



828 West Taft Avenue
 Orange, CA 92865
 714-282-6111
 714-282-6117 Fax
 www.8e6.com

Web Filtering Appliances Heat Up the Hardware vs. Software Debate

By The Forsite Group

Introduction

Hardware appliances inevitably surpass their software-based counterparts when it comes to enterprise-class concerns...

One of the few constants in the IT and security industries—besides the relentless rate of change—is the recurring battle between advocates of dedicated hardware appliances and backers of software-based devices. Predictably, these arguments occur when a product or technology begins to gain critical mass and the associated market starts to show some profit potential.

The outcome of these altercations is equally predictable. Hardware appliances inevitably surpass their software-based counterparts when it comes to enterprise-class concerns like performance, capabilities, scalability, and ease of configuration and management.

Still, the hardware vs. software debate continues. Web filters are the latest products to be caught in this war of words. These devices are the only effective way for IT and security managers to detect and deter systematic abuse of employee Internet privileges. Thus they've become increasingly essential to businesses, government agencies, and other "connected" organizations.

The Extent of the Damage

30 percent to 40 percent of Internet use in the workplace is unrelated to business.

IDC

A little perspective can go a long way here. This isn't about a few end-users bidding on eBay auctions or checking scores of their favorite teams. This is employee abuse on a massive scale. According to IDC, the premier source for global market intelligence, 30 percent to 40 percent of Internet use in the workplace is unrelated to business.

Those figures help explain why Web filters are a very hot ticket. According to IDC, secure content management (SCM) appliances have "exploded onto the security scene" ("Worldwide Secure Content Management 2004–2008: A Holistic View of Antivirus, Web Filtering and Messaging Security"). IDC indicates that global sales of SCM appliances reached \$130.8 million in 2003 (the most recent year for which figures were given). That represents an 89 percent increase over the previous year. While this is a fraction of the \$3.4 billion spent on SCM software that year, the appliance market is growing faster than the software market and is actually expected to surpass \$1 billion by 2008. Global revenue for the entire SCM market, which includes antivirus software, messaging-security software, and SCM services, is projected to reach \$7.5 billion by 2008, for a CAGR of 16.9 percent.

Working Hard or Getting Soft?

Inevitably, software-based products begin to show their inherent limitations at some point. If a software Web filter is implemented on a firewall, it's only a matter of time before the firewall's general-purpose CPU starts to bog down because it's being asked to do double duty.

The buzz is building. There's plenty of money to be made or lost. The scene is set for the latest round in the software vs. hardware debate. IT managers who want to remain unscathed—and confident they've made the right choice—should take a closer look both at Web filtering and at what hardware and software can actually deliver.

Let's start with the basics: Essentially, Web filters should be able to accomplish four tasks:

1. Monitor employee Internet activity (including Web site visits and attempted IM and peer-to-peer activity)
2. Block inappropriate behavior (denying access to porn sites, for example)
3. Report on how employees are using or abusing their Internet privileges
4. Enable companies to automatically enforce their Appropriate Web Usage guidelines

In other words, Web filters are intended to give IT managers complete control over all Internet use. At least that's the theory; some history should help determine how well it matches reality.

Products generally start out as software, piggybacked on top of another piece of equipment (routers, firewalls, and proxy servers all began as software-based devices). This makes perfect sense. Developing a software-based product is far faster (and easier) than building a dedicated platform. In the short term, software-based products do some good and are better than nothing at all.

Inevitably, software-based products begin to show their inherent limitations at some point. If a software Web filter is implemented on a firewall, it's only a matter of time before the firewall's general-purpose CPU starts to bog down because it's being asked to do double duty. In some cases, one function ends up stealing cycles from the other, so either the filter or the firewall can no longer do its job at the required speed. In the worst case, both devices slow down. Either way, network performance and security are both compromised. That makes it far easier for a virus or worm to slip by unnoticed or for a Denial of Service (DoS) attack to overwhelm the firewall and connected servers.

