

Configurer l'interface de gestion FTD (Firepower Threat Defense)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Interface de gestion sur les périphériques ASA 5500-X](#)

[Architecture d'interface de gestion](#)

[Journalisation FTD](#)

[Gérer FTD avec FDM \(gestion intégrée\)](#)

[Interface de gestion sur les appareils matériels FTD Firepower](#)

[Intégrer le FTD au FMC - Scénarios de gestion](#)

[Scénario 1. FTD et FMC sur le même sous-réseau.](#)

[Scénario 2. FTD et FMC sur différents sous-réseaux. Le plan de contrôle ne passe pas par le FTD.](#)

[Informations connexes](#)

Introduction

Ce document décrit le fonctionnement et la configuration de l'interface de gestion de Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

- FTD exécuté sur l'appliance matérielle ASA5508-X
- FTD exécuté sur l'appliance matérielle ASA5512-X
- FTD qui s'exécute sur le matériel FPR9300
- FMC qui fonctionne sur 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

FTD est une image logicielle unifiée qui peut être installée sur les plates-formes suivantes :

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

L'objectif de ce document est de démontrer :

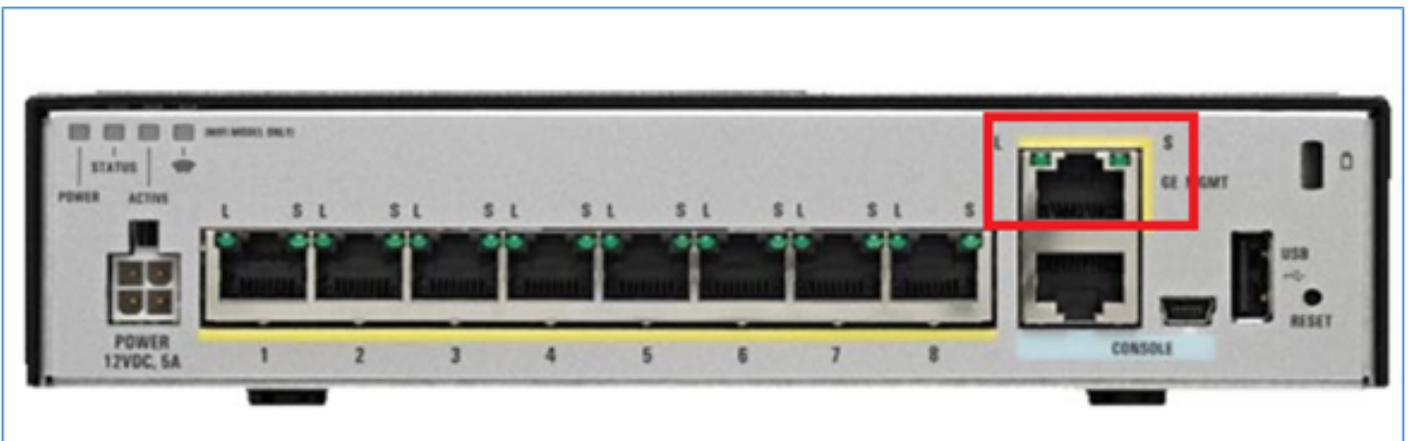
- Architecture d'interface de gestion FTD sur les périphériques ASA5500-X
- Interface de gestion FTD lorsque FDM est utilisé
- Interface de gestion FTD sur les gammes FP41xx/FP9300
- Scénarios d'intégration FTD/Firepower Management Center (FMC)

Configurer

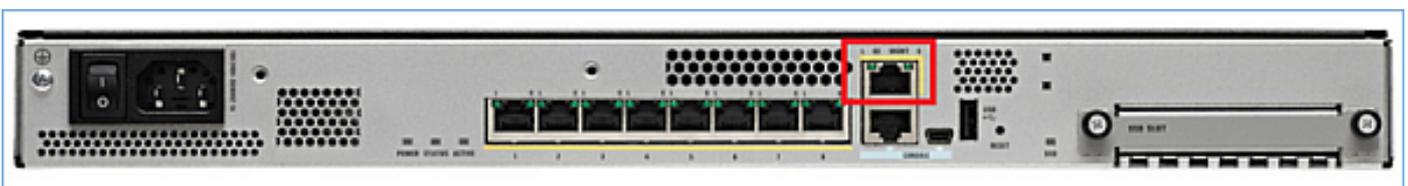
Interface de gestion sur les périphériques ASA 5500-X

Interface de gestion sur les périphériques ASA5506/08/16-X et ASA5512/15/25/45/55-X.

