Firepower Threat Defense（FTD）管理インターフェイスの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

[設定](#)

- [ASA 5500-X デバイスの管理インターフェイス](#)
- [管理インターフェイス アーキテクチャ](#)
- [FTD のロギング](#)
- [FDM での FTD の管理（オンボックス管理）](#)
- [FTD Firepower ハードウェアアプライアンスの管理インターフェイス](#)
- [FTD と FMC の統合 - 管理シナリオ](#)
  - [シナリオ 1.FTDとFMCが同じサブネット上にある。](#)
  - [シナリオ 2.異なるサブネット上のFTDとFMC。コントロール プレーンが FTD を通過しない。](#)

[関連情報](#)

はじめに

このドキュメントでは、Firepower Threat Defense（FTD）での管理インターフェイスの動作と設定について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

- ASA5508-Xハードウェアアプライアンスで稼働するFTD
- ASA5512-Xハードウェアアプライアンスで稼働するFTD
- FPR9300ハードウェアアプライアンスで稼働するFTD
- 6.1.0（ビルド330）で稼働するFMC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

FTDは、次のプラットフォームにインストールできる統合ソフトウェアイメージです。

- 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 ルータ モジュール

このドキュメントの目的は以下の事項の説明です。

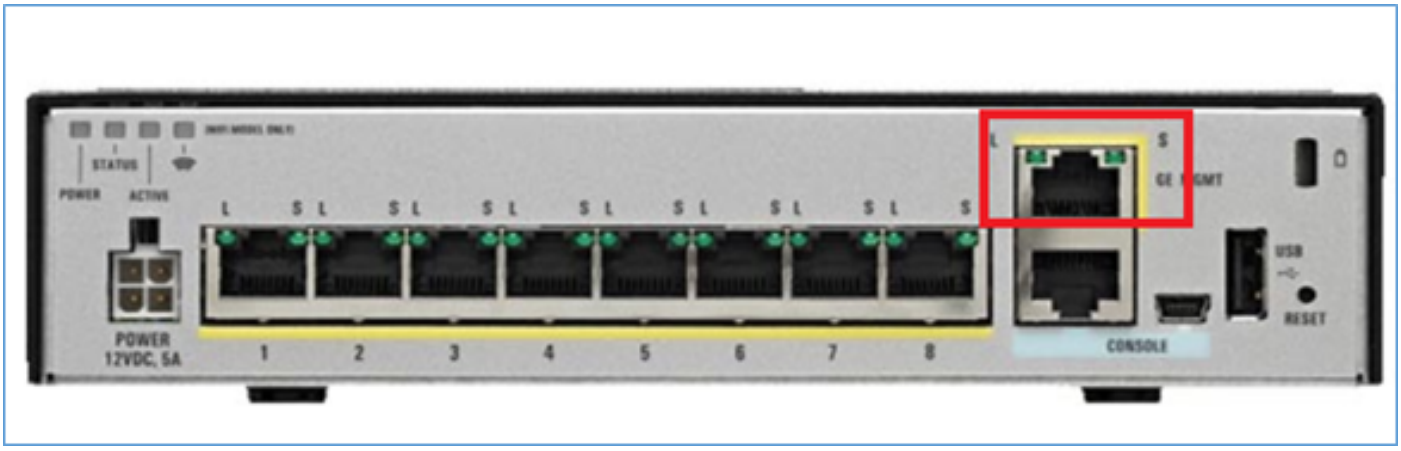
- ASA5500-X デバイスの FTD 管理インターフェイス アーキテクチャ
- FDM 使用時の FTD 管理インターフェイス
- FP41xx/FP9300 シリーズでの FTD 管理インターフェイス
- FTD/Firepower Management Center（FMC）の統合のシナリオ

設定

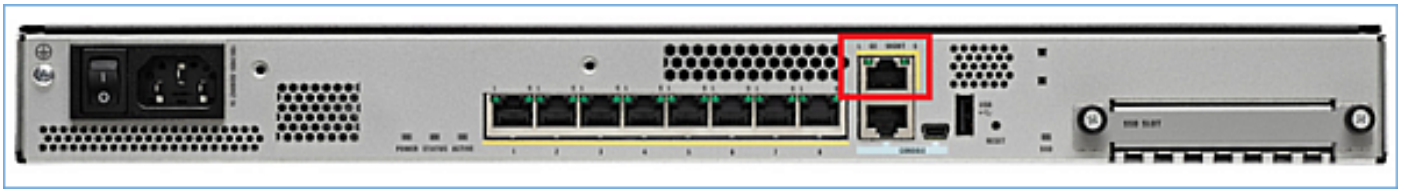
ASA 5500-X デバイスの管理インターフェイス

ASA5506/08/16-X および ASA5512/15/25/45/55-X デバイスの管理インターフェイス。

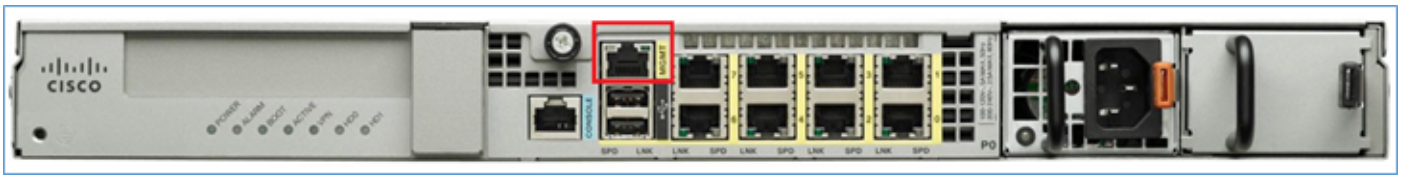
以下は ASA5506-X の画像です。



以下は ASA5508-X の画像です。



以下は ASA5555-X の画像です。



FTD イメージが 5506/08/16 にインストールされている場合、管理インターフェイスは Management1/1 と表示されます。5512/15/25/45/55-X デバイスでは、これが Management0/0 と表示されます。FTD コマンドライン インターフェイス (CLI) から show tech support を実行すると、この表示を確認できます。

