CHAPTER 5

インターフェイスの設定

この章では、物理イーサネット インターフェイスを設定してイネーブルにする方法、冗長インターフェイス ペアを作成する方法、およびサブインターフェイスを追加する方法について説明します。ファイバと銅線の両方のイーサネット ポートがある場合（ASA 5510 以降のシリーズの適応型セキュリティ アプライアンスに搭載されている 4GE SSM など）、この章ではインターフェイス メディア タイプの設定方法について説明します。各インターフェイス（物理、冗長、またはサブインターフェイス）では、名前、セキュリティ レベル、および IP アドレス（ルーテッド モードのみ）を設定する必要もあります。

（注） ASA 5505 適応型セキュリティ アプライアンスのインターフェイスを設定するには、第 7 章「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」を参照してください。

マルチ コンテキスト モードでインターフェイスを設定するには、第 6 章「マルチ モードのインターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

インターフェイスの概要

この項では、物理インターフェイス、冗長インターフェイス、およびサブインターフェイスについて説明します。次の項目を取り上げます。

物理インターフェイスの概要

この項では、物理インターフェイスについて説明します。次の項目を取り上げます。

- 「物理インターフェイスのデフォルト設定」（P.5-2）
- 「コネクタ タイプ」（P.5-2）
- 「Auto-MDI/MDIX 機能」（P.5-2）

物理インターフェイスのデフォルト設定

デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は、オートネゴシエーションに設定されます。

コネクタ タイプ

ASA 5550 適応型セキュリティ アプライアンスと、ASA 5510 以降の適応型セキュリティ アプライアンスの 4GE SSM には、銅線 RJ-45 とファイバ SFP の 2 つのコネクタ タイプがあります。RJ-45 がデフォルトです。

ファイバ SFP コネクタを使用するには、メディア タイプを SFP に設定する必要があります。ファイバ インターフェイスでは、速度は固定であり、二重通信はサポートされていませんが、インターフェイスをリンク パラメータ ネゴシエーションあり（デフォルト）またはネゴシエーションなしに設定することができます。

Auto-MDI/MDIX 機能

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

冗長インターフェイスの概要

論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してセキュリティ アプライアンスの信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

その後のすべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。

この項では、冗長インターフェイスの概要を説明します。次の項目を取り上げます。

- 「冗長インターフェイスとフェールオーバーのガイドライン」（P.5-3）
- 「冗長インターフェイスの MAC アドレス」（P.5-3）
- 「冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン」（P.5-3）

冗長インターフェイスとフェールオーバーのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的なコンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
- フェールオーバーが発生しているかどうか冗長インターフェイスをモニタできます。必ず論理冗長インターフェイス名を参照してください。
- アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバ インターフェイスの MAC アドレスに関係なく使用されます（「インターフェイスの設定」（P.5-5）または「セキュリティ コンテキストの設定」（P.9-20）を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン

メンバー インターフェイスを追加する場合は次のガイドラインに従います。

- 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
- 物理インターフェイスを冗長インターフェイスに追加すると、名前、IP アドレス、およびセキュリティ レベルは削除されます。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

- 冗長インターフェイス ペアを構成する物理インターフェイスで設定できるのは物理パラメータだけです。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

VLAN サブインターフェイスと 802.1Q トランキングの概要

サブインターフェイスを使用すると、1 つの物理インターフェイスまたは冗長インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはセキュリティ アプライアンスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

この項では、次のトピックについて取り上げます。

- 「最大サブインターフェイス数」（P.5-4）
- 「物理インターフェイス上のタグなしパケットの禁止」（P.5-4）

最大サブインターフェイス数

プラットフォームに許容されるサブインターフェイスの数を決定するには、付録 A「機能のライセンスと仕様」を参照してください。

物理インターフェイス上のタグなしパケットの禁止

物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスまたは冗長インターフェイスをイネーブルにする必要があるため、物理インターフェイスまたは冗長インターフェイスでは、トラフィックを名前指定しないことで通過させないようにします。物理インターフェイスまたは冗長インターフェイスでタグなしパケットを通過させる場合は、通常どおり name コマンドを設定できます。

