

# Web Access Control

## CONTENTS

### Product (manufacturer)

**N14** E-Safe Gateway 3.0 (Aladdin)

**N14** E-Trust (Computer Associates)

**N14** Internet Manager (Elron)

**N16** Messaging Management System (Tumbleweed)

**N16** Mimesweeper (Baltimore)

**N16** Securi-Q Suite (Group Technologies)

**N18** Super Scout (Surf Control)

**N18** Web Security 2.0 (Symantec)

**N10** Overall ratings

**N10** Recommendation

**N13** Individual rating

**N12** Legal issues

**N19** Lab notes

**N20** Lab results

**N20** Features

## Web Access Control

Any IT manager who doesn't monitor the Internet access of his company is guilty of negligence. *PC Professionell* tested all the Content Security programs available on the market which protect networks against unauthorised access. The tests show that there are significant differences in the use of filtering rules and the analysis of e-mails.

It makes no difference whether hackers gain access to company resources from outside the LAN or whether the source of the risk is the company's own staff: Anyone not taking any measures in a corporate network to prevent any illegal actions may be committing an offence. Take for example the "Golden Jackpot verdict" of the Hamburg Provincial Court of Appeal.

The following content security programs were tested by *PC Professionell*: Aladdin E-Safe-Gateway 3.0, E-Trust from Computer Associates, Baltimore Mimesweeper, Elron Internet Manager, Group Technologies Securi-Q, Symantec Web Secure 2.0, Tumbleweed Messaging Management System. The clear winner of the test is Mimesweeper from Baltimore as it offered the best monitoring and filter functions.

### Content-aware checking of all LAN traffic

Content security is more than just checking network traffic for possible attacks by hackers or checking for viruses. It's more a question of analysing content and checking all network traffic. Generally speaking, a distinction is made between the filtering of Web (http and ftp) contents and mail contents. Program packages such as Mimesweeper from Baltimore or Internet Manager from Elron and Aladdin E-Safe-Gateway 3.0 offer extensive Web and mail

filtering options. The other software products tested only concentrate on certain aspects. Take, for example, Tumbleweed and Group Technologies that focus on mail or Web filtering.

Content Security software works on the basis of rule-based mappings of security guidelines in the network. With the exception of Group Technologies Securi-Q, which only filters mail traffic, all the products are installed in the Internet gateway, i.e. on the central node between the LAN and the Internet.

### **Web filtering and URL blocking**

The simplest way of regulating Internet traffic in a company is to block certain URLs. Apart from the groupware Securi-Q, which is restricted to only mail filtering, all the products offer URL blocking using blacklists. Whitelists can also be defined - this is, however, very time consuming as all the pages allowed by the administrator have to be entered.

## **RECOMMENDATION**

*PC Professionell* Editor's Recommendation

### **Mimesweeper**

Mimesweeper from Baltimore Technologies is the only software program in the *PC Professionell* test to offer convincing content security for both Internet and mail in one package. The suite of different products for mail and Internet monitoring combines flexibility in defining rules with an excellent performance. Baltimore's Mimesweeper therefore receives the "Editor's recommendation".

A blacklist contains Internet addresses to which access is generally denied. Using additional lists drawn up within the company, the administrator can tell, for example, that a particular server is not available. On account of the large number of domains, creating these types of exclusion lists is very time-consuming.

For this reason, all the products offer standard lists, which, like antivirus products, are updated regularly. Elron, Aladdin, Symantec or Baltimore allow you to add different categories of lists to the selection of blocked sites. They also allow you to create your own blacklists.

It therefore makes sense not only to block pornographic, violent and racist pages in the LAN but also to prevent undesired private surfing. This may include, for example, blocking access to shopping portals, travel agents and job pages. However, administrators shouldn't rely solely on the standard blacklists provided. The lists provided by Elron, for example, only refer to American sites and with regard to the domains only cover rudimentary European sites found in the index. Aladdin, on the other hand, works together with Surf Control, the renowned Internet watchdog in the US, which also manages detailed blacklists in Europe.

As well as static URL blocking, dynamic software filter functions (content inspection tools) are of interest. Lists with word indexes can be defined using keywords, whenever one of these words occurs on a Web site, access is blocked. All the products offer pre-defined lists with keywords from a variety of different areas.

### **Dynamic filtering**

Dynamic site filtering involves deciding, from the context of a page or a term, through semantic analysis, whether a site should actually be blocked.

