セキュアファイアウォールの用語のデコード（Firepowerを初めて使用するユーザ向け）

内容

はじめに

このドキュメントでは、さまざまな一般的なCisco Firewall Jargonsについて説明します。また、あるCLIモードから別のCLIモードに移行する方法についても説明します。

前提条件

要件

このトピックについて学習するための前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Firepower Threat Defense(FTD)
- Cisco Firepowerデバイス管理(FDM)
- Firepower eXtensible Operating System（FXOS）
- Firepower Chassis Manager（FCM）
- 適応型セキュリティ アプライアンス（ASA）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

一般的に使用される技術用語

FTD:Firepower Threat Defense（火力による脅威に対する防御）

FTDは、従来のファイアウォールを超えた機能を提供する次世代ファイアウォールです。侵入防御システム(IPS)、高度なマルウェア防御(AMP)、URLフィルタリング、セキュリティインテリジェンスなどのサービスが含まれます。FTDはASA（適応型セキュリティアプライアンス）と非常によく似ていますが、追加機能があります。FTDは、LINAとSNORTの2つのエンジンで動作します。

LINA:Linuxベースの統合ネットワークアーキテクチャ

FTDデバイスでは、ASAをLinaと呼びます。LINAは、FTDが実行される単なるASAコードです。Linaは主にネットワーク層のセキュリティに重点を置いています。アプリケーション検査および制御機能を通じて、一部のレイヤ7ファイアウォール機能が組み込まれています。

SNORT

Snortエンジンは、ネットワーク侵入検知/防御システムです。Snortの主な機能には、パケット検査による異常の特定、ルールベースの検出、リアルタイムアラート、ロギングと分析、および他のセキュリティツールとの統合などがあります。Snortには、パケットヘッダーだけでなく、パケットの内容に基づいてL7インスペクション（アプリケーション層トラフィック）を実行する機能があります。

アプリケーション層で特定のパターンやシグニチャを定義する独自のカスタムルールを柔軟に作成できるため、検出機能が強化されます。パケットのペイロードを評価することにより、ディープパケットインスペクションを実行する暗号化されたパケットの復号化もここで実行できます。

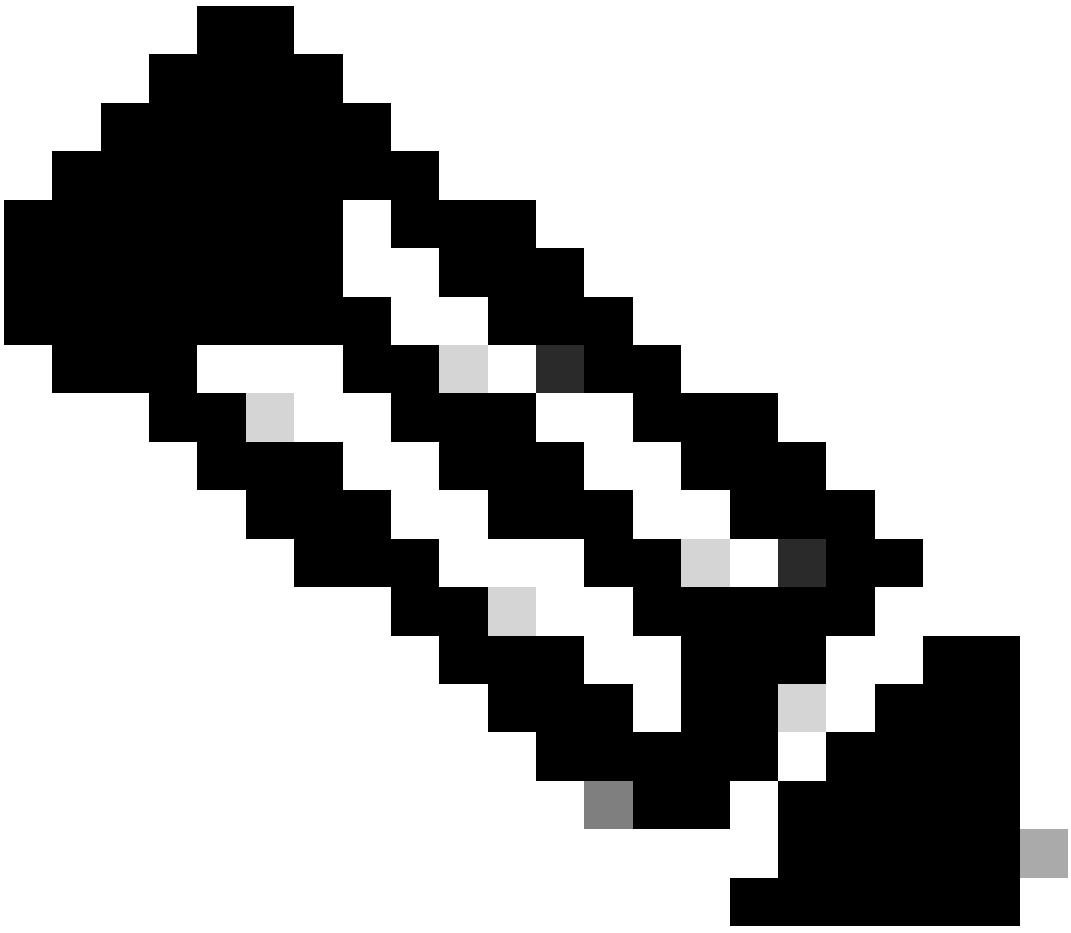
FXOS:Firepower Extensible Operating System

