配置 Firepower 威胁防御 (FTD) 管理接口

目录

简介

本文档介绍 Firepower 威胁防御 (FTD) 管理接口的运行和配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

- 在ASA5508-X硬件设备上运行的FTD
- 在ASA5512-X硬件设备上运行的FTD
- 在FPR9300硬件设备上运行的FTD
- 运行在6.1.0(build 330)上的FMC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FTD是可在以下平台上安装的统一软件映像：

- 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路由器模块

本文档旨在演示：

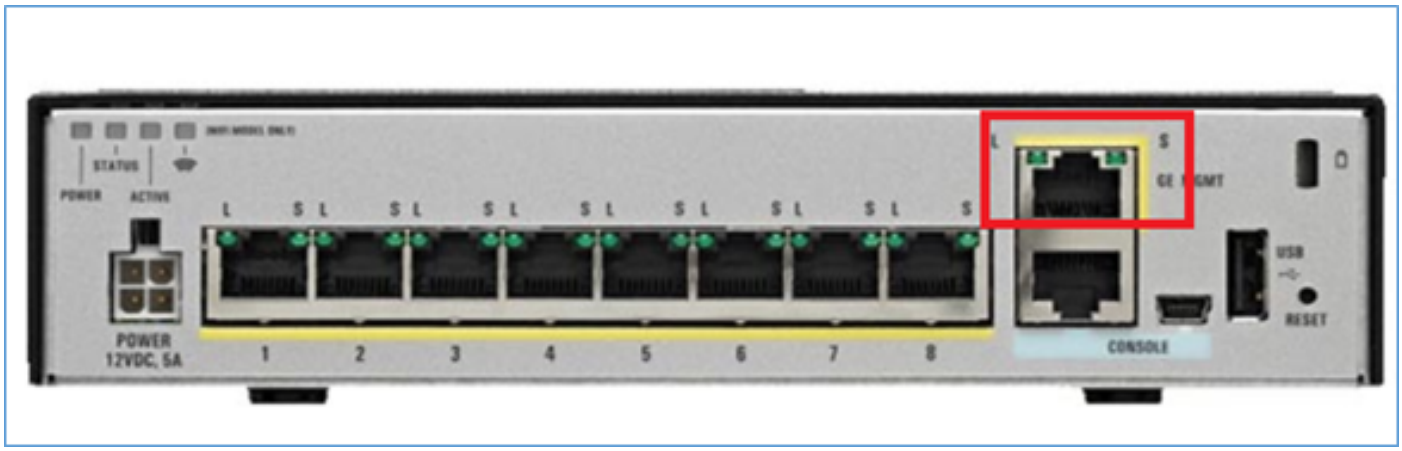
- ASA5500-X设备上的FTD管理接口架构
- 使用FDM时的FTD管理界面
- FP41xx/FP9300系列上的FTD管理接口
- FTD/Firepower管理中心(FMC)集成方案

配置

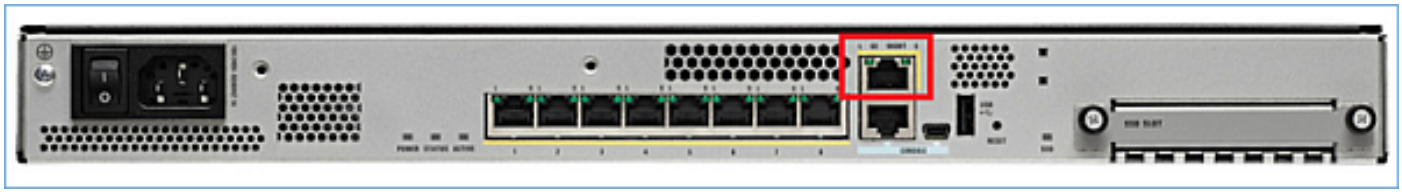
ASA 5500-X设备上的管理接口

ASA5506/08/16-X和ASA5512/15/25/45/55-X设备上的管理接口。

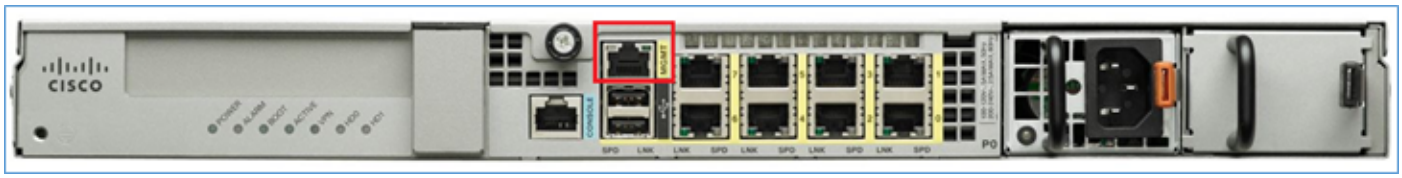
这是ASA5506-X的映像：



这是ASA5508-X的映像：



这是ASA5555-X的映像：



当FTD映像安装在5506/08/16上时，管理接口显示为Management1/1。在5512/15/25/45/55-X设备上，此命令变为Management0/0。在FTD命令行界面(CLI)中，可以在show tech-support输出中进行验证。

