Guía de inicio de Cisco Firepower 1010

Primera publicación: 2019-06-13

Última modificación: 2022-02-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CAPÍTULO 1

¿Qué aplicación y administrador son adecuados para usted?

Su plataforma de hardware puede ejecutar uno de los dos sistemas operativos. Para cada sistema operativo, tiene la opción de elegir los administradores. Este capítulo explica las opciones de administrador parael sistema operativo.

Sistemas operativos

Puede utilizar sistemas operativos de Secure Firewall ASA o Cisco Secure Firewall Threat Defense (antes Firepower Threat Defense) en su plataforma de hardware:

- ASA: el ASA es un firewall tradicional y avanzado con estado y un concentrador VPN.

  Es posible que desee utilizar el ASA si no necesita las capacidades avanzadas del Protección frente a amenazas o si necesita una función exclusiva del ASA que aún no está disponible en el Protección frente a amenazas. Cisco proporciona herramientas de migración de ASA a Protección frente a amenazas para ayudarle a convertir su ASA en Protección frente a amenazas si comienza con ASA y luego vuelve a crear la imagen en Protección frente a amenazas.

- Protección frente a amenazas: la protección frente a amenazas es un firewall de última generación que combina un firewall avanzado con estado, un concentrador VPN y un IPS de última generación. En otras palabras, la Protección frente a amenazas combina lo mejor de la funcionalidad ASA con la mejor funcionalidad IPS y firewall de última generación.

  Recomendamos utilizar la Protección frente a amenazas en lugar del ASA porque contiene la mayoría de las funciones principales del ASA, además de funciones adicionales de IPS y firewall de última generación.

Para crear imágenes entre el ASA y la Protección frente a amenazas, consulte la Guía de recreación de imágenes de Cisco Secure Firewall ASA y Threat Defense.

Administradores

La Protección frente a amenazas y el ASA son compatibles con varios administradores.

Administradores de Protección frente a amenazas

Tabla 1: Administradores de Protección frente a amenazas

Administrador	Descripción
Cisco Secure Firewall Management Center (antes Firepower Management Center)	El Centro de administración es un potente administrador de varios dispositivos basado en la web que se ejecuta en su propio hardware de servidor o como dispositivo virtual en un hipervisor. Debería utilizar el Centro de administración si desea un administrador de varios dispositivos y necesita todas las funciones de la Protección frente a amenazas. El Centro de administración también proporciona un potente análisis y control del tráfico y los eventos. En la versión 6.7 y posteriores, el Centro de administración puede administrar la Protección frente a amenazas desde la interfaz externa (u otros datos) en lugar de desde la interfaz de administración estándar. Esta característica es útil para implementaciones de sucursales remotas. **Nota** El Centro de administración no es compatible con otros administradores porque el Centro de administración es el propietario de la configuración de la Protección frente a amenazas y no tiene permiso para configurar la Protección frente a amenazas directamente, obviando el Centro de administración. Para comenzar a utilizar el Centro de administración en la red de administración, consulte Implementación de Protección frente a amenazas con el Centro de administración, en la página 5. Para comenzar a utilizar el Centro de administración en una red remota, consulte Implementación de la Protección frente a amenazas con control remoto del Centro de administración, en la página 47.
Administrador del dispositivo Cisco Secure Firewall (antes Firepower Device Manager)	El Administrador del dispositivo es un administrador de dispositivos simplificado basado en la web. Debido a que está simplificado, algunas características de Protección frente a amenazas no son compatibles con Administrador del dispositivo. Debería utilizar el Administrador del dispositivo si solo administra un número reducido de dispositivos y no necesita un administrador de varios dispositivos. **Nota** Tanto el Administrador del dispositivo como el CDO en modo FDM pueden detectar la configuración en el firewall, por lo que puede utilizar el Administrador del dispositivo y el CDO para administrar el mismo firewall. El Centro de administración no es compatible con otros administradores. Para comenzar a utilizar el Administrador del dispositivo, consulte Implementación de Protección frente a amenazas con el Administrador del dispositivo, en la página 91.

Administrador	Descripción
Cisco Defense Orchestrator(CDO)	CDO ofrece dos modos de administración: • (versión 7.2 y posteriores) Modo de centro de administración en la nube con todas las funciones de configuración de un centro de administración local. Para la función de análisis, puede utilizar tanto Cisco Secure Cloud Analytics en la nube como un centro de administración local. • Modo de administrador de dispositivos con una experiencia de usuario simplificada. Este modo no se trata en esta guía. Debido a que CDO está basado en la nube, no hay gastos operativos de CDO en sus propios servidores. CDO también administra otros dispositivos de seguridad, como los ASA, por lo que puede utilizar un único administrador para todos sus dispositivos de seguridad. Para comenzar con el aprovisionamiento de CDO, consulte Implementación de Protección frente a amenazas con CDO, en la página 119.
API REST de Secure Firewall Threat Defense	La API REST de protección frente a amenazas le permite automatizar la configuración directa de la Protección frente a amenazas. Esta API es compatible con el Administrador del dispositivo y CDO porque ambos pueden detectar la configuración en el firewall. No puede utilizar esta API si está administrando la Protección frente a amenazas con Centro de administración. La API REST de protección frente a amenazas no se trata en esta guía. Para obtener más información, consulte la Guía de API REST de Cisco Secure Firewall Threat Defense.
API REST de Cisco Secure Firewall Management Center	La API REST del Centro de administración le permite automatizar la configuración de las políticas del Centro de administración que más adelante se pueden aplicar a los administradores de la Protección frente a amenazas. Esta API no gestiona la Protección frente a amenazas directamente. La API REST del Centro de administración no se trata en esta guía. Para obtener más información, consulte la Guía de inicio rápido de la API REST Cisco Secure Firewall Management Center .

Administradores de ASA

Tabla 2: Administradores de ASA

Administrador	Descripción
Adaptive Security Device Manager (ASDM)	ASDM es un administrador del dispositivo basado en Java que proporciona una funcionalidad ASA completa. Debe utilizar ASDM si prefiere utilizar una GUI sobre la CLI y solo necesita administrar un pequeño número de ASA. ASDM puede detectar la configuración en el firewall, por lo que también puede utilizar la CLI, el CDO o el CSM con ASDM. Para comenzar con ASDM, consulte Implementación de ASA con ASDM, en la página 171.

Administrador	Descripción
CLI	Debe utilizar la CLI de ASA si prefiere las CLI sobre las GUI. La CLI no se trata en esta guía. Para obtener más información, consulte las guías de configuración de ASA.
CDO	CDO es un administrador de múltiples dispositivos simplificado y basado en la nube. Debido a que está simplificado, algunas características de ASA no son compatibles con CDO. Debe utilizar CDO si desea un administrador de varios dispositivos que ofrezca una experiencia de administración simplificada. Y como CDO está basado en la nube, no hay gastos generales de ejecución de CDO en sus propios servidores. CDO también administra otros dispositivos de seguridad, como la Protección frente a amenazas, por lo que puede utilizar un único administrador para todos sus dispositivos de seguridad. CDO puede detectar la configuración en el firewall, por lo que también puede utilizar la CLI o ASDM. CDO no se trata en esta guía. Para empezar en CDO, vea la página de inicio de CDO.
Cisco Security Manager (CSM)	CSM es un potente administrador de varios dispositivos que se ejecuta en su propio hardware de servidor. Debe usar CSM si necesita administrar un gran número de ASA. CSM puede detectar la configuración en el firewall, por lo que también puede utilizar la CLI o ASDM. CSM no es compatible con la administración de Protección frente a amenazas. CSM no se trata en esta guía. Para obtener más información, consulte la guía del usuario de CSM.
API REST de ASA	La API REST de ASA le permite automatizar la configuración de ASA. Sin embargo, la API no incluye todas las características de ASA y ya no se mejora. La API REST de ASA no se trata en esta guía. Para obtener más información, consulte la Guía de inicio rápido del API REST de Cisco Secure Firewall ASA.

CAPÍTULO 2

Implementación de Protección frente a amenazas con el Centro de administración

¿Este capítulo es para usted?

Para ver todos los sistemas operativos y administradores disponibles, consulte ¿Qué aplicación y administrador son adecuados para usted?, en la página 1. Este capítulo hace referencia a la Protección frente a amenazas con el Centro de administración.

Este capítulo explica cómo completar la configuración inicial de su Protección frente a amenazas y cómo registrar el firewall en un Centro de administración situado en su red de administración. Para la implementación en sucursales remotas en las que el Centro de administración esté en una sede central, consulte Implementación de la Protección frente a amenazas con control remoto del Centro de administración, en la página 47.

En una implementación típica en una red grande, instalará varios dispositivos administrados en segmentos de red. Cada dispositivo controla, inspecciona, supervisa y analiza el tráfico y, a continuación, informa a un administrador del Centro de administración. El Centro de administración proporciona una consola de administrador centralizada con una interfaz web que puede utilizar para realizar tareas, de administración, análisis e informes en servicio para proteger su red local.

Sobre el firewall

El hardware puede ejecutar el software Protección frente a amenazas o el software ASA. Para cambiar entre Protección frente a amenazas y ASA es necesario que vuelva a crear una imagen para el dispositivo. También es necesario que lleve a cabo una una recreación de imagen si necesita una versión de software diferente a la instalada. Consulte Recreación de la imagen del dispositivo de defensa contra amenazas de Firepower o ASA de Cisco.

El firewall ejecuta un sistema operativo subyacente llamado Cisco Secure Firewall Extensible Operating System (FXOS). El firewall no es compatible con el Administrador del chasis Cisco Secure Firewall de FXOS; solo se admite una CLI limitada para la resolución de problemas. Consulte Guía de resolución de problemas de Cisco FXOS para Firepower 1000/2100 Series que ejecuta Firepower Threat Defense para obtener más información.

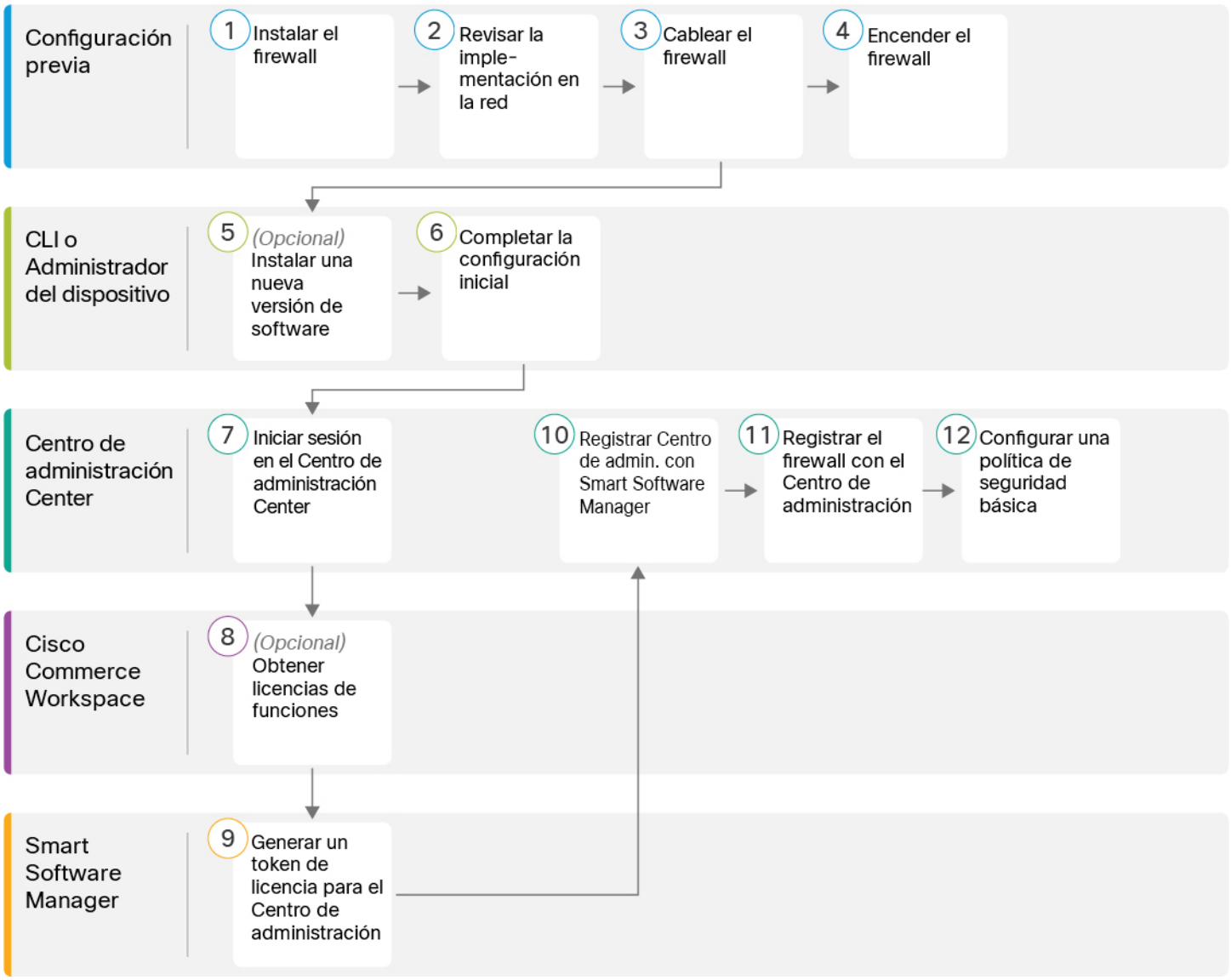
Declaración de recopilación de privacidad: el firewall no necesita ni recopila de forma activa información de identificación personal. Sin embargo, puede utilizar información de identificación personal en la configuración, por ejemplo, para los nombres de usuario. En este caso, un administrador podrá ver esta información cuando trabaje con la configuración o cuando utilice SNMP.

Antes de comenzar

Implemente y lleve a cabo la configuración inicial del Centro de administración. Consulte la Guía de instalación del hardware de Cisco Firepower Management Center 1600, 2600 y 4600 o Guía de inicio de Cisco Firepower Management Center Virtual.

Procedimiento completo

Consulte las siguientes tareas para implementar la Protección frente a amenazas con el Centro de administración en su chasis.



1	Configuración previa	Instale el firewall. Consulte la guía de instalación del hardware.
2	Configuración previa	Revisar la instalación en la red, en la página 8.
3	Configuración previa	Cablear el dispositivo (6.5 y posterior), en la página 10 Cablear el dispositivo (6.4), en la página 12.
4	Configuración previa	Encender el firewall, en la página 13.
5	CLI	(Opcional) Comprobar el software e instalar una nueva versión, en la página 14

6	CLI o Administrador del dispositivo	Completar la configuración inicial de la Protección frente a amenazas, en la página 15.
7	Centro de administración	Iniciar sesión en el Centro de administración, en la página 24.
8	Cisco Commerce Workspace	Obtener licencias para el Centro de administración, en la página 24: comprar licencias de funciones.
9	Smart Software Manager	Obtener licencias para el Centro de administración, en la página 24: generar un token de licencia para el Centro de administración.
10	Centro de administración	Obtener licencias para el Centro de administración, en la página 24: registrar el Centro de administración con el servidor de licencias Smart.
11	Centro de administración	Registrar la Protección frente a amenazas con el Centro de administración, en la página 25
12	Centro de administración	Configurar una norma de seguridad básica, en la página 28

Revisar la instalación en la red

6.5 e implementación posterior

La interfaz de administración específica 1/1 es una interfaz especial con sus propios ajustes de red. De forma predeterminada, la interfaz de administración 1/1 está activada y configurada como un cliente DHCP. Si su red no incluye un servidor DHCP, puede configurar la interfaz de administración para que utilice una dirección IP estática durante la configuración inicial en el puerto de la consola. Puede configurar otras interfaces después de conectar la Protección frente a amenazas al Centro de administración. Tenga en cuenta que los Ethernet de 1/2 a 1/8 están habilitados como puertos de switch de forma predeterminada.

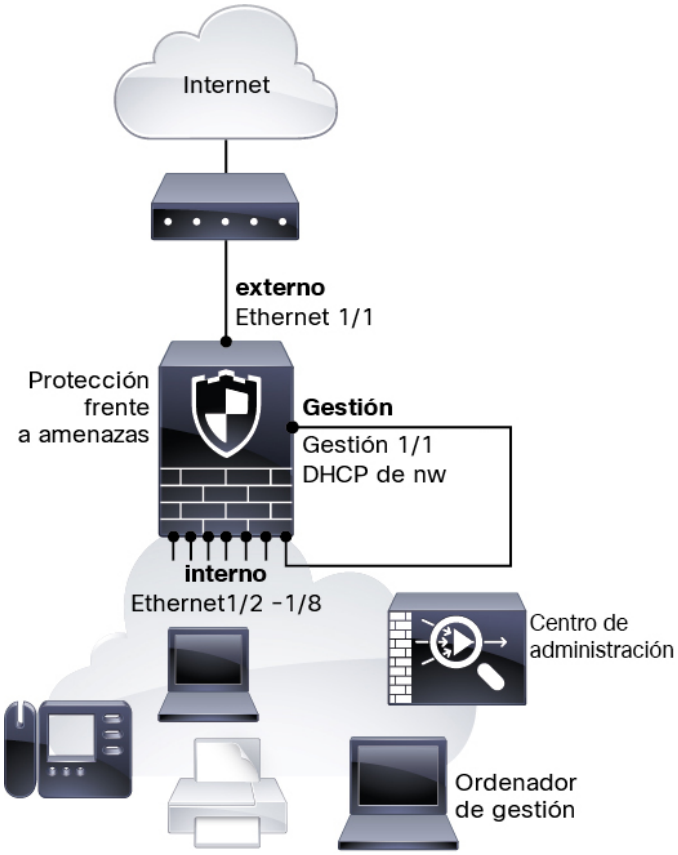
Nota En la versión 6.5 y anteriores, la interfaz de administración se configura con una dirección IP (192.168.45.45).

La siguiente figura muestra la implementación de red recomendada para Firepower 1010.

El Centro de administración solo puede comunicarse con la Protección frente a amenazas en la interfaz de administración. Además, tanto el Centro de administración como la Protección frente a amenazas necesitan acceso a Internet de la administración para obtener licencias y actualizaciones.

En el siguiente diagrama, el Firepower 1010 actúa como gateway de Internet para la interfaz de administración y el Centro de administración conectando la administración 1/1 directamente a un puerto interno del switch y conectando el Centro de administración y el equipo de administración a otros puertos internos del switch. (Esta conexión directa está permitida porque la interfaz de administración es independiente de las otras interfaces de la Protección frente a amenazas).

Figura 1: Instalación en la red recomendada



6.4 Implementación

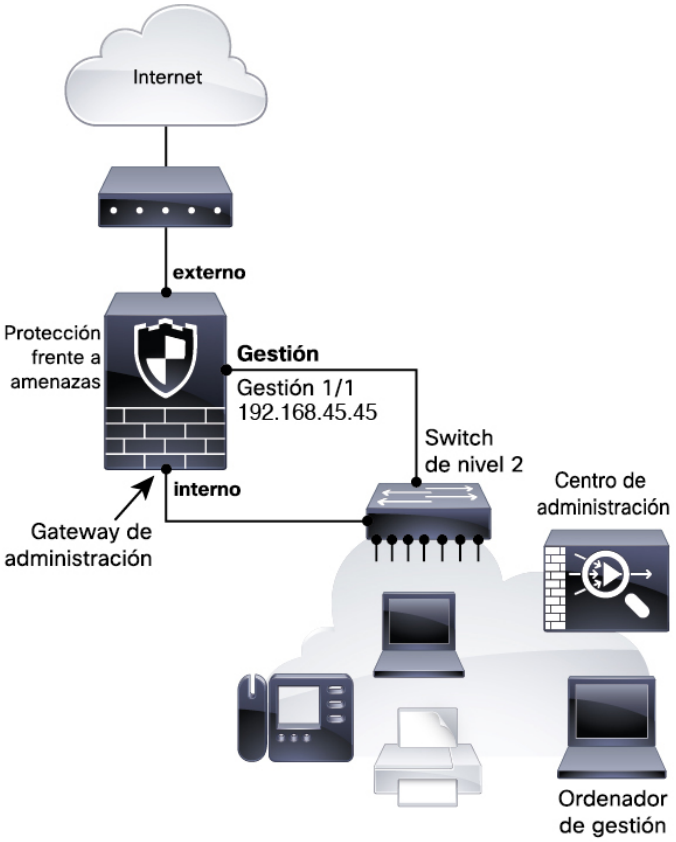
La interfaz de administración específica 1/1 es una interfaz especial con sus propios ajustes de red. De forma predeterminada, solo está activada y configurada con una dirección IP (192.168.45.45) la interfaz de administración 1/1. Esta interfaz también ejecuta inicialmente un servidor DHCP; después de seleccionar el Centro de administración como administrador durante la configuración inicial, el servidor DHCP se desactiva. Puede configurar otras interfaces después de conectar la Protección frente a amenazas al Centro de administración.

La siguiente figura muestra la implementación de red recomendada para Firepower 1010.

El Centro de administración solo puede comunicarse con la Protección frente a amenazas en la interfaz de administración. Además, tanto el Centro de administración como la Protección frente a amenazas necesitan acceso a Internet de la administración para obtener licencias y actualizaciones.

En el siguiente diagrama, el Firepower 1010 actúa como gateway de Internet para la interfaz de administración y el Centro de administración conectando la administración 1/1 a una interfaz interna a través de un switch de capa 2, y conectando el Centro de administración y el equipo de administración al switch. (Esta conexión directa está permitida porque la interfaz de administración es independiente de las otras interfaces del Protección frente a amenazas).

Figura 2: Instalación en la red recomendada

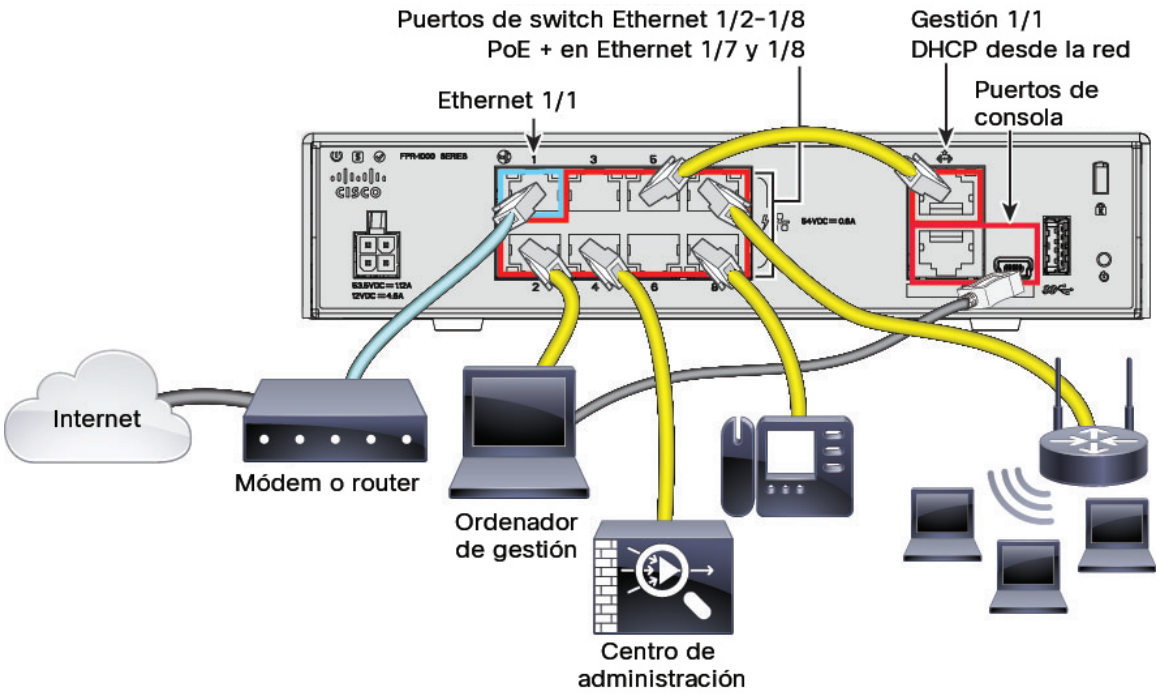


Cablear el dispositivo (6.5 y posterior)

Para el cableado recomendado en Firepower 1010, consulte la siguiente ilustración, que muestra una topología de ejemplo que utiliza Ethernet1/1 como interfaz externa y las interfaces restantes como puertos de switch en la red interna.

Nota Se pueden utilizar otras topologías y su implementación variará en función de sus requisitos. Por ejemplo, puede convertir los puertos de switch en interfaces de firewall.

Figura 3: Cableado de Firepower 1010



Nota Para la versión 6.5 y anteriores, la dirección IP predeterminada de Gestión 1/1 es 192.168.45.45.

Procedimiento

Paso 1 Instale el chasis. Consulte la guía de instalación del hardware.

Paso 2 Conecte la de administración 1/1 directamente a uno de los puertos de switch, Ethernet1/2 a 1/8.

Paso 3 Conecte por cable a los puertos de switch, Ethernet1/2 a 1/8 lo siguiente:

- Centro de administración
- Ordenador de gestión
- Otros terminales

Paso 4 Conecte el ordenador de gestión al puerto de consola. Debe utilizar el puerto de consola para acceder a la CLI para la configuración inicial en caso de que no utilice SSH para la interfaz de administración o utilice Administrador del dispositivo para la configuración inicial.

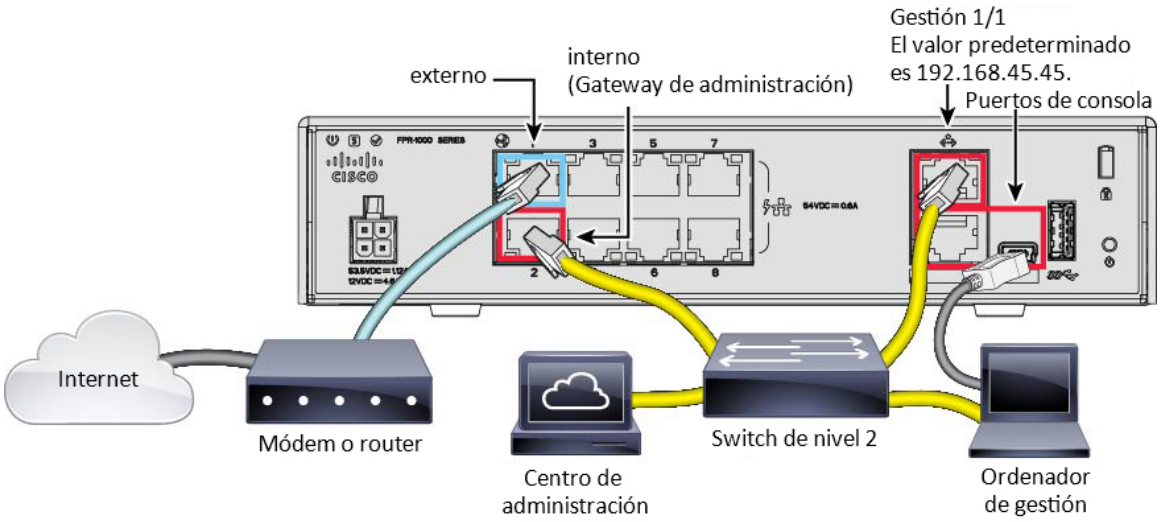
Paso 5 Conecte Ethernet 1/1 a su router externo.

Cablear el dispositivo (6.4)

Para un cableado recomendado en Firepower 1010, consulte la siguiente ilustración, que muestra una topología de ejemplo con un switch de capa 2.

Nota Se pueden utilizar otras topologías y su implementación variará en función de sus requisitos.

Figura 4: Cableado de Firepower 1010



Procedimiento

Paso 1 Instale su hardware y familiarícese con él siguiendo la guía de instalación del hardware.

Paso 2 Conecte lo siguiente al switch Ethernet de la capa 2:

- Interfaz interna (por ejemplo, Ethernet 1/2)
- Interfaz de gestión 1/1
- Centro de administración
- Ordenador de gestión

Nota Tanto el Firepower 1010 como el Centro de administración tienen la misma dirección IP de administración predeterminada: 192.168.45.45. Esta guía da por hecho que establecerá diferentes direcciones IP para sus dispositivos durante la configuración inicial. Tenga en cuenta que el Centro de administración en la versión 6.5 y posteriores utiliza de forma predeterminada un cliente DHCP para la interfaz de administración; no obstante, si no hay ningún servidor DHCP, el valor predeterminado será 192.168.45.45.

Paso 3 Conecte el ordenador de gestión al puerto de consola. Debe utilizar el puerto de consola para acceder a la CLI para la configuración inicial en caso de que no utilice SSH para la interfaz de gestión.

Paso 4 Conecte la interfaz externa (por ejemplo, Ethernet 1/1) al router externo.

Paso 5 Conecte otras redes a las interfaces que faltan.

Encender el firewall

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Antes de empezar

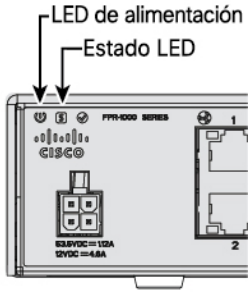
Es importante que proporcione una alimentación fiable para su dispositivo (con una fuente de alimentación ininterrumpida (UPS), por ejemplo). Si se pierde la fuente de alimentación sin apagar primero se pueden provocar daños graves en el sistema de archivos. Hay muchos procesos que se ejecutan en segundo plano todo el tiempo y, si se pierde la fuente de alimentación, el sistema no se puede apagar adecuadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

(Opcional) Comprobar el software e instalar una nueva versión

Para comprobar la versión del software e instalar una versión diferente, si es necesario, siga estos pasos. Le recomendamos que instale su versión de destino antes de configurar el firewall. Como alternativa, puede realizar una actualización una vez que esté en funcionamiento, pero la actualización, que conserva su configuración, puede llevar más tiempo que este procedimiento.

¿Qué versión debo ejecutar?

Cisco recomienda ejecutar una versión Gold Star indicada con una estrella dorada junto al número de versión en la página de descarga de software. También puede consultar la estrategia de versiones descrita en https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; Por ejemplo, este boletín describe la numeración de las versiones a corto plazo (con las características más recientes), la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para un período de tiempo más largo) o la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para el período de tiempo más largo, para la certificación del gobierno).

Procedimiento

Paso 1 Conéctese a la CLI. Consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 44 para obtener más información. Este procedimiento se muestra a través del puerto de consola, pero también puede utilizar SSH en su lugar.

Inicie sesión con el usuario **administrador** y la contraseña predeterminada **Admin123**.

Se conecta a la CLI de FXOS. La primera vez que inicie sesión, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se cambió la contraseña, y no lo sabe, debe llevar a cabo una restauración de fábrica para recuperar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el Procedimiento de restauración de fábrica.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 2 En la CLI de FXOS, muestre la versión en ejecución.

scope ssa

show app-instance

Ejemplo:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Paso 3 Si desea instalar una nueva versión, lleve a cabo estos pasos.

a) Si necesita establecer una dirección IP estática para la interfaz de administración, consulte Completar la configuración inicial de Protección frente a amenazas mediante la CLI, en la página 20. La interfaz de administración utiliza por defecto DHCP.

Tendrá que descargar la nueva imagen de un servidor accesible desde la interfaz de administración.

b) Lleve a cabo el procedimiento de recrear la imagen que aparece en la guía de resolución de problemas de FXOS.

Completar la configuración inicial de la Protección frente a amenazas

Puede completar la configuración inicial de Protección frente a amenazas mediante la CLI o Administrador del dispositivo.

Completar la configuración inicial de Protección frente a amenazas mediante Administrador del dispositivo

Conéctese a Administrador del dispositivo para realizar la configuración inicial de la Protección frente a amenazas. Cuando lleva a cabo la configuración inicial con Administrador del dispositivo, *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se conserva al cambiar a Centro de administración para la gestión, además de la configuración de acceso del administrador y la interfaz de administración. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso o las zonas de seguridad. Cuando utiliza la CLI, solo se conservan la configuración de acceso del administrador y la interfaz de administración (por ejemplo, no se conserva la configuración de la interfaz interna de forma predeterminada).

Antes de empezar

- Implemente y lleve a cabo la configuración inicial del Centro de administración. Consulte la Guía de instalación del hardware de Cisco Firepower Management Center 1600, 2600 y 4600. Necesitará conocer la dirección IP o el nombre de host del Centro de administración antes de configurar el Protección frente a amenazas.
- Utilice una versión actual de Firefox, Chrome, Safari, Edge o Internet Explorer.

Procedimiento

Paso 1 Inicie sesión en Administrador del dispositivo.

a) Introduzca una de las siguientes URL en su navegador.

- Interno (Ethernet1/2 a 1/8)—**https://192.168.95.1**.Puede conectarse a la dirección interna en cualquier puerto interno del switch (Ethernet1/2 a 1/8).
- Administración: **https://***management_ip*. La interfaz de administración es un cliente DHCP, por lo que la dirección IP depende de su servidor DHCP. Es posible que deba atribuir la dirección IP de administración a una dirección estática como parte de este proceso, por lo que le recomendamos que utilice la interfaz interna para no desconectarse.

b) Inicie sesión con el nombre de usuario **admin** y la contraseña predeterminada **Admin123**.

c) Se le pedirá que lea y acepte el contrato de licencia del usuario final y que cambie la contraseña de administrador.

Paso 2 Utilice el asistente de configuración cuando inicie sesión por primera vez en Administrador del dispositivo para completar la configuración inicial. De manera opcional, puede omitir el asistente de configuración haciendo clic en **Omitir configuración del dispositivo** al final de la página.

Después de completar el asistente de configuración, además de la configuración predeterminada de la interfaz interna (Ethernet1/2 a 1/8, que son puertos de switch en la VLAN1), tendrá una configuración para una interfaz externa (Ethernet1/1) que se mantendrá cuando cambie a la administración del Centro de administración.

a) Configure las siguientes opciones para las interfaces externas y de administración y haga clic en **Siguiente**.

1. **Dirección de la interfaz externa**: esta interfaz suele ser la gateway de Internet y puede utilizarse como interfaz de acceso del administrador. No se puede seleccionar una interfaz externa alternativa durante la configuración inicial del dispositivo. La primera interfaz de datos es la interfaz externa predeterminada.

   Si desea utilizar una interfaz diferente de la externa (o interna) para el acceso al administrador, tendrá que configurarla manualmente después de completar el asistente de configuración.

   Configure IPv4: la dirección IPv4 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, una máscara de subred y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv4. No puede configurar PPPoE con el asistente de configuración. PPPoE puede ser necesario si la interfaz está conectada a un módem DSL, a un módem por cable o a otra conexión con su ISP, y su ISP utiliza PPPoE para proporcionar su dirección IP. Puede configurar PPPoE después de completar el asistente.

   Configure IPv6: la dirección IPv6 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, un prefijo y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv6.

2. **Interfaz de administración**

   No verá la configuración de la interfaz de administración si ha realizado la configuración inicial desde la CLI. Tenga en cuenta que la configuración de la dirección IP de la interfaz de administración no está incluida en el asistente de configuración. Consulte el paso Paso 3, en la página 17 para establecer la dirección IP de administración.

   Servidores DNS: el servidor DNS para la interfaz de administración del firewall. Introduzca una o varias direcciones de servidores DNS para la resolución de nombres. El valor predeterminado son los

servidores DNS públicos de OpenDNS. Si edita los campos y quiere volver a los predeterminados, haga clic en **Usar OpenDNS** para volver a cargar las direcciones IP adecuadas en los campos.

Nombre de host del firewall: el nombre de host para la interfaz de administración del firewall.

b) Configure los **Ajustes de la hora (NTP)** y haga clic en **Siguiente**.

1. **Zona horaria**: seleccione la zona horaria del sistema.
2. **Servidor de hora NTP**: seleccione si desea utilizar los servidores NTP predeterminados o introducir manualmente las direcciones de sus servidores NTP. Puede agregar varios servidores para proporcionar copias de seguridad.

c) Seleccione **Iniciar periodo de evaluación de 90 días sin registro**.

No registre el Protección frente a amenazas con Smart Software Manager; todas las licencias se realizan en el Centro de administración.

d) Haga clic en **Finalizar**.

e) Se le solicitará que elija **Administración en la nube** o **Independiente**. Para la administración del Centro de administración, seleccione **Independiente** y, a continuación, **Lo tengo**.

Paso 3 (Puede que sea necesario) Configure una dirección IP estática para la interfaz de administración. Seleccione **Dispositivo** y, a continuación, haga clic en el enlace **Configuración del sistema** > **Interfaz de administración**.

Si desea configurar una dirección IP estática, asegúrese también de establecer la gateway predeterminada para que sea una gateway única en lugar de las interfaces de datos. Si utiliza el DHCP, no tiene que configurar nada.

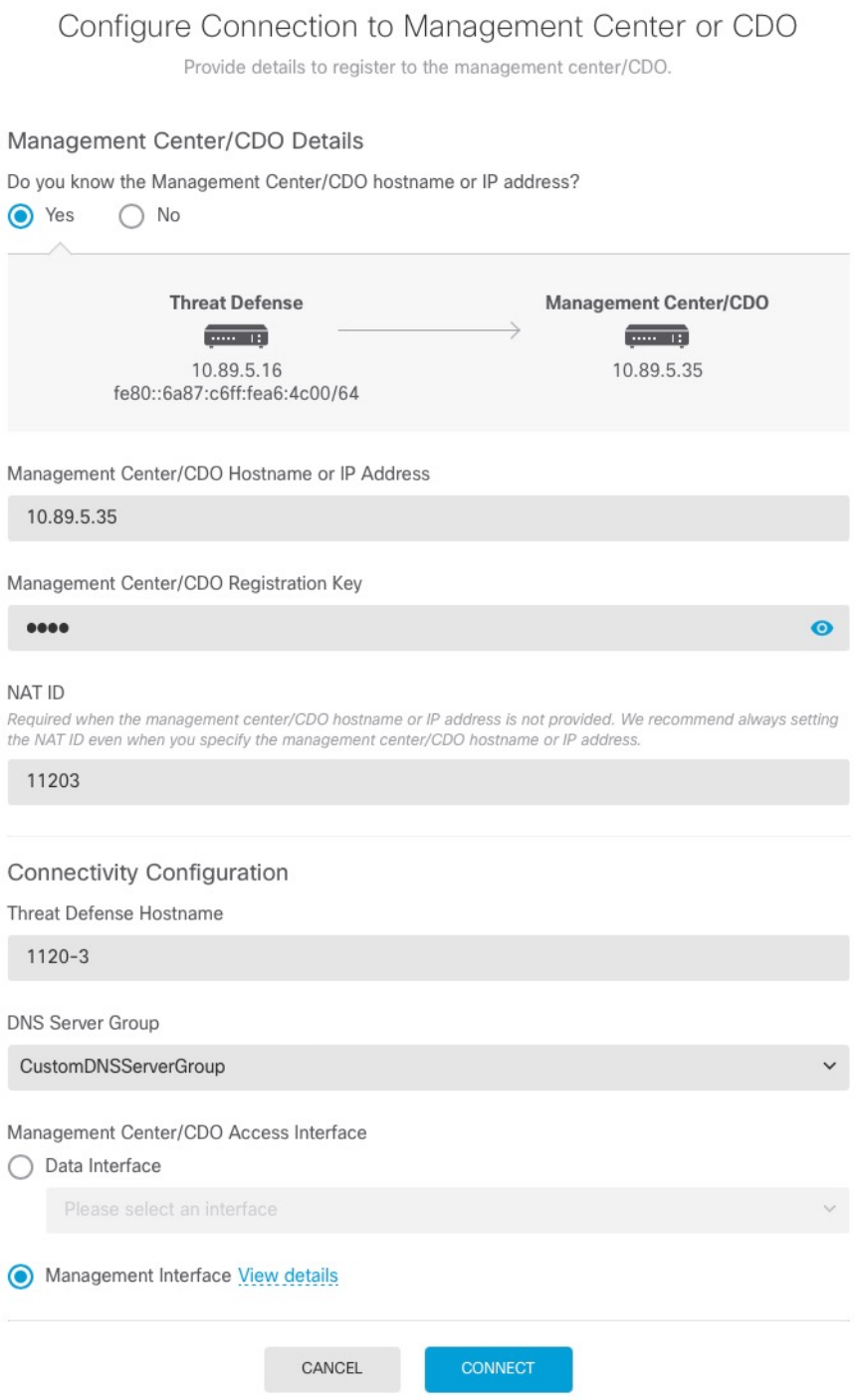
Paso 4 Si desea configurar interfaces adicionales, incluida una interfaz distinta de la externa o la interna, seleccione **Dispositivo** y, a continuación, haga clic en el enlace del resumen de **Interfaces**.

Consulte Configurar el firewall en Administrador del dispositivo, en la página 110 para obtener más información sobre la configuración de interfaces en Administrador del dispositivo. No se conservará otra configuración de Administrador del dispositivo cuando registre el dispositivo en el Centro de administración.

Paso 5 Seleccione **Dispositivo** > **Configuración del sistema** > **Administración central**, y haga clic en **Proceder** para configurar la administración del Centro de administración.

Paso 6 Configure los **Detalles del centro de administración/CDO**.

Figura 5: Detalles del centro de administración/CDO



a) Para las preguntas **¿Conoce el nombre de host o la dirección IP del Centro de gestión/CDO?**, haga clic en **Sí** si puede acceder al Centro de administración mediante una dirección IP o un nombre de host, o **No** si el Centro de administración está detrás de la NAT o no tiene una dirección IP pública o un nombre de host.

Al menos uno de los dispositivos, ya sea el Centro de administración o la Protección frente a amenazas, debe tener una dirección IP accesible para establecer el canal de comunicación bidireccional con cifrado SSL entre los dos dispositivos.

b) Si responde **Sí**, introduzca la **dirección IP o el nombre de host del centro de administración/CDO**.

c) Especifique la **Clave de registro del centro de administración/CDO** .

Es una clave de registro de un solo uso a su elección que también especificará en el Centro de administración cuando registre el dispositivo Protección frente a amenazas. La clave de registro no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-). Esta ID se puede utilizar para el registro de múltiples dispositivos en el Centro de administración.

d) Especifique una **ID de NAT**.

Esta ID es un string único de un solo uso a su elección que también especificará en el Centro de administración. Este campo es necesario si solo especifica la dirección IP en uno de los dispositivos; pero le recomendamos que especifique la ID de NAT incluso si conoce la dirección IP de ambos dispositivos. El ID de la NAT no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-). Esta ID *no* se puede utilizar para el registro de ningún otro dispositivo en el Centro de administración. La ID de NAT se utiliza en combinación con la dirección IP para verificar que la conexión proviene del dispositivo correcto; solo después de la autenticación de la dirección IP / ID de NAT se comprobará la clave de registro.

Paso 7 Configure la **Configuración de conectividad**.

a) Especifique el **Nombre de host del FTD**.

b) Especifique el **Grupo de servidores DNS**.

Elija un grupo existente o cree uno nuevo. El grupo de DNS predeterminado se llama **CiscoUmbrellaDNSServerGroup** e incluye los servidores OpenDNS.

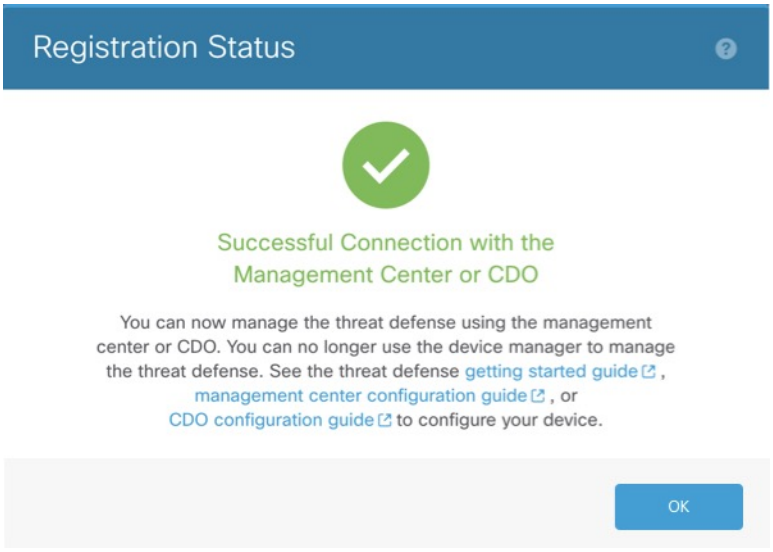
c) En la **Interfaz de acceso al centro de administración/CDO**, seleccione **administración**.

Paso 8 Haga clic en **Conectar**. El cuadro de diálogo del **Estado de registro** muestra el estado actual del cambio al Centro de administración. Después del paso de **Guardar la configuración de registro del centro de administración/CDO**, vaya al Centro de administración, y agregue el firewall.

Si desea cancelar el traspaso al Centro de administración, haga clic en **Cancelar registro**. De lo contrario, no cierre la ventana del navegador Administrador del dispositivo hasta que se haya completado el paso de **Guardar la configuración de registro del centro de administración/CDO**. Si lo hace, el proceso se detendrá y no continuará hasta que se vuelva a conectar a Administrador del dispositivo.

Si permanece conectado a Administrador del dispositivo tras el paso de **Guardar la configuración de registro del centro de administración/CDO**, en algún momento le aparecerá el cuadro de diálogo de **Se ha conectado correctamente al centro de administración/CDO**, tras el cual se le desconectará de Administrador del dispositivo.

Figura 6: Conexión correcta



Completar la configuración inicial de Protección frente a amenazas mediante la CLI

Conéctese a la CLI de Protección frente a amenazas para llevar a cabo la configuración inicial: configurar la dirección IP de administración, la gateway y otras configuraciones de red básicas con el asistente de configuración. La interfaz de gestión específica es una interfaz especial con sus propios ajustes de red. En la versión 6.7 y posteriores: si no desea utilizar la interfaz de administración para el acceso al administrador, puede utilizar la CLI para configurar una interfaz de datos en su lugar. También configurará los ajustes de comunicación de Centro de administración. Cuando lleva a cabo la configuración inicial con Administrador del dispositivo (versiones 7.1 o posteriores), *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se conserva al cambiar a Centro de administración para la gestión, además de la configuración de la interfaz de acceso del administrador y la interfaz de administración. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso.

Procedimiento

Paso 1 Conéctese a la CLI de Protección frente a amenazas, ya sea desde el puerto de consola o mediante SSH a la interfaz de administración, que obtiene una dirección IP de un servidor DHCP de forma predeterminada. Si tiene intención de cambiar la configuración de red, recomendamos utilizar el puerto de la consola para que no se desconecte.

El puerto de consola se conecta a la CLI de FXOS. La sesión SSH se conecta directamente a la CLI de Protección frente a amenazas.

Paso 2 Inicie sesión con el nombre de usuario **admin** y la contraseña **Admin123**.

En el puerto de consola, conéctese a la CLI de FXOS. La primera vez que inicie sesión en FXOS, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se ha cambiado la contraseña y no lo sabe, debe volver a crear el dispositivo para restablecer la contraseña a la predeterminada. Consulte la guía de resolución de problemas de FXOS para el procedimiento de restablecer la imagen.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 3 Si se conectó a FXOS desde el puerto de consola, conéctese a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Paso 4 La primera vez que inicie sesión en Protección frente a amenazas, se le solicitará que acepte el contrato de licencia del usuario final (EULA) y, si utiliza una conexión SSH, que cambie la contraseña del administrador. A continuación, se le presenta el script de configuración de la CLI.

Nota No puede volver a abrir el asistente de configuración de la CLI a menos que borre la configuración; por ejemplo, al restablecer la imagen. Sin embargo, todos estos ajustes pueden cambiarse más tarde en la CLI mediante los comandos de **configuración de red**. Consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Los valores predeterminados o los introducidos anteriormente aparecen entre paréntesis. Para aceptar los valores introducidos anteriormente, pulse **Intro**.

Consulte las siguientes directrices:

- **Introduzca la gateway predeterminada de IPv4 para la interfaz de administración**: los ajustes de las **interfaces de datos** solo se aplican a la administración del Centro de administración remoto o la administración del Administrador del dispositivo; debe establecer una dirección IP de gateway para la Administración 1/1 cuando utilice el Centro de administración en la red de administración. En el ejemplo de implementación perimetral que se muestra en la sección de implementación de red, la interfaz interna actúa como gateway de administración. En este caso, debe establecer la dirección IP de la gateway para que sea la dirección IP de interfaz interna *prevista*; después debe usar el Centro de administración para establecer la dirección IP interna.

- **Si su información de red ha cambiado, tendrá que volver a conectarse**. Si está conectado a SSH pero cambia la dirección IP en la configuración inicial, se desconectará. Vuelva a conectarse con la nueva dirección IP y la contraseña. Las conexiones de la consola no se ven afectadas.
- **¿Administrar el dispositivo de forma local?** Introduzca **No** para utilizar Centro de administración. Si responde **Sí** significa que utilizará Administrador del dispositivo en su lugar.
- **¿Configurar el modo de firewall?**: Le recomendamos que configure el modo de firewall en la configuración inicial. Si cambia el modo del firewall después de la configuración inicial se borrará la configuración que esté en ejecución.

Ejemplo:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Paso 5 Identifique el Centro de administración que administrará esta Protección frente a amenazas.

configure manager add {*nombre de host* | *dirección_IPv4* | *dirección_IPv6* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*nombre de host* | *dirección_IPv4* | *dirección_IPv6* | **DONTRESOLVE**}: especifica la FQDN o la dirección IP de Centro de administración. Si Centro de administración no es directamente direccionable, utilice **DONTRESOLVE** y especifique también el *id_nat*. Al menos uno de los dispositivos, ya sea el Centro de administración o el Protección frente a amenazas, debe tener una dirección IP accesible para establecer el canal de comunicación bidireccional con cifrado SSL entre los dos dispositivos. Si especifica **DONTRESOLVE** en este comando, el Protección frente a amenazas debe tener una dirección IP o nombre de host accesible.
- *reg_key*: especifica la clave de registro de un solo uso de su elección que también especificará en el Centro de administración cuando registre la Protección frente a amenazas. La clave de registro no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-).
- *id_nat*: especifica una cadena única y exclusiva de su elección que también podrá determinar en Centro de administración cuando registre la Protección frente a amenazas si un lado no especifica una dirección IP o nombre de host accesible. Es necesario si establece el Centro de administración como **DONTRESOLVE**. El ID de la NAT no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-). Este ID no se puede utilizar para ningún otro dispositivo que se registre en el Centro de administración.

Ejemplo:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Si Centro de administración está detrás de un dispositivo NAT, introduzca un ID de NAT único junto con la clave de registro y especifique DONTRESOLVE en lugar del nombre de host, por ejemplo:

Ejemplo:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Si la Protección frente a amenazas está detrás de un dispositivo NAT, introduzca una ID de NAT única junto con la dirección IP o el nombre de host del Centro de administración, por ejemplo:

Ejemplo:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Qué hacer a continuación

Registre su firewall en Centro de administración.

Iniciar sesión en el Centro de administración

Utilice el Centro de administración para configurar y controlar la Protección frente a amenazas.

Antes de empezar

Para obtener información sobre los navegadores compatibles, consulte las notas de la versión que esté utilizando (consulte https://www.cisco.com/go/firepower-notes).

Procedimiento

Paso 1 Con un navegador compatible, introduzca la siguiente URL.

https://*fmc_ip_address*

Paso 2 Introduzca su nombre de usuario y contraseña.

Paso 3 Haga clic en **Iniciar sesión**.

Obtener licencias para el Centro de administración

Protección frente a amenazas proporciona todas las licencias para Centro de administración. Puede adquirir las siguientes licencias:

- **Amenazas**: inteligencia de seguridad e IPS de última generación
- **Malware**: protección frente al malware
- **URL**: filtrado de URL
- **VPN con RA**: AnyConnect Plus, AnyConnect Apex o AnyConnect solo VPN

Para obtener una descripción general más detallada sobre Cisco Licensing, visite cisco.com/go/licensingguide

Antes de empezar

- Tener una cuenta principal en Smart Software Manager.

  Si aún no tiene una cuenta, haga clic en el enlace para configurar una nueva cuenta. Smart Software Manager le permite crear una cuenta principal para su organización.

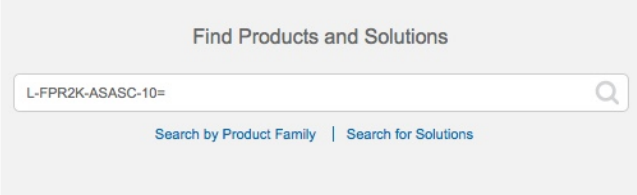
- Su cuenta de licencias de Smart Software debe cumplir los requisitos de la licencia de cifrado seguro (3DES/AES) para utilizar algunas funciones (que se activan mediante el indicador de cumplimiento de exportación).

Procedimiento

Paso 1 Compruebe que su cuenta de licencias Smart contenga las licencias disponibles que necesita.

Cuando adquirió su dispositivo en Cisco o en un distribuidor, sus licencias deberían haberse vinculado a su cuenta de licencias Smart Software. Sin embargo, si necesita agregar licencias usted mismo, utilice el campo de búsqueda **Buscar productos y soluciones** en Cisco Commerce Workspace. Busque las siguientes PID de licencia:

Figura 7: Búsqueda de licencia



Nota Si no se encuentra una PID, puede agregarla manualmente a su pedido.

- Combinación de licencias de amenazas, malware y URL:
  - L-FPR1010T-TMC=

  Cuando agregue una de las PID anteriores a su pedido, podrá elegir una suscripción basada en el plazo correspondiente a una de las siguientes PID:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN con RA: consulte la Guía de pedidos de Cisco AnyConnect.

Paso 2 Si aún no lo ha hecho, registre el Centro de administración con el servidor de Smart Licensing.

Para registrarse, es necesario que genere un token de registro en Smart Software Manager. Consulte Guía de administración del Cisco Secure Firewall Management Center para obtener instrucciones detalladas.

Registrar la Protección frente a amenazas con el Centro de administración

Registre la Protección frente a amenazas en el Centro de administración manualmente utilizando la dirección IP o el nombre de host del dispositivo.

