



の Firepower Threat Defense の論理デバイス Firepower 4100/9300

Firepower 4100/9300 は柔軟なセキュリティプラットフォームが1つまたは複数の論理デバイスをインストールすることができます。FTDをFMC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、Firepower 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 Firepower 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 Threat Defense 用のクラスタリング](#)を参照してください。FXOS CLI を使用する場合は、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。

- [Firepower 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 \(14 ページ\)](#)
- [コンテナ インスタンスのライセンス \(24 ページ\)](#)
- [コンテナ インスタンスの要件と前提条件 \(25 ページ\)](#)
- [論理デバイスに関する注意事項と制約事項 \(26 ページ\)](#)
- [インターフェイスの設定 \(29 ページ\)](#)
- [論理デバイスの設定 \(35 ページ\)](#)
- [Firepower Threat Defense の論理デバイスの履歴 \(48 ページ\)](#)

Firepower 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 Firepower Chassis Manager で、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ために論理デバイスに割り当てる mgmt-type タイプのインターフェイスとは区別されます。

このインターフェイスのパラメータを設定するには、CLIから設定する必要があります。FXOS の CLI にこのインターフェイスに関する情報を表示するには、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。

インターフェイス タイプ

各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は論理デバイス間で共有できません。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- **Data-sharing** : 通常のデータに使用します。コンテナ インスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス (FTD 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の拡張性 \(3 ページ\)](#) を参照してください。共有インターフェイスは、ブリッジグループメンバインターフェイス (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、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。
- **Firepower-eventing** : FTD デバイス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、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。管理インターフェイスを参照してください。Firepower イベント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。

- **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 番のポートチャンネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシおよび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ので、シャーシとアプリケーションの間の不一致が生じることがあります。

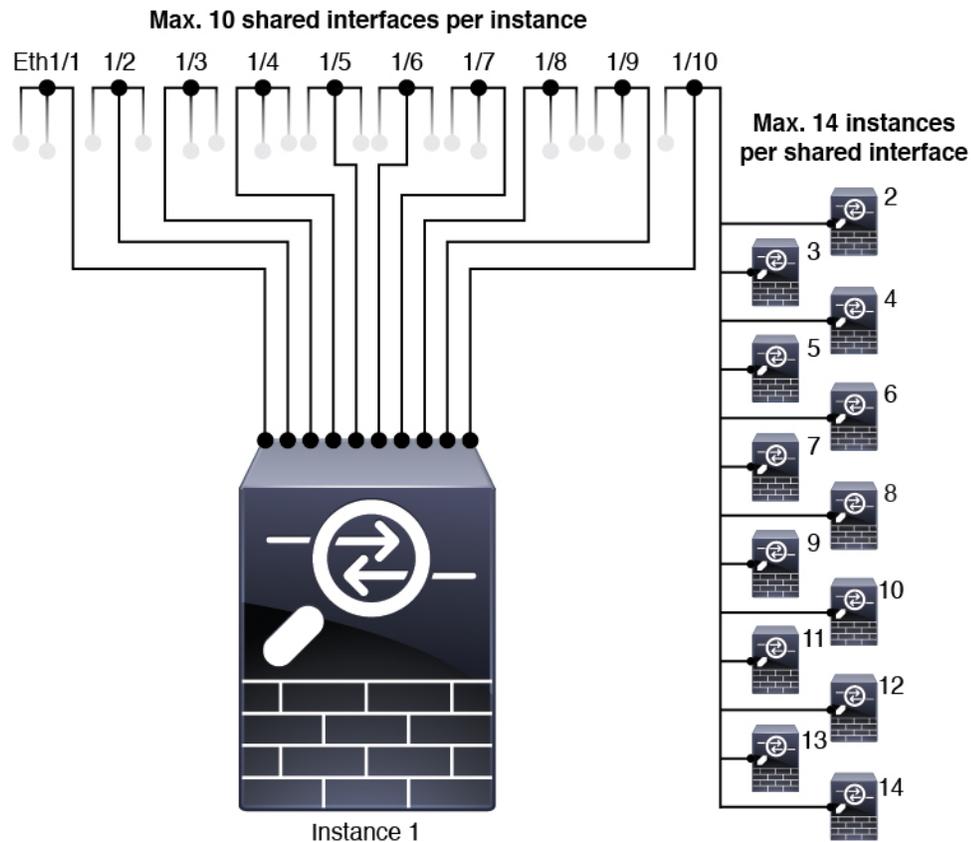
アプリケーションのインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、アプリケーション内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

コンテナ インスタンスは、data-sharing タイプのインターフェイスを共有できます。この機能を使用すると、柔軟なネットワーク展開をサポートするだけでなく、物理インターフェイスの使用率を一定に維持することができます。インターフェイスを共有する場合、シャーシは一意的 MAC アドレスを使用して適切な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シ内のフルメッシュトポロジのニーズによって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してい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、シャーシは 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。親インターフェイスの数とその他の導入決定に応じて、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、論理デバイ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-Channel1、Port-Channel2、Port-Channel3 の代わりに、その EtherChannel のサブインターフェイス (Port-Channel1.100、200、300) 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。

論理デバイスの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ことになる可能性があります。たとえば、Port-Channel1.100 を論理デバイス 1 および 2 と共有するとともに、Port-Channel1.200

を論理デバイス 2 および 3 と共有するのではなく、Port-Channel1.100 および 200 を論理デバイス 1、2、3 (1つの VLAN グループ) と共有します。

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-Channel1、Port-Channel2、Port-Channel3 の代わりに Port-Channel1.100、Port-Channel2.200、Port-Channel3.300 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。

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。

共有インターフェイスの使用状況の例

インターフェイス共有および拡張性の例については、次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 1: 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 \(6 ページ\)](#)
- [表 2: 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 \(8 ページ\)](#)
- [表 3: 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 \(10 ページ\)](#)
- [表 4: 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 \(12 ページ\)](#)

