

Teleworking and the New Economy

*Greater savings, productivity and ROI from
teleworking with Secure Remote Access*

CONTENTS

Benefits of Teleworking in the New Economy	2
Inherent Risks of Teleworking	4
SonicWALL Secure Remote Access and Network Security Solutions	5
Conclusion	8



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Abstract

With the new economic challenges of rising fuel costs, credit uncertainty and tighter operating budgets, businesses are increasing their use of teleworking to boost productivity, expand and retain staffing resources, reduce IT and facilities overhead, provide business flexibility and ensure business continuity. Employees, partners and consultants use laptops, PDAs, smartphones, home PCs and public kiosks to access mission-critical corporate resources from outside the traditional network perimeter. But greater access comes with greater risk. This paper provides an overview of how teleworking enhances productivity, the associated security risks, and how Secure Remote Access and Network Security solutions from SonicWALL® address these concerns by delivering an underlying platform that makes remote access secure, scalable and easy to manage. SonicWALL solutions provide powerful, granular and complete remote access, driving the cost and complexity out of running a high performance, distributed network.

Benefits of Teleworking in the New Economy

Several factors contribute to the growing number of teleworkers and the increase in alternative work environments in the new economy. Teleworkers enjoy personal cost savings and flexibility, leading to increased job satisfaction and retention. Ubiquitous remote connectivity technology enables people to be productive virtually anywhere and at any time—while traveling, in the field or at home. As a result, companies benefit from extended work hours and improved employee productivity and morale. Teleworking also cuts operational costs associated with energy and facilities, and delivers a greater return on technology investment.

Responding to economic burdens on the workforce

Attracting and retaining skilled professionals from the widest staffing pool gives businesses an edge over their competition in a challenging economy. Fuel costs eat away at worker compensation. Lending rates directly influence decisions to purchase commute vehicles or relocating closer to work sites. For today's workers selecting an employer, the economic impact of gas prices, real estate and credit rates are now added to ongoing concerns over traffic gridlock, pollution, global warming, foreign oil dependency, road stress and life/work balance.

As 10-hour workdays occur more frequently, employers and employees increasingly blend professional and personal tasks. Many employees regularly respond to email and work on critical projects from home.

Out of FORTUNE Magazine's 100 "Best Places to Work" in 2008, 84 offered telecommuting. In a study of technology workers, 37% said they would take 10% off their salaries (an average of \$7,400) for the opportunity to telecommute¹. Research shows that employees who telework often express greater job satisfaction than their onsite peers, and they may also experience reduced levels of stress, due to control they have over organizing their tasks on a day-by-day basis.² AT&T found two-thirds of workers offered jobs by competitors remained with the company, citing telework as a major factor in their decision.³ It is clear that companies must embrace teleworking in order to maintain their competitive edge.

¹ The Dice Group, 2008

² Life Lines, Susan Hirshorn. Occupational Health & Safety Canada. Don Mills: Dec 2003. Vol. 19, Iss. 8; pg. 22

³ The Telework Coalition

Increasing productivity and profitability

Today's business needs to be conducted away from the office. Workers are commuting longer distances, taking hours from their workdays. Critical business is transacted on home PCs, on third-party partner or customer network computers, or on public access Internet kiosks in airports, hotels and cafés.

The average office-bound worker spends the equivalent of 30 working days per year commuting, traveling or engaging in office chit-chat.⁴ Converting some of this down time into productive time is a clear win for employers. For example, IBM estimates that teleworking boosts employee productivity about 20 percent.⁵ British Telecom found productivity rose 31 percent among its 9,000 teleworkers due to lack of disruptions, stress and commuting time.⁶ Dow Chemical reported teleworking increased productivity by 32.5% (10% through decreased absenteeism, 16% by working at home and 6.5% by avoiding the commute.)⁷

Employers also gain increased productivity and organizational responsiveness resulting in faster completion times for important initiatives. Since 2001, U.S. worker productivity has increased 4.6% annually. Due to the significant technology investments made over the last decade, more industries are now realizing increased workforce efficiencies. Companies are gaining this productivity by using technology to enable current workers to do more work, by hiring temporary workers, and by outsourcing, instead of hiring more full-time employees.⁸ For distributed organizations, secure, available and cost-effective remote access is crucial to increased productivity.

