



## 論理デバイス Firepower 4100/9300

Firepower 4100/9300は柔軟なセキュリティプラットフォームが1つまたは複数の論理デバイスをインストールすることができます。この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイアベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、[Firepower 4100/9300 シャーシの ASA クラスター](#)を参照してください。FXOS CLIを使用する場合は、FXOS CLIコンフィギュレーションガイドを参照してください。高度なFXOSの手順とトラブルシューティングについては、FXOS コンフィギュレーションガイドを参照してください。

- [Firepower インターフェイスについて \(1 ページ\)](#)
- [論理デバイスについて \(3 ページ\)](#)
- [ハードウェアとソフトウェアの組み合わせの要件と前提条件 \(3 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(4 ページ\)](#)
- [インターフェイスの設定 \(6 ページ\)](#)
- [論理デバイスの設定 \(9 ページ\)](#)
- [論理デバイスの履歴 \(17 ページ\)](#)

## Firepower インターフェイスについて

Firepower 4100/9300 シャーシは、物理インターフェイスおよびEtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

## シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報をFXOS CLIで表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

```
firepower(local-mgmt) # show mgmt-port
```

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

## インターフェイスタイプ

各インターフェイスは、次のいずれかのタイプになります。

- **Data** : 通常のデータに使用します。データインターフェイスは論理デバイス間で共有できません。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- **Mgmt** : アプリケーションインスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。
- **Firepower-eventing** : FTD デバイスのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。Firepower Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。Firepower-eventing インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の論理デバイスと通信することはできません。
- **Cluster** : クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。

## シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシとアプリケーションの間に不一致が生じることがあります。

## 論理デバイスについて

論理デバイスでは、1つのアプリケーションインスタンス（ASAまたはFirepower Threat Defenseのいずれか）および1つのオプションデコレータアプリケーション（Radware DefensePro）を実行し、サービスチェーンを形成できます。

論理デバイスを追加するときに、アプリケーションインスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。



- (注) Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーションインスタンスタイプ（ASAまたはFTD）をインストールする必要があります。現時点では、異なるタイプはサポートされていません。モジュールは異なるバージョンのアプリケーションインスタンスタイプを実行できることに注意してください。

Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーションインスタンスタイプ（ASAまたはFTD）をインストールする必要があります。現時点では、異なるタイプはサポートされていません。モジュールは異なるバージョンのアプリケーションインスタンスタイプを実行できることに注意してください。

## スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイスタイプを追加できます。

- **スタンドアロン**：スタンドアロン論理デバイスは、スタンドアロンユニットまたはハイアベイラビリティペアのユニットとして動作します。
- **クラスタ**：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュールデバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3つすべてのモジュールが。

## ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

### Firepower 9300 の要件

Firepower 9300 には、3つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- セキュリティモジュールタイプ：Firepower 9300 のすべてのモジュールは同じタイプである必要があります。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。
- ASA および FTD のアプリケーションタイプ：シャーシ、ASA、または FTD には、1 つのアプリケーションタイプのみインストールできます。
- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーションインスタンスタイプを実行することもたとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

### Firepower 4100 の要件

Firepower 4100 は複数のモデルに搭載されています。次の要件を参照してください。

- クラスタリング：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASA および FTD のアプリケーションタイプ：Firepower 4100 は、1 つのアプリケーションタイプのみを実行できます。

## 論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

## Firepower インターフェイスに関する注意事項と制約事項

### 次のインラインセット FTD

- リンク ステータスの伝達はサポートされます。

### ハードウェアバイパス

- FTD をサポート。ASA の通常のインターフェイスとして使用できます。

- FTD はインラインセットでのみ ハードウェアバイパス をサポートします。
- ハードウェアバイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできません。
- ハードウェアバイパス インターフェイスを EtherChannel に含めたり、ハードウェアバイパス 用に使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。
- ハードウェアバイパス ハイ アベイラビリティではサポートされていません。

### デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャンネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

## 一般的なガイドラインと制限事項

### ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。ASA の場合、展開後に、ファイアウォール モードをトランスペアレントに変更することができます。[ASA のトランスペアレント ファイアウォール モードへの変更 \(13 ページ\)](#) を参照してください。

### ハイ アベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。

- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、[フェールオーバーのシステム要件](#)を参照してください。

#### コンテキストモード

- ASA ではマルチ コンテキスト モードはサポートされていません。
- 展開後に、ASA のマルチ コンテキスト モードを有効にします。
- ので TLS 暗号化アクセラレーション を有効にできます。

