Descodificar la terminología de firewall seguro (para personas nuevas en Firepower)

Contenido

Introducción

Este documento describe diferentes jergas populares de firewall de Cisco. En este documento también se explica cómo puede pasar de un modo CLI a otro.

Prerequisites

Requirements

No hay requisitos previos para aprender este tema.

Componentes Utilizados

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

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Administración de dispositivos Cisco Firepower (FDM)
- Firepower eXtensible Operating System (FXOS)
- Administrador de chasis Firepower (FCM)
- Dispositivo de seguridad adaptable (ASA)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Terminologías técnicas de uso común

FTD: Firepower Threat Defence

FTD es un firewall de última generación que ofrece mucho más que firewalls tradicionales. Incluye servicios como el sistema de prevención de intrusiones (IPS), la protección frente a malware avanzado (AMP), el filtrado de URL, la inteligencia de seguridad, etc. FTD es muy similar a ASA (dispositivo de seguridad adaptable), pero con funcionalidad añadida. FTD funciona en 2 motores, LINA y SNORT.

LINA: arquitectura de red integrada basada en Linux

Nos referimos a ASA como Lina en los dispositivos FTD. LINA no es más que un código ASA en el que se ejecuta FTD. Lina se centra principalmente en la seguridad de la capa de red. Incorpora algunas capacidades de firewall de capa 7 a través de sus funciones de inspección y control de aplicaciones.

SNORT

El motor Snort es un sistema de detección y prevención de intrusiones en la red. Las características clave de snort incluyen inspección de paquetes para identificar anomalías, detección basada en reglas, alertas en tiempo real, registro y análisis, e integración con otras herramientas de seguridad. Snort tiene la capacidad de realizar una inspección L7 (tráfico de capa de aplicación), no solo basándose en un encabezado de paquete, sino también en el contenido de los paquetes.

Tiene la flexibilidad de escribir sus propias reglas personalizadas para definir patrones o firmas específicos en la capa de aplicación, lo que mejora las funciones de detección. Realiza una inspección profunda de paquetes mediante la evaluación de la carga útil de los paquetes. Incluso

puede realizar el descifrado de los paquetes cifrados aquí.

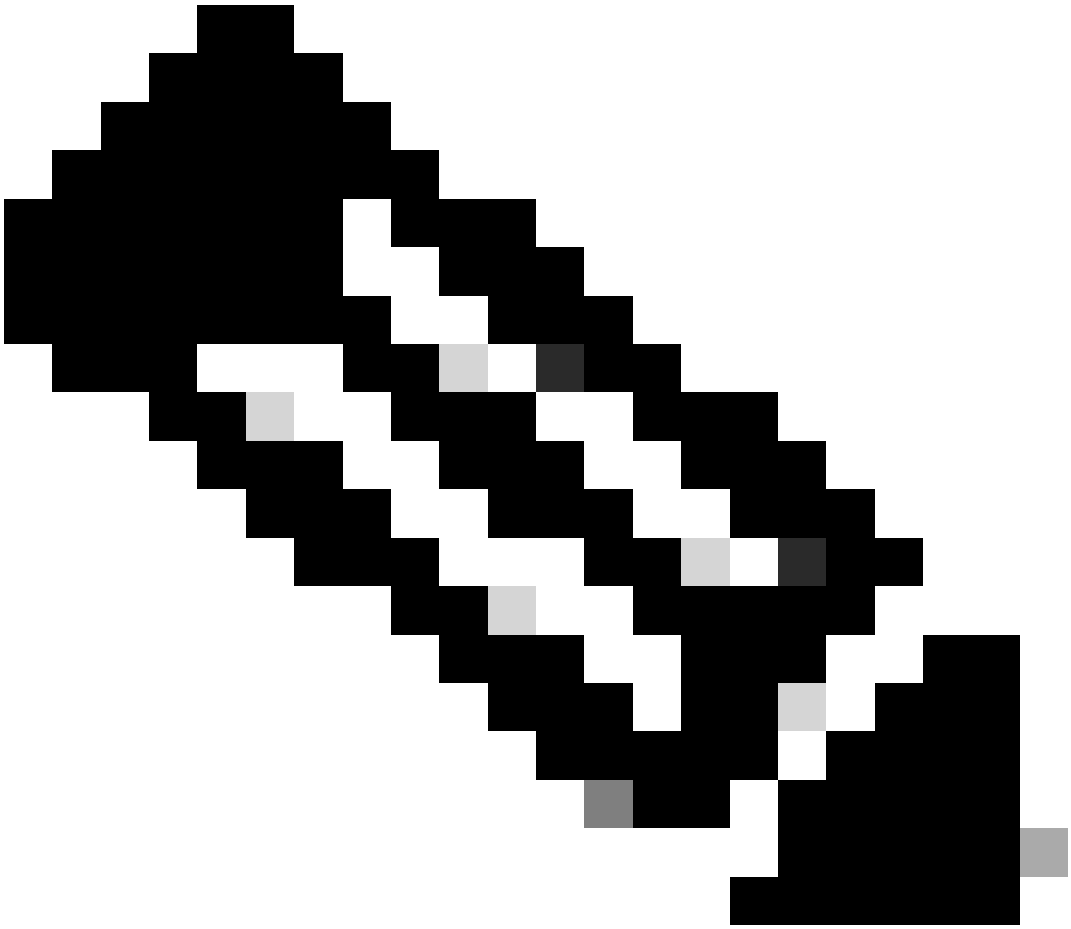
FXOS: sistema operativo ampliable Firepower

