Secure Telecommuting for Shared Broadband Access Points

SONICWALL

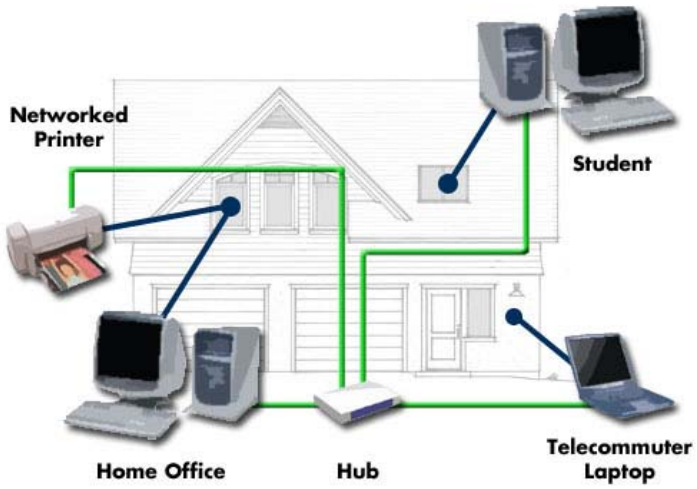
Introduction

If you're one of the growing number of companies whose workers telecommute from home via virtual private networks (VPNs) and broadband Internet services, you know that these remote endpoints present a potential security risk. But you may not be aware that even conventional VPN firewalls, designed to protect telecommuters against Internet-born intrusions, are not enough to ensure the integrity of the VPN link. When securing remote endpoints, network administrators need to look beyond the employee's computer alone and consider the company it keeps. Many telecommuters now share their broadband connections with other household members. These home networks offer a vulnerable "back door" that can expose your VPN and corporate network to a range of attacks--attacks that traditional VPN firewalls don't always prevent.

This white paper explores the risks posed by home networking and shared broadband access, and explains why conventional telecommuter firewalls fail to provide complete protection. The paper then describes a new-generation VPN firewall, SonicWALL's TELE3 TZX with an integrated 4-port switch that provides the first comprehensive, cost-effective solution to the problem. The TELE3 TZX isolates an employee's corporate computer from other household systems, shielding their VPN connection and the corporate network from vulnerable home networks. With the TELE3 TZX, network administrators can finally secure VPN endpoints easily and economically, even in heterogeneous home network environments.

Telecommuting Today: Risks on the Rise

A rapidly growing number of workers (tens of millions in the U.S. alone, according to recent estimates) now spend at least part of their time telecommuting from home. Of these, an increasing percentage are using VPNs and broadband connections to access their corporate networks. Many of these workers, moreover, share their residential broadband connection with other household users, linked together by a home network.



It is not uncommon for households with multiple computers to share resources such as printers, scanners, and Internet connections by setting up a home network. These type of unprotected and unmanaged home networks represent a significant risk to businesses supporting telecommuting.

The home networks may be as simple as two computers connected by a hub. They may be as sophisticated as a large multisegment LAN with switches, routers, multiple PCs, file servers, printers and other shared resources. They may be wired or wireless. In any case, the problem is the same. Since all computers on the network are connected directly or indirectly to the VPN appliance, any attack that compromises any machine on the network can put the VPN and, through it, your corporate network in jeopardy.

The threats can take a variety of forms. Most consist of malicious code: viruses, worms and Trojan Horses. Such “malware” can invade home systems through any number of channels, including direct penetration of the “always-on” broadband connection, as well as e-mail attachments, software downloads and active Web content such as Java applets or ActiveX controls. Malicious code might also be surreptitiously planted on home computers by hackers exploiting security holes during home user activities such as peer-to-peer file exchange, networked multiplayer gaming, instant messaging and home videoconferencing.

Once on the PC, malware could pass through the VPN tunnel and use host scanning to find and infect vulnerable machines on the corporate network. Or hostile code could “zombify” the home PC and launch denial-of-service (DOS) attacks on the company network via the VPN. Another

danger comes from attacks such as those perpetrated by the Back Orifice and Subseven trojans, in which malicious content infects the home computer and allows a hacker to commandeer the PC. The hacker could then infiltrate the internal corporate network, assuming all the rights and privileges of an authorized user. The well-publicized October, 2000 attack on Microsoft, resulting in the theft of vital source code, is believed to have taken place in just this fashion.

