Software For Internet Access Control

We take a look at some of the software packages which control and/or monitor users' Internet access at the office.

By Mike Lewis

Let's face it, we all enjoy those moments when the boss is not around and we can take time out to visit our favourite Web sites - to read up on last night's football, perhaps, or take in the latest Dilbert cartoon. Managers will generally overlook this sort of behaviour, just as they tolerate staff chatting at the water cooler or making occasional personal phone calls. But when non-work related use of the Internet becomes excessive, the boss will rightly want to see it stopped.

No one knows exactly how much time users spend on personal Web surfing at work, but the figures are certainly high. A study by AC Nielsen suggests that Australian employees waste an average of 6.8 hours per week on non-work Internet access - that's nearly 20% of their working time. In the UK the Chartered Institute of Personnel Development estimates that the time wasted costs around £2.5 million per year. In fact, the practice is now so common that a term has been coined for it: cyber slacking.

It is management's job to prevent employees from abusing their Internet access in this way. Managers will lay down sensible guidelines - sometimes called an acceptable use policy (AUP) - specifying how much personal Web surfing will be tolerated and under what circumstances (for advice on drafting an AUP, see *Your Internet Acceptable Use Policy*, PCSA Update 153). Once the guidelines have been agreed, it will fall on the IT department to enforce them.

Fortunately, there are many tools available to help with this. These include monitoring software which can track Internet usage within a workgroup or company, reporting on the sites which users visit and the time they spend doing so. Going further, you can set up sophisticated filtering systems which block access to any sites which are not relevant to the employees' work or, conversely, which deny access to all sites except those specifically allowed by management.

How It Works

Monitoring and blocking tools usually work by categorising Web sites according to their theme and content - entertainment, politics, sport, on-line auctions, adult material, job searches and so forth. The existence of these categories does not itself imply any form of censorship. It is up to the company's management to decide a policy in respect of each category. Thus, the company might decide that access to certain categories should be completely blocked, others should be allowed for limited periods or only at certain times of the day, and others should be freely permitted.

Often different policies will apply to different users. For example, if a manager was worried that staff were wasting company time booking their holidays online, you might be asked to deny access to sites in the travel category or perhaps to allow it during lunch breaks only. But that might not apply to those secretaries whose jobs include booking their bosses' business trips.

How does the filtering software know which category a given site falls into? Some products come with massive databases which purport to list virtually every Web site that the average employee is ever likely to visit. These databases, which are usually updated every day, typically contain many millions of URLs. Filtering tools that rely on this type of database usually work very well, but sooner or later users will discover sites which are not listed - at least, for a while - and which are therefore outside the scope of the filtering policies.

Other products rely on keyword analysis to determine the categories. When a user requests a URL, the software intercepts the page, extracts keywords from its text, and applies an algorithm to decide the category which the site belongs to. The program then enforces whatever policies have been laid down for that category. This has the advantage that every site which a user visits will always be included in the filtering process. It also avoids the effort of regularly downloading updates to the database. However, keyword analysis can never be completely accurate. You have probably heard of filtering products that bar access to perfectly respectable sites, placing, say, a site promoting breast cancer awareness in the "adult content" category. To be fair, this is a weakness of both types of filtering tools, since those that rely on a database also use keyword analysis to categorise pages within the database.

Monitoring vs Blocking

As well as establishing which categories to allow and which to block, management must also decide what action to take when users attempt to surf to restricted sites. One option is simply to monitor the situation at a high level. You might be asked merely to produce periodic reports which summarise the time spent visiting each category - perhaps analysed by department or time of day - but which do not identify individual users. This approach might be appropriate where managers just want to keep an overall eye on staff surfing habits, perhaps to help them decide if they need an acceptable use policy in the first place. It can also help IT staff to determine patterns of Web traffic, which can in turn be useful in planning resources and eliminating bottlenecks.

Going further, you might opt for a system which reports on specific users' violations of the AUP. Most monitoring tools will supply this information in the form of a periodic report. Some products can also send an email to the boss, or pop up an alert on his or her screen, as soon as a violation takes place. Think carefully before implementing that sort of system. The idea of alarm bells ringing every time a user takes a peek at the local cinema guide might not be the best way of promoting good staff relations.

