Secure Content Management:
Protected, Productive Networks For Today's Schools and Libraries

The need for secure content, current technology directions, solution alternatives and application examples.

CONTENT

SONICWALL

Abstract: *Today's schools and libraries increasingly rely on the Internet for efficient access to information and resources. But organizations are faced with many challenges when it comes to managing the risks to internal networks and data. The risks can be classified in four categories: attacks to data and the network, abuses and inappropriate use of resources by authorized users, legal liabilities based on recent legislation requiring network managers to provide safe and appropriate environments for all network users, and the ability to efficiently administer networks. Some threats fall into multiple risk categories. For example, viruses, phishing programs, spyware and other external threats tax network support teams, erode bandwidth and can result in legal liabilities and vulnerabilities. Abuse of instant messaging and inappropriate peer-to-peer applications pose additional liabilities and can reduce productivity. The stakes are even higher with new legislation: schools stand to lose federal funding if they do not meet the requirements mandated by the Children's Internet Protection Act (CIPA) of 2000.*

This paper overviews the need for and characteristics of emerging technologies for controlling access to networks. Content filtering is compared to alternative site blocking approaches, and overall secure content management solution architectures are introduced. To assist users that are evaluating content management solutions, integrated solutions are compared with standalone appliances and critical features for both options are described. Application examples are included to illustrate the benefits of secure content management for different organizations. Throughout, the organizational needs are discussed in terms of protection, productivity, liability and administration requirements.

The information presented in this paper represents the industry experience of the SonicWALL® research and development team and reflects the requirements that can be met by applying SonicWALL secure content management solutions. The SonicWALL solutions are referenced in the conclusion to this paper, and can be reviewed in detail on the SonicWALL Web site: http://www.sonicwall.com.

The Importance of Secure Content Management

Key Issues For Schools and Libraries

Schools and libraries, while vulnerable to many of the same security threats as businesses, also have some unique requirements for controlling access. The driving factors for security requirements in schools and libraries include:

- **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.[1]
- **Keeping students focused**—Non-educational Web sites distract students from the curriculum. Similarly, instant messaging and peer-to-peer file sharing shift focus away from studies, and can also negatively impact network bandwidth.
- **Minimizing 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. Network administrators need tools to manage the use of peer-to-peer applications, and to foster an environment that discourages and prevents the duplication and transfer of copyrighted materials.
- **Meeting the requirements of the CIPA**—Schools and libraries must adhere to certain conditions to receive discounted rates for Internet access as stipulated by the Federal E-rate program[2]. Under the

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

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 content management technology to prevent minors from accessing harmful materials. 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).

Other Dangers of Unrestricted Access

The use of the Internet is on the rise, as are the risks of uncontrolled access. When staff, students, or other users inadvertently or deliberately access sites containing inappropriate, illegal, or dangerous content, serious consequences result:

- **Impacted productivity**—Restricting access to inappropriate Web sites helps schools and libraries prevent excessive non-productive Web surfing and preserves network bandwidth. Surveys of businesses report growing incidences of inappropriate network usage, and with children on their networks, the possibilities for inappropriate behavior increases for schools and libraries.

- **Liability exposure**—Network users who visit pornographic or racist/hate sites represent a major legal liability concern. As employers, schools and libraries are vulnerable. 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.[3] School districts and libraries need to shield themselves from potential legal liability that can arise if an employee is repeatedly exposed to offensive material on a co-worker's computer or anywhere in the workplace. Other sources of liability exposure include peer-to-peer networking and file sharing, which have opened the door to charges of copyright violations and high-profile litigation. When employees, students, or library patrons use the Internet to download MP3s, full-length DVDs, or copyrighted software, the network operator is legally liable.

- **Hacker attacks and privacy violations**—Instant messaging, peer-to-peer file sharing and multimedia downloads make networks vulnerable to backdoor attacks. According to TrueSecure, 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 using instant messaging and peer-to-peer networks to entice users to download and view JPEG images infected with malware.[5] In addition, automatically downloaded files such as Java applets and ActiveX scripts can threaten employee privacy. Hackers sometimes use these scripts to read cookies that Web sites write to user desktops. The cookies can reveal personal information—such as sites visited or buying habits—about school and library employees, students and library patrons.

