Configurar a interface de gerenciamento do Firepower Threat Defense (FTD)

Contents

Introduction

Este documento descreve a operação e configuração da interface de gerenciamento do Firepower Threat Defense (FTD).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

- FTD executado no dispositivo de hardware ASA5508-X
- FTD executado no dispositivo de hardware ASA5512-X
- FTD executado no dispositivo de hardware FPR9300
- FMC executado em 6.1.0 (compilação 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FTD é uma imagem de software unificada que pode ser instalada nestas plataformas:

- 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
- Módulo de roteador ISR

O objetivo deste documento é demonstrar:

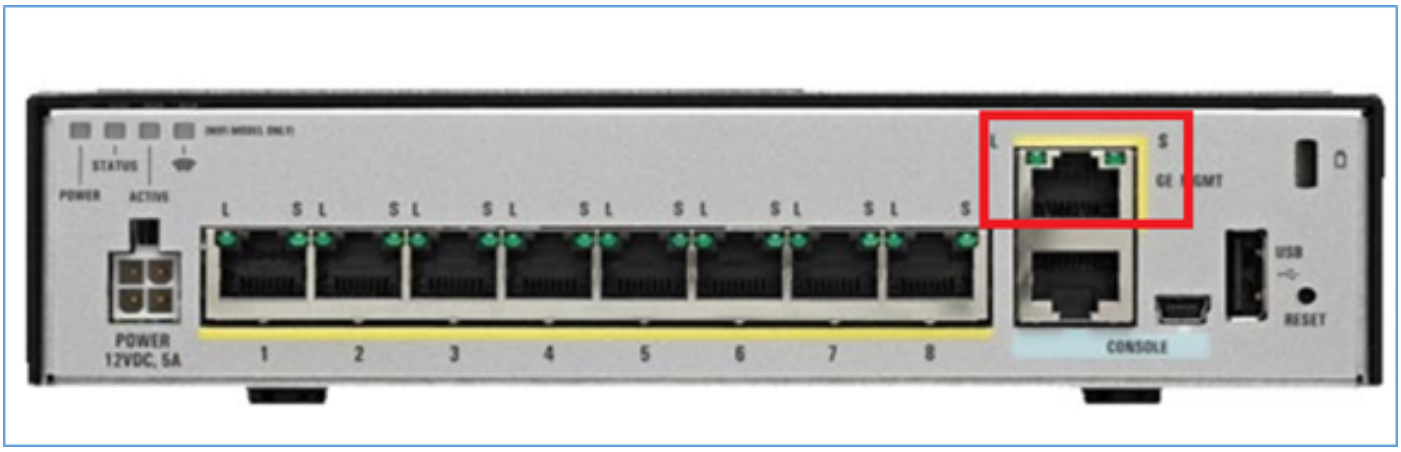
- Arquitetura de interface de gerenciamento do FTD nos dispositivos ASA5500-X
- Interface de gerenciamento do FTD quando o FDM é usado
- Interface de gerenciamento do FTD no FP41xx/FP9300 Series
- Cenários de integração do FTD/Firepower Management Center (FMC)

Configurar

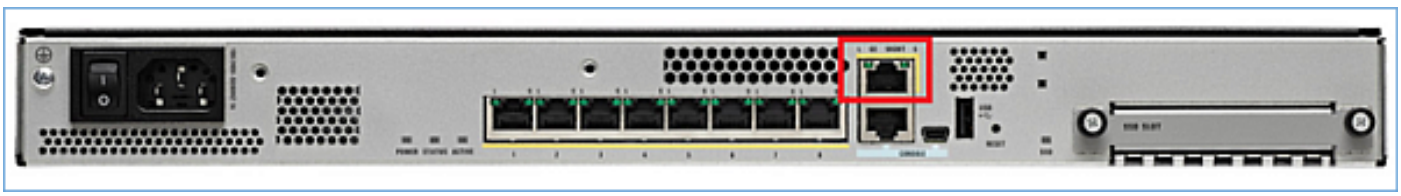
Interface de gerenciamento nos dispositivos ASA 5500-X

A interface de gerenciamento nos dispositivos ASA5506/08/16-X e ASA5512/15/25/45/55-X.

