Firepower 4100/9300 の Firepower Threat Defense クラスタ

クラスタリングを利用すると、複数の Firepower Threat Defense 装置をグループ化して 1 つの論理デバイスにすることができます。クラスタリングは、Firepower 9300 および Firepower 4100 シリーズ上の Firepower Threat Defense 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 （11 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。クラスタを Firepower 4100/9300 シャーシ に展開すると、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（デフォルトではポート 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 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。

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。

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。ここでは、各メンバーのロールの特長について説明します。

マスターおよびスレーブ ユニットのロール

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 （11 ページ）を参照してください。

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. 優先順位が高い他のユニットがこの選定要求に応答します。優先順位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 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。

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。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポート チャネル 48）です。シャーシ内クラスタリングでは、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、シャーシ間通信のために、Firepower 4100/9300 シャーシ のこの 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。

2 シャーシのシャーシ間クラスタの場合、シャーシと他のシャーシの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

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。

制御トラフィックには次のものが含まれます。

- マスター選定。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

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。この IP アドレスは、FXOS でもアプリケーション内でも手動で設定することはできません。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。

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、EtherChannel でポートがアクティブかどうかを判断するためにリンク ステータスと cLACP プロトコル メッセージをモニタします。インターフェイスがダウンしている場合は、/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。

デコレータ アプリケーションのモニタリング

インターフェイスに Radware DefensePro アプリケーションなどのデコレータ アプリケーションをインストールした場合、ユニットがクラスタ内にとどまるには /Firepower Threat Defense デバイス、デコレータ アプリケーションの両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。一旦クラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか3秒ごとにモニタします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

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：Firepower Threat Defense 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、Firepower Threat Defense 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。Firepower Threat Defense 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：Firepower Threat Defense 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。問題の解決後、クラスタリングを再度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 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	○	—
MAC アドレス テーブル	○	—
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	なし	—
中央集中型 VPN（サイト間）	なし	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。

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。

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。

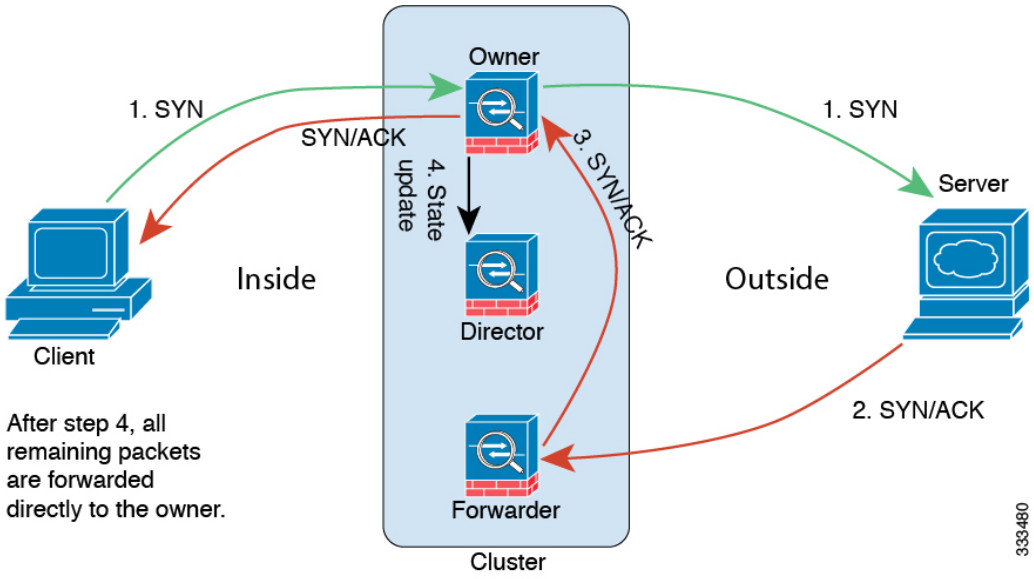
- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie 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。

Firepower Threat Defense の機能とクラスタリング

Firepower Threat Defense 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。

- サイト間 VPN
- 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 リレーはサポート対象です。
- 高可用性
- 統合ルーティングおよびブリッジング

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。

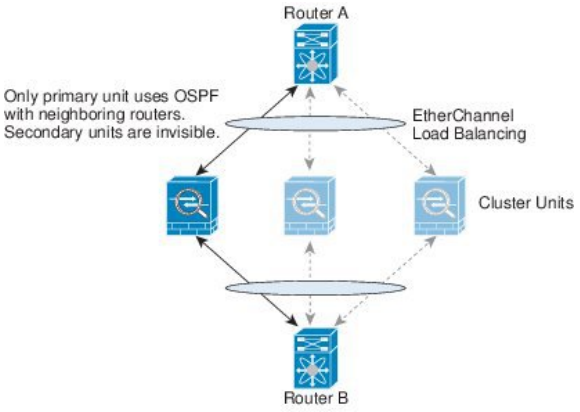
- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング

- 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。インバウンドおよびアウトバウンドの 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、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。接続のオーナーではない /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。

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。接続を受信したメンバーにアドレスが 1 つも残っていない場合、他のメンバーには使用可能なアドレスがまだ残っていても、接続はドロップされま

す。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。

Firepower 4100/9300 シャーシ でのクラスタ化前提条件

インター シャーシ クラスタ化に関する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。
- 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。時間を手動で設定しないでください。

スイッチ前提条件

- Firepower 4100/9300 シャーシでクラスタリングを設定する前に、必ずスイッチの設定を完了し、シャーシからのすべての EtherChannel をスイッチに正常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。

