解密安全防火墙术语（适用于新接触Firepower的人员）

目录

简介

本文档介绍各种常用的Cisco防火墙术语。本文档还介绍了如何从一种CLI模式切换到另一种模式。

先决条件

要求

学习本主题之前没有任何要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全防火墙管理中心(FMC)
- 思科Firepower威胁防御(FTD)
- 思科Firepower设备管理(FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- 自适应安全设备(ASA)

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。

常用技术术语

FTD：Firepower威胁防御

FTD是下一代防火墙，可提供超越传统防火墙的更多功能。它包括入侵防御系统(IPS)、高级恶意软件防护(AMP)、URL过滤、安全情报等服务。FTD与ASA（自适应安全设备）非常相似，但具有附加功能。FTD运行2个引擎，即LINA和SNORT。

LINA：基于Linux的集成网络架构

我们将ASA称为FTD设备中的Lina。LINA只是FTD在其上运行的ASA代码。Lina主要关注网络层安全。它通过其应用检测和控制功能集成了一些第7层防火墙功能。

SNORT

Snort引擎是网络入侵检测与防御系统。Snort的主要功能包括数据包检测（用于识别其中的异常）、基于规则的检测、实时警报、日志记录和分析以及与其他安全工具的集成。Snort能够执行L7检测（应用层流量），不仅基于数据包报头，还基于数据包的内容。

您可以灵活地编写自己的自定义规则，以在应用层定义特定模式或签名，从而增强检测功能。它通过评估数据包的负载来执行深度数据包检测。您甚至可以在此处执行加密数据包的解密。

