# Interfaz de administración de la defensa de la amenaza de FirePOWER de la configuración (FTD)

## Contenido



## Introducción

Este documento describe la operación y la configuración de la interfaz de administración en la defensa de la amenaza de FirePOWER (FTD).

## Prerequisites

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

- FTD que se ejecuta en el dispositivo de hardware ASA5508-X
- FTD que se ejecuta en el dispositivo de hardware ASA5512-X
- FTD que se ejecuta en el dispositivo de hardware FPR9300
- FMC que ejecuta 6.1.0 (estructura 330)

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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

# Antecedentes

FTD es una imagen del software unificada que se puede instalar en las Plataformas siguientes:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Servicios web del Amazonas (AWS)
- KVM
- Módulo del router ISR

El propósito de este documento es demostrar:

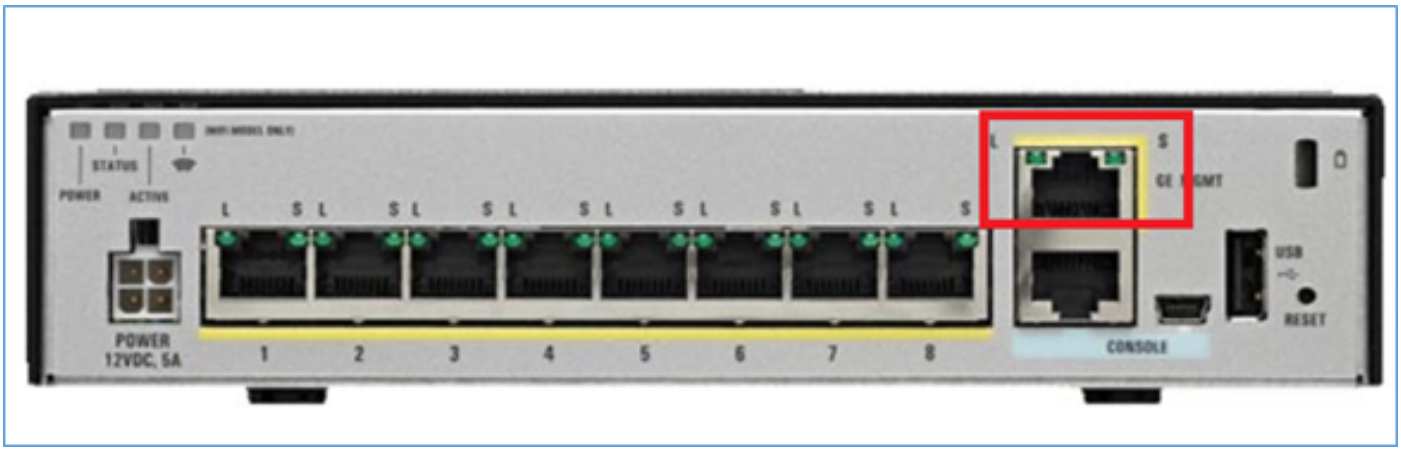
- Arquitectura de la interfaz de administración FTD en los dispositivos ASA5500-X
- Interfaz de administración FTD cuando se utiliza FDM
- Interfaz de administración FTD en las FP41xx/FP9300 Series
- Escenarios de la integración del centro de administración FTD/Firepower (FMC)

# Configurar

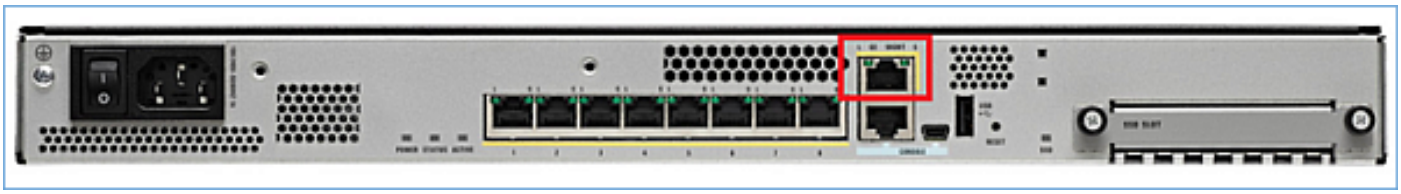
## Interfaz de administración en los dispositivos ASA 5500-X

La interfaz de administración en los dispositivos ASA5506/08/16-X y ASA5512/15/25/45/55-X.

