高可用性

ここでは、アクティブ/スタンバイフェールオーバーを設定して、Firewall Threat Defense システムのハイアベイラビリティを実現する方法について説明します。

- Secure Firewall Threat Defense のハイ アベイラビリティについて （1 ページ）
- 設定同期の最適化 （19 ページ）
- ハイアベイラビリティの要件と前提条件 （20 ページ）
- 高可用性 のガイドライン （20 ページ）
- ハイ アベイラビリティ ペアの追加 （23 ページ）
- オプションの高可用性パラメータの設定 （26 ページ）
- 高可用性 の管理 （29 ページ）
- 高可用性のモニタリング （36 ページ）
- 高可用性の履歴 （37 ページ）

Secure Firewall Threat Defense のハイ アベイラビリティについて

フェールオーバーとも呼ばれるハイアベイラビリティを設定するには、専用フェールオーバーリンク（および任意でステート リンク）を介して相互に接続された 2 台の同じ Firewall Threat Defense デバイスが必要です。Firewall Threat Defense はアクティブ/スタンバイ フェールオーバーをサポートしています。つまり 1 台のユニットがアクティブなユニットとなりトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニターされます。所定の条件に一致すると、フェールオーバーが行われます。

（注） ハイ アベイラビリティは、パブリック クラウドで実行される Firewall Threat Defense Virtual ではサポートされていません。Firewall Threat Defense Virtual デバイスの高可用性設定の詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。

高可用性 のシステム要件

この項では、高可用性 コンフィギュレーションにある Firewall Threat Defense デバイスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

高可用性コンフィギュレーションの2台の装置は、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。 さらに、コンテナ インスタンスでは、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。

  Firepower 9300 の場合、高可用性は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、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間に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ペアを Firewall Management Center に追加した後にリソースプロファイルを変更する場合は、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[システム（System）]** > **[インベントリ（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。

  両方のユニットでプロファイルを同じにする必要がある確立されたハイアベイラビリティペアのインスタンスに異なるプロファイルを割り当てる場合、次の手順を実行する必要があります。

  1. ハイ アベイラビリティを解除します。
  2. 両方のユニットに新しいプロファイルを割り当てます。
  3. ハイアベイラビリティを再確立します。

- インターフェイスの数とタイプが同じであること。

  プラットフォーム モード では、高可用性 を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。高可用性を有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でそのインターフェイスを変更してから、アクティブユニットで同じ変更を行います。

高可用性 コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してくださ

い。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

高可用性コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- 同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。
- ソフトウェア バージョンが同じであること。
- Firewall Management Center 上で、同じドメインまたはグループに入っていること。
- 同じ NTP コンフィギュレーションであること。脅威に対する防御のための NTP 時刻同期の設定を参照してください。
- 非コミットの変更で、Firewall Management Center 上で完全に展開していること。
- どのインターフェイスでも、DHCP または PPPoE は変更していないこと。
- （Firepower 4100/9300）同じフローオフロードモードを使用し、両方とも有効または無効になっている。

高可用性ペアでの Firewall Threat Defense デバイスのライセンス要件

高可用性構成の両方の Firewall Threat Defense ユニットは、ライセンスが同じである必要があります。

高可用性構成には 2 つのライセンス資格（ペアの各デバイスに 1 つずつ）が必要です。

高可用性を確立する前に、どのライセンスがセカンダリ/スタンバイデバイスに割り当てられているかどうかは問題にはなりません。高可用性の設定中に、Firewall Management Center はスタンバイユニットに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブユニットに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブユニットに Essentials ライセンスと IPS ライセンスが割り当てられており、スタンバイユニットに Essentials ライセンスのみが割り当てられている場合、Firewall Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイユニット用に使用可能な IPS ラインセンスを取得します。ライセンスアカウントで十分な数の資格が購入されていなければ、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバー リンクまたはステートフル フェールオーバー リンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、または EtherChannel）はいずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。サブインターフェイスを使用することもできませんマルチインスタンスモードのシャーシで定義されたサブインターフェイスを除きます。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。

Firewall Threat Defense は、ユーザー データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません（マルチインスタンスシャーシのサブインターフェイスのみ）。フェールオーバーリンクに対してシャーシの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。

（注） フェールオーバーまたはステートリンクとして EtherChannel を使用している場合、ハイアベイラビリティを確立する前に、両方のデバイスで同じメンバインターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- Firepower 4100/9300：フェールオーバー 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。
- リンクのサイジングについては、次のガイドラインを参照してください。

表 *1:* フェールオーバー リンクのサイズ

モデル	結合フェールオーバー リンクとステート リンクのインターフェイス サイズ
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Firepower 2100	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105：1 Gbps Cisco Secure Firewall 3110：1 Gbps Cisco Secure Firewall 3120：1 Gbps Cisco Secure Firewall 3130：10 Gbps Cisco Secure Firewall 3140：10 Gbps
Firepower 4100	10 Gbps
Firepower 9300	10 Gbps

交替頻度は、ユニットのホールド時間と同じです。

（注） 設定が大きく、ユニットのホールド時間が短い場合、メンバーインターフェイスを交互に切り替えると、セカンダリユニットの参加/再参加を防止できます。この場合、セカンダリユニットが参加するまで、メンバーインターフェイスの 1 つを無効にします。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- Firewall Threat Defense デバイスのフェールオーバーインターフェイスと同じネットワークセグメント（ブロードキャストドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因に

なったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、大規模な構成とトラフィックの多いネットワークを使用する場合は、ステート リンクとフェールオーバー リンクに専用のインターフェイスを使用することを検討する必要があります。

ステートフル フェールオーバー リンク専用のインターフェイス

ステートリンク専用のデータインターフェイス（物理、またはEtherChannel）を使用できます。専用のステートリンクの要件についてはフェールオーバー リンクのインターフェイス （4 ページ）、ステートリンクの接続についてはフェールオーバー リンクの接続 （5 ページ）を参照してください。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンしている場合、フェールオーバー動作は、フェールオーバー リンクが正常化するまで停止されます。

耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの Firewall Threat Defense デバイス間のフェールオーバーインターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたは Inter-Switch Link（ISL）がダウンすると、両方の Firewall Threat Defense デバイスがアクティブになります。したがって、次の図で示されている 2 つの接続方式は推奨**しません**。

図 *1:* 単一のスイッチを使用した接続*推奨

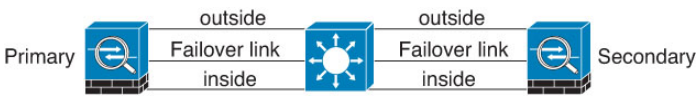
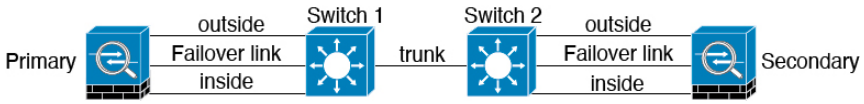


