



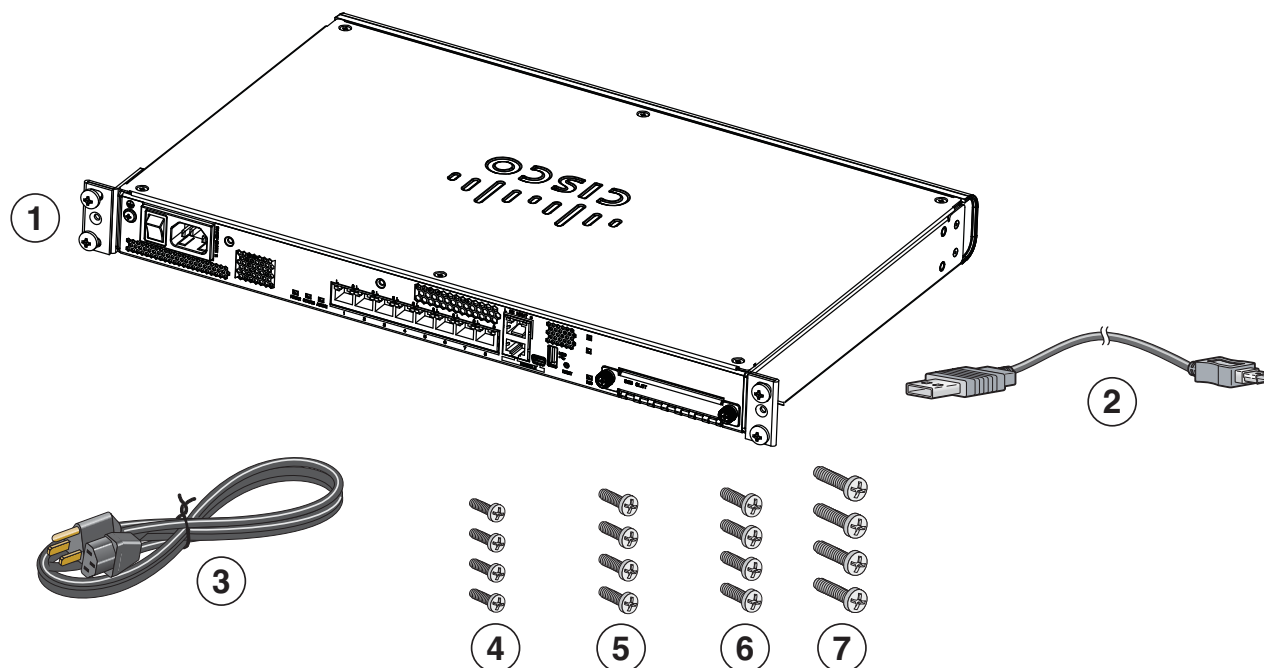
Cisco ASA 5508-X および ASA 5516-X 向けクイック スタート ガイド

初版:2015 年 4 月 7 日

最終更新日:2016 年 5 月 11 日

1. 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ります。ご注意ください。



353664

1	ASA 5508-X または ASA 5516-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	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)		

2. ライセンス要件

ASA ライセンス

ASA 5508-X または ASA 5516-X には、**基本**ライセンスがデフォルトで含まれています。使用資格を満たした場合は、**Strong Encryption (3DES/AES)** ライセンスも一緒に含まれます。また、次のライセンスを購入することもできます。

- セキュリティ コンテキスト
- AnyConnect Plus または Apex

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、<http://www.cisco.com/go/license> を参照してください。

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される場合は、<http://www.cisco.com/go/ccw> を参照してください。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 の [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 FirePOWER モジュールは、ASA とは別個のライセンス メカニズムを使用します。事前にインストールされているライセンスはありませんが、次のライセンス用のライセンス アクティベーション キーを取得できる印刷した PAK が箱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 キーの生成も要求もしません。これは、更新を使用する権利を提供するものです。

