

[www.securecomputing.com](http://www.securecomputing.com)

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.



**Secure Computing Corporation**

**Corporate Headquarters**

4810 Harwood Road  
San Jose, CA 95124 USA  
Tel +1.800.379.4944  
Tel +1.408.979.6100  
Fax +1.408.979.6501

**European Headquarters**

East Wing, Piper House  
Hatch Lane  
Windsor SL4 3QP UK  
Tel +44.1753.410900  
Fax +44.1753.410901

**Asia/Pac Headquarters**

1604-5 MLC Tower  
248 Queen's East Road  
Wan Chai Hong Kong  
Tel +852.2520.2422  
Fax +852.2587.1333

**Japan Headquarters**

Level 15 JT Bldg.  
2-2-1 Toranoman Minato-Ku  
Tokyo 105-0001 Japan  
Tel +81.3.5114.8224  
Fax +81.3.5114.8226

© November 2005 Secure Computing Corporation. All Rights Reserved.  
SF-MILCS-TP-NowGov, Secure Computing, SafeWord, SideWinder, SmartFilter, Type Enforcement, SoftFaker, SecureSupport, SecureOS, MobilePass, G2 Firewall, Besa, SideWinder G2, enterprise strong, PremierAccess, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, Application Defender, RemoteAccess, On-Box Power-It-On!, Sentinel, and Securing connections between people, applications, and networks are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.

# Protecting HTTP traffic: Why Web filtering should be your first line of defense

## Table of contents

Introduction .....	2
Access and security: a tradeoff?.....	2
Key drivers of corporate security policy .....	3
Risks to the network.....	5
A word on attacks from inside.....	6
Sophisticated attacks .....	6
How SmartFilter Web filtering stops sophisticated attacks .....	7
Controlling user access and privileges.....	8
SmartFilter: an important component of a successful IT security strategy .....	8
Conclusion .....	9

## Introduction

Access to the Internet brings tremendous value to any organization, not just as a means of global communication, but as a way to enable employees to access competitive information, and research markets and opportunities. It further empowers organizations to strengthen relationships with key vendors, clients and suppliers by creating secure remote connections via VPNs and extranets, through which critical information can be shared with organizations outside of the corporate walls.

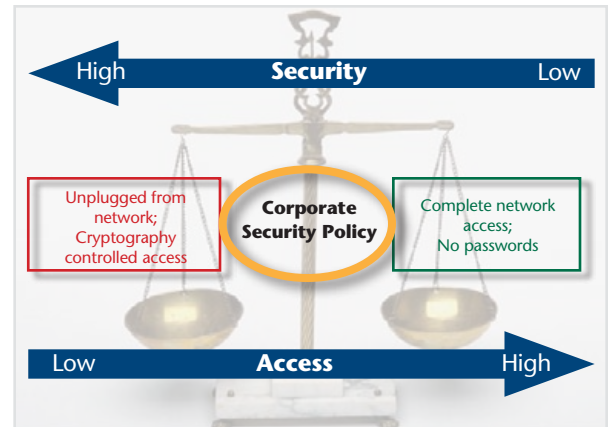
But along with those vital competitive advantages, employee access to the Internet and all of its related applications—most of all Web surfing—poses serious productivity, liability, and security concerns. Productivity and liability concerns have been recognized for years now, but of serious concern is the growing security threat to which organizations are exposed when their employees browse the Internet. Unrestricted, such browsing opens doors that allow viruses, Trojans, spyware, and other malware into your network that will very likely if not certainly decrease productivity, cause network disruptions, or even steal vital proprietary information.

Corporate networking teams are recognizing the value of Web filtering as part of a multi-layered strategy that includes a variety of means to combat the ever-growing threats to their organizations which leverage the Internet as a means of delivery. In fact, the Internet has become a major tool for industrial spies, foreign agents and others intent on doing harm for personal gain, retribution, or political reasons. Much of what was once protected and secured technical and proprietary information is now on the network, and if the attacker knows the right tricks and the owner of the data has not taken the right precautions, that information can be easily retrieved.

