

FMC による FTD への管理アクセスの設定 (HTTPS および SSH)

目次

[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](#)

[設定 管理アクセス](#)

[ステップ 1. FMC GUI による FTD インターフェイスの設定 IP。](#)

[ステップ 2. 設定 外部認証。](#)

[ステップ 3. 設定 SSH アクセス。](#)

[ステップ 4. 設定 HTTPS アクセス。](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料は Firepower Threat Defense (FTD) (HTTPS および SSH) に Firesight 管理センター (FMC) によって管理アクセスの設定を説明したものです。

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 テクノロジーのナレッジ
- ASA の基本的な知識 (適応型セキュリティ アプライアンス (ASA) ソフトウェア)
- HTTPS および SSH (セキュアシェル) による ASA の管理アクセスのナレッジ

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くものです。

- 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) ソフトウェア バージョン 6.0.1 で以上に動作する ASA (5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X) のた

めの Firepower Threat Defense イメージ、

- ソフトウェア バージョン 6.0.1 で以上に動作する ASA (5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X) のための ASA Firepower Threat Defense イメージ、
- Firepower Management Center (FMC) バージョン 6.0.1 および それ 以上

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。


背景説明

Firepower Threat Defense (FTD) の手始めによって、全体の ASA 関連するコンフィギュレーションは GUI で行われます。

ソフトウェア バージョン 6.0.1 を実行する FTD デバイスで **システム 支援診断 cli** を入力すると同時に ASA 診断 CLI はアクセスされます。ただし、ソフトウェア バージョン 6.1.0 を実行する FTD デバイスで CLI はコンバージし、全体の ASA コマンドは CLISH で設定されます。

```
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管理アクセスを直接得るために、HTTPS か SSH によって管理アクセスを設定して下さい。この資料が SSH または HTTPS 上の管理アクセスを外部に得るために必要な必要な設定を提供したものです。

注: ソフトウェア バージョン 6.0.1 を実行するユーザを認証するために FTD デバイスで CLI はローカルユーザによって外部認証設定する必要がありますアクセスすることができません。ただし、ソフトウェア バージョン 6.1.0 を実行する FTD デバイスで CLI はローカル**管理者ユーザ**によって外部認証が他のすべてのユーザ向けに必要となる間、アクセスされます

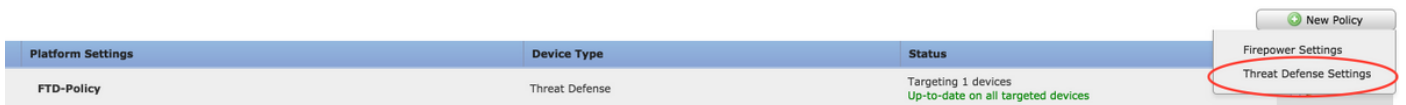
注: ソフトウェア バージョン 6.0.1 を実行する FTD デバイスで診断 CLI は FTD の br1 のために設定される IP に直接アクセスできません。ただし、ソフトウェア バージョン 6.1.0 を実行する FTD デバイスでコンバージした CLI は管理アクセスのために設定されるあらゆるインターフェイスにアクセス可能ですが、インターフェイスは IP アドレスで設定する必要があります。

設定