A third option is to deploy a tool which actually blocks access to restricted sites. This is perhaps the fairest system from the user's viewpoint, as it will prevent them from accidentally straying into areas which they should steer clear of. Ideally, the software should display a polite message explaining the situation, perhaps with a link to your AUP document.

You might want to allow the user to override a block if they feel they have a particular reason for doing so - on the understanding that this action will be reported to management. It would be useful if the user could add a note to the report explaining the reasons for their action, but unfortunately none of the leading blocking programs directly supports this.

"As well as establishing which categories to allow and which to block, management must also decide what action to take when users attempt to surf to restricted sites."

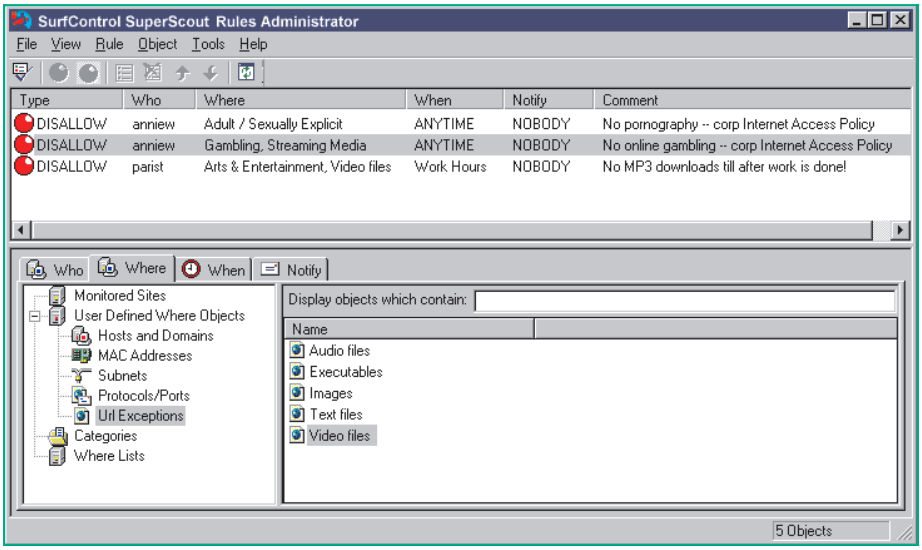

Figure 1 - The Rules Administrator in SuperScout.

What's Available

Let's now take a look at some of the specific monitoring and filtering tools currently available. In general, these products are designed for corporate use and are network-based. They are usually integrated with a firewall or proxy server, or run on a dedicated node on the network. Most of them are software-only, but some come in the form of hardware/software packages. In all cases, the tools are designed to be operated by an administrator whose job is to implement the policies laid down by management.

As well as products intended for corporate use, some filtering tools are available for home users - typically to give parents control over their children's surfing habits. Because these run on stand-alone PCs, they lack the central administration features that corporate users need. However, they cost considerably less than corporate products, and so might appeal to very small companies or user groups.

Superscout Web Filter

This is part of the Surf Control family of filtering and blocking tools, which also includes the popular Cyber Patrol, a product aimed at the home and educational markets. But Web Filter is very much a corporate tool, a fact reflected in its pricing: from US$2,300 for the first 100 users.

Web Filter is based on a database of around 1½ million URLs, or over 690 million distinct Web pages. These are divided into some 40 categories. The database is provided by the vendor and is automatically updated every night. The administrator uses the categories in the database to establish policies for monitoring and filtering (Figure 1). You have a great deal of freedom in how you do this. For example, filtering can be based on site categories, URLs, individual users, user groups, time of day and amount of time spent visiting each page. You can establish filters either positively or negatively - that is, to ban access to categories which are deemed undesirable or, conversely, to allow access only to the categories which management approves of.

In addition, Web Filter lets you regulate high-bandwidth activities such as streaming audio or video, or access to files with certain extensions - to prevent excessive downloading of MP3 files, for example. This can be combined with the category- and time-based filters. Thus you could allow users to view streaming video after

"As well as products intended for corporate use, some filtering tools are available for home users - typically to give parents control over their children's surfing habits."