Es un sistema operativo en el que se ejecuta el dispositivo FTD. En función de las plataformas, FXOS se utiliza para configurar las funciones, supervisar el estado del chasis y acceder a las funciones avanzadas de solución de problemas.

El FXOS de Firepower 4100/9300 y Firepower 2100 con el software Adaptive Secure Appliance en modo de plataforma permite realizar cambios de configuración, mientras que en otras plataformas, con la excepción de funciones específicas, es de solo lectura.

FCM: administrador de chasis Firepower

FCM es una GUI utilizada para administrar el chasis. Solo está disponible para los modelos 9300, 4100 y 2100 que ejecuten ASA en modo de plataforma.



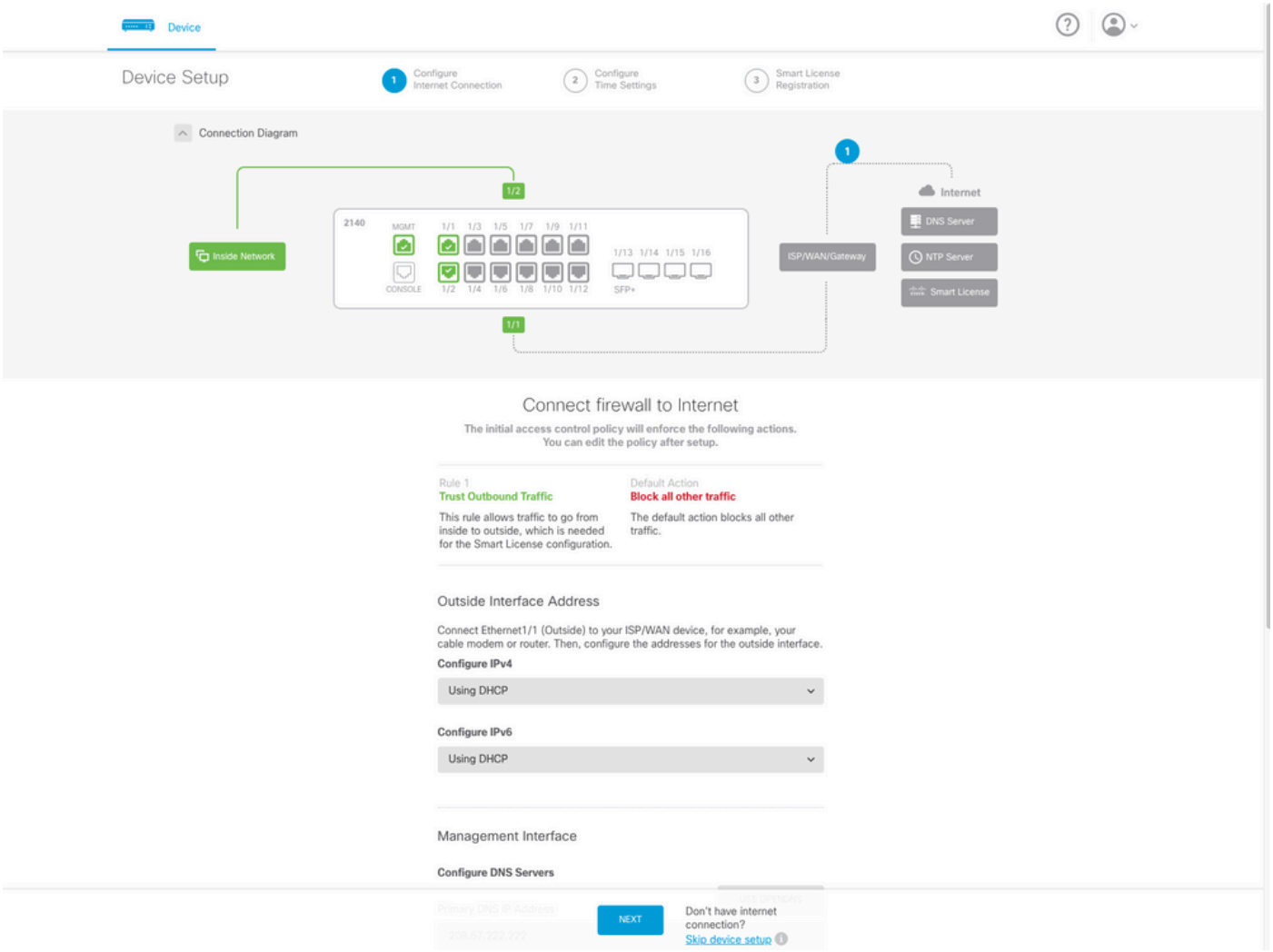
Nota: Puede tomar una analogía de un portátil. FXOS es el sistema operativo (SO

Windows en el portátil), que se ejecuta en el chasis (portátil). Podemos instalar FTD (instancia de aplicación) en él, que se ejecuta en Lina y Snort (componentes).

A diferencia de ASA, no puede administrar FTD a través de CLI. Necesita una gestión independiente basada en GUI. Existen dos tipos de servicios: FDM y FMC.

FDM: gestión de dispositivos Firepower

- FDM es una herramienta de gestión integrada. Proporciona una interfaz basada en Web para configurar, administrar y supervisar las directivas de seguridad y la configuración del sistema.
- Una gran ventaja de utilizar FDM es que no necesita una licencia adicional para ello.
- Solo puede gestionar un FTD con un FDM.

