

Securing the Everywhere Network

Rethink your security in the age of the disappearing network perimeter

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Table of Contents

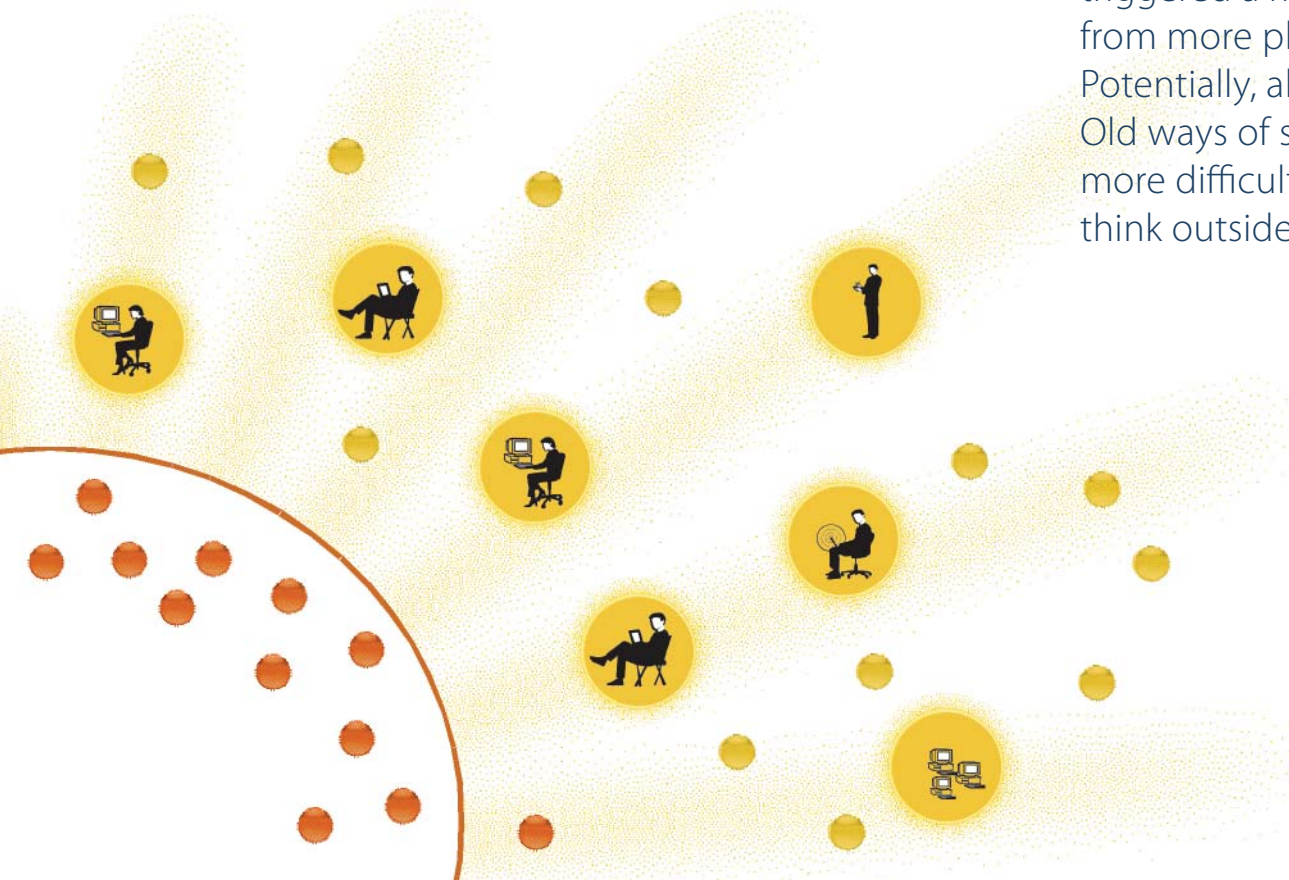
Overview	1
A new world: the fundamental shift in remote access	2
Everywhere networking: boon and burden	3
The impact: users and devices are harder for IT to control	4
The everywhere network is insecure	5
Securing business on the everywhere network	6
Conclusions	7

Overview

Think you can fully protect your business resources with a traditional hardened LAN?

Better think again.

