Firepower Threat Defense 用のクラスタリング

クラスタリングを利用すると、複数の FTD ユニットを 1 つの論理デバイスにグループ化できます。クラスタリングは、Firepower 9300 および Firepower 4100 シリーズ 上の FTD デバイスでのみサポートされます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。クラスタリングでサポートされない機能 （7 ページ）を参照してください。

Firepower4100/9300シャーシでのクラスタリングについて

クラスタは、1 つの論理ユニットとして機能する複数のデバイスから構成されます。Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポート チャネル 48）を作成します。シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通

信にFirepower 9300バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信用にこのEtherChannelに物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタ ブートストラップ コンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成がFirepower 4100/9300 シャーシ スーパーバイザからプッシュされます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのようにEtherChannelに制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部でEtherChannelテクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。 シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。

  （注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。クラスタリングの参考資料 （37 ページ）も参照してください。

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがFirepower 4100/9300 シャーシ スーパバイザから各ユニットに対してプッシュされます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバの 1 つが**マスター** ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバは**スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （7 ページ）を参照してください。

クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。シャーシ間クラスタリングでは、このインターフェイスにメンバインターフェイスはありません。このクラスタ タイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

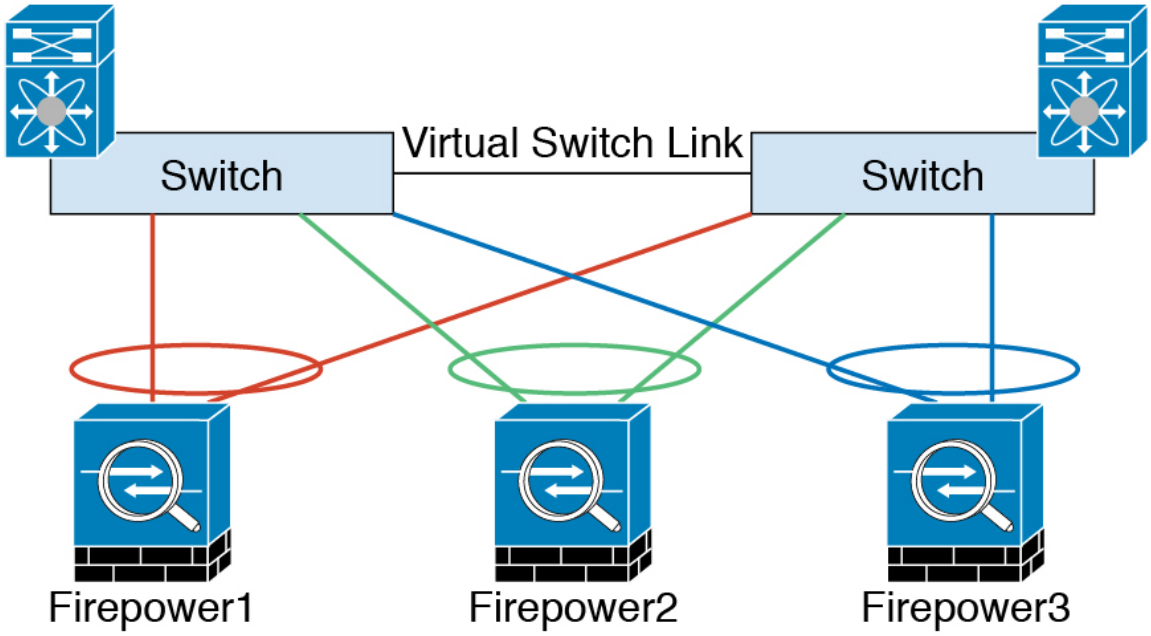
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 9300 シャーシ インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット 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 インターフェイスの IP アドレスを自動生成します。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ2スイッチングだけが許可されています。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インター

フェイスによって各ユニットに直接接続できます。この管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。管理インターフェイスは、独自のローカル認証、IP アドレス、およびスタティック ルーティングを使用します。クラスタの各メンバーは、管理ネットワーク上で、それぞれに異なる IP アドレスを使用します。これらの IP アドレスは、ブートストラップ構成の一部としてユーザが設定します。

管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。診断論理インターフェイスはオプションであり、ブートストラップ構成の一部としては設定されません。診断インターフェイスは、他のデータ インターフェイスと併せて設定できます。診断インターフェイスを設定する場合、メイン クラスタ IP アドレスを、そのクラスタの固定アドレス（常に現在のマスターユニットに属するアドレス）として設定します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカル アドレスを使用できるようにします。このメイン クラスタ IP アドレスによって、診断アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタへのアクセスをシームレスに続行できます。TFTP や syslog などの発信管理トラフィックの場合、マスター ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

クラスタ インターフェイス

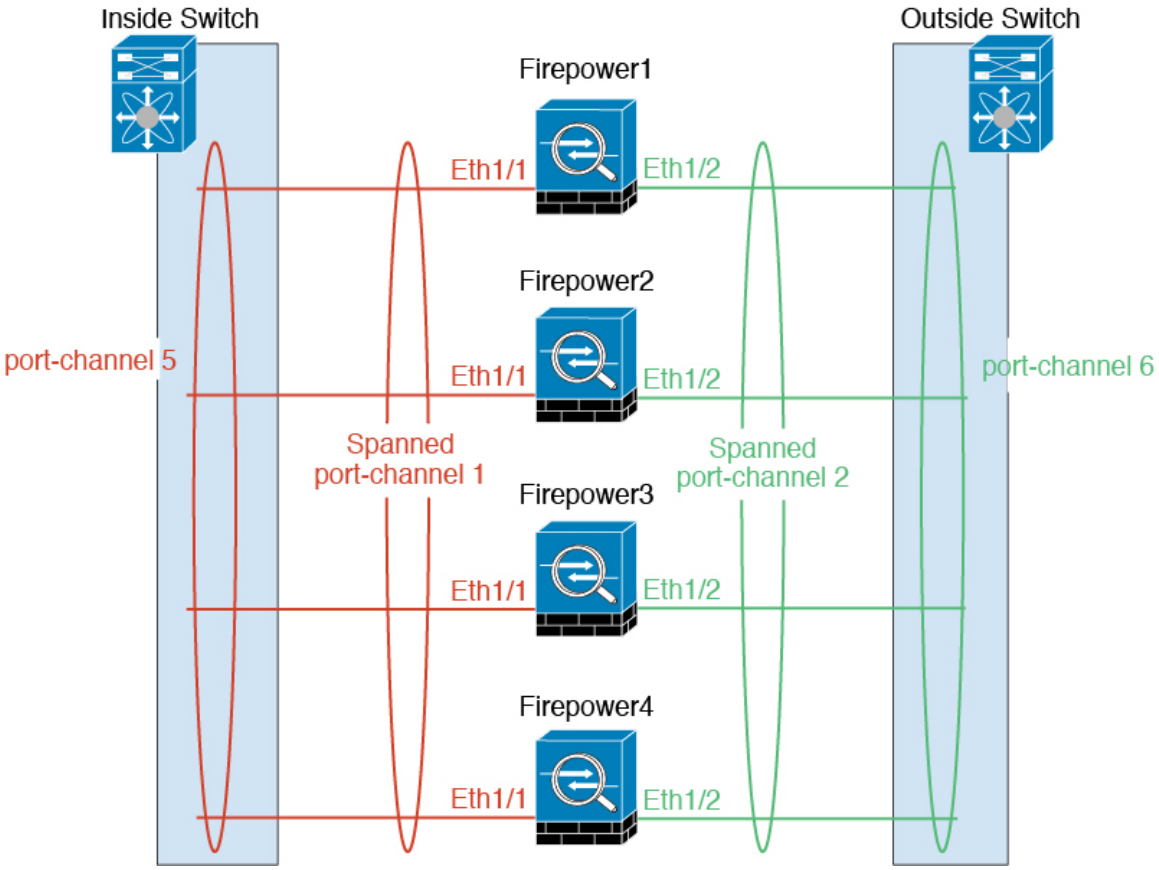
シャーシ内クラスタリングでは、物理インターフェイスと EtherChannel（ポート チャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