Otherwise, a user who activates the filter for pornographic content may, for example, block access to useful medical content. Although it is possible to define exception rules with all the systems tested, it is very time consuming.

Dynamic filtering works well in Symantec's Tools Web Control and in Websweeper. Aladdin E-Safe is also worthy of praise here. Tumbleweed and Elron, however, which, apart from URL blocking, do not offer Web filtering, both give a poor performance in this case. With these products, the filter engine raises the alarm and blocks access every time an index term is found.

### **Monitoring of e-mails for internal security**

As far as mail security is concerned, comprehensive content-aware filtering is particularly important for two reasons. First, it enables undesired promotional mails and spam to be intercepted at the gateway, thus preventing employee's

mailboxes from filling up with junk. Secondly, it enables internal guidelines regarding the handling of e-mails to be defined via sets of rules.

So the administrator can prevent restricted company information from being divulged to the outside world by e-mail or prevent employees from handling incoming file attachments in a careless manner. Mail security tools such as Tumbleweed, Group Technologies or Mailsweeper perform well in this situation. Securi-Q allows a wide range of possible rule definitions: ranging from the size of mails sent through analysis of content and text to the bit pattern comparison of attachments.

Although Elron's Mail Inspector offers the same functionality, it is by far not as powerful and flexible with regard to defining rules, it is however easy to handle: Symantec, on the other hand, dispenses with mail security entirely and Aladdin restricts itself largely to checking incoming mails and the prevention of spam mail.

### **Reporting as a side effect**

A welcome side effect of mail and Internet filtering is the statistical evaluation of network traffic. In this respect, Elron Internet Manager deserves due recognition. The software program features good statistics functions and a top ten list of the most popular domains or the workstation with the highest surf occurrences in the company. Complex security programs such as Mimesweeper also offer statistics functions, which could, however, be more extensive.

### **Verdict**

The prevention of access to particular Web sites calls for a URL blocker with regularly updated indices. When selecting software, the emphasis should therefore be on extensive filter lists maintained in Germany for URL blocking and the content-aware analysis of pages.

Anyone on the lookout for a program offering Web filtering would find an easy-to-handle solution in Symantec's Web Security.

If comprehensive security guidelines are to be set up for both Internet traffic and mail traffic, then Baltimore Mimesweeper is very good on account of its overall performance in the field of mail and Web filtering.

((Chart))

### **OVERALL RATING CONTENT SECURITY**

<b>Mimesweeper</b>	<b>85</b>
<b>Super Scout</b>	<b>83</b>
<b>Messaging Management System</b>	<b>82</b>
<b>Securi-Q Suite</b>	<b>82</b>
<b>E-Safe Gateway 3.0</b>	<b>80</b>
<b>Web Security 2.0</b>	<b>73</b>
<b>Internet Manager</b>	<b>68</b>
<b>E-Trust Content Inspection</b>	<b>62</b>

## **INDIVIDUAL RATING**

### **PcPro's evaluation criteria**

The content security programs are evaluated on the basis of the four criteria: performance (40%), features (30%), operation (20%) and service (10%).

#### **Performance**

Performance is an important criterion and accounts for 40% of the overall rating. This includes both the benchmark results and the results collected by the *PCPro* lab technicians during the tests. In addition to a good engine which checks Web and mail contents in accordance with the set of rules with as little delay as possible, the rule definitions offered are particularly important. Rules which are as flexible as possible offer advantages as do extensive options which apply when a rule is violated. This applies both to the intentional blocking of sites as well as to the definition of exceptional conditions.

#### **Features**

The highest number of points in the category features which accounts for 30% of the overall rating is given to the programs which offer content security for both mail and the Internet. Good pre-defined sets of rules are also taken into account. Standard templates which automatically block certain content without the administrator having to create black lists or lists of keywords also produce a good result. The regular update of these URL and keyword lists is a must. An integrated virus scan feature and security options which offer protection against attacks by hackers such as Denial of Service or bombing of the mail server offer further advantages.

#### **Operation**

The criterion operation accounts for 20% in the overall rating. The most important points in this case are the design of the graphical interface and interactive behaviour. Programs which support users in creating rules or evaluating logs and statistics can gain extra points here.

#### **Service**

Service accounts for 10% of the overall rating. Important points here are in particular German-speaking support, hotline and product information as well as troubleshooting on the Web pages.

