Configure Firepower Threat Defense (FTD) Management Interface

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Post-7.4 Software Releases
- Pre-7.4 Releases
  - Management Interface on ASA 5500-X Devices
  - Management Interface Architecture (pre-7.4 releases)
  - FTD Logging
  - Manage FTD with FDM (On-Box Management)
  - Management Interface on FTD Firepower Hardware Appliances
  - Integrate FTD with FMC - Management Scenarios

Related Information

Introduction

This document describes the operation and configuration of the Management Interface on Cisco Secure Firewall Threat Defense (formelly knowns as Firepower Threat Defense (FTD)).

Note: FTD software versions 7.4 and later support merged Management and Diagnostic interfaces, also known as the Converged Management Interface (CMI).
CMI is enabled by default, and can be disabled by users. For more details see section "Merged management and diagnostic interfaces" at https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/770/management-center-device-config-77/get-started-device-management.html.

The information covered in this document is mainly applicable to firewalls with disabled CMI (unmerged diagnostic and management interfaces).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

- FTD that runs on ASA5508-X hardware appliance

- FTD that runs on ASA5512-X hardware appliance
- FTD that runs on FPR9300 hardware appliance
- FMC that runs on 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

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
- The Management interface on Cisco Secure Firewall devices (1xxx, 12xx, 31xx, 42xx)
- FTD/Firepower Management Center (FMC) integration scenarios

Configure

Post-7.4 Software Releases

As of 7.4, by default the firewall uses the Converged Management Interface (CMI) mode:

<#root>

FTD3100#

show management-interface convergence

management-interface convergence

NAT is used as an internal implementation of CMI:

- An internal private IPv4 address (203.0.113.130) is automatically configured in data plane for IPv4.
- An internal private IPv6 address (fd00:0:1:1::2) is automatically configured in data plane for IPv6.

<#root>

FTD3100#

show interface ip brief

```
Interface                  IP-Address      OK?          Method Status      Protocol
Internal-Data0/1           unassigned      YES          unset  up          up
Port-channel5              192.0.2.1       YES          unset  up          up
Ethernet1/1                unassigned      YES          unset  admin down  down
Ethernet1/2                unassigned      YES          unset  admin down  down
```

```
Ethernet1/5                unassigned      YES           unset  admin down  down
Ethernet1/6                unassigned      YES           unset  admin down  down
Ethernet1/7                unassigned      YES           unset  admin down  down
Ethernet1/8                unassigned      YES           unset  admin down  down
Ethernet1/9                unassigned      YES           unset  admin down  down
Ethernet1/10               unassigned      YES           unset  admin down  down
Ethernet1/11               unassigned      YES           unset  admin down  down
Ethernet1/12               unassigned      YES           unset  admin down  down
Ethernet1/13               unassigned      YES           unset  admin down  down
Ethernet1/14               unassigned      YES           unset  admin down  down
Ethernet1/15               unassigned      YES           unset  admin down  down
Ethernet1/16               unassigned      YES           unset  admin down  down
Internal-Control1/1        unassigned      YES           unset  up          up
Internal-Data1/1           169.254.1.1     YES           unset  up          up
Internal-Data1/2           unassigned      YES           unset  up          up

Management1/1              203.0.113.130   YES           unset  up          up  <----
```

For more details refer to this document https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/222680-claifry-the-purpose-of-ip-address-203-0.html

Pre-7.4 Releases

Management Interface on ASA 5500-X Devices

Note: Most of the ASA 5500-X devices have been announced as End-of-Life and End-of-Sale: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/eos-eol-notice-listing.html

---

When an FTD image is installed on a ASA 55xx device, 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:

```
<#root>

>

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:

