Configuración del Acceso de administración a FTD (HTTPS y SSH) vía FMC

Contenido

Introducción

Este documento describe la configuración del Acceso de administración a una defensa de la amenaza de FirePOWER (FTD) (HTTPS y SSH) vía el centro de administración de FireSIGHT (FMC).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología de FirePOWER
- Conocimiento básico de ASA (dispositivo de seguridad adaptante)
- Conocimiento del Acceso de administración en el ASA vía HTTPS y SSH (shell seguro)

Componentes Utilizados

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

- Imagen adaptante de la defensa de la amenaza de FirePOWER del dispositivo de seguridad (ASA) para el ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), que se ejecuta en la versión de software 6.0.1 y arriba
- Imagen de la defensa de la amenaza ASA FirePOWER para el 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 arriba
- Versión 6.0.1 y posterior del centro de administración de FirePOWER (FMC)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Con el inicio de la defensa de la amenaza de FirePOWER (FTD), la configuración relacionada entera ASA se hace en el GUI.

En los dispositivos FTD que funcionan con la versión de software 6.0.1, se accede el ASA CLI de diagnóstico mientras que usted ingresa el **soporte de sistema de diagnóstico-CLI**. Sin embargo, en los dispositivos FTD que funcionan con la versión de software 6.1.0, se converge el CLI y los comandos enteros ASA se configuran en el 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 tener el Acceso de administración directamente de una red externa, usted debe configurar el Acceso de administración vía el HTTPS o SSH. Este documento proporciona la configuración necesaria requerida para tener el Acceso de administración sobre SSH o el HTTPS externamente.

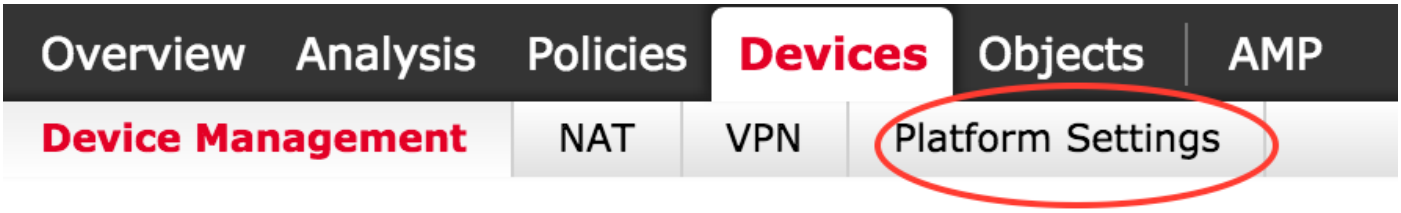
> **Note**: En los dispositivos FTD que funcionan con la versión de software 6.0.1, el CLI no se puede acceder por un usuario local, una autenticación externa se debe configurar para autenticar a los usuarios. Sin embargo, en los dispositivos FTD que funcionan con la versión de software 6.1.0, el CLI es accedido por el usuario del admin local mientras que una autenticación externa se requiere para el resto de los usuarios

> **Note**: En los dispositivos FTD que funcionan con la versión de software 6.0.1, el CLI de diagnóstico no es directamente accesible sobre el IP que se configura para **br1 del** FTD. Sin embargo, en los dispositivos FTD que funcionan con la versión de software 6.1.0, el CLI convergido es accesible sobre cualquier interfaz configurada para el Acceso de

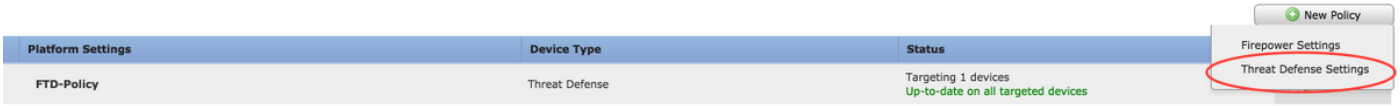
administración, sin embargo, la interfaz se debe configurar con una dirección IP.

