Cisco ASA 5506-X シリーズ クイックスタートガイド

改訂：2022 年 3 月 22 日

Cisco ASA 5506-X シリーズ クイックスタートガイド

Cisco ASA 5506-X シリーズは、強力なデスクトップ ファイアウォールです。

（注） ASA バージョン 9.16 は、ASA 5506-X でサポートされる最終バージョンです。

（注） ASA 5506-X は、バージョン 9.9(x) 以前の ASA FirePOWER モジュールのみをサポートしています。

ライセンス要件

特別な機能を有効化するには、ライセンスが必要です。

ASA ライセンス

ASA 5506-X には、注文されたバージョンに応じて**基本**ライセンスまたは **Security Plus** ライセンスが含まれます。**Security Plus** ライセンスによって、複数のファイアウォール接続、VPN 接続、フェールオーバー機能と VLAN が提供されます。

ライセンスの使用に制限を付ける場合は、**Strong Encryption**（**3DES/AES**）ライセンスもプリインストールします。このライセンスは、アメリカ合衆国の輸出管理ポリシーによって、一部の国では使用可能できません。Strong Encryption ライセンスによって、VPN トラフィックなどの高度に暗号化されたトラフィックが許可されます。無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、https://www.cisco.com/go/license を参照してください。

必要に応じて、**AnyConnect Plus** または **Apex** ライセンスを購入することができます。このライセンスによって、AnyConnect VPN クライアントの接続が許可されます。

基本ライセンスから Security Plus ライセンスへのアップグレード、または AnyConnect ライセンスの購入を希望する場合は、http://www.cisco.com/go/ccw を参照してください。また、『Cisco AnyConnect 発注ガイド』および『AnyConnect 使用許諾によく寄せられる質問（FAQ）』も参照してください。製品認証キー（PAK）が記載された電子メールを受け取ると、ライセンスアクティベーションキーを取得できます。AnyConnect ライセンスの場合、ユーザーセッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。

（注） ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。ライセンスのシリアル番号を表示するには、**show version | grep Serial** コマンドを入力するか、ASDM で [Configuration] > [Device Management] > [Licensing Activation Key] > > ページを参照してください。

ASA FirePOWER ライセンス（ASA 9.9(x) 以前でサポート）

ASA FirePOWER モジュールは、ASA とは別のライセンス メカニズムを使用します。ライセンスはプリインストールされていませんが、次のライセンスのライセンス アクティベーション キーを取得できる PAK がプリントアウトに含めてボックスに同梱されています。

- **Control および Protection**：Control は「Application Visibility and Control（AVC）」または「Apps」とも呼ばれます。Protection は、「IPS」とも呼ばれます。これらの機能を自動的に更新するには、ライセンス用のアクティベーション キーに加え、「使用権」サブスクリプションも必要になります。

  Control（AVC）の更新には、シスコ サポート契約が含まれます。

  Protection（IPS）の更新には、http://www.cisco.com/go/ccw から IPS サブスクリプションを購入する必要があります。このサブスクリプションには、ルール、エンジン、脆弱性、および位置情報を更新する権利が含まれます。
  注：この使用権サブスクリプションは、ASA FirePOWER モジュールの PAK/ライセンス アクティベーション キーの生成や要求はしません。これは、更新を使用する権利を提供するだけです。

購入できるその他のライセンスには、次のものがあります。

- **Advanced Malware Protection（AMP）**
- **URL フィルタリング**

これらのライセンスによって、ASA FirePOWER モジュールの PAK/ライセンス アクティベーション キーが生成されます。詳細については『Cisco Firepower システム機能ライセンス』を参照してください。

Control と Protection のライセンス、およびその他のオプションのライセンスをインストールする方法については、ライセンスのインストール （13 ページ）を参照してください。

ASA 5506W-X ワイヤレス アクセス ポイント

ASA 5506W-X には、ASA に統合されている Cisco Aironet 702i ワイヤレス アクセス ポイントが含まれています。アクセス ポイントは、GigabitEthernet 1/9 インターフェイス上で内部的に ASA に接続します。すべての WiFi クライアントは GigabitEthernet 1/9 ネットワークに属します。ASA 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規定されます。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。

アクセス ポイントには、個々のデバイス管理を可能にする Autonomous Cisco IOS イメージが組み込まれています。ASA 5506W-X を Cisco Unified Wireless Network に追加し、ワイヤレス LAN コントローラを使用する場合は、Lightweight イメージをインストールできます。ユニファイド モードでの Lightweight イメージの使用の詳細については、『シスコ ワイヤレス コントロール構成ガイド』の「自律アクセス ポイントの Lightweight モードへの変換」の章を参照してください。

- サポートされるアクセス ポイント ソフトウェアについては、『Cisco ASA Compatibility』[英語] 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 Series documentation』を参照してください。