シャーシ間クラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシの同じメンバー インターフェイスを含みます。上流に位置するスイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロード バランシング機能を基本的動作の一部として備えています。



VSS または vPC への接続

インターフェイスの冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

コンフィギュレーションの複製

クラスタ内のすべてのユニットは、単一の設定を共有します。設定変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

Firepower Threat Defense の機能とクラスタリング

FTD の一部の機能はクラスタリングではサポートされず、一部はマスター ユニットのみでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- リモート アクセス VPN（SSL VPN および IPsec VPN）
- DHCP クライアント、サーバ、およびプロキシ。DHCP リレーはサポートされています。
- 高可用性
- 統合ルーティングおよびブリッジング
- デッド接続検出（DCD）

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバ ユニットからマスター ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスター ユニットに送り返されます。

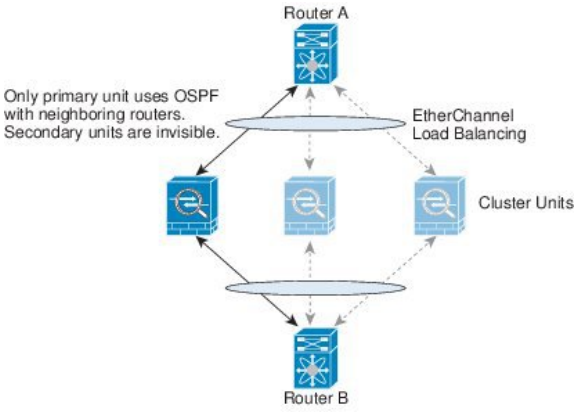
中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
- スタティック ルート モニタリング

ダイナミック ルーティングとクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *1:* ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の Firepower Threat Defense デバイス に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、着信と発信とで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない Firepower Threat Defense デバイス に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシー チェックの結果に応じてパケットの接続を最終的には作成しない可能性があるため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- ダイナミック PAT 用 NAT プール アドレス分散：マスター ユニットは、アドレスをクラスタ全体に均等に分配します。メンバが接続を受信したときに、そのメンバのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバにはまだ使用可能なア

ドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- マスター ユニットによって管理されるダイナミック NAT xlate：マスター ユニットが xlate テーブルを維持し、スレーブ ユニットに複製します。ダイナミック NAT を必要とする接続をスレーブ ユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

SIP インスペクションとクラスタリング

制御フローは、任意のユニットで作成できますが（ロードバランシングのため）、その子データ フローは同じユニットに存在する必要があります。

syslog とクラスタリング

- クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ設定で割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。

SNMP とクラスタリング

SNMP エージェントは、個々の Firepower Threat Defense デバイス を、その診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスター ユニットのポーリングに失敗します。

FTP とクラスタリング

- FTP D チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバーによって所有されている場合は、D チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

Cisco TrustSec とクラスタリング

マスター ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。マスター ユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致決定を下せます。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスター ユニットだけが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスター ユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的にマスター ユニットに転送されます。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

クラスタリングのライセンス

FTD はスマート ライセンスを使用します。個別のユニットではなく、クラスタ全体にライセンスを割り当てます。ただし、クラスタの各ユニットは機能ごとに個別のライセンスを使用します。

クラスタ メンバーを FMC に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタのライセンスは、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [ライセンス（License）]** 領域で変更できます。

（注） FMCにライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、FMC にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのスレーブ ユニットがクラスタをいったん離れてから再参加することになります。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

- Firepower 9300：。クラスタには最大 6 ユニットを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。シャーシ内クラスタリングとシャーシ間クラスタリングをサポートします。
- Firepower 4100 シリーズ：シャーシ間クラスタリングを使用して最大 6 ユニットをサポートします。

シャーシ間のクラスタリング ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower 4100 シリーズ：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシに設置されているセキュリティ モジュールの数はさまざまでかまいません。
- イメージアップグレード時を除き、同じ FXOS ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングのすべてのデータ インターフェイスが EtherChannel であることに注意してください。（インターフェイス モジュールの追加または削除や、EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（スレーブ ユニットから始めて、マスターで終わります）。

- 同じ NTP サーバを使用する必要があります。 また、Firepower Threat Defense の場合、Firepower Management Center は同じ NTP サーバを使用する必要があります。手動で時間を設定しないでください。

シャーシ間クラスタリングのスイッチ要件

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

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- ASR 9006 でデフォルト以外の MTU を設定する場合は、クラスタ デバイスの MTU よりも 14 バイト大きい ASR インターフェイス MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタ デバイスの MTU と ASR *IPv4* MTU を一致させる必要があることに注意してください。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内のデバイスへのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再起動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効にすることで、スパンド EtherChannel との互換性を高めることができます。

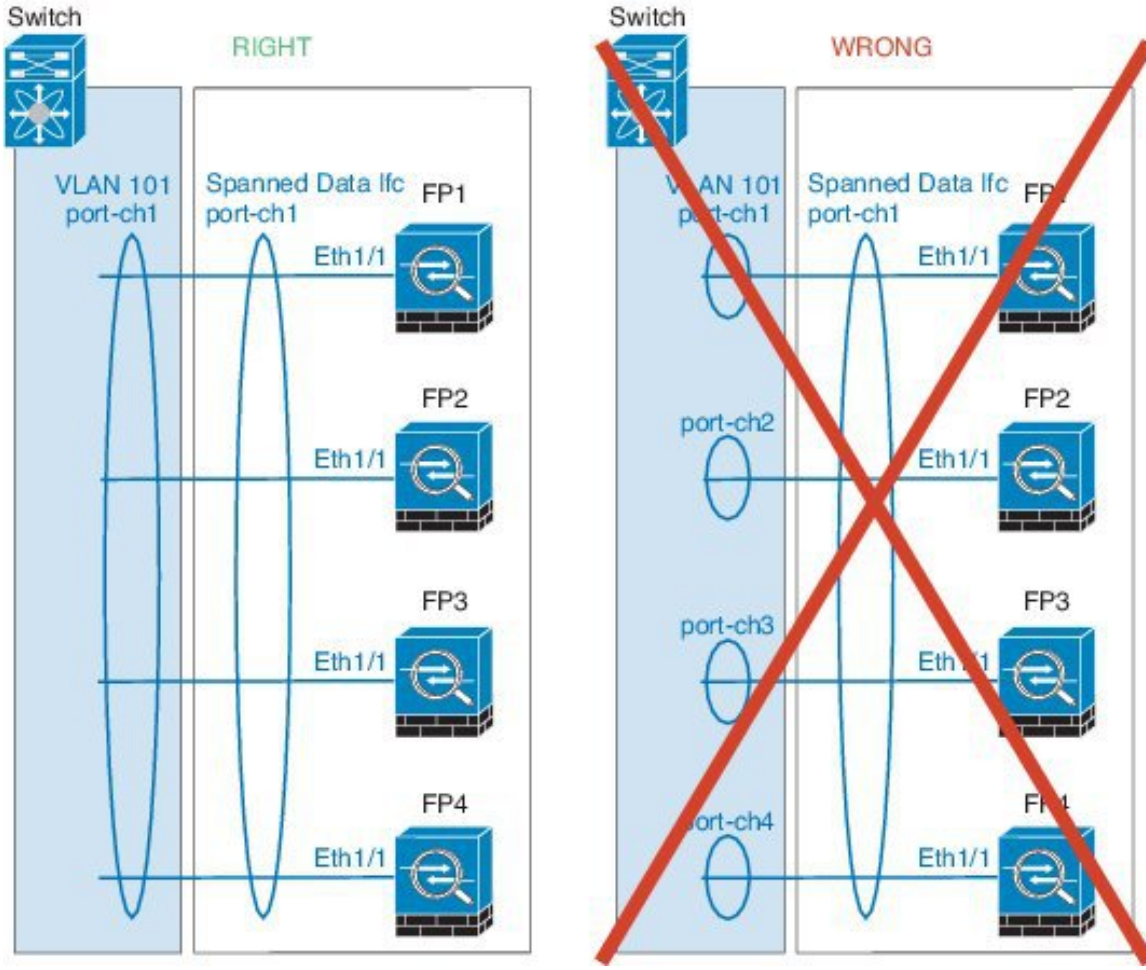
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

