NEC

NEC AUSTRALIA Pty. Ltd.
A.B.N. 86 001 217 527

Customer Delivery Division

Title
INTERNET CONTENT FILTERING

Document No.:	**DN-BFS-00037**	Issue:	**D**

□ APPROVED DOCUMENT

ISSUE HISTORY

Issue	Date	Description	DCN

Original Author	Origination Date
G. Dodd	
This Issue Prepared By	Date
G. Dodd	19/03/2012

Internet Content Filtering on the BFS Kiosks

TABLE OF CONTENTS

Page

DISCLAIMER

This document is for information only. NEC does not necessarily endorse any suggestions, solutions, or third-party software products that may be mentioned, or linked to, in this document. The listed links are provided as is, with no guarantee of the effectiveness or reliability of the information. NEC does not guarantee that these links will be maintained or functional at any given time. Use the information below at your own discretion.

1. DOCUMENT AIM

This document attempts to provide an introduction to internet content filtering and to provide some references that may assist you in making informed decisions on using filtering and software selection.

2. WHAT ARE INTERNET FILTERS?

Internet filters are software tools that can help monitor web content viewed on a particular computer or network. In the case of family safety settings, Internet filters can also help parents manage who kids can communicate with or how long kids can use the computer.

2.1 How setting Internet filters can help

- Computer Host Administrators, school administrators, parents and guardians can protect users from viewing inappropriate material as well as identify which websites those computer users can visit.
- Administrators, parents and guardians can block sites by content type or only allow access to certain sites.
- You can prevent unwanted, explicit sexual content from appearing in your search results.
- Businesses can block websites or programs that they don't want their employees to use at work.
- Internet filters can warn you about and block you from suspicious websites that might be fraudulent (also known as *phishing filters*).
- Internet filters can keep spam out of your inbox (also known as *spam filters*).

On the Internet, content filtering (also known as *information filtering*) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable. Content filtering is used by corporations as part of their Internet firewall and also by home computer owners; especially by parents to screen the content their children have access to from a computer.

Whether to protect computer users from inappropriate content or keep employees productive, Internet filters can help. As the name suggests, Internet filters restrict unwanted, inappropriate and possibly harmful content.

While they all serve the same basic function, there are different types to choose from, making knowing the differences crucial to forming an informed decision.

Critics of content filtering programs point out that it is not difficult to unintentionally exclude desirable content. The links in Section 4 provide some additional information.

3. TYPES OF FILTER AND POSITION

3.1 Position - Client-Side vs. Server-Side

Client-side filtering is installed directly onto the PC like any other software program. From there, it monitors Internet activity, blocking inappropriate content. Both home users and businesses can use client-side Internet filtering.

Server-side filtering typically resides on the company server, controlling access for all connected computers. BusinessFilters.com warns that server-side filtering isn't very customizable, making a client-side solution more viable. While both may utilize the same blocking or filtering tactics, client-side software typically has more customization, a broader feature set and more frequent updates.

3.2 Web Filter - General

A Web filter is a program that can screen an incoming Web page to determine whether some or all of it should not be displayed to the user. The filter checks the origin or content of a Web page against a set of rules provided by company or person who has installed the Web filter.

A Web filter allows an enterprise or individual user to block out pages from Web sites that are likely to include objectionable advertising, pornographic content, spyware, viruses, and other objectionable content. Vendors of Web filters claim that their products will reduce recreational Internet surfing among employees and secure networks from Web-based threats.

Some Web filter products also provide reporting so that the installer can see what kind of traffic is being filtered and who has requested it. Some products provide soft blocking (in which a warning page is sent to the user instead of the requested page while still allowing access to the page) and an override capability that allows an administrator to unlock a page.

While a Web filter can also screen out a certain amount of malware, security experts advise other forms of protection as well, such as the installation of desktop and network antivirus software. A Web filter is often installed as part of a proxy server and firewall.

3.3 Black & White List Filters

Blacklist filtering, according to www.geeks.com, is one of the more popular methods, because of its ease of use. This type of software requires the internet provider, parent or administrator to manually enter websites deemed inappropriate. After the website is recorded by the software, further access will be denied.

Whitelist filters use the same principle, just in reverse. This much-stricter method requires the internet provider, parent or administrator to specify websites that can be accessed instead of ones that can't. In other words, this method filters out the majority of the Internet, allowing access only to specifically pre-determined websites.

3.4 Keyword and Content Filters

Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out. Content is typically screened for pornographic content and sometimes also for violence- or hate-oriented content

Content filtering and the products that offer this service can usually be divided into Web filtering (the screening of Web sites or pages) and e-mail filtering (the screening of e-mail for spam or other objectionable content).

