Decode Secure Firewall Terminology (For People New to Firepower)

Contents

Introduction

This document describes different popular Cisco Firewall Jargons. This document also covers a way on how you can move from one CLI mode to another.

Prerequisites

Requirements

There are no prior requirements to learn this topic.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Cisco Firepower Device Management (FDM)
- Firepower Extensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- Adaptive Security Appliance (ASA)

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. If your network is live, ensure that you understand the potential impact of any command.

Commonly Used Technical Terminologies

FTD: Firepower Threat Defence

FTD is a Next-Generation firewall which offers more beyond traditional firewalls. It includes services like Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), URL Filtering, Security Intelligence and so on. FTD is very similar to ASA (Adaptive Security Appliance) but with added functionality. FTD runs on 2 engines, LINA and SNORT.

LINA: Linux-based Integrated Network Architecture

We refer ASA as Lina in FTD devices. LINA is nothing but simply a ASA code that FTD runs on. Lina has its primary focus on Network layer security. It does incorporate some Layer 7 firewall capabilities through its application inspection and control features.

SNORT

Snort engine is network intrusion detection and prevention system. Key features of snort includes Packet Inspection to identify anomalies in them, Rule-Based Detection, Real-Time Alerts, Logging and analysis and Integration with other security tools. Snort has ability to perform L7 inspection (application layer traffic), not just based on a packet header but also content of the packets.

You get the flexibility to write your own custom rules to define specific patterns or signatures at application layer, which enhances the detection capabilities. It does deep packet inspection by evaluating the payload of the packets. You can even perform the decryption of the encrypted packets here.

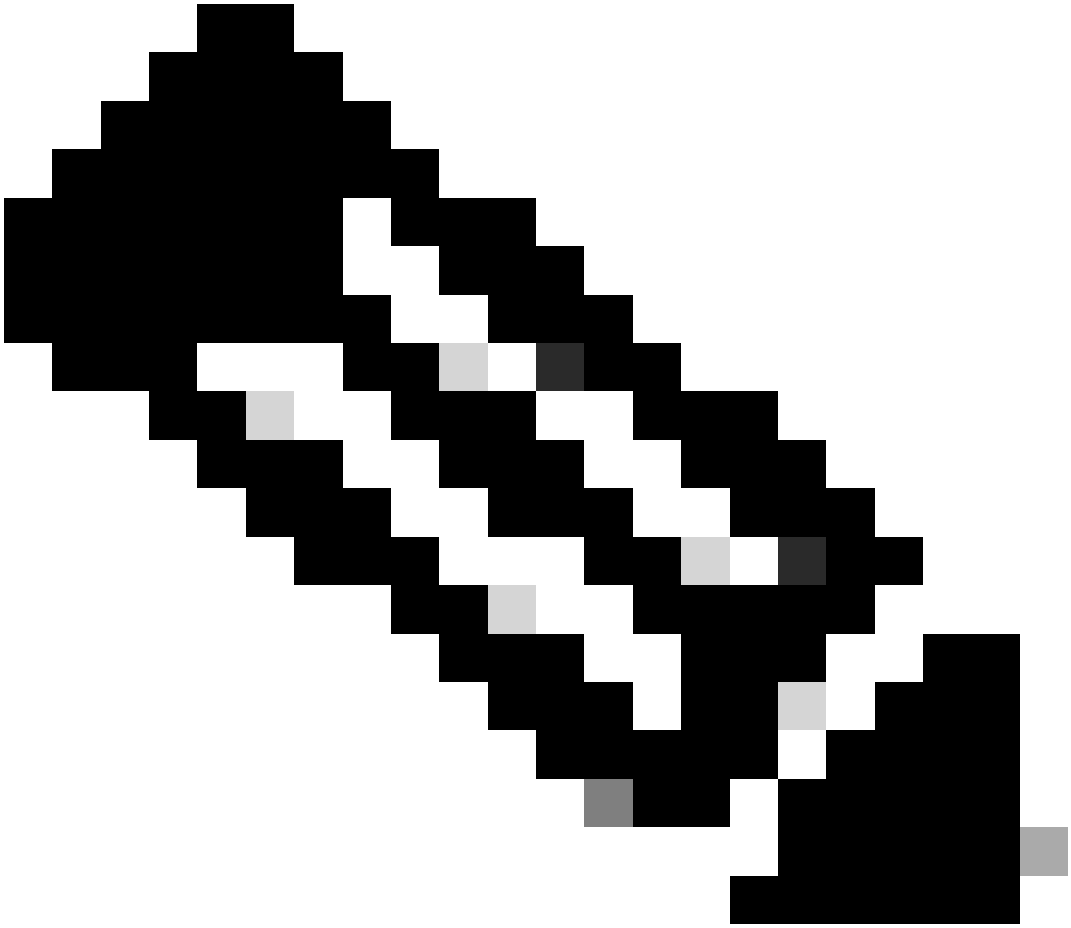
FXOS: Firepower Extensible Operating System

