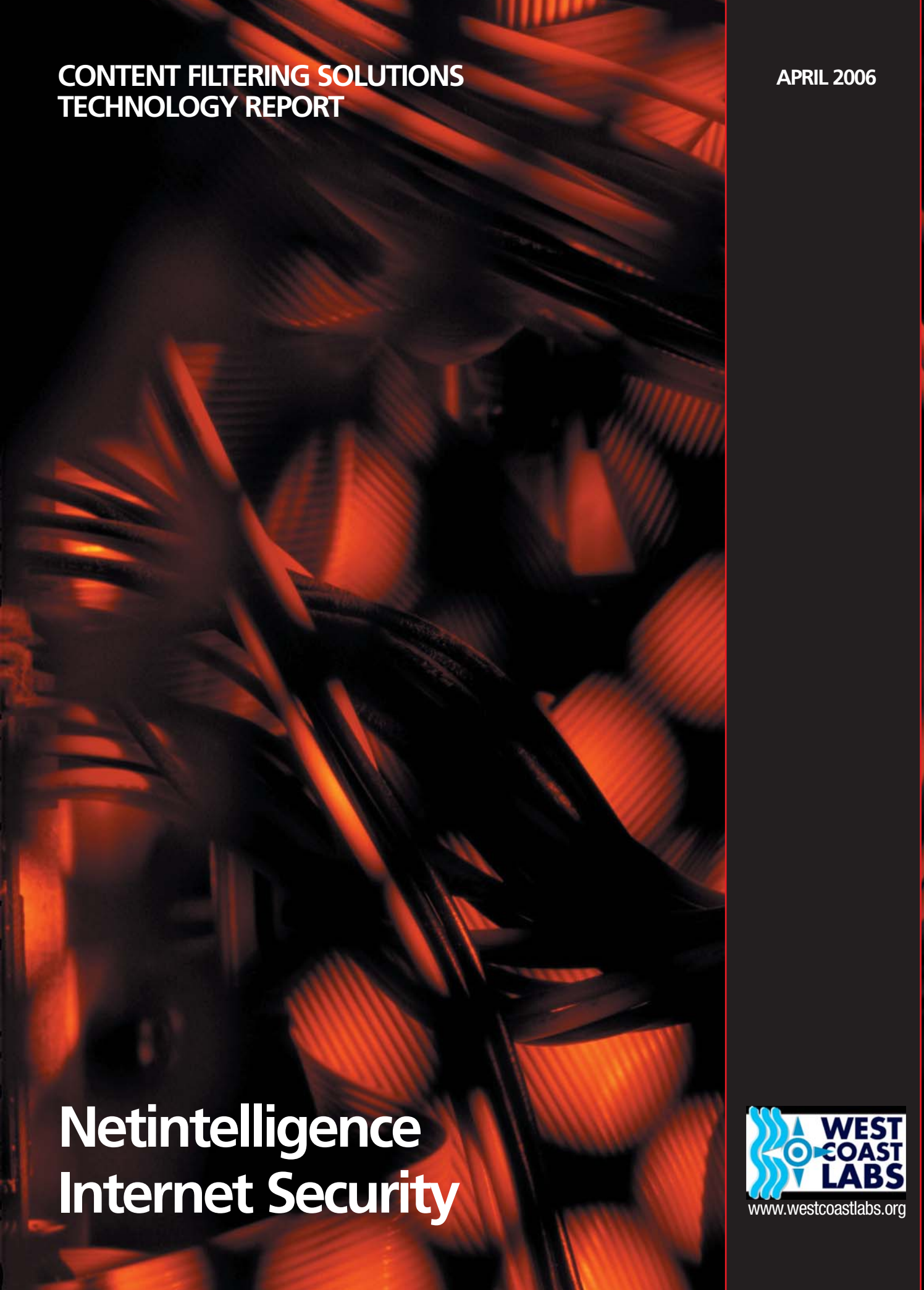
CONTENT FILTERING SOLUTIONS TECHNOLOGY REPORT

APRIL 2006



Netintelligence Internet Security

WEST COAST LABS

www.westcoastlabs.org

Contents

Netintelligence Internet Security

Netintelligence
PROTECTS

West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

Content filtering – the stakes are high!