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

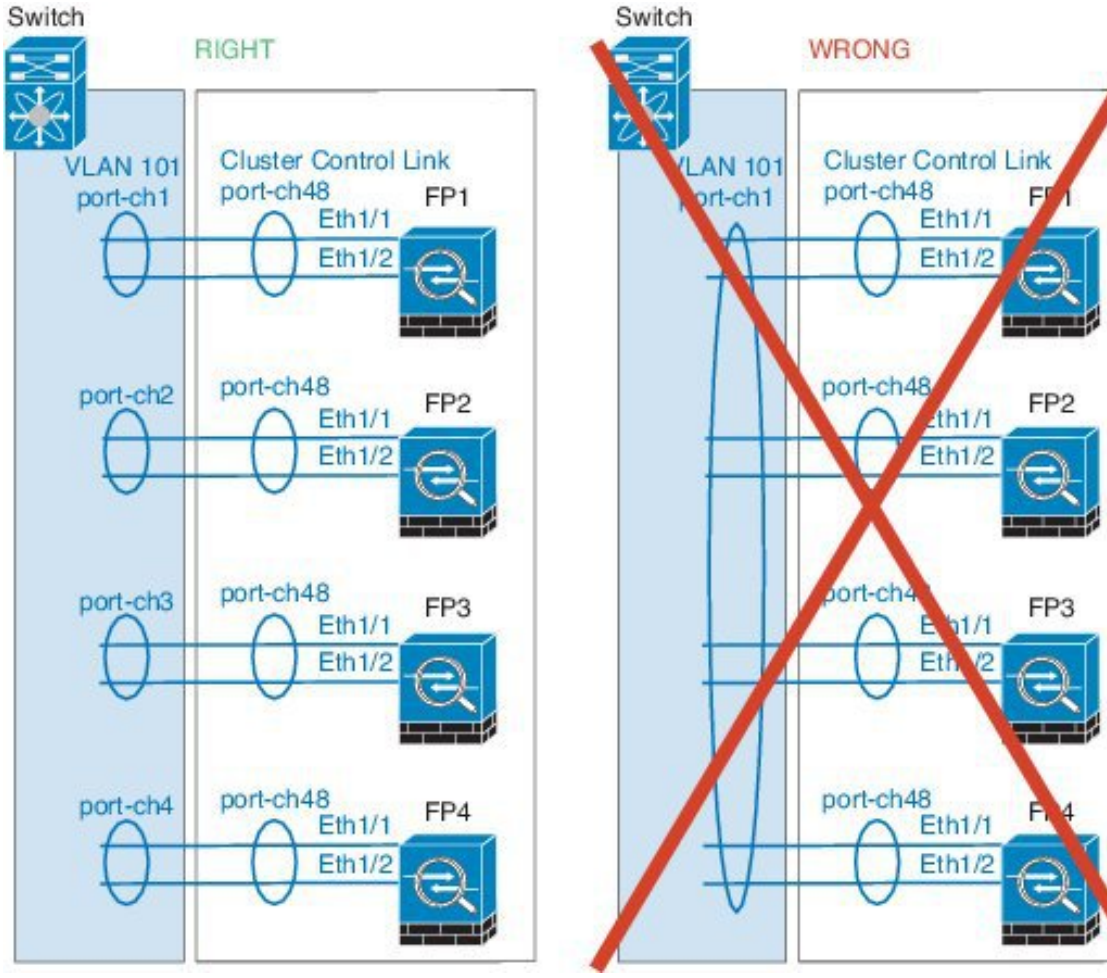
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないため、クラスタリングで ISSU を使用することは推奨されません。
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタ ユニット EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



その他のガイドライン

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバ ポートがダウンし、サーバが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージがクラスタに送信されます。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。

- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

クラスタリングの設定

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。その後、ユニットを FMC に追加し、1 つのクラスタにグループ化できます。

FXOS：Firepower Threat Defense クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

Firepower Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワーク マスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレスおよび/または NAT ID
  - DNS サーバの IP アドレス。
  - FTD ホスト名とドメイン名

手順

ステップ 1 インターフェイスを設定します。

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

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタ ユニットから 1 つ の EtherChannel にメンバ インターフェイスを結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （12 ページ）を参照してください。

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

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

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

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

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

シャーシ内クラスタリングのメンバインターフェイスを追加しないでください。メンバを追加すると、シャーシはこのクラスタがシャーシ間クラスタであると判断し、たとえば、使用できるのはスパンド Etherchannel のみになります。

[インターフェイス（Interfaces）] タブで、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、[動作状態（Operation State）] を [失敗（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。

各シャーシに同じメンバインターフェイスを追加します。各シャーシでは、クラスタ制御リンクはデバイスローカルな EtherChannel です。デバイスごとにスイッチで個別の Etherchannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （12 ページ） を参照してください。

