Firepower Device Manager 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 デバイスに含まれている Firepower Device Manager の Web ベース デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスの初期設定を実行する方法について説明します。

Firepower Device Manager では、小規模ネットワークに最も多く使用されるソフトウェアの基本機能を設定できます。特に、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向けに設計されていて、高性能の多機能デバイス マネージャを使用して多数の Firepower Threat Defense デバイスが含まれる大規模ネットワークを制御する必要のない用途に適しています。

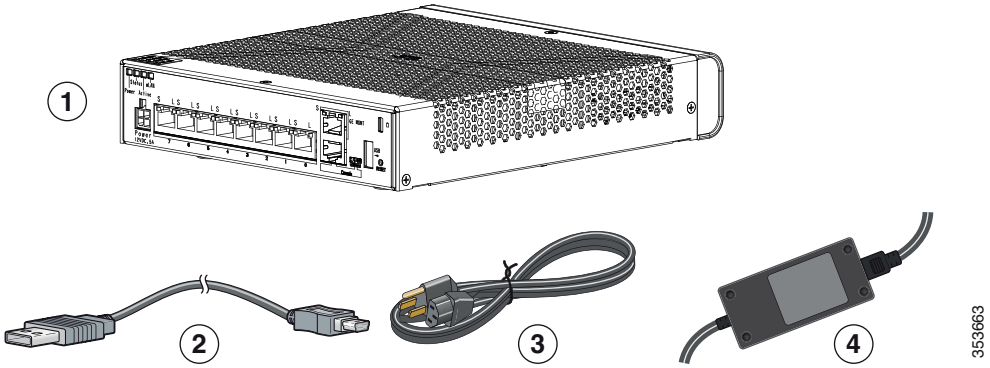
膨大な数のデバイスを管理する場合、または Firepower Threat Defense で対応できる複雑な機能および構成を使用する場合は、一体型の Firepower Device Manager ではなく Firepower Management Center を使用してデバイスを構成してください。

CLI セットアップ ウィザードを使用して、Firepower Threat Defense デバイスのネットワーク接続を設定したり、デバイスを Firepower Management Center に登録にすることができます（http://www.cisco.com/go/ftd-asa-quick 参照）。

2. パッケージの内容

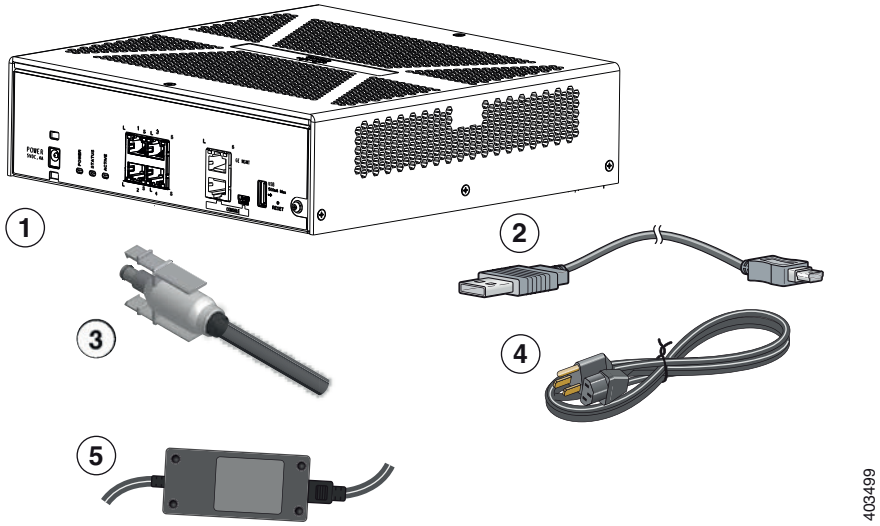
この項では、シャーシのパッケージの内容について説明します。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。

図 1 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

図 2 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

注：Firepower Device Manager を使用して Firepower Threat Defense デバイスを設定するデフォルト設定（内部アドレスと管理アドレスを含む）が、バージョン 6.2 で変更されました。バージョン 6.2 のデフォルト トポロジについては図 3（3 ページ）を、バージョン 6.1 のデフォルト トポロジについては図 4（4 ページ）を参照してください。

