Firepower Management Center を使用した Cisco Firepower Threat Defense (Firepower 2100 シリーズ用) クイック スタート ガイド

バージョン 6.2.1(またはそれ以降)

初版:2017 年 5 月 15 日

このガイドの目的

このガイドでは、Firepower Threat Defense セキュリティ アプライアンスの初期設定を実行する方法と、Firepower Management Center にアプライアンスを登録する方法について説明します。大規模ネットワークの一般的な導入では、複数の管理対象アプライアンスがネットワーク セグメントにインストールされ、トラフィックが分析用にモニタされて管理する Firepower Management Center にレポートされます。Firepower Management Center は、管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供します。

単一またはごく少数のアプライアンスのみが含まれるネットワークでは、Firepower Management Center のような高性能の多機能デバイス マネージャを使用する必要がなく、一体型の Firepower Device Manager を使用できます。Firepower Device Manager の Web ベースのデバイス セットアップ ウィザードを使用して、小規模ネットワークの導入に最もよく使用されるソフトウェアの基本機能を設定できます(『Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Device Manager Quick Start Guide』を参照)。

ライセンス要件

Firepower Threat Defense セキュリティ アプライアンスには、Cisco Smart Licensing が必要です。Smart Licensing により、ライセンスの購入とライセンスのプールの一元管理を行うことができます。製品認証キー(PAK)ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンス キーに関連付けられません。Smart Licensing を利用すれば、ライセンスの使用状況やニーズをひと目で評価することもできます。

また、Smart Licensing では、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

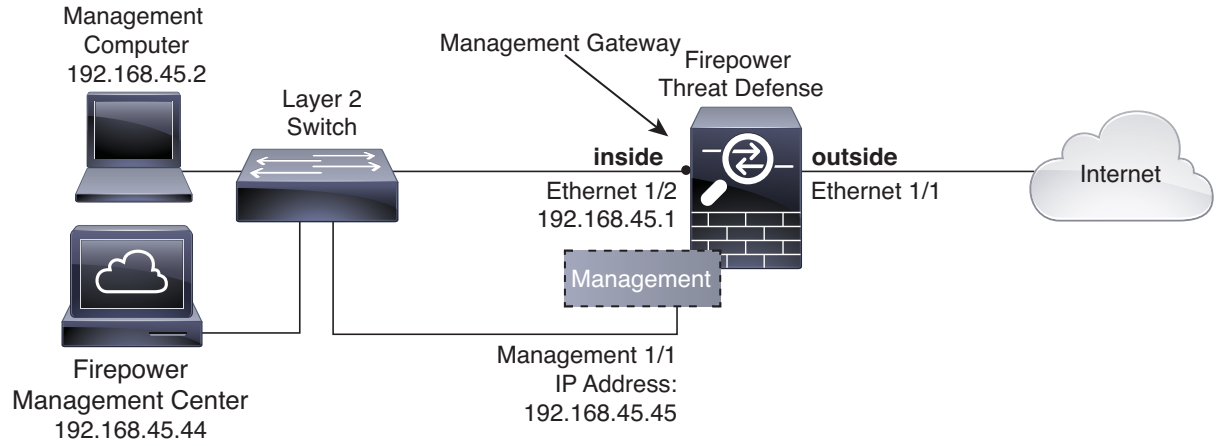
Firepower 機能のスマート ライセンスを複数購入する場合は、それらのライセンスを Cisco Smart Software Manager（http://www.cisco.com/web/ordering/smart-software-manager/index.html）で管理できます。Smart Software Manager では、組織のマスター アカウントを作成できます。Cisco Smart Software Manager の詳細については、『*Cisco Smart Software Manager User Guide*』を参照してください。

Firepower Threat Defense セキュリティ アプライアンスまたは Firepower Threat Defense Virtual を購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンス（Threat、Malware、URL Filtering）はオプションです。Firepower Threat Defense ライセンスの詳細については、『Firepower Management Center Configuration Guide』の「Licensing the Firepower System」を参照してください。

ネットワークへの Firepower Threat Defense の導入

次の図に、Firepower 2100 シリーズで推奨される Firepower Threat Defense のネットワーク配置を示します。

図 1 導入シナリオの例



設定例では、次の動作によって上記のネットワーク導入を有効化します。

- **内部 --> 外部**へのトラフィック フロー
- **DHCP** からの**外部 IP アドレス**
- **内部**上のクライアントに対する **DHCP**。
- **管理 1/1** は、Firepower Threat Defense を設定し、Firepower Management Center に登録するために使用されます。

  管理インターフェイスは、更新にインターネット アクセスが必要です。内部インターフェイスと同じネットワーク上に管理を配置すると、Firepower Threat Defense セキュリティ アプライアンスを内部のスイッチのみで導入して、内部インターフェイスをゲートウェイとして示すことができます。

