Cisco ASA for Firepower 9300 クイック スタート ガイド

初版:2015 年 7 月 16 日
最終更新日:2017 年 10 月 9 日

1. Firepower 9300 用 ASA について

Firepower 9300 セキュリティ アプライアンスは、ASA のアプリケーションを実行する、最大 3 つのセキュリティ モジュールを装着できます。

Firepower eXtensible Operating System（FXOS）1.1.3 以降では、複数のシャーシで最大 6 台の ASA を搭載するようにシャーシ間クラスタを作成できます。

ASA の Firepower 9300 との連携方法

Firepower 9300 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 システムをスーパバイザ上で実行します。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スーパバイザ上で設定できます。

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、スーパバイザ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。管理インターフェイスのみをモジュール間で共有できます。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 をスーパバイザで使用します。Firepower 9300 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、スーパバイザは選択された 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 ASA クラスタとして展開できます。クラスタリングを使用する場合は、シャーシのすべてのモジュールがクラスタに属している必要があります。FXOS 1.1.2 以前では、シャーシ内クラスタリングのみサポートされます。FXOS 1.1.3 ではシャーシ間クラスタリングをサポートします。

シャーシのすべてのモジュールに ASA ソフトウェアをインストールする必要があります。異なるソフトウェア タイプは現在サポートされていません。

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する必要があります。

（注）ASA 管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます。Firepower Chassis Manager では、シャーシ管理インターフェイスは、[Interfaces] タブの上部に [MGMT] と表示されます）。

内部 Telnet 接続を使用して、Firepower 9300 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 9300 ASA セキュリティ モジュールのライセンス要件（2 ページ）を参照してください。

Firepower 9300 ASA セキュリティ モジュールのライセンス要件

Firepower 9300 上の 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 9300 スーパバイザと ASA に分割されています。

- Firepower 9300：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スーパバイザで設定します。Firepower 9300 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。（FXOS 1.1.3 以降）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るため追加の操作は不要です。

（注）FXOS 1.1.2 以前および 2.3.0 以前のスマート 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要求して強力な暗号化（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

スーパバイザで、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 タイプのインターフェイスを設定する必要があります。シャーシ間クラスタリングでは、クラスタ インターフェイスにメンバー インターフェイスを追加することも必要です。

はじめる前に

- 管理インターフェイスが必要です。ASA 管理インターフェイスは、シャーシの管理のみに使用される シャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます。Firepower Chassis Manager では、シャーシ管理インターフェイスは、[Interfaces] タブの上部に [MGMT] と表示されます）。
- シャーシ間クラスタリングの場合：
  - 全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つ EtherChannel である必要があります。
  - 各シャーシに同じ管理、データ、およびクラスタ インターフェイスを追加します。

手順

1. [Interfaces] を選択して [Interfaces] 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. [Add Port Channel] をクリックします。
   b. [Port Channel ID] に、1 ～ 47 の値を入力します。
   c. [Enable] はオンのままにします。
   d. [Type] で、[Management] または [Data] を選択します。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。[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. 単一インターフェイスの場合:

a. インターフェイス行で [Edit] アイコンをクリックして、[Edit Interface] ダイアログボックスを開きます。

b. [Enable] をオンにします。

c. [Type] で、[Management] または [Data] をクリックします。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。

d. [OK] をクリックします。

4. シャーシ間クラスタリングでは、ポート チャネル 48 にメンバー インターフェイスを追加し、クラスタ制御リンクとして使用します。各シャーシに同じメンバ インターフェイスを追加します。

スタンドアロン ASA の展開

手順

1. [Logical Devices] を選択して [Logical Devices] ページを開きます。
2. [Add Device] をクリックして [Add Device] ダイアログボックスを開きます。
3. [Device Name] には、論理デバイスの名前を指定します。この名前は、Firepower 9300 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. [Template] では、[asa] を選択します。
5. [Image Version] では、ASA ソフトウェア バージョンを選択します。
6. [Device Mode] では、[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。[Provisioning - *device name*] ウィンドウが表示されます。
8. [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 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 Configuration] ダイアログボックスを閉じます。
12. [Save(保存)] をクリックします。Firepower 9300 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. [Logical Devices] を選択して [Logical Devices] ページを開きます。
2. [Add Device] をクリックして [Add Device] ダイアログボックスを開きます。
3. [Device Name] には、論理デバイスの名前を指定します。この名前は、Firepower 9300 スーパバイザ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. [Template] では、[Cisco Adaptive Security Appliance] を選択します。
5. [Image Version] では、ASA ソフトウェア バージョンを選択します。

6. [Device Mode] では、[Cluster] オプション ボタンをクリックします。
7. [Create New Cluster] ラジオ ボタンをクリックします。
8. [OK] をクリックします。
9. 画面中央のデバイス アイコンをクリックします。

   [ASA Configuration] ダイアログボックスが [Cluster Information] タブが選択された状態で表示されます。
10. [Chassis ID] フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。
11. サイト間クラスタリングの場合、[Site ID] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。
12. [クラスタ キー(Cluster Key)] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

    共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック(接続状態アップデートや転送されるパケットなど)には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。
13. [Cluster Group Name] を設定します。これは、ASA 設定のクラスタ グループ名です。