これは、FTDデバイスが稼働するオペレーティングシステムです。プラットフォームに応じて、FXOSを使用して機能を設定し、シャーシのステータスを監視し、高度なトラブルシューティング機能にアクセスします。

プラットフォームモードの適応型セキュアアプライアンスソフトウェアを搭載したFirepower 4100/9300およびFirepower 2100のFXOSでは設定の変更が可能ですが、特定の機能を除く他のプラットフォームでは読み取り専用です。

FCM:Firepowerシャーシマネージャ

FCMは、シャーシの管理に使用されるGUIです。プラットフォームモードでASAを実行する9300、4100、2100でのみ使用できます。



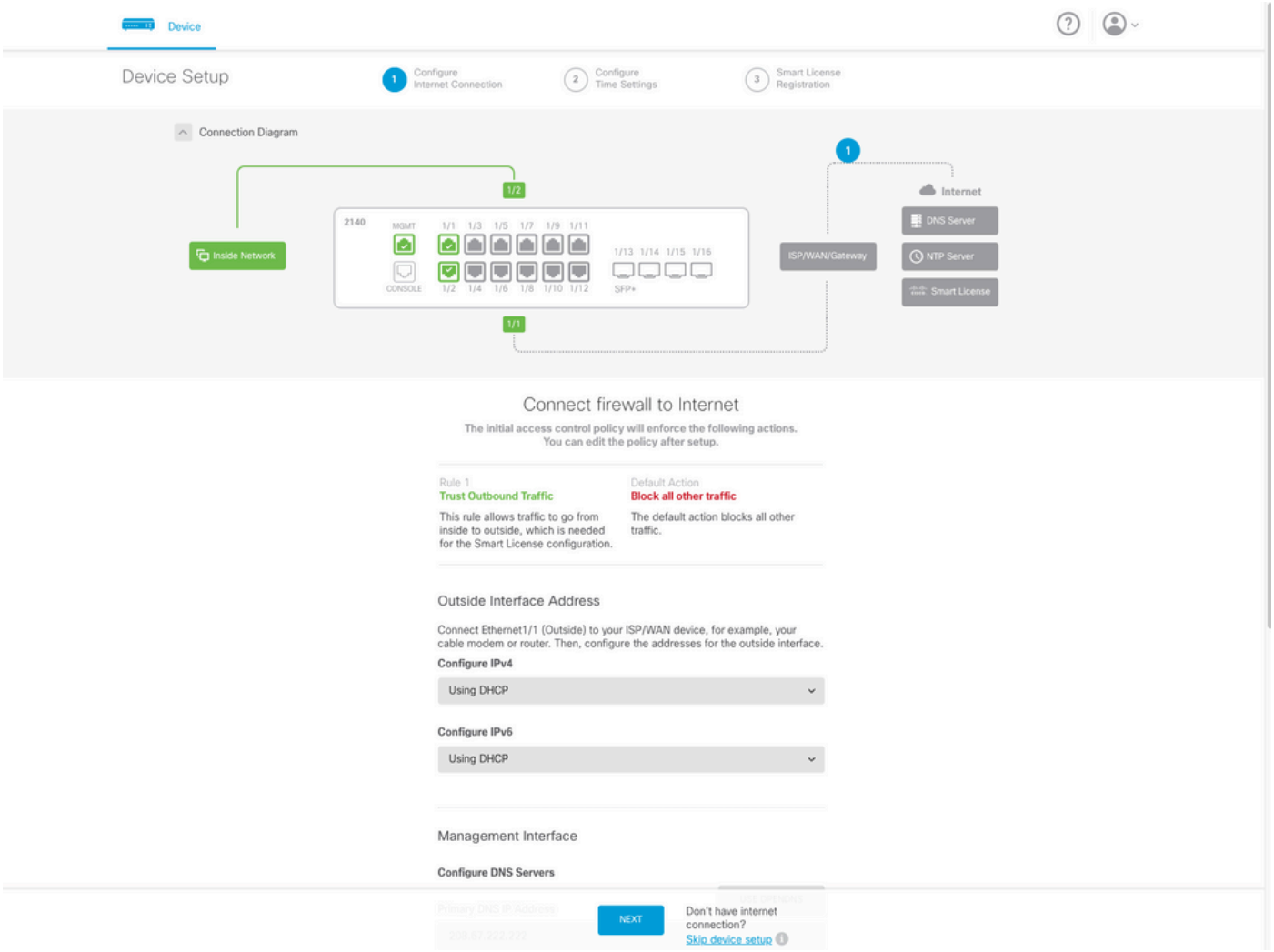
注：ラップトップに例えることができます。FXOSは、シャーシ（ラップトップ）上で動作するオペレーティングシステム（ラップトップ内のWindows OS）です。FTD（アプリケーションインスタンス）は、LinaおよびSnort（コンポーネント）上で稼働し、インス