```
<#root>

>

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
```

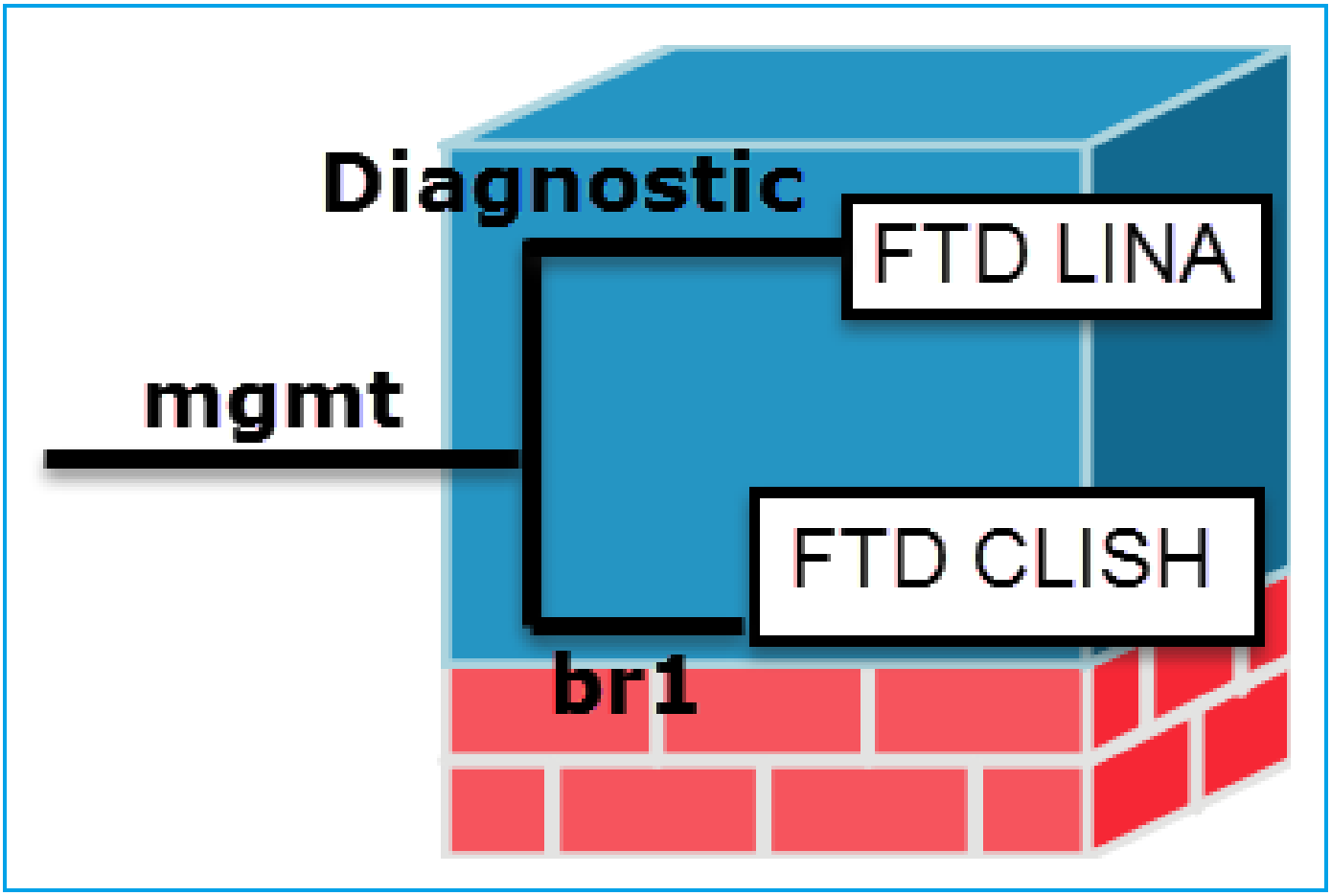
```
                            Number of accelerators: 1
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4

 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

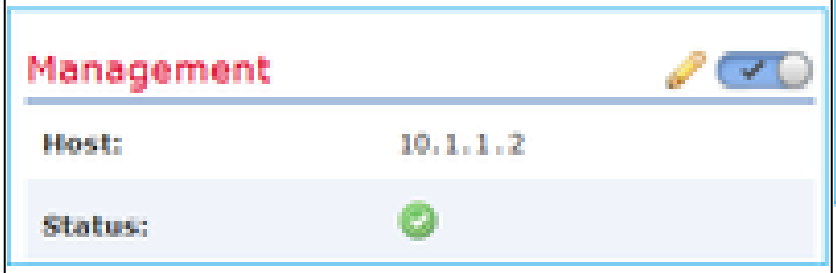
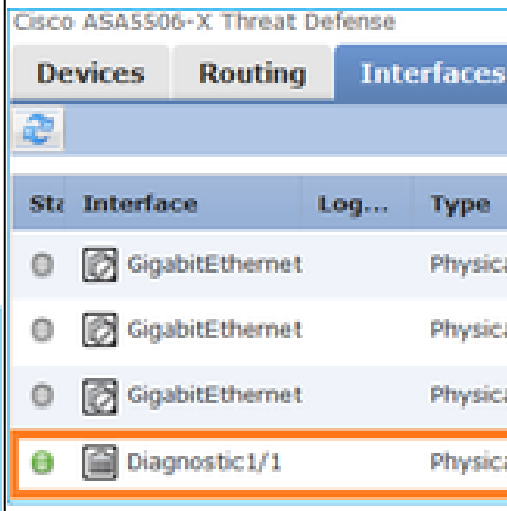