    名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。
14. [Management Interface] をクリックして、先に作成した管理インターフェイスを選択します。
15. 管理インターフェイスの [Address Type] を選択します。

    この情報は、ASA 設定で管理インターフェイスを設定するために使用されます。

    a. [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。

    b. 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。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。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 つをメイン クラスタ 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。

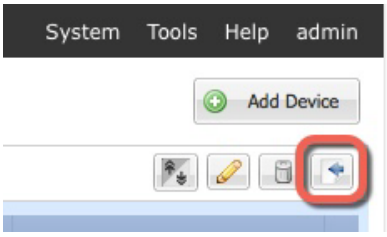
    c. [ネットワーク マスク(Network Mask)] または [プレフィックス長(Prefix Length)] に入力します。

    d. **ネットワーク ゲートウェイ**を入力します。

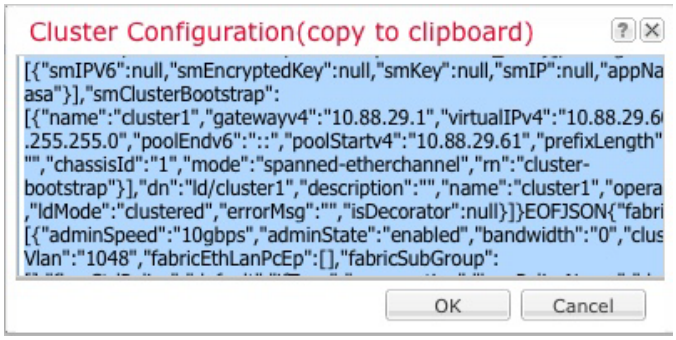
    e. **仮想 IP アドレス**を入力します。

    この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。
16. [Settings] タブの [Password] に、「admin」ユーザのパスワードを入力します。管理者ユーザはパスワードの回復に役立つ場合があります。
17. [OK] をクリックして、[ASA Configuration] ダイアログボックスを閉じます。
18. シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

    a. 最初のシャーシの Firepower Chassis Manager で、右上の [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. [Join an Existing Cluster] を選択します。

e. [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. [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。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **Chassis ID**：一意のシャーシ ID を入力します。
- **Site ID**：正しいサイト ID を入力します。
- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。

h. [OK] をクリックします。

i. [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 9300 スーパバイザから ASA CLI にアクセスする必要があることがあります。

手順

1. たとえば、コンソール ポートからか、SSH を使用して Firepower 9300 スーパバイザ CLI に接続します。
2. ASA に接続します。

   connect module *slot* **console**

   例：

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

   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 の [Logical Devices] 画面を参照して、いずれのモジュールが標準出荷単位であるのかを確認するか、または ASA CLI を使用して確認します。

3. モジュールに初めて接続するときは、FXOS モジュールの 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。

   イネーブル化
   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、このモジュール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-1-2" in state MASTER
           ID        : 2
           Version   : 9.5(2)
           Serial No.: FCH183770GD
           CCL IP    : 127.2.1.2
           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-1-3" in state SLAVE
           ID        : 4
           Version   : 9.5(2)
           Serial No.: FCH19057ML0
           CCL IP    : 127.2.1.3
           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-1-1" in state SLAVE
           ID        : 1
           Version   : 9.5(2)
           Serial No.: FCH19057ML0
           CCL IP    : 127.2.1.1
           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-2-1" in state SLAVE
           ID        : 3
           Version   : 9.5(2)
           Serial No.: FCH19057ML0
           CCL IP    : 127.2.2.1
   ```

```
CCL MAC   : 0015.c500.020f
Last join : 20:19:57 UTC Nov 4 2015
Last leave: 20:24:55 UTC Nov 4 2015
```

別のモジュールが標準出荷単位の場合は、接続を終了し、正しいスロット番号に接続します。接続の終了については、以下を参照してください。

6. コンソール接続を終了するために「**~**」と入力します。Telnet アプリケーションに切り替わります。「**quit**」と入力してスーパバイザ CLI を終了します。

4. ASA のライセンス権限付与の設定

FXOS 1.1.2 以前および 2.3.0 以前のスマート ソフトウェア マネージャ サテライト

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。CLI を使用して ASA 設定でこのライセンス（古いバージョン用）およびその他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 9300 スーパバイザでシスコ 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。

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. 次の機能の 1 つ以上をリクエストします。
   - 強力な暗号化（3DES）

     feature strong-encryption
   - ASA 9.5(1) 以前：モバイル SP（GTP/GPRS）

     feature mobile-sp
   - ASA 9.5(2) 以降：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

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 9300 スーパバイザでシスコ 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。FXOS 1.1.3 以降の場合、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。FXOS 1.1.2 以前および 2.3.0 以前のスマート ソフトウェア マネージャ サテライト導入の場合は、4. ASA のライセンス権限付与の設定（7 ページ）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. [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（[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。

   注：[Install ASDM Launcher] をクリックすると、一部の Java 7 バージョンでは、ASDM 用 ID 証明書のインストール [英語] 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 Firepower 9300 のマニュアル [英語] を参照してください。