



## 論理デバイス

---

- [論理デバイスについて \(1 ページ\)](#)
- [論理デバイスの要件と前提条件 \(11 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(16 ページ\)](#)
- [スタンドアロン論理デバイスの追加 \(22 ページ\)](#)
- [ハイ アベイラビリティ ペアの追加 \(31 ページ\)](#)
- [クラスタの追加 \(32 ページ\)](#)
- [Radware DefensePro の設定 \(55 ページ\)](#)
- [TLS 暗号化アクセラレーションの設定 \(61 ページ\)](#)
- [論理デバイスの管理 \(66 ページ\)](#)
- [\[論理デバイス \(Logical Devices\) \] ページ \(76 ページ\)](#)
- [サイト間クラスタリングの例 \(79 ページ\)](#)
- [論理デバイスの履歴 \(83 ページ\)](#)

## 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 の場合は、異なるアプリケーションタイプ (ASA および FTD) 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。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。

## 論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

アプリケーションインスタンスは次の展開タイプで実行します。

- **ネイティブ インスタンス**：ネイティブ インスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブインスタンスを1つだけインストールできます。
- **コンテナ インスタンス**：コンテナ インスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。マルチインスタンス機能は、FMC を使用する Firepower Threat Defense でのみサポートされています。ASA ではサポートされていません。



(注) マルチインスタンス機能は、実装は異なりますが、ASA マルチコンテキストモードに似ています。マルチコンテキストモードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Firepower Threat Defense のフル機能のサポートが可能です。マルチコンテキストモードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。マルチコンテキストモードは Firepower Threat Defense では利用できません。

Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。

## コンテナ インスタンス インターフェイス

コンテナ インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイス (VLAN または物理) を共有することができます。ネイティブのインスタンスは、VLAN サブインターフェイスまたは共有インターフェイスを使用できません。共有インターフェイスの拡張性およびコンテナ インスタンスの VLAN サブインターフェイスの追加を参照してください。

## シャーシがパケットを分類する方法

シャーシに入ってくるパケットはいずれも分類する必要があります。その結果、シャーシは、どのインスタンスにパケットを送信するかを決定できます。

- 一意のインターフェイス : 1つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループメンバー インターフェイス (トランスペアレント モードまたはルーテッド モード)、インラインセット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意の MAC アドレス : シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有の MAC アドレスが使用されます。固有の MAC アドレスがないと、アップストリームルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。ただし、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

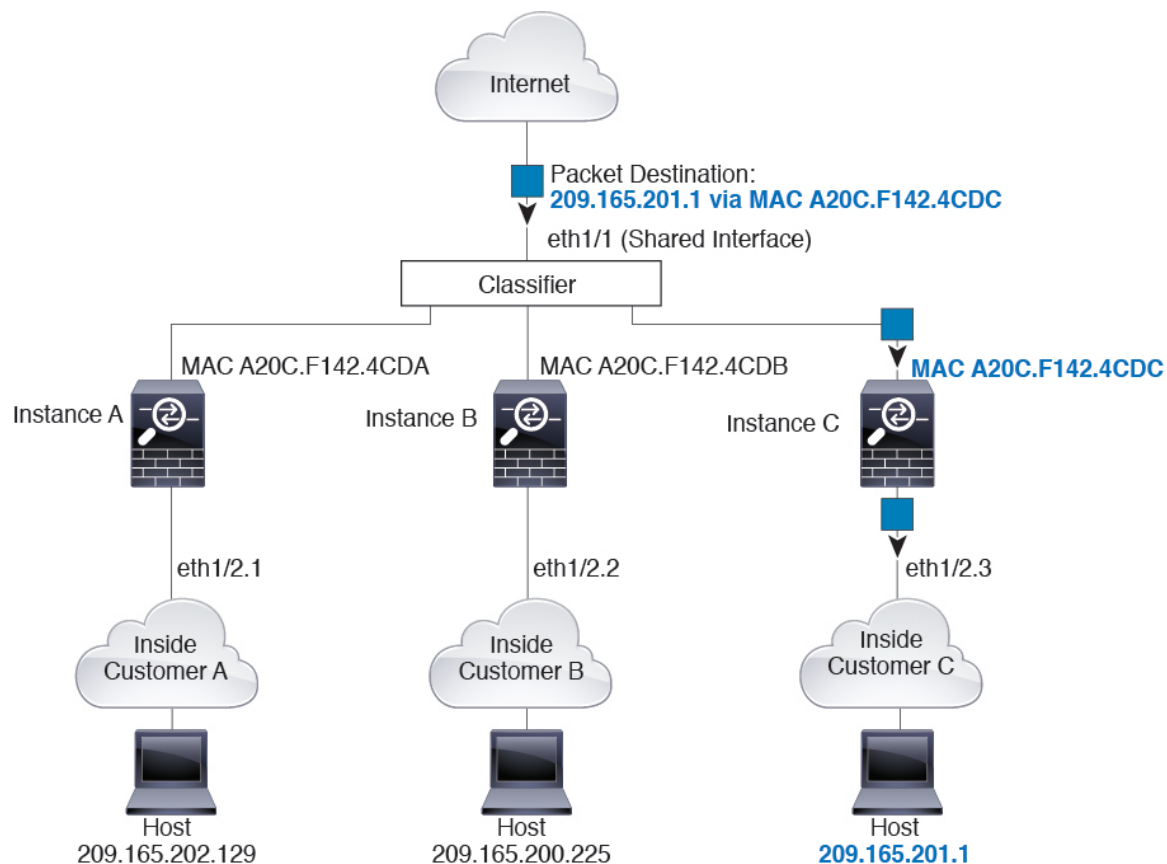


(注) 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製されて各インスタンスに送信されます。

## 分類例

次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンス C にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

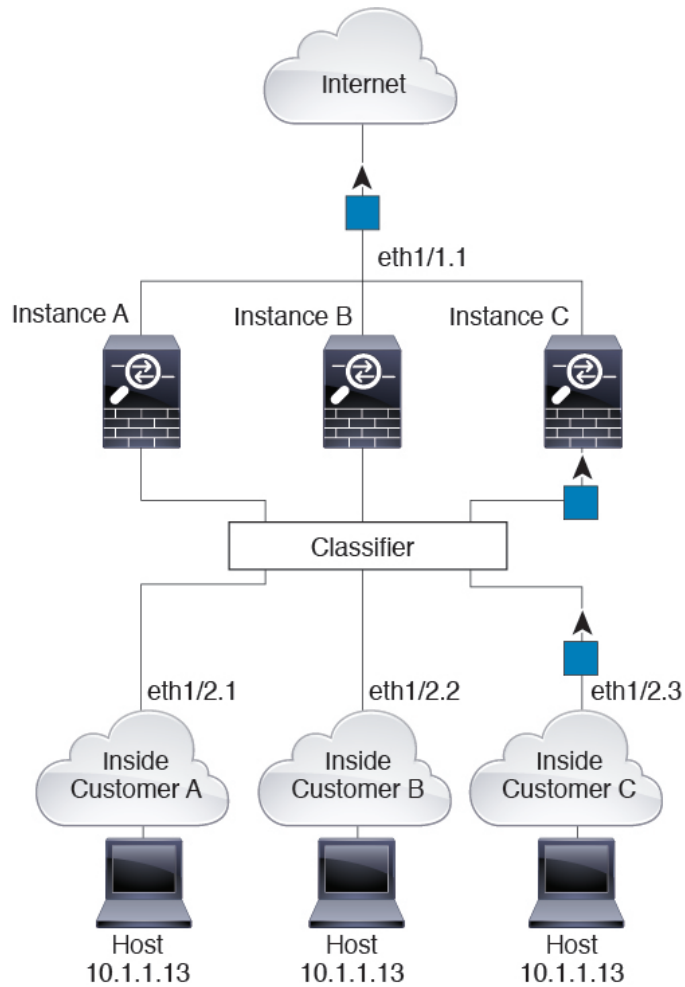
図 1: MAC アドレスを使用した共有インターフェイスのパケット分類



内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンスCに割り当てられているためです。

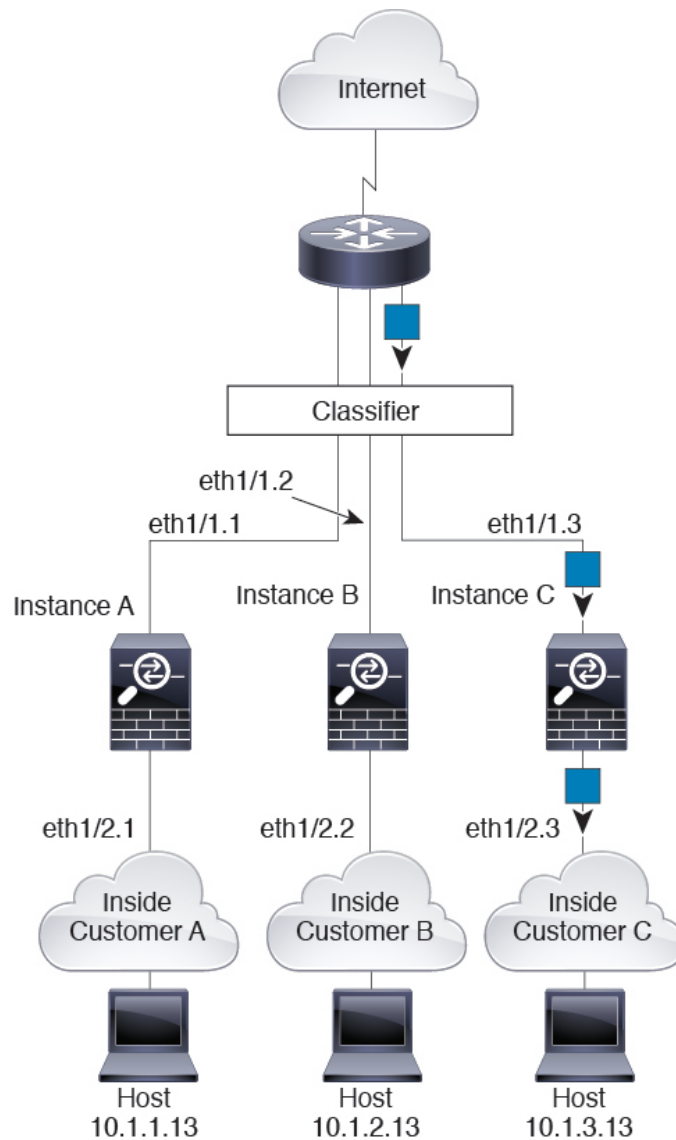


図 2: 内部ネットワークからの着信トラフィック



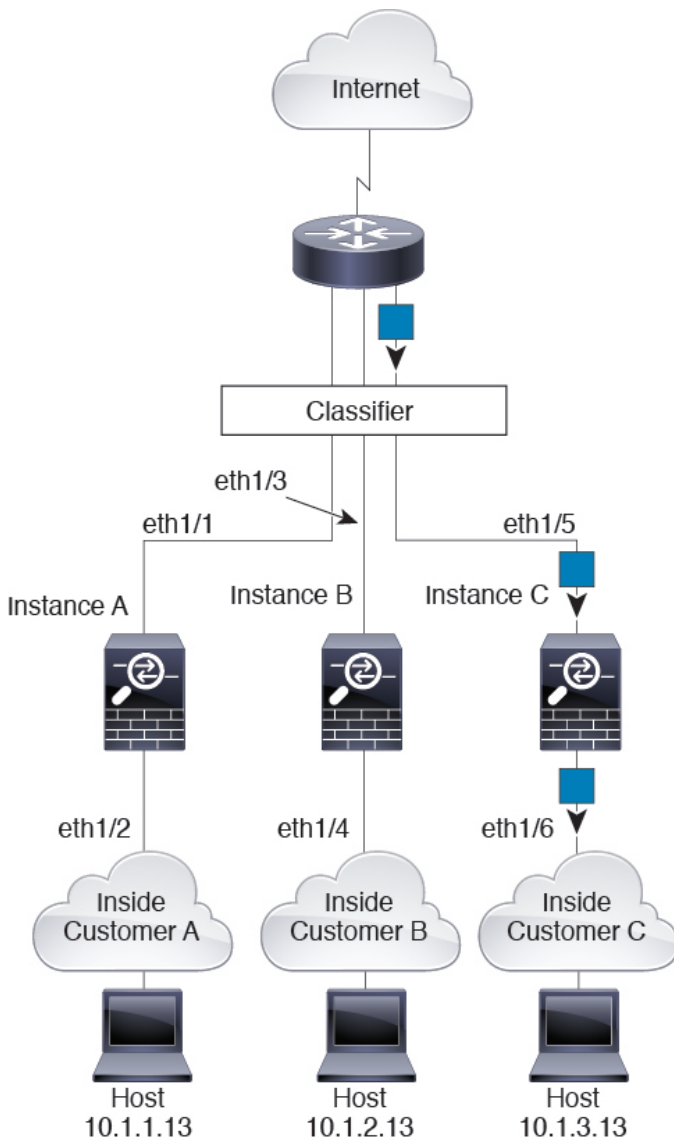
トランスパレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンスCに割り当てられているためです。

図 3: トランスパアレントファイアウォールインスタンス



インラインセットの場合は一意のインターフェイスを使用する必要があります。また、それらのセットは物理インターフェイスか、またはEtherChannelである必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/5 で、このイーサネットがインスタンスCに割り当てられているためです。

図 4: FTD のインラインセット

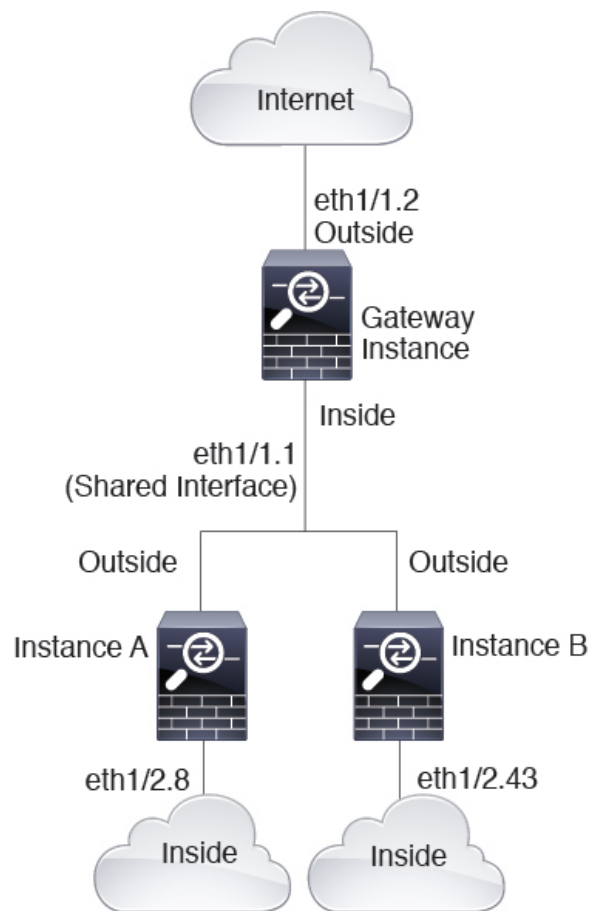


## コンテナ インスタンスのカスケード

別のインスタンスの前にコンテナインスタンスを直接配置することをカスケード コンテナ インスタンスと呼びます。1つのインスタンスの外部インターフェイスは、別のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスのコンフィギュレーションを単純化する場合、最上位インスタンスの共有パラメータを設定することで、インスタンスをカスケード接続できます。