9: Ext: Management0/0       : address is a89d.21ce.fde6, irq 0
```

Management Interface Architecture (pre-7.4 releases)

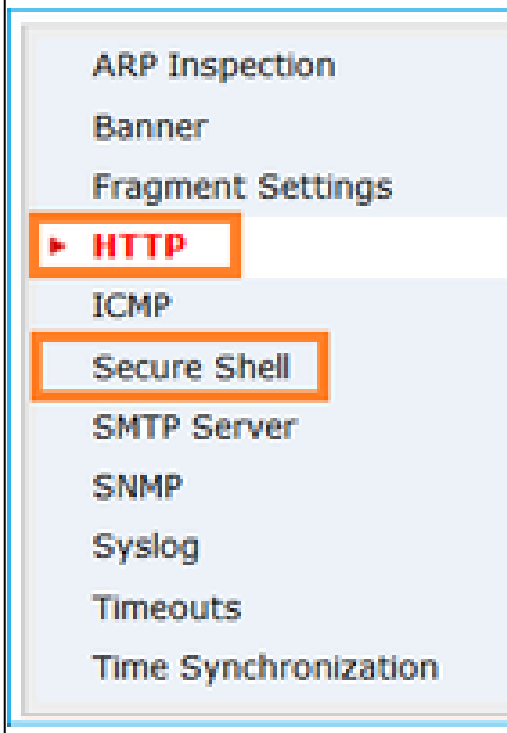
The Management interface is divided into 2 logical interfaces: **br1** (**management0** on FPR2100/4100/9300 appliances) and **diagnostic:**



	Management - **br1/management0**	Management - **Diagnostic**
Purpose	• This interface is used in order to assign the FTD IP that is	• Provides remote access (for exan

<table>
<tr><td></td><td>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.</td><td>SNMP) to ASA engine.
• Used as a source for LINA-level AAA, SNMP etc messages.</td></tr>
<tr><td>Mandatory</td><td>Yes, since it is used for FTD/FMC communication
(the sftunnel terminates on it)</td><td>No and it is not recommended to
configure it. The recommendation is to
a data interface instead* (check the not</td></tr>
<tr><td>Configure</td><td>This interface is configured during FTD installation (setup).
Later you can modify the br1 settings as follows:
<#root>
>
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.

</td><td>The interface can be configured
from FMC GUI:
Navigate to Devices > Device Manage
Select the Edit button and navigate to Interfaces

</td></tr>
