FMCを介したFTD（HTTPSおよびSSH）への管理アクセスの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[管理アクセスの設定](#)
[ステップ1:FMC GUIを使用してFTDインターフェイスにIPを設定します。](#)
[ステップ2：外部認証を設定します。](#)
[ステップ3:SSHアクセスを設定します。](#)
[ステップ4:HTTPSアクセスを設定します。](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、Firesight Management Center(FMC)を介したFirepower Threat Defense(FTD)（HTTPSおよびSSH）への管理アクセスの設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識
- ASA（適応型セキュリティアプライアンス）の基礎知識
- HTTPSおよびSSH（セキュアシェル）を介したASAでの管理アクセスに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 適応型セキュリティアプライアンス(ASA)Firepower Threat Defense Image for ASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。ソフトウェアバージョン

6.0.1以降で稼働します。
- ASA用ASA Firepower Threat Defense(FTD)イメージ(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)。ソフトウェアバージョン6.0.1以降で稼働します。
- Firepower Management Center(FMC)バージョン6.0.1以降。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Firepower Threat Defense(FTD)の開始時には、ASA関連の設定全体がGUIで実行されます。

ソフトウェアバージョン6.0.1が稼働するFTDデバイスでは、system support diagnostic-cliを入力すると、ASA診断CLIにアクセスします。ただし、ソフトウェアバージョン6.1.0が稼働するFTDデバイスでは、CLIが統合され、ASAコマンド全体がCLISHに設定されます。

```
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
```

外部ネットワークから直接管理アクセスを取得するには、HTTPSまたはSSHを介して管理アクセスを設定する必要があります。このドキュメントでは、外部からSSHまたはHTTPSを介して管理アクセスを取得するために必要な設定について説明します。

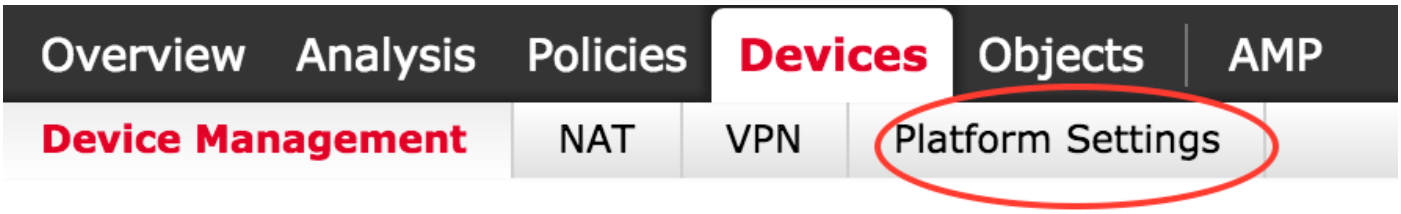
> **注：**ソフトウェアバージョン6.0.1が稼働するFTDデバイスでは、ローカルユーザはCLIにアクセスできません。ユーザを認証するには、外部認証を設定する必要があります。ただし、ソフトウェアバージョン6.1.0が稼働するFTDデバイスでは、ローカルの**admin**ユーザがCLIにアクセスし、その他すべてのユーザには外部認証が必要です。

> **注：**ソフトウェアバージョン6.0.1が稼働するFTDデバイスでは、FTDの**br1**に設定されたIPを介して診断CLIに直接アクセスできません。ただし、ソフトウェアバージョン6.1.0が稼働するFTDデバイスでは、管理アクセスが設定された任意のインターフェイスを介して統合CLIにアクセスできますが、インターフェイスはIPアドレスで設定する必要があります。

