

管理访问的配置对FTD的(HTTPS和SSH)通过FMC

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配置在FTD接口的IP。](#)

[步骤2.配置外部验证。](#)

[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

本文通过Firesight管理中心(FMC)描述管理访问的配置对Firepower威胁防御(FTD)的(HTTPS和SSH)。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识
- 基础知识ASA (可适应安全工具)
- 管理访问知识在ASA的通过HTTPS和SSH (安全壳程序)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA的(5506X/5506H-X/5506W-X、ASA 5508-X， ASA 5516-X)可适应安全工具(ASA) Firepower威胁防御镜像，在软件版本6.0.1运行以上

- ASA Firepower威胁ASA的(5515-X、ASA 5525-X , ASA 5545-X , ASA 5555-X , ASA 5585-X)防御镜像，在软件版本6.0.1运行以上
- Firepower管理中心(FMC)版本6.0.1和以上


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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

使用起始Firepower威胁防御(FTD)，整个ASA相关的配置在GUI被执行。

在运行软件版本6.0.1的FTD设备上，当您输入**系统支持诊断CLI**，ASA诊断CLI访问。然而，在运行软件版本6.1.0的FTD设备，CLI聚合，并且整个ASA命令在CLISH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
```

为了获得管理访问直接地从外部网络，您必须通过HTTPS或SSH配置管理访问。本文提供要求的必要的配置获得在SSH或HTTPS的管理访问外部。

