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 （15 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 （40 ページ）
- クラスタの追加 （42 ページ）
- Radware DefensePro の設定 （73 ページ）
- 設定（Configure） TLS 暗号化アクセラレーション （84 ページ）
- 論理デバイスの管理 （89 ページ）
- 論理デバイスのモニタリング （98 ページ）
- サイト間クラスタリングの例 （100 ページ）
- 論理デバイスの履歴 （103 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ときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。

（注） Firepower 9300 の場合、異なるアプリケーション タイプ（ASA と 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 のすべての 3 つのモジュール アプリケーション インスタンスは、1 つの論理デバイスに属しています。

（注） Firepower 9300 の場合、すべてのモジュールがクラスタに属している必要があります。1 つのセキュリティ モジュールにスタンドアロン論理デバイスを作成し、残り 2 つのセキュリティ モジュールを使用してクラスタを作成することはできません。

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 インスタンスへの 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。

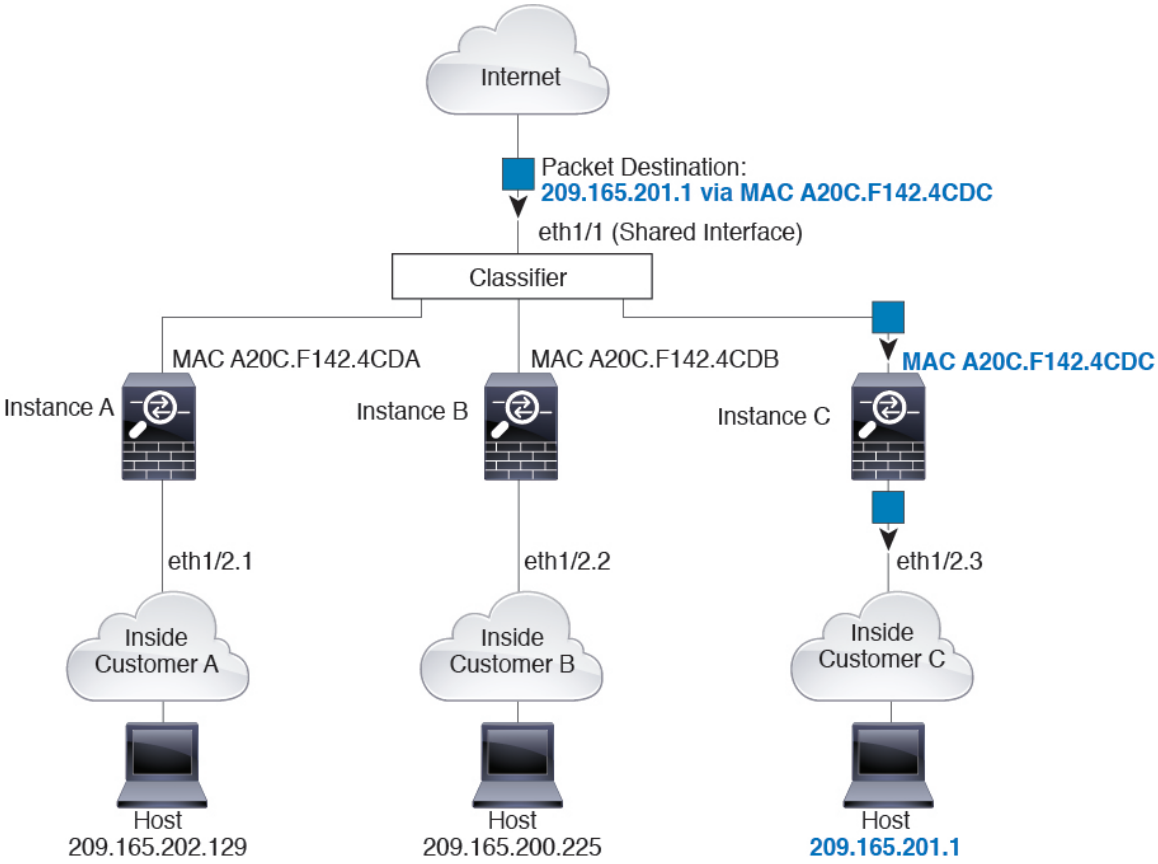
- 一意のインターフェイス：1 つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループ メンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意の MAC アドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイ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固有の 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

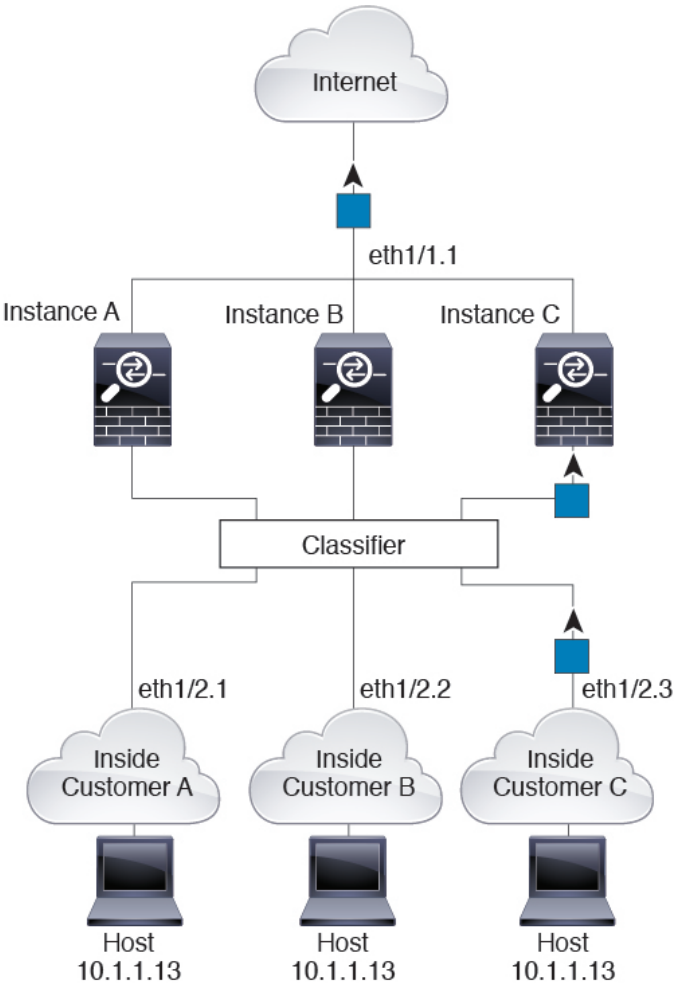
次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンスCにはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

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



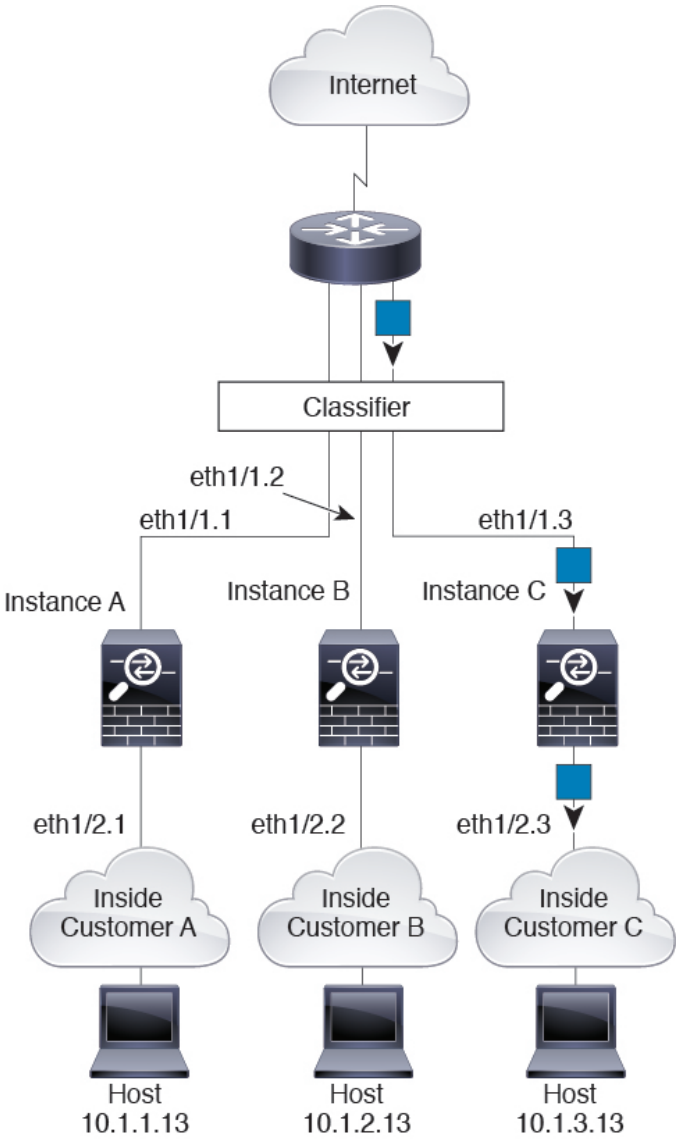
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *2*: 内部ネットワークからの着信トラフィック



