FMC를 통해 FTD(HTTPS 및 SSH)에 대한 관리 액세스 구성

목차

소개

이 문서에서는 FMC(FireSIGHT Management Center)를 통한 FTD(Firepower Threat Defense)(HTTPS 및 SSH)에 대한 관리 액세스 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 기술 지식
- ASA에 대한 기본 지식(Adaptive Security Appliance)
- HTTPS 및 SSH를 통한 ASA의 관리 액세스 지식(Secure Shell)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.1 이상에서 실행되는 ASA(5506X/5506H-X/5506W-X/5506W-X, ASA 5508-X, ASA 5516-X)용 ASA(Adaptive Security Appliance) Firepower Threat Defense 이미지

- 소프트웨어 버전 6.0.1 이상에서 실행되는 ASA용 ASA Firepower Threat Defense 이미지(5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X)
- 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FTD(Firepower Threat Defense)가 시작되면서 전체 ASA 관련 컨피그레이션이 GUI에서 수행됩니다.

소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서 ASA 진단 CLI는 **시스템 지원 diagnostic-cli**를 입력할 때 **액세스합니다**. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서 CLI가 통합되고 전체 ASA 명령이 CLISH에 구성됩니다.

```
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
```

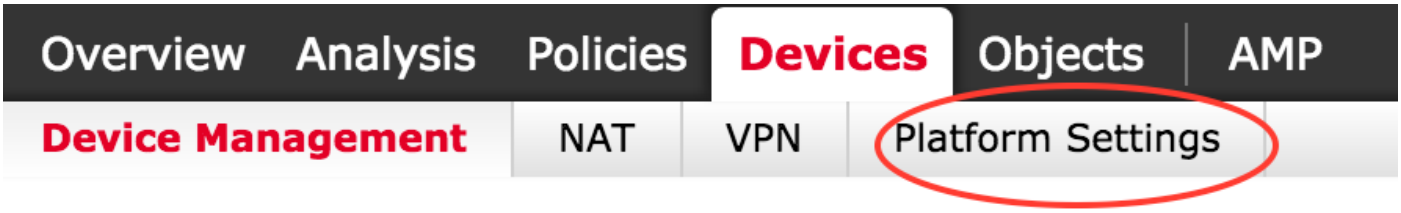
외부 네트워크에서 직접 관리 액세스를 얻으려면 HTTPS 또는 SSH를 통해 관리 액세스를 구성해야 합니다. 이 문서에서는 SSH 또는 HTTPS를 통해 외부에서 관리 액세스를 얻는 데 필요한 컨피그레이션을 제공합니다.

> **참고:** 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서 로컬 사용자가 CLI에 액세스할 수 없습니다. 사용자를 인증하려면 외부 인증을 구성해야 합니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서 CLI는 로컬 **관리자** 사용자가 액세스하지만 다른 모든 사용자는 외부 인증이 필요합니다.

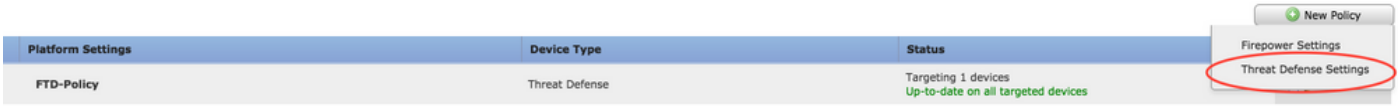
> **참고:** 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서는 FTD의 **br1**에 대해 구성된 IP를 통해 진단 CLI에 직접 액세스할 수 없습니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서는 관리 액세스를 위해 구성된 모든 인터페이스를 통해 통합 CLI에 액세스할 수 있지만 IP 주소로 인터페이스를 구성해야 합니다.

구성

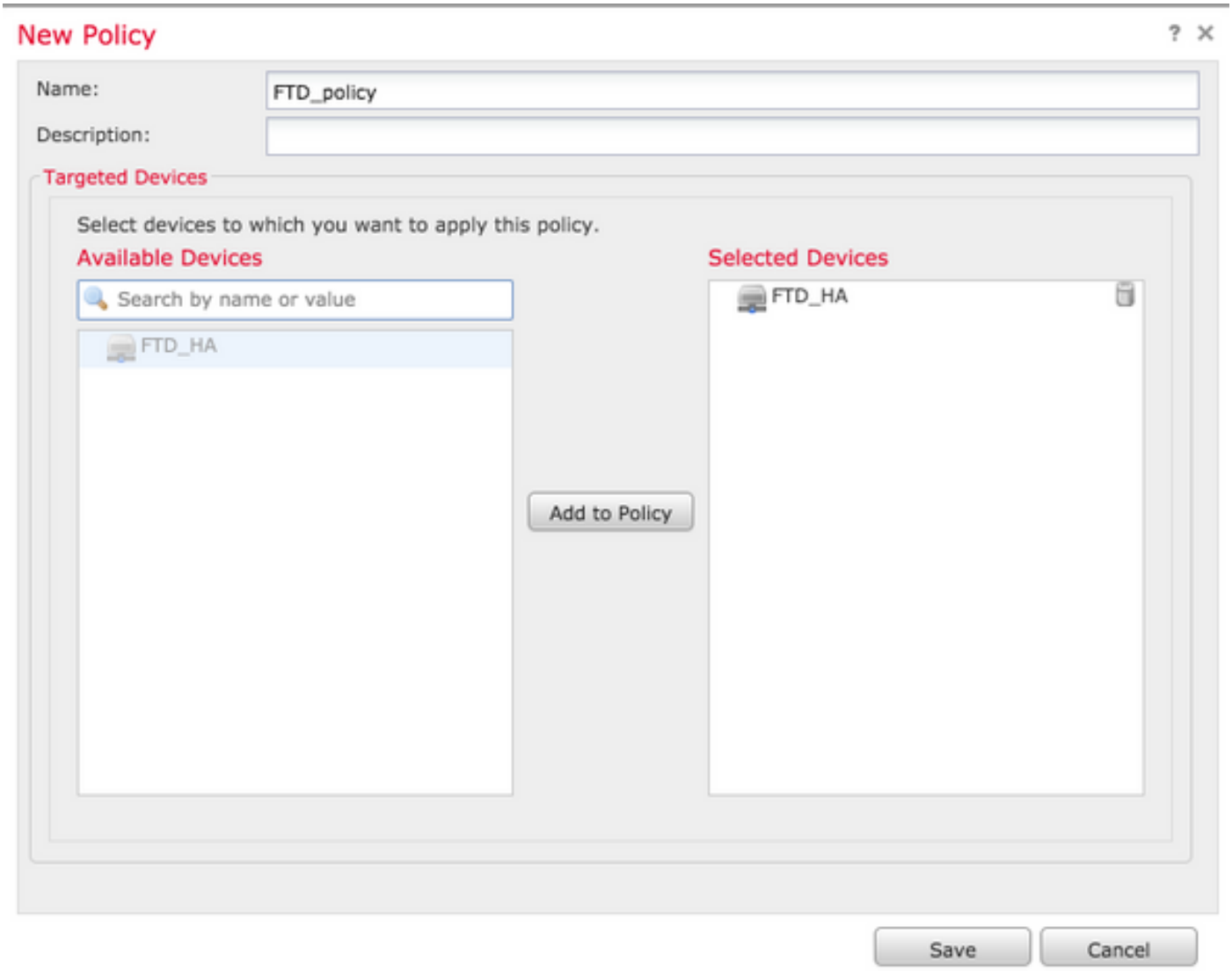
모든 Management Access 관련 컨피그레이션은 이미지에 표시된 대로 **Devices**에서 Platform Settings(**플랫폼 설정**) 탭으로 이동할 때 구성됩니다.