注意：在运行软件版本6.0.1的FTD设备上，CLI不可能由本地用户访问，外部验证必须配置为了验证用户。然而，当外部验证为其他用户时，要求在运行软件版本6.1.0的FTD设备，CLI由本地**管理员用户**访问

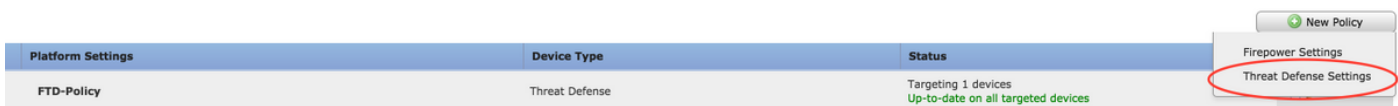
注意：在运行软件版本6.0.1的FTD设备上，诊断CLI在为FTD的br1配置的IP不是直接可访问的。然而，在运行软件版本6.1.0的FTD设备，聚合的CLI在为管理访问配置的所有接口是可访问，然而，必须配置接口用IP地址。

配置

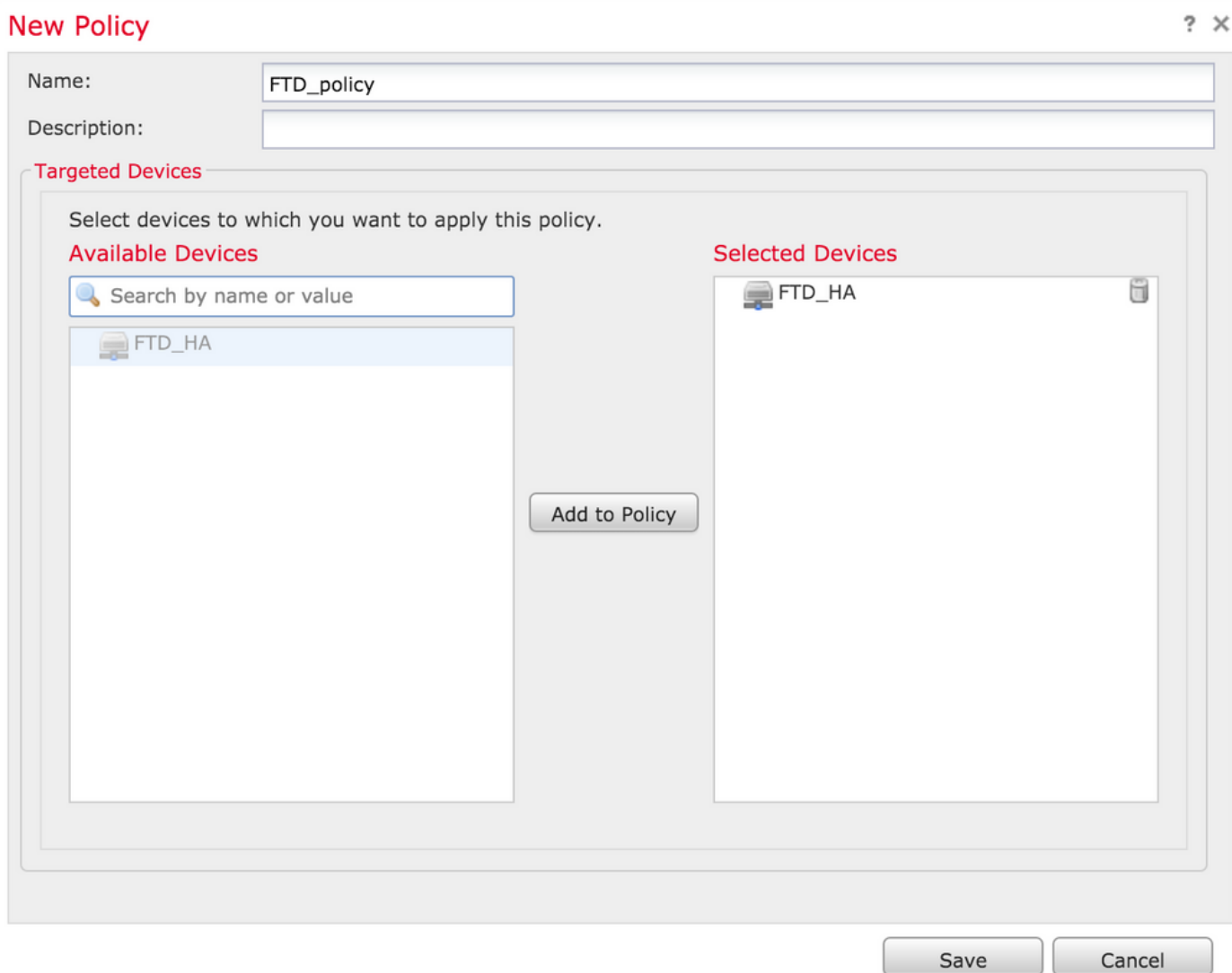
所有管理访问相关的配置配置，当您导航对在设备的**平台设置选项卡**，如镜像所显示，：



二者之一编辑存在的策略，当您点击铅笔图标或创建一项新的FTD策略，当您点击新的策略按钮并且选择类型作为威胁防御设置，如镜像所显示，：



如镜像所显示，选择FTD设备运用此策略并且单击“Save”，：



配置管理访问

这些是采取的四个主要步骤配置管理访问。

步骤1.通过FMC GUI配置在FTD接口的IP。

配置在FTD通过SSH或HTTPS是可访问的接口的IP。编辑存在的接口，当您导航对FTD的接口选项卡。

注意：在运行软件版本6.0.1的FTD设备上，在FTD的默认管理接口是diagnostic0/0接口。然而，在运行软件版本6.1.0的FTD设备，所有接口支持除了诊断接口的管理访问。

有配置诊断接口的六个步骤。

步骤1.导航对**设备>设备管理**。

步骤2.选择设备或FTD HA团星。

步骤3.导航对**接口选项卡**。

步骤4.如镜像所显示，点击**铅笔图标配置/编辑接口**获得管理访问，：



Status	Interface	Logical Name	Type	Interface Objects	MAC Address (Active/Standby)	IP Address	
<input checked="" type="checkbox"/>	GigabitEthernet0/0	transit	Physical			172.16.5.2/30(Static)	
<input checked="" type="checkbox"/>	GigabitEthernet0/1	inside	Physical			172.16.8.1/24(Static)	