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 3 つの 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共有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 1: 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	Number of Instances	転送テーブルの使用率 (%)
32 : <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	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 	16 %
30 : <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • インスタンス 1 • インスタンス 2 	14%
14 : <ul style="list-style-type: none"> • 14 (各 1) 	1	14 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 14 	46 %
33 : <ul style="list-style-type: none"> • 11 (各 1) • 11 (各 1) • 11 (各 1) 	3 : <ul style="list-style-type: none"> • 1 • 1 • 1 	33 : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 11 (各 1) • 11 (各 1) • 12 (各 1) 	3 : <ul style="list-style-type: none"> • 1 • 1 • 1 	34 : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 30 (各 1) 	1	6 : <ul style="list-style-type: none"> • 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	Number of Instances	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共有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 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	Number of Instances	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	Number of Instances	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共有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 3: 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	Number of Instances	転送テーブルの使用率 (%)
32 : <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	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 	16 %
30 : <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • インスタンス 1 • インスタンス 2 	14%
14 : <ul style="list-style-type: none"> • 14 (各 1) 	1	14 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 14 	46 %
14 : <ul style="list-style-type: none"> • 7 (各 1) • 7 (各 1) 	2: <ul style="list-style-type: none"> • 1 • 1 	14 : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	1	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 	21 %
32 : <ul style="list-style-type: none"> • 16 (各 8) • 16 (各 8) 	2	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 	20 %

専用インターフェイス	共有インターフェイス	Number of Instances	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 タンス 2 • インスタンス 3-イン 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 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 タンス 3 • インスタンス 4-イン タンス 5	59%
14 : • 12 (2 ea.)	10	7 : • インスタンス 1-イン 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 9300 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共有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 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	Number of Instances	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	Number of Instances	転送テーブルの使用率 (%)
112 : <ul style="list-style-type: none"> • 56 (各 8) • 56 (各 8) 	4 : <ul style="list-style-type: none"> • 2 • 2 	14 : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 140 (各 10) 	10	14 : <ul style="list-style-type: none"> • インスタンス 1-インスタンス 14 	46 %
140 : <ul style="list-style-type: none"> • 70 (各 10) • 70 (各 10) 	20 : <ul style="list-style-type: none"> • 10 • 10 	14 : <ul style="list-style-type: none"> • 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、**scope fabric-interconnect** で **show detail** コマンドを入力します。次に例を示します。

```

Firepower# scope fabric-interconnect
DFirepower /fabric-interconnect # show detail

Fabric Interconnect:
  ID: A
  Product Name: Cisco FPR9K-SUP
  PID: FPR9K-SUP
  VID: V02
  Vendor: Cisco Systems, Inc.
  Serial (SN): JAD104807YN
  HW Revision: 0
  Total Memory (MB): 16185
  OOB IP Addr: 10.10.5.14
  OOB Gateway: 10.10.5.1
  OOB Netmask: 255.255.255.0
  OOB IPv6 Address: ::
  OOB IPv6 Gateway: ::
  Prefix: 64
  Operability: Operable
  Thermal Status: Ok
  Ingress VLAN Group Entry Count (Current/Max): 0/500
  Switch Forwarding Path Entry Count (Current/Max): 16/1021
  Current Task 1:
  Current Task 2:
    
```

Current Task 3:

Firepower Threat Defense のインラインセット リンク ステートの伝達

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。

FTD 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、FTD 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。

論理デバイスについて

論理デバイスでは、1つのアプリケーションインスタンス（ASA または Firepower Threat Defense のいずれか） および 1つのオプションデコレータアプリケーション（Radware DefensePro）を実行し、サービス チェーンを形成できます。

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



- (注) Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ（ASA または FTD）をインストールする必要があります。現時点では、異なるタイプはサポートされていません。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 タイプを実行できます。

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ユニット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スループットの向上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つのみ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 \(3 ページ\)](#) 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 \(33 ページ\)](#) 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：入力インターフェイスと関連付けられているインスタンスが 1 つのみの場合、シャーシはパケットをそのインスタンスに分類します。ブリッジグループ メンバ 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一意の MAC アドレスが使用されます。一意の MAC アドレスがないと、アップストリーム ルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。ただし、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