연필 아이콘을 클릭할 때 존재하는 정책을 수정하거나 **New Policy** 버튼을 클릭할 때 새 FTD 정책을 생성하고 이미지에 표시된 것처럼 유형을 **Threat Defense Settings(위협 방어 설정)**로 선택합니다.



이 정책을 적용할 FTD 어플라이언스를 선택하고 이미지에 표시된 대로 **Save(저장)**를 클릭합니다.



관리 액세스 구성

다음은 관리 액세스를 구성하기 위해 수행하는 4가지 주요 단계입니다.

1단계. FMC GUI를 통해 FTD 인터페이스에서 IP를 구성합니다.

SSH 또는 HTTPS를 통해 FTD에 액세스할 수 있는 인터페이스에서 IP를 구성합니다. FTD의 **Interfaces** 탭으로 이동할 때 존재하는 인터페이스를 편집합니다.

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

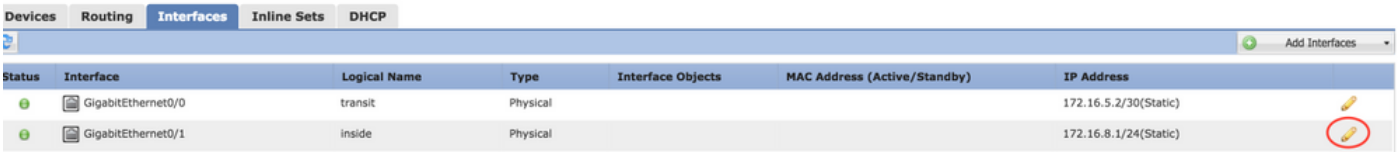
진단 인터페이스를 구성하는 6단계가 있습니다.

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

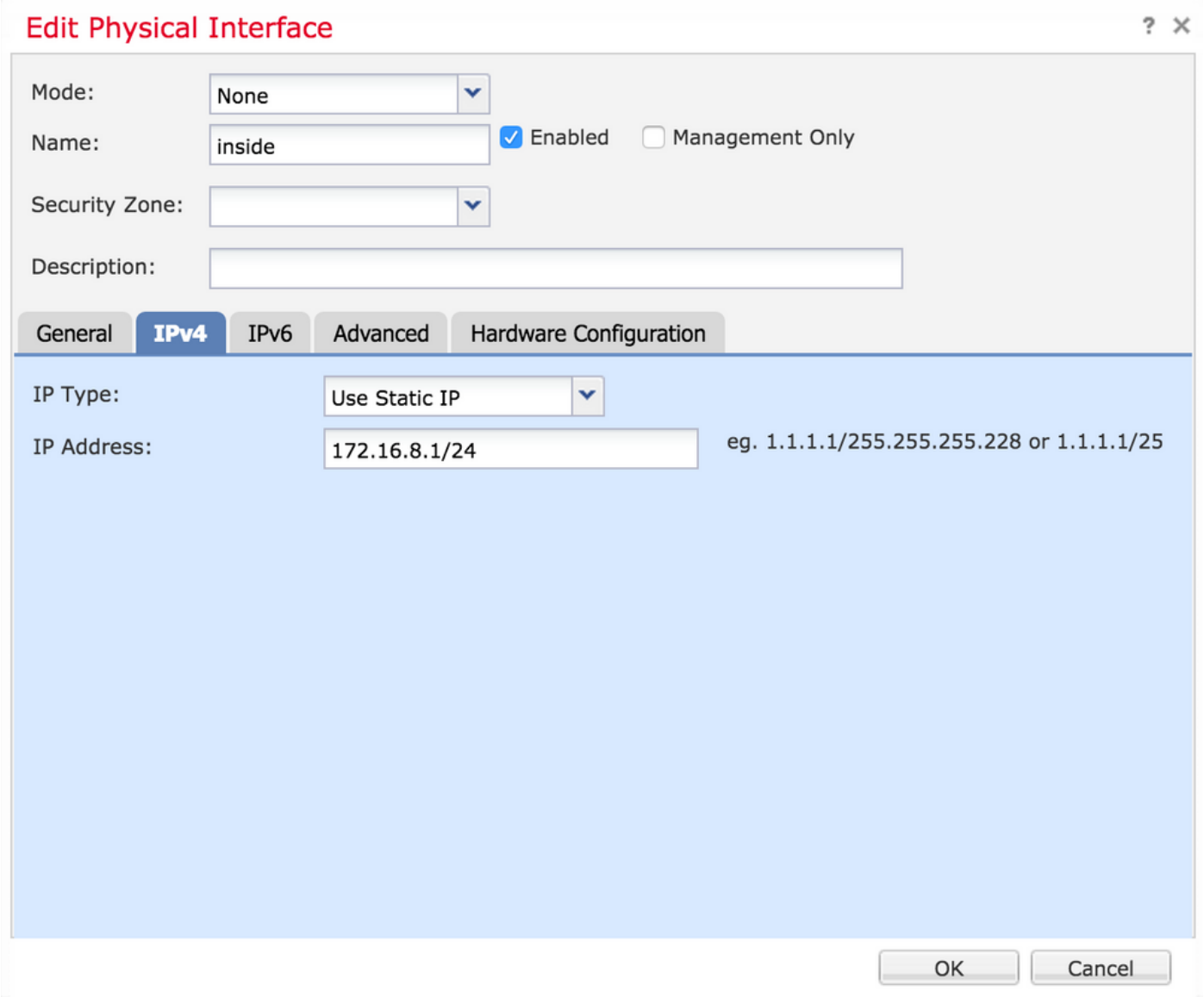
2단계. 디바이스 또는 FTD HA 클러스터를 선택합니다.

