Firepower Management Center を使用した Cisco Firepower Threat Defense (ASA 5508-X、ASA 5516-X 用) クイック スタート ガイド

初版: 2016 年 8 月 10 日

最終更新日: 2017 年 5 月 15 日

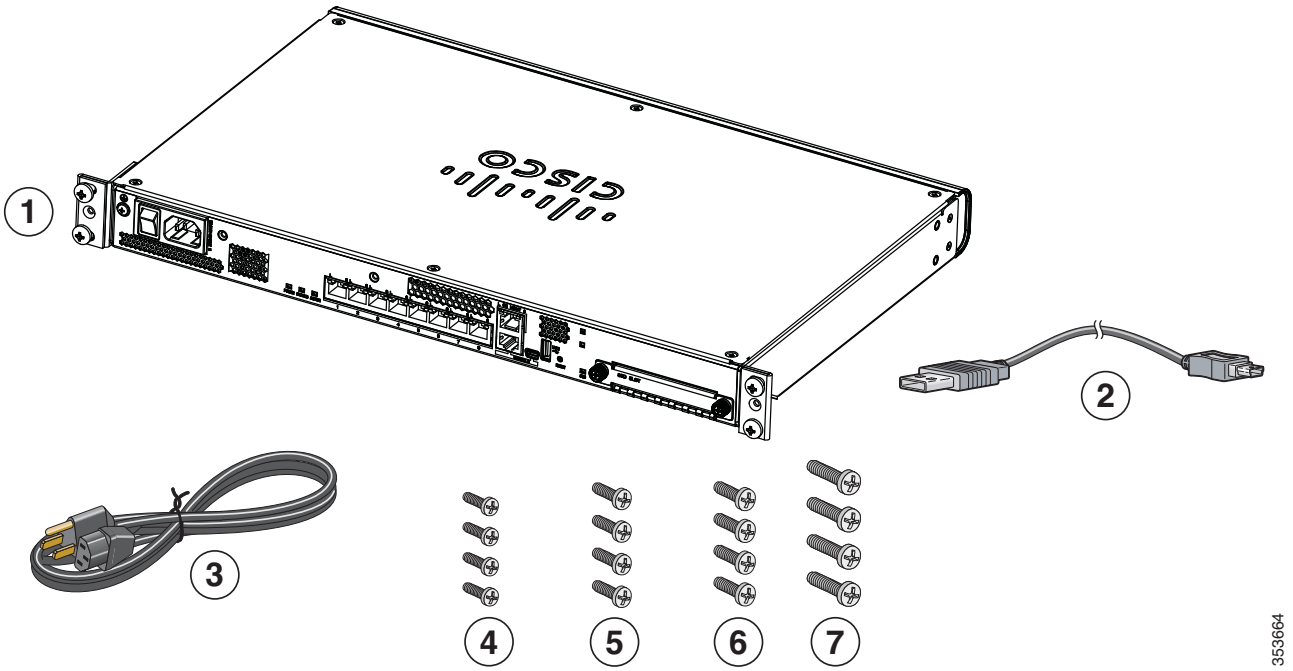
1. このガイドの対象読者

このガイドでは、Firepower Threat Defense デバイスの初期設定を実行する方法と、Firepower Management Center にデバイ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、複数の管理対象デバイスがネットワーク 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 Firepower Management Center に送信されます。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一元管理コンソールを提供します。

単一またはごく少数のデバイ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 (http://www.cisco.com/go/fdm-quick 参照)。

2. パッケージの内容

この項では、シャーシのパッケージの内容について説明します。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。



1	ASA 5508-X または ASA 5516-X シャーシ	2	青いコンソール ケーブルおよびシリアル PC ターミナル アダプタ（DB-9 to RJ-45）
3	電源ケーブル	4	4 本の 10-32 プラス ネジ（ラック マウント用）
5	4 本の 12-24 プラス ネジ（ラック マウント用）	6	4 本の M6 プラス ネジ（ラック マウント用）
7	4 本の M4 プラス ネジ（ラック マウント用）		

3. ライセンス要件

Firepower Threat Defense デバイスには、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できます。

