Configuración de la interfaz de gestión de Firepower Threat Defence (FTD)

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Interfaz de gestión en dispositivos ASA 5500-X](#)
[Arquitectura de interfaz de administración](#)
[Registro FTD](#)
[Gestión de FTD con FDM (gestión integrada)](#)
[Interfaz de gestión en appliances de hardware Firepower FTD](#)
[Integración de FTD con FMC - Escenarios de gestión](#)
[Situación 1. FTD y FMC en la misma subred.](#)
[Situación 2. FTD y FMC en diferentes subredes. El plano de control no pasa por el FTD.](#)
[Información Relacionada](#)

Introducción

Este documento describe el funcionamiento y la configuración de la interfaz de administración en Firepower Threat Defence (FTD).

Prerequisites

Requirements

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 se ejecuta en la versión 6.1.0 (compilación 330)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

FTD es una imagen de software unificada que se puede instalar en estas plataformas:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100 y FPR9300
- VMware (ESXi)
- Servicios web de Amazon (AWS)
- KVM
- módulo de router ISR

El objetivo de este documento es demostrar:

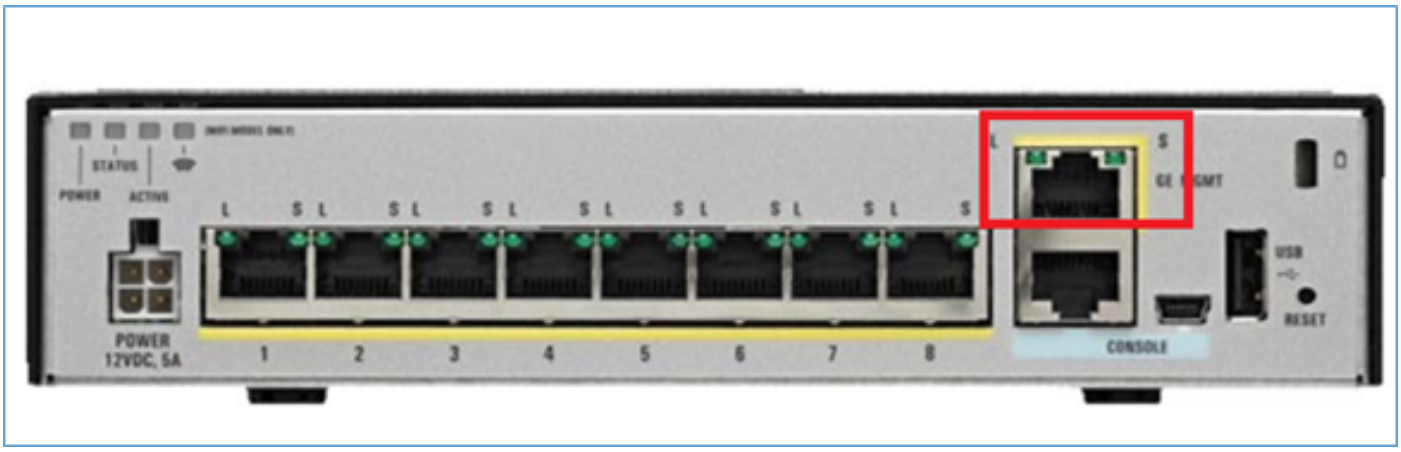
- Arquitectura de interfaz de administración FTD en dispositivos ASA5500-X
- Interfaz de gestión de FTD cuando se utiliza FDM
- Interfaz de gestión de FTD en las series FP41xx/FP9300
- Situaciones de integración de FTD/Firepower Management Center (FMC)

Configurar

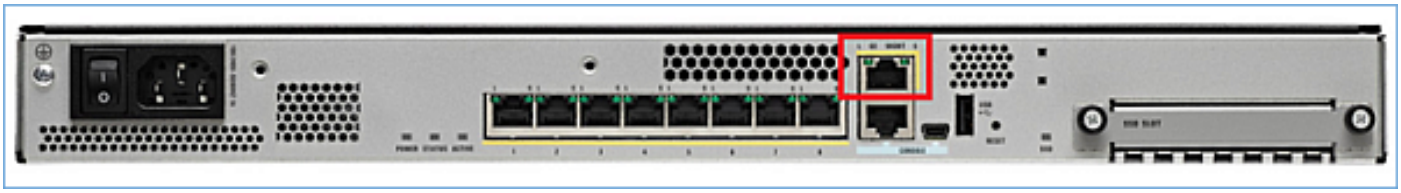
Interfaz de gestión en dispositivos ASA 5500-X

