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

本文档介绍通过Firesight管理中心(FMC)对Firepower威胁防御(FTD)（HTTPS和SSH）进行管理访问的配置。

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）基础知识
- 通过HTTPS和SSH（安全外壳）了解ASA上的管理访问

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，运行在软件版本6.0.1及更高版本上。
- 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，运行在软件版本6.0.1及更高版本上。
- 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，当您进入系统支持diagnostic-cli时，可访问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，整个ASA命令在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
```

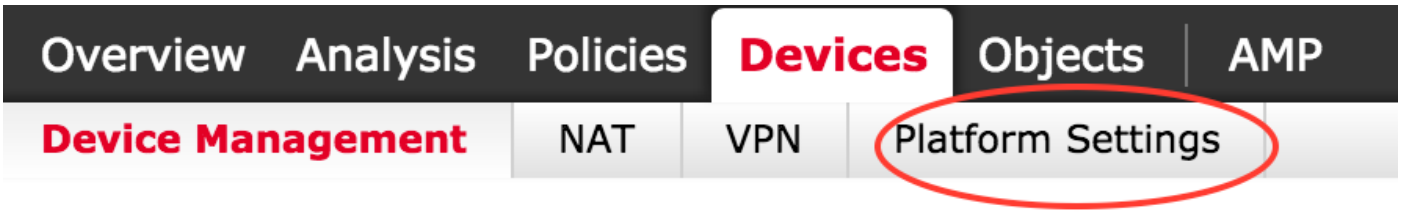