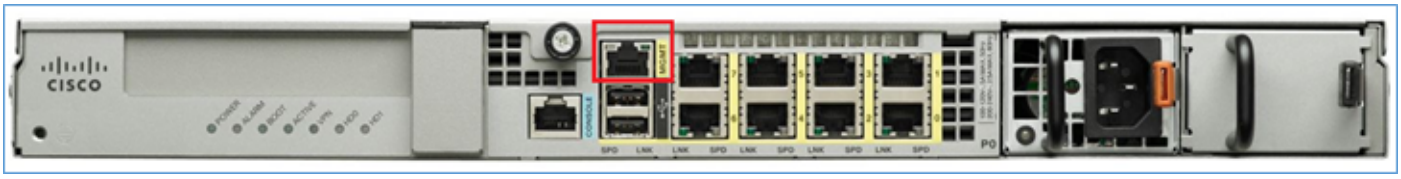
Esta é a imagem do ASA5506-X:



Esta é a imagem do ASA5508-X:



Esta é a imagem do ASA5555-X:



Quando uma imagem FTD é instalada em 5506/08/16, a interface de gerenciamento é mostrada como **Management1/1**. Em dispositivos 5512/15/25/45/55-X, isso se torna **Management0/0.** Na Interface de Linha de Comando (CLI) do FTD, isso pode ser verificado na saída **show tech-support**.

Conecte-se ao console FTD e execute o comando:

```
> 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
```

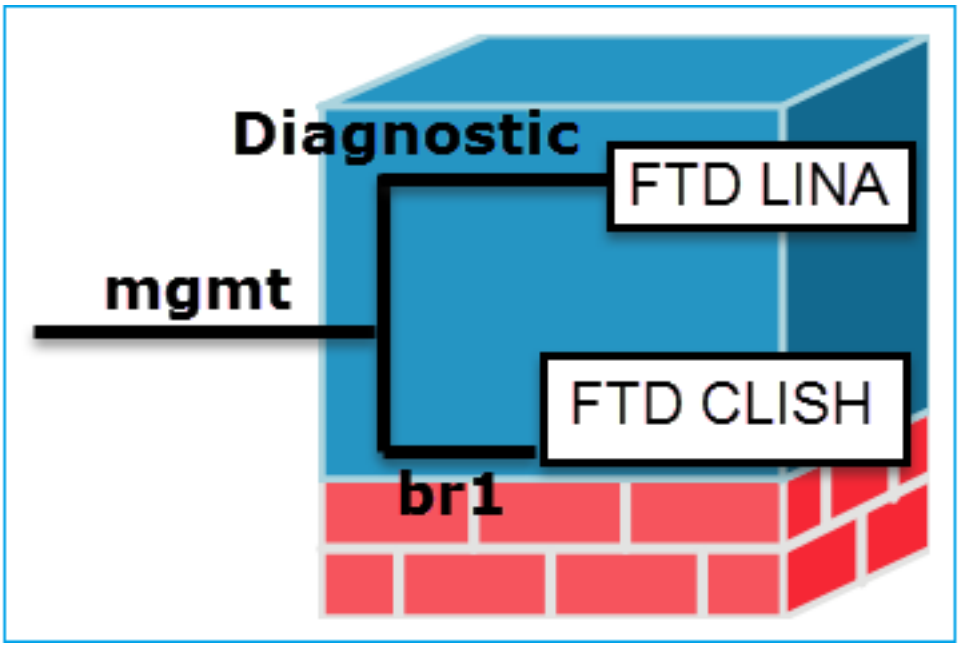
ASA5512-X:

```
> 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
```

Arquitetura da interface de gerenciamento

A interface de gerenciamento é dividida em 2 interfaces lógicas: **br1 (management0 nos dispositivos FPR2100/4100/9300) e diagnóstico:**



	Gerenciamento – **br1/management0**	Gerenciamento – **Diagnóstico**
Propósito	• Esta interface é usada para atribuir o IP FTD usado para comunicação FTD/FMC. • Encerra o sftunnel entre FMC/FTD. • Usado como origem para syslogs baseados em regras. • Fornece acesso SSH e HTTPS à caixa FTD.	• Fornece acesso remoto (por exemplo, SNMP) ao mecanismo ASA. • Usado como fonte para mensagens syslogs de nível LINA, AAA, SNMP, etc.
Obrigatório	**Sim**, pois é usado para comunicação FTD/FMC	**Não** e não é recomendável

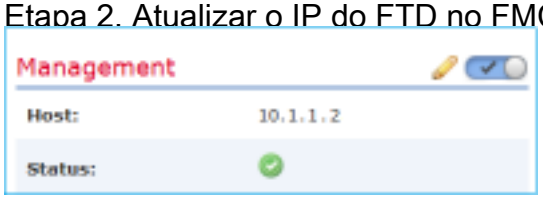
(o sftunnel termina nele)

