



Firepower 4100/9300 の論理デバイス

Firepower 4100/9300 は柔軟なセキュリティプラットフォームが1つまたは複数の論理デバイスをインストールすることができます。Threat Defense を Management Center に追加する前に、シャーシインターフェイスを設定し、論理デバイスを追加し、Secure Firewall Chassis Manager または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。この章では、基本的なインターフェイスの設定、および Secure Firewall Chassis Manager を使用したスタンドアロンまたはハイアベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、「[Firepower 4100/9300 のクラスタリング](#)」を参照してください。FXOS CLI を使用するには、FXOS CLI コンフィギュレーションガイドを参照してください。高度なFXOSの手順とトラブルシューティングについては、『FXOS 構成ガイド』を参照してください。

- [インターフェイスについて \(1 ページ\)](#)
- [論理デバイスについて \(19 ページ\)](#)
- [コンテナ インスタンスのライセンス \(29 ページ\)](#)
- [論理デバイスの要件と前提条件 \(30 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(38 ページ\)](#)
- [インターフェイスの設定 \(42 ページ\)](#)
- [論理デバイスの設定 \(48 ページ\)](#)
- [論理デバイスの履歴 \(62 ページ\)](#)

インターフェイスについて

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

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または シャーシマネージャによって、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表

示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

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

FirePOWER connect local-mgmt

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

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



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

インターフェイスタイプ

物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel (ポートチャネル) インターフェイスは、次のいずれかのタイプになります。

- **Data** : 通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスと通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- **Data-sharing** : 通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス (脅威に対する防御 Management Center 専用) で共有できます。各コンテナインスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、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、パッシブインターフェイス、クラスター、またはフェールオーバーリンクではサポートされません。
- **Mgmt** : アプリケーションインスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。

す。個別のシャーシ管理インターフェイスについては、[シャーシ管理インターフェイス \(1 ページ\)](#) を参照してください。



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

- **Eventing** : Management Center デバイスを使用した脅威に対する防御のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、脅威に対する防御 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。詳細については、[管理センター構成ガイド](#) を参照してください。Eventing インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の論理デバイスと通信することはできません。後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。



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

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

- **Cluster** : クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用できるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Device Manager および CDO はクラスタリングをサポートしていません。



(注) この章では、**FXOS VLAN** サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、[FXOS インターフェイスとアプリケーションインターフェイス \(5 ページ\)](#) を参照してください。

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

表 1: インターフェイスタイプのサポート

アプリケーション	データ	データ： サブインターフェイス	データ共有	データ共有： サブインターフェイス	管理	イベント (Eventing)	クラスタ (EtherChannelのみ)	クラスタ： サブインターフェイス
Threat Defense	スタンドアロンネイティブインスタンス	対応	—	—	—	対応	対応	—
	スタンドアロンコンテナインスタンス	対応	対応	対応	対応	対応	—	—
	クラスタネイティブインスタンス	対応 (シャージ間クラスタ専用の EtherChannel)	—	—	—	対応	対応	対応
	クラスタコンテナインスタンス	対応 (シャージ間クラスタ専用の EtherChannel)	—	—	—	対応	対応	対応

アプリケーション		データ	データ : サブインターフェイス	データ共有	データ共有 : サブインターフェイス	管理	イベント (Eventing)	クラスタ (EtherChannel のみ)	クラスタ : サブインターフェイス
ASA	スタンドアロンネイティブインスタンス	対応	—	—	—	対応	—	対応	—
	クラスタネイティブインスタンス	対応 (シャリシ間クラスタ専用の EtherChannel)	—	—	—	対応	—	対応	—

FXOS インターフェイスとアプリケーションインターフェイス

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

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

VLAN サブインターフェイス

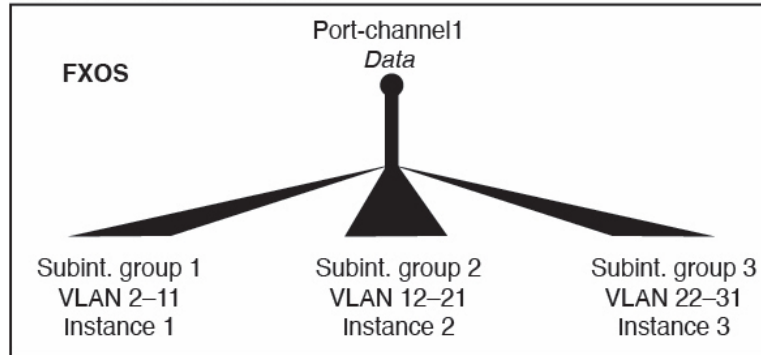
すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

スタンドアロンモードのコンテナインスタンスの場合のみ、FXOS で VLAN サブインターフェイスを作成することもできます。マルチインスタンスクラスタは、クラスタタイプのインターフェイスを除いて、FXOS のサブインターフェイスをサポートしません。アプリケーション定義のサブインターフェイスは、FXOS 制限の対象にはなりません。サブインターフェイスを作成するオペレーティングシステムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイスグループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しま

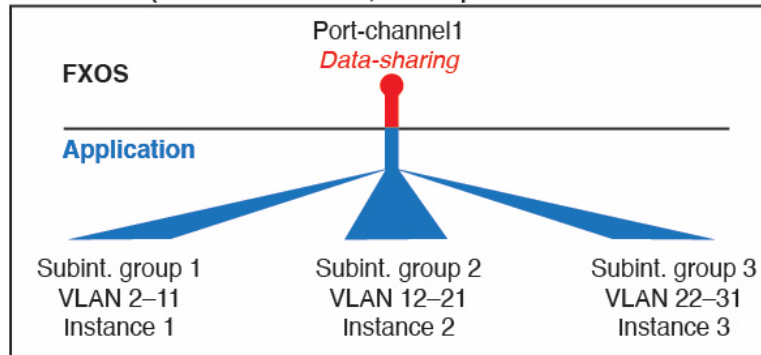
すが、これはお勧めしません。このシナリオを実現する3つの方法については、次の図を参照してください。

図 1: FXOS の VLAN とコンテナインスタンスのアプリケーション

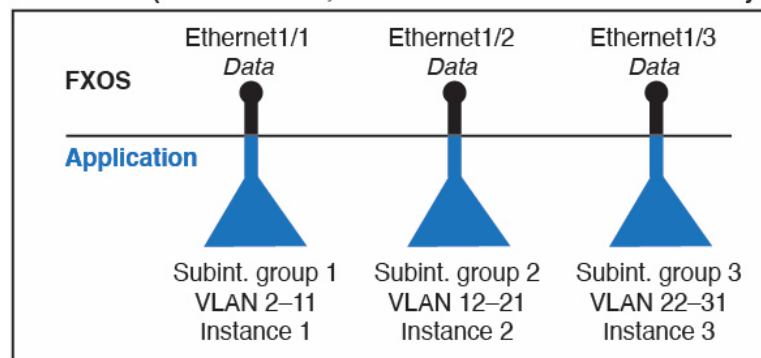
Scenario 1 (recommended)



Scenario 2 (not recommended, worse performance)



Scenario 3 (recommended, but lacks EtherChannel redundancy)



シャーシとアプリケーションの独立したインターフェイスの状態

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

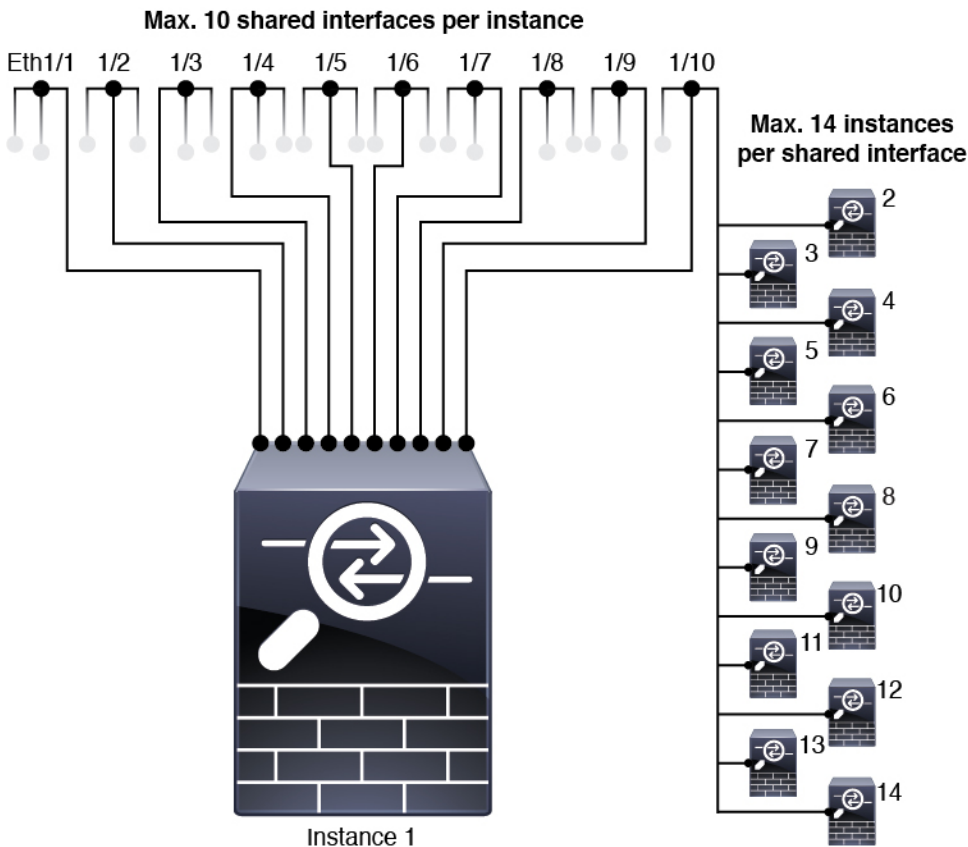
アプリケーション内のインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、アプリケーション内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

インスタンスは、データ共有タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャースは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャース内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャースは VLAN サブインターフェイスの転送用に VLAN グループテーブルも保持します。最大 500 個の VLAN サブインターフェイスを作成できます。

共有インターフェイスの割り当てに次の制限を参照してください。



共有インターフェイスのベストプラクティス

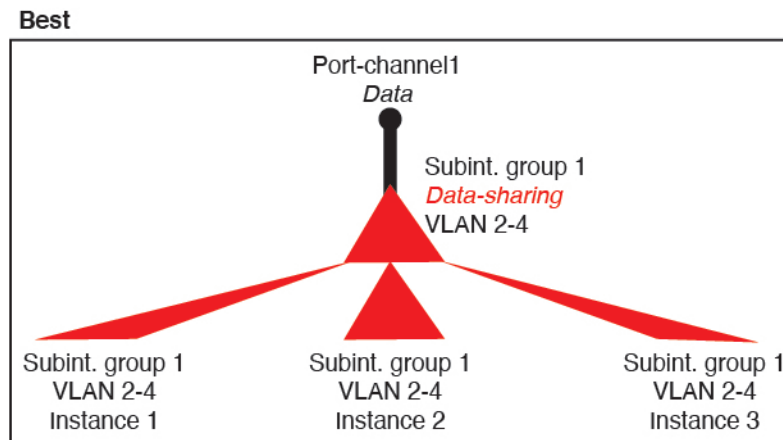
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナインスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性の高いものから低いものの順に次の手順を実行します。

1. 最適：単一の親の下のサブインターフェイスを共有し、インスタンスグループと同じサブインターフェイスのセットを使用します。

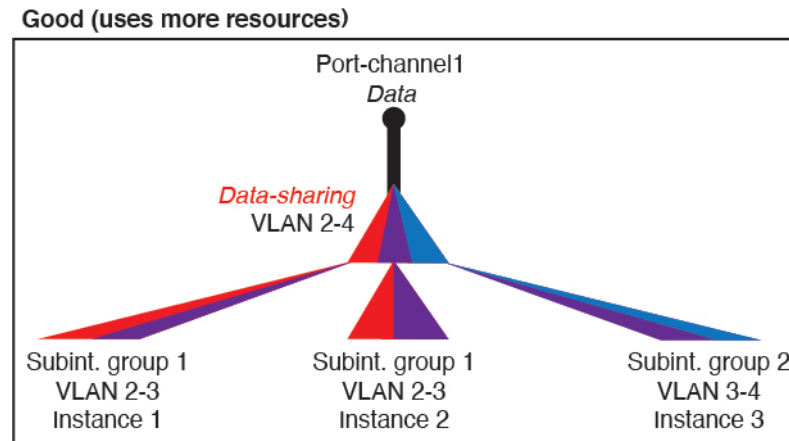
たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.2、3、4）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループテーブルの拡張性は転送テーブルよりも優れています。

図 2: 最適：単一の親のサブインターフェイスグループを共有



インスタンスグループと同じサブインターフェイスのセットを共有しない場合は、（VLAN グループよりも）より多くのリソースを設定で使用するようになる可能性があります。たとえば、Port-Channel1.2 および 3 をインスタンス 1 および 2 と共有するとともに Port-Channel1.3 および 4 をインスタンス 3 と共有する（2つの VLAN グループ）のではなく、Port-Channel1.2、3、および 4 をインスタンス 1、2、および 3 と共有（1つの VLAN グループ）します。

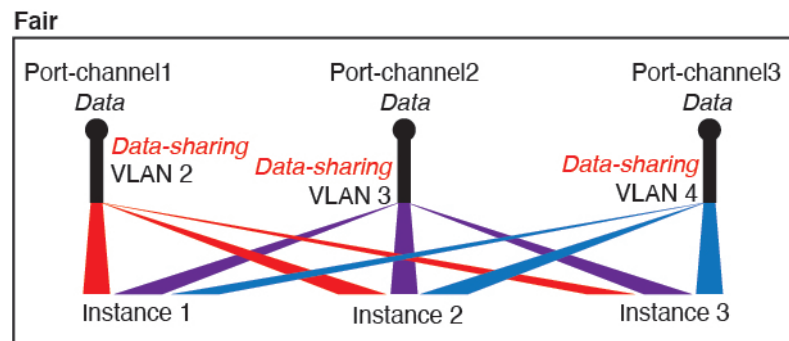
図 3: 良好: 単一の親の複数のサブインターフェイスグループを共有



2. 普通: 親の間でサブインターフェイスを共有します。

たとえば、Port-Channel2、Port-Channel4、およびPort-Channel4ではなく、Port-Channel1.2、Port-Channel2.3、およびPort-Channel3.4を共有します。この使用法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLANグループを利用しています。

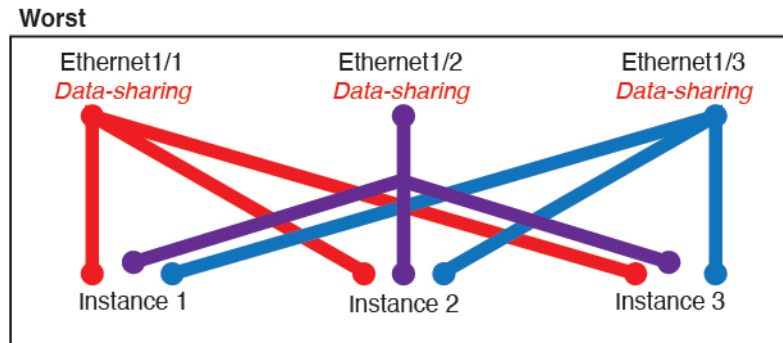
図 4: 普通: 個別の親のサブインターフェイスを共有



3. 最悪: 個々の親インターフェイス（物理または EtherChannel）を共有します。

この方法は、最も多くの転送テーブルエントリを使用します。

図 5: 最悪: 親インターフェイスを共有



共有インターフェイスの使用状況の例

インターフェイスの共有と拡張性の例について、以下の表を参照してください。以下のシナリオは、すべてのインスタンス間で共有されている管理用の1つの物理/EtherChannel インターフェイスと、ハイアベイラビリティで使用する専用のサブインターフェイスを含むもう1つの物理/EtherChannel インターフェイスを使用していることを前提としています。

- 表 2: 3 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス (11 ページ)
- 表 3: 3 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス (13 ページ)
- 表 4: 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス (15 ページ)
- 表 5: 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス (17 ページ)

3 つの SM-44 と firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 9300 の SM-44 セキュリティモジュールに適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 2: 3つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
32 : • 8 • 8 • 8 • 8	0	4 : • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30 : • 15 • 15	0	2: • インスタンス 1 • インスタンス 2	14%
14 : • 14 (各 1)	1	14 : • インスタンス 1-イン スタンス 14	46 %
33 : • 11 (各 1) • 11 (各 1) • 11 (各 1)	3 : • 1 • 1 • 1	33 : • インスタンス 1-イン スタンス 11 • インスタンス 12 - イン スタンス 22 • インスタンス 23 - イン スタンス 33	98%
33 : • 11 (各 1) • 11 (各 1) • 12 (各 1)	3 : • 1 • 1 • 1	34 : • インスタンス 1-イン スタンス 11 • インスタンス 12 - イン スタンス 22 • インスタンス 23 - イン スタンス 34	102 % 許可しない
30 : • 30 (各 1)	1	6 : • インスタンス 1-イン スタンス 6	25 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
30 : <ul style="list-style-type: none"> • 10 (各 5) • 10 (各 5) • 10 (各 5) 	3 : <ul style="list-style-type: none"> • 1 • 1 • 1 	6 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 2 • インスタンス 2-インスタンス 4 • インスタンス 5-インスタンス 6 	23 %
30 : <ul style="list-style-type: none"> • 30 (各 6) 	2	5 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 5 	28%
30 : <ul style="list-style-type: none"> • 12 (各 6) • 18 (各 6) 	4 : <ul style="list-style-type: none"> • 2 • 2 	5 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 2 • インスタンス 2-インスタンス 5 	26 %
24 : <ul style="list-style-type: none"> • 6 • 6 • 6 • 6 	7	4 : <ul style="list-style-type: none"> • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4 	44 %
24 : <ul style="list-style-type: none"> • 12 (各 6) • 12 (各 6) 	14 : <ul style="list-style-type: none"> • 7 • 7 	4 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 2 • インスタンス 2-インスタンス 4 	41%

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 9300 上の 3 つの SM-44 セキュリティモジュールに適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブル リソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 3: 3つの SM-44 を備えた Firepower 9300 上の 1つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
168 : • 168 (4 ea.)	0	42 : • インスタンス 1 - インスタンス 42	33%
224 : • 224 (16 ea.)	0	14 : • インスタンス 1 - インスタンス 14	27 %
14 : • 14 (各 1)	1	14 : • インスタンス 1 - インスタンス 14	46 %
33 : • 11 (各 1) • 11 (各 1) • 11 (各 1)	3 : • 1 • 1 • 1	33 : • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70 : • 70 (5 ea.)	1	14 : • インスタンス 1 - インスタンス 14	46 %
165 : • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.)	3 : • 1 • 1 • 1	33 : • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
70 : • 70 (5 ea.)	2	14 : • インスタンス 1 - インスタンス 14	46 %
165 : • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.)	6 : • 2 • 2 • 2	33 : • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%
70 : • 70 (5 ea.)	10	14 : • インスタンス 1 - インスタンス 14	46 %
165 : • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.)	30 : • 10 • 10 • 10	33 : • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	102 % 許可しない

1 つの SM 44 を備えた Firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 1 つの SM-44 を備えた Firepower 9300 に適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 4:1つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
32 : • 8 • 8 • 8 • 8	0	4 : • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	16 %
30 : • 15 • 15	0	2: • インスタンス 1 • インスタンス 2	14%
14 : • 14 (各 1)	1	14 : • インスタンス 1-イン スタンス 14	46 %
14 : • 7 (各 1) • 7 (各 1)	2: • 1 • 1	14 : • インスタンス 1-イン スタンス 7 • インスタンス 8-イン スタンス 14	37 %
32 : • 8 • 8 • 8 • 8	1	4 : • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	21 %
32 : • 16 (各 8) • 16 (各 8)	2	4 : • インスタンス 1-イン スタンス 2 • インスタンス 3-イン スタンス 4	20 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
32 : • 8 • 8 • 8 • 8	2	4 : • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	25 %
32 : • 16 (各 8) • 16 (各 8)	4 : • 2 • 2	4 : • インスタンス 1-インスタンス 2 • インスタンス 3-インスタンス 4	24 %
24 : • 8 • 8 • 8	8	3 : • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10 : • 10 (各 2)	10	5 : • インスタンス 1-インスタンス 5	69%
10 : • 6 (各 2) • 4 (各 2)	20 : • 10 • 10	5 : • インスタンス 1-インスタンス 3 • インスタンス 4-インスタンス 5	59%
14 : • 12 (2 ea.)	10	7 : • インスタンス 1-インスタンス 7	109% 許可しない

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 1 つの SM-44 を備えた Firepower 4150 に適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイス

スを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

1つのSM-44を備えたFirepower 9300は、最大14のインスタンスをサポートできます。

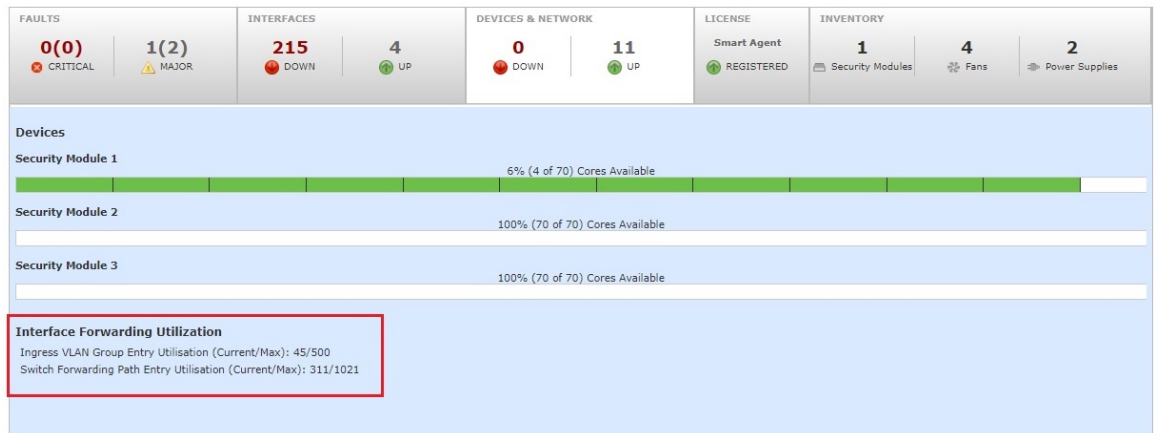
表 5: 1つのSM-44を備えたFirepower 9300上の1つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
112 : • 112 (各 8)	0	14 : • インスタンス 1-インスタンス 14	17%
224 : • 224 (16 ea.)	0	14 : • インスタンス 1-インスタンス 14	17%
14 : • 14 (各 1)	1	14 : • インスタンス 1-インスタンス 14	46 %
14 : • 7 (各 1) • 7 (各 1)	2: • 1 • 1	14 : • インスタンス 1-インスタンス 7 • インスタンス 8-インスタンス 14	37 %
112 : • 112 (各 8)	1	14 : • インスタンス 1-インスタンス 14	46 %
112 : • 56 (各 8) • 56 (各 8)	2: • 1 • 1	14 : • インスタンス 1-インスタンス 7 • インスタンス 8-インスタンス 14	37 %
112 : • 112 (各 8)	2	14 : • インスタンス 1-インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
112 : ・ 56 (各 8) ・ 56 (各 8)	4 : ・ 2 ・ 2	14 : ・ インスタンス 1-インスタンス 7 ・ インスタンス 8-インスタンス 14	37 %
140 : ・ 140 (各 10)	10	14 : ・ インスタンス 1-インスタンス 14	46 %
140 : ・ 70 (各 10) ・ 70 (各 10)	20 : ・ 10 ・ 10	14 : ・ インスタンス 1-インスタンス 7 ・ インスタンス 8-インスタンス 14	37 %

共有インターフェイス リソースの表示

転送テーブルと VLAN グループの使用状況を表示するには、[デバイスとネットワーク (Devices & Network)] > [インターフェイス転送の使用率 (Interface Forwarding Utilization)] エリアを参照します。次に例を示します。



Threat Defense のインラインセット リンク ステート伝達サポート

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバ

イスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

脅威に対する防御 アプリケーションでインラインセットを設定し、リンク ステート伝達を有効にすると、脅威に対する防御 はインラインセット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インラインインターフェイス ペアの2番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンク ステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、シャーシからリンク ステートの変更が伝達されるまで最大4秒かかります。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルーターが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。



(注) 同じインラインセットに対してハードウェア バイパス およびリンクステートの伝達を有効にしないでください。

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 脅威に対する防御 のいずれか) および1つのオプション デコレータ アプリケーション (Radware DefensePro) を実行し、サービスチェーンを形成できます。

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



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

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- **スタンドアロン** : スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- **クラスタ** : クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性 (管理、ネットワークへの統合) を提供し、同時に複数デバ

イスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールがネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。Device Manager はクラスタリングをサポートしていません。

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 Management Center を使用する 脅威に対する防御 でのみサポートされています。ASA または Device Manager を使用する 脅威に対する防御 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、および脅威に対する防御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。脅威に対する防御ではマルチコンテキストモードは使用できません。

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。マルチインスタンスクラスタは、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。クラスタ制御リ

リンクは例外で、クラスター EtherChannel のサブインターフェイスを使用できます。共有インターフェイスの拡張性 (7 ページ) およびコンテナ インスタンスの VLAN サブインターフェイスの追加 (46 ページ) を参照してください。



- (注) 本書では、FXOS VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、FXOS インターフェイスとアプリケーション インターフェイス (5 ページ) 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。



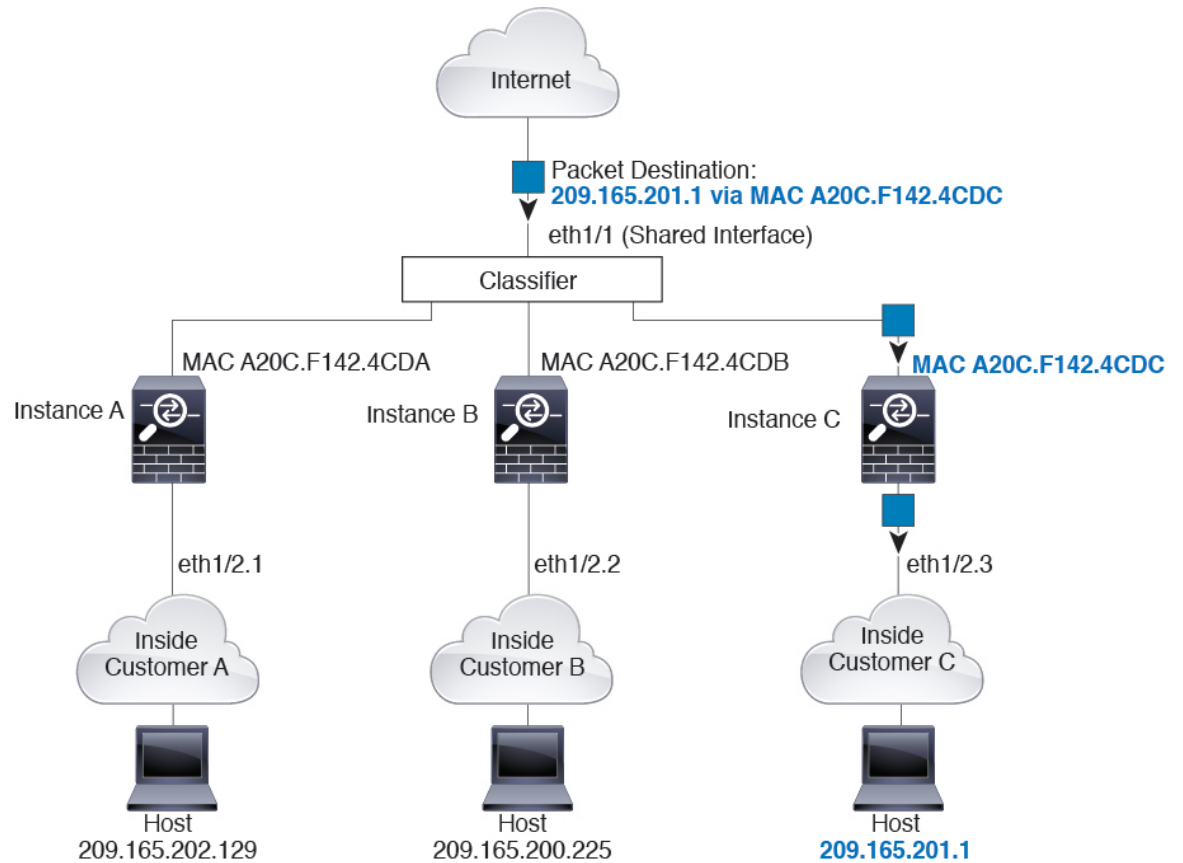
- (注) 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製されて各インスタンスに送信されます。

分類例

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

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。

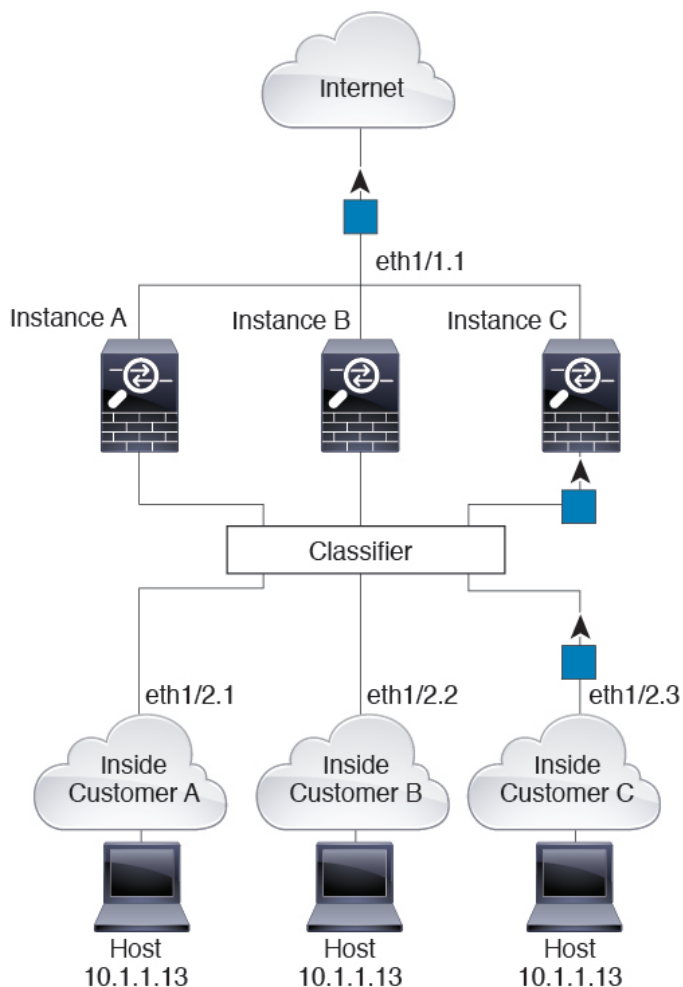
図 6: MAC アドレスを使用した共有インターフェイスのパケット分類



内部ネットワークからの着信トラフィック

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。

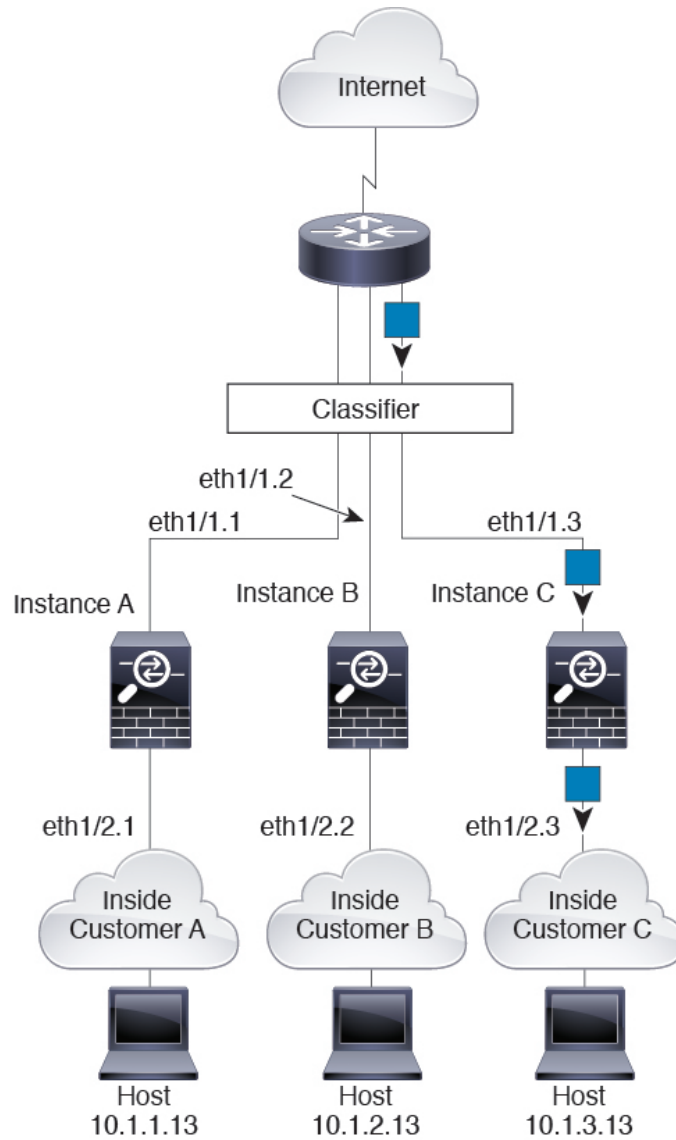
図 7: 内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォール インスタンス

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のホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンスCに割り当てられているためです。

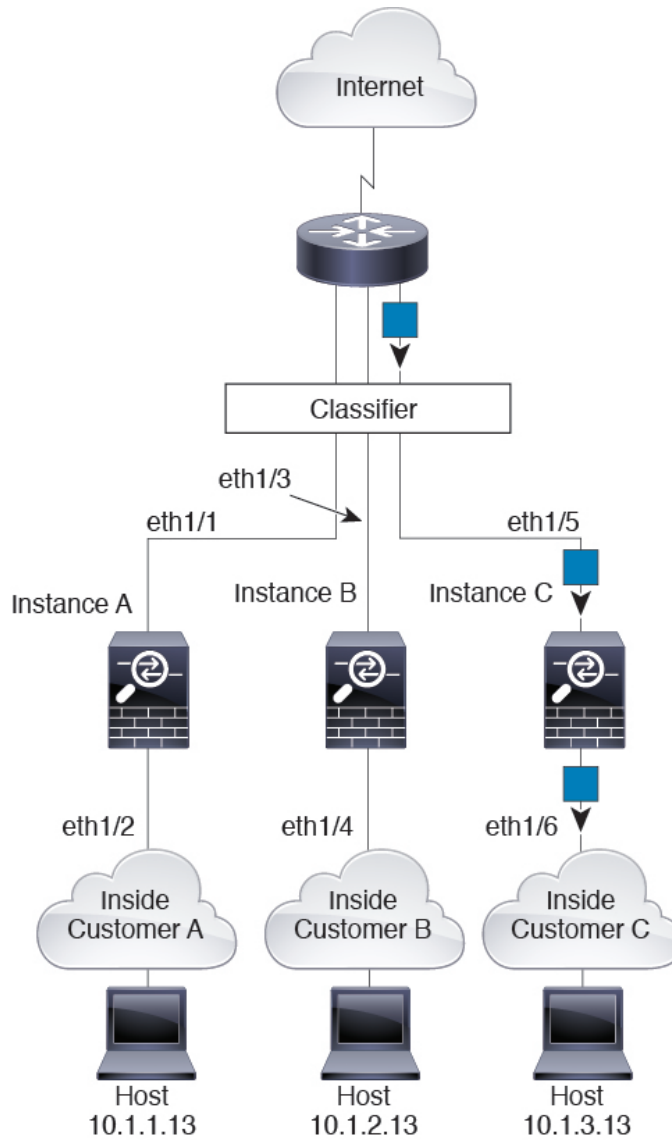
図 8: トランスペアレントファイアウォールインスタンス



インラインセット

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

図 9: インラインセット

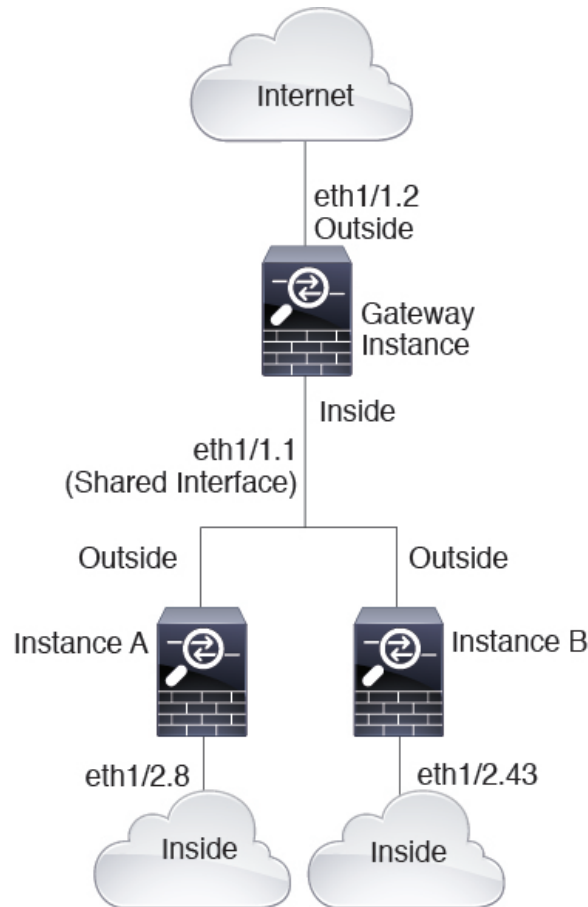


コンテナ インスタンスのカスケード

別のインスタンスの前にインスタンスを直接配置することをインスタンスのカスケードと呼びます。一方のインスタンスの外部インターフェイスは、もう一方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 10: インスタンスのカスケード



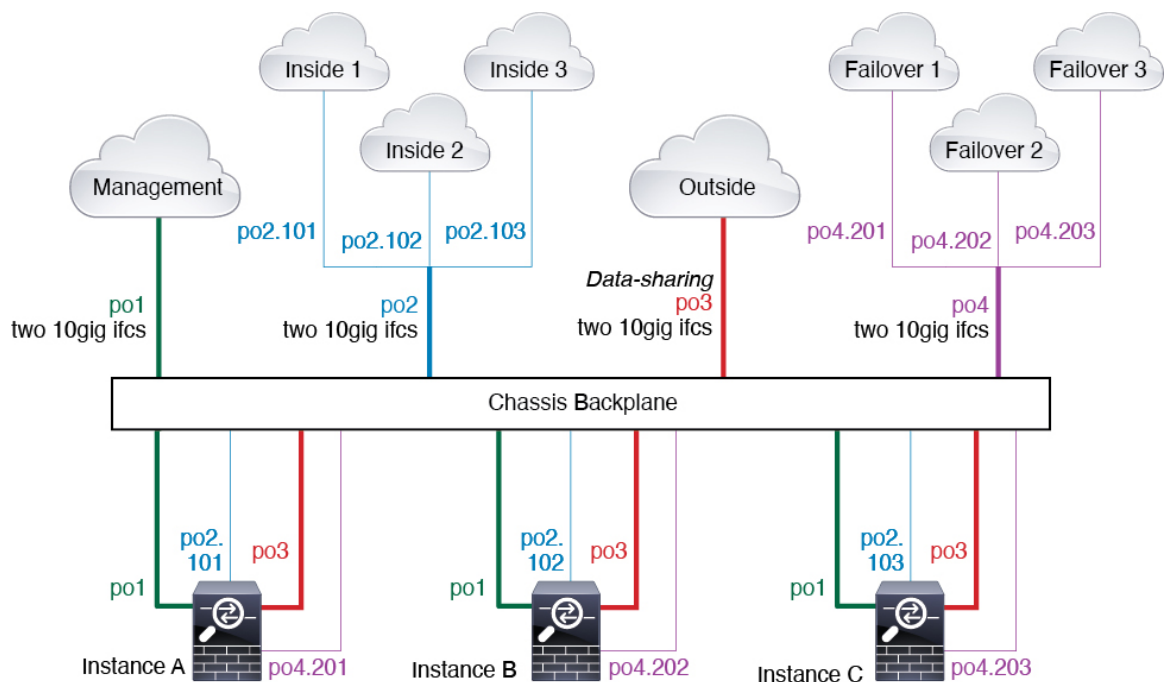
(注) 高可用性を備えたカスケードインスタンス（共有インターフェイスを使用）を使用しないでください。フェールオーバーが発生し、スタンバイユニットが再参加すると、MAC アドレスが一時的に重複し、停止が発生する可能性があります。代わりに、外部スイッチを使用してゲートウェイインスタンスと内部インスタンスに一意的なインターフェイスを使用して、それらのインスタンス間でトラフィックを渡す必要があります。

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ンネル1インターフェイス（管理タイプ）を使用します。この EtherChannel には2つの10ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ管理ネットワークで一意的な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外部ネットワークで一意的な 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

シャーシは、各インスタンスの共有インターフェイスが一意的な MAC アドレスを使用するように、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。

インスタンス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、インスタンス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 で始まり、アドレスが重複するリスクがあるため、手動 MAC アドレスの先頭は A2 にしないでください。

シャーシは、次の形式を使用して MAC アドレスを生成します。

A2xx.yyyz.zzzz

xx.yy はユーザー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。

ユーザー定義のプレフィックスは、16 進数に変換される整数です。ユーザー定義のプレフィックスの使用方法を示す例を挙げます。プレフィックスとして 77 を指定すると、シャーシは 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 (xyyy)。

A24D.00zz.zzzz

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

A2F1.03zz.zzzz

コンテナインスタンスのリソース管理

コンテナインスタンスごとのリソース使用率を指定するには、FXOS で 1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。モデルごとに使用可能なリソースを表示するには、[コンテナインスタンスの要件と前提条件 \(32 ページ\)](#) を参照してください。リソース プロファイルを追加するには、[コンテナインスタンスにリソースプロファイルを追加 \(48 ページ\)](#) 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スループット（接続数、VPN セッション数、および TLS プロキシセッション数）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）。複数のインスタンスを使用する場合は、インスタンスに割り当てる CPU コアの割合に基づいてスループットを計算する必要があります。たとえば、コアの 50% でコンテナインスタンスを使用する場合は、最初にスループットの 50% を計算する必要があります。さらに、コンテナインスタンスで使用可能なスループットは、ネイティブインスタンスで使用可能なスループットよりも低い場合があります。

インスタンスのスループットを計算する方法の詳細については、<https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html> を参照してください。

コンテナインスタンスおよびハイ アベイラビリティ

2 つの個別のシャーシでコンテナインスタンスを使用してハイ アベイラビリティを使用できます。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。

詳細な要件については、「[ハイアベイラビリティの要件と前提条件 \(33 ページ\)](#)」と「[ハイアベイラビリティペアの追加 \(56 ページ\)](#)」を参照してください。

コンテナインスタンスおよびクラスタリング

セキュリティモジュール/エンジンごとに1つのコンテナインスタンスを使用して、コンテナインスタンスのクラスタを作成できます。詳細な要件については、[クラスタリングの要件と前提条件 \(34 ページ\)](#) を参照してください。

コンテナインスタンスのライセンス

すべてのライセンスがコンテナインスタンスごとではなく、セキュリティエンジン/シャーシ (Firepower 4100 の場合) またはセキュリティモジュール (Firepower 9300 の場合) ごとに使用されます。次の詳細情報を参照してください。

- Essentialsライセンスがセキュリティモジュール/エンジンごとに1つ自動的に割り当てられます。
- 機能ライセンスは各インスタンスに手動で割り当てますが、セキュリティモジュール/エンジンにつき機能ごとに1つのライセンスのみを使用します。たとえば、3つのセキュリティモジュールを搭載した Firepower 9300 の場合、使用中のインスタンスの数に関係なく、モジュールにつき1つの URL フィルタリングライセンスが必要で、合計3つのライセンスが必要になります。

次に例を示します。

表 6: Firepower 9300 のコンテナインスタンスのサンプルライセンスの使用状況

Firepower 9300	インスタンス	ライセンス
セキュリティモジュール 1	インスタンス 1	Essentials、URL フィルタリング、マルウェア防御
	インスタンス 2	Essentials、URL フィルタリング
	インスタンス 3	Essentials、URL フィルタリング
セキュリティモジュール 2	インスタンス 4	Essentials、IPS
	インスタンス 5	Essentials、URL フィルタリング、マルウェア防御、IPS

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 3	インスタンス 6	Essentials、マルウェア防御、IPS
	インスタンス 7	Essentials、IPS

表 7: ライセンスの総数

Essentials	URL フィルタリング	マルウェア防御	IPS
3	2	3	2

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。

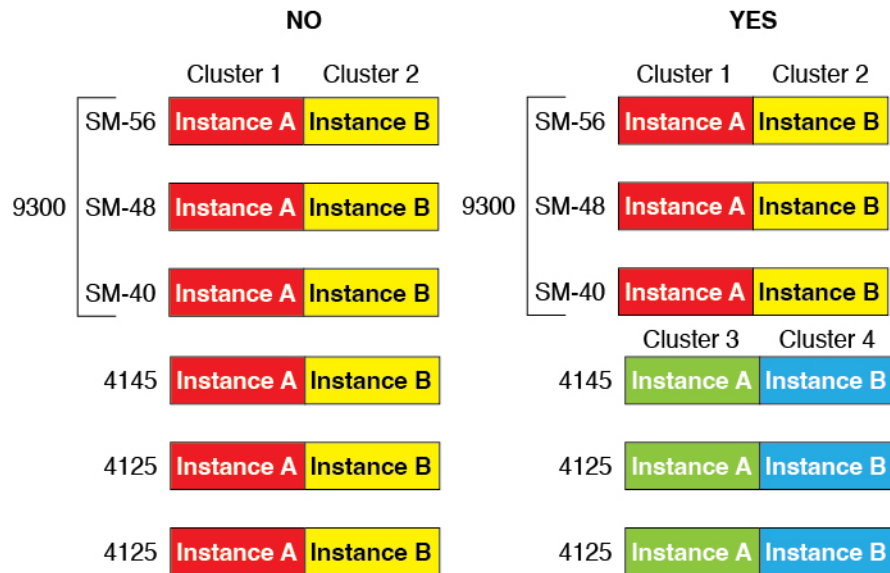
ハードウェアとソフトウェアの組み合わせの要件と前提条件

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-48 をモジュール 1、SM-40 をモジュール 2、SM-56 をモジュール 3 としてインストールできます。
- **ネイティブインスタンスのクラスタリング** : 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-40 を、シャーシ 2 に 3 つの SM-40 をインストールできます。同じシャーシに 1 つの SM-48 および 2 つの SM-40 をインストールする場合、クラスタリングは使用できません。
- **コンテナインスタンスのクラスタリング** : 異なるモデルタイプのインスタンスを使用してクラスタを作成できます。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。ただし、同じクラスタ内に Firepower 9300 と Firepower 4100 を混在させることはできません。



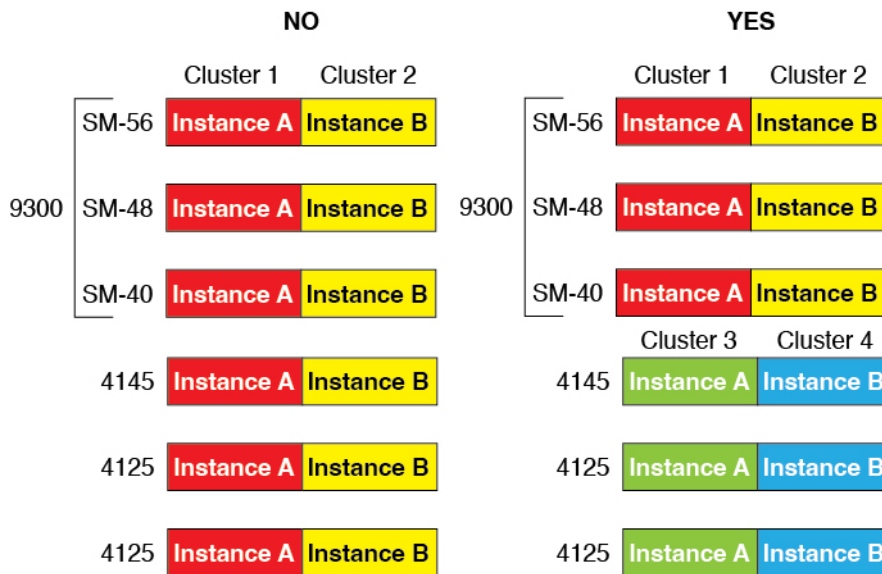
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-40、SM-48、および SM-56 があります。SM-40 モジュール間、SM-48 モジュール間、および SM-56 モジュール間にハイアベイラビリティペアを作成できます。
- ASA および Threat Defense のアプリケーションタイプ：異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモジュール 2 に ASA をインストールし、モジュール 3 に Threat Defense をインストールすることができます。
- ASA または Threat Defense のバージョン：個別のモジュールで異なるバージョンのアプリケーションインスタンスタイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に Threat Defense 6.3 を、モジュール 2 に Threat Defense 6.4 を、モジュール 3 に Threat Defense 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。
- ネイティブインスタンスのクラスタリング：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。
- コンテナインスタンスのクラスタリング：異なるモデルタイプのインスタンスを使用してクラスタを作成できます。たとえば、Firepower 4145 および 4125 のインスタンスを使用し

て1つのクラスタを作成できます。ただし、同じクラスタ内に Firepower 9300 と Firepower 4100 を混在させることはできません。



- 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 Threat Defense のアプリケーションタイプ：Firepower 4100 は、1つのアプリケーションタイプのみを実行できます。
- Threat Defense 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脅威に対する防御を個別のコンテナインスタンスとして実行できます。

コンテナインスタンスの要件と前提条件

マルチインスタンスでのハイアベイラビリティまたはクラスタリングの要件については、「[ハイアベイラビリティの要件と前提条件 \(33 ページ\)](#)」および「[クラスタリングの要件と前提条件 \(34 ページ\)](#)」を参照してください。

サポートされるアプリケーションタイプ

- Threat Defense Management Center を使用

最大コンテナインスタンスとモデルあたりのリソース

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あたり 40 GB に設定されます。

表 8: モデルごとの最大コンテナ インスタンス数とリソース

モデル	最大コンテナ インスタンス 数	使用可能な CPU コア	使用可能な RAM	使用可能なディスクス ペース
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 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 9300 SM-40 セキュリ ティ モジュール	13	78	334 GB	1359 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

Management Center の要件

Firepower 4100 シャーシまたは Firepower 9300 モジュール上のすべてのインスタンスに対して、ライセンスの実装のために同じ Management Center を使用する必要があります。

ハイアベイラビリティの要件と前提条件

- ハイアベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
 - 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
 - 同じモデルであること。
 - 高可用性論理デバイスに同じインターフェイス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、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。

- コンテナインスタンスでは、各装置で同じリソースプロファイル属性を使用する必要があります。
- コンテナインスタンス向け：高可用性を備えたカスケードインスタンス（共有インターフェイスを使用）を使用しないでください。フェールオーバーが発生し、スタンバイユニットが再参加すると、MAC アドレスが一時的に重複し、停止が発生する可能性があります。代わりに、外部スイッチを使用してゲートウェイインスタンスと内部インスタンスに一意のインターフェイスを使用して、それらのインスタンス間でトラフィックを渡す必要があります。
- 他のハイアベイラビリティシステム要件については、[高可用性のシステム要件](#)を参照してください。

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

Threat Defense は、次のモデルでのクラスタリングをサポートしています。

- Firepower 9300：クラスタには最大 16 ノードを含めることができます。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てすることができます。複数のシャーシによるクラスタリングと、1 つのシャーシ内のセキュリティモジュールに分離されたクラスタリングがサポートされます。
- Firepower 4100：複数のシャーシでクラスタリングを使用して、最大 16 ノードがサポートされます。

ユーザの役割

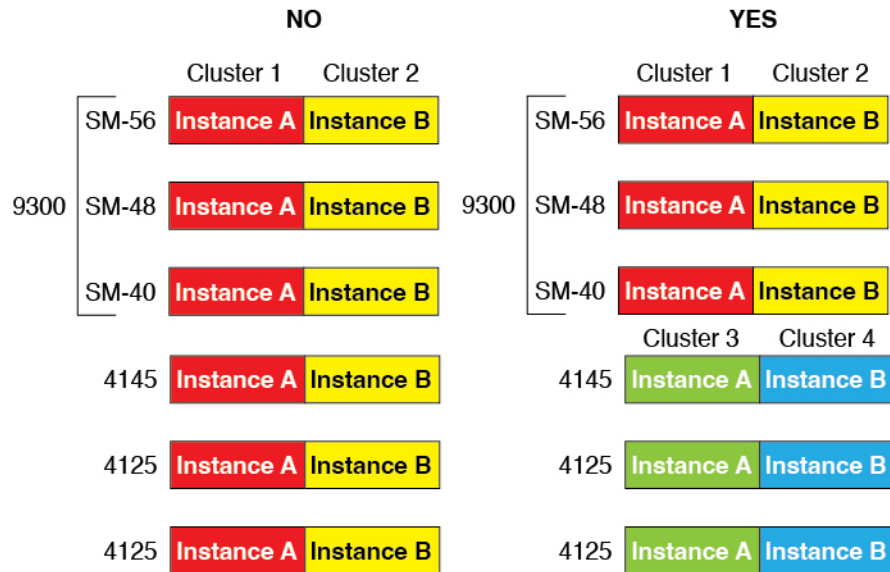
- 管理者
- アクセス管理者
- ネットワーク管理者

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：

- ネイティブインスタンスのクラスタリング—Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティモジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。

- コンテナインスタンスのクラスタリング—クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することをお勧めします。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティモジュールタイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。

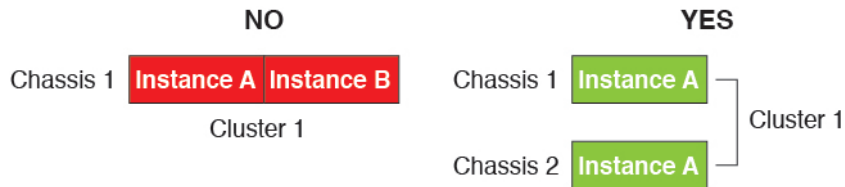


- イメージアップグレード時を除き、同じ FXOS およびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- 同じ管理インターフェイス、EtherChannel、アクティブインターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュールタイプを使用できます。複数のシャーシによるクラスタでは、すべてのデータインターフェイスを EtherChannel にする必要のあることに注意してください。
(インターフェイスモジュールの追加や削除、または 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 (データノードから始めて、制御ノードで終わります)。
- 同じ NTP サーバを使用する必要があります。脅威に対する防御では、Management Center も同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。

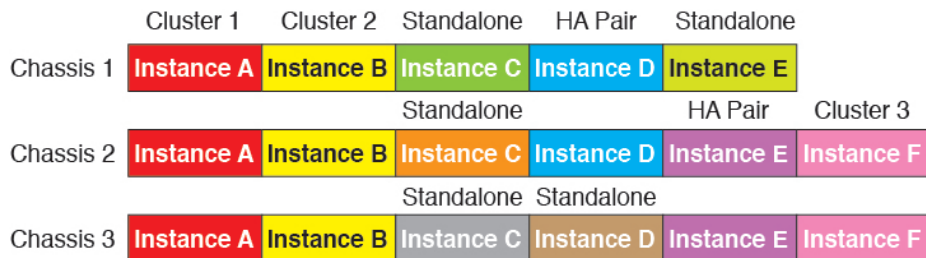
マルチインスタンス クラスタリングの要件

- セキュリティモジュール/エンジン間クラスタリングなし：特定のクラスタでは、セキュリティモジュール/エンジンごとに 1 つのコンテナインスタンスのみを使用できます。同

じモジュール上で実行されている場合、同じクラスタに2つのコンテナインスタンスを追加することはできません。



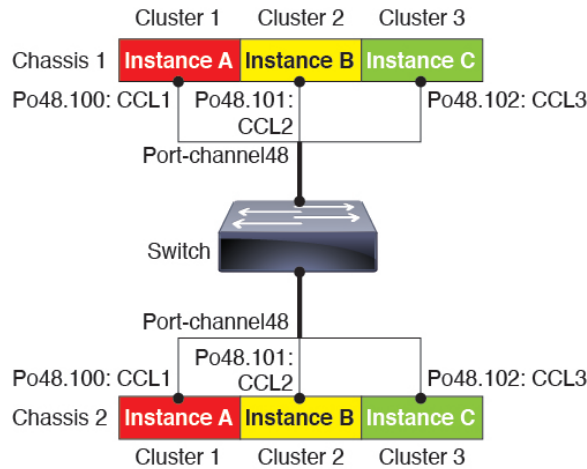
- クラスタとスタンドアロンインスタンスの混在：セキュリティモジュール/エンジン上のすべてのコンテナインスタンスがクラスタに属している必要はありません。一部のインスタンスをスタンドアロンノードまたは高可用性ノードとして使用できます。また、同じセキュリティモジュール/エンジン上で別々のインスタンスを使用して複数のクラスタを作成することもできます。



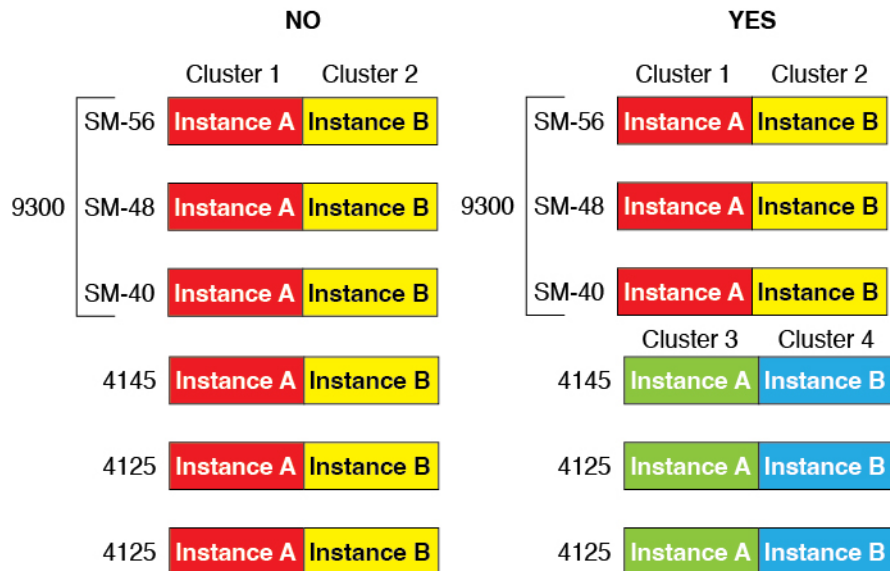
- Firepower 9300の3つすべてのモジュールはクラスタに属している必要があります。Firepower 9300の場合、クラスタには3つすべてのモジュールで1つのコンテナインスタンスが必要です。たとえば、モジュール1と2のインスタンスを使用してクラスタを作成し、モジュール3のネイティブインスタンスを使用することはできません。



- リソースプロファイルの一致：クラスタ内の各ノードで同じリソースプロファイル属性を使用することを推奨します。ただし、クラスタノードを別のリソースプロファイルに変更する場合、または異なるモデルを使用する場合は、リソースの不一致が許可されます。
- 専用クラスタ制御リンク：複数のシャーンによるクラスタの場合、各クラスタには専用のクラスタ制御リンクが必要です。たとえば、各クラスタは、同じクラスタタイプのEtherChannelで個別のサブインターフェイスを使用したり、個別のEtherChannelを使用したりできます。



