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 Firewall シャーシ マネージャ 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 の ASA クラスタを参照してください。FXOS CLI を使用するには、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。

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 Firewall シャーシ マネージャ によって、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や、論理デバイスがオフラインになっている場合でも、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。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

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。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは1つまたは複数の論理デバイス/コンテナインスタンス（Firewall Threat DefenseFirewall Management Center 専用）で共有できます。
- 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。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス（1 ページ）を参照してください。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Firewall Management Center デバイスを使用した Firewall Threat Defense のセカンダリ管理インターフェイスとして使用します。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 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。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。

スタンドアロン展開とクラスタ展開での Firewall Threat Defense および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *1*：インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ファイアウォール脅威防御	スタンドアロン ネイティブ インスタンス	対応	—	—	—	○	○	—	—
	スタンドアロン コンテナ インスタンス	○	○	○	○	○	○	—	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	—
	クラスタ コンテナ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	○

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定 （シャーシ間クラスタリング専用の EtherChannel）	—	—	—	対応	—	対応	—

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーションの連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

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ため、シャーシとアプリケーションの間で不一致が発生することがあります。

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 Firewall 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場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

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ネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。

のハードウェアとソフトウェアの要件と前提条件

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。可能な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。次の要件を確認します。

- セキュリティモジュール タイプ：Firepower 9300 には、さまざまなタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2、SM-56 をモジュール 3 としてインストールできます。

- ネイティブインスタンスとコンテナインスタンス：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを1つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール1とモジュール2にネイティブインスタンスをインストールできますが、モジュール3にはコンテナインスタンスをインストールできます。
- 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。空のスロットを含め、シャーシ内にある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が、各シャーシにインストールされているセキュリティモジュールの数はさまざまでかまいません。たとえば、シャーシ1に2つのSM-40を、シャーシ2に3つのSM-40をインストールできます。 同じシャーシに1つのSM-48および2つのSM-40をインストールする場合、クラスタリングは使用できません。
- 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。 ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシにはSM-40、SM-48、およびSM-56があります。SM-40モジュール間、SM-48モジュール間、およびSM-56モジュール間にハイアベイラビリティペアを作成できます。
- ASAおよびFirewall Threat Defenseのアプリケーションタイプ：異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール1とモジュール2にASAをインストールし、モジュール3にFirewall Threat Defenseをインストールすることができます。
- ASAまたはFirewall Threat Defense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、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール1にFirewall Threat Defense 6.3を、モジュール2にFirewall Threat Defense 6.4を、モジュール3にFirewall Threat Defense 6.5をインストールできます。

Firepower 4100の要件

Firepower 4100には複数のモデルがあります。次の要件を確認します。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブ インスタンスを1つのみインストールできます。
- 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Firewall Threat Defense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。

インターフェイスに関する注意事項と制限事項

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では、Burned-In MAC Address を使用します。
- EtherChannel: EtherChannelの場合は、そのチャ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透過的になります。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からです。ポートチャネル インターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

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

Firewall Threat Defenseと ASA 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。

ハイ アベイラビリティ

- アプリケーション設定内で高可用性を設定します。
- 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。 データ共有インターフェイスはサポートされていません。

コンテキストモード

- 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。

ハイアベイラビリティの要件と前提条件

- 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。

- 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
- 同じモデルであること。
- 高可用性論理デバイスに同じインターフェイスを割り当てること。
- 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ますが、2 つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。
- その他のハイ 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。

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無効になっています。インターフェイスの有効化、Etherchannel の追加、VLAN サブインターフェイスの、インターフェイスプロパティの編集、を実行できます。

（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 構成では元のコマンドが保持されます。構成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 [管理状態（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無効になっています。

手順

ステップ 1 [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ページを開きます。

[インターフェイス]ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、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ます。

ステップ 2 インターフェイスを有効にするには、[disabled **Slider disabled**（  ）] をクリックして、[enabled **Slider enabled**（  ）] に変更します。

[はい]をクリックして、変更を確認します。視覚的表現の対応するインターフェイスがグレイから緑に変化します。

ステップ 3 インターフェイスを無効にするには、[有効なスライダ（enabled **Slider enabled**（  ））] をクリックして、[無効なスライダ（disabled **Slider disabled**（  ））] に変更します。