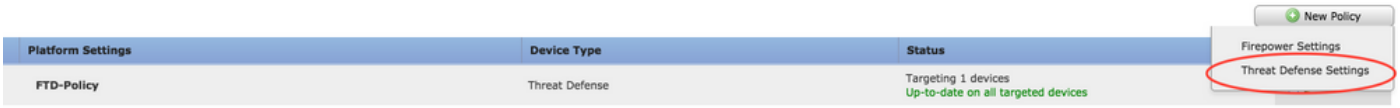
設定

図に示すように、[Devices] の[Platform Settings] タブに移動すると、管理アクセス関連のすべて

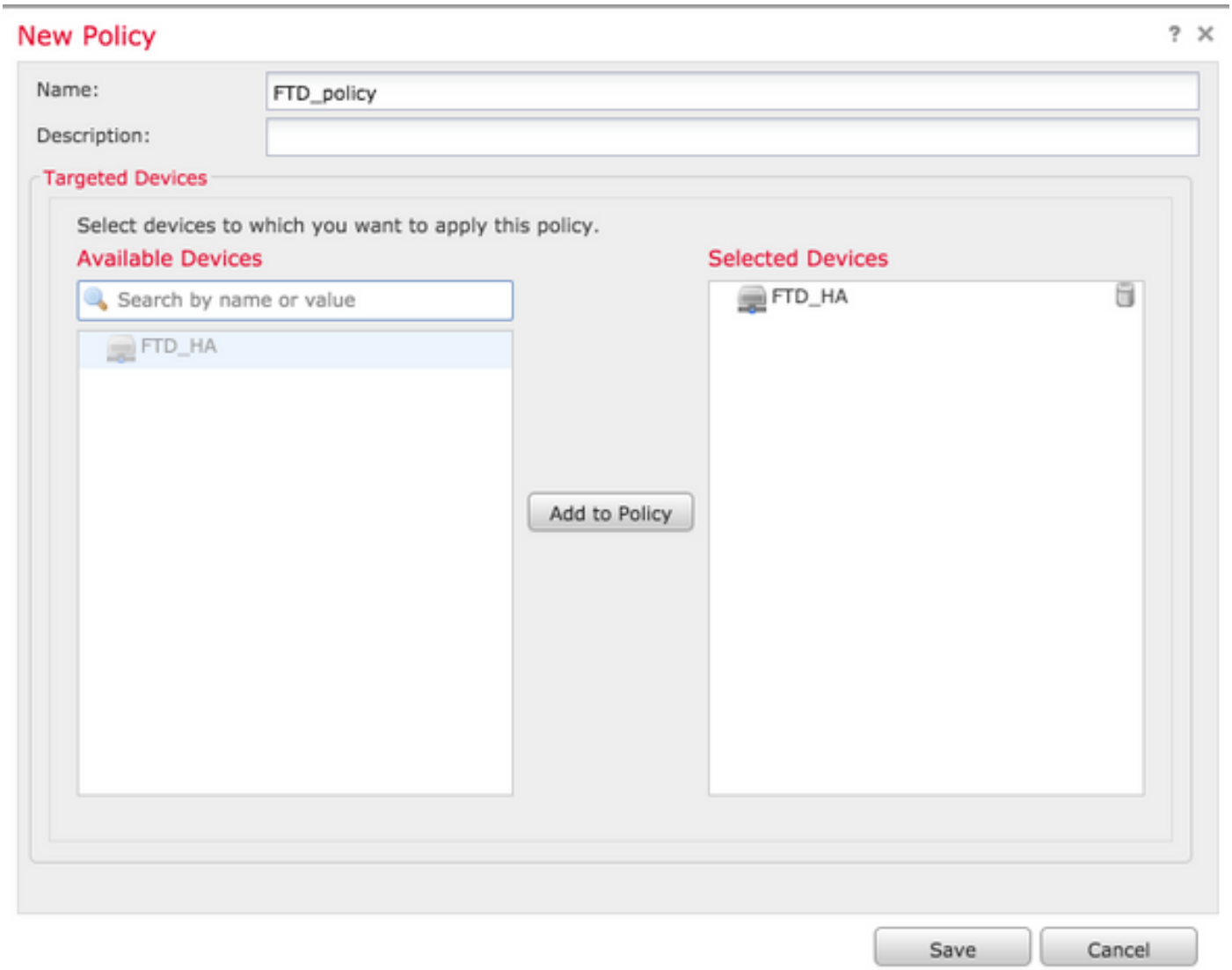
の設定が構成されます。



次の図に示すように、鉛筆アイコンをクリックして存在するポリシーを編集するか、[New Policy] ボタンをクリックして新しいFTDポリシーを作成し、[Threat Defense Settings] として[type]を選択します。



このポリシーを適用するFTDアプライアンスを選択し、図に示すように[Save] をクリックします。



管理アクセスの設定

管理アクセスを設定するために実行する4つの主要な手順を次に示します。

ステップ1:FMC GUIを使用してFTDインターフェイスにIPを設定します。

SSHまたはHTTPS経由でFTDにアクセスできるインターフェイスにIPを設定します。FTDの [Interfaces] タブに移動するときに、存在するインターフェイスを編集します。

> **注：**ソフトウェアバージョン6.0.1が稼働するFTDデバイスでは、FTDのデフォルトの管理インターフェイスはdiagnostic0/0インターフェイスです。ただし、ソフトウェアバージョン6.1.0が稼働するFTDデバイスでは、診断インターフェイスを除くすべてのインターフェイスで管理アクセスがサポートされています。