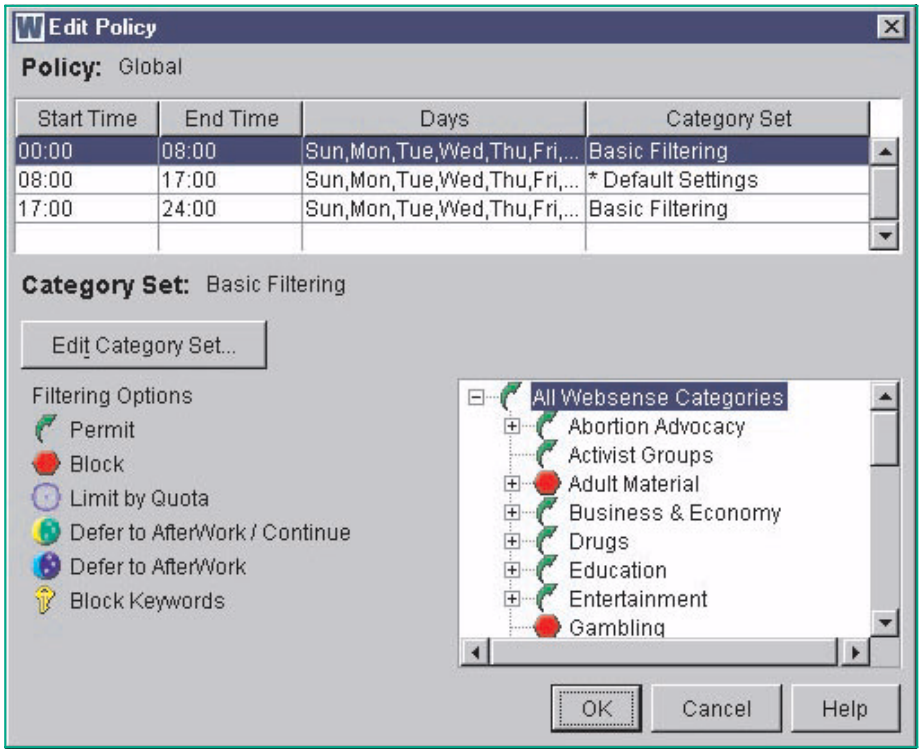

Figure 2 - Websense's Policy Editor.

office hours, or at other times if the feed is coming from, say, sites listed in the training category, but to disallow it in all other cases.

Like most of the products described in this article, Web Filter provides an abundance of reports. Over 60 standard reports are included, and these can be customised in a vast number of ways. They can show individual users' surfing patterns, highlighting people or groups who persistently offend against the AUP, as well as activities or sites which are particularly prone to abuse. You can arrange for reports to be printed on paper, emailed to managers or published on an intranet server. This can be done either on demand or according to a pre-defined schedule.

Surf Control also offers an OEM package, aimed at ISPs and vendors of Internet appliances (Internet-ready PCs, Web TV etc). Vendors can use this to incorporate monitoring and filtering tools into their products or services. It uses the same URL database as Web Filter, and also has a content analysis tool which helps vendors track and categorise the content of Web sites for themselves.

Websense Enterprise

One of the most successful products in its category, Websense claims over 14,000 corporate users, including many international businesses and government departments. It is built around a database of 2.8 million sites, or 500 million pages, in 78 categories. This is updated automatically by overnight downloads. Figure 2 shows the program's policy editing screen.

Given the size of the database, it is likely that Websense will trap just about every page your users will ever visit. However, if the user does discover a site which is not listed, the program will attempt to categorise it on-the-fly by analysing its text. Alternatively, you can arrange for the page in question to be forwarded to an administrator for human review. For an extra cost, you can extend the database to cover so-called premium categories. These can be used to control access to banner ads, instant messaging services, software downloads and pay-to-surf sites, as well as high-bandwidth activities such as streaming audio and video, on-line radio and personal file storage.

