Configure Firepower Threat Defense (FTD) Management Interface

Contents

Introduction

This document describes the operation and configuration of the Management Interface on Firepower Threat Defense (FTD).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

- FTD running on ASA5508-X hardware appliance
- FTD running on ASA5512-X hardware appliance
- FTD running on FPR9300 hardware appliance
- FMC running 6.1.0 (build 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FTD is a unified software image that can be installed on the following platforms :

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Amazon Web Services (AWS)
- KVM
- ISR router module

The purpose of this document is to demonstrate:

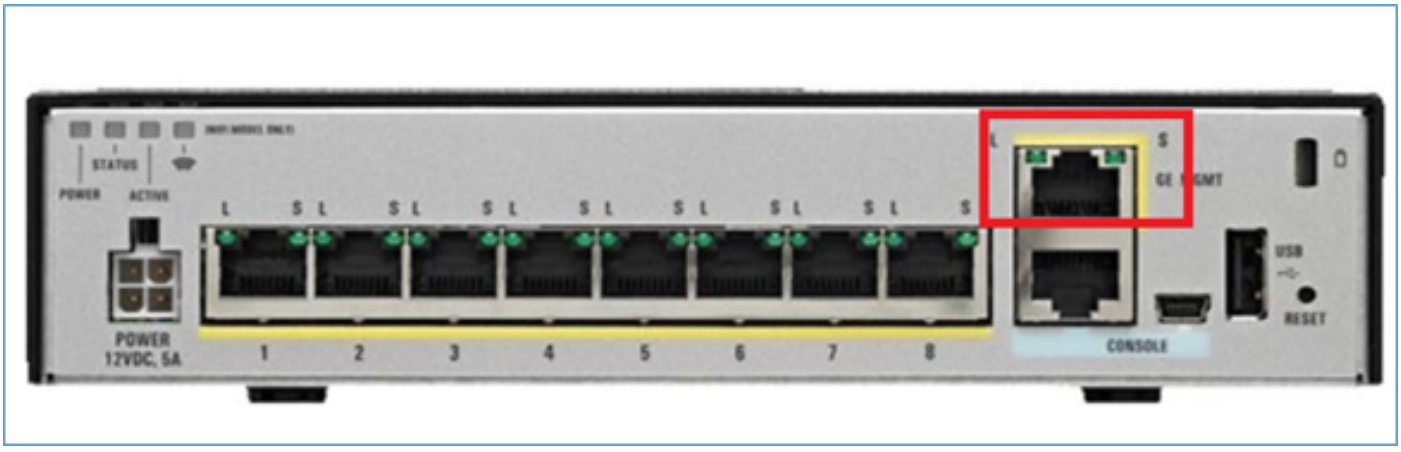
- FTD Management interface architecture on ASA5500-X devices
- FTD Management interface when FDM is used
- FTD Management interface on FP41xx/FP9300 series
- FTD/Firepower Management Center (FMC) integration scenarios

Configure

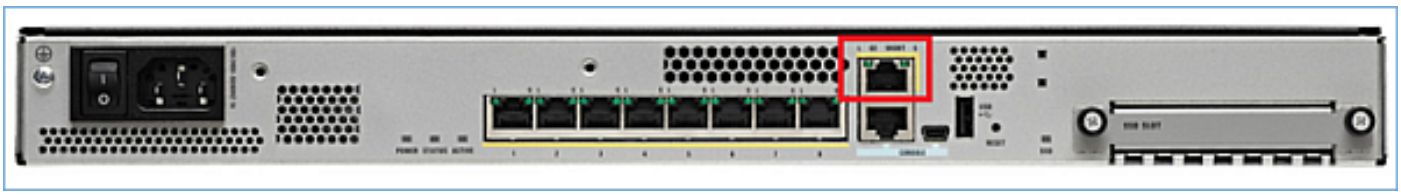
Management Interface on ASA 5500-X Devices

The Management interface on ASA5506/08/16-X and ASA5512/15/25/45/55-X devices.

