進化するIPS&DDoS対策でセキュリティの脅威に対抗

企業システムを狙った不正侵入やサービス妨害などのサイバー攻撃が後を絶たない。攻撃者の手口が巧妙化、複雑化しており、既存のセキュリティ対策だけでは防ぎ切れないのが実情だ。進化する攻撃は、「進化するセキュリティ対策」で防ぐ。その専用アプライアンスとして注目されるのが、セキュアソフトのIPS(不正侵入防御システム)製品「SecureSoft Sniper IPS」とDDoS(分散型サービス妨害)対策製品「SecureSoft Sniper DDX」だ。

企業や事業者に欠かせない高パフォーマンスのIPS

不正アクセスによる顧客情報の漏えい、Webサイトの改ざん、サービス妨害など企業活動を阻害するサイバー攻撃が深刻化している。万一、顧客情報などが流失すれば、攻撃された企業は被害者ではなく、顧客情報を守れなかった加害者になる恐れもある。

セキュリティ対策ではファイアウォールの導入が一般的だが、システムの脆弱性を狙った攻撃で、社内システムの情報が流出してしまう最近の不正侵入では、ファイアウォールだけでは対応が困難な場合もある。

株式会社セキュアソフト
営業本部
常務執行役員
荻原 博 氏

こうした脅威からシステムやサービスを防御するのがIPSである。企業内やデータセンター内のネットワークを通過するすべてのパケットを監視・分析。不正侵入や疑わしい動き(振る舞い)を検知した場合、管理者に通知し、必要に応じてネットワークを遮断したり、プロセスを停止したりして攻撃を防御する。

IPS市場の中で、企業やデータセンター事業者などに導入されているのがセキュアソフトの「SecureSoft Sniper IPS」だ。ファイアウォールやIPS機能などを搭載したUTM(統合脅威管理)製品とは一線を画す。「IPS専用アプライアンスならではの高い性能や安定性、日本語GUIによる使いやすさなどが多くのユーザーから評価されています」とセキュアソフトの荻原博氏は述べる。

特徴の一つが高いパフォーマンスだ。近年、クラウド基盤となるデータセンター内のネットワークは10Gbpsといった高速化が進展。それに伴い、セキュリティ対策製品にも高速処理性能が求められている。SecureSoft Sniper IPSは10Gbps対応モデルを提供するなど、増大するネットワークトラフィックに合わせたソリューションを拡充している。

ハードとソフトを組み合わせ高速・高精度の検知と防御を実行

「10Gbps環境での侵入検知・防御を実現するのが、進化するSniperエンジンです。ハードウエアとソフトウエアで同時にパケットの分析処理を行い、ワイヤレートでの処理性能を発揮しています」と技術部長の神山竜二氏は説明する。

具体的には、ネットワークを通過する不正パケットの遮断やパターンマッチングによる脅威の判定をハードウエアで処理する。さらに詳細な解析が必要なパケットはソフトウエアで処理。不正と判定されたパケットはパターンマッチングのシグネチャに自動的に反映される自動学習機能により、検知精度がさらに高まる仕組みだ。

また、レイヤー 7のアプリケーションまでパケットを分析する独自開発のALSIエンジンを搭載し、より高い検知機能を提供する。加えて、パケットの収集能力を高めるX-Drier技術を適用した独自開発の専用NIC(Network Interface Card)を含め、高速・高性能の処理を実現しているという。

株式会社セキュアソフト
技術本部　技術サポートグループ
技術部長
神山 竜二 氏

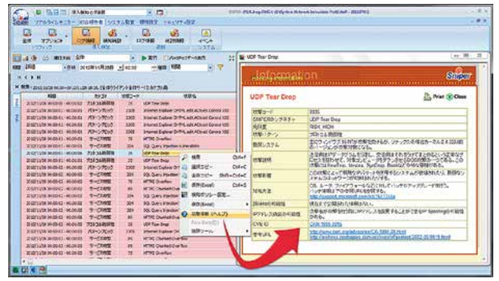
先駆的なDDoS対策専用製品で新たな脅威に迅速に対応

IPSによる不正侵入検知・防御とともに、セキュリティ強化で欠かせないのがDDoS対策だ。DDoS攻撃は以前から知られているが、近年は攻撃者の手口が複雑巧妙化し、攻撃を防ぎにくくなっている。例えば、多数のボットを踏み台に攻撃を仕掛けたり、あたかも正常なサーバーアクセスのように見せかけ、多数の端末から攻撃してサービスを停止させたりする。荻原氏は、「DDoS攻撃の手法が進化しています。そのため、高性能な専用アプライアンスでなければ攻撃を防ぎ切れなくなっているのです」と強調する。

こうした状況を受け、セキュアソフトではIPSで培った技術やノウハウを活かし、DDoS対策専用アプライアンス「SecureSoft Sniper DDX」をいち早く市場に投入している。ALSIエンジンで、なりすましなどのDDoS攻撃を検知・防御することもその一例だ。そして、攻撃の特性やしきい値などパターン別に防御する振る舞いベース、自動学習機能による検知・防御、DDoS攻撃を操る不正プログラムを防ぐシグネチャベースの対策を組み合わせ、最新の遮断技術を実装する。

これらアプライアンスの優位性に加え、豊富な経験を持つセキュリティのエキスパートで構成されるセキュリティ緊急対応チーム「Sniper CERT」が脅威の状況に応じたシグネチャを作成、製品に反映する体制を整備。高い技術と運用の体制を評価して、SecureSoft Sniper IPSとSecureSoft Sniper DDXを併用し、セキュリティを強化する事業者もあるという。

日本語による分かりやすいユーザーインタフェース
分かりやすいGUIで日本語表示。トラフィック情報や検知ログ情報などを同時に確認でき、管理者の作業を効率化



IPS、DDXともに導入したら終わりではなく、運用・管理をいかに効率よく行えるかがポイントになる。アプライアンス本体に内蔵された管理サーバーにはWebブラウザーからアクセスできる。画面表示やレポートは完全日本語で分かりやすく、管理者は管理画面で攻撃の傾向を確認しながら、適切な対応が可能になる。

神山氏は「新たな攻撃への対応や、企業ごとに攻撃の傾向が異なることからチューニングが重要です」と述べる。セキュアソフトでは、IPSのログを解析し、レポート報告とチューニング推奨設定値を提出する定期チューニングサービスや、セキュリティの専門家が常時監視し、緊急時の対応をサポートする24時間セキュリティ監視・運用サービスなどを用意している。企業・組織のセキュリティ状況を把握する診断サービスを提供する計画もあるという。

重要なシステム、サービスを脅威から守るためにも、まずIPS及びDDoS対策のソリューションを検討したい。

不正侵入をリアルタイムに阻止するIPS製品
「SecureSoft Sniper IPS 10G」

DDoS攻撃を遮断するDDoS対応システム
「SecureSoft Sniper DDX ND4000」

セキュアソフト社内にある検証システム

セキュアソフトの製品を実際に使用して攻撃内容を検証する。社内にあるので、きめ細かな対応が可能

securesoft
株式会社セキュアソフト
〒150-0011
東京都渋谷区東3丁目14番15号 MOビル2F
TEL：03-5464-9966
URL：http://www.securesoft.co.jp/