

SOPHOS' WS1000 WEB SECURITY APPLIANCE

EFFICIENTLY, EASILY, EFFECTIVELY, THE SOPHOS DEDICATED ANTI-MALWARE DEVICE KEEPS MALWARE FROM REACHING YOUR NETWORK.

By Barry Nance

January, 2007



Sophos' WS1000 Web Security Appliance is exactly what companies have been looking for – a high-performance, reliable, effective and easy-to-use answer to keeping malware off their networks. It thwarts virtually all malware without hindering or slowing clients' Web access.

Virus programmers are cyber vandals who waste bandwidth, delete files, throw egotistical messages on your screen and use your e-mail address book as a springboard for perpetuating themselves across the Internet. Spam authors waste your time and your productivity.

However, developers of spyware are even worse. Spyware programmers are cyber thieves who hijack your computers, steal your keystrokes, rifle through your files for password and credit card data and pepper your screen with advertisements every time you perform an Internet search.

Stopping spyware via gateways at each Internet connection point is clearly superior to cleaning it off individual server and desktop computers. Cleaning spyware at the desktop or on the server is tedious to administer and consumes computing resources that the client and the server should rather devote to your business. The gateway approach is cleaner, simpler to administer, more direct, more reliable and more effective.

Installing an anti-malware gateway between your network and the World Wide Web is the ideal way to combat spyware.

Network Testing Labs has created a special testing environment (see the Testbed and Methodology section of this review) for evaluating anti-malware products, and we're on a quest for the best. When we discovered that Sophos had released the new WS1000 Web Security Appliance, we invited Sophos to submit a unit for testing in our Alabama lab.

The most important criteria in our evaluation was the ability to identify and thwart all or virtually all spyware. We also looked for useful reports, timely alerts, ease of use and ease of deployment. Protecting our network from users who roam the Web too freely was our goal.

The WS1000 Web Security Appliance proved to be an accurate, quick and easy to use device. It turned aside virtually all spyware, and its effect on the responsiveness of our clients' Web experience was nil. **The WS1000 wins the appliance-based anti-malware Network Testing Labs World Class award.**

Preventing malware

With considerable speed and efficiency, the WS1000 Web Security Appliance keeps malware from getting onto your network. Focusing on HTTP and FTP traffic, the WS1000 analyzes Internet packets both for content and for source.

The WS1000 defends against spyware, viruses, Trojans, worms, adware and phishing attacks. To support its anti-malware device and keep its protection up-to-date, Sophos uses automated tools to continuously investigate billions of unique web pages. Every day, the vendor identifies more than 5,000 new malware-hosting Web sites, and it smoothly and unobtrusively updates customers' malware definitions every five minutes.

Table 1 shows the malware recognition success rate of the WS1000 Web Security Appliance. It identified and diverted an astounding 99% of the malware instances we tested with.

| <i>Sophos</i> | |
|--------------------------------------------------------------|------------------|
| <i>WS1000 Web Security Appliance</i> | |
| <i>Success rate against a suite of 150 malware instances</i> | 99% (148 of 150) |

Table 1. Ability to stop malware.

Not only does the WS1000 quickly thwart malware, it keeps any existing malware already on a client machine from "phoning home," i.e., sending your private data back to

the malware author or sponsor. Such infection can occur when employees take notebook computers on the road and access the Internet through unprotected Internet access points.

Client responsiveness

The speed with which an anti-spyware gateway product processes Web traffic governs the responsiveness that users experience as they browse. Even the most accurate anti-spyware tool is useless if it slows content delivery to a glacial crawl.

Table 2 shows the performance of the WS1000 device. The WS1000 processed Internet traffic quickly enough that our users noticed no degradation of their Internet experience.

| | <i>Latency</i> | <i>Proxy transaction rate</i> |
|--------------------------------------|----------------|-------------------------------|
| <i>Sophos</i> | | |
| <i>WS1000 Web Security Appliance</i> | 15 ms | 125 trans/sec. |

Table 2. Latency and throughput (performance) results.

In our accuracy and performance tests, we used fresh material for each test to negate the effects, if any, of caching by gateways or other devices. We reasoned that most people browsing the Web do not choose to repeatedly run (or download) the same executable files over and over again.

Sophos uses the concept of “Web Reputation,” based on historical malware and traffic data to derive a reputation score for various Web hosts, URLs, and IP addresses. The WS1000 appliance determines the relative risk of Web sites that a user requests in a browser window. This approach speeds up the end-user experience by adapting the scope of the scan to the assessed risk of the web page; the higher the risk, the more its content is blocked or scanned. blocking known bad sites outright yet letting through unimpeded content from known good URLs. Sophos calls this function “Risk Sensitive Scanning,” and it is clearly designed to deliver high levels of user responsiveness and performance without compromising security.

A WS1000 Web Security Appliance is a 1-U, rack-mountable unit that incorporates an Intel Pentium D dual-core, 3.4 GHz CPU, 4 GB of memory and two 160 GB SATA, 7,500 rpm hard drives. It runs a hardened Linux operating system that’s optimized for the Sophos software. Each appliance can support up to 1,000 users, and multiple appliances can be deployed behind a layer 4 load balancer to scale up to larger sites.

Ease of Use

The WS1000 appliance offers a central console with an intuitive, easy-to-navigate user interface. Sophos claims you're never more than three clicks to anywhere as you operate the UI – a claim that our tests show is more than warranted.

Configuring security policies on the WS1000 is as easy as selecting how you want to treat low- and medium-risk sites and noting which file types you would like to block (i.e., how you want the system to respond to Web pages with each of the WS1000's four levels of risk). For more granular control over employees' Internet access, an administrator can easily tailor the WS1000 to block specific categories of offensive Web pages, such as gambling, pornography or fantasy league sports sites. Similarly, an administrator can block all adware or all potentially unwanted applications.