Web filtering technology is an effective policy enforcement tool that has become a necessary part of any IT organization. Web filtering isn't just about keeping users away from porn sites. Web sites that are often contained in one or more of the categories filtered out by URL filtering technology are very often the point of origin for dangerous attacks. Pornography sites, for example, are offensive to many people. Blocking access to them prevents the creation of an adverse work environment, but that prevention also helps to keep out the malware (malicious software) that is often contained on those offensive sites. Web filtering also protects against several other HTTP/Web threats as part of a multi-layered strategy that guards against a constant stream of increasingly sophisticated attacks.

## Access vs. security: A tradeoff?

Clearly, the competitive benefits enjoyed by a company that makes full use of the Internet will be diminished if access is completely denied. Very few companies could even survive without the Internet in today's business climate. Yet, allowing unrestricted access brings massive risks of financial loss and legal liability. There is a tradeoff between security and access that IT and security officers must address, as shown in Figure 1 below.



Almost any employee who can will use the office computer for some non-legitimate business use. This may be very minor, taking the form of an employee checking personal email, or shopping for a gift online. On the other hand, it can be extreme, with employees downloading network-clogging images, playing online games, or viewing pornography. A *Vault.com* survey revealed that 34 percent of employees surveyed surf non-work-related Web sites at work "a few times a week," 37 percent said "a few times a day," and 14.6 percent said "constantly." Only 13 responded that they never surf non-work-related sites.

But it is a matter of degree. A staggering 12.6 percent of respondents said they spend over two hours a day surfing non work related sites. While management may wish to create a positive and friendly workplace by allowing *some* degree of personal access, two hours a day is clearly too much by any measure.

Many organizations grant employees some flexibility in personal Internet time. But personal Internet time must be balanced against the need for productivity and the need to maintain security and privacy. Clearly, it must be restricted. An effective policy would, for example, allow personal Web surfing or email during lunch hours or breaks, while still maintaining Web filtering policies to prevent access to objectionable or potentially harmful content 100 percent of the time. Such a policy may allow limited use of Web

surfing, but would completely prohibit access to P2P file sharing sites or instant messaging—which can be conduits for malware. Policies can also be applied differently to different groups of users or allow overrides when necessary. Simply monitoring of employee surfing habits through a reporting feature would also provide management with information that it needs to take action when necessary, and to craft new policies in response to usage trends.

On one end of the scale, absolute security can be provided by completely eliminating or drastically restricting network access to the computer and securing physical access, through a plethora of increasingly secure methods from multiple password authentication to controlled access to the location of the computer itself. The Internet has become part and parcel of day-to-day business, and you can only place restrictions up to the point where those restrictions do not hinder the normal operation of your enterprise. Increased security often comes at a cost to a business, in that the power of the computer to speed business transactions and provide access to information for knowledge workers can be compromised. And too, increased security that comes at the cost of ease of use quickly becomes useless, as employees will reject or work around security measures that are too difficult.

On the other side of the spectrum is completely unsecured and unfettered access to networks and to the computer itself. This provides unacceptably high network, data and legal liability for almost all organizations, and such a policy—or lack thereof—is just a disaster waiting to happen. The sweet spot in the middle is where security policy makers must define and enforce a corporate security policy that is fair, enforceable, and does not present an undue burden on end users; while still preventing the damage that can be caused by unauthorized Web surfing.

Software and hardware solutions are a key part of a successful corporate security policy that balances security with access and ease of use.

## Key drivers of corporate security policy

A corporate security policy is more than just a static document; it is one that can and must change in response to new regulations, and new threats that may not have existed when the original policy was created. It must be enforced with technology, and it must be communicated to all parties for it to be effective. Some of the key drivers behind the security policy include:

*Legal concerns.* Federal law prohibits maintaining a “hostile work environment,” which has been broadly interpreted to include allowing objectionable Web content to exist in the workplace. An employer has both an ethical and a legal obligation to create a work environment that is free from adverse or offensive material. No HR director would permit an employee to display pornographic photos in their work area. And so too, the computer screen must be free from such objectionable material. Already, the courts have seen several lawsuits filed by employees who have been exposed to pornography or other inappropriate Web content. Such litigation could be costly, and also could damage a company’s good reputation. An American Management Association study showed that 27 percent of Fortune 500 companies have faced sexual harassment claims stemming from employee misuse of the Internet. Just because a company has not overtly allowed it, doesn’t mean they are not liable. Not taking any proactive action to prevent it—such as installing a Web filter—could mean an employer could be subject to lawsuits and heavy fines, regardless of their best intentions.