It is an operating system on which FTD device runs. Depending on the platforms FXOS is used to configure features, monitoring chassis status, and accessing advanced troubleshooting features.

FXOS on Firepower 4100/9300 and Firepower 2100 with the Adaptive Secure Appliance software in platform mode allow configuration changes, while in other platforms with the exception of specific features it is read only.

FCM: Firepower Chassis Manager

FCM is a GUI used to manage Chassis. It is only available for 9300, 4100, 2100 running ASA in Platform mode.

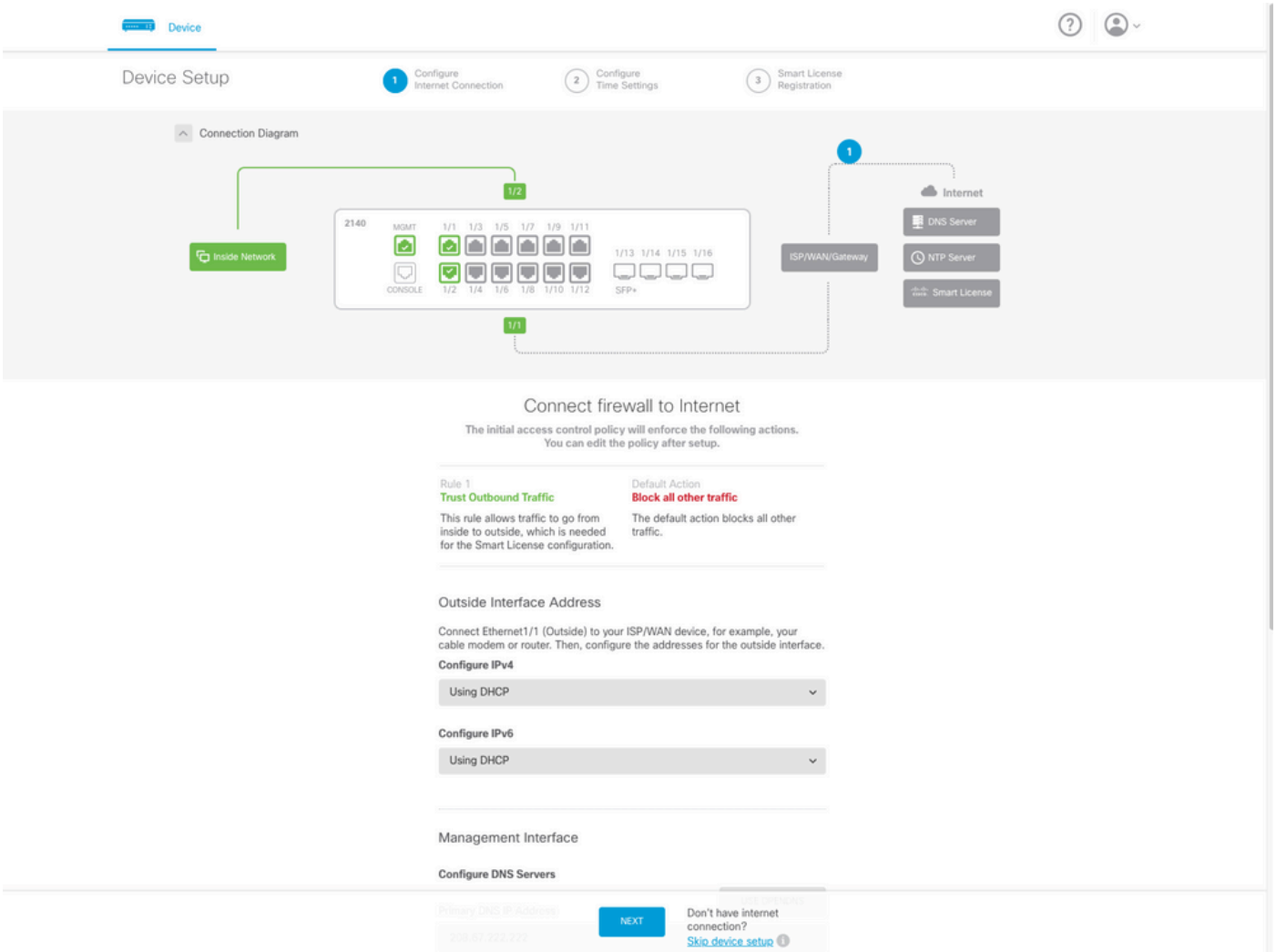


