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。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）ごとに、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 モードでのインターフェイスの設定方法については、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。

この章には、次の項があります。

# 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

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自動ネゴシエーションに設定されています。

### 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 という 2 つのコネクタ タイプがあります。デフォルトは RJ-45 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 インターフェイスの速度は固定で、二重通信はサポートされませんが、インターフェイスでリンク パラメータのネゴシエーションを行う（デフォルト）か行わないかを設定できます。

### 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、デフォルトの自動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、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、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からなる物理インターフェイスのペアです。アクティブ インターフェイスに障害が発生すると、スタンバイ インターフェイスがアクティブになり、トラフィックの受け渡しを開始します。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、必要であればフェールオーバーと共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。

後続のセキュリティ アプライアンスのコンフィギュレーションはすべて、メンバーの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について説明します。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

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ってください。

- フェールオーバーまたはステート リンクに冗長インターフェイスを使用する場合、プライマリ装置だけでなくセカンダリ装置の基本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 リンクに冗長インターフェイスを使用する場合、2 つの装置の間にスイッチまたはハブを設置する必要があります。2 つの装置を直接接続することはできません。スイッチまたはハブがない場合、プライマリ装置のアクティブなポートをセカンダリ装置のスタンバイ ポートに直接接続することもできます。
- 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監視できます。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監視していると、冗長インターフェイスに障害が発生したことは表示されません。物理インターフェイスの両方に障害が発生した場合だけ、冗長インターフェイスに障害が発生したことが表示されます。

## 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追加され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内のメンバー インターフェイスの順序を変更すると、使用する MAC アドレスは、変更後の順序で先頭になる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。これはメンバー 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（P.5-6 の「インターフェイスの設定」または P.9-22 の「セキュリティ コンテキストの設定」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物理インターフェイスを使用するためのガイドライン

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ってください。

- 両方のメンバー インターフェイスの物理タイプが同じである必要があります。たとえば、両方ともイーサネットでなければなりません。
- 冗長インターフェイスに物理インターフェイスを追加すると、名前、IP　アドレス、およびセキュリティ レベルが削除されます。

**注意**　すでにコンフィギュレーションに設定されている物理インターフェイスを使用している場合、名前を削除するとそのインターフェイスを参照しているコンフィギュレーションはすべて消去されます。

- 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、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 でタグ付けした複数の論理インターフェイスに分割できます。1 つ以上の VLAN サブインターフェイスを持つ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 によってトラフィックを物理インターフェイス上で分割できるため、物理インターフェイスやセキュリティ 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。

ここでは、次の項目について説明します。

- 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

使用するプラットフォームで許容されるサブインターフェイス数を判別するには、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

サブインターフェイスを使用する場合、通常はトラフィックが物理インターフェイスを通過することを禁止します。これは物理インターフェイスをタグのないパケットが通過してしまうためです。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。トラフィックがサブインターフェイスを通過するには、物理インターフェイスまたは冗長インターフェイスがイネーブルになっている必要があるため、トラフィックが通過しないように物理インターフェイスまたは冗長インターフェイスに name コマンドを使用しないでください。物理インターフェイスまたは冗長インターフェイスにタグのないパケットを通過させるには、通常通り name コマンドを設定します。

## インターフェイスのデフォルトの状態

インターフェイスは、デフォルトで次の状態になっています。

- 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できるようにするには、メンバーの物理インターフェイスもイネーブルにする必要があります。
- 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できるようにするには、物理インターフェイスもイネーブルにする必要があります。

## 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、明示的なセキュリティ 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 を割り当てる場合があります。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、P.5-10 の「同じセキュリティ レベルの通信のイネーブル化」を参照してください。

各レベルは、次の動作を制御します。

- ネットワーク アクセス：デフォルトでは、高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイス（発信）へのアクセスは、暗黙的に許可されます。高位のセキュリティ インターフェイス上のホストは、それより低いセキュリティ インターフェイス上のホストすべてにアクセスできます。アクセスは、インターフェイスにアクセスリストを適用すると制限できます。

  同じレベルのセキュリティ インターフェイスの場合、同じセキュリティ レベルまたはそれより低いレベルの他のインターフェイスへのアクセスは、暗黙的に許可されます。
- 検査エンジン：一部のアプリケーション検査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の場合、検査エンジンはどちらの方向のトラフィックにも適用されます。
  - NetBIOS 検査エンジン：発信接続のみに適用されます。
  - SQL*Net 検査エンジン：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、着信データ接続のみセキュリティ 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）フィルタリングおよび FTP フィルタリングは、発信接続（高位レベルから低位レベルへの接続）に対してのみ適用されます。

