Configuración del acceso a la gestión para SSH y HTTPS en FTD mediante FDM

Contenido

Introducción

Este documento describe el procedimiento para configurar y verificar la lista de acceso de administración para SSH y HTTPS en FTD administrado localmente o remoto.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

- Cisco Secure Firewall Threat Defence con la versión 7.4.1 gestionada por FDM.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

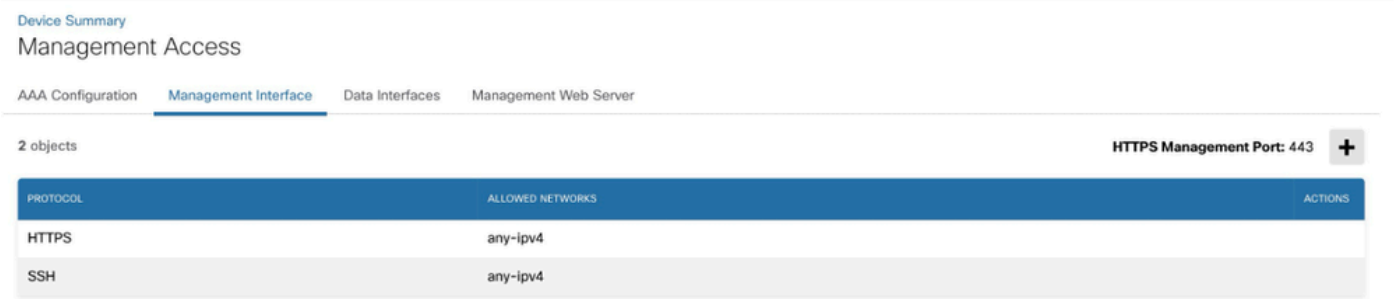
Configurar

El FTD se puede gestionar localmente mediante FDM o mediante FMC. En este documento, se hace hincapié en el acceso a la gestión a través de FDM y CLI. Con CLI, puede realizar cambios para FDM y FMC de escenario.

Precaución: Configure las listas de acceso SSH o HTTPS de una en una para evitar el bloqueo de sesiones. En primer lugar, actualice e implemente un protocolo, verifique el acceso y, a continuación, continúe con el otro.

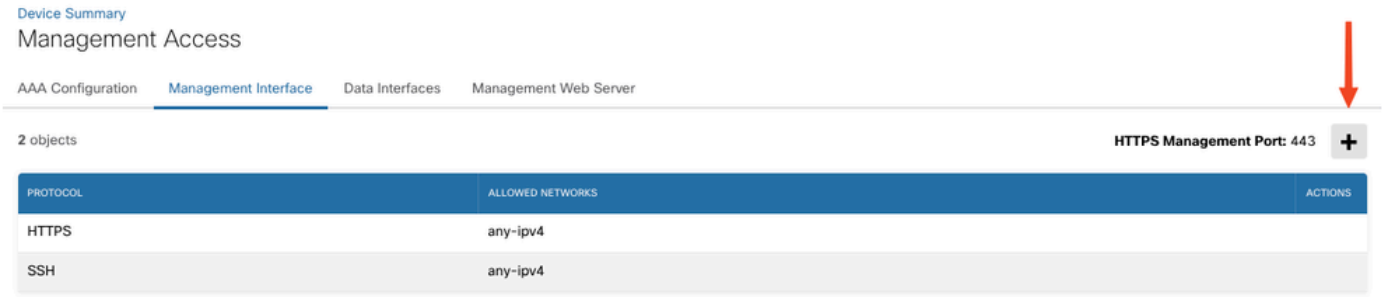
Pasos de FDM:

Paso 1: Inicie sesión en Firepower Device Manager (FDM) y navegue hasta System Settings > Management Access > Management Interface .