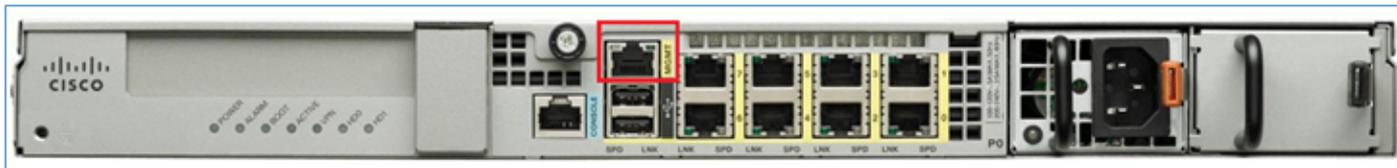
Voici l'image de l'ASA5506-X :



Voici l'image de l'ASA5508-X :



Voici l'image de l'ASA5555-X :



Lorsqu'une image FTD est installée sur 5506/08/16, l'interface de gestion est affichée sous la forme Management1/1. Sur les périphériques 5512/15/25/45/55-X, il devient Management0/0. À partir de l'interface de ligne de commande (CLI) FTD, ceci peut être vérifié dans le résultat de show tech-support.

Connectez-vous à la console FTD et exécutez la commande suivante :

```
<#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-Contro1/1 : 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

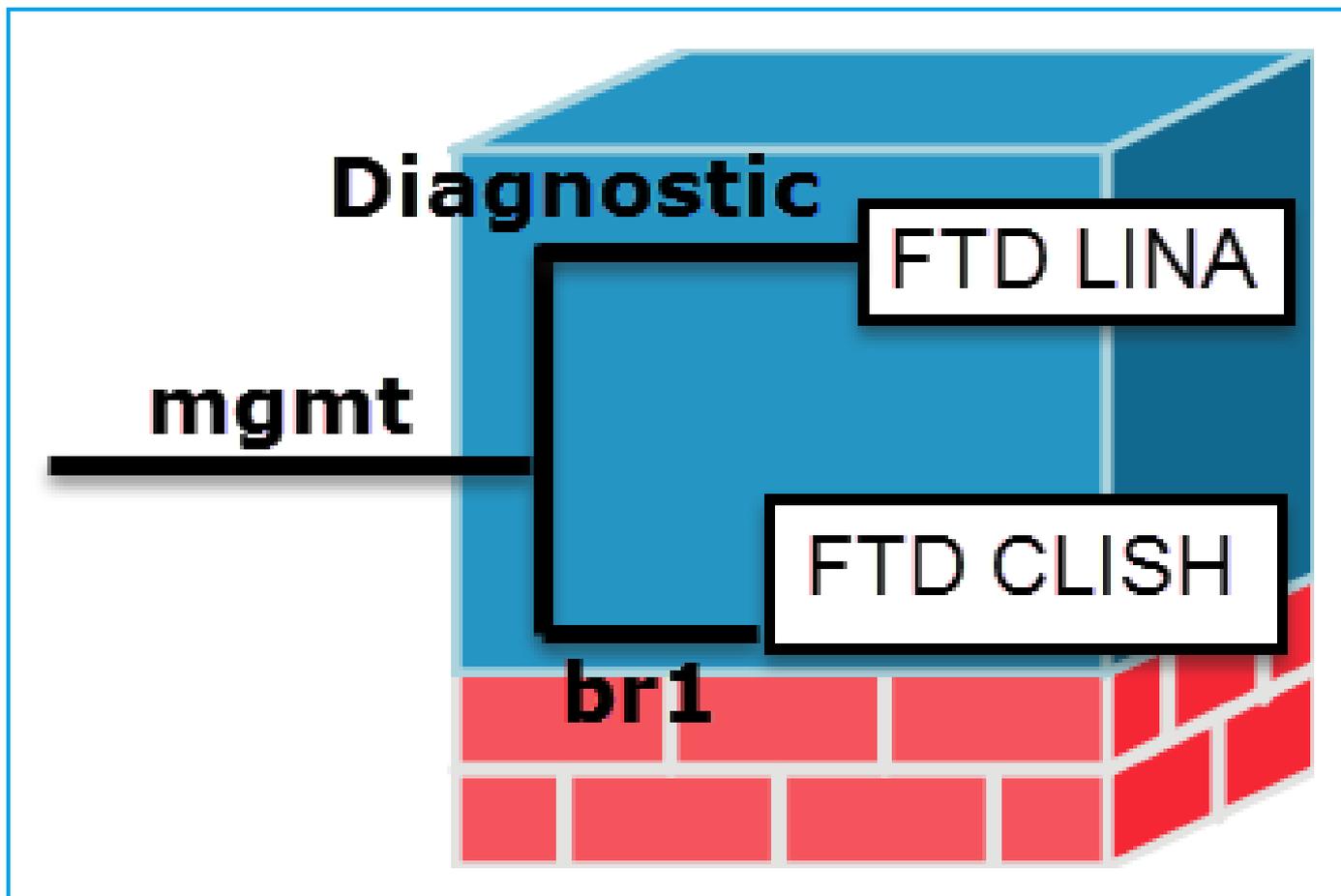
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4

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

Architecture d'interface de gestion

L'interface de gestion est divisée en 2 interfaces logiques : br1 (management0 sur les appliances FPR2100/4100/9300) et diagnostic :



	Gestion - br1/management0	Gestion - Diagnostic
Objectif	<ul style="list-style-type: none"> • Cette interface est utilisée afin d'attribuer l'IP FTD qui est utilisé pour la communication FTD/FMC. • Termine le sftunnel entre FMC/FTD. • Utilisé comme source pour les syslogs basés sur des règles. • Fournit un accès SSH et HTTPS au boîtier FTD. 	<ul style="list-style-type: none"> • Fournit un accès à distance (exemple, SNMP) au moteur. • Utilisé comme source pour les messages syslog de niveau AAA, SNMP, etc.
Obligatoire	Oui, car il est utilisé pour la communication FTD/FMC (le sftunnel se termine dessus)	Non et il n'est pas recommandé de le configurer. La recommandation est d'utiliser une interface de données à la place (consultez la remarque ci-dessous)
Configurer	Cette interface est configurée lors de l'installation de FTD (configuration). Vous pouvez ensuite modifier les paramètres br1 comme	L'interface peut être configurée depuis l'interface FMC :

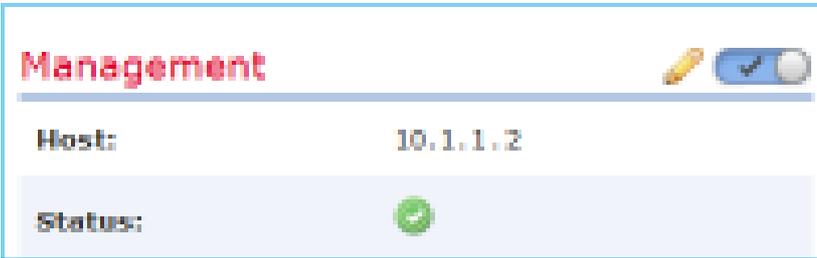
suit :