> **Note**: You can take an analogy of a laptop. FXOS is Operating System (Windows OS in laptop), which runs on chassis (laptop). We can install FTD (application instance) on it, which runs on Lina and Snort (components).

Unlike ASA, you cannot manage FTD via CLI. You need an separate GUI based management. There are 2 types of such services which exist : FDM and FMC.

FDM: Firepower Device Management

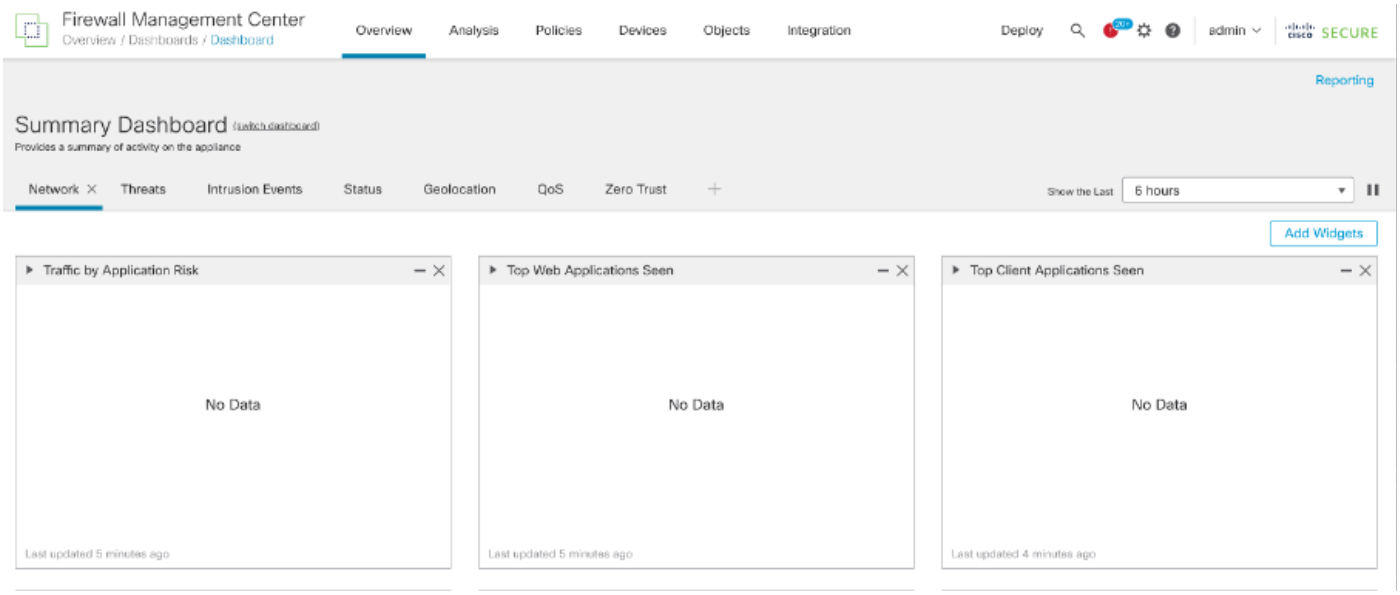
- FDM is a On-box management tool. It provides a web-based interface for configuring, managing and monitoring security policies and system settings.
- One big advantage of using FDM is that you do not an extra license for this.
- You can only manage 1 FTD with 1 FDM.



