ファイアウォール サービス モジュール（FWSM）の FAQ

目次

概要

このドキュメントには、Catalyst 6500 シリーズ Firewall Services Module（FWSM; ファイアウォール サービス モジュール）に関する Frequently Asked Questions（FAQ）が記載されています。

注: ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

サポートされている機能

Q. FWSM、Intrusion Detection System Module 2（IDSM2）、および VPN Service Module（VPNSM）をサポートするのに必要な最小のコード バージョンは何ですか。

A. 適切なコード バージョンは、6500 または 7600 シャーシのスーパーバイザ モジュールの種類、および稼働するソフトウェアの種類（CatOS（ハイブリッド）または Cisco IOS（ネイティブ））によって異なります。 モジュールと Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の特定のコード バージョンについては、次の表を参照してください。

	Sup1（MSFC を搭載）		Sup2（MSFC を搭載）		Sup720	
モジュール	Cisco IOS	CatOS	Cisco IOS	CatOS	Cisco IOS	CatOS
FWSM	12.1(13)E	7.5(1)	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDS	サポー	7.6(1)	12.1(	7.6(1)	12.2(1	8.2(1)

M2	ト対象外		19)E		4)SX1	
VPN SM	サポート対象外	サポート対象外	12.2(14)SY	サポート対象外	12.2(17a)SX10	サポート対象外 *

* サポートが導入予定になっています。

注: CatOS（ハイブリッド）と Cisco IOS（ネイティブ）の違いについては『Cisco Catalyst 6500 シリーズ スイッチでの Cisco Catalyst と Cisco IOS のオペレーティング システムの比較』を参照してください。

Q. FWSM、Intrusion Detection System Module 2（IDSM2）、および VPN Service Module（VPNSM）を同じシャーシで稼働させられますか。

A. はい。スイッチで、Cisco IOS ソフトウェア リリース 12.2(14)SY（Sup2）または 12.2(17a)SX10（Sup720）の最小バージョンとともに統合 Cisco IOS ソフトウェアが稼働する場合、同じシャーシでこれらのモジュールを実行できます。 現在のところ、同じ 6500 または 7600 シャーシで、これらのサービス モジュールをサポートできる CatOS バージョンはありません。

Q. FWSM の設定オプションと管理オプションには、どのようなものがあるのですか。

A. 設定オプションおよび管理オプションには、次のものがあります。

オプション	バージョン	説明
Management Center for Firewalls	バージョン 1.1.1 以降*	これは複数のファイアウォールを設定および管理するための Web ベースのインターフェイスです。 **注:** オブジェクト グループ化でのサービス グループのサポートは制限されています。 サービス グループは正常に解釈されますが、すぐに（各エントリに）展開されます。 これは、**icmp-type**、**protocol**、および **service** キーワードを伴うコマンドに影響します。 この制限事項は、バージョン 1.3 以前に適用されます。
Monitoring Center for Security	バージョン 1.2 以降*	これは Cisco のセキュリティ デバイスをモニタリングするための Web ベースのインターフェイスです。 ソフトウェアは、柔軟性の高いレポートや警告オプションを使用して、複数の Cisco セキュリティ デバイスからの syslog 管理を中央集中型で行います。
Monitorin	バー	これはネットワーク セキュリティに関係するサービスの状態とパフォーマンスについて、

g Center for Performance	ジョン 2.0 以降*	モニタリングおよびトラブルシューティングを行うための Web ベースのインターフェイスです。 Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) が、プロトコルの基盤として使用されます。
PDM	バージョン 2.1	これは単一のファイアウォールの設定、管理およびモニタリングするための Web ベースのインターフェイスです。 PIX Device Manager (PDM) は PIX ファイアウォールでローカルでインストールする必要があります。
Telnet	N/A	Telnet では、Command-Line Interface (CLI; コマンドライン インターフェイス) によるファイアウォールへのアクセスが提供されます。 **注:** Telnet アクセスを (一般的に Outside インターフェイスとして知られている) 最も低いセキュリティ インターフェイスに許可するには、管理用の IPsec を設定する必要があります。
セキュアシェル (SSH)	N/A	SSH では、セキュアなリモート CLI によるファイアウォールへのアクセスが提供されます。
SNMP	N/A	SNMP では、FWSM のモニタリング方式が提供されます。 **注:** SNMP は FWSM では読み取り専用です。
Syslog	N/A	Syslog では、FWSM のモニタリング方式が提供されます。

* このソフトウェアは、CiscoWorks VPN/Security Management Solution (VMS) バンドルの一部です。 このソフトウェアでは、企業ネットワークへのブラウザ ベースのインターフェイスを通して Cisco のセキュリティ デバイスを管理するための、統合されたアプローチが提供されます。

