

Configurazione dell'interfaccia di gestione Firepower Threat Defense (FTD)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Interfaccia di gestione sui dispositivi ASA 5500-X](#)

[Architettura interfaccia di gestione](#)

[Registrazione FTD](#)

[Gestione FTD con FDM \(gestione integrata\)](#)

[Interfaccia di gestione su appliance hardware Firepower FTD](#)

[Integrazione FTD con FMC - Scenari di gestione](#)

[Scenario 1. FTD e FMC nella stessa subnet.](#)

[Scenario 2. FTD e FMC su subnet diverse. Il control-plane non passa attraverso l'FTD.](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il funzionamento e la configurazione dell'interfaccia di gestione su Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

- FTD eseguibile sull'appliance hardware ASA5508-X
- FTD eseguibile sull'appliance hardware ASA5512-X
- FTD eseguibile su appliance hardware FPR9300
- FMC eseguito in 6.1.0 (build 330)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

FTD è un'immagine software unificata che può essere installata sulle seguenti piattaforme:

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

Il presente documento ha lo scopo di dimostrare:

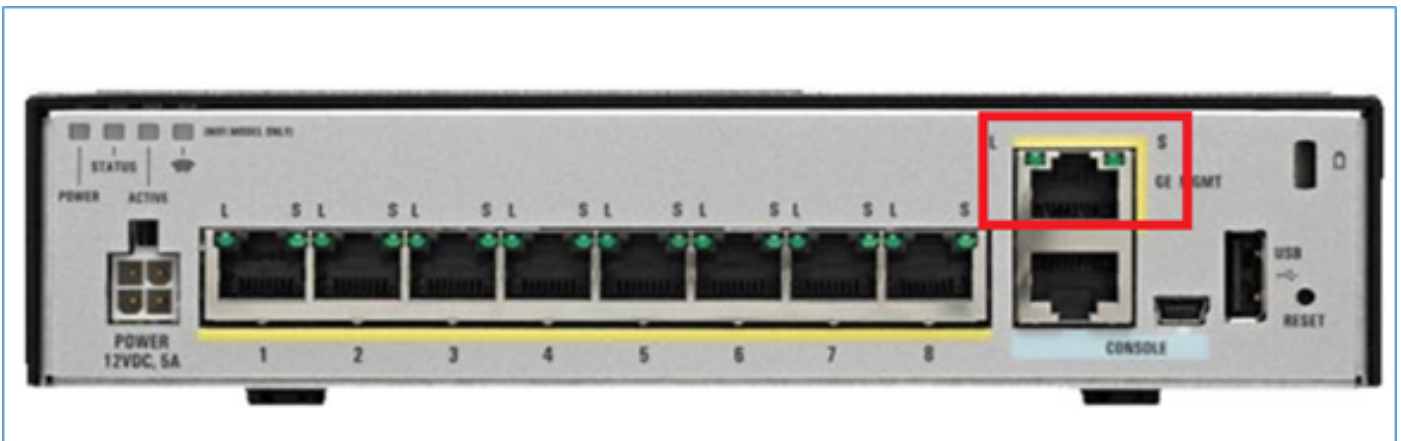
- Architettura dell'interfaccia di gestione FTD sui dispositivi ASA5500-X
- Interfaccia di gestione FTD quando viene utilizzato FDM
- Interfaccia di gestione FTD su FP41xx/FP9300
- Scenari di integrazione FTD/Firepower Management Center (FMC)

Configurazione

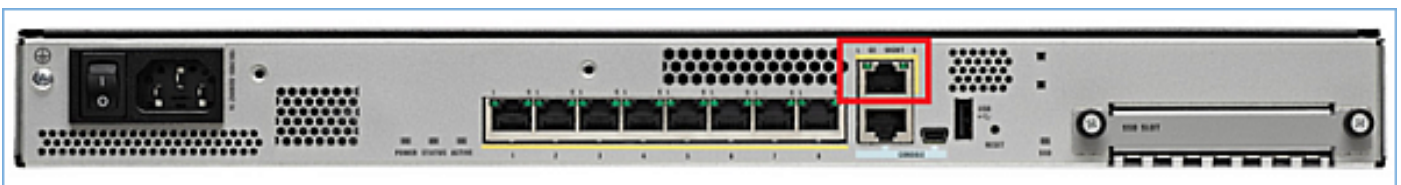
Interfaccia di gestione sui dispositivi ASA 5500-X

L'interfaccia di gestione sui dispositivi ASA5506/08/16-X e ASA5512/15/25/45/55-X.

