

通过FMC配置对FTD (HTTPS和SSH) 的管理访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[配置管理访问](#)

[步骤1.通过FMC GUI在FTD接口上配置IP。](#)

[步骤2.配置外部身份验证。](#)

[步骤3.配置SSH访问。](#)

[步骤4.配置HTTPS访问。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何通过Firesight管理中心(FMC)配置对Firepower威胁防御(FTD) (HTTPS和SSH) 的管理访问。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识
- ASA (自适应安全设备) 的基本知识
- 通过HTTPS和SSH (安全外壳) 在ASA上管理访问的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 适用于ASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)的自适应安全设备 (ASA)Firepower威胁防御映像，运行于软件版本6.0.1更高。

- 适用于ASA(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)的ASA Firepower威胁防御映像，运行于软件版本6.0.1及更高版本。
- Firepower管理中心(FMC)6.0.1版及更高版本。


本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

随着Firepower威胁防御(FTD)的启动，整个ASA相关配置将在GUI上完成。

在运行软件版本6.0.1的FTD设备上，当您输入系统支持diagnostic-cli时，将访问**ASA诊断CLI**。但是，在运行软件版本6.1.0的FTD设备上,CLI已收敛，并且整个ASA命令都在CLISH上配置。

```
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
```

要直接从外部网络获得管理访问，必须通过HTTPS或SSH配置管理访问。本文档提供了通过SSH或HTTPS从外部获得管理访问所需的必要配置。

注意：在运行软件版本6.0.1的FTD设备上，本地用户无法访问CLI，必须配置外部身份验证才能对用户进行身份验证。但是，在运行软件版本6.1.0的FTD设备上，本地管理员用户访问CLI，而所有其他用户都需要外部身份验证。

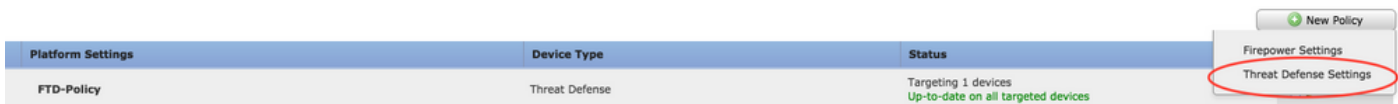
注意：在运行软件版本6.0.1的FTD设备上，不能通过为FTD的br1配置的IP直接访问诊断CLI。但是，在运行软件版本6.1.0的FTD设备上，可以通过为管理访问配置的任何接口访问融合CLI，但必须为接口配置IP地址。