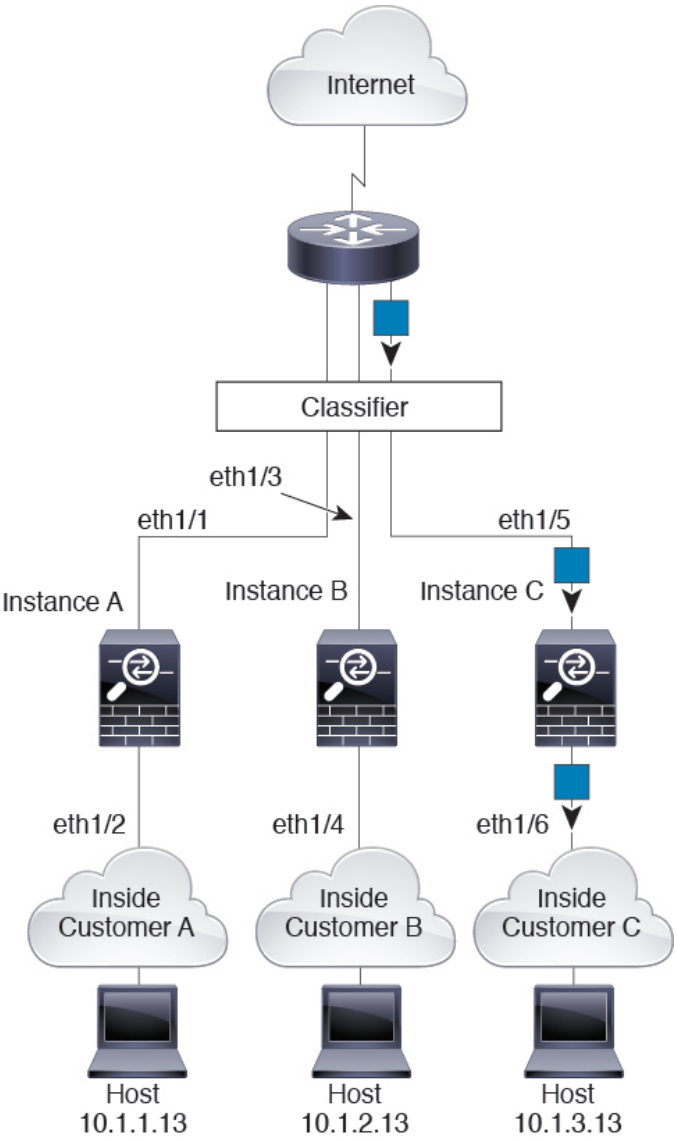
トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *3:* トランスペアレント 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、一意のインターフェイスを使用する必要があり、そのインターフェイスは物理インターフェイスまたは 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 のホストに向けられた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

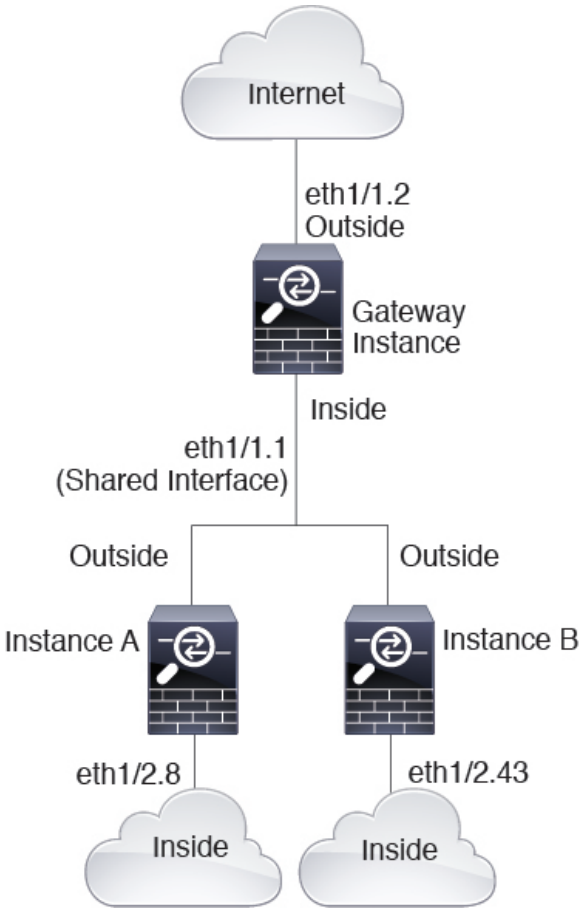


コンテナ インスタンスのカスケード

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

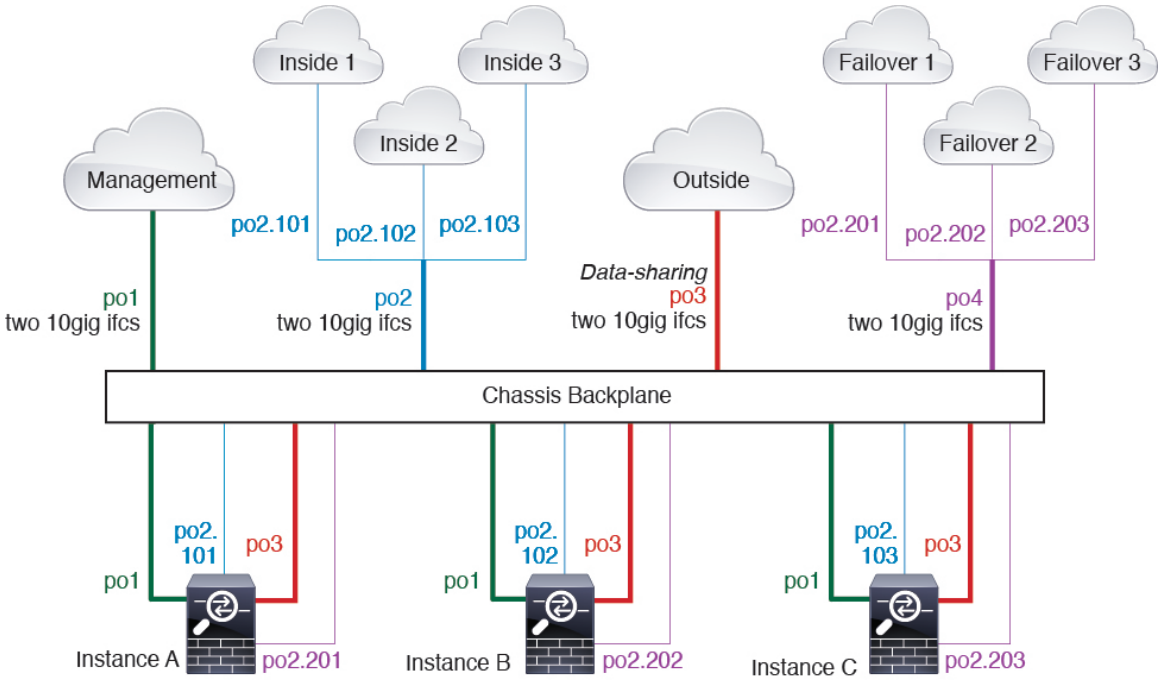


一般的な複数インスタンス展開

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の 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の 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の 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の 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。

A2*xx.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あり、*zz.zzzz* はシャーシ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の場合、プレフィックス 77 を設定すると、シャーシは 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シ ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.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。

A2**F1.03***zz.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場合は、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 40 GB に設定されます。モデルごとの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 （14 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 インスタンスのリソース プロファイルの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：約 21,000,000 ～ 24,000,000

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す。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。

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。

各ハイ アベイラビリティ ペアには専用のフェールオーバー リンクが必要です。データ共有インターフェイスを使用することはできません。親インターフェイス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。

（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す。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。 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モジュール間に高可用性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、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、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

たり、最大 6 つのモジュールを組み合わせたりできます。. 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：

- Firepower4100シリーズ：すべてのシャーシが同一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。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成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、インターフェイスが同じスパンドEtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。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。手動で時間を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リストについては、「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 メンバの場合。
  - 合計 4 クラスタ メンバ
  - 各サイト 2 メンバ
  - メンバあたり 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 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 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 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 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）のサイズ未満になってはなりません）。

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 Threat Defense

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ごとに 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 コア数	使用可能な RAM	使用可能なディスク容量
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
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。
- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイ アベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイ アベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 詳細については、ハイ アベイラビリティに関するアプリケーション コンフィギュレーション ガイドの章を参照してください。

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 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。
- 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

シャーシ間クラスタリングのスイッチ

- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。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（アジャセンシー）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。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。
- 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るので、ロード バランス 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にすることで、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。