[はい]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。

（注）
- QSFPH40G-CUxMの場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。
- ポートのSFPを別のSFPモジュールに交換しても、インターフェイスの速度、デュプレックス、および自動ネゴシエーションは自動的に更新されません。インターフェイスを再構成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有効にするには、[有効（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）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （2 ページ）を参照してください。

- **データ**
- **管理**
- [クラスタ（Cluster）] : [クラスタ（Cluster）] タイプは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 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） [デュプレックス（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 （任意） **デバウンス時間（ミリ秒）**を明示的に設定します。0 から 15000 ミリ秒の値を入力します。

（注）
デバウンス時間の設定は、1G インターフェイスではサポートされていません。

ステップ 9 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。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。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。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。

- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

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。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）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 [一時停止（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）] または [ダウン（Down）] 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 [ポート チャネルの追加（Add Port Channel）] をクリックし、[ポート チャネルの追加（Add Port Channel）] ダイアログボックスを開きます。

ステップ 3 [ポート チャネル ID（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、ポートチャネル

48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。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 チャネルを有効にするには、[有効化（Enable）] チェックボックスをオンにします。ポート チャ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 [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （2 ページ）を参照してください。

- **データ**
- **管理**
- **クラスタ**

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に適した [管理速度（Admin Speed）] を設定します。

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。

ステップ 7 データインターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

インターフェイスの場合、モードは常にアクティブです。

ステップ 8 メンバーインターフェイスに適した [管理デュプレックス（Admin Duplex）] を設定します（[全二重（Full Duplex）] または [半二重（Half Duplex）]）。

指定したデュプックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。

ステップ 9 ポート チャ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。

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

ヒント
複数のインターフェイスを一度に追加できます。個々のインターフェイスを複数選択するには、**Ctrl** キーを押しながら必要なインターフェイスをクリックします。インターフェイスの範囲を選択するには、範囲の最初にあたるインターフェイスを選択し、次に **Shift** キーを押しながらその範囲の最後にあたるインターフェイスをクリックします。

ステップ 10 ポートチャ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 11 [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_278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またはトランスペアレント ファイアウォール モード ASA を展開できます。

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、そのイメージを Firepower 4100/9300 シャーシ。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

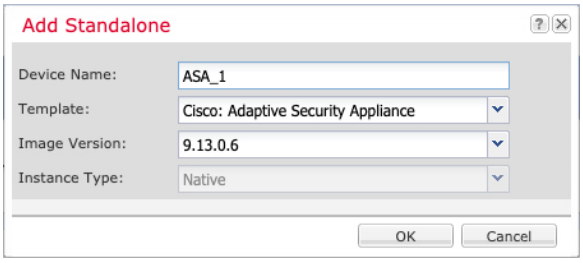
- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id

- 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 **[追加（Add）] > [スタンドアロン（Standalone）]** 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。

この名前は、シャーシスーパーバイザ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。これはアプリケーション設定で使用されるデバイス名ではありません。

（注）
論理デバイスの追加後にこの名前を変更することはできません。

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

ステップ 3 [データ ポート（Data Ports）] 領域を展開し、デバイスに割り当てる各ポートをクリックします。

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。後で、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。これには、IP アドレスの設定も含まれます。

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。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。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 [一般情報（General Information）] ページで、次の手順を実行します。

a) （Firepower 9300 の場合）[セキュリティモジュールの選択（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。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

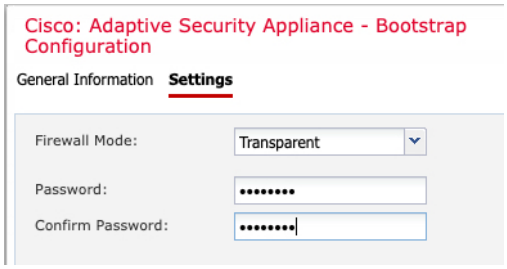
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。

