# The Proventia Network Intrusion Prevention System Protection Engine

## Highlights

- ***Stop threats before they impact your networks***
- ***Protect your network and the assets on your network such as servers, desktops and network infrastructure***
- ***Protect the systems that run your business such as VoIP, Data Storage, Databases, Webservers, and Server Farms***
- ***Conserve network bandwidth by eliminating worms, attacks and the misuse (abuse) of the network by eliminating skype, instant messaging and peer-to-peer file sharing***
- ***Prevent the loss of information by hardening your network against attacks and monitoring for and preventing data leakage.***

**Staying ahead of the threat – the protection engine inside the IBM Proventia Network Intrusion Prevention System.**

The IBM Proventia® Network Intrusion Prevention System (IPS) stops Internet threats before they impact business and delivers protection to all three layers of the network: core, perimeter and remote segments.

The basis for Proventia Network IPS' unique form of security lies in its engine, which enables preemptive protection against a wide variety of Internet threats. Proventia's protection engine is built upon years of security intelligence gathered by the IBM Internet Security Systems™ X-Force® research and development team. The X-Force team is a world-renowned security research organization dedicated to proactive examination of threats and the underlying software vulnerabilities they seek to exploit.

As a result, Proventia's protection engine can stop entire classes of attack – including new and unknown threats – without updates. Other IPS solutions can only hope to match individual protection signatures with exploits – a process that is too slow to stop evolving threats and results in higher rates of false positives and false negatives.

The Proventia Network IPS protection engine has the ability to prevent the following classes of network threats:

- Application Specific Attacks
- Backdoors
- Botnets
- Cross-site scripting
- Data leakage via Webmail attachments
- Denial of Service (DoS)
- Distributed denial of service (DDoS)
- Insider threats
- Instant messaging
- Operating System Specific Attacks
- Peer-to-peer
- Protocol tunneling
- Rootkits
- Spear phishing
- Spam
- Spyware
- SQL injection
- Trojans
- Worms
- Viruses

In order to prevent entire attack categories, Proventia's protection engine employs multiple intrusion prevention technologies working in tandem, including:

- Port assignment
- Port following
- Protocol analysis
- Protocol tunneling
- Pattern matching
- Heuristics
- RFC compliance checking
- Statistical analysis
- TCP reassembly
- Flow assembly

**Primary Network Threats Stopped by the Proventia Protection Engine**

While Internet threats continue to evolve, older attack methods cannot be discounted and many attackers build upon known intrusion techniques to evade detection. The Proventia protection engine is dedicated to stopping the following list of Internet threats:

Backdoors – provide system entry points that bypass traditional login verification.

Botnets – collections of compromised computers that perform tasks at the behest of a controller – usually with malicious intent to spread spam and/or malware.

Cross-site scripting (XSS) – a Web-based exploit used to embed malicious code into a supposedly legitimate link that can execute on a user's computer, typically in an attempt to steal information.

Distributed Denial of service (DDoS) – utilizes a multitude of compromised systems to attack a single target with a flood of messages to shut the target system down.

Insider threats – can introduce viruses, worms and Trojans into a network, or attempt to steal proprietary data.

Instant messaging – can be used to introduce Trojans, viruses and other malware into the network.

Peer-to-peer (P2P) networks– facilitate the transfer of files infected with Trojans and viruses designed to introduce denial of service attacks and corrupt data.

Protocol tunneling – layers malicious data usually within a higher level protocol, allowing it to traverse network segments where lower level protocols might be blocked.

Rootkits – a collection of tools or programs that provide hackers with administrator level privileges or root access to a network or system.

Spam – a common carrier for spyware and phishing scams that entice users to visit malicious Web sites, and then potentially introduce malware to the network.

Spear phishing – specifically targets a narrow audience by mimicing e-mails and Web sites from online auction sites or well known banks.

Spyware – can be used to track a user's Internet use, steal personal information and install other malware.

SQL injection –
piggybacks malicious SQL code on intended commands through the dynamic logic layer of a Web application in order to trick the application into providing database access.

Trojans –
harbor dangerous code inside apparently harmless programming or data.

Viruses –
replicate through file transfer- as e-mail attachments, in downloaded files or via CD or diskette.

Worms –
a virus that self-replicates by resending itself as an e-mail attachment or part of a network message.

**Multi-layered prevention technologies within the Proventia protection engine**

The Proventia protection engine combines the power of multiple threat prevention technologies – all working in concert to stop Internet threats. The Proventia protection engine utilizes the following attack prevention methods:

Port assignment –
IPS' should not assume that a particular type of traffic will appear on a particular TCP/IP port. If they do and the traffic type matches the assumed port, and is allowed through, attackers could gain access. Proventia inspects all traffic regardless of the port that traffic is destined to.

Port following –
tracks communication sessions to ensure that the port initially used to establish a connection is the only one used. This prevents hackers who access an open port with authentic credentials from connecting to another open port to transfer data unnoticed. Proventia's port following works in conjunction with other port-aware protection technologies to stop information theft.

Protocol analysis –
examines network traffic for deviant behavior that does not match accepted norms and can decode protocols down to Layer 2 of the OSI model. Protocol analysis enables Proventia to detect anomalous behavior without relying on signatures.

Protocol tunneling –
sometimes used in conjunction with port assignment, Proventia detects and prevents protocol tunneling to find malicious and/or proprietary data embedded in higher level protocols that could be allowed to traverse network segments where lower level protocols might be blocked. Protocol tunneling prevents hackers from bypassing firewalls to gain uncontested network access and prevents both insiders and hackers from establishing and using tunnels to extract data from within a corporation.

Stateful pattern matching –
uses advanced algorithms to detect attack patterns – but only in particular portions of traffic where an attack could actually exist – greatly reducing false positives. Proventia uses stateful pattern matching in conjunction with heuristics to prevent evolving threats that change their patterns to evade detection.

Heuristics –
identifies and stops malicious code based on its behavior, rather than matching a particular attack signature or pattern. Heuristics can prevent evolving threats which will change minor aspects of their signatures to bypass traditional IPS solutions.

RFC compliance checking –
compares traffic against RFC standards for network communications between hosts, and between applications and the network stack. If the traffic does not conform, Proventia blocks it.

Statistical analysis –
creates a baseline of network activity over time and then constantly compares current activity to the baseline to identify and prevent deviations. Proventia uses statistical analysis to stop attacks without breaking down network traffic.

TCP reassembly –
reassembles network packets, examining them for potential threats.

Flow assembly –
analyzes the entire network connection – not just the individual packets – to block malicious traffic that may have been inserted into the communication stream to take advantage of an open connection. Flow assembly complements TCP reassembly by analyzing traffic at a higher level to prevent advanced threats.

**The Proventia Protection Engine Advantage – Multi-layered Prevention Technologies Working in Concert**

The protection engine within the Proventia Network IPS appliance is the result of continuous research into the nature of vulnerabilities and attack methods. As threats continue to evolve, but older exploits never truly become extinct, IBM ISS constantly strengthens the Proventia protection engine with technologies designed to block entire classes of threat – both new and old.

**Learn More**

For more information about the Proventia Network IPS appliance and preemptive protection, please visit **ibm.com**/services/us/iss or call 1 800 776-2362.

© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
10-07
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

GTB03006-USEN-00