CHAPTER 7

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

この章では、ASA 5505 適応型セキュリティ アプライアンスのスイッチ ポートと VLAN インターフェイスを設定する方法について説明します。

（注） 他のモデルのインターフェイスを設定するには、第 5 章「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、ASA 5505 適応型セキュリティ アプライアンスのポートおよび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。

ASA 5505 のポートおよびインターフェイスについて

ASA 5505 適応型セキュリティ アプライアンスでは、組み込みスイッチがサポートされています。次の 2 種類のポートおよびインターフェイスを設定する必要があります。

- 物理スイッチ ポート：適応型セキュリティ アプライアンスには、ハードウェアのスイッチング機能を使用して、レイヤ 2 でトラフィックを転送する 8 つのファスト イーサネット スイッチ ポートがあります。これらのポートのうちの 2 つは PoE ポートです。詳細については、「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。」（P.7-5）を参照してください。これらのインターフェイスを、PC、IP 電話、DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。
- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。最大 VLAN インターフェイス数の詳細については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」を参照してください。VLAN インターフェイスを使用することにより、別々の VLAN、たとえばホーム VLAN、ビジネス VLAN、インターネット VLAN などに装置を分けることができます。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、VLAN 1 上のスイッチ ポートが VLAN 2 上のスイッチ ポートと通信する場合、適応型セキュリティ アプライアンスはセキュリティ ポリシーをトラフィックに適用し、2 つの VLAN 間でルーティングまたはブリッジングします。

（注） サブインターフェイスは、ASA 5505 適応型セキュリティ アプライアンスでは使用できません。

ライセンスで使用できる最大アクティブ VLAN インターフェイス数

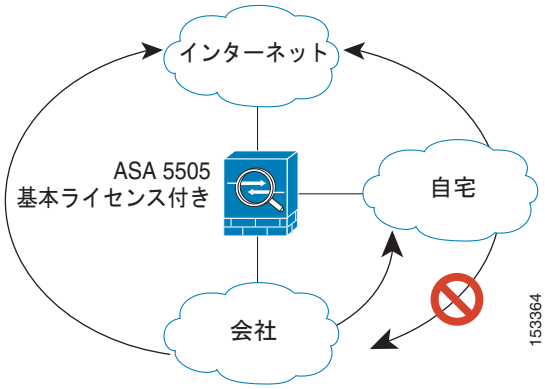
トランスペアレント ファイアウォール モードでは、基本ライセンスはアクティブ VLAN を 2 つ、Security Plus ライセンスは 3 つ設定できます。そのうちの 1 つは、フェールオーバー用です。

ルーテッド モードでは、基本ライセンスはアクティブ VLAN を 3 つまで、Security Plus ライセンスは 20 まで設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

基本ライセンスの場合、3 つめの VLAN は他の 1 つの VLAN にのみトラフィックを開始するように設定できます。図 7-1 のネットワークの例では、ホーム VLAN はインターネットと通信できますが、ビジネス VLAN とは接続を開始できません。