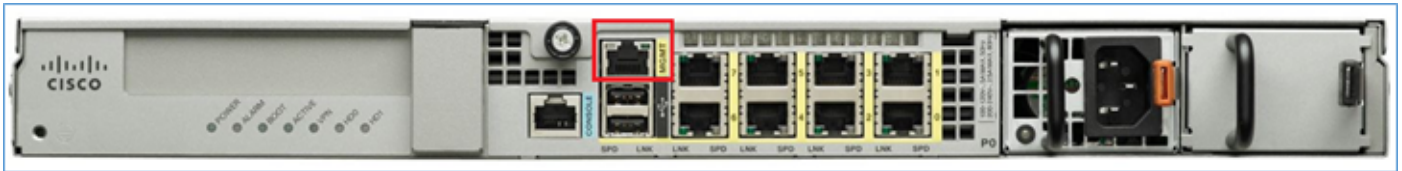
Questa è l'immagine di ASA5506-X:



Questa è l'immagine di ASA5508-X:



Questa è l'immagine di ASA5555-X:



Quando un'immagine FTD viene installata nella versione 5506/08/16, l'interfaccia di gestione viene visualizzata come Management1/1. Sui dispositivi 5512/15/25/45/55-X, diventa Management0/0. Dall'interfaccia della riga di comando FTD (CLI) è possibile verificare questa condizione nell'output show tech-support.

Connettersi alla console FTD ed eseguire il comando:

```
<#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
```

ASA 5512-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

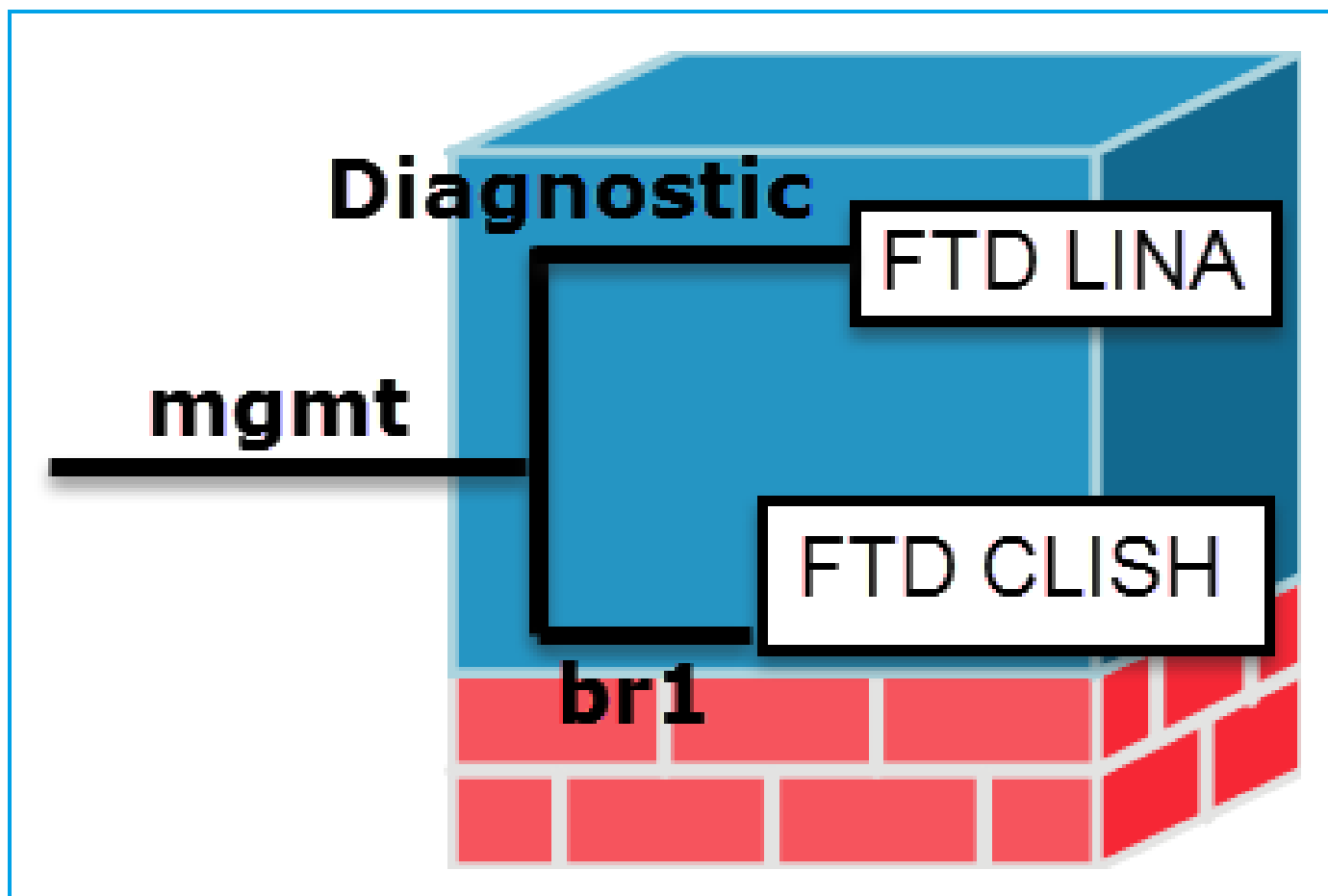
```
0: Int: Internal-Data0/0 : address is a89d.21ce.fde6, irq 11
1: Ext: GigabitEthernet0/0 : address is a89d.21ce.fdea, irq 10
2: Ext: GigabitEthernet0/1 : address is a89d.21ce.fde7, irq 10
3: Ext: GigabitEthernet0/2 : address is a89d.21ce.fdeb, irq 5
4: Ext: GigabitEthernet0/3 : address is a89d.21ce.fde8, 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
```