要直接从外部网络获得管理访问，您必须通过HTTPS或SSH配置管理访问。本文档提供通过SSH或HTTPS外部获取管理访问权限所需的必要配置。

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admin用户访问CLI，而所有其他用户都需要外部身份验证。

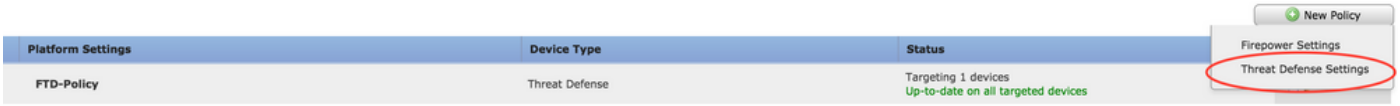
注意：在运行软件版本6.0.1的FTD设备上，无法通过为FTD的br1配置的IP直接访问诊断CLI。但是，在运行软件版本6.1.0的FTD设备上，可以通过为管理访问配置的任何接口访问融合CLI，但是，必须使用IP地址配置该接口。

配置

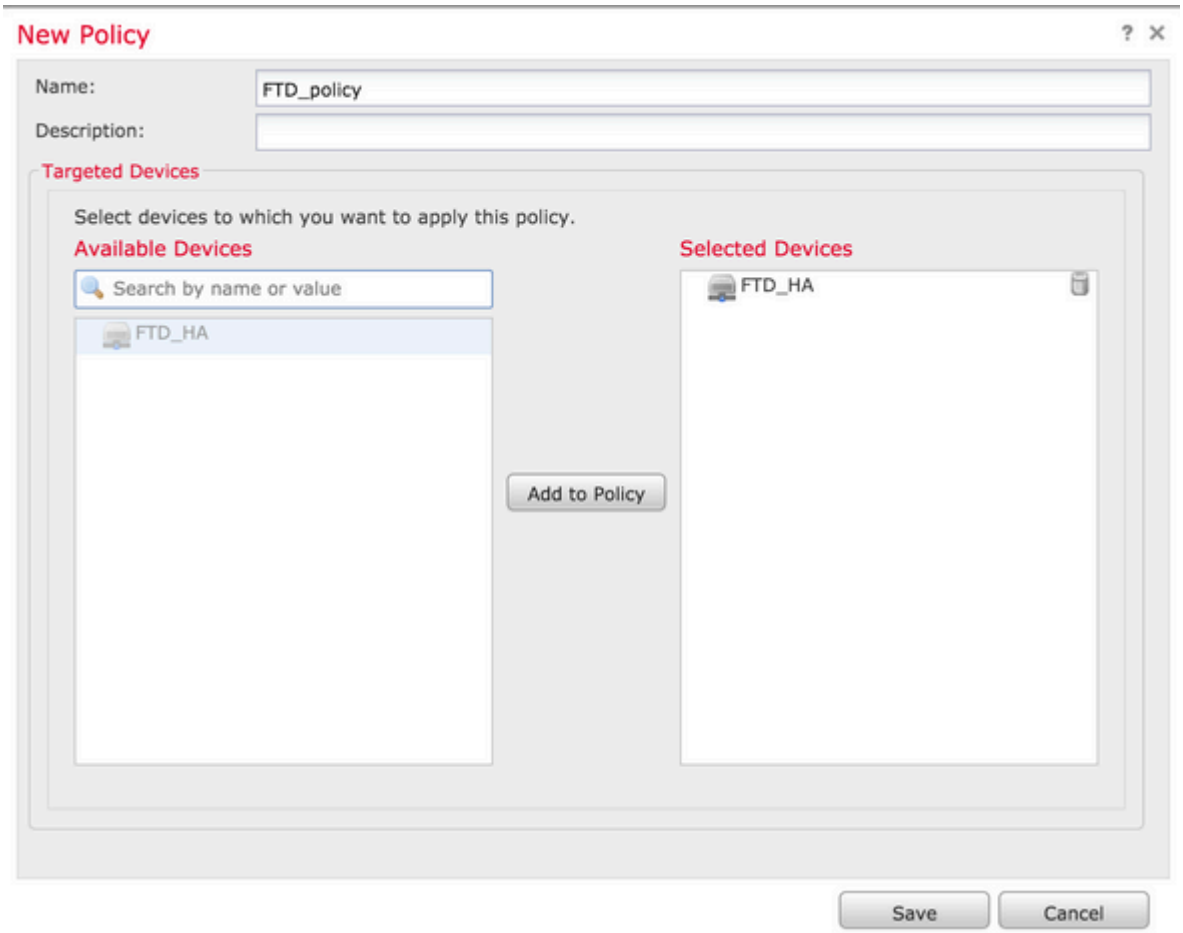
导航到设备中的平台设置选项卡时，配置所有管理访问相关的配置，如图所示：



单击铅笔图标编辑存在的策略，或者单击New Policy 按钮创建新的FTD策略，然后选择Threat Defense Settings作为类型，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时采取的四个主要步骤。

步骤1.通过FMC GUI在FTD接口上配置IP。

