Adding White Lists to your Internet Protection Arsenal

Eliminating the use of Anonymous Proxies and other Internet Surfing Threats

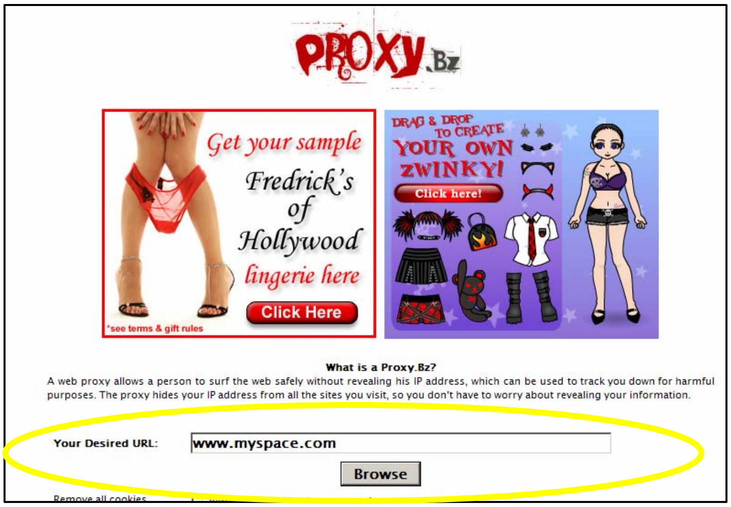
Introduction

Schools today have numerous tools at their disposal to help protect children from the perils of the Internet. Acceptable Use Policies, web filters, URL monitors and even private intranets are all intended to block the bad, while enabling our children to find the best on the web. Nevertheless, as hard as schools try to protect kids, students intentionally, or unintentionally, continue to find inappropriate or time wasting material. To circumvent the protection measures mandated by the government, some students have turned to Anonymous Proxy servers, which allow them to surf any web site without detection. One new weapon in the battle is White Listing, which blocks all web sites except those that teachers want students to access. White Listing is showing success at the classroom level by not only protecting students from inappropriate web use, but it is also increasing available time on task and saving schools valuable bandwidth.

The Challenge

The Children's Internet Protection Act (CIPA) requires schools to install a "technology protection measure" to help shield students from online material that is harmful to minors. According to recent research, nearly all public schools have technologies or procedures in place to control web content on all Internet enabled computers. Despite this, another survey says that 42 percent of students age 10 to 17 had viewed pornography in the past year. While some inappropriate access is due to new sites that web filters have not found, pop ups, file sharing services and social networking sites – another threat is the use of proxy servers.

Anonymous Proxies



What is a Proxy.Bz?

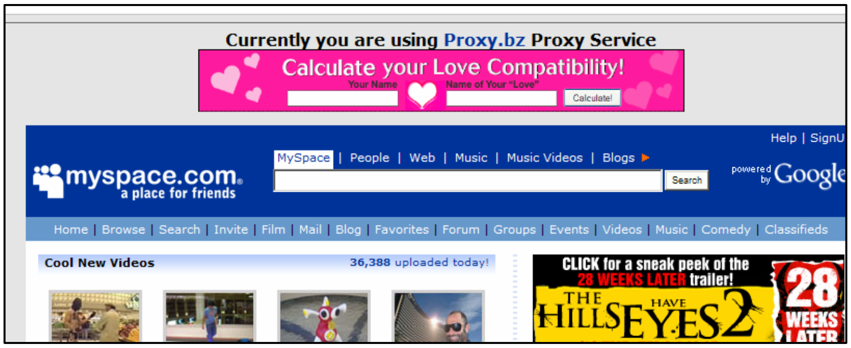
A web proxy allows a person to surf the web safely without revealing his IP address, which can be used to track you down for harmful purposes. The proxy hides your IP address from all the sites you visit, so you don't have to worry about revealing your information.

Your Desired URL: www.myspace.com

The sole purpose of Anonymous Proxies is to mask someone's web surfing activities from Internet filtering devices that are commonly implemented in schools to restrict Internet activity. A proxy server is a computer or an application program that services the requests of its clients by making requests of other servers. A client connects to the proxy server, then requests a file, connection, web page, or other resource available from a different server. An Anonymous Proxy offers an opening through an Internet filter that enables students to surf the web without restriction.

Here is is one example of an anonymous proxy web site called www.proxy.bz :

Assume that your Internet filter does not block www.proxy.bz. If they can get to this site, they can then **anonymously browse to any other website** on the Internet. If the user types in www.myspace.com into the "Your Desired URL:" box they will immediately be redirected to that site.