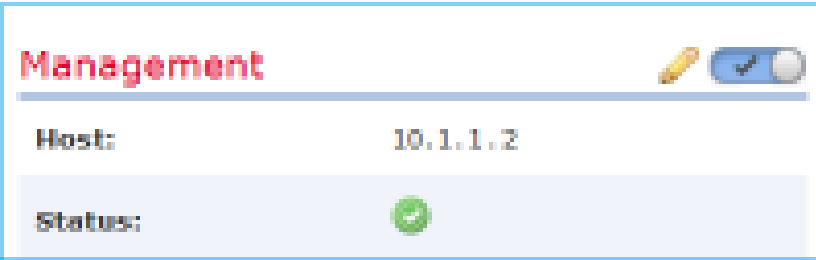
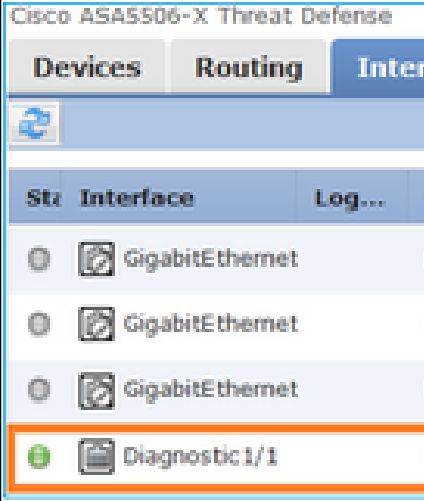
Architettura interfaccia di gestione

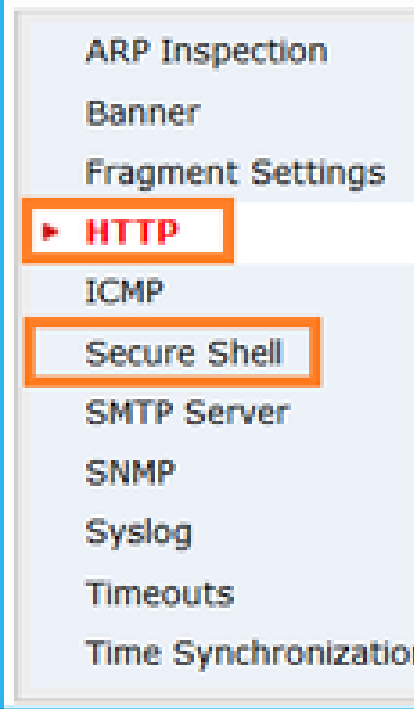
L'interfaccia di gestione è divisa in due interfacce logiche: br1 (management0 sugli accessori

FPR2100/4100/9300) e diagnostica:



	Gestione - br1/gestione0	Gestione - Diagnostica
Scopo	<ul style="list-style-type: none"> • Questa interfaccia viene usata per assegnare l'indirizzo IP FTD usato per la comunicazione FTD/FMC. • Termina il tunnel tra FMC/FTD. • Utilizzato come origine per i syslog basati su regole. • Fornisce accesso SSH e HTTPS alla casella FTD. 	<ul style="list-style-type: none"> • Fornisce accesso remoto (ad esempio, SNMP) al motore FTD. • Utilizzato come origine per i syslog basati su regole, syslog, AAA, SNMP, ecc.
Obbligatorio	Sì, poiché è utilizzato per la comunicazione FTD/FMC (sftunnel termina su di esso)	No e si sconsiglia di configurarlo. Si consiglia di utilizzare un'altra interfaccia dati* (vedere la seguente)
Configurazione	Questa interfaccia viene configurata durante l'installazione di FTD (impostazione).	L'interfaccia può essere configurata dalla GUI del CCP:

	<p>In seguito sarà possibile modificare le impostazioni di br1 come indicato di seguito:</p> <pre><#root> > configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1</pre> <p>Setting IPv4 network configuration. Network settings changed.</p> <pre>></pre> <p>Passaggio 2. Aggiornare l'indirizzo IP FTD su FMC.</p> 	<p>Selezionare Dispositivi > Gestisci dispositivi,</p> <p>Selezionare il pulsante Modifica per la Interfaccia</p> 
<p>Limita accesso</p>	<ul style="list-style-type: none"> • Per impostazione predefinita, solo l'utente admin può connettersi all'interfaccia secondaria FTD br1. • Per limitare l'accesso SSH, usare la CLI di CLISH <pre>> configure ssh-access-list 10.0.0.0/8</pre>	<p>L'accesso all'interfaccia diagnostica può essere controllato da FTD</p> <p>Dispositivi > Impostazioni piattaforma > Secure Shell</p> <p>e</p> <p>Dispositivi > Impostazioni piattaforma > HTTP</p> <p>rispettivamente</p>

		
<p>Verifica</p>	<p>Metodo 1 - Da CLI FTD:</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>Metodo 2 - Dall'interfaccia GUI del CCP</p> <p>Dispositivi > Gestione dispositivi > Dispositivo > Gestione</p>	<p>Metodo 1 - Da CLI LINA:</p> <pre> <#root> firepower# show interface ip brief .. Management1/1 192.168.1.1 Y firepower# show run interface m1/1 ! interface Management1/1 management-only nameif diagnostic security-level 0 ip address 192.168.1.1 255 </pre> <p>Metodo 2 - Dall'interfaccia GUI</p> <p>Selezionare Dispositivi > Gestione dispositivi,</p> <p>selezionare il pulsante Modifica Interfacce</p>

* estratto tratto dalla [guida utente di FTD 6.1](#).

Routed Mode Deployment

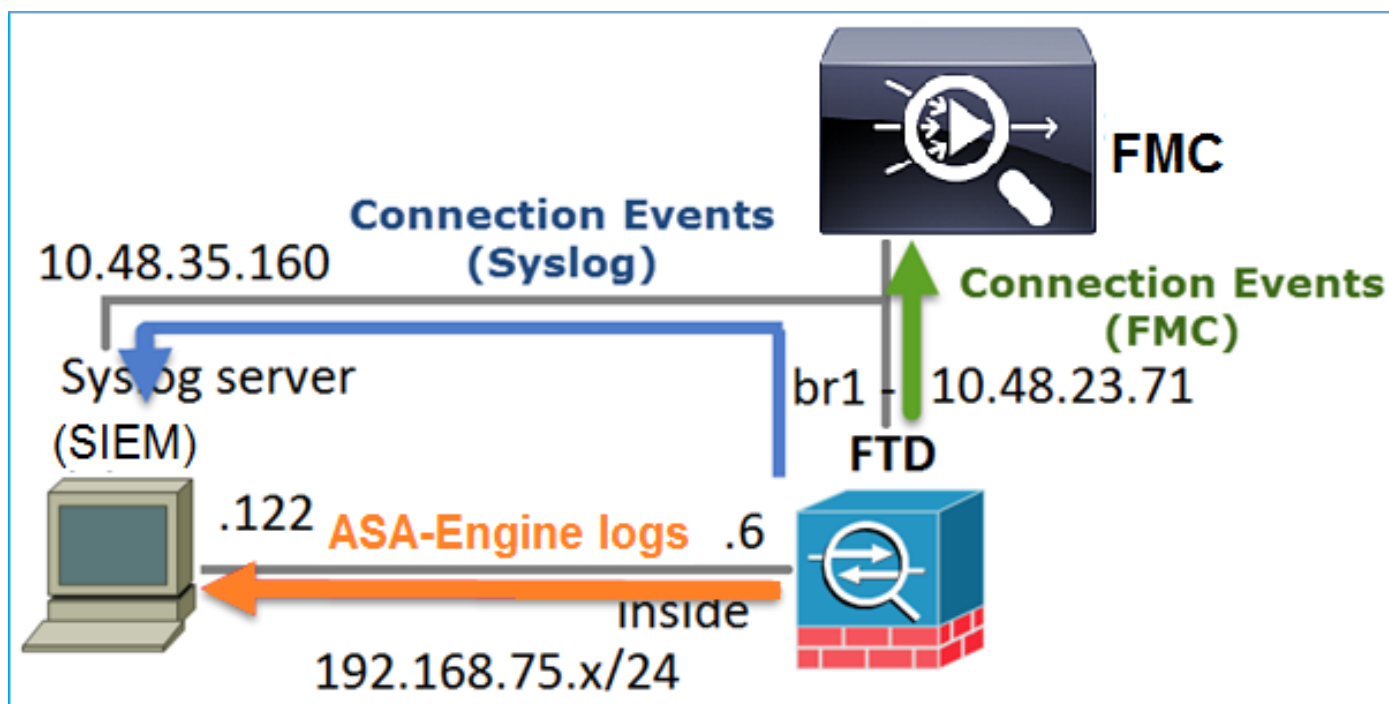
We recommend that you do not configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