購入可能なその他のライセンスには、以下が含まれます。

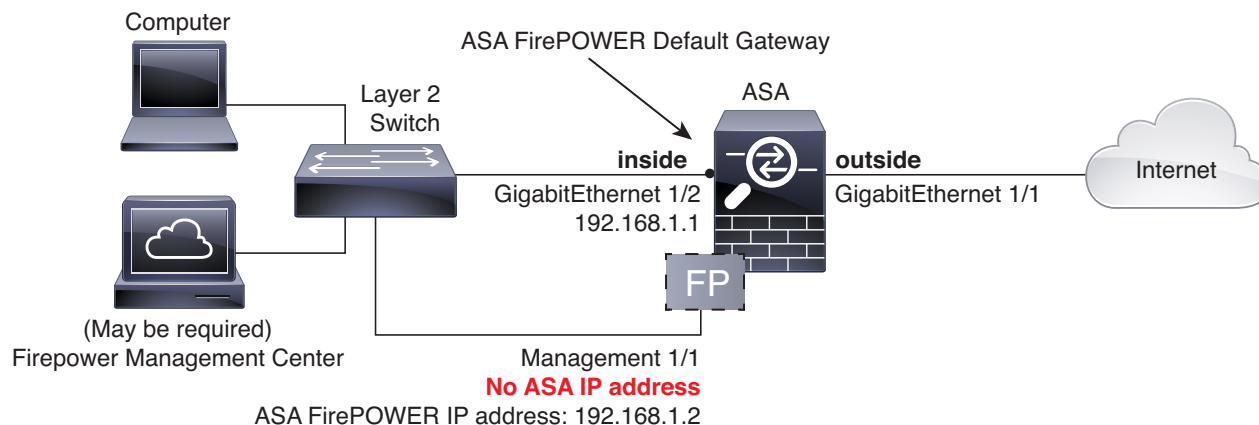
- **Advanced Malware Protection (AMP)**
- **URL フィルタリング**

これらのライセンスは、ASA FirePOWER モジュール用の PAK/ライセンス アクティベーション キーを生成します。発注情報については、『Cisco ASA with FirePOWER Services Ordering Guide』を参照してください。また、『Cisco Firepower System Feature Licenses』[英語] も参照してください。

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](#)、6ページを参照してください。

3. ネットワークでの ASA 5508-X または ASA 5516-X の導入

次の図に、ASA FirePOWER モジュールを使用した ASA 5508-X または ASA 5516-X の推奨ネットワーク配置を示します。



(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。

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。

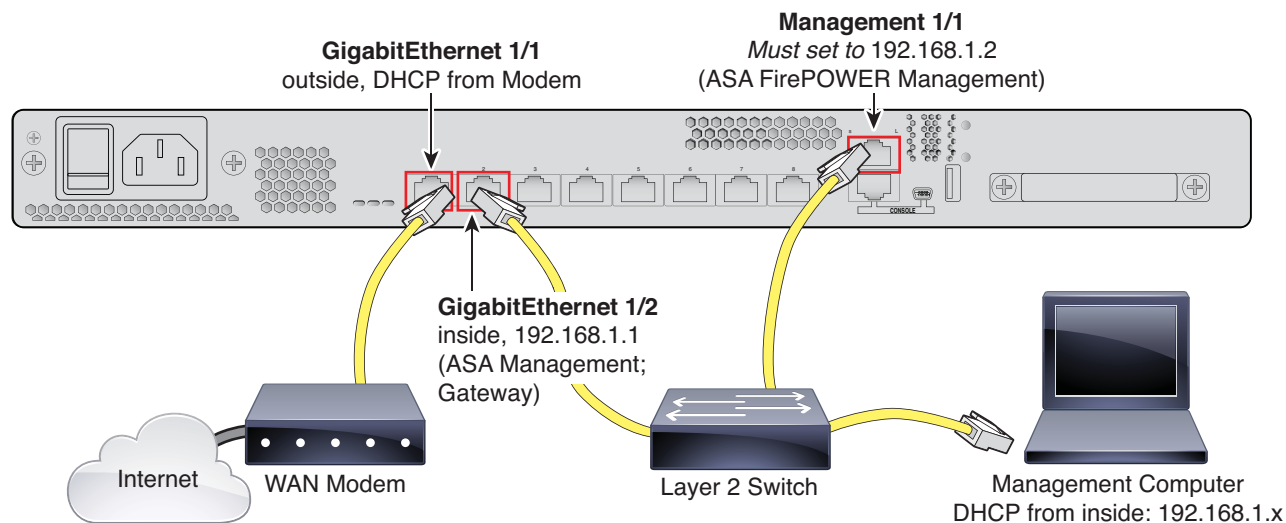
- 内部 --> 外部へのトラフィック フロー
- DHCP からの外部 IP アドレス
- 内部上のクライアントに対する DHCP。
- 管理 1/1 は ASA FirePOWER モジュールに属します。インターフェイスは動作中ですが、それ以外は ASA では未設定です。ASA FirePOWERモジュールは、このインターフェイスを使用してASA内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。