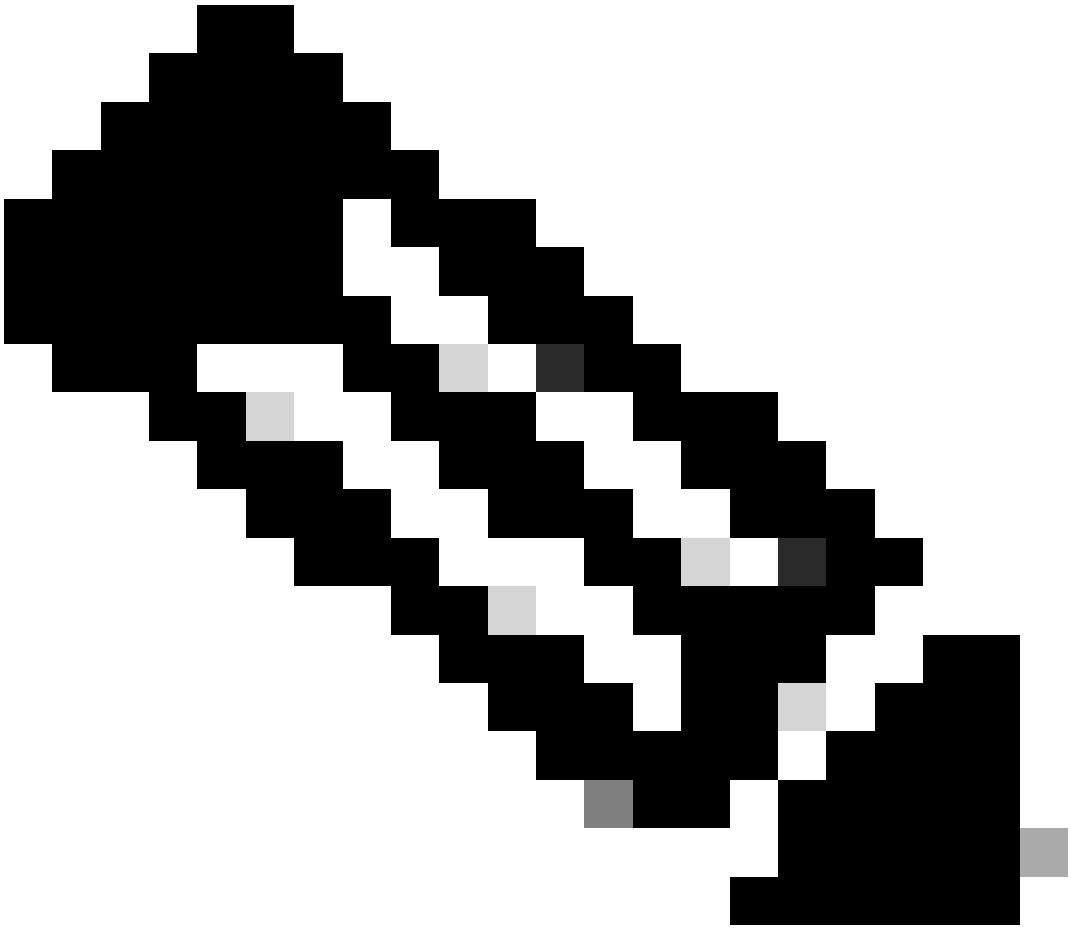
FDM

FMC: Firepower Management Center

- FMC is a centralized management solution for Cisco FTD devices, Cisco ASA devices with Firepower Services. It also provides you with GUI which you can use to configure, manage and monitor FTD devices.
- You can use a hardware FMC device or a virtual FMC device.
- This requires a separate license to function.
- One plus point of FMC is you can manage multiple FTD devices with 1 FMC device.