Of course, the first scenario above (hostile code spreading to corporate systems) might be prevented by anti-virus software on the company network. But even assuming the latest AV software running in all the right places on the LAN, the network would still be vulnerable to "first strike" infections by new, unrecognized code. Nor would such anti-virus software protect against the second and third scenarios (DOS and hacker intrusions launched from a household member's PC).

Wireless home networks present a special risk. Unless fully secured by measures such as encryption and password protection, such networks are vulnerable to "drive-by" hackers, who can tap into the network over the airwaves from points near the house (even from cars traveling through the neighborhood). Having penetrated the network, wireless hackers can then launch any of the attacks described above.

Yet another danger comes from would-be intruders inside the home, such as a telecommuter's own mischievous child or roommate. Working from their own PCs on the home network, such in-home hackers could gain unrestricted access to the VPN and could do serious harm, whether motivated by actual malice or just idle curiosity.

Whatever the modus operandi, any of the above attacks can have disastrous consequences, resulting in:

- Destruction or damage of valuable data
- Theft of sensitive information
- Disruption of operations and downtime (e.g., by crashing systems or degrading network performance)

The financial impact is often considerable. Several high-profile attacks such as the Nimda and Code Red trojans have cost individual companies millions of dollars, including the expense of recovery, downtime and lost business. According to Information Week, the total cost of virus attacks and computer cracking ran to $266 billion in 2001.

Why Conventional Solutions are Inadequate

Recognizing that always-on broadband connections are tempting targets (and available around the clock) for hackers, companies have increasingly turned to security appliances that combine VPN and firewall capabilities. Installed at the telecommuter's premises, such devices simultaneously perform VPN encryption and defend the client computer against Internet-borne intrusions. Many companies also guard the telecommuter's computer with measures such as anti-virus and attachment blocking.

The trouble with these traditional approaches is that they focus only on the telecommuter's computer and fail to take into account the other machines and users on the home network. Most traditional VPN firewalls, for example, make no distinction among the various computers attached to them (i.e., between trusted workers and untrusted household members). Once the VPN tunnel is up and running, it's an open door that any device or user on the home network can walk through.

Even those VPN firewalls that do feature user-level authentication (ULA) don't fully solve the problem. Whether using passwords, certificates, secure IDs or other techniques, ULA does allow the VPN firewall to distinguish between individual home network users (based on their IP addresses), allowing authorized workers to enter the VPN and blocking unauthorized home users. But such safeguards can be bypassed by hackers (outside or inside the home) using IP spoofing, thus accessing the VPN by passing an unauthorized home machine off as an authorized one.

What to do, then? Extend corporate security policies and protections to the entire home network? That's out of the question, being neither appropriate nor even possible in most cases. How about detaching the telecommuter's work computer from the home network, and installing two separate broadband connections and Internet accounts--one for the telecommuter, one for other household members? That's both expensive, requiring costly duplication of services and equipment, and highly restrictive, preventing the household from sharing appropriate network resources such as printers and file servers.

Instead, the real answer lies in isolating the telecommuter's work system and VPN connection from other systems on the home network, while still allowing all systems to share a broadband connection as well as appropriate resources. Yet there is no practical, cost-effective, straightforward way to perform this isolation with traditional VPN firewalls. Using conventional equipment, the only way to achieve such separation while still providing firewall protection to all machines would be to deploy

two firewalls: an outer firewall to which home users attach, and an inner VPN firewall, serving as the VPN endpoint, to which the telecommuter connects. But this is hardly an ideal solution. It's expensive, requiring two firewalls instead of one. It also demands that the home (i.e., outer) firewall allow VPN tunnel negotiation and traffic to pass through, which may necessitate some additional configuration problems. Alternatively companies could issue just one firewall for use by the telecommuter only. Other home users would then work outside the firewall, connecting directly to the broadband access device (e.g., DSL modem). But leaving home users to surf the Internet without any firewall protection ultimately defeats the purpose since it would force the household purchase its own, second firewall.

