

为Firepower 2100配置FDM机上管理服务

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍如何为安装了FTD的firepower 2100系列配置Firepower设备管理(FDM)机上管理服务。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Firepower 2100、FTD软件安装。
- Cisco FTD (Firepower威胁防御) 基本配置和故障排除。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Firepower 2100 系列。
- 思科FTD版本6.2.3

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

本文档的主要目的是指导您完成为firepower 2100系列启用FDM机上管理所需的步骤。

您有两个选项可以管理Firepower 2100上安装的Firepower威胁防御(FTD)：

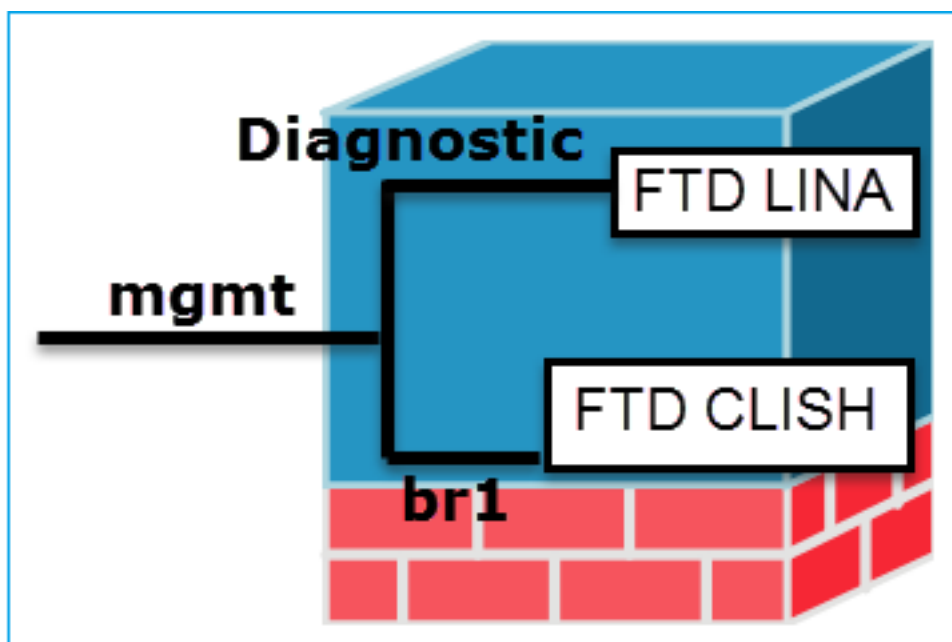
- FDM机上管理。

- Cisco FMC (Firepower管理中心) 。

注：不能同时使用FDM和FMC来管理firepower 2100中安装的FTD。在firepower 2100 FTD上启用FDM机上管理后，除非禁用本地管理并将管理重新配置为使用FMC，否则无法使用FMC管理FTD。另一方面，向FMC注册FTD会禁用FTD上的FDM机上管理服务。

注意：目前，思科没有任何将FDM firepower配置迁移到FMC的选项，反之亦然，当您选择为firepower 2100中安装的FTD配置何种管理类型时，请将此考虑在内。

管理接口分为两个逻辑接口，br1(FPR2100/4100/9300设备上的管理0)和诊断：



管理 — br1/management0

- 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。

必需 是，因为它用于FTD/FMC通信(sftunnel terminate on it)。

管理 — 诊断

- 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。

否，不建议对其进行配置。建议改用数据接口（请查看下面

注：将诊断接口的IP地址保留为不用的优点是，您可以将管理接口与任何其他数据接口放在同一网络中。如果配置诊断接口，则其IP地址必须与管理IP地址位于同一网络，并且它视为常规接口，不能与任何其他数据接口位于同一网络。由于管理接口需要互联网访问才能进行更新，因此将管理接口与内部FTD接口置于同一网络意味着您可以仅使用交换机在LAN上部署FTD，并将内部接口指定为管理接口的默认网关（这仅适用于FTD在路由模式下部署的情况）。

FTD可以安装在firepower 2100设备中。Firepower机箱运行自己的操作系统FXOS (Firepower可扩展操作系统) 来控制设备的基本操作，而FTD逻辑设备安装在模块/刀片上。

注意：您可以使用称为FCM (Firepower机箱管理器) 或FXOS CLI (命令行界面) 的FXOS GUI (图形用户界面) 配置firepower机箱功能；但是，当FTD安装在firepower 2100系列 (仅FXOS CLI) 上时，GUI FCM不可用。