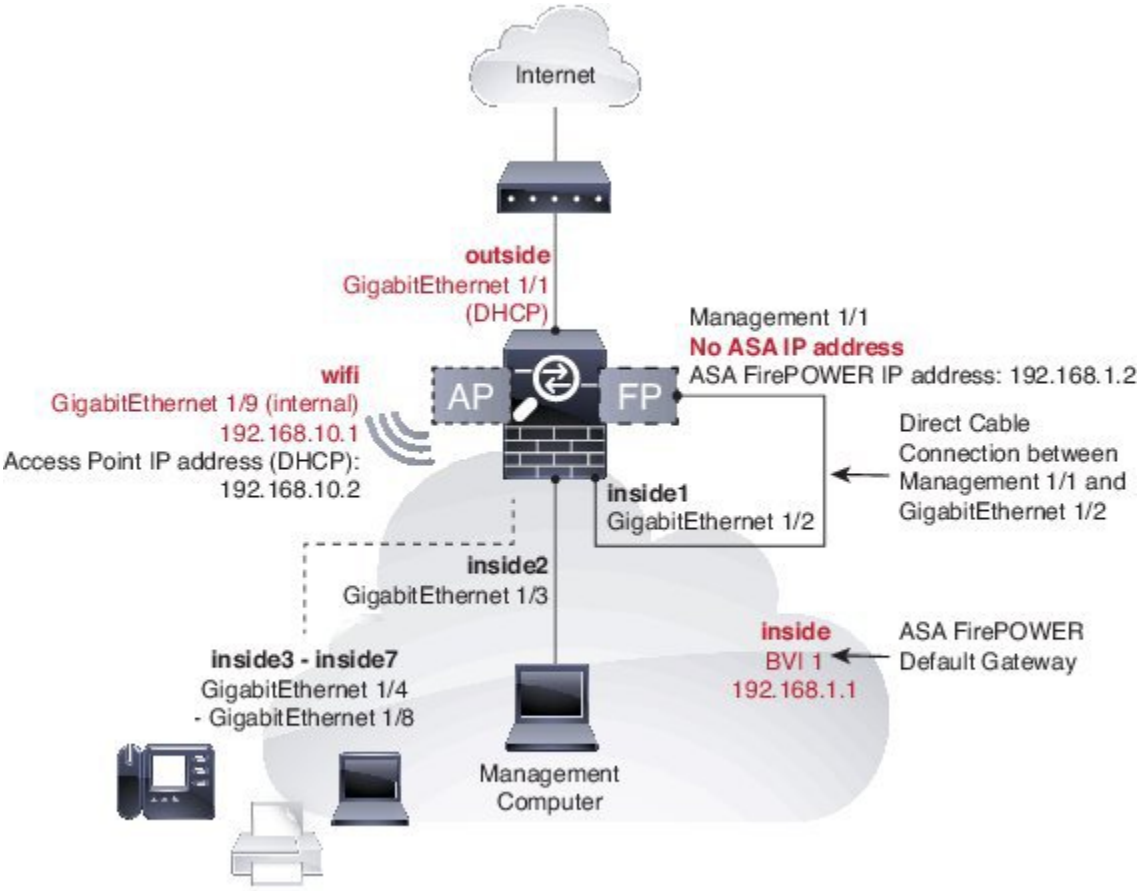
ネットワークでの ASA 5506-X の導入

お使いのバージョンのプロシージャを参照してください。

ASA 9.7 以降

次の図は、ASA FirePOWER モジュール（ASA 9.9(x) 以前でサポート）および組み込みワイヤレスアクセスポイント（ASA 5506W-X）を使用した ASA 5506-X の推奨ネットワーク展開を示しています。この配置には、外部以外のすべてを含む内部ブリッジ グループ（別名ソフトウェア スイッチ）と Wi-Fi インターフェイスが含まれるので、これらのインターフェイスを外部スイッチの代わりとして使用できます。