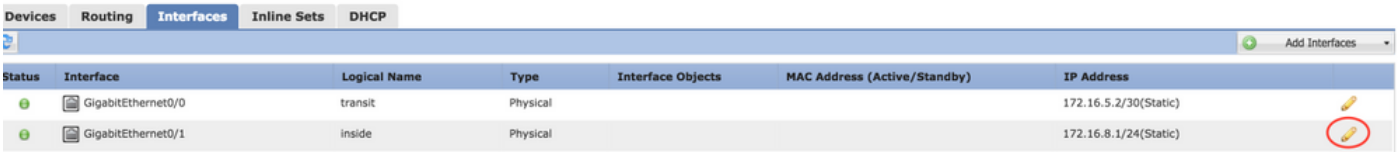
診断インターフェイスを設定するには、6つのステップがあります。

ステップ1：に移動します。 **[Device] > [Device Management]。**

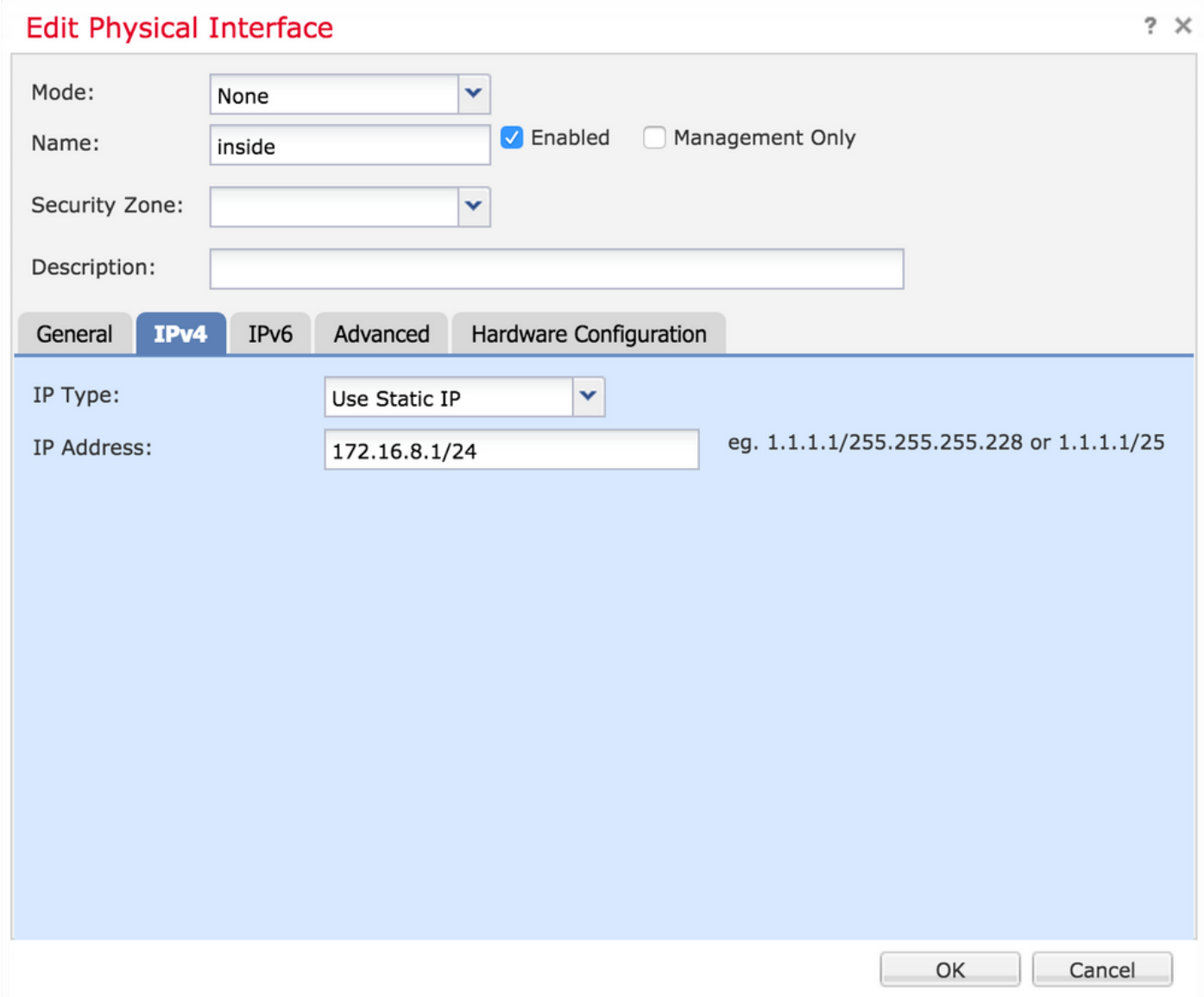
ステップ2：デバイスまたはFTD HAクラスタを選択します。

ステップ3:[Interfaces] タブに移動します。

ステップ4：図に示すように、**鉛筆アイコン**をクリックして、インターフェイスを設定/編集し、管理アクセスを取得します。



ステップ5:[enable] チェックボックスをオンにして、インターフェイスを有効にします。[Ipv4] タブに移動し、[IP Type]に[static]または[DHCP] を選択します。次の図に示すように、インターフェイスのIPアドレスを入力し、[OK] をクリックします。



ステップ6:[Save] をクリックし、ポリシーをFTDに展開します。

> **注**：ソフトウェアバージョン6.1.0のデバイスでは、診断インターフェイスを使用してSSH経由でConverged CLIにアクセスすることはできません

ステップ2：外部認証を設定します。

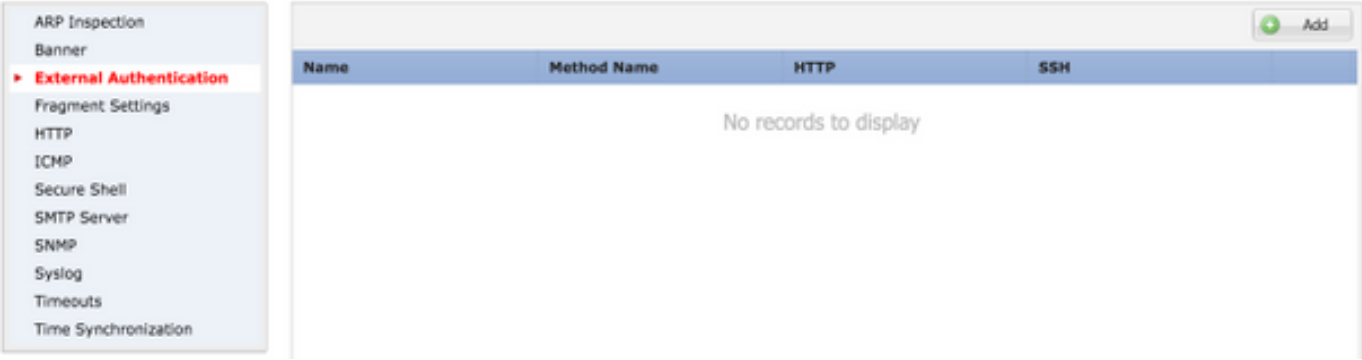
外部認証により、ユーザ認証のためにFTDをActive DirectoryまたはRADIUSサーバに統合することが容易になります。ローカルに設定されたユーザは診断CLIに直接アクセスできないため、これは必要な手順です。診断CLIおよびGUIには、Lightweight Directory Access Protocol(LDAP)またはRADIUSを介して認証されたユーザのみがアクセスします。

外部認証を設定するには6つの手順があります。

ステップ1：に移動します。 **[Devices] > [Platform Settings]**

ステップ2：鉛筆アイコンをクリックして存在するポリシーを編集するか、[New Policy] ボタンをクリックして[type as] を選択し、新しいFTDポリシーを作成します。 **脅威対策の設定。**