インターフェイスのデフォルトの状態

インターフェイスには、次のデフォルト状態があります。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュ

リティ レベルの通信のイネーブル化」（P.5-9）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけがセキュリティ アプライアンスを通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。

- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

インターフェイスの設定

インターフェイスを設定するには、次の手順を実行します。概要については、「インターフェイスの概要」（P.5-1）を参照してください。

（注） フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 14 章「ハイ アベイラビリティ」を参照してください。ただし、この手順を使用して速度やデュプレックスなどの物理インターフェイスのプロパティを設定できます。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインに移動します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。物理インターフェイスを編集するか、サブインターフェイスまたは冗長インターフェイスを追加できます。

- 物理インターフェイスまたはその他の既存のインターフェイスを編集するには、そのインターフェイス行を選択して、[Edit] をクリックします。

  [Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
- サブインターフェイスを追加および設定するには、次の手順を実行します。
  a. [Add] > [Interface] をクリックします。

     [Add Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
  b. [Hardware Port] ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイスを選択します。
  c. [VLAN ID] フィールドに、1 ～ 4095 の VLAN ID を入力します。

     一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。
  d. [Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

     許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
  e. ステップ 2 に従ってインターフェイスの設定を続行します。
- 冗長インターフェイスを追加および設定するには、次の手順を実行します。
  a. [Add] > [Redundant Interface] をクリックします。

     [Add Redundant Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。
  b. [Redundant ID] フィールドで、1 ～ 8 の整数を入力します。
  c. [Primary Interface] ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

     サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。
  d. [Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。
  e. ステップ 2 に従ってインターフェイスの設定を続行します。

ステップ 2　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 3　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「デフォルトのセキュリティ レベル」（P.5-4）を参照してください。

ステップ 4　（任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] をオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

ステップ 5　インターフェイスがまだイネーブルでない場合は、[Enable interface] をオンにします。

ステップ 6　IP アドレスを設定するには、次のいずれかのオプションを使用します。

ルーテッド ファイアウォール モードでは、すべてのインターフェイスに対する IP アドレスを設定します。トランスペアレント ファイアウォール モードでは、インターフェイスごとに IP アドレスを設定するのではなく、全体 セキュリティ アプライアンス またはコンテキスト全体に IP アドレスを設定します。トラフィックを通過させない Management 0/0 管理専用インターフェイスの場合は例外となりま

す。トランスペアレント ファイアウォール モードのセキュリティ アプライアンス全体またはコンテキスト全体の管理 IP アドレスを設定するには、[管理 IP アドレス] ペインを参照してください。Management 0/0 インターフェイスまたはサブインターフェイスの IP アドレスを設定するには、この手順を使用します。

フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブで、スタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] をクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] をクリックします。
  - **a.** （任意）オプション 61 用に、デフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[For the client identifier in DHCP option 61] > [Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。
  - **b.** （任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
  - **c.** （任意）アドミニストレーティブ ディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。
  - **d.** （任意）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

    [Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

    [Track IP Address] : トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [SLA ID] : SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

    [Monitoring Options] : [Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
  - **e.** （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。
  - **f.** （任意）セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにするには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をクリックします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。
- PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。

a. [Group Name] フィールドで、グループ名を指定します。

b. [PPPoE Username] フィールドで、ISP から提供されたユーザ名を指定します。

c. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。

d. [Confirm Password] フィールドに、パスワードを再入力します。

e. PPP 認証の場合は、[PAP]、[CHAP]、または [MSCHAP] のいずれかをクリックします。

PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

f. （任意）フラッシュ メモリにユーザ名とパスワードを保存するには、[Store Username and Password in Local Flash] をオンにします。