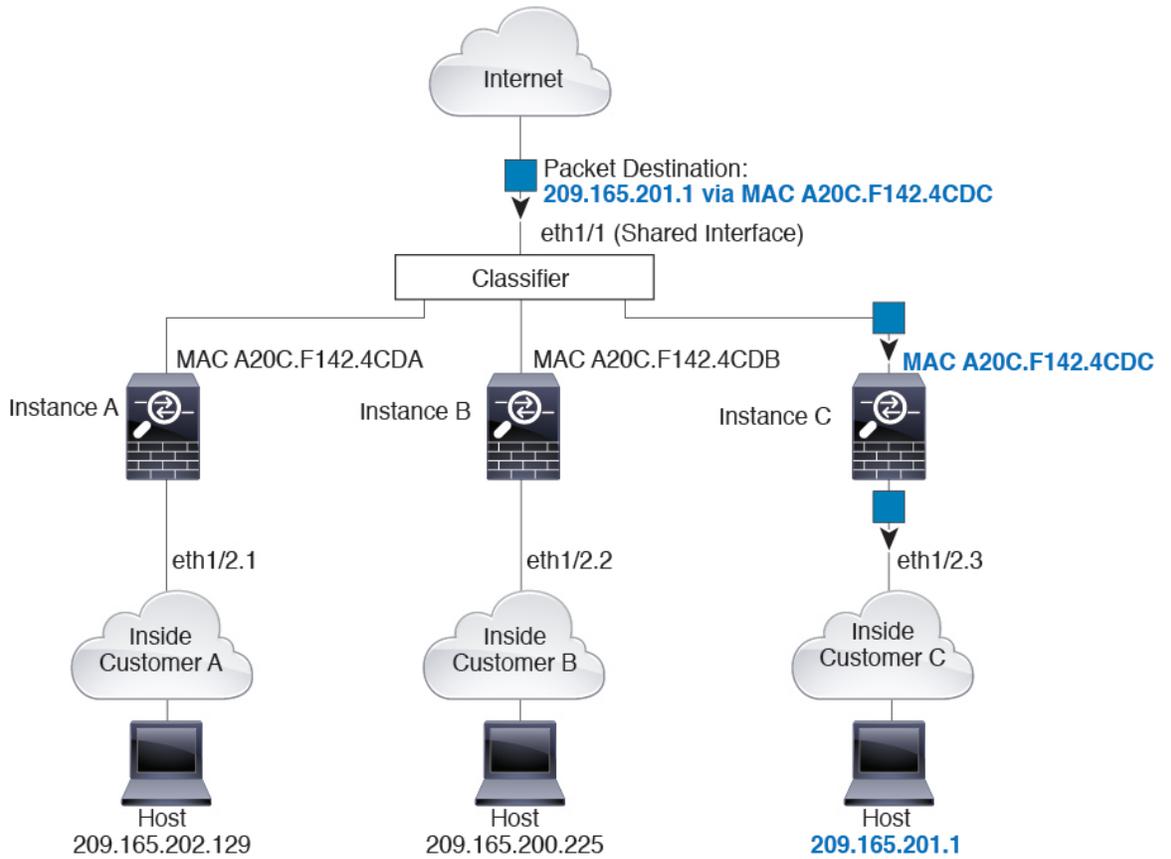


- (注) 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製されて各インスタンスに送信されます。

分類例

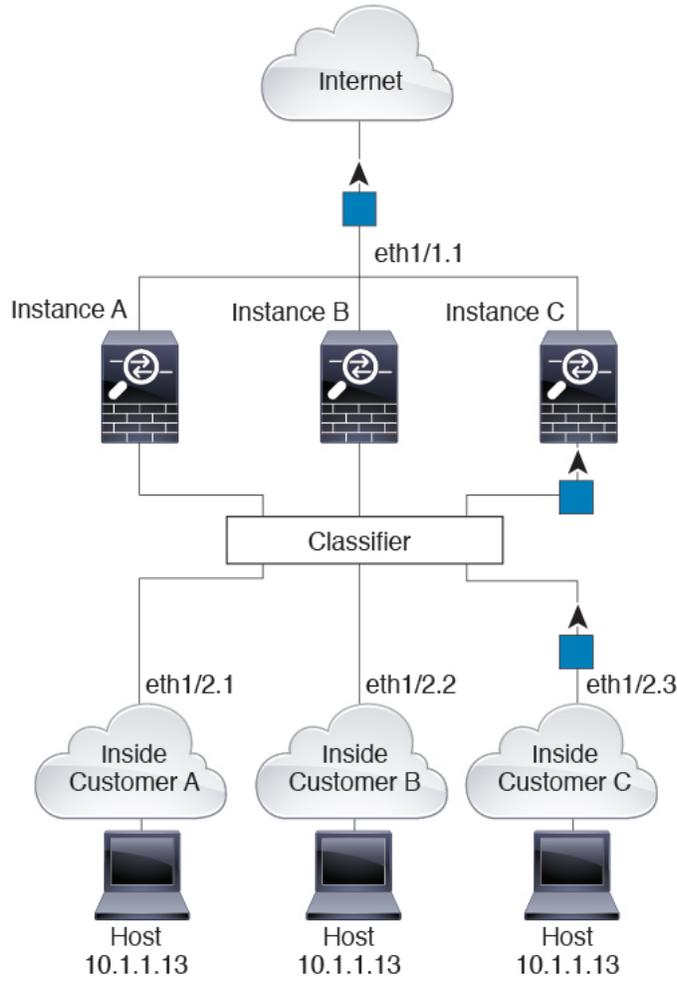
次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンス C にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

図 1: MAC アドレスを使用した共有インターフェイスのパケット分類



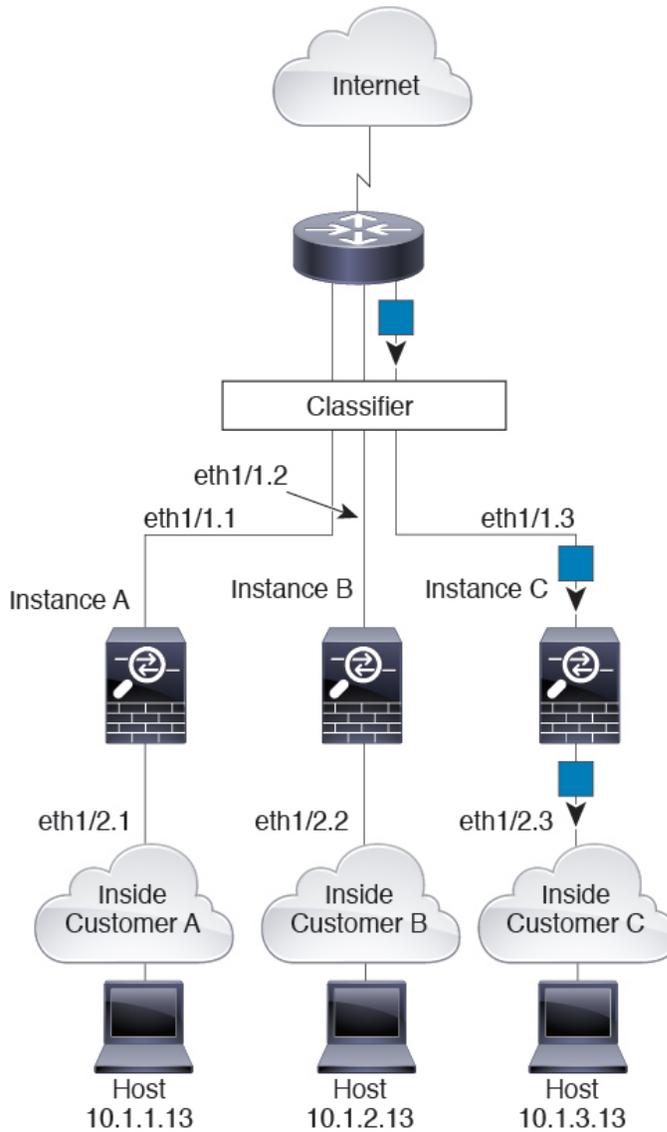
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンス C のホストを示します。分類子は、パケットをインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 2: 内部ネットワークからの着信トラフィック



