



ハイ アベイラビリティ

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、脅威に対する防御 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 \(36 ページ\)](#)
- [設定の同期失敗のトラブルシューティング \(37 ページ\)](#)
- [高可用性の履歴 \(38 ページ\)](#)

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 Threat Defense デバイスが必要です。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 Threat Defense Virtual ではサポートされていません。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脅威に対する防御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 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に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。

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。
- 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。
- NTP 設定が同じであること。[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、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。
- (Firepower4100/9300) 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 Threat Defense デバイスのライセンス要件

高可用性構成の両方の Threat Defense ユニットの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、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、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い場合は、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）。

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とステートリンクの組み合わせには、10 GB のデータインターフェイスを使用することを推奨します。
- 他のすべてのモデル : 1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

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。

- 脅威に対する防御 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、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバーリンク専用のインターフェイス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 リンクとデータ リンクの中断の回避

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た場合、フェールオーバーが必要かどうかの決定に、Threat Defense デバイスはデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクの正常性が復元されるまで停止されます。

耐障害性フェールオーバー 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

2つの Threat Defense デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の 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 ❖❖❖非推奨

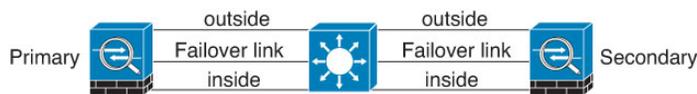
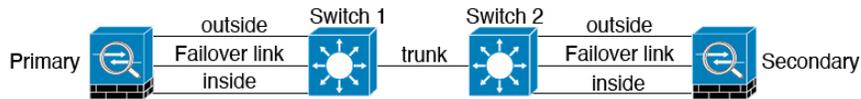


図 2: 2つのスイッチを使用した接続：非推奨



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、別の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

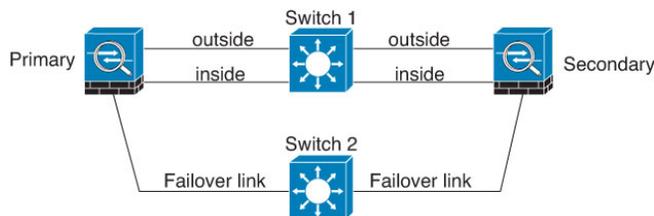
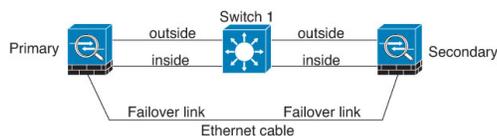


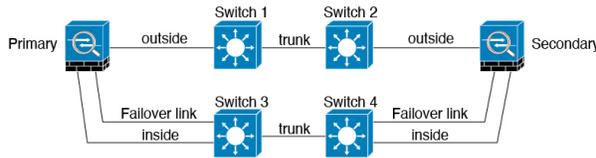
図 4: ケーブルを使用した接続



シナリオ 3 : 推奨

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:セキュアスイッチを使用した接続



シナリオ 4 : 推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバーリンクに冗長インターフェイスを使用します。

