7000 および 8000 シリーズ デバイスのハイ アベイラビリティ

次の各トピックでは、Firepower システムにおける Firepower 7000 シリーズおよび 8000 シリーズ デバイスのハイ アベイラビリティの設定方法について説明します。

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて

7000 および 8000 シリーズ デバイス ハイ アベイラビリティを利用することで、2 つのピア デバイス間または 2 つのピア デバイス スタック間のネットワーキング機能と設定データの冗長性を確保できます。

2 つのピア デバイスまたは 2 つのピア デバイス スタックを、ポリシーの展開、システムの更新、登録を行う単一の論理システムとして機能するハイ アベイラビリティ ペアとして構成することにより、構成の冗長性を実現できます。その他の設定データは、システムによって自動的に同期されます。

（注） スタティック ルート、非 SFRP IP アドレス、およびルーティングの優先順位は、ピア デバイスまたはピア デバイス スタック間で同期されません。各ピア デバイスまたはピア デバイス スタックは、独自のルーティング インテリジェンスを維持します。

関連トピック

SFRP
仮想スイッチの詳細設定

デバイスのハイ アベイラビリティ要件

7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアを構成するには、以下に従う必要があります。

- 単一デバイスと単一デバイスのペア、またはデバイス スタックとデバイス スタックのペアのみを構成できます。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、ヘルス モニタの使用を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンスモードに入り、フェールオーバーがトリガーされます。

  （注） デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定する必要があります。
- 両方のデバイスまたはデバイス スタックのプライマリ メンバーが同じモデルである必要があり、銅ケーブルまたは光ファイバの同じインターフェイスが必要です。
- デバイス スタックのハードウェア構成は同一でなければなりませんが、インストール済みのマルウェア ストレージ パックについてはその限りではありません。たとえば、Firepower 8290 と別の 8290 のペアを構成することができます。どちらかのスタック内でマルウェア ストレージ パックが、どのデバイスに存在しなくても、1 つのデバイスにのみ、またはすべてのデバイスに存在しても構いません。

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。
- マルチドメイン展開では、7000 または 8000 シリーズ デバイスのハイ アベイラビリティまたはリーフ ドメイン内のデバイス スタックのみを確立できます。

（注） フェールオーバーとリカバリの後に、SFRP はマスター ノードにプリエンプション処理します。

デバイス ハイ アベイラビリティ フェールオーバーとメンテナンス モード

7000 および 8000 シリーズ デバイス ハイ アベイラビリティのフェールオーバーは、手動または自動で行われます。手動でフェールオーバーをトリガーするには、ペアを構成するデバイスまたはスタックのいずれかでメンテナンス モードを開始します。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわれた場合、システム更新時、または管理者権限によりデバイスがシャットダウンされた場合に発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタックで NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、ディスク フル エラー、または 2 つのスタック構成のデバイス間のリンク障害が起きた場合にも発生します。スタンバイのデバイスまたはスタックの正常性がアクティブデバイス同様に損なわれている場合は、フェールオーバーは行われず、クラスタは縮退状態になります。また、いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、フェールオーバーは行われません。アクティブ スタックからスタック ケーブルを切断すると、そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックのセカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。

（注） ハイ アベイラビリティ ペアのアクティブなメンバーがメンテナンス モードになり、アクティブ ロールが他のペア メンバーにフェールオーバーされた場合、元のアクティブ ペアのメンバーは、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

ハイ アベイラビリティ ペアの設定展開とアップグレードの動作

このトピックでは、ハイ アベイラビリティ ペアでの 7000 および 8000 シリーズ デバイス（およびスタック）のアップグレードと展開の動作について説明します。

展開時の動作

ハイ アベイラビリティ ペアのメンバーに同時に設定の変更を展開します。展開は、両方のピアについて成功するか失敗するかのいずれかです。Firepower Management Center は、アクティブ デバイスに展開します。この展開に成功すると、次に変更がスタンバイに展開されます。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。Snort® の再起動によるトラフィックの動作および展開またはアクティブ化された際に Snort プロセスを再起動する設定を参照してください。

アップグレード時の動作

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に 1 つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイをアップグレードします。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレード プロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブをアップグレードします。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