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

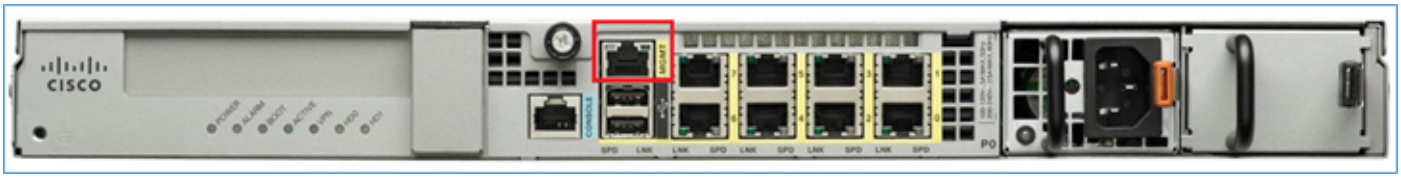
Esta es la imagen de ASA5506-X:



Esta es la imagen de ASA5508-X:



Esta es la imagen de ASA5555-X:



Cuando se instala una imagen FTD en 5506/08/16, la interfaz de administración se muestra como **Management1/1**. En los dispositivos 5512/15/25/45/55-X, esto se convierte en **Management0/0.** Desde la Interfaz de línea de comandos (CLI) de FTD, esto se puede verificar en el resultado **show tech-support**.

Conéctese a la consola FTD y ejecute 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
```

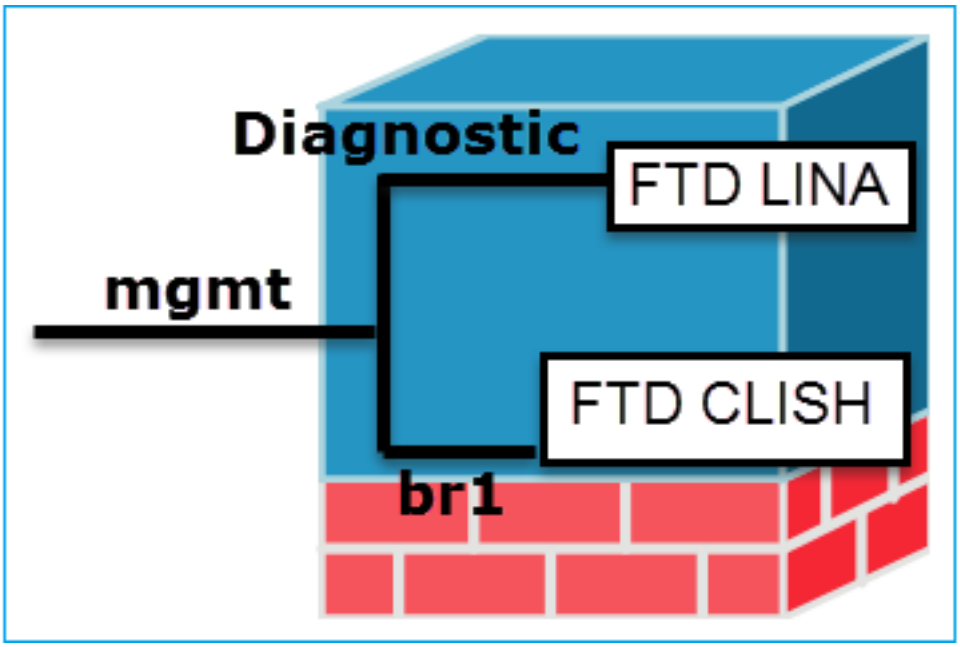
ASA5512-X:

```
> 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
```

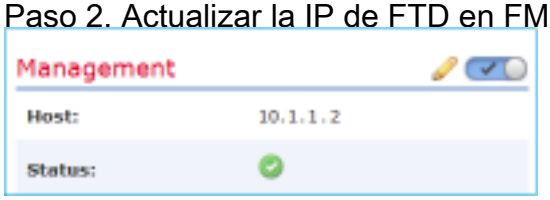
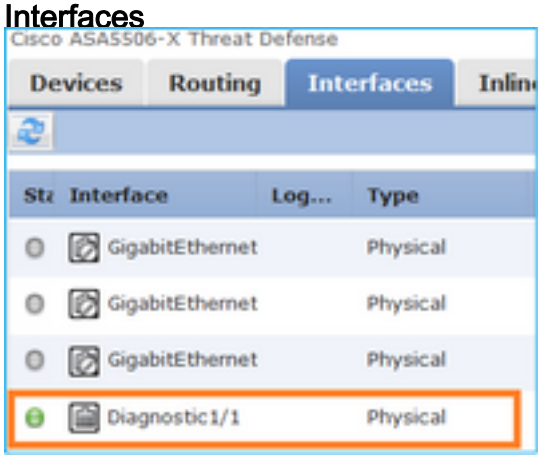
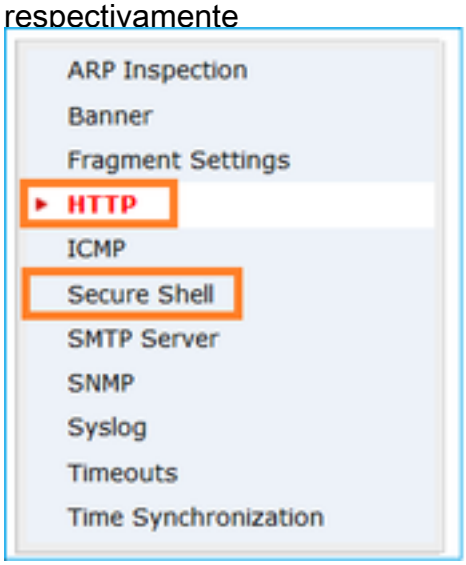
Arquitectura de interfaz de administración

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



	Gestión: **br1/management0**	Gestión - **Diagnóstico**
Propósito	• Esta interfaz se utiliza para asignar la IP de FTD que se utiliza para la comunicación FTD/FMC. • Finaliza el sftunnel entre FMC/FTD. • Se utiliza como origen para los registros del sistema basados en reglas. • Proporciona acceso SSH y HTTPS al cuadro	• Proporciona acceso remoto (por ejemplo, SNMP) al motor ASA. • Se utiliza como fuente para los syslogs de nivel LINA, AAA, mensajes SNMP, etc.

	FTD.	
Obligatoria	**Sí**, ya que se utiliza para la comunicación FTD/FMC (el sftunnel termina en él) Esta interfaz se configura durante la instalación de FTD (configuración). Más adelante podrá modificar la configuración de br1 de la siguiente manera:	**No** y no se recomienda configurarlo. La recomendación es utilizar una interfaz de datos* (consulte la nota siguiente) La interfaz se puede configurar desde la GUI de FMC: Vaya a **Devices > Device Management,** Seleccione el botón **Edit** y navegue hasta **Interfaces**

Configurar	`>configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1`
	`Setting IPv4 network configuration.`
	`Network settings changed.`
	
	`>`
	Paso 2. Actualizar la IP de FTD en FMC.
	 
		
		El acceso a la interfaz de diagnóstico puede controlarse mediante FTD **Dispositivos > Configuración de plataforma > Secure Shell** y **Dispositivos > Configuración de la plataforma> HTTP** respectivamente
		 

Restringir el acceso	• De forma predeterminada, sólo el usuario **admin** puede conectarse a la subinterfaz FTD br1. • Para restringir el acceso SSH se utiliza CLISH CLI `> configure ssh-access-list 10.0.0.0/8`	

Verificación	Método 1 - Desde CLI de FTD:
	
	`> show network`
	`...`
	`=======[ br1 ]=======`
	`State : Enabled`
	`Channels : Management & Events`
	`Mode :`
	`MDI/MDIX : Auto/MDIX`
	`MTU : 1500`
	`MAC Address : 18:8B:9D:1E:CA:7B`
		Método 1: desde CLI de LINA:
		
		`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`

```
----------------------[ IPv4 ]-----
Configuration : Manual
Address : 10.1.1.2
Netmask : 255.0.0.0
Broadcast : 10.1.1.255
----------------------[ IPv6 ]-----
```

Método 2: desde la GUI del FMC
Devices > Device Management > Device > Management