连接到FTD控制台并运行命令：

```
<#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>

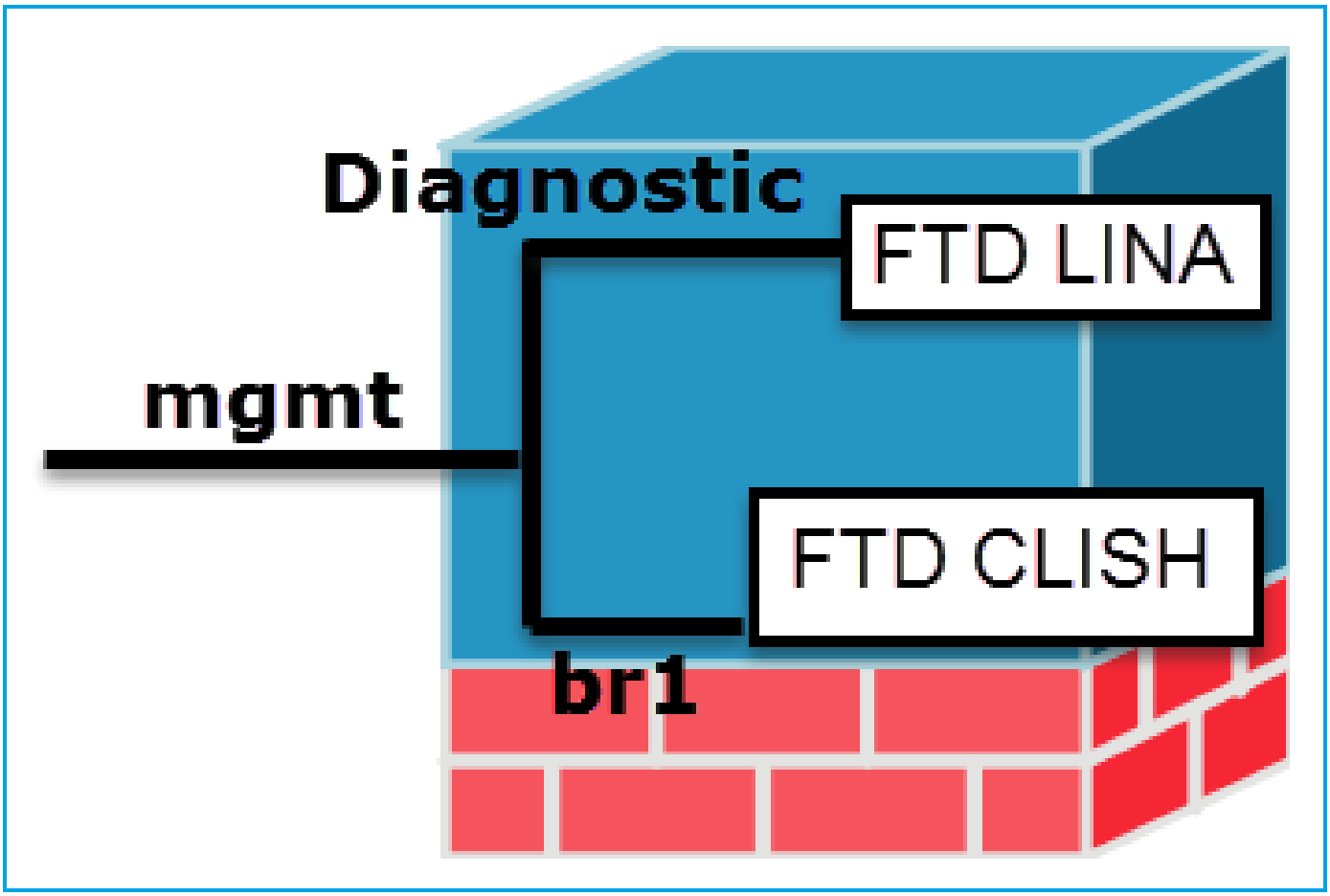
>

show tech-support

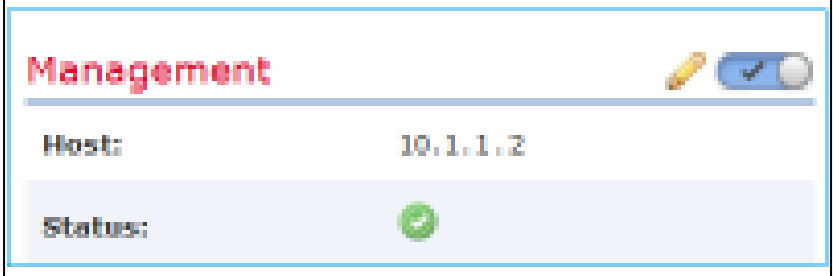
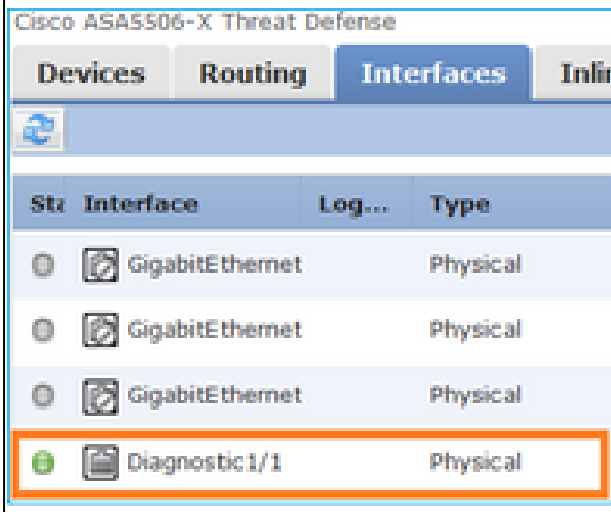
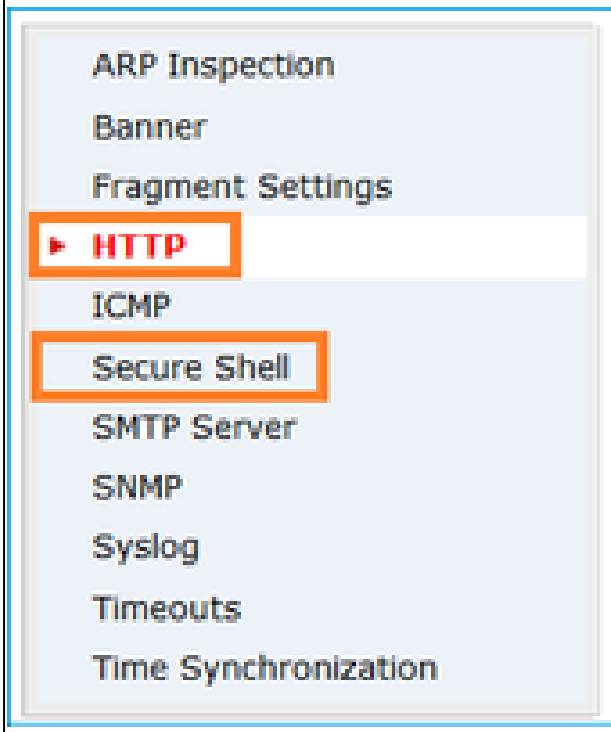
```
------------------[ FTD5512-1 ]--------------------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 330)
UUID                      : 8608e98e-f0e9-11e5-b2fd-b649ba0c2874
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
-----------------------------------------------------

