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 アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定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設定については、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、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。次の事項を取り上げます。

ASA 5505 ポートおよびインターフェイスの概要

ASA 5505 適応型セキュリティ アプライアンスは内蔵スイッチをサポートしています。設定を行う必要のあるポートおよびインターフェイスは、次の 2 種類です。

- 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 8 個のファースト イーサネット スイッチ ポートがあり、これらはハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。これらのポートの 2 つは PoE ポートです。詳細については、P.7-5 の「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 コマンドを設定できます。」を参照してください。このようなインターフェイスは、PC、IP 電話、DSL モデムなどのユーザ機器に直接接続することができます。あるい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、このインターフェイスは、ファイアウォールおよび VPN サービスに適用される設定済みセキュリティ ポリシーを使用して、VLAN ネットワーク相互間のトラフィックをレイヤ 3 で転送します。これらのインターフェイスは、透過モードでファイアウォール サービスに適用される設定済みセキュリティ ポリシーを使用して、同一ネットワーク上の VLAN 相互間のトラフィックをレイヤ 2 で転送します。最大 VLAN インターフェイスの詳細については、「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」の項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、たとえば自宅用 VLAN、仕事用 VLAN、インターネット用 VLAN などに装置を分けることができます。

スイッチ ポートを個別の 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。しかし、VLAN 1 のスイッチ ポートが VLAN 2 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 2 つの VLAN 間のトラフィックとルートまたはブリッジに適用します。

（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利用できません。

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

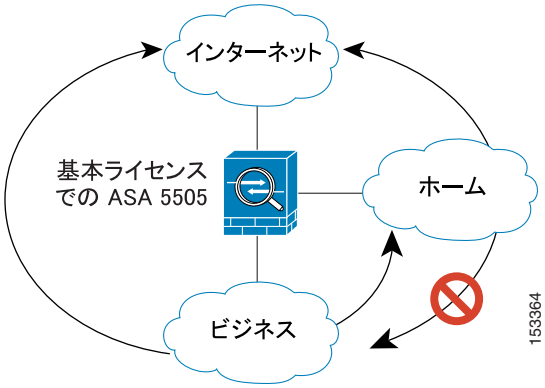
透過ファイアウォール モードでは、基本ライセンスの場合はアクティブ VLAN を 2 つ、Security Plus ライセンスの場合は 3 つ設定できます。そのうちの 1 つは、フェールオーバー用です。

ルーテッド モードでは、基本ライセンスはアクティブ VLAN を最大 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 VLAN とは、**nameif** コマンドが設定された VLAN のことです。

基本ライセンスでは、3 つ目の VLAN は、別の VLAN へのトラフィックを開始する目的でのみ設定できます。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

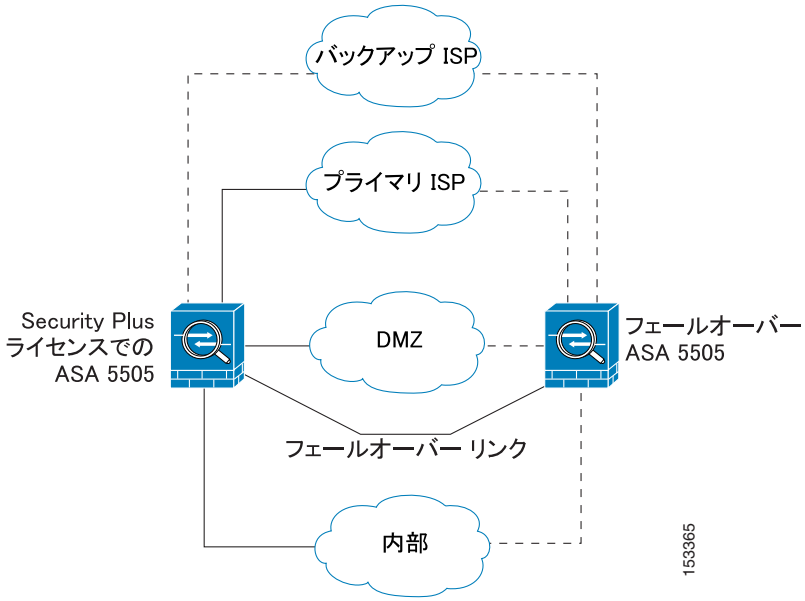


Security Plus ライセンスを利用して、20 までの VLAN インターフェイスを設定できます。トランクポートを設定して、1 つのポートで複数の VLAN を使用できます。

（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



インターフェイスのデフォルト 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 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。

透過ファイアウォール モードでは、各 VLAN に固有の MAC アドレスがあります。手動で MAC アドレスを割り当てる場合、生成された MAC アドレスを上書きできます。

Power Over Ethernet

イーサネット 0/6 およびイーサネット 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り、それらのスイッチ 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。もう一度イネーブルにすると電源が復元されます。

接続されているデバイスの種類（Cisco または IEEE 802.3af）など、PoE スイッチ ポートの状態を確認するには、**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監視

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監視するには、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監視できます。SPAN を使用しないと、監視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 は、1 つの宛先ポートにのみイネーブルにできます。

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（最小～最大）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のレベルには 100 を割り当てる必要があります。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。

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適応型セキュリティ 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、高セキュリティ ホストから低セキュリティ ホストへの接続が確立済みの場合に、低セキュリティ ホストから高セキュリティ 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** コマンドを設定できます。

VLAN インターフェイスの設定

設定できる VLAN の数については、P.7-2 の「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」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 リンクの設定については、第 14 章「高可用性」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。

ここでは、次の項目について説明します。

Interfaces > Interfaces

Interfaces タブで、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できます。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、トラフィックが通過できるインターフェイスは 2 つだけです。

フィールド

- Name：インターフェイスの名前を表示します。
- 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。
- 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。
- Restrict Traffic Flow：このインターフェイスから他の 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を設定する場合、3 番目の VLAN だけを設定できます。

  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 ネットワークに、そして 3 つ目を自宅のネットワークにそれぞれ割り当てます。自宅の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、自宅の VLAN で Restrict Traffic Flow オプションを使用できます。ビジネス ネットワークは自宅の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することができます。このオプションをイネーブルにしておくと、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。インターフェイスがダウンすると、バックアップ インターフェイスに切り替わります。

  バックアップ インターフェイスは、プライマリ インターフェイスのデフォルト ルートがダウンしなければ、トラフィックが通過しません。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。

  プライマリがダウンした場合に、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双方のインターフェイスのデフォルト ルートを設定して、プライマリのダウン時にバックアップ 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、1 つは下位の管理ディスタンスのプライマリ インターフェイスにして、もう 1 つは上位ディスタンスのバックアップ インターフェイス用にします。デュアル ISP サポートを設定するには、P.16-42 の「スタティック ルート トラッキング」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。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：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。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。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：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
•	•	•	—	—

Add/Edit Interface > General

Add/Edit Interface > General タブで、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、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。

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。

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

- Switch Ports：この VLAN インターフェイスにスイッチ ポートを割り当てます。
  - Available Switch Ports : すべてのスイッチ ポートを一覧表示します。他のインターフェイスに割り当てられているものも表示されます。
  - Selected Switch Ports：このインターフェイスに割り当てられたスイッチ 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：スイッチ ポートをインターフェイスから削除します。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 なので、インターフェイスからスイッチ ポートを削除すると、そのスイッチ ポートは VLAN 1 に再度割り当てられます。
- 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。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。
- 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。P.5-19 の「PPPoE IP Address and Route Settings」を参照してください。

- 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		
			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、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。
- 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 によりランダムな値が割り当てられます。
- Mac Address Cloning：MAC アドレスを手動で割り当てます。

  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。透過モードでは、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 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。

- 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を設定する場合、3 番目の VLAN だけを設定できます。

  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 ネットワークに、そして 3 つ目を自宅のネットワークにそれぞれ割り当てます。自宅の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、自宅の VLAN で Restrict Traffic Flow オプションを使用できます。ビジネス ネットワークは自宅の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することができます。このオプションをイネーブルにしておくと、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：VLAN ID をリストから選択します。

- Select 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。インターフェイスがダウンすると、バックアップ インターフェイスに切り替わります。バックアップ インターフェイスは、プライマリ インターフェイスのデフォルト ルートがダウンしなければ、トラフィックが通過しません。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。

  プライマリがダウンした場合に、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双方のインターフェイスのデフォルト ルートを設定して、プライマリのダウン時にバックアップ 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、1 つは下位の管理ディスタンスのプライマリ インターフェイスにして、もう 1 つは上位ディスタンスのバックアップ インターフェイス用にします。デュアル ISP サポートを設定するには、P.16-42 の「スタティック ルート トラッキング」を参照してください。

  - Backup Interface：VLAN ID をリストから選択します。

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
•	•	•	—	—

スイッチ ポートの設定

この項では、フェールオーバーを設定する方法について説明します。次の項目を取り上げます。

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索用のスパニング 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 ポートの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を Yes または No で示します。
- 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 インターフェイスの名前を一覧表示します。
- Mode：モードは Access または Trunk です。Access ポートは 1 つの VLAN に割り当てられます。Trunk ポートは、802.1Q タグ付けを使用して複数の VLAN を処理できます。トランク モードは、Security Plus ライセンスでのみご利用いただけます。
- Protected：スイッチ ポートが保護されているかどうかを Yes または No で示します。このオプションを指定すると、同じ VLAN 上の他のスイッチ ポートと通信できなくなります。スイッチ ポート間で相互通信するのを防ぐのは、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、VLAN 内のアクセスを許可する必要がなく、感染やセキュリティ違反が発生した際に、個々のデバイスを相互に孤立させる場合です。たとえば、3 つの Web サーバをホスティングする DMZ の場合、Protected オプションを各スイッチ ポートに設定すると、Web サーバを相互に孤立させることができます。内部および外部ネットワークは 3 つの Web サーバと通信でき、またその逆も可能ですが、Web サーバどうしが通信することができません。
- 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 Switch Port

Edit Switch Port ダイアログボックスで、モードの設定、VLAN へのスイッチ ポート割り当て、Protected オプションの設定ができます。

フィールド

- Switch Port：表示のみ。選択したスイッチ ポートの 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 access モードに設定します。このスイッチ ポートに割り当てる 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 タブの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 trunk モードに設定します。トランク モードは、Security Plus ライセンスでのみご利用いただけます。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 ポートはタグのないパケットをサポートしていません。ネイティブの VLAN のサポートはなく、このコマンドに特定のタグが指定されていないパケットをすべてドロップします。VLAN を設定済みの場合、変更を適用すると、Interfaces > Interfaces タブでそれぞれの 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：このオプションを指定すると、スイッチ ポートは他の保護されたスイッチ ポートと同じ VLAN 上で通信できなくなります。スイッチ ポート間で相互通信するのを防ぐのは、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、VLAN 内のアクセスを許可する必要がなく、感染やセキュリティ違反が発生した際に、個々のデバイスを相互に孤立させる場合です。たとえば、3 つの Web サーバをホスティングする DMZ の場合、Protected オプションを各スイッチ ポートに設定すると、Web サーバを相互に孤立させることができます。内部および外部ネットワークは 3 つの Web サーバと通信でき、またその逆も可能ですが、Web サーバどうしが通信することができません。
  - Isolated：このスイッチ ポートを保護されたポートに設定します。
- 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 があります。Auto 設定がデフォルトです。PoE ポート イーサネット 0/6 または 0/7 の auto 以外のものに二重通信を設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。
- Speed：Auto 設定がデフォルトです。PoE ポート イーサネット 0/6 または 0/7 の auto 以外のものに速度を設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。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、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 Auto 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
•	•	•	—	—