

設定 Firepower 威脅防禦 (FTD) 管理介面

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[ASA 5500-X 裝置的管理介面](#)

[管理介面架構](#)

[FTD 記錄](#)

[藉由 FDM 管理 FTD \(機上管理\)](#)

[FTD Firepower 硬體設備管理介面](#)

[整合 FTD 與 FMC - 管理情境](#)

[案例 1. FTD和FMC位於同一子網中。](#)

[案例 2. 不同子網上的FTD和FMC。控制層面並不通過 FTD。](#)

[相關資訊](#)

簡介

本文件說明 Firepower 威脅防禦 (FTD) 上之管理介面的操作和組態。

必要條件

需求

本文件沒有特定需求。

採用元件

- 在ASA5508-X硬體裝置上運行的FTD
- 在ASA5512-X硬體裝置上運行的FTD
- 在FPR9300硬體裝置上運行的FTD
- 在6.1.0(build 330)上運行的FMC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FTD是可在以下平台上安裝的整合軟體映像：

- 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 路由器模組

本文旨在說明：

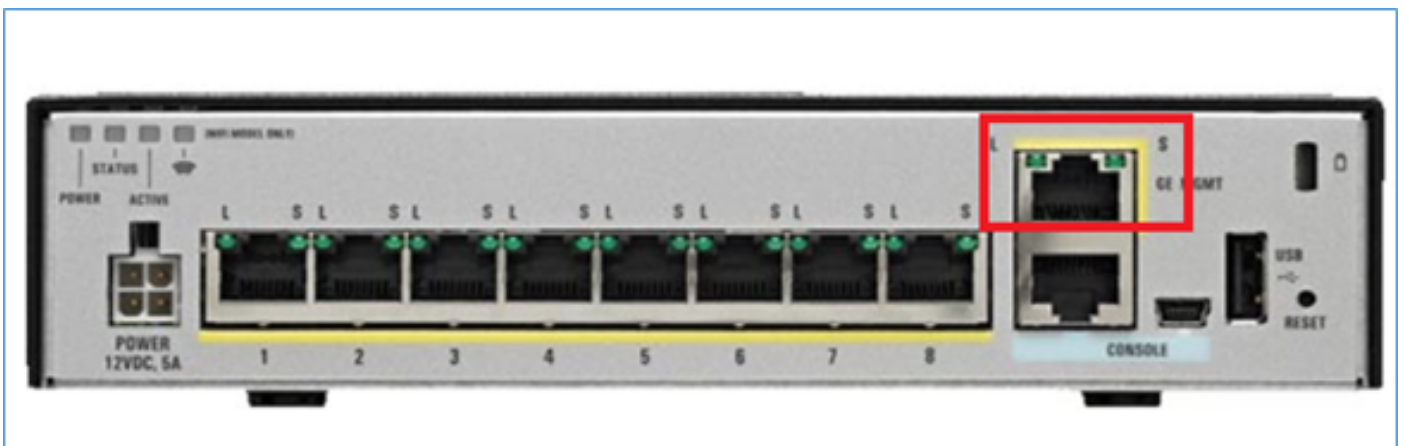
- ASA 5500-X 裝置上的 FTD 管理介面架構
- 使用 FDM 時的 FTD 管理介面
- FP41xx/FP9300 系列上的 FTD 管理介面
- FTD/Firepower 管理中心 (FMC) 整合情況

