SonicWALL Customers Protected From Sasser Worm By Advanced Intrusion Prevention Service

Submitted by: Write Angle Communications
Tuesday, 4 May 2004

London, UK - May 4, 2004 - SonicWALL Inc., a leading provider of integrated security, productivity and mobility solutions, today announced that SonicWALL's new Intrusion Prevention Service (IPS), officially released yesterday, protects customers from both externally-originating Sasser worm attacks as well as internal propagation of the worm.

The Sasser worm takes advantage of a weakness in the Local Security Authority Subsystem of the Windows 2000 and Windows XP operating systems. The worm creates a File Transfer Protocol (FTP) server on infected hosts and also uses these hosts to scan for vulnerable systems connected to the Internet. Once a vulnerable target has been found, the worm establishes a remote connection to the target system and installs itself on the targeted system via an FTP request back to the original infected host. The propagation does not require any user intervention (such as opening an attachment) and the worm can cause random crashing/rebooting of infected computer systems.

"Small to mid-size businesses need advanced intrusion prevention services like SonicWALL's to protect them from disruptive and highly sophisticated worms like Sasser," said Douglas Brockett, SonicWALL vice president of worldwide marketing. "The size of one's business is almost irrelevant when confronted with a threat that propagates rapidly and indiscriminately."

SonicWALL's Intrusion Prevention Service (IPS) adds a layer of protection not found in stateful packet inspection firewalls. Using a high-performance deep packet inspection engine, SonicWALL's IPS is able to analyze packet contents as a whole rather than just packet header information, allowing for the identification and prevention of threats, such as Sasser, that disguise themselves deep inside network communications.

SonicWALL's optional, subscription-based Intrusion Prevention Service not only proactively identifies malicious code coming into the network from the outside, it can also monitor traffic and stop worms from propagating internally. Employees can release the worm into the internal network by accessing the Internet from home with a vulnerable mobile computer and then bringing the system into the office and connecting to the network locally.

Using the combination of SonicWALL's IPS and any appliance running SonicOS Enhanced software, the worm outbreak can be isolated within a security zone and prevented from spreading itself to other zones within the network. Security zones are logical groupings of networks to which Intrusion Prevention, Content Filtering, Anti-Virus enforcement and access rules can be applied.

"As hackers and virus writers become ever more sophisticated, companies need to find ways to ensure their networks are protected at all times – even before the latest virus signature updates and OS patches are ready," said Paul Webb, managing director of Blue River Systems, a Surrey-based security solutions reseller and SonicWALL Gold Partner. "Intrusion prevention systems will identify suspicious traffic and stop a potential infection before it can harm corporate resources and employee productivity. SonicWALL's solution is particularly robust with over 1700 signatures and granular management

capabilities. As a result, my customers remain worry-free even during outbreaks like the current Sasser worm."

As part of its Distributed Enforcement Architecture, SonicWALL also offers its Global Security Client software to provide security for mobile workers outside of the gateway firewall by blocking network access through vulnerable ports. The SonicWALL architecture gives business the ability to extend security policies to all internal nodes on the networks as well as all remote or wireless nodes connecting into the network.

# # #

For Additional Information Contact:

Katy Sutcliffe
Marketing Manager
SonicWALL UK, Middle East & Africa
Tel: +44 (0)1344 668090
Email: ksutcliffe@sonicwall.com

Paul Shlackman
Write Angle Communications
Tel: +44 (0)20 8868 4101
Mobile: +44 (0)7775 655363
Email: paul.shlackman@writeanglecomm.com

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, intrusion detection and prevention, SSL, anti-virus, and content filtering, along with award-winning security management solutions. Together, these products and technologies provide the most comprehensive distributed enforcement 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.