STORMSHIELD

INTRUSION PREVENTION (IPS)

Features

SECURITY OF INFORMATION TECHNOLOGIES

The way the Internet is used evolves rapidly all the time. Where traffic was once limited to the exchange of multimedia, today it consists of large volumes of application-based data and interactive content.

Data transactions are increasingly complex and simply using a firewall to block forbidden traffic these days is no longer enough. Modern threats have become much more complicated and are specially crafted to bypass conventional protection mechanisms, with a particular preference for signature-based systems.

To detect and block such threats, new-generation security technologies that can identify abnormal behavior are what we need.

Intrusion Prevention (IPS)

Most network attacks primarily use web pages or authorized services such as email, instant messaging or IP telephony. Each of these applications uses a unique communications protocol.

To block such attacks without affecting a company's day-to-day business activity, protocol analysis is imperative. In evaluating intrusion prevention technologies, inspection performance and detection quality are key considerations.

Optimal efficiency is achieved by the IPS sharing synergies with other technologies. Integrating an IPS with an application firewall, user recognition or vulnerability audit enhances its relevance. An IPS system can lie at the heart of a multifunction firewall deployed at segmentation points. It can also operate in transparent mode without the need to modify an existing network infrastructure.

Stormshield's IPS is the result of 10 years of research. It combines several protocol and behavioral analysis technologies to offer zero-day protection, detecting and blocking most threats even before they are published.

Stormshield's IPS signature lists are updated automatically and the Stormshield security team adds large numbers of signatures to their lists every day. Stormshield develops the most effective protection technology to address each new security loophole.

Because the IPS function provides uniquely high levels of efficiency, it is reflected in performance measurements for all Stormshield Network Security products. Stormshield Network Security's combination of technologies allows you to choose the most appropriate protection for each threat, rather than depending solely on signatures.

The result is optimum security levels which meet all your needs. Every Stormshield Network Security appliance comes with IPS by default. Different configuration profiles are automatically selected, depending on which applies most to the nature of the traffic flow. The result is higher security levels for all.

Developed within Stormshield Network Security's operating system, the IPS engine offers real-time analysis of different traffic flows. It does not cut or copy either the data or the exchanges between the operating system and the detection software. The architecture is tailored to optimize performance and is particularly effective at high throughput levels or where absence of latency is a critical factor, such as in VoIP applications.

Zero-Day Protection

Zero-day protection eliminates the period of vulnerability for your enterprise. Protection is available, even when vulnerabilities are exploited before public notification. Every zero-day protection signature targets an abnormal behavior. The database is updated frequently to enable immediate detection of new threats.

Network security is a race against time in which attacks are often one step ahead of defenses. Some attacks, known as zero-day exploits, spread before any official communication can be issued. Hackers take advantage of them before software companies or the world at large can be notified.

Once a threat is identified, protection signatures are created and deployed as rapidly as possible. This is far more effective than waiting for days or even weeks for corrective action to be taken. But however short the period, the vulnerability is real. Anyone who is responsible for network security has to be constantly on the lookout for effective zero-day protection to counter zero-day exploits.

Stormshield Network Security's intrusion prevention engine has been designed to maximize its zero-day protection capabilities. A number of complementary technologies are deployed:

- Protocol inspection
- Abnormal behavior detection
- Hidden interactive connection detection (e.g. C&C, Botnet)
- And proactive creation of contextual protection signatures

These 4 forms of analysis are effective because they don't have to wait for a vulnerability to appear. The linchpin of Stormshield Network Security's zero-day protection is protocol inspection.

Stormshield's security watch teams anticipate future attacks by continuously adding new inspections for each protocol. Thus, the SIP voice protocol already incorporates various levels of protection against identity theft and denial of service. These effective analyses are activated on all appliances.

VoIP & CoIP

The implementation of IP telephony has seen enormous growth in recent years. Maturing technology and falling costs have coincided with the convergence of voice and data.

- The ability of the phone system to now carry network data enables resource optimization
- The network can also manage the telephony system and carry voice data

However, these developments have been accompanied by a rise in malicious attacks exposing vulnerabilities associated with both technologies. IP networks and voice protocol weaknesses can be exploited by denial of service attacks at both the application and protocol levels.

Identity theft and unauthorized recording of telephone conversations can pave the way to malicious data access. SQL injection attacks result in the theft of confidential information. An effective security system is now a prerequisite for any organization wishing to protect its telephony and network assets.

Stormshield's network protection solutions allow customers to secure all of their network assets. They guarantee the security of IP telephony systems, while their advanced functionality enables them to deal with the special requirements of real-time data and all aspects of converged voice and data networks.

REAL-TIME IP TELEPHONY SYSTEM PERFORMANCE

To ensure that security concerns do not prejudice performance levels, all standard Stormshield Network Security appliances are supplied with the Intrusion Prevention Engine pre-activated. In addition, quality of service parameters are configured and managed to address problems such as latency and jitter.

IP TELEPHONY

The vulnerabilities inherent in any IP telephony system represent a risk to security. Attacks can lead to denials of service, remote code vulnerabilities and the hijacking of sensitive data. Stormshield Network Security solutions contain the Stormshield Network Vulnerability Manager.

The service delivers specific reports, seeks vulnerable devices and suggests appropriate corrective measures. Effective procedures can then be implemented to manage the vulnerability risks within an IP telephony system. Adapted filtering and security policies can be applied to vulnerable hosts in just one click.

ABOUT

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space CyberSecurity, run the Stormshield brand and offer innovative end-to-end security solutions both in France and worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

All trademarks are the property of their respective companies.

STORMSHIELD

Phone
+33 9 69 32 96 29

The cost of a call may vary according to the country you are calling from and your telecoms operator.

WWW.STORMSHIELD.EU

Netasq
Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq - FRANCE