步骤5.选择**Enable复选框**启用接口。导航对**Ipv4选项卡**，选择IP类型作为**静态或DHCP**。如镜像所显示，现在请输入接口的一个IP地址并且点击OK键，：

Edit Physical Interface ? X

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. 点击“Save”然后实施策略对FTD。

注意： 诊断接口不可能用于访问在SSH的聚合的CLI在有软件版本的6.1.0设备

步骤2. 配置外部验证。

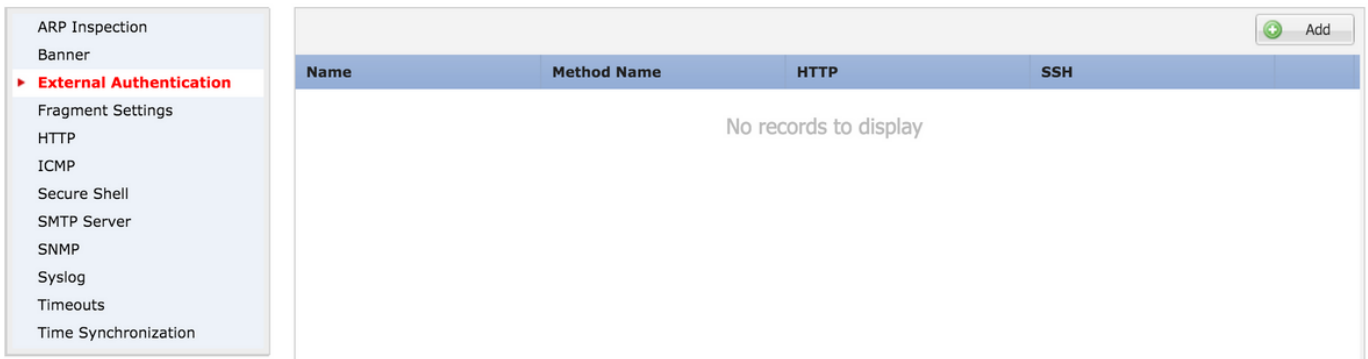
外部验证实现FTD的集成到活动目录或RADIUS服务器用户认证的。因为本地配置的用户没有直接访问对诊断CLI，这是必要步骤。诊断CLI和GUI由通过轻量级目录访问协议(LDAP)或RADIUS验证的用户仅访问。

有配置外部验证的6个步骤。

步骤1. 导航对**设备>平台设置**。

第二步：二者之一编辑存在的策略，当您点击铅笔图标或创建一项新的FTD策略，当您点击**新的策略**按钮并且选择类型作为**威胁防御设置**。

步骤3.如镜像所显示，导航对**外部验证**选项卡，：



第四步：因为您点击**Add**，如镜像所显示，对话框出现：

- **HTTP的Enable (event)**启用此选项提供访问在HTTPS的FTD。
- **SSH的Enable (event)**启用此选项提供访问在SSH的FTD。
- **命名回车名称**对于LDAP连接。
- **说明回车**外部验证对象的一个可选说明。
- **IP地址回车**存储外部验证服务器的IP的网络对象。如果没有网络对象配置通过单击创建新的在 (+)图标。
- **验证方法精选的**RADIUS或LDAP协议验证的。
- **启用SSL Enable (event)**此选项加密验证流量。
- **服务器类型**选择服务器类型。著名的服务器类型是MS活动目录、Sun、OpenLDAP和Novell。默认情况下，选项设置自动查出服务器类型。
- **端口回车**验证发生的端口。
- **超时回车**认证请求的超时值。
- **基础DN回车**提供内用户应该存在的范围的基础DN在。
- **LDAP范围**选择LDAP范围查找。范围在同一个级别内或在子树内查找。
- **用户名回车**绑定的用户名对LDAP目录。
- **验证密码回车**此用户的密码。