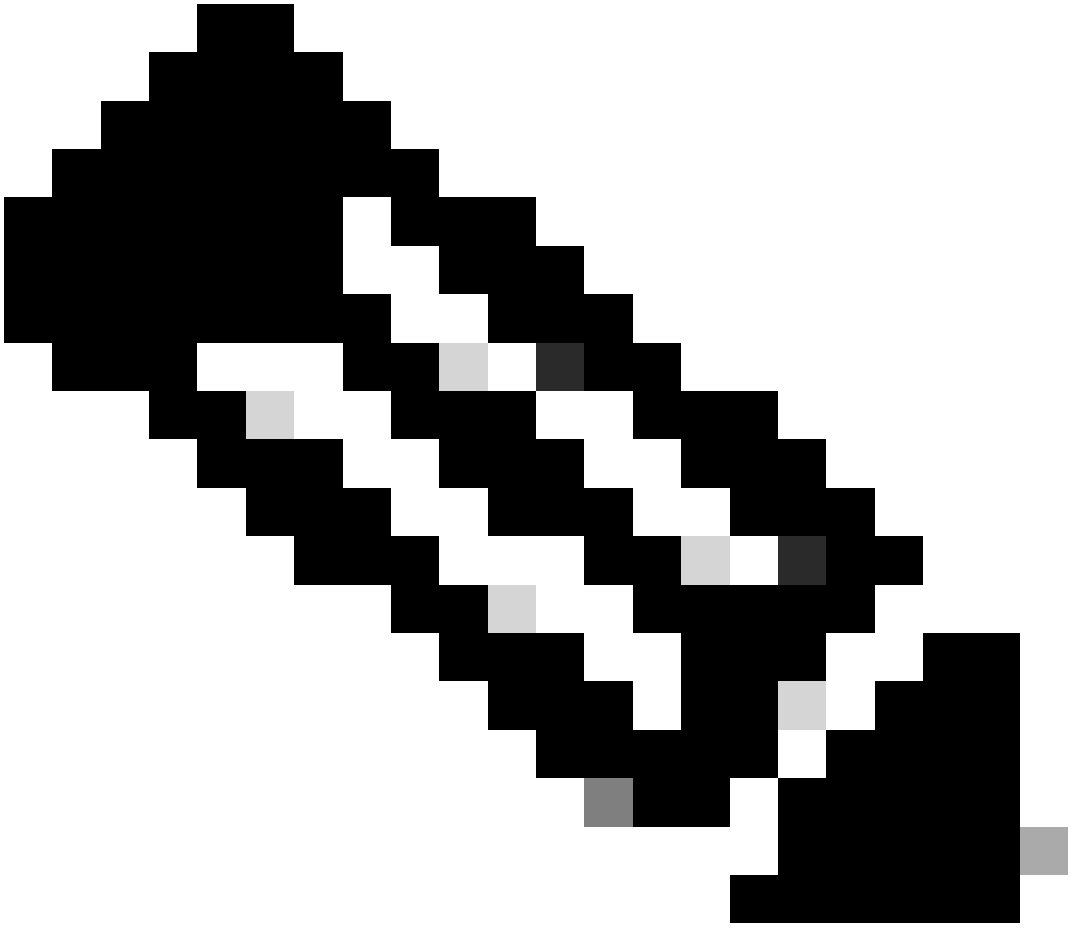
FXOS：Firepower可扩展操作系统

它是运行FTD设备的操作系统。根据平台的不同，FXOS用于配置功能、监控机箱状态和访问高级故障排除功能。

在平台模式下使用自适应安全设备软件的Firepower 4100/9300和Firepower 2100上的FXOS允许更改配置，而在其他平台（特定功能除外）中，该功能是只读的。