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
```

管理接口架构

管理接口分为两个逻辑接口： br1(FPR2100/4100/9300设备上的management0)和诊断：



	管理- br1/management0	管理 — 诊断
目的	• 此接口用于分配用于FTD/FMC通信的FTD IP。 • 终止FMC/FTD之间的sftunnel。 • 用作基于规则的系统日志的源。 • 提供对FTD框的SSH和HTTPS访问。	• 提供对ASA引擎的远程访问（例如，SNMP）。 • 用作LINA级系统日志、AAA、SNMP等消息的源。
必需	是，因为它用于FTD/FMC通信 （sftunnel在其上终止）	否，不建议使用 进行配置。建议使用 改为使用数据接口*（请查看下面的说明）
配置	此接口在FTD安装（设置）期间配置。 以后，您可以按如下方式修改br1设置： <#root> > **configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1**	可以配置接口 从FMC GUI: 导航到设备>设备管理， 选择Edit按钮并导航到Interfaces

	Setting IPv4 network configuration. Network settings changed. > 第二步：更新FMC上的FTD IP。 	
限制访问	• 默认情况下，只有admin用户可以连接到FTD br1子接口。 • 要限制SSH访问，请使用CLISH CLI > configure ssh-access-list 10.0.0.0/8	对诊断接口的访问 可由FTD控制 Devices > Platform Settings > Secure Shell (SSH) 和 Devices > Platform Settings> HTTP 分别 

验证	方法1 — 从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 — 从FMC GUI Devices > Device Management > Device > Management	方法1 — 从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 — 从FMC GUI 导航到设备>设备管理， 选择Edit按钮并导航到Interfaces

*摘自FTD 6.1用户指南。

Routed Mode Deployment

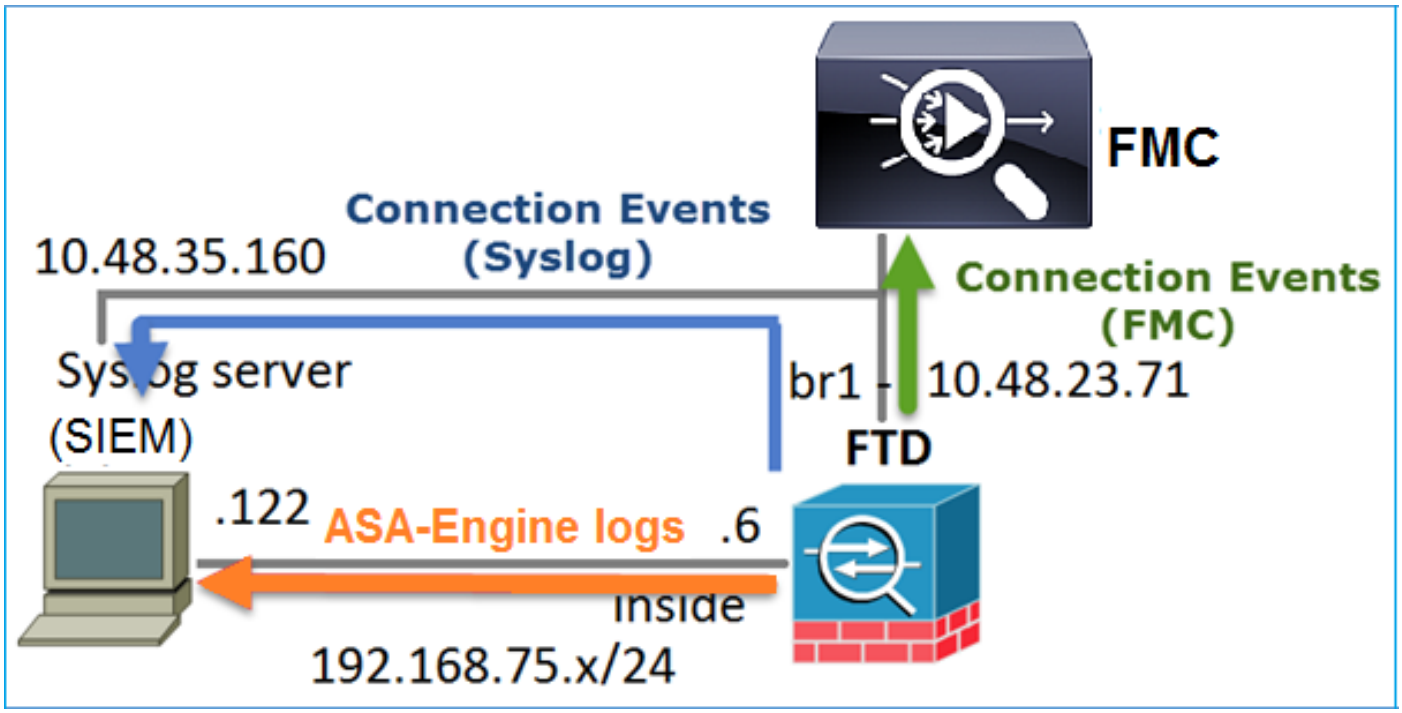
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

- 当用户从Platform Settings配置FTD日志记录时，FTD会生成系统日志消息（与传统ASA上相同），并且可以使用任何数据接口作为源（包括诊断）。在这种情况下生成的系统日志消息示例：

