Demystifying Internet Content Filtering
for Businesses, Schools, and Libraries

*Why it's needed, how it works, and
solutions from SonicWALL®*

CONTENTS

SONICWALL

Abstract

Businesses, schools, and libraries with Internet connections need the ability to control access to objectionable or inappropriate content and network threats. Without that control, these organizations risk productivity loss, security breaches, erosion of available bandwidth, and legal liability. The stakes are even higher for schools and libraries, which stand to lose federal funding if they do not provide the content filtering mandated by the Children's Internet Protection Act (CIPA) of 2000.

When selecting a filtering solution, businesses and schools need to be aware of the different approaches to filtering and their deployment methods. Depending on the level of filtering required, they can choose broadly between a site blocking and content monitoring approach. Both approaches can be deployed through client software, standalone or integrated filtering solutions—each deployment method varies in terms of effectiveness, cost, and manageability.

This white paper makes the business case for content filtering, explains solution options, and describes how SonicWALL solutions enable optimum protection and productivity for businesses, schools, and libraries of all sizes.

Importance of Content Filtering

For businesses

As Internet use grows in business, so do the risks of uncontrolled access. When workers inadvertently or deliberately access sites containing inappropriate, illegal, or dangerous content, organizations lose productivity, expose themselves to legal liability, and in some cases experience degraded network performance. There are also a growing number of security risks from Trojans and worms that can be introduced into the network causing serious damage. An effective filtering solution can help solve these problems by blocking access to inappropriate Web sites or those that can detract from employee productivity.

Improving employee productivity

Restricting Web access to inappropriate sites helps companies prevent excessive non-productive Web surfing and preserves network bandwidth. According to a survey by SonicWALL and its partner Cerberian, employees report:[1]

- 16% have knowingly surfed pornography sites at work at least once
- 40% have seen co-workers surf pornography sites
- 32% have seen co-workers surf gambling sites
- 91% have seen people shopping online
- 85% have seen co-workers surf sports-related pages
- 55% spend more than 10% of their time at work surfing the Web for personal reasons, which is roughly equivalent to four hours per week, or nearly nine days a year (see figure 1)

---

[1] 2004 Web Usage Survey, Cerberian and SonicWALL, May 26, 2004. (Cerberian is an application services company that provides Internet access control solutions.)
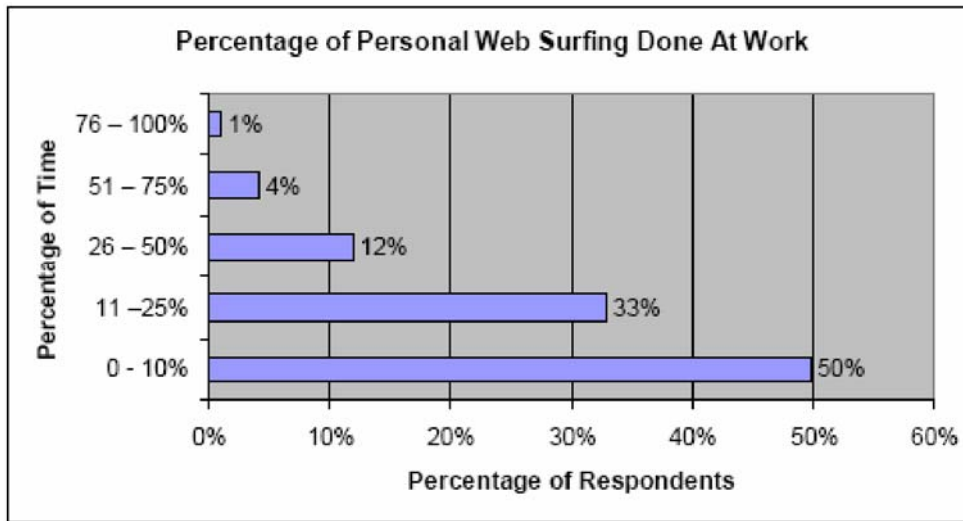
Percentage of Personal Web Surfing Done At Work

Figure 1 – Percentage of personal Web surfing done at work (source: SonicWALL and Cerberian)

Minimizing liability exposure

Employees who visit pornographic or racist/hate sites represent a major legal liability concern. A 2004 study by the Employment Law Alliance (ELA) reported that 24% of workers said that they or their co-workers use workplace computers to visit pornographic Web sites, engage in sex talk through instant messaging, or pursue other sexually-oriented Internet activities.[2] Businesses need to shield themselves from potential legal liability that can arise if an employee repeatedly sees offensive material on a co-worker's computer.

