

Firepower 2100用のFDM On-Box Management Serviceの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、FTDがインストールされたFirePOWER 2100シリーズのFirePOWERデバイス管理(FDM)オンボックス管理サービスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower 2100、FTDソフトウェアのインストール
- Cisco Firepower Threat Defense(FTD)の基本設定とトラブルシューティング

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 Firepower 2100 シリーズ
- Cisco FTDバージョン6.2.3

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。

背景説明

このドキュメントの主な目的は、FirePOWER 2100シリーズのFDMオンボックス管理を有効にするために必要な手順を説明することです。

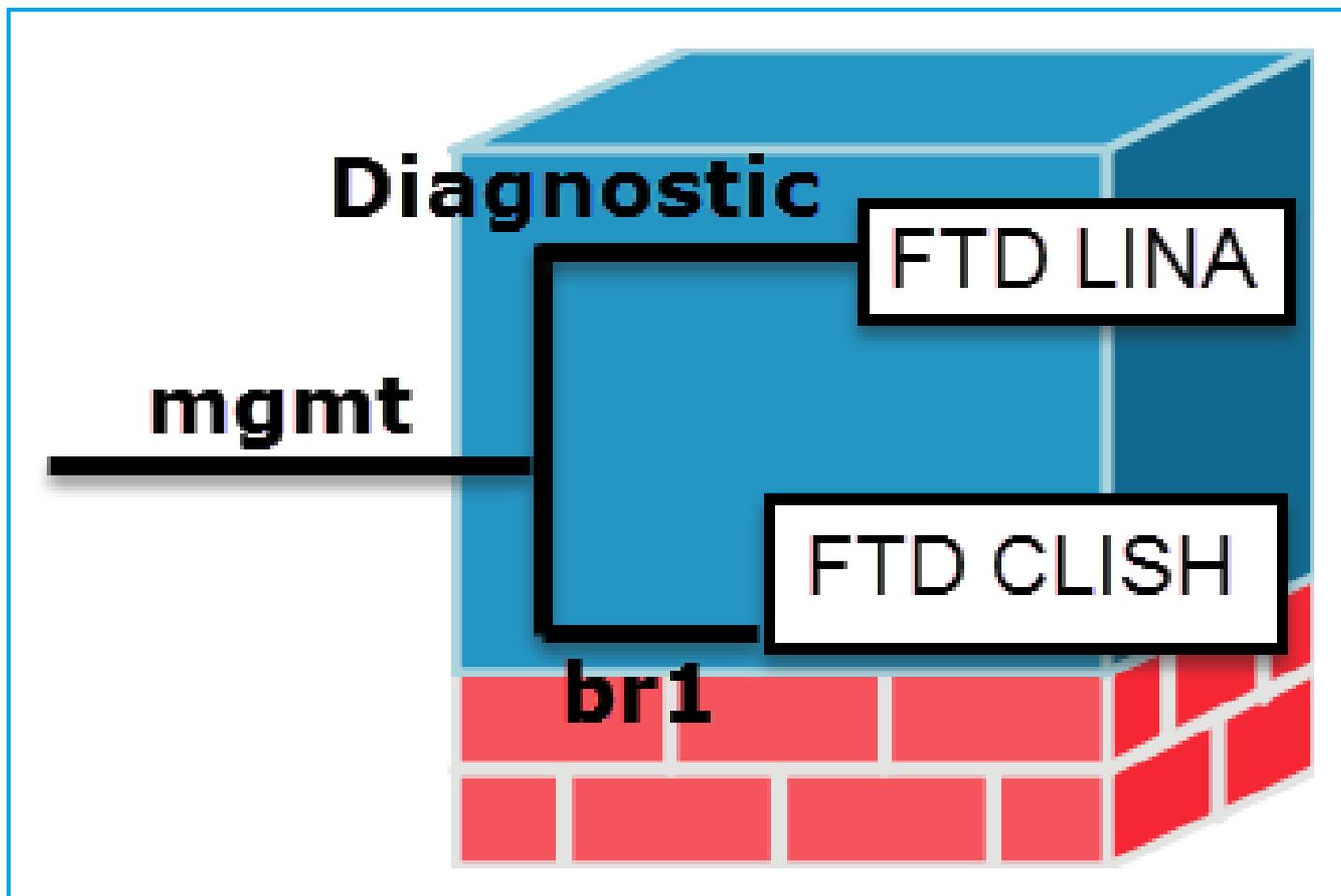
Firepower 2100にインストールされたFirepower Threat Defense(FTD)を管理するには、次の2つのオプションがあります。