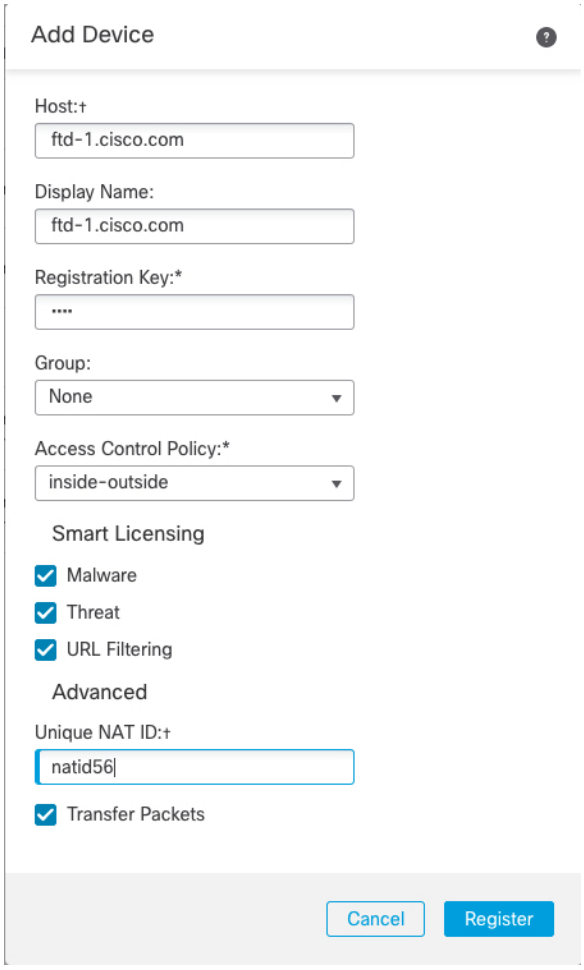
Antes de empezar

- Recopile la siguiente información que determinó en la configuración inicial de Protección frente a amenazas:
  - La dirección IP o nombre de host de la Protección frente a amenazas, y la ID de NAT
  - La clave de registro del Centro de administración

Procedimiento

Paso 1 En el Centro de administración, seleccione **Dispositivos** > **Administración de dispositivos**.

Paso 2 En la lista desplegable **Agregar**, seleccione **Agregar dispositivo**.



Establezca los siguientes parámetros:

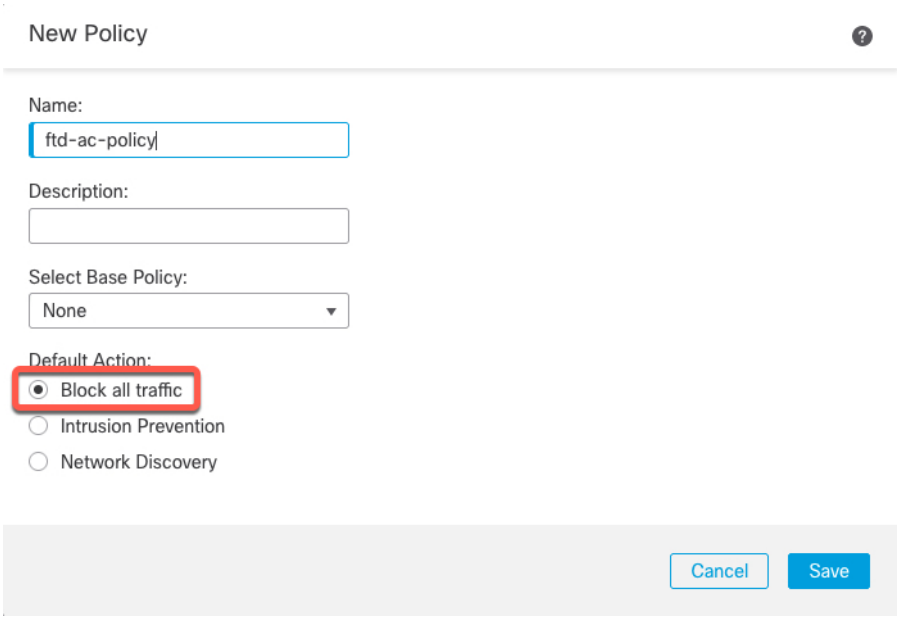
- **Host**: introduzca la dirección IP o el nombre del host de Protección frente a amenazas que desee agregar. Puede dejar este campo en blanco si ha especificado tanto la dirección IP y una ID de NAT del Centro de administración en la configuración inicial de la Protección frente a amenazas.

  Nota En un entorno de alta disponibilidad, cuando, los Centros de administración están detrás de una NAT, puede registrar la Protección frente a amenazas sin una IP o nombre de host en el Centro de administración principal. Sin embargo, para registrar la Protección frente a amenazas en un Centro de administración secundario, debe proporcionar una dirección IP o nombre de host para la Protección frente a amenazas.

- **Nombre de visualización**: introduzca el nombre de la Protección frente a amenazas que desee que aparezca en el Centro de administración.

- **Clave de registro**: introduzca la misma clave de registro que especificó en la configuración de inicial de Protección frente a amenazas.
- **Dominio**: asigne el dispositivo a un dominio inferior si tiene un entorno con varios dominios.
- **Grupo**: asígnelo a un grupo de dispositivos si utiliza grupos.
- **Política de control de acceso**: seleccione una política inicial. A menos que ya cuente con una política personalizada que sepa que debe utilizar, seleccione **Crear nueva política** y **Bloquear todo el tráfico**. Puede cambiar esto más tarde para permitir el tráfico; ver Permitir el tráfico de dentro hacia afuera, en la página 41.

Figura 8: Nueva política



- **Licencias Smart**: asigne las licencias Smart que necesite para las funciones que desea implementar: **malware** (si desea utilizar la inspección de malware), **amenazas** (si pretende utilizar la prevención de intrusiones) y **URL** (si quiere implementar el filtrado de URL basado en categorías). **Nota:** Puede aplicar una licencia VPN de acceso remoto Client Secure tras agregar el usuario, desde la página de **Sistema** > **Licencias** > **Licencias Smart**.
- **ID de NAT única**: especifique la ID de NAT que especificó durante la configuración de inicial de Protección frente a amenazas.
- **Transferir paquetes**: permite que el dispositivo transfiera paquetes a Centro de administración. Si se desencadenan eventos como IPS o Snort con esta opción activada, el dispositivo envía información de metadatos de los eventos y datos sobre el paquete al Centro de administración para su inspección. Si la desactiva, solo se enviará la información del evento al Centro de administración, pero no se enviarán los datos del paquete.

Paso 3 Haga clic en **Registrar** o, si desea agregar otro dispositivo, haga clic en **Registrar y agregar otro** y confirme que el registro se ha realizado correctamente.

Si se ha completado, el dispositivo se agrega a la lista. Si ha ocurrido un error, verá un mensaje. Si no puede registrar el Protección frente a amenazas, compruebe los siguientes elementos:

- Ping: acceda a la dirección IP del Centro de administración con el siguiente comando:

  ping system *dirección_ip*

  Si el ping no se realiza correctamente, compruebe la configuración de red con el comando **show network**. Si necesita cambiar la dirección IP de administración de Protección frente a amenazas, utilice el comando **configure network** {**ipv4** | **ipv6**} **manual**.

- Clave de registro, ID de NAT y la dirección IP Centro de administración: compruebe que está utilizando la misma clave de registro y, si se utiliza, el ID de NAT en ambos dispositivos. Puede establecer la clave de registro y el ID de NAT en Centro de administración mediante el comando **configure manager add**.

Para obtener más información sobre la resolución de problemas, consulte https://cisco.com/go/fmc-reg-error.

Configurar una norma de seguridad básica

Esta sección describe cómo configurar una política de seguridad básica con la siguiente configuración:

- Interfaces interna y externa: asigne una dirección IP estática a la interfaz interna y utilice DHCP para la interfaz externa.
- Servidor DHCP: utilice un servidor DHCP en la interfaz interna para los clientes.
- Ruta predeterminada: agregue una ruta predeterminada a través de la interfaz externa.
- NAT: utilice la interfaz PAT en la interfaz externa.
- Control de acceso: permita el tráfico desde dentro hacia fuera.

Para configurar una política de seguridad básica, complete las siguientes tareas.

1	Configurar interfaces (6.5 y posterior), en la página 29 Configurar interfaces (6.4), en la página 33.
2	Configurar el servidor DHCP, en la página 36.
3	Añadir la ruta predeterminada, en la página 37.
4	Configurar NAT, en la página 38.
5	Permitir el tráfico de dentro hacia afuera, en la página 41.
6	Implementar la configuración, en la página 42.

Configurar interfaces (6.5 y posterior)

Agregue la interfaz VLAN1 para los puertos de switch o convierta los puertos de switch en interfaces de firewall, asigne interfaces a las zonas de seguridad y configure las direcciones IP. Normalmente, deberá configurar al menos un mínimo de dos interfaces para tener un sistema que pase tráfico significativo. Normalmente, tendrá una interfaz externa que da al router ascendente o a Internet, y una o más interfaces internas para las redes de su organización. De forma predeterminada, Ethernet1/1 es una interfaz de firewall normal que puede utilizar como externa y las interfaces restantes son puertos de switch en la VLAN1; después de agregar la interfaz VLAN1, puede convertirla en su interfaz interna. También puede asignar puertos de switch a otras VLAN o convertir puertos de switch a interfaces de firewall.

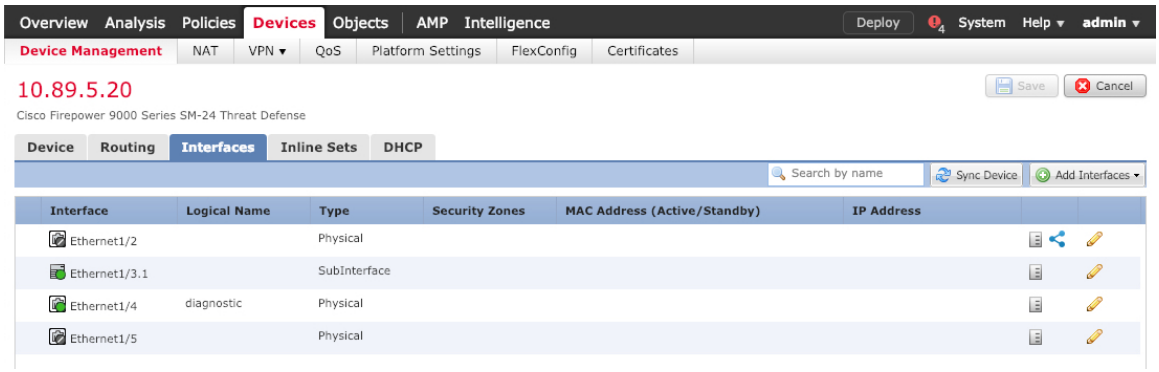
Una situación típica de enrutamiento de borde es obtener la dirección de la interfaz externa a través de DHCP de su ISP, mientras que usted define direcciones estáticas en las interfaces internas.

El siguiente ejemplo configura una interfaz interna de modo enrutado (VLAN1) con una dirección estática y una interfaz externa de modo enrutado mediante DHCP (Ethernet1/1).

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del dispositivo.

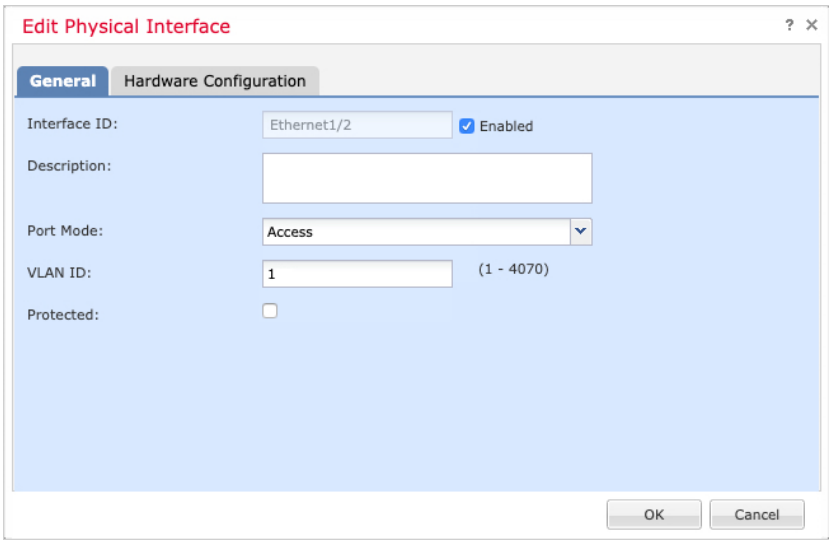
Paso 2 Haga clic en **Interfaces**.



Paso 3 (Opcional) Desactive el modo de puerto de switch para cualquiera de los puertos de switch (Ethernet1/2 a 1/8) haciendo clic en el deslizador de la columna **SwitchPort** para que se muestre como desactivado ().

Paso 4 Active los puertos del switch.

a) Haga clic en **Editar** (✎) para el puerto del switch.



b) Active la interfaz marcando la casilla de verificación **Activar**.

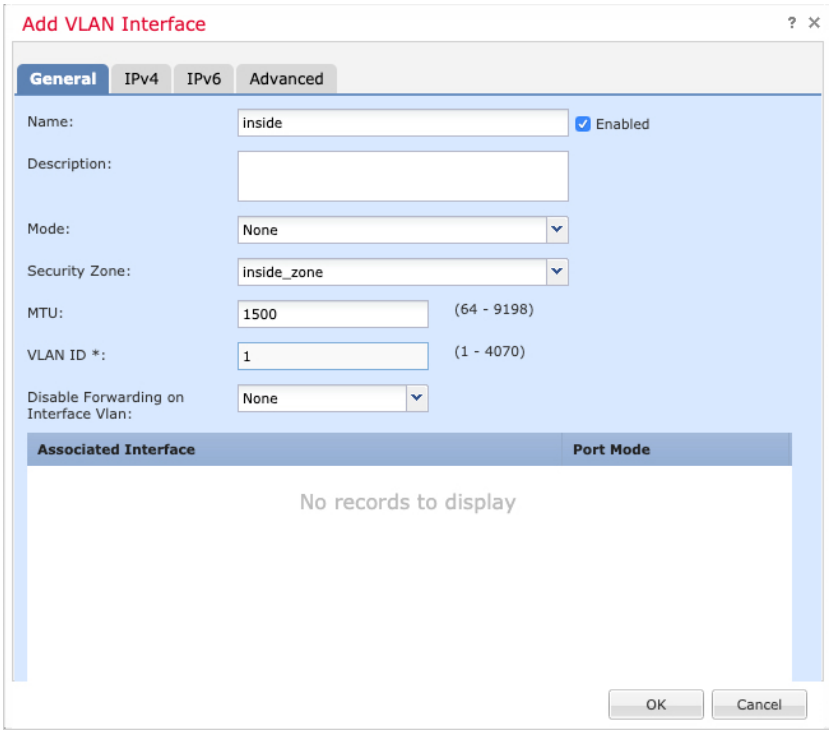
c) (Opcional) Cambie la ID de VLAN; el valor predeterminado es 1. A continuación, agregará una interfaz VLAN para que coincida con esta ID.

d) Haga clic en **Aceptar**.

Paso 5 Agregue la interfaz VLAN *interna*.

a) Haga clic en **Agregar interfaz** > **Interfaz VLAN**.

Aparece la pestaña **General**



b) Introduzca un **nombre** de hasta 48 caracteres de longitud.

Por ejemplo, asigne un nombre a la interfaz: **interna**.

c) Active la casilla **Activado**.

d) Deje el **modo** establecido en **Ninguno**.

e) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad interna existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, agregue una zona llamada **inside_zone**. Cada interfaz debe asignarse a una zona de seguridad o a un grupo de interfaces. Una interfaz solo puede pertenecer a una zona de seguridad, pero también puede pertenecer a varios grupos de interfaces. Aplicará su norma de seguridad en función de las zonas o los grupos. Por ejemplo, puede asignar la interfaz interna a la zona interna; y la interfaz externa a la zona externa. A continuación, puede configurar su política de control de acceso para permitir que el tráfico pase de dentro hacia fuera, pero no de fuera hacia dentro. La mayoría de las políticas solo admiten zonas de seguridad; puede utilizar zonas o grupos de interfaz en políticas NAT, políticas de prefiltro y políticas de QoS.

f) Establezca la **ID de VLAN** en **1**.

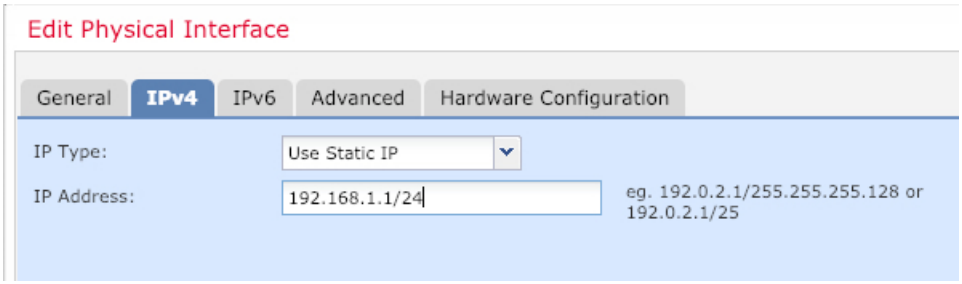
De forma predeterminada, todos los puertos de switch están configurados en VLAN1; si elige una ID de VLAN diferente aquí, también debe editar cada puerto de switch para que se encuentre en la nueva ID de VLAN.

No puede cambiar la ID de VLAN después de guardar la interfaz; la ID de VLAN es la etiqueta de VLAN utilizada y la ID de interfaz de su configuración.

g) Haga clic en la pestaña **IPv4** o **IPv6**.

- **IPv4**: elija **Usar IP estática** en la lista desplegable e introduzca una dirección IP y una máscara de subred en notación con barra.

  Por ejemplo, introduzca **192.168.1.1/24**

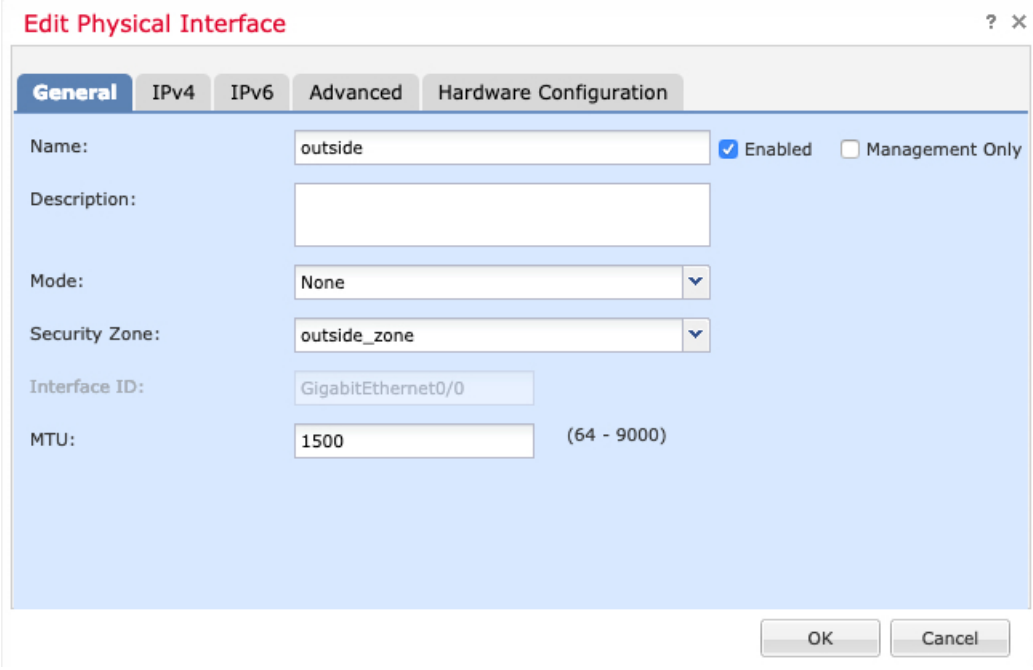


- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

h) Haga clic en **Aceptar**.

Paso 6 Haga clic en **Editar** (✎) para el Ethernet1/1 que quiera utilizar para la *externa*.

Aparece la pestaña **General**.



Nota Si ha configurado previamente esta interfaz para el acceso del administrador, la interfaz ya tendrá un nombre, se activará y se direccionará a ella. No debe modificar ninguno de estas configuraciones básicas porque interrumpiría la conexión de gestión de Centro de administración. Aún puede configurar la zona de seguridad en esta pantalla a través de las políticas de tráfico.

a) Introduzca un **nombre** de hasta 48 caracteres de longitud.

   Por ejemplo, asigne un nombre a la interfaz: **externa**.

b) Active la casilla **Activado**.

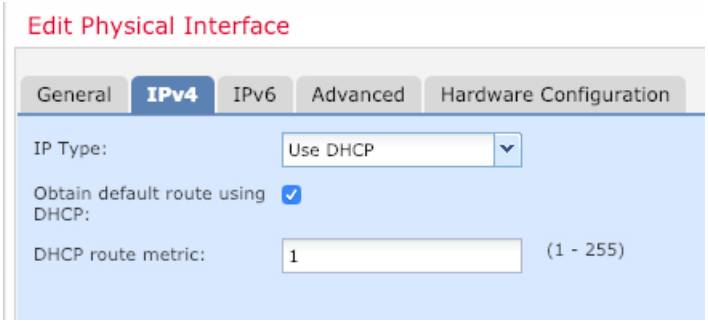
c) Deje el **modo** establecido en **Ninguno**.

d) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad externa existente o agregue una nueva haciendo clic en **Nueva**.

   Por ejemplo, añada una zona llamada **outside_zone**.

e) Haga clic en la pestaña **IPv4** o **IPv6**.

   - **IPv4**: elija **Usar DHCP** y configure los siguientes parámetros opcionales:
     - **Obtener la ruta predeterminada mediante DHCP**: obtiene la ruta predeterminada del servidor DHCP.
     - **Métrica de la ruta DHCP**: asigna una distancia administrativa a la ruta aprendida entre 1 y 255. La distancia administrativa predeterminada para las rutas aprendidas es 1.



- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

f) Haga clic en **Aceptar**.

Paso 7 Haga clic en **Guardar**.

Configurar interfaces (6.4)

Active las interfaces de la Protección frente a amenazas, asígnelas a zonas de seguridad y configure las direcciones IP. Normalmente, deberá configurar al menos un mínimo de dos interfaces para tener un sistema que pase tráfico significativo. Normalmente, tendrá una interfaz externa que da al router ascendente o a Internet, y una o más interfaces internas para las redes de su organización. Algunas de estas interfaces pueden ser "zonas desmilitarizadas" (DMZ), donde se colocan activos de acceso público, como el servidor web.

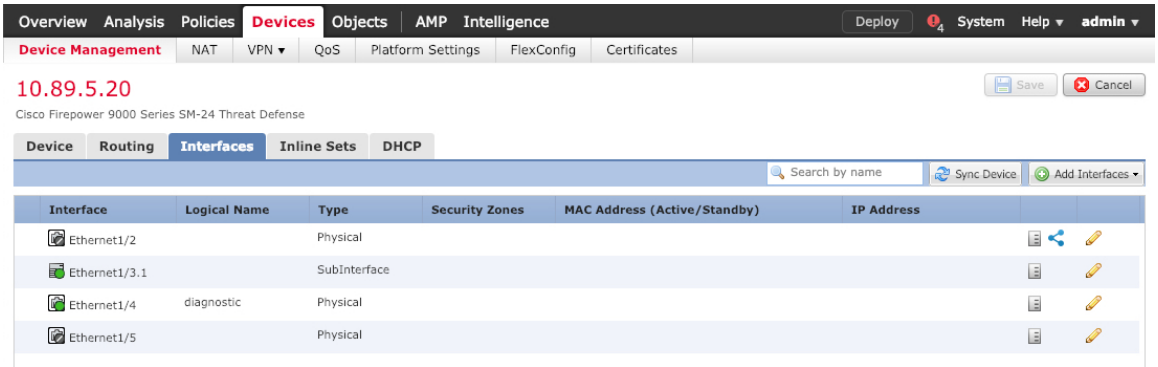
Una situación típica de enrutamiento de borde es obtener la dirección de la interfaz exterior a través de DHCP de su ISP, mientras que usted define direcciones estáticas en las interfaces interiores.

El siguiente ejemplo configura una interfaz interna de modo enrutado con una dirección estática y una interfaz externa de modo enrutado mediante DHCP.

Procedimiento

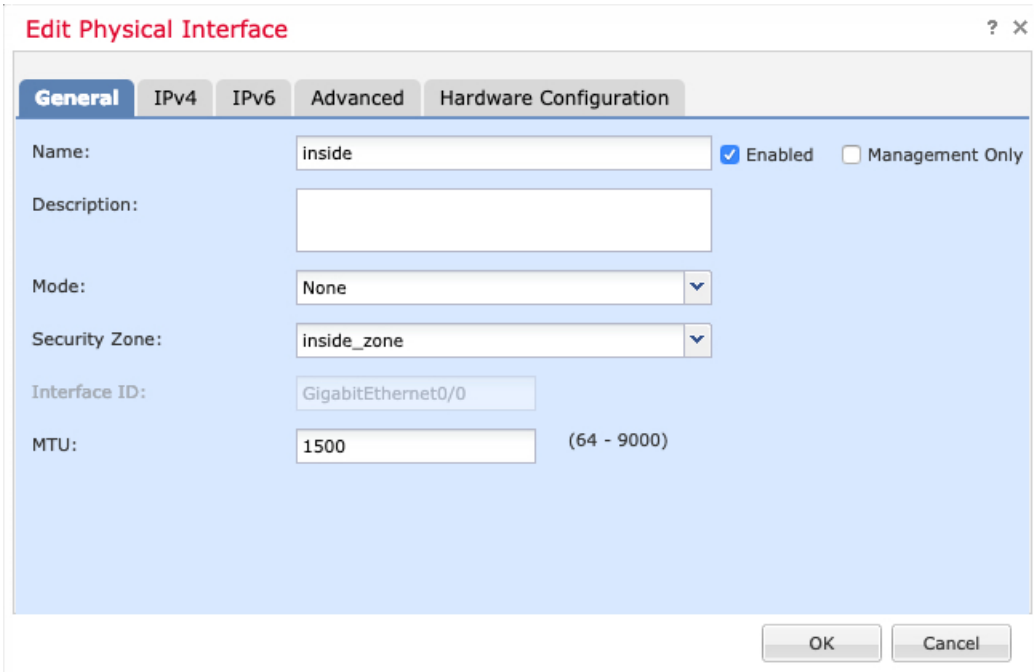
Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del firewall.

Paso 2 Haga clic en **Interfaces**.



Paso 3 Haga clic en **Editar** (✎) de la interfaz que desea utilizar para el *interior*.

Aparece la pestaña **General**



a) Introduzca un **nombre** de hasta 48 caracteres de longitud.

Por ejemplo, asigne un nombre a la interfaz: **interna**.

b) Active la casilla **Activado**.

c) Deje el **modo** establecido en **Ninguno**.

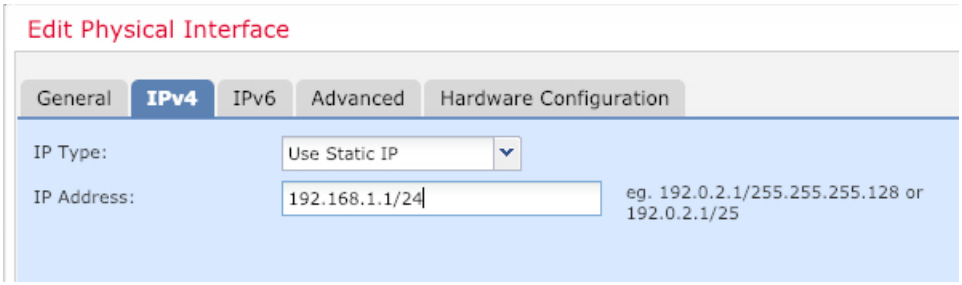
d) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad interna existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, agregue una zona llamada **inside_zone**. Cada interfaz debe asignarse a una zona de seguridad o a un grupo de interfaces. Una interfaz solo puede pertenecer a una zona de seguridad, pero también puede pertenecer a varios grupos de interfaces. Aplicará su norma de seguridad en función de las zonas o los grupos. Por ejemplo, puede asignar la interfaz interna a la zona interna; y la interfaz externa a la zona externa. A continuación, puede configurar su política de control de acceso para permitir que el tráfico pase de dentro hacia fuera, pero no de fuera hacia dentro. La mayoría de las políticas solo admiten zonas de seguridad; puede utilizar zonas o grupos de interfaz en políticas NAT, políticas de prefiltro y políticas de QoS.

e) Haga clic en la pestaña **IPv4** o **IPv6**.

- **IPv4**: elija **Usar IP estática** en la lista desplegable e introduzca una dirección IP y una máscara de subred en notación con barra.

  Por ejemplo, introduzca **192.168.1.1/24**

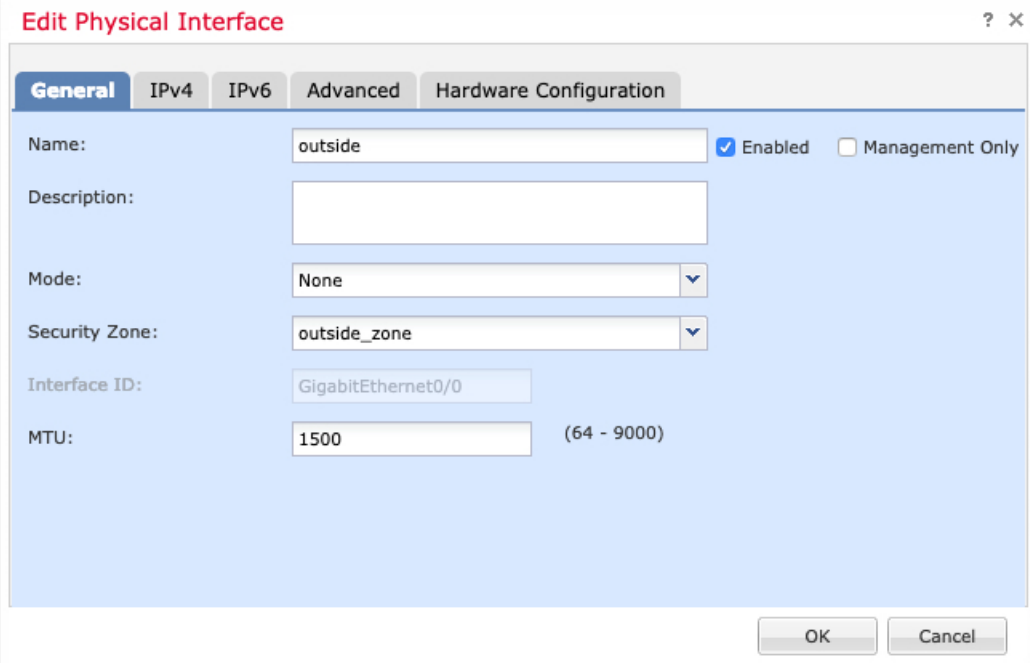


- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

f) Haga clic en **Aceptar**.

Paso 4 Haga clic en **Editar** (✎) de la interfaz que desea utilizar para el *exterior*.

Aparece la pestaña **General**.



Nota Si ha configurado previamente esta interfaz para el acceso del administrador, la interfaz ya tendrá un nombre, se activará y se direccionará a ella. No debe modificar ninguno de estas configuraciones básicas porque interrumpiría la conexión de gestión del Centro de administración. Aún puede configurar la zona de seguridad en esta pantalla a través de las políticas de tráfico.

a) Introduzca un **nombre** de hasta 48 caracteres de longitud.

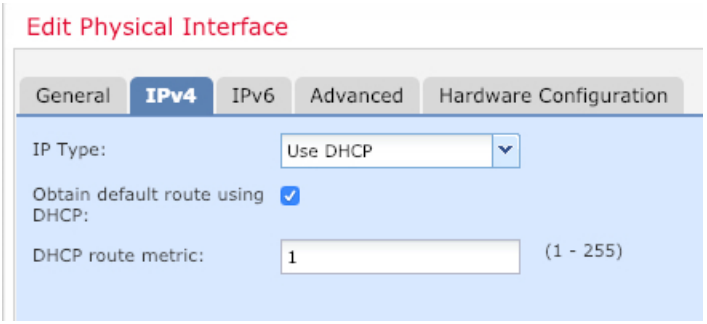
Por ejemplo, asigne un nombre a la interfaz: **externa**.

b) Active la casilla **Activado**.
c) Deje el **modo** establecido en **Ninguno**.
d) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad externa existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, añada una zona llamada **outside_zone**.

e) Haga clic en la pestaña **IPv4** o **IPv6**.

- **IPv4**: elija **Usar DHCP** y configure los siguientes parámetros opcionales:
  - **Obtener la ruta predeterminada mediante DHCP**: obtiene la ruta predeterminada del servidor DHCP.
  - **Métrica de la ruta DHCP**: asigna una distancia administrativa a la ruta aprendida entre 1 y 255. La distancia administrativa predeterminada para las rutas aprendidas es 1.



- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

f) Haga clic en **Aceptar**.

Paso 5 Haga clic en **Guardar**.

Configurar el servidor DHCP

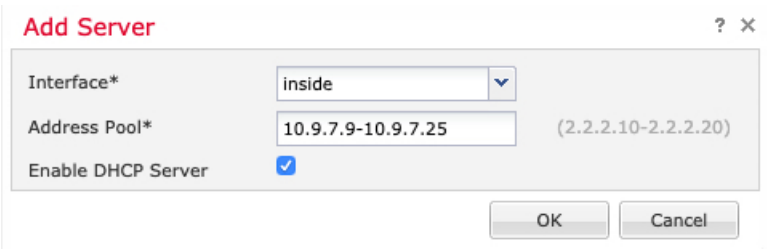
Active el servidor DHCP si desea que los clientes utilicen DHCP para obtener direcciones IP de Protección frente a amenazas.

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del dispositivo.

Paso 2 Seleccione **DHCP** > **Servidor DHCP**.

Paso 3 En la página **Servidor**, haga clic en **Agregar** y configure las siguientes opciones:



- **Interfaz**: elija la interfaz en la lista desplegable.

- **Conjunto de direcciones**: establezca el rango de direcciones IP de menor a mayor que utiliza el servidor DHCP. El rango de direcciones IP debe estar en la misma subred que la interfaz seleccionada y no puede incluir la dirección IP de la propia interfaz.
- **Habilitar servidor DHCP**: habilite el servidor DHCP en la interfaz seleccionada.

Paso 4 Haga clic en **Aceptar**.

Paso 5 Haga clic en **Guardar**.

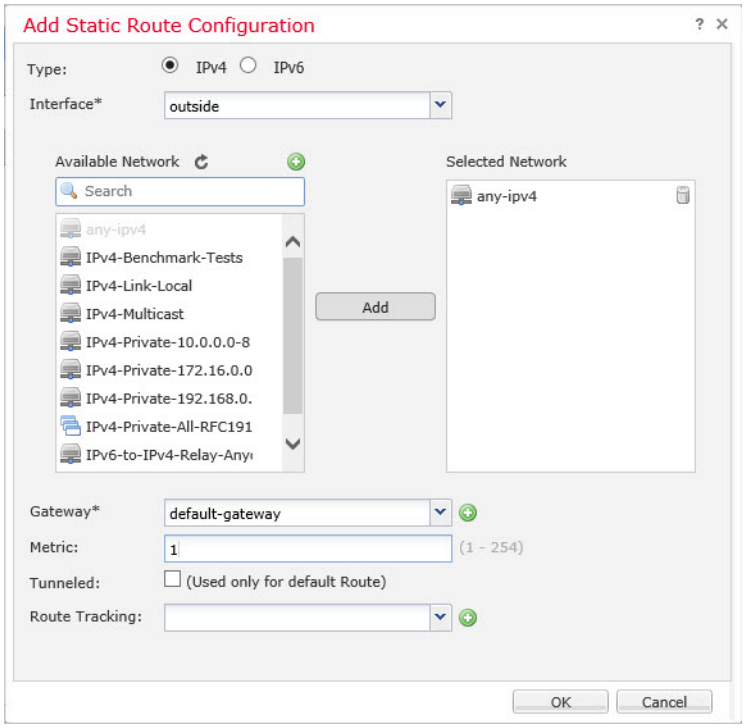
Añadir la ruta predeterminada

La ruta predeterminada suele señalar hacia el router ascendente que se puede alcanzar en la interfaz externa. Si utiliza DHCP para la interfaz externa, es posible que su dispositivo ya haya recibido una ruta predeterminada. Si necesita agregar manualmente la ruta, siga este procedimiento. Si ha recibido una ruta predeterminada del servidor DHCP, se mostrará en la tabla **Rutas IPv4** o **Rutas IPv6** en la página **Dispositivos** > **Administración de dispositivos** > **Rutas** > **Ruta estática**.

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del dispositivo.

Paso 2 Seleccione **Rutas** > **Ruta estática**, haga clic en **Agregar ruta** y determine lo siguiente:

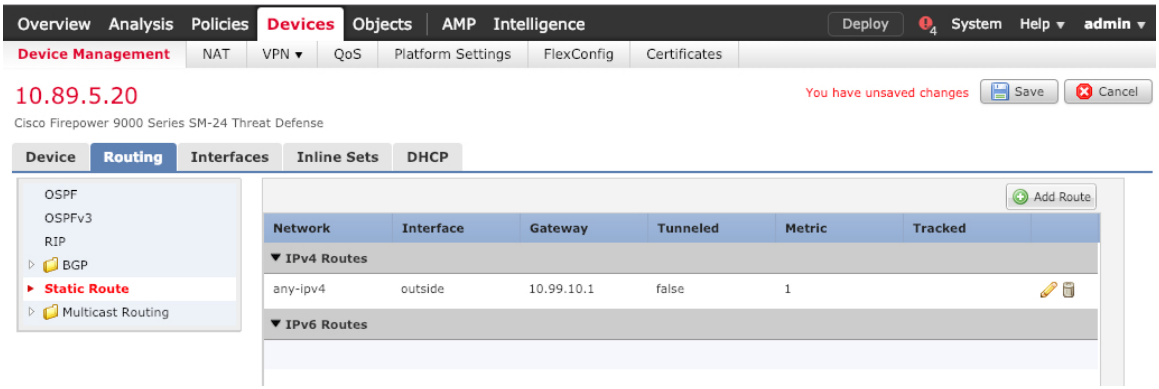


- **Tipo**: haga clic en el botón de opción **IPv4** o **IPv6** en función del tipo de ruta estática que esté agregando.
- **Interfaz**: elija la interfaz de salida; normalmente la interfaz externa.

- **Red disponible**: seleccione **any-ipv4** para una ruta predeterminada IPv4 o **any-ipv6** para una ruta predeterminada IPv6 y haga clic en **Agregar** para moverla a la lista **Red seleccionada**.
- **Gateway** o **Gateway de IPv6**: introduzca o seleccione el router de gateway que sea el siguiente salto para esta ruta. Puede proporcionar una dirección IP o un objeto de redes/host.
- **Métricas**: introduzca el número de saltos hacia la red de destino. Los valores válidos van de 1 a 255; el valor predeterminado es 1.

Paso 3 Haga clic en **Aceptar**.

La ruta se agrega a la tabla de rutas estáticas.



Paso 4 Haga clic en **Guardar**.

Configurar NAT

Una regla NAT típica convierte las direcciones internas a un puerto en la dirección IP de la interfaz externa. Este tipo de regla NAT se denomina *traducción de dirección del puerto de interfaz (PAT)*.

Procedimiento

Paso 1 Seleccione **Dispositivos** > **NAT**y haga clic en **Nueva política** > **NAT de Threat Defense**.

Paso 2 Asigne un nombre a la política, seleccione los dispositivos en los que la desea aplicar y haga clic en **Guardar**.

La política se agrega al Centro de administración. Aún tiene que añadir reglas a la política.

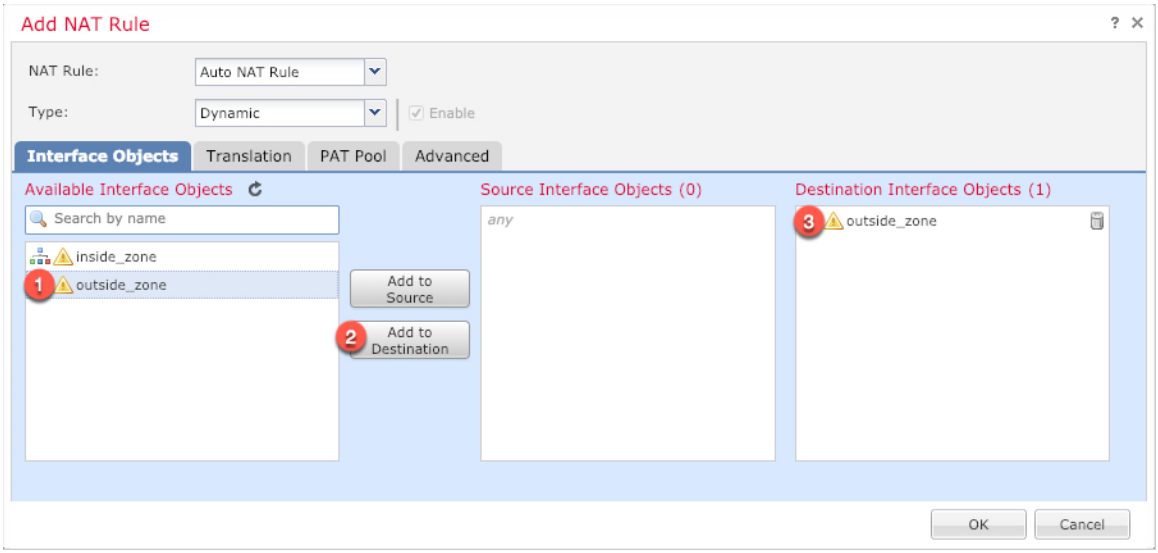
Paso 3 Haga clic en **Agregar regla**.

Aparece el cuadro de diálogo **Agregar regla NAT**.

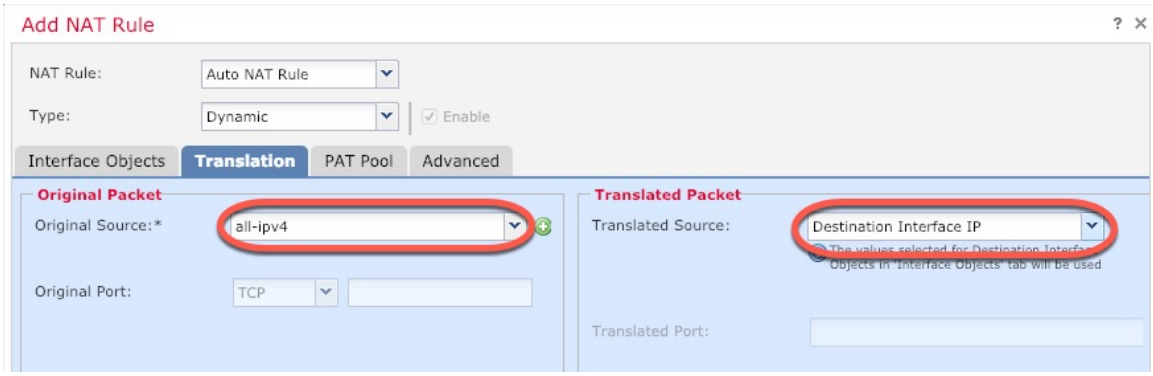
Paso 4 Configure las opciones de regla básicas:

- **Regla NAT**: elija una **regla NAT automática**.
- **Tipo**: seleccione **Dinámico**.

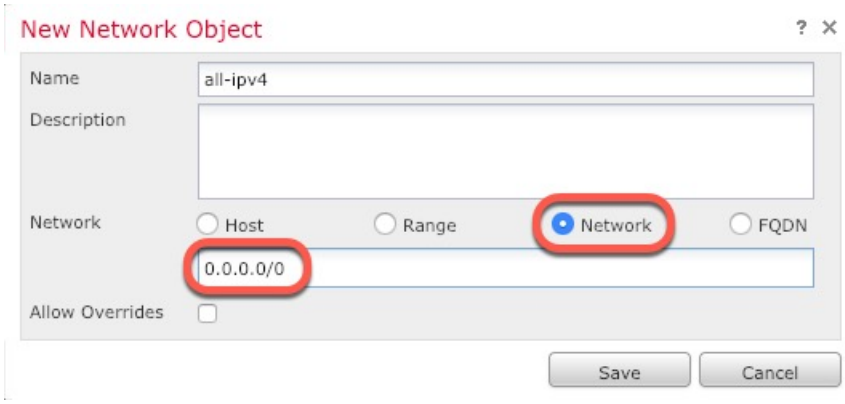
Paso 5 En la página **Objetos de interfaz**, agregue la zona exterior del área **Objetos de interfaz disponibles** al área **Objetos de interfaz de destino**.



Paso 6 En la página **Traducción**, configure las siguientes opciones:



- **Fuente original**: haga clic en **Agregar** (+) para agregar un objeto de red para todo el tráfico IPv4 (0.0.0.0/0).

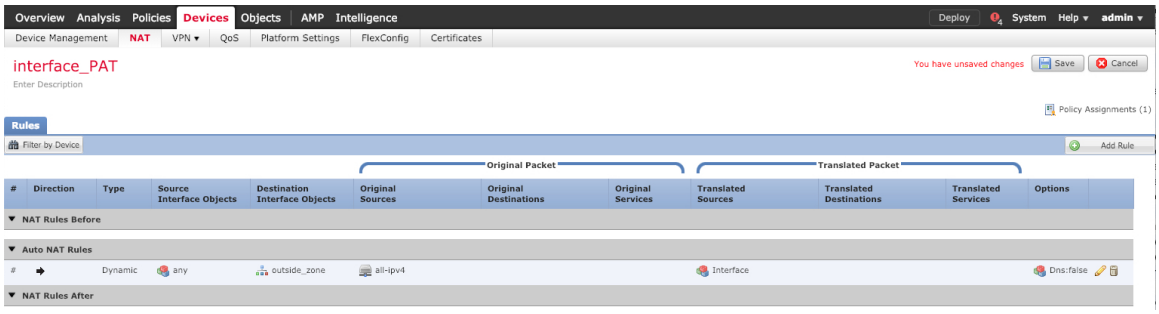


Nota No puede utilizar el objeto **any-ipv4** definido por el sistema, ya que las reglas NAT automáticas añaden NAT como parte de la definición del objeto y no puede editar objetos definidos por el sistema.

- **Fuente traducida**: seleccione la **IP de la interfaz de destino**.

Paso 7 Haga clic en **Guardar** para agregar la regla.

La regla se guarda en la tabla **Reglas**.



Paso 8 Haga clic en **Guardar** en la página de **NAT** para guardar los cambios.

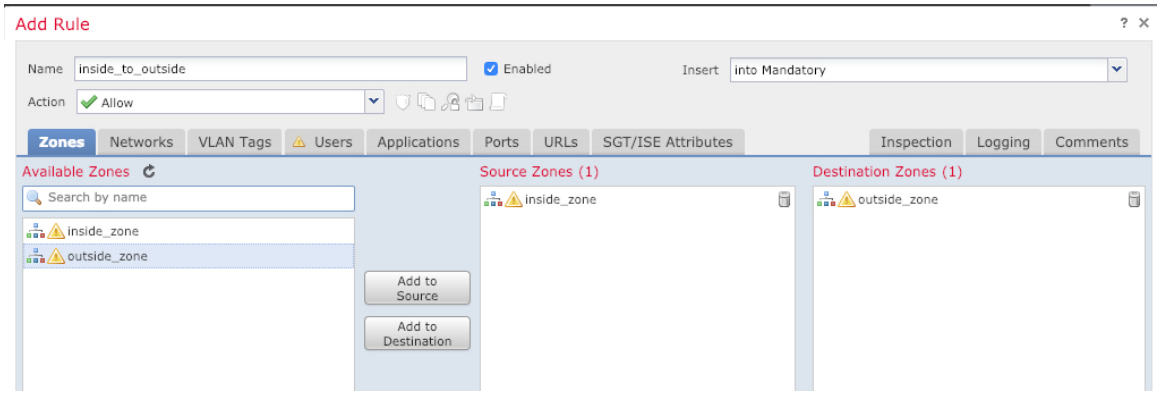
Permitir el tráfico de dentro hacia afuera

Si creó una política básica de control de acceso **Bloquear todo el tráfico** cuando registró la Protección frente a amenazas, entonces debe agregar reglas a la política para permitir el tráfico a través del dispositivo. El siguiente procedimiento agrega una regla para permitir el tráfico de la zona interna a la zona externa. Si tiene otras zonas, asegúrese de agregar reglas que permitan el tráfico a las redes adecuadas.

Procedimiento

Paso 1 Seleccione **Política** > **Política de acceso** > **Política de acceso** y haga clic en **Editar** ( ) para la política de control de acceso asignada a la Protección frente a amenazas.

Paso 2 Haga clic en **Agregar regla** y establezca los siguientes parámetros:

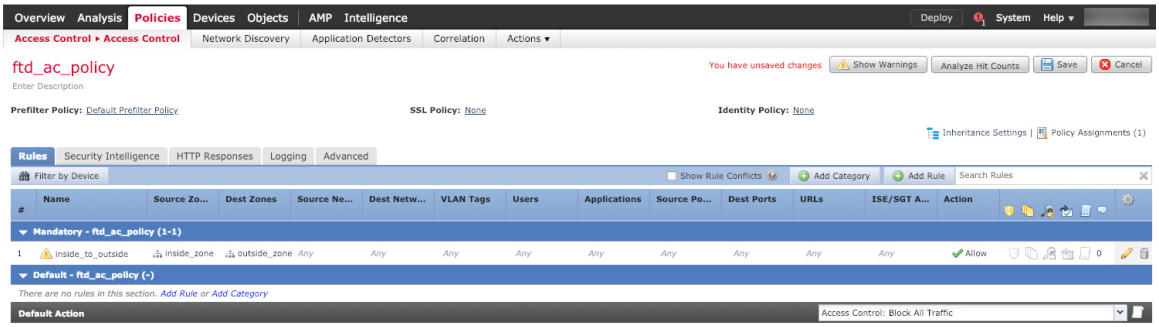


- **Nombre**: nombre esta regla, por ejemplo, **inside_to_outside**.
- **Zonas de origen**: seleccione la zona interna de las **Zonas disponibles** y haga clic en **Agregar al origen**.
- **Zonas de destino**: seleccione la zona externa de las **Zonas disponibles** y haga clic en **Agregar al destino**.

Deje la otra configuración como está.

Paso 3 Haga clic en **Agregar**.

La regla se agrega a la tabla **Reglas**.



Paso 4 Haga clic en **Guardar**.

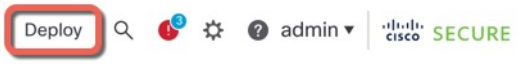
Implementar la configuración

Implementar los cambios de configuración en Protección frente a amenazas; ningún cambio estará activo en el dispositivo hasta que los implemente.

Procedimiento

Paso 1 Haga clic en **Implementar** en la parte superior derecha.

Figura 9: Implementar



Paso 2 Haga clic en **Implementar todo** para implementar en todos los dispositivos o haga clic en **Implementación avanzada** para implementar en los dispositivos seleccionados.

Figura 10: Implementar todo

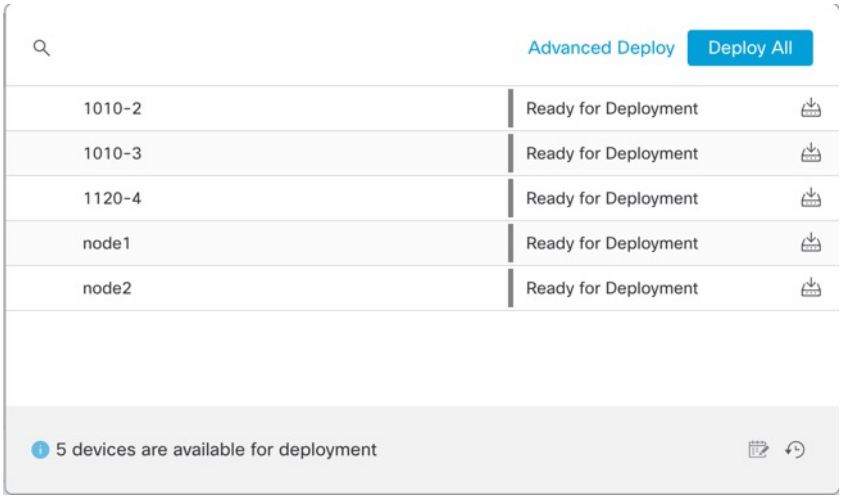
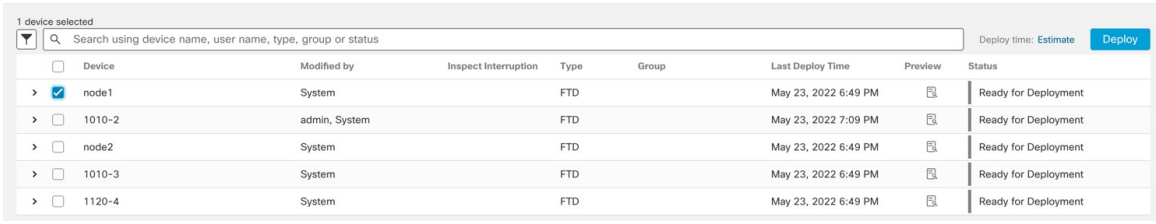
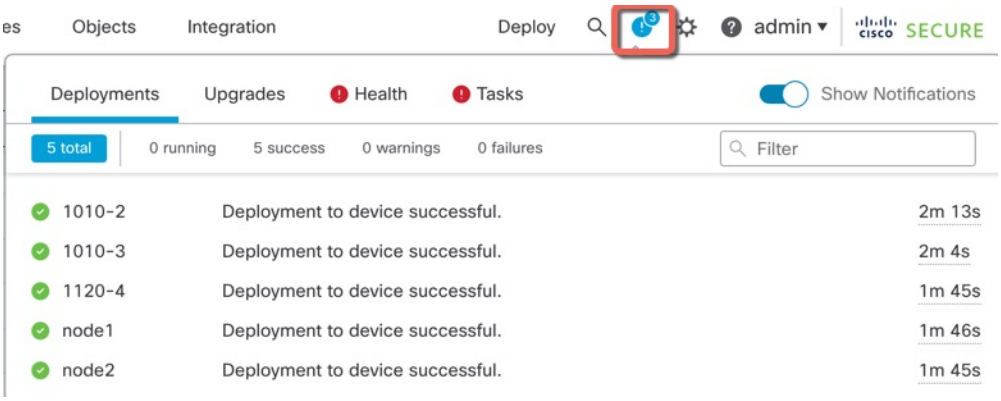


Figura 11: Implementación avanzada



Paso 3 Compruebe que la implementación se realiza correctamente. Haga clic en el icono a la derecha del botón **Implementar** en la barra de menú para ver el estado de las implementaciones.