設定

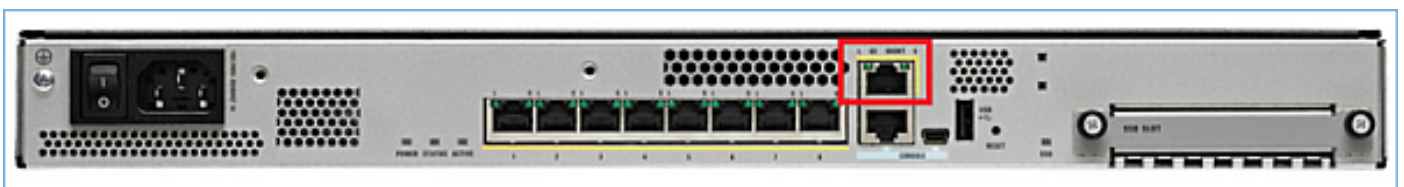
ASA 5500-X 裝置的管理介面

ASA5506/08/16-X 及 ASA5512/15/25/45/55-X 裝置的管理介面。

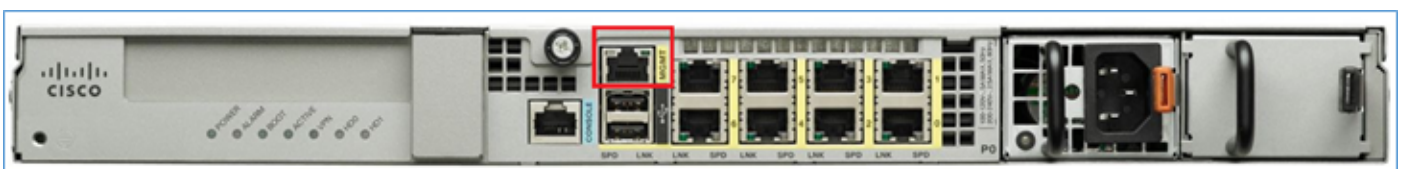
此為 ASA5506-X 的映像檔：



此為 ASA5508-X 的映像檔：



此為 ASA5555-X 的映像檔：



當FTD映像安裝在5506/08/16上時，管理介面顯示為Management1/1。在5512/15/25/45/55-X裝置上，此命令變為Management0/0。在FTD指令行介面(CLI)上，可以在show tech-support輸出中驗證這點。