図 7-1　基本ライセンスでの ASA 5505 適応型セキュリティ アプライアンス

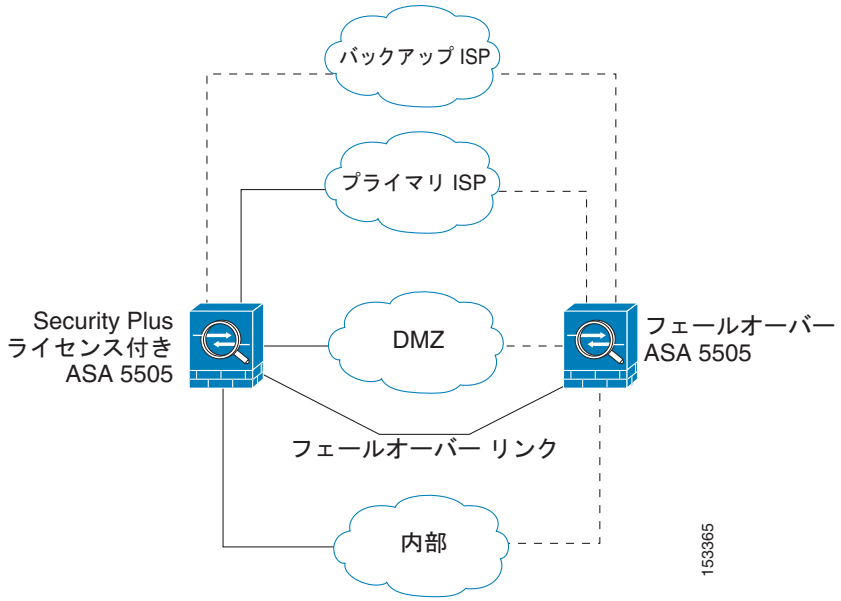


Security Plus ライセンスでは、20 の VLAN インターフェイスを設定できます。トランク ポートを設定して、1 つのポートで複数の VLAN を使用できます。

（注） ASA 5505 適応型セキュリティ アプライアンスは、Active/Standby フェールオーバーをサポートしますが、ステートフル フェールオーバーをサポートしていません。

ネットワークの例については、図 7-2 を参照してください。

図 7-2　Security Plus ライセンスでの ASA 5505 適応型セキュリティ アプライアンス



デフォルト インターフェイス コンフィギュレーション

ご使用の適応型セキュリティ アプライアンスに工場出荷時のデフォルト コンフィギュレーションが含まれている場合、インターフェイスは次のように設定されています。

- 外部インターフェイス（セキュリティ レベル 0）は VLAN 2 です。

  イーサネット 0/0 が VLAN 2 に割り当てられ、イネーブルになります。

  VLAN 2 の IP アドレスは DHCP サーバから取得します。
- 内部インターフェイス（セキュリティ レベル 100）は VLAN 1 です。

  イーサネット 0/1 ～イーサネット 0/7 が VLAN 1 に割り当てられ、イネーブルになります。

  VLAN 1 の IP アドレスは 192.168.1.1 です。

configure factory-default コマンドを使用して、工場出荷時のデフォルト コンフィギュレーションを復元します。

この章の手順に従い、デフォルト コンフィギュレーションを変更します。たとえば、VLAN インターフェイスの追加を行います。

工場出荷時のデフォルト コンフィギュレーションになっていない場合は、すべてのスイッチ ポートが VLAN 1 ですが、その他のパラメータは未設定です。

VLAN MAC アドレス

ルーテッド ファイアウォール モードでは、すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。

トランスペアレント ファイアウォール モードでは、各 VLAN に固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。

Power Over Ethernet

Ethernet 0/6 および Ethernet 0/7 は、IP 電話や無線アクセス ポイントなどのデバイス用に PoE をサポートしています。非 PoE デバイスをインストールした場合やこれらのスイッチ ポートに接続しない場合、適応型セキュリティ アプライアンスはスイッチ ポートに電源を供給しません。

[Edit Switch Port] ダイアログボックスでスイッチ ポートをシャットダウンすると、デバイスへの電源がディセーブルになります。再度イネーブルにするよう入力すれば、電源が復元します。

接続されているデバイスのタイプ（Cisco または IEEE 802.3af）など、PoE スイッチ ポートのステータスを確認するには、**show power inline** コマンドを使用します。

SPAN を使用したトラフィックのモニタリング

1 つまたは複数のスイッチ ポートを出入りするトラフィックをモニタするには、スイッチ ポート モニタリングとも呼ばれる SPAN をイネーブルにします。SPAN をイネーブルにしたポート（宛先ポートと呼ばれる）は、特定の送信元ポートで送受信するすべてのパケットのコピーを受信します。SPAN 機能を使用すれば、スニファを宛先ポートに添付して、すべてのトラフィックをモニタできます。SPAN を使用しないと、モニタするポートごとにスニファを添付しなければなりません。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。

SPAN 監視をイネーブルにするには、Command Line Interface ツールを使用し、**switchport monitor** コマンドを入力する必要があります。詳細については、『*Cisco Security Appliance Command Reference*』の **switchport monitor** コマンドを参照してください。