Figura 12: Estado de la implementación



Acceder a la Protección frente a amenazas y a la CLI de FXOS

Utilice la interfaz de línea de comandos (CLI) para configurar el sistema y solucionar los problemas básicos. No puede configurar políticas a través de una sesión de CLI. Puede acceder a la CLI conectándose al puerto de consola.

También puede acceder a CLI de FXOS para solucionar problemas

Nota Como alternativa, puede utilizar SSH para la interfaz de administración del dispositivo Protección frente a amenazas. A diferencia de una sesión de consola, la sesión SSH se establece de forma predeterminada en la CLI de Protección frente a amenazas, desde la que puede conectarse a CLI de FXOS mediante el comando **connect fxos**. Puede conectarse después a la dirección en una interfaz de datos si abre esa interfaz para las conexiones SSH. El acceso SSH para las interfaces de datos está desactivado de forma predeterminada. Este procedimiento describe el acceso al puerto de consola, cuyo valor predeterminado es CLI de FXOS.

Procedimiento

Paso 1 Para iniciar sesión en la CLI, conecte su ordenador de gestión al puerto de consola. Firepower 1000 va con un cable de serie USB A a B. Instale las unidades USB de serie necesarias para su sistema operativo (consulte la guía de hardware de Firepower 1010). El puerto de consola de forma predeterminada es CLI de FXOS. Utilice la siguiente configuración de serie:

- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada

Se conecta a la CLI de FXOS. Inicie sesión en la CLI con el nombre de usuario **admin** y la contraseña que estableció en la configuración inicial (la predeterminada es **Admin123**).

Ejemplo:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Paso 2 Acceda a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Después de iniciar sesión, para obtener información sobre los comandos disponibles en la CLI, introduzca **help** o **?**. Para obtener información sobre cómo utilizarla, consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Paso 3 Para abandonar la CLI de Protección frente a amenazas, introduzca el comando **exit** o **logout**.

Este comando le devuelve al mensaje de CLI de FXOS. Para obtener información sobre los comandos disponibles en la CLI de FXOS, introduzca **?**.

Ejemplo:

```
> exit
firepower#
```

Apagar el firewall

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su sistema de firewall.

El chasis de Firepower 1010 no cuenta con un interruptor de alimentación externo. Puede apagar el dispositivo mediante la página de gestión de dispositivos del Centro de administración o la CLI de FXOS.

Desactive el firewall mediante Centro de administración

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación o pulsa el interruptor de alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su firewall.

Puede apagar el sistema correctamente con el Centro de administración.

Procedimiento

Paso 1 Elija **Dispositivo** > **Administración de dispositivos**.

Paso 2 Junto al dispositivo que desea reiniciar, haga clic en el icono de editar ( ).

Paso 3 Haga clic en la pestaña **Dispositivo**.

Paso 4 Haga clic en el icono de apagar dispositivo ( ) en la sección **Sistema**.

Paso 5 Cuando se le solicite, confirme que desea apagar el dispositivo.

Paso 6 Si tiene una conexión de consola al firewall, monitorice los mensajes del sistema una vez que este se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si no tiene una conexión de consola, espere aproximadamente 3 minutos para asegurarse de que el sistema se ha apagado.

Paso 7 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

Apagar el dispositivo en la CLI

Puede utilizar la CLI de FXOS para apagar el sistema de forma segura y apagar el dispositivo. Se accede a la CLI conectándose al puerto de la consola; consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 44.

Procedimiento

Paso 1 En el CLI de FXOS, conéctese a local-mgmt:

firepower # **connect local-mgmt**

Paso 2 Ejecute el comando **shutdown**:

firepower(local-mgmt) # **shutdown**

Ejemplo:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Paso 3 Supervise las indicaciones del sistema cuando el firewall se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Paso 4 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

¿Qué es lo siguiente que debe hacer?

Para continuar con la configuración de la Protección frente a amenazas, consulte los documentos disponibles para su versión de software en Navegación por la documentación de Cisco Firepower.

Para obtener información relacionada con el uso del Centro de administración, consulte la Guía de configuración del Centro de administración de Firepower.

CAPÍTULO 3

Implementación de la Protección frente a amenazas con control remoto del Centro de administración

¿Este capítulo es para usted?

Para ver todos los sistemas operativos y administradores disponibles, consulte ¿Qué aplicación y administrador son adecuados para usted?, en la página 1. Este capítulo se aplica para la Protección frente a amenazas en una sucursal remota que utiliza el Centro de administración de una sede central.

Cada Protección frente a amenazas controla, inspecciona, supervisa y analiza el tráfico y, a continuación, informa a un Centro de administración administrador. El Centro de administración proporciona una consola de administrador centralizada con una interfaz web que puede utilizar para realizar tareas administrativas, de administración, análisis e informes en servicio para proteger su red local.

- Un administrador de la sede central configura previamente la Protección frente a amenazas en la CLI o mediante el Administrador del dispositivo y, a continuación, envía la Protección frente a amenazas a la sucursal remota.
- El administrador de la sucursal conecta y enciende la Protección frente a amenazas.
- El administrador central completa la configuración de la Protección frente a amenazas utilizando el Centro de administración.

Nota La implementación de sucursales remotas requiere la versión 6.7 o posterior.

Sobre el firewall

El hardware puede ejecutar el software Protección frente a amenazas o el software ASA. Para cambiar entre Protección frente a amenazas y ASA es necesario que vuelva a crear una imagen para el dispositivo. También es necesario que lleve a cabo una una recreación de imagen si necesita una versión de software diferente a la instalada. Consulte Recreación de la imagen del dispositivo de defensa contra amenazas de Firepower o ASA de Cisco.

El firewall ejecuta un sistema operativo subyacente llamado Cisco Secure Firewall Extensible Operating System (FXOS). El firewall no es compatible con el Administrador del chasis Cisco Secure Firewall de FXOS; solo se admite una CLI limitada para la resolución de problemas. Consulte Guía de resolución de problemas

de Cisco FXOS para Firepower 1000/2100 Series que ejecuta Firepower Threat Defense para obtener más información.

Declaración de recopilación de privacidad: el firewall no necesita ni recopila de forma activa información de identificación personal. Sin embargo, puede utilizar información de identificación personal en la configuración, por ejemplo, para los nombres de usuario. En este caso, un administrador podrá ver esta información cuando trabaje con la configuración o cuando utilice SNMP.

Cómo funciona la gestión remota

Para permitir que el Centro de administración administre la Protección frente a amenazas a través de Internet, utilice la interfaz externa para la administración del Centro de administración en lugar de la interfaz de administración. Debido a que la mayoría de las sucursales remotas solo tienen una única conexión a Internet, el acceso externo al Centro de administración hace posible que se pueda gestionar de forma centralizada.

Nota Puede utilizar cualquier interfaz de datos *any* para acceder al administrador, por ejemplo, la interfaz interna si tiene un Centro de administración interno. Sin embargo, esta guía trata sobre todo el acceso a la interfaz externa, ya que es la situación más probable para las sucursales remotas.

La interfaz de administración es una interfaz especial configurada por separado de las interfaces de datos de Protección frente a amenazas y tiene su propia configuración de red. Los ajustes de red de la interfaz de administración se siguen usando aunque active el acceso al administrador en una interfaz de datos. Todo el tráfico de administración viene o va desde la interfaz de gestión. Cuando se habilita el acceso al administrador en una interfaz de datos, la Protección frente a amenazas reenvía el tráfico de administración entrante por la placa base a la interfaz de administración. Para el tráfico de gestión saliente, la interfaz de gestión lo reenvía por la placa base a la interfaz de datos.

Acceder al administrador desde una interfaz de datos tiene las siguientes limitaciones:

- Solo puede habilitar el acceso al administrador en una sola interfaz de datos física. No puede utilizar una subinterfaz o un EtherChannel.
- Esta interfaz no puede ser solo de administración.
- Solo modo de firewall enrutado, mediante una interfaz enrutada.
- PPPoE no es compatible. Si su ISP requiere PPPoE, deberá colocar un router compatible con PPPoE entre la Protección frente a amenazas y el módem WAN.
- La interfaz debe estar solo en el VRF global.
- SSH no está activado de forma predeterminada para las interfaces de datos, por lo que deberá habilitar SSH más adelante con el Centro de administración. Como la gateway de la interfaz de gestión se cambiará para que sean las interfaces de datos, tampoco puede utilizar SSH para la interfaz de gestión desde una

red remota a menos que agregue una ruta estática para ella mediante el comando **configure network static-routes**.

- La alta disponibilidad no es compatible. Debe utilizar la interfaz de administración en este caso.

La siguiente figura muestra el Centro de administración en la sede central y la Protección frente a amenazas con acceso al administrador en la interfaz externa.

Tanto la Protección frente a amenazas como el Centro de administración necesitan una dirección IP pública o un nombre de host para permitir la conexión de gestión entrante; es necesario que conozca esta IP para la configuración inicial. De forma opcional, también puede configurar el DNS dinámico (DDNS) para la interfaz externa para dar cabida a las cambiantes asignaciones de IP del DHCP.

Figura 13:

Antes de comenzar

Implemente y lleve a cabo la configuración inicial del Centro de administración. Consulte la Guía de instalación del hardware de Cisco Firepower Management Center 1600, 2600 y 4600 o Guía de inicio de Cisco Firepower Management Center Virtual.

Procedimiento completo

Consulte las siguientes tareas para implementar la Protección frente a amenazas con el Centro de administración en su chasis.

Figura 14: Procedimiento completo

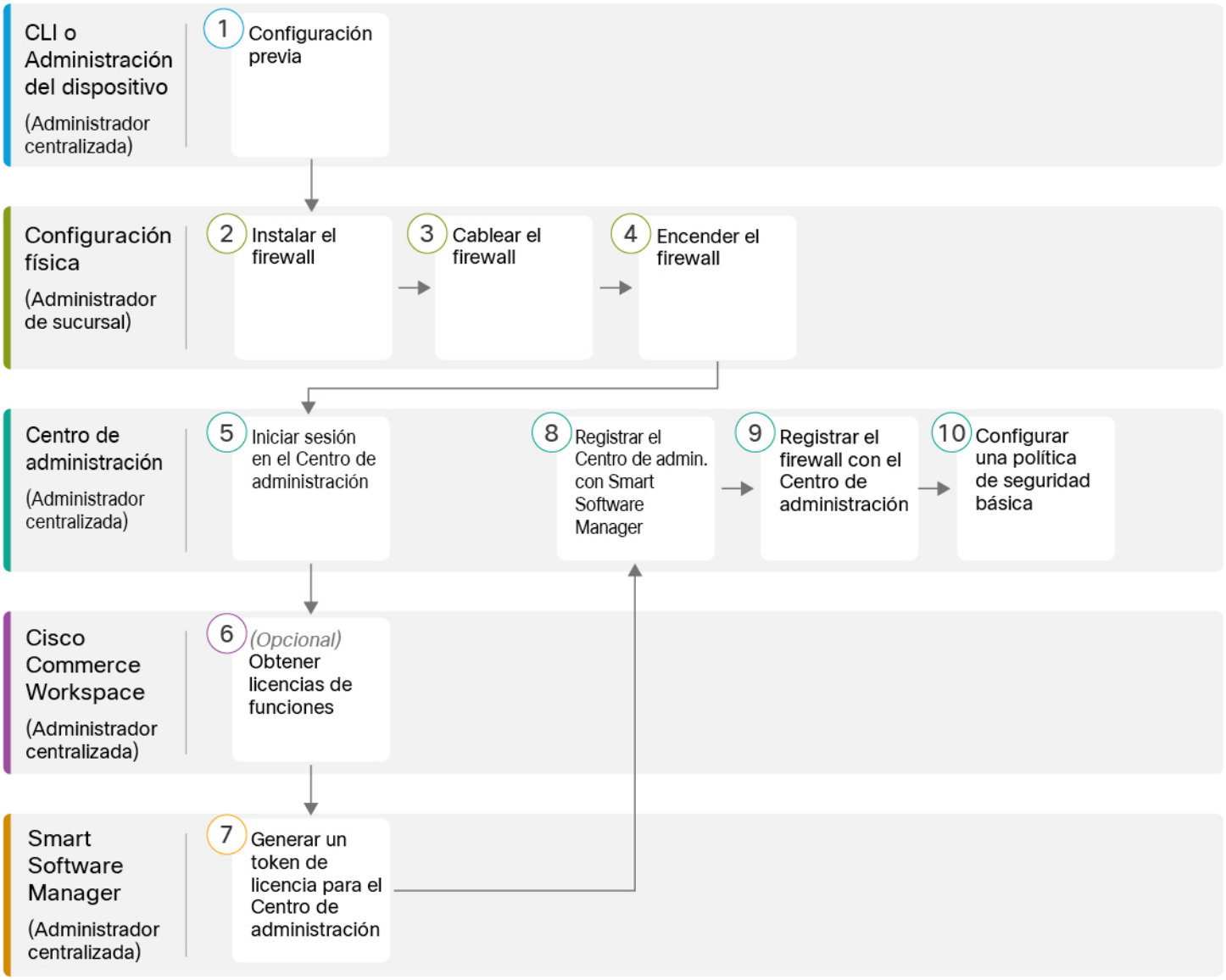


Figura 15: Procedimiento completo

1	CLI o Administrador del dispositivo (Administrador centralizada)	• (Opcional) Comprobar el software e instalar una nueva versión, en la página 52 • Configuración previa con la CLI, en la página 59 • Configuración previa mediante Administrador del dispositivo, en la página 53
2	Configuración física (Administrador de sucursal)	Instale el firewall. Consulte la guía de instalación del hardware.
3	Configuración física (Administrador de sucursal)	Cablear el firewall, en la página 64.
4	Configuración física (Administrador de sucursal)	Encender el dispositivo, en la página 65
5	Centro de administración (Administrador centralizada)	Administrador central: Iniciar sesión en el Centro de administración, en la página 24.
6	Cisco Commerce Workspace (Administrador centralizada)	Obtener licencias para el Centro de administración, en la página 67: comprar licencias de funciones.
7	Smart Software Manager (Administrador centralizada)	Obtener licencias para el Centro de administración, en la página 67: generar un token de licencia para el Centro de administración.
8	Centro de administración (Administrador centralizada)	Obtener licencias para el Centro de administración, en la página 67: registrar el Centro de administración con el servidor de licencias Smart.
9	Centro de administración (Administrador centralizada)	Registrar la Protección frente a amenazas con el Centro de administración, en la página 68.

10	Centro de administración (Administrador centralizada)	Configurar una norma de seguridad básica, en la página 71.

Configuración previa del administrador central

Debe preconfigurar la Protección frente a amenazas antes de enviarla a la sucursal.

(Opcional) Comprobar el software e instalar una nueva versión

Para comprobar la versión del software e instalar una versión diferente, si es necesario, siga estos pasos. Le recomendamos que instale su versión de destino antes de configurar el firewall. Como alternativa, puede realizar una actualización una vez que esté en funcionamiento, pero la actualización, que conserva su configuración, puede llevar más tiempo que este procedimiento.

¿Qué versión debo ejecutar?

Cisco recomienda ejecutar una versión Gold Star indicada con una estrella dorada junto al número de versión en la página de descarga de software. También puede consultar la estrategia de versiones descrita en https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; Por ejemplo, este boletín describe la numeración de las versiones a corto plazo (con las características más recientes), la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para un período de tiempo más largo) o la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para el período de tiempo más largo, para la certificación del gobierno).

Procedimiento

Paso 1 Conéctese a la CLI. Consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 82 para obtener más información. Este procedimiento se muestra a través del puerto de consola, pero también puede utilizar SSH en su lugar.

Inicie sesión con el usuario **administrador** y la contraseña predeterminada **Admin123**.

Se conecta a la CLI de FXOS. La primera vez que inicie sesión, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se cambió la contraseña, y no lo sabe, debe llevar a cabo una restauración de fábrica para recuperar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el Procedimiento de restauración de fábrica.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
```

```
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 2 En la CLI de FXOS, muestre la versión en ejecución.

scope ssa

show app-instance

Ejemplo:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Paso 3 Si desea instalar una nueva versión, lleve a cabo estos pasos.

a) Si necesita establecer una dirección IP estática para la interfaz de administración, consulte Configuración previa con la CLI, en la página 59. La interfaz de administración utiliza por defecto DHCP.

Tendrá que descargar la nueva imagen de un servidor accesible desde la interfaz de administración.

b) Lleve a cabo el procedimiento de recrear la imagen que aparece en la guía de resolución de problemas de FXOS.

Configuración previa mediante Administrador del dispositivo

Conéctese a Administrador del dispositivo para realizar la configuración inicial de la Protección frente a amenazas. Cuando lleva a cabo la configuración inicial con Administrador del dispositivo, *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se conserva al cambiar al Centro de administración para la gestión, además de la configuración de acceso del administrador y la interfaz de administración. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso o las zonas de seguridad. Cuando utiliza la CLI, solo se conservan la configuración de acceso del administrador y la interfaz de administración (por ejemplo, no se conserva la configuración de la interfaz interna de forma predeterminada).

Antes de empezar

- Implemente y lleve a cabo la configuración inicial del Centro de administración. Consulte la Guía de instalación del hardware de Cisco Firepower Management Center 1600, 2600 y 4600. Necesitará conocer la dirección IP o el nombre de host del Centro de administración antes de configurar la Protección frente a amenazas.
- Utilice una versión actual de Firefox, Chrome, Safari, Edge o Internet Explorer.

Procedimiento

Paso 1 Conecte su equipo de administración a la interfaz interna (Ethernet1/2 a 1/8)

Paso 2 Encienda el firewall.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Paso 3 Inicie sesión en Administrador del dispositivo.

a) Introduzca la siguiente URL en su navegador: **https://192.168.95.1**
b) Inicie sesión con el nombre de usuario **admin** y la contraseña predeterminada **Admin123**.
c) Se le pedirá que lea y acepte el contrato de licencia del usuario final y que cambie la contraseña de administrador.

Paso 4 Utilice el asistente de configuración cuando inicie sesión por primera vez en Administrador del dispositivo para completar la configuración inicial. De manera opcional, puede omitir el asistente de configuración haciendo clic en **Omitir configuración del dispositivo** al final de la página.

Después de completar el asistente de configuración, además de la configuración predeterminada de la interfaz interna (Ethernet1/2 a 1/8, que son puertos de switch en la VLAN1), tendrá una configuración para una interfaz externa (Ethernet1/1) que se mantendrá cuando cambie a la administración del Centro de administración.

a) Configure las siguientes opciones para las interfaces externas y de administración y haga clic en **Siguiente**.

1. **Dirección de la interfaz externa**: esta interfaz suele ser la gateway de Internet y puede utilizarse como interfaz de acceso del administrador. No se puede seleccionar una interfaz externa alternativa durante la configuración inicial del dispositivo. La primera interfaz de datos es la interfaz externa predeterminada.

   Si desea utilizar una interfaz diferente de la externa (o interna) para el acceso al administrador, tendrá que configurarla manualmente después de completar el asistente de configuración.

   Configure IPv4: la dirección IPv4 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, una máscara de subred y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv4. No puede configurar PPPoE con el asistente de configuración. PPPoE puede ser necesario si la interfaz está conectada a un módem DSL, a un módem por cable o a otra conexión con su ISP, y su ISP utiliza PPPoE para proporcionar su dirección IP. Puede configurar PPPoE después de completar el asistente.

   Configure IPv6: la dirección IPv6 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, un prefijo y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv6.

2. **Interfaz de administración**

   No verá la configuración de la interfaz de administración si ha realizado la configuración inicial desde la CLI.

   Los ajustes de la interfaz de administración se utilizan aunque active el acceso al administrador en una interfaz de datos. Por ejemplo, el tráfico de administración que se enruta por la placa base a través de la interfaz de datos resolverá los FQDN utilizando los servidores DNS de la interfaz de administración y no los servidores DNS de la interfaz de datos.

   Servidores DNS: el servidor DNS para la dirección de administración del sistema. Introduzca una o varias direcciones de servidores DNS para la resolución de nombres. El valor predeterminado son los

servidores DNS públicos de OpenDNS. Si edita los campos y quiere volver a los predeterminados, haga clic en **Usar OpenDNS** para volver a cargar las direcciones IP adecuadas en los campos.

Nombre de host del firewall: el nombre de host para la dirección de administración del sistema.

b) Configure los **Ajustes de la hora (NTP)** y haga clic en **Siguiente**.

1. **Zona horaria**: seleccione la zona horaria del sistema.
2. **Servidor de hora NTP**: seleccione si desea utilizar los servidores NTP predeterminados o introducir manualmente las direcciones de sus servidores NTP. Puede agregar varios servidores para proporcionar copias de seguridad.

c) Seleccione **Iniciar periodo de evaluación de 90 días sin registro**.

No registre la Protección frente a amenazas con Smart Software Manager; todas las licencias se realizan en el Centro de administración.

d) Haga clic en **Finalizar**.

e) Se le solicitará que elija **Administración en la nube** o **Independiente**. Para la administración del Centro de administración, seleccione **Independiente** y, a continuación, **Lo tengo**.

Paso 5 (Puede que sea necesario) Configure la interfaz de administración. Consulte la interfaz de administración en **Dispositivo** > **Interfaces**.

La interfaz de administración debe tener la gateway configurada para interfaces de datos. Por defecto, la interfaz de administración recibe una dirección IP y una gateway desde el DHCP. Si no recibe una gateway desde el DHCP (por ejemplo, no conecta esta interfaz a una red), entonces la gateway se conectará por defecto a las interfaces de datos, y no necesitará configurar nada. Si ha recibido una gateway desde DHCP, en su lugar necesita configurar esta interfaz con una dirección IP estática y ajustar la gateway a las interfaces de datos.

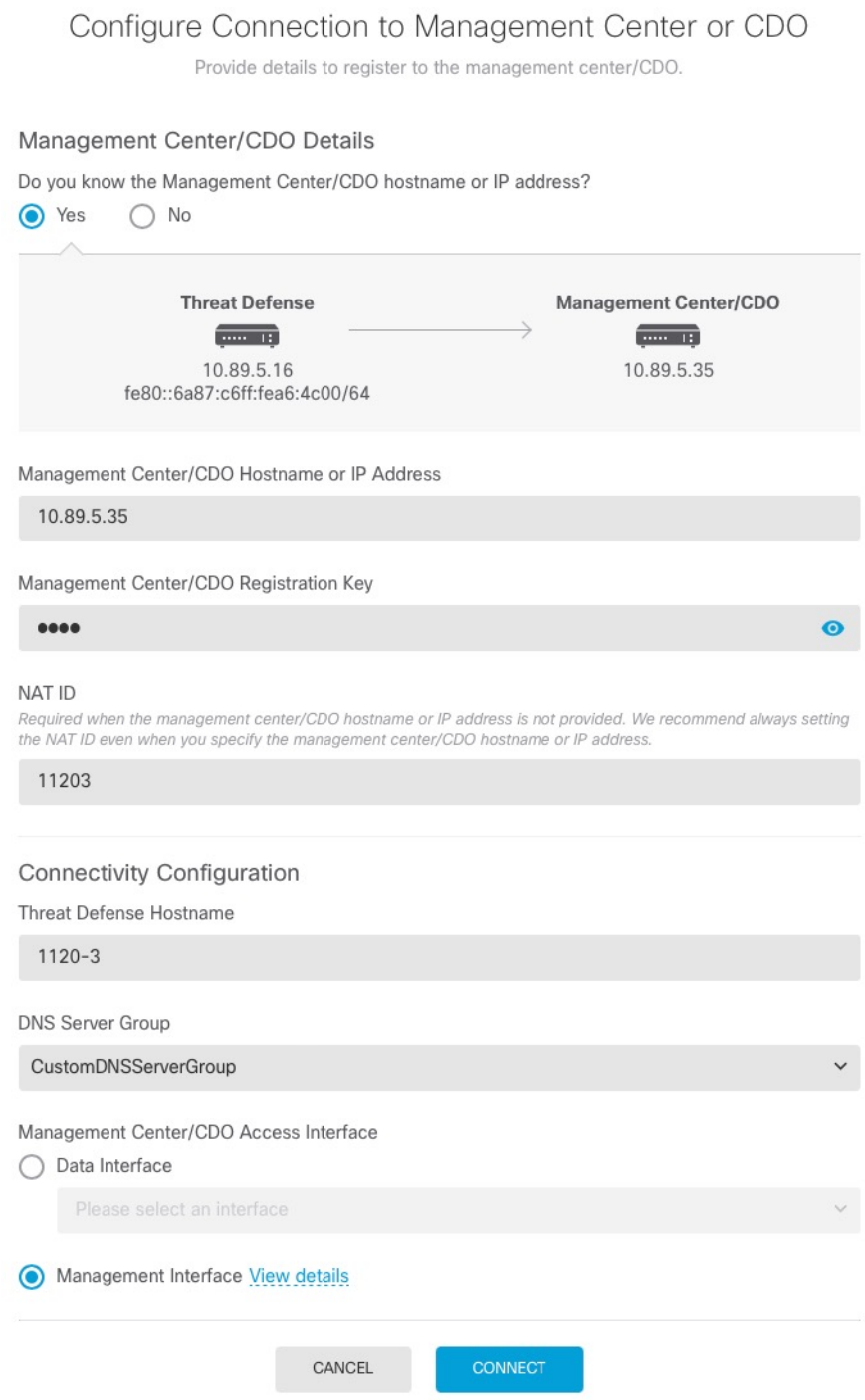
Paso 6 Si desea configurar interfaces adicionales, incluida una interfaz distinta de la externa o la interna que desee utilizar para el acceso al administrador, seleccione **Dispositivo** y, a continuación, haga clic en el enlace del resumen de **Interfaces**.

Consulte Configurar el firewall en Administrador del dispositivo, en la página 110 para obtener más información sobre la configuración de interfaces en Administrador del dispositivo. No se conservará otra configuración de Administrador del dispositivo cuando registre el dispositivo en el Centro de administración.

Paso 7 Seleccione **Dispositivo** > **Configuración del sistema** > **Administración central**, y haga clic en **Proceder** para configurar la administración del Centro de administración.

Paso 8 Configure los **Detalles del centro de administración/CDO**.

Figura 16: Detalles del centro de administración/CDO



a) Para las preguntas **¿Conoce el nombre de host o la dirección IP del Centro de gestión/CDO?**, haga clic en **Sí** si puede acceder al Centro de administración mediante una dirección IP o un nombre de host, o **No** si el Centro de administración está detrás de la NAT o no tiene una dirección IP pública o un nombre de host.

Al menos uno de los dispositivos, ya sea el Centro de administración o la Protección frente a amenazas, debe tener una dirección IP accesible para establecer el canal de comunicación bidireccional con cifrado SSL entre los dos dispositivos.

b) Si responde **Sí**, introduzca la **dirección IP o el nombre de host del centro de administración/CDO**.

c) Especifique la **Clave de registro del centro de administración/CDO** .

Es una clave de registro de un solo uso a su elección que también especificará en el Centro de administración cuando registre el dispositivo Protección frente a amenazas. La clave de registro no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-). Esta ID se puede utilizar para el registro de múltiples dispositivos en el Centro de administración.

d) Especifique una **ID de NAT**.

Esta ID es un string único de un solo uso a su elección que también especificará en el Centro de administración. Este campo es necesario si solo especifica la dirección IP en uno de los dispositivos; pero le recomendamos que especifique la ID de NAT incluso si conoce la dirección IP de ambos dispositivos. El ID de la NAT no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-). Esta ID *no* se puede utilizar para el registro de ningún otro dispositivo en el Centro de administración. La ID de NAT se utiliza en combinación con la dirección IP para verificar que la conexión proviene del dispositivo correcto; solo después de la autenticación de la dirección IP / ID de NAT se comprobará la clave de registro.

Paso 9 Configure la **Configuración de conectividad**.

a) Especifique el **Nombre de host del FTD**.

Este FQDN se utilizará para la interfaz exterior, o cualquier interfaz que seleccione como **Interfaz de acceso al centro de administración/CDO**.

b) Especifique el **Grupo de servidores DNS**.

Elija un grupo existente o cree uno nuevo. El grupo de DNS predeterminado se llama **CiscoUmbrellaDNSServerGroup** e incluye los servidores OpenDNS.

Estos ajustes establecen el servidor DNS de la interfaz de *datos*. El servidor DNS de administración que estableció con el asistente de configuración se utiliza para el tráfico de administración. El servidor DNS de datos se utiliza para DDNS (si está configurado) o para las políticas de seguridad que se aplican a esta interfaz. Es probable que seleccione el mismo grupo de servidor DNS que utilizó para la administración, porque tanto la administración como el tráfico de administración y de datos acceden al servidor DNS a través de la interfaz externa.

En el Centro de administración, los servidores DNS de la interfaz de datos están configurados en la política de configuración de la plataforma que ha asignado a este Protección frente a amenazas. Cuando agrega el Protección frente a amenazas al Centro de administración, se mantiene la configuración local, y los servidores DNS *no* se agregan a una política de configuración de la plataforma. Sin embargo, si después asigna una política de configuración de plataforma al Protección frente a amenazas que incluye una configuración de DNS, esa configuración sobrescribirá la local. Recomendamos que configure de forma activa la configuración de la plataforma DNS para que coincida con esta configuración y sincronizar el Centro de administración y el Protección frente a amenazas.

Además, el Centro de administración solo mantiene los servidores DNS locales solo se conservan si se detectaron en el registro inicial.

c) Para la **Interfaz de acceso al centro de administración/CDO**, seleccione **externa**.

Puede elegir cualquier interfaz configurada, pero esta guía asume que está utilizando una externa.

Paso 10 Si elige una interfaz de datos distinta a la externa, agregue una ruta predeterminada.

Verá un mensaje en el que se le indicará que compruebe si tiene una ruta predeterminada a lo largo de la interfaz. Si ha seleccionado externa, ya ha configurado esta ruta dentro del asistente de configuración. Si selecciona una interfaz diferente, necesita configurar de forma manual una ruta predeterminada antes de conectarse al Centro de administración. Consulte Configurar el firewall en Administrador del dispositivo, en la página 110 para obtener más información acerca de las rutas estáticas en Administrador del dispositivo.

Paso 11 Haga clic en **Añadir un método DNS dinámico (DDNS)**.

El DDNS garantiza que el Centro de administración pueda acceder a la Protección frente a amenazas con su nombre de dominio completo (FQDN) si cambia la dirección IP de Protección frente a amenazas. Para configurar el DDNS, consulte **Dispositivo** > **Configuración del sistema** > **Servidor DDNS**.

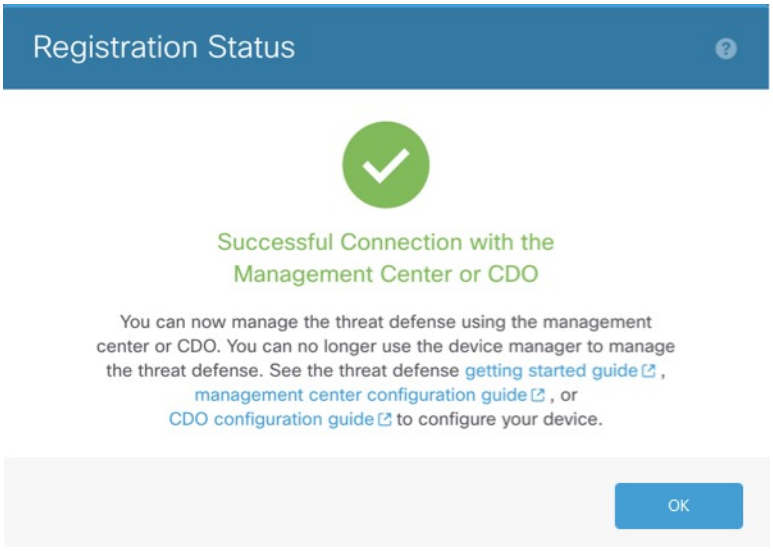
Si configura el DDNS antes de agregar la Protección frente a amenazas al Centro de administración, la Protección frente a amenazas agrega automáticamente certificaciones para todas las CA principales del paquete de CA raíz de confianza de Cisco para que la Protección frente a amenazas pueda validar la certificación del servidor DDNS para la conexión HTTPS. La Protección frente a amenazas es compatible con cualquier servidor DDNS que utilice la especificación de API remota DynDNS (https://help.dyn.com/remote-access-api/).

Paso 12 Haga clic en **Conectar**. El cuadro de diálogo del **Estado de registro** muestra el estado actual del cambio al Centro de administración. Después del paso de **Guardar la configuración de registro del centro de administración/CDO**, vaya al Centro de administración, y agregue el firewall.

Si desea cancelar el traspaso al Centro de administración, haga clic en **Cancelar registro**. De lo contrario, no cierre la ventana del navegador Administrador del dispositivo hasta que se haya completado el paso de **Guardar la configuración de registro del centro de administración/CDO**. Si lo hace, el proceso se detendrá y no continuará hasta que se vuelva a conectar a Administrador del dispositivo.

Si permanece conectado a Administrador del dispositivo tras el paso de **Guardar la configuración de registro del centro de administración/CDO**, en algún momento le aparecerá el cuadro de diálogo de **Se ha conectado correctamente al centro de administración/CDO**, tras el cual se le desconectará de Administrador del dispositivo.

Figura 17: Conexión correcta



Configuración previa con la CLI

Conéctese a la CLI de Protección frente a amenazas para llevar a cabo la configuración inicial. Cuando utiliza la CLI para la configuración inicial, solo se conservan los valores de configuración de la interfaz de acceso del administrador y de la interfaz de administración.Cuando lleva a cabo la configuración inicial con Administrador del dispositivo (versiones 7.1 o posteriores), *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se conserva al cambiar a Centro de administración para la gestión, además de la configuración de la interfaz de acceso del administrador y la interfaz de administración. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso.

Antes de empezar

Implemente y lleve a cabo la configuración inicial del Centro de administración. Consulte la Guía de instalación del hardware de Cisco Firepower Management Center 1600, 2600 y 4600. Necesitará conocer la dirección IP o el nombre de host del Centro de administración antes de configurar el Protección frente a amenazas.

Procedimiento

Paso 1 Encienda el firewall.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Paso 2 Conéctese a la CLI de Protección frente a amenazas en el puerto de consola.

El puerto de consola se conecta a la CLI de FXOS.

Paso 3 Inicie sesión con el nombre de usuario **admin** y la contraseña **Admin123**.

La primera vez que inicie sesión en FXOS, se le pedirá que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si la contraseña ya se ha cambiado y no sabe cuál es, debe volver restablecer la imagen en el dispositivo para volver a configurar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el procedimiento de restablecer la imagen.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 4 Conéctese a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Paso 5 La primera vez que inicie sesión en Protección frente a amenazas, se le solicitará que acepte el contrato de licencia del usuario final (EULA) y, si utiliza una conexión SSH, que cambie la contraseña del administrador. A continuación, se le presenta el script de configuración de la CLI para los ajustes de la interfaz de administración.

Los ajustes de la interfaz de administración se utilizan aunque active el acceso del administrador en una interfaz de datos.

Nota No puede volver a abrir el asistente de configuración de la CLI a menos que borre la configuración; por ejemplo, al restablecer la imagen. Sin embargo, todos estos ajustes pueden cambiarse más tarde en la CLI mediante los comandos de **configuración de red**. Consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Los valores predeterminados o los introducidos anteriormente aparecen entre paréntesis. Para aceptar los valores introducidos anteriormente, pulse **Intro**.

Consulte las siguientes directrices:

- **¿Configurar IPv4 a través de DHCP o de forma manual?** Elija **Manual**. Aunque no tenga previsto utilizar la interfaz de gestión, debe establecer una dirección IP, por ejemplo, una dirección privada. No puede configurar una interfaz de datos para la administración si la interfaz de gestión está establecida en DHCP, ya que la ruta predeterminada, que debe ser **interfaces de datos** (consulte la siguiente viñeta), puede sobrescribirse por otra recibida del servidor DHCP.
- **Introduzca la gateway predeterminada IPv4 para la interfaz de gestión**: configure la gateway como **interfaz de datos**. Esta configuración reenvía el tráfico de gestión a través de la placa base para que se pueda enrutar a través de la interfaz de datos de acceso del administrador.
- **Si la información de la red ha cambiado, tendrá que volver a conectarse**. Si está conectado con SSH, se desconectará. Puede volver a conectarse con la nueva dirección IP y contraseña si su equipo de administración está en la red de administración. No podrá volver a conectarse desde una red remota debido al cambio de ruta predeterminado (a través de las interfaces de datos). Las conexiones de la consola no se ven afectadas.
- **¿Administrar el dispositivo de forma local?** Introduzca **No** para utilizar Centro de administración. Si responde **Sí** significa que utilizará Administrador del dispositivo en su lugar.
- **¿Configurar el modo de firewall?** Introduzca **enrutado**. El acceso al administrador externo solo es compatible en el modo de firewall enrutado.

