

# The Small Office Solutions Newsletter



Ronald L. Herold, Ph.D.

Local and Wide Area Networks  
e-Commerce and Custom Applications  
e-mail and WEB Presence

3612 Hummer Road, Annandale, VA 22003  
Tel: (703) 573-2222 Fax: (703) 573-2263  
E-mail: ronsolve@rrr.org Web: www.rrr.org

March 3, 2008

## In This Issue

- Overview
- What Content Control Solves
- The Range of Content Control for Web Surfing
- Acceptable Use Policy
- Acceptable Use Policy – Training for Staff
- Implementing Content Control
- Content Control Reporting
- Content Control and Network Load Reduction
- RRR Solutions Content Control Trafficker

## Overview

I don't consider myself an alarmist. I don't have a new whiz bang device or service that I feel some strong need to thrust upon my customers on a regular basis. With this newsletter – I am going to have to ask your indulgence as I do think there are new needs that are not being addressed. I apologize in advance for the length of this newsletter – but I think you will find it very educational and quite necessary in making your Information Technology decisions in the near future.

The operating systems we use – are based upon XP (circa 2002) and Windows Server 2003 (circa 2003). It is now 2008 and unfortunately – Microsoft has not seen fit to 'upgrade' these operating systems to the current date. Yes – Microsoft offers patches for

security purposes to fix the 'holes' in the code that they, themselves, allowed to exist in the earlier releases. However, this effort simply fixes old issues and doesn't really address what has happened in the past 5 years on the Internet.

At a time in the very distant (by computer standards) past – viruses were transmitted via floppies. This is an almost non-existent threat in 2008. After floppies, email became the mode of distribution for viruses. For years email was the major source of viruses. To a larger extent (although not completely addressed), this threat has diminished. So what is the current threat? It's the Internet itself.

Today's threats come in many forms. Purposefully errant web sites are a large source of issues. Protocols like P2P are another form. Search engines like Google (and others) that inadvertently index sites that are dangerous. These malicious sites are offered up as a result of searches. [I should mention that this is, to the best of my knowledge, not intentional. However, it still happens]. Google just removed over 40,000 links from its search results that it discovered went to dangerous sites. Social networking sites and pornographic sites are additional examples of destinations that can be dangerous.

Firewalls are just a first step in protecting your network. We all have a firewall of some sort or another. A firewall keeps the outside world – out. However, it doesn't stop the inside world from surfing, communicating or otherwise

exposing the inside world to the outside. A much more thorough solution is needed in 2008 than wasn't needed in 2003.

In this newsletter – I am going to present in detail some of the threats that need to be addressed and offer a tested solution that RRR Products offers. As an educated consumer – I strongly believe my customers will better accept a solution that addresses a problem they understand. The general term for the issue and solution is “Content Control”

### What Content Control Solves

As the head of a business – one must always evaluate the risks inherent with an action and then take the level of steps necessary to address the issue. So what is the issue that we are addressing when we talk about Content Control?

There are four main problems that content control can help solve:

**Malware infections of your network** – The web has surpassed email as the main vector for desktop and server infection. Google recently scrutinized 4.5 million web pages and found that one in 10 contained malicious code that could infect a user's PC<sup>1</sup>. Many of these pages are related to porn and free offer sites, but can also come through infected web servers and the download of executable files. Content control is one of several layers (e.g. antispyware, anti-virus) that are needed to secure today's small business networks.

1 BBC News, May 11, 2007 - <http://news.bbc.co.uk/2/hi/technology/6645895.stm>

**Misuse of employee time** – excessive time spent on personal web surfing, especially on addictive sites such as MySpace and YouTube, can take a toll on an employee's performance. Salary.com reported in 2006 that the average worker admits to spending nearly an hour a day *outside of lunch and breaks* surfing the internet for personal reasons – a truly astonishing

figure!

**Misuse of company resources** – excessive bandwidth use, and the use of corporate server and workstation space to store large amounts of personal downloads, can be expensive and slow down the entire network, especially for hosted applications. Peer-to-peer software used for gaming and music sharing is notorious for crippling networks because they consume a disproportionate amount of network resources by opening multiple connections.

**Liability** – inappropriate content on the network, especially pornography, can lead to a hostile work environment and ultimately a lawsuit.