*Intellectual Property concerns.* Intellectual property and trade secrets aren’t usually kept in a vault; rather, they are most often stored electronically. And while security officers make every attempt to protect that electronic data through policy enforcement technology, hackers are at the same time making their own best attempt to get through the technological barriers that have been erected through technological means of their own.

Several high-profile cases of intellectual property theft have made the news, no doubt countless others go unreported. In most cases, appropriate security policy and technological enforcement could have prevented the theft. The well-known case of two Lucent Technologies employees, who in 2001 were arrested on charges of stealing trade secrets, is just one example. The engineers had taken valuable technology secrets for their own personal gain. The two had formed a company which had received financing from a Chinese communications equipment maker. Lucent’s suspicions were aroused and officials contacted the FBI, who determined that the two had indeed transferred the source code for Lucent’s PathStar system to a password-protected site owned by the two employees.

In many cases, very little technological sophistication is required to execute the theft. Take for example, the case involving Bell Imaging Technology, where in 2001 an employee was able to steal trade secrets because his wife was employed as an engineer with an affiliated company, was able to access the documents and bring them home with her. Another case involving MasterCard International underscored the vulnerability of large corporations. In this case, a catering employee with no technical knowledge stole confidential papers and offered to sell them to MasterCard's competition.

*Compliance.* Several federal and state regulations have come into existence over the past few years, addressing corporate governance issues, privacy concerns and disclosure. These regulations are primarily policy-driven, but enforcement of the policies must be done through technological means.

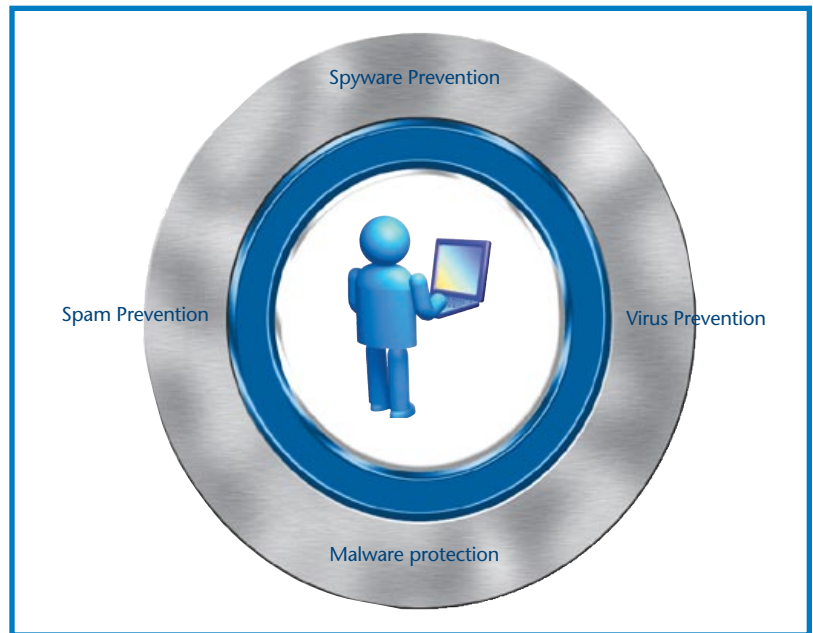
Mandates, such as HIPAA, Gramm-Leach-Bliley, the Children's Internet Protection Act (CIPA) and the California Information Practice Act (SB 1386) require consumer privacy to be protected through technological means, and call for a multi-layered approach to protecting data such as social security numbers, account numbers and other personal information. This multi-layered approach includes firewalling and strong authentication, but should also include Web filtering technology as a first line of defense in keeping out viruses, Trojans and other malware that could enter into the network when users view Web sites that could have been blocked using a Web filter. Malware can easily compromise the network and the protected data therein.

Web filtering is one of the main technologies that is used to enforce all of the above policy drivers. Corporate security policy should entail an assessment of the risks to both the network and the business, and focus efforts to deploying multiple layers of security to secure the network and its use.