Ejemplo:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:
```

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Paso 6 Configure la interfaz externa para el acceso al administrador.

configure network management-data-interface

A continuación, se le pedirá que configure los ajustes de red básicos para la interfaz externa. Consulte la siguiente información para utilizar este comando:

- La interfaz de gestión no puede utilizar DHCP si desea utilizar una interfaz de datos para la gestión. Si no configuró la dirección IP de forma manual durante la configuración inicial, puede hacerlo ahora con el comando **configure network** {**ipv4** | **ipv6**} **manual**. Si aún no ha establecido el gateway de la interfaz de administración en **interfaces de datos**, este comando lo establecerá ahora.
- Cuando agrega la Protección frente a amenazas al Centro de administración, el Centro de administración detecta y mantiene la configuración de la interfaz, incluida la siguiente configuración: nombre de interfaz

y dirección IP, ruta estática al gateway, servidores DNS y servidor DDNS. Para obtener más información sobre la configuración del servidor DNS, consulte la información más abajo. En el Centro de administración, puede cambiar más tarde la configuración de la interfaz de acceso del administrador, pero no realice cambios que puedan impedir que la Protección frente a amenazas o el Centro de administración restablezcan la conexión de administración. Si la conexión de administración se interrumpe, la Protección frente a amenazas incluye el comando **configure policy rollback** para restaurar la implementación anterior.

- Si configura una URL para la actualización del servidor DDNS, la Protección frente a amenazas agrega automáticamente certificados para todas las CA principales del paquete de CA raíz de confianza de Cisco para que la Protección frente a amenazas pueda validar el certificado del servidor DDNS para la conexión HTTPS. El Protección frente a amenazas es compatible con cualquier servidor DDNS que utilice la especificación de API remota DynDNS (https://help.dyn.com/remote-access-api/).
- Este comando establece el servidor DNS de la interfaz de *datos*. El servidor DNS de administración que estableció con el script de configuración (o mediante el comando **configure network dns servers**) se utiliza para el tráfico de gestión. El servidor DNS de datos se utiliza para DDNS (si está configurado) o para las políticas de seguridad que se aplican a esta interfaz.

  En el Centro de administración, los servidores DNS de la interfaz de datos están configurados en la política de configuración de la plataforma que ha asignado a esta Protección frente a amenazas. Cuando agrega el Protección frente a amenazas al Centro de administración, se mantiene la configuración local, y los servidores DNS *no* se agregan a una política de configuración de la plataforma. Sin embargo, si después asigna una política de configuración de plataforma a la Protección frente a amenazas que incluye una configuración de DNS, esa configuración sobrescribirá la local. Recomendamos que configure de forma activa la configuración de la plataforma DNS para que coincida con esta configuración y sincronizar el Centro de administración y la Protección frente a amenazas.

  Además, el Centro de administración solo mantiene los servidores DNS locales solo se conservan si se detectaron en el registro inicial. Por ejemplo, si ha registrado el dispositivo mediante la interfaz de administración pero luego configura una interfaz de datos con el comando **configure network management-data-interface**, debe configurar todos estos ajustes en el Centro de administración de forma manual, incluidos los servidores DNS, para que coincidan con la configuración de la Protección frente a amenazas.
- Puede cambiar la interfaz de administración después de registrar la Protección frente a amenazas en el Centro de administración, ya sea en la interfaz de administración o en otra interfaz de datos.
- El FQDN que estableció en el asistente de configuración se utilizará para esta interfaz.
- Puede borrar toda la configuración del dispositivo como parte del comando; esta opción se puede usar para la recuperación, pero no le recomendamos que la utilice para la configuración inicial o el funcionamiento normal.
- Para desactivar la administración de datos, introduzca el comando **configure network management-data-interface disable**.

Ejemplo:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Ejemplo:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Paso 7 (Opcional) Limite el acceso a la interfaz de datos al Centro de administración en una red específica.

configure network management-data-interface client *dirección_ip máscara de red*

De forma predeterminada, se permiten todas las redes.

Paso 8 Identifique el Centro de administración que administrará este Protección frente a amenazas.

configure manager add {*nombre de host* | *dirección_IPv4* | *dirección_IPv6* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*nombre de host* | *dirección_IPv4* | *dirección_IPv6* | **DONTRESOLVE**}: especifica la FQDN o la dirección IP del Centro de administración. Si no Centro de administración es directamente direccionable, utilice **DONTRESOLVE**. Al menos uno de los dispositivos, ya sea el Centro de administración o el Protección frente a amenazas, debe tener una dirección IP accesible para establecer el canal de comunicación bidireccional con cifrado SSL entre los dos dispositivos. Si especifica **DONTRESOLVE** en este comando, el Protección frente a amenazas debe tener una dirección IP o nombre de host accesible.
- *reg_key*: especifica la clave de registro de un solo uso de su elección que también especificará en el Centro de administración cuando registre el Protección frente a amenazas. La clave de registro no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z, a–z, 0–9) y el guion (-).
- *nat_id*: especifica una cadena única y para solo una vez de su elección que también especificará en el Centro de administración. Cuando utilice una interfaz de datos para la gestión, debe especificar el ID de la NAT en *el Protección frente a amenazas y el Centro de administración* para el registro. El ID de la NAT no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A–Z,

a–z, 0–9) y el guion (-). Este ID no se puede utilizar para ningún otro dispositivo que se registre en el Centro de administración.

Ejemplo:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Paso 9 Apague el Protección frente a amenazas para poder enviar el dispositivo a la sucursal remota.

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación o pulsa el interruptor de alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su sistema.

a) Introduzca el comando **shutdown**.
b) Observe el LED de alimentación y el LED de estado para comprobar que el chasis está apagado (no están encendidos).
c) Después de que el chasis se haya apagado correctamente, puede desconectar la alimentación para desconectar físicamente la alimentación del chasis si es necesario.

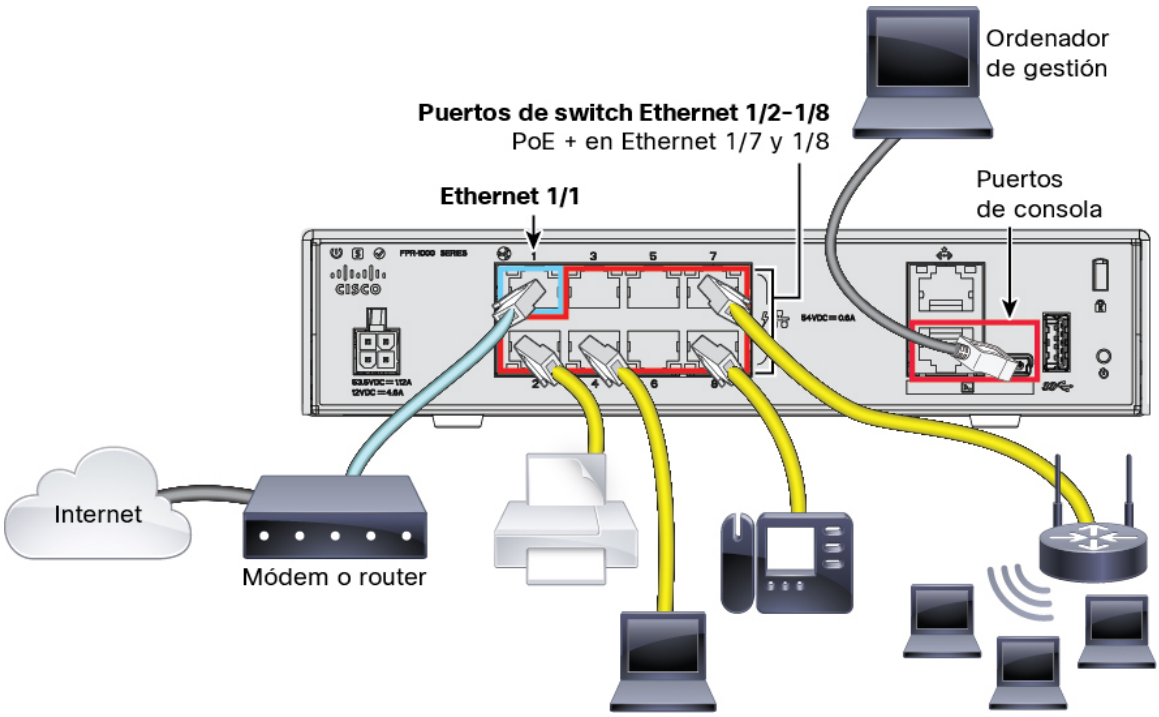
Instalación de sucursales

Después de que reciba el Protección frente a amenazas de la sede central, solo tiene que cablear y encender el firewall para que tenga acceso a Internet desde la interfaz externa. El administrador central puede completar la configuración.

Cablear el firewall

El Centro de administración y su ordenador de gestión residen en una sede remota y pueden acceder al Protección frente a amenazas a través de Internet. Para cablear el Firepower 1010, consulte los siguientes pasos.

Figura 18: Cableado de una implementación de gestión remota



Procedimiento

Paso 1 Instale el chasis. Consulte la guía de instalación del hardware.

Paso 2 Conecte la interfaz externa (Ethernet 1/1) al router externo.

Paso 3 Cablee los puntos finales internos a los puertos de switch, Ethernet1/2 a 1/8.

Paso 4 (Opcional) Conecte el ordenador de gestión al puerto de consola.

En la sucursal, no es necesaria la conexión de la consola para el uso diario; sin embargo, puede ser necesario para la resolución de problemas.

Encender el dispositivo

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Antes de empezar

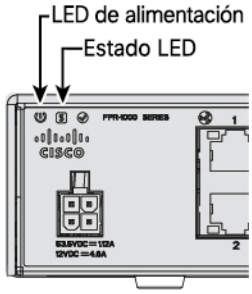
Es importante que proporcione una alimentación fiable para su dispositivo (con una fuente de alimentación ininterrumpida (UPS), por ejemplo). Si se pierde la fuente de alimentación sin apagar primero se pueden provocar daños graves en el sistema de archivos. Hay muchos procesos que se ejecutan en segundo plano todo el tiempo y, si se pierde la fuente de alimentación, el sistema no se puede apagar adecuadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

Configuración posterior del administrador central

Después de que el administrador de la sucursal en remoto conecte por cable el Protección frente a amenazas para que tenga acceso a Internet desde la interfaz externa, puede registrar el Protección frente a amenazas en el Centro de administración y completar la configuración del dispositivo.

Iniciar sesión en el Centro de administración

Utilice el Centro de administración para configurar y controlar la Protección frente a amenazas.

Antes de empezar

Para obtener información sobre los navegadores compatibles, consulte las notas de la versión que esté utilizando (consulte https://www.cisco.com/go/firepower-notes).

Procedimiento

Paso 1 Con un navegador compatible, introduzca la siguiente URL.

https://*fmc_ip_address*

Paso 2 Introduzca su nombre de usuario y contraseña.

Paso 3 Haga clic en **Iniciar sesión**.

Obtener licencias para el Centro de administración

Protección frente a amenazas proporciona todas las licencias para Centro de administración. Puede adquirir de forma opcional las siguientes licencias de funciones:

- **Amenazas**: inteligencia de seguridad e IPS de última generación
- **Malware**: protección frente al malware
- **URL**: filtrado de URL
- **VPN con RA**: AnyConnect Plus, AnyConnect Apex o AnyConnect solo VPN

Para obtener una descripción general más detallada sobre Cisco Licensing, visite cisco.com/go/licensingguide

Antes de empezar

- Tener una cuenta principal en Smart Software Manager.

  Si aún no tiene una cuenta, haga clic en el enlace para configurar una nueva cuenta. Smart Software Manager le permite crear una cuenta principal para su organización.

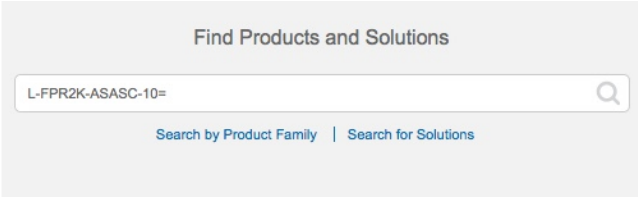
- Su cuenta de licencias de Smart Software debe cumplir los requisitos de la licencia de cifrado seguro (3DES/AES) para utilizar algunas funciones (que se activan mediante el indicador de cumplimiento de exportación).

Procedimiento

Paso 1 Compruebe que su cuenta de licencias Smart contenga las licencias disponibles que necesita.

Cuando adquirió su dispositivo en Cisco o en un distribuidor, sus licencias deberían haberse vinculado a su cuenta de licencias Smart Software. Sin embargo, si necesita agregar licencias usted mismo, utilice el campo de búsqueda **Buscar productos y soluciones** en Cisco Commerce Workspace. Busque las siguientes PID de licencia:

Figura 19: Búsqueda de licencia



Nota Si no se encuentra una PID, puede agregarla manualmente a su pedido.

- Combinación de licencias de amenazas, malware y URL:

- L-FPR1010T-TMC=

Cuando agregue una de las PID anteriores a su pedido, podrá elegir una suscripción basada en el plazo correspondiente a una de las siguientes PID:

- L-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

- VPN con RA: consulte la Guía de pedidos de Cisco AnyConnect.

Paso 2 Si aún no lo ha hecho, registre Centro de administración con Smart Software Manager.

Para registrarse, es necesario que genere un token de registro en Smart Software Manager. Consulte la Centro de administración guía de configuración para obtener instrucciones detalladas. Para el aprovisionamiento sin apenas intervención, debe activar **la asistencia en la nube para el aprovisionamiento sin apenas intervención** cuando se registre con Smart Software Manager o después. Consulte la página **Sistema** > **Licencias** > **Licencias Smart**.

Registrar la Protección frente a amenazas con el Centro de administración

Registre la Protección frente a amenazas en el Centro de administración.

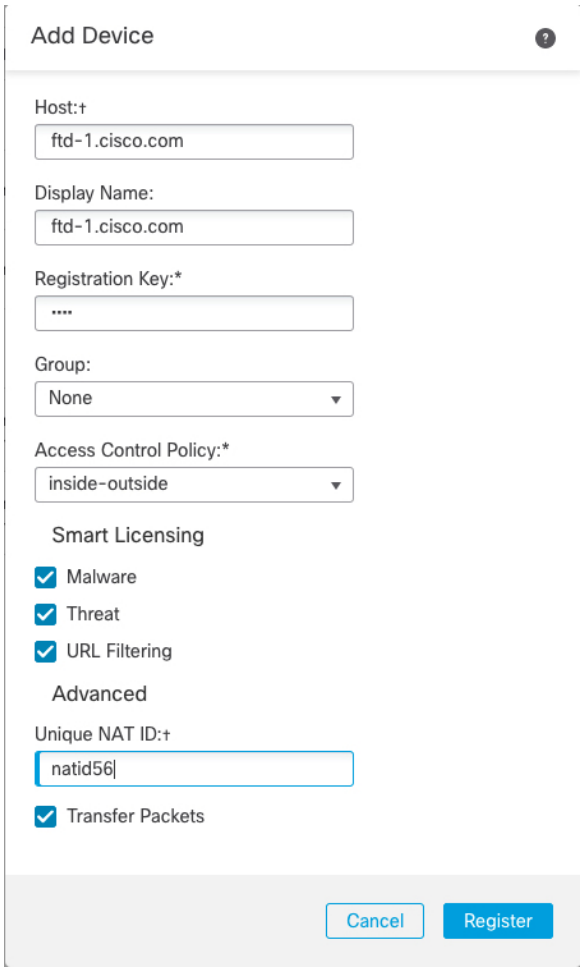
Antes de empezar

- Recopile la siguiente información que estableció en la configuración inicial de Protección frente a amenazas:
  - La dirección IP o nombre de host de la Protección frente a amenazas, y la ID de NAT
  - La clave de registro del Centro de administración

Procedimiento

Paso 1 En el Centro de administración, seleccione **Dispositivos** > **Administración de dispositivos**.

Paso 2 En la lista desplegable **Agregar**, seleccione **Agregar dispositivo**.



Establezca los siguientes parámetros:

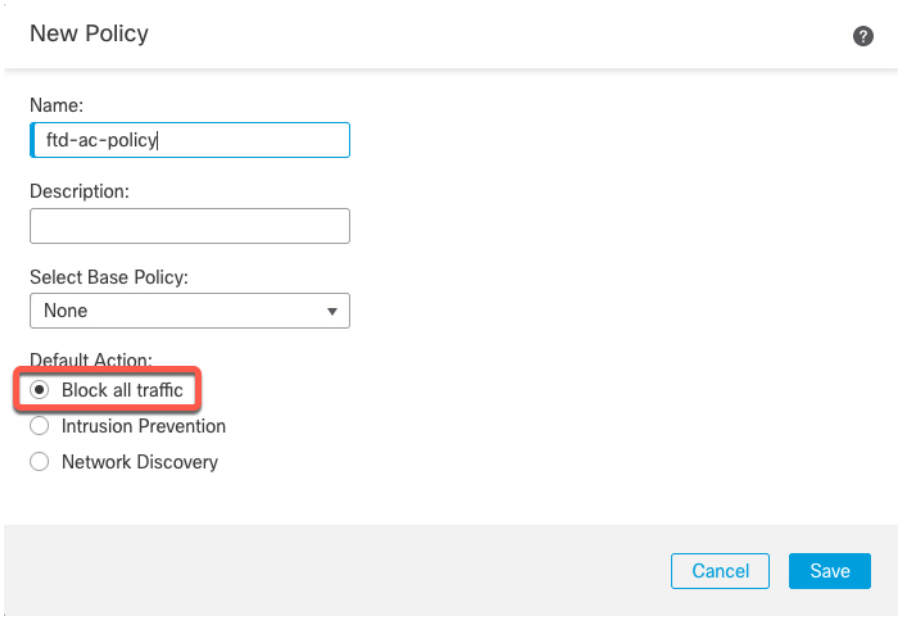
- **Host**: introduzca la dirección IP o el nombre del host de Protección frente a amenazas que desee agregar. Puede dejar este campo en blanco si ha especificado tanto la dirección IP y una ID de NAT del Centro de administración en la configuración inicial de la Protección frente a amenazas.

  Nota En un entorno de alta disponibilidad, cuando, los Centros de administración están detrás de una NAT, puede registrar la Protección frente a amenazas sin una IP o nombre de host en el Centro de administración principal. Sin embargo, para registrar la Protección frente a amenazas en un Centro de administración secundario, debe proporcionar una dirección IP o nombre de host para la Protección frente a amenazas.

- **Nombre de visualización**: introduzca el nombre de la Protección frente a amenazas que desee que aparezca en el Centro de administración.
- **Clave de registro**: introduzca la misma clave de registro que especificó en la configuración de inicial de Protección frente a amenazas.
- **Dominio**: asigne el dispositivo a un dominio inferior si tiene un entorno con varios dominios.
- **Grupo**: asígnelo a un grupo de dispositivos si utiliza grupos.

- **Política de control de acceso**: seleccione una política inicial. A menos que ya cuente con una política personalizada que sepa que debe utilizar, seleccione **Crear nueva política** y **Bloquear todo el tráfico**. Puede cambiar esto más tarde para permitir el tráfico; ver Permitir el tráfico de dentro hacia afuera, en la página 41.

Figura 20: Nueva política



- **Licencias Smart**: asigne las licencias Smart que necesite para las funciones que desea implementar: **malware** (si desea utilizar la inspección de malware), **amenazas** (si pretende utilizar la prevención de intrusiones) y **URL** (si quiere implementar el filtrado de URL basado en categorías). **Nota:** Puede aplicar una licencia VPN de acceso remoto Client Secure tras agregar el usuario, desde la página de **Sistema** > **Licencias** > **Licencias Smart**.
- **ID de NAT única**: especifique la ID de NAT que especificó durante la configuración de inicial de Protección frente a amenazas.
- **Transferir paquetes**: permite que el dispositivo transfiera paquetes a Centro de administración. Si se desencadenan eventos como IPS o Snort con esta opción activada, el dispositivo envía información de metadatos de los eventos y datos sobre el paquete al Centro de administración para su inspección. Si la desactiva, solo se enviará la información del evento al Centro de administración, pero no se enviarán los datos del paquete.

Paso 3 Haga clic en **Registrar** y confirme que el registro se ha realizado correctamente.

Si se ha completado, el dispositivo se agrega a la lista. Si ha ocurrido un error, verá un mensaje. Si no puede registrar el Protección frente a amenazas, compruebe los siguientes elementos:

- Ping: acceda a la CLI de Protección frente a amenazas y haga ping a la dirección IP de Centro de administración con el siguiente comando:

  ping system *dirección_ip*

  Si el ping no se realiza correctamente, compruebe la configuración de red con el comando **show network**. Si necesita cambiar la dirección IP de administración de Protección frente a amenazas, utilice el comando **configure network management-data-interface**.

- Clave de registro, ID de NAT y dirección IP Centro de administración: compruebe que está utilizando la misma clave de registro y, si se utiliza, el ID de NAT en ambos dispositivos. Puede establecer la clave de registro y el ID de NAT en Protección frente a amenazas mediante el comando **configure manager add**.

Para obtener más información sobre la resolución de problemas, consulte https://cisco.com/go/fmc-reg-error.

Configurar una norma de seguridad básica

Esta sección describe cómo configurar una política de seguridad básica con la siguiente configuración:

- Interfaces interna y externa: asigne una dirección IP estática a la interfaz interna. Ha configurado los ajustes básicos para la interfaz externa como parte de la configuración de acceso del administrador, pero todavía necesita asignarla a una zona de seguridad.
- Servidor DHCP: utilice un servidor DHCP en la interfaz interna para los clientes.
- NAT: utilice la interfaz PAT en la interfaz externa.
- Control de acceso: permita el tráfico desde dentro hacia fuera.
- SSH: active SSH en la interfaz de acceso del administrador.

Configurar interfaces

Agregue la interfaz VLAN1 para los puertos de switch o convierta los puertos de switch en interfaces de firewall, asigne interfaces a las zonas de seguridad y configure las direcciones IP. Normalmente, deberá configurar al menos un mínimo de dos interfaces para tener un sistema que pase tráfico significativo. Normalmente, tendrá una interfaz externa que da al router ascendente o a Internet, y una o más interfaces internas para las redes de su organización. De forma predeterminada, Ethernet1/1 es una interfaz de firewall normal que puede utilizar como externa y las interfaces restantes son puertos de switch en la VLAN1; después de agregar la interfaz VLAN1, puede convertirla en su interfaz interna. También puede asignar puertos de switch a otras VLAN o convertir puertos de switch a interfaces de firewall.

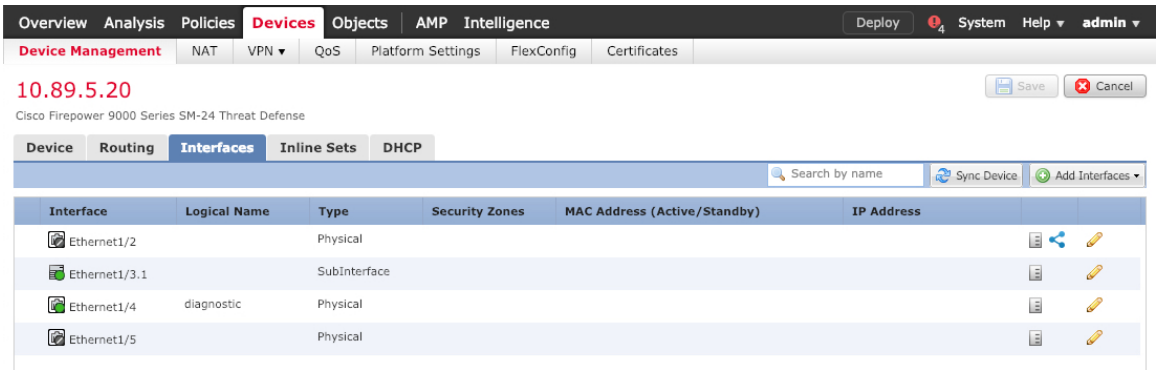
Una situación típica de enrutamiento de borde es obtener la dirección de la interfaz externa a través de DHCP de su ISP, mientras que usted define direcciones estáticas en las interfaces internas.

El siguiente ejemplo configura una interfaz interna de modo enrutado (VLAN1) con una dirección estática y una interfaz externa de modo enrutado mediante DHCP (Ethernet1/1).

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en el **Editar** ( ) del dispositivo.

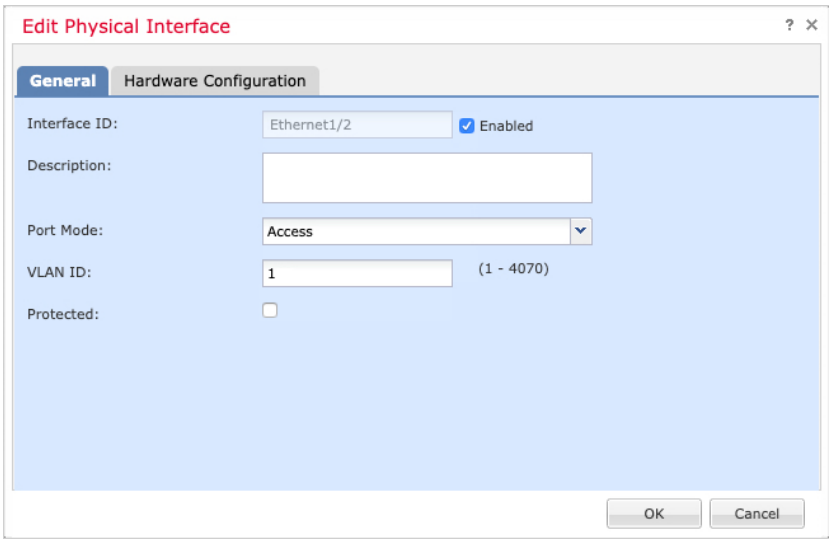
Paso 2 Haga clic en **Interfaces**.



Paso 3 (Opcional) Desactive el modo de puerto de switch para cualquiera de los puertos de switch (Ethernet1/2 a 1/8) haciendo clic en el deslizador de la columna **SwitchPort** para que se muestre como desactivado ( ).

Paso 4 Active los puertos del switch.

a) Haga clic en **Editar** ( ) para el puerto del switch.



b) Active la interfaz marcando la casilla de verificación **Activar**.

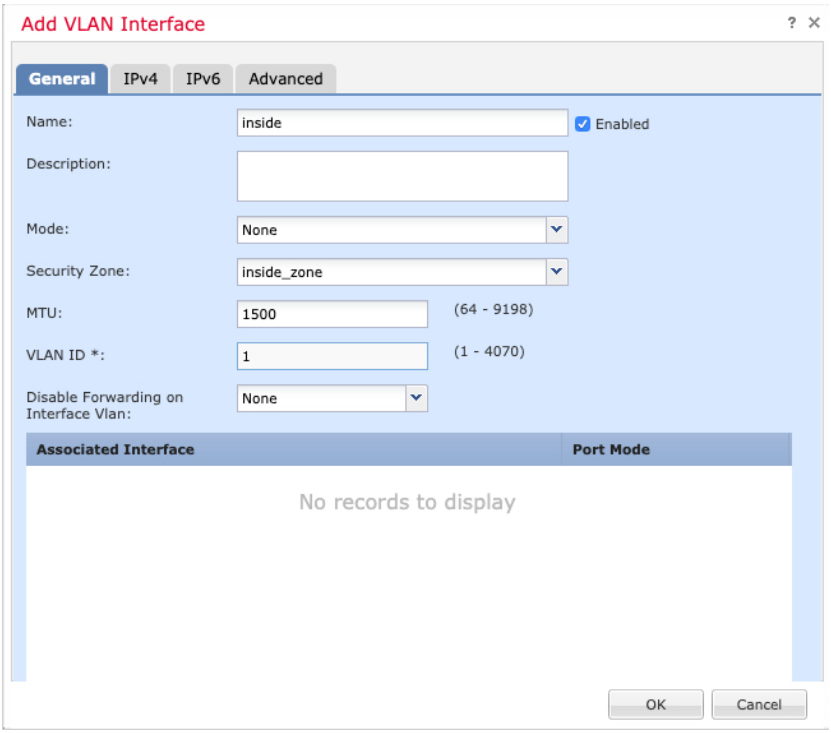
c) (Opcional) Cambie la ID de VLAN; el valor predeterminado es 1. A continuación, agregará una interfaz VLAN para que coincida con esta ID.

d) Haga clic en **Aceptar**.

Paso 5 Agregue la interfaz VLAN *interna*.

a) Haga clic en **Agregar interfaz** > **Interfaz VLAN**.

Aparece la pestaña **General**



b) Introduzca un **nombre** de hasta 48 caracteres de longitud.

Por ejemplo, asigne un nombre a la interfaz: **interna**.

c) Active la casilla **Activado**.

d) Deje el **modo** establecido en **Ninguno**.

e) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad interna existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, agregue una zona llamada **inside_zone**. Cada interfaz debe asignarse a una zona de seguridad o a un grupo de interfaces. Una interfaz solo puede pertenecer a una zona de seguridad, pero también puede pertenecer a varios grupos de interfaces. Aplicará su norma de seguridad en función de las zonas o los grupos. Por ejemplo, puede asignar la interfaz interna a la zona interna; y la interfaz externa a la zona externa. A continuación, puede configurar su política de control de acceso para permitir que el tráfico pase de dentro hacia fuera, pero no de fuera hacia dentro. La mayoría de las políticas solo admiten zonas de seguridad; puede utilizar zonas o grupos de interfaz en políticas NAT, políticas de prefiltro y políticas de QoS.

f) Establezca la **ID de VLAN** en **1**.

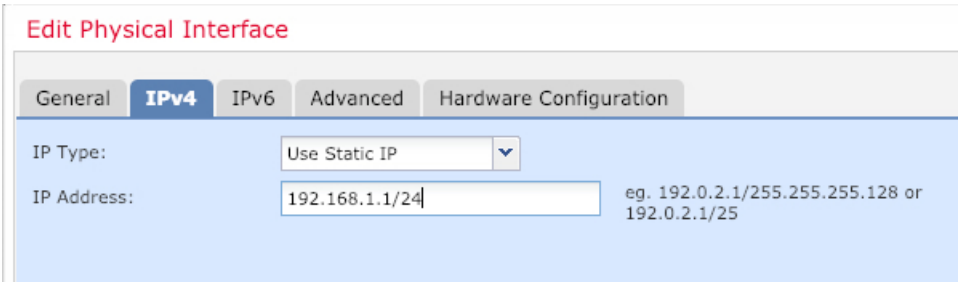
De forma predeterminada, todos los puertos de switch están configurados en VLAN1; si elige una ID de VLAN diferente aquí, también debe editar cada puerto de switch para que se encuentre en la nueva ID de VLAN.

No puede cambiar la ID de VLAN después de guardar la interfaz; la ID de VLAN es la etiqueta de VLAN utilizada y la ID de interfaz de su configuración.

g) Haga clic en la pestaña **IPv4** o **IPv6**.

- **IPv4**: elija **Usar IP estática** en la lista desplegable e introduzca una dirección IP y una máscara de subred en notación con barra.

Por ejemplo, introduzca **192.168.1.1/24**

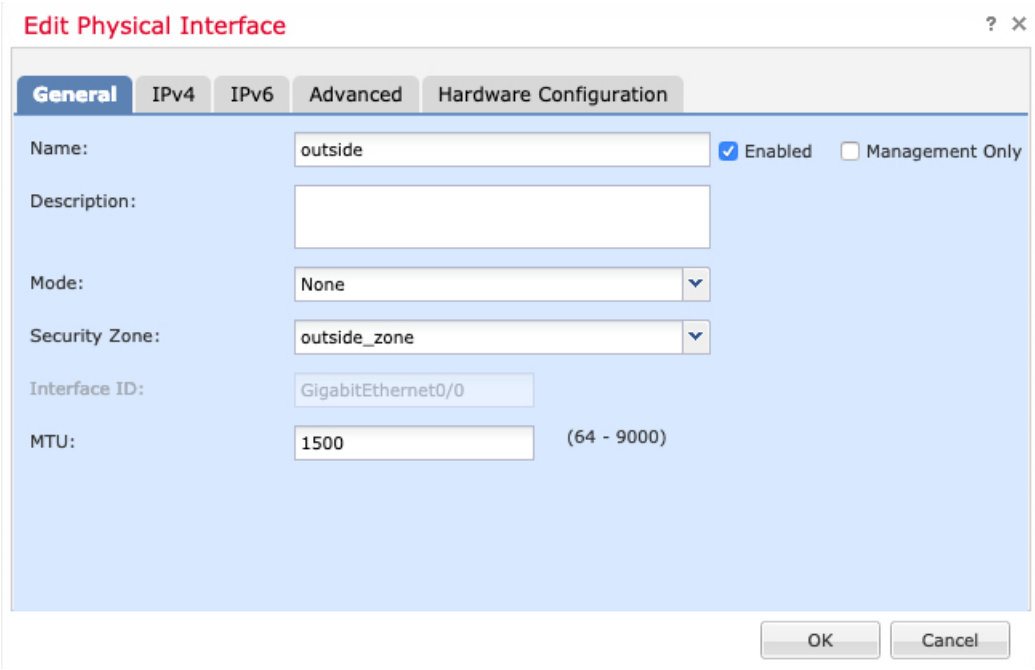


- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

h) Haga clic en **Aceptar**.

Paso 6 Haga clic en **Editar** (✎) para el Ethernet1/1 que quiera utilizar para la *externa*.

Aparece la pestaña **General**.



Ya ha configurado esta interfaz para el acceso al administrador, por lo que ya estará nombrada, activada y direccionada. No debe modificar ninguno de estas configuraciones básicas porque interrumpiría la conexión de gestión de Centro de administración. Todavía debe configurar las zona de seguridad en esta pantalla para las políticas de tráfico de paso.

a) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad externa existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, añada una zona llamada **outside_zone**.

b) Haga clic en **Aceptar**.

Paso 7 Haga clic en **Guardar**.

Configurar el servidor DHCP

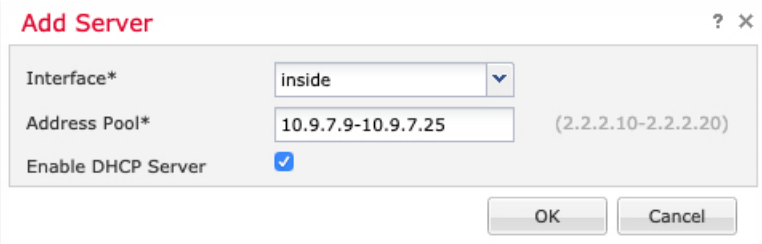
Active el servidor DHCP si desea que los clientes utilicen DHCP para obtener direcciones IP de Protección frente a amenazas.

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del dispositivo.

Paso 2 Seleccione **DHCP** > **Servidor DHCP**.

Paso 3 En la página **Servidor**, haga clic en **Agregar** y configure las siguientes opciones:



- **Interfaz**: elija la interfaz en la lista desplegable.
- **Conjunto de direcciones**: establezca el rango de direcciones IP de menor a mayor que utiliza el servidor DHCP. El rango de direcciones IP debe estar en la misma subred que la interfaz seleccionada y no puede incluir la dirección IP de la propia interfaz.
- **Habilitar servidor DHCP**: habilite el servidor DHCP en la interfaz seleccionada.

Paso 4 Haga clic en **Aceptar**.

Paso 5 Haga clic en **Guardar**.

Configurar NAT

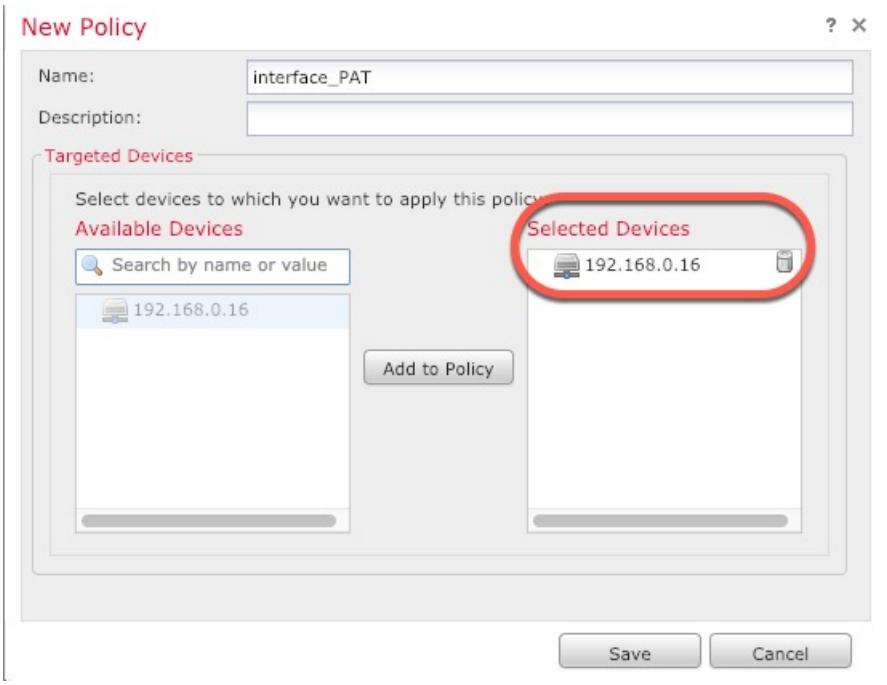
Configurar NAT

Una regla NAT típica convierte las direcciones internas a un puerto en la dirección IP de la interfaz externa. Este tipo de regla NAT se denomina *traducción de dirección del puerto de interfaz (PAT)*.

Procedimiento

Paso 1 Seleccione **Dispositivos** > **NAT**y haga clic en **Nueva política** > **NAT de Threat Defense**.

Paso 2 Asigne un nombre a la política, seleccione los dispositivos en los que la desea aplicar y haga clic en **Guardar**.



La política se agrega al Centro de administración. Aún tiene que añadir reglas a la política.

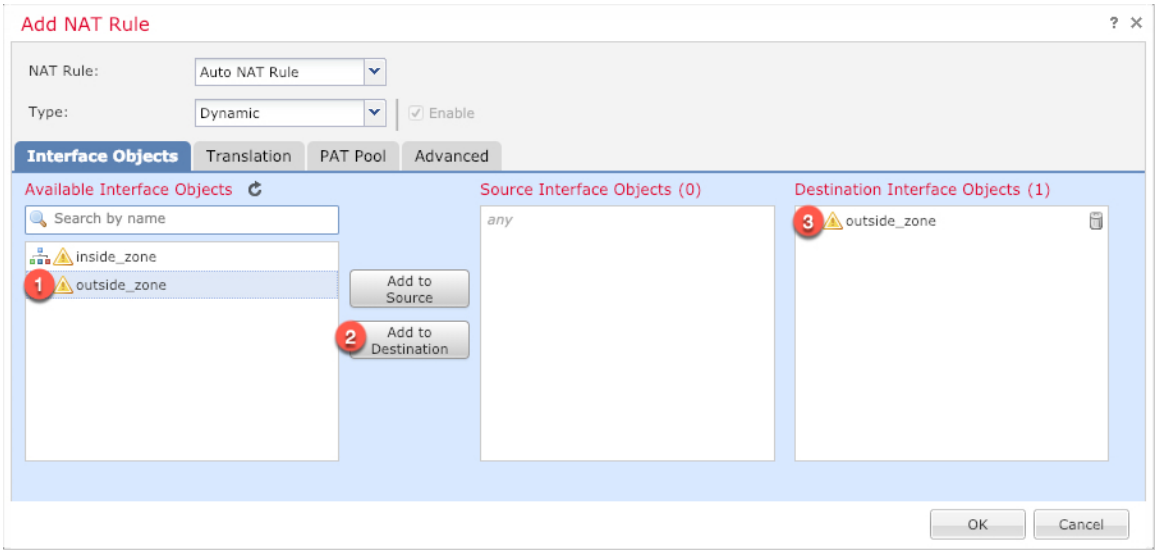
Paso 3 Haga clic en **Agregar regla**.

Aparece el cuadro de diálogo **Agregar regla NAT**.

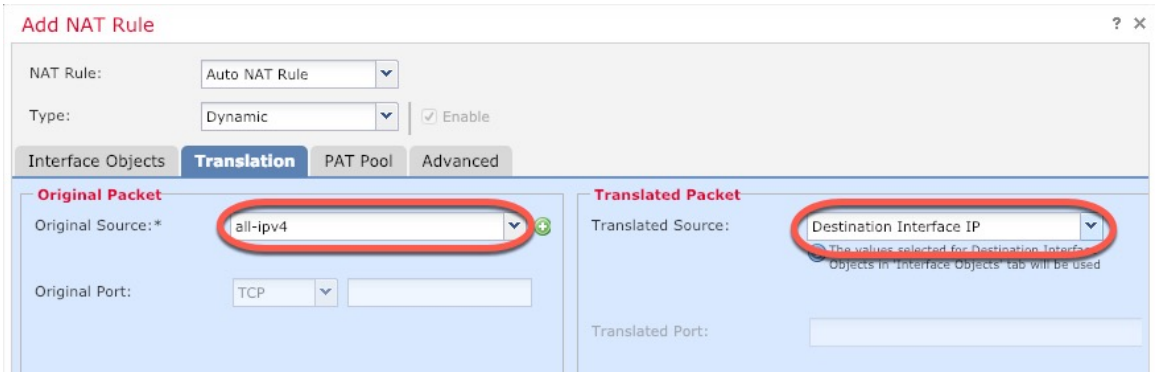
Paso 4 Configure las opciones de regla básicas:

- **Regla NAT**: elija una **regla NAT automática**.
- **Tipo**: seleccione **Dinámico**.

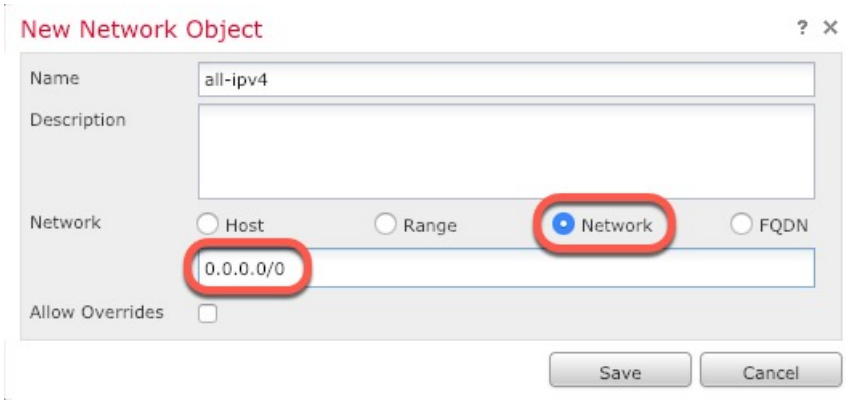
Paso 5 En la página **Objetos de interfaz**, agregue la zona exterior del área **Objetos de interfaz disponibles** al área **Objetos de interfaz de destino**.



Paso 6 En la página **Traducción**, configure las siguientes opciones:



- **Fuente original**: haga clic en **Agregar** (+) para agregar un objeto de red para todo el tráfico IPv4 (0.0.0.0/0).

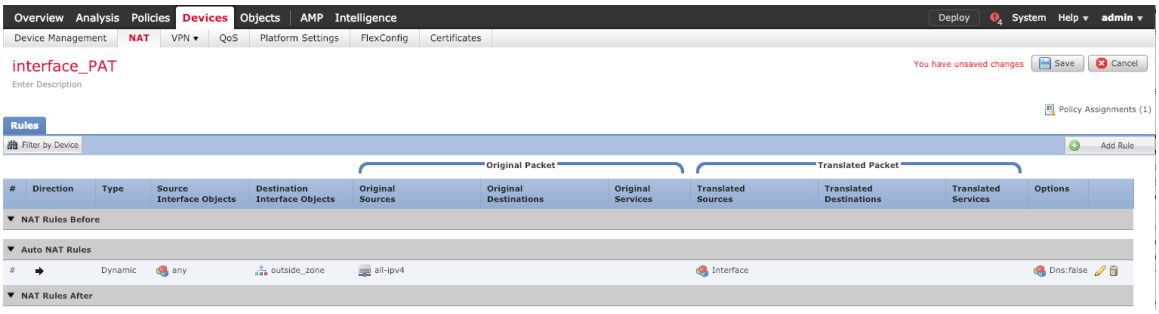


Nota No puede utilizar el objeto **any-ipv4** definido por el sistema, ya que las reglas NAT automáticas añaden NAT como parte de la definición del objeto y no puede editar objetos definidos por el sistema.

- **Fuente traducida**: seleccione la **IP de la interfaz de destino**.

Paso 7 Haga clic en **Guardar** para agregar la regla.

La regla se guarda en la tabla **Reglas**.



Paso 8 Haga clic en **Guardar** en la página de **NAT** para guardar los cambios.

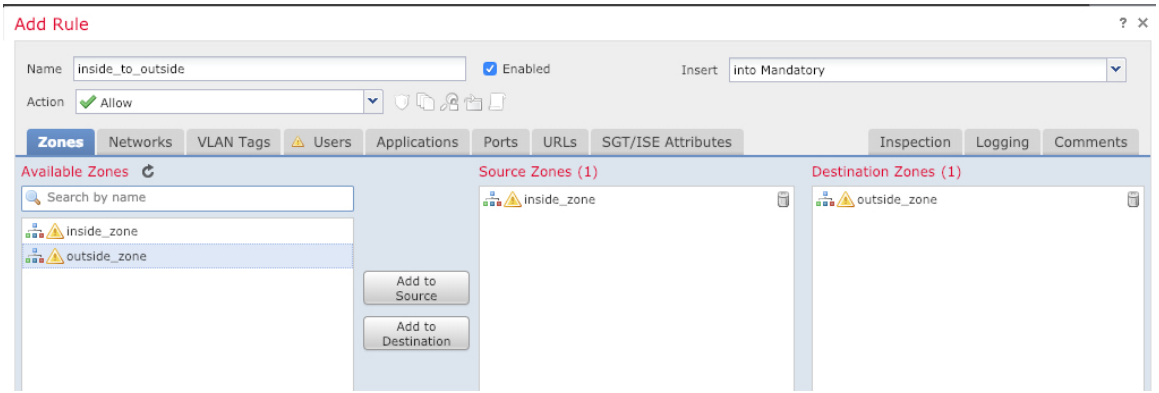
Permitir el tráfico de dentro hacia afuera

Si creó una política básica de control de acceso **Bloquear todo el tráfico** cuando registró la Protección frente a amenazas, entonces debe agregar reglas a la política para permitir el tráfico a través del dispositivo. El siguiente procedimiento agrega una regla para permitir el tráfico de la zona interna a la zona externa. Si tiene otras zonas, asegúrese de agregar reglas que permitan el tráfico a las redes adecuadas.

Procedimiento

Paso 1 Seleccione **Política** > **Política de acceso** > **Política de acceso** y haga clic en **Editar** (✎) para la política de control de acceso asignada a la Protección frente a amenazas.

Paso 2 Haga clic en **Agregar regla** y establezca los siguientes parámetros:

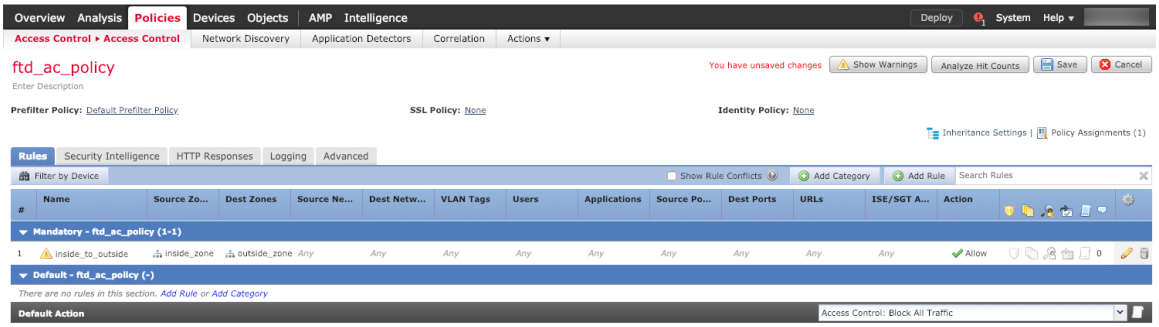


- **Nombre**: nombre esta regla, por ejemplo, **inside_to_outside**.
- **Zonas de origen**: seleccione la zona interna de las **Zonas disponibles** y haga clic en **Agregar al origen**.
- **Zonas de destino**: seleccione la zona externa de las **Zonas disponibles** y haga clic en **Agregar al destino**.

Deje la otra configuración como está.

Paso 3 Haga clic en **Agregar**.

La regla se agrega a la tabla **Reglas**.



Paso 4 Haga clic en **Guardar**.

Configurar SSH en la interfaz de datos de acceso al administrador

Si ha habilitado el acceso al Centro de administración en una interfaz de datos, como la externa, debe habilitar SSH en esa interfaz mediante este procedimiento. Esta sección describe cómo activar las conexiones SSH en una o más interfaces de *datos* en Protección frente a amenazas. SSH no es compatible con la interfaz lógica de diagnóstico.

Nota SSH está activado de forma predeterminada en la interfaz de gestión; sin embargo, esta pantalla no afecta para el acceso al SSH de gestión.

La interfaz de gestión es independiente de las otras interfaces del dispositivo. Se utiliza para configurar y registrar el dispositivo en el Centro de administración. SSH para interfaces de datos comparte la lista de usuarios internos y externos con SSH para la interfaz de administración. Otros ajustes se configuran por separado: para interfaces de datos, active SSH y acceda a las listas mediante esta pantalla; el tráfico SSH para las interfaces de datos utiliza la configuración de rutas regular y no cualquier ruta estática configurada en la configuración o en la CLI.

Para configurar una lista de acceso de SSH en la interfaz de administración, consulte el comando **configure ssh-access-list** en Referencias de comandos en Cisco Secure Firewall Threat Defense. Para configurar una ruta estática, consulte el comando **configure network static-routes**. De forma predeterminada, configure la ruta predeterminada a través de la interfaz de administración en la configuración inicial.

Para utilizar SSH, no necesita una regla de acceso que permita la dirección IP del host. Solo tiene que configurar el acceso SSH con esta sección.

Solo puede utilizar SSH en una interfaz accesible; si su host SSH se encuentra en la interfaz externa, solo puede iniciar la conexión de gestión directamente a la interfaz externa.

El dispositivo permite un máximo de 5 conexiones SSH simultáneas.

Nota Después de que un usuario realice tres intentos fallidos consecutivos de iniciar sesión en la CLI a través de SSH, el dispositivo interrumpe la conexión SSH.

Antes de empezar

- Puede configurar usuarios internos de SSH en la CLI mediante el comando **configure user add**;. De forma predeterminada, hay un usuario **administrador** para el que ha configurado la contraseña durante la configuración inicial. También puede configurar usuarios externos en LDAP o RADIUS si configura la **autenticación externa** en los ajustes de la plataforma.
- Necesita objetos de red que definan los hosts o las redes a las que dará permiso para realizar conexiones SSH al dispositivo. Puede agregar objetos como parte del procedimiento, pero si desea utilizar grupos de objetos para identificar un grupo de direcciones IP, asegúrese de que los grupos que se necesitan en las reglas ya existen. Seleccione **Objetos** > **Administración de objetos** para configurar objetos.

Nota No puede el objeto de red **any** proporcionado por el sistema. En su lugar, utilice **any-ipv**4 o **any-ipv6**.

Procedimiento

Paso 1 Seleccione **Dispositivos** > **Configuración de la plataforma** y cree o edite la política de Protección frente a amenazas.

Paso 2 Seleccione **Secure Shell**.

Paso 3 Identifique las interfaces y las direcciones IP que permiten conexiones SSH.

Utilice esta tabla para limitar las interfaces que aceptarán conexiones SSH y las direcciones IP de los clientes que pueden realizar esas conexiones. Puede utilizar direcciones de red en lugar de direcciones IP individuales.

a) Haga clic en **Agregar** para añadir una nueva regla, o haga clic en **Editar** para modificar una regla existente.
b) Configurar las propiedades de la regla:
   - **Dirección IP**: el objeto o grupo de red que identifica los host o las redes a con permiso para realizar conexiones SSH. Seleccione un objeto del menú desplegable o agregue un nuevo objeto de red haciendo clic en +.
   - **Zonas de seguridad**: agregue las zonas que contienen las interfaces a las que permitirá conexiones SSH. Para las interfaces que no estén en una zona, puede escribir el nombre de la interfaz en el campo debajo de la lista de zona de seguridad seleccionada y hacer clic en **Agregar**. Estas reglas se aplicarán a un dispositivo solo si el dispositivo incluye las interfaces o zonas seleccionadas.
c) Haga clic en **OK** (Aceptar).

Paso 4 Haga clic en **Guardar**.

Ahora puede ir a **Implementar** > **Implementación** e implementar la política en los dispositivos asignados. Los cambios no estarán activos hasta que los implemente.

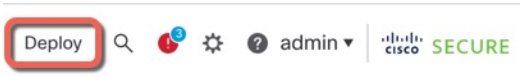
Implementar la configuración

Implementar los cambios de configuración en Protección frente a amenazas; ningún cambio estará activo en el dispositivo hasta que los implemente.

Procedimiento

Paso 1 Haga clic en **Implementar** en la parte superior derecha.

Figura 21: Implementar



Paso 2 Haga clic en **Implementar todo** para implementar en todos los dispositivos o haga clic en **Implementación avanzada** para implementar en los dispositivos seleccionados.

Figura 22: Implementar todo

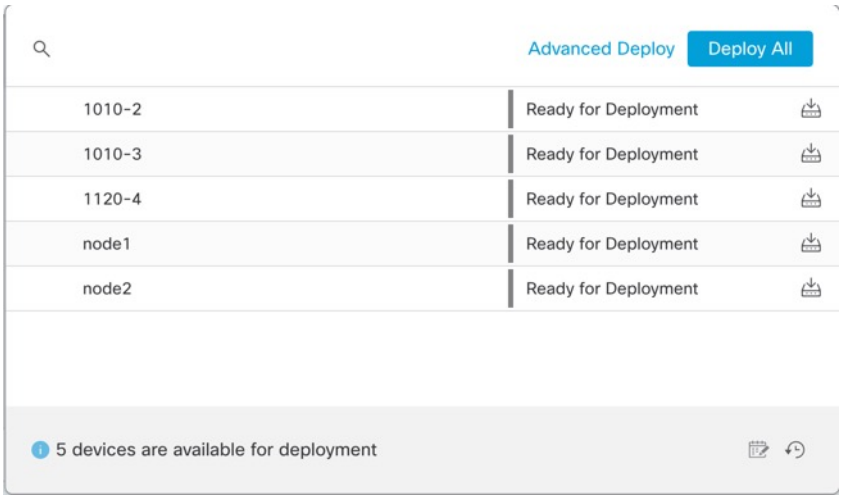
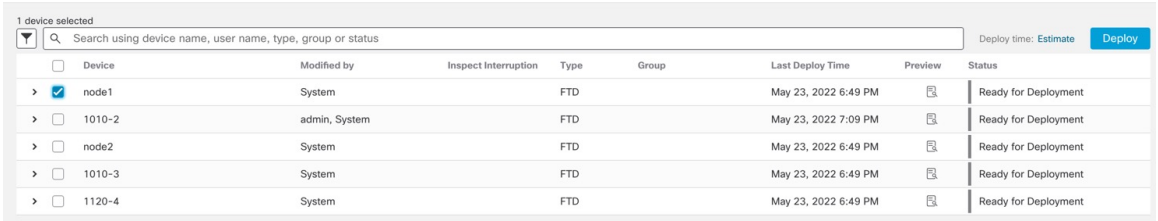
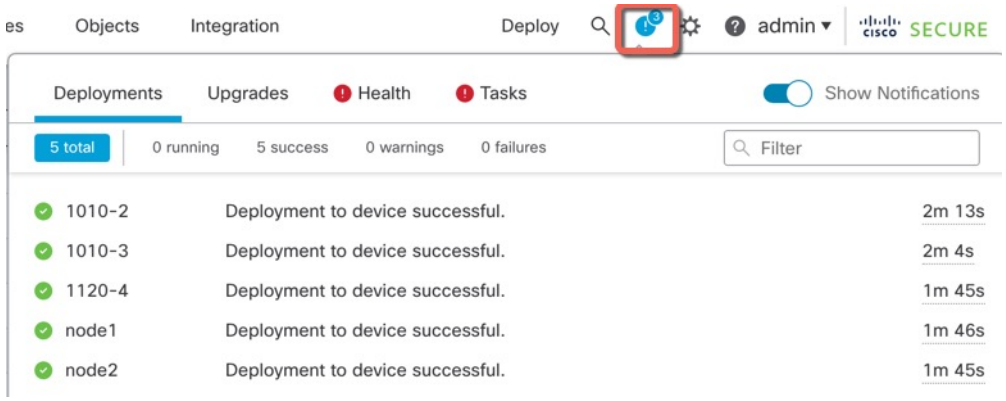


Figura 23: Implementación avanzada



Paso 3 Compruebe que la implementación se realiza correctamente. Haga clic en el icono a la derecha del botón **Implementar** en la barra de menú para ver el estado de las implementaciones.

Figura 24: Estado de la implementación



Acceder a la Protección frente a amenazas y a la CLI de FXOS

Utilice la interfaz de línea de comandos (CLI) para configurar el sistema y solucionar los problemas básicos. No puede configurar políticas a través de una sesión de CLI. Puede acceder a la CLI conectándose al puerto de consola.

También puede acceder a CLI de FXOS para solucionar problemas

Nota Como alternativa, puede utilizar SSH para la interfaz de administración del dispositivo Protección frente a amenazas. A diferencia de una sesión de consola, la sesión SSH se establece de forma predeterminada en la CLI de Protección frente a amenazas, desde la que puede conectarse a CLI de FXOS mediante el comando **connect fxos**. Puede conectarse después a la dirección en una interfaz de datos si abre esa interfaz para las conexiones SSH. El acceso SSH para las interfaces de datos está desactivado de forma predeterminada. Este procedimiento describe el acceso al puerto de consola, cuyo valor predeterminado es CLI de FXOS.

Procedimiento

Paso 1 Para iniciar sesión en la CLI, conecte su ordenador de gestión al puerto de consola. Firepower 1000 va con un cable de serie USB A a B. Instale las unidades USB de serie necesarias para su sistema operativo (consulte la guía de hardware de Firepower 1010). El puerto de consola de forma predeterminada es CLI de FXOS. Utilice la siguiente configuración de serie:

- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada

Se conecta a la CLI de FXOS. Inicie sesión en la CLI con el nombre de usuario **admin** y la contraseña que estableció en la configuración inicial (la predeterminada es **Admin123**).

Ejemplo:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Paso 2 Acceda a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Después de iniciar sesión, para obtener información sobre los comandos disponibles en la CLI, introduzca **help** o **?**. Para obtener información sobre cómo utilizarla, consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Paso 3 Para abandonar la CLI de Protección frente a amenazas, introduzca el comando **exit** o **logout**.

Este comando le devuelve al mensaje de CLI de FXOS. Para obtener información sobre los comandos disponibles en la CLI de FXOS, introduzca **?**.

Ejemplo:

```
> exit
firepower#
```

Solucionar problemas de conectividad de administración en una interfaz de datos

Soporte de modelo—Protección frente a amenazas

Cuando utilice una interfaz de datos para Centro de administración en lugar de utilizar la interfaz de administración específica, debe tener cuidado al cambiar la configuración de la interfaz y de la red del Protección frente a amenazas en el Centro de administración para no interrumpir la conexión. Si cambia el tipo de interfaz de administración después de agregar el Protección frente a amenazas al Centro de administración (de datos a administración o de administración a datos), si las interfaces y los ajustes de red no están configurados correctamente, puede perder la conectividad de la administración.

Este tema le ayuda a solucionar problemas por perder la conectividad de gestión.

Ver el estado de la conexión de administración

En el Centro de administración, compruebe el estado de conexión de administración en la página **Dispositivos** > **Administración de dispositivos** > **Dispositivo** > **Administración** > **Detalles de acceso de FMC** > **Estado de conexión**.

En la CLI de Protección frente a amenazas, introduzca el comando **sftunnel-status-brief** para ver el estado de la conexión de administración. También puede utilizar **sftunnel-status** para ver información más detallada.

Consulte el siguiente ejemplo de salida para ver una conexión inactiva; no hay información de canal conectado "conectado a", ni información de frecuencia:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consulte el siguiente ejemplo de salida para ver una conexión activa; con información de canal conectado e información de frecuencia:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Vea la información sobre la red de Protección frente a amenazas

En la CLI del Protección frente a amenazas, consulte la configuración de red de la interfaz de datos de acceso de administración y Centro de administración:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
```

```
Configuration            : Disabled

===============[ Proxy Information ]================
State                    : Disabled
Authentication           : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers              :
Interfaces               : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                    : Enabled
Link                     : Up
Name                     : outside
MTU                      : 1500
MAC Address              : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration            : Manual
Address                  : 10.89.5.29
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

Compruebe que el Protección frente a amenazas se ha registrado con el Centro de administración

En la CLI de Protección frente a amenazas, compruebe que se ha completado el registro del Centro de administración. Tenga en cuenta que este comando no mostrará el estado *actual* de la conexión de administración.

show managers

```
> show managers
Type                     : Manager
Host                     : 10.89.5.35
Registration             : Completed

