ASA/PIX：トランスペアレント モードでのアクティブ/アクティブ 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でトランスペアレントモードのアクティブ/アクティブフェールオーバーを設定する方法を中心に説明します。

注：マルチコンテク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、ASA/PIX 7.xアクティブ/スタンバイテクノロジーの概要を示す設定例を紹介します。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/アクティブ 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/アクティブ フェールオーバーの概要
- 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
- デバイスの初期化と設定の同期
- コマンドの複製
- フェールオーバー トリガ
- フェールオーバー アクション

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバーを利用できるのは、マルチ コンテキスト モードのセキュリティ アプライアンスだけです。アクティブ/アクティブ フェールオーバーでは、どちらのセキュリティ アプライアンスでもネットワーク トラフィックを通過させられます。

アクティブ/アクティブ フェールオーバーでは、セキュリティ アプライアンス上のセキュリティ コンテキストをフェールオーバー グループに分割します。フェールオーバー グループとは、端的には 1 つ以上のセキュリティ コンテキストの論理グループです。セキュリティ アプライアンス

にはフェールオーバー グループを 2 つまで作成できます。管理コンテキストは常にフェールオーバー グループ 1 のメンバになります。デフォルトでは、未割り当てのセキュリティ コンテキストもすべてフェールオーバー グループ 1 のメンバになります。

アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループがフェールオーバーの基本単位となります。インターフェイス障害モニタリング、フェールオーバー、およびアクティブ/スタンバイ ステータスは、すべてユニットではなくフェールオーバー グループの属性です。アクティブ側のフェールオーバー グループに障害が発生するとスタンバイ ステータスに変わり、一方で、スタンバイ側のフェールオーバー グループがアクティブになります。アクティブになるフェールオーバー グループのインターフェイスでは、障害が発生したフェールオーバー グループのインターフェイスの MAC アドレスと IP アドレスが引き継がれます。ここでスタンバイ ステートになったフェールオーバー グループのインターフェイスでは、スタンバイ側の MAC アドレスと IP アドレスが引き継がれます。

注：ユニットでフェールオーバーグループに障害が発生しても、ユニットに障害が発生したわけではありません。ユニットには、トラフィックを通過させる別のフェールオーバーグループを引き続き設定できます。

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

アクティブ/スタンバイ フェールオーバーにおけるように、アクティブ/アクティブ フェールオーバー ペアの一方のユニットがプライマリ ユニットになり、他方のユニットがセカンダリ ユニットになります。アクティブ/スタンバイ フェールオーバーとは異なり、この割り当ては、両方のユニットが同時に起動した場合にどちらのユニットがアクティブになるかということを示しているわけではありません。この場合、プライマリ/セカンダリの割り当てでは、次の 2 つの操作が行われます。

- 両方のユニットが同時に起動した際に、ペアに対してどちらのユニットが実行コンフィギュレーションを提供するかを判定する。
- 両方のユニットが同時に起動した際に、どのユニットで各フェールオーバー グループがアクティブ ステートとなるかを判定する。構成内の各フェールオーバー グループがプライマリかセカンダリのユニット プリファレンスに設定される。ペアの1つのユニットで両方のフェールオーバーグループをアクティブ状態に設定し、もう1つのユニットでスタンバイステートのフェールオーバーグループを含めることができます。ただし、より一般的な設定では、各フェールオーバーグループに異なるロール優先度を割り当てて、各フェールオーバーグループを異なるユニットでアクティブにし、デバイスにトラフィックを分散します。**注：セキュリティアプライアンスでは、負荷分散**サービスは提供されません。ロード バランシングは、セキュリティ アプライアンスにトラフィックを受け渡すルータで処理される必要があります。

どのユニットで各フェールオーバー グループがアクティブになるかは、次のように判定されます。

- ユニットが起動した際にピア ユニットが利用できない場合、そのユニットでは両方のフェールオーバー グループがアクティブになります。
- ピアユニットがアクティブ（両方のフェールオーバーグループがアクティブ状態）のときにユニットが起動すると、フェールオーバーグループのプライマリまたはセカンダリの設定に関係なく、アクティブユニットでフェールオーバーグループがアクティブ状態のままになります。フェールオーバーが発生する。**no failover active** コマンドにより、手動でフェールオーバー グループを他方のユニットに強制的に割り当てる。**preempt** コマンドでフェールオーバー グループを設定しており、優先ユニットでは、ユニットが利用可能になった時点で、そのフェールオーバー グループが自動的にアクティブになる。

- 両方のユニットが同時に起動する際に、設定の同期が行われた後で、優先ユニットで各フェールオーバー グループがアクティブになります。

デバイスの初期化と設定の同期

フェールオーバー ペアの一方あるいは両方のユニットが起動した際に、設定の同期が行われます。設定の同期は次のように行われます。

- ユニットが起動した際にピア ユニットがアクティブの場合（ユニットで両方のフェールオーバー グループがアクティブ）、プライマリかセカンダリかにかかわらず、起動ユニットからアクティブ ユニットにコンタクトして実行コンフィギュレーションが取得されます。
- 両方のユニットが同時に起動すると、セカンダリ ユニットでは、プライマリ ユニットから実行コンフィギュレーションが取得されます。

レプリケーションが開始されると、設定を送信する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 mate」というメッセージが表示され、完了すると「End Configuration Replication to mate 複製中、設定を送信するユニットで入力されたコマンドはピアユニットに正しく複製できず、設定を受信するユニットで入力されたコマンドは、受信した設定で上書きされる可能性があります。設定の複製プロセスでは、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実行しないでください。レプリケーションは、構成のサイズによって異なりますが、数秒から数分かかることがあります。

コンフィギュレーションを受信するユニットでは、コンフィギュレーションは実行メモリにのみ存在します。同期後に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、アクティブステートのフェールオーバーグループ1があるユニットのシステム実行スペースで**write memory all**コマンドを入力します。このコマンドはピア ユニットに複製され、そこでコンフィギュレーションのフラッシュ メモリへの書き出しが実行されます。このコマンドで**all**キーワードを使用すると、システムとすべてのコンテキストコンフィギュレーションが保存されます。

注：外部サーバに保存されたスタートアップコンフィギュレーションは、ネットワーク上のいずれかのユニットからアクセス可能で、ユニットごとに個別に保存する必要はありません。代替策として、コンテキスト コンフィギュレーション ファイルをプライマリ ユニットのディスクから外部サーバにコピーしておいてから、セカンダリ ユニットのディスクにコピーすることができます。ユニットをリロードすると、コピーしたコンテキスト コンフィギュレーション ファイルを使用できるようになります。

コマンドの複製

両方のユニットが稼働すると、次のように、一方のユニットから他方のユニットにコマンドが複製されます。

- セキュリティ コンテキストに入力されたコマンドは、セキュリティ コンテキストがアクティブ ステートになっているユニットからピア ユニットに複製されます。**注：** ユニット上で所属するフェールオーバー グループがアクティブ ステートになっている場合、そのユニットのコンテキストがアクティブ ステートであると見なされます。
- システム実行スペースで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートになっているユニットから、フェールオーバー グループ 1 がスタンバイ ステートになっているユニットに複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートになっているユニットから、フェールオーバー グループ 1 がスタンバイ ステートになっているユニットに複製されます。

すべての設定コマンドとファイルコマンド(copy、rename、delete、mkdir、rmdirなど)は、次の例外を除いて複製されます。show、debug、mode、firewall、failover lan unit コマンドは複製されません。

コマンド複製のための適切なユニットでのコマンドの入力に失敗すると、設定の同期が崩れます。これらの変更は、次回の初期設定の同期で失われる可能性があります。

同期が崩れた設定を再度同期させるには、write standby コマンドを使用できます。アクティブ/ライトのstandbyActiveフェイルオーバーの場合、write standbyコマンドは次のように動作します。

- システム実行スペースで write standby コマンドを入力すると、セキュリティ アプライアンス上のシステム設定とセキュリティ コンテキストのすべての設定がピア ユニットに書き出されます。これには、スタンバイ ステートになっているセキュリティ コンテキストの設定情報が含まれています。アクティブ ステートのフェールオーバー グループ 1 があるユニットのシステム実行スペースで、コマンドを入力する必要があります。注：ピアユニット上でアクティブ状態のセキュリティコンテキストがある場合、write standbyコマンドを使用すると、それらのコンテキストを介したアクティブな接続が終了します。write standbyコマンドを入力する前に、コンフィギュレーションを提供するユニットでfailover activeコマンドを使用して、そのユニットですべてのコンテキストがアクティブであることを確認します。
- あるセキュリティ コンテキストで write standby コマンドを入力すると、そのセキュリティ コンテキストの設定だけがピア ユニットに書き出されます。セキュリティ コンテキストがアクティブ ステートになっているユニットのセキュリティ コンテキストで、コマンドを入力する必要があります。

ピア ユニットへの複製時には、複製されたコマンドはフラッシュ メモリには保存されません。複製されたコマンドは実行コンフィギュレーションに追加されます。両方のユニットで複製されたコマンドをフラッシュ メモリに保存するためには、変更したユニットで write memory コマンドか copy running-config startup-config コマンドを使用します。このコマンドはピア ユニットに複製され、ピア ユニット上のフラッシュ メモリへのコンフィギュレーションの書き出しが実行されます。

フェールオーバー トリガ

アクティブ/アクティブフェールオーバーでは、次のいずれかのイベントが発生すると、ユニット レベルでフェールオーバーをトリガーできます。

- ユニットにハードウェア障害がある。
- ユニットに電源障害がある。
- ユニットにソフトウェア障害がある。
- no failover active コマンドか failover active コマンドがシステム実行スペースで入力された。

次のイベントのいずれかが発生すると、フェールオーバー グループ レベルでフェールオーバーがトリガーされます。

- グループ内で障害が発生したモニタリング対象のインターフェイスが多すぎる。
- no failover active group group_id コマンドか failover active group group_id コマンドが入力された。

フェールオーバー アクション

アクティブ/アクティブ フェールオーバー構成では、フェールオーバーはシステム ベースではな

くフェールオーバー グループ ベースで発生します。たとえば、プライマリ ユニットで両方のフェールオーバー グループをアクティブに割り当てている場合、フェールオーバー グループ 1 で障害が発生すると、プライマリ ユニットではフェールオーバー グループ 2 がアクティブのまま残り、セカンダリ ユニットではフェールオーバー グループ 1 がアクティブになります。

注：アクティブ/アクティブフェールオーバーを設定する場合は、両方のユニットのトラフィックの合計が各ユニットのキャパシティ内にあることを確認してください。

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。障害イベントごとに、ポリシー、フェールオーバーの発生の有無、アクティブフェールオーバーグループのアクション、スタンバイフェールオーバーグループのアクションが示されます。

障害イベント	**ポリシー**	**アクティブ グループ アクション**	**スタンバイ グループ アクション**	**注意事項**
ユニットでの電源障害またはソフトウェア障害	フェールオーバー	スタンバイに移行。障害発生とマーキング。	スタンバイに移行。アクティブを障害としてマークする	フェールオーバー ペア内の一方のユニットに障害が発生すると、そのユニットではアクティブ フェールオーバー グループがすべて障害発生とマーキングされ、ペア ユニットではアクティブになります。
アクティブ フェールオーバー グループでの基準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 グループに障害発生とマーキング。	アクティブになる	なし
スタンバイ フェールオーバー グループでの基準を超えたインターフェイス障害	フェールオーバーなし	アクションなし	スタンバイ グループに障害発生とマーキング。	スタンバイ フェールオーバー グループが障害発生とマーキングされていると、インターフェイスの障害の基準を超えていても、アクティブ フェールオーバー グループではフェールオーバーが試行されません。
以前のアクティブ フェールオーバー	フェール	アクションなし	アクションなし	preempt コマンドで設定されていない限り、現在のユニットでのフェールオーバ

グループの復旧	オーバーなし			ー グループがアクティブのままで残ります。
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	アクティブになる	アクティブになる	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、両方のユニットのフェールオーバー グループがアクティブになります。
ステートフル フェールオーバーリンクの障害	フェールオーバーなし	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るとセッションが終了されます。
運用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	該当なし	該当なし	各ユニットでフェールオーバー インターフェイスが障害発生とマーキングされます。フェールオーバー リンクがダウンしている間は、ユニットではスタンバイ ユニットにフェールオーバーできないため、できるだけ早急にフェールオーバー リンクを復元する必要があります。

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 ユニットが引き継ぐ際に、クライアントで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（透過ファイアウォール モードで稼働している場合）
- 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 クライアントでは CallManager との接続が失われます。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。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。

フェールオーバー設定の制限項目

次のタイプの IP アドレスではフェールオーバーを設定できません。

- DHCP で取得される IP アドレス
- PPPoE で取得される IP アドレス
- IPv6 形式のアドレス

さらに、次の制約があります。

- ASA 5505 適応型セキュリティ アプライアンスではステートフル フェールオーバーはサポートされていません。
- ASA 5505 適応型セキュリティ アプライアンスではアクティブ/アクティブ フェールオーバーはサポートされていません。
- ASA 5505 適応型セキュリティ アプライアンスで Easy VPN リモートが有効になっていると

、フェールオーバーを設定できません。
- マルチ コンテキスト モードでは、VPN のフェールオーバーはサポートされていません。

サポートされていない機能

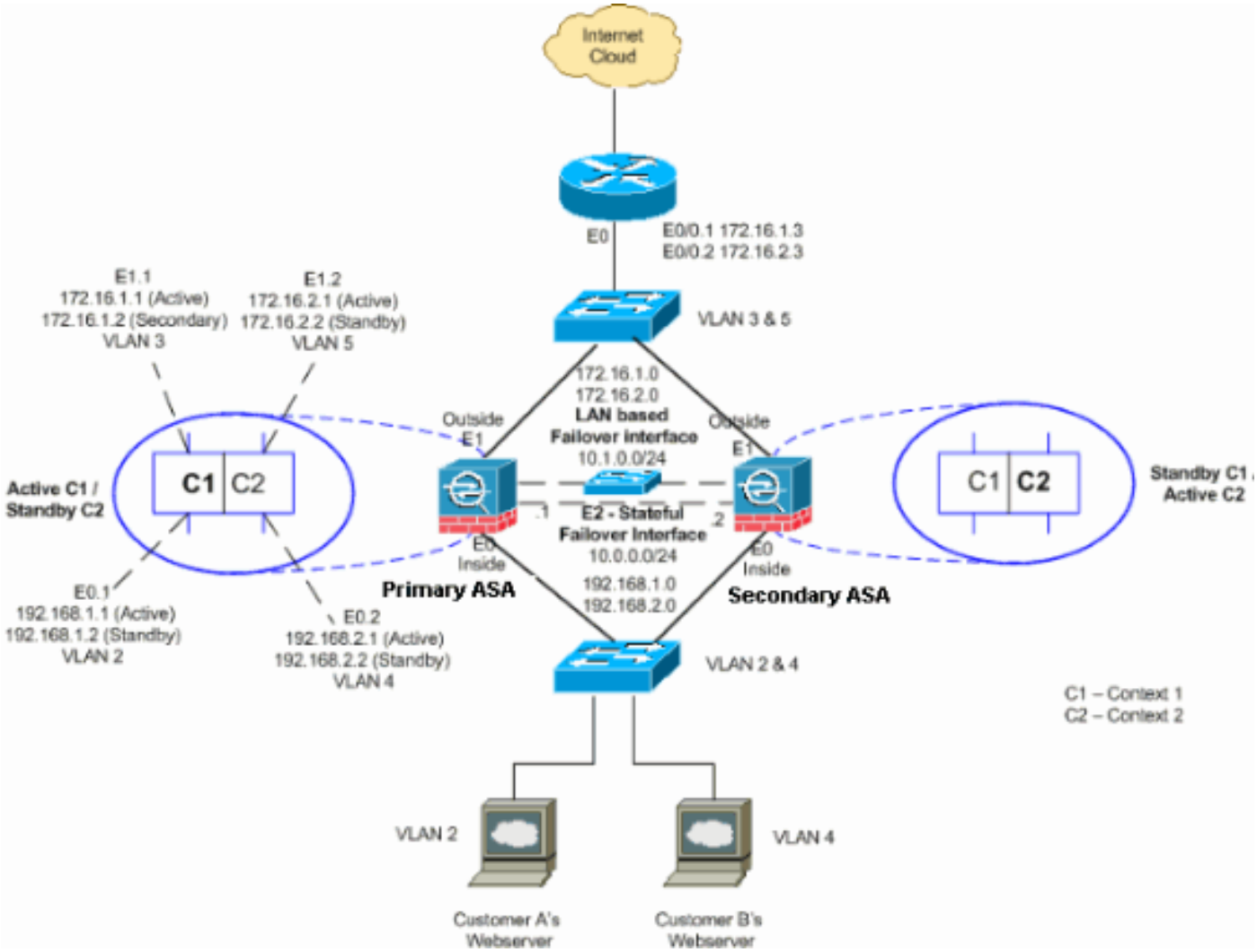
マルチ コンテキスト モードでは、次の機能はサポートされていません。

- ダイナミック ルーティング プロトコルセキュリティ コンテキストでサポートされているのはスタティック ルートだけです。マルチ コンテキスト モードでは OSPF や RIP を有効にできません。
- VPN
- マルチキャスト

LAN ベースでのアクティブ/アクティブ 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アクティブ/アクティブフェールオーバーを設定する方法について説明します。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：ユニットを直接リンクするためにクロスイーサネットケーブルを使用する代わりに、プライマリユニットとセカンダリユニットの間で専用スイッチを使用することを推奨します。

このセクションでは、次の項目について説明しています。

プライマリ ユニットの設定

次の手順を実行して、アクティブ/アクティブ フェールオーバー構成でのプライマリ ユニットを設定します。

1. まだ設定していない場合は、アクティブ側とスタンバイ側の IP アドレスを、各データ インターフェイス (ルーテッド モード) 用、管理 IP アドレス (トランスペアレント モード) 用、あるいは管理専用インターフェイス用に設定します。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。インターフェイス アドレスは、各コンテキスト内で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。トランスペアレント ファイアウォール モードで、各コンテキストの管理 IP アドレスを入力する必要があります。**注：専用のステートフ**ェイ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。**failover interface ip**コマンドを使用して、後の手順で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します。
   ```
   hostname/context(config-if)#ip address active_addr netmask standby standby_addr
   ```

   この例では、プライマリASAのcontext1の外部インターフェイスは次のように設定されています。
   ```
   ASA/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
   ```

   context2 については、次のようになります。
   ```
   ASA/context2(config)#ip address 192.168.2.1 255.255.255.0
                                    standby 192.168.2.2
   ```

   ルーテッド ファイアウォール モードでは、管理専用インターフェイスに関して、このコマンドは各インターフェイスに対してインターフェイス コンフィギュレーション モードで入力されます。トランスペアレント ファイアウォール モードでは、このコマンドはグローバル コンフィギュレーション モードで入力されます。
2. システム実行スペースで基本的なフェールオーバー パラメータを設定します。(PIX セキュリティ アプライアンスのみ) 次のように、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
   ```

   次のように、ユニットをプライマリ ユニットに割り当てます。

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

次のように、フェールオーバー リンクを指定します。

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

この例では、インターフェイス ethernet 3 を LAN ベースのフェールオーバー インターフェイスに使用しています。

```
ASA(config)#failover lan interface LANFailover ethernet3
```

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。ASA 5505適応型セキュリティアプライアンスでは、phy_ifはVLANを指定します。このインターフェイスは、（オプションでのステートフル フェールオーバー リンクを除いて）他の目的に使用することはできません。次のように、フェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定します。

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

この例では、フェールオーバー インターフェイスのアクティブ IP アドレスに 10.1.0.1 を使用し、スタンバイ IP アドレスに 10.1.0.2 を使用しています。

```
ASA(config)#failover interface ip LANFailover
      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 IP アドレスのサブネット マスクの識別は不要です。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。

セカンダリ ユニットの設定

LANベースのアクティブ/アクティブフェールオーバーを設定するときは、フェールオーバーリンクを認識するためにセカンダリユニットをブートストラップする必要があります。これにより、セカンダリ ユニットはプライマリ ユニットと通信して、プライマリ ユニットから実行コンフィギュレーションを受信できます。

次の手順を実行して、アクティブ/アクティブ フェールオーバー構成でのセカンダリ ユニットを起動します。

1. （PIX セキュリティ アプライアンスのみ）次のように、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。次のように、プライマリ ユニットに使用した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
   ```

   ```
   ASA(config)#failover lan interface LANFailover ethernet3
   ```

   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。ASA 5505適応型セキュリティアプライアンスでは、phy_ifはVLANを指定します。次のように、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
```

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

注：このコマンドは、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。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。インターフェイスを有効にします。

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

3. 次のように、このユニットをセカンダリ ユニットに割り当てます。

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

注：この手順はオプションです。これは、以前に設定されていない限り、デフォルトではユニットが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
```

フェールオーバーを有効にすると、アクティブ ユニットでは実行メモリ内の設定がスタンバイ ユニットに送信されます。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。**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。

5. 実行コンフィギュレーションの複製が完了したら、次のコマンドを入力して、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
```

6. 必要な場合は、プライマリ側でアクティブなフェールオーバー グループをすべて、セカンダリ ユニットで強制的にアクティブ ステートにします。セカンダリ ユニットでフェールオーバー グループを強制的にアクティブにするには、プライマリ ユニットのシステム実行スペースで次のコマンドを入力します。

```
hostname#no failover active group group_id
```

group_id 引数には、セカンダリ ユニットでアクティブにするグループを指定します。

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:Context1の設定

```
ASA/context1(config)#show running-config
: Saved
:
ASA Version 7.2(3)




!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

プライマリASA:Context2の設定

```
ASA/context2(config)#show running-config
: Saved
:
ASA Version 7.2(3)




!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context2. ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
```

```
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

プライマリ ASA

```
ASA(config)#show running-config
: Saved
:
ASA Version 7.2(3) <system>
!
 !--- Use the firewall transparent command !--- in
global configuration mode in order to !--- set the
firewall mode to transparent mode.

firewall transparent
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
```

```
!
interface Ethernet0
!
interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
!--- Configure "no shutdown" in the stateful failover
interface as well as !--- LAN Failover interface of both
Primary and secondary ASA/PIX. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
 description LAN Failover Interface
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
!--- Command to assign the interface for LAN based
failover failover lan interface LANFailover Ethernet3
!--- Configure the Authentication/Encryption key
failover key *****
failover link stateful Ethernet2
!--- Configure the active and standby IP's for the LAN
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
standby 10.0.0.2
failover group 1
failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!
```

```
context context1
  allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
  join-failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

セカンダリ ASA

```
ASA#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover key *****
failover interface ip LANFailover 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(config-subif)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:45 UTC Jan 17 2009
Group 2 last failover at: 06:12:43 UTC Jan 17 2009

  This host:    Primary
  Group 1       State:          Active
                Active time:    359610 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
```

```
                context2 Interface inside (192.168.2.2): Normal
                context2 Interface outside (172.16.2.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3900 (sec)

                context1 Interface inside (192.168.1.2): Normal
                context1 Interface outside (172.16.1.2): Normal
                context2 Interface inside (192.168.2.1): Normal
                context2 Interface outside (172.16.2.1): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         48044      0          48040      1
        sys cmd         48042      0          48040      1
        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         2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       72081
        Xmit Q:         0       1       48044
```

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: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:46 UTC Jan 17 2009
Group 2 last failover at: 06:12:41 UTC Jan 17 2009

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3975 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

  Other host:   Primary
  Group 1       State:          Active
                Active time:    359685 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)
```

```
                context1 Interface inside (192.168.1.1): Normal
                context1 Interface outside (172.16.1.1): Normal
                context2 Interface inside (192.168.2.2): Normal
                context2 Interface outside (172.16.2.2): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         940        0          942        2
        sys cmd         940        0          940        2
        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          2          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1419
        Xmit Q:         0       1       940
```

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(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None
Other host -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None

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

セカンダリ ユニット

```
ASA(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None
Other host -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  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(config)#show failover interface
        interface stateful Ethernet2
                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
        interface LANFailover Ethernet3
                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
```

セカンダリ ユニット

```
ASA(config)#show failover interface
        interface LANFailover Ethernet3
                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 stateful Ethernet2
                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。

注：特定のインターフェイスでヘルスモニタリングを有効にするには、グローバルコンフィギュレーションモードでmonitor-interfaceコマンドを使用します。

```
monitor-interface <if_name>
```

プライマリ ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

セカンダリ ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Secondary - Active
                Interface inside (192.168.1.1): 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は、show failoverコマンドでIPアドレスが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のままになま。フェールオーバーが機能するには、フェールオーバー IP アドレスを設定する必要があります。フェールオーバーのさまざ

まな状態の詳細については、『show failover』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またはフェールオーバーグループが、FTPを使用して期待どおりにトラフィックを渡すことをテストします。たとえば、異なるインターフェイス上のホスト間でファイルを送信するとします。
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/アクティブフェールオーバーの場合は、ホストを接続するインターフェイスを含むフェールオーバーグループがアクティブになっているユニットで、次のコマンドを入力します。
   ```
   hostname(config)#no failover active group group_id
   ```
3. 同じ2つのホスト間で別のファイルを送信するには、FTPを使用します。
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/アクティブフェールオーバーの場合は、ホストを接続するインターフェイスを含むフェールオーバーグループがアクティブになっているユニットで、次のコマンドを入力します。
   ```
   hostname(config)#failover active group group_id
   ```

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。

フェールオーバー グループがスタンバイ ステートになっているユニットのシステム実行スペースで、次のコマンドを入力します。

```
hostname#failover active group group_id
```

あるいは、フェールオーバー グループがアクティブ ステートになっているユニットのシステム実行スペースで、次のコマンドを入力します。

```
hostname#no failover active group group_id
```

システムでこのコマンドを入力すると、実行スペースによって、すべてのフェールオーバーグループがアクティブになります。

```
hostname#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には（フェールオーバーがディセーブルになっている場合でも）、「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

障害が発生したアクティブ/アクティブ フェールオーバー グループを非障害ステートに復元するには、次のコマンドを入力します。

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

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ます。

1. フェールオーバーのシステム メッセージ
2. デバッグ メッセージ
3. SNMP

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。

Primary Lost Failover communications with mate on interface interface_name (プライマリで、インターフェイス interface_name のペアの相手とのフェールオーバー通信が失われた)

このフェールオーバー メッセージは、フェールオーバー ペアのうちの片方のユニットがペアのもう一方のユニットと通信できなくなっている場合に表示されます。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。

(Primary) Lost Failover communications with mate on interface interface_name

指定したインターフェイスに接続されているネットワークが正しく機能することを確認します。

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。詳細については、『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』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。詳細については、『**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**』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** コマンドを発行します。

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

同様に、failover holdtime unit msec [time] は、フェールオーバー リンクでユニットが hello メッ

セージを受信するはずの時間枠を示しており、この時間が経過すると、ピア ユニットで障害が発生したものと宣言されます。

詳細については、『failover polltime』を参照してください。

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。

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) フェールオーバー設定
- 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