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

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

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

ステップ 2 [論理デバイス（Logical Devices）] を選択します。

ステップ 3 **[追加（Add）] > [クラスタ（Cluster）]** をクリックし、次のパラメータを設定します。

a) [Device Name] にデバイス名を入力します。

この名前は、シャーシ スーパ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。

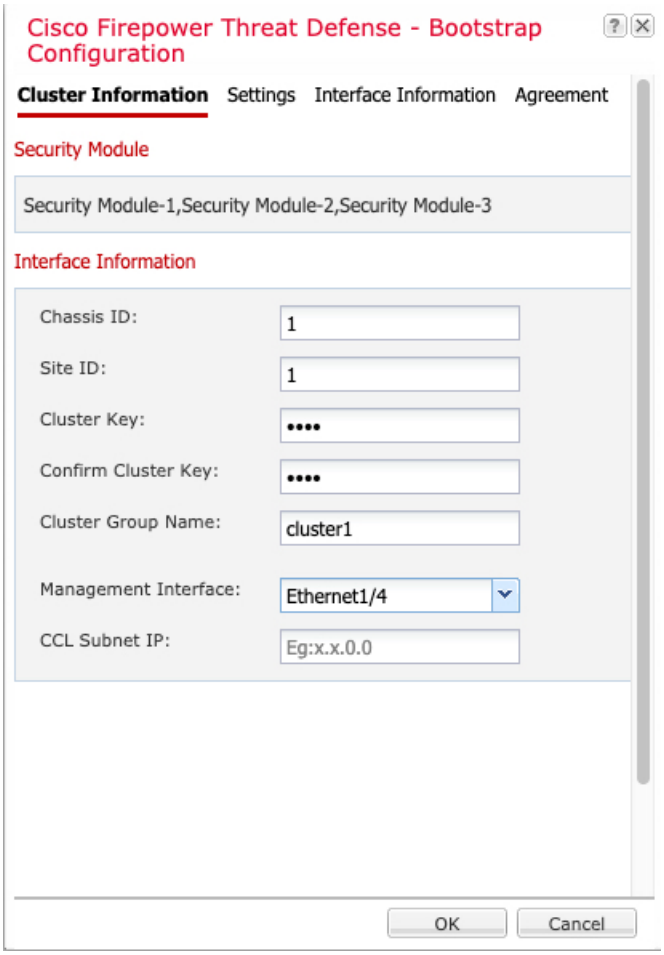
b) [Template] には、[Cisco Firepower Threat Defense] を選択します。
c) [Image Version] を選択します。
d) [Instance Type] では、[Native] タイプのみがサポートされます。
e) [Usage] では、[Cluster] オプション ボタンをクリックします。
f) [OK] をクリックします。

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

ステップ 4 画面中央のデバイス アイコンをクリックします。

初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CLI の設定を使用してほとんどの値を変更できます。

ステップ 5 [Cluster Information] ページで、次の手順を実行します。



a) シャーシ間クラスタリングでは、[Chassis ID] フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバインターフェイスを追加した場合にのみ表示されます。

b) サイト間クラスタリングの場合、[Site ID] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。

c) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

d) [クラスタ グループ名（Cluster Group Name）] を設定します。これは、論理デバイス設定のクラスタ グループ名です。

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

e) [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。

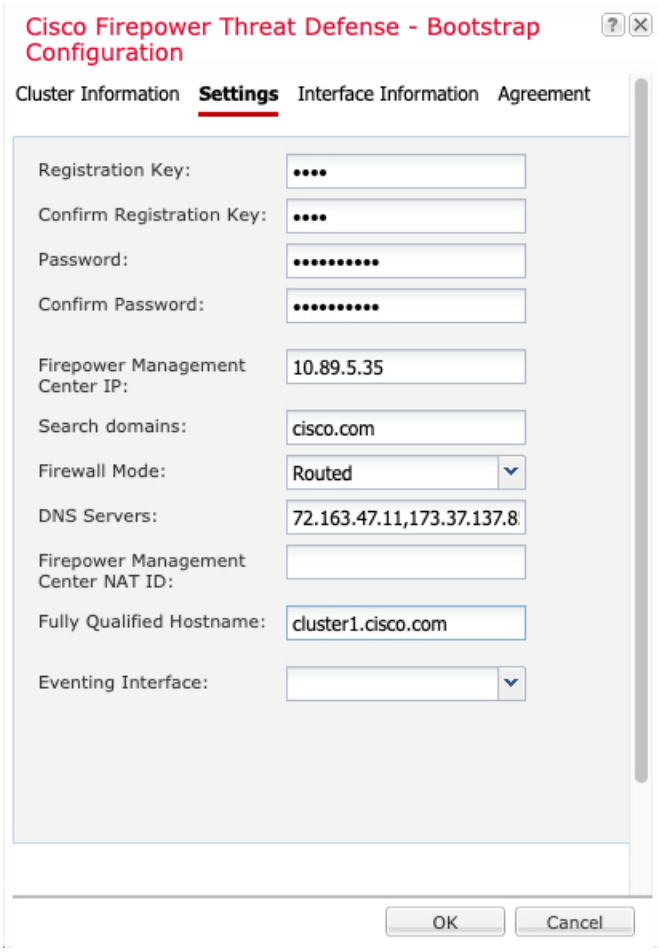
ハードウェア バイパス 対応のインターフェイスをマネジメント インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

f) **CCL サブネット IP** を *a.b*.**0.0** に設定します。

Cluster Control Link のデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定します（ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワークが使用されます。

シャーシは、シャーシ ID とスロット ID（*a.b.chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

ステップ 6 [Settings] ページで、以下を実行します。



a) [Registration Key] フィールドに、登録時に Firepower Management Center とクラスタ メンバー間で共有するキーを入力します。

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。

b) FTD 管理ユーザの CLI アクセス用パスワードを [Password] に入力します。

c) [Firepower Management Center の IP（Firepower Management Center IP）] フィールドに、管理側の Firepower Management Center の IP アドレスを入力します。

d) [ドメインの検索（Search Domains）] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。

e) [ファイアウォール モード（Firewall Mode）] ドロップダウン リストから、[トランスペアレント（Transparent）] または [ルーテッド（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。

f) [DNS Servers] フィールドに、DNS サーバのカンマ区切りのリストを入力します。

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

g) [完全修飾ホスト名（Fully Qualified Hostname）] フィールドに、FTD デバイスの完全修飾名を入力します。

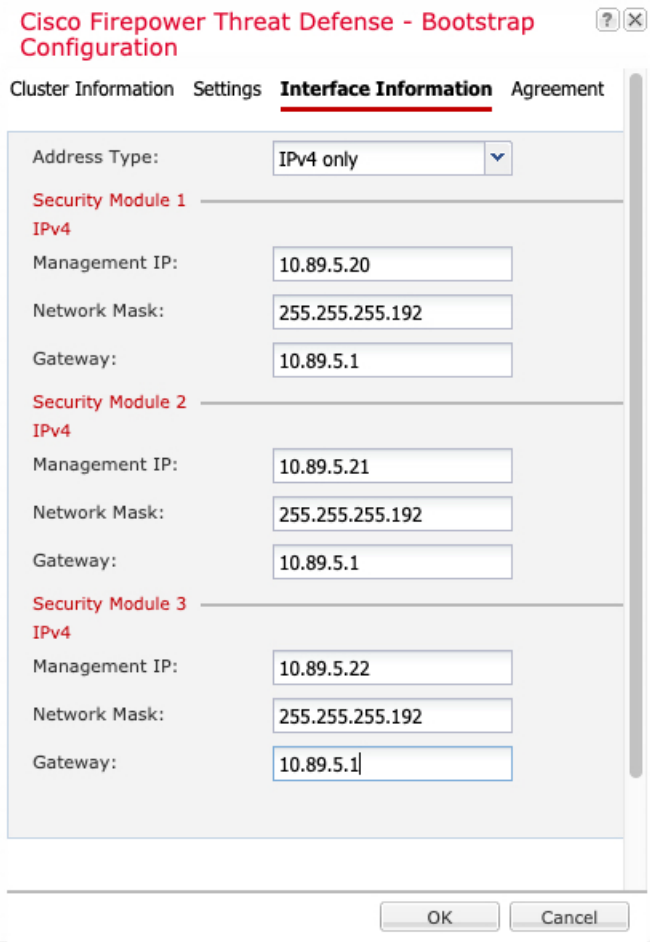
有効な文字は、a ～ z の文字、0 ～ 9 の数字、ドット（.）、およびハイフン（-）です。最大文字数は 253 です。

h) [イベンティング インターフェイス（Eventing Interface）] ドロップダウン リストから、Firepowerイベントを送信するインターフェイスを選択します。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。

Firepowerイベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。ハードウェア バイパス対応のインターフェイスを Eventing インターフェイスとして割り当てると、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。

ステップ 7 [Interface Information] ページで、クラスタ内の各セキュリティ モジュールの管理 IP アドレスを設定します。[アドレス タイプ（Address Type）] ドロップダウン リストからアドレスのタイプを選択し、セキュリティ モジュールごとに次の手順を実行します。

（注） モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。



a) [Management IP] フィールドで、IP アドレスを設定します。

モジュールごとに同じネットワークの固有の IP アドレスを指定します。

b) [Network Mask] または [Prefix Length] に入力します。

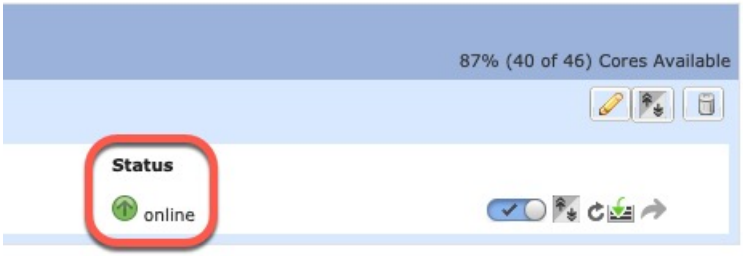
c) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 8 [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 9 [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 10 [Save] をクリックします。

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



ステップ 11 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

a) 最初のシャーシの Firepower Chassis Manager で、右上にある [Show Configuration] アイコン（ ） をクリックして、表示されるクラスタの設定をコピーします。

b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [必要な操作（I want to:）]> [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) **[OK]** をクリックします。

e) [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **シャーシ ID（Chassis ID）**：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

g) **[保存（Save）]** をクリックします。

ステップ 12 管理 IP アドレスを使用してマスター ユニットを Firepower Management Center に追加します。

すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

Firepower Management Center がスレーブ ユニットを自動的に検出します。

クラスタ メンバーの追加

既存のクラスタ内の FTD クラスタ メンバを追加または置き換えます。

（注） この手順における FXOS の手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。ただし、Firepower Management Center に新しいモジュールを追加する必要があります。Firepower Management Center の手順までスキップします。

始める前に

- 置き換える場合は、Firepower Management Center から古いクラスタ メンバーを削除する必要があります。新しいユニットに置き換えると、Firepower Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

手順

ステップ 1 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。

ステップ 2 右上の [Show Configuration] アイコン（  ）をクリックして、表示されるクラスタの設定をコピーします。

ステップ 3 新しいシャーシの Firepower Chassis Manager に接続して、**[追加（Add）]** > **[クラスタ（Cluster）]** をクリックします。

ステップ 4 [Device Name] に論理デバイスの名前を入力します。

ステップ 5

ステップ 6

ステップ 7

ステップ 8

ステップ 9 **[OK]** をクリックします。

ステップ 10 [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

ステップ 11 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **シャーシ ID（Chassis ID）**：一意のシャーシ ID を入力します。
- **Site ID**：サイト間クラスタリングの場合、このシャーシのサイト ID（1 ～ 8）を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- **Cluster Key**：（事前に入力されていない）同じクラスタ キーを入力します。
- [管理 IP（Management IP）]：各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 Firepower Management Center で、**[Devices]** > **[Device Management]** を選択してから **[Add]** > **[Add Device]** を選択して、新しい論理デバイスを追加します。

ステップ 14 **[Add]** > **[Add Cluster]** を選択します。

ステップ 15 ドロップダウン リストから現在の [Master] デバイスを選択します。

クラスタにすでに含まれているマスターデバイスを選択した場合、既存のクラスタの名前が自動入力され、[スレーブデバイス（Slave Devices）] ボックスに選択可能なすべてのスレーブ デバイスが表示されます。これには、FMC に追加したばかりの新しいユニットが含まれます。

ステップ 16 [Add] をクリックし、次に [Deploy] をクリックします。

クラスタは新しいメンバーを追加して更新されます。

FMC：クラスタの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意（Any）	Access Admin Administrator Network Admin

クラスタ ユニットのいずれかを新しいデバイスとして Firepower Management Center に追加します。FMC は、他のすべてのクラスタ メンバーを自動検出します。

始める前に

- クラスタを追加するためのこの方法には、Firepower Threat Defense バージョン 6.2 以降が必要です。以前のバージョンのデバイスを管理する必要がある場合には、そのバージョンの Firepower Management Center コンフィギュレーション ガイドを参照してください。
- クラスタを Management Center に追加する前に、すべてのクラスタ ユニットが FXOS 上の正常に形成されたクラスタ内に存在している必要があります。また、どのユニットがマス

ター ユニットかを確認することも必要です。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用します。

手順

ステップ 1 FMC で、**[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択してから、**[追加（Add）] > [デバイスの追加（Add Device）]** の順に選択して、クラスタを展開したときに割り当てた管理 IP アドレスを使用して、クラスタ ユニットのいずれかを追加します。

最適なパフォーマンスを得るため、マスターユニットの追加を推奨しますが、任意のユニットを追加できます。

FMC は、マスター ユニットを識別して登録した後、すべてのスレーブ ユニットを登録します。マスターユニットが正常に登録されていない場合、クラスタは追加されません。クラスタがシャーシで稼働状態になかったか、その他の接続問題が原因で、登録エラーが発生する場合があります。こうした状況では、クラスタ ユニットを再度追加することをお勧めします。

[デバイス（Devices）] > [デバイス管理（Device Management）] ページにクラスタ名が表示されます。クラスタを展開して、クラスタ ユニットを表示します。現在登録されているユニットには、ロード アイコンが表示されます。クラスタ ユニットの登録をモニタするには、システム ステータス アイコンをクリックし、[タスク（Tasks）] タブを選択します。FMC は、ユニットの登録ごとにクラスタ登録タスクを更新します。いずれかのユニットの登録に失敗した場合には、クラスタ メンバーの照合 （34 ページ） を参照してください。

ステップ 2 デバイス固有の設定を行うには、クラスタの編集アイコン（  ）をクリックします。クラスタを全体として設定することはできますが、クラスタのメンバー ユニットは設定できません。

ステップ 3 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブに、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定が表示されます。

- [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして、[クラスタ ステータス（Cluster Status）] ダイアログ ボックスを開きます。[クラスタ ステータス（Cluster Status）] ダイアログ ボックスで、[照合（Reconcile）] をクリックしてスレーブの登録を再試行することもできます。
- ライセンス付与資格を設定するには、[ライセンス（License）] 領域で編集アイコン（  ）をクリックします。

ステップ 4 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）]** タブの右上のドロップダウン メニューで、クラスタ内の各メンバーを選択できます。

