瞭解安全防火牆術語（適合剛接觸Firepower的使用者）

目錄

簡介

本文檔介紹了各種常用的思科防火牆術語。本文檔還介紹了如何從一個CLI模式切換到另一個CLI模式。

必要條件

需求

之前沒有學習此主題的要求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower威脅防禦(FTD)
- Cisco Firepower裝置管理(FDM)
- Firepower eXtensible 作業系統 (FXOS)
- Firepower Chassis Manager (FCM)
- 調適型安全裝置(ASA)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

常用技術術語

FTD：Firepower威脅防禦

FTD是次世代防火牆，提供超越傳統防火牆的更多功能。它包括入侵防禦系統(IPS)、高級惡意軟體防護(AMP)、URL過濾、安全情報等服務。FTD與ASA（調適型安全裝置）非常類似，但具有附加功能。FTD在2個引擎上執行，LINA和SNORT。

LINA：基於Linux的整合網路架構

我們將ASA稱為FTD裝置中的Lina。LINA只是FTD執行的ASA程式碼。Lina的主要重點是網路層安全。它確實透過其應用檢測和控制功能整合了一些第7層防火牆功能。

SNORT

Snort引擎是網路入侵檢測和防禦系統。Snort的主要功能包括辨識異常的資料包檢測、基於規則的檢測、即時警報、日誌記錄和分析，以及與其他安全工具的整合。Snort能夠執行L7檢測（應用層流量），不僅基於資料包報頭，還基於資料包的內容。

您可以靈活地編寫自己的自定義規則，以在應用層定義特定的模式或簽名，從而增強檢測功能。它透過評估資料包的負載來執行深度資料包檢測。您甚至可以在此處執行加密資料包的解密。

