インターフェイス管理

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 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。管理 IP アドレスの変更も参照してください。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（Firepower Threat DefenseFMC 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、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。

（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： FMC デバイスを使用した Firepower Threat Defense のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、Firepower Threat Defense 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倫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。FDM 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。FTD 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 FTD 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
FTD	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	対応	—	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	—
	クラスタ コンテナ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	対応
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（シャー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。

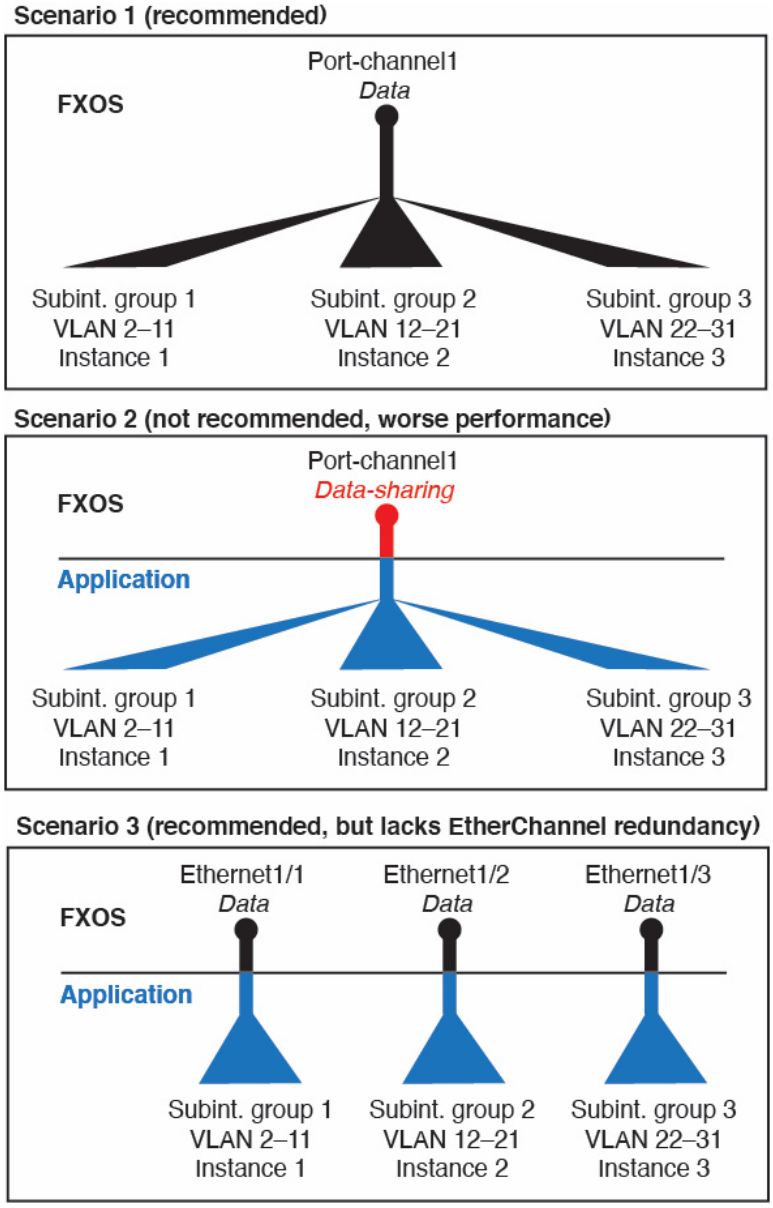
続くセクションでは、インターフェイスの FXOS とアプリケーション間の連携について説明します。

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



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。

ハードウェア バイパス ペア

Firepower Threat Defense では、Firepower 9300 および 4100 シリーズの特定のインターフェイスモジュールを使用することで、ハードウェア バイパス 機能を有効にできます。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 機能は、Firepower Threat Defense アプリケーション内で設定されます。これらのインターフェイスを ハードウェア バイパス ペアとして使用する必要はありません。これらは、ASA と Firepower Threat Defense アプリケーションの両方について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 対応のインターフェイスをブレークアウト ポート用に設定することはできないため注意してください。ハードウェア バイパス 機能を使用するには、ポートを EtherChannel として設定しないでください。そうでない場合は、これらのインターフェイスを通常のインターフェイス モードの EtherChannel メンバとして含めることができます。

ハードウェア バイパス がインラインペアで有効になっている場合、スイッチのバイパスが最初に試行されます。スイッチのエラーが原因でバイパス設定が失敗した場合は、物理バイパスが有効になります。

（注） ハードウェアバイパス（FTW）は、VDP/Radware などのサードパーティ製アプリケーションを使用したサービスチェイニングにインストールされた Firepower Threat Defense ではサポートされません。

（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 およびリンク状態の伝達を有効にしないでください。

Firepower Threat Defense は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアで ハードウェア バイパス をサポートします。

- Firepower 9300
- Firepower 4100 シリーズ

これらのモデルでサポートされている ハードウェア バイパス ネットワーク モジュールは以下のとおりです。

- Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR-NM-6X1SX-F）

- Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10SR-F）
- Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR-NM-6X10LR-F）
- Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR-NM-2X40G-F）
- Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド（FPR-NM-8X1G-F）

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6
- 7 および 8

ジャンボ フレーム サポート

Firepower 4100/9300 シャーシは、デフォルトで有効になっているジャンボ フレームをサポートします。Firepower 4100/9300 シャーシにインストールされた特定の論理デバイスのジャンボ フレーム サポートを有効にするには、論理デバイスのインターフェイスに適切な MTU の設定を構成する必要があります。

Firepower 4100/9300 シャーシのアプリケーションでサポートされている最大 MTU は、9184 です。

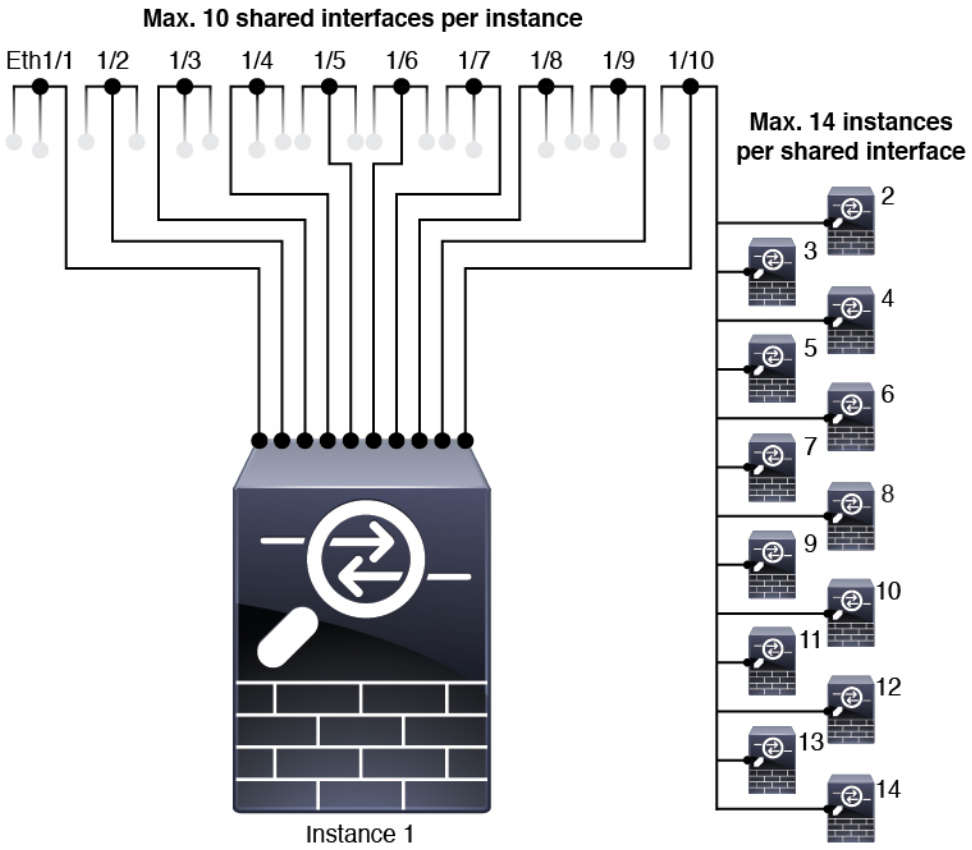
（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

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、シャーシは一意の 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、シャーシ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。 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

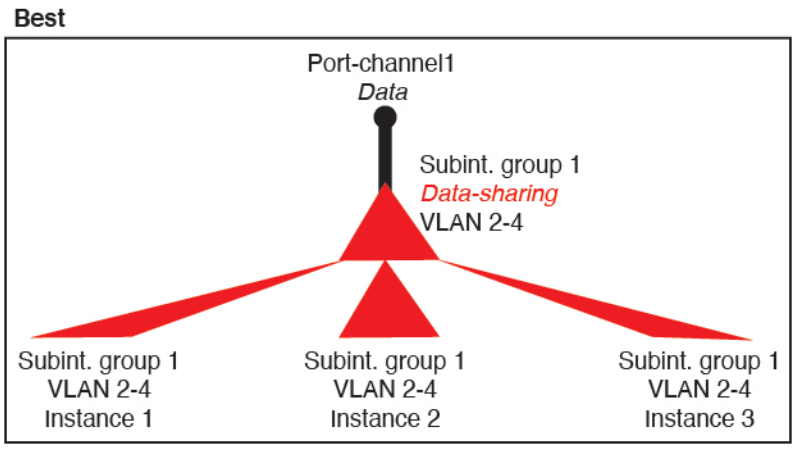
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1 つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナインスタンスで VLAN を分割できます。

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。

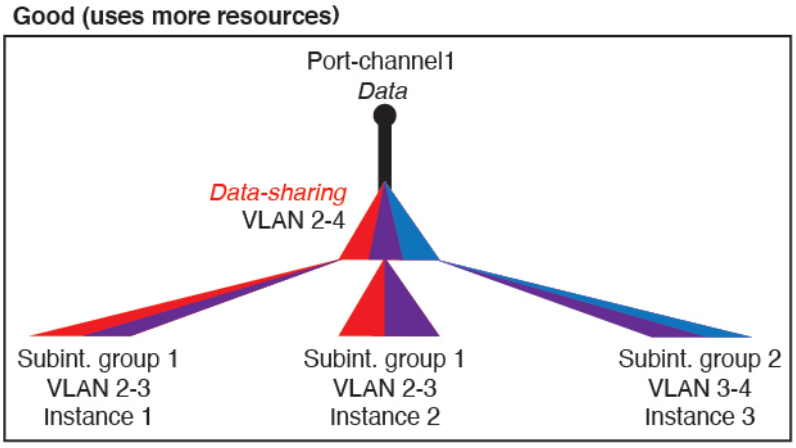
   たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模なEtherChannelを作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.2、3、4）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

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こと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。

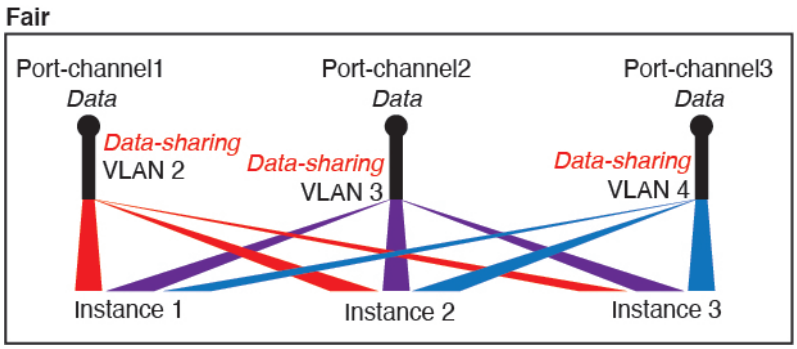
図 *3:* 良好：単一の親の複数のサブインターフェイスグループを共有



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。この使用方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。

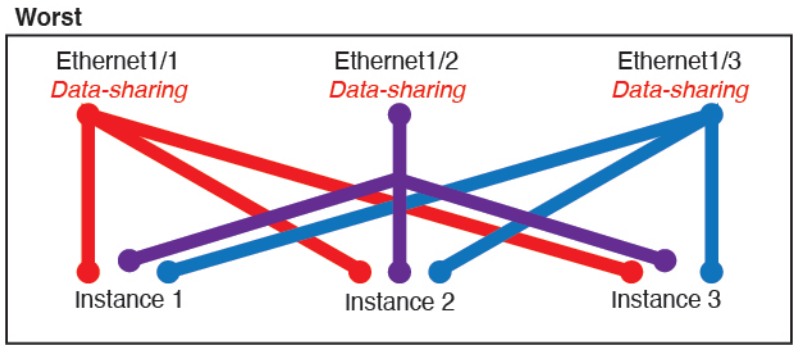
図 *4*: 普通：個別の親のサブインターフェイスを共有



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 （12 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 （14 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 （16 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 （18 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%

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（%）
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 %
30： • 10（各 5） • 10（各 5） • 10（各 5）	**3**： • 1 • 1 • 1	**6**： • 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： • 30（各 6）	**2**	**5**： • インスタンス 1 - インスタンス 5	28%
30： • 12（各 6） • 18（各 6）	**4**： • 2 • 2	**5**： • 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 %

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（%）
24： • 6 • 6 • 6 • 6	**7**	**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	44 %
24： • 12（各 6） • 12（各 6）	**14**： • 7 • 7	**4**： • 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 %

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（%）
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%
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 %

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（%）
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 %

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（%）
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 %
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 %

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（%）
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

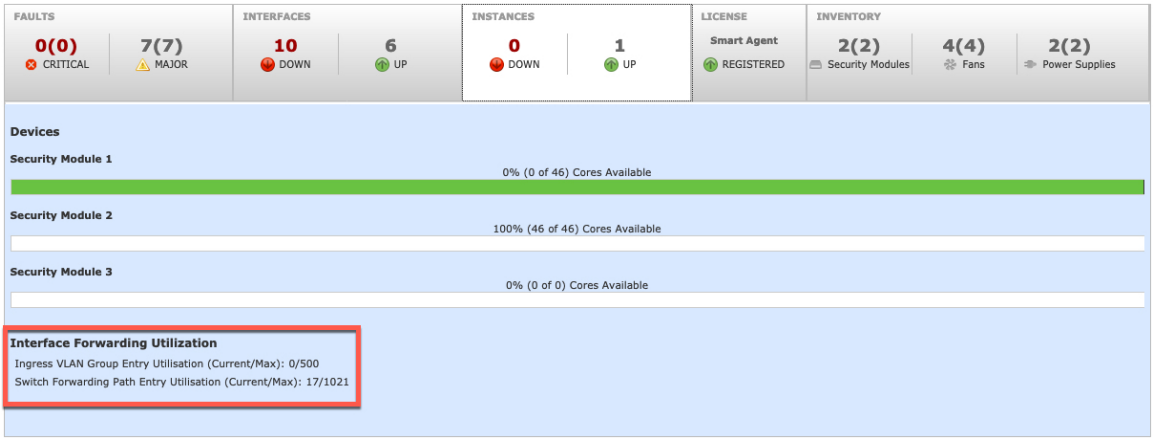
専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 112（各 8）	**0**	**14**： • インスタンス 1 - インスタンス 14	17%

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（%）
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 %
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 %

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（%）
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、**[インスタンス（Instances）]>[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。



FTD 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。

Firepower 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、Firepower 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。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。

（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 およびリンク状態の伝達を有効にしないでください。

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。FTD 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。

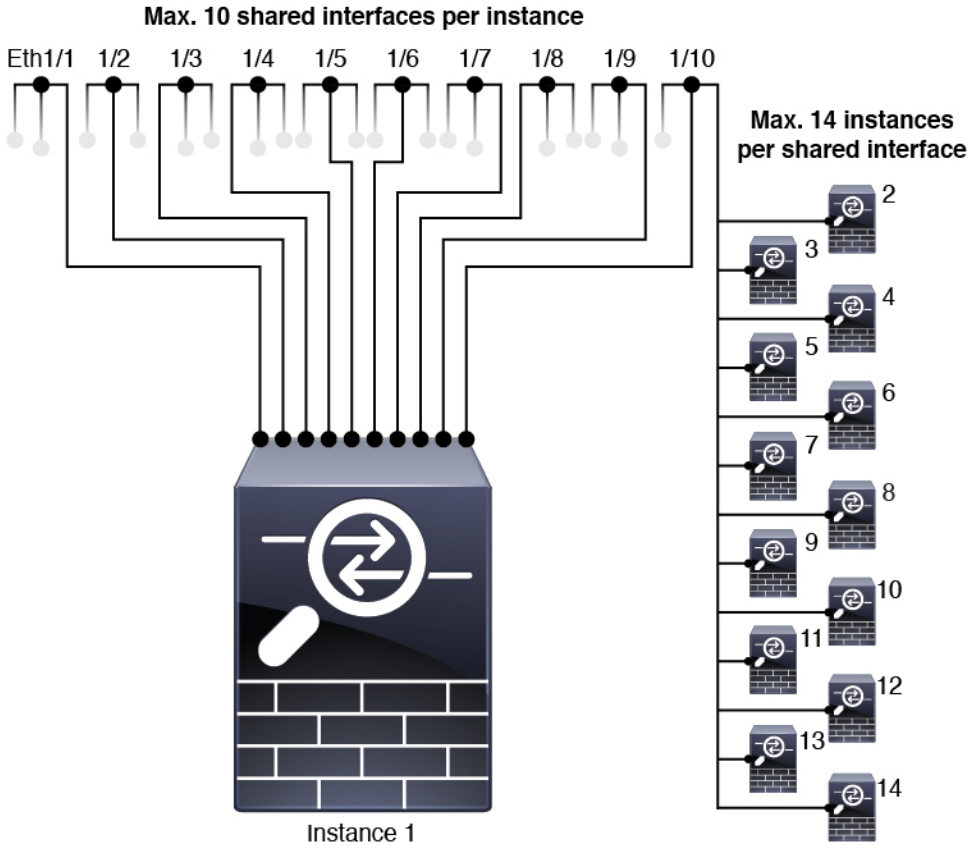
- サブインターフェイスはデータまたはデータ共有タイプのインターフェイス、およびクラスタタイプのインターフェイスでサポートされます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。
- マルチインスタンス クラスタリングの場合、データインターフェイス上の FXOS サブインターフェイスはサポートされません。ただし、クラスタ制御リンクではサブインターフェイスがサポートされているため、クラスタ制御リンクには専用の EtherChannel または EtherChannel のサブインターフェイスを使用できます。アプリケーショ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。
  - Firepower Threat Defense 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。
  - Firepower Threat Defense 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 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ません。
- リンク ステート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

- Firepower Threat Defense 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。
- Firepower Threat Defense 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ークアウト 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 を参照してください。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、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、ブレークアウト ポートを設定できます。

（注）

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ディセーブルになっています。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ディセーブルにするには、[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。

- **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]：Firepower Threat Defense 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） 以前に設定した**ネットワーク制御ポリシー**を選択します。

ステップ 9 （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 10 [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（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。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 チャネルをディセーブルにするには、**[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。

- **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]：Firepower Threat Defense 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）]）。

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

ステップ 9 ポート チャ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、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（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

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 クラスタリングの場合、クラスタ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。FTD 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。

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。

- **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す。

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。

ブレークアウト ケーブルの設定

Firepower 4100/9300 シャーシで使用するブレークアウト ケーブルを設定するには、次の手順に従います。ブレークアウト ケーブルを使用すると、1 つの 40 Gbps ポートの代わりに 4 つの 10 Gbps ポートを実装できます。

始める前に

ハードウェア バイパス 対応のインターフェイスをブレークアウト ポート用に設定することはできません。

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。

ブレークアウト ケーブルに対応できるインターフェイスが、現在そのように設定されていない場合は、そのインターフェイスの行に [ブレークアウト ポート（Breakout Port）] アイコンが表示されます。ブレークアウト ケーブルを使用するように設定されているインターフェイスの場合、個々のブレークアウト インターフェイスが別々にリストされます（例：イーサネット 2/1/1、2/1/2、2/1/3、2/1/4）。

ステップ 2 1 つの 40 Gbps インターフェイスを 4 つの 10 Gbps インターフェイスに変換するには、次の手順を実行します。

a) 変換するインターフェイスの [ブレークアウト ポート（Breakout Port）] アイコンをクリックします。

[ブレークアウト ポートの作成（Breakout Port Creation）] ダイアログボックスが開いて、続行の確認を求められ、シャーシのリブートについての警告が表示されます。

b) [はい（Yes）] をクリックして確定します。

シャーシが再起動し、指定したインターフェイスが 4 つの 10 Gbps インターフェイスに変換されます。

ステップ 3 4 つの 10 Gbps ブレークアウト インターフェイスを 1 つの 40 Gbps インターフェイスに再度変換するには、次の手順を実行します。

a) いずれかのブレークアウト インターフェイスの [削除（Delete）] をクリックします。

確認のダイアログボックスが開き、続行するかどうかの確認が求められるとともに、4 つのブレークアウトインターフェイスが削除され、シャーシが再起動すると警告されます。

b) [はい（Yes）] をクリックして確定します。

シャーシが再起動し、指定したインターフェイスが 1 つの 40 Gbps インターフェイスに変換されます。

モニタリング インターフェイス

Firepower Chassis Manager の [インターフェイス（Interfaces）] ページから、シャーシにインストールされているインターフェイスのステータスの表示、インターフェイスのプロパティの編集、インターフェイスの有効化または無効化、ポート チャネルの作成を行えます。

[インターフェイス（Interfaces）] ページは、2 つのセクションで構成されています。

- 上部のセクションには、シャーシに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表示されます。インターフェイスのいずれかにマウスのカーソルを合わせると、そのインターフェイスの詳細情報が表示されます。

  インターフェイスは、それぞれの現在のステータスを示すために色分けされています。

  - 緑色：そのインターフェイスはインストールされており、有効になっています。
  - ダーク グレイ：そのインターフェイスはインストールされていますが、無効になっています。
  - 赤色：インターフェイスの動作状態に問題があります。
  - 淡い灰色：インターフェイスがインストールされていません。

（注） ポート チャネルのポートとして機能するインターフェイスは、このリストに表示されません。

- 下部のセクションには、[All Interfaces] と [**ハードウェア バイパス**] の 2 つのタブが含まれています。**[All Interfaces]** タブ：インターフェイスごとに、インターフェイスを有効または無効にできます。[Edit] をクリックすると、インターフェイスのプロパティ（速度やインターフェイス タイプなど）を編集することもできます。**ハードウェア バイパス**については、ハードウェア バイパス ペア （7 ページ）を参照してください。

（注） ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバインターフェイスが含まれていない場合は、[Operation State] を [Failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバ インターフェイスを必要としないため、この動作状態は無視して構いません。

インターフェイスのトラブルシューティング

エラー：スイッチの転送パスに1076のエントリがあり、1024の制限を超えています。インターフェイスを追加する場合は、論理デバイスに割り当てられている共有インターフェイスの数を減らすか、論理デバイス共有インターフェイスの数を減らすか、または共有されていないサブインターフェイスを使用します。サブインターフェイスを削除すると、このメッセージが表示されます。これは、残りの設定が [Switch Forwarding Path] テーブル内に収まるように最適化されなくなったためです。削除の使用例に関するトラブルシューティング情報については、FXOS コンフィギュレーション ガイドを参照してください。'scope fabric-interconnect' の 'show detail' を使用して、現在の [Switch Forwarding Path Entry Count] を表示します。

論理デバイスから共有サブインターフェイスを削除しようとしたときにこのエラーが表示される場合は、新しい設定が共有サブインターフェイス向けのこのガイドラインに従っていないためです。同じ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使用します。1 つの論理デバイスから共有サブインターフェイスを削除すると、さらに多くの VLAN グループを作成できるため、転送テーブルの使用効率が低くなります。この状況に対処するには、CLI を使用して共有サブインターフェイスを同時に追加および削除し、同じ論理デバイスのグループに対して同じサブインターフェイスのセットを維持する必要があります。

詳細については、次のシナリオを参照してください。これらのシナリオは、次のインターフェイスと論理デバイスから始まります。

- 同じ親で設定された共有サブインターフェイス：Port-Channel1.100（VLAN 100）、Port-Channel1.200（VLAN 200）、Port-Channel1.300（VLAN 300）
- 論理デバイス グループ：LD1、LD2、LD3、LD4