次の図に、ゲートウェイの背後に2つのインスタンスがあるゲートウェイインスタンスを示します。

図 5: コンテナ インスタンスのカスケード

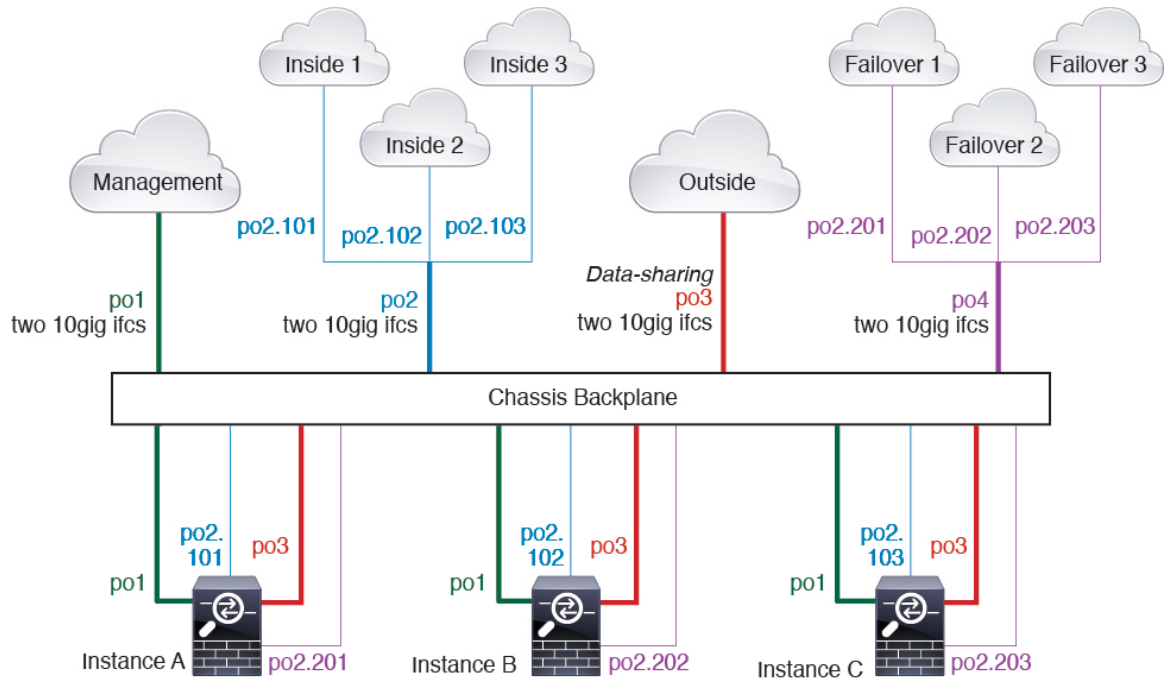


## 一般的な複数インスタンス展開

次の例には、ルーテッドファイアウォールモードのコンテナインスタンスが3つ含まれます。これらには次のインターフェイスが含まれます。

- **管理**：すべてのインスタンスがポートチャネル1インターフェイス（管理タイプ）を使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意的 IP アドレスを使用します。
- **内部**：各インスタンスがポートチャネル2（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。
- **外部**：すべてのインスタンスがポートチャネル3インターフェイス（データ共有タイプ）を使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意的 IP アドレスを使用します。

- フェールオーバー：各インスタンスがポートチャネル4（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの 10 ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。



## コンテナ インスタンス インターフェイスの自動 MAC アドレス

FXOS シャーシは、各インスタンスの共有インターフェイスが一意的な MAC アドレスを使用するように、コンテナインスタンスインターフェイスの MAC アドレスを自動的に生成します。

アプリケーション内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、アプリケーション内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まるため、アドレスが重複するリスクがあることから手動 MAC アドレスを A2 で始めることはできません。



- (注) MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意的な MAC アドレスを使用します。

FXOS シャーシは、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yyはユーザ定義のプレフィックスまたはシステム定義のプレフィックスで、zz.zzzzはシャースが生成した内部カウンタです。システム定義のプレフィックスは、IDPROMにプログラムされている Burned-in MAC アドレス プール内の最初の MAC アドレスの下部 2 バイトと一致します。**connect fxos**を使用し、次に**show module**を使用して、MAC アドレスプールを表示します。たとえば、モジュール 1 について示されている MAC アドレスの範囲が b0aa.772f.f0b0 ~ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例を挙げます。プレフィックスとして 77 を指定すると、シャースは 77 を 16 進数値 004D (yyxx) に変換します。MAC アドレスで使用すると、プレフィックスはシャースネイティブ形式に一致するように逆にされます (xyyy)。

A24D.00zz.zzzz

プレフィックス 1009 (03F1) の場合、MAC アドレスは次のようになります。

A2F1.03zz.zzzz

## コンテナ インスタンスのリソース管理

コンテナ インスタンスごとのリソース使用率を指定するには、FXOS で 1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40GB に設定されます。モデルごとに使用可能なリソースを表示するには、[コンテナ インスタンスの要件と前提条件 \(15 ページ\)](#) を参照してください。リソース プロファイルを追加するには、[コンテナ インスタンスにリソース プロファイルを追加](#) を参照してください。

## マルチインスタンス機能のパフォーマンス スケーリング係数

プラットフォームの最大接続数は、ネイティブ インスタンスがメモリと CPU を使用するために計算されます (この値は **show resource usage** に示されます)。ただし、マルチインスタンス機能を使用する場合、使用可能な最大接続数は、1 つのネイティブ インスタンス用の接続数未満 (約 70 ~ 80 %) になり、ネットワークによってはスケーリングが改善または悪化する可能性があります。たとえば、次の比較を参照してください。

- Firepower 9300 SM-24
- ネイティブ インスタンスの最大同時接続数 : 30,000,000
- マルチインスタンスの最大同時接続数 (単一インスタンスを使用する場合) : 約 21,000,000 ~ 24,000,000

複数のインスタンスを使用する場合は、インスタンスに割り当てる CPU コアの割合に基づいてスループットを計算する必要があります。インスタンスのスループットを計算する方法の詳細については、<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-742018.html> を参照してください。

## コンテナインスタンスおよびハイアベイラビリティ

2つの個別のシャーシでコンテナインスタンスを使用してハイアベイラビリティを使用できません。たとえば、それぞれ10個のインスタンスを使用する2つのシャーシがある場合、10個のハイアベイラビリティペアを作成できます。ハイアベイラビリティはFXOSで構成されません。各ハイアベイラビリティペアはアプリケーションマネージャで構成します。

詳細な要件については、「[ハイアベイラビリティの要件と前提条件 \(15 ページ\)](#)」と「[ハイアベイラビリティペアの追加 \(31 ページ\)](#)」を参照してください。



(注) クラスタリングはサポートされません。

## 論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

### 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 に異なる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-36 をモジュール 1、SM-40 をモジュール 2、SM-44 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せん。
- **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。同じシャーシに1つのSM-24および2つのSM-36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SM-36、SM-40、およびSM-44を配置できます。SM-36モジュール間、SM-40モジュール間、およびSM-44モジュール間のハイアベイラビリティペアを作成できます。
- ASA およびFTD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FTDをインストールすることができます。
- 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、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。

- 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。
- FTD コンテナインスタンスのバージョン：同じモジュール上で異なるバージョンのFTDを個別のコンテナインスタンスとして実行できます。

## クラスタリングの要件と前提条件

### クラスタ モデルのサポート

- Firepower 9300上のASA：最大16モジュール。たとえば、16のシャーシで1つのモジュールを使用したり、8つのシャーシで2つのモジュールを使用して、最大16のモジュールを組み合わせることができます。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。シャーシ内、シャーシ間、およびサイト間クラスタリングでサポート。



- Firepower 4100 シリーズ 上の ASA : 最大 16 個のシャーシ。シャーシ間、およびサイト間クラスタリングでサポート。
- FTDFirepower 9300 : 1 シャーシ内に最大 3 モジュール。6 モジュールたとえば、3 つのシャーシで 2 つのモジュールを使用したり、2 つのシャーシで 3 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせてたりできます。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。シャーシ内およびシャーシ間クラスタリングでサポート。
- FTDFirepower 4100 シリーズ : 最大 6 シャーシ。シャーシ間クラスタリングでサポート。
- Radware DefensePro : ASA によるシャーシ内クラスタリングでサポート。
- Radware DefensePro : FTD によるシャーシ内クラスタリングでサポート。

### クラスタリングハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ :

- Firepower 4100 シリーズ : すべてのシャーシが同じモデルである必要があります。Firepower 9300 : 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。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 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。
- イメージアップグレード時を除き、同じ FXOS ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じバンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワークモジュールタイプを使用できます。シャーシ間クラスタリングでは、すべてのデータインターフェイスを EtherChannel とする必要があります。(インターフェイスモジュールの追加または削除、あるいは EtherChannel の設定などにより) クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います(スレーブ ユニットから始めて、マスターで終わります)。
- 同じ NTP サーバを使用する必要があります。Firepower Threat Defense のため、Firepower Management Center は同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。
- ASA : 各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。スレーブ ユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defense では、すべてのライセンスは Firepower Management Center で処理されます。

### シャーシ間クラスタリングのスイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『[Cisco FXOS Compatibility](#)』を参照してください。

### サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect (DCI) に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバーの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1つのメンバーに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバーの場合。
  - 合計 4 クラスタ メンバー
  - 各サイト 2 メンバー
  - メンバーあたり 5 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 5 Gbps (2/2 x 5 Gbps)。

- 3 サイトの 6 メンバーの場合、サイズは増加します。
  - 合計 6 クラスタ メンバー
  - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps (3/2 x 10 Gbps)。

- 2 サイトの 2 メンバーの場合。
  - 合計 2 クラスタ メンバー
  - 各サイト 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク (10 Gbps) のサイズ未満にはなりません)。

## 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。
- 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が、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- コンテナインスタンスでは、各装置で同じリソースプロファイル属性を使用する必要があります。
- 他のハイアベイラビリティシステム要件については、アプリケーションの構成ガイドのハイアベイラビリティに関する章を参照してください。

## コンテナインスタンスの要件と前提条件

### サポートされるアプリケーションタイプ

- Firepower 脅威防御

### FTD：モデルごとの最大コンテナインスタンス数とリソース

各コンテナインスタンスに対して、インスタンスに割り当てる CPU コアの数と RAM を指定できます。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスあたり 40 GB に設定されます。

表 1: モデルごとの最大コンテナインスタンス数とリソース

モデル	最大コンテナインスタンス数	使用可能な CPU コア	使用可能な RAM	使用可能なディスクスペース
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB

モデル	最大コンテナ インスタンス 数	使用可能な CPU コア	使用可能な RAM	使用可能なディスクス ペース
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 セキュリ ティモジュール	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 セキュリ ティモジュール	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 セキュリ ティモジュール	13	78	334 GB	1359 GB
Firepower 9300 SM-44 セキュリ ティモジュール	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 セキュリ ティモジュール	15	94	334 GB	1341 GB
Firepower 9300 SM-56 セキュリ ティモジュール	18	110	334 GB	1314 GB

## 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。

### 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。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。

### マルチインスタンスと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。
- コンテナインスタンスによる複数インスタンス機能はFMCを使用するFTDに対してのみ使用できます。
- コンテナインスタンスの場合、各共有インターフェイスを最大14のコンテナインスタンスに割り当てることができます。
- 特定のコンテナインスタンスの場合、最大10個の共有インターフェイスを割り当てることができます。
- FTD コンテナインスタンスの場合、1つの Firepower Management Center でセキュリティモジュール/エンジンのすべてのインスタンスを管理する必要があります。
- の1つのコンテナインスタンスで TLS 暗号化アクセラレーションを有効にできます。
- FTD コンテナインスタンスの場合、次の機能はサポートされていません。
  - クラスタ
  - Radware DefensePro リンク デコレータ
  - FMC バックアップおよび復元
  - FMC UCAPL/CC モード

## クラスタリングガイドラインと制限事項

### シャーン間クラスタリングのスイッチ

- ASR 9006 でデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも14バイト大きい ASR インターフェイス MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR IPv4 MTU と一致する必要があります。
- クラスタ制御リンクインターフェイスのスイッチでは、クラスタユニットに接続されるスイッチポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port** (Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照) を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合がありますので、ロードバランシング アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー

プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。

- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイリンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンクパスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャンネルバンドルのダウンタイムは、設定されているキープアライブインターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャンネルでのハッシュアルゴリズムを固定に変更します。

#### Router(config)# port-channel id hash-distribution 固定

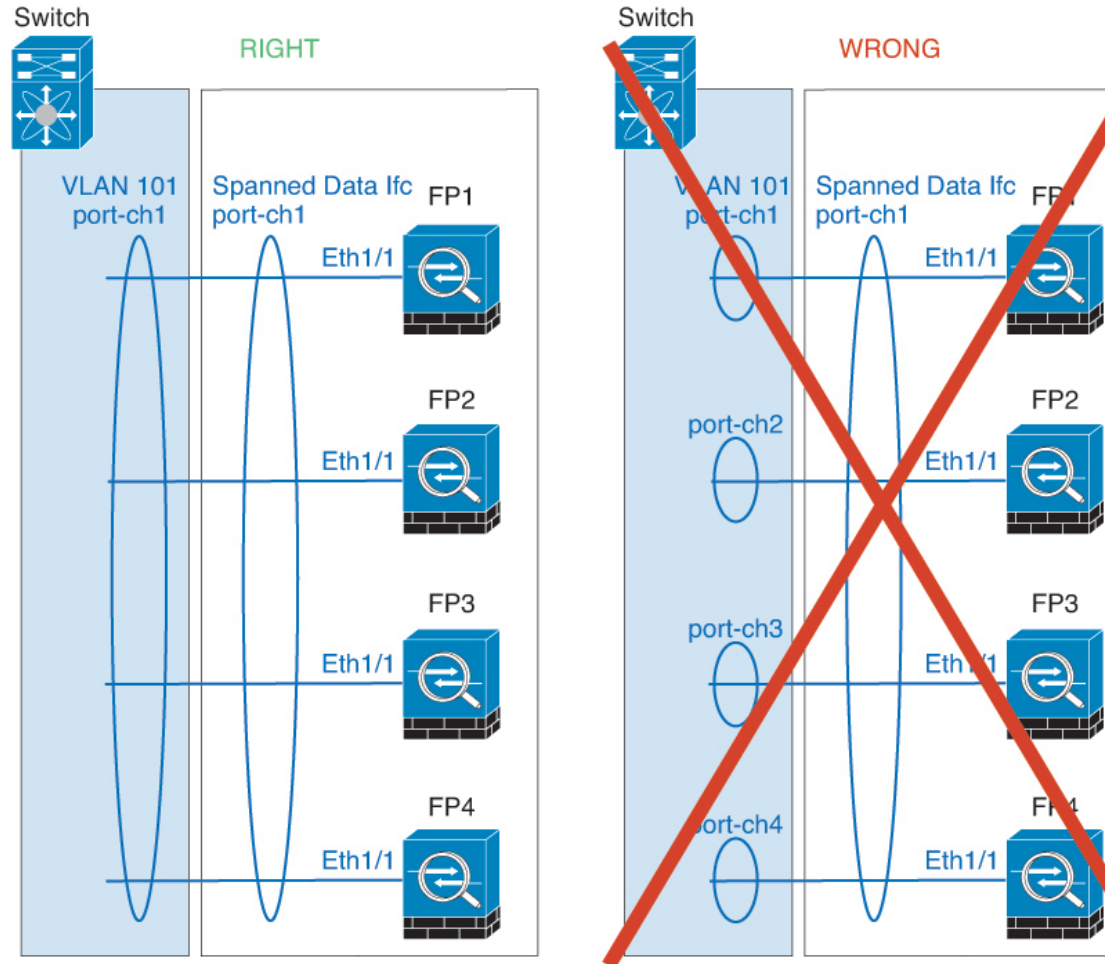
アルゴリズムをグローバルに変更しないでください。VSS ピアリンクに対しては適応型アルゴリズムを使用できます。

- Firepower 4100/9300 クラスタは LACP グレースフルコンバージェンスをサポートしていません。したがって、接続されている Cisco Nexus スイッチで LACP グレースフルコンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速 (fast)] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービスソフトウェアアップグレード (ISSU) を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。

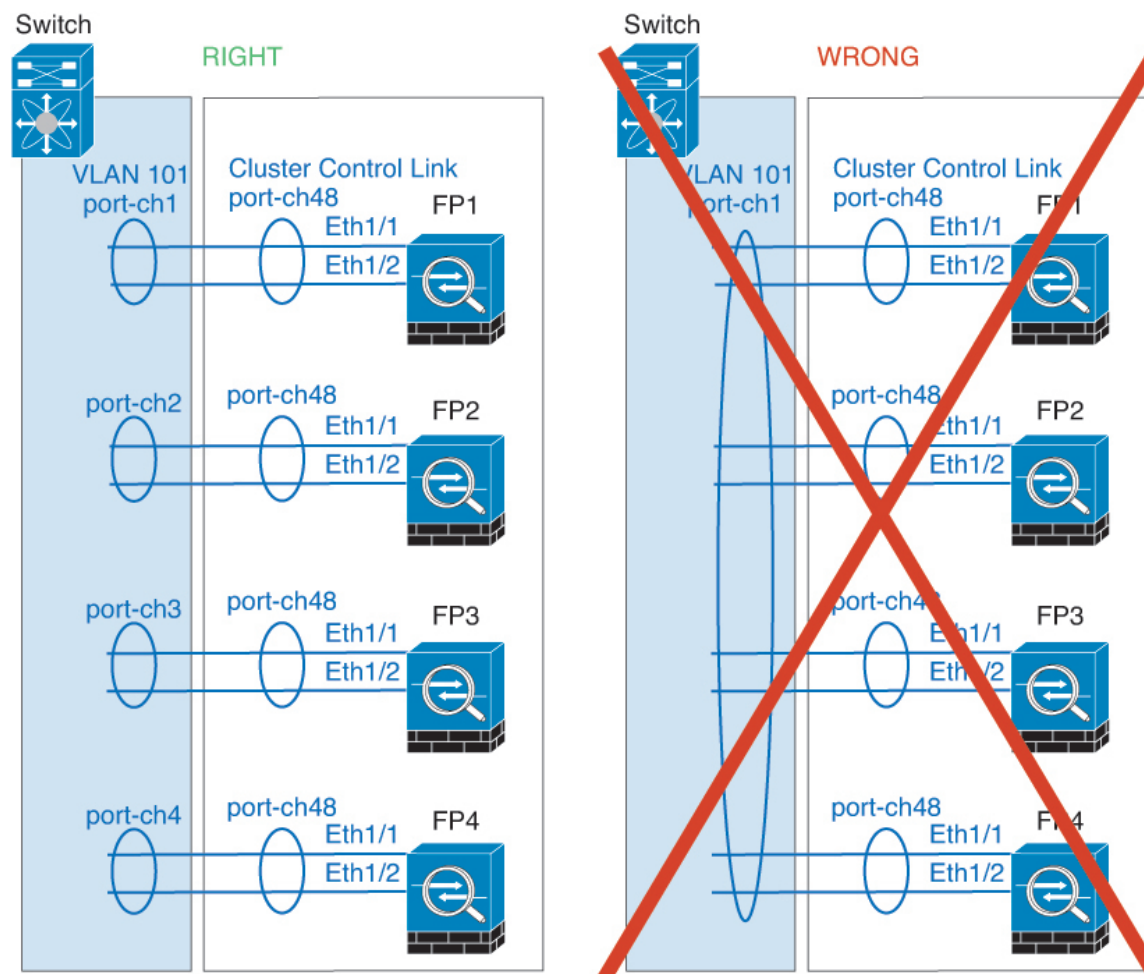
### シャーシ間クラスタリングの EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェアバージョンでは、クラスタユニットはスイッチスタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチソフトウェアバージョンにアップグレードできます。
- スパンド EtherChannel とデバイスローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel とデバイスローカル EtherChannel に対してスイッチを適切に設定します。