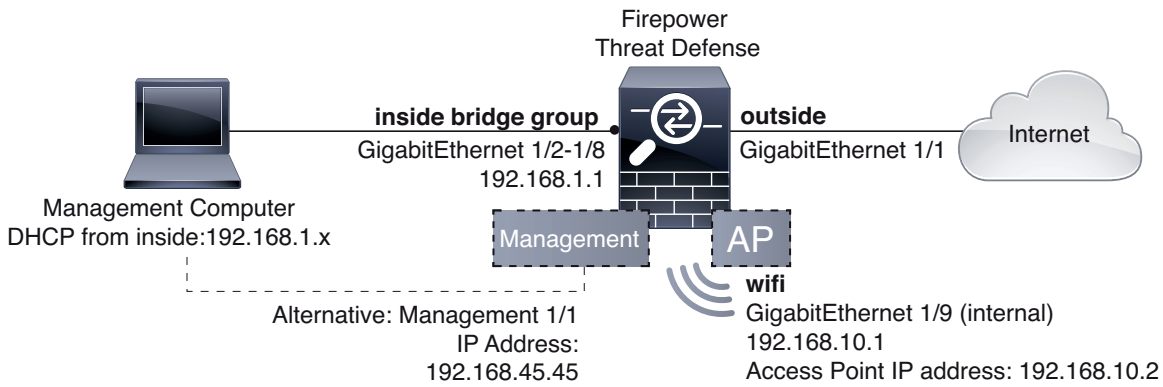
デフォルト設定について（バージョン 6.2）

最初のデータ インターフェイスおよび ASA 5506W-X 上の Wi-Fi インターフェイスを除き、これらのデバイス モデル上の他のすべてのデータ インターフェイスは「内部」のブリッジ グループに構造化されて、有効化されます。内部ブリッジ グループ上に DHCP サーバがあります。エンドポイントまたはスイッチを任意のブリッジ インターフェイスにプラグイン可能で、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。

デフォルト設定およびブリッジされたインターフェイスの必須設定オプションに関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』を参照してください。

次の図は、組み込み型ワイヤレス アクセスポイントを備えた ASA 5506W-X などの ASA 5506-X シリーズ アプライアンスで推奨される Firepower Threat Defense のネットワークの導入を示しています。

図 3　　推奨されるネットワーク配置 - バージョン 6.2



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** DHCP サーバーは内部のブリッジ グループにあります。ブリッジド インターフェイスのいずれかにエンドポイントまたはスイッチを直接接続することができ、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。アクセス ポイント自体およびそのすべてのクライアントの Wi-Fi インターフェイス上に DHCP サーバーがあります。

HTTPS アクセスは、内部のブリッジ グループで有効になるため、デフォルト アドレスの 192.168.1.1 で任意の内部ブリッジ グループ メンバーのインターフェイスを介して Firepower Device Manager を開くことができます。

- また、**Management 1/1** に接続し、Firepower Device Manager を使用してデバイスのセットアップや管理を行うこともできます。DHCP サーバーは管理インターフェイス上にあります。管理コンピュータをこのインターフェイスに直接接続し、192.168.45.0/24 ネットワーク上のアドレスを取得できます。

  HTTPS アクセスは管理インターフェイス上で有効になるため、デフォルト アドレスの 192.168.45.45 で管理インターフェイスを介して Firepower Device Manager を開くことができます。

  管理 IP アドレスのデフォルト ゲートウェイはデータ インターフェイスを使用してインターネットへのルーティングを行います。したがって、Management 物理インターフェイスをネットワークに配線する必要はありません。

  注：物理的な管理インターフェイスは、Management 論理インターフェイスと Diagnostic 論理インターフェイスの間で共有されます。『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Interfaces」の章を参照してください。

- Firepower Threat Defense システムには、ライセンスおよびアップデート用のインターネット アクセスが必要です。システムは、外部インターフェイスのゲートウェイ経由でシステム データベースのアップデートを取得できます。管理ポートまたはネットワークからインターネットまでの明示的なルートを用意する必要はありません。デフォルトでは、データ インターフェイスを介して内部ルートが使用されます。

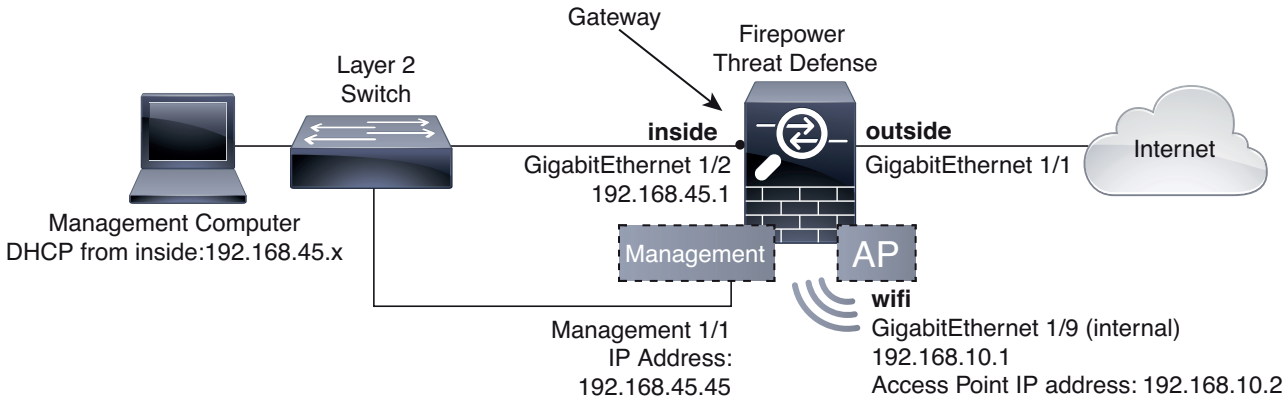
デフォルト設定について（バージョン 6.1）

デフォルト設定は、スイッチを使用して同じネットワークに管理インターフェイスおよび内部インターフェイスを接続すると仮定しています。内部インターフェイスが DHCP サーバーとして設定されているため、同じスイッチに管理ワークステーションを接続し、同じネットワーク上の DHCP を介してアドレスを取得できます。これで、Firepower Device Manager Web インターフェイスを開くことができます。