ステップ3：図に示すように、[External Authentication] タブに移動します。



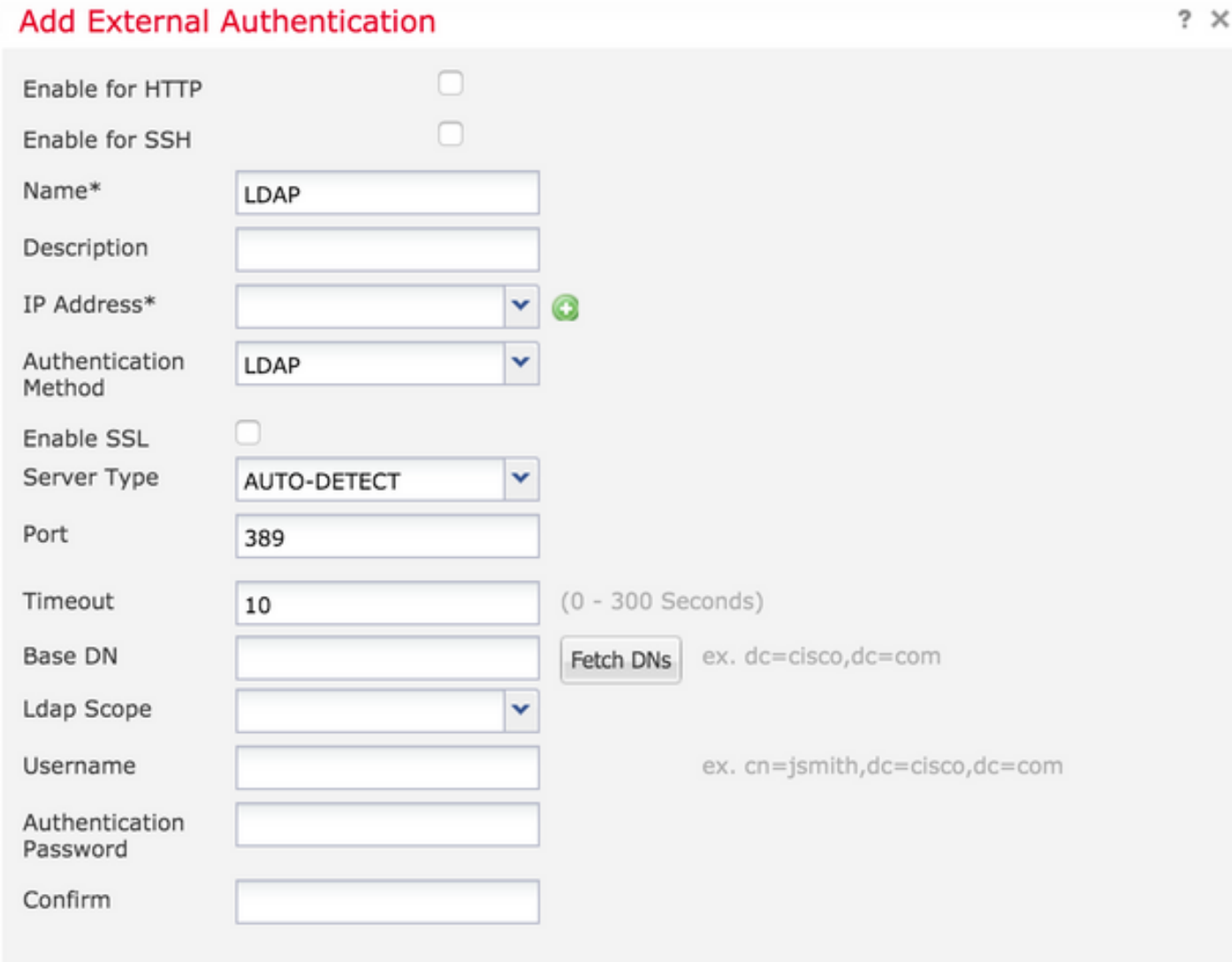
ステップ4:[Add] をクリックすると、次の図のようなダイアログボックスが表示されます。

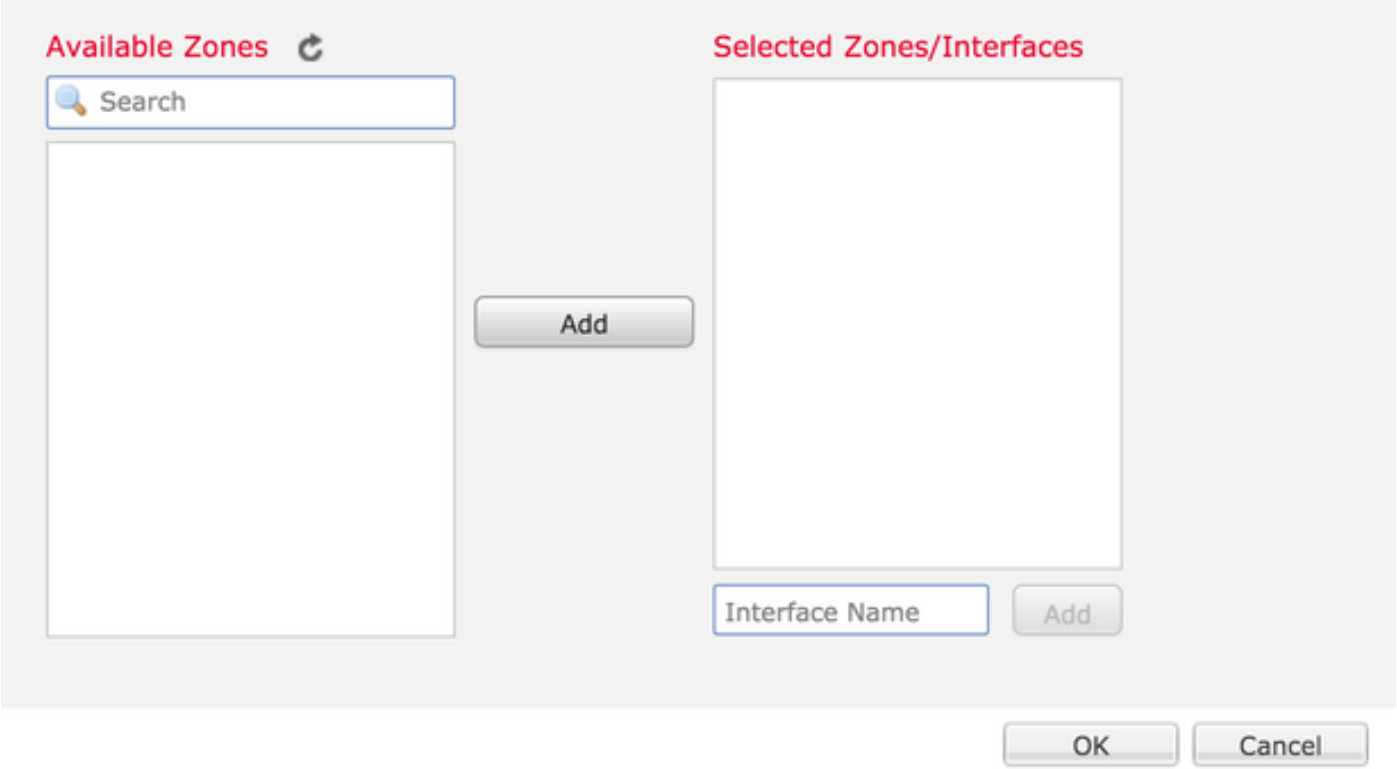
- **Enable for HTTP**:FTD over HTTPSへのアクセスを提供するには、このオプションを有効にします。
- **Enable for SSH**：このオプションを有効にすると、SSH経由でFTDにアクセスできます。
- **Name**:LDAP接続の名前を入力します。
- **Description**：外部認証オブジェクトの説明（オプション）を入力します。
- **IP address**：外部認証サーバのIPを保存するネットワークオブジェクトを入力します。設定されているネットワークオブジェクトがない場合は、新しいネットワークオブジェクトを作成します。**(+)**アイコンをクリックします。
- **Authentication Method**：認証にRADIUSまたはLDAPプロトコルを選択します。
- **Enable SSL**：認証トラフィックを暗号化するには、このオプションを有効にします。
- **Server Type**：サーバタイプを選択します。よく知られているサーバタイプは、MS Active Directory、Sun、OpenLDAP、およびNovellです。デフォルトでは、このオプションはサーバタイプを自動検出するように設定されています。
- **Port**：認証が実行されるポートを入力します。
- **Timeout**：認証要求のタイムアウト値を入力します。
- **Base DN**：ユーザが存在できる範囲を指定するベースDNを入力します。
- **LDAP Scope**：検索するLDAPスコープを選択します。スコープは同じレベル内にあるか、サブツリー内を参照します。
- **Username**:LDAPディレクトリにバインドするユーザ名を入力します。