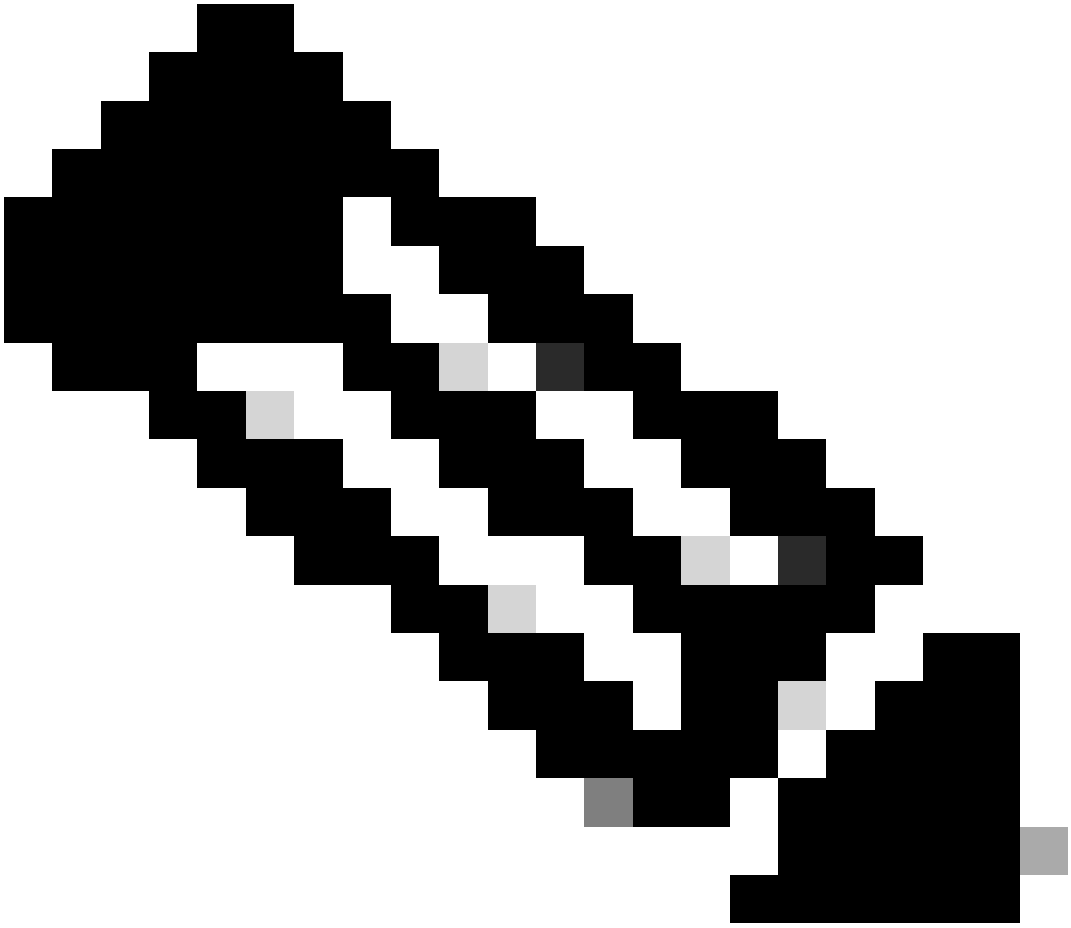
FXOS： Firepower可擴展作業系統

它是FTD裝置執行的作業系統。根據FXOS用於配置功能、監控機箱狀態和訪問高級故障排除功能的平台。

Firepower 4100/9300和Firepower 2100上的FXOS以及平台模式下的自適應安全裝置軟體允許配置更改，而在其他平台中，除特定功能外，FXOS是只讀的。