連接至 FTD 主控台並執行指令：

```
<#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

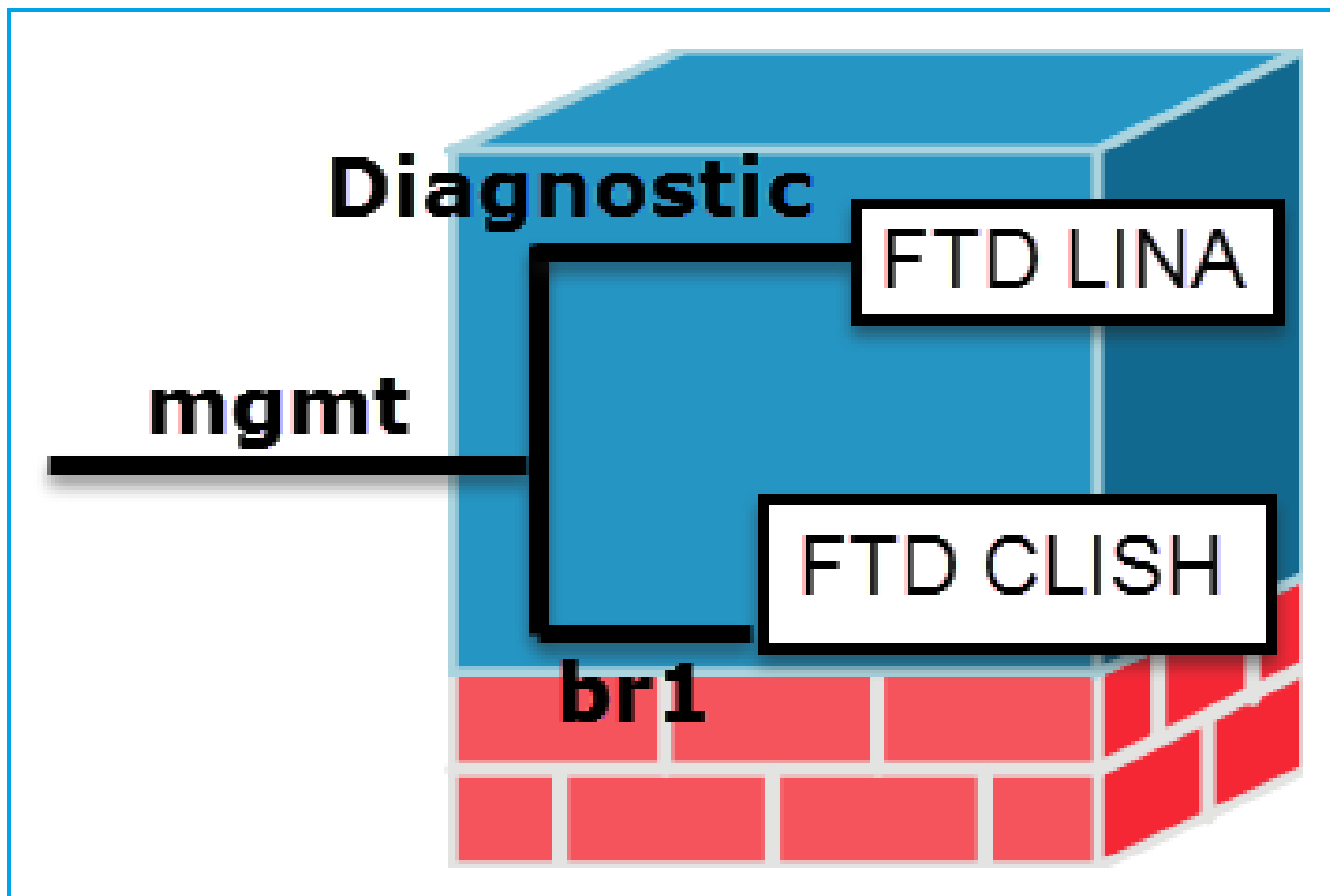
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4

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

管理介面架構

管理介面分為兩個邏輯介面：br1(FPR2100/4100/9300裝置上的management0)和診斷：



	管理 — br1/management0	管理 - 診斷
目的	<ul style="list-style-type: none"> • 使用此介面是為了指派用於 FTD/FMC 通訊的 FTD IP。 • 終止 FMC/FTD 之間的 sftunnel。 • 用作規則型系統日誌的來源。 • 提供 SSH 和 HTTPS 存取權限給 FTD 裝置。 	<ul style="list-style-type: none"> • 提供對ASA引擎的遠端訪問 (例如 , SNMP) 。 • 用作 LINA 層級系統日誌、AAA、SNMP 等訊息的來源。
必填	是，因為它用於 FTD/FMC 通訊 (其 sftunnel 已終止)	否，也不建議 設定。建議改為使用資料介面* (請查看以下附註)
設定	<p>本介面在 FTD 安裝 (設定) 期間設定。</p> <p>往後您可以修改 br1 設定，方法如下：</p> <pre><#root> ></pre>	<p>介面可以透過 FMC GUI 設定：</p> <p>導覽至「裝置」>「裝置管理」，選擇「編輯」按鈕並導覽至「介面」</p>

```
configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1
```


Setting IPv4 network configuration.
Network settings changed.

>

步驟 2.更新FMC上的FTD IP。

Management

Host: 10.1.1.2

Status: 

Cisco ASA5506-X Threat Defense









Devices

Routing

Interfaces

Infir



Sta	Interface	Log...	Type
	 GigabitEthernet		Physical
	 GigabitEthernet		Physical
	 GigabitEthernet		Physical
	 Diagnostic 1/1		Physical

限制訪問

- 預設情況下，只有管理使用者可以連接到 FTD br1 子介面。
- 要限制SSH訪問，可使用CLISH CLI

```
> configure ssh-access-list 10.0.0.0/8
```

診斷界面的存取權限

可由 FTD 控制

「裝置」>「平台設定」>

安全殼層

和

「裝置」>「平台設定」>「HTTP」

分別

ARP Inspection

Banner

Fragment Settings

▶ HTTP

ICMP

Secure Shell

SMTP Server

SNMP

Syslog

Timeouts

Time Synchronization

方法 1 - 從 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 ]-----
```

方法 2 - 從 FMC GUI :

「裝置」 > 「裝置管理」 > 「裝置」 > 「管理」

方法 1 - 從 LINA CLI :

```
<#root>
firepower#
show interface ip brief

..
Management1/1 192.168.1.1 YES unset up u
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
```

方法 2 - 從 FMC GUI :