```
<#root>
>
configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 2. Mettez à jour l'IP FTD sur FMC.



Accédez à Périphériques > Gestion des périphériques,

Cliquez sur le bouton Edit et accédez à Interfaces



Restreindre l'accès

- Par défaut, seul l'utilisateur admin peut se connecter à la sous-interface FTD br1.
- Pour restreindre l'accès SSH, utilisez l'interface CLI CLISH

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

Accès à l'interface de diagnostic peut être contrôlé par FTD

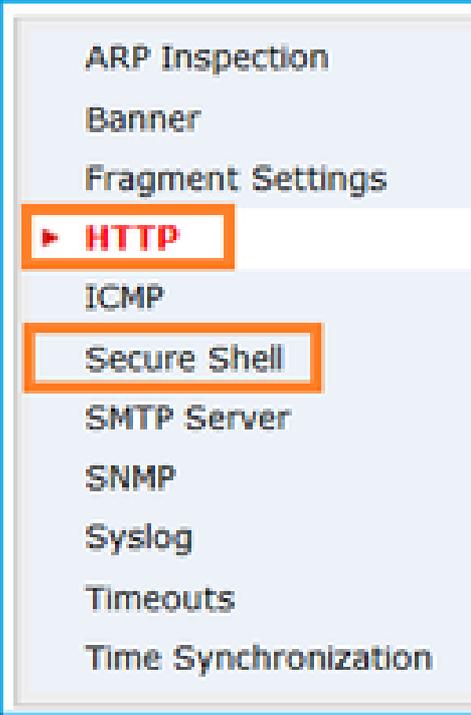
Périphériques > Paramètres de la forme >

Secure Shell

et

Périphériques > Paramètres de la forme > HTTP

respectivement

		 <p> ARP Inspection Banner Fragment Settings ▶ HTTP ICMP Secure Shell SMTP Server SNMP Syslog Timeouts Time Synchronization </p>
<p>Vérifier</p>	<p>Méthode 1 - À partir de FTD CLI :</p> <pre> <#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]----- </pre> <p>Méthode 2 - À partir de l'interface FMC</p> <p>Périphériques > Gestion des périphériques > Périphérique > Gestion</p>	<p>Méthode 1 - À partir de LINA CLI</p> <pre> <#root> firepower# show interface ip brief .. Management1/1 192.168.1.1 YES 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 </pre> <p>Méthode 2 - À partir de l'interface</p> <p>Accédez à Périphériques > Gestion des périphériques, cliquez sur le bouton Edit et accédez à Interfaces</p>

* extrait du [guide de l'utilisateur FTD 6.1](#).

