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 Chassis 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 Chassis 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、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
Firewall Threat Defense	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。

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 インターフェイスモードに入ります。

scope eth-uplink

scope fabric a

ステップ 2 インターフェイスを有効にします。

enter interface *interface_id*

enable

例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

（注）
すでにポートチャネルのメンバであるインターフェイスは個別に変更できません。ポートチャネルのメンバであるインターフェイスで **enter interface** コマンドまたは **scope interface** コマンドを使用すると、オブジェクトが存在しないことを示すエラーを受け取ります。ポートチャネルに追加する前に、**enter interface** コマンドを使用してインターフェイスを編集する必要があります。

ステップ 3 （任意）デバウンス時間を設定します。

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

例：

（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 4 （オプション）インターフェイスタイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data キーワードがデフォルトのタイプです。**cluster** キーワード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 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 6 インターフェイスの速度を設定します。

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

ステップ 7 インターフェイスのデュプレックスモードを設定します。

set admin-duplex {**fullduplex** | **halfduplex**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

ステップ 8 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 9 設定を保存します。

commit-buffer

例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

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（1GBインターフェイスと10GB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 インターフェイス モードを開始します。

scope eth-uplink

scope fabric a

ステップ 2 ポートチャネルを作成します。

create port-channel *ID*

enable

ステップ 3 メンバ インターフェイスを割り当てます。

create member-port *interface_id*

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（1GBインターフェイスと10GBインターフェイスなど）を混在させることはできません。

例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

ステップ 4 （任意） インターフェイス タイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data キーワードがデフォルトのタイプです。デフォルトの代わりにこのポートチャネルをクラスタ制御リンクとして使用する場合以外は、**cluster** キーワードを選択しないでください。

ステップ 5 ポートチャネルのメンバーに適したインターフェイス速度を設定します。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

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。デフォルトは **10gbps** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

ステップ 6 （任意） ポートチャネルのメンバーに適したデュプレックスを設定します。

set duplex {**fullduplex** | **halfduplex**}

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。デフォルトは **fullduplex** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

ステップ 7 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 8 データインターフェイスの LACP ポート チャネル モードを設定します。

非データインターフェイスの場合、モードは常にアクティブです。

set port-channel-mode {**active** | **on**}

例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

ステップ 9 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 10 設定をコミットします。

commit-buffer

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_225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（FXOS では、MGMT、management0 のような名前で表示されます）。
- 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 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 2 アプリケーション インスタンスのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号を書き留めます。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

scope slot *slot_ID*

slot_id は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) アプリケーション インスタンスを作成します。

enter app-instance asa *devicename*

*Device_name*は、1 ～ 64 文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例：

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) ASA イメージバージョンを選択します。

set startup-version *version*

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) スロット モードを終了します。

exit

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 終了して ssa モードにします。

exit

例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 3 論理デバイスを作成します。

enter logical-device *device_name* **asa** *slot_id* **standalone**

以前に追加したアプリケーション インスタンスと同じ*device_name*を使用します。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 4 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name*：この名前は Firepower 4100/9300 シャーシ スーパーバイザによって使用されます。これは ASA の設定で使用するインターフェイス名ではありません。
- *description*：フレーズを引用符（"）で囲み、スペースを追加します。

管理インターフェイスは、シャーシ管理ポートと同じではありません。ASA のデータ インターフェイスを後で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。

例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) ファイアウォール モード（「ルーテッド」または「トランスペアレント」）を指定します。

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

ルーテッドモードでは、デバイスはネットワーク内のルータ 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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) IPv6 管理インターフェイスを設定します。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 6 設定を保存します。

commit-buffer

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。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State（管理状態）] が [Enabled（有効）] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- ---------------
--------------- ------------ ------------ ---------- ---------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
       Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
       Container   Default-Small Not Applicable  None
```

ステップ 7 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。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

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 （9 ページ）およびEtherChannel（ポート チャネル）の追加 （12 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。
- 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 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

Firepower /ssa # **scope logical-device** *device_name*

ステップ 3 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ます。

Firepower /ssa/logical-device # **delete external-port-link** *name*

インターフェイス名を表示するには、**show external-port-link**コマンドを入力します。

管理インターフェイスの場合、新しい管理インターフェイスを追加する前に、現在のインターフェイスを削除し、**commit-buffer** コマンドを使用して変更をコミットします。

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

ステップ 5 設定を確定します。

commit-buffer

トランザクションをシステムの設定にコミットします。

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。
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 FXOS コマンド： **set cluster-control-link network**

機能	バージョン	詳細
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 FXOS コマンド：**set port-channel-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。 次のコマンドが変更されました。**site-id**
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。 変更されたコマンドはありません。
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。 変更されたコマンドはありません。
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。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

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。