Teleworkers need around-the-clock access to key information, collaboration tools and business applications. According to a Nemertes benchmark, "87% of employees work at locations other than the headquarters building or campus, typically at a regional facility sales office, retail store or a home office."⁹ A viable solution needs to address the remote access needs of teleworkers, as well as handle the additional security risks they bring about.

Reducing operational costs

Teleworking can cut operations costs for power, cooling, desktop computers, furniture, phone land lines, as well as real estate. In 2005, Sun Microsystems reported saving \$255 million in real estate costs over four years by eliminating or avoiding the need for 7,700 cubicles and workstations.¹⁰ IBM estimates that eliminating office space for 10,000 teleworkers saves the company \$75 million a year¹¹. At the same time, office space costs have skyrocketed. Eliminating office space for even a thousand teleworkers can potentially save millions of dollars a year.

Rising fuel costs have also dramatically increased the cost of business travel. Secure remote access technology facilitates teleconferencing and remote collaboration by enabling real-time communication, file and application sharing between distant locations, without incurring airfare and hotel costs. In 2006, full-time teleworking at Hewlett-Packard saved almost 2.5 million round trips and avoided 85 million miles of road travel.¹²

⁴ Economics of Teleworking, Noel Hodson, 1992

⁵ Lisa Phifer. Business Communications Review. Hinsdale: Oct 2003. Vol. 33, Iss. 10; pg. 28

⁶ The Telework Coalition

⁷ The Telework Coalition

⁸ The price of efficiency, James C. Cooper, BusinessWeek, March 22, 2004, pg. 40

⁹ Handling the remote-office revolution, Johna Till Johnson. Network World. Framingham: Feb 16, 2004.

¹⁰ The FactPoint Group, 2008

¹¹ Economics of Teleworking, Noel Hodson, 1992

¹² The FactPoint Group (2008)

A greater return on investment

A desktop PC that used to cost \$2,000 three years ago is under \$500 today, and the price of portable PCs has dropped even more dramatically. As mobile computing has become more cost-effective and popularly embraced, WiFi-enabled laptops, ultra-portable PDAs and 3G cellular smartphones have overtaken the predominant business role of traditional desktops. At the same time, the subscription costs for residential broadband service have decreased to \$25-\$50 per month. As a result, the number of high-speed connections in U.S. households more than doubled—from 10.7 million to 22.3 million between 2001 and 2003 alone, according to Yankee Group¹³. Many more employees can be cost-effectively equipped to work anywhere, any time

By implementing teleworking, businesses inherently support operational continuity. The need for remote business continuity could be triggered by natural disasters, terrorist activities, pandemic threats, or even something as simple as a snow storm, power outage, or any other event that keeps workers from getting to the office. Disruptions to normal business operations often result in missed opportunities, lost revenue and a damaged reputation. Remote access for teleworkers is crucial for any effective disaster recovery plan.

Working green

Teleworking dovetails into corporate initiatives for “working green” by reducing emissions due to employee commuting, enhancing brand image and community relations, as well as customer and employee loyalty. A worker who telecommutes just one work day automatically reduces their weekly emissions by 20%. Teleworking initiatives by Hewlett-Packard and IBM alone respectively reduced 28,000 and 50,000 tons of annual carbon dioxide emissions.¹⁴

Inherent Risks of Teleworking

Without proper security measures in place, anytime, anywhere access introduces a number of risks for organizations. For example, unsafe user behavior can leave sensitive corporate information behind on a public machine, easily accessible to curious outsiders. More serious risks can come from viruses that may be inadvertently transmitted from an infected end-user device to other computers on your corporate network. The biggest risk comes from sophisticated malicious hackers. They may launch a full-fledged attack against your company in an attempt to hijack your computing resources and sabotage your operations and reputation.

