
Intrusion Prevention: Does IT Security Need Something More?

Single Pass Architecture Complements IPS

Although IPSEs might be called the flavor of the week by some security analysts, they are more than foundational to hoards of security vendors. Today's inline (network-based) IPSEs have proven that intrusion detection is only half the battle, and many intrusion prevention providers are getting swallowed up by larger security software vendors that obviously believe in the technology. Check Point Software Technologies, as an example, recently agreed to buy intrusion prevention provider Source-fire for \$225 million.

John Pescatore, senior Gartner analyst, says, "As applications have become more complicated and as the Internet has become a bigger channel through firewalls, attacks have started moving up to the application level and going right through the firewall. So we now need to block those forms of attacks, too. Intrusion prevention is just a reality of dealing with business on the Internet. What we believe has been critical is that intrusion prevention technologies do react to vulnerabilities as the vendors release them rather than wait for the attacks and then react."

Intrusion Prevention Challenges

While intrusion detection devices identify potential threats, IPS technologies actually block malicious traffic before it delivers the payload?but this is just on the one hand. On the other hand, even the most basic IPS devices present challenges including network performance, policy setting, and across-the-board complexity. Vendors are racing to provide intrusion prevention solutions; however, some are realizing that a better, more innovative approach is necessary to attract buyers. But it's not just innovation that's doing the security trick; all-in-one appliances are also proving effective.

Gajraj Singh, vice president of iPolicy Networks, says his company's innovative "single pass architecture" technology on its intrusion prevention-based firewall family

goes beyond conventional intrusion prevention methods. "The software includes a single pass inspection engine that provides high speed layer 3 to layer 7 packet inspection, a rule engine that delivers an optimized common rule tree for multiple security function enforcement and an optimized knowledge-base of attacks, worms, and traffic patterns."

Singh says while this unique approach provides a very fast multilayer packet analysis (which translates into very low latency) as compared to traditional point solution approaches (such as separate firewall, intrusion detection, worm detection, spyware



detection, and URL filtering software or appliances), it also enables the unique advantage of correlated security enforcement, logging, monitoring, notification, and reporting.

Beyond The "God Box"

Enterprises have been looking for this kind of all-in-one, "god-box" security solution that does it all. Singh says iPolicy's technology takes this approach even a step further, providing a higher caliber solution. "Our single pass architecture differentiates us from the general god-box approach. For instance, we do not suffer from the performance impact of turning on all the security features, a common drawback in the traditional god-box approach." The nonperformance impact, he says, is what separates the iPolicy IPF (intrusion prevention firewall) family from traditional intrusion prevention systems. "Also, the correlated security enforcement and reporting capability of our IPF to the single pass approach provides

better security management, something that is not available in the other intrusion prevention solutions," says Singh.

Elsewhere in this space, companies such as Netscreen, Cisco, and Check Point are providing IDS/IPS solutions, but their products are lacking in performance and unification, according to Singh. "Traditional firewall vendors are catching up by adding intrusion detection and prevention for threat mitigation, but with IDS/IPS turned on, their performance suffers significantly. URL filtering is usually external to the firewall system. In addition, the management system for each

of the security functions is separate."

iPolicy's intrusion prevention technology would fall

in line with Gartner's view on what companies should be looking for when evaluating enterprise security vendors. Pescatore says, "When we look specifically at intrusion prevention, there are a couple of key criteria. First, any intrusion prevention system can not impede the network. It has to be in-line, it has to work, it has to fail closed, and it has to meet all of the criteria we have for making sure network performance is not impacted."

The Firewall Does It All

iPolicy Network's line of IPF solutions includes various models to suit multisized enterprise requirements: the iPolicy 2000 at 140 or 200Mbps; the iPolicy 3300 at 350Mbps; and the 4000 series at 600, 1,200, and 2,000Mbps. Singh comments, "The iPolicy IPF solution can be deployed as a complete network protection solution leveraging stateful firewall, in-line bidirectional intrusion detection and prevention, and URL filtering in one appliance." Singh says

iPolicy's technology successfully blocks worms, attacks, and Trojans; mitigates DoS/DDoS attacks; and prevents blended threats from entering the network, in addition to providing access control.

iPolicy's single pass architecture was designed with low latency in mind. Singh says, "This is because we do not inspect packets for each security function. Low latency is important in today's enterprises with growing deployments of time sensitive XoIP [anything over IP] applications." He says single pass also provides real-time intrusion prevention without requiring complex integration of firewall, IDS, and network devices on part of the user. A single point of management is also something that iPolicy has addressed with its IPF technology. Singh says that a single point management of all security functions helps to reduce complexity and makes configuration, monitoring, and report viewing easier.

iPolicy's technology also includes the iPolicy Security Manager, which provides unified security configuration in one console. The security manager includes support for eIQ Network Security Analyzer, a popular Syslog-based report generation and monitoring tool that can integrate inputs from a variety of network and network security devices. This helps enterprise customers comply with regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA.

iPolicy Networks initially developed high speed integrated security products with central unified management for carriers and service providers. In 2004 iPolicy extended the same architecture on lower cost hardware for enterprise deployment.

by Chris A. MacKinnon