Routed Mode Deployment

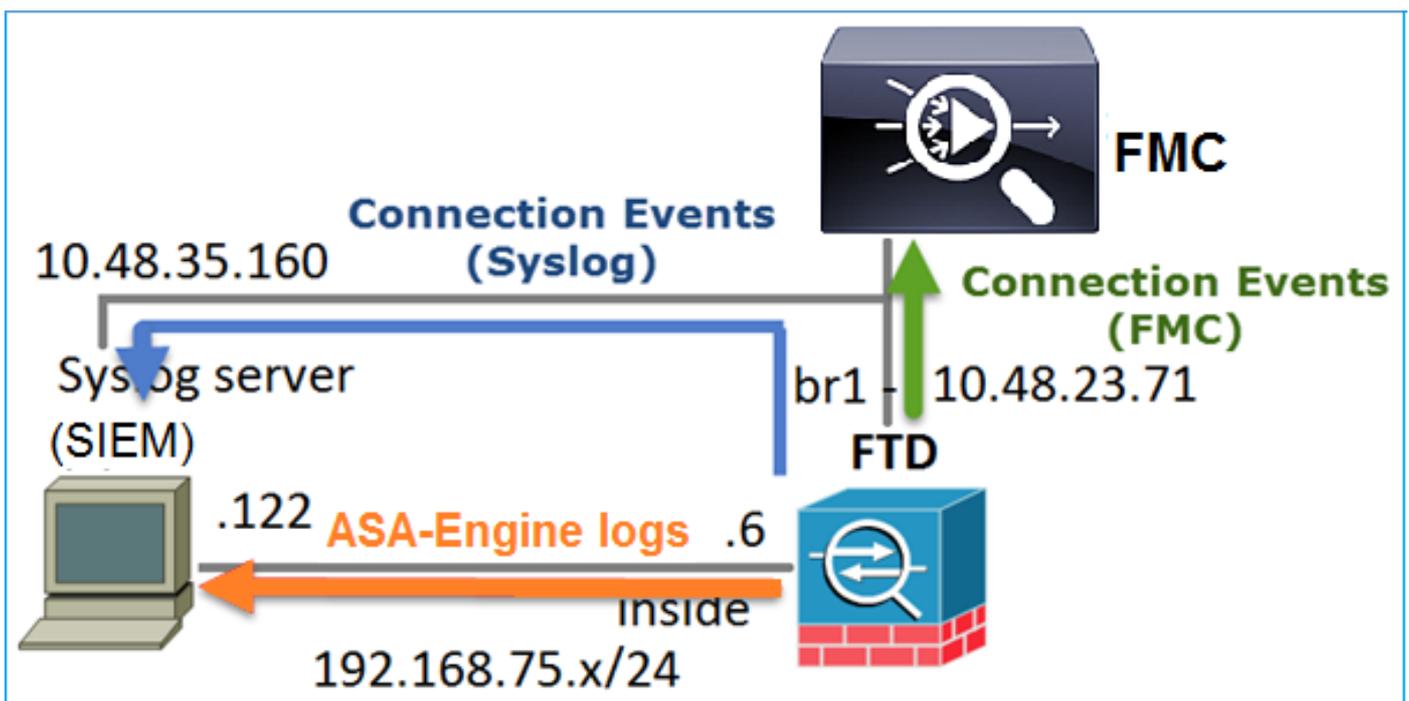
We recommend that you do not configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

Journalisation FTD

- Lorsqu'un utilisateur configure la journalisation FTD à partir des paramètres de la plateforme, le FTD génère des messages Syslog (comme sur l'ASA classique) et peut utiliser n'importe quelle interface de données comme source (y compris le diagnostic). Un exemple de message syslog qui est généré dans ce cas :

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

- D'autre part, lorsque la journalisation au niveau de la règle de la politique de contrôle d'accès (ACP) est activée, le FTD crée ces journaux via l'interface logique br1 comme source. Les journaux proviennent de la sous-interface FTD br1 :



