

# Configuración del acceso de gestión a FTD (HTTPS y SSH) a través de FMC

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración del acceso a la gestión](#)

[Paso 1. Configure IP en la interfaz FTD a través de la GUI de FMC.](#)

[Paso 2. Configuración de la autenticación externa.](#)

[Paso 3. Configure el acceso SSH.](#)

[Paso 4. Configure el acceso HTTPS.](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe la configuración del acceso de administración a Firepower Threat Defense (FTD) (HTTPS y SSH) a través de Firesight Management Center (FMC).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower
- Conocimiento básico de ASA (Adaptive Security Appliance)
- Conocimiento de Management Access en ASA a través de HTTPS y SSH (Secure Shell)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Imagen de defensa frente a amenazas de Adaptive Security Appliance (ASA) para ASA

(5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ), que se ejecuta en la versión de software 6.0.1 y posterior.

- Imagen de ASA Firepower Threat Defense para ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X), que se ejecuta en la versión de software 6.0.1 y posterior.
- Firepower Management Center (FMC) versión 6.0.1 y posterior.


The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Con el inicio de Firepower Threat Defense (FTD), toda la configuración relacionada con ASA se realiza en la GUI.

En los dispositivos FTD que ejecutan la versión de software 6.0.1, se accede a la CLI de diagnóstico ASA cuando se ingresa la **CLI de diagnóstico del soporte del sistema**. Sin embargo, en los dispositivos FTD que ejecutan la versión de software 6.1.0, la CLI es convergente y los comandos ASA completos se configuran en CLISH.

```
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
```

Para obtener acceso de administración directamente desde una red externa, debe configurar el acceso de administración a través de HTTPS o SSH. Este documento proporciona la configuración necesaria necesaria para obtener acceso de administración sobre SSH o HTTPS externamente.

**Nota:** En los dispositivos FTD que ejecutan la versión de software 6.0.1, un usuario local no puede acceder a la CLI, se debe configurar una autenticación externa para autenticar a los usuarios. Sin embargo, en los dispositivos FTD que ejecutan la versión de software 6.1.0, el usuario **administrador** local accede a la CLI mientras que se requiere una autenticación externa para todos los demás usuarios.

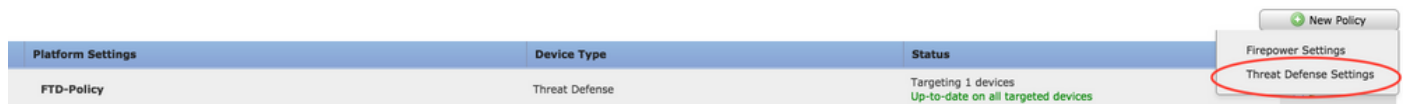
**Nota:** En los dispositivos FTD que ejecutan la versión de software 6.0.1, la CLI de diagnóstico no es accesible directamente a través de la IP configurada para **br1** del FTD. Sin embargo, en los dispositivos FTD que ejecutan la versión de software 6.1.0, la CLI convergente es accesible a través de cualquier interfaz configurada para el acceso de administración; sin embargo, la interfaz debe configurarse con una dirección IP.

# Configurar

Toda la configuración relacionada con el acceso de administración se configura a medida que navega a la pestaña **Configuración de plataforma** en **Dispositivos**, como se muestra en la imagen:



Edite la política que existe al hacer clic en el icono del lápiz o cree una nueva política FTD al hacer clic en el botón **Nueva política** y seleccione el tipo como **Configuración de Threat Defense**, como se muestra en la imagen:



Seleccione el dispositivo FTD para aplicar esta política y haga clic en **Guardar**, como se muestra en la imagen:

**New Policy** ? X

Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

- FTD\_HA

**Selected Devices**

- FTD\_HA

## Configuración del acceso a la gestión

Estos son los cuatro pasos principales realizados para configurar el acceso a la administración.

### Paso 1. Configure IP en la interfaz FTD a través de la GUI de FMC.

Configure una IP en la interfaz a través de la cual se puede acceder al FTD a través de SSH o HTTPS. Edite las interfaces que existen mientras navega a la pestaña **Interfaces** del FTD.

**Nota:** En los dispositivos FTD que ejecutan la versión de software 6.0.1, la interfaz de administración predeterminada en el FTD es la interfaz diagnostic0/0. Sin embargo, en los dispositivos FTD que ejecutan la versión de software 6.1.0, todas las interfaces admiten acceso de administración excepto la interfaz de diagnóstico.

