

The Enterprise Protection Suite



SurfControl E-mail Filter[™]

Messaging Security Made Simple & Effective

Every incoming or outgoing e-mail can expose your organization to damaging Internet threats—viruses, spyware, spam, phishing, confidential data loss, and more. To keep your organization secure in the face of rapidly-evolving threats—without draining IT resources—you need an e-mail security solution that is easy to administer and updated automatically against emerging threats. By controlling the threats, you'll benefit from enhanced security, increased productivity, optimized network resources and limited legal liability.

- **Manage Usage Policies & Compliance**
- **Reduce Costs & Administration**



Policy Management Made Easy

SurfControl E-mail Filter gives you flexibility and control, with an easy-to-use drag-and-drop rules engine including predefined rules for spam, blended threat and virus protection. Unlimited e-mail rules are fully customizable to your organization's needs, and can be grouped by threat category for ease of management. Managers can allow, delete, isolate, or delay any e-mail that triggers your organization's e-mail policy rules. Flexible notification options let you copy the appropriate manager, sender, and/or recipient based on the type of policy violation. Extensive message handling options include mail compression, stripping file attachments, HTML stripping, corporate disclaimers, and file attachment management. (See Screenshot No. 4)

Simplified Message Administration

Use SurfControl's Message Administrator to analyze and take action on isolated e-mails quickly and easily—the client or Web-based format make it simple to access remotely. Automatic management of each isolated queue deletes, releases, or saves e-mails after they have aged a designated length of time—for hands free administration.

Control and Convenience for End Users

Keep your employees' inboxes free from unsolicited mail, without getting in the way of mission critical e-mail. SurfControl's End-User Spam Management (EUSM) ensures that users receive all e-mail of a legitimate nature. EUSM enables e-mail users in your organization to manage their own suspected spam quarantine and to create their own whitelist and blacklist rules. (See Screenshot No. 8)

Secure Remote Management

SurfControl's remote management capabilities let you put e-mail content review into the hands of designated, appropriate managers in any location, providing flexible filtering for ease of management, anywhere at anytime. Managers can take action on questionable messages from their office or while on the road. Human Resources, IT, and other managers can remotely administer SurfControl and monitor activity, including reports, dictionaries, and authentication rights. (See Screenshot No. 5)

Flexible Deployment for Any Organization

SurfControl E-mail Filter puts you in control of your e-mail usage with flexible, scalable, and high-performance solutions to best fit the e-mail messaging security needs of your organization. SurfControl's gateway solution acts as a mail relay host and works with all standard SMTP mail servers, including Exchange, Lotus Domino, GroupWise, Sendmail, and others. (See SMTP Network Configuration No. 7)

Adaptive Threat Intelligence Service™ First to Detect ... First to Protect™

SurfControl's Adaptive Threat Intelligence Service powers SurfControl E-mail Filter with the dynamic Anti-Spam Agent Database and real-time threat technologies, providing, continuous, and comprehensive protection. SurfControl's Global Team of Threat Detection Experts provide 24/7 integrated analysis and research of all Internet threats, stemming from all Internet sources, ensuring security against emerging threats before they impact your enterprise.

Blended Threat Protection - Defense In Depth

■ Dynamic Threat Detection

■ **Anti-Spam Agent (ASA)** provides complete coverage for today's blended threat attacks, including spam, phishing fraud, and messages with malicious URL links. The ASA uses three powerful techniques to protect your business:

- **Digital Fingerprints**—continuously updated by our Global Threat Experts with the electronic fingerprints of e-mail risks in 17 categories—allowing your organization to define precisely what you want to treat as spam. (See Screenshot No. 1)
- **Heuristics**—uses thousands of rules to accurately analyze e-mail to detect "attack-like" characteristics and filter them according to the sensitivity you choose.
- **LexiRules**—provide rapid response protection against the newest blended threat attacks. Using advanced Boolean language analysis, LexiRules are precisely targeted at an outbreak to accurately identify new attacks as they emerge.