Registrazione FTD

- Quando un utente configura la registrazione FTD dalle impostazioni della piattaforma, l'FTD genera messaggi Syslog (come sull'ASA classico) e può utilizzare qualsiasi interfaccia dati come origine (compresa la diagnostica). Esempio di messaggio syslog generato in questo caso:

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

- D'altra parte, quando la registrazione a livello di regola dei criteri di controllo dell'accesso (ACP) è abilitata, l'FTD crea questi registri tramite l'interfaccia logica br1 come origine. I log hanno origine dalla sottointerfaccia FTD br1:



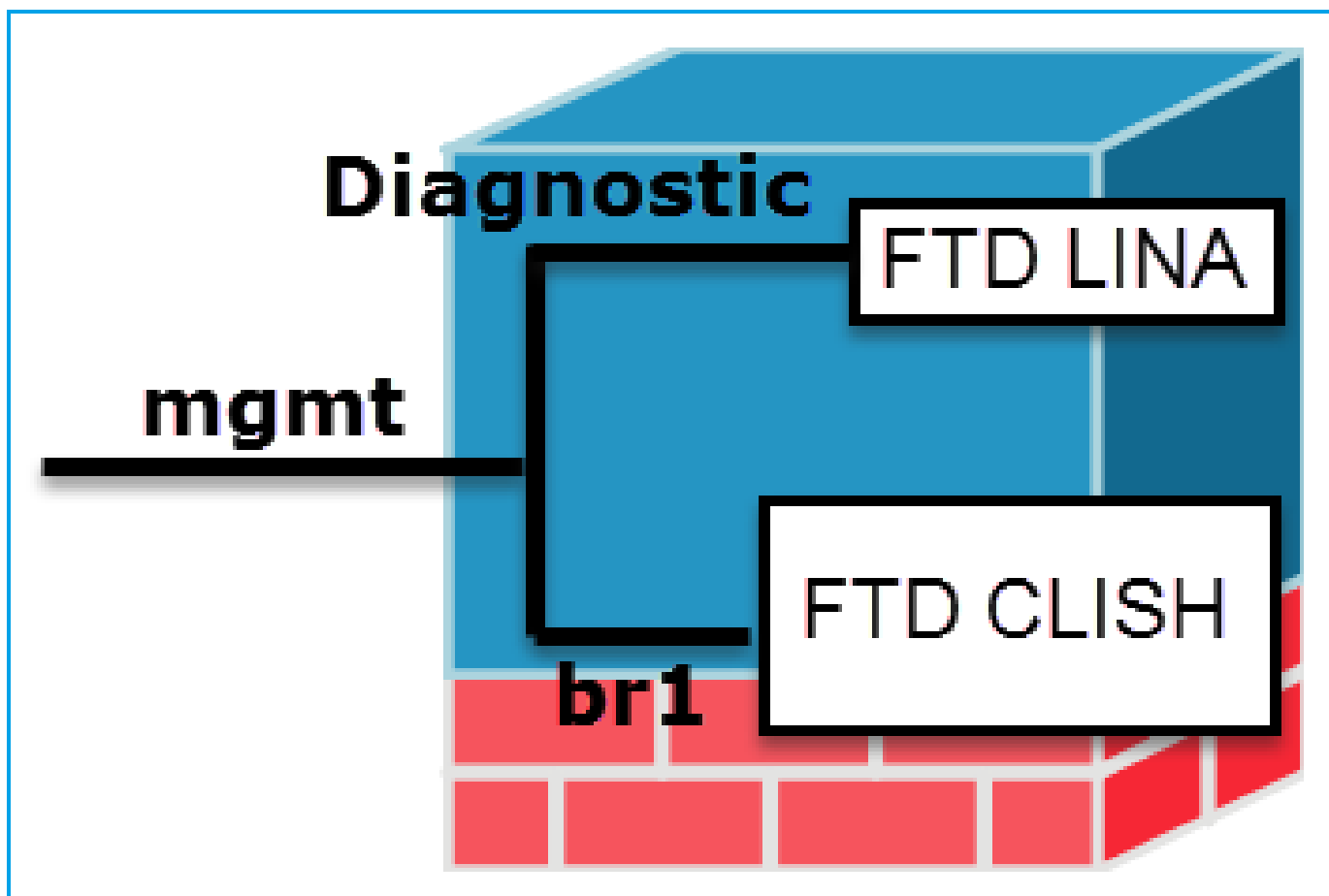
Gestione FTD con FDM (gestione integrata)