  同じセキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックにもフィルタリングが適用できます。
- NAT 制御：NAT 制御をイネーブルにする場合、低位のセキュリティ インターフェイス（外部）上のホストにアクセスする高位のセキュリティ インターフェイス（内部）上のホストに NAT を設定する必要があります。

  NAT 制御がない場合、または同じレベルのセキュリティ インターフェイスの場合は、任意のインターフェイス間で NAT を使用するように選択することも、NAT を使用しないように選択することもできます。外部インターフェイスに対して NAT を設定すると、特殊なキーワードが必要になる場合があることに留意してください。
- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン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では、両方向に対して **established** コマンドが設定できます。

# 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、P.5-2 の「インターフェイスの概要」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 リンクおよびステート リンクの設定については、第 14 章「高可用性」を参照してください。ただし、この手順を使用して速度や二重通信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、インターフェイスを選択して **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 フィールドで、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。

     許容されるサブインターフェイス数は、プラットフォームによって異なります。ID は、設定した後で変更することはできません。
  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 フィールドで、名前を 48 文字以内で入力します。

**ステップ 3**　Security level フィールドで、0（最小）～ 100（最大）のレベルを入力します。

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

**ステップ 4**　（オプション）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の IP アドレスを設定します。透過ファイアウォール 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、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。透過ファイアウォール モードでセキュリティ アプライアンス全体またはコンテキスト管理 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、次の手順に従います。

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. （オプション）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. （オプション）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. （オプション）管理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、既知のルートの管理ディスタンスは 1 になります。
  d. （オプション）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です。1 ～ 500 の範囲の値を指定できます。

     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、ルートの次の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。1 ～ 2147483647 の範囲の値を指定できます。

Monitoring Options：Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスで、トラッキングされた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. （オプション）リースを更新するには、**Renew DHCP Lease** をクリックします。

f. （オプション）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。このオプションを指定した場合、DHCP クライアントが IP アドレス要求を要求する 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 フラグをリスンし、フラグが 1 に設定されていれば応答パケットをブロードキャストします。このオプションを指定しないと、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とユニキャスト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 フィールドで、パスワードを再入力します。

e. PPP 認証の場合、PAP、CHAP、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鍵を生成します。

f. （オプション）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. （オプション）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、P.5-19 の「PPPoE IP Address and Route Settings」を参照してください。

**ステップ 7**　（オプション）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 リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

**ステップ 8**　（オプション）メディア タイプ、二重通信、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。

デフォルトは RJ-45 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。

指定できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、常に 1000 Mbps です。また、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、デフォルトの自動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、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、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**　（オプション）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**　（オプション）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 H.H.H 形式（H は 16 ビットの 16 進数）で MAC アドレスを入力します。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、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、新たなアクティブ装置はアクティブ MAC アドレスを使用して、ネットワークの中断を最小限に抑え、元の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焼き付け済み 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焼き付け済み MAC アドレスを使用します。冗長インターフェイスは追加され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内のメンバー インターフェイスの順序を変更すると、使用する MAC アドレスは、変更後の順序で先頭になる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、メンバー インターフェイスの MAC アドレスに関係なく、割り当てられた 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もできます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセス コントロールを行っている場合があります。

**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。同じセキュリティのインターフェイス間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。各インターフェイスで異なるセキュリティ レベルを使用したときに、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と、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

**（注）** NAT 制御をイネーブルにした場合、同じセキュリティ レベルのインターフェイス間に NAT を設定する必要はありません。

同じセキュリティ レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

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

ここでは、次の項目について説明します。



## 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一覧表示されます。サブインターフェイスは、インターフェイス ID の後の *.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：インターフェイスの名前を表示します。
- Enabled：インターフェイスがイネーブルかどうかを Yes または No で示します。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、そのインターフェイス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。透過モードの場合「native」が表示されます。透過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 モードのみ。サブネット マスクを表示します。
- Redundant：このインターフェイスが冗長インターフェイスかどうかを Yes または No で示します。
- 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ーかどうかを Yes または No で示します。
- Management Only：インターフェイスにセキュリティ アプライアンスへの、管理専用のトラフィックを許可する場合を示します。
- 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 リンクに割り当てたインターフェイス（Failover: Setup タブを参照）は、このペインで削除できません。
- Enable traffic between two or more interfaces which are configured with same security levels：セキュリティ レベルが同じ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 レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。
- Enable traffic between two or more hosts connected to the same interface：同一インターフェイスの送受信トラフィックをイネーブルにします。