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

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

[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

How Secure Content Management Works

Securing content starts with controlling access to certain Web sites based on predetermined criteria. At a basic level, user access to Internet content is controlled using the URL address or the URL content category, such as nudity or gambling. Basic content management solutions can also examine the way the content is delivered, such as through Java applets or ActiveX scripts, and determine access permissions accordingly. More advanced content management solutions also provide the ability to block applications such as instant messaging and peer-to-peer services.

Site Blocking Versus Content Monitoring

Secure content management 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 evaluates each request to determine whether it should be allowed or denied based on school policy.

Site Blocking

The site blocking approach for content management typically uses list-based or URL-based filters to identify and block certain Web sites. Some solutions rely on white lists that allow access to only those sites that appear on the list. Other solutions use black lists, which permit access to all sites *except* those on the black list. The black list approach is preferable for schools whose users need less restrictive Internet access. With a black list approach, the database of Web sites is organized into categories, such as "violence" or "drugs," and network administrators can selectively block categories.

The effectiveness and manageability of site blocking depends on a number of factors:

- **Database size**—A larger database allows more sites to be added to the restricted list.
- **Update frequency**—New sites continually emerge, and many existing sites are relocated. Most site blocking solutions update their databases on a daily basis, often automatically downloading new URLs every night.
- **Category organization**—Definition of categories must be carefully considered to accomplish effective restrictions while allowing access when appropriate. For example, a high school might require categories for both pornography and sex education, allowing them to block inappropriate material while still providing access to educational sites providing details 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 compares the keyboard data to 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. For example, a Web site about cancer research could be blocked because it contains the word "breast."

More advanced content monitoring solutions not only examine the individual words on the page, but also evaluate context and other data such as HTML tags. Armed with this information, advanced content monitoring solutions can more accurately assess Web sites and consequently more accurately control blocking.

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

Solution Architectures

Content management software can be embedded on a networked device such as a proxy server, caching appliance, or firewall, or it can reside 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 where parental control is the primary application. Client software solutions include 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 for defining policies and a separate gateway or firewall that enforces the content management policies. These solutions are more manageable than client-based solutions because an administrator can create a policy once on the gateway and then apply it across all desktops. However, most standalone solutions require organizations to purchase and manage two separate hardware devices in addition to content management software. They also require additional storage to be purchased as needed, when the policy database grows to exceed the storage available. Key vendors of standalone solutions include SonicWALL®, 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 SonicWALL®, Symantec™ and WatchGuard®.

Evaluating Solutions

Depending on the levels of protection, performance and manageability required, schools and libraries should choose between an integrated solution and a standalone appliance. Both alternatives can combine Internet content management with dynamic threat protection techniques to control access and secure the network against an array of threats from viruses, spyware, worms, instant messaging and peer-to-peer applications.

At the core of both integrated and standalone solutions 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. These databases can be managed and maintained by the content filtering solution vendor, and made available at multiple locations for performance efficiency and high availability. A rating is returned to the requestor 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. If the requested Web site is denied, a custom block message informs the user that the site has been blocked according to policy.

Integrated Content Management and Firewalls

Content filtering integrated on a firewall is a cost-effective content management solution that is ideal for schools and libraries with small to mid-sized networks. This alternative integrates the existing firewall technology, or is installed simultaneously with a new firewall solution. A typical service will make available 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 a service provider.