Web Filters: The Appliance Advantage

Device type	Hardware Appliance	Software-based
Platform	Single-purpose	Multipurpose
CPU	Dedicated	Shared
Memory	Dedicated	Shared
Other processing resources	Dedicated	Shared
Architecture	Pass-by	Pass-through
Performance	Remains stable regardless of load	Degrades as load increases
Potential bottleneck	No	Yes
Single point-of-failure	No	Yes
Maximum end-users	30,000+	Unknown (depends on CPU, load, other variables)
Scalability	Simple; add another appliance	Difficult; integrate software on another host
Configuration	Simple; via dedicated GUI	Complex
Management	Simple; via dedicated GUI	Difficult

Unscalable Software

A dedicated appliance like the R3000 Internet Filter from 8e6 Technologies does a far more effective job at identifying and filtering out undesirable or dangerous Web traffic than any software-based device.

Performance is only part of the problem. Scalability is another key issue. As the number of Internet users at a company climbs, the load on a Web filter rises correspondingly. This is lethal for a software-based Web filter; ultimately, there are simply too many end-users trying to tap into too few cycles. The software can't service the requests, creating a bottleneck or letting blocked Web sites get through to the end user.

In a perfect world, software-based devices would be retired gracefully once dedicated hardware appliances were available to replace them. In the real world, vendors have far too much invested in R&D, marketing, and branding to pull products from the shelves. They may also honestly dispute the claims of rivals, marshalling counterclaims, test reports, and case studies to back up their beliefs.

Ultimately, it's IT professionals and security managers who get hurt—along with their companies. A dedicated appliance like the R3000 Internet Filter from 8e6 Technologies does a far more effective job at identifying and filtering out undesirable or dangerous Web traffic than any software-based device. Understanding why this is the case means assessing the underlying technology. Before doing that, however, it's time to address the only question that skeptical IT and security managers want answered: "Do I really need this device?"

End-Users: The Enemy Within

Security analysts estimate that that 90 percent of all employee computers harbor at least 30 spyware programs.

IDC

The short answer is "Yes."

It's impossible to imagine today's companies doing business without the Internet, whether they're using it to deliver product literature, perform transaction-based sales, fulfill requests from partners and customers, and so on. Unfortunately, it's equally impossible to imagine any end-user PC without Internet access—and that's where the trouble starts.

The Web has always been a hostile environment. It's also enormously alluring, even to end-users who've taken the HR handbook and the corporate Web usage policy to heart. Even the best employees will want to look up a recipe, read the review of a new toy they're thinking of giving as a birthday present, check out how their favorite college basketball team is doing in the playoffs, or any one of a myriad of seemingly innocent activities that involves visiting "safe" Web sites.

But how do end-users know a safe site from an unsafe one? Hackers don't post friendly warnings like "This site will load your computer with spyware." In fact, users don't know, which is why some security analysts estimate that that 90 percent of all employee computers harbor at least 30 spyware programs. That also explains why, in a recent IDC study of 600 North American organizations, spyware was considered a "very serious" threat to network security, ahead of spam, hackers, and cyberterrorism.

Spyware is an executable file that exists for only one reason, to spy on a PC and gather information about it (often for sale). It's also ideal for scanning and stealing sensitive business data, corrupting files, monitoring applications, reading browsers, snooping e-mail, and even downloading other spyware.

The Instant Messaging Mess

Spyware is only the proverbial tip of the security iceberg. End-users exchanging IMs with a friend outside the company can easily and unknowingly download malware that contains a worm or virus. Once this code is secretly installed on a PC and exploits a back door or a known flaw in a popular program like Windows, it can quickly proliferate across the network. At some predetermined time, this parasitic code can launch an attack against the network that's hosting it. If it succeeds in bringing the network down, even for a short time, the losses can be astronomical. Damage to a company's reputation can be even more expensive, especially if the organization is supposed to be both Web-savvy and secure, like eBay or Amazon.

Worse, that malicious code can use one company's network resources to launch a third-party attack on another company, usually as part of a distributed Denial of Service (DoS) attack. Established legal precedent holds a company liable in part for damages if its computers and network are used to stage an attack on another company.