A good printed manual with tips and tricks and important information is a bonus. Training and support in setting up the software are particularly important for complex products.

	<b>OVERALL RATING</b> <b>100%</b>	<b>PERFORMANCE</b> <b>40%</b>	<b>FEATURES</b> <b>30%</b>	<b>OPERATION</b> <b>20%</b>	<b>SERVICE</b> <b>10%</b>
Mimesweeper	1 85	92	95	75	84
Super Scout	2 83	83	86	82	82
Messaging Management System	3 82	90	78	82	88
Securi-Q Suite	4 82	88	76	80	85
E-Safe Gateway 3.0	5 80	83	72	84	80
Web Security 2.0	6 73	72	70	78	82
Internet Manager	7 68	65	65	70	60
E-Trust Content Inspection	8 62	50	60	65	75

-----> better    -----> better    -----> better    -----> better    -----> better

## LEGAL ISSUES

### Monitoring made easy?

**Virus-infected file attachments and malicious code: content monitoring software helps to prevent any damage. However, the use of this software may not violate any legislation in force.**

### Labour-Management Relations Act (BetrVG)

If content security software is used in a company or if there are plans to do so, the staff must be informed. The legislature stipulates, in accordance with the Labour-Management Relations Act, Paragraph 86 BetrVG that the works committee must be informed of any monitoring of e-mail traffic.

This not only applies when e-mails are retrieved or filtered in accordance with particular filtering rules. The fact that a content security monitoring program is potentially able to retrieve e-mails and also check staff surfing behaviour is sufficient.

Whether the e-mails are actually retrieved or not is of no importance.

### Clarification with regard to the use of content security software

There is a simple solution for preventing any dispute and breach of trust between IT managers and staff in the company. An agreement regarding the use of content security management drawn up by the two sides involved inspires trust.

Such an agreement may for example stipulate which protective measures are required, whether only access to particular Web pages is checked or the whether file attachments are filtered. This would provide staff with the opportunity to understand how the software is used.

## **ALADDIN E-Safe Gateway 3.0**

An integrated virus scanner and software-based port and protocol filter make E-Safe Gateway 3.0 a good desktop firewall.

In a corporate network, E-Safe allows the administrator to equip all local PCs with a uniformly configured desktop firewall. This can also be administered remotely. So virus and content inspection can be carried out on computers on the basis of integrated scanners and filters. As an alternative or even additionally, the system administrator can use the product to check all Internet and mail traffic on entry in the company network.

In the test, E-Safe pulls off an excellent performance and good scan rates in virus detection and blocking of malicious code. However, when it comes to content-aware filtering of Web pages and mail traffic, E-Safe cannot keep up with the leaders Baltimore, Tumbleweed and Group Technologies.





The user is able to define his own blacklists or use a large number of lists supplied by Aladdin. They are drawn up in conjunction with Surf Control.

The mail filters are designed for blocking spam mail, spoof mails and relay mails. E-Safe does not provide for content-aware filtering of mail on the basis of keywords or the monitoring of attachments and outgoing mails.

**Verdict:** Gateway's strengths are the desktop firewall functions. Five licences cost DM 3,000.

((Screenshot))

*E-Safe Gateway filters Web traffic reliably and offers simple easy-to-use functions for URL and mail inspection.*

Performance (40%)	
Features (30%)	
Operation (20%)	
Service (10%)	
Overall rating	<b>GOOD</b>

## **COMPUTER ASSOCIATES E-Trust Content Inspection**

The E-Trust family from Computer Associates is a program package for setting up and checking security rules that are in effect within a company network.

The products E-Trust Content Inspection and E-Trust Firewall are used to check Internet access. However, Content Inspection only filters viruses and aggressive code. The package does not offer any URL-based access control using blacklists or whitelists. Content-aware content inspection is not possible with E-Trust.

The software program E-Trust Firewall, which is also installed on the gateway, allows Web access control. This enables the administrator to define detailed rules that allow access to the local network from either an external or internal source.

However, Firewall does not function on a purely protocol basis and does not offer content-aware access control.

Only individual Web pages can be blocked for users or groups or individual ports can be closed, e.g. for Napster and Co. E-Trust Firewall from Computer Associates does not analyse e-mails or Web site contents.

Verdict: E-Trust is the tail-ender, so to speak, in the test environment, the package costs DM 1,570. However, the fact that the program took last place in the test does not indicate the poor quality of the program components, but rather the lack of software tools within the E-Trust Suite. They should enable content-aware checking and control of both incoming and outgoing mail traffic.

