



ANTI SPAM SOLUTIONS TECHNOLOGY REPORT

SurfControl RiskFilter



JANUARY 2007

CONTENTS

SurfControl RiskFilter

SurfControl, Inc., 5550 Scotts Valley Drive, Scotts Valley CA, 95066, USA
Tel: (831) 440-2500 • www.surfcontrol.com

SurfControl plc., Riverside, Mountbatten Way, Congleton, Cheshire, CW12 1DY, UK
Tel: +44 (0) 1260 296 200 • www.surfcontrol.com



- Introduction3
- Test Network4
- Test Methodology5
- Product Testing Reporting6
- Checkmark Certification7
- The Product8
- Test Report9
- Test Results14
- West Coast Labs Conclusion15
- Security Features Buyers Guide16



INTRODUCTION



As the war for corporate inboxes intensifies, and unmonitored emails disrupt effective and secure working practices, Anti-Spam solutions continue to evolve to deal with this menace.

In this, the second Anti-Spam Technology Report, we examine the functionality and performance of the leading products in this market, which are aimed specifically at the SME network environments.

A key objective of the testing is to replicate the installation, configuration and use of the solutions in a real-world business environment to enable readers of the White Paper – prospective buyers – to make a meaningful assessment of the product that is right for protecting their corporate email environment.

Test Engineers have evaluated how the solutions install to ensure timely and effective spam protection. Consideration has also been given to the level of security administrator expertise and technical support required to facilitate both out-of-the-box operation and thereafter product training to ensure maximum effective spam protection.

This reports provides an independent assessment of effectiveness with regard to:

- The features and functionality of the solution.
- Integration into a network infrastructure.
- The level of user administration required to operate the product effectively.
- Spam detection capability and rates of detection.

TEST NETWORK

WCL has a number of domains that collect genuine spam. These domains receive varying levels of spam and are consistent with different email environments.

To reflect the email usage within a corporate environment, within each domain are a number of designated user accounts with a variety of email practices and needs including some that are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists.

The multiple domains designated for testing purposes were those that, between them, receive spam at a level consistent with the defined requirements of testing.

Software solutions included in the test program were installed on servers that meet the minimum specifications required by the vendor. Appliance-based solutions were installed on the network according to the vendor's recommended placing.

For hosted services, WCL testes through identified email domains and changed the MX records to divert the mail stream through the hosted service.

TEST METHODOLOGY



WCL initially performed the testing with an “out-of-the-box” configuration, changing only those settings on the solution needed to ensure correct operation in line with the vendor’s recommended installation and configuration procedures.

Further testing was then performed following the vendor’s advice for the tuning or training of the solution under test. WCL fine-tuned the solution each day of the test, spending no more than half an hour per day undertaking such work.

Throughout the course of testing, a mixture of email was sent to the test domains from other email addresses and domains controlled by WCL to mirror genuine email activity common in business, for example, requesting meetings, sending notifications to groups and non-business related social emails.

Emails were also sent from web-based accounts such as Hotmail and Google’s Gmail in order to simulate external users sending non-business related social emails, and home workers.

Thus, during the testing period the domains received some spam, some list/newsgroup mailings and “genuine” individual emails.

PRODUCT TEST REPORTING

Product evaluation addresses three specific areas* - Management/Administration, Functionality, Performance plus Additional Feature Testing.

1. MANAGEMENT/ADMINISTRATION

- Ease of Setup/Installation
- Ease of Use
- Logging and reporting function
- Rule creation
- Customization
- Content Categories

2. FUNCTIONALITY

- Email Processing Steps
- Allow/Blocking of Email
- Quarantine Area
- Additional functionality reporting
- Steps to Process Email
- Block Email Addresses
- Blacklist/Whitelist
- Allow Email Addresses

3. PERFORMANCE

- Volume or Percentage of spam detected
- False positive rate
- Spam incorrectly passed through
- Legitimate mail blocked
- Legitimate subscription mail blocked

CHECKMARK CERTIFICATION

Upon completion of the testing, individual product results are analyzed, resulting in accreditation to one of the two Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-

- Checkmark Anti-Spam Certification - Premium - 97% and over Catch Rate.
- Checkmark Anti-Spam Certification - Standard - 90% and over Catch Rate.



THE PRODUCT

SURFCONTROL RISKFILTER

With its hardened Linux kernel, flexible policy setting and robust connection management, SurfControl RiskFilter protects against viruses, phishing, confidential data leakage and spam in an easy-to-deploy secure messaging appliance.

