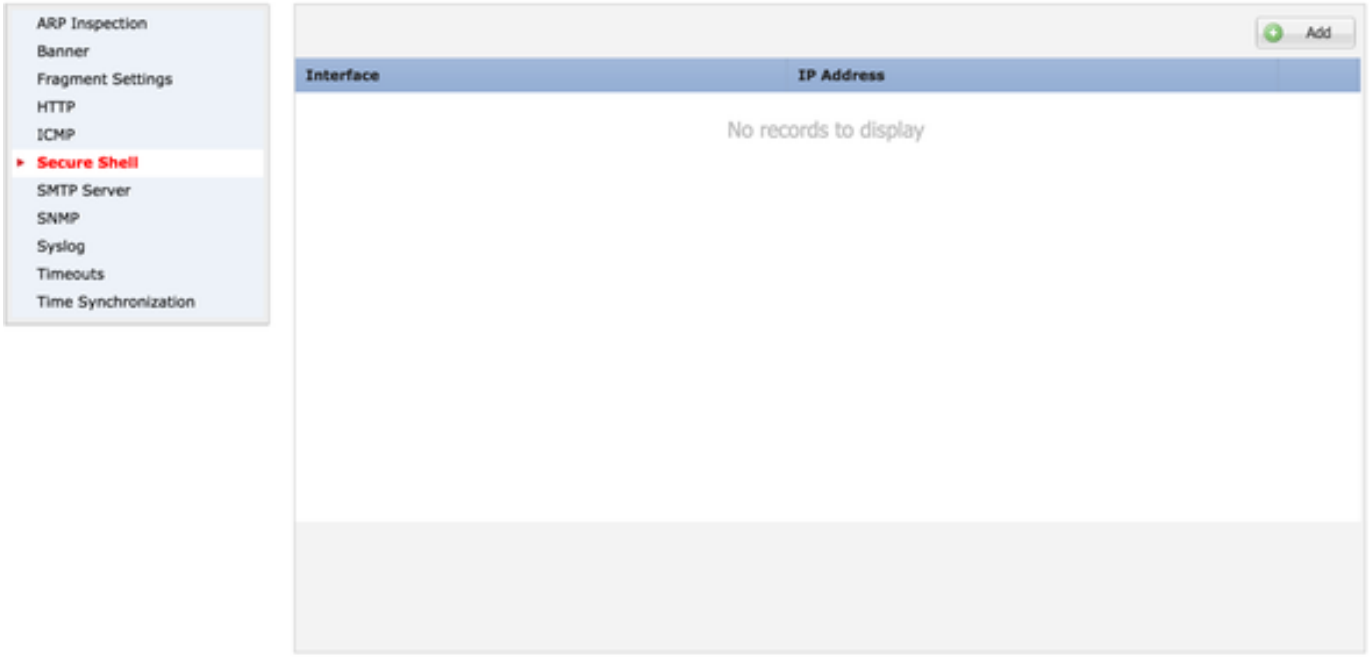
Timeout(시간 초과): 원하는 SSH 시간 초과를 분 단위로 입력합니다.

Enable Secure Copy(Secure Copy 활성화) - 디바이스가 SCP(Secure Copy) 연결을 허용하고 SCP 서버로 작동하도록 구성하려면 이 옵션을 활성화합니다.



6.0.1 및 6.1.0 디바이스의 경우:

아래의 단계는 SSH를 통한 관리 액세스를 특정 인터페이스와 특정 IP 주소로 제한하도록 구성되어 있습니다.