セキュリティ レベルの概要

各 VLAN インターフェイスには、0 ～ 100（最下位～最上位）までのセキュリティ レベルを割り当てる必要があります。たとえば、内部ビジネス 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。ホーム ネットワーク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。

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適応型セキュリティ アプライアンスを通過することを許可されます。

- 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。

VLAN インターフェイスの設定

設定可能な VLAN 数については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」（P.7-2）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、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 リンクを設定するには、第 14 章「ハイアベイラビリティ」を参照してください。

Easy VPN をイネーブルにすると、VLAN インターフェイスを追加または削除できません。また、セキュリティ レベルまたはインターフェイス名の変更もできません。インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。

この項では、次のトピックについて取り上げます。

[Interfaces] > [Interfaces]

[Interfaces] タブでは、設定済みの VLAN インターフェイスを表示します。VLAN インターフェイスを追加または削除したり、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たり、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することができます。

トランスペアレント 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。

フィールド

- [Name]：インターフェイス名を表示します。
- [Switch Ports]：この VLAN インターフェイスに割り当てられたスイッチ ポートを表示します。
- [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。
- [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。
- [Restrict Traffic Flow]：このインターフェイスから別の VLAN への接続開始が制限されているかどうかを示します。

  基本ライセンスでは、このオプションを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネス ネットワークにアクセスする必要がないので、ホーム VLAN で [Restrict Traffic Flow] オプションを使用できます。ビジネス ネットワークはホーム ネットワークにアクセスできますが、その反対はできません。

2 つの VLAN インターフェイスに名前をすでに設定している場合、必ず [Restrict Traffic Flow] オプションをイネーブルにしてから 3 番目のインターフェイスに名前を付けてください。ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスでは、3 つの VLAN インターフェイスがフル機能を持つことは許可されていません。

（注） Security Plus ライセンスにアップグレードすれば、このオプションを削除して、このインターフェイスのフル機能を取得できます。このオプションをイネーブルにしたままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

- [Backup Interface]：このインターフェイスに使用されるバックアップ ISP インターフェイスを示します。インターフェイスに障害が発生すると、バックアップ インターフェイスに切り替わります。

  プライマリ インターフェイスによるデフォルト ルートに障害が発生しない限り、バックアップ インターフェイスはトラフィックを通過させません。このオプションは Easy VPN で便利です。バックアップ インターフェイスがプライマリになると、セキュリティ アプライアンスは新しいプライマリ インターフェイスに VPN ルールを適用します。

  プライマリに障害が発生した場合に、トラフィックがバックアップ インターフェイスを通過できるようにするには、プライマリとバックアップの両方のインターフェイスにデフォルト ルートを設定して、プライマリでの障害発生時にバックアップ インターフェイスを使用できるようにします。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。デュアル ISP サポートを設定するには、「スタティック ルート トラッキング」（P.16-44）を参照してください。
- [VLAN]：このインターフェイスの VLAN ID 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。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。
- [Add]：インターフェイスを追加します。Easy VPN をイネーブルにしている場合、VLAN インターフェイスを追加できません。
- [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 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ている場合（[[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編集することはできません。Easy VPN をイネーブルにすると、セキュリティ レベルまたはインターフェイス名を編集できません。

- [Delete] : 選択したインターフェイスを削除します。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。Easy VPN をイネーブルにしている場合、VLAN インターフェイスを削除できません。
- [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
•	•	•	—	—

[Add/Edit Interface] > [General]

[Add/Edit Interface] > [General] タブでは、VLAN インターフェイスを追加または編集できます。

フェールオーバーにインターフェイスを使用する場合は、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。このパラメータを設定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。その他のパラメータは無視されます。

Easy VPN をイネーブルにすると、セキュリティ レベルまたはインターフェイス名を編集できません。インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。

インターフェイスをフェールオーバー リンクまたはステート リンクとして割り当てた後で、そのインターフェイスを [Interfaces] ペインから編集または削除することはできません。ただし、唯一の例外として、物理インターフェイスをステート リンクとして設定している場合は、その速度とデュプレックスを設定できます。

フィールド

- [Switch Ports] : スイッチ ポートを VLAN インターフェイスに割り当てます。
  - [Available Switch Ports] : 他のインターフェイスに現在割り当てられている場合でも、すべてのスイッチ ポートを一覧表示します。
  - [Selected Switch Ports] : このインターフェイスに割り当てられているスイッチ ポートを一覧表示します。
  - [Add] : 選択したスイッチ ポートをインターフェイスに追加します。次のメッセージが表示されます。

    「*switchport* is associated with *name* interface.Adding it to this interface, will remove it from *name* interface.Do you want to continue?」

    [OK] をクリックして、スイッチ ポートを追加します。

スイッチ ポートをインターフェイスに追加する場合、このメッセージは常に表示されます。コンフィギュレーションがない場合でも、スイッチ ポートは VLAN 1 インターフェイスにデフォルトで割り当てられています。

  - [Remove] : インターフェイスからスイッチ ポートを削除します。スイッチ ポートのデフォルト VLAN インターフェイスは VLAN 1 であるため、インターフェイスからスイッチ ポートを削除すると、基本的にそのスイッチ ポートは VLAN 1 に単に再割り当てされます。

- [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。この設定に加えて、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）と名前を事前に設定する必要があります。
- [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。プライマリまたはバックアップ ISP インターフェイスは管理専用に設定できません。
- [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。
- [IP Address] : ルーテッド モードの場合のみ、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および比較するため、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 config 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。「PPPoE IP Address and Route Settings」（P.5-19）を参照してください。

- [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。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。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]

[Add/Edit Interface] > [Advanced] タブでは、MTU、VLAN ID、MAC アドレスなどのオプションを設定できます。

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 モードの場合は、コンテキスト設定で MTU を設定します。
- [VLAN ID] : このインターフェイスの VLAN ID を 1 ～ 4090 の範囲で設定します。VLAN ID を割り当てない場合、ASDM により ID がランダムに割り当てられます。
- [Mac Address Cloning] : 手動で MAC アドレスを割り当てます。

  ルーテッド モードではデフォルトで、すべての VLAN が同じ MAC アドレスを使用します。トランスペアレント モードでは、VLAN は固有の MAC アドレスを使用します。スイッチに必要な場合、またはアクセス コントロールの目的で、固有の VLAN を設定したり、生成された VLAN を変更したりすることができます。

  - [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。
- [Block Traffic] : この VLAN インターフェイスから別の VLAN への接続開始を制限します。

  基本ライセンスでは、このオプションを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

  たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネス ネットワークにアクセスする必要がないので、ホーム VLAN で [Restrict Traffic Flow] オプションを使用できます。ビジネス ネットワークはホーム ネットワークにアクセスできますが、その反対はできません。

  2 つの VLAN インターフェイスに名前をすでに設定している場合、必ず [Restrict Traffic Flow] オプションをイネーブルにしてから 3 番目のインターフェイスに名前を付けてください。ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスでは、3 つの VLAN インターフェイスがフル機能を持つことは許可されていません。したがって、インターフェイスを設定できません。

（注）　Security Plus ライセンスにアップグレードすれば、このオプションを削除して、このインターフェイスのフル機能を取得できます。このオプションをイネーブルにしたままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

  - [Block Traffic from this Interface to]：リスト内の VLAN ID を選択します。

- [Select Backup Interface]：このインターフェイスのバックアップ ISP インターフェイスを示します。インターフェイスに障害が発生すると、バックアップ インターフェイスに切り替わります。プライマリ インターフェイスによるデフォルト ルートに障害が発生しない限り、バックアップ インターフェイスはトラフィックを通過させません。このオプションは Easy VPN で便利です。バックアップ インターフェイスがプライマリになると、セキュリティ アプライアンスは新しいプライマリ インターフェイスに VPN ルールを適用します。

  プライマリに障害が発生した場合に、トラフィックがバックアップ インターフェイスを通過できるようにするには、プライマリとバックアップの両方のインターフェイスにデフォルト ルートを設定して、プライマリでの障害発生時にバックアップ インターフェイスを使用できるようにします。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。デュアル ISP サポートを設定するには、「スタティック ルート トラッキング」（P.16-44）を参照してください。

  - [Backup Interface]：リスト内の VLAN ID を選択します。

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
•	•	•	—	—

スイッチ ポートの設定

この項では、スイッチ ポートの設定方法について説明します。次の項目を取り上げます。

- 「[Interfaces] > [Switch Ports]」（P.7-12）
- 「Edit Switch Port」（P.7-13）

注意　ASA 5505 適応型セキュリティ アプライアンスは、ネットワーク内のループ検出用のスパニングツリー プロトコルをサポートしていません。したがって、適応型セキュリティ アプライアンスとのすべての接続は、ネットワーク ループ内で終わらないようにする必要があります。

[Interfaces] > [Switch Ports]

[Switch Ports] タブで、スイッチ ポート パラメータを表示します。

フィールド

- [Switch Port]：セキュリティ アプライアンスのスイッチ ポートを一覧表示します。
- [Enabled]：スイッチ ポートがイネーブルかどうか（[Yes] または [No]）を示します。
- [Associated VLANs]：スイッチ ポートが割り当てられている VLAN インターフェイスを一覧表示します。トランク スイッチ ポートは複数の VLAN に割り当てることができます。
- [Associated Interface Names]：VLAN インターフェイス名を一覧表示します。
- [Mode]：モードはアクセスまたはトランクです。アクセス ポートは 1 つの VLAN に割り当てることができます。トランク ポートは、802.1Q タギングを使用して複数の VLAN を伝送できます。トランク モードが使用できるのは Security Plus ライセンスだけです。
- [Protected]：スイッチ ポートが保護されているかどうか（[Yes] または [No]）を示します。このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。
- [Edit]：スイッチ ポートを編集します。

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 Switch Port

[Edit Switch Port] ダイアログボックスでは、モードの設定、VLAN へのスイッチ ポート割り当て、および [Protected] オプションを設定できます。

フィールド

- [Switch Port]：*表示専用*。選択したスイッチ ポート ID を示します。
- [Enable Switch Port]：このスイッチ ポートをイネーブルにします。
- [Mode and VLAN IDs]：モードと割り当てた VLAN を設定します。
  - [Access VLAN ID]：モードをアクセス モードに設定します。このスイッチ ポートを割り当てる VLAN ID を入力します。デフォルトでは、VLAN ID を [Interfaces] > [Interfaces] で設定した VLAN インターフェイス コンフィギュレーションから取得します。VLAN の割り当てはこのダイアログボックスで変更できます。変更を適用する場合、必ず [Interfaces] > [Interfaces] タブを新しい情報で更新してください。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、VLAN を [Interfaces] > [Interfaces] タブから追加

し、スイッチ ポートを [Add/Edit Interface] > [General] タブで指定することをお勧めします。どちらの場合も、VLAN を [Interfaces] > [Interfaces] タブで追加してからスイッチ ポートを割り当てる必要があります。

  - [Trunk VLAN IDs] : モードを、802.1Q タグ付けを使用するトランク モードに設定します。トランク モードが使用できるのは Security Plus ライセンスだけです。このスイッチ ポートに割り当てる VLAN ID をカンマで区切って入力します。トランク ポートでは、タグが付いていないパケットはサポートされません。ネイティブ VLAN サポートはなく、このコマンドで指定されたタグが含まれていないパケットはすべて、適応型セキュリティ アプライアンスによってドロップされます。VLAN を設定済みの場合、変更を適用すると、[Interfaces] > [Interfaces] タブで、各 VLAN に追加されたこのスイッチ ポートを確認できます。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、VLAN を [Interfaces] > [Interfaces] タブから追加し、スイッチ ポートを [Add/Edit Interface] > [General] タブで指定することをお勧めします。どちらの場合も、VLAN を [Interfaces] > [Interfaces] タブで追加してからスイッチ ポートを割り当てる必要があります。

- [Isolated] : このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。
  - [Isolated] : 保護ポートとしてこのスイッチ ポートを設定します。
- [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。[Full]、[Half]、または [Auto] があります。デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 でデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。
- [Speed] : デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 で速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。デフォルトの [Auto] 設定には、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 [Auto] 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
•	•	•	—	—