- **确认重新输入密码。**
- **联机建立接口**可用的接口A列表在FTD的显示。


- **选定区域和建立接口**此显示认证服务器访问的接口列表。

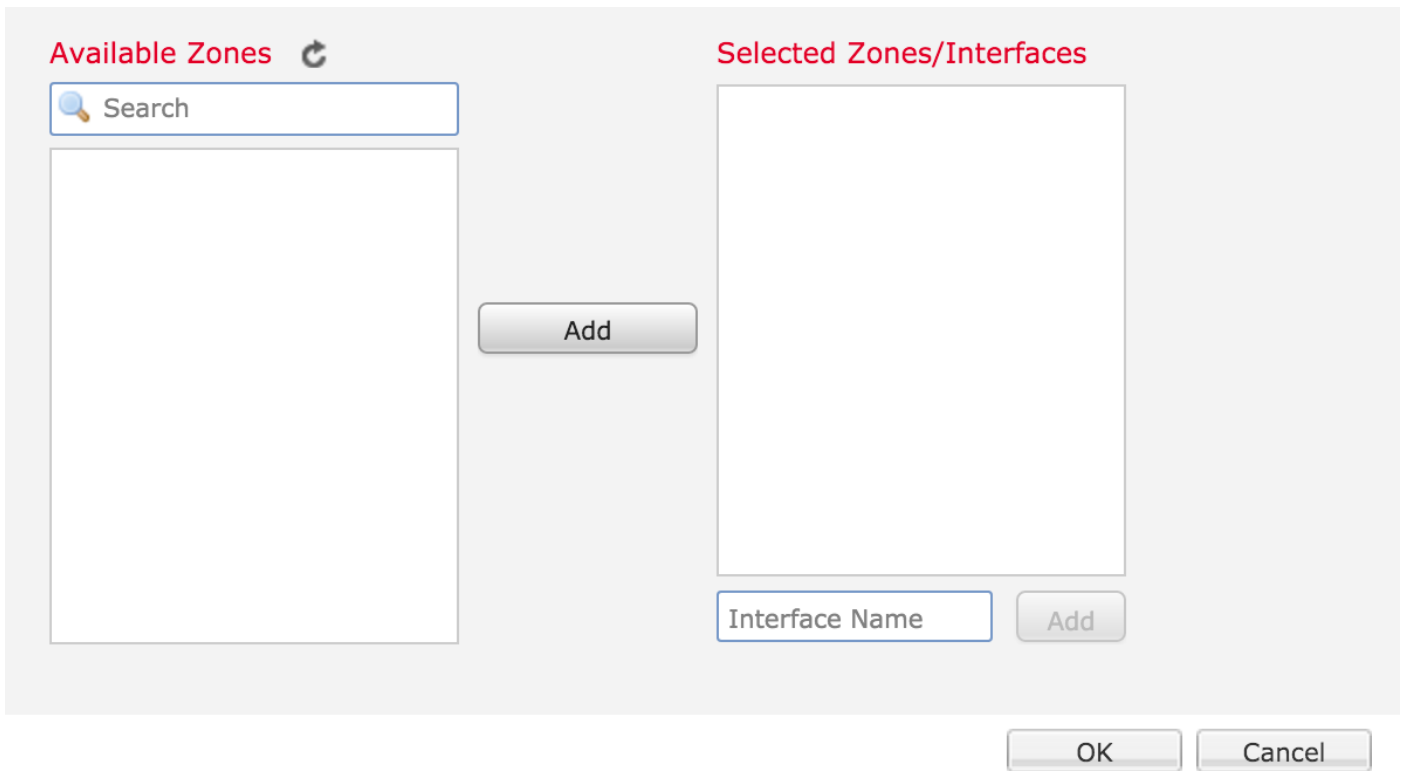
对于RADIUS验证，没有服务器类型基础DN或LDAP范围。端口是RADIUS端口1645。

秘密回车RADIUS的密钥。

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"/> 
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="password"/>
Confirm	<input type="password"/>



第五步：一旦配置被执行，请点击OK键。

步骤6.保存策略并且部署它到Firepower威胁防御设备。

注意： 外部验证不可能用于访问在SSH的聚合的CLI在有软件版本的6.1.0设备

步骤3.配置SSH访问。

SSH对聚合的CLI的提供直接访问。请使用此选项直接地访问CLI和运行调试指令。此部分描述如何配置SSH为了访问FTD CLI。

注意： 在运行软件版本6.0.1的FTD设备上，在平台设置的SSH配置提供对诊断CLI的访问直接地和没有CLISH。您需要连接到在br1配置的IP地址访问CLISH。然而，在运行软件版本6.1.0的FTD设备，所有接口导航对聚合的CLI，当访问在SSH

有配置在ASA的SSH的6个步骤

仅在6.0.1设备上：

这些步骤在FTD设备被执行与软件版本少于6.1.0和非常地比6.0.1。在6.1.0设备上这些参数从OS被继承。

步骤1.导航对**Devices>Platform**设置。

第二步：二者之一编辑存在的策略，当您点击铅笔图标或创建一项新的Firepower威胁国防政策，当您点击**新的策略**按钮并且选择类型作为**威胁防御**设置。

步骤3.导航对**Secure Shell**部分。如镜像所显示，页出版，：

SSH版本：选择SSH版本启用在ASA。 有三个选项：

- **1**：Enable (event)仅SSH版本1
- **2**：Enable (event)仅SSH版本2
- **1和2**：启用两SSH版本1和2

超时：输入希望的SSH超时以分钟。