>
```

Haga ping al Centro de administración

En la CLI de Protección frente a amenazas, utilice el siguiente comando para hacer ping en el Centro de administración desde las interfaces de datos:

ping *fmc_ip*

En la CLI de Protección frente a amenazas, utilice el siguiente comando para hacer ping en el Centro de administración desde las interfaces de datos, que deberían tener rutas por la placa base hasta las interfaces de datos:

ping system *fmc_ip*

Capturar paquetes en la interfaz interna de Protección frente a amenazas

En la CLI de Protección frente a amenazas, capture paquetes en la interfaz de la placa base interna (nlp_int_tap) para ver si se están enviando paquetes de administración:

capture *nombre* **interface nlp_int_tap trace detail match ip any any**

show capture*Nombre* **trace detail**

Compruebe el estado de la interfaz interna, las estadísticas y el recuento de paquetes

En la CLI de Protección frente a amenazas, consulte la información sobre la interfaz de la placa base interna, nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Comprobar enrutamiento y NAT

En la CLI de Protección frente a amenazas, compruebe que se agregó la ruta predeterminada (S*) y que existen reglas NAT internas para la interfaz de administración (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
```

```
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Comprobar otras configuraciones

Consulte los siguientes comandos para comprobar que todas las demás configuraciones están presentes. También puede ver muchos de estos comandos en la página del **Dispositivos** > **Administración de dispositivos** > **Dispositivo** > **Administración** > **Información de acceso a FMC** > **Salida de CLI** del Centro de administración.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Compruebe si la actualización de DDNS se ha realizado correctamente

En la CLI de Protección frente a amenazas, compruebe la actualización de DDNS se ha realizado correctamente:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Si la actualización ha provocado un error, utilice los comandos **debug http** y **debug ssl**. Para los errores de validación de certificados, compruebe que los certificados de origen están instalados en el dispositivo:

show crypto ca certificates *trustpoint_name*

Para comprobar el funcionamiento de DDNS:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Compruebe los archivos de registro de Centro de administración

Consulte https://cisco.com/go/fmc-reg-error.

Revertir la configuración si el Centro de administración pierde la conectividad

Si utiliza una interfaz de datos en Protección frente a amenazas para el Centro de administración, e implementa un cambio en la configuración del Centro de administración que afecte a la conectividad red, puede restablecer la la configuración desde el Protección frente a amenazasa a última configuración implementada para restaurar la conectividad de la administración. A continuación, puede ajustar los valores de la configuración en Centro de administración para mantener la conectividad de red y volver a implementarla. Puede utilizar la función de reversión incluso si no pierde la conectividad; no está limitada a la resolución de problemas.

Consulte las siguientes directrices:

- Solo la implementación anterior está disponible localmente en Protección frente a amenazas; no se puede revertir a implementaciones previas.
- La reversión no es compatible con las implementaciones de alta disponibilidad o de clústeres.
- La reversión solo afecta a las configuraciones que se pueden establecer en el Centro de administración. Por ejemplo, la reversión no afecta a ninguna configuración local relacionada con la interfaz de administración específica, que solo se puede configurar en la CLI de Protección frente a amenazas. Tenga en cuenta que si ha cambiado la configuración de la interfaz de datos después de la última implementación del Centro de administración mediante el comando **configure network management-data-interface** y, a continuación, utiliza el comando de reversión, dicha configuración no se conservará; volverán a la configuración del Centro de administraciónimplementada por última vez.
- El modo UCAPL/CC no se puede revertir.

- Los datos de certificado SCEP fuera de banda que se actualizaron durante la implementación anterior no se pueden revertir.
- Durante la reversión, se perderán las conexiones porque se borrará la configuración actual.

Antes de empezar

Soporte de modelo—Protección frente a amenazas

Procedimiento

Paso 1 En la CLI de Protección frente a amenazas, vuelva a la configuración anterior.

configure policy rollback

Después de la reversión, el Protección frente a amenazas notifica al Centro de administración que la reversión se completó correctamente. En el Centro de administración, la pantalla de implementación mostrará un banner que indica que la configuración se ha revertido.

Si la reversión ha provocado un error, consulte https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html para problemas comunes de implementación. En algunos casos, la reversión puede fallar después de que se restablezca el acceso a Centro de administración; en este caso, puede resolver los problemas de configuración de Centro de administración, y volverlos a implementar desde Centro de administración.

Ejemplo:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Paso 2 Compruebe que se ha restablecido la conexión de administración.

En el Centro de administración, compruebe el estado de conexión de administración en la página **Dispositivos** > **Administración de dispositivos** > **Dispositivo** > **Administración** > **Detalles de acceso de FMC** > **Estado de conexión**.

En la CLI de Protección frente a amenazas, introduzca el comando **sftunnel-status-brief** para ver el estado de la conexión de administración.

Si tarda más de 10 minutos en restablecer la conexión, debe solucionar el problema de conexión. Consulte Solucionar problemas de conectividad de administración en una interfaz de datos, en la página 83.

Desactive el firewall mediante Centro de administración

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación o pulsa el interruptor de alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su firewall.

Puede apagar el sistema correctamente con el Centro de administración.

Procedimiento

Paso 1 Elija **Dispositivo** > **Administración de dispositivos**.

Paso 2 Junto al dispositivo que desea reiniciar, haga clic en el icono de editar ( ).

Paso 3 Haga clic en la pestaña **Dispositivo**.

Paso 4 Haga clic en el icono de apagar dispositivo ( ) en la sección **Sistema**.

Paso 5 Cuando se le solicite, confirme que desea apagar el dispositivo.

Paso 6 Si tiene una conexión de consola al firewall, monitorice los mensajes del sistema una vez que este se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si no tiene una conexión de consola, espere aproximadamente 3 minutos para asegurarse de que el sistema se ha apagado.

Paso 7 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

¿Qué es lo siguiente que debe hacer?

Para continuar con la configuración de la Protección frente a amenazas, consulte los documentos disponibles para su versión de software en Navegación por la documentación de Cisco Firepower.

Para obtener información relacionada con el uso del Centro de administración, consulte la Guía de configuración del Centro de administración de Firepower.

CAPÍTULO 4

Implementación de Protección frente a amenazas con el Administrador del dispositivo

¿Este capítulo es para usted?

Para ver todos los sistemas operativos y administradores disponibles, consulte ¿Qué aplicación y administrador son adecuados para usted?, en la página 1. Este capítulo hace referencia al Protección frente a amenazas con el Administrador del dispositivo.

Este capítulo explica cómo completar la configuración inicial y los ajustes de su Protección frente a amenazas mediante el asistente de configuración de dispositivos basado en la web .

Administrador del dispositivo sirve para configurar las funciones básicas del software que se utilizan con mayor frecuencia en las redes pequeñas. Está especialmente diseñado para redes con uno o pocos dispositivos para los que prefiere no utilizar un administrador de varios dispositivos de gran potencia para controlar una red grande con muchos dispositivos Administrador del dispositivo.

Sobre el firewall

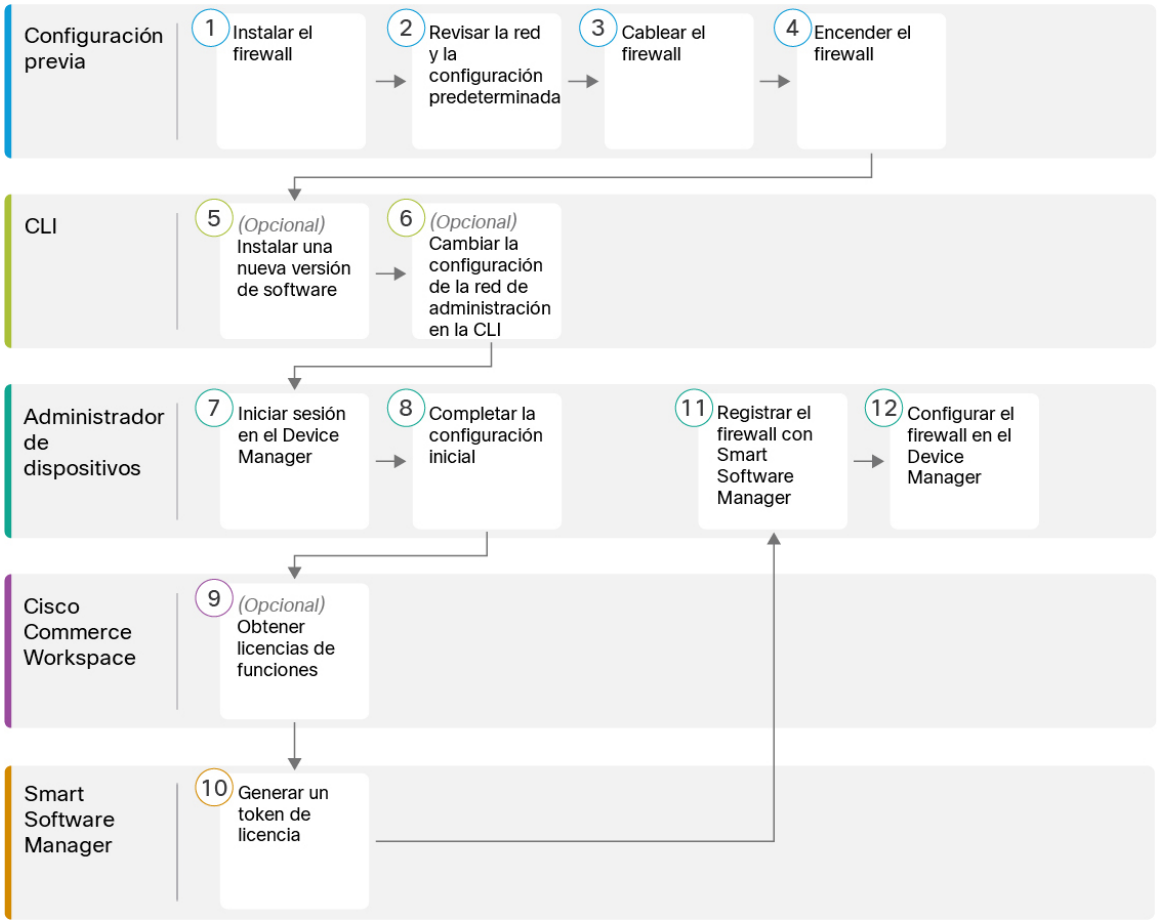
El hardware puede ejecutar el software Protección frente a amenazas o el software ASA. Para cambiar entre Protección frente a amenazas y ASA es necesario que vuelva a crear una imagen para el dispositivo. También es necesario que lleve a cabo una una recreación de imagen si necesita una versión de software diferente a la instalada. Consulte Recreación de la imagen del dispositivo de defensa contra amenazas de Firepower o ASA de Cisco.

El firewall ejecuta un sistema operativo subyacente llamado Cisco Secure Firewall Extensible Operating System (FXOS). El firewall no es compatible con el Administrador del chasis Cisco Secure Firewall de FXOS; solo se admite una CLI limitada para la resolución de problemas. Consulte Guía de resolución de problemas de Cisco FXOS para Firepower 1000/2100 Series que ejecuta Firepower Threat Defense para obtener más información.

Declaración de recopilación de privacidad: el firewall no necesita ni recopila de forma activa información de identificación personal. Sin embargo, puede utilizar información de identificación personal en la configuración, por ejemplo, para los nombres de usuario. En este caso, un administrador podrá ver esta información cuando trabaje con la configuración o cuando utilice SNMP.

Procedimiento completo

Consulte las siguientes tareas para implementar Protección frente a amenazas con Administrador del dispositivo en su chasis.



1	Configuración previa	Instale el firewall. Consulte la guía de instalación del hardware.
2	Configuración previa	Revisar la implementación de la red y la configuración predeterminada, en la página 93.

3	Configuración previa	Cablear el dispositivo, en la página 96.
4	Configuración previa	Encender el firewall, en la página 13.
5	CLI	(Opcional) Comprobar el software e instalar una nueva versión, en la página 98
6	CLI	(Opcional) Cambie la configuración de la red de administración en la CLI, en la página 100.
7	Administrador del dispositivo	Iniciar sesión en Administrador del dispositivo, en la página 102.
8	Administrador del dispositivo	Complete la configuración inicial, en la página 102.
9	Cisco Commerce Workspace	(Opcional) Configurar licencias, en la página 104: obtener licencias de funciones.
10	Smart Software Manager	Configurar licencias, en la página 104: generar un token de licencia.
11	Administrador del dispositivo	Configurar licencias, en la página 104: registrar el dispositivo con el servidor Smart Licensing.
12	Administrador del dispositivo	Configurar el firewall en Administrador del dispositivo, en la página 110.

Revisar la implementación de la red y la configuración predeterminada

Puede administrar el Protección frente a amenazas con Administrador del dispositivo desde la interfaz de administración 1/1 o desde la interfaz interna. La interfaz de gestión específica es una interfaz especial con sus propios ajustes de red.

La siguiente figura muestra la implementación de red recomendada. Si conecta la interfaz externa directamente a un cable módem o un módem DSL, recomendamos poner el módem en modo puente para que Protección frente a amenazas lleve a cabo todas las rutas y las NAT para las redes internas. Si necesita configurar PPPoE para que la interfaz externa se conecte a su ISP, puede hacerlo tras completar la configuración inicial en Administrador del dispositivo.

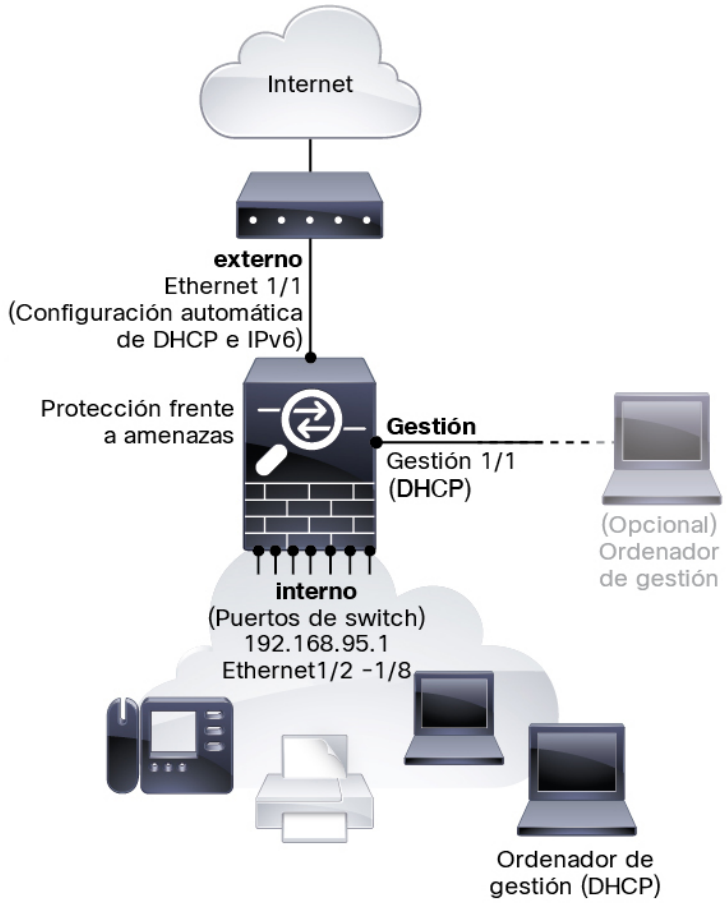
Nota Si no puede utilizar la dirección IP de administración predeterminada (por ejemplo, su red de administración no incluye un servidor DHCP), puede conectarse al puerto de la consola y llevar a cabo la configuración inicial en la CLI, en la que se incluye la dirección IP de administración, la gateway y otros ajustes básicos de red.

Si necesita cambiar la dirección IP interna, puede hacerlo después de completar la configuración inicial en el Administrador del dispositivo. Por ejemplo, puede ser necesario cambiar la dirección IP interna si:

- (7.0 y posterior) La dirección IP interna es 192.168.95.1. (6.7 y anterior) La dirección IP interna es 192.168.1.1. Si la interfaz externa intenta obtener una dirección IP en la red 192.168.1.0, que es una red predeterminada común, la concesión DHCP provocará un error y la interfaz externa no obtendrá una dirección IP. Este problema ocurre porque Protección frente a amenazas no puede tener dos interfaces en la misma red. En este caso, debe cambiar la dirección IP interna para que esté en una nueva red.
- Si agrega Protección frente a amenazas a una red interna existente, tendrá que cambiar la dirección IP interna para que esté en esa red.

La siguiente figura muestra la implementación de red predeterminada para Protección frente a amenazas utilizando Administrador del dispositivo con la configuración predeterminada.

Figura 25: Instalación en la red recomendada



Nota Para la versión 6.7 y anteriores, la dirección IP interna de es 192.168.1.1.

Para la versión 6.5 y anteriores, la dirección IP predeterminada de Administración 1/1 es 192.168.45.45.

Configuración predeterminada

La configuración del firewall tras la configuración inicial incluye lo siguiente:

- **interna**: dirección IP (7.0 y posterior) 192.168.95.1; (anterior a 7.0) 192.168.1.1.
  - (6.5 y posterior) **Switch de hardware:** Ethernet 1/2 a 1/8 que pertenece a VLAN 1
  - (6.4) **Switch de software** (rutas y puentes integrados): Ethernet 1/2 a 1/8 que pertenece a la interfaz de grupo de puente (BVI) 1
- **externa**: Ethernet 1/1, dirección IP del DHCP IPv4 y configuración automática de IPv6
- flujo de tráfico **interno → externo**
- **administración**: administración 1/1 (gestión)
  - (6.6 y posterior) dirección IP de DHCP
  - (6.5 y anterior) dirección IP 192.168.45.45

Nota La interfaz administración 1/1 es una interfaz especial independiente de las interfaces de datos que se utiliza para la administración, licencias Smart y actualizaciones de la base de datos. La interfaz física se comparte con una segunda interfaz lógica, la interfaz de diagnóstico. El diagnóstico es una interfaz de datos, pero se limita a otros tipos de tráfico de gestión (al dispositivo y desde el dispositivo), como syslog o SNMP. La interfaz de diagnóstico no se utiliza normalmente. Consulte Guía de configuración del dispositivo de administración Cisco Secure Firewall para obtener más información.

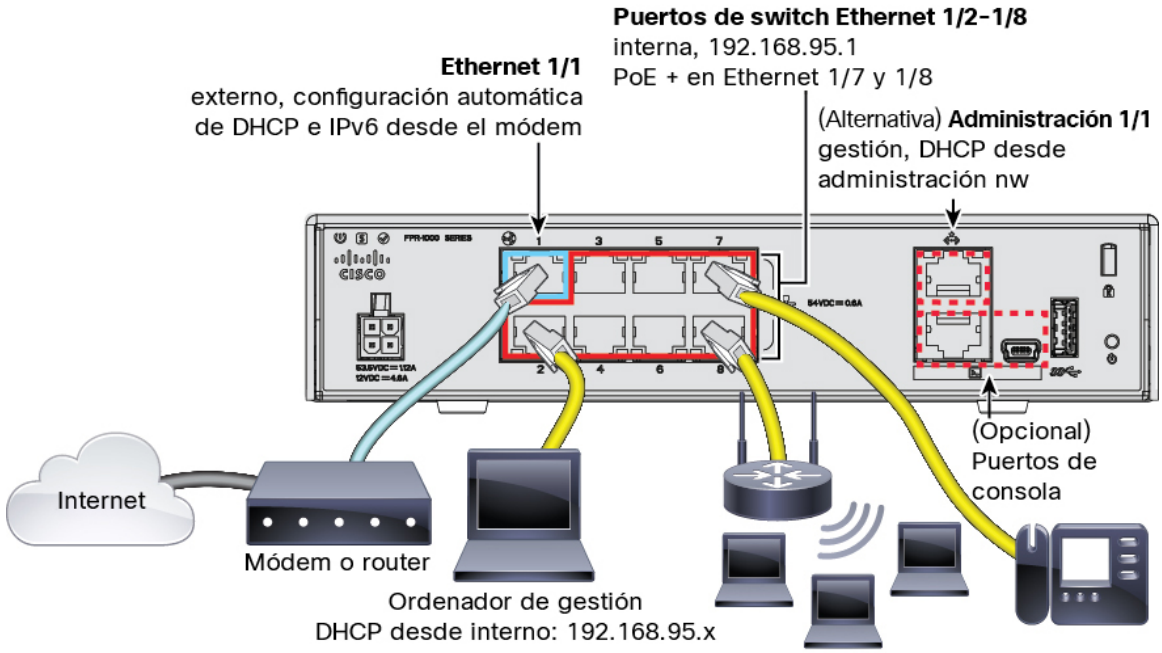
- **Servidor DNS para gestión**: OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35 o los servidores que especifique durante la configuración. Los servidores DNS que se obtienen a partir del DHCP no se utilizan nunca.
- **NTP**: servidores Cisco NTP: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org o servidores que especifique durante la configuración
- **Rutas predeterminadas**
  - **Interfaces de datos**: obtenidas de DHCP externo o de una dirección IP de gateway que especifique durante la configuración
  - **Interfaz de gestión**: (6.6 y posteriores) Obtenida del DHCP de administración. Si no recibe una gateway, la ruta predeterminada es a través de la placa base y de las interfaces de datos. (6.5 y anteriores) A través de la placa base y de las interfaces de datos

Tenga en cuenta que la interfaz de gestión necesita acceso a Internet para las licencias y las actualizaciones, ya sea a través de la placa base o mediante un gateway de Internet independiente. Tenga en cuenta que solo el tráfico que se origina en la interfaz de gestión puede pasar por la placa base; de lo contrario, la gestión no permite el tráfico directo a través del que entra en gestión desde la red.

- **Servidor DHCP**: activado en la interfaz interna y (6.5 y anteriores solo) interfaz de gestión
- **Acceso a Administrador del dispositivo**: todos los hosts permitidos en la administración y en la interfaz interna.
- **NAT**: interfaz PAT para todo el tráfico de interno a externo

Cablear el dispositivo

Figura 26: Cableado de Firepower 1010



Nota Para la versión 6.7 y anteriores, la dirección IP interna es 192.168.1.1.

Para la versión 6.5 y anteriores, la dirección IP predeterminada de Gestión 1/1 es 192.168.45.45.

Nota En la versión 6.5 y posteriores, Ethernet1/2 a 1/8 se configuran como puertos de switch de hardware; PoE+ también está disponible en Ethernet 1/7 y 1/8. En la versión 6.4, Ethernet1/2 a 1/8 se configuran como miembros del grupo de puente (puertos de switch de software); PoE+ no está disponible. El cableado inicial es el mismo para ambas versiones.

Administre Firepower 1010 en Gestión 1/1 o Ethernet 1/2 a 1/8. La configuración predeterminada también configura Ethernet1/1 como externa.

Procedimiento

Paso 1 Instale su hardware y familiarícese con él siguiendo la guía de instalación del hardware.

Paso 2 Conecte su equipo de administración a una de las siguientes interfaces:

- Ethernet 1/2 a 1/8: conecte el ordenador de gestión directamente a uno de los puertos internos del switch (Ethernet 1/2 a 1/8). La interfaz interna tiene una dirección IP predeterminada (192.168.95.1) y también ejecuta un servidor DHCP para proporcionar direcciones IP a los clientes (incluido el equipo de administración), por lo que debe asegurarse de que estas configuraciones no entren en conflicto con ninguna configuración de red interna existente (consulte Configuración predeterminada, en la página 95).
- Gestión 1/1 (con la etiqueta MGMT): conecte Gestión 1/1 a su red de gestión y asegúrese de que su ordenador de gestión esté en la red de gestión o tenga acceso a ella. Gestión 1/1 obtiene una dirección IP de un servidor DHCP de su red de gestión; si utiliza esta interfaz, debe determinar la dirección IP asignada al Protección frente a amenazas para que pueda conectarse a la dirección IP desde su equipo de administración.

  Si necesita cambiar la dirección IP de gestión 1/1 predeterminada para configurar una dirección IP estática, también debe conectar su equipo de administración al puerto de consola. Consulte (Opcional) Cambie la configuración de la red de administración en la CLI, en la página 100.

Paso 3 Conecte la red externa a la interfaz Ethernet 1/1.

De manera predeterminada, la dirección IP se obtiene mediante DHCP IPv4 y autoconfiguración IPv6, pero puede establecer una dirección estática durante la configuración inicial.

Paso 4 Conecte los dispositivos internos a los puertos de switch que quedan, Ethernet 1/2 a 1/8.

Ethernet 1/7 a 1/8 son puertos PoE+.

Encender el firewall

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Antes de empezar

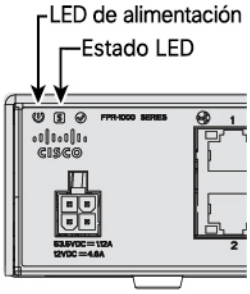
Es importante que proporcione una alimentación fiable para su dispositivo (con una fuente de alimentación ininterrumpida (UPS), por ejemplo). Si se pierde la fuente de alimentación sin apagar primero se pueden provocar daños graves en el sistema de archivos. Hay muchos procesos que se ejecutan en segundo plano todo el tiempo y, si se pierde la fuente de alimentación, el sistema no se puede apagar adecuadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

(Opcional) Comprobar el software e instalar una nueva versión

Para comprobar la versión del software e instalar una versión diferente, si es necesario, siga estos pasos. Le recomendamos que instale su versión de destino antes de configurar el firewall. Como alternativa, puede realizar una actualización una vez que esté en funcionamiento, pero la actualización, que conserva su configuración, puede llevar más tiempo que este procedimiento.

¿Qué versión debo ejecutar?

Cisco recomienda ejecutar una versión Gold Star indicada con una estrella dorada junto al número de versión en la página de descarga de software. También puede consultar la estrategia de versiones descrita en https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; Por ejemplo, este boletín describe la numeración de las versiones a corto plazo (con las características más recientes), la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para un período de tiempo más largo) o la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para el período de tiempo más largo, para la certificación del gobierno).

Procedimiento

Paso 1 Conéctese a la CLI. Consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 114 para obtener más información. Este procedimiento se muestra a través del puerto de consola, pero también puede utilizar SSH en su lugar.

Inicie sesión con el usuario **administrador** y la contraseña predeterminada **Admin123**.

Se conecta a la CLI de FXOS. La primera vez que inicie sesión, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se cambió la contraseña, y no lo sabe, debe llevar a cabo una restauración de fábrica para recuperar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el Procedimiento de restauración de fábrica.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 2 En la CLI de FXOS, muestre la versión en ejecución.

scope ssa

show app-instance

Ejemplo:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Paso 3 Si desea instalar una nueva versión, lleve a cabo estos pasos.

a) Si necesita establecer una dirección IP estática para la interfaz de administración, consulte (Opcional) Cambie la configuración de la red de administración en la CLI, en la página 100. La interfaz de administración utiliza por defecto DHCP.

Tendrá que descargar la nueva imagen de un servidor accesible desde la interfaz de administración.

b) Lleve a cabo el procedimiento de recrear la imagen que aparece en la guía de resolución de problemas de FXOS.

(Opcional) Cambie la configuración de la red de administración en la CLI

Si no puede utilizar la dirección IP de administración predeterminada, puede conectarse al puerto de la consola y llevar a cabo la configuración inicial en la CLI, en la que se incluye la dirección IP de administración, la gateway y otros ajustes básicos de red. Solo puede configurar los ajustes de la interfaz de gestión; no puede configurar interfaces internas o externas, que puede configurar más tarde en la GUI.

Nota No puede volver a abrir el script de configuración de la CLI a menos que borre la configuración; por ejemplo, al restablecer la imagen. Sin embargo, todos estos ajustes pueden cambiarse más tarde en la CLI mediante los comandos de **configuración de red**. Consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Procedimiento

Paso 1 Conéctese al puerto de consola de Protección frente a amenazas. Consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 114 para obtener más información.

Inicie sesión con el usuario **administrador** y la contraseña predeterminada **Admin123**.

Se conecta a la CLI de FXOS. La primera vez que inicie sesión, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se ha cambiado la contraseña y no lo sabe, debe volver a crear el dispositivo para restablecer la contraseña a la predeterminada. Consulte la guía de resolución de problemas de FXOS para el procedimiento de restablecer la imagen.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 2 Conéctese a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Paso 3 La primera vez que inicie sesión en Protección frente a amenazas, se le solicitará que acepte el contrato de licencia de usuario final (EULA). A continuación, se le presenta el script de configuración de la CLI.

Los valores predeterminados o los introducidos anteriormente aparecen entre paréntesis. Para aceptar los valores introducidos anteriormente, pulse **Intro**.

Consulte las siguientes directrices:

- **Introduzca la gateway predeterminada IPv4 de la interfaz de gestión**. Si establece una dirección IP manual, introduzca las **interfaces de datos** o la dirección IP del router de la gateway. La configuración de **interfaces de datos** envía tráfico de gestión saliente a través de la placa base para salir de una interfaz de datos. Esta configuración es útil si no dispone de una red de gestión independiente que pueda acceder a Internet. El tráfico que se origina en la interfaz de gestión incluye el registro de licencias y las actualizaciones de la base de datos que requieren acceso a Internet. Si utiliza **interfaces de datos**, todavía puede utilizar el Administrador del dispositivo (o SSH) en la interfaz de administración si está conectada directamente a la red de administración, pero para la administración remota de determinadas redes o hosts, debe agregar una ruta estática mediante el siguiente comando **configure network static-routes**. Tenga en cuenta que la administración de Administrador del dispositivo en las interfaces de datos no se ve afectada por esta configuración. Si utiliza DHCP, el sistema utiliza la gateway proporcionada por DHCP y utiliza las **interfaces de datos** como método de reserva si DHCP no proporciona una gateway.
- **Si su información de red ha cambiado, tendrá que volver a conectarse**. Si está conectado a SSH mediante la dirección IP predeterminada pero cambia la dirección IP en la configuración inicial, se desconectará. Vuelva a conectarse con la nueva dirección IP y la contraseña. Las conexiones de la consola no se ven afectadas.
- **¿Administrar el dispositivo de forma local?** Introduzca **sí** para utilizar el Administrador del dispositivo o el CDO/Administrador del dispositivo. Si contesta **no** significa que pretende utilizar el Centro de administración para administrar el dispositivo.

Ejemplo:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Manage the device locally? (yes/no) [yes]: yes

>
```

Paso 4 Inicie sesión en Administrador del dispositivo en la nueva dirección IP de administración.

Iniciar sesión en Administrador del dispositivo

Inicie sesión en Administrador del dispositivo para configurar su Protección frente a amenazas.

Antes de empezar

- Utilice una versión actual de Firefox, Chrome, Safari, Edge o Internet Explorer.

Procedimiento

Paso 1 Introduzca la siguiente URL en su navegador.

- (7.0 y posteriores) Interno (Ethernet1/2 a 1/8)—**https://192.168.95.1**.Puede conectarse a la dirección interna en cualquier puerto interno del switch (Ethernet1/2 a 1/8).
- (6.7 y anteriores) Interno (Ethernet1/2 a 1/8)—**https://192.168.1.1**.Puede conectarse a la dirección interna en cualquier puerto interno del switch (Ethernet1/2 a 1/8).
- (6.6 y posteriores) Administración: **https://***management_ip*. La interfaz de administración es un cliente DHCP, por lo que la dirección IP depende de su servidor DHCP. Si ha cambiado la dirección IP de administración en la configuración de la CLI, introduzca esa dirección .
- (6.5 y anteriores) Administración: **https://192.168.45.45**. Si ha cambiado la dirección IP de administración en la configuración de la CLI, introduzca esa dirección .

Paso 2 Inicie sesión con el nombre de usuario del **administrador**, y lacontraseña predeterminada **Admin123**.

Qué hacer a continuación

- ejecutar a través del asistente de configuración Administrador del dispositivo; ver Complete la configuración inicial, en la página 102.

Complete la configuración inicial

Utilice el asistente de configuración cuando inicie sesión por primera vez en Administrador del dispositivo para completar la configuración inicial. Después de que complete el asistente de configuración, debería tener un dispositivo en funcionamiento con algunas políticas básicas:

- Una interfaz externa (Ethernet1/1) y otra interna. Los puertos Ethernet1/2 a 1/8 son puertos de conmutación en la interfaz VLAN1 interna (6.5 y posteriores) o miembros del grupo de puentes internos en BVI1 (6.4).
- Zonas de seguridad para las interfaces interna y externa.
- Una regla de acceso que confía en todo el tráfico interno y externo.
- Una regla NAT de interfaz que traduce todo el tráfico interno y externo a puertos únicos en la dirección IP de la interfaz externa.
- Un servidor DHCP que se ejecuta en la interfaz interna.

Nota Si ha realizado el procedimiento (Opcional) Cambie la configuración de la red de administración en la CLI, en la página 100, entonces algunas de estas tareas, concretamente cambiar la contraseña de administrador y configurar las interfaces externa y de administración, deberían haberse completado.

Procedimiento

Paso 1 Se le pedirá que lea y acepte el contrato de licencia del usuario final y que cambie la contraseña de administrador.

Debe completar estos pasos para continuar.

Paso 2 Configure las siguientes opciones para las interfaces externas y de administración y haga clic en **Siguiente**.

Nota Su configuración se implementa en el dispositivo cuando hace clic en **Siguiente**. La interfaz se llamará "outside" y se agregará a la zona de seguridad "outside_zone". Asegúrese de que la configuración sea correcta.

a) **Interfaz externa**: este es el puerto de datos que conectó a su router de gateway. No se puede seleccionar una interfaz externa alternativa durante la configuración inicial del dispositivo. La primera interfaz de datos es la interfaz externa predeterminada.

Configure IPv4: la dirección IPv4 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, una máscara de subred y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv4. No puede configurar PPPoE con el asistente de configuración. PPPoE puede ser necesario si la interfaz está conectada a un módem DSL, a un módem por cable o a otra conexión con su ISP, y su ISP utiliza PPPoE para proporcionar su dirección IP. Puede configurar PPPoE después de completar el asistente.

Configure IPv6: la dirección IPv6 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, un prefijo y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv6.

b) **Interfaz de administración**

Servidores DNS: el servidor DNS para la dirección de administración del sistema. Introduzca una o varias direcciones de servidores DNS para la resolución de nombres. El valor predeterminado son los servidores DNS públicos de OpenDNS. Si edita los campos y quiere volver a los predeterminados, haga clic en **Usar OpenDNS** para volver a cargar las direcciones IP adecuadas en los campos.

Nombre de host del firewall: el nombre de host para la dirección de administración del sistema.

Paso 3 Configure los ajustes de la hora del sistema y haga clic en **Siguiente**.

a) **Zona horaria**: seleccione la zona horaria del sistema.

b) **Servidor de hora NTP**: seleccione si desea utilizar los servidores NTP predeterminados o introducir manualmente las direcciones de sus servidores NTP. Puede agregar varios servidores para proporcionar copias de seguridad.

Paso 4 (Opcional) Configure las licencias smart del sistema.

La compra del dispositivo Protección frente a amenazas incluye automáticamente una licencia básica. Todas las demás licencias adicionales son opcionales.

Debe tener una cuenta de Smart License para obtener y aplicar las licencias que requiere el sistema. Inicialmente, puede utilizar la licencia de evaluación de 90 días y configurar Smart Licensing más tarde.

Para registrar el dispositivo ahora, haga clic en el enlace para iniciar sesión en su cuenta de Smart Software Manager y vea Configurar licencias, en la página 104.

Para utilizar la licencia de evaluación, seleccione **Iniciar periodo de evaluación de 90 días sin registro**.

Paso 5 Haga clic en **Finalizar**.

Qué hacer a continuación

- Aunque puede seguir utilizando la licencia de evaluación, le recomendamos que registre y obtenga la licencia de su dispositivo; vea Configurar licencias, en la página 104.
- También puede optar por configurar el dispositivo mediante Administrador del dispositivo; consulte Configurar el firewall en Administrador del dispositivo, en la página 110.

Configurar licencias

Protección frente a amenazas utiliza la licencia de Smart Software, que le permite comprar y administrar un conjunto de licencias de forma centralizada.

Cuando registra el chasis, el Smart Software Manager emite un certificado de ID para comunicarse con el chasis y el Smart Software Manager. También asigna el chasis a la cuenta virtual correspondiente.

Para obtener una descripción general más detallada sobre Cisco Licensing, visite cisco.com/go/licensingguide

La licencia básica se incluye automáticamente. Smart Licensing no le impide utilizar las funciones del producto que aún no haya adquirido. Puede comenzar a utilizar una licencia inmediatamente, siempre y cuando esté registrado con Smart Software Manager y adquiera la licencia más tarde. Esto le permite implementar y utilizar una función y evitar retrasos debido a la aprobación del pedido de compra. Vea las siguientes licencias:

- **Amenazas**: inteligencia de seguridad e IPS de última generación
- **Malware**: protección frente al malware
- **URL**: filtrado de URL
- **VPN con RA**: AnyConnect Plus, AnyConnect Apex o AnyConnect solo VPN

Antes de empezar

- Tener una cuenta principal en Smart Software Manager.

  Si aún no tiene una cuenta, haga clic en el enlace para configurar una nueva cuenta. Smart Software Manager le permite crear una cuenta principal para su organización.

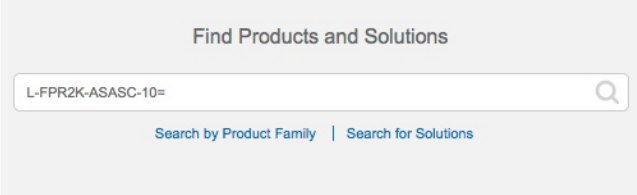
- Su cuenta de licencias de Smart Software debe cumplir los requisitos de la licencia de cifrado seguro (3DES/AES) para utilizar algunas funciones (que se activan mediante el indicador de cumplimiento de exportación).

Procedimiento

Paso 1 Compruebe que su cuenta de licencias Smart contenga las licencias disponibles que necesita.

Cuando adquirió su dispositivo en Cisco o en un distribuidor, sus licencias deberían haberse vinculado a su cuenta de licencias Smart Software. Sin embargo, si necesita agregar licencias usted mismo, utilice el campo de búsqueda **Buscar productos y soluciones** en Cisco Commerce Workspace. Busque las siguientes PID de licencia:

Figura 27: Búsqueda de licencia



Nota Si no se encuentra una PID, puede agregarla manualmente a su pedido.

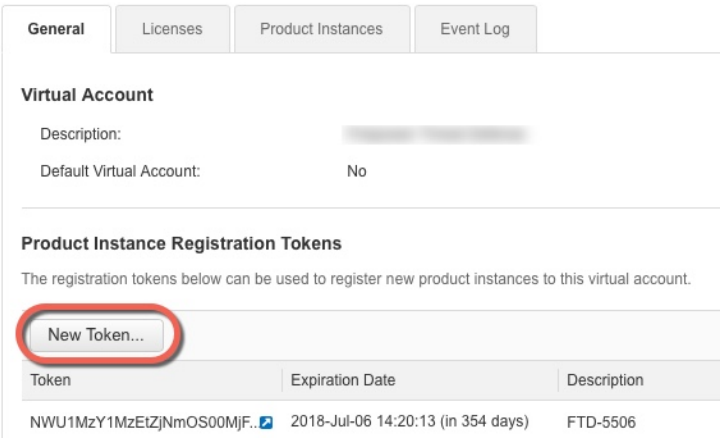
- Combinación de licencias de amenazas, malware y URL:
  - L-FPR1010T-TMC=

  Cuando agregue una de las PID anteriores a su pedido, podrá elegir una suscripción basada en el plazo correspondiente a una de las siguientes PID:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN con RA: consulte la Guía de pedidos de Cisco AnyConnect.

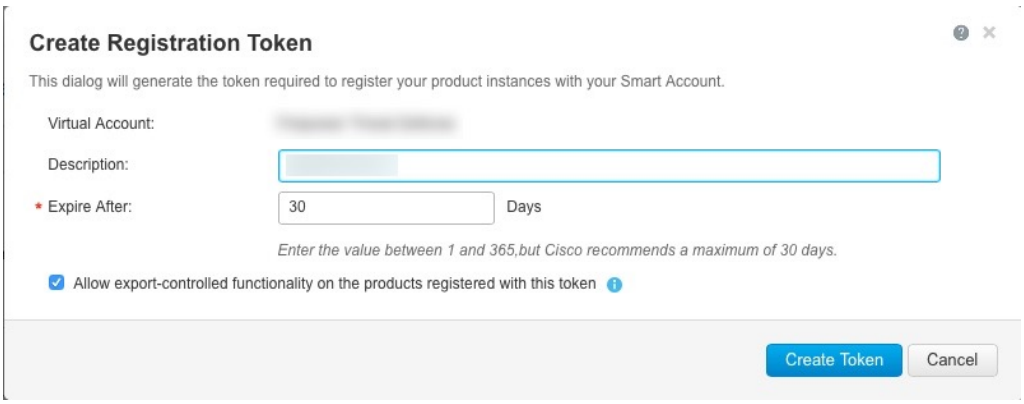
Paso 2 En el Smart Software Manager, solicite y copie un token de registro para la cuenta virtual a la que desea agregar este dispositivo.

a) Haga clic en **Inventario**.

b) En la pestaña **General**, haga clic en **Nuevo token**.



c) En el cuadro de diálogo **Crear token de registro**, introduzca la siguiente configuración y haga clic en **Crear token**:



- **Descripción**
- **Caduca después de**: Cisco recomienda 30 días.
- **Permitir la funcionalidad controlada por la exportación en los productos registrados con este token**: activa el indicador de cumplimiento de la exportación si se encuentra en un país que permite un cifrado seguro. Debe seleccionar esta opción ahora si planea utilizar esta funcionalidad. Si habilita esta funcionalidad más adelante, deberá volver a registrar su dispositivo con una nueva clave de producto y volver a cargar el dispositivo. Si no ve esta opción, su cuenta no es compatible con la funcionalidad de exportación controlada.

El token se agrega a su inventario.

d) Haga clic en el icono de la flecha hacia la derecha del token para abrir el cuadro de diálogo **Token** para poder copiar el ID del token en el portapapeles. Deje este token preparado para usarlo más adelante en el procedimiento cuando necesite registrar el Protección frente a amenazas.

Figura 28: Ver token

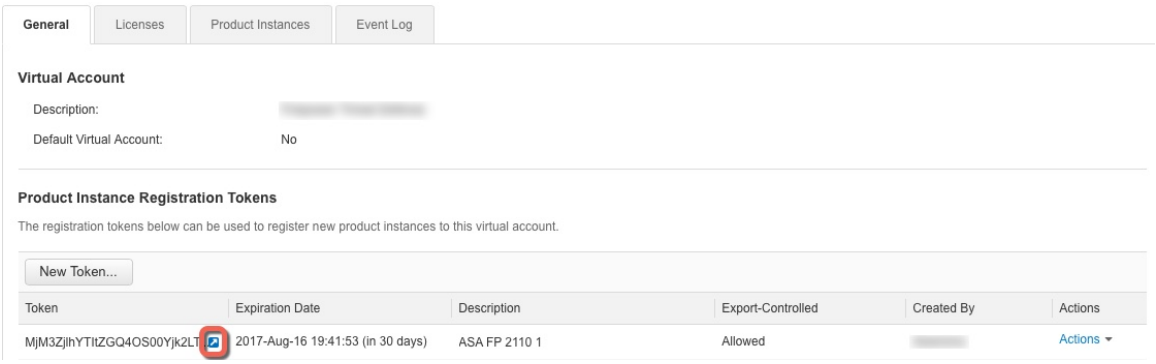
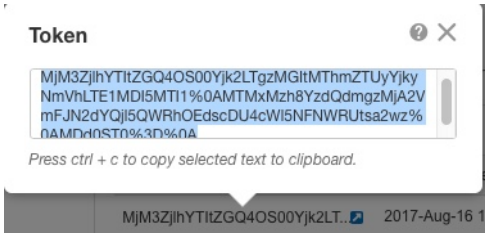


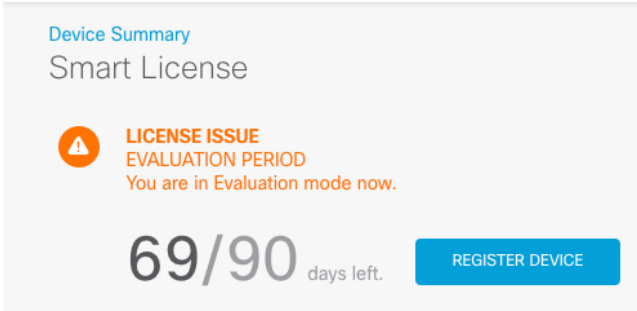
Figura 29: Copiar token



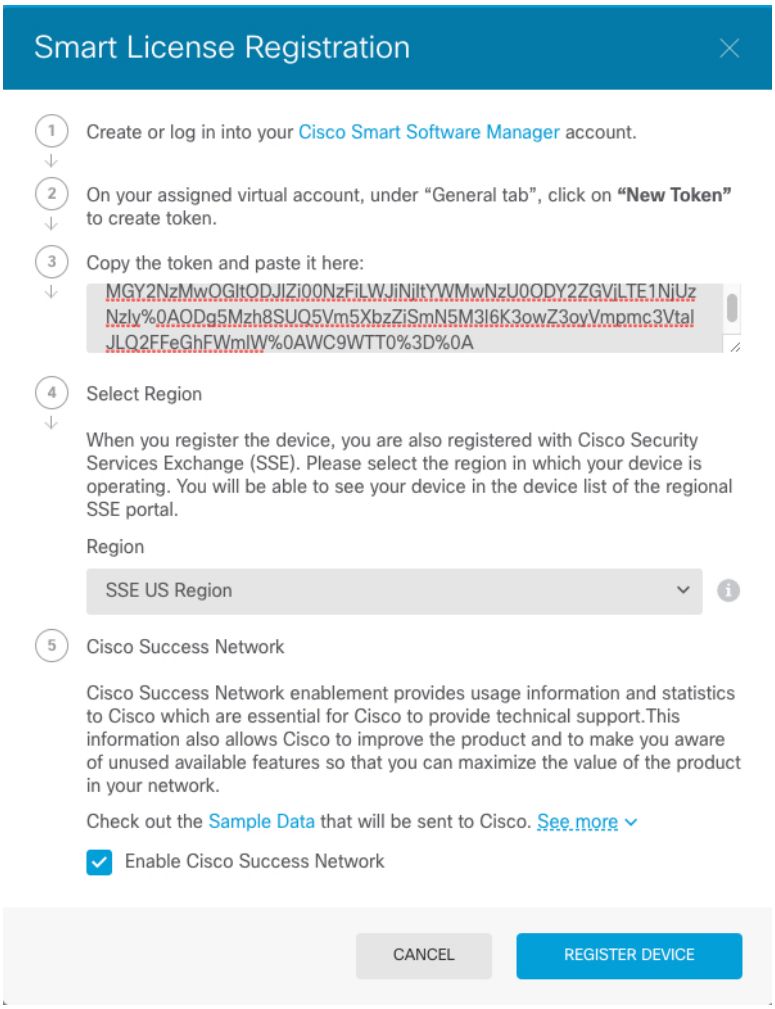
Paso 3 En el Administrador del dispositivo, haga clic en **Dispositivo** y, a continuación, en el resumen de **licencias Smart**, haga clic en **Ver configuración**.

Verá la página de **licencias Smart**.

Paso 4 Haga clic en **Registrar dispositivo**.

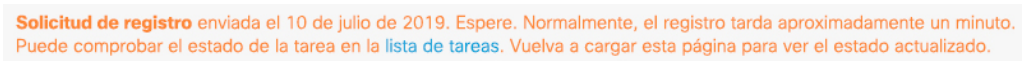


A continuación, siga las instrucciones del cuadro de diálogo **Registro de licencias Smart** para pegar el token:

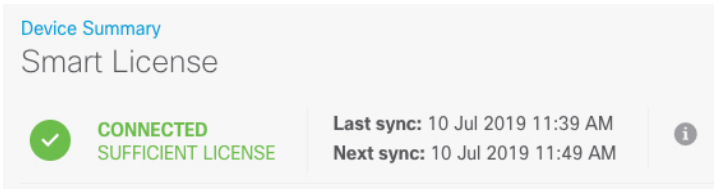


Paso 5 Haga clic en **Registrar dispositivo**.

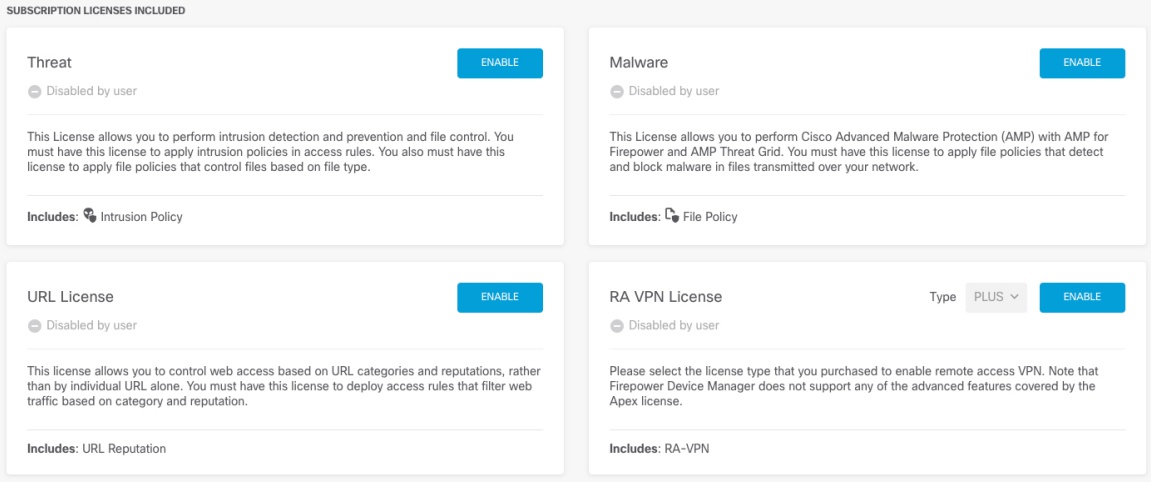
Vuelva a la página **licencias Smart**. Mientras el dispositivo se registra, verá el siguiente mensaje:



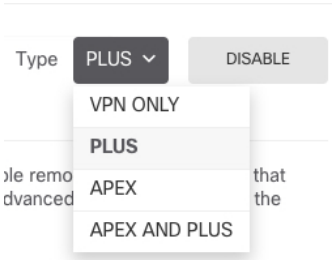
Después de que el dispositivo se registre correctamente y actualice la página, verá lo siguiente:



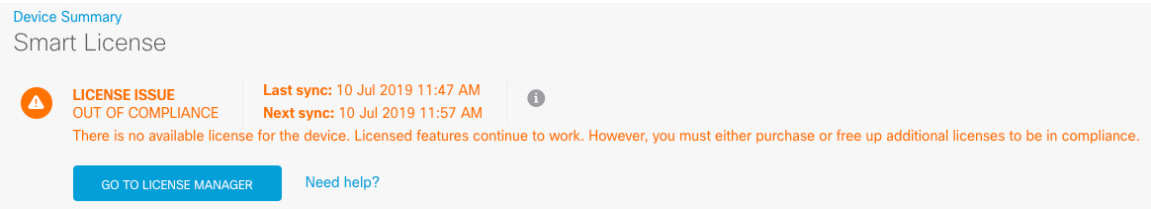
Paso 6 Haga clic en el control **Activar/Desactivar** de cada licencia opcional como prefiera.



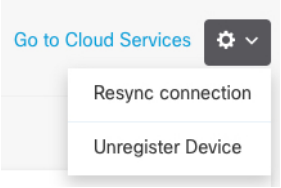
- **Activar**: registra la licencia con su cuenta de Cisco Smart Software Manager y activa las funciones controladas. Ahora puede configurar e implementar políticas controladas por la licencia.
- **Desactivar**: anula el registro de la licencia con su cuenta de Cisco Smart Software Manager y desactiva las funciones controladas. No puede configurar las características en nuevas políticas, ni puede implementar políticas que utilicen la función.
- Si activó la licencia **VPN con RA**, seleccione el tipo de licencia que desea usar: **Plus**, **Apex**, **Solo VPN** o **Plus y Apex**.



Después de activar las funciones, si no tiene las licencias en su cuenta, verá el siguiente mensaje de incumplimiento después de actualizar la página:



Paso 7 Seleccione **Resincronizar conexión** de la lista desplegable del equipo para sincronizar la información de la licencia con Cisco Smart Software Manager.



Configurar el firewall en Administrador del dispositivo

Los siguientes pasos son una descripción general de otras características que puede configurar. Haga clic en el botón de ayuda (**?**) de una página para obtener información detallada sobre cada paso.

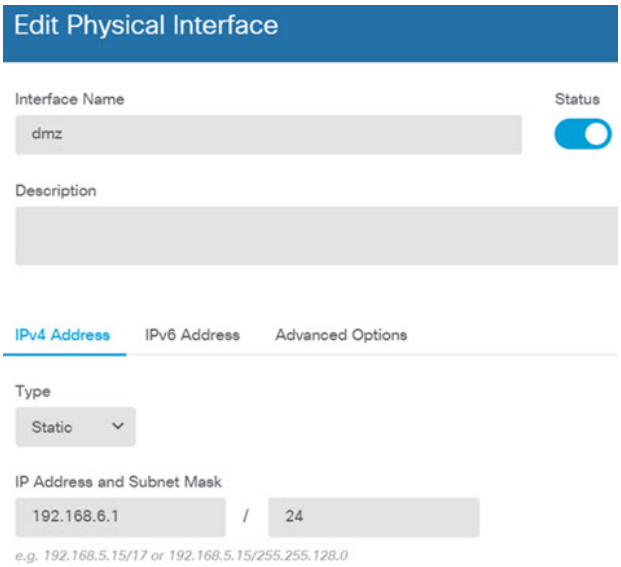
Procedimiento

Paso 1 Si desea convertir una interfaz de grupo de puente (6.4) que desea convertir un puerto de switch a una interfaz de firewall (6.5 y posterior), seleccione **Dispositivo** y haga clic en el enlace del resumen de **interfaces**.

Haga clic en el icono de edición ( ) de cada interfaz para configurar el modo y definir la dirección IP y otros ajustes.

En el siguiente ejemplo se configura una interfaz para usarla como una "zona desmilitarizada" (DMZ), donde se colocan activos accesibles públicamente como su servidor web. Haga clic en **Guardar** cuando haya terminado.

Figura 30: Editar interfaz



Paso 2 Si ha configurado nuevas interfaces, seleccione **Objetos** y, a continuación, **Zonas de seguridad** del índice.

Editar o crear nuevas zonas según corresponda. Cada interfaz debe pertenecer a una zona, ya que configura políticas basadas en zonas de seguridad, no en interfaces. No puede colocar las interfaces en zonas al

configurarlas, por lo que siempre debe editar los objetos de zona después de crear nuevas interfaces o cambiar el objetivo de las interfaces ya existentes.

El siguiente ejemplo muestra cómo crear una nueva zona dmz para la interfaz dmz.

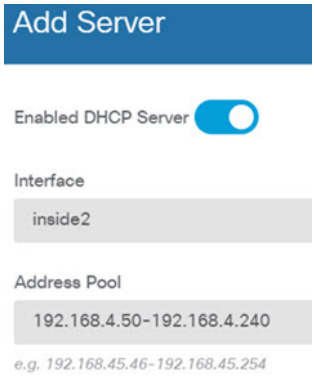
Figura 31: Objeto de zona de seguridad

Paso 3 Si desea que los clientes internos utilicen DHCP para obtener una dirección IP del dispositivo, seleccione **Dispositivo** > **Configuración del sistema** > **servidor DHCP** y, a continuación, seleccione la pestaña **Servidores DHCP**.

Ya hay un servidor DHCP configurado para la interfaz interna, pero puede editar el conjunto de direcciones o incluso eliminarlo. Si ha configurado otras interfaces internas, es muy habitual configurar un servidor DHCP en esas interfaces. Haga clic en + para configurar el servidor y el conjunto de direcciones para cada interfaz interna.

También puede ajustar con precisión la lista de WINS y DNS proporcionada a los clientes en la pestaña **Configuración**. El siguiente ejemplo muestra cómo configurar un servidor DHCP en la interfaz inside2 con el conjunto de direcciones 192.168.4.50-192.168.4.240.

Figura 32: Servidor DHCP



Paso 4 Seleccione **Dispositivo**, haga clic en **Ver configuración** (o **Crear primera ruta estática**) en el grupo **Rutas** y configure una ruta predeterminada.

La ruta predeterminada suele señalar hacia el router ascendente o ISP que reside fuera de la interfaz externa. Una ruta IPv4 predeterminada es para any-ipv4 (0.0.0.0/0), mientras que una ruta IPv6 predeterminada es

para any-ipv6 (::0/0). Cree rutas para cada versión de IP que utilice. Si utiliza DHCP para obtener una dirección para la interfaz externa, es posible que ya tenga las rutas predeterminadas que necesita.

Nota Las rutas que defina en esta página son solo para las interfaces de datos. No afectan a la interfaz de gestión. Establezca el gateway de administración en **Dispositivo** > **Ajustes del sistema** > **Interfaz de gestión**.

En el siguiente ejemplo se muestra una ruta predeterminada para IPv4. En este ejemplo, el isp-gateway es un objeto de red que identifica la dirección IP del gateway del ISP (debe obtener la dirección de su ISP). Puede crear este objeto haciendo clic en **Crear nueva red** en la parte inferior de la lista desplegable **Gateway**.

Figura 33: Ruta predeterminada

Paso 5 Seleccione **Políticas** y configure las políticas de seguridad para la red.

El asistente de configuración del dispositivo activa el flujo de tráfico entre la zona interior y la zona exterior, y la interfaz NAT entre todas las interfaces cuando se dirige a la interfaz exterior. Incluso al configurar nuevas interfaces, si las agrega al objeto dentro de la zona, la regla de control de acceso se aplica automáticamente a ellas.

Sin embargo, si tiene varias interfaces internas, necesita una regla de control de acceso para permitir que el tráfico fluya entre la zona interior. Si agrega otras zonas de seguridad, necesita reglas para permitir el tráfico entrante y saliente para esas zonas. Estos serían los cambios mínimos.

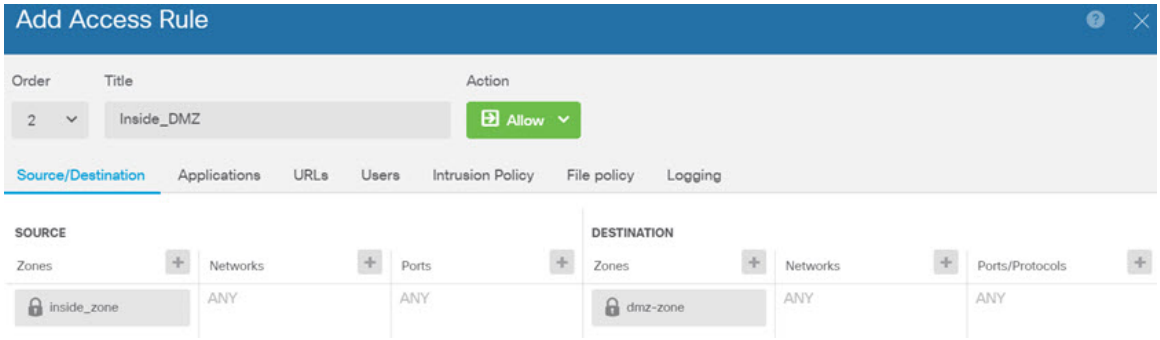
Además, puede configurar otras políticas para proporcionar servicios adicionales y ajustar con precisión las reglas de acceso y NAT para obtener los resultados que su organización necesita. Puede configurar las siguientes políticas:

- **Descifrado de SSL**: si desea inspeccionar las conexiones cifradas (como HTTPS) para detectar intrusiones, malware, etc., debe descifrar las conexiones. Utilice la política de descifrado SSL para determinar qué conexiones deben descifrarse. El sistema vuelve a cifrar la conexión después de inspeccionarla.
- **Identidad**: si desea relacionar la actividad de la red con usuarios individuales o controlar el acceso a la red en función de pertenecer a un grupo de usuarios o por usuario, utilice la política de identidad para determinar el usuario asociado a una dirección IP de origen.

- **Inteligencia de seguridad**: utilice la política de inteligencia de seguridad para desconectar rápidamente las conexiones con las direcciones IP o URL de la lista negra. Al incluir en la lista negra los sitios maliciosos conocidos, no es necesario que los tenga en cuenta en su política de control de acceso. Cisco proporciona información actualizada sobre direcciones y URL maliciosas conocidas para que la lista negra de inteligencia de seguridad se actualice continuamente. Con la fuente, no es necesario editar la política para agregar o eliminar elementos de la lista negra.
- **NAT (traducción de direcciones de red)**: utilice la política de NAT para convertir direcciones IP internas en direcciones enrutables externas.
- **Control de acceso**: utilice la política de control de acceso para determinar las conexiones que estarán permitidas en la red. Se puede filtrar por zona de seguridad, dirección IP, protocolo, puerto, aplicación, URL, usuario o grupo de usuarios. También aplica políticas de intrusión y archivos (malware) mediante reglas de control de acceso. Utilice esta política para implementar los filtros de URL.
- **Intrusión**: utilice las políticas de intrusión para inspeccionar las amenazas conocidas. Aunque aplique políticas de intrusión mediante reglas de control de acceso, puede editar las políticas de intrusión para activar o desactivar de forma selectiva ciertas reglas de intrusión.

El siguiente ejemplo muestra cómo permitir el tráfico entre la zona interior y la zona dmz en la política de control de acceso. En este ejemplo, no hay opciones configuradas en ninguna de las otras pestañas, excepto en **Registro**, que está seleccionado **Al final de la conexión**.

Figura 34: Política de control de acceso



Paso 6 Seleccione **Dispositivo**, haga clic en **Ver configuración** en el grupo **Actualizaciones** y configure los horarios de actualización para las bases de datos del sistema.

Si utiliza políticas de intrusión, configure actualizaciones periódicas para las reglas y las bases de datos de VDB. Si utiliza las fuentes de inteligencia de seguridad, establezca un horario de actualizaciones . Si utiliza la geolocalización en alguna política de seguridad como criterio coincidente, programe las actualizaciones para esa base de datos.

Paso 7 Haga clic en el botón **Implementar** del menú y, a continuación, haga clic en el botón Implementar ahora ( ) para implementar los cambios en el dispositivo.

Los cambios no estarán activos en el dispositivo hasta que los implemente.

Acceder a la Protección frente a amenazas y a la CLI de FXOS

Utilice la interfaz de línea de comandos (CLI) para configurar el sistema y solucionar los problemas básicos. No puede configurar políticas a través de una sesión de CLI. Puede acceder a la CLI conectándose al puerto de consola.

También puede acceder a CLI de FXOS para solucionar problemas

Nota Como alternativa, puede utilizar SSH para la interfaz de administración del dispositivo Protección frente a amenazas. A diferencia de una sesión de consola, la sesión SSH se establece de forma predeterminada en la CLI de Protección frente a amenazas, desde la que puede conectarse a CLI de FXOS mediante el comando **connect fxos**. Puede conectarse después a la dirección en una interfaz de datos si abre esa interfaz para las conexiones SSH. El acceso SSH para las interfaces de datos está desactivado de forma predeterminada. Este procedimiento describe el acceso al puerto de consola, cuyo valor predeterminado es CLI de FXOS.

Procedimiento

Paso 1 Para iniciar sesión en la CLI, conecte su ordenador de gestión al puerto de consola. Firepower 1000 va con un cable de serie USB A a B. Instale las unidades USB de serie necesarias para su sistema operativo (consulte la guía de hardware de Firepower 1010). El puerto de consola de forma predeterminada es CLI de FXOS. Utilice la siguiente configuración de serie:

- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada

Se conecta a la CLI de FXOS. Inicie sesión en la CLI con el nombre de usuario **admin** y la contraseña que estableció en la configuración inicial (la predeterminada es **Admin123**).

Ejemplo:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Paso 2 Acceda a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Después de iniciar sesión, para obtener información sobre los comandos disponibles en la CLI, introduzca **help** o **?**. Para obtener información sobre cómo utilizarla, consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Paso 3 Para abandonar la CLI de Protección frente a amenazas, introduzca el comando **exit** o **logout**.

Este comando le devuelve al mensaje de CLI de FXOS. Para obtener información sobre los comandos disponibles en la CLI de FXOS, introduzca **?**.

Ejemplo:

```
> exit
firepower#
```

Ver la información de hardware

Utilice la interfaz de línea de comandos (CLI) para ver la información sobre su hardware, incluido el modelo de dispositivo, la versión de hardware, el número de serie y los componentes del chasis, incluidas las fuentes de alimentación y los módulos de red. Puede acceder a la CLI conectándose al puerto de la consola; consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 114.

Procedimiento

Paso 1 Para mostrar el modelo de hardware del dispositivo, utilice el comando **show model**.

>**show model**

Ejemplo:

```
> show model
Cisco Firepower 1010 Threat Defense
```

Paso 2 Para mostrar el número de serie del chasis, utilice el comando **show serial-number**.

>**show serial-number**

Ejemplo:

```
> show serial-number
JMX1943408S
```

Esta información también se muestra en el resultado **show version system**, **show running-config** y **show inventory**.

Paso 3 Para mostrar información sobre todos los productos de Cisco instalados en el dispositivo de red a los que se ha asignado un identificador de producto (PID), un identificador de versión (VID) y un número de serie (SN), utilice el comando **show inventory**.

>**show inventory**

a) Desde la CLI de Protección frente a amenazas:

Ejemplo:

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) Desde la CLI de FXOS:

Ejemplo:

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

Apagar el firewall

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su sistema de firewall.

