Firepower Management Center を使用した Cisco Firepower Threat Defense（ASA 5506-X シリーズ用）クイック スタート ガイド

初版：2016 年 8 月 10 日

最終更新日：2018 年 12 月 3 日

Warning: Firepower Threat Defense の 6.3 以降のリリースを ASA 5506-X、5506W-X、および 5506H-X にインストールすることはできません。これらのプラットフォームに関してサポートされる Firepower Threat Defense の最後のリリースは 6.2.3 です。

1. 対象読者

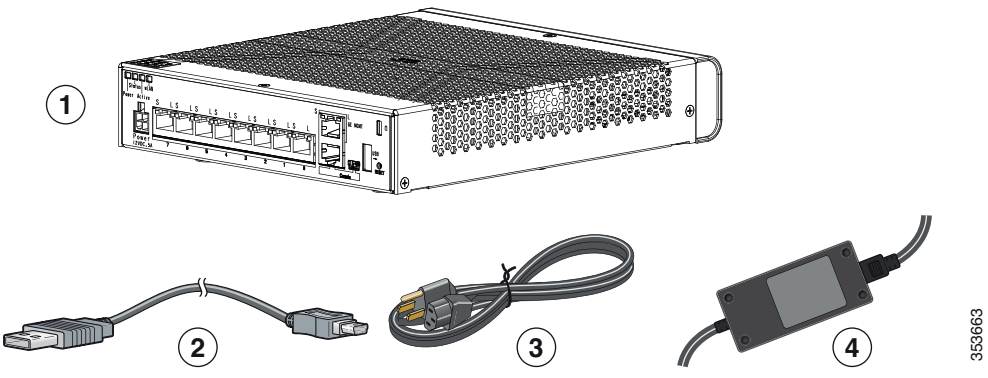
このガイドでは、Firepower Threat Defense デバイスの初期設定を実行する方法と、Firepower Management Center にデバイスを登録する方法について説明します。大規模ネットワークの一般的な導入では、複数の管理対象デバイスがネットワーク セグメントにインストールされ、トラフィックが分析用にモニターされて Firepower Management Center にレポートされます。Firepower Management Center は、管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供します。

単一またはごく少数のデバイスが含まれるネットワークでは、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

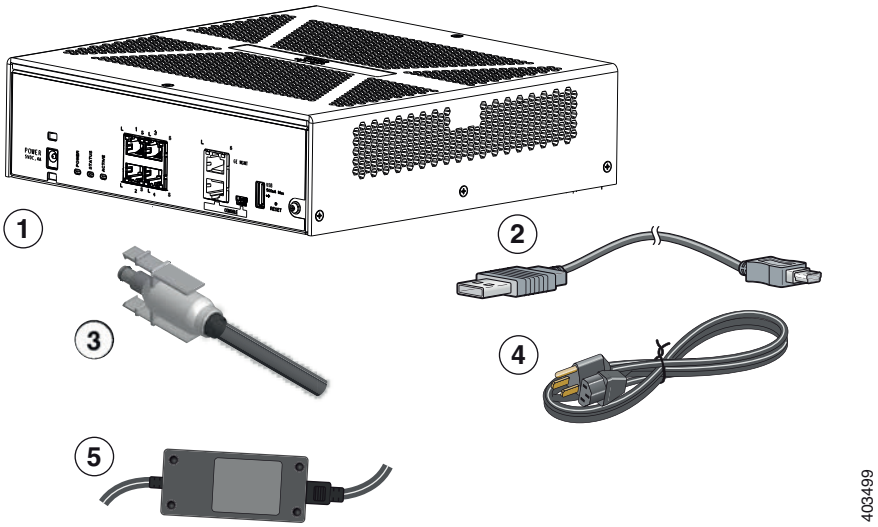
この項では、シャーシのパッケージの内容について説明します。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。