A multilayered strategy does not mean using multiple, point solutions that each address only a narrow focus. Instead, each of several integrated solutions will naturally overlap areas of focus to provide multiple coverage in-depth. Web filtering's stated goal is to enforce an Internet use policy by blocking access to categorized Web sites. But in so doing, the filter's function crosses over into the functions offered by other security solutions, creating a double layer of protection against viruses, spam, spyware, and other types of attacks.

The security policy should call for multiple, integrated security solutions to secure as many layers that comprise a network and its use, such as:

1. Who has access to the network, through either physical or virtual means
2. Internal monitoring and filtering of employee requests for information from both inside and outside the network, mixed with granting access to remote employees and other authorized users



3. Defense against increasingly sophisticated attacks and intrusion attempts from outside the network
4. Finally, allowing customers and constituents access to specific information without jeopardizing other information contained on the network.

In addition to these concerns, there are bandwidth drain/utilization and productivity issues to be managed. The growing popularity of peer-to-peer file sharing networks, instant messaging, online photo albums and other online novelties cause a glut of unauthorized bandwidth-hogging applications to infiltrate the network—often consuming such a large amount of bandwidth that vital, day-to-day business

activities become impeded. In this case, the Web filter supplements the utility of caching appliances as a means of preserving bandwidth by blocking access to sites that offer these types of online services.

Network access policies that provide security include both technology and behavioral requirements for employees. For example, policy can require that PCs not be left unattended without logging off of them, requiring complex passwords (containing a combination of both alpha and numeric characters of a minimum length) and that these be changed regularly. These passwords integrate with directory structures (NTLM, LDAP) that can permit/deny access to different network segments, hardware, and processes. The use of strong authentication such as tokens are examples of technologies that can be applied to restrict network access. Both internal and perimeter firewalls are commonly used as control points throughout any network. All of these solutions work hand-in-hand with the Web filter to ensure security at every level.

Monitoring and filtering of employee requests for information are an important part of any security policy. The use of technologies such as messaging, P2P, Web surfing, or e-mail opens up an organization to a security risk that must be managed.

## Risks to the network

The Web filter is concerned primarily with HTTP-based threats to the network. HTTP threats that need to be protected against include threats revolving around messaging, email, P2P fileshare, spyware, adware, hijackers, cookies, DRM, malware, phishing, spam, worms, and employee Web surfing. Protecting against all of these threats requires a multi-layered content security strategy. Web filtering is a critically important component of this strategy, since HTTP communications are one of the primary methods used to exploit people, applications and networks.

*IM attacks.* Instant messaging lets people communicate and share files easily. When controlled and restricted, it can be an excellent way to communicate with key customers and partners; but it can also expose the organization to increased risk. IM is unencrypted, and all files that are transmitted bypass normal corporate security transmission restrictions. Use of IM also exposes the organization by opening up a way for attackers to send viruses, worms, and other malware. Security experts recommend blocking or restricting access to IM clients. If IM needs to be used for legitimate business purposes, choose a single, proprietary solution and block access to the common, publicly-available freeware varieties.

*Email attacks.* Email attachments are a well documented means of spreading worms, viruses and malware, and often provide a convenient point of entry for hackers into a network. HTML email with embedded Javascript or ActiveX can wreak havoc on the network. Executables can be blocked at the firewall, but in addition to sending harmful attachments via email, hackers often use emails to entice recipients to click on links that take them to Web sites that are known to contain malware. The URL filter ensures that if the recipient clicks on such a site, the request will be blocked.

*P2P attacks.* Many of the executable files downloaded through popular P2P file sharing networks contain malicious code. Yet the popularity of downloading content such as music files via peer networks continues to grow, opening up the network to viruses, spyware, and other malware. Many security officers choose to block access to P2P file sharing networks completely, and to set the Web filter to prevent access to file-sharing Web sites.

*Phishing and pharming attacks.* Phishing is when an attacker attempts to fraudulently acquire sensitive information, such as passwords or account numbers, by fooling the recipient of an email into thinking that the email is from a trusted institution. The email is in reality from someone impersonating the trusted institution. A pharming attack involves hijacking a Web browser for the purpose of redirecting requests or spoofing the address bar. These dangerous attacks can also be prevented through a combination of means, starting with preventing users from downloading executables using a firewall for perimeter protection. Fraudulent emails can be caught using anti-spam and anti-fraud technology, and a Web filter can block the bogus Web sites.