Firepower 4100/9300 シャーシ 上のクラスタリングのガイドライン

高可用性/

高可用性/ は、クラスタリングではサポートされません。

その他のガイドライン

- 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。
- 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。これは予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。
- スパンドインターフェイスに接続された Windows 2003 サーバ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 メッセージを制限しないと、大量の ICMP メッセージがクラスタに返送されます。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。

Firepower4100/9300シャーシでのクラスタリングのデフォルト

- 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。インターフェイス ヘルス モニタリングは、デフォルトで、すべてのインターフェイス上で有効です。

Firepower 4100/9300 シャーシ のクラスタリング設定

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 Management Center に追加し、1 つのクラスタにグループ化できます。

Firepower 4100/9300 シャーシ スーパバイザからのクラスタの展開

クラスタリングの設定手順についての詳細は、Firepower 4100/9300 シャーシのドキュメンテーションを参照してください。

論理デバイスを Firepower 4100/9300 シャーシ に追加するときは、スタンドアロン ユニットまたはクラスタのどちらを展開するかを選択できます。クラスタを展開する場合は、新しいクラスタを作成することも、既存のクラスタに参加することもできます（シャーシ間クラスタリング）。Firepower Chassis Manager を使用したシャーシ間クラスタリングの場合は、最初のシャーシを展開した後、基本設定をクリップボードにコピーしておくと、既存のクラスタに参加して次のシャーシを展開する際に、その設定を Firepower Chassis Manager にコピーできます。各追加シャーシに設定する必要があるのは、一意のシャーシ ID と管理 IP のみです。

Management Center へのクラスタの追加

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 Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

論理デバイスを Management Center に追加し、これらをクラスタにグループ化します。

始める前に

- どのユニットがマスター ユニットであるかを確認するには、Firepower Chassis Manager の [論理デバイス（Logical Devices）] 画面を参照します。
- すべてのクラスタ ユニットは、Management Center に追加する前に、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。

手順

ステップ 1 Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、**[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、各ユニットを別個の管理対象デバイスとして追加します。

（注） Management Center のハイ アベイラビリティを使用する場合、スタンバイ Management Center にも各ユニットが正常に登録されていることを確認してから、アクティブな Management Center 上での作業を継続し、クラスタを形成します。各ユニットの登録ステータスを確認するために、スタンバイ Management Center にログインします。

ステップ 2 **[追加（Add）] > [クラスタの追加（Add Cluster）]** の順に選択し、ユニットをクラスタにグループ化します。

a) ドロップダウンリストから [マスター（Master）] デバイスを選択します。

対象となる他のすべてのメンバーは、[スレーブデバイス（Slave Devices）] ボックスに追加されます。

b) クラスタの [名前（Name）] を指定します。

c) [OK] をクリックします。

クラスタ オブジェクトが [デバイス（Devices）] 画面に追加され、メンバー ユニットがその下に表示されます。現在のマスター ユニットは、ユニット名の後の「（マスター）（(master)）」で表示されます。

（注） 後からFXOSシャーシのクラスタにさらにユニットを追加する場合は、Management Centerに各ユニットを追加し、その後すぐにそれらをクラスタのスレーブ ノードとして追加する必要があります。

ステップ 3 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 4 **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]** タブから、[全般（General）]、[ライセンス（License）]、[システム（System）]、および [ヘルス（Health）] の設定を確認できます。このタブは、ライセンス付与の設定をする際に役立ちます。[デバイス（Devices）] タブでは、マスター ユニットのみの管理 IP アドレスを変更できます。

ステップ 5 （任意） 診断インターフェイスを設定するには、次の手順を実行します。

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) IPv4 アドレス プールか IPv6 アドレス プール、またはその両方を追加します。

b) 診断インターフェイスを編集するには、[インターフェイス（Interfaces）] タブをクリックします。

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

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。

e) [マスク（Mask）] に、クラスタ IP プールのサブネット マスクを入力します。

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

g) 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 6 必要に応じて他のデバイスレベルの設定も行います。

ステップ 7 [保存（Save）]、[展開（Deploy）] の順にクリックします。

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

Firepower 9300 デバイスにモジュールを追加する場合や、シャーシを追加する場合などには、既存のクラスタに新しいクラスタ メンバーを追加できます。

始める前に

FXOS シャーシのクラスタにさらにユニットを追加するときには、Management Center に各ユニットを追加し、その後すぐにそれらをクラスタのスレーブ ノードとして追加する必要があります。

手順

ステップ 1 Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択し、**[追加（Add）]** > **[デバイスの追加（Add Device）]** の順に選択して、新しい論理デバイスを追加します。

ステップ 2 [追加（Add）] > [クラスタの追加（Add Cluster）] を選択します。 >

ステップ 3 ドロップダウン リストから現在の [マスター（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、Management Center 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 4 [追加（Add）] をクリックし、次に [導入（Deploy）] をクリックします。

クラスタが更新され、新しいメンバーが追加されます。

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 Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

クラスタ メンバーを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、Management Center からメンバーを削除する必要があります。そのメンバーが引き続きクラスタの正常な構成要素であると Firepower Chassis Manager に示されている場合は、メンバーを削除しないでください。Management Center から削除しても、そのメンバーは引き続きクラスタの有効な構成要素であるため、これがマスターユニットになって Management Center でそれを管理できなくなる場合に問題が発生する可能性があります。

手順

ステップ 1 Management Center 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ごみ箱をクリックします。

ステップ 2 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、Management Center デバイス リストからも削除されます。

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

障害が発生したインターフェイスなど、ユニットがクラスタから削除された場合、ユニット CLI にアクセスして、クラスタに手動で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 （6 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

クラスタリングの履歴

機能	バージョン（Version）	詳細（Details）
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
6 つのモジュールのシャーシ間クラスタリング、およびサイト間クラスタリング。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。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。 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 9300 および Firepower 4100 の Firepower Threat Defense