FCM：Firepower机箱管理器

FCM是用于管理机箱的GUI。它仅适用于在平台模式下运行ASA的9300、4100和2100。

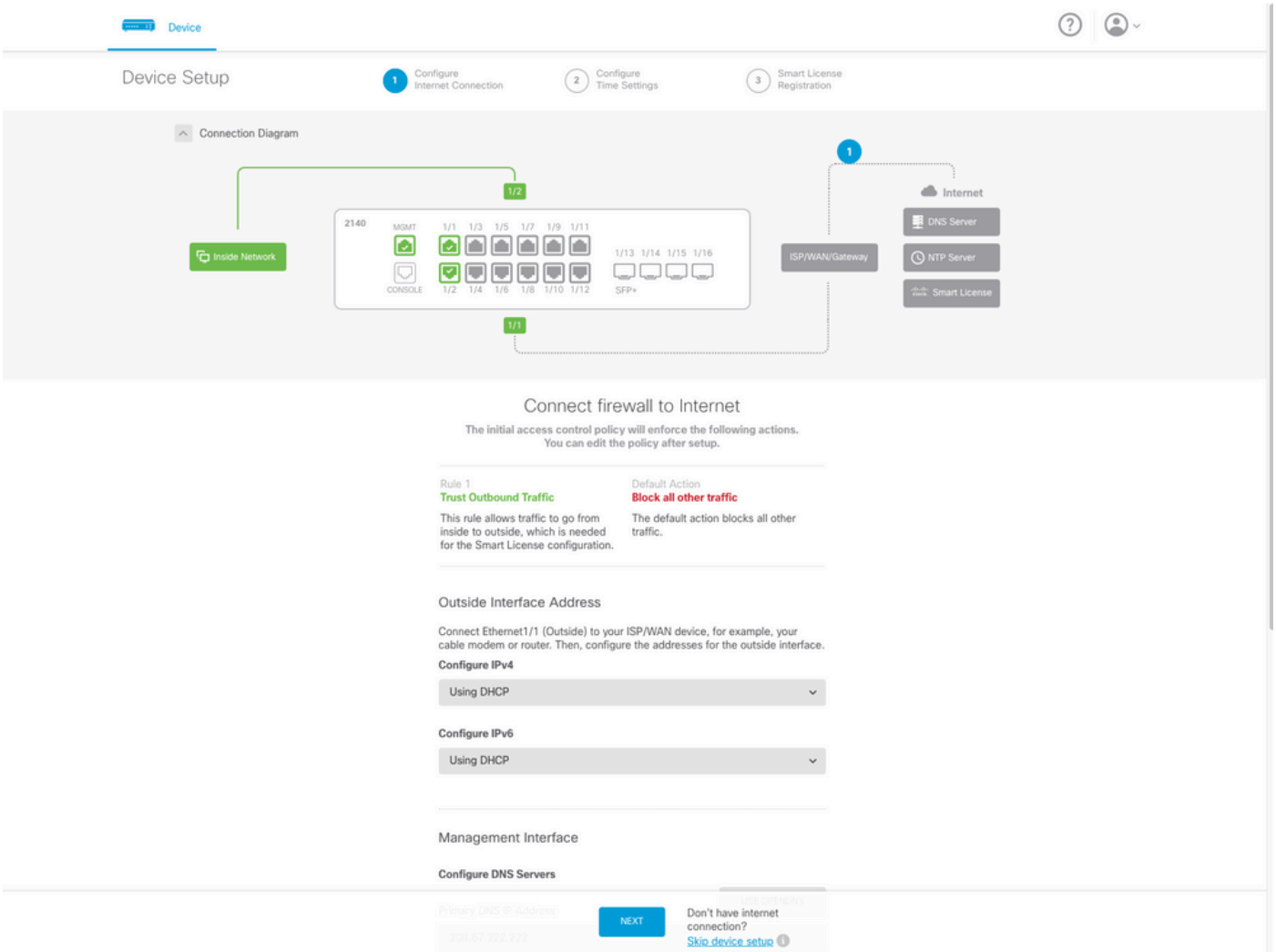


注意：您可以拿笔记本电脑打个比方。FXOS是在机箱（笔记本电脑）上运行的操作系统（笔记本电脑中的Windows操作系统）。我们可以在其上安装FTD（应用程序实例），它运行在Lina和Snort（组件）上。

与ASA不同，您无法通过CLI管理FTD。您需要一个单独的基于GUI的管理。此类服务有两种类型：FDM和FMC。

FDM：Firepower设备管理

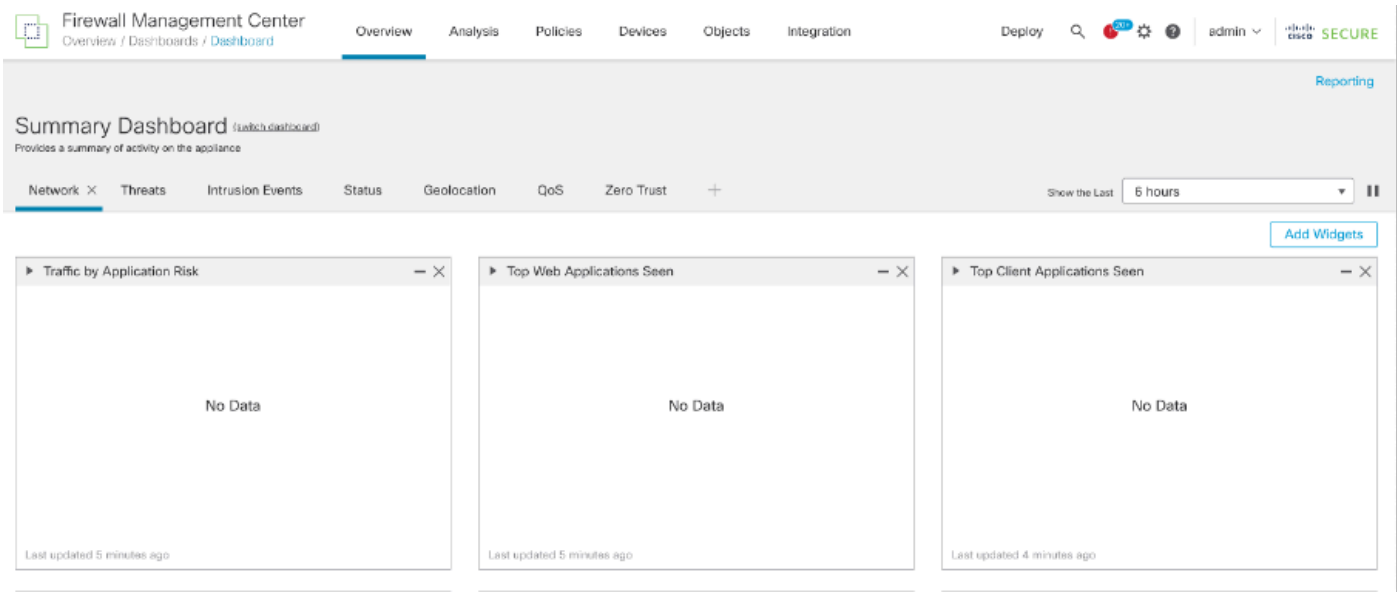
- FDM是一种机上管理工具。它提供了一个基于Web的界面，用于配置、管理和监控安全策略和系统设置。
- 使用FDM的一大优势在于，您不需要额外的许可证来实现此功能。
- 只能使用1个FDM管理1个FTD。