Configurar

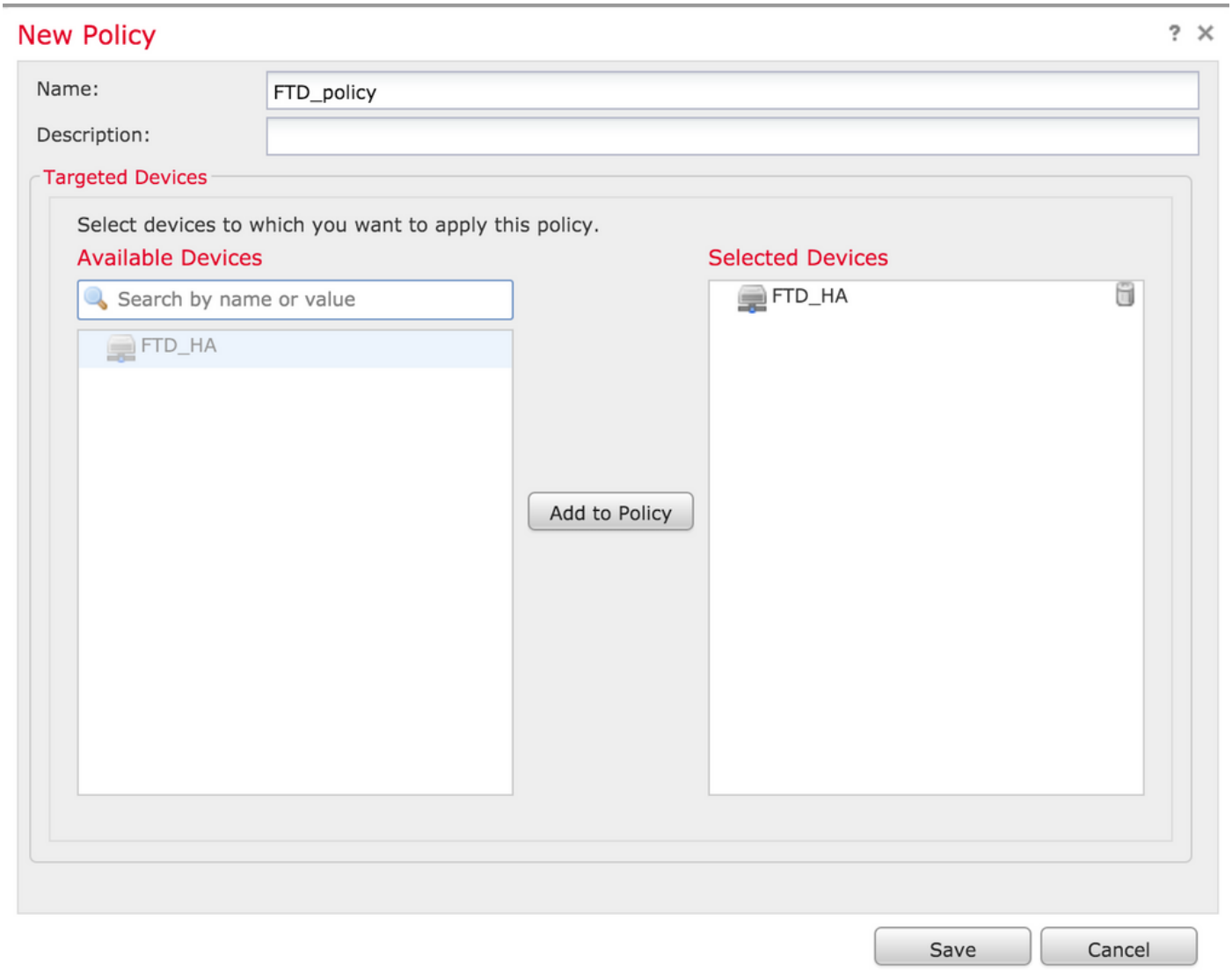
Toda la configuración relacionada del Acceso de administración se configura como usted navega a la lengueta de las **configuraciones de la plataforma** en los **dispositivos**, tal y como se muestra en de la imagen:



Cualquiera edita la directiva que existe mientras que usted hace clic en el icono del lápiz o crea una nueva directiva FTD como usted hace clic el **nuevo** botón de la **directiva** y selecciona el tipo como **configuraciones de la defensa de la amenaza**, tal y como se muestra en de la imagen:



Seleccione el dispositivo FTD para aplicar esta directiva y para hacer clic la **salvaguardia**, tal y como se muestra en de la imagen:



Configure el Acceso de administración

Éstos son los cuatro pasos principales tomados para configurar el Acceso de administración.

Paso 1. IP de la configuración en la interfaz FTD vía FMC GUI.

Configure un IP en la interfaz sobre la cual el FTD es accesible vía SSH o el HTTPS. Edite las interfaces que existen mientras que usted navega a la lengueta de las **interfaces del** FTD.

> **Note**: En los dispositivos FTD que funcionan con 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 funcionan con la versión de software 6.1.0, todas las interfaces soportan el Acceso de administración excepto la interfaz de diagnóstico.

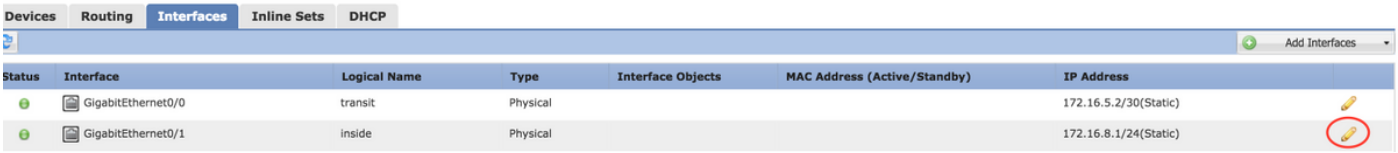
Hay seis pasos para configurar la interfaz de diagnóstico.