Standalone Appliances

For larger networks and environments requiring more comprehensive content control abilities, a standalone content filtering appliance maximizes the protection of any network from today's sophisticated Internet threats. Although it requires the purchase of additional hardware, ease of installation and use make this an attractive solution. The appliance can be dropped in to the existing network without any reconfiguration of existing hardware or software. Appliances are also an affordable way to upgrade existing firewalls by introducing new functionality without an actual upgrade on the firewall itself. A standalone appliance can affordably combine Internet content management with real-time gateway anti-virus and anti-spyware capabilities, and the best appliances are rich in features and functionality and deliver superior value for the investment. Beyond these advantages and basic Web site access controls, other advantages of a standalone appliance include:

- **Seamless integration**—Appliances can be easily installed in virtually any network, and combined with any existing firewall. Plug-and-play designs speed installation, making them drop-in solutions that eliminate the need for additional servers or hardware.
- **Dynamic rating engine**—Built-in capabilities can dynamically evaluate new URLs. Real-time analysis of page content, context for flagged words, HTML tags and other data can produce a rating and category for immediate access or blocking based on the organizations' predetermined policies. New ratings can be automatically added to a master ratings database for subsequent requests.
- **Protection from attacks**—Deep packet inspection technology can block viruses, worms, Trojans, spyware, phishing, malicious code and other attacks before they are able to infect a network. Appliances can scan and clean network traffic over a multitude of ports and protocols including HTTP, SMTP, POP3, FTP and NetBIOS.
- **Advanced security for bandwidth protection and reduced legal liabilities**—Appliances can provide controls for managing instant messaging, peer-to-peer and multimedia applications.
- **Management and reporting capabilities**—Integrated support 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 1). Advanced reporting and analysis tools provide granular insight into network usage through custom reports.

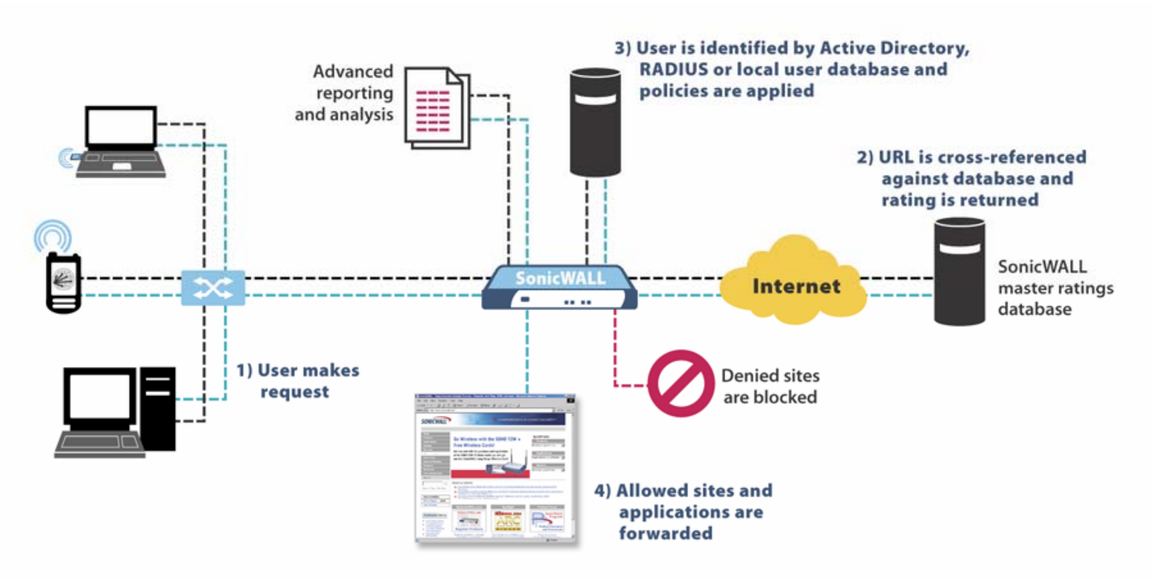
Advanced reporting and analysis
3) User is identified by Active Directory, RADIUS or local user database and policies are applied
2) URL is cross-referenced against database and rating is returned
SonicWALL
Internet
SonicWALL master ratings database
1) User makes request
Denied sites are blocked
4) Allowed sites and applications are forwarded

Figure 1. SonicWALL CSM 2100 CF

Critical Features and Associated Benefits

Whether evaluating and selecting an integrated content management solution or a standalone appliance, customers can identify superior solutions as those that offer many of features described in this section. The features cover the three key functional requirements of a secure content management solution—protection, productivity and liability—while also providing scalability and ease of administration. At the end of this section, Table 1 summarizes the features by these categories.