導覽至「裝置」 > 「裝置管理」，
選擇「編輯」按鈕並導覽至「介面」

*摘自[FTD 6.1使用手冊](#)。

Routed Mode Deployment

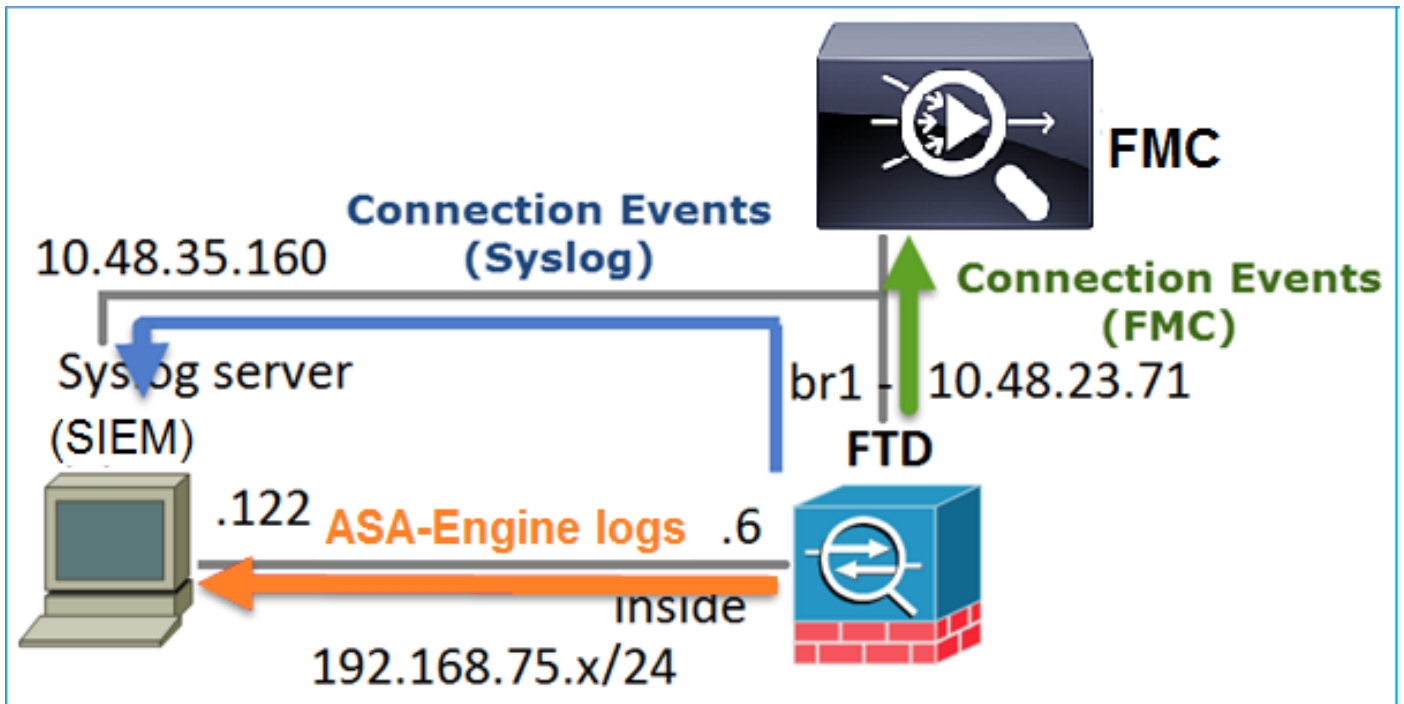
We recommend that you do not configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

- 當使用者從平台設定配置FTD日誌記錄時，FTD將生成系統日誌消息（與傳統ASA上相同），並且可以使用任何資料介面作為源（包括診斷）。在該情況下產生的系統日誌訊息範例：