Hay seis pasos para configurar la interfaz de diagnóstico.

Paso 1. Vaya a **Device > Device Management (Dispositivo > Administración de dispositivos)**.

Paso 2. Seleccione Device o FTD HA Cluster .

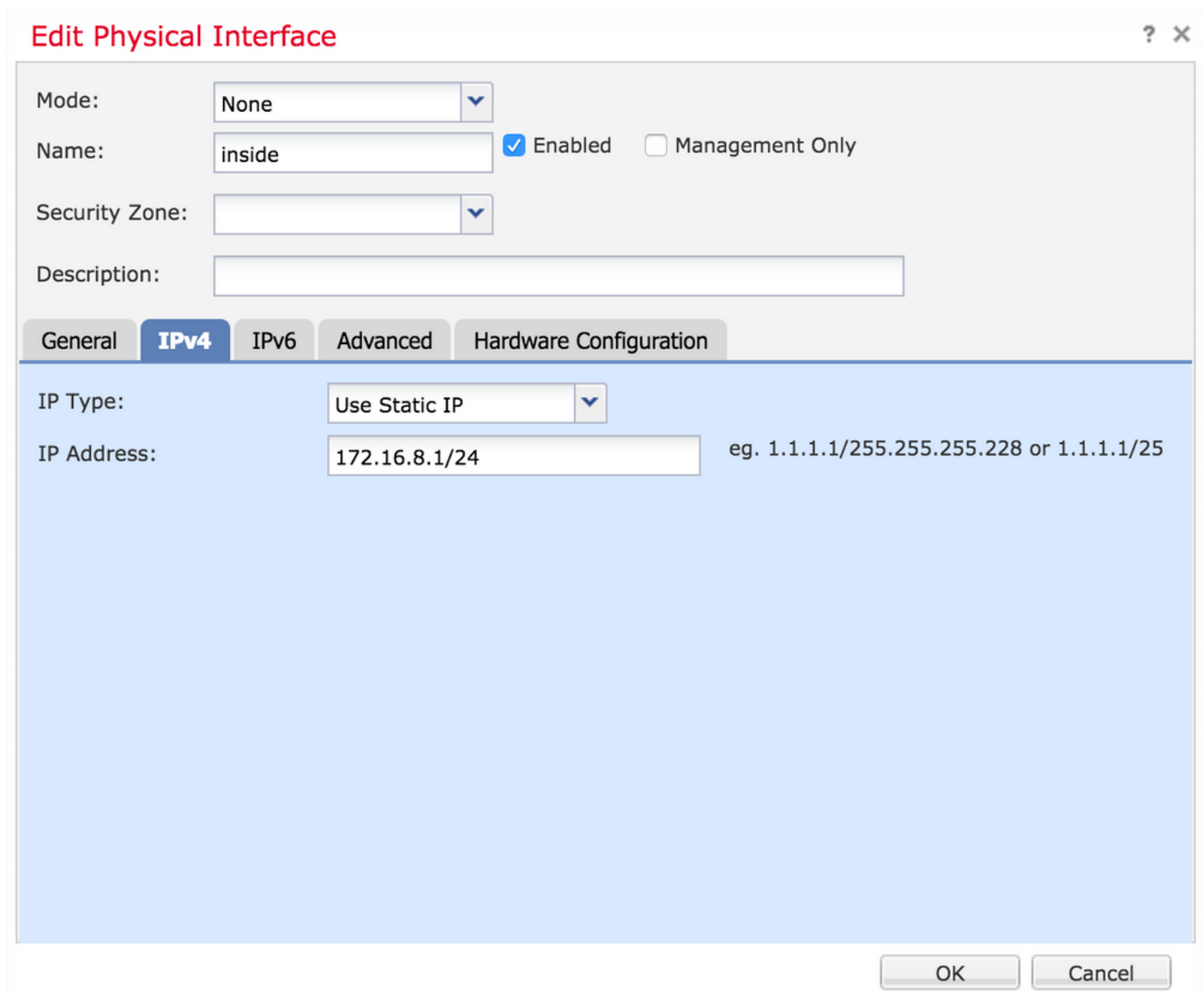
Paso 3. Vaya a la pestaña **Interfaces**.

