

# SonicWALL To Offer Intrusion Detection And Prevention Capabilities Across Product Line

Submitted by: Write Angle Communications

Tuesday, 24 February 2004

---

London, UK - 24 February 2004 - SonicWALL, Inc. (NASDAQ: SNWL), a leading provider of integrated security, productivity and mobility solutions, today announced that a full-featured Intrusion Prevention Service will be available as a yearly subscription for the TZ 170 and PRO 2040, PRO 3060, PRO 4060, and PRO 5060 platforms.

This new technology will deliver a configurable, high performance stateful signature engine for extended protection to key Internet services such as Web, e-mail, file transfer, Windows services, and DNS. This enhances the payload inspection technology currently driving SonicWALL's Complete Anti-Virus rapid e-mail attachment blocking and SonicWALL's Content Filtering Service. The new capabilities are designed to protect against known buffer overflow vulnerabilities in software, as well as various worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in the deep packet inspection engine will provide a proactive defense against newly discovered application vulnerabilities.

"Once again, SonicWALL has taken a key technology advance—previously expensive and with limited availability—and integrated it into easy-to-use, cost-effective, and widely available platforms for the broader market," noted Douglas Brockett, SonicWALL's vice president of worldwide marketing.

"SonicWALL's customers have come to expect nothing less than value innovation in our products, as we offer easily-deployed, highly relevant technology when our customers need it, at a price they can afford."

Malicious attacks targeting application vulnerabilities have been plaguing networks since Nimda and Code Red in 2001 and SQL Slammer and MS Blaster in 2003 infected computers worldwide. Costs associated with these attacks grew to over \$50 billion last year alone. More recently, threats have come from the use of peer-to-peer and instant messenger applications, including the recent Mydoom virus, which was propagated through the file sharing application Kazaa as well as through e-mail. Changes in the method and delivery of attacks have led to the need to enhance the detection and prevention capabilities of the firewall protecting the network at the perimeter.

"Through integrated services like SonicWALL Complete AV on the current SonicWALL security platform, we've successfully given customers active protection against virus threats," said Keith Biggin, technical development manager at SonicWALL Gold Partner, System Software Solutions. "The new intrusion detection and protection capability, on top of SonicWALL's already superior feature set, will provide a further layer of protection for our customers' networks. A major benefit is its ability to proactively identify suspicious traffic without the performance deterioration you see with other solutions. By incorporating the latest technologies into its security architecture SonicWALL is ensuring we continue to offer customers solutions that are excellent value as well as giving us a high return on investment."

The SonicOS security engine currently recognizes and protects against various traffic anomalies, port scanning reconnaissance activities, various packet level intrusion and Denial of Service attacks, as well as actively blocking forbidden, unwanted, or malicious URLs and Web-based content, including spyware, cookies, ActiveX, and Java archives. In addition, the security engine works in conjunction with dynamic security service updates from SonicWALL to provide real-time deep packet inspection blocking of malicious e-mail.

Features of the new Intrusion Prevention Service include:

**Deep Packet Inspection Engine** – The SonicWALL Deep Packet Inspection framework supports complete signature matching across ordered TCP fragments without performing any reassembly. In the case where packets arrive out of order, they are buffered and reordered by the Deep Packet Inspection Engine. This method of packet processing results in more efficient use of processor and memory for greater performance.

**Signature Database** – The SonicWALL Intrusion Prevention Services ships with 1,700 stateful signatures that detect and prevent against application exploits, vulnerabilities, worms and network attacks in over 50 protocols, providing comprehensive protection from malicious attacks. Additional signature categories include the ability to block popular instant messenger and peer-to-peer applications from traversing the SonicWALL appliance.

**Signature Updates** – Signatures of new exploits, vulnerabilities, worms and attacks are automatically downloaded to the SonicWALL appliance through SonicWALL's distributed enforcement architecture for all customers with an active subscription. The distributed enforcement architecture reduces the total cost of managing an Intrusion Prevention deployment by ensuring that signatures are always up to date.

**Policy Management** – The SonicWALL Intrusion Prevention Service simplifies deployment and management through pre-configured global policies and grouping of attacks by priority. In addition, the policy includes granular configurability to remove false positives by allowing signatures to be individually set to detect and/or prevent.

**Central Management** – The SonicWALL Intrusion Prevention Service is centrally managed through the SonicWALL Global Management System. This award-winning management capability eases the total cost of ongoing management of Intrusion Prevention deployments spanning multiple locations, such as branch offices, tele-workers, remote offices, retail stores, or medical clinics. Policies are centrally created and deployed to all remote SonicWALL appliances, ensuring all remote locations are protected from attacks and compliant with the corporate policy.

The SonicWALL Intrusion Prevention Service will be available on the SonicWALL TZ 170 and PRO 2040, 3060, 4060, and 5060 models in Q2, 2004. Pricing starts at £350 per year per appliance.

About SonicWALL, Inc.

SonicWALL, Inc. is a leading provider of integrated network security, mobility, and productivity solutions for the SMB, enterprise, e-commerce, education, healthcare, retail/point-of-sale, and government markets. Core technologies include firewall, VPN, wireless, SSL, anti-virus, and content filtering, along with award-winning security management solutions. Together, these products and technologies provide the most comprehensive Distributed Security Architecture available. SonicWALL, Inc. is headquartered in Sunnyvale, CA. SonicWALL trades on the NASDAQ exchange under the symbol SNWL. For more information, contact SonicWALL at +44 (0)1344 668090 or visit the company Web site at <http://www.sonicwall.com>.

# # #

For Additional Information Contact:

Katy Sutcliffe

Marketing Manager

SonicWALL UK, Middle East & Africa

Tel: +44 (0)1344 668090

Email: [ksutcliffe@sonicwall.com](mailto:ksutcliffe@sonicwall.com)

Paul Shlackman

Write Angle Communications

Tel: +44 (0)20 8868 4101

Mobile: +44 (0)7775 655363

Email: [paul.shlackman@writeanglecomm.com](mailto:paul.shlackman@writeanglecomm.com)

NOTE: SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.