FCM：Firepower機箱管理器

FCM是用於管理機箱的GUI。它僅適用於在平台模式下運行ASA的9300、4100、2100。

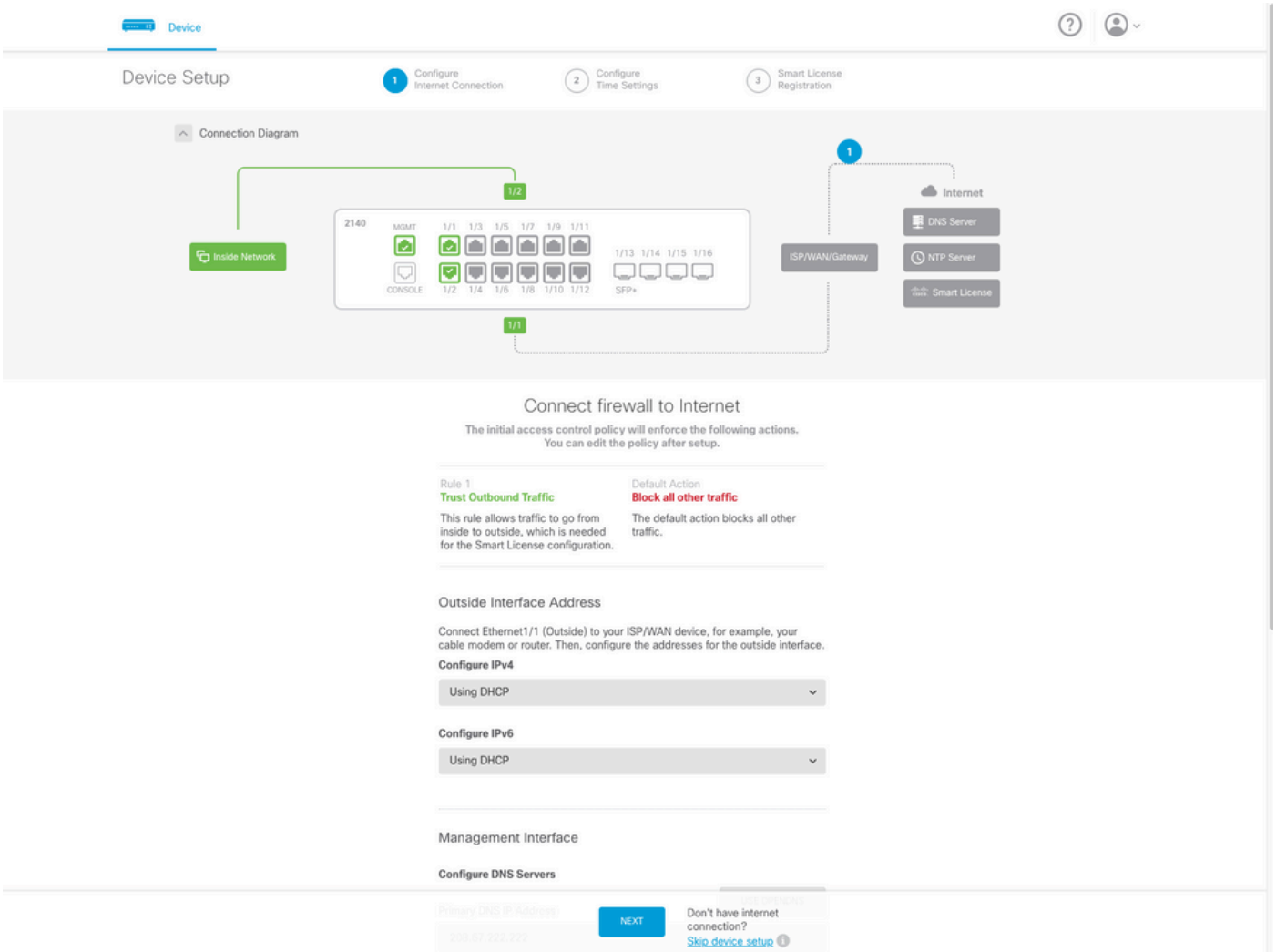


注意：您可以拿筆記型電腦來打個比方。FXOS是在機箱（筆記型電腦）上運行的作業系統（筆記型電腦中的Windows作業系統）。我們可以在其上安裝FTD（應用程式執行個體），其在Lina和Snort（元件）上執行。

與ASA不同，您無法通過CLI管理FTD。您需要單獨的基於GUI的管理。此類服務有兩種型別：FDM和FMC。

FDM：Firepower裝置管理

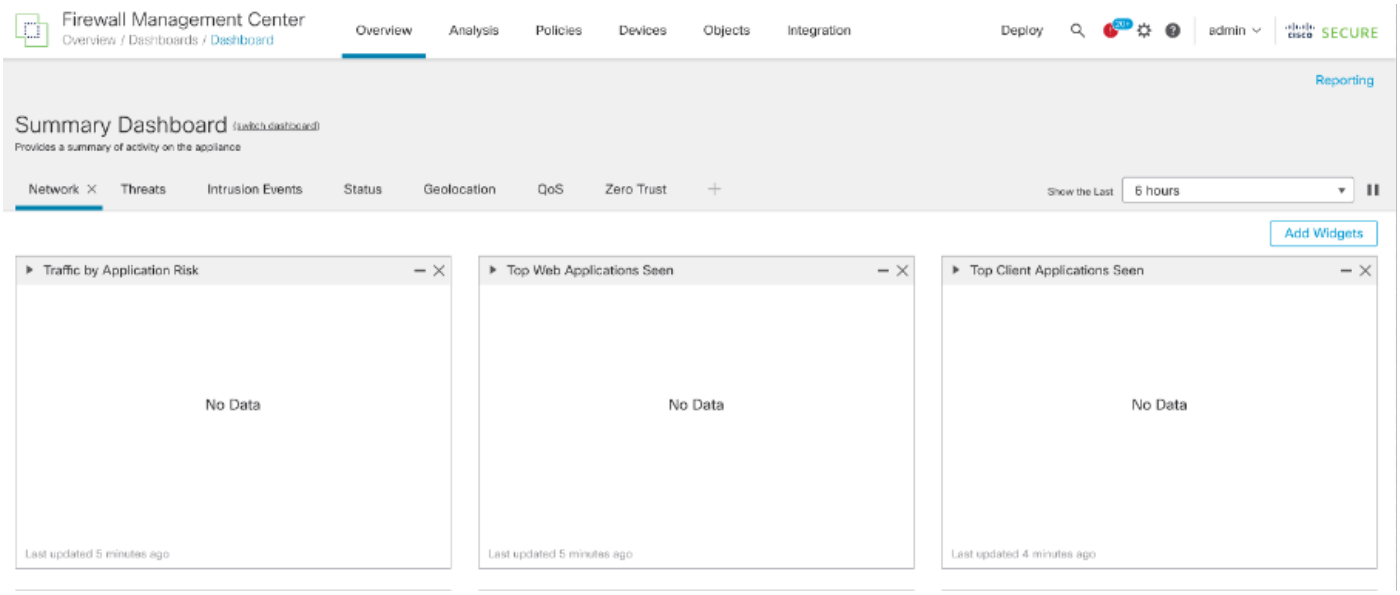
- FDM是機上管理工具。它提供了一個基於Web的介面，用於配置、管理和監控安全策略和系統設定。
- 使用FDM的一大優點是，您不需要額外的授權。
- 您只能使用1個FDM管理1個FTD。