In today's business environment, the network is everywhere. Dramatic advances in remote access technology have triggered a mobile revolution. More people are working from more places using more devices than ever before. Potentially, all users are remote and all devices unsafe. Old ways of securing corporate resources have gotten more difficult, expensive and ineffective. You've got to think outside the perimeter.



A new world: the fundamental shift in remote access

New Web 2.0 mobile devices, services and business solutions are introduced every day. VoIP has turned even phone calls into another form of remote data access. Workers can get a 3G wireless broadband Internet connection to their laptop, PDA or smartphone from virtually anywhere.

This shift has created a new world of doing business. Work happens wherever you are—at field offices or home offices, partner sites or manufacturing sites, airports or hotels. “The office” is no longer restricted to a specific site behind a hardened perimeter. Business networking is now everywhere networking.



*The traditional network
perimeter is disappearing.*

Everywhere networking: boon and burden



Everywhere networking streamlines facilities and energy costs, eliminates commuting time and expenses, builds global business partnerships, broadens markets and staffing pools, shortens customer response times, and helps attract and retain skilled workers. As remote access plays a bigger role in keeping your business competitive, making sure your core systems are available and reliable from anywhere is more important than ever.

But this boon puts a burden on security. Executives and managers expect full access to files and applications over standard Web browsers. Accountants require access to sensitive financials on remote data center mainframes. Salespeople demand secure access from PDAs and public kiosks at hotels, airports and convention centers. "Outside" partners, vendors and consultants need secure access to "inside" application resources from "outside" devices, traversing internal and external firewalls.

***Over 90% of the workforce
went mobile or remote during 2006*.***

The impact: users and devices are harder for IT to control

Laptops and other mobile devices are replacing hard-cabled LAN desktops. IT-issued and personal mobile devices move in and out of the network, traversing internal and external firewalls. It's harder for IT to control what users do with their mobile devices, and how these devices expose business data to security threats.

With everywhere networking, any user or device is potentially unsafe, whether they connect remotely or directly into the LAN. The most dangerous threats can often come from within. IT is overwhelmed controlling end-users and their remote endpoint devices. Costly attempts at hardening an everywhere perimeter with "smart" infrastructure are ultimately ineffective. From a business or technology standpoint, it's time for new strategies.

***67% of businesses reject useful new technology
because of security fears.****



The everywhere network is insecure

Today's everywhere network connects employees, partners and customers over multiple Internet and intranet, private and public, wired and wireless networks. In the everywhere network, the remaining perimeter concentrates around application resources in the data center. While perimeter firewall defenses still provide a crucial layer of protection at the gateway, they can't do it all everywhere.



Web-based global access to business resources is a lot like e-commerce. To keep it safe, take a page from the playbook of successful e-business innovators. To secure online transactions, they apply technologies like Secure Sockets Layer Virtual Private Networking (SSL VPN).

How can anyone keep it safe?

Securing business on the everywhere network

Instead of just securing your resource perimeter, you need to secure communications to those resources. To secure communications, you need to know you can trust each user and their endpoint device, and have policy in place for permitting access only to appropriate resources.

Ideally, you should confirm every user's identity, whether they are "inside" or "outside" the traditional LAN, and scan every node device to check its integrity (for instance, whether it has a valid device certificate or current anti-virus signature). Then, and only then, can it be advisable to give users policy-based access to resources behind your firewall. To accomplish all of this, you need a comprehensive remote access security solution using SSL VPN.



60% of businesses want security "health" checks of any node before connection.*

Conclusions



Today's business networking is done everywhere. Traditional hardened perimeter solutions just can't secure it all. Secure remote access technology from SonicWALL enables business communications on the everywhere network by:

- confirming the identity and security state of each endpoint device
- controlling admission based on the level of trust for remote users and their devices
- permitting access based on the resources those users are authorized to use.

How Can I Learn More?

- Download the Nemertes Whitepaper “The Center is Everywhere”
- Listen to an archived Webcast
- Opt-in to receive SonicWALL Newsletters

For feedback on this e-book or other SonicWALL e-books or whitepaper, please send an e-mail to feedback@sonicwall.com.

Forward to a Friend

About SonicWALL

SonicWALL® is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high performance business network. For more information, visit the company Web site at www.sonicwall.com.

*Statistical references: Nemertes Research