展開タイプとデバイス ハイ アベイラビリティ

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ構成は、Firepower システム展開（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて決定します。同時に複数のロールを持たせてシステムを展開することもできます。4つの展開タイプのうち、ハイ アベイラビリティを用いた冗長性をもたらすためにデバイスまたはスタックの構成が必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス ハイ アベイラビリティを使用しても使用しなくてもネットワークの冗長性を確立できます。各展開タイプにおけるハイ アベイラビリティの概要については、以降の各項を参照してください。

（注） レイヤ 3 の冗長性については、デバイス ハイ アベイラビリティを使わずに、Cisco Redundancy Protocol（SFRP）により実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つのデバイスまたは 2 つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。

パッシブ展開での冗長性

一般に、パッシブ インターフェイスは中央スイッチのタップ ポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブ インターフェイスで分析することが可能になります。複数のデバイスが同じタップ フィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。ハイ アベイラビリティ ペアとして構成されているデバイスは、アクティブまたはスタンバイのいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

インライン展開での冗長性

インラインセットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうかに依存します。冗長インライン セットは、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。

冗長インラインセットを展開するには、循環ルーティングを防止する一方で、トラフィックがインラインセットのいずれか1つだけを通過できるようにネットワーク トポロジーを設定します。インライン セットのいずれかで障害が発生すると、周辺ネットワーク インフラストラクチャがゲートウェイ アドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

ルーテッド展開での冗長性

IP ネットワーク内のホストは、既知のゲートウェイ アドレスを使用して、トラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッド インターフェイスがゲートウェイ アドレスを共有し、そのアドレスに対するトラ

フィックを常に1つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数のIPアドレスを維持する必要があります。1つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、スタンバイインターフェイスがアドレスのアドバタイズを開始します。

ハイ アベイラビリティ ペアのメンバーではないデバイスでは、複数のルーティングされたインターフェイス間で共有するゲートウェイ IP アドレスの設定し、SFRP によって冗長性を確保します。SFRP は、7000 または 8000 シリーズ デバイスのハイ アベイラビリティを使用しても使用しなくても設定できます。また、OSPF や RIP などのダイナミック ルーティングを使用して冗長性を確保することもできます。

スイッチド展開での冗長性

スイッチド展開では、高度な仮想スイッチ設定の 1 つであるスパニング ツリー プロトコル（STP）を使用して冗長性を確保します。STP はブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、スタンバイ リンクを設定することなく、冗長リンクでスイッチドインターフェイスの自動スタンバイを行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャスト ネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。

（注） 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアに展開する予定の仮想スイッチを設定する際には、STP を有効にするよう強く推奨します。

デバイスのハイ アベイラビリティ設定

7000 または 8000 シリーズ デバイスのハイ アベイラビリティを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイスのペアを構成した後は、ペアを構成する個々のデバイスのライセンス オプションを変更することはできませんが、ハイ アベイラビリティ ペア全体のライセンスは変更できます。スイッチド インターフェイスまたはルーテッド インターフェイスで設定しなければならないインターフェイス属性がある場合、システムはハイ アベイラビリティ ペアを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはハイ アベイラビリティ ペアを完成させて、正常なステータスに設定します。

ハイ アベイラビリティ ペアを確立した後、[デバイス管理（Device Management）]ページでは、ピア デバイスまたはスタックが単一のデバイスとして扱われます。デバイスのハイ アベイラビリティ ペアは、アプライアンス リストではハイ アベイラビリティ アイコン（  ）が表示されます。ユーザが行った設定変更は、いずれもペアを構成するデバイスの間で同期されます。[デバイス管理（Device Management）] ページには、ハイ アベイラビリティ ペアのどのデ

バイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。

デバイスのハイ アベイラビリティ ペアの登録を Firepower Management Center から削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイスのハイ アベイラビリティ ペアを Firepower Management Center から削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。

登録が削除されたハイ アベイラビリティ ペアは、別の Firepower Management Center に登録できます。ハイ アベイラビリティ ペアを構成する一方のデバイスを登録するには、ペアのうちアクティブ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。ハイ アベイラビリティ ペアのうちスタック構成のデバイスを登録するには、どちらか一方のスタックのプライマリ デバイスにリモート管理を追加してから、そのデバイスを Firepower Management Center に追加します。これにより、ペア全体が追加されます。