Essa interface é configurada durante a instalação do FTD (configuração). Posteriormente, você poderá modificar as configurações de br1 da seguinte maneira:

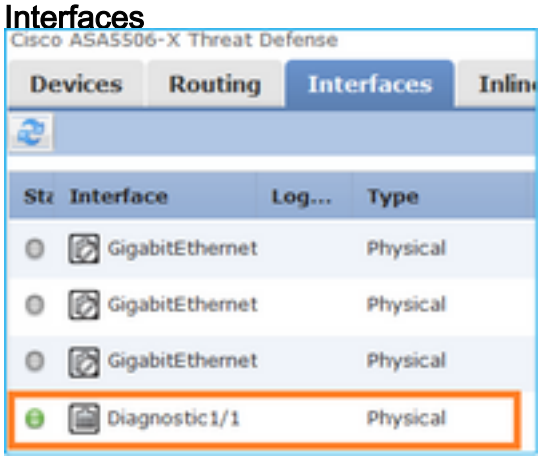
Configurar

```
 >configure network ipv4 manual 10.1.1.2
255.0.0.0 10.1.1.1
Setting IPv4 network configuration.
Network settings changed.

>
```

Etapa 2. Atualizar o IP do FTD no FMC.



configurá-lo. A recomendação é usar uma interface de dados em vez disso* (verifique a nota abaixo)
A interface pode ser configurada na GUI do FMC:
Navegue até **Dispositivos > Gerenciamento de dispositivos,** Selecione o botão **Editar** e navegue até **Interfaces**

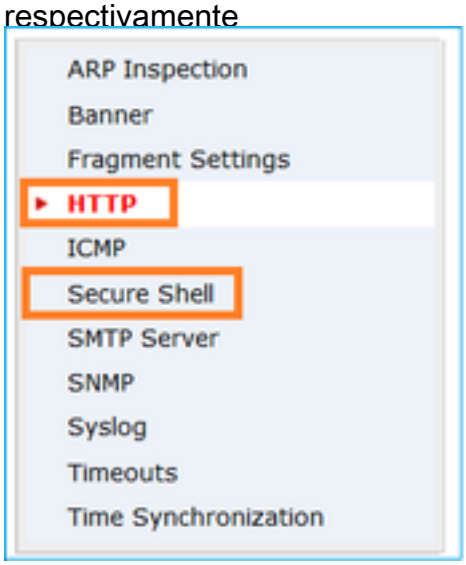


O acesso à interface de diagnóstico pode ser controlado pelo FTD **Dispositivos > Configurações da plataforma > Secure Shell** e **Dispositivos > Configurações da plataforma > HTTP** respectivamente

Restringir acesso

- Por padrão, somente o usuário **admin** pode se conectar à subinterface br1 do FTD.
- Para restringir o acesso SSH, use CLISH CLI

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



Verificar

Método 1 – Na CLI do FTD:

```
  > show network
...
=======[ br1 ]=======
State : Enabled
Channels : Management & Events
Mode :
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 18:8B:9D:1E:CA:7B
---------------------[ IPv4 ]-----
```

Método 1 – Na CLI do LINA:

```
  firepower# show interface ip brief
..
Management1/1 192.168.1.1 YES unset up up

firepower# show run interface m1/1
!
interface Management1/1
management-only
nameif diagnostic
security-level 0
```

```
Configuration : Manual
Address : 10.1.1.2
Netmask : 255.0.0.0
Broadcast : 10.1.1.255
----------------------[ IPv6 ]-----
```

Método 2 – Na GUI do FMC
Dispositivos > Gerenciamento de dispositivos > Dispositivo > Gerenciamento

```
ip address 192.168.1.1 255.255.255.0
```

Método 2 – Na GUI do FMC
Navegue até **Dispositivos > Gerenciamento de dispositivos,** Selecione o botão **Editar** e navegue até **Interfaces**

* trecho extraído do guia do usuário do FTD 6.1.