FTD コンソールに接続して、次のコマンドを実行します。

<#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 の場合

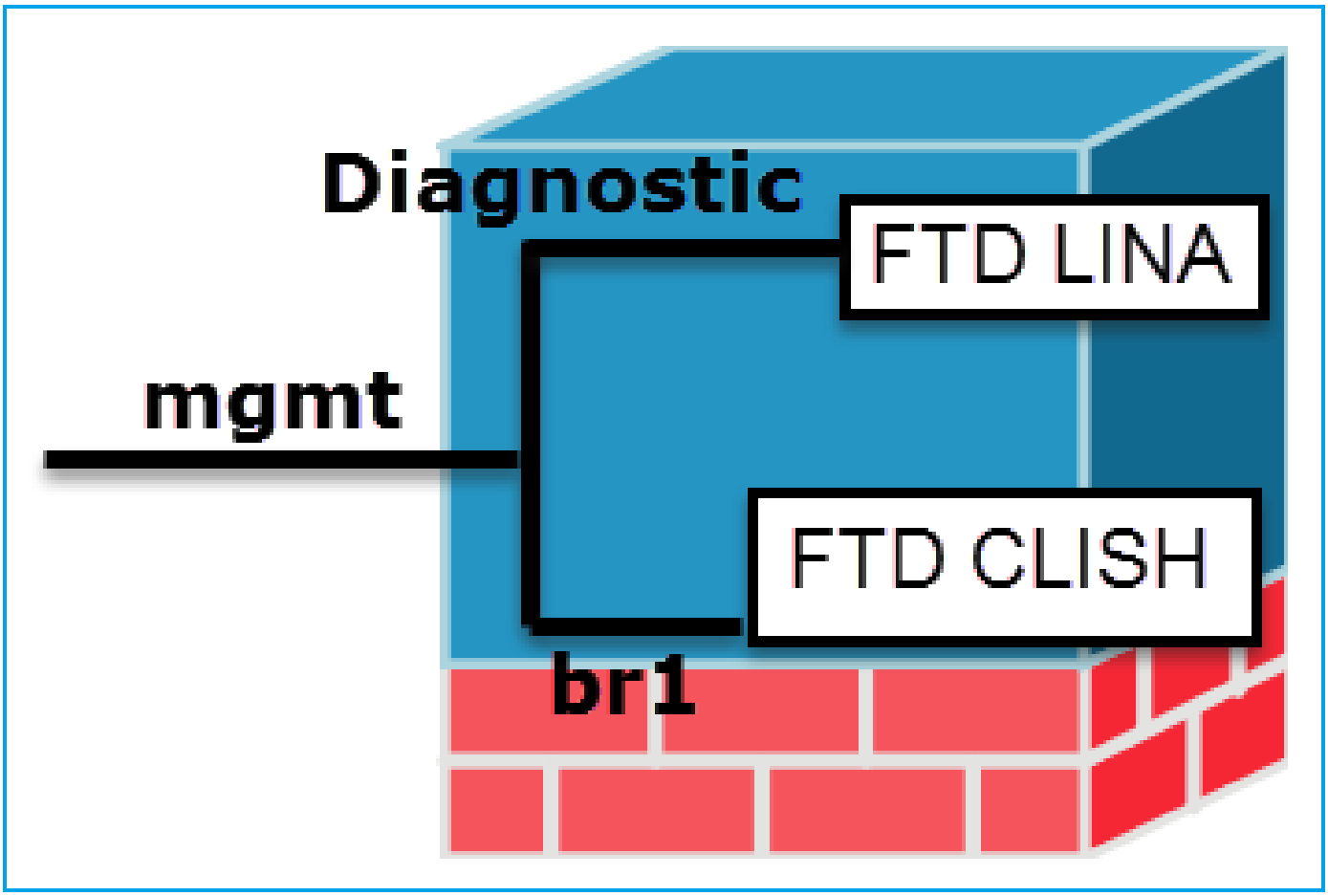
<#root>

```
>

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
```

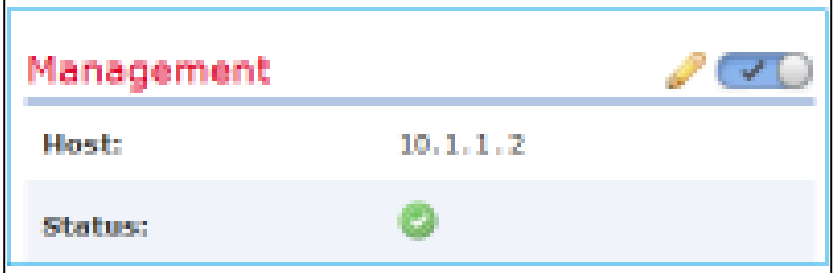
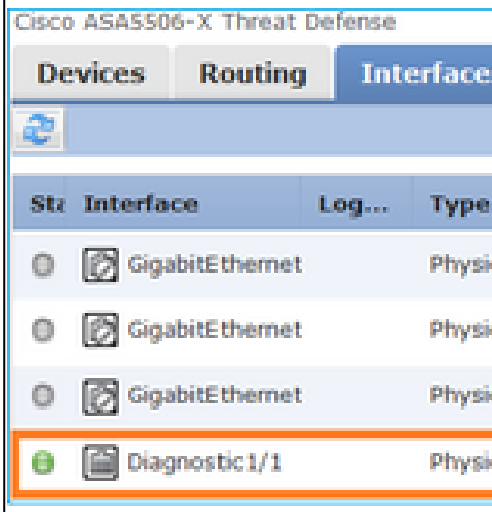
管理インターフェイス アーキテクチャ

