

Content Filtering Solutions

Why content filtering is essential

For all its obvious advantages, the internet has created a lot of problems for companies, governments and individuals. The provision of cheap, global communications and access to the World Wide Web brings undeniable benefits but can also be a channel for all sorts of criminal and offensive activity. So how do we keep the benefits while preventing the less savory aspects? There are no easy answers, and much depends on your point of view.

Internet purists, for instance, claim that traffic should be free to flow and that any form of control or censorship goes against the fundamental principles that have made the internet such a force in the world.

On the other hand, governments argue that it is their duty to monitor traffic. As we know, the internet is a convenient vehicle for all sorts of criminal activity, from international terrorism to money laundering.

To allow those communications to go unchecked would be irresponsible, as most people would agree.

Equally, few people would argue that hard-core pornography, particularly that involving children, should be allowed to travel unchecked over the internet. But then we start to get into gray areas. For example, while some societies may be comfortable with bare flesh and fruity language, others may find it offensive.

Attitudes to freedom of expression will also vary from society to society, and will tend to change over time. Remember that racist and sexist jokes were commonplace in the 1960s and 1970s but are now widely frowned upon in most Western societies.

So for most of us, a certain level of control and monitoring of email traffic and internet access are acceptable and even desirable. The only question is, how much.

In some sectors, there are hard-and-fast rules to help. Schools, for instance, need to show a duty of care for their students, and must prevent them receiving indecent messages or accessing inappropriate websites.

Companies also have a duty of care to their employees to protect them from unwanted material in the workplace, and they may have additional regulations to follow according to their particular industry sector.

Most companies will also want to protect confidential information from leaking out to competitors, which can easily happen in a free-flowing networked environment. Furthermore, the penalties for failing to show due care can be severe. In a recent notorious case, for example, a New England schoolteacher faced a jail term of up to 40 years for displaying lewd images on a classroom computer, although doubts over the computer's security protection have now forced a retrial.

Several companies have also faced lawsuits from employees because they failed to prevent racist or other offensive material from circulating on the corporate network. The employees argue they have a right to work in a clean environment, and that

their employers should take reasonable steps to ensure it happens.

The stakes for organizations are therefore high and rising, and they will also differ according to company size, industry sector and prevailing social attitudes. Fortunately, technology has advanced and provides a wide range of tools to help companies manage their email and web traffic to meet their specific needs. Equally important, the proper deployment of these tools can demonstrate a genuine will to comply with regulations and to protect users.

In reality, though, no technological solution alone will guarantee complete success. The criminals and purveyors of illicit material are constantly seeking new ways to avoid detection – image spam being just one recent example. The developers of security products continue to build extra intelligence into their systems to keep abreast of the changing threat landscape, but this is a cat-and-mouse game that shows no sign of ending.

All companies can do is train their staff well, deploy the right tools intelligently and make sure their defenses are kept up to date. This report is intended to help you choose the best product for your needs.

THE WEST COAST LABS TECHNICAL TEAM

Thanks to our content filtering project team at West Coast Labs, which comprises: **Matt Garrad, Richard Thomas, Rob Tanner, Chris Elias and Paul Jones**

westcoast labs

US Sales: Sue Collier - scollier@westcoast.com

UK Sales: Mark Thomas - mthomas@westcoast.com

China Sales: Jesse Song - jsong@westcoast.com

EMEA & Asia Sales: Chris Thomas - cthomas@westcoast.com

PureMessage for Unix Sophos

Developer's Statement

PureMessage for UNIX's flexible policy capabilities and multiple threat reduction technologies enable better security and greater control for multi-divisional or multinational corporations, email service providers and higher education institutions.

Product

Sophos PureMessage for Unix

Manufacturer

Sophos

Contact details

www.sophos.com

Full Product Test Report

www.westcoastlabs.com

Sophos PureMessage for Unix is a gateway email solution that can be installed on RedHat Enterprise Linux, SuSe Linux, Debian, Sun Solaris on SPARC and FreeBSD to give excellent coverage of the major enterprise-level *nix operating systems.

Users that are comfortable with *nix will find the installation straightforward. The software installs both its own Postfix installation and a PostGreSQL backend database to manage the quarantine facilities.

During installation, the user is prompted to enter not only details such as the DNS server that will be used (this is important, as there needs to be a DNS entry for the service to function properly), domain name



and server name as expected, but also some user details.

The first of these is a PureMessage specific user to start and stop the service. The second user is an administrator, used as an initial login to the manager interface. This interface is web-based, SSL encrypted, and runs on a non-standard high port.

Upon logging into this interface, the user is presented with a dashboard that gives an overview of the current status of the local services, plus shortcuts to the most common tasks, such as quarantine management and software updates. Also available are a series of options presented as tabs: Policy, Quarantine, Reports, Local Services, Server Groups and Support.

Every page has links to a well-written and clearly presented manual. The main page of each tab has an overview of

the functionality offered within the submenus, and each page also has a number of other help options specific to its place in the menu structure. These include an Administrator's Reference based upon the major group heading, and an About This Page link.

West Coast Labs' principal objective in the tests conducted was to test the ability of PureMessage to filter emails based upon a language policy – to this end, the server was set up with a number of users, each grouped into departments, and with different rules applying. Some groups were allowed to receive emails with medical terms that might otherwise have tripped language filters, and others had completely unfettered access to send and receive whatever they wished. Also included in the 'acceptable' usage policy applied, was the ability to scan for word obfuscation attempts – one of the common tricks used in order to get around systems such as this.

West Coast Labs' engineers not only used the selection of phrases (presented in regular expression type format) that comes supplied with PureMessage, but also tested against several phrases and words added in by hand. The policy manager allows exception lists to be set up quite simply.

WEST COAST LABS VERDICT

PureMessage for Unix offers a considerable amount of flexibility. It can adapt not only to the changing nature of the internet, but also to different types of organization, to make it a serious heavyweight contender for any Linux-based mail servers.

CHECKMARK CERTIFICATION

For full details of the Checkmark Certifications for PureMessage, please visit www.check-mark.com and use the search facility by vendor or product name.

Download the complete White Paper Product Test Report at www.westcoastlabs.com

