

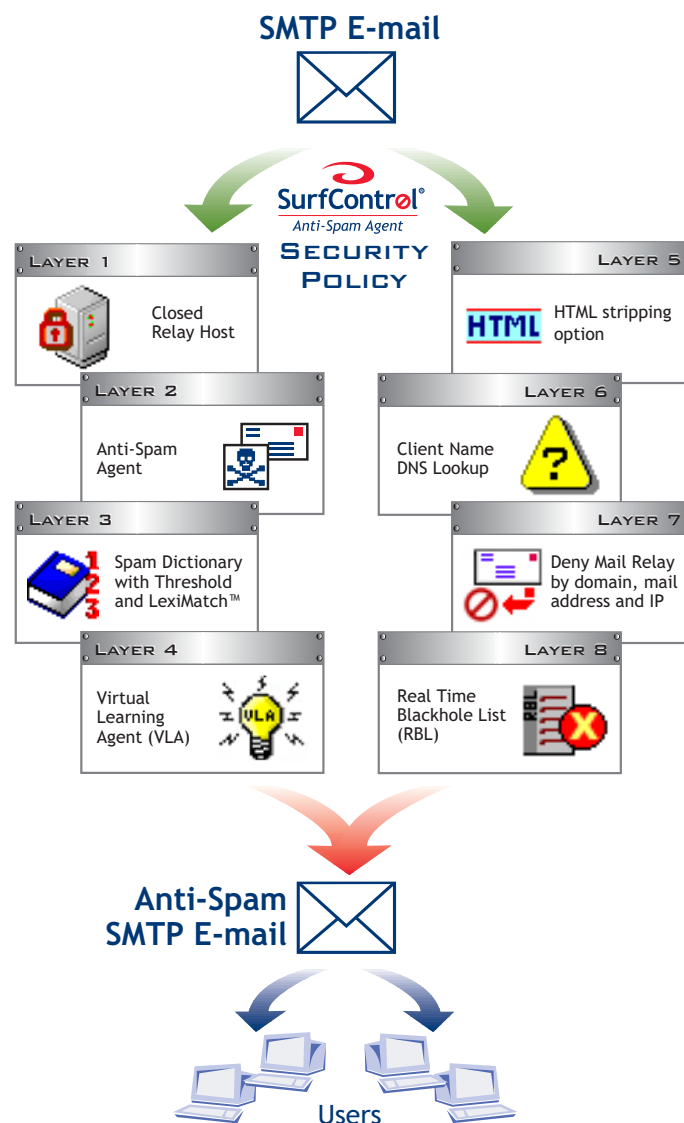
Anti-Spam Management with SurfControl E-mail Filter

Spam is a huge problem for companies. It's snowballing out of control and increasing exposure to legal liability risk, degraded bandwidth, lost productivity, and wasted network resources. According to research firm IDC, by 2005 the number of e-mails exchanged every day will exceed 35 billion. Estimates for the percentage of e-mail messages that can be classified as spam range from 20% to more than 60%.

Spam has become a major concern for enterprises struggling to cope with these unsolicited and nuisance, commercial and junk messages, often containing obscene or inappropriate content, which are flooding corporate networks and stuffing inboxes everywhere. Spam, if left unmanaged, has the potential to increase a company's legal liability, reduce productivity, and affect network resources and bandwidth.

Spam is challenging to manage as humans, spammers sending their latest offerings as well as coworkers sending jokes and junk mail to others, generate it. SurfControl's anti-spam management features offer the most intelligent and effective technology a company can use to protect its people, systems and business, because SurfControl E-mail Filter along with the optional Anti-Spam Agent has multiple layers of security for unparalleled spam protection.

Following the procedures listed in this document to implement the multiple spam layers using SurfControl E-mail Filter and its optional offerings will help effectively manage your organization's spam and junk mail.