((Screenshot))

*The current program status can be checked at any time in the control centre of E-Trust Content Inspection.*

Performance (40%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Features (30%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Operation (20%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Service (10%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Overall rating	<b>SUFFICIENT</b>

## **ELRON Internet Manager**

Elron's Internet Manager product family is a package that not only offers content inspection for Web and mail, but also virus checking and network security functions. Although all programs are only available in English they are easy to understand and simple to use.

The most important components are Web Inspector and Mail Inspector. Both products are simple to use. As opposed to Mimesweeper and Tumbleweed, rule definitions do not have to be carried out first. Comprehensive sets of rules are difficult to set up. The handling and flexibility of the rule engine quickly reaches its limits, the interface becomes difficult to understand.

Mail Inspector works with a similar full-text analysis engine as Web Inspector to enable rule-based filtering for incoming and outgoing mails. Predefined filter lists are also available here. However, the administrator has to manually define the rules for use in a LAN. Anti spamming is already integrated in Mail Inspector. Mail Inspector does not allow virus filtering however. To do this, the administrator has to use the program Virus Protection, which is contained in the software package.

Verdict: Internet Manager is only partially convincing. The cost of 25 user licences for Message Inspector and Web inspector is DM 3,000 and around DM 2,200 respectively.

((Screenshot))

*Web Inspector blocks access to Internet pages using predefined blacklists or specified text phrases.*

Performance (40%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Features (30%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Operation (20%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Service (10%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Overall rating	<b>SATISFACTORY</b>

## **TUMBLEWEED**

### **Messaging Management System**

Tumbleweed specialises in content security for e-mail traffic. Internet access checking is only integrated at a rudimentary level in the Messaging Management system (MMS) via the Web Filter module. In spite of this, Tumbleweed's MMS Mail Inspection is the ultimate on the market.





The options offered by MMS for mail monitoring are almost inexhaustible. Mails can be checked on the basis of keywords and the bit structure can be encoded so that the internal network architecture in subdomains or mail headers cannot be recognised. Rules for handling attachments can also be defined.

Comprehensive statistics functions provide information about mail traffic. Network Associates' engine is integrated as a virus scanner and it ensures constant updated protection against dangerous code and destructive attachments. As an option, Tumbleweed Integrated Messaging Exchange (IME) can also be connected to MMS. IME ensures the secure transfer of mail in the VPN (Virtual Private Network) via automatic encoding.

Verdict: As far as the field of mail inspection is concerned, MMS is one step ahead. The price model is however unusual. The cost of using Tumbleweed's MMS depends on the volume of mail traffic. Based on a minimum number of transactions, prices start at around DM 4,500.

((Screenshot))

*Tumbleweed offers content security via flexible sets of rules which can be quickly defined thanks to good wizards.*

Performance (40%)	
Features (30%)	
Operation (20%)	
Service (10%)	
Overall rating	<b>GOOD</b>

### **PC Professionell Editor's recommendation**

#### **BALTIMORE**

##### **Mimesweeper**

Mimesweeper is a collection of several tools for monitoring mail traffic and Internet access.

After the complicated installation of Mimesweeper on the gateway system, the administrator defines the security guidelines using the Policy Editor. Mail and Internet traffic is monitored and blocked on the basis of these guidelines.

Mimesweeper has an extremely flexible rule language. This allows guidelines for content inspection to be drawn up down to the smallest detail in line with user requirements. So, for example, mails can be blocked on the strength of their size or number of contents. Internet access by users can also be blocked for any period of time, if, for example, users repeatedly access racist pages. The blocking and content inspection technology from Baltimore is excellent. This applies for both static and dynamic blocking.

At a price of DM 2,250 for each module for 25 users, Mimesweeper offers a good price/performance ratio. However, the costs quickly rise as a function of the number of users and on top of this there is an annual charge of DM 450 for regular updates.

Verdict: Overall, the winner of the test, Mimesweeper, offers content-aware content security in conjunction with excellent virus scanning and defence. The integrated statistics and reporting functions are also good.