```
security-level 0
ip address 192.168.1.1 255.255.255.0
```

Método 2: desde la GUI del FMC
Vaya a **Devices > Device Management,** seleccione el botón **Edit** y navegue hasta **Interfaces**

* extracto tomado de la guía del usuario de FTD 6.1.

Routed Mode Deployment

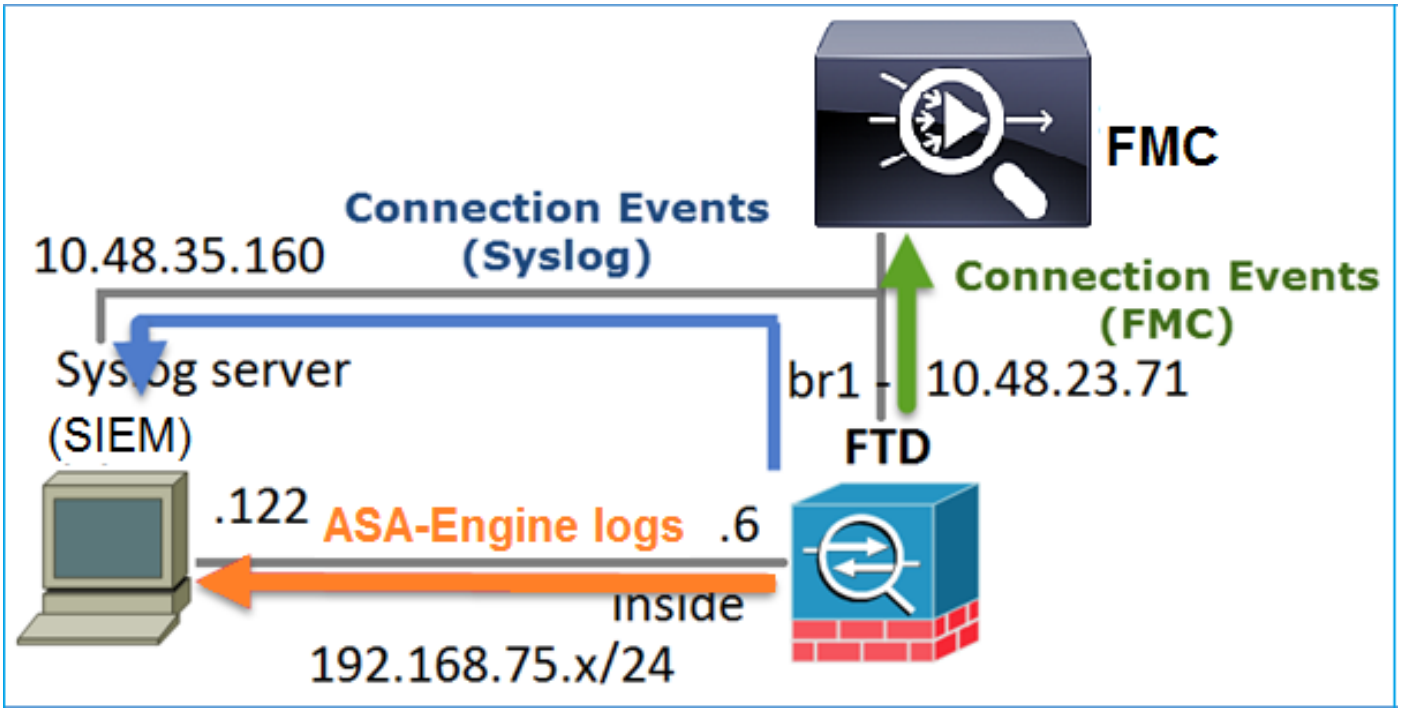
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure 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 de FTD desde **Configuración de la plataforma,** el FTD genera mensajes Syslog (los mismos que en el ASA clásico) y puede utilizar cualquier interfaz de datos como origen (incluye el diagnóstico). Un ejemplo de un mensaje syslog que se genera en ese caso:

```
May 30 2016 19:25:23 firepower : %ASA-6-302020: Built inbound ICMP connection for faddr
192.168.75.14/1 gaddr 192.168.76.14/0 laddr 192.168.76.14/0
```

- Por otro lado, cuando el **registro de nivel de regla de la** política de control de acceso (ACP) está habilitado, el FTD origina estos registros a través de la interfaz lógica **br1** como origen. Los registros se originan desde la subinterfaz FTD br1:



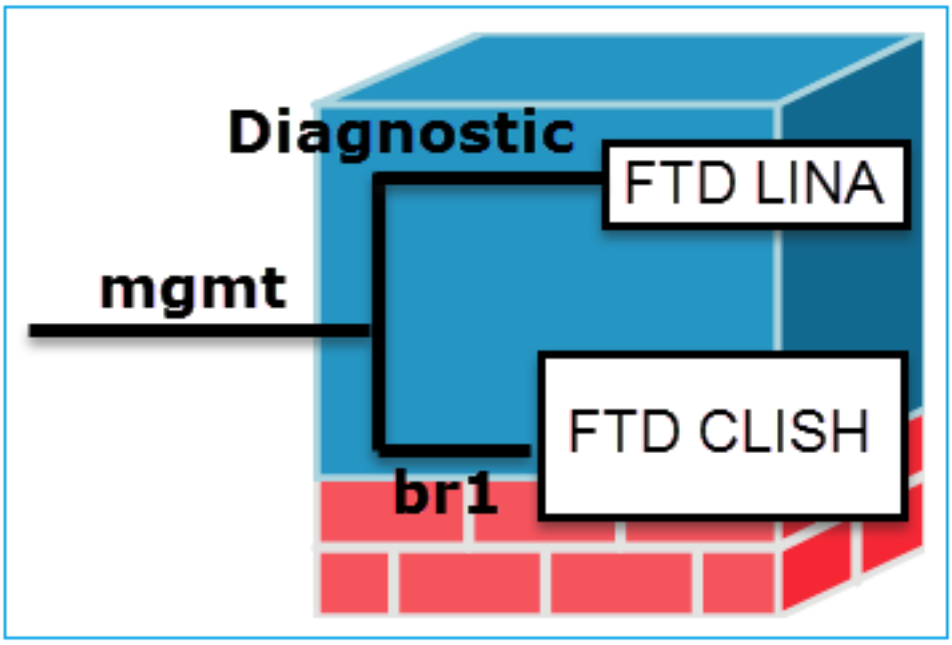
Gestión de FTD con FDM (gestión integrada)

A partir de la versión 6.1, un FTD instalado en dispositivos ASA5500-X se puede gestionar mediante FMC (gestión externa) o mediante Firepower Device Manager (FDM) (gestión integrada).

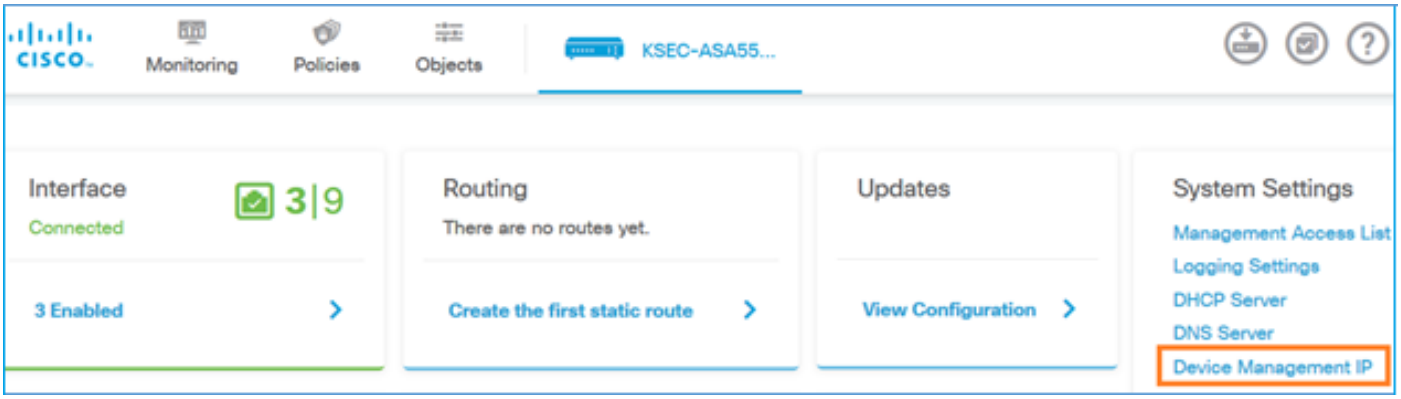
Salida de FTD CLISH cuando el dispositivo está gestionado por FDM:

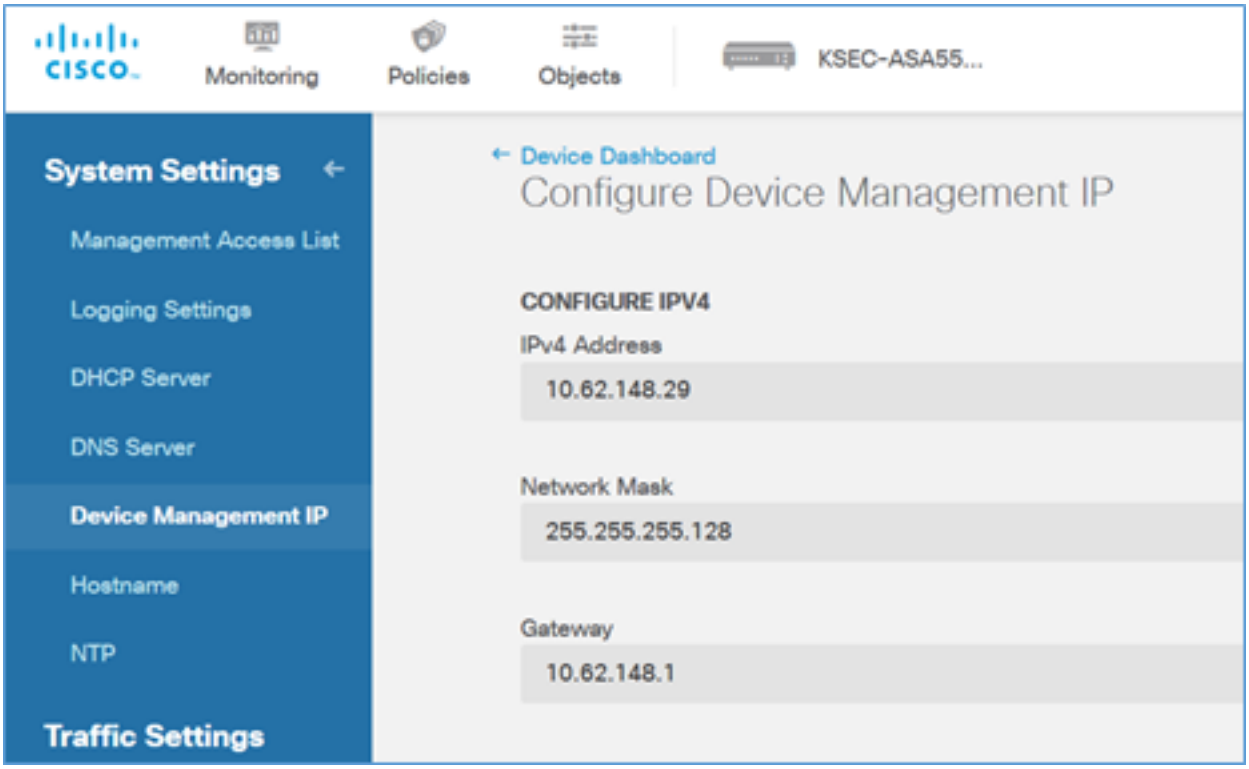
```
> show managers
Managed locally.
>
```

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



Desde la interfaz de usuario de FDM se puede acceder a la interfaz de administración desde el **Panel de dispositivos > Configuración del sistema > IP de administración de dispositivos**:





Interfaz de gestión en appliances de hardware Firepower FTD

FTD también se puede instalar en appliances de hardware Firepower 2100, 4100 y 9300. El chasis Firepower ejecuta su propio sistema operativo denominado FXOS, mientras que el FTD se instala en un módulo/blade.

dispositivo FPR21xx

dispositivo FPR41xx

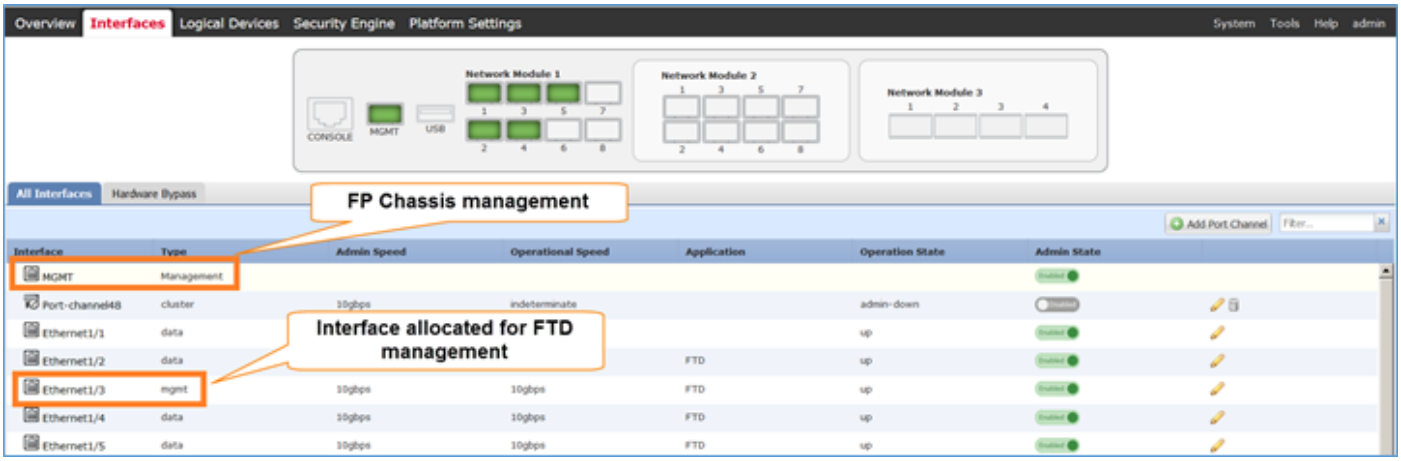
Dispositivo FPR9300

En FPR4100/9300, esta interfaz es solo para la administración del chasis y no se puede usar/compartir con el software FTD que se ejecuta dentro del módulo FP. Para el módulo FTD, asigne una interfaz de datos independiente para la gestión de FTD.

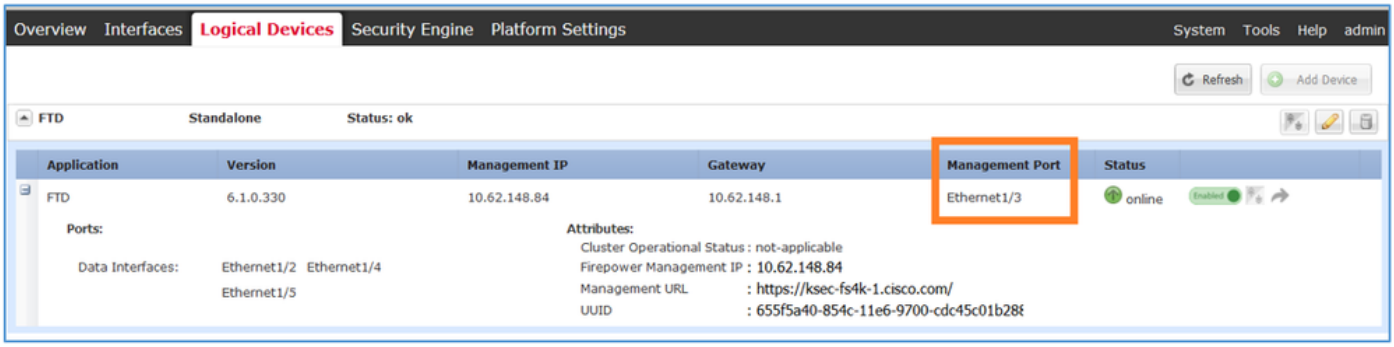
En FPR2100, esta interfaz se comparte entre el chasis (FXOS) y el dispositivo lógico FTD:

```
> show network
===============[ System Information ]===============
Hostname                  : ftd623
Domains                   : cisco.com
DNS Servers               : 192.168.200.100
                            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#
```

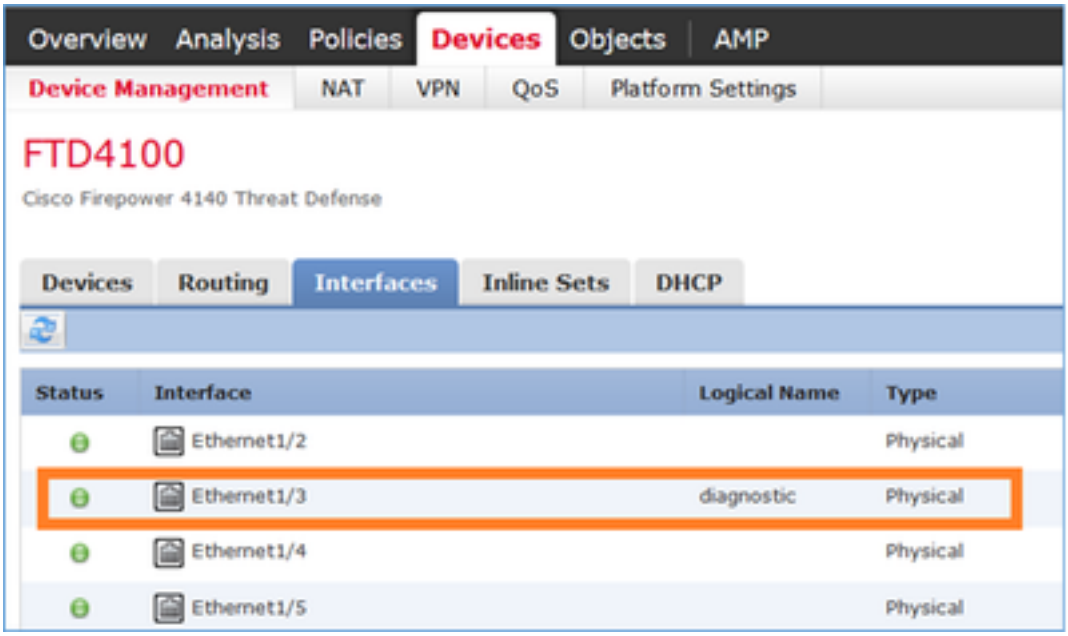
Esta captura de pantalla es de la interfaz de usuario de Firepower Chassis Manager (FCM) en FPR4100, donde se asigna una interfaz independiente para la gestión de FTD. En este ejemplo, se elige Ethernet1/3 como la interfaz de administración FTD: p1



Esto también se puede ver en la pestaña **Logical Devices**: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
```