Anti-Spam Feature	How to Implement this Feature
<p>Closed Relay Host</p> <p>SurfControl E-mail Filter is a Closed Relay</p>	<p>SurfControl E-mail Filter automatically protects against spammers using your mail server to send their spam messages using an "Open Relay" since SurfControl is a Closed Relay Host. SurfControl is "locked-down" by default ensuring that Spammers cannot take advantage of your presence on the Internet.</p>
<p>Anti-Spam Agent</p> <p>Anti-Spam Agent is an optional subscription capability of SurfControl E-mail Filter. ASA compares e-mails with a constantly updated database of known spam and junk mail and lets a company decide what content it wants to restrict or allow based on content like pornography, illegal or commercial or media type like JPEG, MPEG or GIF.</p> <p>SurfControl's unique digital signature recognition technology guarantees no "false positives" with ASA. This means only classified spam messages would be stopped and all appropriate e-mail will be delivered to the intended recipient.</p> <p>ASA's unique digital signature makes it highly effective against Spammers who change ISPs, IP addresses or use free temporary e-mail accounts.</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Rules Administrator • Enable the Spam Rule <ul style="list-style-type: none"> - Double Click on the Anti-Spam Agent object in the Spam rule properties and ensure that the desired ASA categories are selected. (Figure #1) - The default action is Discard, which takes advantage for ASA's 100% accuracy. If you would prefer to review these messages, change the action to Isolate. • Schedule daily updates to the Anti-Spam Agent through the Scheduler, which can be launched from the Start menu. • Have your employees make their submissions to the Anti-Spam Agent by emailing: submit@antispamagent.surfcontrol.com
<p>Spam Dictionary with Threshold and LexiMatch</p> <p>Use SurfControl's extensive Spam Dictionary and Adult Dictionary of spam-related words and phrases for lexical content scanning</p> <p>SurfControl provides detailed textual analysis, and both Dictionary Threshold and LexiMatch allow you to customize policies for your spam management.</p> <p>This provides heuristic detection of e-mail that is possibly spam and is useful for detecting new spam that has not been registered in the Anti-Spam Agent.</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Rules Administrator • Enable the Spam Rule • Double Click on the Dictionary Threshold object in the Spam rule properties and ensure that the desired Threshold weighting is selected. (Figure #2) <ul style="list-style-type: none"> - The Spam rule uses a Dictionary Threshold value of 120, so depending on how aggressive your organization wants to be the threshold value could be modified. A lower value could be configured for a more aggressive detection of spam messages, which could result in a greater number of false triggers. - Additional spam words can be added to the Spam Dictionary, and the Spam dictionary words and their weights can be customized to adjust your spam detection results. Word/phrase weightings can be customized to suit your spam filtering results, lower weights being more conservative and higher weights being more aggressive. • See Figure #3 for the overview of Spam rule • Enabling the Offensive/Derogatory rule will further help with spam management with use of the Adult Dictionary.
<p>Virtual Learning Agent</p> <p>This is a neural network engine that is pre-trained on the Adult Category (30% of Spam is estimated to be Adult in nature) among other categories. The VLA can also be pointed to a repository of spam messages in order to build an extremely accurate Neural Network that will recognize that type of message in the future.</p>	<p>To configure a rule once the VLA has been trained is a single drag-n-drop of the trained category</p> <ul style="list-style-type: none"> • Open the SurfControl E-mail Rules Administrator, and create a new rule. Enter a rule name and description. • Drag and drop the Virtual Learning Agent object, located in the What tab, into the rule workspace • Select the Adult category and any new Spam categories that you have created. • Drag and drop Isolate from the Actions tab and drop it below the VLA object in your rules workspace.
<p>HTML Stripper</p> <p>SurfControl E-mail Filter can be set to strip HTML out of e-mail message. People like to e-mail jokes, chain letters and other such seemingly harmless content to friends, family and colleagues in HTML format. That's why spammers and virus authors often embed malicious code in amusing, compelling and innocent looking e-mail messages.</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Rules Administrator, and create a new rule. Enter a rule name and description. • From the Tools Menu, select Options and activate the 'Show advanced objects' item. • Drag and drop the HTML Stripper object, located in the What tab, into the rule workspace • Select your desired HTML stripping option (Figure #4): <ul style="list-style-type: none"> - Remove active HTML components, choosing from the following: Scripts - JavaScript, VBScript, etc; IFrame - Independent HTML frames; Active links; ActiveX and software objects; Java applets - Remove HTML body from multi-part message and deliver the text-only message body - For HTML only message, remove all active HTML components - For HTML only message, remove HTML body, messages may be delivered with no body.