Routed Mode Deployment

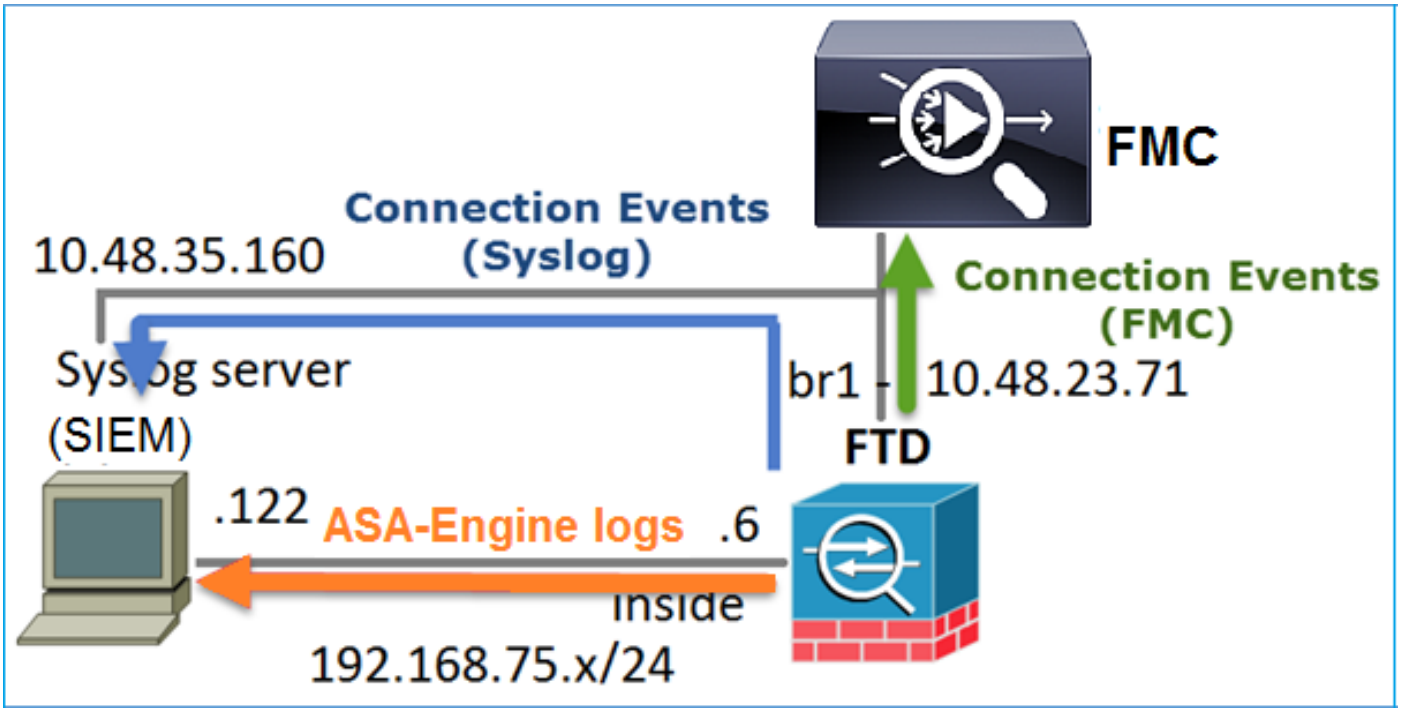
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

Registro FTD

- Quando um usuário configura o registro de FTD a partir de **Configurações da plataforma,** o FTD gera mensagens de Syslog (iguais às do ASA clássico) e pode usar qualquer Interface de dados como origem (inclui o Diagnóstico). Um exemplo de mensagem de syslog gerada nesse caso:

```
May 30 2016 19:25:23 firepower : %ASA-6-302020: Built inbound ICMP connection for faddr
192.168.75.14/1 gaddr 192.168.76.14/0 laddr 192.168.76.14/0
```

- Por outro lado, quando o **registro de nível de regra** da política de controle de acesso (ACP) é ativado, o FTD origina esses registros por meio da interface lógica **br1** como origem. Os registros são originados na subinterface br1 do FTD:



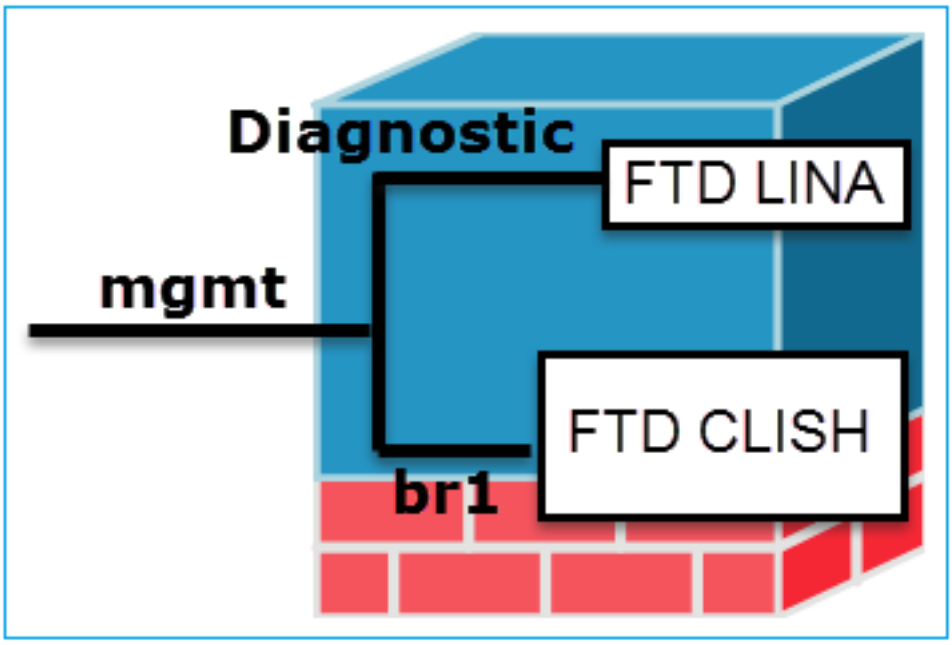
Gerenciar FTD com FDM (gerenciamento integrado)