Currently you are using Proxy.bz Proxy Service
Calculate your Love Compatibility!
Your Name
Name of Your "Love"
Calculate!
Help | SignU
myspace.com
a place for friends
MySpace | People | Web | Music | Music Videos | Blogs
Search
powered by Google
Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds
Cool New Videos
36,388 uploaded today!
CLICK for a sneak peek of the 28 WEEKS LATER trailer!
THE HILLS HAVE EYES 2
28 WEEKS LATER

In this example, My Space opens without triggering any filters even if it is on your administrator's restricted web site list. How can this be? If you notice on the Address Bar of the browser, Internet Explorer has never left www.proxy.bz; it has simply opened www.myspace.com within the browser window itself.

Here are some excerpts from students sharing this information on the web:

Posted: 03-20-2007 07:02 PM Post subject:

1. **Alex** my school blocked not only myspace but proxies as well. how do i bypass this?

2. **me** ok if you want a proxy that works try www.mathcookbook.com …. if not google proxy and u can find them around. They probably won't all be blocked

3. **liam** i got two that may possibly work for you, hope they help https://www.stday.com http://www.ultrareach.net

4. **dan** yep, it worked for me. thanks!

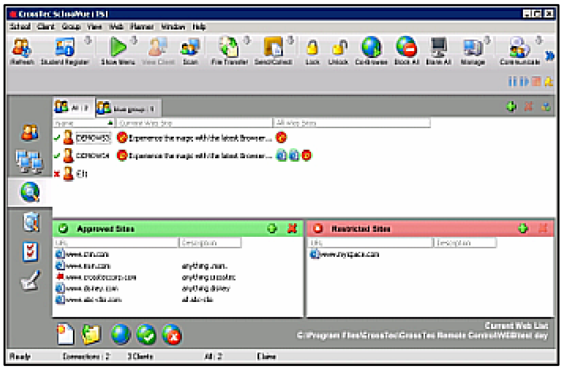
Posted: 03-26-2007 04:47 AM Post subject:

> Well, if you know a bit of php scripting or some java, you can set up a site with an in-browser browser, meaning a php site that loads content inside it. Odds are your filter won't catch this, most don't./ Or you can VNC to an unfiltered computer. My old school filter blocked download.com, lmao. Yet I could easily get porn on it...sad.

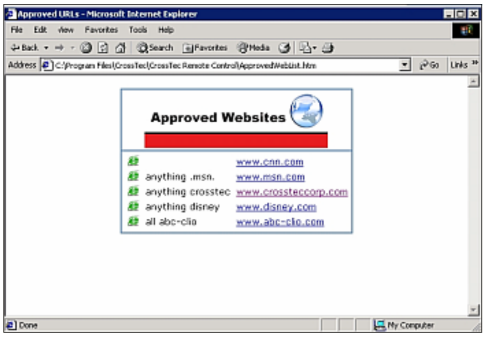
A Google search of "Anonymous Proxies" finds well over a million sites. Of course, web filters can block proxy sites, like any other site, but only once they are found and entered into the blocked database. Unfortunately, more come on-line every day including those that students themselves create. One of the more publicized cases involved a 16-year old in Spokane, Washington who created his own Proxy site based in the Turks and Caicos. He stated the school district's content filter hampered student research. With his Proxy, students could access research sites the filters would block -- but they also could easily visit adult or other inappropriate web sites. By the time the district learned of the Proxy, it had been used over 3,000 times.

What is a school to do?

According to recent research, ninety-six percent of schools use blocking or filtering software; 93 percent say teachers or other staff members monitor student internet access; 83 percent have a written contract that parents must sign; 77 percent record the web sites visited; 76 percent have a contract that students must sign; 45 percent have an honor code; and 39 percent allow access only to their own intranet.



A new, simple, solution to the problem is white listing. White Lists are created at the classroom level and serve as a last, and best, line of defense. Using applications such as CrossTec SchoolVue, a teacher can easily create a list of applications and web sites that they want students to access during a particular class. If a student tries to access any other site, or application, they get an error message. SchoolVue empowers the instructor to limit what a single student, group of students, entire class or classroom can use and not use while the SchoolVue client is running. Teachers can easily add new web sites or applications to the "Approved" list.