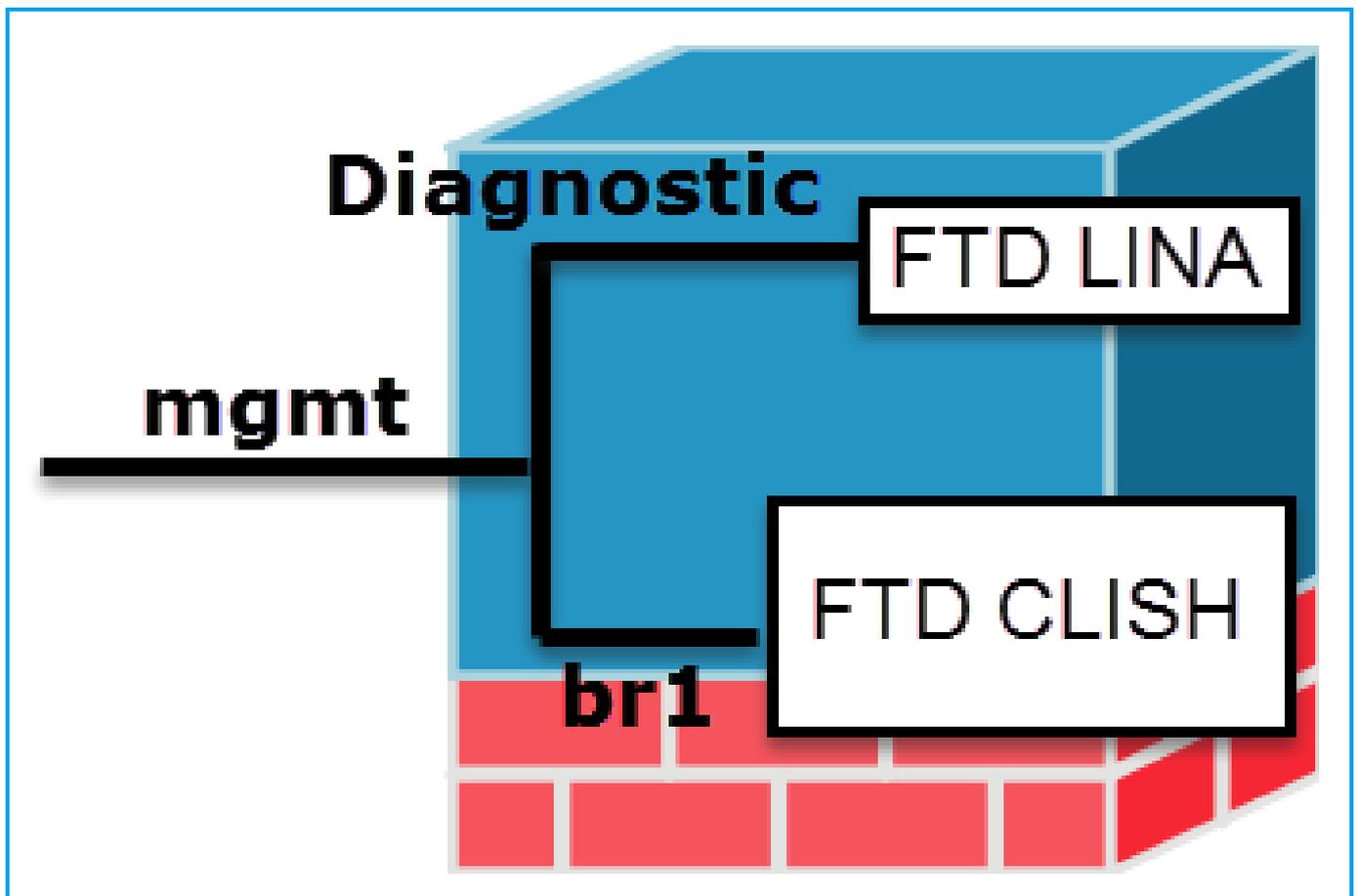
Gérer FTD avec FDM (gestion intégrée)

À partir de la version 6.1, un FTD installé sur les appliances ASA5500-X peut être géré soit par FMC (gestion off-box), soit par Firepower Device Manager (FDM) (gestion on-box).