A partire dalla versione 6.1, un FTD installato sugli accessori ASA5500-X può essere gestito da FMC (gestione off-box) o da Firepower Device Manager (FDM) (gestione on-box).

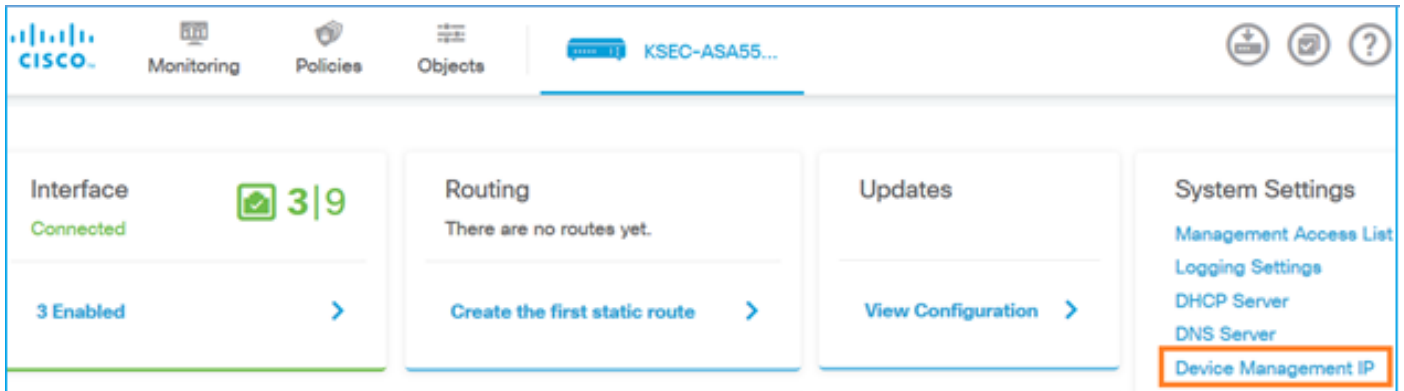
Output da FTD CLISH quando il dispositivo è gestito da FDM:

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

FDM utilizza l'interfaccia logica br1. Ciò può essere visualizzato come:



Dall'interfaccia utente di FDM, l'interfaccia di gestione è accessibile dal Dashboard dispositivi > Impostazioni di sistema > IP di gestione dispositivi:



Interfaccia di gestione su appliance hardware Firepower FTD

FTD può essere installato anche su appliance hardware Firepower 2100, 4100 e 9300. Lo chassis Firepower esegue il proprio sistema operativo denominato FXOS mentre FTD è installato su un modulo/blade.

accessorio FPR21xx



Appliance FPR41xx



accessorio FPR9300



Sulle schede FPR4100/9300 questa interfaccia è solo per la gestione dello chassis e non può essere utilizzata/condivisa con il software FTD in esecuzione all'interno del modulo FP. Per il modulo FTD allocare un'interfaccia dati separata che per la gestione FTD.