デバイス設定で管理 IP アドレスを変更する場合、FMC で新しいアドレスを一致させてネットワーク上のデバイスに到達できるようにし、[管理（Management）] 領域で [ホスト（Host）] アドレスを編集します。

FMC：データ インターフェイスと診断インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。個別インターフェイスとして実行できる唯一のインターフェイスである診断インターフェイスを設定することもできます。

（注） シャーシ間クラスタリングにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、クラスタの横にある 編集アイコン（✎） をクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 3 （任意） インターフェイスに VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 4 データ インターフェイスの 編集アイコン（✎） をクリックします。

ステップ 5 シャーシ間クラスタの場合は、EtherChannel の手動グローバル MAC アドレスを設定します。

潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスター ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

a) [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

b) [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

[スタンバイ MAC アドレス（Standby MAC Address）] は設定しないでください。無視されます。

ステップ 6 に従い、名前、IP アドレス、およびその他のパラメータを設定します。

ステップ 7 [OK] をクリックします。他のデータ インターフェイスについても前述の手順を繰り返します。

ステップ 8 （任意） 診断インターフェイスを設定します。

診断インターフェイスは、個別インターフェイス モードで実行できる唯一のインターフェイスです。syslog メッセージや SNMP などに、このインターフェイスを使用できます。

a) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）]** を選択して、IPv4 または IPv6 アドレス プールを追加します。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。仮想 IP アドレスはこのプールには含まれませんが、同一ネットワーク上に存在している必要があります。各ユニットに割り当てられる正確なローカル アドレスを事前に決定することはできません。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** で、診断インターフェイスの 編集アイコン（✎） をクリックします。

c) [IPv4] タブで、[仮想 IP アドレス（Virtual IP Address）] とマスクを入力します。この IP アドレスは、そのクラスタの固定アドレスで、常に現在のマスター ユニットに属します。

d) 作成したアドレス プールを [IPv4 アドレス プール（IPv4 Address Pool）] ドロップダウン リストから選択します。

e) [IPv6] > [基本（Basic）] タブで、作成したアドレス プールを [IPv6 アドレス プール（IPv6 Address Pool）] ドロップダウンリストから選択します。

f) 通常どおり、他のインターフェイス設定を行います。

ステップ 9 [保存（Save）] をクリックします。

これで、[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できます。変更はポリシーを導入するまで有効になりません。

FXOS：クラスタ メンバの削除

ここでは、メンバーを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因でクラスタ メンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまで一時的であり、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページのクラスタ ステータスを確認します。

FMC を使用した FTD では、FMC デバイス リストにデバイスを残し、クラスタリングを再度有効にした後にすべての機能を再開できるようにする必要があります。

- アプリケーションでのクラスタリングの無効化：アプリケーション CLI を使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力してログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

  デバイスが非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合、管理インターフェイスは無効になります。

  クラスタリングを再度有効にするには、FTD で **cluster enable** を入力します。

- アプリケーション インスタンスの無効化：[Logical Devices] ページの Firepower Chassis Manager で [Disable] スライダ（ ） クリックします。[Enable] スライダ（ ） を使用して後で再度有効にすることができます。

- セキュリティ モジュール/エンジン のシャットダウン：[Module/Engine] ページの Firepower Chassis Manager で、[Power Off] アイコン（ ） をクリックします。

- シャーシのシャットダウン：[Overview] ページの irepower Chassis Manager で、 [Shut down] アイコン（ ） をクリックします。

永久削除

次の方法を使用して、クラスタ メンバを永久に削除できます。

FMC を使用した FTD の場合、シャーシのクラスタリングを無効にした後でユニットを FMC デバイスから削除してください。

- アプリケーション インスタンスの削除[Logical Devices] ページの Firepower Chassis Manager で [delete] アイコン（） クリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加することもできます。
- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

FMC：クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

新規クラスタ メンバーの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

FXOS に新しいクラスタ メンバーを追加すると、Firepower Management Center によりメンバーが自動的に追加されます。

始める前に

- インターフェイスの設定が他のシャーシと交換用ユニットで同じ設定になっていることを確認します。

手順

ステップ 1 FXOS のクラスタに新しいユニットを追加します。『FXOS コンフィギュレーション ガイド』を参照してください。

新しいユニットがクラスタに追加されるまで待機します。Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照するか、または Firepower Threat Defense の **show cluster info** コマンドを使用してクラスタ ステータスを表示します。

ステップ 2 新しいクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニタするには、次のように表示します。

- [クラスタ ステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [現在のクラスタの概要（Current Cluster Summary）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、FMC はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。
- システム ステータス アイコン > [タスク（Tasks）] タブ：FMC にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

クラスタ メンバーの置換

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意（Any）	Access Admin Administrator Network Admin

既存クラスタ内のクラスタ メンバーを置き換えることができます。Firepower Management Center は交換ユニットを自動検出します。ただし、Firepower Management Center 内の古いクラスタ メンバーは手動で削除する必要があります。また、この手順は再初期化したユニットにも適用されます。その場合は、ハードウェアが同じでも新しいメンバーとして表示されます。

始める前に

- インターフェイス設定が他のシャーシに関する交換ユニットと同じであることを確認します。

手順

ステップ 1 新しいシャーシの場合、可能であれば、FXOS内の古いシャーシの設定をバックアップして復元します。

Firepower 9300 のモジュールを交換する場合は、次の手順を実行する必要はありません。

古いシャーシのバックアップ FXOS 設定がない場合は、最初に新規クラスタ メンバーの追加（30 ページ）の手順を実行します。

以下のすべての手順については、FXOS コンフィギュレーション ガイド[英語]を参照してください。

a) 設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォームの構成時の設定を含んでいる XML ファイルをエクスポートします。
b) 交換用シャーシに設定ファイルをインポートします。
c) ライセンス契約に同意します。
d) 必要に応じて、論理デバイスのアプリケーションインスタンスバージョンをアップグレードして、残りのクラスタと一致させます。

ステップ 2 Firepower Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、古いユニットの横にある [delete] アイコン（🗑） をクリックします。

ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、FMC デバイス リストからも削除されます。

ステップ 4 新しいクラスタ メンバーまたは再初期化したクラスタ メンバーは自動的に追加されます。交換用ユニットの登録状況をモニタするには、次のように表示します。

- [クラスタ ステータス（Cluster Status）] ダイアログボックス（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** タブ > [全般（General）] 領域 > [現在のクラスタの概要（Current Cluster Summary）] リンク）で、シャーシ上でクラスタに追加中のユニットに「クラスタに追加中...（Joining cluster...）」と示されます。クラスタに追加された後に、FMC はこれの登録を試み、ステータスが「登録可能（Available for Registration）」に変わります。登録が完了すると、ステータスが「同期状態（In Sync）」に変わります。登録に失敗すると、ユニットは「登録可能（Available for Registration）」の状態に留まります。この場合、[照合（Reconcile）] をクリックして再登録を強制します。
- システム ステータス アイコン > [タスク（Tasks）] タブ：FMC にすべての登録イベントとエラーが表示されます。
- **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**：デバイスの一覧表示ページでクラスタを展開して、左側にロードアイコンがある場合は、ユニットが登録中であることを示しています。

スレーブ メンバーの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower 4100 および 9300 上の FTD	任意（Any）	Access Admin Administrator Network Admin