An interesting feature of the program is the "continue/defer" setting. If a user attempts to navigate to a blocked page, you can give them the option of going there anyway - on the understanding that this action will be reported to management - or of deferring the access to a permitted time, such as a lunch break. In the latter case, the site will be automatically bookmarked on a free site provided by the vendor. This makes it easy for the user to return at the permitted time. Websense also allows you to give users a daily ration of personal Web access for them to use as they like.

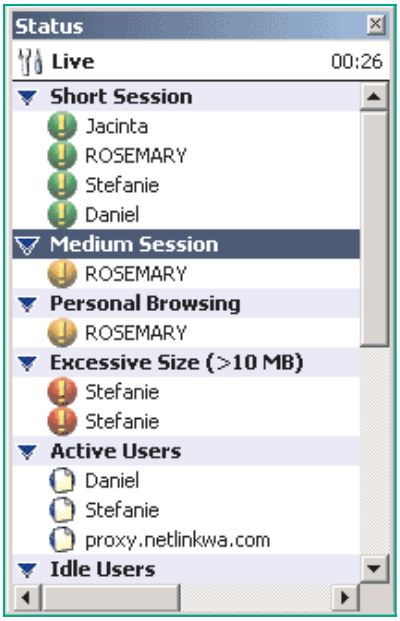

Figure 3 - The Status Window in Web Spy Live.

IM Web Inspector

This product is somewhat smaller than the others described here and consequently easier to administer. With a starting price of US$875 it is also less expensive than most. It only runs under Windows NT or Windows 2000, and relies on the operating system's authentication procedure to identify users. This means that you don't have to worry about setting up separate user accounts or passwords, as is the case with most of the other products described here.

Instead of providing a database of URLs, Web Inspector comes with 11 customisable keyword dictionaries, one for each of its target categories. As the user navigates to a page, the software tests it against the keywords, assigns it to a category, and then applies the appropriate filtering policy. After the page has been categorised, its details are cached to avoid having to analyse it again the next time it is requested. Although this means that you won't have the responsibility of maintaining a large URL database, you might need to put some initial effort into reviewing and customising the keyword lists.

Where particularly close control of Web surfing is required, you can monitor users' activities in real time - peering over their shoulders, as it were, from the comfort of your own workstation. As they navigate to a site, you can see the same content that the user is viewing, and in theory make an instant decision on whether or not to grant access to it. In practice, this is not a particularly efficient way of monitoring Web usage, and you will probably prefer to rely on the program's automatic filtering tools, which work well enough in most cases.

Web Inspector provides over a hundred reports. These categorise users' surfing

habits by site, time of day, time spent at the site, user name, department and overall network utilisation. In addition, the administrator can set up triggers which alert managers of particular policy violations. These alerts can be viewed through the program's administrative interface or emailed to the appropriate people.

St Bernard iPrism

Unlike the products described so far, iPrism uses a combined hardware/software approach. It consists of a dedicated rack-mounted hardware unit (the iPrism "appliance"), plus a Java-based administrative console running on a separate PC. The console software, which is very simple to install and configure, provides a friendly point-and-click interface, making it easy to add users and define policies. According to St Bernard, the entire system can be set up in about half an hour. Prices start at US$3,500 for up to 60 users.

For its filtering, iPrism uses a central database. This consists of "millions of URLs" (the company declines to say exactly how many) in 60 categories, to which administrators can add a further six categories of their own. Pages are initially added to the database by an algorithmic process called iGuard. According to the company, every page is also individually reviewed and categorised by a human reviewer. Updates are posted to the database every day. You can either download these from a secure Web site at a time convenient to yourself or arrange to have the updated data automatically sent to your iPrism appliance overnight.

The product offers some 30 packaged reports and 60 customisable queries. The range of pre-defined reports is smaller than for other filtering products, but they will still provide all the information which the administrator is likely to need. The program also supports a range of alerts and triggers. For example, you could arrange for it to send you an email when attempts are made to access particularly undesirable sites or when total bandwidth usage exceeds a given threshold.

WebFilter

One of the more expensive products in its category (prices start at US$4,000 for up to 250 users), this is another combined hardware/software solution. The hardware is a Linux box which is intended to be attached to a non-switching hub. Some knowledge of command-line Linux is needed to configure this unit but once this has been done, all the administrative tasks can be performed within a Web browser. One snag is that the product identifies users by their IP addresses rather than by a log-in name, and therefore does not cater for roaming users or users who share a PC.