El chasis de Firepower 1010 no cuenta con un interruptor de alimentación externo.Puede apagar el firewall con Administrador del dispositivo, o puede utilizar la CLI de FXOS.

Desactive el firewall mediante Administrador del dispositivo

Puede apagar el sistema correctamente con Administrador del dispositivo.

Procedimiento

Paso 1 Utilice Administrador del dispositivo para apagar el firewall.

Nota Para la versión 6.4 y anteriores, introduzca el comando **shutdown** en la CLI de Administrador del dispositivo.

a) Haga clic en **Dispositivo** y, a continuación, en el enlace **Configuración del sistema** > **Reiniciar/Apagar**.
b) Haga clic en **Apagar**.

Paso 2 Si tiene una conexión de consola al firewall, monitorice los mensajes del sistema una vez que este se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si no tiene una conexión de consola, espere aproximadamente 3 minutos para asegurarse de que el sistema se ha apagado.

Paso 3 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

Apagar el dispositivo en la CLI

Puede utilizar la CLI de FXOS para apagar el sistema de forma segura y apagar el dispositivo. Se accede a la CLI conectándose al puerto de la consola; consulte Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 114.

Procedimiento

Paso 1 En el CLI de FXOS, conéctese a local-mgmt:

firepower # **connect local-mgmt**

Paso 2 Ejecute el comando **shutdown**:

firepower(local-mgmt) # **shutdown**

Ejemplo:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Paso 3 Supervise las indicaciones del sistema cuando el firewall se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Paso 4 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

¿Qué es lo siguiente que debe hacer?

Para continuar con la configuración del Protección frente a amenazas, consulte los documentos disponibles para su versión de software en Navegación por la documentación de Cisco Firepower.

Para obtener información relacionada con el uso de Administrador del dispositivo, consulte Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager.

¿Qué es lo siguiente que debe hacer?

CAPÍTULO 5

Implementación de Protección frente a amenazas con CDO

¿Este capítulo es para usted?

Para ver todos los sistemas operativos y administradores disponibles, consulte ¿Qué aplicación y administrador son adecuados para usted?, en la página 1. Este capítulo se aplica al Protección frente a amenazas que utiliza el Cisco Secure Firewall Management Center en la nube de Cisco Defense Orchestrator (CDO). Para utilizar CDO con la funcionalidad de Administrador del dispositivo, consulte la documentación de CDO.

Nota Centro de administración en la nube es compatible con Protección frente a amenazas 7.2 y posterior. En versiones anteriores, puede utilizar la funcionalidad de Administrador del dispositivo de CDO.

Cada Protección frente a amenazas controla, inspecciona, monitoriza y analiza el tráfico. CDO proporciona una consola de administración centralizada con una interfaz web que puede utilizar para realizar tareas administrativas y de administración en servicio para proteger su red local.

Sobre el firewall

El hardware puede ejecutar el software Protección frente a amenazas o el software ASA. Para cambiar entre Protección frente a amenazas y ASA es necesario que vuelva a crear una imagen para el dispositivo. También es necesario que lleve a cabo una una recreación de imagen si necesita una versión de software diferente a la instalada. Consulte Recreación de la imagen del dispositivo de defensa contra amenazas de Firepower o ASA de Cisco.

El firewall ejecuta un sistema operativo subyacente llamado Cisco Secure Firewall Extensible Operating System (FXOS). El firewall no es compatible con el Administrador del chasis Cisco Secure Firewall de FXOS; solo se admite una CLI limitada para la resolución de problemas. Consulte Guía de resolución de problemas de Cisco FXOS para Firepower 1000/2100 Series que ejecuta Firepower Threat Defense para obtener más información.

Declaración de recopilación de privacidad: el firewall no necesita ni recopila de forma activa información de identificación personal. Sin embargo, puede utilizar información de identificación personal en la configuración, por ejemplo, para los nombres de usuario. En este caso, un administrador podrá ver esta información cuando trabaje con la configuración o cuando utilice SNMP.

Acerca de la administración de Protección frente a amenazas de CDO

Cisco Secure Firewall Management Center en la nube

La Centro de administración en la nube ofrece muchas de las mismas funciones que los Centro de administración locales, se siente igual y tiene el mismo aspecto. Cuando utiliza CDO como administrador principal, puede utilizar un Centro de administración local solo para el análisis. El Centro de administración local no es compatible con la configuraciones de política ni las actualizaciones.

Métodos de incorporación de CDO

Puede incorporar un dispositivo de las siguientes maneras:

- Aprovisionamiento sin apenas intervención con el número de serie:
  - Un administrador de la sede central envía el Protección frente a amenazas a la sucursal remota. No se necesita una configuración previa. De hecho, no debe configurar nada en el dispositivo, ya que el aprovisionamiento sin apenas intervención no funciona con dispositivos preconfigurados.

Nota El administrador central puede registrar previamente el Protección frente a amenazas en CDO utilizando el número de serie del Protección frente a amenazas antes de enviar el dispositivo a la sucursal.

  - El administrador de la sucursal conecta y enciende el Protección frente a amenazas.
  - El administrador central completa la configuración del Protección frente a amenazas mediante CDO.

  También puede incorporarlo con un número de serie utilizando el Administrador del dispositivo si ya ha empezado con la configuración del dispositivo, aunque ese método no se trate en esta guía.

- Asistente de incorporación con el registro en la CLI: utilice este método manual si necesita realizar cualquier configuración previa o si está utilizando una interfaz de administrador que no es compatible con el aprovisionamiento sin apenas intervención.

Interfaz de acceso al administrador Protección frente a amenazas

Puede utilizar la interfaz de administración o la interfaz externa para el acceso al administrador. Sin embargo, esta guía incluye el acceso a la interfaz externa. El aprovisionamiento sin apenas intervención solo es compatible con la interfaz externa.

La interfaz de administración es una interfaz especial configurada por separado de las interfaces de datos de Protección frente a amenazas y tiene su propia configuración de red. Los ajustes de red de la interfaz de administración se siguen usando aunque active el acceso al administrador en una interfaz de datos. Todo el tráfico de administración viene o va desde la interfaz de gestión. Cuando se habilita el acceso al administrador en una interfaz de datos, el Protección frente a amenazas reenvía el tráfico de administración entrante por la placa base a la interfaz de administración. Para el tráfico de gestión saliente, la interfaz de gestión lo reenvía por la placa base a la interfaz de datos.

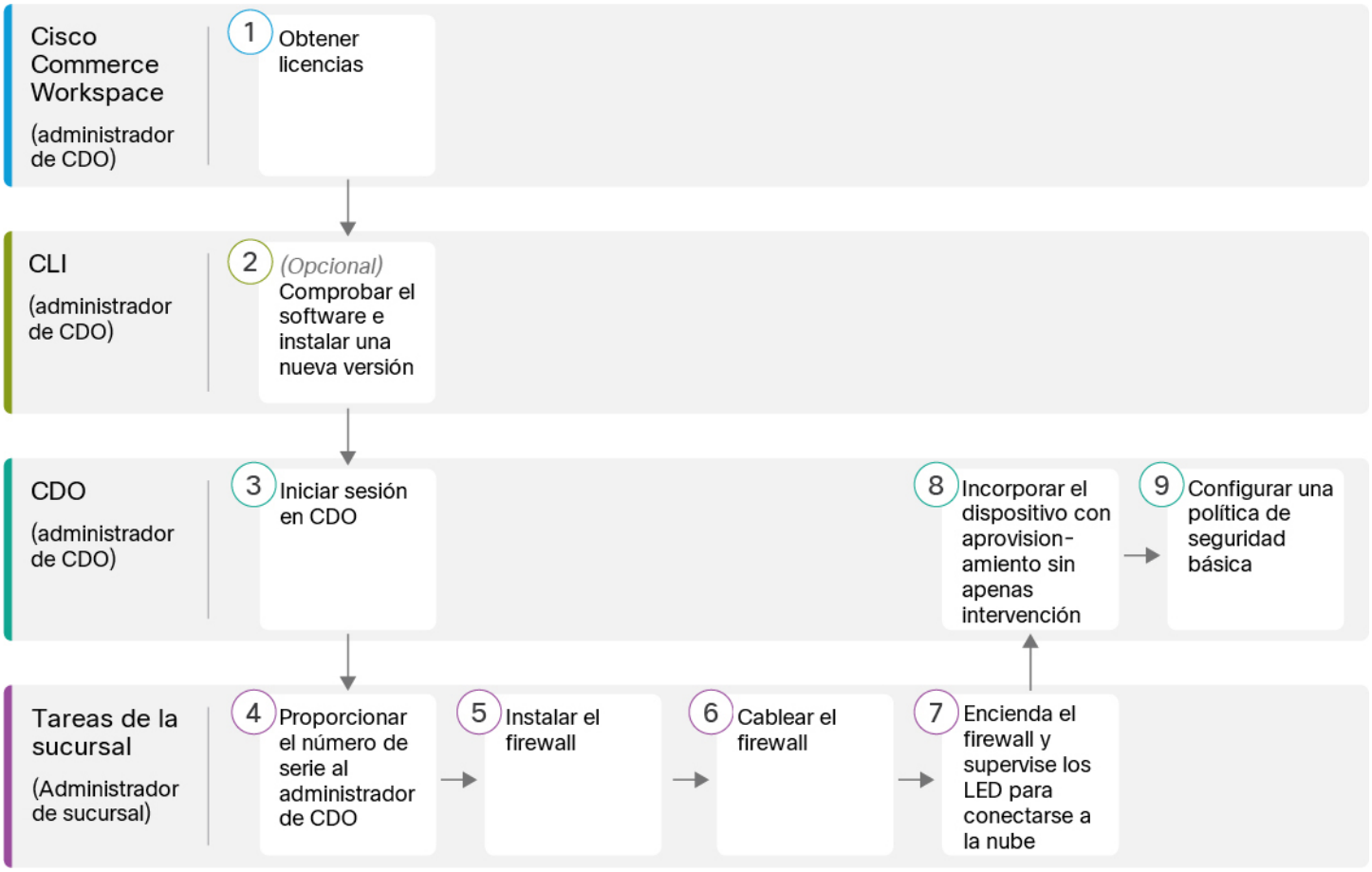
Acceder al administrador desde una interfaz de datos tiene las siguientes limitaciones:

- Solo puede habilitar el acceso al administrador en una sola interfaz de datos física. No puede utilizar una subinterfaz o un EtherChannel.
- Esta interfaz no puede ser solo de administración.
- Solo modo de firewall enrutado, mediante una interfaz enrutada.
- PPPoE no es compatible. Si su ISP requiere PPPoE, deberá colocar un router compatible con PPPoE entre la Protección frente a amenazas y el módem WAN.
- La interfaz debe estar solo en el VRF global.
- SSH no está activado de forma predeterminada para las interfaces de datos, por lo que deberá habilitar SSH más adelante con el Centro de administración. Como la gateway de la interfaz de gestión se cambiará para que sean las interfaces de datos, tampoco puede utilizar SSH para la interfaz de gestión desde una red remota a menos que agregue una ruta estática para ella mediante el comando **configure network static-routes**.

Procedimiento completo: aprovisionamiento sin apenas intervención

Consulte las siguientes tareas para implementar Protección frente a amenazas con CDO mediante el aprovisionamiento sin apenas intervención.

Figura 35: Procedimiento completo: aprovisionamiento sin apenas intervención



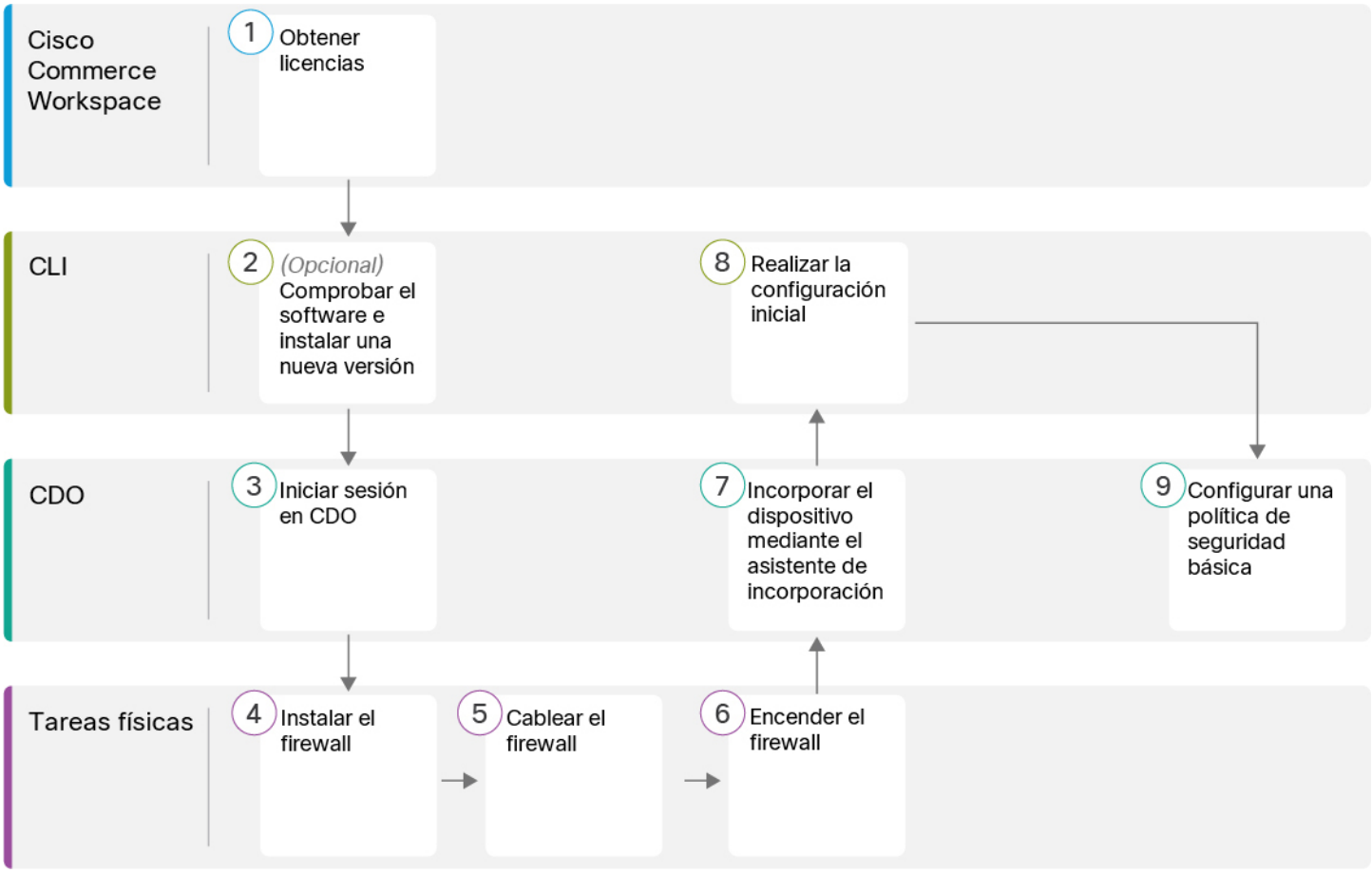
1	Cisco Commerce Workspace (Administrador de CDO)	Obtener licencias, en la página 125.
2	CLI (Administrador de CDO)	(Opcional) Comprobar el software e instalar una nueva versión, en la página 126.
3	CDO (Administrador de CDO)	Iniciar sesión en CDO, en la página 128.
4	Tareas de la sucursal (Administrador de sucursal)	Proporcione el número de serie del firewall al administrador central, en la página 132.

5	Tareas de la sucursal (Administrador de sucursal)	Instale el firewall. Consulte la guía de instalación del hardware.
6	Tareas de la sucursal (Administrador de sucursal)	Cablear el firewall, en la página 133.
7	Tareas de la sucursal (Administrador de sucursal)	Encienda el firewall, en la página 134.
8	CDO (Administrador de CDO)	Incorpore un dispositivo con aprovisionamiento sin apenas intervención, en la página 135.
9	CDO (Administrador de CDO)	Configurar una norma de seguridad básica, en la página 150.

Procedimiento completo: asistente de incorporación

Consulte las siguientes tareas para incorporar el Protección frente a amenazas a CDO con el asistente de incorporación.

Figura 36: Procedimiento completo: asistente de incorporación



1	Cisco Commerce Workspace	Obtener licencias, en la página 125.
2	CLI	(Opcional) Comprobar el software e instalar una nueva versión, en la página 126.
3	CDO	Iniciar sesión en CDO, en la página 128.
4	Tareas físicas	Instale el firewall. Consulte la guía de instalación del hardware.
5	Tareas físicas	Cablear el firewall, en la página 136.
6	Tareas físicas	Encender el firewall, en la página 137.
7	CDO	Incorporar un dispositivo con el asistente de incorporación, en la página 138.

8	CLI o Administrador del dispositivo	• Lleve a cabo la configuración inicial con la CLI, en la página 140. • Realizar la configuración inicial con Administrador del dispositivo, en la página 144.
9	CDO	Configurar una norma de seguridad básica, en la página 150.

Configuración previa del administrador central

Esta sección describe cómo obtener licencias de funciones para su firewall; cómo instalar una nueva versión de software antes de implementarla; y cómo iniciar sesión en CDO.

Obtener licencias

CDO proporciona todas las licencias para el Protección frente a amenazas. Puede adquirir de forma opcional las siguientes licencias de funciones:

- **Amenazas**: inteligencia de seguridad e IPS de última generación
- **Malware**: protección frente al malware
- **URL**: filtrado de URL
- **VPN con RA**: AnyConnect Plus, AnyConnect Apex o AnyConnect solo VPN

Para obtener una descripción general más detallada sobre Cisco Licensing, visite cisco.com/go/licensingguide

Antes de empezar

- Tener una cuenta principal en Smart Software Manager.

  Si aún no tiene una cuenta, haga clic en el enlace para configurar una nueva cuenta. Smart Software Manager le permite crear una cuenta principal para su organización.

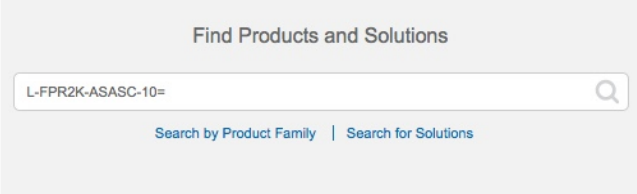
- Su cuenta de licencias de Smart Software debe cumplir los requisitos de la licencia de cifrado seguro (3DES/AES) para utilizar algunas funciones (que se activan mediante el indicador de cumplimiento de exportación).

Procedimiento

Paso 1 Compruebe que su cuenta de licencias Smart contenga las licencias disponibles que necesita.

Cuando adquirió su dispositivo en Cisco o en un distribuidor, sus licencias deberían haberse vinculado a su cuenta de licencias Smart Software. Sin embargo, si necesita agregar licencias usted mismo, utilice el campo de búsqueda **Buscar productos y soluciones** en Cisco Commerce Workspace. Busque las siguientes PID de licencia:

Figura 37: Búsqueda de licencia



Nota Si no se encuentra una PID, puede agregarla manualmente a su pedido.

- Combinación de licencias de amenazas, malware y URL:
  - L-FPR1010T-TMC=

  Cuando agregue una de las PID anteriores a su pedido, podrá elegir una suscripción basada en el plazo correspondiente a una de las siguientes PID:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN con RA: consulte la Guía de pedidos de Cisco AnyConnect.

Paso 2 Si todavía no lo ha hecho, registre CDO con Smart Software Manager.

Para registrarse, es necesario que genere un token de registro en Smart Software Manager. Consulte la documentación de CDO para obtener instrucciones detalladas.

(Opcional) Comprobar el software e instalar una nueva versión

Para comprobar la versión del software e instalar una versión diferente, si es necesario, siga estos pasos. Le recomendamos que instale su versión de destino antes de configurar el firewall. Como alternativa, puede realizar una actualización una vez que esté en funcionamiento, pero la actualización, que conserva su configuración, puede llevar más tiempo que este procedimiento.

¿Qué versión debo ejecutar?

Cisco recomienda ejecutar una versión Gold Star indicada con una estrella dorada junto al número de versión en la página de descarga de software. También puede consultar la estrategia de versiones descrita en https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; Por ejemplo, este boletín describe la numeración de las versiones a corto plazo (con las características más recientes), la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para un período de tiempo más largo) o la numeración de las versiones a largo plazo (versiones de mantenimiento y parches para el período de tiempo más largo, para la certificación del gobierno).

Antes de empezar

En el aprovisionamiento sin apenas intervención, si inicia sesión y después cambia la contraseña, desactiva el proceso de aprovisionamiento sin apenas intervención. Solo debe iniciar sesión y completar una nueva

imagen si ya sabe que necesita cambiar la versión del software. Si ha iniciado sesión y desea restaurar la capacidad de aprovisionamiento sin apenas intervención sin instalar software, puede llevar a cabo una restauración de fábrica. Consulte la guía de resolución de problemas de FXOS.

Procedimiento

Paso 1 Encienda el firewall y conéctese al puerto de consola. Consulte Encender el firewall, en la página 137 y Acceder a la Protección frente a amenazas y a la CLI de FXOS, en la página 161 para obtener más información.

Inicie sesión con el usuario **administrador** y la contraseña predeterminada **Admin123**.

Se conecta a la CLI de FXOS. La primera vez que inicie sesión, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si ya se cambió la contraseña, y no lo sabe, debe llevar a cabo una restauración de fábrica para recuperar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el Procedimiento de restauración de fábrica.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 2 En la CLI de FXOS, muestre la versión en ejecución.

scope ssa

show app-instance

Ejemplo:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Paso 3 Si desea instalar una nueva versión, lleve a cabo estos pasos.

a) Si necesita establecer una dirección IP estática para la interfaz de administración, consulte Lleve a cabo la configuración inicial con la CLI, en la página 140. La interfaz de administración utiliza por defecto DHCP.

   Tendrá que descargar la nueva imagen de un servidor accesible desde la interfaz de administración.

b) Lleve a cabo el procedimiento de recrear la imagen que aparece en la guía de resolución de problemas de FXOS.

Paso 4 Parra el aprovisionamiento sin apenas intervención, *no inicie sesión en el firewall* tras la recreación de imagen; el inicio de sesión inicia la configuración inicial. El aprovisionamiento sin apenas intervención solo funciona en firewalls con instalaciones nuevas que no se han configurado.

Iniciar sesión en CDO

CDO utiliza Cisco Secure Sign-On como su proveedor de identidad y Duo Security para la autenticación multifactor (MFA). CDO requiere MFA, que proporciona una capa adicional de seguridad en la protección de su identidad de usuario. La autenticación de dos factores, un tipo de MFA, requiere dos componentes o factores, para garantizar la identidad del usuario que se conecta a CDO.

El primer factor es un nombre de usuario y una contraseña y el segundo es una contraseña de un solo uso (OTP) que se genera a petición de Duo Security.

Después de establecer sus credenciales de Cisco Secure Sign-On, puede iniciar sesión en CDO desde su panel de Cisco Secure Sign-On. Desde el panel de Cisco Secure Sign-On, también puede iniciar sesión en otros productos de Cisco compatibles.

- Si tiene una cuenta de Cisco Secure Sign-On, continúe a Iniciar sesión en CDO con el inicio de sesión seguro de Cisco, en la página 131.
- Si no tiene una cuenta de Cisco Secure Sign-On, continúe a Crear una nueva cuenta de inicio de sesión seguro de Cisco, en la página 128.

Crear una nueva cuenta de inicio de sesión seguro de Cisco

El flujo de trabajo de inicio de sesión inicial es un proceso de cuatro pasos. Debe completar los cuatro pasos.

Antes de empezar

- **Instale DUO Security**: le recomendamos que instale la aplicación Duo Security en un teléfono móvil. Revise la Guía de autenticación de dos factores de Duo: guía de inscripción si tiene preguntas sobre la instalación de Duo.
- **Sincronización de la hora**: va a utilizar su dispositivo móvil para generar una contraseña de un solo uso. Es importante que el reloj de su dispositivo se sincronice con la hora real ya que la OTP se basa en la hora. Asegúrese de que el reloj del dispositivo esté configurado a la hora correcta.
- Utilice una versión actualizada de Firefox o Chrome.

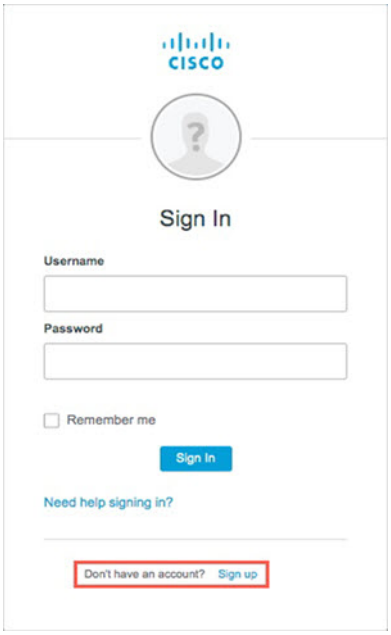
Procedimiento

Paso 1 **Regístrese para obtener una nueva cuenta de Cisco Secure Sign-On.**

a) Navegue a https://sign-on.security.cisco.com.

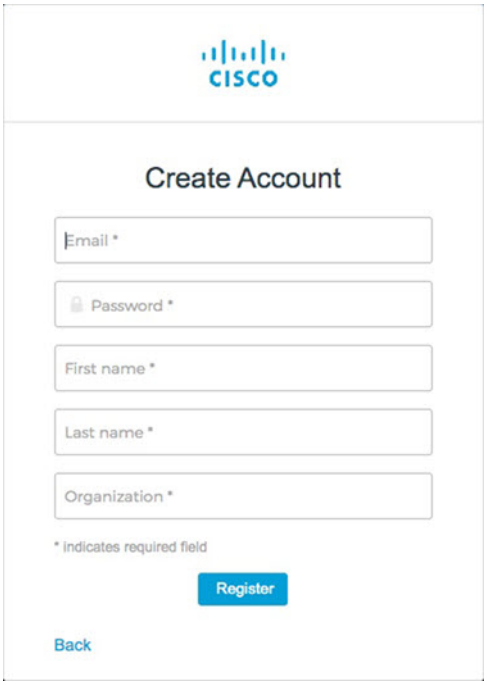
b) En la parte inferior de la pantalla de inicio de sesión, haga clic en **Registrarse**.

Figura 38: Inscripción en Cisco SSO



c) Rellene los campos del cuadro de diálogo **Crear cuenta** y haga clic en **Registrar**.

Figura 39: Crear cuenta



Consejo Introduzca la dirección de correo electrónico que piensa utilizar para iniciar sesión en CDO y añada un nombre de organización para representar a su empresa.

d) Después de hacer clic en **Registrar**, Cisco le envía un correo electrónico de verificación a la dirección con la que se registró. Abra el correo electrónico y haga clic en **Activar cuenta**.

Paso 2 **Configure la autenticación de varios factores con Duo.**

a) En la pantalla **Configurar autenticación de varios factores**, haga clic en **Configurar**.
b) Haga clic en **Iniciar configuración** y siga las indicaciones para elegir un dispositivo y verificar el emparejamiento de ese dispositivo con su cuenta.

Para obtener más información, consulte la Guía de autenticación de dos factores de Duo: guía de inscripción. Si ya tiene la aplicación Duo en su dispositivo, recibirá un código de activación de esta cuenta. Duo es compatible con varias cuentas en un solo dispositivo.

c) Al final del asistente, haga clic en **Continuar para iniciar sesión**.
d) Inicie sesión en Cisco Secure Sign-On con la autenticación de dos factores.

Paso 3 (Opcional) **Configure Google Authenticator como un autenticador adicional.**

a) Elija el dispositivo móvil que está vinculando con Google Authenticator y haga clic en **Siguiente**.
b) Siga las instrucciones del asistente de configuración para configurar Google Authenticator.

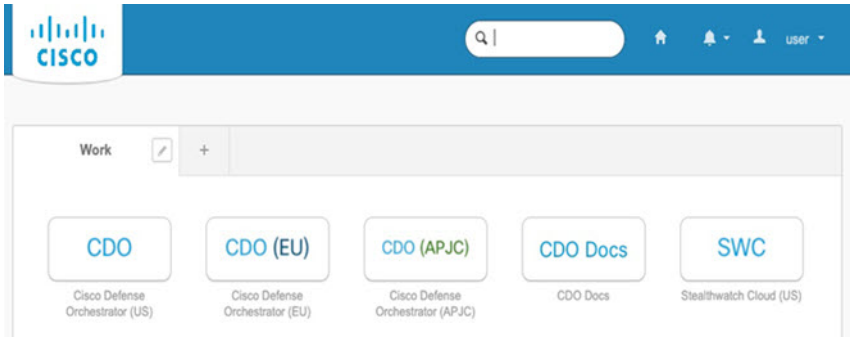
Paso 4 **Configure las opciones de recuperación de la cuenta de su cuenta de Cisco Secure Sign-On.**

a) Elija una pregunta y una respuesta de "contraseña olvidada".
b) Elija un número de teléfono de recuperación para restablecer su cuenta mediante SMS.
c) Elija una imagen de seguridad.
d) Haga clic en **Crear mi cuenta**.

Ahora verá el panel de Cisco Security Sign-On con los mosaicos de CDO. También puede ver otros mosaicos de aplicaciones.

Consejo Puede arrastrar los mosaicos por el panel para ordenarlos como desee, crear pestañas para agrupar mosaicos y cambiar el nombre de las pestañas.

Figura 40: Panel de Cisco SSO



Iniciar sesión en CDO con el inicio de sesión seguro de Cisco

Inicie sesión en CDO para incorporar y administrar su dispositivo.

Antes de empezar

Cisco Defense Orchestrator (CDO) utiliza Cisco Secure Sign-On como su proveedor de identidad y Duo Security para la autenticación multifactor (MFA).

- Para iniciar sesión en CDO, primero debe crear su cuenta en Cisco Secure Sign-On y configurar MFA con Duo; vea Crear una nueva cuenta de inicio de sesión seguro de Cisco, en la página 128.
- Utilice una versión actualizada de Firefox o Chrome.

Procedimiento

Paso 1 En un navegador web, vaya a https://sign-on.security.cisco.com/.

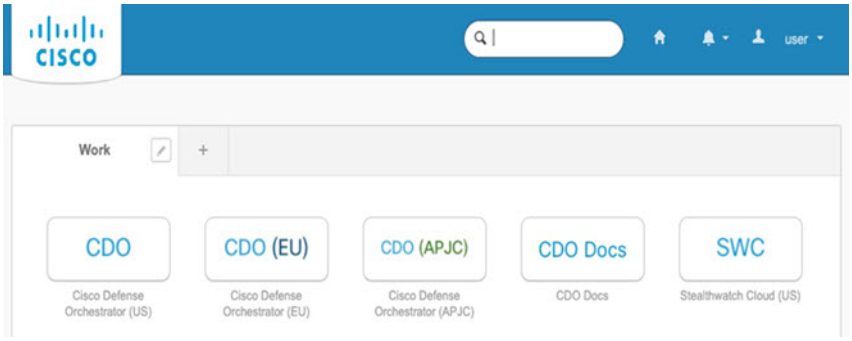
Paso 2 Introduzca su **Nombre de usuario** y **Contraseña**.

Paso 3 Haga clic en **Iniciar sesión**.

Paso 4 Reciba otro factor de autenticación con Duo Security y confirme su inicio de sesión. El sistema confirma su inicio de sesión y muestra el panel Cisco Secure Sign-On.

Paso 5 Haga clic en el mosaico de CDO correspondiente en el panel de Cisco Secure Sign-on. El mosaico de **CDO** le dirige a https://defenseorchestrator.com, el mosaico de **CDO (EU)** le dirige a https://defenseorchestrator.eu y el mosaico de **CDO (APJC)** le dirige a https://www.apj.cdo.cisco.com.

Figura 41: Panel de Cisco SSO



Paso 6 Haga clic en el logotipo del autenticador para elegir **Duo Security** o **Google Authenticator**, si ha configurado ambos autenticadores.

- Si ya tiene un registro de usuario en un arrendatario existente, ha iniciado sesión en ese arrendatario.
- Si ya tiene un registro de usuario en varios arrendatarios, podrá elegir a qué arrendatario de CDO conectarse.
- Si aún no tiene un registro de usuario de un arrendatario existente, podrá obtener más información sobre CDO o solicitar una cuenta de prueba.

Implementar el firewall con el aprovisionamiento sin apenas intervención

Después de que reciba el Protección frente a amenazas de la sede central, solo tiene que cablear y encender el firewall para que tenga acceso a Internet desde la interfaz externa. El administrador central puede completar la configuración.

Proporcione el número de serie del firewall al administrador central

Antes de instalar el firewall o desechar la caja de envío, anote el número de serie para que pueda coordinarse con el administrador central.

Procedimiento

Paso 1 Desembale el chasis y sus componentes.

Realice un inventario de su firewall y de su embalaje antes de conectar cualquier cable o de encender el firewall. También debe familiarizarse con el diseño del chasis, los componentes y los LED.

Paso 2 Registre el número de serie del firewall.

El número de serie del firewall se puede encontrar en la caja de envío. También se puede encontrar en una etiqueta en la parte inferior del chasis del firewall.

Paso 3 Envíe el número de serie del firewall al administrador de red CDO de su departamento de TI/sede central.

Su administrador de red necesita su número de serie del firewall para facilitar el aprovisionamiento sin apenas intervención, conectarse al firewall y configurarlo de forma remota.

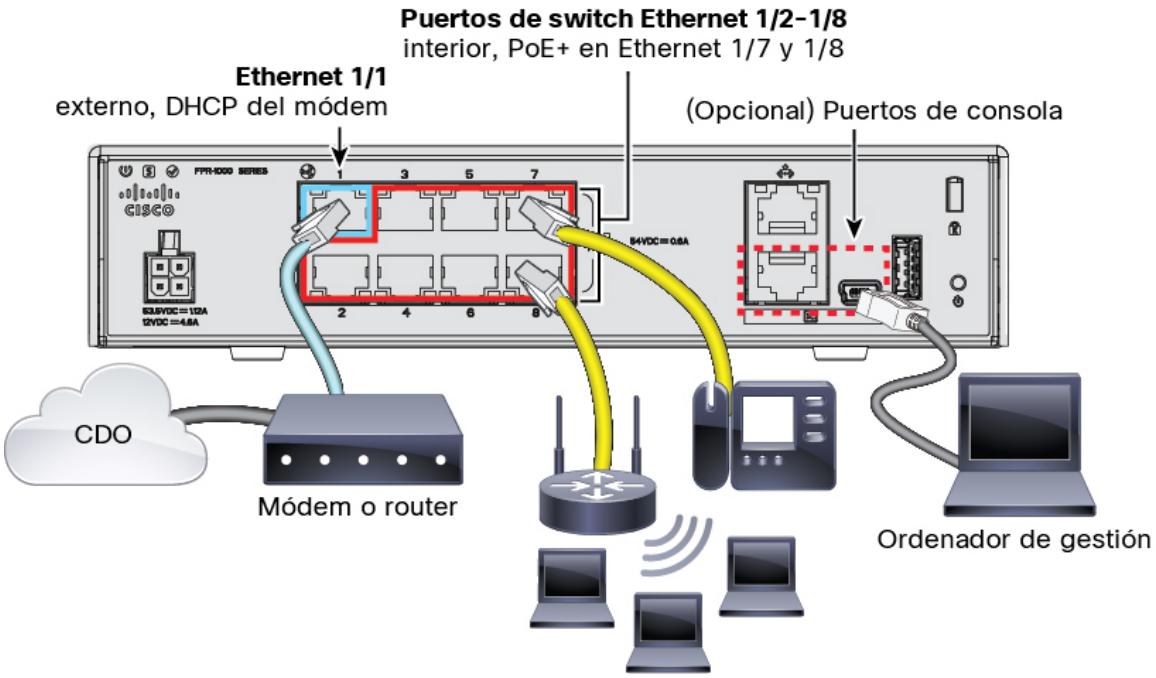
Comuníquese con el administrador de CDO para desarrollar una línea de tiempo de incorporación.

Cablear el firewall

En este tema se describe cómo conectar Firepower 1010 a su red para que se pueda administrar por CDO.

Si ha recibido un firewall en su sucursal y su tarea es conectarlo a la red, mire este vídeo. El vídeo describe su firewall y la secuencia de luces LED del firewall que indican su estado. Si lo necesita, podrá confirmar el estado del firewall con su departamento de TI con solo mirar los LED.

Figura 42: Cableado de Firepower 1010



El aprovisionamiento sin apenas intervención admite la conexión a CDO en Ethernet 1/1 (exterior).

Nota Ethernet 1/2 a 1/8 se configuran como puertos de switch de hardware; PoE+ también está disponible en Ethernet 1/7 y 1/8.

Procedimiento

Paso 1 Instale el chasis. Consulte la guía de instalación del hardware.

Paso 2 Conecte el cable de red de la interfaz Ethernet 1/1 al módem de red de área amplia (WAN). El módem WAN es la conexión de su sucursal a Internet y también será la ruta de su firewall a Internet.

Paso 3 Cablee los puntos finales internos a los puertos de switch, Ethernet1/2 a 1/8.

Ethernet 1/7 a 1/8 son puertos PoE+.

Paso 4 (Opcional) Conecte el ordenador de gestión al puerto de consola.

En la sucursal, no es necesaria la conexión de la consola para el uso diario; sin embargo, puede ser necesario para la resolución de problemas.

Encienda el firewall

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

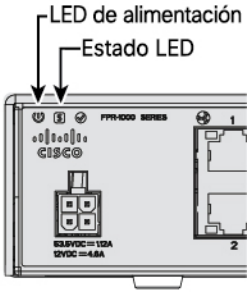
Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

Paso 4 Observe el LED de estado en la parte posterior o superior del dispositivo; cuando el dispositivo se inicia correctamente, el LED de estado parpadea rápidamente en verde.

Si hay un problema, el LED de estado parpadea rápidamente en ámbar. Si es el caso, llame a su departamento de TI.

Paso 5 Observe el LED de estado en la parte posterior o superior del dispositivo; cuando el dispositivo se conecta a la nube de Cisco, el LED de estado parpadea lentamente en verde.

Si hay un problema, el LED de estado parpadea en ámbar y verde y el dispositivo no se ha conectado a Cisco Cloud. Si esto sucede, compruebe que el cable de red esté conectado a la interfaz Ethernet 1/1 y al módem WAN. Si unos 10 minutos después de ajustar el cable de red, el dispositivo no consigue conectarse a la nube de Cisco, llame a su departamento de TI.

Qué hacer a continuación

- Póngase en contacto con su departamento de TI para confirmar el cronograma y las actividades de incorporación. Debe contar con un plan de comunicación con el administrador de CDO en su sede central.
- Después de completar esta tarea, el administrador de CDO podrá configurar y administrar el dispositivo en remoto. Eso es todo.

Incorpore un dispositivo con aprovisionamiento sin apenas intervención

Incorpore el Protección frente a amenazas mediante el aprovisionamiento sin apenas intervención y el número de serie del dispositivo.

Procedimiento

Paso 1 En el panel de navegación de CDO, haga clic en **Inventario** y, a continuación, presione el botón más azul (+) para **Incorporar** un dispositivo.

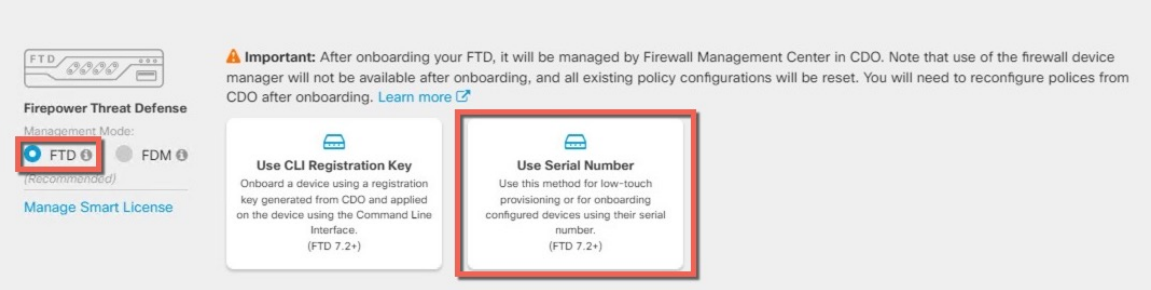
Paso 2 Seleccione la ficha **FTD**.

Paso 3 En el **Modo de administración**, asegúrese de que el **FTD** está seleccionado.

Puede hacer clic en **Administrar licencia Smart** en cualquier momento posterior a la selección del **FTD** como modo de administración para inscribirse en o modificar las licencias inteligentes existentes disponibles para su dispositivo. Consulte Obtener licencias, en la página 125 para ver qué licencias están disponibles.

Paso 4 Seleccione **Utilizar número de serie** como método de incorporación.

Figura 43: Utilizar número de serie



Paso 5 En el área **Conexión**, introduzca el **Número de serie del dispositivo** y el **Nombre del dispositivo** y, a continuación, haga clic en **Siguiente**.

Paso 6 En el área **Restablecer contraseña**, haga clic en el botón de selección **Sí, este dispositivo nunca se ha configurado o registrado para un administrador** y, a continuación, haga clic en **Siguiente**.

Paso 7 En la **Asignación de política**, utilice el menú desplegable para seleccionar una política de control de acceso para el dispositivo. Si no tiene ninguna política configurada, seleccione la **Política de control de acceso predeterminada**.

Paso 8 En la **Licencia de subscripción**, marque cada una de las licencias de funciones que desea activar. Haga clic en **Siguiente**.

Paso 9 (Opcional) Agregue etiquetas a su dispositivo para ayudar a filtrar y ordenar en la página **Inventario**. Introduzca una etiqueta y seleccione el botón azul de más (+). Las etiquetas se aplican al dispositivo una vez que se incorpora a CDO.

Qué hacer a continuación

Desde la página **Inventario**, seleccione el dispositivo que acaba de incorporar y seleccione cualquiera de las opciones que aparecen bajo el panel de **Administración** situado a la derecha.

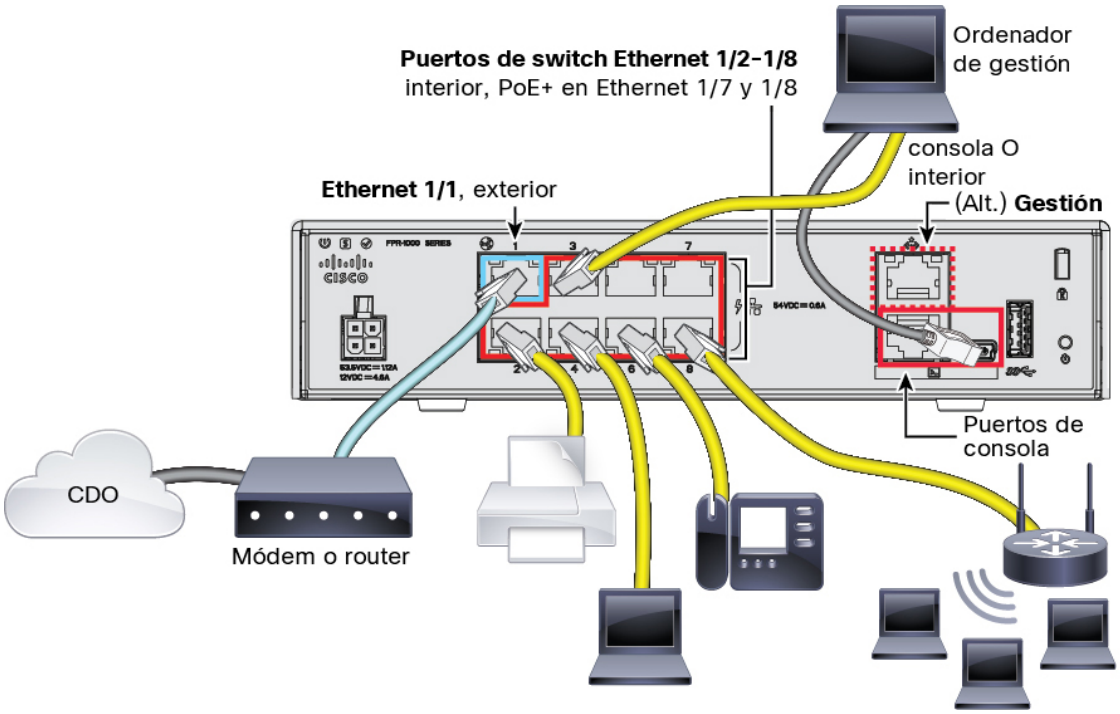
Implementar el firewall con el asistente de incorporación

Esta sección describe cómo configurar el firewall para su incorporación con el asistente de incorporación de CDO.

Cablear el firewall

En este tema se describe cómo conectar Firepower 1010 a su red para que se pueda administrar por CDO.

Figura 44: Cableado de Firepower 1010



Puede conectarse a CDO desde la interfaz externa o la interfaz de administración, según la interfaz que establezca para el acceso del administrador durante la configuración inicial. Esta guía muestra la interfaz externa.

Nota Ethernet 1/2 a 1/8 se configuran como puertos de switch de hardware; PoE+ también está disponible en Ethernet 1/7 y 1/8.

Procedimiento

Paso 1 Instale el chasis. Consulte la guía de instalación del hardware.

Paso 2 Conecte la interfaz externa (Ethernet 1/1) al router externo.

De manera alternativa, también puede utilizar la interfaz de administración para el acceso del administrador. Sin embargo, esta guía trata sobre todo el acceso a la interfaz externa, ya que es la situación más probable para las sucursales remotas.

Paso 3 Cablee los puntos finales internos a los puertos de switch, Ethernet1/2 a 1/8.

Ethernet 1/7 a 1/8 son puertos PoE+.

Paso 4 Conecte el ordenador de gestión al puerto de consola o a una interfaz interna.

Si realiza la configuración inicial mediante la CLI, deberá conectarse al puerto de consola. Puede que el puerto de consola también sea necesario para la resolución de problemas. Si realiza la configuración inicial con Administrador del dispositivo, conéctese a una interfaz interna.

Encender el firewall

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Antes de empezar

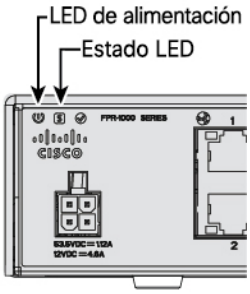
Es importante que proporcione una alimentación fiable para su dispositivo (con una fuente de alimentación ininterrumpida (UPS), por ejemplo). Si se pierde la fuente de alimentación sin apagar primero se pueden provocar daños graves en el sistema de archivos. Hay muchos procesos que se ejecutan en segundo plano todo el tiempo y, si se pierde la fuente de alimentación, el sistema no se puede apagar adecuadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

Incorporar un dispositivo con el asistente de incorporación

Incorpore el Protección frente a amenazas con el asistente de incorporación de CDO mediante una clave de registro de la CLI.

Procedimiento

Paso 1 En el panel de navegación de CDO, haga clic en **Inventario** y, a continuación, presione el botón más azul () para **Incorporar** un dispositivo.

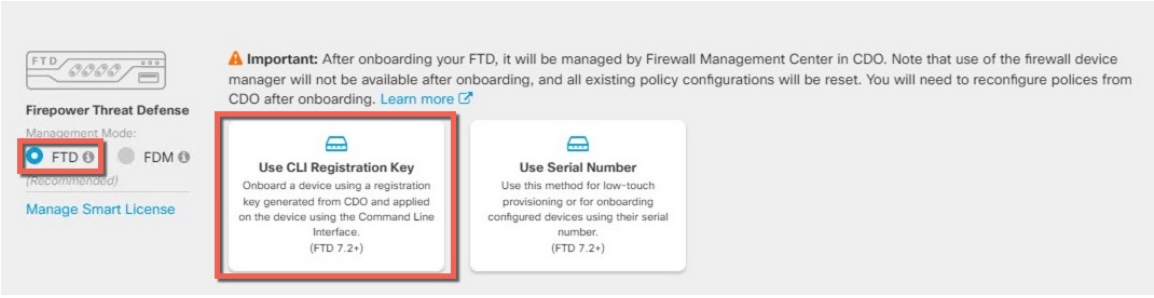
Paso 2 Seleccione la ficha **FTD**.

Paso 3 En el **Modo de administración**, asegúrese de que el **FTD** está seleccionado.

Puede hacer clic en **Administrar licencia Smart** en cualquier momento posterior a la selección del **FTD** como modo de administración para inscribirse en o modificar las licencias inteligentes existentes disponibles para su dispositivo. Consulte Obtener licencias, en la página 125 para ver qué licencias están disponibles.

Paso 4 Seleccione **Usar la clave de registro de la CLI** como método de incorporación.

Figura 45: Usar la clave de registro de la CLI



Paso 5 Introduzca el **Nombre del dispositivo** y haga clic en **Siguiente**.

Paso 6 En la **Asignación de política**, utilice el menú desplegable para seleccionar una política de control de acceso para el dispositivo. Si no tiene ninguna política configurada, seleccione la **Política de control de acceso predeterminada**.

Paso 7 En la **Licencia de subscripción**, haga clic en botón de selección del **Dispositivo FTD físico** y después revise cada una de las licencias de funciones que desea activar. Haga clic en **Siguiente**.

Paso 8 Para la **Clave de registro de la CLI**, CDO genera un comando con la clave de registro y otros parámetros. Debe copiar este comando y utilizarlo en la configuración inicial de Protección frente a amenazas.

configure manager add *cdo_hostname registration_key nat_id display_name*

Complete la configuración inicial en la CLI o con Administrador del dispositivo:

- Lleve a cabo la configuración inicial con la CLI, en la página 140: Copie este comando en la CLI de FTD después de completar el script de inicio.
- Realizar la configuración inicial con Administrador del dispositivo, en la página 144Copie las partes *cdo_hostname*, *registration_key* y *nat_id* del comando en los campos **Nombre de host/dirección IP del centro de administración/CDO**, **Clave de registro del centro de administración/CDO** e **ID de NAT**.

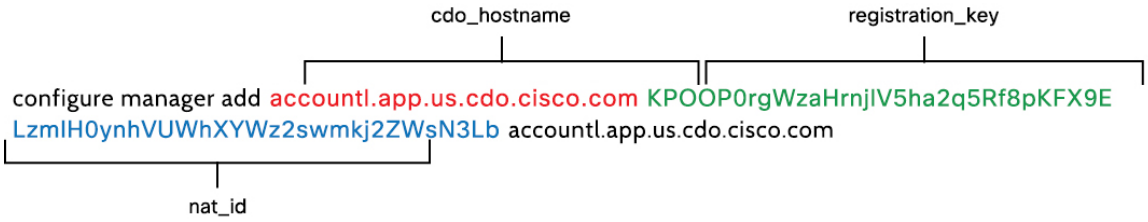
Ejemplo:

Comando de ejemplo para la configuración de CLI:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Componentes de comandos de muestra para la configuración de la GUI:

Figura 46: Configure el administrador de agregación de componentes de comandos



Paso 9 Haga clic en **Siguiente** en el asistente de incorporación para empezar con el registro del dispositivo.

Paso 10 (Opcional) Agregue etiquetas a su dispositivo para ayudar a filtrar y ordenar en la página **Inventario**. Introduzca una etiqueta y seleccione el botón azul de más ( ). Las etiquetas se aplican al dispositivo una vez que se incorpora a CDO.

Qué hacer a continuación

Desde la página **Inventario**, seleccione el dispositivo que acaba de incorporar y seleccione cualquiera de las opciones que aparecen bajo el panel de **Administración** situado a la derecha.

Llevar a cabo la configuración inicial

Lleve a cabo la configuración inicial de Protección frente a amenazas mediante la CLI o Administrador del dispositivo.

Lleve a cabo la configuración inicial con la CLI

Conéctese a la CLI de Protección frente a amenazas para llevar a cabo la configuración inicial. Cuando utiliza la CLI para la configuración inicial, solo se conserva la configuración de la interfaz de administración y de la interfaz de acceso al administrador. Cuando lleva a cabo la configuración inicial con Administrador del dispositivo, *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se mantiene al cambiar a CDO para la administración, además por supuesto de la interfaz de administración y la configuración de acceso del administrador. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso.

Procedimiento

Paso 1 Conéctese a la CLI de Protección frente a amenazas en el puerto de consola.

El puerto de consola se conecta a la CLI de FXOS.

Paso 2 Inicie sesión con el nombre de usuario **admin** y la contraseña **Admin123**.

La primera vez que inicie sesión en FXOS, se le solicitará que cambie la contraseña. Esta contraseña también se utiliza para el inicio de sesión de Protección frente a amenazas para SSH.

Nota Si la contraseña ya se ha cambiado y no sabe cuál es, debe volver restablecer la imagen en el dispositivo para volver a configurar la contraseña predeterminada. Consulte la guía de resolución de problemas de FXOS para el procedimiento de restablecer la imagen.

Ejemplo:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Paso 3 Conéctese a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Paso 4 La primera vez que inicie sesión en Protección frente a amenazas, se le solicitará que acepte el contrato de licencia del usuario final (EULA). A continuación, se le presenta el script de configuración de la CLI para los ajustes de la interfaz de administración.

Los ajustes de la interfaz de administración se utilizan aunque active el acceso del administrador en una interfaz de datos.

Nota No puede volver a abrir el asistente de configuración de la CLI a menos que borre la configuración; por ejemplo, al restablecer la imagen. Sin embargo, todos estos ajustes pueden cambiarse más tarde en la CLI mediante los comandos de **configuración de red**. Consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Los valores predeterminados o los introducidos anteriormente aparecen entre paréntesis. Para aceptar los valores introducidos anteriormente, pulse **Intro**.

Consulte las siguientes directrices:

- **¿Configurar IPv4 a través de DHCP o de forma manual?** Elija **Manual**. Aunque no tenga previsto utilizar la interfaz de gestión, debe establecer una dirección IP, por ejemplo, una dirección privada. No puede configurar una interfaz de datos para la administración si la interfaz de gestión está establecida en DHCP, ya que la ruta predeterminada, que debe ser **interfaces de datos** (consulte la siguiente viñeta), puede sobrescribirse por otra recibida del servidor DHCP.
- **Introduzca la gateway predeterminada IPv4 para la interfaz de gestión**: configure la gateway como **interfaz de datos**. Esta configuración reenvía el tráfico de gestión a través de la placa base para que se pueda enrutar a través de la interfaz de datos de acceso del administrador.
- **¿Administrar el dispositivo de forma local?**: introduzca **no** para utilizar CDO. Si responde **Sí** significa que utilizará Administrador del dispositivo en su lugar.
- **¿Configurar el modo de firewall?** Introduzca **enrutado**. El acceso al administrador externo solo es compatible en el modo de firewall enrutado.