在通过SSH或HTTPS访问FTD的接口上配置IP。导航到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。

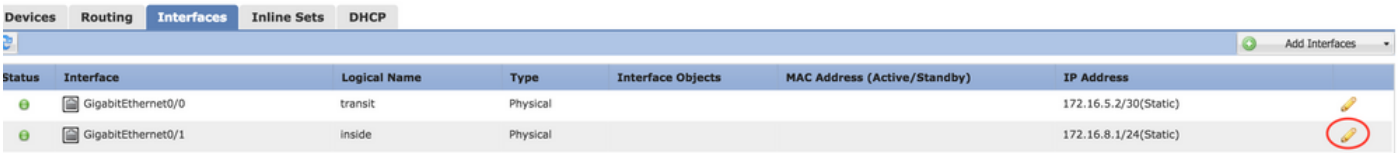
配置诊断接口有六个步骤。

步骤1.导航至 Device > Device Management。

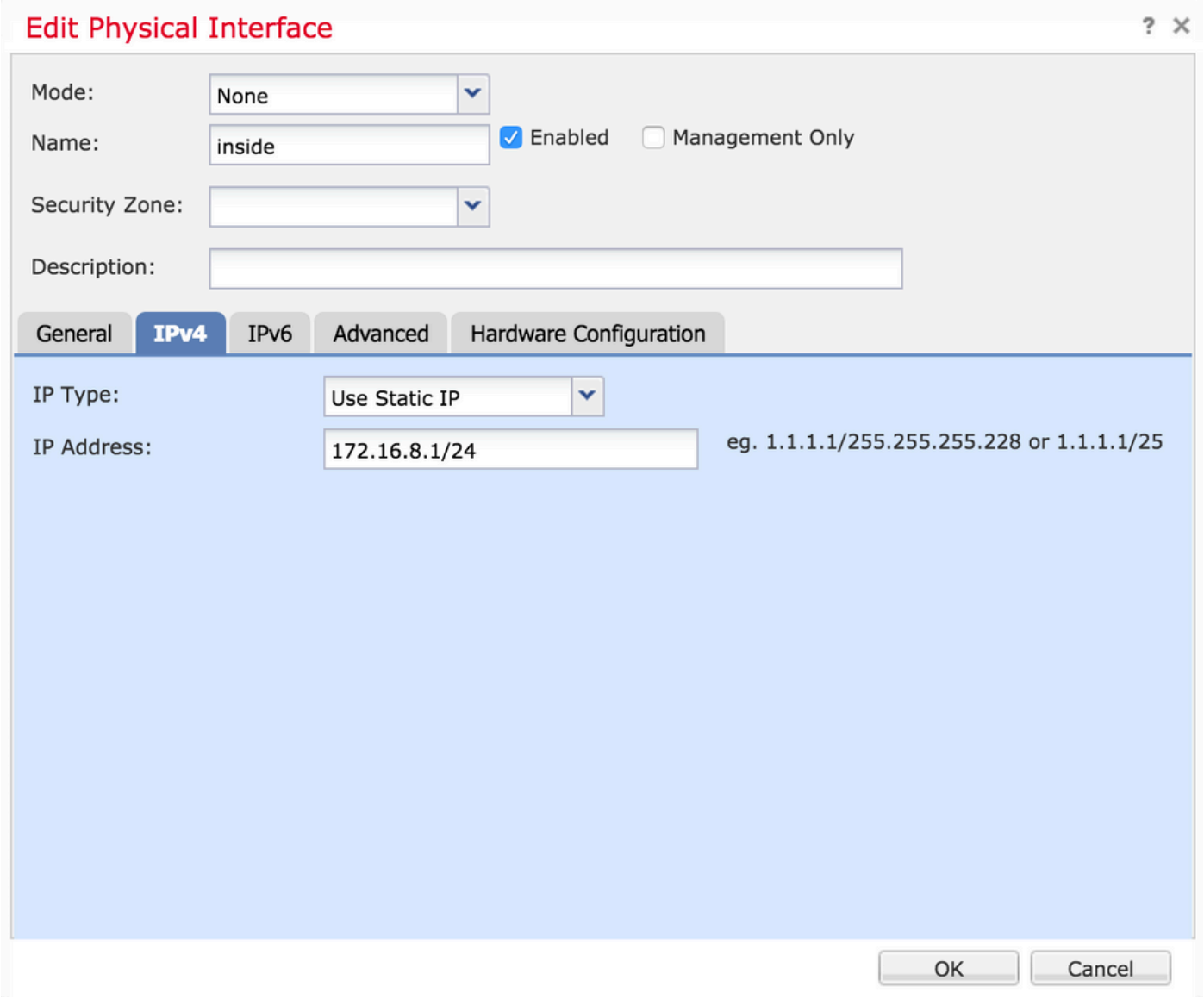
步骤2.选择Device或FTD HA Cluster。

步骤3.导航到Interfaces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：



步骤5.选中enable复选框以启用接口。导航到Ipv4选项卡，选择IP Type作为static或DHCP。现在输入接口的IP地址，然后单击OK，如图所示：



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，诊断界面无法用于通过SSH访问融合CLI

步骤2.配置外部身份验证。

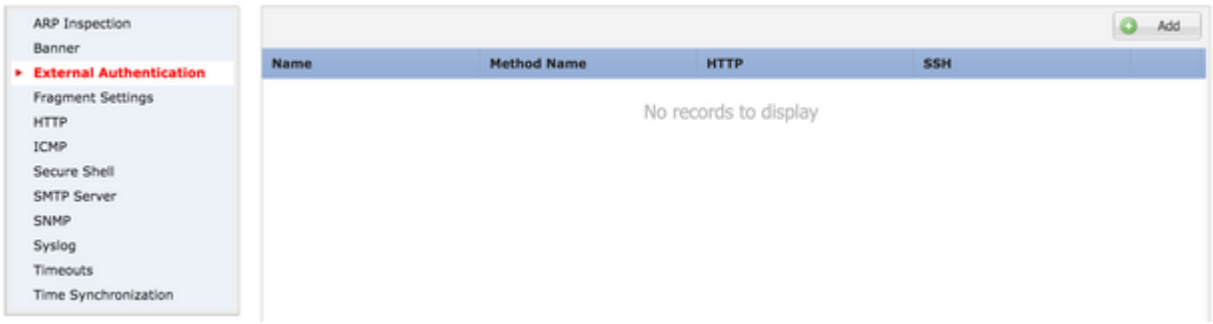
外部身份验证有助于将FTD集成到Active Directory或RADIUS服务器以进行用户身份验证。这是必要步骤，因为本地配置的用户无权直接访问诊断CLI。只有通过轻量级目录访问协议(LDAP)或RADIUS进行身份验证的用户才能访问诊断CLI和GUI。

