



Internet Monitoring vs. Filtering and Blocking

This document describes the advantages and disadvantages of monitoring Internet activity and of filtering and blocking Internet access. It explains how WebSpy software can be used as part of an Internet monitoring policy.

About Internet Monitoring

Internet monitoring describes the process used by organizations to assess exactly what Internet resources their members are accessing. This is usually aided by some form of monitoring software that will report on all aspects of Internet browsing such as time spent browsing, size of resources downloaded as well as the content of resources accessed.

Monitoring is often used in conjunction with an Internet Acceptable Usage Policy (IAUP), which, by informing employees about acceptable behavior and monitoring practices, encourages acceptable and responsible Internet usage.

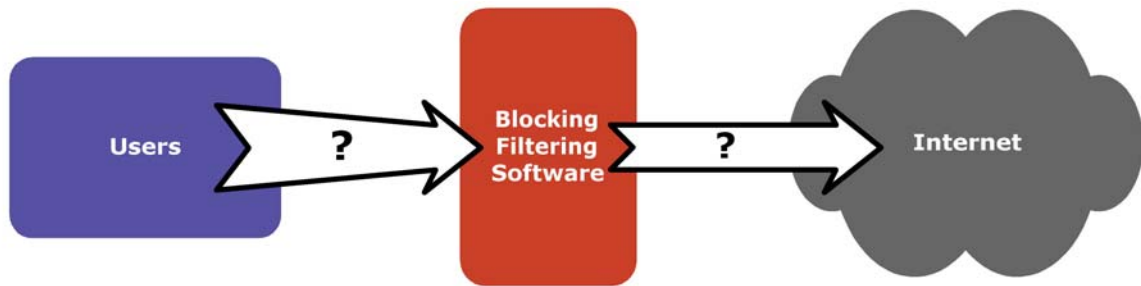
About Filtering and Blocking

Filtering and blocking prevents users from accessing or receiving inappropriate resources. Organizations create a list of inappropriate content using keywords, file types and protocols, and the software restricts access to such material. Alternatively, organizations can subscribe to independently created third party blocking and filtering lists.

Disadvantages of Blocking and Filtering

Filtering and blocking measures implemented in organizations have proven to be unsuccessful for a number of reasons, such as:

- Administrators or managers remain unaware of what sites users are trying to access and as such they are unable to add these sites to their blocking or filtering lists. They have no idea whether the user was able to access the site successfully or not and therefore cannot be proactive towards restricting access again.
- A third-party "Blocked Site List" transfers control of an organization's Internet use to an outside party, with no provision for customizing the list to suit the organization's needs
- Thousands of new web sites are published on the World Wide Web every day, so there is no way that anyone could keep up with these numbers to keep blocking lists comprehensively updated.
- Filtering all inappropriate URL requests is extremely time and resource intensive. It places extra load on your network, increasing the response times for accessing Internet resources.
- There is significant cost and effort involved in keeping third-party blocking lists up to date.



You don't know what's leaving your organization...



And while you know what's **not** coming in, you don't know what *is* ...

Why Monitor?

Misuse of Internet resources costs organizations millions of dollars each year in lost productivity, legal costs, bandwidth and connection fees. The traditional method of reducing this misuse has been to implement blocking and filtering measures as discussed previously.

However, blocking and filtering is no longer a complete solution. The following are some reasons why monitoring has become the preferred approach to encouraging appropriate Internet usage.

- Monitoring is a proactive process that can be used with an open policy for acceptable Internet usage.
- Administrators and managers can see inappropriate browsing as soon as it occurs and act swiftly to identify problem areas or users.
- It is often difficult to determine what to and what not to block. Blocking and filtering lists are very much dependent on what the creator considers inappropriate. In some cases this may lead to the creation of incomprehensive or simply useless blocking or filtering lists.
- Blocking and filtering measures are easily circumvented. Users find ways around these measures by using common practices such as the hiding of URLs through connecting directly to a computer or server name. Monitoring enables you to evaluate the effectiveness of blocking and filtering.
- Most blocking and filtering software only tells you about the unacceptable sites users have been trying to access. You can't tell when they were browsing, how long they spent browsing or how much they downloaded.

- Blocking may prevent users from accessing important, useful resources on the basis of out-of-date blocking lists, or inappropriate keyword lists. This reduces the usefulness of providing Internet access in the first place.

Why WebSpy for Internet Monitoring?

Monitoring is now seen as the preferred method for reducing Internet misuse because it can be used with an IAUP to encourage responsible use of Internet resources by the employees themselves. That is, users will know they are being monitored and as such will adapt their browsing patterns to complement any guidelines or policies outlined in the IAUP.

WebSpy has taken a proactive step towards reducing the costs associated with inappropriate Internet usage with the WebSpy suite of Internet Monitoring software.

Internet monitoring with WebSpy provides the following advantages:

- It provides complete reporting on every site visited by all users, including time spent browsing, size of resources downloaded, any protocols accessed and even content.
- Monitoring highlights current browsing behavior, which leads to proactive enforcement of an IAUP.
- WebSpy provides a keyword and profile system that allows an organization to categorize all sites quickly and effectively. This overcomes problems associated with newly published sites as inappropriate sites can be identified based on the user-defined categories that they fit into.
- All web hits are logged and profiled on complete URL strings to detect and categorize most web sites.
- Live monitoring alerts a network administrator or manager to a user who is browsing inappropriately while the browsing is occurring, enabling more effective management of inappropriate Internet use.
- Free and publicly available keyword and profile updates can be downloaded quickly and easily from the WebSpy website at www.webspy.com.
- All WebSpy products involve a single, inexpensive, up-front fee to cover all Internet monitoring requirements.

WebSpy Monitoring vs. Blocking and Filtering

Monitoring	Blocking/Filtering
Complete reporting on every site visited by each user, including size of resources downloaded, time spent browsing and any protocols accessed.	Administrators or managers are unaware of what sites are being accessed. Therefore access to these sites cannot be restricted.
Organizations can see the browsing habits of their users and have the ability to determine what browsing is and is not appropriate.	Third-party blocked site lists prevent an organization from determining what sites it considers appropriate or inappropriate.

Monitoring software such as *Analyzer* and *Live* gives users the ability to create customized categories to overcome the problem of newly published web sites.

Monitoring highlights current browsing patterns for your organization and leads to proactive enforcement of an appropriate IAUP.

Monitoring allows users access to useful materials, while notifying managers when inappropriate browsing occurs.

Thousands of new web sites are published on a daily basis. Blocking and filtering lists cannot be feasibly updated in a timely or comprehensive manner.

Rather than start with an IAUP, Internet misuse only becomes an issue when problems such as liability, bandwidth, lost profits and profitability occur.

Blocking and filtering is not always accurate, restricting access to useful materials and possibly letting inappropriate materials through - without you knowing.

Further Reading

- For more information about WebSpy Internet usage and monitoring products: <http://www.webspy.com/>
- For more information on Internet Monitoring: <http://www.webspy.com/files/articles/webmonitoring.pdf>
- For more information on various Internet Statistics including Internet misuse: <http://www.internetstats.com/>
- For more information on creating your own policies for limiting risks related to the Internet and e-mail: <http://www.epolicyinstitute.com/>