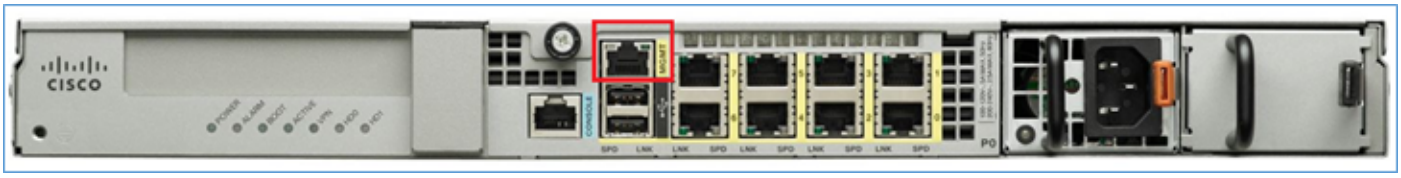
Ésta es la imagen de ASA5506-X:




Ésta es la imagen de ASA5508-X:



Ésta es la imagen de ASA5555-X:



Cuando una imagen FTD está instalada en 5506/08/16 la interfaz de administración se muestra como **Management1/1**. En los dispositivos 5512/15/25/45/55-X éste se convierte en **Management0/0.** Del comando line interface(cli) FTD esto se puede verificar en la salida del tecnología-**soporte de la demostración**.

Conecte con la consola FTD y funcione con el comando:

```
> show tech-support
-----------------[ BSNS-ASA5508-1 ]-----------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 330)
UUID                      : 04f55302-a4d3-11e6-9626-880037a713f3
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(2)

Compiled on Tue 23-Aug-16 19:42 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 13 hours 43 mins

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is d8b1.90ab.c852, irq 255
 2: Ext: GigabitEthernet1/2  : address is d8b1.90ab.c853, irq 255
 3: Ext: GigabitEthernet1/3  : address is d8b1.90ab.c854, irq 255
 4: Ext: GigabitEthernet1/4  : address is d8b1.90ab.c855, irq 255
 5: Ext: GigabitEthernet1/5  : address is d8b1.90ab.c856, irq 255
 6: Ext: GigabitEthernet1/6  : address is d8b1.90ab.c857, irq 255
 7: Ext: GigabitEthernet1/7  : address is d8b1.90ab.c858, irq 255
 8: Ext: GigabitEthernet1/8  : address is d8b1.90ab.c859, irq 255
 9: Int: Internal-Data1/1    : address is d8b1.90ab.c851, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13:   Ext: Management1/1       : address is d8b1.90ab.c851, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0
```

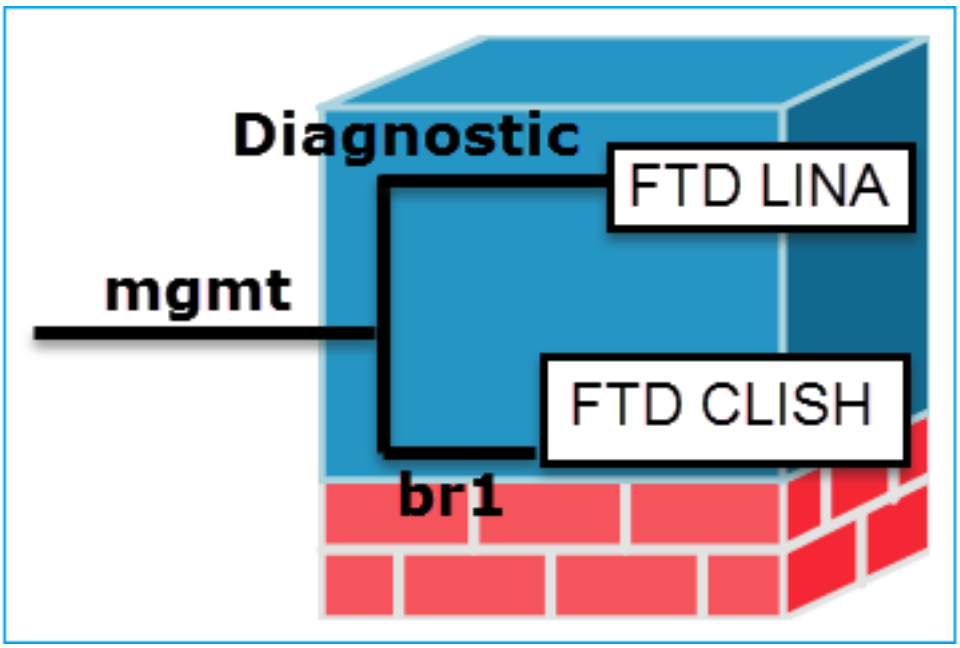
## ASA5512-X:

```
> show tech-support
------------------[ FTD5512-1 ]-------------------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 330)
UUID                      : 8608e98e-f0e9-11e5-b2fd-b649ba0c2874
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
```