## インターフェイスの設定

デフォルトでは、物理インターフェイスはディセーブルになっています。インターフェイスを有効にし、EtherChannels、インターフェイス プロパティを編集して。



- (注) FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。



## インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。



#### 手順

**ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。

[Interfaces] ページには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

**ステップ 2** インターフェイスを有効にするには、[disabled スライダ ()] をクリックします。これで、[enabled スライダ ()] に変わります。

[Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変わります。

- ステップ 3** インターフェイスを無効にするには、[enabled スライダー (  ) ] をクリックします。これで、[disabled スライダー (  ) ] に変わります。
- [Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

---

## 物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

### 始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

### 手順

---

- ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** 編集するインターフェイスの行の [Edit] をクリックし、[Edit Interface] ダイアログボックスを開きます。
- ステップ 3** インターフェイスをイネーブルにするには、[Enable] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。
- ステップ 4** インターフェイスの [タイプ (Type) ] を次から選択します。 **Data**、**Mgmt**、**Firepower-eventing**、または **Cluster**。
- Cluster** タイプは選択しないでください。デフォルトでは、Cluster Control Link はポートチャンネル 48 に自動的に作成されます。
- ステップ 5** (任意) [Speed] ドロップダウン リストからインターフェイスの速度を選択します。
- ステップ 6** (任意) インターフェイスで [Auto Negotiation] がサポートされている場合は、[Yes] または [No] オプション ボタンをクリックします。
- ステップ 7** (任意) [Duplex] ドロップダウン リストからインターフェイスのデュプレックスを選択します。
- ステップ 8** [OK] をクリックします。
-

## EtherChannel (ポートチャネル) の追加

EtherChannel (別名ポートチャネル) には、同じタイプのメンバーインターフェイスを最大16個含めることができます。リンク集約制御プロトコル (LACP) では、2つのネットワークデバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

各メンバーインターフェイスが LACP 更新を送受信するように、Firepower 4100/9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブモードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネルグループに接続されていることがチェックされます。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止 (Suspended)] 状態になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [Suspended] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも1つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended)] 状態に戻ります。

### 手順

- 
- ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** インターフェイステーブルの上にある [Add Port Channel] をクリックして、[Add Port Channel] ダイアログボックスを開きます。
- ステップ 3** [Port Channel ID] フィールドに、ポートチャネルの ID を入力します。有効な値は、1 ~ 47 です。
- クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、別の ID で EtherChannel を設定し、インターフェイスにクラスタタイプを選択できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。



- ステップ 4** ポートチャンネルを有効化するには、**[Enable]**チェックボックスをオンにします。ポートチャンネルをディセーブルにするには、**[Enable]**チェックボックスをオフにします。
- ステップ 5** インターフェイスの **[Type]** を次から選択します。 **Data**、**Mgmt**、**Firepower-eventing**、または **Cluster**。
- デフォルトの代わりに、このポートチャンネルを **Cluster Control Link** として使用する場合以外は、**Cluster** タイプを選択しないでください。
- ステップ 6** ドロップダウン リストでメンバー インターフェイスの **[Admin Speed]** を設定します。
- ステップ 7** **[Admin Duplex]**、**[Full Duplex]** または **[Half Duplex]** を設定します。
- ステップ 8** ポート チャンネルにインターフェイスを追加するには、**[Available Interface]** リストでインターフェイスを選択し、**[Add Interface]** をクリックしてそのインターフェイスを **[Member ID]** リストに移動します。同じタイプと速度の最大 16 のインターフェイスを追加できます。
- ヒント** 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、**Ctrl** キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift** キーを押しながら最後のインターフェイスをクリックして選択します。
- ステップ 9** ポートチャンネルからインターフェイスを削除するには、**[Member ID]** リストでそのインターフェイスの右側にある **[Delete]** ボタンをクリックします。
- ステップ 10** **[OK]** をクリックします。

## 論理デバイスの設定

Firepower 4100/9300 シャーシに、スタンドアロン論理デバイスまたはハイ アベイラビリティ ペアを追加します。

クラスタリングについては、[#unique\\_271](#) を参照してください。

## スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロン デバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュールクラスタと単一のスタンドアロン デバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッドファイアウォール モード ASA を展開できます。To change the ASA to transparent firewall mode, complete this procedure, and then see [ASA のトランスペアレント ファイアウォール モードへの変更 \(13 ページ\)](#) .

