

NETWORK TESTING LABS REVIEW:

MAKE INTERNET RISKS AND PERILS DISAPPEAR

WE FIND MCAFEE'S EMAIL AND WEB SECURITY APPLIANCE THE ANSWER TO OUR NEED FOR INTERNET SECURITY.

By Barry Nance

Category: Network Security



McAfee's Email and Web Security appliance easily beat Barracuda Spam Firewall and Barracuda WebFilter appliances in our tests. The Email and Web Security appliance thwarted far more malware, stopped far more spam and phishing attempts, recognized far more "bad guy" URLs and performed far faster.

The Email and Web Security appliance was far easier to use, far more scalable, far simpler to install and configure, far more reliable and – if that weren't enough – far, **far** less expensive.

McAfee's Email and Web Security appliance is without a doubt the clear and obvious answer to the risks and perils you face on the Internet.

McAfee Email and Web Security Appliance – again – earns the Network Testing Labs World Class Award for best Internet gateway security product.

The bad guys spend 24 hours a day cooking up malicious Internet Web sites, unwanted advertisements you can't get rid of, annoying unsolicited emails slyly asking for your bank account access data and insidious software to rifle through your computers looking for sensitive financial information.

The Internet can be a downright dangerous place.

Spam, spyware, viruses, Trojans, rootkits, phishing attempts and other criminal or quasi-criminal activities are stealing our credit card data and passwords, throwing up unwanted and inappropriate advertisements on our screens, slowing our computers to a crawl, deleting or modifying our files, tracking our keystrokes, broadcasting e-mail to all the people in our address books, scamming us out of our money and allowing hackers to remotely control our computers.

Network administrators spend inordinate amounts of time deleting persistent malware, advising victimized users, restoring corrupted data files and otherwise cleaning up messes. Users spend far too much time dealing with spam and phishing attempts. And what assurance do you have that some hidden, unnoticed computer program isn't collecting data from your computers and "phoning it home?"

Make the Bad Guys Disappear

There is an answer. You can install a filtering device between your network and the Internet to keep the malware off your network.

In fact, the point at which your network connects to the Internet is the absolute best place to stop the bad guys in their tracks. When done correctly, an Internet security appliance keeps the unwanted stuff from getting onto your network – it's as if you made the bad guys disappear completely.

An Internet gateway that keeps malware off your network in the first place is far more effective and less expensive than the after-the-fact cleaning of individual server and desktop computers.

The ideal Internet gateway accurately recognizes and thwarts malware and other unwanted computer programs. It keeps email in the form of spam or phishing attempts from clogging up people's inboxes. It's capable of denying (or, at your option, warning about) access to dangerous or potentially dangerous Web sites. The ideal gateway blocks attempts to steal sensitive data and prevents accidental leakage of company intellectual property. It's easy to administer, simple to set up and configure, reliable and scalable. Last but certainly not least, the ideal gateway performs so well that users don't know it's there.

Several vendors offer Internet security appliances that filter traffic at the Internet connection point. In this review, we look at two vendors' products to find out which is your best buy.

In our lab, we intensively stress-tested McAfee's Email and Web Security Appliance (EWS) model 3100 (which includes McAfee's SiteAdvisor technology) alongside Barracuda Network's Web Filter model 210 appliance as well as Barracuda Network's Spam Filter model 200.

The most important criterion in our evaluation was the ability to block spam, phishing attempts, malware and access to malicious Web sites. Because we expected a responsive Internet experience, we measured each device's Internet traffic delay (i.e., latency). Keeping malware from "phoning home" (sending our data file contents or keystrokes to the bad guys) was similarly important. We also looked for reliability, scalability, ease of use and ease of deployment.

We found that McAfee Email and Web Security Appliance exhibited the greatest accuracy, quickest performance and highest ease of use. Its SiteAdvisor module did an excellent job of blocking access to malicious Web sites. The Email and Web Security Appliance kept virtually all malware from penetrating our network, and its effect on the responsiveness of our clients' Internet experience was negligible.