セキュリティ アプライアンスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドをセキュリティ アプライアンスに送信して、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再度認証できます。

g. （任意）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。詳細については、「PPPoE IP Address and Route Settings」（P.5-19）を参照してください。

ステップ 7　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　（任意）メディア タイプ、デュプレックス、および速度を設定するには、[Configure Hardware Properties] ボタンをクリックします。

a. ASA 5550 適応型セキュリティ アプライアンスまたは 4GE SSM を使用している場合は、[Media Type] ドロップダウン リストから [RJ-45] または [SFP] を選択できます。

RJ-45 がデフォルトです。

b. RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

c. 速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。
Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴ

シエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

d. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 9　（任意）MTU を設定するには、[Advanced] タブをクリックして、[MTU] フィールドに 300 ～ 65,535 バイトの値を入力します。

デフォルトは 1500 バイトです。

ステップ 10　（任意）MAC アドレスをこのインターフェイスに手動で割り当てるには、[Advanced] タブで、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。

フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このフィールドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバ インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

ステップ 11　[OK] をクリックします。

同じセキュリティ レベルの通信のイネーブル化

デフォルトでは、セキュリティ レベルが同じインターフェイス同士は通信できません。同一セキュリティ レベルのインターフェイス間での通信を許可すると、101 を超える通信インターフェイスを設定できます。インターフェイスごとに異なるレベルを使用し、同じセキュリティ レベルにインターフェイスを割り当てないようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

（注）　NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

同じインターフェイスに接続されているホスト間の通信をイネーブルにすることもできます。

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。

- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

[Interface] フィールドの説明

この項では、次のトピックについて取り上げます。

Interfaces

フィールド

- [Interface]：インターフェイス ID を表示します。割り当てられているすべてのインターフェイスが自動的に表示されます。サブインターフェイスは、インターフェイス ID とそれに続く *.n* で示されます。*n* はサブインターフェイス番号です。冗長インターフェイスは、Redundant *n* と呼ばれます。
- [Name]：インターフェイス名を表示します。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。デフォルトでは、すべてのインターフェイスはコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- [Security Level]：インターフェイスのセキュリティ レベルを 0 ～ 100 の範囲で示します。デフォルトのセキュリティ レベルは 0 です。
- [IP Address]：IP アドレスが表示されます。トランスペアレント モードの場合「native」が表示されます。トランスペアレント モードのインターフェイスは IP アドレスを使用しません。IP アドレスをコンテキストまたはセキュリティ アプライアンスに設定するには、[管理 IP アドレス] ペインを参照してください。
- [Subnet Mask]：ルーテッド モードの場合のみ。サブネット マスクを表示します。
- [Redundant]：インターフェイスが冗長インターフェイスであるかどうか（[Yes] または [No]）を示します。
- [Member]：このインターフェイスが冗長インターフェイスのメンバであるかどうか（[Yes] または [No]）を示します。
- [Management Only]：インターフェイスでセキュリティ アプライアンスへのトラフィックが許可されるか、または管理のためだけかを示します。
- [MTU]：MTU を表示します。デフォルトでは、MTU は 1500 です。

- [Active MAC Address]：アクティブな MAC アドレスを示します。[Add/Edit Interface] > [Advanced] タブで手動で割り当てると表示されます。
- [Standby MAC Address]：スタンバイ MAC アドレス（フェールオーバー用）を示します。手動で設定すると表示されます。
- [Description]：説明を表示します。
- [Add] > [Interface]：サブインターフェイスを追加します。
- [Add] > [Redundant Interface]：冗長インターフェイスを追加します。
- [Edit]：選択したインターフェイスを編集します。
- [Delete]：選択したサブインターフェイスまたは冗長インターフェイスを削除します。物理インターフェイスは削除できません。フェールオーバー リンクまたはステート リンクとしてインターフェイスを割り当てた場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで削除することはできません。
- [Enable traffic between two or more interfaces which are configured with same security levels]：同じセキュリティ レベルのインターフェイス間の通信をイネーブルにします。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。
- [Enable traffic between two or more hosts connected to the same interface]：同一インターフェイスを出入りするトラフィックをイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Edit Interface] > [General (Physical Interface)]

