ASA/PIX：トランスペアレント モードでのアクティブ/スタンバイ フェールオーバーの設定

内容

概要

フェールオーバー設定には、同一セキュリティ アプライアンスが 2 台、専用のフェールオーバー リンク（およびオプションでステートフル フェールオーバー リンク）で相互に接続されている必要があります。アクティブ インターフェイスおよび装置のヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。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。

セキュリティ アプライアンスでは、次の 2 つのフェールオーバー コンフィギュレーションをサポートしています。

- アクティブ/アクティブ フェールオーバー
- アクティブ/スタンバイ フェールオーバー

各フェールオーバー設定には、フェールオーバーを決定して実行する固有の方法があります。アクティブ/アクティブ フェールオーバーの場合は、どちらのユニットもネットワーク トラフィックを渡すことができます。これにより、ネットワークにロード バランシングを設定できます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードで稼働するユニットでのみ使用できます。アクティブ/スタンバイ フェールオーバーの場合は、一方のユニットのみがトラフィックを渡すことができ、もう一方のユニットはスタンバイ状態で待機します。アクティブ/スタンバイ フェールオーバーは、シングル コンテキスト モードかマルチ コンテキスト モードのどちらで稼働するユニットでも使用できます。どちらのフェールオーバー設定でも、ステートフル フェールオーバーまたはステートレス（標準）フェールオーバーがサポートされます。

トランスペアレント ファイアウォールは、*bump-in-the-wire* または *ステルス ファイアウォール* のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。セキュリティ アプライアンスによって、その内部ポートおよび外部ポート上に同じネットワークが接続されます。ファイアウォールはルーティング ホップではないため、トランスペアレント ファイアウォールを既存のネットワークに簡単に導入できます。IP アドレスの再設定は必要ありません。デフォルトのルーテッド ファイアウォール モードまたは透過型ファイアウォール モードで稼働するように、適応型セキュリティ アプライアンスを設定できます。多くのコマンドが両方のモードではサポートされないため、モードを変更すると適応型セキュリティ アプライアンスによって設定がクリアされます。すでにデータを入力したコンフィギュレーションが用意されている場合、モードを変更する前に必ずそのコンフィギュレーションをバックアップしてください。新しいコンフィギュレーションを作成する際に、このバックアップ コンフィギュレーションを参照用に使用できます。トランスペアレント モードでファイアウォール アプライアンスを設定するときの詳細は、「PIX/ASA：透過型ファイアウォールの設定例」を参照してください。

このドキュメントでは、ASA セキュリティ アプライアンスにトランスペアレント モードでアク

ティブ/スタンバイ フェールオーバーを設定する方法を中心に取り上げています。

注：マルチコンテキストモードで稼働するユニットでは、VPNフェールオーバーはサポートされていません。VPN のフェールオーバーは、**アクティブ/スタンバイ フェールオーバー** 構成でのみ使用できます。

フェールオーバーには管理インターフェイスを使用しないことを推奨いたします。特に、ステートフル フェールオーバーの場合、一方のセキュリティ アプライアンスから他方のセキュリティ アプライアンスに常に接続情報が送信されるので、管理インターフェイスの使用は推奨されません。フェールオーバー用のインターフェイスは、通常のトラフィックを渡すインターフェイスと少なくとも同じ容量である必要があります。さらに、ASA 5540 のインターフェイスはギガビットですが、管理インターフェイスは FastEthernet のみです。管理インターフェイスは管理トラフィック専用に設計されており、management0/0として指定されています。ただし、**management-onlyコマンドを使用して任意のインターフェイスを管理専用インターフェイスに設定できます**。また、Management 0/0 については、管理専用モードを無効にして、他のインターフェイスと同じようにトラフィックを受け渡すようにすることができます。management-only コマンドの詳細は、『**Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 8.0**』を参照してください。

この設定ガイドでは、PIX/ASA 7.x のアクティブ/スタンバイ テクノロジーの概要と併せて、設定例を紹介しています。このテクノロジーの基礎になっている理論背景についての詳細は、『ASA/PIX コマンド リファレンス ガイド』を参照してください。

前提条件

要件

ハードウェア要件

フェールオーバー設定に含める 2 台のユニットは、ハードウェア構成が同じである必要があります。同じモデル、同じ数と種類のインターフェイス、さらに同じ大きさの RAM が使用されている必要があります。

注：2つのユニットは、同じサイズのフラッシュメモリを持つ必要はありません。フェールオーバー設定内でフラッシュ メモリ サイズが異なるユニットを使用する場合は、フラッシュ メモリ サイズが小さい方のユニットに、ソフトウェア イメージ ファイルおよび設定ファイルを格納するのに十分な領域があることを確認してください。十分な領域がない場合、フラッシュ メモリが大きい方のユニットから、フラッシュ メモリが小さい方のユニットへの設定の同期が失敗します。

ソフトウェア要件

フェールオーバー設定に含める 2 台のユニットは、動作モード (ルーテッドまたはトランスペアレント、シングルまたはマルチ コンテキスト) が同じである必要があります。 両方のユニットでは、メジャー (1 番目の番号) とマイナー (2 番目の番号) ソフトウェア バージョンが同じである必要がありますが、アップグレード プロセスの間は、異なるバージョンのソフトウェアを使用できます。たとえば、1 つのユニットをバージョン 7.0(1) からバージョン 7.0(2) にアップグレードしても、フェールオーバーをアクティブに保つことができます。ただし、長期的な互換性を保つため、両方のユニットを同じバージョンにアップグレードすることを推奨します。

フェールオーバー ペア上でのソフトウェアのアップグレード方法の詳細は、『Cisco セキュリティ アプライアンス コマンドライン コンフィギュレーション ガイド、バージョン 8.0』の「*ダウンタイムを発生させないフェールオーバー ペアのアップグレードの実行*」セクションを参照して

ください。

ライセンス要件

ASA セキュリティ アプライアンス プラットフォームでは、少なくとも 1 つのユニットに**無制限（UR）ライセンス**が備わっている必要があります。

注：追加の機能と利点を得るには、フェールオーバーペアのライセンスをアップグレードする必要がある場合があります。詳細は、『PIX/ASA：フェールオーバー ペアのライセンス キーのアップグレード』を参照してください。