ASA 5506-X および 5506W-X



1	ASA 5506-X または ASA 5506W-X シャーシ	2	USB コンソール ケーブル（タイプ A からタイプ B）
3	電源ケーブル	4	電源

ASA 5506H-X



1	ASA 5506H-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	電源コード固定ロック	4	電源ケーブル
5	電源		

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することもできます。

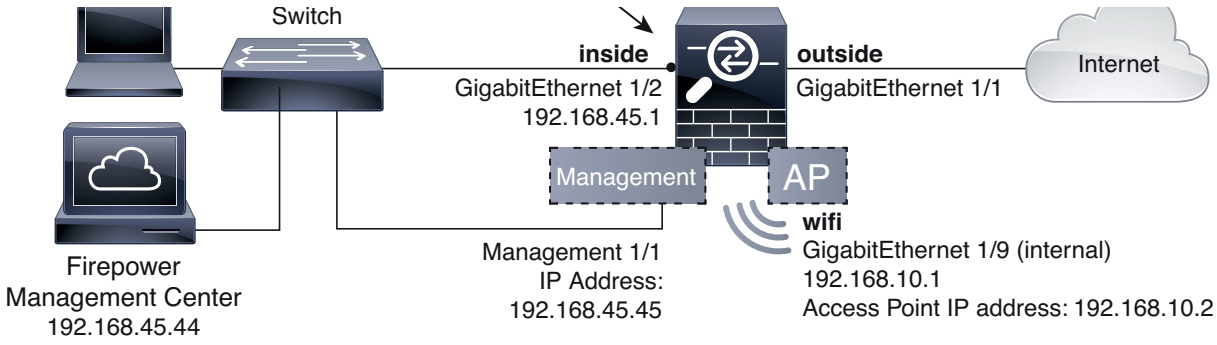
また、スマート ライセンスでは、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録さえしていれば、すぐにライセンスの使用を開始し、後でライセンスを購入することができます。これにより、発注書が承認されるまで待たなくても、特定の機能を導入して使用できるようになります。

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 デバイスや 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 5506-X シリーズ アプライアンスおよび組み込みワイヤレス アクセス ポイント（ASA 5506W-X）で推奨される Firepower Threat Defense ネットワーク導入を示します。



注：導入には、別々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**
- （ASA 5506W-X）**WiFi <--> 内部**、**WiFi --> 外部**へのトラフィック フロー
- **内部**および **WiFi** 上のクライアントに対する **DHCP** アクセス ポイントおよびそのすべてのクライアントが ASA を DHCP サーバーとして使用します。
- **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。

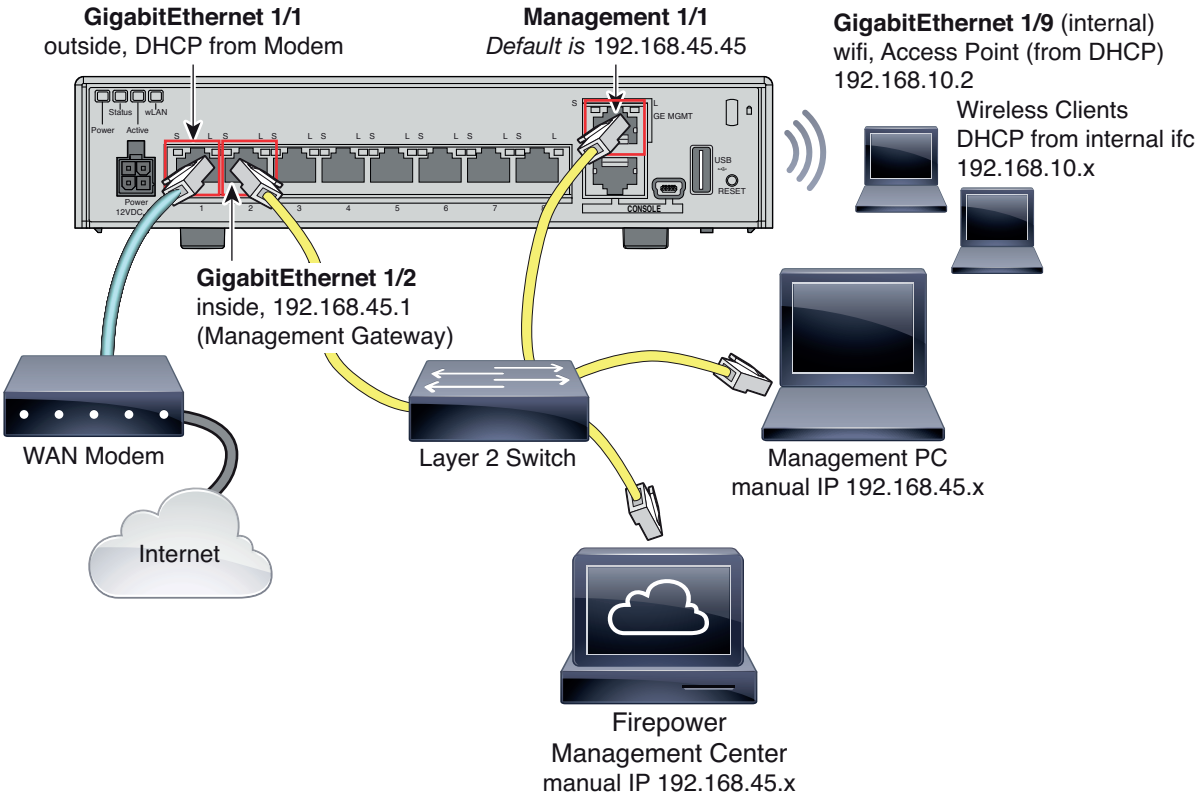
  管理インターフェイスは、更新にインターネット アクセスが必要です。内部インターフェイスと同じネットワーク上に管理を配置すると、Firepower Threat Defense デバイスを内部のスイッチのみで導入して、内部インターフェイスをゲートウェイとして示すことができます。