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

- 另一方面，當啟用存取控制原則 (ACP) 規則層級日誌記錄時，FTD 透過 br1 邏輯介面做為來源產生這些日誌。日誌記錄由 FTD br1 子介面產生：



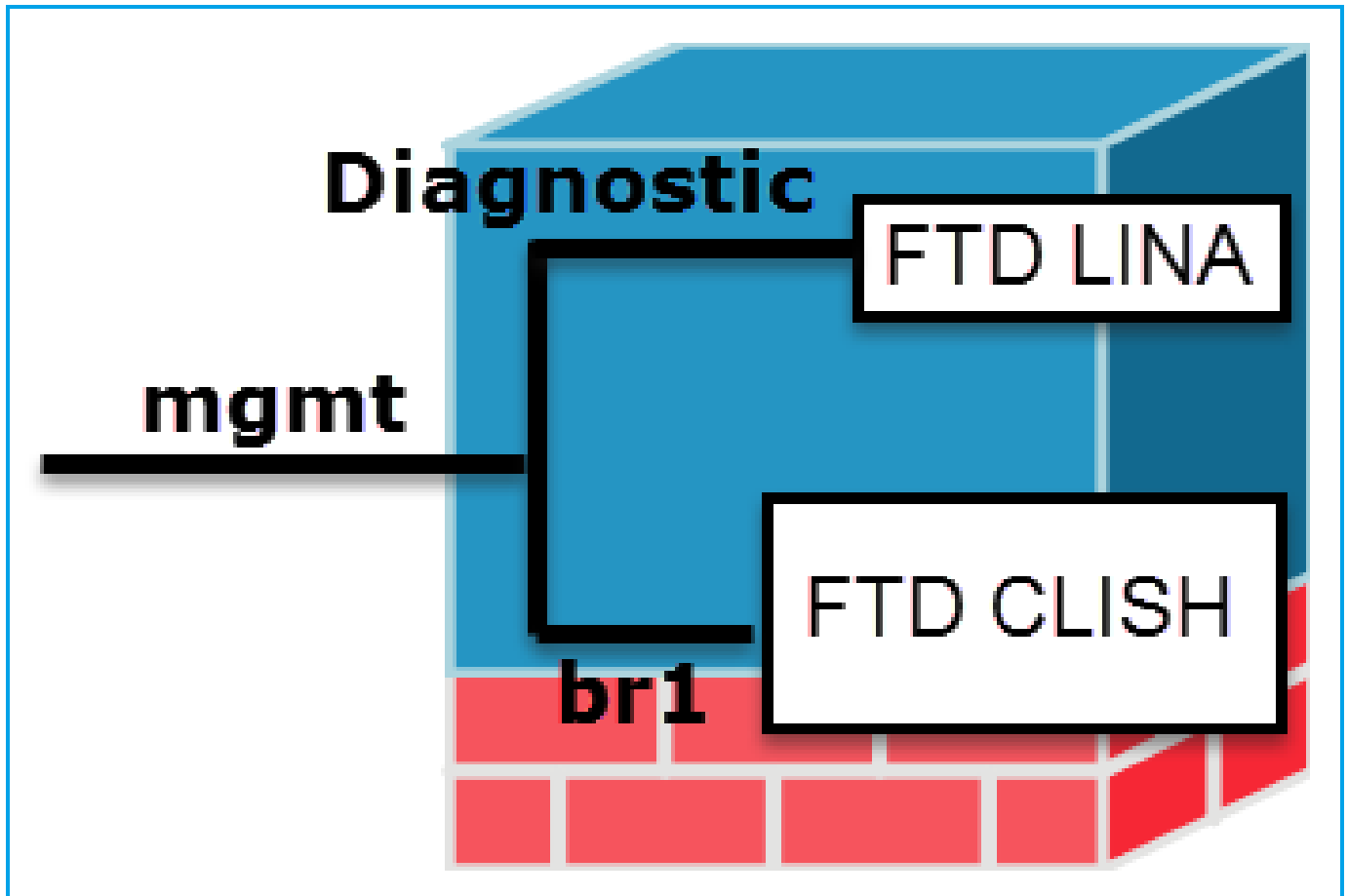
藉由 FDM 管理 FTD (機上管理)

從 6.1 版本開始，安裝在 ASA5500-X 設備上的 FTD 可以透過 FMC (機下管理) 或 Firepower 裝置管理員 (FDM) (機上管理) 加以管理。

