"AT LAST: How You Can Keep Kids Using the Internet Focused During Class"

Many kids are quite savvy these days about getting around products that filter the Internet for inappropriate content. They can relatively easily evade basic Web content filters by making the computer they're using pretend it's another one somewhere else. And traditional URL blockers, which stop only a list of *known* bad websites from being seen, have zero flexibility when it comes to a site that isn't on the blacklist: they'll allow it.

After that you get category filters. These content filters still use a blacklist, but it's larger and chopped up into categories: social networking, instant messaging, porn, music video, humor and bad taste, just to name a few. This ends up a bit like measuring a cloud with a ruler (how many categories is enough?), but it has the advantage of giving the administrator the ability to turn specific categories on or off.

Why a True Content Filter Is Better Than a URL Blocker

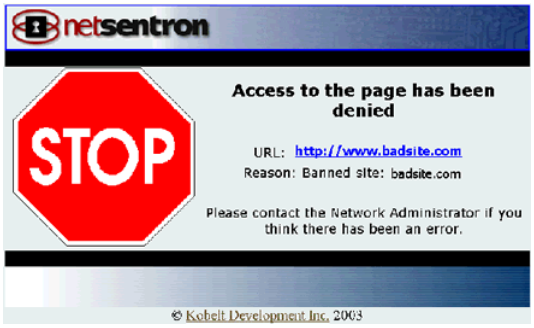
The next generation of content filters is called true or intelligent because those have ways of dealing with sites they don't know about. They're typically built on the foundation of a traditional, categorized blacklist which takes care of the sites that are known to be commonly thought of as inappropriate. After that, though, if somebody wants to see a site that isn't on the list, the newer technology comes into action.

With these intelligent content filters, the administrator has entered certain words and phrases that usually indicate objectionable content. Then weightings have to be applied: we wouldn't want to block out sites on cancer research or chicken recipes or swimming techniques because the word 'breast' was taken as the sole indicator of 'bad content'. The actual content of websites is checked against the words and weightings, and algorithms determine whether the site should be shown or not.

Nowadays, a savvy student can get a computer to pretend it's a different one at another location (called "spoofing" or using a proxy server), or try searches for links to sites through Google, and evade many Web filters like URL blockers that way.

What the NetSentron's Content Filter Does

The NetSentron's content filter is a true content filter. This filter goes beyond the abilities of most other filters: working together with the tools that make up the rest of the NetSentron, providing the network administrator with an inexpensive, comprehensive and effective means to keep students safe on the Internet.



NetSentron's True Content Filter politely but firmly blocks inappropriate websites.

For the traditional blacklist segment, the NetSentron currently has 82 categories that can be selectively

filtered out. Administrators can also customize the filter, entering individual sites they wish to be automatically blocked, or those they want to be always viewed (whitelisted).

When a user wants to see a website, whether going directly to the URL (site name) or doing a Google search, the NetSentron will *quadruple-filter* the Internet:

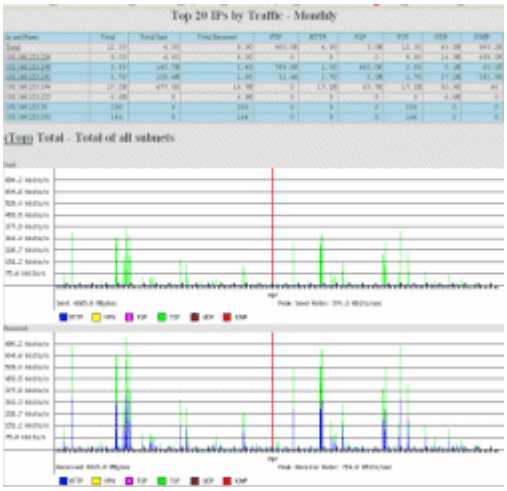
1. The URL is checked against the blacklist for outright bad sites
2. Extension types of files found on the website are inspected to see if they are dangerous
3. The site is checked for a negative ICRA (the non-profit Family Online Safety Institute's Internet Content Rating Association) rating
4. The site's content is checked against the administrator-entered words and phrases, together with weightings.

Only after all of these checks are passed will the site be shown—even results inside a Google or Facebook search (for example).

That takes care of normal searching and entering addresses in the URL bar of the browser. But what about when the student is spoofing—making it appear as if they are using a different computer at another location?

How the NetSentron Stops Students From 'Spoofing Off'

In this case, the NetSentron assists the administrator by doing several things. First, all *outgoing firewall ports*, by which the school's network interfaces with the Internet, can be blocked with the exception of a specific handful. This means data can only be sent out a few ports, and those few not tens of thousands remain to be watched. This will also stop some online gaming as certain games use certain ports. Port as well as individual computer activity can be monitored using the NetSentron's bandwidth monitoring tool. Where a specific student went and when is recorded. If a student is spoofing, the trail remains and the administrator can shut down access to the end site.



NetSentron's Bandwidth Monitoring clearly shows inappropriate activity.

The NetSentron's true content filter includes a category for known proxy sites. Should a student—or anyone—be spoofing and try to attack the school's network, the NetSentron's firewall module will, through stateful packet inspection, stop those attack packets from getting in. Further, NetSentron's Intrusion Detection System can record where and when an attacker is present.

In this manner, using the NetSentron's true content filter in conjunction with the bandwidth monitor, and the NetSentron's firewall, a network administrator can easily and inexpensively monitor and keep safe the school's network and students when they are on the Internet.

Visit *www.netsentron.com*

or call us for free, friendly advice at 1.800.661.1755