- **Authentication password**：このユーザのパスワードを入力します。
- **Confirm**：パスワードを再入力します。
- **Available Interfaces**:FTDで使用可能なインターフェイスのリストが表示されます。
- **Selected zones and interfaces**：認証サーバへのアクセス元のインターフェイスのリストが表示されます。

RADIUS認証には、サーバタイプのベースDNまたはLDAPスコープはありません。ポートはRADIUSポート1645です。

Secret:RADIUSの秘密キーを入力します。





ステップ5：設定が完了したら、[OK]をクリック**します。**

ステップ6:ポリシーを保存し、Firepower Threat Defenseデバイスに展開します。

> **注**：ソフトウェアバージョン6.1.0のデバイスでは、外部認証を使用してSSH経由でConverged CLIにアクセスすることはできません

ステップ3:SSHアクセスを設定します。

SSHは、統合CLIへの直接アクセスを提供します。CLIに直接アクセスしてdebugコマンドを実行するには、このオプションを使用します。このセクションでは、FTD CLIにアクセスするためのSSHの設定方法について説明します。

> **注**：ソフトウェアバージョン6.0.1が稼働するFTDデバイスでは、プラットフォーム設定のSSH設定により、CLISHではなく診断CLIに直接アクセスできます。CLISHにアクセスするには、**br1**で設定されたIPアドレスに接続する必要があります。ただし、ソフトウェアバージョン6.1.0が稼働するFTDデバイスでは、SSH経由でアクセスすると、すべてのインターフェイスが統合CLIに移動します

ASAでSSHを設定するには6つの手順があります

6.0.1デバイスのみ：

これらの手順は、ソフトウェアバージョンが6.1.0未満および6.0.1より大きいFTDデバイスで実行されます。6.1.0デバイスでは、これらのパラメータはOSから継承されます。

ステップ1:[Devices] > [Platform Settings] に移動します。

ステップ2：鉛筆アイコンをクリックして存在するポリシーを編集するか、[New Policy] ボタンをクリックして[Threat Defense Settings] として[type] を選択し、新しいFirepower Threat Defenseポリシーを作成します。

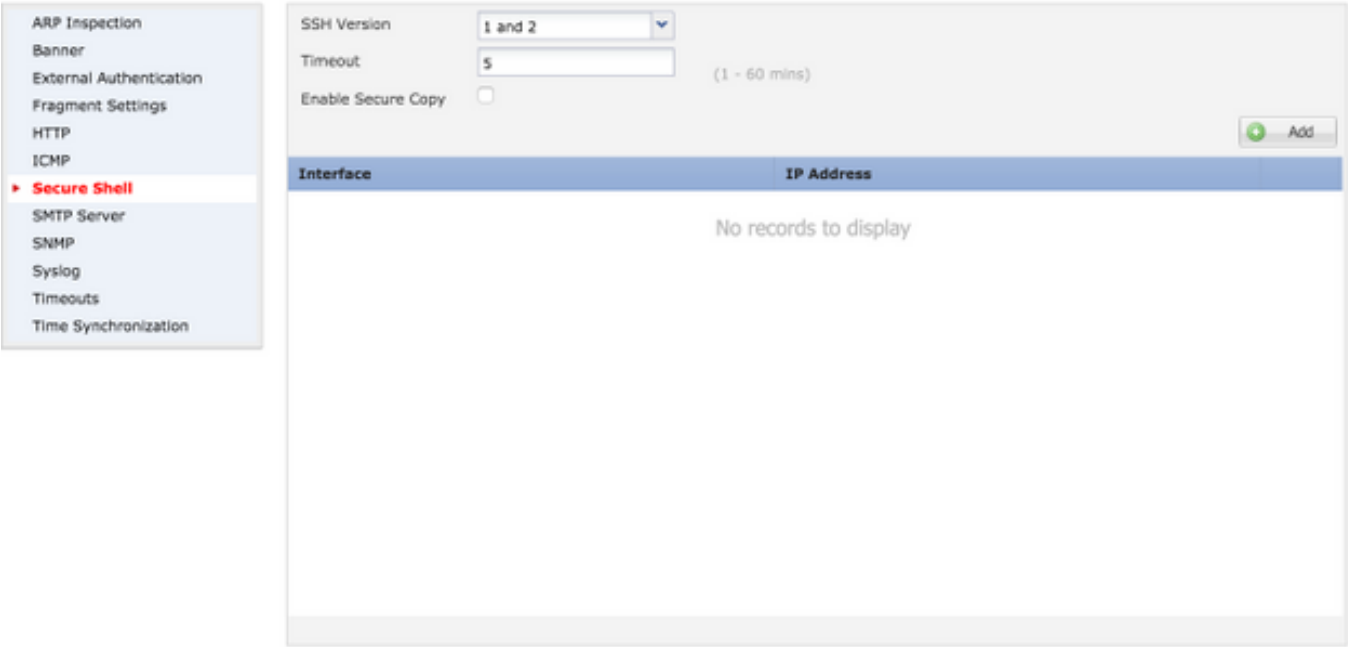
ステップ3:[Secure Shell] セクションに移動します。図に示すように、ページが表示されます。