- **スパンド EtherChannel** : クラスタ ユニット スパンド EtherChannel (クラスタのすべてのメンバに広がる) の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャンネルグループ内にあることを確認してください。



- **デバイスローカル EtherChannel** : クラスタ ユニット デバイス ローカル EtherChannel (クラスタ制御リンク用に設定された EtherChannel もこれに含まれます) は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



### サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間 (RTT) 20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタメンバーには接続を再分散できません。
- クラスタの実装では、着信接続用の複数のサイトでメンバーが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタローカリゼーションを有効にすると、ローカルディレクタのロールは (サイト ID に従って) 常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生するとローカルディレクタは同じサイトの新しいオーナーを選択します (注: サイト間でトラフィックが非対称で、元のオーナーに



障害が発生した後もリモートサイトから継続的なトラフィックがある場合、リモートサイトのユニットが re-hosting ウィンドウ内でデータパケットを受信する場合はこのリモートサイトのユニットが新しいオーナーとなることがあります)。

- ディレクタローカリゼーションの場合、次のトラフィックタイプはローカリゼーションをサポートしていません：NAT または PAT トラフィック、SCTP 検査済みトラフィック、フラグメンテーションオーナーのクエリ。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じMACアドレスを共有する必要があります。サイト1のクラスタメンバーがサイト2のメンバーに接続を転送するとき、宛先MACアドレスは維持されます。MACアドレスがサイト1のルータと同じである場合にのみ、パケットはサイト2のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイアウォール用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol (FHRP) を使用して、各サイトで同じ仮想IPおよびMACアドレスの宛先を提供します。データVLANは、オーバーレイトランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイルータ宛てのトラフィックがDCI経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイルータが1つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- スパンド EtherChannel を使用したルーテッドモードでは、サイト固有のMACアドレスを設定します。OTVまたは同様のものを使用してサイト全体にデータVLANを拡張します。グローバルMACアドレス宛てのトラフィックがDCI経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが1つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのクラスタユニットに到達できるようにフィルタを削除する必要があります。ダイナミックルーティングは、サイト間クラスタが拡張セグメントのファーストホップルータとして機能する場合はサポートされません。

### その他のガイドライン

- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることとなります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラーメッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。

- シャーシ内では、スタンドアロンモードで一部のシャーシセキュリティ モジュールをクラスタ化し、他のセキュリティモジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

#### デフォルト

- クラスタのヘルスチェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネットヘルスマonitoringが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5分後と、2に設定された増加間隔で合計で3回試行されます。
- HTTPトラフィックでは、5秒間の接続複製遅延がデフォルトで有効になっています。

## スタンドアロン論理デバイスの追加

スタンドアロン論理デバイスは単独またはハイアベイラビリティユニットとして使用できます。ハイアベイラビリティの使用率の詳細については、[ハイアベイラビリティペアの追加 \(31 ページ\)](#) 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 の場合は、異なるアプリケーションタイプ (ASA および FTD) 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。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** [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：

**Add Device** [?] [X]

Device Name:

Template:

Image Version:

Instance Type:

Usage:  Standalone  Cluster

OK Cancel

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。

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) [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** [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。

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。

The screenshot shows the 'Cisco: Adaptive Security Appliance - Bootstrap Configuration' page with the 'Settings' tab selected. Under 'General Information', there are three fields: 'Password' and 'Confirm Password' (both masked with dots), and 'Firewall Mode' (a dropdown menu set to 'Routed').

**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。

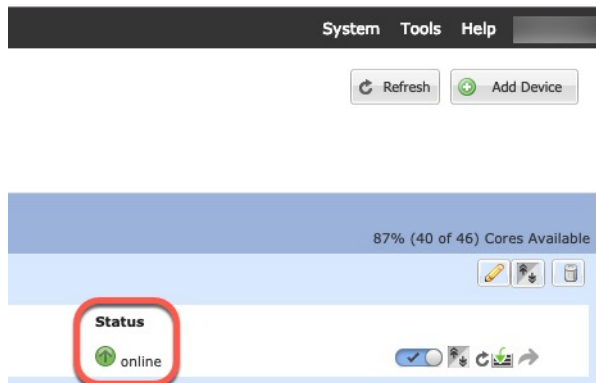
**ステップ 8** 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

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 コンフィギュレーションガイドを参照してください。

## スタンドアロン Firepower Threat Defense 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。

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できます。

## 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。



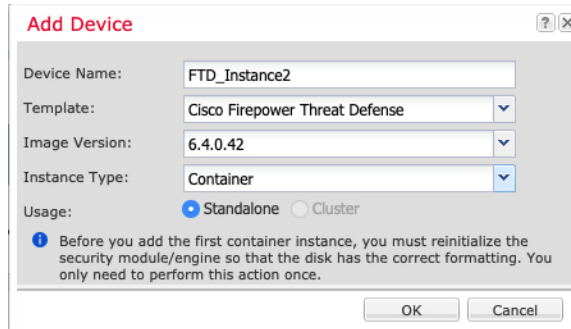
(注) Firepower 9300 の場合は、異なるアプリケーションタイプ (ASA および FTD) をシャーシ内の別個のモジュールにインストールすることができます。別個のモジュールでは、異なるバージョンのアプリケーションインスタンスタイプも実行できます。

- 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)。
- 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。必要に応じて、すべてのイベントのトラフィック (Web イベントなど) を運ぶ `firepower-eventing` インターフェイスも作成できます。詳細については、「[インターフェイスタイプ](#)」を参照してください。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、[コンテナインスタンスにリソースプロファイルを追加](#)に従ってリソースプロファイルを追加します。
- コンテナインスタンスの場合、最初にコンテナインスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティモジュール/エンジンを再度初期化する必要があります。[セキュリティモジュール (Security Modules)] または [セキュリティエンジン (Security Engine)] を選択して、[再初期化 (Reinitialize)] アイコン (🔄) をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。詳細については、[セキュリティモジュール/エンジンの最初期化](#)を参照してください。
- 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
  - FMC 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス
  - FTD ホスト名とドメイン名

## 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。

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。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

c) [Image Version] を選択します。

d) [インスタンスタイプ (Instance Type)] : [コンテナ (Container)] または [ネイティブ (Native)] を選択します。

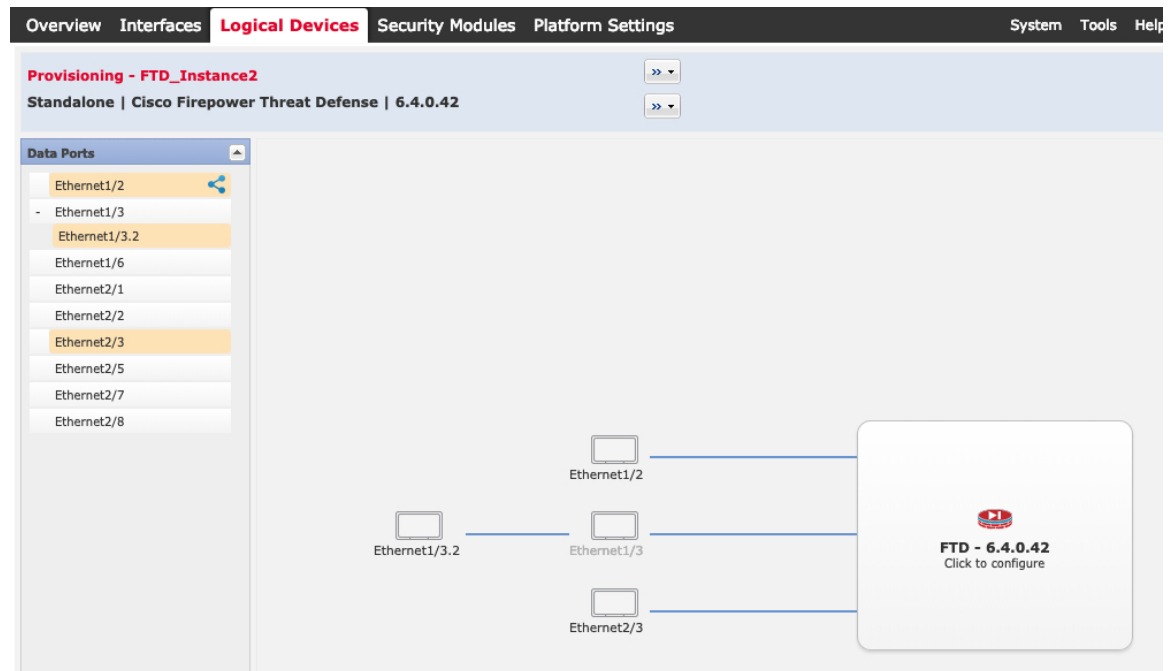
ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース (CPU、RAM、およびディスク容量) を使用するため、ネイティブインスタンスを1つのみインストールできます。コンテナインスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

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インターフェイスをそれぞれクリックします。



[Interfaces] ページでは、以前に有効にしたデータとデータ共有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 FMC の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。

コンテナインスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナインスタンスに割り当てることができます。データ共有インターフェイスは [Sharing] アイコン (🔗) で示されます。

ハードウェアバイパス対応のポートは次のアイコンで表示されます: 🔄。特定のインターフェイスモジュールでは、インラインセットインターフェイスに対してのみハードウェアバイパス機能を有効にできます (FMC 設定ガイドを参照)。ハードウェアバイパスは、停電時にトラフィックがインラインインターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェアバイパスペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェアバイパス機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

**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。



Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

Security Module(SM) and Resource Profile Selection

SM 1 - Ok SM 2 - Ok SM 3 - Empty

SM 1 - 40 Cores Available

Resource Profile: Default-Small

Interface Information

Management Interface: Ethernet1/4

Management

Address Type: IPv4 only

IPv4

Management IP: 10.89.5.22

Network Mask: 255.255.255.192

Network Gateway: 10.89.5.1

- 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) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後で異なるリソースプロファイルを割り当てると、インスタンスがリロードされ、約 5 分かかることがあります。確立されたハイ アベイラビリティ ペアの場合に、異なるサイズのリソースプロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

- c) [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、シャーン管理ポートとは別のものです。
- d) 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)]。
- e) [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的 IP アドレスを設定します。
- f) [Network Mask] または [Prefix Length] に入力します。
- g) **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)] タブで、次の項目を入力します。

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

Registration Key:

Confirm Registration Key:

Password:

Confirm Password:

Firepower Management Center IP:

Permit Expert mode for FTD SSH sessions:

Search domains:

Firewall Mode:

DNS Servers:

Firepower Management Center NAT ID:

Fully Qualified Hostname:

Eventing Interface:

- a) 管理 FMC の [Firepower Management Center IP] を入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。
- b) コンテナ インスタンスに対して、**FTD SSH セッションでエキスパート モードを許可するかどうか**を [Yes] または [No] で指定します。エキスパート モードでは、高度なトラブルシューティングに FTD シェルからアクセスできます。

このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ (No)] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパートモードを使用します。このモードを開始するには、FTD CLI で **expert** コマンドを使用します。

- c) カンマ区切りリストとして [検索ドメイン (Search Domains)] を入力します。
- d) [Firewall Mode] を [Transparent] または [Routed] に選択します。

ルーテッドモードでは、FTD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、トランスパ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。

- e) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、FMCのホスト名を指定する場合、FTDはDNSを使用します。

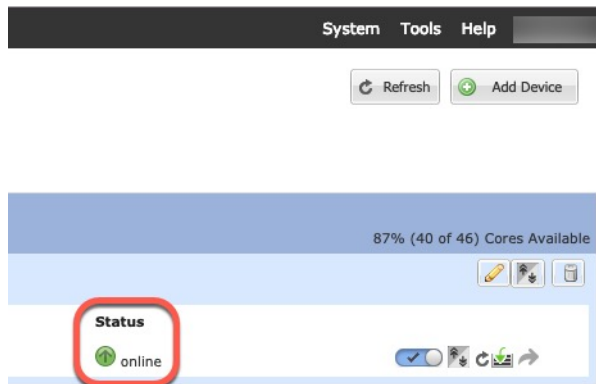
- f) FTDの[Fully Qualified Hostname]を入力します。
- g) 登録時にFMCとデバイス間で共有する[Registration Key]を入力します。  
このキーには、1～37文字の任意のテキスト文字列を選択できます。FTDを追加するときに、FMCに同じキーを入力します。
- h) CLIアクセス用のFTD管理ユーザの[Password]を入力します。
- i) Firepowerイベントの送信に使用する[Eventing Interface]を選択します。指定しない場合は、管理インターフェイスが使用されます。  
このインターフェイスは、Firepower-eventingインターフェイスとして定義する必要があります。

**ステップ7** [Agreement] タブで、エンドユーザライセンス (EULA) を読んで、同意します。

**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** [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10** FTDを管理対象デバイスとして追加し、セキュリティポリシーの設定を開始するには、FMC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の要件と前提条件 (15 ページ) 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つのシャーシの間でハイアベイラビリティトラフィックをやり取りします。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、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。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。

コンテナインスタンスの場合、フェールオーバーリンク用の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。親インターフェイスまたはEtherChannelでサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバーリンクとして使用することをお勧めします。同じ親のすべてのサブインターフェイスをフェールオーバーリンクとして使用する必要があることに注意してください。あるサブインターフェイスをフェールオーバーリンクとして使用する一方で、他のサブインターフェイス（または親インターフェイス）を通常のデータインターフェイスとして使用することはできません。

**ステップ 3** 論理デバイスでハイアベイラビリティを有効にします。

**ステップ 4** 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。

## クラスタの追加

クラスタリングを利用すると、複数のデバイスをグループ化して1つの論理デバイスとすることができます。クラスタは、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）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。複数のモジュールを含む Firepower 9300 は、1つのシャーシ内のすべてのモジュールをクラスタに格

ループ化する、シャーシ内クラスタリングをサポートします。複数のシャーシをまとめてグループ化する、シャーシ間クラスタリングも使用できます。シャーシ間クラスタリングは、Firepower 4100 シリーズなどの単一モジュール デバイスの唯一のオプションです。

## Firepower 4100/9300 シャーシのクラスタリングについて

クラスタは、1つの論理ユニットとして機能する複数のデバイスから構成されます。Firepower 4100/9300 シャーシにクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャンネル 48）を作成します。

シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。

シャーシ間クラスタリングでは、シャーシ間通信用にこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシスーパーバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。シャーシ間クラスタリングでは、すべてのデータインターフェイスでスパンド EtherChannel を使用します。



---

(注) 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

---

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。

### プライマリ ユニットとセカンダリ ユニットの役割

クラスタのメンバの1つがプライマリ ユニットになります。プライマリ ユニットは自動的に決定されます。他のすべてのメンバはセカンダリ ユニットになります。

すべてのコンフィギュレーション作業は標準出荷単位でのみ実行する必要があります。コンフィギュレーションはその後、セカンダリ単位に複製されます。

## クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。

シャーシ間クラスタリングでは、このインターフェイスにメンバーインターフェイスはありません。このクラスタタイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、EtherChannel に 1 つ以上のインターフェイスを追加する必要があります。

2メンバシャーシ間クラスタの場合、シャーシと別のシャーシとの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

### シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロードバランシングが低下するので、すべてのリターントラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