While the WS1000 already has controls for blocking access to offensive and unwanted websites, the company is also planning a further WS1000 enhancement by integrating SurfControl's URL classification engine, which will provide full-featured productivity filtering.

The WS1000 produces a wide range of useful reports. These reports gave us a clear picture of malware activity, both in detail and in summary for the entire network. They reveal, for example, blocked Web site accesses, suspicious machines, traffic levels and gateway performance data. The reports also highlight the identity of any of your servers or clients that have attempted to access malware "call-home" sites.

Deploying a WS1000 is easy and consists simply of cabling the box to your network, powering up and assigning an IP address. The WS1000 Web Security Appliance documentation is clear, comprehensive and easy to follow.

Conclusion

The Sophos WS1000 Web Security Appliance is an excellent tool for stopping malware from getting onto your network. It's effective, accurate quick, reliable and intuitive to use. We suggest you take a close look at the WS1000.

What's Bad About Malware

Malware is, collectively, damaging or annoying software and data files that you didn't knowingly install on your computers or, if you knowingly installed it, the malware turns out to be not quite the software you thought you were getting. Typically, malware deletes files, changes files, reveals file contents, throws pop-up advertisements onto your screen, slows down a computer, allows a remote attacker to control your computer, attempts to convince you to supply credit card and password data, tracks your keystrokes, threatens to blackmail you, sends e-mail to everyone in your address book and otherwise ruins your day (or perhaps your life). Malware typically also propagates itself and can install additional malware instances on your computers.

Malware leverages the Windows operating environment, both server and client, in clever ways. Because virtually all users' logons are Administrator-privilege accounts, all the software that users run, even inadvertently, can fully control any aspect of the PC that the software (or malware) developer wishes.

With free rein over a PC's files and programs, including Windows operating system files, a malware instance can configure a computer to run the malware perpetually and thwart attempts to remove the malware (i.e., a *rootkit*). The malware thus becomes part of Windows itself.

Malware can cost your company the time, effort and expense of extricating its residue from infected computers. A study by The Radicati Group, entitled "Corporate Anti-Spyware Market, 2005-2009," says the number of anti-spyware tool licenses will increase from 16 million in 2005 to over 540 million in 2009. Companies are concerned about spyware's security risks, regulatory compliance and employee productivity losses, the report says. The study also revealed that the administrative cost of dealing with spyware-infected computers will quickly rise as spyware programs become increasingly devious, reaching about \$265 per user in 2007.

The following table identifies five common types of spyware.

| Category | Typical Action |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Keystroke Logger (AKA Trackware) | Captures keystrokes (including personal information and passwords) or tracks the Web sites you visit. |
| Trojan | Enables remote control of your computer by a hacker, often for Distributed Denial of Service attacks. |
| Droneware | Sends spam or turns your PC into a host for offensive Web images. |
| Dialer | Auto-dials area code 900 or expensive long distance calls via your modem. |
| Adware | Pops up unsolicited and annoying advertisement-laden browser windows or hijacks your Internet search (Yahoo, Google, etc.) results. |

Testbed and Methodology

We primarily looked for the ability to identify and block malware (such as keystroke loggers, browser hijackers, adware, rootkits, dialers, data miners and trojans). We wanted the WS1000 to prevent malware from sending data from our network (i.e., “phoning home”), scan traffic quickly, receive frequent spyware definition updates and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 150 malware samples, and we moved the collected material to an isolated, quarantined network. We thus were able to simulate the Internet within our lab.

The quarantined network consisted of three subnets.

- Subnet 1 had 10 client machines with a variety of operating systems, including Windows NT, 98, 2000, ME, XP, Red Hat Linux and Macintosh OS X.
- Subnet 2 contained three Web servers (Microsoft IIS, Netscape Enterprise Server and Apache), three e-mail servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and Netware) and two database servers (Oracle 8i and Microsoft SQL Server).
- Subnet 3, simulating the "Internet," had Web servers and clients that contained the malware instances and which sported “bad guy” IP addresses and URLs. Systems on the first two subnets accessed the third subnet as if it were the real Internet.

To measure performance, we used two time-synchronized protocol analyzers on the “Internet” and local network sides of the gateway device and examined the resulting packet captures to know the time taken by a device to forward or discard each network message.

The WS1000 connected our simulated "Internet" to the other two subnets. Client and server machines started off in a pristine state for each test.

Our clients and servers attempted to download malware from the simulated "Internet." We noted how well the WS1000 identified malware traffic and blocked attempts by the malware to send data back to the source. We gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL or OCX, possibly marked with the “Hidden” attribute) and directories as well as Registry and Start Menu changes.

Security Report Card

Grade scale is 1 through 5, with 1 = Failing and 5 = Perfect

| Category and weight (%) | Sophos WS1000 Web Security Appliance |
|------------------------------------------------|-------------------------------------------------|
| Identifying and thwarting malware (40%) | 5 |
| Performance (20%) | 5 |
| Ease of Use (10%) | 5 |
| Reports (10%) | 4 |
| Deployment (10%) | 5 |
| Documentation (10%) | 5 |
| Overall score | 4.9 |

Vendor Details

WS1000 Web Security Appliance

Price: \$4,500 for appliance. For 1,000 users, \$9.75/user/year

Sophos, Inc.

3 Van de Graaff Drive

2nd Floor

Burlington, MA 01803

(866) 866-2802 or (781) 494-5800

www.sophos.com

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking (4th Edition)*, *Network Programming in C* and *Client/Server LAN Programming*.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

You can e-mail him at barryn@erols.com.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.