CHAPTER 1

FWSM について

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 サーバまたは FTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（*非武装地帯*（DMZ）と呼ばれる）上に配置します。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。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

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）、トランスペアレント（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ているネットワークに言及する場合、*外部*ネットワークはファイアウォールの手前にあるネットワーク、*内部*ネットワークはファイアウォールの背後にある保護されているネットワーク、*DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。FWSM を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

この章では、次の内容について説明します。

新機能

表 1-1 Ç… FWSM Version 4.1(1) ÇÃêVã@î\Çšé¶ÇµÇ‹Ç²ÅB

表 1-1　FWSM Version 4.1(1) ÇÃêVã@î

ã@î\	ê‡ñæ
ÉvÉâÉbÉgÉtÉHÅ[ÉÄã@î	
ÉvÉâÉCÉ}ÉäÇ®ÇÊÇ—ÉZÉJÉìÉ_Éä ÉuÉåÅ[ÉhÇÃå¬ïþÇÃÉzÉXÉgñºÇÃégóp	ÉvÉâÉCÉ}ÉäÇ®ÇÊÇ—ÉZÉJÉìÉ_Éä FWSM Ç…å¬ïþÇÃÉzÉXÉgñºÇšê›íËÇŠÇÍÇ»Ç¢èÍçáÅAÉvÉâÉCÉ}ÉäÇ®ÇÊÇ—ÉZÉJÉìÉ_Éä ÉzÉXÉgñºÇ™ê›íËÇŠÇÍÇ»Ç¢èÍçáÅAÉvÉâÉCÉ}ÉäÇ®ÇÊÇ—ÉZÉJÉìÉ_Éä ÉzÉXÉgñºÇÕìØÇ¹Ç…Ç»ÇËÇ‹Ç²ÅB ïœçXÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**hostname** *primary_hostname* [**secondary** *secondary_hostname*]
ÉtÉ@ÉCÉAÉEÉHÅ[Éãã@î	
ÉAÉNÉZÉâÉåÅ[ÉVÉáÉì ÉpÉXÇ…ñ¢âšàà ARP Çšä‹Çfi UDP ÉZÉbÉVÉáÉìÇÃçÏê¨	ARP ÉãÉbÉNÉAÉbÉvÇ™é³îsÇµÇ¾èÍçáÇÝÇ‡ÉAÉNÉZÉâÉåÅ[ÉVÉáÉì ÉpÉXÇ™çÏê¨ÇŠÇÍÇÈÇÊÇ§Ç… FWSM Çšê›íËÇµÇ¾èÍçáÅAARP ÉãÉbÉNÉAÉbÉvÇ™ê¨å˜Ç²ÇÈÇ‹ÇÝÅAà¹êÊ IP ÉAÉhÉåÉXÇ÷ÇÃà»ç~ÇÃÇ²ÇÞÇƒÇÃÉpÉPÉbÉgÇ™ÉhÉçÉbÉvÇŠÇÍÇ‹Ç²ÅBÇ±ÇÃã@î\ÇšégópÇµÇ»Ç¢èÍçáÅAà»ç~ÇÃäe UDP ÉpÉPÉbÉgÇÕÅAÉAÉNÉZÉâÉåÅ[ÉVÉáÉì ÉpÉXÇ…ÇÊÇËÉhÉçÉbÉvÇŠÇÍÇÈëOÇ…ÉZÉbÉVÉáÉìä«óùÉpÉXÇšíþâflÇ²ÇÈÇ¾ÇflÅAÉZÉbÉVÉáÉìä«óùÉpÉXÇÃÉIÅ[ÉoÅ[ÉçÅ[ÉhÇ™î¦ê¹Ç²ÇÈÇ±ÇýÇ™Ç†ÇËÇ‹Ç²ÅB í«â¡ÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**sysopt connection udp create-arp-unresolved-conn**
DCERPC ägí£ã@î\ÅFRemote Create Instance ÉÅÉbÉZÅ[ÉWÇÃÉTÉ|Å[Ég	ñ{ÉäÉäÅ[ÉXÇÝÇÕÅADCERPC Inspection Ç™ägí£ÇŠÇÍÅARemoteCreateInstance RPC ÉÅÉbÉZÅ[ÉWÇÅüç³Ç™ÉTÉ|Å[ÉgÇŠÇÍÇÈÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅB ïœçXÇŠÇÍÇ¾ÉRÉ}ÉìÉhÇÕ†ÇËÇ‹Ç¼ÇÒÅB
NAT/PAT Global Pool ÇÃégópÇ…ä÷Ç²ÇÈägí£ã@î\	NAT/PAT ÉRÉìÉtÉBÉMÉÖÉåÅ[ÉVÉáÉìÇÃÉOÉçÅ[ÉoÉã ÉvÅ[ÉãÇÃégópÇší«ê’Ç®ÇÊÇ—ä«óùÇÝÇ´Ç‹Ç²ÅB í«â¡ÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**show global usage**
çÌèúÉ}Å[ÉNÇÃïtÇ¢Ç¾ê⁄ë±ÇÃÉäÉZÉbÉg	çÌèúÉ}Å[ÉNÇÃïtÇ¢Ç¾ê⁄ë±ÇÃÉäÉZÉbÉgÅiRSTÅjÉpÉPÉbÉgÇÃëóêMÇšñŠå¯Ç…ÇÝÇ´ÇÈÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅBñ{ÉäÉäÅ[ÉXÇ©ÇÁÅAÉäÉZÉbÉg ÉpÉPÉbÉgÇÕÉfÉtÉHÉãÉgÇÝëóêMÇŠÇÍÇ»Ç¢ÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅBíºëOÇÃìÆçÏÇšïúåŠÇÝÇ´ÇÈÇÃÇÝÅAFWSM Ç…ÇÊÇËÅAçÌèúÉ}Å[ÉNÇÃïtÇ¢Ç¾ìØÇ¹ 5 É^ÉvÉãÅiëóêMåŠ IP Ç®ÇÊÇ—É|Å[ÉgÅAà¹êÊ IP Ç®ÇÊÇ—É|Å[ÉgÅAÉvÉçÉgÉRÉãÅjÇÝ SYN ÉpÉPÉbÉgÇ™éÛêMÇŠÇÍÇÈÇýÅAÉäÉZÉbÉg ÉpÉPÉbÉgÇ™ëóêMÇŠÇÍÇ‹Ç²ÅB í«â¡ÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**service reset connection marked-for-deletion**