デフォルト設定に関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』を参照してください。

次の図は、組み込み型ワイヤレス アクセスポイントを備えた ASA 5506W-X などの ASA 5506-X シリーズ アプライアンスで推奨される Firepower Threat Defense のネットワークの導入を示しています。

図 4　推奨されるネットワーク配置 - バージョン 6.1



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。
- **管理 1/1** は、Firepower Device Manager を使用してデバイスのセットアップおよび管理を実行するために使用されます。Firepower Device Manager は、このボックスに含まれるシンプルな単一デバイスのマネージャです。

  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、Management 論理インターフェイスと Diagnostic 論理インターフェイスの間で共有されます。『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Interfaces」の章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ネットワークと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。これらの前提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場合、初期設定は簡単です。ASA 5506-X 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、内部ネットワークに接続された管理コンピュータ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。

バージョン 6.2

図 5　バージョン 6.2 の ASA 5506W-X（Wi-Fi あり）、5506-X（Wi-Fi なし）

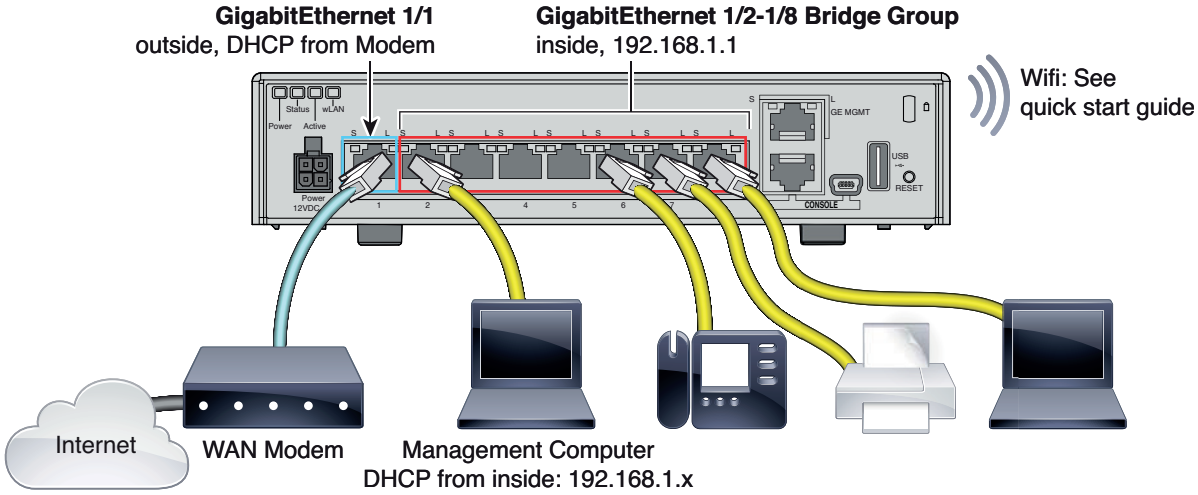
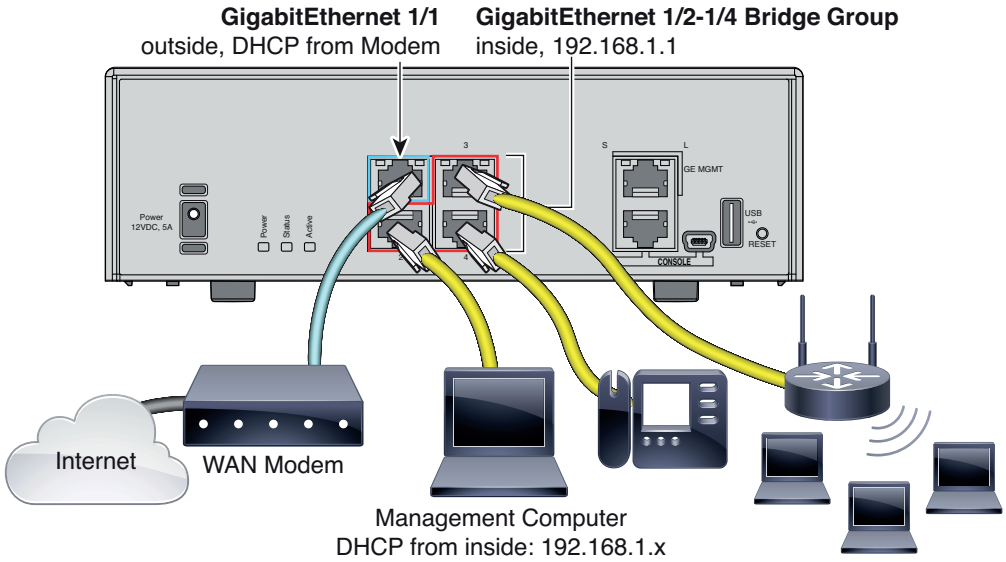