When companies provide staff with personal computers they know they are equipping them with a tool that can be used for both good and ill. Most acknowledge that the office PC will be used for the occasional personal email, and possibly some online shopping or holiday-booking during lunchtimes.

But there are limits, and the PC, a tool that is meant to deliver efficiency, can rapidly turn into a device for whiling away office hours in games, chatting to friends and relatives, and sometimes more sinister activities, such as accessing pornographic websites. Numerous surveys have confirmed this to be the case. For instance an online poll of 10,000 American office workers last July, revealed that they spent more than two hours a day surfing the web for non-business related information, or sending personal emails.

That is why companies should always write acceptable usage policies for staff, outlining exactly what will - and will not - be tolerated. Unfortunately, even the best policies are rarely read in any great detail, and can often end up at the bottom of a desk drawer. Regular security awareness training can help, but the stakes are high. Apart from the obvious loss of efficiency if staff spend their time on games and private emails, there are greater dangers still.

If staff use the corporate network to send offensive or libellous messages by email, or download illegal images or pirated music, then the company may become legally liable for allowing the offences to take place. Companies must therefore ensure policies are followed to the letter, and while training and trust are key elements to making it happen, the policy needs some technology to back it up.

Content filtering systems are designed for this purpose, to translate the policy into action and to report back quickly on any breaches.

Content filtering – the stakes are high!

In this Technology Report West Coast Labs has tested the effectiveness of leading content filtering systems under strictly controlled laboratory conditions to ensure fairness. The tests were based on how well the products would perform in enforcing a hypothetical, but typical, Acceptable Usage Policy for email and the internet - devised by the West Coast team. The Draft Acceptable Usage Policy can be found in Appendix 2.

The policy lays out general principles both for email usage and for internet access. Like most policies, it allows a certain amount of personal use for staff, but impresses on them that this should be 'reasonable', and that if they have any doubts, to check with their manager. It also states explicity that all traffic can be monitored and recorded, thereby reminding users that nothing they do on the company network is private.

It also spells out actions that are forbidden. These include sending offensive messages, breaching copyright by downloading pirated material, or generally clogging up the network with trivial traffic. In other words, it is a typical acceptable usage policy that tries to explain why the rules are in place, where the boundaries lie, and the penalties for crossing them.

A good content filtering system should be expected to block any attempt to access websites outside the terms of the policy, and stop users from sending illicit emails. It should also log any attempts to breach the policy. At the same time, it should not get in the way of day-to-day business. A system that starts blocking legitimate emails and stopping users from using the internet for their work is worse than no system at all.

Test objective and scenario

The aim of this Technology Report is to evaluate participating solutions in the field of Content Filtering. Participation in this report is open to solutions that offer content filtering of email and/or web traffic.

The report examines the functionality and performance of participating solutions, which are aimed at the SME environments.

The objective is, thru a real-world test environment, to provide an independent validation of content filtering effectiveness with particular reference to:

- A detailed view of the features, functionality and performance of the solutions.
- The extent to which the security policy is enforced.
- The completeness and accuracy of the logs produced.

On completion of the Testing and based on the product performance, appropriate Checkmark Certifications will be awarded based on achieving the following performance criteria.

Certification – Checkmark

Upon successful completion of the testing, participating solutions will be accredited to Checkmark Certifications for either Email or Web Filtering subject to achieving the following performance:-

Email Filtering PREMIUM

Checkmark PREMIUM Certification for Email Filtering
100% of attempts to send emails in contravention of the security policy will fail and that such attempts will be logged.

Email Filtering

Checkmark STANDARD Certification for Email Filtering
Over 95% of attempts to send emails in contravention of the security policy will fail and that such attempts will be logged.

Web Filtering PREMIUM

Checkmark PREMIUM Certification for Web Filtering
100% of all attempts to access web sites outside the terms of the security policy should be blocked and that such attempts will be logged.

