

# WLAN Security Adoption Still Trailing Despite Widespread Use of Wireless in the Workplace

Submitted by: Write Angle Communications

Monday, 15 November 2004

---

London, UK – 15 November, 2004 – Around 70 percent of British organisations are either already using or planning to use wireless connectivity as part of everyday business. Yet security remains top of the list when it comes to wireless networking concerns, with more than a third of companies admitting that they would have no way of knowing if their wireless security measures were breached. These are some of the main findings of an independent survey\*, commissioned by SonicWALL, Inc., (Nasdaq: SNWL), released today.

The study of wireless networking issues and attitudes in the UK involved interviews with directors and senior IT managers at more than 400 businesses. By far the majority of participants (47 percent) represented enterprises with 1000-plus PCs. Small-to-medium sized businesses (101 to 999 PCs) made up 39 percent of respondents while small business accounted for the remainder.

Around half the survey participants have already deployed wireless local area networking (WLAN) while a further 20 percent are considering implementing it in the coming 12 months. Almost two thirds of firms (64 percent) named flexibility in their top three reasons for the increasing popularity of wireless networking. Other key motivating factors were productivity (37 percent) and support for business change (33 percent). Asked who benefits most from WLAN access, nearly three quarters of respondents (72 percent) said it was employees through improved access to the Internet and corporate LAN. Other suggested benefits included departmental specific functions (stock taking, order entry and so on) and Internet access for visitors. Each of these polled votes from around a third (29 percent) of participants.

Security is still the single biggest fear factor with wireless technology. More than three quarters (77 per cent) of firms cited it as a key concern although management (30 per cent) and cost (24 per cent) also ranked in the top three worries. Interestingly, fewer than one fifth (16 per cent) of respondents failed to see any benefit from wireless, compared with more than 30 per cent in a similar SonicWALL-backed survey published a year ago.

Asked to rank the primary requirements of a WLAN solution in order of importance just over one third (36 per cent) of participants rated seamless roaming as the top priority closely followed by single point of management (34 per cent). On the security side single point of management was rated even more important with almost half (46 per cent) of respondents ranking it as top priority followed by automated policy checking (34 per cent) and enforced IPSec Virtual Private Network (VPN) connectivity (31 per cent).

Revealingly VPN is at the forefront of remote access security, in use by 80 per cent of companies yet only 20 percent use it for Wireless LAN access. Instead just under half of firms rely on the basic Wired Equivalent Privacy security standard and another 18 per cent use its successor Wi-Fi Protected Access (WPA) in one form or another. This is a little surprising in view of their much publicised flaws.

Most firms (69 percent) have understood the message that wireless is insecure and have deployed their WLAN in a secure firewall zone (or DMZ). While this protects the company at the network level, the fact that they still use WEP means that there is still more to do to protect the application layer. The next

stage will be to introduce encryption to protect confidentiality and deep packet inspection for quarantining worms, viruses and Trojans from spreading via the WLAN.

More than 80 percent of those with WLANs said they enforced security policies governing usage yet less than half (44 percent) had ever had their WLANs audited. When asked how they would know if they was a breach of security on the WLAN just 16 percent of respondents (73) chose to answer the question. Of those that did respond 38 percent admitted they would have no idea.

“It is interesting to see just how fast WLANs have grown in popularity in a single year,” said Mike Smart, European product manager for SonicWALL. “There is still much work to be done to educate the market about the dangers of relying on wireless protocols for security, especially when VPN is in widespread use and offers a much safer alternative.”

“Many companies have taken on board the message that they need to have enforced security policies,” he continued. “The next phase will be to audit these policies and deploy technologies like intrusion prevention, that will better enable firms to determine when the WLANs are breached. Legislative pressures such as Sarbanes-Oxley and Basel II will play a part in ensuring this happens sooner rather than later.”

- ends -

\* Carried out by ITelligence, the independent research arm of Reed Business Information Limited

About SonicWALL, Inc.

SonicWALL, Inc. is the leading provider of integrated Internet security appliances offering access security, transaction security and security services for the enterprise, e-commerce, SME, education and government markets. Core technologies include firewall, VPN, SSL, high availability, anti-virus, strong authentication with digital certificates, vulnerability assessment and content filtering. 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

#### Safe Harbor Regarding Forward-Looking Statements

Certain statements in this press release are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. The forward-looking statements include but are not limited to statements regarding the growth in use of wireless LANs, the security of wireless protocols, or the ability to detect security breaches. These forward-looking statements are based on the opinions and estimates of management at the time the statements are made and are subject to certain risks and uncertainties that could cause actual results to differ materially from those anticipated in the forward-looking statements. In addition, please see the "Risk Factors" described in our Securities and Exchange Commission filings, including our Annual Report on Form 10-K for the year ended December 31, 2003 and Form 10-Q for subsequent periods, for a more detailed description of the risks facing our business. All forward-looking statements included in this release are based upon information available to SonicWALL as of the date of the release, and we assume no obligation to update any such forward-looking statement.

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.