図 6　　バージョン 6.2 の ASA 5506H-X



手順

1. 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。
2. ローカルの管理ワークステーションを GigabitEthernet 1/2（または、内部のブリッジ グループ メンバーのインターフェイス）に接続します。
3. DHCP を使って IP アドレスを取得するようにワークステーションを設定します。ワークステーションは、192.168.1.0/24 ネットワークのアドレスを取得します。

   注：管理ワークステーションを接続する方法には、他にいくつかあります。管理ポートに直接接続することもできます。ワークステーションは、192.168.45.0/24 ネットワークの DHCP を介してアドレスを取得します。別のオプションとして、ワークステーションをスイッチに接続したまま、そのスイッチを GigabitEthernet1/2 などの内部ポートの 1 つに接続することもできます。ただし、スイッチのネットワーク上の他のデバイスが DHCP サーバを実行していないことを確認する必要があります。内部ブリッジグループの 192.168.1.1 で実行しているものと競合するからです。

バージョン 6.1

図 7　バージョン 6.1 の ASA 5506W-X（Wi-Fi あり）、5506-X（Wi-Fi なし）

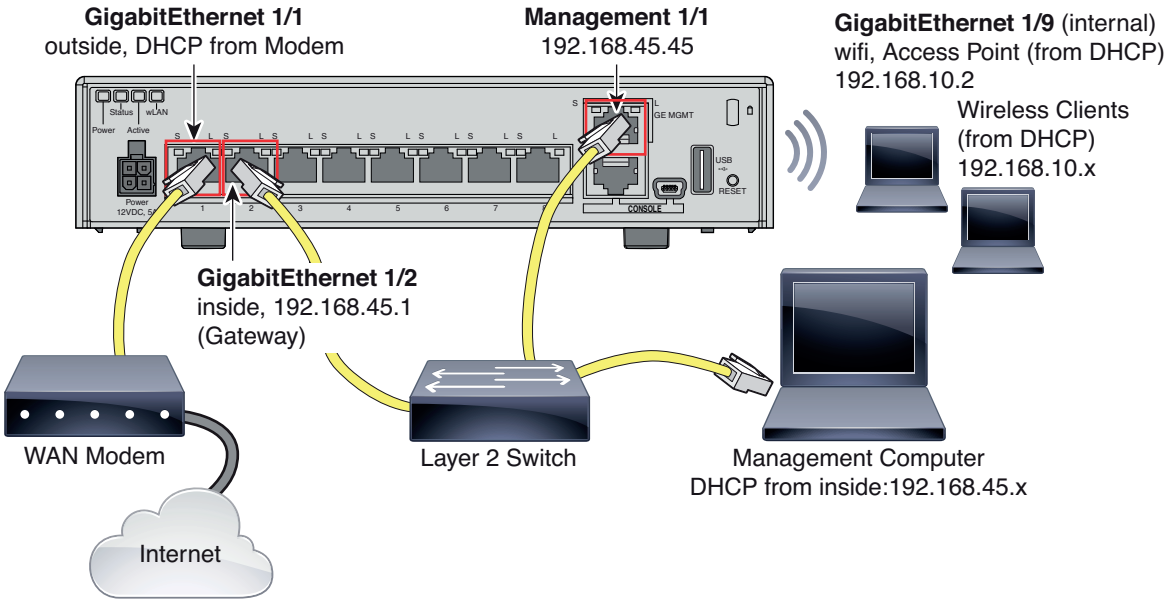
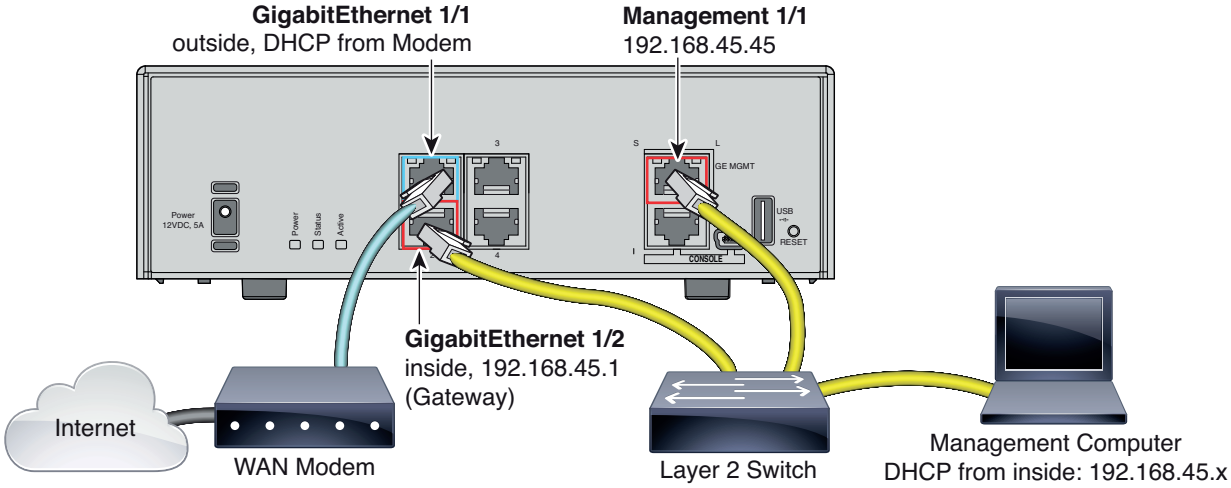