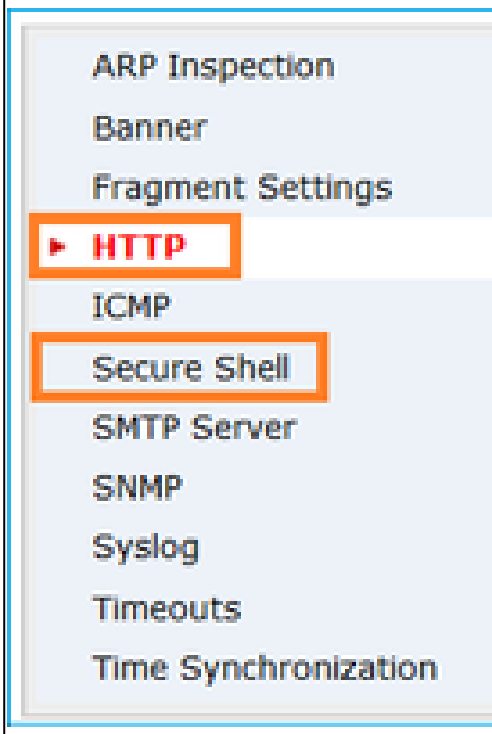
管理インターフェイスは、br1(FPR2100/4100/9300アプライアンスではmanagement0)と

diagnosticの2つの論理インターフェイスに分けられます。



	管理- br1/management0（管理0）	管理 - 診断
目的	• このインターフェイスは、FTD/FMC 通信に使用される FTD の IP を割り当てるために使用されます。 • FMC/FTD 間における sftunnel の終端となります。 • ルールベースの syslog の送信元として使用されます。 • SSH および HTTPS による、FTD アプライアンスへのアクセスを可能にします。	• ASAエンジンへのリモートア（SNMPなど）を提供します • LINA レベルの syslog、AAA などによるメッセージの送信て使用されます。
Mandatory	はい、FTD/FMC 通信に使用されるため （sftunnel が終端します）	いいえ、設定することは 推奨されません。代わりにデータフェイスを 使用することをお勧めします（後参照）
設定	このインターフェイスは、FTD のインストール（設定	FMC GUI からインターフェイスを

	）の間に設定されます。 br1 の設定は後で次のように変更できます。 <#root> > **configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1** Setting IPv4 network configuration. Network settings changed. > ステップ 2：FMCでFTD IPを更新します。  	設定できます [デバイス（Devices）] > [デバイス （Device Management）] に移動し [編集（Edit）] ボタンを選択して、 ーフェイス（Interfaces）] に移動 
アクセスの制限	• デフォルトでは、admin ユーザのみが FTD br1 サブインターフェイスに接続できます。 • SSHアクセスを制限するには、CLISH CLIを使用します > configure ssh-access-list 10.0.0.0/8	FTD では、診断インターフェイス セスを制御できます。 FTD によって制御できます [Devices] > [Platform Settings] > [Secure Shell] と [Devices] > [Platform Settings] > [H それぞれに対応

<table>
<tr>
<td></td>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>確認</td>
<td>方法 1 - FTD CLI から:

<#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 – FMC GUI から:

[Devices] > [Device Management] > [Device] > [Management]</td>
<td>方法 1：LINA CLI の場合

<#root>

firepower#
show interface ip brief

..
Management1/1 192.168.1.1 YES ur

firepower#
show run interface m1/1

!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.

方法 2 – FMC GUI から:

[デバイス（Devices）] > [デバイス（Device Management）] に移動し

[編集（Edit）] ボタンを選択して、インターフェイス（Interfaces）] に移動</td>
</tr>
</table>

* FTD 6.1ユーザガイドからの抜粋。

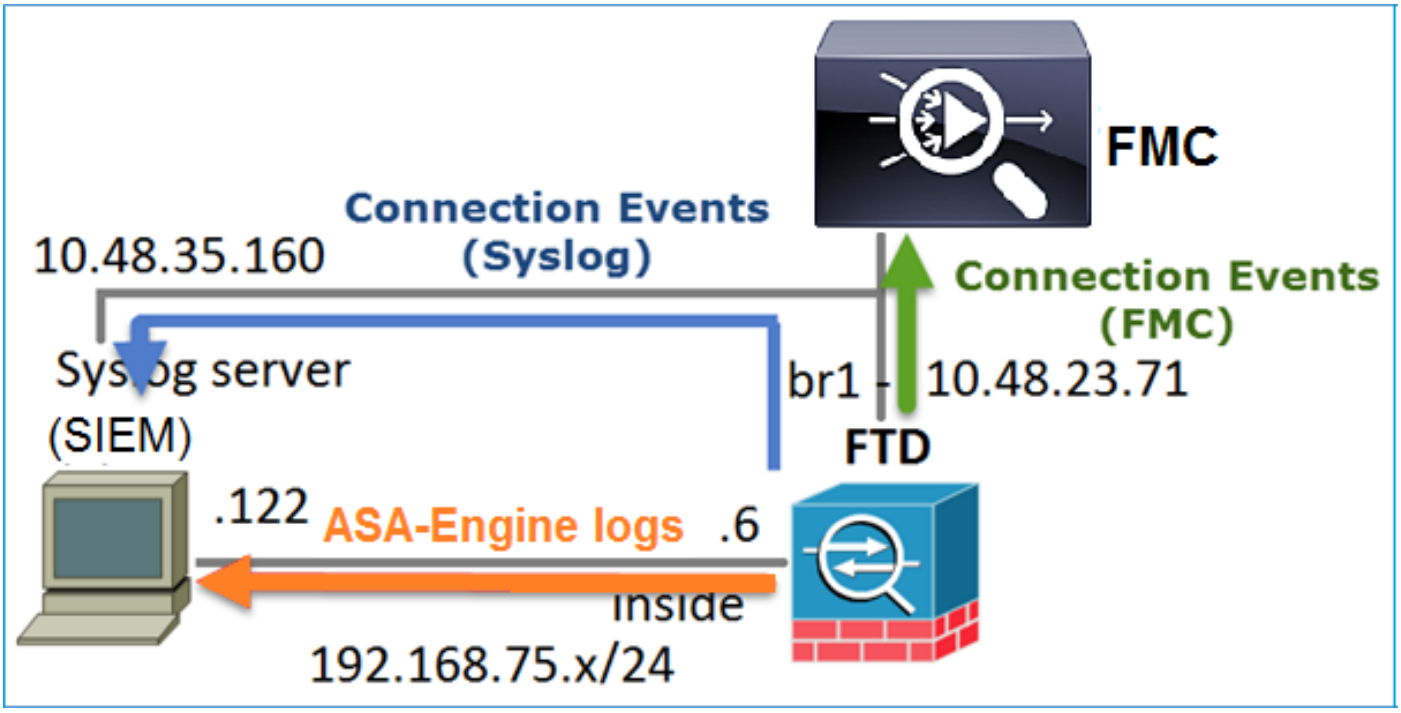
> **Routed Mode Deployment**
>
> We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other 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 のロギング

- ユーザがプラットフォーム設定からFTDロギングを設定すると、FTDは（従来のASAと同じ）Syslogメッセージを生成し、送信元として任意のデータインターフェイスを使用できます（診断を含む）。その場合に生成される syslog メッセージの例を次に示します。

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

- 一方、アクセスコントロールポリシー(ACP)ルールレベルロギングが有効な場合、FTDは送信元としてbr1論理インターフェイスを介してこれらのログを発信します。FTD br1 サブインターフェイスが、ログの送信元になります。



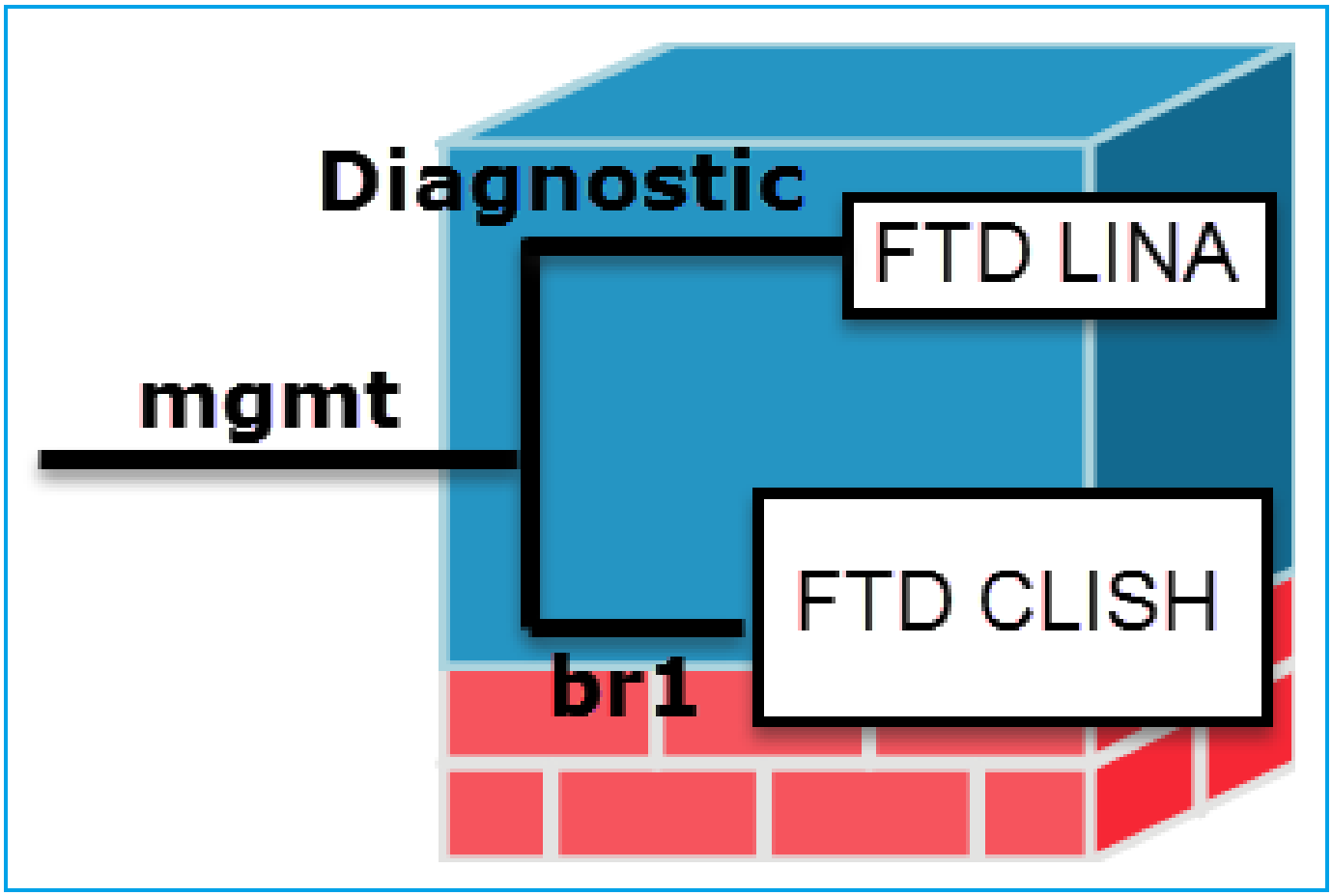
FDM での FTD の管理（オンボックス管理）

6.1 バージョン以降、ASA5500-X アプライアンスにインストールされている FTD は、FMC（オフボックス管理）または Firepower Device Manager（FDM）（オンボックス管理）のいずれかで管理できます。