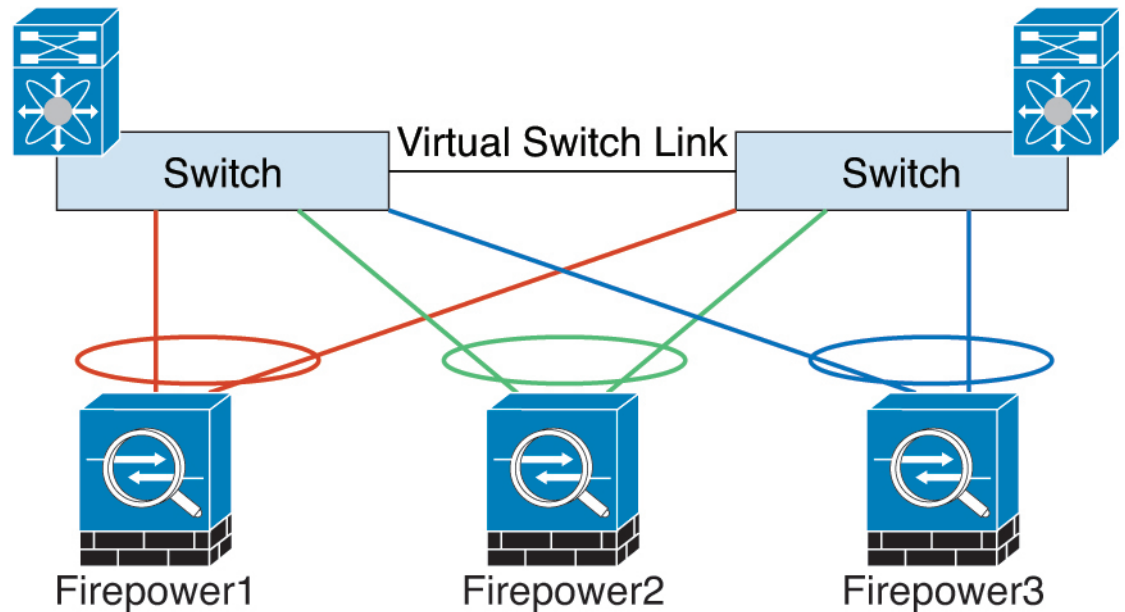


(注) クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

### シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリン

クがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 4100/9300 シャーシ インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



### シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間 (RTT) が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

### クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット 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 インターフェイスの IP アドレスを自動生成します。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。サイト間トラフィックには、オーバーレイ トランスポート 仮想化 (OTV) を使用することをお勧めします。

### 管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

## 管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。

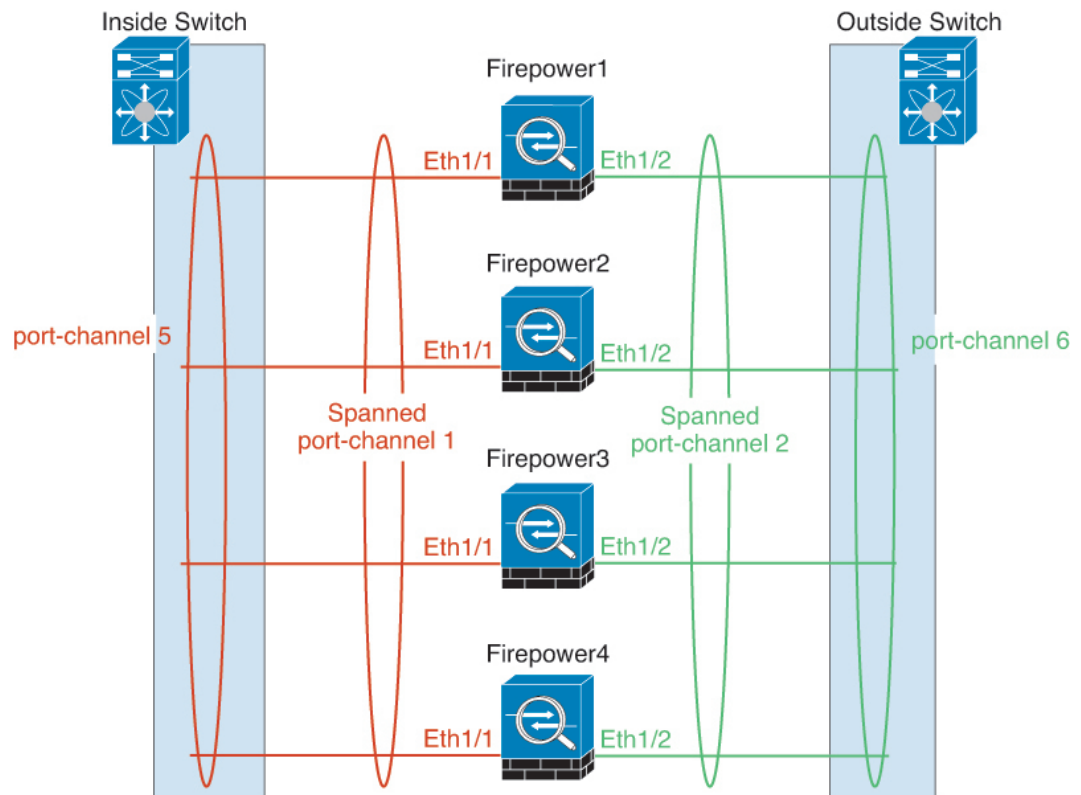
ASA の場合は、メインクラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の標準出荷単位に属します。アドレス範囲も設定して、現在の標準出荷単位を含む各単位がその範囲内のローカルアドレスを使用できるようにする必要があります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。標準出荷単位が変更されると、メインクラスタ IP アドレスは新しい標準出荷単位に移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の標準出荷単位に関連付けられています。個々のメンバーを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、標準出荷単位を含む各単位は、ローカル IP アドレスを使用してサーバに接続します。

Firepower Threat Defense では、同じネットワークの各単位に管理 IP アドレスを割り当てます。各単位を FMC に追加するときは、次の IP アドレスを使用します。

## スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッドモードでは、EtherChannel は単一の IP アドレスを持つルーテッドインターフェイスとして設定されます。トランスペアレントモードでは、IP アドレスはブリッジグループメンバーのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。





## サイト間クラスタリング

サイト間インストールの場合、次の推奨ガイドラインに従う限り、クラスタリングを利用できます。

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッドモードでサポートされます。

サイト ID は、LISP インспекションを使用するフローモビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクタ ローカリゼーション、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング : [クラスタリングの要件と前提条件 \(12 ページ\)](#)
- サイト間のガイドライン : [クラスタリング ガイドラインと制限事項 \(17 ページ\)](#)

- サイト間での例：[サイト間クラスタリングの例](#) (79 ページ)

## ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

## ASA クラスタの作成

クラスタは、Firepower 4100/9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3つのすべてのモジュールでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

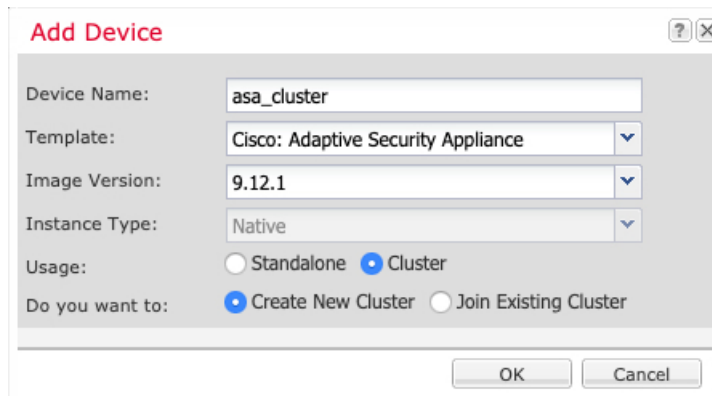
マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

### 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。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレスおよび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** インターフェイスを設定します。
  - ステップ 2** [論理デバイス (Logical Devices)] を選択します。
  - ステップ 3** [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。

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内部で使用します。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。

- b) [テンプレート (Template)] には、[Cisco 適応型セキュリティ アプライアンス (Cisco Adaptive Security Appliance)] を選択します。
- c) [Image Version] を選択します。
- d) [Instance Type] では、[Native] タイプのみがサポートされます。
- e) [Usage] では、[Cluster] オプションボタンをクリックします。
- f) [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。
- g) [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 4** このクラスタに割り当てるインターフェイスを選択します。

デフォルトでは、すべての有効なインターフェイスが割り当てられています。

**ステップ 5** 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 6** [クラスタ情報 (Cluster Information)] ページで、次の手順を実行します。

Cisco: Adaptive Security Appliance - Bootstrap Configuration

**Cluster Information** Settings

**Security Module**

Security Module-1, Security Module-2, Security Module-3

**Interface Information**

Chassis ID: 1

Site ID: 1

Cluster Key: \*\*\*\*

Confirm Cluster Key: \*\*\*\*

Cluster Group Name: asa\_cluster

Management Interface: Ethernet1/4

CCL Subnet IP: Eg:x.x.0.0

**DEFAULT**

Address Type: IPv4 only

**IPv4**

Management IP Pool: 10.89.5.10 - 10.89.5.22

Virtual IPv4 Address: 10.89.5.25

Network Mask: 255.255.255.192

Network Gateway: 10.89.5.1

OK Cancel

- a) シャーシ間クラスタリングでは、**シャーシ 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。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバーインターフェイスを追加した場合にのみ表示されます。

- b) サイト間クラスタリングの場合、[サイト ID (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。
- c) [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。

- d) [クラスタ グループ名 (Cluster Group Name)] を設定します。これは、論理デバイス設定のクラスタ 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。

- e) [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。

- f) (任意) **CCL サブネット IP** を *a.b.0.0* に設定します。

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。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。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定します (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) のアドレスを除く)。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

シャーシは、シャーシ ID とスロット ID (*a.b.chassis\_id.slot\_id*) に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

- g) 管理インターフェイスの [アドレスタイプ (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。次の情報を設定します。

- [管理IPプール (Management IP Pool)] : 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。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。現在のマスターユニットに属する仮想 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。

- ネットワークマスクまたはプレフィックス長

- ネットワークゲートウェイ

- [仮想IPアドレス (VIRTUAL IP address)] : 現在のマスターユニットの管理 IP アドレスを設定します。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、プールに含まれてはなりません。

**ステップ 7** [設定 (Settings)] ページで、以下を実行します。

Cisco: Adaptive Security Appliance - Bootstrap Configuration

Cluster Information **Settings**

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Firewall Mode: Routed

- a) [Firewall Mode] ドロップダウン リストから、[Transparent] または [Routed] を選択します。

ルーテッドモードでは、FTD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。

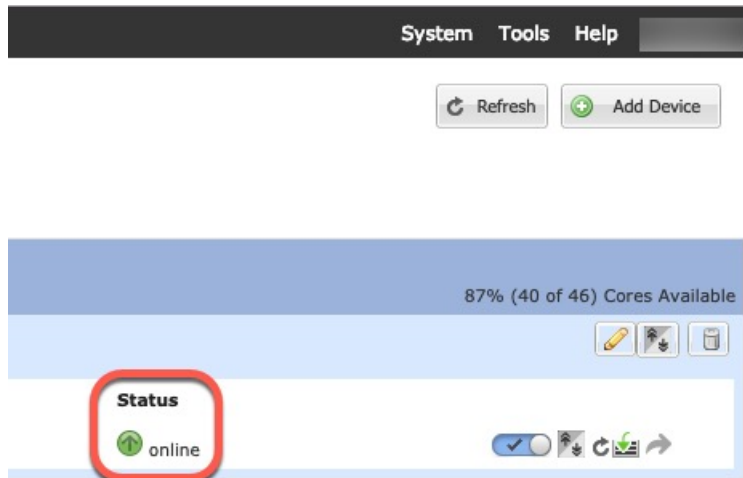
- b) 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

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。


**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** [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 [ステータス (Status) ] に [オンライン (Online) ] と表示されている場合、残りのクラスタシャーシを追加するか、シャーシ内クラスタリングでアプリケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding) ] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



**ステップ 10** 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、右上にある [設定を表示 (Show Configuration) ] アイコン (  ) をクリックして、表示されるクラスタの設定をコピーします。
- b) 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。
- c) [必要な操作 (I want to:)] > [既存のクラスタへの参加 (Join an Existing Cluster) ] を選択します。
- d) [構成のコピー (Copy config) ] チェックボックスをオンにし、[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。
- e) [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。
- f) 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。

- [シャーシ ID (Chassis ID) ] : 一意のシャーシ ID を入力します。

- サイト ID (Site ID) : 正しいサイト ID を入力します。

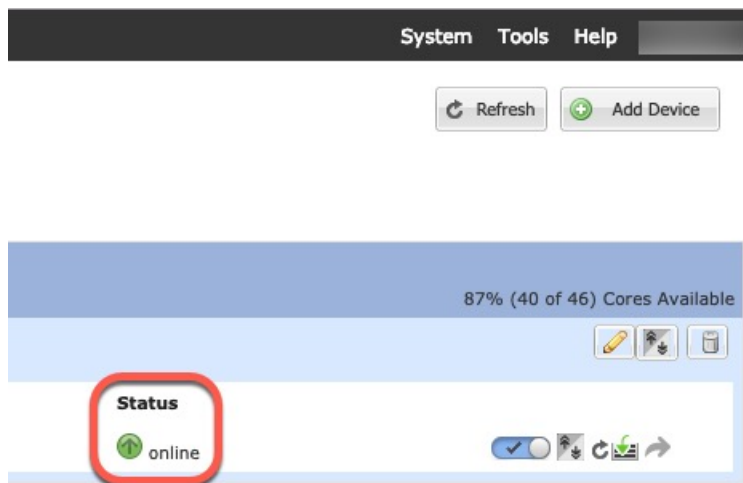
- クラスタ キー (Cluster Key) : (事前に入力されていない) 同じクラスタ キーを入力します。

[OK] をクリックします。

- g) [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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status) ] に [オンライン (Online) ] と表示されたら、アプリケーション

ンでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



**ステップ 11** マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

## クラスタ メンバの追加

ASA クラスタ メンバを追加または置き換えます。




(注) この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

### 始める前に

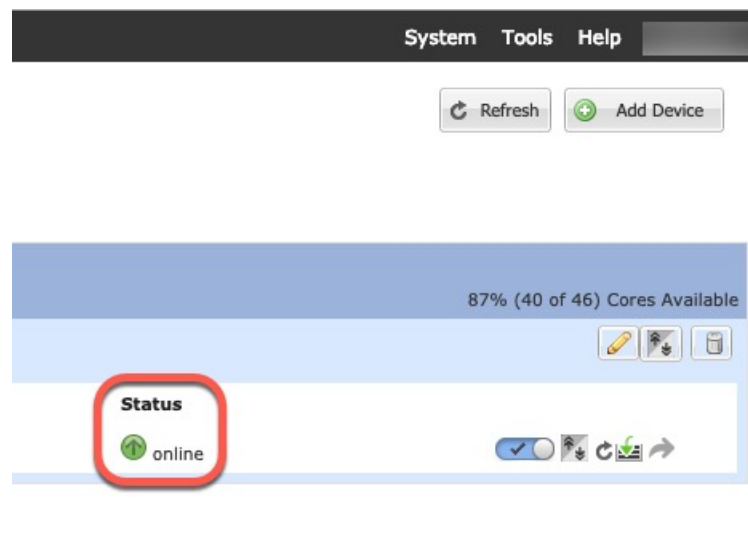
- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。
- マルチコンテキストモードでは、最初のクラスタメンバの ASA アプリケーションでマルチコンテキストモードを有効にします。追加のクラスタメンバはマルチコンテキストモード設定を自動的に継承します。



## 手順

- ステップ 1** 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。
- ステップ 2** 右上の [設定を表示 (Show Configuration) ] アイコン (  ) をクリックして、表示されるクラスタの設定をコピーします。
- ステップ 3** 新しいシャーシの Firepower Chassis Manager に接続して、[デバイスの追加 (Add Device) ] をクリックします。
- ステップ 4** [Device Name] に論理デバイスの名前を入力します。
- ステップ 5** [Template] では、[Cisco Adaptive Security Appliance] を選択します。
- ステップ 6** [Image Version] では、ASA のソフトウェアバージョンを選択します。
- ステップ 7** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 8** [既存のクラスタへの参加 (Join an Existing Cluster) ] を選択します。
- ステップ 9** [Copy config] チェックボックスをオンにして、[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。
- ステップ 10** [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。
- ステップ 11** 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。
- [シャーシ ID (Chassis ID) ] : 一意のシャーシ ID を入力します。
  - **サイト ID (Site ID)** : 正しいサイト ID を入力します。
  - **クラスタ キー (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。
- [OK] をクリックします。
- ステップ 12** [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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status) ] に [オンライン (Online) ] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding) ] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



## Firepower Threat Defense クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

## Firepower Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップコンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3つのすべてのモジュールでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

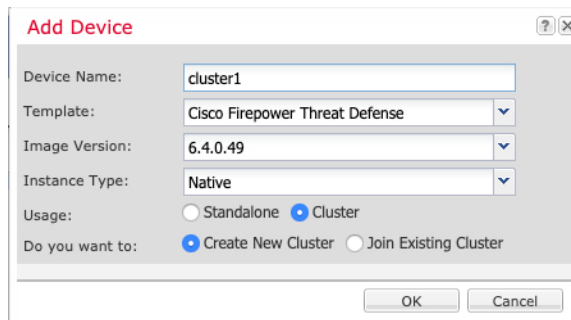
### 始める前に

- 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](https://www.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。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワークマスク
  - ゲートウェイ IP アドレス

- FMC 選択した IP アドレス/NAT ID
- DNS サーバの IP アドレス
- FTD ホスト名とドメイン名

## 手順

- ステップ 1** インターフェイスを設定します。
- ステップ 2** [論理デバイス (Logical Devices)] を選択します。
- ステップ 3** [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。

この名前は、シャード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内部で使用します。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。

- b) [Template] では、[Cisco Firepower Threat Defense] を選択します。
- c) [Image Version] を選択します。
- d) [Instance Type] の場合、[Native] タイプのみがサポートされます。
- e) [Usage] では、[Cluster] オプションボタンをクリックします。
- f) [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。
- g) [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 4** このクラスタに割り当てるインターフェイスを選択します。  
デフォルトでは、すべての有効なインターフェイスが割り当てられます。

- ステップ 5** 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 6** [クラスタ情報 (Cluster Information)] ページで、次の手順を実行します。

図 6:

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box. The 'Cluster Information' tab is selected. The 'Security Module' section shows 'Security Module-1, Security Module-2, Security Module-3'. The 'Interface Information' section contains the following fields: Chassis ID (1), Site ID (1), Cluster Key (\*\*\*\*), Confirm Cluster Key (\*\*\*\*), Cluster Group Name (cluster1), Management Interface (Ethernet1/4), and CCL Subnet IP (Eg:x.x.0.0). There are 'OK' and 'Cancel' buttons at the bottom.