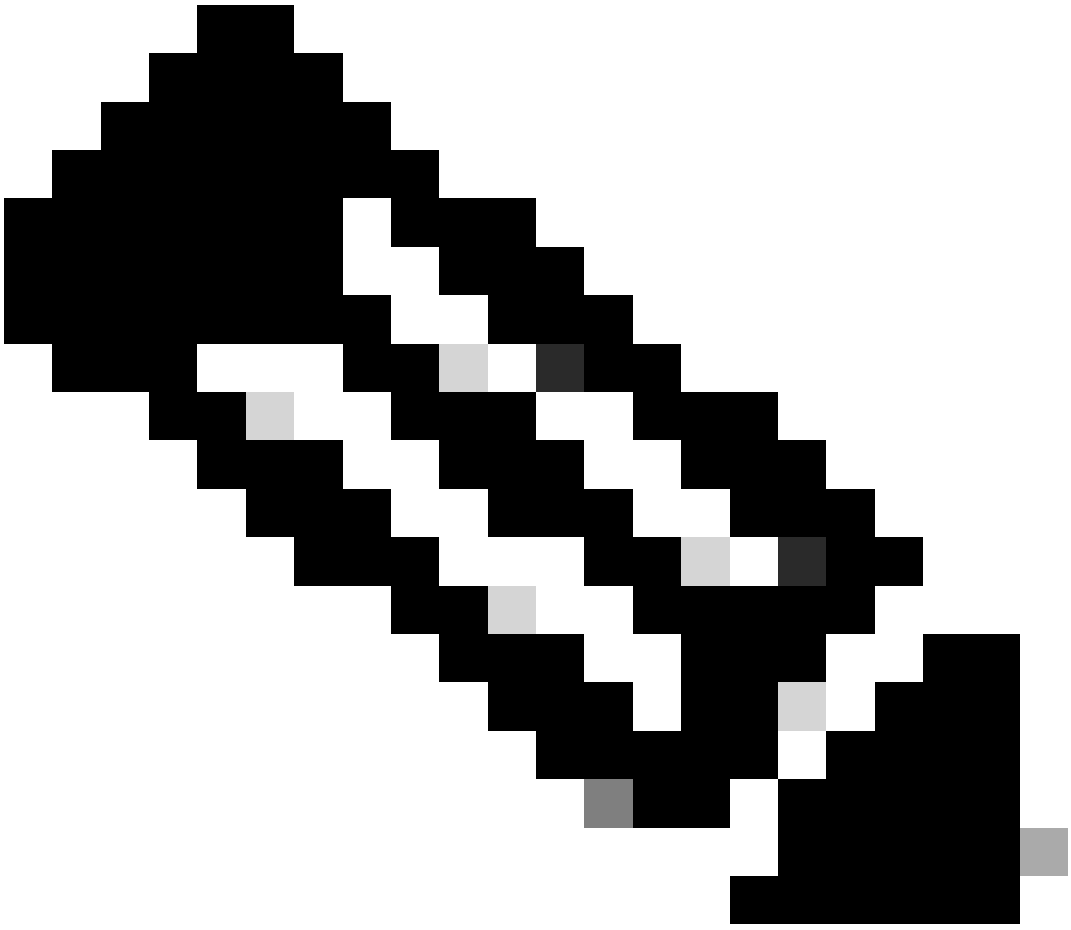
FDM

FMC：Firepower管理中心

- FMC是适用于Cisco FTD设备（具备Firepower服务的Cisco ASA设备）的集中管理解决方案。它还提供可用于配置、管理和监控FTD设备的GUI。
- 您可以使用硬件FMC设备或虚拟FMC设备。
- 这需要单独的许可证才能运行。
- FMC的一个加点是您可以使用1个FMC设备管理多个FTD设备。