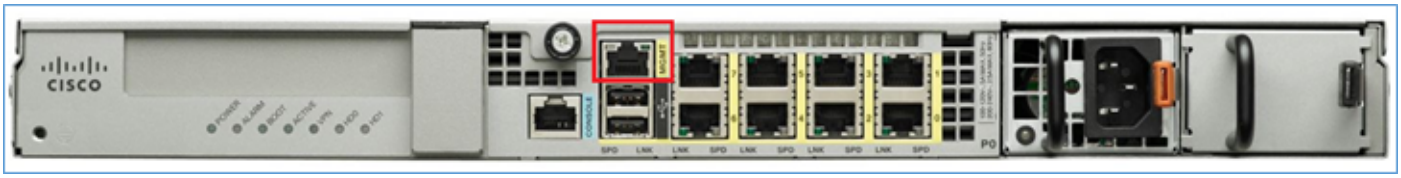
This is the image of ASA5506-X:



This is the image of ASA5508-X:



This is the image of ASA5555-X:



When an FTD image is installed on 5506/08/16 the management interface is shown as **Management1/1**. On 5512/15/25/45/55-X devices this becomes **Management0/0.** From the FTD Command Line Interface (CLI) this can be verified in the **show tech-support** output.

Connect to the FTD console and run the command:

```
> 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
```

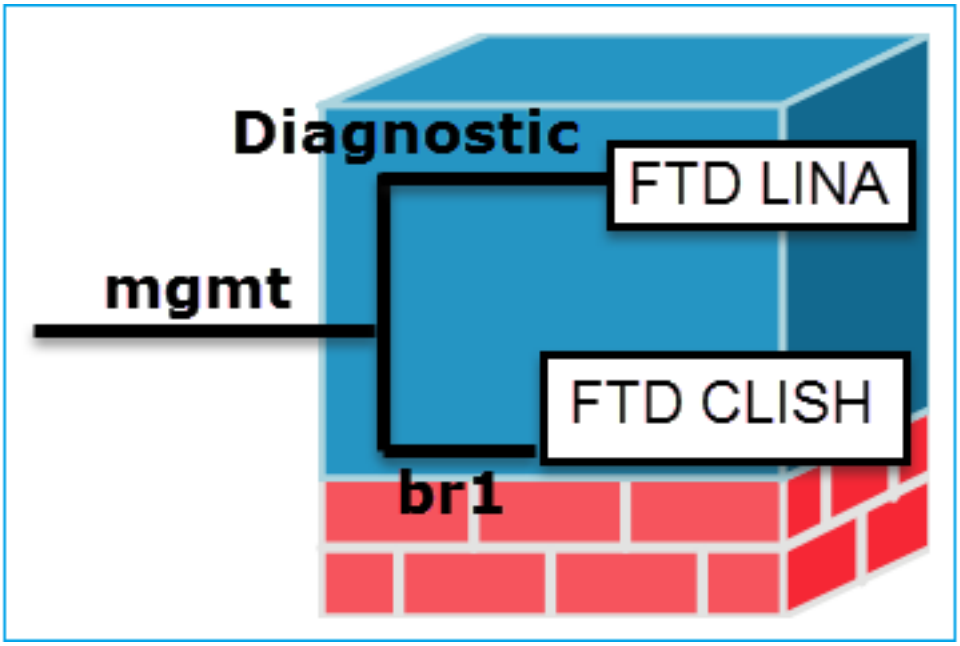
ASA5512-X:

```
> 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
```

Management Interface Architecture

The Management interface is divided into 2 logical interfaces: **br1** (**management0** on FPR2100/4100/9300 appliances) and **diagnostic:**

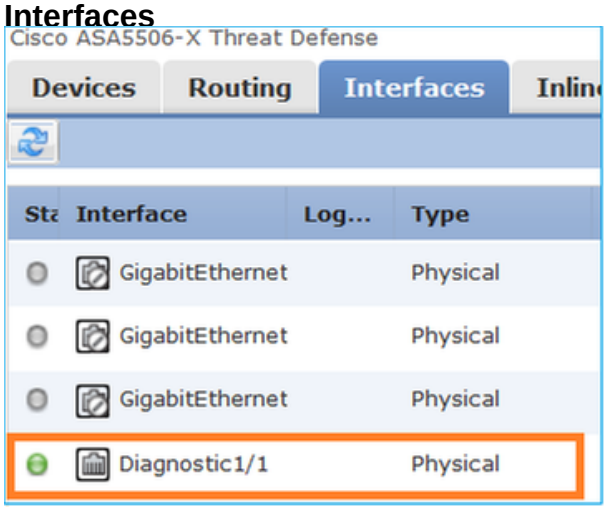


	Management - **br1/management0**	Management - **Diagnostic**
Purpose	• This interface is used in order to assign the FTD IP that is used for FTD/FMC communication. • Terminates the sftunnel between FMC/FTD. • Used as a source for rule-based syslogs. • Provides SSH and HTTPS access to the FTD box.	• Provides remote access (e.g. SNMP) to ASA engine. • Used as a source for LINA-level syslogs, AAA, SNMP etc messages.
Mandator	**Yes**, since it is used for FTD/FMC	**No** and it is not recommended to