SSHバージョン:ASAで有効にするSSHバージョンを選択します。次の3つのオプションがあります。

- **1**:SSHバージョン1のみを有効にする
- **2**:SSHバージョン2のみを有効にする
- **1 および 2**:SSHバージョン1と2の両方を有効にします

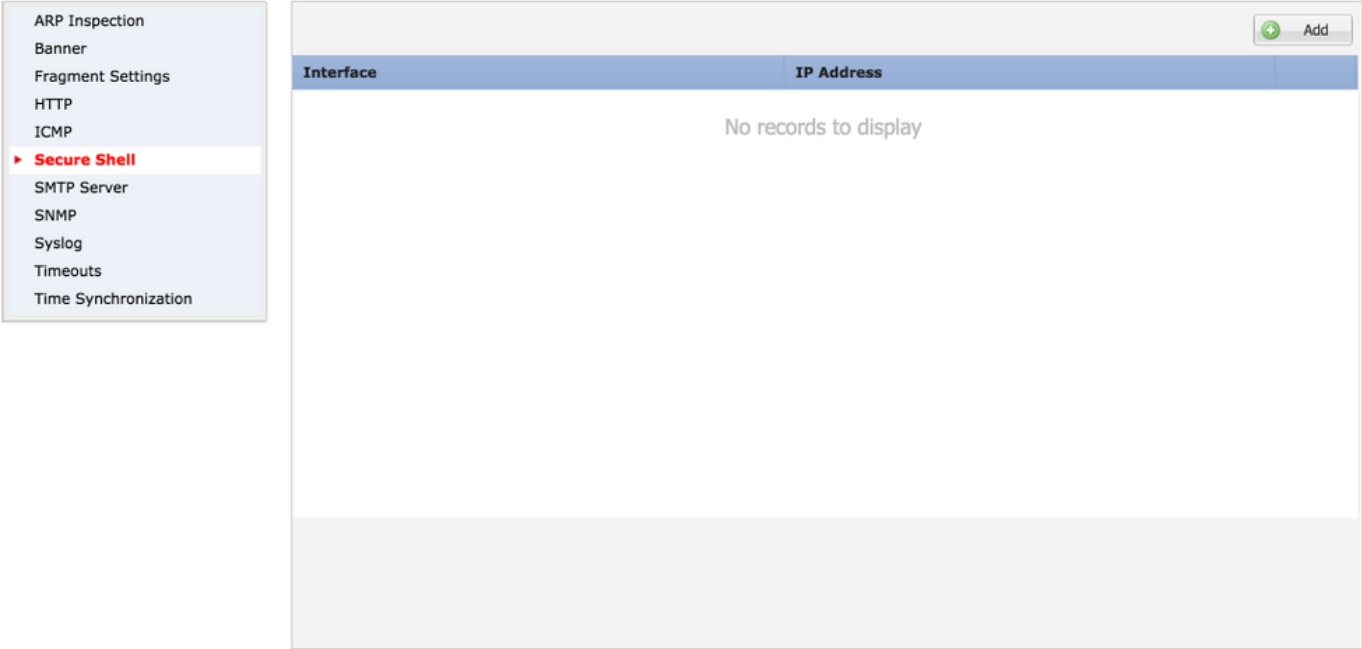
タイムアウト：必要なSSHタイムアウトを分単位で入力します。

Enable Secure Copy：デバイスがSecure Copy(SCP)接続を許可し、SCPサーバとして動作するように設定するには、このオプションを有効にします。