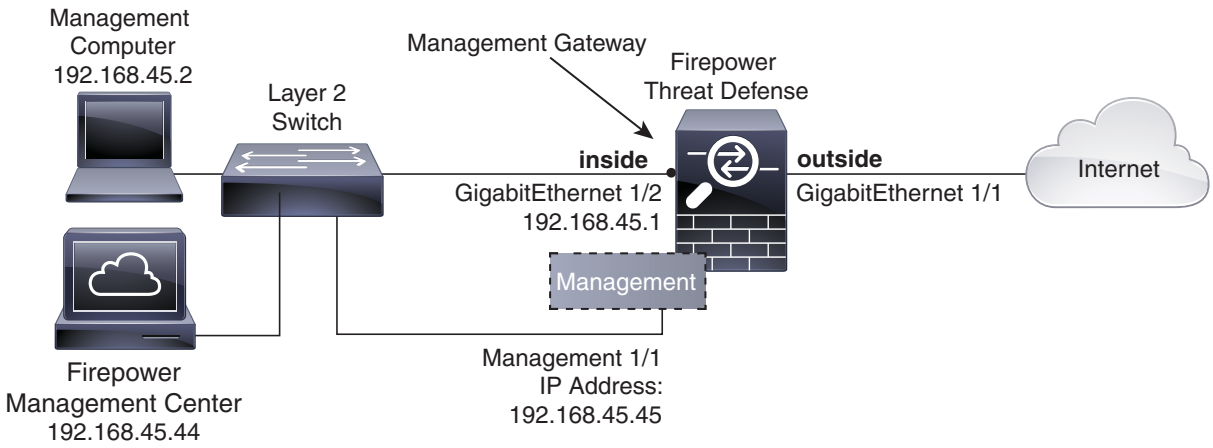
また、Smart Licensing では、まだ購入していない製品の機能も使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

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 デバイスまたは 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 のライセンスに関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Licensing the System」の章を参照してください。

4. ネットワークへの Firepower Threat Defense の導入

次の図に、ASA 5508-X または ASA 5516-X で推奨される Firepower Threat Defense のネットワーク導入を示します。



（注）導入環境内で別の内部スイッチを使用する必要があります。

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**のクライアントに対する **DHCP**。
- **Management 1/1** は、Firepower Threat Defense デバイスをセットアップし、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 デバイ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「Interfaces for Firepower Threat Defense」の章を参照してください。

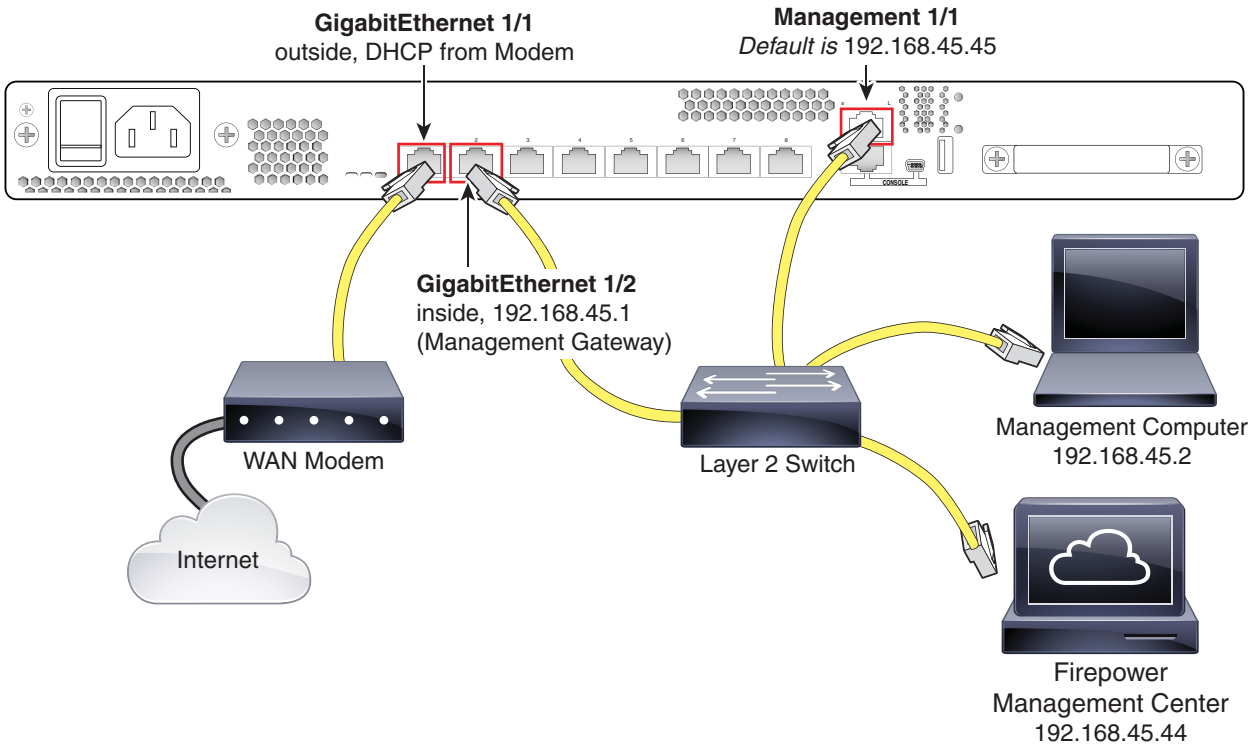
- **内部**インターフェイスでの **Firepower Management Center のアクセス**