Web Filtering

Checkmark STANDARD Certification for Web or Email Filtering
Over 95% of all attempts to access web sites outside the terms of the security policy should be blocked and that such attempts will be logged.

www.check-mark.com

Test Methodology

The Web Filtering and Email Filtering test methodologies have been developed to replicate in a short space of time a number of hits on sites or emails received that fall outside of the prescribed Acceptable Usage Policy, along with providing genuine sites or emails as a control group.

Web Filtering

- **TEST I** - A proprietary piece of software has been developed to load in a list of specially researched URLs from a file. This switches through the list changing web page every 6 (six) seconds until it either runs out of URLs or receives an END command. The HTML code from each web page is appended to a log. The appropriate engineer then analyses the logs to ascertain if any pages have been passed through the solution.

- **TEST II** - The list from TEST I is re-run through the software. This is accompanied by two human operators manually following a pre-specified and specifically researched list of URLs in a pre-specified order and also by a background load provided by specialist hardware. The logs are then appended again to a log file and checked further.

Email Filtering

Before commencing this test, the solution is configured so that offensive email is NOT bounced back to the original sender. An inbox for each sub-domain is configured to accept mail to all users and redirect them into one inbox.

- **TEST I** - Two scripts have been created to simulate internal and external users. The external email addresses are taken from the West Coast Labs' spam feed, the internal addresses can be created as random names. Each script is accompanied by a number of email bodies as text files which are to be attached.

Test Methodology

These are run over two separate networks, with the internal script being run on the internal network and the external script being run completely separately. Each script has a number of emails containing offensive language included. At the end of the running script, the inbox is checked and the functionality of the filtering confirmed.

- **TEST II** - The scripts from TEST I are re-run. The specialist hardware is configured to provide a background load of email traffic. At the end of the script, the inbox is checked and the functionality of the filtering confirmed once more.

The product

Netintelligence says… about the product Netintelligence Internet Security

Netintelligence Internet Security is a web based security service that protects the mobile workforce, by securing the end point the moment it connects to the web - regardless of location, time or connection type

Netintelligence says… about the Netintelligence Internet Security Business Benefits

A comprehensive Internet security service which is activated the moment an Internet connection is detected.
Netintelligence offers the next generation of internet security product - the 'Online' security service. A comprehensive internet security service which is activated the moment an Internet connection is detected, protecting laptops/desktops and enforcing policies in real time, regardless of whenever or wherever they connect to the web.
Combining core functionality of Anti Virus, Anti Spyware, Web Blocking, Instant Messenger & P2P control, Firewall, Asset and Usage Management with comprehensive reporting - Netintelligence Internet Security enables the central application and enforcement of policies across physical, geographical boundaries & time zones.

www.netintelligence.com

The product (continued)

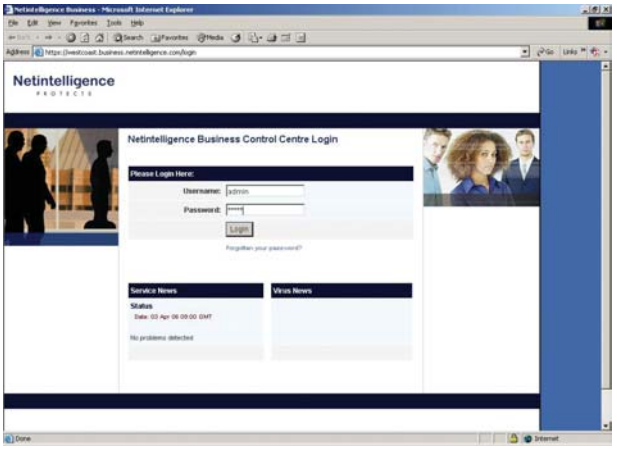
Net Intelligence says… about the Netintelligence Internet Security Technical Benefits

Netintelligence utilises the internet to provide the perfect mechanism for the enforcement of security policy at the end point level. The Netintelligence service offers a full web based deployment, administration and reporting platform, which can be controlled centrally and managed remotely. No additional hardware or system integration is required; organisations simply deploy a light client to each end point. Once installed, the client will manage both the activities of the user and will deliver unified threat protect at the same time. When connected to the internet, the client automatically receives new policies, updates and anti virus/spyware signatures without the need for any user intervention. The organisation receives real time user activity back from the clients - providing constant monitoring and a 'whole world' view regardless of the end point's location, connectivity or time.

www.netintelligence.com

Test report

Introduction



The Netintelligence solution is based around two separately available services that compliment each other to provide a fully-fledged web and email content filtering solution. Netintelligence takes a slightly different approach to Content Filtering to some other more traditional content filtering products, however such an approach does not mean that the end result is different.