図 *2*：*2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、異なるスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *3*：異なるスイッチを使用した接続

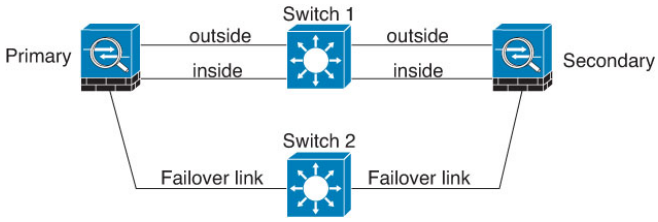
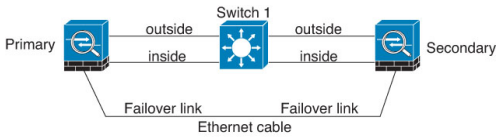


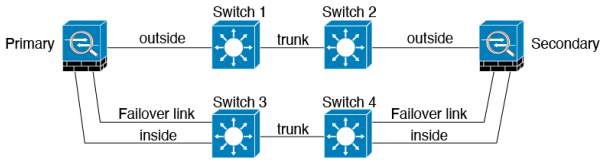
図 *4*：ケーブルを使用した接続



シナリオ 3：推奨

Firewall Threat Defense データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *5*：セキュアなスイッチを使用した接続



高可用性 の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上にアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。通常、フェールオーバーが発生すると、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワークデバイスは、MAC と IP アドレスのペアリングの変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） 推奨されてはいますが、スタンバイアドレスは必須ではありません。スタンバイ IP アドレスがなければ、アクティブ装置はネットワーク テストを実行してスタンバイ インターフェイスの状態を確認することはできません。できることはリンク ステートの追跡のみです。また、管理目的でそのインターフェイス上のスタンバイ装置に接続することもできません。

ステートリンクのIPアドレスおよびMACアドレスは、フェールオーバー時に変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ 高可用性 の場合、フェールオーバーイベント中の IP アドレスと MAC アドレスの使用方法については、次を参照してください。

1. アクティブ装置は常に、プライマリ装置のIPアドレスとMACアドレスを使用します。
2. アクティブ装置がフェールオーバーすると、スタンバイ装置は障害が発生した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
3. 障害が発生した装置がオンライン状態に戻ると、スタンバイ状態になり、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずに起動した場合、プライマリ装置のMAC アドレスを認識していないため、セカンダリ装置がアクティブ装置になり、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。このため、ネットワーク トラフィックが中断することがあります。同様に、新しいハードウェアでプライマリ装置をスワップ アウトすると新しい MAC アドレスが使用されます。

高可用性を無効にし、フェールオーバー設定を無効状態に設定した場合は、高可用性を手動で再開するか、デバイスを再起動する必要があります。デバイスを再起動するのではなく、コマンド **configure high-availability resume** を使用して高可用性を再開することをお勧めします。フェールオーバー設定が無効なスタンバイ装置をリロードすると、スタンバイ装置はアクティブ装置として起動し、プライマリ装置の IP アドレスと MAC アドレスを使用します。これにより、IP アドレスが重複し、ネットワークトラフィックが中断されます。**configure high-availability resume** コマンドを使用してフェールオーバーを有効にし、トラフィックフローを復元します。

（注） スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。セカンダリ装置がプライマリ装置より先にオンラインになった場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスを使用するように、プライマリ装置とセカンダリ装置の両方で仮想MACアドレスを設定することをお勧めします。仮想MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの

ARPテーブルをクリアする必要がある場合があります。MACアドレスが変わった場合、Firewall Threat Defense デバイスはスタティックNATアドレスに対してGratuitous ARPを送信しません。そのため、接続されたルータはこれらのアドレスのMACアドレス変更を認識できません。

仮想 MAC アドレス

Firewall Threat Defense デバイス には仮想 MAC アドレスを設定する複数の方法があります。1 つの方法だけ使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合、使用される MAC アドレスは多くの変数によって決まるため、予測できないことがあります。

マルチインスタンス機能の場合、FXOS シャーシはすべてのインターフェイスに対してプライマリ MAC アドレスのみ自動生成します。プライマリおよびセカンダリ MAC アドレスの両方で、生成された MAC アドレスを仮想 MAC アドレスで上書きすることができますが、セカンダリ MAC アドレスを事前に定義することは必須ではありません。セカンダリ MAC アドレスを設定すると、セカンダリ装置のハードウェアが新しい場合に、to-the-box 管理トラフィックが中断されないようになります。

フェールオーバーでの MAC アドレス テーブルの更新

フェールオーバー時、新しいアクティブ デバイスとして指定されたデバイスは、MAC テーブル内の各 MAC アドレス エントリに対してマルチキャスト パケットを生成し、それをすべてのブリッジグループインターフェイスに送信します。このアクションにより、ブリッジグループ内の上流スイッチは、新しいアクティブデバイスのインターフェイスでルーティングテーブルを更新し、正確なトラフィック転送を保証します。

マルチキャストパケットの生成および上流スイッチのルーティングテーブルを更新するのにかかる時間は、MACアドレステーブルのエントリ数とブリッジ グループ インターフェイスの数によって異なります。フェールオーバーイベント中に発生した遅延に関連する統計を表示するには、コマンド **show failover statistics state-switch-delay** を使用します。

ステートフル フェールオーバー

ステートフェールオーバー中にアクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ Firewall Threat Defense デバイス に渡されます。

- NAT 変換テーブル
- TCP 接続状態と UDP 接続状態（HTTP 接続状態を含む）。その他の IP プロトコル タイプとICMPは、新しいパケットが到着すると新しいアクティブデバイスで確立されるため、アクティブ装置によって解析されません。

- Snort 接続状態、インスペクションの結果、およびピン ホールに関する情報（TCP の厳密な適用を含む）。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションおよびピン ホール。
- スタティック/ダイナミック ルーティング テーブル：ステートフル フェールオーバーは OSPF や EIGRP などのダイナミック ルーティング プロトコルに参加します。そのため、アクティブ装置上のダイナミック ルーティング プロトコルを介して学習されたルートは、スタンバイ装置のルーティング情報ベース（RIB）テーブルに保持されます。フェールオーバーイベントが発生した場合、最初はアクティブなセカンダリ装置にプライマリ装置をミラーリングするルールがあるため、パケットは通常は最小限の切断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれます。

（注） ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイス上に構成された DHCP サーバは DHCP クライアントにアドレスを付与する前に ping を送信してアドレスが使用されていないことを確認するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS には関係ありません。
- アクセス コントロール ポリシーの決定：トラフィックの一致（URL、URL カテゴリ、地理位置情報などを含む）、侵入検知、マルウェア、およびファイル タイプに関する決定は、フェールオーバー時に維持されます。ただし、フェールオーバー時に評価される接続には、次の注意事項があります。
  - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に App-ID 判定が完了および同期していれば、同期は正常に行われます。
  - 侵入検知状態：フェールオーバーの途中でピックアップが発生すると、新しいインスペクションは完了しますが古い状態は失われます。

