



astaro
internet security

Network Security Whitepaper

**Content Filtering: Monitoring and
Measuring Web Use Delivers
Productivity Payback**

Version: 1.00
Release date: May 6, 2004
Author: Alan Radding



Content Filtering: Monitoring and Measuring Web Use Delivers Productivity Payback

Astaro www.astaro.com info@astaro.com
3 New England Executive Park, Burlington MA, 01803 USA
Pfinztalstrasse 90, 76227 Karlsruhe, Germany

Table of Contents

You can't manage what you don't measure.....	3
Measure Web Activity Through Content Filtering	3
Content Filtering and Reporting for Effective Management	5
Recommendations.....	7
Selecting content filtering tools	8
Astaro Content Filtering Solution	9
Conclusion.....	10

You can't manage what you don't measure

In the online world, one surprising form of measurement is content filtering. Although most people think of content filtering primarily as a way to block access to proscribed online content, which it does quite effectively, it also helps companies measure and manage for greater worker productivity. This occurs when a content filtering product tracks and reports on the websites visited by employees and the activities they engage in. The biggest payback from content filtering, in fact, may arise from the resulting productivity gains rather than from blocking access to websites.

Content filtering not only controls which individual websites and types of websites employees may visit but gives the manager crucial visibility into what workers do online and how they use their time. It also alerts the manager when workers are doing things that may put the organization at risk or, at the least, violate company rules. In short, content filtering tracks and measures employee activity on the Internet: which sites employees are visiting, what they are doing there, and how much time they spend doing it. With this knowledge the company can effectively manage the time employees spend online for maximum company benefit in addition to simply blocking access to specific websites and categories of websites.

In this paper, we will look at how managers can use content filtering to better manage their workforce. This paper explains what content filtering is, how to select a content filtering product, and how to use that product to improve workforce productivity.

Categories of Online Activity Managers Monitor and Block to Improve Productivity

Pornography
Shopping/Auctions
Criminal activities
Entertainment
Drugs
Leisure activities
Job seeking
Terror/Weapons
Gambling
Hate groups

Measure Web Activity Through Content Filtering

One of the first things they teach in business school is that you can't manage what you can't measure; at least you can't manage it very well. If you don't know specifically where a situation or process or person stands and you can't track things as they change, you are managing blind. Measurement is the way managers make situations and change visible and specific. With measurement, managers can set goals, establish direction, and track progress and change.

People at work spend a lot of time on the Internet. In a published national survey conducted by Nielsen/NetRatings, in Feb. 2004 employees spent on average 78 minutes on the Internet. During the month, on average, they engaged in 66 online sessions and visited 104 websites. Given that these are national averages, it means that some workers spent very little or no time on the Internet while many others spent much more time, hours not minutes surfing the Internet.

Do you know how much time your employees spend surfing the Internet? Do you know how much of that time is spent pursuing non-company business? Such activity ranges from checking stock prices for personal investments to viewing pornography to downloading

music files. Some of this activity only costs you lost productivity. Other activity, such as unauthorized downloads of copyrighted material like music, could leave you facing legal liability issues.

As a manager, you need to know what your employees are doing online if you are to manage productivity and manage risk. Even with written policies governing behavior on the Internet, you still must monitor and measure activity to ensure those policies are being followed.

Content filtering is a security function that controls, monitors, measures, and reports on access to particular websites and types of websites by individuals, based on the individual's specific IP address. Content filtering products typically use a database of URLs, the content of which has already been classified, and white and black lists of acceptable and unacceptable websites and pages to control user access to specific websites.

Specifically, content filtering products perform the following functions:

- Identification—identifies individual users by their IP address and can associate IP addresses with named users through links to LDAP-compliant enterprise directories
- Monitoring—tracks the activities users engage in online, following their visits to websites and individual pages on the website and activities such as downloading files
- Control—restricts access to websites and categories of websites that may not be visited and blocks specified types of activities
- Measurement—logs and stores data on website visits and activities including dates and time spent
- Reporting—generates reports based on information captured in the log

Some content filtering tools also provide export functions that allow managers to export log data to Excel spreadsheets and other tools for further analysis.