注：フェールオーバーに参加する両方のセキュリティアプライアンスのライセンス済み機能（SSL VPNピアやセキュリティコンテキストなど）は同一である必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA セキュリティ アプライアンス バージョン 7.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- PIX セキュリティ アプライアンス バージョン 7.x 以降

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

アクティブ/スタンバイ フェールオーバー

このセクションではアクティブ/スタンバイ フェールオーバーについて説明されており、次のトピックが含まれています。

アクティブ/スタンバイ フェールオーバーの概要

アクティブ/スタンバイ フェールオーバーを利用すると、スタンバイ セキュリティ アプライアンスを使用して故障したユニットの機能を引き継ぐことができます。アクティブなユニットが故障すると、そのユニットはスタンバイ状態に変わり、スタンバイ ユニットがアクティブ状態に変わります。アクティブになったユニットは、故障したユニットの IP アドレスか、トランスペアレント ファイアウォールの場合の管理 IP アドレスと、MAC アドレスを引き継ぎ、トラフィックの受け渡しを開始します。スタンバイ状態になったユニットは、スタンバイ IP アドレスと MAC アドレスを受け継ぎます。ネットワーク デバイスで認識される MAC と IP のアドレス対応は変わらないので、ネットワークのどこにも ARP エントリの変更やタイムアウトは発生しません。

注：マルチコンテキストモードの場合、セキュリティアプライアンスはすべてのコンテキストを含むユニット全体をフェールオーバーできますが、個々のコンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリ ステータスとアクティブ/スタンバイ ステータス

フェールオーバー ペアの 2 つのユニットの間の主な違いは、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かということ、つまり、どの IP アドレスを使用し、どちらのユニットがプライマリでアクティブにトラフィックを受け渡すかということに関係します。

コンフィギュレーションでどちらのユニットがプライマリに指定されており、どちらのユニットがセカンダリに指定されているのかに基づき、ユニットの間にはいくつかの違いが存在します。

- 両方のユニットが同時に起動された場合（そして動作ヘルスが同等である場合）、常にプライマリ ユニットがアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスが常に、アクティブな IP アドレスに結び付けられます。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 リンクを通してプライマリ MAC アドレスを取得できない場合は、このルールに対する例外が発生します。この場合は、セカンダリ MAC アドレスが使用されます。

デバイスの初期化と設定の同期

フェールオーバー ペアの一方または両方のデバイスがブートすると、設定の同期が発生します。設定は、常にアクティブ ユニットからスタンバイ ユニットに同期化されます。スタンバイ ユニットでは初期起動が完了すると、アクティブ ユニットとの通信に必要なフェールオーバー コマンドを除いて実行コンフィギュレーションがクリアされ、アクティブ ユニットからユニットのコンフィギュレーション全体がスタンバイ ユニットに送信されます。

アクティブ ユニットは次のようにして決定されます。

- ユニットがブートして、ピアがすでにアクティブとして動作していることが検出されると、そのユニットはスタンバイ ユニットになります。
- ユニットがブートして、ピアが検出されない場合、そのユニットはアクティブ ユニットになります。
- 両方のユニットが同時にブートした場合は、プライマリ ユニットがアクティブ ユニットになり、セカンダリ ユニットがスタンバイ ユニットになります。

注：セカンダリユニットが起動し、プライマリユニットが検出されない場合は、アクティブユニットになります。自身の MAC アドレスをアクティブ IP アドレスとして使用します。プライマリ ユニットが使用可能になると、セカンダリ ユニットでは MAC アドレスがプライマリ ユニットの MAC アドレスに変更されるので、ネットワーク トラフィックが中断する可能性があります。この問題を回避するには、フェールオーバー ペアに仮想 MAC アドレスを設定します。詳細は、こ

のドキュメントの「ケーブル ベースのアクティブ/スタンバイ フェールオーバーの設定」セクションを参照してください。

複製が始まると、アクティブ ユニットのセキュリティ アプライアンス コンソールに「Beginning configuration replication: Sending to mateEnd Configuration Replication to mate複製の間は、アクティブ ユニットで入力したコマンドはスタンバイ ユニットに正しく複製できず、スタンバイ ユニットで入力されたコマンドは、アクティブ ユニットから複製される設定で上書きされる可能性があります。コンフィギュレーションの複製プロセスに含まれるフェールオーバー ペアのいずれのユニットでも、コマンドを入力しないでください。コンフィギュレーションのサイズにより、複製には数秒から数分かかる可能性があります。

セカンダリ ユニットでは、同期動作に応じてプライマリ ユニットからの複製メッセージを監視できます。

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

スタンバイ ユニットでは、コンフィギュレーションは実行メモリ上だけに存在しています。同期の後でコンフィギュレーションをフラッシュ メモリに保存するには、次のコマンドを入力します。

- シングル コンテキスト モードの場合は、アクティブ ユニットで **copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットでコンフィギュレーションがフラッシュ メモリに書き込まれます。
- マルチ コンテキスト モードの場合は、アクティブ ユニットで、システム実行スペースおよびディスクの各コンテキスト内から、**copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットでコンフィギュレーションがフラッシュ メモリに書き込まれます。外部サーバ上のスタートアップ コンフィギュレーションのコンテキストは、どちらのユニットからもネットワーク経由でアクセスできるので、ユニットごとに個別に保存する必要はありません。または、アクティブ ユニットからディスク上のコンテキストを外部サーバにコピーした後、そのコンテキストをスタンバイ ユニットのディスクにコピーして、ユニットをリロードするときに利用できるようにすることもできます。

コマンドの複製

コマンドの複製は、常に、アクティブ ユニットからスタンバイ ユニットに向かって行われます。コマンドがアクティブ ユニットで入力されると、フェールオーバー リンクを経由してスタンバイ ユニットに送られます。コマンドを複製するために、アクティブなコンフィギュレーションをフラッシュ メモリに保存する必要はありません。

注：スタンバイユニットで行われた変更は、アクティブユニットには複製されません。スタンバイ ユニットでコマンドを入力すると、セキュリティ アプライアンスに「**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.」というメッセージが表示されます。これでコンフィギュレーションは同期しません。このメッセージは、コンフィギュレーションに影響を与えないコマンドを入力した場合でも表示されます。

アクティブ ユニットで **write standby** コマンドを入力すると、スタンバイ ユニットでは、アクティブ ユニットとの通信に使用するフェールオーバー コマンドを除く実行コンフィギュレーションがクリアされ、アクティブ ユニットからコンフィギュレーション全体がスタンバイ ユニットに送信されます。

マルチ コンテキスト モードの場合、システム実行スペースで **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。コンテキスト内で write standby コマンドを入力した場合は、コンテキストのコンフィギュレーションのみが複製されます。

複製されたコマンドは、実行コンフィギュレーションに格納されます。複製されたコマンドをスタンバイ ユニットのフラッシュ メモリに保存するには、次のコマンドを入力します。

- シングル コンテキスト モードの場合は、アクティブ ユニットで **copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットでコンフィギュレーションがフラッシュ メモリに書き込まれます。
- マルチ コンテキスト モードの場合は、アクティブ ユニットで、システム実行スペースおよびディスクの各コンテキスト内から、**copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットでコンフィギュレーションがフラッシュ メモリに書き込まれます。外部サーバ上のスタートアップ コンフィギュレーションのコンテキストは、どちらのユニットからもネットワーク経由でアクセスできるので、ユニットごとに個別に保存する必要はありません。または、アクティブ ユニットからディスク上のコンテキストを外部サーバにコピーした後、このコンテキストをスタンバイ ユニットのディスクにコピーすることもできます。

フェールオーバー トリガ

ユニットが障害状態になる可能性があるのは、次のいずれかのイベントが発生した場合です。

- ユニットにハードウェア障害または電源障害がある。
- ユニットにソフトウェア障害がある。
- 多くの監視対象インターフェイスで障害が発生する。
- アクティブ ユニットで **no failover active** コマンドが入力される。または、スタンバイ ユニットで **failover active** コマンドが入力される。

フェールオーバー アクション

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単位で発生します。マルチ コンテキスト モードが稼働しているシステムであっても、個別のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、それぞれの障害イベントでのフェールオーバー アクションを示してあります。表では、障害イベントごとに、フェールオーバー ポリシー（フェールオーバーするかしないか）、アクティブ ユニットで実行されるアクション、スタンバイ ユニットで実行されるアクション、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が示されています。表には、フェールオーバーの動作が示されています。

障害イベント	ポリシー	アクティブ アクション	スタンバイ アクション	注意事項

アクティブ ユニットの障害（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	監視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 メッセージを受信することはありません。
以前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	アクションなし	なし
スタンバイ ユニットの障害（電源またはハードウェア）	フェールオーバーなし	スタンバイを障害としてマークする	該当なし	スタンバイ ユニットが障害としてマークされると、アクティブ ユニットでは、インターフェイス障害のしきい値を超えてもフェールオーバーが試行されません。
動作中のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー リンクがダウンしている間は、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、できる限り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。
起動時のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	アクティブになる	起動時にフェールオーバー リンクがダウンすると、両方のユニットがアクティブになります。
ステートフル フェールオー	フェー	アクションなし	アクションなし	ステート情報が古くなり、フェールオーバーが発生す

バー リンクの障害	ルオーバーなし			るとセッションが終了されます。
アクティブ ユニットでのインターフェイス障害がしきい値を超過	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
スタンバイ ユニットでのインターフェイス障害がしきい値を超過	フェールオーバーなし	アクションなし	スタンバイを障害としてマークする	スタンバイ ユニットが障害としてマークされると、アクティブ ユニットでは、インターフェイス障害のしきい値を超えてもフェールオーバーが試行されません。

標準およびステートフル フェールオーバー

セキュリティ アプライアンスでは、標準とステートフルという 2 種類のフェールオーバーがサポートされています。このセクションでは、次の項目について説明します。

- 標準フェールオーバー
- ステートフル フェールオーバー

標準フェールオーバー

フェールオーバーが発生すると、すべてのアクティブな接続が終了されます。新しいアクティブ ユニットが引き継いだ後で、クライアントでは接続を再確立する必要があります。

ステートフル フェールオーバー

ステートフル フェールオーバーが有効になっていると、アクティブ ユニットからスタンバイ ユニットに対して接続ごとのステート情報が継続的に引き渡されます。フェールオーバーが発生した後は、同じ接続情報を新しいアクティブ ユニットで使用できます。サポート対象のエンドユーザ アプリケーションでは、同じ通信セッションを維持するために接続し直す必要はありません。

スタンバイ ユニットには次のようなステート情報が渡されます。

- NAT 変換テーブル
- TCP 接続状態

- UDP 接続状態
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ファイアウォールが**トランスペアレント ファイアウォール** モードで稼動している場合に限る）
- HTTP 接続状態（HTTP 複製が有効になっている場合）
- ISAKMP および IPSec の SA テーブル
- GTP PDP 接続データベース

ステートフル フェールオーバーが有効になっていても、次の情報はスタンバイ ユニットには渡されません。

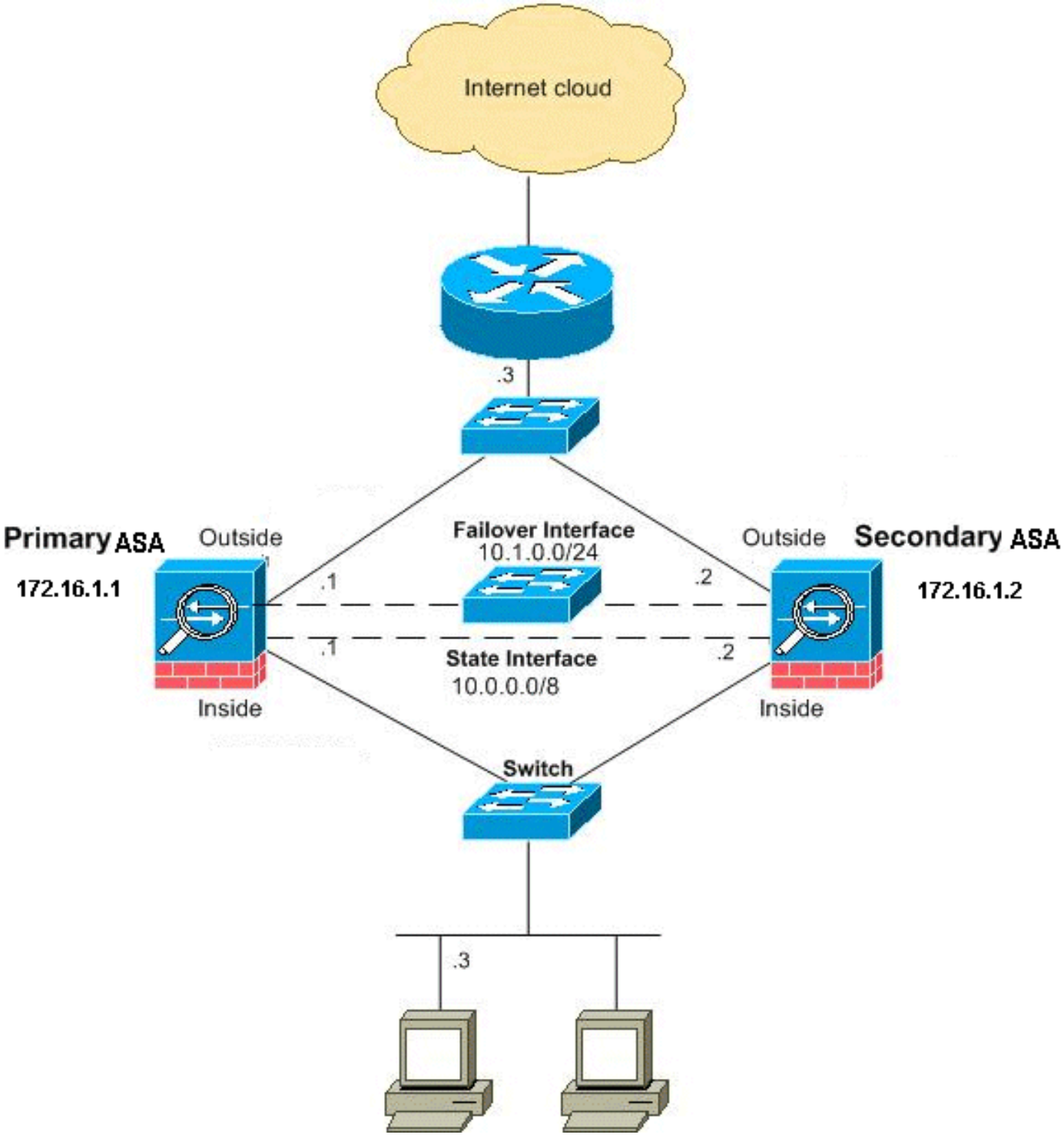
- HTTP 接続テーブル（HTTP 複製が有効になっていない場合）
- ユーザ認証（uauth）テーブル
- ルーティング テーブル
- セキュリティ サービス モジュールのステート情報

注： アクティブな Cisco IP SoftPhone セッション中にフェールオーバーが発生すると、コール セッションのステート情報がスタンバイ ユニットに複製されるため、コールはアクティブのままになります。コールが終了すると、IP SoftPhone クライアントは Cisco CallManager との接続がなくなります。これが発生する理由は、スタンバイ ユニットには CTIQBE ハングアップ メッセージに関するセッション情報がないためです。一定時間内に Cisco CallManager から応答を受信しない場合、IP SoftPhone クライアントでは、Cisco CallManager に到達できないと見なして登録解除します。

LAN ベースのアクティブ/スタンバイ フェールオーバーの設定

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



このセクションでは、イーサネット フェールオーバー リンクを使用してトランスペアレント モードでアクティブ/スタンバイ フェールオーバーを設定する方法を説明しています。LAN ベースのフェールオーバーを設定する場合は、セカンダリ デバイスがプライマリ デバイスから実行コンフィギュレーションを取得できるように、先にセカンダリ デバイスでブートストラップを実行して、フェールオーバー リンクを認識させる必要があります。

注：ケーブルベースのフェールオーバーからLANベースのフェールオーバーに変更する場合は、ケーブルベースのフェールオーバー設定で完了した、各インターフェイスのアクティブおよびスタンバイIPアドレスの割り当てなど、多くの手順をスキップできます。

プライマリ ユニットの設定

LAN ベースのアクティブ/スタンバイ フェールオーバー コンフィギュレーションでプライマリ ユ

ニットを設定するには、次の手順を実行します。この手順では、プライマリ ユニットでフェールオーバーを有効にするために必要な最低限の設定を行います。マルチ コンテキスト モードの場合、特に指示がない限り、すべての手順をシステム実行スペースで実行します。

アクティブ/スタンバイ フェールオーバー ペアのプライマリ ユニットを設定するには、次の手順を実行します。

1. まだ行っていない場合は、管理インターフェイス (トランスペアレント モード) に、アクティブとスタンバイの IP アドレスを設定します。 スタンバイ IP アドレスは、現在スタンバイ ユニットであるセキュリティ アプライアンスで使用されます。これはアクティブ IP アドレスと同じサブネットにある必要があります。**注：専用のステートフル**フェールオーバーインターフェイスを使用する場合は、ステートフルフェールオーバーリンクのIPアドレスを設定しないでください。専用ステートフル フェールオーバー インターフェイスを設定するには、後のステップで failover interface ip コマンドを使用します。
   ```
   hostname(config-if)#ip address active_addr netmask
                          standby standby_addr
   ```

   各インターフェイスに IP アドレスが必要なルーテッド モードとは異なり、透過型ファイアウォールにはデバイス全体に割り当てられた IP アドレスがあります。セキュリティ アプライアンスでは、この IP アドレスをシステム メッセージまたは AAA 通信などのセキュリティ アプライアンスから発信されるパケットの送信元アドレスとして使用します。この例では、プライマリ ASA の IP アドレスは以下のように設定されています。
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   ここでは、172.16.1.1 がプライマリ ユニットに使用され、172.16.1.2 がセカンダリ (スタンバイ) ユニットに割り当てられます。**注：マルチコンテキス**トモードでは、各コンテキスト内からインターフェイスアドレスを設定する必要があります。コンテキストを切り替えるには、changeto context コマンドを使用します。コマンド プロンプトが hostname/context(config-if)# に変わります。ここでは、context が現在のコンテキストの名前になります。
2. (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーを有効にします。
   ```
   hostname(config)#failover lan enable
   ```

3. ユニットをプライマリ ユニットとして指定します。
   ```
   hostname(config)#failover lan unit primary
   ```

4. フェールオーバー インターフェイスを定義します。フェールオーバー インターフェイスとして使用するインターフェイスを指定します。
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   このドキュメントでは、「failover」 (Ethernet0 のインターフェイス名) がフェールオーバー インターフェイスに使用されています。
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   if_name 引数により、*phy_if 引数で指定されているインターフェイスに名前が割り当てられます*。phy_if 引数には Ethernet1 のような物理ポート名を指定できますが、Ethernet0/2.3 のような事前に作成されたサブインターフェイスを指定することもできます。フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。
   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

このドキュメントでは、フェールオーバー リンクを設定するために、10.1.0.1 がアクティブ ユニットに使用され、10.1.0.2 がスタンバイ ユニットに使用され、「failover」が Ethernet0 のインターフェイス名になっています。

```
hostname(config)#failover interface ip failover 10.1.0.1
                        255.255.255.0 standby 10.1.0.2
```

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネット内にある必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。フェールオーバー リンクの IP アドレスと MAC アドレスはフェールオーバー時には変化しません。フェールオーバー リンクのアクティブ IP アドレスは常にプライマリ ユニットに存在し、スタンバイ IP アドレスはセカンダリ ユニットに存在します。インターフェイスを有効にします。

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

次の例では、Ethernet3 がフェールオーバーに使用されます。

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

5. （オプション）ステートフル フェールオーバーを有効にするには、ステートフル フェールオーバー リンクを設定します。ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。

```
hostname(config)#failover link if_name phy_if
```

次の例では、フェールオーバー リンクのステート情報を交換するための Ethernet2 のインターフェイス名として「state」を使用しています。

```
hostname(config)#failover link state Ethernet2
```

注：ステートフルフェールオーバーリンクがフェールオーバーリンクまたはデータインターフェイスを使用する場合は、if_name引数を指定する*必要があります*。**if_name 引数では、phy_if 引数で指定されているインターフェイスに論理名が割り当てられます。***phy_if引数*には、Ethernet1などの物理ポート名、またはEthernet0/2.3などの以前に作成されたサブインターフェイスを指定できます。このインターフェイスは、フェールオーバーリンクとしてオプションを除き、他の目的には使用しないでください。ステートフル フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。**注：ステートフル**フェールオーバーリンクでフェールオーバーリンクまたはデータインターフェイスが使用されている場合は、この手順をスキップしてください。インターフェイスのアクティブとスタンバイの IP アドレスはすでに定義してあります。

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

次の例では、ステートフル フェールオーバー リンクのアクティブ IP アドレスとして 10.0.0.1 が使用され、スタンバイ IP アドレスとして 10.0.0.2 が使用されています。

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                        standby 10.0.0.2
```

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネット内にある必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。データ インターフェイスを使用していない場合、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスはフェールオーバー時には変化しません。アクティブ IP アドレスは常にプラ

イマリ ユニットに存在し、スタンバイ IP アドレスはセカンダリ ユニットに存在します。インターフェイスを有効にします。**注：ステートフル**フェールオーバーリンクでフェールオーバーリンクまたはデータインターフェイスが使用されている場合は、この手順をスキップしてください。インターフェイスはすでに有効になっています。

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

注：このシナリオでは、ステートフルフェールオーバーリンクにEthernet2が使用されます。

```
hostname(config)#interface ethernet2

hostname(config-if)#no shutdown
```

6. フェールオーバーを有効にします。

```
hostname(config)#failover
```

注：プライマリ・デバイスでfailoverコマンドを最初に発行してから、セカンダリ・デバイスで発行します。セカンダリ デバイス上で failover コマンドを発行した後、セカンダリ デバイスでは即座にプライマリ デバイスからコンフィギュレーションが取得され、スタンバイとしてセカンダリ デバイス自体が設定されます。プライマリ ASA はアップしたままであり、トラフィックの受け渡しが正常に行われます。そのため、プライマリ ASA 自体がアクティブデバイスとしてマークされます。この時点以降、アクティブ デバイス上で障害が発生する場合は、常にスタンバイ デバイスがアクティブになります。

7. システム コンフィギュレーションをフラッシュ メモリに保存します。

```
hostname(config)#copy running-config startup-config
```

セカンダリ ユニットの設定

セカンダリ ユニットで必要な設定は、フェールオーバー インターフェイスについてだけです。セカンダリ ユニットでは、最初にプライマリ ユニットと通信するためにこれらのコマンドが必要です。プライマリ ユニットからコンフィギュレーションがセカンダリ ユニットに送信された後、2 つのコンフィギュレーションで永続的に異なっているのは、**failover lan unit** コマンドだけです。このコマンドにより、それぞれのユニットがプライマリまたはセカンダリとして指定されています。

マルチ コンテキスト モードの場合、特に指示がない限り、すべての手順をシステム実行スペースで実行します。

セカンダリ ユニットを設定するには、次の手順を実行します。

1. (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーを有効にします。

```
hostname(config)#failover lan enable
```

2. フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用したものと同じ設定を使用します。フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

```
hostname(config)#failover lan interface if_name phy_if
```

このドキュメントでは、Ethernet0 が LAN フェールオーバー インターフェイスに使用されています。

```
hostname(config)#failover lan interface failover Ethernet3
```

if_name 引数により、*phy_if* 引数で指定されているインターフェイスに名前が割り当てられます。フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

このドキュメントでは、フェールオーバー リンクを設定するために、10.1.0.1 がアクティブ ユニットに使用され、10.1.0.2 がスタンバイ ユニットに使用され、「failover」が Ethernet0 のインターフェイス名になっています。

```
hostname(config)#failover interface ip failover 10.1.0.1
                    255.255.255.0 standby 10.1.0.2
```

注：このコマンドは、プライマリユニットでフェールオーバーインターフェイスを設定したときにプライマリユニットで入力したコマンドとまったく同じように入力します。インターフェイスを有効にします。

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

たとえば、このシナリオでは、Ethernet0 がフェールオーバーに使用されます。

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

3. （オプション）このユニットをセカンダリ ユニットとして指定します。

```
hostname(config)#failover lan unit secondary
```

注：この手順はオプションです。これは、ユニットが事前に設定されていない限り、デフォルトでセカンダリとして指定されるためです。

4. フェールオーバーを有効にします。

```
hostname(config)#failover
```

注：フェールオーバーを有効にすると、アクティブユニットは実行メモリ内のコンフィギュレーションをスタンバイユニットに送信します。構成が同期すると、「Beginning configuration replication:*「Sending to mate」および「End Configuration Replication to mate」*というメッセージが表示されます。

5. 実行コンフィギュレーションの複製が完了した後で、コンフィギュレーションをフラッシュメモリに保存します。

```
hostname(config)#copy running-config startup-config
```

設定

このドキュメントでは、次の構成を使用します。

プライマリ ASA
ASA#**show running-config**

```
 ASA Version 7.2(3)
!
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif failover

  description LAN Failover Interface
!
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
```

```
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

セカンダリ ASA

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
```

```
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

確認

show failover コマンドの使用

このセクションでは、**show failover** コマンドの出力について説明しています。各ユニットで、**show failover** コマンドを使用してフェールオーバー ステータスを確認できます。

プライマリ ASA

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

セカンダリ ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

状態を確認するには、**show failover state** コマンドを使用します。

プライマリ ASA

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure            00:02:36 UTC Jan 1 1993

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

セカンダリ ユニット

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None
```

```
====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

フェールオーバー ユニットの IP アドレスを確認するには、**show failover interface** コマンドを使用します。

プライマリ ユニット

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
```

セカンダリ ユニット

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

監視対象インターフェイスの表示

監視対象インターフェイスのステータスを表示するには、次のようにします。シングル コンテキスト モードの場合は、グローバル設定モードで **show monitor-interface コマンドを入力します。** マルチコンテキスト モードの場合は、コンテキストに show monitor-interface を入力します。

プライマリ ASA

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

セカンダリ ASA

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

注：フェールオーバーIPアドレスを入力しない場合、show failoverコマンドでは、IPアドレスに対して0.0.0.0と表示され、インターフェイスの監視は待機状態になります。さまざまなフェールオーバー状態についての詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』の「*show failover*」セクションを参照してください。

実行コンフィギュレーションでのフェールオーバー コマンドの表示

実行設定内のフェールオーバー コマンドを表示するには、次のコマンドを入力します。

```
hostname(config)#show running-config failover
```

すべてのfailover コマンドが表示されます。マルチ コンテキスト モードで稼働するユニットでは、システム実行スペースで **show running-config failover** コマンドを入力します。デフォルト値を変更していないコマンドを含めて、実行コンフィギュレーションでのフェールオーバー コマンドを表示するには、**show running-config all failover** コマンドを入力します。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

1. アクティブ ユニットやフェールオーバー グループが、別々のインターフェイス上でホスト間でファイルを送信するために FTP などで期待どおりにトラフィックを通過させていることをテストします。
2. 次のコマンドを使用して、強制的にスタンバイ ユニットにフェールオーバーさせます。アクティブ/スタンバイ フェールオーバーの場合は、アクティブ ユニットで次のコマンドを入力します。
   ```
   hostname(config)#no failover active
   ```
3. FTP を使用して、同じ 2 つのホスト間で別のファイルを送信します。
4. テストが失敗した場合は、**show failover command** を入力してフェールオーバーのステータスを調べます。
5. 終了したら、次のコマンドを使用してユニットまたはフェールオーバー グループをアクティブ ステータスに戻すことができます。アクティブ/スタンバイ フェールオーバーの場合は、アクティブ ユニットで次のコマンドを入力します。
   ```
   hostname(config)#failover active
   ```

強制フェールオーバー

強制的にスタンバイ ユニットをアクティブにするには、次のいずれかのコマンドを入力します。

スタンバイ ユニットで次のコマンドを入力します。

```
hostname#failover active
```

アクティブ ユニットで次のコマンドを入力します。

```
hostname#no failover active
```

フェールオーバーの無効化

フェールオーバーをディセーブルにするには、次のコマンドを入力します。

```
hostname(config)#no failover
```

アクティブ/スタンバイ ペアでフェールオーバーを無効にすると、再起動するまで各ユニットのアクティブとスタンバイのステートが保持されます。たとえば、スタンバイ ユニットはスタンバイ モードのままなので、どちらのユニットでもトラフィックの受け渡しが開始されません。スタンバイ ユニットをアクティブにする（フェールオーバーが無効にされている場合でも）には、「強制フェールオーバー」セクションを参照してください。

アクティブ/アクティブ ペアでフェールオーバーを無効にすると、どのユニットが優先に設定されているかに関係なく、フェールオーバー グループは現在アクティブになっているユニットでアクティブ状態のままになります。システム実行スペースで no failover コマンドを入力できます。

障害ユニットの復元

故障したユニットの障害状態を解除するには、次のコマンドを入力します。

```
hostname(config)#failover reset
```

障害状態のユニットを障害解除状態に復元した場合、ユニットは自動的にはアクティブになりません。（強制的または通常の）フェールオーバーによってアクティブにされるまで、復元されたユニットまたはグループはスタンバイ状態のままになります。 ただし、preempt コマンドを使用して設定されているフェールオーバー グループは例外です。以前アクティブであり、フェールオーバー グループが preempt コマンドを使用して設定されていて、障害が発生したユニットが優先ユニットである場合、そのフェールオーバー グループはアクティブになります。

トラブルシュート

フェールオーバーが発生すると、両方のセキュリティ アプライアンスからシステム メッセージが送信されます。このセクションでは、次の項目について説明しています。

- フェールオーバー監視
- ユニット障害
- %ASA-3-210005：LU 割り当て接続の失敗
- フェールオーバーのシステム メッセージ
- デバッグ メッセージ
- SNMP
- 既知の問題

フェールオーバー監視

次の例では、フェールオーバーによりネットワーク インターフェイスの監視が開始されなかった場合の動作を説明しています。フェールオーバーが発生しても、ネットワーク インターフェイス

で他方のユニットからの 2 番目の hello パケットが受信されるまでは、そのインターフェイスの監視が開始されません。これには約 30 秒かかります。スパニング ツリー プロトコル（STP）が稼動するネットワーク スイッチにユニットが接続されている場合は、スイッチで設定されている forward delay 時間（通常は 15 秒に設定）の 2 倍に、この 30 秒の遅延を加えた時間がかかります。これは、ASA のブートアップ時およびフェールオーバー イベントの直後に、ネットワーク スイッチで一時的なブリッジ ループが検出されるためです。このループが検出されると、forward delay 時間だけ、これらのインターフェイスでのパケットの転送が停止されます。その後、スイッチはさらに forward delay 時間だけ listen モードに入り、この間はブリッジ ループのリッスンが行われ、トラフィックの転送は行われません（つまり、フェールオーバーの hello パケットは転送されません）。転送遅延時間 2 回分（30 秒）の後、トラフィック フローが再開されます。各 ASA は、他方のユニットから 30 秒に相当する hello パケットを受信するまで、waiting モードに留まります。ASA では、トラフィックを渡している間は、hello パケットを受信しないことを理由に他のユニットを障害扱いにすることはありません。他のすべてのフェールオーバー、つまり、電源、インターフェイスのリンク喪失、およびフェールオーバー ケーブルの hello の監視は引き続き行われます。

フェールオーバーに関しては、ASA インターフェイスに接続するすべてのスイッチ ポートで PortFast をイネーブルにすることを強く推奨いたします。さらに、これらのポートではチャネリングとトランキングを無効にする必要があります。ASA のインターフェイスがフェールオーバーの間にダウンした場合、スイッチでは、ポートの状態が listening から learning を経て forwarding に移行するまでの間、30 秒間待つ必要はありません。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

まとめると、フェールオーバーの問題を絞り込むには次の手順を確認します。

- 「待機」/「障害」状況のインターフェイスに接続されているネットワーク ケーブルを調べて、可能であれば交換します。
- 2 つのユニットの間に接続されているスイッチがある場合は、「待機」/「障害」状態のインターフェイスに接続されているネットワークが正常に機能していることを確認します。
- 「待機」/「障害」状況のインターフェイスに接続されているスイッチ ポートを調べて、可能であれば、そのスイッチの別の FE ポートを使用します。
- インターフェイスに接続されているスイッチ ポートで、PortFast を有効にしてあり、トランキングとチャネリングを無効にしてあることを確認します。

ユニット障害

この例では、フェールオーバーによって障害が検出されています。プライマリ ユニットの インターフェイス 1 が障害の原因であることに注意してください。ユニットは、障害のために waiting モードに戻っています。故障したユニットでは、ネットワークから自分自身が削除され（インターフェイスがダウン）、ネットワークには hello パケットが送信されなくなります。アクティブ ユニットは、故障したユニットの交換後にフェールオーバー通信が再開されるまで、waiting 状態

に留まります。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

LU 割り当て接続の失敗

次のエラー メッセージが表示される場合、メモリの問題が存在する可能性があります。

```
LU
```

この問題はシスコ バグ ID CSCte80027 (登録ユーザのみ) に記述されています。 この問題を解決するには、この不具合が修正されているソフトウェア バージョンにファイアウォールをアップグレードします。この不具合が修正されている ASA ソフトウェア バージョンは、8.2(4)、8.3(2)、8.4(2) などです。

フェールオーバーのシステム メッセージ

セキュリティ アプライアンスでは、フェールオーバーに関連する多数のシステム メッセージが優先レベル 2 で発行され、これは重大な状態を示しています。これらのメッセージを表示するには『Cisco セキュリティ アプライアンスのロギング設定とシステム ログ メッセージ』を参照して、ロギングを有効にし、システム メッセージの説明を参照してください。

注：スイッチオーバー内では、フェールオーバーによってインターフェイスが論理的にシャットダウンされ、syslog 411001および411002メッセージが**生成さ**れます。これは正常な動作です。

デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス』を参照してください。

注：デバッグ出力はCPUプロセスで高い優先順位が割り当てられるため、システムのパフォーマンスに大きく影響する可能性があります。このため、**debug fover** コマンドの使用は、特定の問題のトラブルシューティングまたは Cisco テクニカルサポート要員とのトラブルシューティング セッション中だけにしてください。

SNMP

フェールオーバーに対する SNMP syslog トラップを受け取るには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義して、Cisco syslog MIB を SNMP 管理ステーションにコンパイルします。詳細は、『**Cisco セキュリティ アプライアンス コマンド リファレンス**』で **snmp-server** コマンドと logging コマンドを参照してください。

フェールオーバー ポーリング時間

フェールオーバー ユニットのポーリング時間とホールド時間を指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。

failover polltime unit msec [time] は、スタンバイ ユニットの存在を調べる時間間隔を表すために hello メッセージをポーリングします。

同様に、failover holdtime unit msec [time] は、ユニットがフェールオーバー リンクで hello メッセージを受信する必要のある時間間隔の設定を表します。この時間が経過すると、ピア ユニットは障害として宣言されます。

アクティブ/スタンバイ フェールオーバー設定でデータ インターフェイス ポーリング時間とデータ インターフェイス ホールド時間を指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトのポーリング時間とホールド時間を復元するには、このコマンドの **no** 形式を使用します。

failover polltime interface [msec] *time* **[holdtime** *time***]**

データ インターフェイス上で hello パケットが送信される頻度を変更するには、**failover polltime interface** コマンドを使用します。このコマンドは、アクティブ/スタンバイ フェールオーバーでのみ使用できます。アクティブ/アクティブ フェールオーバーの場合は、**failover polltime interface** コマンドではなく、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。

インターフェイス ポーリング時間の 5 倍未満の **holdtime 値は入力できません。**より高速なポーリング時間の場合は、セキュリティ アプライアンスではより高速に障害を検出し、フェールオーバーをトリガーすることが可能です。ただし、ネットワークが一時的に輻輳している場合、より高速な検出によって不要な切り替えが発生する可能性があります。ホールド時間の半分を超えてもインターフェイスで hello パケットが受信されない場合、インターフェイス テストが開始されます。

コンフィギュレーションには、failover polltime unit コマンドと failover polltime interface コマンドのどちらも含めることができます。

次の例では、インターフェイス ポーリング時間の頻度は 500 ミリ秒、ホールド時間は 5 秒に設定されています。

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』の「failover polltime」のセクションを参照してください。

フェールオーバー設定での証明書/秘密鍵のエクスポート

プライマリ デバイスによって秘密キー/証明書がセカンダリ ユニットへ自動的に複製されます。証明書および秘密鍵を含むコンフィギュレーションをスタンバイ ユニットに複製するには、アクティブ ユニットでコマンド **write memory** を発行します。スタンバイ ユニット上のすべての鍵および証明書は消去され、アクティブ ユニットのコンフィギュレーションによって再入力されます

。

注：アクティブデバイスから証明書、キー、およびトラストポイントを手動でインポートし、スタンバイデバイスにエクスポートしないでください。

警告：フェールオーバー メッセージの複合化に失敗しました。

エラー メッセージ：

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

この問題はフェールオーバーのキー設定が原因で発生します。この問題を解決するには、フェールオーバー キーを削除し、新規の共有キーを設定します。

問題：トランスペアレントActive/Standbyマルチモードフェールオーバーを設定した後、フェールオーバーは常にフラッピングします

両方のASAの内部インターフェイスが直接接続され、両方のASAの外部インターフェイスが直接接続されている場合、フェールオーバーは安定しています。ただし、スイッチが間で使用されると、フェールオーバーがフラッピングします。

ソリューション：この問題を解決するには、ASAインターフェイスでBPDUを無効にします。

ASA モジュール フェールオーバー

Advanced Inspection and Prevention Security Services Module（AIP-SSM）または Content Security and Control Security Services Module（CSC-SSM）がアクティブ ユニットとスタンバイ ユニットで使用されている場合、フェールオーバーに関しては ASA と無関係に動作します。**モジュールはアクティブ ユニットとスタンバイ ユニットに手動で設定される必要があり、フェールオーバーによってモジュールのコンフィギュレーションが複製されることはありません。**

フェールオーバーについては、AIP-SSM モジュールまたは CSC-SSM モジュールを備えたどちらの ASA ユニットも、同じハードウェア タイプである必要があります。たとえば、プライマリ ユニットに ASA-SSM-10 モジュールが含まれている場合、セカンダリ ユニットにも ASA-SSM-10 モジュール含まれている必要があります。

フェールオーバー メッセージのブロック割り当ての失敗

エラー メッセージ `%PIX|ASA-3-105010: (Primary) Failover message block alloc failed`

説明：ブロック メモリが削除されました。これは一時的なメッセージであり、セキュリティ アプライアンスは復旧します。*セカンダリ ユニットが問題であれば*、「*Primary*」の箇所は「*Secondary*」と表示されます。

推奨処置：現在のブロック メモリを監視するために、**show blocks** コマンドを使用します。

AIP モジュール フェールオーバーの問題

フェールオーバーが設定されている 2 台の ASA があり、それぞれが AIP-SSM を備えている場合

は、AIP-SSM の設定を手動で複製する必要があります。フェールオーバー メカニズムによって複製されるのは、ASA の設定だけです。AIP-SSM はフェールオーバーに含まれません。

まず、フェールオーバーについては、AIP-SSM は ASA とは無関係に動作します。フェールオーバーに関して、ASA の観点から必要なことは、AIP モジュールが同じハードウェア タイプであることだけです。その他には、フェールオーバーの他の部分と同様に、アクティブとスタンバイの間での ASA のコンフィギュレーションが同期している必要があります。

AIP のセットアップについて言えば、AIP は事実上独立したセンサーです。これら 2 つの間ではフェールオーバーは存在せず、相互に認識していません。コードのバージョンとは無関係に実行することが可能です。つまり、バージョンは一致している必要がなく、ASA では、フェールオーバーに関して、AIP 上でのコードのバージョンを問いません。

AIP 上で設定した管理インターフェイス IP を介して、ASDM により AIP への接続が開始されます。つまり、通常は HTTPS を介してセンサーに接続します。接続は、センサーのセットアップ方法に依存します。

IPS（AIP）モジュールとは無関係に ASA のフェールオーバーが発生する可能性があります。接続先は管理 IP であるため、引き続き同じ AIP に接続されています。他方の AIP に接続するには、その管理 IP に再接続して設定およびアクセスを行う必要があります。

「ASA：ASA から AIP SSM へのネットワーク トラフィックの送信の設定例』を参照してください。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）を介して Advanced Inspection and Prevention Security Services Module（AIP-SSM）（IPS）にネットワーク トラフィックを送信する方法の詳細および設定例が示されています。

既知の問題

バージョン 8.x のソフトウェアとバージョン 6.x の ASDM をフェールオーバー コンフィギュレーションに使用しているときに、セカンダリ ASA で ASDM にアクセスしようとした場合、次のエラーが表示されます。

```
:The name on the security certificate is invalid or does not match the name of the site
```

証明書では、発行者とサブジェクト名は、アクティブ ユニットの IP アドレスになります。スタンバイ ユニットの IP アドレスではありません。

ASA バージョン 8.x では、内部（ASDM）証明書はアクティブ ユニットからスタンバイ ユニットに複製されます。その結果、このようなエラー メッセージが表示されます。ただし、バージョン 7.x のコードを実行する 5.x の ASDM 上で同じファイアウォールが動作している場合、ASDM にアクセスしようとすると次の通常のセキュリティ警告が表示されます。

```
The security certificate has a valid name matching the name of the page you are trying to view
```

証明書を確認すると、発行者とサブジェクト名がスタンバイ ユニットの IP アドレスになっています。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco PIX Firewall ソフトウェア
- Firewall Services Module（FWSM; ファイアウォール サービス モジュール）フェールオーバ

一設定

- FWSM フェールオーバー トラブルシューティング
- Cisco Secure PIX ファイヤウォール でのフェールオーバーの仕組み
- テクニカル サポートとドキュメント – Cisco Systems