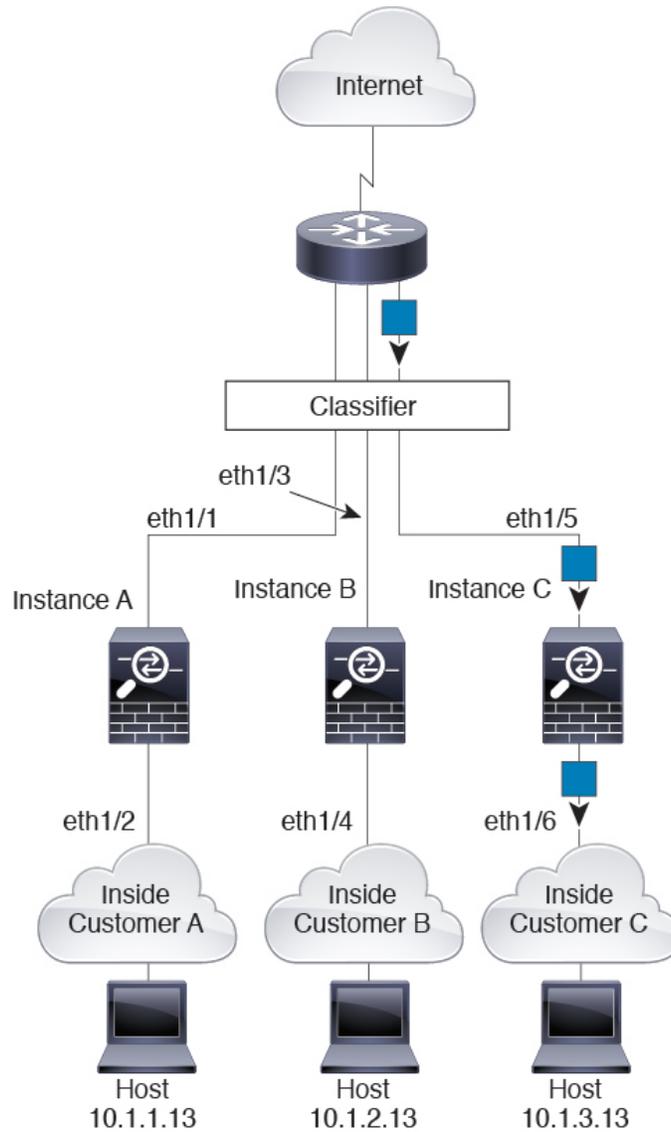
トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンスCに割り当てられているためです。

図 3: トランスパアレント ファイアウォール インスタンス



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

図 4: FTD のインラインセット

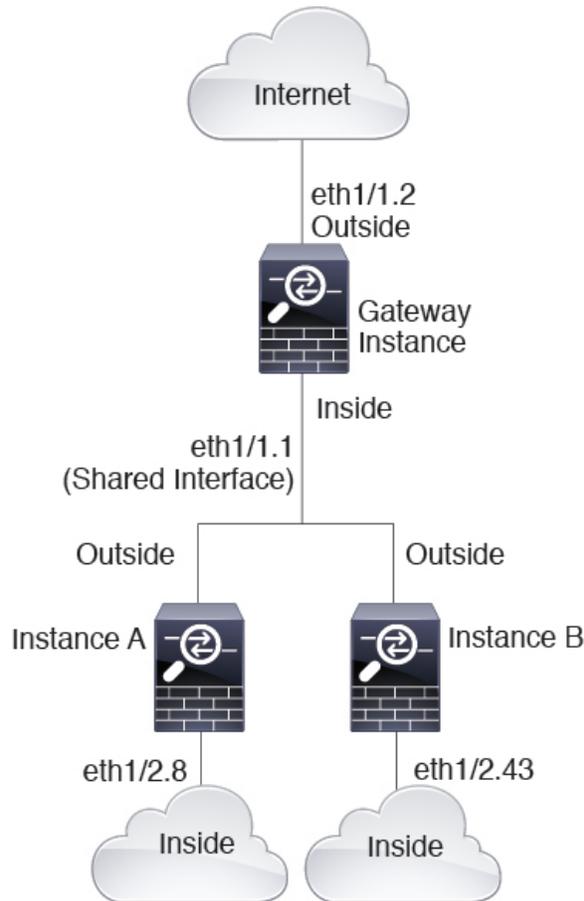


コンテナ インスタンスのカスケード

別のインスタンスの前にコンテナ インスタンスを直接配置することをカスケード コンテナ インスタンスと呼びます。1つのインスタンスの外部インターフェイスは、別のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスの設定を単純化する場合、最上位の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できます。

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

図 5: コンテナ インスタンスのカスケード

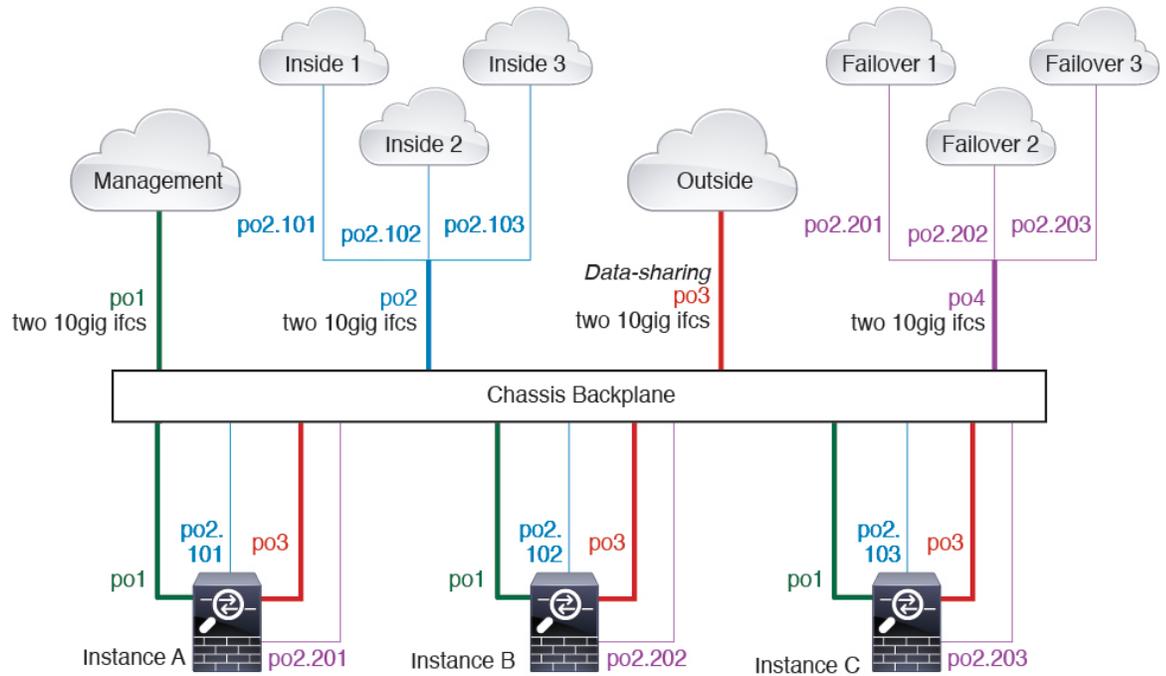


一般的な複数インスタンス展開

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

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

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



コンテナ インスタンス インターフェイスの自動 MAC アドレス

FXOS シャーシは、各インスタンスの共有インターフェイスが一意の 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。