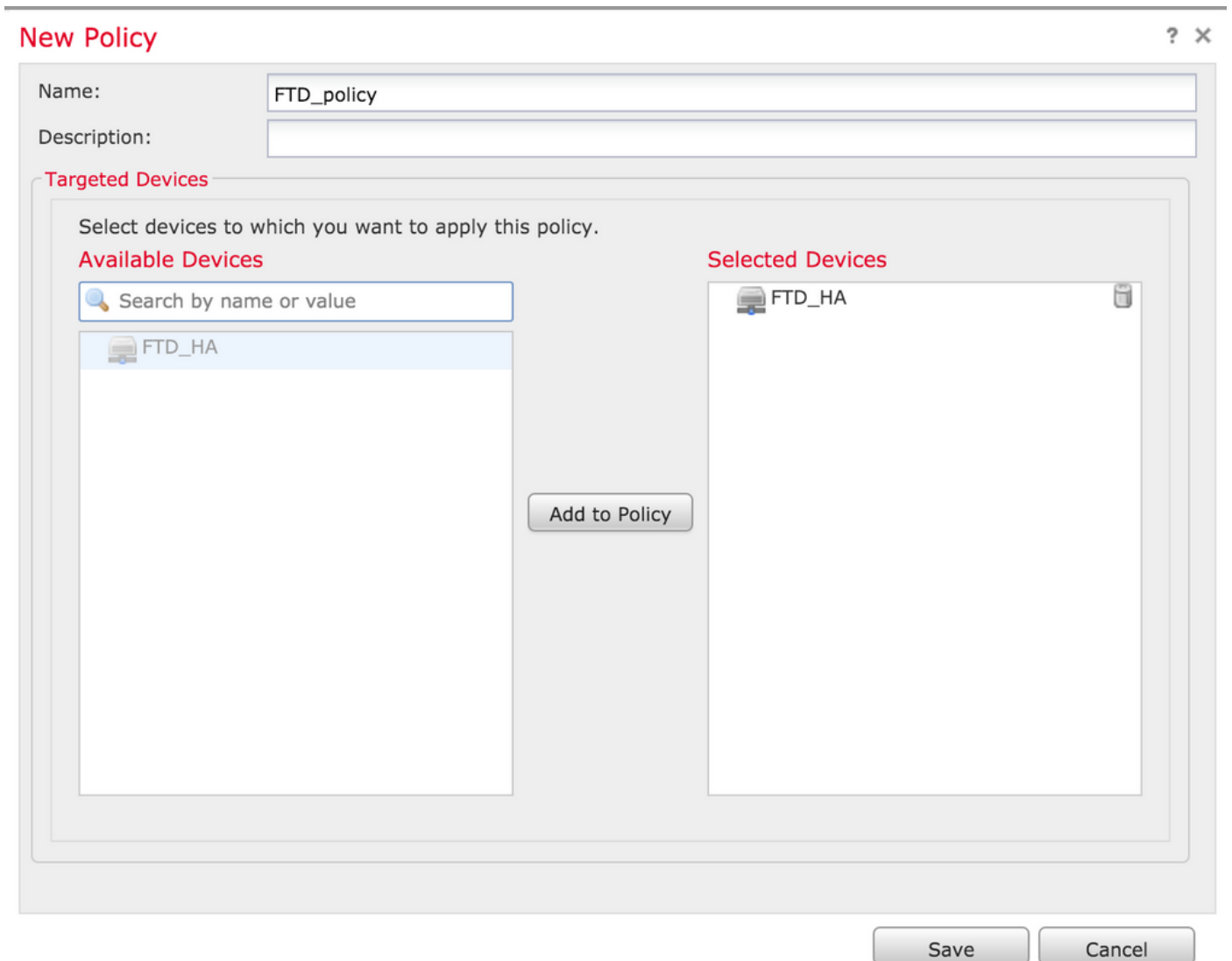
すべての管理アクセス 関連するコンフィギュレーションはイメージに示すようにあなたでデバイスのプラットフォーム Settings タブへのナビゲート、設定されます:



どちらかは **New Policy** ボタンをクリックし、脅威防衛設定として『Type』を選択すると同時に鉛筆アイコンをクリックするか、または新しい FTD ポリシーを作成すると同時にポリシーを編集し、イメージに示すように存在します:



このポリシーを適用し、イメージに示すように、『SAVE』をクリックするために FTD アプリアンスを選択して下さい:



管理アクセスを設定して下さい

これらは管理アクセスを設定するために踏まれる 4 つの主要なステップです。

ステップ 1. FMC GUI による FTD インターフェイスの設定 IP。

FTD が SSH か HTTPS によってアクセス可能であるインターフェイスの IP を設定して下さい。FTD の **Interfaces** タブにナビゲートすると同時にあるインターフェイスを編集して下さい。

注: ソフトウェア バージョン 6.0.1 を実行する FTD デバイスで FTD のデフォルトの マネージメント 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 を実行する FTD デバイスですべてのインターフェイスは診断インターフェイスを除く管理アクセスをサポートします。

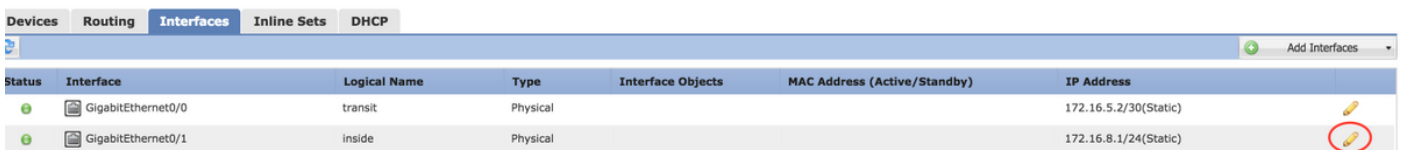
診断インターフェイスを設定する 6 つのステップがあります。



ステップ 1. デバイス > デバイス管理へのナビゲート。

ステップ 2. デバイスが FTD HA クラスタを選択して下さい。

ステップ 3. **Interfaces** タブへのナビゲート。

ステップ 4. 設定するために鉛筆アイコンをクリックして下さい/イメージに示すように管理アクセスを、得るためにインターフェイスを編集して下さい:



| Status | Interface | Logical Name | Type | Interface Objects | MAC Address (Active/Standby) | IP Address | |
|--------|--------------------|--------------|----------|-------------------|------------------------------|-----------------------|---|
| ● | GigabitEthernet0/0 | transit | Physical | | | 172.16.5.2/30(Static) |  |
| ● | GigabitEthernet0/1 | inside | Physical | | | 172.16.8.1/24(Static) |  |

ステップ 5. インターフェイスをイネーブルに設定するために **Enable** チェックボックスを選択して下さい。Ipv4 タブにナビゲートして下さい、**スタティック**か **DHCP** として IP 型を選択して下さい。この場合インターフェイスのための IP アドレスを入力し、イメージに示すように、『OK』をクリックして下さい:

Edit Physical Interface



Mode: ▾

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▾

IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

OK Cancel

ステップ 6. FTD にポリシーを『SAVE』をクリックし、次に展開して下さい。

注: 診断インターフェイスがソフトウェア バージョン 6.1.0 が付いているデバイスの SSH 上のコンバージした CLI にアクセスするのに使用することができません

ステップ 2.設定 外部認証。