FMC



Note: You cannot use both the FDM and FMC to manage an FTD device. Once the FDM On-Box management is enabled, it is not possible to use an FMC to manage the FTD, unless you disable the

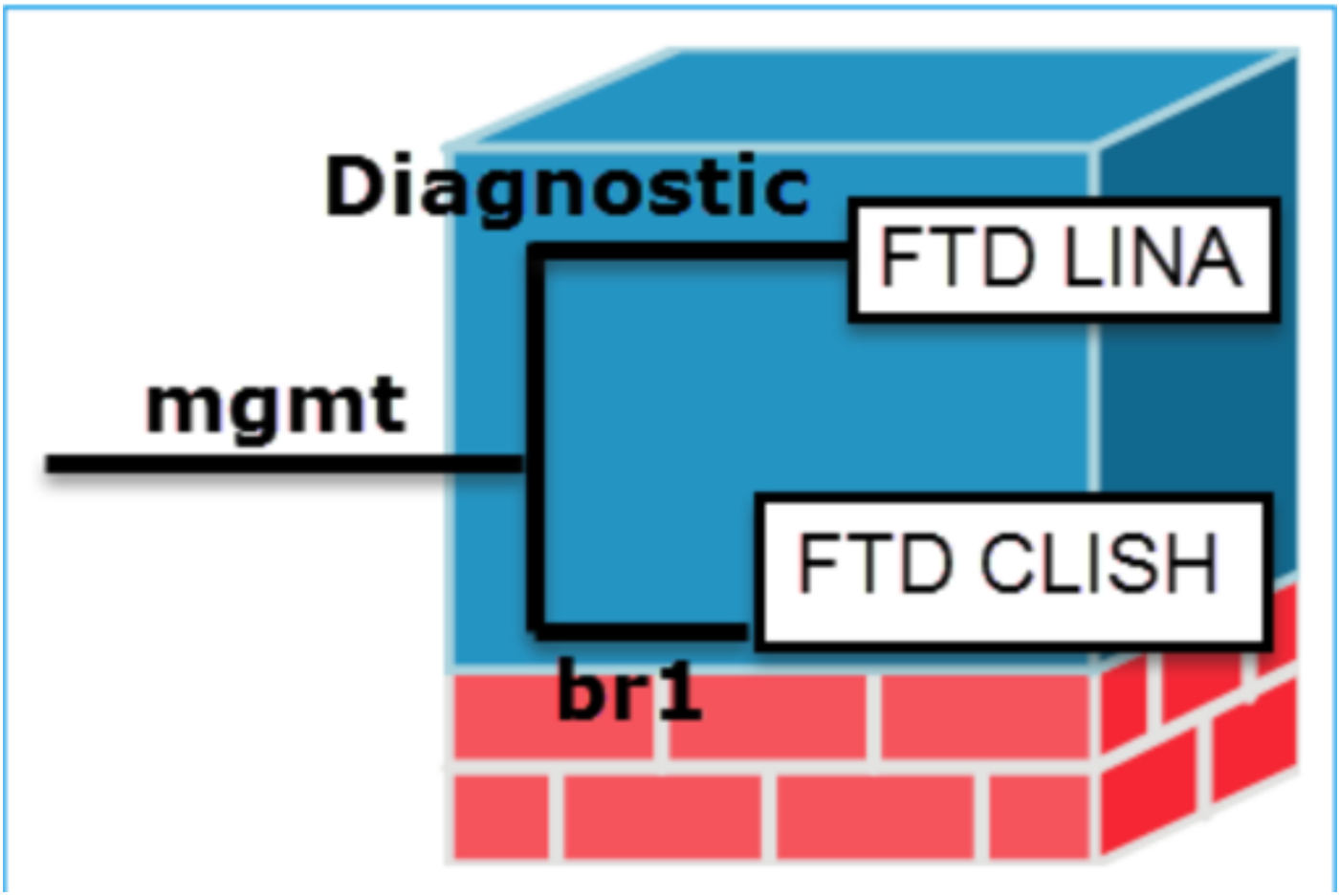
local management and re-configure the management to use an FMC. On the other hand, register the FTD to an FMC disables the FDM On-Box management service on the FTD.

CLISH: Command Line Interface Shell

CLISH is command-line interface used in Cisco Firepower Threat Defense (FTD) devices. You can run commands on FTD using this CLISH mode.