クラスタ メンバーを完全に削除する必要がある場合（たとえば、Firepower 9300 でモジュールを削除する場合、またはシャーシを削除する場合）は、FMC からメンバーを削除する必要があります。

始める前に

メンバーが正常なクラスタの一部である場合、またはメンバーを一時的に無効にするだけの場合は、メンバーを削除しないでください。FXOS のクラスタから完全に削除するには、FXOS：クラスタ メンバの削除 （28 ページ）を参照してください。FMC から削除した後もメンバーがクラスタの一部である場合、トラフィックは引き続き通過し、FMC で管理不能なマスターユニットになることもあります。

手順

ステップ 1 ユニットが FMC から削除できる状態であることを確認します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択して、クラスタの編集アイコン（  ）をクリックします。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブ > [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして [クラスタ ステータス（Cluster Status）] ダイアログボックスを開きます。

c) 削除するデバイスが「削除可能」状態であることを確認します。

ステータスが古い場合は、[照合（Reconcile）] をクリックして強制的に更新します。

ステップ 2 FMC で、**[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、スレーブユニットの横にある [delete] アイコン（  ） をクリックします。

ステップ 3 ユニットを削除することを確認します。

ユニットがクラスタから削除され、FMC デバイス リストからも削除されます。

クラスタ メンバーの照合

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

クラスタ メンバーの登録に失敗した場合、シャーシから Firepower Management Center に対してクラスタ メンバーシップを照合することができます。たとえば、FMC が特定のプロセスで占領されているか、またはネットワークに問題がある場合、スレーブ ユニットの登録に失敗することがあります。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、クラスタの 編集アイコン（✎） をクリックします。

ステップ 2 [クラスタ（Cluster）] タブ > [全般（General）] 領域で、[現在のクラスタの概要（Current Cluster Summary）] リンクをクリックして [クラスタ ステータス（Cluster Status）] ダイアログボックスを開きます。

ステップ 3 [照合（Reconcile）] をクリックします。

クラスタ ステータスの詳細については、FMC：クラスタのモニタリング （36 ページ）を参照してください。

メンバーの非アクティブ化

ログインしているユニット以外のメンバーを非アクティブにするには、FTD CLI で次のステップを実行します。この手順の目的は、メンバーを一時的に非アクティブにし、FMC のデバイス リスト内にユニットを保持する必要があります。

（注） ユニットが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールを使用する必要があります。

手順

ステップ 1 FTD CLI にアクセスします。

ステップ 2 ユニットをクラスタから削除します。

cluster remove unit *unit_name*

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままになるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
> cluster remove unit ?

Current active units in the cluster:
ftd1
ftd2
ftd3

> cluster remove unit ftd2
WARNING: Clustering will be disabled on unit ftd2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

ステップ 3 クラスタリングを再び有効にするには、クラスタへの再参加 （35 ページ）を参照してください。

クラスタへの再参加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower 4100 および 9300 上の Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

ユニット（障害が発生したインターフェイスなど）がクラスタから削除された場合は、そのユニットのCLIにアクセスして、手動でクラスタに再参加させる必要があります。クラスタへの再参加を試行する前に、障害が解決されていることを確認します。クラスタからユニットが削除される理由の詳細については、クラスタへの再参加 （39 ページ）を参照してください。

手順

ステップ 1 クラスタに再参加させる必要のあるユニットの CLI に、コンソール ポートからアクセスするか、管理インターフェイスへの SSH を使用してアクセスします。ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用してログインします。

ステップ 2 クラスタリングを有効にします。

cluster enable

FMC：クラスタのモニタリング

クラスタのモニタリングは、Firepower Management Center および FTD CLI で実行できます。

- **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブ > [一般（General）] エリア > [現在のクラスタの概要（Current Cluster Summary）] リンク > [クラスタのステータス（Cluster Status）] ダイアログボックス。

  クラスタ メンバ状態には、以下が含まれます。

  - 同期中（In Sync）：装置は FMC に登録されています。
  - 登録可能（Available for Registration）：装置はクラスタの一部ですが、まだ FMC に登録されていません。装置が登録に失敗した場合、[照合（Reconcile）] クリックして登録を再試行することができます。
  - 削除可能（Available for Deletion）：装置は FMC に登録されていますが、クラスタの一部ではなく、削除する必要があります。
  - クラスタに参加中（Joining cluster）：装置がシャーシ上でクラスタに参加していますが、参加は完了していません。参加後に FMC に登録されます。

  このダイアログボックスを更新するには、閉じてから再度開きます。

- システム ステータス アイコン > [タスク（Tasks）] タブ。

  [タスク（Tasks）] タブには、装置の登録ごとに、クラスタ登録タスクの更新が表示されます。

- **[デバイス（Devices）] > [デバイス管理（Device Management）] >** *cluster_name*。

  デバイスの一覧表示ページでクラスタを展開すると、IP アドレスの隣の「（master）」と表示されるマスター装置を含めて、すべてのメンバ装置を表示できます。登録中の装置には、ロード中のアイコンが表示されます。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタ パフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- 合計 UDP スループットの 90 %
- トラフィックの組み合わせに応じて、イーサネット MIX（EMIX）の合計スループットの 60 %

たとえば、TCP スループットについては、3 つのモジュールを備えた Firepower 9300 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、合計スループットの最大値は約 270 Gbps（2 シャーシ × 135 Gbps）の 80 %、つまり 216 Gbps となります。

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシ アプリケーションのモニタリング

シャーシ アプリケーションのヘルス モニタリングは常に有効になっています。Firepower 4100/9300 シャーシ スーパバイザは、Firepower Threat Defense アプリケーションを定期的に確認します（毎秒）。Firepower Threat Defense デバイス が作動中で、Firepower 4100/9300 シャーシ スーパバイザと 3 秒間通信できなければ、Firepower Threat Defense デバイス は syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシ スーパバイザが 45 秒後にアプリケーションと通信できなければ、Firepower Threat Defense デバイス をリロードします。Firepower Threat Defense デバイス がスーパバイザと通信できなければ、自身をクラスタから削除します。

装置のヘルス モニタリング

マスター ユニットは、各スレーブ ユニットをモニタするために、クラスタ制御リンク経由でキープアライブ メッセージを定期的に送信します。各スレーブ ユニットは、同じメカニズムを使用してマスター ユニットをモニタします。装置のヘルス チェックが不合格になると、その装置はクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニタして EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には Firepower Threat Defense アプリケーションに通知します。ヘルス モニタリングを有効にすると、デフォルトですべての物理インターフェイスがモニタされます（EtherChannel インターフェイスの主要な EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。Firepower Threat Defense デバイス がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済み

メンバーであるか、またはクラスタに参加しようとしているかによって異なります。Firepower Threat Defense デバイスは、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、Firepower Threat Defense デバイスはクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます。

シャーシ間クラスタリングでは、クラスタから EtherChannel を追加または削除した場合、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは 95 秒間中断されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローの状態情報は、クラスタ制御リンクを介して共有されます。