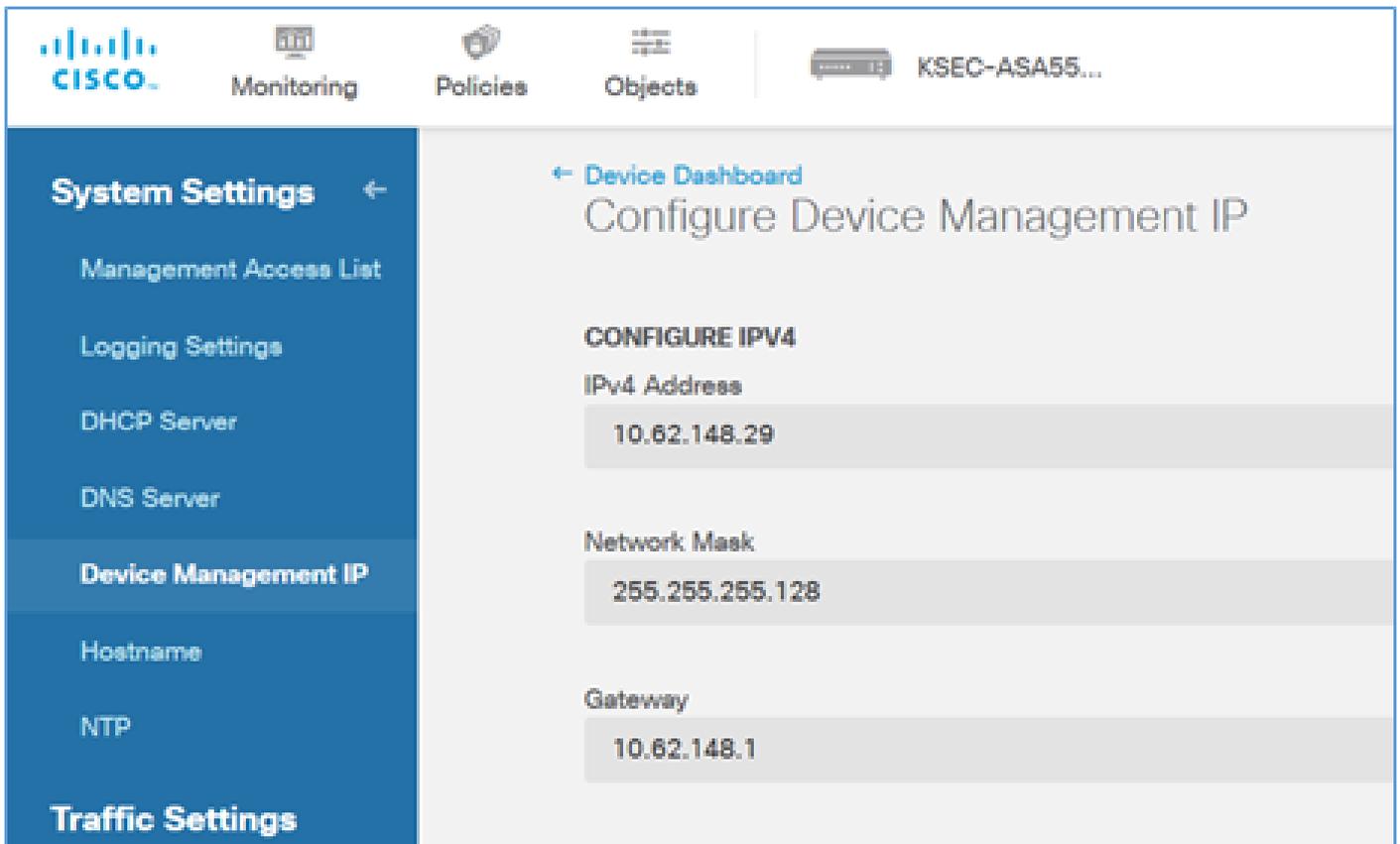
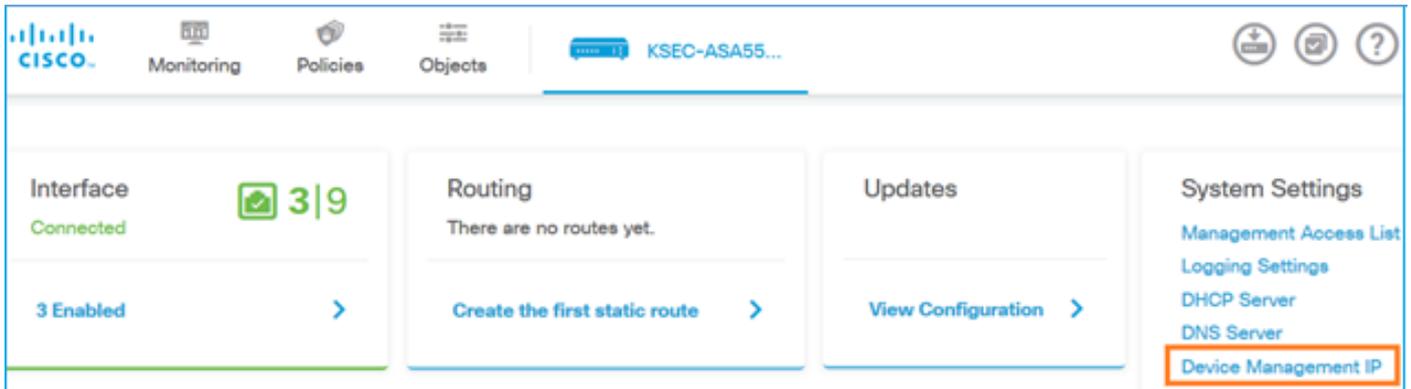
Sortie de FTD CLISH lorsque le périphérique est géré par FDM :

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

FDM utilise l'interface logique br1. Cela peut être visualisé comme suit :



Dans l'interface utilisateur de FDM, l'interface de gestion est accessible à partir de Device Dashboard > System Settings > Device Management IP :



Interface de gestion sur les appareils matériels FTD Firepower

Le FTD peut également être installé sur les appliances matérielles Firepower 2100, 4100 et 9300. Le châssis Firepower exécute son propre système d'exploitation appelé FXOS tandis que le FTD est installé sur un module/une lame.