外部認証はユーザ認証のためのアクティブ ディレクトリか RADIUSサーバに FTD の統合を促進します。これはローカルで設定されたユーザに診断 CLI にダイレクトアクセスがないので必要なステップです。診断 CLI および GUI は Lightweight Directory Access Protocol (LDAP) が RADIUS によって認証されるユーザによってだけアクセスされます。

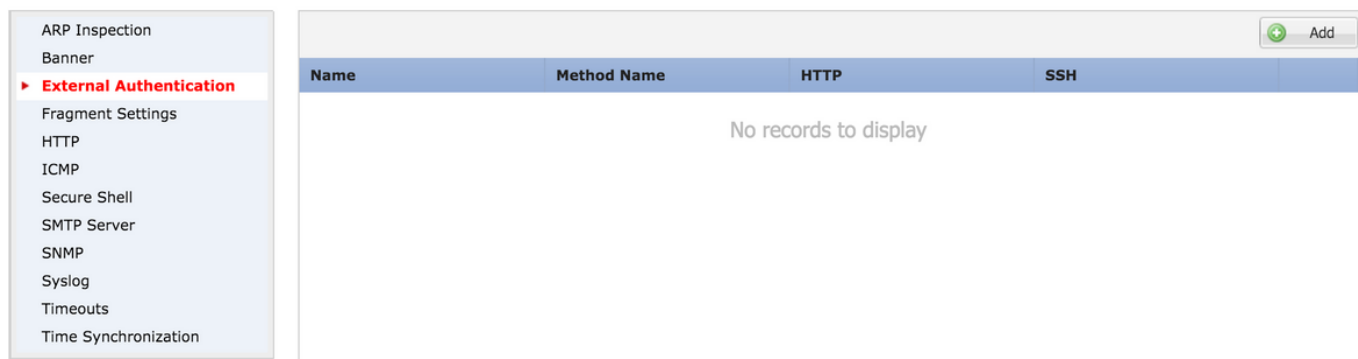
外部認証を設定する 6 つのステップがあります。

ステップ 1.デバイス > プラットフォーム設定へのナビゲート。

呼び出します。どちらかは **New Policy** ボタンをクリックし、**脅威防衛設定**として『Type』を選択すると同時に鉛筆アイコンをクリックするか、または新しい FTD ポリシーを作成すると同時

に存在 します ポリシーを編集しま。

ステップ 3.イメージに示すように外部認証タブに、ナビゲート して下さい:



ステップ 4 『Add』 をクリック すると同時に、ダイアログボックスはイメージに示すように現わ
れます:

- **HTTP のためのイネーブル**はアクセスを提供するこのオプションを HTTPS 上の FTD 有効に
します。
- **SSH-のためのイネーブル**はアクセスを提供するこのオプションを SSH 上の FTD 有効にし
ます。
- **名前**は LDAP 接続の名前を入力します。
- **記述**は外部認証 オブジェクトのためのオプション の 記述を入力します。
- **IP アドレス**は外部認証サーバの IP を保存するネットワーク オブジェクトを入力します。 あ
ればネットワーク オブジェクトはのクリックによって作成します新しいものを (+) アイコ
ン設定されません。
- **認証方式**選り抜き RADIUS か認証のための LDAPプロトコル。
- **SSL イネーブル**を認証 トラフィックを暗号化するこのオプション 有効に して下さい。
- **サーバ タイプ**はサーバタイプを選択します。 よく知られている な サーバタイプは MS アク
ティブ ディレクトリ、Sun、OpenLDAP および Novell です。 デフォルトで、オプションは
サーバタイプを自動検出する設定されます。
- **ポート**は認証が起こるポートを入力します。
- **タイムアウト**は認証要求のタイムアウト値を入力します。
- **基礎 DN** はユーザがいるはずであるスコープを提供するためにベース DN を入力します。
- **LDAP スコープ**は LDAP スコープを検知 するために選択します。 スコープは同じレベルの内
にまたはサブツリーの内で検知 するためにあります。

- **ユーザ名**は LDAP ディレクトリに結合 するためにユーザ名を入力します。
- **認証**はこのユーザ向けのパスワードにパスワード入ります。
- もう一度入力しますパスワードを**確認**して下さい。
- **利用可能** FTD の利用可能 な インターフェイスの A リストを表示する**インターフェイス**させます。
- **指定ゾーン**はこれを表示します認証サーバがアクセスされるインターフェイスのリストを**インターフェイス**させ。

RADIUS認証に関しては、サーバタイプ ベース DN または LDAP スコープがありません。ポートは RADIUSポート 1645 です。

秘密は RADIUS のための秘密鍵を入力します。

Add External Authentication



| | | |
|-------------------------|--|--|
| Enable for HTTP | <input type="checkbox"/> | |
| Enable for SSH | <input type="checkbox"/> | |
| Name* | <input type="text" value="LDAP"/> | |
| Description | <input type="text"/> | |
| IP Address* | <input type="text"/> <input type="button" value="v"/> <input type="button" value="+"/> | |
| Authentication Method | <input type="text" value="LDAP"/> <input type="button" value="v"/> | |