<http://www.surfcontrol.com/products/email/riskfilter/>

SURFCONTROL SAYS ABOUT THE PRODUCT'S BUSINESS BENEFITS...

Every incoming or outgoing e-mail can expose your organization to viruses, spyware, confidential data loss, regulatory violations and more. To keep your business secure in the face of rapidly evolving threats, you need visibility, control and comprehensive protection customized to your own environment and policies.

SurfControl RiskFilter secure messaging appliance, powered by SurfControl's team of Global Threat Experts, offers continuous protection against inbound and outbound threats. With a hardened Linux kernel, a robust Mail Transfer Agent at its core, flexible policy setting and secure e-mail connection management, RiskFilter delivers enterprise-ready scalability and complete e-mail security with exceptional visibility and control.

<http://www.surfcontrol.com/products/email/riskfilter/>

SURFCONTROL SAYS ABOUT THE PRODUCT'S TECHNICAL BENEFITS...

SurfControl RiskFilter delivers lightening-fast performance and maximum uptime thanks to its advanced architecture. With a hardened Linux kernel, a robust Mail Transfer Agent at its core and secure e-mail connection management, RiskFilter allows enterprise-ready scalability and complete e-mail security. Remote Access via a secure Web browser makes it simple to delegate administrative rights and to hand off management elements to designated, appropriate managers, providing ease of administration, anywhere at anytime. Key administration features, such as updates to the Anti-Spam Agent and Anti-Virus Agent databases, can be automatically scheduled during set up so you have instant hands free administration.

<http://www.surfcontrol.com/products/email/riskfilter/>

TEST REPORT



INTRODUCTION

SurfControl's RiskFilter appliance is a rackmountable device designed to aid in the removal of spam as a threat to network stability. The front of the device provides access to the main power and reset switches along with the CD and floppy disk drives. To the rear of the appliance are located the PS2 mouse and keyboard connections, VGA port, and two network interface cards. Alongside these are serial cable connectors allowing for a direct console connection from a separate client machine. The fascia of the appliance is mounted on a swing-hinge granting easy access to the available controls and drives, without the need to constantly remove and replace the fascia.

Upon initial contact with SurfControl, the client is provided with a questionnaire requesting basic networking information relating to the intended network. Using this information, SurfControl then performs an initial setup procedure on the appliance allowing for a more rapid deployment to the host network. Also supplied with the appliance are a hardware guide and administrator's guide which are both detailed and well-written, aiding the deployment of the appliance to the network.

TEST REPORT

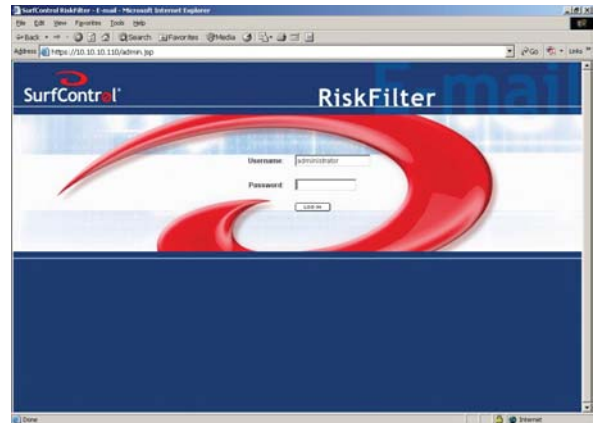
INSTALLATION AND CONFIGURATION

The correct installation and connection of the RiskFilter appliance is easily performed thanks to the descriptive Getting Started Guide that is supplied with the appliance. Once this initial hardware setup is complete the device must be registered so that the administrator may make full use of the update and security features supplied by RiskFilter.

Browsing to one of two available web-interfaces carries out activation of the RiskFilter appliance. Once logged in the user can enter the supplied activation code and is then requested to supply user information relevant to the system administrator. Once complete, access to the full list of features is granted and the appliance may be configured to best suit the needs of the organization.

For the purposes of this report, the main focus during setup was on the spam detection settings, however the device can also be further configured to protect the host network from email borne viruses. This protection is provided by the use of a McAfee anti-virus engine and provides the administrator with options to remove, quarantine, or clean the offending attachment(s). This engine is kept up-to-date using a realtime online update procedure.

Setup of the mail management, including the options relating directly to spam management, black and white lists, and mail relays, may be quickly carried out using the setup processes and procedures that are described in detail in the administrator's guide. The device may thus soon be configured to protect the host network.