図 8　バージョン 6.1 の ASA 5506H-X



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）
   - 管理 1/1 インターフェイス（Firepower Device Manager 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 Device Manager 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 Device Manager の起動

Firepower Device Manager に初めてログインする際には、デバイスのセットアップ ウィザードを使用してシステムの初期設定を完了します。

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。4. ネットワークへの Firepower Threat Defense の導入（3 ページ）に示したデフォルトの「外部」インターフェイスを使用します。

次に、内部のブリッジ グループに含まれる他のデータ ポートのいずれかに管理コンピュータを接続します。また、Management 物理インターフェイスに接続することもできます。

Management 物理インターフェイスをネットワークに接続する必要はありません。デフォルトでは、システムのライセンスとデータベースおよびその他のアップデートは、インターネットに接続するデータ インターフェイス（通常、外部インターフェイス）経由で取得されます。独立した管理ネットワークを使用する場合は、Management インターフェイスをネットワークに接続し、初期セットアップ完了後に独立した管理ゲートウェイを設定することもできます。

手順

1. ブラウザを開き、Firepower Device Manager にログインします。CLI での初期設定を完了していない場合は、Firepower Device Manager を **https://***ip-address* で開きます。このアドレスは次のいずれかになります。
   - （バージョン 6.2 以降）内部のブリッジ グループ インターフェイスに接続されている場合は **https://192.168.1.1**。
   - （バージョン 6.1）管理物理インターフェイスに接続されている場合は **https://192.168.45.45**。
2. ユーザー名 **admin** とパスワード **Admin123** を使用してログインします。
3. これがシステムへの初めてのログインであり、CLI セットアップウィザードを使用していない場合、エンドユーザライセンス契約を読んで承認し、管理パスワードを変更するように求められます。これらのステップを完了しなければ、次のステップに進めません。
4. 外部インターフェイスと管理インターフェイスについて以下のオプションを設定し、[次へ（Next）] をクリックします。

注：[次へ（Next）] をクリックすると、インターフェイスの設定がデバイスに導入されます。インターフェイスは「outside」という名前で「outside_zone」セキュリティ ゾーンに追加されます。設定値が正しいことを確認します。

a. [外部インターフェイス（Outside Interface）]：これは、ゲートウェイモードまたはルータに接続するためのデータポートです。初期デバイス セットアップ時に、代わりの外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

[IPv4 の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、手動で静的 IP アドレス、サブネット マスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。

[IPv6 の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、手動で静的 IP アドレス、プレフィックス マスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b. **[管理インターフェイス（Management Interface）]**

[DNS サーバ（DNS Servers）]：システムの管理アドレスの DNS サーバ。名前解決に使用する DNS サーバのアドレスを 1 つ以上入力します。デフォルトは、OpenDNS パブリック DNS サーバーです。フィールドを編集した後、デフォルトに戻す場合は、[OpenDNS を使用（Use OpenDNS）] をクリックすると該当する IP アドレスがフィールドにリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

注：デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスを設定する場合は、アウトバウンドとインバウンドのトラフィックに対してシステムから 2 つのデフォルト アクセス ルールが提供されます。初期セットアップ後に、これらのアクセスルールに戻って編集できます。

5. システム時刻を設定し、[次へ（Next）] をクリックします。

a. **[タイムゾーン（Time Zone）]**：システムのタイムゾーンを選択します。

b. **[NTP タイム サーバ（NTP Time Server）]**：デフォルトの NTP サーバを使用するか、手動で NTP サーバのアドレスを入力するかを選択します。バックアップ用に複数のサーバを追加できます。

6. システムのスマート ライセンスを設定します。

システムに必要なライセンスを取得して適用するには、スマート ライセンス アカウントが必要です。最初は 90 日間の評価ライセンスを使用して、後でスマート ライセンスを設定するので構いません。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager アカウントにログインし、新しいトークンを生成して編集ボックスにそのトークンをコピーします。

評価ライセンスを使用するには、**[登録せずに 90 日間の評価期間を開始する（Start 90 day evaluation period without registration）]** を選択します。後でデバイスを登録し、スマートライセンスを取得するには、メニューからデバイスの名前をクリックして **[デバイスダッシュボード（Device Dashboard）]** に進み、[スマートライセンス（Smart Licenses）] グループのリンクをクリックします。

7. [完了（Finish）] をクリックします。

次の作業

デバイス セットアップ ウィザードが完了したら、ポップアップにデバイスを設定するための次のオプションが表示されます。

- 他のインターフェイスをネットワークに接続している場合は、[インターフェイスの設定（Configure Interfaces）] を選択して、接続されているインターフェイスをそれぞれ設定します。
- デフォルトのアクセス ルールを変更する場合は、[ポリシーの設定（Configure Policy）] を選択して、トラフィック ポリシーの設定および管理を行います。

