Dekodieren Sie die sichere Terminologie der Firewall (für Personen ohne FirePOWER).

Inhalt

Einleitung

In diesem Dokument werden verschiedene gängige Cisco Firewall-Jargon beschrieben. In diesem Dokument wird auch beschrieben, wie Sie von einem CLI-Modus in einen anderen wechseln können.

Voraussetzungen

Anforderungen

Es gibt keine vorherigen Voraussetzungen, um dieses Thema zu lernen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco FirePOWER-Gerätemanagement (FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- Adaptive Security Appliance (ASA)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Gebräuchliche technische Terminologien

FTD: Firepower Threat Defense

FTD ist eine Firewall der nächsten Generation, die mehr bietet als herkömmliche Firewalls. Dazu gehören Services wie Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), URL-Filterung, Sicherheitsinformationen usw. FTD ähnelt stark der ASA (Adaptive Security Appliance), bietet jedoch zusätzliche Funktionen. FTD läuft auf 2 Engines, LINA und SNORT.

LINA: Linux-basierte integrierte Netzwerkarchitektur

In FTD-Geräten nennen wir ASA Lina. LINA ist nichts weiter als ein ASA-Code, auf dem FTD läuft. Lina legt den Schwerpunkt auf die Sicherheit auf der Netzwerkschicht. Es umfasst einige Layer-7-Firewall-Funktionen, die über die Funktionen zur Anwendungsinspektion und -kontrolle bereitgestellt werden.

SNORT

Die Snort Engine ist ein System zur Erkennung und Verhinderung von Netzwerkzugriffen. Zu den wichtigsten Funktionen von Snort gehören die Paketprüfung, um darin enthaltene Anomalien zu identifizieren, die regelbasierte Erkennung, Echtzeitwarnungen, Protokollierung und Analyse sowie die Integration in andere Sicherheitstools. Snort kann eine L7-Prüfung (Datenverkehr auf Anwendungsebene) durchführen, die nicht nur auf einem Paket-Header, sondern auch auf dem Inhalt der Pakete basiert.

Sie erhalten die Flexibilität, eigene benutzerdefinierte Regeln zu schreiben, um bestimmte Muster oder Signaturen auf Anwendungsebene zu definieren, was die Erkennungsfunktionen verbessert. Es führt eine Deep Packet Inspection durch, indem es die Nutzlast der Pakete auswertet. Hier

können Sie sogar die Entschlüsselung der verschlüsselten Pakete durchführen.