- FDMオンボックス管理
- Cisco Firepower Management Center(FMC)

 注:FDMとFMCの両方を使用して、FirePOWER 2100にインストールされたFTDを管理することはできません。Firepower 2100 FTDで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設定しない限り、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。

 注意：現時点では、シスコにはFDM FirePOWER構成をFMCに（またはその逆に）移行するオプションがありません。FirePOWER 2100にインストールされたFTDに対して設定する管理タイプを選択する際は、この点を考慮してください。

管理インターフェイスは、br1(FPR2100/4100/9300アプライアンスではmanagement0)と診断の2つの論理インターフェイスに分かれています。



	管理 : br1/management0	管理 - 診断
目的	<ul style="list-style-type: none"> このインターフェイスは、FTD/FMC 通信に使用される FTD の IP を割り当てるために使用されます。 FMC/FTD 間における sftunnel の終端となります。 ルールベースの syslog の送信元として使用されます。 SSH および HTTPS による、FTD アプライアンスへのアクセスを可能にします。 	<ul style="list-style-type: none"> ASAエンジンへのリモートアクセス (SNMPなど) を提供します。 LINAレベルのsyslog、AAA、SNMPなどのメッセージの送信元として使用されます。
Mandatory	はい。FTD/FMC通信に使用されるため (sftunnelが終端します) 。	いいえ。設定することは推奨されません。代わりにデータインターフェイスを使用することをお勧めします (以下の注を参照) 。

 注：診断インターフェイスのIPアドレスをオフのままにしておくと、管理インターフェイスを他のデータインターフェイスと同じネットワークに配置できるという利点があります。診断インターフェイスを設定する場合、そのIPアドレスは管理IPアドレスと同じネットワーク

 上に存在する必要があるため、他のデータインターフェイスと同じネットワーク上に存在できない通常のインターフェイスとしてカウントされます。管理インターフェイスは更新のためにインターネットアクセスを必要とするため、管理インターフェイスを内部FTDインターフェイスと同じネットワークに配置すると、LAN上のスイッチだけを使用してFTDを展開し、内部インターフェイスを管理インターフェイスのデフォルトゲートウェイとして指定できます（これは、FTDがルーテッドモードで展開される場合にのみ適用されます）。

FTDはfirepower 2100アプライアンスにインストールできます。Firepowerのシャーシは、Firepower eXtensible Operating System(FXOS)と呼ばれる独自のオペレーティングシステムを実行してデバイスの基本動作を制御し、FTD論理デバイスはモジュールブレードにインストールされます。

 注:Firepower Chassis Manager(FCM)と呼ばれるFXOSグラフィックユーザインターフェイス(GUI)またはFXOSコマンドラインインターフェイス(CLI)を使用してFirepowerシャーシの機能を設定できます。ただし、FTDがFirepower 2100シリーズにインストールされている場合、FXOS CLIだけはGUI FCMを使用できません。

Firepower 21xxアプライアンス :

