



## The evolving branch office

With nearly 90% of companies operating a virtual workplace and large percentages of employees working away from home office or the primary data center (if there is one), IT must support ever-increasing numbers of remote and virtualized workers. So, when creating or renewing the branch network infrastructure, organizations must pay close attention to shifting IT architectures, staff usage habits, and performance expectations. This E-Guide details the security and optimization best practices for various types of branch offices.

*Sponsored By:*

 The logo for SonicWall, featuring the word "SONICWALL" in a bold, blue, sans-serif font with a registered trademark symbol. A blue swoosh underline is positioned above the letters "WALL".



# The evolving branch office

## Table of Contents:

[Security and optimization for the backhauled branch](#)

[Security and optimization for the direct-to-Internet branch](#)

[Security and optimization for the micro-branch](#)

[Resources from SonicWALL](#)

## Security and optimization for the backhauled branch

By John Burke

With nearly 90% of companies operating a virtual workplace and large percentages of employees working away from home office or the primary data center (if there is one), IT must support ever-increasing numbers of remote and virtualized workers. So, when creating or renewing the branch network infrastructure, organizations must pay close attention to shifting IT architectures, staff usage habits, and performance expectations.

With fixed-location offices of any significant size (more than 10 employees, say), IT must decide whether to provide the office with direct connectivity to the Internet and whether to connect it to the WAN (for organizations large enough to have one, that is).

In this article, we'll examine branches without direct connection to the Internet and with direct connections to the WAN. In these "backhauled" branches, all Internet traffic gets routed via the main data center or network hub, through the WAN, to the branch. With this approach, branch designers need to consider both security and optimization.

IT should assume that centralized firewalls, malware filters, and IDS/IPS systems have screened Internet traffic going to the branch. Branch security devices should focus on the branch itself -- i.e., protecting computers there (including servers, if there are any) from one another. Desktops remain the main vector for malware infections and security breaches, after all. If removable media or a Trojan webpage infect one desktop, IT must make sure others aren't immediately in danger. The success of attacks like Conficker in subverting host defenses makes network security a necessary adjunct to host-based security.

So, if the organization is using network access control (NAC), branch network closets should be hosting some of the NAC equipment. If NAC is not on the menu:

- The simplest (but most extreme) solution is for IT to simply block all direct inter-desktop communication. For example, some organizations assign a separate VLAN to each desktop system, forcing any traffic headed from desktop to desktop to go through a router, which can do basic filtering, and possibly other gear, such as an IDS/IPS system, firewall, or unified threat management (UTM) box.
- More permissive organizations can set switch ACLs to allow systems to speak to one another, but only over specific, approved ports and protocols.

IT may also have to protect each branch from other branches. Although any organization with a traditional hub-and-spoke WAN should be watching and filtering the WAN at its center(s) for malicious traffic, the rise of any-to-any WANs built on MPLS render this steadily less sufficient.

The branch network stack should also -- to whatever degree is dictated by overall policy -- be providing a logging/auditing point for tracking use of the network. The branch router provides a point to log traffic patterns and watch for anomalous behavior and if a PC is over taken and turned into an army of spam-spewing zombies, or tries to infect other PCs, this is where IT can see.

Of course, security is only half of the picture; performance is the other. When user demands push past the performance or capacity limits of the existing WAN, IT has three choices: re-engineer systems to reduce demand, upgrade connections, or use optimization to make the most of existing bandwidth.

Optimization focused on caching and compression of file, backup and Web traffic is often critical to ensure that capacity is available for other applications. Likewise, traffic prioritization, shaping and conditioning ensures that bandwidth goes first to the applications the organization prefers, and that the link behaves as well as possible (e.g., by mitigating packet loss or adjusting each stream's packet sizes to allow for the needs of other applications). Protocol accelerations make LAN-friendly applications stop trying to treat the 3 Mbit WAN link like a 100 Mbit LAN connection. These accelerations typically emphasize cutting out roundtrips between clients and hosts.

IT can provide these functions using appliances in the branch connecting back to appliances in the main data center. Sizing the appliance to balance capacity and budgetary needs is the main challenge. Now, too, many carriers and service providers offer optimization as a service on WAN or Internet links.

Next up, branches connecting straight to the Net.