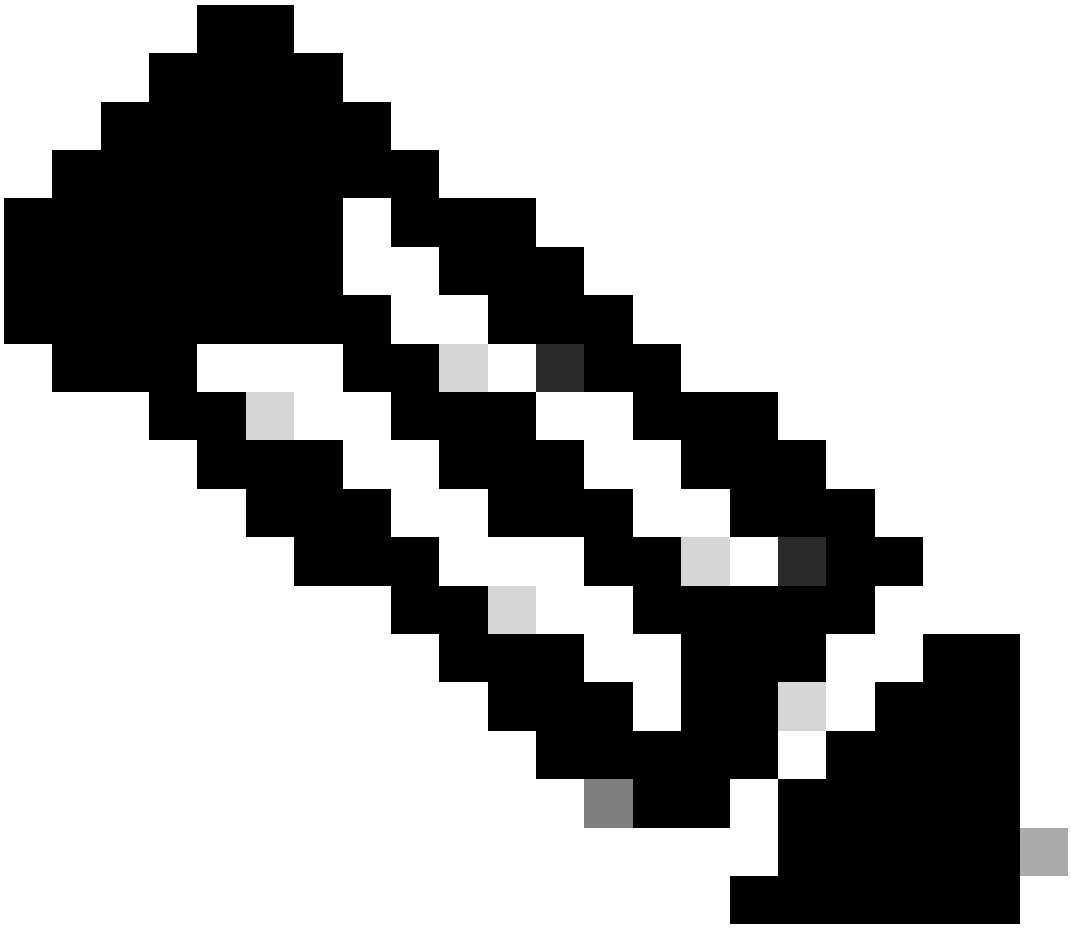
FDM

FMC：Firepower管理中心

- FMC是思科FTD裝置（具備Firepower服務的思科ASA裝置）的集中管理解決方案。此功能也提供可用於設定、管理及監控FTD裝置的GUI。
- 您可以使用硬體FMC裝置或虛擬FMC裝置。
- 這需要單獨的許可證才能運行。
- FMC的一個優點是您可以使用1個FMC裝置來管理多個FTD裝置。