表 1-1　FWSM Version 4.1(1) ÇÃêVã@î\ （続き）

ã@î\	ê‡ñæ
PPTP-GRE ÇÃÉ^ÉCÉÄÉAÉEÉg	PPTP åüç³ÇÃåãâþÇýÇµÇƒç\ízÇŠÇÍÇÈ GRE ê⁄ë±ÇÃÉ^ÉCÉÄÉAÉEÉgÇšê›íËÇÝÇ´ÇÈÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅB ïœçXÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**timeout pptp-gre**
ä«óùã@î	
Syslog ÉÅÉbÉZÅ[ÉWÇÃñºëO ÇÃï\é¶Ç‹Ç¾ÇÕîÒï\é¶	syslog ÇšÉRÉìÉ\Å[ÉãÅAsyslog ÉTÅ[ÉoÇ®ÇÊÇ— FTP syslog ÉTÅ[ÉoÇ…ê¹ê¨Ç²ÇÈÇýÇ´Ç…ñºëOïœä²ÇšìKópÇÝÇ´ÇÈÇ©Ç«Ç§Ç©Çšê›íËÇÝÇ´Ç‹Ç²ÅB í«â¡ÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**logging names**
ÉgÉâÉìÉXÉyÉAÉåÉìÉg ÉÇÅ[ÉhÇÝÇÃã§óLä«óùÉCÉiÉ^Å[ÉtÉFÉCÉX	ÉuÉäÉbÉW ÉOÉãÅ[ÉvÇ…ëÆÇŠÇÍÇ»Ç¢ä«óù VLAN Çší«â¡ÇÝÇ´ÇÈÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅBÇ±ÇÃ VLAN ÇÕÅAÉ}ÉãÉ` ÉRÉìÉeÉLÉXÉgÇÝÉVÉìÉOÉãä«óù VLAN Çšã§óLÇÝÇ´ÇÈÇÃÇÝÅAÉ}ÉãÉ` ÉRÉìÉeÉLÉXÉg ÉÇÅ[ÉhÇÝì¡Ç…ñšÇ…óßÇøÇ‹Ç²ÅB ÉgÉâÉìÉXÉyÉAÉåÉìÉg ÉÇÅ[ÉhÇÝí«â¡ÇŠÇÍÇ¾ÉRÉ}ÉìÉhÅF**management-only**
ÉeÉBÉAÉ_ÉEÉì Syslog ÇÃägí£ã@î\	ê⁄ë±Ç™ÉeÉBÉAÉ_ÉEÉìÇŠÇÍÇÈÇýÇ´ÇÃêVÇµÇ¢ syslog Ç™í«â¡ÇŠÇÍÇ‹ÇµÇ¾ÅB í«â¡ÇŠÇÍÇ¾ syslog ÉÅÉbÉZÅ[ÉWÅF302030 Å` 33
SNMP ÉoÉbÉtÉ@ÇÃägí£ã@î\	SNMP óvãÅÇ™ÇÊÇËå¯ó¶ìIÇ…àµÇÌÇÍÇÈÇÊÇ§Ç…Ç»ÇËÇ‹ÇµÇ¾ÅBÇ±ÍÇ…ÇÊÇËÅAëºÇÃÉvÉçÉZÉXÇÝè\ï™Ç»ÉuÉçÉbÉNÇšégópÇÝÇ´ÇÈÇÊÇ§Ç…ÅASNMP Ç…äÑÇËìñÇƒÇÁÍÇÈÉuÉçÉbÉNÇ™Ç²ÇŒÇ,Ç¦âšïŽÇŠÇÍÇ‹Ç²ÅB ïœçXÇŠÇÍÇ¾ÉRÉ}ÉìÉhÇÕÇ†ÇËÇ‹Ç¼ÇÒÅB
ÉgÉâÉuÉãÉVÉÖÅ[ÉeÉBÉìÉOã@î	
crashinfo ÇÃägí£ã@î\	crashinfo ÇÃägí£ã@î\Ç…ÇÊÇËÅAÉNÉâÉbÉVÉÖèÓïÒê¹ê¨ÇÃêMóäê´Ç™â¸ëPÇŠÇÍÇ‹ÇµÇ¾ÅB ïœçXÇŠÇÍÇ¾ÉRÉ}ÉìÉhÇÕÇ†ÇËÇ‹Ç¼ÇÒÅB

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティ ポリシーによって決められます。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。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。ここでは、よく使用される一部の機能について説明します。他の機能については説明を省略しています。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。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

FWSM は IP フラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全リアセンブリ、および FWSM を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

通過トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と認可のいずれかまたは両方を要求することができます。FWSM は、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。

インターネット フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。FWSM を、次のインターネット フィルタリング製品のいずれかを実行している別のサーバと連携させて使用することをお勧めします。

- Websense Enterprise
- Sentian（N2H2）

アプリケーション検査の適用

インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、FWSM でディープ パケット検査を実行する必要があります。

接続制限の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。FWSM では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続は、送信元と宛先間で必要なハンドシェイクを完了しなかった接続要求です。

（注） TCP SYN クッキー保護を使用して SYN 攻撃からサーバを保護する場合、保護するサーバの TCP SYN バックログ キューより低い初期接続制限を設定する必要があります。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバにアクセスできなくなります。

スイッチにおける ファイアウォール サービス モジュール の動作

FWSM は、スイッチのスーパーバイザおよび内蔵 MSFC の両方で Cisco IOS ソフトウェア（「スーパーバイザ IOS」）が使用されている Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載できます。

（注） Catalyst Operating System（OS; オペレーティング システム）はサポートされていません。

FWSM は独自の OS で動作します。

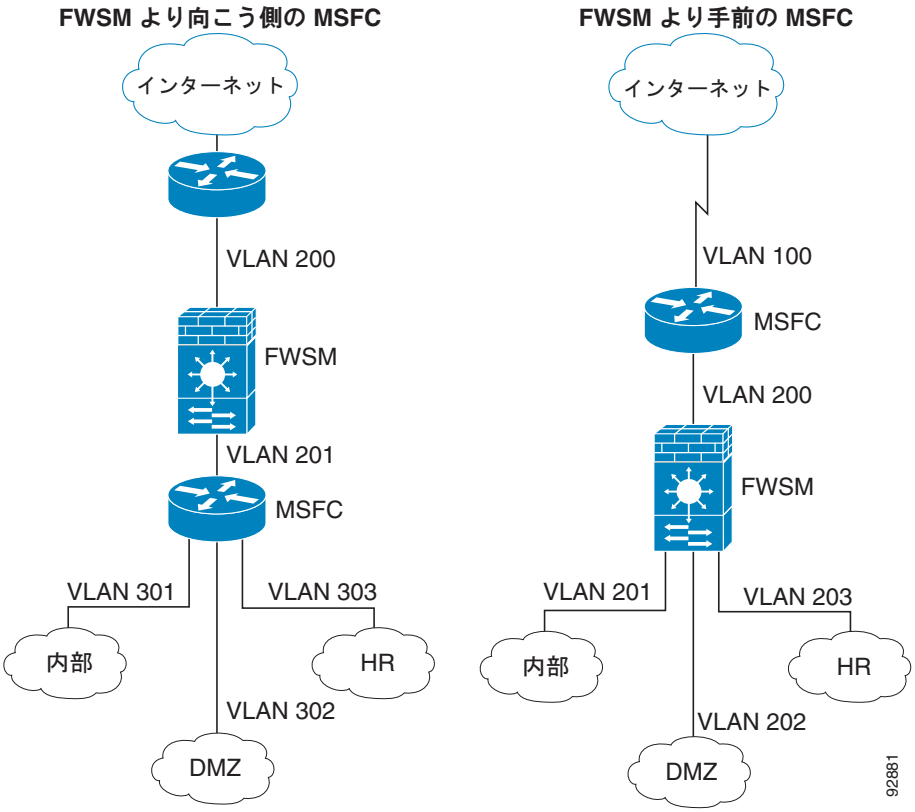
MSFC の使用方法

スイッチにはスイッチング プロセッサ（スーパーバイザ）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 1（P.A-2）を参照してください）。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。

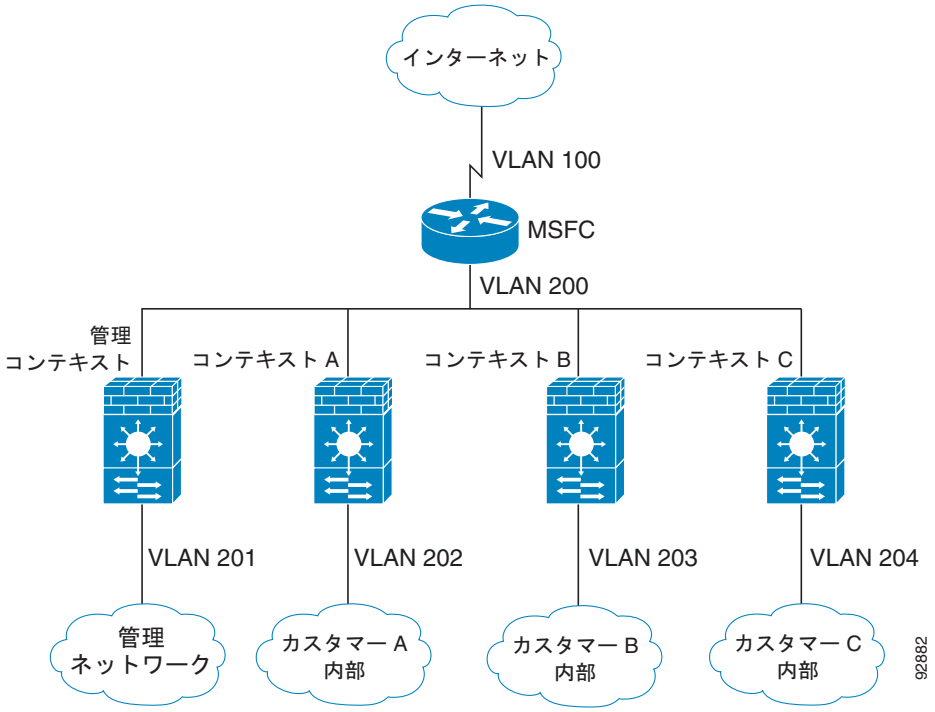
左側の例では、MSFC は VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは FWSM を通過しません。右側の例では、FWSM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

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、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- トランスペアレント

ルーテッド モードでは、FWSM は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、FWSM は「bump-in-the-wire（BITW）」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。FWSM では、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。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。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、ファイアウォールを攻撃者から見えないようにするためにも便利です。ルーテッド モードではブロックされるトラフィックのために、トランスペアレント ファイアウォールを使用することもできます。たとえば、トランスペアレント 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トランスペアレント 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 フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） 「TCP ステート バイパスの設定」（P.21-11）に示す機能では、パケット フローをカスタマイズできます。

ただし、FWSM のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  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。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロール プレーン パス」も通過する場合があります。

  （注） セッションの最初のパケットを構成するパケット フラグメントは、8,500 バイトを超えることはできません。セッションは確立されますが、最初の 8,500 バイトだけが送信されます。このセッションのそれ以降のパケットについては、この制限の影響を受けません。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセス リストとの照合チェック
  - ルート ルックアップの実行
  - NAT 変換（xlates）の割り当て
  - 「アクセラレーション パス」でのセッションの確立

  レイヤ 7 検査が必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、複数のチャネルを持つプロトコルで必要です。複数のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

  （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アクセラレーション パスの処理を実行します。コントロール 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。

- 確立済みの接続かどうか。

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、アクセラレーション パスを通過します。アクセラレーション 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 ルックアップ
- TCP シーケンス番号のチェック
- 既存セッションに基づく NAT 変換
- レイヤ 3 ヘッダー調整およびレイヤ 4 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 はアクセラレーション 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 検査を必要とするプロトコルのデータ パケットも、アクセラレーション 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コントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、検査またはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 検査を必要とするプロトコルのコントロール 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 をいくつかのパーティションに分けて複数の仮想デバイス（セキュリティ コンテキストと呼びます）に配置できます。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、複数のスタンドアロン デバイスを使用することに似ています。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 モードの場合、FWSM には、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とんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、FWSM の基本設定を識別します。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、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

（注） マルチ コンテキスト モードでは、スタティック ルーティングのみをサポートします。