```
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，当启用访问控制策略(ACP)规则级别日志记录时，FTD通过br1作为源创建这些日志。日志源自FTD br1子接口：



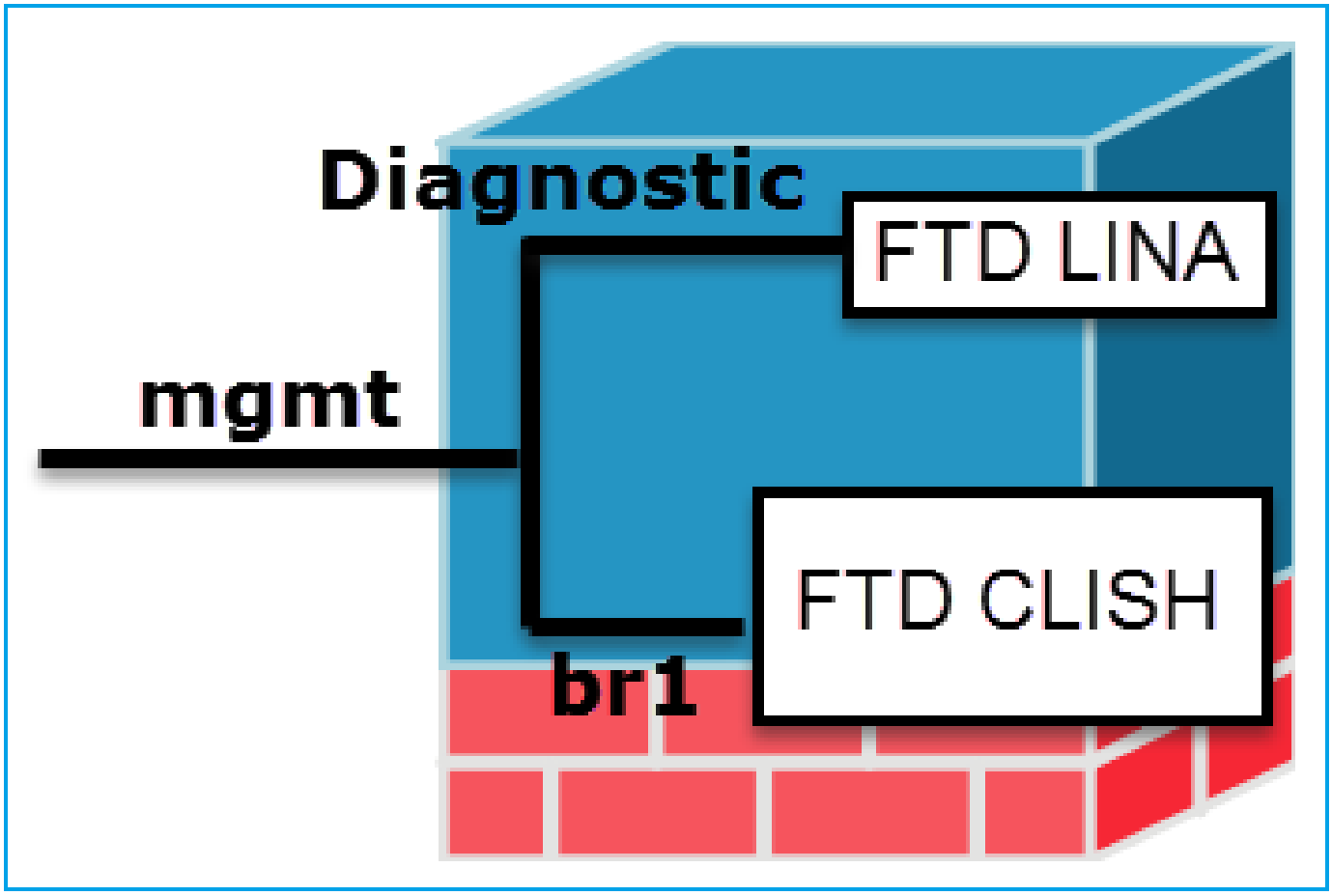
使用FDM管理FTD（机上管理）

从6.1版本开始，ASA5500-X设备上安装的FTD可以通过FMC（机外管理）或Firepower设备管理器(FDM)（机内管理）进行管理。