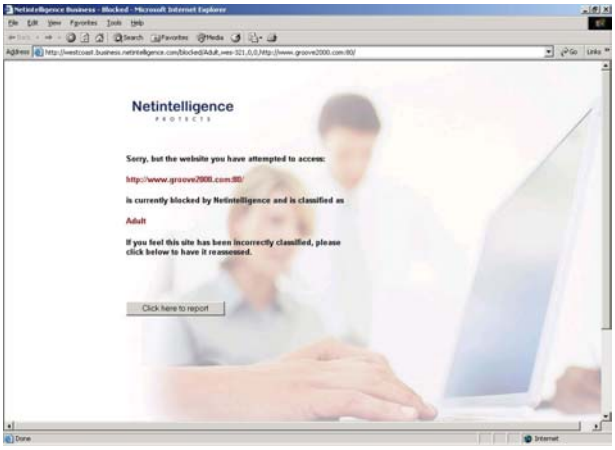
At its most basic level of explanation, the web filtering functionality is implemented by a piece of client software that is installed upon Windows user machines, and is then controlled via policies implemented through an SSL secured web interface. This client software provides continuous cover whenever an installed machine is connected to the internet and requires no extra hardware to be purchased. The solution also provides AntiVirus, AntiSpyware, Instant Messaging and P2P control. When a user does try to access a page outside of the Acceptable Usage Policy put in place by the administrator they will receive a block page informing them that they have been refused access to a particular site.

The second part of the Netintelligence solution is the email filtering protection. The procedure for setting this up involves switching the corporate mail exchanger (MX) records and then implementing a policy in a similar manner to the web filtering.

Test report (continued)

Installation and Configuration

For each machine that a company requires to be monitored, the web filtering is handled by a small piece of client software that is deployed to the box. This can either be installed via the Netintelligence interface itself, or a separate application may be downloaded that allows for a remote installation.



Once this client has been installed the machines can start to communicate back to Netintelligence, and not only can the filtering functionality commence, but also a series of reports may then be run about the machine itself. These include a Machine Summary, Installed Software and changes to the hardware and software to enable administrators to track changes.

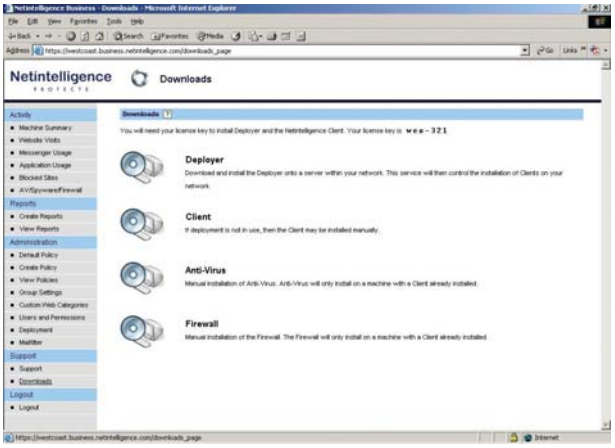
The set up of the email filtering side of the solution was also straightforward – the initial stage involves altering the corporation's MX records so that they are changed over to point to Netintelligence's servers. Once the changes have propagated around the relevant DNS servers, the default policy needs to be put in place and then protection can begin.

Setting up the default policy is an easy to understand and simple to implement process that involves the user logging into the same web interface as the web filtering, and then configuring a policy under the MailFilter heading of the Administration section.