Another source of liability exposure is peer-to-peer networking and file sharing, which have opened the door to charges of copyright violations and high-profile litigation. The legal liability exposure when employees use the Internet to download MP3s, full-length DVDs, or copyrighted software is burgeoning: the Recording Industry Association of America (RIAA) recently collected a $1 million fine from an organization found to have copyrighted music files on its corporate network.[3] In addition, the Motion Picture Association of America and other groups have warned CEOs of Fortune 1000 companies that their corporations will be held liable for breaking copyright laws if employees use company networks to download music or movies illegally.

Preventing hacker attacks and protecting privacy

Blocking instant messaging, peer-to-peer file sharing and multimedia also helps protect the network from backdoor attacks. The threat is rising. As of December 2003, 45% of the free files collected via KaZaA contained viruses, Trojan horse programs, or backdoor programs.[4] The latest threat comes from a new virus which uses instant messaging and peer-to-peer networks to entice users to download and view JPEG images infected with malware[5]. Blocking peer-to-peer file sharing and multimedia protects against this threat to network resources. In addition, blocking automatically-downloaded files such as Java applets and

---

[2] "Sex in the Workplace," Employment Law Alliance, Steve Hirschfeld, February 2004

[3] *Electronic Musician*, April 2002

[4] "2003/2004 Trends and Predictions in Network Security", *TrueSecure*, December 2003

[5] "Face Time Warns Enterprise of New JPEG Virus Propagating Via Instant Messaging and Peer-to-Peer Networks", Face Time Communications, September 2004

ActiveX scripts helps protect employee privacy. Hackers sometimes use these scripts to read cookies that Web sites write to employee desktops. The cookies can reveal personal information about employees, such as sites visited or buying habits.

For schools and libraries

Schools and libraries benefit from content filtering for many of the same reasons as businesses. In addition, content filtering addresses certain other requirements unique to schools and libraries:

- *Protecting students*—Students need to be protected from inappropriate Web content and chat rooms. Nearly 90% of sexual solicitations of children are made in chat rooms and through instant messaging.[6]

- *Keeping students focused*—Shielding students from distraction caused by non-educational Web sites helps keep them focused on the curriculum. Similarly, blocking instant messaging and peer-to-peer file sharing eliminates another distraction while preserving network bandwidth.

- *Legal liability*—The explosive growth of peer-to-peer file sharing on campuses has introduced significant liability concerns, most notably in the area of copyright infringement. Schools must avoid being found complicit in enabling illegal student activity. A comprehensive content-filtering solution provides network administrators with the tools to manage the use of peer-to-peer applications. It also helps ensure that the school cannot be perceived as fostering an environment that facilitates the duplication and transfer of copyrighted materials.

- *Protecting federal funding*—Schools and libraries must adhere to certain conditions to receive discounted rates for Internet access as stipulated by the Federal E-rate program. Under the Children's Internet Protection Act (CIPA), K-12 public schools and libraries are entitled to federal assistance for Internet access only if they adopt an Internet Safety Policy and install filtering technology to prevent minors from accessing harmful materials[7]. CIPA applies to all schools and libraries that receive discounted rates for the purchase of equipment and services used to access the Internet through the E-rate program, the Library Services and Technology Act (LSTA), or Title III of the Elementary and Secondary Education Act (ESEA).

How Content Filtering Works

Content filtering involves denying or allowing access to certain Web sites based on predetermined criteria. Basic content filtering restricts users' access to Internet content based on the URL or URL content category, such as nudity or gambling, or based on the way the content is delivered, such as through Java applets or ActiveX scripts. More advanced filtering solutions also provide the ability to block applications like instant messaging and peer-to-peer services.