いずれかのオプションを選択するか、またはポップアップを閉じて [デバイスダッシュボード（Device Dashboard）] に戻ることができます。

7. Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- (ASA 5506-X を除く) 外部および内部インターフェイス。その他のデータ インターフェイスは設定されません。
- (ASA 5506-X モデル）外部インターフェイス、および他のすべてのデータ インターフェイスが含まれている内部ブリッジ グループ。
- 内部インターフェイスおよび外部インターフェイスのセキュリティ ゾーン。
- 内部から外部へのトラフィックをすべて信頼するアクセス ルール。
- 内部から外部へのトラフィックをすべて外部インターフェイスの IP アドレスで一意のポートに変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバー。

次の手順では、設定可能なその他の機能の概要を示します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン（**?**）をクリックしてください。

手順

1. **[デバイス（Device）]** を選択してから、**[スマート ライセンス（Smart License）]** グループの **[設定の表示（View Configuration）]** をクリックします。

   オプションの脅威のライセンスを使用する場合は、**[有効化（Enable）]** をクリックします。

   注： ISA 3000 は脅威のライセンスのみサポートします。マルウェアまたは URL フィルタリング ライセンスはサポートしません。したがって、ISA 3000 ではマルウェアや URL フィルタリングのライセンスを必要とする機能は設定できません。

   登録していない場合は、このページから登録できます。**[登録の要求（Request Register）]** をクリックして、手順に従います。評価ライセンスの有効期限が切れる前に登録してください。

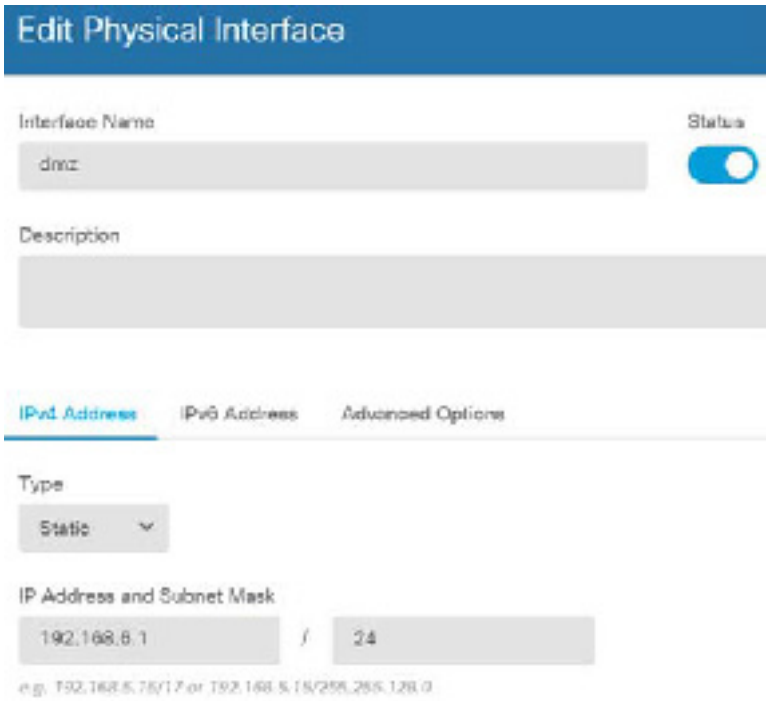
   たとえば、有効な脅威ライセンスは次のようになります。

2. 他のインターフェイスを配線した場合は、**[デバイス（Device）]** を選択してから、**[インターフェイス（Interfaces）]** グループの **[設定の表示（View Configuration）]** をクリックして、配線した各インターフェイスを設定します。

   ASA 5506-X はすべての非外部データ インターフェイスを含むブリッジ グループで事前設定済みのため、これらのインターフェイスを設定する必要はありません。ただし、ブリッジ グループを分割する場合は、ブリッジ グループを編集して個別に扱うインターフェイスを除去できます。その後、別のネットワークをホストするようにこれらのインターフェイスを設定できます。

   その他のモデルの場合は、他のインターフェイス用のブリッジ グループを作成するか、個別ネットワークを設定するか、またはそれらを組み合わせることができます。各インターフェイスの編集アイコンをクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら [保存（Save）] をクリックします。



3. 新しいインターフェイスを設定した場合は、**[オブジェクト（Objects）]** を選択してから、目次から **[セキュリティゾーン（Security Zones）]** を選択します。

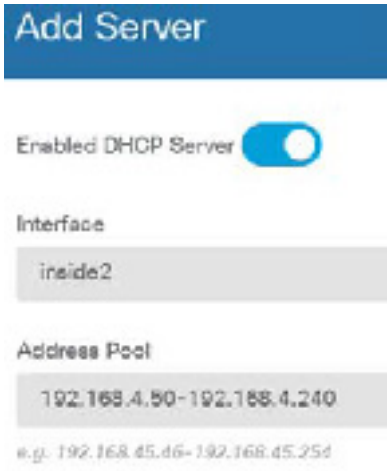
   必要に応じて新しいゾーンを編集または作成します。インターフェイスではなくセキュリティ ゾーンに基づいてポリシーを設定するため、各インターフェイスはゾーンに属している必要があります。インターフェイスの設定中はインターフェイスをゾーンに配置できないため、常に、新しいインターフェイスの作成後または既存のインターフェイスの目的の変更後にゾーン オブジェクトを編集する必要があります。