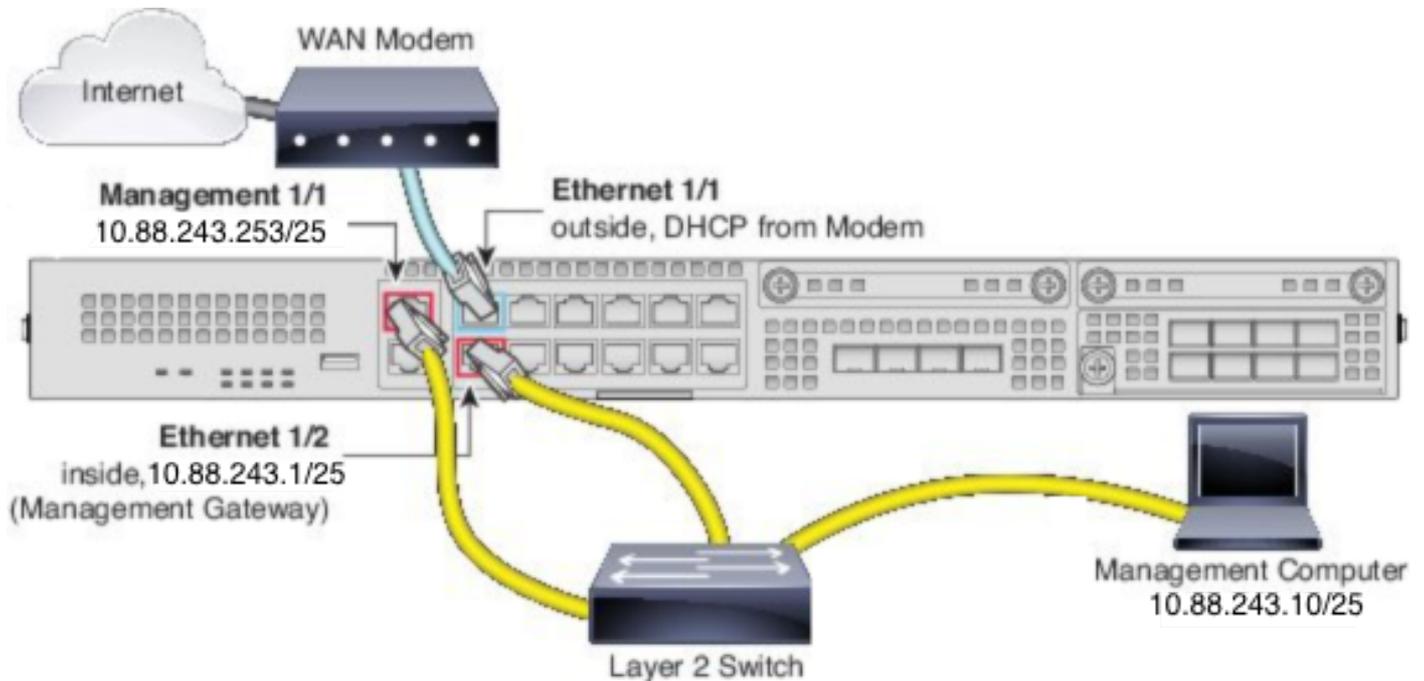


 注:firepower 2100シリーズでは、管理インターフェイスはシャーシのFXOSとFTD論理デバイス間で共有されます。

設定

ネットワーク図

デフォルト設定では、特定のfirepower 2100インターフェイスが内部および外部ネットワークに使用されることを前提としています。これらの期待に基づいてネットワークケーブルをインターフェイスに接続すると、初期設定が簡単になります。Firepower 2100シリーズのケーブル配線については、次の図を参照してください。



注:図は、レイヤ2スイッチを使用する単純なトポロジを示しています。その他のトポロジを使用でき、導入は基本的な論理ネットワーク接続、ポート、アドレッシング、および設定要件によって異なります。