Paso 4. Haga clic en el **icono del lápiz** para configurar/editar la interfaz para obtener acceso a la administración, como se muestra en la imagen:



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)

Paso 5. Seleccione la casilla de verificación **enable** para habilitar las interfaces. Vaya a la pestaña **IPv4**, elija el tipo de IP como **estático** o **DHCP**. Ahora ingrese una dirección IP para la interfaz y haga clic en **Aceptar**, como se muestra en la imagen:



### 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

Paso 6. Haga clic en **Guardar** y, a continuación, implemente la política en el FTD.

**Nota:** La interfaz de diagnóstico no se puede utilizar para acceder a la CLI convergente

sobre SSH en dispositivos con la versión de software 6.1.0

## Paso 2. Configuración de la autenticación externa.

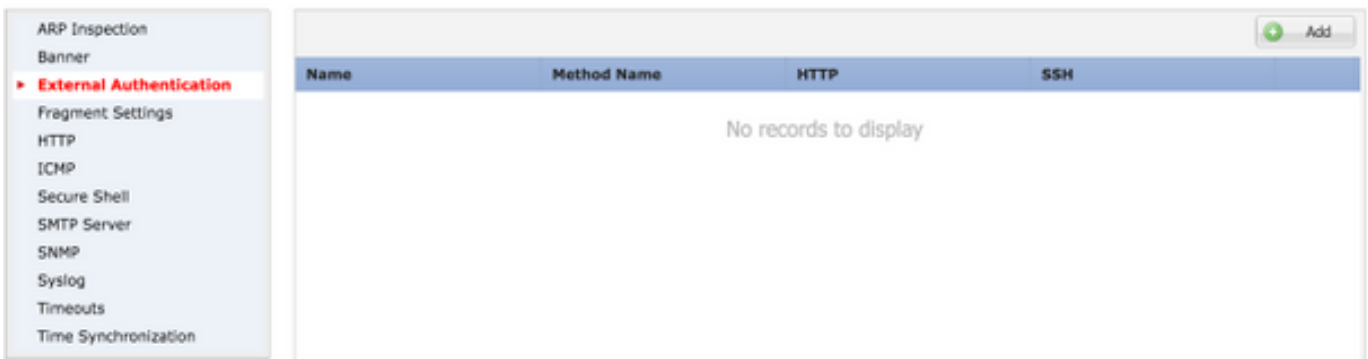
La autenticación externa facilita la integración de FTD en un Active Directory o servidor RADIUS para la autenticación de usuarios. Este es un paso necesario porque los usuarios configurados localmente no tienen acceso directo a la CLI de diagnóstico. A la CLI de diagnóstico y a la GUI sólo acceden los usuarios autenticados mediante el protocolo ligero de acceso a directorios (LDAP) o RADIUS.

Hay 6 pasos para configurar la autenticación externa.

Paso 1. Vaya a **Devices > Platform Settings**.

Paso 2. Puede editar la política que existe al hacer clic en el icono del lápiz o crear una nueva política FTD al hacer clic en el botón **Nueva política** y seleccionar tipo como **Configuración de Threat Defence**.

Paso 3. Vaya a la ficha **Autenticación externa**, como se muestra en la imagen:



Paso 4. Al hacer clic en **Agregar**, aparece un cuadro de diálogo como se muestra en la imagen:

- **Habilitar para HTTP** - Active esta opción para proporcionar acceso al FTD a través de HTTPS.
- **Enable for SSH** - Active esta opción para proporcionar acceso al FTD sobre SSH.
- **Name** - Introduzca el nombre para la conexión LDAP.
- **Description** - Introduzca una descripción opcional para el objeto External Authentication.
- **Dirección IP**: introduzca un objeto de red que almacena la IP del servidor de autenticación externo. Si no hay ningún objeto de red configurado, cree uno nuevo. Haga clic en el icono (+).

- **Authentication Method:** Seleccione RADIUS o el protocolo LDAP para la autenticación.
- **Habilitar SSL:** active esta opción para cifrar el tráfico de autenticación.
- **Tipo de servidor** - Seleccione el tipo de servidor. Los tipos de servidor conocidos son MS Active Directory, Sun, OpenLDAP y Novell. De forma predeterminada, la opción está configurada para detectar automáticamente el tipo de servidor.
- **Port** - Introduzca el puerto sobre el que se realiza la autenticación.
- **Tiempo de espera:** introduzca un valor de tiempo de espera para las solicitudes de autenticación.
- **DN base:** introduzca un DN base para proporcionar un ámbito dentro del cual el usuario pueda estar presente.
- **Ámbito LDAP** - Seleccione el alcance LDAP que desea buscar. El alcance se encuentra dentro del mismo nivel o dentro del subárbol.
- **Nombre de usuario** - Ingrese un nombre de usuario para enlazar al directorio LDAP.
- **Contraseña de autenticación:** introduzca la contraseña para este usuario.
- **Confirmar:** vuelva a introducir la contraseña.
- **Interfaces disponibles** - Se muestra una lista de interfaces disponibles en el FTD.
- **Zonas e interfaces seleccionadas** - Muestra una lista de interfaces desde las que se accede al servidor de autenticación.