A partir da versão 6.1, um FTD instalado nos dispositivos ASA5500-X pode ser gerenciado pelo FMC (gerenciamento externo) ou pelo Firepower Device Manager (FDM) (gerenciamento integrado).

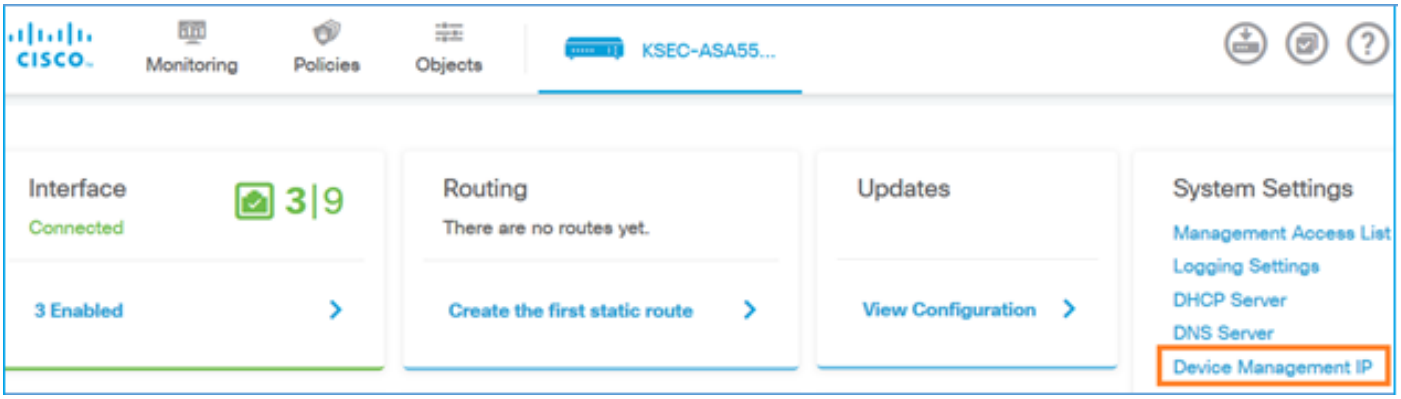
Saída de CLISH do FTD quando o dispositivo é gerenciado pelo FDM:

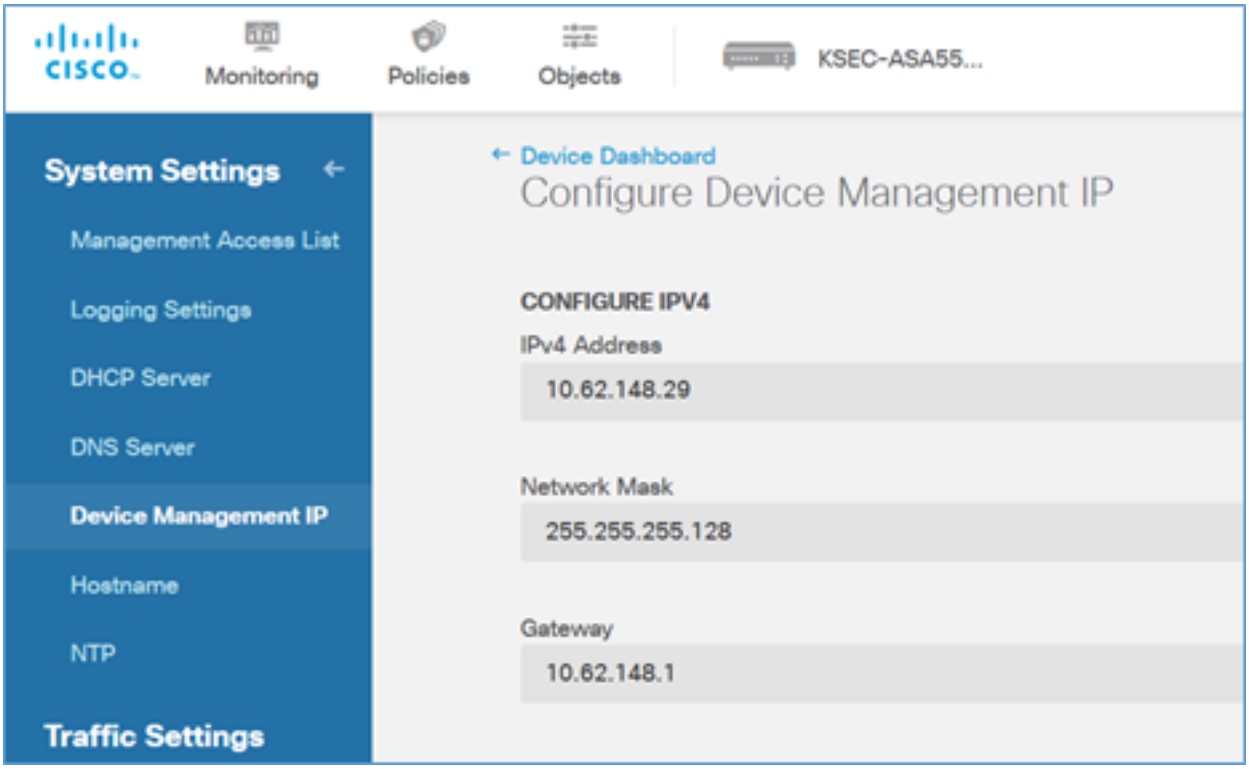
```
> show managers
Managed locally.
>
```

O FDM usa a interface lógica br1. Isso pode ser visualizado da seguinte maneira:



Na interface de usuário do FDM, a interface de gerenciamento pode ser acessada em **Painel do dispositivo > Configurações do sistema > IP de gerenciamento do dispositivo**:





Interface de gerenciamento nos dispositivos de hardware Firepower do FTD

O FTD também pode ser instalado nos dispositivos de hardware Firepower 2100, 4100 e 9300. O chassi Firepower executa seu próprio sistema operacional denominado FXOS, enquanto o FTD é instalado em um módulo/blade.

Dispositivo FPR21xx

Dispositivo FPR41xx

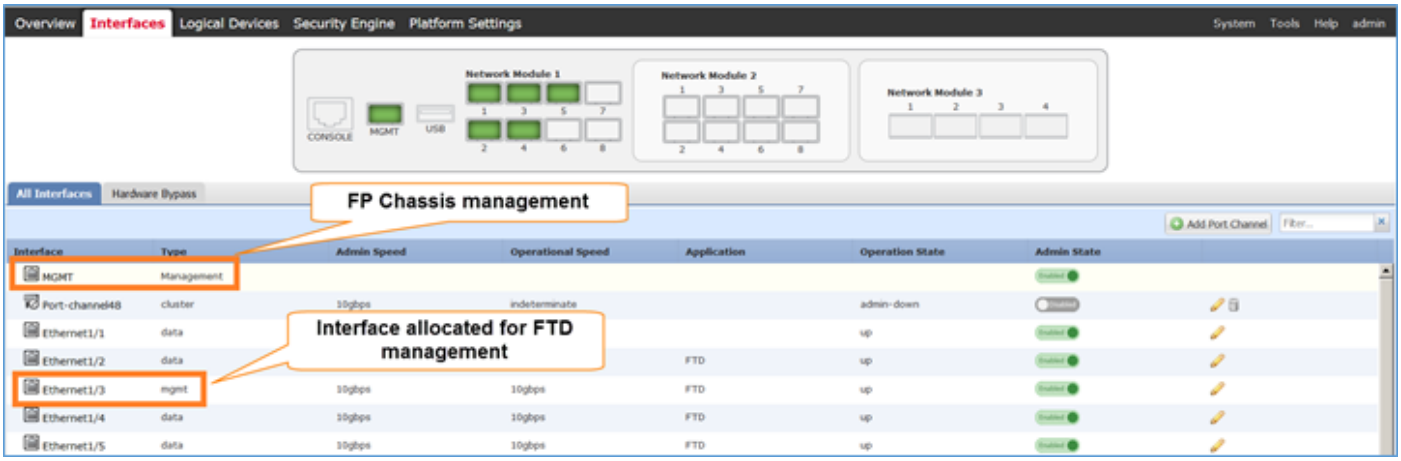
Dispositivo FPR9300

No FPR4100/9300, essa interface é apenas para o gerenciamento de chassi e não pode ser usada/compartilhada com o software FTD executado no módulo FP. Para o módulo FTD, aloque uma interface de dados separada para o gerenciamento de FTD.