トールできます。

ASAとは異なり、CLIではFTDを管理できません。個別のGUIベースの管理が必要です。このようなサービスには、FDMとFMCの2種類があります。

FDM:Firepowerデバイス管理

- FDMはオンボックス管理ツールです。セキュリティポリシーとシステム設定を構成、管理、および監視するためのWebベースのインターフェイスを提供します。
- FDMを使用する大きな利点の1つは、追加のライセンスがないことです。
- 1つのFDMで管理できるFTDは1つのみです。

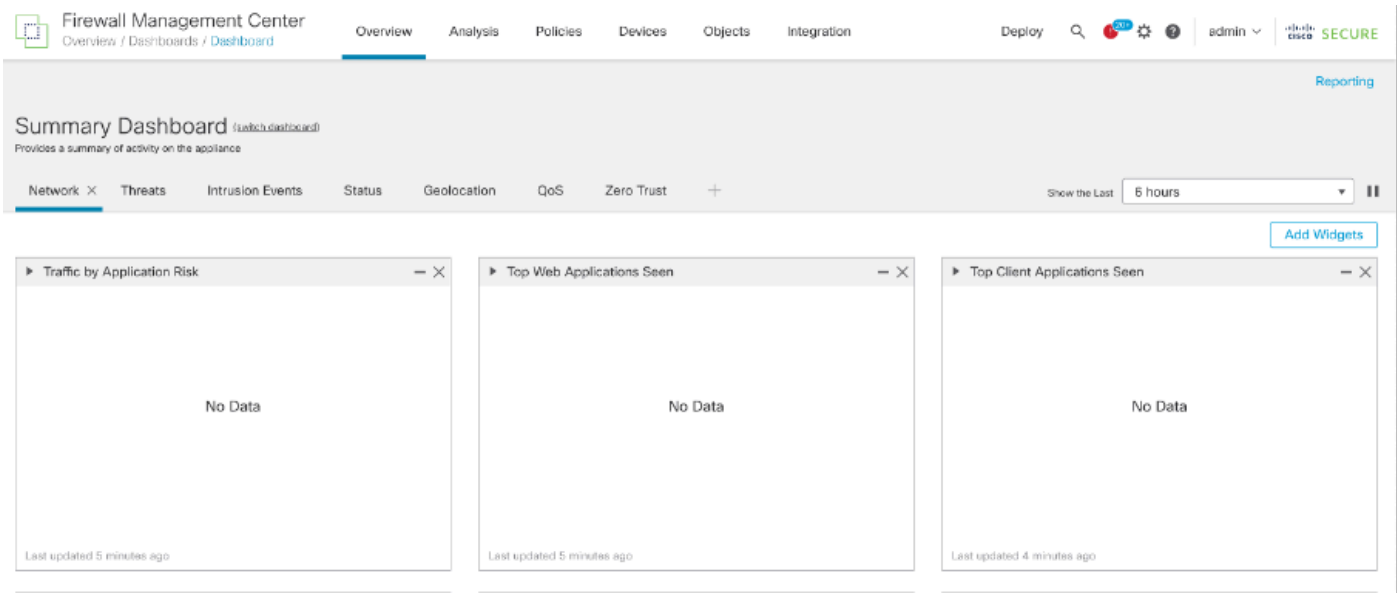