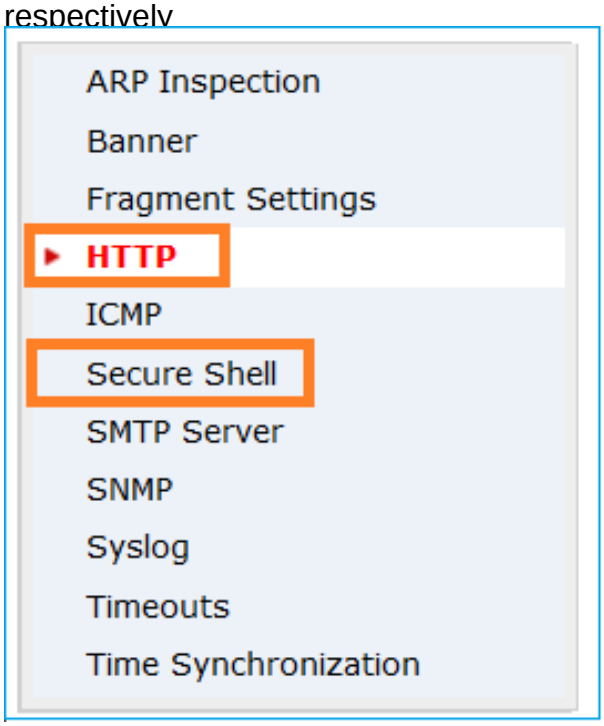
y

communication
(the sftunnel terminates on it)

configure it. The recommendation is to use
a data interface instead* (check the note below)
The interface can be configured from FMC GUI:
Navigate to **Devices > Device Management,**
Select the **Edit** button and navigate to **Interfaces**



The access to the diagnostic interface can be controlled by FTD
Devices > Platform Settings > Secure Shell
and
Devices > Platform Settings> HTTP
respectively

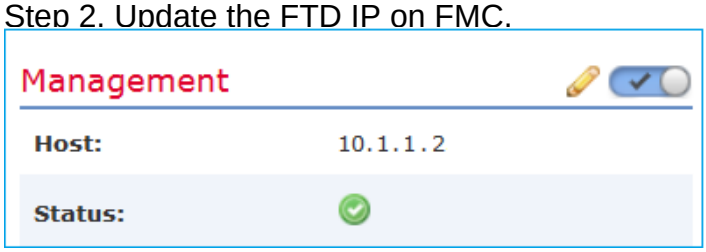


Configure

This interface is configured during FTD installation (setup).
Later you can modify the br1 settings as follows:

```
 >configure network ipv4 manual 10.1.1.2
255.0.0.0 10.1.1.1
Setting IPv4 network configuration.
Network settings changed.

>
```

Step 2. Update the FTD IP on FMC.



Restrictin g access

- By default, only the **admin** user can connect to the FTD br1 subinterface.
- Restricting SSH access is done using the CLISH CLI

```
 >configure network ipv4 manual 10.1.1.2
255.0.0.0 10.1.1.1
Setting IPv4 network configuration.
Network settings changed.

>
```

Verify

Method 1 - From FTD CLI:

```
  > show network
...
=======[ br1 ]=======
State : Enabled
Channels : Management & Events
```

Method 1 - From LINA CLI:

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

firepower# show run interface m1/1
```

```
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 ]-----
```

Method 2 – From FMC GUI
Devices > Device Management > Device > Management