Firepower 21xx设备：

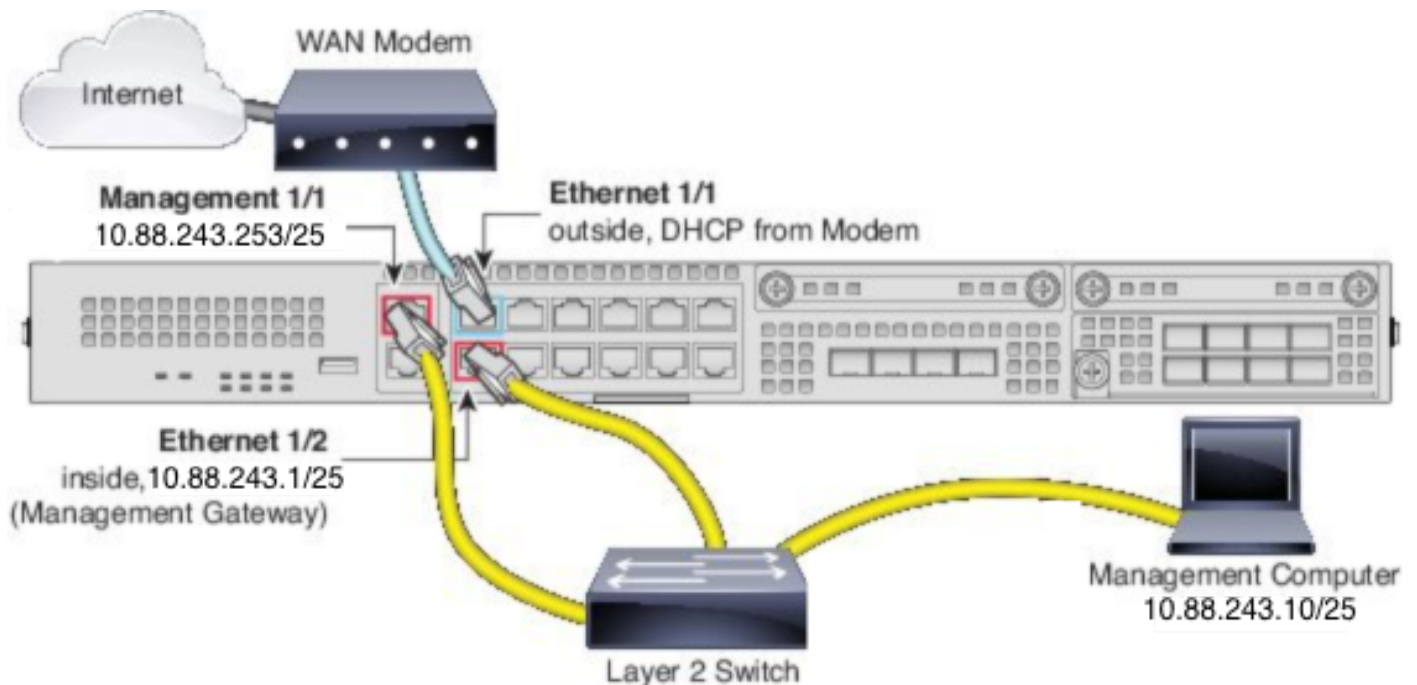


注：在firepower 2100系列上，管理接口在机箱FXOS和FTD逻辑设备之间共享。

配置

网络图

默认配置假设某些firepower 2100接口用于内部和外部网络。如果根据这些期望将网络电缆连接到接口，则初始配置更易于完成。要为Firepower 2100系列布线，请参见下一个映像。