配置外部身份验证有6个步骤。

步骤1.导航至 Devices > Platform Settings。

第2步：编辑在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，然后选择类型作为 威胁防御设置。

步骤3.导航到外部身份验证选项卡，如图所示：



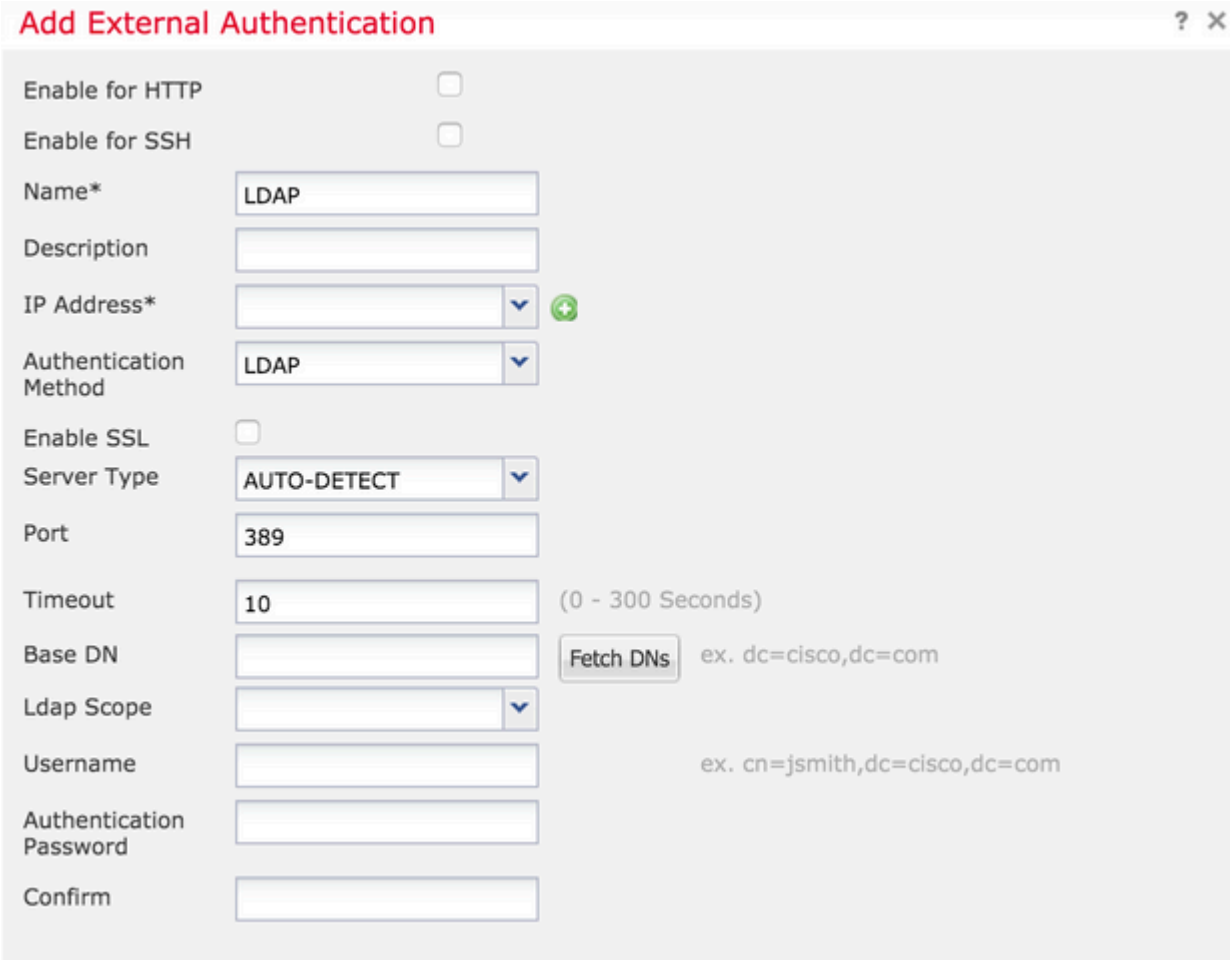
步骤4.单击Add时，将显示一个对话框，如图所示：

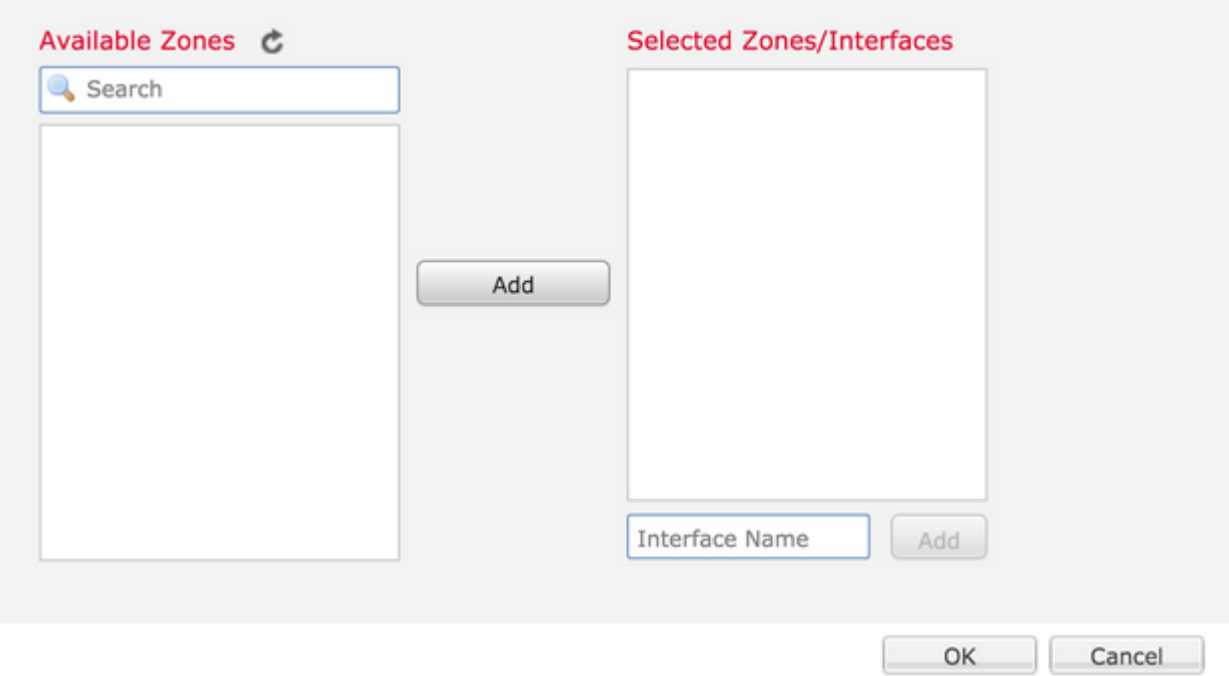
- Enable for HTTP — 启用此选项提供通过HTTPS访问FTD。
- Enable for SSH — 启用此选项以提供通过SSH访问FTD。
- Name — 输入LDAP连接的名称。
- 说明 — 输入外部身份验证对象的可选说明。
- IP地址 — 输入存储外部身份验证服务器的IP的网络对象。如果没有配置网络对象，请创建一个新对象。点击(+)图标。
- Authentication Method — 选择用于身份验证的RADIUS或LDAP协议。
- 启用SSL — 启用此选项以加密身份验证流量。