FDM

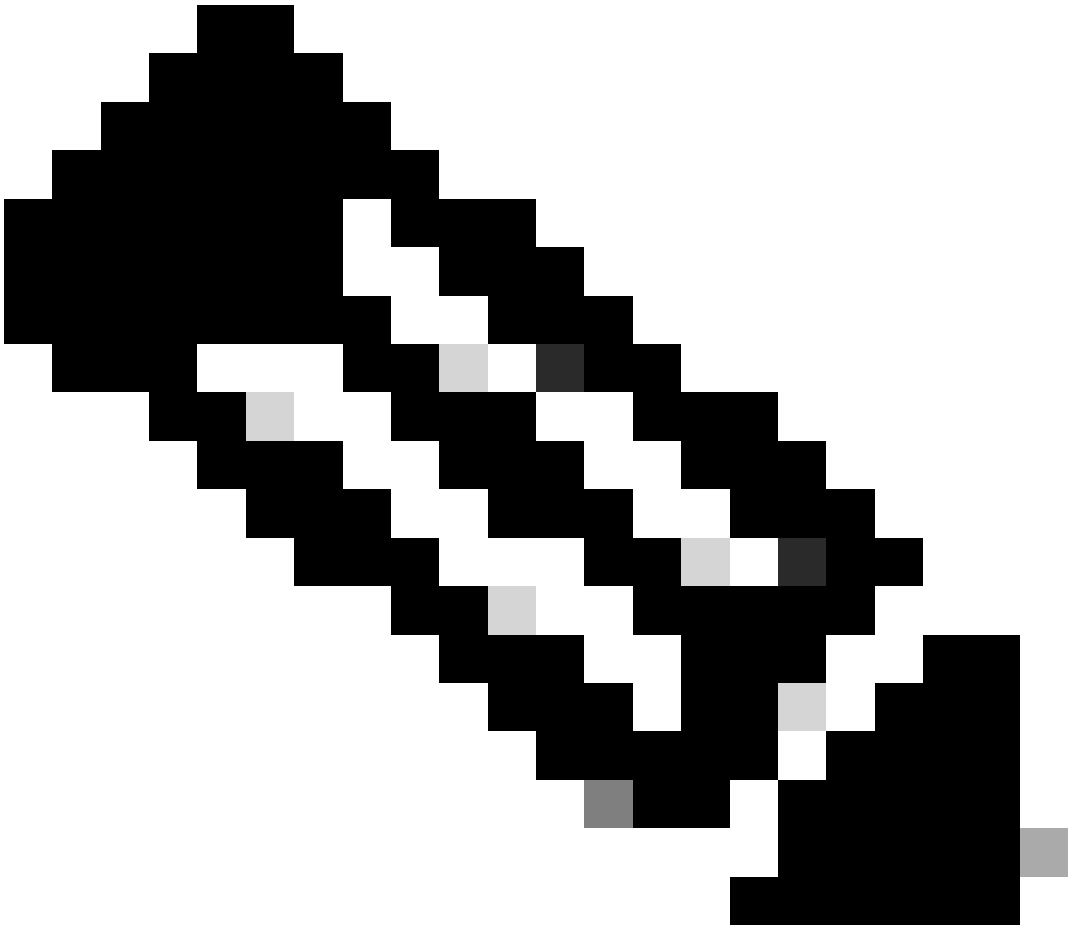
FMC:Firepower Management Center（Firepower管理センター）

- FMCは、Cisco FTDデバイス、Cisco ASAデバイスおよびFirepower Services向けの一元管理ソリューションです。また、FTDデバイスの設定、管理、および監視に使用できるGUIも提供します。
- ハードウェアFMCデバイスまたは仮想FMCデバイスを使用できます。
- この機能を使用するには、別途ライセンスが必要です。