Q. SVI とは何ですか。 SVI を複数設定できますか。

A. SVI は Switched Virtual Interface (スイッチ仮想インターフェイス) を表しています。 SVI は、スイッチの論理的なレイヤ 3 インターフェイスを表します。 CatOS バージョン 7.6(1) よりも前、および Cisco IOS ソフトウェア リリース 12.2(14)SY よりも前では、ファイアウォール VLAN の一部として許可される SVI は 1 つだけです。 つまり、FWSM と Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチフィーチャ カード) の間に、レイヤ 3 インターフェイスを 1 つだけ設定できます。 SVI を複数設定しようとすると、Command-Line Interface (CLI; コマンドライン インターフェイス) のエラー メッセージが生成されます。

CatOS バージョン 7.6(1) 以降および Cisco IOS ソフトウェア リリース 12.2(14)SY 以降では、FWSM で複数の SVI がサポートされています。 デフォルトでサポートされる SVI は、1 つだけ

です。 スイッチでの複数の SVI サポートを有効にするには、次のコマンドのいずれかを使用してください。

- CatOS では、「set firewall multiple-vlan-interfaces enable 」と入力します。Cisco IOS では、「firewall multiple-vlan-interfaces 」と入力します。

スイッチを FWSM VLAN 用に設定して、SVI が複数あることを示すエラー メッセージを受け取る場合、スイッチや MSFC の設定を調べて、ファイアウォール VLAN の一部としてレイヤ 3 インターフェイス (または VLAN インターフェイス) が 1 つだけ存在することを確認します。

注: SVI は 1 つだけ使用します。 これにより、ポリシー ルーティングを含む複雑な設定を回避できます。

Q. FWSM は SNMPv3 をサポートしますか。

A. いいえ。

Q. FWSM では、VLAN がいくつサポートされますか。

A. FWSM バージョン 1.1 では VLAN が 100 サポートされ、FWSM バージョン 2.1 では VLAN が 250 サポートされます。

Q. FWSM では、access-list compiled コマンドはサポートされていますか。

A. FWSM では CLI での 10 秒間入力がない場合、アクセス リストが自動的にハードウェアにコンパイルされるため、ターボ アクセス リストは不要です。 FWSM バージョン 2.1 では、アクセス リストがコンパイルされる際の指定を可能にする追加機能が提供されます。

Q. FWSM では、IOS Open Shortest Path First (OSPF) の auto-cost reference-bandwidth コマンドはサポートされていますか。

A. いいえ。 FWSM では接続される物理ポートは考慮されません。 OSPF コストは ospf cost コマンドを使用して、各インターフェイスに手動で設定する必要があります。

Q. 同じネットワークに FWSM の 2 つの異なるインターフェイスが接続されているトポロジで、Open Shortest Path First (OSPF) プロトコルを実行できますか。

A. はい。 この機能は、バージョン 2.1 以降でサポートされています。

Q. FWSM では、どのようなルーティング プロトコルがサポートされているのですか。

A. サポートされるルーティング プロトコルは、OSPF (Open Shortest Path First) および Routing Information Protocol (RIP) です。 FWSM の詳細については、『Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール』ページで入手可能なドキュメントを参照してください。

Q. FWSM では、マルチキャスト (インターネット グループ管理プロトコル (IGMP) v2 とスタブ マルチキャスト ルーティング) はサポートされていますか

。

A. はい。 この機能は、FWSM バージョン 2.1 以降でサポートされています。 バージョン 1.1 が稼働している場合、回避策として Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネリングを使用できます。

Q. FWSM では、URL フィルタリングはサポートされていますか。

A. はい。 バージョン 1.1 以降で Websense がサポートされており、バージョン 2.1 では N2H2 のサポートが追加されています。

Q. フラグメント化されたパケットが FWSM で廃棄されるのはなぜですか。

A. デフォルトでは、フラグメント化されたパケットは FWSM を通過できません。 この機能を設定するには、fragment コマンドを使用できます。 この動作は、PIX ファイアウォールの動作とは異なります。 フラグメント化されたパケットを使用する一般的なプロトコルは、Open Shortest Path First（OSPF）および Network File System（NFS; ネットワーク ファイル システム）です。

Q. FWSM では、VPN 接続を終端させられますか。

A. FWSM では、VPN の機能はサポートされていません。 VPN 接続の終端は、スイッチや VPN サービス モジュールが担当します。 トリプル DES ライセンスは、Telnet、Secure Shell（SSH; セキュアシェル）、およびセキュア HTTP（HTTPS）経由で低セキュリティ インターフェイスに接続するなどの、管理目的専用で提供されます。