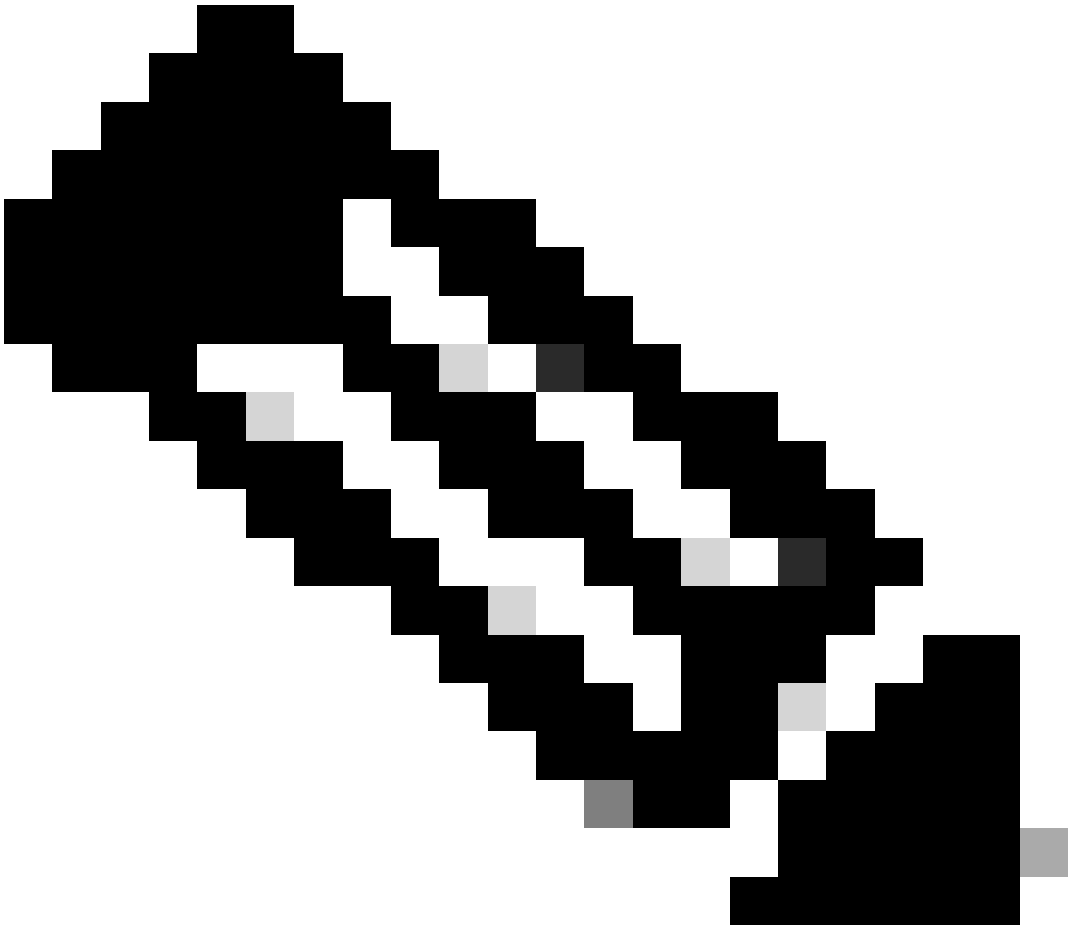
FXOS: erweiterbares FirePOWER-Betriebssystem

Es ist ein Betriebssystem, auf dem FTD-Gerät läuft. Je nach Plattform wird FXOS verwendet, um Funktionen zu konfigurieren, den Chassis-Status zu überwachen und auf erweiterte Funktionen zur Fehlerbehebung zuzugreifen.

FXOS auf Firepower 4100/9300 und Firepower 2100 mit der Adaptive Secure Appliance Software im Plattformmodus ermöglichen Konfigurationsänderungen, während es auf anderen Plattformen mit Ausnahme bestimmter Funktionen schreibgeschützt ist.

FCM: FirePOWER-Chassis-Manager

FCM ist eine grafische Benutzeroberfläche zur Verwaltung von Chassis. Sie ist nur für die Router 9300, 4100 und 2100 verfügbar, die ASA im Plattformmodus ausführen.