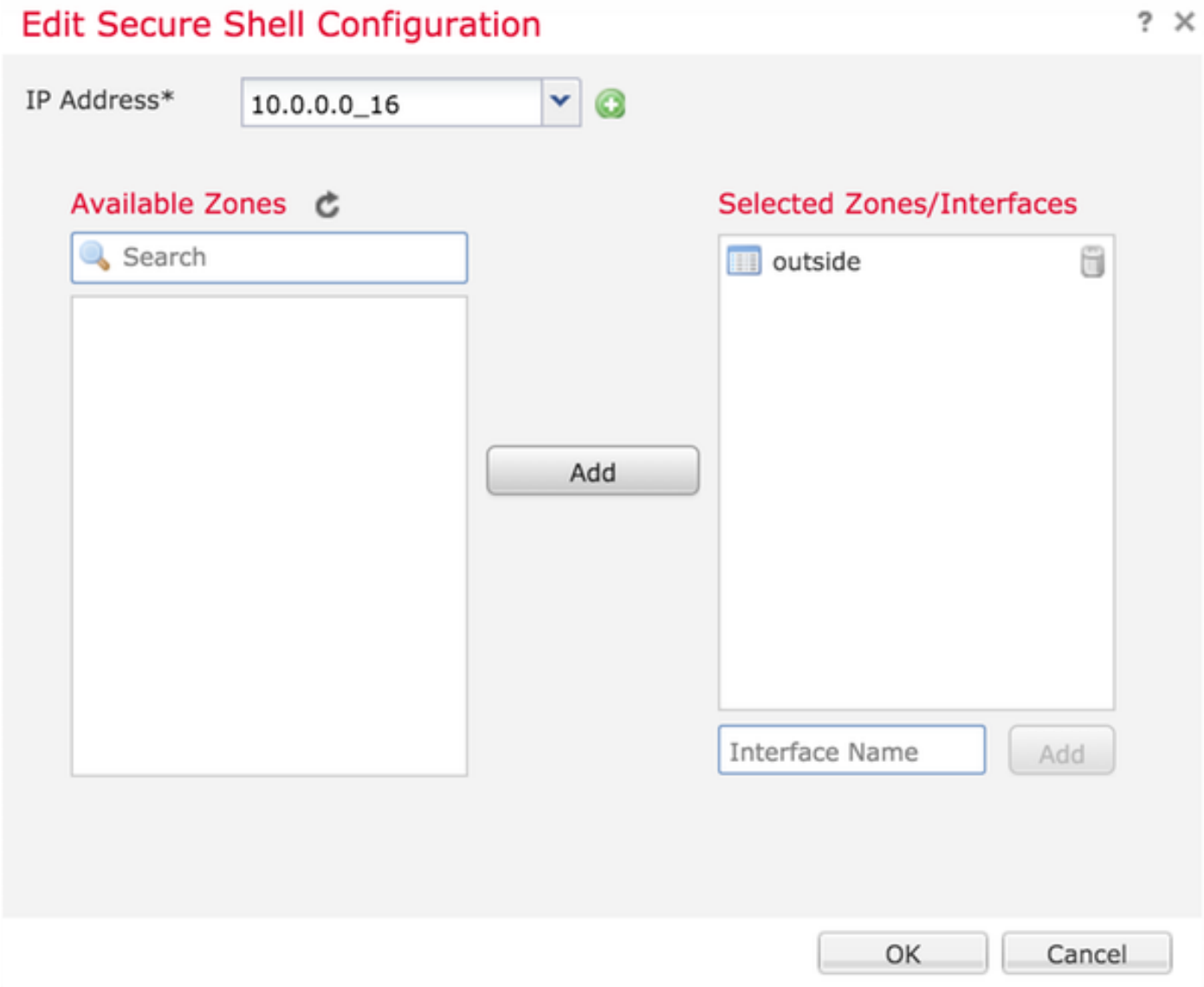


1단계. **Add(추가)**를 클릭하고 아래의 옵션을 구성합니다.

IP address(IP 주소) - SSH를 통해 CLI에 액세스할 수 있는 서브넷이 포함된 네트워크 개체를 선택합니다. 네트워크 개체가 없으면 **(+)** 아이콘을 클릭하여 개체를 생성합니다.