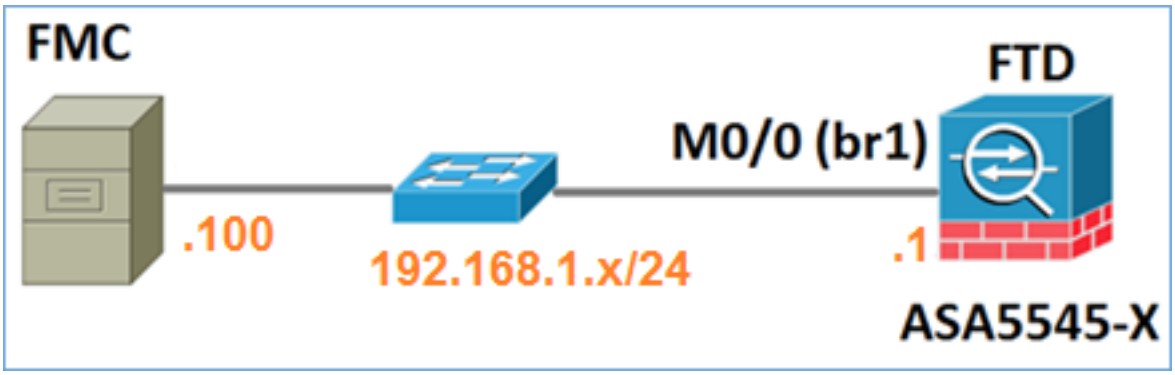
```
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input 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 …
>
```