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

## 始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシにアップロードします。



(注) Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ (ASA または FTD) をインストールする必要があります。現時点では、異なるタイプはサポートされていません。モジュールは異なるバージョンのアプリケーション インスタンス タイプを実行できることに注意してください。

Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ (ASA または FTD) をインストールする必要があります。現時点では、異なるタイプはサポートされていません。モジュールは異なるバージョンのアプリケーション インスタンス タイプを実行できることに注意してください。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この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ポートと同じではありません (また、[Interfaces] タブの上部に [MGMT] として表示されず)。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス

## 手順

**ステップ 1** [論理デバイス (Logical Devices)] を選択します。

**ステップ 2** [デバイスの追加 (Add Device)] をクリックし、次のパラメータを設定します。

a) デバイス名を入力します。

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。

c) [Image Version] を選択します。

d) [使用方法 (Usage)] 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。

- e) [使用方法 (Usage) ]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。
- f) [OK] をクリックします。  
[Provisioning - *device name*] ウィンドウが表示されます。

**ステップ 3** [Data Ports] 領域を展開し、デバイスに割り当てるポートをそれぞれクリックします。

以前に [Interfaces] ページで有効にしたデータインターフェイスのみを割り当てることができます。後ほど ASA でこれらのインターフェイスを有効にして設定します (IP アドレスの設定を含む)。

**ステップ 4** 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

**ステップ 5** [General Information] ページで、次の手順を実行します。

- a) (Firepower 9300 の場合) [Security Module Selection] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。
- b) [Management Interface] を選択します。  
このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。
- c) 管理インターフェイスを選択します。[Address Type] : [IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。
- d) [Management IP] アドレスを設定します。  
このインターフェイスの一意の IP アドレスを設定します。
- e) ネットワーク マスクまたはプレフィックス長を入力します。
- f) ネットワーク ゲートウェイ アドレスを入力します。

**ステップ 6** [Settings] タブをクリックします。

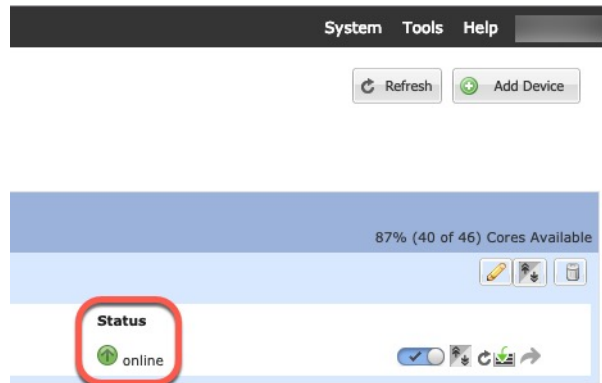
**ステップ 7** 管理者ユーザの [Password] を入力して確認します。

事前設定されている ASA 管理者ユーザ/パスワードは、パスワードの回復に役立ちます。FXOS アクセスが可能な場合、管理者ユーザ パスワードを忘れたときにリセットできます。

**ステップ 8** [OK] をクリックして、設定ダイアログボックスを閉じます。

**ステップ 9** [Save] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定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。[論理デバイス (Logical Devices) ] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



**ステップ 10** セキュリティポリシーの設定を開始するには、ASA コンフィギュレーションガイドを参照してください。

## ハイアベイラビリティペアの追加

または ASA ハイアベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

### 始める前に

- ハイアベイラビリティフェールオーバーを設定される2つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- ハイアベイラビリティシステム要件については、[フェールオーバーのシステム要件](#)を参照してください。

### 手順

- ステップ 1** 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイアベイラビリティは推奨されず、サポートされない可能性があります。
- ステップ 2** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 3** フェールオーバーリンクとステートリンクに1つまたは2つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイアベイラビリティトラフィックを交換します。統合されたフェールオーバーリンクとステートリンクには、10GBのデータインターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。同じネットワークセグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

**ステップ 4** 論理デバイスでハイアベイラビリティを有効にします。 [ハイアベイラビリティのためのフェールオーバー](#)を参照してください。

**ステップ 5** ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

(注) ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

## ASA のトランスペアレント ファイアウォール モードへの変更

Firepower 4100/9300 シャーシのルーテッドファイアウォールモード ASA のみを導入できます。ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。スタンドアロン ASA の場合、ファイアウォールモードを変更すると設定が消去されるため、Firepower 4100/9300 シャーシから設定を再展開して、ブートストラップ設定を回復する必要があります。ASA はトランスペアレントモードのまま、ブートストラップ設定が機能した状態になっています。クラスタ化 ASA の場合、設定は消去されないため、FXOS からブートストラップ設定を再導入する必要はありません。