■ **Internet Threat Database** - Constantly updated URL filtering. The URLs listed in SurfControl's Internet Threat Database help companies ward off harmful Web links within e-mails, including spyware, phishing fraud, malicious code, and inappropriate content. The Internet Threat Database is constantly updated by SurfControl's Global Threat Experts to ensure automated protection and minimize your window of vulnerability to newly emerging threats. (See Screenshot No. 2)

■ **Anti-Virus Agent** - Protection against costly virus outbreaks. SurfControl's Anti-Virus Agent (AVA), powered by McAfee, protects organizations from virus infected e-mails. The AVA checks messages against the continuously updated virus signature database and allows the e-mail to be handled according to each company's policy—to clean, delete, or isolate the message.

■ **HTML Parser** - detects when an e-mail is in HTML format and automatically parses it to defeat spammer techniques designed to circumvent most e-mail filtering solutions.

■ E-mail Connection Management

■ **Closed Relay** - protects against attackers using your mail server to send their messages using an "Open Relay" since SurfControl is a Closed Relay Host.

■ **Denial of Service** - SurfControl can detect and protect you when your system is under attack.

■ **Directory Harvest Attack** - protects corporate e-mail systems by ensuring that the only mail getting into your network are the ones with valid recipient addresses.

■ **Reverse DNS Lookup Allow** - verifies the sender of each message against your configured spoof detection features.

■ **Realtime Blackhole List (RBL)** - supports multiple RBLs from third party RBL services and blocks messages sent from "open relay" servers.

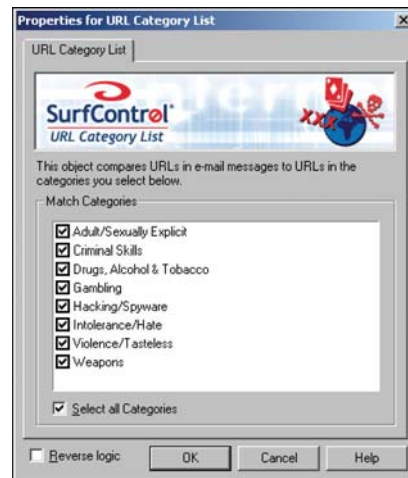
"The amount of time and labor this has saved us is extraordinary. The SurfControl E-mail Filter has been rock solid for us."

- **Michael Sherwood**
Chief Information Officer
City of Oceanside

1 Anti-Spam Agent



2 Internet Threat Database



■ Custom Risk Protection

- **Whitelists & Blacklists** - lets you create your own database of individuals from whom you do or do not want to receive e-mail.
- **Virtual Image Agent** - reduces legal liability by filtering out inappropriate adult images from your e-mail network.
- **HTML Stripper** - strips out active HTML code to defeat an attacker's efforts to launch a blended threat attack.

Reporting on E-mail Usage at Your Fingertips

SurfControl E-mail Filter leverages multiple techniques to get the most accurate possible picture of your organization's e-mail risks. SurfControl gives you the tools to identify the e-mail threats you currently face, and then implement simple rules to minimize their impact on your network and your business.

Easy to use and customizable, SurfControl's reporting capabilities put all the information at your fingertips—where e-mails are coming from and which policies are being triggered. Give secure access to managers in the business, schedule reports to be run on a regular basis, automatically e-mail or publish reports, and save reports in multiple file formats—all from an intuitive and easy-to-access Web-based interface. (See Screenshot No. 6)

■ Secure Your Confidential Data

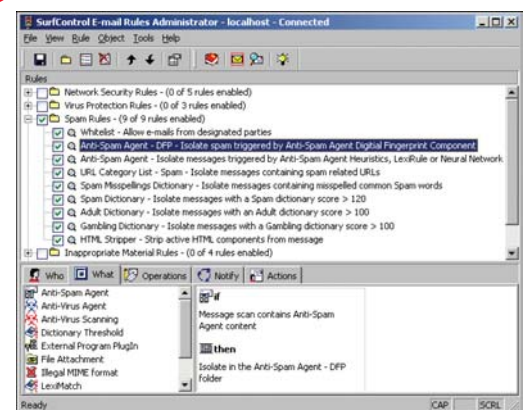
- **Customize Your Content Filtering** - SurfControl's customizable dictionaries provide quality content out-of-the-box and are extensively customizable to manage your compliance and confidential data needs. SurfControl provides 10 dictionary language packs covering 16 risk categories, allowing you to pick and choose which categories demand filtering and which are acceptable for business use. You can also create your own dictionaries focused on any category or language you choose.
- **Filter Content Simply and Effectively** - SurfControl's unique LexiMatch technology uses advanced Boolean language analysis making content filtering accurate and simple to deploy.
- **Intelligent & Dynamic Content Filtering** - SurfControl's unique Virtual Learning Agent (VLA) uses artificial intelligence to protect your business from e-mail risks like confidential data loss. The VLA can be easily trained to understand any content you choose. For confidential data it will learn to recognize your organization's unique critical documents, and then effectively control their distribution according to your e-mail acceptable use policy.