3단계. Interfaces(인터페이스) 탭**으로** 이동합니다.

4단계. **연필 아이콘**을 클릭하여 다음 이미지와 같이 관리 액세스를 얻기 위해 인터페이스를 구성/편집합니다.



5단계. **활성화** 확인란을 선택하여 인터페이스를 활성화합니다. Ipv**4** 탭으로 이동하고 IP Type(IP 유형)을 **고정 또는 DHCP로 선택합니다**. 이제 인터페이스에 대한 IP 주소를 입력하고 이미지에 표시된 대로 **OK**를 클릭합니다.



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

> **참고**: 진단 인터페이스를 사용하여 소프트웨어 버전 6.1.0의 디바이스에서 SSH를 통한 통합 CLI에 액세스할 수 없습니다.

2단계. 외부 인증을 구성합니다.

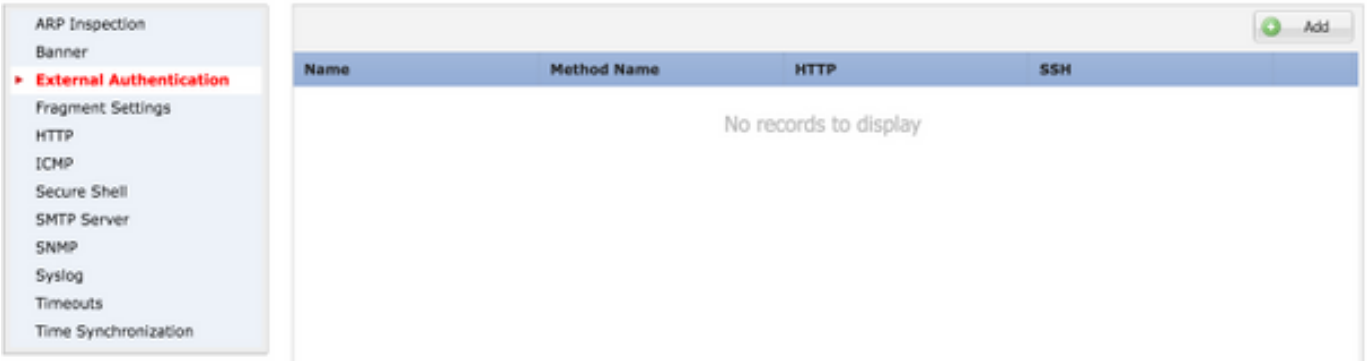
외부 인증은 사용자 인증을 위해 FTD를 Active Directory 또는 RADIUS 서버에 통합할 수 있도록 합니다. 로컬로 구성된 사용자는 진단 CLI에 직접 액세스할 수 없으므로 이 단계는 필수입니다. 진단 CLI 및 GUI는 LDAP(Lightweight Directory Access Protocol) 또는 RADIUS를 통해 인증된 사용자만 액세스할 수 있습니다.

외부 인증을 구성하는 6단계가 있습니다.

1단계. 다음으로 이동합니다. **디바이스 > 플랫폼 설정.**

2단계. 연필 아이콘을 클릭할 때 존재하는 정책을 수정하거나 **New Policy** 버튼을 클릭할 때 새 FTD 정책을 생성하고 유형을 선택합니다. **위협 방어 설정.**

3단계. 이미지에 표시된 대로 **외부 인증** 탭으로 이동합니다.



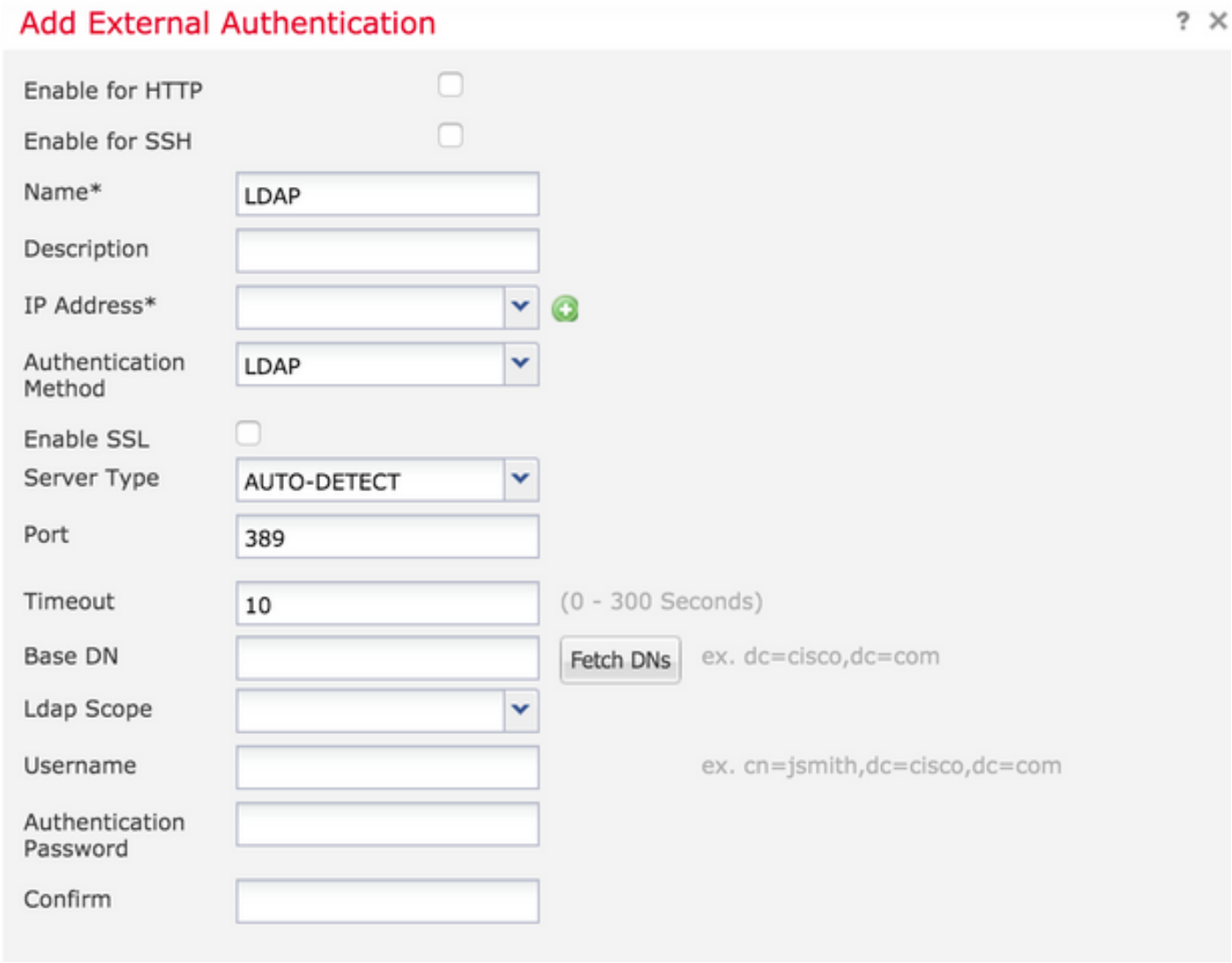
4단계. **Add(추가)**를 클릭하면 다음과 같은 대화상자가 나타납니다.