- 共有インターフェイスなし：共有タイプのインターフェイスは、クラスタリングではサポートされません。ただし、同じ管理インターフェイスとイベントインターフェイスを複数のクラスタで使用することはできます。
- サブインターフェイスなし：マルチインスタンスクラスタは、FXOS 定義の VLAN サブインターフェイスを使用できません。クラスタ制御リンクは例外で、クラスタ EtherChannel のサブインターフェイスを使用できます。
- シェアードモデルの混在：クラスタインスタンスごとに同じセキュリティモジュールまたはシェアードモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティモジュールタイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。たとえば、Firepower 9300 SM-56、SM-48、および SM-40 のインスタンスを使用して 1 つのクラスタを作成できます。または、Firepower 4145 および 4125 でクラスタを作成できます。



- 最大 6 ノード：クラスタ内では最大 6 つのコンテナインスタンスを使用できます。

スイッチ要件

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

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

インターフェイスに関する注意事項と制約事項

VLAN サブインターフェイス

- 本書では、FXOS VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、[FXOS インターフェイスとアプリケーションインターフェイス \(5 ページ\)](#) を参照してください。
- サブインターフェイス（および親インターフェイス）はコンテナインスタンスにのみ割り当てることができます。



(注) コンテナインスタンスに親インターフェイスを割り当てる場合、タグなし（非 VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。クラスタタイプのインターフェイスの場合、親インターフェイスを使用することはできません。

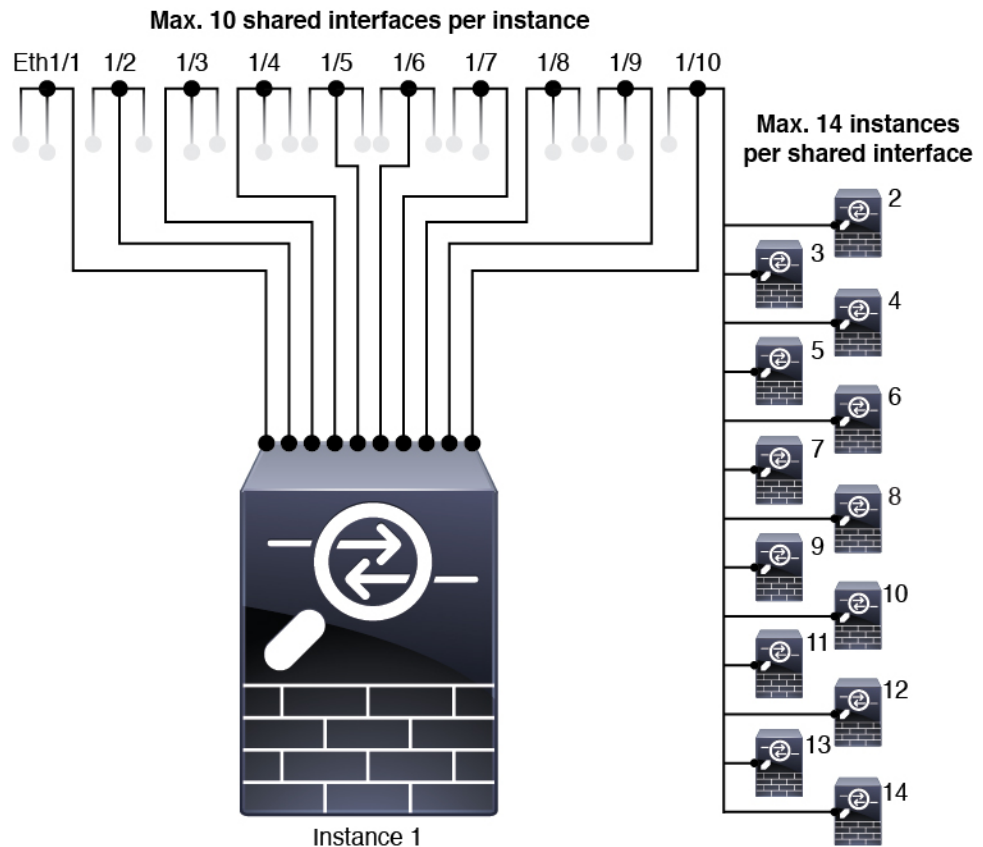
- サブインターフェイスはデータまたはデータ共有タイプのインターフェイス、およびクラスタタイプのインターフェイスでサポートされます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。
- マルチインスタンス クラスタリングの場合、データインターフェイス上の FXOS サブインターフェイスはサポートされません。ただし、クラスタ制御リンクではサブインターフェイスがサポートされているため、クラスタ制御リンクには専用の EtherChannel または EtherChannel のサブインターフェイスを使用できます。アプリケーション定義のサブインターフェイスは、データインターフェイスでサポートされていることに注意してください。
- 最大 500 個の VLAN ID を作成できます。

- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
 - 脅威に対する防御 インラインセットに、またはパッシブ インターフェイスとしてサブインターフェイスを使用することはできません。
 - フェールオーバーリンクに対してサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバーリンクとしての使用が制限されます。一部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、一部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。

データ共有インターフェイス

- ネイティブインスタンスでは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。
- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance1 ~ Instance14 に Ethernet1/1 を割り当てることができます。

インスタンスごとの最大共有インターフェイス数：10 たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- クラスタでは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。

- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
 - トランスペアレント ファイアウォール モード デバイスで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。
 - 脅威に対する防御 インラインセットでまたはパッシブ インターフェイスとして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。
 - フェールオーバーリンクに対して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。

次に対するインラインセット Threat Defense

- 物理インターフェイス（通常かつブレイクアウトポート）と Etherchannel のサポート。サブインターフェイスはサポートされません。
- リンク ステータスの伝達はサポートされます。
- 同じインラインセットに対して ハードウェア バイパス およびリンク状態の伝達を有効にしないでください。

ハードウェア バイパス

- 脅威に対する防御 をサポート。ASA の通常のインターフェイスとして使用できます。
- 脅威に対する防御 はインラインセットでのみハードウェア バイパス をサポートします。
- ハードウェア バイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできません。
- ハードウェア バイパス インターフェイスを EtherChannel に含めたり、ハードウェア バイパス 用に使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。
- ハードウェア バイパス は高可用性ではサポートされません。
- 同じインラインセットに対して ハードウェア バイパス およびリンク状態の伝達を有効にしないでください。

デフォルトの MAC アドレス

ネイティブインスタンス向け：

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

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワーク

アプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

コンテナインスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定する場合、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。[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 \(27 ページ\)](#) 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

脅威に対する防御のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。

ハイ アベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。データ共有インターフェイスはサポートされていません。

マルチインスタンス

- コンテナインスタンスによる複数インスタンス機能は Management Center を使用する 脅威に対する防御 に対してのみ使用できます。
- 脅威に対する防御 コンテナ インスタンスの場合、1 つの 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。
- 脅威に対する防御 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。
 - Radware DefensePro リンク デコレータ
 - Management Center UCAPL/CC モード
 - ハードウェアへのフローオフロード

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、インターフェイスプロパティを編集できます。



インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスは無効になっています。VLAN サブインターフェイスの場合、管理状態は親インターフェイスから継承されます。



手順

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

[インターフェイス (Interface)] ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

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

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

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

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

物理インターフェイスの設定

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



- (注) QSFPH40G-CUxM の場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。

始める前に

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

手順

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

[All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの行で[編集 (Edit)] をクリックし、[インターフェイスを編集 (Edit Interface)] ダイアログボックスを開きます。

ステップ 3 インターフェイスを有効にするには、[有効化 (Enable)] チェックボックスをオンにします。インターフェイスを無効化するには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ (Type)] を選択します。

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

- **データ**
 - [データ共有 (Data-sharing)] : コンテナインスタンスのみ。
- **管理**
 - [Firepower-eventing] : 脅威に対する防御のみ。
 - [クラスタ (Cluster)] : [クラスタ (Cluster)] タイプは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャンネル 48 に自動的に作成されます。

ステップ 5 (任意) [速度 (Speed)] ドロップダウンリストからインターフェイスの速度を選択します。

ステップ 6 (任意) インターフェイスで [自動ネゴシエーション (Auto Negotiation)] がサポートされている場合は、[はい (Yes)] または [いいえ (No)] オプション ボタンをクリックします。

ステップ 7 (任意) [Duplex] ドロップダウンリストからインターフェイスのデュプレックスを選択します。

ステップ 8 (任意) **デバウンス時間 (ミリ秒)** を明示的に設定します。0 から 15000 ミリ秒の値を入力します。

ステップ 9 [OK] をクリックします。

EtherChannel (ポートチャネル) の追加

EtherChannel (ポートチャネルとも呼ばれる) は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ (銅と光ファイバ) の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量 (1GB インターフェイスと 10GB インターフェイスなど) を混在させることはできません。リンク集約制御プロトコル (LACP) では、2 つのネットワークデバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。



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

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバーインターフェイスの両端が正しいチャネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

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

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

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

手順

- ステップ 1** [インターフェイス (Interfaces)] を選択して、[インターフェイス (Interfaces)] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** インターフェイス テーブルの上にある [ポート チャネルの追加 (Add Port Channel)] をクリックし、[ポート チャネルの追加 (Add Port Channel)] ダイアログボックスを開きます。
- ステップ 3** [ポート チャネル ID (Port Channel ID)] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ~ 47 です。
- クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。
- ステップ 4** ポート チャネルを有効にするには、[有効化 (Enable)] チェックボックスをオンにします。ポート チャネルを無効化するには、[Enable] チェックボックスをオフにします。
- ステップ 5** インターフェイスの [タイプ (Type)] を選択します。
- インターフェイスタイプの使用方法の詳細については、[インターフェイス タイプ \(2 ページ\)](#) を参照してください。
- データ
 - [データ共有 (Data-sharing)] : コンテナインスタンスのみ。
 - 管理
 - [Firepower-eventing] : 脅威に対する防御のみ。
 - クラスタ
- ステップ 6** ドロップダウン リストでメンバーインターフェイスに適した [管理速度 (Admin Speed)] を設定します。
- 指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。
- ステップ 7** データまたはデータ共有インターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。

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

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

- ステップ 9** ポートチャンネルにインターフェイスを追加するには、[Available Interface] リストでインターフェイスを選択し、[Add Interface] をクリックしてそのインターフェイスを [Member ID] リストに移動します。

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

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。

- ステップ 10** ポートチャンネルからインターフェイスを削除するには、[Member ID] リストでそのインターフェイスの右側にある [Delete] ボタンをクリックします。

- ステップ 11** [OK] をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

ネットワーク配置に応じて、250 ~ 500 の VLAN サブインターフェイスをシャーシに追加できます。シャーシには最大 500 個のサブインターフェイスを追加できます。

マルチインスタンス クラスターリングの場合、クラスタータイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナインスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

本書では、FXOS VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。FXOS サブインターフェイスとアプリケーションサブインターフェイスを使用するタイミングの詳細については、「[FXOS](#)

[インターフェイスとアプリケーション インターフェイス \(5 ページ\)](#)」を参照してください。

手順

ステップ 1 [Interfaces] を選択して [All Interfaces] タブを開きます。

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

ステップ 2 [Add New > Subinterface] をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイスの [タイプ (Type)] を選択します。

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

- データ
- データ共有
- [クラスタ (Cluster)]: クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用できません。

データインターフェイスおよびデータ共有インターフェイスの場合: タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。

ステップ 4 ドロップダウン リストから親インターフェイスを選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できません。

ステップ 5 [Subinterface ID] を 1 ~ 4294967295 で入力します。

この ID は、*interface_id.subinterface_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 1 ~ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開し、その下にあるすべてのサブインターフェイスを表示します。

論理デバイスの設定

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

クラスタリングについては、[Firepower 4100/9300 のクラスタリング](#)を参照してください。

コンテナインスタンスにリソースプロファイルを追加

コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソースプロファイルを作成します。論理デバイス/アプリケーションインスタンスを展開するときに、使用するリソースプロファイルを指定します。リソースプロファイルはCPUコアの数を設定します。RAMはコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに40GBに設定されます。

- コアの最小数は6です。



(注) コア数が少ないインスタンスは、コア数が多いインスタンスよりも、CPU使用率が比較的高くなる場合があります。コア数が少ないインスタンスは、トラフィック負荷の変化の影響を受けやすくなります。トラフィックのドロップが発生した場合には、より多くのコアを割り当ててください。

- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティモジュール/シャーシモデルによって異なります。「[コンテナインスタンスの要件と前提条件（32 ページ）](#)」を参照してください。

シャーシには、「Default-Small」と呼ばれるデフォルトリソースプロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

リソースプロファイルを割り当て後に変更すると、問題が発生します。次のガイドラインを参照してください。

- 使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。
- 脅威に対する防御インスタンスを Management Center に追加した後にリソースプロファイルの設定を変更する場合は、Management Center の [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [システム (System)] > [インベントリ (Inventory)] ダイアログボックスで各ユニットのインベントリを更新します。

- インスタンスに別のプロファイルを割り当てると、再起動します。
- 両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを割り当てる場合、次の手順を実行する必要があります。
 1. ハイアベイラビリティを解除します。
 2. 両方のユニットに新しいプロファイルを割り当てます。
 3. ハイアベイラビリティを再確立します。
- 確立されたクラスタ内のインスタンスに異なるプロファイルを割り当てる場合は、プロファイルが一致する必要がないため、最初に新しいプロファイルをデータノードに適用します。すべてが復帰したら、新しいプロファイルを制御ノードに適用できます。

手順

ステップ 1 [プラットフォーム設定 (Platform Settings)] > [リソースプロファイル (Resource Profiles)] を選択し、[追加 (Add)] をクリックします。

[リソースプロファイルの追加 (Add Resource Profile)] ダイアログボックスが表示されます。

ステップ 2 次のパラメータを設定します。

- [名前 (Name)] : プロファイルの名前を 1 ~ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
- [説明 (Description)] : プロファイルの説明を最大 510 文字で設定します。
- [コア数 (Number of Cores)] : プロファイルのコア数を 6 ~ 最大数 (偶数) で設定します。最大数はシャーシによって異なります。

ステップ 3 [OK] をクリックします。

スタンドアロン Threat Defense の追加

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

一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用できます。

始める前に

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



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

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません (また、[インターフェイス (Interfaces)] タブの上部に [MGMT] として表示されます)。
- 後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。詳細については、[FTD コマンドリファレンスの configure network management-data-interface](#) コマンドを参照してください。
- また、少なくとも1つのデータタイプのインターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック (Web イベントなど) を運ぶ [firepower-eventing](#) インターフェイスも作成できます。詳細については、「[インターフェイス タイプ \(2 ページ\)](#)」を参照してください。
- コンテナインスタンスに対して、デフォルトのプロファイルを使用しない場合は、[コンテナインスタンスにリソースプロファイルを追加 \(48 ページ\)](#) に従ってリソースプロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるようにセキュリティモジュール/エンジンを再度初期化する必要があります。[セキュリティモジュール (Security Modules)] または [セキュリティエンジン (Security Engine)] を選択し、[再初期化 (Reinitialize)] をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスに置き換える場合は、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。
- 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
 - Management Center 選択した IP アドレス/NAT ID

- DNS サーバの IP アドレス
- 脅威に対する防御 ホスト名とドメイン名

手順

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

ステップ 2 [追加 (Add)] > [スタンドアロン (Standalone)] をクリックし、次のパラメータを設定します。

a) デバイス名を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

(注) 論理デバイスの追加後にこの名前を変更することはできません。

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

c) [Image Version] を選択します。

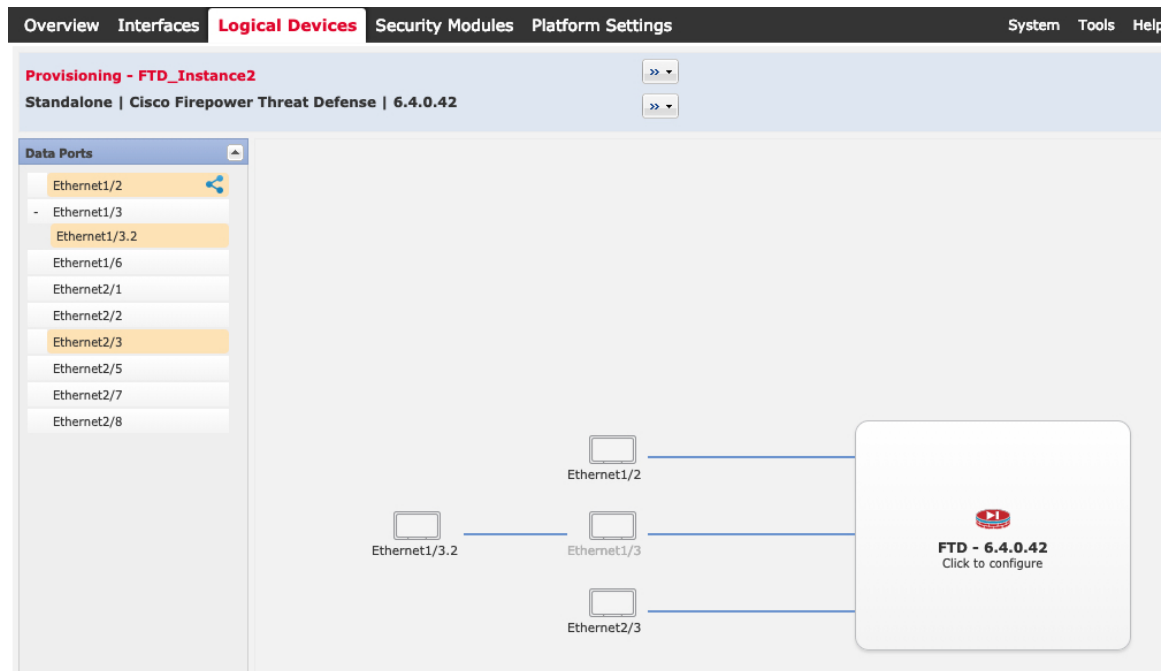
d) [インスタンスタイプ (Instance Type)] : [コンテナ (Container)] または [ネイティブ (Native)] を選択します。

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

e) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[Interfaces] ページでは、以前に有効にしたデータとデータ共有インターフェイスのみを割り当てることができます。後で Management Center のこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

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

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

ステップ 4 画面中央のデバイス アイコンをクリックします。

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

ステップ 5 [一般情報 (General Information)] ページで、次の手順を実行します。

- a) (Firepower 9300 の場合) [セキュリティモジュールの選択 (Security Module Selection)] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。
- b) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後で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、この操作に約 5 分かかることがあります。

(注) 両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを後で割り当てる場合、次の手順を実行する必要があります。

1. ハイアベイラビリティを解除します。
2. 両方のユニットに新しいプロファイルを割り当てます。
3. ハイアベイラビリティを再確立します。

- c) [Management Interface] を選択します。
このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーマン管理ポートとは別のものです。
- d) 管理インターフェイスを選択します。[アドレスタイプ (Address Type)] : [IPv4のみ (IPv4 only)]、[IPv6のみ (IPv6 only)]、または [IPv4およびIPv6 (IPv4 and IPv6)]。
- e) [Management IP] アドレスを設定します。
このインターフェイスに一意の IP アドレスを設定します。
- f) [Network Mask] または [Prefix Length] に入力します。
- g) ネットワーク ゲートウェイ アドレスを入力します。

ステップ 6 [設定 (Settings)] タブで、次の項目を入力します。

The screenshot shows the 'Settings' tab of the 'Cisco Secure Firewall Threat Defense - Bootstrap Configuration' dialog. The fields are as follows:

- Management type of application instance: FMC (dropdown)
- Permit Expert mode for FTD SSH sessions: yes (dropdown)
- Search domains: cisco.com (text)
- Firewall Mode: Routed (dropdown)
- DNS Servers: 10.89.5.67 (text)
- Fully Qualified Hostname: td2.cisco.com (text)
- Password: [Redacted]
- Confirm Password: [Redacted]
- Registration Key: [Redacted]
- Confirm Registration Key: [Redacted]
- CDO Onboard: [Redacted]
- Confirm CDO Onboard: [Redacted]
- Firepower Management Center IP: 10.89.5.35 (text)
- Firepower Management Center NAT ID: test (text)
- Eventing Interface: [Redacted]

- a) ネイティブ インスタンスの場合は、[アプリケーションインスタンスの管理タイプ (Management type of application instance)] ドロップダウン リストで [FMC] を選択します。
 ネイティブインスタンスは、マネージャとしての **Device Manager** もサポートしています。論理デバイスを展開した後にマネージャタイプを変更することはできません。
- b) 管理 Management Center の [Firepower Management Center IP] を入力します。Management Center の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。
- c) **FTD SSH セッションからエキスパート モード**、[Yes]、または [No] 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 脅威に対する防御 シェルからアクセスできます。
 このオプションで [Yes] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ (No)] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザーのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。
 マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパートモードを使用します。このモードを開始するには、脅威に対する防御 CLI で **expert** コマンドを使用します。
- d) カンマ区切りリストとして [検索ドメイン (Search Domains)] を入力します。
- e) [Firewall Mode] を [Transparent] または [Routed] に選択します。

ルーテッドモードでは、脅威に対する防御はネットワーク内のルータホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファ

「ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。

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

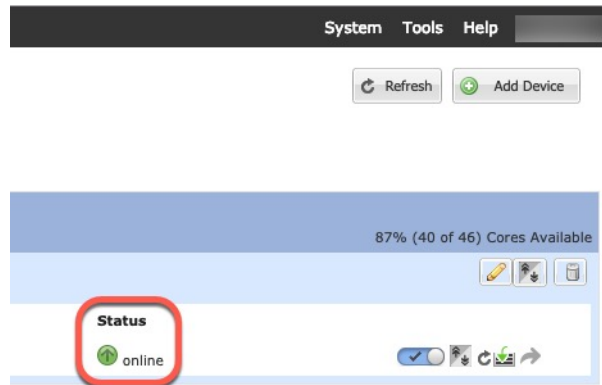
- f) [DNS Servers] をカンマ区切りのリストとして入力します。
たとえば、Management Centerのホスト名を指定する場合、脅威に対する防御はDNSを使用します。
- g) 脅威に対する防御の [Fully Qualified Hostname] を入力します。
- h) 登録時に Management Center とデバイス間で共有する [Registration Key] を入力します。
このキーには、1～37文字の任意のテキスト文字列を選択できます。脅威に対する防御を追加するときに、Management Center に同じキーを入力します。
- i) CLI アクセス用の 脅威に対する防御 管理ユーザの [Password] を入力します。
- j) イベントの送信に使用する [イベントィングインターフェイス (Eventing Interface)] を選択します。指定しない場合は、管理インターフェイスが使用されます。
このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。
- k) コンテナインスタンスの場合は、[ハードウェア暗号化 (Hardware Crypto)] を [有効 (Enabled)] または [無効 (Disabled)] に設定します。
この設定により、ハードウェアのTLS暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。この機能はデフォルトでイネーブルになっています。セキュリティモジュールごとに最大16個のインスタンスについてTLS暗号化アクセラレーションを有効にできます。この機能は、ネイティブインスタンスでは常に有効になっています。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。

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

ステップ8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ9 [保存 (Save)] をクリックします。

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



- ステップ 10** 脅威に対する防御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、Management Center コンフィギュレーションガイドを参照してください。

ハイアベイラビリティペアの追加

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

始める前に

[ハイアベイラビリティの要件と前提条件（33 ページ）](#) を参照してください。

手順

- ステップ 1** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 2** フェールオーバーリンクとステートリンクに1つまたは2つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシの間でハイアベイラビリティトラフィックをやり取りします。統合されたフェールオーバーリンクとステートリンクには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクが帯域幅の大半を必要とします。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。同じネットワークセグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

コンテナインスタンスの場合、フェールオーバーリンク用のデータ共有インターフェイスはサポートされていません。親インターフェイスまたはEtherChannelでサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバーリンクとして使用することをお勧めします。同じ親のすべてのサブインターフェイスをフェールオーバーリ

リンクとして使用する必要があることに注意してください。あるサブインターフェイスをフェールオーバーリンクとして使用する一方で、他のサブインターフェイス（または親インターフェイス）を通常のデータインターフェイスとして使用することはできません。

- ステップ 3** 論理デバイスでハイ アベイラビリティを有効にします。 [ハイ アベイラビリティ](#) を参照してください。
- ステップ 4** ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