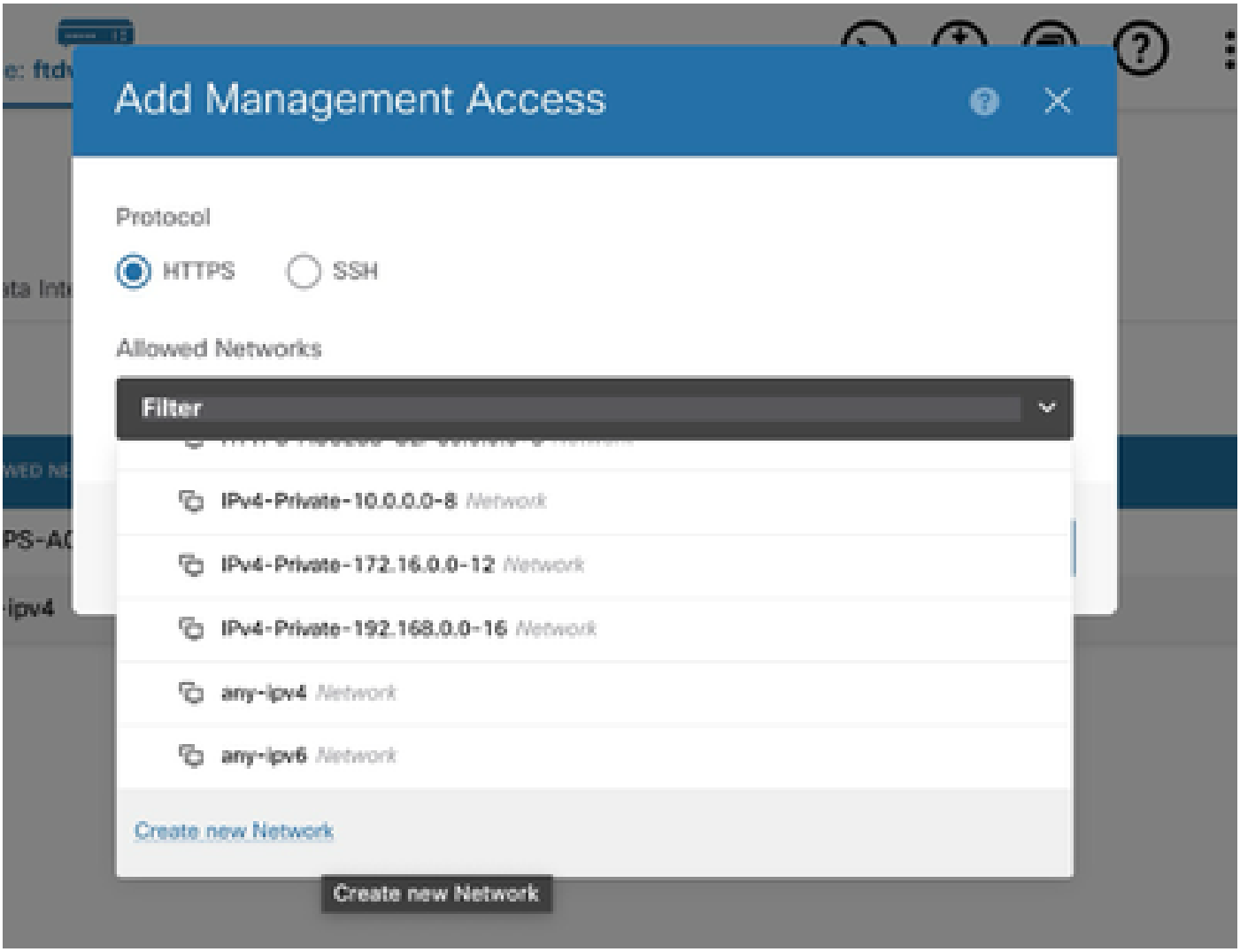
De forma predeterminada, se permite cualquier acceso a ipv4 en el puerto de administración para SSH y HTTPS

Paso 2: Haga clic en el + icono para abrir la ventana para agregar la red.