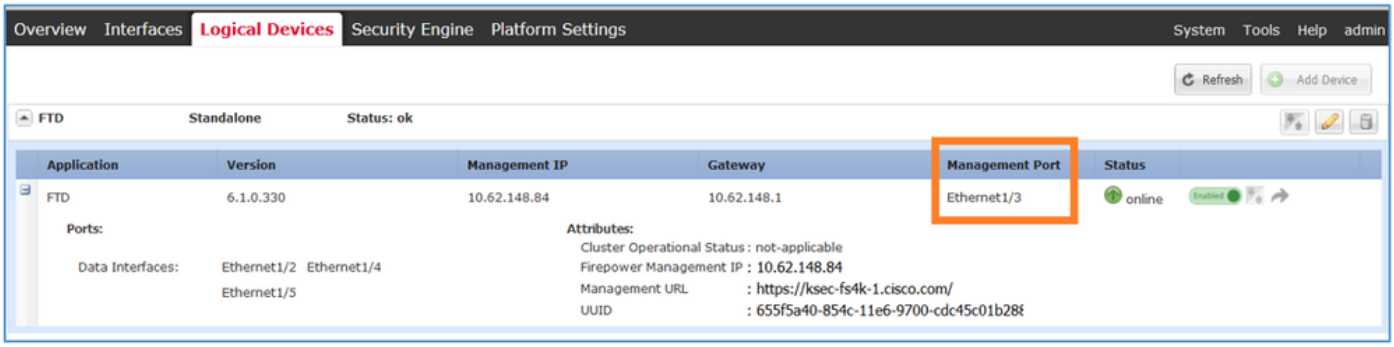
No FPR2100, essa interface é compartilhada entre o chassi (FXOS) e o dispositivo lógico FTD:

```
> 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#
```

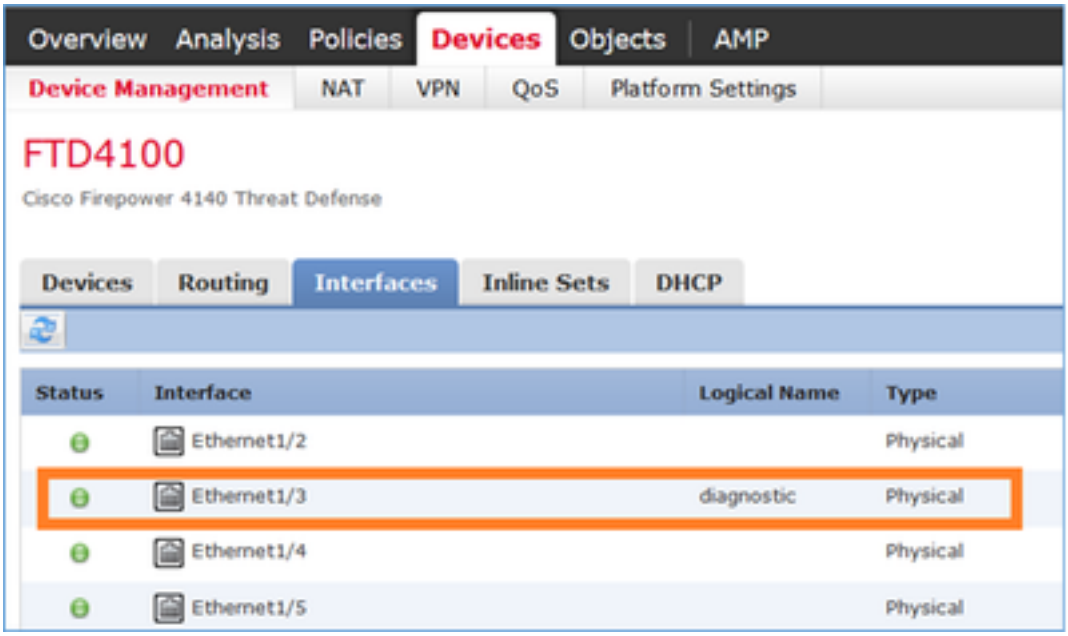
Esta captura de tela é da interface do usuário do Firepower Chassis Manager (FCM) no FPR4100, onde uma interface separada para o gerenciamento do FTD é alocada. Neste exemplo, Ethernet1/3 é escolhida como a interface de gerenciamento FTD: p1