Paso 1. Navegue al **dispositivo > a la Administración de dispositivos.**

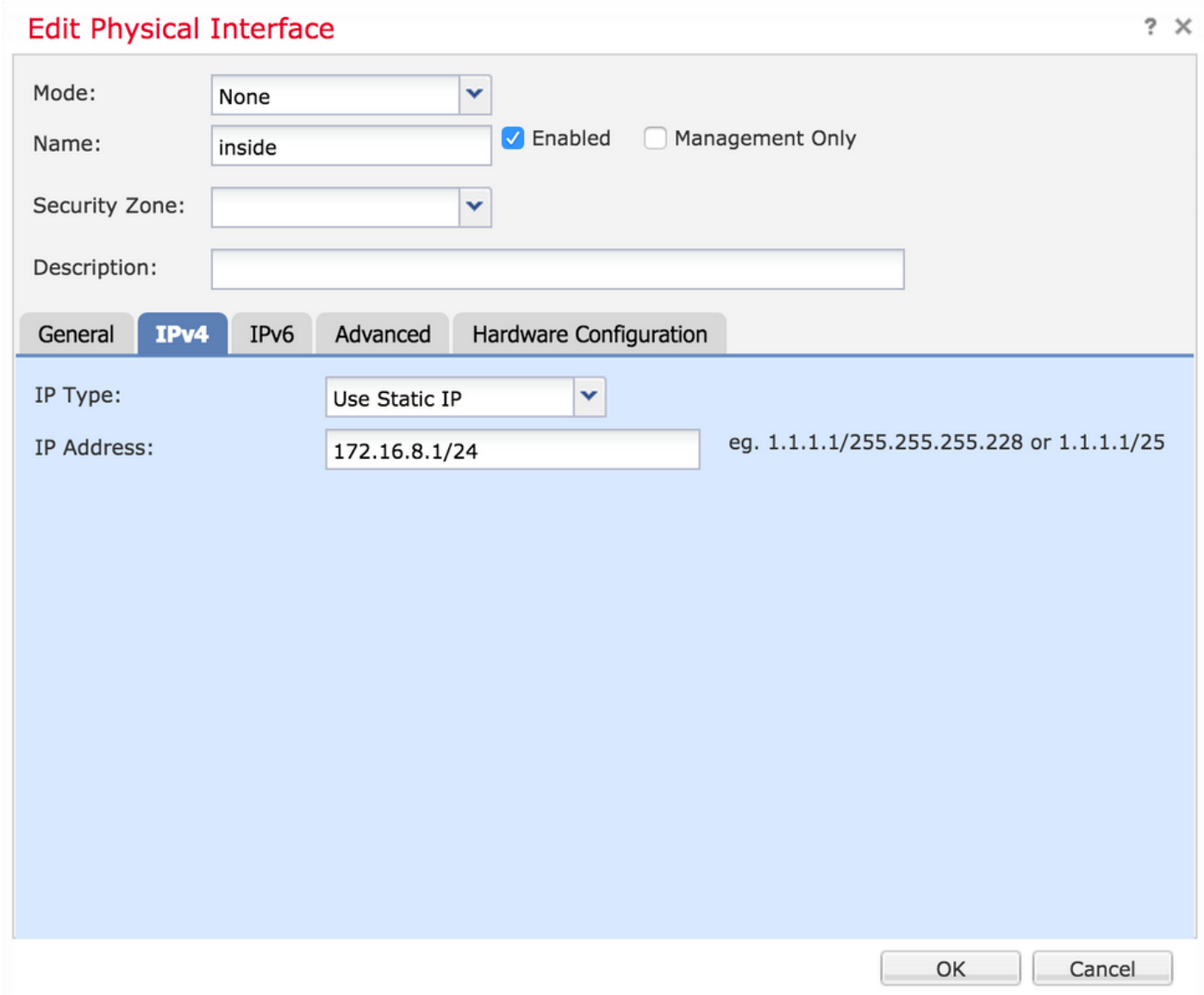
Paso 2. Seleccione el dispositivo o el cluster FTD HA.

Paso 3. Navegue a la lengueta de las **interfaces**.

Paso 4. Haga clic el **icono del lápiz** para configurar/edite la interfaz para tener el Acceso de administración, tal y como se muestra en de la imagen:



Paso 5. Seleccione el checkbox del **permiso** para habilitar las interfaces. Navegue a la lengueta **Ipv4**, elija el tipo IP como los **parásitos atmosféricos o DHCP**. Ahora ingrese un IP Address para la interfaz y haga clic la **AUTORIZACIÓN**, tal y como se muestra en de la imagen:



Paso 6. Haga clic la **salvaguardia** y después despliegue la directiva al FTD.

Note: La interfaz de diagnóstico no se puede utilizar para acceder el CLI convergido sobre

SSH en los dispositivos con la versión de software 6.1.0

Paso 2. Autenticación externa de la configuración.

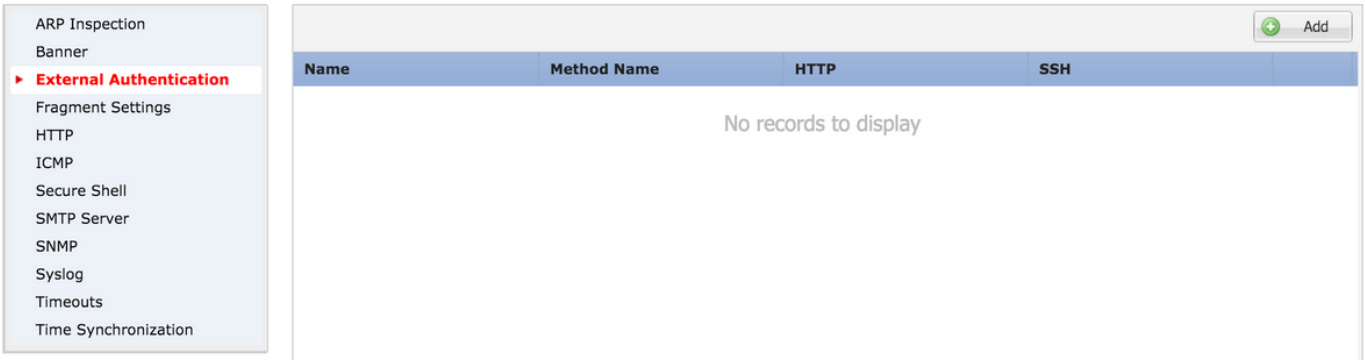
La autenticación externa facilita la integración del FTD a un Active Directory o a un servidor de RADIUS para la autenticación de usuario. Esto es un paso necesario porque los usuarios localmente configurados no tienen acceso directo al CLI de diagnóstico. El CLI de diagnóstico y el GUI son accedidos solamente por los usuarios que se autentican vía el Lightweight Directory Access Protocol (LDAP) o el RADIUS.

Hay 6 pasos para configurar la autenticación externa.