デバイスのハイ アベイラビリティ ペアを確立したら、ハイ アベイラビリティ リンク インターフェイスを設定する必要があります。

（注） ハイ アベイラビリティ ペアのデバイスを使用してダイナミック NAT、HA 状態共有、または VPN を設定する場合は、ハイ アベイラビリティ リンク インターフェイスを構成する必要があります。詳細については、「HA リンク インターフェイスの設定」を参照してください。

Firepower 7000/8000 シリーズ ハイ アベイラビリティの確立

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

（注） この手順では、7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアの確立について説明します。Firepower Threat Defense のハイ アベイラビリティの確立については、Firepower Threat Defense ハイ アベイラビリティ ペアの追加を参照してください。

7000 & 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をスタンバイとして指定します。システムは、マージした設定を、ペア内のデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

マルチドメイン展開では、ハイ アベイラビリティ ペアのデバイスは同じドメインに属している必要があります。

始める前に

すべての要件が満たされていることを確認します。デバイスのハイ アベイラビリティ要件 （2 ページ）を参照してください。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 [追加（Add）] ドロップダウン メニューから、[高可用性の追加（Add High Availability）] を選択します。

ステップ 3 名前を入力します。

ステップ 4 [デバイス タイプ（Device Type）] で [Firepower] を選択します。

ステップ 5 デバイスまたはスタックにロールを割り当てます。

a) [アクティブ ピア（Active Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

b) [スタンバイ ピア（Standby Peer）] のデバイスまたはスタックをハイ アベイラビリティ ペア用に選択します。

ステップ 6 [追加（Add）]をクリックします。このプロセスではデータの同期が行われるため、プロセスが完了するまでに数分かかります。

次のタスク

HA 状態共有、ダイナミック NAT、または VPN をデバイスに設定する予定の場合は、高可用性ペアの各デバイスで HA リンク インターフェイスを作成します。HA リンク インターフェイスの詳細については、HA リンク インターフェイスの設定を参照してください。

デバイスのハイ アベイラビリティの編集

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後は、デバイス設定を変更すると、通常はハイ アベイラビリティ ペア全体の設定も変更されます。

[一般（General）] セクションのステータス アイコンにマウスのポインタを合わせると、ハイ アベイラビリティ ペアのステータスが表示されます。また、ペア内のデバイスまたはスタックのどれがアクティブ ピアで、どれがスタンバイ ピアであるかも確認できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスのハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [ハイ アベイラビリティ（High Availability）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、ハイ アベイラビリティ ペアの設定を変更します。

高可用性ペアの個々のデバイスの設定

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後でも、ペア内の個々のデバイスに対して設定できる属性がいくつかあります。ペアリングされたデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 [デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、ペアリングされた個々のデバイスに変更を加えます。

高可用性ペアの個々のデバイス スタックの設定

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数	サポートされるドメイン数	アクセス
該当なし	Control	Firepower 8140、Firepower 8200 ファミリ、Firepower 8300 ファミリ	リーフのみ	Admin/Network Admin

高可用性ペアにスタック構成の 8000 シリーズ デバイスを設定すると、編集可能なスタック属性が制限されます。ペアリングされたスタックの名前は編集できます。また、高可用性ペアのデバイスでのインターフェイスの設定 （10 ページ）で説明している手順に従って、スタックのネットワーク設定を編集できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 設定を編集するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [スタック（Stacks）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

ステップ 5 [一般（General）] セクションの横にある編集アイコン（  ）をクリックします。

ステップ 6 [名前（Name）] を入力します。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

高可用性ペアのデバイスでの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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアの個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、ペアのピア デバイスにも同等のインターフェイスを設定する必要があります。ペアリングされたスタックの場合は、スタックのプライマリ デバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するときに、その仮想ルータを設定するスタックを選択します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 インターフェイスを設定するデバイスの高可用性ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 [選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

ステップ 5 個々のデバイスに設定する場合と同じようにインターフェイスを設定します。

関連トピック

仮想ルータ設定

デバイスのハイアベイラビリティペアにおけるアクティブ ピアの切り替え

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアを確立した後、アクティブなピア デバイスまたはスタックをスタンバイに手動で切り替えることができます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 アクティブ ピアを変更するデバイスのハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。