Q. FWSM では、RADIUS や TACACS+ 用の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）はサポートされていますか。

A. AAA は FWSM を通過するトラフィックと FWSM 管理の両方に対してサポートされています。 詳細については、『ファイアウォール サービス モジュールのドキュメンテーション』を参照してください。

FWSM では、ダウンロード可能なアクセス リストおよび VPN の例外を除いて、PIX ファイアウォールと類似する機能を提供しています。 この点に留意した上で、これらの PIX ファイアウォールのドキュメントを FWSM のコンフィギュレーション用のガイドに使用できます。

- Cisco Secure PIX Firewall（5.2～6.2）で認証と有効化を行う方法
- PIX バージョン 5.2 以降におけるユーザの認証、許可、アカウンティングの実行

Q. FWSM のパスワード回復は、どのように実行するのですか。

A. パスワードの回復についての情報は、次のドキュメントを参照してください。

- バージョン 1.1(1) については、『FWSM コンフィギュレーション ガイド 1.1(1)』の「パスワードの変更と回復」を参照してください。
- バージョン 1.1(2) と 1.1(3) については、『FWSM コンフィギュレーション ガイド 1.1(2)』の「Changing and Recovering Passwords」を参照してください。

Q. FWSM では、ジャンボ フレームはサポートされていますか。

A. はい、FWSM では、ジャンボ フレームをサポートできます。

Q. FWSM は、送信元アドレスをループバック アドレスとして含むパケットを受信したときにどのように応答しますか。

A. パケットを無効として処理し、破棄します。 デフォルトで、FWSM は、ループバック アドレス、ブロードキャスト アドレス、宛先ホスト アドレスなどの無効な送信元アドレスを含むパケットを破棄します。 次のようなログ メッセージが生成されます。

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Q. FWSM では、PVLAN はサポートされていますか。

A. PVLAN は、ソフトウェア バージョン 3.1 よりサポートが開始されます。 3.1 よりも前のソフトウェア バージョンが稼働している場合の唯一可能な回避策は、PVLAN の混合（promiscuous）ポートをクロスケーブルを使用して通常のアクセス ポートに接続し、続いてそのアクセス ポートの VLAN でファイアウォールが適用されるようにします。

Q. FWSM では、アクセス リスト ライン番号はサポートされていますか。

A. この機能は、ソフトウェア バージョン 3.1 以降でのみサポートされています。

Q. FWSM 上でユーザが持てる接続の数を制限できますか。

A. はい、Modular Policy Framework を使用して接続を制限できます。 接続数を制限するには、次の手順を実行します。

1. トラフィックと照合するためにクラス マップを作成します。
2. クラス マップをポリシー マップに配置して、ポリシー マップで制限する接続を使用します。
3. サービス ポリシーを使用してポリシー マップを適用します。

詳細な情報と手順については、『接続の制限およびタイムアウトの設定』を参照してください。

Q. FWSM でのマルチキャストの実装には制限がありますか。

A. はい。 FWSM では、Security Services Module（SSM; セキュリティ サービスモジュール）用に予約済みなので、グループ名としての 232.x.x.x のサブネットはサポートされていません。

Q. FWSM では、ダイレクト ブロードキャストは許可されますか。

A. いいえ。 ルータとは異なり、FWSM ではインターフェイスを介したダイレクト ブロードキャストは許可されません。 類似の回避策は、1 つのインターフェイスから別のインターフェイスへブロードキャストを転送するために、組み込み DHCP リレー機能を使用することです。

Q. HTTP インスペクション エンジンでは、HTTP セッションで非 HTTP トラフィックや標準外トラフィックを検出できますか。

A. はい。 拡張 HTTP インスペクション機能を備えた Application Firewall では、これらのトラフィックを検出して、制御できます。 詳細については、『アプリケーション インスペクション エ

ンジンの概要』を参照してください。

Q. ASA と FWSM のノーマライズ機能には互換性がありますか。

A. FWSM では、TCP のノーマライズは TCP complex (コントロールプレーン) に渡されるトラフィックのみに適用します。 正常なデータ プレーン (高速パス) トラフィックは、影響を受けていません。 これは、ASA トラフィックはすべてノーマライザの対象になるという点で、ASA とは異なります。

FWSM では、ノーマライザが無効になるとモジュールは 2.3 の動作に戻ります。 ところが、**control-point tcp-normalizer** を無効にすると、厳密な TCP チェックが防止され、実行されません。このチェックには、FWSM 内でのレイヤ 7 インスペクションのためにコントロール プレーンで受信される TCP パケット上での、out-of-sequence セグメントの検出や TCP オプションのモニタリングなどが含まれます。 そのため、これを無効にしないことを推奨いたします。 FWSM では、デフォルトの TCP マップ パラメータでのチューニングは許可されていません。