Appliance FPR21xx



Appliance FPR41xx



Appliance FPR9300



Sur le FPR4100/9300, cette interface est uniquement destinée à la gestion du châssis et ne peut pas être utilisée/partagée avec le logiciel FTD qui s'exécute à l'intérieur du module FP. Pour le module FTD, affectez une interface de données distincte qui assure la gestion FTD.

Sur le FPR2100, cette interface est partagée entre le châssis (FXOS) et l'appliance logique FTD :

```
<#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

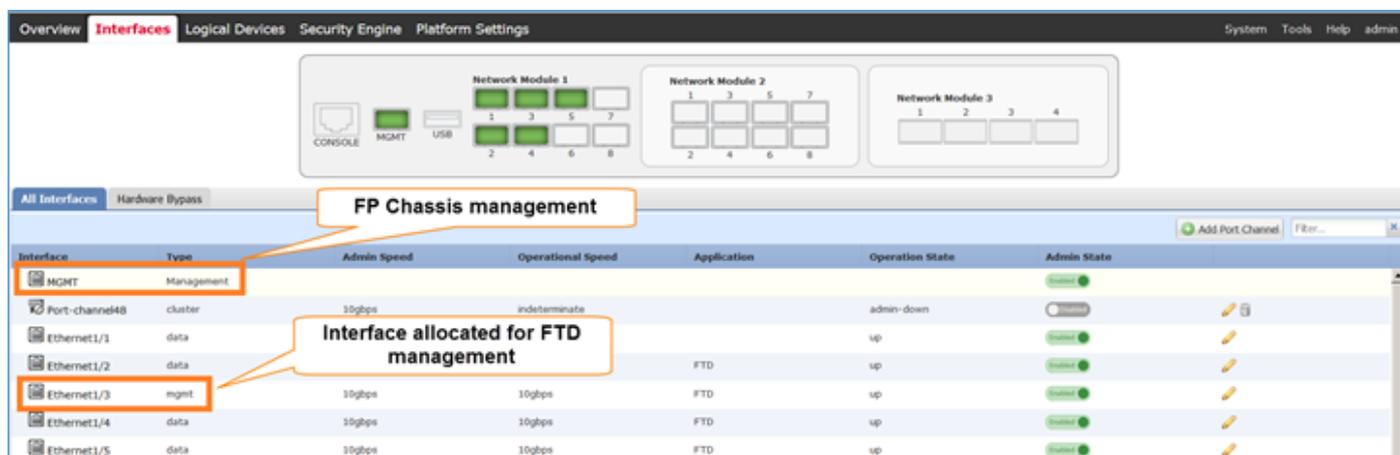
>

connect fxos

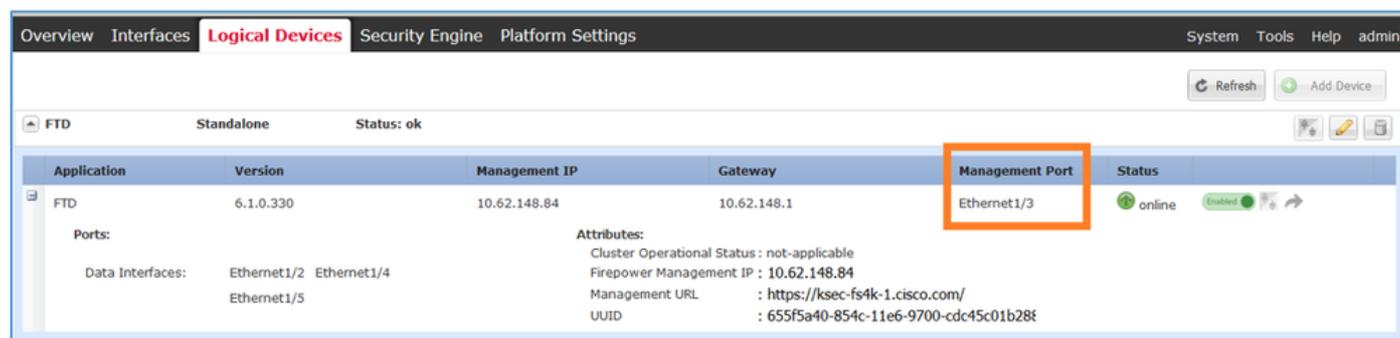
Cisco Firepower Extensible Operating System (
FX-OS
) Software
...
firepower#

```

Cette capture d'écran provient de l'interface utilisateur de Firepower Chassis Manager (FCM) sur le FPR4100, où une interface distincte pour la gestion FTD est allouée. Dans cet exemple, Ethernet1/3 est choisi comme interface de gestion FTD : p1