Para la autenticación RADIUS, no hay tipo de servidor Base DN o Ámbito LDAP. El puerto es el puerto RADIUS 1645.

**Secreto** - Introduzca la clave secreta para RADIUS.

## Add External Authentication



Enable for HTTP

Enable for SSH

Name\*

Description

IP Address\*

Authentication Method

Enable SSL

Server Type

Port

Timeout  (0 - 300 Seconds)

Base DN   ex. dc=cisco,dc=com

Ldap Scope

Username  ex. cn=jsmith,dc=cisco,dc=com

Authentication Password

Confirm

**Available Zones**

**Selected Zones/Interfaces**

Paso 5. Una vez finalizada la configuración, haga clic en **Aceptar**.

Paso 6. Guarde la política e implémtela en el dispositivo Firepower Threat Defense.



**Nota:** La autenticación externa no se puede utilizar para acceder a la CLI convergente sobre SSH en dispositivos con la versión de software 6.1.0

### Paso 3. Configure el acceso SSH.

SSH proporciona acceso directo a la CLI convergente. Utilice esta opción para acceder directamente a la CLI y ejecutar los comandos debug. Esta sección describe cómo configurar SSH para acceder a la CLI de FTD.

**Nota:** En los dispositivos FTD que ejecutan la versión de software 6.0.1, la configuración SSH en Configuración de plataforma proporciona acceso a la CLI de diagnóstico directamente y no a CLISH. Debe conectarse a la dirección IP configurada en **br1** para acceder a CLISH. Sin embargo, en los dispositivos FTD que ejecutan la versión de software 6.1.0, todas las interfaces navegan a la CLI convergente cuando se accede a través de SSH

Hay 6 pasos para configurar SSH en el ASA

#### Solo en dispositivos 6.0.1:

Estos pasos se realizan en dispositivos FTD con una versión de software inferior a 6.1.0 y superior a 6.0.1. En los dispositivos 6.1.0, estos parámetros se heredan del sistema operativo.

Paso 1. Vaya a **Devices>Platform Settings**.

Paso 2. Puede editar la política que existe al hacer clic en el icono del lápiz o crear una nueva directiva de Firepower Threat Defense al hacer clic en el botón **Nueva política** y seleccionar tipo como **Configuración de Threat Defense**.