<tr><td>Restrict access</td><td>• By default, only the admin user can connect to the FTD br1 subinterface.
• To restrict SSH access is done with the use of the CLISH CLI

> configure ssh-access-list 10.0.0.0/8</td><td>The access to the diagnostic interface
can be controlled by FTD
Devices > Platform Settings >
Secure Shell
and
Devices > Platform Settings> HTTP
respectively</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
</td>
</tr>
<tr>
<td>Verify</td>
<td>Method 1 - From FTD CLI:

<#root>

>

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]-----

Method 2 – From FMC GUI

Devices > Device Management > Device > Management</td>
<td>Method 1 - From LINA CLI:

<#root>

firepower#

show interface ip brief

..
Management1/1 192.168.1.1 YES uns

firepower#

show run interface m1/1

!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.2

Method 2 – From FMC GUI

Navigate to Devices > Device Manage

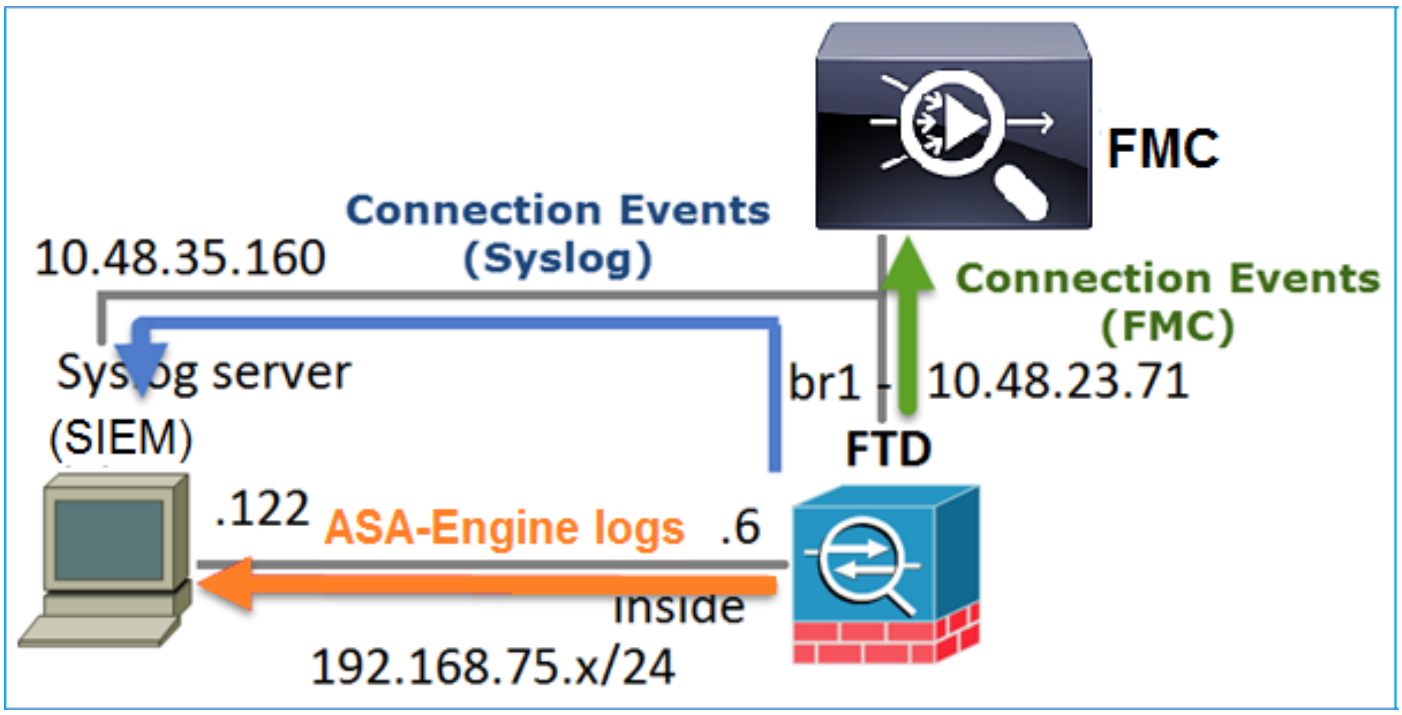
select the Edit button and navigate to Interfaces</td>
</tr>
</table>

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 (includes the Diagnostic). An example of a syslog message that is generated in that case:

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

- 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:

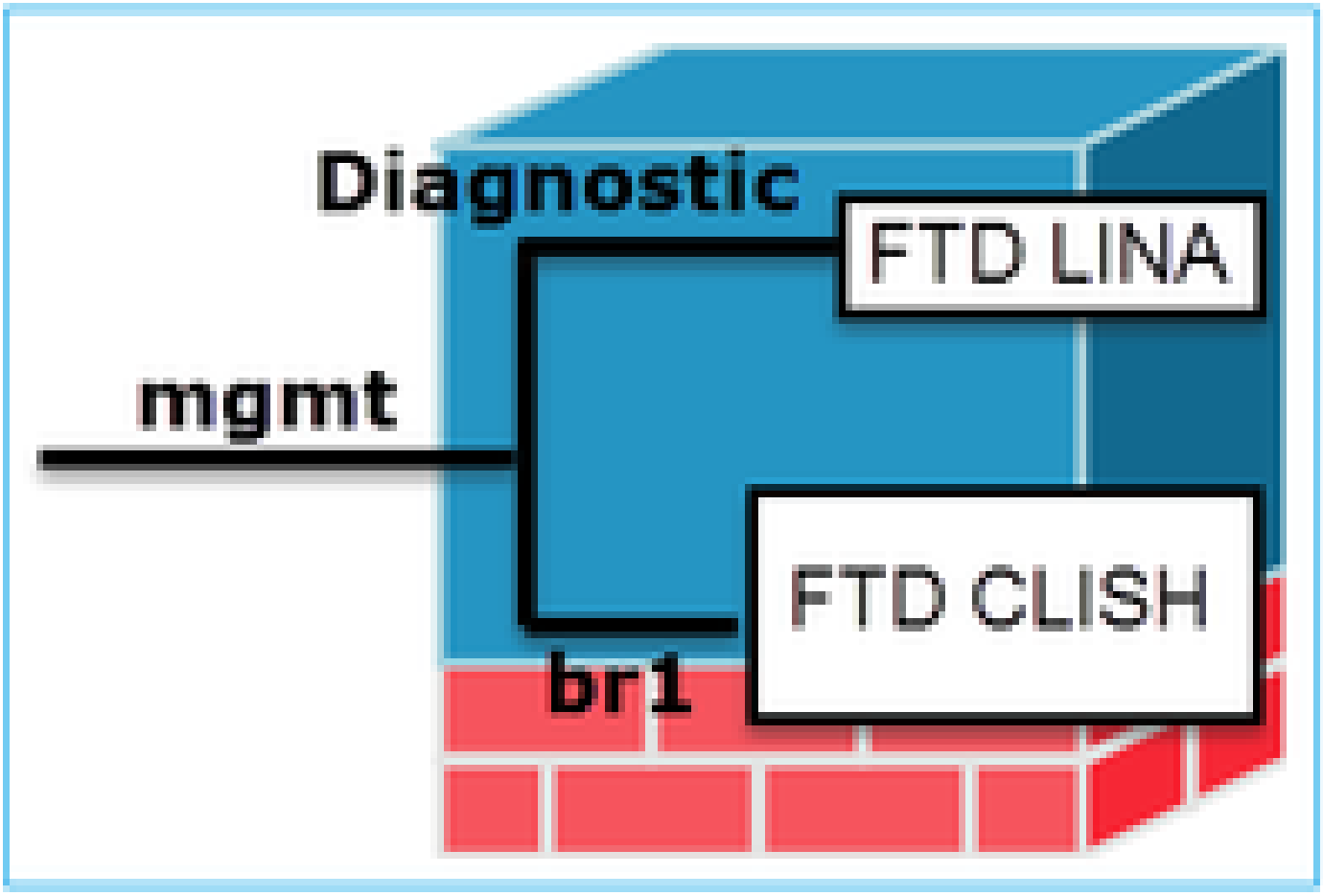
```
<#root>