### 手順

**ステップ 1** [アプリケーションのコンソールへの接続 \(16 ページ\)](#) に従って、ASA コンソールに接続します。クラスタの場合、プライマリユニットに接続します。フェールオーバーペアの場合、アクティブユニットに接続します。

**ステップ 2** コンフィギュレーションモードに入ります。

```
enable
```

```
configure terminal
```

デフォルトでは、イネーブルパスワードは空白です。

**ステップ 3** ファイアウォールモードをトランスペアレントに設定します。

**firewall transparent**

**ステップ 4** 設定を保存します。

**write memory**

クラスタまたはフェールオーバー ペアの場合、この設定はセカンダリ ユニットに複製されます。

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
End Configuration Replication to slave.

asa(config)#
```

**ステップ 5** Firepower Chassis Manager の [Logical Devices] ページで、[Edit] アイコンをクリックして ASA を編集します。

[Provisioning] ページが表示されます。

**ステップ 6** デバイスのアイコンをクリックして、ブートストラップ設定を編集します。設定の値を変更し、[OK] をクリックします。

少なくとも 1 つのフィールド ([Password] フィールドなど) の値を変更する必要があります。ブートストラップ設定の変更に関する警告が表示されます。[Yes] をクリックします。

**ステップ 7** ASA に設定を再配置する **保存** をクリックします。シャーシ間クラスタまたはフェールオーバーペアの場合、各シャーシでステップ 5 ~ 7 を繰り返してブートストラップ設定を再導入します。

シャーシ/セキュリティ モジュールがリロードし、ASA が再度稼働するまで数分待ちます。ASA は、これでブートストラップ設定が機能するようになりますが、トランスペアレントモードのままです。

## ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合 (ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインターフェイスの EtherChannel への再割り当てなど)、そのインターフェイスがセキュリティポリ

シーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。



(注) 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

### 始める前に

- [物理インターフェイスの設定 \(7 ページ\)](#) および [EtherChannel \(ポート チャンネル\) の追加 \(8 ページ\)](#) に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには (たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます)、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバーインターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。ASA がリロードし (管理インターフェイスを変更するとリロードします)、(現在未割り当ての) 管理インターフェイスも EtherChannel に追加できます。
- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にスレーブ/スタンバイ ユニットでインターフェイスを変更してから、マスター/アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

### 手順

- ステップ 1** Firepower Chassis Manager で、[Logical Devices] を選択します。
- ステップ 2** 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。
- ステップ 3** [Data Ports] 領域でデータ インターフェイスの選択を解除して、そのインターフェイスの割り当てを解除します。
- ステップ 4** [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。
- ステップ 5** 次のように、管理インターフェイスを置き換えます。

このタイプのインターフェイスでは、変更を保存するとデバイスがリロードします。

  - a) ページ中央のデバイス アイコンをクリックします。

- b) [General/Cluster Information] タブで、ドロップダウンリストから新しい [Management Interface] を選択します。
- c) [OK] をクリックします。

**ステップ 6** [保存 (Save) ] をクリックします。

## アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

### 手順

**ステップ 1** 、モジュール CLI に接続します。

**connect module slot\_number console**

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot\_number* として **1** を使用します。

例 :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

**ステップ 2** アプリケーションのコンソールに接続します。 デバイスの適切なコマンドを入力します。

**connect asa**

**connect ftd**

**connect vdp**

例 :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

**ステップ 3** アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA : **Ctrl-a, d** と入力
- FTD : と入力



- vDP : **Ctrl-],.** と入力

**ステップ 4** FXOS CLI のスーパーバイザ レベルに戻ります。

- a) ~ と入力

Telnet アプリケーションに切り替わります。

- b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

## 論理デバイスの履歴

機能	バージョン	詳細
Firepower 4100 シリーズ のサポート	9.6(1)	FXOS 1.1.4 では、ASA クラスタリングは、Firepower 4100 シリーズ のシャーシ間クラスタリングをサポートします。 変更された画面はありません。
6 つのモジュールのシャーシ間クラスタリング、および FirePOWER 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 変更された画面はありません。
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4 (1.150)	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次の画面を導入しました。 <b>[Configuration] &gt; [Device Management] &gt; [High Availability and Scalability] &gt; [ASA Cluster Replication]</b>