These four types of problems incorporate a wide range of cultural, social, legal and commercial concerns. Thus, policing network use is not simply a case of thinking of all the possible forms of abuse that might exist on your network and patching them individually. Rather, it is a case of integrating a clearly defined policy with sound network administration and sensitive management of staff. We need to control the Content of what is transmitted and received from the Internet.

### The Range of Content Control for Web Surfing

Somewhere between Big Brother and a Big Family – is the correct solutions to Content Control for web surfing for your business.

The diagram that follows shows a range from extreme laxity to severity. Its up to you to choose what you feel is reasonable for you organization

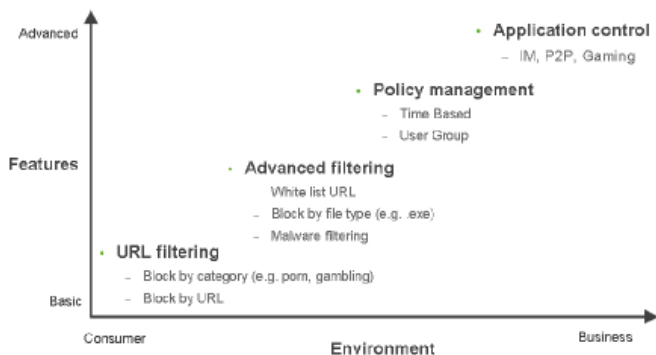


Once you have decided where on the spectrum your business resides – you need to write an Acceptable Use Policy. RRR Solutions can provide a leg up on that effort. We have 'draft' policies that can be customized to your particular office.

There is an entire **Special Feature Section** on Acceptable Use Policy which I have moved to the very end of this newsletter – so as not to interrupt the flow regarding Content Control.

### Implementing Content Control

Okay – this is the slightly technical part of the newsletter – where I talk a little about the different kinds of threats. My purpose is to acquaint my reader with the various kinds of threats by their technical names and descriptions. The chart that follows shows various Content Controlled solutions and where they get implemented.



1. Spam Blocking - Spam Blocking should use an intelligent email filter that identifies Spam—unsolicited bulk email, even when that spam is sent through as an image. Spam Blockers usually take advantage of the public DNS blacklist to block connections from known spammers. Spam Blockers also generate reports of messages that have been held as spam. That way – you can review the reports and later release the message – if desired.

2. Phishing Blocker - A Phishing Blocker inspects an email for phishing content or to identify fraudulent, emails. A phishing email attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

3. Spyware Blocker – A Spyware Blocker examines web requests from your protected network, and does the following:

- Uses virus signatures to detect and identify specific viruses.
- Prevents keyloggers, a computer program that captures and stores the keystrokes of a computer user.
- Provides a URL blacklist to block known spyware websites (for example, www.gator.com).
- Provides a URL blacklist to block websites that require cookies.
- Blocks harmful Active X controls that are known to be spyware applications.
- Examines the IP addresses of websites that users visit, and compares those IP addresses against a list of offending subnets.

4. Web Filtering – is configured to allow blocking (or unblocking) web access by:

- Category – such as Pornography, Gambling, Illegal Drugs, Hate, Social Networking (myspace or youtube for example)
- Specific URLs
- MIME Types
- File Extensions – such as .exe

**In protecting your office in the current environment – web filtering is the most overlooked of the filters.**

5. Virus Blocker – A Virus blocker should scan both Emails and web downloads. Good systems use multiple virus scanners as no single implementation is going to be 100% capable.
6. Intrusion Prevention – Intrusion Prevention is your basic firewall. This prevents attacks from malicious sites to your server using various protocols including http and ftp.
7. Protocol Control – Protocol Control is extremely important today. It allows and disallows various protocols. File and music sharing protocols need to be limited not only because they are sometime used in an illegal fashion – but also because they use tremendous bandwidths and have an extensive impact on your entire network.

While it is not necessary to fully understand each element of Content Control – it is important to understand that connection of your corporate network to the Internet allows many vectors by which an unfortunate incident can occur.

**Content Control Reporting**

If a business is going to actually control the content of what personnel in the office are going to be allowed access to on the Internet, then there are three reporting requirements:

1. Blocked access needs to be obvious. This can best be accomplished within the confines of when the event is occurring – and usually with immediate display in the browser or other access client
2. Quarantined email should be itemized and be available for delivery – just in case desired email is misclassified and is not really supposed to be quarantined. Daily

reporting (or more frequent) is the norm in this area. Reporting on demand generated by the user would also be valuable to the user and a work load savings for the administrator

3. Corporate reporting to the administrator of the network’s behavior and the user’s behavior is also required. Reports showing those users that try to abuse the system as well as the level of filtering of emails and traffic that are being accomplished by the content controller across the entire network are also valuable.