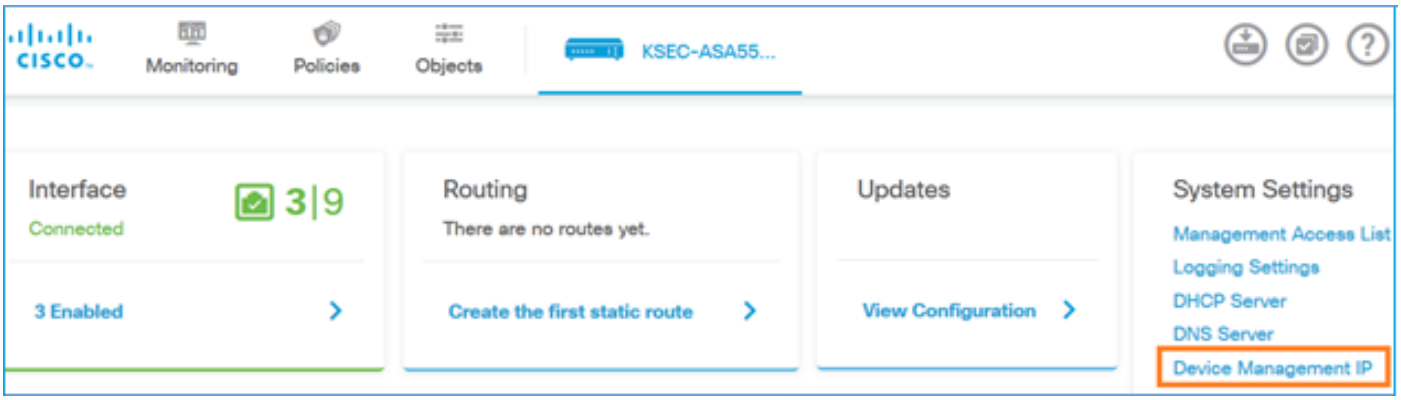
デバイスが FDM によって管理されているときの FTD CLISH からの出力は、次のようになります。

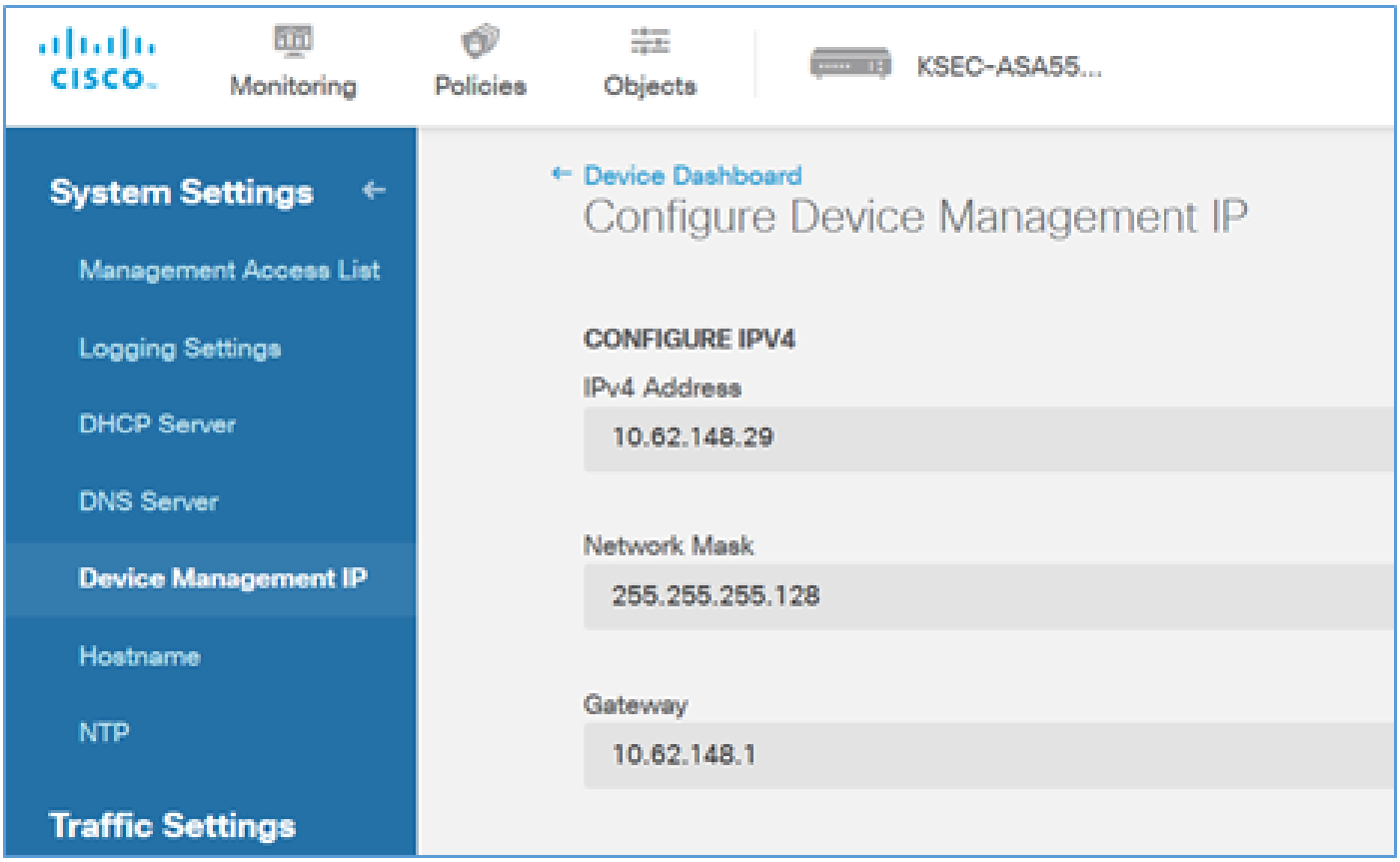
```
<#root>

>

show managers

Managed locally.
>
```