- 服务器类型 — 选择服务器类型。众所周知的服务器类型是MS Active Directory、Sun、OpenLDAP和Novell。默认情况下，此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。
- Timeout — 输入身份验证请求的超时值。
- Base DN — 输入基本DN以提供用户可存在的范围。
- LDAP范围 — 选择要查找的LDAP范围。作用域位于同一级别或要在子树中查看。
- Username — 输入要绑定到LDAP目录的用户名。
- Authentication password — 输入此用户的密码。
- Confirm — 重新输入密码。

- 可用接口 — 显示FTD上可用接口的列表。
- Selected zones and interfaces — 显示从中访问身份验证服务器的接口的列表。

对于RADIUS身份验证，没有服务器类型Base DN或LDAP Scope。端口是RADIUS端口1645。

Secret — 输入RADIUS的密钥。





步骤5.完成配置后，点击OK。

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，无法使用外部身份验证通过SSH访问融合CLI

步骤3.配置SSH访问。

SSH提供到融合CLI的直接访问。使用此选项直接访问CLI和运行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配置提供直接访问诊断CLI而不是CLISH的权限。您需要连接到br1上配置的IP地址才能访问CLISH。但是，在运行软件版本6.1.0的FTD设备上，通过SSH访问时，所有接口都会导航到融合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.导航到设备>平台设置。

步骤2. 编辑在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Firepower威胁防御策略，然后选择type as Threat Defense Settings。

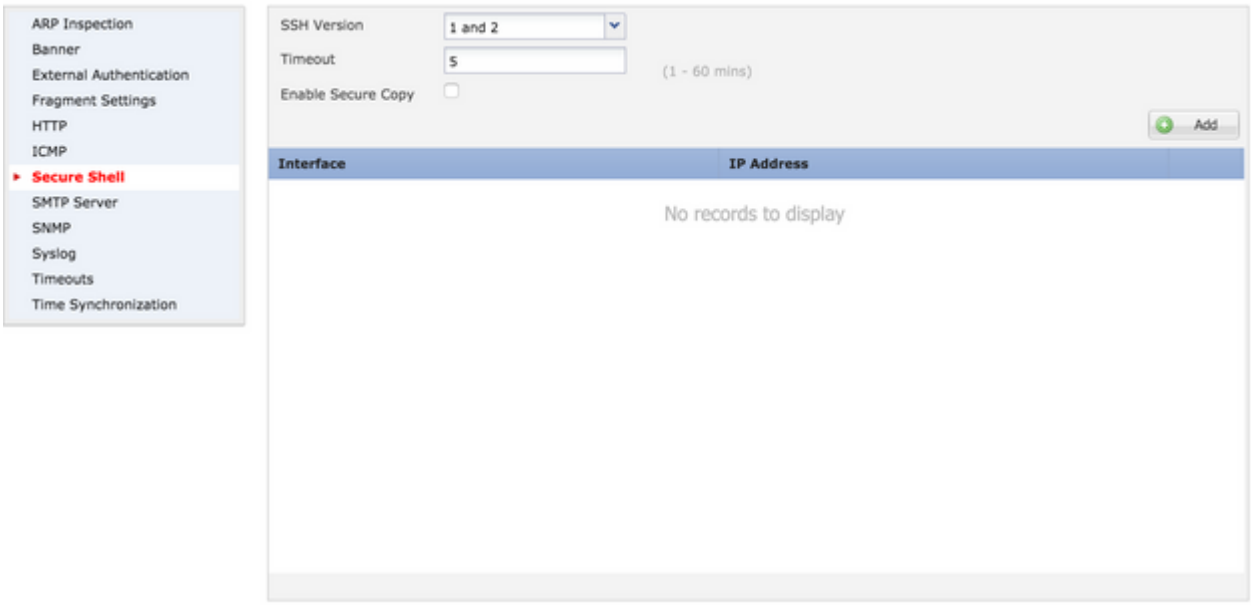
步骤3.导航到Secure Shell部分。此时将显示一个页面，如图所示：

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第1版
- 2:仅启用SSH第2版
- 1 and 2:启用SSH第1版和第2版

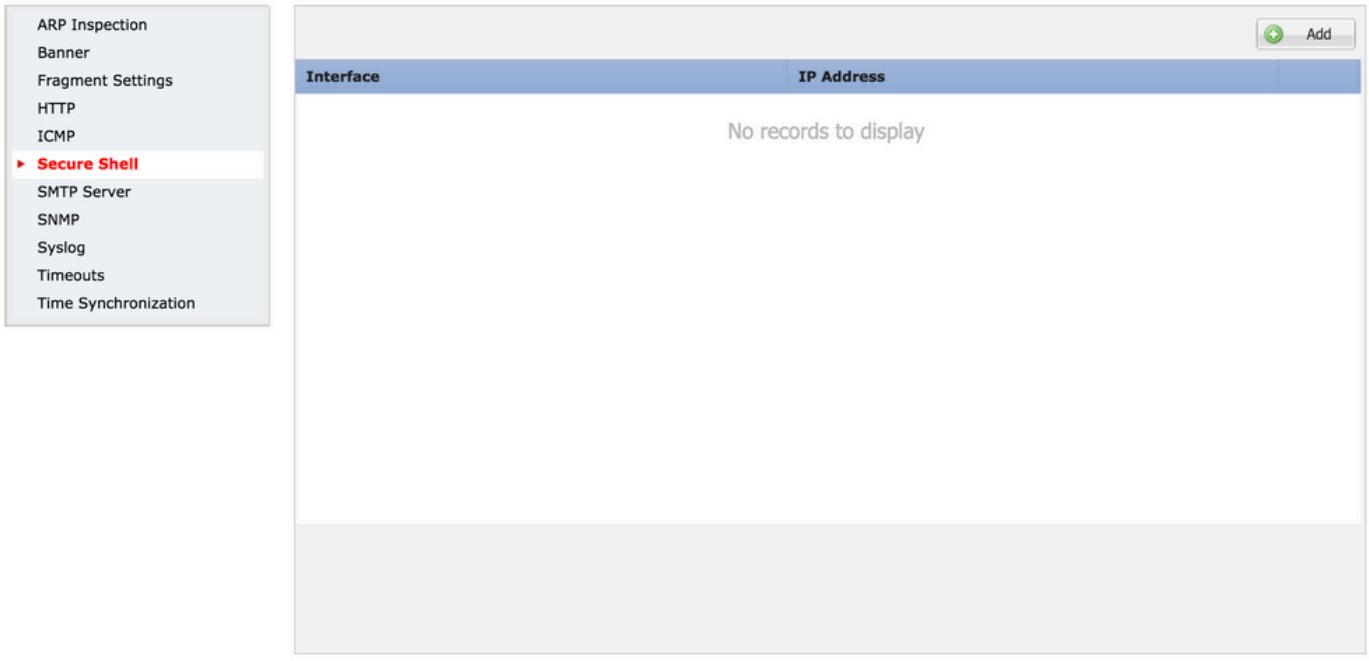
超时：输入所需的SSH超时（以分钟为单位）。

Enable Secure Copy — 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。