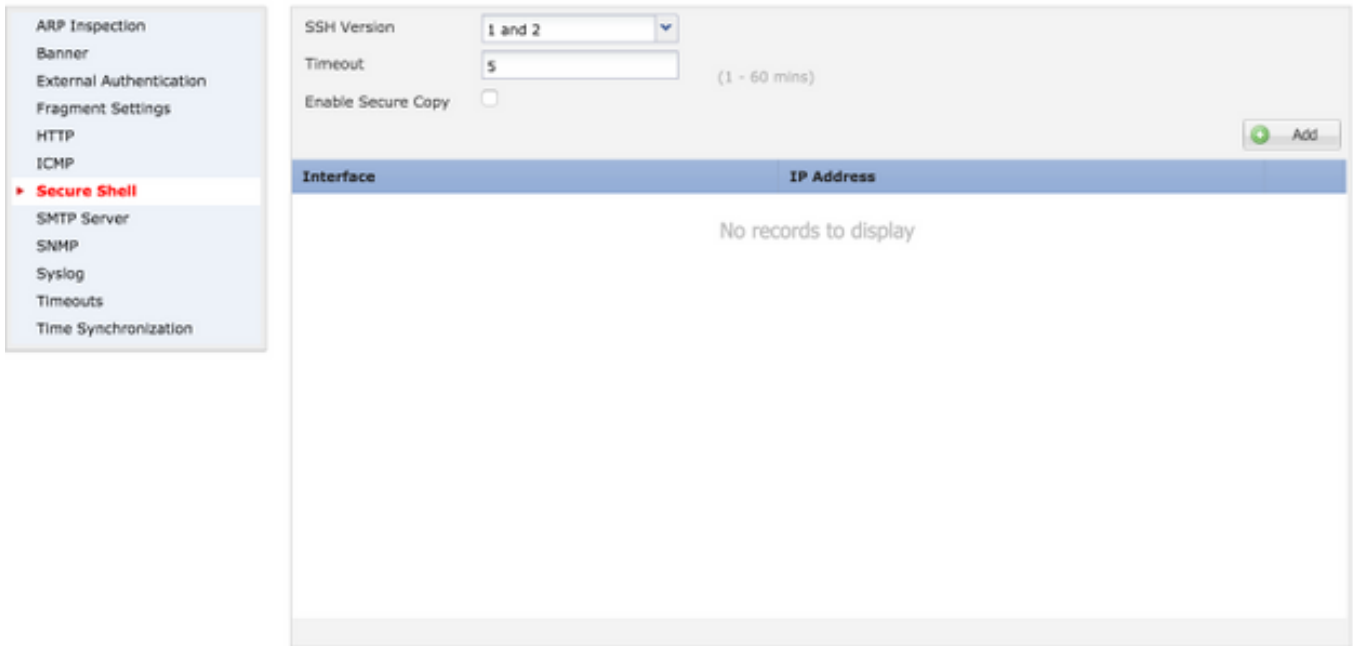
Paso 3. Vaya a la sección **Secure Shell**. Aparece una página, como se muestra en la imagen:

**Versión SSH:** Seleccione la versión de SSH que desea activar en el ASA. Hay tres opciones:

- **1:** Habilitar sólo SSH versión 1
- **2:** Habilitar sólo SSH versión 2
- **1 y 2:** Habilitar las versiones 1 y 2 de SSH

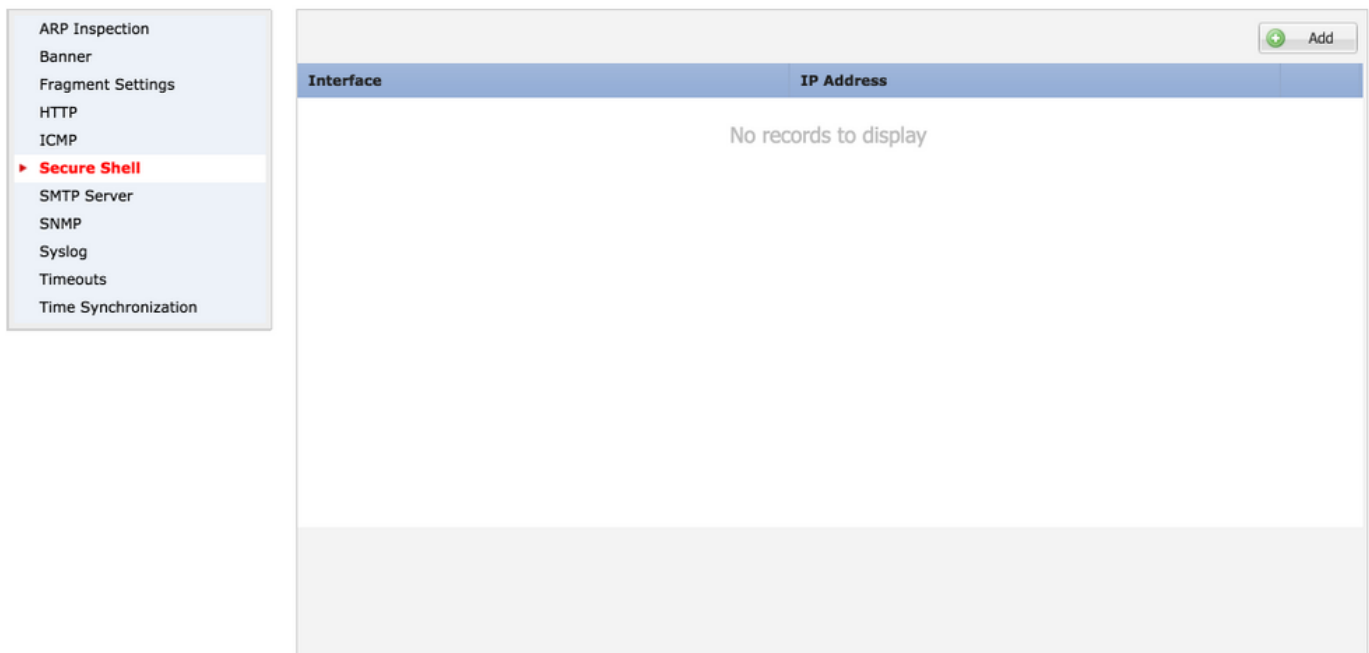
**timeout (tiempo de espera):** Introduzca el tiempo de espera SSH deseado en minutos.