Hinweis: Man kann eine Analogie von einem Laptop nehmen. FXOS ist Betriebssystem

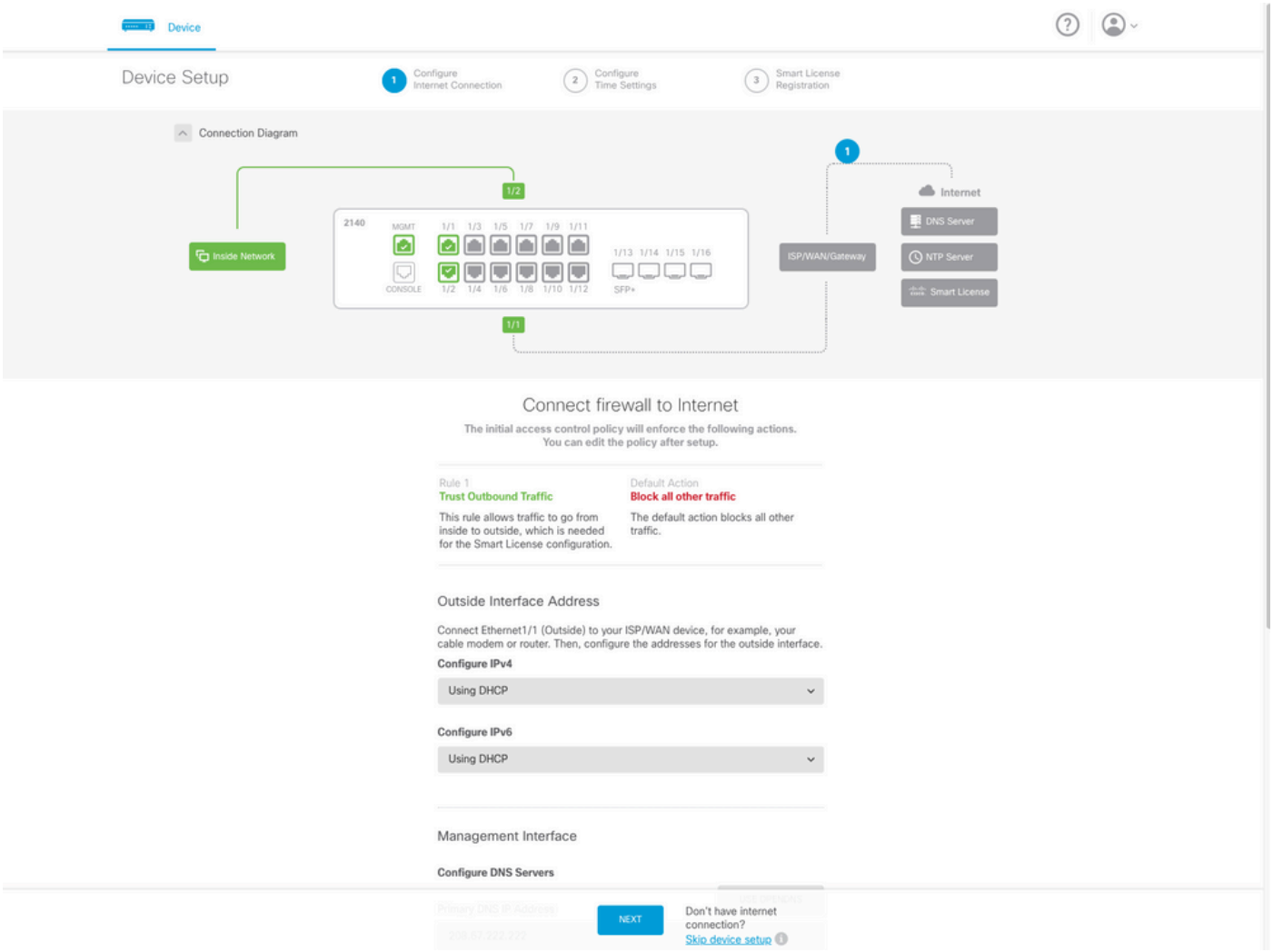
---

(Windows OS in Laptop), das auf Chassis (Laptop) läuft. Wir können FTD (Anwendungsinstanz) darauf installieren, die auf Lina und Snort (Komponenten) läuft.

Im Gegensatz zu ASA kann FTD nicht über die CLI verwaltet werden. Sie benötigen eine separate, GUI-basierte Verwaltung. Es gibt zwei Arten solcher Dienste: FDM und FMC.

FDM: FirePOWER-Gerätemanagement

- FDM ist ein integriertes Verwaltungstool. Es bietet eine webbasierte Schnittstelle zum Konfigurieren, Verwalten und Überwachen von Sicherheitsrichtlinien und Systemeinstellungen.
- Ein großer Vorteil von FDM ist, dass Sie dafür keine zusätzliche Lizenz erwerben.
- Sie können nur 1 FTD mit 1 FDM verwalten.