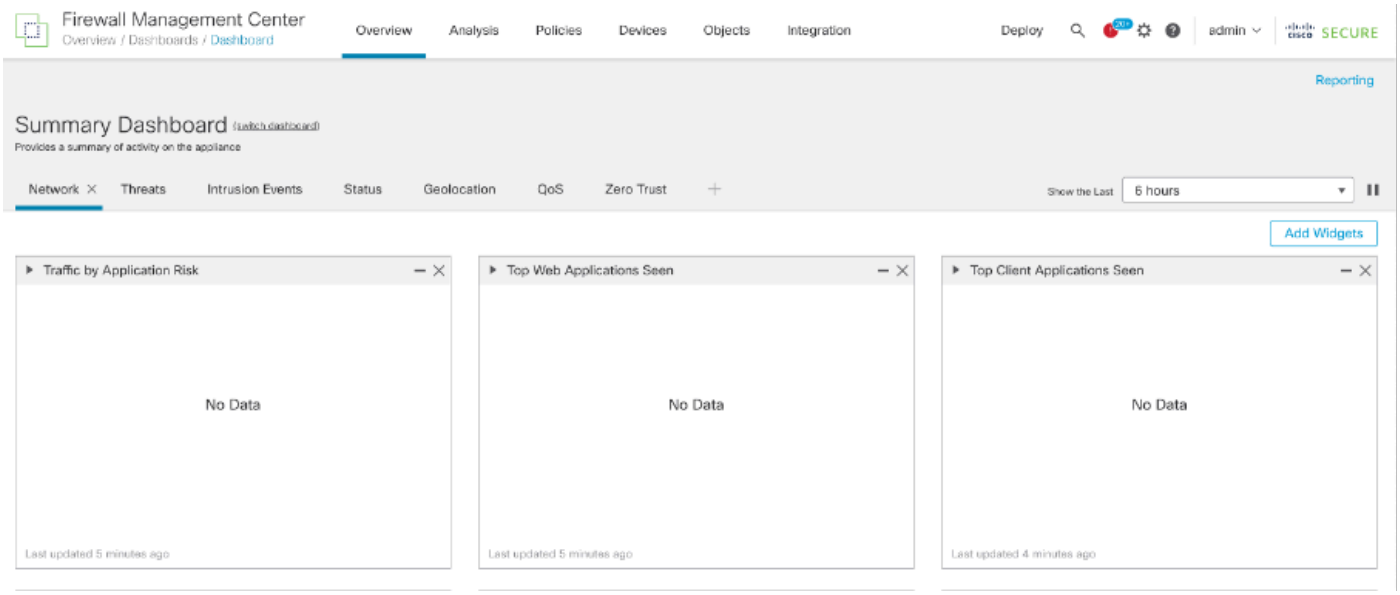


FDM

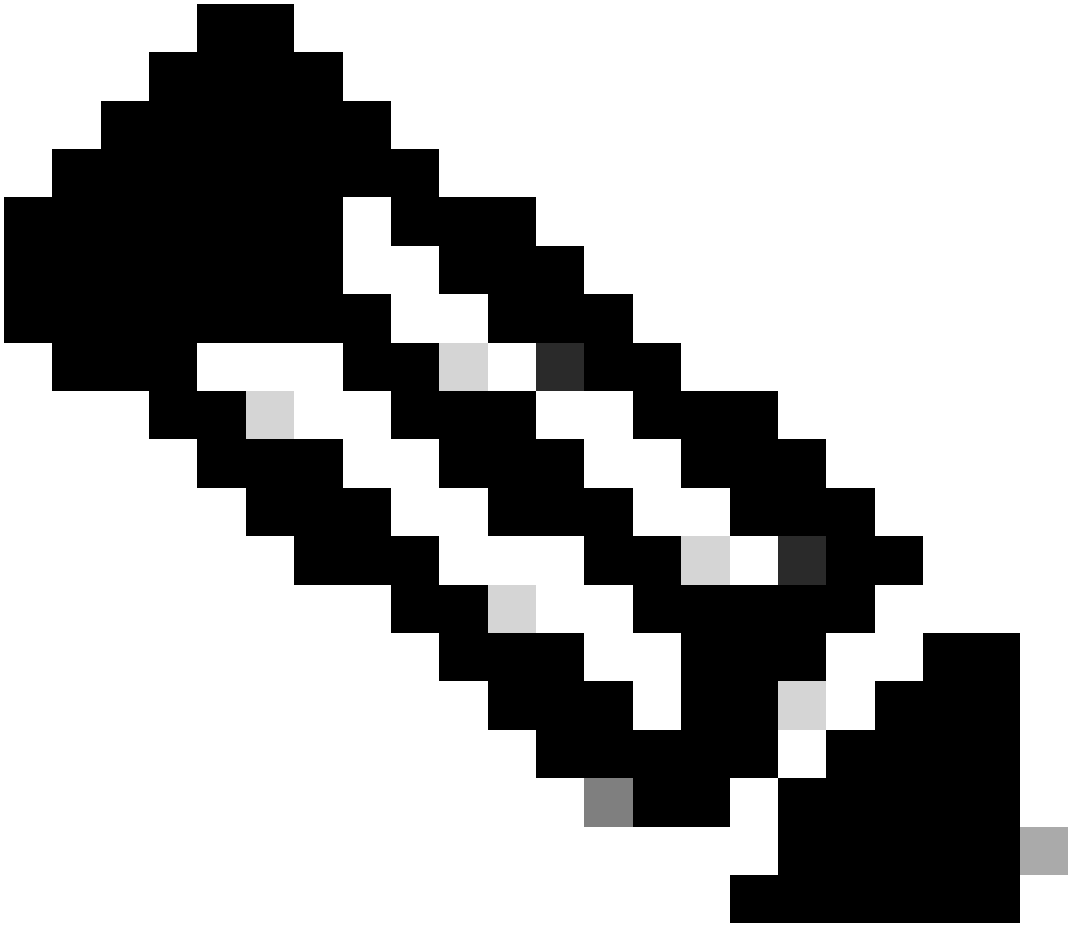
FMC: FirePOWER Management Center

- FMC es una solución de gestión centralizada para dispositivos Cisco FTD, dispositivos Cisco ASA con Firepower Services. También le proporciona una GUI que puede utilizar para configurar, administrar y monitorear dispositivos FTD.

- Puede utilizar un dispositivo FMC de hardware o un dispositivo FMC virtual.
- Esto requiere una licencia independiente para funcionar.
- Un punto positivo de FMC es que puede administrar varios dispositivos FTD con un dispositivo FMC.



FMC



Nota: No puede utilizar tanto el FDM como el FMC para gestionar un dispositivo FTD. Una vez habilitada la gestión integrada de FDM, no es posible utilizar un FMC para gestionar el FTD, a menos que desactive la gestión local y vuelva a configurar la gestión para utilizar un FMC. Por otra parte, si se registra el FTD en un FMC, se desactiva el servicio de gestión integrada de FDM en el FTD.