IM exchanges also can jeopardize company compliance with a variety of state and federal regulations. For example, the Sarbanes-Oxley Act (SOX) mandates that IM exchanges, which may seem as casual as a phone call, must be treated as formal correspondence. Like e-mail, IM communications must be captured and stored. Similarly, both the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers Inc. (NASD) identify IM traffic as communications with the public that companies must monitor and save.

Wasting Time On the Web

A survey of more than 175,000 PCs at 560 companies found that 77 percent had been involved in some form of file-sharing activity.

AssetMetrix

Although it's not a straightforward security issue, personal Web browsing is costing companies a bundle. A recent study states that an employee earning \$40,000 annually who wastes an hour a day on non-work-related online activity costs his or her employer \$5,000 per year in lost productivity. In a midsized business with 2,500 employees who match that profile, \$12.5 million in lost productivity is dropping straight to the bottom line. And in a finding sure to bring out the Scrooge in the most benevolent employer, Nielsen/NetRatings notes that 46 percent of online holiday shopping is conducted at work.

Inappropriate online activities are not restricted to surfing. Nielsen/NetRatings also finds that more than 72 percent of Internet users download music and watch videoclips. That helps explain why some companies have calculated that more than 80 percent of their Internet capacity is being used to access non-business Web sites, reports Ernst & Young.

Downloading music isn't just a bandwidth hog. The RIAA (Recording Industry Association of America) doesn't look favorably on anyone downloading copyright-protected music without paying for it. A quick Google search reveals that hundreds of Web sites exist for just this purpose. A survey of more than 175,000 PCs at 560 companies, conducted by AssetMetrix, found that 77 percent had been involved in some form of file-sharing activity, so it's almost certain that illegal sharing of music and videos is taking place. If employees are caught pirating music, the fines, according to eCommerce Times can run to \$150,000 per illegally downloaded work. What's more, companies are often held liable for these penalties.

Who Pays for Pornography?

70 percent of all Internet porn traffic occurs during the 9 to 5 workday.

SexTracker

Finally, there's the "illicit" Internet browsing expressly forbidden by most companies' acceptable Web-usage policies. Viewing or downloading adult material is probably the one that comes to mind first, but it's hardly the only one. Online gambling keeps some employees glued to the screen, though for the wrong reasons.

The first myth to demolish when it comes to online pornography is that it's a private activity that people do at home. According to SexTracker, "70 percent of all Internet porn traffic occurs during the 9 to 5 workday." Nielsen/NetRating has determined that 21 percent of all adult sites are accessed from work. Meanwhile, 70 percent of employees surveyed by NFO Worldwide admit to viewing or sending adult-oriented e-mail at work.

The second misconception is that viewing pornography is a victimless crime. State and federal courts have consistently upheld the principle that pornography is a form of sexual harassment and contributes to a "hostile work environment." To reinforce this message, the courts also have been known to levy very hefty fines: Chevron Corp. and Morgan Stanley Dean Witter have both settled multimillion dollar sexual harassment lawsuits that were filed as a result of internally circulated e-mails that contained offensive content.

Internet Filters Up Close

21 percent of all adult sites are accessed from work.

Nielsen/NetRating

The basic task for an Internet filter is—filtering. But how a device implements this function directly affects its performance and overall capabilities, as well as the performance of the network it's running on.

Software-based Web filters use the pass-through method. This is an inline technique that introduces an additional network device (the filter itself) in the connection path. This has several drawbacks. All outbound Web requests have to be handed off to the filter, which then performs a lookup to decide whether to block or allow them. If the request is OK'd, the filter redirects it back to its host, which then passes it along until it reaches the Internet. This process is reversed for inbound traffic.

The primary problem with this approach is that the software-based filter has to "touch" all Web traffic. And even then, it only performs a lookup once it has captured the request or the reply. This approach is a blueprint for a bottleneck. If the filter is swamped with requests, there's sure to be a slowdown. An Internet filter should improve performance by making more bandwidth available, not slow it down.