ステップ 3 次の操作を実行できます。

- ハイ アベイラビリティ ペアでスタンバイ ピアをアクティブ ピアにすぐに切り替える場合は、[はい（Yes）] をクリックします。

- キャンセルして [デバイス管理（Device Management）] ページに戻る場合は、[いいえ（No）] をクリックします。

高可用性ピアのメンテナンス モードへの切り替え

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイス高可用性ペアを設定した後で、デバイスのメンテナンスを実行するために、いずれかのピアをメンテナンス モードに切り替えることで、手動でフェールオーバーをトリガーできます。メンテナンス モードでは、システムが管理目的で管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、ピアを再度有効にして、通常の動作を再開できます。

（注） 高可用性ペアの両方のピアを同時にメンテナンス モードにしないでください。これを行うと、そのペアではトラフィックを検査できなくなります。

ステップ 1 **[Devices]** > **[Device Management]** を選択します。

ステップ 2 メンテナンス モードを開始するピアの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

次のタスク

- メンテナンスが完了したら、メンテナンス モード切り替えアイコン（）を再度クリックして、ピアのメンテナンス モードを終了します。

高可用性ペアのスタック内のデバイスの交換

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数	サポートされるドメイン数	アクセス
該当なし	Control	Firepower 8140、8200 ファミリ、8300 ファミリ	任意（Any）	Admin/Network Admin

高可用性ペアのメンバーになっているスタックをメンテナンス モードに切り替えた後で、スタック内のセカンダリ デバイスを別のデバイスと交換できます。選択できるデバイスは、現在スタックのメンバーにも、ペアにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

ステップ 3 [はい（Yes）] をクリックして、メンテナンス モードを確定します。

ステップ 4 デバイス交換アイコン（  ）をクリックします。

ステップ 5 ドロップダウンリストから [交換デバイス（Replacement Device）] を選択します。

ステップ 6 [交換（Replace）] をクリックして、デバイスを交換します。

ステップ 7 メンテナンス モード切り替えアイコン（  ）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

（注） デバイス設定を再展開する必要はありません。

デバイスのハイ アベイラビリティ状態共有

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペアのデバイスまたはスタックで、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳密な TCP 適用
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

ただし、状態共有を有効にすると、システムパフォーマンスが低下することに注意してください。

ハイ アベイラビリティ状態共有を設定するには、あらかじめハイ アベイラビリティ ペアの両方のデバイスまたはスタック構成のプライマリ デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。Firepower 82xx ファミリおよび 83xx ファミリには 10 G の HA リンクが必要ですが、他のモデルのデバイスには 1 G の HA リンクで十分です。

HA リンク インターフェイスを変更する前に、状態共有を無効にする必要があります。

（注） ペアを構成するデバイスでフェールオーバーが発生した場合は、アクティブデバイス上の既存の SSL 暗号化セッションがすべて終了されます。ハイ アベイラビリティ状態共有を設定しているとしても、これらのセッションをスタンバイデバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、スタンバイ デバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。

厳密な TCP の適用

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、ハイ アベイラビリティ ペアのデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インライン セット、仮想ルータ、および仮想スイッチで有効にすることができます。

単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワーク トラフィックが意図されたものとは異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の 2 つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ～ 192.168.2.1 からの許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリーム ピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピアデバイスまたはスタックでも即時に接続をブロックします。

ハイ アベイラビリティ ペアの状態共有を確立するときに、次のオプションを設定できます。

[有効（Enabled）]

状態共有を有効にするには、このチェック ボックスをクリックします。チェック ボックスをクリアすると、状態共有が無効になります。

Minimum Flow Lifetime

最小セッション時間（ミリ秒）を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ～ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

Minimum Sync. Interval

セッションの更新メッセージ間隔（ミリ秒）を指定します。0～65535 の整数を使用できます。最小同期間隔を設定することで、特定の接続が最小有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

HTTP URL の最大文字数（Maximum HTTP URL Length）

ペアを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ～ 225 の整数を使用できます。

関連トピック

HA リンク インターフェイスの設定

デバイスのハイ アベイラビリティ状態共有の確立

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

デバイスのハイ アベイラビリティ状態共有を使用すると、ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスまたはスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。

注意 7000 または 8000 シリーズ デバイスのハイ アベイラビリティ状態共有オプションを変更すると、プライマリ デバイスとセカンダリ デバイスの Snort プロセスが再起動され、両方のデバイスのトラフィック インスペクションが一時的に中断されます。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細は Snort® の再起動によるトラフィックの動作を参照してください。

ステップ 1 デバイスのハイ アベイラビリティ ペアのデバイスごとに HA リンク インターフェイスを設定します。HA リンク インターフェイスの設定を参照してください。

ステップ 2 **[Devices]** > **[Device Management]** を選択します。

ステップ 3 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 4 [状態共有（State Sharing）] セクションの横にある編集アイコン（）をクリックします。

ステップ 5 状態共有の値を下げてペア内のピアの準備状況を改善するか、値を上げてパフォーマンスを向上できるようにします。

展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨します。

ステップ 6 [OK] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

関連トピック

HA リンク インターフェイスの設定
Snort® の再起動シナリオ

トラブルシューティングのためのデバイスのハイアベイラビリティの状態共有統計情報

以下の項では、デバイスごとに表示可能な統計情報と、7000 および 8000 シリーズ デバイスのハイ アベイラビリティ ペアの状態共有設定をトラブルシューティングするためにどのように利用できるかを説明します。

受信メッセージ（ユニキャスト）（Messages Received (Unicast)）

ペアを構成するピアから受信した、ハイ アベイラビリティ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信パケット数（Packets received）

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[Packets Received] カウンタは、デバイスが受信したこれらのデータ パケットとその他の制御パケットの数を表示します。

値は、ピアデバイスが送信したパケット数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずです。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Total Bytes Received

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。ペアを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

Protocol Bytes Received

受信したプロトコル オーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコルデータと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコルデータが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコルバイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコルバイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

送信メッセージ（Messages Sent）

ペアを構成するピアに送信した、ハイ アベイラビリティ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

送信バイト数（Bytes Sent）

ピアに送信したハイ アベイラビリティ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていないはずです。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

Tx Errors

システムがペアを構成するピアに送信するメッセージ用にスペースを割り当てるときに、メモリ割り当てに失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

Tx Overruns

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムがHAリンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値（9918 または 9922）未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

最近のログ（Recent Logs）

システム ログには、最新のハイ アベイラビリティ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されていてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、ハイ アベイラビリティ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

デバイス ハイ アベイラビリティの状態共有統計情報の表示

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

状態共有を確立した後は、[ハイ アベイラビリティ（High Availability）] ページの [状態共有（State Sharing）] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク状態
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、送受信されたハイ アベイラビリティ同期トラフィックのさまざまな側面に関するカウンタで、その他のエラー カウンタも含まれます。さらに、ハイ アベイラビリティ ペアのデバイスごとの最新システム ログも表示できます。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 編集するデバイス ハイ アベイラビリティ ペアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [状態共有（State Sharing）] セクションで、統計情報表示アイコン（  ）をクリックします。

ステップ 4 ハイ アベイラビリティ ペアがデバイス スタックで構成されている場合、表示する [デバイス（Device）] を選択します。

ステップ 5 次の操作を実行できます。

- [更新（Refresh）] をクリックして統計情報を更新します。
- [表示（View）] をクリックして、ハイ アベイラビリティ ペアのデバイスごとの最新システム ログを表示します。

デバイス高可用性ペアの分離

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数	サポートされるドメイン数	アクセス
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

7000 または 8000 シリーズ デバイス高可用性ペアを分離（分断）すると、次のようになります。

- アクティブなピア（デバイスまたはスタック）は、完全な展開機能を維持します
- スタンバイ ピア（デバイスまたはスタック）はインターフェイス設定を失って、アクティブ ピアにフェールオーバーします。ただし、インターフェイス設定をアクティブのままにすることを選択すると、スタンバイ ピアは通常の動作を再開します。
- スタンバイ ピアは、常にパッシブ インターフェイスの設定を失います。
- メンテナンス モードのピアは、通常の動作を再開します。

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 分断する高可用性ペアの横にある HA の分断アイコン（  ）をクリックします。

ステップ 3 必要に応じて、スタンバイ ピアのインターフェイス設定を削除するためのチェックボックスをオンにします。

この手順により、管理インターフェイス以外のすべてのインターフェイスを管理のためにダウンさせます。

ステップ 4 [Yes] をクリックします。