Firepower 4100 用 Cisco ASA クイック スタート ガイド

初版: 2016 年 3 月 21 日
最終更新日: 2016 年 5 月 9 日

1. Firepower 4100 用 ASA について

Firepower 4100 セキュリティ アプライアンスには、ASA のアプリケーションを実行できる、単一のセキュリティ エンジンが組み込まれています。

ASA の Firepower 4100 との連携方法

Firepower 4100 セキュリティ アプライアンスは、Firepower eXtensible Operating System（FXOS）という独自のオペレーティング システムを実行します。Firepower Chassis Manager Web インターフェイスまたは CLI を使用して、ハードウェア インターフェイスの設定、スマート ライセンシング、およびその他の基本的な操作パラメータを設定できます。

すべての物理インターフェイスの動作は、外部 EtherChannel の設定を含め、Firepower 4100 によって所有されます。2 種類のインターフェイス（データと管理）を作成できます。必要に応じて導入時に ASA にインターフェイスを割り当てることも、後で行うこともできます。これらのインターフェイスでは、ASA 設定と同じ ID を Firepower 4100 で使用します。Firepower 4100 は内部バックプレーン EtherChannel 越しに ASA にネットワーク トラフィックを提供します。

ASA を展開すると、Firepower 4100 は選択された ASA イメージをダウンロードし、デフォルト設定を確立します。ASA は、スタンドアロンの論理デバイス、または 6 シャーシまでの ASA クラスタとして展開できます。

ASA 管理

ASA を展開するときに、展開した ASA にクライアントから ASDM でアクセスできるように、管理インターフェイスと管理クライアント情報を事前設定できます。

内部 Telnet 接続を使用して、Firepower 4100 CLI から ASA CLI にアクセスすることもできます。ASA から、管理インターフェイスとデータ インターフェイスのいずれかによる SSH または Telnet アクセスを後で設定できます。

（注） ASDM アクセスのライセンス要件については、Firepower 4100 用 ASA のライセンス要件（1 ページ）を参照してください。

Firepower 4100 用 ASA のライセンス要件

Firepower 4100 用 ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 4100 と ASA に分割されています。

- Firepower 4100：License Authority との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャを Firepower 4100 で設定します。Firepower 4100 自体の稼働にライセンスは必要ありません。

- ASA：必要な標準ティア ライセンスなど、すべてのライセンス権限付与を ASA で設定します。その他のオプションのライセンスも利用できます。強力な暗号化ライセンスは、Firepower 4100 で登録トークンを適用すると、対象となるお客様の場合自動的に有効化されるため追加の操作は不要です。

(注) スマート ソフトウェア マネージャ サテライト導入では、ASDM（および VPN などの機能）を使用する前に、ASA ソフトウェア内で権限付与をリクエストして強力な暗号化（3DES/AES）のライセンスを有効にする必要があります。この作業は ASA CLI で実行する必要があります（FXOS CLI からアクセス可能）。評価ライセンスの場合は、強力な暗号化ライセンスを取得できません。

2. ASA の展開

Firepower Chassis Manager を使用してスタンドアロン ASA または ASA のクラスタを展開できます。CLI の手順については、FXOS の構成ガイドを参照してください。

インターフェイスの設定

Firepower 4100 で、ASA 用の導入設定に組み込むことのできる管理タイプのインターフェイスを設定します。また、少なくとも 1 つのデータ型インターフェイスを設定する必要があります。クラスタの場合は、シャーシ間のクラスタ制御リンクとして機能するポート チャネル 48 のクラスタ タイプのインターフェイスに、少なくとも 1 つのメンバー インターフェイスを追加する必要があります。