  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** インターフェイスおよび **WiFi** インターフェイス上の **Firepower Management Center アクセス**

  注：内部ネットワーク上に独立した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。さまざまな導入構成例については、『*Firepower Management Center Configuration Guide*』の「Interfaces for Firepower Threat Defense」の章を参照してください。

ASA 5506-X シリーズで上記のシナリオのように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 アドレスが DHCP を使用して取得されますが、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. 電源コードを Firepower Threat Defense デバイスに接続し、電源コンセントに接続します。

   電源コードを差し込むと電源が自動的にオンになります。電源ボタンはありません。
2. Firepower Threat Defense デバイスの背面にある電源 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。
3. Firepower Threat Defense デバイスの背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 インターフェイスがゲートウェイ デバイス（ケーブルモデム、ルータなど）に接続されていることを確認します。エッジ導入の場合、インターネット対応ゲートウェイに接続されていなければなりません。データ センター導入の場合、バックボーン ルータに接続されている必要があります。

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。

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。
   - モニター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. ユーザー名 **admin** およびパスワード **Admin123** でログインします。
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。
   - 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 IPv4 か IPv6 またはその両方
   - DNS セットアップ
   - 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。数分かかることがあります。

```
Update policy deployment information
 - add device configuration
```

センサーを Management Center に登録し、Management Center を使用してセンサーを管理できます。センサーを Management Center に登録すると、センサー上の FirePOWER サービス管理機能が無効になることに注意してください。

センサーを Management Center に登録する場合は、一意の英数字による登録キーが常に必要です。ほとんどの場合、センサーを Management Center に登録するには、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。
'configure manager add [hostname | ip address] [registration key]'

ただし、センサーと Management Center が NAT デバイスにより分離されている場合は、この一意の登録キーと一緒に一意の NAT ID を入力する必要があります。'configure manager add DONTRESOLVE [registration key] [NAT ID]'

後で Management Center の Web インターフェイスを使用してこのセンサーを Management Center に追加する場合は、同じ登録キーと、必要に応じて同じ NAT ID を使用する必要があります。