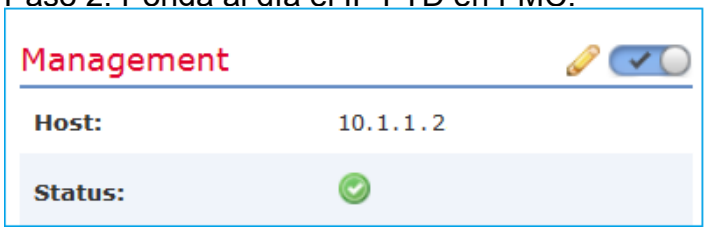
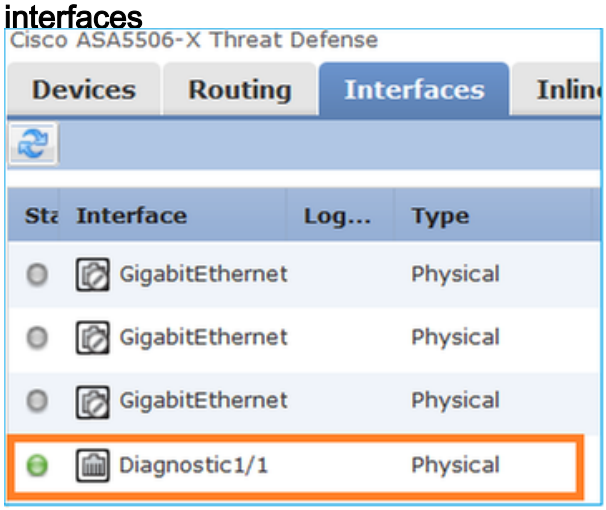
```
---------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(2)

Compiled on Fri 18-Aug-16 15:08 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 4 hours 37 mins

Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
            ASA: 1764 MB RAM, 1 CPU (1 core)
Internal ATA Compact Flash, 4096MB
BIOS Flash MX25L6445E @ 0xffbb0000, 8192KB

Encryption hardware device: Cisco ASA Crypto on-board accelerator (revision 0x1)
                            Boot microcode        : CNPx-MC-BOOT-2.00
                            SSL/IKE microcode     : CNPx-MC-SSL-SB-PLUS-0005
                            IPSec microcode       : CNPx-MC-IPSEC-MAIN-0026
                            Number of accelerators: 1
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4

 0: Int: Internal-Data0/0    : address is a89d.21ce.fde6, irq 11
 1: Ext: GigabitEthernet0/0  : address is a89d.21ce.fdea, irq 10
 2: Ext: GigabitEthernet0/1  : address is a89d.21ce.fde7, irq 10
 3: Ext: GigabitEthernet0/2  : address is a89d.21ce.fdeb, irq 5
 4: Ext: GigabitEthernet0/3  : address is a89d.21ce.fde8, irq 5
 5: Ext: GigabitEthernet0/4  : address is a89d.21ce.fdec, irq 10
 6: Ext: GigabitEthernet0/5  : address is a89d.21ce.fde9, irq 10
 7: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 0
 8: Int: Internal-Data0/1    : address is 0000.0001.0003, irq 0
   9: Ext: Management0/0       : address is a89d.21ce.fde6, irq 0
```

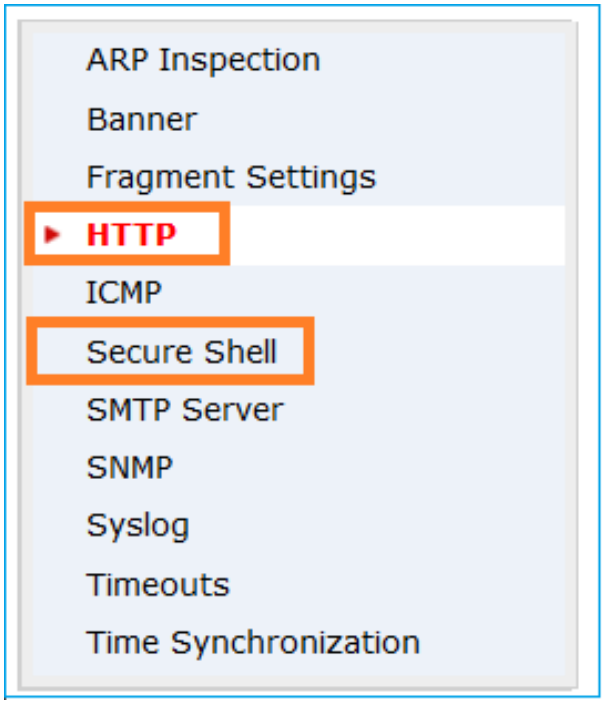
## Arquitectura de la interfaz de administración