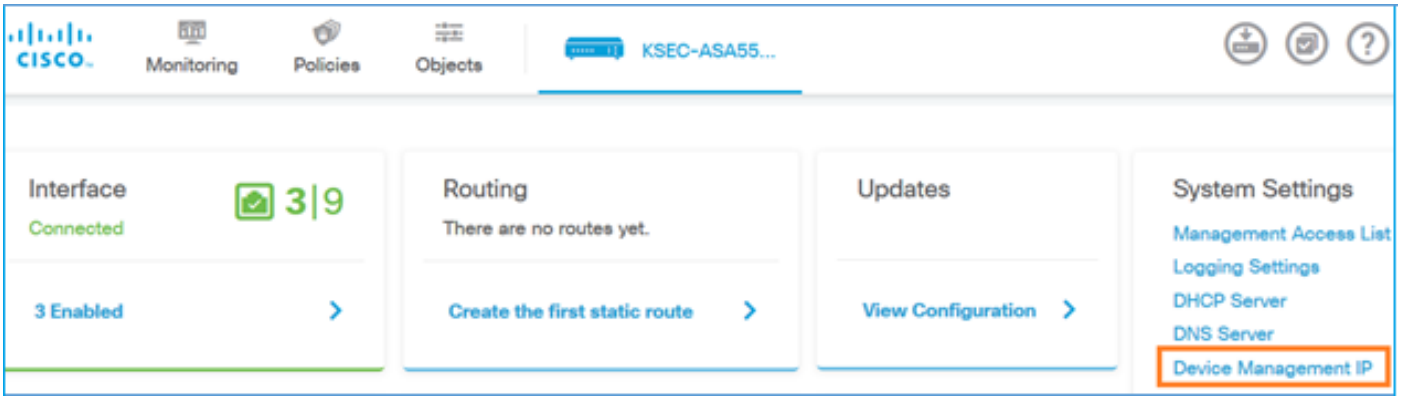
当设备由FDM管理时，FTD CLISH的输出：

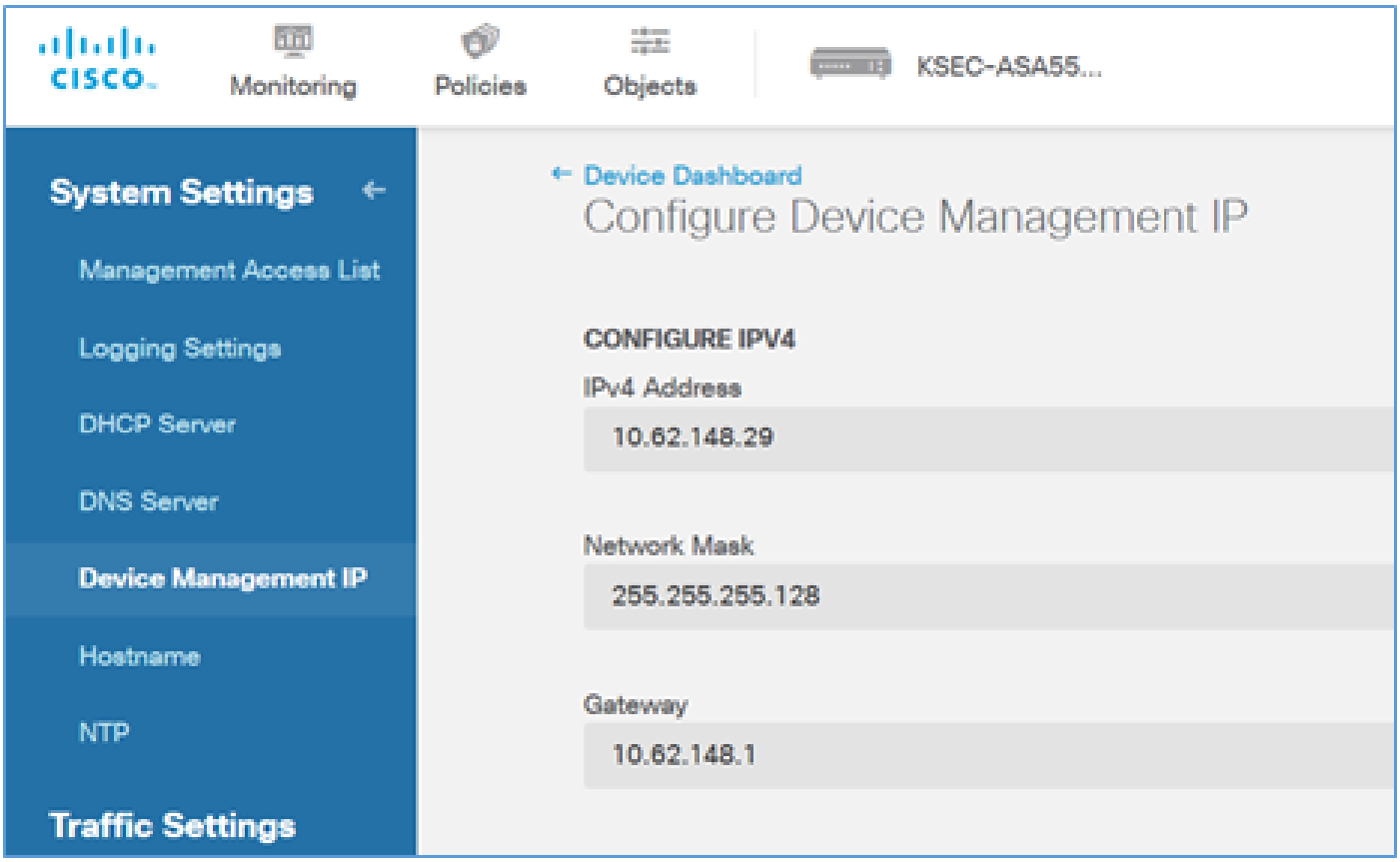
```
<#root>

>

show managers

Managed locally.
>
```

FDM使用br1逻辑接口。上述内容可以图形表示为：



从FDM UI可以从设备控制面板>系统设置>设备管理IP访问管理接口：





FTD Firepower硬件设备上的管理接口