  物理的な管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。『Firepower Management Center Configuration Guide』の「Firepower Threat Defense」を参照してください。

- **内部**インターフェイスでの **Firepower Management Center のアクセス**

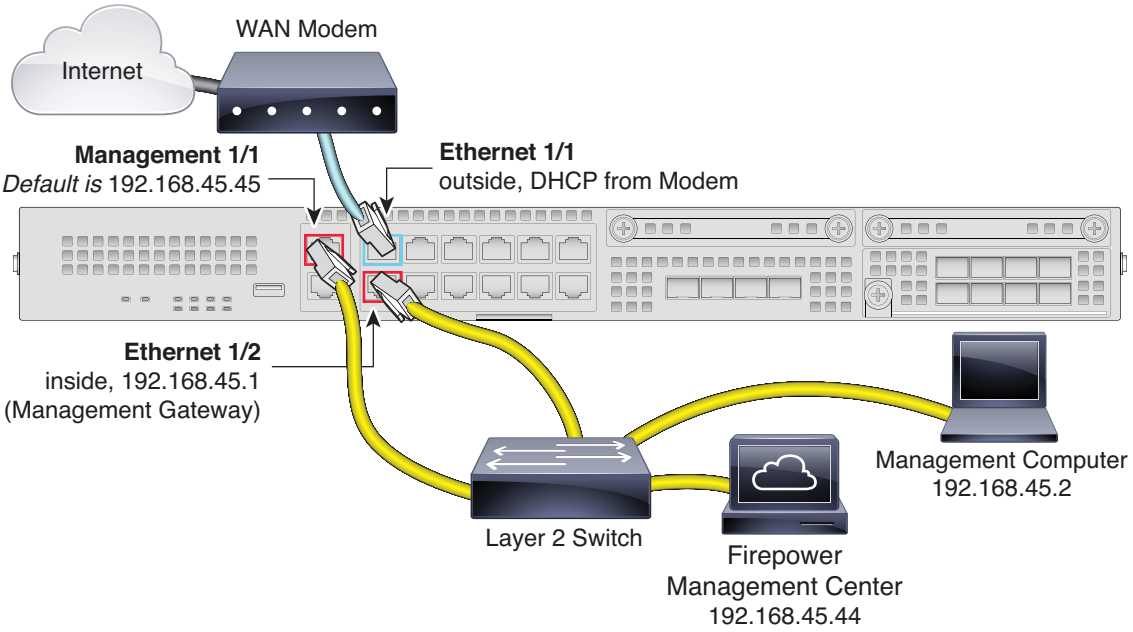
  （注）内部ネットワーク上に別のルータを導入すると、管理と内部の間でルーティングできます。別の導入設定例については、『Firepower Management Center Configuration Guide』の「Interfaces for Firepower Threat Defense」を参照してください。

インターフェイスの接続

デフォルト設定では、特定の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と仮定しています。これらの想定に基づいてインターフェイスにネットワーク ケーブルを接続していると、初期設定がしやすくなります。Firepower 2100 シリーズで上記のシナリオをケーブル接続するには、次の図を参照してください。

（注）次の図は、レイヤ 2 スイッチを使用する簡単なトポロジを示しています。他のトポロジも使用でき、基本的な論理ネットワーク接続、ポート、アドレッシング、構成の要件によって導入方法が異なります。

図 2　デフォルト設定のインターフェイス接続



手順

1. 以下の機器のケーブルをレイヤ 2 イーサネット スイッチに接続します。
   - イーサネット 1/2 インターフェイス（内部）
   - Management 1/1 インターフェイス（Firepower Management Center 用）
   - ローカルの管理コンピュータ
   - Firepower Management Center

   （注）管理インターフェイスは Firepower Management のみに属する独立したデバイスとして動作するため、内部インターフェイスと管理インターフェイスを同じネットワーク上で接続できます。
2. イーサネット 1/1（外部）インターフェイスを WAN デバイス（ケーブル モデムなど）に接続します。

Firepower 2100 セキュリティ アプライアンスへの電源の投入

システムの電源は、シャーシの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフル シャットダウンがサポートされ、システム ソフトウェアおよびデータの破損のリスクが軽減されます。

手順

1. 電源ケーブルを Firepower 2100 セキュリティ アプライアンスに接続し、電源コンセントに接続します。
2. セキュリティ アプライアンスの背面にある電源スイッチを押します。
3. セキュリティ アプライアンスの前面にある PWR LED を確認します。緑色に点灯している場合は、セキュリティ アプライアンスの電源が入っています。
4. セキュリティ アプライアンスの前面にある SYS LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