配置

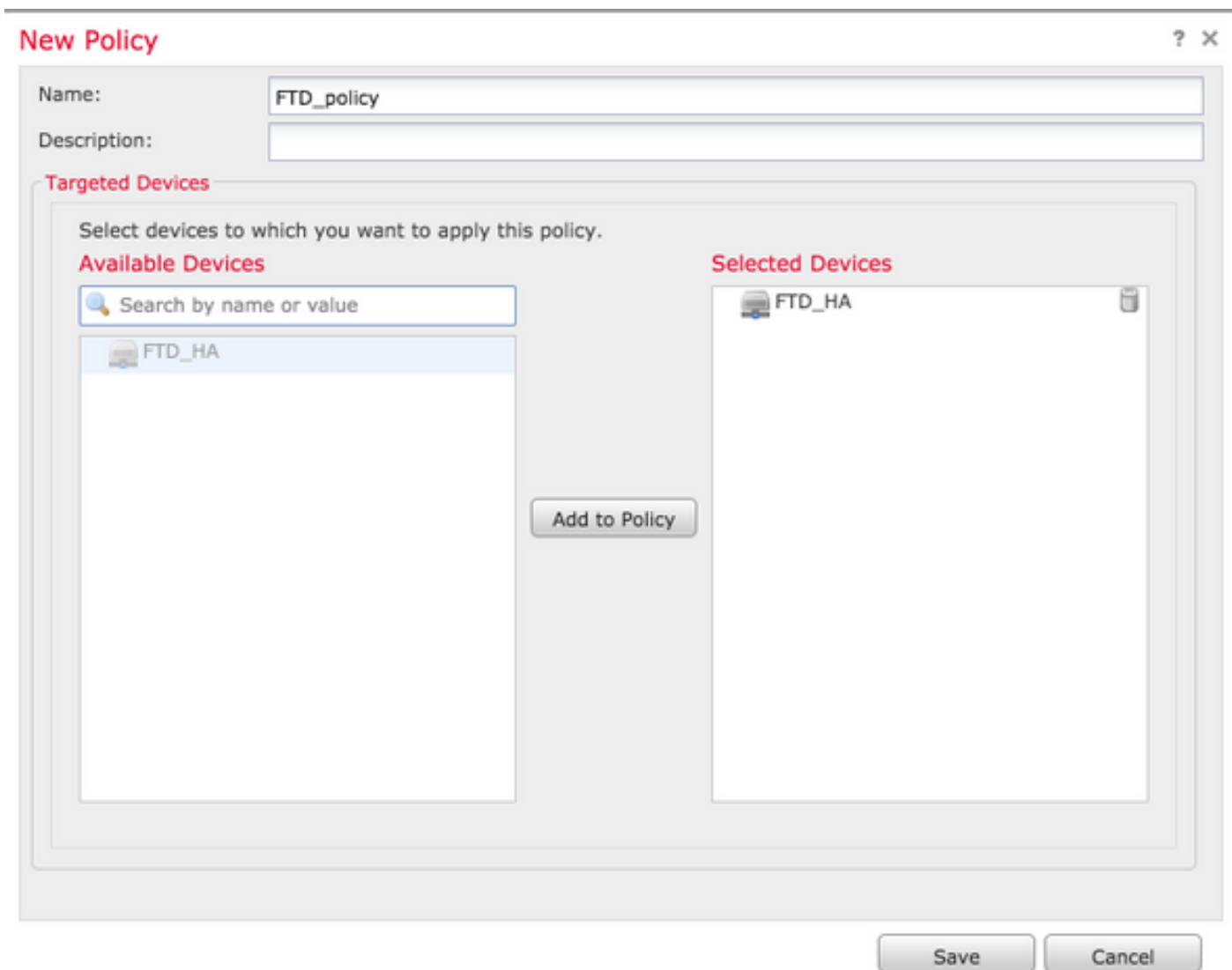
当您导航至“设备”中的“平台设置”选项卡时，将配置所有与管理访问相关的配置，如图所示：



编辑点击铅笔图标时存在的策略，或者在点击“新建策略”按钮时创建新的FTD策略，并选择“威胁防御设置”类型，如图所示：



选择要应用此策略的FTD设备，然后单击**Save**，如图所示：



配置管理访问

以下是配置管理访问所采取的四个主要步骤。

步骤1.通过FMC GUI在FTD接口上配置IP。

在可通过SSH或HTTPS访问FTD的接口上配置IP。在导航至FTD的Interfaces选项卡时编辑**存在**的接口。

注意：在运行软件版本6.0.1的FTD设备上，FTD上的默认管理接口是diagnostic0/0接口。但是，在运行软件版本6.1.0的FTD设备上，除诊断接口外，所有接口都支持管理访问。

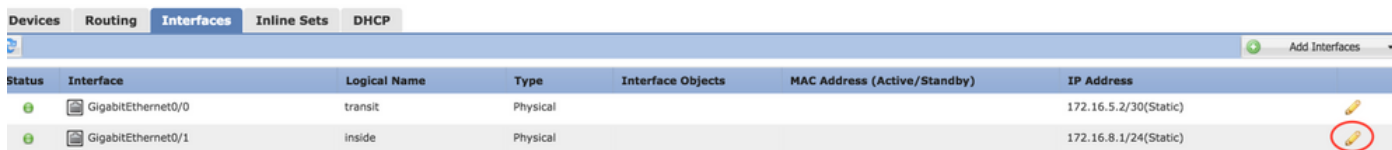
配置诊断接口有六个步骤。

步骤1.导航至 **设备>设备管理**。

步骤2.选择设备或FTD HA集群。

步骤3.导航至“**接口**”选项卡。

步骤4.单击铅笔**图标**配置/编辑接口以获得管理访问权限，如图所示：



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)	

步骤5.选中启用复**选框**以启用接口。导航至“**Ipv4**”选项卡，选择IP Type(IP类型)为**静态或DHCP**。现在，输入接口的IP地址，然后单击**OK**，如图所示：