6.0.1および6.1.0デバイス：

これらの手順は、SSHを介した管理アクセスを特定のインターフェイスおよび特定のIPアドレスに制限するように設定されています。

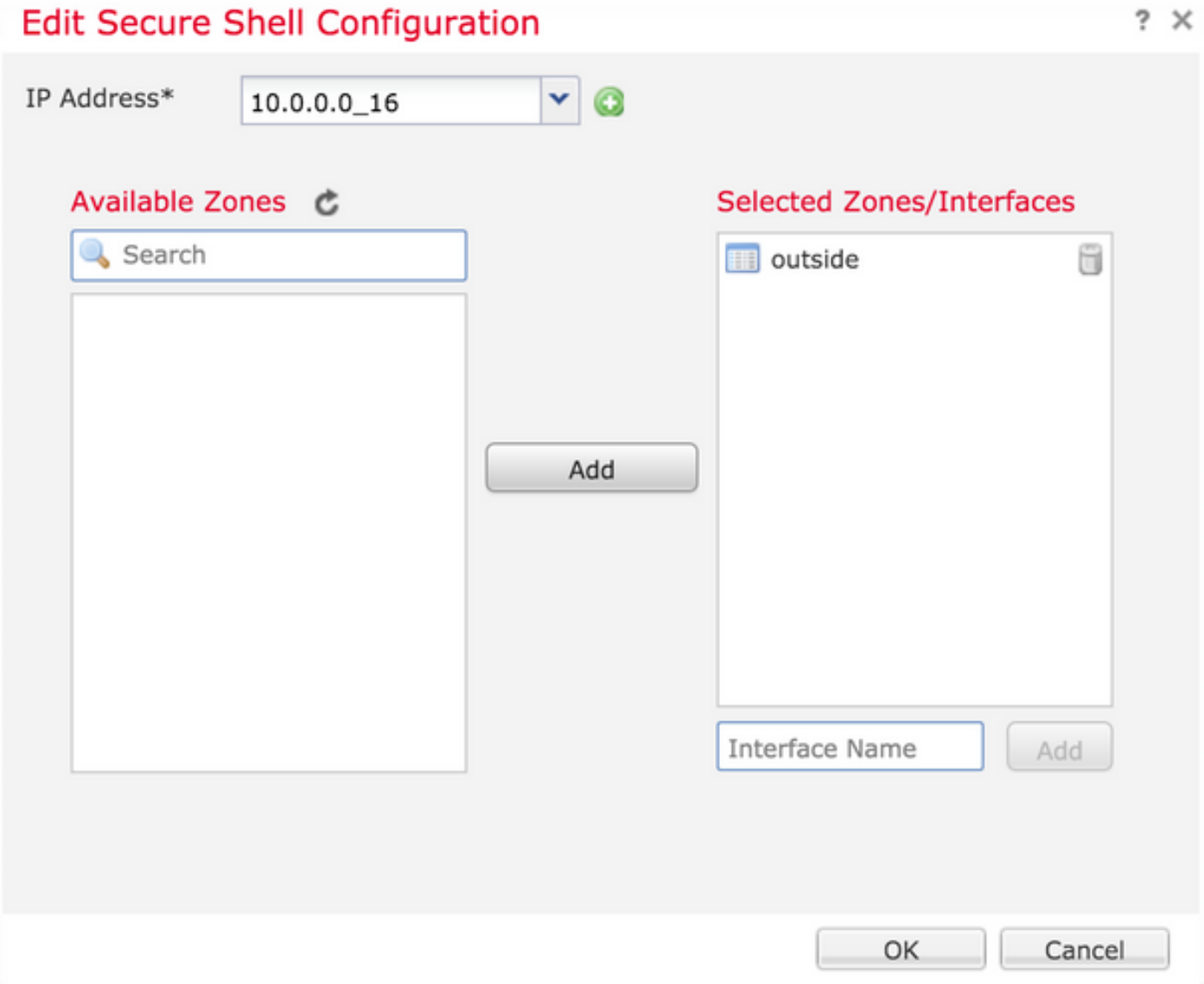


ステップ1:[Add] をクリックし、次のオプションを設定します。

IPアドレス:SSH経由でCLIにアクセスできるサブネットを含むネットワークオブジェクトを選択します。ネットワークオブジェクトがない場合は、**(+)**アイコンをクリックしてネットワークオブジェクトを作成します。

選択したゾーン/インターフェイス：SSHサーバにアクセスするゾーンまたはインターフェイスを選択します。

ステップ2：図に示すように、[OK] をクリックします。



SSHの設定は、このコマンドを使用して統合CLI（6.0.1デバイスのASA Diagnostic CLI）で表示されます。

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

ステップ3:SSH設定が完了したら、[Save] をクリックし、ポリシーをFTDに展開します。

ステップ4:HTTPSアクセスを設定します。

1つ以上のインターフェイスへのHTTPSアクセスを有効にするには、プラットフォーム設定の [HTTP] セクションに移動します。HTTPSアクセスは、分析のために診断セキュアWebインターフェイスからパケットキャプチャを直接ダウンロードするのに特に便利です。

HTTPSアクセスを設定するには6つの手順があります。

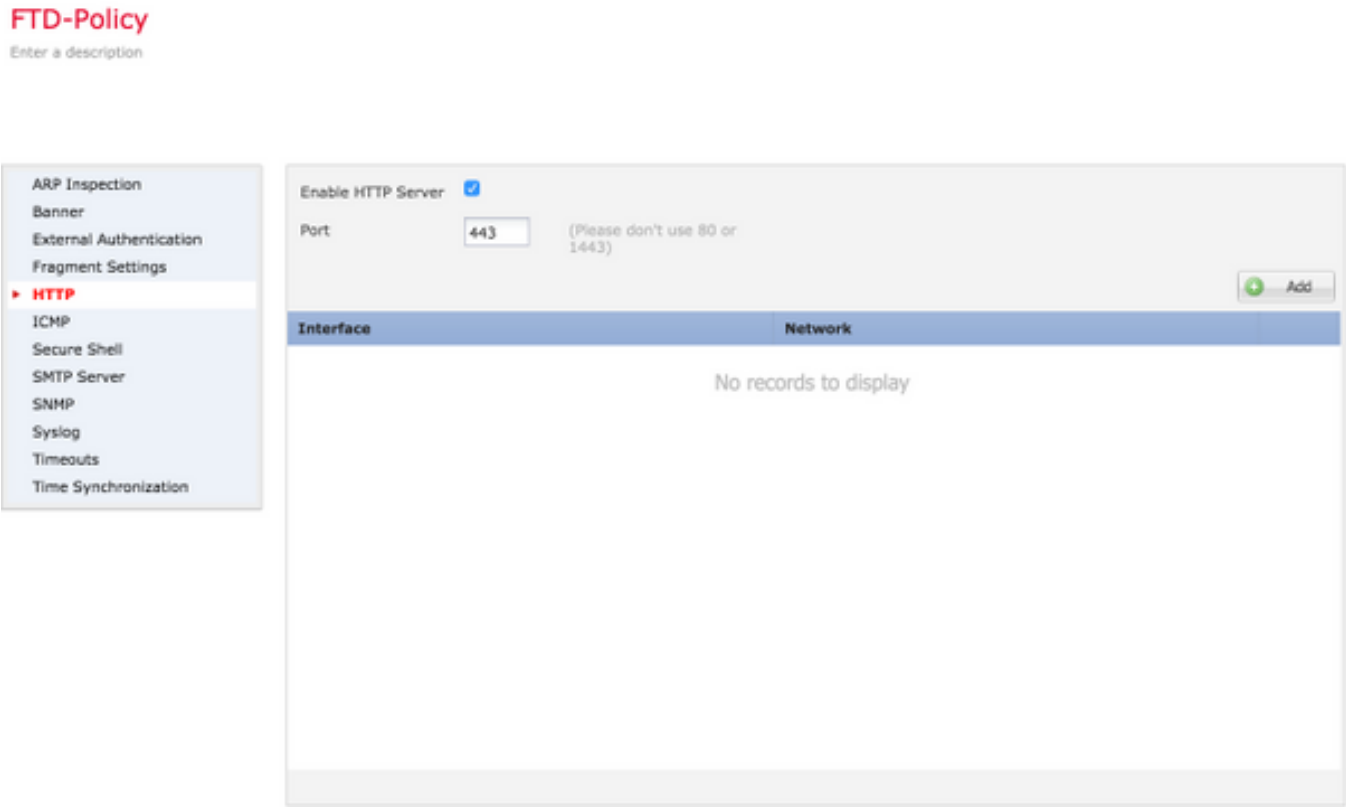
ステップ1:[Devices] > [Platform Settings] に移動します。