FMC



注意：不能同时使用FDM和FMC来管理FTD设备。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

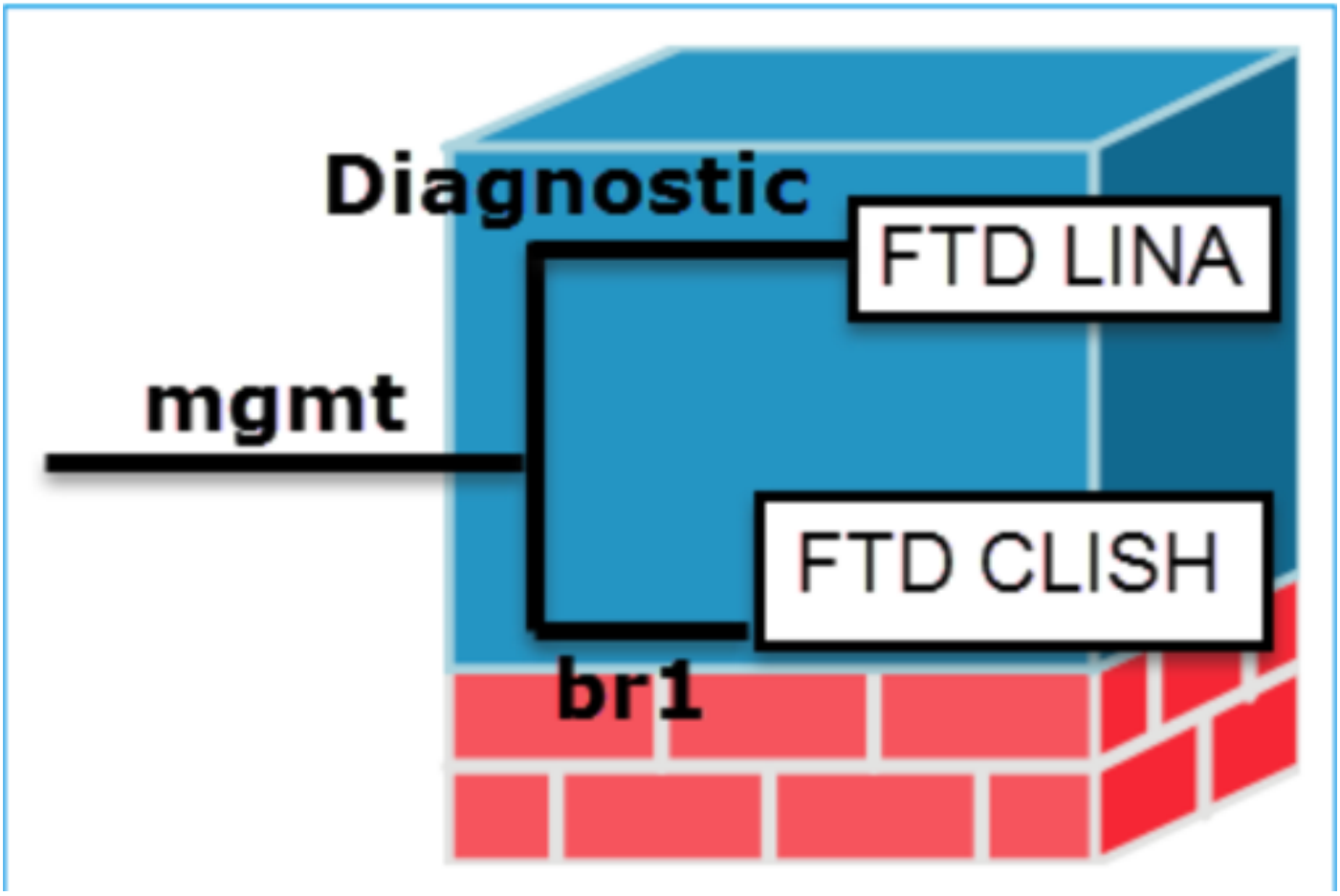
FTD会禁用FTD上的FDM机上管理服务。

CLISH：命令行界面Shell

CLISH是Cisco Firepower威胁防御(FTD)设备中使用的命令行界面。您可以使用此CLISH模式对FTD运行命令。

诊断管理

FTD设备有两个管理接口：诊断管理接口和FTD管理接口。如果必须访问LINA引擎，我们使用诊断管理接口。如果必须访问SNORT引擎，则使用FTD管理接口。两者是不同的接口，需要不同的接口IP地址。