Isso também pode ser visto na guia **Dispositivos lógicos**:p2



No FMC, a interface é mostrada como **diagnóstico:** p3



Verificação da CLI

```
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
```

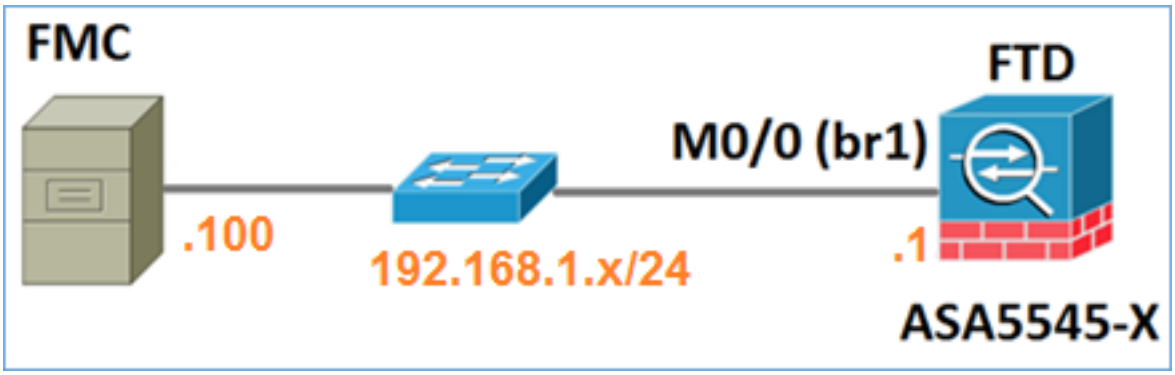
```
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input 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 …
>
```

Integrar FTD com FMC – Cenários de gerenciamento

Estas são algumas das opções de implantação que permitem gerenciar o FTD executado em dispositivos ASA5500-X do FMC.

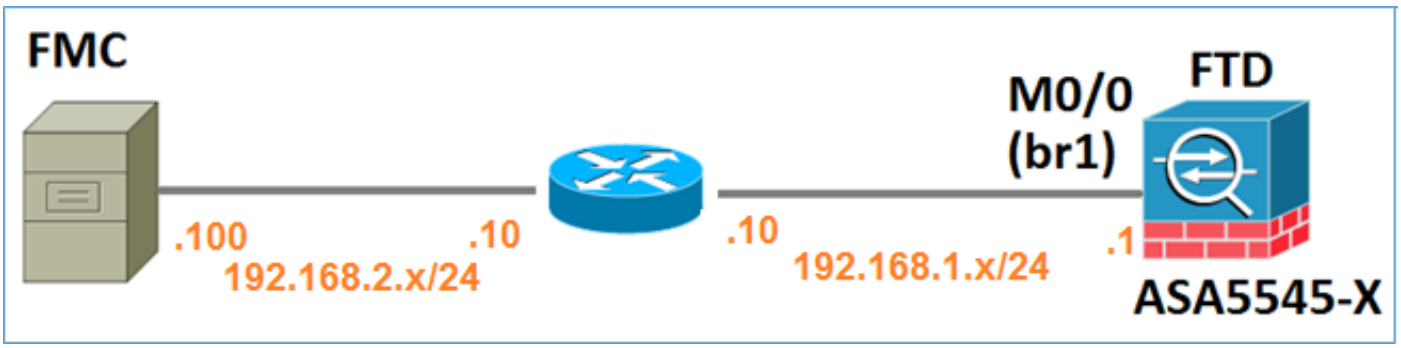
Cenário 1. FTD e FMC na mesma sub-rede.

Essa é a implantação mais simples. Como visto na figura, o FMC está na mesma sub-rede da interface FTD br1:



Cenário 2. FTD e FMC em sub-redes diferentes. O plano de controle não passa pelo FTD.

Nesta instalação, o DTF deve ter uma rota em direção ao CVP e vice-versa. No FTD, o próximo salto é um dispositivo L3 (roteador):



Informações Relacionadas

- Notas de versão do sistema Firepower, Versão 6.1.0
- Nova imagem do dispositivo Cisco ASA ou Firepower Threat Defense
- Guia de configuração do Cisco Firepower Threat Defense para Firepower Device Manager, versão 6.1
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.