Integración de FTD con FMC - Escenarios de gestión

Estas son algunas de las opciones de implementación que permiten gestionar el FTD que se ejecuta en los dispositivos ASA5500-X desde FMC.

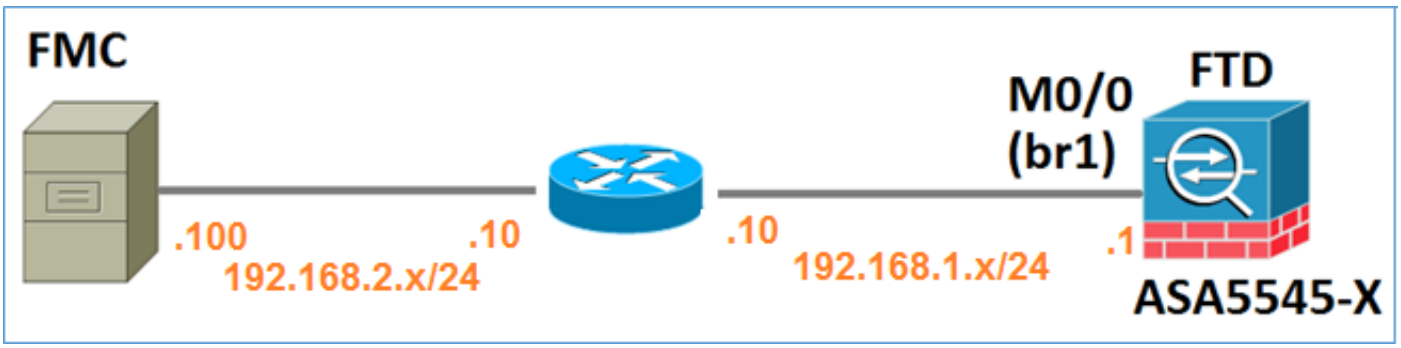
Situación 1. FTD y FMC en la misma subred.

Esta es la implementación más sencilla. Como se puede ver en la figura, el FMC se encuentra en la misma subred que la interfaz FTD br1:



Situación 2. FTD y FMC en diferentes subredes. El plano de control no pasa por el FTD.

En esta implantación, el FTD debe tener una ruta hacia el CSP y viceversa. En FTD, el salto siguiente es un dispositivo L3 (router):



Información Relacionada

- Notas de la versión del sistema Firepower, versión 6.1.0
- Recreación de la imagen del dispositivo Cisco ASA o Firepower Threat Defence
- Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager, versión 6.1
- Soporte Técnico y Documentación - Cisco Systems

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).