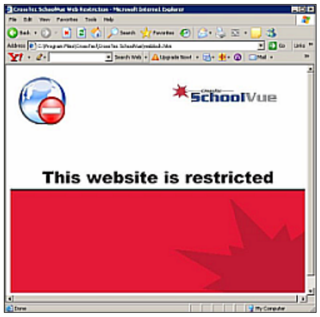


C:\Program Files\CrossTec\CrossTec Remote Control\ApprovedWebList.htm

Approved Websites

	www.cnn.com
anything .msn.	www.msn.com
anything crosstec	www.crossteccorp.com
anything disney	www.disney.com
all abc-clio	www.abc-clio.com

For example in an electronic drafting class, perhaps the teacher wants only to permit AutoCAD and the Internet to run. Now any game or even MS Office application that the student clicks will not run. To restrict Internet use, the teacher might approve just access to the school's web site and maybe Autodesk's site and nasa.gov so they can grab ideas for drawings. If they head for ESPN, IM, web mail or a proxy server – they get a list of approved sites they CAN use. Even domains linked from the allowed site(s) will not work. If a student has a suggestion for a new site, the teacher can easily type in the URL and grant access to it. They don't have to send a message to the tech coordinator and wait for the site to allowed.



This website is restricted

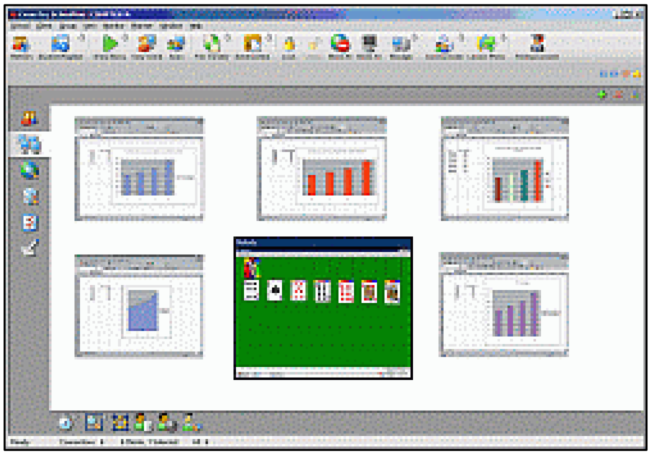
By restricting applications and web sites to only those approved and suggested for class work, teachers have found that students gain substantial time on task and are more focused on the lesson. Another benefit is a decrease in bandwidth usage. If students are not able to download or access media files or spend time surfing, then more bandwidth is left available for more necessary applications and use. The lab will also typically see a reduced incidence of Malware and other technical distractions associated with inappropriate web use.

Multi-Tiered Approach:

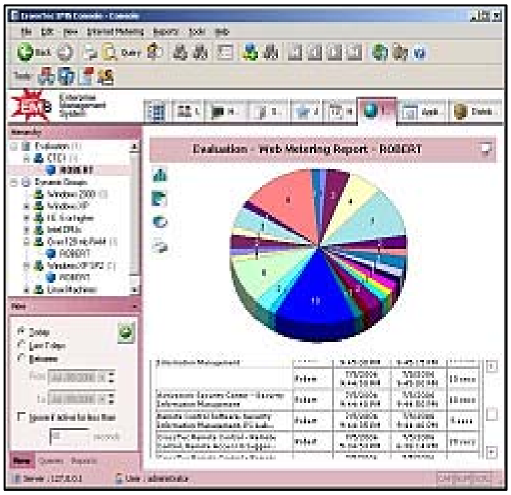
Because of the ever-increasing threats posed by new technology, including new Web 2.0, it is up to schools to mitigate the risks. One of the best approaches in the fight for your students, and not against them, is a multi-tiered attack which should include student education, an acceptable use policy, a tested web filter, monitoring and white listing.

The first step is informing students of the dangers posed by various types of sites and outline tactics to avoid being victimized by online predators. This approach will not only help students become better “Netizines” at school but will provide them with the knowledge to be safer outside of the schools network where most of the other protections may not be available.

Make sure your acceptable-use policies limit computer access to educational purposes only and prohibit access for personal uses. To address social networking policies, you should inform students, and parents, that disciplinary action including prosecution may be taken against them if their off-campus communications causes disruption in school or interferes with another student's rights.



Administrators should not only have a good web filtering system but they should also invest in monitoring technologies intended to show them where students are on the web--and where they're trying to go. While not intended to replace teachers who walk around their classrooms, electronic monitoring enables the instructor to be “everywhere in the room at once.” One monitoring technology lets the teacher see thumbnails of what is on each students’ screen. This feature, which is also contained in CrossTec SchoolVue, provides a single screen containing constantly updating images of student progress. Besides providing a great way to keep students on-task, it also can alert the instructor if someone is having trouble with a given concept or exercise. With SchoolVue teachers can also capture a screen shot of a student’s desktop or an entire screen session of student activity and play it back to administrators or parents.



Another monitoring technology tracks and records every site students visit, including when they logged on and off and how long they were on each site. While SchoolVue contains this ability for a given classroom, other programs such as CrossTec EMS Plus can provide this for an entire district or school. Reports can be generated for specific grades, departments or even individuals. EMS Plus can also create these reports for application use.