Content Filtering and Reporting for Effective Management

Unlike other security functions, which generally aim to protect the organization's systems and data and thwart various types of threats, content filtering primarily serves the purposes of management. The objective is to understand how employees are using the Internet and collect the information necessary to enforce corporate Internet usage policy as well as to block access to problematic websites.

Managers cite a combination of reasons for deploying content filtering:

- Productivity management—ensure workers are spending their time online doing the organization's work, minimize personal Internet activity
- Network performance management—ensure sufficient network resources are available for the organization's business rather than being diverted for personal use
- Legal risk management—identify and eliminate online activities that may open the organization to legal liabilities, such as violating copyrights or compromising the organization by visiting inappropriate sites (pornographic or hate sites)
- Security—prevent the downloading of files and applications that could introduce security risks

The primary means by which managers effectively manage online activity is through content filtering reports and policy. Generally reports address one of two issues, network traffic and online activity.

The network traffic reports typically detail network resource (bandwidth) consumption. These reports detail which groups, departments, or individuals consumed the most network bandwidth in a given period. Using these reports, managers can identify the biggest consumers of network resources. From there, managers can implement policies that reign in those consuming excessive amounts network bandwidth. If need be, managers can use the report as the basis for a chargeback program that holds groups and departments financially responsible for their resource consumption. Faced with having to pay for bandwidth, users will cut back unnecessary usage.

The online activity reports detail what groups and individuals do online. Specifically, these reports identify what websites were visited at what date and time, how long the user spent online and how long he or she visited a particular site, and what data was accessed or downloaded. Using this report, the manager can quickly identify time spent at websites unrelated to the company's business or the employee's job function. Based on the nature of the site visited, the manager can make reasonable assumptions about the activity, whether it is personal business, such as vacation travel or investment planning, or entertainment.



Content Filtering: Monitoring and Measuring Web Use Delivers Productivity Payback

Astaro www.astaro.com info@astaro.com
 3 New England Executive Park, Burlington MA, 01803 USA
 Pfinztalstrasse 90, 76227 Karlsruhe, Germany

User Report									
date/time	ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE	OUT	USED TIME	MILISEC	%TIME
	Period: 2004Apr30-2004Apr30								
	User: 192.168.1.53								
	Sort: BYTES, reverse								
date/time	65.214.53.98:443	96	1.324.028	27.26%	0.00%	100.00%	00:00:15	15.260	8.48%
date/time	65.214.53.101:443	94	1.296.659	26.69%	0.00%	100.00%	00:00:12	12.585	7.00%
date/time	65.214.53.99:443	94	1.296.214	26.69%	0.00%	100.00%	00:00:06	6.177	3.43%
date/time	www.google.com	35	294.578	6.06%	0.00%	100.00%	00:00:31	31.359	17.44%
date/time	news.google.com	30	144.321	2.97%	0.00%	100.00%	00:00:08	8.400	4.67%
date/time	www.adelphiapowerpage.com	28	138.361	2.85%	0.00%	100.00%	00:00:22	22.925	12.75%
date/time	yahoo.knowledgestorm.com	12	124.122	2.56%	0.00%	100.00%	00:00:09	9.780	5.44%
date/time	passthrough.fw-notify.net	194	42.835	0.88%	3.01%	96.99%	00:00:09	9.827	5.46%
date/time	img.mediaplex.com	4	33.814	0.70%	0.00%	100.00%	00:00:02	2.199	1.22%
date/time	www.playboy.com	4	33.736	0.69%	0.00%	100.00%	00:00:00	976	0.54%
date/time	loqin.passport.com:443	2	28.984	0.60%	0.00%	100.00%	00:00:00	79	0.04%
date/time	it	1	15.399	0.32%	0.00%	100.00%	00:00:00	403	0.22%
date/time	pestpatrol.com	1	15.323	0.32%	0.00%	100.00%	00:00:01	1.987	1.10%
date/time	www.google.de	1	15.303	0.32%	0.00%	100.00%	00:00:00	39	0.02%
date/time	notice.knowledgestorm.com	12	14.739	0.30%	0.00%	100.00%	00:00:04	4.674	2.60%
date/time	hp	1	13.817	0.28%	0.00%	100.00%	00:00:00	67	0.04%
date/time	www.teamingup.net	3	3.951	0.08%	0.00%	100.00%	00:00:06	6.082	3.38%
date/time	www.knowledgestorm.com	11	3.848	0.08%	0.00%	100.00%	00:00:02	2.487	1.38%
date/time	toshiba.tzo.com:8080	2	3.162	0.07%	0.00%	100.00%	00:00:00	0	0.00%
date/time	www.adelphiapow1083342396.511	1	3.070	0.06%	0.00%	100.00%	00:00:00	285	0.16%
date/time	adserver.yahoo.com	2	2.525	0.05%	0.00%	100.00%	00:00:01	1.255	0.70%
date/time	statse.webtrendslive.com	4	2.334	0.05%	0.00%	100.00%	00:00:12	12.777	7.10%
date/time	24.48.91.199:443	6	1.770	0.04%	0.00%	100.00%	00:00:15	15.140	8.42%
date/time	localhost:8216	1	1.371	0.03%	100.00%	0.00%	00:00:00	485	0.27% DENIED
date/time	adfarm.mediaplex.com	2	1.339	0.03%	0.00%	100.00%	00:00:01	1.039	0.58%
date/time	www.download.windowsupdate.com	2	942	0.02%	0.00%	100.00%	00:00:12	12.984	7.22%
date/time	66.255.137.99:443	1	885	0.02%	0.00%	100.00%	00:00:00	579	0.32%
TOTAL		644	4.857.430	100.00%	0.05%	99.95%	00:02:59	179.850	100.03%