   次の例は、DMZ インターフェイス用の新しい DMZ ゾーンを作成する方法を示しています。

4. 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DHCP サーバー（DHCP Server）]** を選択してから、[DHCP サーバー（DHCP Servers）] タブを選択します。

   すでに内部インターフェイス用に構成されている DHCP サーバがありますが、アドレス プールを編集したり、それを削除したりすることができます。他の内部インターフェイスを設定する場合、それらのインターフェイスに DHCP サーバを設定するのが非常に一般的です。[+] をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

   [構成（Configuration）] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例は、inside2 インターフェイス上の DHCP サーバをアドレス プール 192.168.4.50-192.168.4.240 を使用して設定する方法を示しています。



5. **[デバイス（Device）]** を選択してから、**[ルーティング（Routing）]** グループで [設定の表示（View Configuration）]（または **[最初のスタティックルートを作成（Create First Static Route）]**）をクリックし、デフォルトルートを構成します。

   デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは any-ipv4（0.0.0.0/0）用で、デフォルトの IPv6 ルートは any-ipv6（::0/0）用です。使用する IP バージョンごとにルートを作成します。DHCP を使用して外部インターフェイスのアドレスを取得している場合は、必要なデフォルト ルートがすでに存在している可能性があります。

   注： このページで定義するルートはデータ インターフェイス専用です。管理インターフェイスには影響しません。[デバイス（Device）] > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** で管理ゲートウェイを設定します。

   次の例に、IPv4 のデフォルト ルートを示します。この例では、isp-gateway は ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです（ISP からアドレスを取得する必要があります）。このオブジェクトは、**[ゲートウェイ（Gateway）]** ドロップダウン リストの下部で **[新しいネットワークの作成（Create New Network）]** をクリックして作成します。

6. **[ポリシー（Policies）]** を選択し、ネットワークのセキュリティ ポリシーを設定します。

   デバイス セットアップ ウィザードにより、内部ゾーンと外部ゾーンの間のトラフィック フロー、および外部インターフェイスに向かうすべてのインターフェイスのインターフェイス NAT が有効になります。新しいインターフェイスを設定する場合でも、そのインターフェイスを内部ゾーン オブジェクトに追加するとアクセス制御ルールが自動的に適用されます。

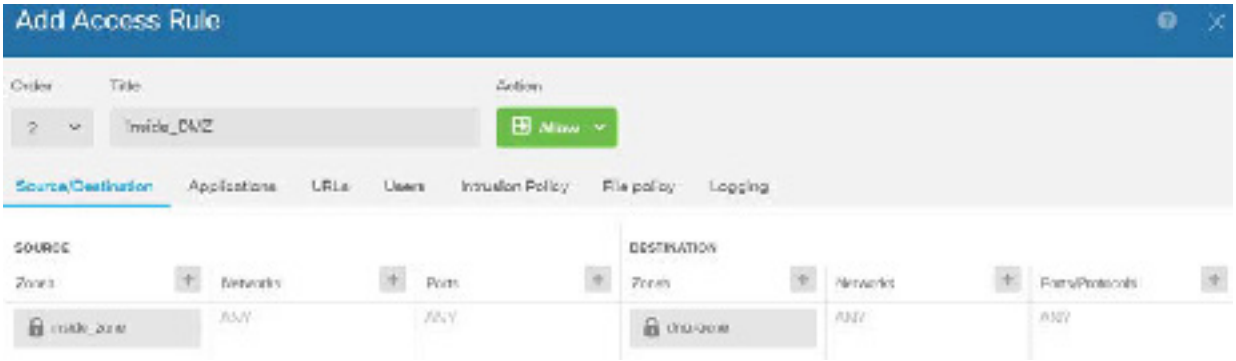
   ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとの双方向トラフィックを許可するルールが必要です。これらは最小限の変更です。

   さらに、追加のサービスを提供するために他のポリシーを設定し、組織が必要とする結果を取得するために NAT およびアクセス ルールを調整することができます。以下のポリシーを設定できます。

   - **[SSL 復号（SSL Decryption）]**：暗号化された接続（HTTPS など）の侵入マルウェアを検査する場合、または URL およびアプリケーション使用ポリシーへのコンプライアンスを適用する場合は、接続を復号化する必要があります。SSL 復号ポリシーを使用して、どの接続を復号する必要があるか判断します。検査後にシステムが接続を再暗号化します。
   - **[アイデンティティ（Identity）]**：個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。
   - **[セキュリティインテリジェンス（Security Intelligence）]**：ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
   - **[NAT]（ネットワーク アドレス変換）**：NAT ポリシーを使用して内部 IP アドレスを外部のルーティング可能なアドレスに変換します。

- **[アクセス制御（Access Control）]**：アクセス制御ポリシーを使用してネットワーク上で許可する接続を決定します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザ グループでフィルター処理できます。また、アクセス コントロール ルールを使用して、侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタ リングを実装します。
- **[侵入（Intrusion）]**：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しても、侵入ポリシーを編集して特定の侵入ルールを有効または無効にすることができます。

次の例は、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間のトラフィックを許可する方法を示しています。この例では、**[接続終了時（At End of Connection）]** が選択されている **[ロギング（Logging）]** 以外のタブではオプションは設定されていません。



