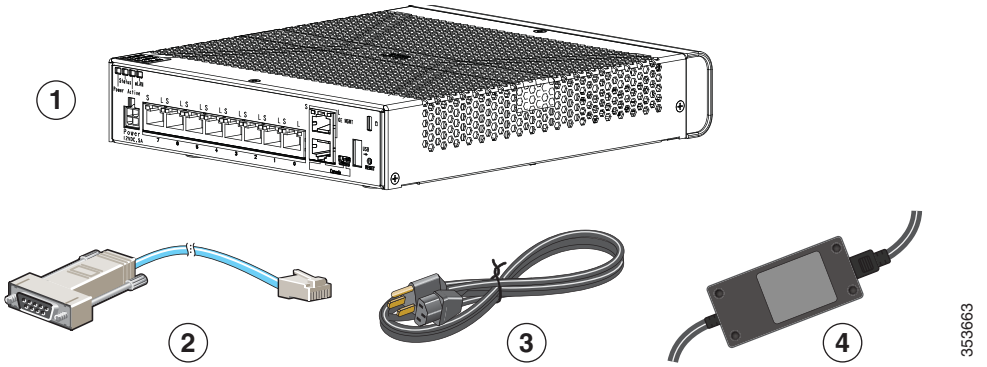
Cisco ASA 5506-X クイック スタート ガイド

リリース:15/03/02

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ることにご注意ください。



1	ASA 5506-X、ASA 5506W-X、または 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	電源ケーブル	4	電源モジュール

2. 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。

   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. 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。
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。

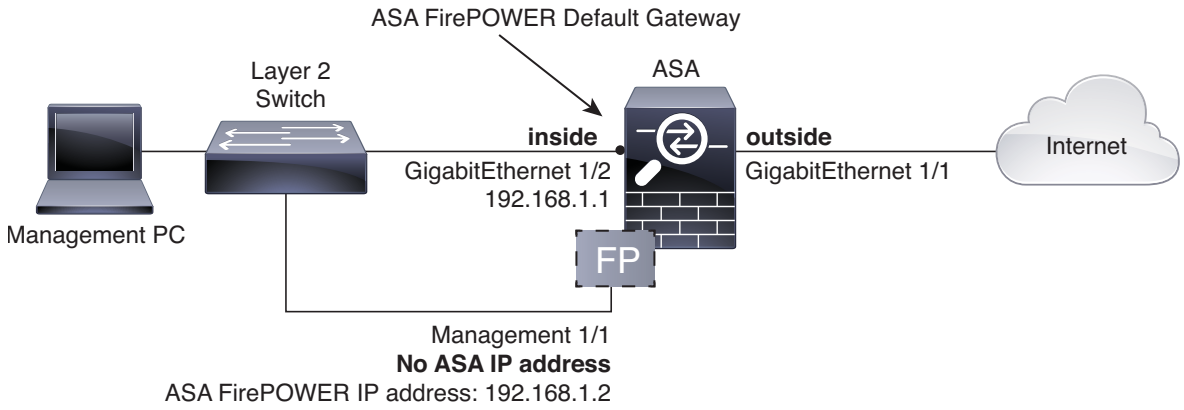
3. ASA FirePOWER モジュールの初期設定の変更

ASA の出荷時デフォルト設定では、**管理 1/1** インターフェイスへの Adaptive Security Device Manager(ASDM)接続が有効化されています。ASA FirePOWER モジュールを使用する場合、デフォルト設定を使用しないことが推奨されます。ここでは、新しい設定の適用方法について説明します。以下のモジュールを使用します。

- ASA FirePOWER モジュール:更新用にインターネット アクセスが必要です。

この設定により、内部ネットワーク、ネットワーク、外部ネットワークに対して使用可能な基本設定も有効になります。

次の図は、ASA FirePOWER モジュールおよびを使用した ASA 5506-X の推奨ネットワーク展開を示しています。



この手順を使用して、コンソールASA ポートに接続し、以下の動作を設定する新規設定に貼り付けることができます。

- 内部 --> 外部へのトラフィック フロー
- DHCP の外部 IP アドレス
- 内部ネットワークおよび ネットワーク上のクライアントに対する DHCP。
- 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。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。
- 内部インターフェイス上での ASDM アクセス