启用安全的复制启用此选项配置设备 允许安全Copy(SCP)连接和作为SCP服务器。

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

SSH Version: 1 and 2
Timeout: 5 (1 - 60 mins)
Enable Secure Copy:

Interface	IP Address
No records to display	

在6.0.1和6.1.0设备上：

这些步骤配置通过SSH限制管理访问对特定接口和对特定IP地址。

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

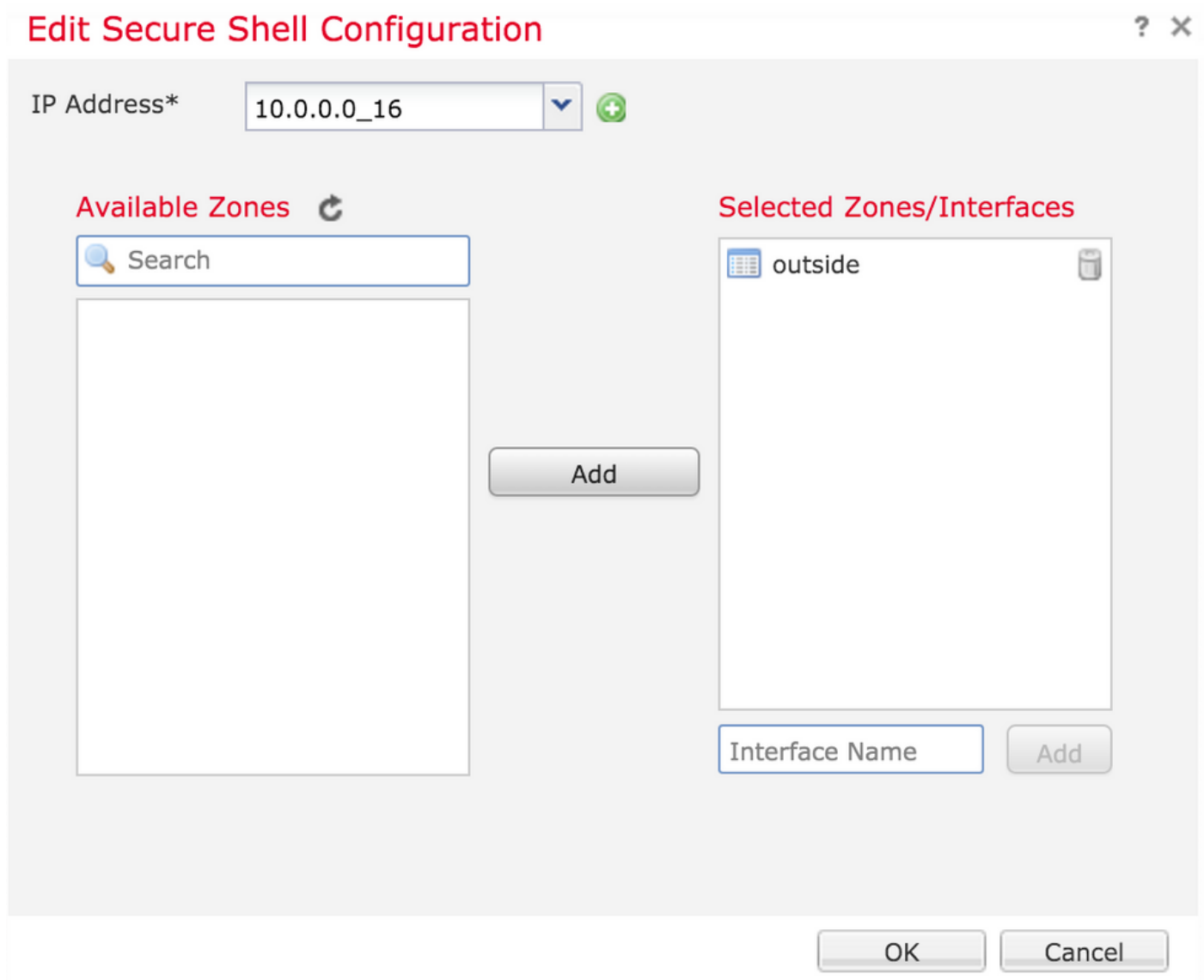
Interface	IP Address
No records to display	

步骤1.单击添加并且配置这些选项：

IP 地址：选择包含子网允许访问在SSH的CLI的网络对象。如果网络对象不存在，请创建一，您点击(+)图标。

选定区域/接口：选择SSH服务器访问的区域或接口。

步骤2.如镜像所显示，点击OK键，：



SSH的配置在聚合的CLI (ASA在6.0.1设备的诊断CLI查看)使用此命令。

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

第三步：一旦SSH配置被执行，请点击“Save”然后实施策略对FTD。

步骤4.配置HTTPS访问。

为了启用对一个或更多接口的HTTPS访问，请导航对在平台设置的HTTP部分。HTTPS访问是特别地有用的下载从诊断安全Web接口的数据包捕获直接地分析的。

有配置HTTPS访问的6个步骤。

步骤1.导航对设备>平台设置

第二步：二者之一编辑存在的平台设置策略，当您点击在策略旁边的**铅笔图标**或创建一项新的FTD策略，当您点击**新的策略**。选择类型作为**Firepower威胁防御**。

第三步：当您导航对HTTP部分，如镜像所显示，页出版。

Enable (event) HTTP服务器：启用此选项做启用在FTD的HTTP服务器。

波尔特：选择FTD接受管理连接的端口。

FTD-Policy

Enter a description