**Content Control and Network Load Reduction**

One of the side benefits of Content Control is to unburden the working servers within your network and the network traffic in general. This results in increased responsiveness from your internal servers. To best accomplish this – a ‘device’ that is separate from your servers should provide the content filtering and interface to the Internet. This unburdens your internal network and servers of this responsibility.

In an implementation that has been under test and use for over 3 months now – the RRR Solutions Content Control Trafficker has typically reduced the number of email connections to the RRR internal SBS by 97.31%.

A breakdown of these emails on a daily basis is show below for February 19, 2008.

Scanned emails (SMTP)	8,861	
Spam connection rejected using DSNBLs	8,106	91.48%
Spam & Quarantined	508	5.73%
Clean & Passed	247	2.79%

Below is a graphical depiction that displays blockage by the hour. The red is the spam detected and the green is the valid email passed.



We can provide additional detailed reports showing the positive effects on our network and how this system will help you, as a business person, provide a more responsive, safer and less threatening Information Technology work environment. We would be pleased to discuss the benefits and specifics of your office.

Not having to process these 8,000 plus connections (and others where web surfing is either dangerous or inappropriate) by RRR's SBS server has reduced the burden on the server and made the entire network more responsive.

### **RRR Solutions Content Control Trafficker**

Providing a solution to content control is complex – especially for the small business environment. Disallowing certain types of traffic enhances the value and responsiveness in the SBS server and limits access from the outside and the inside of the network. Over the past 3 months we have developed and branded a product to address all the issues of internet connectivity from email to spam filtering to web surfing.

We have taken into account the needs of small business and their budgets. A General Motors solution is just not an option. The RRR Solutions Content Control Trafficker (CCT) is affordable and complete. It is minimally invasive making the set up time and cost reasonable. It consists of two parts – one hardware and the other a software subscription to maintain the filtering software and update it with the current list of threats.

Our Context Controller:

1. is a Black box solution – complete, stable and tested
2. is available via lease or purchase.
3. is a total solution that comes with RRR's technical support to set up the CCT and to maintain it.
4. allows RRR Solutions to support your efforts to write an Acceptable Use Policy

# SPECIAL FEATURE SECTION – ACCEPTABLE USE POLICY

## Acceptable Use Policy

Before sitting down to write an Acceptable Use Policy (AUP), you must first decide your goals for implementing web content control. At a minimum, it should be to keep malware and inappropriate content off your network. This generally includes pornographic sites which are both inappropriate and a common source for malware. The argument here is that, if blocked, no reasonable employee is going to raise his hand in a company meeting to ask why he can't access Playboy.com anymore.

On the other extreme of the continuum is what we term "Big Brother." This company blocks all websites except for those work-related sites explicitly approved and added to the pass list.

Once you have decided what is and isn't acceptable use, the creation of a written AUP is rather straightforward. There are, however, a few best practices to keep in mind.

### **1. Use clear and non-technical language.**

This can sometimes be a problem if the members of the team drafting the document are predominantly from a technical background and might have a different perspective on what is obviously network abuse and what is not. Non-technical users are often unaware of how their activities impact bandwidth, how attachments over web mail might bypass corporate virus scanning, and how downloading a free screen saver can infect their computer with malware.

**2. Keep it short.** The shorter the policy, the greater the chance that it will be read, understood, and referred to in the future. The goal is to have a policy that employees find easy to use and understand.

**3. Stress the spirit of the law rather than the letter.** Base your AUP on simple, inviolable principles that can be seen as reasonable by both technical and non-technical staff members. As a minimum, those principles should include the

following:

- Although a certain amount of personal internet use is acceptable, it should be kept to a necessary minimum and not impinge on the user's ability to do his or her job;
- Accessing pornographic, violent, abusive or hate sites is unacceptable;
- Using the network to harass or bully other staff members is unacceptable;
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization is prohibited;
- Sites, defined by the network administrator, deemed to be a security risk or excessively demanding of network bandwidth should be avoided;
- Staff should not expose the company to litigation for copyright infringement, by engaging in activities such as pirating music, videos, or software.