(See Screenshot No. 3)

3 Virtual Learning Agent



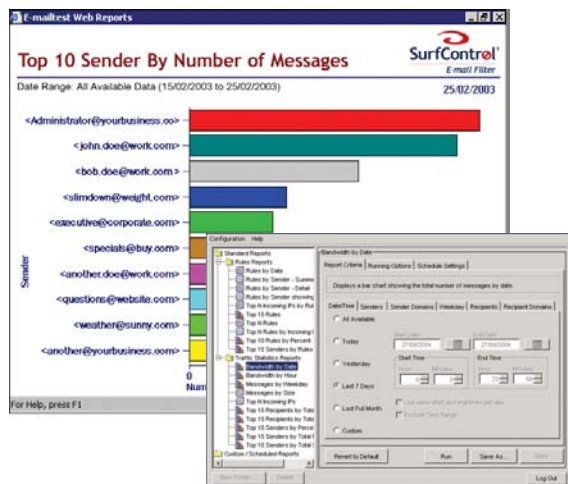
4 Rules Administrator



5 Remote Management



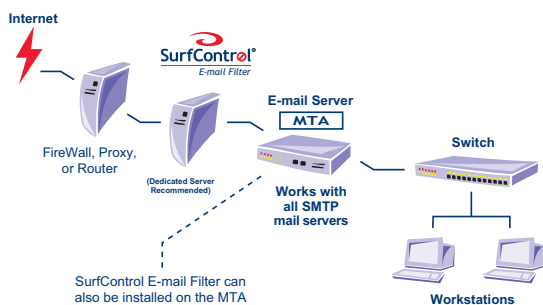
6 Reporting and Analysis



Unified, Multi-point Protection Keeps Your Enterprise Safe, **Productive** and **Profitable**

The emergence of sophisticated blended threats makes achieving airtight enterprise security more challenging than ever. SurfControl E-mail Filter works within the SurfControl Enterprise Protection Suite to provide nonstop protection for every point of vulnerability—the Web, e-mail, IM, P2P, and mobile workstations. SurfControl Enterprise Protection Suite fights spam, phishing, spyware, porn, viruses and malicious code even when they blend multiple methods of propagation. Inbound and outbound content is constantly filtered at the network perimeter and the desktop so that you can operate your business confidently and without interruption.

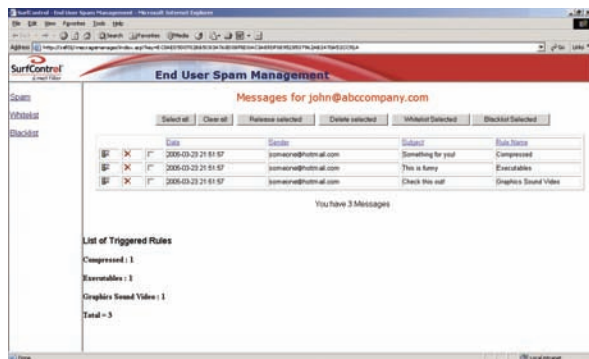
7 SMTP Network Configuration



■ Dynamic Threat Databases deliver continuous protection:

- Anti-Spam Agent™ stops blended threat attacks
- 17 threat categories
- Comprehensive international language coverage
- SurfControl Internet Threat Database detects malicious URLs inside e-mail messages
- Anti-Virus Agent™ scans and cleans virus infected e-mails
- Real-time Threat Technologies utilizes artificial intelligence to extend threat identification
- Virtual Image Agent™ scans and filters adult images
- Virtual Learning Agent™ is a unique A.I. based tool, which can be trained to protect your intellectual property.

8 End User Spam Management



Download and install your **FREE** no-obligation 30 day trial of any SurfControl product now.

www.surfcontrol.com