Internet Content Filtering

Better Practices for ISP's

There are many ways that content can be filtered for the user at a home or office. For parents at a home there primary concern may be pornography and chat rooms. For an owner or manager of a company your primary concern would also include time wasting sites like online games, shopping, news, and many more. Companies have a bigger challenge because they may have employees that need different levels of filtering. You may not want to block everyone from online shopping. There is probable someone that needs to do that.

This article will talk about the basics of Internet content filtering. It will also describe a filtering solutions created by PowerNOC that companies and ISP's can use to create a filtering solution that can't be circumvented.

Different Filtering Methods

There are a few different ways that filtering is done.

Keyword Filtering is one of the simplest yet very ineffective ways of filtering. The program doing the filtering scans the URL and page that is being accessed. It looks for common keywords. Sex, breast, female are some examples. This will block a fair amount of the unwanted pages. However, it has many downsides.

Pros – Such filtering programs are very inexpensive and even free.

Cons – Does only a fair job at catching unwanted sites. Blocks too many wanted sites. For example, if you did a search for “breast cancer” the search would be blocked.

Ways Around It – Using foreign words for sex, breast, female, etc. If someone is seeking out pornography they usually don't care about the words or the language on the page.

Solutions – Get a list that includes foreign keywords.

Black Listing is very effective. This method matches the Internet address being accessed against a list of known bad sites. However, the effectiveness depends on the quality of the lists you are using.

Pros – Stops over 90% of the unwanted sites.

Cons - If the list is not kept up-to-date then it becomes less effective.

Ways Around It – Connecting to another computer that is not on the black list and using it's Internet connection to view web sites. Searching for pictures using a common image search engine. Many search engines like images.google.com will store thumbnail copies of images on the Internet. Someone looking for pornography could use a search engine that is not on the black list to find small pictures. If they were to click on the picture to then go to the link they would most likely be blocked.

Solutions – Make sure the black list includes search engines like images.google.com that store thumbnail image previews. Then switch to using a safe search engine like www.family-source.com.

Real-time Content Analysis is usually used with a white and black list. If a web site is not on the white list (Good Sites) or the black list (Bad Sites) then a computer quickly looks at the web site before it lets you look at it. The computer tries to figure out what type of web site it is. If it can figure it out then access will be granted if it's a good site and denied if it is bad.

Pros – Blocks many of the new unseen sites that are added every day.

Cons – It may make a wrong choice as to the content of the web site.

Ways Around It – This method is the hardest one to get around. People will try to use the same tactics that are used in the "Black List" method, but with less success. Also if a bad web site is miss judged by the computer then it will allow the web site.

Solutions – The same type of solutions used in the "Black List" method can be used here. Another solution is to use a filtering system that keeps a history of visited sites. Then browse through this list every week or so to see were people are going. Keep in mind that you don't want to rely on the history that is kept in the web browser. This history can be cleared out or changed.

Different Implementations of Filtering Systems and Programs

Here we will go over the filtering systems. These are the actual programs or computers that do the filtering. The filtering systems will use some or all of the filtering methods shown above.

Client Side Filtering

Client side filtering relies on the computer that the user is using to access the Internet. The user installs a program on their computer. There are many of these types of filtering programs available.

Pros – Can start filtering today. The user does not need to switch Internet providers. User has many options.

Cons – Relies on software and settings installed on the users computer. Can greatly slow users Internet connection. This is because it relies on the power and speed of your computer, so making filtering decisions can take time. May need to be installed on every computer.

Because the filtering happens on the same computer that is used to access the Internet there are ways around this filtering. There are programs that can be installed to bypass the filter. Also, settings can be changed on the computer to bypass the filter.

ISP Proxy Filter

With this system, you sets up a safe gateway to the Internet (a proxy). This proxy will access the Internet and give users only the safe pages. The ISP gives a customer a proxy server address that they put into their web browser settings. When this proxy address is set the user will access the Internet via the safe proxy server. It is also best to install software on the computer that makes it hard to change the browsers proxy settings.

Pros – It is very fast. The ISP's fast servers are doing the filtering. Set up and configuring is simpler to installing the client side filtering programs.

Cons – If the proxy settings are removed from your computer then the filtering is bypassed. Also, a new browser can be installed that will bypass the proxy server.

PowerNOC Solution – ISP Forced Proxy with Firewall

Our system uses a proxy server like the above example but the setting to redirect Internet traffic to the proxy is on the ISP's servers. If filtering is added an account then all Internet traffic is forced to use the proxy.

We are also able to block other types of Internet, like file sharing and chat rooms. This is done using the firewall option in our WISP Billing System. We create a unique firewall for each user. Not only will this block other unwanted Internet services it will also block many computer viruses.

A log of the web sites visited is created. This log is kept on your servers. Users can then review these logs to see what is being accessed.

All of this is done on your servers, this means there are no settings on the users computer that can be changed to get around the Internet filtering.

When you implement PowerNOC's WISP Billing System you are able to secure the Internet in a way that is effective. You can create a filtering system that can not be bypassed.