Test report (continued)

The Interface

The main point of interaction is a web portal that is accessed over an SSL secured link that provides access to set up default rules for both mail and web traffic along with exceptions by group if necessary. These exceptions can allow, for example, the technical team in a company to access network security sites whilst the rest of the users do not have that ability.

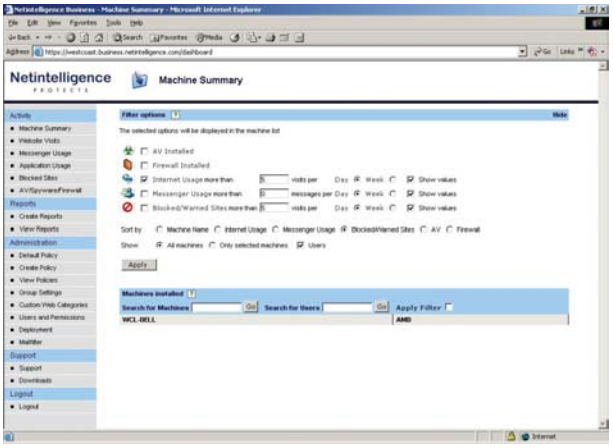


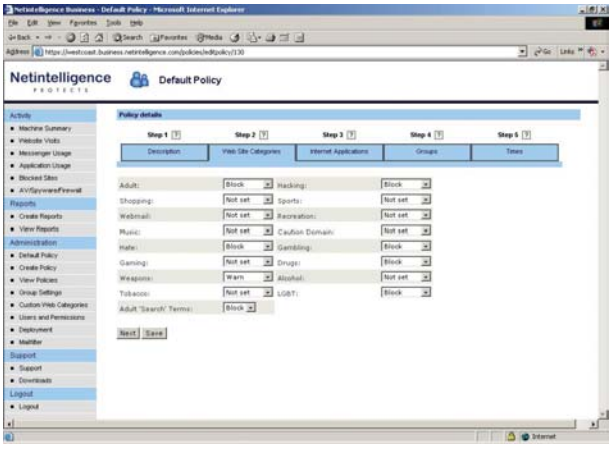
The interface itself has been designed with ease of use as the main priority, and have taken care to ensure that the users are not overwhelmed with too much data on any one screen, although this does not mean that the options available are in any way limited. Upon login, the user is presented with a list of machines that have the client software installed, along with their online status and a set of filter options that can be used to limit this display if required.

The main menu has been split into Activity, Reports, Administration and Support, with the majority of the options, as expected, being under Administration. From this section, users can alter the default policy, as well as create entirely new policies from scratch. This is a simple process, entailing not much more than a few keystrokes to enforce a wide-ranging Acceptable Usage Policy.

The Netintelligence solution has further broken down this web filtering policy creation and editing into a series of steps to make it even easier for users to implement, with the first stage of five involving giving the policy a name and description. Following this, the solution provides a list of categories and asks the user to specify actions that relate to each category.

Test report (continued)





Already supplied are pre-specified categories that cover subjects such as Adult, Weapons, Hate, Hacking, Drugs and Shopping, and user specified categories can be added in under a separate subsection of the main menu.

Each category may have one of four actions applied to it – Block, Allow, and Allow Only (which overrides all other options) are included, and there is also the useful option of Warn. This facility allows a company to let the users to view sites that might be on the edges of acceptability but reminds them that their internet activity is being monitored.

The next stage allows the users to lockdown internet applications. These currently include IM and P2P clients, newsgroup blocking and Computer Usage blocking which blocks any use of the affected machines.

The fourth stage of the process involves the specification of the groups to which the policy should apply. This ensures that different policies can apply to different users or groups within the company. After locking down the rules to the aforementioned groups, the final stage involves providing an active time frame for the enforcement of the policy. This has the scope of being restricted to individual days, weekdays or all days between specific time frames or a catch-all timeframe of Always.

The Activity part of the menu has a number of short summary reports as options – these include Machine Summary, Website Visits, Messenger

Test report (continued)

Usage, Application Usage, Blocked Sites, each of which can be restricted by both machine and user. There is also a section called AV/Spyware/Firewall that allows the Netintelligence AV and firewall software components to be downloaded onto machines that do not currently have them installed. Also displayed down the right hand side of the screen is a list of top ten viruses with links to an external site for verification.