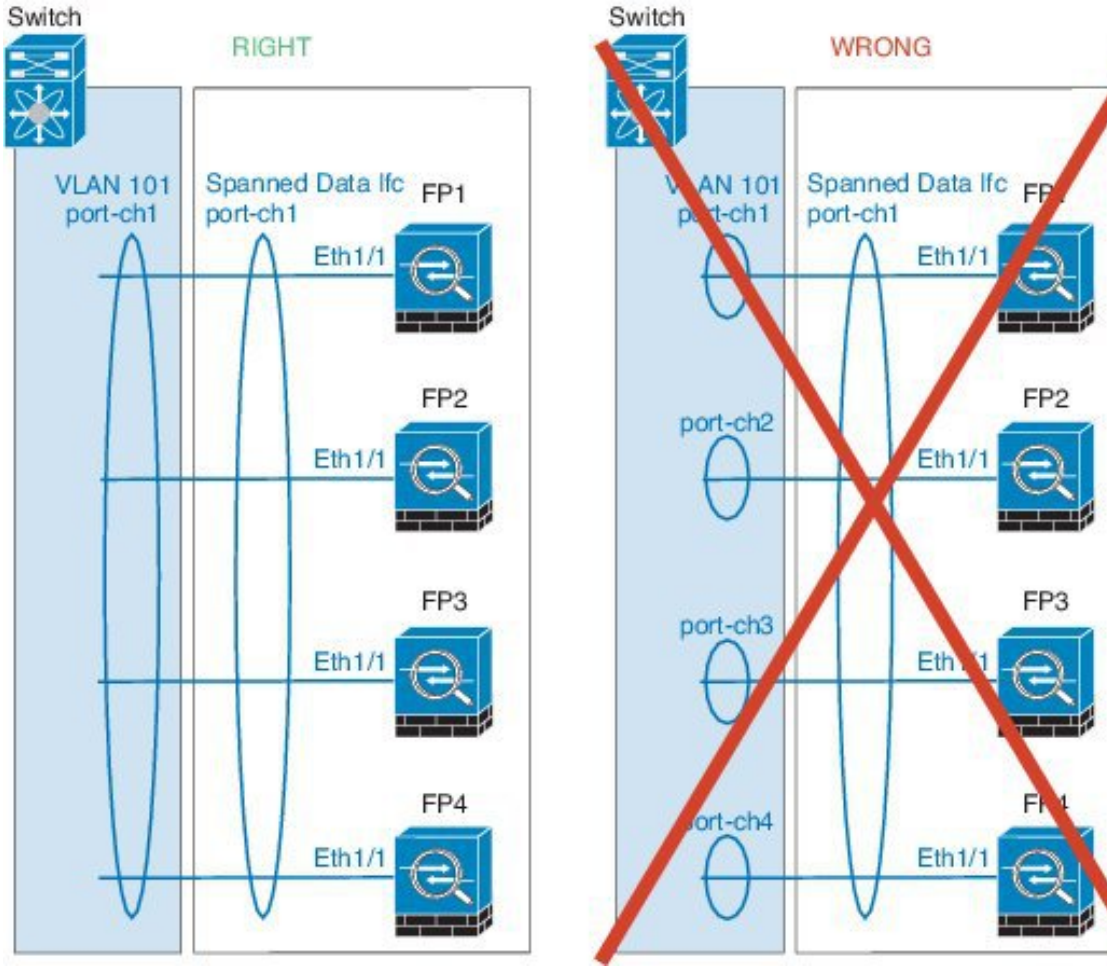
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

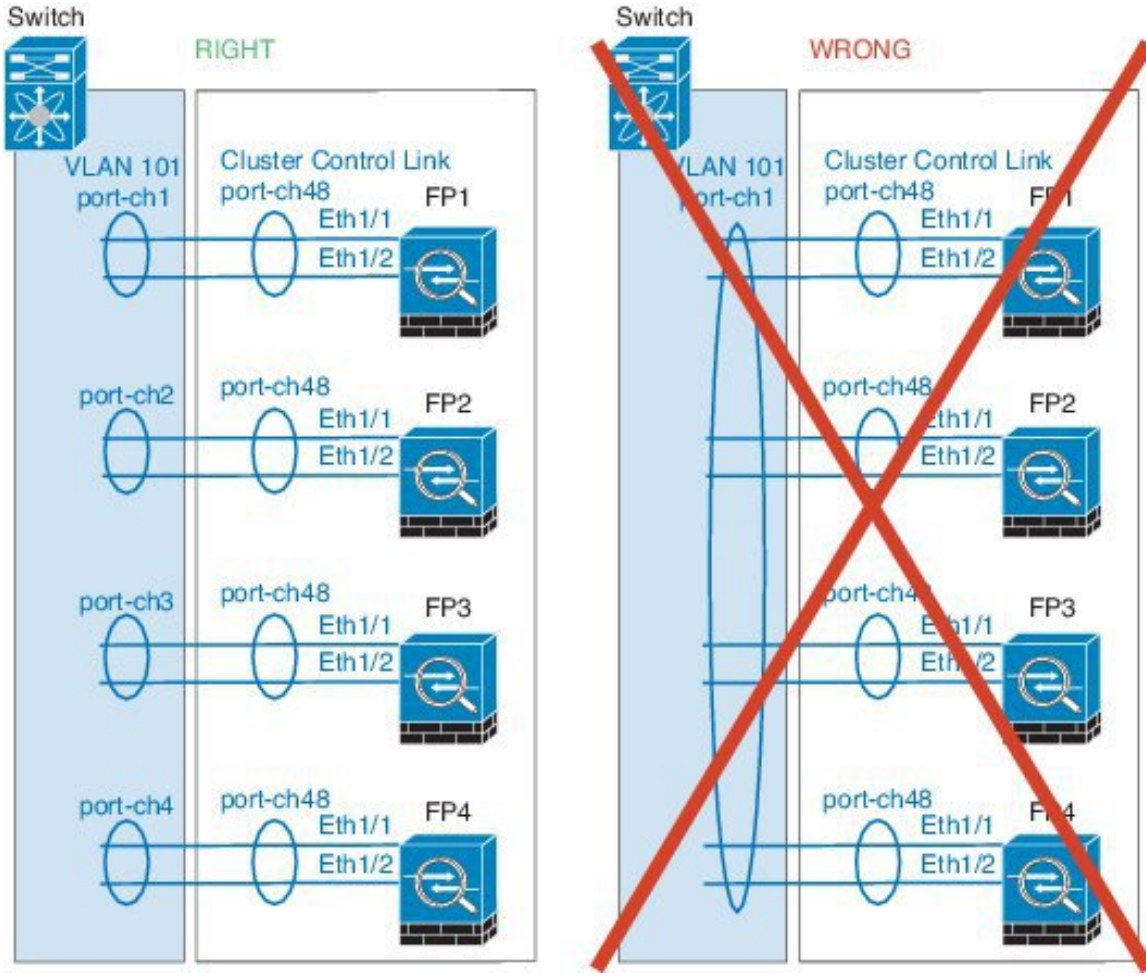
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [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。
- 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、接続オーナーと同じサイトからローカル ディレクタ権限が常に選択されます（サイト ID に応じて）。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では、次のトラフィック タイプの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 のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション 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 メンバがサイト 2 のメンバ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

- ユニットを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。これは予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、サーバが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージがクラスタに送信されます。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、デフォルトでイネーブルになり、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 モニタリングがイネーブルになっています。
- 失敗したクラスタ制御リンクのクラスタ自動再結合機能は、5 分おきに無制限に試行されるように設定されています。
- 失敗したデータ インターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されるように設定されています。
- HTTP トラフィックは、5 秒間の接続レプリケーション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（40 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導入できます。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（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（Firepower 4100/9300 シャーシ への論理デバイスのソフトウェア イメージのダウンロードを参照） にダウンロードします。

（注） Firepower 9300 の場合、異なるアプリケーション タイプ（ASA と 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（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

例：

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

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

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

scope slot *slot_id*

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

例：

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

c) アプリケーション インスタンスを作成します。

enter app-instance asa *device_name*

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

例：

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

d) ASA イメージ バージョンを設定します。

set startup-version *version*

例：

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

e) スロット モードを終了します。

exit

例：

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

f) ssa モードを終了します。

exit

例：

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

例：

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

ステップ 3 論理デバイスを作成します。

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

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

例：

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

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

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

set description *description*

exit

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

管理インターフェイスは、シャーシ管理ポートと同じではありません。ASA のデータ インターフェイスを後で有効にして設定します。これには、IP アドレスの設定も含まれます。

例：

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

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap asa

例：

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

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

create bootstrap-key FIREWALL_MODE

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

exit

ルーテッドモードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、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」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

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

例：

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

c) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

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

d) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **default**

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

set gateway *gateway_address*

exit

例：

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

e) IPv6 管理インターフェイス設定を設定します。

create ipv6 *slot_id* **default**

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

set gateway *gateway_address*

exit

例：

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

f) 管理ブートストラップ モードを終了します。

exit

例：

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

ステップ 6 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェア バージョンをダウンロードし、アプリケーション インスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

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

```
Container   Default-Small Not Applicable  None
```

ステップ 7 セキュリティ ポリシーの設定を開始するには、ASA コンフィギュレーション ガイドを参照してください。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

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導入できます。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することができます。

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（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（Firepower 4100/9300 シャーシ への論理デバイスのソフトウェア イメージのダウンロードを参照）にダウンロードします。

  （注） Firepower 9300 の場合、異なるアプリケーション タイプ（ASA と 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（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。
- また、少なくとも 1 つのデータ型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 インスタンスのリソース プロファイルの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。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 インスタンスとコンテナ インスタンスを交換する場合は、必ずネイティブ 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/エンジンの再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 アドレスおよび/または 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 セキュリティ サービス モードを開始します。

scope ssa

例：

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

ステップ 2 使用する Firepower Threat Defense バージョンのエンドユーザ ライセンス契約書に同意します。このバージョンの EULA をまだ同意していない場合のみ、この手順を実行する必要があります。