The screenshot shows the configuration interface 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, there is a 'Port' field with the value '443' and a note: '(Please don't use 80 or 1443)'. An 'Add' button with a green plus icon is located in the top right corner. At the bottom, there is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying the text 'No records to display'.

步骤4. Click**添加**如镜像所显示，并且apage出现：

IP地址回车允许得以进入对诊断接口的HTTPS的子网。如果网络对象不存在请创建一使用**(+)**选项。

选定区域/接口类似于SSH，HTTPS配置需要有在哪些配置的接口通过HTTPS是可访问。选择FTD将通过HTTPS访问的区域或接口。

Edit HTTP Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

HTTPS的配置在聚合的CLI (ASA在6.0.1设备的诊断CLI查看)使用此命令。

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

第五步：一旦必要的配置是完成挑选OK。

第六步：一旦所有必填信息输入点击“Save”然后请实施策略到设备。

验证

当前没有可用于此配置的验证过程。

故障排除

这些是排除故障的管理访问问题基本步骤在FTD。

步骤1:保证接口启用和配置用IP地址。

第二步：保证外部验证工作如配置，并且其从适当的接口的可接通性指定在平台设置的外部验证部分。

第三步：保证在FTD的路由是准确的。在FTD软件版本6.0.1中，请导航对**系统支持诊断CLI**。运行**仅管理的show route**命令和的**show route**为各自FTD和管理接口发现路由。

在FTD软件版本6.1.0中，请运行命令直接地在聚合的CLI。

相关信息

- [思科Firepower威胁ASA的防御快速入门指南](#)
- [技术支持和文档 - Cisco Systems](#)