- a) シャーシ間クラスタリングでは、**シャーシ 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。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバーインターフェイスを追加した場合にのみ表示されます。

- b) サイト間クラスタリングの場合、[**サイト ID (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。FlexConfig 機能。ディレクタのローカリゼーション、サイトの冗長性、クラスタフローモビリティなどの冗長性と安定性を向上させるためのサイト間クラスタの追加カスタマイズは、Firepower Management Center flexconfig 機能を使用した場合にのみ設定できます。

- c) [**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。

- d) [**クラスタ グループ名 (Cluster Group Name)**] を設定します。これは、論理デバイス設定のクラスタ 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。

- e) [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。

ハードウェアバイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

- f) (任意) **CCL サブネット IP** を *a.b.0.0* に設定します。

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。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。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定します (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) のアドレスを除く)。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

シャーシは、シャーシ ID とスロット ID (*a.b.chassis\_id.slot\_id*) に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

## ステップ 7 [設定 (Settings) ] ページで、以下を実行します。

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The fields are as follows:

- Registration Key: [Redacted]
- Confirm Registration Key: [Redacted]
- Password: [Redacted]
- Confirm Password: [Redacted]
- Firepower Management Center IP: 10.89.5.35
- Search domains: cisco.com
- Firewall Mode: Routed
- DNS Servers: 72.163.47.11,173.37.137.8
- Firepower Management Center NAT ID: [Empty]
- Fully Qualified Hostname: cluster1.cisco.com
- Eventing Interface: [Empty]

Buttons: OK, Cancel

- a) [登録キー (Registration Key) ] フィールドに、登録時に Firepower Management Center とクラスタ メンバー間で共有するキーを入力します。
- このキーには、1～37文字の任意のテキスト文字列を選択できます。FTDを追加するときに、FMCに同じキーを入力します。
- b) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

- c) [Firepower Management Center の IP (Firepower Management Center IP) ] フィールドに、管理側の Firepower Management Center の IP アドレスを入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。
- d) (任意) [Search Domains] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。
- e) (任意) [ファイアウォール モード (Firewall Mode) ] ドロップダウンリストから、[トランスペアレント (Transparent) ] または [ルーテッド (Routed) ] を選択します。

ルーテッドモードでは、FTD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。

- f) (任意) [DNSサーバ (DNS Servers) ] フィールドに、DNS サーバのカンマ区切りのリストを入力します。

たとえば、FMCのホスト名を指定する場合、FTDはDNSを使用します。

- g) (任意) [Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。このパスフレーズは、新しいデバイスとしてクラスタを追加するときにFMCでも入力します。

通常は、ルーティングと認証の両方の目的で両方のIPアドレス（登録キー付き）が必要です。FMCがデバイスのIPアドレスを指定し、デバイスがFMCのIPアドレスを指定します。ただし、IPアドレスの1つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意のNAT IDを指定する必要があります。NAT IDとして、1～37文字の任意のテキスト文字列を指定できます。FMCおよびデバイスでは、初期登録の認証と承認を行うために、登録キーおよびNAT ID（IPアドレスではなく）を使用します。

- h) (任意) [Fully Qualified Hostname] フィールドに、FTD デバイスの完全修飾名を入力します。

有効な文字は、a～zの文字、0～9の数字、ドット（.）、およびハイフン（-）です。最大文字数は253です。

- i) (任意) [Eventing Interface] ドロップダウンリストから、Firepower イベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

Firepower イベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。ハードウェアパイパス対応のインターフェイスをEventingインターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

**ステップ 8** [インターフェイス情報 (Interface Information)] ページで、クラスタ内のセキュリティモジュールのそれぞれに管理 IP アドレスを設定します。[アドレスタイプ (Address Type)] ドロップダウンリストからアドレスのタイプを選択し、セキュリティモジュールごとに次の手順を実行します。

(注) モジュールがインストールされていない場合でも、シャーシの3つすべてのモジュールスロットで IP アドレスを設定する必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Settings **Interface Information** Agreement

Address Type: IPv4 only

**Security Module 1**  
IPv4  
Management IP: 10.89.5.20  
Network Mask: 255.255.255.192  
Gateway: 10.89.5.1

**Security Module 2**  
IPv4  
Management IP: 10.89.5.21  
Network Mask: 255.255.255.192  
Gateway: 10.89.5.1

**Security Module 3**  
IPv4  
Management IP: 10.89.5.22  
Network Mask: 255.255.255.192  
Gateway: 10.89.5.1

OK Cancel

- [Management IP] フィールドで、IP アドレスを設定します。  
モジュールごとに同じネットワーク上の一意の IP アドレスを指定します。
- [Network Mask] または [Prefix Length] に入力します。
- ネットワーク ゲートウェイ アドレスを入力します。

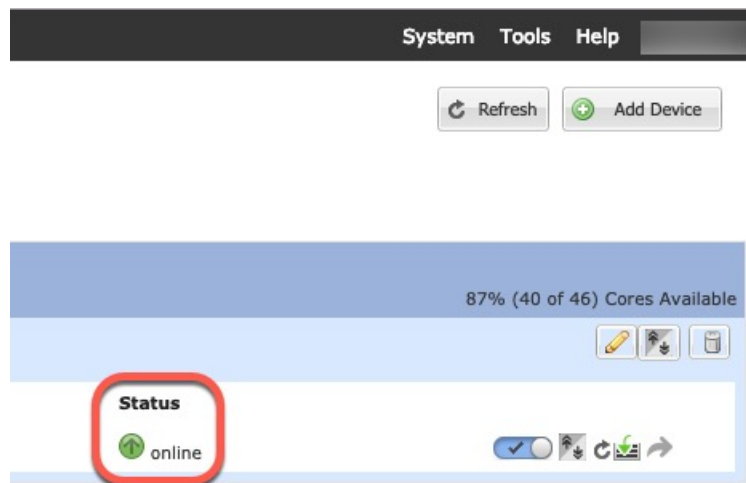
**ステップ 9** [利用規約 (Agreement)] タブで、エンドユーザライセンス (EULA) を読んで、同意します。

**ステップ 10** [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 11** [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 [ステータス (Status)] に [オンライン (Online)] と表示されている場合、残りのクラスタシャーシを追加するか、シャーシ内クラスタリングでアプリ

ケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



**ステップ 12** 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。

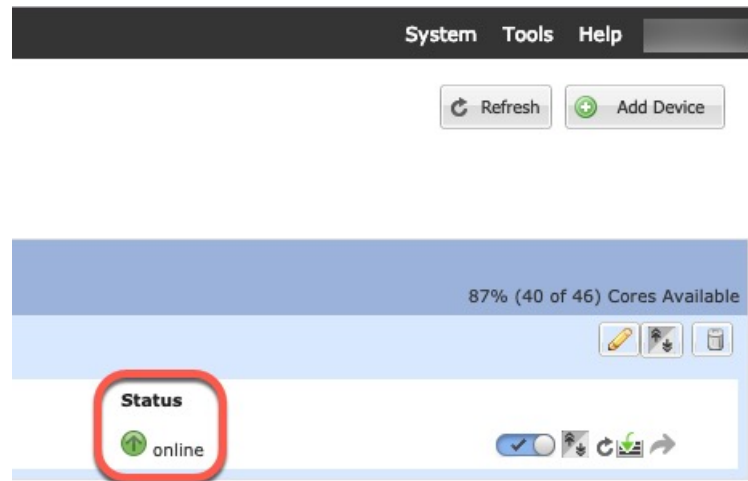
- a) 最初のシャーシの Firepower Chassis Manager で、右上にある [設定を表示 (Show Configuration)] アイコン (  ) をクリックして、表示されるクラスタの設定をコピーします。
- b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。
- c) [必要な操作 (I want to:)] > [既存のクラスタへの参加 (Join an Existing Cluster)] を選択します。
- d) [構成のコピー (Copy config)] チェックボックスをオンにし、[OK] 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。
- e) [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。
- f) 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。
  - [シャーシ ID (Chassis ID)] : 一意のシャーシ ID を入力します。
  - **Site ID** : サイト間クラスタリングの場合、このシャーシのサイト ID (1 ~ 8) を入力します。ディレクトアのローカリゼーション、サイトの冗長性、クラスタフローモビリティなどの冗長性と安定性を向上させるためのサイト間クラスタの追加カスタマイズは、Firepower Management Center flexconfig 機能を使用した場合にのみ設定できます。
  - [クラスタ キー (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。
  - [管理 IP (Management IP)] : 各モジュールの管理アドレスを、他のクラスタメンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。



[OK] をクリックします。

g) [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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status)] に [オンライン (Online)] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



- ステップ 13** 管理 IP アドレスを使用して、Firepower Management Center にマスターユニットを追加します。
- すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。
- Firepower Management Center がスレーブ ユニットの自動検出を行います。

## クラスタメンバーの追加

既存のクラスタ内の FTD クラスタメンバーを追加または置き換えます。FXOS に新しいクラスタメンバーを追加すると、Firepower Management Center によりメンバーが自動的に追加されます。




- (注) このプロシージャにおける FXOS の手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。

### 始める前に

- 置き換える場合は、Firepower Management Center から古いクラスタメンバーを削除する必要があります。新しいユニットに置き換えると、Firepower Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

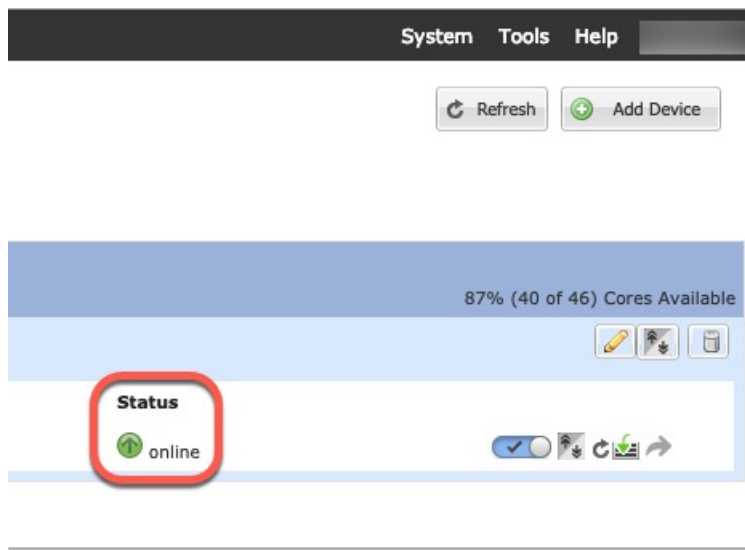
### 手順

- 
- ステップ 1** 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。
- ステップ 2** 右上の [設定を表示 (Show Configuration)] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
- ステップ 3** 新しいシャーシの Firepower Chassis Manager に接続して、[デバイスの追加 (Add Device)] をクリックします。
- ステップ 4** [デバイス名 (Device Name)] に論理デバイスの名前を入力します。
- ステップ 5** [テンプレート (Template)] には、[Cisco Firepower 脅威に対する防御 (Cisco Firepower Threat Defense)] を選択します。
- ステップ 6** [イメージバージョン (Image Version)] では、FTD ソフトウェアバージョンを選択します。
- ステップ 7** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 8** [既存のクラスタへの参加 (Join an Existing Cluster)] を選択します。
- ステップ 9** [構成のコピー (Copy config)] チェックボックスをオンにし、[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。
- ステップ 10** [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。
- ステップ 11** 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。
- [シャーシ ID (Chassis ID)] : 一意のシャーシ ID を入力します。
  - **Site ID** : サイト間クラスタリングの場合、このシャーシのサイト ID (1 ~ 8) を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
  - **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。
  - [管理 IP (Management IP)] : 各モジュールの管理アドレスを、他のクラスタメンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

**ステップ 12** [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。各クラスタメンバーの [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。各クラスタメンバーの論理デバイスの [ステータス (Status)] に [オンライン (Online)] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません (Security module not responding)] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



## Radware DefensePro の設定

Cisco Firepower 4100/9300 シャーシは、単一ブレードで複数のサービス（ファイアウォール、サードパーティの DDoS アプリケーションなど）をサポートできます。これらのアプリケーションとサービスは、リンクされて、サービス チェーンを形成します。

## Radware DefensePro について

現在サービスされているサービス チェーン コンフィギュレーションでは、サードパーティ製の Radware DefensePro 仮想プラットフォームを ASA ファイアウォールの手前、または Firepower Threat Defense の手前で実行するようにインストールできます。Radware DefensePro は、Firepower 4100/9300 シャーシに分散型サービス妨害 (DDoS) の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。Firepower 4100/9300 シャーシでサービス チェーンが有効になると、ネットワークからのトラフィックは主要な ASA または Firepower Threat Defense ファイアウォールに到達する前に DefensePro 仮想プラットフォームを通過する必要があります。



- (注)
- Radware DefensePro 仮想プラットフォームは、*Radware vDP* (仮想 DefensePro)、またはシンプルに *vDP* と呼ばれることがあります。
  - Radware DefensePro 仮想プラットフォームは、リンク デコレータと呼ばれることもあります。

## Radware DefensePro の前提条件

Radware DefensePro を Firepower 4100/9300 シャーシに導入する前に、**etc/UTC** タイムゾーンで NTP サーバを使用するように Firepower 4100/9300 シャーシを構成する必要があります。Firepower 4100/9300 シャーシの日付と時刻の設定の詳細については、[日時の設定](#)を参照してください。

## サービス チェーンのガイドライン

### モデル

- ASA : Radware DefensePro (vDP) プラットフォームは、次のモデルの ASA でサポートされています。
  - Firepower 9300
  - Firepower 4110
  - Firepower 4115
  - Firepower 4120
  - Firepower 4125
  - Firepower 4140
  - Firepower 4145
  - Firepower 4150
- Firepower Threat Defense : Radware DefensePro プラットフォームは、次のモデルの Firepower Threat Defense でサポートされています。
  - Firepower 9300
  - Firepower 4110 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。
  - Firepower 4115
  - Firepower 4120 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。

- Firepower 4125
- Firepower 4140
- Firepower 4145
- Firepower 4150

#### その他のガイドライン

- サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro (vDP) アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

## スタンドアロンの論理デバイスでの Radware DefensePro の設定

スタンドアロン ASA または Firepower Threat Defense 論理デバイスの前にある単一のサービス チェーンに Radware DefensePro をインストールするには、次の手順に従います。



- (注) Firepower 4120 または 4140 セキュリティ アプライアンス上で ASA の前に Radware vDP をインストールする場合、FXOS CLI を使用してデコレータを展開する必要があります。Radware DefensePro を、Firepower 4100 デバイス上で ASA の前にあるサービス チェーンにインストールして設定する方法の詳細な CLI 手順については、『FXOS CLI Configuration Guide』を参照してください。

#### 始める前に

- vDP イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロード](#)を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード](#)を参照)。
- Radware DefensePro アプリケーションは、シャーシ内クラスタのスタンドアロン構成で導入できます。シャーシ内クラスタリングについては、[シャーシ内クラスタの Radware DefensePro の設定 \(59 ページ\)](#) を参照してください。

#### 手順

- ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定](#)に従ってインターフェイスを有効にし、そのタイプを mgmt に設定してください。あるいは、アプリケーション管理インターフェイスを共有できます。
- ステップ 2** [Logical Devices] を選択して [Logical Devices] ページを開きます。

[論理デバイス (Logical Devices)] ページに、シャーンに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが表示されます。