A2xx.yyzz.zzzz

xx.yy はユーザ定義のプレフィックスまたはシステム定義のプレフィックスであり、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)。

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 \(25 ページ\)](#) 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 \(35 ページ\)](#) 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、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。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。

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。

- 基本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台のセキュリティ 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、モジュールごとに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。
- ハイ アベイラビリティについては、[高可用性ペアでの FTD デバイスのライセンス要件](#)を参照してください。

次に例を示します。

表 5: Firepower 9300 のコンテナ インスタンスのライセンスの使用状況

Firepower 9300	インスタンス (Instance)	ライセンス
セキュリティ モジュール 1	インスタンス 1	基本、URL フィルタリング、マルウェア
	インスタンス 2	基本、URL フィルタリング
	インスタンス 3	基本、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	基本、脅威
	インスタンス 5	、URL フィルタリング、マルウェア、脅威の基本します。

Firepower 9300	インスタンス (Instance)	ライセンス
セキュリティ モジュール 3	インスタンス 6	基本、マルウェア、脅威
	インスタンス 7	基本、脅威

表 6: ライセンスの総数

基本	URL フィルタリング	Malware	脅威
3	2	3	2

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 7: 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 4120	3	46	101 GB	125.6 GB
Firepower 4140	7	70	222 GB	311.8 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-44 セキュリ ティ モジュール	14	86	218 GB	628.4 GB

Firepower 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 Firepower Management Center (FMC) を使用する必要があります。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower のインターフェイスに関するガイドラインと制限事項

VLAN のサブインターフェイス

- ネットワーク導入に応じて、最大 500 の VLAN ID を使用してシャーシあたり 250 ~ 500 のサブインターフェイスを作成できます。
- 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でのみサポートされます。
- 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。



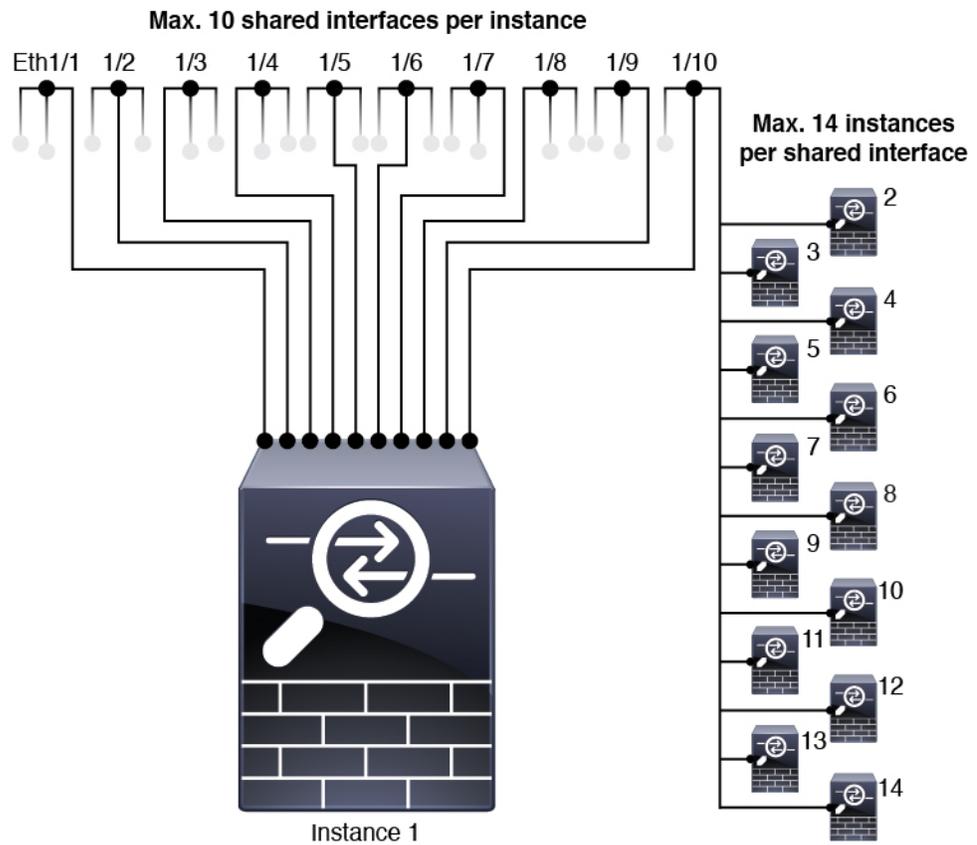
(注) コンテナインスタンスに親インターフェイスを割り当てる場合、タグなし（非 VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。

- 論理デバイスアプリケーション内の次の制限事項を確認してください。インターフェイスの割り当てを計画する際は、これらの制限事項に留意してください。
 - FTD インラインセットのサブインターフェイスを使用することはできません。また、パッシブ インターフェイスとして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使用し、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

- 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、Instance14 を介して Instance1 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：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。



- ネイティブ インスタン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。
- 論理デバイスアプリケーション内の次の制限事項を確認してください。インターフェイスの割り当てを計画する際は、これらの制限事項に留意してください。
 - トランスペアレント ファイアウォール モードデバイスとの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。
 - FTD 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。

インラインセット FTD

- 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ていません。
- リンク状態の伝達はサポートされています。