図 6:冗長インターフェイスを使用した接続

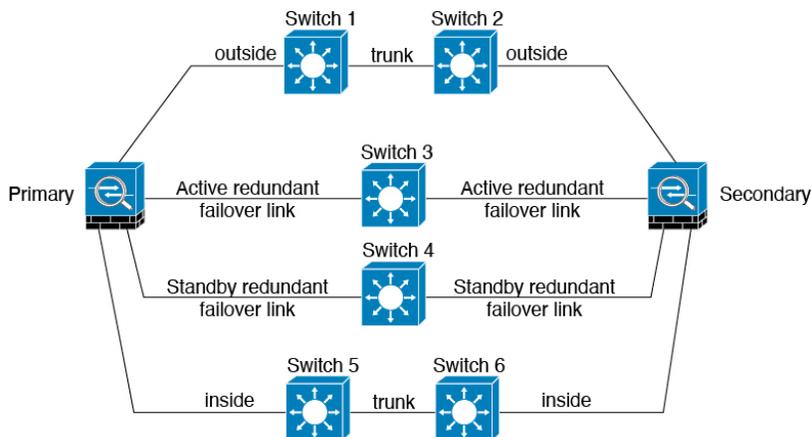
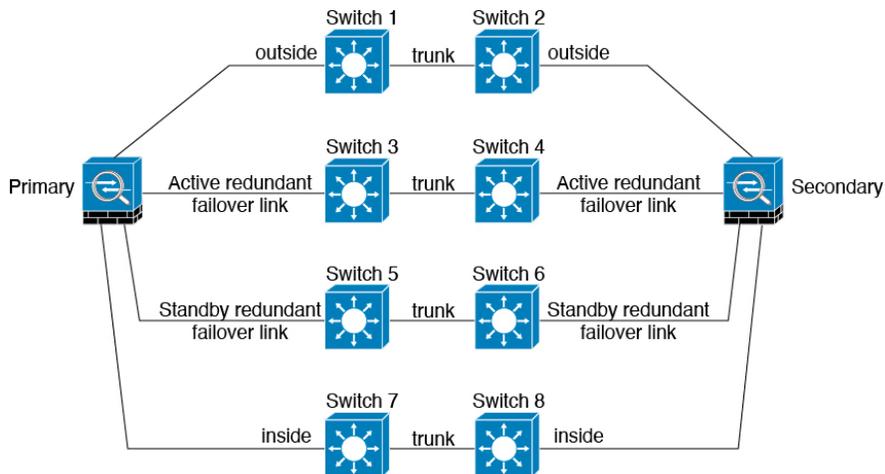


図 7: Inter-Switch Link (ISL) を使用した接続



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のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、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 アドレスの組み合わせについて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) スタンバイアドレスを設定することが推奨されていますが、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。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステートリンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

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 アドレスの使用については、次を参照してください。

1. アクティブな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. アクティブ装置が故障すると、スタンバイ装置は故障した装置の 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. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ 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ブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、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。これによって、ネットワークトラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

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。

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。Threat Defense デバイスは MAC アドレスを変更するときに、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 アドレスの変更を認識できません。

仮想 MAC アドレス

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つの方法のみを使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素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では、FXOS シャーシがすべてのインターフェイスのプライマリ MAC アドレスのみを自動生成します。プライマリ MAC アドレスとセカンダリ 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、セカンダリユニット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。

ステートフル フェールオーバー

ステートフル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 Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- 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 セッションとピンホール。

- **スタティックおよび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ダイナミックルーティングプロトコル（OSPF や EIGRP など）に参加するため、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による学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリユニットには最初にプライマリユニット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中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ています。



(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、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、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 とは関連性はありません。
- **アクセス コントロール ポリシーの判断**：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイルタイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような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されていれば、正常に同期は行われます。
 - **侵入検知状態**：フェールオーバーの際、フロー中に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**：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
 - **ファイル タイプ検出とブロッキング**：ファイルタイプは、フェールオーバー前に特定される必要があります。元のアクティブデバイスでファイルを特定している間にフェールオーバーが発生すると、ファイルタイプの同期は失われます。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る場合でも、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ー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ーと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。フェールオーバーの時点でアクティブ認証していたユーザーには、再度認証を求めるプロンプトが表示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から独立しているため、一般的に、フェールオーバーはこの機能には影響しません。具体的には次のとおりです。
 - 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した場合、ファイルイベントは生成されず、検出も発生しません。
 - 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）：事前分類中にフェールオーバーが発生した場合、検出は失敗します。
 - ファイルダイナミック分析（クラウドとの接続性）：フェールオーバーが発生しても、システムはクラウドにファイルを提出できます。
 - 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した場合、システムはファイル/アーカイブ内の可視性を失います。
 - カスタムブロッキング：フェールオーバーが発生した場合、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判断。ただし、フェールオーバーの時点で処理されていたDNSベースの判断は完了しません。
- RA VPN：リモートアクセスVPN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ASA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 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ず、新しいアクティブノードは、既存のインスペクションの判定を再利用して、正しいポリシールールを照合することができません。
- 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、スパン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。ポートは引き続き STP に参加しています。したがって、ポートがグ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witch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witch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

脅威に対する防御デバイスは、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、脅威に対する防御デバイスがテストを実行する方法について説明します。

装置のヘルスマニターリング

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。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。

- **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。
- **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。
- **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。

ハートビートモジュールの冗長性

HA の各ユニットは、クラスタ制御リンクを介してブロードキャスト キープアライブ ハートビート パケットを定期的送信します。コントロールプレーンがトラフィックの処理でビジー状態になっていると、ハートビートパケットがピアに届かなかつたり、CPU の過負荷が原因でピアがハートビートパケットを処理しないことがあります。設定可能なタイムアウト期間内にピアがキープアライブステータスを伝えられない場合、誤ったフェールオーバーまたはスプリットブレインシナリオが発生します。

データプレーンのハートビートモジュールは、コントロールプレーンでのトラフィックの輻輳による誤ったフェールオーバーまたはスプリットブレインの発生を回避するために役立ちます。

- 追加のハートビートモジュールは、コントロールプレーン モジュールと同様に機能しますが、データ プレーン トランスポート インフラストラクチャを使用してハートビート メッセージを送受信します。
- ピアがデータプレーンでハートビートパケットを受信すると、カウンタが増加します。
- コントロールプレーンでのハートビート転送が失敗した場合、ノードはデータプレーンのハートビートカウンタをチェックします。カウンタが増加している場合、ピアは稼働しており、この状況ではクラスタはフェールオーバーを実行しません。



- (注)
- HA が有効な場合、追加のハートビートモジュールは常にデフォルトで有効になっています。データプレーンの追加のハートビートモジュールのポーリング間隔を設定する必要はありません。このモジュールは、コントロールプレーンに設定したものと同一ハートビート間隔を使用します。

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

脅威に対する防御デバイスでは、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思われ見なされます。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思われ見なされ、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思われ見なされます。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思なされます。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思なされ、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思なされます。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思なされ、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があります。
- **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 は管理上ダウンしています。
- **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 1:

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、 <i>num</i> 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、 <i>num</i> 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 2: 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 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/セカンダリの役割とアクティブ/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、1つのユニットをプライマリとして設定し、もう1つのユニットをセカンダリとして設定します。設定中に、プライマリユニットのポリシーは、セカンダリユニットに同期化されます。この時点で、2つのユニットは、デバイスおよびポリシー設定に関して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マonitoringに関しては、別々のデバイスとして引き続き表示されます。

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットが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 ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニット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 ユニットが常にアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。この規則の例外は、セカンダリ ユニットがアクティブであり、フェールオーバーリンク経由でプライマリ ユニットの 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 ユニットの 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起動された場合は、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ユニットごとに行われます。

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）、アクティブユニットが行うアクション、スタンバイユニットが行うアクション、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 3: 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	注意
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	適用対象外	アクティブになる アクティブに故障とマークする	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 メッセージは受信されません。
以前にアクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	動作なし	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	適用対象外	スタンバイユニット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、アクティブユニット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、ユニットはスタンバイユニット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。

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	注意
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	動作なし	動作なし	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。
アクティブユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイユニット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、アクティブユニットはフェールオーバーを行いません。

設定同期の最適化

一時停止または再開フェールオーバーの後にノードの再起動かノードの再参加があった場合、参加ユニットは実行中の設定をクリアします。アクティブユニットは、完全な設定同期のために設定全体を参加ユニットに送信します。アクティブユニットに大きい設定がある場合、参加ユニットが設定を同期するまでに数分かかります。

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。

設定同期の最適化のガイドラインと制限事項

- **Threat Defense** バージョン 7.2 以降では、設定同期最適化機能がデフォルトで有効になっています。
- **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機能をサポートし、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、設定同期最適化機能は効果を発揮しません。
- アクティブユニットは、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。アクティブユニットとスタンバイユニット間のフェールオーバーフラッピングの間、設定同期最適化機能はトリガーされず、完全な設定同期が実行されます。

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ーできますが、スイッチポートはモニターできません。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せん。



(注) バージョン 6.5 以降を新規にインストールして Management Center バージョン 6.5 以降で管理している Firepower 1010 デバイスの場合、デフォルトのインターフェイスのタイプはスイッチポートになります。スイッチポート機能はフェールオーバーに対応していないため、それらのインターフェイスのスイッチポートをオフにし、展開してからフェールオーバーを作成します。6.5 より前のバージョンからアップグレードした Firepower 1010 システムの場合、デフォルトのインターフェイスはアップグレード前のバージョンと同じになります。

- 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 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、スパン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損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

interface interface_id spanning-tree portfast

この回避策は、ルーテッドモードおよびブリッジグループインターフェイスの両方に接続されている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。ポートは引き続き STP に参加しています。したがって、ポートがグ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。

- 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** (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。
- [Cisco Secure Firewall Threat Defense Virtual スタートアップガイド](#) を参照し、Threat Defense Virtual のデバイス設定で高可用性を確認してください。

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。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。



(注) データインターフェイスのマネージャアクセスでは、ルーテッドモードのみがサポートされること。

- NTP設定が同じであること。[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。
- データインターフェイスのマネージャアクセスの場合：
 - マネージャアクセスには、両方のデバイスで同じデータインターフェイスを使用します。
 - 冗長マネージャアクセスデータインターフェイスはサポートされていません。
 - DHCPは使用できません。静的IPアドレスのみがサポートされています。DDNSやゼロタッチプロビジョニングなど、DHCPに依存する機能は使用できません。

- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定 (**configure manager add** コマンド) を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。



(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 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** 登録キーを使用した **Management Center** へのデバイスの追加に従って、両方のデバイスを 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、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 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、どのインターフェイスがフェー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。スタンバイアドレスを設定することが推奨されていますが、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 フェールオーバー基準の編集

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。

仮想 MAC アドレスを設定します。

- 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ます、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、フェー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 **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。

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

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 Threat Defense 高可用性ペアのノードステータスの更新 \(30 ページ\)](#)。これにより、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 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 Threat Defense 高可用性ペアのノードステータスの更新

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、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 Management Center に送信されるためです。ただし、デバイスと 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 Management Center で更新されないことがあります。

Management Center とデバイスの間で通信障害が発生したり、通信チャン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 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-アクティブの状態で、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。

マネージャアクセスにデータインターフェイスを使用する場合、再開するまで管理接続は切断されます。

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-availability.
```

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。

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 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 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、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 Threat Defense HA ユニットの交換 \(32 ページ\)](#)
- [バックアップなしでのセカンダリ Threat Defense HA ユニットの交換 \(33 ページ\)](#)

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

次に示す手順に従って、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 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спек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спек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 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、Threat Defense と 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 Threat Defense デバイスの登録を Management Center から解除します。「[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 Threat Defense を Management Center に登録します。「[登録キーを使用した Management Center へのデバイスの追加](#)」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 Threat Defense HA ユニットの交換

次に示す手順に従って、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** 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спек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спек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、Threat Defense と 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 Threat Defense デバイスの登録を Management Center から解除します。「[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 Threat Defense を Management Center に登録します。「[登録キーを使用した Management Center へのデバイスの追加](#)」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。

マネージャアクセスに管理インターフェイスを使用する場合：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。

マネージャアクセスにデータインターフェイスを使用する場合：次の詳細を確認してください。

- 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データインターフェイスは、マネージャアクセスインターフェイスを除いてシャットダウンされます。マネージャアクセスインターフェイスは、スタンバイ IP アドレスを使用して稼働状態を維持するため、管理接続を維持できます。
- プライマリユニットがスタンバイ状態の場合：
 - マネージャアクセス用の IP アドレスは、Management Center 設定では永続的に交換されます（プライマリユニットはスタンバイ IP アドレスを使用し、セカンダリユニットはアクティブ IP アドレスを使用します）。
 - Management Center が管理接続を開始したとき、デバイスのホスト名が指定されている場合は、交換された IP アドレスが正しいホスト名に関連付けられるように DNS サーバーを更新する必要があります。
 - 高可用性を解除すると、スタンバイユニットへの展開が行われます。IP アドレスが交換されたために管理接続がまだ再確立されていない場合、展開が失敗する可能性があります。この場合は、後で（管理接続が確立された後に）展開を手動でトリガーする必要があります。アクティブユニットに変更を展開する前に、必ずスタンバイユニットへの展開を完了してください。

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) 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 Management Center への登録（35 ページ）も参照してください。



注意 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спек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спек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 **Threat Defense 高可用性ペアのノードステータスの更新（30 ページ）**。これにより、高可用性ペアのステータスと 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、その他のアクションのアイコン (⋮) をクリックし、[解除 (Break)] を選択します。

ステップ 3 スタンバイペ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。

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

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 Management Center に登録する場合または 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。

- 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 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 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 **その他** (⋮) をクリックし、[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) Management Center にペアを登録できます。
- 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

[...]
```
 - 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 Management Center を特定します。[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。
 - [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、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表示されます。

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。

設定の同期失敗のトラブルシューティング

フェールオーバーペアを形成すると、参加ユニットは実行コンフィギュレーションをクリアし、アクティブユニットから設定全体を複製します。設定全体の同期が完了すると、参加ユニットはスタンバイ準備完了の役割を担い、フェールオーバーペアを確立します。ユニットがフェールオーバーペアに参加すると、アクティブユニットの設定変更はスタンバイユニットにも複製され、両方のユニットの同期が維持されます。

スタンバイユニットが設定変更コマンドの複製に失敗した場合、設定の同期失敗を報告し、フェールオーバーを無効にして高可用性を終了します。ここでは、スタンバイユニットによつ

て報告された設定の同期失敗エラーを特定し、トラブルシューティングする手順について説明します。

設定の同期エラーまたは統計情報を表示するには、SSH セッションまたは Threat Defense CLI を介して以下の CLI コマンドを使用します。

- **show failover config-sync errors all** : フェールオーバーに関連するすべての設定同期エラーを表示します。
- **show failover config-sync stats all** : フェールオーバーの設定の同期に関する統計情報を表示します。

高可用性を再度有効にするには、以下を実行します。

- アクティブユニットで **failover reset** コマンドを実行して、フェールオーバーを再度有効にします。
- フェールオーバーを再度有効にできない場合は、スタンバイユニットが複製に失敗した設定変更を削除または更新してから、フェールオーバーを再度有効にします。

高可用性の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
マネージャ アクセス データインターフェイスでの高可用性のサポート	7.4	7.4	Threat Defense の高可用性を備えたマネージャアクセス用のデータインターフェイスを使用できるようになりました。
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 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。
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。

機能	最小 Management Center	最小 Threat Defense	詳細
<p>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。</p>	<p>7.1</p>	<p>任意 (Any)</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。
<p>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。</p>	<p>7.1</p>	<p>任意 (Any)</p>	<p>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。</p>

機能	最小 Management Center	最小 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	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • DELETE ftddevicepairs • PUT ftddevicepairs • POST ftddevicepairs • GET ftddevicepairs

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。