Keyword and content filtering software takes a similar approach to black and whitelist filters, only filtering out websites with specific words or pre-defined content. For example, a home Internet filter might offer to filter out pornographic content. The software will then try to determine, through the words used on the site and previously set-up database of information, whether a specific site is pornographic.

If so, the user will be denied. According to www.geeks.com, this method is often ineffective, because it tends to block legitimate websites misinterpreted as inappropriate. Conversely, if the keyword or content filter is set too low, it may allow unwanted content through, unable to recognize the site for what it is.

3.5 Email Filtering (for SPAM)

Spam is unsolicited e-mail on the Internet. (E-mail that is wanted is sometimes referred to as *ham*).The term spam is said to derive from a famous Monty Python sketch ("Well, we have Spam, tomato & Spam, egg & Spam, Egg, bacon & Spam...") that was current when spam first began arriving on the Internet. SPAM is a trademarked Hormel meat product that was well-known in the U.S. Armed Forces during World War II.

From the sender's point-of-view, spam is a form of bulk mail, often sent to a list obtained from a spam robot (spambot) or to a list obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail.

Spam is roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message since everyone shares the cost of maintaining the Internet.

Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. It has become a major problem for all Internet users.

3.6 Types vs. Methods

While both client-side and server-side Internet filtering are two different types, within those types there are methods that specify just how the software goes about filtering content.

Understanding the methods, such as blacklisting filters and keyword filters, is important to making an informed decision about what to buy. In other words, knowing whether a filter is client- or server-based isn't enough.

You should also find out the method used and evaluate whether that's the right method for your organization, family or company.

4. LINKS

The following web sites may be of assistance.

Internet Industry Association (IIA)

www.iia.net.au/index.php/initiatives/guide-for-users.html

Australian Communications and Media Authority (ACM)

www.acma.gov.au

Wikipedia (Content Filtering)

http://en.wikipedia.org/wiki/Content_filtering

Wikipedia (Content Control Software)

http://wikipedia.org/wiki/Content-control_software

iiNet (Content Filtering)

www.iinet.net.au/legal/filtering.html

Virgin Mobile (Content Filtering FAQs)

http://virginmobile.custhelp.com/app/answers/detail/a_id/6737/~/content-filtering-faq

Peacefire.org (Content Filtering and Filtering Software)

www.peacefire.org

Electronic Frontiers Australia

www.efa.org.au/about/

5. IS THERE CONTENT FILTERING ON THE KIOSK COMPUTERS?

Depending on the kiosk site (sites using their own broadband or sites using the BFS broadband), content filtering is available in some form, or may be implemented.

5.1 Content Filtering via Internet Explorer (available on all kiosk computers)

The kiosk computers have a rudimentary form of web filtering available via Internet Explorer's ***Parental Controls***.

To set ***Parental Controls***, you must have access to the Site Administrator Password. Note that this password is held by the Kiosk Host Administrator or their delegate and should be protected.

To set up the controls, carry out the following:

- Log on as Site Administrator
- Start Internet Explorer (IE)
- On the IE toolbar:
    - Click on TOOLS, then
    - CONTENT, then
    - Parental Controls
- Choose a User and follow the prompts to set the controls to your requirements.

When setting the web restriction level (i.e. High, Medium or Custom), be aware that not all content within the selected area can automatically be blocked, as objectionable content is subjective. It is also true to say that quite legitimate sites can also be blocked.

5.2 Sites Using the BFS Broadband Service

Sites that are connected to the internet via the BFS broadband service have another layer of protection. The BFS broadband service provider currently uses FortiGuard Web Filtering. The 'filter' has been set in an attempt to provide the safest possible internet access.

Where feasible, the following types of sites are examples of those blocked:

- Hacking
- Racism and hate
- Violence
- Adult materials
- Gambling
- Extremist Groups
- Pornography
- Peer-to-peer File Sharing

If a web site URL is entered and that site is blocked, kiosk users will not be allowed access and will see a message on the screen like: ***"You have tried to access a web page which is in violation of your internet usage policy"***.

If you believe that the site to be visited is a legitimate site and should not be blocked, advise the BFS helpline and it will be investigated.

5.3 Sites Using their Own Broadband

Sites using their own broadband service MAY have content filtering supplied by their provider, or via servers on their own internal network.

If this is not the case, those sites should look at purchasing and installing a product suited to their own needs. The BFS programme does not provide this type of product.

5.4 Supervision

Notwithstanding the above, one of the best forms of 'protection' is for sites to provide supervision and monitoring of kiosk use whenever possible.

Quis custodiet ipsos custodies?

"Who will guard the guards themselves?"

or

"Who watches the watchmen?"

- Juvenal, from his Satires, VI, Lines 347-348