ハードウェアバイパス

- FTD でサポートされています。ASA の通常のインターフェイスとして使用できます。
- FTD はインライン セットを含むハードウェア バイパスのみをサポートします。
- 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 ハイ アベイラビリティではサポートされていません。

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 チャンネル 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した場合、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（22 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

FTD 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 のシステム要件](#)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

- マルチ コンテキスト モードは ASA でのみサポートされています。
- 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

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 プロパティを編集して。

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 [Interfaces] を選択して、[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、[disabled スライダ ()] をクリックします。これで、[enabled スライダ ()] に変わります。

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

ステップ 3 インターフェイスを無効にするには、[enabled スライダ ()] をクリックします。これで、[disabled スライダ ()] に変わります。

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

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。

始める前に

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

手順

ステップ 1 [Interfaces] を選択して [Interfaces] ページを開きます。

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

- ステップ 2** 編集するインターフェイスの行で[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にするには、[有効化 (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 [Type] を次から選択します。 **Data**、**Data-sharing**、**Mgmt**、**Firepower-eventing**、または **Cluster**。
- Cluster** タイプは選択しないでください。デフォルトでは、Cluster Control Link はポートチャネル 48 に自動的に作成されます。
- ステップ 5** (任意) [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) [デュプレックス (Duplex)] ドロップダウンリストからインターフェイスのデュプレックスを選択します。
- ステップ 8** [OK] をクリックします。

EtherChannel (ポート チャネル) の追加

EtherChannel (別名ポートチャネル) には、同じタイプのメンバーインターフェイスを最大 16 個含めることができます。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ンネル 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られ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られるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended)] または [ダウン (Down)] 状態に戻ります。

手順

-
- ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。
- [All Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** インターフェイス テーブルの上にある [ポート チャンネルの追加 (Add Port Channel)] をクリックし、[ポート チャンネルの追加 (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 チャンネル ID (Port Channel ID)] フィールドに、ポート チャンネルの ID を入力します。有効な値は、1 ~ 47 です。
- ポートチャンネル 48 は、クラスタ化された論理デバイスを展開するときのクラスタ制御リンクとして予約されています。クラスタ制御リンクにポートチャンネル 48 を使用しない場合は、別の ID で EtherChannel を設定し、インターフェイスにクラスタ タイプを選択できます。シャーシ内クラスタリングでは、インターフェイスをクラスタ EtherChannel に割り当てないでください。
- ステップ 4** ポート チャン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 チャンネルを無効にするには、[有効化 (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 [Type] を次から選択します。Data、Data-sharing、Mgmt、Firepower-eventing、または Cluster。
- デフォルトの代わりに、このポートチャンネルを Cluster Control Link として使用する場合は、[Cluster] タイプを選択しないでください。
- ステップ 6** ドロップダウン リストでメンバ インターフェイスの [Admin Speed] を設定します。

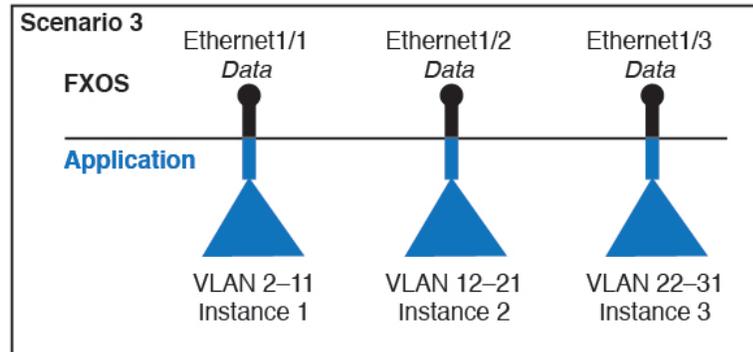
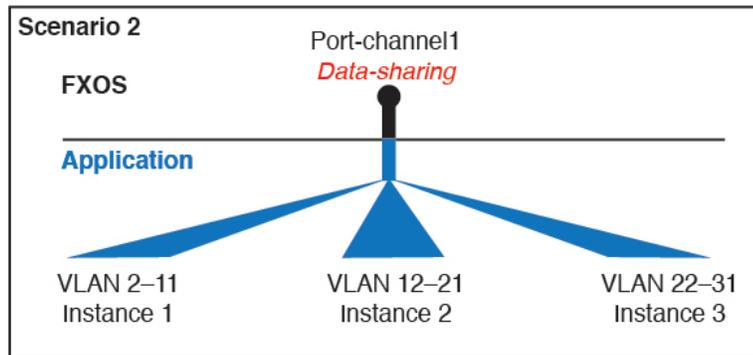
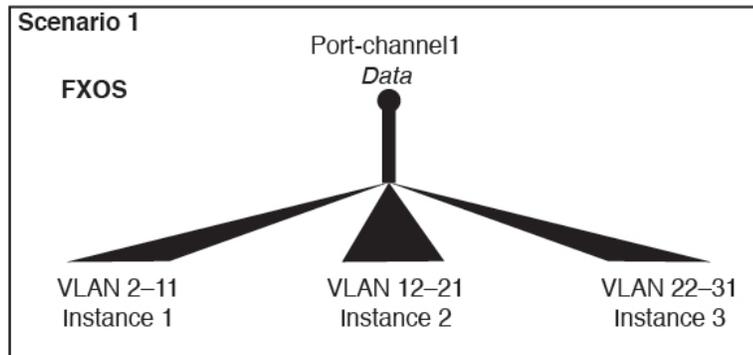
- ステップ 7** データまたはデータ共有インターフェイスに対して、LACP ポートチャンネル [Mode]、[Active] または [On] を選択します。
- 非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。
- ステップ 8** [Admin Duplex]、[Full Duplex] または [Half Duplex] を設定します。
- ステップ 9** ポートチャンネルにインターフェイスを追加するには、[Available Interface] リストでインターフェイスを選択し、[Add Interface] をクリックしてそのインターフェイスを [Member ID] リストに移動します。同じタイプで同じ速度のインターフェイスを最大 16 個追加できます。
- ヒント** 一度に複数のインターフェイスを追加できます。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 インスタンスへの 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。

インターフェイスごとの VLAN ID は一意であることが必要です。またコンテナインスタンス内では、すべての割り当てられたインターフェイスで VLAN ID が一意であることが必要です。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。

