



ファイアウォール サービス モジュール

この章では、ファイアウォール サービス モジュール (WS-SVC-FWM-1-K9) について説明します。

ファイアウォール サービス モジュールは、インターネットなどの外部ネットワーク上のユーザによる無断アクセスから、内部ネットワークを保護します。



(注)

スーパーバイザ エンジンとモジュールの特定の組み合わせは、ご使用のシャーシでサポートされない場合があります。サポートされていないモジュールとスーパーバイザ エンジンに関する具体的な情報については、システムで稼働するソフトウェア バージョンのリリース ノートを参照してください。



(注)

*内部*とは、ファイアウォールによって保護されたネットワーク、またはネットワーク リソースを指します。*外部*とは、ファイアウォールによって保護されていないネットワークを指します。

ファイアウォール サービス モジュールには、次の機能があります。

- モジュールの多重化 — 1 つの Cisco 7600 シリーズ ルータ シャーシ内で複数のファイアウォール サービス モジュールをサポートします。
- スイッチ ファブリック 互換
- インターフェイス設定 — 通常の IOS CLI から実行します。
- URL フィルタリングの強化 — モジュールは、Websense Windows NT または UNIX ベースのサーバ上に定義されたポリシーによって、外部への URL 要求をチェックします。サーバが URL 要求を業務目的に合わない Web サイトの 17 項目の特徴リストと突き合わせ、サーバからの応答に応じて、モジュールは接続を許可または拒否します。
- セキュリティ — Cisco Firewall は、ステートフルインスペクションファイアウォールからコンテンツ フィルタリング機能まで、ネットワーク環境を将来の攻撃から守るのに役立つ最新のセキュリティ テクノロジーを提供します。もう 1 つのセキュリティ機能は、ASA (アダプティブセキュリティ アルゴリズム) です。これはファイアウォールが管理するネットワークの間に、ファイアウォールで保護されたエリアを確保します。

ステートフルでコネクション型の ASA は、送信元および宛先アドレス、TCP シーケンス番号 (予測不可能)、ポート番号、および追加的な TCP フラグに基づいてセッション フローを生成します。セキュリティ ポリシーを接続テーブルの各エントリに適用することによって、内向きおよび外向きのトラフィックをすべて管理できます。

- パフォーマンス — 最大 6 ギガビットのスループットによって、ファイアウォールは極めて過酷なネットワーク環境下でも防護機能を発揮できます。
- 信頼性 — Cisco Firewall は、ファイアウォール サービス モジュール内で統合ステートフルフェールオーバー機能を使用することで、オペレーションクリティカルなネットワーク環境に、適応力の高いセキュリティ サービスを提供します。障害が発生すると、ネットワークトラフィックは自動的にホットスタンバイ モジュールに転送されます。この際、並列接続が維持され、プライマリ モジュールとスタンバイ モジュール間で自動的に状態の同期がとられます。
- Network Address Translation (NAT; ネットワーク アドレス変換) と Port Address Translation (PAT; ポート アドレス変換) — Cisco Firewall は NAT および PAT サービスを提供することで、内部ネットワークの IP アドレスを隠蔽するとともに、内部ネットワーク用のネットワーク アドレス空間を拡張します。
- DoS 攻撃による攻撃の防止 — Cisco Firewall は、ネットワークを停止させる可能性のあるアクセスの試みからファイアウォールとネットワークを保護します。
- スケーラビリティ — 1 つの Cisco 7600 シリーズ ルータ シャーシは、最大 2 つのモジュールをサポートします。

次の PIX ファイアウォール機能は、このモジュールではサポートされていません。

- Virtual Private Network (VPN; バーチャルプライベート ネットワーク) (モジュールは、管理目的でのみ IPSec VPN をサポートします。)
- IDS (侵入検知システム) の Syslog メッセージ
- PFM (PIX ファイアウォール マネージャ)
- CSPM
- コンジット
- DHCP クライアント

前面パネルの LED を図 7-1 に示し、表 7-1 で説明します。

図 7-1 ファイアウォール サービス モジュール (WS-SVC-FWM-1-K9)

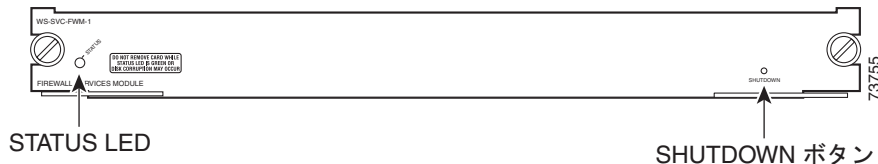


表 7-1 ファイアウォール サービス モジュール STATUS LED の説明

色 / 状態	説明
グリーン	すべての診断テストが正常に終了し、モジュールは動作可能。
レッド	各ポートのテストを除く診断テストでエラーが発生
オレンジ	次の 3 つの状態のいずれかを示しています。 <ul style="list-style-type: none"> モジュールは起動中で、セルフテスト診断シーケンス中 モジュールはディセーブル状態 モジュールはシャットダウン状態
消灯	ファイアウォール モジュールの電源はオフ

SHUTDOWN ボタンは、ファイアウォール サービス モジュールを手動でシャットダウンするために使用します。損傷を防ぐため、電源を遮断する前にファイアウォール サービス モジュールのシャットダウン プロセスを実行する必要があります。ファイアウォール サービス モジュールが CLI または NAM シャットダウン コマンドに応答しない場合は、SHUTDOWN ボタンを使用してシャットダウンすることができます。

ファイアウォール サービス モジュールの詳細については、『[Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 2.3](#)』を参照してください。