在6.0.1和6.1.0设备上：

这些步骤配置为将通过SSH的管理访问限制为特定接口和特定IP地址。

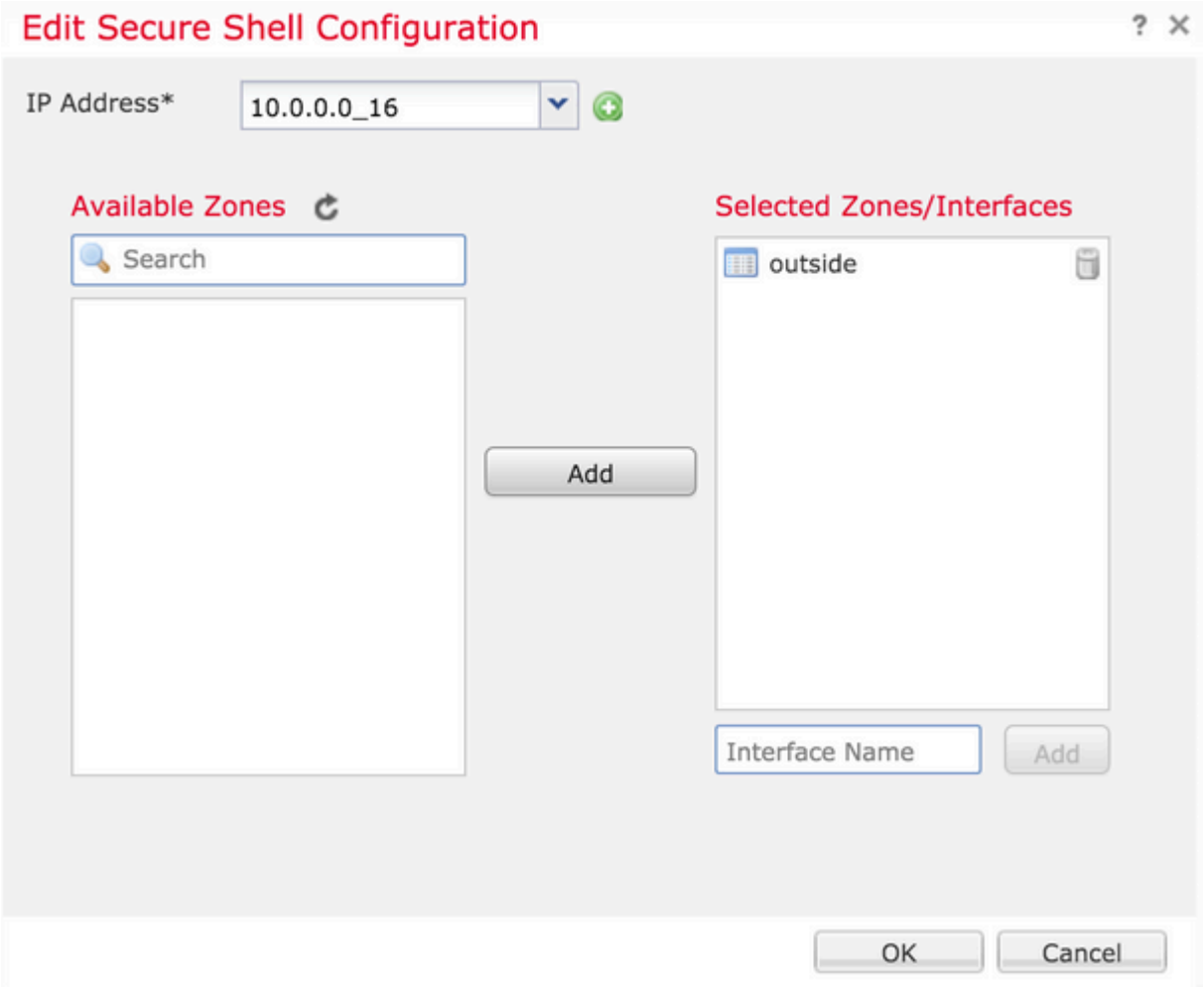


步骤1.单击Add并配置以下选项：

IP 地址：选择包含允许通过SSH访问CLI的子网的网络对象。如果不存在网络对象，请在点击(+)图标时创建一个对象。

所选区域/接口：选择用于访问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，请导航到平台设置中的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供分析特别有用。

配置HTTPS访问有6个步骤。

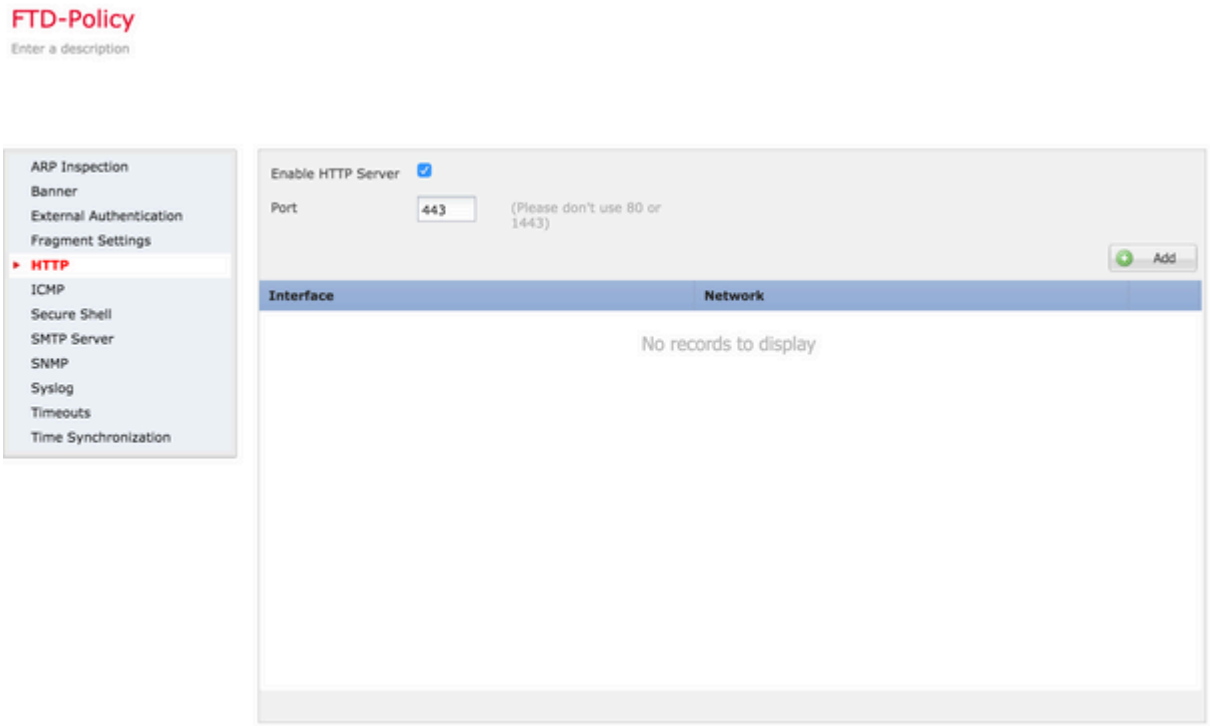
步骤1.导航到设备>平台设置

步骤2.编辑在点击策略旁边的铅笔图标时存在的平台设置策略，或在点击New Policy时创建新的FTD策略。选择类型为Firepower威胁防御。

步骤3.导航到HTTP部分时，将显示如图所示的页面。

启用HTTP服务器：启用此选项，以便在FTD上启用HTTP服务器。

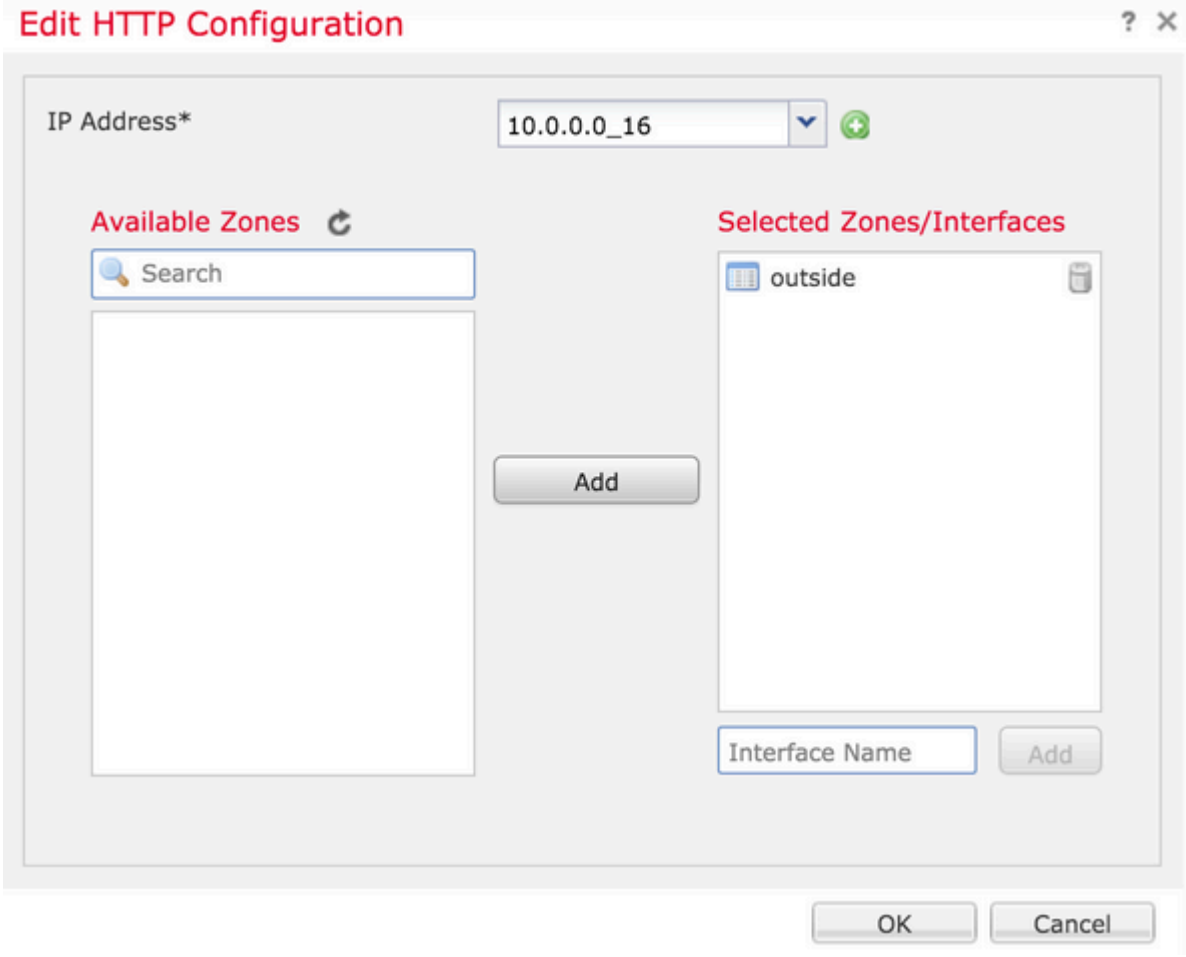
Port：选择FTD接受管理连接的端口。



第4步：点击Add，页面将会显示，如图所示：

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

所选区域/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。



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.完成必要的配置后，选择OK。

步骤6.输入所有必需信息后，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

以下是对FTD上的管理访问问题进行故障排除的基本步骤。

步骤1.确保接口已启用且配置了IP地址。

步骤2.确保外部身份验证按配置工作，并可从Platform Settings的External Authentication部分中指定的相应接口访问。

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。运行命令show route和show route management-only，分别查看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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。