Paso 1. Navegue a los **dispositivos > a las configuraciones de la plataforma.**

Paso 2. Cualquiera edita la directiva que existe mientras que usted hace clic en el icono del lápiz o crea una nueva directiva FTD mientras que usted hace clic el **nuevo** botón de la **directiva** y selecciona el tipo como **configuraciones de la defensa de la amenaza.**

Paso 3. Navegue a la lengueta de la **autenticación externa**, tal y como se muestra en de la imagen:



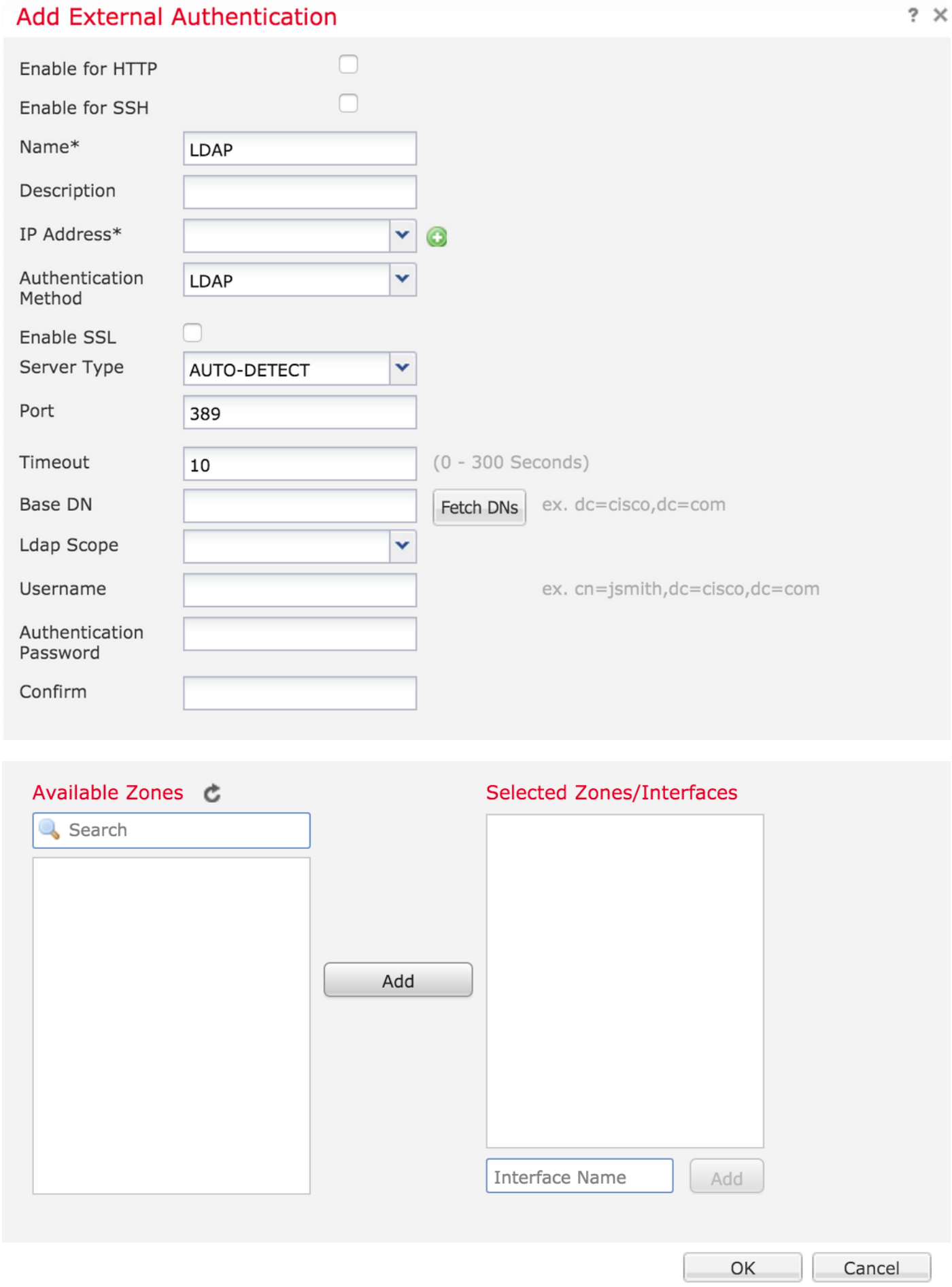
Paso 4. Como usted hace clic en **agregue**, un cuadro de diálogo aparece tal y como se muestra en de la imagen:

- **Permiso para el** permiso **HTTP** esta opción para proporcionar el acceso el FTD sobre el HTTPS.
- **Permiso para el** permiso **SSH-** esta opción para proporcionar el acceso el FTD sobre SSH.
- **El nombre** ingresa el nombre para la conexión LDAP.
- **La descripción** ingresa una descripción opcional para el objeto de la autenticación externa.
- **El direccionamiento IP** ingresa un objeto de red que salve el IP del servidor de autenticación externa. Si hay no se configura ningún objeto de red crea un nuevo haciendo clic en **(+) el** icono.

- **Autenticación** RADIUS Método-**selecto** o protocolo LDAP para la autenticación.
- **Permita al SSL-permiso** esta opción para cifrar el tráfico de la autenticación.
- **El tipo de servidor** selecciona el tipo de servidor. Los tipos de servidor bien conocidos son Active Directory, Sun, OpenLDAP y Novell MS. Por abandono, la opción se fija auto-para detectar el tipo de servidor.
- **El puerto** ingresa el puerto sobre el cual la autenticación ocurre.
- **El descanso** ingresa un valor de agotamiento del tiempo para los pedidos de autenticación.
- **La base DN** ingresa una base DN para proporcionar un alcance dentro del cual el usuario deba estar presente.
- **El alcance LDAP** selecciona el alcance LDAP para mirar. El alcance está dentro del mismo nivel o mirar dentro de la sub-estructura.
- **Username** ingrese un nombre de usuario para atar al directorio LDAP.
- **La autenticación contraseña-ingresa la** contraseña para este usuario.
- **Confirme** entran la contraseña de nuevo.
- **Disponible interconecta la** lista A de interfaces disponibles en el FTD se visualiza.
- **Las zonas seleccionadas e interconectan** esto muestran una lista de interfaces sobre de la cual accedan al servidor de autenticación.

Para la autenticación de RADIUS, no hay base DN del tipo de servidor o alcance LDAP. El puerto es el puerto RADIUS 1645.

El secreto ingresa la clave secreta para el RADIO.