FMC



附註：您無法同時使用FDM和FMC來管理FTD裝置。啟用FDM內建管理後，除非停用本機管理並將管理重新設定為使用FMC，否則無法使用FMC來管理FTD。另一方面，向FMC註

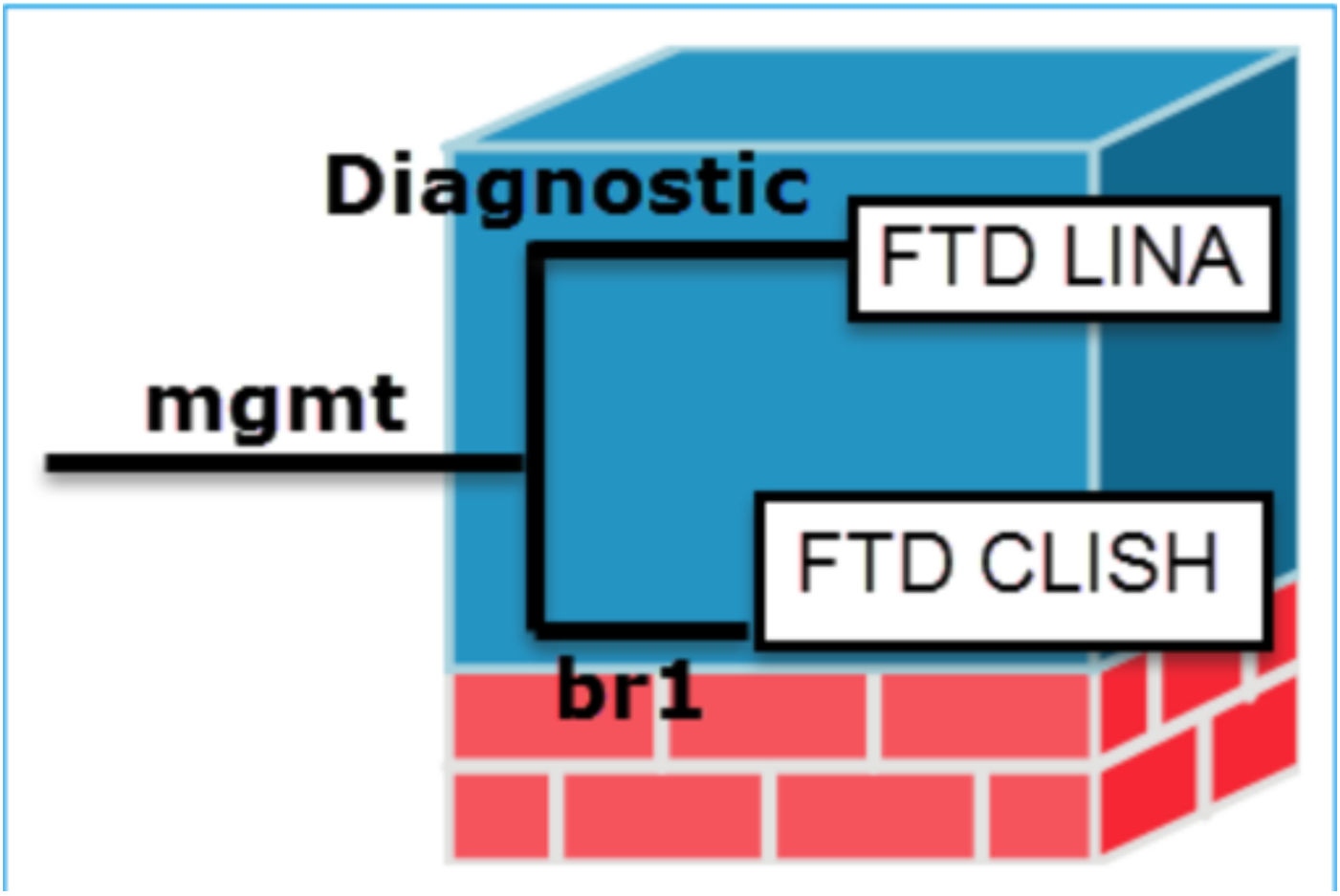
冊FTD會停用FTD上的FDM機上管理服務。

CLISH：指令行介面Shell

CLISH是Cisco Firepower威脅防禦(FTD)裝置中使用的命令列介面。您可以使用此CLISH模式在FTD上執行指令。

診斷管理

FTD裝置中有兩個管理介面、診斷管理介面和FTD管理介面。如果必須存取LINA引擎，則會使用診斷管理介面。如果必須存取SNORT引擎，則使用FTD管理介面。兩者都是不同的介面，需要不同的介面IP地址。