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

步骤6.单击**Save**，然后将策略部署到FTD。

注意：在软件版本为6.1.0的设备上，诊断接口不能用于通过SSH访问融合CLI

步骤2.配置外部身份验证。

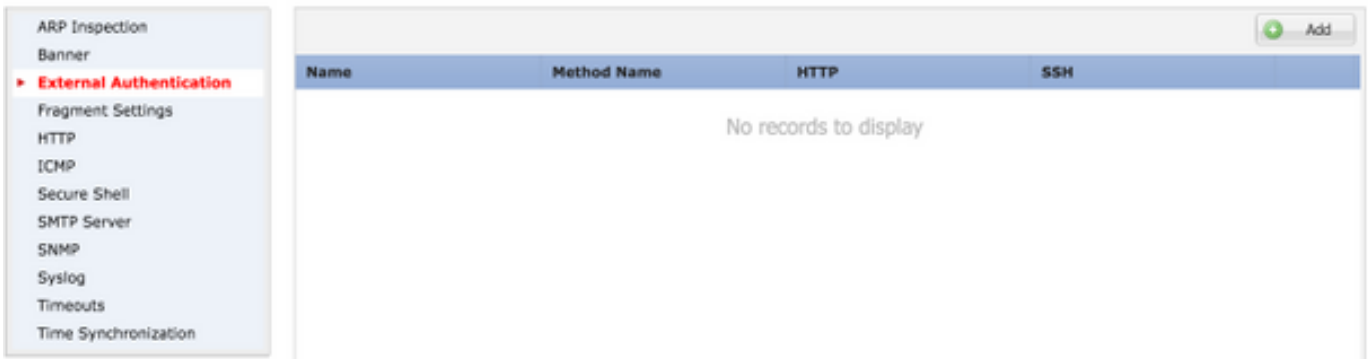
外部身份验证有助于将FTD集成到Active Directory或RADIUS服务器以进行用户身份验证。这是必要的步骤，因为本地配置的用户无法直接访问诊断CLI。诊断CLI和GUI仅由通过轻量级目录访问协议(LDAP)或RADIUS进行身份验证的用户访问。