### モード

次の表に、この機能を使用できるモードを示します。

| 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：表示のみ。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、および二重通信を設定できます。
- 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、内部インターフェイスから外部インターフェイス（低いセキュリティ レベル）へ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も、それぞれのインターフェイスの相対セキュリティ レベルに影響されます。
- 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 モードのみ。マルチコンテキスト モードでは、IP アドレスをコンテキスト コンフィギュレーションに設定します。
  - 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 アドレスをダイナミックに設定します。

    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に送信した DHCP 要求に応答がない場合、要求を再送信します。要求の合計送信回数は、再送信回数と最初の送信になります。たとえば、再送信回数を 4 に設定すると、DHCP 要求が 5 回まで送信されます。

DHCP Learned Route Metric : 管理ディスタンスを既知のルートに割り当てます。1 ～ 255 の範囲の値を設定します。フィールドが空白の場合、既知のルートの管理ディスタンスは 1 になります。

Enable tracking：DHCP の既知のルートのトラッキングをイネーブルにします。

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

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です。1 ～ 500 の範囲の値を指定できます。

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、ルートの次の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。1 ～ 2147483647 の範囲の値を指定できます。

Monitoring Options：Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスで、トラッキングされた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。このオプションを指定した場合、DHCP クライアントが IP アドレス要求を要求する 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 フラグをリスンし、フラグが 1 に設定されていれば応答パケットをブロードキャストします。このオプションを指定しないと、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とユニキャストの両方を受信できます。

Renew DHCP Lease：DHCP のリース期間を更新します。

- Use PPPoE：PPPoE で IP アドレスをダイナミックに設定します。

Group Name：グループ名を指定します。

PPPoE Username：ISP で使用できるユーザ名を指定します。

PPPoE Password：ISP で使用できるパスワードを指定します。

Confirm Password：ISP で使用できるパスワードを指定します。

PPP Authentication：PAP、CHAP、MSCHAP から選択します。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鍵を生成します。

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 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。

IP Address and Route Settings：PPPoE IP Address and Route Settings ダイアログボックスが表示され、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）240 文字以内で入力します。1 行で入力し、改行はできません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

### モード

次の表に、この機能を使用できるモードを示します。

| 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と、イネーブル状態の物理インターフェイスを選択でき、そこにサブインターフェイスが追加されます。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 モードでは、VLAN はシステム コンフィギュレーションのみに設定できます。
- 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。使用できるサブインターフェイスの数は、使用するプラットフォームによって異なります。ID は、設定した後で変更することはできません。
- 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、内部インターフェイスから外部インターフェイス（低いセキュリティ レベル）へ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も、それぞれのインターフェイスの相対セキュリティ レベルに影響されます。
- 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 モードのみ。マルチコンテキスト モードでは、IP アドレスをコンテキスト コンフィギュレーションに設定します。
  - 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 アドレスをダイナミックに設定します。

    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に送信した DHCP 要求に応答がない場合、要求を再送信します。要求の合計送信回数は、再送信回数と最初の送信になります。たとえば、再送信回数を 4 に設定すると、DHCP 要求が 5 回まで送信されます。

DHCP Learned Route Metric：管理ディスタンスを既知のルートに割り当てます。1 ～ 255 の範囲の値を設定します。フィールドが空白の場合、既知のルートの管理ディスタンスは 1 になります。

Enable tracking：DHCP の既知のルートのトラッキングをイネーブルにします。

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

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です。1 ～ 500 の範囲の値を指定できます。

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、ルートの次の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。1 ～ 2147483647 の範囲の値を指定できます。

Monitoring Options：Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスで、トラッキングされた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。このオプションを指定した場合、DHCP クライアントが IP アドレス要求を要求する 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 フラグをリスンし、フラグが 1 に設定されていれば応答パケットをブロードキャストします。このオプションを指定しないと、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とユニキャストの両方を受信できます。

Renew DHCP Lease：DHCP のリース期間を更新します。

— Use PPPoE：PPPoE で IP アドレスをダイナミックに設定します。

Group Name：グループ名を指定します。

PPPoE Username：ISP で使用できるユーザ名を指定します。

PPPoE Password：ISP で使用できるパスワードを指定します。

Confirm Password：ISP で使用できるパスワードを指定します。

PPP Authentication：PAP、CHAP、MSCHAP から選択します。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鍵を生成します。