管理介面

ASA平台模式

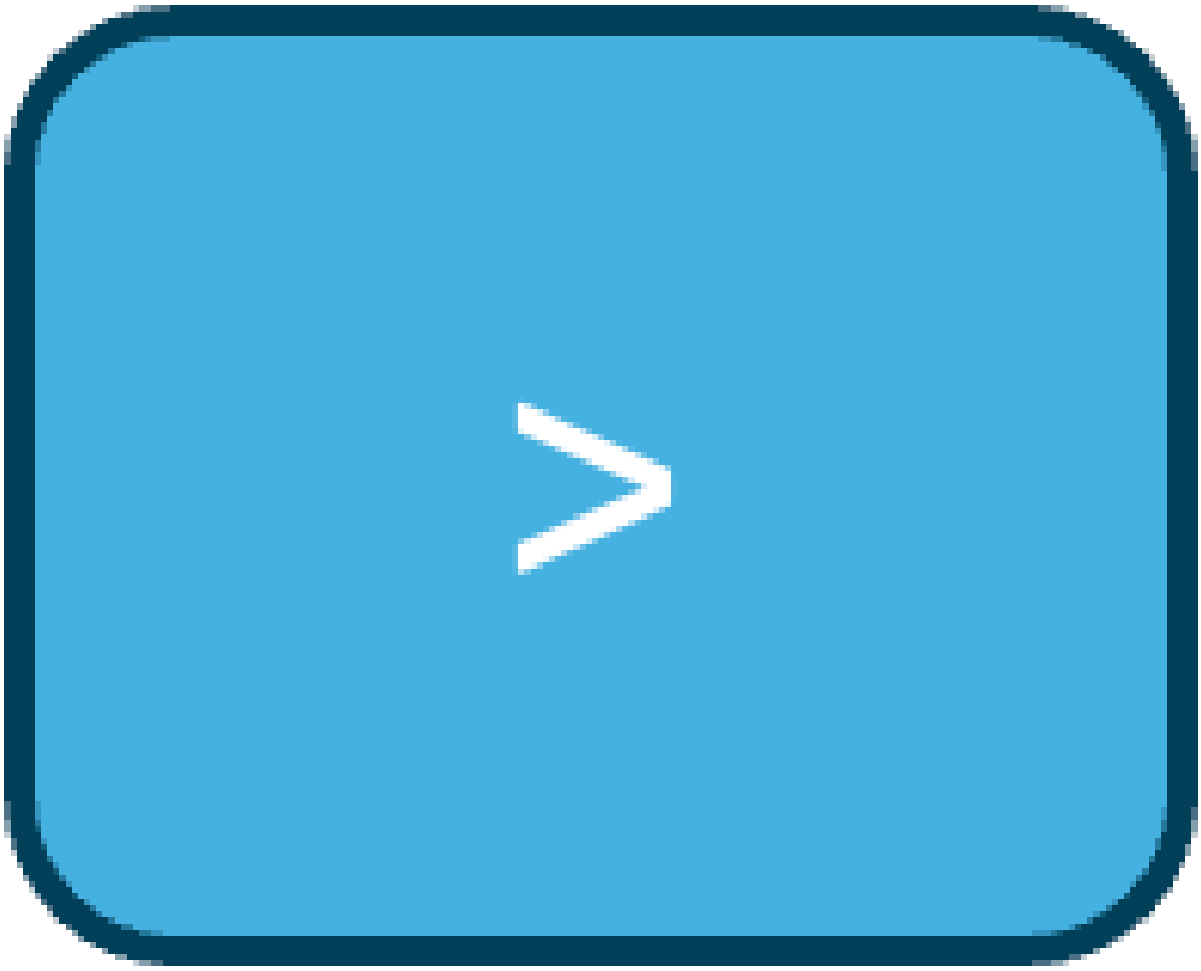
1. 在Platform模式下，您必須在FXOS中配置基本操作引數和硬體介面設定，例如啟用介面、建立EtherChannel、NTP、映像管理等。
2. 所有其他配置必須透過ASA CLI/ASDM完成。
3. 您擁有FCM存取權。