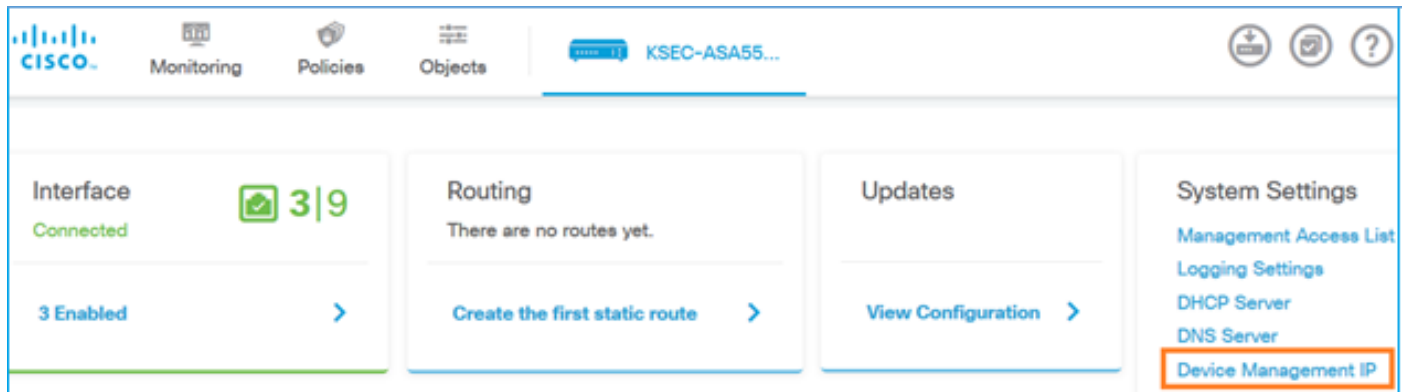
裝置由 FDM 管理時，來自 FTD CLISH 的輸出：

```
<#root>
>
show managers
Managed locally.
>
```

FDM 使用 br1 邏輯介面。其視覺化結果為：



在 FDM UI 中，可以從「裝置儀表板」>「系統設定」>「裝置管理 IP」存取管理界面：





FTD Firepower 硬體設備管理介面

FTD 也可以安裝於 Firepower 2100、4100 和 9300 硬體設備。Firepower 機箱執行名稱為 FXOS 的專用作業系統，而 FTD 安裝於模組/刀鋒。

FPR21xx 設備



FPR41xx 設備



FPR9300 設備



在 FPR4100/9300 上，此介面僅用於機箱管理，不能與在 FP 模組內執行的 FTD 軟體搭配使用/共用。為 FTD 模組分配一個單獨的資料介面，用於 FTD 管理。