Site blocking versus content monitoring

Filtering solutions employ one of two basic approaches: site blocking or content monitoring. While there are considerable differences between these two approaches, both are based on pass-through filtering technology. That is, all requests for Web pages pass through an Internet control point such as a firewall, proxy server, or caching device. The device then inspects each request to determine whether it should be allowed or denied.

---

[6] "Risk Factors for and Impact of Online Sexual Solicitations of Youth," Mitchell et al., *Journal of the American Medical Association*, June 2001

[7]"Internet Safety Policies and CIPA: An E-rate Primer for Schools and Libraries", E-rate Central

Site blocking

The site blocking approach to filtering typically uses list-based or URL-based filters to identify and block certain Web sites. Some solutions rely on "white lists", which permit access only to the sites on the list. For example, a retail store might create a white list containing only the company's Web site, shipping Web sites, and supplier Web sites. Other solutions use "black lists," which permit access to all sites *except* those on the black list. The black list approach is preferable for businesses and schools whose users need less restrictive Internet access in order to engage in research activities. With a black list approach, the database of Web sites is organized into categories such as "violence" or 'drugs" and network administrators can select a set of categories to block.

The effectiveness and manageability of site blocking depends on a number of factors. The larger the database, the more inappropriate Web sites it is likely to block. However, with new sites being created daily and many existing ones being relocated, update frequency is also critical. Most site blocking solutions update their databases on a daily basis, often automatically downloading new URLs every night. Another important factor is how the database is organized into categories. For example, a high school could create a category for both pornography and sex education – this would allow them to block inappropriate material while still providing access to educational sites on the human reproductive system.

A general limitation of site blocking is that it focuses exclusively on HTTP-based Web traffic. It does not block instant messaging, e-mail attachments, peer-to-peer applications, and other applications that could contain security threats.

Content Monitoring

The most basic level of content monitoring uses a keyword-blocking approach. Instead of blocking URLs, it analyzes the data being sent against a user-defined library of words and phrases. When a match to one of the blocked words or phrases is detected, the solution filters or blocks the data, or in some cases even closes the application. The problem with this approach is that it can inadvertently block legitimate pages based on the fact that they contain one or more targeted keywords – e.g. a Web site on cancer research could be blocked because it contains the word "breast".

More advanced content monitoring solutions not only examine the words on the page, they also look at the context in which these words are used as well as other data such as HTML tags. Armed with this information, they can build a clearer picture of the Web site and determine whether or not it should really be blocked.

Another valuable advantage of content monitoring is that the user can monitor and filter content not only from Web sites, but also chat rooms, instant messaging, e-mail attachments, and Windows applications.

Solution architectures

Filtering software is typically either embedded on a networked device, such as a proxy server, caching appliance, or firewall, or resides by itself on a dedicated server running the Microsoft Windows, Linux, or UNIX operating system. The three common deployment methods vary in terms of effectiveness, cost and manageability.

Client solutions

Installed on the desktop, client solutions are most suited for home environments, for parental controls. The software includes a management interface and a database of blocked Web sites; the parent downloads database updates via the Internet. Leading providers of client solutions include Zone Labs, Net Nanny®, and Internet Service Providers (ISPs) such as Microsoft® MSN and AOL®.

Standalone solutions

Standalone solutions consist of a dedicated database server and a separate gateway or firewall that enforces the content filtering policies on the server. These solutions are more manageable than client-based solutions because the administrator can create a filtering policy once on the gateway and then apply it across all desktops. However, most standalone solutions require the businesses and schools to purchase and manage two separate hardware devices in addition to content filtering software. They also need to purchase additional storage for their database server as the database of Web sites grows. Key vendors of software/server solutions include Websense and SurfControl®.

Integrated solutions

Integrated solutions consolidate management and processing in a single gateway or firewall, thereby reducing capital and operational expenses. However, when the gateway or firewall is also used for services like anti-virus and intrusion prevention, performance can suffer. Key vendors of integrated content filtering solutions include Symantec™ and WatchGuard®.

SonicWALL Content Filtering Solutions

Depending on performance and management requirements, businesses, schools, and libraries can choose between the SonicWALL Content Filtering Service (CFS), which is an integrated solution, and the SonicWALL Content Security Manager 2100 Content Filter (CSM 2100 CF), a standalone solution.