- ファイル マルウェア ブロッキング：フェールオーバーの前にファイルの判定結果を利用できるようにする必要があります。
- ファイル タイプの検出およびブロッキング：フェールオーバーの前にファイル タイプを特定する必要があります。元のアクティブデバイスでファイルを特定しているときにフェールオーバーが発生すると、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされていても、新しいアクティブ デバイスはファイルをダウンロードします。

- アイデンティティポリシーによるユーザアイデンティティの決定。ISE セッションディレクトリを介して受動的に収集されたユーザと IP アドレスのマッピングや、キャプティブポータル経由のアクティブ認証が含まれます。フェールオーバー時にアクティブに認証されるユーザは、再認証を要求されることがあります。
- ネットワーク AMP：クラウド ルックアップは各デバイスに依存していないため、通常、フェールオーバーはこの機能に影響しません。詳細：
  - 署名ルックアップ：ファイルの送信中にフェールオーバーが発生すると、ファイルイベントは生成されず、検出は行われません。
  - ファイルストレージ：ファイルの保存中にフェールオーバーが発生した場合、元のアクティブデバイスに保存されます。ファイルの保存中に元のアクティブなデバイスがダウンした場合、ファイルは保存されません。
  - ファイルの事前分類（ローカル分析）：事前分類の途中でフェールオーバーが発生すると、検出は失敗します。
  - ファイルの動的分析（クラウドへの接続）：フェールオーバーが発生すると、システムがクラウドにファイルを送信する場合があります。
  - アーカイブ ファイル サポート：分析中にフェールオーバーが発生すると、システムはファイル/アーカイブを表示できなくなります。
  - カスタムブラックリスト：フェールオーバーが発生すると、イベントは生成されません。
- セキュリティインテリジェンスの決定。ただし、フェールオーバー時に進行中の DNS ベースの決定は完了しません。
- RA VPN：リモート アクセス VPN のエンド ユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。
- すべての接続から、確立された接続だけがスタンバイ デバイスに複製されます。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Firewall Threat Defense デバイス に渡されません。

- GREv0 および IPv4-in-IP 以外のプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されません。新しいアクティブ ノードでは、正しいポリシー ルールを照合するために既存のインスペクション判定を再利用することはできません。
- 復号された TLS/SSL 接続：復号状態は同期されず、アクティブユニットに障害が発生すると、復号された接続がリセットされます。新しいアクティブユニットへの新しい接続を確立する必要があります。復号されていない接続（つまり、TLS/SSL[復号しない（Do Not Decrypt）] ルールアクションに一致する）は影響を受けず、正しく複製されます。
- TCP ステート バイパス接続。
- マルチキャスト ルーティング。

ハイ アベイラビリティのためのブリッジ グループの要件

ブリッジ グループを使用する場合は、ハイ アベイラビリティに関して特別な考慮事項があります。

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行しているスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング状態に移行できます。ポートがブロッキング状態の間のブリッジ グループ メンバーインターフェイスでのトラフィックの損失を回避するために、次の回避策のいずれかを設定できます。

- アクセス モードのスイッチ ポート：スイッチで STP PortFast 機能を有効にします。

```
interface interface_id
  spanning-tree portfast
```

  PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは STP に参加し続けます。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- スイッチ ポートがトランク モードになっている場合、または STP PortFast を有効にできない場合は、フェールオーバー機能または STP の安定性に影響を与える、次のあまり望ましくない回避策のいずれかを使用できます。
  - ブリッジ グループおよびメンバー インターフェイスでインターフェイス モニタリングを無効にします。
  - フェールオーバー基準のインターフェイス保留時間を、ユニットがフェールオーバーする前に STP が収束できる大きな値に増やします。
  - スイッチの STP タイマーを短くして、STP がインターフェイス保留時間よりも早く収束できるようにします。

フェールオーバーのヘルス モニタリング

Firewall Threat Defenseデバイスは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニターします。この項では、各装置の状態を判断するために、Firewall Threat Defenseデバイスがテストを実行する方法について説明します。

装置のヘルス モニターリング

Firewall Threat Defense デバイスは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバーリンクを含む各データインターフェイスでLANTESTメッセージを送信し、ピアが応答するかどうかを確認します。Firewall Threat Defenseデバイスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- Firewall Threat Defenseデバイスがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- Firewall Threat Defense デバイスがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- Firewall Threat Defenseデバイスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

ユニットは、モニター対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に、インターフェイス テストを実行します。1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、デバイスはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）] > [フェールオーバートリガー条件（Failover Trigger Criteria）]** を参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したデバイスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

インターフェイスにIPv4およびIPv6アドレスが設定されている場合、デバイスはIPv4を使用してヘルス モニタリングを実行します。インターフェイスにIPv6アドレスだけが設定されている場合、デバイスはARPではなくIPv6ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャストpingテストの場合、デバイスはIPv6全ノード アドレス（FE02::1）を使用します。

インターフェイス テスト

Firewall Threat Defenseデバイスでは、次のインターフェイス テストが使用されます。各テストの時間は約1.5秒。

1. リンクアップ/ダウンテスト：インターフェイス ステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、デバイスは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、デバイスはネットワーク アクティビティを実行します。

2. ネットワーク アクティビティ テスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはARPテストを開始します。

3. ARPテスト：ARPが正しく応答するかどうかをテストします。各ユニットは、ARPテーブル内の最新のエントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットがARP応答を受信しない場合、デバイスは、ARPテーブル内の「次の」エントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、デバイスはブートストラップpingテストを開始します。

4. ブロードキャストPingテスト：ping応答が正しいかどうかをテストします。各ユニットがブロードキャストpingを送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARPテストを使用してテストが再開されます。両方の装置がARPおよびブロードキャストpingテストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Normal (Waiting)：インターフェイスは起動していますが、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Normal (Not-Monitored)：インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- Link Down (Waiting)：インターフェイスまたは VLAN は管理上ダウンしており、ピア ユニットの対応するインターフェイスからまだ hello パケットを受信していません。
- Link Down (Not-Monitored)：インターフェイスまたは VLAN は管理上ダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- No Link：インターフェイスの物理リンクがダウンしています。
- No Link (Waiting)：インターフェイスの物理リンクがダウンしており、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。
- No Link (Not-Monitored)：インターフェイスの物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー トリガーおよび検出タイミング

Firepower ハイアベイラビリティペアでは、次のイベントでフェールオーバーがトリガーされます。

- アクティブユニットの 50% を超える Snort インスタンスがダウンした場合
- アクティブユニットのディスク容量使用率が 90% を超えた場合
- アクティブユニットで **no failover active** コマンドが実行された場合、またはスタンバイユニットで **failover active** コマンドが実行された場合
- アクティブユニットで障害が発生したインターフェイスの数がスタンバイユニットよりも多くなった場合
- アクティブデバイスのインターフェイス障害が設定されたしきい値を超えた場合