A company-specific policy can be based on this list and adapted as necessary for the circumstances. Keep in mind that the internet is changing rapidly, and it would be tedious to rewrite the policy every time a new technology or phenomenon like MySpace presents itself as a threat. By clearly articulating a small set of guiding principals, you will avoid having to constantly revisit and rewrite the AUP in the future.

RRR Products can help you write an AUP! We have developed a generic AUP that we can help you tailor to your organization

## Acceptable Use Policy – Training for Staff

There is, in short, a need for training. Staff who are aware of the exact nature of the threats that the internet poses – and the issues of security and proper behavior that accompany access to a company network – are more likely to accept and comply with the AUP. Additionally, they will be better equipped to obey the spirit of the policy, make intelligent decisions when surfing the internet, and avoid malware traps.

AUP training should ideally cover five areas:

**(a) External Threats**

If your AUP contains restrictions on employees' online actions in order to protect your network from spyware or virus outbreaks – and it should – you should spend some time explaining what form these threats might take and why specific provisions exist in the AUP to prevent behavior that might leave the network vulnerable.

Unsophisticated users may not understand why it is dangerous to download email attachments from people they don't know or install software from the internet. These users need to be made aware of how their actions, such as downloading a codec to play a free movie, can compromise the network. A brief explanation of the threats presented by malware, phishing sites (i.e. website spoofing) and other traps will make your staff more prudent surfers and less likely to fall into such traps.

**(b) Monitoring**

Staff who are aware that network monitoring is taking place (or even possible) are much more likely to comply with the AUP, including those parts that govern acceptable online behavior. It should be made abundantly clear that everything staff does on the corporate network and every website they visit using company connectivity is visible to the administrator and traceable directly to them. Although it is probably undesirable to overplay the "Big Brother" hand, you will usually find that a simple awareness that their online actions are subject to monitoring will prevent the vast majority of incidents of staff accessing inappropriate material. A good line to take might be something like this: "Yes, we do log network traffic and bandwidth use, and we routinely review those logs to ensure everything is running smoothly. We don't mind if you spend a little time surfing for your own private purposes, as long as it doesn't interfere with your job or otherwise violate the AUP."

**(c) Bandwidth Issues**

Sites like YouTube that offer streaming audio and video may be relatively secure and present a low level of threat in terms of malware, but if many users on a network visit them, the excess bandwidth usage can really slow things down. This problem is becoming more widespread as an increasing number of commercial sites contain streaming video advertisements as well as major

events like the NCAA basketball tournament. An explanation that bandwidth is limited, that a slowdown affects everyone on the network, and that it costs money to add additional DSL or T1 lines should help to underline prohibitions contained in the AUP. It should further be explained that peer-to-peer applications used for music sharing and gaming are notorious for clogging networks because they open multiple connections to grab more bandwidth.

**(d) Issues under civil law**

This topic covers three main areas that can mostly be avoided with good common sense.

First, the viewing and sharing of inappropriate material can create a hostile work environment.

'Inappropriate material' includes all images, cartoons, and messages that are sexually explicit, contain ethnic slurs, or promote racial, religious, or gender stereotypes. Viewing and sharing this material can lead to litigation.

Second, if an employee uses corporate web access to post malicious, defamatory or libelous material on the internet, a court may decide that the company is jointly liable with the poster, on the basis that it provided the means for him or her to carry out the act. Employees should be strongly discouraged from any action, private or business-related, that might invite litigation. On a related topic, it may well be useful to point out that email is a comparatively insecure mode of communication. Private opinions written into an email, even after being deleted, can easily be recovered in a forensic investigation.

Third, employees should never download or install unlicensed software of any kind. Doing so exposes the company to litigation and the network to risk. A recent pirated version of Windows Vista, in addition to being illegal, contained a virus that infected the host computer. Employees should be instructed to avoid downloading pirated and DRM (digitally rights-managed) material on to the corporate network. Media files from services such as Apple's iTunes are generally licensed to the downloader's personal computer, and not to a company network. The presence of DRM material on a multi-user network, even if it is kept secure from most users, will almost certainly be a breach of the vendor's terms and conditions – and, once again, the company may be jointly liable with the

user should the vendor seek redress in the courts.

### **(e) Password Security**

Although not traditionally part of an AUP, an overview of password security is always a useful part of any IT training program, especially if you use any hosted applications, such as [SalesForce.com](https://www.salesforce.com). Employees should be told why it is a bad idea to share passwords or to use easily guessable ones.