| Enable SSL | <input type="checkbox"/> | |
| Server Type | <input type="text" value="AUTO-DETECT"/> <input type="button" value="v"/> | |
| Port | <input type="text" value="389"/> | |
| Timeout | <input type="text" value="10"/> (0 - 300 Seconds) | |
| Base DN | <input type="text"/> <input type="button" value="Fetch DNs"/> ex. dc=cisco,dc=com | |
| Ldap Scope | <input type="text"/> <input type="button" value="v"/> | |
| Username | <input type="text"/> ex. cn=jsmith,dc=cisco,dc=com | |
| Authentication Password | <input type="text"/> | |
| Confirm | <input type="text"/> | |

The screenshot shows a configuration window with two main panels. The left panel, titled 'Available Zones', contains a search bar with a magnifying glass icon and the word 'Search' inside. Below the search bar is a large empty rectangular area. The right panel, titled 'Selected Zones/Interfaces', also contains a large empty rectangular area. Between the two panels is a button labeled 'Add'. Below the right panel is an input field labeled 'Interface Name' and another button labeled 'Add'. At the bottom right of the window are two buttons labeled 'OK' and 'Cancel'.

ステップ 5 設定がされたら、『OK』をクリックして下さい。

ステップ 6.ポリシーを保存し、Firepower Threat Defense デバイスにそれを展開して下さい。

注: 外部認証がソフトウェアバージョン 6.1.0 が付いているデバイスの SSH 上のコンバージした CLI にアクセスするのに使用することができません

ステップ 3.設定 SSH アクセス。

SSH はコンバージした CLI にダイレクトアクセスを提供します。直接 CLI にアクセスし、debug コマンドを実行するこのオプションを使用して下さい。このセクションは FTD CLI にアクセスするために SSH を設定する方法を記述します。

注: ソフトウェアバージョン 6.0.1 を実行する FTD デバイスでプラットフォーム設定の SSH 設定は診断 CLI にアクセスを CLISH を直接およびない提供しません。CLISH にアクセスするために br1 で設定される 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 を実行する FTD デバイスですべてのインターフェイスはコンバージした CLI に SSH にアクセスされたときナビゲートします

ASA の SSH を設定する 6 つのステップがあります

6.0.1 デバイスだけ:

これらのステップはソフトウェアバージョンが付いている FTD デバイスでより少しより 6.1.0 および非常により 6.0.1 実行されます。6.1.0 デバイスでこれらのパラメータは OS から受継がれます。

ステップ 1. Devices>Platform 設定へのナビゲート。