コンフィギュレーション

Firepower 2100シリーズでFDMオンボックス管理を有効にするには、次の手順を実行します。

1. FPR2100シャーシにコンソールアクセスし、FTDアプリケーションに接続します。

```
firepower# connect ftd  
>
```

2. FTD管理IPアドレスを設定します。

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

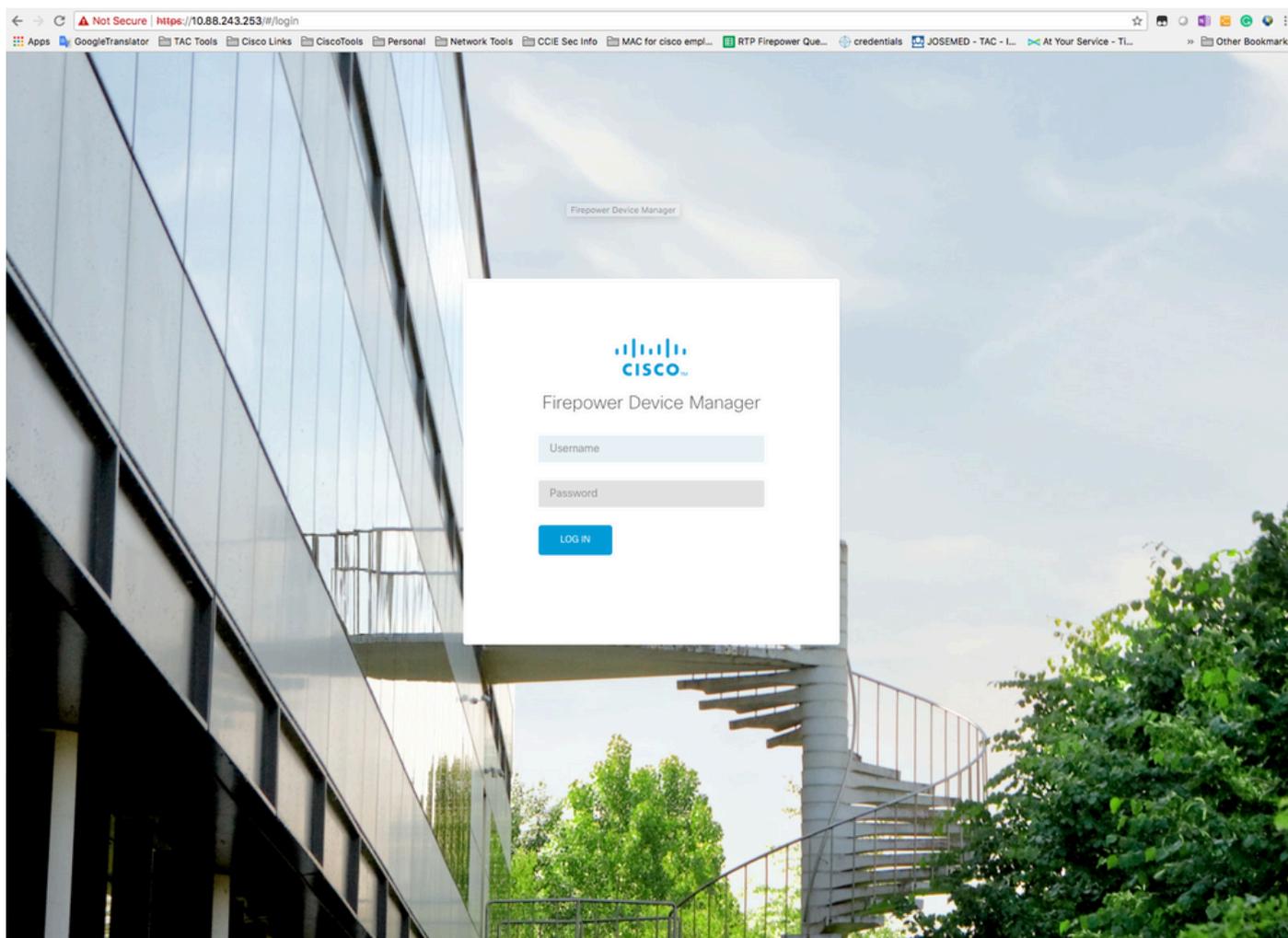
3. 管理タイプをローカルに設定します。

```
>configure manager local
```

