Learn the BEST Way
To Keep Kids Safe Online!

Internet Content Filtering

FOR

Administrators

A Reference for All of Us!

KDI
404 - 17768 65A Avenue
Surrey, BC V3S 5N4
Canada

Call Us Toll Free: 1.800.661.1755

www.netsentron.com

Introduction

This discussion assumes that you are aware of why you would install an Internet content filter in the first place. If you want more information on this topic, get your free copy of the white paper "Five Things You Must Know When Selecting an Internet Content Filter" from www.netsentron.com.

What you may not yet be aware of is that there are options available to you about how to filter websites. Each has varying levels of effectiveness.

How Most Content Filters Work

Most commonly, a content filter product is a passive tool. It works like this:

1. An administrator sees a bad website.
2. The administrator enters the bad website's address (URL) into a list of banned sites.
3. When someone tries to visit that bad site, the content filter recognizes the URL from the list, and blocks them from seeing it.

This is called using a 'Blacklist' to filter out inappropriate websites.

Pros:	*Cons:*
• Easy to set up and run	• Inflexible, only blocks those sites specifically named
• Always blocks those sites on blacklist	• Time-consuming to manage – URLs of bad sites must constantly be updated
	• Expensive to upkeep

The main shortfall of the Blacklist method of Web content filtering is that the filter "only knows what it knows." If a site is inappropriate but its URL is not on the list, the viewer will be able to see it.

The Next Option

Beyond a URL blocker (the "Blacklist" method), the administrator can use a "keyword blocker." This method worked fine in the early days of the Internet, but now it is too powerful and indiscriminate a tool given the considerable range of Web content available. Try to block porn sites using the word "breast", and the filter will also block websites on breast cancer, chicken recipes and athletic sites.

Then a category system was developed. The URLs of inappropriate sites were collected under between 12 and 72 categories, depending on preferences of the filters' developers.

A bad website could be classified under Gambling, Porn, Hate, Online Shopping, Dating, etc. The administrator could choose what categories to block.

Unfortunately, the same Pros and Cons apply as above. A website that is inappropriate but not included on the categorized list will slip through. Even the top Blacklist filter vendors cannot keep up with the thousands of websites constantly appearing and disappearing, no matter what their claims.

A Different Kind of Content Filter

Since a Blacklist is unable to keep pace with every new website that materializes, and keyword blockers are too rough and indiscriminate, a different kind of content filter had to be developed. Instead of being a passive tool, waiting for a banned URL to come up before blocking anything, the new filter had to be active. This content filter had to be intelligent.

A "True" Web Content Filter uses algorithms and weightings with key words and phrases to actively check a website's content *before the viewer can see it*. So if a search is for 'how to swim using the breast stroke', the true content filter will show athletic sites with appropriate content. Sites having 'breast' and 'nude', however, will be blocked. This is a great advancement over the original keyword blocker filters.

While work does need to be done at activation, an advantage over URL blockers is that once it has been set up, the true content filter does not require any maintenance because it intelligently checks each website before showing it to the viewer.

True Content Filter

Pros:	*Cons:*
• Checks content of *every webpage* before delivering to screen • Catches inappropriate content regardless of the source • No need to maintain after setup	• More time to set up at start • May take more computing power, and delay delivering Web content

The Best Way to Filter Internet Content

The tradeoffs of the URL blocker and the True content filter approaches can be both made use of and alleviated by the use of a third approach: the **Combination Filter**.

The combination filter begins with the URL blocker. The webpage address is checked against the Blacklist and possibly against a Whitelist (of allowed sites). If the URL is not on either list, then it is 'Gray' and the true content filter will now be used to determine whether or not the site is safe for viewing.

Combination Filter

Pros:	*Cons:*
• Uses the speed of URL blocker • Uses the logic of the True content filter to cover unclassified sites • Not necessary to constantly update Blacklist—only periodically	• More time-consuming to set up at start than Blacklist alone

The combination filter will quickly block the obviously bad websites, and can block content through search engines, proxy servers, and on pages of social networking or other unlisted sites.

An Example of an Effective Combination Filter

KDI's NetSentron is an example of an effective combination filter that is part of a firewall and network management device. Unlike simpler filters which can easily be evaded, the NetSentron's True Content Filter **QUADRUPLE-FILTERS** website content in order to determine whether it is safe for viewing. Checking for:

1. outright bad websites by their URL
2. file types that are dangerous
3. ICRA rating (the non-profit Family Online Safety Institute's Internet Content Rating Association)
4. content including banned words and phrases and their weightings.

Only if a website has passed these four filtering stages will it be displayed.

Some of the other powerful things the NetSentron can allow you to do include:

- Administrator sets the threshold for phrase and word counts; fully customizable
- Blocks annoying popups and other advertising sites/images through the advertising URL block list
- Can work in a 'whitelist' mode where all sites except those listed are blocked - useful for Kiosks or other public access machines
- Is able to log the user name when using one of the following authentication methods: built in user list, Ident, NT Domain or Active Directory authentication
- Ability to switch off filtering for specified URLs, parts of URLs, Machine IP addresses and user names
- Can block specified machine IPs and user names
- Comes with an easy to read log analyzer allowing you to drill down to find the specific information on users, IP addresses, URLs, allowed and denied sites/files, as well as specific date and time ranges.

For more information on Web Content Filtering, get your copy of *"Five Things You Must Know When Selecting an Internet Content Filter"* at www.netsentron.com.