((Screenshot))

*Mailsweeper from Baltimore monitors incoming and outgoing messages on the gateway. The price/performance ratio is very good.*

Performance (40%)	■ ■ ■ ■ ■
Features (30%)	■ ■ ■ ■ ■
Operation (20%)	■ ■ ■ □ □
Service (10%)	■ ■ ■ ■ □
Overall rating	<b>GOOD</b>

## **GROUP TECHNOLOGIES**

### **Securi-Q Suite**

Securi-Q Suite consists of different modules that extend an Exchange or Lotus mail server to include various security functions. Watchdog, for example, protects the mail server against spoofing, bombing and other attacks by hackers and also checks all mail traffic for contamination by viruses.

Securi-Q-Wall provides content inspection. Using rules, the tool analyses mail traffic and protects against spam mail as well as unpermitted or undesired mail content.

Both the set-up and configuration of the Securi-Q Suite are simple compared with other complex programs such as MMS or Mimesweeper. The Securi-Q tools can be mastered quickly.

Exception handling proved to be excellent, i.e. the system's response on violation of defined rules. Various actions including immediate alerts can be defined via warn levels.

The suite also offers modules such as Trailer, Crypt and Safe. Trailer allows mails to be automatically given headers and footers under the control of rules. Crypt allows encoding and VPN mail tunnelling. Safe allows the audit-proof filing of all mail transactions.

Verdict: Securi-Q can be purchased for DM 5000 and is easy to use. The suite also includes a host of useful add-on tools, for example, for encoding.

((Screenshot))

*A highlight of the Securi-Q Suite is the clearly laid out and meaningful management interfaces.*

Performance (40%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Features (30%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Operation (20%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Service (10%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Overall rating	<b>GOOD</b>

## **SURF CONTROL** **Super Scout**

URL blocking lists are the heart of Super Scout. Various blacklists with indexed Web sites are available in around 40 different categories. Surf Control publishes both blacklists and whitelists.

In addition to the controlled blocking of selected sites, Web filter also allows the general blocking of access to particular sites, ordered by topic.

With Web-Business, Surf Control also offers specific URL filters. They are not only used to block individual topics but are also used to specifically enable access to particular Web sites depending on the line of business of the company in question.

An integrated mail filter which implements rule-based checking of electronic mail monitors e-mail traffic in accordance with a company's internal security guidelines.

Risk filters are a special feature from Surf Control. They automatically filter chain letters, spam mails and other e-mail on the gateway on the basis of predefined lists with keywords. These predefined lists are maintained in an excellent manner and are constantly updated.

Super Scout's strengths include the statistics and reporting functions for Web and e-mail filtering. Current activities and violations of rules can be viewed in real time. The alerting functions are poor, however.

Verdict: 50 user licences for Mail and Web Filter cost around DM 6,900, the price is reasonable.

((Screenshot))

*Super Scout from Surf Control allows flexible design of rules and scheduled access control to the Web.*

Performance (40%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Features (30%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Operation (20%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Service (10%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Overall rating	<b>GOOD</b>

## **SYMANTEC** **Web Security 2.0**

Symantec Web Security 2.0 is a pure content filtering program for http and ftp proxies. The software is available for Windows NT/2000 and Sun Solaris. It is installed on the gateway server.

The filtering functions of Web Security are simple. Access to specific http sites can be controlled on the basis of black or whitelists. Using text analysis on

demand, the administrator blocks individual pages from being retrieved by the user. If forbidden content is accessed, Web Security issues a freely configurable informative message. The administrator is able to look at Web traffic and blocked accesses via a log file and simple statistics and reporting functions. Comprehensive reports can be processed further by exporting them into Excel or Crystal Reports. On the whole, reporting and altering functions are poorly developed.

Symantec gets a bonus point, however, for its well maintained blacklists. Here you can select the set which best meets your personal requirements from various predefined sets. The blacklists can be regularly updated via the Internet.

Web Security is an ideal program if you only a small number of monitoring rules are to be used for Internet traffic. This product does not include any mail filters.

Verdict: 25 licences cost around DM 2,600. Web Secure does not offer content security for mail and offers only a small number of filter rules for the network.

((Screenshot))

*Due to its ease of use and restricted functions Web Secure is suitable for use in small networks.*

Performance (40%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Features (30%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Operation (20%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Service (10%)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Overall rating	<b>SATISFACTORY</b>

## **LAB NOTES**

### **Web control**

Content monitoring is a double-edged sword. On the one hand, a company is obliged to carry out all reasonable measures for preventing unlawful actions such as access to racist or violent content. Yet on the other hand, content inspection can also be used for the illegal monitoring of employees.