ASA裝置模式

1. 在Firepower 2100中，從第9.13（包括）版開始引入裝置模式下的ASA。
2. 裝置模式允許您配置ASA中的所有設定。FXOS CLI僅提供高級故障排除命令。
3. 此模式中沒有FCM。

FTD上的不同提示

CLISH



CLISH

根模式/專家模式

專家模式

Lina模式

Lina模式

FXOS模式

FXOS模式

如何在不同的提示之間移動

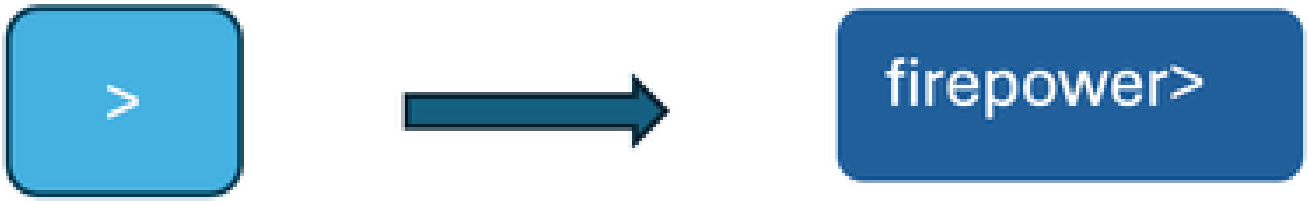
CLISH模式至FTD根模式

將模式更改為專家模式

```
> expert
```

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

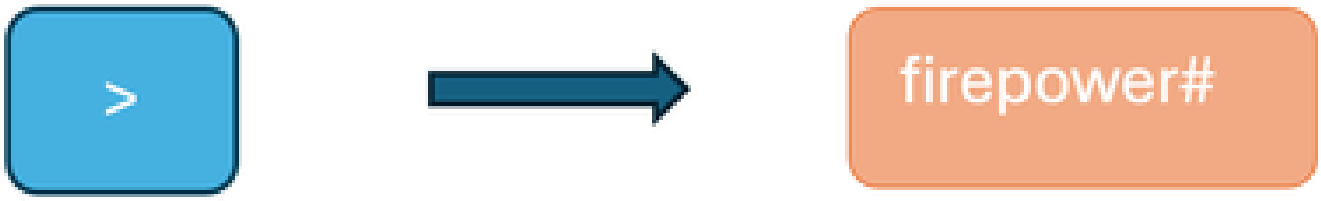
CLISH模式至Lina模式



將模式複製到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



關閉模式至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

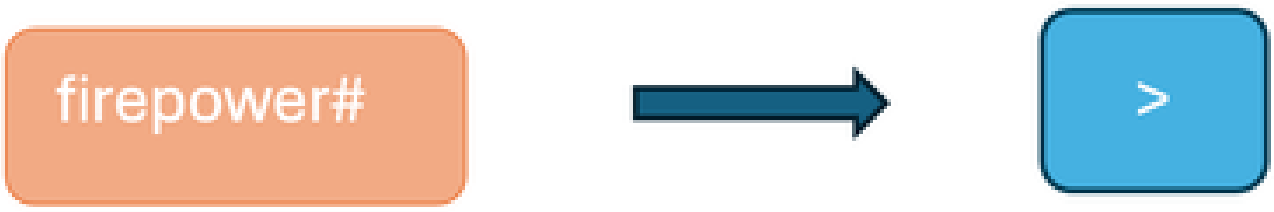
Lina模式的專家

```
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系列裝置）



FXOS轉為清潔模式

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

FXOS至FTD CLISH模式（4100/9300系列裝置）

此示例顯示如何連線到模組1上的威脅防禦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
>
```

退出控制檯：

輸入~，然後輸入quit退出Telnet應用程式。

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

相關檔案

有關可在firepower裝置上運行的各種命令的詳細資訊，請參閱FXOS命令參考(FTD命令參考)。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。