

Content Filtering

Quinn A. Matthews, CCNA, CCA

Senior Network Engineer/Practice Manager

Are You or One of Your Partners Affected by Compliances?

How many of us are under one or more compliances such as HIPPA, Sarbanes-Oxley or Graham-Leach-Bliley? Are you partners with or do business with a company or organization that is under one of these compliances? Over the last few years, we have all heard talk about. If you're not currently required to meet one of these compliances, you probably have a business relationship with a company that is. They are going to be looking at you before long and asking "What are you doing about data security and data integrity." That time has come, and content filtering is but one step in the IT tapestry of network and data security in addition to a number of other reasons to implement content filtering.

Have you experienced your "protected" data leaving your company via the internet? There are many situations where protected or sensitive information has left an organization and found its way to a blog site or competitor.

Why Content Filter

A 2004 Employment Law Alliance(ELA), nearly one-quarter of workers (24%) purported that they or their coworkers use workplace computers to visit pornographic web sites, engage in sexual talk through instant messaging, or pursue other sexually oriented Internet activities.

Downloading of MP3s and full-length DVDs from web sites has become a major concern. The Recording Industry Association of America (RIAA) recently collected a \$1 million fine from an organization found to have copyrighted music files on the corporate network. In addition, the RIAA, the Motion Picture Association of America, and other groups recently warned CEOs of Fortune 1000 companies that their corporations will be liable for copyright laws if employees use company networks to acquire music or movies illegally.

The government sector is much like the private sector, with the addition of ensuring public funds are used appropriately. Law suits, either originating from the HR point-of-view or outside sources, are a costly use of tax payer money.

Schools, and not just schools as we think of them, but any after-school programs (community centers that offer programs to children) are also at risk and under the same compliances (e.g. CIPA (Children's Internet Protection Act) COPA (Child Online Protection Act)).

Beyond the prevalent problems with adult content on the internet, is online shopping, news, streaming audio/video, travel site, job searches, etc... Once you can close the loop on non-business related internet activity, productivity will increase. The bottom line is - time spent browsing the web is time not spent with customers or other tasks required for normal business operations.

With a T1 connection to the internet that is 1.4MB/second, suppose you have (20) users streaming audio at 56K. The math equates to a little over 1MB a second leaving only .3MB for business traffic. For many, this 80% of misappropriated resources can be a significant proportion of your resources directly affecting your ability to conduct business, which could include timely responsive to your customers.

Use of a Content Filter to Curb Human Error

Fringe web sites with questionable content are accessed by mistyping a legitimate web address or clicking a pop-up window. Some have even gone as far as to change the "CLOSE" button to the actual web page pop-up. One such case involved a user attempting to close what they thought was a pop-up window and in actuality installed a program that took over the desktop. No matter which icon the user clicked, it resulted with an open browser to a spam website.

Selecting a Content Filter

Hardware

Hardware solutions unlike software solutions eliminate time consuming separate installations OS and software. They're easier to administer upgrades whereas some OS upgrades may break or cause conflicts with pre-existing software installations.

Low Learning Curve

Look for a filter with a low learning curve. With limited bandwidth already, you probably prefer not to choose a solution that requires a strain on your IT skill-sets to install, configure and manage - including new training and certifications. We have enough invested in our current network infrastructures without having to learn skills for filtering our internet connections.

Simplified Administration

It is recommended that easy on-going management come into play when we evaluating solutions for content filtering - such as database updates, system updates, and ease of configuration changes.

Reporting

Compiling reports should be smooth and easy to read, yet provide flexibility to drill down and pulling out details for decision-making is an important factor to consider.

Reduced End-User Interaction

Less operator interaction for the end-user will benefit you, as end-users have a tendency to experiment with things, like anti-virus. How many times has a user disabled their anti-virus within your organization - the consensus reason? It slows down my computer!

How and Where Content Filterers fit into networks

Sniffers and Passive systems

Passively monitors internet traffic. When a packet is sent to the internet, the filtering system passes it to the classification system for a "block-no block" decision. If it is a "block", the filter system sends a pack to the end station that causes the connection to close. Timing is the big factor here, if this does not happen extremely fast, the content of the blocked site may make it to the end station.

Proxy filters

A proxy server acts as an interacting service between the workstation and the internet. Web browsers will go directly to the web server for the web site requested. When a proxy is in place, the proxy requests the page for the end station and the proxy server decides whether to block or not block. This usually involves changing the firewall to block all internet traffic except for the proxy server, or add the proxy server to the web browser. Most users have gotten sophisticated enough to remove this. Proxy servers add a tremendous amount of latency to the network. If the proxy server should go down, all internet traffic stops.

In-line

An in-line filtering system is located between your organization's network and the internet. As far as anyone on a company workstation is concerned, the system isn't there. Because the system sees every packet, it can examine each one to decide if it needs filtering. Filtering can be done through the use of user-level filtering or kernel-level filtering. In-line filters handle 100% of the network traffic because every packet goes through the filtering system. In addition, each packet, no matter to what port it is directed, can be examined for HTTP, IM, and P2P packets - and blocked or passed as required. Installation of an in-line filtering appliance is generally easy. They require no reconfiguration of any user system and almost no network configuration. All that's required is plugging it into your network between the internal core switch and outside firewall.

Because a dedicated system is being used and the filtering is being done at a low level, the system is fast. Also, because a total hardware/software solution is being provided, the designers can tune the device drivers and filtering system to make optimal use of the hardware. This allows the software to use the hardware to greatest efficiency. One of the techniques one such filtering appliance manufacturer uses is "zero latency" filtering. When a request for a new web site comes in, it is immediately passed through and sent to the web server. The appliance then makes the "block-no block" decision, while the web server is processing the request. If the decision is made to block, the system redirects the user to a screen explaining the situation. Any traffic from the web server to the user is blocked by the appliance. If the decision is made to not block, the system will let traffic from the web server reach the user.

In summary, content filters address compliancy requirements, helps make the best use of your internet resources, and generally increased productivity is a result. In is my opinion, the best way to proceed with content filtering is with a feature rich content filtering appliance that is easy to maintain.

#

Quinn A. Matthews, CCNA, CCA
(937) 384-0444 ext 2406
Email: quinn.matthews@digitalcontrols.com
Senior Network Engineer/Practice Manager

Quinn Matthews has been a member of Digital Controls service team for X years. As a Senior Network Engineer, Quinn is responsible for various networking practices across a variety of business segment customers at Digital Controls.

Digital Controls Corporation is a local IT services and software company. Digital Controls Technology Services Group provides services to IT in the key areas of security, data storage management, networking, Microsoft infrastructure, and product sourcing. These services are delivered through consulting, professional services, on-site and remote managed services.

Digital Controls Corporation. All Rights Reserved. Published June 2008.