Vous pouvez également le voir dans l'onglet Logical Devices : p2



Sur FMC, l'interface est affichée comme 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

Vérification CLI

```
<#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
```

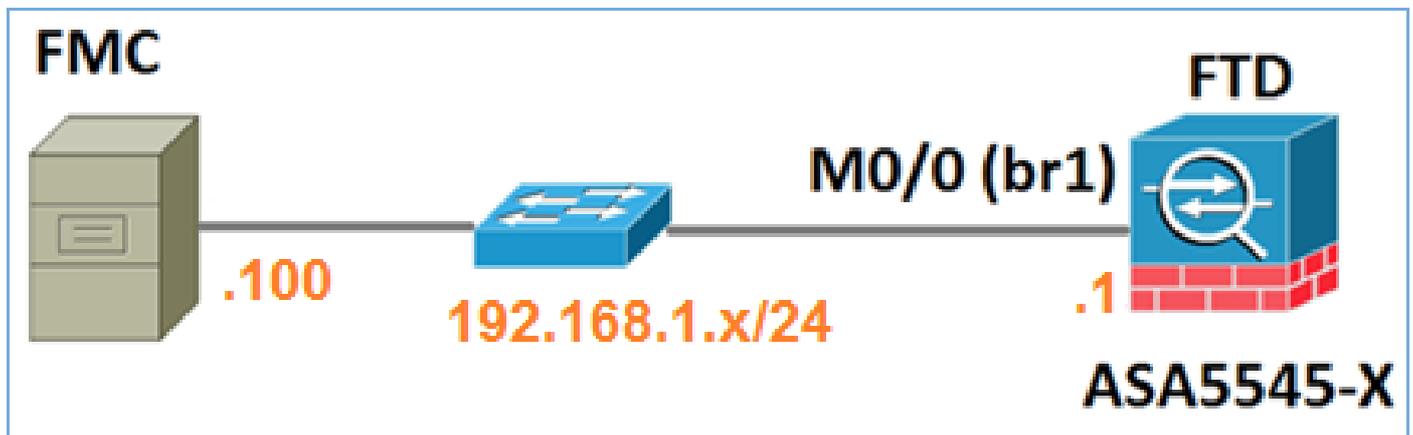
... output omitted ...
>

Intégrer le FTD au FMC - Scénarios de gestion

Voici quelques-unes des options de déploiement qui permettent de gérer le FTD qui s'exécute sur les périphériques ASA5500-X à partir de FMC.

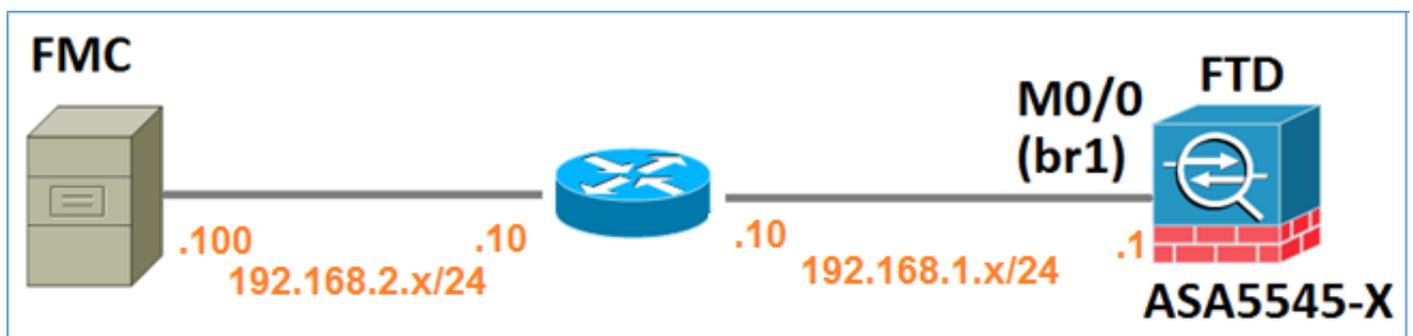
Scénario 1. FTD et FMC sur le même sous-réseau.

Il s'agit du déploiement le plus simple. Comme le montre la figure, le FMC se trouve sur le même sous-réseau que l'interface FTD br1 :



Scénario 2. FTD et FMC sur différents sous-réseaux. Le plan de contrôle ne passe pas par le FTD.

Dans ce déploiement, le FTD doit avoir une route vers le FMC et vice versa. Sur FTD, le saut suivant est un périphérique de couche 3 (routeur) :



Informations connexes

- [Notes de version du système Firepower, version 6.1.0](#)
- [Réinstallez le périphérique Cisco ASA ou Firepower Threat Defense](#)
- [Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager, version 6.1](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.