FDM では br1 論理インターフェイスが使用されます。それを図で示します。



FDM の UI で、管理インターフェイスにアクセスするには、[デバイスダッシュボード（Device Dashboard）] > [システム設定（System Settings）] > [デバイス管理IP（Device Management IP）] の順に移動します。





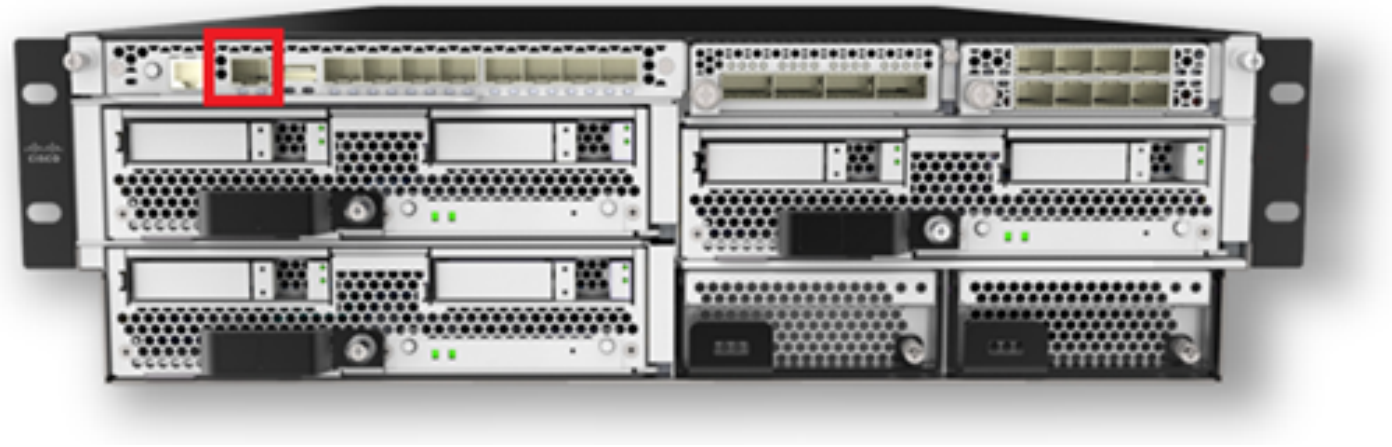
FTD Firepower ハードウェアアプライアンスの管理インターフェイス

FTD は、Firepower 2100、4100、9300 ハードウェアアプライアンスにもインストールできます。Firepower のシャーシは FXOS と呼ばれる独自の OS を実行し、FTD はモジュールやブレードにインストールされます。

FPR21xx アプライアンス

FPR41xx アプライアンス

FPR9300 アプライアンス



FPR4100/9300 では、このインターフェイスは、シャーシ管理専用であり、FP モジュール内で動作する FTD ソフトウェアでは使用または共有できません。FTD モジュール向けには、FTD を管理する個別のデータインターフェイスを割り当てます。