The program is unusual in the way that it categorises sites. Instead of relying on an existing database of URLs, it routes all users' navigation requests to the product's vendor, who then proceeds to categorise the pages in question. This is done partly by applying keyword algorithms and partly by human reviewers. The result is eventually returned to the customer's site, where the URL and category are added to a locally-held database. The cycle takes about three days, during which time access must either be granted or refused on a blanket basis, neither of which is very satisfactory. Customers can choose to share the results of the categorisation process, in which case their databases will grow much faster than would otherwise be the case.

For each category, the administrator can choose to block, permit or monitor any access attempts, but this is done very much on an all-or-nothing basis - you cannot establish different rules for different groups of users. Separate policies can be applied to four fixed time periods per day, but the same periods must be used for everyone. In fact, the program really only supports two types of user: those who are subject to the full weight of the AUP, and those who are completely exempt from it. This is a surprisingly onerous limitation, especially given the high cost of the product.

"Web Spy Live is a real-time monitoring tool that lets you see exactly what your users are doing on the Internet while they are doing it."

Web Spy Live

Web Spy Live is a real-time monitoring tool that lets you see exactly what your users are doing on the Internet while they are doing it. It works through a set of triggers which are defined by the administrator. Using these triggers, you can monitor the size of files users are downloading, the types of files, the overall time spent on a surfing session, and the categories of sites that users are visiting. The program supports 11 customisable site categories; Web sites are assigned to these categories by a keyword analysis process.

The program displays its results in two unobtrusive windows which can be kept open on the administrator's desktop. The status window (Figure 3) shows a summary of the alerts which the triggers have generated, along with a list of all the users who are currently on line. You can drill down into an alert to see more details of the action which caused it. The other window gives you a detailed view of exactly what each of your users is currently getting up to. The program doesn't generate reports, nor can it be used to block access to banned sites, but it does provide a useful real-time monitoring capability. At present, it is only available as an add-on to Web Spy's Analyzer, which is a log-file analysis program. The cost is around US$800 for an unlimited number of users.

SurfinGate

SurfinGate is different from other products described here in that it does not filter by URL or site category. Instead, it targets particular types of downloads. Specifically, it can block the downloading of high-bandwidth files, such as audio and movies, as well as files containing active content - EXEs, ActiveX controls, Java applets and the like. The administrator can decide exactly which types of downloads to ban, and this can be done at user, group or department level. Although there is no central URL database, the product does let you set up a "white list" of permitted sites. So you could, for instance, ban all software downloads except those from companies that you deal with regularly.

You would probably not want to use SurfinGate on its own for general Web monitoring or filtering. The product is best employed as a second line of defence, in conjunction with one of the more general filtering tools, to give you enhanced control over users' surfing and downloading habits. At US$49 per user, SurfinGate is priced with smaller companies in mind.

Conclusions

Once a company has implemented an acceptable use policy for Internet access, it will probably fall on the IT department to police it. As this article has shown, a good choice of tools is available to help with this. These tools can be used to monitor overall Web surfing, to report on specific breaches of the policy, or to block access to sites which are deemed to be undesirable.

However, it is a mistake to think of the filtering or blocking tool as a substitute for creating a sensible AUP in the first place. If the policies are poorly drafted or cause resentment among the staff, the best tool in the world won't make them work. It is also important not to be panicked into creating a policy without careful thought, nor of hastily choosing the software to enforce it. It is true that Internet abuse costs businesses millions of dollars per year in lost productivity. But alcohol abuse costs them at least 10 times as much. So keep the problem in perspective.

PCNA

Products And Vendors

IM Web Inspector
Elron Software
http://www.elronsw.com

St. Bernard iPrism
St. Bernard Software
http://www.stbernard.com

Superscout Web Filter
SurfControl
http://www.surfcontrol.com

SurfinGate
Finjan Software
http://www.finjan.com

WebFilter
NetSpective
http://www.getnetspective.com

Websense Enterprise
Websense
http://www.websense.com

WebSpy Live
WebSpy
http://www.webspy.com

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.