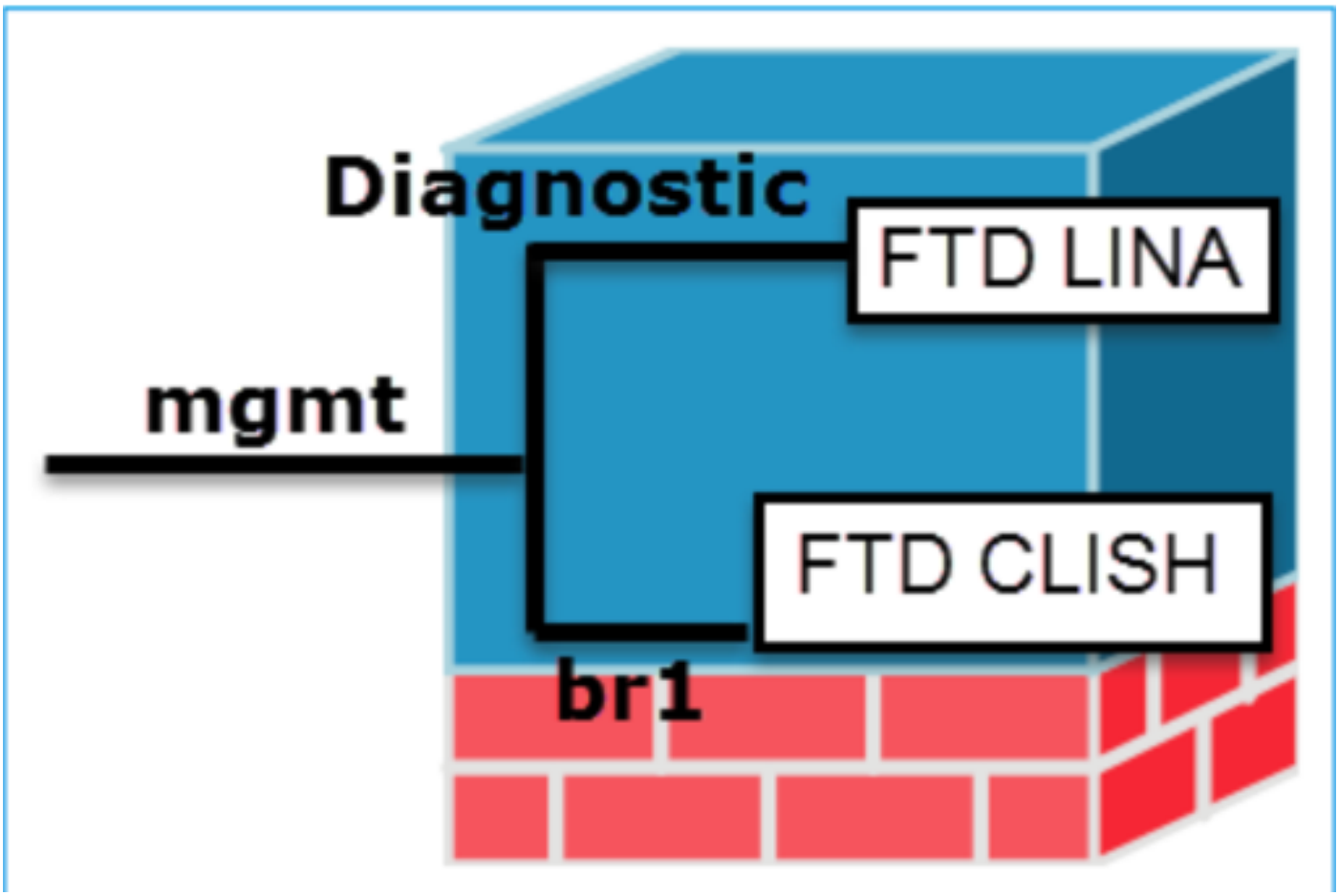
CLISH: Shell de interfaz de línea de comandos

CLISH es una interfaz de línea de comandos utilizada en dispositivos Cisco Firepower Threat Defense (FTD). Puede ejecutar comandos en FTD utilizando este modo CLISH.

GESTIÓN DE DIAGNÓSTICO

Tenemos 2 interfaces de administración en el dispositivo FTD, interfaz de administración de diagnóstico e interfaz de administración FTD. Si tenemos que acceder al motor LINA, utilizamos la interfaz de gestión de diagnóstico. Si tenemos que acceder al motor SNORT, utilizamos la interfaz de gestión de FTD. Ambas son interfaces diferentes y necesitan direcciones IP de interfaz

diferentes.