  （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」の章を参照してください。

ASA 5508-X または ASA 5516-X 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。

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。
   - GigabitEthernet 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

   （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. GigabitEthernet 1/1（外部）インターフェイスを ISP/WAN モデムまたはその他の外部デバイスに接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。

5. Firepower Threat Defense デバイスの電源投入

手順

1. 電源ケーブルを Firepower Threat Defense デバイスに接続し、電源コンセントに接続します。
2. Firepower Threat Defense デバイスの背面にある電源ボタンを押します。
3. Firepower Threat Defense デバイスの前面にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。
4. Firepower Threat Defense デバイスの前面にあるステータス LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

6. Firepower Management 用のデバイス設定

最初に CLI にアクセスするときに、セットアップ ウィザードによって、Firepower Threat Defense デバイ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デバイスのスタティック 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 インターフェイスをゲートウェイのデバイス（ケーブル モデムやルータなど）に接続し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。データセンターの導入では、バックボーン ルータになります。

管理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シングおよびデータベースの更新には、インターネット アクセスが必要です。

手順

1. たとえば、コンソール ポートから、または SSH を使用して、デバイスに接続します。
   - モニタとキーボードが取り付けられたデバイスの場合は、コンソールからログインします。
   - デバイスの管理インターフェイスへのアクセスでは、管理インターフェイスのデフォルト IPv4 アドレス（192.168.45.45）に SSH を実行します。
2. ユーザ名 **admin** およびパスワード **Admin123** を使用してログインします。
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。
   - Accept EULA
   - 新しい管理者パスワード
   - IPv4 または IPv6 の設定
   - 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 IPv4 か IPv6 またはその両方
   - DNS の設定
   - HTTP プロキシ
   - 管理モード
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]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.133.128.47
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.0
Enter the IPv4 default gateway for the management interface []: 10.133.128.1
Enter a fully qualified hostname for this system [firepower]: laurel.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.33.16.6
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.

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」の章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。これには数分かかる可能性があります。

```
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、ユーザ生成の 1 回しか使用できないキーです。37 文字以下にする必要があります。有効な文字は、英数字（A-Z、a-z、0-9）、およびハイフン（-）です。デバイスを 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、このデバイスを管理する 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。デバイスを 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.
```

デバイスと 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を登録するため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

- 次の項の説明に従って、デバイスを Firepower Management Center に登録します。

7. デバイスの 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 Smart Licensing を設定します。以下の Cisco 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/）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-ASA5516T-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. デバイスを追加するには、[Device Management] ページ（[Devices] > [Device Management]）を使用します。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」の章を参照してください。
3. CLI 設定時に、デバイスに設定済みの管理 IP アドレスを入力します。
4. CLI 設定時にデバイスで指定されたの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. [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

- デバイスのポリシーとデバイス設定を構成します。デバイスを 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することができます。

6. 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 の構成ガイドまたは Firepower Management Center のオンライン ヘルプを参照してください。