配置外部身份验证有6个步骤。

步骤1.导航至 **设备(Devices)>平台设置(Platform Settings)**。

步骤2.编辑点击铅笔图标时存在的策略，或在点击New Policy按钮时创建新的FTD策略，并**选择**类型为 **威胁防御设置**。

步骤3. 导航至External Authentication(外部身份验证)选项卡，如图所示：



步骤4. 单击“添加”时，将出现一个对话框，如图所示：

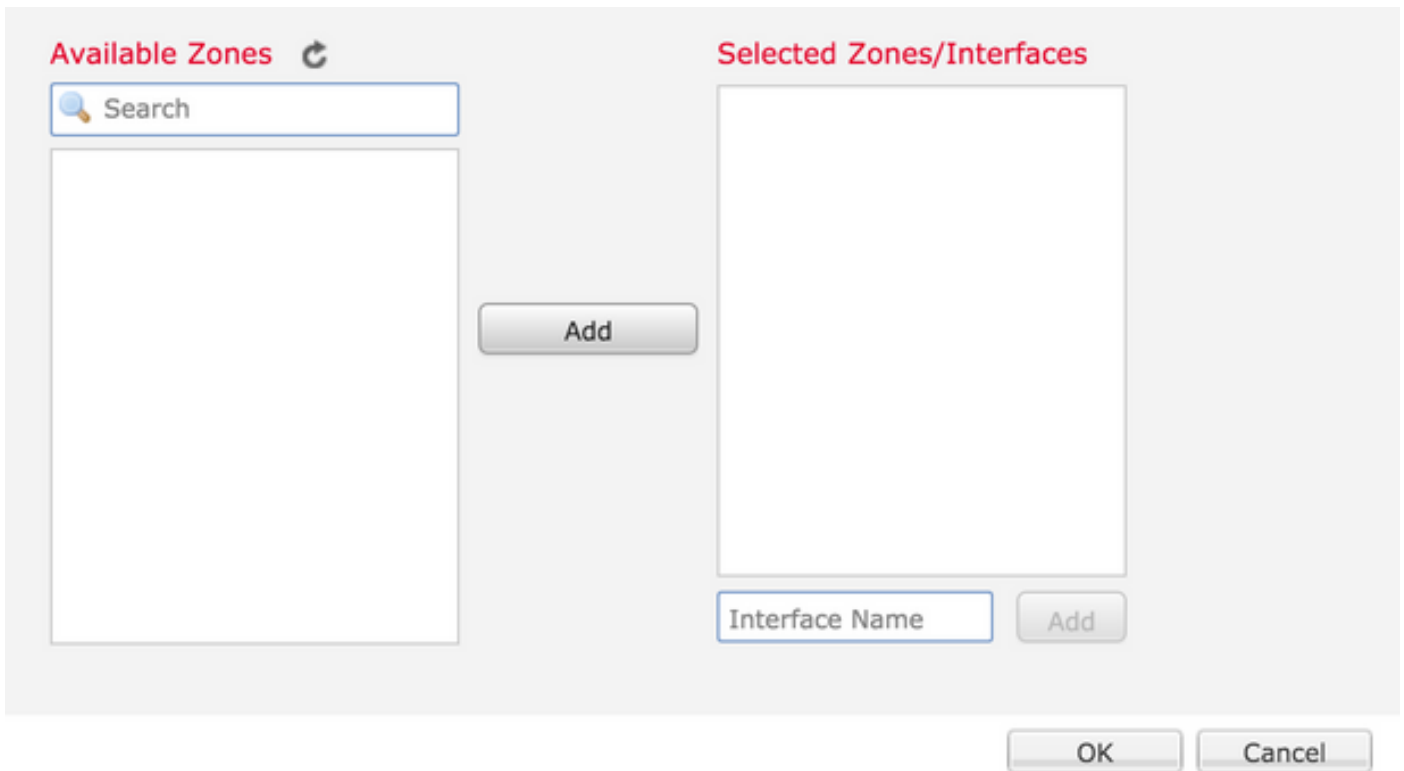
- **启用HTTP** — 启用此选项以提供对HTTPS的FTD访问。
- **启用SSH** — 启用此选项以通过SSH提供FTD访问。
- **名称** — 输入LDAP连接的名称。
- **说明** — 输入外部身份验证对象的可选说明。
- **IP地址** — 输入存储外部身份验证服务器的IP的网络对象。如果未配置网络对象，请创建新对象。单击(+)图标。
- **身份验证方法** — 选择RADIUS或LDAP协议进行身份验证。
- **启用SSL** — 启用此选项以加密身份验证流量。
- **服务器类型** — 选择服务器类型。众所周知的服务器类型包括MS Active Directory、Sun、OpenLDAP和Novell。默认情况下，该选项设置为自动检测服务器类型。
- **Port** — 输入进行身份验证的端口。
- **超时** — 输入身份验证请求的超时值。
- **基本DN** — 输入基本DN以提供用户可以存在的范围。
- **LDAP范围** — 选择要查看的LDAP范围。范围在同一级别内或在子树内查找。
- **用户名** — 输入要绑定到LDAP目录的用户名。
- **身份验证密码** — 输入此用户的密码。
- **确认** — 重新输入密码。
- **可用接口** — 显示FTD上可用接口的列表。

• **选定区域和接口** — 此列表显示用于访问身份验证服务器的接口列表。
对于RADIUS身份验证，不存在服务器类型Base DN或LDAP范围。端口是RADIUS端口1645。

Secret — 输入RADIUS的密钥。

Add External Authentication ? X

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"/> +
Authentication Method	<input type="text" value="LDAP"/>
Enable SSL	<input type="checkbox"/>
Server Type	<input type="text" value="AUTO-DETECT"/>
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"/>
Username	<input type="text"/> ex. cn=jsmith,dc=cisco,dc=com
Authentication Password	<input type="text"/>
Confirm	<input type="text"/>



步骤5.完成配置后，单击“确定”。

步骤6.保存策略并将其部署到Firepower威胁防御设备。

注意：在软件版本为6.1.0的设备上，外部身份验证不能用于通过SSH访问融合CLI

步骤3.配置SSH访问。

SSH提供对融合CLI的直接访问。使用此选项可直接访问CLI并运行debug命令。本节介绍如何配置SSH以访问FTD CLI。

注意：在运行软件版本6.0.1的FTD设备上，平台设置上的SSH配置提供对诊断CLI的直接访问，而不是CLISH的访问。您需要连接到br1上配置的IP地址以访问CLISH。但是，在运行软件版本6.1.0的FTD设备上，通过SSH访问时，所有接口都导航至融合CLI