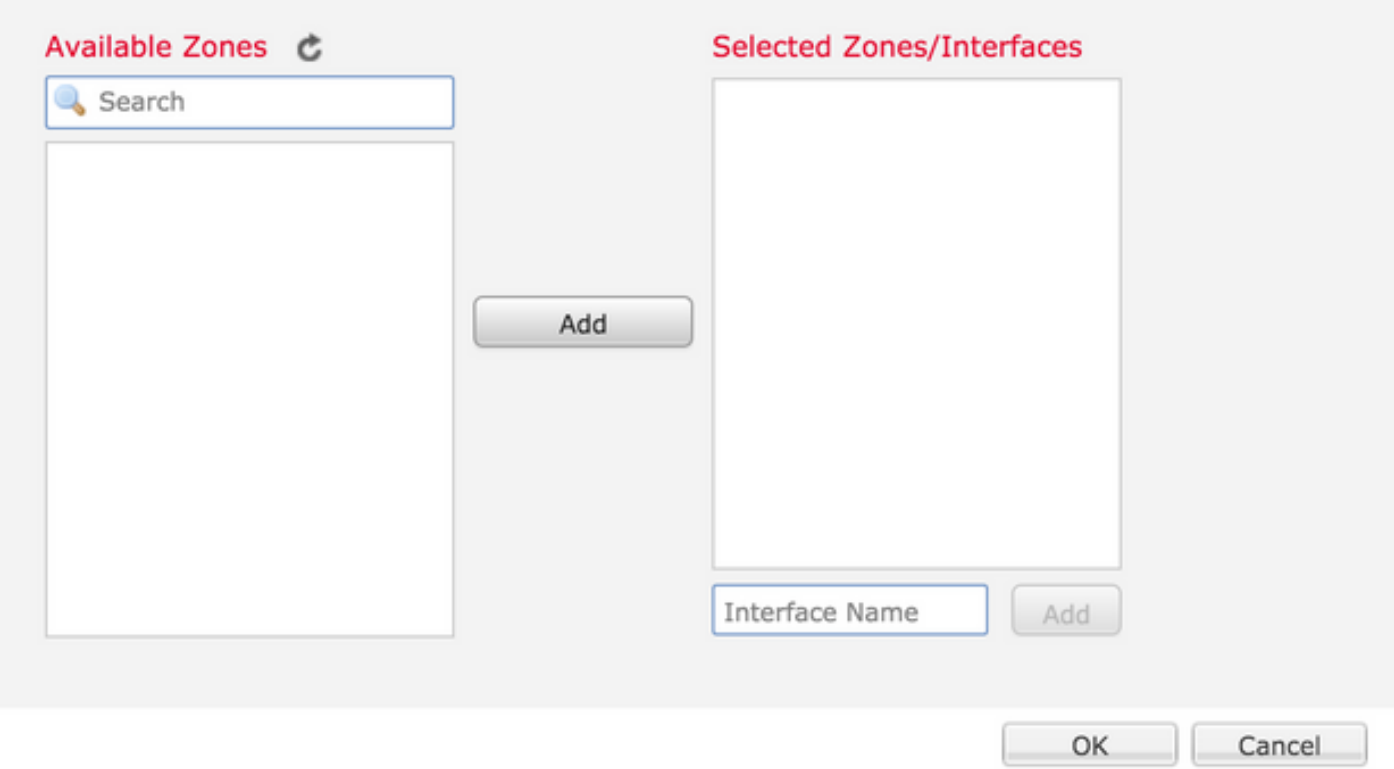
- **Enable for HTTP(HTTP**에 대해 활성화) - HTTPS를 통한 FTD 액세스를 제공하려면 이 옵션을 활성화합니다.
- **Enable for SSH(SSH에 대해 활성화**) - SSH를 통한 FTD에 대한 액세스를 제공하려면 이 옵션을 활성화합니다.
- **Name**(이름) - LDAP 연결의 이름을 입력합니다.
- **Description**(설명) - 외부 인증 객체에 대한 선택적 설명을 입력합니다.
- **IP 주소** - 외부 인증 서버의 IP를 저장하는 네트워크 객체를 입력합니다. 구성된 네트워크 개체가 없으면 새 개체를 만듭니다. **(+)** 아이콘을 클릭합니다.
- **Authentication Method(인증 방법**) - 인증을 위해 RADIUS 또는 LDAP 프로토콜을 선택합니다.
- **Enable SSL**-Enable 이 옵션을 활성화하여 인증 트래픽을 암호화합니다.
- **Server Type**(서버 유형) - 서버 유형을 선택합니다. 잘 알려진 서버 유형은 MS Active Directory, Sun, OpenLDAP 및 NovelI입니다. 기본적으로 이 옵션은 서버 유형을 자동으로 탐지하도록 설정됩니다.
- **Port**(포트) - 인증이 발생하는 포트를 입력합니다.
- **Timeout**(시간 제한) - 인증 요청에 대한 시간 제한 값을 입력합니다.
- **Base DN** - 기본 DN을 입력하여 사용자가 존재할 수 있는 범위를 제공합니다.
- **LDAP Scope**(LDAP 범위) - 확인할 LDAP 범위를 선택합니다. 범위가 동일한 레벨 내에 있거나 하위 트리 내에서 검색됩니다.
- **Username**(사용자 이름) - LDAP 디렉토리에 바인딩할 사용자 이름을 입력합니다.