*Spam attacks.* Spam, or unsolicited "junk mail" in your email box, is a growing problem not only from the perspective of sheer volume, but also because these messages waste time and resources. It may also lead some unwary users to sites that contain malware. Current technologies for blocking Spam include a variety of means: blacklists of known spammers' addresses or domains, challenge/response techniques, and Bayesian filters. Web filtering extends another layer of security in a compelling way by harvesting URLs from identified Spam messages and categorizing them. In this fashion, when Spam finds its way into the network, and inevitably it will, users that feel the need to click on included links can be stopped before the request is sent outside the network.

## A word on attacks from the inside

Risks don't always come from outside attackers, those that would seek to do harm may come from within. A CSI/FBI Computer Crime and Security Survey revealed that over 75 percent of companies cited disgruntled employees as a likely source of hacking attacks, and 45 percent of businesses reported unauthorized access by insiders. A study from a threat management and risk assessment firm discovered that the majority of security and human resources executives say that workplace violence is a bigger problem now than it was two years ago, and 23 percent of those surveyed said that employees had intentionally downloaded viruses over the past 12 months. Outsourcers too are facing similar threats, particularly as companies shift towards a lean operating model and jobs shift to outsourcing agencies. Eighty-eight percent of outsourcers surveyed in another study said employee backlash is their primary concern.

A study conducted by the U.S. Secret Service and CERT Coordination Center/SEI highlighted the prevalence of insider threats in the banking and finance sectors. In one example cited, an employee of an international financial services company who had quit over a dispute concerning his annual bonus planted a "logic bomb," which deleted ten billion files in the company's network. In fact, insiders may well pose a greater threat than unknown attackers, because of their often very detailed knowledge of the company systems.

Many of the "insider" cases cited by the Secret Service study actually involved little technical skill, and in fact most cases involved insiders who were not employed in technical positions. Several of the insider attacks were able to be executed simply because of poor password and account management practices, and in one case, a company assigned default employee passwords that everyone knew to be the employee's office number.

Anyone inside the company can be a data thief, and the Secret Service study indicated that perpetrators did not share a common profile. Many insiders who had perpetrated attacks did not hold technical positions, and had no history of making any type of hacking attacks. Most had not been perceived as "problem" employees. Insiders ranged from 18 to 59 years of age, 42 percent were female, and they came from a variety of racial and ethnic backgrounds and family situations. Inside attackers with a known history of electronic abuses accounted for only nine percent of the incidents.

Incidents from within can also include an employee purposefully attempting to introduce spyware or other malware to the network via the Internet. Filtering can help reduce the risk of such inside attacks by blocking access to sites that host malware, thereby preventing intentional downloads of viruses and other harmful software to infect the network. Strong internet filtering is indispensable as part of a multi-tiered strategy to stop this and other threats from occurring.

## Sophisticated attacks

Hackers are opportunistic, and will take the easiest route to your network if possible. As described above, most attacks can be prevented with simple vigilance, good policy, and a multi-layered defense strategy. Nonetheless, some external attacks on networks are becoming increasingly sophisticated and include spyware, adware, hijackers, cookies, malware, phishing, spam, viruses and worms. To further complicate these things external attacks are becoming increasingly more sophisticated as they leverage employee use of email, Web surfing, messaging and P2P to enable their attacks.

Modern security attacks are rarely brute force attacks on single vulnerabilities. They are usually more complex, jumping from protocol to protocol. For example, an employee may receive a piece of spam email (SMTP). A Web beacon contained in an image in the email sends your identity back to a central site via HTTP after you click on the image to access the site. Another example is when an employee downloads an IM client and inadvertently activates a spyware program that opens a back door to the network. The attacker leverages the employee's machine without his or her knowledge or permission. The spyware program then uses IRC messages (ICMP) to send spam (via SMTP email) to other machines. A third example of a sophisticated multiprotocol attack is to cause a public Web server to experience a buffer overflow that causes active code to be added to the Web pages. The user executes the active code and this opens up a vulnerability in Internet Explorer.

According to the Office of the National Counterintelligence Executive, the Internet has become a major source of foreign collection of US Defense technologies. A report from the agency indicates that use of the Internet by foreign agencies to collect US technological information in 1999 accounted for 27 percent of suspicious contact reports made to the Defense Security Service by the defense industry.