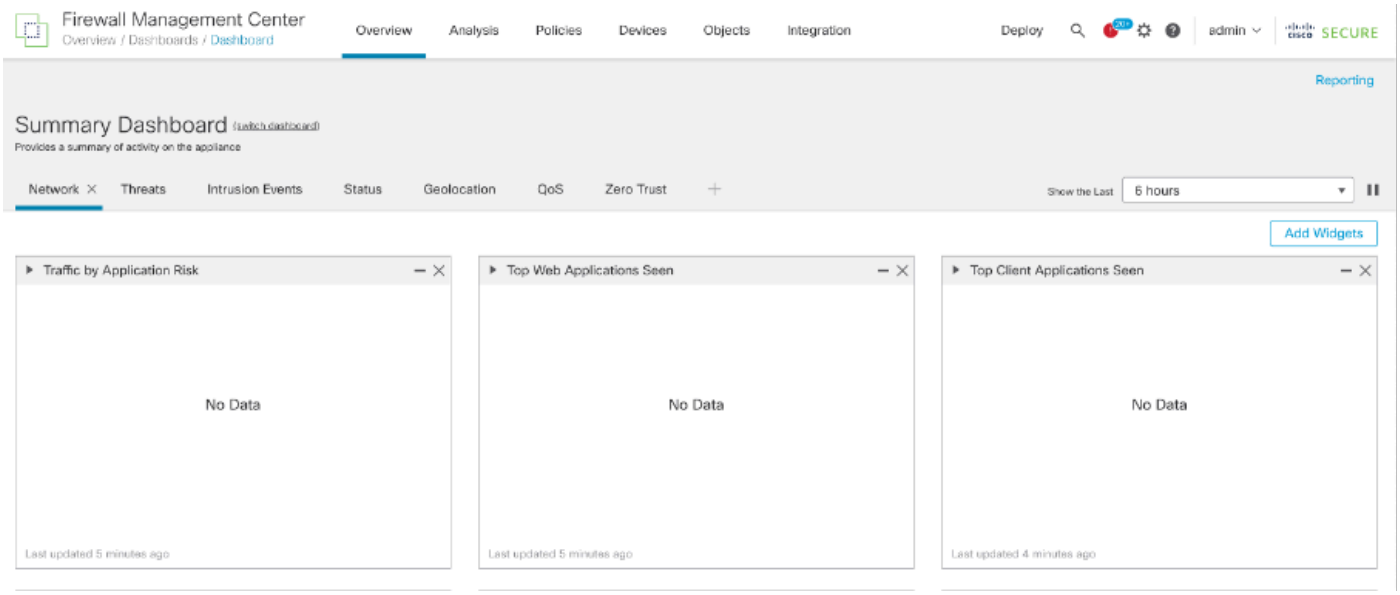


FDM

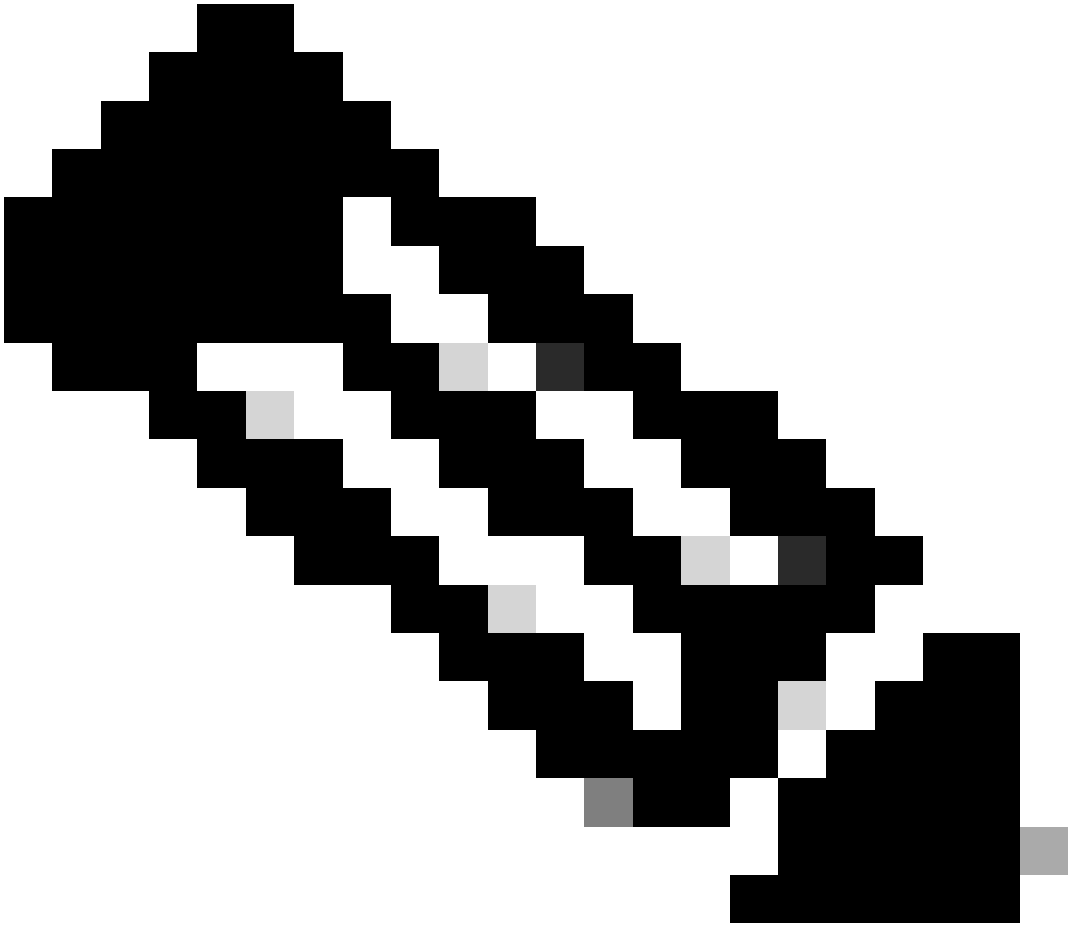
FMC: FirePOWER Management Center

- FMC ist eine zentralisierte Managementlösung für FTD-Geräte von Cisco, Cisco ASA-Geräte mit Firepower-Services. Darüber hinaus erhalten Sie eine Benutzeroberfläche, über die Sie FTD-Geräte konfigurieren, verwalten und überwachen können.

- Sie können ein Hardware-FMC-Gerät oder ein virtuelles FMC-Gerät verwenden.
- Hierfür ist eine separate Lizenz erforderlich.
- Ein Pluspunkt von FMC ist, dass Sie mehrere FTD-Geräte mit einem FMC-Gerät verwalten können.



FMC



Hinweis: Sie können FDM und FMC nicht zur Verwaltung eines FTD-Geräts verwenden. Sobald die FDM On-Box-Verwaltung aktiviert ist, kann die FTD nur noch von einem FMC verwaltet werden, wenn die lokale Verwaltung deaktiviert und die Verwaltung für die Verwendung eines FMC neu konfiguriert wird. Andererseits wird durch die Registrierung des FTD bei einem FMC der FDM On-Box-Managementservice auf dem FTD deaktiviert.