図 *1 : ASA 5506-x 9.7* 以降のネットワーク



上記のネットワーク配置では、デフォルト設定で、次のような動作が可能になります。

- **外部** GigabitEthernet 1/1 インターフェイス、DHCP からの IP アドレス

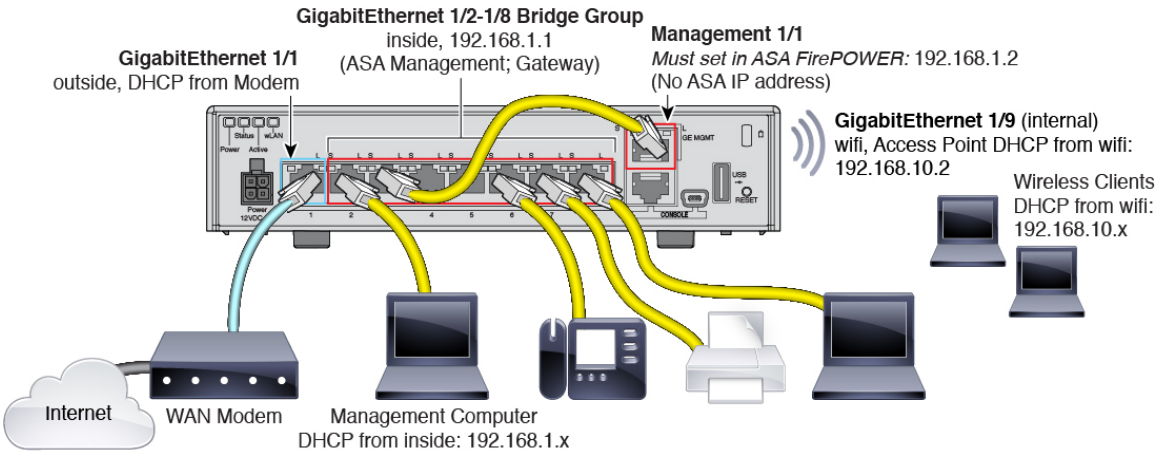
- GigabitEthernet 1/2 ～ 1/8 メンバーインターフェイス（ASA 5506H-X の場合は GigabitEthernet 1/2 ～ 1/4）を含む**内部**ブリッジグループ、192.168.1.1
- （ASA 5506W-X） **Wi-Fi** GigabitEthernet 1/9 インターナル インターフェイス、192.168.10.1
- **内部 --> 外部**トラフィックフロー、これにより内部ユーザーの外部（インターネット）へのアクセスが可能となる
- **内部 --> 内部**メンバーインターフェイスのトラフィックフロー、これによりすべての内部ブリッジ グループ メンバー インターフェイスの通信が可能となる
- （ASA 5506W-X）**Wi-Fi <--> 内部**、**Wi-Fi --> 外部**トラフィック フロー、これにより Wi-Fi ネットワークと内部ネットワークの間の自由な通信が可能となり、Wi-Fi ネットワークの外部（インターネット）へのアクセスが可能となる
- **内部**および **WiFi** 上のクライアントに対する **DHCP** クライアントは、ASA から IP アドレスを受信します。アクセス ポイント自体と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** インターフェイスは、**ASA FirePOWER モジュール**（ASA 9.9(x) 以前でサポート）に属します。これを使用するには、内部または Wi-Fi インターフェイスからの ASA 管理が必要となります。インターフェイスは動作中ですが、それ以外は ASA では未設定です。ASA FirePOWER モジュールは、このインターフェイスを使用して **ASA 内部ネットワークに接続**し、内部インターフェイスを**インターネットへのゲートウェイ**として使用できます。

（注） ASA の設定では、このインターフェイスに IP アドレスを設定しないでください。FirePOWER の設定でのみ IP アドレスを設定してください。ルーティングの観点から、**このインターフェイスは ASA とはまったく別のものとして考慮する**必要があります。

- **内部**インターフェイスおよび **Wi-Fi** インターフェイスの **Adaptive Security Device Manager（ASDM）HTTPS アクセス**
- **ネットワーク アドレス変換（NAT）**：内部、Wi-Fi、および管理から外部へのすべてのトラフィックのインターフェイス ポート アドレス変換（PAT）。プライベートな内部、Wi-Fi、および管理のネットワークから送信された IP アドレスは、パブリックな外部 IP アドレスと固有のポート番号に変換されます。インターネット上ではプライベート IP アドレスはルーティングできませんので、NAT が必要となります。

（注） 内部ネットワーク上に別のルータを配置する場合は、管理と内部の間にルーティングできます。この場合、適切な設定変更を行った Management 1/1 で ASA と ASA FirePOWER モジュールの両方を管理できます。ネットワーク設定とルーティング設定の多くは、代替構成を使用することで可能となります。ただし、管理コンピュータと FirePOWER 管理 IP アドレスの間で NAT を使用する場合は、ASDM を使用して FirePOWER モジュールを管理することはできません（少なくとも、さらに複雑な VPN 設定が必要となります）。自分のコンピュータで ASDM を実行するときは、ASDM はモジュールに設定された実 IP アドレスを使用して FirePOWER モジュールと通信します。代わりに NAT アドレスを指定することはできません。

図 *2:* ケーブル接続



手順

ステップ 1 （ASA 9.9(x) 以前）Management 1/1（ASA FirePOWER モジュールの場合）を GigabitEthernet 1/2 ～ GigabitEthernet 1/8 のいずれかに直接ケーブル接続します。

（注） 管理インターフェイスは ASA FirePOWER モジュールだけに属する別の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は同じネットワークで接続できます。