Finally, the support section includes the manual downloads of the firewall, AV, and filtering client applications, PDF downloads of the manuals, and the ability to change the login password.

Mail filtering is controlled from a sub section of the Administration menu also, and leads off to a separate section of the interface running on a non-standard higher port. This has two major sections, Email and Reporting, and the configuration all takes place under the Email header.

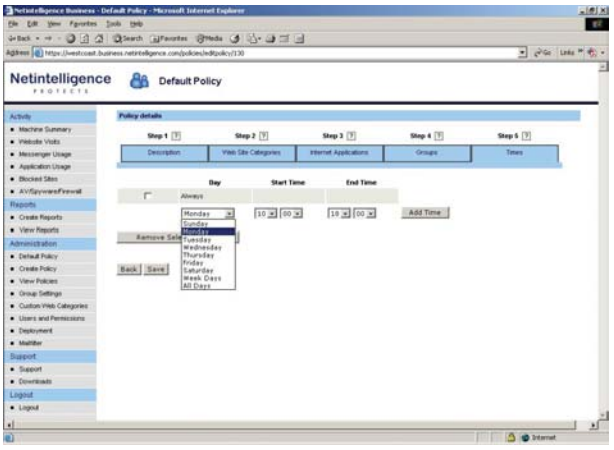
Policies are implemented using a Scenario-Response methodology. Several Scenarios and Responses are already in place, and the ability to either edit these or to create further custom conditions and actions is also in place. The creation of these is very simple, and as soon as they are built they can be incorporated into a policy.

It is possible to apply these policies to domains or groups or to individual accounts, and if the customer has only built an inbound content filtering policy, it is easy to apply a default or completely separate policy to outbound mail.

Also under the main section is Quarantine, for looking at mail where a policy has decided that a mail should be isolated, and phrase lists where there are several lists already supplied and once again, the ability to create custom phrase lists.

Test report (continued)

Testing



Web filtering testing was performed using a list of verified live links selected from the West Coast Labs test suite. These links were chosen to be indicative of both genuine web sites and sites outside of a normal Acceptable Usage Policy.

West Coast Labs uses proprietary software to automatically load these links into a browser both as a standalone test and with a background load of web traffic that is generated using specialist hardware.

The logs from the software were then examined to see if any sites had been allowed through, and these results were compared with the logs on the Netintelligence interface.

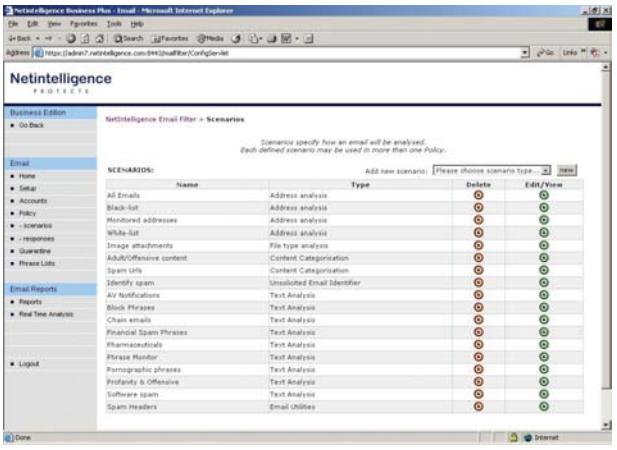
Mail filtering testing was performed using proprietary scripts to replicate both internal and external email and was performed over several separate connections. Along with genuine email traffic that replicates usual business usage and personal email there were several messages that contained phrases or words that fell outside of the Acceptable Usage Policy.

These scripts were run both as a standalone test and with a background load of mail traffic generated using specialist hardware.

The inboxes of the recipients were then examined to see if any messages had got through and were then compared with the logs on the Netintelligence interface.

Test report (continued)

Reporting



Reporting is split between the web filtering section and the mail filtering section. Within the Web filtering functionality it is further broken down into snapshot type reports in the Activity section, and more historical data under the Reports heading.