((Photo))

PCPro editor Bertold Bräckemeier: "Before using content security programs, think long and hard about which filters you will require".

The laboratory test carried out by *PCProfessionell* shows that comprehensive filter rules and the creation of black and whitelists allow almost every type of monitoring. The programs can be used to retrieve the content of e-mails and evaluate then accordingly.

The administrator can also draw up rules for individual employees which restrict mail traffic. It is also possible to monitor the surfing behaviour of individual employees and regulate it accordingly.

The use of content inspection removes the right to a say in the matter of the work's council in accordance with §86 of the **Labour-Management Relations Act (BetrVG)**. Network administrators should point this out to the head of IT or his superiors. The use of such software should be discussed beforehand with the work's council and requires the agreement of the latter. It does not matter whether the content security programs are actually used for monitoring employees or not.

## **CONTENT SECURITY SOFTWARE**

**In PC Professionell's test laboratory the content watchdogs have to prove what they can do. Only Mimesweeper and Elron's Internet Manager manage comprehensive filtering.**

In the test, the differences proved to be in the filter functions: Tumbleweed only implements rudimentary Web filtering, Group Technologies Securi-Q came off badly for lack of Internet filtering functionality. Symantec Web Security offers little checking of a company's internal mail traffic and also Aladdin's E-Safe does not escape unscathed here. Only Mimesweeper and Elron Internet Manager offer extensive functions for both mail and Web filtering. Baltimore Mimesweeper is on step ahead in this area. This is due to the comprehensive rule mechanisms.

### **Laboratory test with hacker sites and mail tests**

All the programs have to pass the same test in the laboratory. First, the software is installed on a Windows-2000 PC which works as a gateway. An exception to this is Securi-Q, which only runs on an Exchange 2000 server.

After set-up, using predefined sets of rules, access to 25 Internet sites/pages from different areas are tested and the blocking qualities of all the products are examined. The test involved a mixture of different sites with racist or pornographic content. Mimesweeper's blocking performance was exemplary.

The technicians also determine how long access via the gateway to a self-created Web site with comprehensive content is delayed by content inspection. In this case, the gateway dials into its own Web server via ISDN to avoid any inaccuracies in measurement due to an Internet connection. Internet access is therefore simulated in the laboratory.

### **Correct handling of 30 suspect mails**

Mail inspection is checked with the help of thirty suspect mails. Half of the mails are sent to from the local network to recipients outside the network. The other half of the mails are either spoof mails or spam mails or mails with pornographic content. Features of interest here are static blocking, the prevention of particular file attachments and

dynamic content inspection. Tumbleweed offers excellent and very comprehensive mail monitoring functions. The *PC Professionell* laboratory technicians create appropriate rules in all programs offering mail filtering.

These rules are used to block mails with particular content. Confidential information undergoes rigorous checking on the basis of a company's own keywords. Group Technologies and Tumbleweed were the frontrunners in this category.

### Download performance

	Position	
E-Safe Gateway 3.0	3	215
E-Trust Content Inspection	7	260
Internet Manager	8	280
Messaging Management System	2	210
Mimesweeper	4	240
Securi-Q Suite	1	200
Super Scout	6	250
Web Security 2.0	5	245

In seconds -----> worse

### Blocked sites

	Position	
E-Safe Gateway 3.0	2	23
E-Trust Content Inspection	7	10
Internet Manager	5	16
Messaging Management System	1	24
Mimesweeper	5	12
Securi-Q Suite	8 <sup>1</sup>	
Super Scout	4	19
Web Security 2.0	3	22

<sup>1</sup> No rating possible (max. 25 sites possible) -----> better

## Blocked mails

	<u>Position</u>	
<b>E-Safe Gateway</b>	<b>6</b>	<b>13</b>
<b>E-Trust Content Inspection</b>	<b>8</b>	<b><sup>1</sup></b>
<b>Internet Manager</b>	<b>5</b>	<b>22</b>
<b>Messaging Management System</b>	<b>3</b>	<b>26</b>
<b>Mimesweeper</b>	<b>1</b>	<b>29</b>
<b>Securi-Q Suite</b>	<b>2</b>	<b>28</b>
<b>Super Scout</b>	<b>3</b>	<b>26</b>
<b>Web Security 2.0</b>	<b>8</b>	<b><sup>1</sup></b>

<sup>1</sup> No rating possible (maximum 30 pages possible) -----> better