8. Firepower Threat Defense デバイスを Firepower Management Center へ登録します。

```
> configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

値は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} は、Firepower Management Center の完全修飾ホスト名または IP アドレスのいずれかを指定します。Firepower Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- *reg_key* は、Firepower Threat Defense モジュールを Firepower Management Center へ登録するために必要な一意の英数字による登録キーです。

注：登録キーは、ユーザーが生成した 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。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。

- *nat_id は、Firepower Management Center と Firepower Threat Defense 間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。*

9. **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、ユーザー生成の 1 回しか使用できないキーです。Firepower Threat Defense 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。

10. 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 でスマート ライセンスを設定します。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、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（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. [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

- 組み込みワイヤレス アクセス ポイントを備えた ASA 5506W-X がある場合は、次の項の説明に従ってアクセス ポイントを有効化します。
- デバイスのポリシーとデバイス設定を構成します。

8. ワイヤレス アクセス ポイント（ASA 5506W-X）の設定

ASA 5506W-X には、デバイスに統合された Cisco Aironet 702i ワイヤレス アクセス ポイントが組み込まれています。このワイヤレス アクセス ポイントは、デフォルトでは無効にされています。ワイヤレス無線を有効化し、SSID およびセキュリティの設定を行うには、アクセス ポイント Web インターフェイスに接続します。

アクセス ポイントは内部で GigabitEthernet1/9 インターフェイスに接続します。すべての Wi-Fi クライアントは GigabitEthernet1/9 ネットワークに属します。使用しているセキュリティ ポリシーにより、Wi-Fi ネットワークが他のインターフェイス上の任意のネットワークにアクセスする方法が決まります。アクセス ポイントには、外部インターフェイスやスイッチ ポートは含まれません。

以下の手順で、アクセス ポイントを設定する方法を説明します。

詳細については、以下のマニュアルを参照してください。

- ワイヤレス LAN コントローラの使用の詳細については、『Cisco Wireless LAN Controller Software documentation』を参照してください。
- ワイヤレス アクセス ポイントのハードウェアおよびソフトウェアの詳細については、Cisco Aironet 700 シリーズのマニュアルを参照してください。

はじめる前に

- ASA 5506W-X デバイスを管理している Firepower Management Center にログインします。この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。

手順

1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択して、Firepower Threat Defense デバイスの編集アイコン（　）をクリックします。

   [インターフェイス（Interfaces）] タブがデフォルトで選択されています。
2. 編集するインターフェイス（今回は、GigabitEthernet1/9）の横にある編集アイコン（　）をクリックします。
   a. [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。
   b. オプションで、[名前（Name）] を追加します。たとえば、AP-FTD などです。
   c. [有効化（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。
   d. 内部インターフェイスと同じゾーンに GigabitEthernet1/9 を追加します。
   e. オプションで、[説明（Description）] を追加します。

f. IP アドレスを設定します。たとえば、192.168.10.2-254 などです。

これは、アクセス ポイント自体の IP アドレスとアクセス ポイント上のクライアントの IP アドレスを指定します。

g. [OK] をクリックします。

3. **[保存（Save）]** をクリックします。
4. [DHCP] をクリックします。
   a. [サーバーの追加（Add Server）] ダイアログ ボックスで [GigabitEthernet1/9] を選択します。
   b. このインターフェイスに以前指定したのと同じ IP アドレス プールを追加します。たとえば、192.168.10.2-254 などです。
   c. [DHCP サーバーの有効化（Enable DHCP Server）] チェック ボックスをオンにして、DHCP サーバーを有効化します。
   d. [OK] をクリックします。
5. **[保存（Save）]** をクリックします。
6. ワイヤレス アクセス ポイントを設定します。

   ワイヤレス アクセス ポイントは、ワイヤレス インターフェイス用に定義された DHCP プールから自身のアドレスを取得します。取得するアドレスは、プール内の最初のアドレスです。サンプル アドレスを使用した場合、該当するアドレスは「192.168.10.2」です。(最初のアドレスが有効でない場合は、プール内の次のアドレスを試してください)。

   a. 新しいブラウザ ウィンドウを使用して、ワイヤレス アクセス ポイントの IP アドレスにアクセスします（例：**http://192.168.10.2**）。アクセス ポイント Web インターフェイスが表示されるはずです。