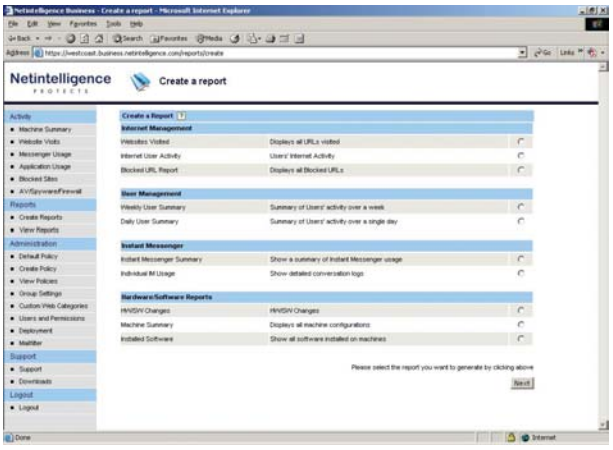
The Activity section reports allow daily and weekly summaries – each of these is a multi tiered report enabling drill down through the data so that it is possible to see exactly who has been looking at a given link. These reports are clear and concise – the illustrations that accompany them are well chosen and certainly add to the value that the reports give.

The Reports section itself deals with more historical data rather than currently snapshot data, and has only has two major options, however there is a wealth of flexibility within those.

The first is Create Reports that allow an administrator to specify the parameters that they wish to see starting with the type of report – these include historical data for all the major sections such as Blocked URLs, Internet User Activity and Websites Visited that are viewable from the Activity section. These reports can each be given a date and time range and there are various options that are related to specific reports. The second option is View Reports that allows a user to look at historical data for reports that have already been run.

Test report (continued)

Results



Following the completion of web testing, West Coast Labs can confirm that the Netintelligence service successfully detected all URLs used in this round of Web Filtering testing.

Following the completion of the mail testing, West Coast Labs can confirm that the Netintelligence service successfully stopped all mails containing offensive content used in this round of Email Filtering testing.

West Coast Labs' conclusion

An important element of the Netintelligence solution is the portability – both laptops and desktops may be protected and the protection is afforded whenever there is an internet connection.This coverage continues whether the device with the client installed is inside or outside of the corporate network.

The set up of the solution also allows portability of control via the secure link so that an administrator who is sitting, for example, with a laptop in an airport can easily control and monitor the situation back at a base site. This ability to ensure policy enforcement at any time and from any location will be appreciated not only by managers but also by the administrators that have to run the services.

Overall, this is a well thought out system that takes a slightly different approach to the problem of Content Filtering but still delivers on its promise. Easy implementation along with concise and well structured reports make this solution well worth investigation.

Having successfully detected all URLs and successfully stopped all mails containing offensive content used in this round of testing, West Coast Labs is therefore pleased to award the Netintelligence the PREMIUM level checkmark certifications for both Email and Web Filtering.

West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

Appendix 1 – Security Features Buyers Guide…

…as Stated by Netintelligence

Additional Security Features

Desktop Anti Virus (files, web pages and email filtration)
Desktop Anti Spyware (files, web pages and email filtration)
Desktop Firewall
Web Filtering & Blocking
Instant Messaging Application Control
Instant Messaging Conversation Recording
P2P Application Control
Binary Newsgroup Control
Computer Usage Control
Application Usage Reporting
Software/Hardware Changes reporting
Machine Asset Control
Machine Asset Build
Web Site recording & usage
Fully customisable policy setting by user, group, organisation
Full web based deployment tools
Full web based management control center
Clients communicate no less than every 10 minutes with the central servers
SOAP over SSL for communication
Service is fully redundant - based out of 3 network centres
Clients can not be removed unless user has admin rights
If end user 'kills process' - it is automatically restarted within 30 seconds
All patches, virus updates etc delivered automatically
Full integration with Mail Filter through control center
Web/content filtering utilise Netintelligence Databases of over 30 million digitally fingerprinted files and urls
Content of Netintelligence Databases assessed by human team - reducing false positives

Appendix 2

Email and Internet Acceptable Usage Policy

The following policy applies to all staff of Company XX ("the Company") and to those offered access to the Company resources.