Q. TCP のノーマライザを有効または無効にする必要がありますか。

A. NP からコントロール プレーンに対して接続に固有な情報を送信できないため、FWSM で TCP ノーマライザが常に正常に機能しない可能性があります。 また、接続に関連付けられている一意の TCP マップを識別できません。 そのため、FWSM は、すべての接続で正常に動作するとは限らない可能性があるデフォルトの TCP マップに依存します。 これらの制限により、ファイアウォールを通過するトラフィックに対して、コントロール プレーンで TCP ノーマライザを有効または無効にする必要性があります。 FWSM では、デフォルトの TCP マップ パラメータでのチューニングは許可されていません。

Q. FWSM がサポートできる mfib エントリの最大数はいくつですか。

A. エントリの最大数は、5000 エントリです。

Q. FWSM でパケットをキャプチャするにはどうすればいいですか。

A. FWSM でパケットをキャプチャすることができます。 ASDM では、パケット キャプチャとしての CLI の使用と **capture** コマンドがサポートされません。 詳細については、『無視されるコマンドと表示専用コマンド』を参照してください。 FWSM でのパケット キャプチャの設定方法については、『パケットのキャプチャ』を参照してください。 パケット キャプチャ機能の設定方法の詳細は、『ASA/PIX/FWSM： CLI および ASDM の設定例を使用してキャプチャするパケット』を参照してください。

Q. FWSM をサポートする ASDM のバージョンは何ですか。

A. FWSM リリースと ASDM リリースの互換性の詳細については、『FWSM および ASDM リリースの互換性』を参照してください。

ライセンス

Q. マルチ コンテキスト モードで稼働する FWSM のライセンスがあります。 ハードウェア障害が発生した場合、スペア用の FWSM のライセンスを取得できますか。

A. スペア用の FWSM のライセンスを取得できます。 ただし、通常のライセンスと同様に、スペア用の FWSM ライセンスを注文する必要があります。 ハードウェア障害が発生した場合、Cisco テクニカルサポートに連絡して障害を確認し、スペア用の FWSM のライセンスを取得してください。 ライセンス情報については、『Cisco ファイアウォール モジュール ソフトウェア リリース 2.2(1)』を参照してください。

Q. FWSM では、複数の共有インターフェイスはサポートされていますか。

A. FWSM では複数の共有インターフェイスはサポートされていませんが、代りに複数のコンテキストに渡った 1 つの VLAN を置くことができます。 詳細については、『コンテキスト間でのリソースとインターフェイスの共有』を参照してください。

VLAN の問題

Q. FWSM に、どのように追加 VLAN を配置するのですか。

A. VLAN 200 を設定に追加する場合は、**nameif** コマンドを使用します。 セキュリティ レベルは、0 ~ 100 の範囲にある必要があります。 コマンド構文の全体は、**nameif vlan200 <interface name> <security level>** となります。

Q. シングル コンテキストのルーテッド モードを使用して、FWSM に VLAN をいくつ配置できますか。

A. シングル コンテキストのルーテッド モードを使用して、FWSM に 1000 の VLAN を配置できます。

Ping の問題

Q. 直接接続されたインターフェイスの FWSM に対して ping を実行できないのはなぜですか。

A. デフォルトでは、各インターフェイスで Internet Control Message Protocol (ICMP) が拒否されます。 このトラフィックをインターフェイスで許可するには、**icmp** コマンドを使用します。 この動作は、PIX の動作とは異なります。

注: **icmp** コマンドでインターフェイスへの ICMP が拒否される場合でも、Address Resolution Protocol (ARP; アドレス解決プロトコル) テーブル内には、正しい MAC アドレスが表示されています。 MAC アドレスが表示されない場合は、次の質問を参照してください。

Q. 直接接続されたインターフェイスの FWSM に対して ping を実行できません。また、そのインターフェイスの Address Resolution Protocol (ARP; アドレス解決プロトコル) エントリが表示されません。 スイッチでは、CatOS (またはハイブリッド) ソフトウェアが稼働しています。 どうすればよいのですか。

A. (CatOS のスーパーバイザ モジュール上で) スイッチにインターフェイスが設定されるよりも前に、(**nameif** コマンドを使用して) FWSM のコンフィギュレーションでインターフェイスを設定するか、(**interface vlan** コマンドを使用して) Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) 上にインターフェイスを設定すると、ARP エントリが

ないか、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の応答がないために、インターフェイスがまったく応答していないように見える可能性があります。

スイッチを設定する前にファイアウォール VLAN に属する FWSM または MSFC のインターフェイスを設定していたら、FWSM または MSFC のエントリを削除してからモジュールをリロードし、再度エントリを追加します。

Q. FWSM を通して ping やトラフィックを通過させられないのはなぜですか。

A. Network Address Translation（NAT; ネットワーク アドレス変換）は、nat 0、nat/global、または static コマンドを使用して設定する必要があります。これらのコマンドでは、高セキュリティのインターフェイス（Inside インターフェイス）から低セキュリティのインターフェイス（Outside インターフェイス）に FWSM を通してトラフィックが転送されます。

また、FWSM を通過するトラフィックを許可するためのアクセス リストを実装するには、access-list コマンドを使用します。 デフォルトで、すべてのインターフェイス上のすべてのトラフィックがアクセス リストによって拒否されます（deny ip any any）。 この動作は、高セキュリティから低セキュリティへのトラフィックを許可し、低セキュリティから高セキュリティへのトラフィックを拒否する、PIX のデフォルト設定と異なっています。 permit ip any any を使用してアクセス リストを設定し、それを高セキュリティ インターフェイスに適用して、FWSM を PIX のように動作させます。

Q. ネットワークに直接接続されている FWSM インターフェイスには ping を実行できますが、他のインターフェイスには ping を実行できません。 これは正常な状態ですか。

A. はい。 これは、PIX ファイアウォールにも存在する組み込みのセキュリティ メカニズムです。

フェールオーバーの問題

Q. バージョンの異なるコードが稼働する 2 つの FWSM 間にフェールオーバーを設定できますか。

A. いいえ。フェールオーバーでは、両方の FWSM で同じコード バージョンが稼働していることが必要です。 フェールオーバー機能のメカニズムでは、ピアのバージョンが確認され、コード バージョンが異なる場合のフェールオーバーが防止されます。 このため、両方 FWSM は同時にアップグレードする必要があります。

Q. 異なるシャーシの 2 つの FWSM 間にフェールオーバーを設定できますか。

A. はい。 しかし、FWSM はすべてのインターフェイス上でレイヤ 2 で接続する必要があります。 つまり、すべてのインターフェースでは相互に（Address Resolution Protocol（ARP; アドレス解決プロトコル）などの）レイヤ 2 ブロードキャスト パケットを交換できる必要があります。 フェールオーバー プロトコルのパケットは、レイヤ 3 ではルーティングできません。

Q. 2 つの FWSM 間でフェールオーバーを設定しましたが、両者で同期が行われていません。 考えられる原因として下記の選択肢から 1 つを選んでください。

A. フェールオーバーを正常に行うためには、設定で次の要件が満たされていることを確認してください。

- 両方の FWSM では、同じコード バージョンが稼働している必要があります。
- 両方の FWSM では、VLAN の数が同じである必要があります。
- FWSM 上のすべての VLAN 間に、レイヤ 2 接続が存在する必要があります。 FWSM が異なるシャーシに存在していて、その間でトランクが設定されている場合、すべての VLAN が存在し、トランクで許可されることを確認してください。

Q. 別々のスイッチ シャーシに分散されている FWSM の 3 つ以上のユニットに対してフェールオーバーを設定できますか。

A. **いいえ。**フェールオーバーの設定がサポートされているのは、たとえば 2 つのユニットのような一対の FWSM に対してだけです。 これらの 2 つのユニットは同じスイッチにあっても、あるいは別の 2 基のスイッチにあってもかまいません。 プライマリの FWSM と同じスイッチにセカンダリの FWSM をインストールすると、モジュール レベルの障害に対処できます。 モジュール レベルの障害、さらに、スイッチ レベルの障害に対処するには、セカンダリの FWSM を別のスイッチにインストールできます。 FWSM はスイッチでフェールオーバーを直接取り扱うわけではなく、スイッチのフェールオーバー動作に対して協調的に動作します。 詳細については、『シャーシ モジュール内およびシャーシ モジュール間の配置』を参照してください。

その他

Q. FWSM には、「Do not remove card while status light is green or disk corruption may occur.」（ステータス表示灯が緑色に点灯している場合はカードを取り外さないでください、そうしないと、ディスクが損傷を受ける可能性があります。 ）と書かれたラベルが貼付されています。 これはどういう意味ですか。

A. ファイアウォール モジュールの取り外しは、次の方法のいずれかで電力を無効にしてから行う必要があります（特定の方式のための優先順位はありません）。

- スイッチの Command Line Interface（CLI; コマンドライン インターフェイス）を使用して、次のコマンドのいずれかを発行します。CatOS：set module power down modCisco IOS ® ソフトウェア-**電源イネーブル** *モジュールスロット無し*
- ブレードの **shutdown** ボタンを押します。
- 物理的にシャーシの電源を落とします。

ステータス表示灯が緑色でなくなったら、モジュールを安全に取り外すことができます。

Q. show module コマンドを使用した後、FWSM で faulty/other というステータスが表示されます。 どうすればよいのですか。

A. ステータスが faulty/other の FWSM をトラブルシューティングするには、次のチェックリストを参照してください。

- スイッチで、サポートされているコード バージョンが稼働していることを確認してください。
- FWSM が同じシャーシにある他のブレードと共存できることを確認してください。 詳細は、『Catalyst 6500 シリーズ リリース ノート』または、Software Advisor（登録ユーザ専用）を

参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。
- スイッチで CatOS またはハイブリッド コードを稼働させる場合、FWSM モジュールが占有しているスロットの設定をリセットします。 これを行うには、次のコマンドを使用します。FWSM の電源をオフにするには、「set module power down mod」と入力します。「clear config mod 」と入力して、スロットに関連付けられているスイッチの設定をクリアし、モジュールに電源を投入します。

詳細は、次のドキュメントを参照してください。

- CatOS が稼働している 4000、5000、および 6000 シリーズ スイッチのハードウェア障害チェックリスト
- 統合 Cisco IOS (ネイティブ モード) を実行している Catalyst 6000 シリーズ スイッチのハードウェアおよびよくある問題のトラブルシューティング

それでも問題が発生する場合は、さらにトラブルシューティングを行うために、シスコ テクニカル サポートにお問い合せください。

Q. FWSM のドキュメンテーションはどこで入手できるのですか。

A. FWSM に関するリリース ノートについては、『Catalyst 6500 シリーズ リリース ノート』を参照してください。 詳細については、『Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール』ページで入手可能なマニュアルを参照してください。

Q. FWSM で表示されるエラー メッセージについての情報はどこで入手できますか。

A. Error Message Decoder (登録ユーザ専用) は、さまざまな FWSM エラー メッセージに関する詳細を提供します。 システム メッセージに関する製品ドキュメントにも有益な情報が含まれています。 さらにサポートが必要な場合は、Cisco テクニカル サポートにお問い合せください。

Q. FWSM の既存の不具合についての情報はどこで入手できますか。

A. 既存の不具合についての詳細は、Bug Toolkit (登録ユーザ専用) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

Q. PIX ファイアウォールとファイアウォール サービス モジュールの違いは何ですか。

A. PIX と FWSM は類似のコードを基盤としています。 しかし、基本的な違いが 2 つあります。PIX (サポートを提供) では、VPN と IDS 機能を提供しています。 FWSM では、VPN と IDS 機能は他のラインカードで提供されるため、これらの機能は提供されていません。 Catalyst 6500 シリーズ Intrusion Detection System (IDSM-2) サービス モジュールの詳細については、『Catalyst 6500 シリーズ Intrusion Detection System (IDSM-2) サービス モジュールのデータ シート』を参照してください。 Catalyst 6500 IPsec VPN サービス モジュールの詳細については、『Catalyst 6500 IPsec VPN サービス モジュール製品のデータ シート』を参照してください。

PIX と FWSM のマイナーな相違点については、次のドキュメントを参照してください。

- PIX テクニカル ドキュメント

- PIX リリース ノート
- PIX コマンド リファレンス
- FWSM テクニカル ドキュメント
- FWSM リリース ノート
- FWSM コマンド リファレンス

Q. FWSM で、インターフェイスごとに複数の access-group コマンドを発行できませんでした。 FWSM では、インターフェイスごとに 1 つのアクセス グループだけが取られるようです。 これは、なぜですか。

A. FWSM で次のコマンドを発行する場合、最後の **access-group** コマンドだけが表示されます。

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

FWSM では、1 方向あたりのインターフェイスごとに許可されるアクセス リストが 1 つだけであることが、この理由です。

Q. FWSM では、xlate エントリにどのような情報が保存されているのですか。

A. Xlate エントリには、次の情報が保存されています。

1. **送信元インターフェイス**：パケットを受信する outside などのインターフェイスです。
2. **送信元 IP アドレス**：パケットの送信元 IP アドレスです。
3. **変換済み IP アドレス**：NAT 設定がない場合は、変換済み IP アドレスと発信元 IP アドレスは同じです。
4. **宛先インターフェイス**：パケットの宛先 IP アドレスのルーティング テーブル検索に基づいて、パケットが送出されるインターフェイスです。

Q. FWSM 上の show perfmon の値と統計情報は何を意味しますか。

A. FWSM のパフォーマンスに関する情報を取得するには、**show perfmon コマンド**を使用します。

```
FWSM#show perfmon FWSM#show console-output Context: my_context PERFMON STATS: Current Average
Xlates 0/s 0/s Connections 0/s 0/s TCP Conns 0/s 0/s UDP Conns 0/s 0/s URL Access 0/s 0/s URL
Server Req 0/s 0/s WebSns Req 0/s 0/s TCP Fixup 0/s 0/s TCP Intercept 0/s 0/s HTTP Fixup 0/s 0/s
FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s
```

Current 列には、現在のインターバルの統計情報が表示されています。ここで、最後の列の Average には、最後に統計情報がクリアされてからの累加平均が表示されています。 これは絶対値ではなくレートのため、/s と表示されます。

コマンド出力に表示される統計情報は、デフォルトでは 120 秒間隔でアップデートされます。 この間隔は、**perfmon interval** コマンドで変更できます。

```
FWSM#perfmon interval 20
```

これは、Current 列で報告される統計情報のレートが、20 秒ごとに計算されることを意味します。 また、**show perfmon** コマンドを入力する時は常には、その時点での統計情報でレートが計算されます。

FWSM にはシリアル コンソール ポートがありませんが、**show perfmon** と **perfmon** コマンドによる出力を含む一部のメッセージはコンソール ポートにのみ表示されます。 **show perfmon** コマ

ンドの出力が含まれるコンソール バッファを表示するには、**show output-console** コマンドを使用してください。

Q. no monitor session servicemodule コマンドの使用は FWSM のパフォーマンスに影響しますか。

A. ASIC のハードウェア制限により、FWSM では トラフィックの複製に SPAN セッションが必要となります。 FWSM ではパケットを複製するため、SPAN セッションを用いて複製を必要とするトラフィックをスイッチに渡します。 このコマンドの影響を受けるトラフィックは、分散 EtherChannel、マルチキャスト、および GRE です。 SPAN セッションを設定し、それを削除しないことを推奨します。

何かの理由でそれを取り除く必要がある場合は、『Field Notice: FN - 61935 - Catalyst 6500 シリーズと 7600 シリーズのサービス モジュールにおける分散 EtherChannel とパケット再循環との非互換性』に該当する可能性がある分散 EtherChannel などの複製された実際のトラフィックが存在しないことを確認します。

Q. Access Control List (ACL; アクセス コントロール リスト) をより多く保存するために、メモリを増加できますか。

A. FWSM では、ACL に割り当てられるメモリが制限されます。 FWSM のリソース割り当ての詳細については、『仕様 - ルール制限』を参照してください。

コンテキスト内の ACL に割り当てられたメモリが超過している場合は、次のような エラー メッセージが表示されます。

- `ERROR: Unable to add, access-list config limit reached`
- `ERROR: Unable to add Policy Rules`
- `Unable to add a hole to Policy Rule`

一部のアクセス リストでは、他よりも多くのメモリが使用されます。 それはアクセス リストの種類によって異なり、システムがサポートできる実際の制限は最大値未満です。 ルールとメモリ割り当ての間のマッピングは、1 対 1 のマッピングではありません。 実際には、ルール、およびハードウェアでのプログラム方法によって異なります。

ACE のメモリ使用量を最適化するためには、次の 2 つのオプションがあります。

- ACE エントリを要約し、簡素化します：これを行うには、次の推奨事項を実行します。可能であれば、連続したホスト アドレスを使用します。 ネットワークへの ACE やオブジェクト グループのホスト設定を集約します。可能な場合は、ホストの代わりにネットワークを使用し、またネットワークの代りに any を使用します。オブジェクト グループの簡素化を試みます。 これにより、ACL が拡張される場合、ACE を何百も節約できる可能性があります。 たとえば、個々のポート設定を 1 つの範囲にグループ化します。
- 各パーティションで ACE に割り当てられるメモリを再パーティション化します。 これには、FWSM モジュールをリブートする必要があります。FWSM では、基本的に ACE に割り当てられるメモリを 12 のパーティションに分け、対応するメモリをそれぞれに割り当てます。これは自動的に実行されます。 バージョン 2.3(2) 以降、持っているコンテキストの数に応じて、メモリを再割り当てするためにリソース マネージャを使用できます。**show context count** コマンドを発行して、コンテキストをいくつ持っているかチェックします。 これは設定からも確認できます。 **show resource acl-partition** コマンドを使用するパーティションの数を確認します。 定義されたコンテキストより多くのパーティションが存在する場合は、

resource acl-partition number-of-partitions コマンドを使用して、パーティションの数とコンテキストの数を一致させることができます。この後、設定を保存して、FWSM をリブートする必要があります。 以前のコマンドでは、このメモリで十分であるか、またはコンテキストに追加する ACE に二度と依存しないかどうかに関係なく、ACE に対してより多くのメモリが提供されます。**注意：** 以前の再マッピングの 1 つの欠点は、別のコンテキストを追加する場合に、再度メモリのマッピングを再割り当てする必要があることです。 このため、各コンテキストに使用できるメモリがさらに小さくなり、現在の ACE 定義が破綻する可能性があります。 FWSM に割り当てられるメモリは有限であり、上述したように事前定義された方法または手動のリソース割り当てによって得られます。

バージョン 4.0 以降では、複数の ACL エントリを保存するためにメモリ リソースを効率的に使用する「ACL 最適化」と呼ばれる機能が FWSM に導入されています。 これは、どの ACL エントリの有効性も失わないように、ACL エントリを可能な限り自動的に集約する組み込みアルゴリズムで処理されます。 このアルゴリズムは、複数の ACL エントリで参照される連続サブネットを 1 つの文に連結し、ポート範囲内の重複を検出します。 この機能はコマンドを使って有効にします。最適化の実行後は、完成した ACL 構成が以前（オリジナル）の ACL 構成とは違って見えます。 この最適化された ACL 構成は検証後も維持され、最適化を無効にすることで CPU の計算過負荷を防ぐことができます。 この機能の詳細については、「アクセス リスト グループの最適化」の項を参照してください。この項には、ACL 最適化の機能性とその構成の詳細情報が記載されています。

バージョン 4.0 では、「アクセス リストの容量の増加」という別の機能も導入されました。 この機能を使用すれば、シングル コンテキスト モードでは 130,000 ACL エントリまで、マルチ コンテキスト モードでは 150,000 ACL エントリまで保存できるようになります。 この機能の詳細については、『Cisco ファイアウォール サービス モジュール ソフトウェア バージョン 4.0』の記事の「アクセス リスト容量の増加」を参照してください。

Q. capture コマンドが FWSM に適用されると停止し、別の capture コマンドがインターフェイスに適用されても、すぐにトラフィックがキャプチャされないのはなぜですか。

A. キャプチャ「x」がすでに適用されているのと同じインターフェイスでキャプチャ「z」を設定する場合、キャプチャ「z」はキャプチャ「x」を置き換えます。 アクティブなキャプチャは、特定のインターフェイスに関連付けられる最後のものです。

唯一の例外は、キャプチャ「x」のアクセス リストがキャプチャ「z」のアクセス リストとオーバーラップする場合です。 この場合、両方のキャプチャは、アクセス リストがオーバーラップするトラフィックをキャプチャし続けます。

Q. FWSM 上の NP-PCcmplx logger frame timeout エラーを解決するにはどうしたらいいですか。

A. このエラーを解決するには、FWSM モジュールをリロードします。

Q. TCP 代行受信を使用して特定のタイプの SYN フラッドから保護するように FWSM を設定するにはどうすればいいですか。

A. TCP 代行受信を使用して特定のタイプの SYN フラッドから保護するように FWSM を設定できます。 詳細については、『FWSM TCP 代行受信および SYN Cookie の説明』を参照してください。

Q. IPv6 パケットを処理するとパフォーマンスの問題が生じる可能性がありますか。

A. はい。 パケットは CPU で処理する必要があるため、IPv6 トラフィックを送信するときにパフォーマンスの問題が生じる可能性があります。 CPU による IPv4 トラフィックと IPv6 トラフィックの処理が異なるため、IPv6 パケット処理が原因で、FWSM に関する特定のパフォーマンスの問題が生じます。

Q. FWSM が独自の MAC アドレスを持つ遠隔サーバに応答しないようにするにはどうすればいいですか。

A. 次のコマンドを使って指定されたインターフェイス上で proxyarp 機能を無効にする必要があります。

"sysopt noproxyarp <interface>"
proxyarp 機能の詳細については、『FWSM コマンド リファレンス ガイド』を参照してください。

Q. FWSM 経由のコールがドロップされないようにするにはどうすればいいですか。

A. この問題を解決するには、H323 と H225 の検査を無効にします。

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Q. FWSM 上の NAT 変換の問題を解決するにはどうすればいいですか。

A. この問題を解決するには、xlate-bypass コマンドを使用します。 デフォルトで、NAT が使用されていない場合でも、FWSM がすべての接続の NAT セッションを生成します。 xlate バイパスと呼ばれる未変換のトラフィックの NAT セッションを無効にすることによって、最大 NAT セッション制限を回避できます。 **xlate-bypass** コマンドは次のように設定できます。

hostname(config)#**xlate-bypass**
xlate-bypass の設定方法については、『Xlate バイパスの設定』を参照してください。

関連情報

- FWSM 基本設定の例
- ファイアウォール サービス モジュール ドキュメント
- ファイアウォール サービス モジュール製品サポート ページ
- テクニカルサポートとドキュメント - Cisco Systems