- **인증 비밀번호** - 이 사용자의 비밀번호를 입력합니다.
- **확인** - 비밀번호를 다시 입력합니다.
- **Available Interfaces**(사용 가능한 인터페이스) - FTD에서 사용 가능한 인터페이스 목록이 표시됩니다.
- **선택한 영역 및 인터페이스** - 인증 서버에 액세스할 수 있는 인터페이스 목록을 표시합니다.

RADIUS 인증의 경우 서버 유형 Base DN 또는 LDAP Scope가 없습니다. 포트는 RADIUS 포트 1645입니다.

Secret(비밀) - RADIUS의 비밀 키를 입력합니다.





5단계. 구성이 완료되면 **확인**을 클릭합니다.

6단계. 정책을 저장하고 Firepower Threat Defense 디바이스에 구축합니다.

> **참고**: 외부 인증은 소프트웨어 버전 6.1.0의 디바이스에서 SSH를 통한 통합 CLI에 액세스하는 데 사용할 수 없습니다.

3단계. SSH 액세스를 구성합니다.

SSH는 통합 CLI에 직접 액세스합니다. 이 옵션을 사용하여 CLI에 직접 액세스하고 디버그 명령을 실행합니다.이 섹션에서는 FTD CLI에 액세스하기 위해 SSH를 구성하는 방법에 대해 설명합니다.

> **참고:** 소프트웨어 버전 6.0.1을 실행하는 FTD 디바이스에서 플랫폼 설정의 SSH 컨피그레이션은 CLISH가 아니라 진단 CLI에 직접 액세스할 수 있도록 합니다. CLISH에 액세스하려면 **br1**에 구성된 IP 주소에 연결해야 합니다. 그러나 소프트웨어 버전 6.1.0을 실행하는 FTD 디바이스에서 모든 인터페이스는 SSH를 통해 액세스하면 통합된 CLI로 이동합니다

ASA에서 SSH를 구성하는 6단계가 있습니다.

6.0.1 디바이스에서만:

이러한 단계는 소프트웨어 버전이 6.1.0 미만이고 6.0.1보다 큰 FTD 장치에서 수행됩니다. 6.1.0 디바이스에서 이러한 매개변수는 OS에서 상속됩니다.

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

2단계. 연필 아이콘을 클릭할 때 존재하는 정책을 편집하거나 **New Policy** 버튼을 클릭할 때 새 Firepower Threat Defense 정책을 생성하고 **Threat Defense 설정**으로 유형을 **선택합니다.**

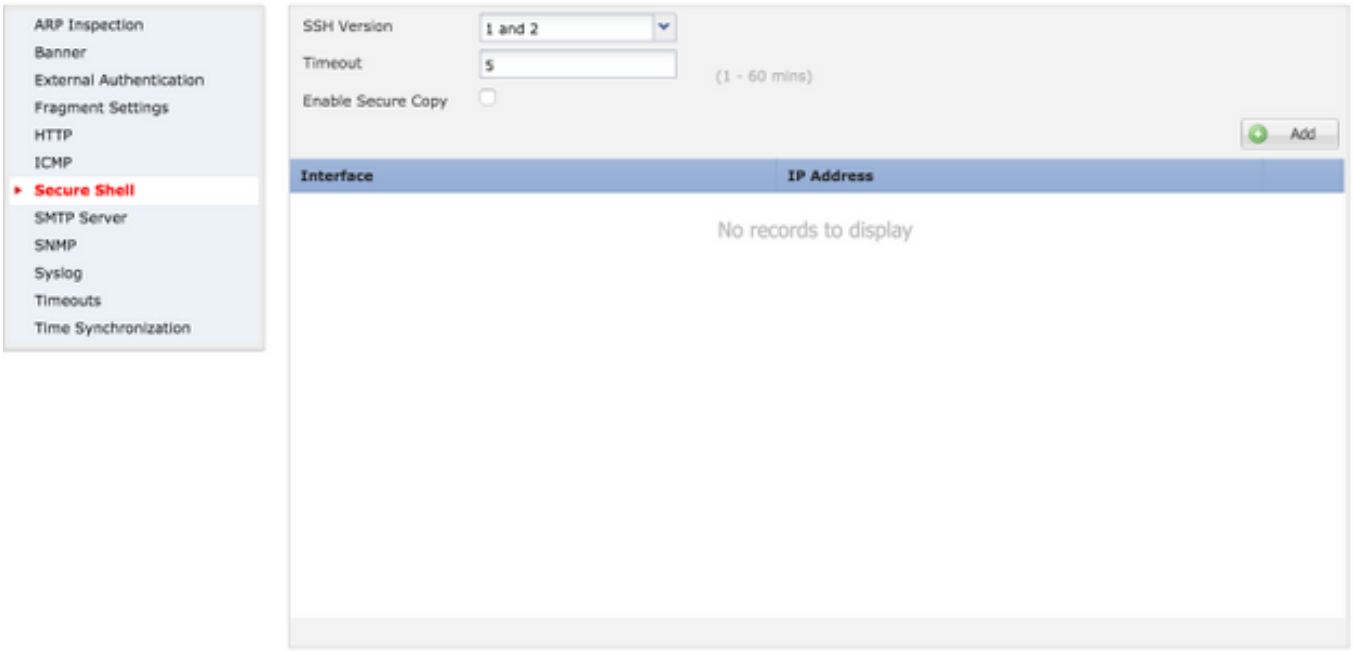
3단계. **Secure Shell** 섹션**으로** 이동합니다. 이미지에 표시된 것처럼 페이지가 나타납니다.