FTD也可以安装在Firepower 2100、4100和9300硬件设备上。当FTD安装在模块/刀片上时，Firepower机箱运行其自己的操作系统，称为FXOS。

FPR21xx设备

FPR41xx设备

FPR9300设备

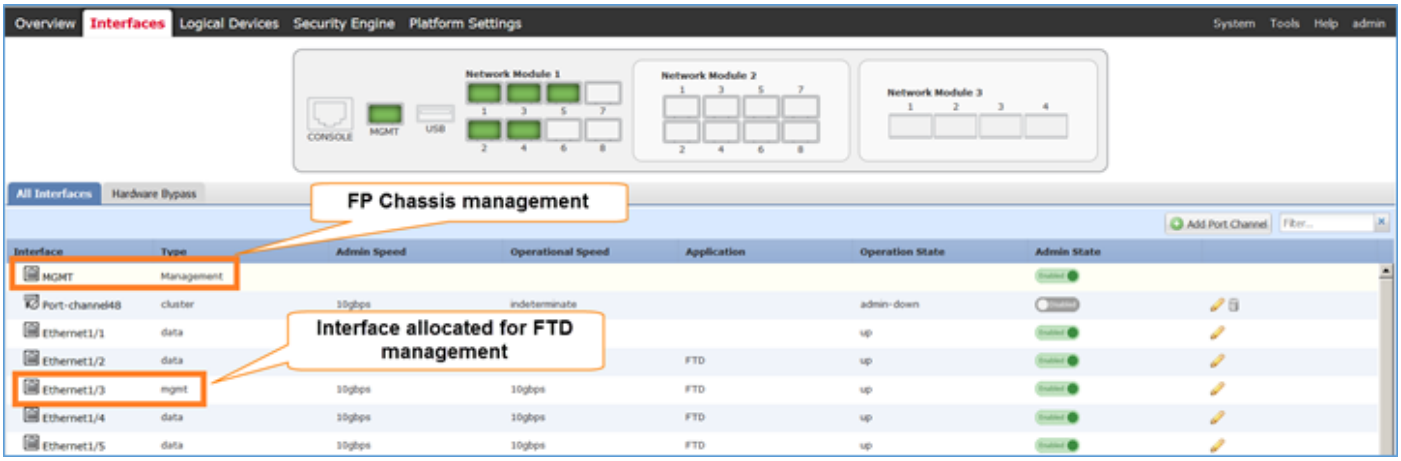
在FPR4100/9300上，此接口仅用于机箱管理，不能与在FP模块内运行的FTD软件一起使用/共享。对于FTD模块，为FTD管理分配单独的数据接口。