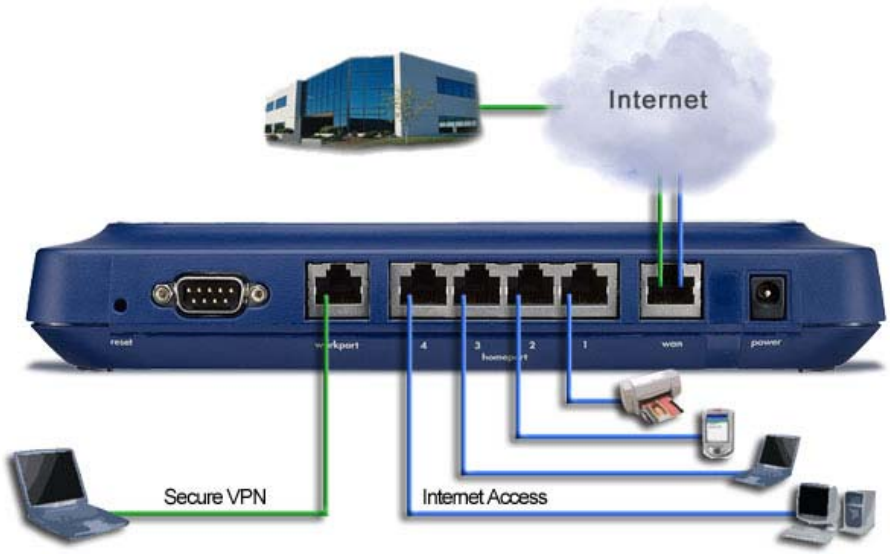
True Isolation, Trusted Connection: The TELE3 TZX

SonicWALL's TELE3 TZX, based on third generation SonicWALL firewall/VPN technology, is the first VPN firewall designed to address the risks posed by telecommuters sharing a broadband connection with home networks. The TELE3 TZX uses a unique WorkPort™ architecture that effectively isolates the telecommuter's work computer and VPN from other home systems, while at the same time enabling all machines to share a broadband Internet connection and local network. In essence, the TELE3 TZX places a hardened firewall *not only between the home and the Internet but also between the two segments of the home network*, separating trusted workers (company telecommuters) from untrusted outsiders (other household members and their machines). In other words, the TELE3 TZX extends enterprise-class security not only to the home/Internet boundary but also into the telecommuter's home itself--something no previous product has done.

The TELE3 TZX is equipped with two ports--the "WorkPort" and the "HomePort." The two ports are physically distinct and split the home network into two different subnets, or "Trusted Zones". The WorkPort connects to the telecommuter's computer and provides a secure VPN connection to the telecommuter's corporate network. The HomePort provides one port to the home computer, or for multiple computers, the TELE3 TZX's integrated switch can support four ports. The HomePort provides access to the Internet--but not to the VPN.

Like incoming traffic from the Internet, all traffic between the two zones is controlled by the TELE3 TZX's hardened stateful packet inspection firewall technology. The TELE3 TZX thus provides a level of *physical* (layer 2) security that exceeds the higher-layer security of ULA schemes (layer 3) alone. By default, the firewall separating the two zones allows only one-way traffic: the work zone can access the home zone, but not the reverse. Both ports permit full access to Internet, sharing a single

public IP address, by virtue of network address translation (NAT) performed by the TELE3 TZX. By partitioning the home network in this way, the TELE3 TZX ensures that any attacks targeting or launched from the home computers cannot penetrate the work computer or corporate VPN.



The TELE3 TZX creates two "trusted zones" by creating a firewall between the HomePort™ and the WorkPort™. This additional layer of manageable protection eliminates the risk of unauthorized access through the corporate VPN, while still maintaining connectivity to home network resources.

The TELE3 TZX can be configured for other usage patterns as well. For example, the HomePort could be given access to a shared device, such as a printer, attached to the WorkPort. But for ultimate IT control, SonicWALL recommends that the default, one-way configuration be maintained and that all shared resources be placed on the HomePort, where they can be accessed by all computers without risk to the work computer or VPN.

In addition to isolating and securing the work zone, the TELE3 TZX also helps to protect the home zone from Internet-born threats. Protections include the Internet firewall, of course, and also optional countermeasures such as enforced network anti-virus and automatic content filtering. HomePort firewall functions are independently configurable to support a range of usage scenarios. For instance, if a home user wanted to set up a

PC as a public ftp or Web server, the HomePort could be configured to allow such incoming traffic.