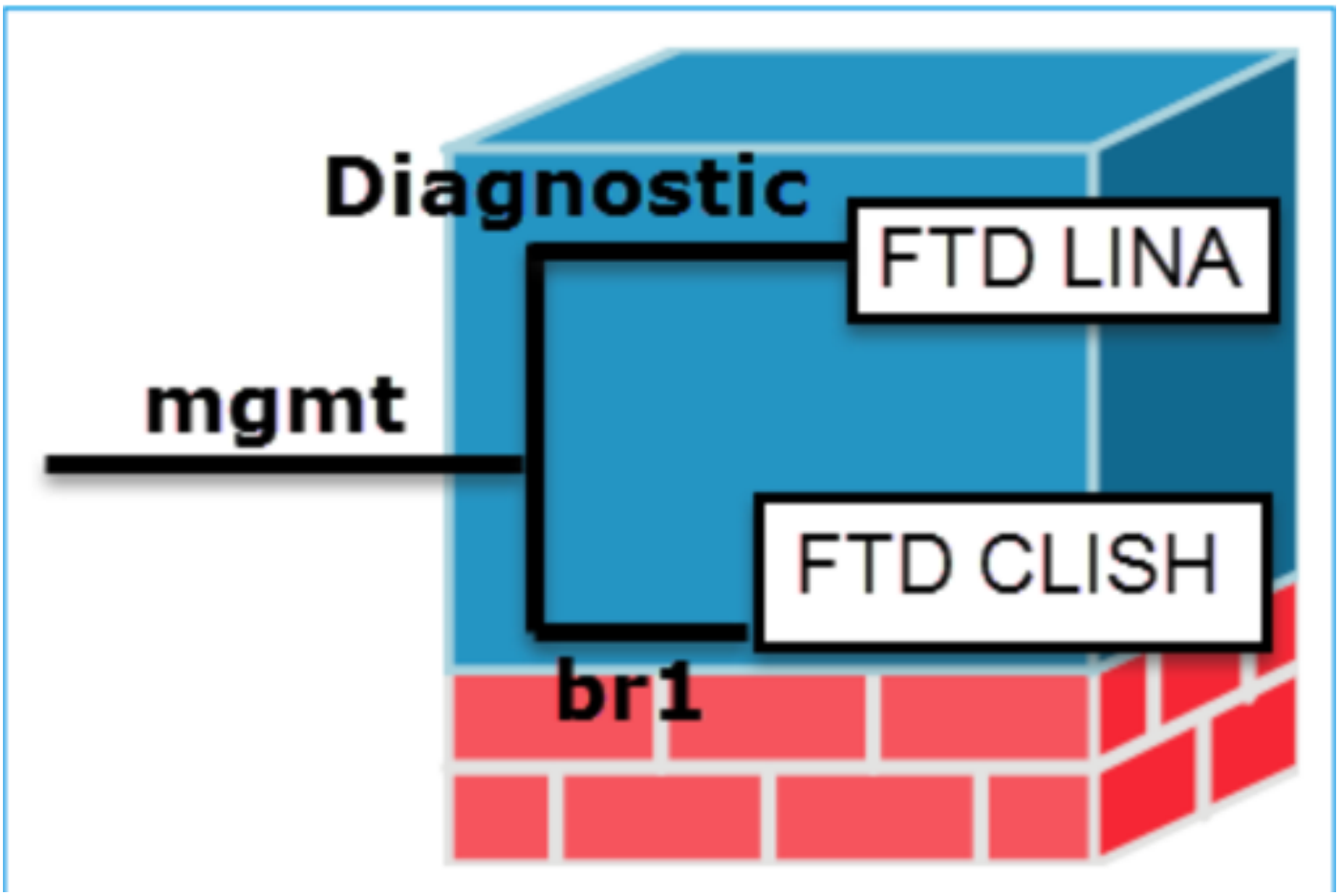
CLISH: Befehlszeilenschnittstellen-Shell

CLISH ist eine Befehlszeilenschnittstelle, die in Cisco FirePOWER Threat Defense (FTD)-Geräten verwendet wird. Sie können Befehle in FTD mit diesem CLISH-Modus ausführen.

DIAGNOSTISCHES MANAGEMENT

Wir haben 2 Management-Schnittstellen in FTD-Gerät, Diagnose-Management-Schnittstelle und FTD-Management-Schnittstelle. Wenn wir auf die LINA-Engine zugreifen müssen, verwenden wir eine Schnittstelle für das Diagnosemanagement. Wenn wir auf die SNORT-Engine zugreifen müssen, verwenden wir die FTD-Management-Schnittstelle. Beide Schnittstellen benötigen

unterschiedliche IP-Adressen.