**Enable Secure Copy** - Active esta opción para configurar el dispositivo para permitir conexiones Secure Copy (SCP) y actuar como servidor SCP.



### En los dispositivos 6.0.1 y 6.1.0:

Estos pasos se configuran para limitar el acceso de administración a través de SSH a interfaces específicas y a direcciones IP específicas.

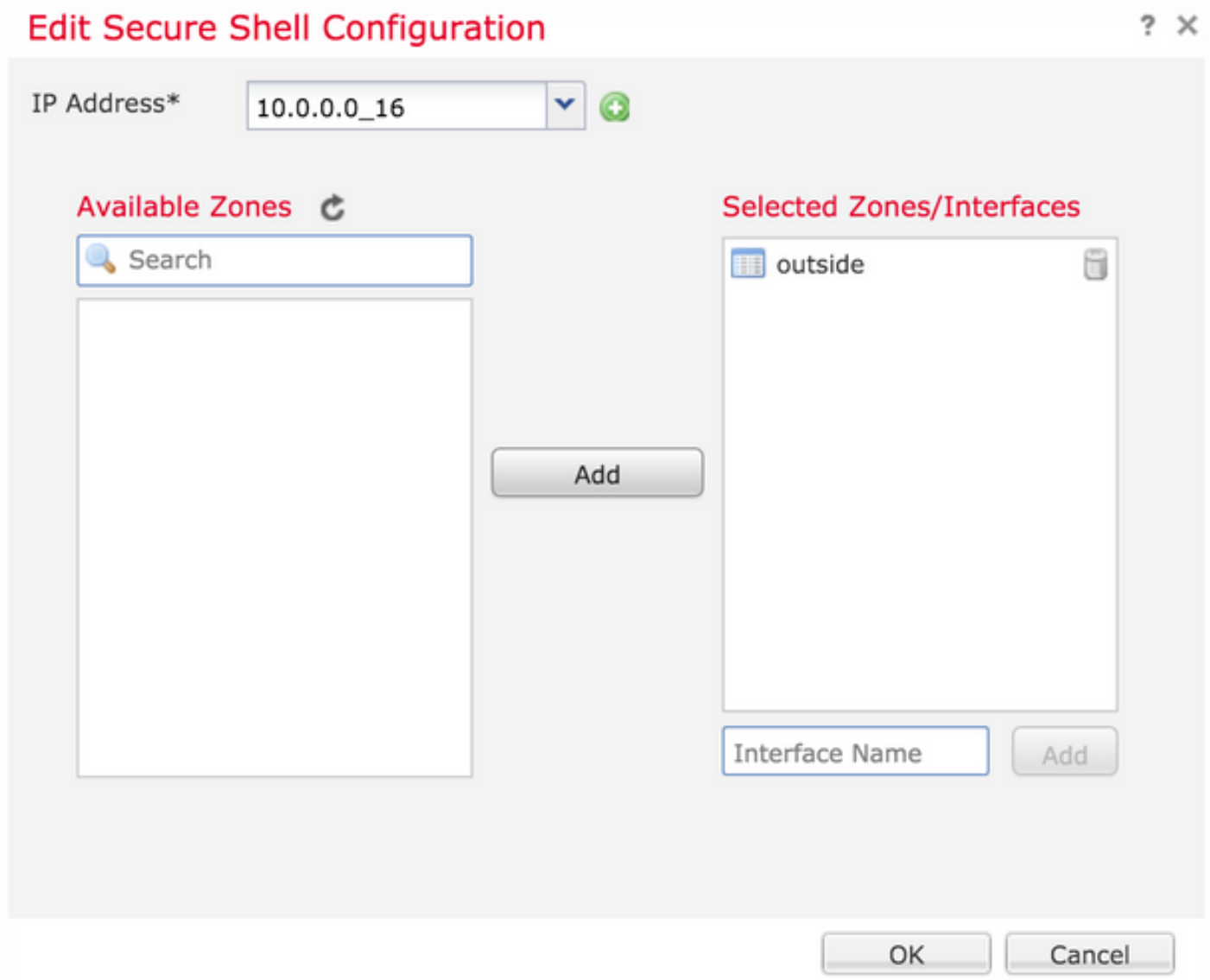


Paso 1. Haga clic en **Agregar** y configure estas opciones:

**Dirección IP:** Seleccione un objeto de red que contenga las subredes a las que se permite acceder a la CLI a través de SSH. Si no hay ningún objeto de red, cree uno al hacer clic en el icono (+).