Anti-Spam Feature	How to Implement this Feature
<p>Client Name DNS Look up for Spoof Detection</p> <p>SurfControl verifies that the sender of each message matches their IP by using this feature. As people get more clever about avoiding spam, spammers are getting more sophisticated to avoid detection. For example, spammers are now disguising their e-mail addresses to look legitimate. With SurfControl's Client Name DNS look up, companies can block these messages</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Monitor • Select Server Configuration icon • Select the SMTP tab • Click Enable Client Name DNS Lookup. (Figure #5) • Choose one of the three options: <ul style="list-style-type: none"> - Log the mismatch - Deny the e-mail if no DNS record for the message header IP address exists. - Deny the e-mail if the DNS does not match the IP address in the HELO string of the message header.
<p>Deny Mail Relay by domain, mail address, and IP</p> <p>You can manage your own RBL type database by entering in the information of known individuals you want to block.</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Monitor • Select Server Configuration icon • Select the SMTP tab • In the Lists section of the UI, right click on Deny List <ul style="list-style-type: none"> - Enter the details of either the domain, e-mail or IP address you would like to deny. (Figure #6)
<p>Real Time Blackhole List (RBL) support</p> <p>SurfControl supports multiple RBL services from third party RBL services.</p> <p>When an e-mail server connects to SurfControl, the connection presents the IP address of the sending host. SurfControl will check against all the subscribed RBLs and verify if the IP address is any of these lists.</p> <p>If there is a match, SurfControl will disconnect the server with an SMTP (RFC821) 552 - You have been Black-listed.</p>	<ul style="list-style-type: none"> • Open the SurfControl E-mail Monitor • Select Server Configuration icon • Select the SMTP tab • Click Enable RBL DNS Lookup. (Figure #7) <ul style="list-style-type: none"> - Subscribe to one or more RBL services of your choice. A few are: <ul style="list-style-type: none"> - Mail-abuse.org - dsbl.org - relays.osirusoft.org - Spews.org • In the Lists section of the UI, right click on Anti-Spam Servers (RBL) <ul style="list-style-type: none"> - Enter the details of RBL service you would like to use. (Figure #8)