Management-Schnittstellen

ASA-Plattformmodus

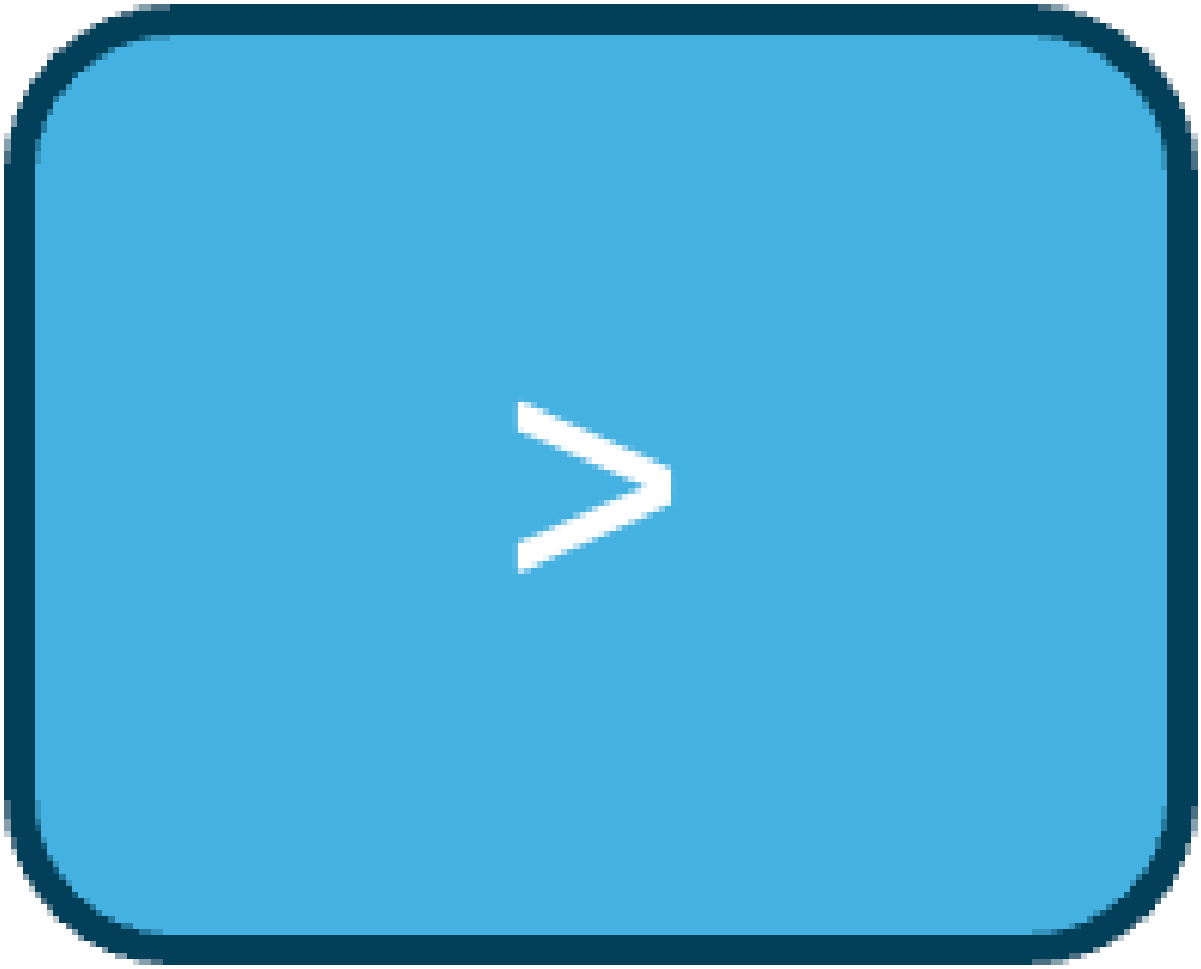
1. Im Plattformmodus müssen Sie grundlegende Betriebsparameter und Einstellungen für die Hardware-Schnittstelle in FXOS konfigurieren, z. B. Schnittstellen aktivieren, EtherChannels einrichten, NTP, Image-Management usw.
2. Alle anderen Konfigurationen müssen über ASA CLI/ASDM erfolgen.
3. Hier haben Sie Zugriff auf den FCM.

ASA Appliance-Modus

1. In Firepower 2100 wurde die ASA im Appliance-Modus 9.13(einschl.) eingeführt.
2. Im Appliance-Modus können Sie alle Einstellungen in der ASA konfigurieren. Nur Befehle zur erweiterten Fehlerbehebung sind über die FXOS-CLI verfügbar.
3. In diesem Modus ist kein FCM vorhanden.