FPR2100 では、このインターフェイスは、シャーシ（FXOS）と FTD 論理アプライアンスの間で共有されます。

<#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

>
```

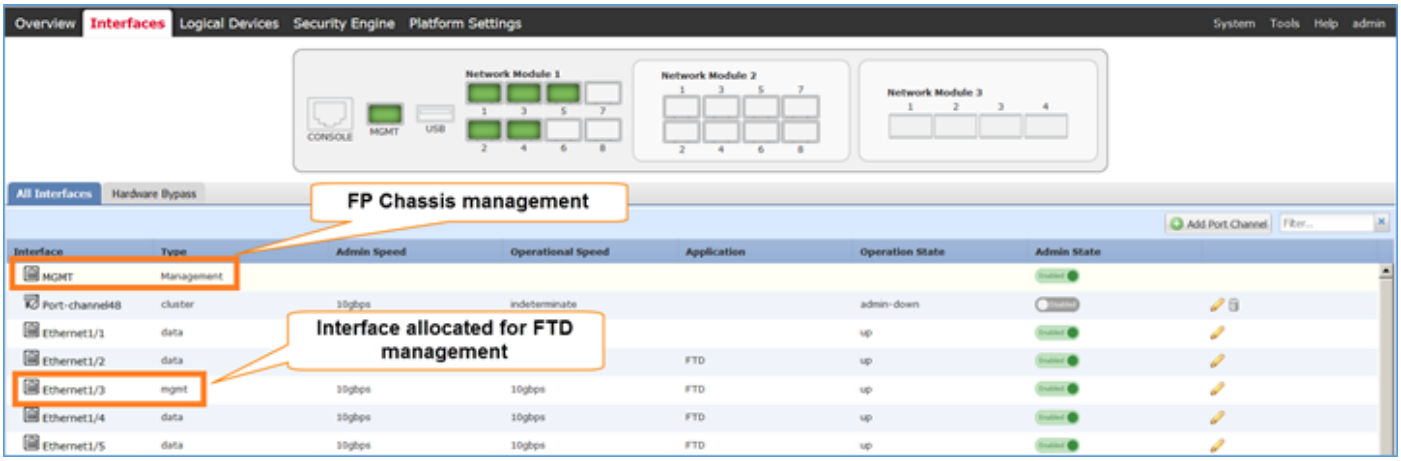
connect fxos

```
Cisco Firepower Extensible Operating System (
```

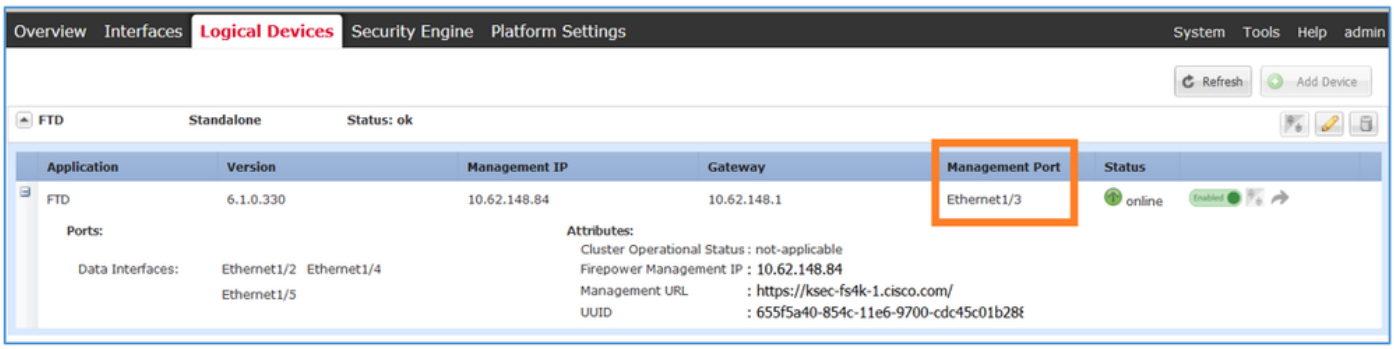
FX-OS

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

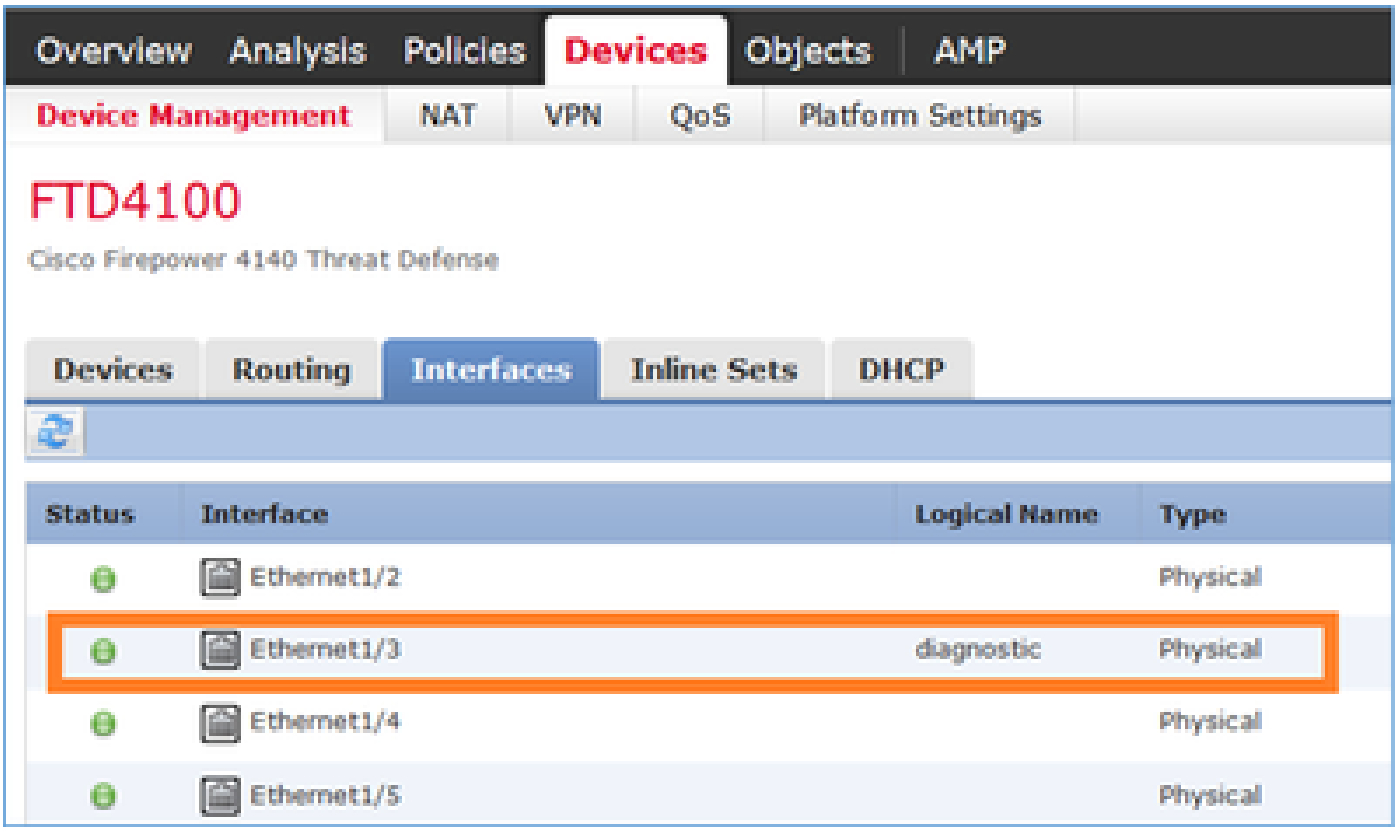
このスクリーンショットは、FTD管理用の個別のインターフェイスが割り当てられているFPR4100のFirepower Chassis Manager(FCM)UIのものです。この例では、Ethernet1/3がFTD管理インターフェイスとして選択されています：p1



これは、Logical Devicesタブでも確認できます。p2



FMCでは、インターフェイスはdiagnostic: p3と表示されます。



CLI を使用した確認

<#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
```