在FPR2100上，此接口在机箱(FXOS)和FTD逻辑设备之间共享：

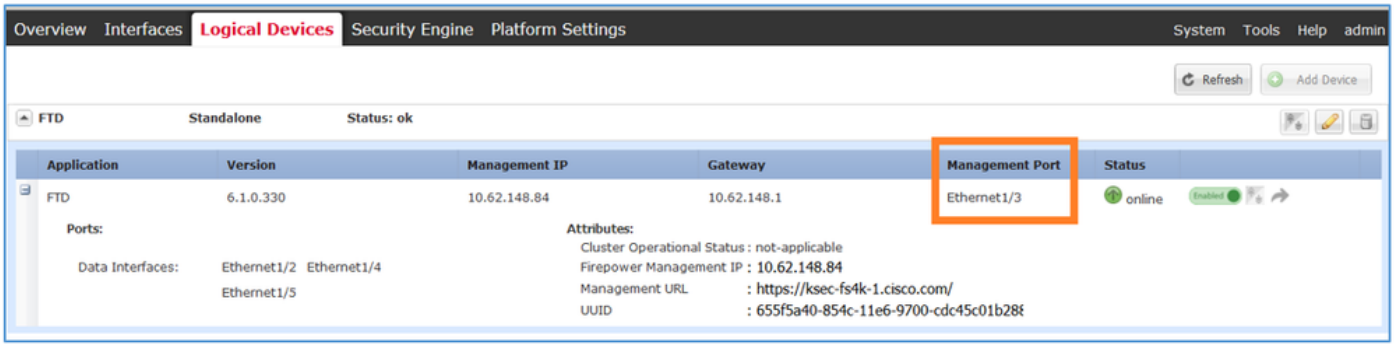
```
<#root>

>

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#
```

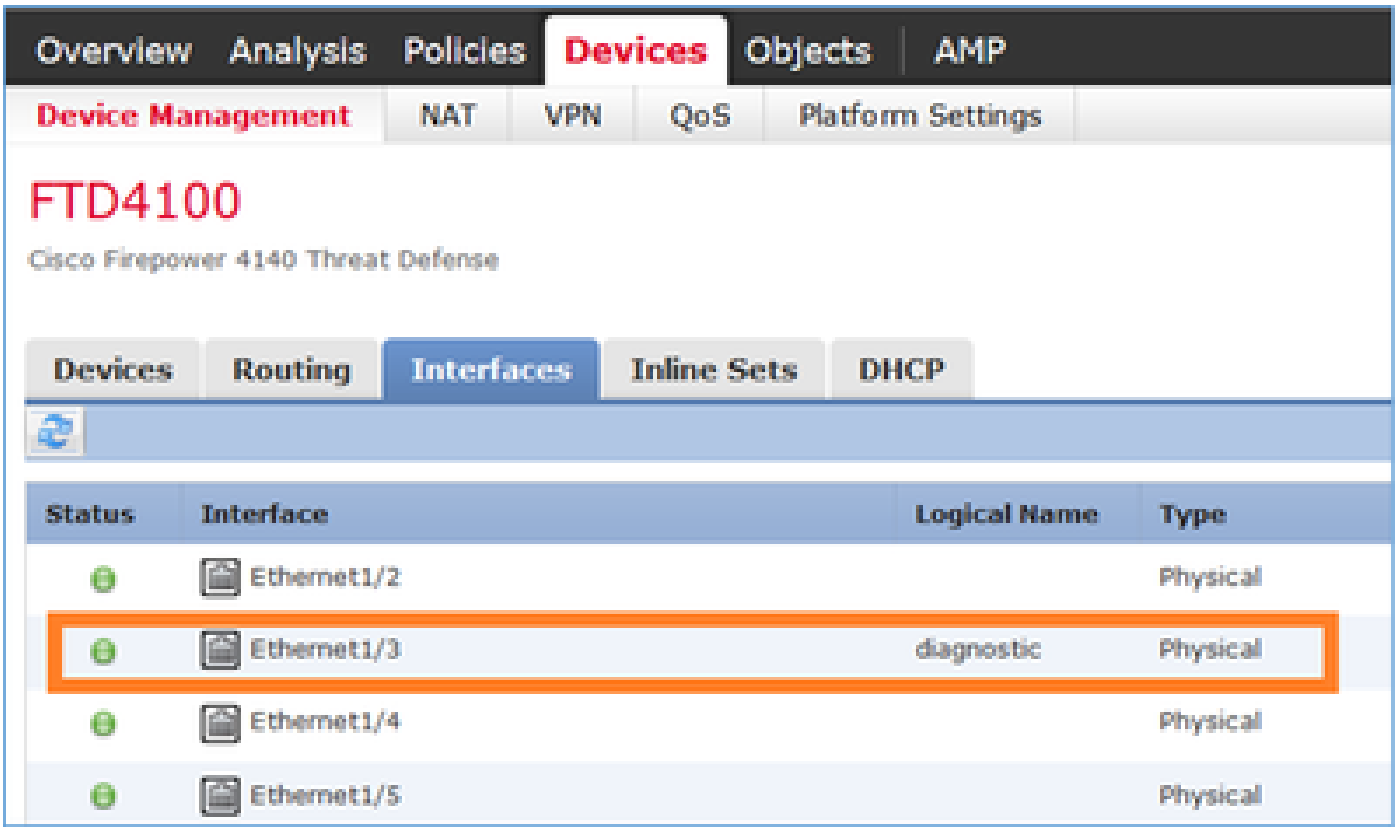
此屏幕截图来自FPR4100上的Firepower机箱管理器(FCM)UI，其中分配了单独的FTD管理接口。在本示例中，选择Ethernet1/3作为FTD管理接口：p1