ステップ 2 コンピュータを GigabitEthernet 1/2 ～ GigabitEthernet 1/8（ASA 5506H-X の場合は GigabitEthernet 1/2 ～ 1/4）のいずれかに配線します。

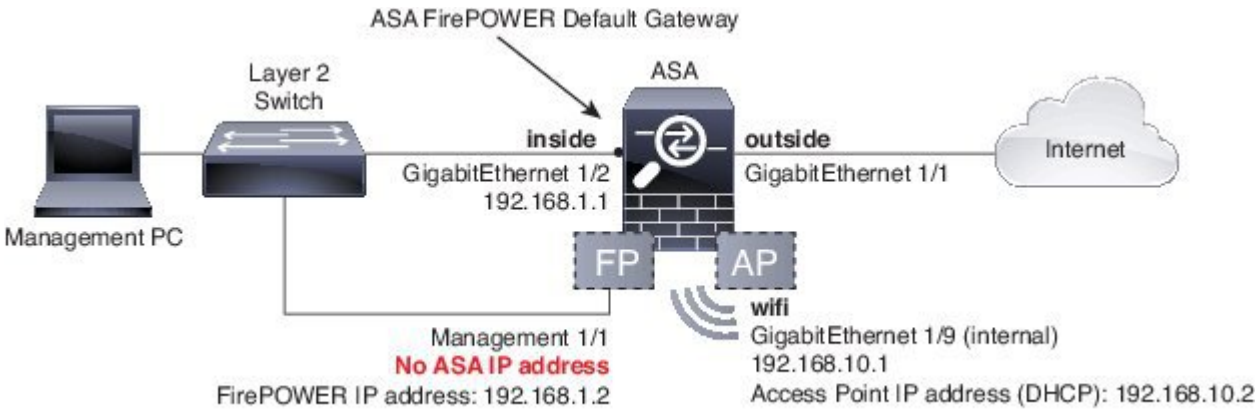
ステップ 3 GigabitEthernet 1/1（外部）を WAN デバイス（たとえばケーブル モデムなど）にケーブル接続します。

（注） ケーブル モデムで 192.168.1.0/24 または 192.168.10.0/24 の外部 IP アドレスが指定された場合、別の IP アドレスを使用するように ASA の設定を変更する必要があります。インターフェイスの IP アドレス、HTTPS（ASDM）アクセス、および DHCP サーバーの設定はすべて、[Startup Wizard] を使用して変更できます。ASDM に接続している IP アドレスを変更すると、ウィザードの終了時に切断されます。新しい IP アドレスに再接続する必要があります。

ASA 9.6 以前

次の図は、ASA FirePOWER モジュールおよび組み込みワイヤレス アクセス ポイント（ASA 5506W-X）を使用した ASA 5506-X の推奨ネットワーク展開を示しています。

図 *3 : ASA 5506-x 9.6* 以前のネットワーク



（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。

上記のネットワーク配置では、デフォルト設定で、次のような動作が可能になります。

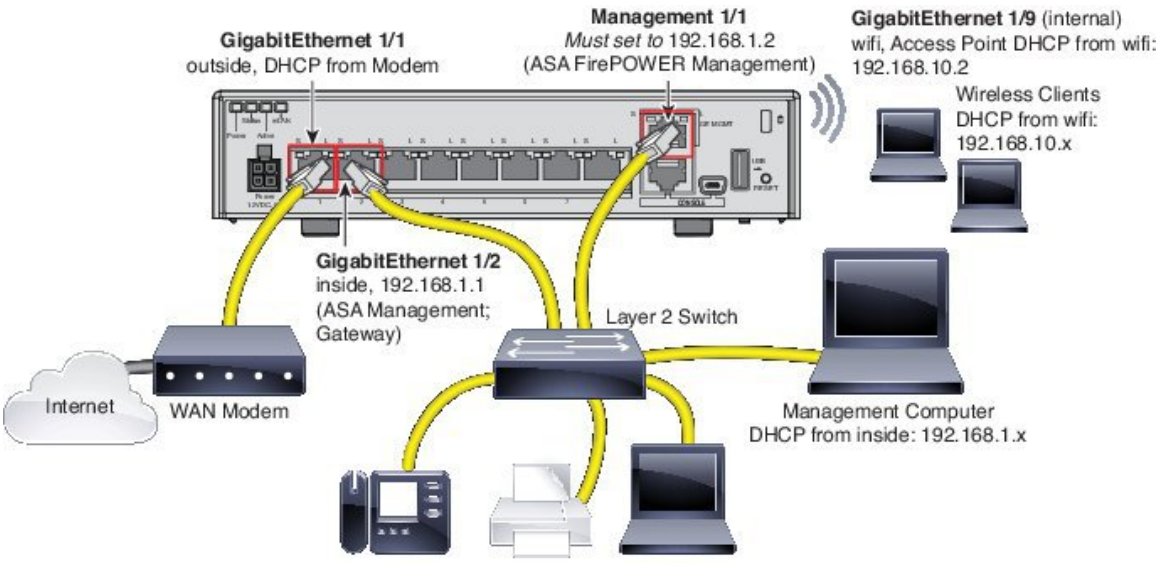
- **外部** GigabitEthernet 1/1 インターフェイス、DHCP からの IP アドレス
- **内部** GigabitEthernet ½ インターフェイス、192.168.1.1
- （ASA 5506W-X） **Wi-Fi** GigabitEthernet 1/9 インターナル インターフェイス、192.168.10.1
- **内部 --> 外部**トラフィックフロー、これにより内部ユーザーの外部（インターネット）へのアクセスが可能となる
- （ASA 5506W-X）**Wi-Fi <--> 内部**、**Wi-Fi --> 外部**トラフィック フロー、これにより Wi-Fi ネットワークと内部ネットワークの間の自由な通信が可能となり、Wi-Fi ネットワークの外部（インターネット）へのアクセスが可能となる
- **内部**および **WiFi** 上のクライアントに対する **DHCP** クライアントは、ASA から IP アドレスを受信します。アクセス ポイント自体と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、**ASA FirePOWER モジュール**に属します。これを使用するには、内部または Wi-Fi インターフェイスからの ASA 管理が必要となります。インターフェイスは動作中ですが、それ以外は ASA では未設定です。ASA FirePOWER モジュールは、このインターフェイスを使用して **ASA 内部ネットワークに接続**し、内部インターフェイスを**インターネットへのゲートウェイ**として使用できます。