（注）スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの PWR LED が緑に点滅します。PWR LED が完全にオフになるまで電源を抜かないでください。

Firepower Management 用セキュリティ アプライアンスの設定

システムをネットワークで正しく機能させるには、初期設定を完了する必要があります。これには、セキュリティ アプライアンスをネットワークに挿入して、インターネットまたは他の上流に位置するルータに接続するために必要なアドレスの設定が含まれます。

最初の起動時またはシステムの再イメージ化後に、CLI のセットアップ ウィザードによって、Firepower Threat Defense セキュリティ アプライアンスの設定に必要な基本のネットワーク設定パラメータのプロンプトが表示され、Firepower Management Center への登録が要求されます。管理 IP アドレスと関連するゲートウェイ ルートは、インターフェイス リストの Firepower Management Center Web インターフェイスまたはセキュリティ アプライアンスのスタティック ルートに含まれて**いません**。これらは、セットアップ スクリプトおよび CLI によってのみ設定できます。

はじめる前に

データ インターフェイスがゲートウェイ デバイス（たとえば、ケーブル モデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンター導入の場合は、これがバックボーン ルータになります。

Management インターフェイスは、インターネットにアクセスできるゲートウェイに接続する必要もあります。システムのライセンスおよびデータベースのアップデートにインターネット アクセスが必要です。

CLI にログインするには、次のいずれかを実行します。

- セキュリティ アプライアンスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、セキュリティ アプライアンスのハードウェア ガイドを参照してください。

  （注）コンソール ポートでは、FXOS CLI ログイン プロンプトがデフォルトの CLI になります。Firepower Threat Defense CLI には、**connect ftd** コマンドを使用してアクセスできます。

- SSH クライアントを使用して、管理 IP アドレス（デフォルトは 192.168.45.45）に接続します。**admin** ユーザ名（デフォルトのパスワードは **Admin123** です）を使用してログインします。

ログインした後、CLI で使用可能なコマンドを確認するには、**help** または **?** を入力してください。

手順

1. [firepower ログイン（firepower login）] プロンプトで、ユーザー名 **admin** とパスワード **Admin123** のデフォルトのクレデンシャルでログインします。

   例：

   ```
   firepower login: admin
   Password:
   Cisco Firepower Extensible Operating System (FX-OS) Software
   ```

```
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.
.
<...output truncated...>
.
firepower #
```

2. Firepower Threat Defense アプリケーションに接続します。

   例：

   ```
   firepower #: connect ftd
   ```

3. Firepower Threat Defense システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。
   - 使用許諾契約の同意
   - 新しい管理者パスワード
   - IPv4 または IPv6 の構成
   - IPv4 または IPv6 の DHCP 設定
   - 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
   - システム名
   - デフォルト ゲートウェイの IPv4、IPv6、またはデータ インターフェイス設定
   - DNS セットアップ
   - HTTP プロキシ
   - 管理モード（ローカル管理は必要なし）
4. セットアップ ウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、**Enter** を押します。

   例：

   ```
   Please enter 'YES' or press <ENTER> to AGREE to the EULA:

   System initialization in progress. Please stand by.
   You must change the password for 'admin' to continue.
   Enter new password:
   Confirm new password:
   You must configure the network to continue.
   You must configure at least one of IPv4 or IPv6.
   Do you want to configure IPv4? (y/n) [y]: y
   Do you want to configure IPv6? (y/n) [n]: y
   Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
   Enter an IPv4 address for the management interface [192.168.45.45]: 192.168.0.43
   Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
   Enter the IPv4 default gateway for the management interface [data-interfaces]: data-interfaces
   Configure IPv6 via DHCP or manually? (dhcp/router/manual) [disable]: manual
   Enter the IPv6 address for the management interface []: 2001:420:1402:200f:e400::22
   Enter the IPv6 address prefix for the management interface []: 76
   Enter the IPv6 gateway for the management interface [data-interfaces]: data-interfaces
   Enter a fully qualified hostname for this system [firepower]: FMC-FP2100
   Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
   208.67.222.222
   Enter a comma-separated list of search domains or 'none' []: cisco.com
   If your networking information has changed, you will need to reconnect.
   Setting IPv6: 2001:420:1402:200f:e400::22 prefix: 76 gateway: 2001:420:1402:200f:e400::1 on
   management0
   ```

```
Setting DNS servers: 72.163.47.11
Setting DNS domains:cisco.com
Setting hostname as FMC-FP2100
DCHP Server Disabled
Setting static IPv4: 192.168.0.43 netmask: 255.255.255.0 gateway: 192.168.0.254 on
management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
```