手順

1. Firepower Chassis Manager で、[インターフェイス（Interfaces）]を選択してインターフェイス ページを開きます。
2. EtherChannel を追加するには、次の手順を実行します。
   a. [ポート チャネルの追加（Add Port Channel）]をクリックします。
   b. [ポート チャネル ID（Port Channel ID）] に、1 ～ 47 の値を入力します。
   c. [有効（Enable）]はオンのままにします。
   d. [タイプ（Type）] で、[管理（Management）]または [データ（Data）]を選択します。含めることのできる管理インターフェイスは 1 つだけです。[クラスタ（Cluster）]は選択しないでください。
   e. 必要に応じて、メンバー インターフェイスを追加します。
   f. [OK]をクリックします。
3. 単一のインターフェイスを追加するには、次の手順を実行します。
   a. インターフェイス行で [編集（Edit）]アイコンをクリックして、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。
   b. [有効（Enable）]をオンにします。
   c. [タイプ（Type）] で、[管理（Management）]または [データ（Data）]をクリックします。含めることのできる管理インターフェイスは 1 つだけです。
   d. [OK]をクリックします。
4. クラスタ制御リンクのポート チャネル 48 にメンバーを追加するには、以下のステップに従います。
   a. インターフェイス行で [編集（Edit）]アイコンをクリックして、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。

b. [使用可能なインターフェイス(Available Interface)]ウィンドウからインターフェイスを選択し、[インターフェイスを追加(Add Interface)]をクリックします。必要に応じて追加のインターフェイス分繰り返します。少なくとも 1 つのインターフェイスが必要です。

c. [OK]をクリックします。

スタンドアロン ASA の展開

手順

1. [論理デバイス(Logical Devices)]を選択して、[論理デバイス(Logical Devices)] ページを開きます。
2. [デバイスの追加(Add Device)]をクリックし、[デバイスの追加(Add Device)] ダイアログボックスを表示します。
3. [デバイス名(Device Name)]に、論理デバイスの名前を指定します。この名前は、Firepower 4100 が管理設定を行ってインターフェイスを割り当てるために使用します。これは ASA 設定で使用されるデバイス名ではありません。
4. [テンプレート(Template)]では、[asa] を選択します。
5. [イメージ バージョン(Image Version)]では、ASA ソフトウェア バージョンを選択します。
6. [デバイス モード(Device Mode)]で、[スタンドアロン(Standalone)] オプション ボタンをクリックします。
7. [OK]をクリックします。[プロビジョニング - デバイス名(Provisioning - device name)]ウィンドウが表示されます。
8. [データ ポート(Data Ports)]領域を展開し、すべてのインターフェイスが ASA に割り当てられていることを確認します。
9. 画面中央のデバイス アイコンをクリックします。[ASA の設定(ASA Configuration)]ダイアログボックスが表示されます。
10. プロンプトに従い、導入オプションを設定します。
11. [OK]をクリックして [ASA の設定(ASA Configuration)] ダイアログボックスを閉じます。
12. [保存(Save)]をクリックします。Firepower 4100 は、指定したソフトウェア バージョンをダウンロードし、セキュリティ エンジンにブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

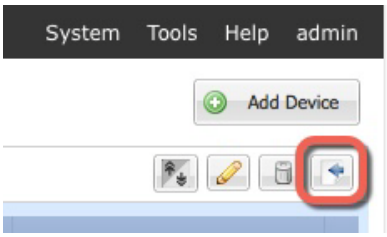
ASA クラスタの展開

手順

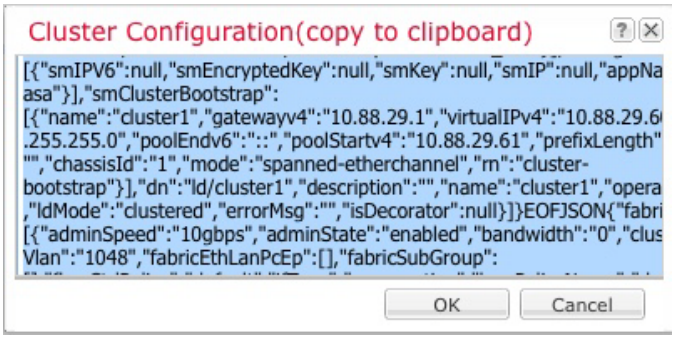
1. [論理デバイス(Logical Devices)]を選択して、[論理デバイス(Logical Devices)] ページを開きます。
2. [デバイスの追加(Add Device)]をクリックし、[デバイスの追加(Add Device)] ダイアログボックスを表示します。
3. [デバイス名(Device Name)]に、論理デバイスの名前を指定します。この名前は、Firepower 4100 がクラスタリング設定と管理設定を行ってインターフェイスを割り当てるために使用します。これは ASA 設定で使用されるクラスタまたはデバイスの名前ではありません。
4. [テンプレート(Template)]では、[asa] を選択します。
5. [イメージ バージョン(Image Version)]では、ASA ソフトウェア バージョンを選択します。
6. [デバイス モード(Device Mode)]では、[クラスタ(Cluster)] オプション ボタンをクリックします。
7. [新しいクラスタの作成(Create a new cluster)]オプション ボタンをクリックします。
8. [OK]をクリックします。[プロビジョニング - デバイス名(Provisioning - device name)]ウィンドウが表示されます。
9. [データ ポート(Data Ports)]領域を展開し、すべてのインターフェイスが ASA に割り当てられていることを確認します。