在ASA上配置SSH有6个步骤

仅在6.0.1设备上：

这些步骤在软件版本低于6.1.0且高于6.0.1的FTD设备上执行。在6.1.0设备上，这些参数从操作系统继承。

步骤1.导航至Devices>Platform Settings。

步骤2.编辑点击铅笔图标时存在的策略，或者在点击New Policy（新策略）按钮时创建新的Firepower威胁防御策略，并选择Threat Defense Settings（威胁防御设置）类型。

步骤3.导航至“安全外壳”部分。系统将显示页面，如图所示：

SSH 版本:选择要在ASA上启用的SSH版本。有三个选项：

- 1:仅启用SSH版本1
- 2:仅启用SSH第2版
- 1 and 2:同时启用SSH版本1和2

超时：输入所需的SSH超时（以分钟为单位）。

启用安全复制 — 启用此选项可将设备配置为允许安全复制(SCP)连接并充当SCP服务器。

The screenshot shows the configuration page for Secure Shell. On the left is a navigation menu with 'Secure Shell' selected. The main area contains the following settings:

- SSH Version: 1 and 2 (dropdown menu)
- Timeout: 5 (input field, with '(1 - 60 mins)' in parentheses)
- Enable Secure Copy:

At the bottom right of the settings area is a green '+ Add' button. Below the settings is a table with two columns: 'Interface' and 'IP Address'. The table is currently empty, displaying 'No records to display'.

在6.0.1和6.1.0设备上：

这些步骤配置为限制通过SSH对特定接口和特定IP地址的管理访问。

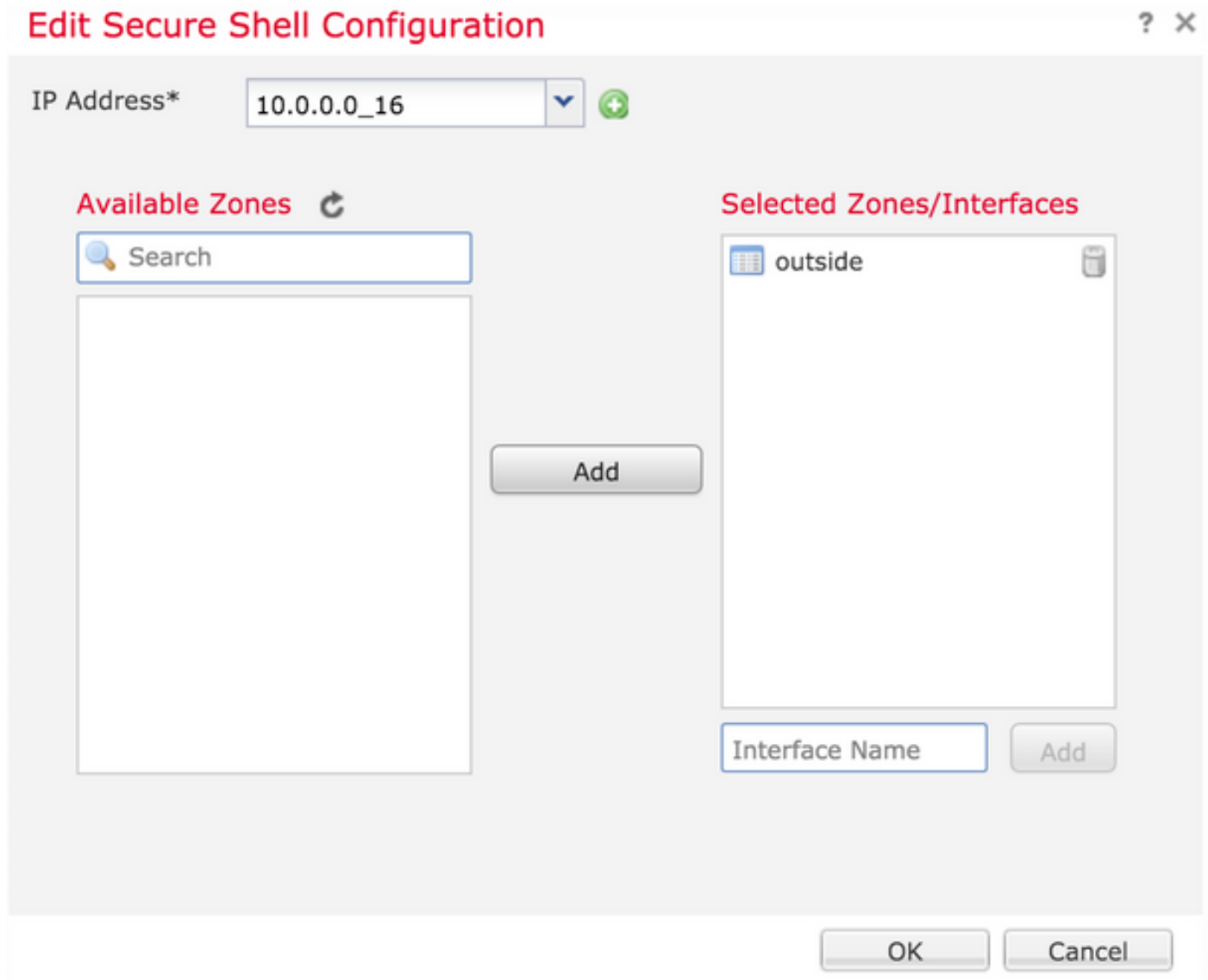
This screenshot is similar to the previous one, showing the configuration page for Secure Shell. The settings (SSH Version, Timeout, Enable Secure Copy) and the '+ Add' button are visible at the top. The table below, with columns 'Interface' and 'IP Address', is empty and displays 'No records to display'.