Ejemplo:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

```
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Paso 5 Configure la interfaz externa para el acceso al administrador.

configure network management-data-interface

A continuación, se le pedirá que configure los ajustes de red básicos para la interfaz externa. Consulte la siguiente información para utilizar este comando:

- La interfaz de gestión no puede utilizar DHCP si desea utilizar una interfaz de datos para la gestión. Si no configuró la dirección IP de forma manual durante la configuración inicial, puede hacerlo ahora con el comando **configure network** {**ipv4** | **ipv6**} **manual**. Si aún no ha establecido el gateway de la interfaz de administración en **interfaces de datos**, este comando lo establecerá ahora.
- Cuando agrega el Protección frente a amenazas a CDO, CDO detecta y conserva la configuración de la interfaz, incluidos los siguientes detalles: la dirección IP y el nombre de la interfaz, la ruta estática al gateway, los servidores DNS y los servidores DDNS. Para obtener más información sobre la configuración del servidor DNS, consulte la información más abajo. En CDO puede hacer cambios en la configuración de la interfaz de acceso al administrador más adelante, pero asegúrese de que no realiza cambios que puedan impedir que el Protección frente a amenazas o el CDO restablezcan la conexión de administración. Si la conexión de administración se interrumpe, el Protección frente a amenazas incluye el comando **configure policy rollback** para restaurar la implementación anterior.
- Si configura una URL para la actualización del servidor DDNS, el Protección frente a amenazas agrega automáticamente certificados para todas las CA principales del paquete de CA raíz de confianza de Cisco para que el Protección frente a amenazas pueda validar el certificado del servidor DDNS para la conexión HTTPS. El Protección frente a amenazas es compatible con cualquier servidor DDNS que utilice la especificación de API remota DynDNS (https://help.dyn.com/remote-access-api/).
- Este comando establece el servidor DNS de la interfaz de *datos*. El servidor DNS de administración que estableció con el script de configuración (o mediante el comando **configure network dns servers**) se utiliza para el tráfico de gestión. El servidor DNS de datos se utiliza para DDNS (si está configurado) o para las políticas de seguridad que se aplican a esta interfaz.

En el CDO, los servidores DNS de la interfaz de datos están configurados en la política de configuración de la plataforma que ha asignado a este Protección frente a amenazas. Cuando agrega el Protección frente a amenazas al CDO, se mantiene la configuración local, y los servidores DNS *no* se agregan a una política de configuración de la plataforma. Sin embargo, si después asigna una política de configuración de plataforma al Protección frente a amenazas que incluye una configuración de DNS, esa configuración sobrescribirá la local. Recomendamos que configure de forma activa la configuración de la plataforma DNS para que coincida con esta configuración y sincronizar el CDO y el Protección frente a amenazas.

Además, el CDO solo mantiene los servidores DNS locales solo se conservan si se detectaron en el registro inicial. Por ejemplo, si registró el dispositivo mediante la interfaz de administración, pero después configura una interfaz de datos con el comando **configure network management-data-interface**, entonces debe configurar manualmente todos esos ajustes en CDO, incluidos los servidores DNS, para que coincidan con la configuración del Protección frente a amenazas.

- Puede cambiar la interfaz de administración después de registrar el Protección frente a amenazas en CDO, ya sea en la interfaz de administración o en otra interfaz de datos.
- El FQDN que estableció en el asistente de configuración se utilizará para esta interfaz.
- Puede borrar toda la configuración del dispositivo como parte del comando; esta opción se puede usar para la recuperación, pero no le recomendamos que la utilice para la configuración inicial o el funcionamiento normal.
- Para desactivar la administración de datos, introduzca el comando **configure network management-data-interface disable**.

Ejemplo:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Ejemplo:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
```

```
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Paso 6 Identifique el CDO que gestionará este Protección frente a amenazas mediante el comando **configure manager add** que generó CDO. Consulte Incorporar un dispositivo con el asistente de incorporación, en la página 138 para generar el comando.

Ejemplo:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Realizar la configuración inicial con Administrador del dispositivo

Conéctese a Administrador del dispositivo para realizar la configuración inicial del Protección frente a amenazas. Cuando lleva a cabo la configuración inicial con Administrador del dispositivo, *toda* la configuración de la interfaz que se haya completado en Administrador del dispositivo se conserva al cambiar a CDO para la gestión, además de la configuración de acceso del administrador y de la interfaz de administración. Tenga en cuenta que no se conservan otros valores de configuración predeterminados, como la política de control de acceso o las zonas de seguridad. Cuando utiliza la CLI, solo se conservan la configuración de acceso del administrador y la interfaz de administración (por ejemplo, no se conserva la configuración de la interfaz interna de forma predeterminada).

Procedimiento

Paso 1 Conecte su equipo de administración a la de una de las siguientes interfaces: Ethernet1/2 a 1/8.

Paso 2 Inicie sesión en Administrador del dispositivo.

a) Introduzca la siguiente URL en su navegador: **https://192.168.95.1**
b) Inicie sesión con el nombre de usuario **admin** y la contraseña predeterminada **Admin123**.
c) Se le pedirá que lea y acepte el contrato de licencia del usuario final y que cambie la contraseña de administrador.

Paso 3 Utilice el asistente de configuración cuando inicie sesión por primera vez en Administrador del dispositivo para completar la configuración inicial. De manera opcional, puede omitir el asistente de configuración haciendo clic en **Omitir configuración del dispositivo** al final de la página.

Después de completar el asistente de configuración, además de la configuración predeterminada de la interfaz interna (Ethernet1/2 a 1/8, que son puertos de switch en la VLAN1), tendrá una configuración para una interfaz externa (Ethernet1/1) que se mantendrá cuando cambie a la administración del CDO.

a) Configure las siguientes opciones para las interfaces externas y de administración y haga clic en **Siguiente**.

1. **Dirección de la interfaz externa**: esta interfaz suele ser la gateway de Internet y puede utilizarse como interfaz de acceso del administrador. No se puede seleccionar una interfaz externa alternativa

durante la configuración inicial del dispositivo. La primera interfaz de datos es la interfaz externa predeterminada.

Si desea utilizar una interfaz diferente de la externa (o interna) para el acceso al administrador, tendrá que configurarla manualmente después de completar el asistente de configuración.

Configure IPv4: la dirección IPv4 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, una máscara de subred y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv4. No puede configurar PPPoE con el asistente de configuración. PPPoE puede ser necesario si la interfaz está conectada a un módem DSL, a un módem por cable o a otra conexión con su ISP, y su ISP utiliza PPPoE para proporcionar su dirección IP. Puede configurar PPPoE después de completar el asistente.

Configure IPv6: la dirección IPv6 para la interfaz externa. Puede utilizar DHCP o introducir manualmente una dirección IP estática, un prefijo y una gateway. También puede seleccionar **Off** para no configurar una dirección IPv6.

2. **Interfaz de administración**

   No verá la configuración de la interfaz de administración si ha realizado la configuración inicial desde la CLI.

   Los ajustes de la interfaz de administración se utilizan aunque active el acceso al administrador en una interfaz de datos. Por ejemplo, el tráfico de administración que se enruta por la placa base a través de la interfaz de datos resolverá los FQDN utilizando los servidores DNS de la interfaz de administración y no los servidores DNS de la interfaz de datos.

   Servidores DNS: el servidor DNS para la dirección de administración del sistema. Introduzca una o varias direcciones de servidores DNS para la resolución de nombres. El valor predeterminado son los servidores DNS públicos de OpenDNS. Si edita los campos y quiere volver a los predeterminados, haga clic en **Usar OpenDNS** para volver a cargar las direcciones IP adecuadas en los campos.

   Nombre de host del firewall: el nombre de host para la dirección de administración del sistema.

b) Configure los **Ajustes de la hora (NTP)** y haga clic en **Siguiente**.

1. **Zona horaria**: seleccione la zona horaria del sistema.
2. **Servidor de hora NTP**: seleccione si desea utilizar los servidores NTP predeterminados o introducir manualmente las direcciones de sus servidores NTP. Puede agregar varios servidores para proporcionar copias de seguridad.

c) Seleccione **Iniciar periodo de evaluación de 90 días sin registro**.

No registre el Protección frente a amenazas con Smart Software Manager; todas las licencias se realizan en CDO.

d) Haga clic en **Finalizar**.

e) Se le solicitará que elija **Administración en la nube** o **Independiente**. Para el Centro de administración en la nube de CDO, seleccione **Independiente** y, a continuación, **Lo tengo**.

La opción **Administración en la nube** es para la función heredada de CDO/FDM.

Paso 4 (Puede que sea necesario) Configure la interfaz de administración. Consulte la interfaz de administración en **Dispositivo** > **Interfaces**.

La interfaz de administración debe tener la gateway configurada para interfaces de datos. Por defecto, la interfaz de administración recibe una dirección IP y una gateway desde el DHCP. Si no recibe una gateway

desde el DHCP (por ejemplo, no conecta esta interfaz a una red), entonces la gateway se conectará por defecto a las interfaces de datos, y no necesitará configurar nada. Si ha recibido una gateway desde DHCP, en su lugar necesita configurar esta interfaz con una dirección IP estática y ajustar la gateway a las interfaces de datos.

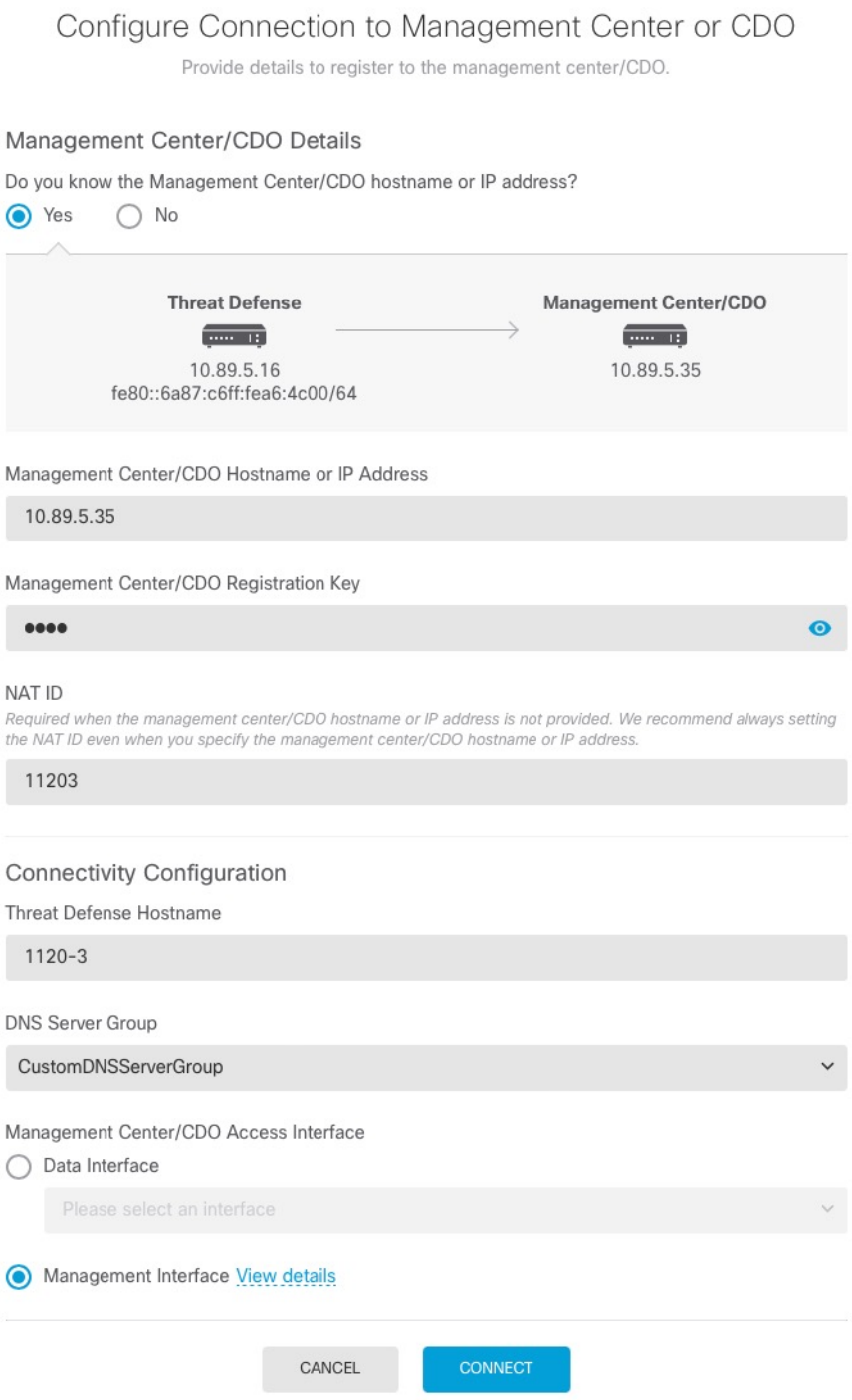
Paso 5 Si desea configurar interfaces adicionales, incluida una interfaz distinta de la externa o la interna que desee utilizar para el acceso al administrador, seleccione **Dispositivo** y, a continuación, haga clic en el enlace del resumen de **Interfaces**.

Consulte Configurar el firewall en Administrador del dispositivo, en la página 110 para obtener más información sobre la configuración de interfaces en Administrador del dispositivo. No se conservará otra configuración de Administrador del dispositivo cuando registre el dispositivo en el CDO.

Paso 6 Seleccione **Dispositivo** > **Configuración del sistema** > **Administración central**, y haga clic en **Proceder** para configurar la administración del Centro de administración.

Paso 7 Configure los **Detalles del centro de administración/CDO**.

Figura 47: Detalles del centro de administración/CDO



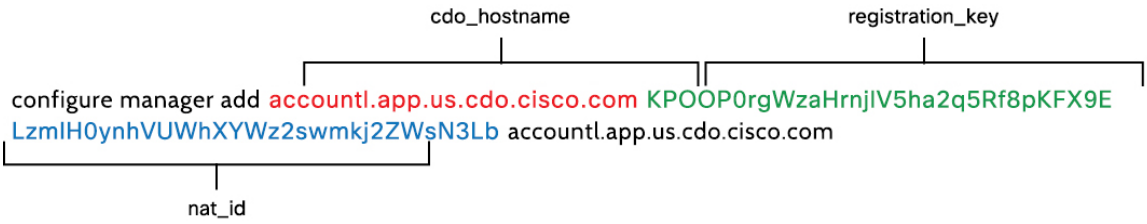
a) En **¿Conoce el nombre de host o la dirección IP del centro de administración/CDO?**, haga clic en **Sí**.

CDO genera el comando **configure manager add**. Consulte Incorporar un dispositivo con el asistente de incorporación, en la página 138 para generar el comando.

configure manager add *cdo_hostname registration_key nat_id display_name*

Ejemplo:

Figura 48: Configure el administrador de agregación de componentes de comandos



b) Copie las partes *cdo_hostname*, *registration_key* y *nat_id* del comando en los campos **Nombre de host/dirección IP del centro de administración/CDO**, **Clave de registro del centro de administración/CDO** e **ID de NAT**.

Paso 8 Configure la **Configuración de conectividad**.

a) Especifique el **Nombre de host del FTD**.

Este FQDN se utilizará para la interfaz exterior o para cualquier interfaz que seleccione como **Interfaz de acceso al centro de administración/CDO**.

b) Especifique el **Grupo de servidores DNS**.

Elija un grupo existente o cree uno nuevo. El grupo de DNS predeterminado se llama **CiscoUmbrellaDNSServerGroup** e incluye los servidores OpenDNS.

Estos ajustes establecen el servidor DNS de la interfaz de *datos*. El servidor DNS de administración que estableció con el asistente de configuración se utiliza para el tráfico de administración. El servidor DNS de datos se utiliza para DDNS (si está configurado) o para las políticas de seguridad que se aplican a esta interfaz. Es probable que seleccione el mismo grupo de servidor DNS que utilizó para la administración, porque tanto la administración como el tráfico de administración y de datos acceden al servidor DNS a través de la interfaz externa.

En el CDO, los servidores DNS de la interfaz de datos están configurados en la política de configuración de la plataforma que ha asignado a este Protección frente a amenazas. Cuando agrega el Protección frente a amenazas al CDO, se mantiene la configuración local, y los servidores DNS *no* se agregan a una política de configuración de la plataforma. Sin embargo, si después asigna una política de configuración de plataforma al Protección frente a amenazas que incluye una configuración de DNS, esa configuración sobrescribirá la local. Recomendamos que configure de forma activa la configuración de la plataforma DNS para que coincida con esta configuración y sincronizar el CDO y el Protección frente a amenazas.

Además, el CDO solo mantiene los servidores DNS locales solo se conservan si se detectaron en el registro inicial.

c) En la **Interfaz de acceso al centro de administración/CDO**, seleccione **externa**.

Puede elegir cualquier interfaz configurada, pero esta guía asume que está utilizando una externa.

Paso 9 Si elige una interfaz de datos distinta a la externa, agregue una ruta predeterminada.

Verá un mensaje en el que se le indicará que compruebe si tiene una ruta predeterminada a lo largo de la interfaz. Si ha seleccionado externa, ya ha configurado esta ruta dentro del asistente de configuración. Si ha seleccionado una interfaz diferente, debe configurar de forma manual una ruta predeterminada antes de

conectarse a CDO. Consulte Configurar el firewall en Administrador del dispositivo, en la página 110 para obtener más información acerca de las rutas estáticas en Administrador del dispositivo.

Paso 10 Haga clic en **Añadir un método DNS dinámico (DDNS)**.

El DDNS garantiza que CDO pueda acceder a Protección frente a amenazas con su nombre de dominio completo (FQDN) si cambia la dirección IP de Protección frente a amenazas. Para configurar el DDNS, consulte **Dispositivo** > **Configuración del sistema** > **Servidor DDNS**.

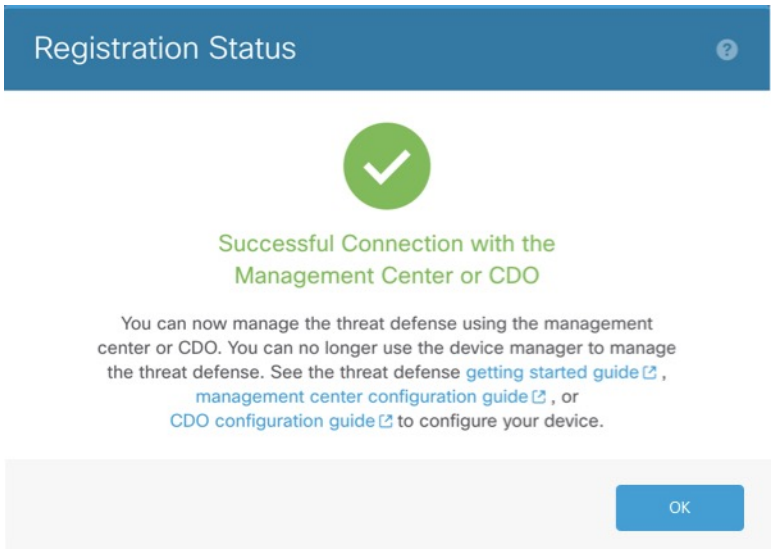
Si configura el DDNS antes de agregar el Protección frente a amenazas a CDO, el Protección frente a amenazas agrega automáticamente certificaciones para todas las CA principales del paquete de CA raíz de confianza de Cisco para que el Protección frente a amenazas pueda validar la certificación del servidor DDNS para la conexión HTTPS. El Protección frente a amenazas es compatible con cualquier servidor DDNS que utilice la especificación de API remota DynDNS (https://help.dyn.com/remote-access-api/).

Paso 11 Haga clic en **Conectar**. El cuadro de diálogo **Estado de registro** muestra el estado actual del cambio a CDO. Después del paso **Guardar la configuración de registro del centro de administración/CDO**, vaya a CDO y agregue el firewall.

Si desea cancelar el cambio a CDO, haga clic en **Cancelar registro**. De lo contrario, no cierre la ventana del navegador de Administrador del dispositivo hasta que se haya completado el paso de **Guardar la configuración de registro del centro de administración/CDO**. Si lo hace, el proceso se detendrá y no continuará hasta que se vuelva a conectar a Administrador del dispositivo.

Si permanece conectado a Administrador del dispositivo tras el paso de **Guardar la configuración de registro del centro de administración/CDO**, en algún momento le aparecerá el cuadro de diálogo **Se ha conectado correctamente al centro de administración/CDO**, tras el cual se le desconectará de Administrador del dispositivo.

Figura 49: Conexión correcta



Configurar una norma de seguridad básica

Esta sección describe cómo configurar una política de seguridad básica con la siguiente configuración:

- Interfaces interna y externa: asigne una dirección IP estática a la interfaz interna. Ha configurado los ajustes básicos para la interfaz externa como parte de la configuración de acceso del administrador, pero todavía necesita asignarla a una zona de seguridad.
- Servidor DHCP: utilice un servidor DHCP en la interfaz interna para los clientes.
- NAT: utilice la interfaz PAT en la interfaz externa.
- Control de acceso: permita el tráfico desde dentro hacia fuera.
- SSH: active SSH en la interfaz de acceso del administrador.

Configurar interfaces

Agregue la interfaz VLAN1 para los puertos de switch o convierta los puertos de switch en interfaces de firewall, asigne interfaces a las zonas de seguridad y configure las direcciones IP. Normalmente, deberá configurar al menos un mínimo de dos interfaces para tener un sistema que pase tráfico significativo. Normalmente, tendrá una interfaz externa que da al router ascendente o a Internet, y una o más interfaces internas para las redes de su organización. De forma predeterminada, Ethernet1/1 es una interfaz de firewall normal que puede utilizar como externa y las interfaces restantes son puertos de switch en la VLAN1; después de agregar la interfaz VLAN1, puede convertirla en su interfaz interna. También puede asignar puertos de switch a otras VLAN o convertir puertos de switch a interfaces de firewall.

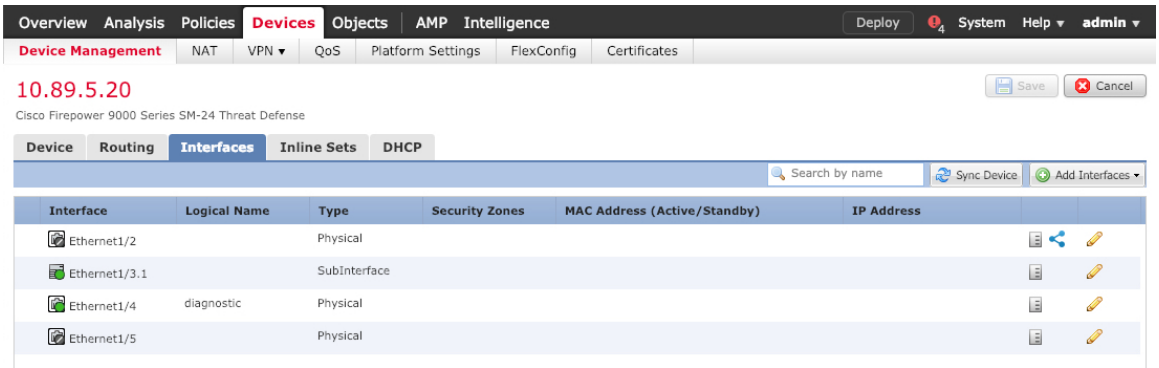
Una situación típica de enrutamiento de borde es obtener la dirección de la interfaz externa a través de DHCP de su ISP, mientras que usted define direcciones estáticas en las interfaces internas.

El siguiente ejemplo configura una interfaz interna de modo enrutado (VLAN1) con una dirección estática y una interfaz externa de modo enrutado mediante DHCP (Ethernet1/1).

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en el **Editar** (✎) del dispositivo.

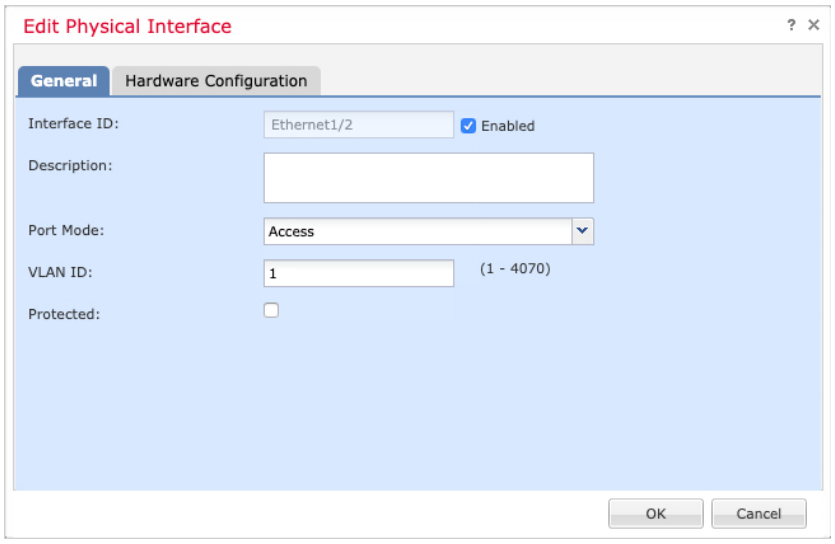
Paso 2 Haga clic en **Interfaces**.



Paso 3 (Opcional) Desactive el modo de puerto de switch para cualquiera de los puertos de switch (Ethernet1/2 a 1/8) haciendo clic en el deslizador de la columna **SwitchPort** para que se muestre como desactivado ( ).

Paso 4 Active los puertos del switch.

a) Haga clic en **Editar** ( ) para el puerto del switch.



b) Active la interfaz marcando la casilla de verificación **Activar**.

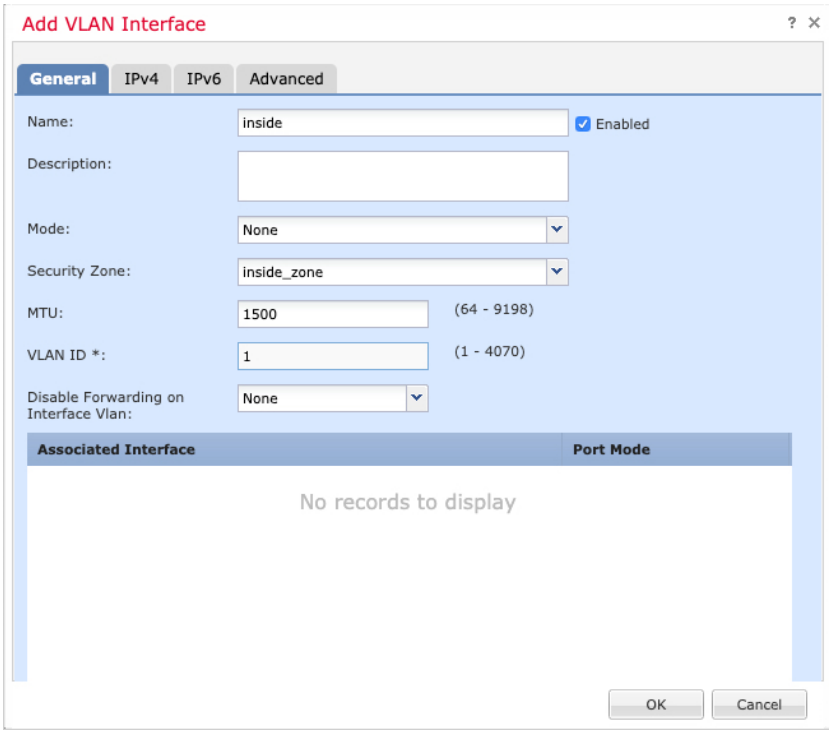
c) (Opcional) Cambie la ID de VLAN; el valor predeterminado es 1. A continuación, agregará una interfaz VLAN para que coincida con esta ID.

d) Haga clic en **Aceptar**.

Paso 5 Agregue la interfaz VLAN *interna*.

a) Haga clic en **Agregar interfaz** > **Interfaz VLAN**.

Aparece la pestaña **General**



b) Introduzca un **nombre** de hasta 48 caracteres de longitud.

Por ejemplo, asigne un nombre a la interfaz: **interna**.

c) Active la casilla **Activado**.

d) Deje el **modo** establecido en **Ninguno**.

e) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad interna existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, agregue una zona llamada **inside_zone**. Cada interfaz debe asignarse a una zona de seguridad o a un grupo de interfaces. Una interfaz solo puede pertenecer a una zona de seguridad, pero también puede pertenecer a varios grupos de interfaces. Aplicará su norma de seguridad en función de las zonas o los grupos. Por ejemplo, puede asignar la interfaz interna a la zona interna; y la interfaz externa a la zona externa. A continuación, puede configurar su política de control de acceso para permitir que el tráfico pase de dentro hacia fuera, pero no de fuera hacia dentro. La mayoría de las políticas solo admiten zonas de seguridad; puede utilizar zonas o grupos de interfaz en políticas NAT, políticas de prefiltro y políticas de QoS.

f) Establezca la **ID de VLAN** en **1**.

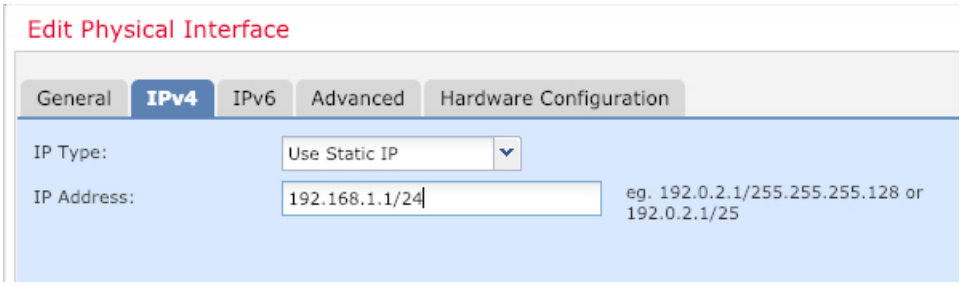
De forma predeterminada, todos los puertos de switch están configurados en VLAN1; si elige una ID de VLAN diferente aquí, también debe editar cada puerto de switch para que se encuentre en la nueva ID de VLAN.

No puede cambiar la ID de VLAN después de guardar la interfaz; la ID de VLAN es la etiqueta de VLAN utilizada y la ID de interfaz de su configuración.

g) Haga clic en la pestaña **IPv4** o **IPv6**.

- **IPv4**: elija **Usar IP estática** en la lista desplegable e introduzca una dirección IP y una máscara de subred en notación con barra.

Por ejemplo, introduzca **192.168.1.1/24**

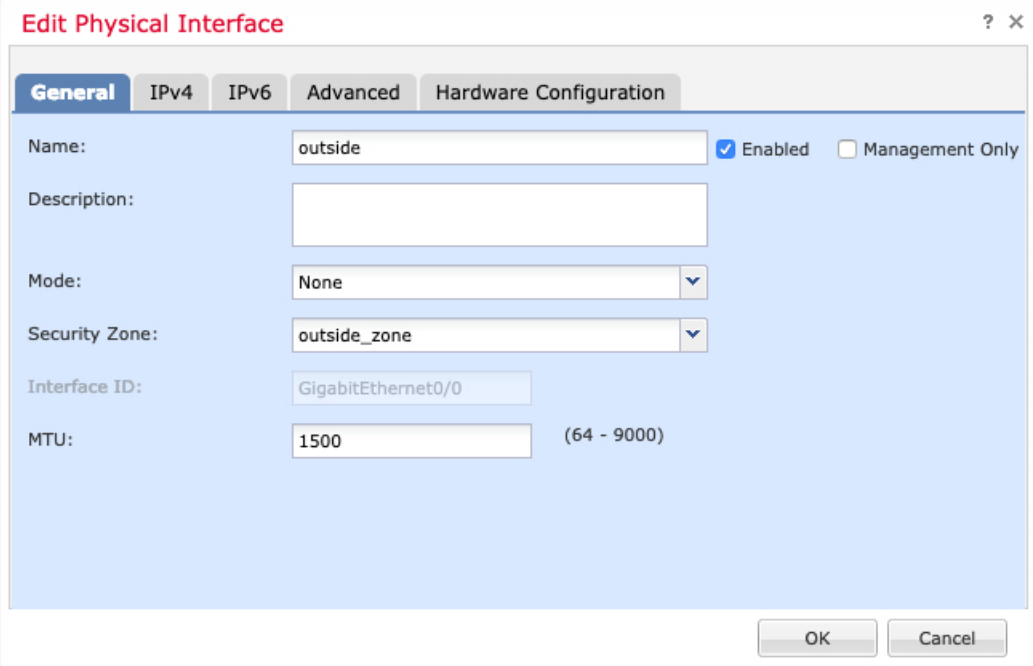


- **IPv6**: compruebe la casilla de verificación **Configuración automática** para la configuración automática sin estado.

h) Haga clic en **Aceptar**.

Paso 6 Haga clic en **Editar** (✎) para el Ethernet1/1 que quiera utilizar para la *externa*.

Aparece la pestaña **General**.



Ya ha configurado esta interfaz para el acceso al administrador, por lo que ya estará nombrada, activada y direccionada. No debe modificar ninguno de estas configuraciones básicas porque interrumpiría la conexión de gestión de Centro de administración. Todavía debe configurar las zona de seguridad en esta pantalla para las políticas de tráfico de paso.

a) En la lista desplegable **Zona de seguridad**, elija una zona de seguridad externa existente o agregue una nueva haciendo clic en **Nueva**.

Por ejemplo, añada una zona llamada **outside_zone**.

b) Haga clic en **Aceptar**.

Paso 7 Haga clic en **Guardar**.

Configurar el servidor DHCP

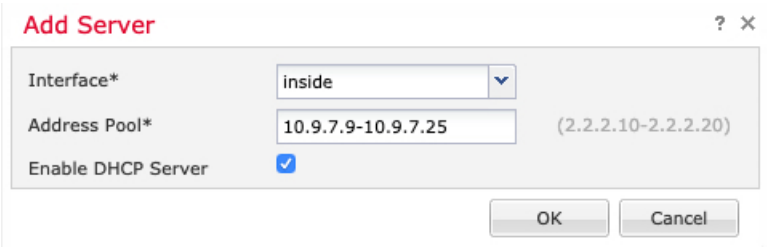
Active el servidor DHCP si desea que los clientes utilicen DHCP para obtener direcciones IP de Protección frente a amenazas.

Procedimiento

Paso 1 Elija **Dispositivos** > **Administración de dispositivos** y haga clic en **Editar** (✎) del dispositivo.

Paso 2 Seleccione **DHCP** > **Servidor DHCP**.

Paso 3 En la página **Servidor**, haga clic en **Agregar** y configure las siguientes opciones:



- **Interfaz**: elija la interfaz en la lista desplegable.
- **Conjunto de direcciones**: establezca el rango de direcciones IP de menor a mayor que utiliza el servidor DHCP. El rango de direcciones IP debe estar en la misma subred que la interfaz seleccionada y no puede incluir la dirección IP de la propia interfaz.
- **Habilitar servidor DHCP**: habilite el servidor DHCP en la interfaz seleccionada.

Paso 4 Haga clic en **Aceptar**.

Paso 5 Haga clic en **Guardar**.

Configurar NAT

Una regla NAT típica convierte las direcciones internas a un puerto en la dirección IP de la interfaz externa. Este tipo de regla NAT se denomina *traducción de dirección del puerto de interfaz (PAT)*.

Procedimiento

Paso 1 Seleccione **Dispositivos** > **NAT**y haga clic en **Nueva política** > **NAT de Threat Defense**.

Paso 2 Asigne un nombre a la política, seleccione los dispositivos en los que la desea aplicar y haga clic en **Guardar**.

La política se agrega al Centro de administración. Aún tiene que añadir reglas a la política.

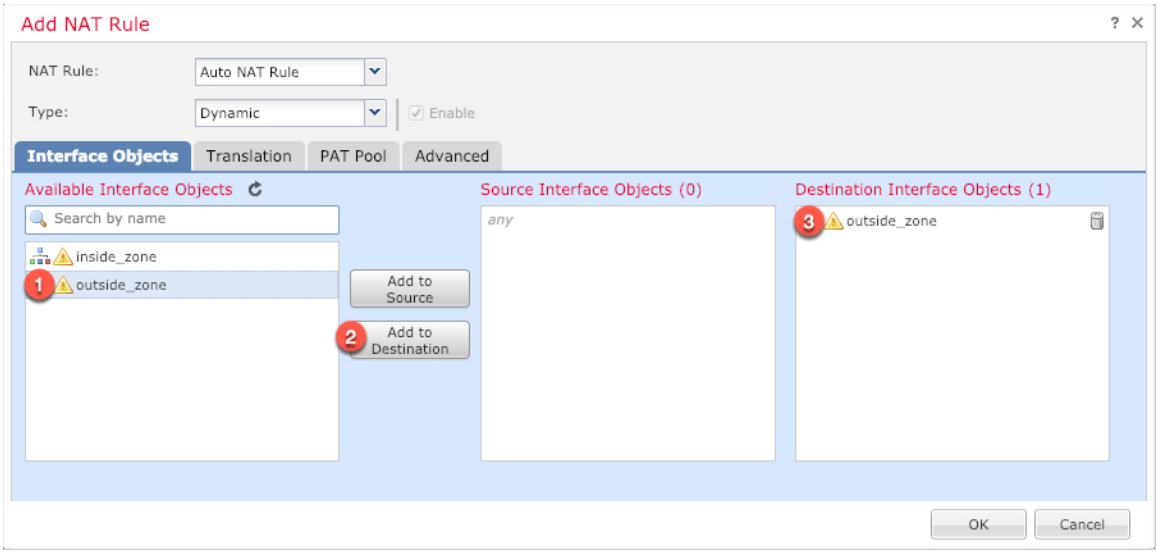
Paso 3 Haga clic en **Agregar regla**.

Aparece el cuadro de diálogo **Agregar regla NAT**.

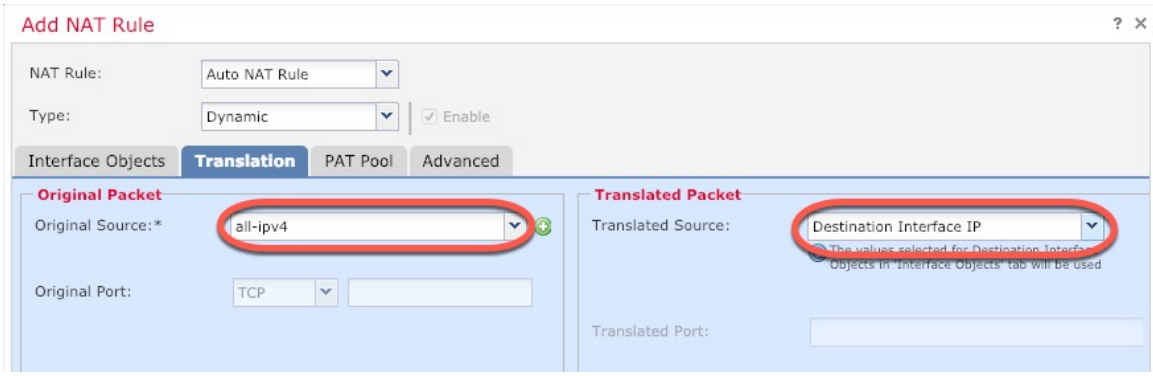
Paso 4 Configure las opciones de regla básicas:

- **Regla NAT**: elija una **regla NAT automática**.
- **Tipo**: seleccione **Dinámico**.

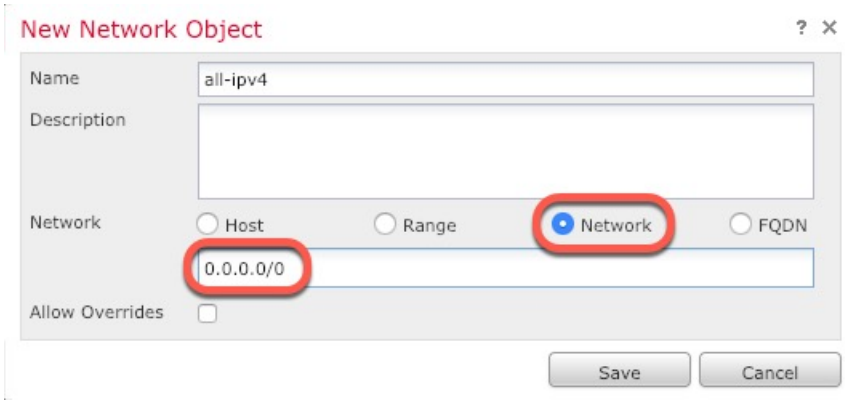
Paso 5 En la página **Objetos de interfaz**, agregue la zona exterior del área **Objetos de interfaz disponibles** al área **Objetos de interfaz de destino**.



Paso 6 En la página **Traducción**, configure las siguientes opciones:



- **Fuente original**: haga clic en **Agregar** (+) para agregar un objeto de red para todo el tráfico IPv4 (0.0.0.0/0).

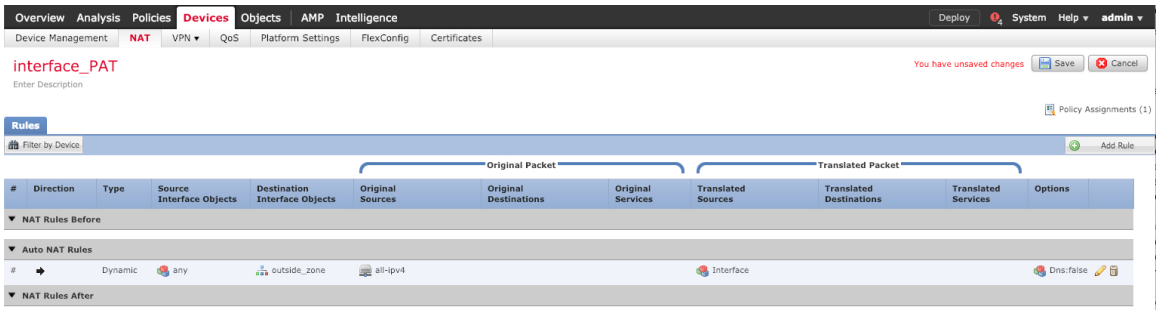


Nota No puede utilizar el objeto **any-ipv4** definido por el sistema, ya que las reglas NAT automáticas añaden NAT como parte de la definición del objeto y no puede editar objetos definidos por el sistema.

- **Fuente traducida**: seleccione la **IP de la interfaz de destino**.

Paso 7 Haga clic en **Guardar** para agregar la regla.

La regla se guarda en la tabla **Reglas**.



Paso 8 Haga clic en **Guardar** en la página de **NAT** para guardar los cambios.

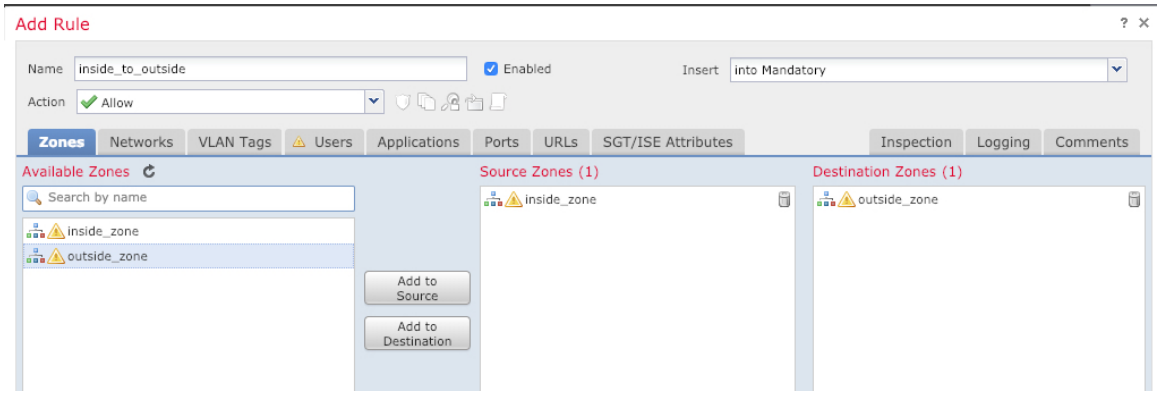
Permitir el tráfico de dentro hacia afuera

Si creó una política básica de control de acceso **Bloquear todo el tráfico** cuando registró la Protección frente a amenazas, entonces debe agregar reglas a la política para permitir el tráfico a través del dispositivo. El siguiente procedimiento agrega una regla para permitir el tráfico de la zona interna a la zona externa. Si tiene otras zonas, asegúrese de agregar reglas que permitan el tráfico a las redes adecuadas.

Procedimiento

Paso 1 Seleccione **Política** > **Política de acceso** > **Política de acceso** y haga clic en **Editar** ( ) para la política de control de acceso asignada a la Protección frente a amenazas.

Paso 2 Haga clic en **Agregar regla** y establezca los siguientes parámetros:

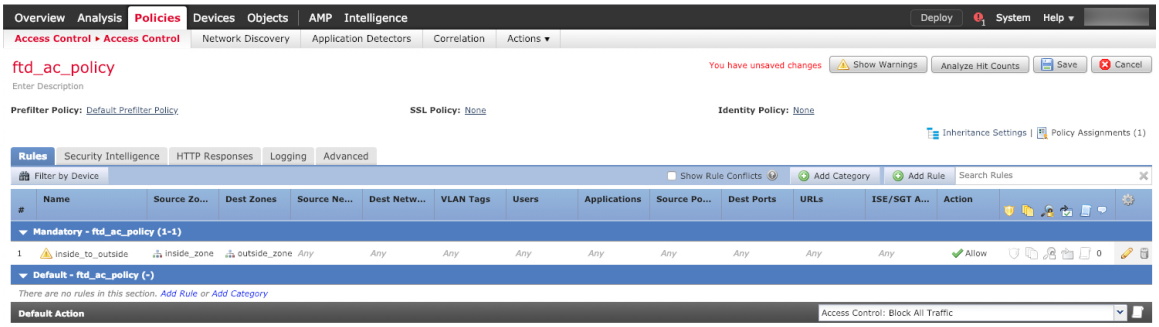


- **Nombre**: nombre esta regla, por ejemplo, **inside_to_outside**.
- **Zonas de origen**: seleccione la zona interna de las **Zonas disponibles** y haga clic en **Agregar al origen**.
- **Zonas de destino**: seleccione la zona externa de las **Zonas disponibles** y haga clic en **Agregar al destino**.

Deje la otra configuración como está.

Paso 3 Haga clic en **Agregar**.

La regla se agrega a la tabla **Reglas**.



Paso 4 Haga clic en **Guardar**.

Configurar SSH en la interfaz de datos de acceso al administrador

Si ha habilitado el acceso al Centro de administración en una interfaz de datos, como la externa, debe habilitar SSH en esa interfaz mediante este procedimiento. Esta sección describe cómo activar las conexiones SSH en una o más interfaces de *datos* en Protección frente a amenazas. SSH no es compatible con la interfaz lógica de diagnóstico.

Nota SSH está activado de forma predeterminada en la interfaz de gestión; sin embargo, esta pantalla no afecta para el acceso al SSH de gestión.

La interfaz de gestión es independiente de las otras interfaces del dispositivo. Se utiliza para configurar y registrar el dispositivo en el Centro de administración. SSH para interfaces de datos comparte la lista de usuarios internos y externos con SSH para la interfaz de administración. Otros ajustes se configuran por separado: para interfaces de datos, active SSH y acceda a las listas mediante esta pantalla; el tráfico SSH para las interfaces de datos utiliza la configuración de rutas regular y no cualquier ruta estática configurada en la configuración o en la CLI.

Para configurar una lista de acceso de SSH en la interfaz de administración, consulte el comando **configure ssh-access-list** en Referencias de comandos en Cisco Secure Firewall Threat Defense. Para configurar una ruta estática, consulte el comando **configure network static-routes**. De forma predeterminada, configure la ruta predeterminada a través de la interfaz de administración en la configuración inicial.

Para utilizar SSH, no necesita una regla de acceso que permita la dirección IP del host. Solo tiene que configurar el acceso SSH con esta sección.

Solo puede utilizar SSH en una interfaz accesible; si su host SSH se encuentra en la interfaz externa, solo puede iniciar la conexión de gestión directamente a la interfaz externa.

El dispositivo permite un máximo de 5 conexiones SSH simultáneas.

Nota Después de que un usuario realice tres intentos fallidos consecutivos de iniciar sesión en la CLI a través de SSH, el dispositivo interrumpe la conexión SSH.

Antes de empezar

- Puede configurar usuarios internos de SSH en la CLI mediante el comando **configure user add**;. De forma predeterminada, hay un usuario **administrador** para el que ha configurado la contraseña durante la configuración inicial. También puede configurar usuarios externos en LDAP o RADIUS si configura la **autenticación externa** en los ajustes de la plataforma.
- Necesita objetos de red que definan los hosts o las redes a las que dará permiso para realizar conexiones SSH al dispositivo. Puede agregar objetos como parte del procedimiento, pero si desea utilizar grupos de objetos para identificar un grupo de direcciones IP, asegúrese de que los grupos que se necesitan en las reglas ya existen. Seleccione **Objetos** > **Administración de objetos** para configurar objetos.

Nota No puede el objeto de red **any** proporcionado por el sistema. En su lugar, utilice **any-ipv**4 o **any-ipv6**.

Procedimiento

Paso 1 Seleccione **Dispositivos** > **Configuración de la plataforma** y cree o edite la política de Protección frente a amenazas.

Paso 2 Seleccione **Secure Shell**.

Paso 3 Identifique las interfaces y las direcciones IP que permiten conexiones SSH.

Utilice esta tabla para limitar las interfaces que aceptarán conexiones SSH y las direcciones IP de los clientes que pueden realizar esas conexiones. Puede utilizar direcciones de red en lugar de direcciones IP individuales.

a) Haga clic en **Agregar** para añadir una nueva regla, o haga clic en **Editar** para modificar una regla existente.
b) Configurar las propiedades de la regla:
   - **Dirección IP**: el objeto o grupo de red que identifica los host o las redes a con permiso para realizar conexiones SSH. Seleccione un objeto del menú desplegable o agregue un nuevo objeto de red haciendo clic en +.
   - **Zonas de seguridad**: agregue las zonas que contienen las interfaces a las que permitirá conexiones SSH. Para las interfaces que no estén en una zona, puede escribir el nombre de la interfaz en el campo debajo de la lista de zona de seguridad seleccionada y hacer clic en **Agregar**. Estas reglas se aplicarán a un dispositivo solo si el dispositivo incluye las interfaces o zonas seleccionadas.
c) Haga clic en **OK** (Aceptar).

Paso 4 Haga clic en **Guardar**.

Ahora puede ir a **Implementar** > **Implementación** e implementar la política en los dispositivos asignados. Los cambios no estarán activos hasta que los implemente.

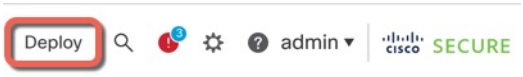
Implementar la configuración

Implementar los cambios de configuración en Protección frente a amenazas; ningún cambio estará activo en el dispositivo hasta que los implemente.

Procedimiento

Paso 1 Haga clic en **Implementar** en la parte superior derecha.

Figura 50: Implementar



Paso 2 Haga clic en **Implementar todo** para implementar en todos los dispositivos o haga clic en **Implementación avanzada** para implementar en los dispositivos seleccionados.

Figura 51: Implementar todo

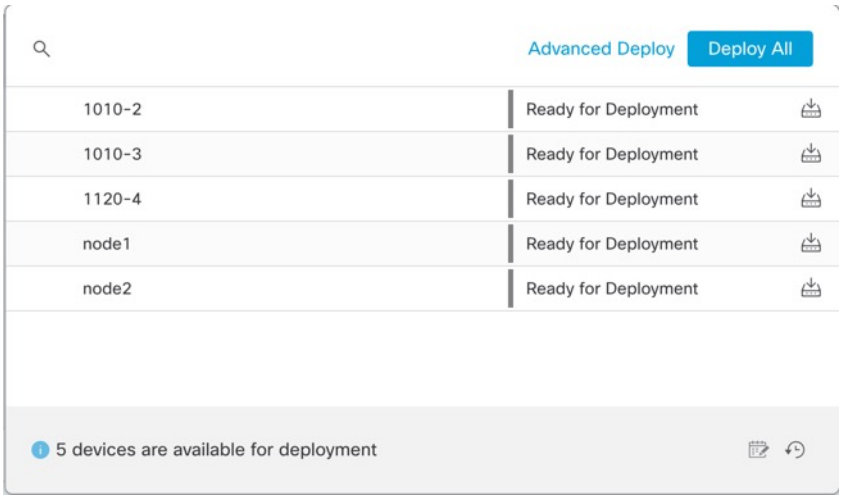
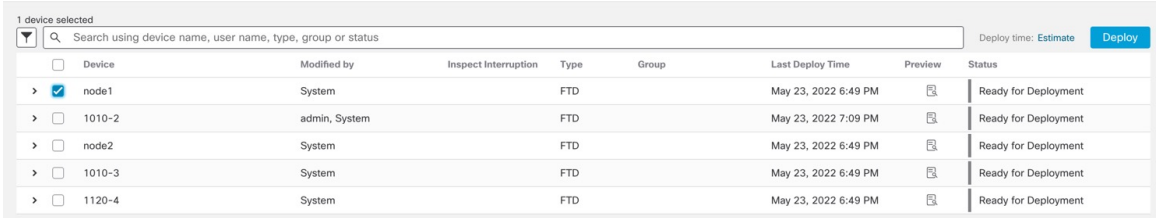
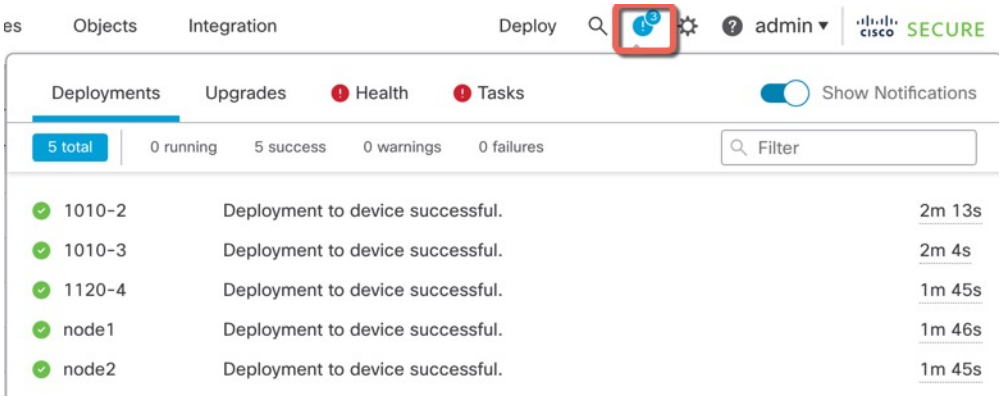


Figura 52: Implementación avanzada



Paso 3 Compruebe que la implementación se realiza correctamente. Haga clic en el icono a la derecha del botón **Implementar** en la barra de menú para ver el estado de las implementaciones.

Figura 53: Estado de la implementación



Resolución de problemas y mantenimiento

Acceder a la Protección frente a amenazas y a la CLI de FXOS

Utilice la interfaz de línea de comandos (CLI) para configurar el sistema y solucionar los problemas básicos. No puede configurar políticas a través de una sesión de CLI. Puede acceder a la CLI conectándose al puerto de consola.

También puede acceder a CLI de FXOS para solucionar problemas

Nota Como alternativa, puede utilizar SSH para la interfaz de administración del dispositivo Protección frente a amenazas. A diferencia de una sesión de consola, la sesión SSH se establece de forma predeterminada en la CLI de Protección frente a amenazas, desde la que puede conectarse a CLI de FXOS mediante el comando **connect fxos**. Puede conectarse después a la dirección en una interfaz de datos si abre esa interfaz para las conexiones SSH. El acceso SSH para las interfaces de datos está desactivado de forma predeterminada. Este procedimiento describe el acceso al puerto de consola, cuyo valor predeterminado es CLI de FXOS.

Procedimiento

Paso 1 Para iniciar sesión en la CLI, conecte su ordenador de gestión al puerto de consola. Firepower 1000 va con un cable de serie USB A a B. Instale las unidades USB de serie necesarias para su sistema operativo (consulte la guía de hardware de Firepower 1010). El puerto de consola de forma predeterminada es CLI de FXOS. Utilice la siguiente configuración de serie:

- 9600 baudios
- 8 bits de datos

- Sin paridad
- 1 bit de parada

Se conecta a la CLI de FXOS. Inicie sesión en la CLI con el nombre de usuario **admin** y la contraseña que estableció en la configuración inicial (la predeterminada es **Admin123**).

Ejemplo:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Paso 2 Acceda a la CLI de Protección frente a amenazas.

connect ftd

Ejemplo:

```
firepower# connect ftd
>
```

Después de iniciar sesión, para obtener información sobre los comandos disponibles en la CLI, introduzca **help** o **?**. Para obtener información sobre cómo utilizarla, consulte Referencias de comandos en Cisco Secure Firewall Threat Defense.

Paso 3 Para abandonar la CLI de Protección frente a amenazas, introduzca el comando **exit** o **logout**.

Este comando le devuelve al mensaje de CLI de FXOS. Para obtener información sobre los comandos disponibles en la CLI de FXOS, introduzca **?**.

Ejemplo:

```
> exit
firepower#
```

Solucionar problemas de conectividad de administración en una interfaz de datos

Cuando utilice una interfaz de datos para el acceso al administrador en lugar de utilizar la interfaz de administración específica, debe tener cuidado al cambiar la configuración de la interfaz y de la red del Protección frente a amenazas en CDO para no interrumpir la conexión. Si cambia el tipo de interfaz de administración después de agregar el Protección frente a amenazas a CDO (de datos a administración o de administración a datos), si las interfaces y los ajustes de red no están configurados correctamente, puede perder la conectividad de la administración.

Este tema le ayuda a solucionar problemas por perder la conectividad de gestión.

Ver el estado de la conexión de administración

En el CDO, compruebe el estado de conexión de administración en la página **Dispositivos** > **Administración de dispositivos** > **Dispositivo** > **Administración** > **Acceso del administrador - Detalles de configuración** > **Estado de conexión**.

En la CLI de Protección frente a amenazas, introduzca el comando **sftunnel-status-brief** para ver el estado de la conexión de administración. También puede utilizar **sftunnel-status** para ver información más detallada.

Consulte el siguiente ejemplo de salida para ver una conexión inactiva; no hay información de canal conectado "conectado a", ni información de frecuencia:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consulte el siguiente ejemplo de salida para ver una conexión activa; con información de canal conectado e información de frecuencia:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Vea la información sobre la red de Protección frente a amenazas

En la CLI de Protección frente a amenazas, consulte la configuración de red de la interfaz de datos de acceso a la administración y al administrador.

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
```

```
MAC Address                : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration              : Manual
Address                    : 10.99.10.4
Netmask                    : 255.255.255.0
Gateway                    : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration              : Disabled

===============[ Proxy Information ]================
State                      : Disabled
Authentication             : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers                :
Interfaces                 : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                      : Enabled
Link                       : Up
Name                       : outside
MTU                        : 1500
MAC Address                : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration              : Manual
Address                    : 10.89.5.29
Netmask                    : 255.255.255.192
Gateway                    : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration              : Disabled
```

Compruebe que el Protección frente a amenazas se registró con CDO

En la CLI de Protección frente a amenazas, compruebe que se completó el registro en CDO. Tenga en cuenta que este comando no mostrará el estado *actual* de la conexión de administración.

show managers

```
> show managers
Type                       : Manager
Host                       : account1.app.us.cdo.cisco.com
Display name               : account1.app.us.cdo.cisco.com
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
Management type            : Configuration
```

Ping CDO

En la CLI de Protección frente a amenazas, utilice el siguiente comando para hacer ping en CDO desde las interfaces de datos:

ping *cdo_hostname*

En la CLI de Protección frente a amenazas, utilice el siguiente comando para hacer ping en el CDO desde las interfaces de datos, que deberían tener rutas por la placa base hasta las interfaces de datos:

ping system *cdo_hostname*

Capturar paquetes en la interfaz interna de Protección frente a amenazas

En la CLI de Protección frente a amenazas, capture paquetes en la interfaz de la placa base interna (nlp_int_tap) para ver si se están enviando paquetes de administración:

capture *nombre* **interface nlp_int_tap trace detail match ip any any**

show capture*Nombre* **trace detail**

Compruebe el estado de la interfaz interna, las estadísticas y el recuento de paquetes

En la CLI de Protección frente a amenazas, consulte la información sobre la interfaz de la placa base interna, nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Comprobar enrutamiento y NAT

En la CLI de Protección frente a amenazas, compruebe que se agregó la ruta predeterminada (S*) y que existen reglas NAT internas para la interfaz de administración (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Comprobar otras configuraciones

Consulte los siguientes comandos para comprobar que todas las demás configuraciones están presentes. También puede ver muchos de estos comandos en la página **Dispositivos** > **Administración del dispositivo** > **Dispositivo** > **Administración** > **Acceso el administrador - Detalles de configuración** > **Salida CLI** de CDO.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Compruebe si la actualización de DDNS se ha realizado correctamente

En la CLI de Protección frente a amenazas, compruebe la actualización de DDNS se ha realizado correctamente:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Si la actualización ha provocado un error, utilice los comandos **debug http** y **debug ssl**. Para los errores de validación de certificados, compruebe que los certificados de origen están instalados en el dispositivo:

show crypto ca certificates *trustpoint_name*

Para comprobar el funcionamiento de DDNS:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Compruebe los archivos de registro de CDO

Consulte https://cisco.com/go/fmc-reg-error.