フィールド

- [Hardware Port]：*表示専用*。インターフェイス ID を表示します。
- [Configure Hardware Properties]：物理インターフェイスでは、[Hardware Properties] ダイアログボックスが開き、メディア タイプ、速度、およびデュプレックスを設定できます。
- [Interface Name]：インターフェイス名を 48 文字以内で設定します。
- [Security Level]：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

- [IP Address]：ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

    [DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

    [Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

    [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

    [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

    [Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

    [Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

    [Renew DHCP Lease]：DHCP リースを更新します。
  - [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

[Group Name]：グループ名を指定します。

[PPPoE Username]：ISP によって提供されたユーザ名を指定します。

[PPPoE Password]：ISP によって提供されたパスワードを指定します。

[Confirm Password]：ISP によって提供されたパスワードを指定します。

[PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash]：ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings]：[PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [General (Subinterface)]

フィールド

- [Hardware Port]：サブインターフェイスを追加する場合、イネーブル状態の任意の物理インターフェイスをサブインターフェイスの追加先として選択できます。インターフェイス ID が表示されない場合、インターフェイスがイネーブルになっているかどうかを確認してください。
- [VLAN ID]：サブインターフェイスでは、1 ～ 4095 の範囲の番号で VLAN ID を設定します。一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細 については、スイッチのマニュアルを確認してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。

- [Subinterface ID]：サブインターフェイス ID を 1 ～ 4294967293 の範囲の整数で設定します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
- [Interface Name]：インターフェイス名を 48 文字以内で設定します。
- [Security Level]：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。
- [IP Address]：ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    [Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

    [DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

    [Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

    [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

    [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

    [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

[Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease]：DHCP リースを更新します。

- [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

  [Group Name]：グループ名を指定します。

  [PPPoE Username]：ISP によって提供されたユーザ名を指定します。

  [PPPoE Password]：ISP によって提供されたパスワードを指定します。

  [Confirm Password]：ISP によって提供されたパスワードを指定します。

  [PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

  [Store Username and Password in Local Flash]：ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

  [IP Address and Route Settings]：[PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [General (Redundant Interface)]

フィールド

- [Redundant ID]：冗長インターフェイス ID を 1 ～ 8 の範囲で設定します。
- [Primary Interface]：プライマリ インターフェイスを設定します。このインターフェイスはデフォルトでアクティブになります。
- [Secondary Interface]：セカンダリ インターフェイスを設定します。
- [Interface Name]：インターフェイス名を 48 文字以内で設定します。
- [Security Level]：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）にトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [Dedicate this interface to management only]：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- [Enable Interface]：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  デフォルトでは、冗長インターフェイスはイネーブルになっています。イネーブルになっている冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。
- [IP Address]：ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [Use Static IP]：IP アドレスを手動で設定します。

    [IP address]：IP アドレスを設定します。

    [Subnet Mask]：サブネット マスクを設定します。
  - [Obtain Address via DHCP]：DHCP から IP アドレスを動的に設定します。

    [For the client identifier in DHCP option 61]：オプション 61 用にデフォルトの内部生成文字列ではなく MAC アドレスを強制的に DHCP 要求パケット内に保存するには、[Use MAC address] をクリックします。一部の ISP では、オプション 61 がインターフェイスの MAC アドレスであると想定しています。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。デフォルトの文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

    [Obtain Default Route Using DHCP]：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

[Retry Count]：4 ～ 16 の範囲で回数を設定します。セキュリティ アプライアンスは最初の試行後に DHCP 要求に応答がない場合、要求を再送信します。合計試行回数は、再試行回数に最初の試行を加えたものになります。たとえば、再試行回数を 4 に設定すると、セキュリティ アプライアンスは DHCP 要求を 5 回まで送信します。