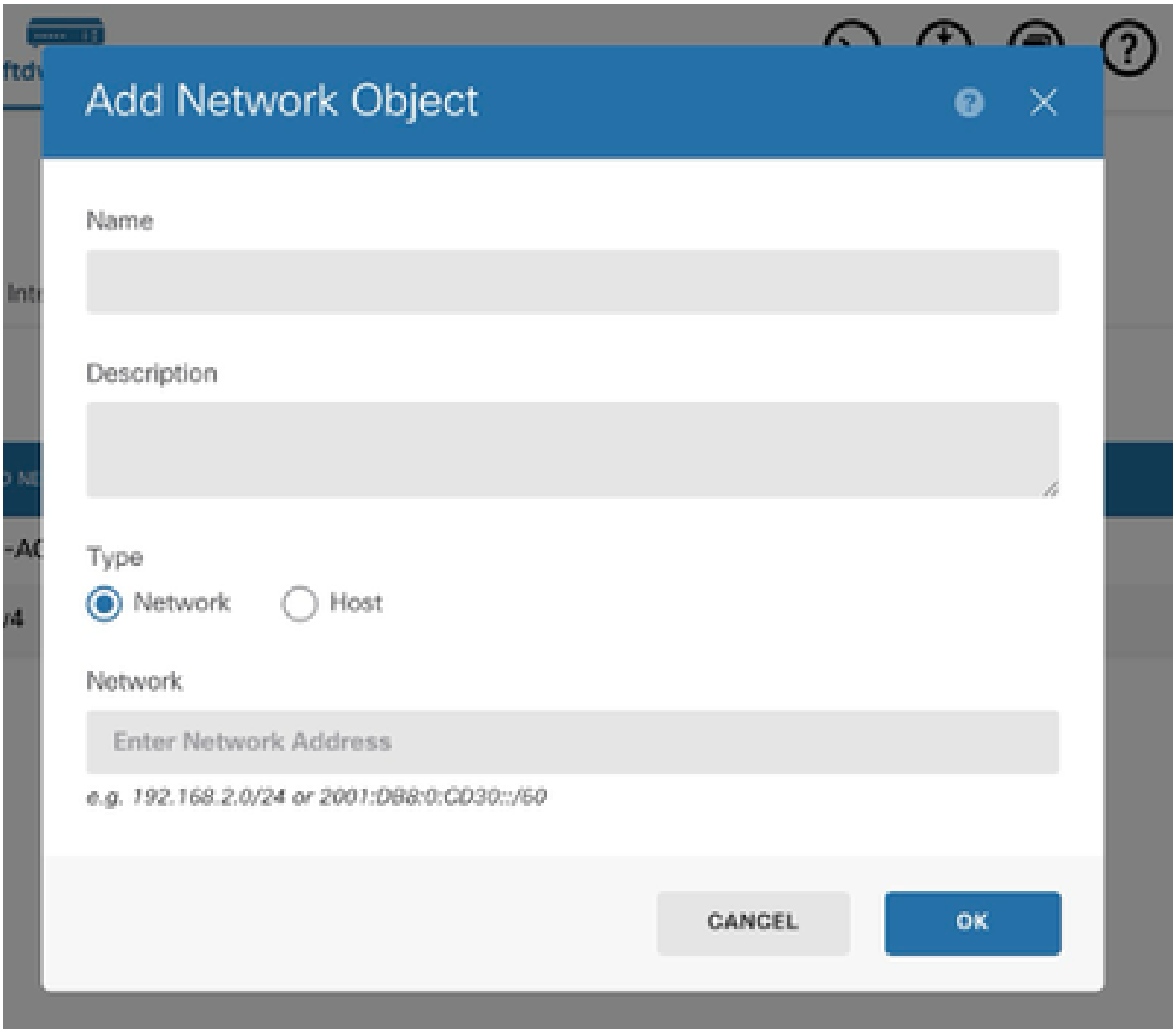
Haga clic en el botón Agregar de la parte superior derecha.

Paso 3: Agregue el objeto de red para tener acceso SSH o HTTPS. Si necesita crear una red nueva, seleccione la opción Create new Network. Puede agregar varias entradas para las redes o el host en el acceso de administración.