# SONICWALL VS SPIRALING TCO

## NO CONTEST

Tired of wasting IT budget deploying and managing so called best-of-breed network security and data protection solutions? If three-fourths of your budget is going toward the maintenance of these solutions, then your total cost of ownership (TCO) is spiraling out of control. But there's a smarter alternative—SonicWALL's high-performance network security, email security, and data protection solutions. SonicWALL is committed to improving performance and productivity by engineering the cost out of building and running secure networks. SonicWALL solutions strategically reduce the cost of acquisition, deployment, and management, providing you higher-performance protection at a lower TCO.

See how at [www.sonicwall.com/lowtco](http://www.sonicwall.com/lowtco)



NETWORK  
SECURITY



SECURE  
REMOTE ACCESS



WEB AND E-MAIL  
SECURITY



BACKUP AND  
RECOVERY



POLICY AND  
MANAGEMENT



PROTECTION AT THE SPEED OF BUSINESS™

## Security and optimization for the direct-to-Internet branch

By John Burke

When IT chooses to connect a branch to both the Internet and the WAN, it creates the "Direct-to-Net" branch: the WAN is only for traffic headed to internal hosts. Although this considerably reduces bandwidth demands on the WAN connections, it can complicate both security and optimization.

With no central pipe through which Internet traffic is channeled, IT has to screen it in every branch. This means firewalls, malware filters and IDS/IPS systems. Doing this via a stack of many single-purpose appliances in each direct-net branch can become daunting both financially and administratively. The alternatives for traditional in-house deployments are to combine security boxes into a unified threat management (UTM) appliance or to integrate security services into the router. A more recent option is to combine security and optimization layers. And, of course, the proliferation of security services on carrier connections, such as "firewall-in-the-cloud" offerings, shows a third path for securing branches.

As with the backhauled branch, direct-net branch security should focus on protecting in-branch systems and branches from one another and on providing an appropriate degree of visibility into the traffic in the branch.

The optimization picture changes, just as the security one does. In this context, with branches working as consumers of Web resources and no compression appliances at the far end of the connection, options for compression pretty much vanish on the Internet link. (It is possible to do one-sided compression of outbound Web traffic since Web browsers can decompress many things.) Caching remains important on both the WAN and the Internet links, even though it becomes less effective overall (i.e., for the entire organization). As the pool of users for which a caching appliance on either link can cache content shrinks, user requests result in fewer cache hits and more repetitive transmissions overall. WAN compression likewise -- working with smaller user pools decreases the opportunity for compressions.

Shaping and prioritization can apply to both Internet and WAN separately. Connections will be smaller, however, and each (WAN and Internet) has fewer traffic streams to manipulate in managing flow and so has fewer possible combinations to try in seeking the right balance: that is, less slack and wiggle-room to play with than on a single network link carrying all the traffic.

One problem that direct-branch connectivity exacerbates is management. By putting service-delivery points for security and optimization in so many more places, direct-branch increases the importance of management platforms that scale well and that offer policy-driven management of groups of appliances. Also, as users become more mobile among different branches, taking laptops from place to place, solutions that are user-sensitive must cope with that mobility gracefully.

Where optimization is application sensitive, separating Internet-mediated SaaS applications from WAN-mediated in-house applications makes it harder to balance the two at the desktop. However, direct-net improves the ability to deliver consistent performance from SaaS solutions. With a backhauled branch, performance is determined by both Internet and WAN performance; direct-net simplifies the picture and puts all users on a more equal footing.

---

As branch offices continue to proliferate (we expect growth rates to bounce back this year) while bandwidth costs continue to plummet and the use of SaaS spreads rapidly, we expect direct-net branches to increase quickly relative to backhauled connections. It will be essential for IT to approach questions of security and network performance up front, with a strategy that encompasses both varieties and with an expectation for coordinated, policy-driven management of all devices and/or services.

But what happens when there is no branch office and no WAN? Next up, micro-branches and mobile workers: what to do when there is no network closet.

## Security and optimization for the micro-branch

By John Burke

Nemertes sees a trend toward smaller and more scattered branches, driven by real-estate prices, green initiatives, and the rise of virtual workplaces enabled by effective unified communications. But even when a branch has no wiring closet -- when it's just a few people with desktops or someone working from home -- IT still needs to think about securing and optimizing the network.