ネイティブ インスタンスの場合、アプリケーション内でのみ VLAN サブインターフェイスを作成できます。コンテナインスタンスの場合、FXOS VLAN サブインターフェイスが定義されていないインターフェイスのアプリケーション内でも VLAN サブインターフェイスを作成できます。これらのサブインターフェイスには FXOS 制限が適用されません。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 を使おうとします。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。



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 [Type] : [Data] または [Data-sharing] を選択します。

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でのみサポートされます。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、データ共有タイプの親インターフェイスとデータタイプのサブインターフェイスを持つことができます。

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

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のペアを Firepower 4100/9300 シャーシに追加します。

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

コンテナ インスタンスのリソース プロファイルの追加

コンテナインスタンスごとにリソースの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。

- コアの最小数は 6 です。
- 内部アーキテクチャにより 8 コアを指定することはできません。
- コアを偶数（6、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（25 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。

現在使用されている場合、リソースプロファイル設定を変更することはできません。それ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。確立されたハイ アベイラビリティ ペア内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

FTD インスタンスを FMC に追加した後にリソース プロファイル設定を変更する場合は、**[Devices] > [Device Management] > [Device] > [System] > [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。

手順

ステップ 1 **[Platform Settings] > [Resource Profiles]** を選択し、**[Add]** をクリックします。

[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。

- **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。
- **Description** : プロファイルの説明を最大 510 文字で設定します。
- **Number of Cores** : シャーシに応じて、プロファイルのコア数を 6 ~ 最大数 (偶数) で設定します。8 コアを指定することはできません。

ステップ 3 **[OK]** をクリックします。

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、そのイメージを Firepower 4100/9300 シャーシ。



(注) Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーションインスタンス タイプ (ASA または FTD) をインストールする必要があります。現時点では、異なるタイプはサポートされていません。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 タイプを実行できます。

- 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 (シャーシ管理インターフェイスは、[Interfaces] タブの上部に [MGMT] として表示されます)。
- また、少なくとも1つのデータ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 \(2 ページ\)](#)」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のリソースプロファイルの追加 \(35 ページ\)](#) 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。[Security Modules] または [Security Engine] を選択し、[[Reinitialize] アイコン (🔧) をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブ インスタンスとコンテナ 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。
- 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の 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 [Logical Devices] を選択します。

ステップ 2 [デバイスの追加 (Add Device)] をクリックし、次のパラメータを設定します。

a) [Device Name] に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 사용되는デバイス名ではありません。

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

c) [Image Version] を選択します。

d) [Instance Type] で [Container] または [Native] を選択します。

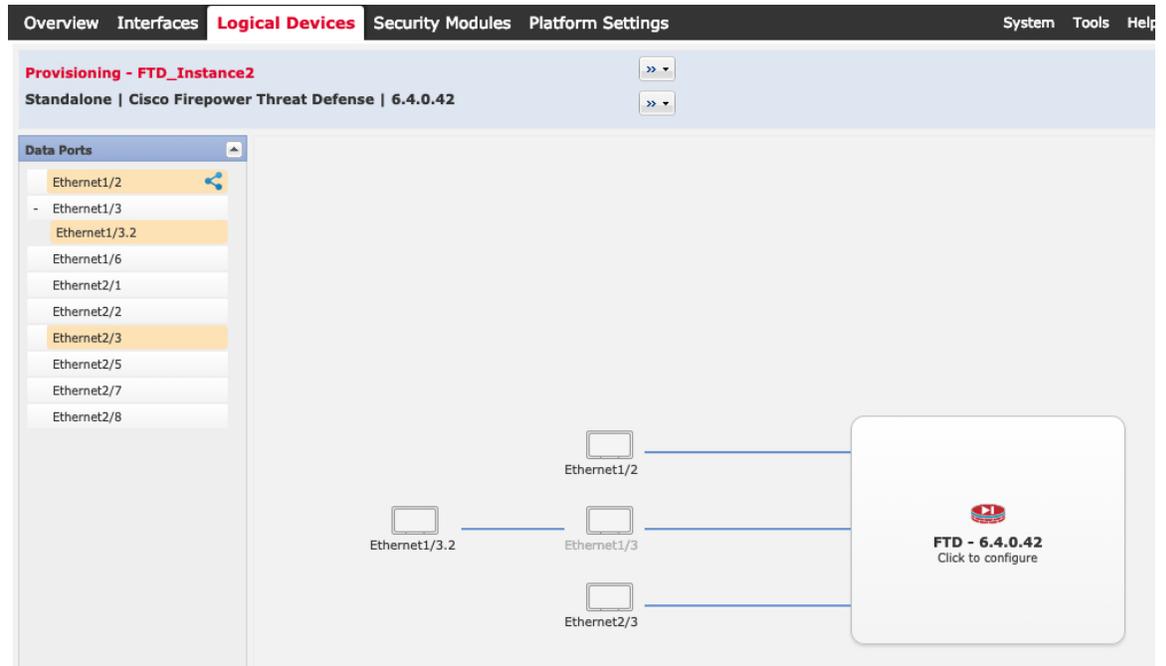
ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース (CPU、RAM、およびディスク容量) を使用するため、ネイティブインスタンスを1つのみインストールできます。コンテナインスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

e) [使用方法 (Usage)] で、[スタンドアロン (Standalone)] オプションボタンをクリックします。

f) [OK] をクリックします。

[プロビジョニング-デバイス名 (Provisioning - device name)] ウィンドウが表示されます。

ステップ 3 [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。後ほど FMC でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

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ができます。データ共有インターフェイスは [sharing] アイコン () で示されます。

ハードウェア バイパス 対応のポートは次のアイコンで表示されます: 。特定のインターフェイス モジュールでは、インラインセット インターフェイスに対してのみハードウェア バイパス機能を有効にできます (FMC コンフィギュレーション 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。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。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 CLI の設定を使用してほとんどの値を変更できます。

ステップ 5 [General Information] タブで、次の手順を実行します。

- a) (Firepower 9300 の場合) [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。

- 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、シャーシ管理ポートとは別のものです。
- d) 管理インターフェイスの [Address Type] を [IPv4 only]、[IPv6 only]、または [IPv4 and IPv6] から選択します。
- e) [Management IP] アドレスを設定します。
このインターフェイス固有の 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。

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

Registration Key: [.....]

Confirm Registration Key: [.....]

Password: [.....]

Confirm Password: [.....]

Firepower Management Center IP: [10.89.5.35]

Permit Expert mode for FTD SSH sessions: [yes]

Search domains: [cisco.com]

Firewall Mode: [Routed]

DNS Servers: [10.89.5.67]

Firepower Management Center NAT ID: [test]

Fully Qualified Hostname: [ftd2.cisco.com]

Eventing Interface: [.....]

- a) 管理 FMC の [Firepower Management Center IP] を入力します。
- b) コンテナ インスタンスに対して、**FTD SSH セッションでエキスパート モードを許可するかどうか**を [Yes] または [No] で指定します。エキスパート モードでは、高度なトラブルシューティングに FTD シェルからアクセスできます。

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

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

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

ルーテッドモードでは、FTDはネットワーク内のルータホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。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のみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

- e) カンマ区切りリストとして [DNS Servers] を入力します。

たとえば、FMC のホスト名を指定する場合、FTD は DNS を使用します。

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

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

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [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。[Logical Devices] ページで、新しい論理デバイスのステータスを確認します。論理デバイスのステータスが [online] と表示されたら、アプリケーションでセキュリティポリシーの設定を開始できます。



ステップ 10 FTD を管理対象デバイスとして追加し、セキュリティポリシーの設定を開始するには、FMC コンフィギュレーションガイドを参照してください。

ハイアベイラビリティペアの追加

FTD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、高可用性用にシャーシを準備する場合は、次のステップ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。
- 高可用性システム要件については、[ハイアベイラビリティのシステム要件](#)を参照してください。

手順

-
- ステップ1** 各論理デバイスは個別のシャーシに配置する必要があります。Firepower 9300でのシャーシ内高可用性は推奨されておらず、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じ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、10GB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れば、別のフェールオーバーおよびステートのリンクを使用できます。ステートリンクには、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状態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ィを有効にします。[Firepower Threat Defenseのハイアベイラビリティ](#)を参照してください。
- ステップ5** ハイアベイラビリティを有効にした後にインターフェイスを変更する必要がある場合は、スタンバイユニットを最初に変更し、次にアクティブユニットを変更します。
-

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

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

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

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

始める前に

- [物理インターフェイスの設定 \(30 ページ\)](#) および [EtherChannel \(ポート チャンネル\) の追加 \(31 ページ\)](#) 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 Firepower イベント インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。FTD がリポートし (管理インターフェイスを変更するとリポートします)、FMC で設定を同期すると、(現在未割り当ての) 管理インターフェイスも EtherChannel に追加できます。
- クラスタリング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。

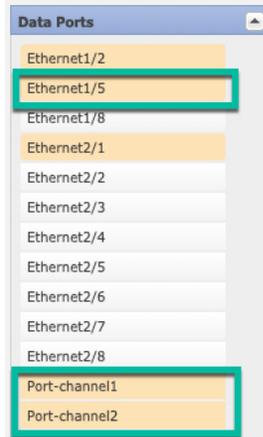
手順

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

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

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

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。

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

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

ステップ 5 [保存 (Save)] をクリックします。

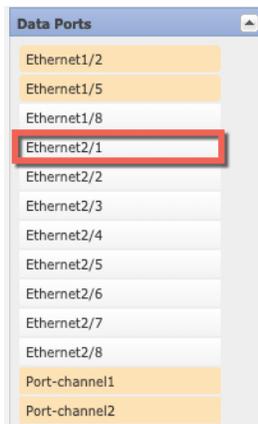
ステップ 6 FMC でインターフェイスを同期します。

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

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

- f) [変更の検証 (Validate Changes)] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。
エラーがある場合は、ポリシーを変更して検証に戻る必要があります。
- g) [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 7 Firepower Chassis Manager で、[データポート (Data Ports)] 領域でデータ インターフェイスの選択を解除し、そのインターフェイスの割り当てを解除します。



ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 FMC でインターフェイスを再度同期します。

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、モジュールに対して同時に複数のセッションを持つことができ、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。

- FTD : **exit** と入力

ステップ 4 FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次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

Firepower Threat Defense の論理デバイスの履歴

機能	バージョン (Version)	詳細
Firepower 4100/9300 上の Firepower Threat Defense のマルチインスタンス機能	6.3.0	

機能	バージョン (Version)	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 Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーション インスタンスを展開するだけでした。</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。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。</p> <p>新規/変更された [Firepower Management Center] 画面 :</p> <ul style="list-style-type: none"> • [Devices] > [Device Management] > [Edit] アイコン > [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)]

機能	バージョン (Version)	詳細
		<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)] > [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： connect ftd <i>name</i>、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 <i>name</i>、show cgroups container、show interface、show mac-address、show subinterface、show tech-support module app-instance、show version</p> <p>サポートされるプラットフォーム： Firepower 4100/9300</p>

機能	バージョン (Version)	詳細
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	6.3.0	<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せん。FXOS でクラスタを展開する際にネットワークを設定できるようになりました。シャーシは、シャーシ ID およびスロット ID (127.2.chassis_id.slot_id) に基づいて、各ユニットのクラスタ制御リンクインターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック (127.0.0.0/8) およびマルチキャスト (224.0.0.0/4) アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。</p> <p>新規/変更された [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 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>

機能	バージョン (Version)	詳細
オンモードでのデータ EtherChannel のサポート	6.3.0	<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)] > [ポートチャンネルの編集 (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>
FTD インラインセットでの EtherChannel のサポート	6.2.0	<p>FTD 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>
6つの FTD モジュールのシャーシ間クラスタリング	6.2.0	<p>FTD 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>

機能	バージョン (Version)	詳細
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	6.1.0	<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>新しい/変更された画面：</p> <ul style="list-style-type: none"> • [Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface] <p>サポートされるプラットフォーム： Firepower 4100/9300</p>
FTD のインラインセットリンクステート伝達サポート	6.1.0	<p>FTD 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、FTD 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	バージョン (Version)	詳細
Firepower 9300 の FTD でのシャーシ内クラスタリングサポート	6.0.1	<p>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。</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>