What do all these attacks have in common? If you could control your HTTP requests, none of these attacks would work. The solution? Sophisticated Web filtering backed up by a robust filtering database can mitigate these risks.

## How SmartFilter Web filtering stops sophisticated attacks

Most people think of Web filtering as a tool for keeping objectionable Web sites, such as pornography sites, out of the workplace. And in fact, Web filtering excels in this regard. SmartFilter® Web filtering applications from Secure Computing® offer an extensive categorized URL database that is

the most thorough and most accurate in the industry. But the fact that is often overlooked is that some Web sites contain active malware. When a visitor comes to one of these Web sites, the malware (Trojans, viruses, spyware, etc.) automatically downloads itself into the computer—without the user having to take any action outside of simply visiting the page. Pornographic sites are particularly well-known for hosting spyware. When an employee visits a pornographic Web site, they aren't just wasting company time and offending their co-workers. They are opening up a door to the network, through which dangerous spyware or other malware may enter.

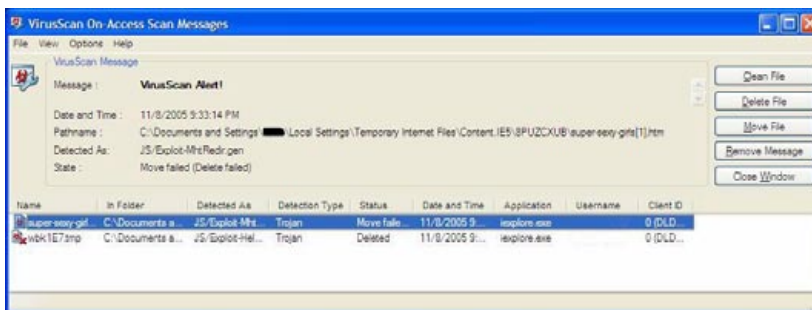
This problem is not going unnoticed. On October 24, 2005, XBIZ News in Cupertino, California, ran the article *Experts Say Most Spyware Generates from Porn Sites*, stating that:

*“Security experts have pointed the finger recently at porn sites as a major contributor to the spyware epidemic. Claiming that porn downloaded from the workplace contributes to more than half of all spyware, some security firms are saying the onus will soon be on company owners to better monitor employee behavior and keep their networks clean. Some security experts are even saying that companies could reduce the amount of spyware and adware on their networks by more than 50 percent if employees would stop visiting porn and gambling sites and employers would start using URL filtering software and set stricter policies outlining the use of company computers.”*

Full article: [http://www.xbiz.com/news\\_piece.php?id=10942](http://www.xbiz.com/news_piece.php?id=10942)

As a case in point, the following is a real and true example demonstrating how high the risk (and how easy it is) to infect computers when going to pornography sites. The screen capture below shows a virus scanner alert capturing and stopping Trojan malware from infecting the computer being used for access. Virus protection and Web filtering are both essential components in protecting your networks.

As a preventative measure against this and other threats, SmartFilter Web filtering is an important part of a multi-layered approach to stopping sophisticated attacks through different means, including the following points on prevention, real-time security updates, spam blocking, and reporting.



**Prevention: Controlling access and privileges.** By doing what it does best, SmartFilter restricts or prohibits access to sites known to contain spyware or other malware, or sites known to be associated with spam. In so doing, SmartFilter goes beyond the primary goal of restricting access to objectionable sites, to keep problems off the network. Filtering is the first line of defense, and minimizes the potential threats that have to be addressed by other layers of the security infrastructure such as firewalls, antivirus, anti-spam, or anti-spyware software. It can also control when and if a user can access or download specific file types, and lastly, reports on computers that have spyware to identify and isolate them.

**Real-time security updates.** SmartFilter security categories are continuously updated by Secure Computing's best-in-class database team, which is supported by world-class tools for harvesting information on bad sites. Secure Computing's sophisticated methods of gathering data on Internet threats, coupled with our automatic download of new database updates to your SmartFilter installation, means you don't have to worry about gathering that data—Secure Computing does it for you. And as soon as we uncover a potential threat, you're covered.