Interfaces de gestión

Modo de plataforma ASA

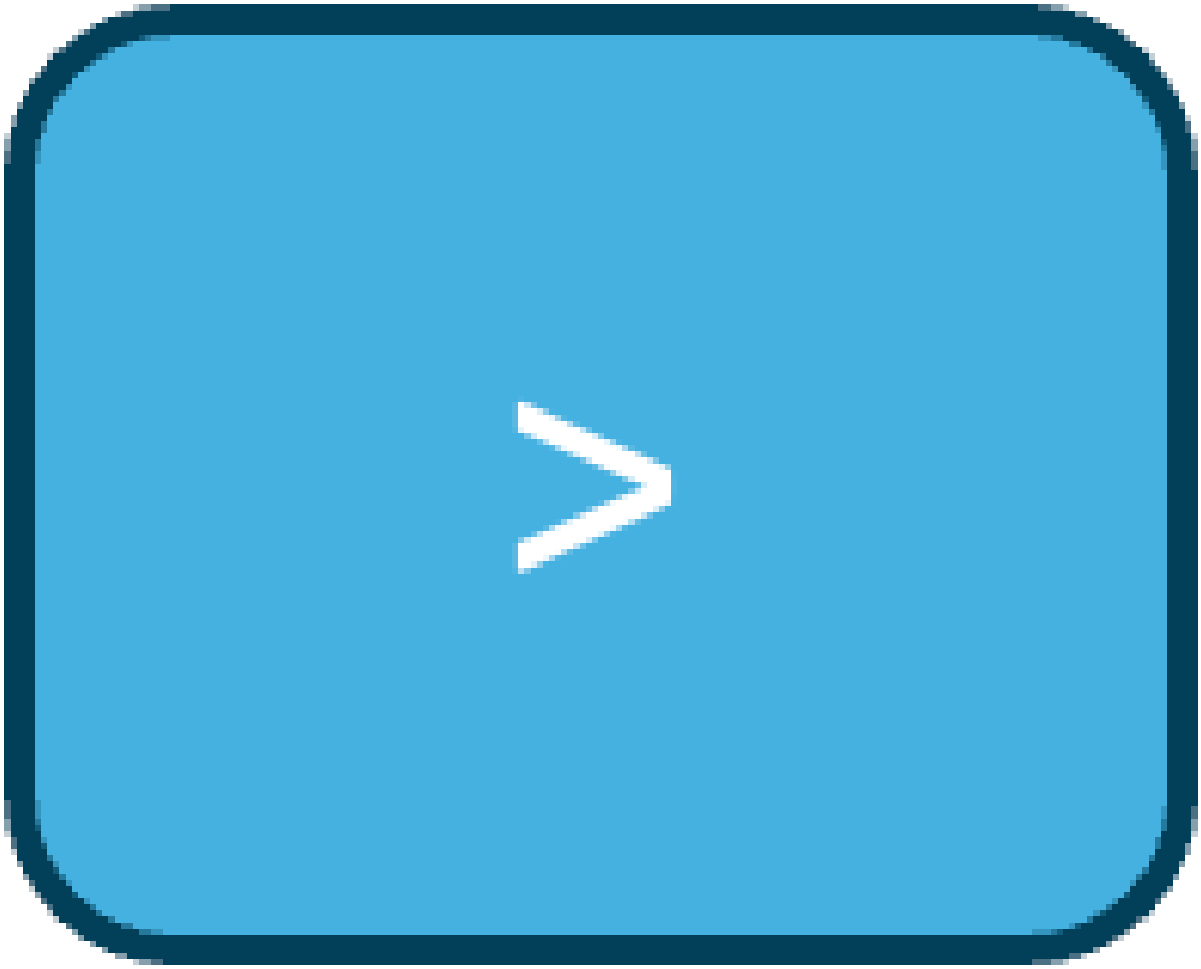
1. En el modo de plataforma, debe configurar parámetros operativos básicos y ajustes de interfaz de hardware en FXOS, como la habilitación de interfaces, el establecimiento de EtherChannels, NTP, la gestión de imágenes y mucho más.
2. Todas las demás configuraciones deben realizarse a través de ASA CLI/ASDM.
3. Tiene acceso a FCM en este ejemplo.

Modo de dispositivo ASA

1. En Firepower 2100, ASA en modo dispositivo se introdujo a partir de la versión 9.13 (incluida).