（注） ASA の設定では、このインターフェイスに IP アドレスを設定しないでください。FirePOWER の設定でのみ IP アドレスを設定してください。ルーティングの観点から、**このインターフェイスは ASA とはまったく別のものとして考慮する**必要があります。

- **内部**インターフェイスおよび **Wi-Fi** インターフェイスの **Adaptive Security Device Manager（ASDM）HTTPS アクセス**
- **ネットワーク アドレス変換（NAT）**：内部、Wi-Fi、および管理から外部へのすべてのトラフィックのインターフェイス ポート アドレス変換（PAT）。プライベートな内部、Wi-Fi、および管理のネットワークから送信された IP アドレスは、パブリックな外部 IP アドレスと固有のポート番号に変換されます。インターネット上ではプライベート IP アドレスはルーティングできませんので、NAT が必要となります。

（注） 内部ネットワーク上に別のルータを配置する場合は、管理と内部の間にルーティングできます。この場合、適切な設定変更を行った Management 1/1 で ASA と ASA FirePOWER モジュールの両方を管理できます。ネットワーク設定とルーティング設定の多くは、代替構成を使用することで可能となります。ただし、管理コンピュータと FirePOWER 管理 IP アドレスの間で NAT を使用する場合は、ASDM を使用して FirePOWER モジュールを管理することはできません（少なくとも、さらに複雑な VPN 設定が必要となります）。自分のコンピュータで ASDM を実行するときは、ASDM はモジュールに設定された実 IP アドレスを使用して FirePOWER モジュールと通信します。代わりに NAT アドレスを指定することはできません。

図 *4*: ケーブル接続



手順

ステップ 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（ASA FirePOWER モジュール用）
- コンピュータ

（注） 管理インターフェイスは ASA FirePOWER モジュールだけに属する別の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は同じネットワークで接続できます。

ステップ 2 GigabitEthernet 1/1（外部）を WAN デバイス（たとえばケーブル モデムなど）にケーブル接続します。

（注） ケーブル モデムで 192.168.1.0/24 または 192.168.10.0/24 の外部 IP アドレスが指定された場合、別の IP アドレスを使用するように ASA の設定を変更する必要があります。インターフェイスの IP アドレス、HTTPS（ASDM）アクセス、および DHCP サーバーの設定はすべて、[Startup Wizard] を使用して変更できます。ASDM に接続している IP アドレスを変更すると、ウィザードの終了時に切断されます。新しい IP アドレスに再接続する必要があります。

ASA の電源投入

ASA の電源を投入し、電源入力の進行状況を確認します。

手順

ステップ 1 電源コードを ASA 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。

ステップ 2 ASA 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。

ステップ 3 ASA 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。

ワイヤレス アクセス ポイント（ASA 5506W-X）を有効化します。

ASA 5506W-X ワイヤレス アクセス ポイントは、デフォルトで無効化されています。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 GUI に接続してください。