SSH 버전: ASA에서 활성화할 SSH 버전을 선택합니다. 세 가지 옵션이 있습니다.

- **1:** SSH 버전 1만 사용
- **2:** SSH 버전 2만 사용
- **1 및 2:** SSH 버전 1 및 2 모두 활성화

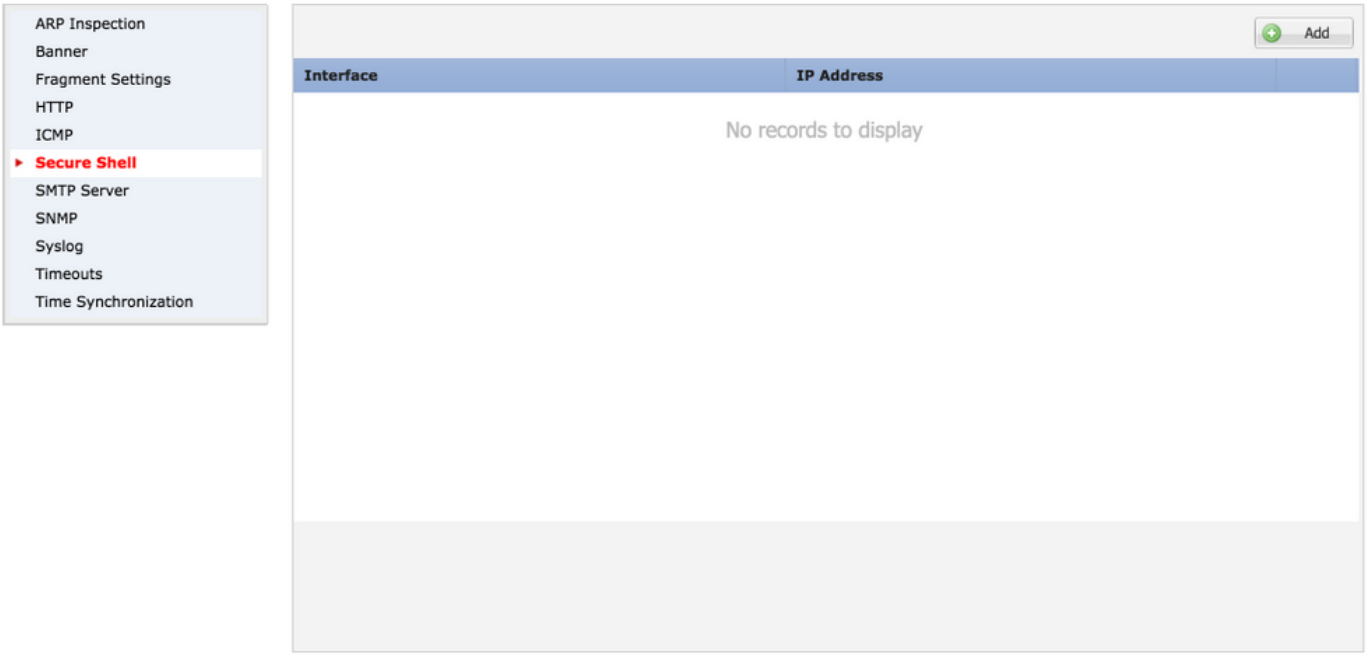
시간 초과: 원하는 SSH 시간 제한을 분 단위로 입력합니다.

Enable Secure Copy(보안 복사 활성화) - SCP(Secure Copy) 연결을 허용하고 SCP 서버 역할을 하도록 디바이스를 구성하려면 이 옵션을 활성화합니다.



6.0.1 및 6.1.0 장치에서:

이러한 단계는 SSH를 통한 관리 액세스를 특정 인터페이스 및 특정 IP 주소로 제한하도록 구성됩니다.