Sul router FPR2100, questa interfaccia è condivisa tra lo chassis (FXOS) e l'appliance logica 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 (

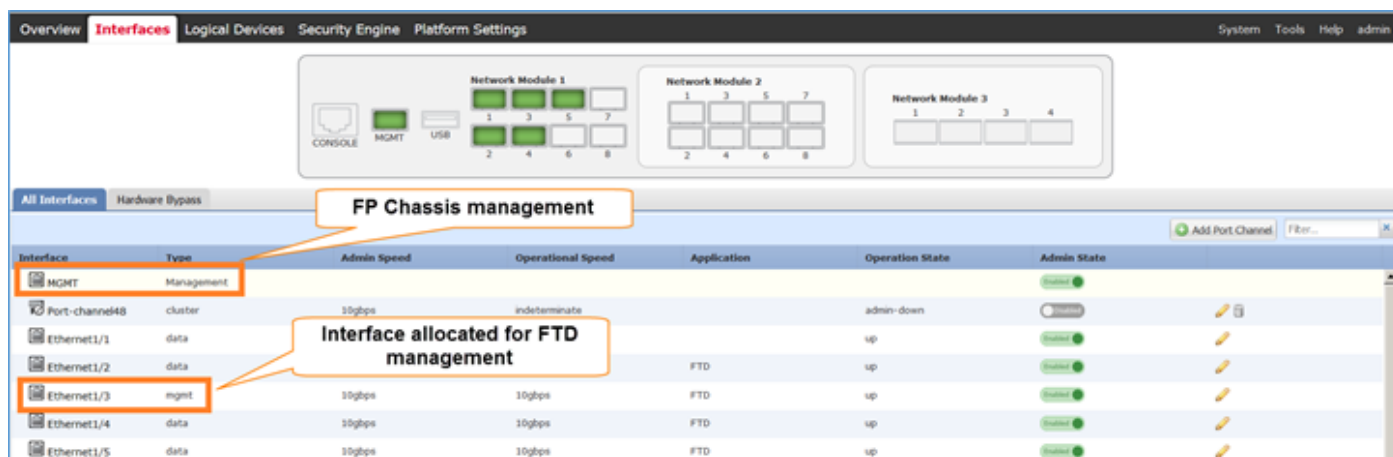
FX-OS

) Software

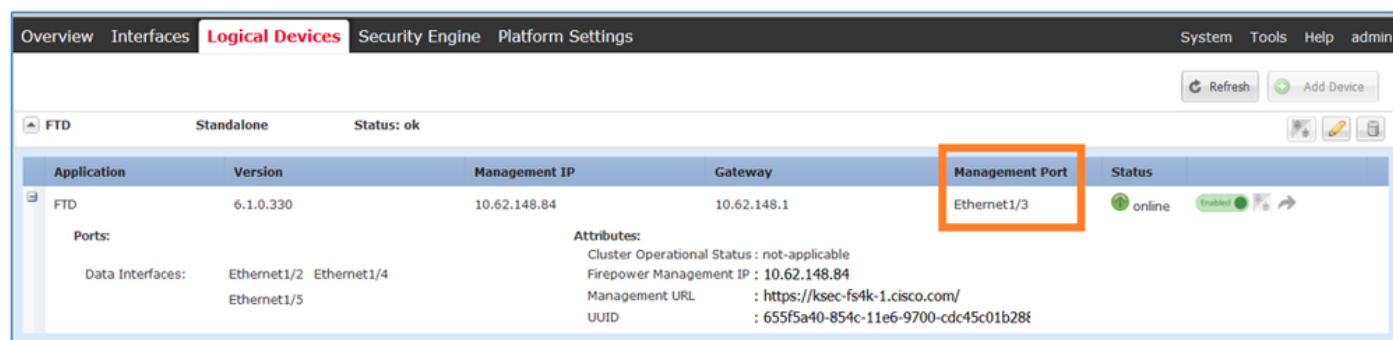
...

firepower#

Questa schermata è tratta dall'interfaccia utente di Firepower Chassis Manager (FCM) su FPR4100, dove è allocata un'interfaccia separata per la gestione FTD. Nell'esempio, viene scelta Ethernet1/3 come interfaccia di gestione FTD: p1



Questa condizione può essere rilevata anche nella scheda Periferiche logiche:p2



Su FMC l'interfaccia è visualizzata come diagnostica: 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