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 [設定（Settings）] タブをクリックします。



ステップ 7 [Firewall Mode] を [Routed] または [Transparent] に指定します。

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

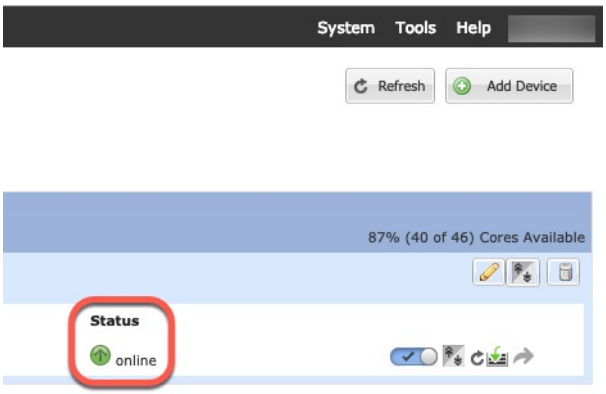
ステップ 8 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザ/パスワードおよびイネーブル 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/イネーブル パスワードを忘れたときにリセットできます。

ステップ 9 [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 10 **[保存（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 11 セキュリティ ポリシーの設定を開始するには、『ASA 設定ガイド』を参照してください。

ハイ アベイラビリティ ペアの追加

Firewall Threat DefenseASA 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

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 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 2 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つのシャーシ間で高可用性トラフィックを交換します。フェールオーバーリンクとステートリンクの組み合わせには、10 GB 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。使用可能なインターフェイスがある場合は、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクには、最も多く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。シャーシ間でスイッチを使用することをお勧めします。この場合、フェールオーバーインターフェイスと同じネットワークセグメント上に他のデバイスを配置できません。

ステップ 3 論理デバイスで高可用性を有効にします。 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 4 高可用性を有効にした後にインターフェイスを変更する必要がある場合は、最初にスタンバイユニットで変更を実行してから、アクティブユニット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やEtherChannel を削除したり、インターフェイスを EtherChannel に再割り当てしたりすると）、必要な調整を行うために、ASA設定に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、幅広い影響を与え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 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 （10 ページ）およびEtherChannel（ポート チャネル）の追加 （11 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に追加する場合(たとえば、すべてのインターフェイスがデフォルトでクラスタに割り当てられる場合)、最初にそのインターフェイスを論理デバイスから割り当て解除してから、EtherChannelに追加する必要があります。新しいEtherChannelの場合、EtherChannelをデバイスに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。最初にデータ/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、制御/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 Firewall シャーシ マネージャで、[論理デバイス]を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックし、その論理デバイスを編集します。

ステップ 3 データ インターフェイスの割り当てを解除するには、[データ ポート（Data Ports）] 領域でそのインターフェイスの選択を解除します。

ステップ 4 [データ ポート（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) [一般/クラスタ情報（General/Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（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

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

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。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

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。

connect asa *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect asa asa1
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** と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

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**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
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>connect asa asa1
asa> ~
```

```
telnet> quit
Connection closed.
Firepower#
```

論理デバイスの履歴

機能	バージョン	詳細
Firepower 4112 用の ASA	9.14(1)	Firepower 4112 を導入しました。 （注） FXOS 2.8.1 が必要です。
Firepower 9300 SM-56 のサポート	9.12.2	SM-56 セキュリティ モジュールが導入されました。 （注） FXOS 2.6.1.157 が必要です。
Firepower 4115、4125、および 4145 向け ASA	9.12(1)	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1 が必要です。
Firepower 9300 SM-40 および SM-48 のサポート	9.12.1	セキュリティ モジュールの SM-40 と SM-48 が導入されました。 （注） FXOS 2.6.1 が必要です。
ASA および Firewall Threat Defense を同じ Firepower 9300 の別のモジュールでサポート	9.12.1	ASA および Firewall Threat Defense 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。

機能	バージョン	詳細
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	9.10.1	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 （注） FXOS 2.4.1 が必要です。 新規/変更された [Firepower Chassis Manager] 画面： **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** > **[クラスタ情報（Cluster Information）]** > [CCL Subnet IP] フィールド
オン モードでのデータ EtherChannel のサポート	9.10.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 （注） FXOS 2.4.1 が必要です。 新規/変更された [Firepower Chassis Manager] 画面： **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[ポート チャネルの編集（Edit Port Channel）]** > **[モード（Mode）]**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]**
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。

機能	バージョン	詳細
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 つのセキュリティ 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。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。