10. 画面中央のデバイス アイコンをクリックします。[ASA の設定(ASA Configuration)]ダイアログボックスが表示されます。
11. プロンプトに従い、導入オプションを設定します。

    (注) [管理 IP プール(Management IP Pool)]フィールドに、開始アドレスと終了アドレスをハイフンで区切って入力し、ローカル IP アドレスのプールを設定します。このうちの 1 つがインターフェイス用に各クラスタ ユニットに割り当てられます。最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の標準出荷単位に属する**仮想 IP アドレス**(メイン クラスタ IP アドレスと呼ばれる)は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つを仮想 IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス(どちらか一方も可)を使用できます。
12. [OK]をクリックして [ASA の設定(ASA Configuration)] ダイアログボックスを閉じます。
13. [保存(Save)]をクリックします。Firepower 4100 は、指定したソフトウェア バージョンをダウンロードし、セキュリティ エンジンにブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。
14. 次のシャーシをクラスタに追加します。
    a. 最初のシャーシの Firepower Chassis Manager で、右上の [クラスタ詳細の表示(Show Cluster Details)]アイコンをクリックします。



    b. 表示されるクラスタ設定テキストを選択してコピーします。



    c. 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。
    d. [既存のクラスタへの参加(Join an Existing Cluster)]を選択します。
    e. [config のコピー(Copy config)]チェックボックスをクリックして、[OK]をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。
    f. [クラスタ詳細のコピー(Copy Cluster Details)]ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK]をクリックします。
    g. 画面中央のデバイス アイコンをクリックします。クラスタ情報は、[シャーシ ID(Chassis ID)] を除き、事前に入力されます。固有のシャーシ ID を入力し、[OK]をクリックします。
    h. [保存(Save)]をクリックします。

3. ASA CLI へのアクセス

初期設定またはトラブルシューティングのために、Firepower 4100 CLI から ASA CLI にアクセスする必要があることがあります。

手順

1. プライマリ Firepower 4100 CLI に接続します。たとえば、コンソール ポートに接続するか、Firepower 管理インターフェイスに SSH で接続します。
2. ASA に接続します。

   connect module 1 console

   例:

   ```
   Firepower> connect module 1 console
   Firepower-module1>
   ```

3. セキュリティ エンジンに初めて接続するときは、FXOS セキュリティ エンジンの CLI に入ります。その後 ASA アプリケーションに接続する必要があります。

   connect asa

   例:

   ```
   Firepower-module1> connect asa
   asa>
   ```

   後続の接続では ASA のアプリケーションに直接接続されます。
4. 特権 EXEC（イネーブル）モードを開始した後、グローバル コンフィギュレーション モードを開始します。デフォルトでは、イネーブル パスワードは空白です。

   enable
   configure terminal

   例:

   ```
   asa> enable
   Password:
   asa# configure terminal
   asa(config)#
   ```

5. ASA クラスタの場合は、必要に応じて、このユニットが標準出荷単位であることを確認します。

   show cluster info

   例:

   ```
   asa(config)# show cluster info
   Cluster cluster1: On
       Interface mode: spanned
       This is "unit-1-1" in state MASTER
           ID        : 2
           Version   : 9.6(1)
           Serial No.: FCH183770GD
           CCL IP    : 127.2.1.1
           CCL MAC   : 0015.c500.019f
           Last join : 01:18:34 UTC Nov 4 2015
           Last leave: N/A
   Other members in the cluster:
       Unit "unit-2-1" in state SLAVE
           ID        : 4
           Version   : 9.6(1)
   ```

```
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.2.1
    CCL MAC   : 0015.c500.018f
    Last join : 20:29:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-3-1" in state SLAVE
    ID        : 1
    Version   : 9.6(1)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.3.1
    CCL MAC   : 0015.c500.017f
    Last join : 20:20:53 UTC Nov 4 2015
    Last leave: 20:18:15 UTC Nov 4 2015
Unit "unit-4-1" in state SLAVE
    ID        : 3
    Version   : 9.6(1)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.4.1
    CCL MAC   : 0015.c500.020f
    Last join : 20:19:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
```

別のシャーシが標準出荷単位の場合は、接続を終了し、正しいシャーシに接続します。接続の終了については、以下を参照してください。

4. スマート ソフトウェア マネージャ サテライト:強力な暗号化(3DES/AES)のライセンスのリクエスト

ASDM を実行したり、VPN などのその他の機能を実行したりするには、強力な暗号化(3DES/AES)のライセンスが必要です。スマート ソフトウェア マネージャ サテライトを使用するときは、CLI を使用して ASA 設定でこのライセンスをリクエストする必要があります。

はじめる前に

- ASA でライセンス権限付与を設定する前に、Firepower 4100 でシスコ スマート ソフトウェア ライセンシングを設定する必要があります。
- ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。ASA CLI から確認することもできます。

手順

1. ASA CLI にアクセスします。3. ASA CLI へのアクセス(5 ページ)を参照してください。
2. ライセンス スマート コンフィギュレーション モードを開始します。

   `license smart`

   例:

   ```
   ciscoasa(config)# license smart
   ciscoasa(config-smart-lic)#
   ```

3. 機能層を設定します。

   `feature tier standard`

   使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

4. 強力な暗号化ライセンスおよびオプションで他の機能のライセンスをリクエストします。
   - 強力な暗号化(3DES/AES)

     feature strong-encryption
   - キャリア(Diameter、GTP/GPRS、SCTP)

     feature carrier
   - セキュリティ コンテキスト

     feature context <1-248>
5. 設定を保存します。

   write memory
6. 「**~**」と入力してコンソール接続を終了します。Telnet アプリケーションに切り替わります。「**quit**」と入力して Firepower 4100 CLI を終了します。

5. ASDM の起動

ASDM には、容易に操作できる多くのウィザードや、個々の ASA 機能設定ツール一式が含まれています。

はじめる前に

- 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 [英語] を参照してください。
- ASDM に接続する前に、Firepower 4100 でシスコ スマート ソフトウェア ライセンシングを設定する必要があります。ASDM を使用するには強力な暗号化(3DES/AES)が必要です。強力な暗号化ライセンスは、Firepower 9300 で登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。スマート ソフトウェア マネージャ サテライトの導入については、4. スマート ソフトウェア マネージャ サテライト:強力な暗号化(3DES/AES)のライセンスのリクエスト(6 ページ)を参照してください。

手順

1. ASAに割り当てた管理インターフェイスに接続されたコンピュータで、Web ブラウザを起動します。
2. [アドレス(Address)]フィールドに URL **https://***ip_address***/admin** を入力します。*ip_address* は ASA を展開したときに管理インターフェイス用に設定した値です。[Cisco ASDM]Web ページが表示されます。
3. 使用可能なオプション([ASDM ランチャーのインストール(InstallASDM Launcher)]、[ASDM の実行(Run ASDM)]、[スタートアップ ウィザードの実行(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 ランチャー(Cisco ASDM-IDM Launcher)]が表示されます。

   (注) [ASDM ランチャーのインストール(Install ASDM Launcher)] をクリックすると、一部の Java 7 バージョンでは、『Install an Identity Certificate for ASDM』に従って ASA の ID 証明書をインストールする必要があります。
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. 次の作業

- ASA/ASDM のすべてのドキュメントのリンクについては、Cisco ASA シリーズ マニュアルのナビゲーション [英語] を参照してください。
- すべての FXOS シャーシのマニュアル [英語] を参照してください。