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

表 *2:*

コマンド	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	デフォルトのフェールオーバー基準を変更します。 インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。 インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。フェールオーバーが発生した場合、フェールオーバーの理由およびその他のハイ アベイラビリティ ペアに関するさまざまな作業をメッセージ センターで表示できます。これらのしきい値は、指定した最小値と最大値の範囲内の値に設定できます。

表 *3: Firewall Threat Defense* フェールオーバー時間

フェールオーバートリガー イベント	最小	デフォルト	最大数
アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター対象インターフェイスまたはフェールオーバーリンクでhelloメッセージを受信しなくなる。	800 ミリ秒	15 秒	45 秒
アクティブユニットインターフェイス物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。	5 秒	25 秒	75 秒

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Firewall Threat Defense デバイスに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーを設定する場合は、一つの装置をプライマリに設定し、もう一つの装置をセカンダリに設定します。設定時に、プライマリ装置のポリシーがセカンダリ装置に同期されます。この時点で、2 つの装置は、デバイスおよびポリシー設定用の単一のデバイスとして機能します。ただし、イベント、ダッシュボード、レポート、およびヘルス モニタリングについては、引き続き個別のデバイスとして表示されます。

フェールオーバーペアの2つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用し、どちらの装置でアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ装置の MAC アドレスは常にアクティブ IP アドレスと組み合わされます。このルールの例外は、セカンダリ装置がアクティブになり、フェールオーバー リンク経由でプライマリ装置の MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイフェールオーバーでは、フェールオーバーは装置ごとに行われます。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *4:* フェールオーバー イベント

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
アクティブユニットが故障(電源またはハードウェア)	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	モニタ対象インターフェイスまたはフェールオーバーリンクでhelloメッセージが受信されることはありません。
以前にアクティブだったユニットが復旧	フェールオーバーなし	スタンバイになる	なし	なし。
スタンバイユニットが故障(電源またはハードウェア)	フェールオーバーなし	スタンバイに故障とマークする	該当なし	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる フェールオーバーリンクに故障とマークする	アクティブになる フェールオーバーリンクに故障とマークする	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステート リンクの障害	フェールオーバーなし	なし	なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
しきい値を超えたアクティブユニットでインターフェイスに障害が発生	フェールオーバー	アクティブを障害としてマークする	アクティブになる	なし。
しきい値を超えたスタンバイユニットでインターフェイスに障害が発生	フェールオーバーなし	なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

設定同期の最適化

デバイスが一時停止後に再起動するか、高可用性を再開する場合、参加するデバイスは実行中の設定をクリアします。次に、アクティブデバイスが、設定全体を参加デバイスに送信して完全に同期します。アクティブデバイスの設定が大規模な場合、このプロセスには数分かかることがあります。

設定同期最適化機能により、設定ハッシュ値を交換して、参加ユニットとアクティブユニットの設定を比較できます。アクティブデバイスと参加デバイスの両方で計算されたハッシュが一致する場合、参加デバイスは完全な設定同期をスキップし、高可用性設定に再参加します。この機能により、さらに迅速なピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。

設定同期の最適化のガイドラインと制限事項

- 設定同期最適化機能は、デフォルトで有効になっています。
- Firewall Threat Defense のマルチコンテキストモードは、完全な設定同期中にコンテキストの順序を共有することによって設定同期最適化をサポートし、後続のノード再参加中にコンテキストの順序を比較できるようにします。
- パスフレーズとフェールオーバー IPsec キーを設定すると、アクティブユニットとスタンバイユニットで計算されたハッシュ値が異なるため、設定同期の最適化で効果を得られません。
- ダイナミック ACL または SNMPv3 を使用してデバイスを設定すると、設定同期最適化は効果を発揮しません。
- アクティブデバイスは、デフォルトの動作として、LAN リンクのフラッピングによって完全な設定を同期します。アクティブデバイスとスタンバイデバイス間のフェールオーバーフラッピングの間、設定同期最適化はトリガーされず、デバイスによって完全な設定同期が実行されます。
- 高可用性設定が中断やアクティブデバイスとスタンバイデバイス間のネットワーク通信の切断から復旧する際に、設定同期最適化がトリガーされます。

設定同期の監視

設定同期最適化機能が有効になっている場合、syslog メッセージが生成され、アクティブユニットと参加ユニットで計算されたハッシュ値が一致するか、一致しないか、または操作がタイムアウトになったかどうかが表示されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

ハイアベイラビリティの要件と前提条件

モデルのサポート

Secure Firewall Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

高可用性 のガイドライン

モデルのサポート

- Firepower 1010：
  - 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の 高可用性 のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、高可用性 を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
  - ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。
- Firepower 9300：シャーシ内ハイ アベイラビリティはサポートされません。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の Firewall Threat Defense Virtual では、レイヤ 2 接続が必要なため、高可用性 はサポートされません。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチで STP PortFast 機能を有効にすることができます。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モード インターフェイスとブリッジ グループ インターフェイスの両方に接続されたスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは STP に参加し続けます。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- Firewall Threat Defense デバイス フェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。

- アクティブ/スタンバイ 高可用性 と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニターすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

- 高可用性ペアの作成中にピアデバイスのいずれかで clish を実行すると、両方のピアデバイスが不明状態になり、高可用性設定が失敗します。

- フェールオーバーの直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバー インターフェイス アドレスになります。

- （フェールオーバー中に）コンバージェンスを向上させるには、どの設定やインスタンスにも関連付けられていない HA ペアのインターフェイスをシャットダウンする必要があります。

- 評価モードでフェールオーバー暗号化を設定すると、システムは暗号化に DES を使用します。エクスポート準拠アカウントを使用してデバイスを登録すると、デバイスはリブート後に AES を使用します。したがって、アップグレードのインストール後など、何らかの理由でシステムがリブートすると、ピアは通信できなくなり、両方のユニットがアクティブユニットになります。デバイスを登録するまで、暗号化を設定しないことを推奨します。評価モードで暗号化を設定する場合は、デバイスを登録する前に暗号化を削除することを推奨します。

- フェールオーバーで SNMPv3 を使用する場合、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットにレプリケートされません。ユーザーを削除して再追加し、設定を再展開して、ユーザーを新しいユニットに強制的にレプリケートする必要があります。

- デバイスは、SNMP クライアントのエンジンデータをピアと共有しません。
- 非常に多数のアクセスコントロールルールとNATルールがある場合、設定のサイズによって効率的な設定のレプリケーションが妨げられる可能性があり、その結果、スタンバイユニットがスタンバイ準備完了状態に達するまでの時間が長くなります。これは、コンソールまたは SSH セッションを介したレプリケーション中にスタンバイユニットに接続する機能にも影響を与える可能性があります。設定のレプリケーションのパフォーマンスを向上させるには、**asp rule-engine transactional-commit access-group** および **asp rule-engine transactional-commit nat** コマンドを使用して、アクセスルールと NAT の両方でトランザクションコミットを有効にします。
- スタンバイロールに移行する 高可用性 ペアのユニットは、アクティブユニットとクロックを同期します。