呼び出します。どちらかは **New Policy** ボタンをクリックし、**脅威防衛設定**として『Type』を選択すると同時に鉛筆アイコンをクリックするか、または Firepower Threat Defense 新しいポリシーを作成すると同時に存在します ポリシーを編集しま。

ステップ 3. **セキュアシェル** セクションへのナビゲート。ページはイメージに示すように、提示されます:

SSH バージョン: ASA で有効になるために SSH バージョンを選択して下さい。3つのオプションがあります:

- 1: イネーブル SSH バージョン 1 だけ
- 2: イネーブル SSH バージョン 2 だけ
- 1 および 2: 両方 SSH バージョン 1 および 2 を有効にして下さい

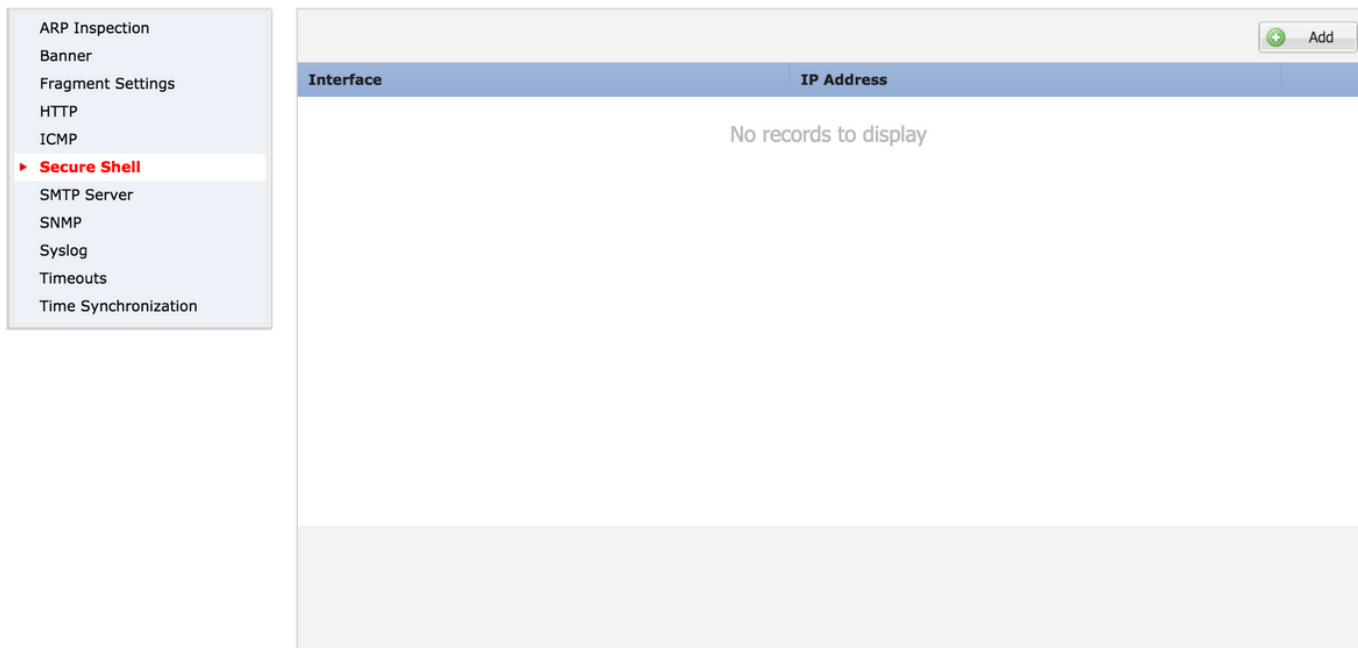
タイムアウト: 分に望ましい SSH タイムアウトを入力して下さい。

セキュアコピーを有効に します デバイスを Copy (SCP) セキュア接続を許可し、SCP サーバとして機能するために設定するこのオプションを有効に して下さい。

The screenshot shows the configuration page for Secure Shell. On the left is a navigation menu with the following items: ARP Inspection, Banner, External Authentication, Fragment Settings, HTTP, ICMP, **Secure Shell** (highlighted), SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main configuration area includes: SSH Version (dropdown menu set to '1 and 2'), Timeout (input field with '5' and '(1 - 60 mins)' label), and Enable Secure Copy (checkbox). Below the configuration fields is a table with two columns: 'Interface' and 'IP Address'. The table is currently empty, displaying 'No records to display'. An 'Add' button is located in the top right corner of the table area.

6.0.1 および 6.1.0 デバイス:

これらのステップは特定のインターフェイスと特定の IP アドレスに SSH によって管理アクセスを制限するために設定されます。



ステップ 1.これらのオプションを『Add』をクリックし、設定して下さい:

IPアドレス SSH 上の CLI にアクセスすることができるサブネットが含まれているネットワークオブジェクトを選択して下さい。ネットワークオブジェクトがない場合、(+) アイコンをクリックするように 1 つを作成して下さい。

指定ゾーン/インターフェイス: SSH サーバがアクセスされるインターフェイスかゾーンを選択して下さい。

ステップ 2.イメージに示すように、『OK』をクリックして下さい:

Edit Secure Shell Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

outside

SSH のための設定はコンバートした CLI (6.0.1 デバイスの ASA 診断 CLI) でこのコマンドを使用して表示されます。

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

ステップ 3 SSH 設定がされたら、FTD にポリシーを『SAVE』をクリックし、次に展開して下さい。

ステップ 4.設定 HTTPS アクセス。

HTTPS アクセスを、ナビゲート プラットフォーム設定の HTTP セクションに 1つ以上のインターフェイスにイネーブルにするため。HTTPS アクセスは分析のための診断セキュア 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してとりわけ役立ちます。

