Growth in Teleworking Presents New Security Challenges

Submitted by: Write Angle Communications
Thursday, 9 May 2002

New Six Point Guide to Help Business and Financial Services
Make the Right Choices to Secure Their Future

LONDON, 8 May 2002 - Two rapidly spreading business trends are starting to transform the way companies operate in the 21st-century and the combination brings new risks to the corporate network, a leading industry security specialist claimed today.

While the growth of business broadband, on the one hand, and the rise in telecommuting, on the other, are set to bring considerable benefits to both employers and workers alike, SonicWALL, the world's leading vendor of Virtual Private Networking (VPN) hardware, today warned that they also create fresh security issues and challenges and announced a series of measures designed to help companies deal with them.

The rise in teleworking is well documented. Last year a government Labour Force Survey* showed that as much as 6% of the UK working population, equivalent to 1.5 million people, work for their employer or client via a remote link. This figure was up 19% from the previous year. The same survey found that by far the largest proportion of homeworkers, around 25 per cent, work in the business and finance sector. Yet a joint report from the DTI and PricewaterhouseCoopers released earlier this year shows 44% of UK businesses have suffered at least one malicious security breach in the past year. Many in the industry fear that the move towards teleworking where the corporate network is accessed from a potentially unsecured home network could increase this dramatically.

For example, how can companies prevent non-secure home networks from compromising their corporate networks? What can be done to protect remote workers against the constant threat of new viruses and worms? What is the best way to expand the telecommuting network without opening new security holes? How can they successfully manage a diversified, constantly changing telecommuting workforce? Finally, and perhaps most important of all, How do companies retain control over a network of widely distributed remote access points?

According to Mike Smart, SonicWALL product manager in the UK, the most popular way to ensure security between a company and its teleworkers is via a VPN – a sort of communications tunnel between the homeworker and central office that is generally accepted as 100% impervious to interception. "Yet, this is not necessarily the case," he explains, "since the vast majority of existing VPN solutions on the market today do not make allowances for the fact that teleworkers may themselves be on a small family network. This means the network activities of other family members could inadvertently leave the VPN

tunnel open to unwelcome visitors.”

To stay safe, SonicWALL recommends businesses should make sure their VPN solutions meet the following criteria:

1. Isolate the telecommuter connection - where the teleworker unit is on a shared network at home it should not be possible for the VPN tunnel to be accessible to anyone else on the home network

2. Enforce network protection at the telecommuter site - companies should consider giving teleworkers security levels at home that comply with the basic minimum corporate standards thereby enforcing a multi-layered defense mechanism that incorporates firewall, anti-virus, content filtering and authentication

3. Scale the telecommuting network infrastructure – the majority of enterprises will require VPN connections with many different users so it is important that the solution should be scalable to allow security measures to be deployed rapidly via a web browser

4. Manage telecommuting security policies - any solution must be capable of being managed remotely by the company’s service professionals so that the VPN links remain in full control of the organisation at all times

5. Perform stateful inspection - where malicious attacks are detected at the application layer rather than at operating system level

6. Comply with standards - IPSec, ICSA certification and PKI

*Source: IES analysis of Labour Force Survey – published August 2001

- ends -

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 (408) 745-9600 or visit the company Web site at http://www.sonicwall.com .

For further information please 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

Distributed via Press Release Wire (https://pressreleases.responsesource.com/)on behalf of Write Angle Communications

Copyright © 1999-2019 ResponseSource, Melrose House, 42 Dingwall Road, Croydon, London, CR9 2DX UK

e: info@responsesource.com t: 0345 370 7777 f: 0345 370 7776 w: https://www.responsesource.com

ResponseSource
Press Release Wire