Not only did McAfee's Email and Web Security Appliance model 3100 perform much faster than the two Barracuda devices (the combination of Spam Firewall 200 and Web Filter 210), we found having both email and Web security in a single appliance much easier to install and administer.

The Email and Web Security Appliance wins the Network Testing Labs World Class Award for gateway-based Internet security.

Malicious Web Site Recognition

McAfee's Email and Web Security Appliance, with SiteAdvisor, correctly identified an amazing 99% of the malicious Web site URLs and IP addresses we exposed it to (see Chart 1.) In contrast, the two Barracuda devices could muster only an 84% recognition rate. The McAfee Email and Web Security Appliance with SiteAdvisor is a highly accurate tool for preventing access to both Web-based malware and malicious or spam originating web sites. The Email and Web Security Appliance's Web site classification kept virtually all malicious and annoying Web sites at bay.

The disparity in success rates between McAfee's Email and Web Security Appliance on the one hand and Barracuda's Spam Firewall and Web Filter on the other hand made us curious. We wanted to know why McAfee exhibited the far stronger security. We found out that Barracuda uses open source software in its devices, but McAfee's in-house engineers designed and developed the security software embedded in the Email and Web Security Appliance. Furthermore, McAfee has the advantage of having **SmartFilter** technology, which it acquired from Secure Computing. Our research also turned up the fact that McAfee is the leading OEM supplier of Web filter technologies to other vendors.

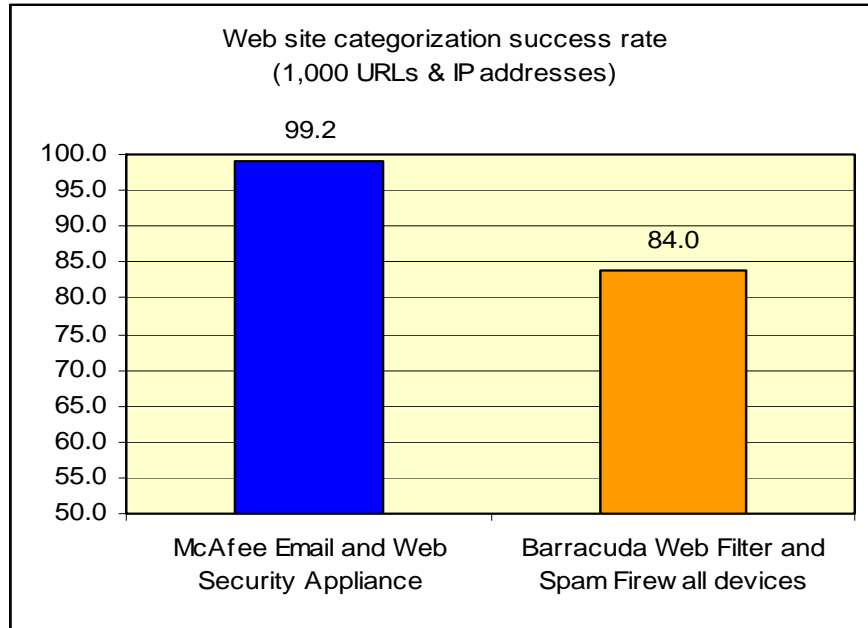


Chart 1. Web site categorization.

SiteAdvisor

SiteAdvisor always stays up to date on the latest threats. It continually crawls the Internet, using intelligent *bots*, or virtual computers. These bots visit nearly every Web site, download content from that site and scan the results for various kinds of malware. The bots even fill out registration forms to determine whether signing up on a site triggers spam. If the site contains malicious code or other suspicious content, SiteAdvisor's bots note the nature of the threat so SiteAdvisor can help you avoid that site.

The SiteAdvisor component knows which Web sites are infected with malware, which sites produce excessive pop-ups, which sites engage in fraudulent practices, which sites contain browser exploits and which sites will target your e-mail address with spam. SiteAdvisor's database is the result of testing virtually every Web site on the Internet for malware behavior. Moreover, in addition to its programmatic evaluation of the Internet, SiteAdvisor uses feedback from customers to assess a Web site's risk.