(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上での ASDM アクセス

(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管理 1/1 で ASA と ASA FirePOWER モジュールの両方を管理できます。

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)
- 管理 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。

2. GigabitEthernet 1/1 (外部) インターフェイスを WAN デバイス (たとえばケーブル モデムなど) に接続します。

注: ケーブル モデムで 192.168.1.0/24 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。

4.ASA の電源投入

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。
2. ASA の背面にある電源ボタンを押します。
3. ASA 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. ASA 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。

5.ASDM の起動

ASDM を実行するための要件については、Cisco.com の『[ASDM release notes](#)』を参照してください。

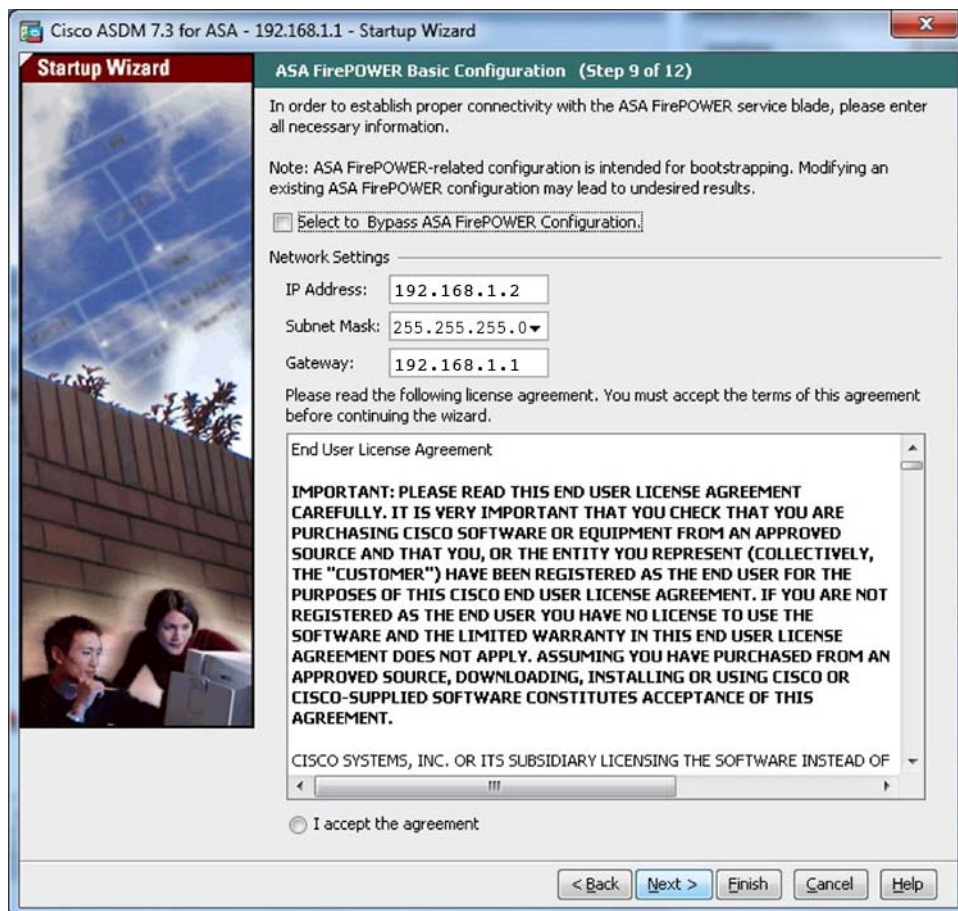
(注) ここでは、ASA FirePOWER モジュールを管理するために、ASDM を使用することを前提としています。FireSIGHT システムを使用する場合は、モジュール CLI に接続し、セットアップ スクリプトを実行する必要があります。『[ASA FirePOWER quick start guide](#)』[英語] を参照してください。