```
!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.255.0
```

Method 2 – From FMC GUI
Navigate to **Devices > Device Management,**
select the **Edit** button and navigate to **Interfaces**

* excerpt taken from [FTD 6.1 user guide]

Routed Mode Deployment

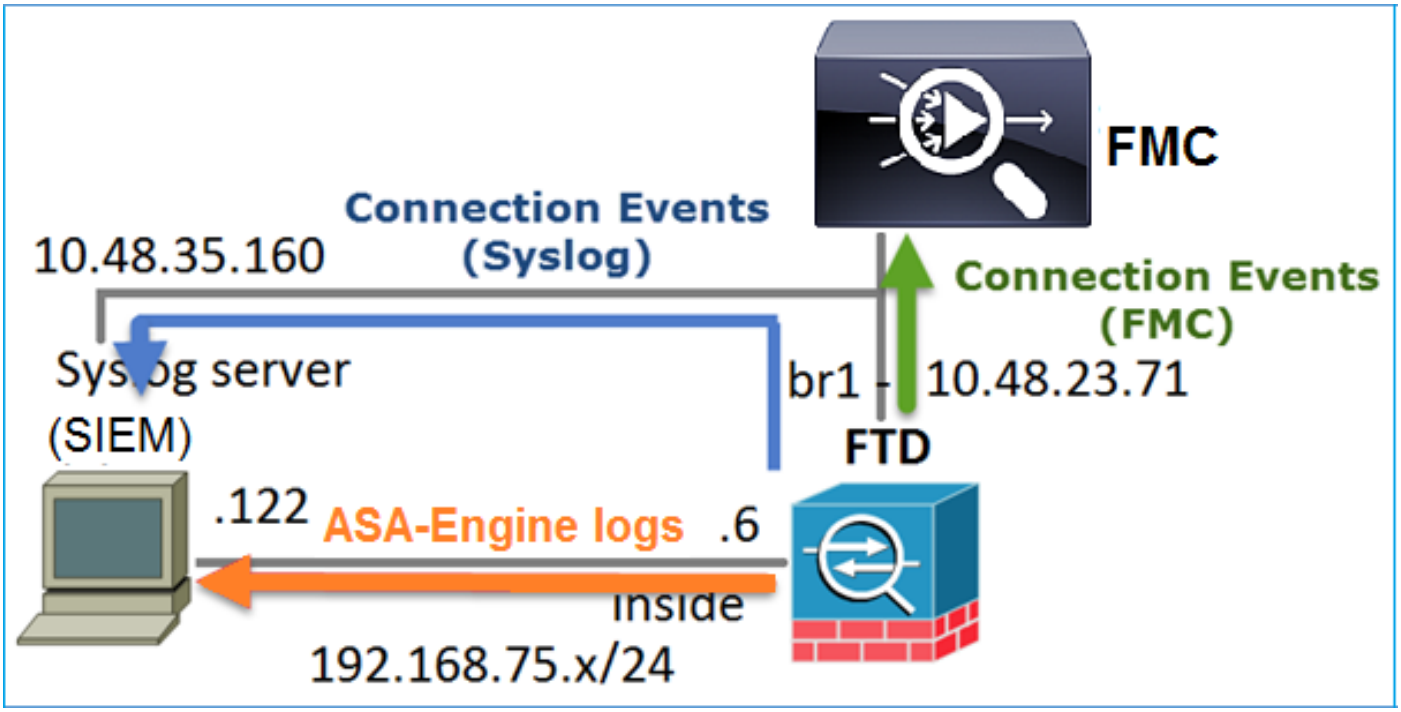
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure 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:

FTD Logging

- When a user configures FTD logging from **Platform Settings,** the FTD generates Syslog messages (same as on classic ASA) and can use any Data Interface as a source (including the Diagnostic). An example of a syslog message that is generated in that case:

```
  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
```

- On the other hand, when Access Control Policy (ACP) **Rule-level logging** is enabled the FTD originates these logs through the **br1** logical interface as a source. The logs are originated from the FTD br1 subinterface:



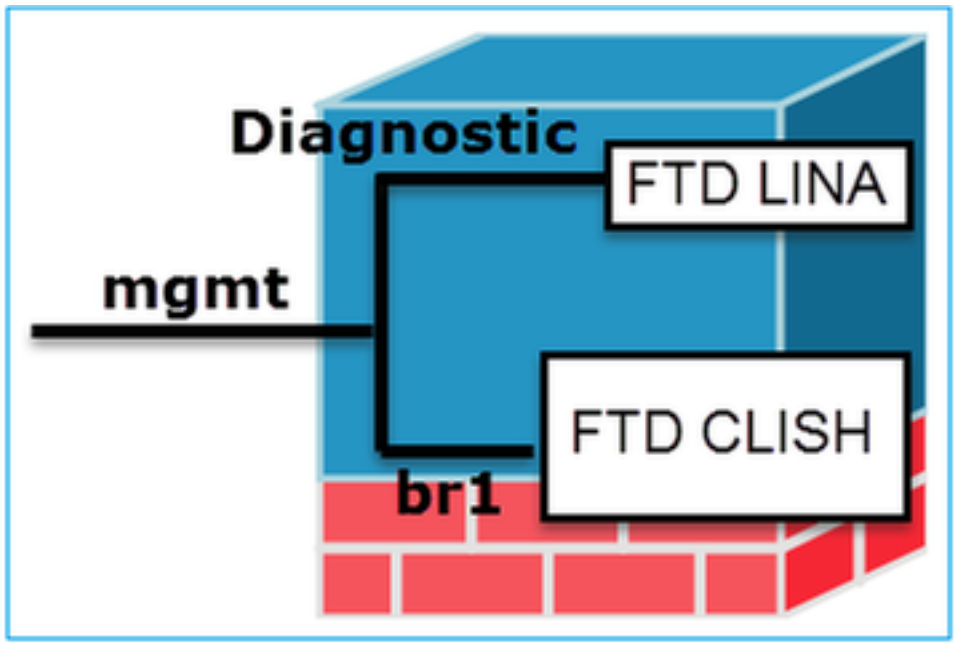
Manage FTD with FDM (On-Box Management)

As from 6.1 version, an FTD that is installed on ASA5500-X appliances can be managed either by FMC (off-box management) or by Firepower Device Manager (FDM) (on-box management).

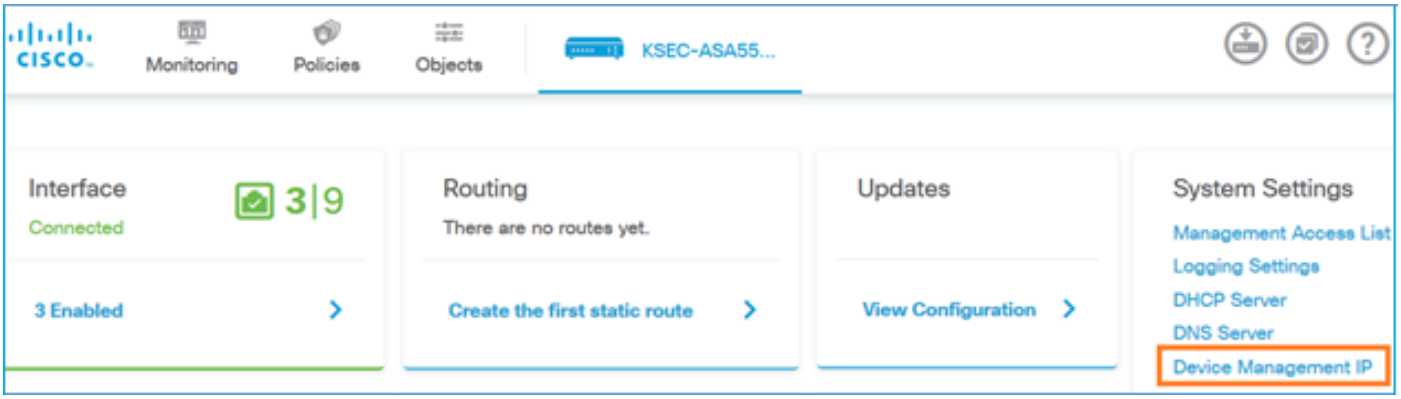
Output from FTD CLISH when the device is managed by FDM:

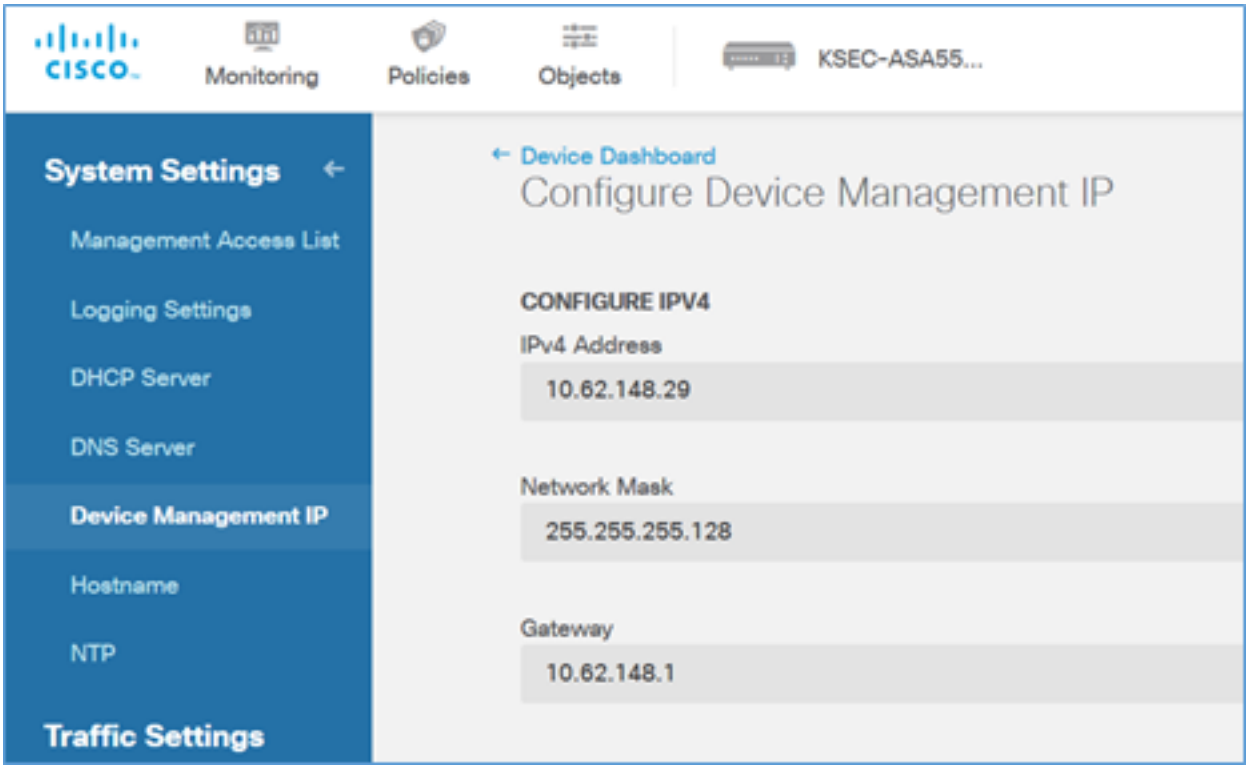
```
> show managers
Managed locally.
>
```

FDM it uses the br1 logical interface. This can be visualized as:



From FDM UI the management interface is accessible from the **Device Dashboard > System Settings > Device Management IP**:





Management Interface on FTD Firepower Hardware Appliances

FTD can be also installed on Firepower 2100, 4100 and 9300 hardware appliances. The Firepower chassis runs its own OS called FXOS while the FTD is installed on a module/blade.

FPR21xx appliance

FPR41xx appliance

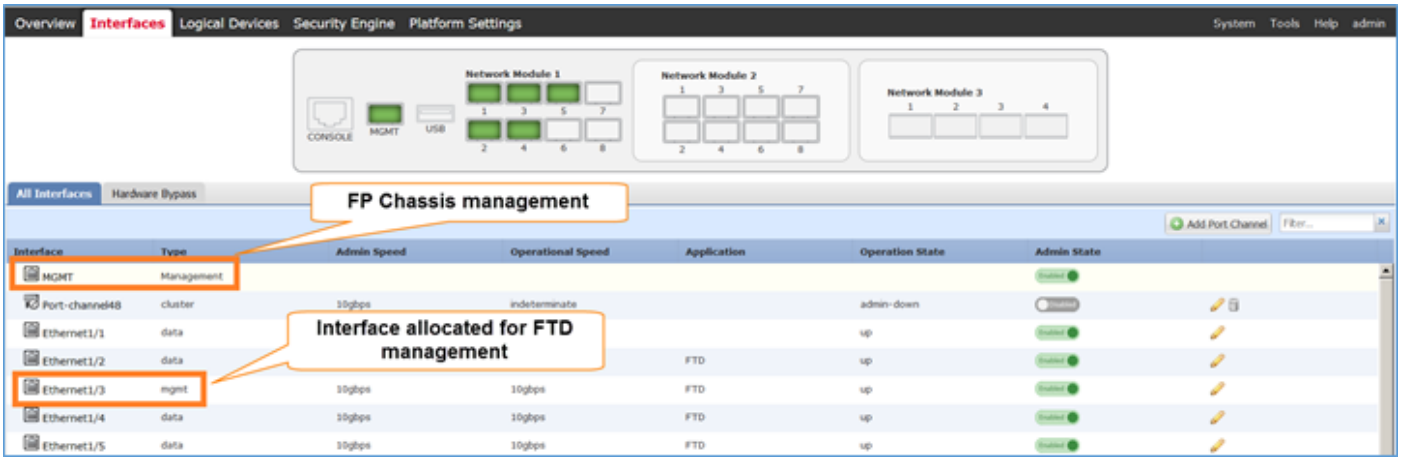
FPR9300 appliance

On FPR4100/9300 this interface is only for the chassis management and cannot be used/shared with the FTD software that runs inside the FP module. For the FTD module allocate a separate data interface that for the FTD management.

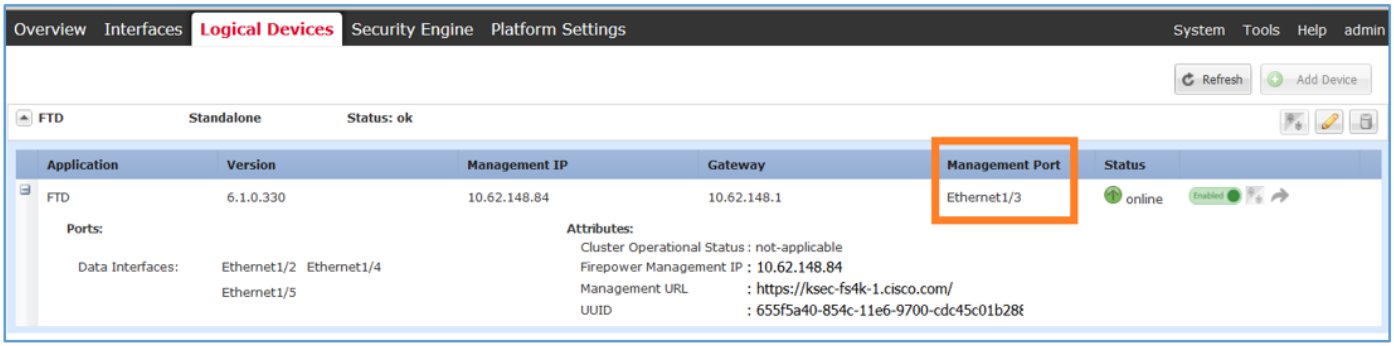
On FPR2100 this interface is shared between the chassis (FXOS) and the FTD logical appliance:

```
> 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#
```

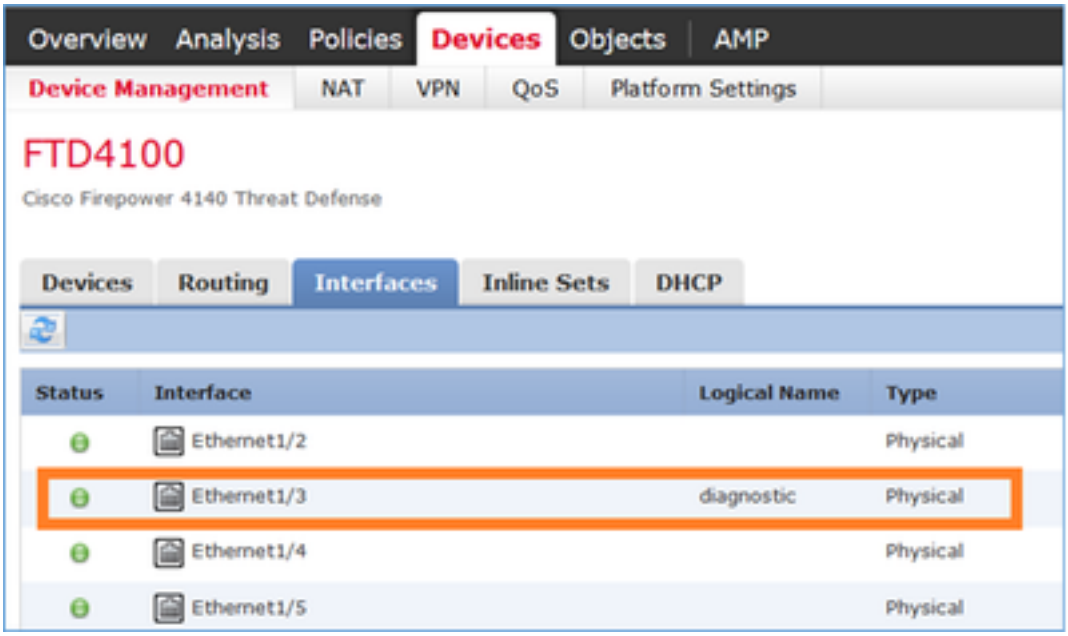
This screenshot is from Firepower Chassis Manager (FCM) UI on FPR4100 where a seperate interface for FTD managment is allocated. In this example Ethernet1/3 is chosen as the FTD management interface: p1



This can be also seen from the **Logical Devices** tab:p2



On FMC the interface is shown as **diagnostic:** p3



CLI Verification