Verschiedene Aufforderungen auf FTD

CLISH



CLISH

Stammmodus/Expertenmodus

Expertenmodus

Lina Mode

Lina Mode

FXOS-Modus

FXOS-Modus

Wechseln zwischen verschiedenen Aufforderungen

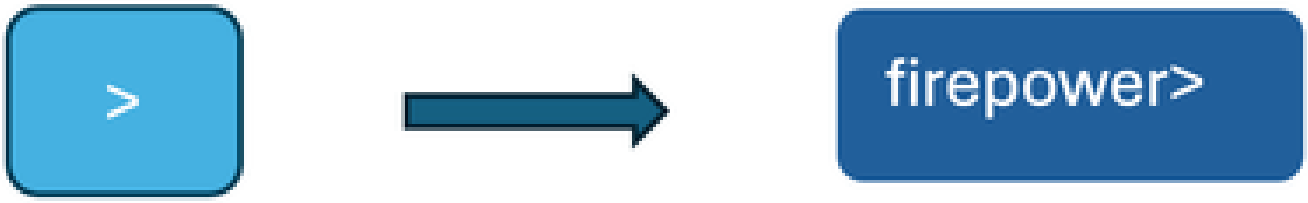
CLISH-Modus in FTD-Root-Modus

Clish-Modus in Expertenmodus

```
> expert
```

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

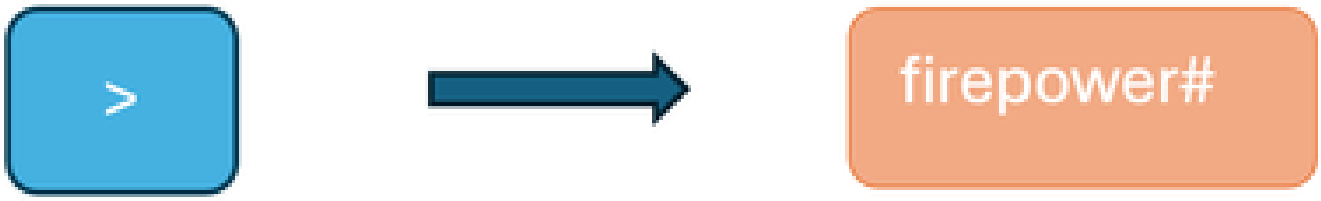
CLISH-Modus in Lina-Modus



Clipmodus in Lina-Modus

```
> 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-Modus in FXOS-Modus



Clickmodus in FXOS-Modus

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

Root-Modus in LINA-Modus

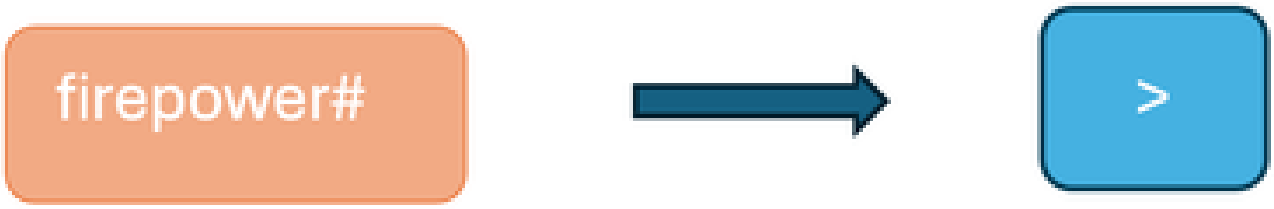
Experte für Lina Mode

```
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#
```

Oder

```
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 auf FTD CLISH Mode (Gerät der Serie 1000/2100/3100)



FXOS in Clickmodus

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

FXOS auf FTD CLISH Mode (Gerät der Serie 4100/9300)

Dieses Beispiel zeigt, wie Sie eine Verbindung mit der Threat Defence-CLI in Modul 1 herstellen:

```
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
>
```

Verlassen Sie die -Konsole:

Geben Sie ~ ein, und beenden Sie die Telnet-Anwendung.

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

Verwandte Dokumente

Weitere Informationen zu verschiedenen Befehlen, die Sie auf Firepower-Geräten ausführen können, finden Sie unter FXOS-Befehlsreferenz , FTD-Befehlsreferenz .

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.