上記の設定を行うには、次の手順を実行します。

手順

1. 付属のコンソール ケーブルまたはミニ USB ケーブルを使用して、コンピュータを ASA のコンソール ポートに接続します。
2. ターミナル エミュレータを起動し、ASA に接続します。USB コンソール ポートの使用手順については、『ハードウェア ガイド』を参照してください。
3. **Enter** キーを押して、次のプロンプトが表示されることを確認します。

   ```
   ciscoasa>
   ```

4. 特権 EXEC モードにアクセスします。

   ```
   enable
   ```

   次のプロンプトが表示されます。

   ```
   Password:
   ```

5. Enter を押します。デフォルトでは、パスワードは空白です。
6. グローバル コンフィギュレーション モードにアクセスします。

   ```
   configure terminal
   ```

7. 設定をクリアします。

   ```
   clear configure all
   ```

8. プロンプトで次の設定をコピー アンド ペーストします。

```
interface gigabitethernet1/1
  nameif outside
  ip address dhcp setroute
  no shutdown
interface gigabitethernet1/2
  nameif inside
  ip address 192.168.1.1 255.255.255.0
  security-level 100
  no shutdown
interface management1/1
  no shutdown
object network obj_any
  subnet 0 0
  nat (any,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

9. 新しい設定を保存します。

```
write memory
```

10. 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。
    - 内部 GigabitEthernet 1/2 インターフェイス（内部）
    - Management 1/1 インターフェイス
    - コンピュータ
11. 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。

4. ASDM の起動

ASDM では、Web ブラウザを使用して ASA を管理できます。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。

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。デフォルト設定を使用しており、「3. ASA FirePOWER モジュールの初期設定の変更」（P.3）は使用しなかった場合は、Management 1/1 インターフェイスに接続する必要があります。
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。
3. [Run Startup Wizard] をクリックします。

   注：代わりに [Install ASDM Launcher] のクリックを選択した場合、場合によっては、『Install an Identity Certificate for ASDM』に従って ASA のアイデンティティ証明書と 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。
4. 画面上の指示に従います。[Cisco ASDM-IDM Launcher] が表示されます。
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。[ASDM Startup Wizard] が表示されます。

   注：[Cannot Connect to the ASA FirePOWER module] ダイアログボックスが表示されても、新規デバイスでは問題ありません。モジュールの IP アドレスをまだ設定していないためです。[Cancel] をクリックします。

6. 必要に応じて、スタートアップ ウィザード画面を設定します。「3. ASA FirePOWER モジュールの初期設定の変更」(P.3)の設定を使用している場合、[ASA FirePOWER Basic Configuration] 画面に到達したら、ASA FirePOWER モジュールに次のネットワーク設定を使用します。
   - 管理インターフェイス:192.168.1.2
   - 管理サブネット マスク:255.255.255.0
   - ゲートウェイ IP:192.168.1.1

   エンド ユーザ ライセンス契約に同意する必要があります。
7. [Next] をクリックして残りの画面に進み、ウィザードを完了します。

5. 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。

6. ASA FirePOWER モジュールの設定

ASDM を使用して、モジュールのセキュリティ ポリシーを設定し、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、FireSIGHT 管理センターを使用して 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 のバージョンに対応する『ASA ファイアウォール コンフィギュレーション ガイド』を参照してください。

手順

1. ASDMの [ASA FirePOWER] ページを使用して、モジュールのセキュリティ ポリシーを設定します。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 FirePOWERHelp Topics] を選択します。
2. 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。
3. [Add] > [Add Service Policy Rule] を選択します。
4. 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。
5. 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。
6. [Rule Actions] ページで [ASA FirePOWER Inspection] タブをクリックします。
7. [Enable ASA FirePOWER for this traffic flow] チェックボックスをオンにします。
8. [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。
9. (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。
10. [Finish]、[Apply] の順にクリックします。

    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。

6. ASA FirePOWER モジュールの設定