シナリオ 1：**あるサブインターフェイスを 1 つの論理デバイスから削除するが、他の論理デバイスに割り当てられたままにする**

サブインターフェイスは削除しないでください。アプリケーション設定で無効にするだけにしてください。サブインターフェイスを削除する必要がある場合は、一般に共有インターフェイスの数を減らして、転送テーブルに収まるようにする必要があります。

シナリオ 2：**1 つの論理デバイスからセット内のすべてのサブインターフェイスを削除する**

CLI で論理デバイスからセット内のすべてのサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。

1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status         INTF         Vlan Status
1    1         configured
                                          100  present
                                          200  present
                                          300  present
2048 512       configured
                                          0    present
2049 511       configured
                                          0    present
firepower(fxos)# exit
firepower#
```

2. 変更する論理デバイスに割り当てられている共有サブインターフェイスを表示します。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # show external-port-link

External-Port Link:
    Name                           Port or Port Channel Name Port Type          App
 Name   Description
    ------------------------------ ------------------------- ------------------
---------- -----------
    Ethernet14_ftd                 Ethernet1/4               Mgmt               ftd
    PC1.100_ftd                    Port-channel1.100         Data Sharing       ftd
    PC1.200_ftd                    Port-channel1.200         Data Sharing       ftd
    PC1.300_ftd                    Port-channel1.300         Data Sharing       ftd
```

3. 論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```
firepower /ssa/logical-device # delete external-port-link PC1.100_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.200_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

シナリオ 3：グループ内のすべての論理デバイスから 1 つのサブインターフェイスを削除する

CLI でグループ内のすべての論理デバイスからサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。次に例を示します。

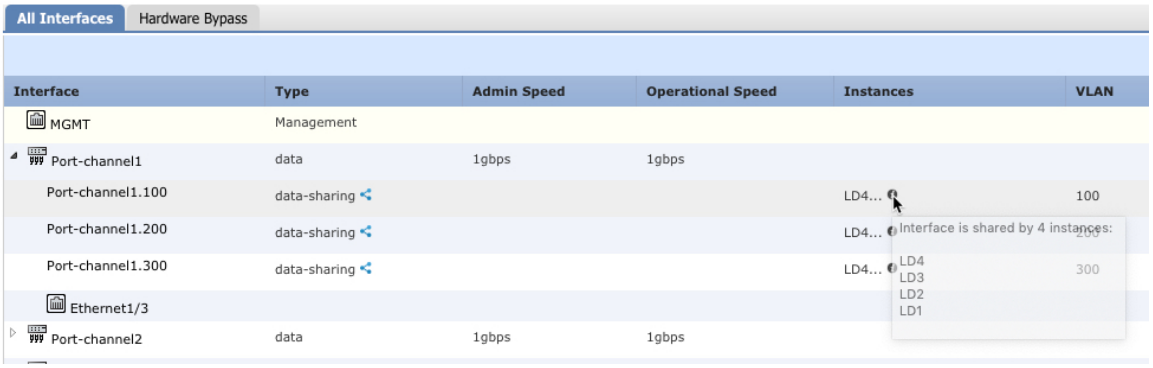
1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
```

```
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status          INTF          Vlan Status
1    1         configured
                                             100  present
                                             200  present
                                             300  present
2048 512       configured
                                             0    present
2049 511       configured
                                             0    present
```

2. 各論理デバイスに割り当てられているインターフェイスを表示し、共通の共有サブインターフェイスに注目してください。同じ親インターフェイス上に存在する場合、それらは 1 つの VLAN グループに属し、**show ingress-vlan-groups** リストと一致しているはずです。Firepower Chassis Manager では、各共有サブインターフェイスにカーソルを合わせて、割り当てられているインスタンスを確認できます。

図 *6*: 共有インターフェイスごとのインスタンス



CLI では、割り当てられたインターフェイスを含むすべての論理デバイスの特性を表示できます。

```
firepower# scope ssa
firepower /ssa # show logical-device expand

Logical Device:
    Name: LD1
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:
```

```
        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:25

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]

    Name: LD2
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:28

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]

    Name: LD3
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd
```

```
    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:2B

        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]

    Name: LD4
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Ok
    Template Name: ftd

    External-Port Link:
        Name: Ethernet14_ftd
        Port or Port Channel Name: Ethernet1/4
        Port Type: Mgmt
        App Name: ftd
        Description:

        Name: PC1.100_ftd
        Port or Port Channel Name: Port-channel1.100
        Port Type: Data Sharing
        App Name: ftd
        Description:

        Name: PC1.200_ftd
        Port or Port Channel Name: Port-channel1.200
        Port Type: Data Sharing
        App Name: ftd
        Description:

        System MAC address:
            Mac Address
            -----------
            A2:F0:B0:00:00:2E
```

```
        Name: PC1.300_ftd
        Port or Port Channel Name: Port-channel1.300
        Port Type: Data Sharing
        App Name: ftd
        Description:

[...]
```

3. 各論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```
firepower /ssa # scope logical device LD1
firepower /ssa/logical-device # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD2
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD3
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD4
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

シナリオ 4：1 つまたは複数の論理デバイスにサブインターフェイスを追加する

CLI でグループ内のすべての論理デバイスにサブインターフェイスを追加し、その後、その追加が同時になるように設定を保存します。

1. 各論理デバイスにサブインターフェイスを追加してから、設定を保存します。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD2
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD3
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD4
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
 ftd
firepower /ssa/logical-device/external-port-link* # commit-buffer
firepower /ssa/logical-device/external-port-link #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

2. Port-Channel1.400 VLAN ID が VLAN グループ 1 に追加されたことを確認できます。

```
firepower /ssa/logical-device/external-port-link # connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status         INTF         Vlan Status
1    1         configured
                                          200  present
                                          100  present
                                          300  present
                                          400  present
2048 512       configured
                                          0    present
2049 511       configured
                                          0    present
firepower(fxos)# exit
firepower /ssa/logical-device/external-port-link #
```

インターフェイスの履歴

機能名	プラットフォームリリース	機能情報
Firepower Threat Defense 動作リンク状態と物理リンク状態の同期	2.9.1	シャーシでは、Firepower 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。Firepower 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。Firepower Threat Defenseからの同期がない場合は、たとえば、Firepower 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、Firepower 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、 Firepower Threat Defense が処理できるようになる前に外部ルータが Firepower 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。 （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 Firepower Threat Defense ではサポートされません。ASA ではサポートされていません。 新規/変更された Firepower Chassis Manager 画面：[Logical Devices] > [Enable Link State] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail**

機能名	プラットフォームリリース	機能情報
クラスタ 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）	2.8.1	マルチインスタンスクラスタで使用するために、クラスタ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。各クラスタには一意のクラスタ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。複数のクラスタタイプのインターフェイスが許可されるようになりました。 新しい/変更された画面： **[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
500 Vlan のサポート（不測事態がない場合）	2.7.1	以前は、親インターフェイスの数とその他の導入の決定事項に応じて、250 から 500 の VLAN がサポートされていました。すべてのケースで 500 の VLAN を使用できるようになりました。
コンテナ インスタンスで使用される VLAN サブインターフェイス	2.4.1	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。 （注） Firepower Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** 新規/変更された FMC 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ
コンテナ インスタンスのデータ共有インターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、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。 （注） Firepower Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Type]**
オン モードでのデータ EtherChannel のサポート	2.4.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Edit Port Channel] > [Mode]**

機能名	プラットフォームリリース	機能情報
Firepower Threat Defense インライン セットでの EtherChannel のサポート	2.1(1)	Firepower 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。
Firepower Threat Defense のインライン セット リンク ステート伝達サポート	2.0(1)	Firepower 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、Firepower 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。
ハードウェア バイパス ネットワーク モジュールのサポート Firepower Threat Defense	2.0(1)	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。 新規/変更された FMC 画面： **[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）]**
Firepower Threat Defense の Firepower イベント タイプ インターフェイス	1.1.4	Firepower Threat Defense で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、Firepower Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Firepower Threat Defense 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。FMC 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。 新規/変更された Firepower Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Type]**

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。