The other serious shortcoming of the pass-through scheme is that it introduces a single point of failure at the Internet access node. If the filter goes down or is backed up, nothing can reach the Web from the organization or reach the organization from the Web.

Dedicated Internet appliances use an alternative approach, known as pass-by filtering. In this case, the standalone filter sits outside the flow of traffic, monitoring Web requests and comparing them against its database. Since it doesn't stop and check every packet, it doesn't slow down traffic. The only time it takes action is when a request or reply matches up to an entry in its database. At that point a TCP reset is sent to the Web server, telling it to kill the request. It then sends a block page to the client. Further, since the standalone filter isn't connected in-line, it doesn't introduce a single point of failure.

Unstable Scalability

Software-based Web filters are scalable only to the point that they begin to interfere with the processing performed by the host device.

In most cases, a dedicated hardware filter should support tens-of-thousands of users.

Scalability is an equally critical concern. Software-based Web filters are scalable only to the point that they begin to interfere with the processing performed by the host device. Given all the variables involved, including the speed of the host's CPU and the general level of activity at the Internet access point, there's no way of knowing beforehand exactly how many simultaneous users a software filter can support. Worse, the number may shrink or grow as other conditions change. This obviously makes network planning, never an exact science, into more of a guessing game than ever.

The number of simultaneous end-users a standalone filter can accommodate should be supplied as part of the unit's spec sheet. Network and security managers should be cautioned, however, to take these figures with a grain of salt—at least until they've been verified on a production network.

That still leaves the question: How many end-users represent an acceptable load? In most cases, a dedicated hardware filter should support tens-of-thousands of users.

Since a filter is going to be dealing with all the Web traffic leaving an organization (including Webmail and IM), it should be able to recognize and filter as many Internet protocols as possible. A good working list includes URLs, IP addresses, HTTP/HTTPS, FTP, and NNTP (newsgroup). A filter should also be able to trigger on file types, including MP3, JPEG, and MPEG.

Similarly, the ability to block inappropriate Web searches can be very useful, since it closes another online door that end-users might try to use to circumvent the filter.

As noted, IM and P2P (peer-to-peer) file sharing are both potentially dangerous applications. To prevent either from opening a security breach, an Internet filter must be able to detect and block both types of traffic. Further, a filter should be able to block port-hopping IM servers, which means that it must be able to detect actual IM packets. Similarly, a Web filter should know P2P packets when it sees them, which enables it to prevent file-sharing sessions from being initiated or makes it possible to terminate them if they're taking place.

How Deep Is the Database?

An Internet filter, whether implemented in hardware or software, is only as good as the database it relies on to identify inappropriate Web sites and other destinations. This isn't simply a matter of size. Hundreds of new sites appear on the Internet each week, many of them built one step ahead of various law enforcement agencies. This means that a filter's database must be updated regularly and those updates must be checked scrupulously to see if they point toward trouble. Further, IT administrators must be able to manage the database efficiently and effectively, adding URLs to the blacklist (to prevent access) and whitelisting others by changing their status from blocked to allowed. Here again, the shared memory used by a software filter limits the number of URLs it can keep on tap, just as the speed of its shared CPU limits how quickly it can decide to block or allow a request.

IT and security managers also must be able to create and apply user/group profiles. This makes it possible to define levels of access, allowing certain individuals or groups to access some sites that other end-users can't reach. Actually, administrators should be able to assign three levels of access: allowed, monitored, and blocked. This would give them the greatest control and the clearest picture of Web usage.

Another particularly useful access control mechanism is the time-based profile. In this case, administrators can permit or deny access to Internet resources based on time of day. The most extensive list of blocked URLs would apply during peak usage hours. This would both save bandwidth and promote productivity (there would be no way for anyone within the corporation to reach anything but business-related sites from, say, 8:00 a.m. to 11:45 a.m.). Conversely, a very short list of blocked sites could be allowed during lunch hours, permitting employees to check on sports sites, shop online, and the like.