手順

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。
2. [Address] フィールドに <https://192.168.1.1/admin> という URL を入力します。[Cisco ASDM] Web ページが表示されます。
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。
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。
[Install ASDM Launcher] をクリックした場合、場合によっては、『[Install an Identity Certificate for ASDM](#)』[英語] に従って ASA の ID 証明書と ASA FirePOWER モジュールの証明書をそれぞれインストールすることが必要になります。
5. ユーザ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。
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管理 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。

7. [Wizards] > [Startup Wizard] を選択します。
8. 必要に応じて追加の ASA 設定を行うか、または ASA FirePOWER の [Basic Configuration] 画面が表示されるまで画面を進みます。



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

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。
10. ASDM を終了し、再起動します。ホームページに ASA FirePOWER のタブが表示されます。

6.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。

7.ASA FirePOWER モジュールの設定

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:別の方法として、Firepower Management Centerを使用して ASA FirePOWER モジュールを管理することもできます。詳細については、『ASA FirePOWER Module Quick Start Guide』[英語] を参照してください。

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ます。印刷した製品認証キー (PAK) が箱に同梱されています。追加ライセンスを発注する場合、電子メールにそのライセンスの PAK を記載する必要があります。

手順

1. [Configuration] > [ASA FirePOWER Configuration] > [Licenses] の順に選択し、[Add New License] をクリックすることによって、シャシのライセンス キーを取得します。
ライセンス キーは、上部付近にあります (例: 72:78:DA:6E:D9:93:35)。
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。あるいは、ブラウザで <http://www.cisco.com/go/license> に移動します。
3. [Get New Licenses] フィールドにカンマで区切られた PAK を入力し、[Fulfill] をクリックします。
4. その他のフィールドでライセンス キーと電子メール アドレスを入力するよう求められます。
5. Web サイトの表示、またはシステムによって自動的に配信されるライセンスの電子メールに添付されている zip ファイルに記載されたライセンス アクティベーション キーをコピーします。
6. [ASDM Configuration] > [ASA FirePOWER Configuration] > [Licenses] > [Add New License] の画面に戻ります。
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。
8. [Verify License] をクリックし、テキストが正しくコピーされたことを確認してから、[Submit License] をクリックします。
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

手順

1. [Configuration] > [ASA FirePOWER Configuration] を選択して、ASA FirePOWER セキュリティ ポリシーを設定します。
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 Help Topics] を選択します。
また、『ASA FirePOWER module user guide』[英語] も参照してください。

ASA セキュリティ ポリシーの設定

手順

1. トラフィックをモジュールに送信するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択します。
2. [Add] > [Add Service Policy Rule] を選択します。
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。

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。
5. **[Rule Actions]** ページで **[ASA FirePOWER Inspection]** タブをクリックします。
6. **[Enable ASA FirePOWER for this traffic flow]** チェックボックスをオンにします。
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。
8. (オプション) 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。
9. **[Finish]** をクリックし、次に **[Apply]** をクリックします。

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。

8. 次の作業

- 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 Module」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/ASDM のすべてのドキュメントのリンクについては、[Navigating the Cisco ASA Series Documentation](#) を参照してください。
- ASA FirePOWER 設定の詳細については、オンライン ヘルプ、『[ASA FirePOWER module user guide](#)』[英語]、または『[FireSIGHT/Firepower Management Center system user guide](#)』[英語] を参照してください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