- FMCのプラスの点は、1台のFMCデバイスで複数のFTDデバイスを管理できることです。



FMC



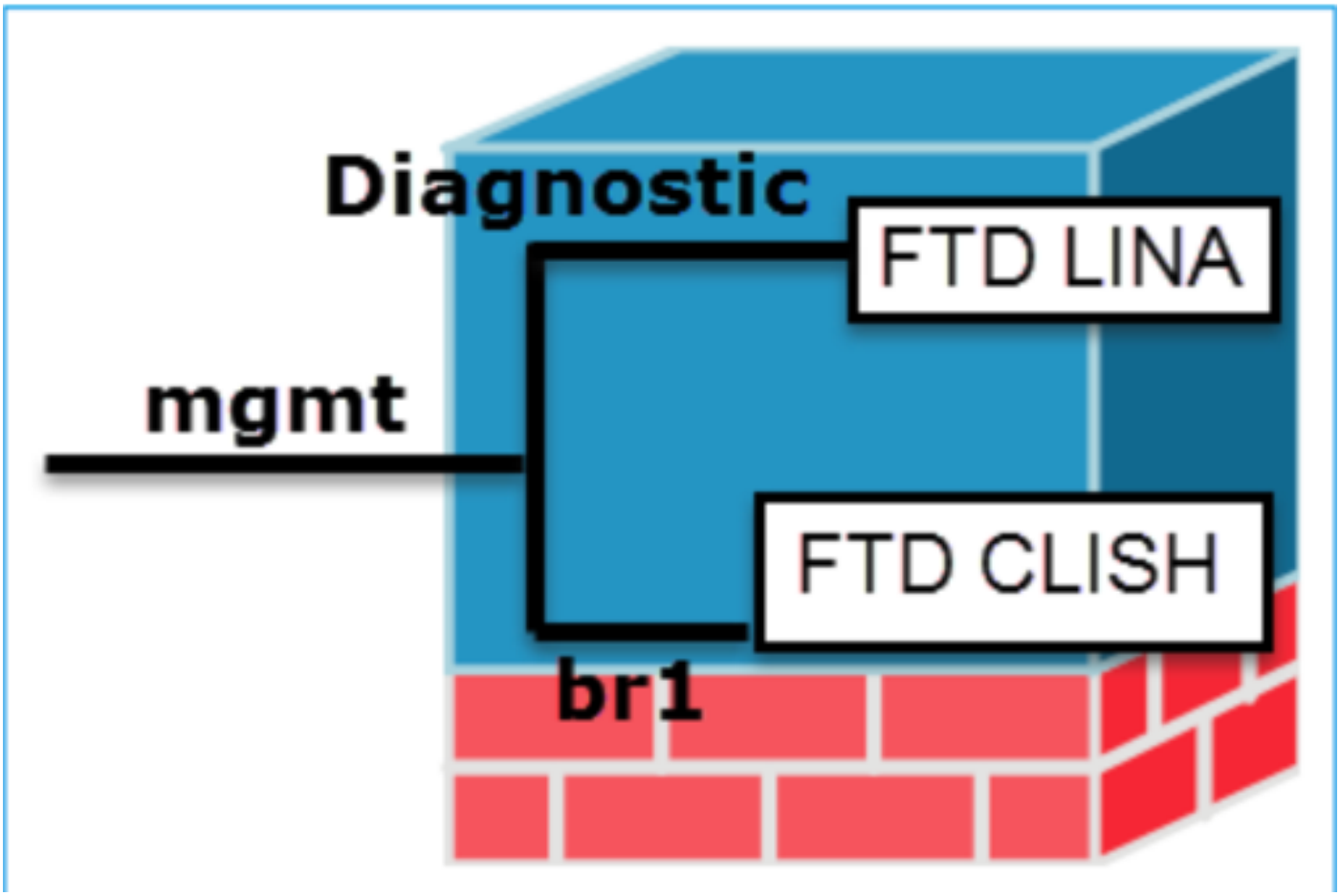
注意: FDMとFMCの両方を使用してFTDデバイスを管理することはできません。FDMオンボックス管理を有効にした後は、ローカル管理を無効にし、FMCを使用するように管理を再構成しない限り、FMCを使用してFTDを管理することはできません。一方、FTDをFMCに登録すると、FTDのFDMオンボックス管理サービスが無効になります。

CLISH：コマンドラインインターフェイスシェル

CLISHは、Cisco Firepower Threat Defense(FTD)デバイスで使用されるコマンドラインインターフェイス(CLI)です。このCLISHモードを使用して、FTDでコマンドを実行できます。