Selected Zones/interfaces(선택한 영역/인터페이스) - SSH 서버에 액세스하는 데 사용되는 영역이나 인터페이스를 선택합니다.

2단계. 그림에 나와 있는 것처럼 **OK(확인)**를 클릭합니다.



다음 명령을 사용하여 통합 CLI(6.0.1 디바이스에서는 ASA 진단 CLI)에서 SSH의 컨피그레이션을 확인합니다.

```
> show running-config ssh
ssh 172.16.8.0 255.255.255.0 inside
```

3단계. SSH 컨피그레이션을 완료한 후에 **Save(저장)**를 클릭한 다음 FTD에 정책을 구축합니다.

4단계. HTTPS 액세스 구성

하나 이상의 인터페이스에 대한 HTTPS 액세스를 활성화하려면 Platform Settings(플랫폼 설정)에서 **HTTP** 섹션으로 이동합니다. HTTPS 액세스는 분석을 위해 진단 보안 웹 인터페이스에서 패킷 캡처를 직접 다운로드할 때 특히 유용합니다.

아래의 여섯 단계를 통해 HTTP 액세스를 구성합니다.

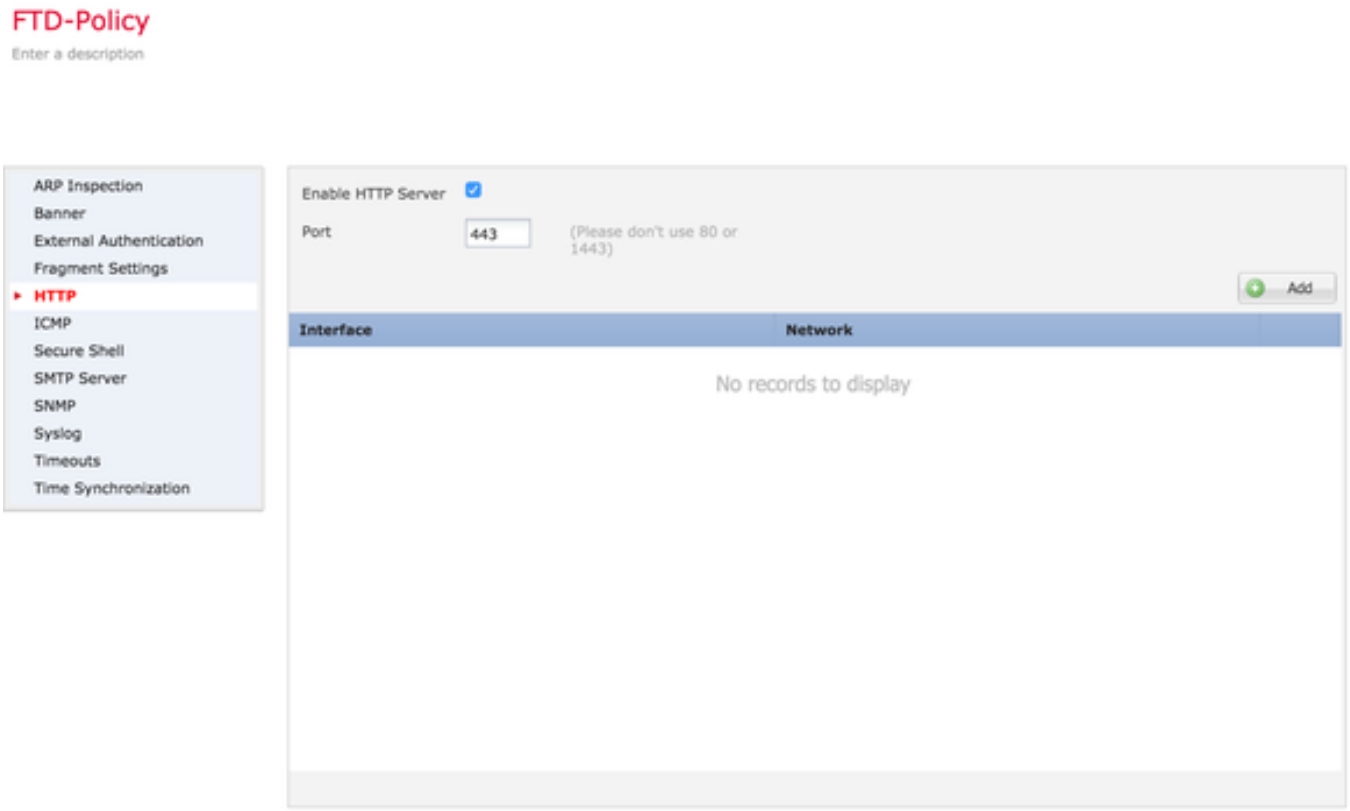
1단계. **Devices(디바이스) > Platform Settings(플랫폼 설정)**로 이동합니다.