>

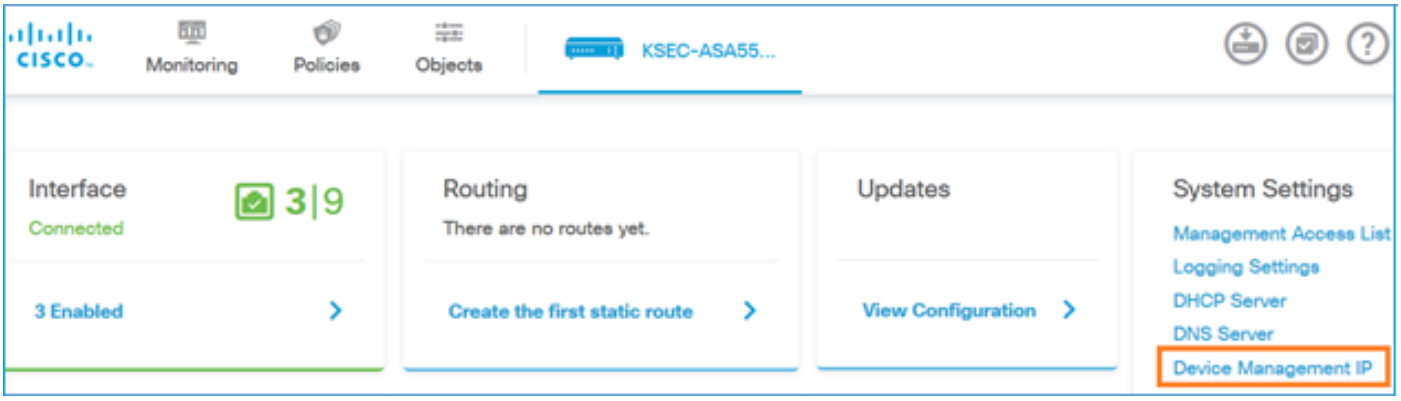
show managers

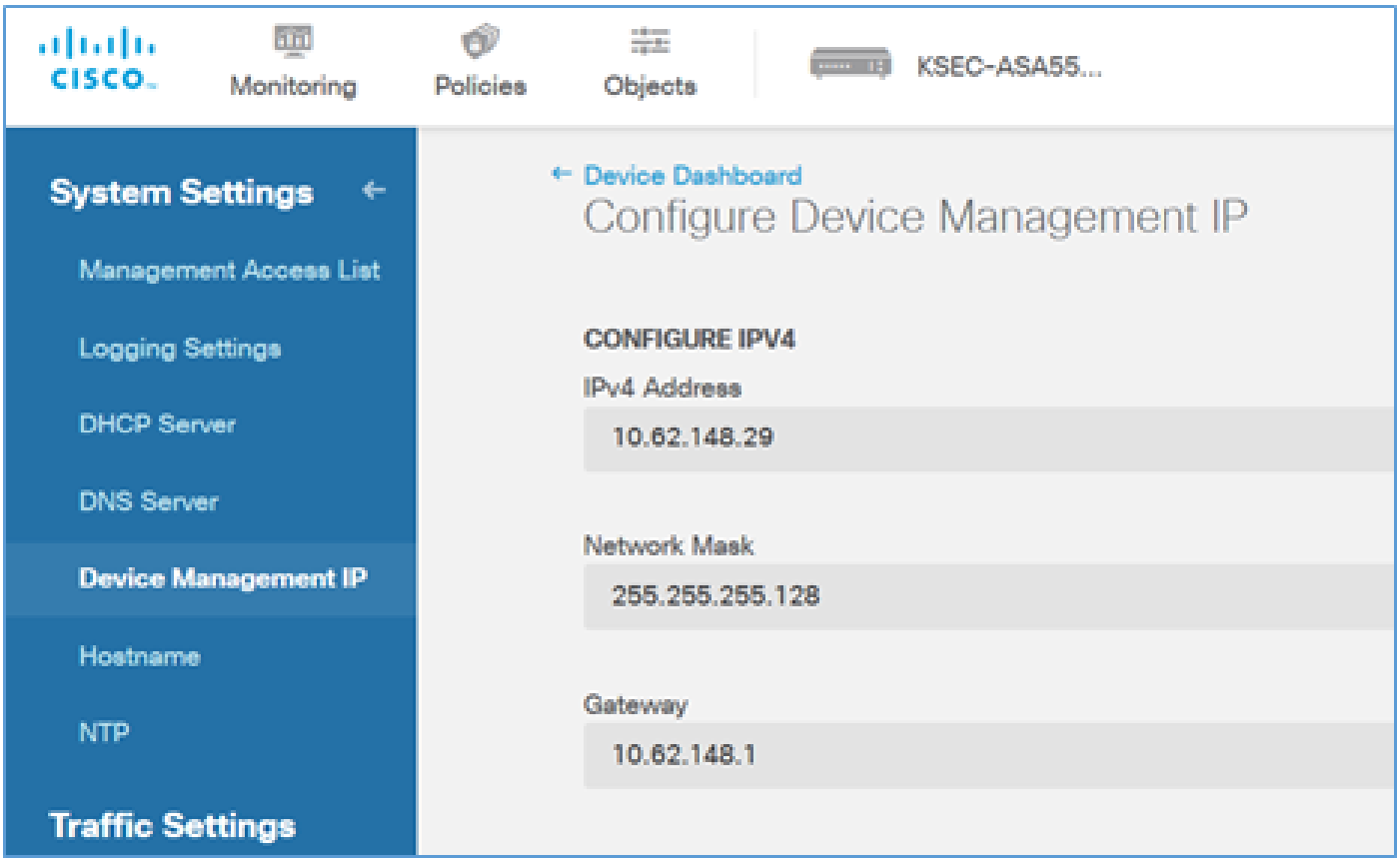
Managed locally.
>
```

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:

```
<#root>

>

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

>

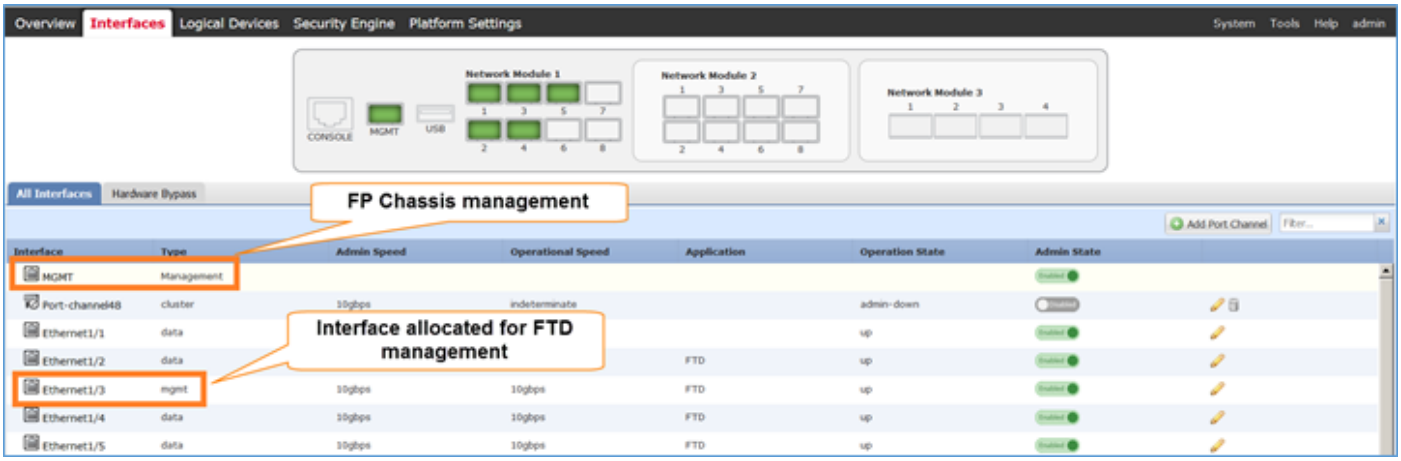
connect fxos

Cisco Firepower Extensible Operating System (

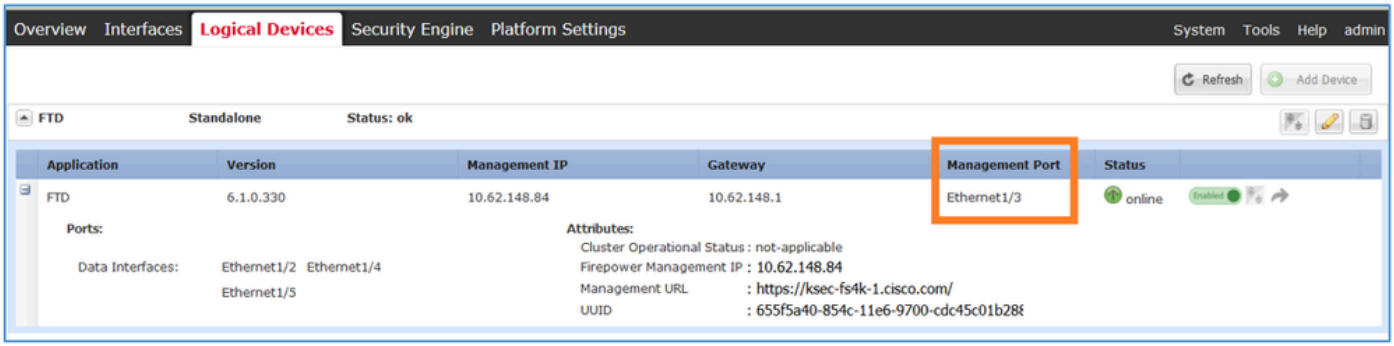
FX-OS
```

```
) Software
...
firepower#
```

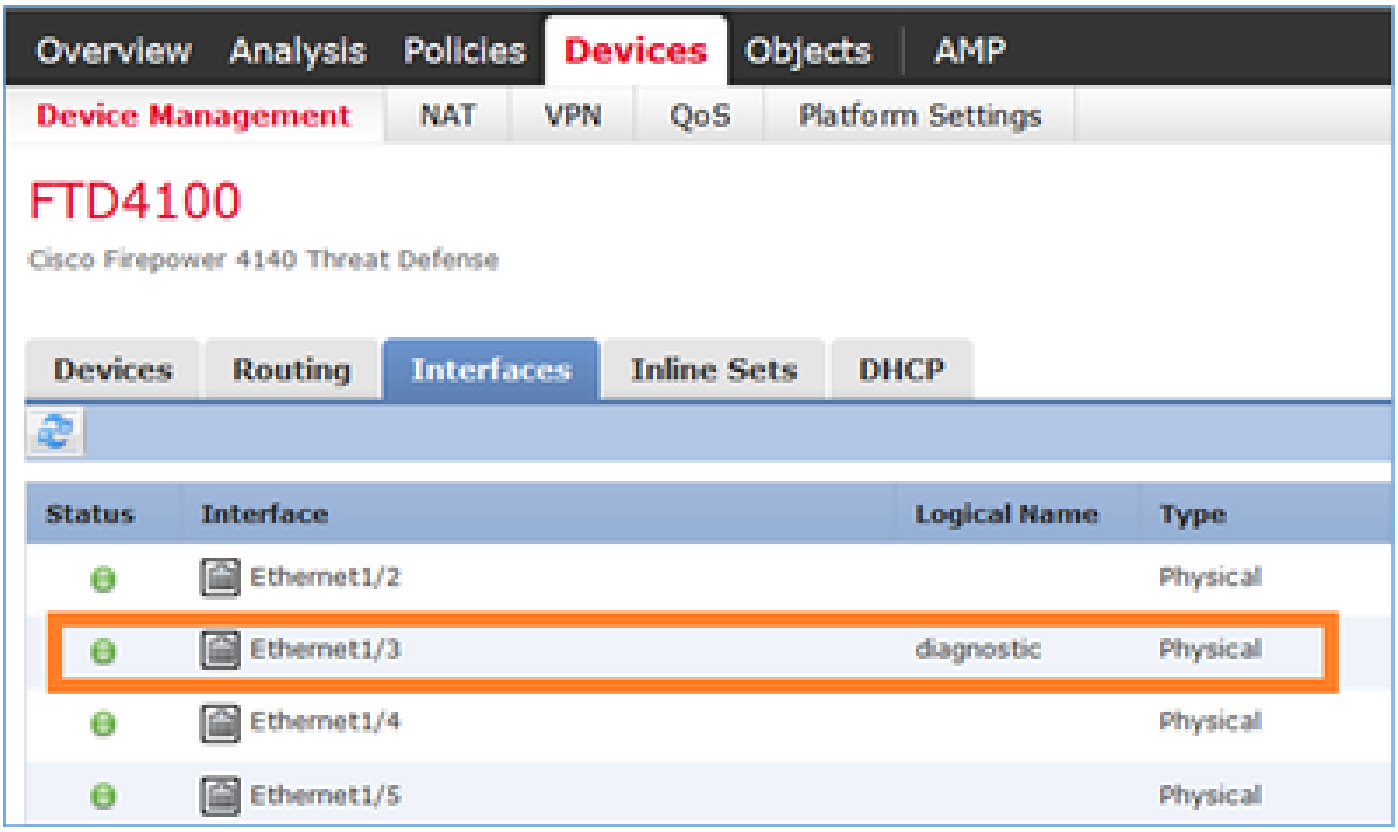
This screenshot is from Firepower Chassis Manager (FCM) UI on FPR4100 where a separate interface for FTD managment is allocated. In this example, Ethernet1/3 is chosen as the FTD management interface: p1



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



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



CLI Verification

<#root>