診断管理

FTDデバイスには、診断管理インターフェイスとFTD管理インターフェイスの2つの管理インターフェイスがあります。LINAエンジンにアクセスする必要がある場合は、診断管理インターフェイスを使用します。SNORTエンジンにアクセスする必要がある場合は、FTD管理インターフェイスを使用します。両方とも異なるインターフェイスであり、異なるインターフェイスIPアドレスを必要とします。



管理インターフェイス

ASAプラットフォームモード

1. プラットフォームモードでは、インターフェイスの有効化、EtherChannelの確立、NTP、

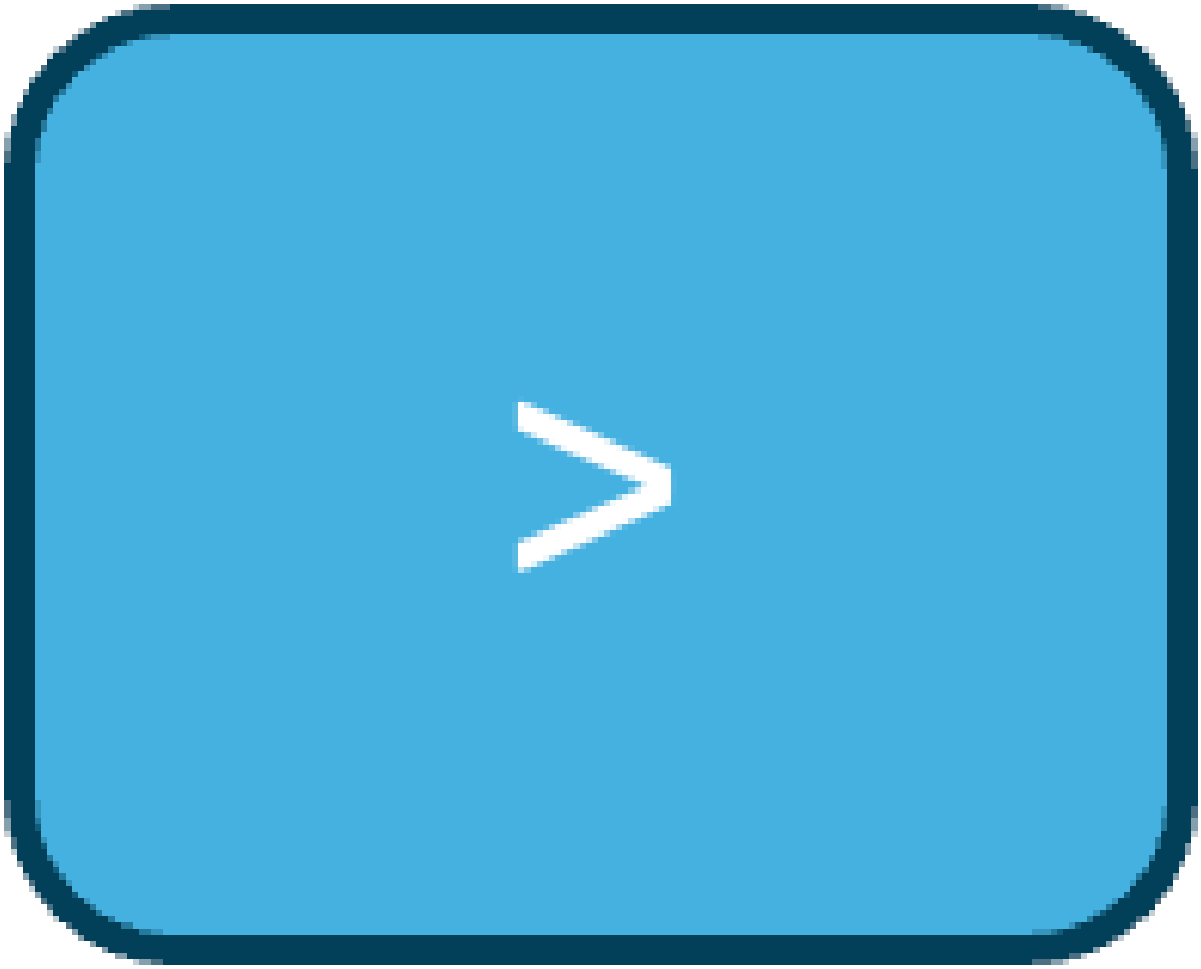
イメージ管理など、FXOSで基本的な動作パラメータとハードウェアインターフェイス設定を設定する必要があります。
2. その他の設定はすべて、ASA CLI/ASDMを介して行う必要があります。
3. これでFCMにアクセスできます。