マスター ユニットで障害が発生した場合は、そのクラスタの他のメンバのうち、プライオリティが最高（番号が最小）のものがマスター ユニットになります。

障害イベントに応じて、Firepower Threat Defense デバイスは自動的にクラスタへの再参加を試みます。

（注） Firepower Threat Defense デバイスが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理/診断インターフェイスのみがトラフィックを送受信できます。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、クラスタリングを再び有効にして、手動でクラスタに再参加する必要があります。
- データ インターフェイスの障害：FTD アプリケーションは自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、FTD アプリケーションはクラスタリングを無効にします。データ インターフェイスの問題を解決した後、手動でクラスタリングを有効にする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。FTD アプリケーションは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：FTD アプリケーションはシャーシアプリケーションの状態が回復したことを検出すると、自動的にクラスタへの再参加を試みます。

- 内部エラー：内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP の状態情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上の状態情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *1:* クラスタ全体で複製される機能

トラフィック	状態のサポート	注記（**Notes**）
アップ タイム	○	システム アップ タイムをトラッキングします。
ARP テーブル	あり	—
MAC アドレス テーブル	あり	—
ユーザ ID	○	—
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	×	—
中央集中型 VPN（サイト間）	×	VPN セッションは、マスター ユニットで障害が発生すると切断されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバーにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

各接続に定義されている次のロールを参照してください。

- オーナー：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。最初のオーナーに障

害が発生すると、新しいユニットがその接続からパケットを受信したときに、ディレクタがそれらのユニットの中から新しいオーナーを選択します。

- バックアップ オーナー：オーナーから受信した TCP/UDP 状態情報を保存して、障害発生時に接続を新しいオーナーにシームレスに転送できるようにするユニット。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせて、関連する状態情報を取得します。これでそのユニットが新しいオーナーになることができます。

  ディレクタ（下記参照）がオーナーと同じユニットでないかぎり、ディレクタもバックアップ オーナーです。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

  1 つのシャーシに最大で 3 つのクラスタ ユニットを格納できる Firepower 9300 でのシャーシ間クラスタリングでは、バックアップ オーナーがオーナーと同じシャーシに配置されている場合、シャーシの障害からフローを保護するために、別のシャーシから追加のバックアップ オーナーが選択されます。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。ディレクタに障害が発生すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じユニットでないかぎり、ディレクタもバックアップ オーナーです（上記参照）。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

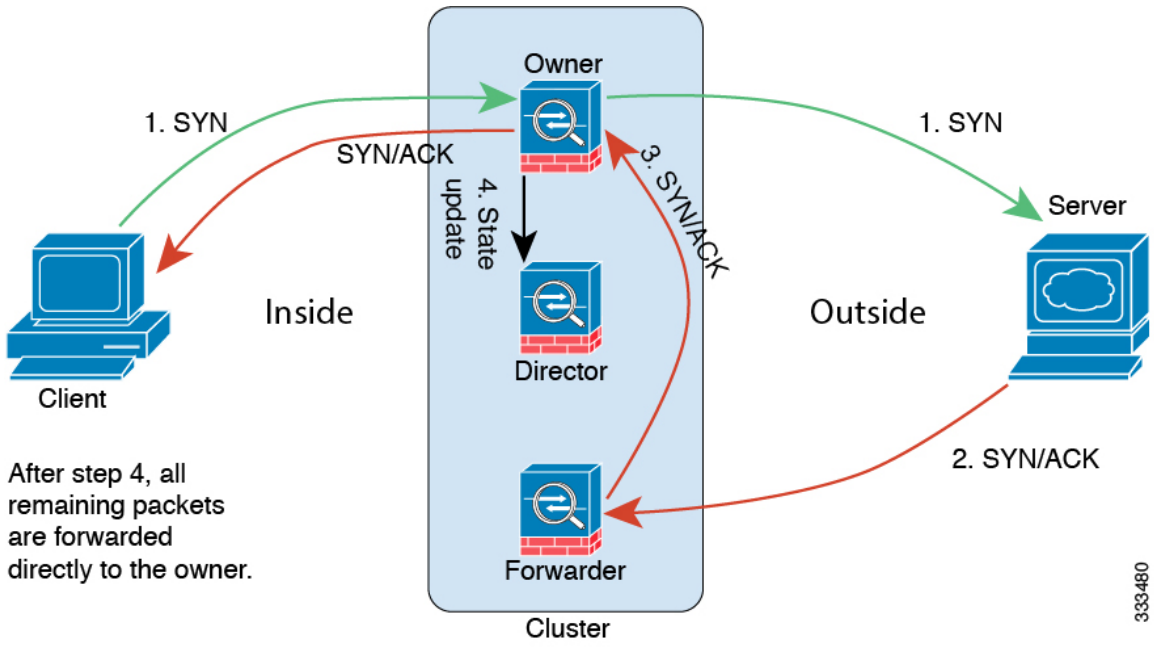
- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化をディセーブ ルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、Firepower Threat Defense デバイスの 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の Firepower Threat Defense デバイス（ロードバランシング方法に基づく）に配信されます。この Firepower Threat Defense デバイスはフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP 状態情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。

6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

クラスタリングの履歴

機能	バージョン（Version）	詳細
強化された Firepower Threat Defense クラスタの Firepower Management Center への追加	6.3.0	Firepower Management Center にクラスタの任意のユニットを追加できるようになりました。他のクラスタ ユニットは自動的に検出されます。以前は、各クラスタ ユニットを個別のデバイスとして追加し、Management Center でグループ化してクラスタにする必要がありました。クラスタ ユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新規/変更された画面： **[デバイス（Devices）]>[デバイス管理（Device Management）]** >[追加（Add）] ドロップダウン メニュー >[デバイス（Devices）]>[デバイスの追加（Add Device）] ダイアログボックス **[デバイス（Devices）]>[デバイス管理（Device Management）]** >[クラスタ（Cluster）] タブ >[全般（General）] 領域 >[クラスタの登録ステータス（Cluster Registration Status）] リンク >[クラスタステータス（Cluster Status）] ダイアログ ボックス サポートされるプラットフォーム：Firepower 4100/9300
中央集中型機能としてのクラスタリングによるサイト間 VPN のサポート	6.2.3.3	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイトツーサイト VPN は、中央集中型機能です。マスター ユニットだけが VPN 接続をサポートします。 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（Version）	詳細
内部エラーの発生後に自動的にクラスタに再参加します。	6.2.3	以前は、多くの内部エラー状態によって、クラスタ ユニットがクラスタから削除され、ユーザが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーション ステータスなどがあります。 新しい/変更されたコマンド：**show cluster info auto-join** 変更された画面はありません。 サポートされているプラットフォーム：Firepower 4100/9300 の Firepower Threat Defense
6 モジュールのシャーシ間クラスタリング、Firepower 4100 サポート	6.2.0	FXOS 2.1.1 では、Firepower 9300 および 4100 でシャーシ間クラスタリングを有効化できるようになりました。Firepower 9300 の場合、最大 6 つのモジュールを含めることができます。たとえば、6 つのシャーシで 1 つのモジュールを使用したり、3 つのシャーシで 2 つのモジュールを使用したり、最大 6 つのモジュールを組み合わせたりできます。Firepower 4100 の場合、最大 6 つのシャーシを含めることができます。 （注） サイト間クラスタリングが、FlexConfig のみを使用してサポートされるようになりました。 変更された画面はありません。 サポートされているプラットフォーム：Firepower 4100/9300 の Firepower Threat Defense
Firepower 9300 用シャーシ内クラスタリング	6.0.1	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > -[クラスタの追加（Add Cluster）]** **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** サポートされているプラットフォーム：Firepower 9300 の Firepower Threat Defense