DIAGNOSTIC MANAGEMENT

We have 2 management interfaces in FTD device, Diagnostic management interface and FTD management interface. If we have to access LINA engine, we use diagnostic management interface. If we have to access SNORT engine, we use FTD management interface. Both are different interfaces and need different interface IP addresses.



Management Interfaces

ASA Platform Mode

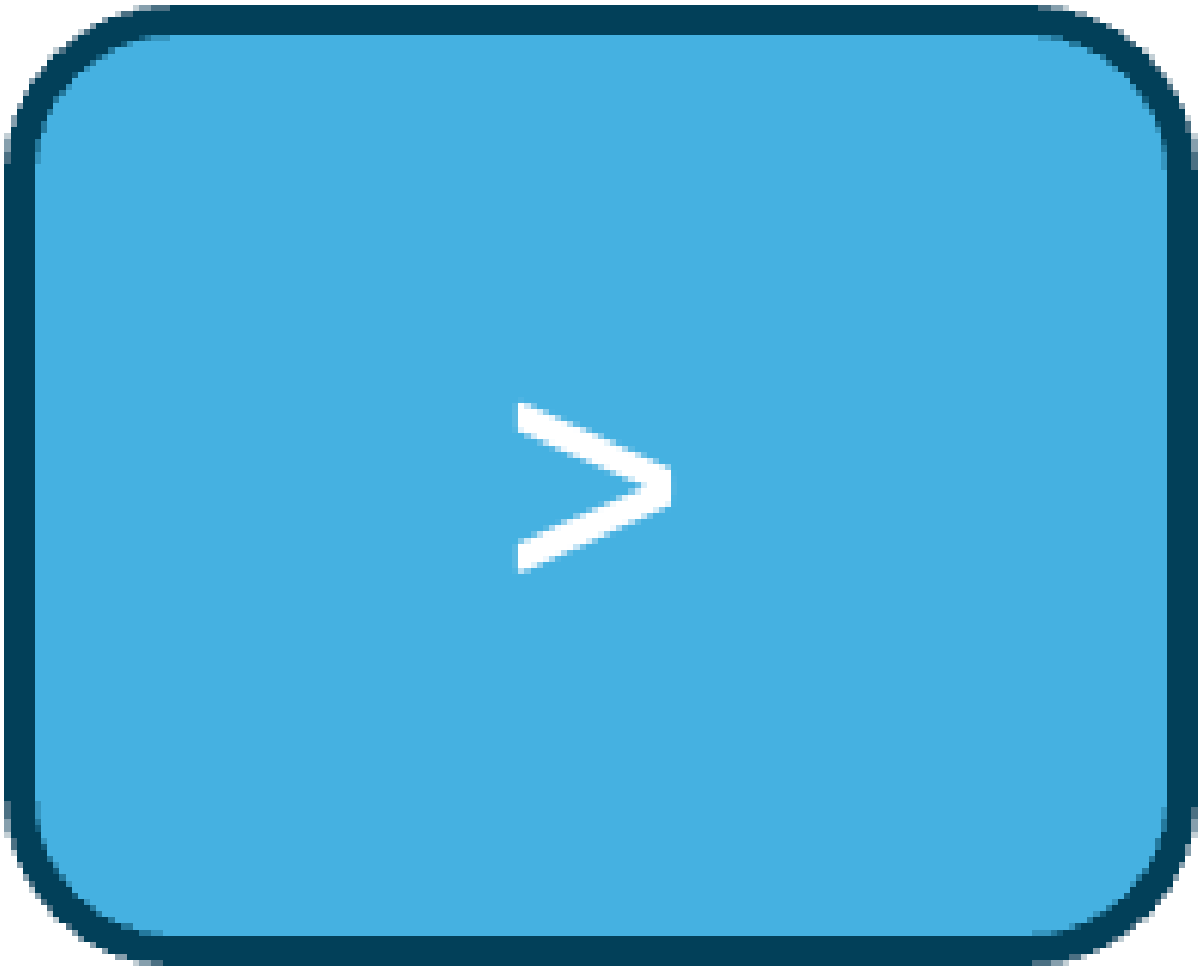
1. When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS like enabling interfaces, establishing EtherChannels, NTP, image management, and more.
2. All other configurations has to be done through ASA CLI / ASDM.
3. You have FCM access in this.