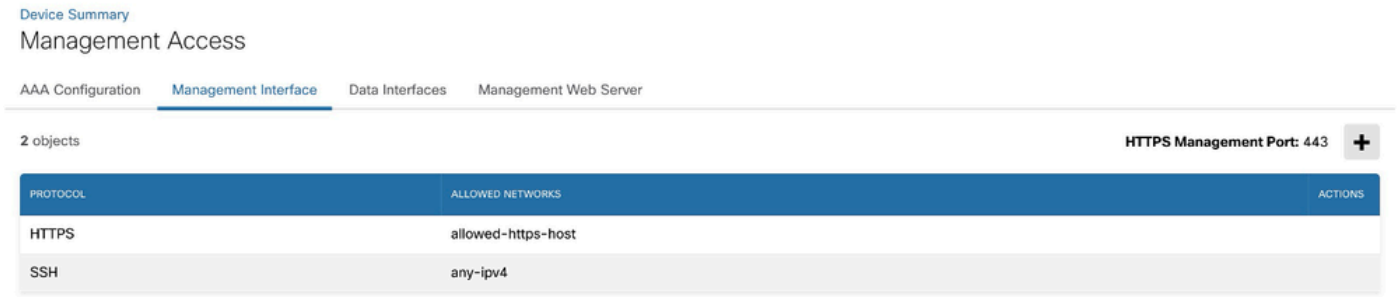
Seleccione la red.

Paso 4 (opcional): La opción Crear nueva red abre la ventana Agregar objeto de red.

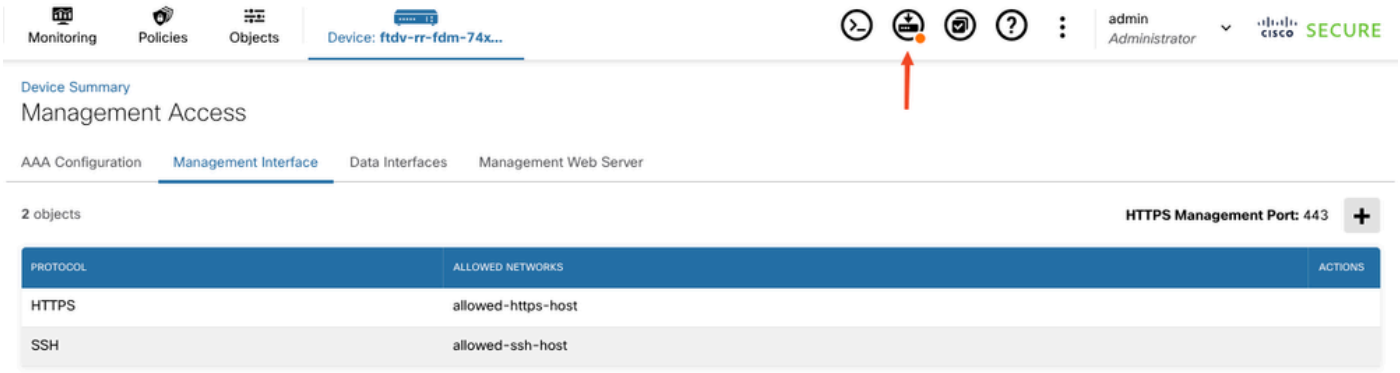


Cree una red de host según sus necesidades.

Paso 5: Compruebe los cambios realizados e implemente.

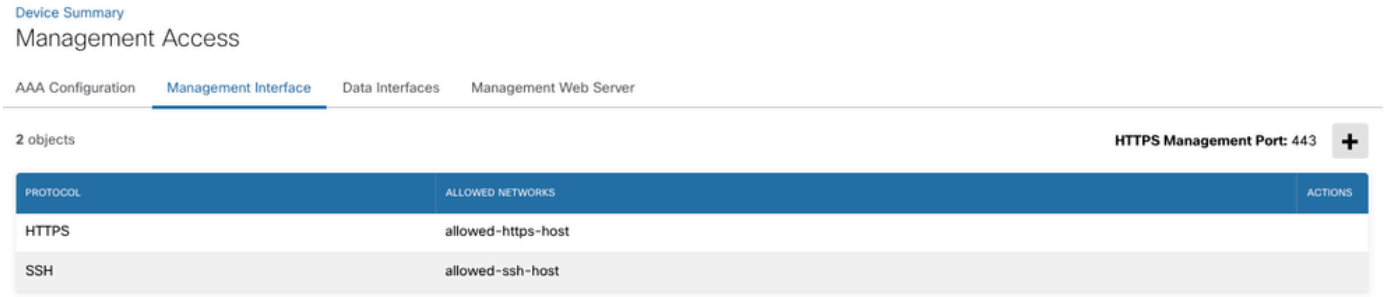


Se ha cambiado el acceso a la gestión HTTPS y se ha eliminado any-ipv4.