始める前に

この手順では、デフォルト設定を使用する必要があります。

手順

ステップ 1 ASA 内部ネットワークに接続されているコンピュータで、Web ブラウザを起動します。

ステップ 2 [Address] フィールドに http://192.168.10.2 と入力します。ユーザー名とパスワードの入力を求められます。

（注） アクセス ポイントに到達できないときに、ASA はデフォルト設定のままで、他のネットワーク問題が見つからない場合、アクセス ポイントをデフォルト設定に復元することができます。ASA CLI にアクセスする必要があります（ASA のコンソール ポートに接続するか、ASDM を使用して Telnet または SSH アクセスを設定します）。ASA CLI から、**hw-module module wlan recover configuration** を入力します。アクセスポイントをさらにトラブルシューティングする必要がある場合は、**session wlan console** コマンドを使用してアクセスポイント CLI に接続します。

ステップ 3 ユーザー名 **cisco** とパスワード **Cisco** を入力します。アクセス ポイント GUI が表示されます。

ステップ 4 左側の [Easy Setup] > [Network Configuration] > をクリックします。

ステップ 5 [Radio Configuration] 領域で、[Radio 2.4GHz] セクションおよび [Radio 5GHz] セクションのそれぞれに対して、次のパラメータを設定し、セクションごとに [Apply] をクリックします。

- **SSID**
- **Broadcast SSID in Beacon**
- **Universal Admin Mode**：**Disable**
- **Security** （お客様が選択）

ステップ 6 左側の [Summary] をクリックし、メインページの [Network Interfaces] で [2.4 GHz] 無線に対応するホットリンクをクリックします。

ステップ 7 [Settings] タブをクリックします。

ステップ 8 [Enable Radio] の設定では、[Enable] ラジオボタンをクリックし、ページ下部の [Apply] をクリックします。

ステップ 9 手順を繰り返して [5 GHz] 無線を設定します。

ステップ 10 詳細については、次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 Series documentation』を参照してください。

ASDM の起動

ここでは、ASA FirePOWER モジュール（ASA 9.9(x) 以前でサポート）を管理するために、ASDM を使用することを前提としています。Firepower Management Center を使用する場合は、モジュール CLI に接続し、セットアップ スクリプトを実行する必要があります。『ASA FirePOWER クイック スタート ガイド』を参照してください。ASA 9.10(x) 以降では、FirePOWER モジュールに関連する手順はすべて無視してください。

始める前に

ASDM を実行するための要件については、Cisco.com の『ASDM リリース ノート』を参照してください。

手順

ステップ 1 ASA に接続されているコンピュータで、Web ブラウザを起動します。

ステップ 2 [Address] フィールドに URL https://192.168.1.1/admin を入力します。[Cisco ASDM] Web ページが表示されます。

管理コンピュータをワイヤレス クライアントとして ASA に接続した場合は、https://192.168.10.1/admin で ASDM にアクセスできます。

ステップ 3 使用可能なオプション（[Install ASDM Launcher] 、[Run ASDM] 、[Run Startup Wizard]） のいずれかをクリックします。

ステップ 4 画面の指示に従ってオプションを選択し、ASDM を起動します。[Cisco ASDM-IDM Launcher] が表示されます。

ステップ 5 ユーザー名とパスワードのフィールドを空のまま残し、[OK] をクリックします。メイン ASDM ウィンドウが表示されます。

（注） **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** ページにログインした後、特権（イネーブル）モードのパスワードを変更します。