Paso 5. Una vez que se hace la configuración, haga clic la **AUTORIZACIÓN.**

Paso 6. Salve la directiva y despliegúela al dispositivo de la defensa de la amenaza de

FirePOWER.

> **Note**: La autenticación externa no se puede utilizar para acceder el CLI convergido sobre SSH en los dispositivos con la versión de software 6.1.0

Paso 3. Acceso de SSH de la configuración.

SSH proporciona el acceso directo al CLI convergido. Utilice esta opción para acceder directamente el CLI y para funcionar con los comandos debug. Esta sección describe cómo configurar SSH para acceder el FTD CLI.

> **Note**: En los dispositivos FTD que funcionan con la versión de software 6.0.1, la configuración SSH en las configuraciones de la plataforma proporciona el acceso al CLI de diagnóstico directamente y no el CLISH. Usted necesita conectar con el IP Address configurado en **br1** para acceder el CLISH. Sin embargo, en los dispositivos FTD que funcionan con la versión de software 6.1.0, todas las interfaces navegan al CLI convergido cuando están accedidas sobre SSH

Hay 6 pasos para configurar SSH en el ASA

En 6.0.1 dispositivos solamente:

Estos pasos se realizan en los dispositivos FTD con la versión de software menos de 6.1.0 y mayor de 6.0.1. En 6.1.0 dispositivos estos parámetros se heredan del OS.

Paso 1. Navegue a las **configuraciones de Devices>Platform.**

Paso 2. Cualquiera edita la directiva que existe mientras que usted hace clic en el icono del lápiz o crea una nueva directiva de defensa de la amenaza de FirePOWER mientras que usted hace clic el **nuevo** botón de la **directiva** y selecciona el tipo como **configuraciones de la defensa de la amenaza.**

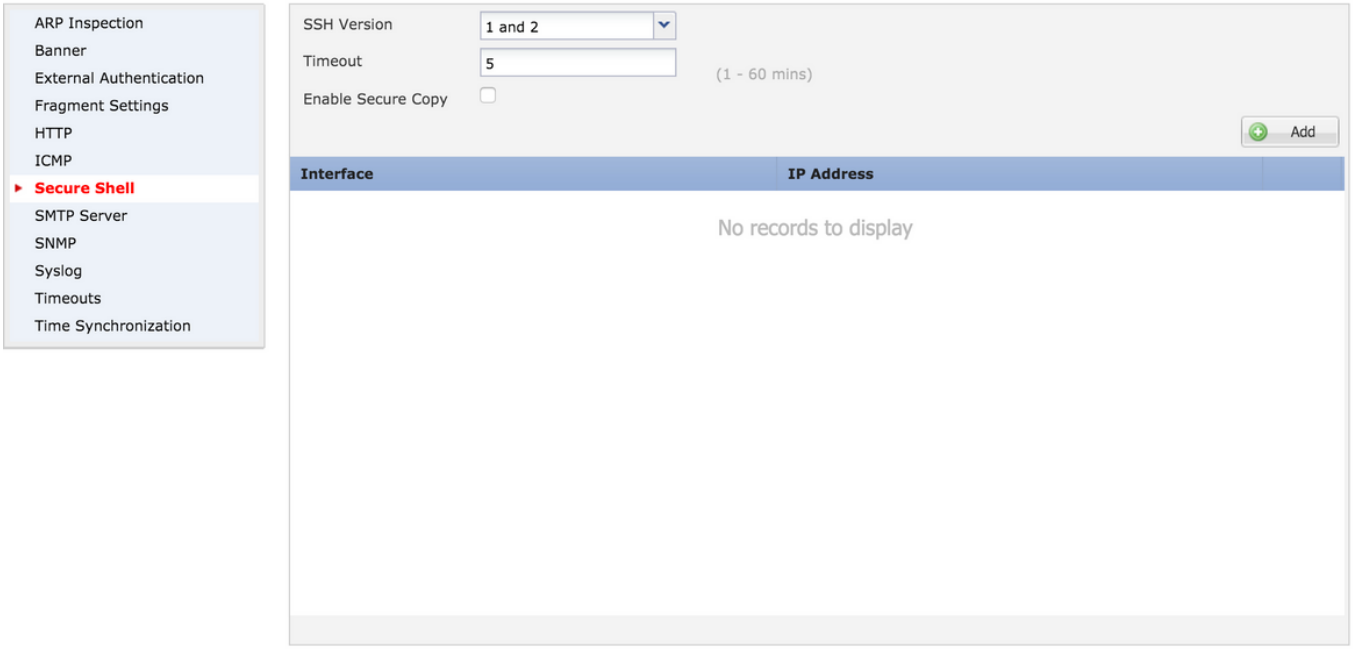
Paso 3. Navegue a la sección del **shell seguro**. Una página aparece, tal y como se muestra en de la imagen:

SSH versión: Seleccione el SSH versión para habilitar en el ASA. Hay tres opciones:

- **1:** SSH versión 1 del permiso solamente
- **2:** SSH versión 2 del permiso solamente
- **1 y 2:** Habilite el SSH versión 1 y 2