在 FPR2100 上，此介面由機箱 (FXOS) 與 FTD 邏輯設備共用：

```
<#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

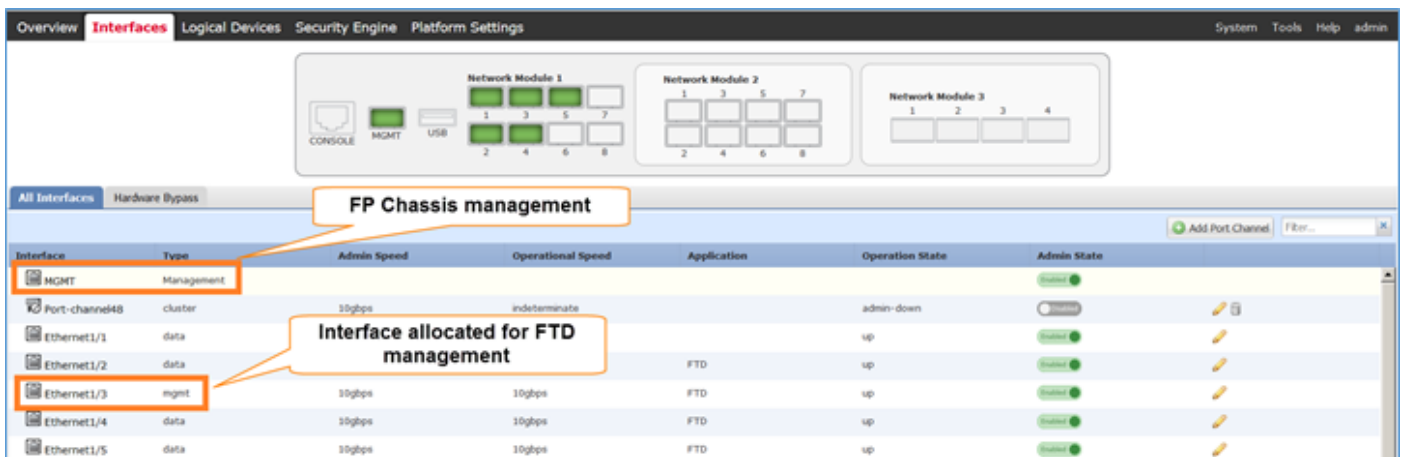
===== [
management0
] =====
State               : Enabled
Channels            : Management & Events
Mode                : Non-Autonegotiation
MDI/MDIX            : Auto/MDIX
MTU                 : 1500
MAC Address         : 70:DF:2F:18:D8:00
----- [ IPv4 ] -----
Configuration       : Manual
Address             : 10.62.148.179
Netmask             : 255.255.255.128
Broadcast           : 10.62.148.255
----- [ IPv6 ] -----
Configuration       : Disabled

>
connect fxos

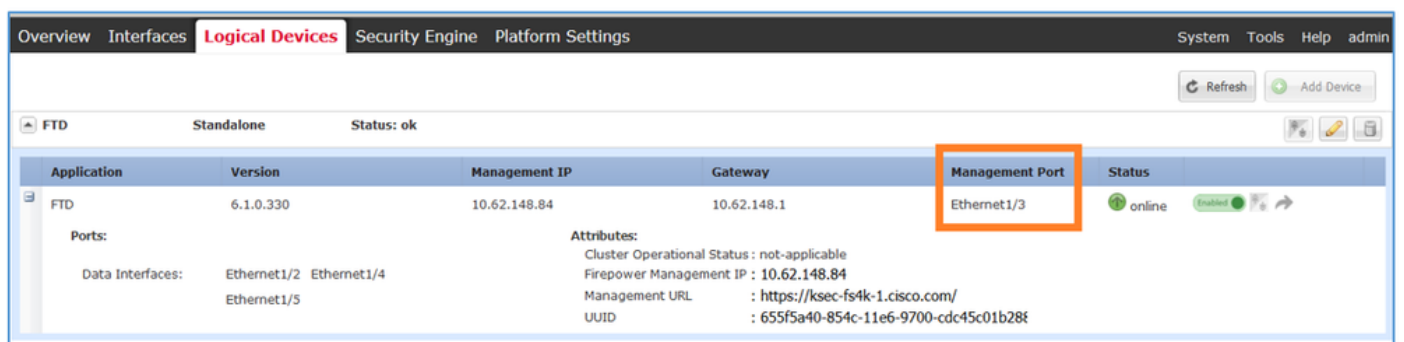
Cisco Firepower Extensible Operating System (
FX-OS
```

) Software
...
firepower#

此螢幕截圖來自FPR4100上的Firepower機箱管理器(FCM)UI，其中分配了單獨的FTD管理介面。在本範例中，Ethernet1/3被選為FTD管理介面：p1



也可以從Logical Devices頁籤：p2中看到此資訊



在FMC上，介面顯示為diagnostic: p3

Overview Analysis Policies **Devices** Objects AMP

Device Management NAT VPN QoS Platform Settings

FTD4100

Cisco Firepower 4140 Threat Defense

Devices Routing **Interfaces** Inline Sets DHCP

Status	Interface	Logical Name	Type
	Ethernet1/2		Physical
	Ethernet1/3	diagnostic	Physical
	Ethernet1/4		Physical
	Ethernet1/5		Physical