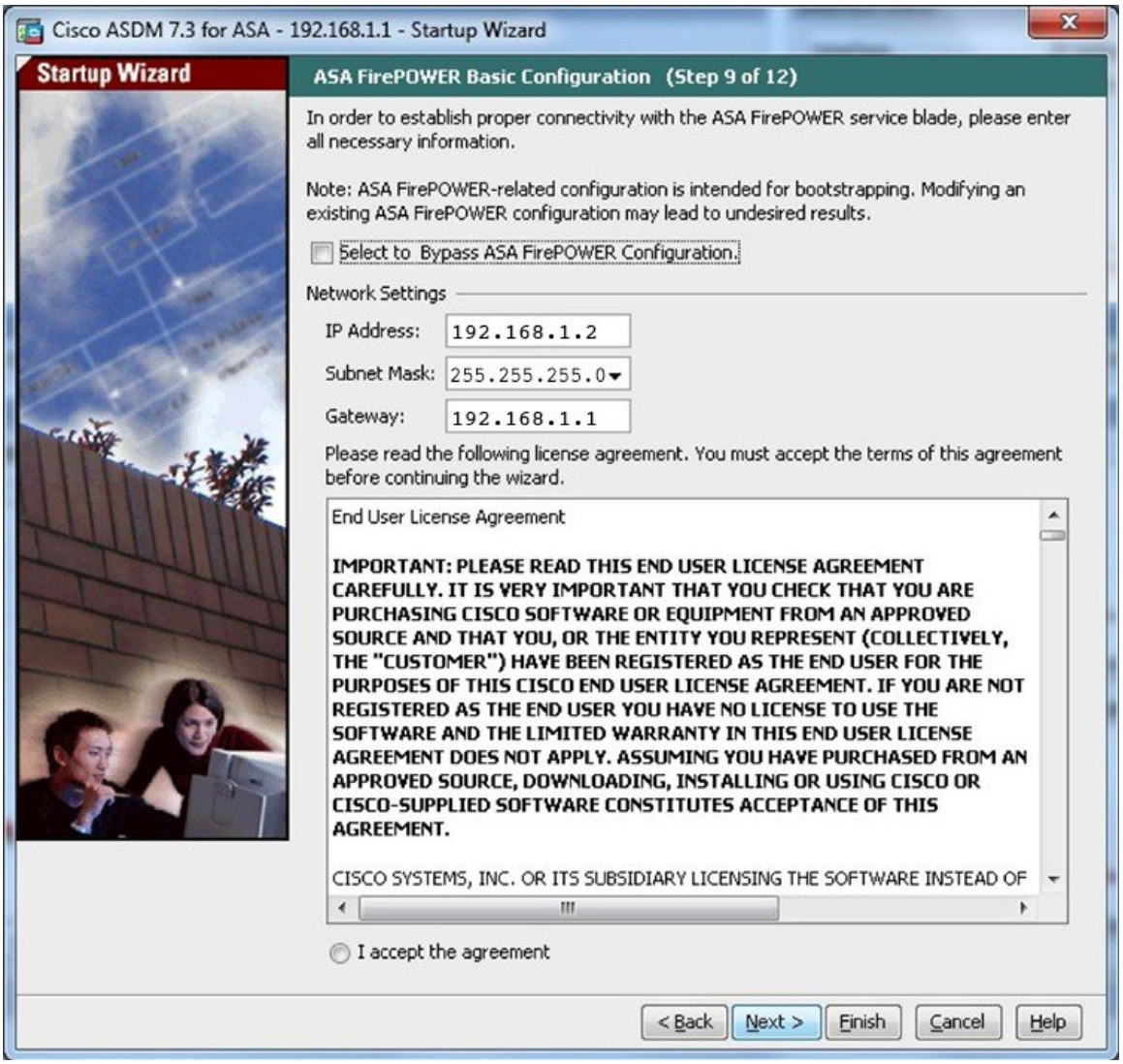
ステップ 6 インストールする ASA FirePOWER モジュールの IP アドレスを指定するよう求められた場合は、ダイアログボックスをキャンセルします。[Startup Wizard] を使用して、まず、モジュールの IP アドレスを正しい IP アドレスに設定する必要があります。

ASDM は ASA バックプレーンを介して ASA FirePOWER モジュールの IP アドレス設定を変更できます。ただし、モジュールを管理するには、ネットワークを介して Management 1/1 インターフェイス上のモジュール（および新しい IP アドレス）にアクセスする必要があります。推奨される展開ではモジュールの IP アドレスが内部ネットワークに存在するため、このアクセスが可能です。IP アドレスを設定した後に ASDM がネットワーク上のモジュールに到達できない場合は、エラーが表示されます。

ステップ 7 [ウィザード（Wizards）] > [スタートアップ ウィザード（Startup Wizard）] を選択します。

ステップ 8 必要に応じて追加の ASA 設定を行うか、または、[ASA FirePOWER Basic Configuration] 画面が表示されるまで、画面を進みます。

図 *5 : ASDM* スタートアップ ウィザード



デフォルト設定を使用するには、次の値を設定します。

- [IP Address]： 192.168.1.2
- [Subnet Mask] ：255.255.255.0
- [Gateway]：192.168.1.1

ステップ 9 [I accept the agreement] をクリックして、[Next] または [Finish] をクリックすると、ウィザードが終了します。

ステップ 10 ASDM を終了し、再起動します。[Home] ページに [ASA FirePOWER] タブが表示されます。

他の ASDM ウィザードおよび詳細設定の実行

ASDMには、セキュリティポリシーを設定するためのウィザードが多数含まれています。使用可能なすべてのウィザードを見るには、[Wizards] メニューを参照してください。

ASA の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェア バージョンに応じたマニュアルを参照してください。

ASA FirePOWER モジュールの設定（ASA 9.9(x) 以前でサポート）

ASDM を使用してライセンスをインストールし、モジュールのセキュリティ ポリシーを設定して、モジュールにトラフィックを送信します。

（注） または、Firepower Management Center を使用して、ASA FirePOWER モジュールを管理できます。詳細については、『ASA FirePOWER Module Quick Start Guide』を参照してください。