7. **[デバイス（Device）]** を選択してから、**[更新（Updates）]** グループで **[設定の表示（View Configuration）]** をクリックし、システムデータベースの更新スケジュールを設定します。

   侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティ ポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

8. メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（ ）をクリックして変更内容をデバイスに展開します。

   変更は、それらを展開するまでデバイスで有効になりません。

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。この手順では、デバイス セットアップ ウィザードを完了していることを前提としています。デバイスを手動で設定した場合は、設定に応じて手順を調整しなければならないことがあります。

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。

手順

1. ワイヤレス インターフェイス GigabitEthernet1/9 を設定して有効化します。
   a. メニューでデバイス名をクリックして **[デバイス ダッシュボード（Device Dashboard）]** に移動し、**[インターフェイス（Interfaces）]** グループのリンクをクリックしてインターフェイスの一覧を開きます。
   b. GigabitEthernet1/9 インターフェイスの編集アイコン（  ）をクリックします。
   c. 次のオプションを設定します。
      - **[インターフェイス名（Interface Name）]**：インターフェイスの名前（**wifi** など）を入力します。
      - **[ステータス（Status）]**：スライダをクリックするとインターフェイスが有効になります。
      - **[Ipv4 アドレス（IPv4 Address）]**：アドレス タイプとして [スタティック（Static）] を選択し、アドレスとサブネット マスクを入力します。たとえば、「192.168.10.1/24」と入力します。
   d. [保存（Save）] をクリックします。
2. Wi-Fi インターフェイスを内部インターフェイスと同じセキュリティ ゾーンに追加します。

   内部インターフェイスは、デバイス セットアップ時に設定し、**inside_zone** という名前のセキュリティ ゾーンに配置してあります。アクセス ポイントの Web インターフェイスに到達できるようにするため、Wi-Fi インターフェイスを同じゾーンに配置する必要があります。
   a. メニューで [オブジェクト（Objects）] をクリックし、目次から [セキュリティ ゾーン（Security Zones）] を選択します。
   b. **inside_zone** の編集アイコン（）をクリックします。
   c. [インターフェイス（Interfaces）] の下の [+] をクリックし、[wifi] インターフェイスを選択します。
3. **inside_zone** セキュリティ ゾーン内のインターフェイス間のトラフィックを許可するアクセス制御ルールを設定します。

   デバイス セットアップ ウィザードにより、**inside_zone** から **outside_zone** に流れるトラフィックを許可するルールが作成されます。これにより、内部ユーザがインターネットにアクセスできるようになります。**wifi** インターフェイスを **inside_zone** に追加することで、インターネット アクセスを許可するルールに Wi-Fi ユーザも含まれることになります。

   ただし、デフォルトのアクションではすべてのトラフィックがブロックされるため、**inside_zone** セキュリティ ゾーン内のインターフェイス間でのトラフィックを有効にするためのルールを作成する必要があります。
   a. メニューで [ポリシー（Policies）] をクリックします。
   b. [アクセス制御（Access Control）] テーブルの上の [+] をクリックします。
   c. ルールでは、少なくとも以下のオプションを設定する必要があります。
      - **[タイトル（Title）]**：ルールの名前を入力します。たとえば、Inside_Inside などと入力します。
      - **[アクション（Action）]**：許可または信頼のいずれか。
      - **[送信元 / 接続先（Source/Destination）]** > **[送信元のゾーン（Source Zones）]**：inside_zone を選択します。
      - **[送信元 / 接続先（Source/Destination）]** > **[接続先のゾーン（Destination Zones）]**：inside_zone を選択します。
   d. **[OK]** をクリックします。
4. ワイアレス インターフェイスに DHCP サーバを設定します。

   DHCP サーバは、アクセス ポイントに接続するデバイスに IP アドレスを割り当てます。また、アクセス ポイント自体にもアドレスを提供します。

a. メニューでデバイス名をクリックして、**[デバイス ダッシュボード（Device Dashboard）]** に移動します。

b. **[システム設定（System Settings）]** > **[DHCP サーバー（DHCP Server）]** をクリックします。

c. DHCP サーバー テーブルの上の [+] をクリックします。

d. 以下の DHCP サーバ プロパティを設定します。

- **[DHCP サーバーの有効化（Enable DHCP Server）]**：スライダをクリックすると、DHCP サーバーが有効になります。
- **[インターフェイス（Interface）]**：**wifi** インターフェイスを選択します。
- **[アドレス プール（Address Pool）]**：DHCP クライアントのアドレス プールを入力します。たとえば、ワイヤレス インターフェイスにサンプル アドレスを使用した場合、プールは 192.168.10.2 ~ 192.168.10.254 になります。プールは、インターフェイスの IP アドレスと同じサブネット上にある必要があり、インターフェイスのアドレスやブロードキャスト アドレスをプールに含めることはできません。

e. **[追加（Add）]** をクリックします。

5. メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（ ）をクリックして変更内容をデバイスに導入します。

導入が完了するまで待機してから続行します。

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。

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 Device Manager を使用した Firepower Threat Defense の管理に関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』、または Firepower Device Manager のオンライン ヘルプを参照してください。