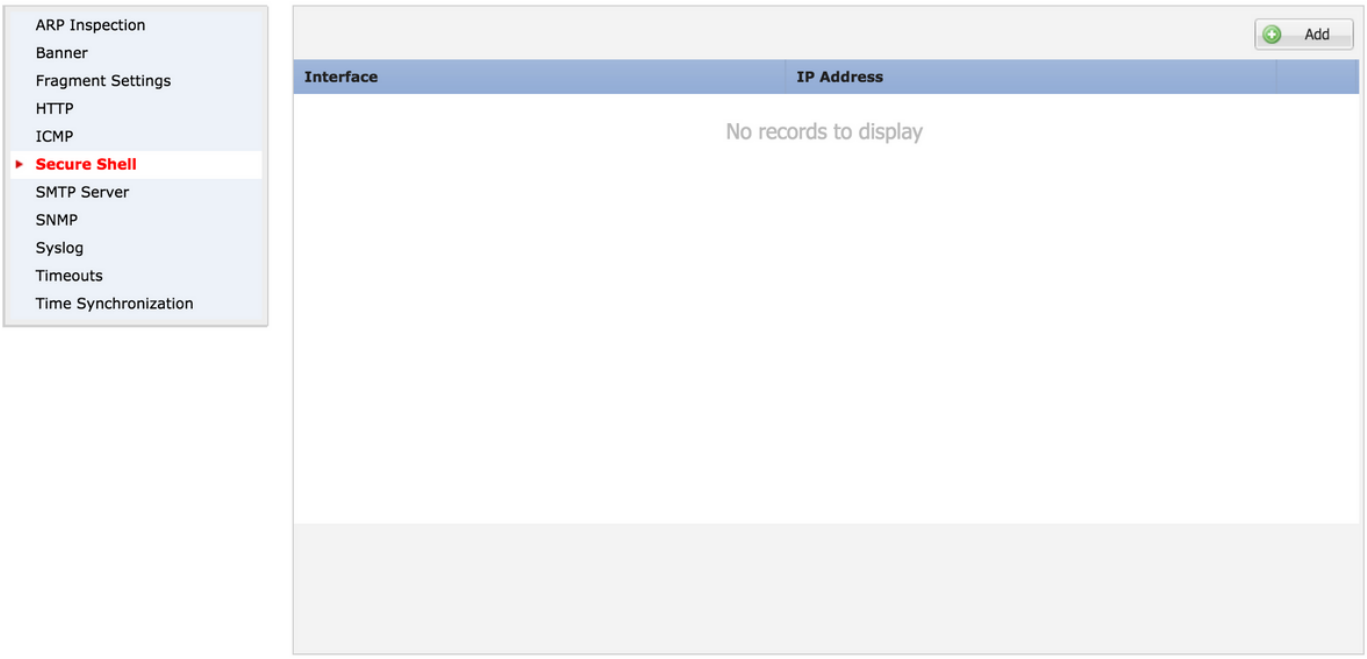
Descanso: Ingrese el tiempo de espera agotado de SSH deseado en los minutos.

Permita al permiso **seguro de la copia** esta opción para configurar el dispositivo para permitir las conexiones seguras de Copy(SCP) y para actuar como servidor de SCP.



En 6.0.1 y 6.1.0 dispositivos:

Estos pasos se configuran para limitar el Acceso de administración vía SSH a las interfaces específicas y a los IP Addresses específicos.

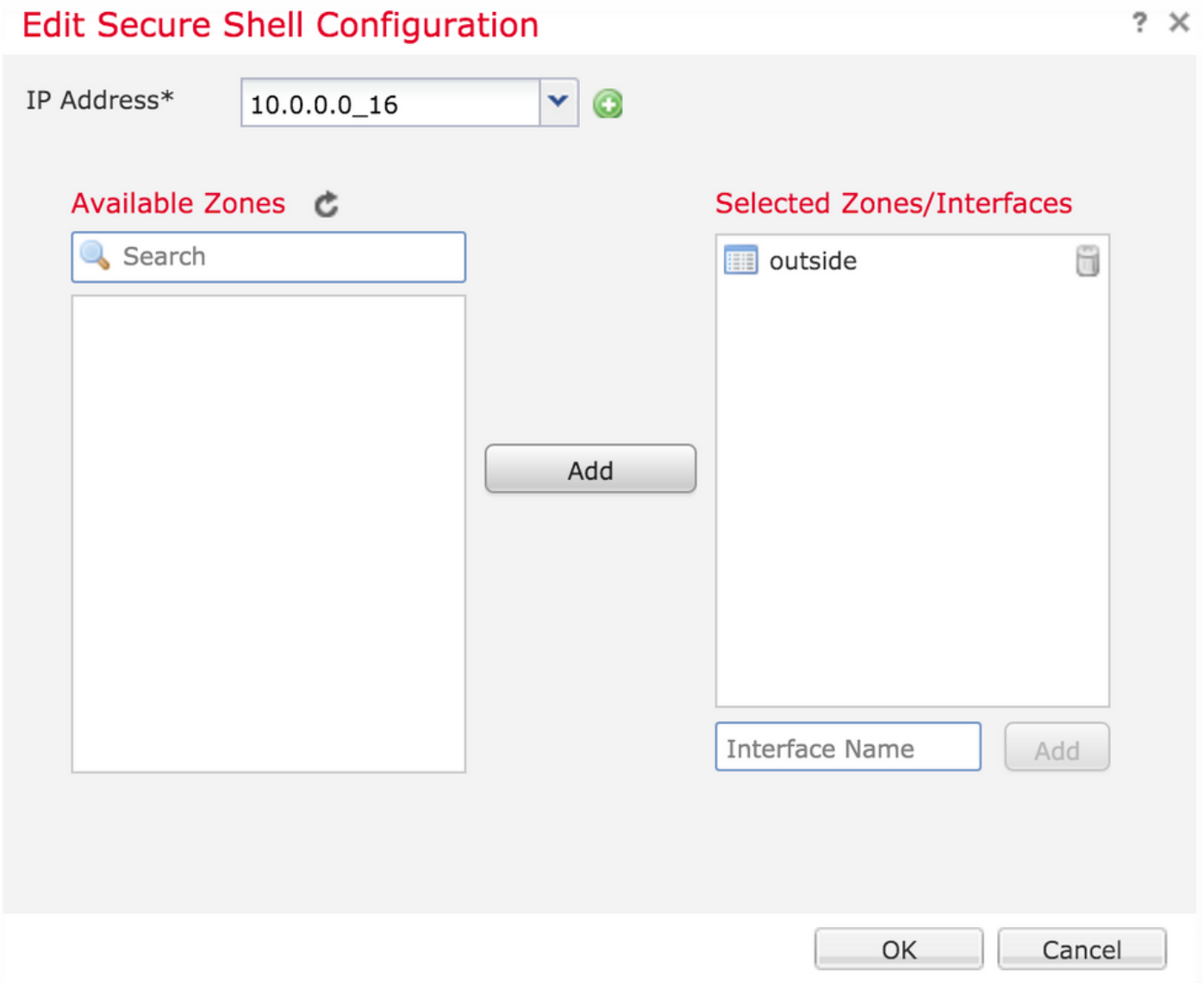


Paso 1. Haga clic **agregan** y configuran estas opciones:

Dirección IP: Seleccione un objeto de red que contenga las subredes que se permiten acceder el CLI sobre SSH. Si un objeto de red no está presente, cree uno como usted hace clic en **(+) el** icono.

Zonas/interfaces seleccionadas: Seleccione las zonas o las interfaces sobre de las cuales acceden al servidor SSH.

Paso 2. Haga Click en OK, tal y como se muestra en de la imagen:



La configuración para SSH se ve en el CLI convergido (ASA CLI de diagnóstico en 6.0.1 dispositivos) usando este comando.

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

Paso 3. Una vez que se hace la configuración SSH, haga clic la **salvaguardia** y después despliegue la directiva al FTD.

Paso 4. Acceso de la configuración HTTPS.

Para habilitar el acceso HTTPS a una o más interfaces, navegue a la sección **HTTP** en las configuraciones de la plataforma. El acceso HTTPS es específicamente útil para descargar a 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. Navegue a los **dispositivos > a las configuraciones de la plataforma**

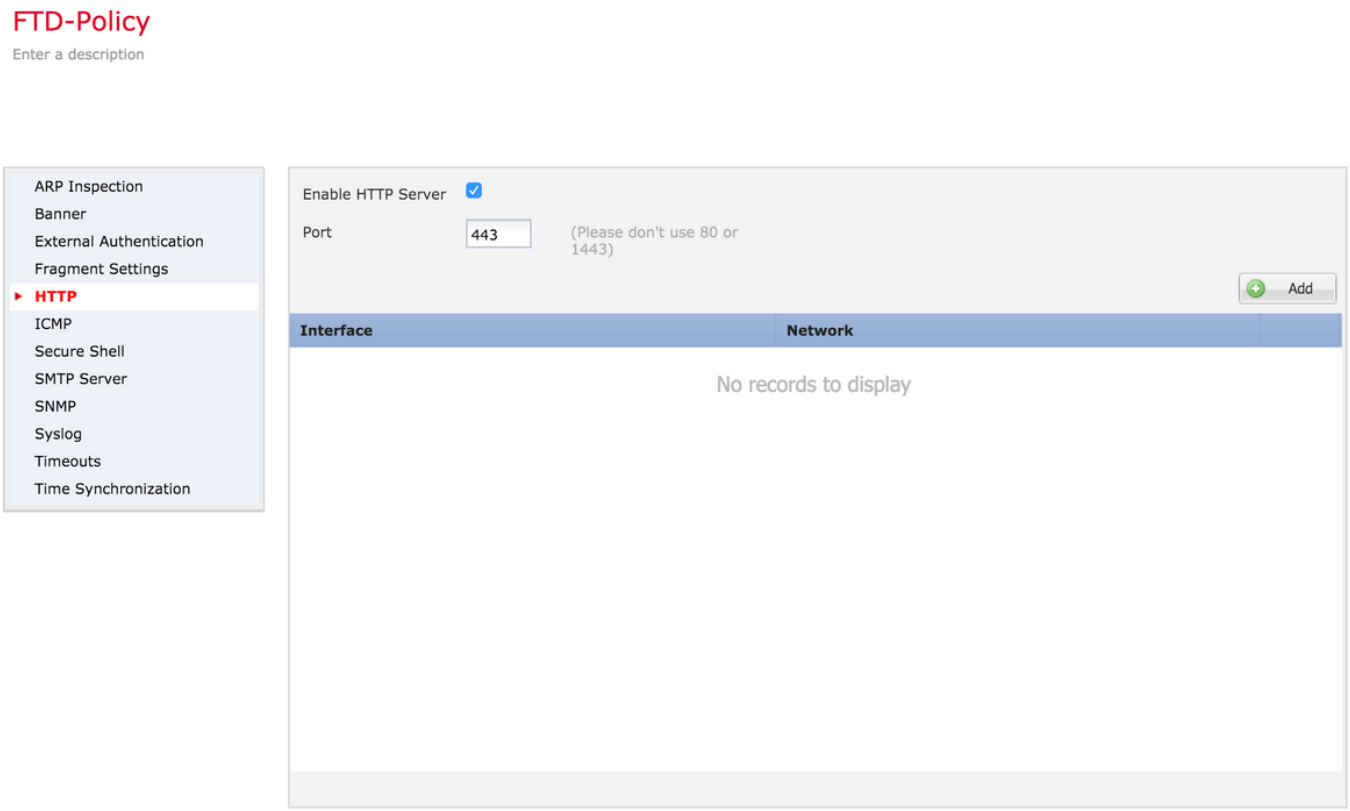
Paso 2. Cualquiera edita la directiva de las configuraciones de la plataforma que existe mientras

que usted hace clic el **icono del lápiz** al lado de la directiva o crea una nueva directiva FTD mientras que usted hace clic la **nueva directiva**. Seleccione el tipo como **defensa de la amenaza de FirePOWER.**

Paso 3. Mientras que usted navega a la sección **HTTP**, una página aparece tal y como se muestra en de la imagen.