*Spam blocking.* Another security solution from Secure Computing, the Sidewinder G2 Security Appliance, includes an integrated, best-of-breed anti-spam engine that stops spam from entering into your network. SmartFilter works with Sidewinder G2's anti-spam engine and other sources to harvest URLs from spam email and categorize them. If a spam email does make its way into your email box, the URLs contained in the spam emails are blocked by SmartFilter before the request leaves the network, so access to the spam-related Web site (which may contain spyware or other malware) is prevented.

*Reporting.* SmartFilter's SmartReporter™ functionality is an essential part of identifying spyware and stopping the damage that results from it. Spyware can come into the network from many different paths, and a multi-layered approach here is the only way to prevent it. SmartReporter's Web usage reports are useful in tracking down a variety of security and liability problems. When spyware gets into your network, even if you don't know where it's located, you know it's there, because a large number of Web requests will come from one given Web site. This is because spyware sends a beacon from the infected workstation to a covert spyware server. The infected computer then sends a constant stream of information—not just consuming bandwidth, but potentially stealing valuable information and transmitting it back to an unknown host. SmartReporter's graphical reports are easy to understand, and make it possible to easily spot a potential infection and pinpoint the infected workstation. And because the solution is highly scaleable, you can view the entire global network, to find infected workstations anywhere.

## Controlling user access and privileges

A major part of network protection comes down to controlling user access. Even if your users mean no harm, they can still very easily bring down the entire network unintentionally by opening the door to malware. SmartFilter is one way to keep that door locked. But in fact, this is only half the battle. Desktop privileges are often set too high by default. According to the Yankee Group, "The biggest reason companies have spyware problems is the user privileges are set too high." Along with effective URL filtering, your security environment should include an enforceable, rigorous policy of authorization and authentication, which controls who has access to what, and when.

Preventing certain types of downloads or attachments that may deliver executables, MP3s, or ZIP files is an important policy item. SmartFilter's advanced policy engine puts an added layer onto your security, which prevents these types of attachments or files from entering the network.

## SmartFilter: an important component of a successful IT security strategy

SmartFilter has long provided networks with protection from users accessing security-related categories such as hacking sites, malicious Web sites, resource sharing, or remote access sites. As the Internet changes, SmartFilter has been tasked with taking on a greater role in our customers' security needs and concerns.

SmartFilter is now, more than ever, a critical component of any organization's network security. Not only does SmartFilter embolden the network's defenses against a myriad of threats, it constrains legal liability, and in doing so, assists in keeping network users on-task and frees up valuable digital resources for critical value-added purposes.

SmartFilter also provides both scheduled and real-time security updates. The application software has the ability to make frequent requests to Secure Computing to see if there is a new update available. Here at Secure Computing, whenever a critical addition is made to any security category, we have the ability to create and post this update to our download server. This combination of SmartFilter requesting frequent updates, and our list team's vigilance for security related sites makes for a powerful new combination extending much greater network protection for our customers.

SmartFilter prevents user access to sites known to propagate viruses, phishing scams, spyware, adware and more. This means that these potential browsing requests are never sent out, freeing bandwidth and other network resources from being taxed. Further, SmartFilter's SmartReporter is capable of identifying desktops that may have become infected by other means when they attempt to "call home"—laptops taken outside the secured network, or programs shared by disk, IM, P2P, and so on.

This does not negate the need for antivirus or anti-spyware solutions whose services come into play once virus or spyware programs are inbound or already in the network. SmartFilter Web filtering acts as a

first line of defense to prevent them from arriving in the first place. SmartFilter is an affordable solution, with one competitive price covering all blocking categories—there's no need to pay extra for full coverage.

As part of a multi-layered security strategy, SmartFilter's powerful Web filtering capability easily fits into almost any network infrastructure. SmartFilter is also available on Secure Computing's Sidewinder G2 appliances. As part our comprehensive Unified Threat Management (UTM) security strategy, which provides anti-virus, anti-spam, and many other protective features and benefits.

## Conclusion

---

Web filtering is a critical component in a layered approach to security, which is the best approach for dealing with the increasing sophistication of today's security threats. Secure Computing's solutions provide sophisticated technology that's equipped to handle these threats, and allow you to fully enjoy the benefits of information exchange and the Internet, without having to worry about malicious content, spam, information theft, or problems associated with unregulated Web surfing.