FWSM について

Firewall Services Module（FWSM）は、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載する、高性能でコンパクトなステートフル ファイアウォール モジュールです。

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。ファイアウォールを使用すると、たとえば、人事ネットワークとユーザ ネットワークを切り離しておくなどといった形で、内部ネットワーク相互間の保護も実現できます。Web、FTP サーバなど、外部ユーザが利用できるようにしなければならないネットワーク リソースがある場合は、ファイアウォールの背後の *Demilitarized Zone*（DMZ; 非武装地帯）と呼ばれる独立したネットワークに配置できます。ファイアウォールは DMZ への限定的なアクセスを認めますが、DMZ にあるのはパブリック サーバだけなので、攻撃を受けても影響を受けるのはサーバだけであり、他の内部ネットワークに影響はありません。認証または許可を要求したり、外部の URL フィルタリング サーバと連動させたりして、特定のアドレスだけを許可することによって、内部ユーザから外部ネットワークへのアクセス（インターネット アクセスなど）も制御できます。

FWSM にはマルチセキュリティ コンテキスト（仮想ファイアウォールに類似）、透過（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール動作、何百ものインターフェイス、およびその他の最先端の機能が多数組み込まれています。

ファイアウォールに接続されたネットワークについて述べる場合、*外部*ネットワークはファイアウォールの向こう側にあり、*内部*ネットワークはファイアウォールの手前にあって保護されています。*DMZ* はファイアウォールの手前にありますが、外部ユーザから一定のアクセスが可能です。FWSM では、多数の内部インターフェイス、多数の DMZ、さらに必要に応じて多数の外部インターフェイスを含め、多数のインターフェイスにさまざまなセキュリティ ポリシーを設定するので、このような用語はあくまでも一般的な用語として使用されます。

この章で説明する内容は、次のとおりです。

セキュリティ ポリシーの概要

セキュリティ ポリシーによって、ファイアウォールを通過して別のネットワークにアクセスさせるトラフィックを決定します。FWSM はアクセス リストで明示的に許可されていないかぎり、どのようなトラフィックも通過させません。トラフィックに、セキュリティ ポリシーをカスタマイズする処理を適用できます。ここでは、次の内容について説明します。

アクセス リストでのトラフィックの許可または拒否

アクセス リストを適用して、トラフィックにインターフェイスの通過を許可できます。透過ファイアウォール モードの場合、EtherType アクセス リストを適用して、IP 以外のトラフィックを通過させることもできます。

NAT の適用

NAT の利点の一部は、次のとおりです。

- 内部ネットワーク上でプライベート アドレスを使用できます。プライベート アドレスはインターネット上でルーティングできません。
- NAT は他のネットワークに対してローカル アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- NAT は IP アドレスのオーバーラップをサポートすることによって、IP ルーティングに伴う問題を解決します。

通過トラフィックに対する AAA の使用

HTTP など特定タイプのトラフィックに、認証または許可あるいはその両方を要求できます。FWSM は RADIUS または TACACS+ サーバにもアカウンティング情報を送信します。

インターネット フィルタリングの適用

アクセス リストを使用すれば特定の Web サイトまたは FTP サーバへの発信アクセスを阻止できますが、インターネットの規模およびダイナミック特性を考慮すると、この方法での Web 使用の設定および管理は実質的ではありません。FWSM と、次のインターネット フィルタリング製品の 1 つを実行する別途サーバを併用することを推奨します。

- Websense Enterprise
- Sentian（N2H2）

アプリケーション検査の適用

ユーザ データ パケットに IP アドレス情報が組み込まれているサービス、またはダイナミックに割り当てられるポート上でセカンダリ チャネルを開始するサービスには、インスペクション エンジンが必要です。これらのプロトコルは、ディープ パケット インスペクションを実行するために FWSM が必要です。

接続制限の適用

TCP/UDP 接続および初期接続を制限できます。接続数および初期接続数を制限することで、DoS 攻撃からシステムを保護できます。FWSM は初期制限によって TCP 代行受信をトリガーします。TCP 代行受信は、TCP SYN パケットでインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。

スイッチにおける Firewall Services Module の動作

FWSM は、Cisco 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載できます。どちらのシリーズも、次の点の除いて構成は同じです。

- Catalyst 6500 シリーズ スイッチは、2 種類のソフトウェア モードをサポートします。
  - スイッチのスーパバイザおよび内蔵 Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の両方で、Cisco IOS ソフトウェア（「スーパバイザ IOS」）を使用
  - スーパバイザ上で Catalyst Operating System（OS; オペレーティング システム）、MSFC 上で Cisco IOS ソフトウェアを使用

  スイッチ本体で実行するコマンドと設定は、両方のモードについて説明します。
- Cisco 7600 シリーズ ルータがサポートするのは、Cisco IOS ソフトウェアだけです。

このマニュアルでは両方のシリーズの総称として、「スイッチ」を使用します。

FWSM は独自の OS で動作します。

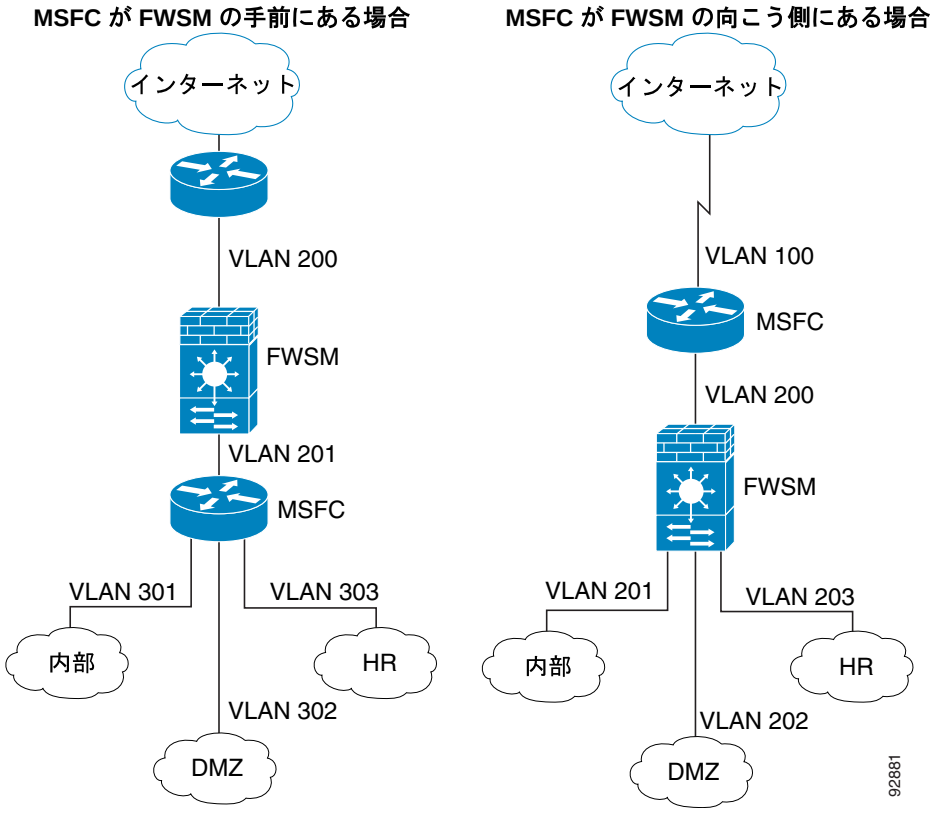
MSFC の使用方法

スイッチにはスイッチング プロセッサ（スーパバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用する場合は、1 つまたは複数の VLAN インターフェイスを MSFC に割り当てることができます（スイッチのソフトウェア バージョンが複数の Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）をサポートする場合は、表 A-1 [p.A-2] を参照）。シングルコンテキスト モードでは、ファイアウォールの向こう側に MSFC を配置することも、ファイアウォールより手前に配置することもできます（図 1-1 を参照）。

MSFC の位置は、割り当てる VLAN によって決まります。たとえば、図 1-1 の左側の例では、FWSM の内部インターフェイスに VLAN 201 を割り当てているので、MSFC はファイアウォールより手前になります。図 1-1 の右側の例では、FWSM の外部インターフェイスに VLAN 200 を割り当てているので、MSFC はファイアウォールの向こう側になります。

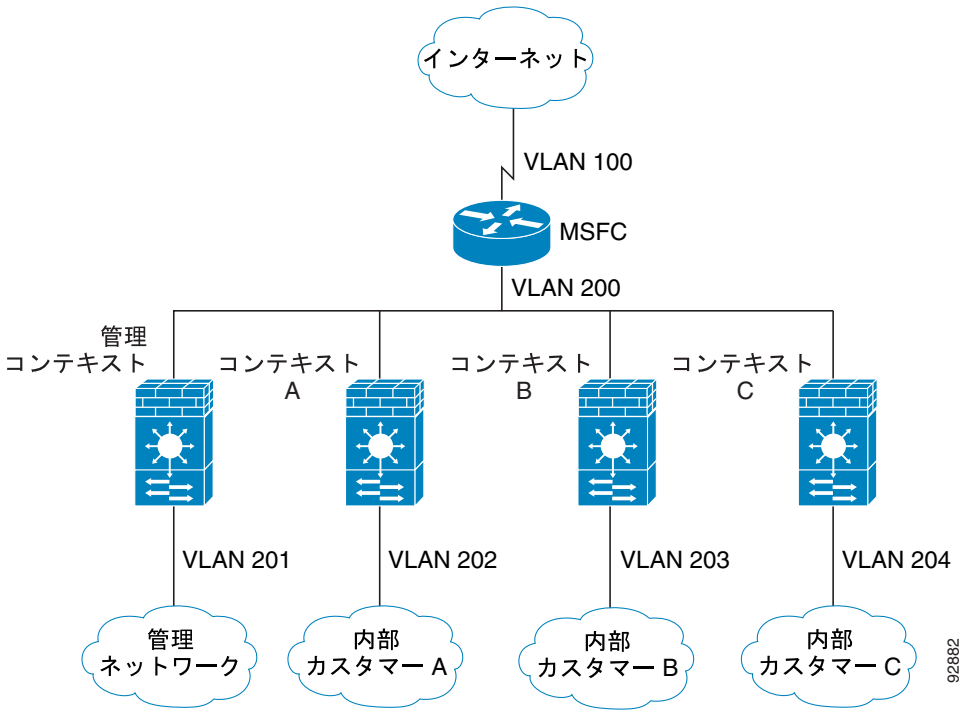
左側の例では、MSFC は VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは FWSM を通過しません。右側の例では、FWSM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC の配置



マルチコンテキスト モードでは、FWSM より手前に MSFC を配置した場合、1 つのコンテキストに限定して接続する必要があります。MSFC を複数のコンテキストに接続すると、MSFC はコンテキスト間をルーティングすることになり、意図に反する可能性があります。マルチコンテキストの場合は通常、あらゆるコンテキストがインターネットとスイッチド ネットワーク間でルーティングされる前に、MSFC を使用します（図 1-2 を参照）。

図 1-2　マルチコンテキストの場合の MSFC の配置



ファイアウォール モードの概要

FWSM は、2 種類のファイアウォール モードで動作可能です。

- ルーテッド
- 透過

ルーテッド モードの場合、FWSM はネットワーク上のルータ ホップとみなされます。

透過モードの場合、FWSM は「ワイヤの凹凸」、すなわち「ステルス ファイアウォール」のように動作し、ルータ ホップにはなりません。FWSM は内部および外部インターフェイスの同一ネットワークに接続します。最大 8 ペアのインターフェイス（ブリッジ グループ）を設定して、コンテキストごとに 8 つの異なるネットワークに接続できます。

ネットワーク構成を簡素化する場合は、透過ファイアウォールを使用します。攻撃側にファイアウォールが見えないようにする場合も、透過モードが便利です。ルーテッド モードでブロックされるトラフィックに透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールはサポート対象外のルーティング プロトコルを許可できます。

マルチコンテキスト モードでは、各コンテキストに対して別個にモードを選択できるため、あるコンテキストを透過モードで実行し、別のコンテキストをルーテッド モードで実行できます。

ステートフル インスペクションの概要

ファイアウォールを通過するあらゆるトラフィックは、Adaptive Security Algorithm（ASA; アダプティブ セキュリティ アルゴリズム）を使用して点検され、通過が許可されるか、または廃棄されるかのどちらかになります。単純なパケット フィルタでも、送信元アドレス、宛先アドレス、およびポートを確認できますが、パケット シーケンスやフラグは確認できません。フィルタの場合はさらに、個々のパケットをフィルタと突き合わせるので、処理が遅くなる可能性があります。

ただし、FWSM などのステートフル ファイアウォールは、次のようにパケットの状態を考慮します。

- 新しい接続かどうか

  新しい接続の場合、ファイアウォールはパケットをアクセス リストと照合し、その他の作業を実行して、パケットを許可するのか拒否するのかを決定する必要があります。この確認を行うために、セッションの最初のパケットは「セッション管理パス」をたどり、さらにトラフィックのタイプによっては、「制御プレーン パス」もたどります。

  セッション管理パスは、次の作業を担当します。

  - アクセス リスト チェックの実行
  - ルート検索の実行
  - NAT 変換（xlate）の割り当て
  - 「高速パス」でのセッション確立

  （パケット ペイロードを点検または変更しなければならない）レイヤ 7 インスペクションが必要なパケットは、さらに制御プレーン パスへ送られます。2 つ以上のチャネルを使用するプロトコルには、レイヤ 7 インスペクション エンジンが必要です。この場合のチャネルとは、well-known ポートの番号を使用するデータ チャネルとセッションごとに異なるポート番号を使用する制御チャネルです。これに該当するプロトコルは、FTP、H.323、および SNMP です。

（注） FWSM は、3 つの特殊なネットワーキング プロセッサ上でセッション管理パスおよび高速パスの処理を実行します。制御プレーン パスの処理は、FWSM へのトラフィックを処理し、設定および管理作業も行う、汎用プロセッサで実行されます。

- 確立された接続かどうか

  接続がすでに確立されている場合、ファイアウォールがパケットを再チェックする必要はありません。一致する大部分のパケットは双方向とも、高速パスを通過します。高速パスは、次の作業を担当します。

  - IP チェックサム検証
  - セッション検査
  - TCP シーケンス番号の検査
  - 既存セッションに基づいた NAT 変換
  - レイヤ 3 およびレイヤ 4 のヘッダー調整

  UDP または他のコネクションレス プロトコルの場合、FWSM は高速パスも使用できるように接続ステート情報を作成します。

  レイヤ 7 のインスペクションを必要とするプロトコルのデータ パケットも、高速パスを通過します。

  確立済みセッション パケットの中には、セッション管理パスまたは制御プレーン パスを通過させなければならないものがあります。セッション管理パスへ送られるパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。制御プレーン パスへ送られるパケットには、レイヤ 7 のインスペクションを必要とするプロトコルの制御パケットが含まれます。

（注）　QoS の互換性を確保するために、FWSM は FWSM を通過するすべてのトラフィックの DSCP ビットを保存します。

セキュリティ コンテキストの概要

1 つの FWSM をセキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストには独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、スタンドアロンのデバイスを複数使用することと同様です。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、管理など数多くの機能がサポートされています。ダイナミック ルーティング プロトコルなど一部の機能はサポートされていません。

マルチコンテキスト モードでは、FWSM にはコンテキストごとに、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほぼすべてのオプションのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーション（シングル モード コンフィギュレーション同様、スタートアップ コンフィギュレーションに相当します）でコンテキストを設定することによって、コンテキストを追加および管理します。システム コンフィギュレーションには FWSM の基本設定が含まれます。システム コンフィギュレーションには、システムそのもののネットワーク インターフェイスまたはネットワーク設定値は含みません。システムがネットワーク リソースにアクセスする必要がある場合に（サーバからコンテキストをダウンロードする場合など）、管理（admin）コンテキストとして指定されたコンテキストの 1 つを使用します。

管理コンテキストは、ユーザが管理コンテキストにログインすると、システム管理者の権限でシステムとその他のすべてのコンテキストにアクセスできるという点を除き、他のコンテキストとまったく同じです。

（注）　マルチコンテキスト モードがサポートするのは、スタティック ルーティングだけです。