Policy Management

Policy management features provide organizations with complete content management control 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 when students are studying the Civil Rights Era.

Similarly, to block a site that does not fall into one of the specified categories, the administrator should be able to tag it as a "blocked domain." For instance, a sports site might be added to the list of blocked domains to maintain productivity during times when popular sporting events are happening.

Content management solutions can also allow administrators to designate certain users and guests to be given bypassed access that disregards 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.

Superior content management 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 policy for students and another for teachers. Similarly, network administrators can create different policies for children and adult patrons at libraries. Network administrators can also choose the hours during which specific content policies 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

This feature lets network administrators block any combination of categories, changing them on demand as organizational policies change. When the administrator changes the policy, the content management solution should immediately begin using the new policy. In addition, administrators should be able to create custom rating categories and specify policies for blocking/allowing the custom subset.

Integrated Dynamic Rating Engine

When users request a new URL that has not been rated in the master ratings database, appliances with an integrated dynamic rating engine can retrieve the page for real-time analysis and classification. If the site is difficult to rate and categorize, the rating engine should categorize it as “other” and flag it for additional review by the network administrator.

Gateway Anti-Virus and Anti-Spyware Protection

Truly secure content management solutions combine large-scale network filtering with real-time gateway anti-virus and anti-spyware capabilities. Deep packet inspection and a dynamically updated signature database can be applied for complete threat protection and to eliminate threats before the network is infected. Superior solutions go beyond simple port blocking to match downloaded, e-mailed and compressed files against an extensive signature database to block viruses, worms, Trojans, spyware, key loggers, phishing and malicious code. Deep packet inspection enables excellent protection while minimizing the number of false positives. When comparing anti-virus and anti-spyware effectiveness, evaluate each solution’s characteristics including high-performance deep packet inspection features for handling:

- Large (unlimited) file sizes
- Thousands of concurrent downloads
- Compressed files (technology for decompressing and scanning files on a per-packet basis)
- Frequently updated signature databases (to avoid attacks by new threats)
- Third-party access to signature database (open solutions that invite multivendor participation in threat detection)

Layered Protection

To provide adequate protection from threats, secure content management solutions must introduce controls and access restrictions in multiple layers on the network. Firewalls and gateways provide first-line defense, especially from external threats, but alone are not adequate for protecting from internal threats and inappropriate uses of the network. Additional controls and traffic inspection techniques must be applied at the packet level, across the entire network.

Application Controls

Solutions should include a range of application and protocol filtering capabilities utilizing intrusion prevention technology. This effectively enables blocking the downloading of peer-to-peer, instant messaging or multimedia applications.

Active Directory integration

Integration with Microsoft® Active Directory® software allows network administrators to create policies that reflect the existing organizational hierarchy and to manage all the users through a single interface with a single sign-on. When an employee moves to a different school or department within the district or when the district goes through re-organization, the content management solution should automatically update policy according to the new roles entered in Active Directory.

Smart URL Parsing

Smart URL parsing enables the content management solution 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 need to support organizational goals for control and protection by being able to specify the users who will be granted Internet access, and assigning the users priorities. Solutions should also support User Level Authentication (ULA), so that the network administrator can require each individual to log on using username and password. ULA works with existing authentication databases such as RADIUS and Active Directory.

Web-based Reporting

Optional reporting packages should be available and easily interfaced with the content management solution, enabling administrators to generate detailed reports on Internet usage and content filtering. An integrated, advanced reporting and analysis tool lets administrators create custom reports and provide granular insight into network usage.