2단계. 정책 옆에 있는 **연필** 아이콘을 클릭하여 기존 플랫폼 설정 정책을 수정하거나, **New Policy(새 정책)**를 클릭하여 새 FTD 정책을 생성합니다. 유형은 **Firepower Threat Defense**로 선택합니다.

3단계. **HTTP** 섹션으로 이동하면 그림에 나와 있는 것과 같은 페이지가 표시됩니다.

Enable HTTP server(HTTP 서버 활성화): FTD에서 HTTP 서버를 활성화하려면 이 옵션을 활성화합니다.

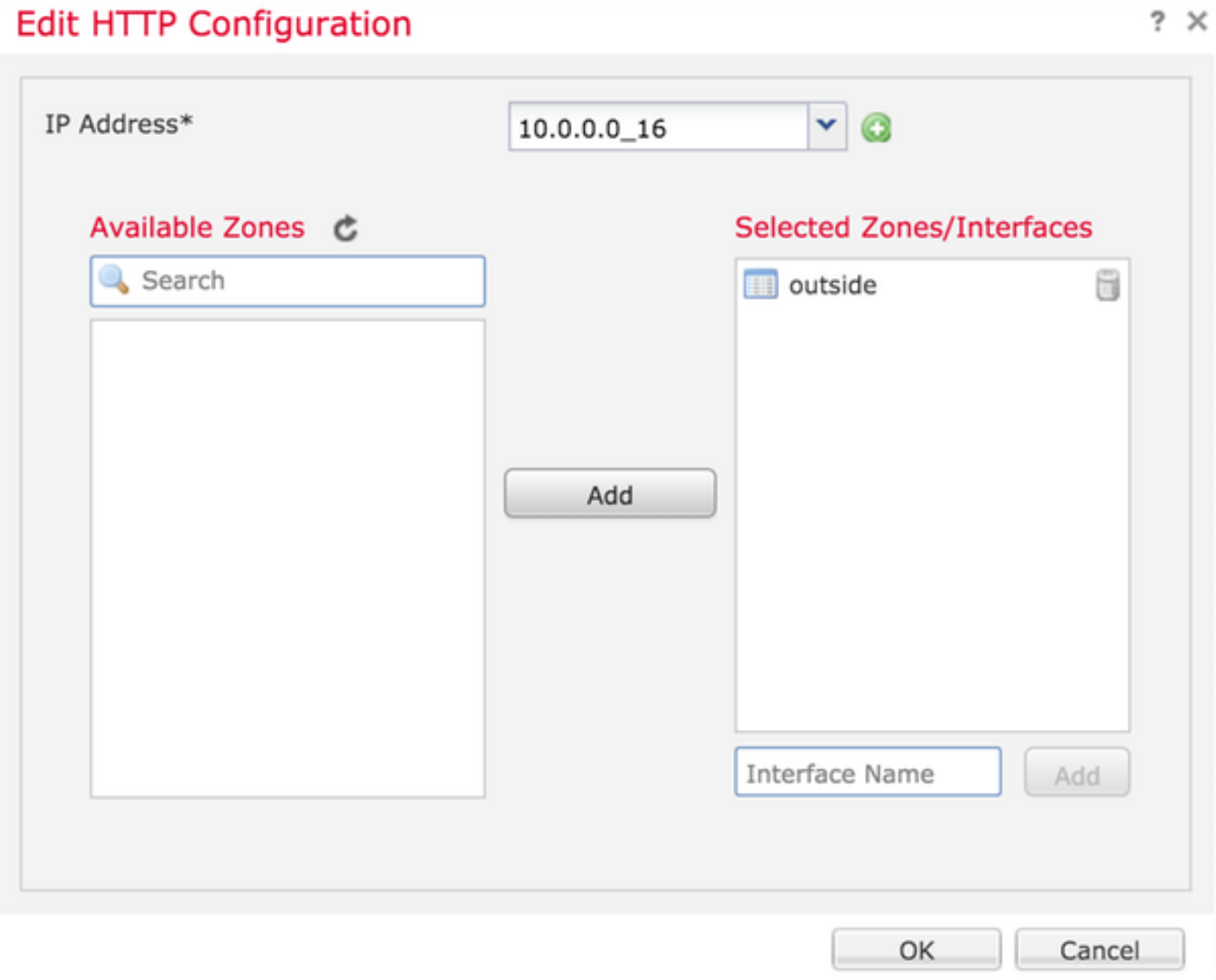
Port(포트): FTP에서 관리 연결을 수락하는 포트를 선택합니다.