At the core of both solutions described here is a rating architecture that leverages a comprehensive database of millions of pre-rated Web sites and domains. When a user attempts to access a Web site, the URL is cross-referenced against a master ratings database located at one of SonicWALL's worldwide co-location facilities. A rating is returned to the appliance and compared to the content filtering policy established by the administrator. If the Web request is permitted, the user is able to view the page and the site is cached on the appliance. If the requested Web site is denied, a custom block message informs the user that the site has been blocked according to policy.

SonicWALL's CSM 2100 CF also features an on-board dynamic rating engine. When users request a new URL that has not been rated in the master ratings database, the dynamic rating engine retrieves the page from its host server for analysis. The engine considers the words on the page, context for each word, and HTML tags. When the analysis is clear, the engine produces a rating and category and immediately blocks or allows the site based on the organization's access policy. The site is also added to the master ratings database for future reference by subsequent requests.

SonicWALL Content Filtering Service

The SonicWALL Content Filtering Service (CFS) is a cost-effective, integrated solution designed for businesses and schools with small to mid-sized networks. Available as an optional service for any SonicWALL security appliance, SonicWALL CFS leverages a continuously updated, comprehensive database of millions of Web sites, domains, and IP addresses. Minimal administrative overhead means that organizations can either manage the solution themselves or outsource the task to their IT service provider.

The following are sample user scenarios for fictional businesses and school districts that would be well served by the SonicWALL CFS.

Smith & Sons, Inc.: Smith & Sons is a small family-run business with 30 employees. The company wants a filtering solution that will help preserve limited network bandwidth for work-related Internet traffic. The company also wants to improve productivity by preventing employees from accessing online shopping and

sports sites during work hours. Without the budget for a dedicated network administrator, Smith & Sons needs a "set and forget" solution.

George Washington School District: *George Washington school district is a mid-sized school district with 16 schools distributed across a 5,000 square miles radius. Each school has a mixture of desktop computers and laptops used either by administrators or students. The district needs a firewall, as well as filtering capabilities to ensure compliance with CIPA. It also needs a low-maintenance solution because a small technical staff supports the entire district.*

SonicWALL's Content Filtering Service (CFS) is ideal for both organizations because it:

- Is easy to install and manage - installs on any SonicWALL firewall, and automatically pushes out filtering policies and updates to all users

- Scales easily to accommodate more users - the organization simply installs an appliance in the new building

- Provides granular policy control, so each school can set its own filtering policies based on students' grade levels and needs

- Allows administrators to assign "bypass filter" privileges to certain users, such as a teacher who needs access to a breast cancer Web site

- Increases security and privacy by blocking automatically downloadable files like Java, ActiveX and cookies

SonicWALL Content Security Manager 2100 Content Filter

The SonicWALL Content Security Manager 2100 Content Filter (CSM 2100 CF) is an affordable alternative to enterprise-class content management solutions, designed for businesses and schools with demanding content filtering requirements. This full-featured, appliance-based content filtering solution integrates seamlessly into virtually any network, whether it uses a SonicWALL or third-party firewall. Unlike other standalone filtering solutions, the SonicWALL CSM 2100 CF is highly scalable and does not consume additional bandwidth as the organization adds new users or applies more complex filtering policies.