[DHCP Learned Route Metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

[Enable tracking]：DHCP の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

[Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

[SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

[Monitoring Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

[Enable DHCP Broadcast flag for DHCP request and discover messages]：セキュリティ アプライアンスが DHCP クライアント パケットにブロードキャスト フラグを設定できるようにします。このオプションにより、DHCP クライアントが IP アドレスを要求する Discover を送信すると DHCP パケット ヘッダーのブロードキャスト フラグが 1 に設定されます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。このオプションを選択しないと、ブロードキャスト フラグは 0 に設定され、DHCP サーバは提供された IP アドレスを使用してクライアントに応答パケットをユニキャストします。DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

[Renew DHCP Lease]：DHCP リースを更新します。

- [Use PPPoE]：PPPoE を使用して IP アドレスを動的に設定します。

[Group Name]：グループ名を指定します。

[PPPoE Username]：ISP によって提供されたユーザ名を指定します。

[PPPoE Password]：ISP によって提供されたパスワードを指定します。

[Confirm Password]：ISP によって提供されたパスワードを指定します。

[PPP Authentication]：[PAP]、[CHAP]、または [MSCHAP] のいずれかを選択します。PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

[Store Username and Password in Local Flash]：ユーザ名とパスワードを、セキュリティ アプライアンス上の NVRAM の特定の場所に保存します。Auto Update Server が **clear configure** コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

[IP Address and Route Settings]：[PPPoE IP Address and Route Settings] ダイアログが表示され、アドレッシングおよびトラッキングのオプションを選択できます。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

[Add/Edit Interface] > [Advanced]

フィールド

- [MTU]：300 ～ 65,535 バイトの範囲で MTU を設定します。デフォルトは 1500 バイトです。マルチ コンテキスト モードの場合は、コンテキスト設定で MTU を設定します。
- [Mac Address Cloning]：手動で MAC アドレスを割り当てます。

  デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

  サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

  - [Active Mac Address]：MAC アドレスを H.H.H 形式でインターフェイスに割り当てます。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。
  - [Standby Mac Address]：フェールオーバーを使用する場合は、スタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Hardware Properties

フィールド

- [Hardware Port]：*表示専用*。インターフェイス ID を表示します。
- [Media Type]：メディア タイプを RJ45 または SFP に設定します。デフォルトの設定は RJ45 です。
- [Duplex]：インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて [Full]、[Half]、または [Auto] があります。
- [Speed]：インターフェイスの速度オプションが表示されます。使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

PPPoE IP Address and Route Settings

[PPPoE IP Address and Route Settings] ダイアログでは、PPPoE 接続のアドレッシングおよびトラッキング オプションを選択できます。

インターフェイスでの PPPoE の使用の詳細については、「インターフェイスの設定」（P.5-5）を参照してください。

フィールド

- [IP Address] エリア：IP アドレスを PPP から取得する方法または IP アドレスを指定する方法を選択します。次のフィールドがあります。
  - [Obtain IP Address using PPP]：セキュリティ アプライアンスを選択してイネーブルにし、PPP を使用して IP アドレスを取得します。
  - [Specify an IP Address]：セキュリティ アプライアンスは、PPPoE サーバとネゴシエートするのではなく、IP アドレスとマスクを指定してアドレスを動的に割り当てます。
- [Route Settings] エリア：ルートおよびトラッキングの設定を行います。次のフィールドがあります。
  - [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。

    [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。
  - [Enable tracking]：PPPoE の既知のルートのルート トラッキングをイネーブルにするには、このチェックボックスをオンにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。
  - [Primary Track]：プライマリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  - [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。
  - [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
  - [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。
  - [Monitor Options]：[Route Monitoring Options] ダイアログボックスを開くには、このボタンをクリックします。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
  - [Secondary Track]：セカンダリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  - [Secondary Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。