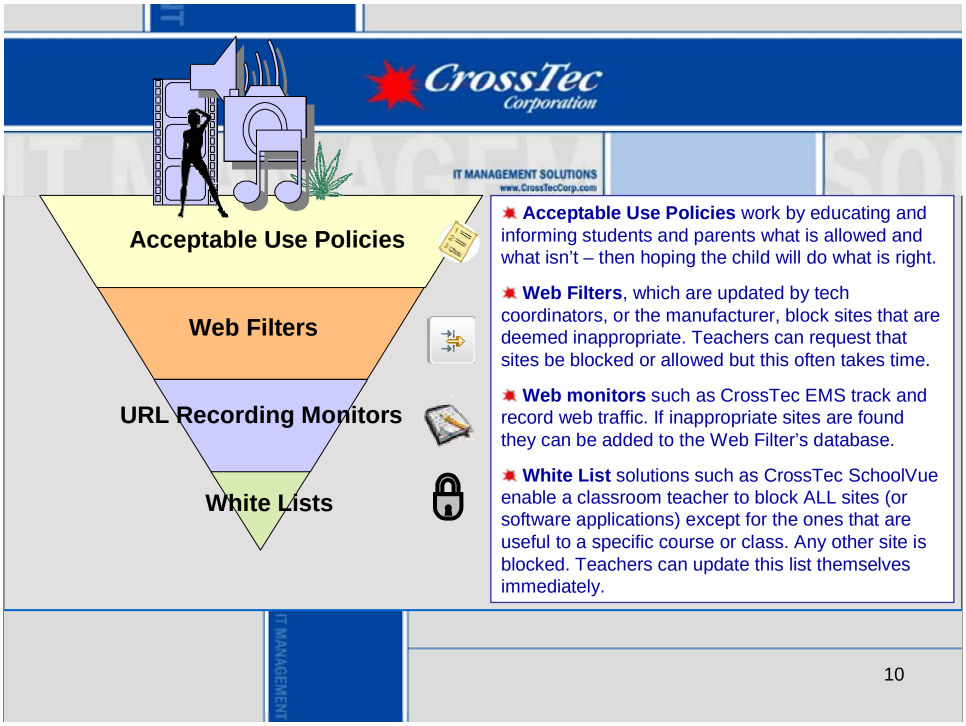
URL and application monitoring is just one feature of EMS Plus. The solution also contains metering so you can restrict use by time, location, grade or group – again reducing threats and bandwidth use. The software also provides software distribution, inventory of hardware and software installed (or missing) on school PCs and powerful cross-platform remote support abilities when paired with its sister product – CrossTec Remote Control.

Once you have established ground rules, set up filters and provided effective monitors, then it is time to protect the individual classroom. The easiest way is to empower the teacher to set policies for each class or even individual students. SchoolVue shows you exactly which active and background URLs are running on Student PCs. The software enables users to drag and drop URLs or applications into "Approved" or "Restricted" lists.

Buttons along the bottom enable the instructor to allow only approved URLs or deny the use of restricted ones or provide open access (which will not override the district web filter). Students will be prevented from visiting prohibited sites.

Conclusion:

Raising student awareness is essential to keeping kids safe online but this is not the only step schools should take. Educators also must practice effective classroom management and oversight, while administrators should explore the use of recording and monitoring technologies intended to determine where students are on the web--and where they are trying to go. To empower the teacher and protect students classroom by classroom – an easy solution is creating specific and individual white lists of only approved web sites (and applications) that students can use. CrossTec SchoolVue enables teachers to create policies that limit sites to the ones that the teacher wants them to visit in order to get the most from a class. SchoolVue also provides a visual way to view all students' desktops from a single screen and provides a list of applications and web sites visited during each class.



- **Acceptable Use Policies** work by educating and informing students and parents what is allowed and what isn't – then hoping the child will do what is right.
- **Web Filters**, which are updated by tech coordinators, or the manufacturer, block sites that are deemed inappropriate. Teachers can request that sites be blocked or allowed but this often takes time.
- **Web monitors** such as CrossTec EMS track and record web traffic. If inappropriate sites are found they can be added to the Web Filter's database.
- **White List** solutions such as CrossTec SchoolVue enable a classroom teacher to block ALL sites (or software applications) except for the ones that are useful to a specific course or class. Any other site is blocked. Teachers can update this list themselves immediately.

10

Stop your students dead in their tracks by helping your administrators enhance their filters and by empowering your teachers with a program that allows them to monitor and block all activity on their student desktops in real-time. Fight back with CrossTec SchoolVue for classrooms and EMS for district or school-wide monitoring. To sign up for a SchoolVue Webinar, Evaluation copy or for other information—please visit: **www.CrossTecCorp.com**