Electronic media are of increasing importance to the Company, both internally and externally. The following policy gives guidance for appropriate usage.

E-mail - General Principles
In general, staff are expected to apply basic good judgement and common sense in their use of e-mail.

You should bear in mind that e-mails are not private to you. The Company has the right to monitor and/or record e-mails or electronic documents that you create, send or receive:

- For security and network management reasons;
- To ensure compliance;
- Where necessary in order to carry out the business of the Company;
- To prevent or detect a crime.

All e-mail recorded messages remain the property of the Company. Furthermore you should be aware that even when you delete a message, a back-up copy is likely to be retained.

You should also remember that e-mails are admissible as evidence in legal proceedings involving the Company. In addition, however carefully the system is protected, hacking is always a possibility and you should be wary of sending confidential information by e-mail. If in any doubt, make sure you ask your manager.

Appendix 2 (continued)

Limited personal use of e-mail is, at the discretion of your manager, acceptable. However, this must not interfere with your work or performance. Unreasonable personal use, including in particular the use of the system for personal business activities or a high volume of personal e-mails, will be considered a serious disciplinary offence.

Employees expressly shall not:

- Use e-mail for personal advertisements or participate in chain letters
- Send or solicit material that is thought to be obscene, abusive, defamatory, sexually explicit, offensive, racist or sexist to the recipient or any other individual or which is intended to annoy, harass or intimidate another person. The soliciting of such e-mails will be considered a serious disciplinary offence.
- Create e-mail congestion by sending trivial messages or unnecessarily copying e-mails.
- Download, copy or transmit to third parties, the works of others without their permission as this may infringe copyright.
- Download unlicensed copyrighted software.

The following are allowed:

- Internal regular reporting
- Sensible requests for information

As a rule of thumb, you must be as careful about sending an electronic message as you would a letter on the Company's headed paper. The Company may be liable for what you do from the Company network whether we know about it or not.

You are expected to protect the integrity, security and confidentiality of your data and equipment. Abuse of the e-mail system will be dealt with under the disciplinary procedure and serious breaches may result in dismissal.

Appendix 2 (continued)

Internet - General Principles:
Use of the Internet by Company employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the Company.

You should bear in mind that the websites visited by you may be monitored and/or recorded:

- For security and network management reasons;
- To ensure compliance with this policy;
- Where necessary in order to carry out the business of the Company;
- To prevent or detect a crime.

The Internet is to be used in a manner that is consistent with the Company's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

Corporate e-mail accounts, Internet IDs and web pages should not be used for anything other than corporate sanctioned communications. Users may be subject to limitations on their use of such resources.

The distribution of any information through the Internet, computer-based services, e-mail, and messaging systems is subject to the scrutiny of the Company. The Company reserves the right to determine the suitability of this information.

Employees are expressly forbidden to:

- Download, transmit or have possession of any pornographic material.
- Transmit, download or store any material that is thought to be obscene, abusive, defamatory, sexually explicit, offensive, racist or sexist or which is intended to annoy, harass or intimidate another person. Transmitting, downloading or storing such material will be considered a serious disciplinary offence.

Appendix 2 (continued)

- Download or install software from the Internet without prior approval from the Company's IT Purchasing department.
- Send or otherwise participate in chain letters.
- Transmit confidential or proprietary matters of the Company.
- Send customer/supplier related info over any public computer system unless with proper agreement and encryption.
- Infringe copyright laws.
- Participating in "chat rooms".
- Use the Company's computer resources to break into another site or to illegally obtain information from another site.

Infringement of these prohibitions will be dealt with under the Company's disciplinary procedures and serious breaches may result in dismissal.

Limited personal use of the Internet is, at the discretion of your manager, acceptable. However, this must not interfere with your work or performance. Unreasonable personal use, including in particular the use of the system for personal business activities or a high volume of personal Internet use, will be considered a serious disciplinary offence.