Installing and configuring McAfee's Email and Web Security Appliance is quick and simple, involving no more than powering it up and assigning it an IP address – it is truly a plug-and-go appliance. The documentation is clear, comprehensive and easy to follow. Setting up the two Barracuda devices is, as you'd expect, twice as much work. The two devices also use up an extra IP address, and the two Barracuda units require twice as much effort to administer.

On one Email and Web Security Appliance screen, an administrator configures Web security policies and acceptable use policies, thus blocking users from time-wasting or obnoxious web sites (such as gambling and pornography) and also preventing users from accessing malicious Web sites. You choose the categories to block, and you choose whether to present users with an alternate Web page or merely warn them to avoid a site.

Configuring the email filtering feature of the Email and Web Security Appliance takes just a few mouse clicks. This feature blocks email-borne spam, malware, phishing attempts and other unwanted email-based traffic.

The combination of Barracuda Spam Firewall 200 and Web Filter 210 gave us disappointing results in our tests. We also note that Barracuda suggests using the Web Filter 210 to handle up to only 100 connections – far less than the capacity of the Email and Web Security Appliance 3100.

The Web Filter 210 can block access to Web sites based on domain, URL pattern, or content category, block downloads based on file type and block applications that access the Internet.

Identifying Malware and Spam

Chart 2 reveals how well the McAfee appliance and two Barracuda devices fared in recognizing actual malware – spyware, viruses, trojans and the like. We confronted the security products with a suite of 500 malware instances, including many “zero-day” threats – i.e., malware that suddenly appears on sites whose URLs were registered just a few moments ago and for which accurate content recognition is paramount.

Incidentally, who would you guess registers the most Web sites every day?
Yes, that's right – malware authors and organizations.

McAfee's Email and Web Security Appliance performs a unique deep content inspection of Internet traffic streams. This deep content inspection even identifies, for instance, spreadsheet files (XLS files) containing social security numbers. Barracuda does not have this.

In further testing, we created a policy that instructed the Email and Web Security Appliance to block, for example, customer account numbers from leaving or entering our network. The McAfee appliance applied this policy correctly, even when called on to scan the interior of attachments for the offending data. Again, Barracuda lacks this capability. Barracuda, unfortunately, does not perform content inspection.

We were also deeply disappointed by the Barracuda devices when we found out that they could scan email in only one direction (either inbound or outbound).

We also noted some security problems with the Barracuda devices themselves. Barracuda recommends that you not do (or even allow) remote (over-the-Internet) administration of the Web Filter/Spam Firewall. These devices have shown themselves to be vulnerable to, for example, "Multiple Cross-Site Scripting" (XSS) attacks. This means that in order to administer remote deployments of the devices at branch offices, you'll have to physically travel to those sites to make the changes in person.

Just when we thought our disappointment in the Barracuda units had reached its maximum, we ran across this gem in the Administrator's Guide: "If the System Load exceeds 50% for more than 5 minutes, the Operating Mode will automatically shift to 'Safe Mode' and will pass traffic without filtering or logging until normal operation can be resumed."