HTTPS アクセスを設定する 6 つのステップがあります。

ステップ 1.デバイス > プラットフォーム設定へのナビゲート

呼び出します。どちらかは『New Policy』をクリックすると同時にポリシーの側の鉛筆アイコンをクリックするか、または新しい FTD ポリシーを作成するので存在しますプラットフォーム設定ポリシーを編集しま。Firepower Threat Defense として型を選択して下さい。

ステップ 3 HTTP セクションにナビゲートすると同時に、ページはイメージに示すように提示されます。

イネーブル HTTPサーバ: FTD の HTTPサーバを有効にするために作るこのオプションを有効にしてください。

Port : FTD が管理接続を許可するポートを選択してください。

FTD-Policy

Enter a description

ARP Inspection
Banner
External Authentication
Fragment Settings
HTTP
ICMP
Secure Shell
SMTP Server
SNMP
Syslog
Timeouts
Time Synchronization

Enable HTTP Server

Port (Please don't use 80 or 1443)

| Interface | Network |
|-----------------------|---------|
| No records to display | |

ステップ 4.Click は追加し、apage はイメージに示すように現われます:

IP アドレスは診断インターフェイスに HTTPS アクセスがあることができ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を使用して 1 つを (+) オプション作成してください。

設定されるインターフェイスがある HTTPS によってアクセス可能であるかどれに SSH と同じような**指定ゾーン/インターフェイス**は HTTPS 設定必要があります。 FTD が HTTPS によってアクセスされるインターフェイスかゾーンを選択してください。

Edit HTTP Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

HTTPS のための設定はコンバージした CLI (6.0.1 デバイスの ASA 診断 CLI) でこのコマンドを使用して表示されます。

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

ステップ 5 必要な設定がされたら『OK』を選択して下さい。

ステップ 6 すべての必要情報が入力されたらデバイスにポリシーを『SAVE』をクリックし、次に展開して下さい。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

これらは FTD の管理アクセス問題を解決するための基本的な手順です。

ステップ 1: インターフェイスが IP アドレスで有効になり、設定されるようにして下さい。

呼び出します。外部認証が設定されるようにはたらき、適切なインターフェイスからの到達可能性 **プラットフォーム設定の外部認証** セクションで規定されてようにして下さい。

ステップ 3 FTD のルーティングをです正確確認して下さい。FTD ソフトウェア バージョン 6.0.1 では、**システム 支援診断 cli** にナビゲートして下さい。管理だけそれぞれ FTD およびマネージメントインターフェイスについてはルーティングを見るためにコマンド **show route** および **show route** を実行して下さい。

FTD ソフトウェア バージョン 6.1.0 では、コンバージした CLI のコマンドを直接実行して下さい。

関連情報

- [ASA 向け Cisco Firepower Threat Defense クイック スタート ガイド](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)