Threat Defense 論理デバイスのインターフェイスの変更

脅威に対する防御論理デバイスでは、インターフェイスの割り当てや割り当て解除、または管理インターフェイスの置き換えを行うことができます。その後、Management Center 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、脅威に対する防御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、脅威に対する防御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 Management Center 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 \(42 ページ\)](#) および [EtherChannel \(ポート チャンネル\) の追加 \(44 ページ\)](#) に従ってインターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスまたはイベントインターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータメンバーインターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。Threat Defense デバイスの再起動（管理インターフェイスの変更により再起動）後、Management Center で設定を同期すると、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。

- クラスターリングやハイアベイラビリティのため、Management Center 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。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼさないことに注意してください。
- マルチインスタンスモードでは、サブインターフェイスを同じ VLAN タグを持つ別のサブインターフェイスと変更するには、最初にインターフェイスのすべての設定 (nameif config を含む) を削除してから、シャーシマネージャからインターフェイスの割り当てを解除する必要があります。割り当てが解除されたら、新しいインターフェイスを追加し、Management Center からインターフェイスの同期を使用します。

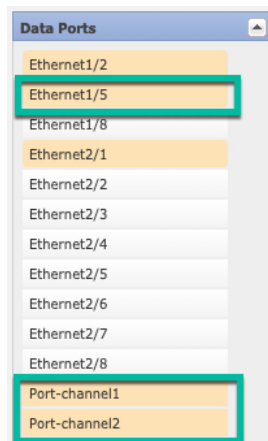
手順

ステップ 1 シャーシマネージャで、[論理デバイス (Logical Devices)] を選択します。

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

ステップ 3 [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

まだインターフェイスを削除しないでください。



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

これらのタイプのインターフェイスでは、変更を保存するとデバイスがリブートします。

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

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

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 Management Center でインターフェイスを同期します。

- a) Management Center にログインします。
- b) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、脅威に対する防御デバイス[編集 (Edit)] (✎) 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インターフェイス設定を手動で転送します。

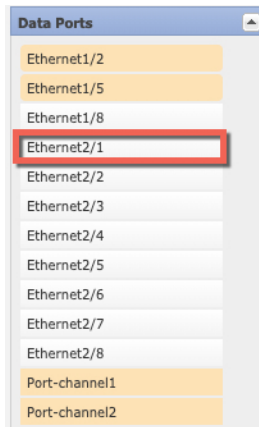
インターフェイスはまだ削除していないため、既存の設定を参照できます。古いインターフェイスを削除して検証を再実行した後も、さらに設定を修正する機会があります。検証を実行すると、古いインターフェイスがまだ使用されているすべての場所が表示されます。

- f) [変更の検証 (Validate Changes)] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

- g) [Save (保存)] をクリックします。
- h) [展開 (Deploy)] > [展開 (Deployment)] をクリックします。
- i) デバイスを選択して [展開 (Deploy)] をクリックし、割り当てられたデバイスにポリシーを展開します。変更はポリシーを導入するまで有効になりません。

ステップ 7 シャーシマネージャ でデータインターフェイスの割り当てを解除するには、[データ ポート (Data Ports)] 領域でそのインターフェイスの選択を解除します。



ステップ 8 [Save] をクリックします。

ステップ 9 Management Center でインターフェイスを再度同期します。

アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

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

connect module slot_number {console | telnet}

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

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

例：

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

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

```
Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd 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 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。

- Threat Defense : 「**exit**」と入力します。

ステップ 4 FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

Telnet セッションを終了します。

a) **Ctrl-],.** と入力

論理デバイスの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	任意 (Any)	<p>シャーシでは、Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Threat Defense アプリケーションインターフェイスの管理状態は考慮されません。Threat Defense からの同期がない場合は、たとえば、Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、Threat Defense が処理できるようになる前に外部ルータが Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。</p> <p>(注) この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する Threat Defense ではサポートされていません。ASA ではサポートされていません。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 : [論理デバイス (Logical Devices)]> [リンク状態の有効化 (Enable Link State)]</p> <p>新規/変更された FXOS コマンド : set link-state-sync enabled、show interface expand detail</p>
コンテナインスタンス向けの Management Center を使用した Threat Defense 設定のバックアップと復元	6.7	任意 (Any)	<p>Threat Defense コンテナインスタンスで Management Center バックアップ/復元ツールを使用できるようになりました。</p> <p>新規/変更された Management Center 画面 : [システム (System)]> [ツール (Tools)]> [バックアップ/復元 (Backup/Restore)]> [管理対象デバイスのバックアップ (Managed Device Backup)]</p> <p>新規/変更された Threat Defense CLI コマンド : restore</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p> <p>(注) FXOS 2.9 が必要です。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
クラスタータイプインターフェイスでの VLAN サブインターフェイスのサポート (マルチインスタンス使用のみ)	6.6	任意 (Any)	<p>マルチインスタンスクラスターで使用するために、クラスタータイプのインターフェイスで VLAN サブインターフェイスを作成できるようになりました。各クラスターには一意のクラスター制御リンクが必要であるため、VLAN サブインターフェイスはこの要件を満たすための簡単な方法を提供します。または、クラスターごとに専用の EtherChannel を割り当てることもできます。複数のクラスターインターフェイスが許可されるようになりました。</p> <p>新規/変更された [Firepower Chassis Manager] 画面： [インターフェイス (Interfaces)] > [すべてのインターフェイス (All Interfaces)] > [新規追加 (Add New)] ドロップダウンメニュー > [サブインターフェイス (Subinterface)] > [タイプ (Type)] フィールド</p> <p>新規/変更された FXOS コマンド：set port-type cluster</p> <p>(注) FXOS 2.8.1 が必要です。</p>
Firepower 4112 上の Threat Defense	6.6	任意 (Any)	<p>Firepower 4112 を導入しました。</p> <p>(注) FXOS 2.8.1 が必要です。</p>
複数のコンテナインスタンスの TLS 暗号化アクセラレーション	6.5	任意 (Any)	<p>Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス (最大 16 個) で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。</p> <p>新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、enter hw-crypto 次に set admin-state enabled FXOS コマンドを使用します。</p> <p>新規/変更された [Firepower Chassis Manager] 画面： [論理デバイス (Logical Devices)] > [デバイスの追加 (Add Device)] > [設定 (Settings)] > の [ハードウェア暗号化 (Hardware Crypto)] ドロップダウンメニュー</p> <p>(注) FXOS 2.7.1 が必要です。</p>
Threat Defense Firepower 4115、4125、および 4145	6.4	任意 (Any)	<p>Firepower 4115、4125、および 4145 が導入されました。</p> <p>(注) FXOS 2.6.1.157 が必要です。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	6.4	任意 (Any)	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) FXOS 2.6.1.157 が必要です。
ASA および Threat Defense を同じ Firepower 9300 の別のモジュールでサポート	6.4	任意 (Any)	ASA および Threat Defense 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 (注) FXOS 2.6.1.157 が必要です。
モジュール/セキュリティエンジンのいずれかの Threat Defense 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	6.4	任意 (Any)	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。 新規/変更された FXOS コマンド : config hwCrypto enable 変更された画面はありません。 (注) FXOS 2.6.1.157 が必要です。

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 4100/9300 の Threat Defense のマルチインスタンス機能	6.3	任意 (Any)	

機能	最小 Management Center	最小 Threat Defense	詳細
			<p>単一のセキュリティエンジンまたはモジュールに、それぞれ Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーションインスタンスを展開するだけでした。</p> <p>柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。</p> <p>2 台の個別のシャーシ上でコンテナインスタンスを使用して高可用性を使用できます。クラスタリングはサポートされません。</p> <p>(注) マルチインスタンス機能は、実装は異なりますが、ASA マルチコンテキストモードに似ています。Threat Defense ではマルチコンテキストモードは使用できません。</p> <p>新規/変更された Management Center 画面：</p> <ul style="list-style-type: none"> • [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 <p>新規/変更された [Firepower Chassis Manager] 画面：</p> <ul style="list-style-type: none"> • [概要 (Overview)]>[デバイス (Devices)] • [インターフェイス (Interfaces)]>[すべてのインターフェイス (All Interfaces)]>[新規追加 (Add New)] ドロップダウンメニュー>[サブインターフェイス (Subinterface)] • [インターフェイス (Interfaces)]>[すべてのインターフェイス (All Interfaces)]>[タイプ (Type)] • [論理デバイス (Logical Devices)]>[デバイスの追加 (Add Device)] • [プラットフォームの設定 (Platform Settings)]>[Mac プール (Mac Pool)] • [プラットフォームの設定 (Platform Settings)]>[リソースのプロファイル (Resource Profiles)] <p>新規/変更された FXOS コマンド：<code>connect ftd name</code>、<code>connect module telnet</code>、<code>create bootstrap-key PERMIT_EXPERT_MODE</code>、<code>createresource-profile</code>、<code>create subinterface</code>、<code>scope auto-macpool</code>、<code>set cpu-core-count</code>、<code>set deploy-type</code>、<code>set port-type data-sharing</code>、<code>set prefix</code>、<code>set resource-profile-name</code>、<code>set vlan</code>、<code>scope app-instance ftd name</code>、<code>show cgroups container</code>、<code>show interface</code>、<code>show mac-address</code>、<code>show</code></p>

機能	最小 Management Center	最小 Threat Defense	詳細
			subinterface、show tech-support module app-instance、show version サポートされるプラットフォーム：Firepower 4100/9300
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	6.3	任意 (Any)	<p>クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID (127.2.chassis_id.slot_id) に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック (127.0.0.0/8) およびマルチキャスト (224.0.0.0/4) アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。</p> <p>新規/変更された [Firepower Chassis Manager] 画面：</p> <ul style="list-style-type: none"> • [論理デバイス (Logical Devices)] > [デバイスの追加 (Add Device)] > [クラスタ情報 (Cluster Information)] > [CCL サブネット IP (CCL Subnet IP)] フィールド <p>新規/変更された FXOS コマンド：set cluster-control-link network</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
オンモードでのデータ EtherChannel のサポート	6.3	任意 (Any)	<p>データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオンモードに設定できるようになりました。Etherchannel の他のタイプはアクティブモードのみをサポートします。</p> <p>新規/変更された [Firepower Chassis Manager] 画面：</p> <ul style="list-style-type: none"> • [インターフェイス (Interfaces)] > [すべてのインターフェイス (All Interfaces)] > [ポートチャネルの編集 (Edit Port Channel)] > [モード (Mode)] <p>新規/変更された FXOS コマンド：set port-channel-mode</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
Threat Defense インラインセットでの EtherChannel のサポート	6.2	任意 (Any)	<p>Threat Defense インラインセットで Etherchannel を使用できるようになりました。</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>

機能	最小 Management Center	最小 Threat Defense	詳細
6 つの Threat Defense モジュールのシャーシ間クラスタリング	6.2	任意 (Any)	<p>Threat Defense のシャーシ間クラスタリングが実現されました。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 :</p> <ul style="list-style-type: none"> • [論理デバイス (Logical Devices)] > [構成 (Configuration)] <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
サポート対象ネットワークモジュールに対する Firepower 4100/9300 でのハードウェアバイパスサポート	6.1	いずれか	<p>ハードウェアバイパスは、停電時にトラフィックがインラインインターフェイスペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。</p> <p>新規/変更された画面 :</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] > [物理インターフェイスの編集 (Edit Physical Interface)] <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
Threat Defense のインラインセットリンクステート伝達サポート	6.1	いずれか	<p>Threat Defense アプリケーションでインラインセットを設定し、リンクステート伝達を有効にすると、Threat Defense はインラインセットメンバーシップを FXOS シャーシに送信します。リンクステート伝達により、インラインセットのインターフェイスの 1 つが停止した場合、シャーシは、インラインインターフェイスペアの 2 番目のインターフェイスも自動的に停止します。</p> <p>新規/変更された FXOS コマンド : show fault grep link-down、show interface detail</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 9300 の Threat Defense での シャーシ内クラスタリング サポート	6.0.1	いずれか	<p>Firepower 9300 が Threat Defense 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。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 :</p> <ul style="list-style-type: none"> • [論理デバイス (Logical Devices)] > [構成 (Configuration)] <p>新規/変更された FXOS コマンド : 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</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

翻訳について

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