ASA Appliance Mode

1. In Firepower 2100, ASA in appliance mode was introduced 9.13(including) onwards.
2. Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
3. There is no FCM in this mode.

Different Prompts on FTD

CLISH



CLISH

Root Mode / Expert Mode

Expert Mode

Lina Mode

Lina Mode

FXOS Mode

FXOS Mode

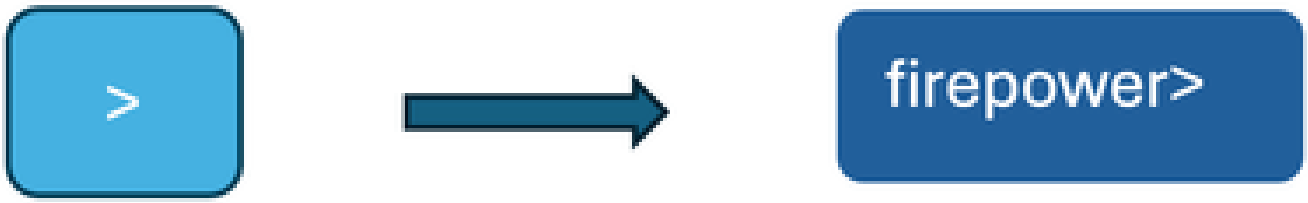
How To Move Between Different Prompts

CLISH Mode to FTD Root Mode

Clish Mode to Expert Mode

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

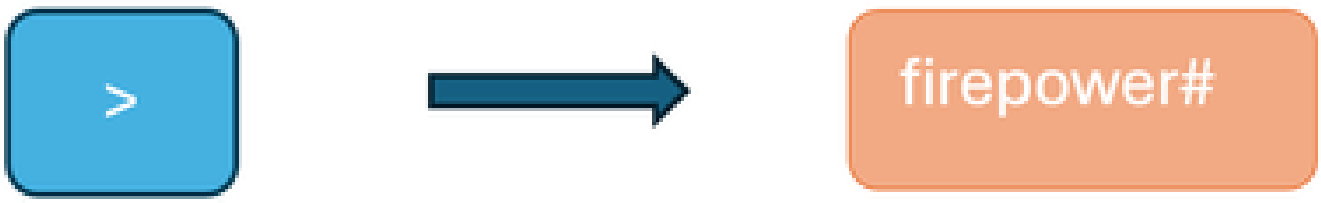
CLISH Mode to Lina Mode



Clish Mode to Lina Mode

```
> 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 Mode to FXOS Mode



Clish Mode to FXOS mode

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

Root Mode to LINA Mode

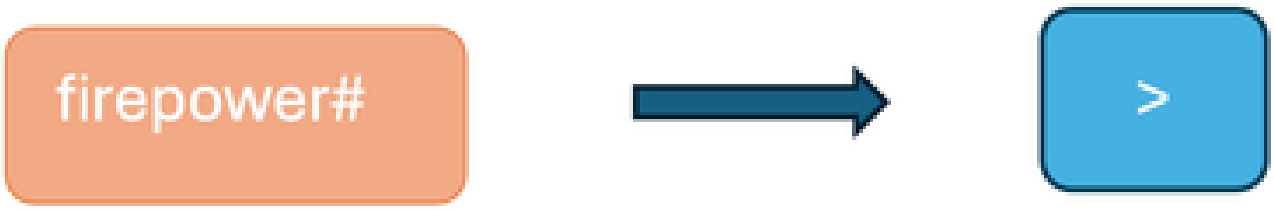
Expert to Lina Mode

```
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#
```

or

```
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 to FTD CLISH Mode (1000/2100/3100 Series Device)



FXOS to Clish Mode

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

FXOS to FTD CLISH Mode (4100/9300 Series Device)

This example shows how to connect to the threat defense CLI on module 1:

```
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
>
```

Exit the console:

Enter **~**, then **quit** to exit the Telnet application.

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

Related Documents

For more information on various commands that you can run on firepower devices, please refer to FXOS Command Reference , FTD command reference .