**Zonas/interfaces seleccionadas:** Seleccione las zonas o interfaces desde las que se accede al servidor SSH.

Paso 2. Haga clic en **Aceptar**, como se muestra en la imagen:



La configuración para SSH se visualiza en la CLI convergente (ASA Diagnostic CLI en dispositivos 6.0.1) con el uso de este comando.

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

Paso 3. Una vez finalizada la configuración de SSH, haga clic en **Guardar** y luego implemente la política en el FTD.

#### Paso 4. Configure el acceso HTTPS.

Para habilitar el acceso HTTPS a una o más interfaces, navegue a la sección **HTTP** en la configuración de la plataforma. El acceso HTTPS es específicamente útil para descargar las capturas de paquetes de la interfaz web segura de diagnóstico directamente para el análisis.

Hay 6 pasos para configurar el acceso HTTPS.

Paso 1. Vaya a **Dispositivos > Configuración de la plataforma**

Paso 2. Puede editar la política de configuración de plataforma que existe al hacer clic en el **icono**

del lápiz junto a la política o crear una nueva política FTD al hacer clic en **Nueva política**. Seleccione el tipo como **Firepower Threat Defense**.

Paso 3. Cuando se desplaza a la sección **HTTP**, aparece una página como se muestra en la imagen.

**Habilitar servidor HTTP:** Active esta opción para habilitar el servidor HTTP en el FTD.

**Puerto:** Seleccione el puerto en el que el FTD acepta conexiones de administración.

## FTD-Policy

Enter a description

The screenshot shows the configuration page for the HTTP server in an FTD policy. On the left is a navigation menu with options: ARP Inspection, Banner, External Authentication, Fragment Settings, **HTTP** (highlighted), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main content area has a section for 'Enable HTTP Server' which is checked. Below it, the 'Port' is set to '443' with a note: '(Please don't use 80 or 1443)'. There is an 'Add' button with a green plus icon. Below this is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying 'No records to display'.

Paso 4. Haga clic en **Agregar** y la página aparecerá como se muestra en la imagen:

**Dirección IP:** introduzca las subredes que tienen permiso para tener acceso HTTPS a la interfaz de diagnóstico. Si no hay ningún objeto de red, cree uno y utilice la opción (+).

**Zonas/Interfaces seleccionadas** - Al igual que SSH, la configuración HTTPS necesita tener una interfaz configurada sobre la cual se pueda acceder a ella a través de HTTPS. Seleccione las zonas o la interfaz a las que se debe acceder al FTD a través de HTTPS.

## Edit HTTP Configuration



IP Address\* 10.0.0.0\_16

Available Zones

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

La configuración para HTTPS se ve en la CLI convergente (ASA Diagnostic CLI en dispositivos 6.0.1) y utiliza este comando.

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

Paso 5. Una vez realizada la configuración necesaria, seleccione **Aceptar**.

Paso 6. Una vez que se haya introducido toda la información necesaria, haga clic en **Guardar** y, a continuación, implemente la política en el dispositivo.

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshoot

Estos son los pasos básicos para resolver problemas de acceso a la administración en el FTD.

Paso 1. Asegúrese de que la interfaz esté habilitada y configurada con una dirección IP.

Paso 2. Asegúrese de que una Autenticación Externa funcione según lo configurado y su alcance desde la interfaz apropiada especificada en la sección **Autenticación Externa** de la **Configuración de Plataforma**.

Paso 3. Asegúrese de que el ruteo en el FTD sea preciso. En la versión 6.0.1 del software FTD, navegue hasta **CLI de diagnóstico de soporte del sistema**. Ejecute los comandos **show route** y **show route management-only** para ver las rutas para el FTD y las interfaces de administración respectivamente.

En la versión 6.1.0 del software FTD, ejecute los comandos directamente en la CLI convergente.

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)