   このアドレスを開くには、内部ネットワークまたは内部ネットワークにルーティング可能なネットワーク上にいる必要があります。

   b. ユーザ名 **cisco** とパスワード **Cisco** を使用してログインします。
   c. 左側の [簡易設定（Easy Setup）] > [ネットワーク設定（Network Configuration）] をクリックします。
   d. [無線構成（Radio Configuration）] 領域で、[無線 2.4 GHz（Radio 2.4GHz）] セクションおよび [無線 5 GHz（Radio 5GHz）] セクションのそれぞれに対して、少なくとも以下のパラメータを設定し、セクションごとに [適用（Apply）] をクリックします。

   - [SSID]：サービス セット識別子。これはワイヤレス ネットワークの名前です。ユーザが Wi-Fi 接続にワイヤレス ネットワークを選択する際は、この名前が表示されます。
   - [ビーコン内のブロードキャスト SSID（Broadcast SSID in Beacon）]：このオプションを選択します。
   - [ユニバーサル Admin モード（Universal Admin Mode）]：[無効（Disable）]。
   - [セキュリティ（Security）]：使用するセキュリティ オプションを任意に選択します。

7. ワイヤレス アクセス ポイント Web インターフェイスにいる間に、無線を有効にします。
   a. 左側の [概要（Summary）] をクリックし、メイン ページの [ネットワーク インターフェイス（Network Interfaces）] で、2.4 GHz 無線に対応するリンクをクリックします。
   b. [Settings] タブをクリックします。
   c. [無線の有効化（Enable Radio）] 設定で [有効化（Enable）] オプション ボタンをクリックし、ページ下部の [適用（Apply）] をクリックします。
   d. 5 GHz 無線について、上記の手順を繰り返します。

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 Management Center に追加すると、Firepower Management Center ユーザー 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。

ワイヤレス アクセス ポイント構成の復元（ASA 5506W-X）

アクセス ポイントに到達できないときに、Firepower Threat Defense に推奨構成が設定されていて、他のネットワークの問題が見つからない場合は、アクセス ポイントのデフォルト構成を復元できます。Firepower Threat Defense CLI にアクセスする必要があります（コンソール ポートに接続するか、Telnet または SSH アクセスを構成します）。

手順

1. Firepower Threat Defense CLI から、システム サポート CLI メニューに移動します。

   ```
   > system support diagnostic-cli
   ```

   例：

   ```
   > system support diagnostic-cli
   Attaching to ASA console... Press 'Ctrl+a then d' to detach.
   Type help or '?' for a list of available commands.
   firepower>
   ```

2. **enable** コマンドを入力して、特権コマンドを有効にします。

   ```
   firepower> enable
   ```

   enable コマンドを発行すると、システムからパスワードが要求されます。デフォルトでは、パスワードは空白です。

   例：

   ```
   firepower> enable
   Password: <by default, the password is blank>
   firepower#
   ```

3. アクセス ポイントのデフォルト構成を復元するコマンドを入力します。

   ```
   firepower# hw-module module wlan recover configuration
   ```

4. アクセス ポイント CLI については、『Cisco IOS Configuration Guide for Autonomous Aironet Access Points（Aironet 自律アクセス ポイント用の Cisco IOS 構成ガイド）』を参照してください。

ワイヤレス アクセス ポイント コンソールのアクセス（ASA 5506W-X）

コマンドライン インターフェイス（CLI）を使用して、ワイヤレス アクセス ポイントの構成およびモニターができます。Firepower Threat Defense CLI からアクセスします（コンソール ポートに接続するか、Telnet または SSH アクセスを構成します）。

手順

1. Firepower Threat Defense CLI から、システム サポート CLI メニューに移動します。

   ```
   > system support diagnostic-cli
   ```

   例：

   ```
   > system support diagnostic-cli
   ```

```
Attaching to ASA console... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower>
```

2. **enable** コマンドを入力して、特権コマンドを有効にします。

   ```
   firepower> enable
   ```

   enable コマンドを発行すると、システムからパスワードが要求されます。デフォルトでは、パスワードは空白です。

   例：

   ```
   firepower> enable
   Password: <by default, the password is blank>
   firepower#
   ```

3. アクセス ポイントまでのセッション

   ```
   firepower# session wlan console
   ```

   例：

   ```
   firepower# session wlan console
   opening console session with module wlan
   connected to module wlan. Escape character sequence is 'CTRL-^X'

   ap>
   ```

4. アクセス ポイント CLI については、『Cisco IOS Configuration Guide for Autonomous Aironet Access Points (Aironet 自律アクセス ポイント用の Cisco IOS 構成ガイド)』を参照してください。

8. 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。