- ステップ 3** スタンドアロン ASA または Firepower Threat Defense 論理デバイスを作成します ([スタンドアロン ASA の追加 \(22 ページ\)](#) または [スタンドアロン Firepower Threat Defense の追加 \(25 ページ\)](#) を参照)。
- ステップ 4** [Decorators] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - 設定 (Radware: Virtual DefensePro - Configuration)] ウィンドウが表示されます。[一般情報 (General Information)] タブで、次のフィールドを設定します。
- ステップ 5** Firepower 4100/9300 シャーンに複数の vDP バージョンをアップロードしている場合は、[バージョン (Version)] ドロップダウンから使用するバージョンを選択します。
- ステップ 6** リソース構成可能な Radware DefensePro アプリケーションがある場合は、[Resource Profile] ドロップダウンの下に、サポートされているリソースプロファイルのリストが表示されます。デバイスに割り当てるリソースプロファイルを選択してください。リソースプロファイルを選択しない場合、デフォルトの設定が使用されます。
- ステップ 7** [Management Interface] ドロップダウンで、この手順のステップ 1 で作成した管理インターフェイスを選択します。
- ステップ 8** デフォルトの [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)]) を選択します。
- ステップ 9** 前のステップで選択した [アドレス タイプ (Address Type)] に基づいて次のフィールドを設定します。
- a) [管理 IP (Management IP)] フィールドには、ローカル IP アドレスを設定します。
  - b) IPv4 のみ (IPv4 only) : [ネットワーク マスク (Network Mask)] を入力します。  
IPv6 のみ (IPv6 only) : [プレフィックス長 (Prefix Length)] を入力します。
  - c) 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 10** デバイスに割り当てる各データ ポートの横にあるチェックボックスをクリックします。
- ステップ 11** [OK] をクリックします。
- ステップ 12** [保存 (Save)] をクリックします。

Firepower eXtensible Operating System は、指定したソフトウェアバージョンをダウンロードし、指定したセキュリティモジュール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。

### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](#) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## シャーシ内クラスタの Radware DefensePro の設定

Radware DefensePro イメージをインストールして ASA または Firepower Threat Defense シャーシ内クラスタの前にサービス チェーンを設定するには、次の手順に従います。



- (注) サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

### 始める前に

- vDP イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロードを参照](#))、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロードを参照](#))。

### 手順

- ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定](#)に従ってインターフェイスを有効にし、そのタイプが mgmt になるように設定してください。そうしない場合、アプリケーション管理インターフェイスを共有できます。
- ステップ 2** ASA または Firepower Threat Defense シャーシ内クラスタを設定します ([ASA クラスタの作成 \(38 ページ\)](#) または [Firepower Threat Defense クラスタの作成 \(46 ページ\)](#) を参照)。
- シャーシ内クラスタを設定する手順の最後で [保存 (Save)] をクリックする前に、以下のステップに従ってクラスタに vDP デコレータを追加しておく必要があります。
- ステップ 3** [デコレータ (Decorators)] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - 設定 (Radware: Virtual DefensePro - Configuration)] ダイアログボックスが表示されます。[一般情報 (General Information)] タブで、次のフィールドを設定します。
- ステップ 4** Firepower 4100/9300 シャーシに複数の vDP バージョンをアップロードした場合は、使用する vDP バージョンを [バージョン (Version)] ドロップダウンで選択します。
- ステップ 5** リソース構成 Radware DefensePro アプリケーションがある場合は、[リソース プロファイル (Resource Profile)] ドロップダウンの下に、サポートされているリソース プロファイルのリストが表示されます。デバイスに割り当てるリソース プロファイルを選択してください。リソース プロファイルを選択しない場合、デフォルトの設定が使用されます。
- ステップ 6** [管理インターフェイス (Management Interface)] ドロップダウンで管理インターフェイスを選択します。
- ステップ 7** vDP デコレータに割り当てる各データ ポートの横にあるチェックボックスをクリックします。
- ステップ 8** [インターフェイス情報 (Interface Information)] タブをクリックします。
- ステップ 9** 使用する [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)] ) を選択します。

**ステップ 10** 各セキュリティモジュールで、次のフィールドを設定します。表示されるフィールドは、前のステップで選択した [アドレス タイプ (Address Type)] により異なります。

- a) [管理 IP (Management IP)] フィールドには、ローカル IP アドレスを設定します。
- b) IPv4 のみ (IPv4 only) : [ネットワーク マスク (Network Mask)] を入力します。  
IPv6 のみ (IPv6 only) : [プレフィックス長 (Prefix Length)] を入力します。
- c) 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 11** [OK] をクリックします。

**ステップ 12** [保存 (Save)] をクリックします。

Firepower eXtensible Operating System は、指定したソフトウェアバージョンをダウンロードし、指定したセキュリティモジュール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。

**ステップ 13** [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。

**ステップ 14** 設定された論理デバイスのリストをスクロールして vDP のエントリを表示します。[Management IP] 列に示されている属性を確認します。

- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*unknown*」と表示される場合は、vDP クラスタの作成を完了するために、DefensePro アプリケーションを入力してマスター IP アドレスを設定する必要があります。
- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*primary*」または「*secondary*」と表示される場合は、アプリケーションはオンラインで、クラスタ化されています。

#### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](http://cisco.com) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## UDP/TCP ポートのオープンと vDP Web サービスの有効化

Radware APSolute Vision Manager インターフェイスは、さまざまな UDP/TCP ポートを使用して Radware vDP のアプリケーションと通信します。vDP のアプリケーションが APSolute Vision Manager と通信するために、これらのポートがアクセス可能でありファイアウォールによってブロックされないことを確認します。オープンする特定のポートの詳細については、APSolute Vision ユーザ ガイドの次の表を参照してください。

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

Radware APSolute Vision で FXOS シャーシ内に配置される Virtual DefensePro アプリケーションを管理するために、FXOS CLI を使用して vDP Web サービスを有効にする必要があります。



## 手順

ステップ 1 FXOS CLI から、vDP のアプリケーション インスタンスに接続します。

```
connect module slot console
```

```
connect vdp
```

ステップ 2 vDP Web サービスを有効化します。

```
manage secure-web status set enable
```

ステップ 3 vDP アプリケーションのコンソールを終了して FXOS モジュール CLI に戻ります。

```
Ctrl ]
```

# TLS 暗号化アクセラレーションの設定

次のトピックでは TLS 暗号化アクセラレーションを紹介します。また、Firepower Management Center を使用して、この機能を有効にする方法やステータスを表示する方法について説明します。

## About TLS 暗号化アクセラレーション

Firepower 4100/9300 は Transport Layer Security 暗号化アクセラレーションをサポートしています。これは、Transport Layer Security/Secure Sockets Layer (TLS/SSL) の暗号化と復号化をハードウェアで実行するもので、これにより次の高速化を実現します。

- TLS/SSL 暗号化および復号化
- VPN (TLS/SSL および IPsec を含む)

TLS 暗号化アクセラレーションはネイティブインスタンスで自動的に有効になり、無効にすることはできません。TLS 暗号化アクセラレーションはセキュリティエンジン/モジュールごとに 1 FTD コンテナインスタンスで有効にすることもできます。

## TLS 暗号化アクセラレーションに関するガイドラインと制限事項

FTD で TLS 暗号化アクセラレーションが有効になっている場合は、次の点に留意してください。

### エンジン障害インスペクション

インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまで TLS/SSL トラフィックはドロップされます。

この動作は FTD `configure snort preserve-connection {enable | disable}` コマンドによって制御されます。

### HTTP のみのパフォーマンス

トラフィックを復号しない FTD コンテナインスタンスで TLS 暗号化アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。TLS/SSL トラフィックを復号する FTD コンテナインスタンスで TLS 暗号化アクセラレーションのみ有効にすることをお勧めします。

### Federal Information Processing Standards (FIPS)

TLS 暗号化アクセラレーションと連邦情報処理標準 (FIPS) が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4 (RC4)
- 単一データ暗号化標準規格 (単一 DES)
- Merkle–Damgard 5 (MD5)
- SSL v3

セキュリティ認定準拠モードで動作するように Firepower Management Center と FTD を設定すると、FIPS が有効になります。このモードで動作しているときに接続を許可するには、FTD コンテナインスタンスで TLS 暗号化アクセラレーションを無効にするか、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- [コモンクライテリア](#)。

### 高可用性 (HA) とクラスタリング

高可用性 (HA) またはクラスタ化された FTD がある場合は、FTD ごとに TLS 暗号化アクセラレーションを有効にする必要があります。1 つのデバイスの TLS 暗号化アクセラレーション構成は、HA ペアまたはクラスタの他のデバイスとは共有されません。

### TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security (TLS) および Datagram Transport Layer Security (DTLS) プロトコルに対して、TLS ハートビートエクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている FMC によって管理されている FTD が、TLS ハートビートエクステンションを使用するパケットを検出した場合、SSL ポリシーの

[Undecryptable Actions] で [Decryption Errors] の FMC 設定で指定されたアクションを実行します。

- ブロック (Block)
- リセットしてブロック (Block with reset)

アプリケーションが TLS ハートビートを使用しているかどうかを確認するには、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。

TLS 暗号化アクセラレーションが FTD コンテナインスタンス で無効になっている場合は、FMC のネットワーク分析ポリシー (NAP) の [Max Heartbeat Length] を設定すると、TLS ハートビートの処理方法を決定できます。

TLS ハートビートの詳細については、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。

### TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、FTD が TLS/SSL トラフィックにより過負荷になっている状態です。FTD で TLS/SSL オーバーサブスクリプションが発生する可能性があります。TLS 暗号化アクセラレーションをサポートする FTD でのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている FMC によって管理される FTD がオーバーサブスクライブされた場合、FTD によって受信されるパケットの扱いは、SSL ポリシーの [Undecryptable Actions] にある [Handshake Errors] の設定に従います。

- デフォルトアクションを継承する (Inherit default action)
- 復号しない (Do not decrypt)
- ブロック (Block)
- リセットしてブロック (Block with reset)

SSL ポリシーの [復号化不可のアクション (Undecryptable Actions)] の [ハンドシェイクエラー (Handshake Errors)] の設定が [復号しない (Do Not decrypt)] で、関連付けられたアクセスコントロールポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われません。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- TLS/SSL の処理能力が高い FTD にアップグレードします。
- SSL ポリシーを変更して、復号の優先順位が高くないトラフィック用に [Do Not Decrypt] ルールを追加します。

TLS オーバーサブスクリプションの詳細については、『*Firepower Management Center 構成ガイド*』の TLS/SSL トラブルシューティングルールの章を参照してください。

パッシブおよびインラインタップの設定はサポートされていません。

TLS 暗号化アクセラレーションが有効になっている場合、TLS/SSL トラフィックはパッシブまたはインラインタップ設定のインターフェイスでは復号できません。

## 1つのコンテナインスタンスの TLS 暗号化アクセラレーションの有効化

ここで説明されているコマンドを使用すると、1つの FTD コンテナインスタンスで TLS 暗号化アクセラレーションを有効化および無効化することができます。

### 手順

**ステップ 1** 設定されているアプリケーションインスタンスを表示します。

**scope ssa**

**show app-instance**

**exit**

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot	ID	Admin State	Oper State	Running Version	Startup Version	Cluster Role
ftd	container1	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD2	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD3	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD4	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				

```
Firepower /ssa # exit
```

**ステップ 2** 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-9300# 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3 コンテナインスタンスでTLS暗号化アクセラレーションを有効化

**config hwCrypto enable instance**

無効にするには、**config hwCrypto disable** コマンドを使用します。

例：

```
config hwCrypto enable container1

WARNING!!!: This command will restart the container instance. Are you sure ? [yes/NO] yes
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108
to enable hardware crypto .... it will take some time.
```

例

次に、モジュール1の **container1** という名前のFTDコンテナインスタンスのTLS暗号化アクセラレーションを有効にして、インスタンスの再起動を求めるプロンプトが表示される例を示します。

```
Firepower-module1>scope ssa
/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
-----
ftd           container1 1           Enabled   Online           6.4.0      6.4.0      Container
Default-Small Not Applicable None
ftd           LD2        1           Enabled   Online           6.4.0      6.4.0      Container
Default-Small Not Applicable None
ftd           LD3        1           Enabled   Online           6.4.0      6.4.0      Container
Default-Small Not Applicable None
ftd           LD4        1           Enabled   Online           6.4.0      6.4.0      Container
Default-Small Not Applicable None

/ssa # exit

Firepower-module1>connect module 1 console
Firepower-module1>config hwCrypto enable container1

WARNING!!!: This command will restart the container instance. Are you sure ? [yes/NO] yes
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108
to enable hardware crypto .... it will take some time.
```

次に、TLS暗号化アクセラレーションを無効にして、プロンプトの再起動を求めるプロンプトが表示される例を示します。

```

Firepower-module1>scope ssa
/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
-----
ftd           container1 1      Enabled      Online          6.4.0      6.4.0      Container
  Default-Small Not Applicable None
ftd           LD2        1      Enabled      Online          6.4.0      6.4.0      Container
  Default-Small Not Applicable None
ftd           LD3        1      Enabled      Online          6.4.0      6.4.0      Container
  Default-Small Not Applicable None
ftd           LD4        1      Enabled      Online          6.4.0      6.4.0      Container
  Default-Small Not Applicable None

/ssa # exit

Firepower-module1>connect module 1 console
Firepower-module1>config hwCrypto disable

WARNING!!: Hardware crypto will be disabled from container identifier container1.
WARNING!!: Container instance container1 will be restarted. Are you sure ? [yes/NO] yes
Removing Hardware Crypto from Container identifier container1..
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108 to disable
hardware crypto for identifier container1 ..... it will take some time.


```

## TLS 暗号アクセラレーションのステータスの表示

このトピックでは、TLS 暗号化アクセラレーションが有効になっているかどうかを確認する方法について説明します。

Firepower Management Center で次のタスクを実行します。

### 手順

- 
- ステップ 1 Firepower Management Center にログインします。
  - ステップ 2 [デバイス (Devices)] > [デバイス管理 (Device Management)] をクリックします。
  - ステップ 3  (編集) をクリックして、管理対象デバイスを編集します。
  - ステップ 4 [デバイス (Device)] ページをクリックします。TLS 暗号化アクセラレーションステータスが [全般 (General)] セクションに表示されます。
- 

## 論理デバイスの管理

論理デバイスを削除したり、ASA をトランスペアレントモードに変換したり、インターフェイスコンフィギュレーションを変更したり、その他のタスクを既存の論理デバイスで実行することができます。

## 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。デバイスの適切なコマンドを入力します。

```
connect asa name
```

```
connect ftd name
```

```
connect vdp 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 asal
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

**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。
- FTD : 「**exit**」 と入力します。
- 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。

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 のスーパーバイザ 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#
```

## 論理デバイスの削除

### 手順

---

**ステップ 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。



[論理デバイス (Logical Devices)] ページに、シャーンに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。

**ステップ 2** 削除する論理デバイスの [削除 (Delete)] をクリックします。

**ステップ 3** [はい (Yes)] をクリックして、この論理デバイスを削除することを確認します。

**ステップ 4** [はい (Yes)] をクリックして、このアプリケーション設定を削除することを確認します。

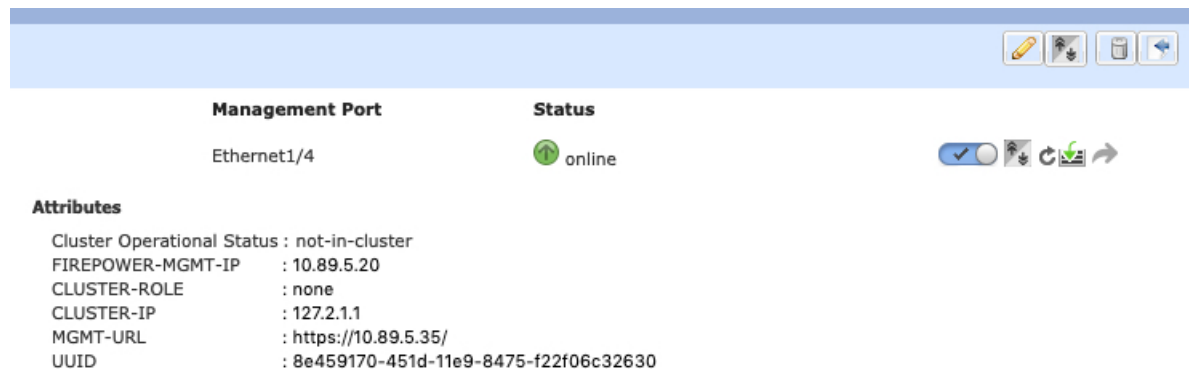
## クラスタメンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

### 一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタメンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページで、のクラスタ ステータスを確認します。



The screenshot shows a table with two columns: Management Port and Status. The Management Port is Ethernet1/4 and the Status is online. Below the table, there are several icons for actions like edit, delete, and refresh. Underneath, there is an 'Attributes' section listing various system parameters.