5. 新しいログイン クレデンシャルを使用して、アプライアンスに再接続します。
6. ファイアウォール モードを設定します。次に例を示します。

```
Configure firewall mode? (routed/transparent) [routed]
```

（注）初期設定でファイアウォール モードを設定することをお勧めします。デフォルト モードはルーテッドです。初期設定後にファイアウォール モードを変更すると、実行コンフィギュレーションが消去されます。詳細については、『Firepower Management Center Configuration Guide』の「Transparent or Routed Firewall Mode」を参照してください。

7. デフォルトのシステム設定が処理されるのを待ちます。数分かかることがあります。

```
Update policy deployment information
    - add device configuration

You can register the sensor to a Management Center and use the Management Center
to manage it. Note that registering the sensor to a Management Center disables
on-sensor FirePOWER Services management capabilities.

When registering the sensor to a Management Center, a unique alphanumeric
registration key is always required. In most cases, to register a sensor
to a Management Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Management Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Management Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Management Center.
```

（注）登録キーは、ユーザが生成した 1 回限り使用できる一意のキーで、37 文字を超えてはなりません。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。セキュリティ アプライアンスを Firepower Management Center に追加するときに、この登録キーを思い出す必要があります。

8. **configure manager add** コマンドを使用して、このセキュリティ アプライアンスを管理する Firepower Management Center アプライアンスを指定します。

登録キーは、ユーザ生成の 1 回しか使用できないキーです。セキュリティ アプライアンス Firepower Management Center のインベントリに追加する必要があります。次に、簡単な例を示します。

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

セキュリティ アプライアンスと Firepower Management Center が NAT デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに DONTRESOLVE を指定します。たとえば次のようにします。

```
>configure manager add DONTRESOLVE my_reg_key my_nat_id
Manager successfully configured.
```

Firepower Management Center およびセキュリティ アプライアンスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。NAT ID は、最初の通信に対する信頼を確立し、正しい登録キーを検索するために、管理対象アプライアンスの登録に使用するすべての NAT ID の中で一意である**必要があります**。

（注）Firepower Management Center または Firepower Threat Defense のいずれかのセキュリティ アプライアンスのうちの少なくとも 1 つは、2 つのアプライアンス間で双方向の SSL 暗号化通信チャネルを確立するために、パブリック IP アドレスを持つ必要があります。

9. CLI を閉じます。

```
> exit
```

次の作業

- 次のセクションで説明されているように、セキュリティ アプライアンスを Firepower Management Center に登録します。

セキュリティ アプライアンスの Firepower Management Center への登録およびスマート ライセンスの割り当て

はじめる前に

- Firepower Management Center でスマート ライセンスを設定します。以下のシスコ スマート アカウントがあることを確認します。Cisco Software Central（https://software.cisco.com/ [英語]）で作成できます。
- Firepower Threat Defense の基本ライセンスがスマート アカウントに追加されていることを確認します（例：L-FP2100T-BASE=）。

手順

1. ブラウザで HTTPS 接続を使用して、上記で入力したホスト名またはアドレスを使用して Firepower Management Center にログインします。たとえば、https://MC.example.com などです。
2. [デバイス管理（Device Management）] ウィンドウを使用して（[デバイス（Devices）] > [デバイス管理（Device Management）]）、セキュリティ アプライアンスを追加します。詳細については、オンライン ヘルプまたは『Firepower Management Center Configuration Guide』の「Managing Devices」を参照してください。
3. CLI 設定時に、セキュリティ アプライアンスに設定済みの管理 IP アドレスを入力します。
4. CLI 設定時に、セキュリティ アプライアンスで指定されたキーと同じ登録キーを使用します。
5. [Smart Licensing] オプション（[Threat]、[URL]、[Advanced Malware]）を選択します。

   これらのライセンスはすでにスマート アカウントにある必要があります。スマート アカウントにアプライアンスの基本ライセンスがあることを確認してください。
6. [登録（Register）] をクリックして、デバイス登録の成功を確認します。

次の作業

- お使いのセキュリティ アプライアンで、ポリシーとデバイスの設定を行います。セキュリティ アプライアンスを Firepower Management Center に追加すると、Firepower Management Center ユーザ インターフェイスを使用してデバイス管理設定を構成したり、アクセス コントロール ポリシーや Firepower Threat Defense システムを使用してトラフィックを管理するためのその他の関連ポリシーを設定および適用したりできます。

次の作業

- Firepower Management Center による Firepower Threat Defense の管理の詳細については、『Firepower Management Center Configuration Guide』または Firepower Management Center のオンライン ヘルプを参照してください。
- すべての Firepower System のマニュアルのリンクについては、Cisco Firepower System マニュアルのナビゲーションを参照してください。