La interfaz de administración se divide en 2 interfaces lógicas: **br1** (**management0** en los dispositivos FPR2100/4100/9300) y **diagnóstico:**




| | | |
|---|---|---|
| **Propósito** | Administración - **br1/management0**<br>• Esta interfaz se utiliza para asignar el IP FTD que se utiliza para la comunicación | Administración - **De diagnóstico**<br>• Proporciona el Acceso Remoto (e.g. SNMP) al motor ASA. |

| | | |
|---|---|---|
| | FTD/FMC.<br>• Termina el sftunnel entre FMC/FTD.<br>• Utilizado como fuente para los Syslog basados en las reglas.<br>• Proporciona el acceso de SSH y HTTPS al cuadro FTD. | • Utilizado como fuente para los Syslog del Lina-nivel, los mensajes AAA, SNMP etc. |
| **Obligatorio** | **Sí**, puesto que se utiliza para la comunicación FTD/FMC<br>(el sftunnel termina en él) | **Ningún** y él no se recomienda a configurelo. La recomendación es utilizar un instead* de la Interfaz de datos (marque la nota abajo) |
| **Configurar** | Esta interfaz se configura durante la instalación FTD (configuración).<br>Usted puede modificar más adelante las configuraciones br1 como sigue:<br><br>`>configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1`<br>`Setting IPv4 network configuration.`<br>`Network settings changed.`<br><br>`>`<br>Paso 2. Ponga al día el IP FTD en FMC.<br>  <br> | La interfaz puede ser configurada de FMC GUI:<br>Navegue a los **dispositivos > a la Administración de dispositivos,**<br>Seleccione el **botón Edit** y navegue a las **interfaces**<br>  <br><br>El acceso a la interfaz de diagnóstico puede ser controlado por FTD **Dispositivos > configuraciones de la plataforma >** Secure Shell y **Dispositivos > plataforma Settings> HTTP** respectivamente |
| **Acceso de restricción** | • Por abandono, solamente el **Usuario administrador** puede conectar con la subinterfaz FTD br1.<br>• El acceso de restricción de SSH se hace usando el CLISH CLI<br><br>`>configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1`<br>`Setting IPv4 network configuration.`<br>`Network settings changed.`<br><br>`>` | |




**Verificación**

Método 1 - De FTD CLI:

```
  > show network
...
=======[ br1 ]=======
State : Enabled
Channels : Management & Events
Mode :
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 18:8B:9D:1E:CA:7B
----------------------[ IPv4 ]-----
Configuration : Manual
Address : 10.1.1.2
Netmask : 255.0.0.0
Broadcast : 10.1.1.255
----------------------[ IPv6 ]-----
```

Método 2 – De FMC GUI

**Dispositivos > Administración de dispositivos > dispositivo > Administración**

Método 1 - De LINA CLI:

```
  firepower# show interface ip brief
..
Management1/1 192.168.1.1 YES unset up up

firepower# show run interface m1/1
!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.255.0
```

Método 2 – De FMC GUI

Navegue a los **dispositivos > a la Administración de dispositivos,** seleccione el **botón Edit** y navegue a las **interfaces**

* extracto tomado del guía del usuario FTD 6.1

### Routed Mode Deployment

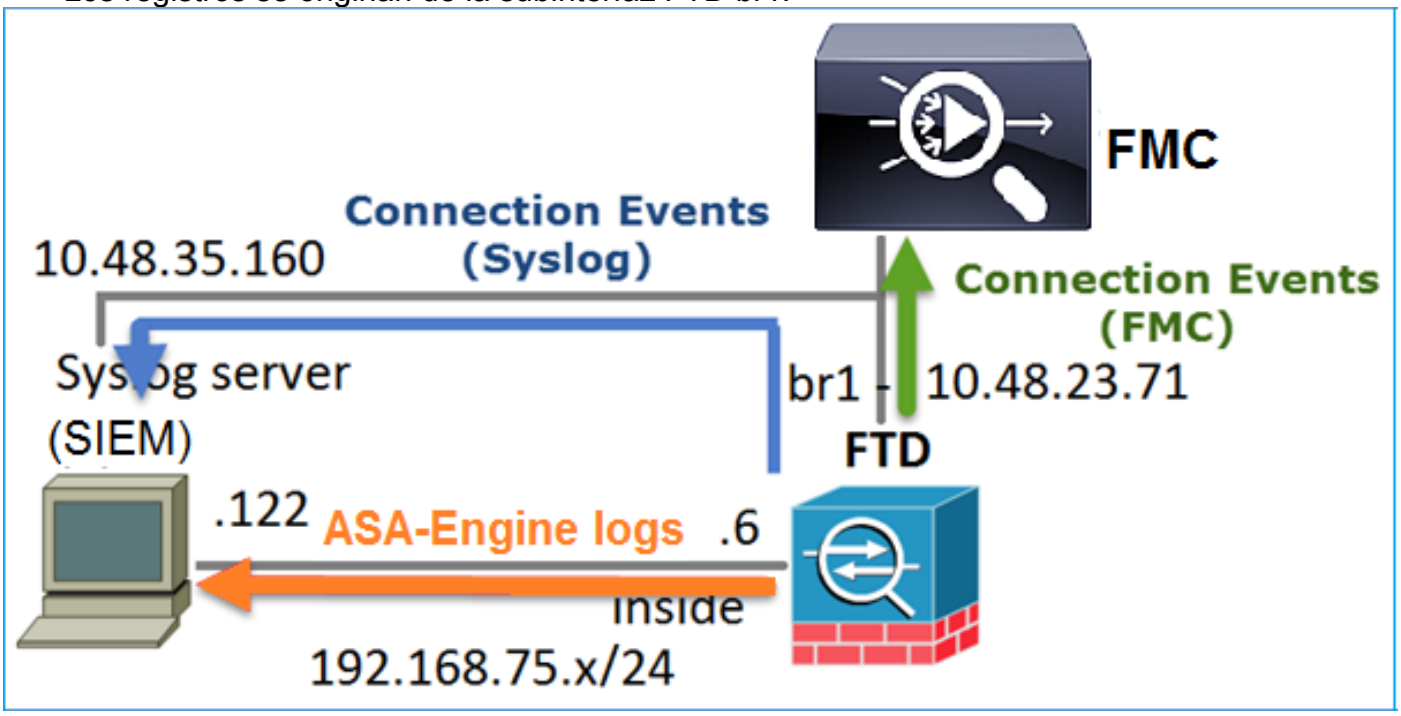
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure the Diagnostic interface, its IP address must be on the same network as the Management IP address, and it counts as a regular interface that cannot be on the same network as any other data interfaces. Because the Management interface requires Internet access for updates, putting Management on the same network as an inside interface means you can deploy the Firepower Threat Defense device with only a switch on the inside and point to the inside interface as its gateway. See the following deployment that uses an inside switch:

## Registro FTD

- Cuando un usuario configura el registro FTD de las **configuraciones de la plataforma, el** FTD genera los mensajes de Syslog (lo mismo que en el ASA clásico) y puede utilizar cualquier Interfaz de datos como fuente (diagnóstico incluyendo). Un ejemplo de un mensaje de Syslog que se genera en ese caso:

```
  firepower# show interface ip brief
..
Management1/1 192.168.1.1 YES unset up up

firepower# show run interface m1/1
!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.255.0
```

- Por otra parte, cuando se habilita el **registro del Regla-nivel de la** directiva del control de acceso (ACP) el FTD origina estos registros a través de la interfaz lógica **br1** como fuente. Los registros se originan de la subinterfaz FTD br1:



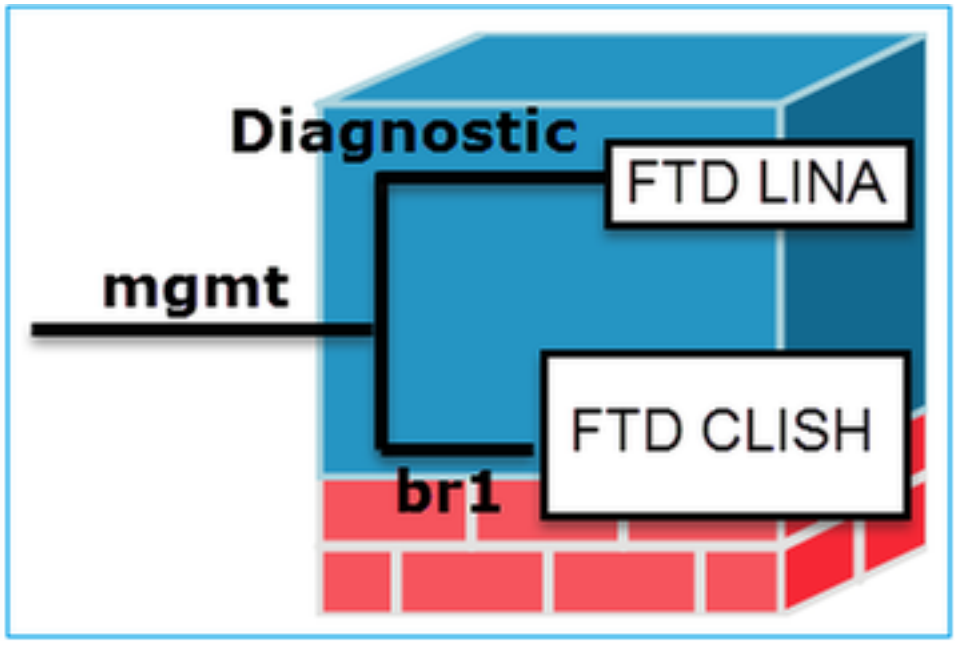

## Maneje FTD con FDM (la Administración del En-cuadro)

Como a partir de la versión el 6.1, un FTD que está instalado en los dispositivos ASA5500-X se puede manejar por FMC (Administración del apagado-cuadro) o por el administrador de dispositivo de FirePOWER (FDM) (Administración del en-cuadro).