Management Port	Status
Ethernet1/4	online

**Attributes**

- Cluster Operational Status : not-in-cluster
- FIREPOWER-MGMT-IP : 10.89.5.20
- CLUSTER-ROLE : none
- CLUSTER-IP : 127.2.1.1
- MGMT-URL : https://10.89.5.35/
- UUID : 8e459170-451d-11e9-8475-f22f06c32630


FMC を使用した FTD では、FMC デバイス リストにデバイスを残し、クラスタリングを再度有効にした後にすべての機能を再開できるようにする必要があります。

- アプリケーションでのクラスタリングの無効化 : アプリケーション CLI を使用してクラスタリングを無効にすることができます。 `cluster remove unit name` コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブユニットでこのコマンドを入力した場合は、新しいマスターユニットが選定されます。

デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック

フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合、管理インターフェイスは無効になります。


クラスタリングを再度有効にするには、ASA で **cluster group name** を入力してから **enable** を入力します。クラスタリングを再度有効にするには、FTD で **cluster enable** を入力します。

- アプリケーションインスタンスの無効化：Firepower Chassis Manager の [Logical Devices] ページで [無効 (Disable)] スライダ (  ) をクリックします。[Enable] スライダ (  ) を使用して後で再度有効にすることができます。
- セキュリティモジュール/エンジンのシャットダウン：Firepower Chassis Manager の [Module/Engine] ページで、[Power Off] アイコン (  ) をクリックします。
- シャーシのシャットダウン：Firepower Chassis Manager の [Overview] ページで、[Shut Down] アイコン (  ) をクリックします。

### 完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

FMC を使用した FTD の場合、シャーシでクラスタリングを無効にした後でユニットを FMC デバイス リストから削除してください。

- 論理デバイスの削除：Firepower Chassis Manager の [Logical Devices] ページで、削除アイコン (  ) をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティモジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

## 論理デバイスに関連付けられていないアプリケーションインスタンスの削除

論理デバイスを削除すると、その論理デバイスのアプリケーション設定も削除するかどうか尋ねられます。アプリケーション設定を削除しない場合、そのアプリケーションインスタンスが削除されるまで、別のアプリケーションを使用して論理デバイスを作成することはできません。セキュリティモジュール/エンジンが論理デバイスとすでに関連付けられていない場合は、アプリケーションインスタンスを削除するために以下の手順を使用できます。

### 手順

- 
- ステップ 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。

[論理デバイス (Logical Devices)] ページに、シャーンに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。論理デバイスのリストの下に、論理デバイスに関連付けられていないアプリケーション インスタンスのリストが表示されます。

**ステップ 2** 削除するアプリケーション インスタンスの [削除 (Delete)] をクリックします。

**ステップ 3** [はい (Yes)] をクリックして、このアプリケーション インスタンスを削除することを確認します。

## Firepower Threat Defense 論理デバイスのインターフェイスの変更

FTD 論理デバイスでは、インターフェイスの割り当てや割り当て解除、または管理インターフェイスの置き換えを行うことができます。その後、FMC でインターフェイス設定を同期できます。

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、FTD の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバなど、FTD の設定における多くの場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ FMC での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。

### 始める前に

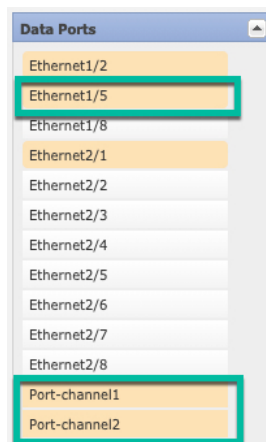
- **物理インターフェイスの設定**および**EtherChannel (ポート チャネル) の追加**に従ってインターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには (たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます)、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスまたは Firepower イベント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。FTD がリポートし (管理インターフェイスを変更するとリポートします)、FMC で設定を同期すると、(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。
- クラスタリングやハイアベイラビリティのため、FMC で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。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さないことに注意してください。

## 手順

- ステップ 1** Firepower Chassis Manager で、[論理デバイス (Logical Devices)] 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。

まだインターフェイスを削除しないでください。



- ステップ 4** 次のように、管理またはイベントインターフェイスを置き換えます：

これら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ブートします。

- ページ中央のデバイス アイコンをクリックします。
- [一般 (General)] または [クラスタ情報 (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。
- [設定 (Settings)] タブで、ドロップダウンリストから新しい [イベントインターフェイス (Eventing Interface)] を選択します。
- [OK] をクリックします。

管理インターフェイスの IP アドレスを変更した場合は、Firepower Management Center でデバイスの IP アドレスを変更する必要があります。[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス/クラスタ (Device/Cluster)] と移動します。[Management] 領域で、ブートストラップ設定アドレスと一致するように IP アドレスを設定します。

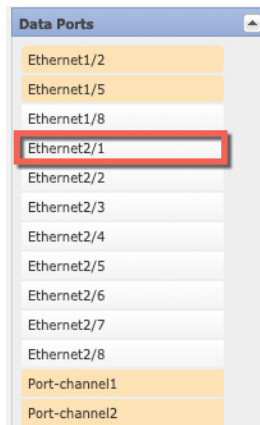
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** FMC でインターフェイスを同期します。
- FMC にログインします。

- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、FTD デバイスの編集アイコン (✎) をクリックします。[インターフェイス (Interfaces)] タブがデフォルトで選択されます。
- c) [インターフェイス (Interfaces)] タブの左上にある [デバイスの同期 (Sync Device)] ボタンをクリックします。
- d) 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス (Interfaces)] ページに表示されます。[クリックして詳細を表示 (Click to know more)] リンクをクリックしてインターフェイスの変更内容を表示します。
- e) インターフェイスを削除する予定の場合は、古いインターフェイスから新しいインターフェイスに任意のインターフェイス設定を手動で転送します。

まだインターフェイスを削除していないので、既存の設定を参照できます。古いインターフェイスを削除して検証を再実行した後も、さらに設定を修正する機会があります。検証では、古いインターフェイスでまだ使用されているすべての場所が表示されます。

- f) [変更の検証 (Validate Changes)] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。  
エラーがある場合は、ポリシーを変更して検証に戻る必要があります。
- g) [Save] をクリックします。
- h) デバイスを選択して [展開 (Deploy)] をクリックし、割り当てられたデバイスにポリシーを展開します。変更はポリシーを導入するまで有効になりません。

**ステップ 7** Firepower Chassis Manager で、[データポート (Data Ports)] 領域でデータ インターフェイスの選択を解除し、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 8** [Save] をクリックします。

**ステップ 9** FMC でインターフェイスを再度同期します。

## 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**および**EtherChannel（ポート チャネル）の追加**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、その後でデバイスに 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、[論理デバイス（Logical Devices）] 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て、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。
- ページ中央のデバイス アイコンをクリックします。
  - [一般/クラスター情報 (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。
  - [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。

---

## 論理デバイスのブートストラップ設定の変更または回復

論理デバイスのブートストラップ設定は、変更することができます。変更した後、直ちに新しい設定を使用してアプリケーションを再起動することも、変更を保存しておいて後で新しい設定を使用してアプリケーション インスタンスを再起動することもできます。

### 手順

- 
- ステップ1** Firepower Chassis Manager で、[論理デバイス (Logical Devices)] 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て、その論理デバイスを編集します。
- ステップ3** ページ中央のデバイス アイコンをクリックします。
- ステップ4** 必要に応じて論理デバイスの設定を変更します。
- ステップ5** [OK] をクリックします。
- ステップ6** [Restart Now] をクリックすると、変更を保存してアプリケーション インスタンスを再起動できるようになります。アプリケーション インスタンスを再起動せずに変更を保存するには、[Restart Later] をクリックします。
- (注) [Restart Later] を選択した場合、アプリケーション インスタンスを再起動する準備が整ってから、[Logical Devices] ページで [Restart Instance] をクリックしてアプリケーション インスタンスを再起動できます。
-

## [論理デバイス (Logical Devices) ] ページ

Firepower Chassis Manager の [Logical Devices] ページを使用して、論理デバイスを作成、編集、削除します。[Logical Devices] ページには、各 Firepower 4100/9300 シャーシセキュリティモジュール/エンジンにインストールされている論理デバイスの情報エリアが含まれています。

各論理デバイス エリアのヘッダーには次の情報が含まれています。

- 論理デバイスの一意の名前。
- 論理デバイスのモード（スタンドアロンまたはクラスタ）。
- [Status] : 論理デバイスの状態を示します。
  - [ok] : 論理デバイスの設定は完了しています。
  - [設定未完了 (incomplete-configuration) ] : 論理デバイス設定は未完了です。

各論理デバイス エリアには次の情報が含まれます。

- [Application] : セキュリティ モジュールで実行しているアプリケーションを示します。
- [Version] : セキュリティ モジュールで実行しているアプリケーションのソフトウェアバージョン番号を示します。



(注) FTD の論理デバイスへの更新は Firepower Management Center を使用して行います。Firepower Chassis Manager の [論理デバイス (Logical Devices) ] > [編集 (Edit) ] および [システム (System) ] > [更新 (Updates) ] ページには反映されません。これらのページで、表示されるバージョンは、FTD 論理デバイスを作成するために使用されたソフトウェアバージョン (CSP イメージ) を示します。

- [Resource profile] : 論理デバイス/アプリケーション インスタンスに割り当てられたリソース プロファイルを表示します。
- [Management IP] : 論理デバイス管理 IP として割り当てられているローカル IP アドレスを示します。
- [Gateway] : アプリケーション インスタンスに割り当てられているネットワーク ゲートウェイ アドレスを示します。
- [Management Port] : アプリケーション インスタンスに割り当てられている管理ポートを示します。
- [Status] : アプリケーション インスタンスの状態を示します。
  - [オンライン (Online) ] : アプリケーションは実行中であり、動作しています。



- [オフライン (Offline) ] : アプリケーションは停止され、使用できません。
- [インストール (Installing) ] : アプリケーションのインストールを実行しています。
- [未インストール (Not Installed) ] : アプリケーションがインストールされていません。
- [インストール失敗 (Install Failed) ] : アプリケーションのインストールに失敗しました。
- [起動中 (Starting) ] : アプリケーションを起動しています。
- [起動失敗 (Start Failed) ] : アプリケーションの起動に失敗しました。
- [開始 (Started) ] : アプリケーションは正常に開始し、アプリケーション エージェントのハートビートを待機しています。
- [停止中 (Stopping) ] : アプリケーションは停止処理中です。
- [停止失敗 (Stop Failed) ] : アプリケーションをオフラインにできませんでした。
- [Not Responding] : アプリケーションは応答不能です。
- [Updating] : アプリケーション ソフトウェアの更新が進行中です。
- [Update Failed] : アプリケーション ソフトウェアの更新に失敗しました。
- [Update Succeeded] : アプリケーション ソフトウェアの更新に成功しました。
- [Unsupported] : このインストール済みアプリケーションはサポートされていません。

セキュリティモジュールが存在しないか障害状態の場合は、その情報がステータスフィールドに表示されます。情報アイコンにカーソルを合わせると、障害に関する詳細情報が表示されます。セキュリティモジュールの障害について詳しくは、[FXOS セキュリティモジュール/セキュリティエンジンについて](#)を参照してください。

- **[Expanded Information]** 領域 : 現在実行中のアプリケーションインスタンスの追加属性を示します。



---

(注) アプリケーションのブートストラップ設定を変更した後、直ちにアプリケーションインスタンスを起動しなければ、**[Attributes]** フィールドには現在実行中のアプリケーションに関する情報が表示され、アプリケーションを再起動するまで変更は反映されません。

---

- **[Ports]** : アプリケーションインスタンスに割り当てられたインターフェイスの名前とタイプを示します。
- **[Cluster Operation Status]** : アプリケーションインスタンスに割り当てられている管理 URL を示します。

- [Management IP/Firepower Management IP] : アプリケーションインスタンスに割り当てられている管理 IP アドレスを示します。
- [Cluster Role] : アプリケーションインスタンス、マスターまたはスレーブのクラスタロールを示します。
- [Cluster IP] : アプリケーションインスタンスに割り当てられている IP アドレスを示します。
- [HA Role] : アプリケーションインスタンス、アクティブまたはスタンバイのハイアベイラビリティ ロールを示します。
- [Management URL] : アプリケーションインスタンスに割り当てられている管理アプリケーションの URL を示します。
- [UUID] : アプリケーションインスタンスの汎用一意識別子を示します。

Firepower Chassis Manager の [Logical Devices] ページから、論理デバイスに対して次の機能を実行できます。

- [Refresh] : [Logical Devices] ページに表示されている情報が更新されます。
- [Add Device] : 論理デバイスを作成できます。
- [Edit] : 既存の論理デバイスを編集できます。
- [Set Version] : 論理デバイス上のソフトウェアをアップグレードまたはダウングレードできます。
- [Delete] : 論理デバイスが削除されます。
- [Show Configuration] : ダイアログボックスが開き、論理デバイスまたはクラスタの構成情報が JSON 形式で表示されます。クラスタに含める追加デバイスを作成する際は、この構成情報をコピーして使用できます。
- [Enable/Disable] : アプリケーションインスタンスが有効化/無効化されます。
- [Upgrade/Downgrade] : アプリケーションインスタンスをアップグレード/ダウングレードできます。
- [Restart Instance] : アプリケーションインスタンスを再起動できます。デバイスのブートストラップ情報を変更した後、アプリケーションインスタンスをまだ再起動していない場合、[Restart Instance] をクリックすることで、既存の管理ブートストラップ情報をクリアし、新しいブートストラップ情報を使用してアプリケーションインスタンスを再起動できます。
- [Reinstall instance] : アプリケーションインスタンスを再インストールできます。
- [Go To Device Manager] : アプリケーションインスタンスに定義されている Firepower Management Center または ASDM へのリンクを提示します。

## サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

### サイト固有のMACアドレスを使用したスバンドEtherChannelルーテッドモードの例

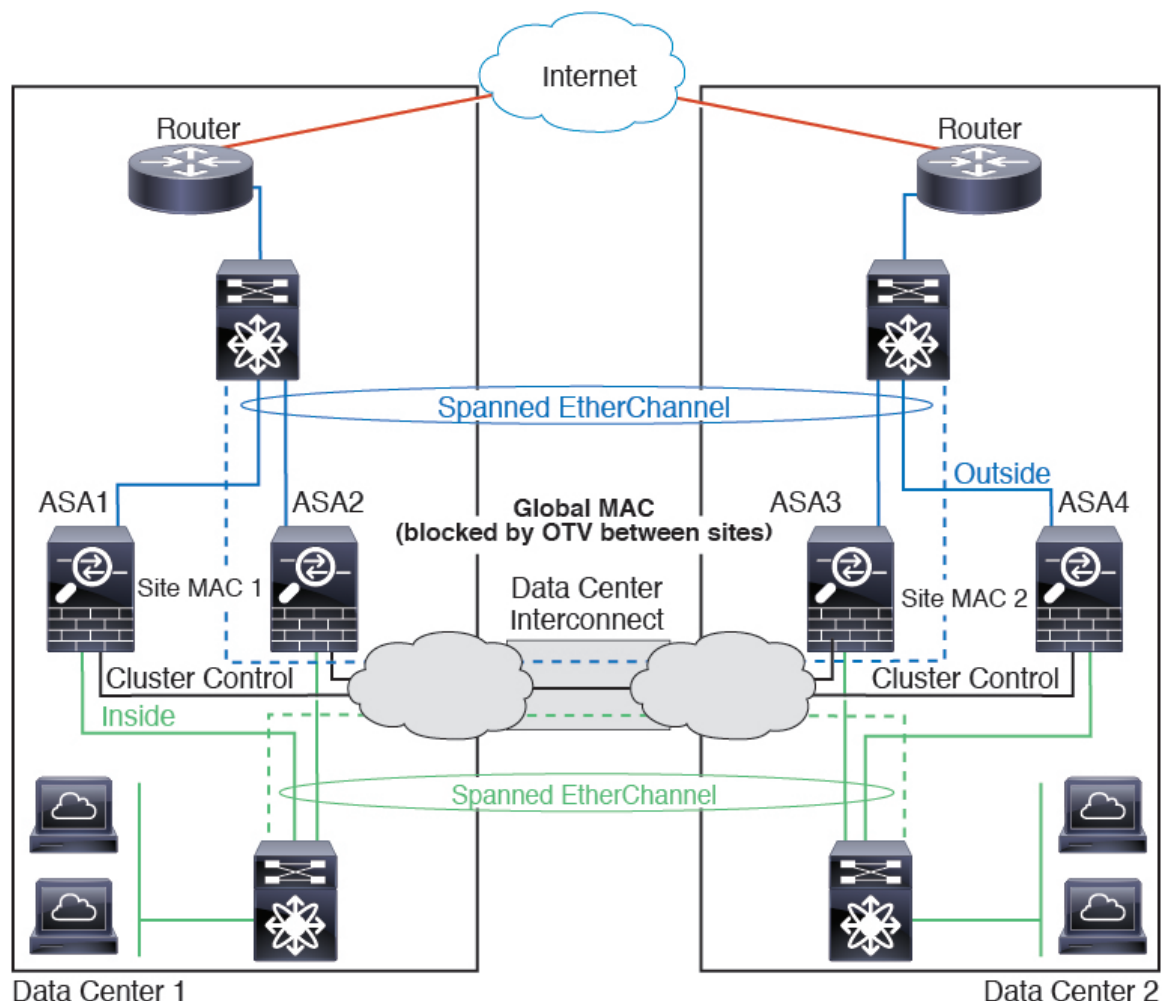
次の例では、各サイトのゲートウェイルータと内部ネットワーク間に配置された（イーストウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタメンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部両方のネットワークに対しスバンドEtherChannelを使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャーシにスパンされます。