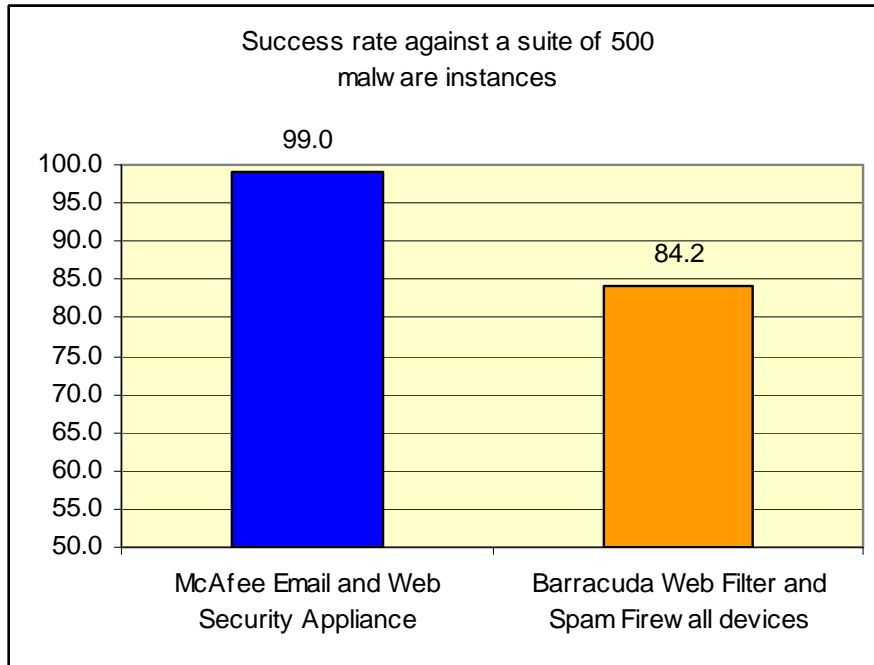


Chart 2. Recognizing and dealing with malware.

We ran a series of tests that asked the McAfee and Barracuda products to correctly identify 18,000 examples of spam and phishing attempts. Chart 3 illustrates the results of these tests. The McAfee Email and Web Security Appliance achieved an astonishing 96% success rate, while the combination of Barracuda Web Filter and Spam Firewall misidentified 26% of the emails.

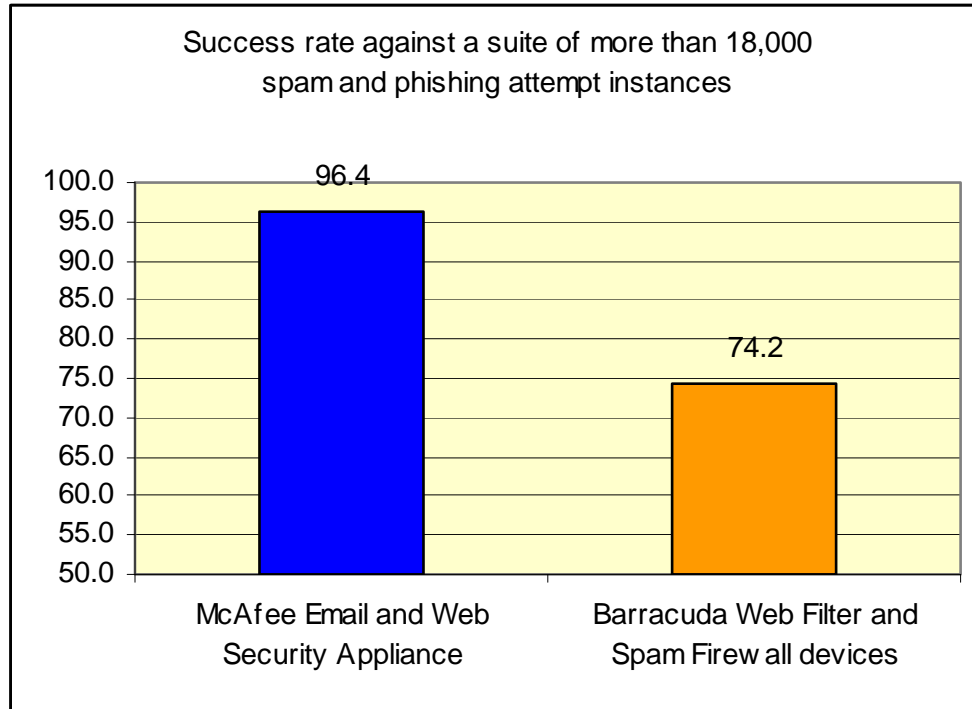


Chart 3. Stopping spam and phishing attempts.

Performance

Responsiveness is an important criterion. The best security product in the world would be useless if it slowed Internet access to a glacial crawl.

To find out which product gave our users the most responsive Internet experience, we tested throughput by using a pair of time-synchronized protocol analyzers linked to their Internet and local network connections and noting the delta times (i.e., packet delay) introduced by each product.

We found that the Email and Web Security Appliance to be the fastest performer. Indeed, McAfee's appliance is so highly optimized that client responsiveness was virtually unaffected – our users were completely unaware the Email and Web Security Appliance was filtering Web and e-mail traffic. Chart 4 is a graph of the resulting latencies, for both non-executable content and executable (computer program) content.