注意:该图显示使用第2层交换机的简单拓扑。也可使用其他拓扑，您的部署可能因基本逻辑网络连接、端口、寻址和配置要求而异。

配置

要在firepower 2100系列上启用FDM机上管理，请按照以下步骤操作。

1.通过控制台访问FPR2100机箱并连接到FTD应用。

```
firepower# connect ftd  
>
```

2.配置FTD管理IP地址。

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

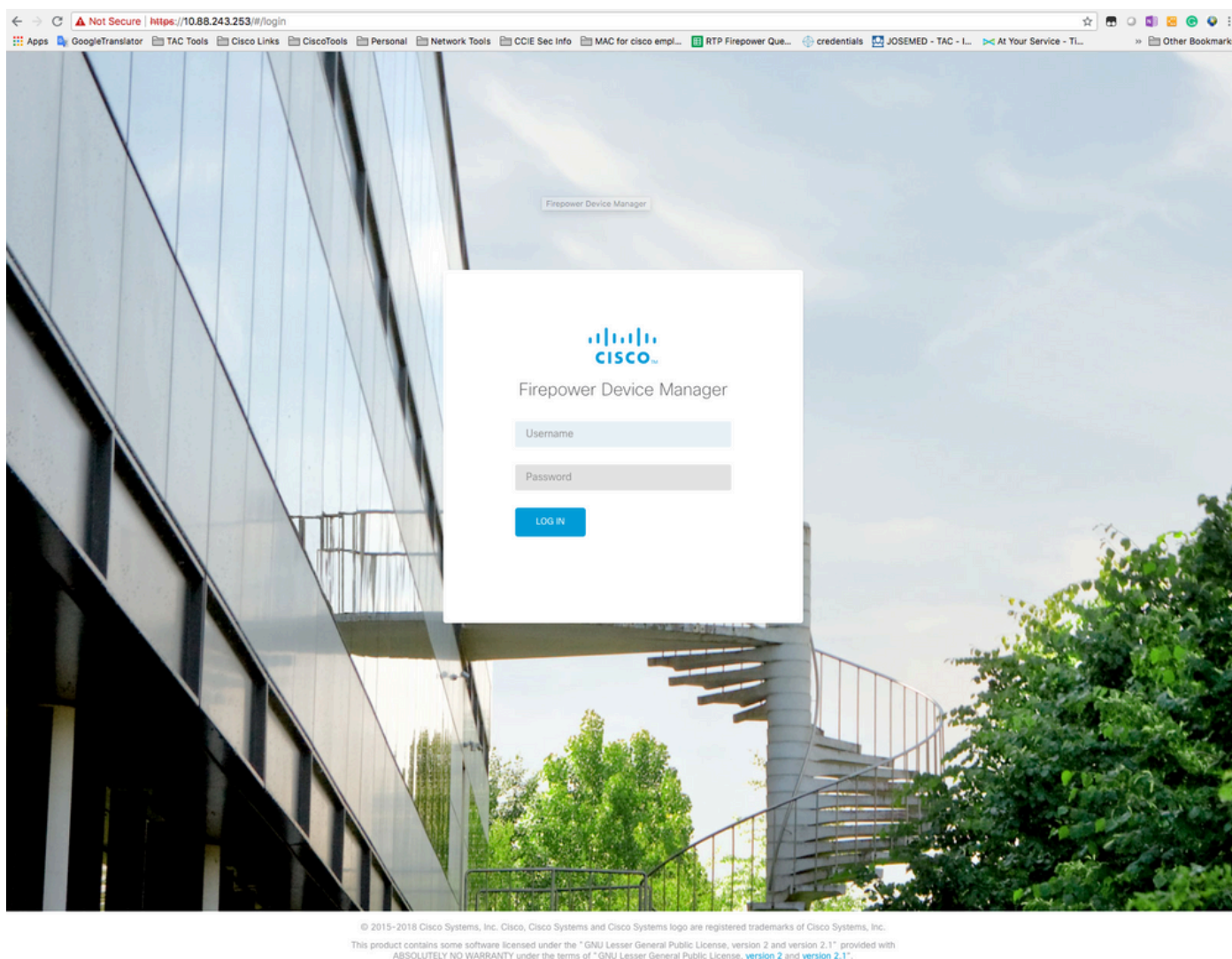
3.将管理类型配置为local。

```
>configure manager local
```

4.配置允许从哪些IP地址/子网对FTD进行本地管理访问。

```
>configure https-access-list 0.0.0.0/0
```

5.打开浏览器并使用https进入您配置为管理FTD的IP地址。这可以打开FDM (箱内) 管理器。



6.登录并使用默认firepower凭证、用户名admin和密码Admin123。

Device Setup

1 Configure Internet Connection 2 Configure Time Settings 3 Smart License Registration

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1	Default Action
Trust Outbound Traffic	Block all other traffic
This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	The default action blocks all other traffic.

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP

Configure IPv6

Using DHCP

Management Interface

Configure DNS Servers

Primary DNS IP Address: 208.67.222.222

NEXT

Don't have internet connection? [Skip device setup](#)

验证

1.使用下一命令验证为FTD配置的网络设置。

```
> show network
===== [ System Information ] =====
Hostname                : firepower
DNS Servers             : 208.67.222.222
                        : 208.67.220.220
Management port        : 8305
IPv4 Default route     :
  Gateway               : 10.88.243.129

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:2C:C8:41:09:80
----- [ IPv4 ] -----
Configuration           : Manual
Address                 : 10.88.243.253
Netmask                 : 255.255.255.128
Broadcast               : 10.88.243.255
----- [ IPv6 ] -----
Configuration           : Disabled
```

```
=====[ Proxy Information ]====  
State : Disabled  
Authentication : Disabled
```

2.使用下一命令验证为FTD配置的管理类型。

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

相关信息

[思科Firepower设备管理器](#)

[使用Firepower管理中心的Firepower 2100系列的思科Firepower威胁防御快速入门指南](#)

[配置Firepower威胁防御\(FTD\)管理接口](#)

[重新映像Firepower 2100系列](#)

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）。