```
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
```

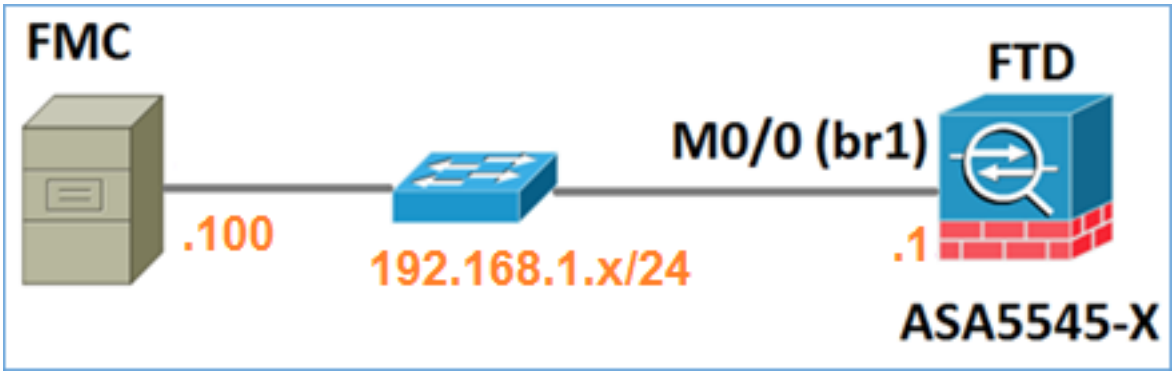
```
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input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