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) イメージ バージョンに範囲を設定します。

scope app ftd *application_version*

例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) ライセンス契約に同意します。

accept-license-agreement

例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
```

```
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 設定を保存します。

commit-buffer

例：

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

e) セキュリティ サービス モードを終了します。

exit

例：

```
Firepower /ssa/app # exit
Firepower /ssa #
```

ステップ 3 アプリケーション インスタンス パラメータ（イメージ バージョンを含む）を設定します。

a) コンテナ インスタンスの場合は、使用可能なリソース プロファイルを表示します。プロファイルを追加する場合は、コンテナ インスタンスのリソース プロファイルの追加を参照してください。

show resource-profile

使用するプロファイル名に注意してください。

例：

```
Firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical
Core Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------
---------------------- ------------- --------------- ------------ -----------
bronze             N/A        N/A          No         all
       6             N/A No              Custom       low end device
silver 1           N/A        N/A          No         all
       8             N/A No              Custom       mid-level
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

scope slot *slot_id*

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

例：

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

c) アプリケーション インスタンスを作成します。

enter app-instance ftd *device_name*

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

例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

d) コンテナ インスタンスの場合は、コンテナにアプリケーション インスタンス タイプを設定します。

set deploy-type container

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。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。

設定の保存後に、インスタンス タイプを変更することはできません。デフォルトのタイプは **native** です。

例：

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

e) コンテナ インスタンスの場合は、リソース プロファイルを設定します。

set resource-profile-name *name*

このプロファイル名はすでに存在している必要があります。

後でさまざまな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、これには約 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。

例：

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

f) Firepower Threat Defense イメージ バージョンを設定します。

set startup-version *version*

EULA に同意するときに上記の手順でメモしたバージョン番号を入力します。

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

g) スロット モードを終了します。

exit

例：

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

h) （任意） Firepower 4110 または 4120 の Radware DefensePro インスタンスを作成します。このためには、論理デバイスの作成前にアプリケーションインスタンスを作成する必要があります（Radware DefensePro はコンテナ インスタンスでサポートされていません）。

enter app-instance vdp *device_name*

exit

Firepower Threat Defense アプリケーション インスタンスに一致するように *device_name* を設定します。論理デバイス設定を確定したら、続いて Firepower Threat Defense 論理デバイスを使用して、サービス チェーン内に Radware DefensePro デコレータを設定する必要があります。スタンドアロンの論理デバイスでの Radware DefensePro の設定 （75 ページ）の手順 4 を参照してください。

例：

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

i) ssa モードを終了します。

exit

例：

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

例：

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

```
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 4 論理デバイスを作成します。

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

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

例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 5 管理およびデータ インターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

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

set description *description*

exit

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

管理インターフェイスは、シャーシ管理ポートと同じではありません。後ほど FMC でデータ 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。

例：

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

ステップ 6 管理ブートストラップ パラメータを設定します。

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。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap ftd

例：

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

b) Firepower Management Center を管理する IP アドレス、ホスト名、または NAT ID を指定します。

次の設定を行います。

- **enter bootstrap-key FIREPOWER_MANAGER_IP**

  set value *IP_address*

  exit

- **enter bootstrap-key FQDN**

  setvalue *fmc_hostname*

  exit

- **enter bootstrap-key NAT_ID**

  set value *nat_id*

  exit

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。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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key
FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

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

create bootstrap-key FIREWALL_MODE

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

exit

ルーテッド モードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、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」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

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

例：

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

d) デバイスと Firepower Management Center との間で共有するキーを指定します。このキーのパスフレーズは、1 ～ 37 文字の範囲で選択できます。を追加するときに、 FMCに同じキーを入力しますFTD。

create bootstrap-key-secret REGISTRATION_KEY

set value

値の入力：*registration_key*

値の確認：*registration_key*

exit

例：

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

e) 管理者のパスワードを指定します。このパスワードは、CLI アクセスを行う管理者ユーザに使用されます。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

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

f) 完全修飾ホスト名を指定します。

create bootstrap-key FQDN

set value *fqdn*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftd1.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) DNS サーバのカンマ区切りリストを指定します。

create bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 検索ドメインのカンマ区切りリストを指定します。

create bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) （任意）FTD SSH セッションからエキスパート モードを許可します。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。

create bootstrap-key PERMIT_EXPERT_MODE

set value {**yes** | **no**}

exit

- **yes**：SSH セッションからこのコンテナ 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。
- **no**：FXOS CLI からコンテナ インスタンスにアクセスするユーザだけがエキスパート モードを開始できます。

デフォルトでは、コンテナインスタンスの場合、エキスパートモードを使用できるのは FXOS CLI から FTD CLI にアクセスするユーザだけです。この制限は、インスタンス間の分離を増やす場合、コンテナインスタンスのみに適用されます。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。

例：

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

j) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **firepower**

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

set gateway *gateway_address*

exit

例：

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

k) IPv6 管理インターフェイス設定を設定します。

create ipv6 *slot_id* **firepower**

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

set gateway *gateway_address*

exit

例：

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

l) 管理ブートストラップ モードを終了します。

exit

例：

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

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェア バージョンをダウンロードし、アプリケーション インスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

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

ステップ 8 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。

例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
```

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

ハイ アベイラビリティ ペアの追加

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

始める前に

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイ アベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 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。
- 他の高可用性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高可用性に関する章を参照してください。

手順

ステップ 1 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイ アベイラビリティは推奨されず、サポートされない可能性があります。

ステップ 2 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 3 フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイアベイラビリティ トラフィックを交換します。統合されたフェールオーバー リンクとステート リンクには、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、データ共有インターフェイスは、フェールオーバー リンクで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 リンクとして使用し、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 4 論理デバイスでハイ アベイラビリテを有効にします。

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

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

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グループ化する、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 シャーシでのクラスタリングについて

クラスタは、単一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、シャーシ間通信のために、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各ユニットに対して、最小限のブートストラップ構成がFirepower 4100/9300 シャーシ スーパーバイザからプッシュされます。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。

標準出荷単位とセカンダリ単位の役割

クラスタのメンバーの1つが標準出荷単位です。標準出荷単位は自動的に決定されます。他のすべてのメンバーはセカンダリ単位です。

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。 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。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。

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。

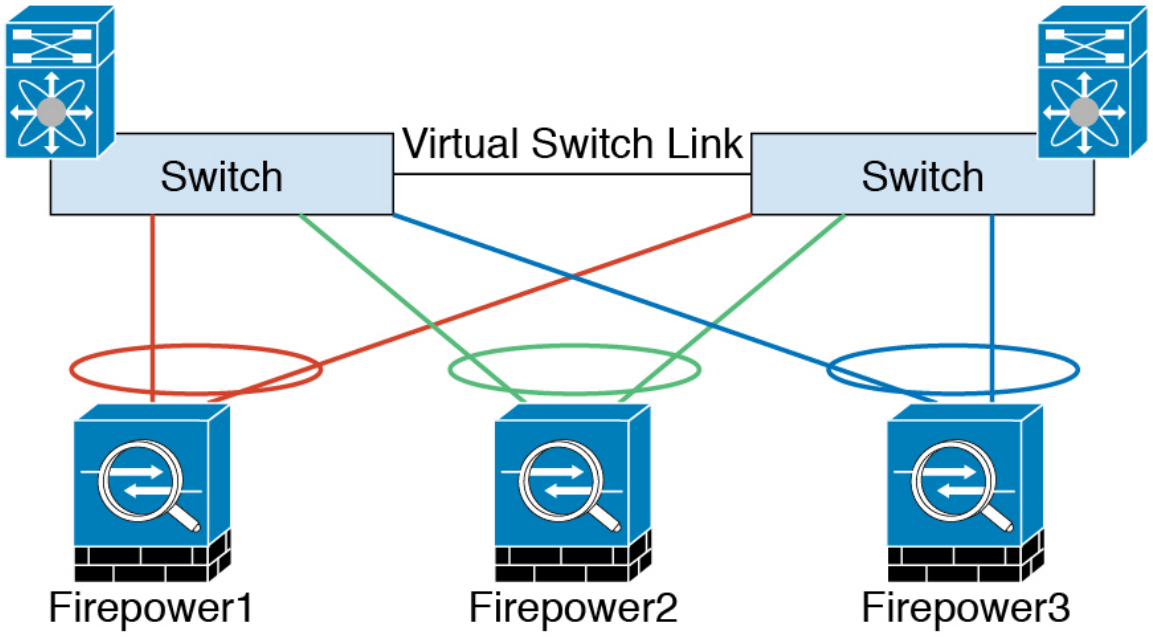
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

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 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。クラスタを展開する場合にこの 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 ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。 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

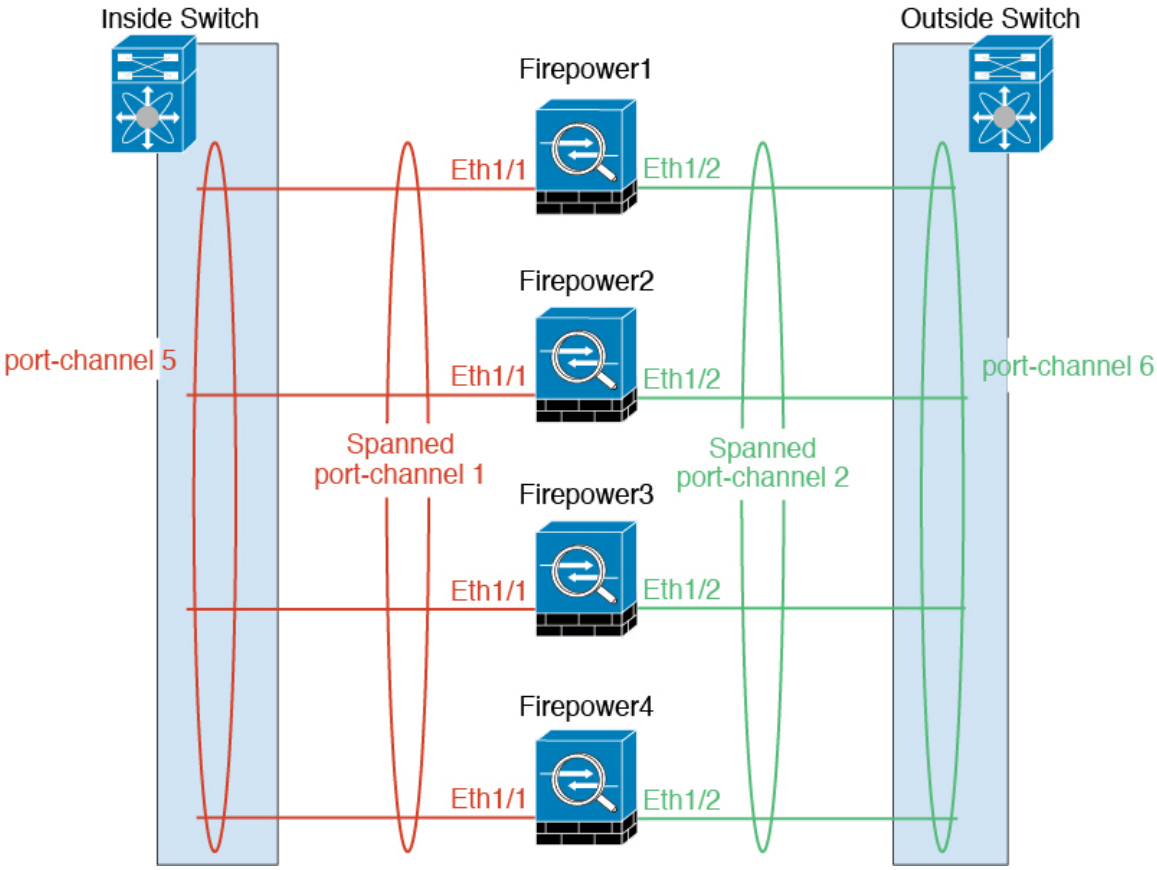
管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

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、MAC フラッピングの原因となる 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 アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの 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 インスペクションを使用したフロー モビリティの有効化、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向上とラウンドトリップ時間の遅延短縮のためのディレクタ ローカリゼーションの有効化、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存在する接続に対するサイト冗長性の有効化の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 （100 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、次のシャーシにほぼ同じ設定を入力します。

ASA クラスタの作成

クラスタは、Firepower 4100/9300 シャーシ スーパ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に自動的に生成されます。

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。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロット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。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ

EtherChannel を追加します。スイッチ上で、すべてのクラスタ ユニットから 1 つの EtherChannel にメンバ インターフェイスを結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （17 ページ）を参照してください。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。シャーシ間クラスタリングでは、Etherchannel のみが割り当てられます。他のインターフェイス タイプを割り当てることはできません。導入後にもクラスタにデータ インターフェイスを追加できます。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

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インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

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

シャーシ内クラスタリングのメンバー インターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタがシャーシ間であると見なし、例えばスパンド Etherchannel のみを使用できるようになります。

各シャーシに同じメンバインターフェイスを追加します。各シャーシでは、クラスタ制御リンクはデバイスローカルな EtherChannel です。デバイスごとにスイッチで個別の Etherchannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （17 ページ） を参照してください。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例：

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

ステップ 3 デフォルトのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

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