データ VLAN は、オーバーレイ トランスポート 仮想化 (OTV)（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックがDCIを通過して他のサイトに送信されないようにするには、グローバルMACアドレスをブロックするフィルタを追加する必要があります。1つのサイトのクラスタユニットが到達不能になった場合、トラフィックが他のサイトのクラスタユニットに送信されるようにフィルタを削除する必要があります。Vaclを使用して、グローバルのMACアドレスのフィルタリングする必要があります。必ずARPインスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタユニット間で共有されるグローバルな仮想MACは、パケットを受信するためだけに使用されます。発信パケットは、各DCクラスタからのサイト固有のMACアドレスを使用します。この機能により、スイッチが2つの異なるポートで両方のサイトから同じグローバルMACアドレスを学習してしまうのを防いでいます。MACフラッピングが発生しないよう、サイトMACアドレスのみを学習します。

この場合のシナリオは次のとおりです。

- クラスタから送信されるすべての出力パケットは、サイトのMACアドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバルMACアドレスを使用して送信されるため、両方のサイトでいずれかのユニットで受信できます。OTVでのフィルタによって、データセンター内のトラフィックがローカライズされます。



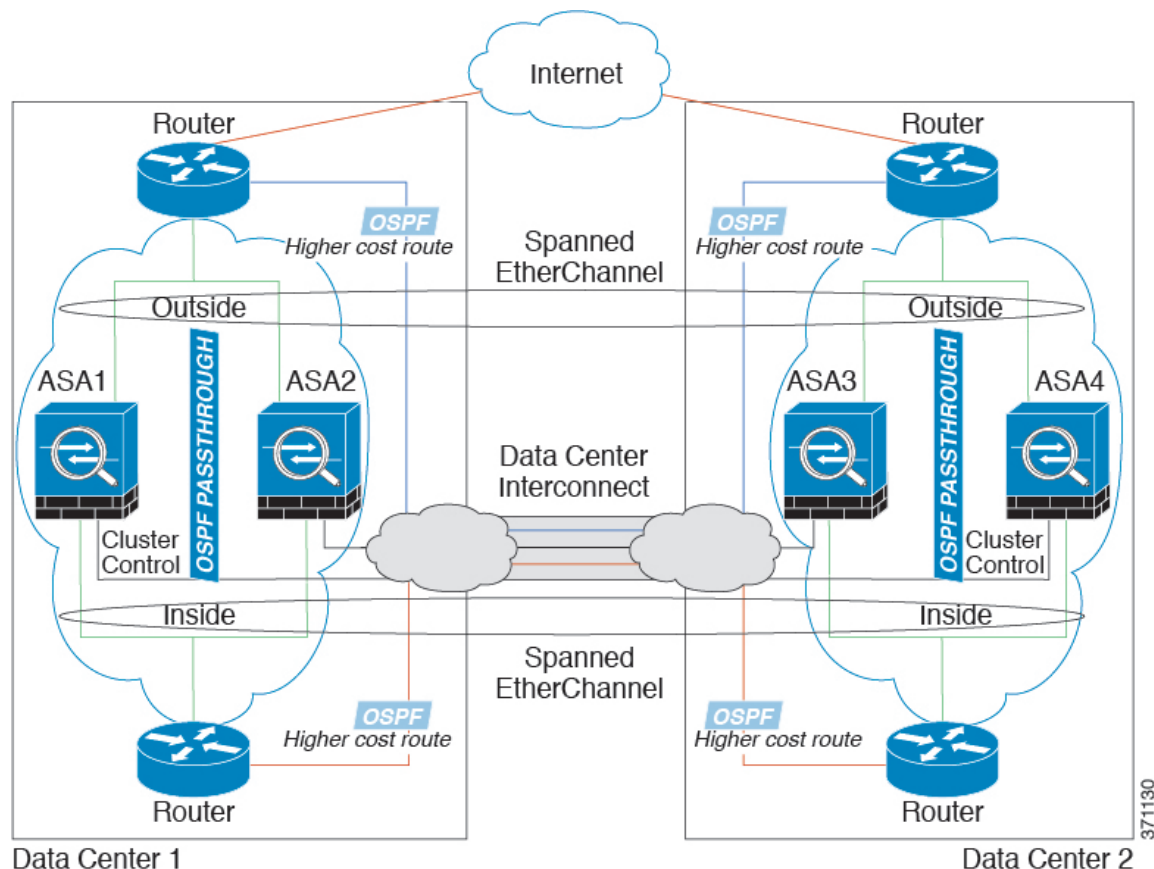
## スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2つのデータセンターのそれぞれに2つのクラスタメンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部のスパンド EtherChannels を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルート割り当てることにより、特定のサイトですべてのクラスタメンバーがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジグループを横断する必要があります。1つのサイトのすべてのクラスタメンバーに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタメンバーに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC : このシナリオでは、データセンター1に1台のスイッチをインストールし、データセンター2に別のスイッチをインストールします。1つのオプションとして、各データセンターのクラスタユニットはローカルスイッチだけに接続し、VSS/vPC トラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCIが余分なトラフィック量を処理できる場合、各ユニットをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC : スwitchの冗長性を高めるには、各サイトに2つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタユニットは、両方のローカルスイッチだけに接続されたデータセンター1のシャーシおよびこれらのローカルスイッチに接続されたデータセンター2のシャーシとはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

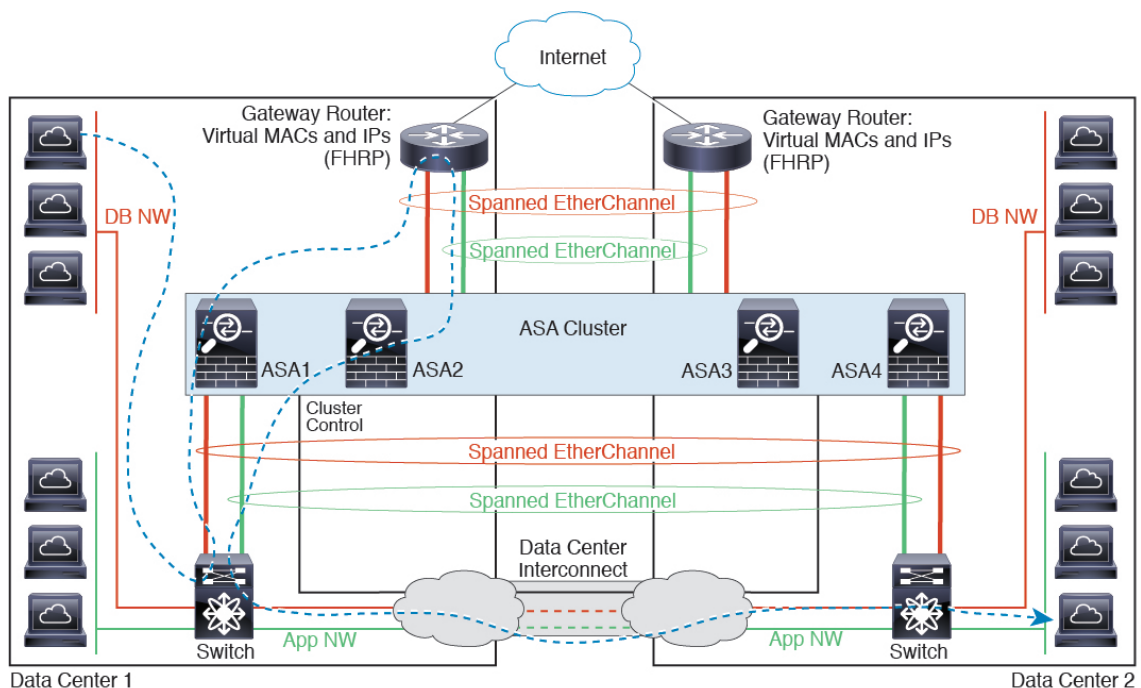


371130

## スパンド EtherChannel トランスペアレントモード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイルータと2つの内部ネットワーク（アプリケーションネットワークとDBネットワーク）間に配置された（イーストウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタメンバーがある場合を示します。クラスタメンバーは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバーは、内部および外部のアプリケーションネットワークとDBネットワークの両方にスパンド EtherChannels を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャージにスパンされます。

各サイトのゲートウェイルータは、HSRPなどのFHRPを使用して、各サイトで同じ宛先の仮想MACアドレスとIPアドレスを提供します。MACアドレスの予期せぬフラッピングを避けるため、ゲートウェイルータの実際のMACアドレスをASA MACアドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト1のゲートウェイがサイト2のゲートウェイと通信する場合に、そのトラフィックがASAを通過して、内部インターフェイスからサイト2に到達しようとして、問題が発生する可能性があります。データVLANは、オーバーレイトランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイルータ宛てである場合にトラフィックがDCIを通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1つのサイトのゲートウェイルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



vPC/VSS オプションについては、[スパンド EtherChannel トランスペアレントモード ノースサウス サイト間の例 \(80 ページ\)](#) を参照してください。

## 論理デバイスの履歴

機能名	プラットフォームリリース	機能情報
Firepower 4115、4125、および 4145	2.6.1	<p>Firepower 4115、4125、および 4145 が導入されました。</p> <p>(注) ASA 9.12(1) が必要です。Firepower 6.4.0 には FXOS 2.6.1.157 が必要です。</p> <p>変更された画面はありません。</p>
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	2.6.1	<p>3 つのセキュリティ モジュール、SM-40、SM-48、および SM-56 が導入されました。</p> <p>(注) SM-40 および SM-48 には ASA 9.12(1) が必要です。SM-56 には、ASA 9.12(2) および FXOS 2.6.1.157 が必要です。</p> <p>すべてのモジュールには、FTD 6.4 および FXOS 2.6.1.157 が必要です。</p> <p>変更された画面はありません。</p>
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	2.6.1	<p>ASA および FTD 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。</p> <p>(注) ASA 9.12(1) が必要です。Firepower 6.4.0 には FXOS 2.6.1.157 が必要です。</p> <p>変更された画面はありません。</p>
FTD ブートストラップ設定については、Firepower Chassis Manager で FMC の NAT ID を設定できるようになりました。	2.6.1	<p>Firepower Chassis Manager で FMC NAT ID を設定できるようになりました。以前は、FXOS CLI または FTD CLI 内でのみ NAT ID を設定できました。通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。FMC がデバイスの IP アドレスを指定し、デバイスが FMC の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要があります。FMC およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。</p> <p>新しい変更された画面：</p> <p><b>[Logical Devices] &gt; [Add Device] &gt; [Settings] &gt; [Firepower Management Center NAT ID] フィールド</b></p>

機能名	プラットフォームリリース	機能情報
モジュール/セキュリティエンジンのいずれかのFTDコンテナインスタンスでのSSLハードウェアアクセラレーションのサポート	2.6.1	<p>これで、モジュール/セキュリティエンジンのいずれかのコンテナインスタンスに対してSSLハードウェアアクセラレーションを有効にすることができるようになりました。他のコンテナインスタンスに対してSSLハードウェアアクセラレーションは無効になっていますが、ネイティブインスタンスには有効になっています。詳細については、『Firepower Management Center Configuration Guide』を参照してください。</p> <p>新規/変更されたコマンド：<b>config hwCrypto enable</b>、<b>show hwCrypto</b></p> <p>変更された画面はありません。</p>



機能名	プラットフォームリリース	機能情報
Firepower Threat Defense のマルチインスタンス 機能	2.4.1	

機能名	プラットフォームリリース	機能情報
		<p>単一のセキュリティ エンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーションインスタンスを展開できるだけでした。ネイティブ インスタンスも引き続きサポートされています。Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。</p> <p>柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。コンテナ インスタンスを展開する場合、割り当てられた CPU コアの数に指定する必要があります。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。このリソース管理を使用すると、各インスタンスのパフォーマンス機能をカスタマイズできます。</p> <p>2つの個別のシャーシでコンテナ インスタンスを使用してハイ アベイラビリティを使用することができます。たとえば、10 個のインスタンスを持つシャーシを 2 つ使用する場合は、10 個のハイ アベイラビリティ ペアを作成できます。クラスタリングはサポートされません。</p> <p>(注) マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチ インスタンス機能では、独立したコンテナ インスタンスを使用できます。コンテナ インスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェア アップデート、および Firepower Threat Defense のフル機能のサポートが可能です。マルチ コンテキスト モードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。</p> <p>(注) FTD バージョン 6.3 以降が必要です。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 :</p> <p>[概要 (Overview) ]&gt;[デバイス (Devices) ]</p> <p>[インターフェイス (Interfaces) ]&gt;[すべてのインターフェイス (All Interfaces) ]&gt;[新規追加 (Add New) ] ドロップダウン メニュー&gt;[サブインターフェイス (Subinterface) ]</p> <p>[Interfaces] &gt; [All Interfaces] &gt; [Type]</p> <p>[論理デバイス (Logical Devices) ]&gt;[デバイスの追加 (Add Device) ]</p> <p>[プラットフォームの設定 (Platform Settings) ]&gt;[Mac プール (Mac Pool) ]</p> <p>[プラットフォームの設定 (Platform Settings) ]&gt;[リソースのプロファイル</p>

機能名	プラットフォームリリース	機能情報
		<p>(Resource Profiles) ]</p> <p>新規/変更された [Firepower Management Center] 画面 :</p> <p><b>[Devices] &gt; [Device Management] &gt; [Edit]</b> アイコン &gt; [Interfaces] タブ</p>
ASA 論理デバイスのトランスペアレントモード展開のサポート	2.4.1	<p>ASA を展開するときに、トランスペアレントまたはルーテッドモードを指定できるようになりました。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 :</p> <p><b>[Logical Devices] &gt; [Add Device] &gt; [Settings]</b></p> <p>新規/変更されたオプション : [Firewall Mode] ドロップダウン リスト</p>
クラスタ制御リンクのカスタマイズ可能な IP アドレス	2.4.1	<p>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。FXOS にクラスタを展開する際にネットワークを設定できるようになりました。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。</p> <p>新規/変更された画面 :</p> <p><b>[Logical Devices] &gt; [Add Device] &gt; [Cluster Information] &gt; [CCL Subnet IP]</b> フィールド</p>
FTD ブートストラップ設定については、FXOS CLI で FMC の NAT ID を設定できるようになりました。	2.4.1	<p>FXOS CLI で FMC NAT ID を設定できるようになりました。以前は、FTD CLI 内でのみ NAT ID を設定できました。通常は、ルーティングと認証の両方の目的で両方の IP アドレス (登録キー付き) が必要です。FMC がデバイスの IP アドレスを指定し、デバイスが FMC の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合 (ルーティング目的の最小要件) は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。FMC およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID (IP アドレスではなく) を使用します。</p> <p>新規/変更されたコマンド : <b>enter bootstrap-key NAT_ID</b></p>
ASA のサイト間クラスタリングの改善	2.1(1)	<p>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。</p> <p>次の画面が変更されました。 <b>[Logical Devices] &gt; [Configuration]</b></p>

機能名	プラットフォームリリース	機能情報
Firepower 9300 上の 6 個の FTD モジュールのシャーシ間クラスタリング	2.1.1	Firepower 9300 で FTD のシャーシ間クラスタリングを有効化できます。最大 6 つのモジュールを搭載することができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用して、最大 6 つのモジュールを組み合わせることができます。 次の画面が変更されました。[Logical Devices] > [Configuration]
Firepower 4100 での FTD クラスタリングのサポート	2.1.1	FTD クラスタで最大 6 個のシャーシをクラスタ化できます。
ASA クラスタでの 16 個の Firepower 4100 シャーシのサポート	2.0(1)	ASA クラスタで最大 16 個のシャーシをクラスタ化できます。
Firepower 4100 での ASA クラスタリングのサポート	1.1.4	ASA クラスタで最大 6 個のシャーシをクラスタ化できます。
Firepower 9300 の FTD でのシャーシ内クラスタリングサポート	1.1.4	Firepower 9300 が FTD アプリケーションでシャーシ内クラスタリングをサポートするようになりました。 次の画面が変更されました。[Logical Devices] > [Configuration]
Firepower 9300 上の 16 個の ASA モジュールのシャーシ間クラスタリング	1.1.3	ASA のシャーシ間クラスタリングが実現されました。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。 次の画面が変更されました。[Logical Devices] > [Configuration]
Firepower 9300 上の ASA のシャーシ内クラスタリング	1.1.1	Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できるようになりました。 次の画面が導入されました。[Logical Devices] > [Configuration]