ステップ2:ポリシーの横にある**鉛筆アイコン**をクリックして存在するプラットフォーム設定ポリシーを編集するか、または**New Policy**をクリックして新しいFTDポリシーを作成します。[Firepower Threat Defense] タイプを選択します。

ステップ3:[HTTP] セクションに移動すると、次の図のようなページが表示されます。

HTTPサーバを有効にします。FTDでHTTPサーバを有効にするには、このオプションを有効にします。

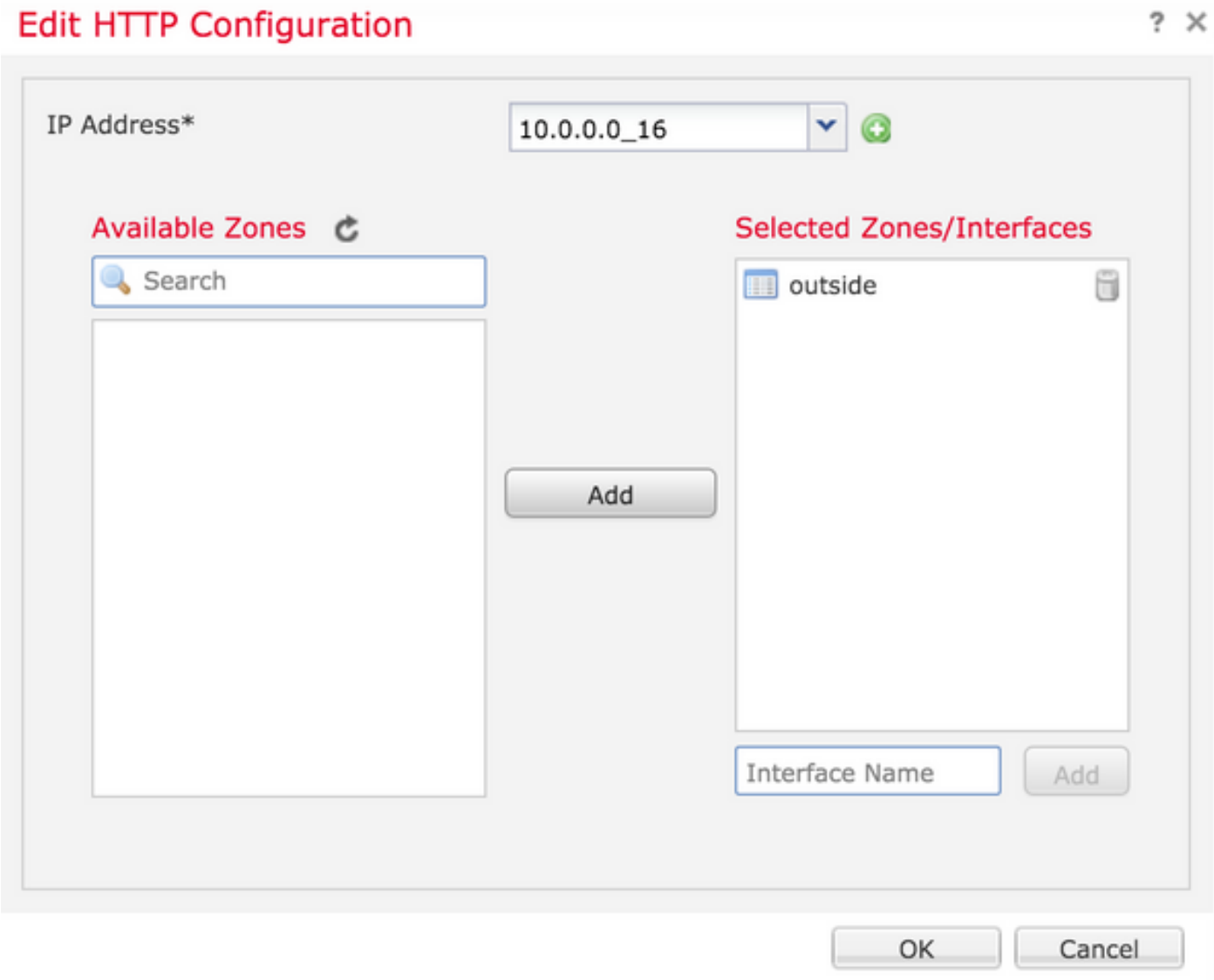
[ポート(Port)]:FTDが管理接続を受け入れるポートを選択します。



ステップ4:[Add] をクリックすると、図のようにページが表示されます。

IPアドレス：診断インターフェイスへのHTTPSアクセスを許可するサブネットを入力します。ネットワークオブジェクトがない場合は、ネットワークオブジェクトを作成し、**(+)**オプションを使用します。

選択されたゾーン/インターフェイス:SSHと同様に、HTTPS設定には、HTTPS経由でアクセスできるインターフェイスが設定されている必要があります。FTDにHTTPS経由でアクセスするゾーンまたはインターフェイスを選択します。



HTTPSの設定は、統合CLI（6.0.1デバイスのASA Diagnostic CLI）で表示され、このコマンドを使用します。

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

ステップ5：必要な設定が完了したら、[OK] を選択します。

ステップ6：必要な情報をすべて入力したら、[Save] をクリックし、ポリシーをデバイスに展開します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

FTDの管理アクセスの問題をトラブルシューティングするための基本的な手順は次のとおりです

。

ステップ1：インターフェイスが有効になっており、IPアドレスが設定されていることを確認します。

ステップ2：外部認証が設定どおりに動作し、**プラットフォーム設定**の「**外部認証**」セクションで指定された適切なインターフェイスから外部認証に到達できることを確認します。

ステップ3:FTDのルーティングが正確であることを確認します。FTDソフトウェアバージョン6.0.1で、**system support diagnostic-cli**に移動します。**show route**コマンドと**show route management-only**コマンドを実行して、FTDと管理インターフェイスのルートをそれぞれ表示します。

FTDソフトウェアバージョン6.1.0では、コンバージドCLIでコマンドを直接実行します。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems