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 コンフィギュレーション 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

Firepower 4100/9300 シャーシは、物理インターフェイス、コンテナ インスタンスの LAN 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論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

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

FirePOWER **connect local-mgmt**

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

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

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を及ぼすことがあります。を参照してください。共有インターフェイスの拡張性 （3 ページ）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、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。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス （2 ページ）を参照してください。

- 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-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。
- 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。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ので、シャーシとアプリケーションの間に不一致が生じることがあります。

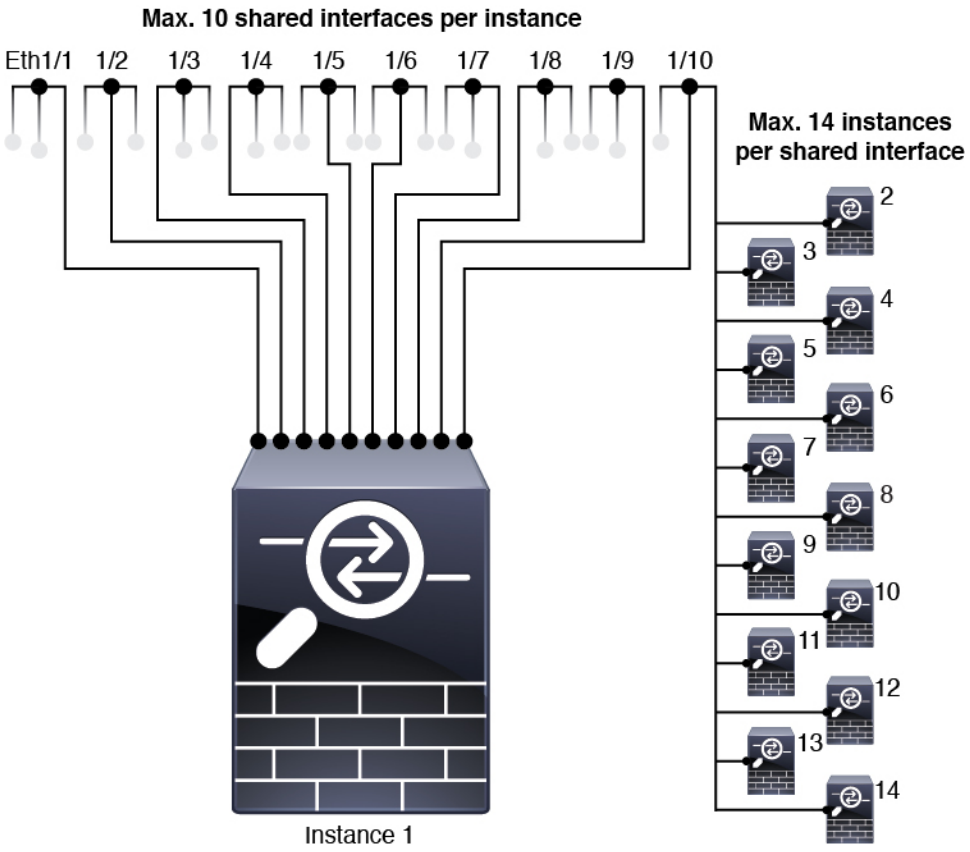
アプリケーションにおけるインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、アプリケーション内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

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場合、シャーシは一意の 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を使用すると、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルのサイズ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他の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ついては、次の制限事項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、拡張性が高いものから低いものへの順序で次の手順に従います。

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。

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 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 *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	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（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（1 ea.） • 11（1 ea.） • 11（1 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%
33： • *11*（*1 ea.*） • *11*（*1 ea.*） • *12*（*1 ea.*）	*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（1 ea.）	**1**	**6**： • インスタンス 1 - インスタンス 6	25 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
30： • 10（5 ea.） • 10（5 ea.） • 10（5 ea.）	**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（6 ea.）	**2**	**5**： • インスタンス 1 - インスタンス 5	28%
30： • 12（6 ea.） • 18（6 ea.）	**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 %
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（6 ea.） • 12（6 ea.）	**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 *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	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（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
33： • 11（1 ea.） • 11（1 ea.） • 11（1 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.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
165： • 55（5 ea.） • 55（5 ea.） • 55（5 ea.）	**3**： • 1 • 1 • 1	**33**： • インスタンス 1 - インスタンス 11 • インスタンス 12 - インスタンス 22 • インスタンス 23 - インスタンス 33	98%

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

1 つの SM 44 を備えた Firepower 9300

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

1 つの SM-44 を備えた Firepower 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	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（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（1 ea.） • 7（1 ea.）	**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（8 ea.） • 16（8 ea.）	**2**	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	20 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率（%）
32： • 8 • 8 • 8 • 8	**2**	**4**： • インスタンス 1 • インスタンス 2 • インスタンス 3 • インスタンス 4	25 %
32： • 16（8 ea.） • 16（8 ea.）	**4**： • 2 • 2	**4**： • インスタンス 1 - インスタンス 2 • インスタンス 3 - インスタンス 4	24 %
24： • 8 • 8 • 8	**8**	**3**： • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10： • 10（2 ea.）	**10**	**5**： • インスタンス 1 - インスタンス 5	69%
10： • 6（2 ea.） • 4（2 ea.）	**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 *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	インスタンス数	転送テーブルの使用率（%）
112： • 112（8 ea.）	**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（1 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
14： • 7（1 ea.） • 7（1 ea.）	**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（8 ea.）	**1**	**14**： • インスタンス 1 - インスタンス 14	46 %
112： • 56（8 ea.） • 56（8 ea.）	**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（8 ea.）	**2**	**14**： • インスタンス 1 - インスタンス 14	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率（%）
112： • 56（8 ea.） • 56（8 ea.）	**4**： • 2 • 2	**14**： • インスタンス 1 - インスタンス 7 • インスタンス 8 - インスタンス 14	37 %
140： • 140（10 ea.）	**10**	**14**： • インスタンス 1 - インスタンス 14	46 %
140： • 70（10 ea.） • 70（10 ea.）	**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、**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ときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。

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

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。

- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 のすべての 3 つのモジュール アプリケーション インスタンスは、1 つの論理デバイスに属しています。

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

論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

アプリケーション インスタンスは次の展開タイプで実行します。

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

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

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

コンテナ インスタンス インターフェイス

コンテナ インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、FXOSでVLANサブインターフェイスを作成し、複数のインスタンス間でインターフェイス（VLANまたは物理）を共有することができます。ネイティブのインスタンスは、VLANサブインターフェイスまたは共有インターフェイスを使用できません。共有インターフェイスの拡張性 （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 （35 ページ）を参照してください。

シャーシがパケットを分類する方法

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

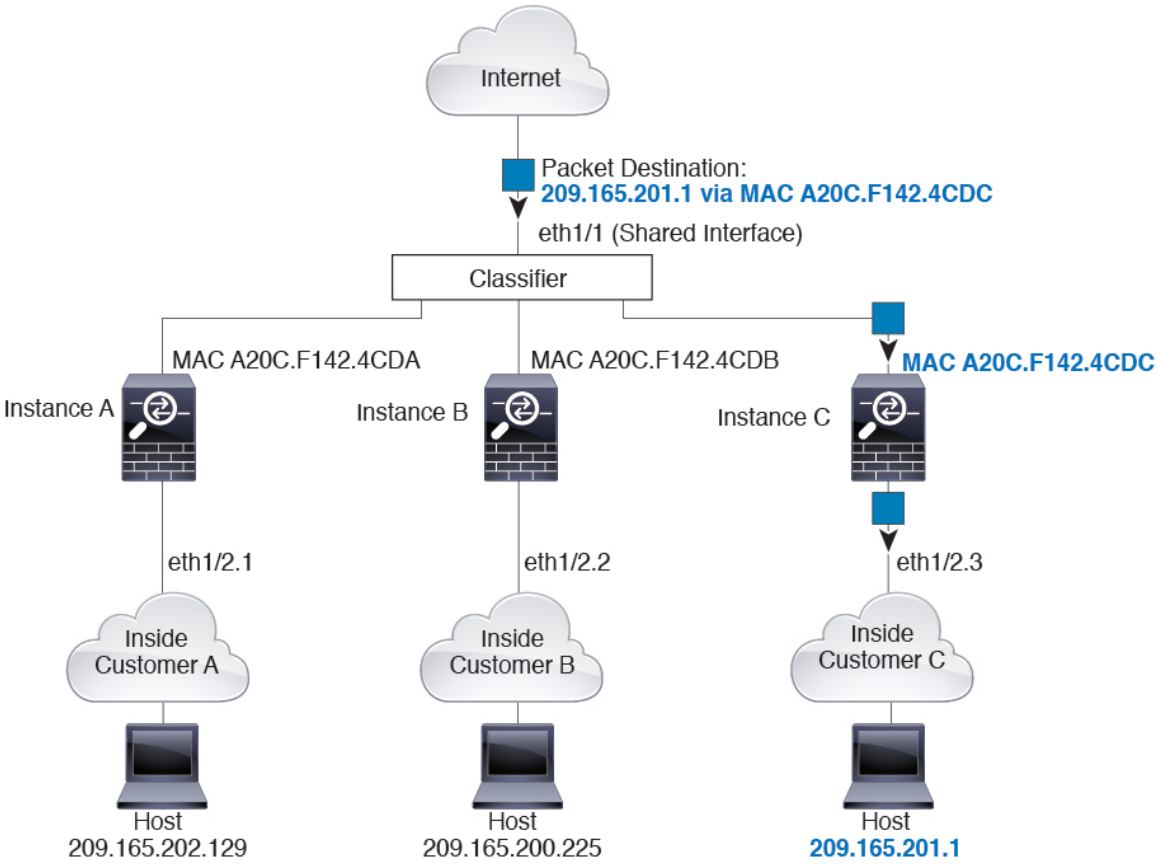
- 一意のインターフェイス：1 つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。ブリッジグループ メンバー インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意の MAC アドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイ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

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

分類例

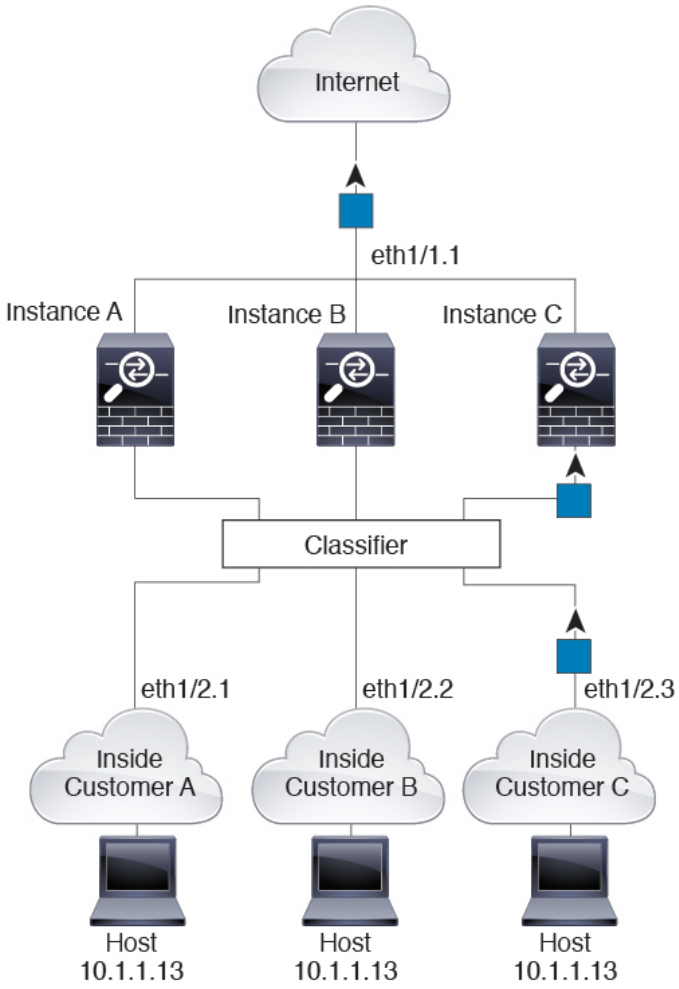
次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンスCにはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

図 *1 : MAC* アドレスを使用した共有インターフェイスのパケット分類



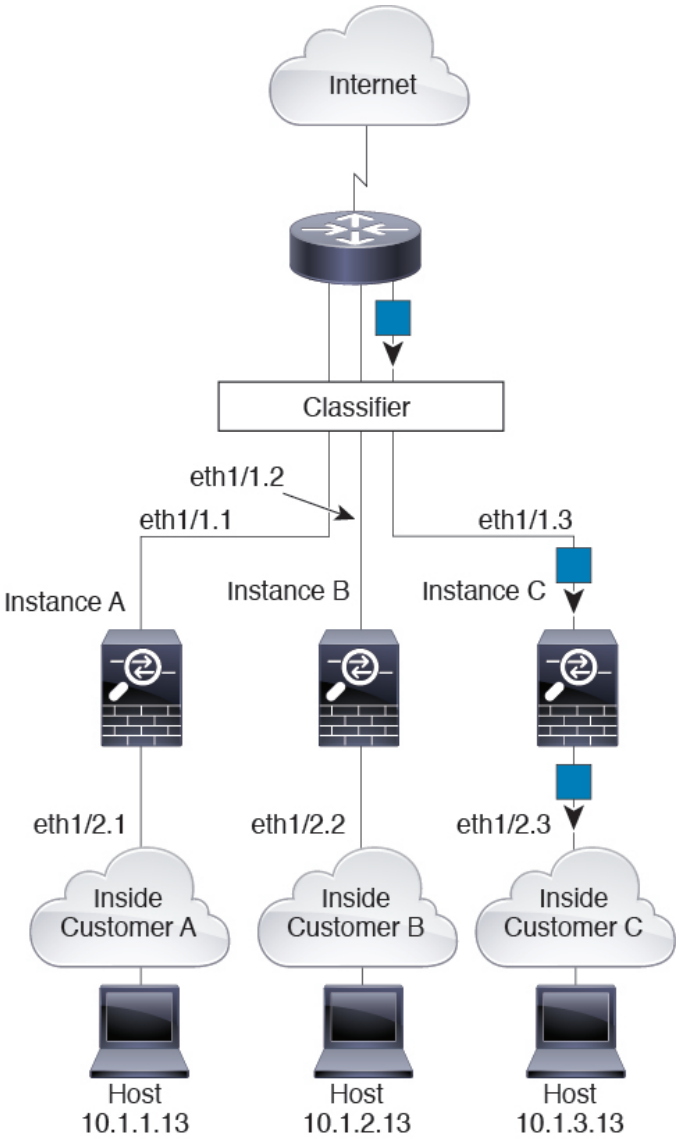
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *2:* 内部ネットワークからの着信トラフィック



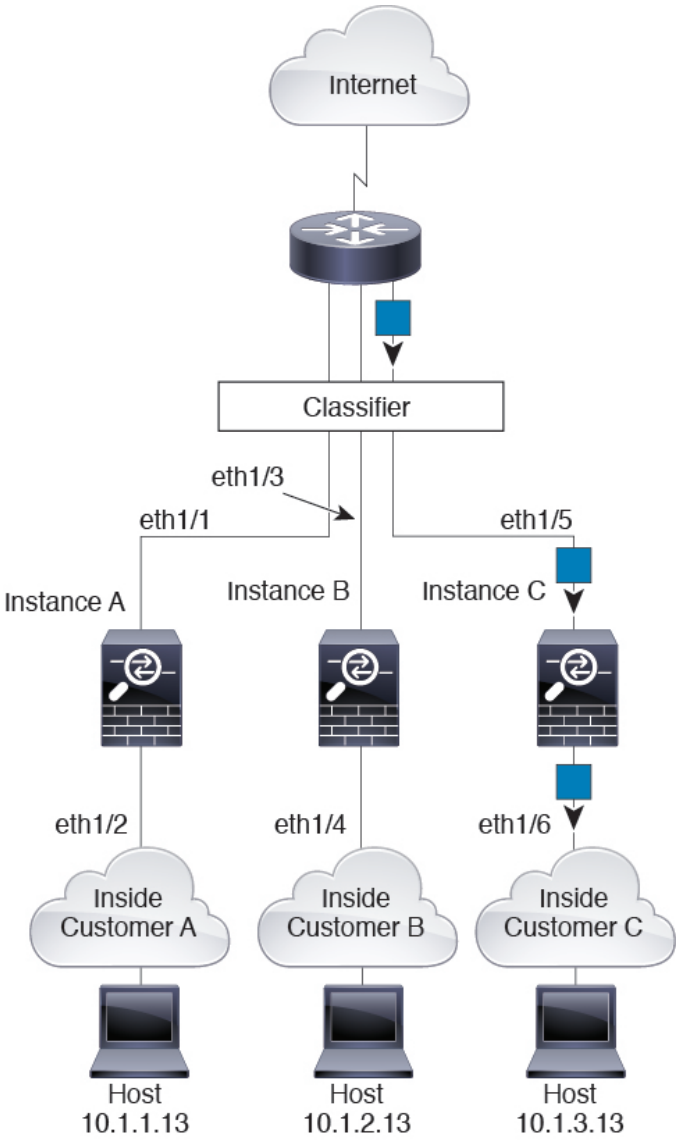
トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *3:* トランスペアレント ファイアウォール インスタンス



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

図 *4 : FTD* のインライン セット

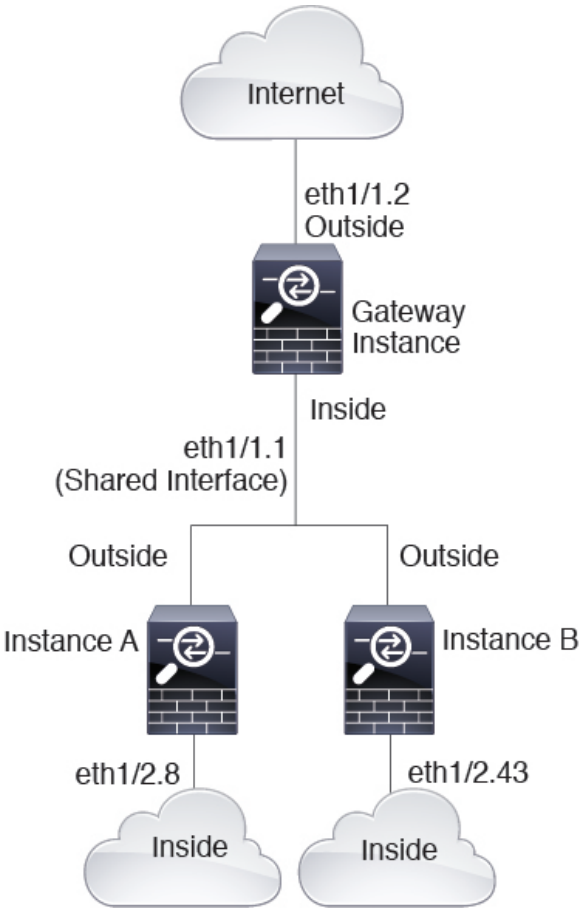


コンテナ インスタンスのカスケード

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

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

図 *5:* コンテナ インスタンスのカスケード

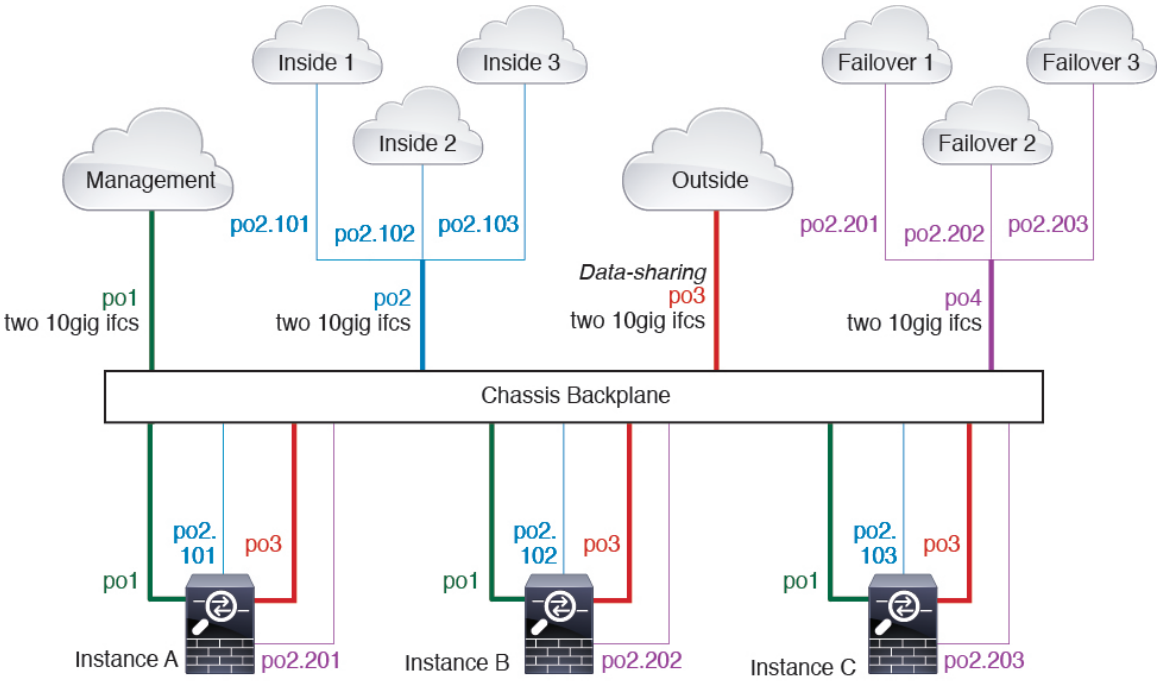


一般的な複数インスタンス展開

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

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

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



コンテナ インスタンス インターフェイスの自動 MAC アドレス

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

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

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

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

FXOS シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

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

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、シャーシは 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスはシャーシ ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

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

A2**F1.03***zz.zzzz*

コンテナ インスタンスのリソース管理

コンテナ インスタンスごとのリソース使用率を指定するには、FXOS で 1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開する場合は、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。モデルごとの使用可能なリソースを表示するには、コンテナ インスタンスの要件と前提条件 （26 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 （37 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、それぞれ 10 個のインスタンスを使用する 2 つのシャーシがある場合、10 個のハイ アベイラビリティ ペアを作成できます。ハイ アベイラビリティは FXOS で構成されません。各ハイ アベイラビリティ ペアはアプリケーション マネージャで構成します。

各装置で同じリソース プロファイル属性を使用する必要があります。

各ハイ アベイラビリティ ペアには専用のフェールオーバー リンクが必要です。データ共有インターフェイスを使用することはできません。親インターフェイスでサブインターフェイスを作成し、各インスタンスのサブインターフェイスを割り当てて、フェールオーバー リンクとして使用することをお勧めします。

（注） クラスタリングはサポートされません。

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	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	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	マルウェア	脅威
3	2	3	2

論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

Firepower 9300 の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- セキュリティモジュール タイプ：Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-36 をモジュール 1、SM-40 をモジュール 2 、SM-44 をモジュール 3 としてインストールできます。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。 同じシャーシに 1 つの SM-24 および 2 つの SM-36 をインストールする場合、クラスタリングは使用できません。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。 ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- ASA および FTD のアプリケーションタイプ：異なるアプリケーション タイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモ

ジュール 2 に ASA をインストールし、モジュール 3 に FTD をインストールすることができます。

- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

Firepower 4100 の要件

Firepower 4100 は複数のモデルに搭載されています。次の要件を参照してください。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100 にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブインスタンスを 1 つのみインストールできます。
- クラスタリング：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASA および FTD のアプリケーションタイプ：Firepower 4100 は、1 つのアプリケーションタイプのみを実行できます。
- FTD コンテナインスタンスのバージョン：同じモジュール上で異なるバージョンの FTD を個別のコンテナインスタンスとして実行できます。

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 4115	7	46	162 GB	308 GB

モデル	最大コンテナインスタンス数	使用可能な CPU コア数	使用可能な RAM	使用可能なディスク容量
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 セキュリティモジュール	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 セキュリティモジュール	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 セキュリティ モジュール	13	78	334 GB	1359 GB
Firepower 9300 SM-44 セキュリティ モジュール	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 セキュリティモジュール	15	94	334 GB	1341 GB
Firepower 9300 SM-56 セキュリティ モジュール	18	110	334 GB	1314 GB

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 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

- ネットワーク展開に応じて、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。

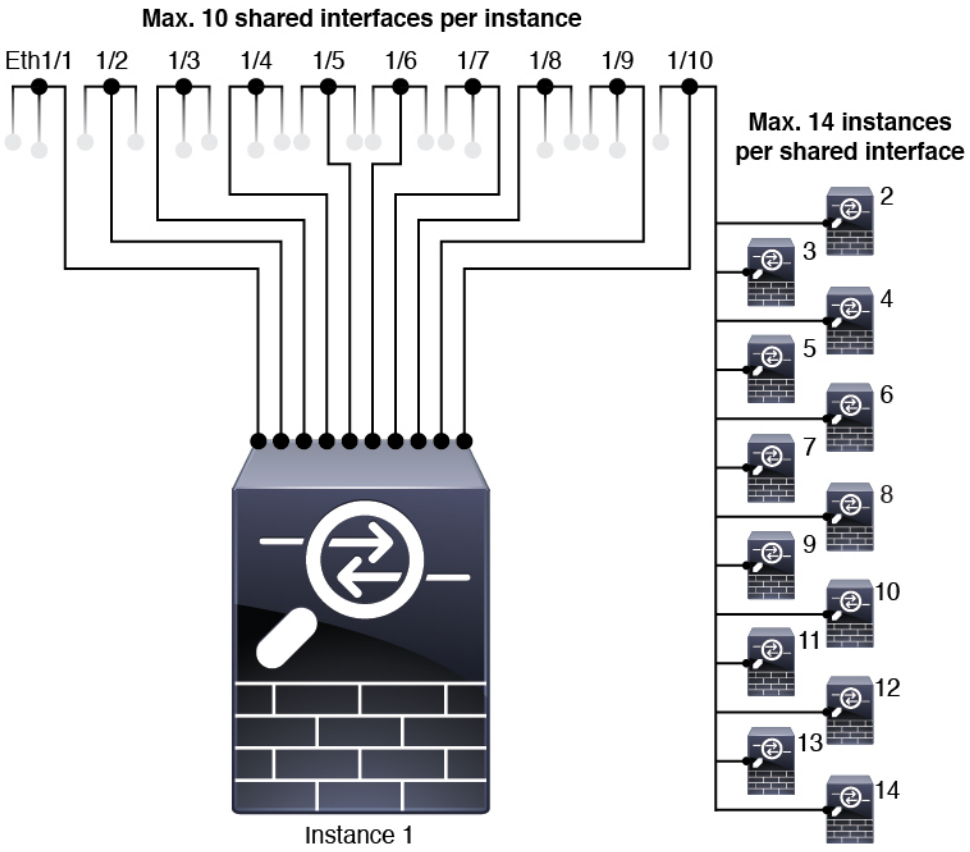
（注） コンテナインスタンスに親インターフェイスを割り当てる場合、タグなし（非 VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。

- 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。
  - 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、Instance1 から 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。



- 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。
  - 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。

次のインライン 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。

ハードウェア バイパス

- FTD 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。
- FTD 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 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 （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、 高可用性 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

- ASA ではマルチ コンテキスト モードはサポートされていません。
- 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ディセーブルになっています。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。

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

[Interfaces] ページには、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 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。

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。

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

[**すべてのインターフェイス（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の [Edit] をクリックし、[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イネーブルにするには、[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） [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 [Auto Negotiation] がサポートされている場合は、[Yes] または [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 [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 インターフェイスはアクティブ モードのみをサポートします。

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 [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。

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

[**すべてのインターフェイス（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 **[Add Port Channel]**をクリックして、**[Add Port Channel]**ダイアログボックスを開きます。

ステップ 3 **[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、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、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 チャネルを有効化するには、**[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 [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、このポートチャネルを Cluster Control Link として使用する場合以外は、**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 リストでメンバー 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 チャネル [Mode]、[Active] または [On] を選択します。

非データまたは非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。同じタイプと速度の最大 16 のインターフェイスを追加できます。

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。

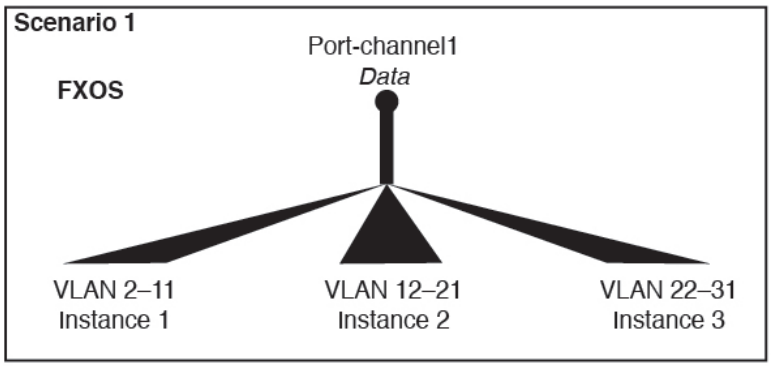
ステップ 11 **[OK]**をクリックします。

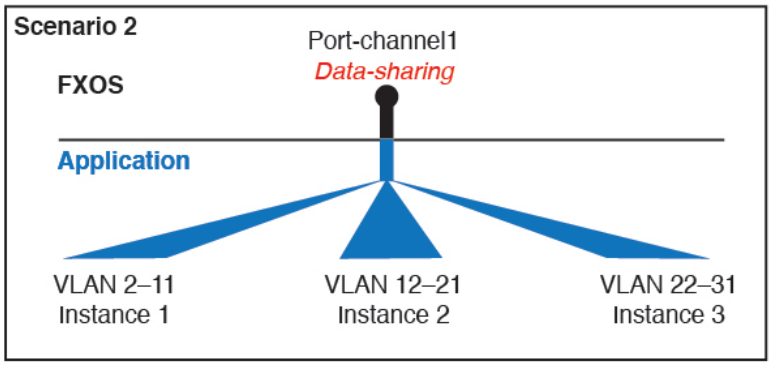
コンテナ インスタンスへの VLAN サブインターフェイスの追加

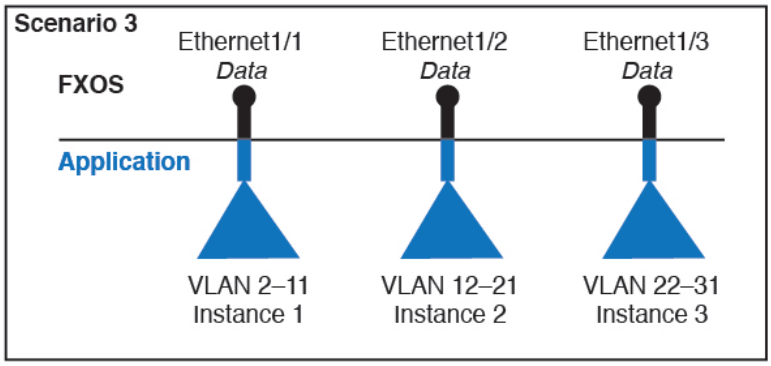
ネットワーク配置に応じて、250 ～ 500 の VLAN サブインターフェイスをシャーシに追加できます。

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 インスタン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。







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 [Interface] 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は、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]（1 ～ 4294967295）を入力します。

この ID は *interface_id.subinterface_id* として親インターフェイスの ID に付加されます。たとえば、サブインターフェイスを ID 100 で Ethernet1/1 に追加する場合、そのサブインターフェイス ID は Ethernet1/1.100 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 [VLAN ID]（1 ～ 4095）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て、その下にあるすべてのサブインターフェイスを表示します。

論理デバイスの設定

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

クラスタ リングについては、Firepower 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使用率を指定するには、1つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 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 （26 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。

使用中のリソースプロファイルの設定を変更することはできません。リソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。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の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。

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]：プロファイルのコア数を 6 ～ 最大数（偶数）で設定します。最大数はシャーシによって異なります。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展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュール クラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

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

始める前に

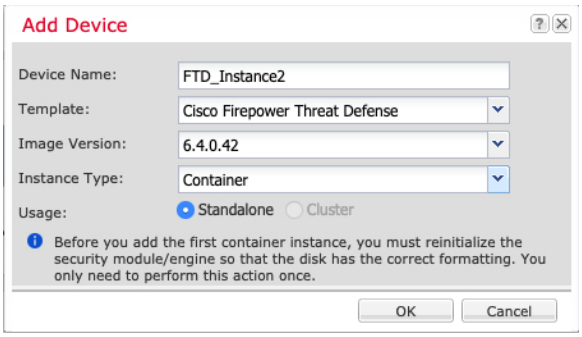
- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。

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

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、[Interfaces] タブの上部に [MGMT] として表示されます）。
- また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック（Web イベントなど）を運ぶ firepower-eventing インターフェイスも作成できます。詳細については、「インターフェイス タイプ （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 （37 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] を選択して、[Reinitialize] アイコン（ ） をクリックします。既存の論理デバイスは削除されて新しいデバイスとして再インストールされるため、ローカルのアプリケーション設定はすべて失われます。ネイティブインスタンスをコンテナインスタンスで置き換えるときには、常にネイティブインスタンスを削除する必要があります。ネイティブインスタンスをコンテナインスタンスに自動的に移行することはできません。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレスや NAT ID
  - DNS サーバの IP アドレス。
  - FTD ホスト名とドメイン名