A remote user’s access device might be a home computer, a friend’s laptop, a shared computer on another company’s network, a wireless PDA, a smartphone or a public kiosk. This remote user device tends to be the weakest point of security, due to non-technical users’ inexperience and lack of IT control over the configuration settings and software updates. It is subject to a number of potential risks, including improper system or networking settings, or lack of the latest operating system or security updates. The remote device may be subject to a virus or a worm infections, Trojan horses and zombies.

Evaluating risks to networks and remote devices

Without IT oversight, home computers, personal laptops and mobile devices are more likely to be improperly configured for file and printer sharing, potentially exposing sensitive information to roommates, spouses and children. Teleworkers may not be using the latest operating system or application software. They may not have installed the latest security updates or kept up with their anti-virus definitions. All-in-all, personal devices are more likely to get infected by viruses or malicious code than corporate devices. And infections

¹³ Telecommunications; What’s On? The battle among broadband providers has moved to a new arena: content Peter Grant. Wall Street Journal. (Eastern edition). New York, N.Y.: Mar 22, 2004.

¹⁴ FactPoint Group, 2008

are slower to be detected and cleaned up on personal devices. Teleworkers increase corporate risks by potentially infecting other corporate machines and by spreading infections to customers and business partners.

Worms and viruses cause damage by slowing down infected systems and networks, corrupting files and applications, and stealing bandwidth. Frequently, worms and viruses spread by emailing themselves to everyone in a user's contact lists or by exploiting network connections. Worms often install a back door on the infected computer that can later be used by spammers for sending junk email or to infect other unauthorized traffic on the network. Although most viruses are successfully controlled by corporate anti-virus software, they still pose significant risks to personal device users.

Trojan horses and zombies are malicious processes disguised as familiar objects, such as shareware programs, pictures or music files, so that even educated users feel safe launching them. Both Trojan horses and zombies may be dormant until a predefined event occurs and then are controlled by a remote hacker. For example, some Trojan horses let attackers control infected PCs remotely. Unless appropriate information security products are deployed, hackers can use this type of malicious software to access corporate resources through an unprotected VPN tunnel, unbeknown to the authorized user.

Additional risks come from the nature of home computing environments. Today, many home computers are connected to wireless home networks (based on IEEE 802.11 wireless LAN standard). Most wireless network equipment is shipping with Wired Equivalent Privacy (WEP) security features turned off (to simplify installation), and many non-technical people do not turn on even rudimentary encryption and authentication available with WEP. Since wireless networks extend outside of the physical property boundaries, anyone just outside of the building can eavesdrop on traffic going through the wireless network or access file shares. Furthermore, sophisticated hackers can easily defeat WEP by exploiting its widely publicized security flaws.

With always-on broadband connections, hackers can take their time penetrating a remote device. Unless products like a personal firewall are properly deployed, port scans, other hacking attempts and intrusions can go undetected for a long time. And hackers can exploit all open ports to steal resources or to damage unprotected connected systems.

SonicWALL Secure Remote Access and Network Security Solutions

In these challenging economic times, businesses are tasked with doing more for less. IT runs the security risk of ineffectively allocating diminishing IT budget resources that could be reapplied in strengthening other security initiatives. To prevent this, IT is increasingly open to simpler, well engineered, yet cost-effective security solutions. Yet traditional "status quo" vendors continue to offer solutions of greater complexity and cost, but without correspondingly greater value. When selecting secure remote access solutions, IT now has a clear alternative to over-priced vendors, without compromising performance or value.

SonicWALL® is committed to providing companies of all size with security solutions of equal or greater value at a significantly lower total cost of ownership. SonicWALL is uniquely positioned in the industry to eliminate costs out of building and running secure networks by strategically reducing costs associated with:

- Operational performance: by delivering elegant, high-utility, real-time security solutions that integrate leading-edge software intelligence with high-performance state-of-the-art commercially available chipsets delivered on industry standard hardware platforms
- Implementation: by providing clientless and thin-client solutions that simplify setup and distribution while seamlessly fitting into the most demanding network infrastructures
- Management: by delivering intuitive, globally-managed, centrally-administered control
- And yet, SonicWALL solutions do not sacrifice performance for cost-efficiency. SonicWALL streamlines the complexity out of secure remote access, freeing resources to enhance productivity

and profitability. SonicWALL has strategically positioned itself as an industry leader in pioneering secure teleworking solutions for organizations of all sizes by enabling the managed integration of its award-winning Secure Remote Access, Network Security Appliance and Global Management System product lines.