手順

ステップ 1 ライセンスのインストール （13 ページ）。

ステップ 2 ASA FirePOWER セキュリティ ポリシーの設定 （14 ページ）。

ステップ 3 ASA から ASA FirePOWER モジュールへのトラフィックの送信 （14 ページ）。

ライセンスのインストール

Control および Protection のライセンスはデフォルトで提供されており、製品認証キー（PAK）を含むプリントアウトがボックスに同梱されています。追加ライセンスを発注した場合は、これらのライセンス用の PAK が電子メールに記載されています。

手順

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Licenses] > > を選択し **[Add New License]** をクリックして、ご使用のシャーシに対応するライセンス キーを取得します。

ライセンス キーは上部付近にあり、たとえば 72:78:DA:6E:D9:93:35 です。

ステップ 2 [Get License] をクリックして、ライセンス ポータルを起動します。または、ブラウザで次の URL に移動します。 https://www.cisco.com/go/license

ステップ 3 カンマで区切られた PAK を [Get New Licenses] フィールドに入力し、[Fulfill] をクリックします。

ステップ 4 ライセンス キーや電子メールアドレスなどのフィールドに入力します。

ステップ 5 Webサイトの表示からか、システムが自動的に配信するライセンスの電子メールに添付されているzipファイルから、結果のライセンス アクティベーション キーをコピーします。

ステップ 6 ASDM の **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Licenses]** > **[Add New License]** 画面に戻ります。

ステップ 7 [License] ボックスにライセンス アクティベーション キーを貼り付けます。

ステップ 8 [Verify License] をクリックしてテキストを正しくコピーしたことを確認し、確認後に [Submit License] をクリックします。

ステップ 9 [Return to License Page] をクリックします。

ASA FirePOWER セキュリティ ポリシーの設定

ASA から ASA FirePOWER モジュールに送信するトラフィックのセキュリティ ポリシーを設定します。

手順

ASA FirePOWER セキュリティ ポリシーを設定するために [Configuration] > [ASA FirePOWER Configuration] > を選択します。

ASA FirePOWER セキュリティ ポリシーの詳細については、ASDM の [ASA FirePOWER] ページを使用します。ポリシーの設定方法について詳しく知るには、任意のページで [Help] をクリックするか、または [Help] > [ASA FirePOWER ヘルプ トピック（ASA FirePOWER Help Topics）] > を選択します。

『ASA FirePOWER module configuration guide』も参照してください。

ASA から ASA FirePOWER モジュールへのトラフィックの送信

ASA FirePOWER モジュールにトラフィックを送信するように ASA を設定します。

手順

ステップ 1 [Configuration] > [Firewall] > [Service Policy Rules] > > の順に選択します。

ステップ 2 [Add] > [Add Service Policy Rule] > を選択します。

ステップ 3 ポリシーを特定のインターフェイスに適用するか、または全体的に適用するかを選択し、[Next] をクリックします。

ステップ 4 トラフィックの一致を設定します。たとえば、インバウンドのアクセス ルールを通過したすべてのトラフィックがモジュールへリダイレクトされるように、一致を [Any Traffic] に設定できます。また、ポート、ACL（送信元と宛先の基準）、または既存のトラフィック クラスに基づいて、より厳密な基準を定義することもできます。このポリシーでは、その他のオプションはあまり有用ではありません。トラフィック クラスの定義が完了したら、[Next] をクリックします。

ステップ 5 [Rule Actions] ページで [ASA FirePOWER Inspection] タブをクリックします。

ステップ 6 [Enable ASA FirePOWER for this traffic flow] チェックボックスをオンにします。

ステップ 7 [ASA FirePOWER Card Fails] 領域で、次のいずれかをクリックします。

- [Permit traffic] ：モジュールが使用できない場合、すべてのトラフィックの通過を検査なしで許可するように ASA を設定します。
- [Close traffic] ：モジュールが使用できない場合、すべてのトラフィックをブロックするように ASA を設定します。

ステップ 8 （任意） トラフィックの読み取り専用のコピーをモジュールに送信する（つまりパッシブ モードにする）には、[Monitor-only] をオンにします。

ステップ 9 [Finish]、[Apply] の順にクリックします。

ステップ 10 この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

次の作業

- ASA の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェア バージョンに応じたマニュアルを参照してください。
- （ASA 9.9(x) 以前）ASA FirePOWER モジュールと ASA 操作の詳細については、『ASA/ASDM のファイアウォール設定ガイド』の「ASA FirePOWER モジュール」の章、または ASDM のオンラインヘルプを参照してください。
- （ASA 9.9(x) 以前）ASA FirePOWER 設定の詳細については、オンラインヘルプ、『ASA FirePOWER モジュール構成ガイド』、またはご使用のバージョンの『Firepower Management Center 構成ガイド』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/