Revertir la configuración si el CDO pierde la conectividad

Si utiliza una interfaz de datos en el Protección frente a amenazas para el acceso del administrador e implementa un cambio de configuración desde el CDO que afecta a la conectividad de red, puede volver a la última configuración implementada en el Protección frente a amenazas para restaurar la conexión de la administración. A continuación, puede ajustar los valores de configuración en CDO para mantener la conectividad de red y volver a implementarla. Puede utilizar la función de reversión incluso si no pierde la conectividad; no está limitada a la resolución de problemas.

Consulte las siguientes directrices:

- Solo la implementación anterior está disponible localmente en Protección frente a amenazas; no se puede revertir a implementaciones previas.
- La reversión solo afecta a las configuraciones que se pueden establecer en el CDO. Por ejemplo, la reversión no afecta a ninguna configuración local relacionada con la interfaz de administración específica, que solo se puede configurar en la CLI de Protección frente a amenazas. Tenga en cuenta que si ha cambiado la configuración de la interfaz de datos después de la última implementación del CDO mediante el comando **configure network management-data-interface** y, a continuación, utiliza el comando de

reversión, dicha configuración no se conservará; volverán a la configuración del CDO implementada por última vez.

- Los datos de certificado SCEP fuera de banda que se actualizaron durante la implementación anterior no se pueden revertir.
- Durante la reversión, se perderán las conexiones porque se borrará la configuración actual.

Procedimiento

Paso 1 En la CLI de Protección frente a amenazas, vuelva a la configuración anterior.

configure policy rollback

Después de la reversión, el Protección frente a amenazas notifica al CDO que la reversión se ha completado correctamente. En el CDO, la pantalla de implementación mostrará un banner que indica que la configuración se ha revertido.

Nota Si la reversión ha provocado un error y la administración de CDO se restaura, consulte https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html para problemas comunes de implementación. En algunos casos, la reversión puede fallar después de restaurar el acceso a la administración del CDO; en este caso, puede resolver los problemas de configuración del CDO y volver a implementarlos desde el CDO.

Ejemplo:

Para el Protección frente a amenazas que utiliza una interfaz de datos para el acceso del administrador:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Paso 2 Compruebe que se ha restablecido la conexión de administración.

En el CDO, compruebe el estado de conexión de administración en la página **Dispositivos** > **Administración de dispositivos** > **Dispositivo** > **Administración** > **Acceso del administrador - Detalles de configuración** > **Estado de conexión**.

En la CLI de Protección frente a amenazas, introduzca el comando **sftunnel-status-brief** para ver el estado de la conexión de administración.

Si tarda más de 10 minutos en restablecer la conexión, debe solucionar el problema de conexión. Consulte Solucionar problemas de conectividad de administración en una interfaz de datos, en la página 162.

Apagar el firewall con CDO

Es importante que apague el sistema correctamente. Si solo desconecta la alimentación o pulsa el interruptor de alimentación se pueden provocar daños graves en el sistema de archivos. Recuerde que hay muchos procesos que se ejecutan en segundo plano todo el tiempo y que desconectar o apagar la alimentación no apaga adecuadamente su firewall.

Puede apagar el sistema correctamente con CDO.

Procedimiento

Paso 1 Elija **Dispositivo** > **Administración de dispositivos**.

Paso 2 Junto al dispositivo que desea reiniciar, haga clic en el icono editar ( ).

Paso 3 Haga clic en la pestaña **Dispositivo**.

Paso 4 Haga clic en el icono apagar dispositivo ( ) en la sección **Sistema**.

Paso 5 Cuando se le solicite, confirme que desea apagar el dispositivo.

Paso 6 Si tiene una conexión de consola al firewall, monitorice los mensajes del sistema una vez que este se apague. Verá el siguiente mensaje:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si no tiene una conexión de consola, espere aproximadamente 3 minutos para asegurarse de que el sistema se ha apagado.

Paso 7 Ahora puede desconectar la batería para extraerla físicamente del chasis si es necesario.

¿Qué es lo siguiente que debe hacer?

Para continuar configurando su Protección frente a amenazas mediante CDO, consulte la página de inicio de Cisco Defense Orchestrator.

¿Qué es lo siguiente que debe hacer?

CAPÍTULO 6

Implementación de ASA con ASDM

¿Este capítulo es para usted?

Para ver todos los sistemas operativos y administradores disponibles, consulte ¿Qué aplicación y administrador son adecuados para usted?, en la página 1. Este capítulo está dirigido a ASA con ASDM.

Este capítulo no trata las siguientes implementaciones, para las cuales debería consultar la guía de configuración de ASA:

- Recuperación de error
- Configuración de la CLI

Este capítulo también le guía en la configuración de una política de seguridad básica; si tiene requisitos más avanzados, consulte la guía de configuración.

Sobre el firewall

El hardware puede ejecutar el software Protección frente a amenazas o el software ASA. Para cambiar entre Protección frente a amenazas y ASA es necesario que vuelva a crear una imagen para el dispositivo. También es necesario que lleve a cabo una una recreación de imagen si necesita una versión de software diferente a la instalada. Consulte Recreación de la imagen del dispositivo de defensa contra amenazas de Firepower o ASA de Cisco.

El firewall ejecuta un sistema operativo subyacente llamado Cisco Secure Firewall Extensible Operating System (FXOS). El firewall no es compatible con el Administrador del chasis Cisco Secure Firewall de FXOS; solo se admite una CLI limitada para la resolución de problemas. Consulte Guía de resolución de problemas de Cisco FXOS para Firepower 1000/2100 Series que ejecuta Firepower Threat Defense para obtener más información.

Declaración de recopilación de privacidad: el firewall no necesita ni recopila de forma activa información de identificación personal. Sin embargo, puede utilizar información de identificación personal en la configuración, por ejemplo, para los nombres de usuario. En este caso, un administrador podrá ver esta información cuando trabaje con la configuración o cuando utilice SNMP.

Acerca de ASA

El ASA proporciona funciones avanzadas de firewall con estado y concentrador VPN en un solo dispositivo.

Puede administrar el ASA mediante uno de los siguientes administradores:

- ASDM (se trata en esta guía): un administrador de dispositivos único incluido en el dispositivo.
- CLI
- CDOf: un administrador de múltiples dispositivos simplificado y basado en la nube
- Cisco Security Manager: un administrador de varios dispositivos en un servidor independiente.

También puede acceder a la CLI de FXOS para solucionar problemas.

Características no compatibles

Características generales de ASA no compatibles

Las siguientes características de ASA no son compatibles con Firepower 1010:

- Modo de múltiples contextos
- Activa/conmutación por error activa
- Interfaces redundantes
- Clustering
- API REST de ASA
- Módulo de ASA FirePOWER
- Filtrado de tráfico Botnet
- Las siguientes inspecciones:
  - Mapas de inspección de SCTP (se admite la inspección de estado de SCTP mediante ACL)
  - Diámetro
  - GTP/GPRS

Características no compatibles de la interfaz VLAN y del puerto de switch

Las interfaces VLAN y los puertos de switch no son compatibles con:

- Routing dinámico
- Routing multidifusión

- Routing basado en políticas
- Routing de trayectoria múltiple de igual coste (ECMP)
- Conjuntos en línea o interfaces pasivas
- VXLAN
- EtherChannels
- Conmutación por error y enlace de estado
- Zonas de tráfico
- Etiquetado del grupo de seguridad (SGT)

Migración de una configuración ASA 5500-X

Puede copiar y pegar una configuración ASA 5500-X en Firepower 1010. Sin embargo, deberá modificar su configuración. Tenga en cuenta también algunas diferencias de comportamiento entre las plataformas.

1. Para copiar la configuración, introduzca el comando **more system:running-config** en el ASA 5500-X.
2. Edite la configuración según sea necesario (ver a continuación).
3. Conéctese al puerto de consola de Firepower 1010 y acceda al modo de configuración global:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Borre la configuración actual con el comando **clear configure all**.
5. Pegue la configuración modificada en la CLI del ASA.

Esta guía asume una configuración predeterminada de fábrica, por lo que si pega una configuración existente, algunos de los procedimientos de esta guía no se aplicarán a su ASA.

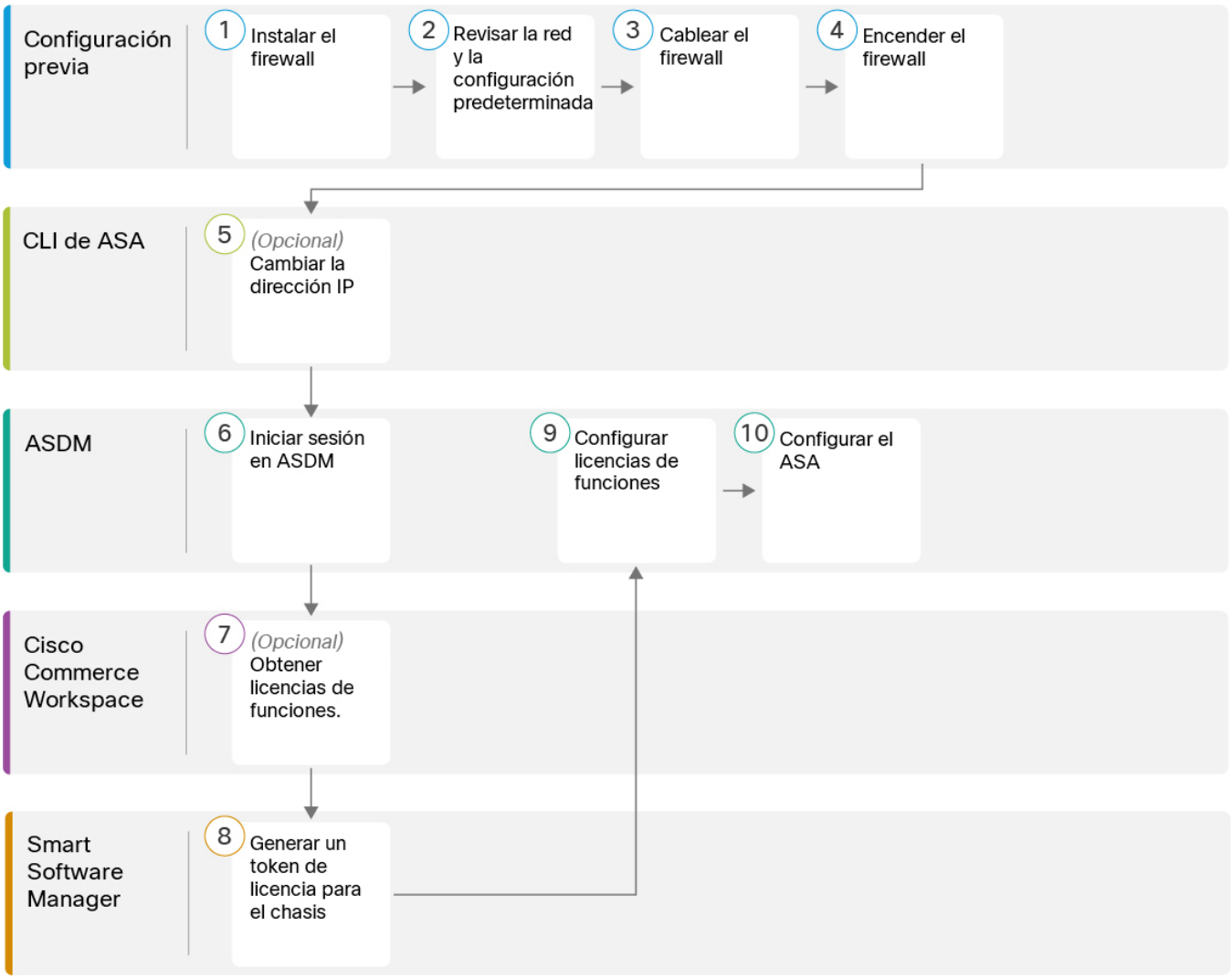
Configuración ASA 5500-X	Configuración de Firepower 1010

Interfaces de firewall Ethernet 1/2 a 1/8	Puertos de switch Ethernet 1/2 a 1/8
	De forma predeterminada, estos puertos Ethernet están configurados como puertos de switch. Para cada interfaz de su configuración, agregue el comando **no switchport** para convertirlas en interfaces de firewall normales. Por ejemplo:
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

Configuración ASA 5500-X	Configuración de Firepower 1010
Licencia PAK	Smart License Las licencias PAK no se aplican al copiar y pegar la configuración. No hay licencias instaladas de forma predeterminada. Smart Licensing requiere que se conecte al servidor de Smart Licensing para obtener sus licencias. Smart Licensing también afecta al acceso de ASDM o SSH (ver a continuación).
Acceso inicial de ASDM	Elimine cualquier VPN u otra configuración de funciones de cifrado seguro, incluso si solo ha configurado un cifrado débil, si no puede conectarse a ASDM o registrarse en el servidor de Smart Licensing. Puede volver a activar estas funciones después de obtener la licencia de cifrado seguro (3DES). El motivo de este problema es que el ASA incluye la capacidad de 3DES de forma predeterminada solo para el acceso a la administración. Si activa una función de cifrado fuerte, el tráfico de ASDM y HTTPS (por ejemplo, hacia y desde el servidor de Smart Licensing) se bloquea. La excepción a esta regla es si está conectado a una interfaz de solo administración, como la Administración 1/1. SSH no se ve afectado.
ID de la interfaz	Asegúrese de cambiar las ID de la interfaz para que coincidan con las nuevas ID de hardware. Por ejemplo, el ASA 5525-X incluye Administración 0/0 y GigabitEthernet 0/0 a 0/5. Firepower 1120 incluye Administración 1/1 y Ethernet 1/1 a 1/8.
boot system comandos El ASA 5500-X permite hasta cuatro comandos **boot system** para especificar la imagen de arranque que se utilizará.	El Firepower 1010 solo permite un comando **boot system**, por lo que debe eliminar todos los comandos excepto uno antes de pegarlo. En realidad, no necesita tener un comando **boot system** *cualquiera* presente en la configuración, ya que no se lee en el inicio para determinar la imagen de arranque. La última imagen de arranque cargada siempre se ejecutará tras la recarga. El comando **boot system** realiza una acción cuando lo introduce: el sistema valida y desempaqueta la imagen y la copia en la ubicación de arranque (una ubicación interna en el disco 0 administrada por FXOS). La nueva imagen se cargará cuando vuelva a cargar el ASA.

Procedimiento completo

Consulte las siguientes tareas para implementar el ASA en su chasis.



1	Configuración previa	Instale el firewall. Consulte la guía de instalación del hardware.
2	Configuración previa	Revisar la implementación de la red y la configuración predeterminada, en la página 176.
3	Configuración previa	Cablear el dispositivo, en la página 179.
4	Configuración previa	Encender el firewall, en la página 13
5	CLI de ASA	(Opcional) Cambiar la dirección IP, en la página 181.
6	ASDM	Iniciar sesión en ASDM, en la página 182.

7	Cisco Commerce Workspace	Configurar licencias, en la página 183: obtener licencias de funciones.
8	Smart Software Manager	Configurar licencias, en la página 183: generar un token de licencia para el chasis.
9	ASDM	Configurar licencias, en la página 183: configurar las licencias de funciones.
10	ASDM	Configurar el ASA, en la página 187.

Revisar la implementación de la red y la configuración predeterminada

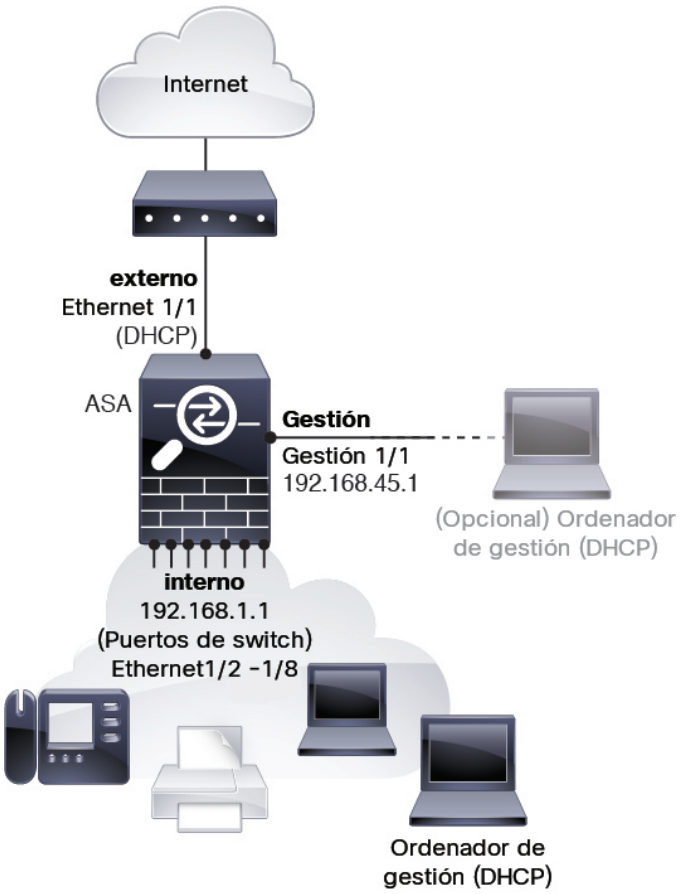
La siguiente figura muestra la implementación de red predeterminada para Firepower 1010 con la configuración predeterminada.

Si conecta la interfaz externa directamente a un cable módem o un módem DSL, recomendamos poner el módem en modo puente para que el ASA lleve a cabo todas las rutas y las NAT para las redes internas. Si necesita configurar PPPoE para que la interfaz externa se conecte a su ISP, puede hacerlo como parte del asistente de configuración inicial de ASDM.

Nota Si no puede utilizar la dirección IP de administración predeterminada para el acceso a ASDM, puede establecer la dirección IP de administración en la CLI del ASA. Consulte (Opcional) Cambiar la dirección IP, en la página 181.

Si necesita cambiar la dirección IP interna, puede hacerlo utilizando el asistente de instalación de ASDM. Por ejemplo, puede ser necesario cambiar la dirección IP interna si:

- Si la interfaz externa intenta obtener una dirección IP en la red 192.168.1.0, que es una red predeterminada común, la concesión DHCP provocará un error y la interfaz externa no obtendrá una dirección IP. Este problema ocurre porque ASA no puede tener dos interfaces en la misma red. En este caso, debe cambiar la dirección IP interna para que esté en una nueva red.
- Si agrega ASA a una red interna existente, tendrá que cambiar la dirección IP interna para que esté en esa red.



Configuración predeterminada de Firepower 1010

La configuración predeterminada de fábrica para Firepower 1010 es la siguiente:

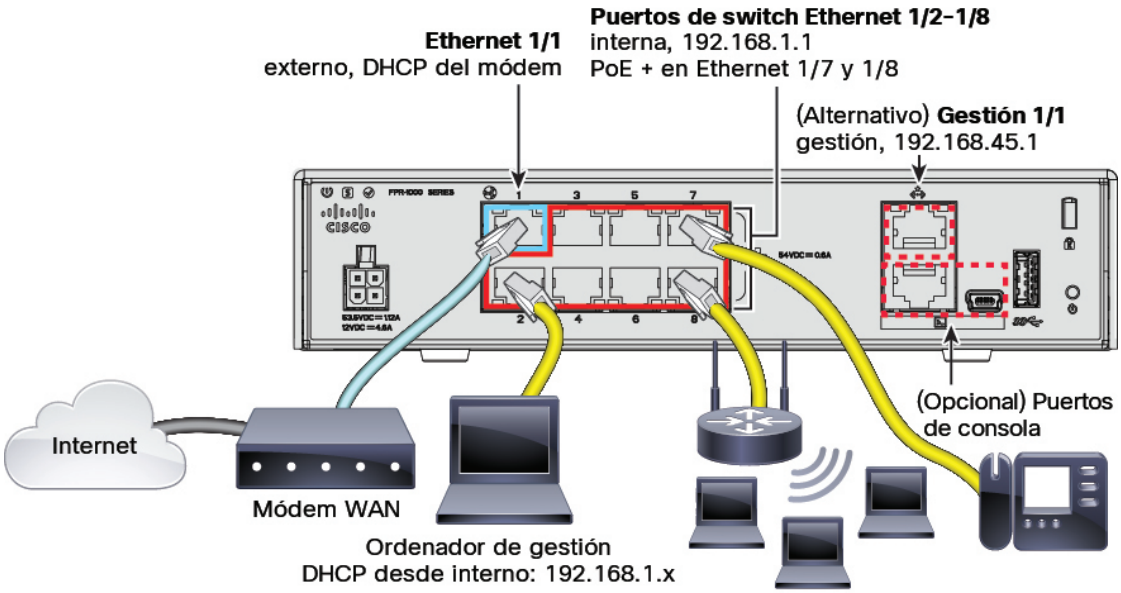
- **Switch de hardware**: Ethernet 1/2 a 1/8 que pertenece a VLAN 1
- flujo de tráfico **interior** → **exterior**: Ethernet 1/1 (exterior), VLAN1 (interior)
- **administración**: administración 1/1 (gestión), dirección IP 192.168.45.1
- **dirección IP externa** desde DHCP, dirección IP interna: 192.168.1.1
- **Servidor DHCP** en la interfaz interna, interfaz de gestión
- **Ruta predeterminada** del DHCP externo
- Acceso **ASDM**: se permiten hosts internos y de administración. Los hosts de administración están limitados a la red 192.168.45.0/24 y los hosts internos están limitados a la red 192.168.1.0/24.
- **NAT**: interfaz PAT para todo el tráfico de interno a externo.
- Servidores **DNS**: los servidores OpenDNS están previamente configurados.

La configuración se trata de los siguientes comandos:

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cablear el dispositivo



Administre Firepower 1010 en Gestión 1/1 o en Ethernet 1/2 a 1/8 (puertos internos del switch). La configuración predeterminada también configura Ethernet 1/1 como externa.

Procedimiento

Paso 1 Instale su hardware y familiarícese con él siguiendo la guía de instalación del hardware.

Paso 2 Conecte su equipo de administración a una de las siguientes interfaces:

- Ethernet 1/2 a 1/8: conecte el ordenador de gestión directamente a uno de los puertos internos del switch (Ethernet 1/2 a 1/8). La interfaz interna tiene una dirección IP predeterminada (192.168.1.1) y también ejecuta un servidor DHCP para proporcionar direcciones IP a los clientes (incluido el equipo de administración), por lo que debe asegurarse de que estas configuraciones no entren en conflicto con

ninguna configuración de red interna existente (consulte Configuración predeterminada de Firepower 1010, en la página 177).

- Gestión 1/1: conecte el equipo de gestión directamente a la gestión 1/1. O conecte Gestión 1/1 a su red de gestión; asegúrese de que el equipo de administración esté en la red de administración, ya que solo los clientes de esa red pueden acceder al ASA. Gestión 1/1 tiene una dirección IP predeterminada (192.168.45.1) y también ejecuta un servidor DHCP para proporcionar direcciones IP a los clientes (incluido el equipo de administración), por lo que debe asegurarse de que estas configuraciones no entren en conflicto con ninguna configuración de red de gestión existente (consulte Configuración predeterminada de Firepower 1010, en la página 177).

  Si necesita cambiar la dirección IP de gestión 1/1 predeterminada, también debe conectar su equipo de administración al puerto de consola. Consulte (Opcional) Cambiar la dirección IP, en la página 181.

Paso 3 Conecte la red externa a la interfaz Ethernet 1/1.

Para licencias Smart Software, ASA necesita acceso a Internet para poder acceder a la autoridad de la licencia.

Paso 4 Conecte los dispositivos internos a los puertos internos del switch que quedan, Ethernet 1/2 a 1/8.

Ethernet 1/7 a 1/8 son puertos PoE+.

Encender el firewall

La alimentación del sistema se controla mediante el cable de alimentación; no hay botón de encendido.

Nota La primera vez que inicie la Protección frente a amenazas, el arranque puede llevar entre 15 y 30 minutos aproximadamente.

Antes de empezar

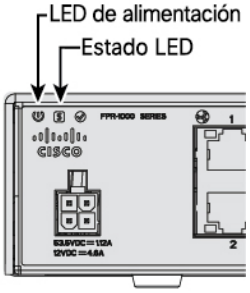
Es importante que proporcione una alimentación fiable para su dispositivo (con una fuente de alimentación ininterrumpida (UPS), por ejemplo). Si se pierde la fuente de alimentación sin apagar primero se pueden provocar daños graves en el sistema de archivos. Hay muchos procesos que se ejecutan en segundo plano todo el tiempo y, si se pierde la fuente de alimentación, el sistema no se puede apagar adecuadamente.

Procedimiento

Paso 1 Conecte el cable de alimentación al dispositivo y conéctelo a una toma eléctrica.

La alimentación se activa automáticamente cuando conecta el cable de alimentación.

Paso 2 Compruebe el LED de encendido en la parte posterior o superior del dispositivo. Si está iluminado en verde fijo, el dispositivo está encendido.



Paso 3 Compruebe el LED de estado en la parte posterior o superior del dispositivo. Después de estar iluminado en verde fijo, el sistema ha pasado el diagnóstico de encendido.

(Opcional) Cambiar la dirección IP

Si no puede utilizar la dirección IP predeterminada para acceder a ASDM, puede establecer la dirección IP de la interfaz de gestión en la CLI del ASA.

Nota Este procedimiento restaura la configuración predeterminada y establece la dirección IP que haya elegido, por lo que si realizó algún cambio en la configuración de ASA que desea conservar, no lo lleve a cabo.

Procedimiento

Paso 1 Conéctese al puerto de consola del ASA e introduzca el modo de configuración global. Consulte Acceder a ASA y a CLI de FXOS, en la página 189 para obtener más información.

Paso 2 Restaure la configuración predeterminada con la dirección IP elegida.

configure factory-default [*dirección_ip* [*máscara*]]

Ejemplo:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
```

```
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Paso 3 Guarde la configuración predeterminada en la memoria flash.

write memory

Iniciar sesión en ASDM

Inicie ASDM para poder configurar ASA.

El ASA incluye la función 3DES de manera predeterminada solo para el acceso a la administración, por lo que puede conectarse al Smart Software Manager y utilizar el ASDM de manera inmediata. Además, también puede utilizar el SSH y SCP si más tarde configura el acceso SSH en el ASA. Otras funciones que requieren cifrado seguro (como el VPN) deben tener el cifrado seguro activado, para lo que es necesario registrarse en el Smart Software Manager.

Nota Si intenta configurar cualquier función que pueda utilizar el cifrado seguro antes de registrarse, incluso aunque solo configure el cifrado débil, se interrumpirá su conexión HTTPS en esa interfaz y no podrá volver a conectarse. La excepción a esta regla es si está conectado a una interfaz de solo administración, como la Administración 1/1. SSH no se ve afectado. Si pierde su conexión HTTPS, puede conectarse al puerto de la consola para reconfigurar el ASA, conectarse a una interfaz de solo gestión, o conectarse a una interfaz que no esté configurada para la función de cifrado seguro.

Antes de empezar

- Consulte las notas de la versión de ASDM en Cisco.com para conocer los requisitos para ejecutar ASDM.

Procedimiento

Paso 1 Introduzca la siguiente URL en su navegador.

- **https://192.168.1.1**: dirección IP de la interfaz interna Puede conectarse a la dirección interna en cualquier puerto interno del switch (Ethernet1/2 a 1/8).
- **https://192.168.45.1**: dirección IP de la interfaz de administración.

Nota Asegúrese de especificar **https://** y no **http://** o solo la dirección IP (que por defecto es HTTP); el ASA no reenvía automáticamente una solicitud HTTP a HTTPS.

Aparece la página web de **Cisco ASDM**. Es posible que vea advertencias de seguridad del navegador porque el ASA no tiene un certificado instalado; puede ignorar estas advertencias y visitar la página web.

Paso 2 Haga clic en una de las opciones disponibles: **Instalar iniciador de ASDM** o **Ejecutar ASDM**.

Paso 3 Siga las instrucciones de la pantalla al iniciar ASDM según la opción que haya seleccionado.

Aparece el **iniciador de Cisco ASDM-IDM**.

Paso 4 Deje los campos de nombre de usuario y contraseña vacíos y haga clic en **OK**.

Aparece la ventana de ASDM principal.

Configurar licencias

El ASA utiliza Smart Licensing. Puede utilizar el Smart Licensing convencional, que requiere acceso a Internet; o puede configurar una reserva de licencia permanente o un Smart Software Manager local (antes conocido como servidor satélite) para la administración sin conexión. Para obtener más información acerca de estos métodos de licencias sin conexión, consulte Funciones de las licencias de la serie ASA de Cisco; esta guía hace referencia a las licencias Smart regulares.

Para obtener una descripción general más detallada sobre Cisco Licensing, visite cisco.com/go/licensingguide

Cuando registra el chasis, el Smart Software Manager emite un certificado de ID para la comunicación entre el firewall y el Smart Software Manager. También asigna el firewall a la cuenta virtual apropiada. no podrá hacer cambios en la configuración hasta que se registre con el Smart Software Managerde las funciones que requieran funciones especiales se verá considerablemente afectado a pesar de que las operaciones no se vean afectadas. Las funciones con licencia son:

- Estándar
- Security Plus: para conmutación por error activa/en espera
- Cifrado seguro (3DES/AES): si su cuenta Smart no está autorizada para el cifrado seguro, pero Cisco ha decidido que le permite utilizar el cifrado seguro, puede añadir una licencia de cifrado seguro manualmente a su cuenta.
- AnyConnect: AnyConnect Plus, AnyConnect Apex o AnyConnect solo VPN.

El ASA incluye la función 3DES de manera predeterminada solo para el acceso a la administración, por lo que puede conectarse al Smart Software Manager y utilizar el ASDM de manera inmediata. Además, también puede utilizar el SSH y SCP si más tarde configura el acceso SSH en el ASA. Otras funciones que requieren cifrado seguro (como el VPN) deben tener el cifrado seguro activado, para lo que es necesario registrarse en el Smart Software Manager.

Nota Si intenta configurar cualquier función que pueda utilizar el cifrado seguro antes de registrarse, incluso aunque solo configure el cifrado débil, se interrumpirá su conexión HTTPS en esa interfaz y no podrá volver a conectarse. La excepción a esta regla es si está conectado a una interfaz de solo administración, como la Administración 1/1. SSH no se ve afectado. Si pierde su conexión HTTPS, puede conectarse al puerto de la consola para reconfigurar el ASA, conectarse a una interfaz de solo gestión, o conectarse a una interfaz que no esté configurada para la función de cifrado seguro.

Cuando solicite el token de registro para el ASA desde el Smart Software Manager, marque la casilla de verificación **Permitir la funcionalidad controlada por exportación de los productos registrados con este token** para que se aplique la licencia de cifrado seguro completa (su cuenta debe cumplir los requisitos). La licencia de cifrado sólido se activa automáticamente para los clientes que cumplan los requisitos cuando se aplica el token de registro en el chasis, por lo que no es necesario hacer nada más. Si su cuenta Smart no está autorizada para el cifrado seguro, pero Cisco ha decidido que le permite utilizar el cifrado seguro, puede añadir una licencia de cifrado seguro manualmente a su cuenta.

Antes de empezar

- Tener una cuenta principal en Smart Software Manager.

  Si aún no tiene una cuenta, haga clic en el enlace para configurar una nueva cuenta. Smart Software Manager le permite crear una cuenta principal para su organización.

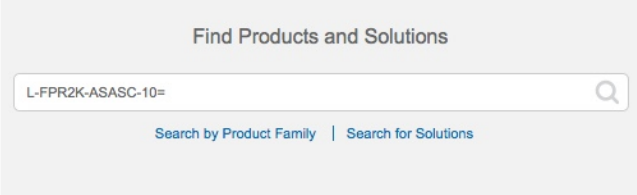
- Su cuenta de Smart Software Manager debe cumplir con los requisitos de la segura licencia de encriptado (3DES/AES) para poder utilizar algunas funciones (que se activan mediante el indicador de cumplimiento de exportación).

Procedimiento

Paso 1 Compruebe que su cuenta de licencias Smart contenga las licencias disponibles que necesita, incluso lo mínimo para la licencia estándar.

Cuando adquirió su dispositivo en Cisco o en un distribuidor, sus licencias deberían haberse vinculado a su cuenta de Smart Software Manager. Sin embargo, si necesita agregar licencias usted mismo, utilice el campo de búsqueda **Buscar productos y soluciones** en Cisco Commerce Workspace. Busque las siguientes PID de licencia:

Figura 54: Búsqueda de licencia

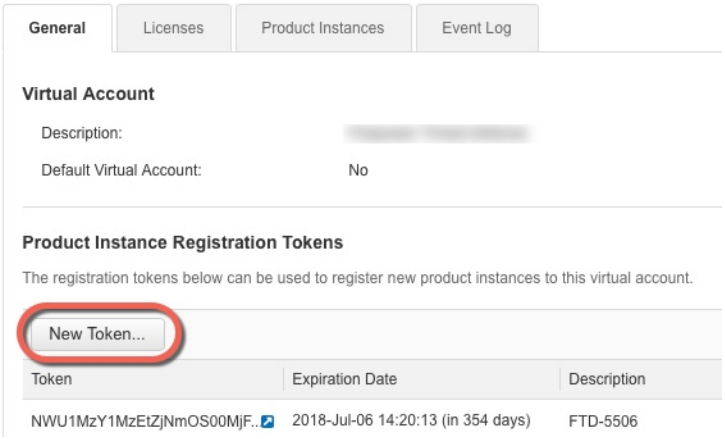


- Licencia estándar: L-FPR1000-ASA=. La licencia estándar es gratuita, pero debe agregarla a su cuenta de licencias Smart Software.
- Licencia Security Plus: L-FPR1010-SEC-PL=. La licencia Security Plus permite la conmutación por error.
- Licencia de cifrado sólido (3DES/AES): L-FPR1K-ENC-K9=. Solo es necesario si su cuenta no está autorizada para un cifrado seguro.
- Anyconnect: consulte la Guía de pedidos de Cisco AnyConnect. No active esta licencia directamente en el ASA.

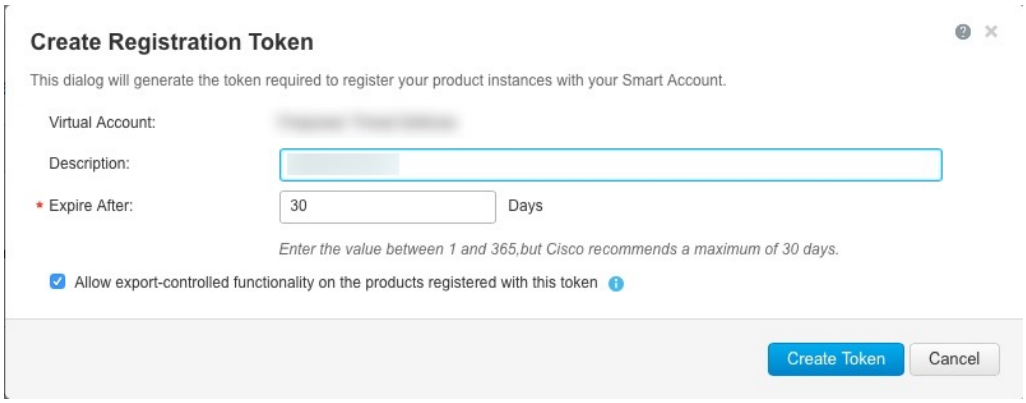
Paso 2 En el Cisco Smart Software Manager, solicite y copie un token de registro para la cuenta virtual a la que desea agregar este dispositivo.

a) Haga clic en **Inventario**.

b) En la pestaña **General**, haga clic en **Nuevo token**.



c) En el cuadro de diálogo **Crear token de registro**, introduzca la siguiente configuración y haga clic en **Crear token**:



- **Descripción**
- **Caduca después de**: Cisco recomienda 30 días.
- **Permitir la funcionalidad controlada por la exportación en los productos registrados con este token**: activa el indicador de cumplimiento de la exportación.

El token se agrega a su inventario.

d) Haga clic en el icono de la flecha hacia la derecha del token para abrir el cuadro de diálogo **Token** para poder copiar el ID del token en el portapapeles. Deje este token preparado para usarlo más adelante en el procedimiento cuando necesite registrar el ASA.

Figura 55: Ver token

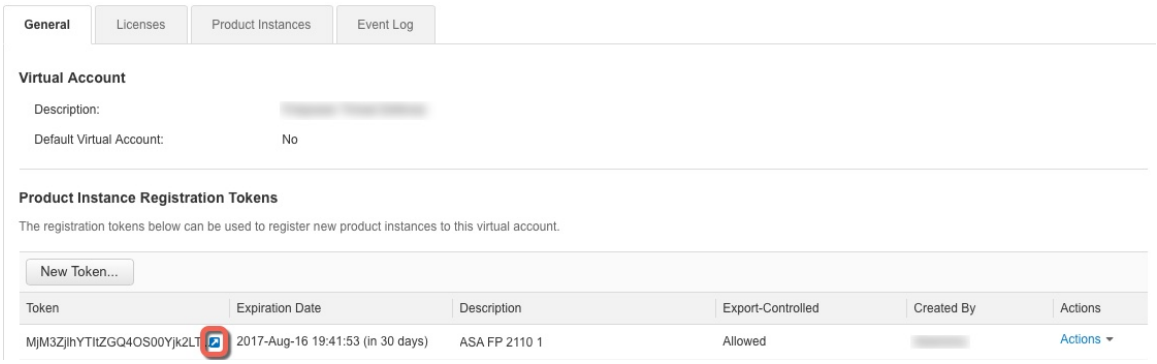
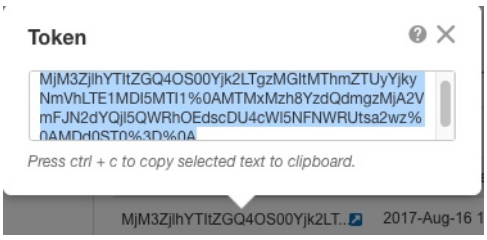


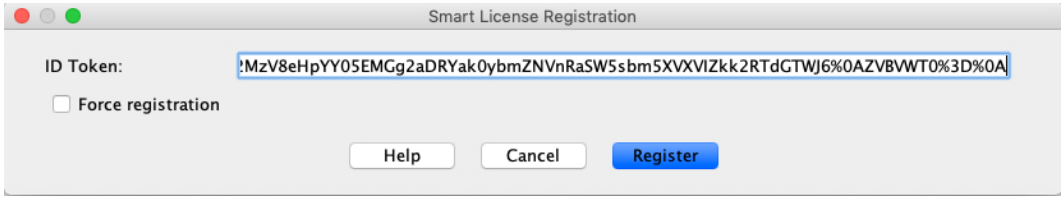
Figura 56: Copiar token



Paso 3 En ASDM, seleccione **Configuración** > **Administración de dispositivos** > **Licencias** > **Licencias Smart**.

Paso 4 Haga clic en **Registrar**.

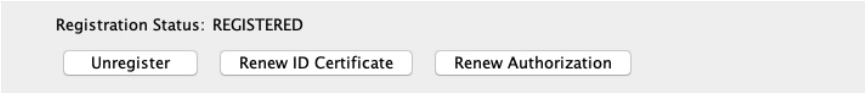
Paso 5 Introduzca el token de registro en el campo **ID de token**.



También puede marcar la casilla de verificación **Forzar registro** para registrar el ASA que ya está registrado, pero que puede que no esté sincronizado con el Smart Software Manager. Por ejemplo, utilice **Forzar registro** si se eliminó accidentalmente el ASA de Smart Software Manager.

Paso 6 Haga clic en **Registrar**.

El ASA se registra en el Smart Software Manager mediante la interfaz externa preconfigurada, y solicita autorización para los derechos de licencia configurados. El Smart Software Manager también aplica la licencia de cifrado seguro (3DES/AES) si su cuenta lo permite. ASDM actualiza la página cuando se actualiza el estado de la licencia. También puede seleccionar **Monitorizar** > **Propiedades** > **Licencia Smart** para comprobar el estado de la licencia, sobre todo si el registro da error.



Paso 7 Establezca los siguientes parámetros:

a) Marque la casilla **Activar configuración de licencia Smart**.

b) En la lista desplegable **Nivel de licencia**, seleccione **Estándar**.

Solo está disponible el nivel estándar.

c) (Opcional) Marque **Activar Security Plus**.

El nivel Security Plus permite la conmutación por error activa/en espera.

Paso 8 Haga clic en **Apply** (Aplicar).

Paso 9 Haga clic en el icono **Guardar** en la barra de herramientas.

Paso 10 Salga de ASDM y vuelva a iniciarlo.

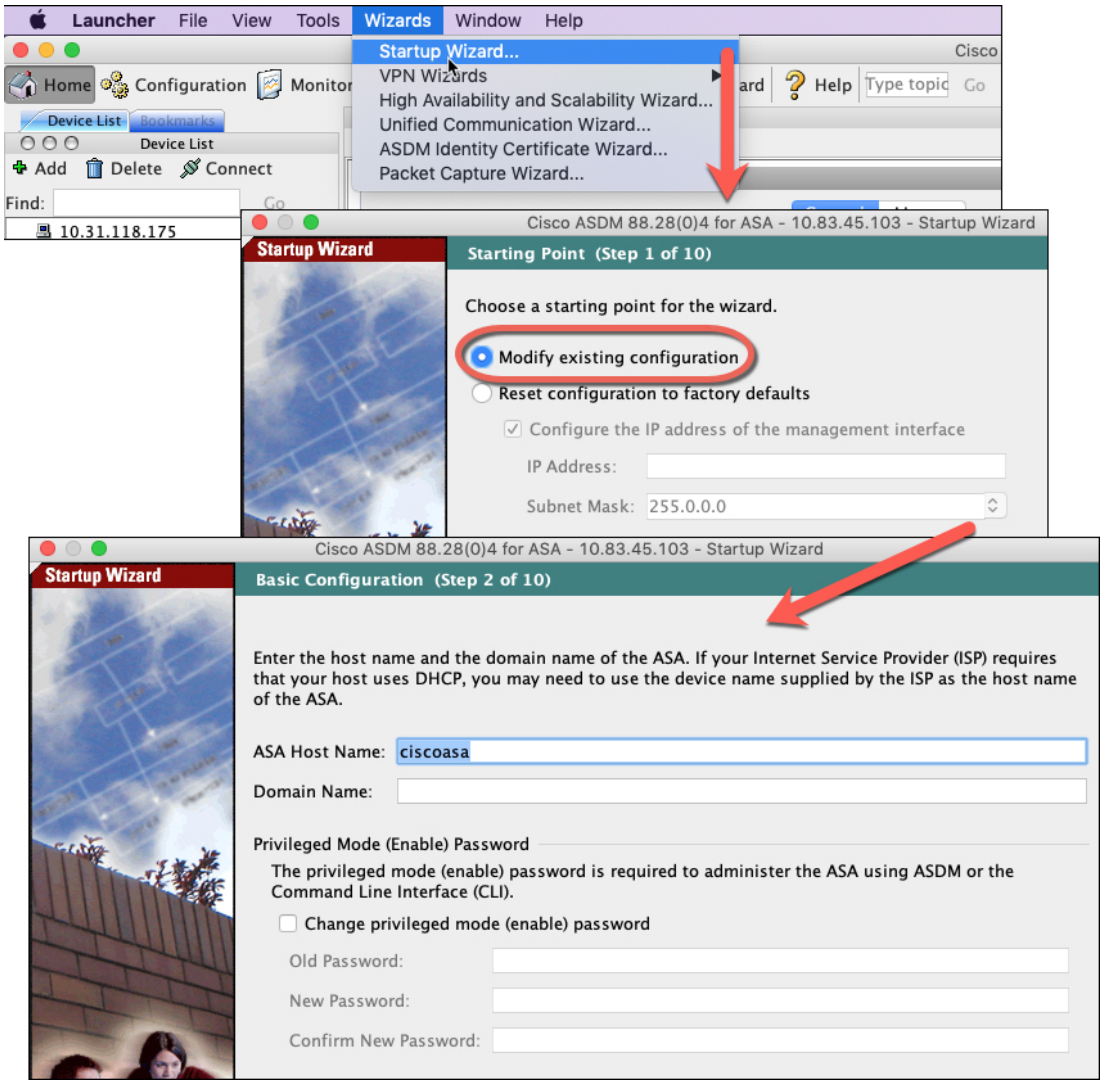
Cuando cambie las licencias, debe reiniciar ASDM para que se muestren las pantallas actualizadas.

Configurar el ASA

Con ASDM, puede utilizar asistentes para configurar las funciones básicas y avanzadas. También puede configurar manualmente las funciones que no estén en los asistentes.

Procedimiento

Paso 1 Seleccione **Asistentes** > **Asistente de inicio** y haga clic en el botón de opción **Modificar configuración existente**.



Paso 2 El **asistente de inicio** le guía a través de la configuración:

- Contraseña de activación
- Interfaces, incluida la configuración de direcciones IP internas y externas, y su activación.
- Rutas estáticas
- El servidor DHCP
- Y mucho más...

Paso 3 (Opcional) Desde el menú **Asistentes**, ejecute otros asistentes.

Paso 4 Para continuar con la configuración del ASA, consulte los documentos disponibles para su versión de software en Navegación por la documentación de la serie ASA de Cisco.

Acceder a ASA y a CLI de FXOS

Puede utilizar la CLI de ASA para solucionar problemas o configurar el ASA en lugar de utilizar ASDM. Puede acceder a la CLI conectándose al puerto de consola. Más tarde puede configurar el acceso SSH al ASA en cualquier interfaz; el acceso SSH está desactivado de forma predeterminada. Para obtener más información, consulte la guía de configuración de operaciones generales de ASA.

También puede acceder al CLI de FXOS de la CLI de ASA para solucionar problemas.

Procedimiento

Paso 1 Conecte su ordenador de gestión al puerto de consola. Firepower 1000 va con un cable de serie USB A a B. Instale las unidades USB de serie necesarias para la guía de hardware de su sistema operativo (consulte la guía de hardware de Firepower 1010). Utilice la siguiente configuración de serie:

- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada

Se conecta a la CLI del ASA. No se necesitan credenciales de usuario para acceder a la consola de forma predeterminada.

Paso 2 Acceso al modo EXEC privilegiado.

enable

Se le pedirá que cambie la contraseña la primera vez que introduzca el comando **enable**.

Ejemplo:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

La contraseña de activación que establezca en el ASA también es la contraseña de usuario **administrador** de FXOS si el ASA no se inicia y entra en el modo de protección de FXOS.

Todos los comandos que no sean de configuración están disponibles en el modo EXEC privilegiado. También puede introducir el modo de configuración desde el modo EXEC privilegiado.

Para salir del modo EXEC privilegiado, introduzca el comando **disable**, **exit** o **quit**.

Paso 3 Acceso al modo de configuración global.

configure terminal

Ejemplo:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Puede comenzar a configurar el ASA desde el modo de configuración global. Para salir del modo de configuración global, introduzca el comando **exit**, **quit** o **end**.

Paso 4 (Opcional) Conéctese a CLI de FXOS.

connect fxos [**admin**]

- **admin**: proporciona acceso como administrador. Sin esta opción, los usuarios tienen acceso en modo solo lectura. Tenga en cuenta que no hay comandos de configuración disponibles incluso en el modo de administrador.

No se le piden las credenciales de usuario. El nombre de usuario actual de ASA se pasa a FXOS y no se requiere otro inicio de sesión. Para volver a la CLI del ASA, introduzca **exit** o escriba **Ctrl-Shift-6**, **x**.

Dentro de FXOS, puede ver la actividad del usuario con el comando **scope security/show audit-logs**.

Ejemplo:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

¿Qué es lo siguiente que debe hacer?

- Para continuar configurando su ASA, consulte los documentos disponibles para su versión de software en Navegar por los documentos de la serie ASA de Cisco.
- Para la resolución de problemas, consulte la guía de resolución de problemas de FXOS.