Verifica 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
```

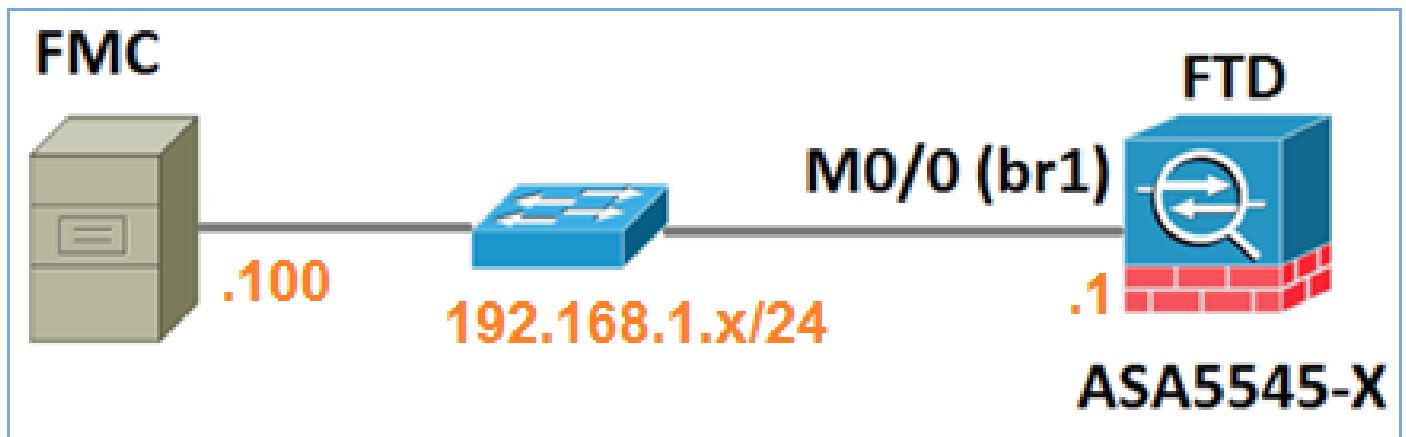
... output omitted ...
>

Integrazione FTD con FMC - Scenari di gestione

Queste sono alcune delle opzioni di implementazione che consentono di gestire FTD in esecuzione sui dispositivi ASA5500-X da FMC.

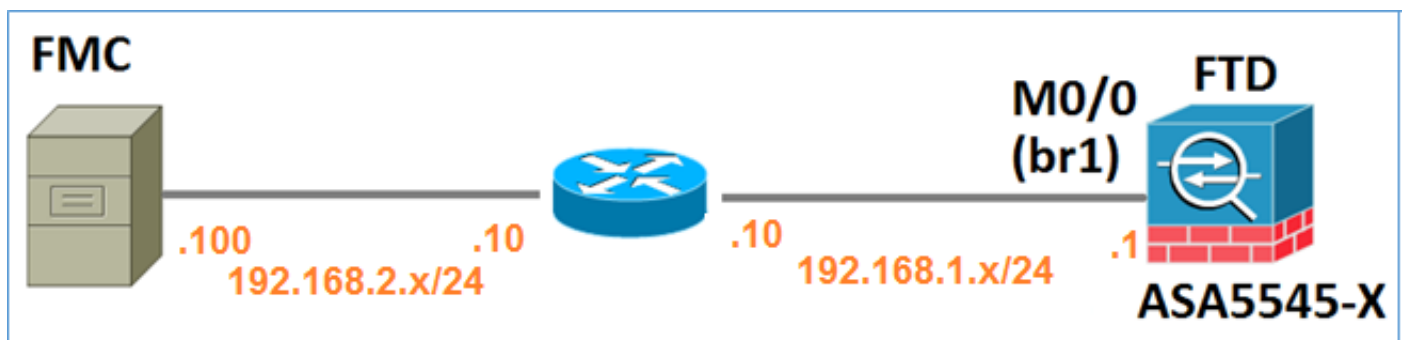
Scenario 1. FTD e FMC nella stessa subnet.

Questa è la distribuzione più semplice. Come illustrato nella figura, il CCP si trova sulla stessa subnet dell'interfaccia FTD br1:



Scenario 2. FTD e FMC su subnet diverse. Il control-plane non passa attraverso l'FTD.

In questa operazione, l'FTD deve avere un percorso verso il CCP e viceversa. Sull'FTD, l'hop successivo è un dispositivo L3 (router):



Informazioni correlate

- [Note sulla versione di Firepower System, versione 6.1.0](#)

- [Ricreare un'immagine di Cisco ASA o del dispositivo Firepower Threat Defense](#)
- [Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager, versione 6.1](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).