ASAアプライアンスモード

1. Firepower 2100では、アプライアンスモードのASAは9.13（含む）以降で導入されました。
2. アプライアンスモードでは、ASAのすべての設定を行うことができます。FXOS CLIから使用できるのは、高度なトラブルシューティングコマンドだけです。
3. このモードにはFCMはありません。

FTDの異なるプロンプト

クリッシュ



クリッシュ

ルートモード/エキスパートモード

エキスパートモード

リナモード

リナモード

FXOSモード

FXOSモード

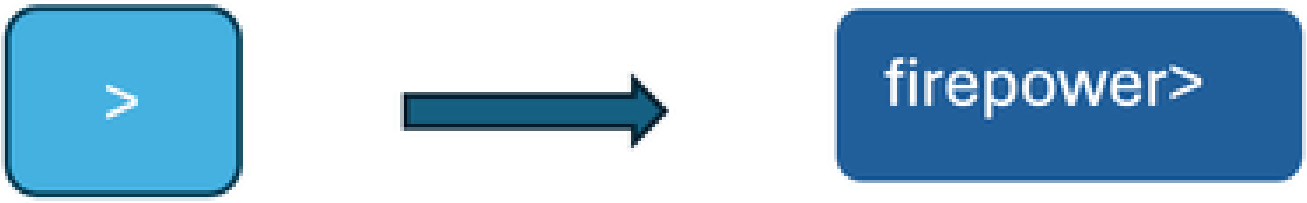
異なるプロンプト間を移動する方法

CLISHモードからFTDルートモード

クリックモードからエキスパートモード

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

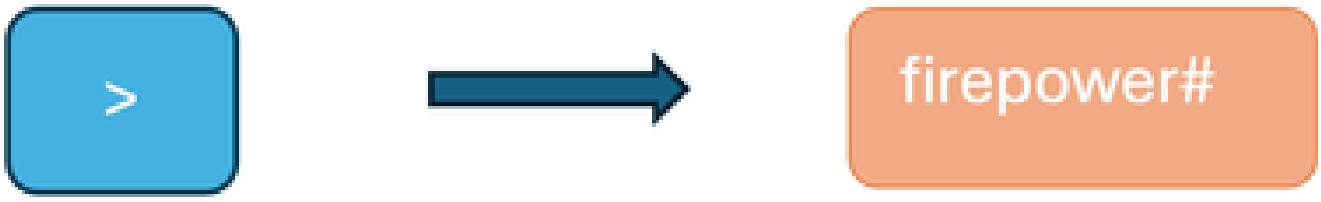
CLISHモードからLinaモード



クリッシュモードからリナモード

```
> 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モードからFXOSモード



ClishモードからFXOSモード

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

ルートモードからLINAモード

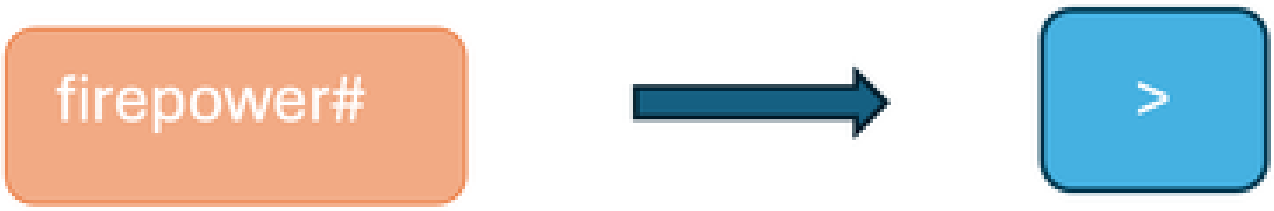
ExpertからLinaモード

```
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#
```

または

```
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からFTDへのCLISHモード（1000/2100/3100シリーズデバイス）



FXOSからClishモード

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

FXOSからFTDへのCLISHモード（4100/9300シリーズデバイス）

次の例は、モジュール1で脅威対策CLIに接続する方法を示しています。

```
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
>
```

コンソールを終了します。

~を入力してからquitを入力し、Telnetアプリケーションを終了します。

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

関連資料

Firepowerデバイスで実行できるさまざまなコマンドの詳細については、『FXOSコマンドリファ

レンス』、『FTDコマンドリファレンス』を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。