管理接口

ASA平台模式

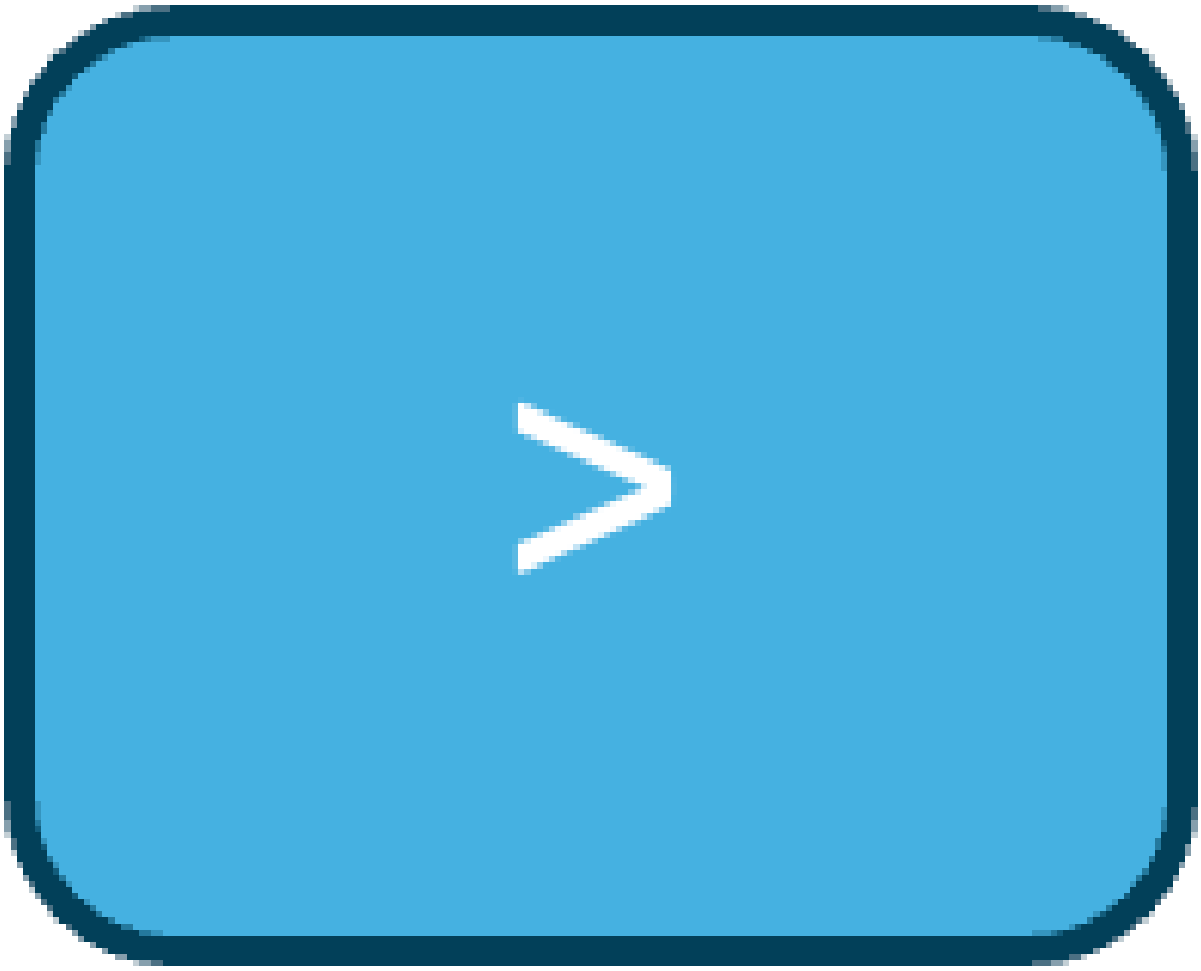
1. 当处于平台模式时，必须在FXOS中配置基本操作参数和硬件接口设置，例如启用接口、建立EtherChannel、NTP、映像管理等。
2. 所有其他配置必须通过ASA CLI/ASDM完成。
3. 您在此具有FCM访问权限。

ASA设备模式

1. 在Firepower 2100中，从9.13（包括）开始引入设备模式下的ASA。
2. 通过设备模式，可以配置ASA中的所有设置。FXOS CLI中仅提供高级故障排除命令。
3. 此模式下没有FCM。