步骤1.单击“添加”并配置以下选项：

IP 地址：选择包含允许通过SSH访问CLI的子网的网络对象。如果网络对象不存在，请在单击(+)图标时**创建**一个对象。

所选区域/接口：选择访问SSH服务器的区域或接口。

步骤2.单击OK，如图所示：



使用此命令，可在融合CLI（6.0.1设备中的ASA诊断CLI）中查看SSH配置。

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

步骤3.完成SSH配置后，单击**Save**，然后将策略部署到FTD。

步骤4.配置HTTPS访问。

要启用对一个或多个接口的HTTPS访问，请导航至平台设置**中的**HTTP部分。HTTPS访问对于直接从诊断安全Web界面下载数据包捕获以便进行分析特别有用。

配置HTTPS访问有6个步骤。

步骤1.导航至Devices > Platform Settings

步骤2.编辑在单击策略旁边的铅笔图标时存在的平台设置策略，或在单击新策略时创建新的FTD策略。选择Firepower威胁防御类型。

步骤3.导航至HTTP部分时，会显示一个页面，如图所示。

启用HTTP服务器：启用此选项可在FTD上启用HTTP服务器。

端口：选择FTD接受管理连接的端口。

FTD-Policy

Enter a description

The screenshot shows the configuration page for an FTD-Policy. On the left is a navigation menu with the following items: ARP Inspection, Banner, External Authentication, Fragment Settings, HTTP (highlighted with a red arrow), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main content area is titled 'Enable HTTP Server' and has a checked checkbox. Below this is a 'Port' field with the value '443' and a note: '(Please don't use 80 or 1443)'. There is an 'Add' button with a green plus icon. Below the port field is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying the text 'No records to display'.

步骤4.单击Add，屏幕上将显示如图所示：

IP地址 — 输入允许对诊断接口进行HTTPS访问的子网。如果网络对象不存在，请创建一个对象并使用(+)选项。

选定区域/接口 — 与SSH类似，HTTPS配置需要配置一个接口，通过该接口可通过HTTPS访问。选择要通过HTTPS访问FTD的区域或接口。

Edit HTTP Configuration



IP Address* 10.0.0.0_16

Available Zones

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

在融合CLI (6.0.1设备中的ASA诊断CLI) 中查看HTTPS配置，并使用此命令。

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

步骤5.完成必要配置后，选择“确定”。

步骤6.输入所有所需信息后，单击**Save**，然后将策略部署到设备。

验证

当前没有可用于此配置的验证过程。

故障排除

以下是排除FTD上的管理访问问题的基本步骤。

步骤1.确保接口已启用并配置了IP地址。

步骤2.确保外部身份验证按配置工作，并且其可达性从平台设置的“外部身份验证”部分中指定的适当接口处进行。

步骤3.确保FTD上的路由准确。在FTD软件版本6.0.1中，导航至**system support diagnostic-cli**。分别运行**show route**和**show route management-only**命令，查看FTD和管理接口的路由。

在FTD软件版本6.1.0中，直接在融合CLI中运行命令。

相关信息

- [技术支持和文档 - Cisco Systems](#)