TELE3 TZX Product Details

The TELE3 TZX has multiple auto-negotiating 10/100 base-T ports. In addition to the single WorkPort connection and the four HomePort connections supported by an integrated four-port switch, a WAN port provides external connection to a DSL modem, cable modem or routing device. Users can connect any industry-standard Ethernet hub or switch to any of the ports, allowing even more devices to share the TELE3 TZX. The TELE3 TZX supports NAT, along with DHCP, PPPOE, static IP and L2TP protocols.

- The TELE3 TZX's high-performance ICSA-certified firewall can process Internet or intrazone traffic at over 75 Mbps.

- SonicWALL's proprietary VPN accelerator ASIC boosts encryption speeds to 20 Mbps--significantly faster than most other home VPN appliances and enough headroom to take full advantage of new, faster home broadband technologies in the future.

- On the WorkPort side, the TELE3 TZX provides IPSec VPN and supports up to five simultaneous tunnels. User level authentication provides an extra measure of security when establishing the VPN.

- The TELE3 TZX features an integrated 4-port MDIX switch on the HomePort that eliminates the need for an external hub or switch, allowing multiple networked devices to connect directly to the TELE3 TZX. The MDIX feature automatically and transparently detects and corrects incorrectly wired cables such as cross-over cables, making network installation substantially simpler and less expensive. This added level of convenience eliminates configuration and compatibility issues that occur in deployments.

- The TELE3 TZX supports bandwidth prioritization by physical or logical port and protocol. So, for instance, greater bandwidth priority might be given to the WorkPort over the HomePort, or to particular applications, such as e-mail or Web browsing (based on logical port and protocol).

A Complete Solution

In addition to its firewall and VPN capabilities, the TELE3 TZX includes integrated support for a variety of value-added security features. SonicWALL Network Anti-Virus, available by subscription, provides automatic policy enforcement and deployment of McAfee anti-virus signature software, assuring that remote users receive and are running the latest updates. The anti-virus service also includes attachment-blocking capabilities, which can reduce exposure to new malicious content even before signatures are released.

SonicWALL's Automatic Content Filtering, also available by subscription, enables network administrators to block access to selected Web sites. Administrators can therefore ensure that remote employees are subject to the Internet content restrictions in effect at the company site. Both SonicWALL Network Anti-Virus and Content Filtering services can be selectively applied to either the WorkPort or HomePort.

Implementing a widely distributed and secure telecommuting program requires a policy-based management platform, allowing administrators to rapidly and easily provision security policies to a fast-changing remote work force. To that end, the TELE3 TZX is supported by SonicWALL's Award-Winning Global Management System (GMS), which enables network administrators to centrally manage employee's remote firewalls through encrypted security tunnels. GMS can be used to manage all aspects of the TELE3 TZX, including configuration, deployment, logging, monitoring and remote installation and upgrading of software and add-on features. Alternatively, TELE3 TZX set-up and configuration can be performed locally (through the WorkPort only), using an intuitive browser-based GUI. Whether performed centrally or locally, installation and configuration are straightforward and take no more than a few minutes.

SonicWALL's family of VPN concentrators makes it easy to fit the TELE3 TZX into companies' existing infrastructure and scale up telecommuting programs, even to thousands of remote endpoints. SonicWALL's GX 650 Gigabit Ethernet VPN Concentrator, for example, can terminate up to 10,000 VPN tunnels. Terminating head-end VPN connections using concentrators, as opposed to corporate firewalls, has several advantages. It offloads the firewall of a substantial processing burden, allowing for better VPN and firewall performance. And it offers the benefits of

seamless centralized management delivered by SonicWALL's Global Management System.

A Secure Future for Home Telecommuting

Inevitably, home networks--incorporating not only PCs but also entertainment devices and even household appliances--will become the norm, rather than the exception. For companies relying on traditional VPN firewalls only, residential networking is likely to bring unending headaches, exposing remote access points to myriad and uncontrollable risks. Fortunately, the TELE3TZX gives network administrators comprehensive control over their dispersed network in an easy-to-deploy, easy-to-manage and cost-effective solution. The TELE3 TZX is the first such product to harden telecommuter VPN connections not only against direct Internet threats but also those that arrive via the "back door"--the residential network itself. With the TELE3 TZX, network administrators can rest assured that their VPN endpoints are secure, even in dynamic mixed-use home environments.