The SonicWALL CSM 2100 CF delivers high performance and fine control over content filtering. It features an onboard dynamic rating engine to analyze and rate new URLs in real time. Integrated support for Active Directory® enables network administrators to manage all users through a single interface, while the option to create custom categories and URL-rating lists provides more granular control over filtering policies (see figure 2). The SonicWALL CSM 2100 CF also blocks instant messaging, peer-to-peer, and multimedia applications for added security and better bandwidth management.
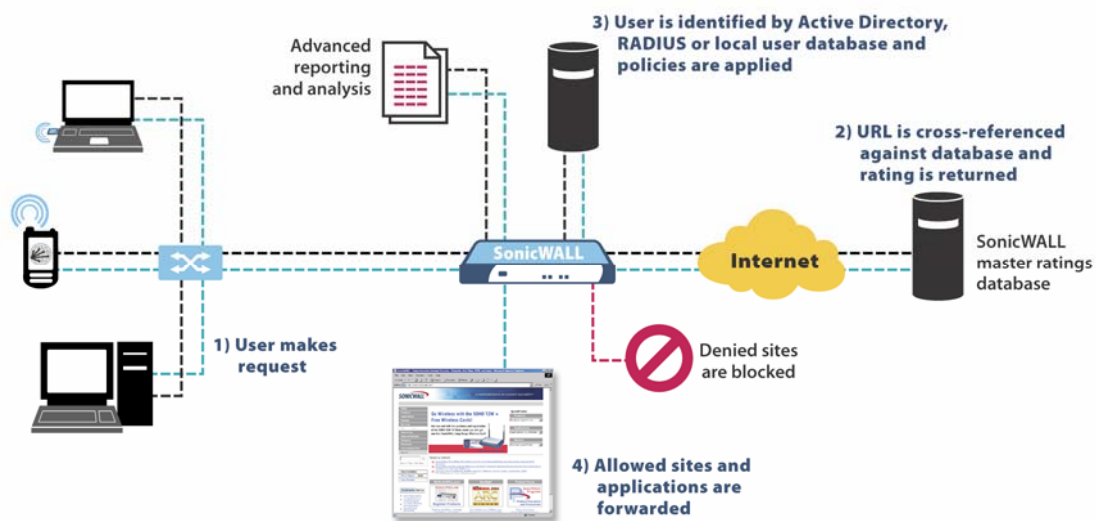
Figure 2: SonicWALL CSM 2100 CF

The following are sample user scenarios for fictional businesses and school districts that would be well served by the SonicWALL Content Security Manager 2100 Content Filter.

Metropolitan Law Offices: This 1000-person law firm has a headquarters and several smaller branch offices. A firewall installed at headquarters protects against network threats and provides anti-virus and basic content filtering. However, the firm is seeking a high-end, dedicated filtering solution that will free up bandwidth on the firewall and offer additional features like the ability to block peer-to-peer file sharing and instant messaging. Centralized management is also important because the firm wants the ability to centrally create, distribute, and enforce policies. The firm has limited IT resources, so easy deployment and manageability are essential.

Martha Washington School District: This is a large school district with over 45 schools. It currently has a server-based filtering solution, which has become too expensive to maintain and manage because it requires two hardware devices in addition to filtering software. Also, the district will soon need to purchase extra server storage to accommodate the growing number of Web sites and ratings. A serious problem is that students continually try to access new sites, some of which are not rated. The ability to rate sites on-the-fly would help the school provide better protection for students while complying with CIPA requirements. Finally, the district wants the ability to see what sites students visit: useful information for fine-tuning the filtering policy.

SonicWALL's Content Security Manager 2100 Content Filter is ideal for the above scenarios because:

- It incorporates all of the most-used features of higher-end solutions at an extremely competitive price point

- Integrates seamlessly with the existing firewall devices from SonicWALL and other vendors, leveraging existing investments

- Provides comprehensive filtering without adversely affecting network performance

- Protects users from inappropriate content even if the URL is not rated, thanks to the built-in dynamic rating engine that rates new sites as they appear

- Blocks peer-to-peer file sharing and instant messaging, freeing up valuable bandwidth and helping avoid legal liabilities associated with downloading copyrighted files

- Provides detailed reporting of network usage and content filtering so the administrator can change filtering policies accordingly

- Integrates with Active Directory for minimal administrative overhead

Features and Benefits

The following are key features of the SonicWALL content filtering solutions. Features marked with an asterisk (*) are available only on the SonicWALL Content Security Manager 2100 Content Filter.

Policy management

SonicWALL filtering solutions provide businesses, schools, and libraries with complete control over filtering by allowing network administrators to override policies for specific sites. An administrator can provide access to an individual site whose rating is disallowed by categorizing it as an "allowed domain." For example, a high school social studies teacher might request access to sites bearing the "Hate/Racism" rating during a unit on the Civil Rights Era.

Similarly, to block a site that does not fall into one of the specified categories, the administrator can identify it as a "blocked domain." For instance, a business might add a sports site to the list of blocked domains in the cache to maintain employee productivity during a popular sports event.