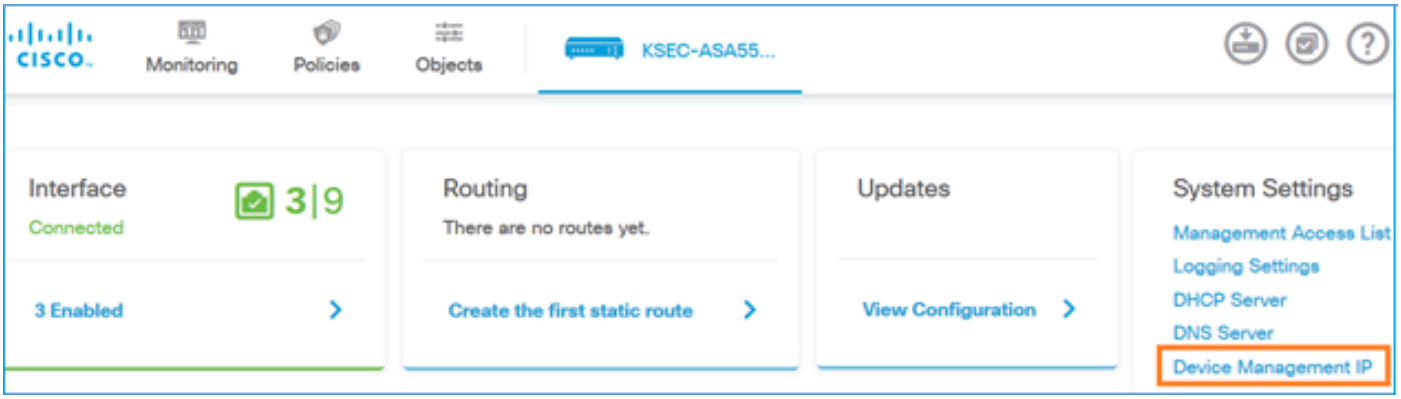
Salida de FTD CLISH cuando el dispositivo es manejado por FDM:

```
> show managers
Managed locally.
>
```

FDM utiliza la interfaz lógica br1. Esto se puede visualizar como:




De FDM UI la interfaz de administración es accesible del **IP del panel > de los ajustes de sistema > de la Administración de dispositivos del dispositivo**:





## Interfaz de administración en los dispositivos de hardware FTD FirePOWER

FTD se puede también instalar en los dispositivos de hardware de FirePOWER 2100, 4100 y 9300. El chasis de FirePOWER ejecuta sus propios FXO llamados OS mientras que el FTD está instalado en un módulo/una cuchilla.

### Dispositivo FPR21xx

### Dispositivo FPR41xx

### Dispositivo FPR9300

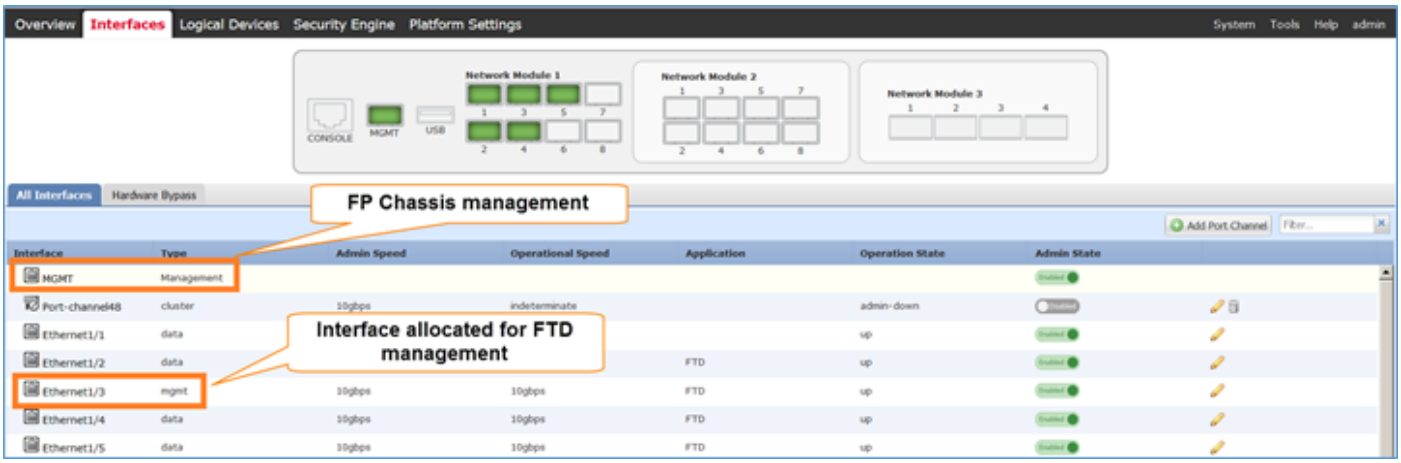
En FPR4100/9300 esta interfaz está solamente para la Administración del chasis y no se puede utilizar/compartir con el software FTD que se ejecuta dentro del módulo FP. Para el módulo FTD afecte un aparato una interfaz de los datos aparte que para la Administración FTD.