CLI 驗證

```
<#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
```

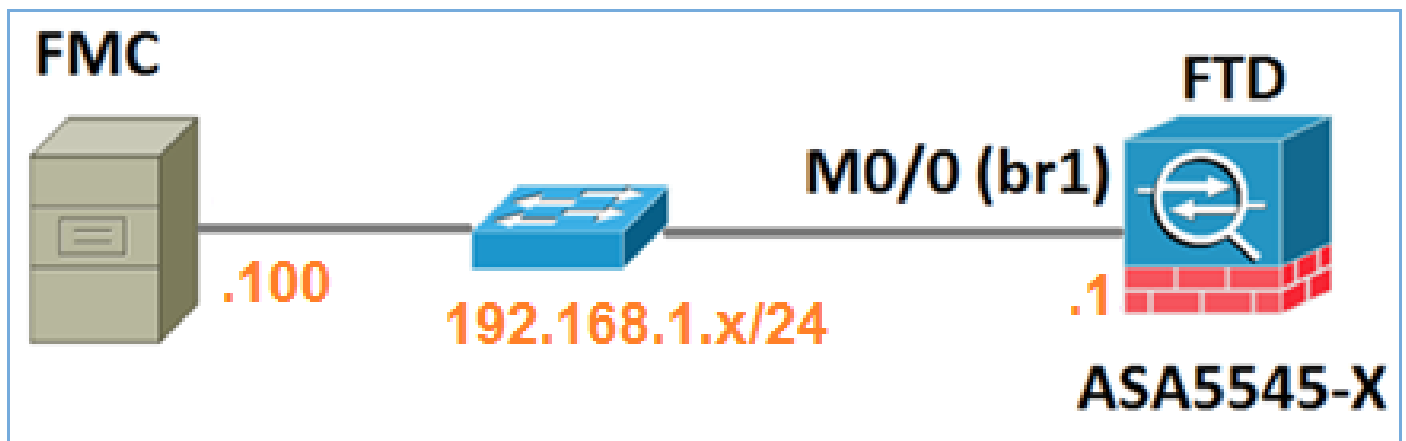
... output omitted ...
>

整合 FTD 與 FMC - 管理情境

以下是允許從FMC管理ASA5500-X裝置上運行的FTD的一些部署選項。

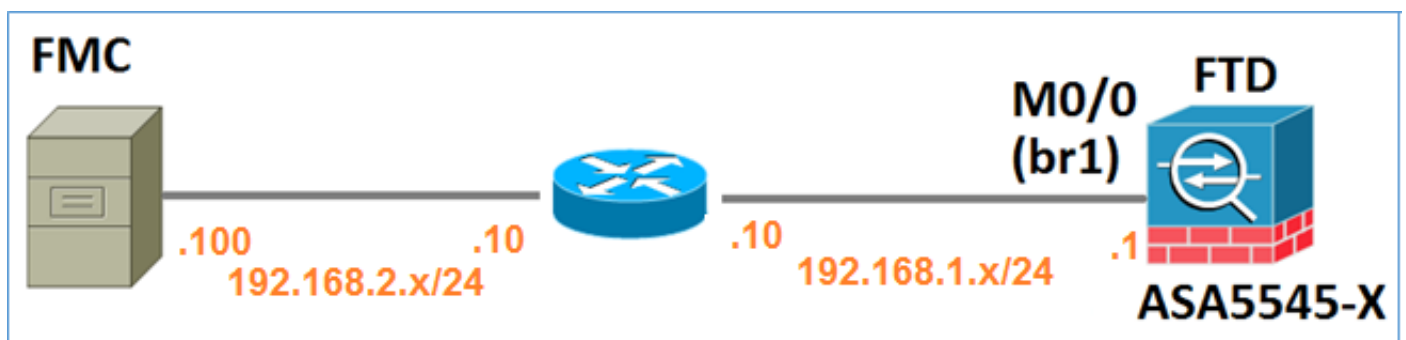
案例 1.FTD和FMC位於同一子網中。

這是最簡單的部署。如圖所示，FMC與FTD br1介面位於同一子網中：



案例 2.不同子網上的FTD和FMC。控制層面並不通過 FTD。

在此部署中，FTD必須具有通向FMC的路由，反之亦然。在 FTD 上，下一個躍點是 L3 裝置（路由器）：



相關資訊

- [Firepower 系統版本資訊, 6.1.0 版本](#)
- [重新安裝 Cisco ASA 或 Firepower 威脅防禦裝置映像檔](#)
- [適用於 Firepower 裝置管理員 6.1 版的 Cisco Firepower 威脅防禦設定指南](#)

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。