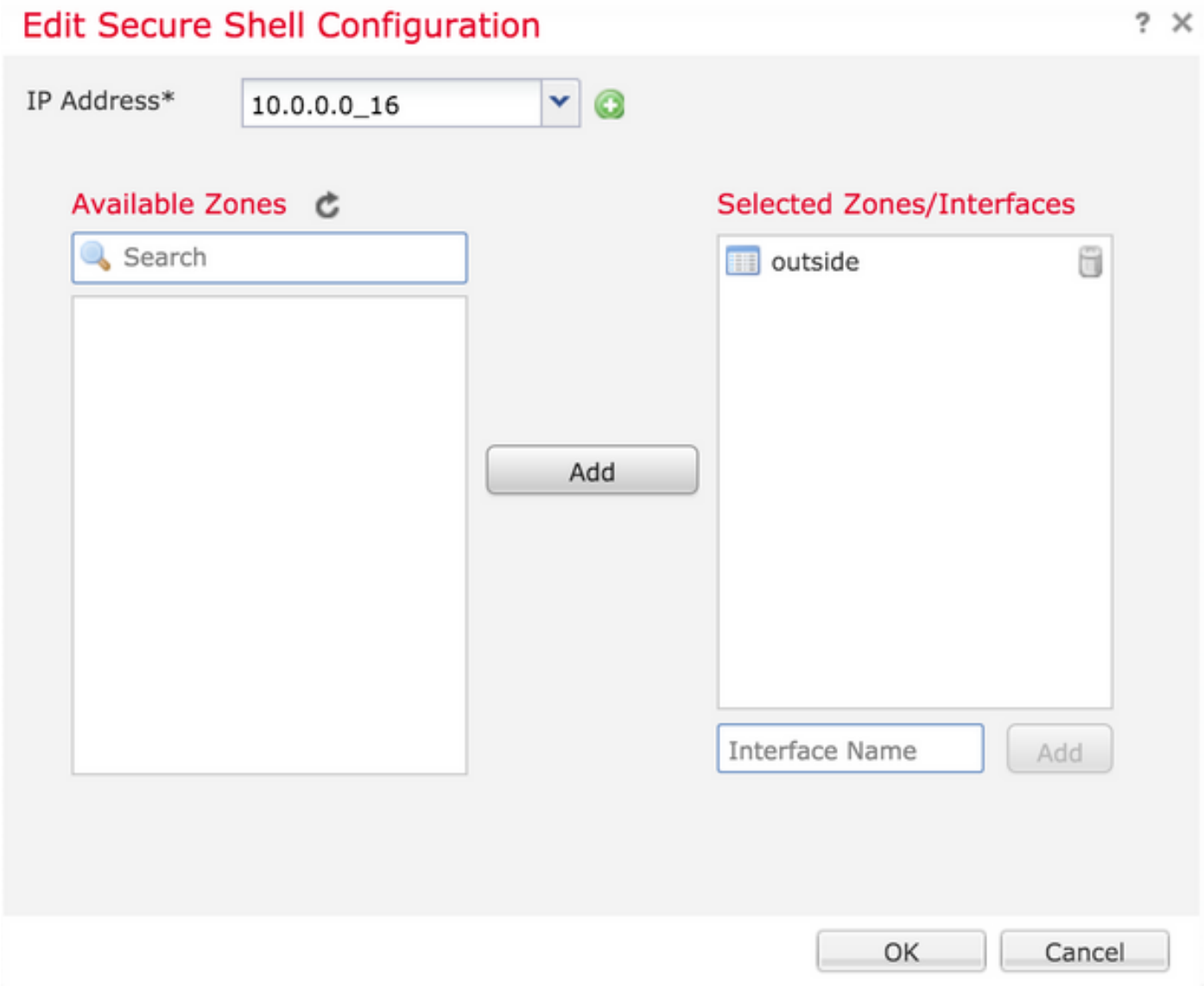


1단계. Add(추가)를 **클릭하고** 다음 옵션을 구성합니다.

IP 주소: SSH를 통해 CLI에 액세스할 수 있는 서브넷이 포함된 네트워크 개체를 선택합니다. 네트워크 객체가 없는 경우 **(+)** 아이콘을 클릭할 때 네트워크 객체**를** 생성합니다.

선택한 영역/인터페이스: SSH 서버에 액세스할 영역 또는 인터페이스를 선택합니다.

2단계. 이미지에 표시된 대로 **확인**을 클릭합니다.



SSH에 대한 컨피그레이션은 컨버지드 CLI(6.0.1 디바이스의 ASA 진단 CLI)에서 이 명령을 사용하여 볼 수 있습니다.

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

3단계. SSH 컨피그레이션이 완료되면 **Save(저장)**를 클릭하고 FTD에 정책을 구축합니다.

4단계. HTTPS 액세스를 구성합니다.

하나 이상의 인터페이스에 대한 HTTPS 액세스를 활성화하려면 플랫폼 설정의 **HTTP** 섹션으로 이동합니다. HTTPS 액세스는 분석을 위해 진단 보안 웹 인터페이스에서 패킷 캡처를 직접 다운로드하는 데 특히 유용합니다.

HTTPS 액세스를 구성하는 6단계가 있습니다.

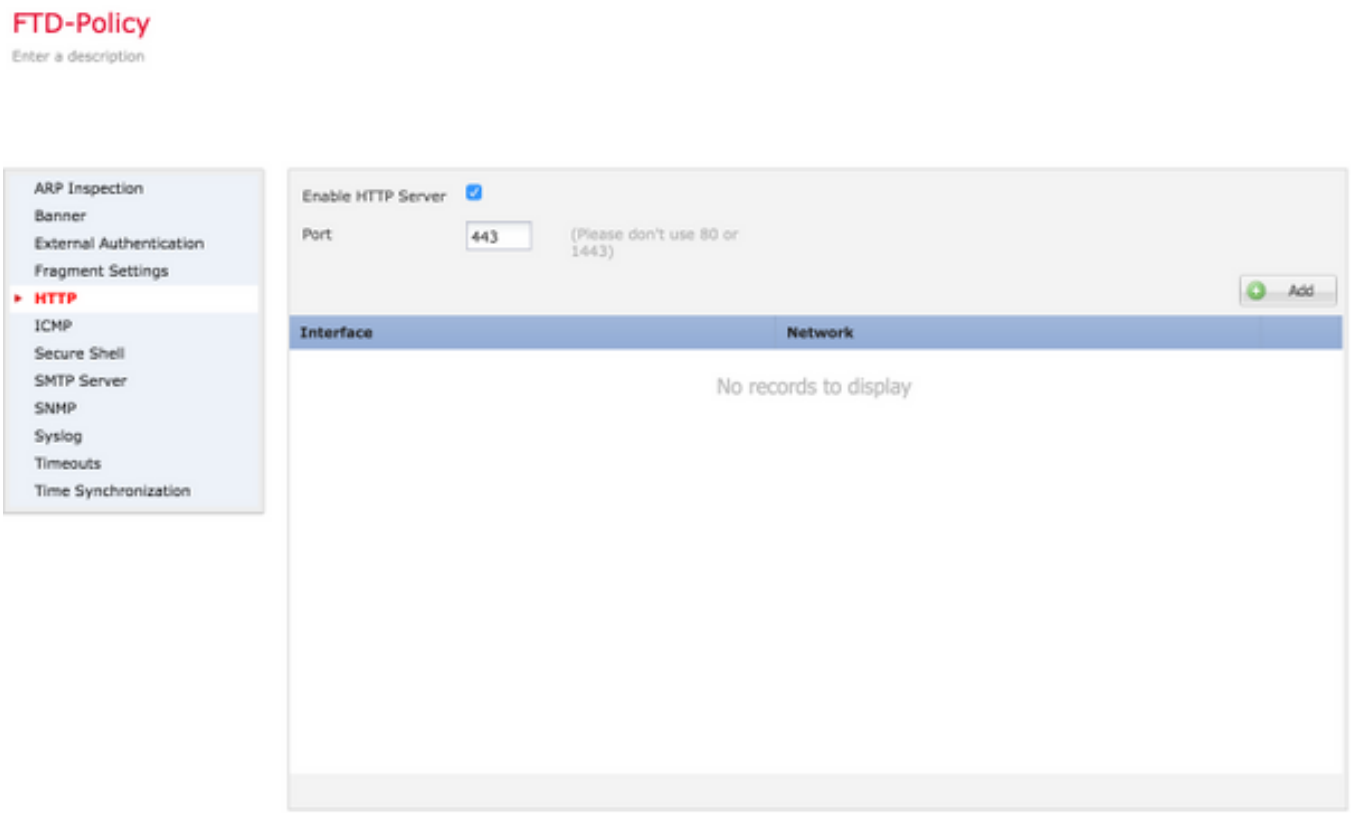
1단계. Devices(디바이스) **> Platform Settings(플랫폼 설정)로 이동합니다.**

2단계. 정책 옆에 있는 **연필 아이콘**을 클릭할 때 존재하는 플랫폼 설정 정책을 편집하거나 **새 정책**을 클릭할 때 새 FTD 정책을 **생성합니다**. 유형을 **Firepower Threat Defense**로 **선택합니다.**

3단계. **HTTP** 섹션으로 이동하면 이미지에 표시된 것처럼 페이지가 나타납니다.

