WHITE PAPER

WEB CONTENT CONTROL:

FIVE STEPS TO A SUCCESSFUL IMPLEMENTATION

Prepared by: Untangle, Inc.
May 1, 2012

untangle™

TABLE OF CONTENTS

INTRODUCTION

Implementing Web Content Control can seem intimidating. It represents the uneasy marriage of the very different disciplines of network administration and human resource management. With a little forethought, however, it becomes straightforward and very effective. There are two primary elements that need to be considered: a) the business requirements that the content control solution must support, and b) the guiding principals for what is reasonable use of the company's network, which is then captured in an acceptable use policy (AUP) document. Once those are established, the rest of the pieces fall neatly into place.

In this paper, we aim to set out a general structure for implementing web content control and creating an AUP within a business setting. The five-step plan we offer here is geared toward the practical realities facing businesses with limited IT and HR resources. We believe it to be a solid framework that can protect your organization from the major threats presented by users on your network and can be implemented and managed in short order. Before digging into the five-step plan, it is important to understand why so many companies today have chosen to implement content control solutions.

WHY IMPLEMENT 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. The Wall Street Journal recently reported that are approximately 403 million active PC threats. Targeted attacks against organizations with fewer than 2,500 employees are on the rise, accounting for 50% of the total. Nearly 18% target companies with fewer than 250 employees. The overall threat has continued to skyrocket, largely due to the commoditization of malware; last year, attacks increased 81% compared to 2010.[1] Some 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. anti-spyware, anti-virus) that are needed to secure today's small business networks.

Misuse of employee time – Excessive time spent on personal web surfing, especially on addictive sites such as Facebook 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 space to store large amounts of personal downloads, can be expensive and slow down the entire network, especially for hosted applications. Peer-to-peer and "torrent" software used for gaming and music sharing is notorious for crippling networks because it consumes a disproportionate amount of network resources by opening multiple connections, not to mention opening up liability for trafficking content that violates intellectual property laws.

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

[1] Wall Street Journal

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.

The five-step planning structure we present, therefore, is aimed at balancing the needs of network integrity, your organization's need to protect itself legally, and the recognition that the Internet is part of employees' everyday life. It is important to keep in mind that staff may resent an overly restrictive policy. Nevertheless, each company needs to decide for itself where to draw the line between acceptable and unacceptable network use.

Throughout the paper we will be referring to "you" – the writer and implementer of the policy. It is recognized that "you" are not necessarily a single individual; indeed, it is desirable that representative group develop your AUP, including those with responsibility for HR and network management. Regardless of team, a common pitfall to be avoided is for IT to spring the policy on the company and create an uncooperative environment.

STEP 1: WRITE THE POLICY

Before sitting down to write the policy, you must first decide your goals for implementing web content control and an acceptable use policy. 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 measure 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. We term this type of company with minimal restrictions as "Big Family." The philosophy can be summed-up as follows:

We consider our employees to be part of one big family. We trust them to manage their own time and commitments. We provide them a lot of latitude in how they meet their objectives.

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. The philosophy is:

Our employees are being paid to do a job, and we expect them to be productive at work. We do not want to see them staying late because they did not accomplish their tasks during the day, and we definitely do not want to be paying overtime because they were surfing the Internet for personal reasons.

Between Big Family and Big Brother, there is an entire continuum of where companies draw the line between acceptable and unacceptable network use (figure 1.) Further, some companies maintain multiple policies. Two common practices are to provide freer access based on time of day, such as during lunch, or by category of worker. In a law firm, for example, lawyers and research associates often require broader access to the web for research than the administrative staff.

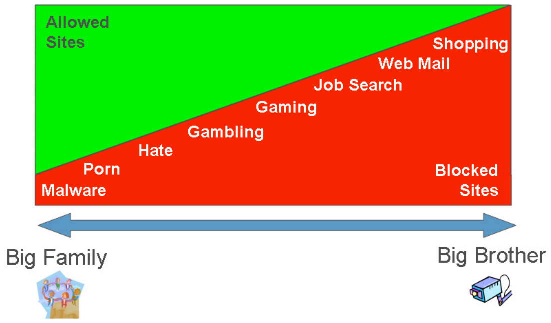

Figure 1: Companies must decide where they fall on the acceptable use continuum.

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 Facebook 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.

Lastly, there is an example AUP for your reference in the appendix of this white paper.

STEP 2: EDUCATE THE TEAM

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 do 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 you job or otherwise violate the AUP.”

It should also be explained that transgressions will be dealt with according to a set disciplinary procedure. We’ll take a more detailed look at such procedures in Step 4, below.

(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 is you use any hosted applications, such as SalesForce.com. Employees should be told why it is a bad idea to share passwords or to use easily guessable ones.

How the training is carried out depends on the nature of your company. However, it is important that technically-oriented trainers do not overestimate the technical sophistication of the staff. It is, therefore, advisable that at least some live training takes place, providing the opportunity for a question-and-answer session with staff. This is likely to be much more effective than simply distributing a booklet or email. However, given that some of the information is relatively complex for IT novices, having an online or printed resource file that everyone can access is also useful.