SonicWALL Secure Remote Access solutions feature the SonicWALL SSL VPN Series for small-to-midsize business (SMB), and the enterprise-leading SonicWALL Aventail® E-Class SSL VPN Series. SonicWALL Aventail E-Class SSL VPNs and SonicWALL SSL VPNs for SMB deliver flexible, scalable cross-platform solutions for secure remote access, disaster recovery, wireless networking and secure extranets, extending clientless mobile access over standard Web browsers to laptops, wireless PDAs and smartphones with unsurpassed granular control. SonicWALL E-Class NSA and NSA solutions feature integrated site-to-site IPSec VPN functionality.

SonicWALL Secure Remote Access

The SonicWALL Secure Remote Access (SRA) Series provides small-to-midsize business (SMB) teleworkers with an easy, affordable and scalable solution for clientless secure remote access to email, files, intranets, applications, remote desktops, servers and other wired or wireless network resources, over a standard Web browser.

SonicWALL Virtual Assist provides a clientless remote support tool for SonicWALL SSL VPN that enables an IT technician to assume control of a teleworker's PC or laptop in order to provide technical assistance. With the teleworker's permission, the technician can gain instant access to the computer using a Web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client.

SonicWALL Virtual Access is a remote PC control tool that enables authorized end-users to gain secure remote access to their unattended Windows-based computers from anywhere. Users simply need to install the Virtual Access agent onto a Windows PC with Internet access and, as long as that PC has a connection to the SonicWALL SSL VPN, the user can connect to that PC from anywhere they have an Internet connection. This is especially useful for remote employees who have the need to connect back to a home office computer or small branch office PC that is not normally connected to the LAN.

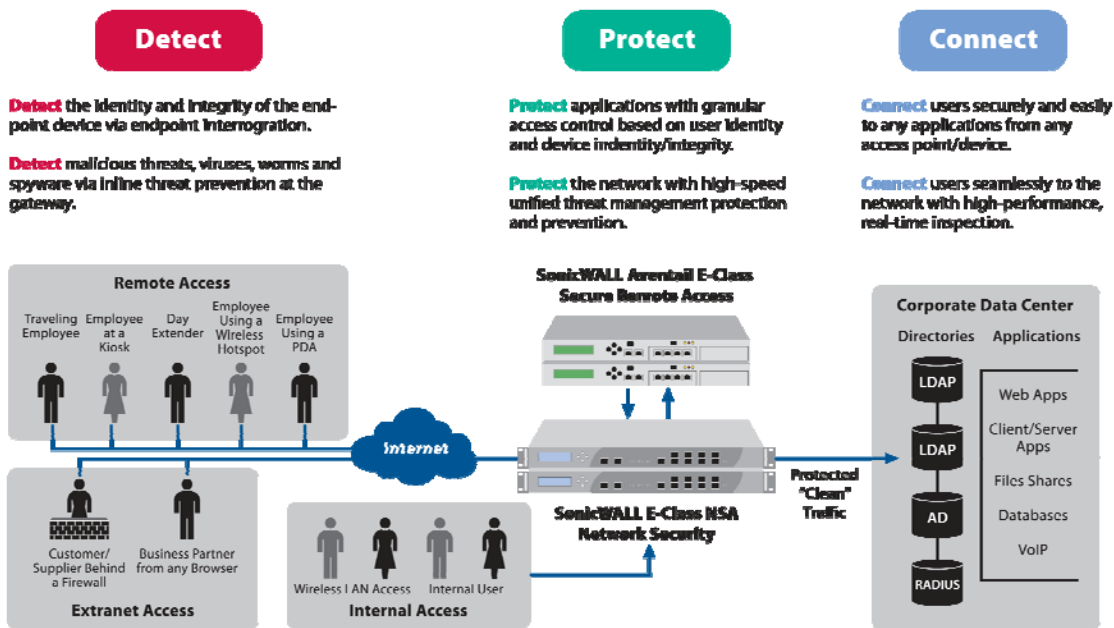
SonicWALL Aventail E-Class Secure Remote Access

Easy-to-use and manage, the award-winning SonicWALL Aventail E-Class SRAs detect the identity and security state of remote devices, protect against unauthorized access by enforcing granular policy, and connect Windows, Macintosh or Linux users seamlessly to mission-critical enterprise resources, delivering an optimal return on technology investment.