This report from Astaro Surf Protection clearly shows the activity of an employee who visited some work related websites, but also spent time pursuing personal interests on the Web.

The manager also will see how much actual time is spent on such non-business activities. Most organizations can easily tolerate a little personal surfing as no more damaging than time spent socializing around the water cooler or coffee cart. Where the manager, however, sees excessive amounts of time spent on personal web surfing, he can take appropriate action. This may entail alerting the employee's immediate supervisor or sending a message directly to the employee. In cases where the abuse is extensive or egregious in some way and may require more forceful action, the online activity report will give the manager solid documentation to support his decision.

The following table summarizes the management actions and options available based on content filtering reports.

Report	Finding	Management action
Network traffic	Excessive consumption of bandwidth	Alert user to resource consumption Initiate policies that address acceptable resource usage Implement a chargeback system Plan for resource consumption
Online activity	Excessive time spent on personal online surfing Excessive time spent on entertainment Visiting inappropriate sites	Initiate policies that address acceptable activity Alert supervisors or users to excessive usage Confront, reprimand, dismiss employee for documented egregious violations of policy
Online activity—downloads	Identify unauthorized download activity Identify situations that create potential company liability Identify activity that presents a security risk	Initiate policies that address acceptable activity Document activity that violates acceptable use policy Take appropriate action to correct the situation

Notice that in each instance, management action should be preceded by policies that define acceptable online activity. In fact, the foundation for all effective security is sound policy well communicated.

Recommendations

Content filtering in conjunction with appropriate online usage policies give managers an effective tool for managing employee online productivity. Yet, it is unrealistic to expect 100% online productivity. Widely published studies suggest that 60% of employees use the Internet for personal purposes.

To manage online activity for maximum productivity, try the following:

- Work with HR, legal, and line management to create a consistent set of web usage policies.

- Establish a baseline of current web activity by running the tracking and reporting sections of the content filtering tool
- Analyze the data to identify problem activity and prioritize problems
- Educate users on the web usage policies and the business reasons behind them.
- Use the content filtering tool regularly to track progress.
- Implement content blocking where needed and appropriate.

Studies show that only 30% of companies actually enforce their usage policies. Without the willingness to enforce policies, managing online usage to improve employee productivity, even with the best content filtering tools, will be fruitless.

Even managers who do not intend to enforce online usage policies, however, will find content filtering useful in their efforts to understand employee behavior and forecast resource needs. In addition, content filtering will enable managers to spot potential security and liability problems early. Finally, for organizations that promote core social values content filtering enables managers to reinforce those core values by controlling which sites employees can visit while blocking objectionable sites.