En FPR2100 esta interfaz se comparte entre el chasis (FXO) y el dispositivo lógico FTD:

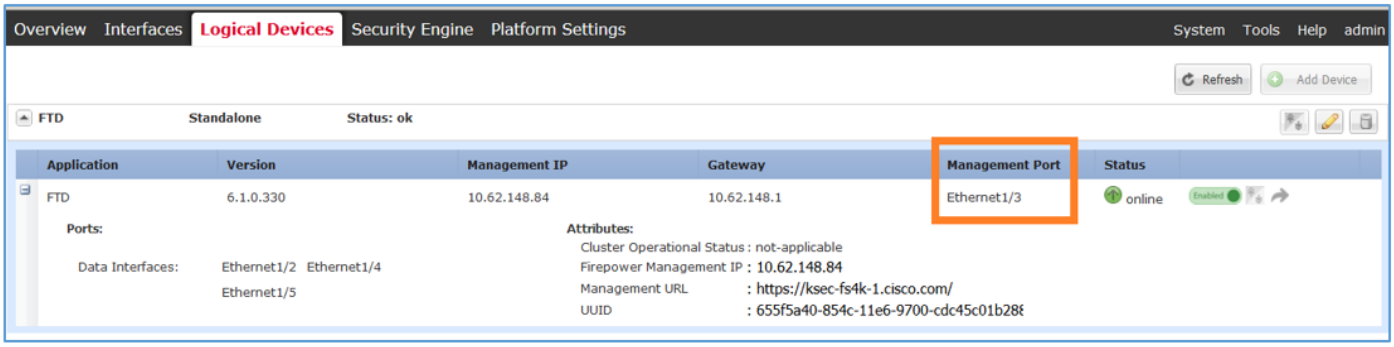
```
> show network
===============[ System Information ]===============
Hostname                  : ftd623
Domains                   : cisco.com
DNS Servers               : 173.38.200.100
                            8.8.8.8
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.62.148.129

==================[ management0 ]===================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
```

```
MAC Address                : 70:DF:2F:18:D8:00
----------------------[ IPv4 ]----------------------
Configuration              : Manual
Address                    : 10.62.148.179
Netmask                    : 255.255.255.128
Broadcast                  : 10.62.148.255
----------------------[ IPv6 ]----------------------
Configuration              : Disabled

> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
...
firepower#
```

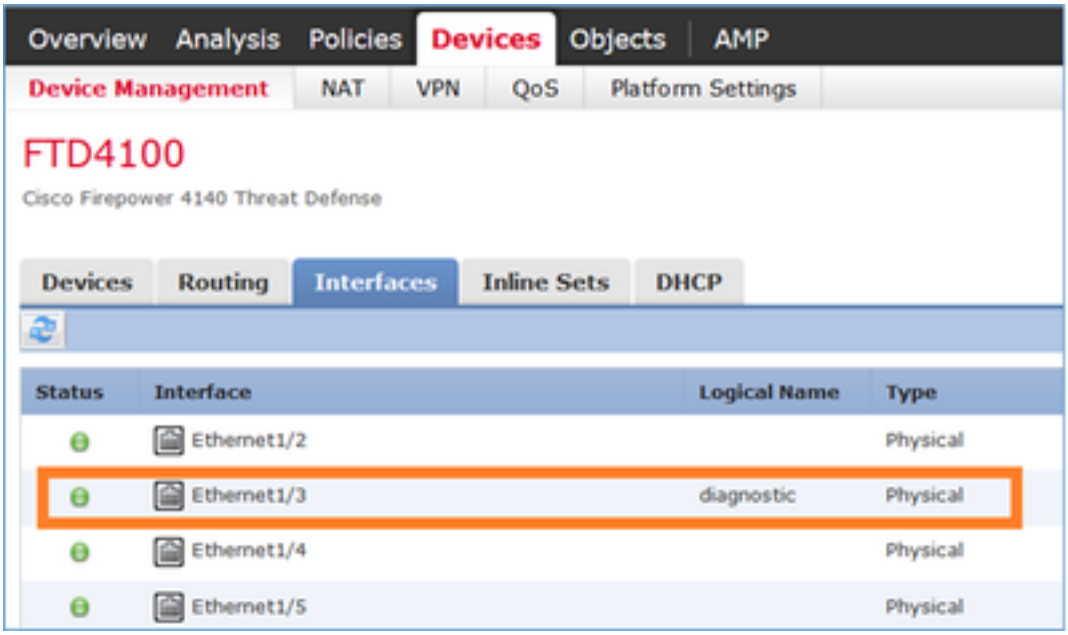
Este tiro de pantalla es del administrador del chasis de FirePOWER (FCM) UI en FPR4100 donde una interfaz diferente para la Administración FTD se afecta un aparato. En este ejemplo Ethernet1/3 se elige como la interfaz de administración FTD: p1