```
asa        9.10.1          cisco      Native                Application Yes
ftd        6.2.3           cisco      Native                Application Yes
ftd        6.3.0           cisco      Native,Container      Application Yes
```

b) イメージ バージョンに範囲を設定します。

scope app asa *application_version*

例：

```
Firepower /ssa # scope asa ftd 9.10.1
Firepower /ssa/app #
```

c) このバージョンをデフォルトとして設定します。

set-default

例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) ssa モードを終了します。

exit

例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name*：Firepower 4100/9300 シャーシ スーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタ名ではありません。まだハードウェアをインストールしていなくても、3 つのセキュリティ モジュールすべてを指定する必要があります。
- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1、2、3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロット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。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 5 クラスタ ブートストラップ パラメータを設定します。

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。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

c) サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

サイト ID を削除するには、値を **0** に設定します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

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。

e) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) セキュリティ モジュール設定のクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （任意） Cluster Control Link IP ネットワークを設定します。

set cluster-control-link network *a*.*b*.**0.0**

Cluster Control Link 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 アドレスを指定できます。

- *a*.*b*.**0.0**：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（127.2.0.0）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。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
 10.10.0.0
```

h) 管理 IP アドレス情報を設定します。

この情報は、セキュリティ モジュール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。

1. ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、この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。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   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。

2. 管理インターフェイスのメイン クラスタ IP アドレスを設定します。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

3. ネットワーク ゲートウェイ アドレスを入力します。

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11
2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) クラスタ ブートストラップ モードを終了します。

   exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップ パラメータを設定します。

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。

a) 管理ブートストラップ オブジェクトを作成します。

   enter mgmt-bootstrap asa

   例：

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

b) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

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

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

create bootstrap-key FIREWALL_MODE

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

exit

ルーテッドモードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、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」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

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

例：

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

d) 管理ブートストラップ モードを終了します。

exit

例：

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

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェア バージョンをダウンロードし、アプリケーション インスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ----------- ------------ ---------------- ------------
ftd        cluster1   1          Enabled     Online           6.4.0.49        6.4.0.49
       Native                   In Cluster      Slave
ftd        cluster1   2          Enabled     Online           6.4.0.49        6.4.0.49
       Native                   In Cluster      Master
ftd        cluster1   3          Disabled    Not Available                    6.4.0.49
       Native                   Not Applicable  None
```

ステップ 8 クラスタに別のシャーシを追加する場合は、この手順を繰り返しますが、固有の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、両方のシャーシで同じ設定を使用します。

インターフェイス コンフィギュレーションが新しいシャーシと同じであることを確認します。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。

ステップ 9 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。

例

シャーシ 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
```

```
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
```

```
commit-buffer
```

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 [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 2 クラスタに別のシャーシを追加する場合は、ASA クラスタの作成 （47 ページ） の手順を繰り返しますが、一意の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、新しいシャーシに同じ設定を使用します。

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、次のシャーシにほぼ同じ設定を入力します。

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に自動的に生成されます。

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。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロット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 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 アドレスおよび/または 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。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタ ユニットから 1 つ の EtherChannel にメンバ インターフェイスを結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （17 ページ）を参照してください。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。 シャーシ間クラスタリングでは、Etherchannel のみが割り当てられます。他のインターフェイス タイプを割り当てることはできません。導入後にもクラスタにデータ インターフェイスを追加できます。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

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インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

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

シャーシ内クラスタリングのメンバー インターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタがシャーシ間であると見なし、例えばスパンド Etherchannel のみを使用できるようになります。

各シャーシに同じメンバインターフェイスを追加します。各シャーシでは、クラスタ制御リンクはデバイスローカルな EtherChannel です。デバイスごとにスイッチで個別の Etherchannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （17 ページ） を参照してください。

d) （任意） Firepower-eventing インターフェイスを追加します。

このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firepower Threat Defense コマンド リファレンスの **configure network** コマンドを参照してください。

シャーシ間クラスタリングの場合、各シャーシに同じイベンティングインターフェイスを追加します。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例：

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

ステップ 3 デフォルトのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

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

```
    ftd        6.3.0          cisco      Native,Container       Application Yes
```

b) イメージ バージョンに範囲を設定します。

scope app ftd *application_version*

例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) このバージョンをデフォルトとして設定します。

set-default

例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) ライセンス契約に同意します。

accept-license-agreement

例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

e) ssa モードを終了します。

exit

例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope app ftd 6.3.0.21
Firepower /ssa/app # set-default
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。

enter logical-device *device_name* **ftd** *slots* **clustered**

- *device_name*：Firepower 4100/9300 シャーシ スーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタ名ではありません。
- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1、2、3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロット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。

例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 5 クラスタ ブートストラップ パラメータを設定します。

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。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

c) サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

サイト ID を削除するには、値を **0** に設定します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

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。

e) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) セキュリティ モジュール設定のクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （任意） Cluster Control Link IP ネットワークを設定します。

set cluster-control-link network *a*.*b*.**0.0**

Cluster Control Link 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 アドレスを指定できます。

- ***a.b*.0.0**：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（127.2.0.0）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。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
 10.10.0.0
```

h) クラスタ ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップ パラメータを設定します。

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。

a) 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap ftd

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) Firepower Management Center を管理する IP アドレス、ホスト名、または NAT ID を指定します。

次の設定を行います。

- **enter bootstrap-key FIREPOWER_MANAGER_IP**

  set value *IP_address*

  exit

- **enter bootstrap-key FQDN**

  setvalue *fmc_hostname*

exit

- **enter bootstrap-key NAT_ID**

  set value *nat_id*

  exit

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。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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key NAT_ID
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value sc0rpius15
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

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

create bootstrap-key FIREWALL_MODE

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

exit

ルーテッド モードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。これに対し、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」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

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

例：

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

d) デバイスと FMC との間で共有するキーを指定します。

enter bootstrap-key-secret REGISTRATION_KEY

set value

値の入力：*registration_key*

値の確認：*registration_key*

exit

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。

例：

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

e) CLI アクセスのFTD管理ユーザのパスワードを指定します。

enter bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

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

f) 完全修飾ホスト名を指定します。

enter bootstrap-key FQDN

set value *fqdn*

exit

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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdcluster1.example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) DNS サーバのカンマ区切りリストを指定します。

enter bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

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。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 検索ドメインのカンマ区切りリストを指定します。

enter bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) クラスタ内の各セキュリティ モジュールの管理 IP アドレスを設定します。

（注） Firepower 9300 の場合、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。

IPv4 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。

   enter ipv4 *slot_id* **firepower**

2. ゲートウェイ アドレスを設定します。

   set gateway *gateway_address*

3. IP アドレスとマスクを設定します。

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

4. 管理 IP モードを終了します。

   exit

5. シャーシの残りのモジュールに対して手順を繰り返します。

IPv6 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。

   enter ipv6 *slot_id* **firepower**

2. ゲートウェイ アドレスを設定します。

   set gateway *gateway_address*

3. IP アドレスとプレフィックスを設定します。

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

4. 管理 IP モードを終了します。

   exit

5. シャーシの残りのモジュールに対して手順を繰り返します。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.35 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.36 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3211
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3212
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

j) 管理ブートストラップ モードを終了します。

exit

例：

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

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: ziggy$tardust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェア バージョンをダウンロードし、アプリケーション インスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- ---------------
--------------- ----------- ------------ --------------- ------------
ftd        cluster1   1          Enabled     Online          6.4.0.49        6.4.0.49
       Native                   In Cluster      Slave
ftd        cluster1   2          Enabled     Online          6.4.0.49        6.4.0.49
       Native                   In Cluster      Master
ftd        cluster1   3          Disabled    Not Available                   6.4.0.49
       Native                   Not Applicable  None
```

ステップ 8 クラスタに別のシャーシを追加するには、この手順を繰り返しますが、固有の **chassis-id**、固有の管理IPアドレス、および正しい**site-id**を設定する必要があります。そうでない場合は両方のシャーシで同じ設定を使用します。

インターフェイス コンフィギュレーションが新しいシャーシと同じであることを確認します。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。

ステップ 9 管理 IP アドレスを使用してマスター ユニットを Firepower Management Center に追加します。

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 ユニットを自動的に検出します。

例

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
```

```
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.31 mask 255.255.255.0
        exit
      enter ipv4 2 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.32 mask 255.255.255.0
        exit
      enter ipv4 3 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.33 mask 255.255.255.0
```

```
        exit
      exit
    exit
  scope app ftd 6.0.0.837
    accept-license-agreement
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
```

```
  enter mgmt-bootstrap ftd
    enter bootstrap-key FIREPOWER_MANAGER_IP
      set value 10.0.0.100
      exit
    enter bootstrap-key FIREWALL_MODE
      set value transparent
      exit
    enter bootstrap-key-secret REGISTRATION_KEY
      set value
        Value: alladinsane
      exit
    enter bootstrap-key-secret PASSWORD
      set value
        Value: widthofacircle
      exit
    enter bootstrap-key FQDN
      set value ftd.cisco.com
      exit
    enter bootstrap-key DNS_SERVERS
      set value 192.168.1.1
      exit
    enter bootstrap-key SEARCH_DOMAINS
      set value search.com
      exit
    enter ipv4 1 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.31 mask 255.255.255.0
      exit
    enter ipv4 2 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.32 mask 255.255.255.0
      exit
    enter ipv4 3 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.33 mask 255.255.255.0
      exit
    exit
  exit
scope app ftd 6.0.0.837
  accept-license-agreement
  exit
commit-buffer
```

クラスタ メンバの追加

既存のクラスタ内の FTD クラスタ メンバ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

別のシャーシをクラスタに追加するには、Firepower Threat Defense クラスタの作成 （58 ページ） の手順を繰り返します（次の設定を固有のものとして設定する必要のある場合を除きます。そうでない場合には、両方のシャーシに同じ設定を使用します）。

- シャーシ ID（Chassis ID）
- 管理 IP アドレス

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。

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 シャーシにダウンロードします（Firepower 4100/9300 シャーシへの論理デバイスのソフトウェア イメージのダウンロードを参照）。
- 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 （78 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 スタンドアロン構成で 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（28 ページ）を参照）。 Firepower 4110 または 4120 セキュリティ アプライアンス上にイメージをインストールする場合には、設定をコミットする前に、vDP を Firepower Threat Defense イメージとともにインストールする必要があることに注意してください。

ステップ 3 セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

ステップ 4 Radware vDP インスタンスを作成します。

```
Firepower /ssa # scope slot slot_id
Firepower /ssa/slot # create app-instance vdp
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot/* # exit
```

ステップ 5 設定をコミットします。

```
commit-buffer
```

ステップ 6 セキュリティ モジュールの vDP の設置とプロビジョニングを確認します。

Firepower /ssa # **show app-instance**

例：

```
Firepower /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
--------------- -------------
ftd        1          Enabled     Online           6.2.1.62        6.2.1.62        Not
Applicable  None
vdp        1          Disabled    Installing                       8.10.01.16-5    Not
Applicable  None
```

ステップ 7 （オプション）サポートされている利用可能なリソース プロファイルを表示するには：

Firepower /ssa/app # **show resource-profile system**

例：

```
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
    4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

   10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
    2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
    4          16384 No              System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    8          32768 No              System
```

ステップ 8 （オプション）前の手順の使用可能なプロファイルの 1 つを使用して、リソース プロファイルを設定します。

a) 範囲をスロット 1 にします：

Firepower /ssa*# **scope slot 1**

b) DefensePro アプリケーション インスタンスを入力します。

Firepower /ssa/slot* # **enter app-instance vdp**

c) アプリケーション インスタンスを有効にします。

Firepower /ssa/slot/app-instance* # **enable**

d) リソース プロファイルを設定します。

Firepower /ssa/slot/app-instance* # **set resource-profile-name** *resource_profile_name*

e) 設定をコミットします。

Firepower /ssa/slot/app-instance* # **commit-buffer**

ステップ 9 vDP アプリケーションがオンライン状態になった後、論理デバイスにアクセスします。

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

ステップ 10 vDP に管理インターフェイスを割り当てます。論理デバイスのものと同じ物理インターフェイスを使用することも、別のインターフェイスを使用することもできます。

Firepower /ssa/logical-device # **enter external-port-link** *nameinterface_id* **vdp**

Firepower /ssa/logical-device/external-port-link* # **exit**

ステップ 11 vDP の外部管理インターフェイス設定を設定します。

a) ブートストラップ オブジェクトを作成します。

Firepower /ssa/logical-device* # **create mgmt-bootstrap vdp**

b) 管理 IP アドレスを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap* #**create ipv4** *slot_id* **default**

c) ゲートウェイ アドレスを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set gateway** *gateway_address*

d) IP アドレスとマスクを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set ip** *ip_address* **mask** *network_mask*

e) 管理 IP 設定スコープを終了します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**exit**

f) 管理ブートストラップ設定スコープを終了します。

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

ステップ 12 ASA または Firepower Threat Defense フローの前に vDP を配置するデータ インターフェイスを編集します。

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

show external-port-link コマンドを入力して、インターフェイス名を表示します。

ステップ 13 論理デバイスに vDP を追加します。

Firepower /ssa/logical-device/external-port-link* # **set decorator vdp**

vDP を使用するインターフェイスごとに手順を繰り返します。

ステップ 14 サードパーティのアプリケーションがインターフェイスに設定されていることを確認します。

Firepower /ssa/logical-device/external-port-link* # **show detail**

例：

```
Firepower /ssa/logical-device/external-port-link # show detail

External-Port Link:
    Name: Ethernet11_ftd
    Port or Port Channel Name: Ethernet1/1
    App Name: ftd
    Description:
    Link Decorator: vdp
```

ステップ 15 設定をコミットします。

commit-buffer

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

（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 シャーシにダウンロードします（Firepower 4100/9300 シャーシへの論理デバイスのソフトウェア イメージのダウンロードを参照）。

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 シャーシ内クラスタ（ASA クラスタの作成 （47 ページ）を参照）、または Firepower Threat Defense シャーシ内クラスタ（Firepower Threat Defense クラスタの作成 （58 ページ）を参照）を設定します。

ステップ 3 外部（クライアント側）ポートを Radware DefensePro でデコレートします。

enter external-port-link *name interface_name* { **asa** | **ftd** }

セット **decorator vdp**

セット **description ""**

exit

ステップ 4 論理デバイスの外部管理ポートを割り当てます。

enter **external-port-link** *{ mgmt_asa | mgmt_ftd } interface_id { asa | ftd }*

セット **decorator ""**

セット **description ""**

exit

ステップ 5 DefensePro の外部管理ポートを割り当てます。

enter **external-port-link mgmt_vdp** *interface_name { asa | ftd }*

セット **decorator ""**

セット **description ""**

ステップ 6 （オプション）サポートされている利用可能なリソース プロファイルを表示するには：

show resource-profile system

例：

```
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------
---------------------- -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
    4          16384 Yes              System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    6          24576 Yes              System
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

   10          40960 No               System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
    2           8192 No               System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
    4          16384 No               System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    8          32768 No               System
```

ステップ 7 （オプション）前の手順の使用可能なプロファイルの1つを使用して、リソースプロファイルを設定します。

（注） この変更をコミットすると、FXOS シャーシが再起動します。

a) 範囲をスロット 1 にします：

Firepower /ssa*# **scope slot 1**

b) DefensePro アプリケーション インスタンスを入力します。

Firepower /ssa/slot* # **enter app-instance vdp**

c) アプリケーション インスタンスを有効にします。

Firepower /ssa/slot/app-instance* # **enable**

d) リソース プロファイルを設定します。

Firepower /ssa/slot/app-instance* # **set resource-profile-name** *resource_profile_name*

e) 設定をコミットします。

Firepower /ssa/slot/app-instance* # **commit-buffer**

ステップ 8 クラスタ ポート チャネルを設定します。

enter **external-port-link** port-channel48 Port-channel48 *{ asa | ftd }*

セット **decorator ""**

セット **description ""**

exit

ステップ 9 DefensePro の 3 つのすべてのインスタンスの管理ブートストラップを設定します。

enter **mgmt-bootstrap vdp**

enter **ipv4** *slot_id* **default**

set gateway *gateway_address*

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

exit

例：

```
enter mgmt-bootstrap vdp
    enter ipv4 1 default
        set gateway 172.16.0.1
        set ip 172.16.4.219 mask 255.255.0.0
    exit

    enter ipv4 2 default
        set gateway 172.16.0.1
        set ip 172.16.4.220 mask 255.255.0.0
    exit

    enter ipv4 3 default
        set gateway 172.16.0.1
        set ip 172.16.4.221 mask 255.255.0.0
    exit
```

ステップ 10 管理ブートストラップ設定スコープを終了します。

exit

ステップ 11 マスター ブレード上の DefensePro アプリケーション インスタンスを入力します。

connect module *slot* **console**

connect vdp

ステップ 12 マスター ブレードで、管理 IP を設定します。

device clustering management-channel ip

ステップ 13 前のステップで確認した IP を使用して、マスター IP を設定します。

device clustering master set *management-channel ip*

ステップ 14 クラスタを有効化します。

device clustering state set enable

ステップ 15 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 に戻ります。

Ctrl]

ステップ 16 ステップ 10、12、13、14 を繰り返してステップ 11 で確認したマスター IP を設定し、各ブレード アプリケーション インスタンスに対してクラスタを有効化します。

ステップ 17 設定をコミットします。

commit-buffer

（注） この手順を完了したら、DefenseProインスタンスがクラスタに設定されているかどうかを確認する必要があります。

ステップ 18 DefensePro アプリケーションのすべてがクラスタに参加していることを確認します。

device cluster show

ステップ 19 以下のいずれかの方法で、「primary」と「secondary」の DefensePro インスタンスがどれであるかを確認します。

a) DefensePro インスタンスの範囲を指定し、DefensePro のアプリケーション属性のみを表示します。

scope ssa

scope slot *slot_number*

scope app-instance vdp

show app-attri

b) スロットの範囲を指定し、DefensePro インスタンスの詳細を表示します。このアプローチでは、スロット上の論理デバイスと vDP 両方のアプリケーション インスタンス情報が表示されます。

scope ssa

scope *slot_number*

show app-instance 詳細を展開

DefensePro アプリケーションがオンラインでもクラスタ化されていない場合は、CLI に次のように表示されます。

```
App Attribute:
    App Attribute Key: cluster-role
    Value: unknown
```

この「unknown」値が表示された場合は、vDP クラスタを作成するために、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。

DefensePro アプリケーションがオンラインでクラスタ化されている場合は、CLI に次のように表示されます。

```
App Attribute:
    App Attribute Key: cluster-role
    Value: primary/secondary
```

例

```
scope ssa
  enter logical-device ld asa "1,2,3" clustered
     enter cluster-bootstrap
         set chassis-id 1
         set ipv4 gateway 172.16.0.1
         set ipv4 pool 172.16.4.216 172.16.4.218
         set ipv6 gateway 2010::2
         set ipv6 pool 2010::21 2010::26
         set key secret
         set mode spanned-etherchannel
         set name cisco
         set virtual ipv4 172.16.4.222 mask 255.255.0.0
         set virtual ipv6 2010::134 prefix-length 64
     exit
     enter external-port-link Ethernet1-2 Ethernet1/2 asa
         set decorator vdp
         set description ""
     exit
     enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
         set decorator ""
         set description ""
     exit
     enter external-port-link mgmt_asa Ethernet1/1 asa
         set decorator ""
         set description ""
     exit
     enter external-port-link mgmt_vdp Ethernet1/1 vdp
         set decorator ""
         set description ""
     exit
     enter external-port-link port-channel48 Port-channel48 asa
         set decorator ""
         set description ""
     exit
     enter mgmt-bootstrap vdp
         enter ipv4 1 default
             set gateway 172.16.0.1
             set ip 172.16.4.219 mask 255.255.0.0
         exit

         enter ipv4 2 default
             set gateway 172.16.0.1
```

```
            set ip 172.16.4.220 mask 255.255.0.0
        exit

        enter ipv4 3 default
            set gateway 172.16.0.1
            set ip 172.16.4.221 mask 255.255.0.0
        exit
 exit
commit-buffer
scope ssa
   scope slot 1
   scope app-instance vdp
   show app-attri
    App Attribute:
        App Attribute Key: cluster-role
        Value: unknown
```

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。

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]

設定（Configure） TLS 暗号化アクセラレーション

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 個 FTD コンテナ インスタンス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注意事項と制限事項

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）
- Single Data Encryption Standard (single 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。

- Block
- 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が、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（Inherit default action）
- Do not decrypt
- Block
- Block with reset

SSL ポリシーの [Undecryptable Actions] の [Handshake Errors] の設定が [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す。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で TLS 暗号化アクセラレーション を有効化

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 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

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 暗号化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）] タブ 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、ASA をトランスペアレント モードに変換し、インターフェイス コンフィギュレーションを変更し、既存の論理デバイスで他のタスクを実行できます。

アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

手順

ステップ 1 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 asa1
Connecting to asa(asa1) 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
- FTD：**exit** と入力
- vDP：**Ctrl-], .** と入力

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次のように入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

論理デバイスの削除

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 シャーシ上の論理デバイスの詳細を表示します。

Firepower /ssa # **show logical-device**

ステップ 3 削除する論理デバイスごとに、次のコマンドを入力します。

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

ステップ 4 論理デバイスにインストールされているアプリケーションの詳細を表示します。

Firepower /ssa # **show app-instance**

ステップ 5 削除するアプリケーションごとに、次のコマンドを入力します。

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*
c) Firepower /ssa/slot # **exit**

ステップ 6 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

例

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Operational State        Template Name
    ---------- ----------- ---------- ---------- ------------------------ -------------
    FTD                    1,2,3      Clustered  Ok                       ftd
Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance
Application Name     Slot ID     Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                              1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                              2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                              3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

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、**show cluster info** コマンドを使用してアプリケーション内のクラスタ ステータスを確認します。

```
ciscoasa# show cluster info
```

```
Clustering is not enabled
```

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：FXOS CLI で、次の例を参照してください。

  ```
  Firepower-chassis# scope ssa
  Firepower-chassis /ssa # scope slot 1
  Firepower-chassis /ssa/slot # scope app-instance asa asa1
  Firepower-chassis /ssa/slot/app-instance # disable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

  再度有効にするには、次の手順を実行します。

  ```
  Firepower-chassis /ssa/slot/app-instance # enable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

- セキュリティ モジュール/エンジン のシャットダウン：FXOS CLI で、次の例を参照してください。

  ```
  Firepower-chassis# scope service-profile server 1/1
  Firepower-chassis /org/service-profile # power down soft-shut-down
  Firepower-chassis /org/service-profile* # commit-buffer
  Firepower-chassis /org/service-profile #
  ```

  電源を投入するには、次の手順を実行します。

  ```
  Firepower-chassis /org/service-profile # power up
  Firepower-chassis /org/service-profile* # commit-buffer
  ```

```
Firepower-chassis /org/service-profile #
```

- シャーシのシャットダウン：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

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：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- 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が尋ねられます。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 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 インストール済みアプリケーションの詳細を表示します。

Firepower /ssa # **show app-instance**

ステップ 3 削除するアプリケーションごとに、次のコマンドを入力します。

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*

c) Firepower /ssa/slot # **exit**

ステップ 4 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

例

```
Firepower# scope ssa
Firepower /ssa* # show app-instance
Application Name     Slot ID     Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                              1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                              2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                              3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

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、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、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- クラスタリングまたは高可用性のため、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 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

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

ステップ 3 論理デバイスに新しいインターフェイスを割り当てます。

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

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 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

ステップ 5 FMC でインターフェイスを同期します。

a) FMC にログインします。
b) **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択し、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) [保存（Save）] をクリックします。

h) [展開（Deploy）] をクリックし、割り当て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 6 FXOS で、論理デバイスからインターフェイスの割り当てを解除します。

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

show external-port-link コマンドを入力して、インターフェイス名を表示します。

ステップ 7 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

ステップ 8 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、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 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 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

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

ステップ 3 論理デバイスからインターフェイスの割り当てを解除します。

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

show external-port-link コマンドを入力して、インターフェイス名を表示します。

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

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

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

ステップ 5 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

論理デバイスのモニタリング

- **show app**

  使用可能なイメージを表示します。

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

```
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes
```

- **show app-instance**

  アプリケーション インスタンスのステータスと情報を表示します。

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup
 Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ----------- ------------ --------------- ------------
ftd        LD1        1          Enabled     Online           6.4.0.10353
6.4.0.10353     Container   Default-Small Not Applicable  None
ftd        LD2        1          Enabled     Online           6.4.0.10353
6.4.0.10353     Container   Default-Small Not Applicable  None
ftd        LD3        1          Enabled     Online           6.4.0.10353
6.4.0.10353     Container   Default-Small Not Applicable  None
ftd        LD4        1          Enabled     Online           6.4.0.10353
6.4.0.1056      Container   Default-Small Not Applicable  None
```

- **show logical-device**

  論理デバイスの詳細を表示します。

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Oper State               Template
Name
    ---------- ----------- ---------- ---------- ----------------------- -------------

    asa1                   1          Standalone Ok                      asa
```

- **show resource-profile system**

  vDP のリソース プロファイルを表示します。

```
Firepower# scope ssa
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical
Core Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
        4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

        6          24576 Yes             System
```

```
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

       10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
        2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
        4          16384 No              System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

        8          32768 No              System
```

- **show resource-profile user-defined**

  コンテナ インスタンスのリソース プロファイル割り当てを表示します。

```
Firepower# scope ssa
Firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6              low end device
gold                 No               14             highest
silver               No               8              mid-level
```

- **show resource detail**

  アプリケーション インスタンスのリソース割り当てを表示します。

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
    Allocated Core NR: 10
    Allocated RAM (MB): 32413
    Allocated Data Disk (MB): 49152
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

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の導入を示します。

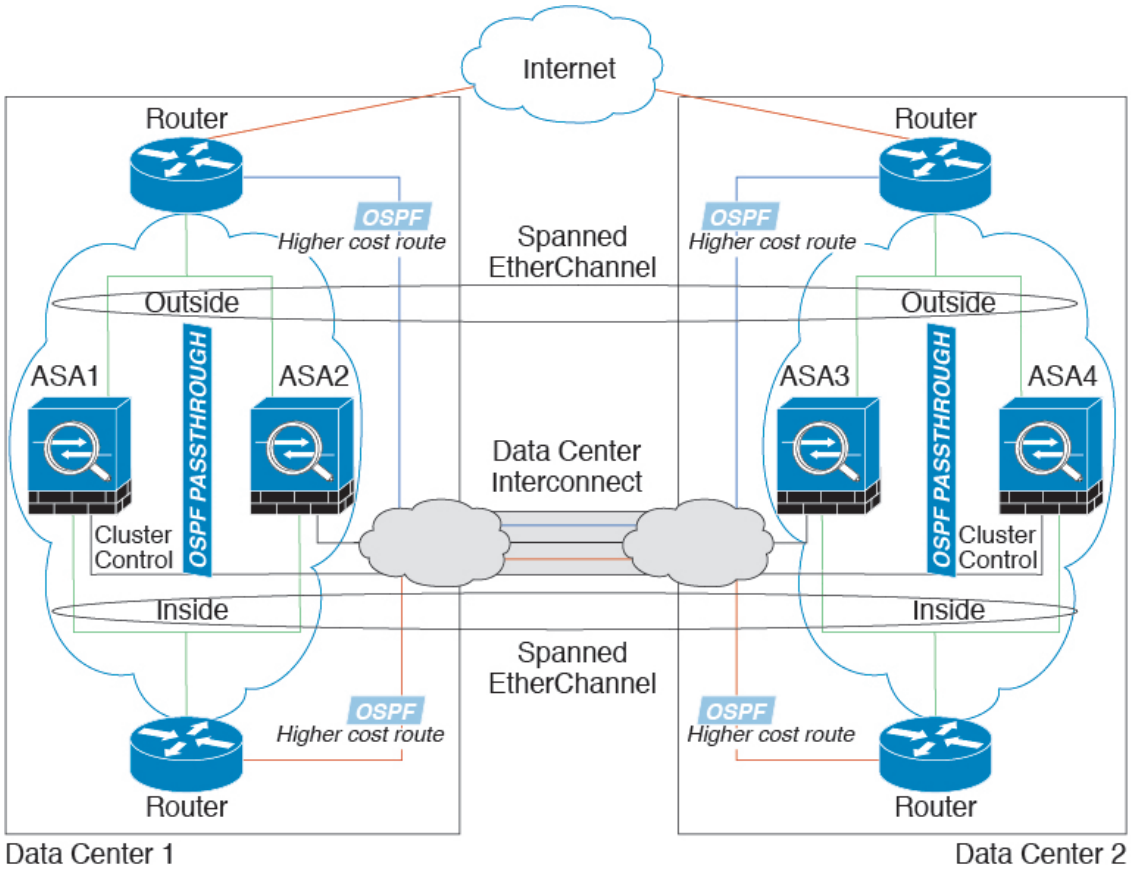
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

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 メンバがある場合を示します。クラスタ メンバは、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ー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 に高コストルートを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：スイッチ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。

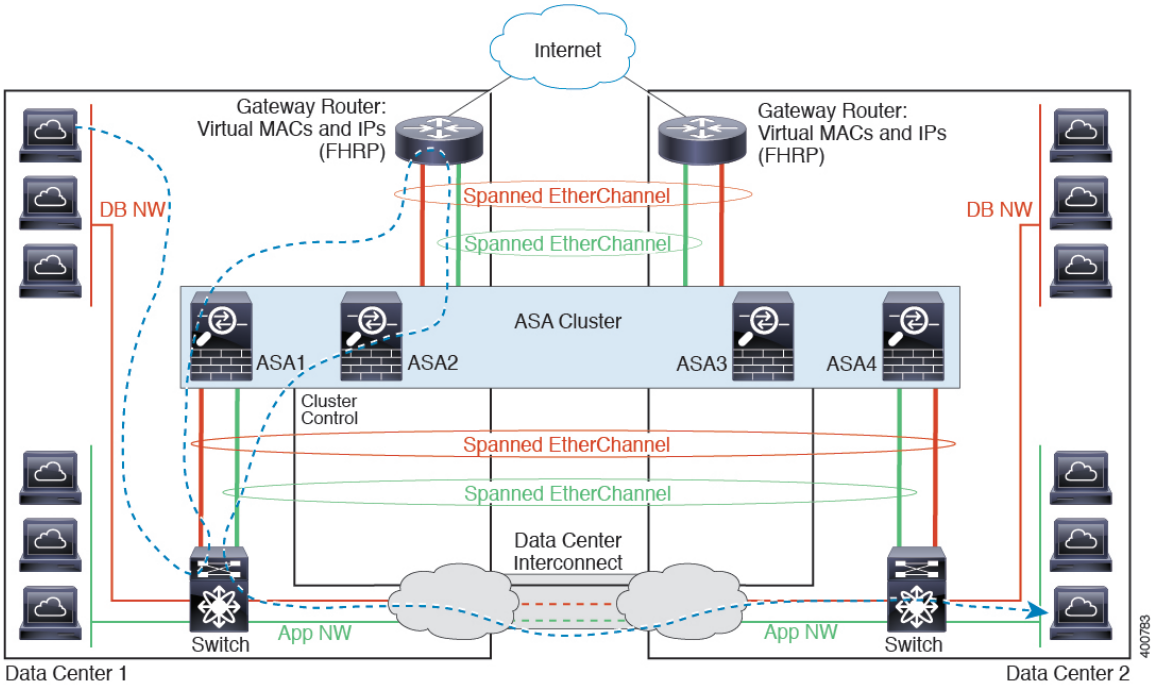


スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

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 メンバがある場合を示します。クラスタ メンバは、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シにスパンされます。

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。予期せぬ MAC アドレスのフラッピングを避けるために推奨されている方法は **mac-address-table static** *outside_interface mac_address* コマンドを使用して、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です。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 （100 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	Firepower 4115、4125、および 4145 が導入されました。 （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。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	2.6.1	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。 （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。 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。 変更されたコマンドはありません。
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	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。 （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。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
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	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。 新しい/変更された画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** > **[Firepower Management Center NAT ID]** フィールド
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	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。 新規/変更されたコマンド：**config hwCrypto enable**、**show hwCrypto**

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
		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 インスタンスのみ展開できました。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。 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 コアの数を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。 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。 （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

機能名	プラットフォーム リリース	機能情報
		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。 （注） FTD バージョン 6.3 以降が必要です。 新規/変更された FXOS コマンド：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**createresource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** 新規/変更された [Firepower Management Center] 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ

機能名	プラットフォーム リリース	機能情報
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	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。 新規/変更されたコマンド：**enter bootstrap-key FIREWALL_MODE**、**set value routed**、**set value transparent**
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	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。 新規/変更されたコマンド： **set cluster-control-link network**

機能名	プラットフォーム リリース	機能情報
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	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。 新規/変更されたコマンド： **enter bootstrap-key NAT_ID**
ASA のサイト間クラスタリングの改善	2.1(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は、ASA アプリケーション内でサイト ID を設定する必要がありました。この新機能により初期展開が簡単になります。ASA 構成内でサイト ID を設定することはできない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。 **set site-id** コマンドが変更されました

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。
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。 次のコマンドが導入されました。**enter mgmt-bootstrap ftd**、**enter bootstrap-key FIREPOWER_MANAGER_IP**、**enter bootstrap-key FIREWALL_MODE**、**enter bootstrap-key-secret REGISTRATION_KEY**、**enter bootstrap-key-secret PASSWORD**、**enter bootstrap-key FQDN**、**enter bootstrap-key DNS_SERVERS**、**enter bootstrap-key SEARCH_DOMAINS**、**enter ipv4 firepower**、**enter ipv6 firepower**、**set value**、**set gateway**、**set ip**、**accept-license-agreement**
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。

機能名	プラットフォーム リリース	機能情報
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。 **enter cluster-bootstrap**、**enter logical-device clustered**、**set chassis-id**、**set ipv4 gateway**、**set ipv4 pool**、**set ipv6 gateway**、**set ipv6 pool**、**set key**、**set mode spanned-etherchannel**、**set port-type cluster**、**set service-type**、**set virtual ipv4**、**set virtual ipv6** コマンドを導入しました