SonicWALL Aventail End Point Control™ (EPC) interrogates every endpoint device to check for specific criteria or attributes needed to adhere to security policy, such as running applications, domain membership, certificates, files, and common anti-virus, anti-spyware and personal firewall applications. SonicWALL Aventail E-Class SSL VPNs offer an array of flexible add-on modules to fit the needs of any enterprise or distributed business:

- SonicWALL Advanced EPC™ enables "virtual" Windows sessions that are automatically and thoroughly removed when ended; purges cache, downloads, cookies, history and passwords; and eases policy management with predefined anti-virus, personal firewall and anti-spyware profiles.
- SonicWALL Aventail Connect Tunnel™ provides an "in-office" experience for IT-managed devices.
- SonicWALL Aventail Connect Mobile™ offers true "in-office" experience for mobile PDA devices and smartphones.
- SonicWALL Aventail Host Access Modules™ support best-of-breed terminal emulation over SSL VPN.

- SonicWALL Aventail Native Access Modules™ provide native protocol access to server-based Citrix applications and Windows Terminal Services sessions over SSL VPN sessions without any additional configuration.
- SonicWALL Aventail Spike License™ acts as a disaster recovery “insurance policy” for future increases in remote users.
- SonicWALL Aventail Advanced Reporting™ delivers powerful analysis of remote access to your resources.



SonicWALL Clean VPN™

The SonicWALL Clean VPN™ solution unites next-generation SSL VPN and Next-Generation Firewall technologies to enforce granular application-layer access policies while comprehensively inspecting all traffic at the gateway, all the while correlating event information to streamline and enhance security efficiencies.

To add a layer of UTM protection to the SonicWALL Clean VPN solution, a SonicWALL Network Security Appliance (NSA) or E-Class NSA component could be deployed in conjunction with the SSL VPN component. SonicWALL's multi-core NSA architecture and patented Reassembly-Free Deep Packet Inspection technology delivers ultra high-speed deep packet inspection, intrusion prevention, gateway anti-virus, gateway anti-spyware, content filtering and Application Intelligence and Control capabilities. The SonicWALL NSA component ensures that all traffic is scanned in real time and decontaminated before entering the corporate network.

Finally, the SonicWALL Global Management System (GMS) component allows administrators to configure and manage their entire Clean VPN implementation from a single management interface. SonicWALL GMS delivers a flexible, powerful and resilient platform to centrally manage and rapidly deploy SonicWALL appliances and security configurations. In addition, it provides centralized real-time monitoring, and delivers comprehensive policy and compliance reports for even the most stringent auditing and regulatory compliance requirements.

Conclusion

Economic benefits and competitive pressures are forcing enterprises to enable workers to work more places more often. Users' own expectations for anywhere access reinforce this need. For economic and technical reasons, older IPSec-based technology is no longer adequate to support the nearly constant need for secure anywhere access. By addressing the IT need for advanced security as well as the end-user need for convenient, flexible access, SonicWALL secure remote access solutions offer today's best choice for remote worker productivity. Every day, teleworkers around the globe depend on SonicWALL solutions, enabling them to securely and cost-effectively access protected network resources from the broadest range of remote locations and devices of any SSL VPN vendor today. SonicWALL delivers powerful, granular and complete remote access, without escalating infrastructure costs or complexity. SonicWALL Secure Remote Access and Network Security solutions offer easy, flexible access options to secured resources and reduce companies' information security risks. By extending secure remote access from more places and to more resources at a low total cost of ownership, SonicWALL increases productivity for teleworkers and all mobile and remote users.



SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com

©2010 SonicWALL is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. 06/2010