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 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。

IP Address and Route Settings：PPPoE IP Address and Route Settings ダイアログボックスが表示され、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）240 文字以内で入力します。1 行で入力し、改行はできません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

### モード

次の表に、この機能を使用できるモードを示します。

| 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 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、内部インターフェイスから外部インターフェイス（低いセキュリティ レベル）へ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も、それぞれのインターフェイスの相対セキュリティ レベルに影響されます。
- 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 モードのみ。マルチコンテキスト モードでは、IP アドレスをコンテキスト コンフィギュレーションに設定します。
  - 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 アドレスをダイナミックに設定します。

    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に送信した DHCP 要求に応答がない場合、要求を再送信します。要求の合計送信回数は、再送信回数と最初の送信になります。たとえば、再送信回数を 4 に設定すると、DHCP 要求が 5 回まで送信されます。

DHCP Learned Route Metric : 管理ディスタンスを既知のルートに割り当てます。1 ～ 255 の範囲の値を設定します。フィールドが空白の場合、既知のルートの管理ディスタンスは 1 になります。

Enable tracking：DHCP の既知のルートのトラッキングをイネーブルにします。

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

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です。1 ～ 500 の範囲の値を指定できます。

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、ルートの次の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。1 ～ 2147483647 の範囲の値を指定できます。

Monitoring Options：Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスで、トラッキングされた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。このオプションを指定した場合、DHCP クライアントが IP アドレス要求を要求する 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 フラグをリスンし、フラグが 1 に設定されていれば応答パケットをブロードキャストします。このオプションを指定しないと、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とユニキャストの両方を受信できます。

Renew DHCP Lease：DHCP のリース期間を更新します。

- Use PPPoE：PPPoE で IP アドレスをダイナミックに設定します。

Group Name：グループ名を指定します。

PPPoE Username：ISP で使用できるユーザ名を指定します。

PPPoE Password：ISP で使用できるパスワードを指定します。

Confirm Password：ISP で使用できるパスワードを指定します。

PPP Authentication：PAP、CHAP、MSCHAP から選択します。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鍵を生成します。

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 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。

IP Address and Route Settings：PPPoE IP Address and Route Settings ダイアログボックスが表示され、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）240 文字以内で入力します。1 行で入力し、改行はできません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。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 リンクに設定すると、入力した説明は固定の説明に上書きされます。

### モード

次の表に、この機能を使用できるモードを示します。

| 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 モードでは、MTU をコンテキスト コンフィギュレーションに設定します。
- Mac Address Cloning：MAC アドレスを手動で割り当てます。

  デフォルトでは、物理インターフェイスは焼き付け済み 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焼き付け済み 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もできます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセス コントロールを行っている場合があります。

  - 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 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。
  - Standby Mac Address：フェールオーバーで使用する場合は、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、新たなアクティブ装置はアクティブ MAC アドレスを使用して、ネットワークの中断を最小限に抑え、元の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

次の表に、この機能を使用できるモードを示します。

| 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：表示のみ。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。デフォルトは RJ45 です。
- Duplex：インターフェイスの二重通信オプションを一覧表示します。Full、Half、Auto があり、インターフェイス タイプによって異なります。
- Speed：インターフェイスの速度オプションを一覧表示します。指定できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、常に 1000 Mbps です。また、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、デフォルトの自動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、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

### モード

次の表に、この機能を使用できるモードを示します。

| 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 ダイアログボックスで、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、P.5-6 の「インターフェイスの設定」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ダイナミックに割り当てます。
- 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と、コンフィギュレーション時にスタティックに定義されたルートになりません。

    PPPoE learned route metric：管理ディスタンスを既知のルートに割り当てます。1 ～ 255 の範囲の値を設定します。フィールドが空白の場合、既知のルートの管理ディスタンスは 1 になります。

- Enable tracking：PPPoE の既知のルートのトラッキングをイネーブルにします。

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

- 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です。1 ～ 500 の範囲の値を指定できます。
- 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、ルートの次の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。1 ～ 2147483647 の範囲の値を指定できます。
- Monitor Options：Route Monitoring Options ダイアログボックスを開きます。Route Monitoring Options ダイアログボックスで、トラッキングされた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です。1 ～ 500 の範囲の値を指定できます。