FTD上的不同提示

CLISH



CLISH

根模式/专家模式

专家模式

Lina模式

Lina模式

FXOS模式

FXOS模式

如何在不同提示之间移动

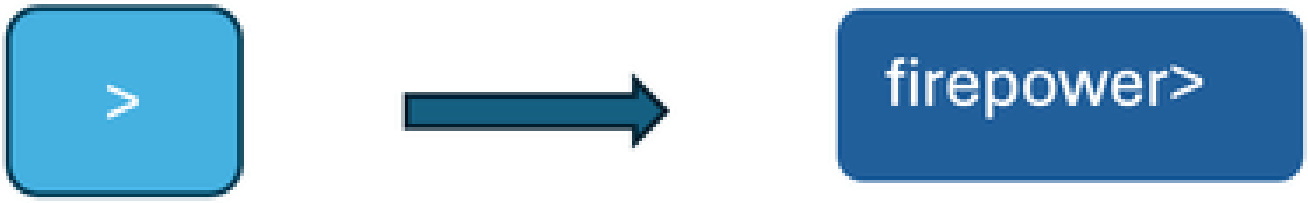
CLISH模式到FTD根模式

Clish模式到Expert模式

```
> expert
```

```
admin@firepower:~$  sudo su
Password:
root@firepower:/home/admin#
```

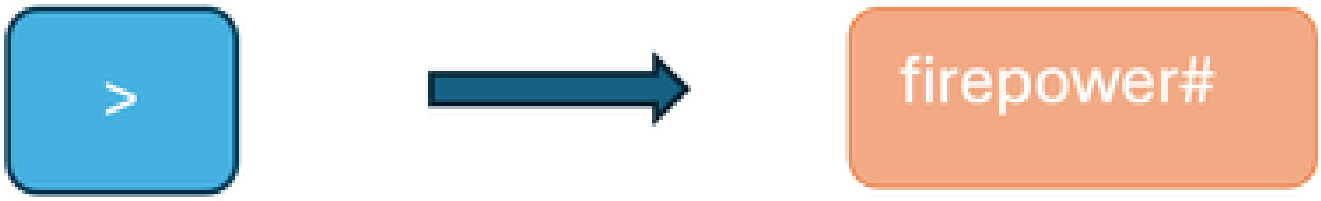
CLISH模式到Lina模式



Clish模式到Lina模式

```
> system support diagnostic-cli
Attaching to Diagnostic CLI . . . Press 'Ctrl+a then d' to detach .
Type help or '?' for a list of available commands .
firepower> enable
Password :
firepower#
```

CLISH模式至FXOS模式



Clish Mode to FXOS mode（清洁模式到FXOS模式）

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.
(------ cropped output -------)
firepower#
```

根模式到LINA模式

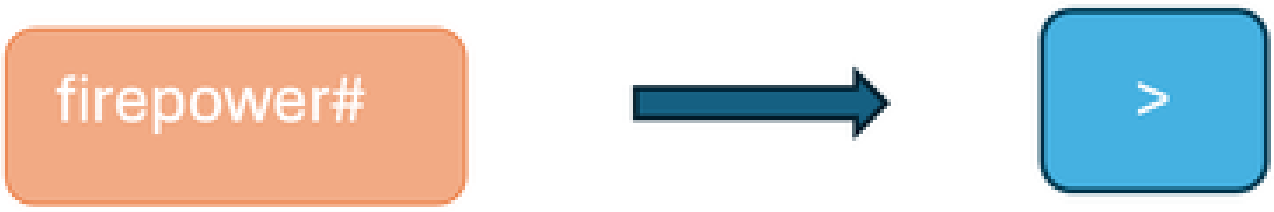
专家到Lina模式

```
root@firepower:/home/admin#
root@firepower:/home/admin#   exit
exit
admin@firepower:~$ exit
logout
>
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

或

```
root@firepower:/home/admin#
root@firepower:/home/admin#   sfconsole
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

FXOS至FTD CLISH模式（1000/2100/3100系列设备）



FXOS至Clish模式

```
firepower# connect ftd
>
To exit the fxos console
> exit
firepower#
```

FXOS至FTD CLISH模式（4100/9300系列设备）

此示例显示如何连接到模块1上的威胁防御CLI：

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1> connect ftd
>
```

退出控制台：

输入~，然后输入quit退出Telnet应用程序。

```
Example:
>exit
Firepower-module1> ~
telnet> quit
firepower#
```

相关文档

有关可在firepower设备上运行的各种命令的详细信息，请参阅FXOS命令参考、FTD命令参考。

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）。