TEST REPORT

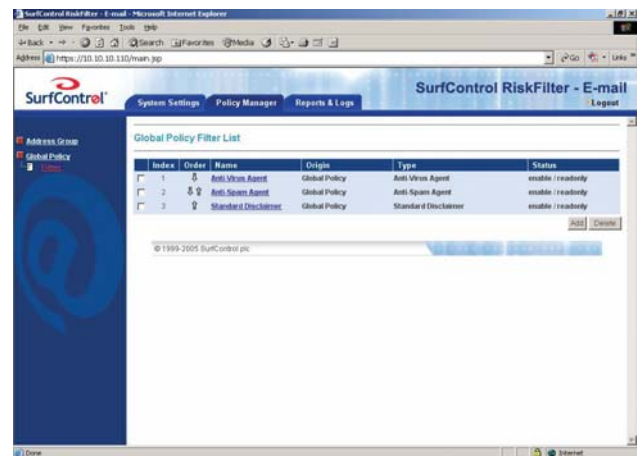
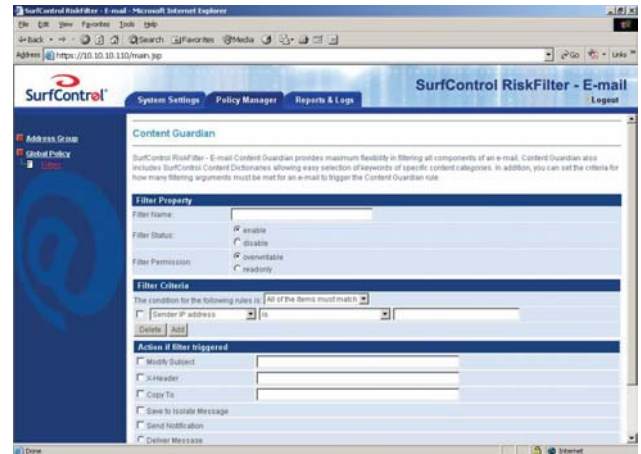
INTERFACE

Control of the RiskFilter appliance is split between two consoles, both accessed via a web browser across a secure SSL connection. Setup of the device, described earlier in the report, is carried out through RiskFilter System Management Console, which is available on the SSL connection and runs on a non-standard port. Logging into this interface presents the administrator with a clean and clear interface that is both easy to navigate and free from the multiple links found in some security appliances and solutions pointing to the same object or page. This easily navigated console allows for quick configuration changes and general day to day administration.

Across the top of this interface runs a series of three options, each providing access to relevant options: Webmin, System, and RiskFilter. The Webmin screen is automatically selected at login and provides the user with a further three option categories. From here the user may choose to allow or deny access to the appliance from a single IP address or range of addresses, change the port number on which the interface listens, enter proxy server information, and change language settings. Allowing the user to configure a single IP address from which to allow access helps harden the appliance against attacks and thus further protect the host network.

The System open allows access to alter information relating to the configuration of the RiskFilter appliance, including system time, network configuration, change passwords, running processes, and the ability to boot up and shut down. From the Network Configuration screen the administrator may alter the IP addresses used by the appliance along with the routing and gateway addresses. Selecting to view the running processes screen displays a list of every application currently running, along with their process ID, owner, and start date.

The final menu option is RiskFilter, which permits the user to perform updates to the RiskFilter email



TEST REPORT



system as well as the SurfControl OS. Also accessed from this menu are the Backup Manager and Cluster Wizard.

The second of the two web interfaces is also accessed across an SSL connection, but on a standard HTTP interface port as opposed to the non-standard port used by the RiskFilter System Management Console. This interface incorporates the same design as that of its counterpart. After logging into the appliance the user is presented with Risk Filter's Dashboard. This gives a brief appraisal of traffic information and reports on the status of the services running on the appliance.

Again similar to the System Management Console, there are three main option categories: System Settings, Policy Manager, and Report and Logs. Selecting one of these three categories displays a different list of options and clicking on each individual entry can further expand the list.

The first option under the System Settings tab is general. From here the user can configure SMTP welcome messages, the administrator's email address, the time in minutes before the console times out, proxy settings, and directory information for the storing of log files and archived messages. Beneath the General settings are the remaining five option categories: receive settings, send settings, user management, license and updates, and help.

Receive Settings enables the administrator to add sender addresses to either black or white lists, which can be entered as domain names or as IP addresses. Selecting to view the send settings allows for configuration of retry intervals and maximum length of time in which RiskFilter should keep trying to deliver a message. The help category provides access to a .PDF version of the administrator's guide and setup wizards, as well as providing a means of communication with the SurfControl support team.