Figure 1:
Anti-Spam Agent

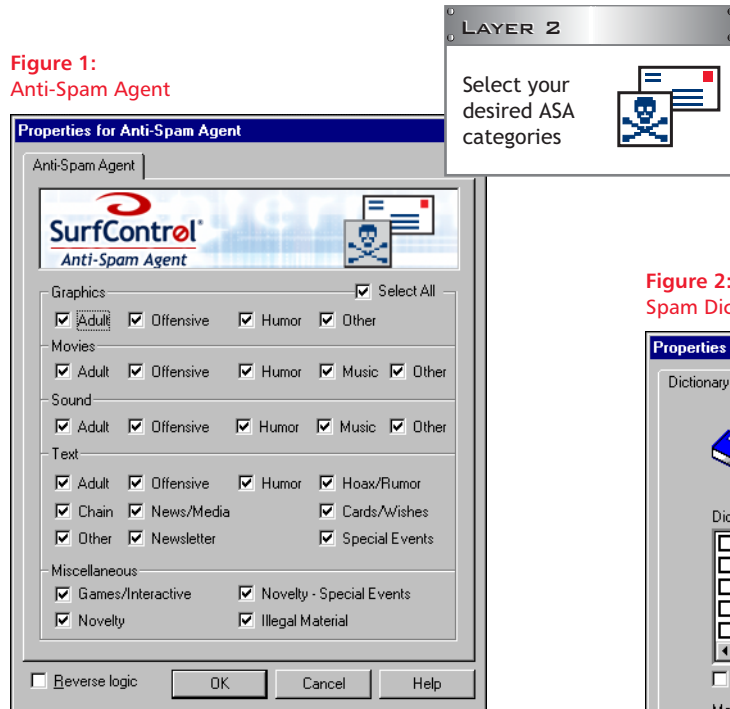


Figure 2:
Spam Dictionary Threshold

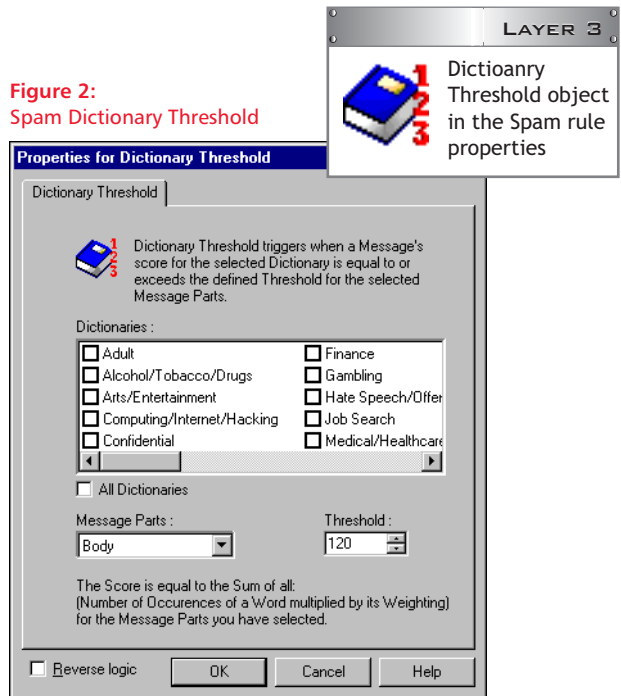


Figure 3:
Completed Spam Rule

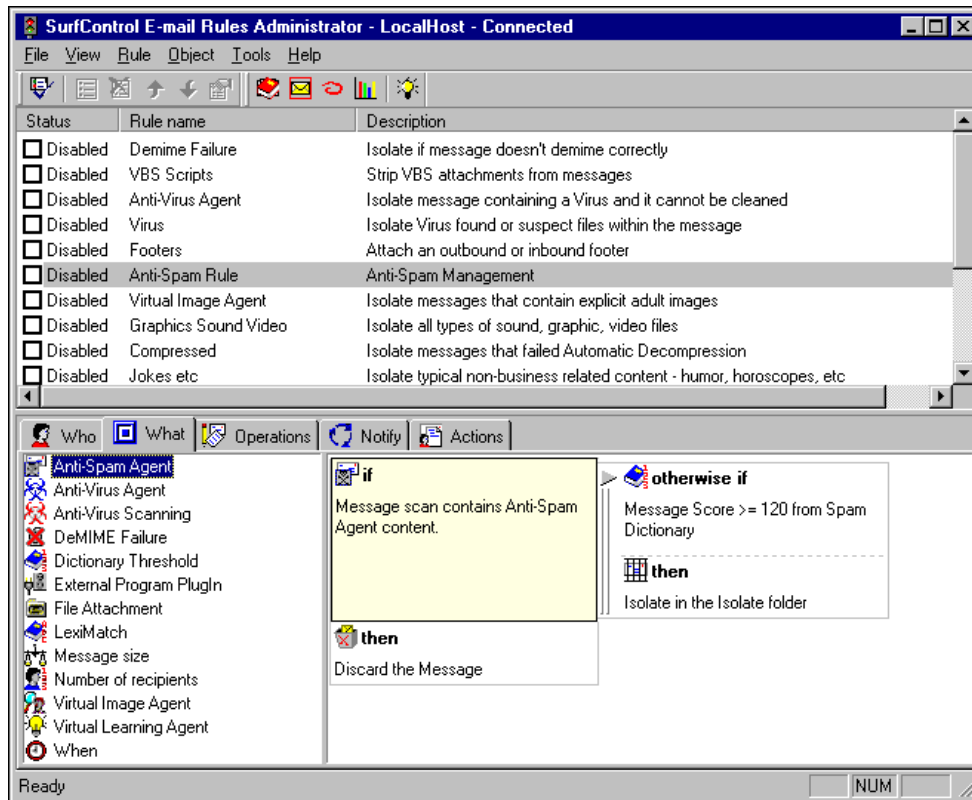


Figure 4:
HTML stripper

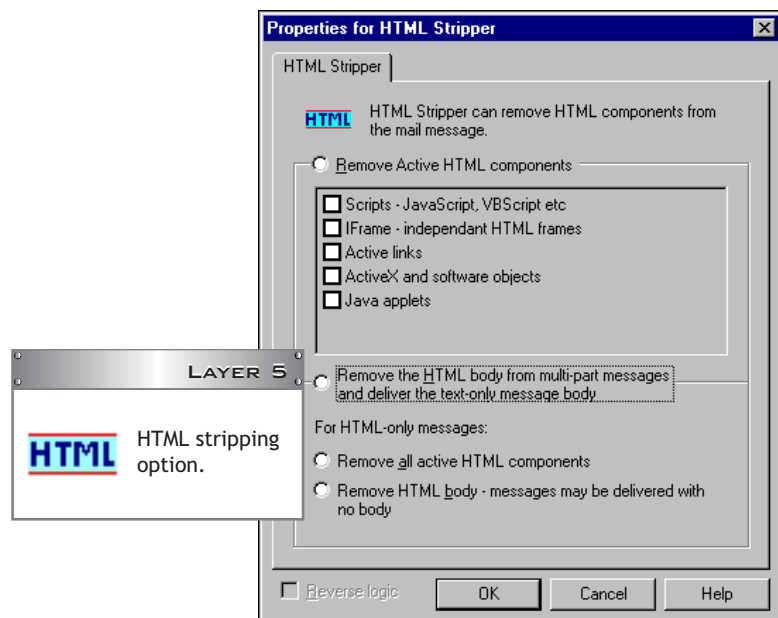


Figure 5:
DNS/server configuration

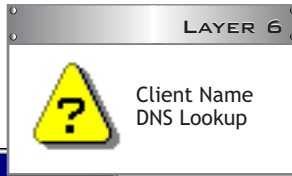
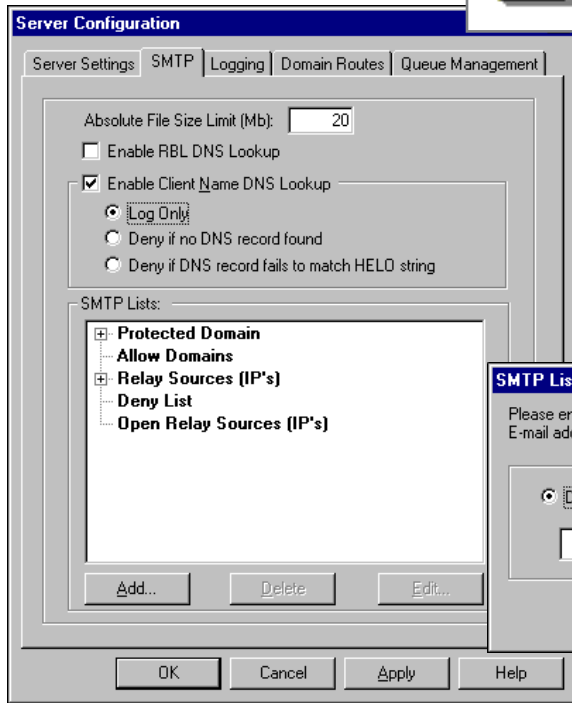


Figure 6:
Deny mail from these domains, etc

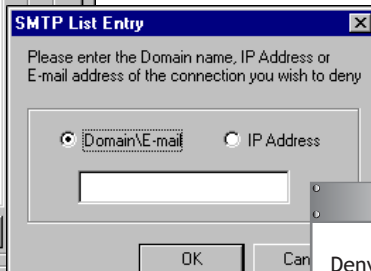


Figure 7:
DNS/server configuration

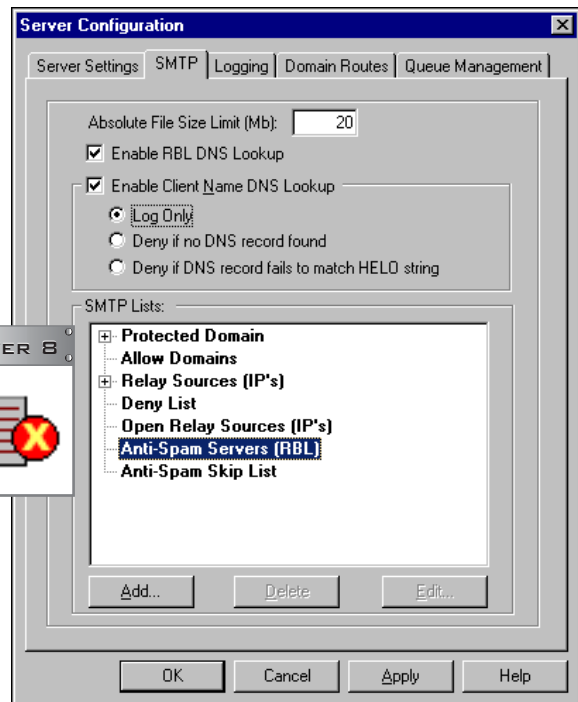


Figure 8:
RBL List services