Servidor HTTP del permiso: Permita a esta opción para hacer para habilitar al servidor HTTP en el FTD.

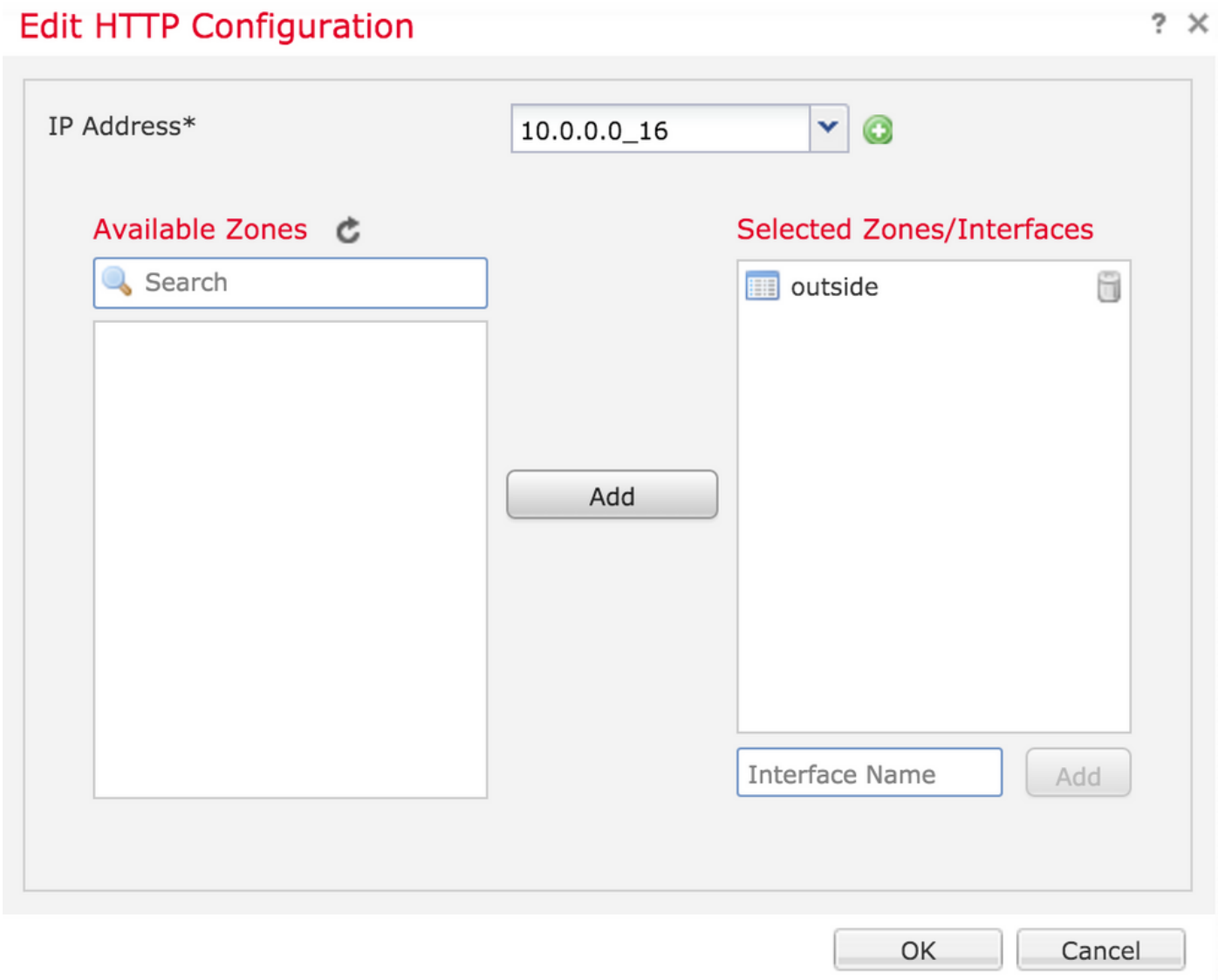
Puerto: Seleccione el puerto en el cual el FTD valida las Conexiones de Administración.



El paso 4.Click **agrega** y el apage aparece tal y como se muestra en de la imagen:

El direccionamiento IP ingresa las subredes que se permiten tener acceso HTTPS a la interfaz de diagnóstico. Si un objeto de red no está presente cree uno usando **(+) la** opción.

Las zonas/los interfaces seleccionados similares a SSH, configuración HTTPS necesitan tener una interfaz configurada sobre cuál es accesible vía el HTTPS. Seleccione las zonas o la interfaz sobre las cuales el FTD debe ser accedido vía el HTTPS.



La configuración para el HTTPS se ve en el CLI convergido (ASA CLI de diagnóstico en 6.0.1 dispositivos) usando este comando.

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

Paso 5. Una vez que la configuración necesaria es **AUTORIZACIÓN** selecta hecha**.**

Paso 6. Una vez que toda la Información requerida ha sido **salvaguardia** ingresada del tecleo y entonces despliegue la directiva al dispositivo.

Verificación

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

Troubleshooting

Éstos son los pasos básicos para resolver problemas el problema del Acceso de 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 trabaje según lo configurado y su accesibilidad de la interfaz apropiada especificado en la sección de la **autenticación externa de las configuraciones de la plataforma**.

Paso 3. Asegúrese que la encaminamiento en el FTD sea exacta. En la versión de software 6.0.1 FTD, navegue al **soporte de sistema de diagnóstico-CLI.** Funcione con los comandos show route y **muestre la Administración-solamente de la ruta** para ver las rutas para el FTD y las interfaces de administración respectivamente.

En la versión de software 6.1.0 FTD, funcione con los comandos directamente en el CLI convergido.

Información Relacionada

- Guía de inicio rápido de la defensa de la amenaza de Cisco FirePOWER para el ASA
- Soporte Técnico y Documentación - Cisco Systems