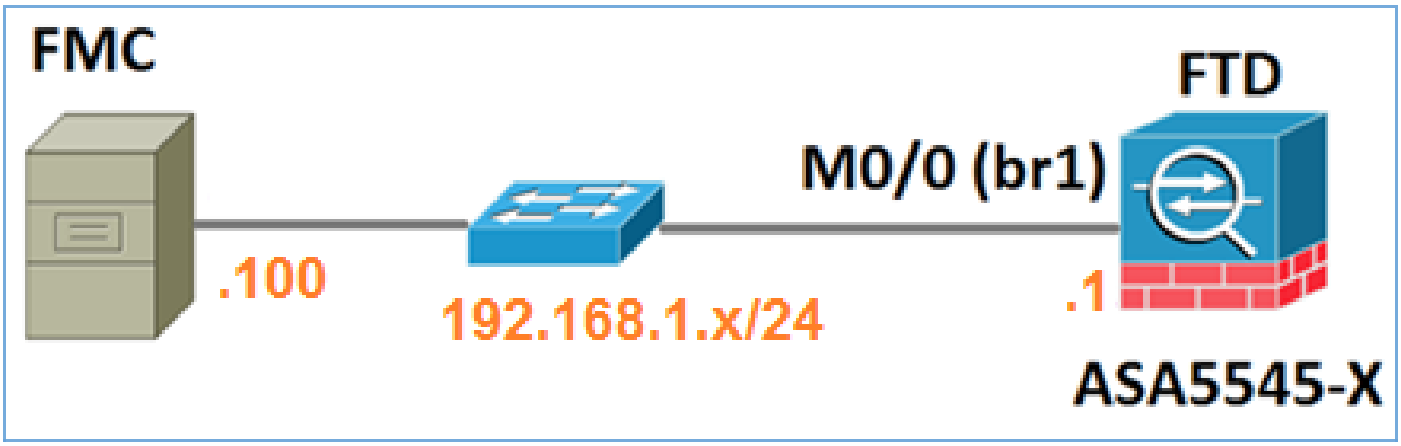
```
        5 minute input rate 2 pkts/sec,  112 bytes/sec
        5 minute output rate 0 pkts/sec,  0 bytes/sec
        5 minute drop rate, 1 pkts/sec
          Management-only interface. Blocked 0 through-the-device packets

… output omitted …
>
```

FTD と FMC の統合 - 管理シナリオ

ASA5500-Xデバイス上で実行されるFTDをFMCから管理できるようにする導入オプションの一部を次に示します。

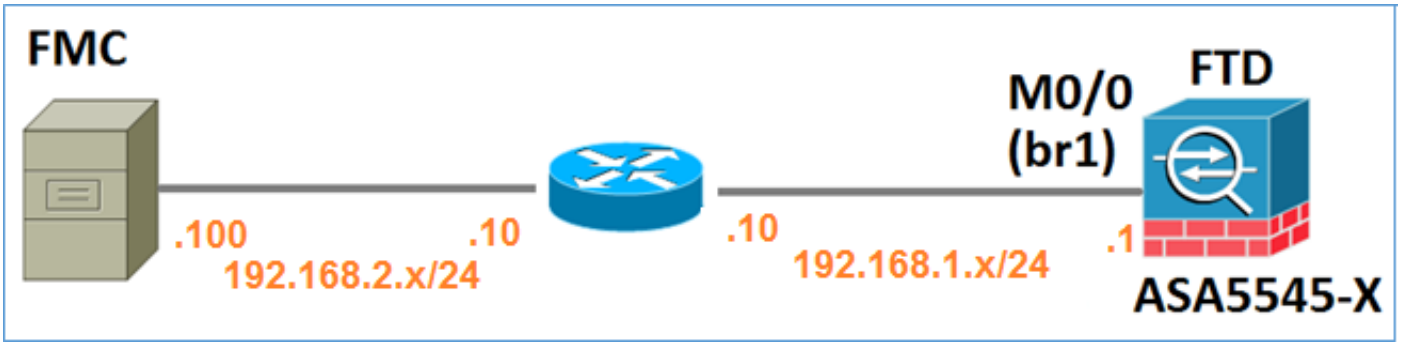
シナリオ 1.FTDとFMCが同じサブネット上にある。

これは最も簡単な方法です。図に示すように、FMCはFTD br1インターフェイスと同じサブネット上にあります。



シナリオ 2.異なるサブネット上のFTDとFMC。コントロール プレーンが FTD を通過しない。

この導入では、FTDにはFMCへのルートが必要で、その逆も同様です。次のように、FTD のネクストホップは L3 デバイス (ルータ) になります。



関連情報

- Firepower システム リリース ノート、バージョン 6.1.0

- Cisco ASA または Firepower Threat Defense デバイスのイメージの再適用
- Cisco Firepower Threat Defense バージョン 6.1 コンフィギュレーション ガイド（Firepower Device Manager 用）
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。