Selecting content filtering tools

The key to selecting the right content filtering tool is the size and currency of the URL database. The Web consists of tens of millions of websites (each identified by a URL), which change frequently. Organizations want to select a tool that contains the largest possible database and which is frequently updated.

This approach to content filtering uses a database of website URLs classified in numerous ways to determine whether or not to block access based on the organization's particular criteria. With database filtering a user request is checked against the database website content category (gambling, hate, pornography, etc.) classification. If accessing that particular category of site is contrary to the organization's acceptable use policy, the request is blocked and the user notified.

The database approach is much more efficient because the actual analysis required to categorize the sites is performed offline. An automated data as opposed to one compiled manually is the most effective off all since its spiders and bots can view far more websites far faster than even large teams of human evaluators.

Another consideration is how the content filtering tool classifies the websites contained in the database. To ensure the highest accuracy with the least false positives (blocking access to acceptable websites) and false negatives (allowing access to unacceptable websites), the tool should use a variety of analytical techniques. The most important techniques include text classification, visual object, recognition, visual porn detection, optical character recognition, and multi-language capability. Information from each analysis step contributes to the final classification. Automated databases typically employ more sophisticated recognition and categorization techniques, resulting in better accuracy and without impacting performance.

Some tools use dynamic filtering rather than database filtering. Dynamic (run-time) filtering assesses the contents of web pages as they are requested to determine if they violate criteria established by the manager. If they violate the criteria, the request is blocked.

The problems with run-time filtering, however, are speed and resource consumption. Accurately analyzing web page content is a very complex process requiring significant CPU power, which slows down the process and saps server processing cycles. Dynamic filters also may have problems distinguishing between acceptable and unacceptable websites. For instance, a dynamic filter may block access to websites dealing with breast cancer mistakenly considering them pornographic sites. Employing more sophisticated analytical techniques would avoid such situations but would require even more processing resources and degrade performance that much more, which would impact employee productivity.

Astaro Content Filtering Solution

Astaro Security Linux includes Astaro Surf Protection, a highly accurate content filtering and reporting tool that uses the most comprehensive URL database available. Surf Protection is simple-to-use but provides powerful monitoring, web categorization and blocking capability.

Surf Protection records all web-related traffic in a log file. Custom reports may be generated from these logs. Reports such as most frequently visited sites, sites visited by employee, or total traffic volume can be displayed. Log data may be exported for further analysis in Excel and other popular tools

The automated URL database used by Surf Protection contains 20 million classified web pages, which are constantly being checked and updated by over 1,000 computers. Using a powerful combination of techniques, including keyword analysis, image recognition, intelligent text classification, and multi-language capability each web URL is assigned to one of the 58 categories. Examples of these categories include shopping, news, religion, pornography and sports.

As the manager, you can decide which categories to block based on your Internet policy. Website classification and blocking combined with white lists (specifically approved sites) and black lists (specifically prohibited sites) provide a proactive means of enforcing policies. If a website from a prohibited category is requested, the request is blocked, the employee is notified that the site is blocked, and the incident is logged for reporting purposes. This approach to web blocking is very fast, accurate, traceable, and easily implemented. As a result, Astaro Surf Protection can help you improve productivity and reduce your legal liability by implementing effective Internet policies.

Astaro Surf Protection is part of Astaro Security Linux, the best-selling open source-based comprehensive network security product, and winner of numerous awards. Now in its fifth release, it is protecting 20,000 networks in more than 60 countries. In addition to its use as a primary security solution, many organizations that have deployed other security tool find it is highly effective and economical to augment their existing security solution with advanced functionality from Astaro, such as URL filtering.



Content Filtering: Monitoring and Measuring Web Use Delivers Productivity Payback

Astaro www.astaro.com info@astaro.com
3 New England Executive Park, Burlington MA, 01803 USA
Pfinztalstrasse 90, 76227 Karlsruhe, Germany

Conclusion

As with any other task, only by measuring online activity can managers effectively manage it. Astaro Surf Protection gives managers a powerful measurement tool that lets them control online activity by employees, boost productivity, and protect the organization from liability and embarrassment. Easy to use, flexible, and comprehensive yet affordable, managers can deploy it quickly and start seeing results right away, usually within 24 hours.