Esto se puede también ver de los **dispositivos lógicos** tab:p2




En FMC la interfaz se muestra como **diagnóstico:** p3




### Verificación CLI

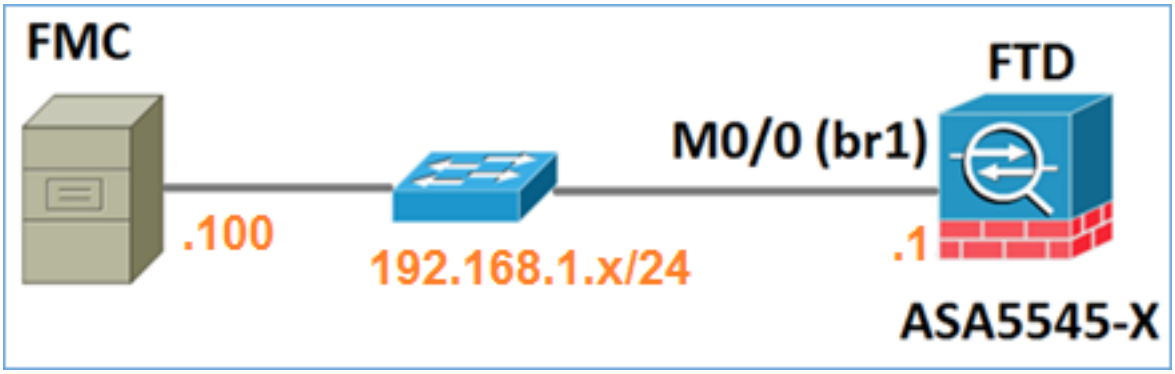
```
FP4100# connect module 1 console
Firepower-module1>connect ftd
Connecting to ftd console... enter exit to return to bootCLI
>
> show interface
… output omitted …

Interface Ethernet1/3 "diagnostic", is up, line protocol is up
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input rate 2 pkts/sec,  101 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 1 pkts/sec
      5 minute input rate 2 pkts/sec,  112 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 1 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets

… output omitted …
>
```

## Integre FTD con FMC - Escenarios de la Administración

Se dan algunas de las Opciones de instrumentación que permiten manejar FTD que se ejecute en los dispositivos ASA5500-X de FMC.

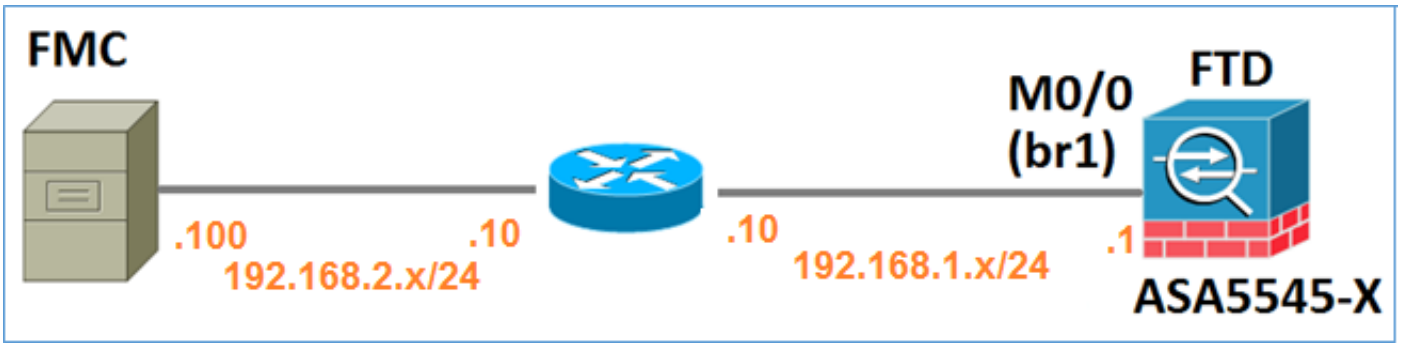
### Escenario 1. FTD y FMC en la misma subred.

Éste es el despliegue más simple. Mientras que puede ser visto en la figura, el FMC está en la misma subred como la interfaz FTD br1:




**Escenario 2. FTD y FMC en diversas subredes. La controle de plano no pasa con el FTD.**

En este despliegue el FTD debe tener una ruta hacia el FMC y vice versa. En FTD el salto siguiente es un dispositivo L3 (router):




## Información Relacionada

- Notas del Sistema XX, versión de FirePOWER, versión 6.1.0
- Nueva imagen Cisco ASA o dispositivo de la defensa de la amenaza de FirePOWER
- Guía de configuración de la defensa de la amenaza de Cisco FirePOWER para el administrador de dispositivo de FirePOWER, versión 6.1
- Soporte Técnico y Documentación - Cisco Systems