2. El modo de dispositivo le permite configurar todos los parámetros del ASA. En la CLI de FXOS sólo están disponibles los comandos avanzados de solución de problemas.
3. No hay FCM en este modo.

Mensajes diferentes en FTD

ESCALAR



ESCALAR

Modo raíz/modo experto

Modo Experto

Modo Lina

Modo Lina

Modo FXOS

Modo FXOS

Cómo desplazarse entre distintos avisos

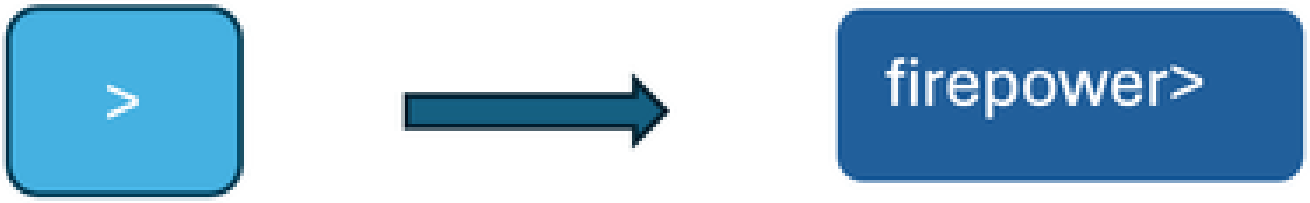
Modo CLISH a modo raíz FTD

Modo de suspensión al modo Experto

```
> expert
```

```
admin@firepower:~$  sudo su
Password:
root@firepower:/home/admin#
```