也可以从Logical Devices选项卡中看到此消息：p2



在FMC上，接口显示为diagnostic:p3



CLI验证

<#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

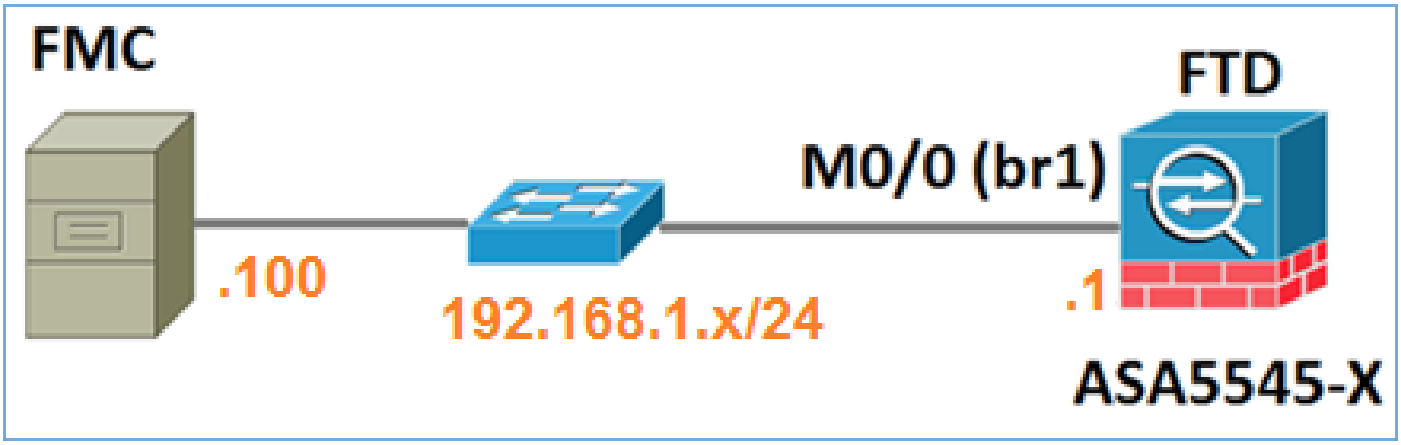
```
      5 minute input rate 2 pkts/sec,  112 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 1 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets

… output omitted …
>
```

将FTD与FMC集成 — 管理方案

以下是允许从FMC管理在ASA5500-X设备上运行的FTD的一些部署选项。

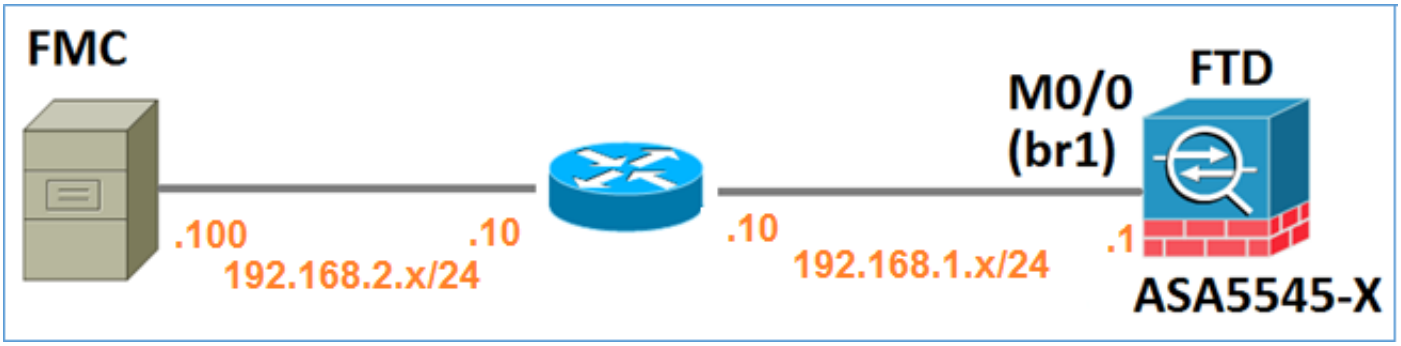
场景 1.FTD和FMC位于同一子网中。

这是最简单的部署。如图所示，FMC与FTD br1接口位于同一子网中：



场景 2：不同子网上的FTD和FMC。控制平面不通过FTD。

在此部署中，FTD必须具有通向FMC的路由，反之亦然。在FTD上，下一跳是第3层设备（路由器）：



相关信息

- Firepower系统版本说明，版本6.1.0
- 重新映像Cisco ASA或Firepower威胁防御设备
- 适用于Firepower设备管理器的思科Firepower威胁防御配置指南，版本6.1

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。