Implementación en FDM

Paso 6 (Opcional): Una vez verificados los cambios realizados anteriormente para HTTPS, repita el mismo procedimiento para SSH.



Objeto de red agregado para SSH y HTTPS.

Paso 7: Por último, implemente los cambios y verifique su acceso al FTD desde la red y el host permitidos.

PASOS DE REPARACIÓN:

Los pasos de CLI se pueden utilizar en caso de que se administren FDM o FMC.

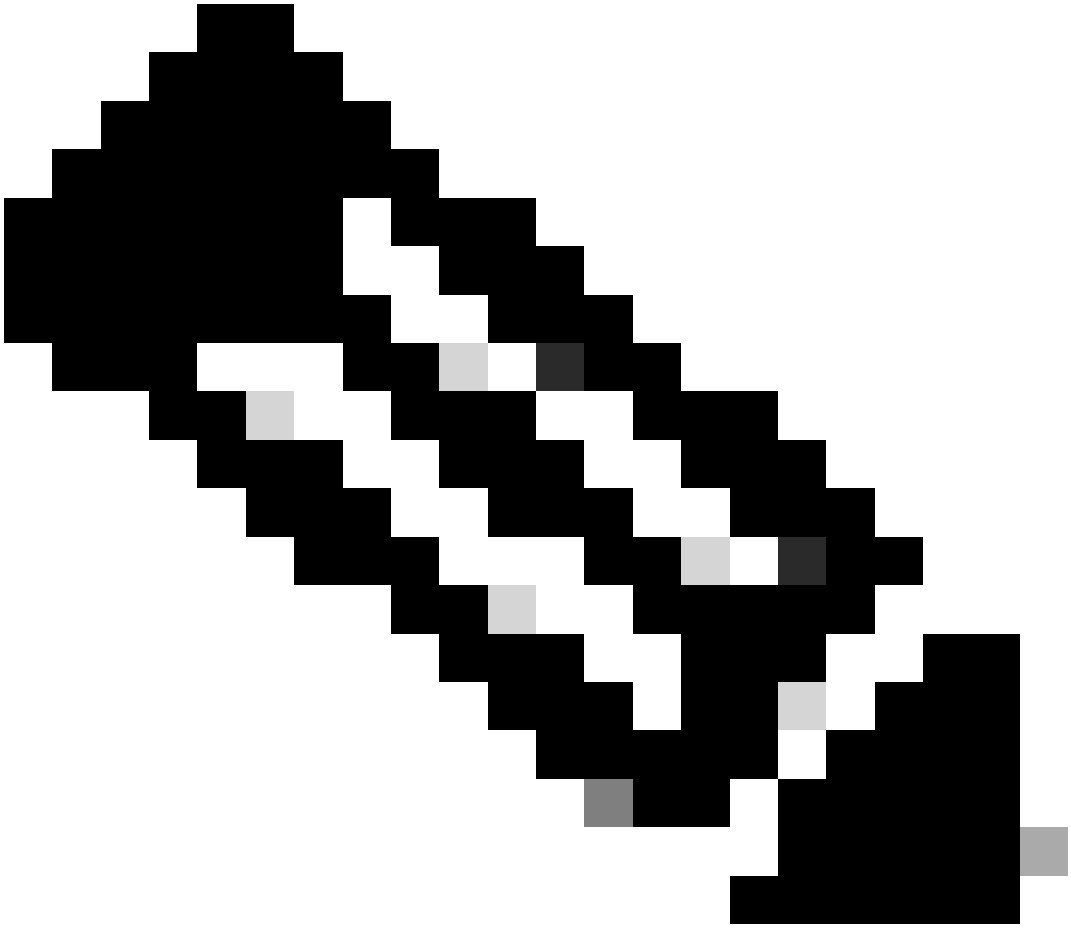
Para configurar el dispositivo para que acepte conexiones HTTPS o SSH desde direcciones IP o redes especificadas, utiliceconfigure https-access-listconfigure ssh-access-listtheorcommand.