HTTP 서버 사용: FTD에서 HTTP 서버를 활성화하려면 이 옵션을 활성화합니다.

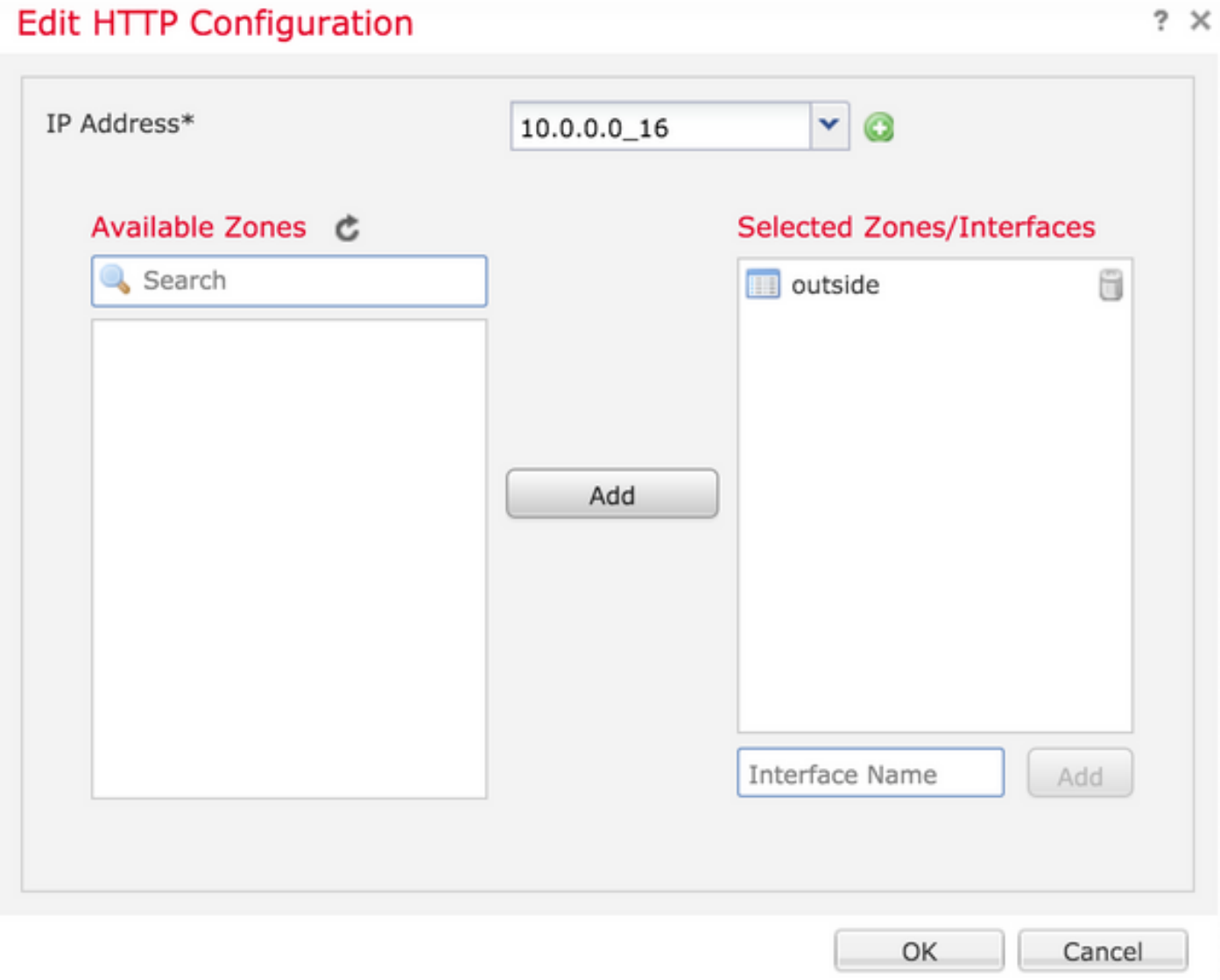
포트: FTD에서 관리 연결을 수락하는 포트를 선택합니다.



4단계. 이미지에 표시된 대로 Add and page(추가 및 페이지)를 클릭합니다.

IP 주소 - 진단 인터페이스에 대한 HTTPS 액세스가 허용되는 서브넷을 입력합니다. 네트워크 개체가 없으면 네트워크 개체를 만들고 **(+)** 옵션을 사용합니다.

Selected zones/Interfaces(선택한 영역/인터페이스) - SSH와 유사하게, HTTPS 컨피그레이션에는 HTTPS를 통해 액세스할 수 있는 인터페이스가 구성되어 있어야 합니다. HTTPS를 통해 FTD에 액세스할 영역 또는 인터페이스를 선택합니다.



HTTPS에 대한 컨피그레이션은 컨버지드 CLI(6.0.1 디바이스의 ASA Diagnostic CLI)에서 보고 이 명령을 사용합니다.

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

5단계. 필요한 컨피그레이션이 완료되면 확인을 **선택합니다.**

6단계. 필요한 정보를 모두 입력했으면 **Save(저장)**를 클릭하고 디바이스에 정책을 구축합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

다음은 FTD에서 관리 액세스 문제를 해결하기 위한 기본 단계입니다.

1단계. 인터페이스가 활성화되었고 IP 주소로 구성되어 있는지 확인합니다.

2단계. 외부 인증이 구성된 대로 작동하며 **플랫폼 설정**의 **외부 인증** 섹션에 지정된 적절한 인터페이스에서 연결되는지 **확인합니다**.

3단계. FTD의 라우팅이 정확한지 확인합니다. FTD 소프트웨어 버전 6.0.1에서 **system support diagnostic-cli로** 이동합니다. 명령 **show route** 및 **show route management-only를 실행하여** 각각 FTD 및 관리 인터페이스의 경로를 확인합니다.

FTD 소프트웨어 버전 6.1.0에서 통합 CLI에서 명령을 직접 실행합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems