9900/9800/9600/8900/8700シリーズ用フィーチャーライセンス

| AT-FL-02/AT-FL-02-B：ファイアウォールライセンス |

| AT-FL-03/AT-FL-03-B：フルレイヤー3ライセンス(IPマルチキャストルーティング)|

| AT-FL-08/AT-FL-08-B：BGP-4ライセンス | AT-FL-09：アドバンストレイヤー3ライセンス(BGP-4) |

| AT-FL-10：ファイアウォールライセンス| AT-FL-11：IPv6ライセンス |

|AT-FL-13/AT-FL-13-B：IPv6ライセンス |

ソフトウェアバージョン2.9.1以降をご使用の方で、新規にフィーチャーライセンスを購入される場合は購入時に「-B」付きの製品名をご指定ください。ソフトウェアバージョン2.9.1より前のバージョンをご使用の方で、既にフィーチャーライセンスをご購入されているお客様はフィーチャーライセンスの更新や再購入の必要なくそのままご使用いただけます。

AT-FL-02（販売終了）/AT-FL-02-B（販売終了）/AT-FL-10（販売終了）

AT-FL-02 対象製品

9606SX/SC、9606T、8748XL、8724XL、8748SL、8724SL

AT-FL-02-B 対象製品

8748SL、8724SL V2、8724SL

AT-FL-10 対象製品

9812T, 9812T-LM, 9816GB, 9816GB-LM

AT-FL-02/AT-FL-02-B・AT-FL-10は、ファイアウォール機能、アドレス変換機能を追加するためのソフトウェアライセンスです。

Firewall(ステートフル・インスペクション)

通信開始から終了までの通信セッションを監視し、送受信パケットに矛盾がないかをチェックします。また、通信していないときはポートをクローズしますので外部からのアクセスを受け付けません。パケットフィルタリングと同程度の高速処理を保ちながら、より強度なセキュリティの確保を可能にします。

アクセス制御(Firewall Policy Rule)

Firewall を設定することにより外部からのアクセスが不能になりますが、このアクセス制御を設定することにより、特定のユーザーのみ Firewall を通過して LAN 内のサーバーなどにアクセスすることが可能です。制御項目はプロトコルやポート番号、IPアドレスなどでの制御のほか、日時などによる制御も可能で、特定のユーザー/アプリケーションに対して、決められた時間内のみのアクセス許可/禁止といった制御が可能です。

攻撃検出機能

Firewallはネットワークを出入りするパケットのチェックを行いますが、それでも中には攻撃を防ぎきれない場合もあります。そこで、Firewall を通過したパケットから不正アクセスを検出する攻撃検出機能を搭載しました。これにより、DoS（Denial of Service：サービス攻撃）などの攻撃を検出し、より安全なネットワーク環境を構築することが可能になります。

検出可能な攻撃

DOS_Attack、HOST_Scan、SMURF_Attack、TCP_Attack、PING of Death、UDP_Attack、FRAG_Attack、PORT_Scan、SYN_Attack、IP_Spoof、LAND

攻撃検出後のアクション

攻撃検出で検知された攻撃に対し、一刻も早く管理者に通知する機能や防御する機能を備えています。

・アラーム発信
外部からL3スイッチへの不正なアタックがあった場合、下記の方法でL3スイッチの状況を管理者などへ通知し、早急な対処を可能にします。
MANAGER：L3スイッチにLOGINしている端末へ警告表示。
SNMP　　：SNMP Trapを送信。

ダイナミック・コンフィグレーション・チェンジ

Trigger機能と組み合わせることで、攻撃を受けたら経路情報を変更したり、一定時間は外部へのアクセスを閉鎖したりと自動的に設定情報を変更しますので、繰り返される攻撃を回避することが可能です。

※　Trigger機能
日時または曜日、あるいはインターフェースのLinkUpまたはDownなど、様々なイベントにトリガーを設定でき

ます。例えば、ルーティング経路の変更設定で、指定した時間内のみ通信を可能にすることなどができます。

アドレス/ポート変換(NAT/ENAT)機能

NAT (Network Address Translation) とは、特定のプライベートアドレスを特定のグローバルアドレスに変換する技術です。この技術によってインターネット接続に必要なグローバルアドレス不足を解消します。また、TCP/UDP プロトコルのポート番号を利用し、複数のプライベートアドレスを 1つのグローバルアドレスに変換する ENAT（Enhanced-NAT）機能により複数の端末で利用することが可能です。 通常、ネットワーク管理部門から提供される IP アドレスは固定で少ないため、このアドレスが流出すると外部からの不正アクセス（盗聴・なりすましなど）の原因となります。
NAT/ENAT 機能を使用すると、外部から内部へのアクセスは行えなくなるため、セキュリティ上もこの機能でアドレス変換することが有効です。

SSHサーバー/クライアント

ネットワーク上で安全なリモートログインを可能にするSecure Shell（SSH）に対応します。本製品をSSHバージョン1（1.5）のサーバー/クライアントとして動作させることができます（IPv4のみ）。

※　対応製品：8748XL、8724XL、8724SL V2、8724SL