Under the Policy Management tab the administrator is presented with four options: address group, queue manager, dictionary manager, and global policy. Possibly the most involving of these is the dictionary manager; it is from here that the administrator controls which words and phrases should be checked for when receiving mail and the relevant spam value to assign. There is a vast array of dictionaries to choose from, covering a wide variety of subjects such as adult, finance, pharmaceuticals, and narcotics.

TEST RESULTS

<u>Type of mail</u>	<u>Detected as genuine</u>	<u>Detected as SPAM</u>
GENUINE	100%	0%
SPAM	1%	99%

SurfControl's RiskFilter performed well, delivering 100% of the genuine mail correctly and correctly classifying 99% of the spam mail.

It is also worth noting that RiskFilter delivers a good proportion of grey and list mail as genuine. This gives an organization the flexibility and opportunity to define policies during a training period without missing mail that could potentially be business critical.

West Coast Labs is pleased to award RiskFilter the Premium Anti-Spam Checkmark.



WEST COAST LABS CONCLUSION



RiskFilter provides any organisation with a strong Spam defence system. This is enhanced by an easy to use interface that allows an Administrator to efficiently configure all aspects of the system.

A large variety of detailed reports are available, allowing an Administrator to keep up to date on all mail traffic within the network.

Overall, RiskFilter is a highly adaptive and intuitive, antispam system that would greatly aid any company or organisation in the constant fight against Spam.

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. When West Coast Labs provide test results for any particular product tested, said results are most relevant at the time of testing and within the context of the specific scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools utilized during that specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

SECURITY FEATURES BUYERS GUIDE

DEVELOPMENTS IN THE PRODUCT OVER THE LAST 12 MONTHS AS STATED BY SURFCONTROL...

Recent enhancements to SurfControl RiskFilter have been designed to deliver additional protection against spam and to help organizations address the broader risks posed by inbound and outbound e-mail including threats from viruses, phishing attacks, spyware, confidential data loss and regulatory violations.

Integration of SurfControl's industry leading database of categorized URLs allows e-mails containing malicious or inappropriate URLs such as phishing sites and sites known to contain spyware to be identified and stopped accordingly. Such URLs are often associated with spam and this provides a critical layer of spam defense.

Support of Transport Layer Security (TLS) allows RiskFilter to send and receive encrypted e-mail traffic, protecting the privacy of e-mails while travelling across the Internet. The implementation of Sender Policy Framework (SPF) helps guard against spoofed e-mails, phishing, fraud and spam and helps distinguish authentic messages from forgeries.

An innovative SMTP Greeting Message Delay feature has been added at the connection-level as a further important layer of protection against spammers. This instantaneous message delay instantly identifies scripted spam clients that do not wait for the initial SMTP greeting.

The addition of customizable spam rules and quarantine folders allows spam identified by different anti-spam techniques to be managed in different ways. For instance, spam identified with the digital fingerprint database has extremely low false-positive rates and customers often choose to delete this spam immediately. Whereas administrators may allow end-users to manage their own spam that has been captured by heuristic-type rules, delivering improved productivity and reduced administration overhead.

ADDITIONAL SECURITY FEATURES CONTINUALLY UPDATED DATABASES:

- Anti-Spam Agent including digital fingerprint and heuristic rules
- Integrated SurfControl URL Database
- Anti-Virus Agent powered by McAfee
- 150+ categorized and weighted dictionaries in multiple languages
- Team of 70+ located in 20 Countries identifying new threats

SECURITY FEATURES BUYERS GUIDE

SURFCONTROL REPORT CENTRAL:

- Real-time dashboard reporting
- Drill-down forensic reporting capability
- Pre-defined, customizable reports
- Delegated access via web-based interface

CONNECTION LEVEL PROTECTION:

- Denial of service protection
- Directory harvest attack protection
- Protected domain closed relay
- Reverse DNS Lookup and SPF authentication for spoofed e-mail protection
- Support for Real-time Blackhole Lists
- Defined trusted IPs for protection against spammers
- Remote user authentication
- Blacklists & whitelists
- Gateway-to-gateway encryption (TLS)
- SMTP Greeting delay

POLICY LEVEL PROTECTION:

- Inbound and outbound filtering
- Pre-defined and custom filtering rules
- Confidential information management
- Business compliance management
- Offensive content management
- HTML parsing and stripping
- Document decomposition
- Customizable dictionary threshold filtering
- E-mail bandwidth management

HIGH AVAILABILITY FEATURES:

- RAID 1 redundancy capabilities
- Support for clustering

[URL: http://www.surfcontrol.com/products/email/riskfilter/](http://www.surfcontrol.com/products/email/riskfilter/)