In the latency chart, smaller numbers signify better performance (and thus also signify the more responsive Internet experience).

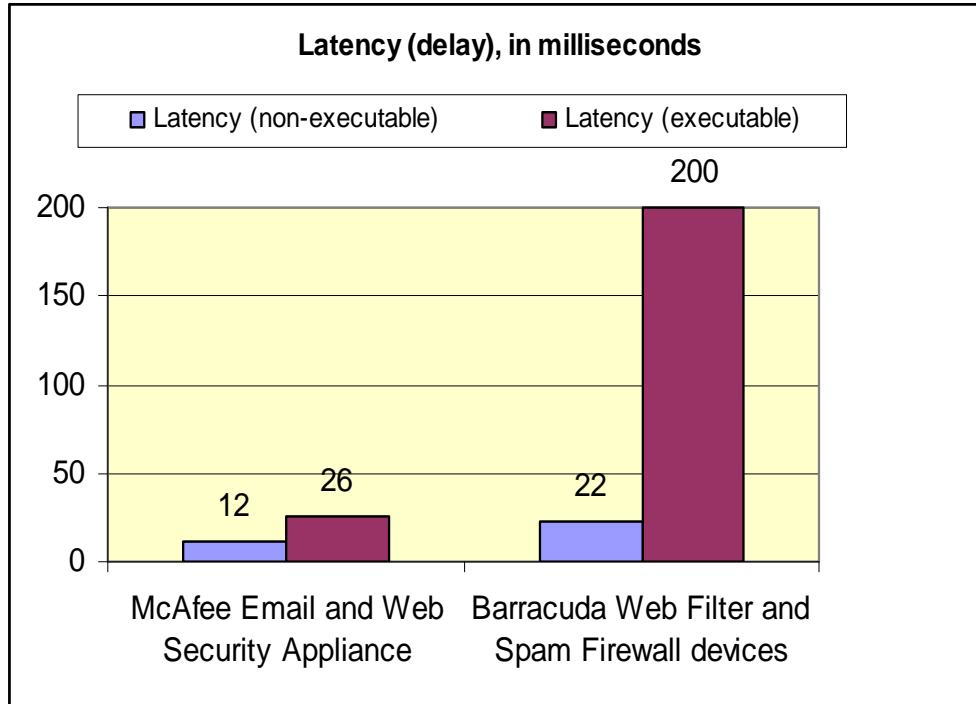


Chart 4. Performance results.

Conclusion

The McAfee Email and Web Security Appliance is the clear winner in our evaluation. Not only was it more accurate, it was faster, more scalable, more reliable and easier to use.

The McAfee Email and Web Security Appliance gave us measurably stronger security against both email-borne and Web-based threats. We recommend you consider using Email and Web Security Appliances in your organization.

Testbed and Methodology

We primarily looked for the ability to identify and block malware (such as viruses, spam, phishing attempts, keystroke loggers, browser hijackers, adware, rootkits, dialers, data miners and Trojans). We wanted a product to prevent malware from sending data from our network (i.e., "phoning home"), identify already-infected clients, scan traffic quickly, receive frequent spyware definition updates and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 500 malware samples, 1,000 malicious URLs/IP addresses and over 18,000 spam/phishing samples. 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 25 client machines with a variety of operating systems, including Windows NT, 98, 2000, 2003, ME, XP, Vista, 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 containing 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 products and examined the resulting packet captures to determine the time taken to forward or discard each network message.

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 products 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 A through F, with F = Failing and A = Perfect

Category and weight (%)	McAfee Email and Web Security Appliance 3100	Barracuda Networks Spam Firewall 200 and Web Filter 210
Identifying and thwarting both malware and spam (30%)	A	D
Performance (20%)	A	D
Ease of Use (10%)	A	C
Reports (10%)	A –	C
Deployment (10%)	A	A
Documentation (10%)	B	B
Overall Score	A –	C
Price	\$3,995 (300 users)	\$8,998 For both units \$4,499 Model 200 (500 users) \$4,499 Model 210 (100 users)

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.