4. FTDへのオンボックス管理アクセスを許可できるIPアドレス/サブネットを設定します。

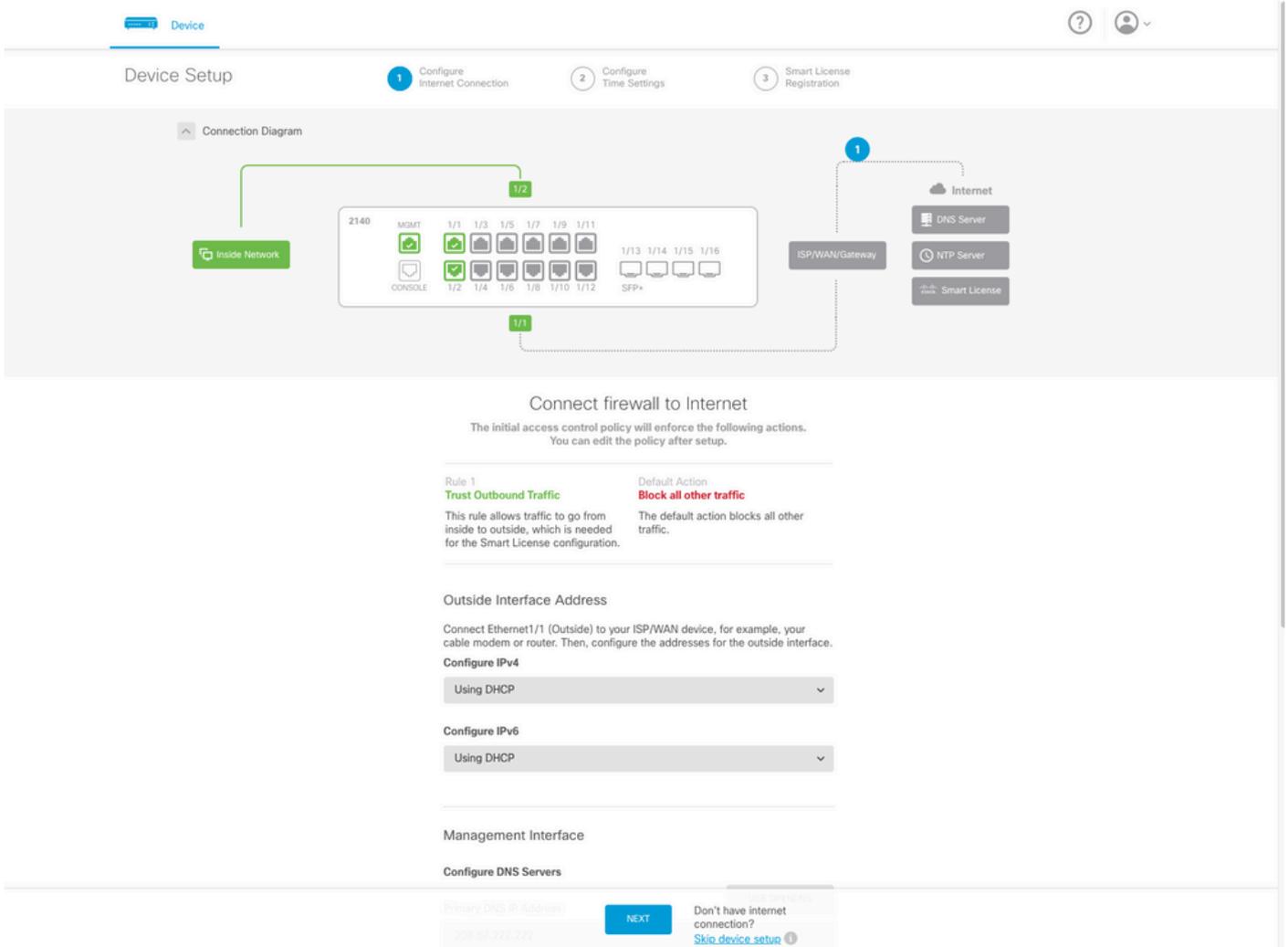
```
>configure https-access-list 0.0.0.0/0
```

5.ブラウザを開き、FTDを管理するように設定したIPアドレスにhttpsでアクセスします。これにより、FDM(On-Box)マネージャが開きます。



© 2015-2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
This product contains some software licensed under the "GNU Lesser General Public License, version 2 and version 2.1" provided with
ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 and version 2.1".

6.ログインし、デフォルトのFirePOWERクレデンシャル、ユーザ名admin、およびパスワードAdmin123を使用します。



確認

1.次のコマンドを使用して、FTDに対して設定したネットワーク設定を確認します。

```
> show network
===== [ System Information ] =====
Hostname                : firepower
DNS Servers             : 10.67.222.222
                       : 10.67.220.220
Management port        : 8305
IPv4 Default route     : 10.88.243.129
  Gateway

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:2C:C8:41:09:80
----- [ IPv4 ] -----
Configuration          : Manual
Address                 : 10.88.243.253
Netmask                 : 255.255.255.128
```

```
Broadcast                : 10.88.243.255
-----[ IPv6 ]-----
Configuration           : Disabled

=====[ Proxy Information ]=====
State                   : Disabled
Authentication          : Disabled
```

2.次のコマンドを使用して、FTDに対して設定した管理タイプを確認します。

```
> show managers
Managed locally.
```

関連情報

- [Cisco Firepowerデバイスマネージャ](#)
- [Firepower Management Centerを使用したFirepower 2100シリーズ向けCisco Firepower Threat Defenseクイックスタートガイド](#)
- [Firepower Threat Defense \(FTD \) 管理インターフェイスの設定](#)
- [Firepower 2100シリーズの再イメージ化](#)

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。