STEP 3: IMPLEMENT MONITORING AND SITE FILTERING

Once you have decided what is and isn’t acceptable use, you need to identify a technology that will support your AUP and business requirements. For example, will everyone fall under the same policy or do some employees require broader access to the Internet than others? Did you want to adjust the policies based on time of day? Is filtering https traffic, a common web filter workaround, important? In addition to web filtering, do you also want to restrict peer-to-peer applications such as Instant Messenger? Do you want to integrate with Active Directory? And are any of your computers shared by multiple users requiring different policies based on log-in?

Further, Web filtering and the part of the AUP that governs it must take into account the extent to which employees need to use the web for work purposes. Essentially, it’s important to decide whether restrictions should be placed using a system of blacklisting (*i.e.* employees can visit all sites except those specifically banned by name or by predefined category) or whitelisting (*i.e.* all sites are banned, except for a few that are useful for work) as might be the case in a retail or clerical environment.

Figure 2 presents a high-level overview of the differences between basic and more advanced content control solutions.

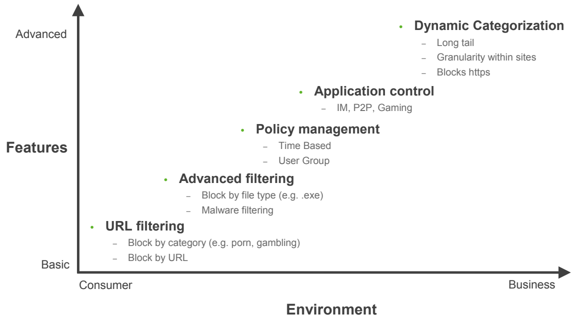

Figure 2: Content control solutions vary by capability and intended use

Filtering works best when combined with network monitoring. A brief but structured examination of usage reports at set points during the working week should be sufficient to identify potential trends and problems as they arise. Beyond being good practice, it lets employees know the policy is being fairly applied.

When it comes to monitoring the web access and behavior of employees, probably the most efficient strategy is to take regular review reports and rotate through each network user’s online activity, working around the entire staff in a random order. Any individuals who give cause for concern can be subject to further monitoring, a warning, or disciplinary action as appropriate, as discussed in the next section.

STEP 4: MANAGE INCIDENTS

Along with a clear AUP, it's important to think through a plan for dealing with incidents and, better yet, to write it down. You should experience fewer problems if everyone is treated consistently and knows exactly where they stand.

We recommend a simple four-stage process to manage most infringements of the policy. The full process is designed for dealing with low-level, persistent offenders. It is anticipated that more serious infringements of the policy would immediately pass to level two, three or – in the case of the most serious abuse – four.

Level one – when a potential problem is noted with a particular employee's Internet use or network behavior, the administrator takes steps to monitor that user's activity more intensively over a set period of, say, two weeks. The employee may not be informed, but it is probably useful to give him or her a short, informal, verbal notification that concerns have been raised and why certain behavior is not acceptable. Whether or not such action is documented at this stage should depend on the nature of the infringement and your policy.

Level two – persistent abuse, or a more significant infringement, should attract a formal, verbal warning from HR. This warning should be documented. Additionally, training and support should be offered to the employee to help him/her avoid future infringement.

Level three – continued persistent abuse or serious infringement should attract a written warning from HR, with full documentation and appropriate retraining.

Level four – habitual abuse and the most serious infringements – accessing serious or illegal pornography, for example – need to be dealt with by HR and higher levels of management. Cases at this level of seriousness can result in litigation should the employee resign or be dismissed. It is therefore vital that every step is documented and a number of different managers are involved in making judgments about the level of the seriousness/threat. If there is any suspicion that a crime has been committed, law enforcement should be notified.

The importance of employee awareness of the exact disciplinary structure, and the necessity of maintaining documentation, cannot be over-stressed. Having clear procedures – especially governing how incidents are reported up the management chain – can also help to avoid problems in the event that a relatively senior individual is engaging in behavior contrary to the AUP.

STEP 5: PERFORM A PERIODIC REVIEW

Finally, it's vital to remember that technology in general and the Internet in particular are evolving rapidly. Given the increasingly social nature of the web, such changes and opportunities are increasingly likely to register with younger team members before they come to the attention of senior management. As such, network managers need to stay on top of trends, monitor network activity, and be prepared to adjust the AUP as necessary when new threats emerge. Many of these trends will first show-up in the reports.

It is recommended that the policy is reviewed at least bi-annually to address emerging challenges. As the policy is updated, changes should be communicated to users.

CONCLUSION

Web filtering has become an essential layer of network security. But unlike other network security solutions such as anti-virus software, content control requires balancing employee needs with that of network security and corporate liability. Filtering is most effective when combined with training, a regular system of usage monitoring, and a clear Acceptable Use Policy. Implementing content control can be straightforward and does not need to take much time. By putting these measures in place, companies greatly decrease the odds of their networks being compromised, reduce their liability, and improve employee productivity.