



## インターフェイスの設定

この章では、各インターフェイスおよびサブインターフェイスの名前、セキュリティ レベル、IP アドレスの設定方法について説明します。マルチコンテキスト モードでは、ハードウェア プロパティの設定およびサブインターフェイスの作成をシステム実行スペースで行い、IP アドレス、名前、セキュリティ レベルをコンテキストごとに設定します。



(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 5 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。

この章には、次の項があります。

- [セキュリティ レベルの概要 \(P.4-2\)](#)
- [インターフェイスの設定 \(P.4-3\)](#)

## セキュリティ レベルの概要

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。

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にアクセスする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对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

デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブ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。マルチコンテキストモードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではその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。



(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タスフル 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タスリンクの設定については、[第 12 章「フェールオーバー」](#)を参照してください。

マルチコンテキストモードでは、次のガイドラインに従ってください。

- 各コンテキスト内でコンテキスト インターフェイスを設定します。
- システム コンフィギュレーションのコンテキストにすでに割り当てられているコンテキスト インターフェイスのみが設定できます。
- システム コンフィギュレーションでは、イーサネット設定および VLAN のみが設定できます。フェールオーバー インターフェイスは例外で、この方法でフェールオーバー インターフェイスは設定しないでください。詳細については、フェールオーバーの章を参照してください。

ここでは、次の項目について説明します。

- [Interfaces \(システム\) \(P.4-3\)](#)
- [Interfaces \(シングルモードとコンテキスト\) \(P.4-6\)](#)

## Interfaces (システム)

### System > Configuration > Interfaces

Interfaces ペインで、設定済みのインターフェイスおよびサブインターフェイスを表示します。セキュリティ コンテキストにインターフェイスを割り当てる前に ([P.7-19 の「セキュリティ コンテキストの設定」](#)を参照)、このペインでインターフェイスを定義します。システム コンフィギュレーションにインターフェイスのネットワーク パラメータがなくても、システムはインターフェイスからコンテキストへの割り当てを制御します。

### フィールド

- **Interface** : インターフェイス ID を表示します。すべての物理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。

フェールオーバーを使用する場合、[Failover: Setup](#) タブで、フェールオーバー リンクに専用の物理インターフェイスを割り当てます。ステータスフル フェールオーバーにオプションのインターフェイスも割り当てられます (フェールオーバーとステータス フォックには同じインターフェイスを使用できますが、分けることをお勧めします)。フェールオーバーでインターフェイスを確実に使用するには、[Interfaces](#) ペインでインターフェイス名を設定しないでください。IP アドレスなどの他の設定が無視されます。すべての関連するパラメータは [Failover: Setup](#)

タブで設定します。物理インターフェイスまたはサブインターフェイスに名前を設定しない限り、フェールオーバーにサブインターフェイスを使用できます。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は、このペインで編集および削除ができなくなります。ただし、ステート リンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。

- **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、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブ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。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではその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。
- **VLAN** : サブインターフェイスに割り当てられた VLAN を示します。物理インターフェイスには「native」が表示されます。タグがない物理インターフェイスという意味です。
- **Description** : 説明を表示します。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。
- **Add** : サブ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。フェールオーバーまたはステート 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、このペインで編集できません。ただし、ステート リンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。
- **Delete** : 選択したサブインターフェイスを削除します。物理インターフェイスまたはコンテキストで割り当てたインターフェイスは削除できません。フェールオーバーまたはステート 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。

## 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 |        |      |
|--------------|----|---------------|--------|------|
| ルールヘッド       | 透過 | シングル          | マルチ    |      |
|              |    |               | コンテキスト | システム |
| •            | •  | —             | —      | •    |

## Add/Edit Interface

### System > Configuration > Interfaces > Add/Edit Interface

**Add Interface** ダイアログボックスでサブインターフェイスを追加できます。**Edit Interface** ダイアログボックスで、インターフェイスまたはサブインターフェイスを編集できます。

フェールオーバーに物理インターフェイスを使用する場合、このダイアログボックスでインターフェイスを設定しないでください。代わりに、[Failover: Setup](#) タブを使用します。特にインターフェイス名は設定しないでください。設定すると、フェールオーバー リンクにインターフェイスを使用できなくなります。他のパラメータは無視されます。

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は、Interfaces ページで編集および削除できなくなります。ただし、ステート リンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。

### 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。
- **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、速度および二重通信を設定できます。
- **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、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブ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。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではその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。

- **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。
- **Sub-interface 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。
- **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。システムの説明はコンテキストの説明に依存しません。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 |        |      |
|--------------|----|---------------|--------|------|
| ルーテッド        | 透過 | シングル          | マルチ    |      |
|              |    |               | コンテキスト | システム |
| •            | •  | —             | —      | •    |

## Hardware Properties

### System > Configuration > Interfaces > Edit Interface > Hardware Properties

Hardware Properties ダイアログボックスで、物理インターフェイスの速度および二重通信を設定できます。

#### 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 |        |      |
|--------------|----|---------------|--------|------|
| ルーテッド        | 透過 | シングル          | マルチ    |      |
|              |    |               | コンテキスト | システム |
| •            | •  | —             | —      | •    |

## Interfaces (シングルモードとコンテキスト)

### Configuration > Interfaces

Interfaces ペインで、設定済みのインターフェイスおよびサブインターフェイスを表示します。サブインターフェイスを追加または削除します (シングルモードのみ)。また、同一セキュリティ レベルのインターフェイス間の通信、または同じ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。

透過ファイアウォール モードでは、2つのインターフェイスのみがトラフィックを通過できます。ただし、プラットフォームに専用管理インターフェイス Management 0/0 がある場合、そのインターフェイス (物理インターフェイスまたはサブインターフェイス) を管理トラフィック用の第3のインターフェイスとして使用できます。

#### 利点

このペインで、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できます。

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 レベルのインターフェイス間で通信を許可する利点としては、次のものがあります。

- 101 以上の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、同一のセキュリティ 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。
- アクセスリストがなくても同じセキュリティ レベルのインターフェイスすべての中で自由にトラフィックが流れるようにできます。

## フィールド

- **Interface** : インターフェイス ID を表示します。すべての物理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。

フェールオーバーを使用する場合、**Failover: Setup** タブで、フェールオーバー リンクに専用の物理インターフェイスを割り当てます。ステートフル フェールオーバーにオプションのインターフェイスも割り当てられます (フェールオーバーとステート トラフィックには同じインターフェイスを使用できますが、分けることをお勧めします)。フェールオーバーでインターフェイスを確実に使用するには、**Interfaces** ペインでインターフェイス名を設定しないでください。IP アドレスなどの他の設定が無視されます。すべての関連するパラメータは **Failover: Setup** タブで設定します。物理インターフェイスまたはサブインターフェイスに名前を設定しない限り、フェールオーバーにサブインターフェイスを使用できます。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は、このペインで編集および削除ができなくなります。ただし、ステートリンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。

マルチコンテキスト モードでは、物理インターフェイスはシステム コンフィギュレーションのみに一覧表示されます。コンテキストにインターフェイスを割り当てると、自動的にコンテキストに一覧表示されます。

- **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、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブ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。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではその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、「**Management IP** 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。
- **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** タブで手動で設定すると表示されます。
- **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。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。



- **Add** : サブ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。フェールオーバーまたはステート 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、このペインで編集できません。ただし、ステートリンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。
- **Delete** : 選択したサブインターフェイスを削除します。物理インターフェイスまたはコンテキストで割り当てたインターフェイスは削除できません。フェールオーバー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 |        |                   |
|--------------|----|---------------|--------|-------------------|
| ルールヘッド       | 透過 | シングル          | マルチ    |                   |
|              |    |               | コンテキスト | システム <sup>1</sup> |
| •            | •  | •             | •      | —                 |

1. Interfaces のシステム ペインについては、「[Interfaces \(システム\) ペイン](#)」を参照してください。

## Add/Edit Interface > General

### Configuration > Interfaces > Add/Edit Interface > General

Add Interface > General タブでサブインターフェイスを追加できます。Edit Interface > General タブで、インターフェイスまたはサブインターフェイスを編集できます。マルチコンテキスト モードでは、インターフェイスはシステム コンフィギュレーションのみに追加できます。インターフェイスをコンテキストに割り当てるには、[P.7-19](#)の「[セキュリティ コンテキストの設定](#)」を参照してください。

フェールオーバーに物理インターフェイスを使用する場合、このダイアログボックスでインターフェイスを設定しないでください。代わりに、**Failover: Setup** タブを使用します。特にインターフェイス名は設定しないでください。設定すると、フェールオーバー リンクにインターフェイスを使用できなくなります。他のパラメータは無視されます。

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は、Interfaces ペインで編集および削除できなくなります。ただし、ステートリンクに設定した物理インターフェイスだけは例外で、速度および二重通信を設定できます。

### 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。
- **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、速度および二重通信を設定できます。一部のインターフェイスでは、メディアタイプも設定できます。マルチコンテキスト モードでは、物理プロパティはシステム コンフィギュレーションのみに設定できます。



- **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。さらに、トラフィックがセキュリティ ポリシーに従って通過できるように、IP アドレス (ルーテッドモードの) と名前を事前に設定する必要があります。デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブ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しておく必要があります。マルチコンテキストモードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではその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。
- **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。
- **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。
- **Sub-interface 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。
- **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。
    - 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。
    - Renew DHCP Lease** : DHCP のリース期間を更新します。
    - 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 プロセスに使用される一意の識別子です。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が開きます。[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。

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



(注) PPPoE はフェールオーバーでサポートされません。マルチコンテキスト モードおよび透過モードでもサポートされません。PPPoE は、フェールオーバーのない、シングルルーテッドモードの場合でのみサポートされます。

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します。

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。マルチコンテキスト モードでは、システムの説明はコンテキストの説明に依存しません。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 |        |                   |
|--------------|----|---------------|--------|-------------------|
| ルーテッド        | 透過 | シングル          | マルチ    | システム <sup>1</sup> |
|              |    |               | コンテキスト |                   |
| •            | •  | •             | •      | —                 |

1. システムの Add/Edit Interfaces ダイアログボックスについては、システムの [Add/Edit Interface](#) ダイアログボックスを参照してください。

## Add/Edit Interface &gt; Advanced

## Configuration &gt; Interfaces &gt; Add/Edit Interface &gt; Advanced

Add/Edit Interface > Advanced タブで、インターフェイスの MTU および MAC アドレスを設定できます。

## 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。

マルチコンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すれば、セキュリティ アプライアンスでは、該当するコンテキストへのパケットの分類が容易になります。固有の MAC アドレスが割り当てられていない共有インターフェイスも使用できますが、いくつか制限があります。詳細については、P.7-3 の「[セキュリティ アプライアンスによるパケットの分類方法](#)」を参照してください。コンテキストの共有インターフェイス用に手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、P.7-19 の「[Security Contexts](#)」を参照してください。MAC アドレスを自動生成する場合、このオプションを使用すれば生成されたアドレスを上書きできます。

シングルコンテキスト モード、またはマルチコンテキスト モードでの未共有インターフェイスの場合、固有の MAC アドレスをサブインターフェイスに割り当てることができます。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 |        |                   |
|--------------|----|---------------|--------|-------------------|
| ルーテッド        | 透過 | シングル          | マルチ    | システム <sup>1</sup> |
|              |    |               | コンテキスト |                   |
| •            | •  | •             | •      | —                 |

1. システムの Add/Edit Interfaces ダイアログボックスについては、システムの Add/Edit Interface ダイアログボックスを参照してください。

## PPPoE IP Address and Route Settings

Configuration > Interfaces > Add/Edit Interface > General > 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。

### 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 アプライアンスは PPP から 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に使用される一意の識別子です。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が開きます。[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。

## Hardware Properties

### Configuration > Interfaces > Edit Interface > Hardware Properties

Hardware Properties ダイアログボックスで、物理インターフェイス、SSM インターフェイス、メディア タイプの速度および二重通信を設定できます。マルチコンテキスト モードでは、システム コンフィギュレーションに設定してください。

#### 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。
- **MAC Address** : 表示のみ。インターフェイスの MAC アドレスを表示します。
- **Media Type** : メディア タイプを RJ45 または SFP に設定します。SFP は、ASA 5500 シリーズ適応型セキュリティ アプライアンスの SSM インターフェイスでのみサポートされています。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 |        |                   |
|--------------|----|---------------|--------|-------------------|
| ルーテッド        | 透過 | シングル          | マルチ    |                   |
|              |    |               | コンテキスト | システム <sup>1</sup> |
| •            | •  | •             | •      | —                 |

1. システムの Hardware Properties ダイアログボックスについては、システムの [Hardware Properties](#) ダイアログボックスを参照してください。