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

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



a) **デバイス名**を入力します。

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

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

c) [Image Version] を選択します。

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

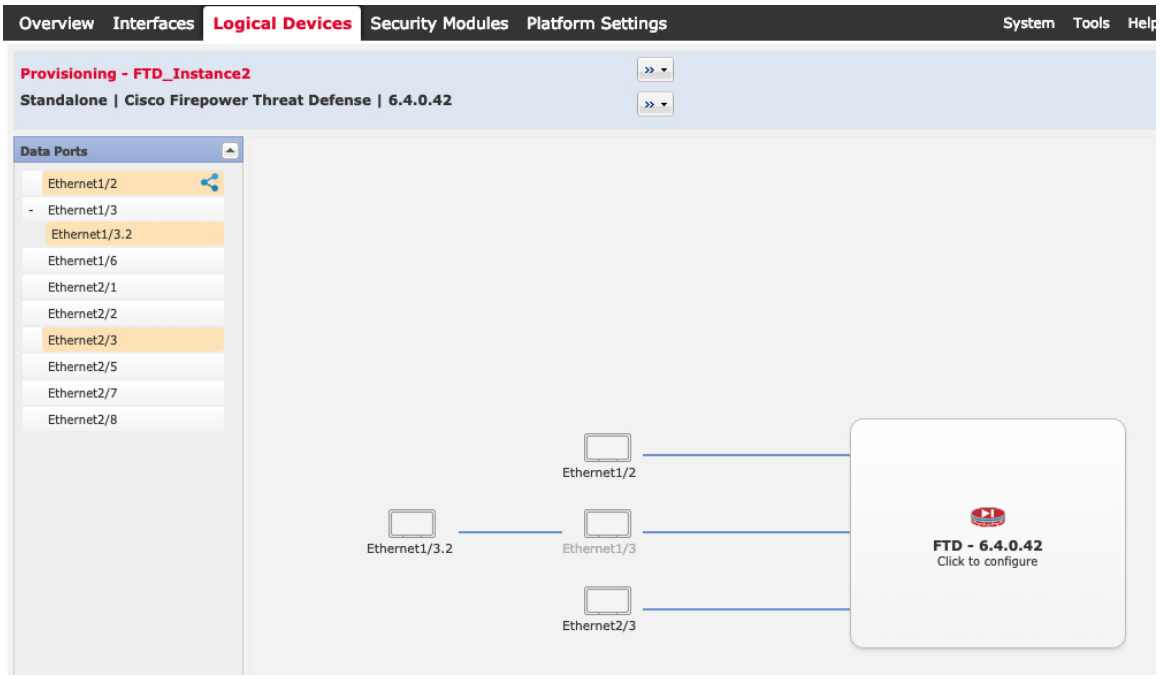
ネイティブ インスタンスはセキュリティ モジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナインスタンスでは、セキュリティ モジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナ インスタンスをインストールできます。

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。

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

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



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

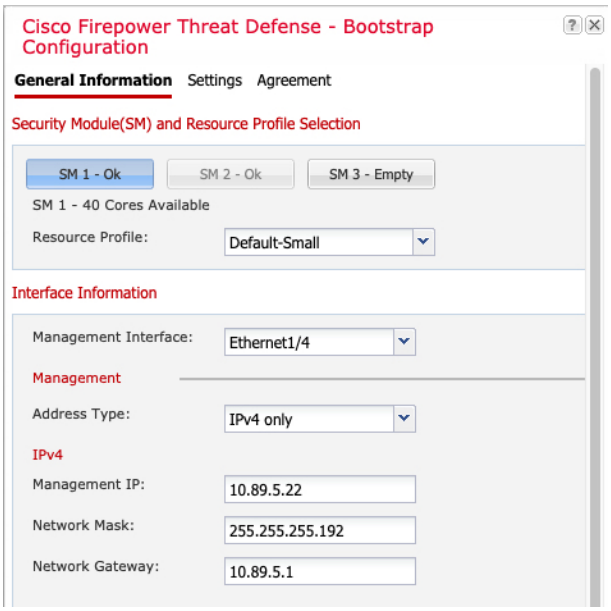
コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナインスタンスに割り当てることができます。データ共有インターフェイスは [Sharing] アイコン（ ） で示されます。

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

ステップ 4 画面中央のデバイス アイコンをクリックします。

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 CCLI 設定のほとんどの値を変更できます。

ステップ 5 [General Information] ページで、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。

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

c) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャー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] として、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6] を選択します。

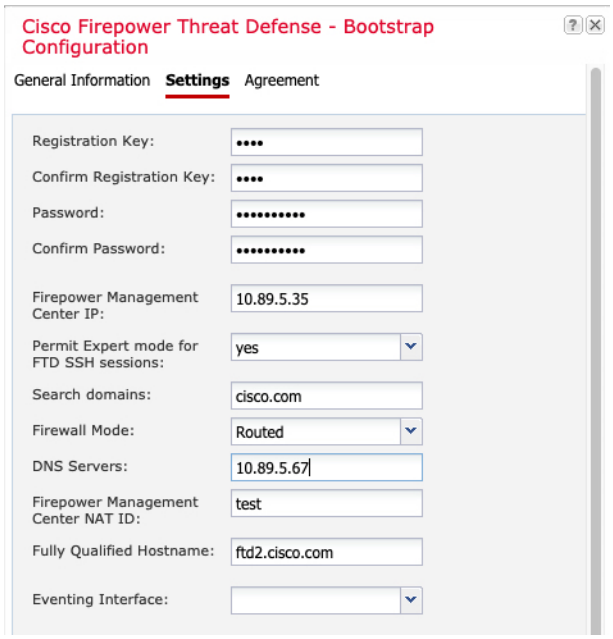
e) [Management IP] アドレスを設定します。

このインターフェイスの一意の IP アドレスを設定します。

f) **ネットワーク マスク**または**プレフィックス長**を入力します。

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 [Settings] タブで、次の手順を実行します。



a) 管理 FMC の [Firepower Management Center IP] を入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

b) **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパートモードでは、高度なトラブルシューティングに 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。[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のみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

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

c) カンマ区切りリストとして [Search Domains] を入力します。

d) [**Firewall Mode**]で[**Transparent**]、または [**Routed**] を選択します。

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

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

e) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

f) FTD の [Fully Qualified Hostname] を入力します。

g) 登録時に FMC とデバイス間で共有する [Registration Key] を入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。FTD を追加するときに、 FMC に同じキーを入力します。

h) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

i) Firepower イベントの送信に使用する [Eventing Interface] を選択します。指定しない場合は、管理インターフェイスが使用されます。

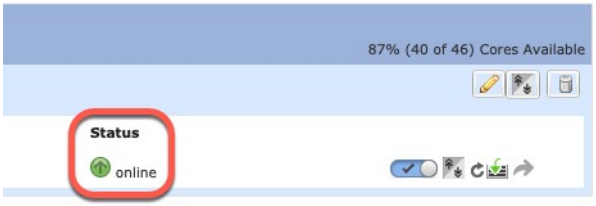
このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