Table 1. Functionality Supported By the Key Features of Content Management Solutions

Features	Protecting Data And Network Assets from Threats	Maximizing Productivity	Reducing Liability	Streamlining Administration
Granular, policy-based controls	■	■	■	
Manual policy bypassing				■
Custom rating categories				■
Dynamic rating engine	■	■	■	■
Virus and spyware protection:				
Port blocking	■	■	■	
Deep packet inspection		■	■	
Layered protection:				
Firewalls and gateways	■	■	■	
Packet inspection	■	■	■	
Application controls	■	■	■	
Active Directory integration				■
Smart URL parsing	■	■	■	
User-level authentication	■	■	■	■
Web-based reporting			■	■

Application Examples

The following fictitious scenarios represent two different types of schools that can benefit from content management solutions. In terms of their network needs, libraries closely resemble these schools. Recommendations are included for the specific types of solutions that would be most appropriate for each scenario.

Small Schools

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.

Recommendation

The above school district would be best served with integrated content management solutions. Small schools and libraries should look for solutions that offer:

- Easy installation and management—The solution should support any firewall, and automatically push out policies and updates to all users.
- Scalability for easily accommodating more users—Adding a new building or new user group should be easily accommodated with affordable add-on appliances.
- Granular policy control—Each school or office should be able to set its own policies based on employee functions, student grade levels or any other classifying characteristics within the user bases.
- Support for “bypass filter” privileges—Certain users, such as teachers or designated managers, should be able to gain unrestricted access to Internet sites.
- Automatic blocking of dangerous files—For increased security and privacy, downloading of Java, ActiveX and cookies must be blocked when specified.

Mid-sized and Large Schools

Martha Washington School District

With more than 45 schools, Martha Washington School District currently has a server-based content management solution that has become too expensive to maintain and manage. 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. Problems exist with students accessing new Web sites that are not yet rated and using bandwidth-intensive applications like instant messaging and peer-to-peer file sharing. The ability to rate sites on the fly would help the school provide better protection for students while complying with CIPA requirements. Application layer protection would help conserve network bandwidth while avoiding legal liabilities associated with file sharing Martha Washington School District is also looking for a dynamically updated gateway anti-virus and anti-spyware solution to protect their network from viruses, worms, Trojans, phishing, annoying spyware and other threats. Finally, the district wants the ability to see what sites students visit—useful information for fine-tuning the content management policy.

Recommendation

The above school district would be best served with advanced content management appliances. Mid-sized and large school districts and libraries should look for solutions that offer:

- All of the most-used features of higher-end content management appliances at an extremely competitive price point.
- The ability to integrate seamlessly with existing firewall devices from multiple vendors, leveraging existing investments.
- Comprehensive content management that does not adversely affect network performance.
- Protection of users from inappropriate content even if the URL is not rated (built-in dynamic rating engine that rates new sites as they appear).
- Blocking of peer-to-peer file sharing and instant messaging, to free up valuable bandwidth and help avoid legal liabilities associated with downloading copyrighted files.
- Ability to leverage deep packet inspection and a dynamically updated signature database to protect the network from a comprehensive array of threats including viruses, worms, Trojans, key loggers, script attacks, spyware and other malicious code.
- Detailed reporting of network usage and content access so the administrator can change policies accordingly.
- Integration with Active Directory for minimal administrative overhead.

Conclusion

Secure content management is essential for schools and libraries seeking to improve productivity, avoid legal liability and achieve CIPA compliance. Today’s institutions have even more pronounced fiduciary and legal responsibility to install content management solutions that protect students and young patrons from objectionable Web sites.

SonicWALL offers two solutions to meet the varying performance, flexibility and cost requirements of schools and libraries:

- SonicWALL Content Filtering Service (CFS) addresses the needs of small and mid-sized organizations that need a cost-effective, integrated content management solution with minimal administration overhead.
- SonicWALL Content Security Manager 2100 Content Filter (CSM 2100 CF) delivers complete content security management by combining comprehensive Internet content management capabilities with dynamic gateway anti-virus and anti-spyware protection.

Because they require only one local device and are subscription-based, both SonicWALL solutions are available at breakthrough price points.

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

©2005 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. G151_US.v2