Finally, an Internet filter must be easy to set up, manage, and maintain. Here again, dedicated hardware devices typically outscore software-based filters. Adding a “foreign” functionality to a product built for another purpose can wind up being a mistake. Even when the setup goes smoothly, however, there’s always a greater chance of trouble, especially under heavy loads when there’s a greater likelihood that competition for resources will destabilize one or both devices. At that point, an Internet filter can quickly become a liability, since it forces IT to spend an inordinate amount of time tending to it. Given that most IT departments are stretched thin these days, introducing a device that is almost certain to need more than its share of handholding can easily force staff to devote less time to other projects.

Internet Filtering, the 8e6 Way

Since the R3000 employs noninvasive pass-by filtering technology, it keeps tabs on Internet traffic without having to interfere with every packet that goes by.

8e6 Technologies is the authority and leading provider of appliance-based Internet filtering and reporting solutions for business, education, government, and ISPs worldwide. Recognizing threats and distractions such as inappropriate Web content, IM, P2P downloads and spyware, 8e6 empowers organizations with turnkey solutions that enforce their Acceptable Use Policies (AUP)—improving productivity, reducing liability, and preserving network resources.

8e6’s line of R3000 Internet Filters and its Enterprise Reporter are dedicated standalone hardware platforms that are completely capable of working in both small to large distributed environments.

Since the R3000 employs noninvasive pass-by filtering technology, it keeps tabs on Internet traffic without having to interfere with every packet that goes by, blocking or redirecting only those that must be filtered out of the data stream. This highly efficient approach to Internet filtering results in robust, highly scalable solution that can support up to 30,000 users per appliance.

Easy Does It

The R3000 is as efficient as it is easy to use. It prevents users from accessing unauthorized Web sites and stops them from accessing IM and sharing P2P files, including music, video, pirated software, and viruses. It also recognizes and filters a comprehensive range of Internet protocols, including URL and IP addresses, FTP, HTTP/HTTPS, and newsgroups. What’s more, to further protect organizations from illicit content, the R3000 can force Google’s SafeSearch mechanism ‘on’ as its default setting (which means Google’s built-in search-engine filter controls can act as a second layer of defense and cannot be turned off by end-users).

8e6 understands that an Internet filter stands or falls by its database, which is why it has combined artificial intelligence and human expertise to ensure comprehensive, up-to-date coverage. High-speed AI utilities collect Web sites on a 24/7 basis, so there’s virtually no chance a URL that should be blocked gets by. To further refine its information, highly trained specialists individually

verify and categorize each site. As a result, 8e6 has built a database of several million sites, organized into 80 overarching categories. In addition, IT and security managers can add or delete sites as needed.

To further increase the flexibility and usefulness of its standalone Internet filter, 8e6 makes it easy to add custom user/group profiles and implement time-based filtering.

Conclusion: Deadly When Undetected

IT and security managers now have a flexible, highly effective tool that enables them to expose and eliminate this abusive behavior: a hardware Web filter.

Employee abuse of Internet privileges is a silent killer. It doesn't have the dramatic impact of massive online identity theft or a DoS attack, but it's every bit as dangerous and damaging. In fact, it may be even more deadly: As long as this sort of misuse remains undetected, it continues to chip away at productivity and profits.

IT and security managers now have a flexible, highly effective tool that enables them to expose and eliminate this abusive behavior: a hardware Web filter. A dedicated appliance is designed and built for a single purpose: filtering. It doesn't share processing power, memory, or other resources with another device, a sure recipe for a slowdown just when a Web filter needs to be in top form. An appliance doesn't introduce a single point of failure, a critical consideration when 24/7 network availability is the order of the day. Further, a Web filtering appliance is far easier to configure and manage than a software-based device. Simply said, IT and security managers who opt for a software-based Web filter are only making things unnecessarily hard on themselves.



For more information on 8e6 Technologies and 8e6 appliance-based solutions for Internet Filtering, Web-use Reporting, and Spam Control, visit www.8e6.com.