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

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 **[Save]** をクリックします。

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



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

ハイ アベイラビリティ ペアの追加

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、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。

- 同じモデルであること。
- ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
- インターフェイスの数とタイプが同じであること。ハイ アベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。

- 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- 他のハイ アベイラビリティ システム要件については、 高可用性 のシステム要件を参照してください。

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

ステップ 2 各論理デバイスに同一のインターフェイスを割り当てます。

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

これらのインターフェイスは、2 つのシャーシ間でハイ アベイラビリティ トラフィックを交換します。統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバー インターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

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

ステップ 4 論理デバイスでハイ アベイラビリテを有効にします。 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でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

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

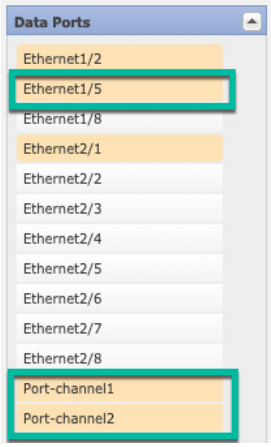
- 物理インターフェイスの設定 （32 ページ）およびEtherChannel（ポート チャネル）の追加 （33 ページ）に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 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がリブートし（管理インターフェイスを変更するとリブートします）、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。

ステップ 1 Firepower Chassis Manager で、[Logical Devices] を選択します。

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

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

まだインターフェイスを削除しないでください。



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

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

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) [Settings] タブで、ドロップダウン リストから新しい [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 アドレスも変更する必要があります。**[Devices]** > **[Device Management]** > **[Device/Cluster]** と移動します。[Management] 領域で、ブートストラップ設定アドレスと一致するように IP アドレスを設定します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 FMC でインターフェイスを同期します。

a) FMC にログインします。

b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

c) [インターフェイス（Interfaces）] タブの左上にある [デバイスの同期（Sync Device）] ボタンをクリックします。

d) 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] ページに表示されます。[クリックして詳細を表示（Click to know more）] リンクをクリックしてインターフェイスの変更内容を表示します。

e) インターフェイスを削除する予定の場合は、古いインターフェイスから新しいインターフェイスに任意のインターフェイス設定を手動で転送します。

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

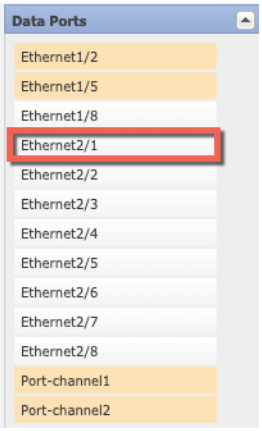
f) [変更の検証（Validate Changes）] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

g) [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 [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

次の手順を使用して、アプリケーションのコンソールに接続します。

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

connect module *slot_number* {**console** | **telnet**}

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

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

例：

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

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

```
Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect ftd *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

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

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- FTD：**exit** と入力

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

Firepower Threat Defense の論理デバイスの履歴

機能	バージョン	詳細
FTD Firepower 4115、4125、および 4145	6.4.0	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1.157 が必要です。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	6.4.0	3 つのセキュリティ モジュール、SM-40、SM-48、および SM-56 が導入されました。 （注） FXOS 2.6.1.157 が必要です。

機能	バージョン	詳細
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	6.4.0	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1.157 が必要です。
モジュール/セキュリティ エンジンのいずれかの FTD コンテナ インスタンスでの SSL ハードウェア アクセラレーションのサポート	6.4.0	これで、モジュール/セキュリティ エンジンのいずれかのコンテナインスタンスに対して SSL ハードウェア アクセラレーションを有効にすることができるようになりました。他のコンテナインスタンスに対して SSL ハードウェア アクセラレーションは無効になっていますが、ネイティブインスタンスには有効になっています。 新規/変更された FXOS コマンド：**config hwCrypto enable** 変更された画面はありません。 （注） FXOS 2.6.1.157 が必要です。

機能	バージョン	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	詳細
		単一のセキュリティエンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブ アプリケーション インスタンスのみ展開できました。 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。 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。 （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。 新規/変更された [Firepower Management Center] 画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ 新規/変更された [Firepower Chassis Manager] 画面： • **[Overview] > [Devices]** • **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** • **[Interfaces] > [All Interfaces] > [Type]**

機能	バージョン	詳細
		• **[Logical Devices] > [Add Device]** • **[Platform Settings] > [Mac Pool]** • **[Platform Settings] > [Resource Profiles]** 新規/変更された FXOS コマンド：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**createresource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	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	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。FXOS にクラスタを展開する際にネットワークを設定できるようになりました。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンクインターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： • **[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 新規/変更された FXOS コマンド：**set cluster-control-link network** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	詳細
オン モードでのデータ EtherChannel のサポート	6.3.0	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。他の種類の EtherChannel は、アクティブ モードのみサポートしています。 新規/変更された [Firepower Chassis Manager] 画面： • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [ポート チャネルの編集（Edit Port Channel）] > [モード（Mode）]** 新規/変更された FXOS コマンド：**set port-channel-mode** サポートされるプラットフォーム：Firepower 4100/9300
FTD インライン セットでの EtherChannel のサポート	6.2.0	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。 サポートされるプラットフォーム：Firepower 4100/9300
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	FTD のシャーシ間クラスタリングを有効化できます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	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	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。 新しい/変更された画面： • **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 4100/9300
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	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。 新規/変更された FXOS コマンド：**show fault |grep link-down**、**show interface detail** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン	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	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。 新規/変更された [Firepower Chassis Manager] 画面： • **[論理デバイス（Logical Devices）] > [構成（Configuration）]** 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** サポートされるプラットフォーム：Firepower 4100/9300