CHAPTER 3

FWSM で使用するスイッチの設定

この章では、FWSM で使用する Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの設定方法について説明します。また、スイッチの CLI を使用して設定する必要のある機能について説明します。その他の手順は ASDM を使用して完了できます。

この章には、次の項があります。

スイッチの概要

この項では、ASDM がサポートするスイッチについて説明します。次の項目を取り上げます。

ASDM がサポートするスイッチのコンフィギュレーション

ASDM を使用して、次のスイッチの機能を設定できます。

- VLAN にポートを割り当てます。
- 管理ステータス、スピード、PortFast などのポートのパラメータを設定します。
- ポート モードをルーテッドまたはスイッチドに設定します。
- VLAN を設定します。
- SVI を設定します。
- ファイアウォール VLAN グループを設定し、FWSM に割り当てます。

（注）　次の機能は ASDM の Configuration > Switch ペインではサポートされていません。

- トランク ポートのコンフィギュレーション
- シャーシ内アクティブ / アクティブ フェールオーバーの VLAN グループ
- シャーシ内フェールオーバーの VLAN グループ

サポートされているスイッチのハードウェアとソフトウェア

Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに FWSM をインストールできます。両シリーズのコンフィギュレーションは同じで、このガイドでは、どちらも一般的に「スイッチ」と呼んでいます。スイッチとは、スイッチ（スーパーバイザ エンジン）およびルータ（MSFC）のことです。

スイッチは 2 つのソフトウェア モードをサポートしています。

- スイッチ スーパーバイザ エンジンおよび統合された MSFC ルータ上の Cisco IOS ソフトウェア
- スーパーバイザ エンジン上の Catalyst オペレーティング システム ソフトウェアおよび MSFC 上の Cisco IOS ソフトウェア（ASDM がサポートしていない）

FWSM は独自のオペレーティング システムを実行します。

（注）　ASDM は、Catalyst オペレーティング システム ソフトウェアをサポートしていません。したがって、このガイドでも、Cisco IOS ソフトウェアのみを取り扱います。Catalyst オペレーティング システムをはじめとする他のハードウェアおよびソフトウェアの設定については、スイッチの設定に CLI を使用する『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

マルチコンテキスト モードでのスイッチの設定

マルチコンテキスト モードでは、管理コンテキストに接続した場合のみ、ASDM を使用してスイッチを設定できます。管理外コンテキストでは ASDM に接続しても、スイッチのコンフィギュレーションにアクセスできません。

CLI でのモジュール インストレーションの検証

スイッチが FWSM を確認し、オンラインになったことを検証するには、次のコマンドを入力してモジュール情報を表示します。

```
Router> show module [mod-num | all]
```

show module コマンドのサンプル出力は、次のようになります。

```
Router> show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1     2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
  2    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3     2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4     6  Firewall Module                        WS-SVC-FWM-1       SAD062302U4
```

（注）　**show module** コマンドは、FWSM の 6 つのポートを示しています。これらは EtherChannel としてまとめた内部ポートです。詳細については、P.3-16 の「CLI での FWSM の内部インターフェイスのカスタマイズ」を参照してください。

ASDM をサポートするスイッチの設定

スイッチの設定に ASDM を使用する前に、CLI を使用してスイッチに SNMP と SSH を設定する必要があります。スイッチを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを使用して、SNMP コミュニティを設定します。

```
Router(config)# snmp-server community string
```

string の引数が 1 ～ 32 文字の英数字から構成されていて、パスワードのように機能するコミュニティ ストリングは、SNMP へのアクセスを許可します。ブランク スペースはコミュニティ ストリングでは使用できません。@ のシンボルは、コンテキストの情報を区切るために使用します。このコマンドを設定するときには、@ のシンボルを SNMP コミュニティ ストリングの一部として使用しないようにします。

このコマンドの他のオプションの詳細については、Cisco IOS コマンド リファレンスを参照してください。

ステップ 2　SSH をイネーブルにするには、次のコマンドを入力します。

```
Router(config)# hostname hostname
Router(config)# ip domain-name domain-name
Router(config)# crypto key generate rsa usage-keys modulus 1024
Router(config)# line vty line-number [ending-line-number]
Router(config)# transport input ssh
Router(config)# ip ssh time-out 120
```

これらのコマンドの詳細については、Cisco IOS コマンド リファレンスを参照してください。

ステップ 3　ASDM を使用してスイッチに接続する際には、**login local**、**login tacacs**、または **login authentication** コマンドを使用して、ASDM ユーザのユーザ名とパスワードを設定します。ユーザ アカウントの詳細については、Cisco IOS ユーザ マニュアルを参照してください。

スイッチとの接続の確立

ASDM でスイッチに接続する場合は、SNMP と SSH のクレデンシャルを求められます。ASDM を再起動するたびに、クレデンシャルを再入力する必要があります。スイッチの IP アドレスと SSH のユーザ名だけが記憶されます。

スイッチのコンフィギュレーションの前提条件の詳細については、P.3-4 の「ASDM をサポートするスイッチの設定」を参照してください。

スイッチとの接続を確立するには、次の手順を実行します。

ステップ 1　**Configuration** をクリックし、次に **Switch** をクリックします。

Switch Credentials ダイアログボックスが表示されます。

ステップ 2　Sup IP Address フィールドで、スイッチ スーパーバイザ エンジンの管理 IP アドレスを入力します。

ステップ 3　SNMP Credentials > Read Community フィールドで、P.3-4 の「ASDM をサポートするスイッチの設定」で設定した SNMP コミュニティ ストリングを入力します。

ステップ 4　SSH Credentials 領域で、次の値を入力します。

- ユーザ名
- パスワード
- イネーブル パスワード

ステップ 5　**OK** をクリックします。

ASDM は、スイッチに接続されると、スイッチのインターフェイスと VLAN 情報をロードします。

ASDM がスイッチに接続できなかった場合は、Switch ボタンをオフにし、Switch Credentials ダイアログボックスに再アクセスするために **Switch** ボタンを再度クリックします。

（注）　**Refresh** ボタンをクリックすると、ASDM は、まず FWSM のコンフィギュレーションをリフレッシュし、次にスイッチのコンフィギュレーションをリフレッシュします。マルチモードでは、現在選択しているコンフィギュレーション（システムまたはコンテキスト）をリフレッシュし、次にスイッチのコンフィギュレーションをリフレッシュします。スイッチだけの別個の Refresh ボタンはありません。

スイッチ ポートの設定

ASDM を使用して、ポート パラメータの設定および VLAN へのスイッチ ポートの割り当てができます。ここでは、次の項目について説明します。

Interfaces ペインの使用

Configuration > Switch > Interfaces ペインでは、ポート パラメータの設定および VLAN へのスイッチ ポートの割り当てだけでなく、簡単なコンフィギュレーション フローのパラメータも多数設定できます。スイッチのコンフィギュレーションは、Configuration > Switch > Interfaces ペインを使用して行えますが、このタスクは、Vlans and Vlan Groups ペインを使用しても可能です。Configuration > Interfaces and Configuration > Security Contexts ペインを使用すると、FWSM のコンフィギュレーションを行うこともできます。このような重複した機能には、次のようなものがあります。

- VLAN のスイッチ仮想インターフェイス（SVI）としての設定、および IP アドレスとマスク（Vlans ペイン）の割り当て
- VLAN の VLAN グループへの割り当て（Vlan Groups ペイン）
- FWSM のインターフェイス パラメータの設定（Configuration > Interfaces ペイン）

Interfaces ペインには、必要な項目で含まれていないものも多いので、コンフィギュレーションを追加する場合は必ず他のペインを確認してください。たとえば、VLAN groups ペインで VLAN グループを追加できますが、Interfaces ペインではできません。

マルチコンテキスト モードでは、システムにいるか、管理コンテキストにいるか、または別のコンテキストにいるかによって、Interfaces ペインが変わります（Configuration > Switch ペインを使用するには、最初に管理コンテキストに接続する必要があります。接続した後で、システムまたは他のコンテキストに表示を切り替えられます）。

システムでは、すべてのコンテキストの VLAN の割り当てを表示できます。各コンテキスト内で、VLAN が現在のコンテキストに割り当てられているかどうかを確認できます。

（注） 各 FWSM にスイッチを接続している内部 EtherChannel には、それぞれ 6 つのポートがあります。これらは、Interfaces ペインに一覧表示されますが、ASDM でこれらのポートを設定することはできません。

ポート パラメータの設定

ポート パラメータには、スピード、管理ステート（up または down）、PortFast 設定、モード（ルーテッドまたはスイッチポート）が含まれます。

スイッチ ポート パラメータを設定するには、次の手順を実行します。

ステップ 1　Configuration > Switch > Interfaces ペインで、設定するポートをクリックします。

編集するセルをクリックして、テーブルの設定を直接編集するか、**Modify Port(s) Parameters** をクリックします。

ステップ 2　次のパラメータを設定します。

- Speed(Mb/s)：ドロップダウン リストから適切な値を選択します。
- Admin St：ドロップダウン リストから Up または Down を選択します。
- Port Fast：スイッチポート モードで、ボックスをクリックして、ポートの STP PortFast をイネーブルにします。STP PortFast は、リスニング ステートとラーニング ステートをバイパスして、ただちにフォワーディング ステートに入るアクセス ポートとして、Layer 2 LAN ポートを設定します。1 台のワークステーションまたはサーバに接続された Layer 2 アクセス ポートの PortFast を使用して、STP がコンバージするのを待機せずに、これらのデバイスがただちにネットワークに接続するのを許可できます。1 台のワークステーションまたはサーバに接続されたインターフェイスは、ブリッジ プロトコル データ ユニット（BPDU）を受信してはいけません。PortFast の設定時には、ポートはまだスパニング ツリー プロトコルを実行しています。PortFast イネーブルのポートは、必要に応じて（優位の BPDU を受信した場合に起こることがあります）、ただちにブロッキング ステートに移行できます。
- Mode：スイッチポート アクセス モードまたはルーテッド モードにモードを設定します。

（注）　ASDM はポートにルーテッド モードを割り当てますが、VLAN にルーテッド ポートを割り当てられないため、FWSM ではそのポートを使用できません。

ステップ 3　モードをルーテッドに設定する場合、**Switch IP Add** と **Mask** のセルをダブルクリックし、値を入力することによって、スイッチの IP アドレスとマスクを設定できます。

マルチコンテキスト モードでコンテキスト内に IP アドレスを設定した場合、コンフィギュレーションを適用する際に ASDM は、IP アドレスがコンテキスト内のアドレスと重複していないことを確認します。システムに IP アドレスを設定すれば、照合は実行されません。

ステップ 4　**Apply** をクリックして変更を適用するか、スイッチポート モードのポートについて、P.3-7 の「VLAN へのポートの割り当て」を参照して引き続き設定を行います。

VLAN へのポートの割り当て

スイッチポート モードでポートを VLAN に割り当てられます。ポートを VLAN に割り当てるには、次の手順を実行します。

ステップ 1　Configuration > Switch > Interfaces ペインで、同じ VLAN に割り当てる 1 つ以上のポートを（スイッチポート モードで）クリックします。連続していないポートを選択するには、Ctrl キーを押した状態でポートをクリックします。連続しているポートを選択するには、Shift キーを押した状態でポートをクリックします。

（注）　FWSM の内部シャーシ 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通信に予約されている VLAN にスイッチ ポートを割り当てないでください。

ステップ 2　**Assign Port(s) to Vlan** をクリックします。

Assign Ports to Vlan ダイアログボックスが表示されます。

ステップ 3　Vlan# ドロップダウン リストで VLAN ID を選択するか、**Add** をクリックして、新しい VLAN を追加します。

VLAN 追加の詳細については、P.3-9 の「VLAN とスイッチド仮想インターフェイスの設定」を参照してください。

また、ポートを 1 つ選択した場合は、Vlan Id セルをクリックし、ドロップダウン リストから VLAN を選択して、テーブルに VLAN を直接設定できます。

ステップ 4　**OK** をクリックします。

ステップ 5　（オプション）既存の VLAN グループに VLAN を割り当てるには、次のオプションのいずれかを使用します。

- Assign the VLAN to a VLAN group that is assigned to an FWSM：FWSM に割り当てられた VLAN グループにある VLAN は、*secured VLAN* と呼ばれます。**Secured** をクリックし、次に **VlanGroup** セルをクリックして、ドロップダウン メニューから VLAN グループ ID を選択します。FWSM に割り当てられた VLAN グループだけが一覧表示されます。マルチコンテキスト モードでは、デフォルトで、VLAN が現在のコンテキストに割り当てられます。システムにいる場合は、VLAN はどのコンテキストにも割り当てられません。
- Assign the VLAN to a VLAN group that is not yet assigned to an FWSM：**VlanGroup** セルをクリックし、ドロップダウン メニューから VLAN グループ ID を選択します。**Secured** をクリックしないでください。FWSM に割り当てられていない VLAN グループだけが一覧表示されます。

VLAN グループの追加と設定の詳細については、P.3-13 の「ファイアウォール VLAN グループの設定」を参照してください。

ステップ 6　（オプション）セキュアな VLAN については、テーブルのセルをダブルクリックし、値を入力して、FWSM のインターフェイス名、セキュリティ レベル、IP アドレス、マスクを設定できます（FWSM が透過モードの場合は、インターフェイス名とセキュリティ レベルのみを設定できます）。マルチコンテキスト モードでは、VLAN が現在のコンテキストに割り当てられている場合に、これらのフィールドの編集のみが行えます。システムでは、これらの設定を編集できません。

FWSM のインターフェイス設定の詳細については、第 5 章「インターフェイスの設定」を参照してください。

ステップ 7　（オプション）VLAN の SVI を作成するには、**Switch IP Add** セルと **Mask** セルをダブルクリックし、値を入力することによって、スイッチ IP アドレスとマスクを設定できます。

複数の SVI を追加する場合は、必ず Vlans ペインのこの機能をイネーブルにしてください。SVI の詳細については、P.3-9 の「VLAN とスイッチド仮想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 モードでコンテキスト内に IP アドレスを設定した場合、コンフィギュレーションを適用する際に ASDM は、IP アドレスがコンテキスト内のアドレスと重複していないことを確認します。システムに IP アドレスを設定すれば、照合は実行されません。

ステップ 8　**Apply** をクリックします。

（注） VLAN が Configuration > Switch > Vlans にないのにポートに割り当てる場合は、Vlan Name、Secured、Vlan Group、Switch IPAdd、Mask のオプションは変更できません。

マルチコンテキスト モードで、新しい VLAN をセキュリティ コンテキストに割り当てる場合は、システム コンフィギュレーションをリフレッシュする必要があります。

VLAN とスイッチド仮想インターフェイスの設定

ASDM によって、VLAN をスーパーバイザに追加でき、MSFC のスイッチ仮想インターフェイス（SVI）になる VLAN を設定できます。SVI で使用する VLAN を FWSM に割り当て（P.3-13 の「ファイアウォール VLAN グループの設定」を参照）、次に FWSM と他の Layer 3 VLAN の間の MSFC ルートに割り当てます。

ここでは、次の項目について説明します。

VLAN のガイドライン

FWSM での VLAN 使用については、次のガイドラインを参照してください。

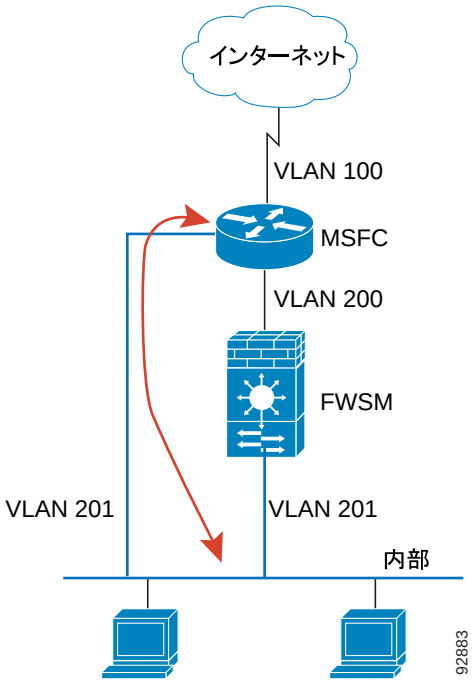
- FWSM ではプライベート VLAN を使用できます。FWSM にプライマリ VLAN を割り当てます。FWSM は、自動的にセカンダリ VLAN トラフィックを処理します。
- 予約済み VLAN を使用することはできません。
- VLAN 1 を使用することはできません。
- 2 ～ 1000 および 1025 ～ 4094 の VLAN ID を使用します。

（注） ルーテッド ポートと WAN ポートは、内部 VLAN を消費するので、1020 ～ 1100 の範囲の VLAN はすでに使用されている可能性があります。

SVI の概要

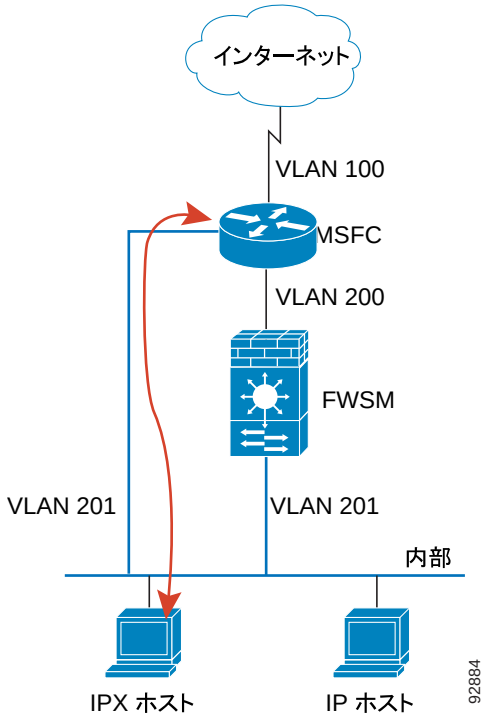
セキュリティ上の理由で、デフォルトでは、1 つの SVI しか MSFC と FWSM の間に存在できません。たとえば、複数の SVI をシステムに誤設定すると、MSFC に内部と外部の VLAN を割り当てることによって、トラフィックが FWSM を通過することを誤って許可してしまうことがあります。図 3-1 を参照してください。

図 3-1　マルチ SVI のミスコンフィギュレーション



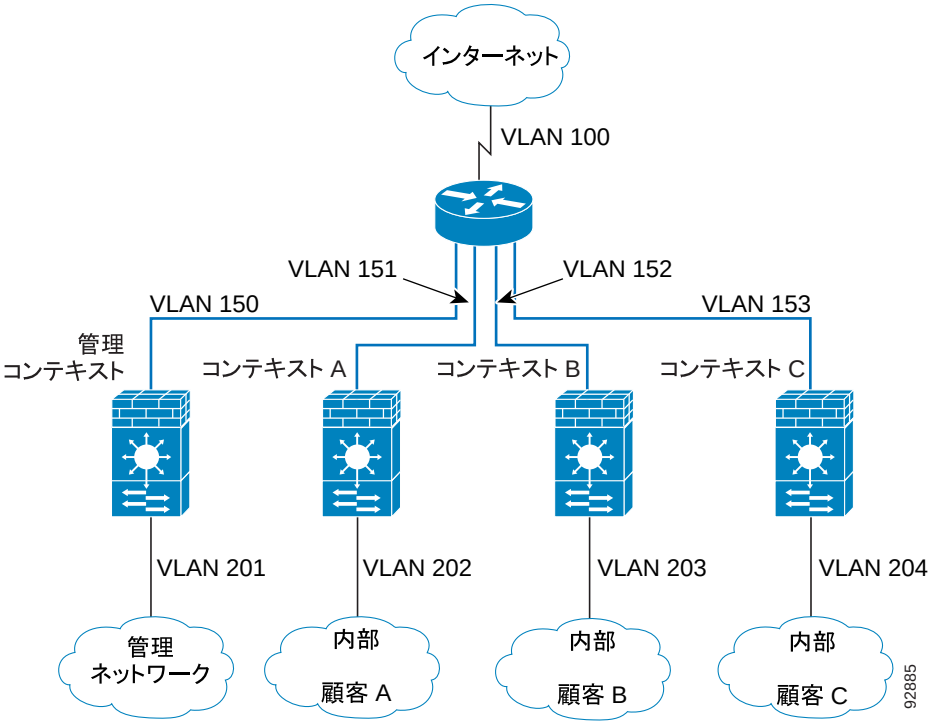
ただし、ネットワーク シナリオによっては、FWSM をバイパスする必要があります。図 3-2 は、IP ホストと同じイーサネット セグメント上の IPX ホストを示しています。FWSM はルーテッド ファイアウォール モードの場合、IP トラフィックのみを処理し、IPX（透過ファイアウォール モードは、オプションで IP 以外のトラフィックを許可します）などの他のプロトコルをドロップするため、IPX トラフィックについては FWSM をバイパスすることもできます。IPX トラフィックのみが VLAN 201 を通過することを許可するアクセスリストを使用して、MSFC を設定してください。

図 3-2　IPX 対応のマルチ SVI



マルチコンテキスト モードの透過ファイアフォールでは、各コンテキストが外部インターフェイスに固有の VLAN を必要とするため、マルチ SVI を使用する必要があります（図 3-3 を参照）。ルーテッド モードでもマルチ SVI を使用できます。その場合、外部インターフェイスで 1 つの VLAN を共有する必要はありません。

図 3-3　マルチコンテキスト モードでのマルチ SVI



VLAN および SVI の設定

VLAN および SVI を設定するには、次の手順を実行します。

ステップ 1　（オプション）Configuration > Switch > Vlans ペインに移動します。

ステップ 2　複数の SVI を FWSM に追加できるようにするには、**Allow to add more than one SVI to FWSM** をクリックします。

ステップ 3　VLAN を追加するには、**Add** をクリックします。

Add Vlan ダイアログボックスが表示されます。

ステップ 4　VLAN を 1 つまたは VLAN の範囲を追加できます。

- VLAN を 1 つ追加するには、**Add single VLAN** をクリックし、次の値を入力します。
  - Vlan Id：VLAN ID を入力します。FWSM で使用できる VLAN の詳細については、P.3-9 の「VLAN のガイドライン」を参照してください。
  - （オプション）Vlan Name：VLAN 名を入力します。デフォルトでは、名前は VLAN *number* です。

－ （オプション）SVI：この VLAN を SVI にする場合は、**SVI** をクリックします。

Switch Interface IP：SVI の IP アドレスを入力します。

Switch Interface Mask：マスクを入力します。

- VLAN の範囲を追加するには、**Add VLAN Range** をクリックし、VLAN ID の範囲をカンマおよびダッシュで区切って入力します。たとえば、2-5,7,10-20 のようになります。

  VLAN の範囲を追加した後で、VLANs テーブルで個別のアトリビュートを設定できます。

ステップ 5　**OK** をクリックします。

VLAN は、Vlans テーブルに追加します。

ステップ 6　（オプション）Vlans テーブルでは、次のインライン編集ができます。

- VLAN 名を変更します。

  スイッチが VTP クライアント モードの場合、VLAN ID が 1 または 1002 ～ 1005 の場合に、VLAN 2 ～ 1001 については、VLAN 名は編集できません。
- **SVI** をオンにして、SVI をイネーブルまたはディセーブルにします。

  マルチ VLAN のこの設定をイネーブルにするには、必ずマルチ SVI をイネーブルにしてください（ステップ 2 を参照）。ただし、マルチ SVI 機能がディセーブルであっても、それらが（FWSM に割り当てられた）セキュアな VLAN でない場合は、マルチ VLAN の SVI ステートをイネーブルにできます。VLAN 1 では SVI ステートは編集できません。
- SVI の IP アドレスとマスクを変更します（SVI がイネーブルの場合）。
- VLAN を VLAN グループに割り当てます。詳細については、次の手順を参照してください。

（注）　Secured and Vlan Groups フィールドは、編集できません。

ステップ 7　VLAN を削除するには、テーブルのその VLAN の行を選択し、**Delete** をクリックします。

このアクションにより、その VLAN に対応する SVI が削除され、VLAN グループに割り当てられている場合は、そのグループからも削除されます。

ステップ 8　**Apply** をクリックします。

（注）　スイッチ上のプライベート VLAN のコンフィギュレーションは、ASDM によってサポートされていません。

ファイアウォール VLAN グループの設定

この項では、VLAN を FWSM に割り当てる方法について説明します。FWSM には、外部の物理インターフェイスはありません。代わりに、VLAN インターフェイスを使用します。FWSM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てに類似しています。FWSM には、スイッチ ファブリック モジュール（存在する場合）または共有バスへの内部インターフェイスがあります。

ここでは、次の項目について説明します。

VLAN グループ ガイドライン

次の VLAN グループのガイドラインを参照してください。

- 最大 16 のファイアウォール VLAN グループを各 FWSM に割り当てられます。たとえば、すべての VLAN を 1 つのグループに割り当てたり、内部グループと外部グループを作成したり、各カスタマーのグループを作成したりすることができます。
- 各グループには、複数の VLAN があります。
- 同じ VLAN を複数の VLAN グループに割り当てることはできません。ただし、複数の VLAN グループを 1 つの FWSM に割り当てたり、1 つの VLAN グループを複数の FWSM に割り当てたりすることができます。たとえば、複数の FWSM に割り当てる VLAN は、各 FWSM に固有の VLAN から別個のグループで存在できます。

（注）　ASDM では、VLAN グループを現在の FWSM とスタンバイ装置にだけ割り当てられます。ただし、同じスイッチ上の異なる FWSM に別の ASDM セッションを開いたり、同じ割り当ての VLAN グループを表示したりすることができるので、FWSM 間で VLAN グループを共有できます。

- シャーシ内のフェールオーバーの場合、ASDM は自動的に同じ VLAN グループをセカンダリ装置に割り当てます。

（注）　VLAN グループを FWSM に割り当てた後でフェールオーバーをイネーブルにすると、ASDM はそのグループをスタンバイ装置に追加しません。同様に、後でフェールオーバーをディセーブルにすると、ASDM は VLAN グループをスタンバイ装置から削除しません。このような変更を行うには、CLI を使用する必要があります。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

- シャーシ内のフェールオーバーの場合は、同じ VLAN をセカンダリ装置に個別に割り当てる必要があります。シャーシ間のトランク ポートの VLAN についても同様です。詳細については、P.3-17 の「フェールオーバー用のスイッチの設定」を参照してください。

VLAN グループの設定および FWSM への割り当て

VLAN グループを作成し、それを FWSM へ割り当てるには、次の手順を実行します。

ステップ 1　Configuration > Switch > Vlan Groups ペインで、VLAN グループを追加または編集するには、**Add** または **Edit** をクリックします。

Add/Edit Firewall Vlan Group ダイアログボックスが表示されます。

ステップ 2　Vlan グループ領域で、Firewall vlan group フィールドに整数で VLAN グループ ID を入力します。

ステップ 3　左のテーブルで 1 つ以上の VLAN ID を選択し、>> ボタンをクリックして、グループに追加します。

VLAN を削除するには、右のテーブルでそれを選択し、<< ボタンをクリックします。

ステップ 4　VLAN グループを現在の FWSM に割り当てるには、**Assign vlan group to current FW module** をクリックします。

マルチコンテキスト モードのデフォルトでは、グループ内の VLAN は現在のコンテキストに割り当てられています。システムにいる場合は、VLAN を割り当てるコンテキストを選択できます（ステップ 6 を参照）。VLAN のコンテキストへの割り当ての詳細については、P.7-20 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。

ステップ 5　シャーシ内のフェールオーバーがイネーブルの場合は、Standby module slot フィールドでスタンバイ装置のモジュール スロット番号を入力します。

同じ VLAN グループを両方のフェールオーバー装置に割り当てる必要があります。モジュール内のフェールオーバーの場合は、VLAN をスタンバイ装置に個別に割り当てる必要があります。FWSM スロットを表示するには、P.3-3 の「CLI でのモジュール インストレーションの検証」を参照してください。

（注）　VLAN グループを FWSM に割り当てた後でフェールオーバーをイネーブルにすると、ASDM はそのグループをスタンバイ装置に追加しません。同様に、後でフェールオーバーをディセーブルにすると、ASDM は VLAN グループをスタンバイ装置から削除しません。このような変更を行うには、CLI を使用する必要があります。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

ステップ 6　（オプション）VLAN グループを現在の FWSM に割り当てると、FWSM のインターフェイスを設定でき、マルチコンテキスト モードでは、コンテキストを設定できます。

インターフェイスの設定の詳細については、第 5 章「インターフェイスの設定」を参照してください。コンテキストへの VLAN の割り当ての詳細については、P.7-20 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。

後で Configuration > Switch > Interfaces テーブルで設定を編集できます。Vlan Groups 領域の設定については、適用後に編集することができません。

a. Firewall Configuration 領域では、FW Interface Name フィールドにインターフェイス名を入力します。

グループに 1 つしか VLAN がない場合、名前はそのままです。ただし、グループに複数の VLAN がある場合は、VLAN ID が名前に付加されます。たとえば、inside という名前を入力すると、グループに VLAN 2、3、4 があれば、その名前は、inside2、inside3、inside4 となります。

b. Security Level フィールドでは、セキュリティ レベルを 0 ～ 100 の間で入力します。

c. FW Interface IP フィールドでは、IP アドレスを入力します。同じ IP アドレスを複数のインターフェイスに割り当てることはできないため、このフィールドは、グループに 1 つしか VLAN がない場合のみ使用できます。システムで、VLAN を 1 つ持つグループがマルチコンテキストに割り当てられていると、マルチコンテキストでは共有 VLAN が同じ IP アドレスを持つことができないため、IP アドレスを割り当てられません。

d. FW Interface Mask フィールドでは、サブネット マスクを入力します。このフィールドは、グループに VLAN が 1 つしかない場合にのみ使用できます。システムで VLAN を 1 つ持つグループがマルチコンテキストに割り当てられていると、マスクを設定できません。

e. マルチコンテキスト モードでは、システムで左のテーブルから 1 つ以上のコンテキスト名を選択し、**>>** ボタンをクリックして、VLAN グループを割り当てるコンテキストを設定します。

新しいコンテキストを追加するには、**Add** をクリックします。コンフィギュレーション ファイルにコンテキスト名と URL を設定する必要があります。

コンテキストを削除するには、右側のテーブルで **<<** ボタンをクリックします。

コンテキスト内にいる場合は、現在のコンテキストが選択され設定はできません。同じ VLAN を別のコンテキストに後で割り当てる場合は、別のコンテキストに移動し、Vlan Groups ペインでグループを編集できます。インターフェイスの設定は、新しい現在のコンテキストに割り当てられます。

マルチコンテキストを選択すると、そのインターフェイスの設定が各コンテキストによって継承されます。

（注） FWSM に割り当てられた VLAN グループに VLAN を追加すると、Firewall Configuration 領域は新しく追加された VLAN にのみ適用されます。

ステップ 7　**OK** をクリックします。

ステップ 8　Vlan Groups ペインで、**Apply** をクリックします。

CLI での FWSM の内部インターフェイスのカスタマイズ

FWSM とスイッチの接続は、6-GB 802.1Q トランキング EtherChannel です。この EtherChannel は、FWSM をインストールしたときに、自動的に作成されます。FWSM 側では、2 つの NP が 3 つのギガビット イーサネットのインターフェイスに個別に接続されており、これらのインターフェイスは、EtherChannel を構成しています。スイッチは、セッション情報に基づいた分散アルゴリズムにしたがって、トラフィックを EtherChannel のインターフェイスに分散します。ロード シェアリングは、パケットごとではなく、フローごとに実行されます。場合によっては、アルゴリズムはトラフィックをインターフェイス間、さらに 2 つの NP 間に不規則に割り当てます。FWSM の潜在的処理能力を十分に活用しないだけでなく、リソースの管理をマルチコンテキストに適用したときに、一貫した不均衡が予測外の動作を引き起こす結果になります。

```
Router(config)# port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip |
src-dst-mac | src-dst-port | src-ip | src-mac | src-port}
```

デフォルトは、**src-dst-ip** です。

フェールオーバー用のスイッチの設定

フェールオーバー用にスイッチを設定するには、次の項目を参照してください。

プライマリ スイッチとセカンダリ スイッチ間へのトランクの追加

スイッチ内のフェールオーバーを使用する場合、2 つのスイッチ間に 802.1Q VLAN トランクを設定して、フェールオーバー リンクおよびステート リンクを伝送する必要があります。トランクでは、QoS がイネーブルになっている必要があります。トランクで QoS がイネーブルになっていると、CoS 値が 5（優先順位がより高い）のフェールオーバーの VLAN パケットがこれらのポートでより高い優先順位で処理されます。

EtherChannel およびトランクを設定するには、スイッチのマニュアルを参照してください。

透過ファイアウォール モードとの互換性の確認

透過モードでフェールオーバーを使用するときにループを回避するには、BPDU の転送をサポートするスイッチ ソフトウェアを使用します。透過ファイアウォール モードのスイッチのサポートの詳細については、P.A-2 の「スイッチのハードウェアおよびソフトウェアの互換性」を参照してください。

FWSM が透過モードの場合は、スイッチの LoopGuard をグローバルにイネーブルにしないでください。LoopGuard は自動的にスイッチと FWSM 間の内部 EtherChannel に適用されます。そのため、フェールオーバーやフォールバックの後で、EtherChannel が err-disable 状態になり、LoopGuard によってセカンダリ装置が切断されます。

迅速なリンク障害検出用自動ステートメッセージのイネーブル化

Catalyst オペレーティング システムのソフトウェア リリース 8.4（1）以降、または Cisco IOS ソフトウェア リリース 12.2（18）SXF5 以降を使用して、スーパーバイザ エンジンは、FWSM の VLAN に関連付けられた物理インターフェイスの状態について、自動ステート メッセージを FWSM に送信できます。たとえば、VLAN に関連付けられたすべての物理インターフェイスがダウンしたとき、自動ステート メッセージが FWSM に VLAN がダウンしたことを伝えます。この情報に基づき、通常はどちら側がリンク障害を起こしたかを判断するのに必要なインターフェイスのモニタリング テストをバイパスすることによって、FWSM が VLAN のダウンを宣言します。自動ステート メッセージは、FWSM がリンク障害を検出する時間を大幅に短縮します（自動ステートのサポートがない場合の最長 45 秒に対し、数ミリ秒）。

スイッチ スーパーバイザは、次の場合に、自動ステート メッセージを FWSM に送信します。

- VLAN に属している最後のインターフェイスがダウンした場合。
- VLAN に属している最初のインターフェイスが復旧した場合。

（注）　シャーシに FWSM を 1 つインストールした場合のみ、スイッチは自動ステート メッセージをサポートします。

Cisco IOS ソフトウェアでは、自動ステート メッセージは、デフォルトでディセーブルになっています。Cisco IOS ソフトウェアで、自動ステート メッセージをイネーブルにするには、次のコマンドを入力します。

```
Router(config)# firewall autostate
```

Catalyst オペレーティング システム ソフトウェアは、自動ステート メッセージがデフォルトでイネーブルになっており、設定はできません。ただし、Catalyst オペレーティング システムの自動ステートは、SVI でのみ使用できます。この機能を利用する場合は、すべての VLAN に「ダミー」の SVI を作成できますが、これらの SVI に IP アドレスは設定しないでください。たとえば、次のコンフィギュレーションによって、マルチ SVI をイネーブルにし、VLAN 55 および 56 の SVI を作成しますが、これらの SVI に IP アドレスは割り当てません。

```
Console> (enable) set vlan 55-56 firewall-vlan 8
Console> (enable) set firewall multiple-vlan-interfaces enable
Console> (enable) switch console
Router> enable
Password: ******
Router# configure terminal
Router(config)# interface vlan 55
Router(config-if)# interface vlan 56
Router(config-if)# end
Router# ^C^C^C
Console> (enable)
```

CLI での Firewall Services Module のブート パーティションの管理

この項では、スイッチから FWSM をリセットする方法とフラッシュ メモリ カードのブート パーティションを管理する方法について説明します。次の事項を取り上げます。

フラッシュ メモリの概要

FWSM は、オペレーティング システム、コンフィギュレーション、その他のデータを保存する 128 MB のフラッシュ メモリ カードを搭載しています。フラッシュ メモリには、6 つのパーティションがあり、Cisco IOS および Catalyst オペレーティング システム ソフトウェア コマンドの **cf:***n* と呼ばれます。

- Maintenance partition（**cf:1**）：メンテナンス ソフトウェアが含まれています。メンテナンス ソフトウェアを使用して、アプリケーション イメージをアップグレードまたはインストールしたり、アプリケーション パーティションをブートできない場合は、アプリケーション イメージのパスワードをリセットするか、クラッシュ ダンプ情報を表示したりします。
- Network configuration partition（**cf:2**）：メンテナンス ソフトウェアのネットワーク コンフィギュレーションが含まれています。FWSM が TFTP サーバに到達して、アプリケーション ソフトウェア イメージをダウンロードできるようにするためには、メンテナンス ソフトウェアに IP 設定が必要です。
- Crash dump partition（**cf:3**）：クラッシュ ダンプ情報を保存します。
- Application partitions（**cf:4** および **cf:5**）：アプリケーション ソフトウェア イメージ、システム コンフィギュレーション、ASDM を保存します。デフォルトで、**cf:4** のイメージがインストールされています。テスト パーティションとして **cf:5** を使用できます。たとえば、ソフトウェアをアップグレードする場合、新しいソフトウェアを **cf:5** にインストールし、問題が起きた場合のバックアップとして古いソフトウェアを保存しておくことができます。各パーティションには、独自のスタートアップ コンフィギュレーションが含まれています。
- Security context partition（**cf:6**）：このパーティションは、64 MB で、ナビゲート可能なファイル システムにセキュリティ コンテキスト コンフィギュレーション（必要に応じて）と RSA キーを保存します。その他のパーティションには、ファイルのリストなどの共通のタスクを実行できるファイル システムがありません。このパーティションは、**copy** コマンドを使用するときに **disk** と呼ばれます。

デフォルトのブート パーティションの設定

デフォルトで、FWSM は、**cf:4** アプリケーション パーティションからブートします。ただし、**cf:5** アプリケーション パーティションからブートするか、**cf:1** メンテナンス パーティションにブートするか選択できます。各アプリケーション パーティションは、独自のスタートアップ コンフィギュレーションを持ちます。

デフォルトのブート パーティションを変更するには、次のコマンドを入力します。

```
Router(config)# boot device module mod_num cf:n
```

n は、1（メンテナンス）、4（アプリケーション）、5（アプリケーション）です。

現在のブート パーティションを表示するには、次のコマンドを入力します。

```
Router# show boot device [mod_num]
```

次の例を参考にしてください。

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

FWSM のリセットまたは特定のパーティションからのブート

この項では、FWSM をリセットまたは特定のパーティションからブートする方法について説明します。CLI または外部 Telnet セッションを通じて到達できない場合は、FWSM をリセットする必要がある場合があります。メンテナンス パーティションにアクセスする必要のある場合、または、バックアップ アプリケーション パーティションの別のソフトウェア イメージからブートする場合は、デフォルトでないブート パーティションからブートする必要がある場合があります。メンテナンス パーティションは、トラブルシューティングに役立ちます。

リセットのプロセスは、数分かかる場合があります。

FWSM をリセットすると、フルメモリ テストの実行も選択できます。FWSM を最初にブートしたときには、部分的なメモリ テストのみが実行されます。フルメモリ テストには、約 6 分かかります。

（注）　FWSM にログインした時に FWSM をリロードするには、**reload** または **reboot** と入力します。これらのコマンドによってデフォルトでないブート パーティションからブートすることはできません。

FWSM をリセットするには、次のコマンドを入力します。

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

cf:*n* の引数は、1（メンテナンス）、4（アプリケーション）、5（アプリケーション）です。パーティションを指定しない場合は、デフォルトのパーティションが使用されます（通常は **cf:4**）。

mem-test-full オプションは、フルメモリ テストを実行します。このテストは、約 6 分かかります。

この例は、スロット 9 にインストールされた FWSM のリセットの方法を示しています。デフォルトのブート パーティションを使用します。

```
Router# hw-module module 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```