Integrate FTD with FMC - Management Scenarios

Given are some of the deployment options that allows to manage FTD that runs on ASA5500-X devices from FMC.

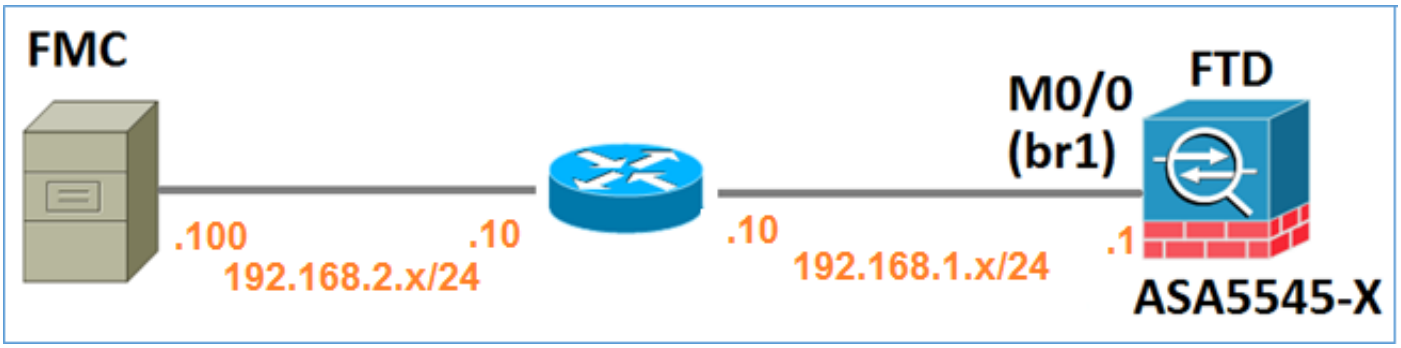
Scenario 1. FTD and FMC on the same subnet.

This is the simplest deployment. As it can be seen in the figure, the FMC is on the same subnet as the FTD br1 interface:



Scenario 2. FTD and FMC on different subnets. Control-plane does not go through the FTD.

In this deployment the FTD must have a route towards the FMC and vice versa. On FTD the next hop is a L3 device (router):



Related Information

- **Firepower System Release Notes, Version 6.1.0**
- **Reimage the Cisco ASA or Firepower Threat Defense Device**
- **Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.1**
- **Technical Support & Documentation - Cisco Systems**