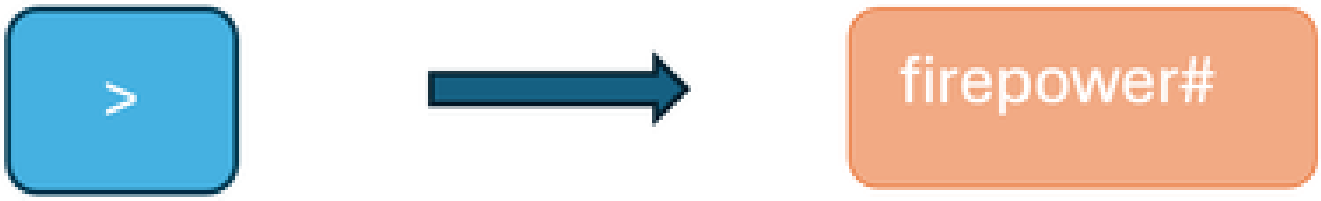
Modo CLISH a modo Lina



Modo de suspensión a modo de línea

```
> system support diagnostic-cli
Attaching to Diagnostic CLI . . . Press 'Ctrl+a then d' to detach .
Type help or '?' for a list of available commands .
firepower> enable
Password :
firepower#
```

Modo CLISH a modo FXOS



Modo de suspensión al modo FXOS

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.
(------ cropped output -------)
firepower#
```

Modo raíz a modo LINA

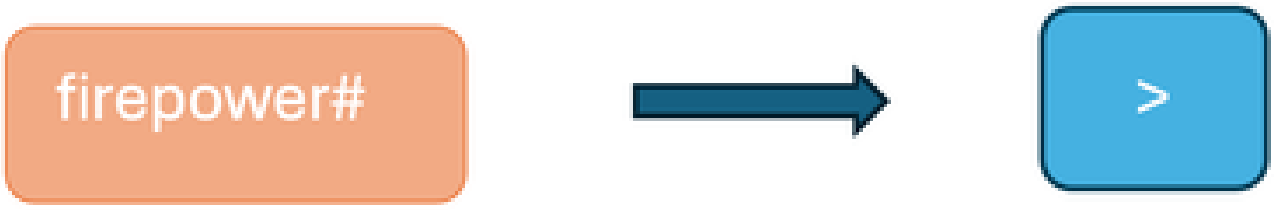
Modo Experto a Línea

```
root@firepower:/home/admin#
root@firepower:/home/admin#   exit
exit
admin@firepower:~$ exit
logout
>
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

or

```
root@firepower:/home/admin#
root@firepower:/home/admin#   sfconsole
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

FXOS a modo FTD CLISH (dispositivo serie 1000/2100/3100)



FXOS a modo de suspensión

```
firepower# connect ftd
>
To exit the fxos console
> exit
firepower#
```

FXOS a modo FTD CLISH (dispositivo serie 4100/9300)

Este ejemplo muestra cómo conectarse a la CLI de defensa contra amenazas en el módulo 1:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1> connect ftd
>
```

Salga de la consola:

Ingrese ~, luego quit para salir de la aplicación Telnet.

```
Example:
>exit
Firepower-module1> ~
telnet> quit
firepower#
```

Documentos Relacionados

Para obtener más información sobre los diversos comandos que puede ejecutar en los dispositivos firepower, consulte Referencia de Comandos de FXOS , Referencia de Comandos de FTD .

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

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

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