```
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

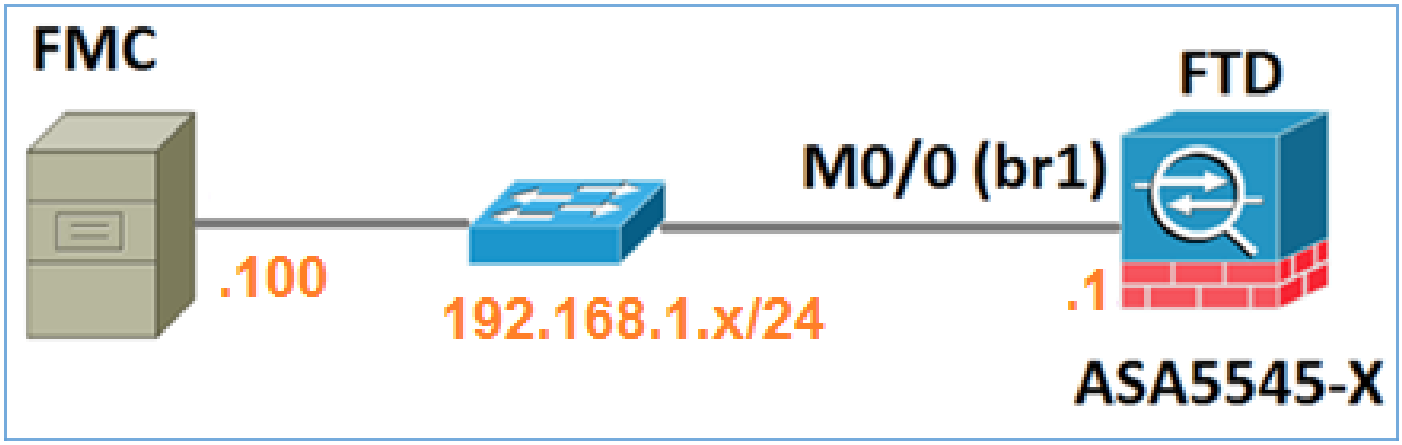
… output omitted …
>
```

Integrate FTD with FMC - Management Scenarios

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

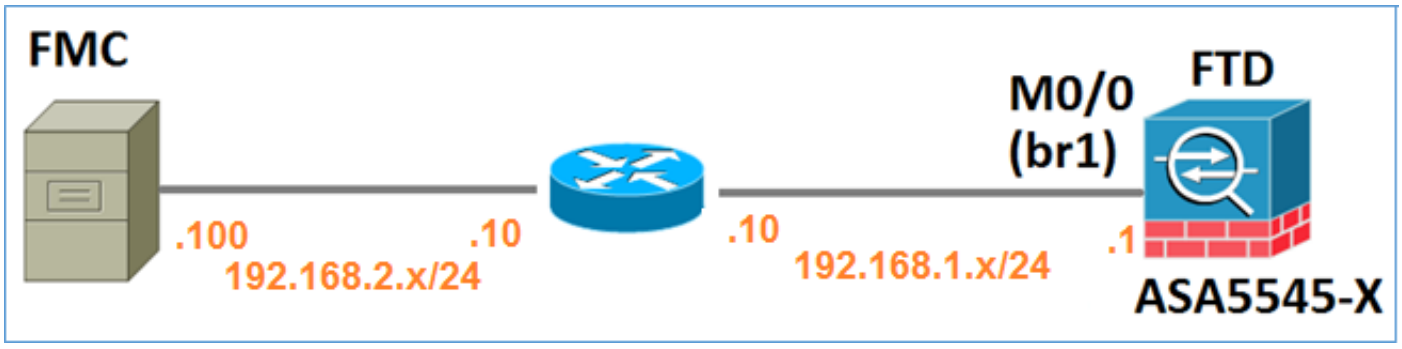
Scenario 1. FTD and FMC on the same subnet.

This is the simplest deployment. As 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

- Technical Support & Documentation - Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/770/management-center-device-config-77/get-started-device-management.html

- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/roadmap/management-center-new-features-by-release.html#new-features-fmc-740