4단계. **Add(추가)**를 클릭하면 그림에 나와 있는 것과 같은 페이지가 표시됩니다.

IP address(IP 주소) - 진단 인터페이스에 대한 HTTP 액세스가 허용되는 서브넷을 입력합니다. 네트워크 개체가 없으면 **(+)** 옵션을 사용하여 개체를 생성합니다.

Selected zones/Interfaces(선택한 영역/인터페이스) - SSH와 마찬가지로 HTTPS 컨피그레이션에서도 HTTPS를 통해 액세스하는 데 사용할 수 있는 인터페이스가 구성되어 있어야 합니다. HTTPS를 통해 FTD에 액세스하는 데 사용할 영역이나 인터페이스를 선택합니다.



다음 명령을 사용하여 통합 CLI(6.0.1 디바이스에서는 ASA 진단 CLI)에서 HTTP의 컨피그레이션을 확인합니다.

```
> show running-config http
http 172.16.8.0 255.255.255.0 inside
```

5단계. 필요한 컨피그레이션을 완료한 후 **OK(확인)**를 선택합니다.

6단계. 모든 필수 정보를 입력한 후에 **Save(저장)**를 클릭한 다음 디바이스에 정책을 구축합니다.

확인하기

현재는 이 컨피그레이션에 사용할 수 있는 확인 절차가 없습니다.

문제 해결

다음은 FTD의 관리 액세스 트러블슈팅을 위한 기본 단계입니다.

1단계. 인터페이스가 활성화되어 있으며 IP 주소를 사용하여 구성되어 있는지 확인합니다.

2단계. 외부 인증이 구성된 대로 작동하며, **Platform Settings(플랫폼 설정)**의 **External Authentication(외부 인증)** 섹션에 지정된 적절한 인터페이스에서 연결이 가능한지 확인합니다.

3단계. FTD의 라우팅이 정확한지 확인합니다. FTD 소프트웨어 버전 6.0.1에서 이렇게 하려면 **system support diagnostic-cli**로 이동한 다음 **show route** 및 **show route management-only** 명령을 실행하여 FTP 및 관리 인터페이스의 경로를 각각 확인합니다.

FTD 소프트웨어 버전 6.1.0에서는 통합 CLI에서 명령을 직접 실행합니다.

관련 정보

- **ASA Cisco Firepower Threat Defense**
- **& - Cisco Systems**