  例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- 高可用性のユニットは、クロックを動的に同期しません。同期が行われるときのイベントの例を次に示します。
  - 新しい 高可用性 ペアが作成される。
  - 高可用性 が中断されて再作成される。
  - フェールオーバーリンクを介した通信が中断され、再確立される。
  - **no failover/failover** または **configure high-availability suspend/resume**（Firewall Threat Defense）コマンドを使用して、フェールオーバーステータスが CLI で手動で変更された。
- 高可用性 を有効にすると、すべてのルートが強制的に削除され、高可用性 の進行がアクティブ状態に変わった後に再度追加されます。このフェーズ中に接続が失われる可能性があります。
- プライマリユニットを置き換える場合は、高可用性を再作成するときに、交換ユニットをセカンダリユニットとして設定し、以前のセカンダリユニットから交換ユニットに設定が複製されるようにする必要があります。交換ユニットをプライマリとして設定すると、運用中ユニットの設定が誤って上書きされます。
- Firepower 1100 および 2100 デバイスが高可用性で展開されており、それらのデバイスで何百ものインターフェイスが設定されている場合、フェールオーバー時間の遅延（秒単位）が増加する可能性があります。

- 高可用性 設定では、一般にポート 53 を使用する短時間の接続はすぐに閉じられ、それらの接続がアクティブからスタンバイに転送または同期されることはありません。そのため、両方の 高可用性 デバイスの接続数に違いが生じる可能性があります。これは、短時間の接続の予期される動作です。長時間（たとえば、30 ～ 60 秒を超える）の接続の比較を試みることができます。
- 高可用性 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方の 高可用性 デバイスで接続数に違いが生じる可能性がありますが、これは予想されることです。
- フェールオーバー LAN リンクがバックツーバックで接続されておらず、代わりに 1 つ以上のスイッチを介して接続されている場合、中間経路内の障害によってアクティブユニットとスタンバイユニットの接続が失われ、アクティブ/スタンバイ状態の一貫性が失われる可能性があります。これは 高可用性 機能には影響しませんが、アクティブユニットとスタンバイユニット間のフェールオーバーリンク経路を確認して回復することをお勧めします。

  フェールオーバー LAN リンクがダウンしている場合、設定はピアユニットに複製されない可能性があるため、設定を展開することは推奨されません。
- Cisco Secure Firewall Threat Defense Virtual スタートアップガイド を参照し、Firewall Threat Defense Virtual のデバイス設定で高可用性を確認してください。
- トランスペアレント モードにおいて、アクティブ ユニットでホットスタンバイ ルータ（HSRP）の MAC アドレスが失われるという問題が発生した場合は、MAC アドレスのスタティック マッピングを作成します。
- 脅威防御デバイス が高可用性の場合、UCAPL または CC コンプライアンスモードは変更できません。高可用性ペアを形成する前に、コンプライアンス モードを変更します。

ハイ アベイラビリティ ペアの追加

アクティブ/スタンバイのハイアベイラビリティペアを確立するには、一方のデバイスをプライマリ、他方をセカンダリとして指定します。Firewall Management Center は、マージした設定をペア内のデバイスに展開します。競合がある場合は、プライマリデバイスの設定が使用されます。

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。

（注） フェールオーバーリンクとステートフル フェールオーバー リンクはプライベート IP スペースにあり、ハイアベイラビリティペアのピア間の通信にのみ使用されます。ハイアベイラビリティが確立された後に、選択したインターフェイスリンクと暗号化設定の変更を行うと、ハイアベイラビリティペアが壊れ、再設定が必要になります。

注意 ハイアベイラビリティペアを作成または破棄すると、プライマリデバイスとセカンダリデバイスで Snort プロセスがただちに再起動され、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。ハイアベイラビリティペアの作成を続けると、プライマリデバイスとセカンダリデバイスで Snort プロセスが再起動され、キャンセルすることができるという警告が表示されます。

始める前に

以下の点について両方のデバイスを確認してください。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。
- ドメインおよびグループが同じであること。
- 通常のヘルス ステータスであり、同じソフトウェアを実行していること。
- ルーティングされているか、またはトランスペアレント モードであること。
- 同じ NTP コンフィギュレーションであること。時刻の同期を参照してください。
- 未確定の変更がない状態で、完全に展開されていること。
- すべてのインターフェイスで DHCP または PPPoE が設定されていないこと。

（注） プライマリデバイスで利用可能な証明書がセカンダリデバイスに存在しない場合は、2 台の Firewall Threat Defense デバイス間でハイアベイラビリティを構成することができます。ハイアベイラビリティが構成されると、証明書がセカンダリデバイス上で同期されます。

手順

ステップ 1 デバイスの追加 に従って、両方のデバイスを Firewall Management Center に追加します。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 3 [追加（Add）] ドロップダウンメニューから、[高可用性（High Availability）] を選択します。

ステップ 4 ハイアベイラビリティペアの表示用の [名前（Name）] を入力してください。

ステップ 5 [デバイス タイプ（Device Type）] では、[Firepower Threat Defense] を選択します。

ステップ 6 ハイアベイラビリティペアの [プライマリピア（Primary Peer）] デバイスを選択します。

ステップ 7 ハイアベイラビリティペアの [セカンダリピア（Secondary Peer）] デバイスを選択します。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 [LANフェールオーバーリンク（LAN Failover Link）] では、フェールオーバーの通信のための十分な帯域幅の [インターフェイス（Interface）] を選択します。

（注）
論理名がなくセキュリティゾーンに属さないインターフェイスのみが、[ハイアベイラビリティペアの追加（Add High Availability Pair）] ダイアログの [インターフェイス（Interface）] ドロップダウンに一覧表示されます。

ステップ 10 識別するための任意の [論理名（Logical Name）] を入力します。

ステップ 11 アクティブなユニットの、フェールオーバー リンクの [プライマリ IP（Primary IP）] アドレスを指定します。

このアドレスは、未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254 または /31）にすることができます。

（注）
169.254.1.0/24 や fd00:0:0:*::/64 は内部で使用されるサブネットです。フェールオーバーやステートリンクには使用できません。

ステップ 12 必要に応じて、[IPv6 アドレスを使用（Use IPv6 Address）] を選択します。

ステップ 13 スタンバイ ユニットのフェールオーバー リンクの [セカンダリ IP（Secondary IP）] アドレスを指定します。この IP アドレスはプライマリ IP アドレスのように、同じサブネット内になければなりません。

ステップ 14 IPv4 アドレスを使用する場合、プライマリとセカンダリの IP アドレス両方に適用されるサブネットマスクを入力します。

ステップ 15 必要に応じて、[ステートフルフェールオーバーリンク（Stateful Failover Link）] では、同じ**インターフェイス**を選択するか、または別のインターフェイスを選択し、ハイアベイラビリティの設定情報を入力します。

このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254 または /31）にすることができます。

（注）
169.254.1.0/24 や fd00:0:0:*::/64 は内部で使用されるサブネットです。フェールオーバーやステートリンクには使用できません。

ステップ 16 必要に応じて、フェールオーバー リンク間の IPsec 暗号化について、[有効（Enabled）] を選択し、さらに [キー生成（key generate）] メソッドを選択します。

ステップ 17 [OK] をクリックします。システム データの同期が行われるため、このプロセスが完了するまでに数分かかります。

次のタスク

デバイスをバックアップします。バックアップを使用することで、障害が発生したデバイスを迅速に交換し、Firewall Management Center からリンク解除せずにハイ アベイラビリティ サービスを復旧できます。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

オプションの高可用性パラメータの設定

最初の高可用性構成を Firewall Management Center で確認できます。高可用性ペアを解除して再設定しないと、これらの設定を編集することはできません。

フェールオーバーの結果を改善するために、フェールオーバートリガー条件を編集できます。インターフェイス モニタリングでは、どのインタフェースがフェイルオーバーに適しているかを判断できます。

スタンバイ IP アドレスとインターフェイス モニタリングの設定

各インターフェイスにスタンバイ IP アドレスを設定します。推奨されてはいますが、スタンバイアドレスは必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。

デフォルトでは、論理名が設定されているすべての物理インターフェイス、Firepower 1010、のすべての VLAN インターフェイスでモニタリングが有効になっています。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。 インターフェイス モニタリングの場合、Firepower 1010 スイッチポートが対象です。

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（Edit）]（✎） をクリックします。

ステップ 3 [High Availability] タブをクリックします

ステップ 4 [モニタ対象インターフェイス（Monitored Interfaces）] エリアで、編集するインターフェイスの横にある [編集（Edit）]（✎） をクリックします。

ステップ 5 [このインターフェイスの障害をモニタする（Monitor this interface for failures）] チェック ボックスをオンにします。

ステップ 6 [IPv4] タブで、[スタンバイIPアドレス（Standby IP Address）] を入力します。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。

ステップ 7 IPv6 アドレスを手動で設定した場合、[IPv6] タブでアクティブ IP アドレスの横にある [編集（Edit）]（✎） をクリックして、[スタンバイIPアドレス（Standby IP Address）] を入力し、[OK] をクリックします。

このアドレスは、アクティブ IP アドレスと同じネットワーク上のフリー アドレスである必要があります。自動生成 [EUI 64の適用（Enforce EUI 64）] アドレスの場合、スタンバイ アドレスは自動的に生成されます。

ステップ 8 **[OK]** をクリックします。

ハイ アベイラビリティ フェールオーバー条件の編集

ネットワーク配置に基づいてフェールオーバー条件をカスタマイズできます。

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（Edit）]（✎） をクリックします。

ステップ 3 [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 4 [フェールオーバートリガー条件（Failover Trigger Criteria）] の横にある [編集（Edit）]（✎）をクリックします。

ステップ 5 [インターフェイス障害しきい値（Interface Failure Threshold）] で、デバイスがフェールオーバーする条件となるインターフェイスの失敗の数または割合を選択します。

ステップ 6 [helloパケット間隔（Hello packet Intervals）] で、フェールオーバー リンクを介して送信される hello パケットの頻度を選択します。

（注）
Firepower 2100 でリモートアクセス VPN を使用する場合は、デフォルトの hello パケット間隔を使用します。使用しない場合は、CPU使用率が高くなる場合があり、フェールオーバーを発生させる可能性があります。

ステップ 7 **[OK]** をクリックします。

仮想 MAC アドレスを設定します。

フェールオーバーのため、Secure Firewall Management Center で以下の方法を使用して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定できます。

- インターフェイスの設定中に、[インターフェイスの編集（Edit Interface）] ページの [詳細（Advanced）] タブ。MAC アドレスの設定 を参照してください。
- [高可用性（High Availability）] ページからアクセスする [インターフェイスMACアドレスの追加（Add Interface MAC Address）] ダイアログボックス。この手順を参照してください。

（注） （MAC アドレスが両方の高可用性ユニットへのすべてのサブインターフェイスに転送されるように）プライマリユニットとセカンダリユニットの両方で MAC アドレスを設定する場合に推奨されるアプローチは、[インターフェイス（Interfaces）] タブを使用して、アクティブおよびスタンバイの両方の高可用性ユニットのサブインターフェイスに MAC アドレスを複製することです。

両方の場所でアクティブ MAC アドレスとスタンバイ MAC アドレスを設定した場合、フェイルオーバーではインターフェイス設定で定義されたアドレスが優先されます。

物理インターフェイスにアクティブ MAC アドレスとスタンバイ MAC アドレスを指定することでフェールオーバー中のトラフィック喪失を最低に抑えることができます。この機能は、フェールオーバーのための IP アドレスのマッピングに冗長性を提供します。

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（Edit）]（） をクリックします。

ステップ 3 [ハイ アベイラビリティ（High Availability）] をクリックします。

ステップ 4 インターフェイス MAC アドレスの横にある [追加（Add）] (+) アイコンを選択します。

ステップ 5 [物理インターフェイス（Physical Interface）] を選択します。

ステップ 6 [アクティブインターフェイスMACアドレス（Active Interface Mac Address）] を入力します。

ステップ 7 [スタンバイインターフェイスMACアドレス（Standby Interface Mac Address）] を入力します。

ステップ 8 [OK] をクリックします。

（注）
詳細については、「Firepower アプライアンスでの FTD 高可用性の設定」の タスク 2、手順 10 ～ 14 を参照してください。

。

高可用性 の管理

この項では、高可用性の設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、高可用性 を有効化した後に 高可用性 装置を管理する方法について説明します。

Firewall Threat Defense 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

Firewall Threat Defense ハイアベイラビリティペアを確立した後、アクティブユニットとスタンバイユニットを手動で切り替えることができます。そうすることで、現在のアクティブユニットにおける持続的な障害やヘルスイベントなどに起因するフェールオーバーを効果的に実施できます。この手順を実行する前に、両方のユニットを完全に展開しておく必要があります。

始める前に

単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新 （29 ページ）。これにより、Firewall Threat Defense ハイ アベイラビリティ デバイス ペアのステータスと Firewall Management Center のステータスが同期されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 アクティブピアを変更するハイアベイラビリティペアの横にある [アクティブピアの切り替え（Switch Active Peer）] 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 デバイスをアクティブ デバイス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。

単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新

Firewall Threat Defense 高可用性ペアのアクティブデバイスまたはスタンバイデバイスが再起動されると、いずれのデバイスについても、Firewall Management Center に正確な高可用性ステー

タスが表示されない場合があります。これは、デバイスが再起動すると、高可用性ステータスがデバイス上でただちに更新され、対応するイベントがFirewall Management Centerに送信されるためです。ただし、デバイスとFirewall Management Center間の通信がまだ確立されていないため、ステータスが Firewall Management Center で更新されないことがあります。

Firewall Management Centerとデバイスの間で通信障害が発生したり、通信チャネルが不安定になったりすると、データの同期が失われる可能性があります。ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスを切り替えると、かなりの時間が経過しても変更が Firewall Management Center に反映されないことがあります。

これらのシナリオでは、ハイ アベイラビリティ ノードのステータスを更新して、ハイ アベイラビリティ ペアのアクティブ デバイスとスタンバイ デバイスに関する正確な情報を取得できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 ノードステータスを更新するハイアベイラビリティペアの横にある [HA ノードのステータス更新（Refresh HA Node Status）] をクリックします。

ステップ 3 [はい（Yes）] をクリックすると、ノードのステータスが更新されます。

ハイ アベイラビリティの中断と再開

高可用性ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバーリンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイ ユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。

高可用性を中断する場合、現在アクティブなデバイスはアクティブなままで、すべてのユーザー接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。

高可用性の中断と高可用性の無効化の主な違いは、中断された高可用性デバイスでは高可用性設定が保持されることです。高可用性を無効化すると、設定は消去されます。そのため、中断されたシステムで高可用性を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバーペアとして再び機能します。

高可用性を中断するには、**configure high-availability suspend** コマンドを使用します。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
```

```
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

アクティブ装置から高可用性を中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置のインターフェイス設定も消去されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

フェールオーバーを再開するには、**configure high-availability resume** コマンドを使用します。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピアユニットとアクティブ/スタンバイ ステータスをネゴシエートします。

（注） ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

Firewall Threat Defense ハイアベイラビリティペアでのユニット交換

バックアップファイルを使用して Firewall Threat Defense 高可用性ペアの障害が発生したユニットを交換するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Restoring Firewall Management Centers and Managed Devices*」を参照してください。

障害が発生したデバイスのバックアップがない場合は、ハイアベイラビリティを解除する必要があります。その後に、交換用デバイスを Secure Firewall Management Center に登録し、ハイアベイラビリティを再確立します。このプロセスは、デバイスがプライマリかセカンダリかによって異なります。

- バックアップなしでのプライマリ Firewall Threat Defense HA ユニットの交換（31 ページ）
- バックアップなしでのセカンダリ Firewall Threat Defense HA ユニットの交換（32 ページ）

バックアップなしでのプライマリ Firewall Threat Defense HA ユニットの交換

次に示す手順に従って、Firewall Threat Defense の高可用性ペアで障害が発生したプライマリユニットを交換します。ここに示した手順に従わないと、既存の高可用性設定を上書きする可能性があります。

⚠

注意 Firewall Threat Defense の高可用性ペアを作成または分断すると、プライマリおよびセカンダリ デバイスの Snort プロセスがすぐに再起動され、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。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスでSnortプロセスが再起動され、キャンセルすることができるという警告が表示されます。

⚠

注意 ディスクのイメージを再作成せずに、センサーまたはFirewall Management Centerから別のデバイスにディスクを移動しないでください。これはサポートされていない構成であり、機能が損なわれる可能性があります。

手順

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。高可用性ペアの解除 （33 ページ）を参照してください。

（注）
切断操作により、Firewall Threat Defense と Firewall Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 障害が発生したプライマリ Firewall Threat Defense デバイスの登録を Firewall Management Center から解除します。「Firewall Management Center からのデバイスの削除（登録解除）」を参照してください。

ステップ 3 交換用の Firewall Threat Defense を Firewall Management Center に登録します。「デバイスの追加」を参照してください。

ステップ 4 登録時には、既存のセカンダリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。ハイ アベイラビリティ ペアの追加 （23 ページ）を参照してください。

バックアップなしでのセカンダリ Firewall Threat Defense HA ユニットの交換

次に示す手順に従って、Firewall Threat Defense の高可用性ペアで障害が発生したセカンダリユニットを交換します。

⚠

注意 Firewall Threat Defense の高可用性ペアを作成または分断すると、プライマリおよびセカンダリデバイスの Snort プロセスがすぐに再起動され、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。ハイ アベイラビリティ ペアの作成を続けると、プライマリ デバイスとセカンダリ デバイスでSnortプロセスが再起動され、キャンセルすることができるという警告が表示されます。

手順

ステップ 1 [強制切断（Force Break）] を選択して、高可用性ペアを分離します。高可用性ペアの解除 （33 ページ）を参照してください。

（注）
切断操作により、Firewall Threat Defense と Firewall Management Center から HA に関連するすべての設定を削除し、後で手動で再作成する必要があります。同じ HA ペアを正常に設定するには、HA 切断操作を実行する前に、すべてのインターフェイス/サブインターフェイスの IP、MAC アドレス、およびモニタリング設定を保存してください。

ステップ 2 セカンダリ Firewall Threat Defense デバイスの登録を Firewall Management Center から解除します。「Firewall Management Center からのデバイスの削除（登録解除）」を参照してください。

ステップ 3 交換用の Firewall Threat Defense を Firewall Management Center に登録します。「デバイスの追加」を参照してください。

ステップ 4 登録時には、既存のプライマリ/アクティブ ユニットをプライマリ デバイスとして使用し、交換したデバイスをセカンダリ/スタンバイ デバイスとして使用して、高可用性を設定します。ハイ アベイラビリティ ペアの追加 （23 ページ）を参照してください。

高可用性ペアの解除

高可用性ペアを解除すると、高可用性設定が両方のユニットから削除されます。

アクティブユニットは稼働状態を維持し、トラフィックを転送します。スタンバイユニットのインターフェイス設定は消去されます。

解除操作の前にアクティブユニットに展開されていなかったポリシーは、解除操作が完了しても引き続き展開されないままになります。解除操作が完了した後に、スタンドアロンデバイスにポリシーを展開してください。

（注）

- Firewall Threat Defense デバイスの高可用性インターフェイスで IPsec が有効になっている場合、デバイスは、暗号化されたパケットを優先順位の高い受信キューに入れることができません。その結果、大量のデータトラフィックのシナリオでは、デバイスが多数の暗号化された接続を効率的に管理および優先順位付けできないため、高可用性を解除しようとしても失敗する可能性があります。デバイスのリソース使用率と最大スループットを表示するには、`show resource usage` コマンドを使用します。
- Firewall Management Center を使用して高可用性ペアに到達できない場合、手動で高可用性を解除するには、各デバイスの CLI に接続し、**configure high-availability disable** を入力します。削除（登録解除）高可用性ペアのと新しい Firewall Management Center への登録（35 ページ）も参照してください。

注意 Firewall Threat Defense の高可用性ペアを解除すると、プライマリユニットとセカンダリユニットの Snort プロセスが直ちに再起動され、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。

始める前に

- 単一の Firewall Threat Defense 高可用性ペアのノードステータスの更新 （29 ページ）。これにより、高可用性ペアのステータスと Firewall Management Center のステータスが同期されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 解除する高可用性ペアの横にある [HAの解除（Break HA）] をクリックします。

ステップ 3 スタンバイピアが応答しない場合は、[強制解除（Force Break）] をオンにします。

ステップ 4 [はい（Yes）] をクリックします。

解除操作によって、アクティブおよびスタンバイユニットから高可用性設定が削除されます。

アクティブユニットに展開されている FlexConfig ポリシーでは、高可用性解除操作後に展開の失敗が表示される場合があります。FlexConfig ポリシーを変更してアクティブユニット上に再展開する必要があります。

次のタスク

アクティブユニット上で FlexConfig ポリシーを使用している場合は、FlexConfig ポリシーを変更して再展開して展開エラーを解消します。

（注） 高可用性を解除した後も、アクティブユニットとして動作していた Firewall Threat Defense デバイスには、スタンバイユニットの IP アドレスが設定されたままになります。これを解決するには、以前アクティブであった Firewall Threat Defense デバイスで追加の展開を実行し、スタンバイユニットの IP アドレスを設定から削除します。

削除（登録解除）高可用性ペアのと新しい Firewall Management Center への登録

Firewall Management Center からペアを登録解除できます。その場合、高可用性ペアはそのまま維持されます。ペアを新しい Firewall Management Center に登録する場合または Firewall Management Center がペアに到達できなくなった場合は、ペアを登録解除できます。

高可用性ペアを登録解除すると、次のようになります。

- Firewall Management Center とペアとの間のすべての通信が切断されます。
- [デバイス管理（Device Management）] ページからペアが削除されます。
- ペアのプラットフォーム設定ポリシーで、NTP を使用して Firewall Management Center から時間を受信するように設定されている場合は、ペアがローカル時間管理に戻されます。
- 設定はそのままになるため、ペアはトラフィックの処理を続行します。

  NAT や VPN などのポリシー、ACL、およびインターフェイス構成は維持されます。

同じまたは別の Firewall Management Center にペアを再登録すると、設定が削除されるため、ペアはその時点でトラフィックの処理を停止します。高可用性設定はそのまま維持されるため、ペア全体を追加できます。登録時にアクセス コントロール ポリシーを選択できますが、トラフィックを再度処理する前に、登録後に他のポリシーを再適用してから設定を展開する必要があります。

始める前に

- この手順では、プライマリユニットへの CLI アクセスが必要です。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 登録解除する高可用性ペアの横にあるを [その他（More）] (⋮) クリックし、**[削除（Delete）]** を選択します。

ステップ 3 [はい（Yes）] をクリックします。デバイス高可用性ペアが登録解除されます。

ステップ 4 プライマリユニットを新しいデバイスとして追加することで、新しい（または同じ）Firewall Management Center にペアを登録できます。

a) 一方のユニットの CLI に接続して、**show failover** コマンドを入力することにより、プライマリユニットを確認します。

出力の最初の行に、このユニットがプライマリかセカンダリかが示されます。

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) プライマリユニットの CLI で、**configure manager add** コマンドを使用して新しい Firewall Management Center を特定します。Firewall Threat Defense 管理インターフェイスの CLI での変更を参照してください。

c) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、**[追加（Add）]** > **[デバイス（Device）]** をクリックします。

プライマリユニットをデバイスとして追加するだけで、Firewall Management Center がセカンダリユニットを検出します。

高可用性のモニタリング

このセクションの手順に従うことで、高可用性のステータスをモニターできます。

フェールオーバー履歴の表示

ハイアベイラビリティの両方のデバイスに関するフェールオーバーの履歴を 1 つのビューに表示できます。履歴は古いものから順番に表示され、すべてのフェールオーバーの理由が示されます。

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（Edit）]（✎） をクリックします。

ステップ 3 [サマリー（Summary）] を選択します。

ステップ 4 [一般（General）] で、[表示（View）]（  ）をクリックします。

ステートフル フェールオーバーの統計情報の表示

ハイ アベイラビリティ ペアのプライマリとセカンダリ デバイス両方のステートフル フェールオーバー リンク統計情報を表示できます。

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（Edit）]（  ） をクリックします。

ステップ 3 [高可用性（High Availability）] を選択します。

ステップ 4 ステートフル フェールオーバー リンクの下にある[表示（View）]（  ）をクリックします。

ステップ 5 統計情報を表示するデバイスを選択します。

高可用性の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
高可用性ペアの登録解除により、ペアを解除せずに再登録できるようになりました。	7.3	任意（Any）	高可用性ペアを削除（登録解除）する場合、CLI でペアを手動で解除し、スタンドアロンデバイスを再登録する必要がなくなりました。プライマリユニットを新しい Firewall Management Center に追加できるようになり、スタンバイユニットが自動的に検出されます。ペアを再登録すると設定が消去されるため、ポリシーを再適用する必要があります。
ポリシーのロールバックは高可用性でサポートされています	7.2	任意（Any）	**configure policy rollback** コマンドは高可用性でサポートされています。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
HA ピアリングを高速化する設定同期最適化機能	7.2	任意（Any）	設定同期最適化機能により、config-hash 値を交換して参加ユニットとアクティブユニットの設定を比較できます。アクティブユニットと参加ユニットの両方で計算されたハッシュが一致する場合、参加ユニットは完全な設定同期をスキップして HA に再参加します。この機能により、さらに迅速な HA ピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	7.1	任意（Any）	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
高可用性グループまたはクラスタ内のルートをクリアします。	7.1	任意（Any）	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在は、高可用性グループまたはクラスタで動作している場合、このコマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループやクラスタ内のすべてのユニットのルーティングテーブルをクリアします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細

FTD のハイアベイラビリティのハードニング	6.2.3	いずれか	バージョン 6.2.3 では、ハイアベイラビリティの FTD デバイスに関する次の機能が導入されています。
			• 高可用性ペアのアクティブまたはスタンバイ FTD デバイスが再起動されると、いずれの管理対象デバイスについても正確な高可用性ステータスが FMC に表示されない可能性があります。ただし、デバイスと FMC の間の通信がまだ確立されていないため、ステータスが FMC でアップグレードされないことがあります。[デバイス（Devices）] > [デバイス管理（Device Management）] ページの [ノードステータスの更新（Refresh Node Status）] オプションを使用すると、高可用性ユニットのステータスを更新して、高可用性ペアのアクティブデバイスとスタンバイデバイスに関する正確な情報を取得できます。
			• FMC UI の [デバイス（Devices）] > [デバイス管理（Device Management）] ページには、新しい [アクティブピアの切り替え（Switch Active Peer）] アイコンがあります。
			• バージョン 6.2.3 には、新しい REST API オブジェクト **Device High Availability Pair Services** が含まれており、次の 4 つの機能を備えています。
			  • **DELETE ftddevicehapairs**
			  • **PUT ftddevicehapairs**
			  • **POST ftddevicehapairs**
			  • **GET ftddevicehapairs**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。