- Debe incluir todos los hosts o redes soportados en un solo comando. Las direcciones especificadas en este comando sobrescriben el contenido actual de la lista de acceso correspondiente.
- Si el dispositivo es una unidad de un grupo de alta disponibilidad gestionado localmente, el cambio se sobrescribe la próxima vez que la unidad activa implemente actualizaciones de configuración. Si se trata de la unidad activa, el cambio se propaga al par durante la implementación.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.
```

```
> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```



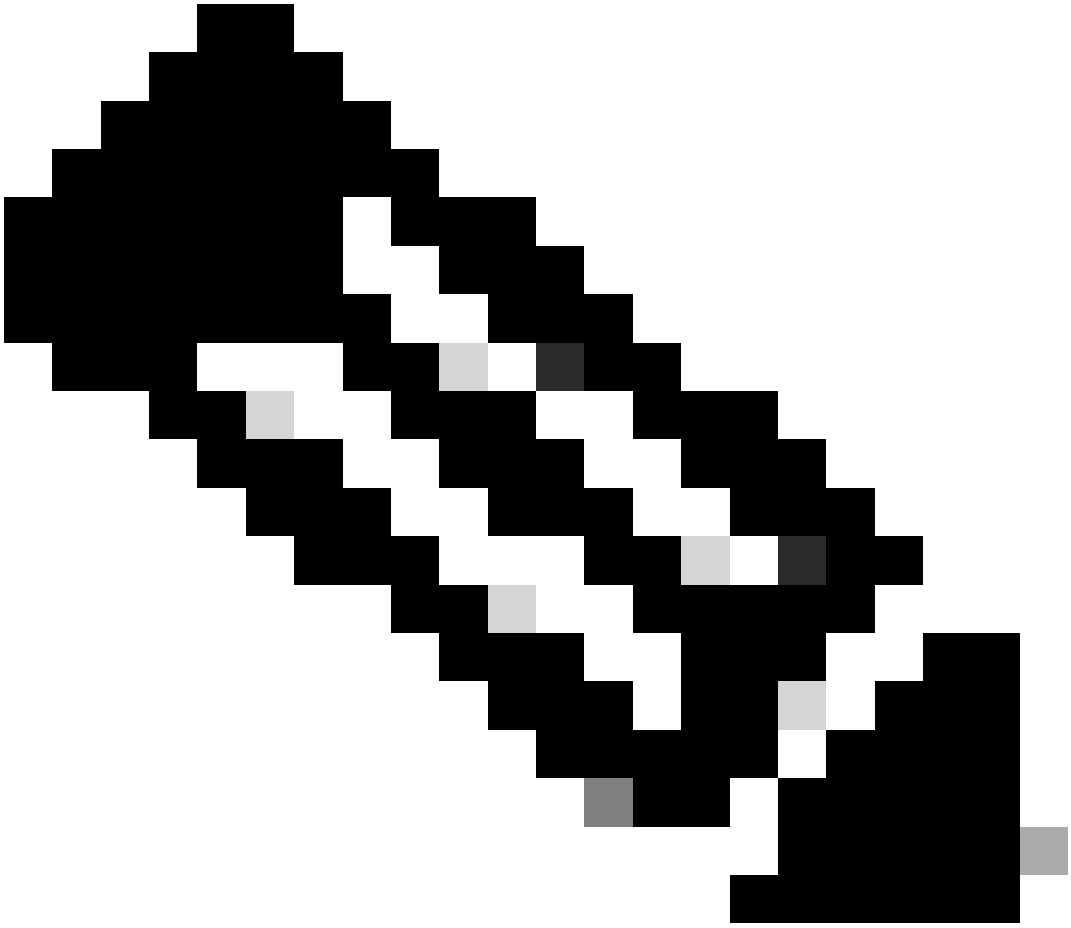
Nota: x.x.x.x/x e y.y.y.y.y/y representa la dirección ipv4 con notación CIDR.

De manera similar, para las conexiones SSH utilice el`configure ssh-access-list`comando con uno o varios comandos separados.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```



Nota: Puede utilizar comandos **configure disable-https-access** oconfigure disable-ssh-accesspara desactivar el acceso HTTPS o SSH respectivamente. Asegúrese de conocer estos cambios, ya que esto puede impedirle participar en la sesión.

Verificación

Para verificar desde CLISH puede utilizar comandos:

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:https
```

Referencias

Referencia de Comandos de Cisco Secure Firewall Threat Defence

Guía de configuración de Cisco Firepower Threat Defence para Firepower Device Manager

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).