Administrators can allow certain users and guests to bypass the filter policy. If an adult library patron asks for unfiltered Web access, for example, the librarian can assign the patron a pre-defined username/password combination with bypass privileges or instantly create a custom account.

SonicWALL filtering solutions offer the ability to create multiple polices representing different filtering levels. This gives administrators the flexibility to enforce custom policies for groups of users on the network. For example, schools can create one filtering policy for students and another for teachers. Similarly, network administrators can create different filtering policies for various different departments within a company. Network administrators can also choose the hours during which content filtering applies. For example, a school might filter certain content categories during school hours, and then remove that filter at the end of the school day.

Custom rating categories

The network administrator can block any combination of categories, changing them on demand as organizational policies change. When the administrator changes the policy, the SonicWALL content-filtering solution immediately begins comparing the ratings in the cache against the new policy. In addition, administrators can create their own custom rating categories and block/allow the subset.

Integrated dynamic rating engine*

When users request a new URL that has not been rated in the master ratings database, the SonicWALL CSM 2100 CF uses its unique dynamic rating engine to retrieve the page from its host server for analysis. The engine considers the words on the page, context for each word, and HTML tags. When the analysis is clear, the engine produces a rating and category and immediately blocks or allows the site based on the

organization's access policy. The site is also added to the master ratings database for future reference by subsequent requests. If the site is more difficult to rate and categorize, the rating engine categorizes it as "other" and flags it for additional review.

Application controls*

Instant messaging, peer-to-peer, and multimedia applications can pose a risk to security and increase liability exposure. Instant messaging, for example, can be used to transmit important company information in unencrypted formats or to transfer file attachments that bypass the security infrastructure. Peer-to-peer networks often are used to acquire copyrighted music files or pornographic material generating liability concerns. And use of multimedia applications during work or school hours can divert bandwidth from applications that are critical. SonicWALL CSM 2100 CF includes the application and protocol filtering capabilities of SonicWALL's deep packet inspection intrusion prevention technology. This effectively enables users to block downloading of peer-to-peer, instant messaging, or multimedia applications.

Active Directory® integration*

Integration with Microsoft Active Directory allows network administrators to create policies that reflect the existing organizational hierarchy and to manage all the users through a single interface. When a user joins a different group within the organization, or when the enterprise goes through re-organization, the SonicWALL content filtering solution automatically updates users' policy according to their new roles as entered in Active Directory.

Smart URL parsing*

Smart URL parsing enables the SonicWALL CSM 2100 CF to make a decision on the status of the URL based on the entire URL—not just its domain and path portions. This provides an added layer of protection by preventing users from accessing cached versions of blocked sites.

User-Level Authentication

Administrators can support organizational goals for control and protection by specifying the users who will be granted Internet access, and their priority. Through User-Level Authentication (ULA), the network administrator can require individuals to log on to the network with their username and password. ULA works with existing authentication databases such as RADIUS and Active Directory (supported in SonicOS version 3.0 or later).

Web-based reporting

SonicWALL CFS can forward data directly to SonicWALL's optional ViewPoint® reporting package to generate detailed reports on Internet usage and content filtering. SonicWALL CSM 2100 CF includes an integrated, advanced reporting and analysis tool that administrators can use to create custom reports providing granular insight into network usage.

Conclusion

Content filtering is essential for businesses seeking to improve productivity and avoid legal liability. Educational institutions and libraries have both a fiduciary and legal responsibility to install filtering solutions in order to protect their students and young patrons from objectionable Web sites. Those that neglect to comply with regulations risk losing federal funding for technology programs.

SonicWALL offers two content filtering solutions to meet the varying performance, flexibility, and cost requirements of different organizations. SonicWALL CFS addresses the needs of small and mid-sized organizations that need a cost-effective, integrated solution with minimal administration overhead. The SonicWALL CSM 2100 CF delivers higher performance and finer control over content filtering. Because they require only one local device and are subscription-based, both SonicWALL content filtering solutions are available at breakthrough price points.

To learn more about SonicWALL content filtering solutions, visit: http://www.sonicwall.com/products