Since the so-called "micro-branch" lives on the Internet and as a defining characteristic has no network infrastructure beyond a router, security and optimization have to be host-based.

The first thing to decide is VPN or no VPN?

Users coming into the corporate network via IPsec or SSL VPN get LAN-like access to applications, so they can see and use everything they could if on campus (assuming you configure the VPN to let them do so, that is). There is no guarantee of LAN-like performance, though. And VPNs can be tricky to get working for everyone, from everywhere, and are usually staff resource intensive, especially for the service desk and desktop management staff fielding "I can't get connected" calls. Outsourcing this is an option.

Without a VPN, IT must make sure any application that remote staff needs has a secure, Internet-accessible front end. Happily, most applications are already headed toward secure Web front ends, but not all are there, and some may not be easy to retrofit. IT should carefully assess whether it is better to speed up migration to Internet-friendly interfaces or to use a VPN or terminal services to provide comprehensive access.

It is important to note that the VPN will not make the end users' computers more secure unless they do all their work through it, including all Internet activity. If they do, they piggy-back on core network security. However, if remote workers use Internet services directly -- and this makes lots of sense for SaaS, Web searches, etc. -- then having the VPN does not add much to the security of the endpoint. In fact, the VPN can create on-site security problems for IT because it gives an "in" on the network to computers that are "in the wild."

If, as security trends in the last decade suggest is wise, IT treats all end-user computers as essentially wild -- untrusted -- then the VPN is just another bunch of untrusted computers. If IT judges off-site computers automatically less secure than on-premise, the VPN is a problem: IT needs to give access to inside applications and data while trusting these computers less and limiting/watching them more.

The VPN is thus a good place for a full network access control (NAC) solution. Beyond requiring authentication to access the network (kind of a given with VPNs anyway), an NAC system can do health checks on connecting computers to see whether IT has been able to keep their OS and application patching up to date and whether they are running antivirus and other security tools.

Once past the VPN question, IT must make sure micro-branch computers have antivirus/anti-malware scanning and additional Web security. Software/service hybrids are ideal, combining local site filtering with continuously updated green/yellow/red lists of good/iffy/known-bad sites.

Lastly, IT should equip remote computers holding sensitive data with whole-disk encryption, whether via OS functionality or a layered application. Here, the main caution is encryption key management.

On the optimization front, if it is needed, a soft client is the only option; optimized NICs or small-office/home-office routers may someday be available but are not for now. Such clients can do significant compression and some traffic conditioning. Ideally, they might be integrated with one or more security functions to cut down on the number of agents required per machine -- always a win for performance and manageability.

With all these endpoint solutions, centralized management and maintenance of the clients is key to their ongoing utility. Old, unpatched or non-updated security software might as well be turned off! Ideally, all tools will share a single policy definition mechanism. That is unlikely to be the case in most environments, so IT must be vigilant in setting policies consistently across all channels. IT should require that policies in each tool be able to use the groups defined in the enterprise directory, if there is one, to minimize redundant effort and the inevitable opportunities for things to get out of sync.

**About the Author:** *John Burke is a principal research analyst with Nemertes Research, where he focuses on software-oriented architectures and management. He develops and manages research projects, conducts strategic seminars, and advises clients. As an analyst, John draws on his experiences as a practitioner and director of IT to better understand the needs of IT executives and the challenges facing vendors trying to sell to them.*

*A frequent speaker, his career began at Johns Hopkins University, where he supported the engineering faculty in its use of computers in research and teaching. He moved on to systems and network administration at The College of St. Catherine, in St. Paul, Minn., and then to directing staff in voice, data, desktop and systems management at the University of St. Thomas, also in St. Paul.*

## Resources from SonicWALL



[Consolidate and Make Your Network More Secure and Stable](#)

[Network Security Solutions for the distributed enterprise](#)

[SonicWALL Centralized Management and Reporting](#)

### **About SonicWALL:**

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. Over one million SonicWALL appliances keep tens of millions of worldwide business computer users safe and in control of their data. SonicWALL's award-winning solutions include network security, secure remote access, content security, backup and recovery, and policy and management technology.